Utilizing Space-Time Coding Metasurface for FMCW Radar Spoofing in RIS-Assisted Communication Systems

Keshuang Han
School of Computer Science
Nanjing University of Posts and Telecommunications
Nanjing, China
Email: 1023041139@njupt.edu.cn

Huangwenqing Shi
School of Computer Science
Nanjing University of Posts and Telecommunications
Nanjing, China
Email: 1023040919@njupt.edu.cn

Runqing Wang
School of Computer Science
Nanjing University of Posts and Telecommunications
Nanjing, China
Email: 1023041109@njupt.edu.cn

Pinchang Zhang
School of Computer Science
Nanjing University of Posts and Telecommunications
Nanjing, China
Email: zpc@njupt.edu.cn

***Abstract*—This paper proposes a frequency modulated continuous wave (FMCW) radar spoofing scheme by using space-time coding metasurface (STCM) in a reconfigurable intelligent surface (RIS)-assisted communication system. Specifically, for this spoofing scheme STCM is employed to induce a time-varying phase to modify the FMCW radar signal frequency. Through frequency decoupling, the proposed scheme can spoof FMCW radar estimations of distance and velocity, respectively, and thus achieves the spoofing attack. Finally, we validate the performance of the proposed spoofing scheme through extensive simulations.**

***Index Terms*—FMCW radar, spoofing attack, RIS, sensing security**

I. Introduction

In recent years, frequency modulated continuous wave (FMCW) radar has gained widespread adoption across various domains due to its precision and reliability. For example, it plays a vital role in advanced driver assistance systems (ADAS), by enhancing automotive security through obstacle detection [1]–[3]. Additionally, FMCW radar finds applications in smart homes and healthcare, facilitating through-wall body tracking [4] and health data monitoring [5]. Moreover, FMCW radar can also offers a cost-effective solution for Unmanned Aerial Vehicle (UAV) positioning [6].

The security of FMCW radar has been extensively researched due to its widespread utilization. Numerous studies have highlighted the susceptibility of FMCW radar to spoofing attacks. In [7]–[9], spoofing schemes based on actively crafting attack signals using active transmitters are proposed. These schemes necessitate prior knowledge of the victim radar's parameters and impose strict synchronization requirements on the crafted attack signals. Conversely, [10] and [11] introduce spoofing schemes based on reflective signal modification. Here, the attack objectives are achieved by injecting attack parameters into the radar signal reflection using specialized equipment. This mode of attack circumvents the need for prior knowledge of radar parameters and temporal synchronization. It is worth noting that achieving precise numerical spoofing still requires access to radar parameter information.

In contrast to active constructive attacks, reflective spoofing schemes offer heightened flexibility, reduced constraints, and superior robustness. These inherent advantages make reflective attacks worthy of more attention. We consider the possibility of combining reflective attack with reflective intelligent surface (RIS) because of its characteristics.

RIS emerge as a promising technology in the realm of 6G communication networks, offering vast potential for enhancing communication efficiency, coverage, and security [12], [13]. Motivated by this potential, we explore the integration of reflective FMCW radar spoofing with RIS to spoof unauthorized radar sensing and safeguard against illicit surveillance.

In this paper, we propose a spoofing scheme for FMCW radar utilizing space-time coding metasurface (STCM), which incorporates time-dimension coding—a consideration absent in traditional RIS techniques [14], [15]. Specifically, we explore the capability of STCM to modify signal frequencies and utilize the modified frequencies to spoof the radar. Finally, we validate the performance of the proposed scheme through simulations.

The rest of this paper is organized as follows. Section II presents the system model. The STCM based FMCW radar

spoofing scheme is proposed in Section III. In Section IV, we provides the simulation results. Finally, Section V concludes this paper.

II. SYSTEM MODEL

A. FMCW Radar Model

FMCW radar continuously transmits periodic signals whose frequency increases linearly with time, which is called chirp signal. Thus, the signal from Tx antenna can be expressed as:

$$x_t(t) = A(t)exp[j\phi(t)] = A(t)exp[j2\pi f_t(t)dt] \quad (1)$$

where $A(t)$ and $\phi(t)$ are amplitude and phase of the transmitted signal $x_t(t)$, respectively. $f_t(t)$ is the linear time-varying frequency with initial value f_c and slope s. FMCW radar sends a sequence of these chirp signals to sensing objects. Once the signals are reflected by the object, radar receives these reflected sigals with Rx antenna and mixes them with the signals that Tx is transmitting now. Assuming that the round-trip time of the signal is t_d, the frequency of the return signal $f_r(t)$ equals to $f_t(t + t_d)$, and then the mixed signal can be expressed as:

$$x_{mix}(t) = \alpha exp[j2\pi(f_r(t) - f_t(t))dt] = \alpha exp[j2\pi f_b dt] \quad (2)$$

where α is a constant representing environment fading and f_b is called **beat frequency**, which stands for the frequency difference between the transmitted signal and the received signal. Because the frequency increases linearly, the frequency f_b is a constant, that is, $f_b = f_r(t) - f_t(t) = f_t(t+t_d) - f_t(t) = s*t_d$. Obviously, the mixed signal $x_{mix}(t)$ contains the round-trip time of the signal, so we can simply estimate the distance of the object d through:

$$d = \frac{ct_d}{2} = \frac{cf_b}{2s} \quad (3)$$

Where c is the speed of light. According to the above, we can simply estimate the object distance.

As for the velocity, we need to consider the Doppler effect. We can compute the velocity similar to the approach outlined in [11], where the **Doppler frequency** f_d is obtained by analyzing the temporal variation of phase. It is easy to know that the round-trip time variation due to relative motion is:

$$\Delta t = \frac{2vt}{c} \quad (4)$$

Therefore, the phase variation due to relative motion can be expressed as:

$$\Delta\phi(t) = f_t(t) * \Delta t = \frac{2f_c vt}{c} + \frac{2vst^2}{c} \quad (5)$$

then, by differentiating $\Delta\phi(t)$ with respect to time, we obtain f_d:

$$f_d = \frac{d(\Delta\phi(t))}{dt} = \frac{2f_c v}{c} + \frac{4vst}{c} \quad (6)$$

we can disregard the latter part of the equation. Therefore, we can finally calculate velocity by:

$$v = \frac{cf_d}{2f_c} \quad (7)$$

B. Problem Formulation

As illustrated in II-A. FMCW radar mainly estimates object's range and velocity by the frequency difference between Tx and Rx, i.e. f_b . It is obvious that if we can modify f_b, we can spoof the radar. We can only modify the frequency of the reflected signals. Suppose we add a frequency change Δf to the reflected signal, then the estimated distance of the radar becomes:

$$d' = \frac{ct'_d}{2} = \frac{c(f_b + \Delta f)}{2s} = d + \Delta d \quad (8)$$

where Δd is the spoofed part of distance with:

$$\Delta d = \frac{c}{2s}\Delta f \quad (9)$$

Δf also has an effect on velocity estimation. Specifically, assuming that the object moves at a uniform velocity, the phase difference between the beginning and the end of a data frame with N chirp becomes:

$$\Delta\Phi' = \Delta\Phi + \Delta f NT \quad (10)$$

That is, the phase change is the sum of the original phase change and accumulation of frequency variation in a frame duration. Then, the Doppler frequency becomes:

$$f'_d = \frac{\Delta\Phi'}{NT} = f_d + \Delta f \quad (11)$$

The velocity is estimated by f'_d as:

$$v' = \frac{c}{2f_c}f'_d = \frac{c}{2f_c}(f_d + \Delta f) = v + \Delta v \quad (12)$$

where Δv is the spoofed part of distance with:

$$\Delta v = \frac{c}{2f_c}\Delta f \quad (13)$$

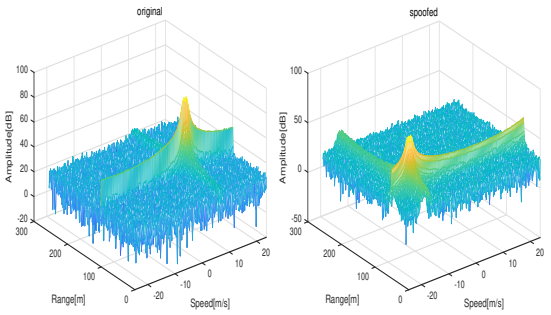
In conclusion, we transform the spoofing of distance and velocity into the modification of reflected signal frequency.

III. FMCW SPOOFING SCHEME USING STCM

RIS can modify the amplitude and phase of signals. However, traditional RIS often only consider controlling the whole nonlinear process by changing the local nonlinear amplitude-phase response in the spatial dimension, ignoring the possibility in the time dimension. Digital coding metasurface is composed of a limited number of basic units arranged according to a specific coding sequence, and the signal is regulated in real time through control devices such as field programmable gate array (FPGA) or Microcontroller Unit (MCU). Those kind of metasurface are called STCM. The STCM modified signal can be expressed as:

$$x'_i(t) = |\Gamma(t)|exp[j\varphi(t)]x_i(t) \quad (14)$$

where $x_i(t)$ and $x'_i(t)$ respectively represent the input and output signal of $i-th$ element of STCM. While $|\Gamma(t)|$ and $\varphi(t)$ are the amplitude and phase changed by STCM, respectively.



(a) original spectrum (b) spoofed spectrum

Fig. 1. Comparison of Original and Spoofed Spectra

STCM can modify the frequency of the signal by time-varying periodic phase. We set the phase to change by $2m\pi$ in a period as in [16]:

$$\Delta\varphi = \varphi(T) - \varphi(0) = 2m\pi \tag{15}$$

Then we can generate a time-varying phase:

$$\varphi(t) = \varphi_0 + \frac{2m\pi}{T}t \tag{16}$$

where φ_0 is the initial phase, T is the period of the phase. Then we can calculate the instantaneous frequency $f_r(t)$ of the reflected wave as:

$$f_r(t) = f_t(t+t_d) + \frac{1}{2\pi}\frac{d\varphi(t)}{dt} = f_t(t+t_d) + \frac{m}{T} \tag{17}$$

Obviously, we introduce a frequency offset of $\frac{m}{T}$ for the reflected signal, i.e. $\Delta f = \frac{m}{T}$. And now we should explore how $\frac{m}{T}$ affect Δd and Δv. As illustrated in (9) and (13), both Δd and Δv seems to be linearly increase with Δf. But if we analyse the resolution of range and velocity ,we can get that Δd should be integer multiple of $\frac{1}{T_c}$, Because the change less than $\frac{1}{T_c}$ cannot be identified due to the range resolution [17]. As for velocity, we know from [17] that the biggest change of velocity is

$$v_{max} = \pm\frac{c}{4f_cT_c} \tag{18}$$

This means that Δv will increase linearly from the minimum value to the maximum value within a frequency change of $\frac{1}{T_c}$, and then overflow to the minimum value. To sum up, Δd only pays attention to the integer multiple of $\frac{1}{T_c}$, while Δv only pays attention to the change within one $\frac{1}{T_c}$. We make the time-varying phase period of STCM $T = T_c$, because $\Delta f = \frac{m}{T}$, and split m into integer plus true fraction form $m = m_1 + m_2$, then Δd is only related to the integer part m_1, and Δv is only related to the fraction part m_2. Finally ,we can manipulate m_1 and m_2 to spoof radar's estimation on d and v, respectively as [11]:

$$\Delta d = \frac{c}{2s}\frac{m_1}{T_c} \tag{19}$$

$$\Delta v = \frac{c}{2f_c}\frac{m_2}{T_c} \tag{20}$$

It is worth noting that if we want to achieve numerical spoof, we still need to know the radar parameters s, f_c and T_c.

IV. SIMULATION

Firstly, in the experimental setup, we configure a FMCW radar with starting frequency $f_c = 77 * 10^9 Hz$, bandwidth $B = c/2$, chirp period $T_c = 4 * 10^-5 s$ and each frame consisted of $N_d = 128$ chirps for sensing objects. The target object is positioned at a distance of $100m$ with a velocity of $5m/s$. The emitted signal collides with the target object, resulting in reflections, and also with an RIS moving at the same state (distance, velocity) as the target object. The signal reflected from the RIS will be modulated by it. Initially, we arbitrarily set the parameter $m = 50.5$. By observing Figure 1, it is evident that the modified signal, termed as the spoofed signal, exhibits peaks not aligned with those of the original signal, indicating the efficacy of our spoofing approach.

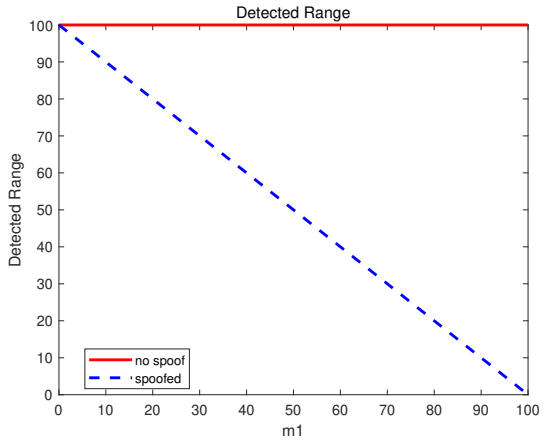


Fig. 2. Spooing distance

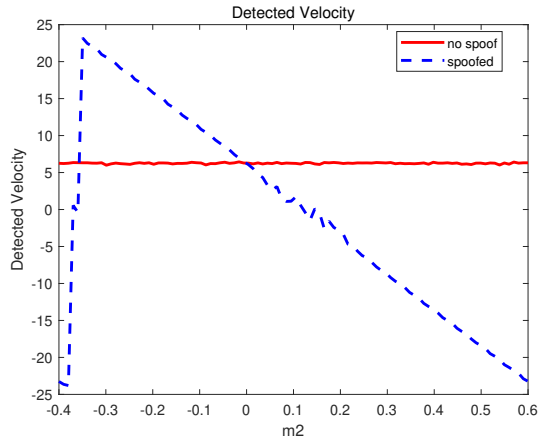


Fig. 3. Spooing velocity

The spoofing performance of the proposed scheme is illustrated in 2 and 3. Object keeps a distance of $100m$ with a velocity of $5m/s$. 2 demonstrates that the original signal accurately reflects this, while the spoofed signal causes the radar's distance estimation to linearly vary from 0 to 100 meters with different values of m_1. Similarly, in 3, the original

signal indicates a constant velocity, whereas the spoofed signal causes the radar's velocity estimation to linearly vary from its minimum to maximum values with different values of m_2. These two figures collectively depict the scheme's performance.

V. Conclusion

In this paper, we proposed an FMCW spoofing scheme utilizing Space-Time-Coding Modulation (STCM), which harnesses the capability of STCM to modify signal frequencies in the temporal dimension. By introducing time-varying phase shift to modify signal frequency and combining with reflective attack mode, we successfully demonstrated the spoofing attack on FMCW radar. The scheme aims to safeguard regions from illicit sensing by leveraging the widespread deployment of metasurfaces. Through extensive simulations, we validated the scheme's accurate spoofing capabilities.

References

[1] S. Sun, A. P. Petropulu, and H. V. Poor, "Mimo radar for advanced driver-assistance systems and autonomous driving: Advantages and challenges," *IEEE Signal Processing Magazine*, vol. 37, p. 98–117, July 2020.

[2] I. Yaqoob, L. U. Khan, S. A. Kazmi, M. Imran, N. Guizani, and C. S. Hong, "Autonomous driving cars in smart cities: Recent advances, requirements, and challenges," *IEEE Network*, vol. 34, no. 1, pp. 174–181, 2019.

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

[4] F. Adib, Z. Kabelac, D. Katabi, and R. C. Miller, "3d tracking via body radio reflections," in *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*, pp. 317–329, 2014.

[5] M. Alizadeh, G. Shaker, J. C. M. De 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.

[6] D. Santos, P. Sebastião, and N. Souto, "Low-cost sdr based fmcw radar for uav localization," in *2019 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC)*, pp. 1–6, IEEE, 2019.

[7] N. Miura, T. Machida, K. Matsuda, M. Nagata, S. Nashimoto, and D. Suzuki, "A low-cost replica-based distance-spoofing attack on mmwave fmcw radar," in *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop*, pp. 95–100, 2019.

[8] R. Komissarov and A. Wool, "Spoofing attacks against vehicular fmcw radar," in *Proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security*, pp. 91–97, 2021.

[9] 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," *Journal of Cryptographic Engineering*, pp. 1–10, 2021.

[10] J. Shenoy, Z. Liu, B. Tao, Z. Kabelac, and D. Vasisht, "Rf-protect: privacy against device-free human tracking," in *Proceedings of the ACM SIGCOMM 2022 Conference*, pp. 588–600, 2022.

[11] R. R. Vennam, I. K. Jain, K. Bansal, J. Orozco, P. Shukla, A. Ranganathan, and D. Bharadia, "mmspoof: Resilient spoofing of automotive millimeter-wave radars using reflect array," in *2023 IEEE Symposium on Security and Privacy (SP)*, pp. 1807–1821, IEEE, 2023.

[12] Z. Zhang, L. Dai, X. Chen, C. Liu, F. Yang, R. Schober, and H. V. Poor, "Active ris vs. passive ris: Which will prevail in 6g?," *IEEE Transactions on Communications*, vol. 71, no. 3, pp. 1707–1725, 2022.

[13] S. Basharat, S. A. Hassan, H. Pervaiz, A. Mahmood, Z. Ding, and M. Gidlund, "Reconfigurable intelligent surfaces: Potentials, applications, and challenges for 6g wireless networks," *IEEE Wireless Communications*, vol. 28, no. 6, pp. 184–191, 2021.

[14] L. Zhang, X. Q. Chen, S. Liu, Q. Zhang, J. Zhao, J. Y. Dai, G. D. Bai, X. Wan, Q. Cheng, G. Castaldi, *et al.*, "Space-time-coding digital metasurfaces," *Nature communications*, vol. 9, no. 1, p. 4334, 2018.

[15] D. Jun-Yan and C. Tie-Jun, "New model of nonlinear metasurfaces space-time-coding digital metasurfaces," *PHYSICS*, vol. 50, no. 5, pp. 293–299, 2021.

[16] J. C. Ke, J. Y. Dai, J. W. Zhang, Z. Chen, M. Z. Chen, Y. Lu, L. Zhang, L. Wang, Q. Y. Zhou, L. Li, *et al.*, "Frequency-modulated continuous waves controlled by space-time-coding metasurface with nonlinearly periodic phases," *Light: Science & Applications*, vol. 11, no. 1, p. 273, 2022.

[17] V. Dham, "Programming chirp parameters in ti radar devices," *Application Report SWRA553, Texas Instruments*, vol. 1457, 2017.