

面向无线感知模型的用户隐私保护方法研究

姜禹^{1,2,3}, 施祺¹, 丛洋¹, 胡爱群^{1,2,4}

¹ 东南大学网络空间安全学院 南京 中国 211189

² 网络通信与安全紫金山实验室 南京 中国 211189

³ 江苏省计算机网络技术重点实验室 南京 中国 211189

⁴ 东南大学移动通信国家重点实验室 南京 中国 210096

摘要 作为通信感知一体化关键技术之一, 基于 Wi-Fi 信道状态信息的无线感知技术展示了广泛的研究与应用前景, 能够实现更细粒度、更高灵敏度的人体活动识别, 适用于智能家居、移动健康监测等领域。然而, 无线感知技术的应用场景往往会涉及大量的个人隐私数据, 随之带来了安全问题。攻击者能够利用无线感知技术, 在未经用户同意的情况下追踪其活动习惯, 从而侵犯用户隐私。因此, 在设计无线感知系统时, 需要考虑安全隐私保护的问题。本文对无线感知模型的用户隐私保护问题进行量化分析, 通过对无线信号传播路径分解得到感知细粒度和感知信噪比两个量化因素, 用于分析模型的感知能力以及感知范围。由于感知细粒度无法直接测量, 本文提出一种基于多子载波复数比的量化因素提取方法, 通过读取信道向量的幅度和角度变化来获得感知细粒度理论值。实验结果表明, 基于多子载波复数比的量化因素提取方法可以更准确地识别人体动作, 并提升动作感知的鲁棒性。利用该提取方法得到的感知细粒度准确反映了感知系统能够分辨的最小动作, 感知信噪比准确反映了系统对某一动作的可感知范围。最后提出了无线感知模型的安全隐私风险评估算法以验证感知模型的安全性和隐私性, 通过对不同级别用户提供针对性的安全引导, 有效保障了感知场景的安全性与隐私性。

关键词 隐私保护; 无线感知; 动作识别; 子载波比

中图分类号 TP393 DOI号 10.19363/J.cnki.cn10-1380/tn.2025.09.01

Research on Security and User Privacy Protection Methods for Wireless Sensing Models

JIANG Yu^{1,2,3}, SHI Qi¹, CONG Yang¹, HU Aiqun^{1,2,4}

¹ School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China

² Purple Mountain Laboratories, Nanjing 211189, China

³ Key Laboratory of Computer Network Technology of Jiangsu Province, Nanjing 211189, China;

⁴ State Key Laboratory of Mobile Communication, Southeast University, Nanjing 210096, China

Abstract Within the landscape of integrated communication sensing, wireless sensing technology leveraging Wi-Fi channel state information has emerged as a pivotal tool with vast potential and extensive research and application prospects. Its capacity to discern finer nuances and exhibit heightened sensitivity in human activity recognition makes it a versatile asset across domains like smart homes and mobile health monitoring. However, the application scenarios of wireless sensing technology often involve vast amounts of personal privacy data, thus raising security concerns. Attackers can exploit wireless sensing technology to track users' activity patterns without their consent, thereby infringing upon user privacy. Therefore, when designing wireless sensing systems, the issues of security and privacy protection need to be considered. This paper quantitatively analyzes the user privacy protection issues of wireless sensing models. It decomposes the wireless signal propagation path to obtain two quantitative factors: sensing granularity and sensing signal-to-noise ratio (SNR), used to analyze the model's sensing capability and sensing range. Since sensing granularity cannot be directly measured, this paper proposes a method for extracting quantitative factors based on the ratio of multi-subcarrier complex numbers. It obtains the theoretical value of sensing granularity by reading changes in the magnitude and angle of the channel vector. Experimental results demonstrate that the extraction method based on the ratio of multi-subcarrier complex numbers can more accurately identify human actions and enhance the robustness of action perception. The sensing granularity obtained using this method accurately reflects the smallest action that the sensing system can discern, while the sensing SNR accurately reflects the system's perceptible range for a particular action. Finally, a security and privacy risk assessment algorithm for wireless sensing models is proposed to validate the security and privacy of sensing models. By providing targeted security guidance for users of different levels, the security and privacy of sensing scenarios are effec-

通讯作者: 姜禹, 博士, 东南大学副教授, Email: jiangyu@seu.edu.cn。

本课题得到国家重点研发计划项目(No. 2022YFB4300300)资助。

收稿日期: 2023-09-04; 修改日期: 2024-03-03; 定稿日期: 2025-08-20

tively safeguarded.

Key words privacy protection; wireless sensing; action recognition; ratio of subcarriers

1 背景

日益拥挤的信道资源, 对下一代移动通信提出了新的要求^[1]。其中, 通信感知一体化(Integrated Sensing and Communication, ISAC)成为一个重要的解决方案^[2]。未来的 6G 无线接入网络将集成传感功能, 传感功能不仅仅是作为辅助方法, 而且作为提供给大量用户的基本服务^[3]。目前的通感一体化方案中, 已经广泛研究并具有广阔前景的是拓展 Wi-Fi 通信信号的感知功能。

Wi-Fi 无线感知技术是非接触感知技术^[4]的重要组成部分, 利用人体动作对 Wi-Fi 信号传播的影响来实现感知功能。近年来基于 Wi-Fi 信号的非接触人体行为感知技术受到国内外研究者的广泛关注, 出现了跌倒检测^[5-8]、手势识别^[9-12]、步态识别^[13-14]、呼吸监测^[15-18]、室内定位^[19-22]等人体行为感知应用。这些技术在老人看护、室内环境监测、人机交互、身份识别、心理分析及健康管理等领域均具有较强的应用潜力。根据所分析的信号特征不同, Wi-Fi 感知技术又可以分为传统的基于接收信号强度指示(Received Signal Strength Indication, RSSI)的感知技术和新兴的基于无线信道状态信息(Channel State Information, CSI)的感知技术。基于 CSI 的感知技术克服了传统基于 RSSI 的感知技术的局限性, 如低精度、易受干扰等, 具有更高的灵敏度和鲁棒性。

RSSI 是一个衡量无线信号接收强度的指标, 由计算 Wi-Fi 所有信道中信号的平均功率获得。由于 RSSI 信息比较容易获得, 在 Wi-Fi 无线感知研究的早期, 研究人员大部分使用 RSSI 信息来进行人员室内定位的识别。最早由微软研究院的 Bahl 和 Padmanabhan^[23]提出了 RADAR 系统, 通过多站点的 RSSI 信息覆盖实现室内人员的定位。

与 RSSI 不同, CSI 包含了每个子载波的信道响应信息, 能够反映环境中多径效应给信号带来的改变。因此, 基于 CSI 的无线感知系统拥有更高的精密度, 不局限于定位应用, 而可以推广到各种颗粒度的人类活动识别上。

基于指纹的 CSI 无线感知方法是假设人类活动与接收到的 CSI 信号有着一一对应的关系, 即提取人类活动的 CSI 指纹信息, 这样动作感知的问题就转换为了模式识别的问题, 解决问题的重点步骤在于特征提取和分类识别算法。从原始数据提取特征

即人体动作指纹, 接下来需要利用不同的分类器来识别动作。对于高维特征空间的复杂问题, 简单分类器不容易产生满意的识别结果。因此, 可以采用机器学习技术来识别 CSI 变化的模式, 并将其与人类行为联系起来。常见的机器学习方法包括动态时间扭曲^[24-25]、支持向量机^[26-27]和隐马尔可夫模型^[28-29]等。

深度学习是机器学习算法的一种, 通过利用深度神经网络(如自动编码器、卷积神经网络、长短期记忆网络和受限玻尔兹曼机等)对数据进行分类, 已经广泛应用于图像识别和语音信号处理领域。用于解决长期依赖问题的长短期记忆网络(Long Short-Term Memory, LSTM)非常适合用于处理 CSI 时序数据。最近几年, 大量基于 CSI 的感知系统^[30-32]使用深度学习尤其是 LSTM 进行分类识别。

基于 CSI 的感知技术的优点之一是精度高和低风险性, 在行为识别、人体定位等领域有着广泛的应用, 但这也带来了许多安全和隐私问题。以下是一些与基于 CSI 的动作识别相关的安全问题:

(1) 隐私泄露: 基于 CSI 的动作识别可以推断出目标的活动轨迹、睡眠时间、出入时间等个人隐私信息。如果这些信息被滥用或泄露, 会对个人的隐私产生重大影响。如文献[9-12]所示, 已经有许多 Wi-Fi 传感应用可以推断粗粒度和细粒度的信息, 如日常活动、手势和按键。这些信息很容易泄露用户的重要隐私信息给恶意黑客和攻击者。此外, 由于 Wi-Fi 信号随时存在, 并且可以穿透墙壁, 受害用户可能没有意识到信息泄露。与图像和视频不同, Wi-Fi 信号不限于照明条件, 因此 Wi-Fi 感知非常容易被恶意利用, 从而对隐私和安全构成潜在威胁。

(2) 位置追踪: CSI 可以用于确定人体在特定空间中的位置^[19-20, 33-34]。攻击者利用这些数据进行目标的位置追踪, 从而导致个人安全问题。

(3) 恶意监视: 基于 CSI 的动作识别技术被恶意使用来监视人们的活动。例如, 入侵者可以利用这项技术获取他人的行为模式, 并在合适的时机实施犯罪行为。这与无线感知的鲁棒性和普适性目标产生冲突: 一方面, 无线感知需要降低信息泄露的风险; 另一方面, 又需要确保在不同情境下能够轻松地 Wi-Fi 信号中推断出所需的信息。

针对这些安全问题, 需要采取措施来加强安全性和保护隐私, 如数据加密、访问控制、安全传输协议、匿名化处理等。

针对物理层跨层安全与隐私保护问题, 文献[35]提出了基于强化学习的数据隐私保护解决方案, 旨在保护 6G 系统中的用户数据隐私。该方案使用强化学习算法来优化数据隐私保护策略, 以提高动态网络中的安全性能, 抵御智能攻击, 而不依赖于攻击模型。此外, 文章还提供了针对身份隐私、数据隐私和位置隐私的保护措施, 以应对 6G 系统中的各种攻击。但这种基于强化学习的数据隐私保护方法在实际的 6G 系统中可能面临一些局限性, 例如高通信开销, 多设备全局优化困难以及隐私数据可能泄露等。

对于 CSI 泄露个人位置隐私的问题, 文献[36]提出了一种技术, 在发射端对传输的 I/Q 样本进行修改, 利用不可逆的随机序列对 CSI 添加随机化信息, 以此达到扭曲 CSI 来保护用户的位置隐私的目的。该技术的局限性主要在于, 它只能防止基于 CSI 的定位攻击, 而不能防止其他类型的定位攻击, 例如基于信号强度指纹的定位攻击。此外, 该技术需要在发射端对传输的 I/Q 样本进行修改, 可能会对系统的性能产生一定的影响。

针对人类行为的隐私保护问题, 文献[37]提出了一种深度网络架构, 通过引入一个新的损失函数来实现其目的。该损失函数将所有分类器组合成一个单一的函数来计算整个网络的损失。通过在损失函数中区分每个分类器的正负权重, 通过故意扰动 CSI 数据, 使一部分分类器误分类, 而其他分类器仍然可以识别行为。这样使得所需保护的私人行为不会被一般分类器识别, 从而实现了隐私保护的目。但该方法存在 CSI 训练数据不足, 只能感知特定动作等局限性。

此外, 针对 CSI 感知系统的安全风险评估算法制定也很重要, 有助于发现和评估系统中潜在的安全风险, 以及采取适当的措施来保护系统和用户的安全。当前对于无线感知技术隐私保护方面的研究, 大多基于物理设备以及无线信道的相关特性, 使用专门的硬件设施^[38-39], 实际应用中不易实现。并且对无线感知技术的感知极限与感知边界等问题没有系统性、可量化的研究方案。本文对无线感知模型的用户隐私保护问题进行量化分析, 并提出了无线感知模型的安全隐私风险评估算法以验证感知模型的安全性和隐私性。

从上述分析可知, 目前基于 CSI 的无线感知技术还面临着采样数据不够均匀密集、缺少感知极限和感知边界理论、感知功能威胁安全和隐私、缺少较完善的 CSI 感知系统安全风险评估算法等问题。本文针对以上问题展开研究工作, 研究内容主要包括以下 3 个方面:

(1) 从 CSI 无线感知的原理出发, 基于传播路径

分解对 CSI 无线感知能力进行量化分析, 从目标因素和环境因素两个角度, 分别得到感知细粒度和感知信噪比两个量化因素, 对感知能力的精度和边界极限进行了研究。

(2) 提出了一种基于多子载波复数比的量化因素提取方法, 将子载波的复数形式相除以消除频偏误差, 选择多个子载波复数比结果作为动作特征, 同时包含幅度和相位信息, 能够在复平面中提取得到感知细粒度的理论值。感知细粒度和感知信噪比的理论值与实验结果相符合, 验证了感知能力量化和感知范围量化的合理性。

(3) 提出了 CSI 感知模型的安全隐私风险评估算法, 并给出安全动作引导的建议。在两个量化因素的分析、提取和验证的基础上, 考虑动作的隐私重要性因素和环境的嘈杂程度因素, 参考信息技术安全评价准则, 对 CSI 感知模型的安全隐私风险进行评估。可以根据评估结果采取相应的措施, 降低潜在的隐私泄露风险, 提高 CSI 感知模型的安全性。

2 CSI 无线感知的感知能力安全量化因素分析

对系统的无线感知能力进行量化, 主要考虑两种因素: 目标因素和环境因素。目标因素为感知体系能够感知到的最小动作幅度, 只与动作本身的幅度朝向等相关; 环境因素是感知体系能够感知到的最远距离, 只与感知系统中的位置相关。通过对这两个因素进行量化分析, 可以深入了解感知系统的感知能力, 从而揭示其中潜在的安全风险和隐私问题。

通过对模型进行量化分析, 可以发现潜在的安全风险和隐私问题, 并为后续的安全和隐私保护工作提供基础和指导。第 2 节从 CSI 无线感知的原理出发, 对无线信号的传播路径进行分解, 从目标因素和环境因素两个角度分析, 分别得到感知细粒度和感知信噪比两个量化因素。

2.1 CSI 无线感知原理

CSI 信道状态信息(Channel State Information, CSI)由多个子载波的信道频率响应组成, 可以描述无线信号在传播过程中受到的环境影响。在 IEEE 802.11n 协议中, 利用 OFDM 和 MIMO 技术, CSI 可以描述无线信号从发射端到接收端的传输方式, 解释了衰落、散射、衍射和功率衰减与距离的结合效应。通常, 接收端的信号向量 Y_i 可以用以下公式来表示,

$$Y_i = H_i X_i + N_i \quad (1)$$

其中, H_i 表示第 i 个子载波的信道增益, Y_i 和 X_i 分别表示第 i 个子载波的接收信号与发射信号, N_i 为对应的

高斯噪声。其中各个子载波的 CSI 可以表示为

$$\hat{H} = \frac{Y}{X} \quad (2)$$

其中, $\hat{H}$ 为无线信道中的信道频率相应(channel frequency response, CFR), CSI 是多子载波信道响应组合, 因此可以被分为不同的子载波组, CSI 矩阵 $\hat{H}$ 可以表示为

$$\hat{H} = [H(f_1), H(f_2), \dots, H(f_i)]^T \quad (3)$$

$H(f_i)$ 为第 i 个子载波的 CSI 复数值, 可以表示为

$$H(f_i) = |H(f_i)|e^{j\angle H(f_i)} \quad (4)$$

其中, $\angle H(f_i)$ 和 $|H(f_i)|$ 分别为每个子载波的相位和幅值。

大多数 CSI 感知都假设人体活动与接收的 Wi-Fi 信号之间具有一对一的映射关系, 这使得可以简单地从 Wi-Fi 信号中提取特征来识别相应的活动。然而, 这种假设是否在实际环境中成立并未得到探究, 因此只能在特定条件下实现较高的准确率。

2.2 目标因素的量化分析

在一个理想的 Wi-Fi 感知模型下, 静态环境中只有一个移动物体, 我们可以将到达接收器的信号路径分为两类: 动态路径和静态路径。

动态路径是由移动目标引起的信号路径, 静态路径分为直接路径(Line of Sight, LoS)和来自墙壁等静态物体的反射路径。将动态和静态路径表示为空间向量, 即动态向量 H_d 和静态向量 H_s , 从而引发信号变化, 对应信道信息的合成向量为 H_t , 如图 1 所示。

$$H_t = H_s + H_d \quad (5)$$

$$|H_t| = |H_s| + |H_d| + 2|H_s||H_d|\cos(\theta_s - \theta_d) \quad (6)$$

其中, H_d 和 H_s 分别表示动态向量 H_d 和静态向量 H_s 的角度。

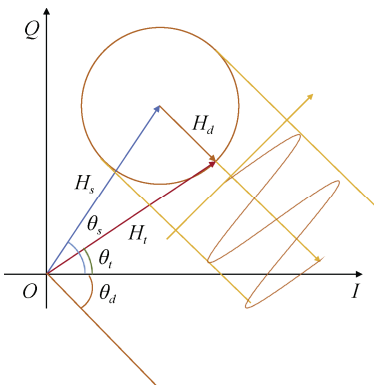


图 1 合成向量的分解示意图

Figure 1 Decomposition diagram of composite vectors

感知能力与动作带来的信号变化幅度有关, 如图 2, 从时刻 t_1 到 t_2 的信号变化幅度为

$$\Delta|H| = |H_{t2}| - |H_{t1}| = \frac{|H_{t2}|^2 - |H_{t1}|^2}{|H_{t2}| + |H_{t1}|} \quad (7)$$

其中, $|H_{t1}|$ 和 $|H_{t2}|$ 分别表示时刻 t_1 和 t_2 的信道信息合成向量的幅度。

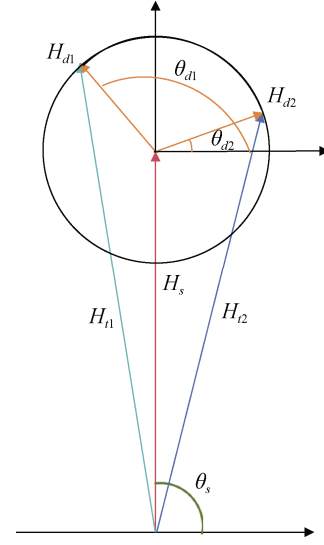


图 2 时刻 t_1 到 t_2 的信号变化的几何示意图

Figure 2 Geometric diagram of signal variation from time t_1 to t_2

当分析感知能力的细粒度时, 即小幅度动作感知, 可以认为 $|H_d| = |H_{d1}| = |H_{d2}|$, 因此,

$$\begin{aligned} \Delta|H| &= \frac{2|H_s||H_d|\cos(\theta_s - \theta_{d2}) \cdot 2|H_s||H_d|\cos(\theta_s - \theta_{d1})}{|H_{t2}| + |H_{t1}|} \\ &= \frac{4|H_s||H_d|\sin\left(\theta_s - \frac{\theta_{d2} + \theta_{d1}}{2}\right)\sin\left(\frac{\theta_{d2} - \theta_{d1}}{2}\right)}{|H_{t2}| + |H_{t1}|} \quad (8) \end{aligned}$$

其中, $|H_s|$ 是信息静态向量的幅度, $|H_{d1}|$ 和 $|H_{d2}|$ 分别是时刻 t_1 和 t_2 的信道信息动态向量幅度, θ_{d1} 和 θ_{d2} 为它们的角度。 $|H_{t1}|$ 和 $|H_{t2}|$ 分别是时刻 t_1 和 t_2 的信道信息合成向量的幅度。

对于人体动作识别来说, 人体自身移动形成的运动路径要远远小于人到感知设备的距离, 因此静态信道向量幅度远大于动态信道向量幅度, 即 $|H_s| \gg |H_d|$, 就有 $|H_{t1}| \approx |H_s|$ 和 $|H_{t2}| \approx |H_s|$ 。动态向量与静态向量的夹角 $\Delta\theta_{sd} = \theta_s - \frac{\theta_{d2} + \theta_{d1}}{2}$, 动作的幅度 $\Delta\theta_{d12} = \theta_{d2} - \theta_{d1}$, 代入式(8)后, 将感知细粒度 G 定义为

$$G = \Delta|H| = 2|H_d| \sin \Delta\theta_{sd} \sin \frac{\Delta\theta_{d12}}{2} \quad (9)$$

可以看出感知细粒度由以下几个因素决定: ①动态向量的大小 $|H_d|$; ②静态向量和动态向量之间的相位差 θ_{sd} ; ③由于细微运动 $\Delta\theta_{d12}$ 引起的动态向量的相位变化。

2.3 环境因素的量化分析

在实际的 Wi-Fi 感知中, 还需要考虑到环境中的噪声。

$$H(f, t) = H_s(f, t) + H_d(f, t) + H_n(f, t) \quad (10)$$

其中, $H(f, t)$ 表示当前环境的信道信息向量, $H_s(f, t)$ 和 $H_d(f, t)$ 分别表示信道信息的静态向量和动态向量, $H_n(f, t)$ 表示环境中的噪声。

在 Wi-Fi 通信系统中, 信噪比(Signal-to-Noise Ratio, SNR)用于量化通信质量的可靠性, 静态路径信号和动态路径信号都可以用于通信。而在 Wi-Fi 感知系统中, 只有动态信号中包含感知信息。而且动态路径信号的噪声和静态信号都会对感知造成一些负面的影响, 因此可以使用感知信噪比(Sensing Signal-to-Noise Ratio, SSNR)来对感知质量进行量化。

$$\text{SSNR} = \frac{P_d}{P_i} = \frac{|H_d(f, t)|^2}{|g(H_s(f, t)) + H_n(f, t)|^2} \quad (11)$$

其中, P_d 是接收信号的功率, P_i 是噪声的功率。 P_i 与静态信号功率成线性相关, g 表示线性相关函数。

接下来使用无线信号的传播模型推导动态信号与位置的关系, 动态信号的功率可以表示为,

$$P_d = \frac{P_t G_t G_r \lambda^2 \sigma}{(4\pi)^3 (r_T r_R)^2} \quad (12)$$

其中, P_t 为发射功率, G_t 和 G_r 分别为发射机和接收机的天线增益, σ 为目标的有效发射面积, λ 是信号波长, r_T 和 r_R 分别为目标到发射机和接收机的距离。

在自由空间传播下, 静态路径即为 LoS 路径,

$$P_{\text{LoS}} = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 r_D^2} \quad (13)$$

其中, r_D 为 LoS 路径的长度。又有 P_i 与静态信号功率成线性相关, 所以,

$$P_i = \gamma P_{\text{LoS}} + b = \gamma \frac{K}{r_D^2} + b \quad (14)$$

r 和 b 为线性相关的斜率和常数, 计 $K = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2}$, 最后,

$$\text{SSNR} = \frac{P_d}{P_i} = \frac{K\sigma}{4\pi(r_T r_R)^2 \left(\gamma \frac{K}{r_D^2} + b \right)} \quad (15)$$

对于给定的 Wi-Fi 设备, r 和 b 具有固定值。给定 Wi-Fi 收发设备对, 发射功率 P_t , 天线增益 G_t 和 G_r , 和信号波长 λ 可以看作是常数。 γ 和 b 也是常数, 可以提前测量。假设目标反射面积为常数且噪声很小(即 b 很小), 可以认为, SSNR 与 $\frac{r_D^2}{(r_T r_R)^2}$ 成正比, 即

$$\text{SSNR} \propto \frac{r_D^2}{(r_T r_R)^2} \quad (16)$$

3 CSI 感知量化因素的提取方法和验证

经过量化分析后, 得到感知细粒度与感知信噪比两个感知能力的量化因素。其中, 感知信噪比只与收发设备与感知目标三者的距离有关, 在实际场景中进行丈量 and 计算就可以得到。感知细粒度与信道向量的幅度和角度变化有关, 无法直接结算得到。第 3 节提出一个基于多子载波复数比的特征提取方法, 在此基础上能够在复平面中读取到角度变化值, 计算得到感知细粒度的理论值。最后, 经过多次实验验证感知细粒度和感知信噪比作为感知能力量化因素的合理性。

3.1 基于多子载波复数比的特征提取方法

CSI 记录了每个子载波的相位信息, 但是原始相位信息存在误差, 主要是接收机和发射机的中心频率往往不能精确同步, 接收机在下变频时, 往往会产生载波频率偏移(Carrier Frequency Offset, CFO), 另外 ADC 也会产生采样频率偏差(Sampling Frequency Offset, SFO)。

第 i 个子载波对应 CSI 的相位信息可以表示为

$$\hat{\varphi}_i = \varphi_i - 2\pi \frac{k_i}{N} \delta + \beta + Z \quad (17)$$

其中, φ_i 是真实相位信息, δ 是接收机的定时偏移, β 是未知的相位偏移, Z 是相位测量噪声。 k_i 表示第 i 个子载波的索引, N 是 FFT 的大小。

由于上述各种误差偏移的存在, 从 CSI 中提取出来的原始相位信息是不能直接拿来用的。一般在数据处理过程中, 会选择对相位进行线性变换处理, 来要消除掉 δ 和 β 部分的误差。

但是如果仅仅将固定间隔的子载波相位相减, 就可以直接消除 β 和 Z 的影响, 只与真实的相位信息相关, 并留下一个 $2\pi \frac{\Delta}{N} \delta$ 的偏移常数。

$$\Delta\varphi = \widehat{\varphi_{i+\Delta}} - \widehat{\varphi_i} = \varphi_{i+\Delta} - \varphi_i - 2\pi \frac{\Delta}{N} \delta \quad (18)$$

其中, $\Delta\varphi$ 表示相位的相减, 其实对应了复数相除, 直接将 CSI 的复数数据相除, 就能获得可以进一步处理的相位信息。

接下来, 以一组抬动手指的 CSI 数据为例, 采集时长为 30 秒, 共 3000 个数据包。

以第 23 位和第 27 位子载波为例, 将这两个子载波的复数数据进行相除, 即两个子载波 CSI 的复数比。

$$\begin{aligned} \text{CSI}_{\text{op}}(t) &= \frac{\text{CSI}_{23}(t)}{\text{CSI}_{27}(t)} = \frac{A_{23}(t)e^{j\varphi_{23}(t)}}{A_{27}(t)e^{j\varphi_{27}(t)}} \\ &= \frac{A_{23}(t)}{A_{27}(t)} e^{j(\varphi_{23}(t) - \varphi_{27}(t))} \end{aligned} \quad (19)$$

其中, CSI_{op} 表示两个子载波复数比后构造出的 CSI 复数序列, $\text{CSI}_{23}(t)$ 和 $\text{CSI}_{27}(t)$ 分别表示第 23 位和第 27 位子载波 CSI 复数序列, A_{23} 和 A_{27} 分别表示对应子载波 CSI 的幅度序列, φ_{23} 和 φ_{27} 分别表示对应子载波 CSI 的相位序列。对于重构的 CSI, 它的幅度和相位分别为

$$A_{\text{op}}(t) = \frac{A_{23}(t)}{A_{27}(t)} \quad (20)$$

$$\varphi_{\text{op}}(t) = \varphi_{23}(t) - \varphi_{27}(t) \quad (21)$$

记录第 23 位和第 27 位子载波的 CSI 复数信息, 将它们的复数形式进行相除, 记录复数比的幅度信息和相位信息, 即它们的幅度比值和相位差, 如图 3 所示。

由于采集到的相位信息与真实相位之间存在较大的偏差, 只观察采集到的相位信息, 很难对动作过程有清晰的判断。但是, 复数比的相位信息, 即相位差波形, 没有做任何处理的情况下, 已经能够很明显地看到对应动作的波动。

3.2 感知细粒度的提取方法

用 3.1 节中的预处理方法, 处理两个子载波复数比的幅度值和相位值, 将幅度和相位波形对应起来, 相当于重新构造了一个优化的 CSI 复数序列, 如图 4 所示。

图中, 蓝色波形分别为第 23 位和第 27 位子载波复数比的幅度和相位原始值, 红色波形为幅度和相位值经过预处理后的波形。

根据处理得到的幅度和相位值, 将以上优化重构的 CSI 数据点画在复平面上, 如图 5 所示。复平面上的波形将 CSI 数据反映的动作在空间中体现了出来, 很好地反应了感知目标抬动手指动作的真实情况。

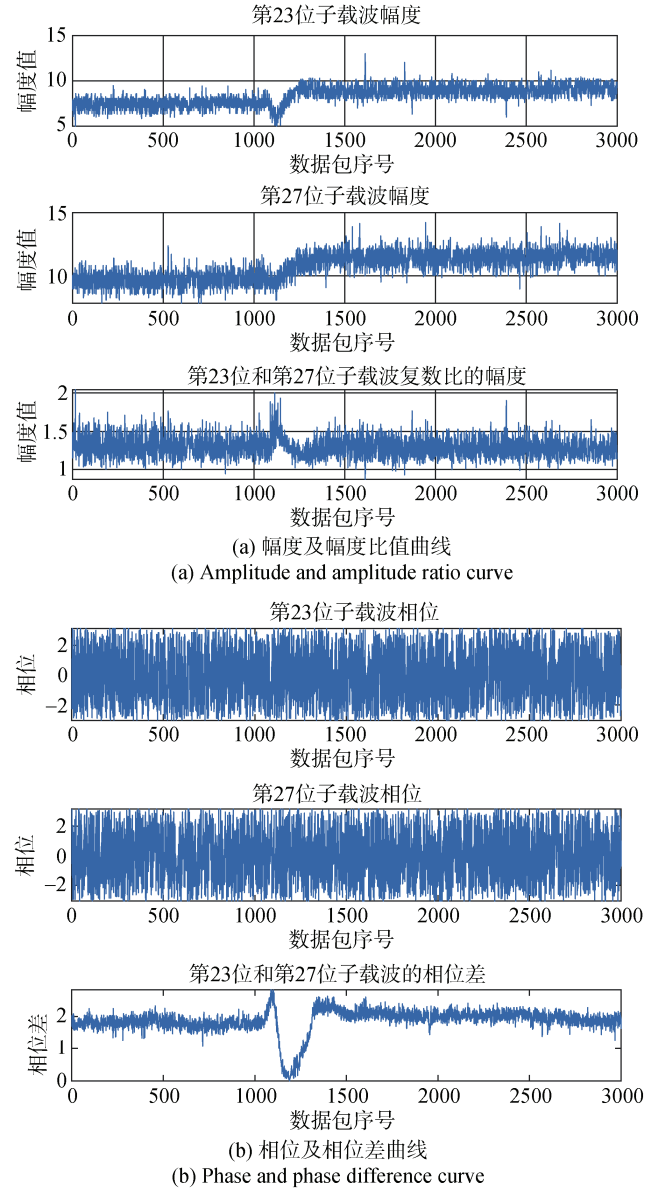


图 3 第 23 位和第 27 位子载波曲线图

Figure 3 Curve plots of the 23rd and 27th subcarriers

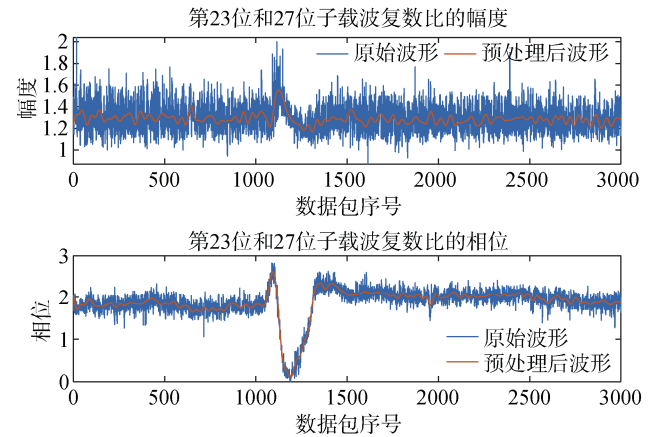


图 4 两个子载波复数比的幅度和相位曲线

Figure 4 The amplitude and phase curves of the complex ratio of two subcarriers

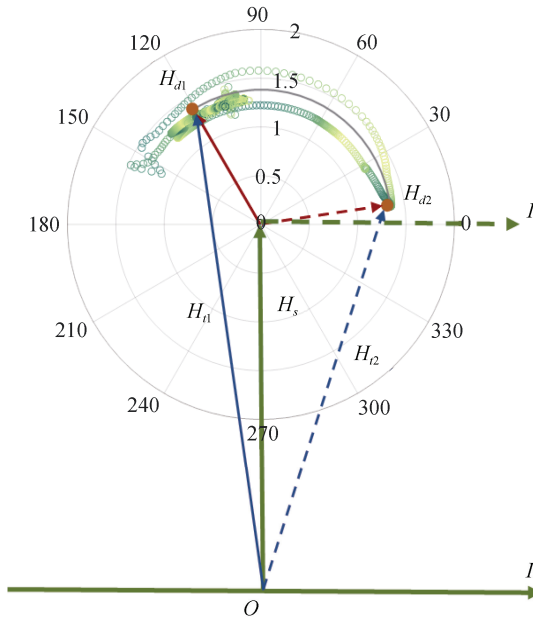


图 5 抬动手指前后的复平面示意图

Figure 5 Schematic diagram of the complex plane before and after lifting the finger

在复平面上将动作变化前后的信道向量标出来, 此时有 $\theta_s = 90^\circ$, 代入式(9)可得

$$G = |H_d| \frac{\sin \theta_2 - \sin \theta_1}{2} \quad (22)$$

根据夹角和幅值的读数, 可以计算出该动作对感知能力的理论值。因此, 子载波复数比的方法, 有助于感知能力的量化计算。

3.3 实验验证

3.3.1 实验设置与动作设计

实验系统使用华为 WS5100 路由器发送 CSI 信号, 使用 ESP32-S3 芯片接收 CSI 信号。通过在 ESP32-S3 上 Ping 路由器, 从路由器的返回信号中提取 CSI 信号。

华为 WS5100 路由器支持双频独立, 单口带宽为 100Mbps, 2.4GHz 和 5GHz 的总带宽达到 1000Mbps。实验环境中的其他计算机等设备大多数连接在 5GHz 的独立 Wi-Fi 上, 因此设定实验设备工作频率为 2.4GHz, 以减少其他工作设备对本实验的信道干扰。工作信道为信道 1, 信道带宽为 20MHz。

实验对象在收发设备的无线信号路径上, 系统将实现对象人体动作的无线感知。ESP32-S3 开发板与 PC 主机相连, 工作人员远程操作 PC, 以避免工作人员的活动对实验环境造成的影响。实验环境选择在较为空旷的大厅, 如图 6 所示。

实验数据在 PC 端处理获得, PC 配置为 Intel Core i5-7500、NVIDIA GeForce GT 730, 系统为 Windows 10 专业版 64 位。



图 6 实验环境

Figure 6 Experimental environment

为了验证系统的感知能力对位置的依赖性, 共选择了 4 个位置分别完成动作采集。位置 1、位置 2 与位置 3 下, 收发设备的距离较近, 为 340 cm。位置 1 位于收发设备连线的中点, 位置 2 与位置 3 处理收发设备连线中位线上, 距离中点分别为 160 cm 和 240 cm。收发设备的距离较远的情况下, 位置 4 为收发设备连线的中点, 收发设备间距离为 520 cm。

图 7 为 4 个位置的几何示意图。

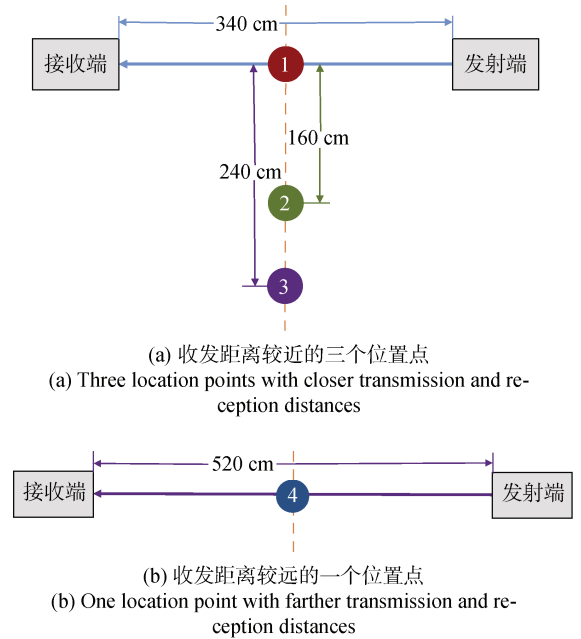


图 7 四个动作采集位置点的平面几何示意图

Figure 7 Planar geometric schematic diagram of four action collection location points.

实验过程中, PC 端调用乐鑫 esp-csi 项目中的 console_test 例程, 对接收到的 ICMP 包处理提取出 328 位的 CSI 信号, 后续处理中只需要其中 1~104 位的信息, 即 52 个子载波信息。

ESP32-S3 最小采集间隔为 10 ms, 持续采集 5 s, 保证实验对象完成一个简单动作。因此, 每个动作对应的单组数据格式为 500×104 的矩阵。

考虑到常见的智能家居场景, 本实验设计了 7

个动作, 分别为静态动作: 无人、坐、站立, 和动态动作: 走动、起立、挥手、踢腿。每个动作共采集 50 组数据, 一共 350 组数据, 每组数据持续 5 s。

七个采集动作中, “走动”规范为在收发设备连线的中位线上来回走动, 即走动数据的场景变化只与收发设备的位置有关。因此位置 1、位置 2 和位置 3 的走动场景相同, 不需要重复采集。静态动作的“无人”不需要人的动作, 只在位置点上放一把椅子。

3.3.2 基于 Bi-LSTM 的人体动作识别网络搭建

LSTM 神经网络只能在单个方向上处理连续的 CSI 数据, 即只考虑过去的 CSI 信息。在实际处理动作识别时, 未来的 CSI 信息也非常重要。例如, 站立和起立动作在活动前期的动作类似, 但后续的变化过程是不同的。在学习这些相似活动的动作特征时, 未来的 CSI 信息起着至关重要的作用。因此, 需要使用双向 LSTM(Bidirectional Long-Short Term Memory, Bi-LSTM)来同时考虑过去和未来的 CSI 信息, 以获得更准确的识别结果。

Bi-LSTM 是由两个 LSTM 模型反向连接组成的, 这种结构允许 Bi-LSTM 在处理时序数据时捕捉到更多的上下文信息, 从而更好地理解时序数据的动态演化过程。

以位置 1 的数据采集为例, 每个动作一共采集了 50 组数据, 使用前 30 组数据作为训练数据, 后 20 组数据作为测试数据。特征提取模块使用基于多子载波比的特征提取算法, 设定输入层大小为 k , 隐藏层参数为 N 。

首先以 $k=8, N=30$ 的参数为例, 进行一次完整的网络训练和测试, 训练时长为 1 分 21 秒, 识别结果如图 8 所示。

接下来需要通过多次实验尝试, 确定合适的隐藏层参数 N 和输入层大小 k 。

固定隐藏层参数 $N=30$, 即一共迭代 30 轮。设定输入层大小 k 取值集合为 $\{5, 6, 7, 8, 9, 10\}$, 每个 k 的取值上进行 6 次神经网络的训练和测试, 每次训练时间稳定在 80~86 s, 计算每次测试的识别准确率, 整理如图 9 所示。

箱型图显示了每组数据的中位数、上下四分位点和最大最小值。图 9 中, 每组数据的均值用红色圆圈标记并连接起来便于对比选取不同输入层大小的识别率。红色圆圈表示每组 k 值 6 次实验准确率的均值, 用直线相连表示准确率与 k 值的关系。网络的测试准确率随着 k 值的增大而增大, 斜率逐渐减小, 选定 $k=8$ 为该神经网络最合适的输入层参数。

混淆矩阵

输出类 \ 目标类	1	2	3	4	5	6	7	
1	20 14.3%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	100.0% 0.0%
2	0 0.0%	17 12.1%	0 0.0%	0 0.0%	0 0.0%	2 1.4%	1 0.7%	85.0% 15.0%
3	0 0.0%	0 0.0%	18 12.9%	0 0.0%	2 1.4%	0 0.0%	0 0.0%	90.0% 10.0%
4	0 0.0%	0 0.0%	0 0.0%	20 14.3%	0 0.0%	0 0.0%	0 0.0%	100.0% 0.0%
5	0 0.0%	0 0.0%	0 0.0%	1 0.7%	18 12.9%	1 0.7%	0 0.0%	90.0% 10.0%
6	0 0.0%	0 0.0%	0 0.0%	0 0.0%	1 0.7%	19 13.6%	0 0.0%	95.0% 5.0%
7	0 0.0%	0 0.0%	0 0.0%	0 0.0%	1 0.7%	0 0.0%	19 13.6%	95.0% 5.0%
	100.0% 0.0%	100.0% 0.0%	100.0% 0.0%	95.2% 4.8%	81.8% 18.2%	86.4% 13.6%	95.0% 5.0%	93.6% 6.4%

图 8 训练后的混淆矩阵

Figure 8 Confusion matrix after training

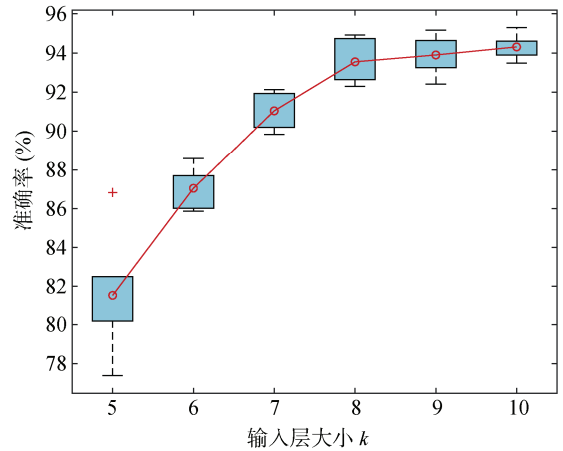


图 9 不同输入大小的网络测试准确率

Figure 9 Accuracy of network testing with different input sizes

继续尝试最适合该神经网络隐藏层的参数。固定输入层大小 $k=8$, 即选择方差最大的前 8 维相位差作为动作特征输入, 设定隐藏层参数 N 的取值集合为 $\{10, 20, 30, 40, 50\}$ 。

每个 N 的取值上进行 6 次神经网络的训练和测试, 以训练时间为横轴, 测试准确率为纵轴, 将测试结果整理在图 10 中。

图中, 不同颜色的圆圈分别表示 N 的不同取值下的测试准确率。黑色星号的坐标对应每组 N 值 6 次实验的训练时间均值和测试准确率均值, 用直线相连表示准确率与 N 值的关系。网络的测试准确率随着 N 值的增大而增大, 同时需要的训练时间也在

增加, 且斜率逐渐减小, 选定 $N=30$ 为该神经网络最合适的隐藏层参数。

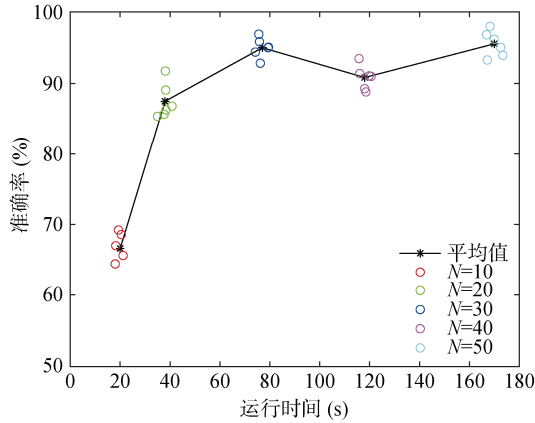


图 10 不同隐藏层参数的网络测试准确率

Figure 10 Accuracy of network testing with different hidden layer parameters

经过以上参数优化后, 选择训练网络都以 $k=8$, $N=30$ 进行训练。接下来在 2.4.1 节中设计的 4 个位置上, 对 7 种动作分别进行 40 次训练和识别, 一共 160 次实验结果。

3.3.3 感知细粒度的验证

结合前文中对感知细粒度的定义, 感知细粒度只与动作的幅度、速度和朝向等有关。计算每种动作的感知细粒度理论值, 并与实验结果的识别率均值相比较, 检查实验结果是否与理论计算值匹配。

整理 160 次实验的识别率, 每次实验中 7 个动作各有一个识别准确率。每种动作对应的 160 次实验结果作为列向量, 用不同的色块表示落在某识别率区间内的次数。比较不同动作的识别准确率, 如图 11 所示。七个动作分别为: 无人、坐、站、走动、起立、挥手、踢腿。

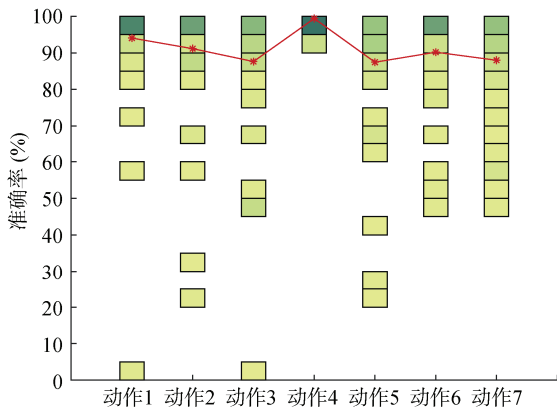


图 11 七种动作的识别准确率对比

Figure 11 Comparison of recognition accuracy for seven types of actions

使用色块表示落在某区间内的点数, 色块的颜色按点数呈线性渐变, 点数由 1 到 50 对应颜色由黄色到绿色, 没有涂色的区域上点数为 0。每组数据的均值用红色星号标记并连接起来便于对比不同位置的识别率。

从图 11 中可以看出, 动作 4 即“走动”的识别率结果分布较为集中, 都在 90% 以上, 识别率的均值也是七个动作中最高的, 明显高于其他几个动作的实验结果。动作 1 即“无人”的识别率结果也比较集中, 识别率均值仅次于动作 4 的结果。动作 3 “站”和动作 5 “起立”的识别率结果较低, 在多次实验的混淆矩阵中可以发现, 这两个动作的识别经常会发生混淆。

根据前文对感知细粒度的定义, 使用基于子载波复数比的特征提取算法, 在重构的复平面中得到动态向量和静态向量的相位变化。即 $\theta_s = 90^\circ$, 有感

$$\text{知细粒度 } G = |H_d| \frac{|\sin \theta_2 - \sin \theta_1|}{2}.$$

表 1 七个动作对应的感知细粒度计算对比

Table 1 Comparison of perceptual fine-grained calculations corresponding to seven actions

动作	θ_1	θ_2	$ H_d $	$G = H_d \frac{ \sin \theta_2 - \sin \theta_1 }{2}$
无人	/	/	0	0
坐	48.32	84.42	0.19	0.0236
站	45.08	93.72	0.21	0.0304
走动	-54.15	74.59	10.36	9.1924
起立	-70.59	12.16	0.55	0.3173
挥手	-62.81	-28.70	0.41	0.0839
踢腿	16.09	30.99	1.27	0.1509

从表 1 中可以看出, 动作 4 即“走动”的感知细粒度明显大于其他动作, 对应实验中动作 4 的识别率也明显超过其他动作的识别率。动作 1 即“无人”实际上感知细粒度为 0, 实验中测量到的夹角和幅值是受到电磁造成影响造成的。由于动作 1 的感知细粒度为 0, 在数据集中与其他动作的差别较为明显, 实际实验时也有着仅次于动作 4 的识别率。其他五个动作的感知细粒度相近, 对应实验中的识别率也较为相近。

3.3.4 感知信噪比的验证

结合前文中对感知信噪比的定义, 感知信噪比只与系统中的位置有关。计算每个位置的感知信噪比理论值, 并与实验结果的识别率均值相比较, 检查实验结果是否与理论计算值匹配。

整理 160 次实验的识别率结果, 每个位置上进行 40 次实验的识别率结果作为一个列向量, 用箱型图表示。比较不同位置上的识别准确率, 在图 12 中用箱型图表示。

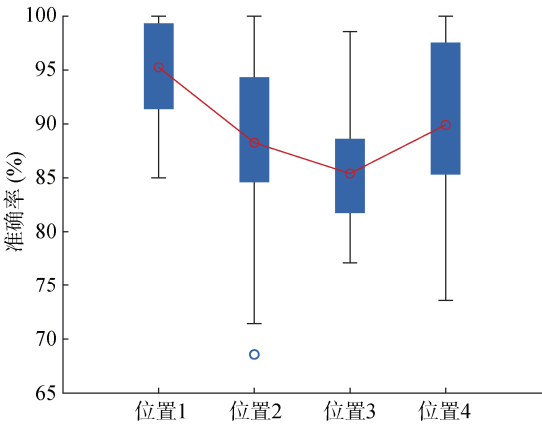


图 12 四个位置上的识别准确率对比
Figure 12 Comparison of recognition accuracy at four positions

箱型图显示了每组数据的中位数、上下四分位点和最大最小值。每组数据的均值用红色圆圈标记并连接起来便于对比不同位置上的识别率。从图 12 中可以看出, 位置 1 处的识别率最高, 位置 4 和 2 处次之, 位置 3 处识别率最低。

根据前文中对感知信噪比 S 的定义, 代入实物图中每个位置的距离, 对每个位置上的感知信噪比进行计算, 如表 2 所示。

表 2 四个位置上感知信噪比的计算对比
Table 2 Comparison of perceived signal to noise ratio calculation at four positions

位置	r_D	$r_T = r_R$	$S = \frac{r_D^2}{(r_T r_R)^2}$
1	3.4m	1.7m	1.38
2	3.4m	2.33m	0.39
3	3.4m	2.98m	0.15
4	5.2m	2.6m	0.59

从表中的结果得知, 四个位置上感知信噪比的大小关系为: $S_1 > S_4 > S_2 > S_3$, 与实际的识别率结果相符合, 进一步验证了感知信噪比定义的合理性。

4 CSI 感知系统的安全隐私保护模型

CSI 感知系统适用于智能家居、移动健康监测等领域, 会涉及大量的个人隐私数据。因此, 在设计 CSI 感知系统时, 需要考虑安全隐私保护的问题。本

文提出了基于 CSI 感知系统的安全隐私保护模型, 在对模型的感知能力量化因素进行分析、提取和验证的基础上, 参考信息技术安全评价准则, 提出一个 CSI 感知系统的安全隐私风险评估算法, 并根据算法提出对应的安全动作引导。

4.1 信息安全风险评估体系理论

信息技术安全评价准则(Information Technology Security Evaluation Criteria, ITSEC)是欧洲白皮书(Trusted Computer System Evaluation Criteria, TCSEC)的衍生标准之一, 于 1991 年由法国、英国、荷兰和德国四个国家联合发布。TCSEC 提出了信息安全的机密性、完整性、可用性的安全属性, 其中提出信息安全风险评估方程,

$$RISK = property \times threaten \times fragility \quad (23)$$

其中, $property$, $threaten$ 和 $fragility$ 分别为隐私泄露概率、威胁因子和脆弱性三个评估指标。隐私泄露概率指的是系统中存在的隐私泄露漏洞被攻击者利用的概率。威胁因子是指存在于系统中的威胁, 如攻击者、病毒、恶意软件等。脆弱性指的是系统中存在的漏洞或弱点, 攻击者可以利用这些漏洞或弱点实现攻击。通过对隐私泄露概率、威胁因子和脆弱性的评估, 可以得出系统的安全风险水平。评估结果可以为系统的安全保护提供指导和依据, 例如确定安全保护策略、制定安全策略、选择安全产品等。ITSEC 标准是信息安全领域中广泛使用的标准之一, 也是欧洲国家和其他一些国家在信息安全领域合作的基础。这些概念和方程为信息安全领域的研究提供了重要的理论依据。

4.2 安全隐私风险因素梳理

CSI 感知模型中的安全隐私主要与感知目标的动作习惯相关, 包括目标的出入时间、活动轨迹、睡眠时间等个人隐私信息。根据信息安全风险评估体系理论, 系统安全风险取决于隐私泄露概率、威胁因子以及脆弱性。类似的, CSI 感知系统中隐私风险的大小取决于感知能力的精确度, 感知目标动作的重要性以及感知环境的嘈杂程度, 这几个因素共同影响感知系统的安全和隐私风险。梳理 CSI 感知模型的安全因素, 本文对感知系统的感知能力因素、感知目标动作的重要性因素和感知环境的嘈杂程度因素分别进行评分。这几个安全因素与整体安全隐私风险的关系如图 13 所示。

感知系统的感知能力因素由感知细粒度和感知信噪比共同决定。感知细粒度指的是感知系统能够分辨的最小动作单位, 通常由动作本身的幅度、速度和朝向等因素决定。感知信噪比指的是感知系统接

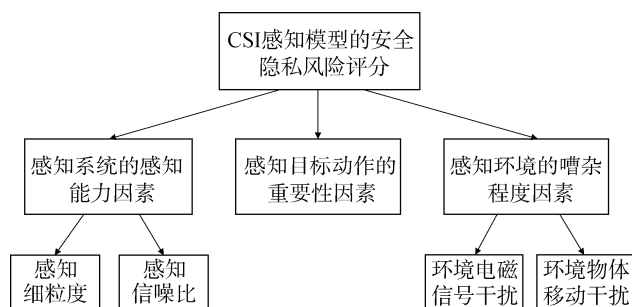


图 13 安全隐私风险的安全因素结构图

Figure 13 Structure diagram of security factors for security and privacy risks

收到的动作相关信号功率与其他信号功率的比值,通常与在系统中所处的位置相关。当感知信噪比低于某阈值时,认为该位置已经超出了感知系统的最大感知范围。

感知目标动作的重要性因素是指当前感知系统检测到目标动作的重要性和敏感程度。当感知系统用于监测个人行动,例如在家庭环境中,系统会记录到家庭成员的出入时间、活动轨迹、睡眠时间,容易造成个人隐私信息泄露。敏感性较高的行为信息泄露,如输入密码、步态习惯等,甚至会造成更加严重的后果。

感知环境的嘈杂程度因素包含了环境物体移动的干扰和电磁信号的干扰。物体移动产生的信号会被感知系统判断为感知目标的动作信号,从而干扰感知系统对人体动作的识别和分类。而电磁信号的干扰也会对感知系统的通信质量产生影响,从而降低感知系统的感知能力和准确性。

接下来, 将对感知系统的感知能力、感知目标动作的重要性以及感知环境的嘈杂程度这三个因素进行更详细的评分。

4.2.1 感知系统的感知能力评分

从第 2 节的分析中可知,感知系统的感知能力可以从目标因素和环境因素两个角度进行量化分析。

目标因素是指感知体系能够识别到目标对象的最小动作幅度，它是影响感知精度的重要因素。在安全隐私保护评估中，目标因素表示系统感知细粒度的能力，与感知目标动作带来的动态路径幅度和动态路径静态路径的夹角有关。 G 表示感知细粒度，由式(3-6)得到 $G = |H_d| \frac{\sin \theta_2 - \sin \theta_1}{\gamma}$ 。

环境因素是指某个位置上的感知信噪比,它是影响感知距离的重要因素。环境因素表示系统能够感知到的最远距离。 S 表示感知信噪比,由式(2-16)

得到 $S = \frac{r_D^2}{(r_T r_R)^2}$ 。

根据第三节的实验验证,感知细粒度越大,感知系统得到的动作信息越丰富,感知精度更高;感知信噪比越大,系统的感知范围也越大,即感知能力更强。因此,CSI感知系统本身的感知能力可以表示为

$$\begin{aligned} \text{Ability} &= \sqrt{G \times S} \\ &= \frac{r_D}{r_T r_R} \sqrt{|H_d| \frac{\sin \theta_2 - \sin \theta_1}{2}} \end{aligned} \quad (24)$$

以一次采集实验为例,采集环境中收发设备距离为 300 cm,感知对象处于收发设备连线的中点上,即 $r_D=3, r_I=r_R=1.5$ 。

对 2.3.2 节作为示例的抬动手指动作在复平面进行分析,如图 14 所示。

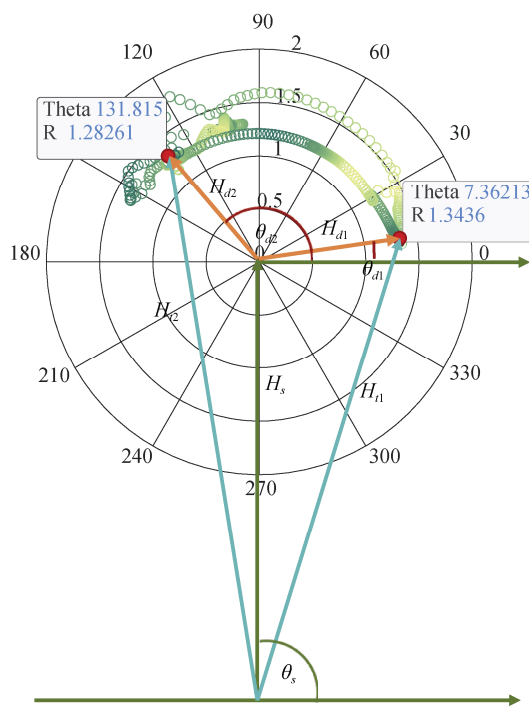


图 14 分析后抬动手指前后的复平面示意图

Figure 14 Schematic diagram of the complex plane before and after lifting the finger after analysis

从图中可以看出 $\theta_s=90^\circ$, $\theta_{d1}=7.362^\circ$, $\theta_{d2}=131.815^\circ$, $|H_{d1}|=1.344$, $|H_{d2}|=1.283$, 因此 $\Delta\theta_{sd}=20.41^\circ$, $\Delta\theta_{d12}=124.45^\circ$ 。因为抬动手指是一个小幅度动作, 动作前后的动作幅度大小相近, 取 $|H_d|=\frac{|H_{d1}|+|H_{d2}|}{2}=1.31$ 。

以上参数代入计算得到, $\text{Ability}_{\text{finger up}} = 0.848$ 。

一个感知系统的感知能力越强, 得到的动作信息越精细, 带来了更大的安全隐私风险。

4.2.2 感知目标动作的重要性评分

感知目标动作的重要性越高, 可能导致的安全隐私风险更大。

室内人员动作按隐私重要程度分级, 可以从以下几个方面来考虑。

(1) 高隐私重要程度: 这类动作涉及个人隐私信息的泄露, 如密码输入、银行卡密码输入、指纹识别等。这些动作涉及个人账户信息、财产信息、生物信息等重要隐私, 泄露可能导致个人信息被盗用或者其他不良后果。

(2) 中等隐私重要程度: 这类动作涉及个人的日常生活信息, 如通话、文字聊天、网络浏览等。这些动作可能包含了个人购买意向、生活习惯等隐私信息, 泄露可能导致用户信息被用于广告投放、个人信息监控等。

(3) 低隐私重要程度: 这类动作不涉及个人隐私信息, 如走路、坐下、伸手等。这些动作并不包含个人敏感信息, 泄露可能只会导致个人行为习惯被了解, 但并不会产生严重后果。

表 3 为基于隐私重要程度分级的评分。

表 3 基于隐私重要程度分级的评分

Table 3 Rating based on privacy importance grading

隐私重要程度	Imp 评分
高	5
中	2
低	1

综上所述, 室内人员动作按隐私重要程度分级是为了在隐私保护方面进行针对性的措施和安排。高隐私重要程度的动作需要更加严格的保护措施, 中等隐私重要程度的动作需要适当的保护措施, 低隐私重要程度的动作则不需要过多的保护措施。

4.2.3 感知环境的嘈杂程度评分

环境的嘈杂程度指感知目标所处环境中的各种干扰因素的综合影响程度。在感知系统中, 环境噪声是影响感知效果的重要因素之一。在环境噪声较大时, 即使感知系统本身的感知能力较强, 但也难以准确地识别到感知目标的行为。

为了更细致地描述环境嘈杂程度, 可以将环境噪声分成不同的级别。例如, 在室内环境中, 噪声可以被分为轻微、中等和严重三个级别。

(1) 轻微噪声包括非相邻信道的微弱电磁信号、背景噪声等, 会对感知系统的性能产生一定的影响;

(2) 中等噪声包括相邻信道的电磁信号、机器噪声等, 会对感知系统的性能产生较大的影响;

(3) 严重噪声包括大声喧哗、邻道大功率信号、物体较大移动变化等, 会对感知系统的性能产生极大的影响, 严重影响系统的准确性和可靠性。

目前的实验环境限制为一个室内环境, 且信号不穿墙, 即收发设备和感知目标都在一个房间内。认为环境噪声由环境电磁信号和环境物体移动构成,

$$Env = Elec + Mov$$

对于环境电磁信号 Elec 和环境物体移动 Mov 变量的评分见表 4 所示。

表 4 基于环境嘈杂程度的评分

Table 4 Rating based on environmental noise level

环境嘈杂程度	Elec 或 Mov 评分
严重	5
中等	2
轻微	1

因此, 在设计感知系统时, 需要根据具体应用场景和环境噪声的级别进行合理的参数选择和系统优化, 以保证系统在复杂的环境中具有良好的性能表现。

4.3 安全隐私评估算法

由于信息安全风险评估体系理论只是一个理论定义, 并没有明确的关于感知安全的安全隐私评估算法。本文从信息安全风险评估体系理论出发, 考虑上文中对感知系统的量化因素, 并加入其他目标和环境的重要程度变化, 提出了一个 CSI 感知系统的安全隐私保护评估算法。

$$PrvRisk = \frac{Imp}{Env} \times Ability \tag{25}$$

其中, Ability 表示 CSI 感知系统的无线感知能力, 由上文中的感知细粒度和感知信噪比共同决定; Imp 表示感知目标当前动作的重要性; Env 表示感知环境的嘈杂程度。

感知系统的无线感知能力越强时, 发生安全隐私泄露的风险概率越大; 感知目标动作的重要性越高时, 一旦发生安全隐私泄露, 产生的后果更严重; 感知环境的嘈杂程度越高时, 发生安全隐私泄露的风险概率越小。

根据以上因素的评分, 给出以下安全隐私评估算法的安全分级表 5。

接下来以两个场景为例, 计算感知系统的安全隐私风险评分并分级。

如图 15 所示, 场景一为放置桌椅柜子的办公室,

有其他人员移动。感知目标进行手机密码解锁动作。

表 5 感知系统的安全隐私风险分级

Table 5 Sensing system security and privacy risk classification

安全隐私风险评估评分	安全隐私风险分级
$[10, +\infty)$	高
$[4, 10)$	中
$(0, 4)$	低

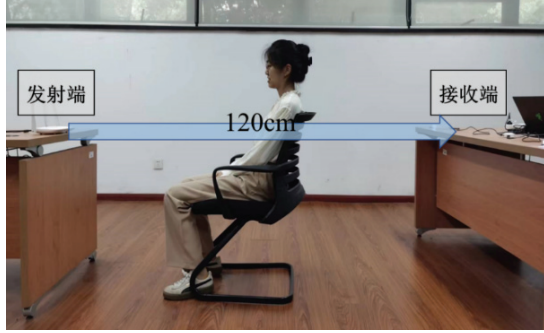


图 15 安全隐私风险评估场景一对应实物图

Figure 15 Security and privacy risk assessment scenario one corresponds to physical images

收发设备之间距离为 120cm, 目标处于收发设备连线的中点上, 线性关系函数的倍率为 10, 因此该位置的感知信噪比为 $S = \frac{10r_D^2}{(r_T r_R)^2} = 111.1$ 。系统进行感知时, 感知目标拿起手机进行密码解锁动作, 动作细粒度为 $G=0.373$ 。

感知系统的感知能力评分为 $Ability = \sqrt{G \times S} = 6.44$ 。目标动作的重要性高, 赋值为 $Imp=5$ 。环境中没有同频信号干扰, $Elec$ 赋值为 1; 办公室中有其他人员的移动干扰, Mov 赋值为 2, 环境的嘈杂程度评分为 $Env = Elec + Mov = 3$ 。

该场景的位置处, 目标进行手机密码解锁动作的安全隐私风险评分为 $PrvRisk = \frac{Imp}{Env} \times Ability = 10.73$, 根据表 5 中的分级, 属于高风险级别, 因此不建议目标继续进行动作。

场景二如图 16 所示, 空旷的大厅, 没有其他人员移动。感知目标进行挥手动作, 用以控制智能家居中设备的开关。

收发设备间距离 r_D 为 340cm, 感知目标在收发设备连线的中位线上, 与收发设备连线中点的距离 h 为 160cm, 设置线性倍率为 10, 该位置上的系统感知

信噪比为 $S = \frac{10r_D^2}{(r_T r_R)^2} = \frac{10r_D^2}{\left[\left(\frac{r_D}{2}\right) + h^2\right]} = 3.892$ 。系统进

行感知时, 感知目标进行一个挥手的动作, 感知细粒度为 $G=2.235$ 。

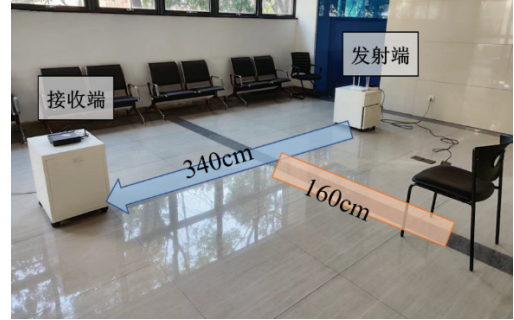


图 16 安全隐私风险评估场景二对应实物图

Figure 16 Security and privacy risk assessment scenario two corresponds to physical images

感知系统的感知能力评分为 $Ability = \sqrt{G \times S} = 2.949$ 。目标动作的重要性中等, 赋值为 $Imp=2$ 。环境中没有同频信号干扰, $Elec$ 赋值为 1; 大厅中没有其他人员的移动干扰, Mov 赋值为 1, 环境的嘈杂程度评分为 $Env = Elec + Mov = 2$ 。

该场景的位置处, 目标进行手机密码解锁动作的安全隐私风险评分为, $PrvRisk = \frac{Imp}{Env} \times Ability = 2.949$ 。根据表 5 中的分级, 属于低风险级别, 因此目标可以继续进行操作。

4.4 安全动作引导方法

在有了 CSI 感知模型的安全隐私风险评估算法的理论基础上, 当感知目标在进行隐私动作时, 需要对感知目标进行安全动作引导方法。首先, 我们需要判断感知目标是否将要进行隐私动作, 如进行手机屏幕解锁动作、输入重要密码等。当被感知的动作隐私重要性较高时, 才需要进一步的隐私保护措施。根据前文 4.2.2 节对感知目标动作的重要性评分 Imp 的定义, 只有评分为 5 时, 才认为动作的隐私重要性较高。

接下来需要判断感知目标在“感知能力场”所处的位置, 即判断对应的感知信噪比。

由前文 2.3 节的推导可知, 给定的 Wi-Fi 设备的参数固定, 可以认为感知能力与 $\frac{r_D^2}{(r_T r_R)^2}$ 成正比。其

中 r_D 为 LoS 路径的长度, r_T 和 r_R 分别为目标到发射机和接收机的距离。

如图 17 是一个在一对收发设备影响下的感知能力场, 图上的两个圆圈的圆心位置分别对应收发设备。在这个场景中, $r_D=8$, 设一个倍率为 10, 即

$$\text{Activity} = \frac{10r_D^2}{(r_T r_R)^2} = \frac{640}{[(x+4)^2 + y^2][(x-4)^2 + y^2]} \quad (26)$$

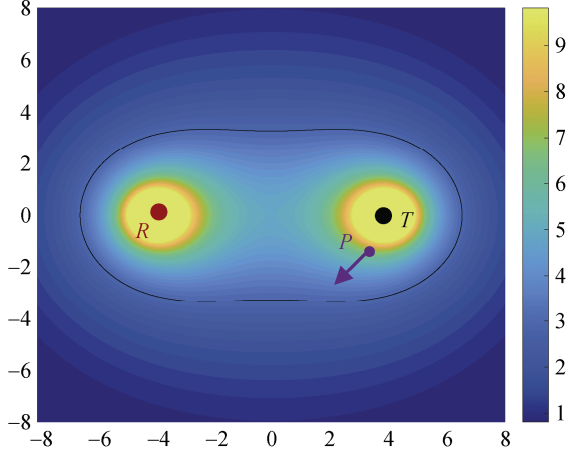


图 17 一对收发设备影响下的感知能力场示意图

Figure 17 Schematic diagram of perception ability field under the influence of a pair of transmitting and receiving devices

图中每条边界线上的感知能力相同, 相邻边界线的感知能力差相同。不同边界线的颜色根据感知能力的数值呈线性变化, 感知能力为 1 对应深蓝色, 感知能力为 10 对应黄色。相邻边界线间的区域, 根据内部边界线的颜色进行填充。

假设发射端 $T(4,0)$, 接收端 $R(-4,0)$, 感知目标 $P(2,-1)$, 那么感知目标的位置上的感知能力为 3.35。我们设置感知能力最大为 2 作为隐私保护的边界, 即感知目标需要从点 P 走到一个感知能力低于 2 的位置, 才能继续进行隐私动作。在图 17 中标注出了感知能力为 2 的边界线, 从点 P 走到边界线上的最短距离为 2.47 m。

在一对收发设备影响下的感知能力场中加入一个噪声点 $N(-1, -1)$, 受到噪声影响后的感知能量场发生变化。图 18 为一对收发设备和一个噪声源影响下的感知能力场示意图, 图中标注出了感知能力为 2 的边界线。从点 P 走到边界上的最短距离为 2.01 m。

综合上文内容, 可以看出系统的感知能力、目标动作的隐私重要性和环境的嘈杂程度给安全隐私保护带来的影响。

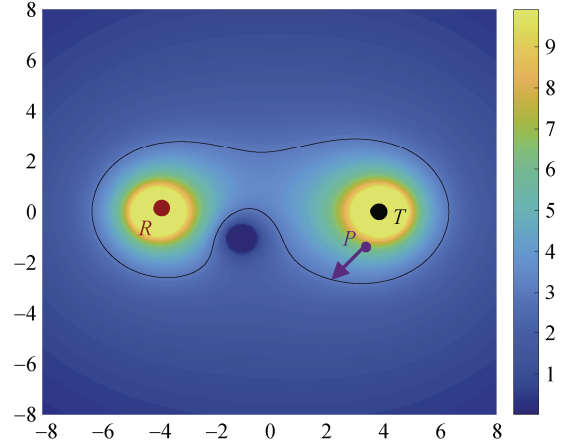


图 18 考虑单噪声源影响下的感知能力场示意图

Figure 18 Schematic diagram of perception ability field considering the influence of a single noise source

5 结论

本文实现了基于乐鑫嵌入式平台 ESP32-S3 的轻量级无线感知系统, 利用商用路由器, 在室内环境中对 7 种常见的简单人体动作进行离线识别。将 Bi-LSTM 神经网络适配到人体动作感知模型中, 在室内 LoS 场景下对 4 个位置上的 7 种动作数据进行学习和测试, 感知模型达到了 90% 以上的识别率均值, 在 CSI 无线感知的应用中具有较高的可行性。研究内容主要包括以下 3 个方面:

(1) 从 CSI 无线感知的原理出发, 基于传播路径分解对 CSI 无线感知的感知能力进行量化分析, 从目标因素和环境因素两个角度, 分别得到感知细粒度和感知信噪比两个量化因素。

(2) 提出了一种基于多子载波复数比的量化因素提取方法, 将子载波的复数形式相除以消除频偏误差, 选择多个子载波复数比结果作为动作特征, 同时包含幅度和相位信息, 能够在复平面中提取得到感知细粒度的理论值。感知细粒度和感知信噪比的理论值与实验结果相符合, 验证了感知精度量化和感知范围量化的合理性。

(3) 提出了 CSI 感知模型的安全隐私风险评估算法, 并给出安全动作引导的建议。在两个量化因素的分析与提取基础上, 考虑动作的隐私重要性因素和环境的嘈杂程度因素, 参考信息技术安全评价准则, 对 CSI 感知模型的安全隐私风险进行评估。可以根据评估结果采取相应的措施, 降低潜在的隐私泄露风险, 提高 CSI 感知模型的安全性。

本文在对 CSI 无线感知系统进行探究和具体实现的过程中, 在固定场景和单一感知目标的条件下得到了比较好的实验效果, 同时也存在更多新的研

究方向有待进一步研究:

(1) 位置依赖性问题。后续的研究中, 可以对子载波复数比的特征进行更深的研究, 并使用多个设备采集数据, 来抵消位置和朝向带来的信号差异。

(2) 跨场景识别问题。未来可以使用迁移学习等方法实现跨场景 CSI 数据的动作训练与识别, 提前训练好两个场景的转换函数, 使用转换函数将原场景的动作识别网络转换到新场景中使用。

(3) 实现 ESP32 的独立工作和实时识别。ESP32-S3 搭载 Xtensa 32 位 LX7 双核处理器, 配备有用于加速神经网络计算和信号处理等工作的指令, 完全可以将数据处理、训练和识别等操作转移到 ESP32-S3 内实现。

参考文献

- [1] Chaudhary S, Johari R, Bhatia R, et al. CRAIoT: Concept, Review and Application(s) of IoT[C]. *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 2019: 1-4.
- [2] Liu F, Cui Y H, Masouros C, et al. Integrated Sensing and Communications: Toward Dual-Functional Wireless Networks for 6G and beyond[J]. *IEEE Journal on Selected Areas in Communications*, 2022, 40(6): 1728-1767.
- [3] Pin Tan D K, He J, Li Y C, et al. Integrated Sensing and Communication in 6G: Motivations, Use Cases, Requirements, Challenges and Future Directions[C]. *2021 1st IEEE International Online Symposium on Joint Communications & Sensing*, 2021: 1-6.
- [4] Khalili A, Soliman A H, Asaduzzaman M, et al. Wi-Fi Sensing: Applications and Challenges[J]. *The Journal of Engineering*, 2020, 2020(3): 87-97.
- [5] Chen S, Yang W, Xu Y, et al. AFall: Wi-Fi-Based Device-Free Fall Detection System Using Spatial Angle of Arrival[J]. *IEEE Transactions on Mobile Computing*, 2023, 22(8): 4471-4484.
- [6] Ding J Y, Wang Y. A Wi-Fi-Based Smart Home Fall Detection System Using Recurrent Neural Network[J]. *IEEE Transactions on Consumer Electronics*, 2020, 66(4): 308-317.
- [7] Shi Z G, Zhang J A, Xu R Y, et al. Environment-Robust Device-Free Human Activity Recognition with Channel-State-Information Enhancement and One-Shot Learning[J]. *IEEE Transactions on Mobile Computing*, 2022, 21(2): 540-554.
- [8] Duan P S, Li J X, Jiao C F, et al. WiBFall: A Device-Free Fall Detection Model for Bathroom[C]. *Mobile Networks and Management*, 2022: 182-193.
- [9] Li C N, Liu M N, Cao Z C. WiHF: Enable User Identified Gesture Recognition with WiFi[C]. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020: 586-595.
- [10] Gao R Y, Li W W, Xie Y X, et al. Towards Robust Gesture Recognition by Characterizing the Sensing Quality of WiFi Signals[J]. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2022, 6(1): 1-26.
- [11] Ma X R, Zhao Y N, Zhang L, et al. Practical Device-Free Gesture Recognition Using WiFi Signals Based on Metalearning[J]. *IEEE Transactions on Industrial Informatics*, 2020, 16(1): 228-237.
- [12] Tan S, Yang J, Chen Y Y. Enabling Fine-Grained Finger Gesture Recognition on Commodity WiFi Devices[J]. *IEEE Transactions on Mobile Computing*, 2022, 21(8): 2789-2802.
- [13] Zhang Y, Zheng Y, Zhang G D, et al. GaitSense: Towards Ubiquitous Gait-Based Human Identification with Wi-Fi[J]. *ACM Transactions on Sensor Networks*, 2021, 18(1): 1-24.
- [14] Zhang L, Wang C, Zhang D Q. Wi-PIGR: Path Independent Gait Recognition with Commodity Wi-Fi[J]. *IEEE Transactions on Mobile Computing*, 2022, 21(9): 3414-3427.
- [15] Zhang D H, Hu Y, Chen Y, et al. BreathTrack: Tracking Indoor Human Breath Status via Commodity WiFi[J]. *IEEE Internet of Things Journal*, 2019, 6(2): 3899-3911.
- [16] Bao N, Du J J, Wu C Y, et al. Wi-Breath: A Wi-Fi-Based Contactless and Real-Time Respiration Monitoring Scheme for Remote Healthcare[J]. *IEEE Journal of Biomedical and Health Informatics*, 2023, 27(5): 2276-2285.
- [17] Li S T, Kristensen A T, Burg A, et al. ComplexBeat: Breathing Rate Estimation from Complex CSI[C]. *2021 IEEE Workshop on Signal Processing Systems (SiPS)*, 2021: 217-222.
- [18] Hussain M, Akbilek A, Pfeiffer F, et al. In-Vehicle Breathing Rate Monitoring Based on WiFi Signals[C]. *2020 50th European Microwave Conference (EuMC)*, 2021. DOI:10.23919/eumc48046.2021.9338026.
- [19] Abbas M, Elhamshary M, Rizk H, et al. WiDeep: Wi-Fi-Based Accurate and Robust Indoor Localization System Using Deep Learning[C]. *2019 IEEE International Conference on Pervasive Computing and Communications PerCom*, 2019. DOI:10.1109/percom.2019.8767421.
- [20] Hoang M T, Yuen B, Dong X D, et al. Recurrent Neural Networks for Accurate RSSI Indoor Localization[J]. *IEEE Internet of Things Journal*, 2019, 6(6): 10639-10651.
- [21] Wang F, Feng J W, Zhao Y L, et al. Joint Activity Recognition and Indoor Localization with WiFi Fingerprints[J]. *IEEE Access*, 2019, 7: 80058-80068.
- [22] Chen X, Li H, Zhou C Y, et al. Fidora: Robust Wi-Fi-Based Indoor Localization via Unsupervised Domain Adaptation[J]. *IEEE Internet of Things Journal*, 2022, 9(12): 9872-9888.
- [23] Bahl P, Padmanabhan V N. RADAR: An in-building RF-based user location and tracking system[C]. *Proceedings IEEE INFOCOM 2000. Conference on computer communications. Nineteenth annual joint conference of the IEEE computer and communications societies*

- ties, 2000, 2: 775-784.
- [24] Deng Z L, Fu X, Cheng Q Q, et al. CC-DTW: An Accurate Indoor Fingerprinting Localization Using Calibrated Channel State Information and Modified Dynamic Time Warping[J]. *Sensors*, 2019, 19(9): 1984.
- [25] Soto J C H, Galdino I, Gouveia B G, et al. Wi-Fi CSI-Based Human Presence Detection Using DTW Features and Machine Learning[C]. *2022 IEEE Latin-American Conference on Communications (LATINCOM)*, 2022. DOI:10.1109/latincom56090.2022.10000702.
- [26] Hao Z J, Yan Y, Dang X C, et al. Endpoints-Clipping CSI Amplitude for SVM-Based Indoor Localization[J]. *Sensors*, 2019, 19(17): 3689.
- [27] Ogawa M, Munetomo H. Wi-Fi CSI-Based Outdoor Human Flow Prediction Using a Support Vector Machine[J]. *Sensors*, 2020, 20(7): 2141.
- [28] Bai Y H, Wang X R. CARIN: Wireless CSI-Based Driver Activity Recognition under the Interference of Passengers[J]. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2020, 4(1): 1-28.
- [29] Cheng X Y, Huang B K. CSI-Based Human Continuous Activity Recognition Using GMM-HMM[J]. *IEEE Sensors Journal*, 2022, 22(19): 18709-18717.
- [30] Tian Y, Li S R, Chen C, et al. Small CSI Samples-Based Activity Recognition: A Deep Learning Approach Using Multidimensional Features[J]. *Security and Communication Networks*, 2021, 2021: 5632298.
- [31] He Z R, Xu G Z, Xu S Y, et al. A Robust CSI- Based Passive Perception Method Using CNN and Attention-Based Bi-Directional LSTM[C]. *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, 2022. DOI:10.1109/globecom48099.2022.10001549.
- [32] Tang Z L, Liu Q Q, Wu M J, et al. WiFi CSI Gesture Recognition Based on Parallel LSTM-FCN Deep Space-Time Neural Network[J]. *China Communications*, 2021, 18(3): 205-215.
- [33] Wu K S, Xiao J, Yi Y W, et al. CSI-Based Indoor Localization[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2013, 24(7): 1300-1309.
- [34] Yang Z, Zhou Z M, Liu Y H. From RSSI to CSI: Indoor Localization via Channel Response[J]. *ACM Computing Surveys*, 2013, 46(2): 1-32.
- [35] Lu X Z, Xiao L, Li P M, et al. Reinforcement Learning-Based Physical Cross-Layer Security and Privacy in 6G[J]. *IEEE Communications Surveys & Tutorials*, 2023, 25(1): 425-466.
- [36] Cominelli M, Kosterhon F, Gringoli F, et al. An Experimental Study of CSI Management to Preserve Location Privacy[C]. *The 14th International Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization*, 2020. DOI:10.1145/3411276.3412187.
- [37] Zhou S W, Zhang W, Peng D, et al. Adversarial WiFi Sensing for Privacy Preservation of Human Behaviors[J]. *IEEE Communications Letters*, 2020, 24(2): 259-263.
- [38] Cominelli M, Gringoli F, Lo Cigno R. AntiSense: Standard-Compliant CSI Obfuscation Against Unauthorized Wi-Fi Sensing[J]. *Computer Communications*, 2022, 185: 92-103.
- [39] Staat P, Mulzer S, Roth S, et al. IR-Shield: A Countermeasure Against Adversarial Physical-Layer Wireless Sensing, arXiv preprint arXiv:2112.01967, 2021.



姜禹 于 2009 年在东南大学信号与信息处理专业获得博士学位。现任东南大学副教授, 硕士生导师, 主要研究领域为无线感知、物理层安全。研究兴趣包括: 无线感知技术, 物理层安全, 无线网络安全, RFID 技术, 物联网技术等。Email: jiangyu@seu.edu.cn



施祺 于 2022 年在东南大学网络空间安全专业获得学士学位。现在东南大学网络空间安全专业攻读硕士学位。研究领域为无线感知。研究兴趣包括: 通信安全、Wi-Fi 感知。Email: seushiqi@163.com



丛洋 于 2023 年在东南大学网络空间安全专业获得硕士学位。研究领域为通信安全。研究兴趣包括: 无线通信安全、工控安全。Email: congyang42@foxmail.com



胡爱群 现任东南大学教授, 博士生导师, 主要研究领域为无线物理层安全、移动通信内生安全理论与技术。Email: aqhu@seu.edu.cn