Spoofing Attacks to Radar Motion Sensors with Portable RF Devices

Daniel Rodriguez
Electrical and Computer Engineering Department
Texas Tech University
Lubbock, TX, USA
https://orcid.org/0000-0001-7215-0831

Jing Wang
Electrical and Computer Engineering Department
Texas Tech University
Lubbock, TX, USA
https://orcid.org/0000-0003-4552-0352

Changzhi Li
Electrical and Computer Engineering Department
Texas Tech University
Lubbock, TX, USA
https://orcid.org/0000-0003-2188-4506

2021 IEEE Radio and Wireless Symposium (RWS) | 978-1-7281-8062-5/20/$31.00 ©2021 IEEE | DOI: 10.1109/RWS50353.2021.9360393

***Abstract*—Radar sensors have shown great potential for surveillance and security authentication applications. However, a thorough analysis of their vulnerability to spoofing or replay attacks has not been performed yet. In this paper, the feasibility of performing spoofing attacks to radar sensor is studied and experimentally verified. First, a simple binary phase-shift keying system was used to generate artificial spectral components in the radar's demodulated signal. Additionally, an analog phase shifter was driven by an arbitrary signal generator to mimic the human cardio-respiratory motion. Characteristic time and frequency domain cardio-respiratory human signatures were successfully generated, which opens possibilities to perform spoofing attacks to surveillance and security continuous authentication systems based on microwave radar sensors.**

Keywords—Biometrics, continuous authentication, Doppler radar, radar sensors, spoofing attacks.

I. Introduction

Doppler and interferometric radars are being widely studied for sensing applications in recent years. These sensors have shown great potential for active shooter and human presence detection, non-contact and unobtrusive cardio-respiratory motion sensing, and security continuous authentication [1]-[5]. Recently, continuous non-contact and unobtrusive physiological biometric authentication is getting much more attention, since a heart/respiratory based biometric is non-volitional (e.g., unknown to the user), unique, and hard to hide [3]-[5]. Additionally, it reduces the disruption and discomfort of using wearables or intentionally engaging with the authentication system. The analysis of human cardio-respiratory and micro-Doppler signatures has also shown to be very effective for presence detection and surveillance purposes. However, a thorough analysis of its vulnerability to spoofing or replay attacks has not been performed yet.

A conventional Doppler/interferometric radar sends a continuous electromagnetic signal towards a target, which produces a phase change to the signal that is related to the target's movement [3]. Therefore, by analyzing the complex demodulated signal, the moving frequency, displacement, and instantaneous speed of the certain target can be obtained [3], [5], [6]. For continuous authentication, different features that are present in the cardio-respiratory motion can be extracted. These features are unique for each subject, making them suitable for authentication. For instance, in [5] invariant descriptors from the recovered cardiac displacement were extracted by segmenting the heart's periodical signal into discrete frames. These frames were selected based on fiducial points that are biomarkers with physical meaning in the cardiac motion cycle. Additionally, unique micro-Doppler features were found in [1] to determine whether a person was carrying a concealed weapon or not. All these systems rely on the analysis of the phase/frequency shifts caused by the target to the radar signal. Therefore, by electronically applying a phase/frequency shift to the reflected signal, a fake target could be realized to perform a spoofing attack as depicted in Fig. 1. For instance, the "vital Doppler" effect used in [2] for human presence detection could be mimicked using a phase shifter and an arbitrary signal generator (ASG). Similarly, an ASG can be combined with a microwave mixer to create micro-Doppler signatures, which could produce a false alarm in the potential active shooter detection system proposed in [1]. For continuous authentication, a sample of the cardio-respiratory signature of the subject is required to properly perform the spoofing task. This sample can be obtained by scanning the subject with a replica radar for a short period of time.

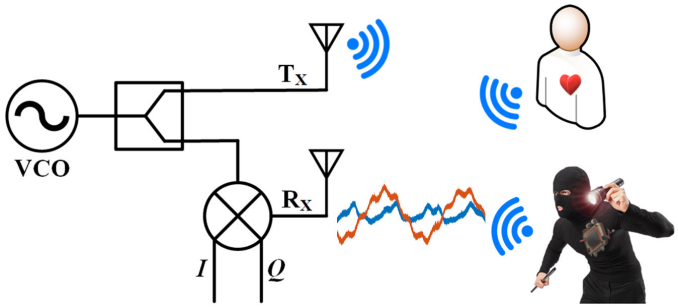

Fig. 1. A real human subject vs. a spoofing device for a continuous-wave radar sensor.

In this paper, the feasibility of electronically mimicking time and frequency domain Doppler signatures with portable devices is studied. First, a simple binary phase-shift keying (BPSK) system was used to generate artificial spectral components in the reflected demodulated signal. Additionally, an analog phase shifter was driven by an ASG to mimic the human cardio-respiratory motion. Experimental results verify the feasibility of performing a spoofing attack to a radar-based monitoring system.

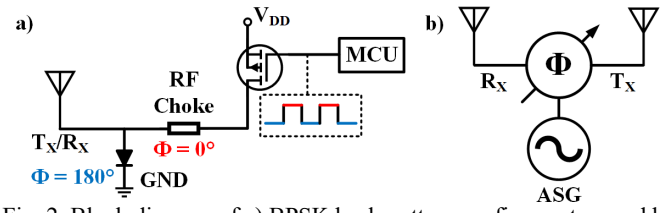

Fig. 2. Block diagram of a) BPSK backscatter spoofing system and b) phase shifter based spoofing system.

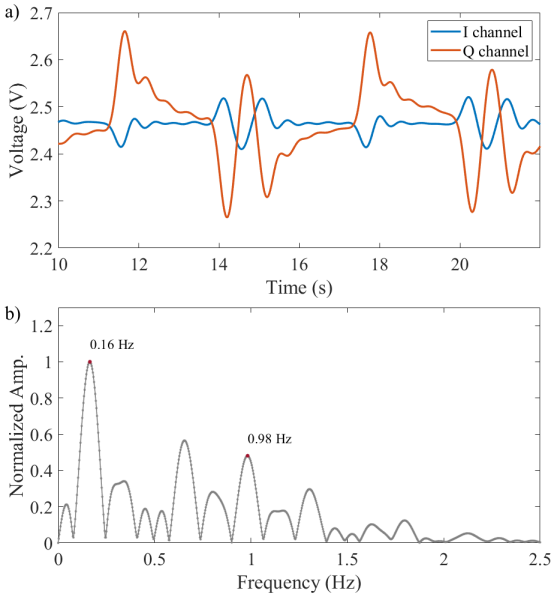

Fig. 3. Cardio-respiratory spoofing results for a) quadrature time domain and b) frequency domain using BPSK tag.

II. Theory

A conventional motion sensing Doppler radar transmits continuous electromagnetic signal towards the target and demodulates the generated echo. The phase of the reflected signal will be directly proportional to any movement performed by the target (e.g., chest movement due to cardio-respiratory activity) [3]-[6]. The typical baseband signals obtained from a quadrature direct conversion receiver can be modeled as $B_I(t) = V_{OI} + \cos(4\pi x(t)/\lambda + \phi)$ and $B_Q(t) = V_{OQ} + \sin(4\pi x(t)/\lambda + \phi)$, where V_{OI} and V_{OQ} are the DC offset voltages, ϕ is the total residual phase accumulated in the circuit and along the transmission path, λ is the wavelength of the wireless signal and $x(t)$ is the mechanical movement. Assuming that the DC offset can be properly calibrated, the displacement signal $x(t)$ can be recovered using arctangent demodulation as $x(t) = \arctan\big(B_Q(t)/B_I(t)\big) \times 4\pi/\lambda$ [6].

All the continuous authentication methods previously discussed are based on identifying certain characteristic displacement $x(t)$. However, if a sample of the displacement signal from a particular person can be obtained, it can be used to electronically modulate the radar's transmitted signal to perform a spoofing attack. Likewise, a false alarm can be triggered on a human presence sensing system by modulating the radar's signal with an ideal cardio-respiratory motion $x(t) = x_r(t) + x_h(t) = m_r \cdot \sin(\omega_r t) + m_h \cdot \sin(\omega_h t)$, where m_r, ω_r and m_h, ω_h are the respiratory and cardiac motion amplitudes and angular frequencies, respectively.

A. BPSK Modulation

BPSK is a simple digital modulation process that applies two different phase shifts to the carrier signal (radar transmitted signal) to achieve up-conversion as depicted in Fig. 2(a). The applied phase shifts are usually separated by 180° and it has the highest noise tolerance among all the phase shift keying (PSK) schemes. The general form of BPSK can be modeled as

$$s_n(t) = A \cdot \cos(2\pi f t + (1-n)\pi), n = 0, 1 \qquad (1)$$

where A and f are the amplitude and frequency of the carrier signal, respectively. When n is periodically changed between 0 and 1, a double side band frequency modulation is applied to the signal $s_n(t)$. The obtained frequency shift will be equal to the frequency associated with the periodic variation of n. However, a fixed BPSK modulation can generate just one spectral component at a time (e.g., heartbeat or respiration). To overcome this issue, the fact that windows from 10 to 20 seconds are commonly used for spectral calculations in cardio-respiratory motion sensing can be exploited. For instance, two different tones can be alternately generated in a sub-window and both will appear in the calculated spectrum. The amplitude of each tone in the frequency domain can be controlled by changing the amount of time that each tone is present in the window.

B. Phase Modulation

To overcome the limitations of the BPSK digital modulation (e.g., one tone generated at a time), an analog microwave phase shifter could be used to mimic a human target by applying a phase shift equal to $(4\pi/\lambda)(x_r(t) + x_h(t))$ to the radar's transmitted signal, where $x_r(t)$ and $x_h(t)$ are the mechanical movements inherent to the heart and chest in the cardiorespiratory process. As depicted in Fig. 2(b), the RX antenna feeds the radar's transmitted signal into the phase shifter, which introduces a phase delay to the signal controlled by an ASG. After the phase delay is applied, the signal is retransmitted towards the radar where after the demodulation process the synthetically applied modulation is recovered.

III. Experimetal Results

To verify the feasibility of performing spoofing attacks to radar sensors, two different experiments were carried out. First, a BPSK backscatter system was used to modulate the signal coming from a 24-GHz radar (InnoSent IVS-162). The BPSK system was composed by a pin diode (MACOM MADP-000907-14020), a microcontroller (Microchip PIC18F24K42T-I), a buffer, and a TX/RX antenna. The pin diode was used to switch between two states, open and short circuit, to reflect the received signal back to the radar with the desired phase shift applied (e.g., $\Gamma = 1$ or $\Gamma = -1$). Whereas the microcontroller (MCU) and the buffer were used to generate the switching signal. To mimic the cardio-respiratory spectrum, the radar's transmitted signal was modulated using a 0.16 Hz tone that was kept for the 83% of the time in a 12 second window. During the remaining 17% of the window, a 0.98 Hz tone was used as the modulating signal. The low and high frequency tones were used to mimic the respiration and cardiac rate of a human subject, respectively. Fig. 3(a)-(b) show the time and frequency domain signals detected by the radar. From Fig. 3(b) the two

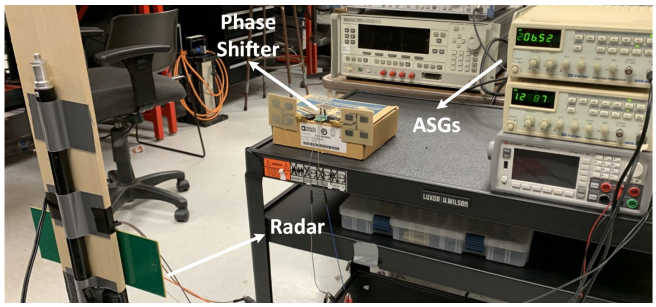

Fig. 4. Experimental setup for the analog phase shifter experiment.

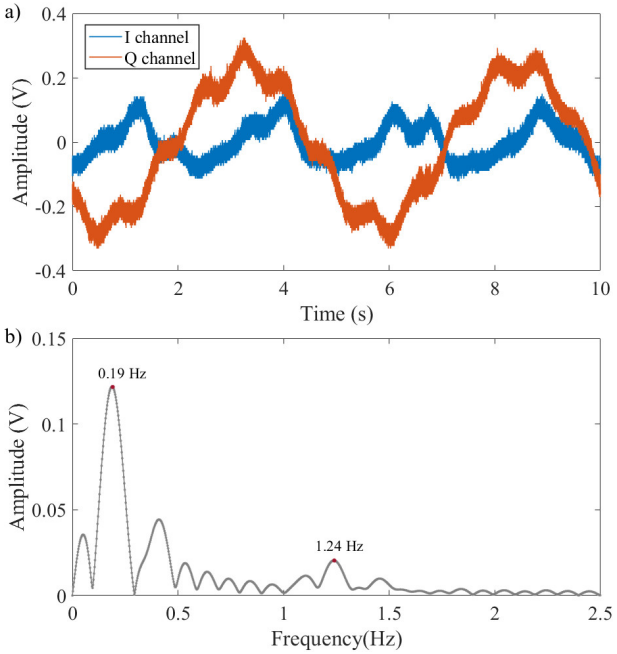

Fig. 5. Cardio-respiratory spoofing results for a) quadrature time domain and b) frequency domain using the analog phase shifter.

programmed tones can be clearly seen in the spectrum, along with the respiration harmonics. This represents a typical vital signs spectrum that can be used to perform spoofing attacks to spectral-based monitoring techniques as those proposed in [2], [3]. However, as depicted in Fig. 3(a), the time domain signal can be identified as a mimicking signal, due to the fact that just one tone is present at a time during the window length and that a digital modulation scheme is used to mimic an analog process, making this type of attacking impractical against time-domain techniques or with complex micro-Doppler signatures as the ones proposed in [1], [4], [5].

To improve the time domain obtained results, an analog phase shifter (Analog Devices HMC935LP5E) was used along with an ASG to modulate the transmitted signal from a 5.8 GHz Doppler radar [7]. The experimental setup is depicted in Fig. 4, the radar was placed 60 cm away from the spoofing device and one antenna was attached to each port of the phase shifter (e.g., input and output), to receive and transmit the phase-modulated signal back to the radar. Two sinusoidal phase shifts were applied to the radar's transmitted signal simultaneously by using two Instek GFG-8210 ASG connected in series, as the phase shifter's control voltage. One ASG was set at 0.2 Hz and the other at 1.23 Hz to mimic the respiratory and cardiac frequencies, respectively. The recovered time and frequency domain signals are depicted in Fig. 5. As shown in Fig 5(a), the recovered time domain signal is mainly sinusoid with a small amplitude distortion. This is the common observed shape obtained from a human subject since the respiratory motion dominates over the cardiac one. On the other hand, the two programmed frequencies were successfully added to the radar baseband output, forming a typical vital signs spectrum as depicted in Fig 5(b). The obtained results verified the possibilities to perform spoofing attacks to human presence, potential shooter detection, and non-contact authentications systems based on complex micro-Doppler/vital-Doppler signatures and displacement measurements obtained from microwave Doppler radars.

IV. Conclusion

Mimicking vital signs were successfully generated to show the potential of the BPSK and phase shifter based spoofing systems to perform spoofing attacks to time and/or frequency domain based surveillance and authentication systems. The BPSK system showed a limited time-domain performance, since it only generates one frequency tone at a time. However, it exhibits a lower hardware complexity and could be used to perform spoofing attacks to frequency-based system. The phase modulation based approach can spoof human vital signs in both time and frequency domains. Finally, the feasibility of performing spoofing attacks to surveillance and authentication systems based on microwave Doppler radars was studied and experimentally verified.

Acknowledgment

The authors wish to acknowledge National Science Foundation (NSF) for funding support under Grant 1808613 and 1718483.

References

[1] Y. Li, Z. Peng, R. Pal and C. Li, "Potential Active Shooter Detection Based on Radar Micro-Doppler and Range-Doppler Analysis Using Artificial Neural Network," in *IEEE Sensors Journal*, vol. 19, no. 3, pp. 1052-1063, 1 Feb.1.

[2] Z. Peng et al., "A Portable FMCW Interferometry Radar With Programmable Low-IF Architecture for Localization, ISAR Imaging, and Vital Sign Tracking," in *IEEE Transactions on Microwave Theory and Techniques*, vol. 65, no. 4, pp. 1334-1344, April 2017.

[3] S. M. M. Islam, A. Rahman, N. Prasad, O. Boric-Lubecke and V. M. Lubecke, "Identity Authentication System using a Support Vector Machine (SVM) on Radar Respiration Measurements," *ARFTG Microwave Measurement Conference*, Boston, MA, USA, 2019.

[4] D. Sasakawa, N. Honma, T. Nakayama and S. Iizuka, "Human Identification Using MIMO Array," in *IEEE Sensors Journal*, vol. 18, no. 8, pp. 3183-3189, 15 April15, 2018.

[5] Feng Lin et al., "Cardiac Scan: A Non-contact and Continuous Heart-based User Authentication System". *Annual International Conference on Mobile Computing and Networking*. pp. 315–328, 2017.

[6] D. Rodriguez and C. Li, "Sensitivity and Distortion Analysis of a 125-GHz Interferometry Radar for Submicrometer Motion Sensing Applications," in *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 12, pp. 5384-5395, Dec. 2019.

[7] J. Wang, T. Karp, J. Muñoz-Ferreras, R. Gómez-García and C. Li, "A Spectrum-Efficient FSK Radar Technology for Range Tracking of Both Moving and Stationary Human Subjects," in *IEEE Transactions on Microwave Theory and Techniques*, vol. 67, no. 12, pp. 5406-5416, Dec. 2019.