Emulation and Malicious Attacks to Doppler and FMCW Radars for Human Sensing Applications

Prateek Nallabolu, *Member, IEEE*, Daniel Rodriguez, *Member, IEEE*,
and Changzhi Li, *Senior Member, IEEE*

***Abstract*— This article presents emulation and adverse attack scenarios for Doppler radar-based motion sensors and frequency-modulated continuous-wave (FMCW) radars employed for noninvasive vital signs measurement and human presence sensing. In contrast to existing radar threat models, the proposed model is tuned to mimic two characteristics of a human target measured by radars, i.e., the motion artifacts generated by a walking human and the inherent chest motion. Electronically synthesizing the abovementioned characteristics can interfere with the normal operation of radar systems used for automation, bioauthentication, and surveillance applications. The attacking/emulation systems were realized using commercially available radio frequency (RF) components. The 5.8-GHz benchtop prototypes of the Doppler- and FMCW-mode systems were designed, and experiments were conducted to validate the threat of these systems. First, a single-sideband (SSB) mixer is utilized to electronically modulate the continuous-wave (CW) signal transmitted by a Doppler radar to resemble a walking human subject. Next, fake human targets are injected into an FMCW radar by using an analog phase shifter that mimics the vital sign motion of a real human subject. In addition to impersonating the human vital sign motion, the FMCW mode spoofing system has the capability to alter the range of the human target without requiring any synchronization with the victim radar. The FMCW mode spoofing system successfully deceived two state-of-the-art human detection algorithms. Finally, a brief discussion is presented on the feasibility of using the proposed Doppler and FMCW mode spoofing device architecture as respective radar target emulators.**

***Index Terms*— Doppler radar, frequency-modulated continuous-wave (FMCW) radar, human presence sensing, radar security, spoofing, vital sign detection.**

I. Introduction

RADAR technology had gained prominence among the military community during World War II (WWII), where they were primarily used to detect enemy aircraft. Over the last two decades, radars have made their way into civilian and commercial applications. With the rapid advancement in radio frequency integrated circuit (RFIC) technology, portable, low-cost, and energy-efficient radar sensors have found increasing applications in health care, automotive, and smart living sectors. Within the healthcare industry, radars have been employed for noncontact vital signs measurement, fall detection, sleep monitoring, and gait recognition, to name a few. With the emerging interest in autonomous driving, radars play a crucial role in realizing advanced driver assistance system (ADAS) functionalities, such as cross-traffic assist, blind-spot detection, and adaptive cruise control. In the growing Internet-of-Things (IoT) era, human–machine interaction is among the core aspects of smart home technology that can be accomplished using radars.

Accurate measurement of target parameters using simple circuitry, low transmit power, and relatively smaller form factor makes Doppler and FMCW radars the front runners for low-cost human sensing applications. Doppler radars measure the motion parameters (velocity and displacement) of a target by detecting the frequency or phase shift of the reflected signal. Due to their high sensitivity to measure motion, Doppler radars have been widely researched for vibration measurement [1], [2], [3], [4], vital signs monitoring [5], [6], [7], [8], [9], [10], [11], sleep apnea monitoring [12], [13], [14], disaster search and rescue operations [15], [16], gesture recognition [17], [18], gait analysis [19], [20], occupancy sensing [21], [22], [23], and motion sensing [24], [25], [26]. Commercially, motion sensors realized using Doppler radars have been extensively used in automatic door activation systems [27]. However, Doppler radars cannot directly measure the range of a target. Frequency-modulated continuous-wave (FMCW) radars provide the ability to measure a target's range while offering lower sensitivity in measuring the target's motion. FMCW radars have found applications in through-the-wall detection [28], [29], [30], [31], [32], [33], [34], [35], [36], human target identification [37], [38], [39], [40], [41], [42], [43], activity recognition [44], [45], [46], [47], and surveillance applications [48], [49], [50], [51]. Moreover, the identical design of both these radars allows for hybrid FMCW-Doppler mode of operation, thereby leveraging the unique advantages of each of the radar operating modes [37], [47].

Radar electronic countermeasures (ECMs) and electronic countercountermeasures (ECCM) have been prevalent military practices since WWII [52]. With millimeter-wave (mmWave) radars becoming ubiquitous in day-to-day applications, it is essential to study the possible ECM techniques against these radars. Since the working principle and the licensed frequency bands for the commercial use of Doppler and FMCW radars are available in the public domain, electronic systems devised

Manuscript received 21 May 2022; revised 8 August 2022; accepted 25 August 2022. Date of publication 29 September 2022; date of current version 7 February 2023. 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: prateekreddyn@gmail.com; daniel-fernando.rodriguez@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.2022.3208026.

Digital Object Identifier 10.1109/TMTT.2022.3208026

to intentionally disrupt the proper functioning of these radars are a significant threat that requires considerable research attention. Although the manufacturers do not reveal the chirp parameters (e.g., bandwidth and chirp duration) of commercial FMCW radars, previous works have shown the possibility of remotely identifying these parameters [53], [54]. Intentional attacks against radar sensors can be broadly classified into jamming and spoofing. Jamming is a technique, in which high-power noise within the operating frequency band is transmitted toward the radar to obstruct its normal operation. Jamming attacks are easy to identify as the radar system will not produce a meaningful output. However, spoofing attacks, wherein the radars' target detection model is deliberately mimicked, are more difficult to recognize due to the high similarity between the spoofed target and a real target. Existing literature on spoofing attacks against radars was mostly confined to automotive FMCW radars [55], [56], [57], [58], [59], [60], [61]. Previous works on FMCW radar spoofing are based on synchronized time-domain attack models, i.e., the attack system has to precisely estimate the time instance at which the victim radar transmits a chirp signal. Moreover, the attack systems require an active chirp waveform generating circuit, which is usually a replica of the victim radar. A passive spoofing attack model based on a backscattering tag was proposed in [62]. However, since the tag generates a double-sideband modulated signal, the spoofed targets appear as mirrored pairs around the range bin corresponding to the physical separation between the radar and the tag, which can be easily detected.

An asynchronous frequency-domain range spoofing model based on a single-sideband (SSB) mixer was presented in [63]. Due to the sideband and local oscillator (LO) suppression offered by the mixer, a single spoofed target can be generated at an arbitrary range bin when compared to the tag-based spoofing system in [62]. However, the frequency-domain spoofing system was limited to generate stationary targets. Although fake stationary targets are a significant threat to several radar-based ADAS functionalities, in the areas of human presence sensing and activity recognition, a stationary target is a less viable threat. Radar-based human presence sensing solutions filter out unwanted stationary targets (clutter) while retaining only the human signatures. Isolating human targets from surrounding clutter is generally based on detecting the inherent chest motion of humans. Therefore, a spoofing system able to create a fake human signature by electronically mimicking the human chest motion would be a more viable threat for these applications. To spoof a target moving with a specific velocity, the phase of the consecutive attack chirps must be varied accordingly. In the case of a stationary human, the peak-to-peak displacement of the inherent chest motion due to respiration is a couple of millimeters. Therefore, the phase change across consecutive chirps is very small (can be estimated based on the operating frequency of the radar and its chirp-to-chirp repetition time). Velocity (or Doppler) spoofing attacks against FMCW radars were demonstrated in [60] and [61]. Both these works used software-defined radio (SDR) as the attack system. The ability of those systems to mimic human chest motion depends on the minimum phase shift generated by the respective SDRs, which is determined by the resolution of the digital-to-analog (DAC) converters used in the transmit chain of the respective SDRs. However, the abovementioned SDR-based spoofing attack models require precise time synchronization with the victim radar and using an active chirp generating circuit as part of the attack system requires additional compensation for the frequency drift caused due to the different reference oscillators used on the attacker and the victim radar [60]. With regard to spoofing attacks against Doppler radars, vital signs spoofing using a binary phase shift keying (BPSK) tag and a phase shifter was demonstrated in [64]. However, using a phase shifter limits the proposed approach to small-amplitude motion spoofing.

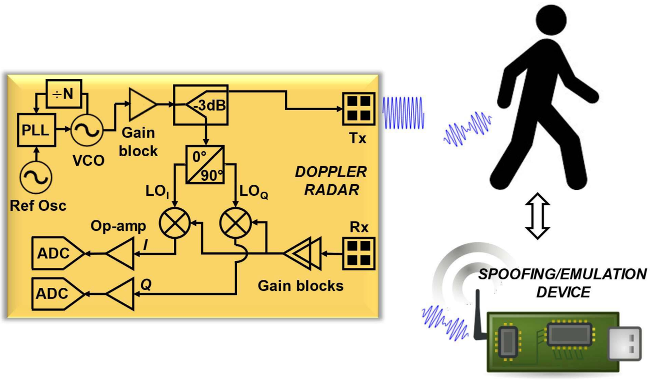


Fig. 1. Top-level representation of the proposed Doppler radar motion spoofing system.

Besides security considerations, radar target emulators (RTEs) have drawn significant interest in recent years. For the large-scale deployment of radars for various sensing applications in the IoT era, it is essential to thoroughly test the performance of the radar under a variety of background conditions. Furthermore, for radar-based human activity recognition integrated with machine learning, an extensive set of training data is required. However, this requires many human subjects, which can be difficult to accomplish. This fosters the need for a low-cost RTE that is tuned to emulate the response of different human activities against Doppler or FMCW radars. Existing radar target simulators in the market are expensive, bulky, and customized for automotive applications [65], [66]. A radar target simulator has been proposed by Nallabolu and Li [67] that can emulate micro-Doppler responses. However, it is restricted to Doppler radar and lacks a comprehensive description of the working of the target simulator.

This work demonstrates a common system architecture for testing (RTE) and analyzing vulnerabilities (spoofing attacks) of Doppler and FMCW radars employed for nonautomotive applications, focusing primarily on human activity sensing and localization. To emphasize the dual application nature of the proposed systems, they will be referred as emulation/spoofing systems hereon. The presented FMCW mode spoofing attacks are asynchronous, i.e., no time synchronization is required with the victim radar. The main contributions of this work include the following.

1) An upconversion SSB mixer-based Doppler radar emulation/spoofing system is proposed that can electronically mimic the motion pattern of a real human

target. The SSB mixer would frequency-modulate the continuous-wave (CW) radio frequency (RF) signal with the motion artifacts of a human subject. The resulting down-converted baseband signal on the receiver chain of the Doppler radar would resemble the motion of a real human subject.

2) An FMCW vital-Doppler emulation/spoofing system that can generate stationary synthetic human signatures at a fixed range is presented. To emulate or spoof the human vital signs signature into an FMCW radar, an analog phase shifter that can generate continuous phase shifts was used to vary the phase of consecutive chirp signals transmitted by the radar. The phase history along the slow-time data mirrored the human cardiopulmonary motion.
3) An FMCW range cum vital-Doppler emulation/spoofing system that can electronically alter the range of a stationary synthetic human is presented.

All the emulation/spoofing systems were realized at 5.8 GHz, and experiments were conducted to validate the proposed threat model. In addition, to the best of our knowledge, the work presented in this article is the first of its kind to conduct a risk assessment against FMCW radars used for human presence sensing while also demonstrating attack scenarios on Doppler radars employed for motion sensing. It also theoretically discusses the similarity between a spoofing system and an RTE's architecture.

The theory of the attack model against Doppler and FMCW radars is presented in Section II. The implemented 5.8-GHz prototypes of the Doppler and FMCW mode emulation/spoofing systems are discussed in Section III. Various experimental results obtained are included in Section IV. Finally, the conclusion is drawn in Section V.

II. Theory

A. Doppler Radar: Motion Emulation and Spoofing

A conventional Doppler radar transmits a CW electromagnetic signal at a fixed frequency f_t. Similar to the Doppler effect in sound waves, the return signal is modulated with the target's motion. The transmitted and received signal can be mathematically represented as

$$T(t) = \cos(2\pi f_t t) \quad (1)$$

$$R(t) = \cos(2\pi (f_t + f_D)t + \varphi) \quad (2)$$

respectively, where $f_D = 2v_m f_t/c$ is the Doppler frequency generated due to the instantaneous target velocity v_m, c is the speed of light, and φ is the total accumulated residual phase. In a quadrature direct-conversion receiver, the generated in-phase $[I(t)]$ and quadrature $[Q(t)]$ baseband signals can be represented as

$$I(t) = \cos(2\pi f_D t + \varphi) \quad (3a)$$

$$Q(t) = \sin(2\pi f_D t + \varphi). \quad (3b)$$

A short-time Fourier transform (STFT) is applied to the complex baseband data $I(t) + jQ(t)$ to observe the variation in motion frequency with time. The direction of the target movement, i.e., movement away or toward the radar, is preserved by the phase relationship between the I/Q channels. Given the motion information of a target, a spoofed response can be injected into the Doppler radar system by electronically modulating the transmitted waveform, as illustrated in Fig. 1. In the proposed Doppler mode spoofing system, an SSB upconversion mixer is used to mix the RF transmitted signal with a recorded or synthetic copy of the intermediate frequency (IF) spoofing signal that resembles the target motion. This modulation signal is recovered in the down-converted baseband data on the radar's receiver chain, creating the illusion of a real moving target. The SSB mixer can be configured to output either the lower sideband (LSB) or the upper sideband (USB) tone. Assuming that the mixer is configured to output the LSB tone, the output of the mixer can be represented as

$$\begin{aligned}\text{mixer}_{\text{LSB}} &= \cos(\omega_t t) \times \cos(\omega_{\text{spoof}} t) \\ &\quad + \sin(\omega_t t) \times \sin(\omega_{\text{spoof}} t) \\ &= \cos((\omega_t - \omega_{\text{spoof}})t) \end{aligned} \quad (4)$$

where $\omega_t = 2\pi f_t$, $\omega_{\text{spoof}} = 2\pi f_{\text{spoof}}$, and f_{spoof} represents the instantaneous frequency of the IF spoofing signal. On the radar end, the emulated/spoofed baseband I/Q data can be calculated as

$$\begin{aligned}I_{\text{spoof}}(t) &= \cos((\omega_t - \omega_{\text{spoof}})t) \times \cos(\omega_t t) \\ &= 0.5 \times \cos(\omega_{\text{spoof}} t) \end{aligned} \quad (5a)$$

$$\begin{aligned}Q_{\text{spoof}}(t) &= \cos((\omega_t - \omega_{\text{spoof}})t) \times \sin(\omega_t t) \\ &= 0.5 \times \sin(\omega_{\text{spoof}} t). \end{aligned} \quad (5b)$$

From (5a) and (5b), it is evident that the phase relationship between the I/Q channels of the IF spoofing signal fed to the mixer is translated to the I/Q baseband data generated by the radar. It is essential to maintain this phase relationship to accurately spoof the intended direction of the target motion.

Similarly, when the mixer is configured to output the USB tone, the output of the mixer and the generated emulated/spoofed I/Q data from the radar can be given as

$$\begin{aligned}\text{mixer}_{\text{USB}} &= \cos(\omega_t t) \times \sin(\omega_{\text{spoof}} t) \\ &\quad + \sin(\omega_t t) \times \cos(\omega_{\text{spoof}} t) \\ &= \sin((\omega_t + \omega_{\text{spoof}})t) \end{aligned} \quad (6)$$

$$\begin{aligned}I_{\text{spoof}}(t) &= \sin((\omega_t - \omega_{\text{spoof}})t) \times \cos(\omega_t t) \\ &= 0.5 \times \sin(\omega_{\text{spoof}} t) \end{aligned} \quad (7a)$$

$$\begin{aligned}Q_{\text{spoof}}(t) &= \sin((\omega_t - \omega_{\text{spoof}})t) \times \sin(\omega_t t) \\ &= 0.5 \times \cos(\omega_{\text{spoof}} t). \end{aligned} \quad (7b)$$

When the mixer outputs the USB tone, the phase relationship is not retained between the I/Q channels of the IF spoofing signal and the radar generated I/Q baseband data. This causes the direction of the spoofed target motion to be reversed. However, if the phase relation between the emulation/spoofing signals fed to the IF ports of the mixer is interchanged, i.e., I_{IF} and Q_{IF} are represented as sine and cosine, respectively, the USB tone will preserve the phase relationship on the radar's end. While the above analysis is limited to a single tone emulation/spoofing signal, complex motions such as a walking human can also be mimicked, where the emulation/spoofing

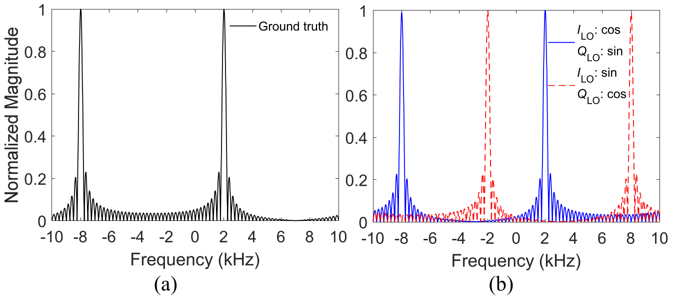


Fig. 2. Complex FFT of (a) I/Q spoofing signals applied to the IF ports of the mixer and (b) emulated/spoofed I/Q baseband data generated by the radar.

signal is a nonstationary signal with a time-varying phase relationship between the I/Q channels. It should be noted that the above analysis is based on the standard notation that the LO I-channel is represented as cosine and Q-channel as sine. The I/Q spoofing signals can be synthetically created, or a recorded target response from an identical radar system can be used. For the accurate generation of synthetic Doppler artifacts using the Doppler radar emulation/spoofing system, prior knowledge is required for the operating frequency of the radar. The operating frequency determines the Doppler frequency generated by a moving target that is required to generate the synthetic motion data fed to the IF ports of the mixer.

A MATLAB simulation was performed to visualize the effect of the LO I/Q channel configuration on the direction of the emulated/spoofed Doppler response for a two-tone spoofing signal. The characteristic of the target motion was assumed to be a summation of two sinusoids: a 2-kHz motion frequency with a positive Doppler response and an 8-kHz motion frequency with a negative Doppler response. The complex fast Fourier transform (FFT) response of the actual target motion is shown in Fig. 2(a). For the standard LO I/Q channel notation, i.e., I_{LO} is represented as cosine and Q_{LO} as sine, the solid blue curve in Fig. 2(b) shows the complex FFT of the obtained radar baseband data after emulation/spoofing. It can be verified that the direction of the electronically induced target motion is preserved in this case. However, when the LO I/Q channel notation is reversed, it is evident from the dotted red curve in Fig. 2(b) that the direction of the target motion is reversed, i.e., an emulated/fake target moving toward the radar appears as moving away and vice-versa.

B. FMCW Radar: Vital-Doppler Emulation/Spoofing

FMCW radars transmit a linearly increasing frequency-modulated waveform commonly referred to as a chirp signal. The received chirp signal reflected off a target is a time-delayed version of the transmitted chirp. The range of the target is precisely estimated by measuring the instantaneous frequency difference between the transmitted and received chirp signals, known as the beat frequency. The amplified received chirp and a copy of the transmitted chirp are fed to a mixer that generates the baseband signal, which is used for further processing. A 1-D FFT on the time-domain baseband signal provides the instantaneous range of the target. To measure the velocity of the target, an FMCW radar transmits a sequence of chirp signals known as a frame. The phase difference between consecutive received chirp signals is used to calculate the target's velocity. For targets exhibiting small-amplitude motion, the measured range of the target remains constant across successive chirp signals while the phase changes.

While measuring a phase-varying small-amplitude motion, the generated baseband signal $B(t)$ can be represented as

$$B(t)_n = \sin\left(\frac{4\pi\gamma d_0 t}{c} + \frac{4\pi f_c d[nT_c]}{c}\right) \tag{8}$$

where $n = 1, 2, \ldots, N$ represents the chirp index, t is the fast time index, d_0 is the nominal distance between the radar and the human subject, f_c is the center frequency of the chirp, T_c is the chirp duration, and γ is the slope of the chirp. $d[nT_c]$ represents the instantaneous distance of the target for the nth chirp's response. The phase history of the range bin d_0 is extracted after performing the 1-D FFT on each chirp's baseband response to recover the target motion. For small-amplitude motion, the baseband signal frequency remains the same across all the chirps, as evident from (8).

Vital sign measurement using FMCW radars falls under the category of small-amplitude motion detection. The human respiration and heartbeat frequency range is around 12–30 and 60–100 beats/min (bpm), respectively. The motion amplitude of respiration is much higher compared to the heartbeat. With the knowledge of these parameters, an analog phase shifter-based emulation/spoofing system is proposed to electronically alter the phase of the chirp signals transmitted by an FMCW radar, as depicted in Fig. 3. By characterizing the phase shifter's output response, a control waveform can be designed, such that the phase shifter's output mimics the human vital sign motion. The phase of the baseband signal for the nth emulated/spoofed chirp can be given as

$$\angle B_{\mathrm{spoof}}(t)_n = \frac{4\pi f_c \begin{pmatrix} d_0^* + a_R \sin[\omega_R n T_c] \\ + a_H \sin[\omega_H n T_c] \end{pmatrix}}{c} \tag{9}$$

where a_R, a_H, ω_R, and ω_H represent the amplitude and frequency of the emulated/spoofed respiration and heartbeat motion, respectively, $d_0^* = d_0 + d^*$, with d^* being the additional range offset generated due to the signal propagation delay through the emulation/spoofing device. A fake human target appears at the range bin d_0^*, and the extracted slow-time phase history reflects the emulated/spoofed cardiorespiratory frequencies. The proposed vital-Doppler emulation/spoofing model is asynchronous, i.e., there is no synchronization between the victim radars' chirp start time and the time instance, at which the vital sign emulation/spoofing control waveform is fed to the phase shifter. Moreover, this emulation/spoofing model does not require extensive information about the FMCW radar's chirp parameters. Limited information about the operating frequency is needed that can be obtained by using a wideband frequency scanning device. However, in this work, such a system is not devised, and the

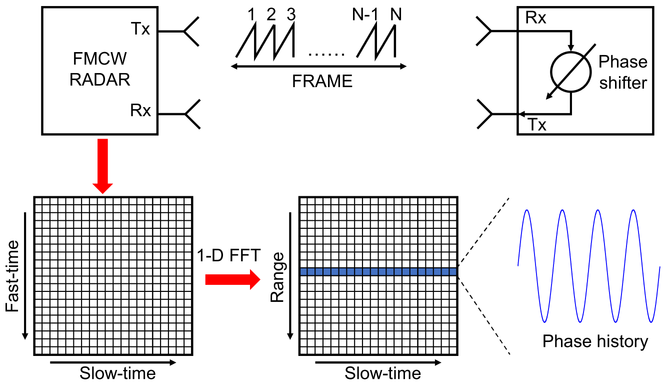


Fig. 3. Illustration of the data postprocessing to measure phase-induced motion using an FMCW radar.

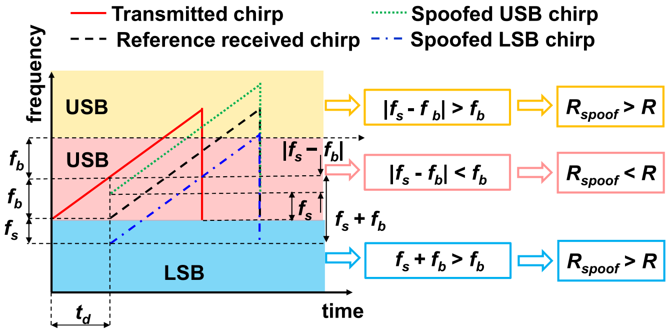


Fig. 4. Frequency versus time illustration of the modulated LSB and USB chirps retransmitted by the FMCW range cum vital-Doppler emulation/spoofing system.

attacker/user is assumed to have prior information about the radar's operating frequency.

C. FMCW Radar: Range Cum Vital-Doppler Emulation/Spoofing

With the phase shifter only FMCW spoofing system discussed above, a fake human target is synthesized at the range corresponding to the physical distance between the radar and the emulation/spoofing system. To alter the range of the synthesized human target, the physical distance needs to be changed. Nallabolu and Li [63] have presented a range spoofing system against FMCW radars that can create a false stationary target at any arbitrary range. Adding the phase shifter to the range spoofing system, the resultant range cum vital-Doppler emulation/spoofing system has the additional capability to electronically vary the range of the synthesized human target. In the proposed FMCW range cum vital-Doppler emulation/spoofing system, a human target can be synthesized at any arbitrary range, i.e., unlike relay attacks, synthetic human signatures closer than the physical separation between the radar and the attacker/emulator can also be generated. This can be achieved because the introduced range spoofing system adds a frequency shift to the incoming chirp signal. The frequency shift and the mixer's output configuration can be controlled to create a fake target at a closer range as well. Fig. 4 illustrates the effect of the mixer's output configuration on the resultant beat frequency measured by the radar.

In an FMCW radar, the time delay between the transmitted and the received waveform translates to the beat frequency after the dechirping process. When the emulation/spoofing device is placed at a distance d from the victim radar, the total time delay t_d is a summation of the round-trip traveling time of the chirp signal and the additional time required to travel through the device itself. Without considering the frequency shift introduced by the emulation/spoofing system, this time delay t_d is responsible for a beat frequency f_b on the radar's end, as shown in Fig. 4. Considering the frequency shift introduced by the emulation/spoofing device, the effective beat frequency as seen by the radar is $f_b + f_s$ and $|f_b - f_s|$ when the mixer is configured to output LSB and USB tones, respectively, as shown in Fig. 4. In the LSB mode, the effective beat frequency is greater than f_b, thereby creating a synthetic target at a distance greater than d. In the USB mode, depending on the frequency shift f_s, synthetic targets can be created at distances less than or greater than the distance d. The synthesized range R_{spoof} and phase φ_{spoof} can be given as

$$\begin{aligned} R_{\text{spoof}} &= \frac{c(f_b + f_s)}{2\gamma}, \quad \text{LSB mode} \\ &= \frac{c|f_b - f_s|}{2\gamma}, \quad \text{USB mode} \end{aligned} \tag{10}$$

$$\varphi_{\text{spoof}} = \varphi_s + \varphi_{vs}. \tag{11}$$

The resultant phase is composed of two components: φ_s caused due to the incoherence between the victim radar's chirp signal and the spoofing signal f_s and the contribution of the phase shifter φ_{vs}.

For the FMCW range cum vital-Doppler attack system, prior knowledge of the chirp parameters is required. Over-the-air estimation of the chirp parameters was demonstrated in [53] and [54]. In addition to the chirp parameters, this attack system requires information on the instantaneous range of the victim radar. To estimate the range information, a radar operating in a different frequency band or other forms of distance measurement sensors can be used. This work assumes that the chirp parameters and the distance to the radar are known to the attacker.

III. Emulation/Spoofing System Prototype

A. Doppler Emulation/Spoofing System

A 5.8-GHz prototype of the proposed Doppler mode emulation/spoofing system was designed. The schematic is shown in Fig. 5(a). The HMC525ALC4 SSB upconversion mixer from Analog Devices is the key component in the design. The recommended LO drive for the mixer is 15 dBm. Due to the physical separation between the radar and the emulation/spoofing system, the transmitted RF signal undergoes significant attenuation derived from the free space path loss equation. Since this incoming RF signal is connected to the LO port of the mixer, multiple gain stages are required to amplify the weak RF signal to 15 dBm. In the prototype, a two-stage amplification is realized using a 40-dB low noise amplifier (LNA) module (Pasternack PE15A1010) followed by a 15-dB LNA (Analog Devices HMC392ALC4). Since the total gain provided by these amplifiers is constant, the physical distance between the victim radar and the emulation/spoofing system

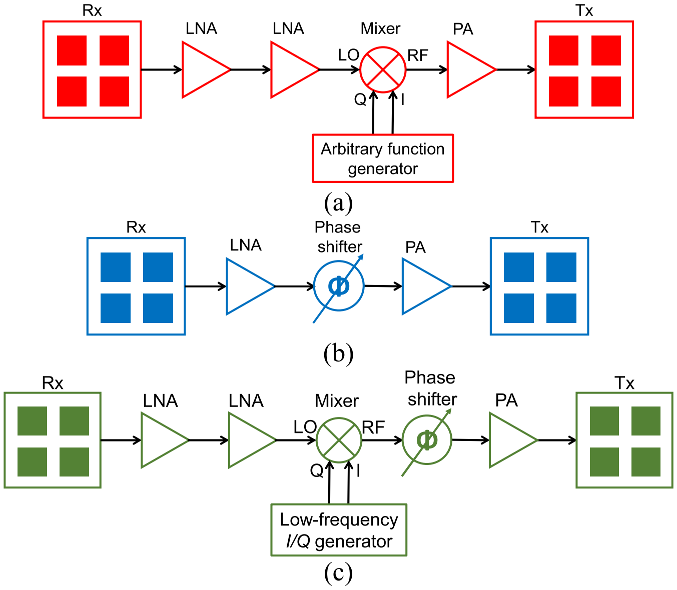


Fig. 5. Schematic of the proposed (a) Doppler radar emulation/spoofing system, (b) FMCW radar vital-Doppler emulation/spoofing system, and (c) FMCW radar range cum vital-Doppler emulation/spoofing system.

is fixed. The ideal separation between the victim radar and the emulation/spoofing system is dictated by the transmitting power of the radar and the minimum acceptable power level at the input of the two-stage amplifiers that generates a 15-dBm output power.

The I/Q spoofing signal is applied to the IF ports of the mixer. A two-channel arbitrary function generator (AFG) TELEDYNE T3AFG120 was used to generate the I/Q spoofing signals. The modulated RF waveform appears at the mixer's RF port, which is connected to the input of a power amplifier (Analog Devices HMC407), which acts as a postamplifier to amplify the modulated signal further. This amplifier is optional and is only required to increase the power level of the modulated waveform if necessary. The transmitter and receiver antennas of the spoofing system were realized using 4 × 4 patch antennas.

B. FMCW Vital-Doppler Emulation/Spoofing System

The proposed FMCW vital-Doppler emulation/spoofing system was realized at 5.8-GHz center frequency. CMD297P34-EVB from Qorvo was used as the analog phase shifter. A patch antenna receives the chirp signal, which is then fed to the phase shifter's input port. The control voltage to the phase shifter was provided from the Model DS360 Ultra Low Distortion function generator. The phase-shifted chirp signal is then retransmitted using a transmit antenna. An amplifier each (HMC392ALC4, HMC407) was added at the input and output ports of the phase shifter to increase the signal strength of the spoofed chirp. The schematic of the emulation/spoofing system is shown in Fig. 5(b).

C. FMCW Range Cum Vital-Doppler Emulation/Spoofing System

To validate the range cum vital-Doppler spoofing, the spoofing system prototype described in [63] was modified. The resultant spoofing system shown in Fig. 5(c) is similar to the abovementioned Doppler spoofing system, with the following changes: the IF ports of the SSB mixer are connected to a low-frequency I/Q generation circuit [63], and the phase shifter is inserted between the mixer and the postamplifier. The SSB mixer can be tuned to vary the range of the spoofed target, while the phase shifter performs the vital signs spoofing.

IV. Experiments

An in-house-designed multimode radar module operating from 5.6 to 6.2 GHz was used as the radar under attack. The control signal to the onboard voltage-controlled oscillator (VCO) can be varied to choose either Doppler or FMCW mode of operation. The control signal to the VCO was provided using the in-built function generator on the RIGOL DS1104Z-S oscilloscope. The I/Q baseband data generated by the radar were amplified using an onboard ac-coupled baseband amplifier and later digitized using an NI USB-6210 DAQ module. Data processing was performed using MATLAB software.

A. Doppler Radar—Walking Human Motion Spoofing

To validate the proposed Doppler radar attack model, experiments were conducted to mimic the motion of a human walking away from the radar. The Doppler radar transmitted a 5.8-GHz signal with a power of 15 dBm. Accordingly, with the two-stage amplifiers in the spoofing system providing a total gain of 55 dB, the maximum physical distance between the radar and the spoofing system was calculated as 15 m. However, in the experimental setup shown in Fig. 6(a), the physical distance was set to 2.5 m, and a 15-dB attenuator was inserted before the first amplifier in the spoofing system, so that the LO drive was set to 15 dBm. Baseband data were initially recorded with a real human subject walking away from the radar. STFT was performed on this data using the spectrogram function in MATLAB, which is shown in Fig. 6(b). The dc level of the recorded I/Q data was removed individually, and the resultant data were fed to the IF ports of the mixer to electronically mimic the fake human motion signature. If needed, amplitude scaling (attenuation) on the dc-removed I/Q data must be performed to meet the P1dB requirement of the SSB mixer. In the first scenario, the postprocessed I/Q baseband response of the real human motion was fed to I_{IF} and Q_{IF} ports of the mixer, respectively. Fig. 6(c) shows the electronically generated signature of a human walking motion. Fig. 6(b) and (c) exhibits a remarkable level of similarity, thereby exposing the vulnerability of conventional Doppler radars to such electronic counterattacks. Fig. 6(d) shows the spoofed Doppler response when the I/Q baseband data of the real human motion were fed to the Q_{IF} and I_{IF} ports of the mixer, respectively. The above scenario depicts the case when the standard LO I/Q notation is reversed, thereby validating the theory presented in Section II-A that the Doppler response gets mirrored.

B. FMCW Radar—Stationary Human Target Spoofing

Experiments were performed in an indoor setup to assess the threat offered by the proposed FMCW mode spoofing

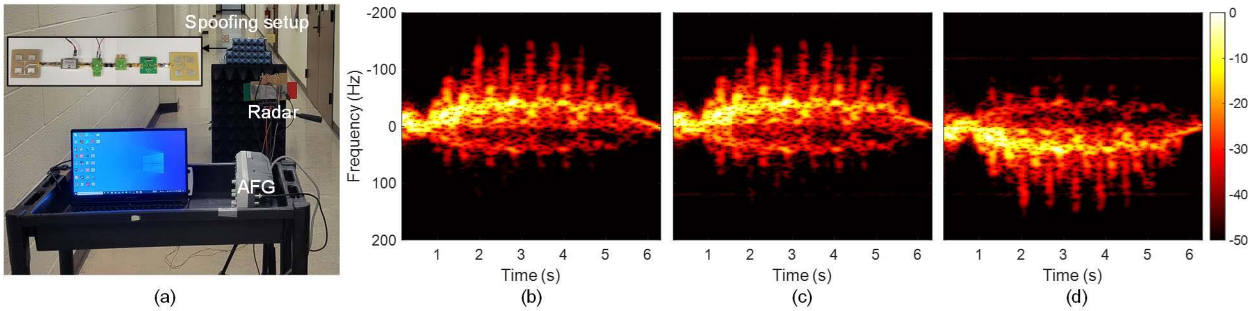


Fig. 6. (a) Experimental setup for the human walking motion emulation/spoofing. The spectrogram of (b) real human walking away from the radar in comparison with spoofed human walking motion with (c) standard LO I/Q channel notation and (d) reversed LO I/Q channel notation.

system. The FMCW radar was configured to transmit a chirp signal with a center frequency of 5.9 GHz, a bandwidth of 400 MHz, and a chirp duration of 4 ms. The spoofing system was mounted on a cart and placed 1.5 m away from the radar. To minimize reflections from the cart itself, microwave absorbers were attached to it. To mimic the cardiopulmonary motion, a multitone 0.6 V_{pp}/0.25 Hz–0.05 V_{pp}/1.2-Hz signal was fed as the control voltage to the phase shifter. The 0.6-V_{pp} control voltage translates to a peak-to-peak phase shift of 50°. The spoofing setup is shown in the inset in Fig. 7(a). Fig. 7(b) shows the obtained range profiles measured for 20 s, i.e., 5000 chirps. A fake human signature can be noticed at 2.4 m. The inset of Fig. 7(b) shows the extracted phase history and its FFT response for the 2.4-m range bin. The FFT of the phase history has two distinct peaks at 0.25 and 1.2 Hz, which corresponds to the spoofed respiration and heartbeat frequencies, respectively. Although the spoofing setup was 1.5 m away from the radar, the spoofed target was generated at 2.4 m. This additional range shift occurs due to the time delay caused due to the chirp signal propagating through the spoofing device. To calibrate this range shift, the spoofing device was placed at three different distances (1, 1.5, and 2.5 m) from the radar, and the range bin of the fake target was measured. From Fig. 7(c), it is evident that the range shift caused by the spoofing device itself corresponds to approximately 0.9 m. A one-time calibration prior to emulation/spoofing can be performed to estimate the range offset generated due to the signal propagation delay through the emulation/spoofing device. After calibration, the calculated range offset can be compensated by physically adjusting the distance of the emulation/spoofing system from the radar to accurately generate a synthetic target at a required range. For example, to emulate/spoof a stationary human at 3 m, for a measured range offset of 0.9 m, the emulation/device should be placed at 2.1 m. For the experiments discussed above, the radar and the spoofing system were deliberately turned on at different time instances to verify that the proposed attack model does not require any time synchronization with the radar.

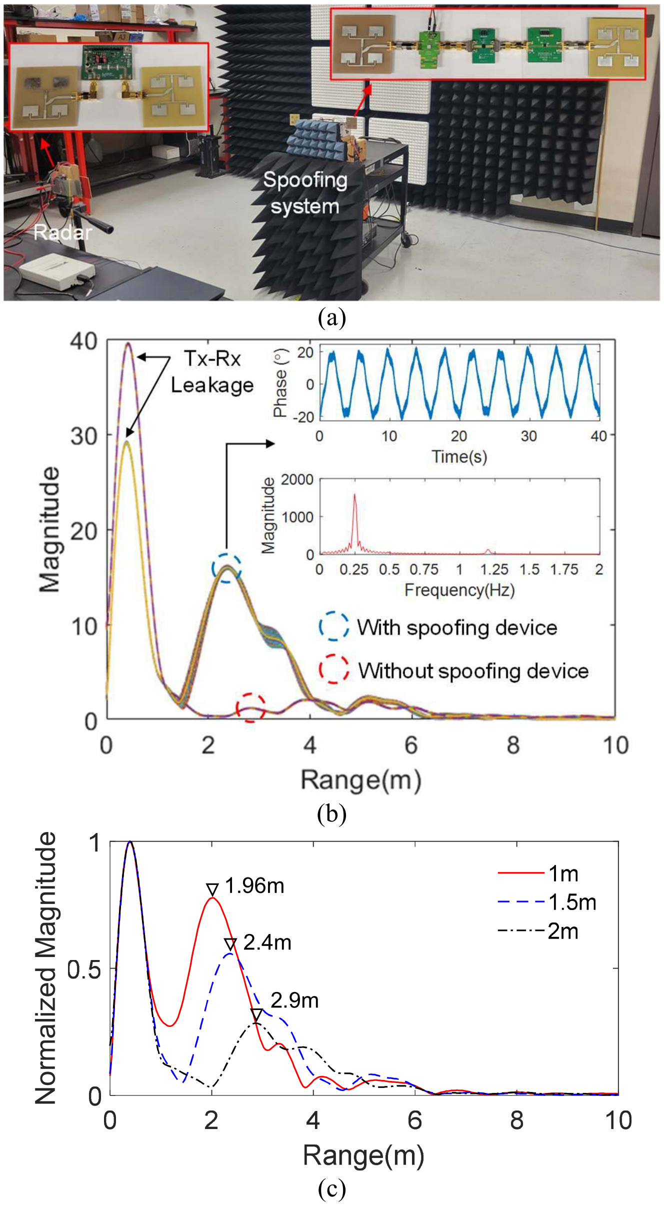
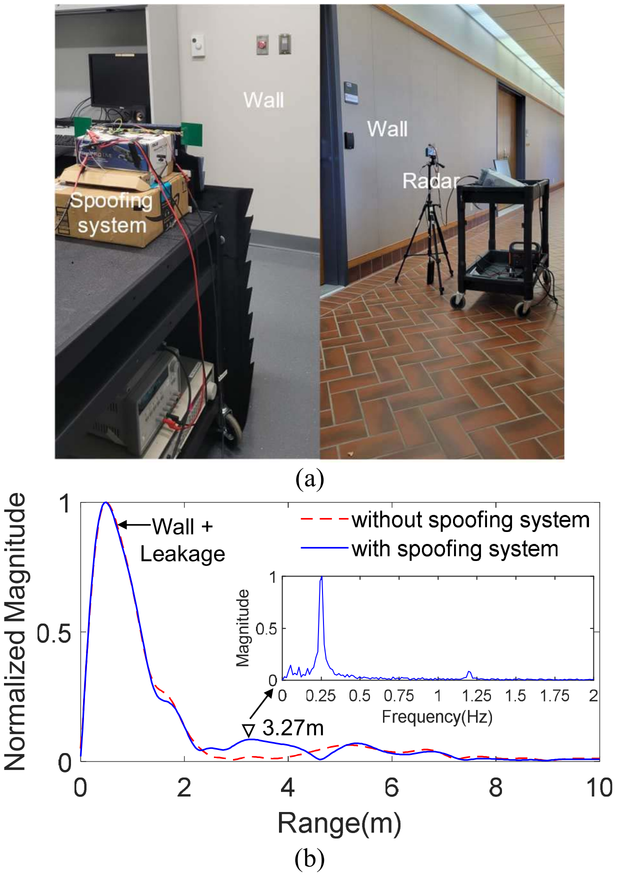


Fig. 7. (a) Experimental setup to demonstrate FMCW radar vital-Doppler spoofing. Comparison of the measured range profiles (b) without and with the spoofing system at 1.5 m and (c) with the spoofing system at various distances from the radar.

C. FMCW Radar—Through-the-Wall Spoofing

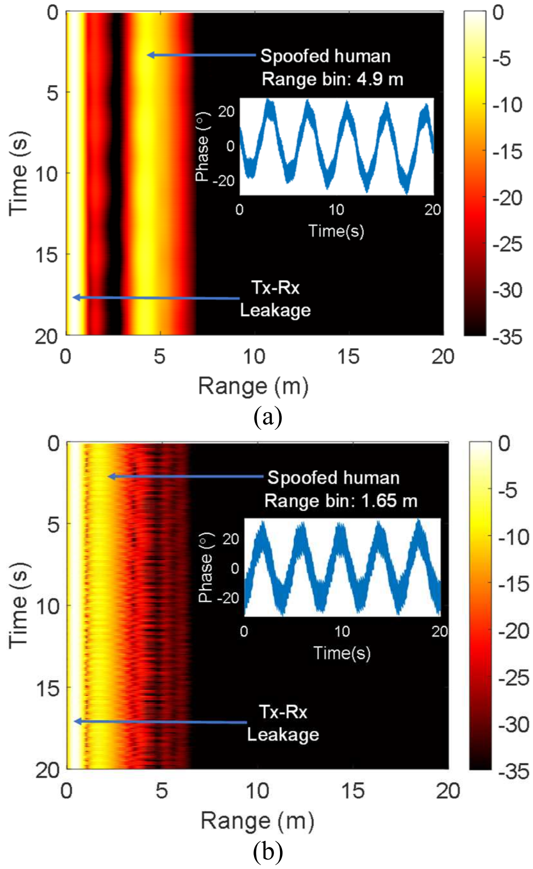
Through-the-wall sensing using radars operating within 1–6 GHz frequency band was demonstrated in [28], [29], [30], [31], [32], [33], [34], [35], and [36]. The attenuation of the 4–140-GHz frequency spectrum when they pass through various solid materials was studied in [36]. Measurements showed



(a)

(b)

Fig. 8. (a) Experimental setup for through-the-wall human subject spoofing. (b) Obtained range profile and the spoofed vital-Doppler spectrum.



(a)

(b)

Fig. 9. Measured 2-D range map and the extracted phase history using the range cum vital-Doppler spoofing system with a low-frequency spoofing signal of (a) 1.5 kHz with mixer set to output LSB tone and (b) 0.7 kHz with the mixer set to output USB tone.

that 4–8-GHz signals undergo less than 10-dB attenuation when passing through concrete blocks, while frequencies up to 80-GHz undergo minimal attenuation through the drywall. Through-the-wall detection of human subjects using radars finds applications in the field of security, where spoofing a fake human target is a significant concern. To verify such a scenario using the spoofing device, an experiment was performed with the setup shown in Fig. 8(a). The radar was placed 0.5 m from the wall, while the spoofing system was placed 1.5 m away on the other side of the wall. The wall was 25 cm wide. Fig. 8(b) shows the comparison between the radar sensing without and with the spoofing device. With the spoofing device, a fake target is seen at 3.27 m, and the measured vital-Doppler frequencies are shown in the inset.

D. FMCW Radar—Range Cum Vital-Doppler Spoofing

Previous work by the authors presented an FMCW mode spoofing system that can create a fake stationary target by up- or downshifting the transmitted chirp signal using an SSB mixer [63]. The spoofed target can be generated at an arbitrary range by changing the low-frequency spoofing signal fed to the IF ports of the mixer. By adding a phase shifter in this work, the resultant spoofing system can mimic a human target at any arbitrary range. To validate the same, experiments were performed with the similar setup shown in Fig. 7(a). The spoofing system was placed 1.5 m away from the radar. In the first scenario, a 1.5-kHz spoofing signal was fed to the mixer that was configured to output the LSB tone, so that a spoofed target at a range farther than 1.5 m is created. The phase shifter was setup to mimic respiration and heartbeat frequencies of 0.25 and 1.2 Hz, respectively. A fake human signature was generated at 4.9 m, as shown in Fig. 9(a). The extracted phase history at 4.9 m is shown in the inset. To spoof a target closer to the radar, the mixer was configured to output the USB tone shifted by 0.7 kHz, which resulted in a fake human target at 1.65 m, as shown in Fig. 9(b). Since the propagation of the chirp signal through the spoofing device adds an additional delay, the effective physical distance between the spoofing device and the radar is greater than the physical separation of 1.5 m. Thus, in the second scenario, a false target was successfully generated at a distance closer than the effective separation between the radar and the spoofing device. To validate this claim, consider the first measurement scenario presented above, where the spoofing system was placed at a distance of 1.5 m from the radar, and a 1.5-kHz spoofing signal was fed to the IF port of the mixer that was configured to output the LSB. For the given chirp parameters, a 1.5-kHz frequency offset in LSB mode should result in a spoofed target at 3.75 m [1.5 m + $(c \times 1500)/2/\gamma$]. From the experimental data, the spoofed target was observed at 4.9 m. This indicates that the FMCW range cum vital-Doppler spoofing system generates an additional range offset of 1.15 m. To validate the observed range offset value, let us evaluate the second attack scenario considered above. With the spoofing system placed 1.5 m away from the radar, the mixer was set to output to a USB tone with a 0.7-kHz spoofing signal. Theoretically, the spoofed human should be observed at 0.45 m (1.5–1.05 m). Considering the additional range offset calculated above, the spoofed human signature should be practically noticed at 1.6 m (1.5 m + 1.15 m − 1.05 m). From the experimental results presented in Fig. 9(b), the spoofed human was generated at 1.65 m, which agrees very well with the theory. To compensate for the additional range offset, a one-time calibration can be performed to estimate the range offset, and the emulation/spoofing signal frequency can be adjusted accordingly to synthesize a fake human at a specific range. From the insets in Fig. 9, it can be observed that the extracted phase is noisy compared to the measured phase shown in the inset in Fig. 7(b). This is because the overall gain of the FMCW vital-Doppler spoofing system is 3 dB higher than the FMCW range cum vital-Doppler spoofing system.

An important parameter characterizing an emulation/spoofing system is the maximum operating range, i.e., the maximum physical separation between the radar and the emulation/spoofing device that allows the accurate generation of synthetic targets. For the proposed Doppler and FMCW range cum vital-Doppler emulation/spoofing architectures, the maximum operating range is primarily limited by the LO drive of the mixer, while other factors such as the gain of the Tx/Rx antennas and total gain offered by the preamplification stages (amplifiers before the SSB mixer) also affect it. In the current device prototypes, the 4 × 4 patch antennas offer an 8-dB realized gain, the total gain of the preamplification stages is 55 dB, and the LO drive of the mixer is 15 dBm. With the radar transmitting 15 dBm of output power, the maximum operating distance is limited to 15 m. For the FMCW vital-Doppler emulation/spoofing device presented in Section III-B, the maximum operating range is limited by the input power requirement of the analog phase shifter. The phase shifter used in the prototype can work at power levels of −10 dBm. Considering the same 55-dB total gain of the preamplification stages, the FMCW vital-Doppler emulation/spoofing system can easily operate at distances up to 30 m and more, depending on the sensitivity of the radar's receiver chain. Alternatively, to achieve the same maximum operating range of 15 m, this system only requires a total preamplification gain of 30 dB. Although this architecture does not have the ability to electronically alter the range of the spoofed/emulated target, the improvement in the maximum operating range is a tradeoff worth considering. In scenarios involving through-the-wall sensing where the RF signal undergoes significant attenuation due to the wall, the proposed FMCW range cum vital-Doppler emulation/spoofing device architecture is unsuitable due to the high LO drive requirement of the SSB mixer. Moreover, in certain scenarios, the FMCW range cum vital-Doppler system generates additional unnecessary Doppler peaks, which will be discussed in detail in Section IV-E.

To improve the maximum operating range of the emulation/spoofing systems, highly directional antennas and additional gain stages can be added to the emulation/spoofing system. Alternatively, for the Doppler and FMCW range cum vital-Doppler emulation/spoofing systems, the SSB mixer can be replaced with custom-designed mixers that require low LO power or injection-locked oscillators (ILOs). ILOs can achieve a locking range of 80 MHz with injection signal strength as low as −20 dBm [68].

E. Discussion

The signal processing for indoor human sensing mainly depends on the activity performed by the human subject. For identifying a walking/running human, the 2-D-FFT (also referred to as range-Doppler FFT) is useful in measuring the instantaneous position and speed of the human subject [37], [43]. A walking/running person also generates multiple Doppler components due to the swinging motion of the arms and legs [39] that are useful in distinguishing it from surrounding moving targets. When a person performs an activity (such as standing up, sitting down, or falling down) wherein his position is relatively constant, a micro-Doppler spectrogram is more convenient in identifying the activity performed [46]. A micro-Doppler spectrogram is obtained by first identifying the range bin of the human target and then performing an STFT along the slow-time data for that specific range bin. For a seated human subject not performing any activity, the inherent chest motion is used to isolate it from surrounding stationary clutter by applying low-pass filtering [69] or a standard deviation approach [37]. To extract the displacement of the chest motion, the range bin of the seated human target is identified, and the unwrapped phase change across consecutive chirp responses is traced [42]. It should be noted that this article focuses only on the emulation/spoofing of stationary human subjects.

For stationary human identification, it is essential to distinguish the human targets from other reflecting or clutter sources in the surroundings. Due to the inherent chest motion of the human body, techniques, such as moving target indicator (MTI) filtering [29], exponential moving average (EMA) filtering [38], [69], and coherent phase difference approach [70], were used to isolate the human targets from nearby stationary targets. To verify the robustness of the proposed FMCW mode vital-Doppler spoofing system against the abovementioned filtering techniques, a high-pass filter (HPF) was applied to the recorded data corresponding to the experimental setup in Fig. 7(a). A built-in MATLAB function was used to realize an infinite impulse response (IIR) HPF with a cutoff frequency of 0.2 Hz and stopband attenuation of 60 dB. Fig. 10(a) shows the output of the HPF with the FMCW mode vital-Doppler spoofing system placed at a distance of 1, 1.5, and 2 m from the radar. Compared to Fig. 7(c), the range maps in Fig. 10(a) have a stronger peak at the location of the spoofed human target, and the surrounding clutter, including the Tx–Rx leakage, is attenuated. In measurement scenarios involving through-the-wall sensing, it is common that the signature of the human target is very weak without additional signal processing. This occurs because the wall has a higher radar cross section (RCS) and also attenuates some of the RF signal passing through it. Signal processing techniques, such as background subtraction [28], [31], [32], and low-pass

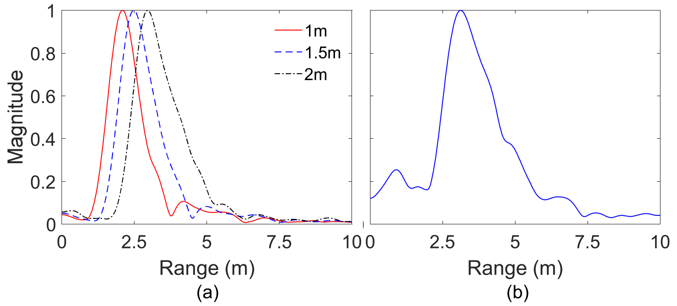


Fig. 10. Range profiles after applying HPF on (a) FMCW vital-Doppler spoofing data [Fig. 6(c)] and (b) through-the-wall human spoofing data [Fig. 7(b)].

filtering [29], [33], were performed to enhance the signature of the human target by suppressing stationary targets. Similarly, HPF was applied to the measure through-the-wall spoofing data in Section IV-C, and the obtained result is shown in Fig. 10(b).

Human target detection based on the standard deviation approach was proposed in [37]. Unlike filtering, this technique is based on the notion that the human body is not a flat reflecting surface, and the tiny motion of the chest causes a significant variation in the range profiles. The reflections from the human body are slightly spread out along the range axis with varying signal strength. By measuring the standard deviation of the measured range profiles along the slow time, the human target can be distinguished from other reflecting sources. Unlike a real human target, the designed spoofing system employs antenna elements to retransmit the spoofed signal. Therefore, the variation in the range profiles of a spoofed human is not comparable to that of a real human. The HMC407 power amplifier used in the spoofing device was configured as a variational gain amplifier (VGA) to vary the signal strength of the retransmitted spoofed chirps. By doing so, variance is induced along the slow time in the range bin corresponding to the spoofed human. The HMC407 has a power-down pin that can be used to control the gain. A sine wave oscillating between 5 and 3.5 V at a frequency of 20 Hz was applied to this pin, so that the spoofed signal has varying power levels, thereby mimicking the amplitude variation in the reflected signals from a true human subject. Fig. 11(a) shows the improvement in the standard deviation of the spoofed human target using the VGA in the spoofing setup. With the VGA on, the obtained phase spectrum had peaks corresponding to the spoofed vital-Doppler frequencies at 0.25 and 1.2 Hz, as shown in Fig. 11(b). In addition, as evident from the inset of Fig. 11(b), there was a small peak at 20 Hz, which was the frequency of the sine wave fed to the power-down pin of the VGA. The effect of the gain variation of the VGA on the measured phase spectrum will be studied in-depth as part of future work. It should be noted that the standard deviation introduced by the VGA does not truly mimic the standard deviation due to the reflections from a human body. However, it is enough to deceive a radar's signal processing backend that relies on the standard deviation approach for identifying human targets. While using the proposed architecture as an RTE, additional work is required to truly mimic the variation due to the reflections from a human body.

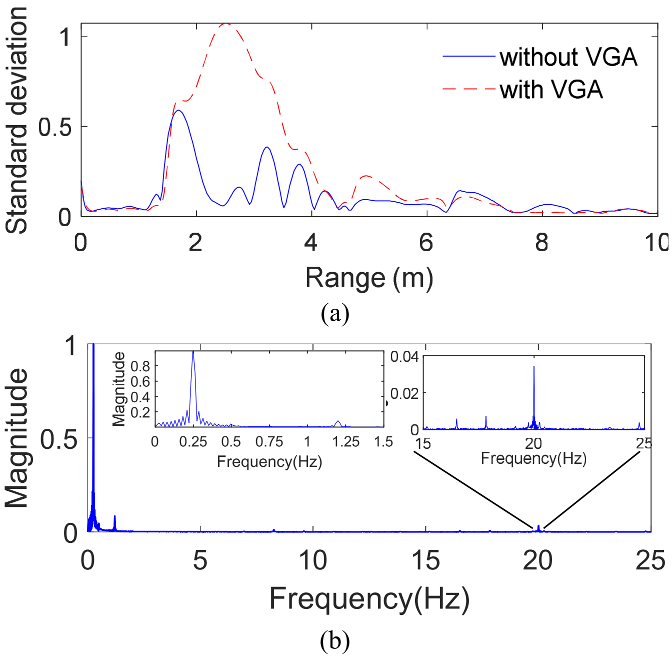


Fig. 11. (a) Comparison of the standard deviation approach without and with the VGA in the spoofing setup. (b) Measured phase spectrum with the VGA as part of the spoofing system.

The FMCW range spoofing system proposed in [63] generates an unintended Doppler frequency due to the phase incoherence of the low-frequency spoofing signal across consecutive chirps. This phase incoherence occurs because a free-running function generator was used to generate the low-frequency spoofing signal that was fed to the IF ports of the SSB mixer. The phase incoherence translates to a Doppler frequency f_D that depends on the chirp repetition rate (CRR) and the spoofing frequency f_s, and can be calculated using the equation

$$f_D = |n \times \mathrm{CRR} - f_s|, \quad n \in I \tag{12}$$

where n is an integer, such that $f_D \in [0, \mathrm{CRR}/2]$. To analyze this effect on the proposed range cum vital-Doppler spoofing system, experiments were performed with different combinations of CRR and the spoofing frequency. In the first case, the CRR and the spoofing frequency were set to 250 and 700 Hz, respectively. This should yield a Doppler frequency of 50 Hz, as evident from Fig. 12(a). In the second case, a Doppler frequency of 4 Hz was generated, corresponding to 249-Hz CRR and 1-kHz spoofing frequency. The measured phase spectrum is shown in Fig. 12(b). Based on the above results, it can be inferred that the FMCW range spoofing system alone can generate spoofed Doppler frequencies. However, the human vital sign frequencies lie in the range of 0.2–2 Hz, which can be difficult to achieve as it requires specific combinations of the CRR and the spoofing frequency. By choosing a spoofing frequency corresponding to the CRR of the victim radar to generate the vital-Doppler frequencies in the required frequency range, it limits the ability to generate the spoofed human targets at arbitrary range bins.

To initially design a proof-of-concept prototype of the emulation/spoofing systems, the 5.8-GHz center frequency

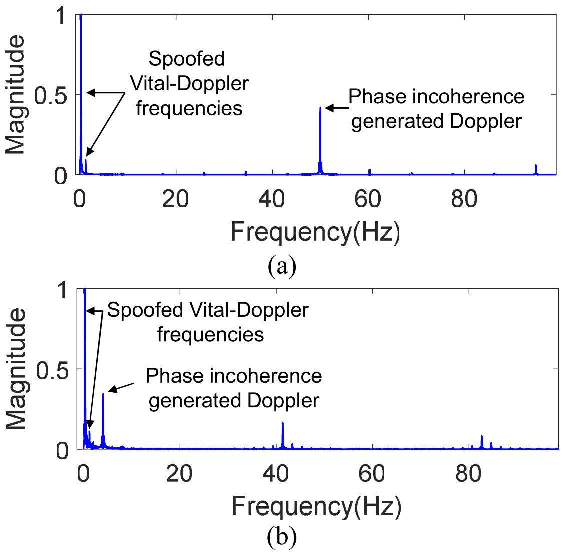


Fig. 12. Effect of the phase incoherence of the spoofing signal (range cum vital-Doppler spoofing system) on the measured phase spectrum when (a) CRR = 250 Hz and f_s = 700 Hz and (b) CRR = 249 Hz and f_s = 1 kHz.

was chosen because the 5.725–5.875-GHz spectrum is an unlicensed frequency band reserved for industrial, scientific, and medical (ISM) applications. Also, several commercial radar products are available in this frequency band. With passive radio sensing based on Wi-Fi signals gaining interest [71], it would be quite interesting to study if the proposed emulation/spoofing architecture can be tuned for this particular application. Commercially, radar sensors for indoor sensing applications are also realized at 24 GHz. Since the 24–24.25-GHz spectrum is also an unlicensed ISM band, many of the RF components, such as amplifiers and mixers, are inexpensive and readily available in the market. A similar emulation/spoofing device can also be realized at 24 GHz using commercially available off-the-shelf components. Alternatively, phase shifters at 24 GHz can be realized using a vector controller [72]. However, with increased frequency, the free space path loss of the electromagnetic waves also increases, thereby affecting the maximum operating range of the emulation/spoofing device. To overcome this challenge, highly directional antennas, additional preamplification stages, and low LO power alternatives to the SSB mixer can be added to the attack system. On the other hand, a major impact would be the recent shift in the operating frequency of short-range radar sensors for IoT applications to the 57–64-GHz band. There is limited availability of inexpensive commercial RF components in the market. To follow this change, new devices and components need to be developed.

Mitigating spoofing attacks against FMCW radars based on randomizing the chirp parameters were presented in [58], [59], [60], [61], and [73]. Since the proposed FMCW spoofing systems are passive attack models, phase randomization of the chirp has minimal effect on the spoofing ability since the attacker is only relaying a frequency- or phase-shifted or both versions of the chirp signal transmitted by the victim radar. In the case of the random frequency hopping technique proposed in [73], since the slope of the randomized chirps remains constant while only changing the center frequency, the proposed FMCW spoofing devices should be able to successfully deceive the radar, provided that the employed RF mixers and phase shifters can operate in the entire frequency band. If the slope of the chirp signals is randomized [63], the proposed FMCW vital-Doppler spoofing system can still carry out attacks, provided that the chirp's frequency is still within the operating range of the phase shifter. However, the FMCW range cum vital-Doppler spoofing system cannot deceive radars with changing chirp slopes. Since the range of the spoofed human target changes with changing chirp slope, the attack is no longer viable in human sensing scenarios.

From the analysis and results presented in Sections IV-A and IV-B, it can be inferred that the architecture of a spoofing device can be used to realize an RTE because the proposed spoofing systems are basically emulating the response of a real target, which is the role of an emulator.

V. Conclusion

With the advancement of RF sensing technology and the several advantages offered compared to other forms of sensing, radars have become a frontrunner in various surround sensing applications in the emerging IoT era. This article presents a feasibility study on electronically replicating the human target response model of Doppler and FMCW radars employed in various day-to-day applications, which may potentially disrupt their normal functionality. The 5.8-GHz proof-of-concept systems were developed to demonstrate the following: 1) mimicking the human walking motion interacting with Doppler radars and 2) emulating human cardiopulmonary motion against FMCW radars while also altering the range of the fake human target. Future work will be focused on identifying the spectral properties of the electronically generated targets that differ from those of a real target and then proposing effective mitigation techniques in terms of waveform design and machine learning-based false target classification. With regard to the RTE, future work could focus on a better match of the subtle characteristics of the emulated target response with that of a real target. For the FMCW mode of operation, the emulation of micro-Doppler responses that span across multiple range bins and coherent range-Doppler responses for scenarios such as a walking/running human could also be studied.

References

[1] J. Wang, X. Wang, L. Chen, J. Huangfu, C. Li, and L. Ran, "Noncontact distance and amplitude-independent vibration measurement based on an extended DACM algorithm," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 1, pp. 145–153, Jan. 2014.

[2] C. Gu, T. Inoue, and C. Li, "Analysis and experiment on the modulation sensitivity of Doppler radar vibration measurement," *IEEE Microw. Wireless Compon. Lett.*, vol. 23, no. 10, pp. 566–568, Oct. 2013.

[3] D. V. Q. Rodrigues, D. Zuo, Z. Tang, J. Wang, C. Gu, and C. Li, "Adaptive displacement calibration strategies for field structural health monitoring based on Doppler radars," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 10, pp. 7813–7824, Oct. 2020.

[4] C. Li *et al.*, "A review on recent progress of portable short-range noncontact microwave radar systems," *IEEE Trans. Microw. Theory Techn.*, vol. 65, no. 5, pp. 1692–1706, May 2017.

[5] C. Li, V. M. Lubecke, O. Boric-Lubecke, and J. Lin, "A review on recent advances in Doppler radar sensors for noncontact healthcare monitoring," *IEEE Trans. Microw. Theory Techn.*, vol. 61, no. 5, pp. 2046–2060, May 2013.

[6] C. Li, J. Cummings, J. Lam, E. Graves, and W. Wu, “Radar remote monitoring of vital signs,” *IEEE Microw. Mag.*, vol. 10, no. 1, pp. 47–56, Feb. 2009.

[7] C. Gu, C. Li, J. Lin, J. Long, J. Huangfu, and L. Ran, “Instrument-based noncontact Doppler radar vital sign detection system using heterodyne digital quadrature demodulation architecture,” *IEEE Trans. Instrum. Meas.*, vol. 59, no. 6, pp. 1580–1588, Jun. 2010.

[8] C. Gu, “Short-range noncontact sensors for healthcare and other emerging applications: A review,” *Sensors*, vol. 16, no. 8, p. 1169, Aug. 2016.

[9] C. Li and J. Lin, “Random body movement cancellation in Doppler radar vital sign detection,” *IEEE Trans. Microw. Theory Techn.*, vol. 56, no. 12, pp. 3143–3152, Dec. 2008.

[10] C. Li, J. Ling, J. Li, and J. Lin, “Accurate Doppler radar noncontact vital sign detection using the RELAX algorithm,” *IEEE Trans. Instrum. Meas.*, vol. 59, no. 3, pp. 687–695, Mar. 2010.

[11] F.-K. Wang, T.-S. Horng, K.-C. Peng, J.-K. Jau, J.-Y. Li, and C.-C. Chen, “Single-antenna Doppler radars using self and mutual injection locking for vital sign detection with random body movement cancellation,” *IEEE Trans. Microw. Theory Techn.*, vol. 59, no. 12, pp. 3577–3587, Dec. 2011.

[12] V. P. Tran, A. A. Al-Jumaily, and S. M. S. Islam, “Doppler radar-based non-contact health monitoring for obstructive sleep apnea diagnosis: A comprehensive review,” *Big Data Cognit. Comput.*, vol. 3, no. 1, p. 3, Jan. 2019.

[13] M. Baboli, A. Singh, B. Soll, O. Boric-Lubecke, and V. M. Lubecke, “Good night: Sleep monitoring using a physiological radar monitoring system integrated with a polysomnography system,” *IEEE Microw. Mag.*, vol. 16, no. 6, pp. 34–41, Jul. 2015.

[14] M. Baboli, A. Singh, B. Soll, O. Boric-Lubecke, and V. M. Lubecke, “Wireless sleep apnea detection using continuous wave quadrature Doppler radar,” *IEEE Sensors J.*, vol. 20, no. 1, pp. 538–545, Jan. 2020.

[15] N. T. P. Van, L. Tang, V. Demir, S. F. Hasan, N. D. Minh, and S. Mukhopadhyay, “Review-microwave radar sensing systems for search and rescue purposes,” *Sensors*, vol. 19, no. 13, p. 2879, Jun. 2019.

[16] K.-M. Chen, D. Misra, H. Wang, H.-R. Chuang, and E. Postow, “An X-band microwave life-detection system,” *IEEE Trans. Biomed. Eng.*, vol. BME-33, no. 7, pp. 697–701, Jul. 1986.

[17] T. Fan *et al.*, “Wireless hand gesture recognition based on continuous-wave Doppler radar sensors,” *IEEE Trans. Microw. Theory Techn.*, vol. 64, no. 11, pp. 4012–4020, Nov. 2016.

[18] S. Skaria, A. Al-Hourani, M. Lech, and R. J. Evans, “Hand-gesture recognition using two-antenna Doppler radar with deep convolutional neural networks,” *IEEE Sensors J.*, vol. 19, no. 8, pp. 3041–3048, Apr. 2019.

[19] J. L. Geisheimer, W. S. Marshall, and E. Greneker, “A continuous-wave (CW) radar for gait analysis,” in *Proc. Conf. Rec. 35th Asilomar Conf. Signals, Syst. Comput.*, Nov. 2001, pp. 834–838.

[20] J. L. Geisheimer, E. F. Greneker, and W. S. Marshall, “High-resolution Doppler model of the human gait,” *Proc. SPIE*, vol. 4744, pp. 8–18, Jul. 2002.

[21] E. Yavari, H. Jou, V. Lubecke, and O. Boric-Lubecke, “Doppler radar sensor for occupancy monitoring,” in *Proc. IEEE Radio Wireless Symp.*, Jan. 2013, pp. 145–147.

[22] E. Yavari, C. Song, V. Lubecke, and O. Boric-Lubecke, “System-on-chip based Doppler radar occupancy sensor,” in *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc.*, Aug. 2011, pp. 1913–1916.

[23] E. Yavari, A. Lee, K. Pang, N. A. McCabe, and O. Boric-Lubecke, “Radar and conventional occupancy sensors performance comparison,” in *Proc. Asia Pacific Microw. Conf.*, Nov. 2014, pp. 444–446.

[24] Q. Lv *et al.*, “High dynamic-range motion imaging based on linearized Doppler radar sensor,” *IEEE Trans. Microw. Theory Techn.*, vol. 62, no. 9, pp. 1837–1846, Sep. 2014.

[25] A. Kalyanaraman, E. Soltanaghaei, and K. Whitehouse, “Doorpler: A radar-based system for real-time, low power zone occupancy sensing,” in *Proc. IEEE Real-Time Embedded Technol. Appl. Symp. (RTAS)*, Apr. 2019, pp. 42–53.

[26] D. Rodriguez, A. Flores, and C. Li, “Self-powered 24-GHz Doppler radar for building entrance monitoring using cross correlation and envelope detection,” in *Proc. IEEE Topical Conf. Wireless Sensors Sensor Netw. (WiSNet)*, Jan. 2019, pp. 1–4.

[27] T. Lenhard, “Commercial radar sensors and applications,” in *Proc. Assoc. Sensors Meas.* Nurnberg, Germany, 2017, pp. 473–477.

[28] N. Maaref, P. Millot, C. Pichot, and O. Picon, “A study of UWB FM-CW radar for the detection of human beings in motion inside a building,” *IEEE Trans. Geosci. Remote Sens.*, vol. 47, no. 5, pp. 1297–1300, May 2009.

[29] M. Ash, M. Ritchie, and K. Chetty, “On the application of digital moving target indication techniques to short-range FMCW radar data,” *IEEE Sensors J.*, vol. 18, no. 10, pp. 4167–4175, May 2018.

[30] F. Fioranelli, S. Salous, I. Ndip, and X. Raimundo, “Through-the-wall detection with gated FMCW signals using optimized patch-like and Vivaldi antennas,” *IEEE Trans. Antennas Propag.*, vol. 63, no. 3, pp. 1106–1117, Mar. 2015.

[31] F. Wang, T. Horng, K. Peng, J. Jau, J. Li, and C. Chen, “Detection of concealed individuals based on their vital signs by using a see-through-wall imaging system with a self-injection-locked radar,” *IEEE Trans. Microw. Theory Techn.*, vol. 61, no. 1, pp. 696–704, Jan. 2013.

[32] F.-K. Wang, T.-S. Horng, K.-C. Peng, J.-K. Jau, J.-Y. Li, and C.-C. Chen, “Seeing through walls with a self-injection-locked radar to detect hidden people,” in *IEEE MTT-S Int. Microw. Symp. Dig.*, Jun. 2012, pp. 1–3.

[33] Y. Z. Wang, Q. H. Liu, and A. E. Fathy, “CW and pulse-Doppler radar processing based on FPGA for human sensing applications,” *IEEE Trans. Geosci. Remote Sens.*, vol. 51, no. 5, pp. 3097–3107, May 2013.

[34] T. S. Ralston, G. L. Charvat, and J. E. Peabody, “Real-time through-wall imaging using an ultrawideband multiple-input multiple-output (MIMO) phased array radar system,” in *Proc. IEEE Int. Symp. Phased Array Syst. Technol.*, Oct. 2010, pp. 551–558.

[35] R. M. Narayanan and M. Zenaldin, “Radar micro-Doppler signatures of various human activities,” *IET Radar, Sonar Navigat.*, vol. 9, no. 9, pp. 1205–1215, 2015.

[36] L. M. Frazier, “Radar surveillance through solid materials,” *Proc. SPIE*, vol. 2938, p. 139, Feb. 1997.

[37] Z. Peng *et al.*, “A portable FMCW interferometry radar with programmable low-IF architecture for localization, ISAR imaging, and vital sign tracking,” *IEEE Trans. Microw. Theory Techn.*, vol. 65, no. 4, pp. 1334–1344, Apr. 2017.

[38] C. Will, P. Vaishnav, A. Chakraborty, and A. Santra, “Human target detection, tracking, and classification using 24-GHz FMCW radar,” *IEEE Sensors J.*, vol. 19, no. 17, pp. 7283–7299, Sep. 2019.

[39] J. A. Nanzer, “A review of microwave wireless techniques for human presence detection and classification,” *IEEE Trans. Microw. Theory Techn.*, vol. 65, no. 5, pp. 1780–1794, May 2017.

[40] K. Han and S. Hong, “Detection and localization of multiple humans based on curve length of I/Q signal trajectory using MIMO FMCW radar,” *IEEE Microw. Wireless Compon. Lett.*, vol. 31, no. 4, pp. 413–416, Apr. 2021.

[41] B. Vandersmissen *et al.*, “Indoor person identification using a low-power FMCW radar,” *IEEE Trans. Geosci. Remote Sens.*, vol. 56, no. 7, pp. 3941–3952, Jul. 2018.

[42] G. Wang, J.-M. Muñoz-Ferreras, C. Gu, C. Li, and R. Gómez-García, “Application of linear-frequency-modulated continuous-wave (LFMCW) radars for tracking of vital signs,” *IEEE Trans. Microw. Theory Techn.*, vol. 62, no. 6, pp. 1387–1399, Jun. 2014.

[43] A. Santra, R. V. Ulaganathan, and T. Finke, “Short-range millimetric-wave radar system for occupancy sensing application,” *IEEE Sensors Lett.*, vol. 2, no. 3, pp. 1–4, Sep. 2018.

[44] X. Li, Y. He, and X. Jing, “A survey of deep learning-based human activity recognition in radar,” *Remote Sens.*, vol. 11, no. 9, p. 1068, Jan. 2019.

[45] B. Erol and M. G. Amin, “Radar data cube processing for human activity recognition using multisubspace learning,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 6, pp. 3617–3628, Dec. 2019.

[46] S. A. Shah and F. Fioranelli, “Human activity recognition: Preliminary results for dataset portability using FMCW radar,” in *Proc. Int. Radar Conf. (RADAR)*. Toulon, France, Sep. 2019, pp. 1–4.

[47] G. Wang, C. Gu, T. Inoue, and C. Li, “A hybrid FMCW-interferometry radar for indoor precise positioning and versatile life activity monitoring,” *IEEE Trans. Microw. Theory Techn.*, vol. 62, no. 11, pp. 2812–2822, Nov. 2014.

[48] A. Rizik, E. Tavanti, H. Chible, D. D. Caviglia, and A. Randazzo, “Cost-efficient FMCW radar for multi-target classification in security gate monitoring,” *IEEE Sensors J.*, vol. 21, no. 18, pp. 20447–20461, Sep. 2021.

[49] Z. Ni and B. Huang, “Gait-based person identification and intruder detection using mm-wave sensing in multi-person scenario,” *IEEE Sensors J.*, vol. 22, no. 10, pp. 9713–9723, May 2022.

[50] H. Cai *et al.*, “Foreign objects intrusion detection using millimeter wave radar on railway crossings,” in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*. Toronto, ON, Canada, Oct. 2020, pp. 2776–2781.

[51] F. P. Martinez and F. C. Galeano, “New microwave sensors for intrusion detection systems,” in *Proc. 33rd IEEE Annu. Int. Carnahan Conf. Secur. Technol.* Madrid, Spain, Oct. 1999, pp. 49–53.

[52] L. Neng-Jing and Z. Yi-Ting, "A survey of radar ECM and ECCM," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 31, no. 3, pp. 1110–1120, Jul. 1995.

[53] 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.*, Jun. 2019, pp. 544–547.

[54] 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)*, Jan. 2020, pp. 46–49.

[55] 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.

[56] 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)*, Aug. 2018, pp. 1–6.

[57] 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)*, Jun. 2012, pp. 15–26.

[58] 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.

[59] 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. Cryptogr. Eng.*, vol. 11, no. 3, pp. 289–298, Jan. 2021.

[60] R. Komissarov and A. Wool, "Spoofing attacks against vehicular FMCW radar," 2021, *arXiv:2104.13318*.

[61] 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*.

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

[63] P. Nallabolu and C. Li, "A frequency-domain spoofing attack on FMCW radars and its mitigation technique based on a hybrid-chirp waveform," *IEEE Trans. Microw. Theory Techn.*, vol. 69, no. 11, pp. 5086–5098, Nov. 2021.

[64] D. Rodriguez, J. Wang, and C. Li, "Spoofing attacks to radar motion sensors with portable RF devices," in *Proc. IEEE Radio Wireless Symp. (RWS)*. San Diego, CA, USA, Jan. 2021, pp. 73–75.

[65] dSPACE GmbH, Paderborn, Germany. *DARTS 9040-G the First True 5 GHz Bandwidth Radar Target Simulator*. (2020). Accessed: Aug. 1, 2022. [Online]. Available: https://www.dspace.com/shared/data/pdf/2021/dSPACE_DARTS-9040-G_TwoPager_2020-12_EN.pdf

[66] Keysight, Santa Rosa, CA, USA. *Radar Scene Emulator*. Accessed: Aug. 1, 2022. [Online]. Available: https://www.keysight.com/us/en/assets/7121-1260/data-sheets/Radar-Scene-Emulator.pdf

[67] P. Nallabolu and C. Li, "Investigating a portable low-cost target simulator for Doppler radars," in *Proc. IEEE USNC-URSI Radio Sci. Meeting (Joint With AP-S Symp.)*, Jul. 2022, pp. 72–73.

[68] 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.

[69] P. Nallabolu, L. Zhang, H. Hong, and C. Li, "Human presence sensing and gesture recognition for smart home applications with moving and stationary clutter suppression using a 60-GHz digital beamforming FMCW radar," *IEEE Access*, vol. 9, pp. 72857–72866, 2021.

[70] E. Hyun, Y.-S. Jin, and J.-H. Lee, "A pedestrian detection scheme using a coherent phase difference method based on 2D range-Doppler FMCW radar," *Sensors*, vol. 16, no. 1, p. 124, Jan. 2016.

[71] W. Li, R. J. Piechocki, K. Woodbridge, C. Tang, and K. Chetty, "Passive WiFi radar for human sensing using a stand-alone access point," *IEEE Trans. Geosci. Remote Sens.*, vol. 59, no. 3, pp. 1986–1998, Mar. 2021.

[72] Z. Peng, L. Lixin Ran, and C. Li, "A 24-GHz low-cost continuous beam steering phased array for indoor smart radar," in *Proc. IEEE 58th Int. Midwest Symp. Circuits Syst. (MWSCAS)*. Fort Collins, CO, USA, Aug. 2015, pp. 1–4.

[73] T. Moon, J. Park, and S. Kim, "BlueFMCW: Random frequency hopping radar for mitigation of interference and spoofing," 2020, *arXiv:2008.00624*.

Prateek Nallabolu (Member, IEEE) received the B.Tech. degree in electronics and communications engineering from Jawaharlal Nehru Technological University, Hyderabad, India, in 2016, and the Ph.D. degree in electrical engineering from Texas Tech University, Lubbock, TX, USA, in 2022.

He will be joining Oculii Corporation (An Ambarella Technology) as an RF Hardware Engineer, focusing on system-level automotive radar design. His current research interests include microwave/millimeter-wave radar systems, radar test systems, and radar security.

Dr. Nallabolu received the IEEE Microwave Theory and Techniques Society Second Place Winner Award in the 2021 High-Sensitivity Motion Radar Student Design Competition. He is an Active Reviewer for the IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES.

Daniel Rodriguez (Member, IEEE) received the B.S. degree in electronics and telecommunication engineering from the Universidad Autonoma del Caribe, Barranquilla, Colombia, in 2014, and the Ph.D. degree in electrical engineering from Tech University, Lubbock, TX, USA, in 2022.

He is currently an Analog Engineer with Intel Corporation, Hillsboro, OR, USA. His current research interests include radar systems, microwave/millimeter-wave sensing, and microwave circuits.

Dr. Rodriguez was awarded as an HSF Scholar in 2019. He received the IEEE MTT-S Graduate Fellowship Award in 2020 and the JT and Margaret Talkington Graduate Fellowship in 2017. He is an Active Reviewer for the IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES, the IEEE JOURNAL OF ELECTROMAGNETICS, RF AND MICROWAVES IN MEDICINE AND BIOLOGY, and the IEEE SENSORS JOURNAL.

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 with Texas Tech University, Lubbock, TX, USA. His current research interests include microwave/millimeter-wave sensing for healthcare, security, energy efficiency, structural monitoring, and human–machine interface.

Dr. Li is a Distinguished Microwave Lecturer of the IEEE Microwave Theory and Techniques Society (MTT-S), in the Tatsuo Itoh Class of 2022–2024. He was a recipient of the IEEE 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.