IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 29 May 2023, accepted 14 June 2023, date of publication 21 June 2023, date of current version 27 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3288423

RESEARCH ARTICLE

A Compound ECCM Technique for FMCW Radars

DOĞANCAN ESER, (Student Member, IEEE), ŞİMŞEK DEMİR, (Member, IEEE), AND SENCER KOÇ, (Member, IEEE)
Department of Electrical and Electronics Engineering, Middle East Technical University, 06800 Ankara, Turkey
Corresponding author: Doğancan Eser (eser.dogancan@metu.edu.tr)

ABSTRACT This paper presents a compound electronic counter-countermeasure (ECCM) technique for frequency-modulated continuous-wave (FMCW) radars to counter electronic countermeasure (ECM) techniques such as coherent spoofing, non-coherent spoofing, and digital radio frequency memory (DRFM) jamming. The proposed technique is based on phase coding in slow time and checking the initial phase of the baseband return signal. A measurement setup was built and operated between 4.3-4.5 GHz for experimental validation. An RF cable of length 12 m was used to emulate the target. The experimental results were analyzed using MATLAB to demonstrate the effectiveness of the ECCM technique in different jamming scenarios. The results indicate that the proposed ECCM technique using phase coding can provide a satisfactory performance in different jamming scenarios. The proposed ECCM technique offers several advantages over existing methods. First, the technique does not entail any frequency bin changes in slow time period, thereby conferring processing benefits. Second, it poses challenges to jammer system in terms of predicting the initial phase of the beat signal. The proposed technique is expected to provide better protection against malicious attacks for FMCW radars.

INDEX TERMS Coherent spoofing, digital radio frequency memory (DRFM), electronic counter-counter measure (ECCM), frequency-modulated continuous-wave (FMCW) radar, phase coding.

I. INTRODUCTION

At the present time, radar systems operate in challenging environments, encountering obstacles such as noise, clutter, and jamming while attempting to detect targets. Noise and clutter represent inherent difficulties associated with radar systems. In contrast, jammers are designed to deceive or disrupt radar operations. As electronic warfare systems continue to advance, the jamming environment has emerged as an area of interest for researchers and nations engaged in electronic warfare. Jamming, a subset of electronic countermeasures (ECM), can be classified into two primary categories based on the mode of attack: deceptive and noise jamming [1].

Noise jamming, one of the earliest techniques employed against radar, involves transmitting high power noise signals to a target receiver to disrupt its functionality. This approach does not necessitate extracting radar parameters or obtaining information about hostile radar, and its implementation is relatively straightforward. However, modern radars are designed to take advantage of coherent processing [2], which allows the suppression of noise signals due to their non-coherence with radar transmit signals. To achieve coherent jamming, repeat-back signals or digital radio frequency memory (DRFM) [3], [4] techniques can be utilized. This type of jammer can generate a coherent signal against radars owing to its ability to transmit replicas of the victim radars' emitted signals. Consequently, they serve as suitable alternatives to deceptive jamming for radars employing frequency modulated continuous wave (FMCW). Another method for deceiving victim radar is to use frequency-domain spoofing for FMCW radars [5], [6]. Rather than using a high-speed analog-to-digital converter (ADC), digital-to-analog converter (DAC), and extensive memory requirements to store the signal, this can be accomplished by adding an intermediate frequency (IF) signal to the victim radar system signal through a low-cost mixer operation. However, in this type of deceptive jamming, the jamming system must possess knowledge of the victim radar's parameters to transmit a

The associate editor coordinating the review of this manuscript and approving it for publication was Brian Ng.

false target signal within a predetermined range. This type of jamming can be subdivided into coherent spoofing and non-coherent spoofing [5].

FMCW radars are extensively used in industrial applications, especially in short-range measurements, owing to their advantages such as low-cost, simple operation, accurate range and velocity measurements. They have wide applications in vehicle collision avoidance systems [7], [8], [9]. Owing to their ability to detect range and velocity even under harsh weather conditions, they are a widely studied topic in research related to autonomous vehicles. Additionally, FMCW radar has various emerging application areas such as human pose estimation, vital signal monitoring, gait monitoring and indoor localization. The proposed millimeter-wave (mmWave)-based assistive rehabilitation system (MARS) [10] pioneered the use of mmWave radar for indoor healthcare, specifically in rehabilitation movements. Human pose estimation using mmWave, RGB camera, and inertial sensors (mRI) [11] extended the approach to multi-modal human pose estimation and established a benchmark for evaluation. Another study [12] combined mmWave radar and camera sensors for multi-object tracking. In a study by authors in [15], vital signal detection of a walking human using FMCW radar was proposed. In [16], another study focused on the estimation of heart rate and breathing rate using mmWave radar. Authors in [17] provided a gait dataset for researchers and proposed a method utilizing deep learning for gait recognition. Furthermore, in [18], a low-cost portable 24-GHz FMCW radar capable of simultaneously recognizing the position and pose of a device-free human in indoor corridor scenes was presented, employing deep learning techniques.

With the increasing use of FMCW radars in both military and civilian applications, immunity to jamming is becoming increasingly important; The increasing utilization of FMCW radars in military and civilian applications emphasizes the growing significance of immunity to jamming. Owing to their immunity to jamming, low probability of intercept (LPI) radar waveform is often preferred. Radar or microwave sensor systems can provide LPI feature using wide-band linear frequency modulation (LFM) against noise jammers. A hostile system may capture the operation frequency band to increase the jamming-to-signal ratio (JSR) using reasonable RF power. Using wide-band LFM signal, the detection ability of the hostile system may be significantly reduced by the radar. The DRFM technique is an indispensable deceptive jamming strategy for wide-band radars. They do not need to know all radar parameters to deceive the victim radar as in the case of frequency-domain spoofing system. To increase immunity against DRFM jammers, several electronic counter-countermeasure (ECCM) techniques can be applied. One of the well known techniques for DRFM jammers is to change the chirp slope. By doing this, false targets can be distinguished from real targets in slow time. Another ECCM technique is frequency hopping. By changing operation frequencies in slow time, false targets can be eliminated with the help of analog filtering for DRFM jammers that attempt to show closer targets. However, the frequency-domain spoofing system can still overcome this ECCM technique because of its ability to add false target to the current chirp signal.

There are several ECCM techniques in the literature based on varying the slope of the chirp signal and frequency hopping [5], [19], [20], [21], [22], [23], [24], [25]. The use of the variable slope of the chirp signal provides different beat signal frequencies in slow time for real targets. It assumes that the jammer signal will not be able to adapt to the current chirp signal for deception purpose. Even if the jammer is able to send the current chirp signal to the victim radar immediately, it can only use the previous chirp signal when it tries to show false target which is closer to the radar than real target [26]. Whereas this assumption holds for DRFM systems, frequency-domain spoofing can still create false targets that appear closer to the radar. However, false targets can be separated from real targets by changing radar parameters in slow time. A hybrid-chirp FMCW radar was proposed in [5] to distinguish false targets from real targets. Whereas the true target beat frequency changes for different slope chirp signals, the spoofing signal frequency is observed to be constant in slow time. Random chirp modulation, which is composed of a changing triangular wave with an up-down or down-up sequence, was suggested as an another ECCM technique in [20] and [21]. The idea behind this technique is based on changing the beat frequency in slow time without an attacker perceiving this variation in the current chirp signal. However, an attacker using two different spoofing systems can deceive this technique [21]. Another technique to resist deception jamming is to apply frequency hopping. BlueFMCW was proposed in [19] as frequency hopping technique, which is applied by dividing the bandwidth into equal sub-intervals. Although the slope remains constant in this technique, random start frequencies were used as an anti-jamming technique. Transmitting chirp signal with different chirp parameters in slow time can be a resistive technique for deception jamming. However, randomly varying parameters in between consecutive slow time measurements such as frequency bins may result in performance degradation in target detection performance [23], [27] or require extra calibration for all frequency bins [5]. It also mitigates obtaining information from slow time signal processing, such as Doppler information [28]. Another important approach of the ECCM technique is to apply phase-coded FMCW (PC-FMCW) signal [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40]. In addition, checking the initial phase of the oscillator can also be an alternative ECCM technique for special types of jammers such as DRFM jammers [41], [42].

This study aims to address the issue of applying a new compound ECCM technique to different types of jammers, including DRFM jammers, non-coherent frequency-domain spoofing, and coherent frequency-domain spoofing.

The proposed method utilizes the initial phase of an oscillator and a phase coded frequency-modulated continuous wave (PC-FMCW) signal in slow time. To the best of our knowledge, no compound ECCM technique has been considered in the literature to counteract different types of jammers. The proposed technique comprises a slow time phase coded signal, which is combined with checking the initial phase of the beat signal. DRFM jammers can be detected by analyzing the changing initial phase of the voltage-controlled oscillator (VCO) for every chirp sequence. Similar to the conventional FMCW radar hardware, this technique does not require any additional hardware component. Additionally, using a PC-FMCW signal in slow time can be used as an ECCM against non-coherent and coherent spoofing. The effectiveness of the proposed method is validated through measurements and simulations. Finally, the advantages and disadvantages of the proposed compound ECCM technique are discussed.

The rest of the paper is organized as follows. In Section II, the theoretical background of the system model and jammer systems for three different jamming scenarios are presented. In Section III, the ECCM technique based on the slow time phase coded signal combined by checking initial phase of beat signal is explained. In Section IV, the proof of concept is presented with measurements and simulations using prototype circuits. Details of the hardware implementation for the measurements are provided in Section IV. A discussion section is also presented in Section IV to evaluate the performance of the proposed ECCM algorithm's. The last section is the conclusion.

II. THEORY OF OPERATION

A. BACKGROUND

A traditional FMCW radar transmits a linear chirp signal in a predetermined bandwidth and receives a delayed replica of the transmitted signal. The beat signal is constructed using a mixing operation between the transmit and receive signals. A frame, composed of beat signal data, is called fast time data. Range evolution is accomplished using signal processing on fast time whereas Doppler velocity is extracted from slow time data which is a combination of fast time data. Fig. 1 shows a schematic of the FMCW radar circuit.

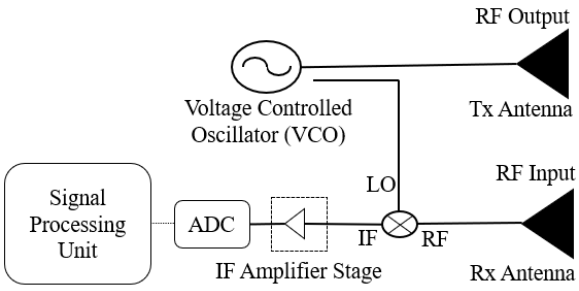


FIGURE 1. Schematic of FMCW radar circuit.

The mathematical model of the transmitted ramp down chirp signal can be written as in [43]

$$x_{T_n}(t) = A_n(t) \times cos(2\pi(f_{max}(t-(n-1)T_{chirp}) - \frac{1}{2}k(t-(n-1)T_{chirp})^2) + \phi_n) \quad (1)$$

where n represents slow time numbering starting from 1, $x_{T_n}(t)$ represents transmitter fast time data, $A_n(t)$ represents the amplitude modulation in the VCO output, and f_{max} is starting frequency of chirp signal, and k is the slope of the chirp signal represented as B/T_{chirp}, B represents bandwidth determined as $f_{max} - f_{min}$, T_{chirp} is the chirp time which is sampled time by ADC, T_{ramp} is the total time for one ramp time which is equal to summation of T_{chirp} and $T_{settling}$ and ϕ_n is the initial phase of chirp signal for different slow time numbers. Fig. 2 shows frequency-time relation of the transmitted chirp signal. It exhibits saw-tooth type frequency modulation. $T_{settling}$ represents the settling time for the steady operation of the VCO.

The received signal is a delayed replica of the transmitted signal. $(t-(n-1)T_{chirp})$ is denoted as t_k for the sake of completeness. Mathematical representation of received signal can be written as

$$x_{R_n}(t) = \sigma \times A_n(t) \times cos(2\pi(f_{max}(t_k-\tau) - \frac{1}{2}k(t_k-\tau)^2) + \phi_n) \quad (2)$$

where σ is the amplitude coefficient of the received signal, τ represents the time delay of the transmitted signal, which is $2\times(R+vt)/c$, R is the target range, v is the radial component of the target's velocity, and c is the speed of light. σ is strongly dependent on the radar cross section of the target.

By using demodulation and low pass filtering, the beat signal (also known as dechirp or deramp signal) can be extracted as a low-frequency component to reduce the sampling rate requirement. The mathematical model of beat signal can be written as follows [35]

$$x_{b_n}(t) = cos(2\pi(f_{max}\tau - t_k(k\tau) + \frac{1}{2}k\tau^2)) \quad (3)$$

where $x_{b_n}(t)$ is the beat signal, τ represents the time delay including the Doppler velocity. The term $\frac{1}{2}k\tau^2$ is typically neglected [35] in low velocity radar applications. Amplitude modulation is also neglected for the sake of simplicity in (3). Using (3), we can equivalently express the beat signal as

$$x_{b_n}(t) = cos(2\pi(f_{max}\tau_0 + f_d t_k - t_k(f_{beat} + k\frac{2v_r t}{c})) \quad (4)$$

where $x_{b_n}(t)$ is the beat signal, and τ_0 represents the time delay without Doppler velocity which is $2\times R/c$, f_d represents the Doppler velocity $f_{max}2v_r/c$ where v_r is the radial velocity and the beat frequency is f_{beat}.

Range and velocity information are included in the beat signal in fast time and slow time respectively [43]. Using fast Fourier transform (FFT), the range-Doppler map can be extracted as illustrated in Fig. 3. The N number FFT is taken in the fast time to extract range information and the M number FFT is taken in slow time to extract the Doppler velocity.

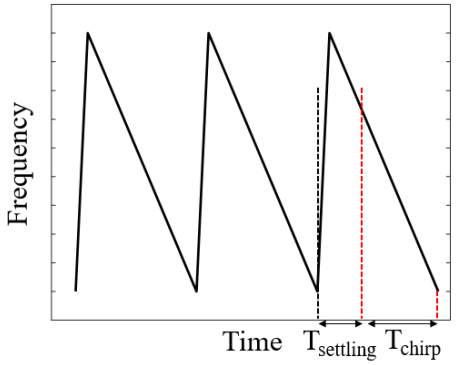


FIGURE 2. Illustration of frequency-time relation of transmitted signal.

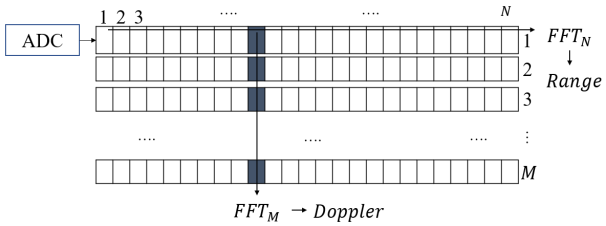


FIGURE 3. Range-Doppler map of FMCW radar.

B. DRFM JAMMER

DRFM jammers can transmit a replica of the received victim radar signal to provide coherent jamming [44]. It can modify some radar parameters such as range, velocity, and radar cross section (RCS) to decept victim radar. However, to create a false target that is closer than real target, the DRFM jammer should follow one chirp behind the radar in slow time [45]. In this study, only closer false targets were investigated. The DRFM model is illustrated in Fig. 4.

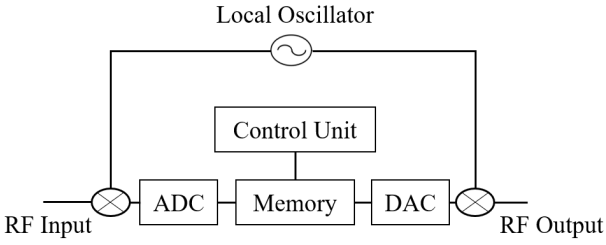


FIGURE 4. Basic DRFM model.

Assuming a perfect DRFM jammer, that can generate false targets with false Doppler velocity, the mathematical model for DRFM jammers can be represented as

$$x_{DJ_{n-1}}(t) = C_n(t) \times cos(2\pi f_{max}(t-\tau_1) - \frac{1}{2}k(t-\tau_1)^2 + \phi_{n-1}) \quad (5)$$

where $x_{DJ_{n-1}}(t)$ represents the DRFM jammer signal that follows the victim radar by one chirp behind in slow time, τ_1 represents the false target delay, and $C_n(t)$ represents the amplitude of the jamming signal. Since it will be multiplied by the current LO signal, the initial phase of the beat signal will vary in slow time although the target Doppler velocity is zero.

C. NON-COHERENT FREQUENCY-DOMAIN SPOOFING

The most important property of frequency-domain spoofing is the generation of a false target without a time delay with nanosecond precision [5], [6]. To realize frequency-domain spoofing, radar signal can be used as the local oscillator (LO) input for the mixer. Automatic gain control (AGC) circuit may require adjusting the LO power in the input of the mixer to maintain a constant insertion loss of mixer, and the mixer's working bandwidth should include the victim radar operation bandwidth. Using a single-sideband (SSB) mixer is also required to configure the output as the upper sideband (USB) or lower sideband (LSB). Thus, the jamming effectiveness can be increased using ECCM techniques. A frequency shift can be added to the IF port of the mixer with a waveform generator using DAC or direct digital synthesis (DDS). Fig. 5 shows a schematic of non-coherent frequency-domain spoofing.

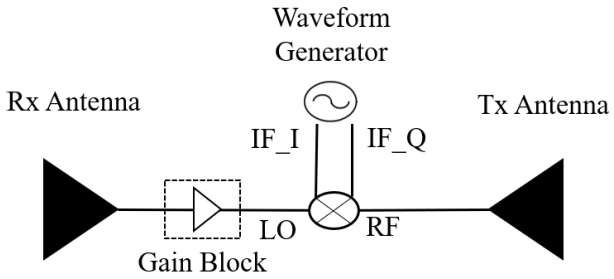


FIGURE 5. Basic non-coherent frequency-domain spoofing circuit schematic.

In this study, spoofing was separated into two parts: coherent and non-coherent. To provide coherency, the spoofing system should know the radar parameters that increase the complexity and cost of the system. The mathematical expression for non-coherent frequency-domain spoofing can be expressed as

$$x_{NCF_n}(t) = D_n(t) \times cos(2\pi(f_{max}(t-\tau) - f_{NCF}t) - \frac{1}{2}k(t-\tau)^2 + \phi_{jamm_n}) \quad (6)$$

where $x_{NCF_n}(t)$ is the non-coherent spoofing signal, f_{NCF} represents the false target frequency shift, $D_n(t)$ represents amplitude modulation of the jamming signal, and ϕ_{jamm_n} is the initial phase of the jamming signal.

D. COHERENT FREQUENCY-DOMAIN SPOOFING

Contrary to non-coherent spoofing, radar parameters especially chirp time should be known in coherent jamming. The initial phase of the spoofing signal should be consistent for each chirp interval. To provide coherency and extract the victim radar parameters, electronic support measurement unit is required. Circuits required to generate spoofing signal will be the same as coherent jamming circuits except for

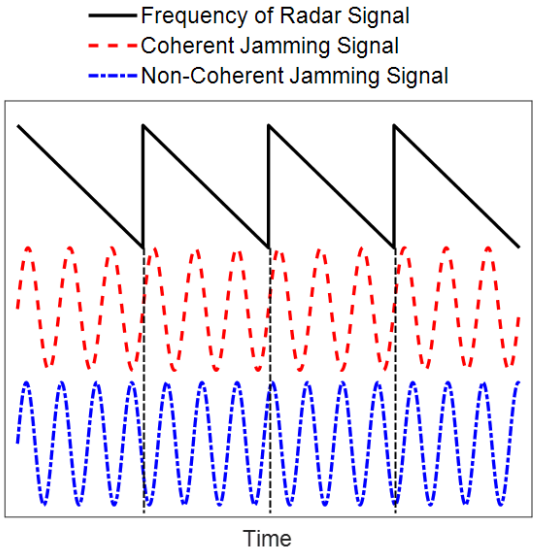


FIGURE 6. Coherent and non-coherent beat signal coming from spoofing unit along with Frequency-Time representation of victim radar signal.

the electronic support unit. The second step is to adjust the frequency of the signal inversely proportional to the chirp time in waveform generator or to maintain initial phase of the spoofing signal constant in slow time. As a result of this process, coherent and non-coherent spoofing can be achieved as illustrated in Fig. 6. Whereas coherent spoofing signals maintain coherency with the radar's transmitted signal, non-coherent spoofing signals lack this property, as depicted in the Fig. 6.

III. PROPOSED ECCM

In the preceding section, three distinct jamming scenarios were presented. To mitigate the effects of these jamming and/or spoofing techniques, a compound ECCM method based on the phase variation of the transmitted signal in slow time was proposed. This paper takes into account the assumption that the chirp time is in a coherent process interval (CPI). There are several advantages of using phase variation as an ECCM method. First, because most FMCW algorithms detect range of the target in the frequency spectrum, phase change has little effect on the detection algorithm. Second, changing the frequency bin in slow time may require recalibration for coupling, noise level, and other factors. Phase variation is also immune to the disadvantages of frequency bin changes. Finally, the jammer system could not predict the initial phase of the beat signal. As a result, applying ECM to an ECCM technique based on phase variation in slow time would be difficult for malicious attacks. Considering all of these benefits, this paper proposes a compound ECCM method based on phase variation in slow time.

A. SLOW TIME PHASE CODED SIGNAL

The slow time phase coded method can be accomplished with a circuit as shown in Fig. 7. In this method, phase variation can be applied before antenna. In this manner, the phase change in the RF signal is transferred to the beat signal in slow time. Radar can adjust randomly or a pre-determined sequence of phase change of the RF signal for each chirp. In this study, only 180° phase variations which is bi-phase modulation were considered. Bi-phase coding (0 and 180-degree phase shift) was chosen over other phase coding techniques due to its enhanced immunity against noise or Doppler shifts, along with simpler implementation in terms of circuit design. With this decision, it is anticipated that the demonstration of the phase coding technique will be facilitated in a simple and efficient manner. In this way, coherent and non-coherent spoofing can be determined by radar. Assuming that a spoofing system will not be able to adapt itself to the phase change at the current chirp signal, the radar will be able to identify false targets. However, this method is not sufficient to determine the DRFM jamming signal because the initial phase of the VCO changes for each chirp. Assuming that DRFM jammers are designed to retransmit the previous signal of the target radar to show closer targets, the phase variation between the initial phase of the previous chirp signal and the current one becomes significant. Radar will not be able to identify phase changes effectively because of uncertainty in the starting point of VCO. In other words, the phase change for the DRFM jamming signal will be probabilistic depending on the random initial phase behavior of the VCO in slow time.

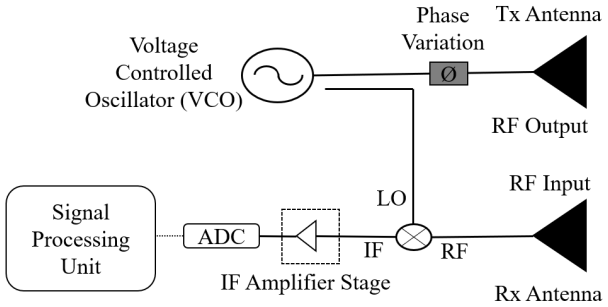


FIGURE 7. Modification for slow time phase coded signal method.

The target beat signals under modification for slow time phase coded method are given in equations (7a), (7b) and (7c) for zero Doppler velocity and different slow time numbers. The beat signals in consecutive slow time numbers are represented as

$$x_{b_1}(t) = cos(2\pi(f_{max_1}\tau_0 - tf_{beat})) \quad (7a)$$

$$x_{b_2}(t) = cos(2\pi(f_{max_2}\tau_0 - (t-1\times T_{ramp})f_{beat})) \quad (7b)$$

$$x_{b_3}(t) = cos(2\pi(f_{max_3}\tau_0 - (t-2\times T_{ramp})f_{beat}) + \pi) \quad (7c)$$

where $x_{b_1}(t)$, $x_{b_2}(t)$ and $x_{b_3}(t)$ represent the different slow time numbering of the beat signal. It can be observed that the beat signal in the third number of slow time has a phase difference of 180° with beat signals in the first and second number of slow time. The amplitude modulation of the beat signal is ignored in this equation for simplicity. Table 1 shows

TABLE 1. Phase representation in slow time for real and false targets for zero doppler velocities.

Slow Time Numbers	Target	Coherent Signal	Non-Coherent Signal	DRFM Jammer
1	$2\pi(\mathrm{f}_{\max_1}\tau_0 - \mathrm{tf}_{\mathrm{beat}})$	$2\pi\mathrm{tf}_{\mathrm{CF}} + \phi_0$	$2\pi\mathrm{tf}_{\mathrm{NCF}} + \phi_1$	$2\pi\mathrm{tf}_{\mathrm{DJ1}} + \phi_4$
2	$2\pi(\mathrm{f}_{\max_2}\tau_0 - \mathrm{tf}_{\mathrm{beat}})$	$2\pi\mathrm{tf}_{\mathrm{CF}} + \phi_0$	$2\pi\mathrm{tf}_{\mathrm{NCF}} + \phi_2$	$2\pi\mathrm{tf}_{\mathrm{DJ2}} + \phi_5$
3	$2\pi(\mathrm{f}_{\max_3}\tau_0 - \mathrm{tf}_{\mathrm{beat}}) + \pi$	$2\pi\mathrm{tf}_{\mathrm{CF}} + \phi_0$	$2\pi\mathrm{tf}_{\mathrm{NCF}} + \phi_3$	$2\pi\mathrm{tf}_{\mathrm{DJ3}} + \phi_6$

the phase of the target and spoofing signals in slow time for a zero Doppler velocity. If the Doppler velocity is considered, the initial phase will change for each chirp. However, considering that the change in Doppler velocity in ramp time is sufficiently small, the initial phase change as a result of the Doppler velocity can be compensated.

B. CHECKING INITIAL PHASE OF BEAT SIGNAL

The aforementioned probabilistic change in the initial phase of the VCO can provide a countermeasure against deceptive jamming. Assuming that the DRFM jammer signal follows one chirp behind the radar signal, the initial phase of the false target generated by DRFM changes for each chirp time as a random process. To explain this phenomenon, the mixing operation of the chirp signal and the previous chirp signal is investigated. The equation for the beat signal as a resulting from DRFM jamming is given as

$$x_{b_{DJ}}(t) = cos(2\pi(f_{max}\tau_1 - f_{DJ}t_k) + \phi_n) \tag{8}$$

where $x_{b_{DJ}}(t)$ DRFM jamming beat signal, f_{DJ} represents the beat frequency of jamming signal, ϕ_n represents the random phase difference as a resulting from the probabilistic change in the VCO. The frequency of the beat signal coming from the DRFM jammer is also a probabilistic parameter because the starting behavior of the VCO will be different for different slow times. Because the DRFM jammer will not be able to predict the VCO initial phase and starting frequency, it will not be easy to use the DRFM jammer for this configuration. As a result, the initial phase of the beat signal remains constant for real targets with zero Doppler velocity.

IV. MEASUREMENTS AND SIMULATIONS

The proof of concept was implemented using both simulations and measurements. In our study, simulations and measurements were conducted in separate scenarios. We performed two distinct measurements, and the results were saved to a text file. Firstly, we measured the beat signal by transmitting it through a 12-meter RF cable, which accurately represents a realistic target. Secondly, we obtained a data set from directly sampled VCO signals, which were then used to create DRFM false targets within the MATLAB simulation environment. Spoofing signals were generated directly within the simulation environment. The measured data from realistic targets were utilized in simulations involving various scenarios, including DRFM false targets, coherent spoofing, and non-coherent spoofing.

A. MEASUREMENTS

The measurement process was partitioned into two parts, each facilitated by a different measurement setup. In the first part, the schematic shown in Fig. 8(a) is implemented using prototype circuits. The VCO was realized using the HMC391 chip from Analog Devices, and to drive the VCO, a driver circuit was designed using the OPA2180 Opamp from Texas Instrument. The VCO tune signal was generated using a 33600A series 120 MHz arbitrary waveform generator (AWG) from Agilent Technologies. At the same time, the AWG is used to provide control signal input to the RF switch, which is HMC349 from Analog Devices. The RF switch was used to choose different paths with nearly 180° phase differences in the center frequency of the RF signal to apply a phase shift for different slow times. Cables with different lengths (4 in and 5 in) were used to provide two different RF paths, with the long cable path denoted as the first path and the short cable path denoted as the second path. To combine these two paths, 3 dB power dividers were used. The experimental setup including the RF switch, which is HMC349 from Analog Devices and 3 dB power divider is shown in Fig. 8(b). Using vector network analyzer and cables of different length, a 180° phase difference was provided, as shown in the measurement in Fig. 8(c). VCO was driven between 5 V and 10 V, providing a signal in 4.3 - 4.5 GHz frequencies with an operational bandwidth of approximately 200 MHz. Whereas 200 μs was the total time to complete one cycle of the ramp, 128 μs was used as the operational chirp time, and the remaining time was used as settling time required for VCO settling. This study did not consider the predistortion of a VCO, which led to the observation of the spectrum spreading effect in both measurements and simulations owing to the non-linear behavior of the VCO. However, this effect did not impede the complete proof of concept of the phase coded algorithm. The RF output was connected to the mixer RF port via a 12-meter cable, with a propagation velocity of 0.85, resulting in an approximately 47 nanosecond time delay, which corresponds to a target distance of 7.06-meter. Our choice of a 12-meter RF cable was due to two considerations: firstly, to prevent spectrum spreading caused by nonlinear behavior of the VCO from affecting our measurements, thereby aiding in the clear demonstration of phase-coded signals; secondly, to align with the typical operational range of short-range radars. The VCO was connected to a 3 dB power divider to sample the local oscillator (LO) signal, and an HMC311 amplifier from Analog Devices was used to drive the mixer. The mixer used in

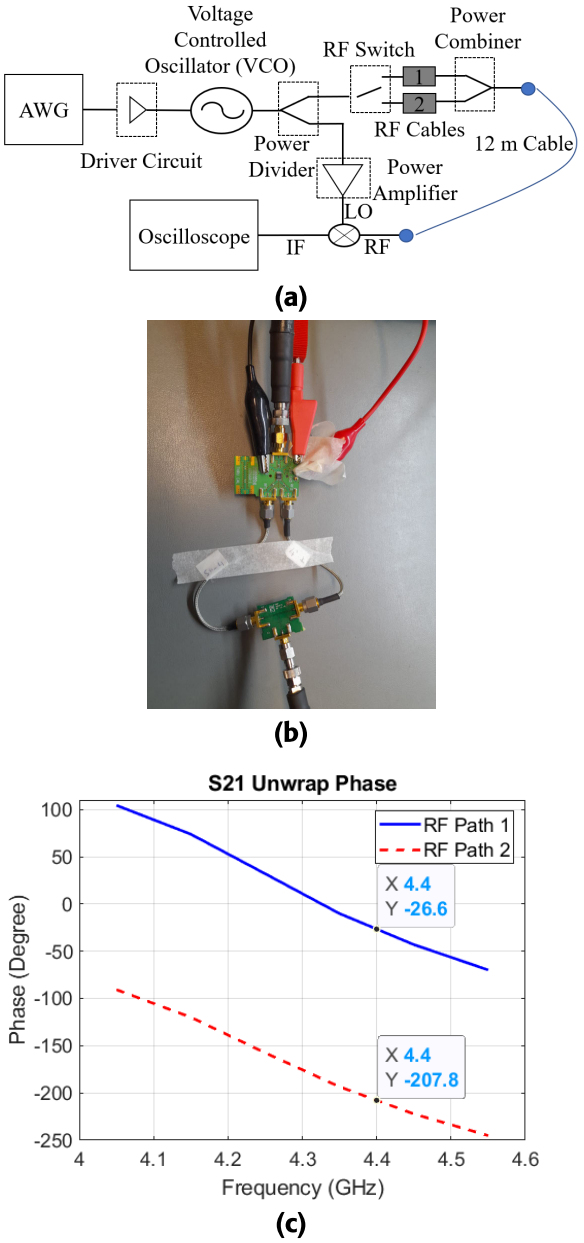


FIGURE 8. Measurement of phase difference in between RF path 1 and 2 (a) Circuit schematic for proposed phase coded signal algorithm (b) Illustration of experiment setup (c) Unwrapped phase measurement of two different RF paths corresponds to 4 and 5 inch RF cables.

this measurement was HMC219B from Analog Devices, and the intermediate frequency (IF) signal was directly connected to an MSOS054A high-definition oscilloscope. The sample rate of the oscilloscope was adjusted to 10 MSPS for this measurement, and the IF signal was recorded for 20 ms. The VCO drive, beat, and RF switch control signals are shown in Fig. 9 for a duration of 1 ms.

The second part of the experiment was conducted in order to generate a down-converted DRFM jammer signal for processing in simulations. To achieve this, the transmitter portion of the schematic in Fig. 8(a) was directly connected to an MSOS054A high-definition oscilloscope to sample the RF

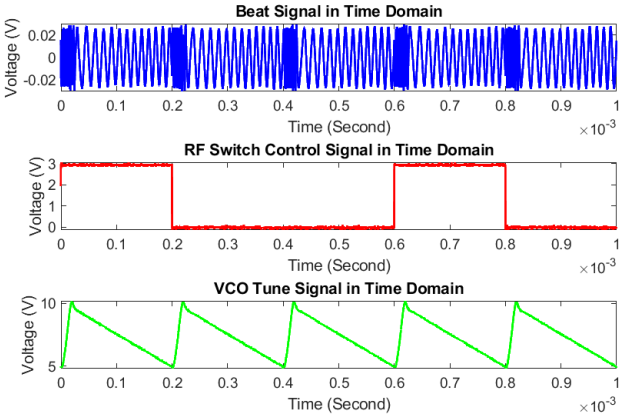
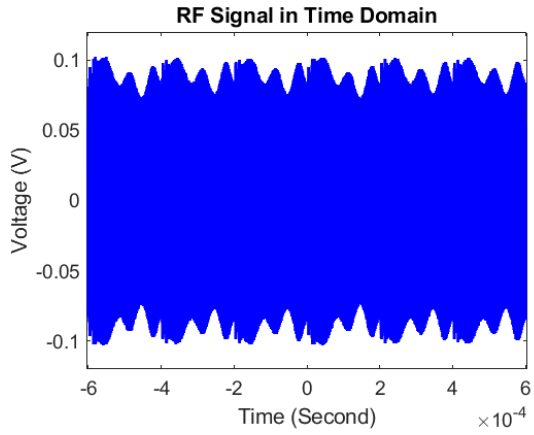


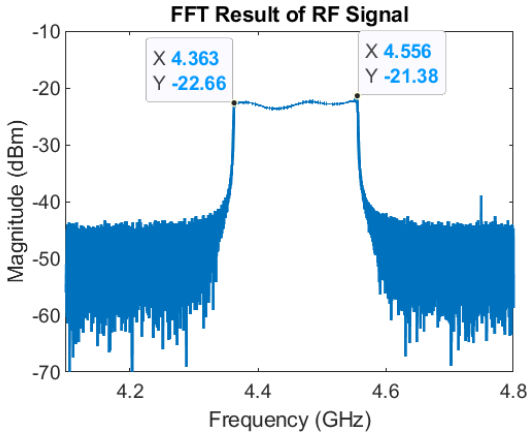
FIGURE 9. Oscilloscope measurement of beat signal coming from 12-meter RF cable, VCO tune signal in between 5 V and 10 V and RF switch control signal.

output signal. Whereas the common approach for sampling involves down-conversion of the signal to reduce the sampling rate and memory requirements, direct sampling was preferred in this study to more accurately simulate malicious DRFM attacks in the simulation environment and account for the starting behavior of the VCO. The oscilloscope's sampling rate was set to its highest level of 20 gigasamples per second, and the time window was set between -0.6 ms and 0.6 ms, resulting in a total sampled time of 1.2 ms and 24 mega points. The measurement results are shown in Fig. 10(a). The time-domain measurement, FFT results, and experimental setup are shown in Fig. 10(a), Fig. 10(b), and Fig. 10(c), respectively. The VCO bandwidth ranged from 4.3 GHz to 4.5 GHz, which is nearly 200 MHz. Measurements were performed in the same configuration for five ramp time, and the chosen paths for these measurements are shown in Fig. 9 as the first path (4 inch cable), first path (4 inch cable), second path (5 inch cable), first path (4 inch cable), etc.

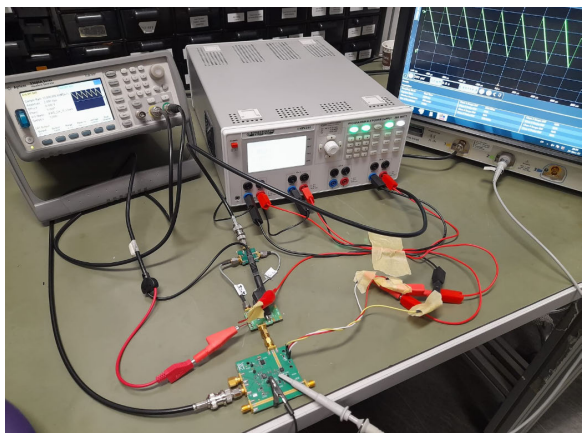
The beat signal for the 12-meter RF cable in the time domain, measured range, and initial phase change are shown in Figures 11(a), 11(b) and 11(c) respectively. The specific arrangement of separating the sampling time and chirp time in our study is driven by the need to account for the settling time requirements of the VCO as shown in Fig. 11(a). Abrupt changes in the VCO tune signal can lead to instability and frequency spreading of the beat signal. To ensure a stable and accurate VCO frequency output, we allocated a settling time within the chirp period. Our chosen 200 μs chirp time with a 128 μs sampling time allows for a realistic and clear demonstration of the beat signal, with 72 μs allocated for VCO settling. A threshold level of -15 dBm was selected to observe the effects of background noise on the phase-coded signal, with an SNR of 8 dB considered as low SNR. The X-axis represents range values, while the Y-axis represents the initial phase of frequency bins. The initial phase corresponds to the 7.23-meter range is shown in the Fig. 11(c). The FFT phase has been shown only for the neighboring frequency bins of the



(a)

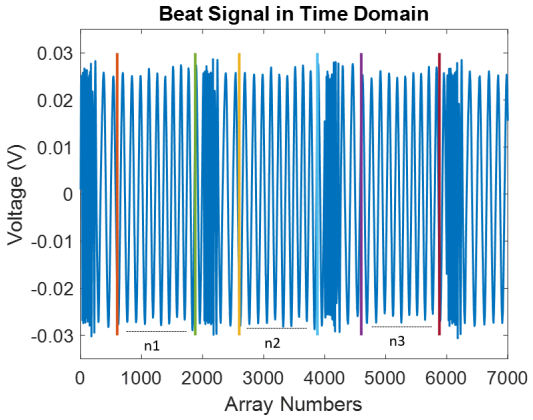


(b)

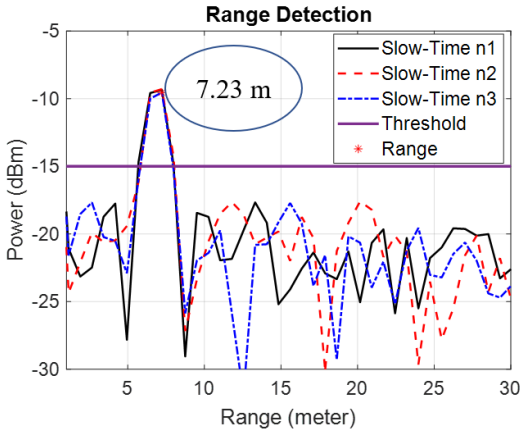


(c)

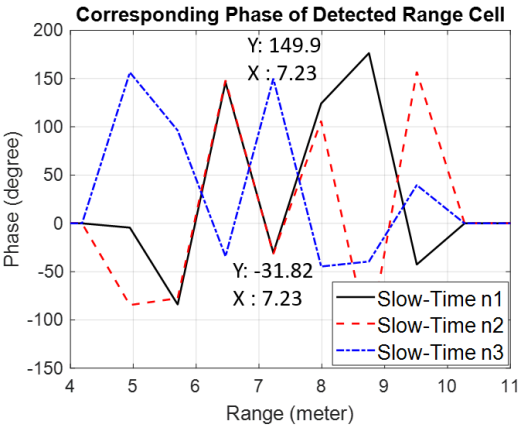
FIGURE 10. Direct sampling of RF signal coming from transmitter part of circuit shown in Fig. 8(a) (a) Oscilloscope measurement of RF output signal (b) Spectrum of RF output signal for 128 microsecond frame and 20 GSPS sampling rate (c) Illustration of experiment setup for RF direct sampling.



(a)



(b)



(c)

FIGURE 11. Beat signal representation corresponding to 12 m RF cable both in time and frequency domain (a) Time domain representation of beat signal for different slow time numbers, n_1, n_2 and n_3. (b) Range spectrum of beat signal for range detection with threshold settled higher than 10 dB of noise floor (c) Initial phase of frequency bins corresponding to detected range cell and neighbors of detected range cell for different slow times.

detected range cells to make the graph more comprehensible. The other frequency bins are filled with zeros.

B. SIMULATIONS

The beat signal was measured using a 12 m RF cable, and the corresponding range was determined to be 7.23-meter. The beat signal was then exported to a text file from the oscilloscope for use in simulations. Malicious attacks were simulated in MATLAB, and the range detection algorithm

was tested in a simulation environment. White Gaussian noise was added to the beat signal, to ensure equal signal-to-noise ratios (SNR) for all jamming scenarios. Initially, a non-coherent spoofing signal was generated in MATLAB with a sampling rate of 10 MSPS and sent to the detection algorithm in combination with the measured beat signal. The frequency of the spoofing signal was adjusted to 39 kHz, which corresponds to a distance of 3.42-meter. To better observe the spoofing and beat signals in the figure, the time interval outside the chirp time is filled with zeros. The non-coherent spoofing signal and beat signal in the time domain, the measured range, and the initial phase change in the frequency domain for different slow times are shown in Fig. 12(a), Fig. 12(b), and Fig. 12(c), respectively.

Second, a coherent spoofing signal was generated in the simulation environment with the same sampling rate of 10 MSPS in MATLAB and was then combined with the measured beat signal in the detection algorithm. The spoofing signal frequency was adjusted to 39 kHz, corresponding to a distance of 3.42-meter, as in the case of non-coherent spoofing. To simplify the illustration, the time interval outside the chirp time was filled with zero to observe only the spoofing and beat signals in Fig. 13(a). The coherent spoofing and beat signals in the time domain, measured range, and initial phase change in the frequency domain for different slow times are shown in Fig. 13(a), Fig. 13(b), and Fig. 13(c), respectively.

Third, a DRFM jamming signal is simulated in this study. The DRFM jamming signal was created by assuming that it follows one chirp behind the LO signal, and the IF signal was constructed by multiplying the LO signal with one chirp behind the RF signal. The RF signal is obtained via direct sampling of the RF output, as explained in the measurement section. To simulate the DRFM jamming signal, the current LO signal was multiplied by the RF signal, one chirp behind in the simulation domain. The aim of this simulation was to realize VCO drift and observe its effect of VCO drift on the jamming signal. Because of the VCO drift, both the frequency and initial phase of the jamming signal exhibit a significant change in slow time. Because the jamming signal follows the RF signal with $n-1$ in slow time, the coherency of the jamming signal is limited or completely lost. Even if there was no drift in the initial VCO frequency, the initial phase of the VCO would differ in the slow time intervals. The jamming signal was created in the simulation domain with a 22.6 ns delay, which corresponds to a 3.42-meter range. In other words, the LO signal was multiplied with one chirp behind the RF signal with a 22.6 ns delay. The IF signal was downsampled to create an equal-sized frame with the beat signal measured by the oscilloscope. Low-pass filtering was applied to the IF signal to eliminate high-frequency components from the multiplication operation. In the measurement, filtering was implemented for the beat signal coming from the 12-meter RF cable using the oscilloscope built-in filtering, which has a 20 MHz cut-off frequency. The DRFM jamming signal was added to the beat signal and sent to the detection algorithm. Six different consecutive slow time simulations were performed to clearly observe the effect of VCO drift. Because of the VCO drift, the jamming signal was not observed at

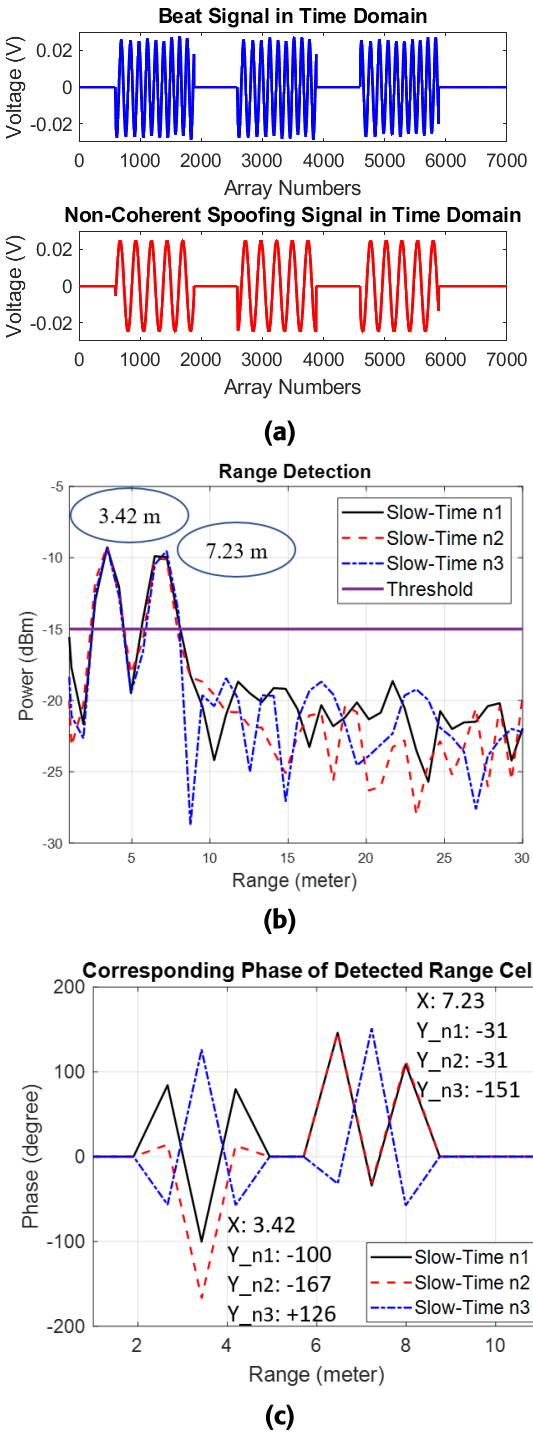
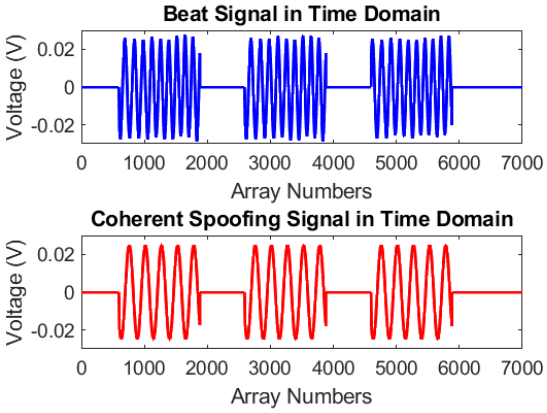
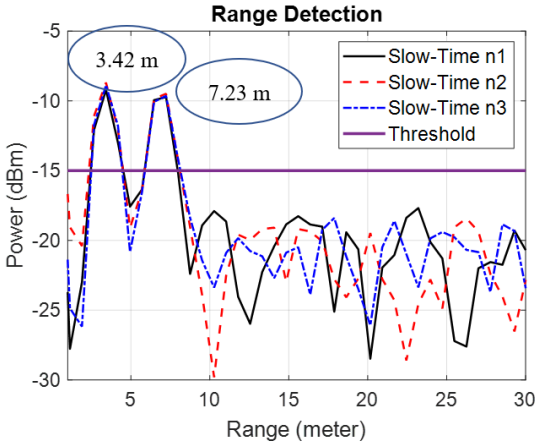


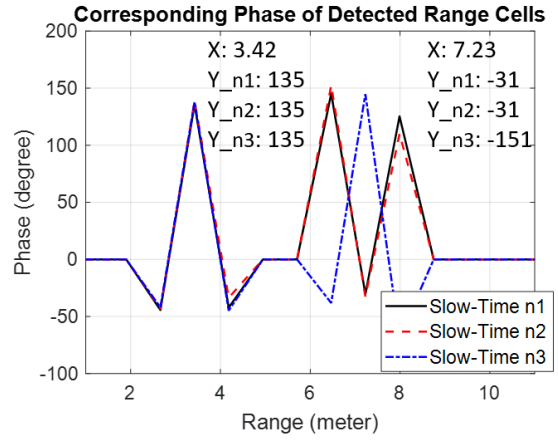
FIGURE 12. Beat signals representation corresponding to 12 m RF cable and non-coherent frequency domain spoofing both in time and frequency domain (a) Time domain representation of beat signals corresponding to 12 m RF cable and non-coherent spoofing signal for different slow time numbers, n_1, n_2 and n_3. (b) Range spectrum of beat signal for range detection with threshold settled higher than 10 dB of noise floor (c) Initial phase of frequency bins corresponding to detected range cell and neighbors of detected range cell for different slow times.



(a)

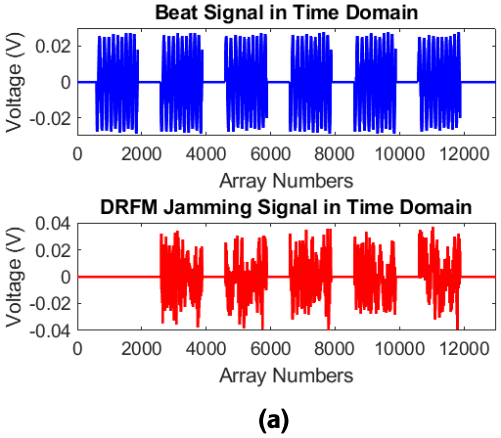


(b)

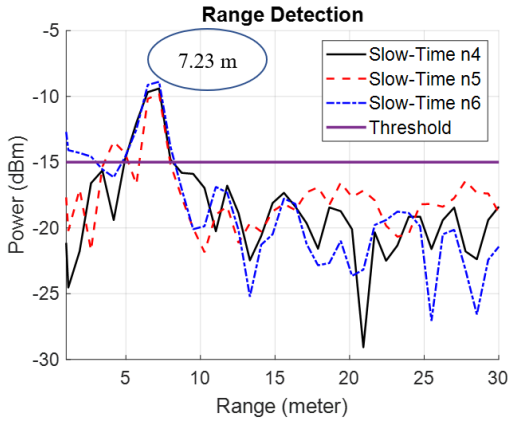


(c)

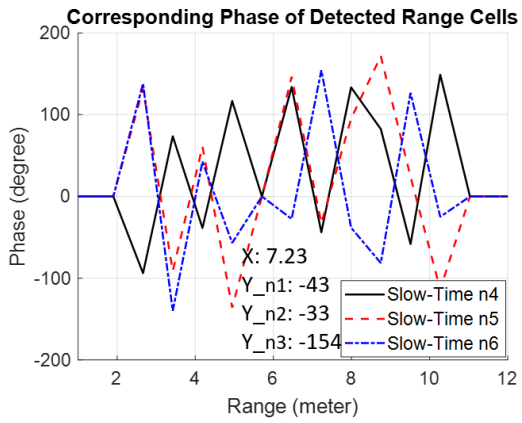
FIGURE 13. Beat signal representation corresponding to 12 m RF cable and coherent frequency domain spoofing both in time and frequency domain (a) Time domain representation of beat signals corresponding to 12 m RF cable and coherent spoofing signal for different slow time numbers, n_1, n_2 and n_3. (b) Range spectrum of beat signal for range detection with threshold settled higher than 10 dB of noise floor (c) Initial phase of frequency bins corresponding to detected range cell and neighbors of detected range cell for different slow times.



(a)



(b)



(c)

FIGURE 14. Beat signal representation corresponding to 12 m RF cable and DRFM jamming both in time and frequency domain (a) Time domain representation of signals corresponding to 12 m RF cable and DRFM jamming for different slow time numbers, n_2, n_3, n_4, n_5 and n_6. (b) Range spectrum of beat signal for range detection with threshold settled higher than 10 dB of noise floor (c) Initial phase of frequency bins corresponding to detected range cell and neighbors of detected range cell for different slow times.

the desired or created frequency for every simulations. The DRFM jamming signal and beat signal coming from the 12-meter RF cable in the time domain, measured range, and initial phase change in the frequency domain for different slow times are shown in Fig. 14(a), Fig. 14(b), and Fig. 14(c).

TABLE 2. Measured ranges for different malicious attacks with/out ECCM.

Frequency Bin Numbers	Range (m)	Percentage of detected range cell out of 30 measurements under coherent spoofing (Target @ 3.42 Meter) with 12 meter RF cable (Target @ 7.06 meter)		Percentage of detected range cell out of 30 measurements under non-coherent spoofing (Target @ 3.42 Meter) with 12 meter RF cable (Target @ 7.06 meter)		Percentage of detected range cell out of 30 measurements under DRFM jamming (Target @ 3.42 Meter) with 12 meter RF cable (Target @ 7.06 meter)	
		without ECCM	with ECCM	without ECCM	with ECCM	without ECCM	with ECCM
4	2.66	0	0	0	0	20	0
5	3.42	100	0	100	0	3.3	0
6	4.18	0	0	0	0	3.3	0
7	4.94	0	0	0	0	3.3	0
9	6.46	3.3	0	3.3	0	0	0
10	7.23	96.7	90	96.7	90	100	90
12	8.75	0	0	0	0	10	0
17	12.55	0	0	0	0	6.6	0

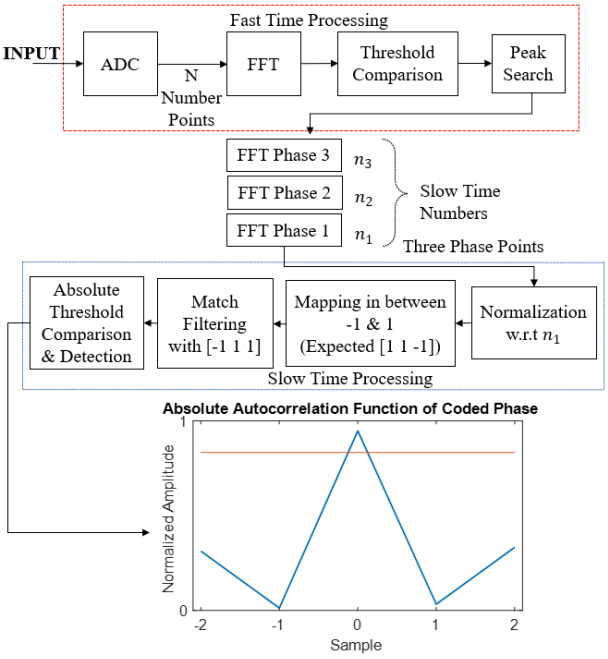


FIGURE 15. Detection algorithm for phase coded signal.

The proposed technique for detecting phase coded signals consists of both fast and slow time processing. A block diagram of the detection algorithm is shown in Fig. 15. Fast time processing is based on the FFT, threshold comparison, and peak search functions, which are applied to an N-point frame. For these simulations, the threshold value was set to 10 dB higher than the noise floor, which was equal to -15 dBm. In other words, if the SNR of the frequency bins was higher than 10 dB above the noise floor, it was considered the measured range. The transmission code used for three consecutive slow time numbers was [1 1 -1], and was used to decode the incoming signal. Normalization was performed with respect to the initial phase of the first slow time. The normalized slow time initial phase information is mapped to 1 and -1 during the decoding process. Match filtering with [-1 1 1] was applied to the decoded signal to generate an absolute autocorrelation function. The final step of the proposed detection algorithm is a threshold comparison of the autocorrelation function.

C. DISCUSSIONS

This study aims to demonstrate the effectiveness of the proposed ECCM technique through both measurements and simulations. Thirty simulations were conducted, covering DRFM jamming, non-coherent spoofing, and coherent spoofing scenarios separately. The range detection outcomes from these simulations were tabulated in Table 2. Throughout all simulations, the false target consistently appeared at 3.42-meter, while the true target remained at 7.06-meter. The table provides information on the frequency bin numbers and their corresponding range cells. Moreover, the table presents the results in terms of the percentage of detected ranges, considering various ECM techniques, both with and without ECCM implemented. The fast-time processing approach was used as the detection algorithm without ECCM. The simulations showed a 90% probability of detecting the true target range with ECCM under ECM. However, a miss detection occurred due to the detection of one of the measurements as 6.43-meter instead of 7.23-meter when using ECCM. This was attributed to the disturbance of the initial phase of different frequency bins, affecting the coding and consequently resulting in incorrect range detection for three slow time numbers. Further improvements in the detection algorithm are necessary to address this issue.

The simulation of the DRFM jammer scenario consider the assumption that the hostile system shows a closer target. This assumption was made to exploit the initial phase difference between the previous and current chirps. The success of the ECCM algorithm in detecting false targets that are displayed farther than the real target depends on the phase noise of the hostile system. However, the incoming signal from DRFM jammers can still deceive the radar. Other ECCM techniques, such as frequency hopping or slope variation, also have vulnerabilities to DRFM jammers attempting to show a false target farther than the real target. The use of phase coded ECCM techniques may be advantageous because of their dependence on the phase noise characteristics of the DRFM system.

To provide phase coding, this study employed a simple coding scheme [1 1 -1], which is a well-known Barker code scheme. The length of the code was chosen as three to decrease the Doppler velocity effect. Shortening the code length decreases the effect of the Doppler velocity. However, to increase the robustness against noise, a longer code such as an 11 chip Barker sequence may be used. Nevertheless, using a longer code may result in computational difficulties and the loss of slow time information, such as Doppler velocity.

V. CONCLUSION

In this study, a compound electronic counter-counter measure (ECCM) technique for FMCW radars was developed to mitigate different jamming scenarios, including coherent and non-coherent spoofing, and DRFM jamming. The proposed technique is based on phase coding in slow time and checking the initial phase of the baseband return signal. Experimental validation was conducted using a measurement setup operating at 4.3-4.5 GHz and a 12-meter RF cable to emulate a real target. Results from simulated jamming scenarios in MATLAB showed the effectiveness of the phase-coded algorithm as an ECCM technique.

Future research should consider incorporating Doppler velocity and conducting outdoor experiments to validate the proposed technique. Moreover, it is important to investigate the mitigation effect of the phase-coded technique on DRFM jammers that aim to show larger range targets. Additionally, improvements can be made to consider the dependency of the DRFM scenario phase noise on the phase-coded algorithm. Overall, the results of this study suggest that the proposed compound ECCM technique based on phase coding in slow time can provide satisfactory performance in various jamming scenarios, making it a promising area for further investigation in the field of FMCW radar.

ACKNOWLEDGMENT

The authors would like to thank ChatGPT, a large language model trained by OpenAI, for providing invaluable assistance in proofreading their manuscript and correcting grammatical mistakes and also would like to thank ChatGPT's contribution in helping them create some sentences in their manuscript. ChatGPT's suggestions greatly improved the clarity and readability of their article.

REFERENCES

[1] L. D. Adamy, *EW 101 A First Course in Electronic Warfare*. Norwood, MA, USA: Artech House, 2001, pp. 178–222.

[2] S. Han, L. Yan, Y. Zhang, P. Addabbo, C. Hao, and D. Orlando, "Adaptive radar detection and classification algorithms for multiple coherent signals," *IEEE Trans. Signal Process.*, vol. 69, pp. 560–572, Dec. 2021, doi: 10.1109/TSP.2020.3047523.

[3] P. E. Pace, *Developing Digital RF Memories and Transceiver Technologies for Electromagnetic Warfare*. Norwood, MA, USA: Artech House, 2022.

[4] S. J. Roome, "Digital radio frequency memory," *IEEE Electron. Commun. Eng. J.*, vol. 2, no. 4, pp. 147–153, Aug. 1990, doi: 10.1049/ecej:19900035.

[5] 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, doi: 10.1109/TMTT.2021.3115804.

[6] P. Nallabolu, D. Rodriguez, and C. Li, "Emulation and malicious attacks to Doppler and FMCW radars for human sensing applications," *IEEE Trans. Microw. Theory Techn.*, vol. 71, no. 2, pp. 805–817, Feb. 2023, doi: 10.1109/TMTT.2022.3208026.

[7] 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.

[8] B.-H. Ku, P. Schmalenberg, O. Inac, O. D. Gurbuz, J. S. Lee, K. Shiozaki, and G. M. Rebeiz, "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.

[9] C. Li, Z. Peng, T. Huang, T. Fan, F. Wang, T. Horng, J. Muñoz-Ferreras, R. Gómez-García, L. Ran, and J. Lin, "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.

[10] A. Sizhe and U. Y. Ogras, "MARS: mmWave-based assistive rehabilitation system for smart healthcare," *ACM Trans. Embedded Comput. Syst.*, vol. 20, no. 5s, pp. 1–22, 2021.

[11] S. An, Y. Li, and U. Ogras, "MRI: Multi-modal 3D human pose estimation dataset using mmWave, RGB-D, and inertial sensors," 2022, *arXiv:2210.08394*.

[12] A. Sengupta, L. Cheng, and S. Cao, "Robust multiobject tracking using mmWave radar-camera sensor fusion," *IEEE Sensors Lett.*, vol. 6, no. 10, pp. 1–4, Oct. 2022.

[13] R. Zhang and S. Cao, "Extending reliability of mmWave radar tracking and detection via fusion with camera," *IEEE Access*, vol. 7, pp. 137065–137079, 2019, doi: 10.1109/ACCESS.2019.2942382.

[14] S. An and U. Y. Ogras, "Fast and scalable human pose estimation using mmWave point cloud," in *Proc. 59th ACM/IEEE Design Autom. Conf.*, Jul. 2022, pp. 889–894.

[15] Y. Hu and T. Toda, "Remote vital signs measurement of indoor walking persons using mm-Wave FMCW radar," *IEEE Access*, vol. 10, pp. 78219–78230, 2022, doi: 10.1109/ACCESS.2022.3193789.

[16] M. Alizadeh, G. Shaker, J. C. M. D. Almeida, P. P. Morita, and S. Safavi-Naeini, "Remote monitoring of human vital signs using mm-Wave FMCW radar," *IEEE Access*, vol. 7, pp. 54958–54968, 2019, doi: 10.1109/ACCESS.2019.2912956.

[17] Z. Meng, S. Fu, J. Yan, H. Liang, A. Zhou, S. Zhu, H. Ma, J. Liu, and N. Yang, "Gait recognition for co-existing multiple people using millimeter wave sensing," in *Proc. AAAI Conf. Artif. Intell.*, 2020, pp. 849–856.

[18] S. Yang and Y. Kim, "Single 24-GHz FMCW radar-based indoor device-free human localization and posture sensing with CNN," *IEEE Sensors J.*, vol. 23, no. 3, pp. 3059–3068, Feb. 2023, doi: 10.1109/JSEN.2022.3227025.

[19] T. Moon, J. Park, and S. Kim, "BlueFMCW: Random frequency hopping radar for mitigation of interference and spoofing," *EURASIP J. Adv. Signal Process.*, vol. 2022, no. 1, pp. 1–17, Jan. 2022, doi: 10.1186/s13634-022-00838-7.

[20] 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.

[21] S. Nashimoto, D. Suzuki, N. Miura, T. Machida, K. Matsuda, and M. Nagata, "Low-cost distance-spoofing attack on FMCW radar and its feasibility study on countermeasure," *J. Cryptograph. Eng.*, vol. 11, no. 3, pp. 289–298, Jan. 2021, doi: 10.1007/s13389-020-00252-5.

[22] B. Tang, W. Huang, and J. Li, "Slow-time coding for mutual interference mitigation," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Proces. (ICASSP)*, Sep. 2018, pp. 6508–6512, doi: 10.1109/ICASSP.2018.8461806.

[23] S. Jin, J. H. Park, and S. Roy, "Slow-time waveform randomization performance under incoherent FMCW radar interference," in *Proc. IEEE 94th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2021, pp. 1–7, doi: 10.1109/VTC2021-Fall52928.2021.9625437.

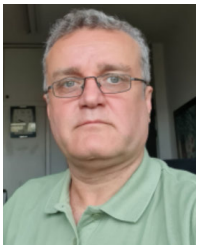
[24] V. Venkatesh, L. Li, M. McLinden, M. Coon, G. M. Heymsfield, S. Tanelli, and H. Hovhannisyan, "A frequency diversity algorithm for extending the radar Doppler velocity Nyquist interval," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 56, no. 3, pp. 2462–2470, Jun. 2020, doi: 10.1109/TAES.2019.2958191.

[25] J. Schuerger and D. Garmatyuk, "Performance of random OFDM radar signals in deception jamming scenarios," in *Proc. IEEE Radar Conf.*, May 2009, pp. 1–6, doi: 10.1109/RADAR.2009.4977015.

[26] J. Akhtar, "Orthogonal block coded ECCM schemes against repeat radar jammers," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 45, no. 3, pp. 1218–1226, Jul. 2009, doi: 10.1109/TAES.2009.5259195.
[27] M. Rameez, M. Dahl, and M. I. Pettersson, "Autoregressive model-based signal reconstruction for automotive radar interference mitigation," *IEEE Sensors J.*, vol. 21, no. 5, pp. 6575–6586, Mar. 2021, doi: 10.1109/JSEN.2020.3042061.
[28] A. Bourdoux and M. Bauduin, "Near-optimal range migration and Doppler ambiguity compensation for FMCW radars," in *Proc. IEEE Radar Conf. (RadarConf)*, Mar. 2022, pp. 1–6, doi: 10.1109/RadarConf2248738.2022.9764358.
[29] F. Uysal, "Phase-coded FMCW automotive radar: System design and interference mitigation," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 270–281, Jan. 2020, doi: 10.1109/TVT.2019.2953305.
[30] J. Reneau and R. R. Adhami, "Phase-coded LFMCW waveform analysis for short range measurement applications," in *Proc. IEEE Aerosp. Conf.*, Jun. 2014, pp. 1–6, doi: 10.1109/AERO.2014.6836285.
[31] U. Kumbul, N. Petrov, C. S. Vaucher, and A. Yarovoy, "Receiver structures for phase modulated FMCW radars," in *Proc. 16th Eur. Conf. Antennas Propag. (EuCAP)*, Mar. 2022, pp. 1–5, doi: 10.23919/EuCAP53622.2022.9769268.
[32] L. Mu, T. Xiangqian, S. Ming, and Y. Jun, "Research on key technologies for collision avoidance automotive radar," in *Proc. IEEE Intell. Vehicles Symp.*, Jun. 2009, pp. 233–236, doi: 10.1109/IVS.2009.5164283.
[33] M. Soumekh, "SAR-ECCM using phase-perturbed LFM chirp signals and DRFM repeat jammer penalization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 42, no. 1, pp. 191–205, Jan. 2006, doi: 10.1109/TAES.2006.1603414.
[34] U. Kumbul, N. Petrov, C. S. Vaucher, and A. Yarovoy, "Smoothed phase-coded FMCW: Waveform properties and transceiver architecture," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 2, pp. 1720–1737, Apr. 2023, doi: 10.1109/TAES.2022.3206173.
[35] F. Lampel, A. Alvarado, and F. M. J. Willems, "Dispersion compensation for phase-coded FMCW radars," in *Proc. 23rd Int. Radar Symp. (IRS)*, Oct. 2022, pp. 36–41.
[36] J. Overdevest, F. Jansen, F. Uysal, and A. Yarovoy, "Doppler influence on waveform orthogonality in 79 GHz MIMO phase-coded automotive radar," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 16–25, Jan. 2020, doi: 10.1109/TVT.2019.2951632.
[37] U. Kumbul, N. Petrov, F. van der Zwan, C. S. Vaucher, and A. Yarovoy, "Experimental investigation of phase coded FMCW for sensing and communications," in *Proc. 15th Eur. Conf. Antennas Propag. (EuCAP)*, Mar. 2021, pp. 1–5, doi: 10.23919/EuCAP51087.2021.9411464.
[38] J. Zhang, D. Zhu, and G. Zhang, "New antivelocity deception jamming technique using pulses with adaptive initial phases," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 2, pp. 1290–1300, Apr. 2013, doi: 10.1109/TAES.2013.6494414.
[39] F. Uysal and S. Orru, "Phase-coded FMCW automotive radar: Application and challenges," in *Proc. IEEE Int. Radar Conf. (RADAR)*, Apr. 2020, pp. 478–482, doi: 10.1109/RADAR42522.2020.9114798.
[40] R. Jason and R. Adhami, "Design of a short range continuous wave compound phase coded linear frequency modulation radar sensor," *Prog. Electromagn. Res. B*, vol. 82, pp. 115–135, 2018, doi: 10.2528/PIERB18082006.
[41] J. Sui, Z. Liu, X. Wei, X. Li, B. Peng, and D. Liao, "Velocity false target identification in random pulse initial phase radar based on compressed sensing," in *Proc. 3rd Int. Workshop Compressed Sens. Theory Appl. Radar, Sonar Remote Sens. (CoSeRa)*, Jun. 2015, pp. 179–183, doi: 10.1109/COSERA.2015.7330288.
[42] W. Xiong, X. Wang, and G. Zhang, "Cognitive waveform design for anti-velocity deception jamming with adaptive initial phases," in *Proc. IEEE Radar Conf. (RadarConf)*, May 2016, pp. 1–5, doi: 10.1109/RADAR.2016.7485306.
[43] M. Song, J. Lim, and D.-J. Shin, "The velocity and range detection using the 2D-FFT scheme for automotive radars," in *Proc. 4th IEEE Int. Conf. Netw. Infrastruct. Digit. Content*, Sep. 2014, pp. 507–510, doi: 10.1109/ICNIDC.2014.7000356.
[44] Z. Guan, Y. Chen, P. Lei, D. Li, and Y. Zhao, "Application of hash function on FMCW based millimeter-wave radar against DRFM jamming," *IEEE Access*, vol. 7, pp. 92285–92295, 2019, doi: 10.1109/ACCESS.2019.2928000.
[45] S. Cheng, X. Luo, C. Dai, and X. Hao, "A novel anti-repeat jamming approach for frequency modulation fuze," in *Proc. IEEE Int. Conf. Unmanned Syst. (ICUS)*, Oct. 2019, pp. 233–238, doi: 10.1109/ICUS48101.2019.8995917.
[46] G. K. Lewis, I. J. Bahl, E. L. Griffin, and E. R. Schineller, "GaAs MMIC's for digital radio frequency memory (DRFM) subsystems," *IEEE Trans. Microw. Theory Techn.*, vol. MTT-35, no. 12, pp. 1477–1485, Dec. 1987, doi: 10.1109/TMTT.1987.1133878.
[47] C. M. Kwak, "Application of DRFM in ECM for pulse type radar," in *Proc. 34th Int. Conf. Infr., Millim., THz. Waves*, Sep. 2009, pp. 1–2, doi: 10.1109/ICIMW.2009.5324673.
[48] R. Komissarov and A. Wool, "Spoofing attacks against vehicular FMCW radar," in *Proc. 5th Workshop Attacks Solutions Hardw. Secur.*, Nov. 2021, pp. 91–97, doi: 10.1145/3474376.3487283.

DOĞANCAN ESER (Student Member, IEEE) received the B.S. and M.S. degrees from the Electrical and Electronics Engineering Department, Middle East Technical University, Turkey, in 2016 and 2019, respectively, where he is currently pursuing the Ph.D. degree.

From 2016 to 2020, he was an Electromagnetic Design Engineer with Meteksan Defence. He is also a Hardware Design Engineer with PRF Development and Research Company, where he is responsible for hardware design, power amplifiers, and electronic warfare techniques. His Ph.D. research focuses on electronic counter-counter measure (ECCM) techniques for frequency-modulated continuous-wave (FMCW) radars.



ŞİMŞEK DEMİR (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees from the Electrical and Electronics Engineering Department, Middle East Technical University, Turkey, in 1991, 1993, and 1998, respectively.

During his Ph.D. studies, he joined the International Research Center for Telecommunication Transmission and Radar, Technische Universiteit Delft, The Netherlands, as a Researcher. He started his academic career with Middle East Technical University as a Research Assistant, in 1995, and became an Assistant Professor, in 2000. He was promoted to an associate professor, in 2006, and then to a full professor, in 2013. He founded PRF Development and Research Company, in 2013. His research interests include radar, microwave circuit design, power amplifiers, antennas, and RF MEMS.

SENCER KOÇ (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees from the Electrical and Electronics Engineering Department, Middle East Technical University, Turkey, in 1979, 1983, and 1987, respectively.

He has been a Full Professor with the Electrical and Electronics Engineering Department, Middle East Technical University, since 2010. His research interests include radar systems, radar signal processing, antennas, computational electromagnetic, and RF MEMS. He has worked on many projects related to these fields and has received funding from various sources, including government agencies and private companies.