Signal Waveform Design for Resilient Integrated Sensing and Communications

Tongyang Xu, Yujin Ye, Christos Masouros

School of Engineering, Newcastle University, Newcastle upon Tyne, UK
School of Electrical Engineering, Southeast University, Jiangsu Province, China
Department of Electronic and Electrical Engineering, University College London, London, UK
Email: tongyang.xu@newcastle.ac.uk, yeyujian@seu.edu.cn, c.masouros@ucl.ac.uk

***Abstract*—The paper presents an experimental study of data-security in a dual-functional integrated sensing and communication (ISAC) system where sensing and communications are carried out using a single hardware platform. The framework is based on orthogonal frequency division multiplexing (OFDM) in a multi-user multiple input multiple output (MIMO) software-defined radio (SDR) testbed. Over-the-air experiments are conducted to study the robustness of the ISAC in communication security. Results reveal that the ISAC system can generate a directional beam for sensing while the beam also carries communication data. Once an eavesdropper is positioned next to a legitimate user within an appropriate distance, the eavesdropper can capture the signal and recover the data. This alerts that the ISAC transmission has risk in leaking data to eavesdroppers when the eavesdropper is positioned within the ISAC sensing beam range. Therefore, a waveform-defined security (WDS) framework is evaluated here to defend against the potential eavesdropping in ISAC systems illustrating a degradation the eavesdropping performance by 7 dB.**

***Index Terms*—Waveform, communications, sensing, integrated sensing and communications (ISAC), OFDM, MIMO, waveform-defined security (WDS), software-defined radio (SDR), over-the-air, prototyping.**

I. Introduction

Wireless communications have undergone substantial advancements from 1G to 5G, with innovations spanning from low-frequency to millimeter wave (mmWave) and TeraHertz (THz) frequencies, boasting GHz signal bandwidth. Massive multiple input multiple output (MIMO) systems now integrate hundreds of antennas, and diverse signal waveforms, including orthogonal frequency division multiplexing (OFDM), and single-carrier frequency division multiple access (SC-FDMA), aiming for evolving communication standards. The exploration of advanced waveform candidates, such as non-orthogonal frequency spacing (NOFS) [1], orthogonal time frequency space (OTFS) [2], and index modulation (IM) [3], sets the stage for future 6G technologies.

In parallel, wireless signals, with their ubiquitous features, drive the popularity of smart applications like radar sensing and radio frequency (RF) sensing. Google's mmWave radar system, 'Soli', [4] explores the potential of mmWave at 60 GHz to interpret subtle finger gestures. Other applications include the integration of cameras with frequency-modulated continuous wave (FMCW) radar for 3D object detection [5], ultra-wideband (UWB) MIMO radar for behind-wall object detection [6], and innovative techniques like inverse synthetic aperture radar (ISAR) for moving object analysis [7]. Furthermore, leveraging WiFi signals for sensing functions [8], particularly estimating human activities, has gained attention. While received signal strength indicator (RSSI) and channel state information (CSI) offer distinct methods for estimating human activities, challenges remain in achieving accurate detections due to resolution limitations and sensitivity to noise.

Therefore, the integration of sensing and communication signals, leading to the concept of integrated sensing and communication (ISAC) [9], is becoming important. We have implemented and tested dual-functional ISAC testbeds [10], [11], [12], in which communication and sensing functions are integrated in one single system using one single signal waveform. The aim is to achieve a balanced trade-off between sensing and communication. Unlike existing pure-sensing and pure-communication system designs, the prototyping testbed can realize sensing and communication using the same time, frequency and spatial resources. The designed dual-functional ISAC waveform can be easily incorporated into existing communication standards where OFDM is used.

However, the dual-functional ISAC has fundamental security issues where sensing signals contain sensitive communication information that could be captured and decoded by eavesdroppers. The sensing beam shares the same waveform with communications utilizing the same time, frequency, and spatial resources. In this case, sensitive information might be leaked to eavesdroppers. This is a critical issue for dual-functional ISAC systems. This work aims to set up an experiment testbed to evaluate and address the security problems in dual-functional ISAC systems via practical validations.

II. Communication Model

We examine a multi-user MIMO-OFDM communication model, where the received signal is formulated as

$$\mathbf{Y} = \mathbf{H}\tilde{\mathbf{X}} + \mathbf{W}, \tag{1}$$

where $\mathbf{Y} = [\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_K]^T \in \mathbb{C}^{K \times L}$ denotes K parallel sample vectors for K receiver-side users, each with L samples. $\mathbf{H} = [\mathbf{h}_1, \mathbf{h}_2, ..., \mathbf{h}_K]^T \in \mathbb{C}^{K \times N}$ is a multiple input multiple output (MIMO) channel matrix, with N as the number of transmitter-side antennas. $\tilde{\mathbf{X}} =$

$[\tilde{\mathbf{x}}_1, \tilde{\mathbf{x}}_2, ..., \tilde{\mathbf{x}}_N]^T \in \mathbb{C}^{N\times L}$ represents the transmission symbol matrix after precoding, and $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, ..., \mathbf{w}_K]^T \in \mathbb{C}^{K\times L}$ indicates K parallel noise vectors for K receiver-side users, each with L noise samples. The expression in (1) can be rephrased as

$$\mathbf{Y} = \mathbf{X} + \underbrace{(\mathbf{H}\tilde{\mathbf{X}} - \mathbf{X})}_{MUI} + \mathbf{W}, \tag{2}$$

where $\mathbf{X} = [\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_K]^T \in \mathbb{C}^{K\times L}$ represents the user-side multicarrier symbol matrix. The term within the bracket in (2) signifies multi-user interference (MUI), and the total power contributed by the MUI term is computed as

$$P_{MUI} = \left\|\mathbf{H}\tilde{\mathbf{X}} - \mathbf{X}\right\|_F^2, \tag{3}$$

where $\|\cdot\|_F$ represents the Frobenius matrix norm. The value of P_{MUI} is determined by the quality of precoding. To minimize P_{MUI}, we optimize $\tilde{\mathbf{X}}$ such that its multiplication with the channel $\mathbf{H}$ approximates $\mathbf{X}$.

III. Sensing Model

Achieving directional or omnidirectional sensing beams from a MIMO system requires the proper design of $\tilde{\mathbf{X}}$. Instead of directly tuning $\tilde{\mathbf{X}}$, it is common practice to design the covariance matrix [13] of sensing signals. The spatial covariance matrix of $\tilde{\mathbf{X}}$ is expressed as

$$\mathbf{R}_d = \frac{1}{L}\tilde{\mathbf{X}}\tilde{\mathbf{X}}^H, \tag{4}$$

where $\mathbf{R}_d$ dictates the sensing beampattern, requiring positive-definiteness and satisfying $L \geq N$.

To realize sensing and communications using a joint waveform, it is necessary to optimize the transmission symbol matrix $\tilde{\mathbf{X}}$, minimizing P_{MUI} in (3) while simultaneously adhering to the MIMO radar constraints in (4).

In an omnidirectional MIMO system, the transmission waveform matrix $\tilde{\mathbf{X}}$ must be orthogonal, ensuring its corresponding covariance matrix is an identity matrix. The optimization problem is formulated as

$$\begin{aligned} \min_{\tilde{\mathbf{X}}} \quad & \left\|\mathbf{H}\tilde{\mathbf{X}} - \mathbf{X}\right\|_F^2 \\ \text{s.t.} \quad & \frac{1}{L}\tilde{\mathbf{X}}\tilde{\mathbf{X}}^H = \frac{P_T}{N}\mathbf{I}_N, \end{aligned} \tag{5}$$

where $\mathbf{I}_N$ is an $N \times N$ identity matrix, and P_T denotes the total transmission power.

In a directional MIMO system, a unique positive-definite covariance matrix $\mathbf{R}_d$ [13] is considered in the MUI optimization problem as

$$\begin{aligned} \min_{\tilde{\mathbf{X}}} \quad & \left\|\mathbf{H}\tilde{\mathbf{X}} - \mathbf{X}\right\|_F^2 \\ \text{s.t.} \quad & \frac{1}{L}\tilde{\mathbf{X}}\tilde{\mathbf{X}}^H = \mathbf{R}_d, \end{aligned} \tag{6}$$

The optimization in (5)(6) requires a trade-off because transmission power has to be properly allocated to communications and sensing.

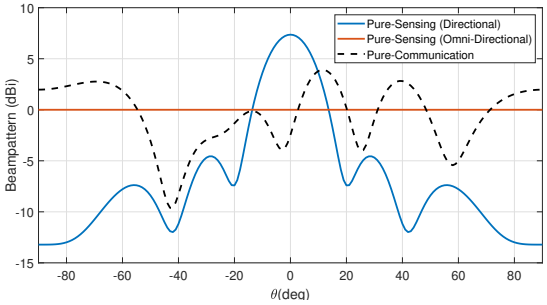

Fig. 1. Sensing beampattern illustration for pure-communication systems (γ=1) using OFDM signals, and pure-sensing systems (γ=0) considering directional and omnidirectional beampatterns.

IV. Dual-Functional ISAC Model

To optimize the trade-off between sensing and communications, previous work in [12] introduced a trade-off factor γ to balance the performance of the communication and sensing. The methodology is to define the preferred sensing waveform $\mathbf{X}_d$ and search for the optimal design of $\tilde{\mathbf{X}}$. The trade-off optimization problem, considering the total power constraint, is formulated as

$$\begin{aligned} \min_{\tilde{\mathbf{X}}} \quad & \gamma\left\|\mathbf{H}\tilde{\mathbf{X}} - \mathbf{X}\right\|_F^2 + (1-\gamma)\left\|\tilde{\mathbf{X}} - \mathbf{X}_d\right\|_F^2 \\ \text{s.t.} \quad & \frac{1}{L}\left\|\tilde{\mathbf{X}}\right\|_F^2 = P_T, \end{aligned} \tag{7}$$

where the first term, $\left\|\mathbf{H}\tilde{\mathbf{X}} - \mathbf{X}\right\|_F^2$, aims to minimize the MUI, while the second term, $\left\|\tilde{\mathbf{X}} - \mathbf{X}_d\right\|_F^2$, aims to enforce the signal waveform to approach the desired sensing waveform $\mathbf{X}_d$. The trade-off factor $0 \leq \gamma \leq 1$ determines the balance between communication and sensing performance.

The two Frobenius norms can be expanded and combined in a single norm format as

$$\begin{aligned} &\gamma\left\|\mathbf{H}\tilde{\mathbf{X}} - \mathbf{X}\right\|_F^2 + (1-\gamma)\left\|\tilde{\mathbf{X}} - \mathbf{X}_d\right\|_F^2 \\ &= \left\|[\sqrt{\gamma}\mathbf{H}^T, \sqrt{1-\gamma}\mathbf{I}_N]^T\tilde{\mathbf{X}} - [\sqrt{\gamma}\mathbf{X}^T, \sqrt{1-\gamma}\mathbf{X}_d^T]^T\right\|_F^2. \end{aligned} \tag{8}$$

We define $\mathbf{A} = [\sqrt{\gamma}\mathbf{H}^T, \sqrt{1-\gamma}\mathbf{I}_N]^T \in \mathbb{C}^{(K+N)\times N}$, $\mathbf{B} = [\sqrt{\gamma}\mathbf{X}^T, \sqrt{1-\gamma}\mathbf{X}_d^T]^T \in \mathbb{C}^{(K+N)\times L}$. Therefore, (7) can be reformulated as

$$\begin{aligned} \min_{\tilde{\mathbf{X}}} \quad & \left\|\mathbf{A}\tilde{\mathbf{X}} - \mathbf{B}\right\|_F^2 \\ \text{s.t.} \quad & \left\|\tilde{\mathbf{X}}\right\|_F^2 = LP_T. \end{aligned} \tag{9}$$

The optimization problem in (9) is non-convex. Here we explore a closed-form sub-optimal solution by employing the straightforward least squares (LS) method under the total power constraint, as follows:

$$\tilde{\mathbf{X}} = \frac{\sqrt{LP_T}}{\|\mathbf{A}^\dagger\mathbf{B}\|_F}\mathbf{A}^\dagger\mathbf{B}, \tag{10}$$

where $(\cdot)^\dagger$ represents the pseudo inverse of the matrix.

To have a better understanding of (7), the trade-off performance between pure-communication systems ($\gamma = 1$) and pure-sensing systems ($\gamma = 0$) is illustrated in Fig. 1. When

the trade-off factor $\gamma = 0$, the waveform closely matches the ideal sensing waveform, as depicted in Fig. 1, noted as 'Pure-Sensing', but deviates significantly from the 'Pure-Communication' waveform. It is noted that the scenario with $\gamma = 0$ would result in performance degradation in communications. In contrast, increasing the trade-off factor to $\gamma = 1$ eliminates the sensing part in (7). As a result, the communication part dominates the ISAC system, and the waveform is more likely to adhere to optimal communication constraints. With $\gamma = 1$, the system exhibits pure communication functionality, and Fig. 1 demonstrates that the sensing beampattern does not have obvious directivity, significantly differing from the omni-directional and directional patterns of the pure-sensing systems. For values of γ between 0 and 1, a trade-off exists between communication and sensing performance. Increasing γ prioritizes communication, sacrificing sensing performance, and vice versa.

V. Waveform-Defined Security

The key reason for data leakage is that both the communication and sensing functions share the same signal waveform. The common solution is to exploit techniques to generate a narrower beam to separate legitimate users and eavesdroppers. A more advanced solution relies on the constructive interference precoding [14] at the legitimate user while leaving destructive interference to eavesdroppers. However, the above solutions require accurate CSI, while in harsh environments, CSI is not always available. In addition, when an eavesdropper is positioned very close to the legitimate user, it is physically impossible to use precoding or beamforming to isolate them. Due to this consideration, a waveform-based security technique, termed waveform-defined security (WDS) [15], was proposed and tested in a WiFi framework to introduce signal inter carrier interference (ICI) to eavesdroppers even CSI is not known. The WDS signal is mathematically given by

$$X_k = \frac{1}{\sqrt{Q}} \sum_{n=0}^{N-1} s_n \exp\left(\frac{j2\pi nk\alpha}{Q}\right), \tag{11}$$

where X_k is the time sample with the index of $k = 0, 1, ..., Q-1$,$Q = \rho N$, the number of time samples, N is the number of sub-carriers, ρ is the oversampling factor, $\frac{1}{\sqrt{Q}}$ is the scaling factor, s_n is the n^{th} single-carrier symbol in one WDS symbol, and $\alpha = \Delta f \cdot T$ is the bandwidth compression factor where Δf is the sub-carrier spacing and T is the time duration of one symbol. The way to define the sub-carrier packing strategy depends on the value of α. Specifically, when α=1, it indicates an OFDM signal. For all other values α <1, a non-orthogonal signal is obtained.

VI. Experiment Setup and Validation

A. Experiment Platform Setup

The experiment is conducted within an indoor laboratory, offering a strong line of sight (LOS) channel condition along with multipath effects. The application scenario of the experiment setup is illustrated in Fig. 2, showing positions for the transmitter, legitimate user (User-1, User-2), and an eavesdropper. In this environment, MIMO precoding is employed to minimize interference and ensure interference-free

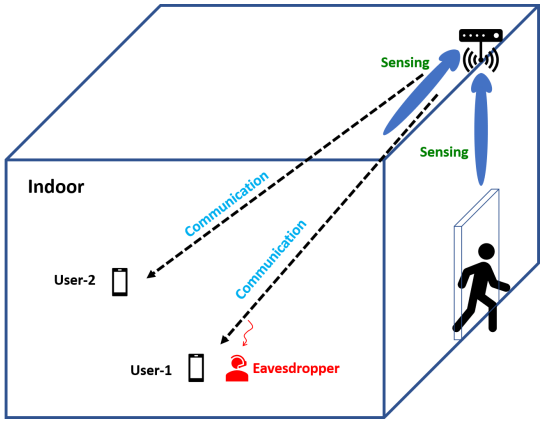

Fig. 2. Application scenario of the dual-functional ISAC experiment and its potential security challenge.

communication for users. Simultaneously, sensing beams can be generated from the same transmitter. In a secure setup where the beam is directed away from the two users, sensing can effectively detect human activities. However, when the beam aligns with the users, it carries user data information. An eavesdropper, situated at a close distance to the legitimate user, can easily decode the data without the need for complex signal processing. The primary objective of this experiment is to assess the potential for data leakage and propose effective solutions to mitigate this challenge.

In the experimental setup depicted in Fig. 3, our MIMO-OFDM platform is designed with N_{Tx}=6 transmitter antennas and supports N_{UE}=2 users operating at a carrier frequency of f_{RF}=2.4 GHz. It is noted that we use partial RF chains from the platform aiming for a simple demonstration. The base station includes an array of six omni-directional antennas arranged in a uniform linear array (ULA) structure at the top, with a spacing of half a wavelength. Each antenna connects to an independent RF chain within the USRP-RIO-2953R to explore the spatial diversity. In this experiment, we configure a sampling rate of 20 MS/s for each signal from an RF chain. We use QPSK modulation format to evaluate the communication performance and its effect on sensing beampattern performance. The number of data sub-carriers is 12, and the inverse fast Fourier transform (IFFT) size is 128. Additionally, each OFDM symbol includes 10 cyclic prefix (CP) samples to mitigate the effects of multipath channel propagation.

The measured results for directional sensing beampattern are displayed in Fig. 3. The theoretical transmitter side directional beampattern from the base station, based on the estimated MIMO channels, serves as a benchmark in Fig. 3(a). Without the trade-off, Fig. 3(b) shows good communication performance, potentially enhancing bit error rate (BER) performance but causing more distorted sensing beampatterns. It is evident that the beampattern is far from the ideal directional one. The impact of γ on communication performance is evident, with a smaller value γ=0.9 leading to more scattered constellation points in Fig. 3(d). On the other hand, the reduction of γ improves the beampattern in Fig. 3(c) where an ideal directional

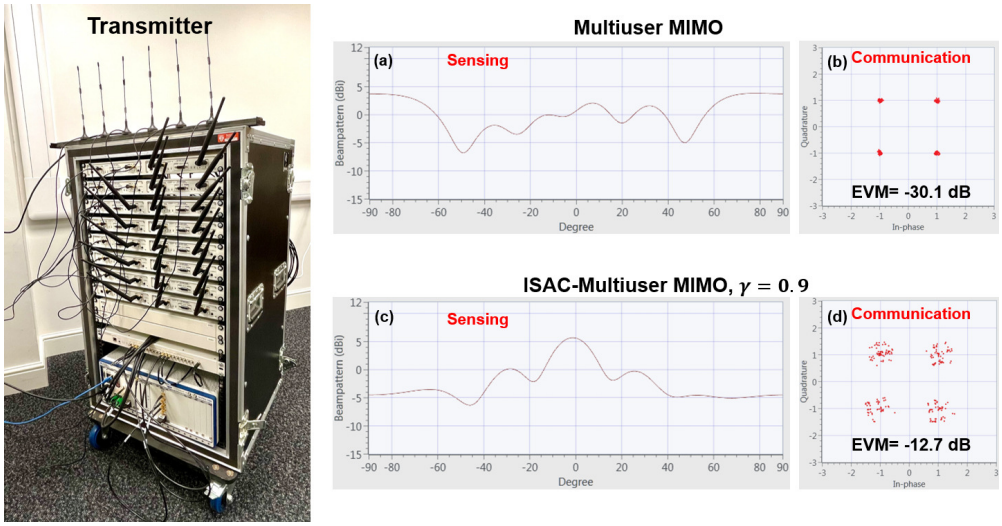

Fig. 3. Dual-functional ISAC experiment transmitter setup and illustration of the trade-off between sensing and communications.

beampattern is illustrated. This displays a trade-off between communication performance and beampattern quality. Fig. 3 highlights that a smaller γ results in a better sensing beampattern but worse communication performance. In the following experiment, we still use the trade-off value γ=0.9, as it shows a clear separation of constellation points while maintaining a relatively ideal beampattern shape.

The experimental ISAC signal framework in this work follows the structure outlined in [16], as depicted in Fig. 4. Here, 20 resource blocks are allocated to create a single frame, with a time duration of 10 ms. The initial resource block is allocated for signaling overhead, primarily designed for MIMO channel estimation. Each resource block includes seven OFDM symbols, and an interleaving OFDM symbol allocation scheme is implemented for the first resource block. Addressing interference stemming from different MIMO antennas, the overhead at each antenna is multiplexed in time, as depicted in Fig. 4. In this configuration, while the data part may encounter interference, the overhead segment remains free of interference leading to accurate CSI estimation and MIMO precoding.

B. Security Issue and Solutions for Dual-Functional ISAC

For the security evaluation, we are doing a comparison experiment as displayed in Fig. 5. Two legitimate users (LU-1, LU-2) are placed in front of the transmitter with sufficient spacing, and their performance serves as an indicator of communication quality. To assess communication security, we introduce an eavesdropper (Eve) positioned next to LU-1 with a 4 cm gap. The expectation is that Eve can intercept the signal directed to LU-1. We evaluate both traditional OFDM-enabled ISAC-multiuser MIMO signals and a security waveform WDS enabled ISAC-multiuser MIMO signals to generate constellation diagrams for LU-1 and Eve.

In the experiment detailed in Fig. 5, we maintain the positions of legitimate users and the eavesdropper for both scenarios while only modifying signal patterns. It is expected that LU-1's performance shows degradation since a portion of the power is allocated to support the sensing function. Conversely, on the eavesdropper side, Eve can successfully detect the signal and recover its constellation points. This is due to the ISAC nature, where a directional sensing beam carrying data information is radiated towards LU-1 and its neighboring Eve. Unfortunately, in this scenario, the directional beam with high power inadvertently aids Eve in capturing and decoding legitimate user signals. This poses a significant challenge for ISAC, especially when a single beam is utilized for both sensing and communication functions.

The principle for the WDS signal is illustrated in Fig. 5 where sub-carriers are non-orthogonally packed resulting in ICI. Without accurate knowledge of α and signal detection algorithms, an eavesdropper cannot decode signals even with perfect capture of legitimate user signals. With such signal configurations, it is observed that the legitimate user, with knowledge of α and signal detection method, can recover signals with similar performance to the OFDM signal. On the other hand, at the eavesdropper, without the knowledge of α and detection algorithms, communication performance becomes worse with the error vector magnitude (EVM) degraded by around 7 dB. This verifies that a proper signal waveform design can help to enhance ISAC security.

VII. Conclusion

The experiment validates the dual-functionality of the proposed ISAC transmission scheme in the real world, providing insights into the trade-off between communication and sensing functions. In addition, the experiment also studies the data leakage issue when a directional ISAC beam is used for sensing and communications. Results show that when an eavesdropper is placed next to a legitimate user, spacing at 4 cm, the eavesdropper can successfully capture legitimate user signals and recover constellations with high accuracy. The observed results contribute to the ongoing research in integrated sensing and communication especially in security considerations, demonstrating the feasibility and

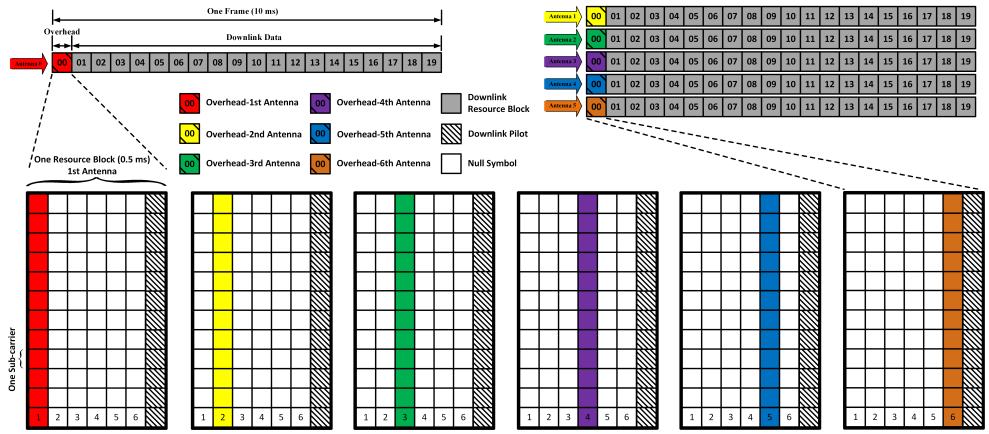

Fig. 4. Frame and resource block structure for the dual-functional sensing and communication multiuser MIMO system.

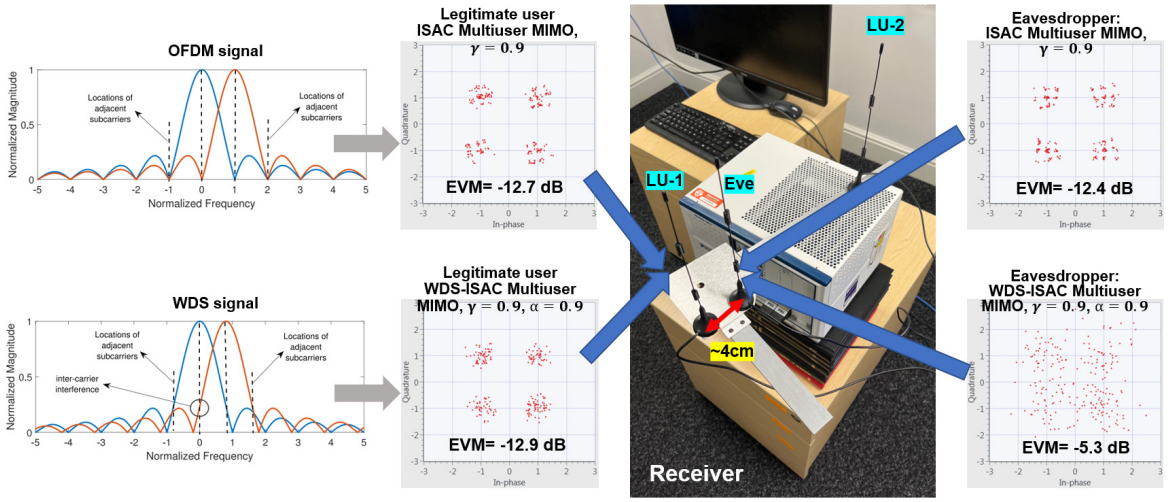

Fig. 5. Dual-functional ISAC experiment receiver setup. The legitimate user and eavesdropper constellation performance for OFDM enabled ISAC system and WDS enabled ISAC system.

potential risks of a dual-functional approach in practical scenarios.

REFERENCES

[1] T. Xu and I. Darwazeh, "Identification and practical validation of spectrally efficient non-orthogonal frequency shaping waveform," *Nature Communications Engineering*, vol. 2, no. 58, 2023.

[2] R. Hadani and et al., "Orthogonal time frequency space modulation," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, 2017, pp. 1–6.

[3] Y. Chen, T. Xu, and I. Darwazeh, "Index modulation pattern design for non-orthogonal multicarrier signal waveforms," *IEEE Transactions on Wireless Communications*, vol. 21, no. 10, pp. 8507–8521, 2022.

[4] J. Lien and et al., "Soli: Ubiquitous gesture sensing with millimeter wave radar," *ACM Trans. Graph.*, vol. 35, no. 4, Jul. 2016.

[5] G. Zhang, H. Li, and F. Wenger, "Object detection and 3D estimation via an FMCW radar using a fully convolutional network," *ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 4487–4491, 2020.

[6] Z. Hu and et al., "Design and analysis of a UWB MIMO radar system with miniaturized Vivaldi antenna for through-wall imaging," *Remote Sensing*, vol. 11, no. 16, 2019.

[7] F. Adib and D. Katabi, "See through walls with WiFi!" New York, NY, USA: Association for Computing Machinery, 2013.

[8] IEEE 802.11bf Task Group (TG), "Status of project IEEE 802.11bf," 2021. [Online]. Available: https://www.ieee802.org/11/Reports/tgbf_update.htm

[9] International Telecommunication Union, "IMT towards 2030 and beyond," https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2030/Pages/default.aspx, June 2023.

[10] T. Xu, F. Liu, C. Masouros, and I. Darwazeh, "An experimental proof of concept for integrated sensing and communications waveform design," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1643–1655, 2022.

[11] ——, "Proof of concept experiments of joint waveform design for integrated sensing and communications," in *1st ACM MobiCom Workshop on Integrated Sensing and Communication Systems (ISACom 2022) (ISACom 2022)*, Sydney, Australia, Oct. 2022.

[12] F. Liu, L. Zhou, C. Masouros, A. Li, W. Luo, and A. Petropulu, "Toward dual-functional radar-communication systems: Optimal waveform design," *IEEE Transactions on Signal Processing*, vol. 66, no. 16, pp. 4264–4279, 2018.

[13] D. R. Fuhrmann and G. San Antonio, "Transmit beamforming for MIMO radar systems using signal cross-correlation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 44, no. 1, pp. 171–186, 2008.

[14] N. Su, F. Liu, Z. Wei, Y.-F. Liu, and C. Masouros, "Secure dual-functional radar-communication transmission: Exploiting interference for resilience against target eavesdropping," *IEEE Transactions on Wireless Communications*, vol. 21, no. 9, pp. 7238–7252, 2022.

[15] T. Xu, "Waveform-defined security: A low-cost framework for secure communications," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10 652–10 667, July 2022.

[16] T. Xu, C. Masouros, and I. Darwazeh, "Waveform and space precoding for next generation downlink narrowband IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5097–5107, Jun. 2019.