Toward Spoofing-Resilient and Communication-Integrated MmWave Radar Sensing

Kun Qian
kunqian@virginia.edu
University of Virginia

Parth Pathak
phpathak@gmu.edu
George Mason University

Abstract

MmWave FMCW radars are integrated into many sensing systems for robust sensing. However, their sensing functions are vulnerable to spoofing attacks and interfered with by backscatter communications, both of which can cause sensor malfunction and system failure. Noticing that radar spoofing and communication share similar signal modulation mechanisms, in this paper, we present SCR, a new Spoofing-resilient and Communication-integrated Radar sensing scheme. SCR is based on the rigorous analysis of the radar sensing model that highlights the differences between modulated spoofing and communication signals and normal sensing signals reflected by natural objects. The key designs of SCR are a novel chirp configuration scheme and signal processing pipeline, which signify different patterns between modulated and normal signals in radar spectra, for reliable detection of spoofing and communication. We have developed SCR and tested it with actual 77 GHz mmWave radar sensors and backscatter prototypes. Our field tests show that SCR can reliably detect fake objects created by modulated signals in both velocity and distance radar sensing domains.

CCS Concepts

• **Hardware → Sensor applications and deployments**; **Wireless devices**.

ACM Reference Format:
Kun Qian and Parth Pathak. 2025. Toward Spoofing-Resilient and Communication-Integrated MmWave Radar Sensing. In *The 23rd Annual International Conference on Mobile Systems, Applications and Services (MobiSys '25), June 23–27, 2025, Anaheim, CA, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3711875.3729155

1 Introduction

Millimeter-wave (mmWave) frequency modulated continuous wave (FMCW) radars are used in a variety of sensing systems nowadays to enhance situational awareness, such as autonomous driving [11, 35, 36, 53], SLAM [18, 34, 44], person monitoring [22, 33, 52, 54], remote health [10, 42, 48], and material analysis [23, 40]. Compared with light-based sensors, mmWave-based sensors enable new sensing functionalities, including sensing through visual blockage [55], sensing around blockage [7], sensing in the dark [43], and coherent velocity measurement [15]. These functionalities bring extra sensing robustness, which is crucial for many safety-critical applications. For example, autonomous vehicles can use mmWave radars to monitor surrounding traffic even under adverse weather or behind obstacles robustly, where cameras and lidars may fail [38, 51].

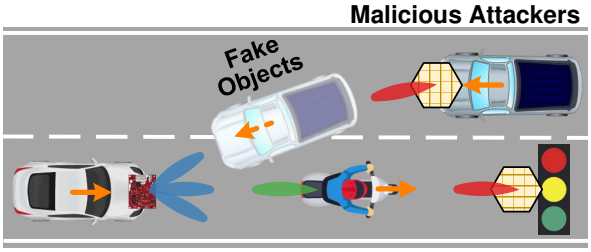

Figure 1: Application of SCR in intelligent transportation. The orange arrows indicate the objects' moving directions.

In addition to exploring new sensing applications and functionalities with mmWave radar, some studies intend to answer the following two questions further:

i) *Is mmWave radar sensing really secure?* Despite being robust against natural environment conditions, mmWave radars are vulnerable to physical adversarial attacks, especially spoofing attacks [27–29, 32, 47, 49]. A spoofing attack manipulates and backscatters the radar signals to force the victim's radar to detect "ghost" objects with false distances, velocities, and angles. Spoofing attacks are hard to detect, since the attacking signals resemble those reflected by actual objects. They pose severe security threats to sensing systems that rely on mmWave radars. For example, an attacker at the roadside can manipulate the radar signals such that the approaching victim's radar measures a false distance from the attacker. Upon falsely ranging the attacker, the radar may trigger the vehicle to apply a sudden brake, potentially causing fatal results.

ii) *Can mmWave radar do more than just sensing?* This question leads to studies on radar backscatter communication [1, 4, 25, 31, 37], which originates from the idea of integrated sensing and communication (ISAC). ISAC enables the sharing of spectrum and hardware between sensing and communication, substantially reducing device cost and form factor while embedding intelligence into network infrastructures. A backscatter tag conveys information to radar by receiving, modulating, and re-radiating radar signals. Ideally, radar backscatter communication can simultaneously support high-precision sensing and massive concurrent communication, potentially reforming the paradigms of many radar applications. For example, with tags attached to transportation infrastructure (*e.g.*, road signs and traffic lights), autonomous vehicles can use mmWave radars to localize them and fetch their information (*e.g.*, real-time speed limit and light color) in all weather conditions.

From the view of radar sensing, both spoofing and communication using backscatters create similar adversarial effects, as they both *modulate non-zero frequency shifts* to radar signals. They are

MobiSys '25, Anaheim, CA, USA

ACM ISBN 979-8-4007-1453-5/2025/06
https://doi.org/10.1145/3711875.3729155

similar to frequency shifts induced by the propagation delay of signals reflected by surrounding natural objects, and a standard FMCW radar will misinterpret them as fake distances and velocities [16, 49]. To accurately detect modulated signals, existing studies use sophisticated chirp configurations or modulation schemes. However, they tend to compromise radar sensing by introducing misleading interferences or reducing sensing range and resolution. For example, to detect spoofing attacks, the radar can transmit chirps with varying parameters and detect discrepancies of modulated frequency shifts [20]. However, chirps with different parameters can not be coherently combined, degrading the radar sensing performance. For backscatter communication, CDMA codes can be used to filter out irrelevant frequency components [8]. However, they spread out modulated signals in radar spectra and interfere with larger sensing regions. Thus, we seek a solution that can detect modulated signals from both spoofing and communication reliably without sacrificing the sensing capability of normal signals.

In this paper, we propose SCR, a new *Spoofing-resilient and Communication-integrated Radar sensing model*. SCR comprises a novel chirp configuration scheme and a signal processing pipeline, with which a radar can detect modulated signals from either spoofing attackers or communication tags while retaining the sensing capability as using the standard chirp configuration scheme and signal processing pipeline. SCR can be seamlessly integrated into any radar sensing scenario. Fig. 1 illustrates how SCR fits in intelligent transportation. The automotive mmWave radar transmits FMCW signals (blue) and may receive signals from three types of objects, *i.e.*, communication tags, spoofing attackers, and natural objects. SCR detects the presence of tags and attackers, as their modulated signals (red) exhibit different patterns from those (green) of normal objects. After detection with SCR, the modulated signals can be further processed to determine whether the target is a legitimate tag or a malicious attacker.

Distinguishing between modulated and normal signals with a standard FMCW radar is challenging because both types of signals create similar peaks in the radar spectra. To overcome this challenge, we revisit the basic radar sensing model and identify the tiny but critical discrepancies between the modulation-induced and delay-induced frequency shifts in radar signals. On this basis, we propose a more rigorous radar sensing model as the guideline for reliably detecting modulated signals. Frequency shifts determine the locations of signal peaks in the two dimensions of radar spectra, *i.e.*, *distance and velocity*. Given a non-zero modulation-induced frequency shift, SCR needs to detect its effect in either the velocity or distance domain.

For the *velocity* domain, we exploit that modulation-induced frequency shifts remain constant while delay-induced frequency shifts vary even within a chirp, as shown in Fig. 2b. Such difference is due to the fact that delay-induced frequency shift is caused by the Doppler effect and is proportional to the frequency of the radar signal. As the chirp's frequency increases linearly with time, the delay-induced frequency shift varies accordingly. In contrast, the modulation-induced frequency shift is solely determined by the modulation rate of the backscatter and is thus constant. This phenomenon is overlooked by existing radar spoofing attackers and communication systems, since the variance of the delay-induced frequency shift is orders of magnitude smaller than the absolute Doppler frequency shift. In contrast, SCR can detect this variance reliably using the sufficiently wide bandwidth of mmWave radar (*e.g.*, 77-81 GHz). Specifically, we propose a *chirp-splitting* scheme, which splits a chirp into two sub-chirps with different frequency bands. SCR calculates velocity spectra for both sub-chirps. By checking peak location variances in the spectra, SCR can detect modulation-induced frequency shifts in the velocity domain reliably.

For the *distance* domain, we exploit that modulation-induced frequency shifts cause aliasing peaks in the velocity domain, while delay-induced frequency shifts don't, as shown in Fig. 2c. This aliasing effect is due to the fact that the frequency range of the velocity domain is much smaller than that of the distance domain. It has been used by spoofing attackers in joint distance and velocity attacks [20, 49]. Fortunately, we find that the aliasing effect only appears when the chirps are transmitted at uniform time intervals, following the Nyquist Sampling Theorem [19]. Thus, SCR employs the nonuniformly sampled chirps to destroy the conditions where this aliasing effect appears. Specifically, we propose a *frame-splitting* scheme, where SCR splits the chirps in a radar frame into two groups. The odd-numbered chirps are uniformly sampled, and the even-numbered chirps are nonuniformly sampled. SCR calculates radar spectra for both groups of chirps. By checking the presence and absence of peaks in the two spectra, SCR can detect modulation-induced frequency shifts in the distance domain reliably.

We implement SCR with a 77 GHz FMCW radar and a backscatter prototype, and conduct extensive field experiments in both indoor and outdoor scenarios to evaluate SCR. Our experiments show that SCR can reliably detect almost all modulated signals from spoofing and communication in various settings. SCR does not modify the parameters of each single chirp in a radar frame. Thus, aside from detecting modulated signals, the mmWave radar can still coherently combine all chirps to achieve distance and velocity sensing performance similar to using standard radar frames with uniform sampled chirps and consistent chirp parameters.

In summary, our main contributions are:

(i) We provide a rigorous analysis of the radar sensing model. The analysis reveals the tiny but critical discrepancies between modulated signals from spoofing and communication and normal signals from objects, laying the theoretical foundation for SCR.

(ii) We design SCR, which is the first spoofing-resilient and communication-integrated radar sensing scheme. SCR can reliably detect modulated signals from spoofing and communication, without sacrificing the radar sensing performance.

(iii) We conduct experiments to verify the feasibility and usefulness of SCR for secure and reliable radar ISAC in real use cases, such as intelligent transportation.

2 Preliminaries

2.1 Principle of FMCW Radar Sensing

A mmWave radar sensor transmits FMCW signals (chirps), whose frequency increases linearly with time. Upon reaching an object, the signal is reflected and returned to the radar. The propagation of the received (Rx) signal introduces a delay compared to the transmitted (Tx) signal, creating a frequency shift between the Tx and Rx signals, denoted by f_δ, as shown in Fig. 2a. Given the frequency slope γ, the radar can estimate the propagation delay as $\tau = \frac{f_\delta}{\gamma}$, and the object's

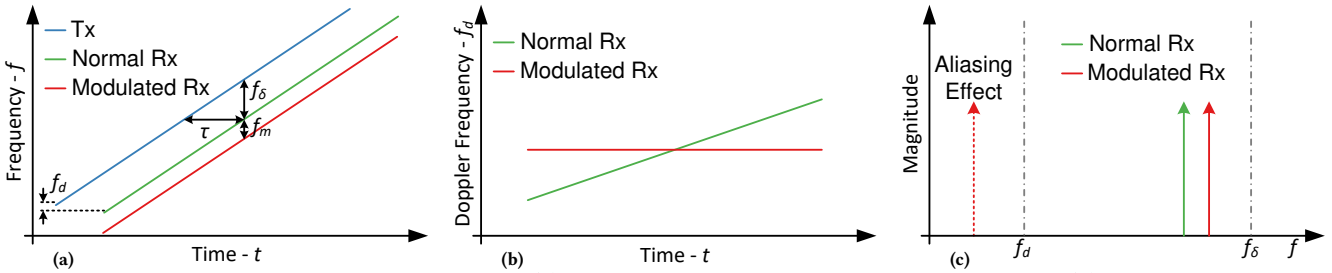

Figure 2: Illustration of radar sensing principle. (a) Frequency shifts between Tx and Rx signals. (b) Comparison between Doppler frequency shifts of normal and modulated signals. (c) Aliasing effect of modulated signal.

distance as $d = \frac{c_0 \tau}{2}$, where c_0 is the speed of light in free space.

To estimate the velocity of an object, the mmWave radar transmits a sequence of chirps and measures the Doppler frequency shift caused by the relative motion between the radar and the object and the change of propagation delay of the signal. As shown in Fig. 2a, the Doppler effect causes a shift f_d to the chirps, which is orders of magnitude smaller than f_δ. Then, the radar can estimate the object's velocity as $v \approx \frac{c_0 f_d}{2 f_c}$, where f_c is the center frequency of the chirp. The velocity v is only the radial velocity of the object. Nonetheless, it is a critical indicator of the object's motion in many scenarios, such as intelligent transportation.

In practice, a radar first applies the Fast Fourier Transform (FFT) to each chirp to obtain the distance spectrum. Then, the radar applies the IFFT across all chirps to obtain the velocity spectrum. Finally, the prominent peaks in the 2D distance-velocity spectrum are detected using the Constant False Alarm Rate (CFAR) algorithm.

2.2 Radar Spoofing and Communication

Radars are used by various sensing systems to perceive environments. Spoofing attacks aim to manipulate the distance and velocity measured by the radars and cause the sensing systems to misbehave. We assume that the adversary has a sensing unit and an attacking unit. The adversary does not need prior knowledge of the victim's radar configuration but uses the sensing unit to receive signals transmitted by the victim's radar and estimate the signal parameters, such as start frequency, chirp slope, and chirp time. Based on this information, the attacking unit calculates the modulated frequency shift and applies it to the following received signals via a backscatter. The backscatter only passively reflects the modulated signals and does not require synchronization with the victim's radar. Without knowledge about the adversary, the victim's radar can only normally treat the signals reflected by the attacker and obtain spoofed distance and velocity. In contrast, a communication backscatter simply modulates data with pre-defined frequency shifts. However, it still unintentionally interferes with standard radars that do not support backscatter communication.

Despite having different objectives, radar spoofing and communication share similar mechanisms for manipulating radar signals. Specifically, both of them introduce non-zero frequency shifts f_m to radar chirps, creating fake peaks in radar spectra. For example, mmSpoof [49] applies frequency shifts from 0 to 400 kHz to spoof both the distance and velocity of the attacker. Omniscatter [1] uses 150 kHz FSK signals for backscatter communication. Fig. 2a shows the returned chirp created by a backscatter. The chirp experiences a modulation-induced frequency shift f_m in addition to the delay-induced frequency shifts f_δ and f_d. f_m can be generated by modulating the reflectance or phase of the incident radar chirps using RF switches or mixers [1, 46, 49].

The modulation-induced frequency shift f_m can create fake peaks in both the distance and velocity domains of radar spectra [20]. Specifically, the distance of the fake object is shifted by $\Delta d = \frac{c_0 f_m}{2\gamma}$, and the velocity is shifted by $\Delta v = \frac{c_0 f_m}{2 f_c}$, away from the actual distance and velocity of the backscatter. f_m is usually comparable to f_δ to create a significant distance shift and much larger than f_d, *i.e.*, $f_m \sim f_\delta \gg f_d$. Hence, Δv is much larger than the range of the velocity domain, and the radar can only observe the aliasing peak within the range $\left[0, \frac{1}{T_c}\right)$ of the velocity spectrum, where T_c is chirp time, the sum of the ramping time T_r and the idle time T_i. This aliasing effect is illustrated in Fig. 2c and has been exploited by existing radar spoofing attackers [49] to decouple the spoofing of distance and velocity.

Unfortunately, the standard radar signal processing pipeline in Sec. 2.1 cannot distinguish modulation-induced frequency shifts from delay-induced ones. Fig. 3 compares the peaks of the two types of frequency shifts in the radar spectra from a simulation. To create the delay-induced frequency shift, a point scatter is placed 5 m away and moves at a velocity of 1 m/s. In contrast, a modulation frequency is calculated and applied to the chirps to create the fake peak at the same locations in the velocity and distance spectra. As the two peaks have similar magnitudes and are very close to each other, it is difficult for the radar to distinguish them. Although the two peaks exhibit different power leakage levels, distinguishing power leakage patterns is extremely difficult in practice due to the lack of ground truth, interference from objects nearby, and noises.

2.3 Detecting Spoofing and Communication

Existing studies mainly rely on randomizing chirp parameters to detect modulated spoofing or communication signals. That is, the radar transmits a sequence of chirps with different parameters, such as slope, chirp time, starting frequency, or starting phase. As a result, the same modulation-induced frequency shift f_m may yield inconsistent patterns in the radar spectra, and can thus be detected. For example, to countermeasure spoofing attacks, the hybrid-chirp scheme [28] alternates the chirp slopes so that a modulation-induced frequency shift creates inconsistent distance shifts. Similarly, BiScatter [31] uses alternating chirp slopes as the preamble for reliable detection and synchronization of backscatter

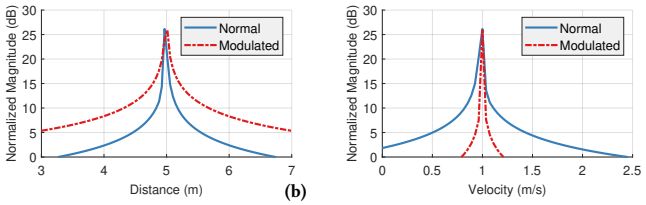

Figure 3: Comparison between delay-induced and modulation-induced peaks in (a) distance and (b) velocity spectrum.

communication packets.

However, these sophisticated chirp schemes contradict the main sensing purpose of the radar, since chirps with different parameters cannot be coherently combined, leading to the loss of sensing performance. For example, alternating chirp slopes reduces the range of the velocity domain by half, making it easier to cause aliasing effects and false velocity estimations. Besides, an attacker could still breach a sophisticated chirp scheme by estimating the parameters of each chirp, either from the last radar frame or in real time.

To this end, we formulate the task of detecting radar spoofing and communication signals as follows. We assume that a spoofing attacker or a communication tag can modulate certain frequency shifts to the backscattered signals. Meanwhile, the victim's radar can only control the chirps that are transmitted. The main objective is to detect modulated spoofing and communication signals without sacrificing the sensing performance of the radar.

3 Designing SCR

SCR is a radar sensing scheme that is resilient to spoofing as well as compatible with communication. The basic principle of SCR is to break the conditions under which modulated signals resemble normal signals. We show that with only the control of chirps, a radar can still detect modulated signals without sacrificing its sensing performance. In what follows, we analyze the differences between radar signals reflected by objects and backscatters (Sec. 3.1). Then, we introduce the novel signal processing algorithms and chirp configuration scheme for detecting modulated signals in both velocity (Sec. 3.2) and distance (Sec. 3.3) domains. Finally, we present how to integrate SCR with the standard radar sensing process (Sec. 3.4).

3.1 Revisiting the Radar Sensing Model

To understand the difference between modulated and normal signals in the view of radar, we rigorously analyze the phase and instantaneous frequency of the radar signal. Fig. 2a illustrates the relations between the Tx and Rx signals. With the linearly increasing frequency, the chirp transmitted by the radar is

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

$s(t,u)$ is a function of the fast time t and slow time u. t is the transmitted time of each sample in the chirp, while u is the starting time of each chirp.

Suppose there is only a single object around, whose distance is d, and velocity object is v, then the signal reflected by the object is an attenuated and delayed version of the transmit signal, *i.e.*,

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

where β is the attenuation coefficient, and $\tau=\frac{2d}{c_0}$ is the propagation delay of the reflected signal. We assume that the object moves at a constant velocity within a radar frame, which is usually only tens of ms. Then, the instantaneous distance between the object and the radar is

$$d(t,u)=d_0-v(t+u), \tag{3}$$

where d_0 is the initial distance at $t=u=0$.

The radar mixes the received signal with the transmitted signal to dechirp and obtain the baseband signal:

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

The high-order phase terms are omitted. Given the baseband signal phase $\angle b(t,u)$, we can calculate the instantaneous frequency shifts of both the fast time t and slow time u,

$$\begin{aligned} f_t'&=\frac{1}{2\pi}\frac{\partial\angle b}{\partial t}\approx\frac{2\gamma\left(d_0-vu\right)}{c_0}-\frac{2f_c v}{c_0},\\ f_u'&=\frac{1}{2\pi}\frac{\partial\angle b}{\partial u}\approx-\frac{2\left(f_c+\gamma t\right)v}{c_0}. \end{aligned} \tag{5}$$

f_t' and f_u' corresponds to f_δ and f_d in Fig. 2a, respectively.

Next, we analyze the effect of the modulation-induced frequency shift. Since it is independent of the delay-induced frequency shift, we omit the latter caused by the backscatter's displacement and movement. With the modulated frequency shift f_m as in Fig. 2a, the received signal is:

$$r(t,u)=s(t,u)e^{j2\pi f_m(t+u)}. \tag{6}$$

Similarly, we obtain the instantaneous frequency shifts with respect to t and u,

$$\begin{aligned} f_t''&=\frac{1}{2\pi}\frac{\partial\angle b}{\partial t}=f_m,\\ f_u''&=\frac{1}{2\pi}\frac{\partial\angle b}{\partial u}=f_m. \end{aligned} \tag{7}$$

By comparing Eq. 5 and Eq. 7, we have two observations. First, the modulation-induced frequency shifts are independent of chirp parameters. In contrast, the delay-induced frequency shifts depend on not only the object's distance d and velocity v, but also the chirp parameters γ and f_c. Second, the modulation-induced frequency shifts of fast and slow time are equal and thus coupled. If f_t'' is sufficiently large to create a nonnegligible distance shift, then the same frequency shift f_u'' will cause aliasing effects in the velocity domain. In contrast, the delay-induced frequency shift f_u' usually does not cause aliasing effects in the velocity domain. These two observations summarize the key discrepancies between modulated and normal signals. Based on the rigorous analysis of the radar sensing model, SCR is designed to detect modulated signals in both velocity and distance domains reliably.

3.2 Detecting Velocity Modulation via Splitting Chirps

We term small modulation-induced frequency shifts (*i.e.*, $f_m\sim f_d$) that only shift the velocity of the backscatter as velocity modulation. The modulation-induced frequency shift f_u'' remains constant regardless of the chirp parameters, according to Eq. 7. In contrast, the delay-induced frequency shift f_u' is proportional to the center frequency f_c of the chirp on average, according to Eq. 5.

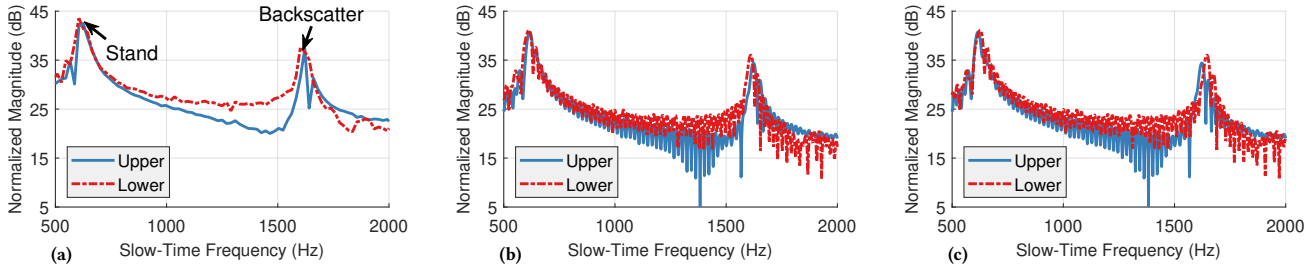

Figure 4: Illustration of detecting velocity modulation with the chirp-splitting scheme. Pseudo-spectra are calculated using (a) standard FFT, (b) steering vectors, and (c) scaled steering vectors.

An intuitive solution to differentiate the two types of frequency shifts is to transmit chirps with different center frequencies and compare the peak locations in their velocity spectra. However, using multiple chirps with different parameters counteracts the main sensing objective of the radar, as discussed in Sec. 2.3. Fortunately, we observe that the chirp frequency varies even within a chirp itself, leading to varying delay-induced frequency shift f_u', as illustrated in Fig. 2b. Thus, if the sweeping bandwidth of the chirp is sufficiently large, we can split the chirp into several sub-chirps with different center frequencies. For example, the chirp bandwidth of a 77 GHz radar can be at most 4 GHz [14]. If we split the 4 GHz chirp into two 2 GHz sub-chirps, then the center frequencies of the two sub-chirps will differ by 2 GHz, which is sufficiently large to cause non-negligible shifts of delay-induced peaks in velocity spectra.

While the chirp-splitting scheme is intuitive, we still need to answer two questions to obtain reliable detection results. The first question is how to estimate peak shifts in velocity spectra accurately? Compared to the absolute signal frequencies around 77 GHz, the 2GHz difference between the center frequencies of the two sub-chirps is orders of magnitude smaller. For example, suppose an object moves at 1 m/s, the frequency shift in slow time is about $2\times 79\text{ GHz}\times\frac{1\text{ m/s}}{c_0}\approx 527$ Hz, but the difference of the frequency shift in slow time is only about $2\times 2\text{ GHz}\times\frac{1\text{ m/s}}{c_0}\approx 13.3$ Hz, according to Eq. 5. Meanwhile, the resolution of the velocity spectrum is limited by the number of chirps and the chirp time. For example, the TI's 77 GHz radar [14] supports at most 512 chirps per frame. Suppose that the chirp time is 100 μs, then the slow-time frequency resolution is $\frac{1}{512\times 100\ \mu s}=19.5$ Hz, greater than the 13.3 Hz frequency difference.

Fortunately, the radar velocity spectrum is usually very sparse, since each object only has a few moving modes and corresponding velocity components. Thus, we can break the limitation of velocity spectrum resolution by explicitly calculating the pseudo-spectrum with finer-grained frequency samples, *e.g.*, with a sampling interval of 1 Hz. Specifically, given N_c chirps, we can form the steering vector for any frequency shift f_d as

$$\vec{a}(f_d)=\left(1, e^{j2\pi f_d T_c}, \cdots, e^{j2\pi f_d (N_c-1)T_c}\right)^T. \tag{8}$$

Then, the pseudo-spectrum can be calculated by correlating the steering vectors with the chirp samples,

$$P(f_d)=\left|\hat{b}^T\vec{a}^*(f_d)\right|, \tag{9}$$

where $\hat{b}$ is the vector of samples at the same distance in the distance spectrum. With finer-grained pseudo-spectrum, we can estimate the difference in frequency shifts smaller than the frequency resolution.

The second question is how to decouple the delay-induced and modulation-induced frequency shifts? In practice, there is usually relative movement between the radar and the backscatter. For example, the radar is on a moving vehicle, and the backscatter is on the roadside signpost. As a result, the modulation-induced frequency shifts may also experience non-zero drifts, making the detection solely based on the invariance of modulation-induced frequency shifts fail. To overcome this issue, we need to eliminate the impact of delay-induced frequency shifts. Fortunately, it is solvable because the differences in delay-induced frequency shifts are deterministic. Specifically, according to Eq. 5, the slow-time frequency shifts of different sub-chirps fulfil

$$\frac{f_u^{(L)}}{f_u^{(U)}}\approx\frac{f_c^{(L)}}{f_c^{(U)}}, \tag{10}$$

where the superscripts L and H indicate the lower and upper halves of the chirp, respectively. It means that, if a natural object creates a frequency shift $f_u^{(U)}$ for the upper sub-chirps, then it will create a frequency shift $f_u^{(L)}=f_u^{(U)}\frac{f_c^{(L)}}{f_c^{(U)}}$ for the lower sub-chirps. Thus, if we use the steering vectors $\vec{a}(f_d)$ for the upper sub-chirps and the corresponding scaled steering vectors $\vec{a}\left(\frac{f_c^{(L)}}{f_c^{(U)}}f_d\right)$ for the lower sub-chirps, the differences in delay-induced frequency shifts can be forcibly mitigated. Meanwhile, the modulation-induced frequency shifts $f_u''=f_d$ will experience a difference of $\left(\frac{f_c^{(L)}}{f_c^{(U)}}-1\right)f_d$ and thus can be detected if $f_d\neq 0$.

To verify the chirp-splitting scheme, we conduct an experiment with a TI's 77 GHz radar and a backscatter. The implementation details are introduced in Sec. 4. We configure the backscatter to modulate the radar signal at 1 kHz and mount it on a metal stand, which also creates outstanding reflections. The radar is placed on a cart. The backscatter is static while we push the cart and the radar on it toward the backscatter. Fig. 4 shows the pseudo-spectra calculated using different methods. As shown in Fig. 4a, the standard IFFT creates peaks for both the stand and the backscatter. However, due to the limited spectrum resolution, it fails to detect the difference in frequency shifts of the lower and upper sub-chirps. Fig. 4b shows the pseudo-spectra generated with the steering vectors, where the difference in frequency shifts becomes measurable. The frequency shifts of both the stand and the backscatter experience non-zero drifts due to the radar's movement, where the peaks in the pseudo-spectrum of the lower sub-chirps shift leftward because of the lower center frequency. This violates the invariance

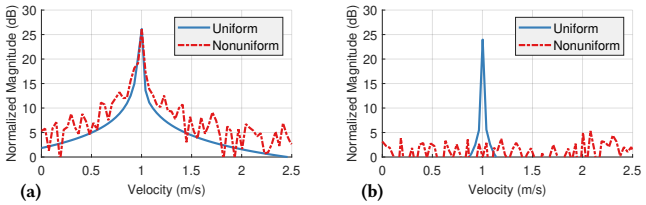

Figure 5: Comparison of the uniform and nonuniform chirp sampling schemes for (a) delay-induced and (b) modulation-induced frequency shifts in velocity spectra.

criterion for detecting modulation-induced frequency shifts. In contrast, as shown in Fig. 4c, with the scaled steering vectors, only the modulation-induced frequency shifts experience a significant peak shift and thus can be reliably detected. In practice, to avoid the peak skews, we calculate the cross-correlation between the spectrum segments around the peaks and identify the peak shift with the largest correlation value.

3.3 Detecting Distance Modulation via Splitting Frames

We term large modulation-induced frequency shifts (*i.e.*, $f_m \sim f_\delta$) that shift the distance of the backscatter as distance modulation. f_t'' remains constant regardless of the chirp parameters, according to Eq. 7. In contrast, the delay-induced fast-time frequency shift f_t' depends on the chirp parameters. Specifically, according to Eq. 5, f_t' is composed of two terms, where the first term $\frac{2\gamma(d_0 - vu)}{c_0}$ is proportional to the chirp slope γ and the second term $\frac{2f_c v}{c_0}$ is proportional to the center frequency f_c.

Ideally, similar to velocity modulation, distance modulation can be detected using different chirp slopes. However, varying frequency slopes within a chirp complicates the radar hardware design and is not supported by existing commercial radars. Besides, detecting differences in $\frac{2f_c v}{c_0}$ with respect to the center frequency f_c is also challenging, since the differences (*e.g.*, 20 Hz) are orders of magnitude smaller than the absolute frequency shifts in fast time (*e.g.*, 20 kHz) and are easily obfuscated. Besides, the distance spectrum is much denser than the velocity spectrum, given objects at diverse distances, which further exacerbates the feasibility of detecting tiny variances of delay-induced frequency shifts.

Instead of detecting modulation in the distance domain, we again resort to detection in the velocity domain and take advantage of the critical aliasing effect. According to Eq. 7, if the modulation rate f_m of the backscatter is sufficiently large to create non-negligible shifts in the distance domain, it will cause the aliasing effect in the velocity domain. Such aliasing effect is illustrated in Fig. 2c. With the standard chirp sampling configuration, where a radar transmits chirps uniformly with equal intervals, *e.g.*, $T_c = 100$ us, the constructive aliasing effect simply wraps the modulation-induced peak into the valid range of the velocity domain without changing the peak magnitude, according to the Nyquist Sampling Theorem [19]. Our further analysis reveals that uniform chirp sampling is not only a sufficient condition but also a necessary condition for distance modulation to create fake peaks in the radar spectrum. In contrast, delay-induced frequency shifts do not cause aliasing effects and are not impacted by chirp sampling schemes.

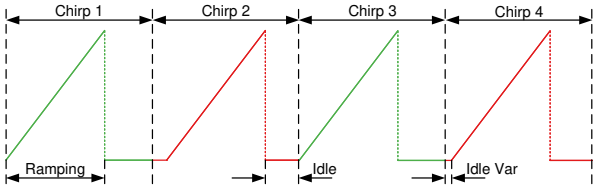

Figure 6: The chirp sampling configuration of SCR.

To verify the aliasing effects with different chirp sampling intervals, we conduct the same simulation as in Sec. 2.2 with both uniform and nonuniform chirp sampling, and demonstrate the results in Fig. 5. For the delay-induced frequency shift from an actual object, the magnitude and location of its peak in the pseudo-spectra remain unchanged, as in Fig. 5a. In contrast, for the modulation-induced frequency shift from a backscatter, its peak disappears with the nonuniform chirp sampling, due to the destructive aliasing effect, as shown in Fig. 5b. Compared with uniform chirp sampling, nonuniform chirp sampling effectively extends the range of the velocity spectrum to avoid the constructive aliasing effect. For example, the chirp idle time resolution supported by TI's radar is 0.01 μs, indicating an unambiguous frequency shift range of 100 MHz, which is sufficient for reliable detection of distance modulation. On this basis, we configure the radar to transmit chirps nonuniformly to break the condition of the constructive aliasing effect used by distance modulation.

However, using the nonuniform chirp sampling scheme eliminates the aliasing peaks of distance modulation and buries the modulated signals into noises, making them impossible to be detected. To reliably detect the modulated signals for spoofing alarms or communication triggering, we combine both uniform and nonuniform chirp schemes in a radar frame. The frame-splitting scheme of SCR is illustrated in Fig. 6. Specifically, we split the radar frame into two groups of chirps, the odd-numbered and even-numbered chirps. The odd-numbered chirps are idled with a random duration, while the even-numbered chirps are uniformly transmitted. During the detection stage, SCR forms the steering vectors for the groups of odd-numbered and even-numbered chirps and calculates their velocity spectra separately. The peaks of delay-induced frequency shifts appear in the spectra of both chirp groups, while those of modulation-induced frequency shifts only appear in the spectrum of uniformly sampled chirps. Thus, SCR can magnify the peaks of the modulation-induced frequency shifts by simply calculating the difference between the two spectra.

To verify the frame-splitting scheme, we conduct an experiment with the TI's 77 GHz radar and the backscatter. We use the same setting as the experiment in Sec. 3.2, except that the modulation rate of the backscatter is increased to 503 kHz to conduct distance modulation. Fig. 7 shows the radar spectra generated with different chirp sampling schemes. On the one hand, Fig. 7a shows the radar spectrum with uniformly sampled chirps. Peaks of both objects and backscatter appear. All objects exhibit non-zero frequency shifts and velocities, since the radar on the cart moves relatively. The peak of the backscatter is due to the constructive aliasing effect. On the other hand, Fig. 7b shows the radar spectrum with nonuniformly sampled chirps. The peak of the backscatter disappears, and the modulated signal is buried in the noise due to the destructive

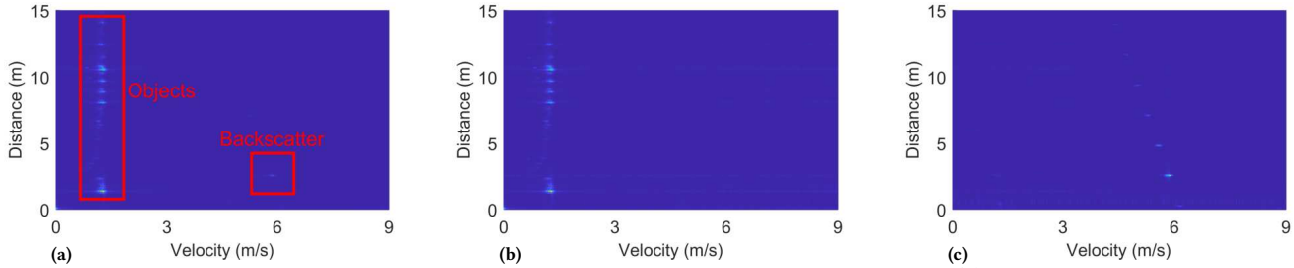

Figure 7: Illustration of detecting distance modulation with the frame-splitting scheme. (a) Radar spectrum with uniformly sampled chirps. (b) Radar spectrum with nonuniformly sampled chirps. and (c) Difference between the radar spectra with uniformly and nonuniformly sampled chirps.

aliasing effect. Meanwhile, the peaks of objects remain unchanged. Finally, Fig. 7c shows the difference between the radar spectra with uniformly and nonuniformly sampled chirps. The peaks of all natural objects are successfully eliminated, while the peaks of backscatters are magnified. To reliably detect the peaks of backscatters, we calculate the magnitude difference of the corresponding peaks in the spectra of both the uniformly and nonuniformly sampled chirps, normalized by the peak magnitude of the uniformly sampled chirps. A normalized peak magnitude difference close to 1 indicates the existence of backscatter modulations. It is worth noting that SCR's frame-splitting scheme detects not only the basic modulation frequency shift, but also the harmonic components caused by the imperfection of the backscatter prototype reliably.

3.4 Putting Everything Together

SCR can be easily integrated with the standard radar sensing pipeline to augment the radar with the capability of detecting modulation-induced frequency shifts. It only requires a slight modification of velocity spectrum generation to address the nonuniformly sampled chirps. Despite this, SCR does not change chirp parameters and thus retains the full sensing performance of the original radar frame. Fig. 8 shows the integration of SCR with the basic radar sensing function. It is composed of three modules, *i.e.*, distance-domain modulation detection, velocity-domain modulation detection, and radar sensing. For distance modulation detection, SCR uses the spectrum of the uniformly sampled chirps to detect peaks. The spectrum is calculated by correlating the steering vectors with chirp samples. Using uniformly sampled chirps guarantees the detection of all delay-induced and modulation-induced peaks. For each peak detected, SCR calculates the peak magnitude difference between the spectra of uniformly and nonuniformly sampled chirps to recognize whether the peak is generated by distance modulation (Sec. 3.3). For velocity modulation detection, SCR uses the spectrum of the upper sub-chirps to detect peaks. For each peak detected, SCR calculates the peak shift between the spectra of upper and lower sub-chirps to recognize whether the peak is generated by velocity modulation (Sec. 3.2). After detecting all possible modulated signals, SCR reuses all chirps to calculate the spectrum for sensing. Thanks to the use of the complete bandwidth and all chirps, SCR achieves the resolution and range of distance and velocity just as using the standard radar frame with uniform sampled chirps. Using the modulation detection results, SCR can further filter out backscatters and retain natural objects only.

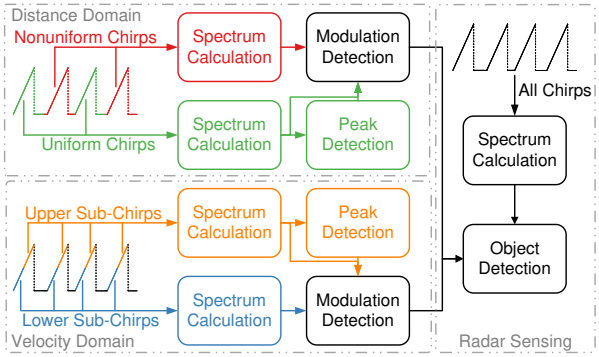

Figure 8: Illustration of integrating SCR with radar sensing.

4 Implementation

We implement SCR with a commercial radar, *i.e.*, a TI's radar [14], and a customized backscatter prototype. Both TI's radar and the backscatter operate at 77 GHz. TI's radar comprises an RF module that configures and transceives chirp signals, and a DSP module that captures and processes the baseband chirp samples. A radar frame of SCR consists of 512 chirps, all of which share the same parameters, as shown in Tab. 1. The chirp sampling configuration of SCR is naturally supported by TI's radar, which allows an idle time variance for each chirp. We set the default idle time for uniformly sampled chirps to 40 μs. For each nonuniformly sampled chirp, we randomly select an idle time variance between -20 μs and 20 μs. The minimum unit of idle time variances is 0.01 μs, indicating an unambiguous frequency shift range of 100 MHz. We develop a Lua script that can be executed in TI's mmWave studio to automatically configure chirp parameters and idle time variances. TI's radar has 3 Tx and 4 Rx. We configure the radar to operate in the Tx beamforming (TXBF) mode, where all Tx are activated to beamform signal to narrow directions during a radar frame. Compared with the MIMO mode, where each Tx is activated at a time, the TXBF mode extends the radar sensing range and is more suitable for outdoor scenarios, such as autonomous driving. The radar can vary beamforming weights across different radar frames to cover different directions. Meanwhile, we apply digital beamforming to the 4 Rx to harness the Rx array gain for both backscatter and object detection. The SCR's signal processing pipeline is implemented in MATLAB.

The backscatter prototype is composed of a few mmWave components from Evarant [9]. Specifically, a 25 dBi E-band rectangular horn antenna is used to receive and reflect Radar signals. An E-band SPDT PIN switch acts as the modulator. One switch output

Start Frequency	Chirp Slope	Ramp Time	ADC Samples	ADC Sample Rate
77 GHz	66 MHz/μs	60 μs	512	10 kHz

Table 1: Chirp parameters used by SCR.

is directly connected to a waveguide short, while the other is connected to a $\frac{1}{4}$ wavelength spacer followed by a waveguide short to introduce a phase shift of π. A TTL driver controls the RF switch to switch between the two outputs at the frequency of the TTL signal. The switching speed of the RF switch is 100 ns, meaning that the maximum modulation frequency is 5 MHz. We program a Digilent FPGA [6] to generate the TTL signal. However, the FPGA only has a 100 MHz clock source, and cannot fine-tune the modulation frequency (*e.g.*, at a step of 1 kHz) when the absolute frequency is very large (*e.g.*, 500 kHz). Thus, the FPGA is only suitable for sole velocity modulation. To accurately control the modulation frequency of the backscatter prototype for the experiment, we use a Siglent waveform generator [45] to generate fine-grained TTL signals. Finally, the RF switch requires ±5 V bias voltages, which are provided by a Rigol DC power supply [39].

5 Experiment

5.1 Experimental Setup

We conduct field tests in both indoor and outdoor environments, as shown in Fig. 9. The indoor scenario is in a lab with corridors, cubicles, and an arena with tables, chairs, and sofas. In the indoor scenario, we mount the backscatter and the mmWave radar separately on two carts so that they can be moved freely. The outdoor scenario is in a parking lot, where we mount the backscatter on a tripod to emulate an intelligent road sign or a fixed spoofing attacker on the roadside. Meanwhile, the radar is mounted on a sedan's hood. The backscatter is configured to create modulated signals with various frequency shifts in both fast and slow times.

We evaluate the detection performance of SCR by analyzing peak shifts in velocity modulation cases and peak magnitude differences in distance modulation cases. We show that natural objects and backscatters create statistically different metric values, and predefined thresholds can be set to distinguish between them reliably.

5.2 Detection Performance of SCR

Detection with different frequency shifts. A backscatter can practically modulate arbitrary frequency shifts for spoofing or communication. We thus evaluate the detection performance of SCR with different modulation-induced frequency shifts. For velocity modulation, we vary the frequency shifts of the backscatter from 0.5 kHz to 11 kHz, corresponding to speeds from 0.95 m/s to 20.9 m/s. Fig. 10a shows the peak shifts with different frequency shifts. When the frequency shift is between 0 and 5 kHz, the peak shift is proportional to the frequency shift, aligning with the analysis in Sec. 3.2. When the frequency shift just exceeds 5 kHz, *i.e.*, the upper boundary of the velocity spectrum, the destructive aliasing effect caused by the nonuniformly sampled chirps is not strong enough, and the peak thus still appears and is wrapped back between -5 kHz and 5 kHz, which is the range of the velocity spectrum. Thus, the measured peak shift is proportional to the wrapped frequency shift. For example, the 7 kHz frequency shift wraps to -3 kHz, and

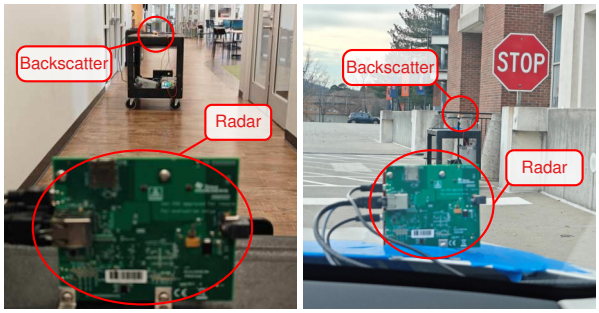

Figure 9: Illustration of the experimental setup.

the corresponding peak shift is around 60 Hz. Fig. 10b shows the classification accuracy with different peak shift thresholds. The selection of the threshold depends on the modulation frequency range. For example, with a threshold of 5 Hz, SCR can detect frequency shifts greater than 0.5 kHz. To detect frequency shifts of integral multiples of 10 kHz, whose peak shifts are close to 0, one solution is to use different co-prime chirp times by controlling their idle times in other radar frames.

For distance modulation, we vary the frequency shifts from 20 kHz to 1 MHz. To avoid obfuscation from surrounding static objects, we add an additional frequency shift of 1 kHz to each case. Fig. 11a shows the peak magnitude differences with different frequency shifts. When the frequency shift exceeds 20 kHz, the destructive aliasing effect caused by the nonuniformly sampled chirps becomes sufficiently strong, leading to prominent peak magnitude differences. The peak magnitude difference increases with the frequency shift. It approaches 1 after the frequency shift increases to 200 kHz, corresponding to a distance shift of only 0.45 m with the chirp parameters in Tab. 1. It indicates that SCR can reliably detect a wide range of distance modulation. Fig. 11b shows the classification accuracy with different peak magnitude difference thresholds. With a threshold of 0.5, SCR can detect distance modulation reliably.

Detection at different distances. We evaluate the detection performance of SCR with the backscatter at different distances. Fig. 12 shows the peak shifts for velocity modulation and the peak magnitude differences for distance modulation. With the increased distance, the received backscatter signal becomes weaker, and is easier to be distorted by interferences and noises. Such impacts are observed in Fig. 12, in terms of slightly smaller peak magnitude differences and larger variances in both metrics at longer distances. Nonetheless, both metrics are still sufficiently robust for detecting velocity and distance modulation, respectively. When the distance exceeds 15 m, the backscatter signal becomes too weak to be detected with the CFAR algorithm. It indicates that SCR can reliably recognize backscatters once the radar detects them.

Detection with different movement conditions. Both radar and backscatter can be stationary or moving in different scenarios. We thus evaluate the detection performance of SCR with different movement conditions. Specifically, we consider four cases: i) SR/SB: both radar and backscatter are stationary; ii) MR/SB: only the radar is moving; iii) SR/MB: only the backscatter is moving; iv) MR/MB: both radar and backscatter are moving. Fig. 13 shows the results of detecting both types of modulations. For velocity modulation, the peak shifts of the backscatter remain consistent in different cases. However, those of natural objects become larger with movements

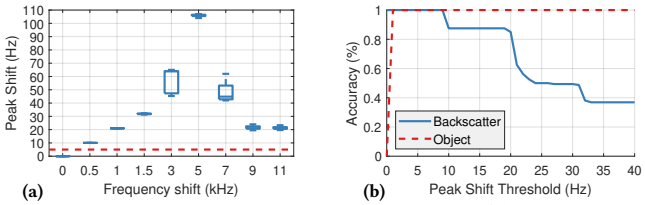

Figure 10: Detection of velocity modulation. (a) Distribution of peak shifts. (b) Classification accuracy.

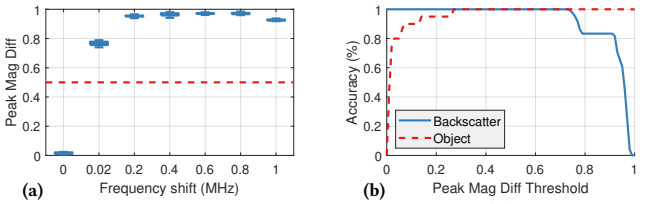

Figure 11: Detection of distance modulation. (a) Distribution of peak magnitude differences. (b) Classification accuracy.

due to a more dynamic velocity spectrum. It thus increases the minimum frequency shift that SCR can reliably detect. For distance modulation, a similar increase in the peak magnitude differences of natural objects is also observed. Nonetheless, the peak magnitude differences of backscatters and objects are still significantly different, ensuring reliable detection of distance modulation.

5.3 Chirp Configuration Analysis

Impact of chirp frequency. Velocity modulation detection relies on the frequency separations between the upper and lower sub-chirps, which are determined by two factors: the total chirp bandwidth and the selection of sub-chirp frequencies. First, we evaluate the impact of the total chirp bandwidth by varying it from 250 MHz to 4 GHz. Fig. 14a shows that the peak shift increases with the total bandwidth, as the frequency separation between the sub-chirps increases proportionally. It indicates that a larger bandwidth is preferred for velocity modulation detection. Second, given the total 4 GHz bandwidth, we select sub-chirps to achieve different frequency separations. Specifically, we let the two sub-chirps align with the lower and upper boundary of the 4 GHz frequency band and decrease the sub-chirp bandwidth from 3 GHz to 250 MHz. As shown in Fig. 14b, the peak shift increases linearly with the frequency separation of the two sub-chirps. Compared with SCR's default sub-chirp selection with a frequency separation of 2 GHz, the 500 MHz sub-chirps with a frequency separation of 3.5 GHz is better. The benefit becomes marginal as the sub-chirp bandwidth is further reduced to 250 MHz. Meanwhile, the adverse effect of reducing the sub-chirp bandwidth appears, as the lower distance resolution with narrower bandwidths leads to stronger interferences from velocity spectra at different distances.

Impact of idle time variance. Idle time variance is the key parameter that enables distance modulation detection of SCR. We thus evaluate the impact of its resolution and range. Fig. 15a shows the peak magnitude differences with different idle time variance resolutions. The detection is successful with the metric value close to 1 when the variance resolution is smaller than 1 μs, since the effective bandwidth of the nonuniformly sampled chirps is sufficiently large

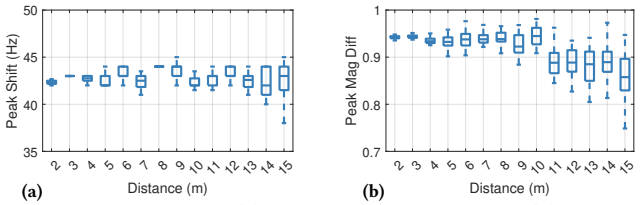

Figure 12: Detection of (a) Velocity modulation and (b) Distance modulation at different distances.

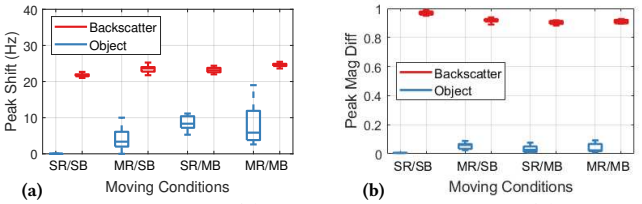

Figure 13: Detection of (a) Velocity modulation and (b) Distance modulation with different moving conditions.

to cover the modulation frequency. When the variance resolution further increases, the detection fails, as the modulation-induced frequency shift introduces the same phase shifts to the chirps as the delay-induced frequency shifts. Thus, it suggests to keep the idle time variance resolution as small as possible. Fig. 15b shows the peak magnitude differences with different idle time variance ranges. The detection is successful when the variance range is above 5 μs. When the variance range further decreases, the discrepancies created by the nonuniformly sampled chirps become too small to indicate the presence of modulation-induced frequency shifts.

Impact of chirp number. The number of chirps in a radar frame determines the resolution of velocity spectra. As both velocity and distance modulation detections are conducted in the velocity domain, we evaluate the impact of chirp number. As shown in Fig. 16a, the peak shifts for velocity modulation detection remain consistent when more than 128 chirps are used. If the chirp number further decreases, it becomes challenging to resolve the peaks in the velocity spectrum, leading to erroneous estimation of peak shifts. For distance modulation detection, the peak magnitude differences gradually decrease with the reduction of the chirp number, as shown in Fig. 16b. Fortunately, the peak magnitude difference is less sensitive to the velocity spectrum resolution than the peak shift. Using only 64 chirps is still sufficient for distance modulation detection.

5.4 Sensing Performance of SCR

A standard radar frame only consists of uniformly sampled chirps for velocity sensing. In contrast, the frame-splitting scheme of SCR has half of the chirps nonuniformly sampled. We thus evaluate its impact on the basic velocity sensing performance. Specifically, we configure the backscatter to modulate signals from 1 kHz to 9 kHz to emulate an object with different velocities. We compare SCR with the standard radar frame and a common radar frame that uses two chirps slopes for modulation detection [20]. According to Eq. 5 and Eq. 7, the dual chirp slope scheme can detect distance modulation by identifying inconsistent modulated peak distances with different chirp slopes. Before comparing the sensing performance of SCR and the dual chirp slope scheme, we conduct experiments and find

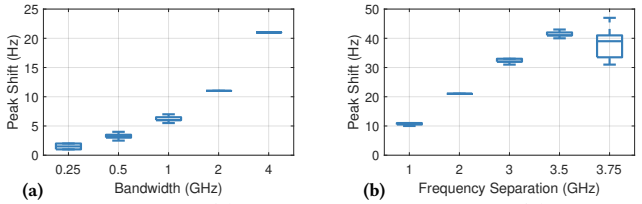

Figure 14: Impact of (a) total chirp bandwidth and (b) sub-chirp frequency separation on velocity modulation detection.

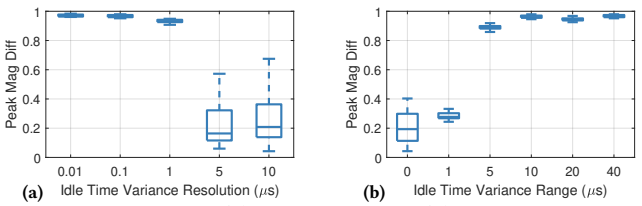

Figure 15: Impact of (a) resolution and (b) range of idle time variance on distance modulation detection.

that they both can detect distance modulation reliably with peak magnitude differences greater than 0.95. The sensing performance of both schemes is shown in Fig. 17. Fig. 17a compares the velocity sensing range of different schemes. The alter-chirp scheme transmits chirps with the two slopes alternatively. SCR achieves the same frequency measurement accuracy and range as the standard scheme. In contrast, the alter-chirp scheme only achieves half of the velocity range. Fig. 17b compares the velocity sensing resolution of different schemes. The group-chirp scheme transmits half of the chirps with one slope first and the rest of the chirps with the other slope then. The sensing resolution is evaluated via the peak widths. Despite retaining the 10 kHz sensing range, the group-chirp scheme has a wider peak width and, thus, worse sensing resolution. In contrast, SCR achieves the same sensing resolution as the standard scheme. Besides, the nonuniform sampling used by SCR does not distort the shape of the peak. In conclusion, SCR maintains the same sensing performance as the standard radar scheme.

5.5 Robustness of SCR

Impact of peak interference. Two peaks close by in a radar spectrum may interfere with each other and cause detection failure. To evaluate SCR's robustness against interference, we simulate an object and a backscatter with different gaps in the velocity and distance domains. Specifically, we fix the modulation frequencies of the backscatter and adjust its velocity and distance to achieve different gaps. Fig. 18 shows the impact of the velocity gap. When the velocity difference of the two peaks is greater than 1 m/s, SCR can reliably detect both velocity and distance modulations. Fig. 19 shows the impact of the distance gap. When the distance difference of the two peaks is greater than 10 cm, SCR can reliably detect both velocity and distance modulations. Due to the sparse surroundings in practice, such small velocity and distance gaps are not common, and the impact of peak interference is thus not significant.

Impact of peak SNR. SCR will be severely impacted by noises if the signal strength is too weak and the peak is not prominent in radar spectra. To evaluate SCR's robustness against noise, we simulate an object and a backscatter separately with different noise

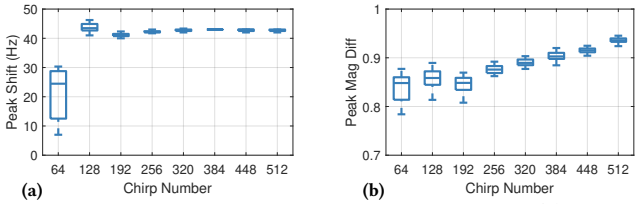

Figure 16: Impact of chirp number on detection of (a) velocity modulation and (b) distance modulation.

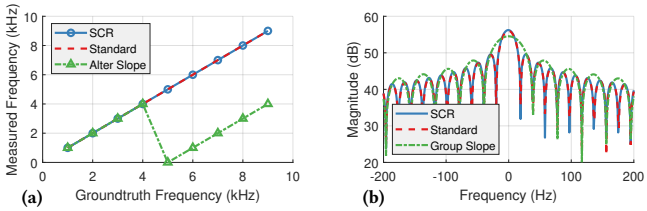

Figure 17: Comparison of sensing performance with different chirp configuration schemes.

Dist FFT	Velocity FFT	Dist Mod	Velocity Mod
2.4 ms	4.1 ms	56.8 ms	545.7 ms

Table 2: Computational time of SCR.

levels. Fig. 20 shows the metrics for both velocity and distance modulation and the peak detection rate of the CFAR algorithm. When the SNR is 0 dB, the CFAR algorithm can hardly detect the peaks, and the metrics for the object and the backscatter are not separable. As the SNR increases, the detection rate of the CFAR algorithm increases, and SCR's metrics become more distinguished. Both CFAR and SCR's detection becomes reliable when the SNR exceeds 3 dB. In practice, SCR can use peak SNR as a confidence indicator for modulation detection.

5.6 Computational Time of SCR

Compared with the standard radar signal processing, SCR needs to calculate additional spectra, detect peaks, and compute metrics, incurring more computational overhead. Tab. 2 shows the execution time of each sub-process for a single radar frame. Specifically, the standard processing only includes FFTs in the distance and velocity domains, which takes 6.5 ms. In contrast, SCR applies FFT to the distance domain and then executes distance and velocity modulation detection processes, which takes 604.9 ms. Thus, a radar can transmit SCR frames at a rate of 1.6 Hz to detect spoofing attacks and backscatter communication. One thing to note is that distance modulation costs 10x less time than velocity modulation, since the former does not require the calculation of high-resolution spectra. It suggests that distance modulation should be used for backscatter communication to achieve a higher data rate.

5.7 Case Study

Backscatter communication for autonomous vehicles. In this scenario, a vehicle with radar approaches a stop sign, and a backscatter next to the stop sign broadcasts the sign information, as shown in Fig. 9. As a comparison, we also test SCR with a corner reflector as a natural object. Due to the limitations of the angular range and the communication distance of the current backscatter prototype, we can only drive the vehicle at a speed of 15 mph at most.

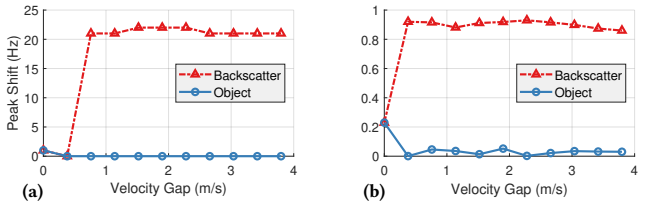

Figure 18: Impact of interference in velocity domain on detection of (a) velocity modulation and (b) distance modulation.

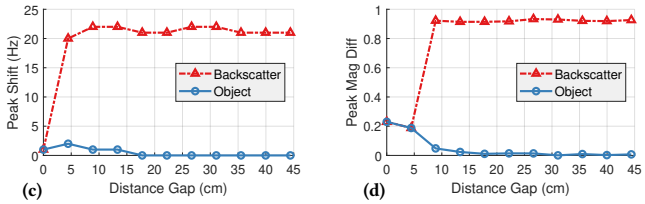

Figure 19: Impact of interference in distance domain on detection of (a) velocity modulation and (b) distance modulation.

Fig. 21 illustrates the performance of SCR as the vehicle approaches the target and decelerates. The CFAR algorithm starts to detect the backscatter around 10 m away. For velocity modulation, SCR can measure the peak shifts of the modulation accurately once the radar detects the backscatter, as in Fig. 21a. The peak shifts of the backscatter are significantly larger than the corner reflector's. Similarly, for distance modulation, the peak magnitude differences of both the backscatter and the object are accurately measured by SCR, as shown in Fig. 21b. The results indicate the effectiveness and robustness of SCR for spoofing and communication detection in autonomous driving scenarios.

Spoofing attack against gesture recognition. In this scenario, a smart home radar interacts with a user, and a malicious attacker nearby creates a modulated peak with a constant velocity and the same distance as the user. Fig. 22a shows the radar spectrogram of the user's gesture, which is polluted by a modulated frequency shift of -1 kHz. Existing research [56] has shown that even a constant modulated frequency can deceive the deep neural network classifiers used by wireless sensing systems. Fig. 22b shows the velocity spectra of both uniform and nonuniform sampled chirps of SCR. By comparing the two spectra, SCR can successfully detect the modulated signal from the attacker and further notify the sensing system. Meanwhile, the frequency shift pattern of the user's gesture remains consistent regardless of chirping sampling schemes, indicating that SCR has a minor impact on radar sensing.

6 Discussion and Future Works

Designing 77 GHz radar backscatters. Existing wireless backscatters mainly operate at sub-6 GHz or low mmWave frequencies, *e.g.*, 24 GHz, due to the lack of commercial RF components and excessive signal attenuation at high mmWave frequencies. MmComb [4] operates at 60 GHz with a maximum modulation rate of 100 MHz. However, limited by the antenna's size and non-retroreflective characteristics, the communication range of mmComb is short. UniScatter [37] exploits the graphene capacitor and Luneburg lens to increase the backscatter size and, thus, the communication range. However, the graphene capacitor suffers from low modulation frequency and high power consumption. More sophisticated designs for backscatters at high mmWave frequencies are needed to realize the full potential of mmWave radar backscatters.

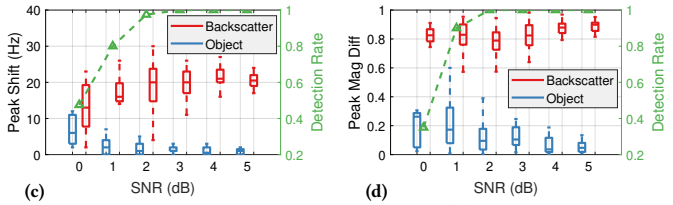

Figure 20: Impact of SNR on detection of (a) velocity modulation and (b) distance modulation.

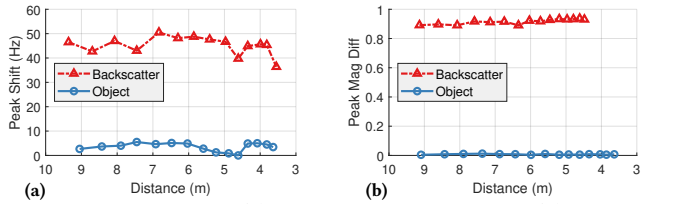

Figure 21: Detection of (a) velocity modulation and (b) distance modulation in driving scenarios.

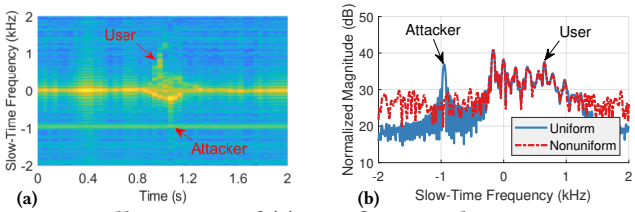

Figure 22: Illustration of (a) spoofing attack against gesture recognition and (b) detection with SCR.

Potential attacks against SCR. SCR increases the cost of spoofing attacks against radar sensing, as an attacker needs to employ more complicated modulation schemes that require additional RF hardware or signal processing. To attack the velocity modulation detection of SCR, the attacker could possibly modulate multiple slightly different frequency shifts with the same magnitudes so that the correlation profile of velocity spectra of sub-chirps becomes noisier, potentially leading to wrong estimation of peak shifts. For distance modulation detection of SCR, the attacker has to apply true time delays (TTD) to radar signals. However, sub-μs TTDs are needed to generate useful distance shifts at decameter levels, which is extremely challenging. According to Sec. 5.5, an adversary can attack SCR by hiding real objects with detectable spoofing attacks. However, synchronizing the attacker's fake distance and velocity with the object's precisely is challenging in practice. A more sophisticated adversary can keep assessing attacking effects by monitoring the victim's reactions via its sensing unit, and adaptively upgrades the attack until it succeeds. However, such an interactive attack scheme requires more sophisticated hardware designs. We plan to study the feasibility of these attacks in future work.

Sensing with nonuniform chirp sampling. Compared with uniform chirp sampling, nonuniform sampling is more sensitive to modulation frequencies and thus has great potential to benefit some sensing tasks. For example, mmEve [50] uses mmWave radar sensors to eavesdrop on smartphone speakers. Considering the similar

effects between vibrations and modulations, we envision using SCR to enhance the performance of similar sensing applications.

Distinguishing between attack and communication. SCR only detects modulated signals from attack and communication. Distinguishing between the two types of modulated signals should be processed by upper-level sensing and communication modules. For example, the radar backscatter communication module can try to decode modulated signals detected by SCR. If the decoding keeps failing, it may indicate attacks instead of communication.

Impact of backscatter modulation schemes. Most existing radar backscatters [1, 46] use frequency modulation since it is naturally compatible with the radar sensing principle. The prominent peaks of modulated frequency shifts can be easily detected by SCR. However, other modulation schemes, such as amplitude and phase modulations, can still be used. While they create more complex frequency shift patterns than frequency modulation, the principle of SCR can still be used to detect these modulated frequency shifts in both velocity and distance domains. We will exploit the extension of SCR to different modulation schemes in future work.

7 Related Work

Spoofing attack against radar. Radar spoofing attacks pose significant security threats to normal radar sensing. They generate signals with fake parameters to deceive radar sensors. Existing spoofing attacks can be classified into active attacks [12, 17, 29, 32, 47] and passive attacks [20, 27, 28, 41, 49], according to the mechanisms of signal generation. The active attacks generate synchronized chirps and transmit them to the victim radar, which triggers false positive detections [47]. While active attacks have high controllability of signal generation, they are limited by the stringent requirement of synchronization in time, frequency, and even phase with the victim radar. As phase-level synchronization is challenging, the victim radar can easily defend against these active attacks by applying phase modulations to transmitted chirps.

In contrast, passive attacks avoid the synchronization requirement by reflecting radar chirps. The attacker modulates frequency shifts to radar chirps to spoof distance and velocity measurements. In [20], an RF switch is used to create desired frequency shifts. MmSpoof [49] replaces the RF switch with a mixer to eliminate strong harmonic components that may expose the attack. Compared with active attacks, passive attacks are immune to countermeasures of randomizing most chirp parameters, such as start frequency and phase. With real-time chirp parameter estimation capability, passive attacks are even resilient against random chirp slopes. Fortunately, thanks to the chirp-splitting and frame-splitting schemes, SCR can reliably detect modulation-induced frequency shifts of the passive attacks. Passive spoofing attacks have also been used to defend against eavesdropper radars [41]. However, the nonuniform chirp sampling scheme of SCR can effectively filter out the modulation-induced signals and pose new eavesdropping threats.

Besides reconfigurable passive attacks, some fully passive reflectors have been designed to spoof radars [5, 57]. Without the modulation capability, they mainly modify the magnitude and polarization of the reflected signals. Due to the fully passive characteristics, these reflectors usually have limited attacking ranges and thus pose less severe threats than the reconfigurable attackers.

Backscatter communication with radar. Radar backscatter communication combines rich radar spectrum resources and low-cost, low-power backscatter technologies to achieve massive connection and accurate sensing [1–4, 8, 16, 24, 25, 31, 37, 46]. For example, Millimetro [46] demonstrates simultaneous communication and localization with 6 backscatter tags. Omniscatter [1] verifies the feasibility of concurrent communication of 1100 tags within 20 m $\times$ 20 m region via a trace-driven evaluation. Besides, Hawkeye [3] and SuperSight [2] show the sub-cm localization precision with backscatter tags in long-range and NLoS regions, respectively. Recently, BiScatter [31] further enables downlink communication from radar to tag. To ensure reliable detection of backscatter signals, existing methods adopt sophisticated modulation schemes in both fast-time [8] and slow-time [1] domains. SCR can serve as the detection module for these radar backscatter communication systems, with the benefits of simplifying signal generation and processing and retaining the original sensing capabilities of radar.

Fully passive backscatter tags [13, 21, 30, 51] have been developed following the idea of chipless RFID that eliminates the IC cost. These tags encode fixed information in the frequency, time, or spatial domain, and act as RF barcodes. Compared with modulation-based backscatters, these tags require more sophisticated signal processing steps for tag detection and information extraction.

Sensing with radar. Radar sensing technologies have evolved from simple target detection to complicated tasks that breakthrough the sensing resolution limitation of radars [7, 26, 33, 40, 42, 44, 53]. For example, mmGPE [52] reconstructs human poses from radar signals. PanoRadar [18] utilizes a rotating radar to image scenes with resolutions close to that of lidar. RF-SCG [10] translates radar signals to seismocardiograms that record the human heart's mechanical activity. Hydra [23] uses radar signals to measure the leaf wetness of plants. However, most existing research assumes that the measured signals are purely from normal objects. Thus, SCR can complement existing radar sensing systems to detect potential spoofing attacks against their sensing functions.

8 Conclusion

We have designed and validated SCR, a spoofing-resilient and communication-integrated mmWave radar sensing system. We conduct a rigorous analysis of the radar sensing model and identify the key differences between the normal sensing signals and modulated spoofing and communication signals, based on which SCR can reliably detect spoofing and communication without sacrificing the sensing performance of the radar. SCR can be seamlessly integrated into the existing radar ISAC systems to provide secure ISAC functions. It also has great potential to enhance the sensing capabilities with the novel nonuniform chirp sampling scheme.

9 Acknowledgement

We appreciate the insightful comments and feedback from the anonymous reviewers and shepherd. We thank Md Sabbir Ahmed for his assistance in the experiment. This work was supported in part by the NSF under Grants CNS-2403124, CNS-2045885, SaTC-2318796, and the CCI under contract number FP00022983_SA001.

References

[1] Kang Min Bae, Namjo Ahn, Yoon Chae, Parth Pathak, Sung-Min Sohn, and Song Min Kim. 2022. OmniScatter: extreme sensitivity mmWave backscattering using commodity FMCW radar. In *Proceedings of the ACM MobiSys*.

[2] Kang Min Bae, Hankyeol Moon, and Song Min Kim. 2024. SuperSight: Sub-cm NLOS Localization for mmWave Backscatter. In *Proceedings of the ACM MobiSys*.

[3] Kang Min Bae, Hankyeol Moon, Sung-Min Sohn, and Song Min Kim. 2023. Hawkeye: Hectometer-range subcentimeter localization for large-scale mmwave backscatter. In *Proceedings of the ACM MobiSys*.

[4] Yoon Chae, Zhenzhe Lin, Kang Min Bae, Song Min Kim, and Parth Pathak. 2024. mmComb: High-speed mmWave Commodity WiFi Backscatter. In *Proceedings of the USENIX Symposium on Networked Systems Design and Implementation (NSDI)*.

[5] Xingyu Chen, Zhengxiong Li, Biacheng Chen, Yi Zhu, Chris Xiaoxuan Lu, Zhengyu Peng, Feng Lin, Wenyao Xu, Kui Ren, and Chunming Qiao. 2023. Metawave: Attacking mmwave sensing with meta-material-enhanced tags. In *Proceedings of the IEEE NDSS*.

[6] Digilent. [n. d.]. Cmod A7-35T: Breadboardable Artix-7 FPGA Module. https://digilent.com/shop/cmod-a7-35t-breadboardable-artix-7-fpga-module.

[7] Laura Dodds, Hailan Shanbhag, Junfeng Guan, Saurabh Gupta, and Haitham Hassanieh. 2024. Around the Corner mmWave Imaging in Practical Environments. In *Proceedings of the ACM MobiCom*.

[8] Manideep Dunna, Kshitiz Bansal, Sanjeev Anthia Ganesh, Eamon Patamasing, and Dinesh Bharadia. 2023. R-fiducial: Millimeter Wave Radar Fiducials for Sensing Traffic Infrastructure. In *Proceedings of the IEEE VTC*.

[9] Eravant. [n. d.]. https://www.eravant.com.

[10] Unsoo Ha, Salah Assana, and Fadel Adib. 2020. Contactless seismocardiography via deep learning radars. In *Proceedings of the ACM MobiCom*.

[11] Chenming He, Chengzhen Meng, Chunwang He, Xiaoran Fan, Beibei Wang, Yubo Yan, and Yanyong Zhang. 2024. See Through Vehicles: Fully Occluded Vehicle Detection with Millimeter Wave Radar. In *Proceedings of the ACM MobiCom*.

[12] David Hunt, Kristen Angell, Zhenzhou Qi, Tingjun Chen, and Miroslav Pajic. 2024. MadRadar A Black-Box Physical Layer Attack Framework on mmWave Automotive FMCW Radars. Proceedings of the IEEE NDSS.

[13] Tatsuya Iizuka, Takuya Sasatani, Toru Nakamura, Naoko Kosaka, Masaki Hisada, and Yoshihiro Kawahara. 2023. MilliSign: mmWave-Based Passive Signs for Guiding UAVs in Poor Visibility Conditions. In *Proceedings of the ACM MobiCom*.

[14] Texas Instruments. [n. d.]. mmWave radar sensors. https://www.ti.com/sensors/mmwave-radar/overview.html.

[15] Texas Instruments. 2020. The fundamentals of millimeter wave radar sensors.

[16] Ali Khaleghi, Aminolah Hasanvand, and Ilangko Balasingham. 2018. Radio frequency backscatter communication for high data rate deep implants. *IEEE Transactions on Microwave Theory and Techniques* 67, 3 (2018), 1093–1106.

[17] Rony Komissarov and Avishai Wool. 2021. Spoofing attacks against vehicular FMCW radar. In *Proceedings of the Workshop on Attacks and Solutions in Hardware Security*.

[18] Haowen Lai, Gaoxiang Luo, Yifei Liu, and Mingmin Zhao. 2024. Enabling Visual Recognition at Radio Frequency. In *Proceedings of the ACM MobiCom*.

[19] HJ Landau. 1967. Sampling, data transmission, and the Nyquist rate. *Proc. IEEE* 55, 10 (1967), 1701–1706.

[20] Antonio Lazaro, Arnau Porcel, Marc Lazaro, Ramon Villarino, and David Girbau. 2022. Spoofing attacks on FMCW radars with low-cost backscatter tags. *MDPI Sensors* 22, 6 (2022), 2145.

[21] Zhengxiong Li, Baicheng Chen, Zhuolin Yang, Huining Li, Chenhan Xu, Xingyu Chen, Kun Wang, and Wenyao Xu. 2019. Ferrotag: A paper-based mmwave-scannable tagging infrastructure. In *Proceedings of the ACM SenSys*.

[22] Ruofeng Liu, Tianshun Yao, Ruili Shi, Luoyu Mei, Shuai Wang, Zhimeng Yin, Wenchao Jiang, and Shuai Wang. 2024. Mission: mmWave Radar Person Identification with RGB Cameras. In *Proceedings of the ACM SenSys*.

[23] Yimeng Liu, Maolin Gan, Huaili Zeng, Li Liu, Younsuk Dong, and Zhichao Cao. 2024. Hydra: Accurate Multi-Modal Leaf Wetness Sensing with mm-Wave and Camera Fusion. In *Proceedings of the ACM MobiCom*.

[24] Mohammad H Mazaheri, Soroush Ameli, Ali Abedi, and Omid Abari. 2019. A millimeter wave network for billions of things. In *Proceedings of the ACM SIGCOMM*.

[25] Mohammad Hossein Mazaheri, Alex Chen, and Omid Abari. 2021. Mmtag: A millimeter wave backscatter network. In *Proceedings of the ACM SIGCOMM*.

[26] Nishant Mehrotra, Divyanshu Pandey, Akarsh Prabhakara, Yawen Liu, and Swarun Kumar. 2024. Hydra: Exploiting Multi-Bounce Scattering for Beyond-Field-of-View mmWave Radar. In *Proceedings of the ACM MobiCom*.

[27] Noriyuki Miura, Tatsuya Machida, Kohei Matsuda, Makoto Nagata, Shoei Nashimoto, and Daisuke Suzuki. 2019. A low-cost replica-based distance-spoofing attack on mmwave fmcw radar. In *Proceedings of the ACM Workshop on Attacks and Solutions in Hardware Security*.

[28] Prateek Nallabolu and Changzhi Li. 2021. A frequency-domain spoofing attack on FMCW radars and its mitigation technique based on a hybrid-chirp waveform. *IEEE Transactions on Microwave Theory and Techniques* 69, 11 (2021), 5086–5098.

[29] Shoei Nashimoto, Daisuke Suzuki, Noriyuki Miura, Tatsuya Machida, Kohei Matsuda, and Makoto Nagata. 2021. Low-cost distance-spoofing attack on FMCW radar and its feasibility study on countermeasure. *Journal of Cryptographic Engineering* (2021), 1–10.

[30] John Nolan, Kun Qian, and Xinyu Zhang. 2021. RoS: passive smart surface for roadside-to-vehicle communication. In *Proceedings of the ACM SIGCOMM*.

[31] Ryu Okubo, Luke Jacobs, Jinhua Wang, Steven Bowers, and Elahe Soltanaghai. 2024. Integrated two-way radar backscatter communication and sensing with low-power iot tags. In *Proceedings of the ACM SIGCOMM*.

[32] Mihai Ordean and Flavio D Garcia. 2022. Millimeter-wave automotive radar spoofing. *arXiv preprint arXiv:2205.06567* (2022).

[33] Anurag Pallaprolu, Phillip Peng, Shaan Sandhu, Winston Hurst, and Yasamin Mostofi. 2024. Crowd Analytics with a Single mmWave Radar. In *Proceedings of the ACM MobiCom*.

[34] Akarsh Prabhakara, Tao Jin, Arnav Das, Gantavya Bhatt, Lilly Kumari, Elahe Soltanaghai, Jeff Bilmes, Swarun Kumar, and Anthony Rowe. 2023. High resolution point clouds from mmwave radar. In *Proceedings of the IEEE ICRA*.

[35] Akarsh Prabhakara, Diana Zhang, Chao Li, Sirajum Munir, Aswin C Sankaranarayanan, Anthony Rowe, and Swarun Kumar. 2022. Exploring mmWave Radar and Camera Fusion for High-Resolution and Long-Range Depth Imaging. In *Proceedings of the IEEE/RSJ IROS*.

[36] Kun Qian, Zhaoyuan He, and Xinyu Zhang. 2020. 3D point cloud generation with millimeter-wave radar. *Proceedings of the ACM IMWUT* 4, 4 (2020), 1–23.

[37] Kun Qian, Lulu Yao, Kai Zheng, Xinyu Zhang, and Tse Nga Ng. 2023. UniScatter: a Metamaterial Backscatter Tag for Wideband Joint Communication and Radar Sensing. In *Proceedings of the ACM MobiCom*.

[38] Kun Qian, Shilin Zhu, Xinyu Zhang, and Li Erran Li. 2021. Robust multimodal vehicle detection in foggy weather using complementary lidar and radar signals. In *Proceedings of the IEEE/CVF CVPR*.

[39] Rigol. [n. d.]. DP800 Series | High Performance Linear DC Power Supplies. https://www.rigolna.com/products/dc-power-loads/dp800/.

[40] Hailan Shanbhag, Sohrab Madani, Akhil Isanaka, Deepak Nair, Saurabh Gupta, and Haitham Hassanieh. 2023. Contactless material identification with millimeter wave vibrometry. In *Proceedings of the ACM MobiSys*.

[41] Jayanth Shenoy, Zikun Liu, Bill Tao, Zachary Kabelac, and Deepak Vasisht. 2022. Rf-protect: privacy against device-free human tracking. In *Proceedings of the ACM SIGCOMM*.

[42] Zhenguo Shi, Tao Gu, Yu Zhang, and Xi Zhang. 2022. mmbp: Contact-free millimetre-wave radar based approach to blood pressure measurement. In *Proceedings of the ACM SenSys*.

[43] Xian Shuai, Yulin Shen, Yi Tang, Shuyao Shi, Luping Ji, and Guoliang Xing. 2021. millieye: A lightweight mmwave radar and camera fusion system for robust object detection. In *Proceedings of the ACM IoTDI*.

[44] Emerson Sie, Xinyu Wu, Heyu Guo, and Deepak Vasisht. 2024. End-to-End Large-Scale SLAM with Small Radars. In *Proceedings of the ACM MobiSys*.

[45] Siglent. [n. d.]. SDG1032X Waveform Generator. https://siglentna.com/product/sdg1032x.

[46] Elahe Soltanaghaei, Akarsh Prabhakara, Artur Balanuta, Matthew Anderson, Jan M Rabaey, Swarun Kumar, and Anthony Rowe. 2021. Millimetro: mmWave retro-reflective tags for accurate, long range localization. In *Proceedings of the ACM MobiCom*.

[47] Zhi Sun, Sarankumar Balakrishnan, Lu Su, Arupjyoti Bhuyan, Pu Wang, and Chunming Qiao. 2021. Who is in control? practical physical layer attack and defense for mmwave-based sensing in autonomous vehicles. *IEEE Transactions on Information Forensics and Security* 16 (2021), 3199–3214.

[48] Mingyue Tang, Pranshu Teckchandani, Jizheng He, Hanbo Guo, and Elahe Soltanaghai. 2024. BSENSE: In-vehicle Child Detection and Vital Sign Monitoring with a Single mmWave Radar and Synthetic Reflectors. In *Proceedings of the ACM SenSys*.

[49] Rohith Reddy Vennam, Ish Kumar Jain, Kshitiz Bansal, Joshua Orozco, Puja Shukla, Aanjhan Ranganathan, and Dinesh Bharadia. 2023. mmspoof: Resilient spoofing of automotive millimeter-wave radars using reflect array. In *Proceedings of the IEEE Symposium on S&P*.

[50] Chao Wang, Feng Lin, Tiantian Liu, Kaidi Zheng, Zhibo Wang, Zhengxiong Li, Ming-Chun Huang, Wenyao Xu, and Kui Ren. 2022. mmEve: eavesdropping on smartphone's earpiece via COTS mmWave device. In *Proceedings of the ACM MobiCom*.

[51] Timothy Woodford, Kun Qian, and Xinyu Zhang. 2023. Metasight: High-Resolution NLoS Radar with Efficient Metasurface Encoding. In *Proceedings of the ACM SenSys*.

[52] Hongfei Xue, Qiming Cao, Chenglin Miao, Yan Ju, Haochen Hu, Aidong Zhang, and Lu Su. 2023. Towards generalized mmwave-based human pose estimation through signal augmentation. In *Proceedings of the ACM MobiCom*.

[53] Bin Yang, Runsheng Guo, Ming Liang, Sergio Casas, and Raquel Urtasun. 2020. Radarnet: Exploiting radar for robust perception of dynamic objects. In *Proceedings of the Springer ECCV*.

[54] Xi Zhang, Yu Zhang, Zhenguo Shi, and Tao Gu. 2023. mmfer: Millimetre-wave radar based facial expression recognition for multimedia iot applications. In *Proceedings of the ACM MobiCom*.

[55] Mingmin Zhao, Yonglong Tian, Hang Zhao, Mohammad Abu Alsheikh, Tianhong Li, Rumen Hristov, Zachary Kabelac, Dina Katabi, and Antonio Torralba. 2018. RF-based 3D skeletons. In *Proceedings of the ACM SIGCOMM*.

[56] Yuxuan Zhou, Huangxun Chen, Chenyu Huang, and Qian Zhang. 2022. WiADv: Practical and robust adversarial attack against WiFi-based gesture recognition system. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 6, 2 (2022), 1–25.

[57] Yi Zhu, Chenglin Miao, Hongfei Xue, Zhengxiong Li, Yunnan Yu, Wenyao Xu, Lu Su, and Chunming Qiao. 2023. TileMask: A Passive-Reflection-based Attack against mmWave Radar Object Detection in Autonomous Driving. In *Proceedings of the ACM CCS*.