Passive Radar based on 802.11ac Signals for Indoor Object Detection

H.C. Yildirim*, L. Storrer*, M. Van Eeckhaute*, C. Desset†, J. Louveaux‡ and F. Horlin*
*Université Libre de Bruxelles - †IMEC - ‡Université Catholique de Louvain

Email: *hasan.can.yildirim@vub.be, {laurent.storrer, mveeckha, fhorlin}@ulb.ac.be, claude.desset@imec.be jerome.louveaux@uclouvain.be*

***Abstract*—Passive radars opportunistically capture communications signals to detect and track targets in the environment. Since Wi-Fi signals are widely available today and have a limited coverage, interestingly they can be used by passive radars in local areas. Until now, passive radars based on Wi-Fi signals have only been designed for 11a/b/n signals, which makes the radar range accuracy insufficient for object detection because of the limited signal bandwidth (20-40 MHz). This paper investigates the use of the recent 11ac signals of much wider bandwidth (80-160 MHz) to significantly improve the range accuracy. The radar works by observing the 11ac preamble transmitted at the beginning of each data burst by the Wi-Fi access point and applies either a two-dimensional cross-correlation or a frequency/time domain channel estimation to build range/Doppler maps of the radar scene. It is shown by simulations that radar processing based on time-domain channel estimation is the only viable solution due to the frequency guard bands introduced in the signal that cause significant sidelobes in the range/Doppler map. Experimental results held in our research lab confirm that the radar is capable of separating objects of small size in an indoor environment (a fan and an electric train in our experiments).**

***Index Terms*—Passive Radar, OFDM radar processing, Wi-Fi, 802.11ac, indoor object detection**

I. Introduction

In order to detect and track objects, active radars are being used since World War I. To do so, radars provide range-Doppler maps (RDM), where each echo is associated with a distance and speed. To be precise and reliable, the active radars require well-designed signals along with high emission power to cover long distances. Thanks to the advances in electronics, the active radars have become more efficient in terms of power consumption and accuracy.

On the other hand, passive radars (PR) are devices that use the signals transmitted by non-cooperative sources as signals of opportunity, in order to build RDMs. Thereby they do not emit any additional signal. This is an excellent opportunity for detecting/tracking targets, along with estimating channel parameters for communication purposes. Moreover, it is well-known that the radar accuracy largely depends on three factors: the ambiguity function of the signals which determines their suitability for radar processing; the bandwidth, which determines the range resolution; the integration time, which determines the speed resolution. One of the main challenges in PR is the requirement to have a perfectly reconstructed reference signal in order to apply radar processing techniques. To do so, a separate reference channel is usually implemented [1], which increases the cost and complexity of the system.

Wi-Fi, based on the IEEE 802.11 standard, is the most popular WLAN technology. 802.11n/ac standards use Orthogonal Frequency Division Multiplexing (OFDM) modulation due to its ability to efficiently deal with time dispersive channels. From a PR point of view, Wi-Fi is an excellent opportunity for various reasons. First, it is widely available today. Second, the ambiguity function analysis of OFDM, studied in [2], provides enough accuracy for target detection. Third, since the bandwidth also determines the accuracy of range estimation, it is appropriate to consider newer versions of this standard. With bandwidths equal to 20 and 40 MHz for 802.11n, the range resolution is limited to 7.5-3.75 meters, as studied in [3]. The 802.11ac amendment [4], builds on 802.11n to further improve the delivered throughput, by allowing higher bandwidths (80-160MHz). This evolution may also significantly improve the PR range accuracy up to 1.875m and 0.9375m range resolutions, respectively. Finally, in 802.11 standards, channel parameters are estimated with the known OFDM symbols in the preamble. Therefore the requirement for a perfectly reconstructed reference signal can be solved by only using the preambles of OFDM frames, and not the random data part.

The literature proposes mainly two methods for OFDM radar processing: Computation of two dimensional cross-correlation functions (2D-CCF) proposed in [1], which involves high computational complexity; frequency domain channel estimation proposed in [5] for active radars, under the assumption that the OFDM subcarriers are fully loaded. However, such an assumption is not realistic for Wi-Fi based PR, since there are empty subcarriers on DC and Guard Bands (GB).

The contribution of this paper is threefold:

- We demonstrate that the emerging 11ac/ax signals offer new opportunities in terms of PR processing. Namely objects or persons can be discriminated based on their range thanks to the increased bandwidth.
- We adapt the radar processing to take the specificities of the 11ac preambles into account. A new method based on the time-domain channel estimation inspired from the communication domain is shown to well circumvent the problems coming from the GB inserted into the signal in frequency domain.
- We experimentally assess the radar in an indoor scenario

and demonstrate its capability to separate real objects.

This paper is structured as follows: in Section II, the 802.11n/ac signals are introduced along with the packet structure. In Section III, the OFDM signal model is introduced and the three radar processing techniques are briefly discussed. In Section IV, the experimental setup is introduced and different radar processing techniques are assessed, by using 802.11n/ac preambles as signal of opportunity. Finally, in Section V, the conclusion is drawn.

Single and double underlines represent vectors and matrices ($\underline{v}$, $\underline{\underline{M}}$); forward and inverse Fourier matrices are denoted with $\underline{\underline{F}}$ and $\underline{\underline{F}}^H$; the frequency domain vectors are represented with a tilde ($\underline{\tilde{s}}$).

II. 802.11n/ac Signals

Each amendment of the 802.11 standard, aims to improve the throughput and reliability of the communication for both indoor and outdoor scenarios. To achieve the desired improvements, the parameters are adapted and new technologies are introduced in the communication chain. Table I shows some of these parameters for 11n and 11ac. From a PR perspective, the effect of these parameters can be summarized as follows:

- Increasing the bandwidth allows for a better range resolution to discriminate target echoes.
- Empty subcarriers on GB and DC are also increased with respect to bandwidth.
- For data-aided PR processing, the reference signal reconstruction is mandatory. However, due to higher modulation orders the reference signal may not be perfectly reconstructed.

The OFDM frame of 802.11ac is shown in Figure 1. It consists of three main blocks: The legacy for backwards compatibility, the Very-High-Throughput (VHT) for the 11ac technology, and the data. For channel estimation, only Legacy-Long Training Field (L-LTF) and VHT-LTF are used.

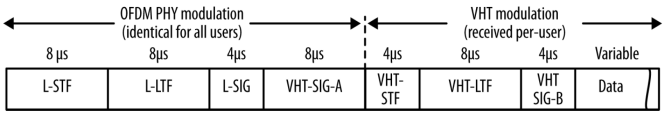

Fig. 1: Wi-Fi packet structure. For a detailed explanation of the standard, refer to [4],[6]

Parameter	802.11n/ac		802.11ac	
Bandwidth [MHz]	20	40	80	160
Number of Subcarriers	64	128	256	512
Guard Bands [Left, Right]	{4,5}	{6,5}	{6,5}	{6,5}
Empty at DC	1	3	3	11
Max. Modulation Order [QAM]	64		256	
Carrier Frequency [GHz]	2.45-5		5	

TABLE I: 802.11ac includes all the parameters from 802.11n for legacy service. For 160 MHz bandwidth, there are additional null carriers besides the ones at DC and GB. When subcarrier indices are denoted with -256 to 255, the empty subcarrier indices are -256 to -251, -129 to -127, -5 to 5, 127 to 129, 251 to 255.

III. OFDM Radar Processing

The OFDM signals in complex baseband can be defined as,

$$\underline{s} = \underline{\underline{F}}^H \, \underline{\tilde{s}} \tag{1}$$

where $\underline{\underline{F}}^H$ is size of Q and Q is the number of subcarriers. The vector $\underline{\tilde{s}}$ contains the complex frequency domain symbols, which are mapped on subcarriers. Since there is GB inserted into OFDM signals, depending on the bandwidth and the standard, some of the elements on the two sides of $\underline{\tilde{s}}$ will be zero. Moreover, the channel model can be defined as,

$$h(\tau) = \sum_{p=1}^{P} \alpha_p \exp(j\phi)\delta(\tau - \tau_p) \tag{2}$$

where P is the total number of multi-path components (MPC); α_p and τ_p are the complex amplitude and propagation delay of each MPC, respectively; ϕ is the random phase due to reflections. The received signal is the convolution of the transmitted signal with the channel impulse response. Therefore, the convolution can be mathematically written by multiplication with a channel matrix $\underline{\underline{H}}$ which is circulant thanks to the addition and removal of a cyclic prefix (CP),

$$\underline{r} = \underline{\underline{H}} \, \underline{s} \tag{3}$$

Since $\underline{\underline{H}}$ is circulant, it can be decomposed as follows,

$$\underline{\underline{H}} = \underline{\underline{F}}^H \, \underline{\underline{\Lambda}}_{\tilde{h}} \, \underline{\underline{F}} \tag{4}$$

where the diagonal elements of $\Lambda_{\tilde{h}}$ are the frequency domain channel coefficients, i.e. the inverse Fourier Transform (IFT) of (2) after sampling. Therefore, by replacing the transmitted signal and the channel matrix with their equivalents, the received signal can be written in time domain as,

$$\underline{r} = \underline{\underline{F}}^H \, \underline{\underline{\Lambda}}_{\tilde{h}} \, \underline{\tilde{s}} \tag{5}$$

or equivalently in the frequency domain,

$$\underline{\tilde{r}} = \underline{\underline{\Lambda}}_{\tilde{h}} \, \underline{\tilde{s}} = \underline{\underline{\Lambda}}_{\tilde{s}} \, \underline{\tilde{h}} \tag{6}$$

where $\underline{\underline{\Lambda}}_{\tilde{s}}$ is a diagonal matrix, defined by $\underline{\tilde{s}}$. Both (5) and (6) show that the transmitted complex symbols are affected by the channel coefficients. From a communication perspective, estimating the parameters of (2) for known preambles at the receiver, allows to equalize the distortions on the data. However, from a radar perspective, MPCs can be seen as the target returns. Their distances are linked to the propagation delay with two-way propagation, $\tau = 2R/c$, where R and c are the target distance and speed of light, respectively.

In the following subsections, we briefly introduce the processing stages to obtain a RDM: Sections III-A/B/C introduce range estimation alternatives, while Section III-D introduces the Doppler estimation.

A. 2D Cross Correlation

Range and Doppler estimations can be handled with two dimensional cross correlations. By applying a two dimensional matched filter on the received signal with time-delayed and Doppler-shifted copies of the transmitted signal, the propagation delay and the Doppler frequency can be estimated. Since this computation has high complexity, methods are proposed in order to reduce the complexity. For the processing of 2D-CCF and proposed methods to reduce its complexity, the reader is referred to [1]. It should be noted that the matched filter response of the signal plays an important role for the radar

accuracy, especially when there are the sidelobes appearing due to the poor auto-correlation properties of the signal.

B. Frequency-Domain Channel Estimation

Assuming that the transmitted sequence is known at the receiver, the channel coefficients can be estimated with frequency-domain least squares estimation (FDLSE), i.e. performing a Fourier Transform (FT) on the received signal and dividing element-wise by the transmitted frequency domain symbols,

$$\hat{\underline{\tilde{h}}} = \underline{\underline{\Lambda}}_{\tilde{s}}^{-1}\, \underline{\tilde{r}} \tag{7}$$

where $\hat{\underline{\tilde{h}}}$ is the estimated frequency domain channel coefficients. In case of PR, computing the IFT of (7) yields to the estimate of the channel impulse response which can be considered as a range profile. If 802.11 compliant signals are considered, there will be zero elements in $\hat{\underline{\tilde{h}}}$ due to the presence of null carriers at GB and DC. When IFT is computed, null carriers will act like a rectangular window in the frequency domain, which yield a sinc function in the time domain. This effect may degrade the radar accuracy.

C. Time-Domain Channel Estimation

The received signal can also be written as,

$$\underline{r} = \underline{\underline{S}}\, \underline{\hat{h}} \tag{8}$$

where $\underline{\hat{h}}$ is the channel coefficients in the time-domain, and $\underline{\underline{S}}$ is a Toeplitz matrix (defined by $\underline{s}$) of size $[Q, L]$, where L is the channel length. Notice that (3) and (8) are identical, since convolution can be written with Toeplitz matrices as well. Therefore, the channel coeffecients can be estimated with a time-domain maximum likelihood estimator (TDMLE),

$$\underline{\hat{h}} = (\underline{\underline{S}}^H \underline{\underline{S}})^{-1}\, \underline{\underline{S}}^H\, \underline{r} \tag{9}$$

Here, to have a unique channel estimation, $S^H S$ must be nonsingular. This can be achieved by $L \leq Q$, i.e. the number of samples in a transmitted signal should be longer than the length of the channel. For more information on frequency and time domain channel estimation techniques, the reader is referred to [7].

D. Doppler Processing

In any radar system, multiple successive signals, separated with a constant time interval, are measured for range estimations. By observing the same range bin over multiple range profiles, we can find the Doppler frequency since moving targets affect the phase of each range bin. Therefore, computing an FFT for each tap yields to Doppler estimations. For more information, the reader is referred to [8].

IV. Experimental Setup & Results

To experimentally assess the PR and compare the different radar processing approaches, two separate USRPs with UBX160 daughterboards are used to implement the Wi-Fi transmitter and the PR [9]. The USRPs are synchronized in frequency and time by sharing the same clock. Transmit/receive antenna gains are 0 dBi, and additional 20 dB amplifiers are added at both sides of the link to increase the power of the received signal. The USRPs are physically co-located. Therefore the range is calculated with two-way propagation. For TDMLE, channel length, L, is chosen to be the length of the CP.Two types of signals are considered. First, fully-loaded OFDM signals of bandwidths equal to 40 and 160 MHz are transmitted. Second, 802.11n/ac compliant signals are transmitted. The compliant OFDM packet consists of 4 VHT-LTF and 30 data symbols. In total, 128 packets are transmitted per measurement.

In Table II, we provide the characteristics of the two targets. Each distance is measured precisely with laser-meters. The speeds are measured with a Doppler radar. Finally, to measure the Radar-Cross-Section (RCS) of each target, separate experiments are conducted. The radar equation is applied on those measurements to obtain an estimate of the RCS values [8]. The mean power of the noise is normalized to 0dB. In the RDM plots, a Blackman window is applied on the Doppler dimension, in order to suppress the sidelobes. For 2D-CCF, the Doppler estimation is integrated within the processing. For the latter two techniques, the FFT-based method is used.

Target	Distance	Speed	RCS
Metallic Fan	1 meter	2.4m/s	0.8dBsm
Toy-Train	3 meters	0.75m/s	2.1dBsm

TABLE II: All values are separately measured for each target. An additional metallic surface is mounted on the train, in order to increase its RCS.

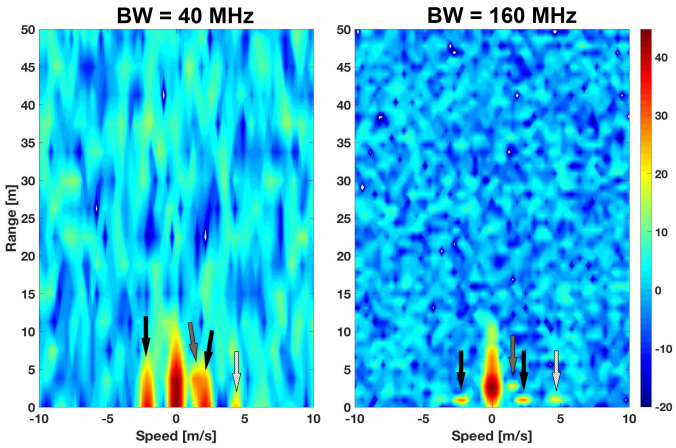

Fig. 2: Measurements with 40 and 160MHz, fully-loaded OFDM signals. Range resolutions are 3.5 and 0.9375 meters, respectively. FDLSE is used for range profile processing. Black, grey and white arrows identify the fan, train and tip of the fan, respectively.

In Figure 2, we provide the two RDMs obtained with fully-loaded OFDM signals. Since all subcarriers are loaded, no additional distortions due to band filtering are expected. For both RDM, we observe a strong and wide peak along range profile, centered at 0 m/s. This effect is known as clutter, and since the experiment takes place in an indoor environment, the clutter echo is strong and it extends to 10 meters. Beyond 10 meters, the MPCs of clutter have lower energy, therefore they are hidden under the noise floor. In case of 40 MHz bandwidth, we observe three different speeds. Since the movement of the

fan has two directions due to its rotation from its center (one approaching, one going away), the same speed appears at two different signs. The third peak at 1 meter range bin corresponds to a reflection from the tip of the fan, which has a higher speed but a lower reflection surface. The train, on the other hand, is not well separated over the range dimension. In case of 160 MHz bandwidth, the train is also clearly observed which shows the interest of using higher bandwidths.

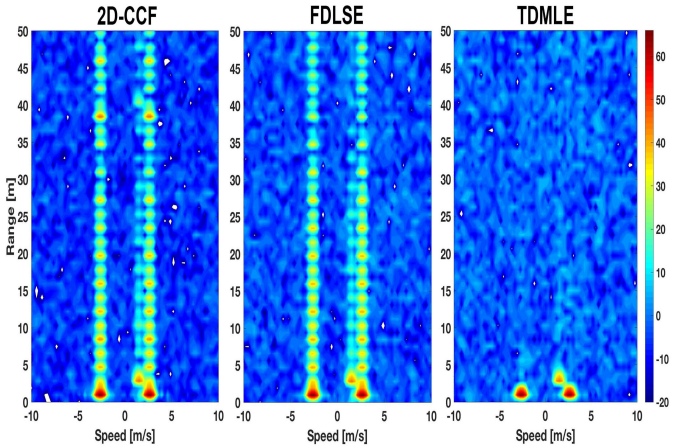

Fig. 3: Numerical results for 160MHz with higher RCS and transmit power. $V_{res} = 0.62m/s$.

Figure 3 compares the three radar processing methods when the actual 11ac preamble is considered. The analysis is first made by simulations in order to reduce the noise and get rid of the clutter. Thanks to the better range resolution, all targets are well separated over the range dimension. With 2D-CCF, we observe additional sidelobes aligned with target peaks through range dimension. The sidelobes are coming from the limited auto-correlation properties of the OFDM waveform. They may be detected as additional targets, and cause a high performance degradation. For FDLSE, we also observe similar but weaker sidelobes. The origin of these sidelobes is due to the GB inserted into OFDM signals. In order to estimate the channel impulse response, i.e. range profile, the IFT of the estimated channel transfer function is computed. In this computation, the effect of empty subcarriers can be seen as a rectangular window in the frequency domain. Since the IFT of a rectangular window yields to a sinc function, such sidelobes appear over the range profile. For TDMLE, the channel estimation is computed in the time domain, and it does not show any additional distortions. In fact, the RDM with TDMLE provides the same result as fully-loaded non-compliant signals. However, there are challenges to implement this technique. First of all, if the transmitted symbols in (9) are not binary, the square matrix must be non-singular in order to compute its inverse. Second, the maximum range is limited by the value of L. However, in terms of range-Doppler distortions, the TDMLE outperforms both 2D-CCF and FDLSE.

Figure 4 shows the experimental comparison for the radar processing methods, where 802.11ac compliant signals are transmitted. As expected, the clutter appears with similar characteristics at 0m/s. Depending on the processing technique, we also see additional sidelobes along the clutter. However, such sidelobes are not visible for moving targets. This is because, the RCS values of the targets are small enough, such that their sidelobes are below the noise floor. In a scenario where detection/tracking is considered for persons or small objects, such RCS values are realistic. With objects such as cars, the RCS values will be much higher. In such a scenario, the sidelobes will not only cause false detections, but they will also hide real targets.

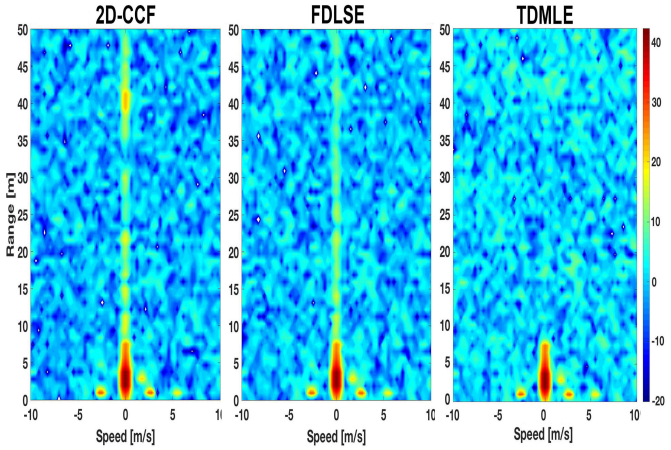

Fig. 4: Experimental results with 802.11ac compliant 160 MHz VHT-LTF signals. $V_{res} = 0.62m/s$

V. Conclusion

It is experimentally shown that passive radars based on 802.11ac signals provide enough accuracy to detect objects in an indoor environment. The passive radar works by capturing the preamble transmitted by the Wi-Fi base station at the beginning of each data burst, which allows us to remove the reference channel. Three different radar processing methods have been compared. While radar processing options based on two-dimensional cross-correlation or frequency-domain channel estimation are shown to have a poor performance due to range sidelobes, using time-domain channel estimation delivers high-accuracy range profiles. Our experiments consisted of detecting a fan and an electric train located a few meters away from the radar, in a 20m^2 room.

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, 2012*.

[2] J. Wang, B. Zhang, and P. Lei, "Ambiguity function analysis for OFDM radar signals," in *RADAR, 2016*.

[3] P. Falcone, F. Colone, C. Bongioanni, and P. Lombardo, "Experimental results for OFDM WiFi-based passive bistatic radar," in *RadarConf, 2010*.

[4] IEEE 802.11 WLAN Commitee, "802.11ac-2013 - IEEE Standard for Information technology," 2013.

[5] C. Sturm, E. Pancera, T. Zwick, and W. Wiesbeck, "A novel approach to OFDM radar processing," in *RadarConf, 2009*.

[6] Matthew Gast, *802.11ac: A Survival Guide*, O'Reilly Media, 2013.

[7] H. Meyr, M. Moeneclaey, and S. A. Fechtel, *Digital Commincation Receivers*, John Wiley & Sons, 2001.

[8] Mark A. Richards, James A. Scheer, and William A. Holm, *Principles of Modern Radar: Basic Principles*, Scitech Publishing, 2010.

[9] ETTUS, "USRP-X310," http://ettus.com.