Spoofing attacks against vehicular FMCW radar

Rony Komissarov\textsuperscript{1} · Sharon Vaisman\textsuperscript{1} · Avishai Wool\textsuperscript{1} \footnote{Avishai Wool \texttt{yash@eng.tau.ac.il} \par Rony Komissarov \texttt{ronykom@gmail.com} \par Sharon Vaisman \texttt{vaisman.sh@gmail.com} \par \textsuperscript{1} Tel Aviv University, Tel Aviv, Israel}

Received: 12 June 2022 / Accepted: 26 April 2023 / Published online: 22 May 2023 © The Author(s), under exclusive licence to Springer-Verlag GmbH Germany, part of Springer Nature 2023

Abstract
The safety and security of the passengers in vehicles in the face of cyber attacks is a key concern in the automotive industry, especially with the emergence of the Advanced driver assistance systems and the vast improvement in autonomous vehicles. Such platforms use various sensors, including cameras, LiDAR and mmWave radar. These sensors themselves may present a potential security hazard if exploited by an attacker. In this paper we propose a system to attack an automotive FMCW mmWave radar, that uses fast chirp modulation. Using a single rogue radar, our attack system is capable of spoofing the distance and velocity measured by the victim vehicle simultaneously, presenting phantom measurements coherent with the laws of physics governing vehicle motion. The attacking radar controls the delay in order to spoof its distance, and uses phase compensation and control in order to spoof its velocity. After developing the attack theory, we demonstrate the spoofing attack by building a proof-of-concept hardware-based system, using a Software Defined Radio. We successfully demonstrate two real-world scenarios in which the victim radar is spoofed to detect either a phantom emergency stop or a phantom acceleration, while measuring coherent range and velocity. We also discuss several countermeasures that can mitigate the described attack.

Keywords Vehicular FMCW · Radar spoofing · ADAS · PBAD

1 Introduction

1.1 Background
The safety and security of the passengers in vehicles in the face of cyber attacks is a key element in the automotive industry, especially with the emergence of the Advanced Driver Assistance Systems (ADAS) and the vast improvement in Autonomous Vehicles (AVs) \cite{43}. The main sensors available on modern self-driving cars are Ultrasonic sensors, mmWave (Millimeter Wave) radars, cameras, and LiDAR \cite{8, 39}. These sensors are used for sensing the physical environment and for safety-critical decisions, such as collision avoidance and intersection management. Adversarial sensor attacks manipulate the input signals to the sensors in order to produce incorrect environment views with the goal of causing attacker-selected, or unsafe, actions. These attacks can be organized into two main categories: Spoofing and Jamming \cite{42}. While the latter attack can be easily detected, mitigating a spoofing attack usually requires more intelligent countermeasures \cite{16}. Spoofing makes it very difficult for the sensor system to recognize that it is under attack, as it provides the victim sensor with seemingly legitimate but actually false data.\footnote{A preliminary version of this paper appeared in ASHES’2021.}

Various sensors of autonomous vehicle are vulnerable to spoofing attacks. Prior work mainly focused on the study of security in perception sensors, primarily the LiDAR and camera. Physical world camera attacks were demonstrated by fooling deep neural networks (DNNs), making objects mislabeled or ignored \cite{7, 33}. For example, in \cite{7}, the researchers caused a “STOP” sign disappear in the eyes of the detector, by adding adversarial stickers onto the sign. Attacks against LiDAR-based perception systems in AVs appear in \cite{2, 3}. The authors found that simply spoofing the LiDAR using common methods is not sufficient due to the use of machine learning object detection models. To mount an attack they leveraged an optimization method to generate adversarial examples to fool a real-world working LiDAR.

Some work has also been done to attack and spoof ranging systems, such as Radar and Ultrasonic sensors \cite{37}. Due...
to the fact that the mmWave radar is crucial in bad weather conditions, an attack to fool its measured distance is a critical physical security threat [11, 32]. Specifically, distance-only spoofing attacks were presented on a mmWave Frequency Modulated Continuous Wave (FMCW) radar [4, 5, 24, 27]. Chauhan et al. [4, 5] examine the feasibility of spoofing the distance measured by an FMCW radar using a Software Defined Radio (SDR). The attack presented used a cable connected to the RF port of the victim. Nashimoto et al. [24, 27] used a weak Arduino platform against an FMCW radar which used the less-common triangular waveform. The attackers synchronised to the victim via half-chirp modulation, and were able to control the delay measured by a victim radar to spoof the range. However, beyond measuring range, FMCW radars are typically used to measure velocity, which they can achieve with high precision [8]. The attack methods in [4, 5, 24, 27] do not spoof the velocity measured by the victim at all.

Recently, Sun et al. [35] constructed several attack scenarios in order to spoof a mmWave radar of a Lincoln MKZ-based AV testbed, using an SDR transceiver system from National Instruments. The attack strategies involved synchronised attack radars on both sides of the road, using a complex setup. Furthermore, the method the attackers used to spoof velocity measurements was by spoofing the distance at subsequent time intervals, but modern mmWave radars have the ability to measure velocity independently from distance. [14].

In order to demonstrate how even a financially limited hacker can spoof a radar, Lazaro et al. [19] constructed a RFID-technology-based spoofing device. They managed to generate a pair of false targets at different ranges and velocities depending on the modulation frequency of the chosen tag. Similarly, Nallabolu and Li [26] created an analog homemade spoofing device capable of creating false targets in various ranges, with no velocity spoofing. These two articles demonstrate well how it is possible to produce cheap spoofing devices, but without any control mechanism that can adjust to any chosen phase shift and manipulate the speed. Moreover, there is a limited control over the types of targets that can be produced.

Extensive research has been done in order to detect, prevent and mitigate such attacks. For example, attack prevention in mmWave radar was presented in the work of Moon et al., which introduces the BlueFMCW [25]. The BlueFMCW is a novel frequency hoping radar, that uses frequency randomization in order to prevent attacks on automotive radar sensors [25].

For attack detection purposes, Physics-Based Attack Detection (PBAD) algorithms were introduced, and they represent a way to detect sensor tampering attacks against autonomous vehicles [10]. Physics-Based Attack Detection techniques use security monitors that create a time-series model of the physical sensor and check the consistency between the received sensor measurements and the physical model. An example for such a technique is “SAVIOR” [30].

While the SAVIOR technique is able to identify sudden sharp changes in the sensor values, it struggles to cope with slow but persistent spoofing attacks. In such attacks, the attacker injects a small perturbation at each time step, which causes damage over time. In order to countermeasure such attacks, multi-sensor PBAD is used [13]. For example, the “Shared Reality” [31] framework verifies that separate sensors perceive the same physical reality, leveraging the fact that there are common physical data between sensors that should be closely related.

1.2 Our contribution

In this work we demonstrate an adversarial radar based on an SDR, which can simultaneously manipulate the range and velocity measured by a victim radar used by an ADAS or AV platform.

The adversarial radar we designed utilizes the advantages of a complex baseband FMCW radar: beyond controlling the delay to spoof the range, we are able to manipulate the signal phase received at the victim radar’s Rx antenna, to spoof the velocity.

Unlike [5, 24, 27], which focused on radars using a triangular chirp waveform, our system addresses the modern saw-tooth waveform (so-called fast chirps), as this chirp waveform is frequently found in contemporary FMCW radars in the AV industry [22, 38]. And unlike [35], we only require a single rogue radar within a vehicle in front of the victim.

After developing the attack theory, we demonstrate the spoofing attack by building a proof-of-concept hardware-based system, using a bladeRF Software Defined Radio. Using the ability to manipulate the velocity and the range measured by the victim radar, we demonstrate two realistic automotive attack scenarios: spoofing a phantom emergency break, and spoofing a phantom acceleration. In both cases, the range and velocity measured by the victim radar are coherent and fit the laws of physics governing vehicular motion. Then, we show that the proposed attack is not detectable by contemporary physics-based attack detection (PBAD) systems: we evaluate its success in evading both single-sensor PBAD like SAVIOR [30] and multi-sensor PBAD systems like Shared Reality [31]. Finally we discuss other countermeasures that can mitigate the attack.

2 The FMCW radar

Generally, radars emit electromagnetic waves and receive the reflection to measure the time of flight. Specifically, in FMCW radar solutions, the transmitted signal is a linear
frequency modulated continuous wave (FMCW) chirp [23]. FMCW radars are common in a variety of industries and applications, such as naval navigation radars, smart ammunition sensors, industrial radars, and in particular automotive radars [17, 20, 34].

Since the frequency component of the chirp is non-constant in time, it is usually described as a frequency over time spectrogram, as described in Fig. 1a. The description of the chirp development in time is given in Fig. 2a.

Modern systems use a saw-tooth waveform chirp with slope $S = \frac{df}{dt}$ and bandwidth parameters depending on the distance and velocity of the object of interest [38, 41]. The state-of-the-art FMCW radars integrated in commercial vehicles use the 76–81 GHz frequency band [9]. Typical FMCW Radar implementations include a Voltage Controlled Oscillator (VCO) which is used to create the necessary chirp waveform. The output of the VCO is amplified by the Power Amplifier (PA), and then transmitted through the Antenna.

In order to improve the precision of the physical measurements, a series of $N$ chirps (a frame) is averaged. The number of chirps $N$ is usually in the range of 50–1000 [22].

### 2.1 Measuring range using FMCW radar

The transmitted FMCW signal is reflected by the object of interest, and gets back to the Rx antenna of the radar after a total delay time $t_d$, as seen in Fig. 1b. The received chirp is then mixed with the currently transmitted signal. The product of the mixing process is called an IF (Intermediate Frequency) signal, and it exhibits a single beat frequency of $f_b$ (Fig. 1c, d). Finally, the IF signal is sampled by the ADC and further processed by a DSP or MCU. The range $d$ of the object is related to the beat frequency $f_b$ by the following equation:

$$d = \frac{c \cdot f_b}{2S}$$

where $S$ is the slope of the Tx chirp and $c$ is the speed of light.

There are several ways to extract the beat frequency of the IF signal. A common way is to use a fast Fourier transform (Range-FFT), to convert the time domain signal into a spectrum with a peak at $f_b$, as depicted in Fig. 1d. Typical IF frequencies are in the range of a few hundred kHz for objects within 100 m. Thus, there is no requirement for a relatively high speed ADC.

### 2.2 Measuring velocity using FMCW radar

To measure velocity, the radar utilizes pairs of chirps $T(t)$ that are transmitted consecutively, as depicted in Fig. 2b. The calculation of the velocity relies on the fact that the change in the beat frequency between adjacent IF signals in the frame is negligible compared to the phase shift of the IF signal. This assumption holds since the phase of the mmWave signal is more sensitive to object movement, in contrast to the return delay, which is practically constant between the chirps in the same frame, due to the Doppler effect and the fast chirp modulation. Similarly to the range measurement, the IF signal $B(t)$ (Fig. 2c) corresponding to each returned chirp $R(t) = T(t - t_d)$ is sampled and further processed, this time in order to calculate its phase, again using range-FFT.

The relative velocity $v$ of the moving object to the radar can be derived from the phase difference $\Delta \varphi_{21}$ between...
adjacent chirps’ IF signals $B_{i+1}, B_i$:

$$v = \frac{\lambda \Delta \psi_{i+1,i}}{4\pi T_c}$$

where $T_c$ and $\lambda$ are the chirp duration and the radar signal wavelength, respectively (see [12]).

3 The adversarial FMCW radar model

3.1 Attack model

In our scenario the victim vehicle is behind the attacker’s vehicle and has an FMCW radar installed, facing forward, as depicted in Fig. 3. We assume the attacker has a modified radar system in his vehicle facing back. The attacker can send a much more powerful signal compared to the real reflected signal arriving at the victim. This assumption easily holds, even without extra amplification, as the attacker’s signal only needs to traverse half of the distance, compared to the victim radar’s signal.

We assume that the victim radar parameters are known to the attacker. This is a reasonable assumption, since there is a small number of vehicular radar manufacturers and their radar’s parameters are known and public. Moreover, vendors are required to file the technical parameters of all transmitting systems with the FCC and the filing documents are public.

Finally, the victim’s true relative distance $\hat{d}$ and relative velocity $\hat{v}$ from the attacker are known to the attacker: they are measured by the attacker’s radar, in order to be able to perform the attack.

3.2 Attack system architecture

The adversarial system is depicted in Fig. 4. The adversarial radar is a modified version of the victim radar: the main change is the additional delay and phase control logic. Our system is a complex baseband (quadrature) radar that simultaneously controls the delay (to spoof range measurements) and phase (to spoof the velocity).

At a high level, the adversarial radar starts by generating internal chirps with the same parameters as the victim, but without transmitting them. Once it receives the chirps transmitted by the victim radar, it mixes the first $n$ chirps out of the frame with its internal chirps to produce its own IF signal. The attack system utilizes this IF signal to synchronise to the victim, and tune the phase and timing of each adversary chirp, to manipulate the victim’s measured velocity and range simultaneously. It sets the delay to $t_d$ and sets the phase to $\psi_d$ compensating for $\Delta \psi_c$ and $\Delta \psi_t$ so the victim radar measures distance $\hat{d}$ and velocity $\hat{v}$.

3.3 Range manipulation

By precisely controlling the time the spoofed signal is received at the victim radar, the attacker can manipulate the victim radar to measure a delay $t_d$, which is different from the original delay $t_d$, leading to an error in the calculated distance. In order to spoof the victim radar to measure an arbitrary distance $\hat{d}$, the attacker should know the exact transmit time of the current frame of chirps. To achieve synchronisation with the victim’s transmit time, the attacker estimates the arrival time to his Rx antenna of the first $n$ chirps in the frame. Since the first $n$ chirps are used in order to synchronise to the victim, only the remaining $N - n$ chirps in the frame are used for the range and velocity manipulation. Due to the fact that $N \gg n$, the chirps used for synchronisation have little effect on the manipulated range and velocity measured by
Fig. 5 The Process of Range and Velocity Spoofing: a The received chirp at the adversary radar (orange) and the synchronised internal chirp (blue). b The changing phase between each internal measured IF signal in the adversary radar. \( \Delta \phi_c \) is the phase accumulated because of frequency difference from the victim, and \( \Delta \phi_t \) is the phase change caused by the relative velocity. c The transmitted adversary signal spectrogram, with the controlled delay \( t_a = t_d/2 + t_m \) corresponding to the spoofed distance \( \hat{d} \). d The initial phase of each adversarial chirp emitted from the attacker as function of time. The phase is composed of the compensation for the phases \( \Delta \phi_c \) and \( \Delta \phi_t \), and the controlled phase \( \phi_m \) corresponding to the spoofed velocity \( \hat{v} \) (colour figure online).

the victim, since it is done by averaging the measurements of each frame, or by using two dimensional range-FFT [22]. The transmission time can be estimated by down-converting the arriving signal and estimating the TOA (Time of Arrival) using a relatively high speed ADC, or by using HCM (Half Chirp Modulation) [11]. Considering that the chirp duration \( T_c \), the true distance \( d \) and also the true delay \( t_d \) are known, the attacker knows when the next chirp will be transmitted, and thus can decide when to emit an adversarial set of chirps, which will modify the delay measured by the victim radar. The attacker can force the victim to measure a distance \( \hat{d} \) corresponding to a specific adversary delay \( t_a \), by delaying or preceding the returned signal the victim senses. Since the adversarial radar is actively transmitting, its spoofed signals will overpower the legitimate echos reflected from the adversarial vehicle.

Controlling the delay: Figs. 4 and 5 show the evolution of the attack signal. First, the adversarial radar enters a “waiting for trigger” mode. When it receives the first chirp, it synchronises with the victim radar using estimation of TOA (Time of Arrival) of the signal, or using an internal HCM. This synchronisation occurs only once in the whole process of position and velocity manipulation. As seen in Fig. 4, when the attacker is synchronised to the victim, it can generate an IF signal \( B_i(t) \) by mixing an internal synchronised version of the victim radar chirp with the incoming signal. This IF signal is depicted in Fig. 5a. Now, it can manipulate the range the victim radar measures by precisely controlling the adversarial delay \( t_a = t_d + t_m \), where \( t_d \) is the actual time of flight (TOF) and \( t_m \) is the manipulated delay the attacker adds. Since the legitimate round trip is \( t_d \), the attacker should transmit the spoofing signal at \( t_d/2 + t_m \), taking into account that the spoofing signal should still traverse the return path, which adds a delay of \( t_d/2 \). This is depicted in Fig. 5c. Therefore in order to spoof a false measured distance \( \hat{d} \) the system should generate a signal with the following added delay \( t_m \):

\[
t_m = \frac{(\hat{d} - d)}{c}
\]

where \( c \) is the speed of light.

3.4 Velocity manipulation

As depicted in Fig. 2, in normal operation, the phase difference the victim radar measures between two consecutive chirps is:

\[
\Delta \phi_{21} = \Delta B_2(t) - \Delta B_1(t) \\
= (\varphi_2 - \varphi_0) - (\varphi_1 - \varphi_0) = \varphi_2 - \varphi_1
\]

where \( \varphi_2 \) and \( \varphi_1 \) are the phases \( \Delta B_1(t)|_{t=t_1} \) and \( \Delta B_2(t)|_{t=t_2} \) of two consecutive IF signals from two consecutive chirps,
and \( t_1, t_2 \) are the delays corresponding to each chirp. As seen in Fig. 2b, the victim FMCW radar expects to receive a delayed cloned version of the signal it sends, i.e., with the same phase \( \phi_0 \), when it hits the Rx antenna. The method for velocity manipulation we propose takes advantage of this fact. To manipulate the velocity, the attacker transmits a frame of chirps with changing phases. The difference \( \Delta \phi_{21} \) is known to the attacker because the true velocity of the victim is known. Therefore, by changing the phase \( \phi_0 \) of the spoofed return signal separately for each chirp, it is possible for the attacker to control the velocity the victim measures. This can be done regardless of the victim radar’s current transmitting chirp phase: the victim’s measured phase difference depends only on the phase difference between consecutive attacker-generated returned chirps, and does not depend on the victim radar itself.

Controlling the phase: As demonstrated in Fig. 4, the attacker sends a sequence of chirps with changing phases. To do so, the attacker utilizes the quadrature manner of the complex baseband radar in order to control the phase of the transmitted chirp, similarly to PSK (Phase Shift Keying) techniques. In order to make the victim radar measure a specific velocity \( \hat{v} \), the phase of each chirp of the signal transmitted by the attacker should change with each consecutive chirp. The manipulated phase between consecutive chirps \( \Delta \psi_{i+1,i} \) is given by:

\[
\Delta \psi_{i+1,i} = \frac{4\pi \hat{v} T_c}{\lambda}
\]  

(2)

Phase accumulation: Although the victim radar and the adversarial radar are both using the same central frequency and sweep bandwidth, there is some difference between them, because of the TCXO (Temperature Controlled Crystal Oscillator) frequency tolerance. Therefore, there is an accumulated phase \( \Delta \psi_c \), with each internal IF signal \( B_i(t - n T_c) \) in the attackers’ radar. Furthermore, there is another phase accumulation \( \Delta \psi_i \), due to the true velocity difference \( v \) between the victim and the adversary. The effect of the phases \( \Delta \psi_c \) and \( \Delta \psi_i \) on the internal IF signals \( B_i(t - n T_c) \) is depicted in Fig. 5b. The attacker takes these phases into account, and compensates them when manipulating the velocity. The total adversarial phase increment \( \Delta \psi_{ai} = \Delta \psi_c + \Delta \psi_i + \phi_m \) of each chirp the attacker sends back consists of the compensation of the phases \( \Delta \psi_c \) and \( \Delta \psi_i \), and the manipulating phase \( \phi_m \). The manipulating phase \( \phi_m \) is the phase determining the current measurement change in relative velocity the victim will measure. By changing this phase with each chirp that the adversary transmits, it can precisely control the velocity \( \hat{v} \) measured by the victim, as described in Fig. 5d. Velocity and distance spoofing can occur independently, as the phase and the timing of the returned chirps are not related to each other. Therefore, the adversarial radar can manipulate both of them simultaneously. The adversary signal \( S_{Adv} \) transmitted by the attacker in order to manipulate both range and velocity is the concatenation (sum) of the \( N - n \) manipulated chirps:

\[
S_{Adv} = \sum_{i=n+1}^{N} T(t - (\frac{t_d}{2} + t_m + i \cdot T_c)) \cdot e^{j i \Delta \psi_{ai}}
\]

Where \( T(t) \) is the chirp transmitted by the victim radar, and \( i \) is an index iterating over the \( N - n \) manipulated chirps.

### 4 The proof of concept setup

The setup we implemented (see Fig. 6) consists of two Software Defined Radios (SDR): one is the attack radar, and the other represents the victim. Both SDRs are models of bladeRF 2.0 micro. The bladeRF 2.0 micro is a 2 x 2 MIMO, 47 MHz–6 GHz frequency range, USB 3.0 Software Defined Radio [29]. It provides a powerful waveform development platform. We used the xA9 model to build the attack radar, and for the victim FMCW radar we used the xA4 model. The libbladeRF open source library was used for communicating with the devices, from a Windows machine. The interface we selected is the bladeRF Synchronous Interface, which allows transmitting bursts of samples at a specified timestamp. The timestamp is a free-running counter in the FPGA, incremented at the sample rate defined, with each outgoing sample. For the ease of prototyping, the victim Tx and Rx were connected to the attacker’s Rx and Tx ports, respectively, by 15 m-long RF cables.

To simulate greater and more realistic distances between vehicles with these cables, a one-time calibration process was carried out. In this process, the victim radar transmitted
a set of chirps and the attack radar immediately returned the signal it received. Then, a fixed delay was added to the response time of the attacker, so the victim radar measured a distance \( d = 60 \text{ m} \). Since the length of the cable imitating the distance was fixed, the relative (true) velocity \( v \) simulated between the victim radar and the attacker was fixed to zero.

To add an arbitrary phase shift \( \Delta\varphi \) to the transmitted spoofed signal, we used the quadrature modulator of the attacking SDR. The attacker controls the transmitted chirps’ phases by utilizing Euler’s formula
\[
A(t) \cdot e^{j\Delta\varphi} = A(t) \cdot \cos \Delta\varphi + jA(t) \cdot \sin \Delta\varphi
\]
and multiplying the in-phase and quadrature-phase parts of the modulator with the controlled amplitudes.

In order to synchronise to the victim, we estimated the TOA, by sensing the first sample of the IF signal which is above an arbitrary threshold of noise. The center frequency \( f_c \) used in the setup was 1 GHz, the full bandwidth of the radar was 28 MHz, the chirp duration \( T_c \) was set to 1 ms, and \( n \) was set to 2 chirps.

5 Results and discussion

We simulated two scenarios: a sudden phantom stop and a sudden phantom acceleration. Each scenario was simulated 15 times. Simultaneous spoofing of distance and velocity is demonstrated in Fig. 7.

Figure 7a describes a scenario where the attacking radar simultaneously spoofs the distance and velocity representing a phantom emergency break in the adversary’s vehicle in front of it: the victim’s measured relative velocity \( \hat{v} \) drops at a constant deceleration of \(-10 \text{ m/s}^2\) spoofing a loss of 120 km/h, and the measured relative distance drops at a quadratic rate from 60 m to 0 over about 3.5 s: This rate of deceleration represents an emergency brake with ABS assistance [18]. Note that the errors are in the order of the bandwidth resolution limit of FMCW, and only limited by the SDR relatively low bandwidth capabilities. Such a scenario will probably trigger an emergency break by the victim.

Figure 7b demonstrates another security hazard: the vehicle in front of the victim is made to appear accelerating, when it actually remains at a fixed distance \( d = 60 \text{ m} \) and a fixed relative velocity \( v = 0 \). In such a case, the victim car might decide it can accelerate, leading to an accident and injuries to the driver and passengers inside of the car. The figure shows that the victim measures a velocity that mimics a fixed acceleration of \( 10 \text{ m/s}^2 \), and the range measurements increase quadratically, matching the desired curve.

Note that in both scenarios the desired spoofed orange curves are within the measured error range, and in particular the measured velocities are very close to the intended values. As we shall see in the next section, these attacks are very difficult for detection, since they are indistinct from a real scenario from the perspective of the victim vehicle. They cannot be easily mitigated by intra-radar PBAD methods, since the distance and velocity measurements are coherent with each other and consistent with the laws of physics.

6 Attack detection algorithms

To deal with sensor spoofing attacks, researchers have suggested Physics-Based Anomaly Detection (PBAD) methods to detect and prevent sensor tampering [10]. These can be divided in two main groups:

```
Fig. 7 Results of simultaneous spoofing of distance and velocity: The green line shows the true range and velocity. The orange curve shows the desired manipulated range and velocity and the blue dots show the average values measured by the victim. The time between the measurements is 250 ms. The shaded area shows the errors (± one standard deviation). a Spoofing an emergency brake. b Spoofing a scenario where an obstacle appears to be moving away from the victim radar (colour figure online)
```
One sensor algorithms (OSA). These methods try to detect physics-based anomalies in real time according to past samples from the same sensor. This kind of technique manages to deal with attacks involving sudden sharp changes in the sensed value. Examples of OSA are Control Invariant [6] and SAVIOR [30]. In this paper we test the SAVIOR algorithm against our attack.

Multiple sensor algorithms (MSA). OSA methods can be manipulated by injecting small perturbations [5] at each time step, which cause a significant drift from the real results over time. To combat such slow but persistent attacks, multi-sensor PBAD methods measure the same physical invariants with different sensors. Under the assumption that attackers are able to manipulate just one sensor, MSA will detect slow but persistent manipulations. Among these techniques one can find LIFE [21] and Shared Reality [31]. In this paper we demonstrate our attack against the Shared Reality algorithm.

6.1 SAVIOR

6.1.1 Theory

SAVIOR [30] is a proposed OSA physics-based anomaly detection system. It uses the Extended Kalman Filter (EKF) to predict the system state, according to past samples and a known noise level [40]. The predicted states are compared with the actual system states at each iteration. If the calculated difference is above a threshold, an alarm is raised and the sensor is considered compromised. In this paper we use a one-dimensional EKF for accelerating targets, called the α–β–γ filter [28]. Let \( d_1, \ldots, d_n \) denote the measured distances in iterations 1, \ldots, n. The filter is divided into two steps: estimation and prediction. In the estimation step we calculate an estimate \( e_n \) as a weighted average between the current measurement \( d_n \) and the prediction \( p_n \) (which was calculated in the previous iteration). The filter also estimates the velocity \( \dot{e}_n \) and the acceleration \( \ddot{e}_n \), as follows:

\[
\begin{align*}
\dot{e}_n &= \tilde{e}_n + \alpha (d_n - p_n) \\
\ddot{e}_n &= \tilde{\ddot{e}}_n + \beta \left( \frac{d_n - p_n}{\Delta t} \right) \\
\alpha &\quad \beta &\quad \gamma
\end{align*}
\]

The values \( \alpha, \beta, \gamma \) are the weighting parameters. Given the estimates in the end of iteration \( n \), the filter predicts the next distance \( p_{n+1} \), velocity \( \dot{p}_{n+1} \) and acceleration \( \ddot{p}_{n+1} \) of the target according to the equations of motion based on the current estimations:

\[
\begin{align*}
p_{n+1} &= e_n + \dot{e}_n \Delta t + \frac{\ddot{e}_n \Delta t^2}{2} \\
\dot{p}_{n+1} &= \dot{e}_n + \ddot{e}_n \Delta t
\end{align*}
\]

The method also includes a threshold: whenever the difference \( |d_n - e_n| \) is above the threshold, an alarm is raised, meaning the sensor is probably manipulated. We chose to base the threshold on the physical measurement error:

\[
\text{error}_d = \frac{c}{2BW} \tag{3}
\]

Where \( c \) is speed of light, \( BW \) is the bandwidth and the division by 2 is because the radar’s beam goes back and forth. For example, with the parameters of our proof of concept (Sect. 4), \( BW \) is 28 MHz so the error is 5.35 m.

6.1.2 Simulation

In our implementation of SAVIOR we used the weight values \( \alpha = 0.5277, \beta = 0.1956, \gamma = 0.01 \) (following [15]). We set the alarm threshold to be 3 times the error. We tested our implementation of the SAVIOR algorithm with 2 kinds of attacks: a (physically impossible) sudden braking, and a physically reasonable attack with the correct initial state, as described in this paper.

Figures 8a and b illustrate SAVIOR against an impossible attack of instantaneously changing the distance from 60 m to 0. Figure 8b shows that SAVIOR immediately detects the attack since the difference between the measured and estimated distances exceeds the threshold. It is important to notice that while SAVIOR gives an immediate alarm, the Kalman filter then adapts to the new measurements and the alarm stops. Finally, in Fig. 8c SAVIOR is tested against the slow but persistent manipulation of our proof of concept. The output of the filter never exceeds the measured samples by more than one standard deviation, meaning that SAVIOR fails to detect the attack.

6.2 Shared reality

6.2.1 Theory

The Shared Reality [31] idea is to compare the values that represent the same physical quantity, but computed by two separate methods that are based on separate sensor measurements. If the computed values diverge beyond a threshold, an alarm is raised.

In the case of an FMCW radar, we can construct an intraradar Shared Reality PBAD, since the radar provides both distance and velocity measurements. The velocity serves as the shared physical quantity: it is measured directly by the radar based on the measured Doppler shift, and separately, it can be calculated as the numerical derivative of the radar’s measured distance.
Following [31] for the case of the FMCW radar, we define the absolute residual error between the samples of measured velocity $v_n$ and derivative of the distance $\dot{d}_n$ to be:

$$\Delta_n = |v_n - \dot{d}_n|$$

Let $S_n$ be the total sum of residuals over time. Then $S_{n+1}$ is calculated by:

$$S_{n+1} = \max(S_n + \Delta_n - b, 0)$$

A bias value $b$ is subtracted in each iteration to offset the normal measurement errors from accumulating over time. The system raises an alarm when $S_n$ exceeds a threshold.

### 6.2.2 Simulation

The physical measurement error of velocity is calculated as the distance error divided by the sampling time error:

$$\text{error}_v = \frac{\text{error}_d}{\Delta t}$$

where $\text{error}_d$ is calculated in Eq. (3) and $\Delta t = 0.262$ sec. In our implementation we set the bias $b$ to be $\text{error}_v/2 = 10.23$ m/sec and we set the alarm threshold to be 15 m/sec.

In the Shared Reality simulation we evaluated two scenarios: In one scenario only the distance is spoofed (as in [4, 5, 24, 27]), and in the other both the distance and velocity are spoofed simultaneously, as presented in Sect. 4.

Figure 9a shows the accumulated residuals for an attack that manipulates only the distance. The figure shows that the difference between the measured velocity and the derivative of the distance accumulates over time until $S_n$ exceeds the threshold and the alarm is raised 1.9 sec after the start of the attack. On the other hand, Fig. 9b shows $S_n$ when both sensors are being manipulated: the residuals do not increase over time, and the Shared Reality system does not detect the attack.

### 7 Countermeasures

As we saw in Sect. 6 our attack is undetected by both SAVIOR and the intra-radar Shared Reality PBAD. Beyond these
unsuccessful approaches we can suggest several countermeasures against our attack:

**Phase randomization.** The velocity spoofing attack relies on the fact that the victim radar is expecting the returned signal to arrive with the same phase it was transmitted at. To break this assumption, one can send chirp signals with randomized phases, which are known to the victim radar. This approach requires more complex circuity, and sending another phase with each chirp adds another phase error to an environment that is already very error-prone.

**Frequency randomization.** Another countermeasure is random frequency hopping, as suggested by [27]. This approach will make the attack radar measure a high beat frequency when implementing the proposed attack, making it hard to synchronize to the victim radar. The authors of [25, 27] evaluated their spoofing method against a frequency-hopping (triangular chirp) radar and showed an anti-countermeasure, indicating that frequency hopping is only a partial mitigation. Nevertheless, even in non-adversarial environments, the large number of vehicles on the same road already leads to frequency spectrum density. Therefore radar manufacturers may introduce random frequency hopping or even Staggered PRI FMCW as an interference mitigation technique [1, 36], which may help mitigate spoofing attacks as a by-product.

**Integration of physically different sensors.** Since modern vehicles are equipped with several range and velocity sensors, an MSA PBAD such as Shared Reality [31] based on a non-radar sensor, (camera or LiDAR), may mitigate the attack. However, there are scenarios, such as bad weather conditions, where the only reliable sensor in the car is the mmWave radar. In such cases, a multi-sensor PBAD might mislead the vehicle with false alarms due to the incorrect measurements from the non-radar sensor.

**RSSI measurements.** Since the attacker must overpower the legitimate echos reflected from his vehicle using the adversarial signal, the victim may be able to use the Received Signal Strength Indicator (RSSI) to countermeasure the attack. For instance, the victim could set a threshold for excessively high RSSI, or could check for a pattern of $N - n$ strong chirps with $n$ weak chirps among the $N$ chirps in the frame. This approach may be difficult to calibrate due to the variability of the RSSI even in non-adversarial environments, and may also fail when there is a legitimate change in the power of the signal received due to weather conditions or a fading channel.

### 8 Conclusions

The security of the ADAS and autonomous vehicles sensors in the face of cyber attacks is crucial for the future of the automotive industry. In this paper, we proposed a system to attack an automotive FMCW mmWave radar, that uses fast chirp modulation. Our attack system is capable of spoofing the distance and velocity measured by the victim vehicle simultaneously, presenting phantom measurements coherent with the laws of physics governing vehicle motion. The attacking radar controls the delay in order to spoof its distance, and uses phase compensation and control in order to spoof its velocity. We demonstrated the spoofing attack by building a proof-of-concept hardware-based system, using a Software Defined Radio. We successfully demonstrated two real-world scenarios, in which the victim radar is spoofed to detect either a phantom emergency stop or a phantom acceleration, measuring coherent range and velocity. Moreover, we show that our attack can overcome physics-based anomaly detection methods by simultaneously manipulating the distance and velocity. We believe that with the proliferation of vehicular FMCW radars, the demonstrated attack system could pose a threat to AV and ADAS safety, and we propose several possible mitigations.

**Acknowledgements** The work of Avishai Wool and Sharon Vaisman was partially supported by award 001567-URP from the Ford Motor Company.

**Data availability statement** Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

### References

1. Bourdoux, A., Parashar, K., Bauduin, M.: Phenomenology of mutual interference of FMCW and PMCW automotive radars. In: 2017 IEEE Radar Conference (RadarConf), pp. 1709–1714. IEEE (2017)
2. Cao, Y., Xiao, C., Cyr, B., Zhou, Y., Park, W., Rampazzi, S., Chen, Q.A., Fu, K., Mao, Z.M.: Adversarial sensor attack on LiDAR-based perception in autonomous driving. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 2267–2281 (2019)
3. Changalvala, R., Malik, H.: LiDAR data integrity verification for autonomous vehicle. IEEE Access 7, 138018–138031 (2019)
4. Chauhan, R.: A platform for false data injection in frequency modulated continuous wave radar. Master’s thesis, Utah State University (2014)
5. Chauhan, R., Gerdes, R.M., Haslrip, K.: Demonstration of a false-data injection attack against an FMCW radar. Embedded Security in Cars (ESCAR) (2014)
6. Choi, H., Lee, W.-C., Aafer, Y., Fei, F., Tu, Z., Zhang, X., Xu, D., Deng, X.: Detecting attacks against robotic vehicles: a control invariant approach. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 801–816 (2018)
7. Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T., Song, D.: Robust physical-world attacks
on deep learning visual classification. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1625–1634 (2018).

8. Fung, M.L., Chen, M.Z., Chen, Y.H.: Sensor fusion: a review of methods and applications. In: 2017 29th Chinese Control And Decision Conference (CCDC), pp. 3853–3860. IEEE (2017).

9. Gao, X., Xing, G., Roy, S., Liu, H.: Experiments with mmwave automotive radar test-bed. In: 2019 53rd Asilomar Conference on Signals, Systems, and Computers, pp. 1–6. IEEE (2019).

10. Giraldo, J., Urbina, D., Cardenas, A., Valente, J., Faisal, M., Ruths, J., Tippenhauer, N.O., Sandberg, H., Candell, R.: A survey of fiber-based target detection in cyber-physical systems. ACM Comput. Surv. (CSUR) 51(4), 1–36 (2018).

11. Goodin, C., Carruth, D., Doude, M., Hudson, C.: Predicting the influence of rain on LiDAR in ADAS. Electronics 8(1), 89 (2019).

12. Iovescu, C., Rao, S.: The fundamentals of millimeter wave sensors. Texas Instruments Whitepaper (2017). https://www.mouser.ee/pdfdocs/mmwavewhitepaper.pdf

13. Ivanov, R., Pajic, M., Lee, I.: Attack-resilient sensor fusion for safety-critical cyber-physical systems. ACM Trans. Embed. Comput. Syst. (TECS) 15(1), 1–24 (2016).

14. Jagielski, M., Jones, N., Lin, C.-W., Nita-Rotaru, C., Shiraishi, S.: Threat detection for collaborative adaptive cruise control in connected cars. In: Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks, pp. 184–189 (2018).

15. Jeong, T., Njonjo, A., Pan, B.: A study on the performance comparison of three optimal alpha-beta-gamma filters and alpha-beta-gamma-eta filter for a high dynamic target. TransNav Int. J. Mar. Navig. Sat. Sea Transp. (2017). https://doi.org/10.12716/1001.11.01.05

16. Kapoor, P., Vora, A., Kang, K.-D.: Detecting and mitigating spoofing attack against an automotive radar. In: 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), pp. 1–6. IEEE (2018).

17. Komissarov, R., Kozlov, V., Filonov, D., Ginzburg, P.: Partially coherent radar units range resolution from bandwidth limitations. Nat. Commun. 10(1), 1–9 (2019).

18. Kudarauskas, N.: Analysis of emergency braking of a vehicle. Transport 22(3), 154–159 (2007).

19. Lazaro, A., Porcel, A., Lazaro, M., Villarino, R., Girbau, D.: Spoofing attacks on FMCW radars with low-cost backscatter tags. Sensors 22(6), 2145–2166 (2022).

20. Lin, J.-J., Li, Y.-F., Hsu, W.-C., Lee, T.-S.: Design of an FMCW radar baseband signal processing system for automotive application. Springerplus 5(1), 42 (2016).

21. Liu, J., Park, J.-M.: Seeing is not always believing: detecting perception error attacks against autonomous vehicles. IEEE Trans. Dependable Secure Comput. 18(5), 2209–2223 (2021).

22. Lutz, S., Ellenrieder, D., Walter, T., Weigel, R.: On fast chirp modulations and compressed sensing for automotive radar applications. In: 2014 15th International Radar Symposium (IRS), pp. 1–6. IEEE (2014).

23. Mitomo, T., Ono, N., Hoshino, H., Yoshihara, Y., Watanabe, O., Seto, I.: A 77 GHz 90 nm CMOS transceiver for FMCW radar applications. IEEE J. Solid State Circuits 45(4), 928–937 (2010).

24. Miura, N., Machida, T., Matsuda, K., Nagata, M., Nashimoto, S., Suzuki, D.: 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, pp. 95–100 (2019).

25. Moon, T., Park, J., Kim, S.: BlueFMCW: random frequency hopping radar for mitigation of interference and spoofing. EURASIP J. Adv. Signal Process. 2022(1), 1–17 (2022).

26. Nallabolu, P., Li, C.: A frequency-domain spoofing attack on FMCW radars and its mitigation technique based on a hybrid-chirp waveform. IEEE Trans. Microw. Theory Tech. 69(11), 5086–5098 (2021).

27. Nashimoto, S., Suzuki, D., Miura, N., Machida, T., Matsuda, K., Nagata, M.: Low-cost distance-spoofing attack on FMCW radar and its feasibility study on countermeasure. J. Cryptogr. Eng. (2021). https://doi.org/10.1007/s13389-020-00252-5

28. Navarro, A.: General properties of alpha beta, and alpha beta gamma tracking filters. NASA STI/Recon Technical Report N 77:24347 (1977).

29. Nuand bladeRF; U.S.: USB. 3.0 software defined radio manual (2016).

30. Quinonez, R., Giraldo, J., Salazar, L., Bauman, E., Cardenas, A., Lin, Z.: SAVIOR: securing autonomous vehicles with robust physical invariants. In: 29th USENIX Security Symposium (USENIX Security 20), pp. 895–912 (2020).

31. Quinonez, R., Safaoui, S., Summers, T., Thuraisingham, B., Cardenas, A.A.: Shared reality: detecting stealthy attacks against autonomous vehicles. In: Proceedings of the 2th Workshop on CPS & IoT Security and Privacy, pp. 15–26 (2021).

32. Ranganathan, A., Danev, B., Francillon, A., Capkun, S.: Physical-layer attacks on chipir-based ranging systems. In: Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, pp. 15–26 (2012).

33. Song, D., Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Tramer, F., Prakash, A., Kohno, T.: Physical adversarial examples for object detectors. In: 12th USENIX Workshop on Offensive Technologies (WOOT’18) (2018).

34. Stove, A.G.: Linear FMCW radar techniques. In: IEE Proceedings F (Radar and Signal Processing), vol. 139, no. 5, pp. 343–350 (1992).

35. Sun, Z., Balakrishnan, S., Su, L., Bhuyan, A., Wang, P., Qiao, C.: Who is in control? Practical physical layer attack and defense for mmWave based sensing in autonomous vehicles. arXiv preprint arXiv:2011.10947 (2020).

36. Tang, T., Wu, C., Elangage, J.: A signal processing algorithm of two-phase staggered PRI and slow time signal integration for MFI triangular FMCW multi-target tracking radars. Sensors 21(7), 2296 (2021).

37. Thing, V.L., Wu, J.: Autonomous vehicle security: a taxonomy of attacks and defences. In: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing ( CPSCom) and IEEE Smart Data (SmartData), pp. 164–170. IEEE (2016).

38. Tong, Z., Renter, R., Fujimoto, M.: Fast chirp FMCW radar in automotive applications. In: IET International Radar Conference 2015, pp. 1–4. IET (2015).

39. Wang, Z., Wu, Y., Niu, Q.: Multi-sensor fusion in automated driving: a survey. IEEE Access 8, 2847–2868 (2019).

40. Welch, G., Bishop, G.: An introduction to the Kalman filter. Technical report, Chapel Hill, NC, USA (1995). https://perso.crans.org/~welch/robot.html

41. Winkler, V.: Range Doppler detection for automotive FMCW radars. In: 2007 European Radar Conference, pp. 166–169. IEEE (2007).
42. Yan, C., Xu, W., Liu, J.: Can you trust autonomous vehicles: contactless attacks against sensors of self-driving vehicle. DEF CON 24(8), 109 (2016)
43. Ziebinski, A., Cupek, R., Erdogan, H., Waechter, S.: A survey of ADAS technologies for the future perspective of sensor fusion. In: International Conference on Computational Collective Intelligence, pp. 135–146. Springer (2016)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.