AttackDeceiver: Anti-spoofing Automotive Radar System using an Interleaving Chirp Waveform

Kaiyi Huang, Shengding Liu, Yanlong Qiu, Yanjiao Chen,
Senior Member, IEEE, and Jin Zhang, *Member, IEEE,*

***Abstract*—Millimeter-wave (mmWave) radars are integral to the safety-critical Advanced Driver Assistant System (ADAS) of modern vehicles, to perform robust and weather-resistant sensing of surrounding objects. However, these radars are vulnerable to adversarial attacks that mislead victim sensors producing incorrect environment observations and potentially causing attacker-selected or unsafe actions. Previous attempts at anti-spoofing have been designed to counter corresponding specific attacks. They cannot effectively handle sophisticated adaptive attacks. To meet the growing demand for driving safety, we present a novel anti-spoofing system called AttackDeceiver that enables resilient surrounding environment sensing under various spoofing attacks via an interleaving chirp waveform. AttackDeceiver leverages the comparison of estimates between the two channels, effectively detecting and mitigating false targets injected by malicious users. In addition, we deceive the attacker into generating unreasonable spoofing velocity for the injected targets. We show the effectiveness of AttackDeceiver using a compact setup with commercial-off-the-shelf (COTS) radars. The experimental results reveal an impressive false target recall (FTR) over 95%, along with an enhancement in real target to the false target plus noise ratio (RFNR) exceeding 10 dB.**

***Index Terms*—Autonomous Vehicles, Frequency-modulated Continuous Wave (FMCW) Radar, Millimeter-wave (mmWave) Radar, Radar Countermeasures, Spoofing Attack, Vehicle Security.**

I. Introduction

Autonomous vehicle (AV) [1] related research has become an extremely prominent topic in the last two decades, due to the vast improvement in sensor technologies such as ultrasonic sensors [2], cameras [3], LiDAR [4], and millimeter-wave (mmWave) radars [5]. These sensors collaborate to form the advanced driver assistance systems (ADAS), which sense the surrounding physical environment and make safety-critical decisions, such as emergency braking [6] and line change assist [7]. In particular, mmWave frequency modulated continuous wave (FMCW) radars serve as a core component of ADAS, as they provide precise and robust object detection even under inclement weather such as fog and low light, where other light-based sensors such as cameras and Lidars would fail [8]–[10]. They are also used for pedestrian and blind spot detection [11], adaptive cruise control [12], multi-lane traffic monitoring [13], and intersection management [14].

Given the broad and crucial application scenarios, researchers have extensively explored various attacks on automotive radars. In these attacks, adversarial sensors attempt to manipulate the received signals of the victim radars to mount attacks. Generally, these attacks can be organized into two main categories: spoofing and jamming [15]. In jamming attacks, the attackers intentionally emit high-energy signals within the bandwidth of the victim radars, lowering their signal-to-noise ratio (SNR), thereby making surrounding objects undetectable [16], [17]. Fortunately, jamming attacks can be easily detected, as they cause the radars to malfunction. In contrast, spoofing attacks are difficult to detect and mitigate. Spoofing attacks inject false targets that mimic the physical patterns of real objects, forcing the victim radars to detect objects not existing [18]–[20]. Pseudo-obstacles can cause the ADAS to perform dangerous driving behaviors such as emergency braking, which can lead to accidents endangering the lives of passengers.

In recent years, research in spoofing attacks has made tremendous progress. Most prior arts have achieved false target injection through time delays [18], [21]–[24] or frequency shifts [25], [26]. By estimating the waveform of the victim radars, the attackers can realize customized spoofing, where the false targets have a reasonable attacker-selected range and velocity [18], [24], [26]. However, the existing spoofing approaches have certain limitations. They assume that all chirps in a frame have the same shape and apply the same time delay or frequency shift to the entire chirp sequence, which provides an opportunity to resist this coarse-grained attack. Nashimoto et al. [25] propose an alternating slope modulation scheme to identify false targets by detecting varying distance measurements. However, this approach cannot assist when the attacker applies fine-grained frequency shifts to each chirp. Based on the random start frequency technique discussed in [18], [23], [24], existing coarse-grained spoofing attacks can be easily extended to fine-grained adaptive attacks. Existing countermeasures [23]–[25] are ineffective against such attacks as they are aimed at counteracting specific corresponding attacks, leaving the sophisticated adaptive spoofing attacks

Kaiyi Huang is with the Department of Computer Science and Engineering, Southern University of Science and Technology, China (email: huangky2019@mail.sustech.edu.cn).

Shengding Liu is with the Department of Computer Science and Engineering, Southern University of Science and Technology, China (email: 12110813@mail.sustech.edu.cn).

Yanlong Qiu is with the Department of Computer Science and Engineering, Southern University of Science and Technology, China, and also with the Department of Computer and Information Science, Temple University, U.S. (email: qiuyl@mail.sustech.edu.cn).

Yanjiao Chen is with the College of Electrical Engineering, Zhejiang University, China (email: chenyanjiao@zju.edu.cn).

Jin Zhang is with Shenzhen Key Laboratory of Safety and Security for Next Generation of Industrial Internet, Research Institute of Trustworthy Autonomous Systems, Department of Computer Science and Engineering, Southern University of Science and Technology, China (email: zhangj4@sustech.edu.cn).

beyond their consideration.

The core challenge is to detect spoofing attacks using received signals that contain reflection and spoofing components in an adaptive fine-grained attack setting. The signals reflected by environmental objects are time-delayed versions of the transmitted signals with a certain Doppler shift. Thus, with knowledge of the transmitted signal waveform, malicious users can introduce false targets that follow similar patterns to real objects, by transmitting carefully designed spoofing signals. As shown in Fig. 1, the COTS radars will receive both the reflection signal (blue arrow) and spoofing signal (red arrow) to sense the surrounding environment. Without any waveform design, they can not distinguish the real targets from the false ones, since all the targets appear as bright spots at a certain distance and speed in the range-Doppler (RD) profiles.

Can we design an anti-spoofing system to defend the chirp-level adaptive attacks? Our key insight is that we can distinguish between spoofing signals from malicious sensors and reflected signals bounced by surrounding objects, leveraging cross-validating the ambient sensing results of two independent channels. Building upon this insight, we present AttackDeceiver, a robust and versatile anti-spoofing automotive radar system using an interleaving chirp waveform. We apply non-identical phase modulation to the chirp sequences of these two channels, so that the real targets remain in their proper position after the phase calibration process, while the false targets are differently shifted in the Doppler domain. The phase modulation process can be seen as a form of signal encryption. The automotive radars are well aware of the initial phase offsets of each chirp, thus they can compensate to bring the real targets back to where they should be. In contrast, the false targets are forced to undergo distinct defender-selected Doppler shifts, as the malicious sensors have no knowledge of the key. The inconsistency of the results between the two channels enables AttackDeceiver to detect and mitigate the injected false targets, thus making the anti-spoofing system robust to state-of-the-art (SOTA) spoofing attacks.

Moreover, the phase modulation provides additional benefits. Firstly, it can mislead malicious sensors to perform inaccurate relative velocity estimation, which may lead to irrational target injection. With downstream velocity reasonableness analysis, we can detect and mitigate false targets, thus expanding the scope of defensible attacks. Secondly, it makes the proposed countermeasures tougher to be detected and defeated. The initial phase shift of each chirp is much more minute compared to the frequency slope, making it notoriously difficult to be accurately estimated. Even assuming malicious users could achieve precise estimation with expensive circuitry, it is almost mission impossible for them to know the proportionality between the motion-induced phase and the artificial-added phase. In addition, we apply frequency slope alternation to extend the application range further. With these approaches, we present the interleaving chirp waveform to distinguish false and real targets, making our system robust and versatile. We summarize our contributions as follows:

- We propose an anti-spoofing automotive radar system called AttackDecive to counter SOTA spoofing attacks. By employing an interleaving chirp waveform, COTS radars would able to detect and mitigate false targets injected by malicious sensors through the comparison of results from multiple channels.
- We design a versatile chirp waveform to differentiate between false and real targets in certain dimensions. The phase modulation and slope alternation are used to counter coarse-grained active generation-based and passive reflection-based spoofing. Moreover, a novel intersection algorithm is presented to fuse multi-channel results with varying specifications and strengths.
- We implement a prototype of AttackDeciver using COTS mmWave radar. We conduct various indoor experiments for feasibility verification and outdoor experiments for usability and robustness evaluation, using commercial 77 GHz radars mounted on vehicles. The experimental results show that AttackDeciver can achieve impressive false target recall over 95%, along with an enhancement in real target to the false target plus noise ratio exceeding 10 dB under various attack scenarios.

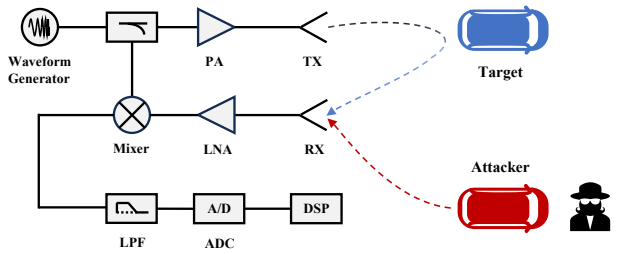


Fig. 1. Block diagram of COTS mmWave radars.

Roadmap. The rest of this paper is organized as follows. Background and related work are presented in Section II. We demonstrate the threat model in Section III. The details of the proposed anti-spoofing system are given in Section IV. In Section V we discuss the usability and robustness of AttackDeceiver. Section VI concludes the paper.

II. Background and Related Work

In this section, we first review the workflow of FMCW radar and present the range and velocity estimation. We then provide a comprehensive survey of the spoofing attacks and countermeasures.

A. Principle of FMCW Radar

Millimeter-wave radars leverage FMCW to sense environments and capture information about surrounding objects. With a fine wavelength, they can achieve high-resolution range and velocity estimation. The transmitted signal consists of a sequence of M chirps. Each chirp sweeps a bandwidth B over a period T_c in the radio-frequency (RF) domain. The m^{th} chirp of the transmitted signal $x(t)$ can be represented as:

$$x(t) = e^{-j(2\pi f_c t_s + \pi \kappa t_s^2 + \phi_0)}, \tag{1}$$

where $t_s = t - mT_c$ is the within-chirp time, f_c is the start frequency, κ is the frequency slope, and ϕ_0 is the initial phase.

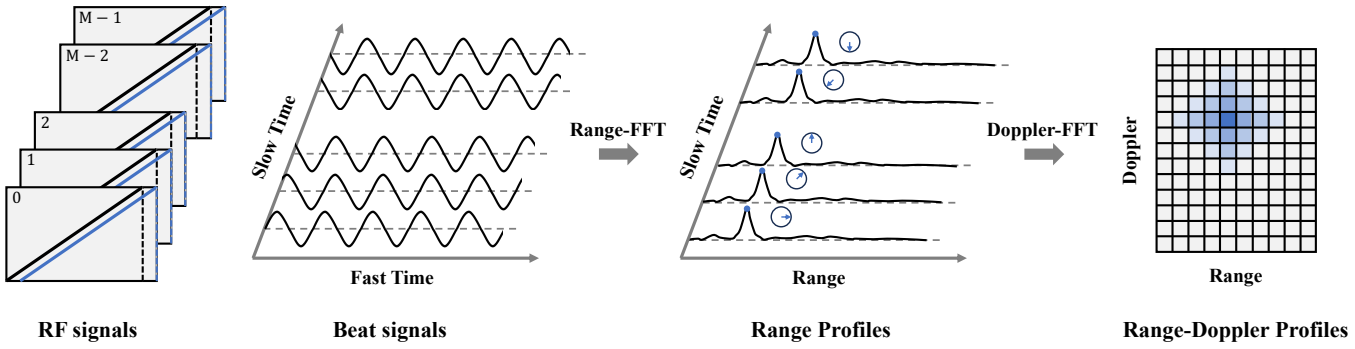


Fig. 2. Signal processing workflow of mmWave FMCW radars.

The chirp sequence propagates through the environment and is then reflected by ambient objects, generating echoes that can be viewed as scaled and delayed versions of the transmitted signal. Eventually, the echoes produced by these objects are superimposed and received by the receiving antennas. Without loss of generality, we assume there are K objects in the environment. Then, the m^{th} segment of the received signal $y(t)$ containing K detection targets can be expressed as:

$$y(t) = \sum_{k=1}^{K} A_k x(t_s - \tau_k), \tag{2}$$

where A_k and τ_k represent the scaling factor and time delay of the k^{th} target.

Afterward, we apply a mixer to combine the transmitted and received signals with the conjugate product. The output signal is then downconverted by a low-pass filter (LPF), to produce the beat signal or the intermediate frequency (IF) signal. The m^{th} segment of the beat signal $h(t)$ can be denoted as:

$$h(t) = x(t) \cdot \overline{y(t)} = \sum_{k=1}^{K} A_k e^{-j(2\pi f_k t_s + \phi_k)}, \tag{3}$$

where f_k and ϕ_k are the beat frequency and phase of the k^{th} target. These beat frequencies and phases embed the range and velocity information of the targets. Utilizing digital signal processing methods, such as fast Fourier transform (FFT), we can obtain the RD profiles and extract the range and velocity information, thus realizing contactless environment sensing.

Range Estimation: The FMCW radars estimate the range of targets by analyzing the received signal in each chirp duration. Assume that only the k^{th} target is in the scene. As shown in Fig. 2, there is a time delay τ_k between the received signal (blue line) and the transmitted signal (black line), resulting in a certain frequency difference Δf_k at any given moment. With the time delay τ_k as an intermediate variable, we can establish the relationship between the range d_k and the frequency difference Δf_k:

$$\tau_k = \frac{2d_k}{c} = \frac{\Delta f_k}{\kappa}. \tag{4}$$

Moreover, the frequency difference Δf_k is exactly the frequency of the beat signal f_k. By applying the range-FFT to the beat signal, we can find the peak corresponding to the k^{th} target in the frequency spectrum, and derive the range by:

$$d_k = \frac{c}{2\kappa} f_k. \tag{5}$$

Velocity Estimation: The FMCW radars estimate the velocity of targets by monitoring the phase change over multiple chirps in a frame. The duration of the chirps is so tight that the object moves below the range resolution. This results in M peaks with the same range in the range profiles, as displayed in Fig. 2. However, each peak has a different phase $\phi_{k,m}$ due to the motion. We assume that all chirps in the frame are equally spaced, and the velocity of the k^{th} target does not change within the frame duration, making the phase difference between neighboring peaks constant. Therefore, we can perform another FFT operation, called Doppler FFT, to obtain the constant phase difference and compute the velocity:

$$v_k = \frac{\Delta d_k}{\Delta T} = \frac{\lambda \omega_k}{4\pi T_c}, \tag{6}$$

where λ is the wavelength, and $\omega_k = \phi_{k,m+1} - \phi_{k,m}$ is the phase difference of the k^{th} target.

In summary, by employing 2D-FFT on the beat signals, we can construct the RD profiles to reveal the range and velocity information of the targets. The concrete values of range and velocity can be estimated by locating the bins with significant intensity in the RD profiles.

B. Radar Spoofing Attacks

Millimeter-wave spoofing attacks have been intensively conducted. Recent works have attempted to launch spoofing attacks by actively generating spoofing signals or passively receiving and modifying radar transmission signals. A comparison among representatives of the generation-based and reflection-based spoofing attack is listed in Table I.

Generation-based Spoofing: In these attacks, the attackers would emit self-generated spoofing signals at the proper time, causing the victim to detect the false targets [18], [22]–[24], [28]. To realize this spoofing attack, the attackers need to satisfy two conditions. Firstly, they need to know the transmitted signal waveform of the victims, to ensure that their injected false targets are similar to the real ones. Secondly,

TABLE I
COMPARISON OF SOTA MMWAVE SPOOFING ATTACK WORKS

Work	Type	Techniques	Spoofing Capability	Attacking Device
S. Nashimoto et al. [23]	Generation-based	Time delay	Range	24GHz FMCW radar
R. Komissarov et al. [18]	Generation-based	Time delay	Range, velocity	Software-defined radio
Z. Sun et al. [24]	Generation-based	Time delay	Range, velocity, angle	Software-defined radio
P. Nallabolu et al. [25]	Reflection-based	Frequency shift	Range	SSB RF mixer
R. Reddy Vennam et al. [26]	Reflection-based	Frequency shift	Range, velocity	Phased array based USRP
X. Chen et al. [27]	Reflection-based	Meta-surface	Range, velocity, angle	Meta-material tags

they need to synchronize with the victims, to ensure that the spoofing signals are transmitted at the expected time. Any minor error in synchronization will expose false targets due to the invalid range or velocity, and result in spoofing failures. Nashimoto et al. [23] achieve precise time synchronization through a wired connection and launch range spoofing attacks in the indoor environment. Komissarov et al. [18] and Sun et al. [24] take a step further. They use expensive specialized circuitry, the software-defined radio (SDR), to achieve wireless nanosecond-level synchronization, unleashing the unrealistic wired setup. Besides, they employ additional designs such as phase compensation and multiple attackers, enabling spoofing in the velocity and angle dimensions.

Reflection-based Spoofing: In these attacks, the attackers manipulate the received signals from the victim radars to achieve spoofing. Since the manipulations are performed on the received signal, the attackers can bypass the waveform estimation and time synchronization. Due to these advantages, many studies on reflective-based spoofing are flourishing. Some existing works use mixers to apply a frequency shift on the received signals and realize spoofing attacks [25], [26]. Nallabolu et al. [25] achieve range spoofing but do not consider the velocity, which makes false targets easy to detect due to the random velocities. Vennam et al. [26] decouple the range and velocity spoofing and demonstrate the performance in a realistic moving environment with vehicles on the road. Some other approaches use meta-surface to realize spoofing attacks [27], [29], [30]. However, this type of attack would be easily detected. Because, in this case, the spoofing signal is filled with strong harmonic frequencies, leading to the appearance of suspected multiple equidistant false targets [26].

Spoofing Countermeasures: To ensure autonomous driving safety, researchers have turned their attention to the spoofing countermeasures. To counter generation-based spoofing attacks, Nashimoto et al. [23] present a half-chirp modulation scheme. However, this countermeasure can only be applied to radars transmitting triangular waveforms, but cannot be adapted to contemporary COTS automotive radars employing a sawtooth waveform, so-called fast chirp. To allow our proposed anti-spoofing system to be widely deployed on existing COTS radars, we will base our design on the fast chirp waveform. In addition, Sun et al. [24] present a randomized phase modulation approach to disable meaningful false target injection by smearing the originally concentrated energy peaks in the Doppler domain uniformly at the malicious user end. Yet this approach simultaneously affects the victim radars. As a result, when multiple radars employing random phase modulation operate in the same scenario, they would interfere with each other and cause the velocity estimation to malfunction. Therefore, we will adopt a gentle approach to achieve spoofing resistance while avoiding mutual interference. In addition, we can also introduce designs in the transmission waveform that are difficult for attackers to be aware of, to make the false targets hard to mimic real ones. For reflection-based spoofing attacks, Nashimoto et al. [25] propose a slope alternation scheme to detect false targets with mismatch measurements. However, this method would fail when the attacker applies fine-grained frequency shifts to each chirp. Thus, we attempt to distort the false targets by deceiving the attackers, and then classify the targets by judging the feasibility of range and velocity values.

III. THREAT MODEL

Attack Scenario: In this paper, we focus on a scenario where AVs are equipped with mmWave radars as the main information source for object detection. Specifically, we assume that the victim AVs are running on the road and malicious users are in the front or on the roadside conducting generation-based or reflection-based spoofing attacks. The objective of the attack is to continuously generate false targets with specific range and velocity to force the ADAS to make dangerous driving maneuvers such as hard braking and emergency lane changing.

Attacker Knowledge: We assume that attackers possess knowledge of the hardware parameters of the victim mmWave radars, including the available RF band and maximum sampling rate. Furthermore, they have comprehensive information about the waveform configuration, such as frequency slope, start frequency, and chirp cycle time. The assumption is reasonable as mmWave sensors must follow standards specified by spectrum licenses, and the information can be accessed through open-source documentation, patent disclosure, and reverse engineering. In addition, methods for estimating radar waveform have been well researched [26], [31], which offer ways of realizing accurate waveform estimation.

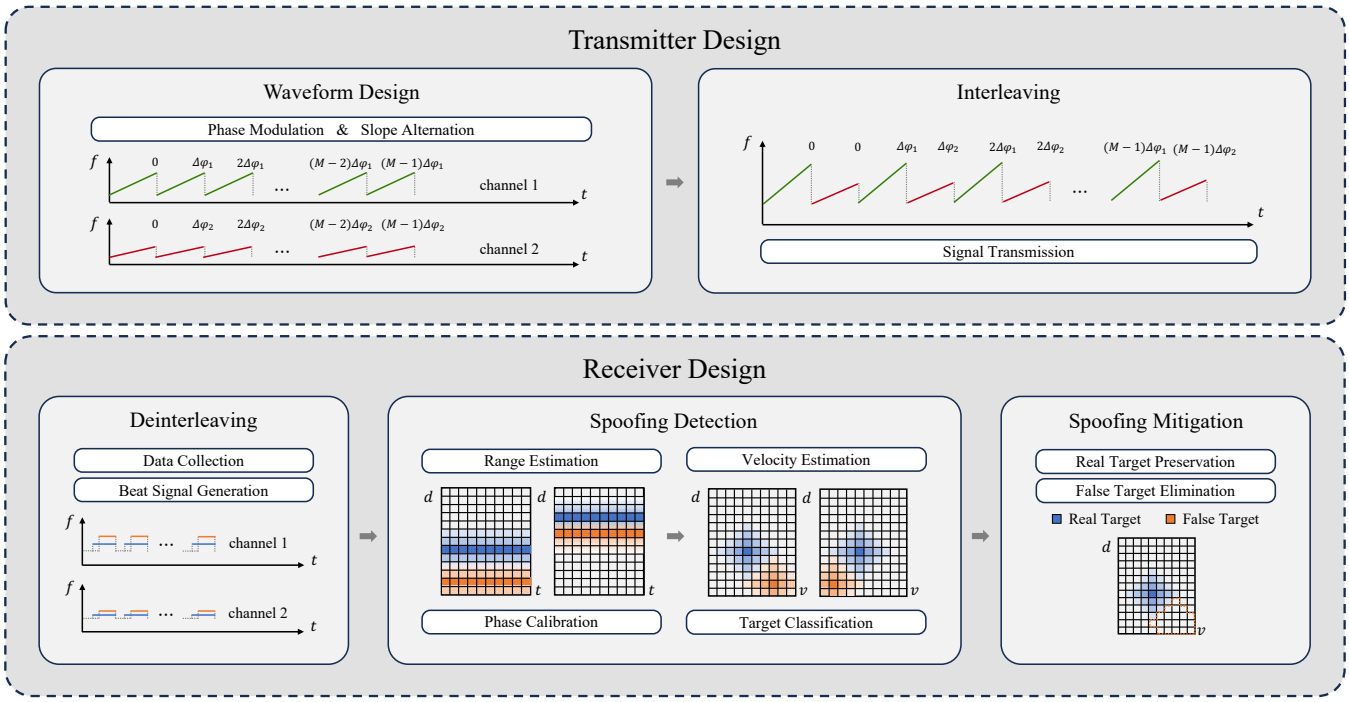


Fig. 3. System architecture of AttackDeceiver.

Attacker Capability: In our setup, the attackers can not directly manipulate the collected data on the victim AVs. However, we assume that they can achieve or bypass high-precision time synchronization. Thus, they can generate and transmit spoofing signals employing time delay or frequency shift, to launch generation-based or reflection-based attacks and cause the victim radars to detect false targets.

IV. AttackDeceiver: Detailed Design

A. Overview

Existing spoofing countermeasures are inadequate in addressing fine-grained adaptive attacks. To safeguard the driving safety of AVs, we propose AttackDeceiver, an anti-spoofing system utilizing an interleaving chirp waveform, to counteract emerging generation-based and reflection-based spoofing attacks. The architecture of AttackDeceiver is shown in Fig. 3. In detail, AttackDeceiver employs two independent channels to sense the environment and handle spoofing attacks. Each channel utilizes distinct frequency slopes and initial phase offsets, causing false targets to produce inconsistent measurements in the range and Doppler domains of the RD profiles. By detecting targets with varying or unreasonable measurements, we can identify all false targets and accurately classify all detected targets. Subsequently, we use range interpolation to standardize the RD profiles from different channels and apply a multi-channel fusion algorithm to mitigate false targets, thereby obtaining the expected RD profiles that reveal only real targets. By shielding RD profiles from spoofing attacks, AttackDeceiver effectively realizes accurate and robust sensing of the environment.

B. Waveform Design

Conventional automotive radars are mostly set up with a fixed frequency slope and initial phase offset for each chirp. With such a waveform design, malicious users can easily realize spoofing attacks by transmitting spoofing signals at the right time, causing the victim radars to mistake false targets for real surrounding objects. To make false targets not share similar patterns with the real ones, we use two independent channels to sense the surroundings. We denote the frequency slopes of the two channels as κ_1, κ_2. Without loss of generality, we set κ_1 to a steeper slope, κ_2 to a flatter slope, and let each channel contain M chirps for each frame. Then, the instantaneous frequency of the m^{th} chirp for channels 1 and 2 can be expressed as:

$$\begin{aligned} f_1(t) &= \kappa_1 t_s + f_c, \\ f_2(t) &= \kappa_2 t_s + f_c, \end{aligned} \tag{7}$$

where $m = 0, 1, \ldots, M-1$, $t_s = t - mT_c$ is the within-chirp time, and f_c is the start frequency.

In addition to the coarse-grained adjustment of adopting different slopes, we also elaborate on the phase offsets at a fine-grained level. Each chirp from the channels is added a phase offset corresponding to its index m. With the design of slope alternation and phase modulation, we can represent the m^{th} chirp signal $x_1(t), x_2(t)$ for channels 1 and 2 as:

$$\begin{aligned} x_1(t) &= e^{-j(2\pi\Phi_1(t) + m\Delta\phi_1)}, \\ x_2(t) &= e^{-j(2\pi\Phi_2(t) + m\Delta\phi_2)}, \\ \Phi_1(t) &= \textstyle\int f_1(t)\, dt = f_c t_s + \frac{1}{2}\kappa_1 t_s^2, \\ \Phi_2(t) &= \textstyle\int f_2(t)\, dt = f_c t_s + \frac{1}{2}\kappa_2 t_s^2, \end{aligned} \tag{8}$$

where $\Phi_1(t), \Phi_2(t)$ are the phase portions due to instantaneous frequency accumulation, and $m\Delta\phi_1, m\Delta\phi_2$ are the artificially added phase offsets.

C. Interleaving

Automotive radar systems frequently employ the multiple-input multiple-output (MIMO) technique to achieve multi-channel environmental sensing. However, this approach is incompatible with certain low-cost commercial radars, as it escalates hardware expenses and complicates system integration. To circumvent the limitations associated with the MIMO technique, we utilize time division multiplexing (TDM) to interleave chirp sequences from two channels, thereby reducing the antenna requirement to a single pair of transmitting and receiving antennas. We formulate the transmission waveform $x(t)$ containing a total of $2M$ chirps as:

$$x(t)=\begin{cases} e^{-j(2\pi\Phi_1(t)+\frac{m}{2}\Delta\phi_1)}, & m=0,2,\ldots,2M-2, \\ e^{-j(2\pi\Phi_2(t)+\frac{m-1}{2}\Delta\phi_2)}, & m=1,3,\ldots,2M-1. \end{cases} \tag{9}$$

D. Deinterleaving

By analyzing the received signal $y(t)$, automotive radars could provide their environment sensing results. Without loss of generality, we assume there are K real ambient targets in the environment, and the attacker attempts to inject S false targets. Consequently, the received signal $y(t)$ can be decomposed into two components: the reflected signal $y_r(t)$ and the spoofing signal $y_f(t)$. The reflected signal $y_r(t)$ consists of K scaled and delayed versions of the transmitted signal, while the spoofing signal $y_f(t)$ comprises S imitation signals. With $\Delta\phi_1'$, $\Delta\phi_2'$ representing the phase offset units of the attacker, the received signal $y(t)$ and its components $y_r(t)$, $y_f(t)$ can be expressed as follows:

$$\begin{aligned} y(t) &= y_r(t) + y_f(t), \\ y_r(t) &= \begin{cases} \sum_{k=1}^{K} A_k e^{-j(2\pi\Phi_1(t-\tau_k)+\frac{m}{2}\Delta\phi_1)}, & m=0,2,\ldots,2M-2, \\ \sum_{k=1}^{K} A_k e^{-j(2\pi\Phi_2(t-\tau_k)+\frac{m-1}{2}\Delta\phi_2)}, & m=1,3,\ldots,2M-1, \end{cases} \\ y_f(t) &= \begin{cases} \sum_{s=1}^{S} A_s e^{-j(2\pi\Phi_1(t-\tau_s^1)+\frac{m}{2}\Delta\phi_1')}, & m=0,2,\ldots,2M-2, \\ \sum_{s=1}^{S} A_s e^{-j(2\pi\Phi_2(t-\tau_s^2)+\frac{m-1}{2}\Delta\phi_2')}, & m=1,3,\ldots,2M-1, \end{cases} \end{aligned} \tag{10}$$

where A_k, A_s are the scaling factors of the real and false targets, τ_k is the round trip time delay and τ_s^c, $c=1,2$ is the attacker-introduced delay of the c^{th} channel.

After collecting the received signal, the mixer would then apply the dechirp operation to obtain the conjugate element-wise product of the received signal $y(t)$ and the reference signal $s(t)$, thereby generating the beat signal $h(t)$:

$$\begin{aligned} h(t) &= s(t)\cdot\overline{y(t)}, \\ s(t) &= \begin{cases} e^{-j2\pi\Phi_1(t)}, & m=0,2,\ldots,2M-2, \\ e^{-j2\pi\Phi_2(t)}, & m=1,3,\ldots,2M-1, \end{cases} \end{aligned} \tag{11}$$

where $s(t)$ is the reference signal devoid of artificially introduced phase offset. Subsequently, we would perform de-interleaving to split the beat signal $h(t)$ into two channels. The m^{th} beat signal segments of channels, containing components corresponding to both real and false targets can be denoted as:

$$\begin{aligned} h_1(t) &= \underbrace{\sum_{k=1}^{K} A_k e^{-j(2\pi f_k^1 t_s+\phi_{k,m}^1-m\Delta\phi_1)}}_{real\ targets} + \underbrace{\sum_{s=1}^{S} A_s e^{-j(2\pi f_s^1 t_s+\phi_{s,m}^1-m\Delta\phi_1')}}_{false\ targets}, \\ h_2(t) &= \underbrace{\sum_{k=1}^{K} A_k e^{-j(2\pi f_k^2 t_s+\phi_{k,m}^2-m\Delta\phi_2)}}_{real\ targets} + \underbrace{\sum_{s=1}^{S} A_s e^{-j(2\pi f_s^2 t_s+\phi_{s,m}^2-m\Delta\phi_2')}}_{false\ targets}, \end{aligned} \tag{12}$$

where $\phi_{k,m}^c$, $\phi_{s,m}^c$ are the intrinsic phase offsets, and $f_k^c = \kappa_c\tau_k$, $f_s^c = \kappa_c\tau_s^c$ are the beat frequencies of the targets.

E. Spoofing Detection

By analyzing the beat signals from channels 1 and 2, we could obtain two sets of estimates for the range and velocity of the detected targets. We can identify false targets through inconsistent estimates when the attacker applies uniform processes to the entire frame. Moreover, in the case of fine-grained adaptive spoofing attacks, we can achieve spoofing detection by inducing the attacker to select unreasonable velocity values for the false targets.

1) Range Estimation: We first perform the range-FFT on the beat signals from channels 1 and 2, to obtain the beat frequencies of the targets. By analogy to Eq. 5, we can derive the range estimates for both real and false targets:

$$\begin{aligned} \hat{d}_k^1 &= \tfrac{c}{2\kappa_1} f_k^1 = c\tau_k, \\ \hat{d}_k^2 &= \tfrac{c}{2\kappa_2} f_k^1 = c\tau_k, \\ \hat{d}_s^1 &= \tfrac{c}{2\kappa_1} f_s^1 = \tfrac{c}{2\kappa_1}(f_a^1 + \Delta f_s^1), \\ \hat{d}_s^2 &= \tfrac{c}{2\kappa_2} f_s^2 = \tfrac{c}{2\kappa_2}(f_a^2 + \Delta f_s^2). \end{aligned} \tag{13}$$

Since the beat frequencies of real targets are proportional to the frequency slopes, the range estimates in channels are equal to $c\tau_k$. In contrast, the beat frequencies of false targets include the component due to the victim-attacker distance f_a^c and the offset introduced by the attacker Δf_s^c. By adjusting the frequency offsets, the attacker can shift the false targets from their actual range to any desired spoofing range.

2) Phase Calibration: After completing the range estimation, the next step is to compute the phase differences and deduce the velocity. By subtracting the phases of neighboring

chirps, we can obtain the phase differences for real and false targets in channels 1 and 2:

$$\begin{aligned}\omega_k^1 &= (\phi_{k,m+1}^1 - \phi_{k,m}^1) - \Delta\phi_1,\\ \omega_k^2 &= (\phi_{k,m+1}^2 - \phi_{k,m}^2) - \Delta\phi_2,\\ \omega_s^1 &= (\phi_{s,m+1}^1 - \phi_{s,m}^1) - \Delta\phi_1',\\ \omega_s^2 &= (\phi_{s,m+1}^2 - \phi_{s,m}^2) - \Delta\phi_2'.\end{aligned} \tag{14}$$

Since we introduce additional phase offsets to the waveform, we would need to compensate for the phase differences, according to the offset units of the channels $\Delta\phi_1$, $\Delta\phi_2$. The compensated phase differences can be then expressed as:

$$\begin{aligned}\omega_k^{1\prime} &= \omega_k^1 + \Delta\phi_1 = \tfrac{4\pi T_c v_k}{\lambda},\\ \omega_k^{2\prime} &= \omega_k^2 + \Delta\phi_2 = \tfrac{4\pi T_c v_k}{\lambda},\\ \omega_s^{1\prime} &= \omega_s^1 + \Delta\phi_1 = \tfrac{4\pi T_c v_{a,s}}{\lambda} + (\Delta\phi_1 - \Delta\phi_1'),\\ \omega_s^{2\prime} &= \omega_s^2 + \Delta\phi_2 = \tfrac{4\pi T_c v_{a,s}}{\lambda} + (\Delta\phi_2 - \Delta\phi_2').\end{aligned} \tag{15}$$

where v_k is the relative velocity between the victim and the k^{th} target, and v_a is the attacker-victim relative velocity.

3) Velocity Estimation: As illustrated in Eq. 6, the velocity of targets depends on the phase difference. With the compensated phase differences, we can provide accurate and consistent velocity estimates for the real targets:

$$\begin{aligned}\hat{v}_k^1 &= \tfrac{\lambda}{4\pi T_c}\omega_k^{1\prime} = v_k,\\ \hat{v}_k^2 &= \tfrac{\lambda}{4\pi T_c}\omega_k^{2\prime} = v_k.\end{aligned} \tag{16}$$

In contrast, besides the component embedding the spoofing velocity, the velocity estimates for false targets are compelled to include the component resulting from phase compensation:

$$\begin{aligned}\hat{v}_s^c &= \tfrac{\lambda}{4\pi T_c}\omega_s^{c\prime} = v_s^c + \tfrac{\lambda\Delta\phi_c}{4\pi T_c},\\ v_s^c &= \tfrac{\lambda}{4\pi T_c}\omega_s^c \;= v_a + \Delta v_s^c = v_a - \tfrac{\lambda\Delta\phi_c'}{4\pi T_c}.\end{aligned} \tag{17}$$

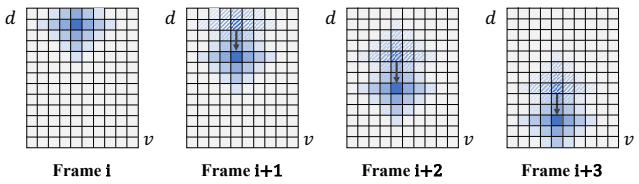
By adjusting the phase offset $\Delta\phi_c'$, the attacker could control the velocity offset Δv_s^c attached to the relative velocity v_a, thereby manipulating the spoofing velocity v_s^c and the estimate on the victim side $\hat{v}_s^c$.

4) Target Classification: To begin with, we would describe the method of utilizing range inconsistencies to detect false targets induced by reflection-based spoofing attacks. In this case, the attacker typically employs a uniform frequency shift Δf to spoof the victim. Consequently, the frequency offsets Δf_1, Δf_2 are both equal to the same value Δf. As a result, the range estimates for these false targets $\hat{d}_s^1$, $\hat{d}_s^2$ would have distinct values:

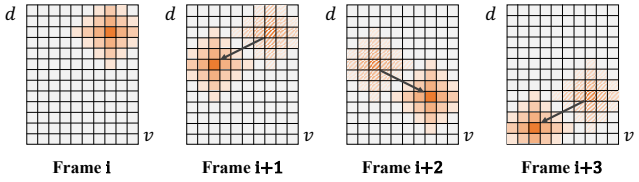
$$\begin{aligned}\hat{d}_s^1 &= \tfrac{c}{2\kappa_1}(f_a^1 + \Delta f_1) = d_a + \tfrac{c}{2\kappa_1}\Delta f,\\ \hat{d}_s^2 &= \tfrac{c}{2\kappa_2}(f_a^2 + \Delta f_2) = d_a + \tfrac{c}{2\kappa_2}\Delta f,\end{aligned} \tag{18}$$

where d_a is the distance between the victim and the attacker.

However, when the attacker attempts to launch generation-based spoofing attacks, the frequency offsets Δf_1, Δf_2 vary proportionally with the attacker-introduced time delay, resulting in the difference in distance estimates disappears. Thus, we utilize the incoherence in velocity to identify false targets.



(a) The variation pattern of the real target.



(b) The variation pattern of the false target.

Fig. 4. Inter-frame phase offset mutation.

From Eq. 17 we can derive the following:

$$\hat{v}_s^1 - \hat{v}_s^2 = \tfrac{\lambda}{4\pi T_c}[(\Delta\phi_1 - \Delta\phi_2) - (\Delta\phi_1' - \Delta\phi_2')], \tag{19}$$

which indicates that the velocity estimates are consistent only when the difference in phase offsets imposed by the attacker match those of the victim. Given that the attacker has minimal knowledge of the victim's phase shifts, it is challenging for him to equalize the velocity estimates.

Furthermore, once the attacker adheres to this condition, his choice of phase offsets would be restricted, leading to the spoofing velocity of false targets failing to meet expectations. We denote the desired spoofing velocity in both channels as $\bar{v}_s$. Then, the velocity offset Δv_s^c can be determined as:

$$\Delta v_s^c = \bar{v}_s - \hat{v}_a^c. \tag{20}$$

where $\hat{v}_a^c$ is the relative velocity estimate on the attacker side. Since we apply additional phase offsets, the attacker would be deceived and obtain biased relative velocity estimate $\hat{v}_a^c$:

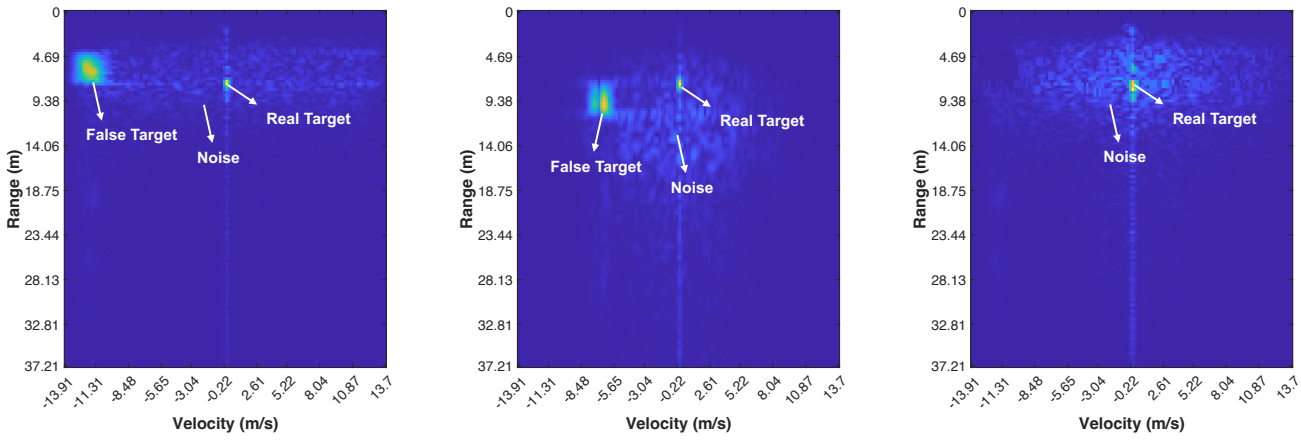
$$\hat{v}_a^c = \tfrac{\lambda}{4\pi T_c}\omega_a^c = v_a - \tfrac{\lambda\Delta\phi_c}{4\pi T_c}, \tag{21}$$

where ω_a^c is the phase difference on the attacker side. As a result, the velocity estimates on the victim side deviate differently from the expected spoofing value $\bar{v}_s$:

$$\hat{v}_s^c = v_a + \Delta v_s^c + \tfrac{\lambda\Delta\phi_c}{4\pi T_c} = \bar{v}_s + \tfrac{\lambda\Delta\phi_c}{2\pi T_c}. \tag{22}$$

Therefore, we can generally detect false targets based on diverse velocity estimates.

Moreover, when the attacker executes fine-grained adaptive attacks with two slightly different spoofing velocities, we can identify false targets by detecting unreasonable fluctuations in velocity estimates. By allowing the two channels to exchange their phase offsets every other frame, we introduce varying deviations to the attacker's velocity estimates $\hat{v}_a^c$ in neighboring frames. Consequently, the attacker would dynamically alter the velocity offset Δv_s^c to maintain the expected spoofing velocity, resulting in the victim observing significant fluctuations in the velocity estimates $\hat{v}_s^c$. In contrast, the velocity estimates of the real targets remain unaffected and change smoothly as the



(a) Channel 1. (b) Channel 2. (c) Fusion result.

Fig. 5. An illustration of the input and output of the multiple channel fusion algorithm.

objects move. Leveraging on the continuity of motion, we can effectively distinguish false targets from real ones.

In summary, by employing three metrics: distinct range estimates, distinct velocity estimates, and similar yet unreasonable estimates, we can effectively classify all the detected targets and derive their range and velocity estimates.

F. Spoofing Mitigation

Next, we would localize regions for detected targets in the RD profiles based on their range and velocity estimates. By preserving the regions corresponding to real targets and interpolating the regions associated with false targets, we could mitigate spoofing attacks and derive unaffected RD profiles through multi-channel fusion. In practical implementation, the beat signals of the channels $h_1(t), h_2(t)$ are sampled and arranged into $N \times M$ matrices $\mathbf{H_1}$, $\mathbf{H_2}$ for the computation of RD profiles. We denote the beat signal matrix of the c^{th} channel as:

$$\begin{aligned} &\mathbf{H_c}[n,m] = h_c[n+mN],\ c{=}1,2, \\ &n{=}0,1,\ldots,N{-}1,\ m{=}0,1,\ldots,M{-}1, \end{aligned} \tag{23}$$

where N is the number of samples in the chirp, M is the number of chirps in the frame, $h_c[l]$ is the discrete beat signal, and $l{=}0,\ 1,\ \ldots,\ NM{-}1$ is the index of the sampled sequence.

We employ Range FFT along columns of the matrices i.e., the fast time dimension, to obtain the range profiles:

$$\mathbf{R_c}[n,m] = FFT(\mathbf{H_c}[n,m]). \tag{24}$$

Subsequently, we apply phase calibration and adopt Doppler FFT along rows of the matrices i.e., the slow time dimension, to derive the RD profiles:

$$\begin{aligned} \mathbf{P_c}[n,m] &= FFT(\mathbf{R_c}[n,m] * e^{-jm\Delta\phi_c})), \\ \mathbf{A_1}[n,m] &= ABS(\mathbf{P_1}[n,m]), \\ \mathbf{A_2}[n,m] &= INTERP(ABS(\mathbf{P_1}[n,m])). \end{aligned} \tag{25}$$

Since different frequency slopes are adopted, the RD profiles from the two channels have different unambiguity ranges and resolutions. Therefore, we standardize the RD profiles from channel 2 through interpolation. Afterward, we obtain the amplitude spectra of RD profiles through modulus calculation. An example of the amplitude spectra of channels 1 and 2 are shown in Fig. 5(a) and 5(b). With all the preprocessing complete, we could feed the amplitude spectra as input and utilize Algorithm 1 to perform the multi-channel fusion.

In Algorithm 1, we sequentially determine regions corresponding to false targets with distinct estimates and those with unreasonable estimates. Initially, we compute the differ-

Algorithm 1: Multiple Channel Fusion.

Input: Amplitude spectra of RD profiles $\mathbf{A_1}$, $\mathbf{A_2}$;
Estimates of false targets with unreasonable values in channel 1: $\mathbf{E_u^1}{=}[(\hat{d}_1^1, \hat{v}_1^1), \ldots, (\hat{d}_U^1, \hat{v}_U^1)]$;
Small quantities of range and velocity ϵ_d, ϵ_v.

Output: Multi-channel fusion result $\mathbf{A_f}$.

```
// false targets with distinct estimates
D = ReLU(A_1 − A_2);
B_d = CFAR(D);
// false targets with unreasonable estimates
B_u = 0;
if U > 0 then
    B_t = CFAR(A_1);
    [B_1, B_2, ..., B_{K+S}] = DBSCAN(B_t);
    for i = 1 to K+S do
        d̂_i^1, v̂_i^1 = EST(B_i);
        for j = 1 to U do
            if ||d̂_i^1 − d̂_j^1|| ≤ ε_d & ||v̂_i^1 − v̂_j^1|| ≤ ε_v then
                B_u = B_u + B_i;
M = B_d + B_u;
A_f = INTERP(A_1, M) + A_1 * (1 − M);
return A_f;
```

ence matrix $\mathbf{D}$ by applying the rectified linear unit (ReLU) function to the element-wise difference of the amplitude spectra $\mathbf{A_1}$, $\mathbf{A_2}$ (line 1). Since the fusion result $\mathbf{A_f}$ is derived by manipulating $\mathbf{A_1}$, we focus solely on the corresponding regions in channel 1. The corresponding regions in channel 2 are irrelevant. Therefore, we employ the ReLU function, a piecewise function that returns the maximum of zero and its input, to set the values in those regions to zero. Thereby, we could obtain the binary matrix $\mathbf{B_d}$ that represents the regions of false targets with distinct estimates, using the constant false alarm rate (CFAR) algorithm (line 2).

Given the difficulty for an attacker to inject false targets with unreasonable values, we initialize the binary matrix $\mathbf{B_u}$ as an all-zero matrix of the same size, indicating the absence of such targets. In scenarios where false targets with unreasonable estimates are present, we employ the CFAR algorithm to identify the regions of all targets in $\mathbf{A_1}$ (lines 5). Subsequently, we apply the DBSCAN algorithm to partition $\mathbf{B_u}$ into $K+S$ binary matrices, with each matrix representing an individual target (lines 6). After that, we match the range and velocity estimates of the detected targets with the values of false targets having unreasonable estimates and superimpose all corresponding matrices onto the binary matrix $\mathbf{B_u}$ (lines 7-11). By integrating $\mathbf{B_d}$ and $\mathbf{B_u}$, we obtain the binary matrix $\mathbf{M}$, which denotes the regions of all false targets in channel 1 (line 12). We then interpolate the internal vacancies within these regions based on the edge values and preserve the result of $\mathbf{A_1}$ for the remaining regions (line 13). As illustrated in Fig. 5(c), the fusion result $\mathbf{A_f}$ mitigates all false targets present in channel 1, preserving only noise and the real targets.

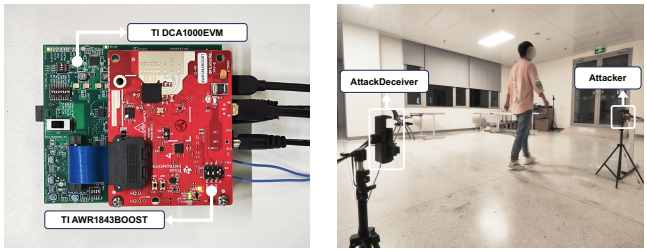
V. Implementation

Hardware Platform: We implement AttackDeceiver and the attacker using the COTS mmWave radar kits provided by Texas Instrument (TI). As illustrated in Fig. 6(a), the radar kit includes a TI AWR1843BOOST sensor board operating at 76–81 *GHz* [32] and a TI DCA1000EVM data collection board [33]. The AWR1843BOOST features three transmitting antennas and four receiving antennas. Through the interleaving and de-interleaving, we enable robust environment sensing with only a pair of antennas. The chirp waveform configurations are detailed in Table II. Specifically, we set the sampling rate to $10\,MHz$, the chirp cycle time to $35\,\mu s$, and the frequency slope of channel 1 to $20\,MHz/\mu s$, to satisfy the requirements of $0.25\,m$ range resolution and $37.5\,m$ maximum range in blind spot detection. Furthermore, we configure the number of chirps per frame in each channel to 128, to accommodate the speed limit of $100\,km/h$.

Software: We use TI mmWave studio version 02.01.01 for radar configuration and MATLAB R2022(a) for radar signal processing. Our software runs on Windows personal computers with an AMD Ryzen 7 3700X CPU equipped with an 8-core processor and 16GB of RAM.

TABLE II
Chirp waveform configurations

Parameter	Value	Parameter	Value
Chirp Idle Time	$6\,\mu s$	Chirp Cycle Time	$35\,\mu s$
Chirps Per Frame	256	Frame Periodicity	$10\,ms$
Samples Per Chirp	256	Sampling Rate	$10\,MHz$
Phase Offset Unit 1	180°	Frequency Slope 1	$20\,MHz/\mu s$
Phase Offset Unit 2	90°	Frequency Slope 2	$10\,MHz/\mu s$



(a) AttackDeceiver setup. (b) Evaluation scenario.

Fig. 6. AttackDeceiver implementation and evaluation scenario.

VI. Evaluation

A. Evaluation Setup

We set up our evaluation scenario in an open space ($6.5\,m \times 12.5\,m$) in the research building. The experimental environment and equipment are shown in Fig. 6(b). We employ one mmWave radar kit as AttackDeceiver and the other as the attacker. Meanwhile, we ask people to walk around within the detection field of AttackDeceiver as the real targets. We conduct experiments with different frequency slopes, phase offsets, distances, and directions. We ensure time synchronization among hardware devices through a wired connection approach. In addition, we explore the impact of movement on the performance of AttackDeceiver in three dynamic cases.

B. Evaluation Metrics

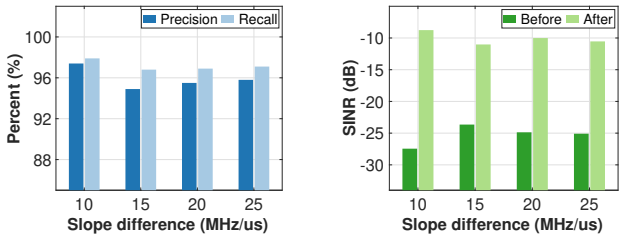
We evaluate the spoofing detection performance of AttackDeceiver by analyzing precision and recall for false targets. The precision and recall are defined as:

$$Precision = \frac{TP}{TP + FP}, \quad Recall = \frac{TP}{TP + FN}. \tag{26}$$

In our context, TP represents the false targets correctly identified as false. Whereas, FP, FN represents the real targets incorrectly identified as false, and the false targets incorrectly identified as real. Therefore, precision reflects the probability that a target identified as false is indeed false, while recall reveals the probability that a target with a false truth value is correctly identified. By utilizing the probabilities of these two types of misclassifications, we can comprehensively assess the detection performance of the system.

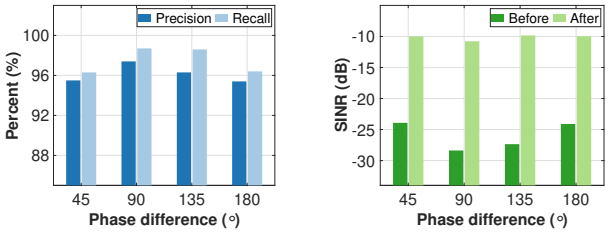
We evaluate the spoofing mitigation performance by comparing the real target to the false target plus noise ratio, (RFNR) before and after multi-channel fusion, which is defined as:

$$RFNR = 10\lg\left(\frac{P_r}{P_f + P_n}\right), \tag{27}$$



(a) Detection performance. (b) Mitigation performance.

Fig. 7. Impact of frequency slopes.



(a) Detection performance. (b) Mitigation performance.

Fig. 8. Impact of phase offsets.

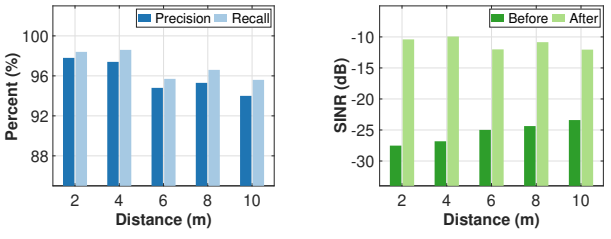
where P_r, P_f, P_n are the power of the real targets, false targets, and noise. Compared to the absolute strength reduction of false targets, the relative RFNR is more stable and can be generalized for a wide range of scenarios. A large RFNR increment indicates good mitigation performance.

C. Overall Performance

We first evaluate the overall performance of AttackDeceiver using the evaluation metrics described above. Since AttackDeceiver is free to set the frequency slopes and phase offsets of the channels, we conduct extensive experiments to investigate the impacts of parameter settings and maximize the overall performance.

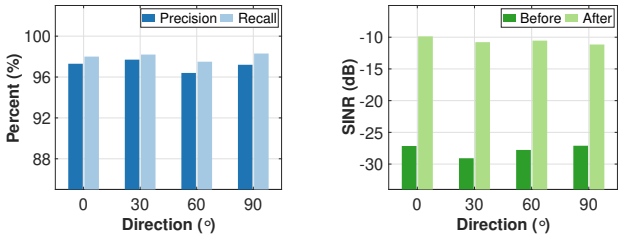
Impact of Frequency Slopes: Since we adopt a fixed chirp cycle time, the frequency slopes of the channels directly determine the maximum unambiguous range and range resolution of the RD profiles. Excessive slope differences may complicate the multi-channel fusion. Therefore, we evaluate the impact of frequency slopes by increasing the slope difference between two channels from $10\,MHz/\mu s$ to $25\,MHz/\mu s$ in increments of $5\,MHz/\mu s$. Fig. 7(a) demonstrates the detection performance of our system. Although the slope difference increase yields a slight decrease in the precision and recall, the overall precision remains above 95% and the overall recall remains above 97%. Besides, as shown in Fig. 7(b), the RFNR before and after mitigation is approximately $-25.27\,dB$ and $-10.08\,dB$. The average improvement of $15.18\,dB$ indicates that our system effectively mitigates false targets.

Impact of Phase Offsets: Besides, we evaluate the impact of the phase offsets by varying the phase offset difference between two channels from $45°$ to $180°$ in increments of $45°$. As illustrated in Fig. 8, the system performance exhibits a symmetric trend with increasing phase difference. The optimal performance is achieved when the phase difference is $90°$.



(a) Detection performance. (b) Mitigation performance.

Fig. 9. Impact of distance.



(a) Detection performance. (b) Mitigation performance.

Fig. 10. Impact of direction.

At this point, the precision reaches 97.4%, the recall reaches 98.7%, and the RFNR has an improvement of $17.60\,dB$. Furthermore, the performance remains robust in the worst-case scenario. The precision attains 95.3%, the recall reaches 96.4%, and the RFNR enhances $13.93\,dB$. The performance result implies that our system enables effective spoofing detection and mitigation.

D. Robustness

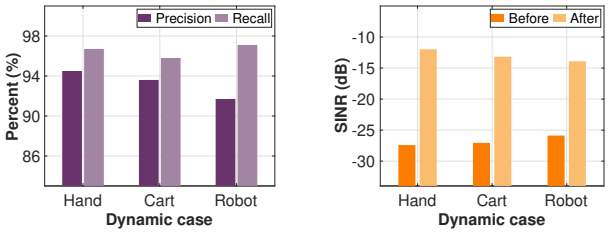
Robustness is a crucial issue for the anti-spoofing system. Thus, we conduct extensive experiments under varying distances and directions to demonstrate the robustness of AttackDeceiver.

Impact of Distance: We commence our evaluation on the impact of distance, by adjusting the separation between the attacker and AttackDeceiver from $2\,m$ to $10\,m$ with a $2\,m$ step. To exclude the influence caused by different directions, we place the attacker in the same incident direction of $0°$. As shown in Fig. 9(a), the precision and recall slightly decline when the distance exceeds $4\,m$. Nevertheless, the average precision and recall beyond $4\,m$ remain above 94% and 95%, indicating that our system sustains high detection performance. As displayed in Fig. 9(b), the variation in distance results in a minor reduction in the RFNR improvement, averaging $0.72\,dB$ per meter. Nonetheless, the RFNR still enhances by over $11.35\,dB$ after mitigation. These performance outcomes suggest that our system is distance-resistant.

Impact of Direction: We then evaluate how the incidence direction affects the performance of our system. We maintain the attacker at a constant distance and control the incidence direction within the COTS radar field-of-view (FOV), varying from $0°$ to $90°$ in $30°$ increments. As presented in Fig. 10(a), the precision and recall are minimally affected by the incidence direction, with average values of 96.9% and 98.1%. Additionally, Fig. 10(b) demonstrates a steady improvement

(a) Handheld. (b) Cart. (c) ROS robot.

Fig. 11. Different dynamic cases.



(a) Detection performance. (b) Mitigation performance.

Fig. 12. Performance of dynamic case.

in the RFNR across different directions. The lowest RFNR improvement still reaches $15.96\,d$B at $90°$. The remarkable performance results reveal the directional robustness of our system.

E. Dynamic Case Study

In the AV scenario, the relative positions of the attacker and the victim vary frequently. Therefore, in this section, we evaluate the performance of our system in certain dynamic scenarios. Since the motion between the attacker and AttackDeceiver is relative, we only test the situations where the attacker is moving. As shown in Fig. 11, we move the attacker using three approaches: handheld, mounted on a cart, and mounted on a ROS-based robot. In these dynamic cases, the attacker moves back and forth facing the AttackDeceiver at a speed of $3\,km/h$, $4\,km/h$, and $8\,km/h$. Meanwhile, people are asked to walk around within the FOV as the detection objectives.

The performance results for the dynamic cases are shown in Fig 12. We can observe that the recall exceeds 96% across various speeds. Whereas, the precision decreases as the speed of the attacker increases. This result indicates that our system tends to misclassify real objects as false ones while the attacker moves fast. The misclassification would lead to the incorrect elimination of some real targets, resulting in an precision of 91.7% in the ROS robot case. The misclassification also impacts the mitigation performance. As depicted in Fig. 12(b), the RFNR improvement decreases with increasing speed. The worst-case RFNR improvement attains $11.97dB$ when the attacker is mounted on the ROS robot. Considering the human ability to sense surrounding objects also diminishes at higher speeds, we deem these results acceptable.

VII. Conclusion

In this work, we present AttackDeceiver, a novel anti-spoofing automotive radar system that detects and mitigates fine-grained adaptive attacks using the COTS mmWave radar kit. It employs an interleaving chirp waveform to detect false targets with different or unreasonable estimates and utilizes multi-channel fusion to reveal the expected unaffected environment leveraging RD profiles. Extensive experiments demonstrate that AttackDeceiver is capable of achieving accurate sensing in a variety of realistic environments. We believe it can be deployed to secure AVs in various scenarios with flexible spoofing attacks.

References

[1] J. Van Brummelen, M. O'brien, D. Gruyer, and H. Najjaran, "Autonomous vehicle perception: The technology of today and tomorrow," *Transportation research part C: emerging technologies*, vol. 89, pp. 384–406, 2018.

[2] J. Borenstein and Y. Koren, "Obstacle avoidance with ultrasonic sensors," *IEEE Journal on Robotics and Automation*, vol. 4, no. 2, pp. 213–218, 1988.

[3] J. Kim, S. Hong, J. Baek, E. Kim, and H. Lee, "Autonomous vehicle detection system using visible and infrared camera," in *2012 12th International Conference on Control, Automation and Systems*. IEEE, 2012, pp. 630–634.

[4] S. Royo and M. Ballesta-Garcia, "An overview of lidar imaging systems for autonomous vehicles," *Applied sciences*, vol. 9, no. 19, p. 4093, 2019.

[5] 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.

[6] S. Rajendar and V. K. Kaliappan, "Recent advancements in autonomous emergency braking: A survey," in *2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*. IEEE, 2021, pp. 1027–1032.

[7] V. K. Kukkala, J. Tunnell, S. Pasricha, and T. Bradley, "Advanced driver-assistance systems: A path toward autonomous vehicles," *IEEE Consumer Electronics Magazine*, vol. 7, no. 5, pp. 18–25, 2018.

[8] 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.

[9] 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.

[10] 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.

[11] D. Solomitckii, C. B. Barneto, M. Turunen, M. Allén, G. P. Zhabko, S. V. Zavjalov, S. V. Volvenko, and M. Valkama, "Millimeter-wave radar scheme with passive reflector for uncontrolled blind urban intersection," *IEEE transactions on vehicular technology*, vol. 70, no. 8, pp. 7335–7346, 2021.

[12] M. E. Russell, A. Crain, A. Curran, R. A. Campbell, C. A. Drubin, and W. F. Miccioli, "Millimeter-wave radar sensor for automotive intelligent cruise control (icc)," *IEEE Transactions on microwave theory and techniques*, vol. 45, no. 12, pp. 2444–2453, 1997.

[13] 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.

[14] P. Nimac, A. Krpič, B. Batagelj, and A. Gams, "Pedestrian traffic light control with crosswalk fmcw radar and group tracking algorithm," *Sensors*, vol. 22, no. 5, p. 1754, 2022.

[15] C. Yan, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," 2016. [Online]. Available: https://api.semanticscholar.org/CorpusID:27264520

[16] H.-R. Chen and P. Pace, *FMCW radar jamming techniques and analysis*. Monterey, California: Naval Postgraduate School, 2013.

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

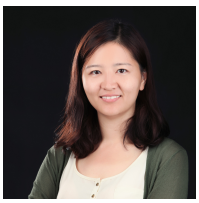
[18] R. Komissarov and A. Wool, "Spoofing attacks against vehicular fmcw radar," in *Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security*, 2021, pp. 91–97.
[19] R. Chauhan, R. M. Gerdes, and K. Heaslip, "Demonstration of a false-data injection attack against an fmcw radar," *Embedded Security in Cars (ESCAR)*, 2014.
[20] R. Chauhan, *A platform for false data injection in frequency modulated continuous wave radar*. Utah State University, 2014.
[21] S. Roome, "Digital radio frequency memory," *Electronics & communication engineering journal*, vol. 2, no. 4, pp. 147–153, 1990.
[22] R. Chauhan, "A platform for false data injection in frequency modulated continuous wave radar," Master's thesis, Utah State University, 2014.
[23] 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, 09 2021.
[24] 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.
[25] 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.
[26] R. Reddy Vennam, I. K. Jain, K. Bansal, J. Orozco, P. Shukla, A. Ranganathan, and D. Bharadia, "mmspoof: Resilient spoofing of automotive millimeter-wave radars using reflect array," in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 1807–1821.
[27] X. Chen, Z. Li, B. Chen, Y. Zhu, C. X. Lu, Z. Peng, F. Lin, W. Xu, K. Ren, and C. Qiao, "Metawave: Attacking mmwave sensing with meta-material-enhanced tags," *Proceedings 2023 Network and Distributed System Security Symposium*, 2023. [Online]. Available: https://www.ndss-symposium.org/ndss2023/
[28] M. Ordean and F. D. Garcia, "Millimeter-wave automotive radar spoofing," 2022. [Online]. Available: https://arxiv.org/abs/2205.06567
[29] 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, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/6/2145
[30] Y. Zhu, C. Miao, H. Xue, Y. Yu, L. Su, and C. Qiao, "Malicious attacks against multi-sensor fusion in autonomous driving," in *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*, ser. ACM MobiCom '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 436–451.
[31] Y. Qiu, J. Zhang, T. Sun, Y. Chen, J. Zhang, and B. Ji, "Waston: Inferring critical information to enable spoofing attacks using cots mmwave radar," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–14, 2024.
[32] Texas Instruments Incorporated, "AWR1843, Single-chip 76-GHz to 81-GHz automotive radar sensor integrating DSP, MCU and radar accelerator," 2020, https://www.ti.com/product/AWR1843.
[33] Texas Instruments Incorporated, "DCA1000EVM, Real-time data-capture adapter for radar sensing evaluation module," 2020, https://www.ti.com/tool/DCA1000EVM.

Kaiyi Huang received his B.E. degree in the Department of Computer Science and Engineering in 2023. He is currently a master student in Computer Science and Engineering, at Southern University of Science and Engineering. His research interests include wireless sensing and security.

Shengding Liu will receive his B.E. degree in the Department of Computer Science and Engineering from Southern University of Science and Technology in 2025. His research interests include mmwave sensing and security and UWB localization.

Yanlong Qiu received his B.E. degree in the Department of Electrical and Electronic Engineering (EEE) from the Southern University of Science and Technology in 2017. He received his Ph.D. in Computer and Information Science at Temple University, USA, and in Computer Science and Engineering at Southern University of Science and Technology, China. His research interests include wireless sensing and security.

Yanjiao Chen received her B.E. degree in Electronic Engineering from Tsinghua University in 2010 and Ph.D. degree in Computer Science and Engineering from Hong Kong University of Science and Technology in 2015. She is currently a Bairen researcher at the College of Electrical Engineering, Zhejiang University, China. Her research interests include computer networks, network security, and the Internet of Things.



Jin Zhang is currently an associate professor with the Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen. She received her B.E. and M.E. degrees in electronic engineering from Tsinghua University, Beijing, in 2004 and 2006 respectively, and received her Ph.D. degree in computer science from Hong Kong University of Science and Technology, Hong Kong, in 2009. She was then employed in HKUST as a research assistant professor. Her research interests are mainly in mobile healthcare and wearable computing, wireless communication and networks, network economics, cognitive radio networks, and dynamic spectrum management. She has published more than 70 papers in top-level journals and conferences. She is the principal investigator of several research projects funded by the National Natural Science Foundation of China, the Hong Kong Research Grants Council, and the Hong Kong Innovation and Technology Commission.