RESEARCH ARTICLE

Obfuscation of Human Micro-Doppler Signatures in Passive Wireless RADAR

ANTONIOS ARGYRIOU, (Senior Member, IEEE)
Department of Electrical and Computer Engineering, University of Thessaly, 38334 Volos, Greece
e-mail: anargyr@uth.gr

ABSTRACT When wireless communication signals impinge on a moving human they are affected by micro-Doppler. A passive receiver of the resulting signals can calculate the spectrogram that produces different signatures depending on the human activity. This constitutes a significant privacy breach when the human is unaware of it. This paper presents a methodology for preventing this when we want to do so by injecting into the transmitted signal frequency variations that obfuscate the micro-Doppler signature. We assume a system that uses orthogonal frequency division multiplexing (OFDM) and a passive receiver that estimates the spectrogram based on the instantaneous channel state information (CSI). We analyze the impact of our approach on the received signal and we propose two strategies that do not affect the demodulation of the digital communication signal at the intended receiver. To evaluate the performance of our approach we use an IEEE 802.11-based OFDM system and realistic human signal reflection models.

INDEX TERMS 802.11, human activity classification, micro-Doppler, OFDM, passive WiFi RADAR.

I. INTRODUCTION

Systems that use wireless WiFi signals for passive tracking, localization, and activity detection have been on the rise for several years [1], [2], [3], [4], [5], [6], [7], [8], [9], [10]. The core idea of these systems is the extraction of the micro-Doppler effects from signals that have impinged on a human. There are two classes of passive techniques that can extract micro-Doppler in WiFi systems, namely Channel State Information (CSI) based systems, and Passive WiFi Radar (PWR) based systems. What we argue in this paper is that these systems, although extremely useful in a plethora of applications, may allow attacks on human privacy from random wireless receivers of opportunity that can detect human activities when we do not want them to do so. To this aim we study CSI-based systems (since they are more dangerous as we will see) and propose an approach that disables the correct extraction of micro-Doppler effects at a receiver when the transmitter desires to do so.

The associate editor coordinating the review of this manuscript and approving it for publication was Jie Tang.

Most PWR systems require a transmitter under the control of the system, i.e. one that it is cooperative and shares a dedicated channel for providing a reference signal to the passive receiver [11] (Fig. 1 left). Other PWR systems like the works in [12] and [13] leverage a reflected signal from a stationary target as a reference waveform but the human activity classification performance is suboptimal when compared to the case that a dedicated reference channel is present. In the previous PWR systems micro-Doppler is estimated by correlating the received signal with the reference signal, and then identifying when this correlation peaks for different candidate Doppler values. More recent works on PWR systems do not require a reflected signal as a reference, but simply strip away from the transmitted signal any data-dependent phase/frequency shifts leaving only Doppler-induced frequency variations [14]. This leads to improved Doppler estimates [14]. Overall we notice that PWR systems are more robust when there is cooperation with the transmitter of the signal. This is something that can be clearly avoided if we want to protect the privacy of users moving around a WiFi access point (AP), making thus PWR systems more safe.
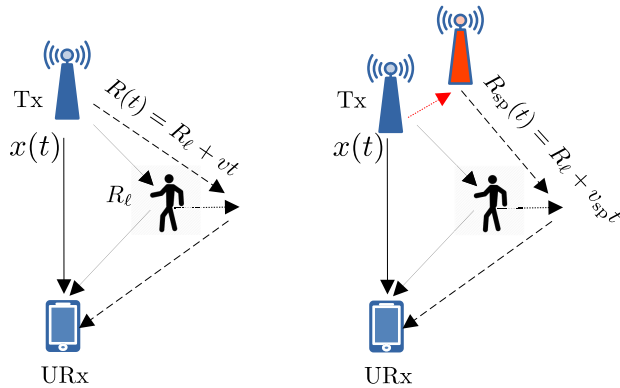
FIGURE 1. Left: The human moves with a speed that generates a change in the path length equal to vt. Right: With the proposed method the spoofed path length (as it appears in the signal) is equal to $(v + v_{SP})t$ and is mimicking the effect of a physical movement of the transmitter to the red location.

Contrary to PWR systems, CSI-based systems [11], [15] do not need a reference channel and as a result are potentially more dangerous. In this case the receiver uses CSI estimates for calculating the signal spectrogram allowing thus the identification of unique micro-Doppler signatures. This type of systems might face more difficulties in accurate micro-Doppler estimation, but pose a serious privacy threat since an arbitrary unauthorized user can deploy them without requiring explicit authorization from the AP that is associated with. The basic idea, described in works such as [15] and [16], is based on the fact that human movement generates variations in the length of the multiple reflected paths from the signal source to the receiver, and consequently the power of the received signal over certain frequency bands (i.e. the channel frequency response (CFR) $H(f, t)$). As seen in Fig. 1(left) the length of the ℓ-th path changes from R_ℓ to $R_\ell + vt$) upon human movement.

It is important to note that this class of techniques is not viewed as threatening to the user but as a low cost approach that enables several applications. Hence, there is little focus on combating these passive systems. Few existing systems in the literature focus on obfuscating parameters of a digital communication signal and are not related to micro-Doppler. As an example friendly Cryptojam [17] obfuscates various PHY layer parameters like the modulation type but it does not affect the waveform and consequently does not obfuscate Doppler or micro-Doppler in reflected signals from humans. Obfuscating the cyclostationary property of digital communication signals has been investigated in [18], something that does not affect channel-induced Doppler. Artificial frequency shifts in a transmitted signal have been proposed in the past as a method to prevent correct demodulation by an adversary [19], and also as a way to spoof the range and velocity of the emitter relative to a receiver [20]. But again these last two methods were not intended to prevent estimation of micro-Doppler signatures. The most closely related work to this paper may be PhyCloak [21] that distorts Doppler information at a passive receiver through a third relay

node that emits simultaneously with the transmitter leading thus to obfuscation. However, this system requires always the presence of a third relay node that is synchronized to the transmitter, while more importantly is not concerned with reflected signals from humans that are affected by micro-Doppler.

As we already stated, in this paper we take a different stance and we argue that these systems can be a threat to privacy. In cases where we do not desire their operation, we should try to prevent them from being used by malicious wireless users. Consequently, we focus on CSI-based schemes where a receiver of opportunity, namely an unauthorized receiver (URx), can calculate the CSI and its frequency-dependent short time scale variations that allow micro-Doppler estimates through a spectrogram. We consider a WiFi transmitter that uses orthogonal frequency division multiplexing (OFDM) and emits a digital communication signal to a desired receiver but it does not want this signal to be used for micro-Doppler estimation by others. *Under this setup we propose to protect humans from disclosure of their micro-Doppler signature by inserting an artificial frequency variation effect in the transmitted signal so as to alter the real micro-Doppler effects. At the same time the artificial signal should not affect signal demodulation.* We accomplish that by injecting either a low frequency modulated (FM) signal in the transmitted waveform that smears the micro-Doppler signature, or a signal that spoofs the *path length changes* that take place in a micro scale as illustrated in Fig. 1(right) and discussed in [15]. We study the received signal and the CSI estimation process at the receiver, and then we investigate the effect of the two aforementioned signal structures on the spectrogram through simulations based on real human activity models. The effect of the first method in the spectrogram is the generation of similar signatures regardless of the user movement speed. For this first *spectrogram smearing* technique we also propose a metric for allowing the evaluation of the effectiveness of our scheme in terms of generating similar waveforms for different user activities.

II. SIGNAL MODEL
For the purpose of this paper we assume that the transmitter (Tx) is static, i.e. it is a base station that is part of the legitimate network with which it communicates (we do not study it). The signal model is that of 802.11a/g/n/ac OFDM where a 20 MHz channel is used [22]. A moving transmitter can also be supported but the resulting expressions become more convoluted without adding any new insights to the core idea of this paper. The 802.11 PHY frame preamble details can be found here [22]. The basic aspects from the 802.11 frame structure that we need to know for this paper is that the preamble of each frame consists of 7 short and repeating known QAM symbols, as it is typically done in the preambles of wireless frames. These known symbol values allow for CSI estimation at a receiver with a process that we will discuss later.

The one-way delay of the WiFi OFDM signal that impinges on the human target is time-varying and equal to

$$\tau_\ell(t) = \frac{R_\ell(t)}{c} = \frac{R_\ell}{c} - \frac{v_\ell t}{c}, \qquad (1)$$

where c is the speed of light, and R_ℓ and $R_\ell(t)$ correspond to the length of the ℓ-th path before the movement and at time t respectively (see Fig. 1). v_ℓ is a speed that results in the so called *path length change* [15] of $v_\ell t$ in time t. Since different body parts travel different distances and have different speed as the human moves, this results in a unique micro-Doppler signature when the effect of all the paths is aggregated.

We will consider the impact of micro-Doppler when the transmitted signal $x(t)$ is the result of multi-carrier modulation and more specifically OFDM. With N subcarriers that are spaced relative to the carrier f_c at locations $f_k = k\Delta f$ Hz that can contain data, pilot symbols, or a combination of both (depending on the standard), the desired baseband OFDM symbol in continuous time is:

$$x(t) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X[k] e^{j2\pi k\Delta ft}, \ 0 \le t \le T_N \qquad (2)$$

$X[k]$ is the complex QAM symbol modulated onto subcarrier k, and $T_N = N/\Delta f$ is the OFDM symbol duration.

The channel transfer function or channel frequency response (CFR) of a wideband time-varying channel over all the paths is

$$H(f,t) = \sum_\ell h_\ell(t) e^{-j2\pi f\tau_\ell(t)}, \qquad (3)$$

where $h_\ell(t)$ is the complex channel gain of the ℓ-th path excluding Doppler. The channel impulse response at time t is time-varying (p.p. 21 [23]):

$$h(\tau,t) = \sum_\ell h_\ell(t)\delta(\tau - \tau_\ell(t)) \qquad (4)$$

To derive the desired expression for the received signal we have to use (2), (3) and (4). At the passive URx the received baseband continuous time signal after transmission in a time-varying frequency selective channel is the convolution of the channel impulse response with the transmitted OFDM signal. We also include the additive white Gaussian noise (AWGN) $w(t)$ and obtain:

$$
\begin{aligned}
y(t) &= \int_{-\infty}^{\infty} h(\tau,t)x(t-\tau)d\tau + w(t) \\
&= \sum_\ell h_\ell(t)x(t-\tau_\ell(t)) + w(t) \\
&= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_\ell h_\ell(t)X[k]e^{j2\pi k\Delta f(t-\tau_\ell(t))} + w(t) \\
&= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X[k]e^{j2\pi k\Delta ft} \sum_\ell h_\ell(t)e^{-j2\pi k\Delta f\tau_\ell(t)} \\
&\quad + w(t)
\end{aligned}
\qquad (5)
$$

$$= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X[k]e^{j2\pi k\Delta ft} H(k\Delta f, t) + w(t) \qquad (6)$$

By replacing (3) to (5) we obtain (6) which is another form of the output signal that we will use. When the CFR is not time-varying by applying DFT to (5), (6) we get the well known result of OFDM where the channel becomes from a frequency selective fading channel to a flat fading channel, i.e. $Y(k\Delta f) = X[k]H(k\Delta f)$. Of course in practice time variations of the CFR cause inter-carrier interference (ICI).

To get another useful expression we can also substitute $\tau_\ell(t)$ from (1) to (5). Then the term $e^{-j2\pi k\Delta f\frac{R_\ell}{c}}$, that is constant phase for the ℓ-th path (i.e. it is not indexed by t) can be merged with $h_\ell(t)$ to be jointly denoted as $h'_\ell(t)$. We then have:

$$y(t) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X[k]e^{j2\pi k\Delta ft} \sum_\ell h'_\ell(t)e^{-j2\pi k\Delta f\frac{v_\ell t}{c}} + w(t) \qquad (7)$$

Note that we do not model a carrier frequency offset (CFO) since we have seen that it affects marginally the resulting spectrograms. We also ignore the sampling clock offset (SCO) at the passive URx since we are not interested in its ability to correctly demodulate OFDM symbols (by sampling when the matched filter output peaks).[1]

III. MICRO-DOPPLER SMEARING & SPOOFING

We can design an artificial signal to have any desired form as long as it does not compromise decoding of $x(t)$. We denote this signal as $x_{sp}(t)$ in the time domain and $X_{sp}(f,t)$ is the Fourier Transform (FT). The two ideas that we investigate are: *Method 1, subcarrier independent micro-Doppler obfuscation with spectrogram smearing. Method 2, subcarrier-dependent spoofing for mimicking path length changes.* We must note that under both scenarios the injected signal does not introduce observable frequency shifts in the scale of an OFDM frame, thus it does not prevent CSI estimation from the nominal receiver that desires to demodulate the transmitted frame. IEEE 802.11 frequency estimation and compensation algorithms are robust to Doppler variations of a few hundred kHz, which is far beyond what we are doing with the artificial signal in this work [25]. The OFDM bit error rate (BER) performance under this range of artificial frequency variations was studied in [20] and no performance degradation was observed.

A. METHOD 1: SMEARING

With the first method we introduce an oscillating sinewave with a frequency of a few 10's of Hz in the transmitted signal $x(t)$ to smear the micro-Doppler effects of human movement that are in this range [26]. Note that we do not have to re-create a specific spectrogram but we only have to destroy the

---

[1]To see how this can be solved for OFDM we refer the reader to related works on the topic, e.g. see [24].

signature that reveals micro-Doppler dependence to different user movement speeds.

To generate the final signal at the transmitter we re-modulate the information signal which consists of the QAM symbols $X[k]$ before IDFT, with a frequency domain signal $X_{sp}(f, t)$. In the time domain this obfuscating signal is defined to be an frequency-modulated (FM) waveform with maximum instantaneous frequency shift δf, and frequency f_m, making thus the instantaneous frequency equal $f_i(t) = f_c + \delta f \cos(2\pi f_m t)$ [27]. This makes the actual time-domain FM *smearing signal* to be:

$$x_{sp}(t) = e^{j\frac{\delta f}{f_m} \sin(2\pi f_m t)} \tag{8}$$

Hence, this waveform produces a signal that in the frequency domain speads between the maximum instantaneous frequencies $-\delta f$ and $+\delta f$, at a rate of f_m Hz. The result is that it smears the frequency domain micro-Doppler signature in that frequency range. An important detail from the literature is that the frequency at which the various human body parts move is very small and in the range of a few Hz [26], [28]. Consequently, the variation of the frequency f_m should be higher that this value which means that just a few tens of Hz for f_m will smear very well the received signal spectrogram.

B. METHOD 2: SPOOFING PATH LENGTH CHANGES
The second approach is based on thinking of what would the signal look like if the transmitter had actually moved. Hence, this technique can be more appropriately referred to as *spoofing* and not simply obfuscation. Note that we can only spoof the phase change in a way that mimics the signal that would be produced if a physical movement of the transmitter took place (to the "new" red location in Fig. 1(right)). The received signal has to be such that the path length change seen in Fig. 1 will not be $v_\ell t$ but $v'_\ell t$ in the same time period of t seconds, that is we want the URx to receive the following signal:

$$y(t) = \sum_{k=0}^{N-1} \frac{X[k]}{\sqrt{N}} e^{j2\pi k \Delta f t} \sum_\ell h'_\ell(t) e^{-j2\pi k \Delta f \frac{v'_\ell}{c} t} \tag{9}$$

This is a form of the signal that we would like to be received at the URx and the question is how to create it. To obtain the above we set the *spoofing signal* equal to $x_{sp}^{(k)}(t) = e^{j2\pi k \Delta f \frac{v_{sp}}{c} t}$, making thus (7):

$$y(t) = \sum_{k=0}^{N-1} \frac{X[k] x_{sp}^{(k)}(t)}{\sqrt{N}} e^{j2\pi k \Delta f t} \sum_\ell h'_\ell(t) e^{-j2\pi k \Delta f \frac{v_\ell}{c} t}$$

$$= \sum_{k=0}^{N-1} \frac{X[k] e^{j2\pi k \Delta f \frac{v_{sp}}{c} t}}{\sqrt{N}} e^{j2\pi k \Delta f t} \sum_\ell h'_\ell(t) e^{-j2\pi k \Delta f \frac{v_\ell}{c} t}$$

$$= \sum_{k=0}^{N-1} \frac{X[k]}{\sqrt{N}} e^{j2\pi k \Delta f t} \sum_\ell h'_\ell(t) e^{-j2\pi k \Delta f \frac{v_\ell - v_{sp}}{c} t} \tag{10}$$

By comparing (9) and (10) we see that the path length change that will be perceived for the ℓ-th path is $v'_\ell = v_\ell - v_{sp}$.

In our implementation instead of sending to each subcarrier complex symbol $X[k]$ we send $X[k] x_{sp}^{(k)}(t)$, that is a subcarrier and time dependent term. In the next section we discuss how these two methods affect the CFR power estimate that will be used for spectrogram estimation by the URx.

IV. IMPACT OF CFR POWER
The CFR power for subcarrier k is estimated after we first match filter the frequency domain received signal of that subcarrier, namely $Y(k \Delta f)$, with the known preamble $X[k]$. Since the spoofing signal has a FT $X_{sp}(f, t)$ this leads to the CFR being equal to:

$$\left| \frac{X^*[k] Y(k \Delta f)}{|X[k]|^2} \right|^2 = |X_{sp}(k \Delta f, t) H(k \Delta f, t)|^2 \tag{11}$$

From the above it is clear that we can select a smearing or spoofing waveform so that it alters completely the CFR power estimate above as a function of frequency or time.

Method 1: With this method the result is straightforward since the signal is independent of subcarriers. This method simply smears the resulting signal over the specified bandwidth of the FM signal obfuscating thus micro-Doppler effects. This bandwidth is approximated to be $2(\frac{\delta f}{f_m} + 1)$ according to Carson's rule.

Method 2: Now we analyze the CFR power, namely $|X_{sp}(k \Delta f, t) H(f, t)|^2$, to understand what takes place. An expression for the CFR power $|H(f, t)|^2$ has been studied in [15], but as we have seen in (9) the path length is now affected by the artificial speed v_{sp}. Hence, we re-calculate the CFR power as in [15] that now becomes for the set of all end-to-end paths $\mathcal{P}$:

$$|X_{sp}(k \Delta f, t) H(k \Delta f, t)|^2$$

$$= \sum_{\ell \in \mathcal{P}} D_1(f, t) \cos(\frac{2\pi v'_\ell t}{c} + \frac{2\pi R_\ell}{c})$$

$$+ \sum_{\ell, m \in \mathcal{P}, \ell \neq m} D_2(f, t) \cos(\frac{2\pi (v_\ell - v_m) t}{c} + \frac{2\pi (R_\ell - R_m)}{c})$$

$$+ \sum_{\ell \in \mathcal{P}} D_3(f, t) \tag{12}$$

The terms D_1, D_2, D_3 are time and frequency dependent and are independent of the path length changes expressed through the speed v_ℓ. From this expression we see that the CFR power is a function of the actual path length changes $v_\ell - v_m$, that are not affected by this type of spoofing, but there are also sinusoidal terms that are affected (in the first summation). The net result is that the correct overall CFR power function is still invalidated by this approach. As we will soon see it has a completely different impact on the Doppler spectrogram than method 1.

V. RESULTS
The objective of our simulations is to evaluate the ability of the two methods to smear the Doppler signature of the human movement. We considered an 802.11-based OFDM
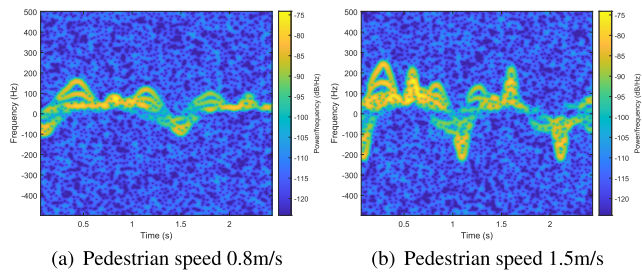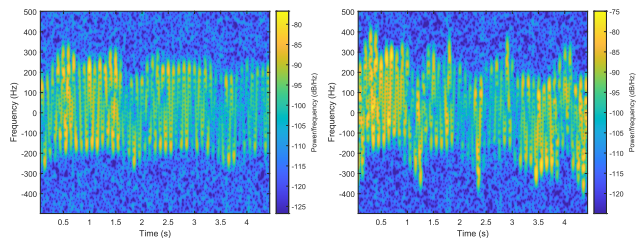
(a) Pedestrian speed 0.8m/s (b) Pedestrian speed 1.5m/s

FIGURE 2. Spectrograms of the received signal (before OFDM DFT) for different pedestrian speeds without any form of smearing.

(a) Pedestrian speed 0.8m/s w/ smear-(b) Pedestrian speed 1.5m/s w/ smear-
ing under method 1   ing under method 1

FIGURE 3. Spectrograms of the received signal (before OFDM DFT) for different pedestrian speeds and smearing under method 1.

system that uses a 20 MHz channel, and 64 subcarriers spaced at Δf =312.5 kHz apart. 52 are data subcarriers while 4 subcarriers are used for pilot signals. We generate signatures for pedestrians that move at different speeds based on publicly available models in [26] and [28]. These channel models generate movement of different human body parts and alter the cross-section of the human depending on the movement pattern.

A. METHOD 1

To illustrate better the effects of this method we noticed that is better to calculate the spectrogram on the received signal itself, i.e. before passing the OFDM signal to the DFT for demodulation. In Fig. 2(a), 2(b) we present spectrogram results for humans moving at different speeds without any form of micro-Doppler smearing. We can easily see the micro-Doppler for the different speeds and the peaks that occur at different frequencies. In Fig. 3(a) and Fig. 3(b) we present results for a pedestrian moving again at 0.8 m/s and 1.5 m/s respectively, under the smearing method 1. It is clear that the Doppler smearing method spreads the resulting signal over an area of $\delta f \approx \pm 200$ Hz in both cases making thus the spectrograms lack any distinguishing features. f_m which was set to 10 Hz is already high enough to cover the moving user that presents peaks in the spectrograms of Fig. 2(a), 2(b) with at most 0.5 s (2 Hz). Higher speed user movements will result in more rapid changes over time that can still be covered with an f_m of a few 10's of Hz.

B. WAVEFORM SIMILARITY

As we have discussed and seen in the last subsection, spoofing with method 1 generates spectrograms that are
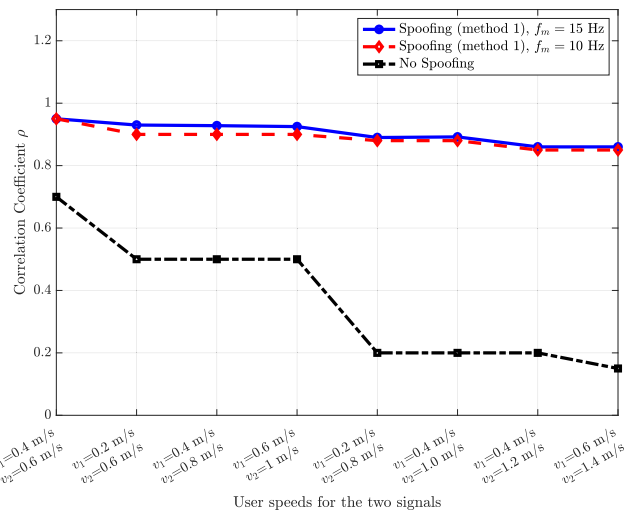

FIGURE 4. Correlation coefficient for two waveforms under different user speeds and method 1.

similar. To provide a systematic way of comparing the results of our spoofing method we use the signal cross-correlation as an evaluation metric. In particular we measure the cross-correlation between two received waveforms $y_1(t)$, $y_2(t)$ at the URx that contain the spoofed signal and correspond to two different user speeds v_1, v_2 respectively:

$$\rho_{v_1, v_2}(\tau) = \frac{\int_{-\infty}^{+\infty} y_1(t) y_2(t - \tau) dt}{\int_{-\infty}^{+\infty} y_1(t) y_2(t) dt} \quad (13)$$

In the above τ is the lag. Using this metric someone can evaluate the "quality" of smearing for specific emitted waveforms and user behavior. Under this metric we obtained correlation results for various pairs of spoofed waveforms in which the user speeds in these pairs are presented in the x axis of Fig. 4. As an example consider data point v_1=0.4 m/s and v_2=0.8 m/s that corresponds to the correlation of two received signals that were subjected to spoofing and the user in one case moved with v_1=0.4 m/s and the other case with v_2=0.8 m/s. This result shows that the received signals are almost identical with $\rho \approx 0.94$. All the results that are presented in this figure show that with the proposed method under different user speeds the correlation coefficient is very high. This is also true for an f_m of 10 Hz which has minor differences relative to the case of f_m equal to 15Hz. We also present the results without spoofing that clearly show lowering correlation when the users move at different speeds and produce considerably different signatures (as it is already evident from Fig. 3). This is expected since we have already seen in the spectrogram that higher user speed generates higher maximum frequencies in the signal.

C. METHOD 2

For the results under method 2 we demodulate each OFDM symbol with DFT, and then we produce a fine estimate of the time-varying CFR power for each one of the used subcarriers. CFR power is estimated for each one of the subcarriers based
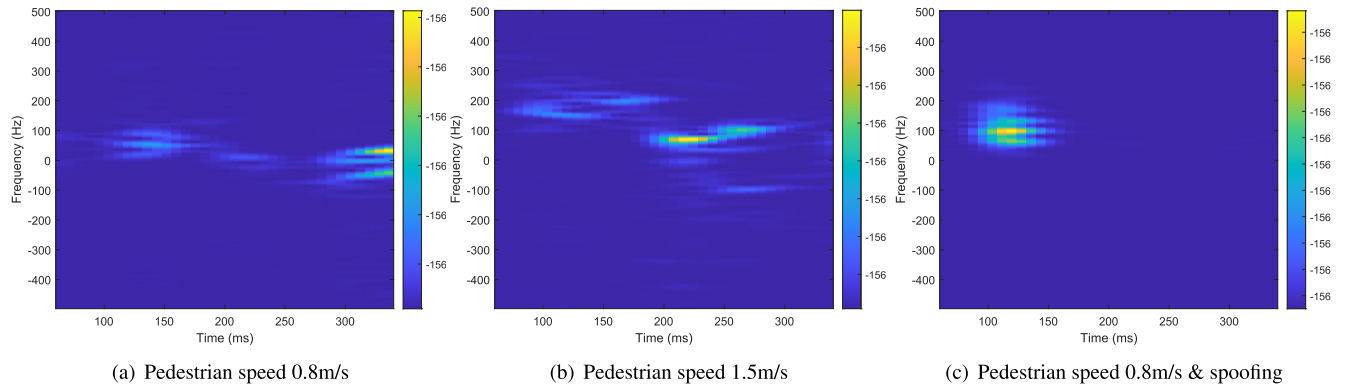
| (a) Pedestrian speed 0.8m/s | (b) Pedestrian speed 1.5m/s | (c) Pedestrian speed 0.8m/s & spoofing |

FIGURE 5. Spectrograms of the CFR power in (11) for different pedestrian speeds without spoofing and with micro-Doppler spoofing under method 2.

on the OFDM symbols in the 802.11 preamble allowing the calculation of $\left|\frac{X^*[k]Y(k\Delta f)}{|X[k]|^2}\right|^2$ since the $X[k]$ are known. From this time-varying CFR power estimate we calculate the spectrogram with a resolution of a single OFDM symbol.

The related results for the spectrogram of the CFR power without spoofing can be seen in Fig. 5(a), Fig. 5(b), and with spoofing in Fig. 5(c). We can now see that for the same human speed we can generate a different spectrogram at the URx which is more similar to a spectrogram of a human moving at a higher speed. Now there is not a consistent smearing all over the frequency range but a shift in frequency and time of the human signature that depends on the path length change $v'_\ell t$. Different values for v_{sp} will result in different placement of the signature in the spectrogram.

VI. DISCUSSION

The methods we introduce in this paper offer a way to obfuscate the micro-Doppler signature of a signal that is observed at a passive adversarial receiver. We showed that our method is indeed successful in doing so. One could ask why does the adversary not use different versions of the signal that are more feature-rich so as to extract the human activity? For classic monostatic RADAR this has been successfully demonstrated in works such as [29] and [30], where besides the Doppler signature, the range differences are used for human activity classification with mmWave RADAR. But for a passive receiver, which is our focus in this paper, ranging is not available like classic pulsed RADAR (by measuring the ToF) [31]. That is why seminal works on passive human activity classification [3], [15] use spectrograms of the received signal or the spectrogram of the CSI estimate that are features of the signal that can be estimated passively. We could envision for example that both the Doppler and AoA of the signal can be estimated if the passive receiver has deployed a phased array multi-antenna system as we demonstrated in [14]. In this case the passive receiver might be able to track the AoA but the Doppler spectrogram would still be smeared with the methods proposed in this paper. Only the bearing of the human could be estimated. For limiting the ability of such a more advanced

receiver to estimate the AoA one could deploy spectrum nulling methods which is a well-known technique in adaptive signal processing for RADAR systems [31].

VII. CONCLUSION

In this paper we presented a new approach protecting humans from disclosing the micro-Doppler signature of their movements in passive wireless RADAR systems. We proposed the insertion of artificial frequency variations in the transmitted signal for smearing the passively estimated spectrogram of the received signal. We investigated two approaches that serve equally well the desired goal. The proposed idea can be used with minimal cost and overhead for protecting the privacy of wireless users from malicious unauthorized passive wireless receivers without any impact on digital communication performance.

REFERENCES

[1] F. Adib and D. Katabi, "See through walls with WiFi!" *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 75–86, Aug. 2013.

[2] S. Dai, A. Tongaonkar, X. Wang, A. Nucci, and D. Song, "NetworkProfiler: Towards automatic fingerprinting of Android apps," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 809–817.

[3] Q. Pu, S. Gupta, S. Gollakota, and S. Patel, "Whole-home gesture recognition using wireless signals," in *Proc. MOBICOM*, 2013, pp. 27–38.

[4] K. Ali, A. X. Liu, W. Wang, and M. Shahzad, "Keystroke recognition using WiFi signals," in *Proc. ACM MOBICOM*, 2015, pp. 90–102.

[5] M. Li, Y. Meng, J. Liu, H. Zhu, X. Liang, Y. Liu, and N. Ruan, "When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals," in *Proc. ACM SIGSAC CCS*. New York, NY, USA: ACM, 2016, pp. 1068–1079.

[6] Y. Wang, J. Liu, Y. Chen, M. Gruteser, J. Yang, and H. Liu, "E-eyes: Device-free location-oriented activity identification using fine-grained WiFi signatures," in *Proc. ACM MOBICOM*, 2014, pp. 617–628.

[7] G. Wang, Y. Zou, Z. Zhou, K. Wu, and L. M. Ni, "We can hear you with Wi-Fi!" in *Proc. ACM MOBICOM*, 2014, pp. 593–604.

[8] B. Chen, V. Yenamandra, and K. Srinivasan, "Tracking keystrokes using wireless signals," in *Proc. ACM MOBISYS*, 2015, pp. 31–44.

[9] D. Kosmanos, A. Argyriou, and L. Maglaras, "Estimating the relative speed of RF jammers in VANETs," *Secur. Commun. Netw.*, vol. 2019, Nov. 2019, Art. no. 2064348, doi: 10.1155/2019/2064348.

[10] A. Argyriou, "Joint estimation of the number of antennas and AoA of a wireless communication transmitter," in *Proc. IEEE Int. Symp. Phased Array Syst. Technol. (PAST)*, Boston, MA, USA, Oct. 2022, pp. 1–4.

[11] W. Li, M. J. Bocus, C. Tang, S. Vishwakarma, R. J. Piechocki, K. Woodbridge, and K. Chetty, "A taxonomy of WiFi sensing: CSI vs passive WiFi radar," in *Proc. IEEE Globecom Workshops (GC Wkshps*, Dec. 2020, pp. 1–6.

[12] F. Adib, Z. Kabelac, D. Katabi, and R. C. Miller, "3D tracking via body radio reflections," in *Proc. NSDI*, 2014, pp. 317–329.

[13] Y. Xie, J. Xiong, M. Li, and K. Jamieson, "MD-track: Leveraging multi-dimensionality for passive indoor Wi-Fi tracking," in *Proc. 25th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*. New York, NY, USA: Association for Computing Machinery, Aug. 2019, pp. 1–16, doi: 10.1145/3300061.3300133.

[14] A. Argyriou, "Passive angle-Doppler profile estimation for narrowband digitally modulated wireless signals," in *Proc. IEEE 12th Sensor Array Multichannel Signal Process. Workshop (SAM)*, Trondheim, Norway, Jun. 2022, pp. 246–250.

[15] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Understanding and modeling of WiFi signal based human activity recognition," in *Proc. 21st Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*. New York, NY, USA: Association for Computing Machinery, Sep. 2015, p. 6576, doi: 10.1145/2789168.2790093.

[16] L. Zhang and H. Wang, "Device-free tracking via joint velocity and AOA estimation with commodity WiFi," *IEEE Sensors J.*, vol. 19, no. 22, pp. 10662–10673, Nov. 2019.

[17] H. Rahbari and M. Krunz, "Friendly CryptoJam: A mechanism for securing physical-layer attributes," in *Proc. ACM WiSec*, 2014, pp. 129–140.

[18] F.-X. Socheleau and S. Houcke, "Hiding cyclostationarity with dispersive filters for covert underwater acoustic communications," in *Proc. 6th Underwater Commun. Netw. Conf. (UComms)*, Aug. 2022, pp. 1–5.

[19] A. Argyriou, "Secrecy in wireless communication through closed-loop receiver de-synchronization," *Phys. Commun.*, vol. 43, Dec. 2020, Art. no. 101195. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S187449072030272X

[20] A. Argyriou, "Range-Doppler spoofing in OFDM signals for preventing wireless passive emitter tracking," in *Proc. IEEE Radar Conf. (Radar-Conf)*, San Antonio, TX, USA, 2023.

[21] Y. Qiao, O. Zhang, W. Zhou, K. Srinivasan, and A. Arora, "PhyCloak: Obfuscating sensing from communication signals," in *Proc. NSDI*, 2016, pp. 685–699.

[22] *IEEE Draft Standard for IT—Telecommunications and Information Exchange Between Systems—LAN/MAN—Specific Requirements—Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications -ad 4: Enhancements for Very High Throughput for Operation in Bandsbelow 6 GHz*, document, Jun. 2012.

[23] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[24] K.-W. Yip, Y.-C. Wu, and T.-S. Ng, "Timing-synchronization analysis for IEEE 802.11a wireless LANs in frequency-nonselective Rician fading environments," *IEEE Trans. Wireless Commun.*, vol. 3, no. 2, pp. 387–394, Mar. 2004.

[25] W. Wang, S. He, L. Sun, T. Jiang, and Q. Zhang, "Cross-technology communications for heterogeneous IoT devices through artificial Doppler shifts," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 796–806, Feb. 2019.

[26] S. Vishwakarma, W. Li, C. Tang, K. Woodbridge, R. Adve, and K. Chetty, "SimHumalator: An open-source end-to-end radar simulator for human activity recognition," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 37, no. 3, pp. 6–22, Mar. 2022.

[27] J. G. Proakis and M. Salehi, *Communication Systems Engineering*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.

[28] R. Boulic, N. Magnenat-Thalmann, and D. Thalmann, "A global human walking model with real-time kinematic personification," *Vis. Comput.*, vol. 6, no. 6, Nov. 1990, Art. no. 344358, doi: 10.1007/BF01901021.

[29] S. An and U. Y. Ogras, "MARS: MmWave-based assistive rehabilitation system for smart healthcare," *ACM Trans. Embedded Comput. Syst.*, vol. 20, no. 5s, pp. 1–22, Sep. 2021, doi: 10.1145/3477003.

[30] S. An, Y. Li, and U. Ogras, "MRI: Multi-modal 3D human pose estimation dataset using mmWave, RGB-D, and inertial sensors," 2022, *arXiv:2210.08394*.

[31] M. A. Richards, *Fundamentals of Radar Signal Processing*. New York, NY, USA: McGraw-Hill, 2005.

ANTONIOS ARGYRIOU (Senior Member, IEEE) received the Diploma degree in electrical and computer engineering from the Democritus University of Thrace, Greece, in 2001, and the M.S. and Ph.D. degrees (Fulbright Scholar) in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2003 and 2005, respectively. Currently, he is an Associate Professor with the Department of Electrical and Computer Engineering, University of Thessaly. From 2007 to 2010, he was a Senior Research Scientist with Philips Research, Eindhoven, The Netherlands, where he led the research efforts on wireless body area networks. From 2004 to 2005, he was a Senior Engineer with Soft.Networks, Atlanta. His research interests include wireless communications, RADAR systems, and statistical signal processing theory and applications. He has served as a Guest Editor for the IEEE TRANSACTIONS ON MULTIMEDIA Special Issue on Quality-Driven Cross-Layer Design. He was also a Lead Guest Editor of the *Journal of Communications* Special Issue on Network Coding and Applications. He serves as a TPC member for several international conferences and workshops.

• • •