A Frequency-Domain Spoofing Attack on FMCW Radars and Its Mitigation Technique Based on a Hybrid-Chirp Waveform

Prateek Nallabolu, *Student Member, IEEE*, and Changzhi Li, *Senior Member, IEEE*

***Abstract*— This article presents a novel spoofing device capable of injecting false target information into a frequency-modulated continuous-wave (FMCW) radar. The spoofing device uses a radio frequency (RF) single-sideband (SSB) mixer to introduce a frequency shift to the incoming RF signal transmitted by the victim radar and retransmits the modulated RF signal. The modulated RF signal resembles a false target. Upon down-conversion on the receiver chain of the victim radar, the modulated RF signal creates an illusion of a real target in the radar signal processing system. The frequency shift can be adjusted to vary the range of the spoofed target. The theory of the spoofing mechanism was developed, and a 5.8 GHz prototype was built for experimental validation. Experimental results demonstrate the ability of the proposed spoofing device to inject a false target at any arbitrary range. A hybrid-chirp FMCW approach was proposed and verified as a countermeasure to distinguish a real target from a spoofed target to mitigate the RF-spoofing attack.**

***Index Terms*— Autonomous vehicle (AV), frequency-modulated continuous-wave (FMCW) radar, millimeter-wave radar, radar countermeasures, spoofing, vehicle safety.**

I. Introduction

AUTONOMOUS vehicle (AV) [1]–[3] related research has gained compelling interest in the last two decades due to the significant advancement in sensor technologies such as cameras [4], [5], ultrasonic sensors [6], LiDAR [7], [8], and millimeter-wave radars [9]–[13]. Sensor fusion has helped to avail the advantages of various sensor technologies concurrently to achieve real-time 360° sensing around the vehicle. The emergence of internet of things (IoT) has enabled the concept of connected vehicles, wherein an AV can communicate with nearby AVs, surrounding road infrastructure, and the internet to create an internet of vehicles (IoV) framework [14], [15]. However, the recent fatal accidents involving cars in autopilot mode have raised serious concerns about the reliability of the sensors employed in self-driving cars [16], [17]. Resources have been directed to improve these sensors' reliability, investigate the possible malicious attacks on AV sensors, and develop defense mechanisms to counter these kinds of attacks.

Intentional attacks on AVs can be broadly classified into attacks on sensors, Vehicular *Ad hoc* Network (VANET) attacks, and electronic control unit (ECU) firmware attacks [18]–[27]. Camera-based sensors are used to visualize the surroundings, identify vehicles, pedestrians, and traffic signs and lights. These sensors can be deceived by blinding them with bright light, wherein a laser or light-emitting diode (LED) is focused on the sensor [28]–[30]. LiDARs provide range information of the targets and are used for collision avoidance and pedestrian detection. Attacks against LiDARs have been demonstrated by relaying back the signal transmitted by the LiDAR from different positions with added delay to create fake echoes [30]–[32]. Ultrasonic sensors operate in the frequency range of 40–50 kHz and are used primarily in parking assist systems. In [33], jamming and spoofing attacks were carried out on a commercial ultrasonic sensor.

Millimeter-wave radars operating in frequency-modulated continuous-wave (FMCW) mode have been employed extensively in AVs due to their ability to determine the targets' range and velocity and work in harsh climate conditions. These radars are used for blind-spot detection, collision avoidance, pedestrian detection, and adaptive cruise control (ACC). Due to their widespread use, special emphasis was laid on investigating the various attacks on automotive radars and identifying solutions to detect these attacks. Jamming and spoofing are the most common threats to automotive radars. In a jamming attack, the attacker intentionally sends out high-energy radio frequency (RF) signals within the bandwidth of the victim radar, saturating its receiver chain, thereby interfering with the victim radar's target detection capability. Jamming of an automotive radar was demonstrated in [28], where the radar could not detect a car present in front of it. In [34], the impact of several jamming techniques like repeater jamming, Gaussian pulse jamming, and tone jamming on FMCW radars was studied using MATLAB simulations and a lab-volt radar training system (LVRTS).

Spoofing is defined as the injection of false target information into a sensor system. Unlike a jamming attack which is easy to identify because the radar cannot detect any targets, a spoofing attack is difficult to identify and mitigate due to the legitimacy of the induced fake targets. FMCW radar spoofing attacks and detection mechanisms were mostly confined to

Manuscript received August 13, 2021; accepted September 20, 2021. Date of publication October 7, 2021; date of current version November 4, 2021. This work was supported by the National Science Foundation (NSF) under Grant ECCS-1808613 and Grant ECCS-2028863. *(Corresponding author: Prateek Nallabolu.)*

The authors are with the Department of Electrical and Computer Engineering, Texas Tech University, Lubbock, TX 79409 USA (e-mail: prateek-reddy.nallabolu@ttu.edu; changzhi.li@ttu.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TMTT.2021.3115804.

Digital Object Identifier 10.1109/TMTT.2021.3115804

concept discussion, and simulations were presented in some previous works [35]–[38]. The spoofing attacks were only discussed in theory, and no experimental results were presented. Digital RF memory (DRFM) technique was presented in [38], where high-speed analog-to-digital converters (ADCs) and digital memory were used to sample RF signals and store them. The stored RF signals were retransmitted using different time delays to deceive the victim's radar. However, the DRFM method suffers from a large memory requirement to store the RF signal. In [39], the author(s) presented a spoofing attack model on FMCW radars, where the attacker uses a microwave absorber to absorb the signal transmitted by the victim radar and determines the precise time when the signal was transmitted. The attacker later sends a time-advanced version of a similar signal to mimic a target at a closer range. This model works on the assumption that the attacker sends an ensemble of spurious signals first and waits for the victim's radar to transmit a signal. In real-time, the automotive radar might be transmitting signals all the time, and it would be difficult to precisely predict the time at which the signal was transmitted. Moreover, the attacker needs to achieve nanosecond-level time synchronization with the victim radar's signal transmission, which is quite challenging to accomplish. A half-chirp modulation scheme was proposed in [40], wherein precise time synchronization with the chirp signal transmitted by the victim radar was attained using a spoofing system that requires a replica of the victim radar. However, the experimental results were obtained in an indoor environment using a wired connection to introduce the signal propagation delay. Further, the results presented were based on triangular FMCW waveforms, which are steadily replaced using so-called fast chirps (sawtooth waveforms) in the modern state-of-the-art automotive FMCW radars. Software-defined radio (SDR) based adversarial radars that can manipulate the range and velocity of the spoofed targets were presented in [41] and [42]. The experimental results presented in [41] did not mimic a practical scenario. Instead, the victim radar and the attack radar were connected using long cables to resemble a true target. Although AV stalling, hard braking, and forced lane change attacks were demonstrated in [42] on a 60 GHz state-of-the-art radar, the proposed approach also suffers from the need to identify the precise signal transmission time of the victim radar down to the nanosecond level.

Most of the existing work related to FMCW radar spoofing demonstrating some degrees of experimental validation rely on relaying a time-delayed or time-advanced version of the victim radar's chirp signal to mimic an actual target using a spoofing setup that requires an identical version of the victim radar. Relaying the chirp signal would initially require precise time synchronization with the victim radar and expensive circuitry to introduce nanosecond-level time delays to the relayed chirp signals.

In this work, an RF mixer-based FMCW radar spoofing system is presented. Unlike previous works that rely on introducing nanosecond-level time delays to the FMCW chirp signal or requiring an identical chirp generating circuit in the spoofing setup, the proposed attack model uses an RF mixer to add a frequency shift to the chirp signal transmitted by the victim radar and retransmits it back toward the radar. Moreover, the proposed approach does not require precise time synchronization with the victim radar. The frequency shift added to the chirp signal can be altered to change the range of the spoofed target. The spoofing system can also generate target distances less than the actual distance between the victim radar and the spoofing device, with certain limitations. A hybrid-chirp FMCW radar is proposed to identify a spoofed target to mitigate threats from the proposed attack model. In the hybrid-chirp FMCW radar, alternating chirps with nonidentical slopes are transmitted and their resulting range plots are compared to distinguish a real target from a spoofed target. A 5.8 GHz benchtop prototype of the spoofing setup is designed and implemented to validate the proposed concept experimentally. To the best of the authors' knowledge, the work presented in this article is the first of its kind to design an FMCW radar spoofing device based on a single-sideband (SSB) mixer and other RF components, and experimentally demonstrate its working in an outdoor environment.

The article is organized as follows. Section II presents the basic working principle of an FMCW radar and the proposed spoofing attack model theory. The details of the benchtop design of the 5.8 GHz spoofing device prototype are presented in Section III. The simulation and experimental results are presented in Section IV. The proposed hybrid-chirp method, which acts as a countermeasure to the proposed spoofing model is presented in Section V. Conclusions are drawn in Section VI.

II. Theory

Fig. 1 represents a high-level illustration of the proposed spoofing attack model. An FMCW radar transmits a chirp signal characterized by the center frequency f_c, bandwidth B, and chirp duration T. The mathematical expression for the transmitted chirp signal can be represented as

$$S_{\mathrm{Tx}}(t) = \exp\left(j\left(2\pi f_c t + \pi \gamma t^2 + \varphi\right)\right) \tag{1}$$

where $t \in [-T/2,\ T/2]$ is called the fast-time, $\gamma = B/T$ represents the slope of the chirp signal, and φ is the initial phase. Signal processing along the fast-time data provides the range information of the target. Ideally, an automotive FMCW radar transmits a sequence of chirps defined as a frame. The range evolution of a target across consecutive chirps in a frame constitutes the slow-time data, which carries the Doppler information of the target. The signal received by the radar upon reflection from a target at a distance R is a time-delayed version of the transmitted chirp given by

$$S_{\mathrm{Rx}}(t) = \sigma S_{\mathrm{Tx}}(t - \tau(R)). \tag{2}$$

In (2), $\tau(R) = 2R/c$ corresponds to the round-trip signal propagation delay, where c is the speed of light in air, and σ represents the amplitude of the signal. A de-chirping operation is performed on the receiver side, where a part of the transmitted signal is mixed with the received signal to obtain a low-frequency baseband signal that contains the range

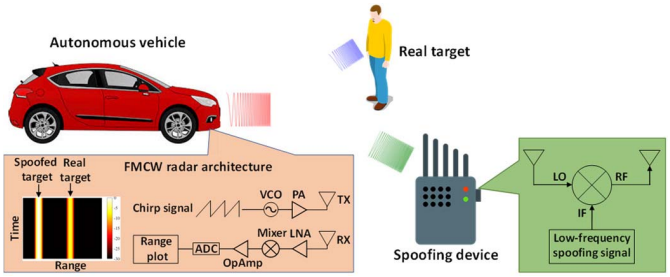

Fig. 1. Illustration of the proposed spoofing attack model on an FMCW radar using an RF mixer.

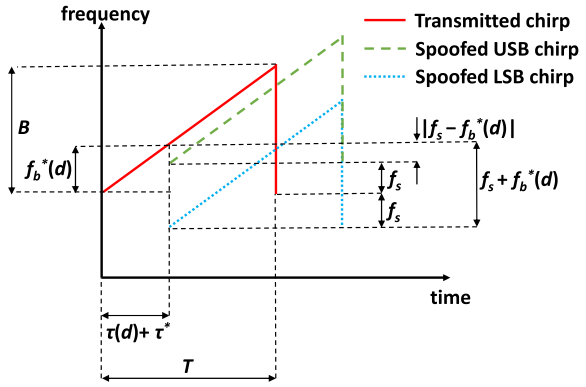

Fig. 2. Time-frequency representation of the chirp transmitted by the victim FMCW radar along with the LSB/USB spoofed chirp signals generated by the spoofing device.

information of the target. The real part of the baseband signal obtained is given by

$$s_b(t) = \mathrm{Re}\left[S_{\mathrm{Tx}}(t)S'_{\mathrm{Rx}}(t)\right] = \sigma \sin\left(\frac{4\pi\gamma Rt}{c} + \frac{4\pi f_c R}{c}\right) \quad (3)$$

where Re[.] denotes the real part of the complex number, and ´denotes the complex conjugate operation. The frequency of the baseband signal generated by a target at a distance R is known as the beat frequency and can be calculated as

$$f_b(R) = \frac{2\gamma R}{c}. \quad (4)$$

From (3), it can be observed that the frequency of the baseband signal carries the range information of a real target. A false target can be spoofed if the chirp signal received by the victim radar is altered such that the de-chirped baseband signal contains the frequency corresponding to the range of the false target. The proposed spoofing device uses an SSB up-conversion mixer to mix the FMCW chirp signal with a low-frequency spoofing signal, resulting in a frequency shift in the chirp signal. This frequency shift is reflected in the victim radar's baseband signal and creates the semblance of a real target. Assuming that the instantaneous distance d between the radar and the spoofing device is known, the spoofing frequency can be calculated accordingly to spoof a target at any arbitrary range. The instantaneous distance d will be referred to as the nominal distance hereon.

The nominal distance between the radar and the spoofing device generates a nominal beat frequency $f_b(d)$ on the receiver side of the radar. The frequency shift introduced by the SSB mixer creates a positive or negative offset to the nominal beat frequency, which gets reflected in the baseband signal obtained after the de-chirping process. The SSB mixer can be configured to output either the upper sideband (USB) or the lower sideband (LSB), which determines the impact of the frequency shift on the nominal beat frequency.

The signal received by the victim radar when the SSB mixer is configured to output the LSB is represented as

$$S_{\mathrm{Rx\_LSB}}(t) = \sigma^* \exp\Big[j\Big(2\pi(f_c - f_s)\big(t - \tau(d) - \tau^*\big) + \pi\gamma\big(t - \tau(d) - \tau^*\big)^2\Big) - \varphi_s\Big] \quad (5)$$

where σ^* is the amplitude of the spoofed chirp, f_s is the spoofing frequency, φ_s represents the initial phase of the spoofing signal when mixed with the RF chirp signal, and τ^* is the additional signal propagation delay through the spoofing setup. This delay adds a positive shift to the nominal beat frequency, represented as $f_b^*(d)$ and referred to as the fundamental beat frequency from now on. The corresponding spoofed beat frequency and the baseband signal generated can be given as

$$f_{\mathrm{spoof\_LSB}} = f_b^*(d) + f_s = f_b(d) + \frac{B\tau^*}{T} + f_s \quad (6)$$

$$s_{\mathrm{spoof\_LSB}}(t) = \sigma^* \sin\left(2\pi f_{\mathrm{spoof\_LSB}} t + \frac{4\pi f_c d}{c} - \varphi_s\right) \quad (7)$$

where $B\tau^*/T$ represents the frequency offset due to the delay τ^*. The phase of the spoofed baseband signal is the resultant of the phase shift the chirp signal undergoes due to the round trip traveling time and the initial phase of the spoofing signal. The effect of φ_s on the slow-time data is discussed later in the article. When the mixer is set to output the LSB, the spoofing device effectively produces a spoofed target at a range greater than the nominal distance. The spoofed range can be calculated as

$$R_{\mathrm{spoof\_LSB}} = \frac{c f_{\mathrm{spoof\_LSB}}}{2\gamma}. \quad (8)$$

Fig. 2 shows the spoofed LSB chirp (blue curve), which undergoes a time delay and positive frequency shift compared to the transmitted chirp (red curve). This causes the spoofed beat frequency to be higher when compared to the nominal beat frequency, mimicking a target at a farther range. The maximum range that can be spoofed depends on the sampling frequency of the ADC used in the receiver chain of the radar.

When the SSB mixer of the spoofing device is set to output the USB, the signal received by the victim radar, the spoofed beat frequency, and the spoofed baseband signal can be mathematically expressed as

$$S_{\mathrm{Rx\_USB}}(t) = \sigma^* \exp\Big[j\Big(2\pi(f_c + f_s)\big(t - \tau(d) - \tau^*\big) + \pi\gamma\big(t - \tau(d) - \tau^*\big)^2\Big) + \varphi_s\Big] \quad (9)$$

$$f_{\mathrm{spoof\_USB}} = \left|f_b^*(d) - f_s\right| \quad (10)$$

$$s_{\text{spoof\_USB}}(t) = \sigma^* \sin\left(2\pi f_{\text{spoof\_USB}} t + \frac{4\pi f_c d}{c} + \varphi_s\right). \quad (11)$$

By choosing the USB output, false targets with a range less than the nominal distance can be spoofed. The spoofed USB chirp (green curve) can be seen in Fig. 2. As the spoofing frequency increases, the spoofed beat frequency decreases, resembling a target closer to the radar. If the spoofing frequency is greater than twice the fundamental beat frequency, the spoofed targets appear at a range greater than d. When the mixer is configured to output the USB tone, targets at a range greater and smaller than the nominal distance can be spoofed, depending on the spoofing frequency. It should be noted that f_s is the frequency of the low-frequency spoofing signal introduced at the intermediate frequency (IF) port of the SSB mixer while $f_{\text{spoof\_LSB}}$ and $f_{\text{spoof\_USB}}$ represent the beat frequencies generated as a result of the spoofing device when the mixer is configured to output the LSB and USB tones, respectively.

Theoretically, the lowest range that can be spoofed depends on the chirp duration T. The chirp duration limits the lowest baseband signal frequency detected on the receiver end of the radar. Ideally, the beat frequency should be greater than the chirp on period, which is calculated as the inverse of the chirp duration. The minimum frequency shift added to the RF chirp signal also depends on the chirp duration. To successfully spoof a target, the spoofing frequency f_s should be greater than the chirp on period.

III. Spoofing Device Design and Prototype

A new approach using a passive SSB RF mixer is investigated to design an FMCW spoofing device without relying on delay line circuits with nanosecond precision. Fig. 3(a) depicts the schematic of the proposed spoofing setup. The spoofing device is designed to operate in the 5.6–6.2 GHz frequency range. A 4 × 4 patch antenna fabricated on an FR-4 substrate acts as the receiving antenna. The received FMCW chirp signal is sent to a low-noise amplifier (LNA) used as the first amplification stage. Due to the free space path loss, the RF signal traveling from the radar to the spoofing device undergoes significant attenuation. The LNA module (Pasternack PE15A1010) is used to provide a 40 dB gain to the incoming FMCW chirp signal. An additional gain block (Analog Devices HMC788A) module is used to further amplify the output signal from the LNA to meet the local oscillator (LO) drive requirement of the SSB mixer. The output of the gain block is provided to the LO input of a single sideband mixer module (Analog Devices HMC525ALC4). The mixer requires an LO drive of 15 dBm. The 40 dB LNA cascaded with the gain block is used to achieve the required LO drive.

The amplified chirp signal is fed to the LO port of the mixer, and a low-frequency sinusoidal spoofing signal that introduces the frequency shift to the chirp signal is fed to the IF port of the mixer. The mixer requires both in-phase/quadrature (I/Q) channels of the low-frequency spoofing signal to generate a single sideband at the RF port of the mixer. Ideally, an RF 90° hybrid would be used to generate the I/Q channels. Since

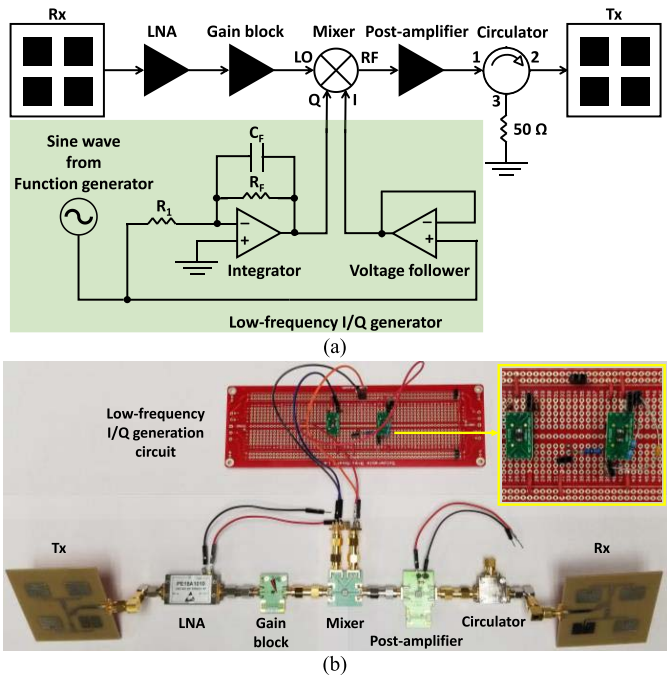

Fig. 3. (a) Schematic of the proposed spoofing device. (b) 5.8 GHz benchtop prototype of the spoofing device.

the signals fed to the IF port are in the kHz or MHz range, a 90° hybrid is not practically feasible. Therefore, an integrator circuit designed using an operational amplifier (op-amp) is used to generate the I/Q channels. The schematic of the integrator circuit is shown in Fig. 3(a). The feedback capacitor C_F is chosen such that the integrator circuit provides unity gain at the frequency corresponding to the spoofing signal. The output of the integrator provides the Q-channel output, while a voltage follower circuit (unity gain buffer) implemented using a similar op-amp (Texas Instruments TLV9001) generates the I-channel output. For the prototype, the resistors R_1 and R_F were chosen to be 100 KΩ and 1 MΩ, respectively. The input to the integrator circuit and the voltage follower is provided using a function generator (Instek GFG-8210) capable of generating sinusoidal output from 0.1 Hz to 10 MHz. The low-frequency I/Q generation circuit is implemented on a solderable breadboard. For further reference in the article, the low-frequency signal fed to the IF ports of the mixer will be referred to as the spoofing signal and the RF signal output at the RF port of the mixer will be described as the LSB/USB spoofed chirp.

The spoofed FMCW chirp at the RF port of the mixer is then fed to a postamplifier which provides additional gain to compensate for the conversion loss of the mixer. The postamplifier is realized using the HMC392ALC4 module from Analog Devices. The output of the postamplifier is connected to a circulator (RF-Lambda RFLC-402-3), which allows signal flow only from the gain block to the transmitting antenna. The circulator is used to suppress any signal received by the transmitting antenna to reach the RF port of the mixer. Since the mixer used in the setup can act as both an up-converter and down-converter, any signal at the RF port would likely affect the I/Q generation circuit connected to

TABLE I
KEY COMPONENTS USED IN THE SPOOFING DEVICE PROTOTYPE

Component	Part	Manufacturer	Key parameters
LNA	PE15A1010	Pasternack	Gain: 40 dB Input P1dB: -26dBm
Gain block	HMC788A	Analog Devices	Gain: 14 dB Input P1dB: 7 dBm
Mixer	HMC525ALC4	Analog Devices	LO drive: 15 dBm Conversion loss: 8 dB
Post-amplifier	HMC392ALC4	Analog Devices	Gain: 17 dB Input P1dB: 3 dBm
Circulator	RFLC-402-3	RF-Lambda	Isolation: 19 dB

the IF ports of the mixer. The circulator can be omitted if the postamplifier has a very good reverse isolation (S_{12}). However, the postamplifier is optional and is used to increase the signal strength when the spoofing device is placed far away from the radar. The transmitting antenna is realized using a similar 4 × 4 patch antenna. Fig. 3(b) shows the picture of the benchtop spoofing device prototype. The major components of the spoofing device prototype are listed in Table I.

IV. SPOOFING ATTACK RESULTS

A. Simulation Results

To initially verify the effectiveness of the proposed spoofing attack model, simulations were carried out in MATLAB software. The simulation model was replicated to mimic a realistic scenario. In the simulation model, the FMCW radar generated a chirp signal from 1 to 300 MHz with a chirp duration of 2 ms. To decrease the computational load, the chirp frequency was considered in the MHz range. The SSB up-conversion mixer was realized by upshifting/downshifting the chirp signal with the frequency of the spoofing signal. To emulate the signal propagation delay between the radar and the spoofing device, an equivalent number of zeros corresponding to the required time delay was added to the end of the chirp signal data array and at the beginning of the spoofed chirp signal data array. The de-chirping operation equivalent to a mixer down-conversion process was achieved by multiplying the chirp signal and the spoofed chirp signal. Finally, a fast Fourier transform (FFT) was applied to the baseband signal to obtain the beat frequency.

The distance between the radar and the spoofing device was assumed to be 1.5 m, corresponding to a nominal beat frequency of 1.5 kHz. The frequency offset added due to the additional signal propagation delay through the spoofing setup was ignored for these simulations, thereby corresponding to a fundamental beat frequency of 1.5 kHz. The FMCW chirp was downshifted to mimic the LSB spoofed chirp. The spoofed chirp was downshifted by various frequencies to demonstrate the effect of the spoofing signal on the generated beat frequency, as shown in Fig. 4(a). The spoofed baseband signals had higher beat frequencies, reciprocating a spoofed target at a range greater than 1.5 m. Similarly, the FMCW chirp was upshifted to simulate the USB spoofed chirp. From Fig. 4(b), it can be observed that a false target with a range

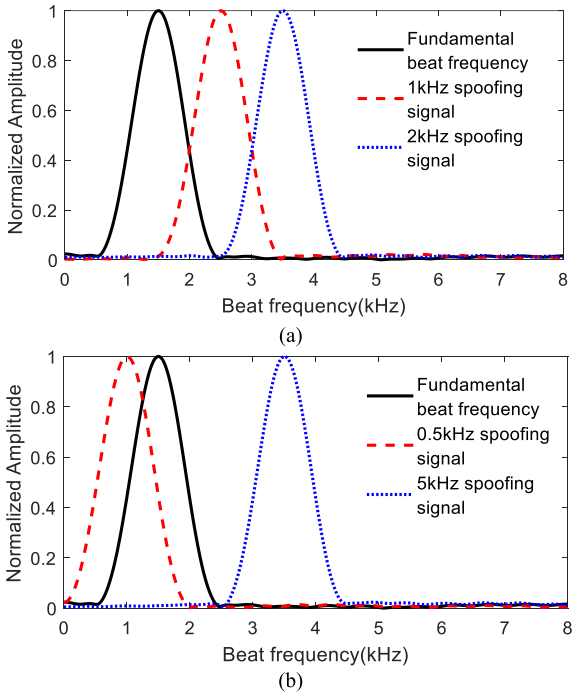

Fig. 4. MATLAB simulation results of the spoofing attack model showing the resultant spoofed beat frequency for varying spoofing signals when the mixer in the spoofing device is configured to output (a) LSB (b) USB.

less than 1.5 m would be created for spoofing frequencies less than 3 kHz. When the spoofing frequency was 5 kHz, which was higher than 2 × 1.5 kHz, the spoofed beat frequency was greater than 1.5 kHz, confirming the theory presented in Section II.

To study the effect of the nonlinearities of the spoofing device components on the spectral peak width of the spoofed target, a system-level simulation was performed using AWR Visual System Simulator (VSS) software. The spoofing device prototype and the 5.8 GHz FMCW radar used for experimental validation were modeled in VSS, as shown in Fig. 5(a). To identify the effect of nonlinearities introduced by the spoofing device, the RF chirp spectrum of a spoofed target and true point-like target was compared at the receiver port of the radar. The bandwidth and chirp duration for the FMCW radar were set to 50 MHz and 5 μs, respectively. For the true target, the simulation setup shown in Fig. 5(a) was simplified by removing the spoofing device components. The propagation delay and the path loss were adjusted to represent a target at 20 m. The radar cross-section (RCS) of the point-like true target was considered to be 1 m^2. For the spoofed target, the nominal distance between the radar and the spoofing device was set to 4 m. To mimic a target at 20 m, the SSB mixer was configured to output the LSB tone, and the frequency of the spoofing signal was set to 1.067 MHz. Fig. 5(b) shows the power spectral density of the received RF chirp for the true target and the spoofed target. The half-power bandwidth (HPBW) was measured as 48 MHz for both the true and spoofed target, indicating that the nonlinearities of the spoofed device do not cause significant spectral widening of the spoofed chirp. It can be observed from Fig. 5(b) that the spectrum of the spoofed chirp was offset by 1 MHz compared

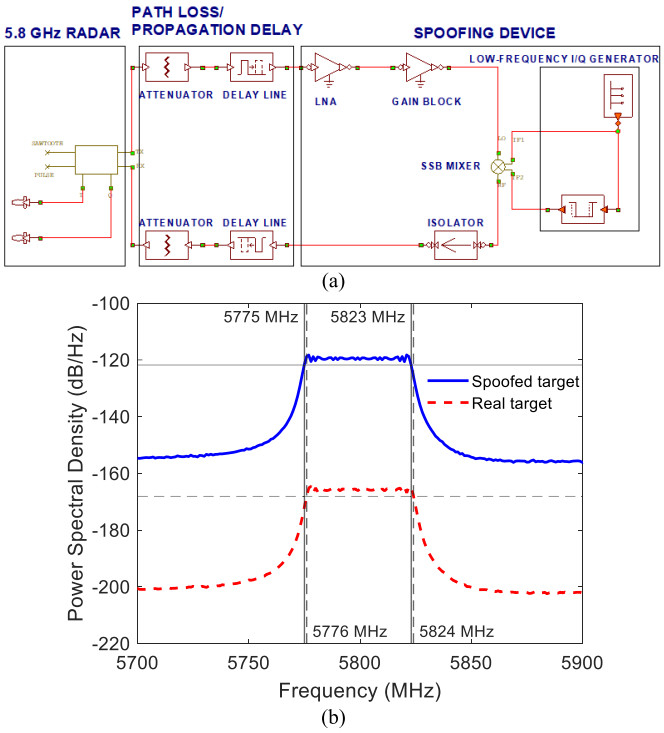

Fig. 5. (a) System-level simulation setup of the proposed spoofing device in AWR VSS software. (b) Comparison of the RF chirp spectrum of a true target and a spoofed target at the received end of the radar.

to that of the true target, which follows the theory presented in Section II. It should be noted that the only signal source in the spoofing device was the function generator that provides the spoofing signal. Since the phase noise of the function generator as well the spoofing device components was not provided by the respective manufacturers, the above simulation does not reflect the effect of any additional phase noise added by the spoofing device.

B. Experimental Results

Experiments were performed using the above-mentioned spoofing device prototype and an in-house designed FMCW radar that operates from 5.6 to 6.2 GHz frequency. The radar shown in the inset in Fig. 6(a) has an onboard sawtooth waveform generator that controls the voltage-controlled oscillator (VCO) to generate the FMCW chirp signal. The shape of the sawtooth waveform can be varied to generate chirps with different time duration and bandwidth within the frequency range. An ac-coupled baseband amplifier is used to amplify the generated baseband signal, which is then transferred to a personal computer (PC) using the audio jack port and processed using MATLAB.

In the first scenario, the spoofing device was placed 1.35 m away from the radar, as shown in Fig. 6(a). To avoid saturation on the radar receiver chain, the postamplifier used in the spoofing device prototype was removed. A 10 dB attenuator was inserted before the 40 dB LNA to make sure that the P1dB input requirement of the LNA was met. The radar was configured to output a chirp signal with a bandwidth of 350 MHz and a time duration of 3 ms. Prior to the spoofing experiments, data

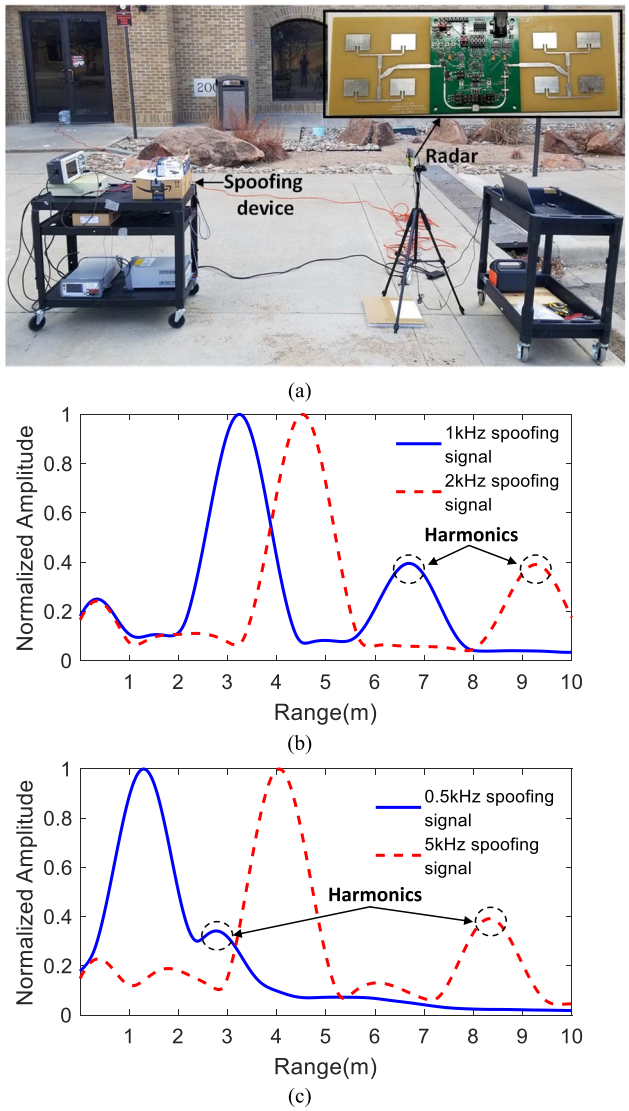

Fig. 6. (a) Experiment setup to demonstrate FMCW radar spoofing. Range plots demonstrating the ability of the spoofing device to mimic targets, when the mixer is configured to output, (b) LSB spoofed chirp, and (c) USB spoofed chirp.

were recorded with a corner reflector placed at 1.35 m. The nominal beat frequency was measured to be 1 kHz. Initially, the mixer in the spoofing device was configured to output the LSB spoofed chirp. A 1 kHz ($C_F = 1.5$ nF) signal was provided by the function generator to the low-frequency I/Q generation circuit. The resultant beat frequency on the receiver side of the radar was 2.5 kHz, resulting in a spoofed target at 3.28 m. With a nominal beat frequency of 1 kHz and spoofing frequency of 1 kHz, the resultant beat frequency should have been 2 kHz. The additional 500 Hz of frequency offset was introduced due to the signal propagation delay through the spoofing device itself. Similarly, a spoofing signal of 2 kHz ($C_F = 820$ pF) generated a false target at 4.58 m, as shown in Fig. 6(b).

To spoof a target at a distance less than 1.35 m, the mixer was configured to output the USB spoofed chirp. As shown in Fig. 6(c), a spoofing frequency of 500 Hz ($C_F = 3$ nF) resembles a spoofed target at 1.2 m. When the spoofing

frequency was 5 kHz ($C_F = 0.3$ nF), which was greater than 3 kHz (2×1 kHz), the resultant spoofed target appeared at a range of 4 m (greater than 1.35 m), proving that targets both closer and farther than the nominal distance can be spoofed when the mixer is set to output the USB spoofed chirp. The results presented above showcase the ability of the proposed spoofing system to induce fake targets at any arbitrary range by varying the frequency of the spoofing signal introduced at the IF ports of the mixer. Fig. 6(b) and (c) shows that harmonics of the spoofed targets were also present. This was caused due to the FMCW radar alone and can be avoided when state-of-the-art commercial FMCW radars are used.

While spoofing state-of-the-art radars operating in the 24 or 77 GHz band, a one-time calibration can be performed to estimate the signal propagation delay through the spoofing device. Once the beat frequency corresponding to the propagation delay is calculated based on the chirp parameters of the victim radar, the frequency of the spoofing signal at the IF ports of the mixer can be adjusted accordingly to generate a spoofed target at the intended range. The frequency range of the spoofing signal depends on the chirp parameters of the victim radar. The 5.8 GHz radar used in the experimental demonstration transmits chirps with a time duration in the millisecond range. The corresponding beat frequency generated by a true target varies from hundreds of Hz to tens of kHz. Therefore, the spoofing frequency is chosen in the Hz/kHz range. For the so-called fast chirps employed in automotive radars, the chirp duration is configured in microseconds, thereby generating beat frequencies in the order of one-tenths to tens of MHz. Consequently, the spoofing frequency can be chosen accordingly to generate realistic spoofed targets.

In the second scenario, the radar was mounted on a tripod and mechanically rotated to perform 2-D scanning of the experimental space. For the experiment setup, a more complex target space was considered, with a human subject seated at 2.7 m and 30°, a corner reflector placed at 3 m and 150°, and the spoofing device positioned at 4 m and 90°, as shown in Fig. 7(a). The chirp parameters were set to 300 MHz and 4 ms. The radar was mechanically rotated from 0° to 180° in steps of 10°. The sawtooth generation circuit on the radar board was bypassed, and the control signal to the VCO was provided using an arbitrary waveform generator (AWG) Teledyne T3AFG120. The AWG was used because it offers more flexibility in controlling the slope and duration of the sawtooth waveform. A 1 kHz spoofing signal was given to the IF ports of the mixer outputting the LSB spoofed chirp, resulting in a spoofed target at 7 m. Fig. 7(b) and (c) showcase the obtained 2-D maps without and with the spoofing device.

In Fig. 7(c), the signature of the cart is not visible. This is because the 2-D range map in Fig. 7(c) represents the normalized baseband signal strength of the targets. The cart being a hollow structure based on plastic material has a relatively low RCS, thus generating a baseband signal with low signal strength. Since the baseband signal strength generated by the spoofed target is very high compared to the cart, the normalized signal strength of the baseband generated by the reflections from the cart is below -40 dB, and hence its signature is not seen in the 2-D map. Since the cart is only

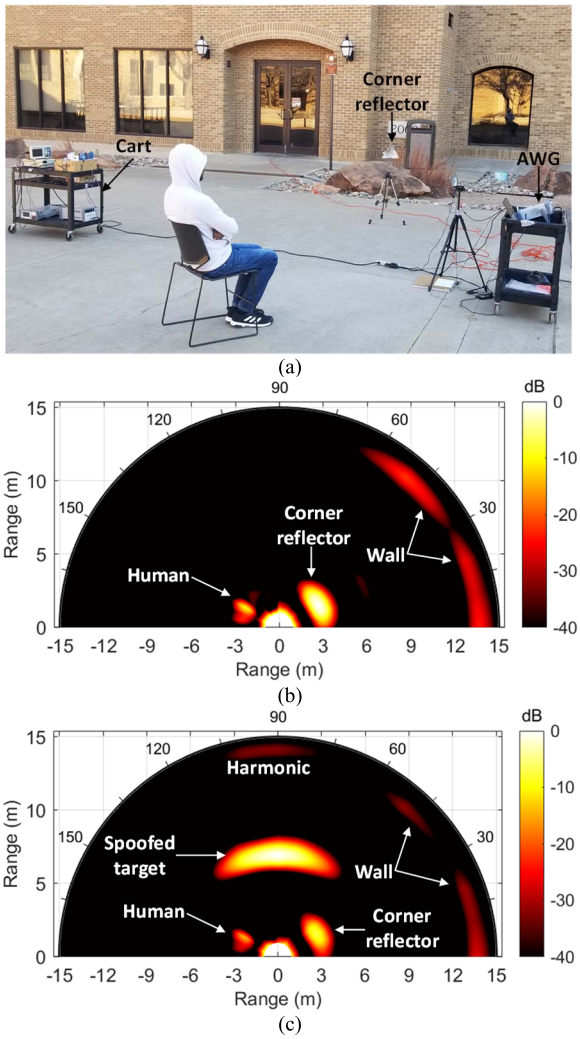

Fig. 7. (a) Experiment setup for the 2-D scanning scenario. The obtained 2-D map (b) without the spoofing device and (c) with the spoofing device.

a supporting structure to hold the spoofing setup, microwave absorbers can be attached to the cart to further minimize any reflections from it. For the result shown in Fig. 7(b), the cart carrying the spoofing device was removed from the experiment setup.

Furthermore, the ability of the spoofing device to make the victim radar unable to detect a real target in its vicinity is also demonstrated. This method is called target blinding. The retransmitted spoofed RF signal from the spoofing device overpowers the signal reflected by a real target, thereby making the radar blind to the real target. In a jamming attack [28], the radar is completely blinded to any target in front of it, making it easier to identify that the radar is under attack. With target blinding, the radar still detects a target signature due to the spoofing system, making it very difficult to realize that the radar is under attack. Fig. 8(a) shows the experimental setup for the target blinding demonstration. Here, the spoofing device was placed 4 m and 90° away from the radar, and a human subject was seated at 2.2 m and 135° in front of the radar. The spoofing device was configured to create a spoofed target signature at 2.2 m. The postamplifier connected at the RF port of the mixer amplified the spoofed RF chirp. The

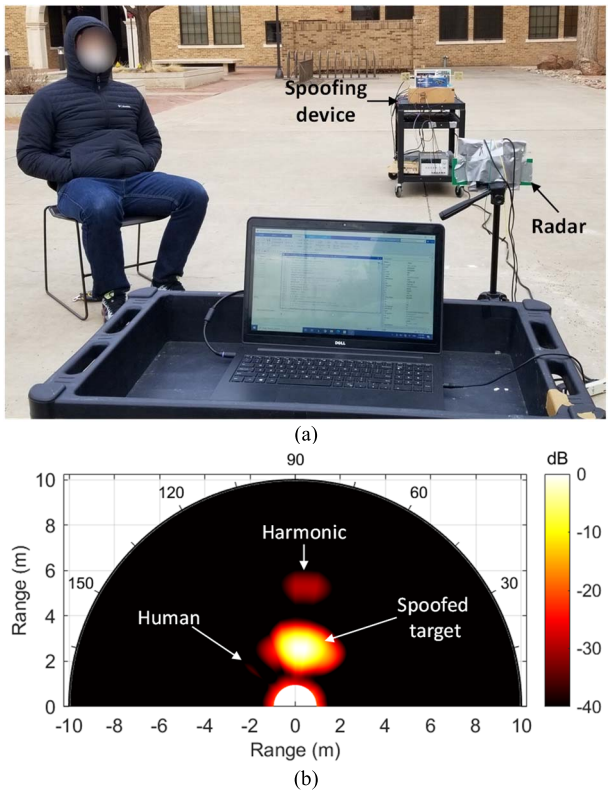

Fig. 8. (a) Experiment setup for target blinding demonstration. (b) Obtained 2-D map showing a powerful signature from the spoofed target overwhelming the reflections from the human subject.

radar was again mechanically rotated to perform 2-D scanning of the environment. The obtained 2-D map shown in Fig. 8(b) indicates that the strong signal from the spoofing device completely overwhelmed the reflections from the human subject, which was seated closer to the radar compared to the spoofing device.

From Figs. 7(a) and 8(a), it can be observed that the signature of the spoofed target is more spread out compared to the signatures of the true targets, i.e., human subject and the corner reflector. This is due to the relatively higher signal strength of the RF spoofed signal at the receiver end of the victim radar when compared to the reflections from the true targets. The RF chirp signal transmitted by the radar undergoes free space path loss before reaching the spoofing device, which is then amplified to 15 dBm to meet the LO drive requirement of the SSB mixer. For the current spoofing device, the SSB mixer has a conversion loss of 7.5 dB and the spoofing signal fed to its IF port has a power of 7 dBm, thus generating an RF spoofed chirp with a power level of -0.5 dBm. The retransmitted RF spoofed chirp undergoes free space path loss before reaching the victim radar. For a nominal distance of 4 m, the free space path loss is 43.75 dB at 5.8 GHz, and hence the signal strength of the spoofed chirp at the receiver end of the radar is -44.25 dBm. For a true target, the chirp signal transmitted by the radar gets reflected off its surface and undergoes attenuation due to the free space path loss. The received signal strength can be estimated using the radar range equation. For the case of a human subject (RCS $=$ 1 m^2) at 2.7 m, the received signal strength is -54 dBm. Similarly, for the corner reflector (RCS $=$ 3.67 m^2) at 3 m, the received signal strength is -48.25 dBm. Compared with the spoofed chirp, the received signal strength of the reflections from the human subject and corner reflector is lower by 10 and 4 dB, respectively. Due to this difference in the signal strength, the signature of the spoofed target spans across a wider range compared to that of the true targets.

C. Discussions

Since a free-running function generator generated the low-frequency spoofing signal, the spoofing device introduces a frequency offset along the slow-time data due to the phase incoherence of the spoofing signal, i.e., the spoofing signal has a varying initial phase when it is mixed with consecutive chirps in a frame. The impact of the spoofing signal phase is shown in Fig. 9. For a real stationary target, the FFT along the slow-time should yield a peak at 0 Hz. When the spoofing device in this work generated a spoofed target, the FFT along the slow-time has a peak at the Doppler frequency corresponding to the frequency offset introduced. The value of the frequency offset depends on the frequency of the spoofing signal and the chirp repetition rate CRR. Mathematically, the frequency offset f_o can be calculated as

$$f_o = m \times \text{CRR} - f_s, \quad m \in I \tag{12}$$

where m is an integer chosen such that f_o lies within CRR/2. When the spoofing frequency is a multiple of the chirp repetition rate, the frequency offset is zero. To demonstrate the effect of the frequency offset on the range-Doppler data, experiments were performed with the setup shown in Fig. 10(a). The radar was attached to a cart and moved manually, while the spoofing device remained stationary. This setup mimics a real-time scenario where the automotive radar is installed on a moving vehicle. The FMCW parameters of the radar were set to a bandwidth of 350 MHz and a chirp repetition rate of 250 Hz. A 10 dB attenuator was placed before the 40 dB LNA, and the postamplifier was removed from the spoofing device. The radar was moved from 2.4 to 1.4 m at a speed of 0.3 m/s. The motion of the radar should ideally generate a Doppler frequency around 11 Hz. In the first case, the spoofing frequency was set to 500 Hz, which is a multiple of the chirp repetition rate and should not generate any frequency offset. From Fig. 10(b), it can be observed that the Doppler frequency was close to 11 Hz. In the second case, the spoofing frequency was set to 700 Hz, generating an offset of 50 Hz. It is evident from Fig. 10(c) that the Doppler frequency was shifted by 50 Hz. In both cases, the mixer was configured to output the LSB spoofed chirp. In the case of the state-of-the-art automotive radars where the chirp repetition time is composed of chirp on time and chirp off time, the chirp repetition rate can be calculated as the inverse of the overall chirp repetition time.

To accurately spoof a target at a specific range, the proposed spoofing attack model works under the assumption that the distance d between the victim radar and the spoofing device, and the transmitted FMCW chirp parameters are known to the attacker. To measure the distance d, a radar operating in a

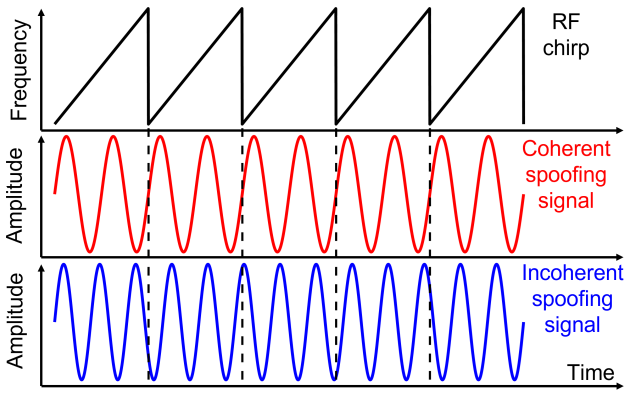

Fig. 9. Phase incoherence of the low-frequency spoofing signal across multiple chirps in a frame.

different frequency band can be used to avoid interference with the spoofing device. Alternatively, a LiDAR or other forms of distance measurement sensor can also be used. The inaccuracy in the estimation of the distance d directly affects the range of the induced spoofed target. Due to the inaccuracy, the false target will be generated with a slight offset from the intended range. Since the phenomenon of spoofing is studied as a threat to AVs, the inaccuracy in the measurement of distance d should not be a major concern. An alternate scenario that can be considered is where the spoofing device is placed at a fixed location on the roadside or a parking lot. The spoofing device can be configured such that any vehicle at a distance d from the spoofing device suffers from a near-range false target detected in its signal processing system. However, it should also be noted that without prior information of the distance d, a spoofed target at a random range can still be generated with the knowledge of the victim radar's chirp parameters. The chirp parameters are required to estimate the frequency range (kHz or MHz) of the spoofing signal. Recent works have demonstrated over-the-air (OTA) chirp synchronization methods, wherein the chirp parameters of an FMCW signal can be measured remotely [43], [44].

The maximum distance between the spoofing device and the victim radar is limited by factors such as average output power of the chirp transmitted by the victim radar, the total gain of the two amplification stages used in the spoofing device, and the LO drive level of the SSB mixer. The employed 5.8 GHz radar transmits a chirp with an average power of 6 dBm while the total gain provided by the two amplification stages is 52 dB and the LO drive of the mixer is 15 dBm. Before the experiments, the power level at the input of the 40 dB LNA was measured at various distances from the radar. At 4 m, the power level was measured as -37 dBm. For a distance of 4 m, after the two-stage amplification, the power level at the LO port of the mixer would be 15 dBm. For distances greater than 4 m, the LO drive level would fall below 15 dBm. For demonstration purpose, the current spoofing setup is limited to a maximum distance of 4 m from the radar.

To increase the maximum operating distance between the victim radar and the proposed spoofing device, additional amplification stages and antennas with high directivity can be added in the spoofing setup. However, the number of additional gain stages that can be added is limited by the overall system's stability. A more viable solution is to use a lower number of gain stages realized using more efficient amplifiers with higher gain and better P1dB specification. Alternatively, the use of injection-locked oscillators (ILOs) can also be explored. Cascaded RF transceivers employed in large multiple-input multiple-output (MIMO) radars are increasingly using ILOs to achieve phase coherence across multiple transceivers due to their lower requirement on the power level of the injection signal. ILOs were able to achieve a frequency locking range of 300 MHz with a -10 dBm injection signal while power levels as low as -20 dBm can achieve a locking range of 85 MHz [45]. The use of an ILO for the spoofing device would significantly reduce the number of amplification stages required. Since the proposed spoofing model relies on estimating the victim radar's chirp parameter, an ILO can be used to initially generate a chirp signal in the same frequency band as the victim radar's chirp. Later, the received chirp signal transmitted by the victim radar can be moderately amplified and fed as the injection signal to the ILO, to achieve phase coherence, which is then fed to the LO port of the SSB mixer. An additional amplification stage providing a gain of 15 dB or an ILO designed for an injection signal power level of 0 dBm can be added to the current spoofing setup to increase the maximum nominal distance to 20 m. The lower the injection signal power level required by the ILO, the higher is the maximum nominal distance. Under this assumption, Fig. 11 demonstrates a MATLAB simulation of the spoofing frequency required to create a false target at 5 m, for varying distances between the radar and the spoofing device. The additional beat frequency due to the signal propagation delay through the spoofing setup is considered as 500 Hz and the mixer is configured to output the USB spoofed chirp.

Additionally, the proposed spoofing device was designed to operate in the linear region. Nonlinearities can be introduced when the power level at the input of the 40 dB LNA is very small or lies above a certain threshold, driving either of the amplifiers used in the spoofing device into saturation in the latter case. For the current spoofing setup, the power level at the input of the 40 dB LNA was adjusted to be -37 dBm to avoid saturating the amplifiers and providing 15 dBm power to the LO port of the SSB mixer. When the spoofing device is closer to the victim radar, attenuators were added to lower the power level to -37 dBm. In the first experimental scenario discussed in Section IV-B, the distance between the radar and the spoofing device was 1.3 m, and the power level measured at the input of the 40 dB LNA was -26 dBm. Therefore, a 10 dB attenuator was added before the LNA to adjust the power level close to -37 dBm. Moreover, the spoofing device was restricted to a maximum distance of 4 m from the radar because the power level at the input of the LNA falls below -37 dBm beyond this distance.Although the current spoofing system is designed to operate at a fixed power level of -37 dBm, using a power detector and a variable gain amplifier (VGA) can improve the dynamic range of the input power level for the linear operation of the spoofing device. Extension of this work would potentially include a spoofing device with the output of the power detector used to adjust

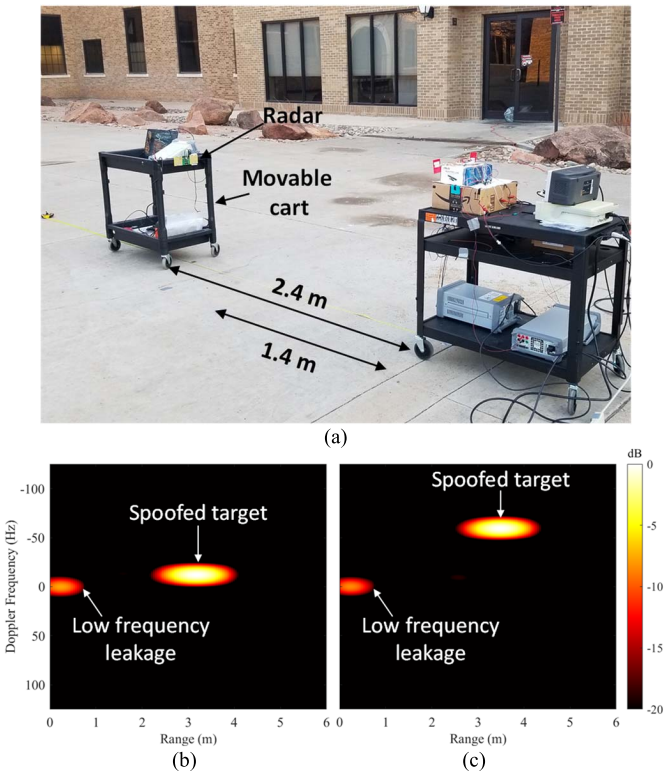

Fig. 10. (a) Experiment setup to demonstrate the effect of the frequency offset on the range-Doppler data. The obtained range-Doppler data for a spoofing frequency of (b) 500 and (c) 700 Hz.

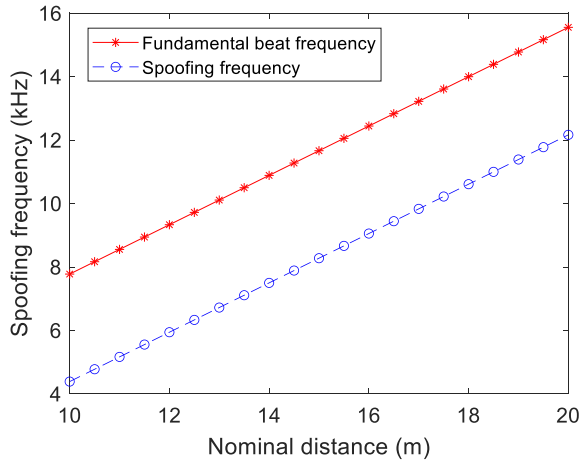

Fig. 11. Variation in the fundamental beat frequency and the spoofing frequency to generate a false target at 5 m with varying nominal distance between the victim radar and the spoofing device.

the gain of the VGA such that the optimal LO drive of the SSB mixer is achieved. Further, an ILO-based spoofing device that can operate at much lower input power levels will also be explored as a viable alternative to the VGA.

To study the impact of the additional phase noise on the spectral peak of the spoofed target, the peak width of the measured baseband spectral data for a true target (corner reflector) and the spoofed target was compared. As an estimate of the peak width, the HPBW was calculated. As shown in Fig. 12, the HPBW was measured as 0.48 and 0.52 kHz

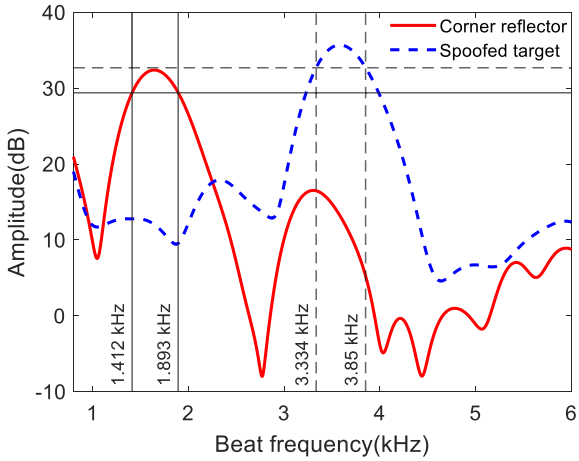

Fig. 12. Comparison of the spectral peak width of a true target (corner reflector) with a spoofed target.

for the corner reflector and spoofed target, respectively. The peak widths were off by 0.03 kHz, indicating that the impact of the additional phase noise due to the spoofing device was minimal.

Finally, the focus of this work was range spoofing using a simple hardware setup, without the need for precise nanosecond time synchronization with the victim radar. An extension of this work would address how to overcome the frequency offset issue and explore range-Doppler spoofing. Future work would also include implementing a spoofing system that can remotely determine the chirp parameters of the victim radar and control the phase of the spoofing signal to vary the Doppler frequency of the spoofed target.

V. Detecting a Spoofed Target

Since the spoofing attacks on automotive radars can have serious implications and prove fatal to human life, there is a need to provide countermeasures to defend against such attacks. The phase incoherence of the spoofing signal mentioned above causes the baseband signals generated across multiple chirps in a frame to have a different initial phase. Taking advantage of this, time-domain averaging can be performed on the baseband signals generated across multiple chirps, which eventually attenuates the baseband signal generated by a spoofed target while retaining the baseband signal generated by a real target. Fig. 13 shows the 2-D map after performing time-domain averaging on the same dataset used to obtain the result shown in Fig. 7(c). However, in some special cases, the spoofed baseband signals may have phase coherence, rendering the time-domain averaging method ineffective. In addition, the time-domain averaging technique also suppresses the signature of the true moving targets in the vicinity of the radar, rendering it ineffective in many practical scenarios.

Mitigation techniques based on random-chirp modulation were discussed in [39]–[42] and [46]. A sequence of random up- or down-chirps with identical bandwidth and chirp duration was proposed theoretically in [39]. Chirp sequences with random start frequency and phase were studied in [40]–[42].

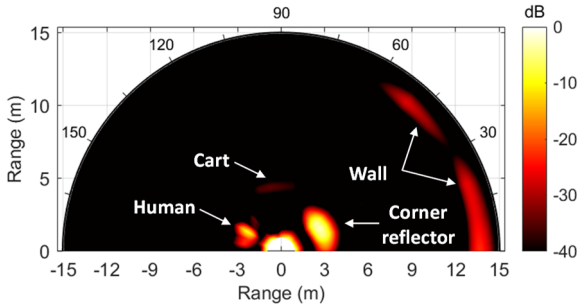

Fig. 13. Suppressing spoofed targets using the time-domain averaging method.

A frequency hopping technique referred to as BlueFMCW was proposed in [46], where the available FMCW bandwidth was divided into equal subintervals, and subchirps with equal slope and random start frequencies were transmitted to mitigate possible spoofing attacks on the radar. Conventional spoofing attacks which rely on transmitting time-delayed or time-advanced versions of the victim radar' chirp can be mitigated using the above-mentioned techniques because the attack radar cannot maintain synchronization with the changing victim radar's chirp signal. However, for two chirps with random start frequency or phase but having identical slopes, the proposed spoofing model can still generate a spoofed target at the same range using the same spoofing frequency.

To identify the fake targets generated using the proposed spoofing model, a hybrid-chirp FMCW radar is proposed where alternate chirps with nonidentical slopes are transmitted. Even though the change in slope leads to a different beat frequency for a real target, the resultant range of the target remains the same. However, for a spoofed target, the change in beat frequency would result in a shift of the spoofed range, assuming it takes time for a spoofing device to detect chirp parameters remotely. This range shift can be used as a measure to identify a spoofed target. Fig. 14(a) depicts a simple experiment of hybrid-chirp waveform with alternating chirps: chirp1 ($B = 300$ MHz; $T = 4$ ms) and chirp2 ($B = 450$ MHz; $T = 4$ ms), and the similar experimental setup shown in Fig. 7(a). The measured range of the spoofed target differs for every alternate chirp. The AWG was used to generate the sawtooth control signal for the hybrid-chirp waveform. Due to the difference in the chirp slope, the range bins for chirp1 and chirp2 correspond to different range values. While processing the baseband data, a calibration step was introduced to make the range bins of both the chirps identical. The calibration was achieved by choosing different numbers of FFT points for chirp1 and chirp2 data. In this case, the slopes of chirp1 and chirp2 were 7.5×10^{10} and 11.25×10^{10}, respectively. The number of FFT points for chirp1 and chirp2 was 6144 and 4096 [$6144 \times (7.5/11.25)$], respectively. Fig. 14(b) and (c) shows the obtained slow-time range map when the radar was pointing toward the spoofing device and corner reflector, respectively. The range of the spoofed target shifted from 6.8 m (chirp1) to 6 m (chirp2), whereas the range of the corner reflector remained constant for the two nonidentical chirps. Since the bandwidth of chirp1 is

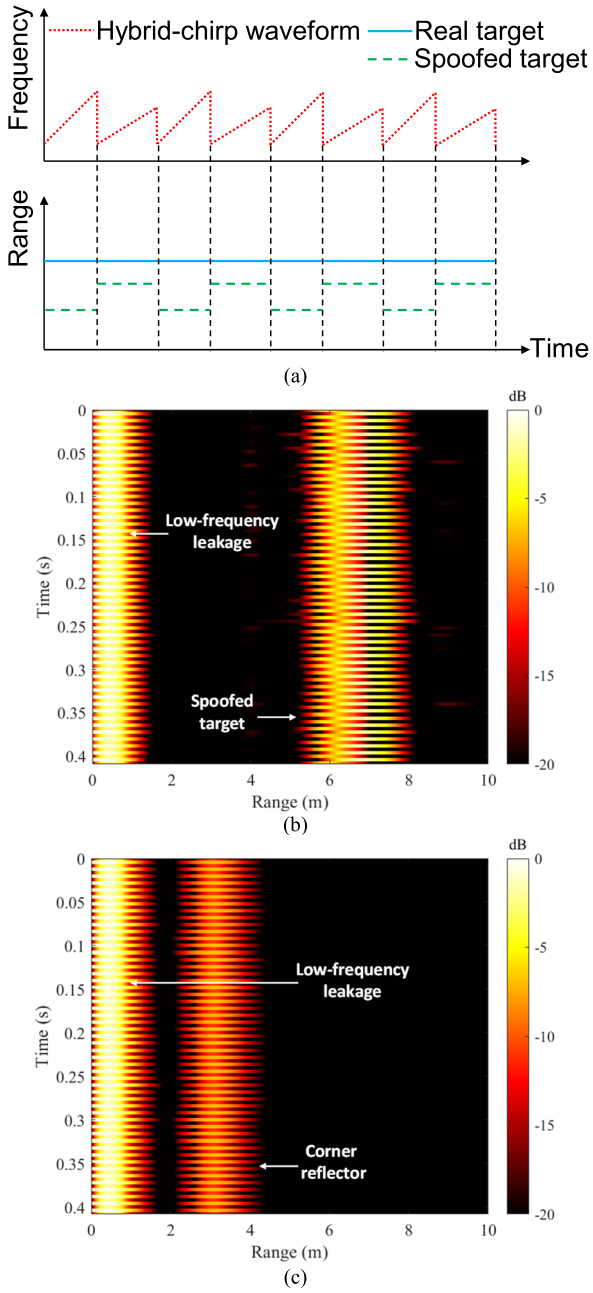

Fig. 14. (a) Illustration of the ability of the proposed hybrid-chirp waveform to distinguish a real target from a spoofed target. The slow-time range map of the (b) spoofed target and (c) corner reflector (real target), when the radar transmitted the hybrid-chirp waveform.

less than that of chirp2, the target is more spread out in the case of chirp1.

The range shift for the spoofed target depends on the nominal distance between the radar and the spoofing device. The nominal distance determines the fundamental beat frequency, which in turn determines the resultant spoofed beat frequency. For a given set of hybrid-chirp parameters, the smaller the nominal distance, the smaller is the range shift, and vice versa. Ideally, the slopes of the two chirps can be chosen such that the range shift for a spoofed target is very high. In such cases, the range data of chirp1 and chirp2 can be simply multiplied to suppress the signature of the spoofed target. In scenarios where

the FMCW radar offers less flexibility in varying its chirp parameters or the spoofing device is very close to the radar, correlation-related techniques may identify spoofed targets based on the range deviation introduced by the hybrid-chirp waveform. For a spoofed target, the correlation of chirp1 and chirp2 range data must have a peak at a nonzero range shift (equivalent to nonzero time lag), whereas the correlation peak must be at zero range shift for a real target. Machine learning-based target classification techniques may also be explored, where the classifier can be trained to identify the range shift patterns of the spoofed targets for different chirp slopes. In a more complex hybrid-chirp waveform, multiple chirps can have different slopes, and the occurrence of the chirps can be randomized.

VI. Conclusion

The threat to FMCW radar systems that are widely employed in AVs was studied using a unique RF-spoofing device. The proposed spoofing device introduces a frequency shift to the FMCW chirp signal using an RF mixer as the key component. The frequency shift results in the victim radar with a conventional FMCW design to detect a fake target. A 5.8 GHz benchtop prototype of the spoofing device was designed, and experiments were performed to demonstrate the ability of the system to inject false target information into the victim radar. The spoofing device can also carry out target blinding attacks, where the victim radar cannot detect real targets in its proximity. Similar spoofing concepts can be implemented at higher frequencies such as 24 and 77 GHz, which are the licensed bands for automotive radars. A hybrid-chirp waveform that acts as a countermeasure to the spoofing attack was proposed. The effectiveness of the hybrid-chirp waveform to identify a spoofed target was demonstrated experimentally. Future work related to the spoofing device hardware would be focused on designing a robust spoofing device capable of varying the power level of the spoofed target and integrating a subsystem to identify the chirp parameters of the victim radar remotely.

References

[1] I. Yaqoob, L. U. Khan, S. M. A. Kazmi, M. Imran, N. Guizani, and C. S. Hong, "Autonomous driving cars in smart cities: Recent advances, requirements, and challenges," *IEEE Netw.*, vol. 34, no. 1, pp. 174–181, Jan. 2020.

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

[3] S. Kuutti, S. Fallah, K. Katsaros, M. Dianati, F. Mccullough, and A. Mouzakitis, "A survey of the state-of-the-art localization techniques and their potentials for autonomous vehicle applications," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 829–846, Apr. 2018.

[4] J. Courbon, Y. Mezouar, and P. Martinet, "Autonomous navigation of vehicles from a visual memory using a generic camera model," *IEEE Trans. Intell. Transp. Syst.*, vol. 10, no. 3, pp. 392–402, Sep. 2009.

[5] L. Heng *et al.*, "Project AutoVision: Localization and 3D scene perception for an autonomous vehicle with a multi-camera system," in *Proc. Int. Conf. Robot. Automat.*, May 2019, pp. 4695–4702.

[6] L. Alonso, V. Milanés, C. Torre-Ferrero, J. Godoy, J. P. Oria, and T. De Pedro, "Ultrasonic sensors in urban traffic driving-aid systems," *Sensors*, vol. 11, no. 1, pp. 661–673, Jan. 2011.

[7] T. Ogawa, H. Sakai, Y. Suzuki, K. Takagi, and K. Morikawa, "Pedestrian detection and tracking using in-vehicle LiDAR for automotive application," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2011, pp. 734–739.

[8] R. Thakur, "Scanning LiDAR in advanced driver assistance systems and beyond: Building a road map for next-generation LiDAR technology," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 48–54, Jul. 2016.

[9] M. Steinhauer, H. Ruoss, H. Irion, and W. Menzel, "Millimeter-wave-radar sensor based on a transceiver array for automotive applications," *IEEE Trans. Microw. Theory Techn.*, vol. 56, no. 2, pp. 261–269, Feb. 2008.

[10] S. T. Nicolson *et al.*, "A low-voltage SiGe BiCMOS 77-GHz automotive radar chipset," *IEEE Trans. Microw. Theory Techn.*, vol. 56, no. 5, pp. 1092–1104, May 2008.

[11] 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 Trans. Microw. Theory Techn.*, vol. 60, no. 3, pp. 845–860, Mar. 2012.

[12] B.-H. Ku *et al.*, "A 77–81-GHz 16-element phased-array receiver with ±50° beam scanning for advanced automotive radars," *IEEE Trans. Microw. Theory Techn.*, vol. 62, no. 11, pp. 2823–2832, Nov. 2014.

[13] Y.-H. Hsiao *et al.*, "A 77-GHz 2T6R transceiver with injection-lock frequency sextupler using 65-nm CMOS for automotive radar system application," *IEEE Trans. Microw. Theory Techn.*, vol. 64, no. 10, pp. 3031–3048, Oct. 2016.

[14] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 241–246.

[15] K. M. Alam, M. Saini, and A. E. Saddik, "Toward social Internet of vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015.

[16] Team Tesla. (Jun. 2016). *A Tragic Loss*. [Online]. Available: https://www.tesla.com/blog/tragic-loss

[17] Team BBC. (Mar. 2018). *Tesla in Fatal California Crash was on Autopilot*. [Online]. Available: https://www.bbc.com/news/world-us-canada-43604440

[18] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 10–21, Feb. 2014.

[19] M. Dibaei *et al.*, "An overview of attacks and defences on intelligent connected vehicles," 2019, *arXiv:1907.07455*. [Online]. Available: http://arxiv.org/abs/1907.07455

[20] A. D. Kumar, K. N. R. Chebrolu, R. Vinayakumar, and K. P. Soman, "A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities," 2018, *arXiv:1810.04144*. [Online]. Available: http://arxiv.org/abs/1810.04144

[21] V. L. L. Thing and J. Wu, "Autonomous vehicle security: A taxonomy of attacks and defences," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Dec. 2016, pp. 164–170.

[22] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017.

[23] G. De La Torre, P. Rad, and K.-K.-R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Gener. Comput. Syst.*, vol. 108, pp. 1092–1111, Jul. 2020.

[24] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.

[25] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin, "The security of autonomous driving: Threats, defenses, and future directions," *Proc. IEEE*, vol. 108, no. 2, pp. 357–372, Feb. 2020.

[26] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, "Attacks on self-driving cars and their countermeasures: A survey," *IEEE Access*, vol. 8, pp. 207308–207342, 2020.

[27] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity attacks in vehicular sensors," *IEEE Sensors J.*, vol. 20, no. 22, pp. 13752–13767, Nov. 2020.

[28] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," in *Proc. DEF CON*, 2016, p. 109

[29] J. Zhang *et al.*, "Detecting and identifying optical signal attacks on autonomous driving systems," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 1140–1153, Jan. 2021.

[30] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," in *Proc. Black Hat Europe*, Nov. 2015, pp. 1–13.

[31] Y. Cao *et al.*, "Adversarial sensor attack on LiDAR-based perception in autonomous driving," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2019, pp. 2267–2281.

[32] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against LiDARs for automotive applications," in *Proc. Int. Conf. Cryptograph. Hardw. Embedded Syst. (CHES)*, Aug. 2017, pp. 445–467.

[33] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu, "Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5015–5029, Dec. 2018.

[34] H. R. Chen, "FMCW radar jamming techniques and analysis," M.S. thesis, Nav. Postgraduate School, Monterey, CA, USA, 2013.

[35] H.-L. Bloecher and J. Dickmann, "Automotive radar sensor interference–thread and probable countermeasures," in *Proc. 19th Int. Radar Symp. (IRS)*, Jun. 2018, pp. 1–7.

[36] P. Kapoor, A. Vora, and K.-D. Kang, "Detecting and mitigating spoofing attack against an automotive radar," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Chicago, IL, USA, Aug. 2018, pp. 1–6.

[37] A. Ranganathan, B. Danev, A. Francillon, and S. Capkun, "Physical-layer attacks on chirp-based ranging systems," in *Proc. 5th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WISEC)*, 2012, pp. 15–26.

[38] S. J. Roome, "Digital radio frequency memory," *Electron. Commun. Eng. J.*, vol. 2, no. 4, pp. 147–153, Aug. 1990.

[39] R. Chauhan, "A platform for false data injection in frequency modulated continuous wave radar," M.S. thesis, Dept. Elect. Comput. Eng., Utah State Univ., Logan, UT, USA, 2014.

[40] S. Nashimoto, D. Suziki, N. Miura, T. Machida, K. Matsuda, and M. Nagata, "Low-cost distance-spoofing attack on FMCW radar and its feasibility study on countermeasure," *J. Cryptograph. Eng.*, vol. 11, pp. 1–10, Jan. 2021.

[41] R. Komissarov and A. Wool, "Spoofing attacks against vehicular FMCW radar," 2021, *arXiv:2104.13318*. [Online]. Available: http://arxiv.org/abs/2104.13318

[42] 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," 2020, *arXiv:2011.10947*. [Online]. Available: http://arxiv.org/abs/2011.10947

[43] M. Gardill, J. Schwendner, and J. Fuchs, "*In-situ* time-frequency analysis of the 77 GHz bands using a commercial chirp-sequence automotive FMCW radar sensor," in *IEEE MTT-S Int. Microw. Symp. Dig.*, Boston, MA, USA, Jun. 2019, pp. 544–547.

[44] M. Gardill, J. Schwendner, and J. Fuchs, "An approach to over-the-air synchronization of commercial chirp-sequence automotive radar sensors," in *Proc. IEEE Topical Conf. Wireless Sensors Sensor Netw. (WiSNeT)*, San Antonio, TX, USA, Jan. 2020, pp. 46–49.

[45] A. Mushtaq, W. Winkler, and D. Kissinger, "A 79-GHz scalable FMCW MIMO automotive radar transceiver architecture with injection-locked synchronization," in *IEEE MTT-S Int. Microw. Symp. Dig.*, Jun. 2019, pp. 690–693.

[46] T. Moon, J. Park, and S. Kim, "BlueFMCW: Random frequency hopping radar for mitigation of interference and spoofing," 2020, *arXiv:2008.00624*. [Online]. Available: http://arxiv.org/abs/2008.00624

Prateek Nallabolu (Student Member, IEEE) received the B.Tech. degree in electronics and communications engineering from Jawaharlal Nehru Technological University, Hyderabad, India, in 2016, and the M.S. degree in electrical engineering from Texas Tech University, Lubbock, TX, USA, in 2018, where he is currently pursuing the Ph.D. degree.

His research interests include microwave circuits and systems, wireless RF sensors, and automotive radar security.

Mr. Nallabolu received the IEEE Microwave Theory and Techniques Society second place winner award in the 2021 High-Sensitivity Motion Radar student design competition.

Changzhi Li (Senior Member, IEEE) received the B.S. degree in electrical engineering from Zhejiang University, Hangzhou, China, in 2004, and the Ph.D. degree in electrical engineering from the University of Florida, Gainesville, FL, USA, in 2009.

He is currently a Professor at Texas Tech University, Hangzhou. His research interest is microwave/millimeter-wave sensing for healthcare, security, energy efficiency, structural monitoring, and human-machine interface.

Dr. Li was a recipient of the IEEE Microwave Theory and Techniques Society (MTT-S) Outstanding Young Engineer Award, the IEEE Sensors Council Early Career Technical Achievement Award, the ASEE Frederick Emmons Terman Award, the IEEE-HKN Outstanding Young Professional Award, the NSF Faculty Early CAREER Award, and the IEEE MTT-S Graduate Fellowship Award. He is an Associate Editor of the IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES and the IEEE JOURNAL OF ELECTROMAGNETICS, RF AND MICROWAVES IN MEDICINE AND BIOLOGY.