Reference-free Amplitude-based WiFi Passive Sensing

FABIOLA COLONE
FRANCESCA FILIPPINI
MARCO DI SEGLIO
Sapienza University of Rome, Italy

PAUL V. BRENNAN
University College London, UK

RUI DU
TONY XIAO HAN
Huawei Technologies Co., Ltd, China

***Abstract* — The parasitic exploitation of WiFi signals for passive sensing purposes is a topic that is attracting considerable interest in the scientific community. In an attempt at meeting the requirements for sensor compactness, easy deployment, and low cost, we resort to a non-coherent signal processing scheme that does not rely on the availability of a reference signal and relaxes the constraints on the sensor hardware implementation. Specifically, with the proposed strategy, the presence of a moving target echo is determined by detecting the amplitude modulation that it produces on the direct signal transmitted from the WiFi access point. We investigate the target discrimination capability of the resulting sensor against the competing interference background and we theoretically characterize the impact of undesired amplitude fluctuations in the received signal that are determined by causes other than the superposition of the target echo, thereby including the waveform properties. Hence, we propose different solutions to address the limitations identified, characterized by different complexities, and we investigate their advantages and drawbacks. The conceived signal processing schemes are thoroughly validated on both simulated and experimental data, collected in different operational scenarios.**

Manuscript received XXXXX 00, 0000; revised XXXXX 00, 0000; accepted XXXXX 00, 0000.

This work was partially supported by the Italian Ministero dell'Università e della Ricerca in the framework of PNRR Partenariati Estesi - Progetto PE14 "RESTART - RESearch and innovation on future Telecommunications systems and networks, to make Italy more smART", CUP B53C22004050001 - D.D. n.1549 del 11/10/2022.

F. Colone, F. Filippini and M. Di Seglio are with the Department of Information Engineering, Electronics and Telecommunications (DIET), Sapienza University of Rome, 00184, Rome, Italy. e-mail: {fabiola.colone, francesca.filippini, marco.diseglio}@uniroma1.it.

P. V. Brennan is with the Department of Electronic and Electrical Engineering, University College London, London WC1E 7JE, U.K. e-mail: p.brennan@ucl.ac.uk.

Rui Du and Tony Xiao Han are with Wireless Technology Lab, Huawei Technologies Co., Ltd. 518129, Shenzhen, P.R. China. e-mail: {ray.du, tony.hanxiao}@huawei.com.

(Corresponding author: *F. Filippini*)

I. INTRODUCTION

In recent years, the steady proliferation of wireless devices has ensured that access points (APs) based on WiFi standards are now available in almost all private and public environments. This has motivated the development of strategies and solutions that enable the parasitic exploitation of these signals for short-range sensing purposes, in both indoor and outdoor areas, see e.g. [1]-[14] and the references therein. The implementation of radio-frequency (RF) based sensing solutions for 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 provides additional benefits in terms of energy consumption and potential interference with pre-existing RF systems operating in the same area. For all these advantages, 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) [1]-[7], to the e-healthcare applications such as human gait recognition or breath detection [8]-[12].

However, most of the techniques proposed in the technical literature set strict requirements on the implementation of the WiFi sensor. As an example, approaches that rely on channel state information (CSI) extraction [4],[8]-[12] require a perfect knowledge of the adopted WiFi Standards and are limited to operation with orthogonal frequency division multiplexing (OFDM) signals. Moreover, they require accurate synchronization in both time, frequency, and phase. On the other hand, WiFi sensors based on passive radar (PR) approaches [1]-[3],[5]-[7],[14]-[15] can, in principle, be 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 former issue has been addressed in recent works [15]-[17] that have focused on the simplification of the PR processing chain with the purpose of streamlining the processing architecture and reducing the computational load. Still, the sensor requires a good copy of the transmitted signal to be available at the receiver since it not only provides a reference in the processing chain (e.g., for matched filtering) but also it inherently offers the required synchronization in time, frequency and phase. The requirement for a good reference signal can be accomplished according to different strategies:

(i) if the AP is accessible, the reference signal can be directly extracted by means of a wired link. This makes available a very good copy of the transmitted signal but requires a dedicated receiving channel and additional infrastructure.
(ii) The reference signal can be obtained using a dedicated antenna steered towards the AP. This strategy also requires a dedicated receiving channel but exploits a wireless link between the AP and the receiver. That simplifies the implementation but the collected signal could be affected by multipath.
(iii) The reference signal can be obtained by demodulating and re-modulating the received signal packet. This strategy requires only one receiving channel but it needs knowledge of the employed IEEE 802.11 Standard, it requires additional processing efforts, and it might be subject to reconstruction errors.
(iv) An alternative approach is to limit the signal processing to *a priori* known portions of the physical layer protocol data unit (PPDU), e.g., the PHY Preamble, without requiring any dedicated receiving channel or reconstruction. However, using limited portions of the available signals implies SNR loss. Moreover, using a synthetic reference signal does not guarantee synchronization in time, frequency and phase with the main echo signal and ad hoc approaches must be implemented to restore the coherency [18].

The aforementioned solutions do not take into account key aspects required to facilitate the widespread use of WiFi-based sensors, such as low cost and low computational complexity, compactness and lightness, as well as the easy deployment and setup.

In this paper, we take this perspective with the aim of enabling a WiFi sensing application that employs a simple, stand-alone and low-cost sensor that could be implemented with commercial off-the-shelf (COTS) hardware components and uses a WiFi passive sensing strategy whose aim is to detect targets without any attempt at isolating or regenerating the reference signal. In order to meet these requirements, we aim to detect the presence of a moving target in the scene by observing the amplitude modulation that it induces on the main source signal. This principle of operation exploits the interference amplitude pattern between the signal transmitted by the AP and multiple reflections from the environment. The analysis of the target induced amplitude modulation not only provides information about its presence but also allows extraction of its Doppler signature across time. Therefore, in the following, we will refer to this approach as interference Doppler processing (IDP). Compared to the passive radar approach, this can be inherently considered as a reference-free approach since it does not require knowledge of the signal transmitted by the AP.

Amplitude-based approaches have been widely investigated in the technical literature. For instance, a similar concept is employed for non-coherent radar but it has also been applied to forward scatter radar (FSR) [19]-[29]. Moreover, typical amplitude-based strategies used in WiFi Sensing are based on the Received Signa Strength Indication (RSSI) extraction [30]-[31]. Thus, it should be noted that although this work may have commonalities with several approaches considered in the general field of sensing, it represents an advancement with respect to each of these. The specific innovative aspects are better clarified in the following.

The purpose of this work is twofold. First, we aim to adopt the considered principle of operation and investigate the proposed strategy for the application in hand. This latter point also includes identification and theoretical characterization of the main limitations of this approach inherently caused by the characteristics of the WiFi signals. It is well known, in fact, that the more the direct signal is constant over time, the higher is the ability of the proposed strategy to discriminate the presence of a target against a competing background based on the amplitude modulation only. This problem has been studied in [29] with reference to a DVB-T based passive FSR application, therefore we follow a similar procedure as the one used therein, however we extend the discussion in order to include real world aspects that are specific to the application in hand, thereby including the peculiar characteristics of the adopted waveforms of opportunity. This provides a broader discussion and a result that allows accurate prediction of the achievable performance for the proposed WiFi sensor.

On the other hand, we propose possible solutions to the main identified limitations and, for each, we investigate advantages and drawbacks both in terms of performance and in terms of complexity. All strategies are tested and thoroughly validated on both simulated and experimental data. To this purpose, *ad hoc* acquisition campaigns have

been conducted by means of an experimental WiFi receiver developed at Sapienza University of Rome using different cooperative targets in order to mimic different application scenarios.

The reminder of the paper is structured as follows. Section II introduces the signal model and the proposed IDP scheme. In Section III, we theoretically characterize the interference background level against which the target discrimination competes and we confirm the validity of the theoretical findings by application to both simulated and real-world WiFi data. In Section IV, we propose different solutions to the problems identified, being the discussion supported by simulated analyses, while Section V is devoted to a thorough experimental validation in real scenarios. Finally, Section VI reports our concluding remarks while mathematical details are reported in the Appendix.

II. INTERFERENCE DOPPLER PROCESSING FOR WIFI SENSING

A. Signal Model

The considered scenario is depicted in Figure 1. During a given observation time, the transmitter (Tx), a WiFi AP, emits a train of consecutive packets. Let $T_s^{(p)}$ be the temporal duration of the pth packet, which is assumed to encompass an integer number of symbols, namely fundamental blocks of the signal, which depend on the adopted modulation. Specifically, the pth packet is composed by $N_s N_{sym}^{(p)} = T_s^{(p)} f_s$ samples, being f_s the employed sampling frequency, $N_{sym}^{(p)}$ the number of symbols inside the pth packet and N_s the number of samples inside each symbol. The signal received by the WiFi sensor (Rx) in Figure 1 contains the coherent superposition of different contributions, namely the direct signal transmitted by the AP and its N_R multipath replicas caused by the reflections on stationary obstacles (e.g., walls, floor, and ceiling), the delayed and Doppler shifted echoes from N_T moving targets, as well as thermal noise.

The discrete version of the complex baseband signal received for the pth WiFi packet emitted by the AP, is then written as

$$x_p(l) = \sum_{r=0}^{N_R} \alpha_{r,p}\, s_p^{(\bar{\tau}_r)}(l) + \sum_{q=1}^{N_T} \beta_{q,p}\; s_p^{(\tau_{q,p})}(l)\, e^{j\varphi_{q,p}(l)} + d_p(l) \qquad (1)$$
$$l = 0, \dots, N_{sym}^{(p)} N_s - 1\ ;\ p = 0, 1, \dots$$

where

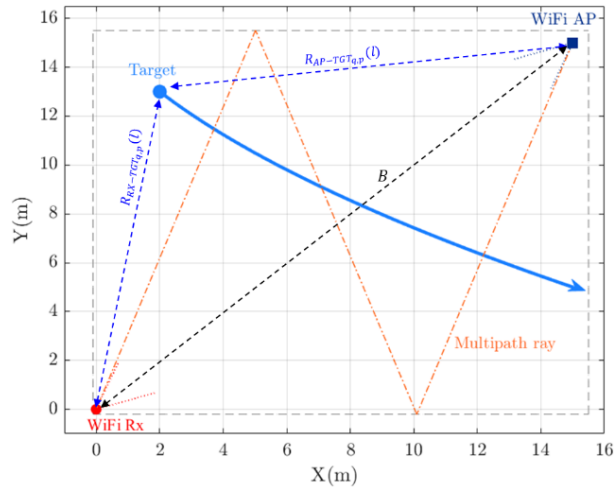


Figure 1. Sketch of the WiFi sensing scenario.

- $s_p^{(\tau)}(l)$ is the resampled version of the waveform transmitted at the pth packet, i.e., $s_p(l)$, delayed by τ. Note that the adopted notation also accounts for fractional delays. In this paper, the pth packet waveform is modeled as a zero-mean unitary power random process whose characteristics depend on the modulation scheme.
- $\alpha_{r,p}$ are the complex amplitudes of the stationary contributions at the pth packet; specifically, $\alpha_{0,p}$ is the amplitude of the direct signal, while $\alpha_{r,p}$ $(r = 1, \dots, N_R)$ is the amplitude of the rth multipath reflection. These parameters encode both the Tx power level and the propagation losses and they are assumed to be constant within the packet whereas they might vary across consecutive packets.
- $\bar{\tau}_r$ is the delay of the rth stationary contribution; in the following, without loss of generality, we assume that the delay of the direct signal is zero, i.e., $\bar{\tau}_0 = 0$, and we measure the delays of all the other contributions with respect to it;
- $\beta_{q,p}$ 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 and, despite target movements, their variation is assumed to be negligible within the packet due to the typical duration of WiFi packets compared with the velocity of the targets of interest;
- $\varphi_{q,p}(l)$ encodes the motion induced phase variation for the qth target echo at the pth packet, and it is defined as $\varphi_{q,p}(l) = 2\pi \frac{R_{q,p}(l)}{\lambda}$, where λ is the wavelength and $R_{q,p}(l) = R_{Tx-TGT_{q,p}}(l) + R_{Rx-TGT_{q,p}}(l) - B$ is 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 additive noise affecting the pth packet at the receiving sensor. It is assumed to be a white, zero-mean complex Gaussian process with variance σ_D^2, statistically independent of the source signal.

With a passive radar approach, the presence of a moving target is detected by first removing the stationary contributions in (1) and then focusing the energy of the target echo by means of a matched filter or alternative techniques [1][15]. This approach requires the availability of a reference signal, namely a good copy of the transmitted signal, which also provides inherent time, phase and frequency synchronization [18]. However, as previously discussed, such approach sets strong requirements on the Rx architecture, above all the need for at least two simultaneous and coherent receiving channels, thus increasing its cost [18].

Aiming at reducing the complexity of the WiFi sensor, we propose to adopt a reference-free approach. For this purpose, a possible strategy is to exploit an amplitude-based processing scheme where the presence of a moving target echo is detected by extracting the amplitude modulation that it produces on the direct signal from the AP.

B. Interference Doppler Processing (IDP) Scheme

Figure 2 sketches the main blocks of the processing scheme proposed for a WiFi sensor to detect the presence of moving target(s) against the stationary scene and to extract its instantaneous Doppler frequency, which is referred to as interference Doppler processing (IDP). It mirrors the approach adopted in FSR but it also includes appropriate modifications to make it effective against WiFi signals.

First, the square modulus of the signal is extracted, thus discarding the phase information:

$$y_p(l) = \left|x_p(l)\right|^2 \qquad (2)$$

Afterwards, based on the assumption that the amplitude modulation produced by the target is much slower that the signal Nyquist sampling rate, the output of Figure 2 undergoes a low-pass filter (LPF) and downsampling (DWS) stage aimed at removing the high frequency amplitude variations due to the signal itself, to its multipath replicas and to the noise. We recall that we are dealing with a pulsed type transmission where the packet emission rate is still higher than Doppler frequency components of the targets of interest. Therefore, a very simple solution to implement this block with WiFi signals is to resort to an

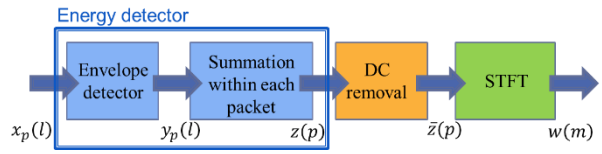


Figure 2. Block diagram of the IDP processing scheme.

energy detector at packet level, namely an integrator, thus setting the cutoff frequency of the LPF equal to the inverse of the packet duration and the output sampling rate equal to the packet emission rate:

$$z(p) = \sum_{l=0}^{N_{sym}^{(p)} N_s - 1} y_p(l) \qquad (3)$$

Once this stage has been performed, the sequence of samples $z(p)$, $p = 0, \dots, N_P - 1$, undergoes DC removal, aimed at cancelling the strongest stationary scene components, above all the direct signal from the AP:

$$\bar{z}(p) = z(p) - z_{DC}(p) \qquad (4)$$

where $z_{DC}(p)$ represents the average value of $z(p)$, evaluated over an appropriate time window T_{DC} around the current sample.

Finally, $\bar{z}(p)$ undergoes a time-frequency analysis that provides as output the typical spectrogram where the presence of a target is detected via its Doppler signature. Specifically, if the packet emission rate is constant over time, i.e., if $T_0^{(p+1)} - T_0^{(p)} = \Delta T_0 \quad \forall p$, $T_0^{(p)}$ being the time instant where the pth packet starts, a short-time Fourier transform (STFT) is implemented that operates against partially overlapped batches of T_{STFT} seconds each, thus encompassing $N_P = \lfloor T_{STFT}/\Delta T_0 \rfloor$ samples:

$$w(m) = \sum_{p=0}^{N_P-1} h(p)\bar{z}(p_0 + p)e^{-j2\pi\frac{mp}{N_P}} \qquad (5)$$

where p_0 is the first packet of the considered batch and $h(p)$ is an appropriate weighting function, used to keep the Doppler sidelobes level under control.

Note that, in practical situations, the sequence $\bar{z}(p)$ collects samples that are not taken at equally spaced time instants, being the sampling rate set by the random packet emission rate. In such case, a possibility is to resort to an appropriate interpolation stage, which basically yields a resampled version of the sequence $\bar{z}(p)$. Provided that the original average packet transmission rate was high enough,

this approach still allows advantage to be taken of the fast Fourier transform (FFT) speed to evaluate the required output. Alternatively, a nonuniform discrete Fourier transform (NDFT) can be implemented at each batch.

C. Example of IDP Results on Simulated Data

To preliminarily investigate the effectiveness of the IDP for WiFi sensing, a simulated dataset has been generated for the scenario depicted in Figure 1. Specifically, a WiFi AP and the WiFi Rx are placed at two opposite corners of the simulated scene while one target crosses the baseline according to a non-rectilinear trajectory. A stream of OFDM modulated WiFi packets is simulated at the Rx containing the direct signal contribution, the signal backscattered by the moving target, as well as thermal noise. Note that, for all simulations reported in this article, the target is modeled as a point-like scatterer. To make the simulation more adherent to reality, more complex target models could be considered. However, this is out of the scope of this work because (i) depending on the target type and observation geometry, the employed model could significantly change (ii) the theoretical derivation and discussion would be considerably complicated but without changing the message of the paper since the main focus of this work is on the impact of the WiFi waveform. Nevertheless, the experimental results reported in Section V will highlight some aspects due to the true target response under different observation geometries.

Table 1
Employed Simulation Parameters

Parameter	Value
Carrier frequency (f_0)	2.4 GHz
Wavelength (λ)	0.1249 m
Sampling frequency (f_s)	20 MHz
Packet repetition interval (PRI)	2 ms
Modulation scheme	OFDM
Constellation	64-QAM
OFDM useful symbol duration	3.2 μs
OFDM Cyclical Prefix (CP) duration	0.8 μs
Number of OFDM symbols per packet	20
Packet duration	80 μs
Considered scenario	Single target, no multipath
Target initial position (x_0,y_0,z_0)	(2,13,1) m
Target initial velocity (v_x,v_y,v_z)	(0.8, -0.8,0) m/s
Target constant acceleration (a_x,a_y,a_z)	(0.1, 0, 0) m/s^2
Target signal-to-noise ratio (SNR)	-15 dB
Direct signal-to-noise ratio (DNR)	25 dB

For the purpose of the following analysis, multipath reflection contributions are assumed negligible.

Table 1 collects the set of parameters employed in the simulation. For simplicity, the direct signal-to-noise ratio, $DNR_p = \sigma_D^{-2}\left|\alpha_{0,p}\right|^2$, and the target signal-to-noise ratio, $SNR_p = \sigma_D^{-2}\left|\beta_{0,p}\right|^2$, are assumed constant across packets during the entire acquisition time of approximately 10 seconds, i.e., $DNR_p = DNR = 25\,dB$ and $SNR_p = SNR = -15\,dB$, $p = 0, \dots, N_P - 1$; moreover, the OFDM packets are all of the same duration of 80 μs. Note that the SNR values provided are defined over a frequency band used for the considered WiFi transmission Standard, in this case corresponding to 20 MHz.

Figure 3 shows the result obtained with the IDP in the bistatic velocity-time plane. The processing scheme detailed in Section II.B has been applied with $T_{DC} = T_{STFT} = 1$ s and a Hamming weighting function $h(p)$ to control Doppler sidelobes. The spectrogram is reported for positive frequency values only (the results are symmetrical about zero since the input signal is a real-valued signal) and is scaled to a reference noise power level ϱ_D as expected at the output of the processing scheme [28]. Figure 3 demonstrates that, by applying the IDP strategy, the WiFi sensor can distinguish the presence of a moving target from the competing background and correctly measure the absolute value of the target Doppler frequency, or equivalently of the target bistatic velocity, i.e., $|v_B|$, across time.

Nevertheless, it is also worth noting that the background level against which the target must compete is quite high. In the considered case study, it appears at approximately 48.8 dB above the reference noise level, which is expected to yield significant masking effects on weak target signatures. A similar problem was addressed in [28] with reference to broadcast radio and television transmissions, where it was shown that this level strongly depends on the modulation adopted by the signal that is being exploited as well as on the DNR.

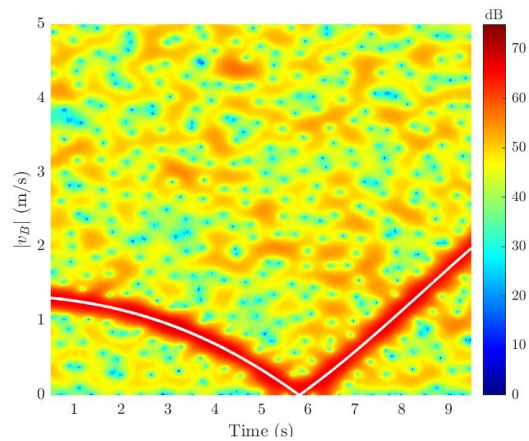


Figure 3. Results of the IDP on simulated data. The white line represents the true target trajectory mapped onto the absolute velocity - time plane.

In the following section we extend the analysis in [28] so that it can also be representative for WiFi signals. Moreover, we generalize the adopted hypotheses to include real-world effects that were not considered in the theoretical development in [28] and are shown to further degrade the performance. The theoretical characterization of the background level represents a key step in the identification of appropriate strategies to mitigate this issue in order to improve the performance of the proposed IDP in WiFi sensing applications. The points above will be addressed in Sections III and IV, respectively.

III. BACKGROUND CHARACTERIZATION

The background level at the output of the IDP chain is evaluated by computing the average power level of the spectrogram under the null hypothesis H_0 (absence of targets), i.e., $E\{|w(m)|^2|H_0\}$, where $E\{\cdot\}$ denotes the expectation operator. As shown in [29], it is expected that the background level increases in the presence of random amplitude fluctuations in the received signal that are determined by causes other than the superposition of the target echo. Therefore, all possible sources of amplitude fluctuation should be properly modeled and included in the analysis. To this purpose we consider the signal at the *p*th packet, as written in (1), under the H_0 hypothesis and assuming that the multipath contributions are negligible with respect to the direct signal:

$$x_p(l) = \alpha_{0,p}\, s_p(l) + d_p(l)$$
$$l = 0, \dots, N_s N_{sym}^{(p)} - 1\ ;\ p = 0, 1, \dots \tag{6}$$

We make very general assumptions for the quantities in (6) in order to model real-world effects that are expected to limit the achievable performance. Specifically:

- The direct signal amplitude $\alpha_{0,p}$ associated with the *p*th packet is modelled as a random variable to encode the unpredictable variations in the Tx power level and propagation loss across packets. Such effect is expected to limit the performance of the IDP since this technique relies on the assumption that the direct signal constituites a stable power reference source. In constrast, if the direct signal power level varies across packets, the observed amplitude modulation cannot be solely attributed to the presence of a target that becomes more difficult to be detected. Specifically, we assume $\alpha_{0,p}$ to be zero-mean with variance $m_{\alpha,2} = E_\alpha\left\{\left|\alpha_{0,p}\right|^2\right\} = DNR_{avg}\,\sigma_D^2$, where we have implicitly defined an average DNR across the processing time. Moreover, we define the parameter $\sigma_{DNR}^2 = \frac{m_{\alpha,4} - m_{\alpha,2}}{\sigma_D^4}$, that encodes the DNR variance across packets and depends on the fourth moment of $\alpha_{0,p}$, $m_{\alpha,4} = E_\alpha\left\{\left|\alpha_{0,p}\right|^4\right\}$.
- The number $N_{sym}^{(p)}$ of symbols inside the *p*th packet is modelled as a random variable to encode the variable length of WiFi packets with first and second moments respectively given by $m_{N,1} = E_N\left\{N_{sym}^{(p)}\right\}$ and $m_{N,2} = E_N\left\{\left(N_{sym}^{(p)}\right)^2\right\}$. As for the direct signal amplitude, this parameter affects the energy detection stage at packet level and determines an unwanted amplitude modulation in the output sequence $z(p)$ that might be responsible of a masking effect on the target echo.
- The waveform $s_p(l)$ transmitted at the *p*th packet might show an inherent amplitude fluctuation depending on the the adopted modulation. In order to model the statistics of the corresponding process, we refer to the two most common modulation schemes used in WiFi Standards [32].

– For DSSS modulated packets, we write the waveform as

$$s_p(l) = s_p(qN_s + n) = c^{(p,q)} b(n)$$
$$q = 0, \dots, N_{sym}^{(p)} - 1,\ n = 0, \dots, N_s - 1 \tag{7}$$

where index $q = \lfloor l/N_s \rfloor$ scans the symbols, while index $n = l - qN_s$ scans the samples within the symbol. In this case, the fundamental block in the waveform is given by the pseudo-noise Barker code $b(n)$ of length $N_s = 11$, used to chip the baseband signal at 11 MHz. $c^{(p,q)}$ is the complex data transmitted at the *q*th symbol of the *p*th packet and is drawn from either a BPSK or a QPSK constellation (M_c-PSK with $M_c = 2,4$) with equiprobable symbols. It is worth noticing that, whilst the complex data stream can randomly take different values within the constellation, the waveform in (7) shows a contant modulus so that it does not contribute to undesired amplitude fluctuations on the received signal and it is expected to be the best performing in terms of background level.

– For OFDM modulated packets

$$s_p(l) = s_p\left(qN_s + n + N_{cp}\right) = \sum_{k=0}^{N_c-1} c_k^{(p,q)}\, e^{j\frac{2\pi}{N_c}kn}$$
$$q = 0, \dots, N_{sym}^{(p)} - 1,\ n = -N_{cp}, \dots, N_c - 1 \tag{8}$$

where $q = \lfloor l/N_s \rfloor$ scans the symbols and $n = l - qN_s - N_{cp}$ scans the samples within the symbol. In this case, the number of samples within the OFDM symbol is equal to

$N_s = N_c(1+\eta)$, where N_c is the number of subcarriers and $\eta = N_{cp}/N_c$ is the fraction of useful symbol samples that is cyclically repeated at the beginning of each symbol, namely the cyclical prefix (CP). Note that, according to the 802.11 WiFi Standard [32], $N_c = 64$ while η may take values equal to $1/4$, $1/8$ or $1/16$. Different sub-carriers are assumed to be modulated by statistically independent streams of equiprobable symbols drawn from a constellation of dimension M_c. Specifically, $c_k^{(p,q)}$ is the constellation symbol transmitted at the *q*th symbol of the *p*th packet using the *k*th subcarrier. We recall that, according to the 802.11 Standard, the available constellations are BPSK ($M_c = 2$), QPSK ($M_c = 4$), 16-QAM ($M_c = 16$) , 64-QAM ($M_c = 64$).

In both DSSS and OFDM cases, the constellation symbols $\{\gamma_m\}_{m=0,..,M_c-1}$ of the adopted constellation map are properly defined in order to guarantee the unitary power characteristic for the resulting waveform $s_p(l)$. Specifically, in the DSSS case, such condition yields $C = \frac{1}{M_c}\sum_{m=0}^{M_c-1}|\gamma_m|^2 = 1$, which in turn requires $|\gamma_m| = 1, m = 0,..,M_c-1$, with the adopted BPSK or QPSK schemes. When OFDM signals are considered, we set the average power of the constellation as $C = \frac{1}{M_c}\sum_{m=0}^{M_c-1}|\gamma_m|^2 = 1/N_c$. In addition, we define

$$\mu = \frac{1}{M_c C^2}\sum_{m=0}^{M_c-1}|\gamma_m|^4 \tag{9}$$

as the scaled fourth moment of the adopted constellation, which yields the values reported in Table 2. With the assumptions above, the theoretical background level at the output of the IDP chain is given by the following unified expression (see Appendix for detailed derivation):

$$\begin{aligned} &E\{|w(m)|^2|H_0\} = \varrho_D \times \{2DNR_{avg} + 1 + \\ &DNR_{avg}^2[\mu - 1 + g(\eta)] + \\ &\frac{\sigma_N^2}{m_{N,1}} N_s\left[\sigma_{DNR}^2 + \left(DNR_{avg}+1\right)^2\right] + \\ &\sigma_{DNR}^2\left[m_{N,1}N_s + \mu - 1 + g(\eta)\right]\} \end{aligned} \tag{10}$$

where ϱ_D denotes the output power level that is solely due to the noise at the Rx, namely the value that would be measured in the absence of direct signal, i.e., $\varrho_D = \sigma_D^4 m_{N,1} N_s \sum_{p=0}^{N_P-1} h^2(p)$. As a consequence, the remaining factor represents the background-to-noise ratio, namely $BNR = E\{|w(m)|^2|H_0\}/\varrho_D$.

The function $g(\eta)$ in eq. (10) depends on the adopted constellation via the parameter μ but it takes non-zero (positive) values only in the presence of a CP, i.e., for $\eta > 0$, thus reflecting the background increment expected due to the cyclical repetition of signal fragments within the waveform. Its expression is reported in Table 2 for the considered waveforms of interest.

Eq. (10) generalizes the result in [29] by introducing additional effects that were not considered before and provides an appropriate tool that can be exploited also for the case of pulsed transmissions as WiFi signals.

Table 2
Expressions for μ and $g(\eta)$.

Modulation		μ	$g(\eta)$
DSSS		1	0
OFDM	BPSK ($M_C = 2$)	1	$\eta\left(\mu - 3 + \frac{3}{(\eta+1)}\right)$
	QPSK ($M_C = 4$)	1	$\eta\left(\mu - 2 + \frac{2}{(\eta+1)}\right)$
	16-QAM ($M_C = 16$)	1.320	$\eta\left(\mu - 2 + \frac{2}{(\eta+1)}\right)$
	64-QAM ($M_C = 64$)	1.381	$\eta\left(\mu - 2 + \frac{2}{(\eta+1)}\right)$

In particular, it shows that the BNR at the output of the IDP scheme takes a minimum value equal to approximately $2DNR_{avg}$ but it might experience a large increase depending on (i) the transmitted waveform and employed modulation, via μ and $g(\eta)$, since these determine the inherent amplitude fluctuation in the waveform; (ii) the fluctuation of the packets length and specifically of the number of symbols included in the employed packets, described by $\sigma_N^2/\, m_{N,1} = \left(m_{N,2} - m_{N,1}^2\right)/\, m_{N,1}$; (iii) the fluctuation of the direct signal power level, described by σ_{DNR}^2. This theoretical expression is validated against experimental data in Section V. In the remainder of this Section a thorough analysis is reported against simulated data. This allows us to better understand the effects of different parameters that can be individually simulated. To this purpose, we consider three case studies, separately addressed in the following.

1) Case study A

In Case Study A, we investigate the effect of packet length fluctuation within the processing interval while removing the signal amplitude fluctuations due to other effects. Therefore, we assume that the DNR is constant across packets, i.e., $\sigma_{DNR}^2 = 0$ (and $DNR_p = DNR_{avg} = DNR$), and we set $\mu = 1$ and $g(\eta) = 0$, which correspond

to a constant amplitude waveform, e.g., DSSS modulated WiFi packets. Accordingly, eq. (10) becomes

$$E\{|w(m)|^2|H_0\} = \varrho_d \times \left\{2DNR + 1 + \frac{\sigma_N^2}{m_{N,1}} N_s (DNR+1)^2\right\} \quad (11)$$

To validate this expression, we simulate streams of DSSS packets with variable lengths. To this aim, the number of symbols inside each packet is drawn from a discrete uniform distribution with mean value $m_{N,1}$and variance σ_N^2. Different values of these two parameters are used in order to obtain different values for the ratio $\sigma_N^2/m_{N,1}$ in (11). The received signal is simulated according to (6) for a target-free and multipath-free scenario. Then, it is sent in input to the IDP scheme and the BNR is numerically evaluated from the output Doppler-time map. In Figure 4, we report the results as a function of the DNR. Different line styles and colors represent the theoretical results for different values of $\sigma_N^2/m_{N,1}$, while different colored markers represent the BNR measured on simulated data. As is apparent, the simulation results confirm the correctness of the theoretical formula in (11).

When $\sigma_N^2 = 0$, the last term in (11) is null therefore the BNR is at its lowest value equal to

$$BNR_{min} = 2DNR + 1 \cong 2DNR \quad (12)$$

As $\sigma_N^2/m_{N,1}$ grows, the last term in (11) becomes progressively larger. In other words, the higher is the amplitude fluctuation due to the varying packet length, the lower is the system capability of discriminating a target from the competing background.

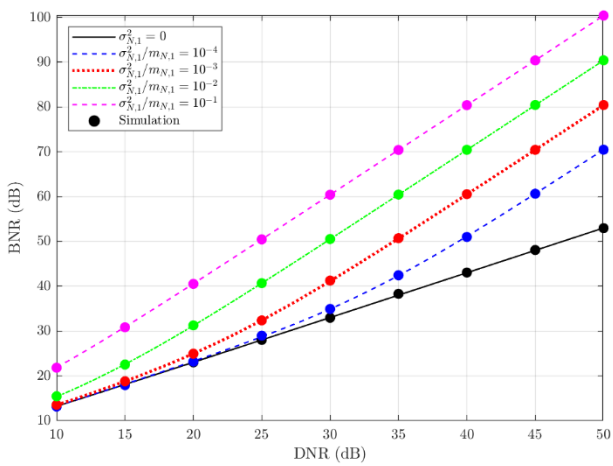


Figure 4. BNR versus DNR for different $\sigma_N^2/m_{N,1}$ values.

In particular, the BNR deviates from the $2DNR$ level even for very small $\sigma_N^2/m_{N,1}$ values. As an example, with the considered discrete uniform distribution for $N_{sym}^{(p)}$, the case $\sigma_N^2/m_{N,1} = 10^{-4}$ (blue line) is representative of a fluctuation of less than $[\pm 1]$ symbol around an average value of $m_{N,1} = 6000$ symbols. Finally, we notice that, for $\sigma_N^2/m_{N,1} \geq 10^{-2}$, the BNR grows proportional to the square of the DNR since the last term in (11) becomes the dominant term in the range of typical DNR values considered. The analysis above reveals that the BNR is very sensitive to packet length fluctuation. However, an easy approach to solve this issue is to crop all packets to a common length. This obviously implies some losses in terms of target SNR since part of the available energy on receive is discarded. However, target detection is expected to largely benefit from the resulting control of the BNR which typically represents the limiting factor. Actually, the capability of detecting moving targets is jointly limited by the background level and the noise contribution via the signal-to-background-plus-noise ratio SBNR=S/(B+N). However, in the considered application we have shown that the background level is typically much higher than the noise floor, especially when amplitude modulated signals are used. By rewriting the SBNR as SBNR= (S/N)/(B/N+1) = SNR/(BNR+1), it is well apparent that the BNR term represents the degrading factor with respect to the original SNR when BNR>>1, therefore, if a sufficient SNR is available, the capability of mitigating the BNR might be critical for target detection.

Therefore, in the following, we will assume that $N_{sym}^{(p)} = N_{sym}, p = 0, \ldots, N_P - 1$.

2) Case study B

In Case Study B, we investigate the effect of the direct signal amplitude fluctuation on the output background by keeping constant the packets duration, i.e., $\sigma_N^2 = 0$, and the waveform amplitude, i.e., using a DSSS packets. With these assumptions, eq. (10) becomes

$$E\{|w(m)|^2|H_0\} = \varrho_d \times \left\{2DNR_{avg} + 1 + \sigma_{DNR}^2 N_{sym} N_s\right\} \quad (13)$$

In Figure 5, we report the BNR versus DNR_{avg} for different values of $\xi = \sigma_{DNR}/DNR_{avg}$ (denoted by different colors) for two different N_{sym} values, represented with different line styles.

From Figure 5, the following comments apply:

- For $\xi = 0$, namely when $DNR_p = DNR_{avg}$, the BNR level is the minimum achievable and equal to $2DNR_{avg}$ regardless of N_{sym}.

- For limited $\xi > 0$, we can identify a DNR_{avg} value from which the BNR curve deviates from the minimum obtainable value and rapidly grows. Moreover, the higher is N_{sym}, the lower is the DNR_{avg} value where the deviation occurs.
- For higher $\xi > 0$, the BNR curve never reaches the lower $2DNR_{avg}$ bound within the ranges of DNR values considered in this analysis. Moreover, for a fixed ξ, the higher is N_{sym}, the higher is the BNR.
- Finally, all simulation results match the corresponding theoretical expressions, meaning that the formula in (13) is able to correctly predict the performance in all cases.

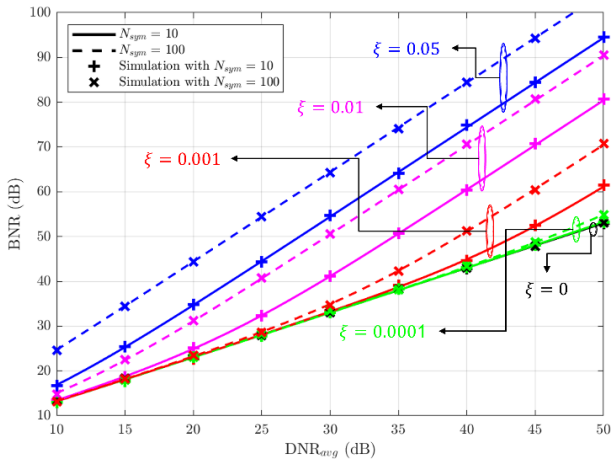


Figure 5. BNR versus DNR for different N_s and ξ values.

3) Case study C

In Case Study C, we assume that both the DNR and the packet lengths are constant across packets, i.e., $\sigma^2_{DNR} = 0$ ($DNR_p = DNR_{avg} = DNR$) and $\sigma^2_N = 0$, and we study the impact of the different WiFi waveforms on the output background. Accordingly, eq. (10) can be written as

$$E\{|w(m)|^2|H_0\} = \varrho_d \times \{2DNR + 1 + DNR^2[\mu - 1 + g(\eta)]\} \quad (14)$$

In Figure 6, we report the theoretical BNR vs DNR curves for different modulation schemes and different constellations, identified by different colors and linestyles. In all cases, the simulated packets are composed of $N_{sym} = 5$ symbols, however as correctly predicted by Eq. (14), under the considered hypotheses, the BNR does not change with the packet duration.

The results in Figure 6 show that:

- the BNR obtained with DSSS packets is equal to 2DNR (solid black curve) since, for a constant amplitude waveform, the second term in (11) is equal to zero.
- With OFDM modulated signals, the BNR is much larger than the one of the black curve.
- When the OFDM packets use a 16-QAM or a 64-QAM constellation (dot-dash blue or dotted magenta curve), the measured BNR is approximately equal to DNR^2 (as observed for the example in Figure 5).
- In contrast, when the employed OFDM constellation is either a BPSK or a QPSK (dashed red or dotted green curves), the obtained background level is up to 10 dB lower than the DNR^2 level. In other words, smaller constellation schemes imply smaller fluctuations in the resulting waveform amplitude that is encoded in a smaller μ value, equal to 1 for both BPSK and QPSK. Actually, from (14) we observe that with such value for μ, the BNR deviates from the lower bound of 2DNR only because of the presence of the CP, whose effect in encoded in $g(\eta)$. In fact, with BPSK and QPSK constellation, the energy associated to the useful portion of any OFDM symbol would be constant regardless of the transmitted data. The fluctuation in the sequence $z(p)$ at the output of the packet energy extractor is only due to the fractions of OFDM symbols cyclically extended to build the CP.

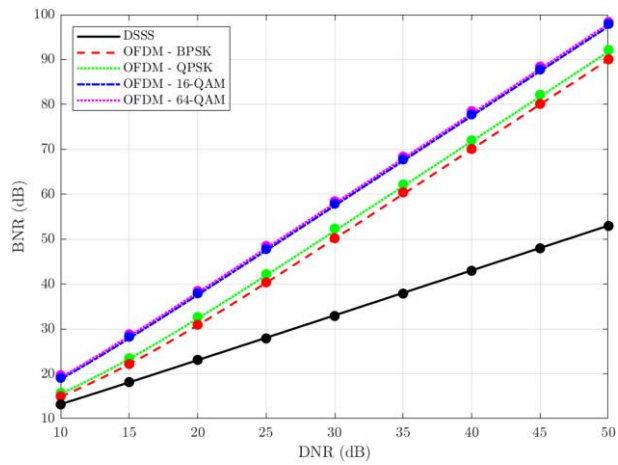


Figure 6. BNR versus DNR with variable waveform.

Based on the theoretical findings and analyses reported in this Section, it is evident that the best performing condition for the IDP scheme is given by a contant amplitude source signal at the input of the STFT stage. We have demonstrated that DSSS modulated packets show favourable conditions, and only yield a BNR increase when the DNR is not strictly constant over time. In contrast, we have shown how the use of OFDM modulated packets could significantly increase the output BNR, potentially preventing small targets from being detected. The following Section presents possible solutions to handle this issue.

IV. BACKGROUND REDUCTION STRATEGIES

Two approaches are proposed in this Section to lower the average background level obtained when exploiting OFDM modulated WiFi transmissions. First, we separately address them in the following subsections; then, we compare them by application against simulated data, under different operative conditions.

A. IDP with Signal - based Background Cancellation

In [29] an effective approach is presented to mitigate the background level when exploiting DVB-T signals as waveforms of opportunity for an amplitude-based sensing system. This approach, named Signal-based Background Cancellation (SBC), exploits the knowledge of the transmitted signal, possibly reconstructed from the received signal itself, to remove its effect on the observed background by direct subtraction from the DC-free amplitude signal. We refer the interested reader to [29] for a comprehensive description.

In Figure 7 the IDP including an SBC stage is sketched and will be referred to as the SBC-IDP in the following. Notice that the SBC in [29] can be easily applied to the WiFi case by assuming that the energy variation across transmitted WiFi packets is known at the receiver, up to a scale factor. This is obtained in Figure 7 by means of a rough reconstruction from the received signal. Under the hypothesis that the main contribution to the background level is the direct signal from the AP, the subtraction of the reconstructed signal prior to the STFT is expected to reduce the background level down to that observed for a constant amplitude waveform.

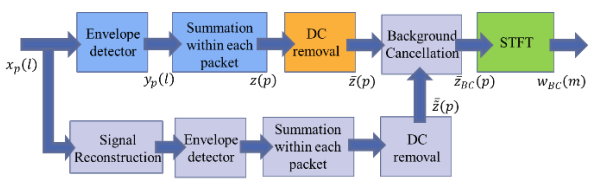


Figure 7. SBC-IDP processing scheme.

This is shown in Figure 8 that reports the result of the SBC-IDP when applied on the same simulated dataset used in Section II.C. Notice that the considered case study includes equal length packets transmitted with a constant Tx power level; therefore, the background level observed in Figure 3 was only due to the waveform properties. By comparing Figure 3 and Figure 8, the advantage of the SBC-IDP solution is evident as the target SNR stays the same while the average background level decreases to approximately 28 dB (i.e., 2·DNR), namely as per a constant-amplitude waveform. The result in Figure 8 demonstrates the effectiveness of the proposed solution to lower the BNR level when OFDM waveforms are exploited.

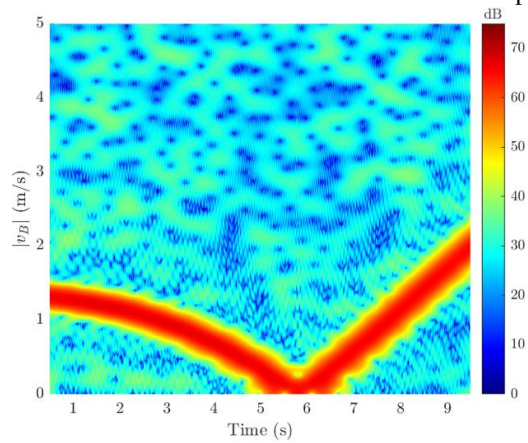


Figure 8. Result of the SBC-IDP.

However, a few additional considerations are in order.

(i) SBC-IDP requires a partial knowledge of the transmitted WiFi signal. Specifically, the waveform energy at packet level should be available or computed from a reasonably good copy of the transmitted waveform, which in turn can be obtained according to the different strategies mentioned in the introduction. Figure 7 shows the case when the signal is reconstructed via demodulation and remodulation [32], thus preserving the "reference-free" characteristic of the proposed scheme.

(ii) Despite the SBC approach requires the reconstruction of the transmitted waveform, we observe that such signal is not used as a reference for time/phase/frequency synchronization since the IDP inherently relies on amplitude information only. Therefore, compared to the case of the reference signal used in passive radar, the implementation of this additional block yields looser requirements on the quality of the regenerated signal.

(iii) In this simulated analysis, we assumed a perfect copy of the transmitted signal to be available. In practical scenarios, reconstruction errors are likely to corrupt the available signal, especially when the DNR degrades or when the target contribution in the received signal becomes larger. Whilst a limited number of errors may be tolerated, the increase in the error rate would obviously prevent the possibility to correctly reconstruct the energy variation of the source signal across packets and in turn to effectively reduce the corresponding background level.

(iv) Despite not considered in the reported simulated results, also slow variations in the Tx power level

could be tracked and mitigated with this approach by properly selecting the parameters of the SBC.

B. WiFi PHY Preamble based IDP

The application in hand also suggests the possibility of an alternative simple solution that maintains the reference-free characteristic of the IDP approach while guaranteeing the desired reduction of the BNR also for amplitude modulated waveforms. Based on the theoretical findings of Section III, in the absence of Tx power level fluctuations, we observe that in order to achieve the 2·DNR lower bound for the BNR, it is sufficient that the energy across packets is kept constant. In turn that can be obtained by selecting and using only time-invariant and data-independent portions of the transmitted packets. This possibility is readily offered by OFDM WiFi packets that, based on the WiFi Standards [32], encompass three main fields (see Figure 9): (i) the PHY Preamble, which is *a priori* defined and is used for synchronization and channel estimation purposes; (ii) the Signal, which is composed by a single OFDM symbol and contains information on the transmission mode for the payload; (iii) the data that encloses the transmitted information and might have a variable number of OFDM symbols. Therefore, we investigate the possibility of limiting the application of the IDP approach to the time-invariant PHY Preamble portion of the packet and refer to this approach as the WiFi PHY Preamble based IDP (WPP-IDP). We observe that, with this position and assuming that the Tx power level variations are negligible, the signal at the output of the energy detector can be written as:

$$z(p) = DNR_{avg}\,\sigma_D^2 \sum_{l=0}^{N_{Preamble}-1} \left| s_p(l) \right|^2 + \sum_{l=0}^{N_{Preamble}-1} \left| d_p(l) \right|^2 + 2\sqrt{DNR_{avg}\,\sigma_D^2} \sum_{l=0}^{N_{Preamble}-1} \Re\left\{ e^{j\arg\{\alpha_{0,p}\}}\; s_p(l) d_p^*(l) \right\} \quad (15)$$

denoting $\Re(\cdot)$ as the real part of $(\cdot)$ and being the first term on the r.h.s. the major contributor to the background level when the DNR is high enough. However, this term is constant across packets since the summation is limited to the invariant preamble fragment, meaning that such term can be effectively cancelled by the DC removal stage of Figure 2 without any additional processing stage.

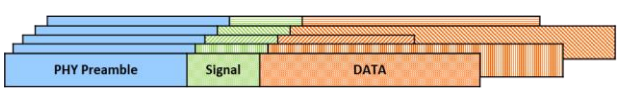


Figure 9. OFDM modulated WiFi packet.

Clearly, we observe that this solution is effective as long as the Tx power level fluctuations are negligible. However, the analysis in Section III.B has shown that such effect becomes apparent only at very high values of the average DNR.

Figure 10 shows the results for the simulated dataset exploited for both Figure 3 and Figure 8, where it is evident that the average BNR level is comparable to that of Figure 8, approximately 28 dB, which corresponds to the 2·DNR lower bound. As expected, the main drawback of this approach is the loss on the target signature obtained by limiting the processing to a small portion of the WiFi packet. Specifically, the maximum peak level in Figure 8 is equal to 67.3 dB while that of Figure 10 is equal to 60.2 dB.

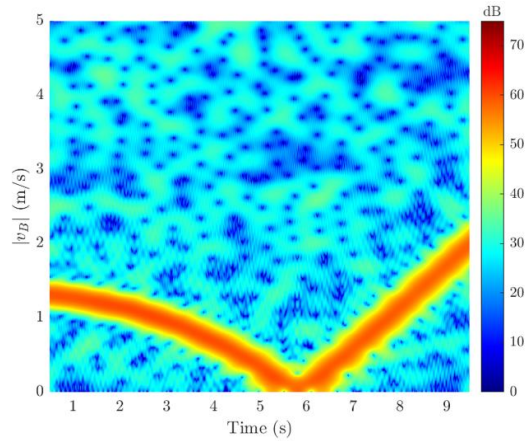


Figure 10. Result of the WPP-IDP.

In fact, as reported in Table 1, the employed simulated dataset is composed of 20 OFDM symbols while the PHY Preamble only includes 4 OFDM symbols, therefore an SNR loss of approximately 7 dB is observed. It is worth mentioning that, when small OFDM constellations are employed, namely BPSK or QPSK, an additional solution is possible to lower the background level. In fact, we have shown in Section III that those constellations have $\mu = 1$ such as the DSSS modulated packets [see eq.(9)]. Therefore, the only factor responsible for a higher BNR level is the presence of the CP, whose effect in encoded in $g(\eta)$ [see Eq.(40) of the Appendix].

This observation suggests that, for packets using these constellations, it is sufficient to remove the CP samples at each OFDM symbol for the background level to reach the lower bound of 2·DNR. Note that this solution would allow keeping a larger packet length with respect to the use of the WPP-IDP, therefore obtaining lower SNR loss at the packet level. However, depending on the employed WiFi Standard, limiting the processing to BPSK or QPSK modulated packets might significantly reduce the packet rate and, in turn, the target integration gain.

C. Comparative analysis against simulated data

Table 3 reports the results obtained with the two described strategies when applied against the same simulated dataset employed in Section III for Figure 6. Specifically, the SBC-IDP and the WPP-IDP approaches are compared in terms of achievable BNR when applied to a stream of OFDM modulated WiFi packets employing a 64-QAM constellation, namely the constellation that yields the highest BNR level with the original IDP. The results in Table 3 confirm the effectiveness of both strategies to achieve the desired lower bound of 2·DNR for the BNR level. A further comparison is reported in Figure 11, where the three different strategies are compared when applied to the simulated scenario described in Table 1 for three different DNR values while keeping the input SNR constant.

Table 3
BNR obtained with IDP, SBC-IDP and WPP-IDP for a stream of OFDM modulated WiFi packets with 64-QAM constellation.

DNR	IDP	SBC-IDP	WPP-IDP
10 dB	19.72 dB	13.25 dB	13.14 dB
20 dB	38.46 dB	22.94 dB	23.02 dB
30 dB	58.43 dB	33.13 dB	32.91 dB
40 dB	77.97 dB	42.98 dB	42.94 dB
50 dB	98.36 dB	53.19 dB	53.01 dB

As evident with the original IDP scheme, the higher the DNR is, the lower is the capability of discriminating the targets against the background despite the target signature amplitude increases. This is due to the larger increase of the BNR that follows a square law as a function of the DNR. In fact, for a DNR of 40 dB, the target signature is buried in the map background and would no longer be detected. By either applying the SBC-IDP or the WPP-IDP, the average background level is correctly lowered. Clearly, as mentioned above, the limited complexity of the WPP-IDP is traded for a higher SNR loss due to the use of a small portion of the available packet. Note that these results have been obtained with a simulated dataset where the multipath contributions are negligible. In practice, especially in indoor scenarios, the signal reflections from the walls, the floor and the ceiling might not be negligible and might jeopardize the WiFi sensing application. To investigate the robustness of these strategies to multipath, let us first consider a scenario where the multipath contribution is limited to a single multipath ray ($N_R = 1$) with the same power level of the direct signal, and delayed by $\bar{\tau}_1$.

Therefore, the received signal in this case is written as:

$$x_p(l) = \alpha_{0,p} s_p(l) + \alpha_{1,p} s_p^{(\bar{\tau}_1)}(l) + d_p(l)$$
$$l = 0, \dots, N_{sym}^{(p)} N_s - 1 \; ; \; p = 0, 1, \dots \qquad (16)$$

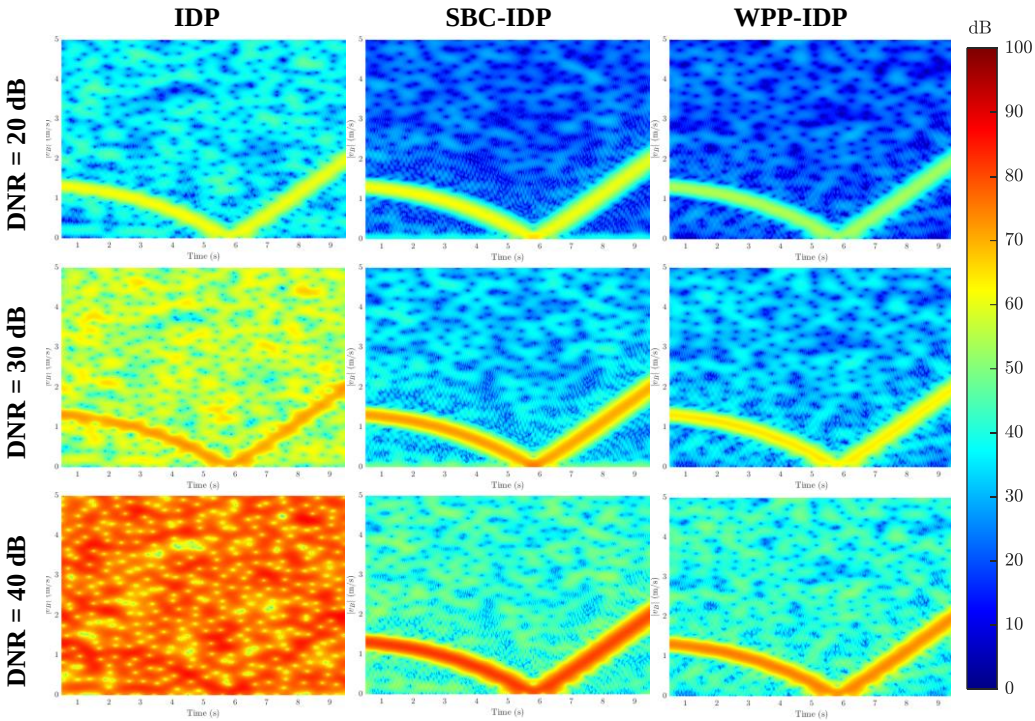
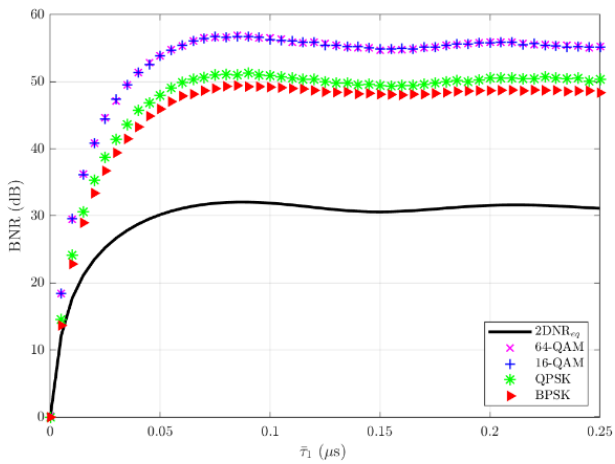


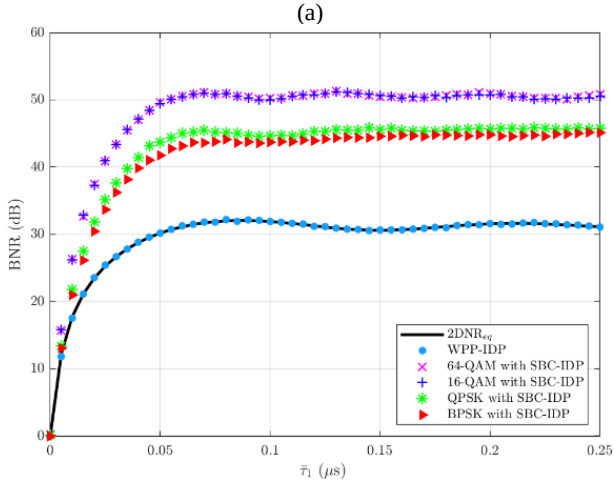
Figure 11. Output of IDP, SBC-IDP and WPP-IPP strategies for different DNR values.

and we assume that $\alpha_{1,p} = |\alpha_{0,p}| e^{j\left[2\pi \frac{\bar{\tau}_1 c}{\lambda} + \pi\right]}$. The amplitudes are set so that each ray taken separately has a power level DNR = 25 dB above noise. The power level of their superposition, namely after coherent summation, appears DNR_{eq} dB above noise and this value depends on the phase of the multipath ray, which in turn depends on the delay $\bar{\tau}_1$.

In Figure 12(a) and (b) we report the measured BNR versus a grid of delay values associated with the multipath ray. More specifically, we compare the result obtained with conventional processing [Figure 12(a)], and the background reduction strategies [Figure 12(b)] namely the SBC-IDP (red, green, blue and magenta markers) and the WPP-IDP (light blue dots). Different colors and markers denote the different OFDM constellations employed for the simulated data generation. Moreover, the black curve represents the lower expected level, corresponding to twice the estimated equivalent DNR_{eq} in input.



(a)



(b)

Figure 12. Measured BNR versus multipath reflection delay $\bar{\tau}_1$ with DNR = 25 dB: (a) IDP (b) SBC-IDP and WPP-IDP.

The following observations are in order:

- For negligible delay values, the multipath reflection represents a destructive interference for the direct signal. This is because the rays are assumed with equal power but with opposite phase.
- When no background reduction strategy is applied, the measured BNR is very high and depends on the employed constellation, as demonstrated above for the multipath-free condition.
- The SBC-IDP reduces the background contribution with respect to the conventional IDP only by few dBs [compare the equally colored markers in Figure 12(a) and (b)]. This is because the energy variation used to perform the SBC is no longer representative of the entire observed fluctuation on the received signal which also depends on the multipath contribution.
- The WPP-IDP approach is able to reach the desired BNR level for all the considered delay values. In fact, although the considered samples are no longer identical to the transmitted signal, namely to the theoretical PHY Preamble described in the Standard, but also contain a delayed copy of it, provided that the stationary scene does not change over time, the energy of the considered portion will still be time invariant.

The above analysis is extended in the following by considering a more realistic scenario where the received signal includes several multipath replicas. The considered geometry is depicted in Figure 13 where the position of the AP and the Rx are indicated together with the $N_R = 20$ multipath rays (in orange) obtained according to a ray tracing approach by including both the single-bounce reflection (dashed lines) and the double-bounce reflections (dash-dot lines) from the walls, the floor, and the ceiling. Three out of the four walls are assumed made of concrete while one is assumed made of glass, and the reflection coefficients are set accordingly [33]. Overall, we assume the multipath contributions to have a multipath-to-noise ratio (MNR) of 20 dB.

Figure 14 shows the outcome of the IDP approach for the described simulated scenario, with or without a background reduction strategy.

Note that, the overall signal has an average signal to noise level of 23.1 dB. The SBC-IDP [Figure 14(b)] decreases the background level with respect to the conventional IDP approach [Figure 14(a)] only of about 6 dB, while the WPP-IDP [Figure 14(c)] yields a reduction of approximately 19.5 dB, obtaining a BNR of approximately 27.8 dB.

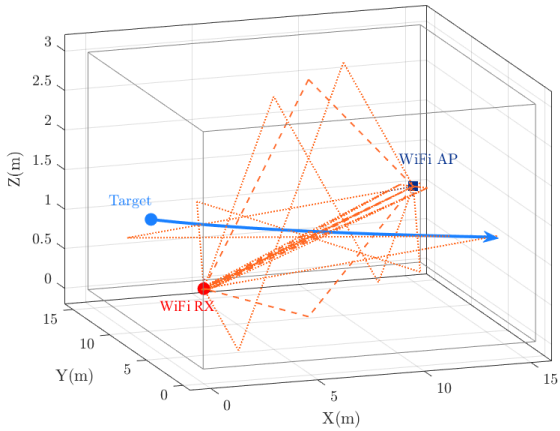
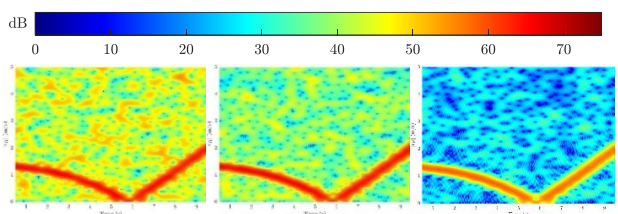


Figure 13. Sketch of the WiFi sensing scenario with multipath rays.

It is worth recalling that the same SNR loss of approximately 7 dB observed comparing Figure 10 and Figure 8 is obtained with the WPP-IDP approach that only employs a small portion of the entire packet, in this case composed of 20 OFDM symbols. Finally, by measuring the ratio between the target peak and the average background level we get a signal-to-background ratio (SBR) that equals 20.4 dB for the conventional IDP, 26.44 dB when the SBC-IDP is applied and 33.01 dB when the WPP-IDP is used. This analysis confirms that such a simple solution is the preferred strategy especially in multipath limited scenarios.



(a) (b) (c)

Figure 14. IDP output for (a) IDP (b) SBC-IDP (c) WPP-IDP.

V. EXPERIMENTAL VALIDATION

In this Section, we demonstrate the effectiveness of the proposed IDP approach against real-world WiFi data; this also allows to investigate the practical benefits of the devised strategies to mitigate the background level. For the purpose of this analysis, an *ad-hoc* acquisition campaign was carried out and different datasets were collected, varying (i) the acquisition geometry (ii) the number and type of targets in the scene (ii) the employed WiFi Standard. For the sake of simplicity, subsection A focuses on datasets collected in a target-free scenario and is mostly intended to investigate the performance in terms of background control, while subsection B reports the results obtained against cooperative targets in order to understand the corresponding advantages in terms of detection capability.

A. Experimental results on target-free data

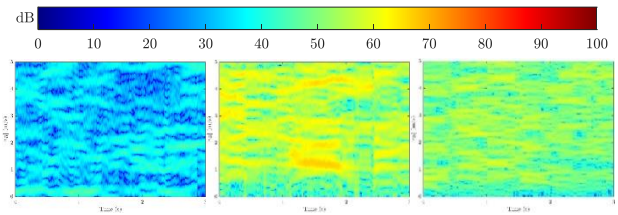
First, we consider experimental data collected in a disturbance-only condition and apply a simple IDP scheme, in order to experimentally demonstrate the validity of the theoretical BNR expression derived in Section III. To this purpose, we have employed three different IEEE 802.11 standards and we have extracted DSSS modulated beacons from dataset #1, QPSK modulated OFDM symbols from the ACK signals of dataset #2 and 16-QAM modulated symbols from the ACK signals of dataset #3. With this approach we were able to test the validity of eq. (10) under different conditions in terms of employed modulation scheme. Additional details for each dataset are reported in Table 4.

Table 4
Disturbance-only datasets parameters.

	Dataset #1	**Dataset #2**	**Dataset #3**
Access Point	D-Link DAP 1160	TP-Link Archer VR600 AC1600	TP-Link Archer VR600 AC1600
Number of targets	0	0	0
Location	Outdoor	Indoor	Outdoor
Carrier Frequency	2.472 GHz	2.472 GHz	5.18 GHz
Employed IEEE 802.11 Standard	IEEE 802.11b	IEEE 802.11n	IEEE 802.11ac
Modulation	DSSS	OFDM with 16-QAM	OFDM with QPSK
Measured DNR	31.5 dB	29.6 dB	30.1 dB

As a first result, Figure 15 shows the output of the IDP scheme in the absolute bistatic velocity-time plane for the three described datasets. In each case, the IDP was applied with $T_{DC} = 0.1\ s$ and $T_{STFT} = 0.5$ s. Moreover, we select $N_{sym} = 100$ for DSSS beacons and $N_{sym} = 2$ for the OFDM ACK packets. Note that, since we only use signalling packets for the purpose of this analysis, their length is intrinsically constant over time. However, we recall that, based on the findings of Section III, if packets with different original lengths were employed, it would be preferrable to limit the packet duration to a constant number of symbols N_{sym}. All the maps in Figure 15 are scaled for the expected ϱ_d, in order for the noise level to be

around 0 dB and for the map values to represent the BNR. In all cases, the input average DNR was measured to be between 29.6 dB and 31.5 dB. From Figure 15, we can notice how the average power level largely differs depending on the employed modulation. In fact, we obtain BNR ≅ 32.6 dB, BNR ≅ 56.6 dB, and BNR ≅ 51.7 dB, for subfigures (a), (b) and (c), respectively.

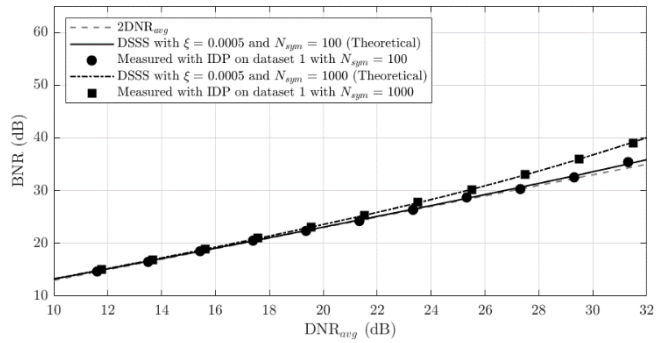


(a) (b) (c)

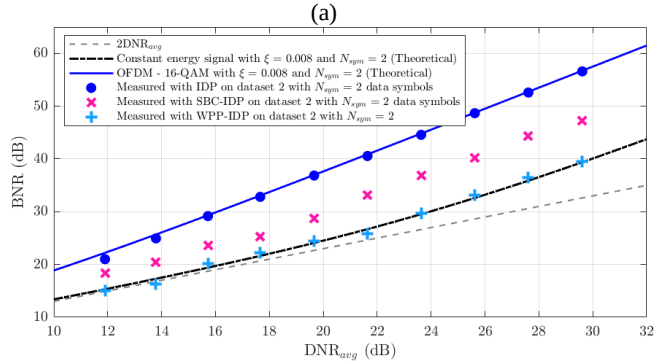
Figure 15. Output of the IDP on: (a) dataset #1 with $N_{sym} = 100$; (b) dataset #2 with $N_{sym} = 2$; (c) dataset #3 with $N_{sym} = 2$.

To understand the BNR behaviour as a function of average DNR, we repeat this analysis by boosting the thermal noise power level in the received signal. Specifically, we add AWGN with gradually increasing power, thus emulating gradually decreasing DNR_{avg} values, and we report in Figure 16 the BNR values measured on the final spectrograms after the application of the IDP. The results are shown in Figure 16 (a), (b) and (c) as black, blue and green colored markers for dataset #1, #2 and #3, respectively. Moreover, in each subfigure, curves with different colors and line styles identify the corresponding theoretical BNR curve, obtained using eq.(10) by properly selecting N_{sym}, μ and $g(\eta)$ depending on the considered datsaset and by fitting the ξ value to the data. Finally, in all subfigures, we also report the $2DNR_{avg}$ bound as dashed-gray curve for comparison.

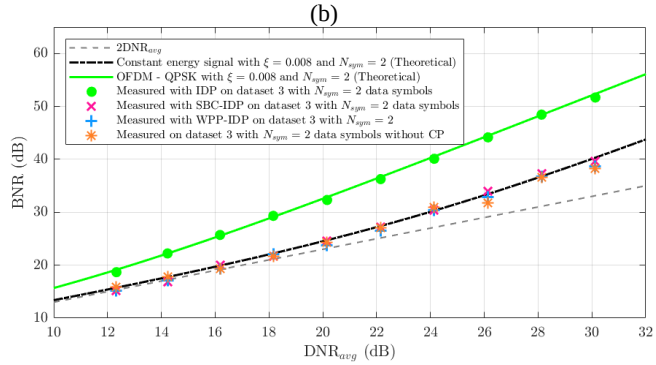
The curves in Figure 16(a) are referred to dataset #1, composed by DSSS-only packets, and are obtained by limiting the packet duration to either $N_{sym} = 100$ or $N_{sym} = 1000$ repetitions of the Barker code. We might observe that, as expected, for low DNRs, the two curves tend to look alike and equal to the dashed-gray one, i.e. the $2DNR_{avg}$ bound. Instead, the larger is the packet duration N_{sym}, the lower is the DNR_{avg} value where the BNR curve deviates from the dashed gray one and grows. This is because of the DNR fluctuation which has higher impact on longer PPDUs. Figure 16(a) further demonstrates the need to account for this power level fluctuation in the theoretical derivation reported in Section III, probably due to non idealities of the system, (e.g. instability of the commercial Aps, non constant sampling at the receiver), in order to obtain a very accurate prediction of the BNR.



(a)



(b)



(c)

Figure 16. Measured BNR vs DNR_{avg} for (a) dataset #1 (b) dataset #2 (c) dataset #3.

However, Figure 16 (a) also confirms that, in the presence of limited DNR fluctuations and for typical DNR_{avg} values, DSSS modulated packets do not require any strategy to lower the BNR level since this is largely comparable with the lower bound of $2 \cdot DNR_{avg}$. Blue and green curves and markers in Figure 16 (b) and (c), instead, respectively refer to datasets #2 and #3, both composed by OFDM modulated packets but employing different constellations.

Observing them, two considerations are in order: (i) as expected, the measured BNR is much higher than that obtained in Figure 16(a) for DSSS modulated packets and does not reach the dashed gray curve for none of the considered DNR values (ii) although the DNR fluctuation is higher than that observed in the DSSS case, it has a smaller impact on the obtained results, both because the

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3276738

packets are much shorter and because the major observed effect is related to the waveform, therefore the green and blue curves do not significantly differ from those shown in Figure 6, obtained with $\sigma^2_{DNR} = 0$. Figure 16 (b) and (c) also report additional colored markers showing the results obtained with the background reduction strategies proposed in Section IV. Note that, in order to enable the application of the SBC-IDP, during the experiments, the transmitted signal was extracted from the employed AP via a wired connection. For both the considered datasets, the use of a WPP-IDP based on $N_{sym} = 2$ OFDM symbols extracted from the PHY Preamble portion of the WiFi PPDUs (light blue markers) is the best performing solution and effectively reduces the measured BNR to the minimum achievable value, represented by the dash-dot black curve. In contrast, although the SBC-IDP (magenta markers) significantly reduces the measured BNR in both cases, the measured values lay on the black curve only for dataset #3 [Figure 16(c)]. Note that, as reported in Table 4, dataset #2 has been collected in an indoor area which is likely to be affected by higher multipath contributions that might jeopardize the effectiveness of the SBC strategy, as shown in Section IV. Finally, for dataset #3 [Figure 16(c)], orange markers are obtained by removing the CP from the QPSK OFDM symbols. As mentioned in Section IV, this solution is also able to effectively lower the BNR. However, we recall that (i) keeping N_{sym} constant, the CP-free solution offers a lower integration gain, since one-fifth of each OFDM symbol is discarded in the considered case; (ii) this solution would not be effective against symbols with larger constellations (with $\mu \neq 1$).

B. Experimental results on data including target echoes

The test data illustrated in this section have been collected using the same setup described above and listed in Table 4. Specifically, datasets #4 only include 802.11b DSSS modulated packets while dataset #5 is composed by OFDM modulated PPDUs.

1) Results for tests with DSSS modulated packets

Dataset #4 is composed by 802.11b beacons, with a nominal beacon interval of 3ms and has been collected with the experimental configuration sketched in Figure 17. It features one person, acting as cooperative target and walking along the direction described by the green arrow, namely along a linear trajectory, orthogonally crossing the Tx-Rx baseline approximately in its middle point (~10 m from both the AP and the Rx).

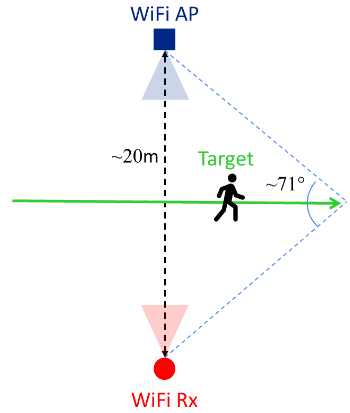


Figure 17. Experimental geometries for dataset #4.

Figure 18 shows the output of the IDP scheme applied to the collected signal, with $N_{sym} = 100$, $T_{DC} = 0.5$ s, $T_{STFT} = 1$ s and a Hamming tapering window for Doppler sidelobes level control. The results reported in Figure 18 shows that the IDP processing can recognize the target signature throughout the entire trajectory, that spans a wide range of bistatic angles, from 180 degrees, when it crosses the baseline, up to approximately 70 degrees, when it stops moving. Note that, based on the intensity of the signature when the target stops moving, at about 16 s, it is expected that the target could be detected well beyond that limit. The high capability of recognizing the presence of a target is certainly favored by the low background level measured on the map which, as demonstrated above, is typically obtained with the employed DSSS modulation. In fact, note that for an average DNR of approximately 23.1 dB measured for this dataset, the average level competing with the target response is of approximately 30 dB (represented by the blue color in this figure).

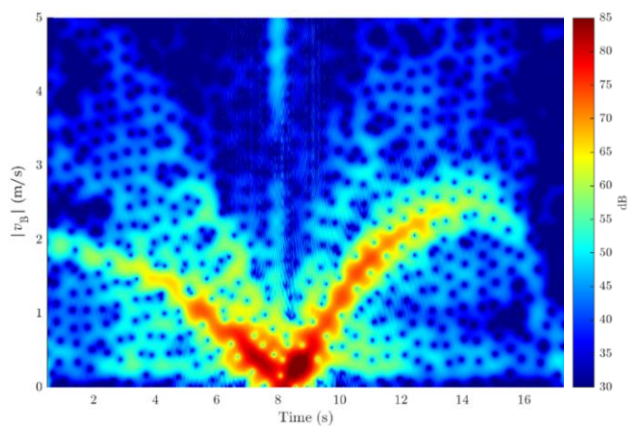
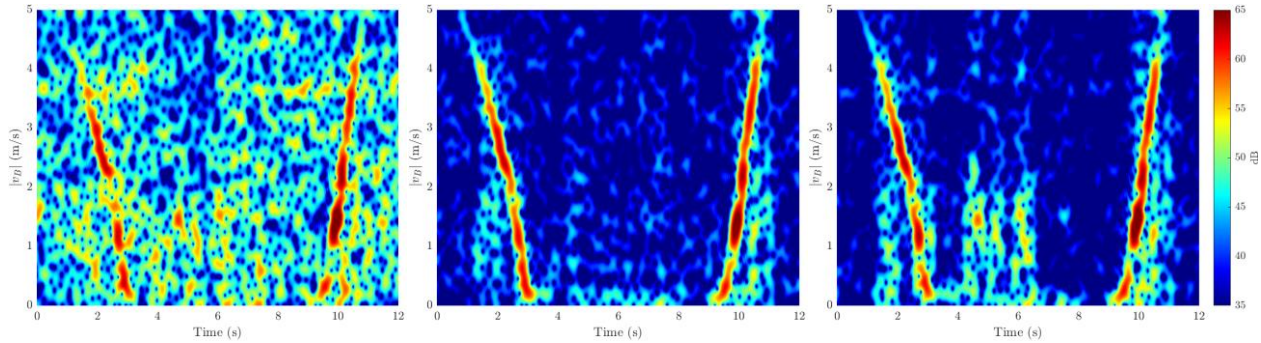


Figure 18. Experimental results for dataset #4.

Finally, note that, compared with the results obtained on simulated data with a point-like target, the following

This article has been accepted for publication in IEEE Transactions on Aerospace and Electronic Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TAES.2023.3276738



(a) (b) (c)

Figure 20. Output of the IDP technique for dataset #5 with
(a) IDP with $N_{sym} = 2$ data symbols; (b) SBC-IDP with $N_{sym} = 2$ data symbols; (c) WPP-IDP with $N_{sym} = 2$.

differences are apparent due to the real target response: (i) an enhancement of the response at the apex of the V-shaped Doppler signature, namely when the target crosses the baseline; (ii) a fading of target signature as its distance from the baseline increases; (iii) a modulation of the signature due to micro-Doppler effects caused by the periodic movement of the target's limbs.

2) Results for tests with OFDM modulated packets

The purpose of this last analysis is to investigate the capability of the proposed IDP technique to detect a small RCS target. To this end, a small drone (DJI Mavic Pro) was exploited as cooperative target. Note that the employed UAV is lightweight (about 730 g) with small size (about 30 x 25 x 8 cm). The experimental configuration is sketched in Figure 19 and the employed setup is the same reported in Table 4 for dataset #3. Specifically, in the performed test, the small UAV gets close to the Tx-Rx baseline along an orthogonal trajectory, stops for 5 seconds, and then moves away. The results are reported in Figure 20, for $T_{DC} = 0.2\ s$ and $T_{STFT} = 0.5\ s$. Note that, in this case, we do not limit the processing to a single constellation, therefore we include both ACK and RTS packets characterized by QPSK and 16-QAM data fields, respectively.

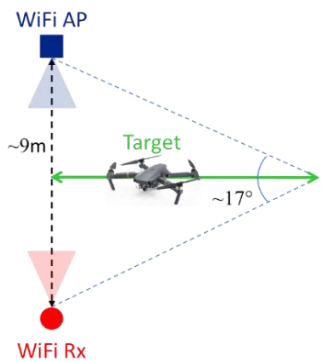


Figure 19. Experimental geometries for dataset #5.

By observing Figure 20, the following comments apply:

1) When $N_{sym} = 2$ are extracted from the data portion of the PPDUs and no background reduction strategy is applied [Figure 20 (a)], the target signature is barely distinguished from the background level.
2) When $N_{sym} = 2$ are extracted from the data portion of the PPDUs and the SBC approach is applied [Figure 20 (b)], the improvement is tremendous and the target echo is easily distinguished for the entire trajectory.
3) When $N_{sym} = 2$ are extracted from the PHY Preamble portion of the PPDUs, namely when a WPP-IDP approach is used [Figure 20 (c)], the target track is entirely visible. Still, the effects of some spurious packets are observed, especially between 4 and 6 s, which corresponds to deviations in the Tx power level. These are effectively estimated and mitigated with the SBC-IDP whereas the WPP-IDP relies on the ideal hypothesis of constant energy preambles.

To elaborate further on the comparison between the SBC-IDP and the WPP-IDP, we should recall that the reference signal used to operate the SBC was made available in this case for analysis purpose; in a practical scenario, it should be reconstructed from the received signal and might be subject to reconstruction errors. Moreover, the need to reconstruct the transmitted waveform as well as the SBC-IDP overall require higher computational load than the WPP-IDP. Also, we recall that the SBC in the considered test is operated in a favorable condition since this dataset was collected in an outdoor scenario, where the multipath contributions are expected to be limited. On the other hand, for the purpose of this analysis, we have limited to $N_{sym} = 2$ OFDM symbols the packets portion processed in all cases; however, if the SBC-IDP is applied, the use of the entire WiFi packet is, in principle, possible, which could enable a higher target SNR. Overall, both the SBC-IDP and the

WPP-IDP can be considered as effective solutions for BNR mitigation when OFDM signals are used and their benefits in term of capability of detection small targets is apparent. The best solution among the two might depend on the specific application.

VI. CONCLUSIONS

In this work, we have investigated the possibility of using a novel, reference-free and amplitude-based processing approach for WiFi based passive sensing. Specifically, we look for the presence of a moving target by observing the amplitude modulation that it produces on the direct signal transmitted from the WiFi AP across time.

The main outcomes of this work are listed below:

(i) The adaptation of the considered principle of operation to the application at hand.

(ii) A theoretical characterization of the average disturbance level measured at the output of the proposed processing and competing with the target, taking into account real-world effects that are expected to limit the achievable performance, such as the waveform properties.

(iii) Validation of the theoretical findings with both simulated and real WiFi data.

(iv) The proposal of two possible solutions that address the identified issues, namely the SBC-IDP and the WPP-IDP, characterized by different complexity and achievable performance.

(v) Extensive testing with experimental data employing different RCS targets and bistatic geometries.

APPENDIX

In this Appendix, we theoretically derive the background level at the output of the IDP scheme based on the signal model in (6) and subsequent definitions, under the null H_0 hypothesis (target absent). To this aim, we follow a similar procedure as that used in [29] but the mathematical developments are extended in order to take into account realistic effects typical of the application under analysis. Specifically, we look for $E\{|w(m)|^2|H_0\}$ that, using (5), can be evaluated as:

$$E\{|w(m)|^2|H_0\} = \sum_{p=0}^{N_P-1}\sum_{p'=0}^{N_P-1} h(p)h(p')\, \mathrm{e}^{-j2\pi\frac{m}{N_P}(p-p')} \times E\{\bar{z}(p_0+p)\bar{z}(p_0+p')\} \quad (17)$$

where $E\{\cdot\}$ denotes the statistical expectation with respect to all the considered random variables, i.e., $E\{\cdot\} = E_{N,\alpha,s,d}\{\cdot\}$. Assuming that different packets are statistically independent and that z_{DC} in eq. (4) is an unbiased estimate of $E\{z(p)\}$, $E\{\bar{z}(p)\bar{z}(p')\} = 0$ when $p \neq p'$, and (32) simplifies as:

$$E\{|w(m)|^2|H_0\} = \sum_{p=0}^{N_P-1} h^2(p)\, E\{\bar{z}^2(p_0+p)\} \quad (18)$$

We can write

$$E\{\bar{z}^2(p)\} = E\{z^2(p)\} - E^2\{z(p)\} \quad (19)$$

where $E\{z(p)\}$ and $E\{z^2(p)\}$ are the first and the second moment of $z(p)$, respectively. Based on definitions in eqs. (2) and (3), these are given by

$$E\{z(p)\} = E_N\left\{\sum_{l=0}^{N_{sym}^{(p)}N_s-1} E_{\alpha,s,d}\left\{\left|x_p(l)\right|^2\right\}\right\} \quad (20)$$

$$E\{z^2(p)\} = E_N\left\{\sum_{l=0}^{N_{sym}^{(p)}N_s-1}\sum_{l'=0}^{N_{sym}^{(p)}N_s-1} E_{\alpha,s,d}\left\{\left|x_p(l)\right|^2\left|x_p(l')\right|^2\right\}\right\} \quad (21)$$

In order to rework eqs. (20)-(21), we write the moments of $x_p(l)$ as

$$E_{\alpha,s,d}\{x_p(l)\} = E_\alpha\{\alpha_{0,p}\}E_s\{s_p(l)\} + E_d\{d_p(l)\} = 0 \quad (22)$$

$$E_{\alpha,s,d}\left\{\left|x_p(l)\right|^2\right\} = E_{\alpha,s,d}\left\{\left|\alpha_{0,p}\right|^2\left|s_p(l)\right|^2 + \left|d_p(l)\right|^2 + 2\Re\{\alpha_{0,p}s_p(l)d_p^*(l)\}\right\} = m_{\alpha,2} + \sigma_D^2 \quad (23)$$

where we used the assumption that the employed waveform $s_p(l)$ is a zero-mean unitary power random process and the disturbance is modeled as a zero-mean complex Gaussian process with variance σ_D^2. Therefore, (20) can be simply evaluated as:

$$E\{z(p)\} = m_{N,1}N_s\left(m_{\alpha,2} + \sigma_D^2\right) \quad (24)$$

Moreover, we can write:

$$
\begin{aligned}
&E_{\alpha,s,d}\left\{\left|x_p(l)\right|^2\left|x_p(l')\right|^2\right\}\\
&= m_{\alpha,4}E_s\left\{\left|s_p(l)\right|^2\left|s_p(l')\right|^2\right\} + 2m_{\alpha,2}\sigma_D^2\\
&+ E_d\left\{\left|d_p(l)\right|^2\left|d_p(l')\right|^2\right\}\\
&+ 4E_{\alpha,s,d}\left\{\Re\{\alpha_{0,p}s_p(l)d_p^*(l)\}\right.\\
&\left.\times\,\Re\{\alpha_{0,p}s_p(l')d_p^*(l')\}\right\}
\end{aligned}
\tag{25}
$$

In order to rework eq. (25), we recall that

$$
E_d\left\{\left|d_p(l)\right|^2\left|d_p(l')\right|^2\right\} = \begin{cases}\sigma_D^4 & \text{if } l \neq l'\\ 2\sigma_D^4 & \text{if } l = l'\end{cases}
\tag{26}
$$

and we compute the last expected value in (25) as

$$
\begin{aligned}
&E_{\alpha,s,d}\left\{\Re\{\alpha_{0,p}s_p(l)d_p^*(l)\}\Re\{\alpha_{0,p}s_p(l')d_p^*(l')\}\right\}\\
&\qquad = \begin{cases}0 & \text{if } l \neq l'\\ \dfrac{1}{2}\sigma_D^2\, m_{\alpha,2} & \text{if } l = l'\end{cases}
\end{aligned}
\tag{27}
$$

The larger order statistics of the random process modelling the waveform, instead, depend on the employed modulation scheme:

– <u>For DSSS modulated packets</u>

$$
E_s\left\{\left|s_p(qN_s+n)\right|^4\right\} = E_s\left\{\left|c^{(p,q)}\right|^4\right\} = C^2\mu = 1
\tag{28}
$$

where we recall that index $q = \lfloor l/N_s \rfloor$ scans the symbols, index $n = l - qN_s$ scans the samples within the symbol, C represents the average power of the employed constellation, defined as $C = \frac{1}{M_c}\sum_{m=0}^{M_c-1}|\gamma_m|^2$ and we used $\mu = 1$ since, in this case, either BPSK or QPSK constellations are adopted.

$$
\begin{aligned}
&E_s\left\{\left|s_p(qN_s+n)\right|^2\left|s_p(q'N_s+n')\right|^2\right\} =\\
&\begin{cases} m_{s,2}^2 = 1, & \text{if } q \neq q'\\ E_s\left\{\left|s_p(qN_s+n)\right|^2\left|s_p(qN_s+n')\right|^2\right\} = 1, & \text{if } q = q'\end{cases}
\end{aligned}
\tag{29}
$$

– <u>For OFDM modulated packets</u>

Assuming that the constellation is scaled so that the waveform is a unitary power process, i.e., $C = 1/N_c$, the fourth order moment of the transmitted waveform, can be expressed as

$$
\begin{aligned}
&E_s\left\{\left|s_p(qN_s+n)\right|^4\right\}\\
&\qquad = \begin{cases}\left[\dfrac{\mu-3}{N_c}+3\right] & \text{if } M_c = 2\\ \left[\dfrac{\mu-2}{N_c}+2\right] & \text{if } M_c \geq 4\end{cases}
\end{aligned}
\tag{30}
$$

Furthermore, we can write

$$
\begin{aligned}
&E_s\left\{\left|s_p(qN_s+n)\right|^2\left|s_p(q'N_s+n')\right|^2\right\} =\\
&E_s\left\{\left|\sum_{k=0}^{N_c-1} c_k^{(p,q)}\, e^{j\frac{2\pi}{N_c}kn}\right|^2\left|\sum_{k\prime=0}^{N_c-1} c_{k'}^{(p,q)}\, e^{j\frac{2\pi}{N_c}k'n'}\right|^2\right\}\\
&= \sum_{k=0}^{N_c-1}\sum_{r=0}^{N_c-1}\sum_{k\prime=0}^{N_c-1}\sum_{r\prime=0}^{N_c-1} E_c\left\{c_k^{(p,q)}c_r^{(p,q)^*}c_{k'}^{(p,q)}c_{r'}^{(p,q)^*}\right\}\\
&\qquad\qquad \times e^{j\frac{2\pi}{N_c}[(k-r)n+(k'-r')n']}
\end{aligned}
\tag{31}
$$

Based on

$$
\begin{aligned}
&E_c\left\{c_k^{(p,q)}c_r^{(p,q)^*}c_{k'}^{(p,q)}c_{r'}^{(p,q)^*}\right\}\\
&= \begin{cases} m_{c,4} & \text{if } k = r = k' = r'\\ C^2 & \text{if } k = r, k' = r', k \neq k' \text{ or}\\ & \quad k = r', k' = r, k \neq r\\ C^2 & \text{if } M_c = 2, k' = k', r = r', r \neq k\\ m_{c,4} & \text{otherwise}\end{cases}
\end{aligned}
\tag{32}
$$

eq. (31) can be reworked as follows

$$
\begin{aligned}
&E_s\left\{\left|\sum_{k=0}^{N_c-1} c_k^{(p,q)}\, e^{j\frac{2\pi}{N_c}kn}\right|^2\left|\sum_{k\prime=0}^{N_c-1} c_{k'}^{(p,q)}\, e^{j\frac{2\pi}{N_c}k'n'}\right|^2\right\} =\\
&\begin{cases}\left[\dfrac{\mu-3}{N_c}+1+\delta(n-n',N_c)+\delta(n+n',N_c)\right] & \text{if } M_c = 2\\ \left[\dfrac{\mu-2}{N_c}+1+\delta(n-n',N_c)\right] & \text{if } M_c \geq 4\end{cases}
\end{aligned}
\tag{33}
$$

where the $\delta(n-n',N_c)$ function accounts for the correlation of the samples inside the OFDM symbol with its repeated portion (CP). Moreover, the additional $\delta(n+n',N_c)$ function in the $M_c = 2$ case is due to the symmetry of the OFDM BPSK symbol, obtained as the IFFT of a real sequence.

Therefore, we have

$$E_s\left\{\left|s_p(qN_s+n)\right|^2\left|s_p(q'N_s+n')\right|^2\right\} = \begin{cases} 1 & \text{if } q \neq q' \\ \left[\frac{\mu-3}{N_c}+1+\delta(n-n',N_c)+\delta(n+n',N_c)\right] & \text{if } q=q', M_c=2 \\ \left[\frac{\mu-2}{N_c}+1+\delta(n-n',N_c)\right] & \text{if } q=q', M_c\geq 4 \end{cases} \quad (34)$$

$$n,n' = -N_{cp},\dots,N_c-1$$

By substituting either eq. (34) or (29) and eqs. (26)-(27) in (25), we obtain:

– For OFDM modulated packets

$$E_{\alpha,s,d}\left\{\left|x_p(l)\right|^2\left|x_p(l')\right|^2\right\} =$$
$$E_{\alpha,s,d}\left\{\left|x_p(qN_s+n)\right|^2\left|x_p(q'N_s+n')\right|^2\right\} = \begin{cases} m_{\alpha,4}+2m_{\alpha,2}\sigma_D^2+\sigma_D^4 & \text{if } q\neq q' \\ m_{\alpha,4}\left[\frac{\mu-3}{N_c}+1+\delta(n-n',N_c)+\delta(n+n',N_c)\right]+ & \\ 2m_{\alpha,2}\sigma_D^2+\sigma_D^4+\delta(n-n')\left(\sigma_D^4+2m_{\alpha,2}\sigma_D^2\right) & \text{, if } q=q', M_c=2 \\ m_{\alpha,4}\left[\frac{\mu-2}{N_c}+1+\delta(n-n',N_c)\right]+2m_{\alpha,2}\sigma_D^2+ & \\ \sigma_D^4+\delta(n-n')\left(\sigma_D^4+2m_{\alpha,2}\sigma_D^2\right) & \text{, if } q=q', M_c\geq 4 \end{cases} \quad (35)$$

$$n,n' = -N_{cp},\dots,N_c-1$$

– For DSSS modulated packets

$$E_{\alpha,s,d}\left\{\left|x_p(l)\right|^2\left|x_p(l')\right|^2\right\} = \begin{cases} m_{\alpha,4}+2m_{\alpha,2}\sigma_D^2+\sigma_D^4 & \text{if } l\neq l' \\ m_{\alpha,4}+4m_{\alpha,2}\sigma_D^2+2\sigma_D^4 & \text{if } l=l' \end{cases} \quad (36)$$

Therefore, eq. (21) becomes

– For OFDM modulated packets and $M_c = 2$

$$E\{z^2(p)\} = \left(m_{N,2}N_s^2+m_{N,1}N_s\right)\left(m_{\alpha,4}+2m_{\alpha,2}\sigma_D^2+\sigma_D^4\right) + m_{\alpha,4}m_{N,1}N_s\left[\frac{N_s}{N_c}(\mu-3)+\frac{4N_{cp}+N_c}{N_s}\right] \quad (37)$$

– For OFDM modulated packets and $M_c \geq 4$

$$E\{z^2(p)\} = \left(m_{N,2}N_s^2+m_{N,1}N_s\right)\left(m_{\alpha,4}+2m_{\alpha,2}\sigma_D^2+\sigma_D^4\right) + m_{\alpha,4}m_{N,1}N_s\left[\frac{N_s}{N_c}(\mu-2)+2\frac{N_{cp}}{N_s}\right] \quad (38)$$

– For DSSS modulated packets

$$E\{z^2(p)\} = m_{N,2}N_s^2\left(m_{\alpha,4}+2m_{\alpha,2}\sigma_D^2+\sigma_D^4\right) + m_{N,1}N_s\left(2m_{\alpha,2}\sigma_D^2+\sigma_D^4\right) \quad (39)$$

Then, we define $DNR_{avg} = \frac{m_{\alpha,2}}{\sigma_D^2}$, $\sigma_{DNR}^2 = \frac{m_{\alpha,4}-m_{\alpha,2}}{\sigma_D^4}$, $\eta = N_{cp}/N_c$ and we use (37)-(39) in (19). Finally, the obtained result is used in (17). By defining

$$g(\eta) = \begin{cases} 0 & \text{for DSSS} \\ \eta\left(\mu-3+\frac{3}{(\eta+1)}\right) & \text{for OFDM with } M_c=2 \\ \eta\left(\mu-2+\frac{2}{(\eta+1)}\right) & \text{for OFDM with } M_c\geq 4 \end{cases} \quad (40)$$

with $\eta = 0.25$, namely with the CP length tipically being one quarter of N_c, we obtain

$$E\{|w(m)|^2|H_0\} = \left\{\sum_{p=0}^{N_P-1}h^2(p)\right\}\sigma_N^2N_sm_{N,1} \times\left\{2DNR_{avg}+1 + DNR_{avg}^2[\mu-1+g(\eta)] + \frac{\sigma_N^2}{m_{N,1}}N_s\left[\sigma_{DNR}^2+\left(DNR_{avg}+1\right)^2\right] + \sigma_{DNR}^2\left[m_{N,1}N_s+\mu-1+g(\eta)\right]\right\} \quad (41)$$

which corresponds to the expression in eq. (10).

REFERENCES

[1] 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.

[2] 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.

[3] D. Pastina, F. Colone, T. Martelli and P. Falcone, "Parasitic Exploitation of Wi-Fi Signals for Indoor Radar Surveillance," in *IEEE Transactions on Vehicular Technology*, vol. 64, no. 4, pp. 1401-1415, April 2015.

[4] H. Wang, D. Zhang, Y. Wang, J. Ma, Y. Wang and S. Li, "RT-Fall: A Real-Time and Contactless Fall Detection System with Commodity WiFi Devices," in *IEEE Transactions on Mobile Computing*, vol. 16, no. 2, pp. 511-526, 1 Feb. 2017.

[5] W. Li, R. J. Piechocki, K. Woodbridge, C. Tang and K. Chetty, "Passive WiFi Radar for Human Sensing Using a Stand-Alone Access Point," in *IEEE Transactions on Geoscience and Remote Sensing*, vol. 59, no. 3, pp. 1986-1998, March 2021.

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

[7] I. Milani, C. Bongioanni, F. Colone, and P. Lombardo, "Fusing Measurements from Wi-Fi Emission-Based and Passive Radar Sensors for Short-Range Surveillance," *Remote Sensing*, vol. 13, no. 18, p. 3556, Sep. 2021.

[8] W. Wang, A. X. Liu, M. Shahzad, K. Ling and S. Lu, "Device-Free Human Activity Recognition Using Commercial WiFi Devices," in *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 5, pp. 1118-1131, May 2017.

[9] 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.

[10] 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.

[11] H. Yan, Y. Zhang, Y. Wang and K. Xu, "WiAct: A Passive WiFi-Based Human Activity Recognition System," in *IEEE Sensors Journal*, vol. 20, no. 1, pp. 296-305, 1 Jan.1, 2020.

[12] 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.

[13] W. Li *et al*., "A Taxonomy of WiFi Sensing: CSI vs Passive WiFi Radar," *2020 IEEE Globecom Workshops*, 2020, pp. 1-6.

[14] W. Li, R. J. Piechocki, K. Woodbridge, C. Tang and K. Chetty, "Passive WiFi Radar for Human Sensing Using a Stand-Alone Access Point," in *IEEE Transactions on Geoscience and Remote Sensing*, vol. 59, no. 3, pp. 1986-1998, March 2021.

[15] 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.

[16] M. Di Seglio, F. Filippini, K. Chetty and F. Colone, "Reducing the computational complexity of WiFi-based passive radar processing," *2022 IEEE Radar Conference (RadarConf22)*, 2022, pp. 01-06.

[17] M. Di Seglio, F. Filippini, C. Bongioanni and F. Colone, "Human and Drone Surveillance via RpF-based WiFi Passive Radar: Experimental Validation," *2022 23rd International Radar Symposium (IRS)*, 2022, pp. 402-407.

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

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

[20] 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.

[21] I. Suberviola, I. Mayordomo, and J. Mendizabal, " Experimental results of air target detection with a GPS forward scattering radar, " *IEEE Geoscience and Remote Sensing Letters*, vol. 9, no. 1, pp. 47–51, Jan. 2012.

[22] C. Kabakchiev, I. Garvanov, V. Behar, and H. Rohling " The experimental study of possibility for radar target detection in FSR using L1-based non-cooperative transmitter" In Proc. 14th Int. Radar Symp., 2013, pp. 625–630.

[23] M. Gashinova, L. Daniel, E. Hoare, V. Sizov, K. Kabakchiev, and M. Cherniakov, " Signal characterization and processing in the forward scatter mode of bistatic passive coherent location systems", *EURASIP J. Adv. Signal Process.* 2013, 36 (2013).

[24] P. Krysik, K. Kulpa and P. Samczyński, "GSM based passive receiver using forward scatter radar geometry," *2013 14th International Radar Symposium (IRS)*, 2013, pp. 637-64.

[25] C. Kabakchiev, V. Behar, I. Garvanov, D. Kabakchieva and H. Rohling, "Detection, parametric imaging and classification of very small marine targets emerged in heavy sea clutter utilizing GPS-based Forward Scattering Radar," *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2014, pp. 793-797.

[26] M. Contu et al., "Passive multifrequency forward-scatter radar measurements of airborne targets using broadcasting signals, " *IEEE Transactions on Aerospace and Electronic Systems*, vol. 53, no. 3, pp. 1067–1087, Jun. 2017.

[27] A. Arcangeli, C. Bongioanni, N. Ustalli, D. Pastina and P. Lombardo, "Passive forward scatter radar based on satellite TV broadcast for air target detection: Preliminary experimental results," *2017 IEEE Radar Conference (RadarConf)*, 2017, pp. 1592-1596.

[28] N. Ustalli, P. Lombardo and D. Pastina, "Detection Performance of a Forward Scatter Radar Using a Crystal Video Detector," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 3, pp. 1093-1114, June 2018.

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

[30] B. Mrazovac, M. Z. Bjelica, D. Kukolj, B. M. Todorovic and D. Samardzija, "A human detection method for residential smart energy systems based on Zigbee RSSI changes," in *IEEE Transactions on Consumer Electronics*, vol. 58, no. 3, pp. 819-824, August 2012.

[31] J. Wilson and N. Patwari, "See-Through Walls: Motion Tracking Using Variance-Based Radio Tomography Networks," in *IEEE Transactions on Mobile Computing*, vol. 10, no. 5, pp. 612-621, May 2011.

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

[33] Jemai, Kumer, Varone and Wagen, "Determination of the Permittivity of Building Materials through WLAN Measurements at 2.4 GHz," *2005 IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2005, pp. 589-593.

FABIOLA COLONE (Senior Member, IEEE) received the degree in Telecommunications Engineering and the Ph.D. degree in Remote Sensing from Sapienza University of Rome, Italy, in 2002 and 2006, respectively. She joined the DIET Dept. of Sapienza University of Rome as a Research Associate in January 2006. From December 2006 to June 2007, she was a Visiting Scientist at the Electronic and Electrical Engineering Dept. of the University College London, London, UK. She is currently a Full Professor at the Faculty of Information Engineering, Informatics, and Statistics of Sapienza University of Rome, where she serves as Chair of the degree programs in Communications Engineering.

The majority of Dr. Colone's research activity is devoted to radar systems and signal processing. She has been involved, with scientific responsibility roles, in research projects funded by the European Commission, the European Defence Agency, the Italian Space Agency, the Italian Ministry of Research, and many radar/ICT companies. Her research has been reported in over 170 publications in international technical journals, book chapters, and conference proceedings. Dr. Colone is co-editor of the book "Radar Countermeasures for Unmanned Aerial Vehicles", IET Publisher. She has been co-recipient of the 2018 Premium Award for Best Paper in IET Radar, Sonar & Navigation.

From 2017 to 2022, she was member of the Board of Governors of the IEEE Aerospace and Electronic System Society (AESS) in which she served as Vice-President for Member Services, and Editor in Chief for the IEEE AESS QEB Newsletters. She is IEEE Senior Member from 2017 and member of the IEEE AESS Radar System Panel from 2019. Dr. Colone is the Associate Editor in Chief for the IEEE Transactions on Radar Systems. She was Associate Editor for the IEEE Transactions on Signal Processing from 2017 to 2020 and she is member of the Editorial Board of the Int. Journal of Electronics and Communications (Elsevier). She was Technical co-Chair of the IEEE 2021 Radar Conference (Atlanta, USA) and of the European Radar Conference EuRAD 2022 (Milan, Italy) and she served in the organizing committee and in the technical program committee of many international conferences.

FRANCESCA FILIPPINI (Member, IEEE) received her M.Sc. degree (*cumLaude*) in Communication Engineering and the Ph.D. degree in Radar and Remote Sensing, from Sapienza University of Rome, in 2016 and 2020, respectively. From January to May 2016, she has been working on her Master Thesis with the Fraunhofer Institute FHR. From February 2020 to November 2022, she was a Post-Doctoral Researcher with the Department of Information Engineering, Electronics and Telecommunications at Sapienza University of Rome. She is currently working as a Staff Engineer Radar Algorithms at Infineon Technologies AG.

Dr. Filippini received the 2020 IEEE AESS Robert T. Hill Best Dissertation Award for her Ph.D. thesis and the 2020 GTTI Best PhD Thesis Award defended at an Italian University in the areas of communications technology. She also received the 2018 Premium Award for the Best Paper in IET Radar, Sonar &Navigation, the Best Paper Award at the 2019 International Radar Conference, the second-Best Student Paper Award at the 2018 IEEE Radar Conference, and the Best Paper Award at the 2017 GTTI Workshop on Radar and Remote Sensing. She is a member of the Board of Governors of the IEEE Aerospace and Electronic System Society, where she is currently serving as Co-Editor in Chief of the IEEE AESS QEB.

MARCO DI SEGLIO (Graduate Student Member, IEEE) received the B.Sc. and M.Sc. (cum laude) degrees in communication engineering from Sapienza University of Rome, Rome, Italy, in 2017 and 2019, respectively. He is currently working toward the Ph.D. degree in radar and remote sensing at the Department of Information Engineering, Electronics and Telecommunications, Sapienza University of Rome. His research interests include the development of advanced signal processing techniques and methodologies for WiFi-based passive radar systems.

PAUL V. BRENNAN graduated from UCL in 1986 with PhD and BSc (Eng) degrees in Electronic Engineering. He is currently Professor of Microwave Electronics and Head of the Sensors, Systems and Circuits Group in the Department of Electronic and Electrical Engineering at UCL. He is active in a variety of areas in the fields of RF/microwave electronics, phased array antennas and radar systems, with support from a wide range of sources including EPSRC, NERC, INNOVATE UK, the EU and industry. He is author or co-author of over 250 publications and a number of patents in the areas of radar imaging and antenna arrays, frequency synthesisers (including a PLL textbook) and MIMO FMCW radar systems. In recent years, he has developed, in collaboration with the British Antarctic Survey, field-ready radar systems to image geophysical phenomena such as snow avalanches, and Antarctic ice shelves.

RUI DU (Member, IEEE) Rui Du received the M.S. and Ph.D. degrees in Information and Communication Engineering from Northwestern Polytechnical University, in 2014 and 2018 respectively. During 2015-2017, he was a visiting PhD student at Microwave Integrated Systems Laboratory, University of Birmingham. He joined Wireless Technology Laboratory, Huawei, 2018. His current research focuses on wireless communication, signal processing, integrated communication and sensing (ISAC) and standardization of wireless communication.

TONY XIAO HAN (Senior Member, IEEE) is currently a Principal Engineer with Huawei Technologies Co., Ltd. He received the B.E. degree in electrical engineering from Sichuan University and the Ph.D. degree in communication engineering from Zhejiang University, Hangzhou, China. He was a Post-Doctoral Research Fellow with the National University of Singapore.

He was the Chair of IEEE 802.11 WLAN Sensing Topic Interest Group (TIG), the Chair of 802.11 WLAN Sensing Study Group (SG), and currently he is serving as the Chair of IEEE 802.11bf WLAN Sensing Task Group (TG). He is the Industry Chair of IEEE ComSoc Integrated Sensing and Communication Emerging Technology Initiative (ISAC-ETI), the Vice Chair of IEEE WTC Special Interest Group (SIG) on ISAC, a Guest Editor of the IEEE Journal on Selected Areas in Communications (JSAC) Special Issue on "Integrated Sensing and Communications (ISAC)", and he has served as the ISAC Workshop Co-Chair of IEEE GLOBECOM 2020. His research interests include wireless communication, signal processing, Integrated Sensing and Communication (ISAC), and standardization of wireless communication.