

RESEARCH ARTICLE

A Replay Attack Against ISAC Based on OFDM

GEORGIOS CHRYSANIDIS¹, YANWEI LIU², AND ANTONIOS ARGYRIOU¹, (Senior Member, IEEE)

¹Department of Electrical and Computer Engineering, University of Thessaly, 38334 Volos, Greece

²Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Corresponding author: Antonios Argyriou (anargyr@uth.gr)

This work was supported by HEAL-Link.

ABSTRACT Integrated sensing and communication (ISAC) is envisioned to be a core element of future 6G and connected vehicular wireless systems. As always wireless security and privacy will still be of utmost importance. Existing research on ISAC has not explored sufficiently security attacks that compromise its sensing operation. In this paper we present a new wireless *range-Doppler replay attack* that can compromise the functionality of ISAC systems that use orthogonal frequency division multiplexing (OFDM) for sensing and data communication. With the proposed attack the adversary detects wireless OFDM transmissions and retransmits the same wireless frame (preamble and data) but with a phase shift that varies across subcarriers and successive OFDM symbols of the frame. This results in the creation of false targets in the range-Doppler images that are created by the ISAC system. Our simulation results for a vehicular scenario show that the ISAC system cannot distinguish the false targets from the real ones even when the attacker uses low transmission power. The implication of this attack is that it may lead to inability of advanced driver assistance systems (ADAS) or connected autonomous vehicular (CAV) systems that use ISAC to operate safely.


INDEX TERMS Integrated sensing and communication (ISAC), joint RADAR communication (JRC), 6G, OFDM RADAR, replay attack, doppler estimation, range estimation, range-Doppler response, connected autonomous vehicles, advanced driver assistance systems (ADAS).

I. INTRODUCTION

Joint RADAR Communication (JRC) systems are a sub-category of integrated sensing and communication (ISAC) systems where RADAR functionality and communication are implemented with the same waveform. ISAC requires careful design of the modulation scheme [1], but also requires consideration of the network topology [2]. The most widely popular ISAC systems are expected to be the ones that leverage existing highly efficient wireless digital communication modulation schemes like orthogonal frequency division multiplexing (OFDM) for building RADAR functionality on top of the primary communication service [3], [4], [5], [6], [7]. ISAC systems based on OFDM have been a relatively recent proposal with several variants being developed around concept for specific applications [8], [9]. In an OFDM system that transmits wireless frames in bursts, time difference of arrival (TDoA) cannot be used reliably for range and Doppler (velocity) estimation due to the non-periodic nature of the

transmissions. Instead, with OFDM the ISAC system can leverage the received echo signal from a real target across the subcarriers to also estimate range besides Doppler [10]. The system relies on the observation that each subcarrier experiences a different phase offset for a certain delay of the signal leading to a straightforward way for estimating range [4], [10]. On the other hand, Doppler can be estimated by using successive OFDM symbols and their returns (emulating thus a pulsed RADAR system) [11]. It can thus create the range-Doppler (RD) response which visualizes in an image the targets that are present. Hence, OFDM-based JRC is particularly appealing primarily because it allows this simple range estimation without calculating the TDoA as in pulsed RADAR [11]. Another advantage is that OFDM wireless communication systems are used everywhere (either in the omnipresent wireless LANs (802.11) or in mobile communications (4G/5G)), allowing thus the embedding of RADAR functionality in a wide class of devices.

But as with any wireless communication system, ISAC can also be the target of security attacks. Communication operations can be disrupted with various types of jamming

The associate editor coordinating the review of this manuscript and approving it for publication was Mohammad S. Khan .

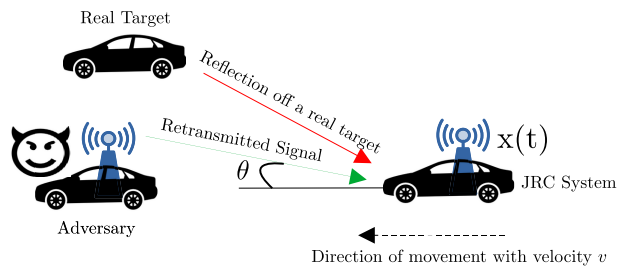


FIGURE 1. A scenario where the attack is to a vehicle that transmits the ISAC OFDM signal $x(t)$. The adversary emits a signal (green) which contains the received signal plus an element that spoofs its range and relative velocity to the ISAC system.

techniques similar to non-ISAC systems [12], but there are robust methods to detect these attacks [12]. With respect to the ISAC literature the focus has been on thwarting attacks that attempt to breach data confidentiality. For example recent works explored how to optimize the ISAC operation subject to the presence of eavesdroppers that want to demodulate the data [13], [14]. Regarding attacks on the RADAR functionality the objective is typically to create fake or ghost targets and potentially prevent the detection of real ones. The literature is more rich in attacks and counter-measures in RADAR-only systems, e.g. see [11] for a discussion on the topic and in the references therein. As an example in a purely RADAR-optimized system a fake target can be detected in certain scenarios with range-angle adaptive matched filters [15]. The authors of that work make use of a frequency diverse array (FDA) RADAR [16] and also require a special type of waveform based on random polyphase codes. Emerging attacks, like the one we will present in this paper, has the purpose of disrupting radar operation but in ISAC OFDM-based systems, something that has not been addressed in the literature.

Despite the great potential for widespread adoption of ISAC functionality we argue that in some cases a malicious OFDM-capable device might desire to compromise the RADAR operation besides the security of the communication link. The attack we investigate in this paper is for an adversary that uses its wireless transmitter to emit a spoofing signal that creates ghost targets in the ISAC system in terms of Doppler and range. In particular the adversary injects a fake target, in terms of speed and range, by re-transmitting an altered OFDM signal that receives, hence the term *replay attack*. The attack is carried out in a way that exploits the used algorithms in the OFDM-based ISAC system. Our basic system model is illustrated in Fig. 1 where besides a legitimate target with a cross section of σ (in m^2), there is an adversary. In our investigated attack the adversary that has a device with the same OFDM communication scheme with the ISAC system, receives the signal, process it, and injects the malicious signal in the same frequency band (green color) that mimics a real target. The actual return signal from the target (red) and that of the transmitted from the adversary (green) can overlap in the time domain at least partially (Fig. 2). In our previous work [10] we introduced the idea of generating fake targets

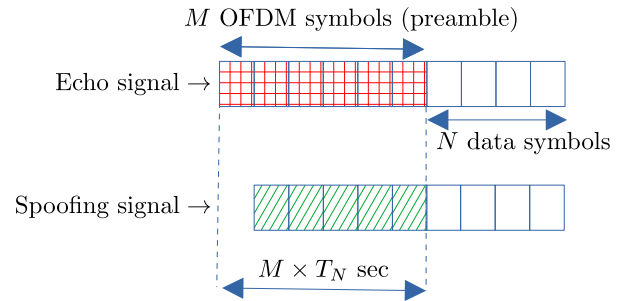


FIGURE 2. The ISAC system uses M OFDM symbols from the reflected echo of the preamble (red) to construct the range-Doppler response. The adversary transmits a fraction of the preamble OFDM symbols (green) that have been altered and may overlap in the time domain with the real echo.

based on OFDM echoes but without considering the presence of real targets.

The contribution of this paper is that it introduces the first of its kind *range-Doppler replay attack for ISAC systems*, a method to compromise the operation of ISAC systems that use OFDM and is applicable in a variety of wireless networks including the ones found in connected autonomous vehicles (CAVs).

Paper Organization: The rest of this paper is organized as follows. Section II describes the signal model when the replay attack is carried out in an ISAC system. Section III presents the proposed attack as well as the algorithms used at the ISAC system for generating the range-Doppler images. Section IV presents the simulation-based evaluation of our attack while Section V concludes this paper.

II. SIGNAL MODEL

We assume that the ISAC system is part of an OFDM wireless communication network which can be WiFi or cellular. The adversary does not need to be part of the same network, i.e. it does not need to decrypt the OFDM modulated symbols but it only has to synchronize with the start of the transmission of a physical layer (PHY) frame, basically it has to know the type of the wireless PHY protocol. The adversary can also use a full-duplex radio which allows for simultaneous transmit and receive, an assumption used in practical wireless networks of CAV systems today [6].

A. RADAR CHANNEL MODEL

We are interested in attacks of the RADAR functionality in the ISAC system, and not its digital communication link. Hence, we focus on the signal models that are used for RADAR signal processing. The large-scale radar channel gain for a target i at distance R_i is assumed to follow the free-space path-loss model set with a path loss exponent equal to 2 and is given by [6], [11], and [17]:

$$G_i = \frac{\lambda^2 \sigma_i}{64\pi^3 R_i^4} \quad (1)$$

The radar cross section (RCS) of the i -th target is denoted as σ_i . The baseband model that we will present also takes into account the two-way delay of the signal that is equal

to $2R_i/c$, c being the speed of light. This delay introduces a phase shift equal to $\exp(-j2\pi f_k \frac{2R_i}{c})$ in the baseband model¹ that depends on the frequency of each subcarrier f_k for OFDM (or the carrier frequency for a single-carrier system). It is more convenient to describe the subcarrier frequency as $f_k = k\Delta f$ where k indexes the subcarrier and Δf is the subcarrier spacing. If λ is the wavelength the Doppler shift is $f_{D_i} = \frac{v_i}{\lambda} \cos(\theta_i)$, where θ_i is the angle between the i -th target or adversary and the ISAC system, and $v_i \cos(\theta_i)$ is their relative velocity. This discussion leads to the baseband complex channel coefficient for a target i becoming equal to:

$$h_i(t, f) = g_i \sqrt{G_i} e^{j2\pi f_{D_i} t} e^{-j2\pi f_k \frac{2R_i}{c}} \quad (2)$$

In the above g is a sample from a complex Gaussian random process that corresponds to Rayleigh fading that is constant (slow fading) for the duration of the RADAR coherent processing interval (CPI) [11]. The CPI indicates the time period for which all the received data are jointly processed to create a single range-Doppler image. In our system model M OFDM symbols are contained in a CPI.

B. SIGNAL MODEL AT THE ISAC SYSTEM

The received signal at the ISAC system will be the aggregate result of the echo signal (red in the figures) and the one transmitted from the adversary (green). The transmitter (Tx) and receiver (Rx) at the ISAC system use the same local oscillator (LO) for up and down-conversion, and so it is reasonable to assume that there is no carrier frequency offset (CFO) between the transmitted signal and its reflected echo. Hence, during typical system operation the only frequency shift observed in the echo is because of Doppler due to the target as captured in (2). However, there will be CFO between the spoofing signal that the adversary emits from its Tx and the LO at the ISAC receiver, something that is modeled with the parameter f_{cfo} in the following equations. Also, there will be amplitude mismatch between the real and spoofed signals captured by different values in the path loss exponent G . Based on the previous discussion the baseband continuous time signal model at the ISAC system becomes:

$$y(t) = h_2(t, f)x_p(t) + h_1(t, f)x_p(t)e^{j2\pi f_{cfo}t} + w(t). \quad (3)$$

In the above h_2 is the two-way channel from the reflection off a real target, and h_1 is the one way channel from the adversary to the receiver of the ISAC system. Regarding other terms in the above expression $x_p(t)$ represents the modulated symbols of the preamble of the wireless frame, and $w(t)$ is the additive white Gaussian noise (AWGN) sample.

C. SAMPLED OFDM SIGNAL

We can expand on the previous model when the transmitted signal, including the preamble $x_p(t)$, has been multi-carrier

¹The delay will be R_i/c for the signal that the adversary generates and arrives at the ISAC receiver.

modulated and more specifically with OFDM. In this case the channel model in (2) because it considers only the LOS path it leads to flat fading for each subcarrier. With N subcarriers that contain pilot and data, the desired OFDM symbol in continuous time is:

$$x(t) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X_p[k] e^{j2\pi f_k t}, \quad 0 \leq t \leq T_N. \quad (4)$$

$X_p[k]$ is the complex symbol of the preamble modulated onto subcarrier k , and if subcarrier spacing is Δf then $T_N = \frac{1}{\Delta f}$ is the OFDM symbol duration (without considering the cyclic prefix (CP)). By sampling this at times $t = n/f_s$, and recalling that the fraction of the subcarrier frequency relative to the sampling rate, i.e. $f_k/f_s = k/N$, we get a digital frequency k/N and the discrete form:

$$x[n] = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X_p[k] e^{j2\pi nk/N}, \quad 0 \leq n \leq N-1. \quad (5)$$

This is effectively the inverse discrete Fourier transform (IDFT) of $X_p[k]$ allowing thus its well known efficient implementation with the fast Fourier transform (FFT) algorithm both at the transmitter and receiver.

Recall that the ISAC system desires to find the range and Doppler (velocity) of the targets which means that it will create the so-called range-Doppler response/image. To do that it samples the analog baseband signal $y(t)$ across the fast-time with rate f_s samples/sec, and across OFDM symbols (slow-time) with rate $1/T_N$ [10]. So we will sample at $t = n/f_s + mT_N$ to generate the 2D discrete signal:

$$y[n, m] = y(t)|_{t=n/f_s+mT_N}$$

Now we will replace (2), (4) into (3) to obtain $y[n, m]$ at the ISAC system:

$$y[n, m] = \frac{g_2 \sqrt{G_2}}{\sqrt{N}} \sum_{k=0}^{N-1} X_p[k] e^{j2\pi f_k (\frac{n}{f_s} - \frac{2R_2}{c})} e^{j2\pi f_{D_2} m T_N} + \frac{g_1 \sqrt{G_1}}{\sqrt{N}} \sum_{k=0}^{N-1} X_p[k] e^{j2\pi f_k (\frac{n}{f_s} - \frac{R_1}{c})} e^{j2\pi (f_{D_1} + f_{cfo}) m T_N} + w[n], \quad 0 \leq n \leq N-1, \quad 0 \leq m \leq M-1. \quad (6)$$

This expression has been simplified by noticing that $e^{j2\pi f_k m T_N} = 1$, since $f_k T_N = k\Delta f T_N = kN$. We also assumed that the Doppler within one OFDM symbol is negligible so $e^{-j2\pi f_{D_2} \frac{n}{f_s}} \approx 1$ [10]. This expression gives the final signal model for each time domain sample n of the m -th OFDM symbol that has duration T_N .

III. FAKE TARGET GENERATION AND RANGE-DOPPLER CALCULATION

A. FAKE TARGET GENERATION

In our system the Tx at the adversary takes the N frequency domain (FD) samples of the m -th OFDM symbol that belong in the received preamble and multiplies them with a discrete

spoofing signal. We set the baseband spoofing signal in FD to be for the m -th OFDM symbol equal to

$$U[k, m] = e^{-j2\pi f_k \frac{R_{sp}}{c}} e^{j2\pi m f_{sp} T_N}, \quad (7)$$

that is it depends on the subcarrier k and OFDM frame m . The baseband signal that is actually transmitted is the IDFT of $U[k, m]X_p[k]$ for subcarrier k , plus of course the cyclic prefix (CP). Consequently after using (7), (6) becomes:

$$\begin{aligned} y[n, m] &= \frac{g_2 \sqrt{G_2}}{\sqrt{N}} \sum_{k=0}^{N-1} X_p[k] e^{j2\pi f_k (\frac{n}{f_s} - \frac{2R_2}{c})} e^{j2\pi f_{D_2} m T_N} \\ &+ \frac{g_1 \sqrt{G_1}}{\sqrt{N}} \sum_{k=0}^{N-1} X_p[k] e^{j2\pi f_k (\frac{n}{f_s} - \frac{R_1 + R_{sp}}{c})} e^{j2\pi (f_{D_1} + f_{CFO} + f_{sp}) m T_N} \\ &+ w[n], \quad 0 \leq n \leq N - 1, \quad 0 \leq m \leq M - 1. \end{aligned} \quad (8)$$

With this method the aggregate resulting signal at the ISAC system contains two sets of FD OFDM signals: One with range-Doppler parameters of the actual target, namely f_{D_2} and R_2 , and another with parameters equal to $f_{D_1} + f_{CFO} + f_{sp}$ and $R_1 + R_{sp}$. One interesting question is if the Tx at the adversary can start transmitting fast enough so that the second part of the composite signal in (8) is indeed present as graphically explained in Fig. 2. In the opposite case the ISAC system receives enough ‘‘clean’’ OFDM symbols that contain only the echo from the target. This is something that depends on the hardware capabilities of the adversary but we evaluate its impact through our simulations. In either case a fake target is created since the data for the fake target will be present in an image creating in the following time periods.

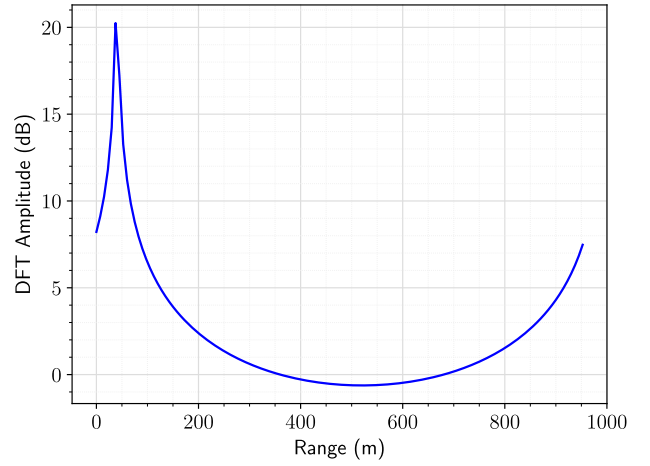
B. THE ISAC RADAR ALGORITHM

The ISAC system receives OFDM signal echoes and it first synchronizes to the start of the first OFDM symbol until the expected number of them is received depending on the size of the preamble. With sampling at $t = n/f_s + mT_N$ the receiver has then access to the 2D signal in (8) which the second part of it has been modified of course with the fake target signal in (7). Now as in any standard OFDM receiver demodulation with DFT is performed so as to calculate the frequency domain symbols. So we have that the result of OFDM demodulation with DFT for the m -th OFDM symbol of the preamble is:

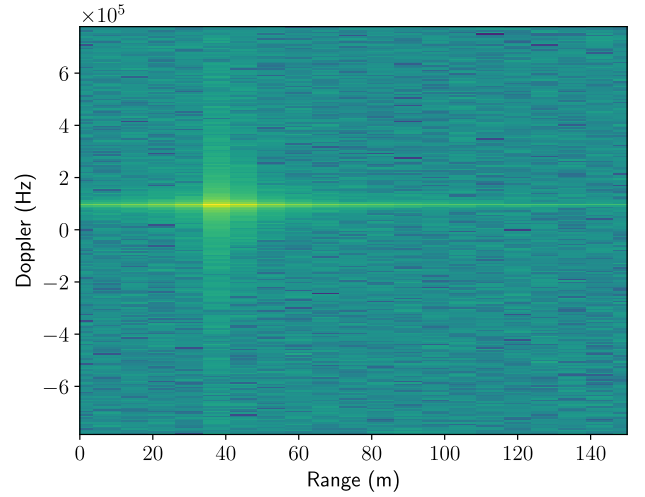
$$\begin{aligned} \tilde{Y}[k, m] &= g_2 \sqrt{G_2} X_p[k] e^{-j2\pi f_k \frac{2R_2}{c}} e^{j2\pi f_{D_2} m T_N} \\ &+ g_1 \sqrt{G_1} X_p[k] e^{-j2\pi f_k \frac{R_1 + R_{sp}}{c}} e^{j2\pi (f_{D_1} + f_{sp} + f_{CFO}) m T_N} \\ &+ w[n], \quad 0 \leq k \leq N - 1, \quad 0 \leq m \leq M - 1. \end{aligned} \quad (9)$$

Upon finishing DFT, the RADAR algorithm at the ISAC system divides then (9) with $X_p[k]$ to remove m -th symbol of the preamble. The resulting signal is:

$$\frac{\tilde{Y}[k, m]}{X_p[k]} = g_2 \sqrt{G_2} e^{-j2\pi f_k \frac{2R_2}{c}} e^{j2\pi f_{D_2} m T_N}$$



(a) DFT of the range bin where the real target resides.



(b) Range-Doppler image.

FIGURE 3. Results for the real target.

$$\begin{aligned} &+ g_1 \sqrt{G_1} e^{-j2\pi f_k \frac{R_1 + R_{sp}}{c}} e^{j2\pi (f_{D_1} + f_{sp} + f_{CFO}) m T_N} \\ &+ w[n], \quad 0 \leq k \leq N - 1, \quad 0 \leq m \leq M - 1. \end{aligned} \quad (10)$$

After collecting N samples for M OFDM symbols, the OFDM-based RADAR at the ISAC system performs 2D DFT on the signal in (10) across the k, m indexes, with sampling rates f_s and $1/T_N$ respectively [10], to obtain the range-Doppler image that exhibits peaks at points (f_{D_2}, R_2) and $(f_{D_1} + f_{CFO} + f_{sp}, R_1 + R_{sp})$.

IV. EVALUATION

The objective of our simulation-based study is to evaluate the ability of the adversary to alter the range-Doppler response/image by generating ghost targets in the ISAC system with the proposed attack. We considered the topology in Fig. 1 where we implemented a custom vehicle movement scenario based on the code and channel model in [12].

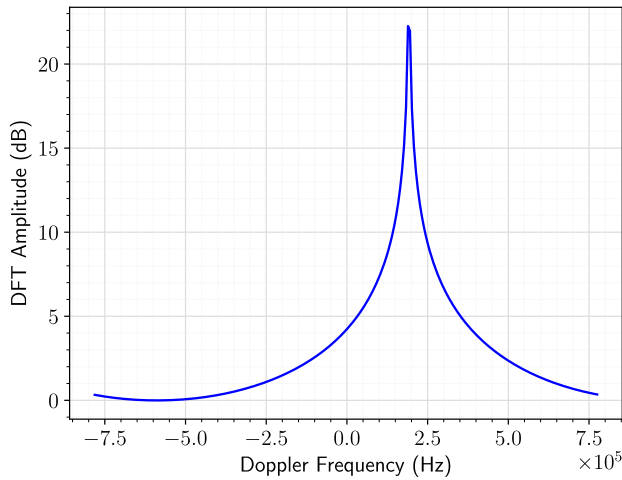


FIGURE 4. DFT of the range bin where the fake target resides with the equal signal power configuration.

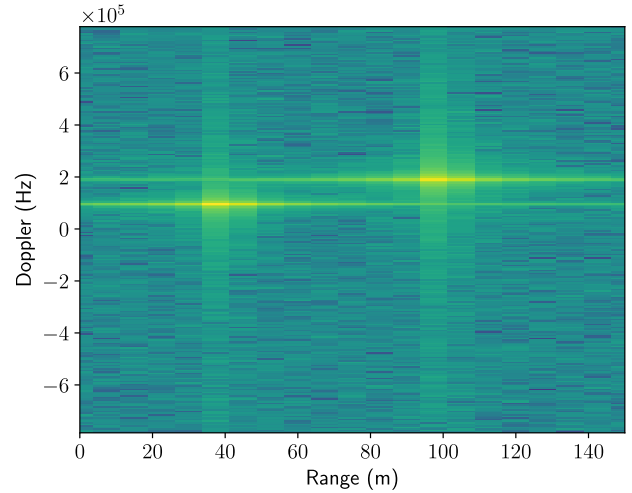
In this scenario the three vehicles move in the same direction as in Fig. 1 with a speed of 80 m/s. The OFDM wireless network uses a carrier frequency of 24 GHz, $N = 128$ subcarriers, a 20 MHz channel, while $M = 256$ OFDM symbols are processed jointly for producing the range-Doppler response. For the selected range of the real target the SNR was approximately 10 dB which makes the detection conditions challenging. Higher SNR, that corresponds to shorter distances, yielded similar behavior in terms of the presented range-Doppler plots.

A. REAL TARGET

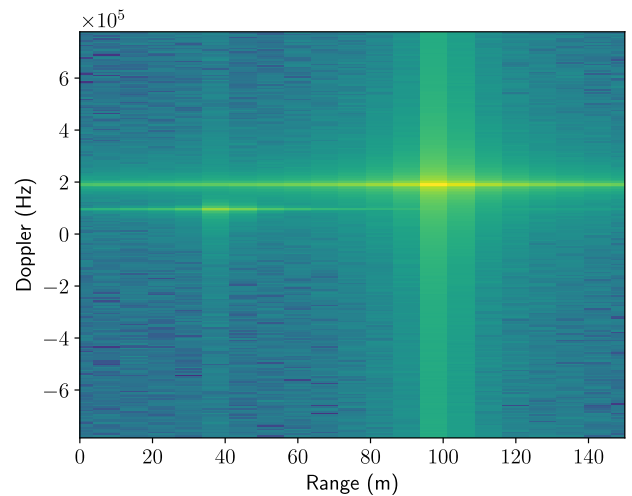
First we consider a case where the attacker cannot transmit fast enough so that the OFDM symbols in the wireless frame that it retransmits and the reflected signals from the real target do not overlap in time as illustrated in Fig. 2. This means that the ISAC system receives for the duration of a single PHY frame the reflected signal only, while the spoofed retransmitted signal arrives with a delay that means the imaging result is plotted in a follow-up range-Doppler image. The real target is at the 100 kHz Doppler bin and 40 m range bin. First we calculate the DFT of (10) for the specific Doppler bin where the target is present so that we can estimate its range and the result is presented in Fig. 4(a). The target is at the 40 m mark. The range-Doppler response is presented in Fig. 4(b) where the target is also clearly visible. These results serve as a baseline to compare with the case that there is a fake target present in the same signal $y(t)$.

B. SPOOFING WITHIN THE DURATION OF A SINGLE WIRELESS FRAME

To evaluate the ability for spoofing within the time duration of an OFDM wireless frame as illustrated in Fig. 2, we consider that the attacker manages to overlap in the time domain a fraction of the OFDM symbols of the wireless frame. For calculating the range-Doppler response at the ISAC system we use the aggregate received signal described in (10). Again,



(a) Equal signal power for the real and fake targets.



(b) Higher power for the fake target relative to the real one.

FIGURE 5. Results for fake target generation within the duration of a single wireless frame.

the real target is located at the 100 kHz and 40 m bins in the range-Doppler response. We have “placed” the ghost target at 200 kHz and 100 m so that its response does not interfere with the response of the real target. First we present results for Doppler for the range bin where the fake target is present in Fig. 4. Fig. 5(a) presents the real and fake targets together in the range-Doppler image. This result highlights that the ghost target even in this scenario behaves in a way consistent with a real target. The two targets are clearly visible while there is no way for the ISAC system to differentiate the two signatures.

We also investigate the case that the adversary emits with higher power by a factor of 5 so that its signature dominates the real target in Fig. 5(b). When we compare Fig. 5(a) and 5(b) we notice in Fig. 5(b) that the fake target is experiencing a clearer signature at the expense of the real target that becomes less prominent. Hence, one goal from the perspective of the attacker is to start transmitting as soon as possible so that the two signatures are overlapped and at

a relatively higher power than the reflected power of real targets. This scenario will create significant problems since a false target will be detected while possibly a real one will be missed.

Another detail of these results is that since the maximum unambiguous range [11] for OFDM Radar is $R_{\text{una}} = c/\Delta f$, a fake range of more than that would result in aliasing in the range-Doppler response. The same result could be accomplished if needed for Doppler. In any case the generation of a fake target would be achieved by the attacker. This means that the attackers do not have to be precise at their settings of the fake range R_{sp} and Doppler f_{sp} .

V. CONCLUSION

In this paper we presented a new replay attack that generates fake targets in ISAC wireless communication systems that use OFDM. The basic idea suggests the insertion of an artificial frequency variation and phase shift at the replayed/re-transmitted signal that depends on the subcarrier k and the specific OFDM symbol indexed by m . This misguides the range-Doppler estimators to produce the a fake target-induced Doppler and range. The final result is an attack scheme that can create problems for OFDM RADAR which is very critical in vehicular applications like ADAS and CAV systems. The proposed attack could be evaluated by OFDM RADAR developers for making the RADAR algorithms more robust against adversaries that use this class of schemes for compromising their operation.

REFERENCES

- [1] L. G. De Oliveira, B. Nuss, M. B. Alabd, A. Diewald, M. Pauli, and T. Zwick, "Joint radar-communication systems: Modulation schemes and system design," *IEEE Trans. Microw. Theory Techn.*, vol. 70, no. 3, pp. 1521–1551, Mar. 2022.
- [2] J. A. Zhang, M. L. Rahman, K. Wu, X. Huang, Y. J. Guo, S. Chen, and J. Yuan, "Enabling joint communication and radar sensing in mobile networks—A survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 1, pp. 306–345, 1st Quart., 2022.
- [3] C. R. Berger, B. Demissie, J. Heckenbach, P. Willett, and S. Zhou, "Signal processing for passive radar using OFDM waveforms," *IEEE J. Sel. Topics Signal Process.*, vol. 4, no. 1, pp. 226–238, Feb. 2010.
- [4] M. Braun, "OFDM radar algorithms in mobile communication networks," Ph.D. thesis, Karlsruhe Institut für Technologie, Germany, 2014.
- [5] M. Kotaru, K. Joshi, D. Bharadia, and S. Katti, "SpotFi: Decimeter level localization using WiFi," in *Proc. ACM Conf. Special Interest Group Data Commun.*, Aug. 2015, pp. 1–11.
- [6] P. Kumari, J. Choi, N. González-Prelcic, and R. W. Heath Jr., "IEEE 802.11ad-based radar: An approach to joint vehicular communication-radar system," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3012–3027, Apr. 2018.
- [7] W. Li, M. J. Bocus, C. Tang, S. Vishwakarma, R. J. Piechocki, K. Woodbridge, and K. Chetty, "A taxonomy of WiFi sensing: CSI vs passive WiFi radar," in *Proc. IEEE Globecom Workshops*, Dec. 2020, pp. 1–6.
- [8] G. K. Carvajal, M. F. Keskin, C. Aydogdu, O. Eriksson, H. Herbertsson, H. Hellsten, E. Nilsson, M. Rydström, K. Vänaas, and H. Wymeersch, "Comparison of automotive FMCW and OFDM radar under interference," in *Proc. IEEE Radar Conf.*, Sep. 2020, pp. 1–6.
- [9] S. P. Lavery and T. Ratnarajah, "Airborne phased array OFDM joint radar-communications system," in *Proc. IEEE Radar Conf.*, Mar. 2022, pp. 1–6.
- [10] A. Argyriou, "False target detection in OFDM-based joint RADAR-communication systems," in *Proc. IEEE Radar Conf.*, May 2023, pp. 1–6.
- [11] M. A. Richards, *Fundamentals of Radar Signal Processing*. New York, NY, USA: McGraw-Hill, 2005.
- [12] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *Veh. Commun.*, vol. 13, pp. 56–63, Jul. 2018.
- [13] H. Du, J. Kang, D. Niyato, J. Zhang, and D. I. Kim, "Reconfigurable intelligent surface-aided joint radar and covert communications: Fundamentals, optimization, and challenges," *IEEE Veh. Technol. Mag.*, vol. 17, no. 3, pp. 54–64, Sep. 2022.
- [14] Y. Yao, F. Shu, Z. Li, X. Cheng, and L. Wu, "Secure transmission scheme based on joint radar and communication in mobile vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 9, pp. 10027–10037, Sep. 2023.
- [15] L. Lan, G. Liao, and J. Xu, "A method to suppress the main-beam deceptive jamming in FDA-MIMO radar with random polyphase codes," in *Proc. IEEE 10th Sensor Array Multichannel Signal Process. Workshop (SAM)*, 2018, pp. 509–513.
- [16] P. Antonik, M. C. Wicks, H. D. Griffiths, and C. J. Baker, "Range-dependent beamforming using element level waveform diversity," in *Proc. Int. Waveform Diversity Design Conf.*, Jan. 2006, pp. 1–6.
- [17] A. Bazzi, C. Kärfelt, A. Péden, T. Chonavel, P. Galaup, and F. Bodereau, "Estimation techniques and simulation platforms for 77 GHz FMCW ACC radars," *Eur. Phys. J. Appl. Phys.*, vol. 57, no. 1, p. 11001, Jan. 2012.



GEORGIOS CHRYSANIDIS received the B.Sc. degree in electrical, electronics, and communications engineering from the Hellenic Air Force Academy and the M.Sc. degree in electrical and computer engineering from the University of Thessaly, Greece, in 2018. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Thessaly. He is currently an Officer with the Hellenic Air Force.



YANWEI LIU received the B.S. degree in applied geophysics from Jiangnan Petroleum University, China, in 1998, the M.S. degree in computer science from China Petroleum University, Beijing, in 2004, and the Ph.D. degree in computer science from the Institute of Computing Technology, Chinese Academy of Sciences, in 2010. Currently, he is an Associate Professor with the Institute of Information Engineering, Chinese Academy of Sciences. His research interests include omnidirectional vision, multiview/3D video/VR video processing, multimedia networking, and digital twin. He serves as a TPC member of several international conferences in the areas of computer vision, multimedia, communications, and networking.



ANTONIOS ARGYRIOU (Senior Member, IEEE) received the Diploma degree in electrical and computer engineering from the Democritus University of Thrace, Greece, in 2001, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, USA, in 2003 and 2005, respectively. He was a Fulbright Scholar with the Georgia Institute of Technology. From 2007 to 2010, he was a Senior Research Scientist with Philips Research, Eindhoven, The Netherlands, where he led the research efforts on wireless body area networks. From 2004 to 2005, he was a Senior Engineer with Soft Networks, Atlanta. Currently, he is an Associate Professor with the Department of Electrical and Computer Engineering, University of Thessaly, Greece. His research interests include wireless communications, RADAR systems, and statistical signal processing theory and applications. He serves as the TPC member for several international conferences and workshops. He has served as a Guest Editor for the Special Issue on Quality-Driven Cross-Layer Design of IEEE TRANSACTIONS ON MULTIMEDIA. He was a Lead Guest Editor for the Special Issue on Network Coding and Applications of *Journal of Communications*.