OFDM based WiFi Passive Sensing: a reference-free non-coherent approach

Francesca Filippini†, Marco Di Seglio†, Carlo Bongioanni†, Paul V. Brennan‡, Fabiola Colone†

†Dept. of Information Engineering, Electronics and Telecommunications, Sapienza University of Rome, Italy
{francesca.filippini, marco.diseglio, carlo.bongioanni, fabiola.colone}@uniroma1.it

‡Department of Electronic and Electrical Engineering, University College London, U.K.
p.brennan@ucl.ac.uk

***Abstract* — WiFi based passive sensing is attracting considerable interest in the scientific community for both research and commercial purposes. In this work, we aim at taking a step forward in an endeavor to achieve good sensing capabilities employing compact, low-cost, and stand-alone WiFi sensors. To this end, we resort to a reference-free non-coherent signal processing scheme, where the presence of a moving target echo is sought by detecting the amplitude modulation that it produces on the direct signal transmitted from the WiFi access point. We first validate the proposed strategy against simulated data, identifying advantages and limitations. Then, we apply the conceived solution on experimental data collected in a small outdoor area with the purpose of detecting a small cooperative drone.**

Keywords* — *ISAC, WiFi signals, passive sensing, non-coherent radar, IEEE 802.11, UAV detection.

I. INTRODUCTION

In recent years, the steadily proliferating use of wireless devices has ensured that access points (APs) based on WiFi standards [1] are now available in almost all private and public environments. The parasitic exploitation of such transmitters as sources of opportunity to perform sensing purposes paves the way to the emerging technology of integrated sensing and communication (ISAC) systems, critical in responding to the growing congestion of the RF spectrum [2][3].

The suitability of WiFi signals for local area and indoor monitoring has been investigated in [4]-[11] and related works. The implementation of such sensing solutions for monitoring public or private areas is very appealing since they are not affected by lighting conditions and they alleviate many privacy concerns and discomfort issues that cameras might cause. Specifically, RF radar sensors do not require any cooperation from the target, such as carrying a wearable device. Finally, the parasitic exploitation of existing RF sources brings in additional benefits in terms of energy consumption and potential interference with pre-existing RF systems operating in the same area. Therefore, nowadays, the field of application of passive WiFi sensing solutions ranges from occupancy estimation, detection and localization of humans or small unmanned aerial vehicles (UAVs) to the e-healthcare applications such as human gait recognition or breath detection.

However, most of the techniques proposed in the technical literature set strict requirements on the implementation of the WiFi sensor. For instance, channel state information (CSI) based approaches [8]-[10] require a perfect knowledge of the adopted WiFi Standards and are limited to work with orthogonal frequency division multiplexing (OFDM) signals. Moreover, they require accurate synchronization in both time, frequency, and phase. On the other hand, WiFi based passive radar (PR) approaches [4]-[7] can be in principle operated with any waveform modulation and have the potential to increase the sensitivity of the sensor. However, they are typically limited by the high computational complexity and the requirement for a reference signal.

The authors have first addressed the computational complexity issue in [7], where a streamlined PR processing chain has been proposed. Then, in [11], the possibility of limiting the passive radar signal processing to *a priori* known portions of the physical layer protocol data unit (PPDU) without requiring any dedicated receiving channel or reconstruction has been considered. However, along with an expected signal-to-noise ratio (SNR) loss, the use of a synthetic reference signal does not guarantee synchronization in time, frequency, and phase with the main surveillance signal and ad hoc approaches must be implemented to restore the coherency.

Despite the recent efforts, to facilitate the widespread use of WiFi-based sensors, key aspects must be taken into account such as the low cost and low computational complexity, the compactness and lightness, as well as the easy deployment and setup. For the above reasons, in this manuscript, we resort to a reference-free non-coherent approach and we investigate the possibility of detecting the presence of a moving target in the observed scene by observing the amplitude modulation that it induces on the main source signal. This principle of operation that exploits the interference amplitude pattern between the transmitted signal and reflections from the environment, has been widely investigated for non-coherent radar and forward scatter radar (FSR) [12]-[14] and has been recently proposed and adapted to the application at hand in [15].

First, we present the proposed strategy approach in Section II; then, in Section III, we validate its effectiveness against simulated WiFi data employing different OFDM constellations. In Section IV, we present some experimental results against real-world data with a small UAV employed as cooperative target. Finally, Section V reports our concluding remarks.

II. INTERFERENCE DOPPLER PROCESSING

We consider a train of consecutive packets emitted by a WiFi AP. Let T_s be the temporal duration of a given packet, composed by $N_s N_{sym} = T_s f_s$ samples, being f_s the employed sampling frequency, N_s the number of samples inside each symbol and N_{sym} the number of symbols inside each packet. Note that, altough a practical transmission tipically includes packets with different durations, we can always assume to cut the packets to a common length of N_{sym} symbols. Proof of the advantage of this choice is reported in [15]. The collected signal is given by the coherent superposition of the direct signal transmitted by the AP, the delayed and Doppler shifted echoes from N_T moving targets, as well as thermal noise. Additionally, the direct signal reflections on stationary obstacles, e.g., walls, might be present. Assuming negligible multipath contributions, the discrete version of the complex baseband signal received for the pth WiFi packet is written as

$$\begin{aligned} & x_p(l) \\ & = \alpha_{0,p} s_p(l) \\ & + \sum_{q=1}^{N_T} \beta_{q,p}\ s_p^{(\tau_{q,p})}(l)\ \mathrm{e}^{j\varphi_{q,p}(l)} + d_p(l) \end{aligned} \qquad (1)$$

$$l = 0, \dots, N_{sym} N_s - 1\ ;\ p = 0, 1, \dots$$

where

- $s_p(l)$ represents the waveform transmitted at the pth packet, $s_p^{(\tau)}(l)$ is its resampled version, delayed by τ. The pth packet waveform is modeled as a zero-mean unitary power random process whose characteristics depend on the modulation scheme.
- $\alpha_{0,p}$ is the complex amplitude of the diret signal at the pth packet, assumed constant within the packet.
- $\beta_{q,p}$ and $\tau_{q,p}$ $(q = 1, \dots, N_T)$ are the complex amplitude and the delay of the qth target echo at the pth packet. The typical duration of WiFi packets compared with the velocity of the targets of interest is such that $\beta_{q,p}$ and $\tau_{q,p}$ variation can be assumed negligible within the packet;
- $\varphi_{q,p}(l)$ encodes the motion induced phase variation for the qth target echo at the pth packet, and it is defined as $\varphi_{q,p}(l) = 2\pi \frac{R_{q,p}(l)}{\lambda}$, being λ the wavelength and $R_{q,p}(l) = R_{Tx-TGT_{q,p}}(l) + R_{Rx-TGT_{q,p}}(l) - B$ the relative bistatic range law of the qth target along the pth packet, being B the distance between the Tx and the Rx, and $R_{Tx-TGT_{q,p}}(l)$ and $R_{Rx-TGT_{q,p}}(l)$ the time-varying distances between the target and the Tx and between the target and the Rx, respectively.
- $d_p(l)$ is the thermal noise affecting the pth packet at the Rx. It is assumed to be a white, zero-mean complex Gaussian process with variance σ_D^2, statistically independent of the source signal.

An illustrative scenario is sketched in Figure 1 as well as the main blocks of the processing scheme proposed in [15] and aimed at recognizing the presence and extracting the instantaneous Doppler frequency of moving targets.

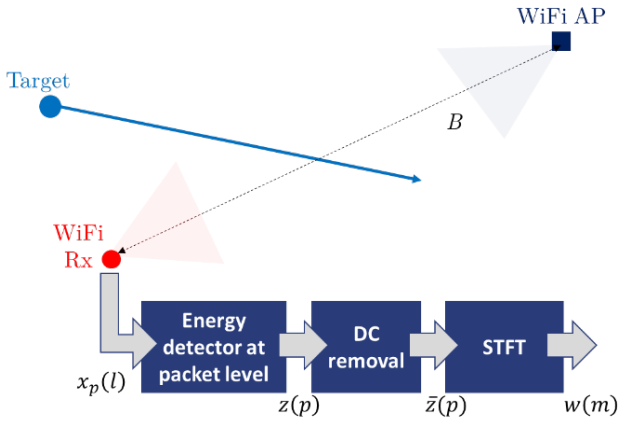


Figure 1. Processing blocks of the Interference Doppler Processing scheme.

This approach is referred to in [15] as Interference Doppler Processing (IDP). First, the square modulus of the signal is extracted, thus discarding the phase information. Then, the output of the square modulus undergoes a low-pass filter and downsampling stage with the purpose of removing the high frequency amplitude variations caused by the signal itself, to its multipath replicas and the noise contribution. A simple way to implement this block with WiFi signals is to resort to an energy detector at packet level, namely:

$$z(p) = \sum_{l=0}^{N_{sym}N_s - 1} \left| x_p(l) \right|^2 \qquad (2)$$

Once this stage has been performed, the obtained sequence undergoes the DC removal stage aimed at removing the strongest stationary scene interferences, such as the direct signal transmitted by the AP:

$$\bar{z}(p) = z(p) - z_{DC}(p) \qquad (3)$$

where $z_{DC}(p)$ denotes the average value of $z(p)$, evaluated over an appropriate time window T_{DC}. Finally, $\bar{z}(p)$ undergoes a time-frequency analysis, which results in a spectrogram where the target Doppler signature is detected. Note that, if the packet emission rate is constant over time, this stage can be implemented with a Short Time Fourier Transform (STFT) against partially overlapped batches of T_{STFT} seconds each, thus encompassing $N_P = \lfloor T_{STFT} / \Delta T_0 \rfloor$ packets:

$$w(m) = \sum_{p=0}^{N_P - 1} h(p) \bar{z}(p_0 + p) e^{-j2\pi \frac{mp}{N_P}} \qquad (4)$$

where p_0 is the first packet of the current batch and $h(p)$ is a weighting function, used to control the Doppler sidelobes level. Otherwise, if the sequence $\bar{z}(p)$ collects samples that are not taken at equally spaced time instants, one can either resort to an appropriate interpolation stage, which basically yields a resampled version of the sequence $\bar{z}(p)$ before proceeding with the FFT, or resort to a nonuniform discrete Fourier transform at each batch.

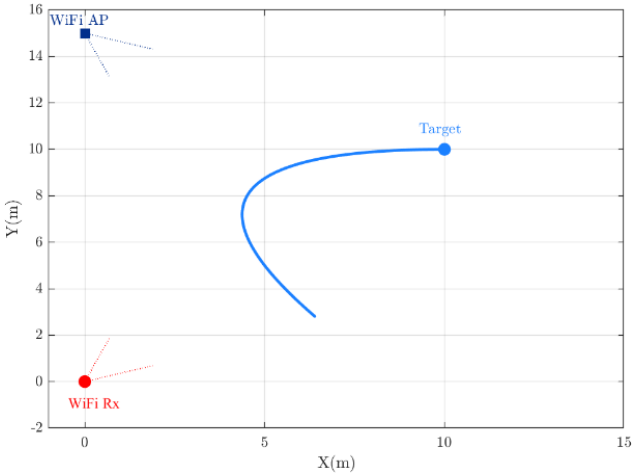


Figure 2. Simulated geometry.

The effectiveness of the proposed approach is demonstrated in the following against both simulated and real WiFi data.

III. VALIDATION AGAINST SIMULATED DATA

We generate a simulated dataset for the scenario depicted in Figure 2. A stream of OFDM modulated WiFi packets is simulated at the receiver, encompassing the signal transmitted by the AP, the signal backscattered by the point-like moving target and thermal noise. Additional details on the simulated scenario are reported in Table 1.

Figure 3 reports the output of the IDP strategy in the absolute bistatic velocity – time plane. The latter is normalized in order for the noise level to be around 0 dB. The target Doppler signature is clearly distinguished during its entire trajectory in Figure 3, demonstrating the capability of recognizing the target motion by only observing the amplitude fluctuation that it produces.

Also, we observe that the average background-to-noise (BNR) level competing with the target response is of approx. 37.5 dB, which is almost equal to DNR[2] and might jeopardize the detection of small radar cross section (RCS) targets. The authors have addressed this issue in [15], where it was shown that the background level depends on different parameters, among which the employed OFDM constellation.

Therefore, we report in Figure 4 the results obtained against simulated datasets using the same parameters as

Table 1 Simulation Parameters.

Parameter	Value
Carrier frequency (f_0)	5.18 GHz
Sampling frequency (f_s)	20 MHz
Packet repetition interval (PRI)	3 ms
Number of OFDM symbols per packet	5
OFDM Constellation	16-QAM
Target initial position (x_0,y_0)	(10, 10) m
Target initial velocity (v_x,v_y)	(-1.5, 0) m/s
Target constant acceleration (a_x,a_y)	(0.2, -0.1) m/s^2
Target signal-to-noise ratio (SNR)	-10 dB
Direct signal-to-noise ratio (DNR)	20dB

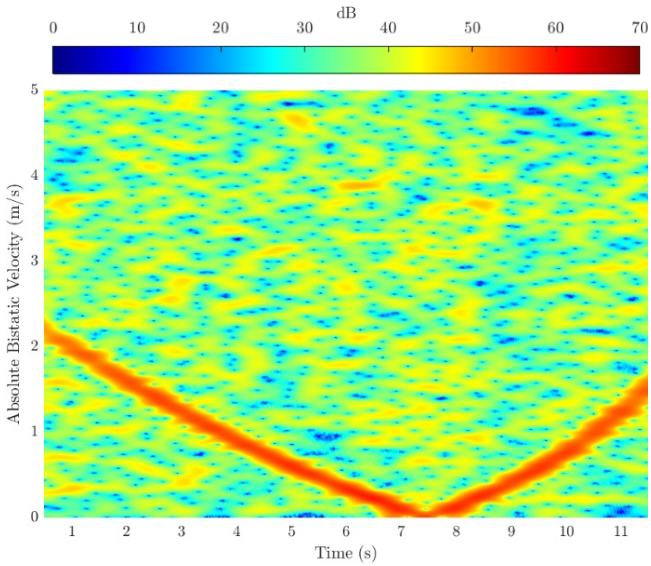


Figure 3. Absolute bistatic velocity-time map after the IDP.

above but with the stream of WiFi packets employing the three remaining OFDM constellations usually employed in WiFi Standards. Specifically, BPSK, QPSK and 64-QAM OFDM modulated packets are used to get Figure 4(a), (b) and (c), respectively.

Observing Figure 4, the different disturbance background levels are evident, being the BPSK [Figure 4(a)] the constellation that yields the darker map, denoting the lower level which in turn is expected to offer the highest capability of discriminating a target. This is confirmed by Table 2, where we report the average BNR for the different considered OFDM constellations, estimated on the final map obtained from simulated data in a target-absent condition. Based on Table 2, we confirm that, with the considered simulation parameters, the BNR level can vary of approximately 8 dB depending on the employed constellation.

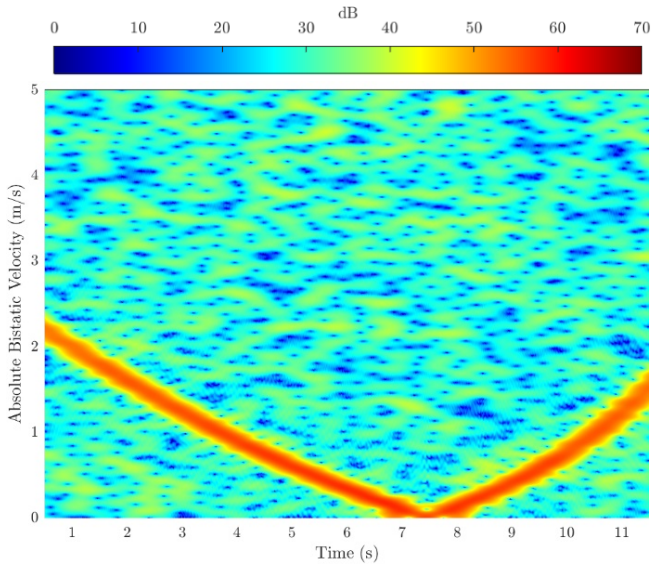
Table 2 Average background level for different OFDM constellations and DNR = 20 dB.

OFDM constellation	DNR	BNR
BPSK	20 dB	31.20 dB
QPSK	20 dB	32.79 dB
16-QAM	20 dB	37.49 dB
64-QAM	20 dB	39.01 dB

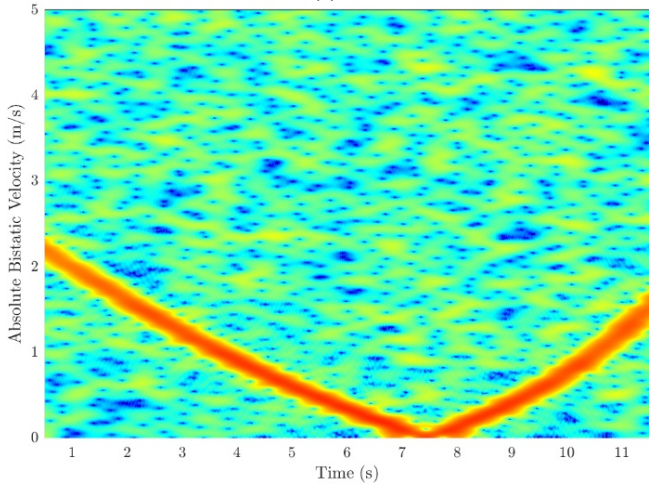
Table 3 Average background level for different OFDM constellations and DNR = 30 dB.

OFDM constellation	DNR	BNR
BPSK	30 dB	50.52 dB
QPSK	30 dB	52.31 dB
16-QAM	30 dB	57.37 dB
64-QAM	30 dB	58.95 dB

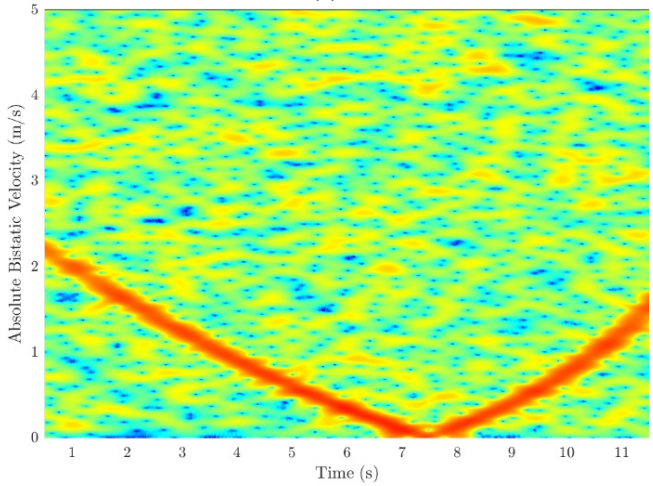
A further demonstration is obtained by observing the results in Table 3, obtained by repeating the analysis considering DNR = 30 dB. Note that, altough high BNR levels might not be an issue for large RCS targets, they might represent a limitation and jeopardise the capability to detect smaller targets.



(a)



(b)



(c)

Figure 4. Results of the IDP approach against streams of OFDM modulated packets with (a) BPSK (b) QPSK (c) 64-QAM constellation.

Based on the results reported in this Section, an appropriate theoretical characterization of the predicted background level is needed and could pave the way for solutions or processing strategies aimed at reducing it.

IV. VALIDATION AGAINST EXPERIMENTAL DATA

In this Section, we demonstrate the effectiveness of the proposed IDP approach on real-world WiFi data, collected during an ad hoc acquisition campaign.

A. Acquisition campaign

The test was conducted in a private outdoor premise, see Figure 5. A commercial WiFi AP (TP-Link Archer VR600 AC1600) was employed and set to transmit signal according to the IEEE 802.11ac Standard [1] at carrier frequency of 5.18 GHz. This device was conneted to a transmitting directive antenna (Ubiquiti UMA-D), see the green square in Figure 5. The employed dataset was collected with an Ubiquiti UMA-D directive antenna, connected to a National Instruments NI USRP-2955 board, see orange square in Figure 5. The NI USRP-2955 board features four receiving channels, independently down converted and simultaneously sampled, operating in the frequency range 10 MHz – 6 GHz, with 80 MHz maximum instantaneous real-time bandwidth and additional gain for each channel from 0 to 95 dB, in 1 dB step. A small DJI Mavic Pro drone (see the red circle in Figure 5) was employed as cooperative target. We extract a one minute long portion of the acquisition, during which the drone moves back and forth twice along the trajectory described by the dashed red line.

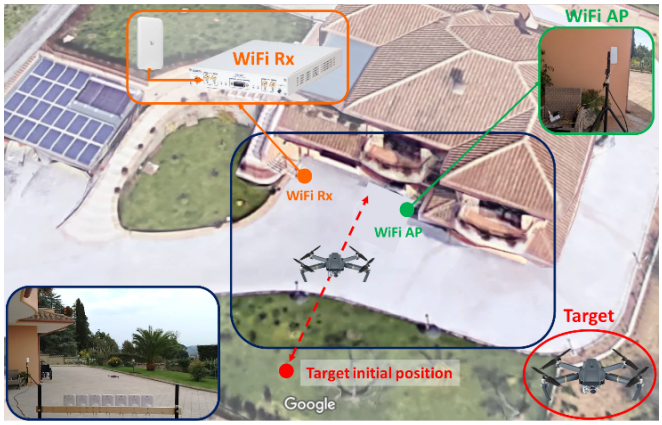


Figure 5. Acquisition geometry.

B. Experimental results

Figure 6 shows the output of the IDP technique on the described dataset. The two subfigures are obtained with OFDM modulated packets with different constellations. Specifically, Figure 6(a) is obtained selecting only ACK packets, while Figure 6(b) is obtained selecting only RTS packets, respectively employing a QPSK and a 16-QAM constellation for the OFDM symbols outside the PHY Preamble. In both cases, we extract $N_{sym} = 2$ of those OFDM symbols.The DC component is removed in a sliding fashion with a window of 0.5s while the STFT is obtained with T_{STFT} = 0.8s, with a Hamming tapering window applied to control the Doppler sidelobe level.

Figure 6 shows that, although the target is characterized by a very low RCS, the proposed solution is able to detect it for a remarkable part of its trajectory against the competing background.

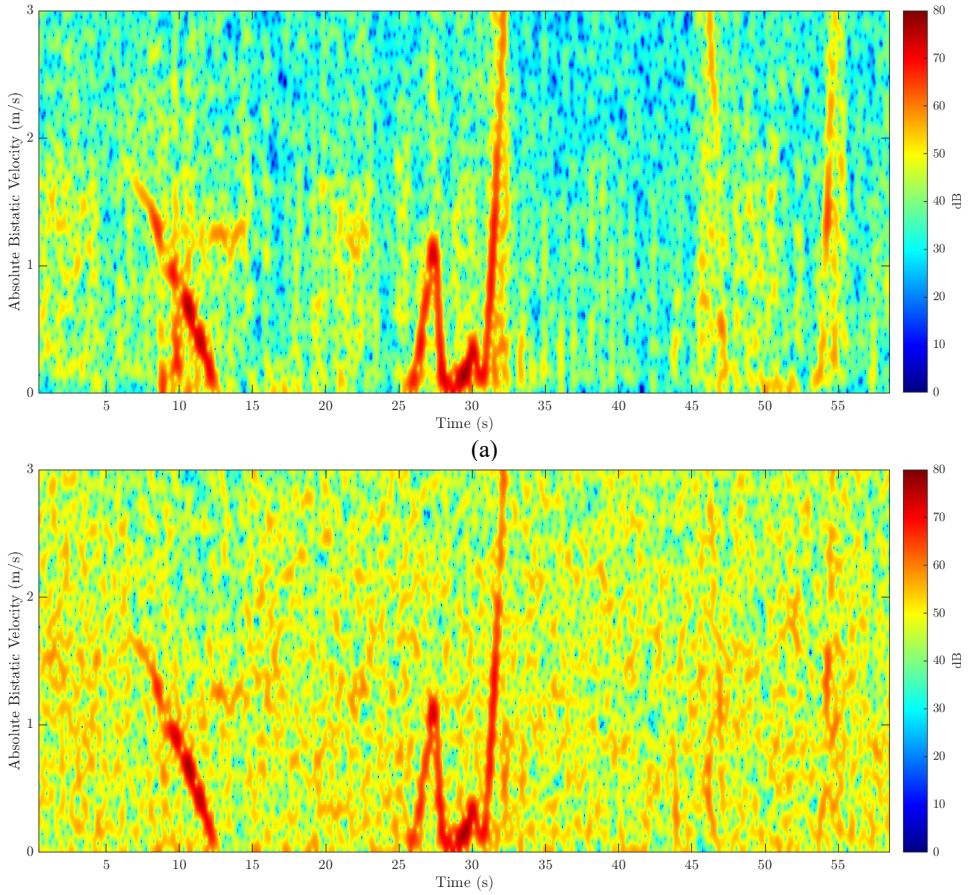


Figure 6. Results of the IDP approach applied to real data with cooperative drone using $N_{sym} = 2$ OFDM symbols with (a) QPSK and (b) 16-QAM constellation.

We recall that this is obtained by only extracting the amplitude information from the collected signal. Specifically, we can clearly recognize the first part of the track between 5s and 35s, during which the target starts from its initial position, marked as a red dot in Figure 5, approaches the AP-Rx baseline, rotates on itself, and then turns back. Note that, when returning to its initial position, the target rapidly changes the altitude, explaining the signature between 25s and 30s.

The aforementioned portion of the target trajectory is recognized in both subfigures regardless of the employed OFDM constellation; however, note that the average background level is quite different between the two subfigures. This confirms what shown before on simulated data, namely that the higher is the number of points in the employed OFDM constellation, the higher is the BNR level which might jeopardize the capability to detect small targets. This is evident in the second portion of the trajectory, between 45s and 55s, where the target return is completely buried below the background level in Figure 6(b). In contrast, some small portion of the track would be visible in Figure 6(a), however the track continuity is jeopardized.

This demonstrates the need to employ strategies that lower the background level to increase the ability to recognize targets.

V. CONCLUSIONS

In this paper we have proposed a reference-free non-coherent approach for WiFi based passive sensing. This approach aims at providing the capability of monitoring a local area while meeting the requirements of compactness, low cost and complexity as well as stand-alone operability. Based on the proposed processing scheme, we look for the presence of a moving target by detecting the amplitude modulation that it produces on the direct signal emitted from the WiFi transmitter. We have validated the proposed strategies against simulated OFDM WiFi data; then we also reported an experimental validation against real-world WiFi data collected in an ad hoc acquisition campaign with a cooperative drone. We have demonstrated the effectiveness of the proposed strategy; however we have also identified the main limitation, represented by an high background level competing with the target response.

REFERENCES

[1] Wireless LAN Medium Access Control (MAC) and physical Layer (PHY) Specifications, IEEE Std. 802.11, 2016.

[2] Y. Cui, F. Liu, X. Jing and J. Mu, "Integrating Sensing and Communications for Ubiquitous IoT: Applications, Trends, and Challenges," in *IEEE Network*, vol. 35, no. 5, pp. 158-167, September/October 2021.

[3] A. Liu *et al*., "A Survey on Fundamental Limits of Integrated Sensing and Communication," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 994-1034, Secondquarter 2022.

[4] F. Colone, P. Falcone, C. Bongioanni and P. Lombardo, "WiFi-Based Passive Bistatic Radar: Data Processing Schemes and Experimental Results," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 48, no. 2, pp. 1061-1079, April 2012.

[5] K. Chetty, G. E. Smith and K. Woodbridge, "Through-the-Wall Sensing of Personnel Using Passive Bistatic WiFi Radar at Standoff Distances," in *IEEE Transactions on Geoscience and Remote Sensing*, vol. 50, no. 4, pp. 1218-1226, April 2012.

[6] H. Sun, L. G. Chia and S. G. Razul, "Through-Wall Human Sensing With WiFi Passive Radar," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 57, no. 4, pp. 2135-2148, Aug. 2021.

[7] F. Colone, F. Filippini, M. Di Seglio and K. Chetty, "On the Use of Reciprocal Filter Against WiFi Packets for Passive Radar," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 4, pp. 2746-2761, Aug. 2022.

[8] B. Tan, Q. Chen, K. Chetty, K. Woodbridge, W. Li and R. Piechocki, "Exploiting WiFi Channel State Information for Residential Healthcare Informatics," in *IEEE Communications Magazine*, vol. 56, no. 5, pp. 130-137, May 2018.

[9] J. Liu, Y. Chen, Y. Wang, X. Chen, J. Cheng and J. Yang, "Monitoring Vital Signs and Postures During Sleep Using WiFi Signals," in *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2071-2084, June 2018.

[10] C. Wu, F. Zhang, Y. Hu and K. J. R. Liu, "GaitWay: Monitoring and Recognizing Gait Speed Through the Walls," in *IEEE Transactions on Mobile Computing*, vol. 20, no. 6, pp. 2186-2199, 1 June 2021.

[11] M. Di Seglio, F. Filippini, C. Bongioanni, and F. Colone, " Reference-free WiFi PHY Preamble based Passive Radar for Human Sensing", *2022 International Radar Conference*.

[12] M. Cherniakov, " Basic principles of forward-scattering radars, " in Bistatic Radar: Principles and Practice: Part III. New York, NY, USA: Wiley, 2007.

[13] M. Gashinova, L. Daniel, A. Myakinkov, and M. Cherniakov, " Forward scatter radar" , in Novel Radar Techniques and Applications Volume 1: Real Aperture Array Radar, Imaging Radar, and Passive and Multistatic Radar. Raleigh, NC, USA: SciTech, 2017, ch. 13, pp. 563–619.

[14] F. Colone, "DVB-T-Based Passive Forward Scatter Radar: Inherent Limitations and Enabling Solutions," in *IEEE Trans. on Aerospace and Electronic Systems*, vol. 57, no. 2, pp. 1084-1104, April 2021.

[15] F. Colone, *et al.*, "Reference-free Non-Coherent WiFi Passive Sensing," *IEEE Transactions on Aerospace and Electronic Systems, Under Review.*