Received: 1 May 2023 | Revised: 11 October 2023 | Accepted: 29 October 2023

IET Radar, Sonar & Navigation

DOI: 10.1049/rsn2.12506

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Comparing reference-free WiFi radar sensing approaches for monitoring people and drones

Marco Di Seglio[1] | Francesca Filippini[1] | Carlo Bongioanni[2] | Fabiola Colone[1]

[1]University of Rome La Sapienza, Department of Information Engineering, Electronics and Telecommunications, Rome, Italy

[2]School of Advanced Defence Studies, Rome, Italy

Correspondence

Marco Di Seglio.
Email: marco.diseglio@uniroma1.it

Abstract

The use of WiFi signals for sensing purposes has attracted a lot of interest from both the radar and communications communities and several techniques have been explored. In the attempt of meeting the requirements for small sensor size, compactness, and easy deployment, the authors consider reference-free approaches, namely approaches that do not require a good copy of the transmitted waveform to be available at the radar receiver. To this end, the authors first resort to a passive radar-based processing scheme that only exploits the invariant *a priori* known initial portion of the physical layer protocol data unit, that is, the PHY Preamble, and its limitations in practical applications is investigated. Specifically, the authors show that, with this approach, an accurate time, phase, and frequency synchronization is essential and a possible strategy is investigated. As an alternative solution the authors consider a forward scatter radar-based approach where only the amplitude modulation of the received signal is exploited to detect the presence of a moving target thus avoiding the need to know the transmitted signal. For the first time, the authors comparatively investigate advantages and drawbacks of the two reference-free approaches and present practical strategies to handle the limitations observed. The results are reported for experimental tests with people and drones using WiFi transmissions in the 2.4 and 5 GHz band.

KEYWORDS

passive radar, radar detection, remote sensing, surveillance, wireless LAN

1 | INTRODUCTION

The parasitic exploitation of WiFi transmissions for short range sensing is a topic that recently attracted considerable research and commercial interest [1–11]. In fact, the ubiquity of WiFi Access Points (APs) in both private and public premises would enable a distributed sensing network aimed at the monitoring of human activity for surveillance purposes as well as for e-healthcare applications, without raising any privacy concerns, as it would be the case for cameras and/or wearable devises.

To this purpose, WiFi-based passive radar (PR) sensors can be considered. According to its principle of operation, a passive receiver collects the echoes from moving targets illuminated by a WiFi access point (AP) as this provides connection services in a local area. Coherent detection of such echoes and subsequent tracking is guaranteed by the availability of a good copy of the transmitted signal at the receiver. In Refs. [1–11] and related works, the suitability of WiFi signals as waveforms of opportunity for PR has been investigated and appropriate signal processing strategies have been proposed for detecting and localising moving targets against the competing background, namely the direct signal from the transmitter, its multipath replicas, and the receiver noise. The effectiveness of such approaches has been proved in several experimental tests against drones, vehicles, and people. Recent works by the authors [12–14] have focused on the simplification of the PR processing chain with the purpose of streamlining the processing architecture and reducing the required computational burden. An effective signal processing chain has been designed

which is robust to current or future IEEE 802.11 standards employing different modulation schemes and reduces potential masking effects in the range domain that would prevent the detection of low radar cross section targets.

However, as previously mentioned, a PR processing scheme is inherently based on the availability of a good copy of the transmitted signal, which can be either (i) extracted directly from the AP in a semi-cooperative configuration, (ii) collected with a dedicated reference antenna, or (iii) extracted from the surveillance signal itself, via demodulation, reconstruction and standard-based remodulation [1].

Nevertheless, to facilitate the widespread use of WiFi-based sensors, key aspects must be considered such as the low cost, the compactness and lightness, as well as the easy deployment and setup. Based on these needs, it is not possible to consider an installation that would require any wiring, as would be necessary to extract the transmitted waveform directly from the AP. Also, adding a dedicated antenna steered toward the transmitter would jeopardize the compactness of the system and require an additional receiving channel. Finally, reconstructing the transmitted signal directly from the surveillance one would complicate the processing and its success would strictly depend on the signal-to-noise ratio (SNR) conditions of the received signal.

In this paper, we take this perspective and consider a scenario where a good copy of the transmitted signal is not available at the receiver. Therefore, we look for reference-free sensing approaches to be employed in such conditions.

To this purpose we first consider a sensing approach where a PR-based processing scheme is applied to the time invariant and standard-based portion of the physical layer protocol data unit (PPDU). Basically, we investigate the possibility of limiting the signal processing to the a priori known PHY Preamble of the WiFi packet and we synthetize the reference signal based on employed 802.11 standard. A similar approach was used in Refs. [10, 11, 15] and shown to allow reasonable radar performance. Specifically, it allows to achieve detection performance similar to a PR scheme that exploits a quite good reference signal, despite a limited loss in terms of SNR. However, for it to be effective, we show that additional processing stages are required in order to restore the time/phase/frequency synchronization that is inherently destroyed when using a synthetically reconstructed signal. To this purpose, the authors of Refs. [15–17] have considered the use of the surveillance signal and, assuming that its strongest contribution is provided by the direct signal coming from the transmitter, they proposed to retrieve the required synchronization from the received signal itself. We consider a similar approach and investigate its suitability for the considered scenarios.

In the attempt to further limiting the requirements on the receiver, we also consider a reference-free non-coherent approach where the capability of detecting the presence of a moving target in the observed scene is obtained by observing the amplitude modulation that it induces on the main source signal. This principle of operation that exploits the interference amplitude pattern between the transmitted signal and reflections from the environment, has been widely investigated for non-coherent radar and forward scatter radar (FSR) [18–20] and has been recently proposed and adapted to the application at hand in Refs. [22, 23]. Based on its principle of operation, it does not require accurate time and phase synchronization; however, it suffers from an inherent sign ambiguity in the target velocity measure and it is expected to be effective when extreme bistatic geometries are considered.

The advantages and drawbacks of the two considered reference-free approaches are comparatively investigated by means of application to different experimental datasets accounting for different operative conditions. Specifically, signals of a commercial WiFi AP in either the 2.4 and 5 GHz bands were exploited to detect cooperative human targets and a commercial drone that were observed under moderate or extreme bistatic geometries. The reported results allow to prove the practical effectiveness of the two reference-free approaches and to identify the best suited solution in each operative scenario.

The main contributions of the paper can be summarized as follows:

1) When a passive radar signal processing scheme is adopted based on the use of a known waveform fragment, the time/phase/frequency synchronization issues arising from such reference-free approach are investigated and possible solutions are proposed to mitigate the observed effects in real-world scenarios.
2) When an amplitude-based reference-free approach is adopted, the performance is investigated under different geometries (from moderate bistatic to extreme bistatic) in order to highlight its sensitivity to the target RCS pattern and to reveal limitations and/or potential benefits compared to more complex approaches.
3) The impact of different reference-free approaches on the sensor complexity is discussed and their experimental performance is investigated and compared to the benchmark solution provided by a passive radar operating with an ideal (perfectly known) reference signal.

The reminder of the paper is organised as follows. Section 2 describes the main blocks of the WiFi based PR signal processing scheme and draws some considerations regarding its implementation in practical scenarios. In Section 3, we investigate the advantages and the drawbacks of the use of the PHY Preamble portion and we present a possible strategy to handle the practical limitations of this approach mostly related to the lack of phase and frequency synchronization. Section 4 is dedicated to the description of the alternative reference-free non-coherent approach proposed to further reduce the complexity of the system. Section 5 is devoted to an experimental validation of the considered approaches based on real-world WiFi data collected in two different geometries and employing different targets of opportunity. Finally, our conclusions are drawn in Section 6.

2 | WiFI-BASED PASSIVE RADAR PROCESSING

Let us consider a PR system exploiting the IEEE 802.11 transmissions of a WiFi AP to detect and localise targets. An effective processing scheme developed to serve this task is reported in Figure 1. This was recently proposed and tested by the authors in Ref. [12] as an alternative to the conventional processing architecture [1], with the aim to (i) improve the range sidelobe control capability (ii) make the processing robust to the presence of mixed modulation transmissions (iii) simplify the clutter cancelation stage while guaranteeing an effective removal of the undesired contributions (iv) reduce the overall computational complexity [13].

2.1 | Processing scheme

According to the scheme reported in Figure 1, first, the collected signals undergo a pre-processing stage, where the WiFi packets are extracted from the received data. Specifically, let N_p represent the number of WiFi packets collected in a given coherent processing interval (CPI) and let $N_s^{(p)}$ be the number of samples inside the pth packet ($p = 0,\ldots,N_p\text{-}1$), sampled with sampling frequency f_s. The discrete time version of the surveillance signal collected at the pth packet is denoted as $s^{(p)}[l], l=0,\ldots,N_s^{(p)}-1$ while $r^{(p)}[l]$ represents the reference signal, namely a good copy of the transmitted signal, needed by the receiver to enable an effective passive radar operation. Once the surveillance and reference signal packets are made available, they undergo a range compression stage followed by an interference removal stage.

According to the approach presented in Ref. [12], the range compression is performed with a supervised version of the Reciprocal Filter (RpF).

Let $S^{(p)}[m]$ and $R^{(p)}[m]$ represent the Discrete Fourier Transform (DFT) of the surveillance and reference signals at the p th packet, respectively, that is, $S^{(p)}[m] = DFT\{s^{(p)}[l]\}$ and $R^{(p)}[m] = DFT\{r^{(p)}[l]\}$. The output of the range compression stage and point-like target response provided by the RpF strategy at the pth packet can be evaluated as

$$\chi^{(p)}[l] = IDFT\left\{\frac{S^{(p)}[m]}{R^{(p)}[m]}\cdot rect_{\left\lfloor \frac{B}{f_s}N_s^{(p)}\right\rfloor}[m]\right\} \quad (1)$$

$$\chi_r^{(p)}[l] = IDFT\left\{\frac{R^{(p)}[m]}{R^{(p)}[m]}\cdot rect_{\left\lfloor \frac{B}{f_s}N_s^{(p)}\right\rfloor}[m]\right\} = N_s^{(p)}\eta[l;B] \quad (2)$$

where $\eta[l; B]$ is a digital-sinc shaped function and the application is limited to a useful bandwidth B, for example, $B = 16.6$ MHz for OFDM transmissions, namely forcing the left and right tails of the packet spectrum to be zero. Note that an appropriate weighting function could be introduced at this stage in Equation (2) to control the range sidelobe level [12].

The analyses in Ref. [12] have shown that, along with the well-known advantages of the RpF, the main drawback is a resulting SNR loss that depends on the deep notches that appear in each packet spectrum $R^{(p)}[m]$, resulting in spikes that significantly amplify the noise level, in turn reducing the resulting target SNR, when the spectrum is inverted to build the RpF. Therefore, an effective solution presented in Ref. [12] is to resort to a supervision strategy. Specifically, we use an

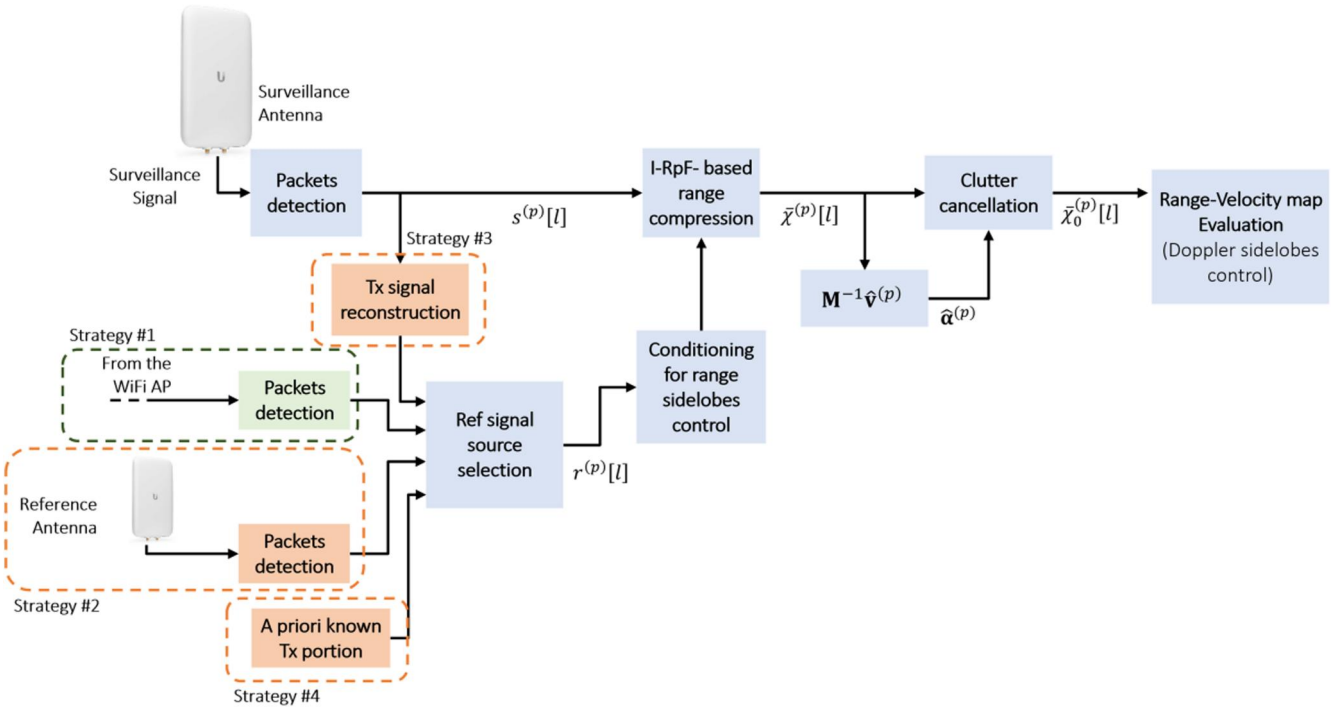


FIGURE 1 WiFi-based passive radar processing scheme.

approach referred to as Interpolated-RpF (I-RpF), based on a thresholding mechanism in the frequency domain.

After the range compression stage has been performed using the RpF approach, the output undergoes the direct signal and clutter cancelation stage. Specifically, according to the approach proposed in Ref. [12] and referred to as ECA-*a priori*, one can leverage the data-independent characteristics of the point-like target response and obtain the clutter cancelled version of range compressed data as

$$\chi_0^{(p)}[l] = \chi^{(p)}[l] - \sum_{k=0}^{K-1} \hat{\alpha}_k^{(p)} \eta[l; B] \tag{3}$$

where K is the cancelation filter length and the disturbance contribution to be subtracted is obtained as a linear combination of known functions $\eta[l; B]$ with coefficients $\hat{\alpha}^{(p)} = \left[\hat{\alpha}_0^{(p)}\ \hat{\alpha}_1^{(p)} \ldots \hat{\alpha}_{K-1}^{(p)}\right]$ evaluated according to a least square approach that minimises the signal power at the output of cancelation filter. For the sake of brevity, we refer the interested reader to Ref. [12] for further details on these techniques.

2.2 | Considerations on the practical implementation and experimental data description

As aforementioned, the described approach is a reference signal-based processing scheme. In fact, a good copy of the transmitted signal is assumed to be available at the receiver and used throughout the processing. In practical implementations, this can be obtained according to different strategies as illustrated in Figure 1 and detailed below:

- In a cooperative scenario, namely when the transmitter is accessible, the reference signal can be directly extracted by means of a wired link, using a directional coupler inserted between the AP and its antenna. This solution is reported in Figure 1 as Strategy #1 and provides a very good copy of the transmitted signal to be used at the receiver.
- The reference signal can be obtained using a dedicated antenna steered towards the AP. This strategy, referred to as Strategy #2, also requires a dedicated receiving channel but exploits a wireless link between the AP and the receiver. That simplifies the practical implementation; however the collected signal could be affected by disturbance other than thermal noise, for example, multipath reflections.
- The reference signal can be obtained by demodulating and re-modulating the received signal packet according to the employed IEEE 802.11 Standard. If the surveillance signal is exploited for this purpose, this strategy, referred to as Strategy #3, requires only one receiving channel, but it needs additional processing efforts and might be subject to reconstruction errors.

Strategies #1-#3 have been extensively tested in the technical literature against both simulated and experimental data showing remarkable performance. However all of these solutions are characterised by a non-negligible implementation complexity since they either require a dedicated receiving channel and additional infrastructure or additional computational complexity, which run against the requirements of low implementation cost and compact system size for these sensors.

Therefore, in this paper, we investigate the possibility for the described PR scheme to operate in a reference-free condition. However, we consider the above implementations as a benchmark for the performance evaluation of the lower cost solutions proposed in the following. To this purpose, we refer to Strategy #1 as it provides the best version of the reference signal at the price of a wired connection to be deployed.

The performance comparison reported in this paper is based on two different experimental datasets that have been collected in different configurations and with different targets. They are briefly described below.

2.2.1 | Dataset A: human surveillance at 2.4 GHz

A dedicated acquisition campaign, carried out in a private outdoor location, shown in Figure 2(a). A commercial wireless AP (TP-Link Archer VR600 AC1600) was exploited as source of opportunity and connected to a transmitting directive antenna (TP-link TL-ANT2409 A).

The AP was configured to transmit signals according to the IEEE 802.11n standard in channel 13 of the WiFi band (f_0 = 2.472 GHz). Accordingly, all packets except beacons use OFDM modulation scheme. A four-channel National Instrument USRP-2955 receiving system was employed and connected to three surveillance antennas, steered towards the monitored area. The sampling frequency on receive was set to be equal to the WiFi channel bandwidth of 20 MHz. In this paper, we use the data from the right-hand antenna in Figure 2(a) and the reference signal that was directly collected from the AP (Strategy #1).

In different tests, one or two people were used as cooperative targets, moving in the scene at different velocities along straight lines departing from the receiver location (see Figure 2(b)). In Figure 2(c) a top view of the acquisition campaign site is reported.

2.2.2 | Dataset B: Drone surveillance at 5 GHz

A different dataset has been collected in the same location described above, aimed at detecting small drones using WiFi signals in the 5 GHz band (see Figure 3(a)). The same TP-Link Archer VR600 AC1600 wireless AP was employed as IO and connected to a transmitting directive antenna (Ubiquiti UMA-D). The WiFi AP was configured to transmit according to the IEEE 802.11ac standard in channel 36 of the WiFi band (f_0 = 5.18 GHz). Seven Ubiquiti UMA-D surveillance antennas were employed and steered towards the monitored area,

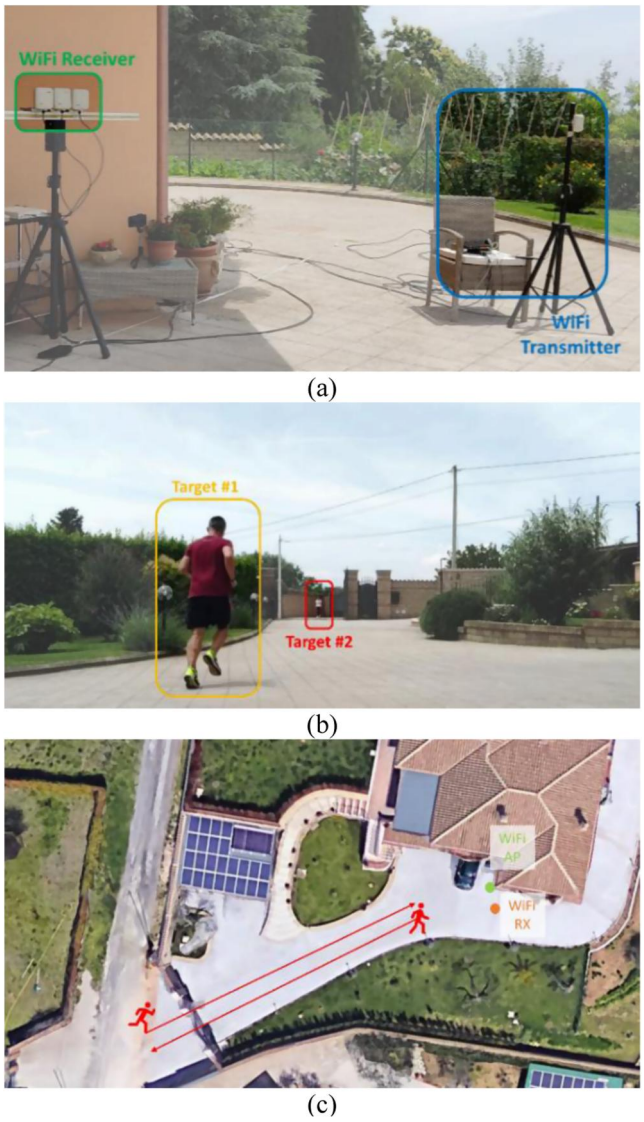


FIGURE 2 Dataset A (a) acquisition geometry (b) cooperative targets (c) top view of the acquisition site.

connected to the USRP-2955 receiving system that provided the 20 MHz sampled version of the collected signals. In this work, we extract the data from the left-hand antenna shown in Figure 3(a). In this case, the exploited geometry is characterised by wide bistatic angles, as shown in Figure 3(a,b) and a small drone (DJI Mavic Pro, shown in Figure 3(a)) was piloted to behave as a cooperative target moving in the scenario, along directions orthogonal to the transmitter-receiver baseline.

3 | REFERENCE-FREE WIFI-BASED PR PROCESSING

Aiming at a reference-free implementation of the PR processing, a possible solution is offered by the structure of any WiFi packet. As is well known, in every WiFi packet three main fields can be identified, namely the PHY Preamble, the Signal containing information on the transmission mode for the payload, and the DATA that encloses the transmitted information. Specifically, the PHY Preamble portion is an invariant and data-independent portion, which is a priori defined based on the employed 802.11 standard and is used for synchronization and channel estimation [21]. As an example, in OFDM modulated packets the PHY preamble is composed by 12 consecutive OFDM symbols.

By exploiting this structure, a way to make a reference signal available without requiring any dedicated receiving channel or reconstruction processing stages is to employ a synthetic PHY Preamble, built as specified by the employed IEEE 802.11 standard. Accordingly, the processing will be limited to the corresponding signal portion. This strategy is referred to as Strategy #4 in Figure 1 and was preliminary considered in Ref. [15].

It is intuitive that this strategy has two main limitations, separately addressed in the following subsections: (i) by limiting the processing to a small portion of the signals, a reduced coherent integration gain must be accepted and (ii) the use of a synthetically built signal inherently implies the lack of synchronization with the collected surveillance signal in both delay, phase and frequency.

3.1 | SNR loss

When the processing is limited only to the preamble portion, composed by $N_{PHY\text{-}PREAMBLE}$ samples, a SNR loss must be accepted due to the corresponding reduction in the coherent integration gain. This loss is measured with respect to the full integration across the $N_p^{(i)}$ packets available for the ith CPI and is evaluated as:

$$L^{(i)} = \frac{N_p^{(i)} N_{PHY-PREAMBLE}}{\sum_{p=p_0^{(i)}}^{p_0^{(i)}+N_p^{(i)}-1} N_s^{(p)}} \tag{4}$$

where $p_0^{(i)}$ is the first packet of the ith CPI. In this paper we consider only the Legacy Preamble portion, composed by the Short Training Field and the Long Training Field each with a duration of eight μs [21].

In order to provide a realistic estimation of the expected SNR loss, we consider the experimental Dataset A described in section 2.2 and we report in Figure 4 the measured loss $L^{(i)}$ over an acquisition time of 10 s. It is estimated in a sliding fashion across partially overlapped CPIs of 0.3s each and using $N_{PHY\text{-}PREAMBLE}$=(8 μs+8 μs)×20 MHz = 320 samples.

We observe that the SNR loss is of approx. 10–11 dB along the entire acquisition. This loss cannot be neglected when dealing with long range surveillance applications.

However, it is worth noticing that, very short-range applications such as indoor surveillance are usually clutter-limited rather than noise-limited, therefore even a high SNR loss might not represent a severe issue.

Moreover, the considered scenario can be regarded as a worst-case condition since: (i) it refers to a high rate transmission, including very long data packets; (ii) it is assumed that

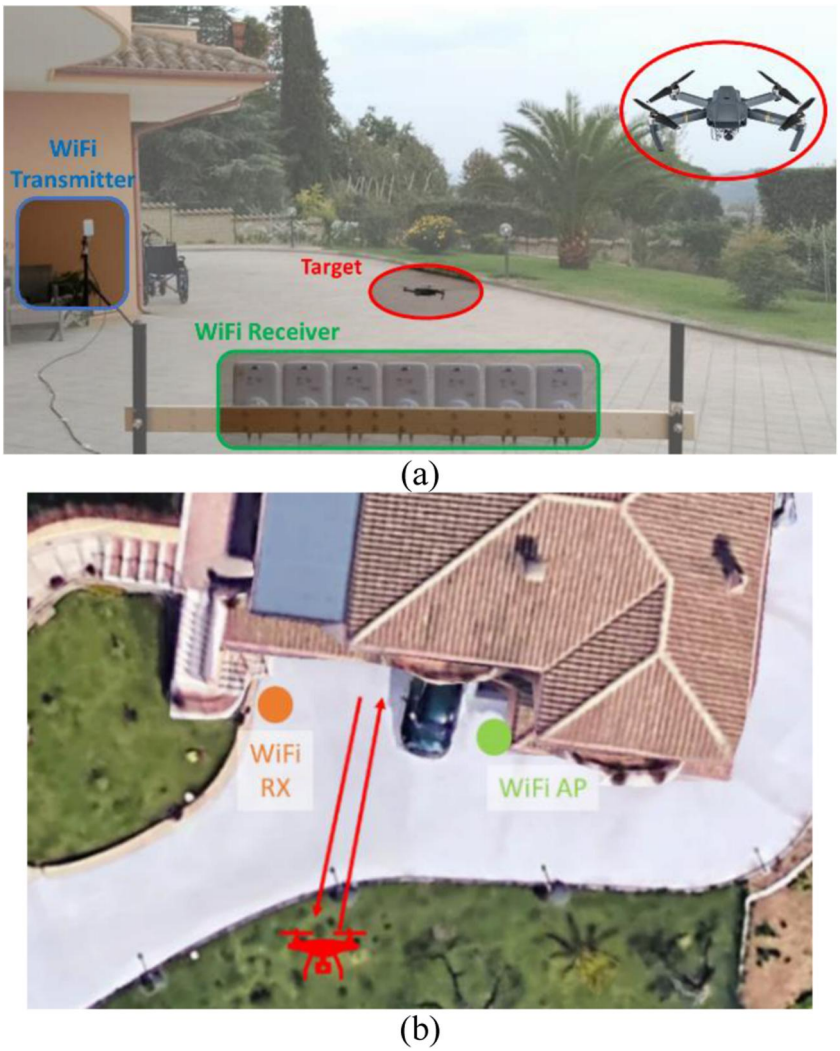


FIGURE 3 Dataset B (a) acquisition geometry and target (b) top view of the acquisition site and trajectory.

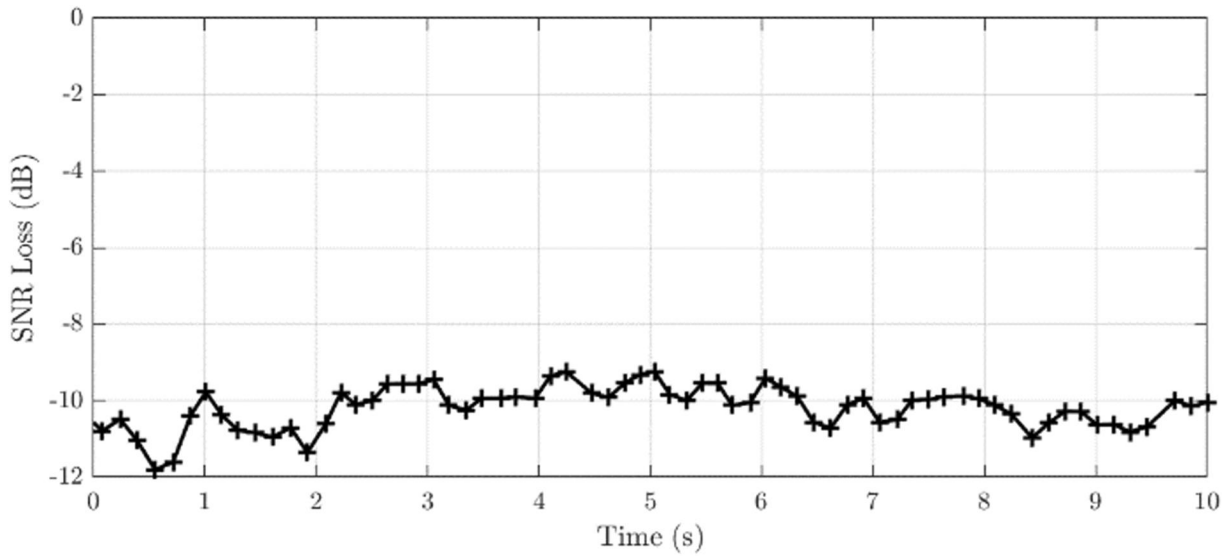


FIGURE 4 SNR loss versus acquisition time for CPI = 0.3s.

a perfect copy of the transmitted signal is available, which might not be the case even when operating with Strategy #1; in other words, the loss due to the use of the a priori known Preamble only should be compared to the case of using an entire packet possibly affected by noise; (iii) if the packet duration changes substantially across consecutive PPDUs, the induced amplitude modulation might result in higher Doppler sidelobes, whose effective control is obtained by means of tapering function which inherently imply a degraded SNR.

For all these reasons, the expected SNR loss for the proposed reference-free Strategy #4 might be smaller than that observed in Figure 4.

3.2 | Synchronization issues

In conventional PR systems, where the reference signal is collected through a dedicated channel (Strategies #1 and #2), a phase-locked multichannel receiver is usually employed. This solution provides a useful time reference to measure the relative delays of echoes in the surveillance signal; in addition, this approach mitigates the frequency drift which is present in the received signals since this is partially compensated for in the cross-correlation stage.

These characteristics are not available if, instead of having a dedicated reference channel, we employ a synthetic signal (as in Strategy #4) which would therefore lack of synchronization with the surveillance signal. To describe this issue, let us write the surveillance signal collected at the pth packet as follows

$$s^{(p)}[l] = a_{0,s}x^{(p)}[l] + a_T x^{(p)}[l - l_T]e^{j2\pi f_{D,T}\left(\frac{l}{f_s}+T^{(p)}\right)} + d_s^{(p)}[l] \tag{5}$$

where $x^{(p)}[l]$ is the transmitted signal; $a_{0,s}$ and a_T are the amplitudes of the direct signal and the target echo, respectively; l_T and $f_{D,T}$ denote the target delay and the Doppler shift induced by the target motion; $T^{(p)}$ is the time instant where the pth packet starts, measured with respect to the beginning of the acquisition and $d_s^{(p)}[l]$ accounts for the disturbance in the surveillance channel, composed by thermal noise, multipath contributions etc. Similarly, the reference signal is

$$r^{(p)}[l] = \left\{a_{0,r}x^{(p)}[l + l_r[p]] + d_r^{(p)}[l]\right\}e^{j\varphi^{(p)}[l]} \tag{6}$$

where the transmitted signal appears with a delay $l_r\,[p]$ and an amplitude $a_{0,r}$ and $d_r^{(p)}[l]$ denotes the disturbance in the reference channel. Finally, $\varphi^{(p)}[l]$ represents the phase difference measured with respect to the surveillance signal.

If both the reference and surveillance signals are collected by a phase-locked multichannel receiver (Strategies #1 and #2), we can assume that the phase difference is negligible, that is, $\varphi^{(p)}[l] \cong 0$. Moreover, the peak of the point-like target response is affected by a constant delay across packets, that is, $l_r\,[p] = l_r$, caused by the different path lengths, for example, introduced by the employed cables. This constant delay can be easily compensated for; therefore, for simplicity, we assume $l_r = 0$.

If a synthetic reference signal is employed (Strategy #4), we can assume $d_r^{(p)}[l]=0$; however, the delay $l_r\,[p]$ might change with the packet and the phase drift $\varphi^{(p)}[l]$ can no longer be neglected. For instance, if the latter only depends on a carrier frequency drift Δf_c, we have

$$\varphi^{(p)}[l] \simeq \Delta f_c\left(\frac{l}{f_s} + T^{(p)}\right) \tag{7}$$

Therefore, when Strategy #4 is used, an appropriate solution to compensate for the delay and phase drift must be sought.

3.3 | Direct-signal based synchronization

If the direct signal represents the main contribution in the surveillance signal ($a_{0,s} \gg a_T$), a possible solution is to estimate the delay $l_r\,[p]$ and phase drift $\varphi^{(p)}[l]$ from the surveillance signal itself and use them for the compensation.

First, we estimate the delay $l_r\,[p]$ from the range compressed version of the input signal $\chi^{(p)}[l]$, as

$$\hat{l}_r[p] = \left\{\left|\chi^{(p)}[l]\right|\right\} \tag{8}$$

Then, once $\hat{l}_r[p]$ is available, $\chi^{(p)}[l]$ is modified as follows

$$\chi'^{(p)}[l] = \chi^{(p)}\left[l - \hat{l}_r[p]\right] \tag{9}$$

By extracting the output of Equation (9) at the first range bin where the direct signal contribution is now located, that is, $\chi'^{(p)}[0]$, its phase drift can be retrieved as

$$\hat{\varphi}[p] = arg\left\{\chi'^{(p)}[0]\right\} \tag{10}$$

Note that we are neglecting the phase drift variation within the single packet, namely we assume $\varphi^{(p)}[l] \cong \varphi^{(p)}$, which is a reasonable choice given the duration of the employed preamble. Once $\hat{\varphi}[p]$ is available, $\chi'^{(p)}[l]$ changes as follows

$$\chi''^{(p)}[l] = \chi'^{(p)}[l]e^{-j\hat{\varphi}[p]} \tag{11}$$

At this stage, $\chi''^{(p)}[l]$ is fed into the subsequent processing stages, as described in Section 2. Based on the above description, we observe that the proposed synchronization approach exploits the direct signal contribution in the surveillance signal without the need to demodulate the received signal, as per Strategy #3. Moreover, it is expected that this strategy is effective also when the dominant contribution in the surveillance signal is represented by a multipath ray.

Figure 5 reports the range-compressed version of the input signal, for three consecutive packets extracted from Dataset A. Specifically, Figure 5(a) shows the results obtained when the

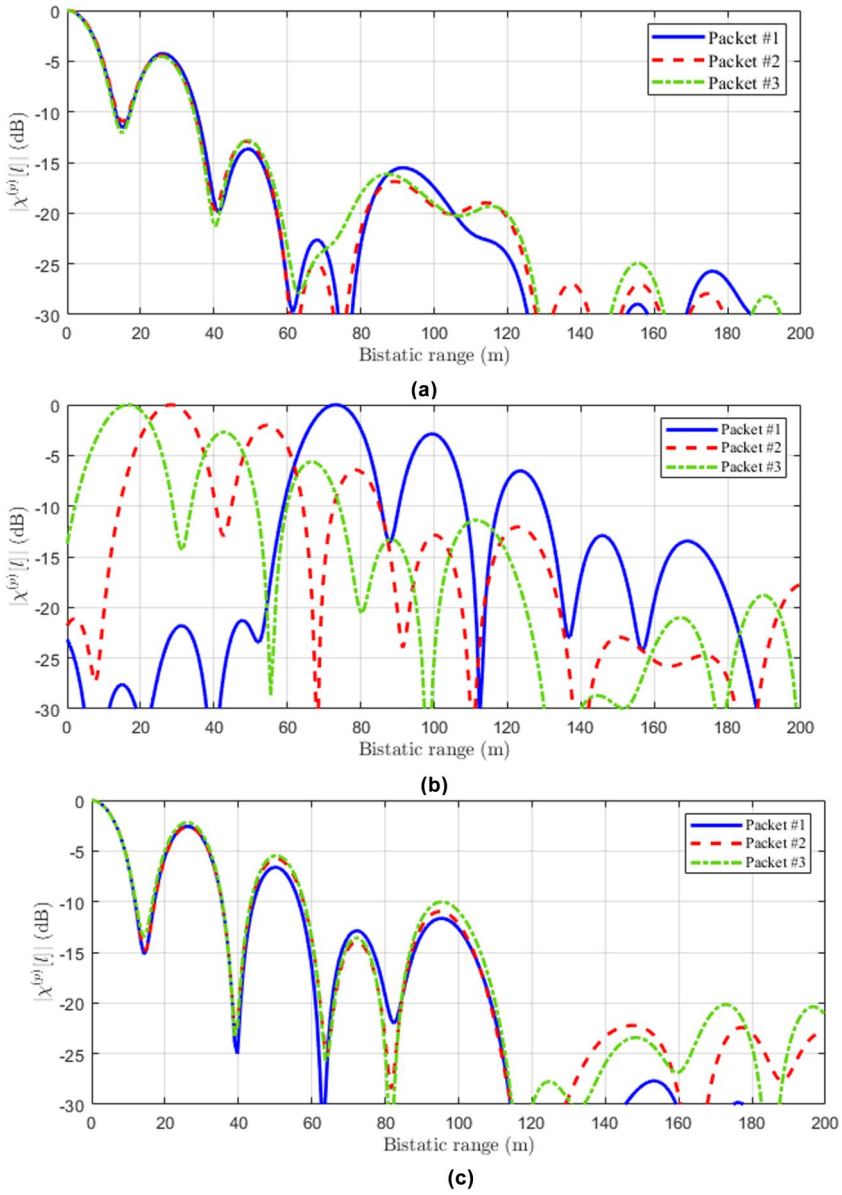


FIGURE 5 Range-compressed version of the surveillance signal for three subsequent packets, using (a) Strategy #1, (b) Strategy #4, (c) Strategy #4 with delay compensation.

reference signal is recorded (Strategy #1) while Figure 5(b) is obtained when the PHY Preamble is employed (Strategy #4) and the lack of time is not addressed, namely $|\chi^{(p)}[l]|$. Comparing these two sub-figures, it is evident that when a phase-locked multichannel receiver is employed to collect both the reference and surveillance signals, the peak is steadily found in the first range bin for all packets.

In contrast, when Strategy #4 is considered to make the reference signal available, the cross-correlation peak wanders from one packet to another in the range domain. Finally, when Strategy #4 is employed and the delay compensation is applied as described in Equations (8) and (9) (see Figure 5(c)), the peak of $\left|\chi'^{(p)}[l]\right|$ is correctly reported in the first range bin for all the considered packets. Note, however, that the cross-correlations in Figure 5(c) slightly differ from those in Figure 5(a); this is mostly due to the mismatch between the synthetic reference signal and the actual direct signal, the latter being modified by the transmitter/receiver hardware (filters, antennas, etc.).

In Figure 6, we report the phase law extracted at the peak location from the time-synchronized cross-correlations, measured across 1500 consecutive packets (a total duration of approx. 1.2 s). As expected, by extracting the phase law from $\chi^{(p)}[l]$ obtained with Strategy #1 (blue line), the measured phase difference is approximately zero across the observed time interval. In contrast, the phase law extracted as in Equation (10) from the first range bin of $\chi'^{(p)}[l]$ shows a large phase drift with a dominant linear component, which accounts for a carrier frequency offset between the received signal and the synthetic one. This clearly demonstrates the need for a phase synchronization stage also.

In Figure 7, we compare the range-velocity maps obtained for a CPI of 0.3 s extracted from Dataset A, during which 716 OFDM packets are collected.

The data file considered was collected for a test where two human targets were present moving as in Figure 2(a). Specifically, target #1 (yellow box) was running away from the

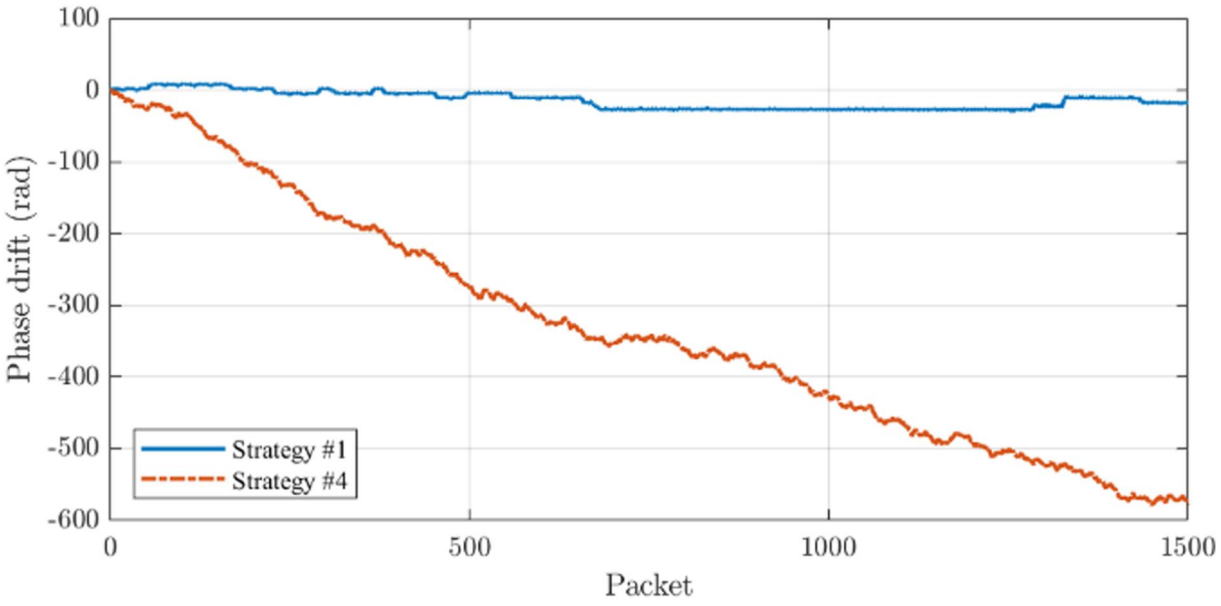


FIGURE 6 phase law $\hat{\varphi}[p]$ estimated with Strategies #1 and #4.

transmitter-receiver (Tx-Rx) pair, while target #2 (red box) was walking towards the receiver.

First of all we look at the results obtained in the absence of a clutter cancelation stage with the aim of understanding the impact of the proposed approach on the direct signal. Specifically, Figure 7(a),(b) are obtained with Strategy #1, while for Figure 7(c),(d) Strategy #4 is employed, respectively avoiding or applying the phase drift and delay compensation. Note that in Figure 7(a), the packet lengths are preserved while in Figure 7(b) all packets are limited to the preamble length to enable a fair comparison with the solutions in Figure 7(c-d).

From Figure 7 we observe that:

- Comparing Figure 7(a) and 7(b), we observe a SNR loss of approximately 5dB. Note that this value is lower than what expected from Figure 4, due to the motivations previously described. Also, from Figure 7(a), we note that the large fluctuations of the PPDU length within the CPI results in high sidelobe level in the Doppler domain.
- When Strategy #4 is employed without compensating for the lack of synchronization (Figure 7(c)), a defocused range-velocity map is obtained.
- When Strategy #4 is employed and the phase drift and delay compensation is applied (Figure 7(d)), the direct signal contribution is effectively focused at zero Doppler and lies in the first range bin. However, an SNR loss of approx. 1dB is experienced with respect to Figure 7(b).

The analyses above have shown that, in the considered scenario, the proposed approach is effective against the strong stationary contributions in the map, above all the direct signal which is inherently exploited for the synchronization stage.

In order to understand the impact of Strategy #4 on the useful target echoes, we report in Figure 8 the results after clutter cancelation. The latter is applied in a sliding fashion, with a time interval of 0.05s for the estimation of the cancelation filter coefficients and an update rate corresponding to the packet rate. It is important to note that the clutter cancelation stage is operated over a range extent of 250m in order to have robust results against fractional delays of the clutter echoes. Specifically, Figure 8(a) reports the range-velocity map obtained for Strategy #1 when limited to the preamble only, while Figure 8(b) is obtained with Strategy #4 after synchronization.

All figures have been obtained after applying a hamming tapering function to control the sidelobes level in the range domain and an ad hoc tapering window in the velocity domain which allows to mitigate the sidelobes arising from a non-uniform packet emission rate [24].

In Figure 8 we observe (i) a slightly different SNR for both targets, with a loss lower than 1 dB obtained for the PHY Preamble based solution and (ii) an overall higher disturbance background level on the map. As mentioned above, this is mainly due to a mismatch between the synthetic reference signal and the direct signal. However, in a clutter-limited scenario, as the one considered in this acquisition, the targets are still easily discriminated against the background. This is clearly apparent in Figure 9 where we reported the detection results obtained after the application of a conventional cell-average constant false alarm rate (CA-CFAR) detection scheme to the maps of Figure 8 and setting the threshold in order to guarantee a false alarm probability $P_{\text{fa}} = 10^{-6}$.

The reported results preliminary demonstrate the effectiveness of the proposed approach to implement a short-range passive surveillance system based on WiFi transmissions and equipped with a single receiving channel. We recall that this result is obtained under the assumption that the direct signal contribution represents the strongest contribution in the

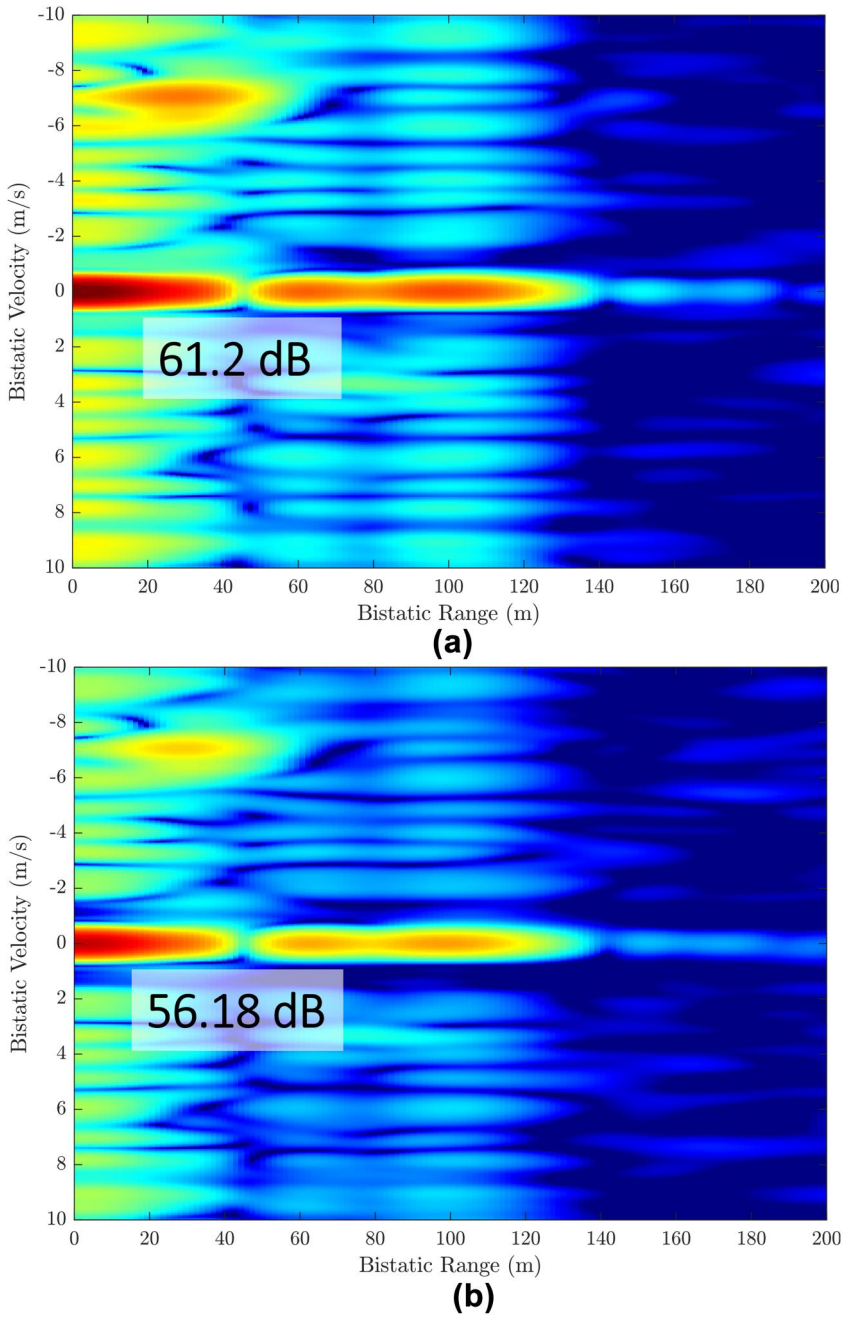


FIGURE 7 Range-velocity map for (a) Strategy #1 with preserved packets length (b) Strategy #1 limited to the PHY Preamble, (c) Strategy #4, (d) Strategy #4 with phase and delay compensation.

collected signal, which is a typical condition in many practical scenarios. However, in order to thoroughly assess its practical performance, extensive validation will be reported in the following on both collected datasets, namely with different bistatic geometries and using different targets of opportunity.

Moreover, in the attempt to further reducing the complexity of the system and complete the analysis, we introduce in the next section an alternative and even simplified processing scheme, presented in Ref. [22], which will represent the lowest cost solution to be employed in the subsequent experimental validation.

4 | AMPLITUDE-BASED REFERENCE-FREE APPROACH

In this section, we describe an alternative and simplified reference-free approach, proposed by the authors in Refs. [22, 23] and referred to as Interference Doppler Processing (IDP). Figure 10 reports the main blocks of the proposed processing scheme, which aims at recognising the presence of a target by observing the amplitude modulation that its motion induces on the main source signal, that is, the direct signal. The principle

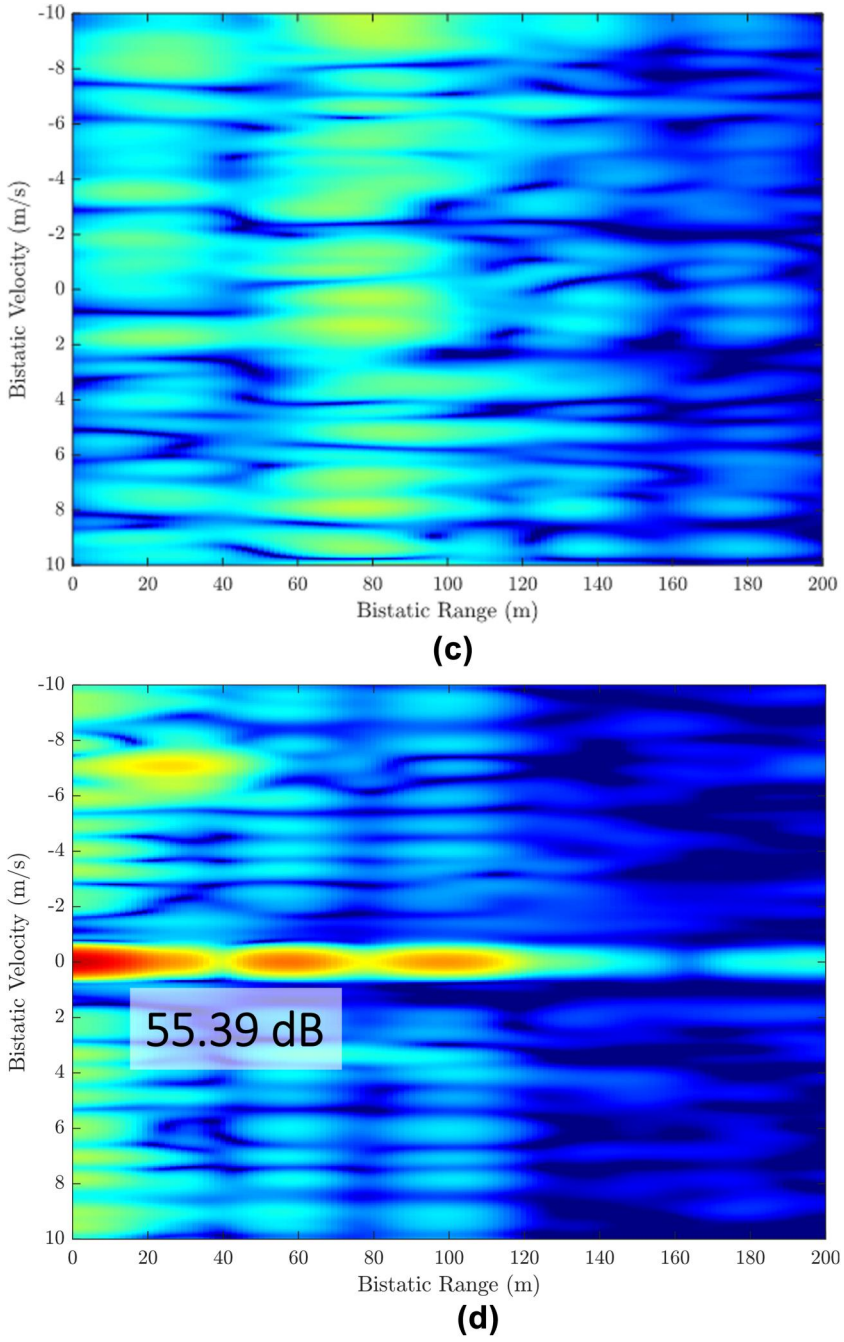


FIGURE 7 (Continued)

of operation of the IDP solution has been widely investigated for non-coherent radar and FSR systems [18–20].

First, the packet energy is extracted, namely the square modulus of the signal is evaluated, followed by an energy detector at packet level, over a portion of N samples

$$z[p] = \sum_{l=0}^{N-1} \left| s^{(p)}[l] \right|^2 \tag{12}$$

Notice that, despite consecutive packets might be of different length, this operation is applied over portions of fixed length N in order to avoid the inherent amplitude modulation due to the variable length of WiFi packets [22].

The obtained sequence undergoes the DC removal stage aimed at removing the strongest stationary scene interferences, such as the direct signal transmitted by the AP:

$$\underline{z}[p] = z[p] - z_{DC}[p] \tag{13}$$

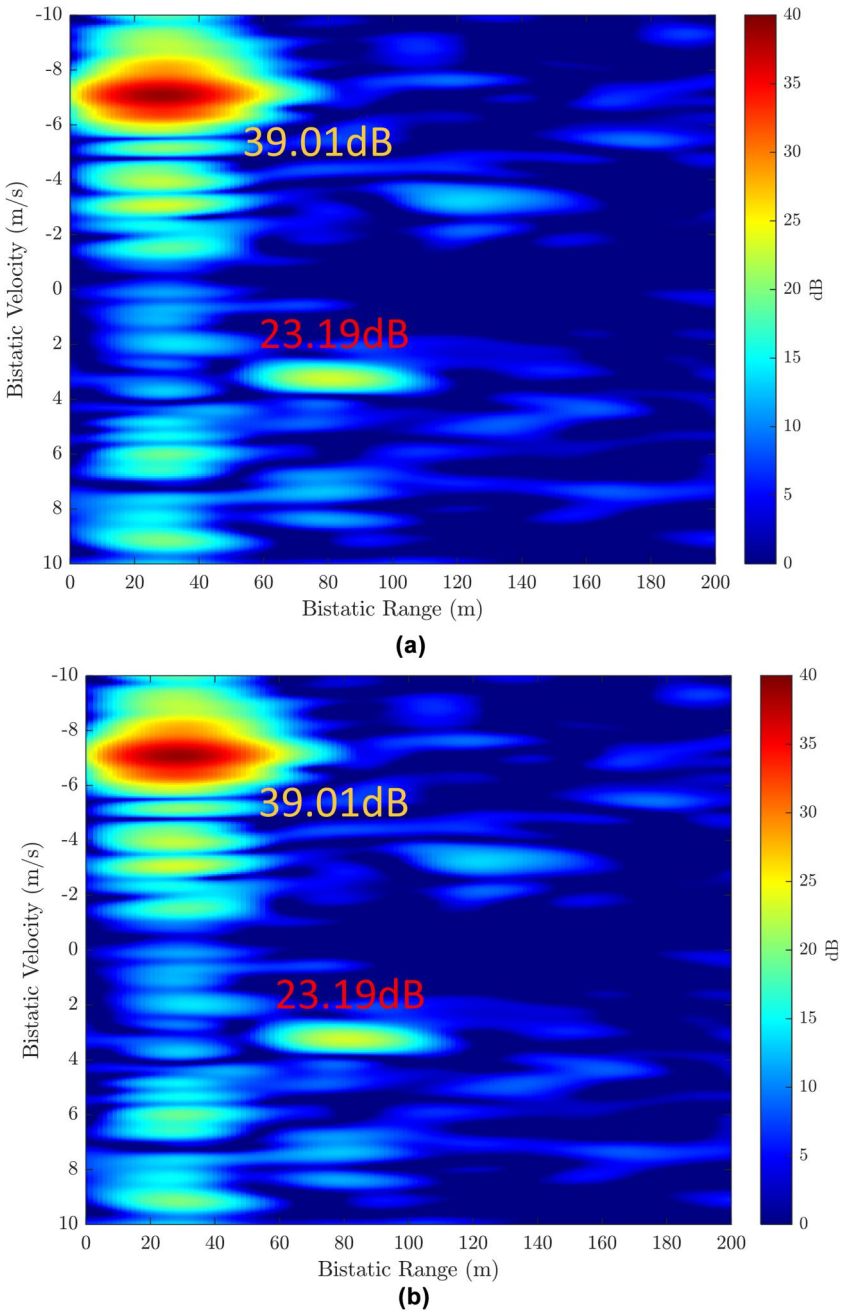


FIGURE 8 Range-velocity map after clutter cancelation for (a) Strategy #1 limited to the PHY Preamble. (b) Strategy #4 with phase-delay compensation.

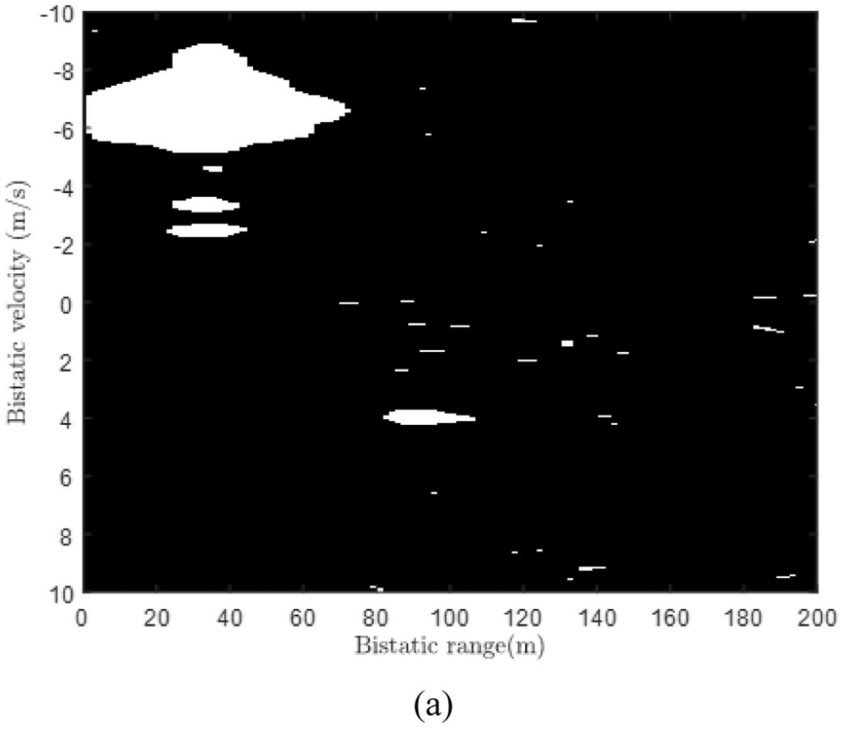
where $z_{DC}[p]$ denotes the average value of $z[p]$, evaluated over an appropriate time window T_{DC}. This stage does not allow to completely remove the interference caused by the intrinsic amplitude modulation of the waveform itself when OFDM modulation schemes are adopted. Such residual interference might yield a high disturbance background in the final output which limits the target discrimination capability [20, 22].

Finally, $\underline{z}[p]$ undergoes a time-frequency analysis, which results in a spectrogram where the target Doppler signature is detected. Note that, if the packet emission rate is constant over time, this stage can be implemented with a Short Time Fourier Transform (STFT) against partially overlapped batches of T_{STFT} seconds each, thus encompassing N_p packets:

$$w[m] = \sum_{p=0}^{N_p-1} h[p]\, \underline{z}[p_0 + p] e^{-j2\pi \frac{mp}{N_p}} \tag{14}$$

where p_0 is the first packet of the current batch and $h[p]$ is a weighting function, used to control the Doppler sidelobes level. Otherwise, one can resort to an appropriate interpolation stage, which basically yields a resampled version of the sequence $\underline{z}[p]$ before proceeding with the FFT, or a nonuniform discrete Fourier transform at each batch can be adopted.

The IDP approach has been extensively investigated in Ref. [22] by means of theoretical, simulated and experimental analyses. It proved to be a feasible solution for a low-cost sensing



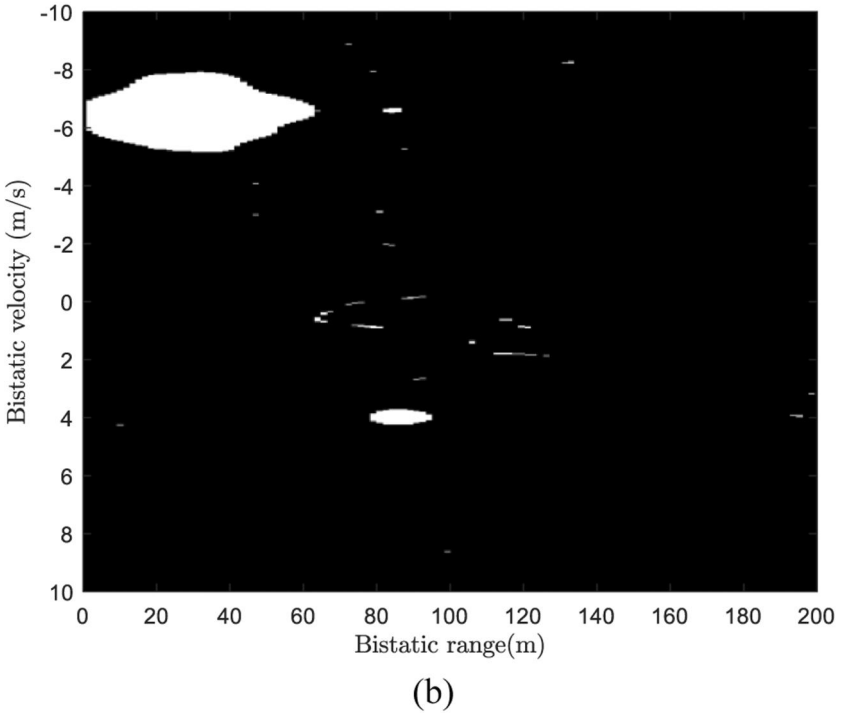


FIGURE 9 Detection results after a CA-CFAR scheme operating with $P_{fa} = 10^{-6}$ on the Range-velocity map obtained for (a) Strategy #1 limited to the PHY Preamble. (b) Strategy #4 with phase-delay compensation.

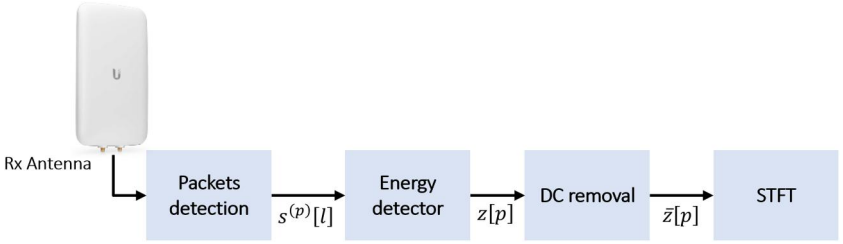


FIGURE 10 Processing blocks of the interference doppler processing scheme.

in short range applications since it allows the detection of moving objects without setting strong requirements in terms of time and frequency synchronization. Basically, a rough time synchronization is needed since the sensor does not measure time difference of arrival (namely ranges) but only allows to extract the target Doppler signature. Moreover, it does not require the receiver to be phase-synchronized with the transmitter of opportunity and this largely simplifies its stand-alone deployment and operation.

Nevertheless, the reduced complexity is paid in terms of inherent limitations set by the IDP principle and, more in general, of the FSR [18–20, 22, 23]. First of all, it yields a symmetric output spectrogram so that only the modulus of the target instantaneous Doppler can be inferred. Moreover, it relies on a reasonable stability of the amplitude of the target return that is typically guaranteed under extreme bistatic geometries while it might be weaker in quasi-monostatic configurations. Finally, since the amplitude modulation of the received signal is due to the constructive/destructive superposition of the direct signal and the target echo, the effect is evident when such contributions arrive at the receiver with comparable delays whereas it fades when the target gets farther [20].

In the following, this approach will be compared with the previously described strategies against real WiFi data, with the aim of identifying the most suited reference-free strategy based on the intended application.

5 | EXPERIMENTAL PERFORMANCE COMPARISON

In this section the effectiveness of different techniques is tested against the two datasets described in Section 2.2 which account for different geometries employing different cooperative targets.

5.1 | Results against human target (dataset A)

In this section we consider an experimental test from Dataset A where only one person is present in the scenario of Figure 2 acting as a cooperative target walking away from the Tx-Rx pair. The total acquisition time is 25 s during which 29,876 packets have been recognized, each characterised by QPSK coded data-fields, with an average packet transmission rate of 1195 packets/s.

Figure 11 shows the results obtained with the three different approaches considered in the paper: (a) PR based on Strategy #1, namely assuming the availability of a good copy of the reference signal extracted through a wired link from the AP, (b) PR based on Strategy #4, namely using an a priori known portion of the transmitted signal a s a reference, (c) IDP approach. Figure 11(a),(b) have been obtained after applying an hamming tapering function in the range domain and an ad hoc weighting function in the velocity domain [24], while Figure 11(c) features an hamming tapering window in the velocity domain.

For a direct comparison between the three different techniques, we use a Doppler-time representation for the outputs. The spectrograms are obtained with a spacing of 0.05s between consecutive CPIs of 0.2s each. For the PR solutions, the output for each CPI is evaluated at the range cell where the target belongs to. All WiFi packets have been cut to a common length of 550 samples, for PR based on Strategy #1 and for the IDP approach. Clearly the PR with Strategy #4 only exploits the Preambles. The cancellation filter coefficients are evaluated with a time interval of 0.1 s for both the PR approaches, when implementing the ECA algorithm, and the IDP, at the DC removal stage. Finally, all the spectrograms are scaled to the average background level in order to directly compare the target discrimination capability achieved with different approaches against the residual interference.

From the achieved results we observe that:

- Using a PR approach with strategy #1 (Figure 11(a)) limited to the PHY preamble portion, the target signature can be distinguished throughout the entire acquisition, from the start of the target's motion until it comes to a stop. In this case, the highest Signal-to-Background-Ratio (SBR) is experienced, partially thanks to the higher number of samples integrated, compared to strategy #4 (Figure 11(b)), which is limited to the sole preamble samples, namely 320 samples. In addition, the PR processing has the capability to detect the target signature

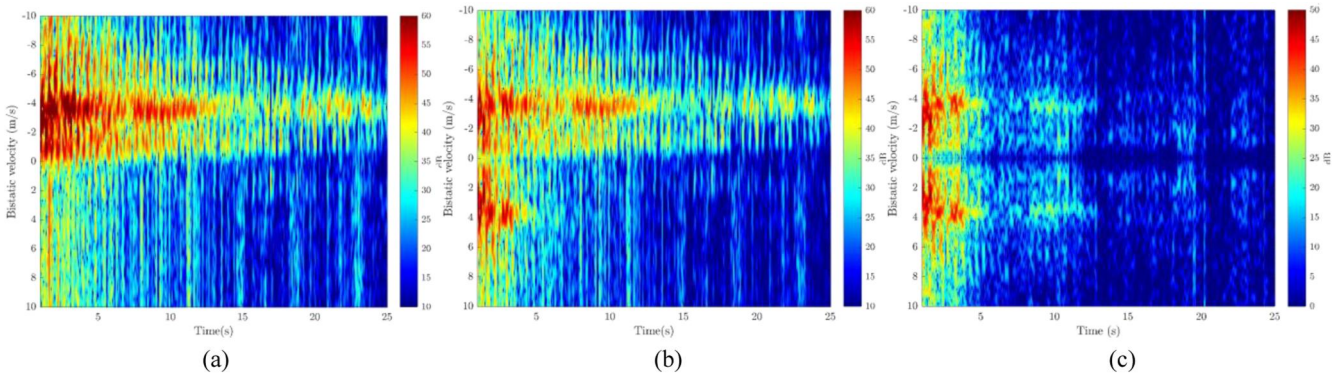


FIGURE 11 Bistatic velocity-time map for (a) PR with Strategy #1, (b) PR with Strategy #4 and phase-delay compensation, (c) IDP.

across multiple range cells, allowing the target to be tracked as it moves from one range bin to another. As a result, this strategy has the potential to cover a wide area and distinguish between multiple targets based on their range and Doppler information. Additionally, the spectrogram is characterised by the micro-Doppler effect arising from the moving arms and legs of the target, which can be clearly discriminated from the background. This is shown in Figure 12(a) where we report an enlarged view of Figure 11(a) over a time interval of 3 s and suggests that a classification of the target activity could, in principle, be achieved.

- PR with Strategy #4 (Figure 11(b)) provides a similar output as the one obtained for Strategy #1, where the target signature is detectable across the whole spectrogram. However, note that there is a Doppler ambiguity in the time interval between 0 and 5 s, when the target is in the first range cell. It can be explained by observing that under this condition, the assumption that the direct signal represents the strongest contribution in the received signal does not hold anymore, at least for the phase estimation stage in Equation (10), and the target returns heavily affect the phase synchronization. In fact, using the simple approach described in section 3.3, the system compensates for the global signal phase due to the superposition of the direct signal and target echo so that it basically computes the amplitude of the received signal yielding a similar ambiguity as for the IDP approach. However, as the target moves away from the Tx-Rx pair, that is, it gradually migrates to farther range bins, the influence of the target echo decreases, hence an effective phase-delay compensation can be carried out. In such condition, the PR based on Strategy #4 yields performance that are largely comparable to the reference-based PR approach (#Strategy 1), as can be seen in Figure 11(b) after 5s. Additionally, Figure 12(b) shows that the micro-Doppler signature is preserved when a synthetic reference signal is exploited despite the lower SNR due to the shorter packet length limited to the Preamble portion.
- When the IDP is employed (Figure 11(c)), the target signature is folded around the zero Doppler. This happens, as previously stated, because the STFT is applied over a real valued signal. Additionally, the effectiveness of the IDP is limited to the echoes arising from the first range cells, which results in a rapid performance degradation as the target moves away from the Tx-Rx pair. In fact, we note that after 5 s, the target signature is largely attenuated as it is mostly due to the sidelobes arising from the second range cell. After 12 s the target signature is completely buried below the background since the target is observed in a quasi-monostatic configuration and it belongs to the third or fourth range cell so that the IDP is only capable of detecting its far sidelobes thus suffering from a severe fading. In this issue, Ref. [20] is addressed and a subband approach is presented to enhance the probability to detect the returns from farther ranges. Despite the decreased performance, it is worth recalling that, compared to the PR approach, the IDP architecture is characterised by a much lower complexity that makes it a practical solution for very short-range applications.

5.2 | Results against drone (dataset B)

Figure 13 reports the output of the three considered approaches for a test from Dataset B. The spectrograms are obtained with a spacing of 0.05s between consecutive CPIs of 0.3s each. The cancelation filter coefficients are evaluated with a time interval of 0.2s for both the PR approaches and the IDP. The WiFi packet have been cut to a common length as in Figure 11. Note that, in this case, the target, a cooperative drone, was observed under extreme bistatic angles and remains in the first range cell throughout the entire acquisition (see Figure 3). The results reported in Figure 13 show that:

- As for Dataset A, the spectrogram obtained when a PR processing scheme is adopted with strategy #1 (Figure 13(a)) shows the best performance, meaning that the target signature shows the highest SBR, thanks to the availability of a good copy of the transmitted signal which allows effective coherent integration within and across entire WiFi packets. Also, the target Doppler signature can be measured unambiguously thanks to the accurate phase synchronization guaranteed with this approach.
- When Strategy #4 is adopted for PR (Figure 13(b)), the target signature appears folded around the zero Doppler for the entire acquisition. This is due to the persistence of the target in the first range cell, which severely affect the phase-delay compensation technique needed to exploit a synthetic reference signal. Consequently, in this regard, similar results are obtained as for the IDP (Figure 13(c)), but with a larger sensor complexity. Additionally, due to the poor phase synchronization accuracy, the target signature is affected by an additional SBR loss compared to the result obtained with Strategy #1 (Figure 13(a)). The low SBR and the incapability of measuring the relative velocity of the target, make this approach the least appealing for this type of scenarios, where the IDP could provide a similar result, with a better SBR, by leveraging simpler hardware.
- When the IDP is employed (Figure 13(c)) the target signature can be discriminated for the entire acquisition, thanks to the persistence of the target in the first range cell, in contrast with the previous dataset where the target signature quickly faded as the target moved away from the first range cell. Apparently, this setup represents the best use case for the IDP, where thanks to the wider bistatic angle the target signature can be continuously detected. Of course, the folding of the spectrogram still represents a limitation, compared to the PR approaches (i.e., strategy #1 in this case), but the perspective of a low complexity sensor used for surveillance is quite appealing, especially aiming at civilian applications, making it the perfect alternative to Strategy #4 of the PR when the absence of the target from the first range cell cannot be guaranteed.

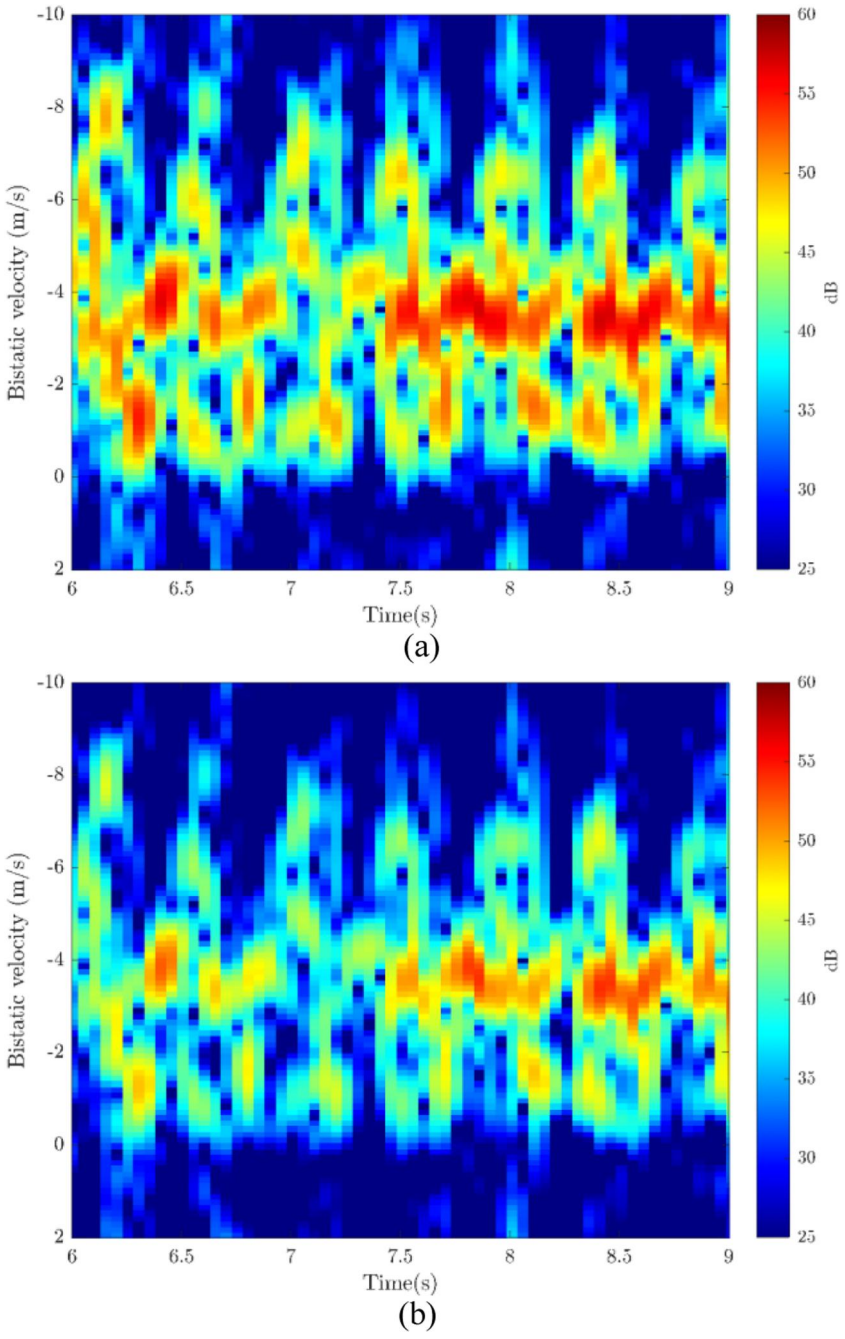


FIGURE 12 Enlarged view of Figure 11(a) and Figure 11(b).

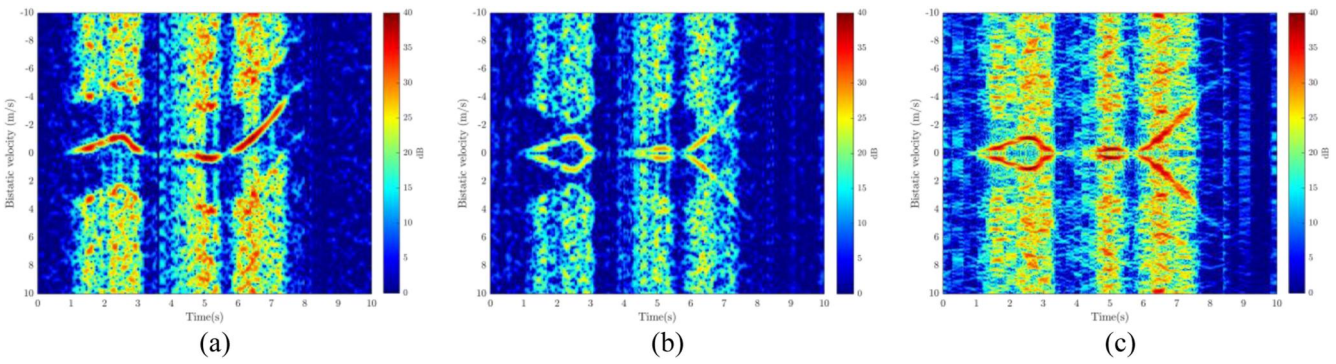


FIGURE 13 Bistatic velocity-time map for (a) PR with strategy #1, (b) PR with strategy #4 and phase-delay compensation, (c) IDP.

6 | CONCLUSION

In this work, we have investigated the possibility of detecting people and drones exploiting the emissions of a WiFi access point without relying on the availability of a good copy of the transmitted signal. To this end, we have considered two different architectural solutions and approaches.

First, we have considered the possibility of exploiting a passive radar approach, with the reference signal being a synthetically built version of the data-independent PHY preamble of the WiFi packets. In order for this solution to work properly and deal with the lack of time/phase synchronization between the reference and surveillance signals, we have proposed a practical solution for many practical scenarios.

Moreover, we have considered an alternative and simplified approach that looks for the presence of a moving target by observing the amplitude fluctuation that its motion produces on the direct signal. This solution is characterized by a lower computational burden and can be easily implemented on commercial off-the-shelf hardware.

The two different solutions have been comparatively assessed and the entire processing schemes have been validated on real WiFi data in different operative scenarios by identifying the advantages and weaknesses of each solution. We have demonstrated that both approaches might represent practical solutions and we provided hints on the best suited solution to be employed under different operative conditions.

AUTHOR CONTRIBUTIONS

Marco Di Seglio: Conceptualisation; Data curation; Formal analysis; Software; Writing – original draft. **Francesca Filippini**: Conceptualisation; Formal analysis; Software; Writing – review & editing. **Carlo Bongioanni**: Data curation; Formal analysis; Software; Writing – review & editing. **Fabiola Colone**: Conceptualisation; Formal analysis; Supervision; Writing – review & editing. All authors have read and agreed to the published version of the manuscript.

ACKNOWLEDGEMENTS

This work was partially supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of Next Generation EU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART", CUP B53C22004050001).

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Research data are not shared.

ORCID

Marco Di Seglio https://orcid.org/0000-0002-2900-297X
Francesca Filippini https://orcid.org/0000-0001-7821-0065
Carlo Bongioanni https://orcid.org/0000-0001-5537-5211
Fabiola Colone https://orcid.org/0000-0002-6694-7534

REFERENCES

1. Colone, F., et al.: WiFi-based passive bistatic radar: data processing schemes and experimental results. IEEE TAES 48(2), 1061–1079 (2012). https://doi.org/10.1109/taes.2012.6178049
2. Chetty, K., Smith, G.E., Woodbridge, K.: Through-the-Wall sensing of personnel using passive bistatic WiFi radar at standoff distances. IEEE TGRS 50(4), 1218–1226 (2012). https://doi.org/10.1109/tgrs.2011.2164411
3. Falcone, P., et al.: Two-dimensional location of moving targets within local areas using WiFi-based multistatic passive radar. IET RSN 8(2), 123–131 (2014). https://doi.org/10.1049/iet-rsn.2013.0207
4. Tan, B., Woodbridge, K., Chetty, K.: A real-time high resolution passive WiFi Doppler-radar and its applications. In: 2014 International Radar Conference (Radar), pp. 13–17. Li (2014)
5. Pastina, D., et al.: Parasitic exploitation of wi-fi signals for indoor radar surveillance. IEEE Trans. Veh. Technol. 64(4), 1401–1415 (2015). https://doi.org/10.1109/tvt.2015.2392936
6. Sun, H., Chia, L.G., Razul, S.G.: Through-wall human sensing with WiFi passive radar. IEEE TAES 57(4), 2135–2148 (2021). https://doi.org/10.1109/taes.2021.3069767
7. Shah, S.A., Fioranelli, F.: RF sensing technologies for assisted daily living in healthcare: a comprehensive review. IEEE AES Magazine 34(11), 26–44 (2019). https://doi.org/10.1109/maes.2019.2933971
8. Li, W., Tan, B., Piechocki, R.: Passive radar for opportunistic monitoring in E-health applications. IEEE Journal of Translational Engineering in Health and Medicine 6, 1–10 (2018). https://doi.org/10.1109/jtehm.2018.2791609
9. Li, W., et al.: Passive WiFi radar for human sensing using a stand-alone access point. IEEE TGRS 59(3), 1986–1998 (2021). https://doi.org/10.1109/tgrs.2020.3006387
10. Yildirim, H.C., et al.: Super resolution passive radars based on 802.11ax Wi-Fi signals for human movement detection. IET Radar, Sonar Navig. 15(4), 323–339 (2021). https://doi.org/10.1049/rsn2.12038
11. Yildirim, H.C., et al.: Passive Radar Based on 802.11ac Signals for Indoor Object Detection," 2019 16th European Radar Conference (EuRAD), pp. 153–156. France, Paris (2019)
12. Colone, F., et al.: On the use of reciprocal filter against WiFi packets for passive radar. IEEE Trans. Aero. Electron. Syst. 58(4), 2746–2761 (2022). https://doi.org/10.1109/taes.2021.3138711
13. Di Seglio, M., et al.: Reducing the computational complexity of WiFi-based passive radar processing. In: 2022 IEEE Radar Conference. New York (2022)
14. Di Seglio, M., et al.: Human and drone surveillance via RpF-based WiFi passive radar: experimental validation. In: 2022 International Radar Symposium. Gdańsk, Poland (2022)
15. Di Seglio, M., et al.: Reference-free WiFi PHY preamble based passive radar for human sensing. In International Conference on Radar Systems (RADAR 2022), pp. 119–124. Edinburgh (2022)
16. Griffiths, D., et al.: Direct signal synchronization for staring passive bistatic radar. In International Conference on Radar Systems (RADAR 2022), pp. 220–225. Hybrid Conference, Edinburgh (2022). https://doi.org/10.1049/icp.2022.2319
17. Cabrera, O., et al.: Comparing phase-locked and non-phase-locked architectures for dual-channel DVB-S passive radar, 2020 17th European Radar Conference (EuRAD 2020), Utrecht, Netherlands, pp. 350–353, (2021), https://doi.org/10.1109/EuRAD48048.2021.00096
18. Cherniakov, M.: Basic principles of forward-scattering radars. In: Bistatic Radar: Principles and Practice: Part III. Wiley, New York (2007)
19. Gashinova, M., et al.: Forward scatter radar. In: Novel Radar Techniques and Applications Volume 1: Real Aperture Array Radar, Imaging Radar, and Passive and Multistatic Radar, pp. 563–619. SciTech, Raleigh (2017). ch. 13
20. Colone, F.: DVB-T-Based passive forward scatter radar: inherent limitations and enabling solutions. IEEE Trans. Aero. Electron. Syst. 57(2), 1084–1104 (2021). https://doi.org/10.1109/taes.2020.3035435
21. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Std. 802, 11, (2016)
22. Colone, F., et al.: Reference-free amplitude-based WiFi passive sensing. IEEE Trans. Aero. Electron. Syst., 1–23 (2023). https://doi.org/10.1109/TAES.2023.3276738

23. Filippini, F., et al.: OFDM based WiFi Passive Sensing: a reference-free non-coherent approach. In: 2023 IEEE Radar Conference (RadarConf23), pp. 1–6. San Antonio (2023). https://doi.org/10.1109/RadarConf2351548.2023.10149694
24. Falcone, P., Colone, F., Lombardo, P.: Doppler frequency sidelobes level control for WiFi-based Passive Bistatic Radar. In: 2011 IEEE RadarCon (RADAR), pp. 435–440. Kansas City (2011). https://doi.org/10.1109/RADAR.2011.5960576

How to cite this article: Di Seglio, M., et al.: Comparing reference-free WiFi radar sensing approaches for monitoring people and drones. IET Radar Sonar Navig. 18(1), 107–124 (2024). https://doi.org/10.1049/rsn2.12506