无源无线电雷达中人体微多普勒特征的混淆

Antonios Argyriou 色萨利大学电气与计算机工程系

arXiv:2303.03001v1 [eess.SP] 6 Mar 2023

摘要——无线通信信号照射到运动的人体时，会受到微多普勒效应的影响。无源接收机可以根据接收到的信号计算谱图，而谱图会因人体活动不同而呈现不同特征。若人体对此毫不知情，这便构成严重的隐私泄露。本文提出一种防止此类泄露的方法：在发射信号中注入频率变化，以混淆微多普勒特征。我们假设系统采用正交频分复用（OFDM），且无源接收机根据瞬时信道状态信息（CSI）估计谱图。我们分析了该方法对接收信号的影响，并提出两种策略，确保不会影响目标接收机对数字通信信号的解调。为评估该方法的性能，我们采用基于IEEE 802.11的OFDM系统和逼真的人体信号反射模型。

索引词—正交频分复用、微多普勒、802.11、无源 WiFi 雷达。

I. 引言

近年来，利用无线 Wi-Fi 信号进行无源跟踪、定位和活动检测的系统日益增多 [1]–[10]。这类系统的核心思想是从照射到人体的信号中提取微多普勒效应。在 Wi-Fi 系统中，有两类无源技术能够提取微多普勒，即基于信道状态信息（CSI）的系统和基于无源 WiFi 雷达（PWR）的系统。本文指出，尽管这类系统在许多应用中极为有用，但也可能使随处可见的无线接收机得以侵犯人体隐私：它们可以在我们不希望其检测人体活动时进行检测。为此，我们研究基于CSI的系统（正如后文将要说明的，这类系统更具风险），并提出一种方法，使发射机在需要时能够阻止接收机正确提取微多普勒效应。

大多数无源WiFi雷达系统都需要一个受系统控制的发射机，即该发射机是协作式的，并通过专用信道向无源接收机提供参考信号 [11]（图 1 左）。其他无源WiFi雷达系统，例如文献 [12], [13] 中的方案，则利用来自静止目标的反射信号作为参考波形；但与存在专用参考信道的情况相比，其人体活动分类性能欠佳。在早期的无源WiFi雷达系统中，通过将接收信号与参考信号进行相关来估计微多普勒，然后确定这种相关在不同候选多普勒值下何时达到峰值。较新的无源WiFi雷达系统研究则不需要

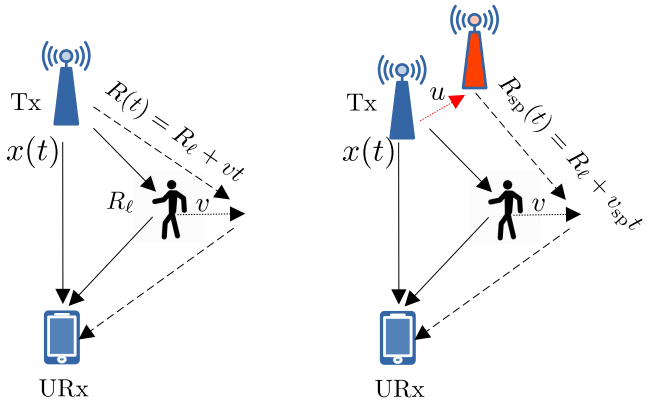


图 1：左：人体以某一速度移动，使路径长度变化 vt。右：采用所提出的方法后，伪造的路径长度（在信号中呈现的长度）为（$v + v_{sp}$）t，模拟了发射机物理移动至红色位置所产生的效果。

将反射信号用作参考，而是只需从发射信号中去除任何依赖于数据的相位/频率偏移，仅保留多普勒引起的频率变化 [14]。这能提高多普勒估计的准确性 [14]。总体而言，我们注意到，与信号发射机协作时，无源WiFi雷达系统的鲁棒性更强。如果我们想保护在 WiFi 接入点（AP）周围活动的用户隐私，就显然可以避免这种协作，从而使无源WiFi雷达系统更加安全。

与无源WiFi雷达系统不同，基于CSI的系统 [11], [15] 可能更具危险性。在这种情况下，接收机使用CSI估计值计算信号频谱图，从而识别独特的微多普勒特征。这类系统在准确估计微多普勒方面可能面临更多困难，但会带来严重的隐私威胁，因为任何未经授权的用户都可以部署这类系统，无需获得其所关联的AP的明确授权。如 [15], [16], 等研究所述，其基本原理是：人体运动会导致信号源到接收机之间多条反射路径的长度发生变化，进而使接收信号在某些频段上的功率发生变化（即信道频率响应（CFR） H（f, t））。如图 1（左）所示，人体运动时，第 ℓ条路径的长度会从 R_ℓ 变为 $R_\ell + vt$）。

需要注意的是，这类技术并不被视为对用户构成威胁，而是一种低成本的

方法，可支持多种应用。因此，人们很少关注如何对抗这些被动系统。现有文献中为数不多的相关系统，着重混淆与微多普勒无关的信号参数。例如，Friendly Cryptojam [17]可防止估计各种物理层参数（如调制类型），但无法防止估计多普勒，更无法防止估计人体反射信号中的微多普勒。过去有人提出在发射信号中加入人工频移，以阻止对手正确解调 [18]，但这一方法同样并非旨在防止估计微多普勒特征。与本文最相关的工作可能是 PhyCloak [19]，它通过一个与发射机同时发射信号的第三中继节点，扭曲无源接收机接收到的多普勒信息。然而，该系统始终需要一个与发射机同步的第三中继节点；更重要的是，它并未针对受微多普勒影响的人体反射信号。

如前所述，本文采取了不同的立场，认为这些系统可能会威胁隐私。在我们不希望其运行的情况下，应设法阻止恶意无线用户使用这些系统。因此，我们重点研究基于CSI的方案：机会接收机，即未授权接收器（URx），能够计算CSI及其随频率变化的短时间尺度变化，并通过谱图实现微多普勒估计。我们考虑一个使用正交频分复用（OFDM）的WiFi发射器，该发射器向目标接收机发射数字通信信号，但不希望其他人利用该信号进行微多普勒估计。在此设置下，我们提出通过在发射信号中插入人工频率变化效应来保护人类，避免其微多普勒特征被泄露，从而模糊真实的微多普勒效应。同时，人工信号不应影响信号解调。我们通过以下方式实现这一目标：向发射波形中注入低频调制（FM）信号，以模糊微多普勒特征；或者注入一种能够欺骗微尺度路径长度变化的信号，如图1所示，并在 [15]中进行了讨论。我们研究接收机处的接收信号和信道状态信息估计过程，然后考察上述两种信号结构对谱图的影响。

II. 信号模型

本文假设发射器（Tx）是静止的，即它是与之通信的合法网络中的一个基站（我们不研究该基站）。信号模型采用 802.11a/g/n/ac OFDM，并使用 20MHz信道 [20]。也可以支持移动发射机，但由此得到的表达式会更加复杂，却不会为本文的核心思想带来新的见解。802.11物理层帧前导码的详细信息见此处 [20]。本文需要了解的 802.11 帧结构基本要点是，每个帧的前导码由 7 个短且重复的已知 QAM 符号组成，这通常用于无线帧的前导码中。这些已知的符号值使接收机能够通过信道状态信息估计来估算信道状态信息，具体过程将在后文讨论。

入射到人体目标上的 WiFi OFDM 信号的单程时延随时间变化，且等于

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

其中， R_ℓ 和 $R_\ell(t)$分别对应运动前和时间 t 时第 ℓ条路径的长度（见图 1）。 v_ℓ是一种速度，会导致在时间 t内产生所谓的路径长度变化 [15] $v_\ell t$ 。人体移动时，其不同身体部位移动的距离和速度各不相同，因此汇总所有路径的影响后，会产生独特的微多普勒特征。

我们将考察发射信号 $x(t)$由多载波调制产生，尤其是采用正交频分复用（OFDM）时微多普勒的影响。设有 N 个子载波，相对于载波 f_c ，分布在 f_k=$k\Delta f$ 赫兹处，可承载数据、导频符号或二者的组合（具体取决于标准）；所需的连续时间基带 OFDM 符号为：

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

$X[k]$是调制到子载波k上的复数 QAM 符号， $T_N = N/\Delta f$ 是 OFDM 符号时长。

宽带时变信道在所有路径上的信道传输函数或信道频率响应（CFR）为

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

其中， $h_\ell(t)$是不包含多普勒效应的第 ℓ条路径的复数信道增益。时间 t处的信道冲激响应是时变的（参见第 21 [21]页）：

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

为推导接收信号，我们必须结合式 (2)、(3) 和 (4)。在被动式 URx 处，经由时变频率选择性信道传输后的接收基带连续时间信号，是信道冲激响应与所发送的正交频分复用信号的卷积。我们还包括

加性高斯白噪声（AWGN） $w(t)$，得到：

$$\begin{aligned} y(t) &= \int_{-\infty}^{\infty} h(\tau,t)x(t-\tau)d\tau + w(t) \\ &= \sum_{\ell} h_\ell(t)x(t-\tau_\ell(t)) + w(t) \\ &= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sum_{\ell} h_\ell(t)X[k]e^{j2\pi k\Delta f(t-\tau_\ell(t))} + w(t) \\ &= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} X[k]e^{j2\pi k\Delta f t}\sum_{\ell} h_\ell(t)e^{-j2\pi k\Delta f\tau_\ell(t)} \\ &\quad + w(t) \qquad (5) \\ &= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} X[k]e^{j2\pi k\Delta f t}H(k\Delta f,t) + w(t) \qquad (6) \end{aligned}$$

将 (3) 代入 (5)，可得到 (6)，这是我们将使用的输出信号的另一种形式。当信道频率响应不随时间变化时，对 (5) 应用离散傅里叶变换，可得到 (6)，即正交频分复用中广为人知的结果：信道由频率选择性衰落信道变为平坦衰落信道，也就是说，$Y(k\Delta f)=X[k]H(k\Delta f)$。当然，在实际应用中，信道频率响应随时间变化会导致载波间干扰 (ICI)。

为了得到另一种有用的表达式，我们也可以将 (1) 中的 $\tau_\ell(t)$ 代入 (5)。然后， $e^{-j2\pi k\Delta f\frac{R_\ell}{c}}$ 这一项（对于第 ℓ 条路径而言是恒定相位，即不以 t 为索引）可以与 $h_\ell(t)$ 合并，记作 $h'_\ell(t)$。于是我们有：

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

请注意，我们不对载波频偏（CFO）进行建模，因为我们发现它对最终谱图的影响很小。包含发射机中的 CFO 和人工频率变化的 OFDM 信号模型已在 [22] 中提出，如有需要，可与本文的思路结合使用。我们还忽略被动式 URx 中的采样时钟偏差（SCO），因为我们并不关心其正确解调 OFDM 符号的能力（即在匹配滤波器输出峰值处进行采样）。[1]

III. 微多普勒涂抹与欺骗

只要不影响 $x(t)$ 的解码，我们就可以设计具有任意所需形式的人工信号。我们将该信号在时域中表示为 $x_{\text{sp}}(t)$，而 $X_{\text{sp}}(f,\ t)$ 表示其傅里叶变换 (FT)。我们研究以下两种思路：方法*1*：采用频谱图涂抹实现子载波无关的微多普勒混淆。方法*2*：采用子载波相关欺骗来模拟路径长度变化。 需要注意的是，在这两种情形下，注入的信号都不会在正交频分复用帧的尺度上引入可观测的频移，因此不会妨碍希望对传输帧进行解调的名义接收器估计信道状态信息。IEEE 802.11 频率估计与补偿算法能够适应数百千赫兹的多普勒变化，远超本研究中人工信号所引入的变化范围 [24]。文献 [25] 研究了这一人工频率变化范围内正交频分复用的误码率性能，未观察到性能下降。

[1]关于如何针对 OFDM 解决这一问题，请参阅该主题的相关工作，例如 [23]。

A. 方法*1*：涂抹

采用第一种方法时，我们在传输信号中$x\ (t)$ 引入一个频率为几十赫兹的振荡正弦波，以涂抹处于这一范围内的人体运动所产生的微多普勒效应 [26]。请注意，我们不必重新创建特定的谱图，只需破坏能够揭示微多普勒与不同用户运动速度之间依赖关系的特征即可。

为了在发射机处生成最终信号，我们在离散傅里叶逆变换之前，使用包含 QAM 符号$X[k]$ 的信息信号对其重新调制，得到频域信号 $X_{\text{sp}}(f,\ t)$。在时域中，该信号被定义为一种频率调制（FM）波形，其最大瞬时频移为 δf，频率为 f_m，因此瞬时频率等于 $f_i(t)=f_c+\delta f\cos(2\pi f_m t)$ [27]。这使得实际的时域 FM扩散信号为：

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

因此，该波形会产生一个信号，使其在频域中以 f_m 赫兹的速率，在最大瞬时频率 $-\delta f$ 和 $+\delta f$之间扩展。其结果是，它会扩散该频率范围内的频域微多普勒特征。文献中的一个重要细节是，各人体部位运动的频率非常低，处于几赫兹的范围内 [26], [28]。因此，频率 f_m 的变化应高于这一数值，这意味着仅需几十赫兹的 f_m ，就能很好地扩散接收信号频谱图。

B. 方法*2*：路径长度变化欺骗

第二种方法是设想发射机实际移动时，信号会是什么样子。因此，这种技术更恰当地称为欺骗，而不只是混淆。请注意，我们只能欺骗相位变化，使其模拟发射机发生物理移动时（移动到图1（右）中的“新”红色位置）所产生的信号。接收信号必须满足：在相同的 t 秒时间内，图1所示的路径长度变化不是 $v_\ell t$ ，而是 $v'_\ell t$ ；也就是说，我们希望 URx 接收到以下信号：

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

这是我们希望 URx 接收到的一种信号形式，问题是如何生成它。

为得到上述结果，我们令 欺骗信号 等于 $x_{\text{sp}}^{(k)}(t) = e^{j2\pi k\Delta f \frac{v_{\text{sp}}}{c} t}$，从而得到式 (7)：

$$\begin{aligned} y(t) &= \sum_{k=0}^{N-1} \frac{X[k]x_{\text{sp}}^{(k)}(t)}{\sqrt{N}} e^{j2\pi k\Delta f t} \sum_{\ell} h_{\ell}^{'}(t) e^{-j2\pi k\Delta f \frac{v_{\ell}}{c} t} \\ &= \sum_{k=0}^{N-1} \frac{X[k]e^{j2\pi k\Delta f \frac{v_{\text{sp}}}{c} t}}{\sqrt{N}} e^{j2\pi k\Delta f t} \sum_{\ell} h_{\ell}^{'}(t) e^{-j2\pi k\Delta f \frac{v_{\ell}}{c} t} \\ &= \sum_{k=0}^{N-1} \frac{X[k]}{\sqrt{N}} e^{j2\pi k\Delta f t} \sum_{\ell} h_{\ell}^{'}(t) e^{-j2\pi k\Delta f \frac{v_{\ell}-v_{\text{sp}}}{c} t} \end{aligned} \tag{10}$$

通过比较（9）和（10），我们可以看到，对于第 ℓ 条路径，将感知到的路径长度变化为 $v_{\ell}^{'} = v_{\ell} - v_{\text{sp}}$。因此，在实际实现中，我们不会向每个子载波发送复符号 $X[k]$，而是发送 $X[k]x_{\text{sp}}^{(k)}(t)$，也就是一个与子载波和时间相关的项。在下一节中，我们将讨论这两种方法会如何影响 URx 用于频谱图估计的 CFR功率估计。

IV. CFR 功率的影响

首先，我们使用已知前导码 $X[k]$ 对该子载波的频域接收信号 $Y(k\Delta f)$ 进行匹配滤波，然后估计子载波 k 的 CFR 功率。由于欺骗信号的傅里叶变换为 $X_{\text{sp}}(f,\ t)$，因此 CFR 等于：

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

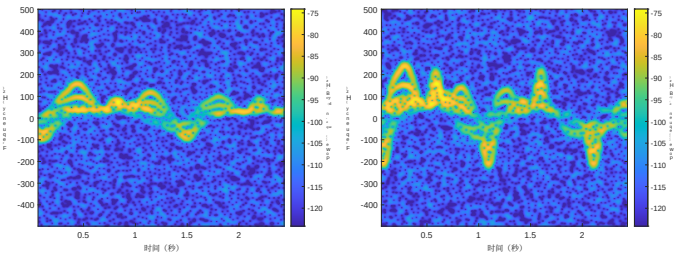
由上文可知，我们可以选择一种扩散或欺骗波形，使其能够完全改变上述 CFR 功率估计随频率或时间的变化。

方法1： 采用此方法，结果十分直观，因为信号与子载波无关。该方法只需将所得信号扩散至调频信号指定的带宽，从而混淆微多普勒效应。根据卡森定则，该带宽近似为 $2(\frac{\delta f}{f_m} + 1)$。

方法2： 现在我们分析 CFR 功率，即 $|X_{\text{sp}}(k\Delta f,\ t)H(f,\ t)|^2$，以了解其中的变化。文献 [15]，已研究过 CFR 功率 $|H(f,\ t)|^2$ 的表达式；但正如我们在式 (9) 中所见，路径长度现在会受到人为速度 v_{sp} 的影响。因此，我们按照 [15] 重新计算 CFR 功率；对于所有端到端路径的集合 $\mathcal{P}$，该式现在变为：

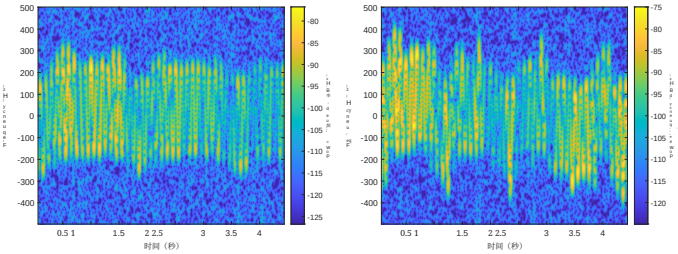
$$\begin{aligned} |X_{\text{sp}}(k\Delta f, t)H(k\Delta f, t)|^2 &= \sum_{\ell\in\mathcal{P}} D_1(f,t)\cos\left(\frac{2\pi v_{\ell}^{'} t}{c} + \frac{2\pi R_{\ell}}{c}\right) \\ &+ \sum_{\ell,m\in\mathcal{P},\ell\neq m} D_2(f,t)\cos\left(\frac{2\pi(v_{\ell}-v_m)t}{c} + \frac{2\pi(R_{\ell}-R_m)}{c}\right) \\ &+ \sum_{\ell\in\mathcal{P}} D_3(f,t) \end{aligned} \tag{12}$$

术语 D_1、D_2、D_3 取决于时间和频率，并且独立于通过速度 v_{ℓ}表示的路径长度变化。从这一表达式可以看出，CFR 功率是实际路径长度变化 $v_{\ell} - v_m$ 的函数，即



(a) 行人速度 0.8米/秒　　(b) 行人速度 1.5米/秒

图2：不同行人速度下，未经任何扩散处理的接收信号（OFDM离散傅里叶变换前）的谱图。



(a) 行人速度为 0.8m/s，带扩散——(b) 行人速度为 1.5m/s，带扩散——在方法1下的方法1

图3：不同的行人速度和方法1下的扩散条件下，接收信号（OFDM离散傅里叶变换前）的频谱图。

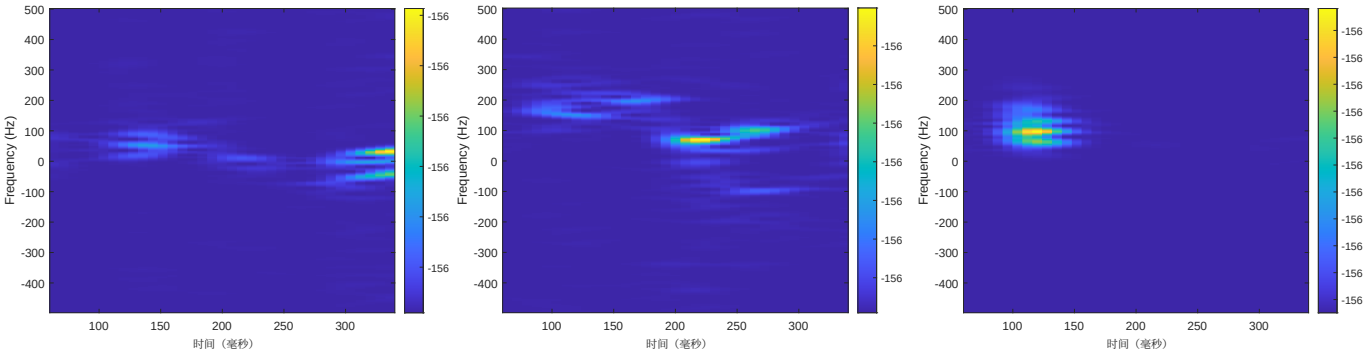
不会受到此类欺骗的影响，但也存在会受到影响的正弦项（在第一个求和式中）。最终结果是，正确的整体 CFR功率函数仍会因这种方法而失效。正如我们很快将看到的那样，与方法1相比，这对多普勒谱图的影响完全不同。

V. 结果

我们进行仿真的目的是评估这两种方法扩散人体运动多普勒特征的能力。我们考虑了一个基于802.11的OFDM系统，该系统使用20MHz信道，包含64个间隔为 Δf=312.5 kHz的子载波。其中52个为数据子载波，另有4个子载波用于导频信号。我们依据 [26], [28]中公开可用的模型，为以不同速度移动的行人生成特征。这些信道模型模拟人体不同部位的运动，并根据运动模式改变人体的横截面。

A. 方法1

为了更好地说明该方法的效果，我们发现，直接对接收信号本身计算谱图效果更好，也就是说，在将正交频分复用信号送入离散傅里叶变换进行解调之前计算。在图 2(a)、2(b) 中，我们展示了不同速度下人体移动且未采用任何微多普勒扩散的谱图结果。我们可以轻松看到不同速度下的微多普勒，以及出现在



（a）行人速度 0.8 米/秒　（b）行人速度 1.5 米/秒　（c）行人速度 0.8 米/秒及欺骗

图 4：方法2下，不同步行速度在未进行欺骗和进行微多普勒欺骗时，式（11）中的 CFR 功率谱图。

不同频率处的峰值。在图 3(a) 和图 3(b) 中，我们展示了行人分别以 0.8米/秒和 1.5 米/秒移动时采用扩散方法 1 的结果。显然，在这两种情况下，多普勒扩散方法都会将信号扩散到 $\delta f \approx \pm 200$ 赫兹的范围内，因此频谱图中不再具有任何可区分的特征。 f_m 设为 10 赫兹时，已经足以覆盖移动用户；该用户在图 2(a)、2(b) 的频谱图中呈现的峰值变化最快为 0.5 秒（2 赫兹）。用户以更高速度移动时，信号随时间变化会更加迅速，但仍可通过几十赫兹的 f_m 覆盖。

B. 方法2

对于方法2下的结果，我们使用离散傅里叶变换对每个 OFDM 符号进行解调，然后针对每个已使用的子载波，精细估计随时间变化的 CFR 功率。根据 802.11 前导码中的 OFDM 符号，对每个子载波的 CFR 功率进行估计，从而可以计算 $\left| \frac{X^*[k]Y}{|X[k]|^2} \left(k\Delta f \right)^2 \right|$，因为 $X[k]$ 是已知的。基于这一随时间变化的 CFR 功率估计，我们计算谱图，其分辨率为单个 OFDM 符号。

未进行欺骗时 CFR 功率谱图的相关结果见图 4(a)、图 4(b)，进行欺骗时的结果见图 4(c)。现在我们可以看到，对于相同的行人速度，我们能够在 URx 处生成不同的谱图，使其更接近于行人以更高速度移动时的谱图。此时，频率范围内不再出现一致的扩散，而是人体特征在频率和时间上的偏移，该偏移取决于路径长度变化$v_\ell' t$。v_{sp} 的不同取值会导致特征在谱图中的位置不同。

VI. 结论

本文提出了一种新方法，可保护人们在无源无线雷达系统中不泄露其动作的微多普勒特征。我们提出在发射信号中加入人工频率变化，以扩散对接收信号进行被动估计所得的谱图。我们研究了两种能够同样有效地实现这一目标的方法。该方案成本和开销极低，可用于保护无线用户的隐私，防止恶意的未授权无线用户侵害隐私，且不会对数字通信性能造成任何影响。

参考文献

[1] F. Adib 和 D. Katabi，“穿墙观察 WiFi！”*SIGCOMM Comput.Commun.Rev.*，第 43 卷第 4 期，第 75–86 页，2013年8月。[2] S. Dai、A. Tongaonkar、X. Wang、A. Nucci 和 D. Song，“Networkprofiler：迈向 Android 应用的自动指纹识别”，载于*2013 Proceedings IEEE INFOCOM*，2013年4月，第 809–817 页。[3] Q. Pu、S. Gupta、S. Gollakota 和 S. Patel，“使用无线信号进行全屋手势识别”，载于*MOBICOM*，2013年，第 27–38 页。[4] K. Ali、A. X. Liu、W. Wang 和 M. Shahzad，“使用 WiFi 信号进行击键识别”，载于*ACM MOBICOM*，2015年，第 90–102 页。[5] M. Li、Y. Meng、J. Liu、H. Zhu、X. Liang、Y. Liu 和 N. Ruan，“当 CSI 遇上公共 WiFi：通过 WiFi 信号推断您的手机密码”，载于*ACM SIGSAC CCS*。美国纽约州纽约市：ACM，2016年，第 1068–1079 页。[6] Y. Wang、J. Liu、Y. Chen、M. Gruteser、J. Yang 和 H. Liu，“E-eyes：使用细粒度 Wi-Fi 特征进行无设备、面向位置的活动识别”，载于*ACM MOBICOM*，2014年，第 617–628 页。[7] G. Wang、Y. Zou、Z. Zhou、K. Wu 和 L. M. Ni，“我们可以通过 Wi-Fi 听到你！”载于*ACM MOBICOM*，2014年，第 593–604 页。[8] B. Chen、V. Yenamandra 和 K. Srinivasan，“使用无线信号跟踪击键”，载于*ACM MOBISYS*，2015年，第 31–44 页。[9] D. Kosmanos、A. Argyriou 和 L. Maglaras，“估计车载自组织网络中射频干扰器的相对速度”，*Security and Communication Networks*，第 2019 卷，文章编号 2064348，2019年11月。 [在线]。可访问：https://doi.org/ 10 1155 2019 2064348 。/ / A. Argyriou, [10] “无线通信发射机天线数量与到达角的联合估计”，载于*IEEE International Sympo- sium on Phased Array Systems and Technology*，美国波士顿，2022年。[11] W. Li、M. J. Bocus、C. Tang、S. Vishwakarma、R. J. Piechocki、K. Woodbridge 和 K. Chetty，“WiFi 感知分类：CSI 与无源 WiFi雷达”，载于*2020 IEEE Globecom Workshops (GC Wkshps*，2020年，第 1–6 页。[12] F. Adib、Z. Kabelac、D. Katabi 和 R. C. Miller，“通过人体无线电反射实现三维跟踪”，载于*NSDI*，2014年。[13] Y. Xie、J. Xiong、M. Li 和 K. Jamieson，“Md-track：利用多维性实现室内被动 Wi-Fi 跟踪”，载于第*25* 届移动计算与网络国际年会，丛书号 MobiCom ’19。美国纽约州纽约市：计算机协会，2019年。 [在线]。可访问：https://doi.org/10.1145/3300061。3300133[14] A. Argyriou，“窄带数字调制无线信号的被动角度-多普勒轮廓估计”，载于*IEEE Sensor Array and Multi- Channel Signal Processing Workshop*，挪威特隆赫姆，2022年。

[15] W. Wang、A. X. Liu、M. Shahzad、K. Ling 和 S. Lu，“理解并建模基于 WiFi 信号的人体活动识别”，载于第*21*届移动计算与网络国际年会论文集，丛书号 MobiCom '15。美国纽约州纽约市：计算机协会，2015年，第 65–76 页。 [在线]。可访问：https://doi.org/10 1145 2789168 2790093 。/ . L. Zhang 和 H. Wang，“通过商用 WiFi 进行无设备跟踪：联合速度与到达角估计”，*IEEE* 传感器期刊，第 19 卷第 22 期，第 10 662–10 673 页，2019年。[17] H. Rahbari 和 M. Krunz，“Friendly Cryptojam：一种保护物理层属性的机制”，载于*ACM WiSec*，2014年，第 129–140 页。[18] A. Argyriou，“通过闭环接收机去同步实现无线通信保密”，《物理通信》，第 43 卷，文章编号 101195，2020年。 [在线]。可访问：https://www.sciencedirect.com/science/article/pii/S187449072030272X [19] Y. Qiao、O. Zhang、W. Zhou、K. Srinivasan 和 A. Arora，“PhyCloak：对通信信号中的感知进行混淆”，载于*NSDI*，2016年。[20] “面向信息技术、电信和系统间信息交换的 IEEE 标准草案 —— 局域网 / 城域网 —— 特定要求 —— 第 11 部分：无线局域网介质访问控制和物理层规范——修订版 4：在 6 GHz 以下频段运行时的超高吞吐量增强”，第 1–385 页，2012年6月。[21] D. Tse 和 P. Viswanath，“无线通信基础”，载于剑桥大学出版社，2005年。[22] A. Argyriou 和 D. Kosmanos，“OFDM 无线通信系统中的多普勒欺骗”，2022年。 [在线]。可访问：https: //arxiv.org/abs/2212 14241 。K.-W. Yip、Y.-C. Wu 和 T.-S. Ng，“频率非选择性莱斯衰落环境下 IEEE 802.11a 无线局域网的定时同步分析”，*IEEE* 无线通信汇刊，第 3 卷第 2 期，第 387–394 页，2004年3月。[24] W. Wang、S. He、L. Sun、T. Jiang 和 Q. Zhang，“通过人工多普勒频移实现异构物联网设备的跨技术通信”，*IEEE* 无线通信汇刊，第 18 卷第 2 期，第 796–806 页，2019年。[25] A. Argyriou，“用于防止无线无源辐射源跟踪的 OFDM 信号距离-多普勒欺骗”，载于*IEEE Radar Conference (Radar- Conf23)*，美国得克萨斯州圣安东尼奥，2023年。[26] S. Vishwakarma、W. Li、C. Tang、K. Woodbridge、R. Adve 和 K. Chetty，“Simhumalator：用于人体活动识别的开源端到端雷达仿真器”，*IEEE* 航空航天与电子系统杂志，第 37 卷第 3 期，第 6–22 页，2022年。[27] J. G. Proakis 和 M. Salehi，通信系统工程，第 2 版。普伦蒂斯·霍尔，2002年。[28] R. Boulic、N. Magnenat-Thalmann 和 D. Thalmann，“具有实时运动学拟人的全局人体行走模型”，《视觉计算》，第 6 卷第 6 期，第 344–358 页，1990年11月。 [在线]。可访问：https://doi.org/10.1007/BF01901021