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

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

[1]University of California San Diego, La Jolla, CA
[2]Northeastern University, Boston, MA

2023 IEEE Symposium on Security and Privacy (SP) | 978-1-6654-9336-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/SP46215.2023.10179371

***Abstract*—FMCW radars are integral to automotive driving for robust and weather-resistant sensing of surrounding objects. However, these radars are vulnerable to spoofing attacks that can cause sensor malfunction and potentially lead to accidents. Previous attempts at spoofing FMCW radars using an attacker device have not been very effective due to the need for synchronization between the attacker and the victim. We present a novel spoofing mechanism called mmSpoof that does not require synchronization and is resilient to various security features and countermeasures of the victim radar. Our spoofing mechanism uses a "reflect array" based attacker device that reflects the radar signal with appropriate modulation to spoof the victim's radar. We provide insights and mechanisms to flexibly spoof any distance and velocity on the victim's radar using a unique frequency shift at the mmSpoof's reflect array. We design a novel algorithm to estimate this frequency shift without assuming prior information about the victim's radar. We show the effectiveness of our spoofing using a compact and mobile setup with commercial-off-the-shelf components in realistic automotive driving scenarios with commercial radars.**

***Index Terms*—Millimeter-wave, FMCW Radar, Reflect array, Autonomous vehicles, Wireless, Sensing, Spoofing.**

1. Introduction

With the advent of autonomous cyber-physical systems, many safety and security critical applications rely on radars for enhanced real-time situational awareness. More specifically, mmWave frequency modulated continuous wave (FMCW) radars are used in many systems today as they provide robust object detection even under adverse weather such as fog and low-light scenarios, where other light-based sensors such as cameras and Lidars fail [1]–[4]. For example, they already play a critical role in advanced driver assistance systems (ADAS) [5] of modern automobiles for pedestrian and blind spot detection, adaptive cruise control, and emergency braking [6], [7]. Due to the precision and robustness of mmWave radars, they are also used to enhance the autonomy of unmanned aerial vehicles [8], [9], multilane traffic monitoring systems [10] and protect critical infrastructure, e.g., through robust detection of unauthorized drones [11], [12]. Given the nature of applications, it is imperative to investigate the security guarantees of mmWave FMCW radars against adversarial threats.

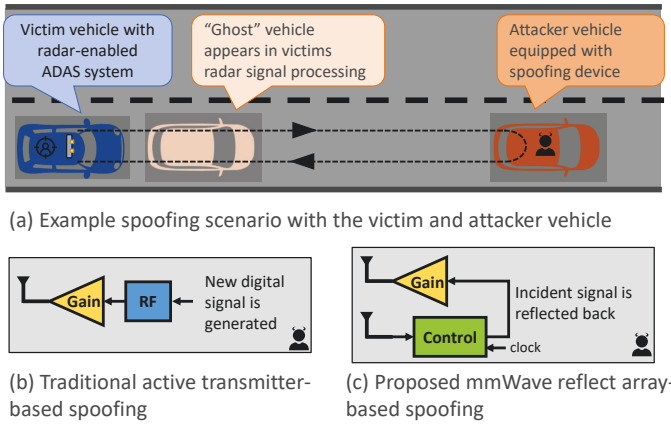


Figure 1: mmSpoof spoofing technique is based on a mmWave reflect array, and it does not require prior knowledge about victim radar, to spoof arbitrary distance and velocity values.

FMCW radars continuously transmit known chirp signal that bounces off objects and get reflected back. The radar receiver processes the received signal and detects the surrounding objects that caused the reflection. There are broadly two categories of attacks on a radar system: Jamming and Spoofing [13], [14]. Radar jamming occurs when the attacker radiates a noise signal at high power in the same frequency band as the radar [15]–[17]. This jamming signal saturates the radar making it blind and unable to operate normally. Since jamming causes the radar to malfunction and fail, it is easily detected [18]–[20]. In contrast, spoofing attacks are hard to detect; they try to manipulate the radar measurements by forcing it to detect "ghost" objects (which are not present in the environment) or miss actual objects in the environment. For instance, an attacker driving ahead of a radar-equipped victim's vehicle can manipulate the radar signals such that the victim radar measures a false distance to the attacker vehicle, as shown in Figure 1(a). Upon falsely detecting the attacker's ghost as a real vehicle, the radar may trigger the vehicle to apply a sudden brake, risking the

DOI 10.1109/SP46215.2023.00113

passenger's life and causing accidents.

Several studies have shown that FMCW radars are vulnerable to spoofing attacks [21]–[27]. In these works, the attacker uses an active transmitter to generate a spoofing signal, which is received by the radar and results in a spoofing attack (as shown in Figure 1(b)). However, these studies have several limitations. Firstly, they require the attacker to have complete knowledge of the radar signal parameters. Secondly, they assume or achieve perfect synchronization between the victim's radar and the attacker's hardware using wires. Finally, these methods are not robust to radar security measures [28]. For example, the radar can introduce short pauses in transmission to detect the spoofing signal or dynamically alter the transmit signal characteristics, such as the frequency sweep slope and the time period of individual chirps, to prevent successful spoofing.

We present mmSpoof, a robust and flexible spoofing mechanism using a millimeter-wave (mmWave) reflect array. Our reflect array captures the incident radar signal and reflects it towards the radar so that it is indistinguishable from the original radar signal but can still cause malicious detection that appears as a ghost object. In contrast to the active transmitter style, mmSpoof is based on the reflection of the radar's signal with a modulation that perturbs the properties of measured distance and velocity by the victim's radar as shown in Figure 1(c). The reflection-based spoofing model allows mmSpoof to eliminate the synchronization requirement between the victim radar and the attacker. Moreover, the security encoding of radar, if any, are preserved in a reflection-based attack, e.g., when the radar is paused, the reflections are paused too, thus making the attack robust to several security features and countermeasures of radar. mmSpoof's spoofing is also flexible to spoof any arbitrary distance and velocity at the radar without requiring synchronization between the victim and the attacker. We further develop a mechanism to learn important radar parameters required for spoofing in the background without assuming they are known to the attacker. In this way, mmSpoof is a robust and flexible spoofing mechanism.

■ **Asynchronous spoofing challenge:** A key challenge for mmSpoof is to flexibly spoof distance and velocity using reflect array without synchronizing it with the victim's radar. The reflect array should apply appropriate modulation to the incident signal to spoof the radar's measurements. For spoofing distance, one naive solution is to apply a configurable delay to the incident signal, which causes an increase in the time-of-flight of the signal as detected by the victim's radar. However, it only increases the distance between the victim and the attacker. We cannot reduce distance as it requires infusing negative delays, making the system non-causal. Our insight is to spoof shorter distances by leveraging the nature of radar chirp waveform that allows us to create a frequency shift (instead of delays) which manifests as a time shift due to a linear frequency-time relationship. It is easy to visualize that if the frequency shift is positive, then radar observes the attacker's ghost object closer than it is, and for a negative frequency shift, it appears farther. Therefore, the attacker can spoof an arbitrary distance on the radar by changing the frequency shift. Next, spoofing velocity is important to give the victim's radar a perception that the attack is realistic. For instance, in the automotive example, the attacker may want the spoofed velocity to lie in the range of typical driving speed limits or follow a specific pattern that mimics a vehicle's natural acceleration or braking. FMCW radar estimates velocity by measuring the Doppler frequency from the reflections received from objects in front of the radar. Therefore, we provide a novel mechanism to alter the Doppler frequency of the reflections by applying an appropriate frequency shift to spoof velocity.

■ **Decoupling distance and velocity challenge:** The next challenge for mmSpoof is to spoof distance and velocity independently. As discussed, applying frequency shift on the reflected signal creates arbitrary variations in the distance as desired, but it also induces random velocity change. i.e., a single knob (*frequency shift*) at the attacker changes two parameters (*distance and velocity*) at the victim's end. We call this issue *coupling* between distance and velocity spoofing and present a novel solution to decouple the two entities and spoof them independently. Our decoupling solution is inspired by two key observations. First, the granularity and fine-tuning of frequency-shift, where a small perturbation in frequency shift allows us to control the velocity spoofing without making significant changes in distance spoofing. Second, we leverage periodicity in velocity variations with frequency shift, i.e., two different frequency-shift would cause the same spoofed velocity. Therefore, we vary the frequency-shift with fine granularity to spoof velocity and with coarse granularity to spoof distance without affecting velocity. Thus, mmSpoof can flexibly and independently spoof distance and velocity.

■ **Realistic power variation challenge:** In addition to the distance and velocity, the attacker must also have control over the received signal strength at the victim's radar, allowing them to manipulate power levels to adhere to path loss regulations with the spoofed distance. For instance, spoofing shorter distances should have higher signal strength than spoofing longer distances. We achieve this by controlling the gain of the reflected signal with the spoofed distance. The distance-to-gain relationship is obtained from the known path loss models at the operating frequency. To attack with realistic power variations, We use a commercial phased array with a built-in gain control mechanism suitable for the required variable-gain spoofing.

■ **Parameter estimation challenge:** The final challenge for mmSpoof is to estimate the frequency-shift at the reflect array that creates flexible distance and velocity spoofing while being robust to various countermeasures in the radar. The frequency-shift calculation depends on important radar parameters such as the start frequency, chirp time, and chirp slope. The security features in radar may change these parameters occasionally or periodically to alter any interference or spoofing. Therefore, it is necessary to estimate these parameters in real-time at the attacker without giving any indication of the attacker's presence to the victim. We develop a novel digital signal processing mechanism to extract radar parameters. Our technique is based on analyzing

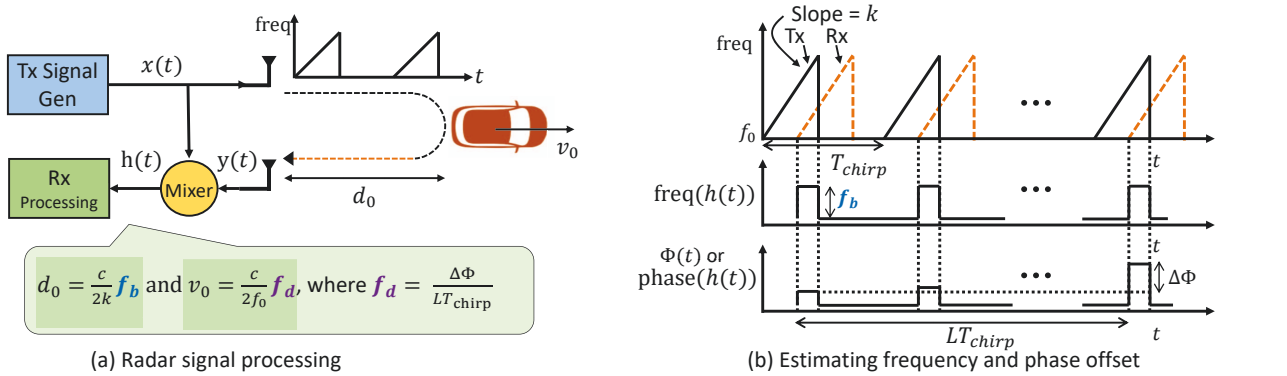


Figure 2: (a) Working principle of radar signal processing: It comprises a Tx signal generator, mixer, and Rx processing block. (b) **Top**: Transmit and receive a chirp signal. **Middle**: Frequency with time for channel $h(t)$ gives frequency offset estimation. **Bottom**: Phase variation of $h(t)$ over multiple chirps in a frame gives the phase offset Φ_Δ.

the spectrogram of the received signal and detecting known patterns of chirps found in the standard FMCW radars. We estimate the radar parameters periodically and use them to create the desired frequency shift for spoofing the radar.

■ **Demonstration and contributions:** We implement a proof-of-concept design of mmSpoof's reflect array using commercial-of-the-shelf components such as mmWave phased arrays with inbuilt mixers, a clock generator, and software-defined radio. We performed various outdoor experiments with a commercial 24 GHz radar mounted on a vehicle. We show that mmSpoof can spoof the radar for up to 100 m, even under mobile scenarios. Experimental results show that mmSpoof indeed creates flexible distance and velocity spoofing under various types of spoofing scenarios. We also present several countermeasures against our spoofing. We summarize our contributions below.

- Design of reflective array-based attack that does not require synchronization with the victim's radar.
- A novel method to independently spoof distance and velocity at victim's radar.
- Procedure to estimate victim's radar parameter and spoof both distance and velocity in real-time, which makes the system robust to several counter-measures.
- A robust attack that can control received signal strength at the radar following the path loss regulations with the spoofed distance.
- Demonstrated our attack's feasibility in static and dynamic scenarios using COTS hardware and spoofing practicality beyond a 100 m range.

2. Background on FMCW Radar

Frequency Modulated Continuous Wave (FMCW) radars transmit periodic frequency-modulated waves whose frequency increases linearly with time [29] as shown in Figure 2(a). One frequency increase cycle from its minimum to the maximum value is called a chirp signal. Radars sends a sequence of these chirps to the target object (Figure 2(b-Top)). One such sequence of chirps constitutes a radar frame. After reflecting from the object, this signal captures the round trip time-of-flight to the object, which carries information about the object's distance and velocity. The round-trip time-of-flight $\tau(t)$ is related to the distance d_0 between the radar and the object and velocity v_0 of the object relative to the radar as follows:

$$\tau(t) = \frac{2(d_0 + v_0 t)}{c} \tag{1}$$

where c is the speed of light. The FMCW radar measures this time-of-flight information through channel measurements from the received signal. The channel $h(t)$ is related to the time-of-flight as follows[1]

$$\begin{aligned} h(t) &= \alpha \exp(-j2\pi(f_b t + \Phi(t))) \\ f_b &= k\tau(t) \quad \text{and} \quad \Phi(t) = f_0 \tau(t) \end{aligned} \tag{2}$$

where f_b is ***beat frequency*** and $\Phi(t)$ is a time-varying phase term as shown in Figure 2(b). The radar parameters are represented by f_0 start frequency, k is chirp slope, and α is a constant that captures the environmental attenuation. Also, note how the beat frequency and the phase term are related to the time-of-flight $\tau(t)$. The radar measures these terms to estimate distance and velocity.

Distance Estimation: The FMCW radar estimates the distance by observing the received signal in a single chirp duration. The effect of velocity can be neglected in a short duration of a single chirp. Distance d_0 is estimated from the measured beat frequency f_b as:

$$\begin{aligned} f_b &= k\tau = \frac{2k}{c} d_0 \\ d_0 &= \frac{c}{2k} f_b \end{aligned} \tag{3}$$

where we approximated the time of flight in (1) at $t = 0$. This gives an estimate of target's distance.

Velocity Estimation: Unlike distance, velocity cannot be estimated using the beat frequency from a single chirp because the duration of the chirp is too small to measure changes in distance within a chirp reliably. Therefore, velocity estimation requires observing the phase change in the channel over multiple consecutive chirps in a frame

1. A detailed derivation of channel $h(t)$ is presented in Appendix A.

(Figure 2(b, Bottom)). We assume that all the chirps in the frame are equispaced, and the velocity does not change within the frame's duration. We then estimate velocity by taking the derivative of phase $\Phi(t)$ with time t as follows:

$$\frac{d\Phi(t)}{dt} = f_0 \frac{d\tau(t)}{dt} = \frac{2f_0}{c} v_0 \tag{4}$$

We refer phase derivative as ***Doppler frequency*** f_d, i.e.,

$$f_d = \frac{2f_0}{c} v_0 \tag{5}$$

Note the above phase differential can be computed practically by simply measuring the slope of phase with time[2]. Clearly, the velocity v_0 is estimated from f_d as

$$v_0 = \frac{c}{2f_0} f_d \tag{6}$$

So to summarize, beat frequency (f_b) from a single chirp gives us the distance estimate, and the Doppler frequency (f_d) gives us the velocity estimate. We will use this overview to explain our spoofing mechanism in Section 3.4.

Maximum measurable velocity: As described above, we use phase values to estimate the velocity in FMCW radar. As the phase values can only take values $\in [0, 2\pi]$, there is a limit on the measurable maximum velocity before it wraps around. The maximum measurable velocity [30] is given by

$$V_{max} = \pm \frac{c}{4f_0 T_{chirp}}, \tag{7}$$

where T_{chirp} is the chirp time.

3. mmSpoof: Spoofing FMCW Radar

We present mmSpoof, our spoofing mechanism for FMCW radars using a mmWave reflect array. mmSpoof has three components: i) reflect array design, ii) spoofing mechanism, and iii) parameter estimation.

3.1. Threat Model and Overview

We assume a victim vehicle equipped with FMCW-based radar for providing advanced driver assistance, including emergency braking and adaptive cruise control functions. The attacker's goal is to manipulate the distance and velocity measured by the victim's vehicle's radar. The adversary does not have any physical access to the victim's vehicle and uses a vehicle equipped with our mmSpoof. Our attack works as follows: The FMCW signal transmitted by the victim's radar is received at our mmSpoof attacker hardware. mmSpoof applies a configurable frequency-shift to the signal and transmits it back to the victim's radar. For the victim's radar, it appears as a regular reflection, and it estimates distance and velocity with the frequency-shifted received signal; this causes the radar to observe a spoofed distance and velocity.

2. In discrete domain, we obtain Doppler frequency as $f_d = \frac{\Delta\Phi}{LT_{chirp}}$, where T_{chirp} is the chirp time, and L is the total number of chirps in a frame, and $\Delta\Phi = \Phi(LT_{chirp}) - \Phi(0)$ is the phase difference between the first and the last frame.

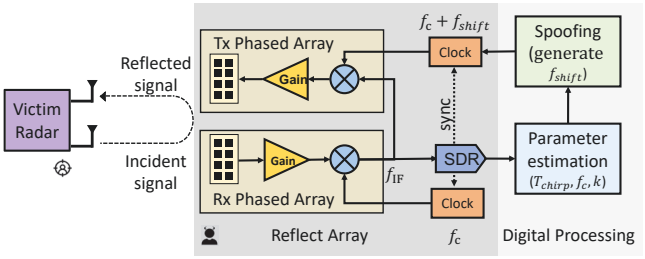


Figure 3: mmSpoof architecture design of our reflect-array. We use a pair of phased arrays with an integrated mixer for our transmit and receive module at the reflect array. We also use a pair of the synchronized clock to provide the IF frequencies to the Tx/Rx mixer with appropriate f_{shift}. Next, the Rx signal is digitized using an SDR that is used by our parameter estimation algorithm. Finally, we obtain f_{shift} using the estimated parameters.

In contrast to prior work [23], [24], our attacker does not require prior knowledge of the victim's radar parameters, such as the start frequency, chirp time, and chirp slope. We estimate these values at the attacker rather than assuming them. Our attack relies on reflections without any active chirp transmission, and we do not assume any wired or wireless synchronization between the victim and the attacker.

3.2. Reflect array architectural design

Reflect array is the main block in mmSpoof (Figure 3) and consists three components: i) Rx phased array, ii) Tx phased array, and iii) Software defined radio (SDR).

Rx phased array: Receive phased array consists of an antenna array that captures the victim radar signal. It then amplifies the weak signal with low-noise amplifiers and downconverts it to an intermediate frequency using a mixer that takes an external clock for the down-conversion. The clock frequency (f_c) is chosen as the difference between the RF and IF frequency. The downconverted IF signal is then sent to the Tx phased array.

Tx phased array: Transmit phased array is similar to the Rx phased array except that the mixer and the array work in the transmit mode, and there is an amplifier to provide signal gain. Here the mixer is fed with a different clock frequency ($f_c + f_{\text{shift}}$) to create the necessary frequency shift f_{shift} in the victim radar signal. The two clocks for the Tx and Rx chain of reflect array are PLL-synchronized. *Creating the configurable frequency shift using a set of mixers and clocks is the crux of mmSpoof's reflect array design architecture.* The Tx phased array transmits the frequency shifted signal towards the victim radar and performs the desired spoofing attack. The advantage of using an IF frequency is twofold: i) It allows us to repurpose commercial phased arrays at mmWave bands, which come with inbuilt mixers to downconvert the mmWave signal to an intermediate frequency. ii) We can use the same IF signal for digital processing using a splitter rather than building a separate mmWave receiver for parameter estimation. This simplifies our reflect array design and can be built using COTS hardware components.

Software Defined Radio (SDR): SDR downconverts the IF signal and samples them with analog to digital converters.

The digital signal is processed in software for parameter estimation and generation of configurable frequency shift.

3.3. How mmSpoof spoofs distance and velocity?

We provide a mechanism to manipulate the distance and velocity estimation on the radar. Our approach is to leverage the standard FMCW radar signal processing (Section 2) and determine the kind of alteration required in the received signal at the radar for the desired spoofing.

Distance spoofing: Say the attacker's vehicle is at a distance d_0 from the victim, but it wants the victim's radar to estimate distance d_{est}, such that

$$d_{est} = d_0 + d_{\text{spoof}}$$

where d_{spoof} is the relative spoofing distance. For this to happen, the attacker must create an additional beat frequency offset at the radar corresponding to the relative spoofing distance. The attacker achieves this by applying a frequency shift $\Delta f_{b-\text{spoof}}$ using the spoofing device as follows:

$$\begin{aligned} f_{b-est} &= f_b + \Delta f_{b-\text{spoof}} \\ \text{where, } \Delta f_{b-\text{spoof}} &= \frac{2k}{c} d_{\text{spoof}} \end{aligned} \tag{8}$$

Thus, if the attacker spoofing device can create a configurable beat frequency offset of $\Delta f_{b-\text{spoof}}$ in (8), then it can create a distance offset d_{spoof} w.r.t. the actual distance between the victim and the attacker.

Velocity spoofing: A configurable Doppler frequency offset can spoof the velocity. Let the attacker have actual velocity v_0, but it wants to spoof the radar to detect a velocity v_{est}:

$$v_{est} = v_0 + v_{\text{spoof}}$$

where v_{spoof} is the relative spoofing velocity. For this spoofing, the attacker must have a mechanism to create a Doppler frequency offset at the radar corresponding to the spoofing velocity.

$$\begin{aligned} f_{d-est} &= f_d + \Delta f_{d-\text{spoof}} \\ \text{where, } \Delta f_{d-\text{spoof}} &= \frac{2f_0}{c} v_{\text{spoof}} \end{aligned} \tag{9}$$

Thus, by setting the configurable doppler frequency offset $\Delta f_{d-\text{spoof}}$, the attacker can spoof the velocity relatively by v_{spoof} units as observed by the victim's radar. Here, we define two spoofing mechanisms: relative and absolute spoofing.

Relative spoofing: Relative spoofing implies that we only spoof relative to the actual distance. In this case, we do not need to know the actual distance d_0 or velocity v_0.

Absolute spoofing: Absolute spoofing indicates that we can spoof any absolute distance or velocity on the radar.

Relative spoofing suffices for most applications. So we assume that the attacker need not know the actual distance and velocity. However, if we get ground truth distance and velocity using other means such as radar, lidar, or camera, mmSpoof can also execute absolute spoofing.

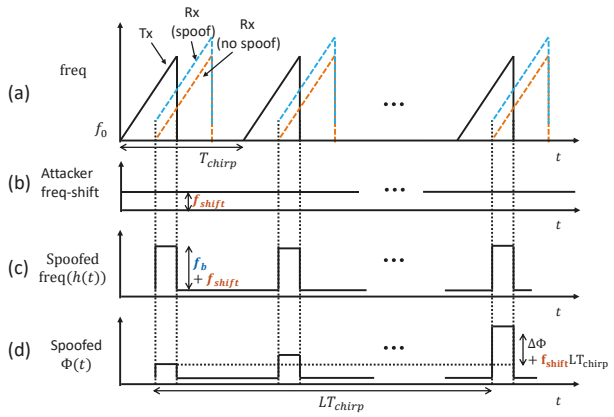


Figure 4: Radar spoofing principle. (a) Shows the Tx chirp and two Rx chirps, one without spoofing (orange) and the other with spoofing (blue). (b) The frequency shift created by attacker reflect array. (c) Radar estimated spoofed beat frequency as $f_b + f_{\text{shift}}$. (d) Radar estimated spoofed phase offset as $\Delta\Phi + f_{\text{shift}} LT_{\text{chirp}}$ for spoofing Doppler frequency and velocity.

3.4. Independently Spoofing Distance and Velocity

So far, we have seen how the victim radar can be spoofed while performing standard radar signal processing due to an alteration in the received signal at the radar. Specifically, modifying beat frequency causes distance spoofing, and modifying Doppler frequency causes velocity spoofing. A natural question is how an attacker can create such alterations for controlled distance and velocity spoofing. It is challenging to independently spoof distance and velocity because creating a frequency shift on the reflected signal generates both beat and Doppler frequency offsets in an uncontrolled manner. For instance, a frequency shift (f_{shift}) on reflected waves changes both beat frequency from f_b to f_{b-est} and doppler frequency from f_d to f_{d-est}.

$$\begin{aligned} f_{b-est} &= f_b + f_{\text{shift}} \\ f_{d-est} &= f_d + f_{\text{shift}} \end{aligned}$$

i.e., creating beat frequency offset and Doppler frequency offset by the same amount.

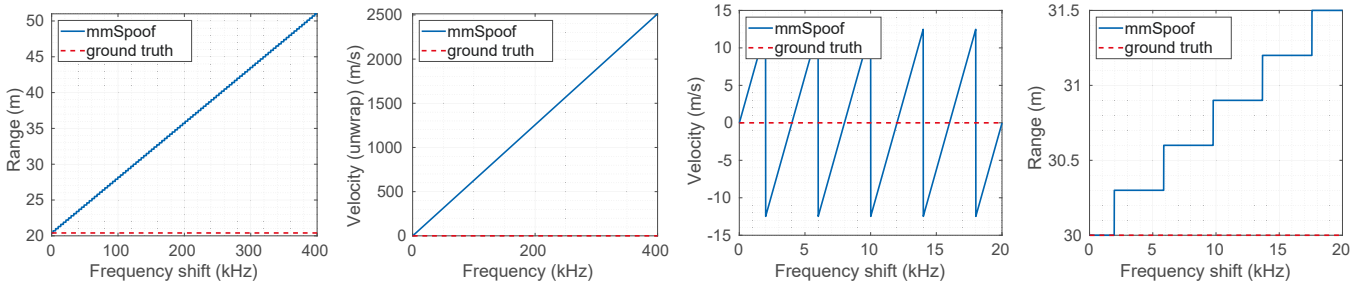
$$\begin{aligned} \Delta f_{b-\text{spoof}} &= f_{\text{shift}} \\ \Delta f_{d-\text{spoof}} &= f_{\text{shift}} \end{aligned} \tag{10}$$

This frequency shift causes a change in both distance and velocity estimated by the radar in an uncontrolled manner:

$$\begin{aligned} \Delta d &= \frac{c}{2k} f_{\text{shift}} \\ \Delta v &= \frac{c}{2f_0} f_{\text{shift}} \end{aligned} \tag{11}$$

We note that a frequency shift in the reflected signal changes both distance and velocity estimations (Figure 4). But does that mean spoofing distance and velocity? No, by spoofing distance and velocity, we mean that the attacker should independently control the distance and velocity.

■ **Coupling of distance and velocity spoofing:** The frequency shift f_{shift} induced on the reflected wave creates both



(a) Distance estimated on radar **(b)** Unwrapped velocity estimated on radar **(c)** Estimated velocity on the radar(Subset) **(d)** Estimated distance on the radar(Subset)

Figure 5: Shows the effect of frequency shift at the mmSpoof's reflect array on (a) distance spoofing and (b) velocity spoofing. In particular, (c) shows a subset of estimated velocity on the radar, which illustrates the periodicity in velocity over time with a linear increase of frequency shift on reflection. (d) shows a subset of estimated distance on the radar with frequency shift, which varies in steps of $\frac{1}{T_{\text{chirp}}}$ frequency.

beat and doppler frequency offsets, but it also creates an uncontrollable dependency on both distance and velocity. We define this as *coupling* – an unwanted artifact in spoofing distance and velocity, i.e., if the attacker tries to spoof distance using f_{shift}, in this process, it also causes a coupling effect that changes the velocity too.

Let us examine how increasing the frequency shift impacts radar distance and velocity estimation. We perform an experiment with $T_{\text{chirp}} = 250\mu s$ ($\frac{1}{T_{\text{chirp}}} = 4\ kHz$) and plotted distance and velocity variations with frequency shift. We linearly increased frequency shift over time and observed the changes in distance and velocity estimation. Figure 5a shows that distance increases linearly with frequency shift. As the frequency shift increases, the estimated velocity oscillates between a min and max value. To show the true effect of a frequency shift on velocity, we plot the unwrapped velocity over frequency shift in Figure 5b. It shows that unwrapped velocity increases linearly with frequency shift. Since both distance and velocity change for the same frequency shift, this approach couples distance and velocity spoofing.

■ **Decoupling distance and velocity spoofing:** A naive way to remove this coupling is to choose f_{shift} to spoof the distance correctly and then remove the unintended coupling in velocity spoofing by providing a variable phase offset on a per-chirp basis. In other words, the attacker can spoof velocity independently if it can somehow modify the reflected signal's phase by $(\Delta f_{d-\text{spoof}} - f_{\text{shift}}) \times \ell T_{\text{chirp}}$ on a per-chirp basis, where $\Delta f_{d-\text{spoof}}$ is defined in (9). This way, the attacker can create velocity spoofing independent of distance. The problem is that it requires the attacker to modify the phase of the reflected signal on the per-chirp basis in addition to creating the frequency shift f_{shift}. Creating a per-chirp phase requires tight synchronization between the attacker and victim vehicle, which is not practical wirelessly due to the typical short nano-second chirp duration.

In contrast, we propose a novel way to remove the distance-velocity coupling without requiring synchronization. Our key insight is to fine-tune frequency shift so that a single shift can cause independent distance and velocity spoofing. We make two observations: First, if we linearly vary the frequency shift on the reflected wave, velocity spoofing follows a periodic pattern with the values going from min to max value multiple times over a short duration while the distance is approximately static. Second, velocity spoofing requires a minimal frequency shift, whereas distance requires a high-frequency shift. It is because variations over a longer time scale (frame level) are required to observe the change in velocity, which means a small change in frequency (inverse relationship with time interval). In contrast, distance varies over a shorter time scale (chirp level), thus requiring a large frequency shift to observe a reasonable change. Also, if the object moves at a higher speed than the radar's range, it wraps the velocity to bring it within range, causing periodicity. For instance, if the radar range is from -12.5 to 12.5 m/s, if the object is moving with a speed of 15 m/s, radar estimates it as -10 m/s, after 12.5 m/s, it wraps around to -12.5 m/s.

With this intuition, we perform a simple study to make our claims concrete. We linearly increase frequency shift from 0 to 20 kHz, with $T_{\text{chirp}} = 250\mu s$ [31]. As demonstrated in Figure 5c, we observe that velocity periodically repeats after every $\frac{1}{T_{\text{chirp}}}$frequency, during which the change in the distance is just 0.6 m (Figure 5d). Hence, we use the periodicity of velocity spoofing and robustness of distance to small frequency shifts as two key ingredients to decoupling distance and velocity spoofing.

Decoupled Velocity spoofing: We can spoof any velocity by giving a frequency shift between 0 and $\frac{1}{T_{\text{chirp}}}$. The spoofed velocity is related to frequency shift as:

$$v_{\text{spoof}} = \frac{c}{2f_0} f_{\text{shift}} \tag{12}$$

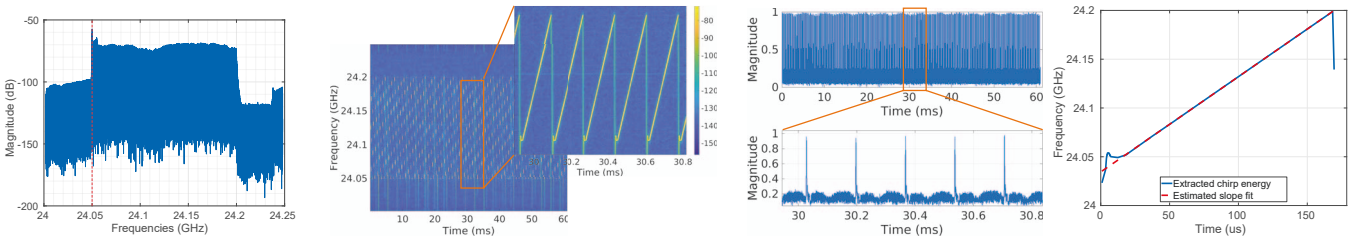
Decoupled Distance spoofing: Unlike velocity, we spoof distance in steps. Our insight is to select frequency shift in multiples of $\frac{1}{T_{\text{chirp}}}$ that causes no change in velocity while spoofing any arbitrary distance as follows:

$$\begin{aligned} \Delta d_{step} &= \frac{c}{2k} \frac{1}{T_{\text{chirp}}} \\ d_{\text{spoof}} &= n \Delta d_{step} \end{aligned} \tag{13}$$

where Δd_{step} is distance step size, and n is the number of distance steps the attacker wants to spoof. One limitation is we can only spoof in multiples of distance step size, similar to quantization accuracy loss in digital systems.

■ **Granularity and Range of Spoofing**

Granularity in distance: We perform distance spoofing in



(a) Analyzing frequencies of the received signal to estimate start frequency (f_0)

(b) Spectrogram of the received signal illustrating victim radar's chirps with frequencies swept and time duration of data collection

(c) Extracting energy out of the chirps and identifying repetitions of chirps and estimate chirp time (T_{chirp})

(d) Extracting single chirp out of the received signal and estimating slope (k)

Figure 6: mmSpoof Parameter estimation at the attacker: estimating different parameters such as radar start frequency, chirp time, and chirp slope.

discrete steps by applying discrete frequency shifts. The distance step size given in (13) is small and negligible in the context of autonomous driving. For instance, a radar with chirp slope $k = 1.95e12$ and chirp time $T_{\text{chirp}} = 250\ \mu s$ gives the distance step of 30 cm, which is in order of the fundamental distance resolution of the radar. Therefore, the effect of the distance step is negligible on the radar.

Granularity in velocity: In contrast to distance, velocity variations are continuous with the frequency shift as described in (12). Therefore, velocity granularity depends on the smallest frequency shift provided at reflect array:

$$\Delta v_{min} = \frac{c}{2f_0}(f_{\text{shift}})_{min} \tag{14}$$

This explains that, theoretically, there is no minimum limit for velocity spoofing. Practically, it is limited by the minimum frequency shift that the hardware provides.

Range: Theoretically, as we increase the frequency shift, both distance and velocity reach their max limit and then start again from the min value. As we see in Figure 5c, with the increase in frequency shift, the estimated velocity sweeps between minimum velocity to the maximum velocity value that radar can handle. Similarly, distance will also sweep between the min and max values as we increase the frequency shift on the reflected wave. Thus, mmSpoof can fully spoof the range available on the radar for distance and velocity.

3.5. Radar Parameter Estimation

To spoof velocity and distance, we first need to estimate the start frequency, slope, and chirp interval time T_{chirp} of the radar. The IF down-converted signal from the reflect array is captured and used for the parameter estimation.

3.5.1. Radar start frequency (f_0) estimation

For carrier start frequency estimation, we sweep the entire bandwidth and analyze the frequency response of the received signal. Capturing the entire bandwidth over time allows us to precisely estimate the energy levels at all the frequencies and identify the start frequency.

For instance, to find the start frequency for the 24 GHz radar, we sweep the entire band, i.e., 24 - 24.25 GHz. Our system is capable of instantly sweeping up to 245.76 MHz bandwidth. Thus, we capture the entire band at 24 - 24.25 GHz and apply FFT over the input time domain signal to determine the frequency response. we apply an averaging function on the frequency response and estimate the start frequency of the radar as illustrated in Figure (6a). This approach can also be made by sweeping smaller bandwidths multiple times to cover the entire band. For instance, we can divide the entire 250 MHz bandwidth into five parts and sweep one 50 MHz at a time. This will reduce the system's higher bandwidth requirement but increase the time to estimate start frequency.

3.5.2. Radar chirp time (T_{chirp}) estimation

From the received signal, we first find out the spectrogram (6b), which gives us the energy levels over different frequencies with respect to time. Typically radar has some idle time within each chirp and also in each frame. The spectrogram will depict chirp time slots with high energy and others with noise, indicating idle time. we remove the noise and focus only on the time slots with relatively high energy. After filtering only the time slots with high-energy signals, we sum the energies across all the frequencies and term them as energy rows. We then identify the time energy rows to find chirp time. Finally, We estimate chirp time by taking the mode of the time gaps between peaks in the energy rows. Figure 6c shows energy rows extracted from the spectrogram, the peaks in the figure correspond to chirp energy levels, and the time difference between these peaks gives us the chirp time.

3.5.3. Radar slope (k) estimation

Now that we have the chirp time and the location of chirps from energy levels, we extract a single chirp to estimate the slope of the chirp, as shown in Figure 6d. The spectrogram of this extracted chirp gives us the energy levels over different frequencies with respect to one chirp time. We first sum the energy levels over all the frequencies and determine the chirp's active time where there are significant energy levels. We track peak energy over all the frequencies for the active chirp time and estimate the corresponding slope.

4. Implementation and Evaluation Setup

In this section, we describe mmSpoof's implementation and the experimental setup used for static and relative velocity experiments between attacker and victim.

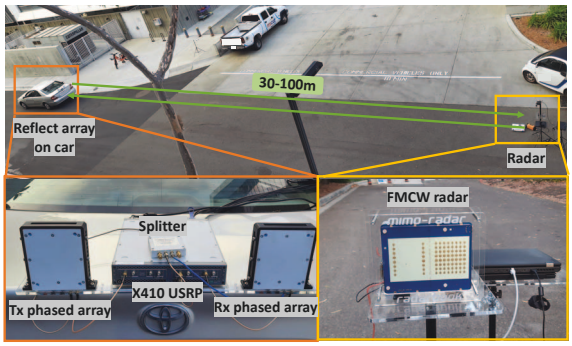


Figure 7: The experimental setup consists of the mmSpoof device mounted on a car, with the radar on a tripod. The top picture shows an overview of the setup, while the bottom figure shows a zoomed-in view.

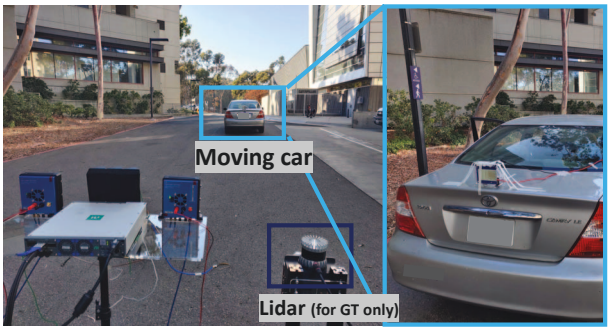


Figure 8: Outdoor experiments showing spoofing with a relative velocity between victim and attacker. The radar is placed on a moving car, and the reflect array is static on a tripod. We use lidar to collect the ground truth.

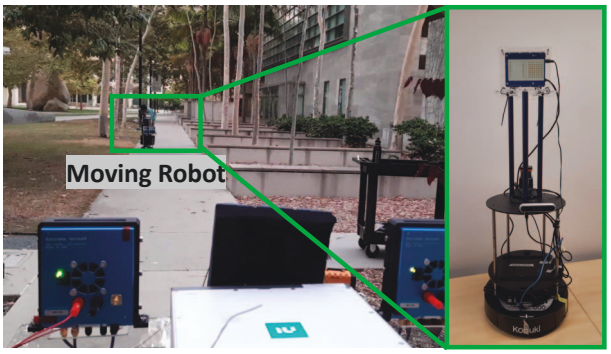


Figure 9: The left figure shows the radar placed on a robot moving with a controlled routine to perform repeatable experiments. The right figure shows how we mount the radar on the robot.

4.1. Implementation of mmSpoof

To implement mmSpoof, we use a set of two commercial off-the-shelf (COTS) phased arrays for receiving and transmitting signals and an X410 USRP for supporting digital processing and providing clocks as shown in Figure 7.

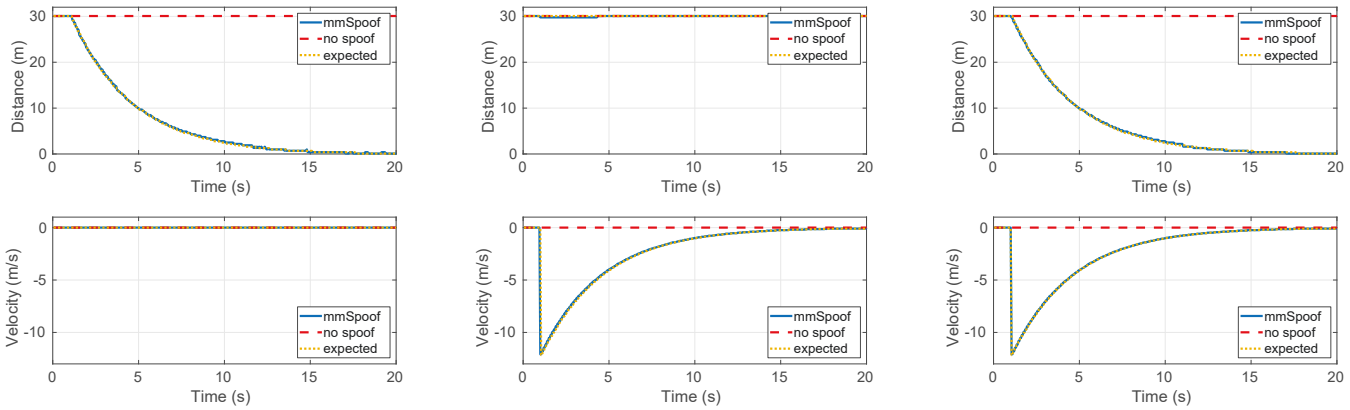
Phased arrays: We used COTS phased arrays from Extreme Waves [32] which support millimeter wave frequencies. These are equipped with 8x4 horizontal and vertical polarized antennas. We used only 8 antennas as a linear array in vertical polarization for beam direction. The phased arrays have an in-built mixer designed to downconvert from the mmWave Radio frequency (RF) range (24.125 GHz) to the Intermediate Frequency (IF) range (2-6 GHz) and to upconvert the signal from the IF range to the mmWave RF range. The Rx phased arrays take a clock as input and downconvert the received RF signal to an IF signal. Similarly, Tx phased arrays take both IF signal and clock as input and upconvert and transmit RF signals. We set the clock for Rx phased array at 5 GHz, and the built-in mixer has a multiplication factor of 4, which is multiplied by the clock creating a 20 GHz clock. The Rx array will receive a signal at 24.125 GHz (radar center frequency) and downconvert RF to IF signal to 4.125 GHz (24.125 GHz - 20 GHz). Further, for the transmitting array, we give clock 5 GHz + $f_{\text{shift}}/4$ (1/4 is because it is multiplied with factor 4 in the mixer) and IF at 4.125 GHz, which then upconverts and transmits at 24.125 + f_{shift} thus creating a frequency offset of f_{shift} on the reflected wave. Also, the gain on phased arrays is controllable, which helps us to control the gain that victims can observe on the radar. The IF signal from Rx phased array is connected to the splitter and sent to both Tx phased array and SDR. The inbuilt mixers in phased arrays also require two clocks (5GHz and 5GHz + $f_{\text{shift}}/4$).

Implementing clock with SDR: We provide a mechanism to generate the clock using SDR. To generate a 5 GHz clock, we first digitally create an exponential signal at 100 kHz and send it to SDR to transmit at 5 GHz. How to generate 5GHz + $f_{\text{shift}}/4$? similar to how we generated a 5 GHz clock, we can generate an exponential signal with 100 kHz + $f_{\text{shift}}/4$ frequency instead of 100 kHz in the other case. SDR's primary job is to take 100 kHz and 100kHz + $f_{\text{shift}}/4$ signals and transmit at 5 GHz frequency. Typically we can use any suitable COTS SDR device for this purpose. We used X410 USRP for transmitting at 5 GHz with a 3.48 Msps sampling rate which is feasible with any 2 TX channels USRP.

Digital Processing: To calculate the required frequency shift for spoofing, we perform parameter estimation using digital samples of the captured radar signal. We collect digital samples from SDR and apply digital processing for parameter estimation. X410 USRP is connected to the Laptop via an SFP cable to do the digital processing. The advantage of having X410 is that it can receive data with a 245.76 Msps sampling rate; this helps us sweep the approximately 250 MHz band and estimate the parameters in a single shot following methods in Section 3.5. Using the desired spoofing distance and velocity and estimated chirp parameters, we calculate f_{shift} and feed it to the USRP to generate the appropriate clocks.

4.2. Experimental setup

We mainly have two components (FMCW radar and reflect array) to evaluate our spoofing design and algorithms. We used a commercial FMCW radar at the victim's end and reflect array at the attacker. Figure 7 summarizes our static setup and Figures 8, 9 demonstrate relative scenarios. Here we discuss how we used the COTS radar as the victim and describe our setup for the three scenarios.



(a) Spoofing only distance **(b)** Spoofing only velocity **(c)** Spoofing both distance and velocity

Figure 10: mmSpoof evaluations showing system abilities in spoofing distance and velocity independently.

We used the 24 GHz Radarbook2 radar platform from INRAS [31]. It is a MIMO radar with two transmit and eight receiver antennas. We use one transmit and eight receive chains to collect the data. For spoofing experiments, we configured the radar with an up-chirp time of 128 μs and 512 samples with up-chirp. A chirp time of 250 μs and 100 chirps per frame. The frame time used is 50 ms. The radar transmits FMCW chirps and estimates the distance and velocity from the received reflections.

For static experiments, we wanted to show how our system performs when there is no relative velocity between the attacker and the victim. As shown in Figure 7, the radar is mounted on a tripod, and reflect array is positioned on the car. We varied our experiments from 30 m to 100 m range and showed our evaluations in Section 5.

We performed two types of experiments to show our system's performance in relative scenarios. First, we showed relative spoofing with radar on the car. As shown in Figure 8, we placed radar on the Toyota Camry car, and reflect array is static on a tripod and evaluated with relative velocity. We also used lidar for collecting ground truth for relative scenarios. Next, we show absolute spoofing with a robot. The goal is to show that if we know the ground truth or actual distance and velocity, mmSpoof can do any absolute spoofing. As illustrated in Figure 9, we mounted the radar on the robot and placed reflect array static on the tripod. We used a robot to perform repeatable experiments and evaluated our system to spoof various scenarios.

5. Experimental Evaluation

In this section, we evaluate mmSpoof in multiple challenging scenarios. The evaluation is mainly divided into two categories: i) Static scenarios where the victim radar and mmSpoof are at a fixed distance and ii) dynamic scenarios where there is a relative motion between the radar and mmSpoof system. For each of the experiments, we evaluate the spoofing accuracy, i.e., the error between the expected and actual spoofed value. Finally, we also evaluate the accuracy of mmSpoof's parameter estimation, which is important to spoof the victim radar accurately.

5.1. Static Scenarios

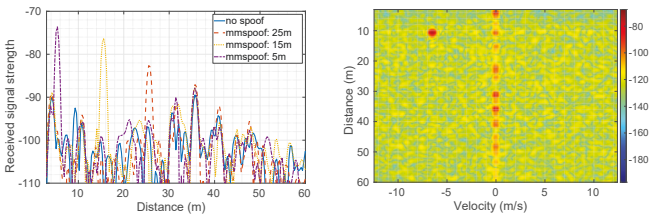
Here, we evaluate mmSpoof for the cases when there is always a fixed distance between the victim and the attacker. Such cases can be encountered either when the attacker and victim are stationary or moving at the same speed in the same direction. We evalaute three spoofing categories: i) only-distance, ii) only-velocity and iii) both distance and velocity spoofing to exhaustively cover all possible cases.

5.1.1. Spoofing distance and velocity independently

In this subsection, we show that mmSpoof can spoof both distance and velocity independently. First, we show that distance can be spoofed independently without spoofing velocity, and then we show velocity-only spoofing.

Only distance spoofing: First, we consider the case where the attacker only spoofs a fixed distance between the victim and itself without any change in velocity. For this scenario, we used the setup shown in Figure 7, where victim radar and mmSpoof attacker are spaced 30 m apart. The victim radar is mounted on a car and the mmSpoof system is kept in line behind it. We conduct the experiments outdoors to mimic a real-world setting. We first examine the reflected signal without spoofing over time (shown as the red curve in Figure 10a) at a fixed distance of 30 m. Next, we turn on our mmSpoof system and spoof a varying distance on the victim's radar. In this particular case, we show how mmSpoof can spoof an exponential decrease in the distance as measured by the victim radar (shown in blue in Figure 10a). Note that the velocity measured by the victim remains unaltered. We can spoof any distance pattern we want to create on the victim's radar without limiting it to an exponential case. We chose exponential as it covers a wide range of distances showing the capability of mmSpoof to spoof any chosen distance.

Only velocity spoofing: Next, we consider the case where the attacker spoofs only the victim's velocity. As before, we



(a) mmSpoof gain control validation with the real car at 35m distance to three spoofing ranges: 25m, 15m, and 5m.

(b) Range-Doppler FFT of mmSpoof spoofing original car at 35m and static(0m/s) case to 10m and 6.5m/s.

Figure 11: Evaluation of mmSpoof's ability to spoof distance with controllable gain, showing the system's ability to spoof a real car with an actual distance of 35m between the victim (car) and attacker (reflect array).

first examine the no spoof case and then apply spoofing to see whether the velocity at the victim's radar is impacted. As shown in Figure 10b, we can accurately spoof velocity with no significant change in the distance. The blue curve shows the exponential rise in the velocity measured at the victim radar because of spoofing and the red dashed line is the measured velocity when there is no spoofing. With mmSpoof, we have a precise and accurate control over the spoofed velocity allowing the attacker to spoof any desired pattern i.e., not limited to the exponential rise.

5.1.2. Simultaneous distance and velocity spoofing

In the previous sections, we showed how mmSpoof could be used to independently spoof a victim's distance and velocity. Now, we will show how we can create specific attack scenarios by simultaneously spoofing both distance and velocity. We use the same experimental setup as before, where the victim radar is mounted on a car that is at a fixed distance of 30 m behind the attacker car equipped with mmSpoof. Both the victim and attacker are moving at the same speed and thus the relative speed as measured by the victim radar without any spoofing is 0 m/s. This is shown as the red curves in Figure 10c where the victim radar measures a fixed distance of 30 m and a relative velocity of 0 m/s. Now, we use our mmSpoof to spoof an exponential drop in distance and an exponential rise in velocity. The blue curve shows the measured values after the spoofing is turned on. This experiment demonstrates that mmSpoof can create any desired pattern in the measured distance and velocity simultaneously. As mentioned, these experiments are evaluated with reflect array on a real car (Figure 7); we show that mmSpoof has a significantly high gain compared to the car reflections, hence the spoofing is feasible even with a car. Furthermore, our setup also has big metal gates and other environmental reflectors, but the spoofing is unaffected by these reflectors.

5.1.3. Realistic gain control with spoofed distance

In this subsection, we discuss how an attacker can control the gain at mmSpoof and change the received signal strength as seen on the victim's radar to mimic real objects or cars. We performed the experiment as shown in Figure 7, with mmSpoof on car and radar static. The actual distance of the car is 35 m. Here we show how an attacker spoof three ranges from 35 m to 25 m, 15 m, and 5 m, respectively. Ideally, if we spoof with the same gain, it is possible for the radar to detect that it may be an anomaly or an outlier and disregard the spoofed distance because of inappropriate distance and gain values. Consequently, the attacker must also have control over gain for an undetectable attack. As demonstrated in Figure 11a, The blue curve is the case with no spoof where the radar detects the range as 35 m. Then for the next three plots, orange, yellow, and purple, the measured distance is 25 m, 15 m, and 5m, respectively. To do this, the attacker spoofs with a relative distance of -10 m, -20 m. and -30 m with an increase in the gain at each spoof. The attacker can control the gain by adjusting the gain parameter to both Tx and Rx phased arrays. With mmSpoof, we have gain control over 30 dB per phased array, which suffices for the target applications. Figure 11b represent a range-Doppler plot, where the actual car is at 35 m, but the attacker is spoofing -15 m and -6 m/s. such that the victim estimates the distance as 10 m.

5.2. Dynamic Scenarios

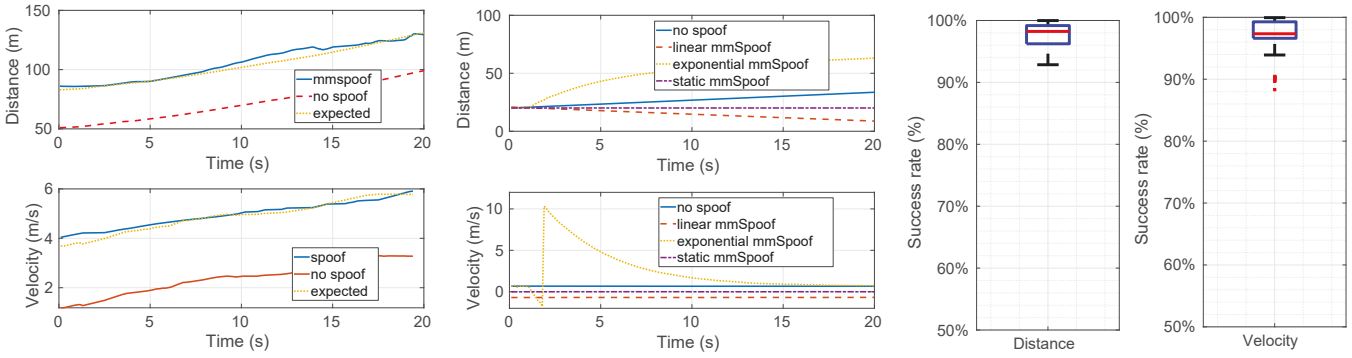
Though spoofing in static scenarios has its own applications, many real-world scenarios need spoofing when there exists a non-zero relative velocity. In this section, we evaluate our system when there is a relative velocity between the attacker and the victim's radar. We perform two kinds of experiments: i) Realistic evaluations with a moving car and ii) controlled experiments by using a Turtle bot.

5.2.1. Relative spoofing with a moving car

Here we will evaluate mmSpoof's spoofing performance against a moving victim car in a realistic setting. We place the radar on a car to mimic the victim vehicle and mount mmSpoof in the line of sight as shown in Figure 8. For a moving car case, we do not have the instantaneous distance and velocity measurements of the victim car. Hence, we spoof a relative distance and velocity with respect to the original distance and velocity of the vehicle. We use a lidar sensor placed near mmSpoof to capture the ground truth distance and velocity of the victim radar.

To showcase the spoofing, we use mmSpoof to spoof a constant offset of 30 m in distance and 2 m/s in velocity with respect to the original distance and velocity of the vehicle. The results are shown in Figure 12a. The measured distance and velocity on the radar are given by the blue dotted line. The thick orange line indicates the estimated distance after outlier removal, and the red dashed line is the ground truth estimated using lidar. As expected, the victim radar measured a distance shifted $\approx 30\ m$, and the measured velocity contains an additional 2 m/s. Note that we can spoof any distance and velocity pattern with mmSpoof and are not limited to this constant offset. mmSpoof supports spoofing ranges of over 100m (Figure 12a).

Unlike static or controlled motion experiments, scenarios with moving cars are not repeatable. Therefore, we cannot show the accuracy of spoofing with error bars at multiple points. Instead, we show the accuracy by comparing the



(a) mmSpoof system spoofing validation with a moving car and capturing groundtruth with lidar.

(b) Using a robot for ground truth collection and evaluating both relative and absolute spoofing.

(c) Spoofing distance validation (moving car scenario)

(d) Spoofing velocity validation (moving car scenario)

Figure 12: Evaluation of mmSpoof's ability to spoof both distance and velocity in dynamic scenarios where there is a non-zero relative velocity between the attacker and victim.

expected results from lidar ground truth to the measured values on the victim's radar. We have over 400 data points out of multiple evaluations to validate the spoofing accuracy. Figure 12c shows that we have a median success rate of 98.23% (≈1.8% error). While the minimum and maximum success rates range from 92.85%(≈7.2% error) to 99.98%. Figure 12d shows that for spoofing velocity in a moving car scenario, we have a median success rate of 97.34%(≈2.7% error). Where minimum and maximum success rates range from 93.91% (≈6.1% error) to 99.43% with a few outliers around 89.86%. Ideally, these errors will be either due to parameter estimation errors or due to channel effect with relative motion. Our system can estimate parameters with very high accuracy (as illustrated in Figure 13), i.e., these distance and spoofing deviations are due to the relative movement between the attacker and the victim. Note that static scenarios are with perfect parameter estimates and no relative motion. Hence, static spoofing scenarios (as given in Figure 10) are near perfect, accurately aligning with the expected plots.

To understand the impact of these errors on spoofing distances and velocity, we provide a few examples. The median 1.8% error distance is small for any practical scenario. For instance, spoofing a 30m scenario, 1.8% error leads to 0.54m deviations. 0.54m deviation in the automotive context is relatively very small. Further, even the worst-case scenario leads to a 2.16m deviation, i.e., spoofing 30m will lead to 27.84m which is acceptable to many target applications. Similarly, 2.7% median and 6.1% maximum deviation in velocity when spoofing an additional 10m/s (22.36 mph) lead to a median error of 0.27m/s and maximum error up to 0.61m/s which for many practical purposes can be considered as insignificant. Thus, we show the practicality of mmSpoof with both static and dynamic scenarios.

5.2.2. Controlled experiments with a robot

In the previous experiment, we showed how mmSpoof can spoof a relative offset on the measured distance and velocity of a vehicle. This experiment shows how we can spoof an absolute distance or velocity on the victim's radar. As mentioned earlier, the instantaneous distance and velocity measurements of the victim's vehicle are required to perform absolute spoofing. Hence, we performed experiments using a Turtle bot [33], which can run with a predefined speed routine. The experiment's goal is to generate arbitrary distance and velocity patterns as we know the instantaneous speed and distance of the robot (predefined values). In a real-world setting, these values can be obtained by using another radar placed on the attacker vehicle, e.g., Lidar. The blue curve in Figure 12b shows the original velocity and distance of the Turtle bot without any spoofing. Now, we use mmSpoof to generate different patterns in distance and velocity. For each experiment, we repeat the same routine on the Turtle bot. As the Turtle bot is moving from 20 m to 35 m, there is a linear increase in distance and positive velocity in the no-spoof case. Next, we perform linear spoofing such that it appears that the robot is coming closer to the attacker with the same velocity, which is shown by the linear decrease in distance and the same absolute negative velocity (red dashed line). Then, we spoof such that the distance increases exponentially while the velocity suddenly rises and decreases exponentially (yellow dotted line). Finally, we spoof a static distance, i.e., the same position where it started with zero velocity (purple dash-dot line). Through this experiment, we show the capability of mmSpoof to spoof any arbitrary pattern of distance and velocity on the victim.

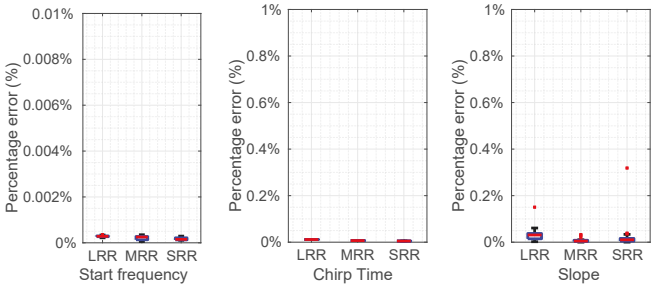
5.3. Parameter estimation

To accurately spoof distance and/or velocity, mmSpoof needs to accurately estimate the start frequency (f_0), chirp time (T_{chirp}), and slope (k) of the victim's radar. We estimated these parameters as discussed in section 3.5.

We evaluated our system's performance with different radar modes in Table 1. In an automotive context, short-range radar (SRR), mid-range radar (MRR), and long-range radar (LRR) are employed for different applications, such as collision avoidance and corner detection [34]. Almost all COTS radar systems use the FMCW mechanism, with variations in chirps parameters to enable different modes. We approximated the parameters based on TI's chirp con-

Radar Modes	f_0 (GHz)	T_{chirp} (μs)	k ($\frac{MHz}{\mu s}$)	Range Max (m)	Range Res (m)	Velocity Max (m/s)	Velocity Res (m/s)
LRR	24.075	114.80	1.0121	228	1.5	27	0.27
MRR	24.050	169.60	0.9765	148	1.0	18	0.18
SRR	24.025	195.20	1.1161	48	0.5	15	0.15

TABLE 1: Configurations of Long/Mid/Short Range Radar (LRR, MRR, and SRR) modes.



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

Figure 13: mmSpoof parameter estimation evaluation showing percentage errors for parameter estimations with respect to three radar modes LRR, MRR, and SRR.

figurations for 77GHz [34] to fit radar configurations at 24 GHz as pointed in Table 1. Radar parameters are considered based on the maximum unambiguous range, range resolution, maximum unambiguous velocity, velocity resolution, and different start frequencies.

We examined our parameter estimation algorithms over 100 experiments with the attacker and victim distance varying from 5m to 100m and in three radar modes. Figure 13a illustrates that the maximum estimation error is less than 0.0005%. We can sweep the entire range and accurately estimate the start frequency of the victim's radar. We have also evaluated the system by varying f_0 between 24 to 24.25 GHz in all scenarios estimation errors are within provided range. Figure 13b gives the box plot of chirp time estimation percentage errors. The chirp time varies for different modes according to the maximum unambiguous velocity requirement. Evaluations indicate that the median error of all three modes is less than 0.02%. Figure 13c demonstrates the box plot of slope estimation percentage errors. The slope varies for all modes as corresponding bandwidth and chirp up-ramp time varies according to the given range and velocity requirements. Our results show that the maximum median error for all modes is less than 0.05%. These results demonstrate the robustness and accuracy of our system with different radar modes. Thus, mmSpoof can potentially estimate radar parameters of any COTS radar with the above modes and spoof with high accuracy.

6. Related Work

Attacks on FMCW radars have been studied for over a decade, with some early works focusing on the theoretical possibilities without any detailed attacker architecture or real-world implications [35]–[39]. Recent demonstrations use either an active transmitter or passive reflection-based attacker, both making certain assumptions or unrealistic setups to do controlled experiments. mmSpoof is the first work that demonstrates the vulnerability of FMCW radars in the wild with commercial-of-the-shelf 24 GHz radar and a robust mmWave reflect array setup.

■ **Active transmitter-based attacks:** Radar spoofing attacks based on active transmitters [21]–[27] generate synchronized chirp waveforms and transmit them towards the radar. The radar receives this spoofing signal and detects ghost objects within the victim radar's field of view. A key requirement for this type of attack is perfect attacker synchronization in frequency, phase and transmission start time with the victim radar. Any mismatch in frequency or phase synchronization would invalidate the spoofing waveform at the victim. For automotive mmWave radars at 24 GHz, the attacker needs sub-nanosecond tight synchronization. It is hard to achieve this level of synchronization wirelessly without specialized hardware on the victim's vehicle. Therefore, these works demonstrate spoofing on a custom SDR with a wired link between the victim and attacker in a controlled lab environment. For instance, the setup of Kommissarov et al. [26] consists of two bladeRF SDRs (victim and attacker) connected by 15 m long RF cables. Asynchronous attacks were attempted with marginal success for distance spoofing in [40]. In contrast, mmSpoof eliminates the need of synchronization as it manipulates and reflects back the victim radar signals and successfully achieves asynchronous distance and velocity spoofing on FMCW radars.

■ **Passive reflection-based attacks:** Attacks based on passive reflections have been proposed to overcome the stringent synchronization requirements of active transmitter-based spoofing. Here, the attacker receives the incident signal, modifies the frequency and phase of the signal, amplifies it, and reflects it back to the victim's radar. The authors in [41], [42] use the backscatter technique for spoofing. One of the main limitations of backscatter is that the reflected signal is infested with strong harmonic frequencies that fall in the radar's band. These harmonics lead to unintentional multiple equispaced objects in radar rather than a single spoofed object which can be easily detected by the radar. In contrast, mmSpoof's attack is truly indistinguishable as it creates the frequency shift using mixers (not using square wave) completely eliminating any harmonics.

Nallabolu et al. [43] uses a reflect array, but they only spoof distance and do not solve for the coupling challenges associated with velocity spoofing. In [43], spoofing distance automatically creates a random velocity change (which can be easily detected). It is not trivial to spoof velocity by applying a synchronized phase shift to every chirp because it breaks the asynchronous principle. Moreover, their prototype is based on non-standard radar frequency (e.g. 5.8 GHz) and has not been demonstrated with automotive radars. In contrast, mmSpoof provides a novel technique to spoof distance and velocity independently without requiring synchronization and demonstrates the spoofing in a realistic mobile environment with vehicles on roads.

■ **Effectiveness of counter-measures:** mmSpoof is resilient to many interference mitigation strategies [28], [36], [44]–

[47]. For instance, BlueFMCW [28] proposes a counterattack by applying random frequency and phase hopping at the victim radar so that an active-transmitter-based attacker cannot control the spoofed distance or velocity at the victim. Our system is resilient to these attacks because it does not transmit new radar chirps but reflects the victim's radar signals after shifting frequency, preserving any modulation on the victim's radar signal. As a result, the attack will still successfully cause distance and velocity offsets.

■ **Other attacks on Automotive vehicles:** Automotive vehicles rely on many sensor data for autonomous functions such as self-driving, lane assist, etc. Several works investigate cyber-attacks or malware [48]–[50], physical attacks on complimentary sensors such as cameras and lidars [51]–[54] and attacks on underlying deep learning models running on sensor data [40], [51], [55], [56]. Unlike these works, mmSpoof's focus is on the physical-layer attack on the FMCW radar, a key ADAS component in both autonomous and semi-autonomous vehicles.

7. Limitation and countermeasures

Our proposed system, mmSpoof is resilient and undetectable to most of the existing defense measures because of its key strengths, such as parameter estimation, removal of needs for synchronization, and gain control. However, it does have a few limitations and countermeasures.

■ **Spoofing directions is not feasible:** Some applications, such as spoofing a car in another lane to the victim's car lane with a shorter distance, require spoofing direction and distance. With the given approach, mmSpoof cannot spoof directions. For instance, a car at 30 degrees angle with a 50m distance and 60 mph can be spoofed at an arbitrary, say 10m distance and 10 mph, but the angle would remain the same 30 degrees, i.e., the angle cannot be spoofed.

■ **Utilizing multiple radars and sensors:** Most autonomous vehicles are equipped with multiple sensors such as cameras, lidars, and multiple radars [57]. If the victim vehicle has multiple radars operating on different frequencies (i.e., 24 GHz and 77 GHz), the two radars would perceive all real objects at the same location. mmSpoof will be able to spoof 24 GHz radar, but 77 GHz radar won't be affected. The current literature has extensive work on spoofing lidar/camera. Adding a strong radar attack makes the entire autonomous system vulnerable. Autonomous vehicles rely on sensor fusion from all sensors; even spoofing only radar degrades the fusion. In adverse conditions with poor light visibility, radar sensors are vital, and spoofing in those conditions may lead to severe accidents.

■ **Ineffective against high-resolution imaging radars:** Recently, a new line of high-resolution radars has emerged that can create a high-resolution 3D image of a vehicle. If the victim uses such a radar in tandem with some advanced perception system [3], they can figure out that the ghost detections are not from an actual object. In this scenario, mmSpoof cannot create arbitrary and controllable spoofing, but it can still degrade the overall system's performance and therefore is a major concern for automotive vehicles.

■ **Randomly changing victim's radar parameters:** The spoofing is invalidated if the victim can randomly change the radar parameters (start frequency, chirp time, and slope) at a rate faster than the attacker's parameter estimation time. For instance, changing the slope for every chirp at the victim makes the estimated parameters at the attacker outdated and leads to erroneous spoofing. However, this will significantly increase the complexity of victims' radar processing.

8. Conclusion

In this work, we present the design of mmSpoof which for the first time implements a practical and truly wireless attack on a mmWave FMCW radar. mmSpoof is designed to work without any prior knowledge about the victim radar and does not require any kind of synchronization. This makes mmSpoof robust to several of the current defense measures proposed by recent literature, such as frequency hopping. Further, with extensive experimentation, we show mmSpoof can independently spoof distance and velocity, creating any desired pattern for a controlled attack on victim radars. Finally, we discuss defense measures that would increase the safety against spoofing attacks like mmSpoof. We believe that the design principles described in mmSpoof highlight the fundamental challenges in securing any passive reflection based ranging and localization system.

Applications: In section 5, we showed the flexibility that mmSpoof provides for spoofing a victim radar with arbitrary distance, velocity, and gain. The control that mmSpoof provides on distance and velocity opens up the avenue for a plethora of attacks and applications. For instance, consider a static scenario where a car is parked in a row with several other cars parked on the sides and a wall/car towards the back. The car can only move forward to come out of the parking space. Now, when an attacker spoofs the victim's radar creating a ghost vehicle in the front, it can result in the car being stuck in the parking lot. Another example of an attack could be a vehicle moving on a freeway can be attacked by a vehicle in front of it in the same lane. With the precise control mmSpoof provided, an attacker can create an exact scenario that would make it appear as if it applied sudden brakes. As a consequence of this, the victim radar will think that the vehicle has come too close to the front vehicle and could trigger an emergency braking system leading to fatal accidents. mmSpoof can also be used to avoid tailgating by another vehicle. Specifically, in the case of tailgating, the vehicle can use mmSpoof system to spoof a constant deceleration case, where the relative velocity constantly decreases, and the distance drops exponentially, as measured by the tailgating car's radar. This would cause the tailgating car to apply brakes and stop tailgating.

9. Acknowledgements

We are grateful to the anonymous reviewers and the shepherd for their valuable feedback, as well as to the WCSNG group for their input. The research for this project was partially supported by NSF grants 2211805 and 2144914.

References

[1] M. Steinhauer, H.-O. Ruoß, H. Irion, and W. Menzel, "Millimeter-wave-radar sensor based on a transceiver array for automotive applications," *IEEE transactions on microwave theory and techniques*, vol. 56, no. 2, pp. 261–269, 2008.

[2] J. Hasch, E. Topak, R. Schnabel, T. Zwick, R. Weigel, and C. Waldschmidt, "Millimeter-wave technology for automotive radar sensors in the 77 ghz frequency band," *IEEE transactions on microwave theory and techniques*, vol. 60, no. 3, pp. 845–860, 2012.

[3] K. Bansal, K. Rungta, S. Zhu, and D. Bharadia, "Pointillism: Accurate 3d bounding box estimation with multi-radars," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 2020, pp. 340–353.

[4] M. Ulrich, S. Braun, D. Köhler, D. Niederlöhner, F. Faion, C. Gläser, and H. Blume, "Improved orientation estimation and detection with hybrid object detection networks for automotive radar," *arXiv preprint arXiv:2205.02111*, 2022.

[5] S. Sun, A. P. Petropulu, and H. V. Poor, "Mimo radar for advanced driver-assistance systems and autonomous driving: Advantages and challenges," *IEEE Signal Processing Magazine*, vol. 37, no. 4, pp. 98–117, 2020.

[6] I. Yaqoob, L. U. Khan, S. A. Kazmi, M. Imran, N. Guizani, and C. S. Hong, "Autonomous driving cars in smart cities: Recent advances, requirements, and challenges," *IEEE Network*, vol. 34, no. 1, pp. 174–181, 2019.

[7] S. Kato, E. Takeuchi, Y. Ishiguro, Y. Ninomiya, K. Takeda, and T. Hamada, "An open approach to autonomous vehicles," *IEEE Micro*, vol. 35, no. 6, pp. 60–68, 2015.

[8] J. Park, S. Park, D.-H. Kim, and S.-O. Park, "Leakage mitigation in heterodyne fmcw radar for small drone detection with stationary point concentration technique," *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 3, pp. 1221–1232, 2019.

[9] D. Solomitckii, M. Gapeyenko, V. Semkin, S. Andreev, and Y. Koucheryavy, "Technologies for efficient amateur drone detection in 5g millimeter-wave cellular infrastructure," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 43–50, 2018.

[10] S. Ingle and M. Phute, "Tesla autopilot: semi autonomous driving, an uptick for future autonomy," *International Research Journal of Engineering and Technology*, vol. 3, no. 9, pp. 369–372, 2016.

[11] M. A. Khan, H. Menouar, A. Eldeeb, A. Abu-Dayya, and F. D. Salim, "On the detection of unauthorized drones-techniques and future perspectives: A review," *IEEE Sensors Journal*, 2022.

[12] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, "Detection, tracking, and interdiction for amateur drones," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 75–81, 2018.

[13] N. C. Currie and C. E. Brown, *Principles and applications of millimeter-wave radar*. Artech House Norwood, MA, 1987.

[14] E. Yeh, J. Choi, N. Prelcic, C. Bhat, and R. W. Heath Jr, "Security in automotive radar and vehicular networks," *submitted to Microwave Journal*, 2016.

[15] H.-R. Chen, "Fmcw radar jamming techniques and analysis," NAVAL POSTGRADUATE SCHOOL MONTEREY CA, Tech. Rep., 2013.

[16] R. Poisel, *Modern communications jamming principles and techniques*. Artech house, 2011.

[17] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *Def Con*, vol. 24, no. 8, p. 109, 2016.

[18] J. Dai, X. Hao, P. Li, Z. Li, and X. Yan, "Antijamming design and analysis of a novel pulse compression radar signal based on radar identity and chaotic encryption," *IEEE Access*, vol. 8, pp. 5873–5884, 2020.

[19] F. Jianli, "Wideband fm anti-jamming method of fmcw radar," in *2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP)*. IEEE, 2021, pp. 777–780.

[20] G. Wang, W. Hong, H. Zhang, and L. Cao, "Investigations on anti-jamming method for 77ghz automotive millimeter-wave radar," in *2016 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*. IEEE, 2016, pp. 1–3.

[21] F. Katsilieris, P. Braca, and S. Coraluppi, "Detection of malicious ais position spoofing by exploiting radar information," in *proceedings of the 16th international conference on information fusion*. IEEE, 2013, pp. 1196–1203.

[22] R. Chauhan, *A platform for false data injection in frequency modulated continuous wave radar*. Utah State University, 2014.

[23] R. Chauhan, R. M. Gerdes, and K. Heaslip, "Demonstration of a false-data injection attack against an fmcw radar," *Embedded Security in Cars (ESCAR)*, 2014.

[24] N. Miura, T. Machida, K. Matsuda, M. Nagata, S. Nashimoto, and D. Suzuki, "A low-cost replica-based distance-spoofing attack on mmwave fmcw radar," in *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop*, 2019, pp. 95–100.

[25] S. Nashimoto, D. Suzuki, N. Miura, T. Machida, K. Matsuda, and M. Nagata, "Low-cost distance-spoofing attack on fmcw radar and its feasibility study on countermeasure," *Journal of Cryptographic Engineering*, vol. 11, no. 3, pp. 289–298, 2021.

[26] R. Komissarov and A. Wool, "Spoofing attacks against vehicular fmcw radar," in *Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security*, 2021, pp. 91–97.

[27] M. Ordean and F. D. Garcia, "Millimeter-wave automotive radar spoofing," *arXiv preprint arXiv:2205.06567*, 2022.

[28] T. Moon, J. Park, and S. Kim, "Bluefmcw: Random frequency hopping radar for mitigation of interference and spoofing," *EURASIP Journal on Advances in Signal Processing*, vol. 2022, no. 1, pp. 1–17, 2022.

[29] S. M. Patole, M. Torlak, D. Wang, and M. Ali, "Automotive radars: A review of signal processing techniques," *IEEE Signal Processing Magazine*, vol. 34, no. 2, pp. 22–35, 2017.

[30] V. Dham, "Programming chirp parameters in ti radar devices," *Application Report SWRA553, Texas Instruments*, 2017.

[31] "Radarbook2," https://inras.at/en/radarbook2/.

[32] "Extreme waves," https://www.extreme-waves.com/.

[33] "Turtle bot," https://www.turtlebot.com/.

[34] "Programming chirp parameters in ti radar devices," https://www.ti.com/lit/an/swra553a/swra553a.pdf?ts=1669158070563.

[35] A. Ranganathan, B. Danev, A. Francillon, and S. Capkun, "Physical-layer attacks on chirp-based ranging systems," in *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, 2012, pp. 15–26.

[36] H.-L. Bloecher and J. Dickmann, "Automotive radar sensor interference–thread and probable countermeasures," in *2018 19th International Radar Symposium (IRS)*. IEEE, 2018, pp. 1–7.

[37] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "Pycra: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 1004–1015.

[38] R. G. Dutta, X. Guo, T. Zhang, K. Kwiat, C. Kamhoua, L. Njilla, and Y. Jin, "Estimation of safe sensor measurements of autonomous system under attack," in *Proceedings of the 54th Annual Design Automation Conference 2017*, 2017, pp. 1–6.

[39] P. Kapoor, A. Vora, and K.-D. Kang, "Detecting and mitigating spoofing attack against an automotive radar," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2018, pp. 1–6.

[40] Z. Sun, S. Balakrishnan, L. Su, A. Bhuyan, P. Wang, and C. Qiao, "Who is in control? practical physical layer attack and defense for mmwave-based sensing in autonomous vehicles," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3199–3214, 2021.

[41] D. Rodriguez, J. Wang, and C. Li, "Spoofing attacks to radar motion sensors with portable rf devices," in *2021 IEEE Radio and Wireless Symposium (RWS)*. IEEE, 2021, pp. 73–75.

[42] A. Lazaro, A. Porcel, M. Lazaro, R. Villarino, and D. Girbau, "Spoofing attacks on fmcw radars with low-cost backscatter tags," *Sensors*, vol. 22, no. 6, p. 2145, 2022.

[43] P. Nallabolu and C. Li, "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*, vol. 69, no. 11, pp. 5086–5098, 2021.

[44] S. Alland, W. Stark, M. Ali, and M. Hegde, "Interference in automotive radar systems: Characteristics, mitigation techniques, and current and future research," *IEEE Signal Processing Magazine*, vol. 36, no. 5, pp. 45–59, 2019.

[45] M. Wagner, F. Sulejmani, A. Melzer, P. Meissner, and M. Huemer, "Threshold-free interference cancellation method for automotive fmcw radar systems," in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2018, pp. 1–4.

[46] G. M. Brooker, "Mutual interference of millimeter-wave radar systems," *IEEE Transactions on Electromagnetic Compatibility*, vol. 49, no. 1, pp. 170–181, 2007.

[47] F. Uysal, "Phase-coded fmcw automotive radar: System design and interference mitigation," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 1, pp. 270–281, 2019.

[48] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity attacks in vehicular sensors," *IEEE Sensors Journal*, vol. 20, no. 22, pp. 13 752–13 767, 2020.

[49] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, "Attacks on self-driving cars and their countermeasures: A survey," *IEEE Access*, vol. 8, pp. 207 308–207 342, 2020.

[50] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The security of autonomous driving: Threats, defenses, and future directions," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 357–372, 2019.

[51] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, and D. Song, "Robust physical-world attacks on deep learning visual classification," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2018, pp. 1625–1634.

[52] Y. Zhu, C. Miao, T. Zheng, F. Hajiaghajani, L. Su, and C. Qiao, "Can we use arbitrary objects to attack lidar perception in autonomous driving?" in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 1945–1960.

[53] Y. Zhu, C. Miao, F. Hajiaghajani, M. Huai, L. Su, and C. Qiao, "Adversarial attacks against lidar semantic segmentation in autonomous driving," in *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, 2021, pp. 329–342.

[54] W. Wang, Y. Yao, X. Liu, X. Li, P. Hao, and T. Zhu, "I can see the light: Attacks on autonomous vehicles using invisible lights," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 1930–1944.

[55] C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, and P. Mittal, "Darts: Deceiving autonomous cars with toxic signs," *arXiv preprint arXiv:1802.06430*, 2018.

[56] A. Chernikova, A. Oprea, C. Nita-Rotaru, and B. Kim, "Are self-driving cars secure? evasion attacks against deep neural networks for steering angle prediction," in *2019 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2019, pp. 132–137.

[57] D. J. Yeong, G. Velasco-Hernandez, J. Barry, and J. Walsh, "Sensor and sensor fusion technology in autonomous vehicles: A review," *Sensors*, vol. 21, no. 6, p. 2140, 2021.

Appendix

We review radar signal processing to understand how radar estimates an object's distance and velocity. The radar transmits a signal $x(t)$ which gets reflected after hitting an object and the radar receives the reflected signal $y(t)$ as follows:

$$x(t) = e^{j2\pi(f_0 + \frac{k}{2}t)t}$$
$$y(t) = \alpha x(t - \tau(t))$$

where f_0 is the start frequency, k is chirp slope, α is a constant that captures the environmental attenuation and $\tau(t)$ is the round-trip time-of-flight in (1). The radar multiplies the received signal $y(t)$ with a conjugate copy of the transmitted signal to obtain the channel $h(t)$, that captures the time-of-flight information as follows:

$$\begin{aligned} h(t) &= y(t) \times \text{conj}(x(t)) \\ &= \alpha x(t - \tau(t)) \times \text{conj}(x(t)) \\ &= \alpha \exp(j2\pi \frac{k}{2} \tau(t)^2) \exp(-j2\pi k \tau(t) t) \exp(-j2\pi f_0 \tau(t)) \\ &\approx \alpha \exp(-j2\pi k \tau(t) t) \exp(-j2\pi f_0 \tau(t)) \end{aligned} \tag{15}$$

where the final equation for $h(t)$ is obtained by simplifying the expression above and making an approximation that the exponential term with $\tau(t)^2$ term is negligible compared to the other two exponential terms. This analysis leads to a simplified expression for the channel as:

$$\begin{aligned} h(t) &= \alpha \exp(-j2\pi(f_b t + \Phi(t))) \\ f_b &= k\tau(t) \quad \text{and} \quad \Phi(t) = f_0 \tau(t) \end{aligned} \tag{16}$$

where f_b is ***beat frequency*** and $\Phi(t)$ is a time-varying phase term as shown in Figure 2(b). Note how the beat frequency and the phase term are related to the time-of-flight $\tau(t)$. The radar measures these terms to estimate distance and velocity.