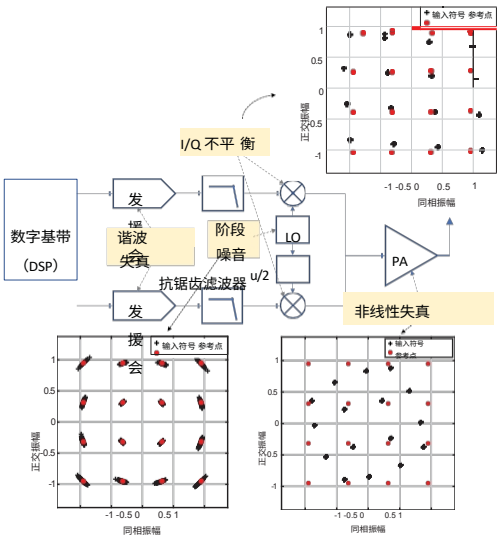
ORACLE：通过卷积神经网络优化无线电分析

库纳尔-桑克、毛罗-贝尔乔万、周凡、沙姆纳兹-里亚兹、斯特拉蒂斯-伊万尼蒂斯和考希克-乔杜里
美国马萨诸塞州波士顿东北大学电气与计算机工程系

本文介绍了 ORACLE 的架构和性能。ORACLE 是一种仅使用物理层 IQ 样本从大量比特相似设备（相同硬件、协议、物理地址、MAC ID）中检测唯一无线电的方法。ORACLE 可训练一个卷积神经网络 (CNN)，在计算时间和准确性之间取得平衡，在一个 16 节点 USRP X310 SDR 测试平台和一个包含 *>100* 个 COTS WiFi 设备的外部数据库中显示出 99% 的分类准确性。我们的工作做出了以下贡献：(i) 研究了导致 IQ 样本变化的发射机链内以硬件为中心的特征；(ii) 针对理想化的静态信道环境，提出了一种 CNN 架构，该架构只需要前端可访问的原始 IQ 样本，而无需信道估计或事先了解通信协议；(iii) 针对动态信道，展示了一种反馈驱动发射机侧修改的原则性方法，该方法利用接收器的 信道估计来提高 CNN 分类器的可区分性。这里的关键创新之处在于通过软件指令有意在发射器侧引入受控的不完美，同时最大限度地减少误码率的变化。与以往施加恒定环境条件的工作不同，ORACLE 采用 "一次培训，随处部署 "的模式，具有近乎完美的设备分类准确性。



I. 导言

感知无线频谱并识别相关频段内的活动无线电直接影响频谱的使用。本文利用机器学习检测嵌入在无线电发射电波中的特征参考信号，迈出了在共享频谱环境中区分无线电的第一步，这一过程被称为*射频指纹识别*。我们的目标是通过无线电硬件前端可利用的信息来实现这一目标。我们分别考虑了训练和验证之间信道未发生变化的情况（理想化）和信道动态变化的情况（实际情况）。我们的方法被称为 ORACLE，其关键创新之处在于它能学习信号通过发射机链时引入的同相（I）和正交相（Q）采样中存在的独特修改。ORACLE 使用卷积神经网络 (CNN) 通过制造过程中固有的随机性造成的设备特定变化来学习和识别单个无线电。这些所谓的*缺陷*存在于构成典型发射链的模拟组件（数模转换器、带通滤波器、混频器和功率放大器）中，即使无线电设备的制造商和品牌/型号相同，也会被区分开来。

图 1：带有各种射频损伤源的典型收发器链。

A. IQ 样本中包含的签名

无线电指纹识别涉及在协议栈中提取可用作设备签名的独特模式（或特征）。事实上，物理（PHY）层、介质访问控制（MAC）层和上层已被用于无线电指纹识别[1]。然而，IP 地址、MAC 地址、国际移动台设备标识（IMEI）号等简单的唯一标识符很容易被伪造。无线电信号强度（RSS）、到达角（AoA）和信道状态信息（CSI）等基于位置的特征容易受到移动性和环境变化的影响。ORACLE 则侧重于设备硬件构成中 固有的发射机特征，这些特征是不变的，恶意代理无法轻易复制。

图 1 显示了 16 QAM 星座中这些所谓发射机特征的示例场景（第三章将对其进行严格研究）。红圈表示由 I（x 轴）和 Q（y 轴）采样形成的理想星座点，黑叉表示由于特定类型的硬件缺陷而偏移的 实际星座点。实际的发射机具有这些偏移的组合，形成其独特的特征，不过我们在图中只显示了由 IQ 不平衡、非线性失真和相位噪声引起的三个图。ORACLE 的目标是通过以下方法学习并有意修改发射机上的部分特征

我们注意到，ORACLE 很容易与其他现有的更高层分类方法结合使用。我们注意到，ORACLE 可以很容易地与其他现有的更高层分类方法结合使用。

B. ORACLE 射频指纹识别的机器学习

机器学习（ML）技术已在图像和语音识别问题上大 显身 手 ， 并在无线领域的应用中稳步发展。ORACLE 完全建立在卷积神经网络架构上，该架构不仅在上述领域取得了成功，还曾用于调制[2]和协议识别[3]。ORACLE 采用分阶段方法实现实用分类。第一步，我们在外部获得的 100 多个 COTS WiFi 无线电数据集（并非所有数据都是比特相似的）上，以及在我们的测试平台（16 个比特相似的 USRP X310 无线电）上展示了 99% 的准确率，我们将这些无线电配置为生成的波形完全相似（相同的 802.11a PHY 帧、调制/协议/Mac ID）。

C. ORACLE 方法

对于在信道不变环境中运行的无线电（以下称为*静态*信道），ORACLE 仅使用原始 IQ 样本来识别无线电。它既不估计信道，也不使用所使用协议的任何先验知识。但是，如果无线电的工作环境发生变化，ORACLE 的性能就会下降。这是因为无线信道通常会对复平面上的 IQ 样本变换产生主要影响。当信道发生变化时（以下称为*动态*信道），ORACLE 将使用复杂解调符号而不是原始 IQ 样本进行训练。这种方法可以消除信道的影响，同时只保留硬件损伤的影响。我们在此发现了一个有趣的现象：使用解调符号进行训练可使低端 SDR （ 如 Ettus N210 USRP）对信道变化保持稳定。然而，使用可变性较低的元件制造的高性能 SDR（如 X310 USRP）则需要额外的步骤。对于此类高端比特相似设备，ORACLE 有一套原则性方法，可有意引入损伤以提高可区分性，同时最大限度地降低每个发射机的误码率 (BER)。这种方法的关键在于，在比特相似无线电中可控地 增加损伤，从而在接收器解调信号中产生一种独特的模式，这种模式与信道变化无关。

总之，本文的主要贡献是

- 我们研究了发射机侧参考信号的不同成因，并直观地展示了它们对 IQ 星座空间的影响。我们确定了可由接收机反馈利用软件 API 进行微调的具体特征。
- 利用 SDR 测试平台和包含 100 多个设备的外部数据库，我们提出了 ORACLE 的设计方案，其中包括一个稳健的 CNN 架构，仅使用原始 1/Q 样本就能在静态信道上返回*大于 99% 的*设备分类准确率。

表 I：用于设备指纹识别的机器学习方法

出版物	方法
富兰克林 *等人*[4]	用于无线设备驱动程序指纹识别的签名主数据库
Gao *等人* [5]	用于 AP 指纹识别的签名主数据库
肯尼迪 *等人*[6]	基于 k-NN 的发射机指纹识别
Brik *et al* [7]	基于 SVM 的网卡识别
Radhakrishnan *等人* [8]	基于 ANN 的无线设备识别
奥谢 *等人*[2]	基于 CNN 的调制识别
陈等人[9]	基于无限隐马尔可夫随机场的分类法
Nyugen *等人* [10]	基于无限高斯混合模型的设备分类

• 我们提出并在 USRP X310 无线电设备上实现了 ORACLE 的增强型设计，它系统地引入了受控损伤，以提高高端比特相似 SDR 的可区分性，同时确保将普通接收器的附加误码率降至最低。这是向 "一次训练，随处部署 "范式迈出的关键一步，该范式允许在现实信道变化条件下进行稳健的 CNN 学习。

II. 相关工作

虽然有关 ML 理论和应用的文献浩如烟海，但我们只回顾与射频指纹识别问题直接相关的工作，其中主要是监督学习。另一方面，无监督学习在没有设备的先验标签信息时非常有效。例如，文献[9]提出了一种基于无限隐马尔可夫随机场（iHMRF）的在线分类算法，利用无监督聚类技术和批量更新进行无线指纹识别。文献[10]使用了发射机特征，其中一种非参数贝叶斯方法（即无限高斯混杂模型）以无监督、被动的方式对多个设备进行分类。然而，在我们的方法中，我们为每个设备独立生成真实数据；因此，标注设备特定数据集是一项成本低廉的任务。有了基本真实数据，我们就可以创建模型，我们采用的是监督学习模式，即在部署网络之前，先收集大量已标注的样本进行训练。这种学习形式主要有两种方法：

A. 基于相似性

相似性测量包括将观察到的给定设备签名与主数据库中的参考进行比较。文献[4]提出了一种被动指纹识别技术，通过收集来自设备的探测请求帧轨迹，识别在符合 IEEE 802.11 标准的节点上运行的无线设备驱动程序。该技术采用有监督的贝叶斯方法来分析收集到 的轨迹并生成设备驱动程序指纹。Gao 等人[5] 描述了一种被动黑盒技术，该技术利用 TCP 或 UDP 数据包到达时间间隔，通过小波分析来确定接入点的类型。然而，这些技术依赖于对供应商特定特征的事先了解。

B. 基于分类

*1) 传统分类：*这种分类方式是利用系统的领域知识检查与预选特征的匹配情 况，即必须事先知道主要特征。肯尼迪等人[6]提出的分类方法是提取数据包中的已知前导码并计算频谱成分。一组对数光谱能量特征将作为 k 近邻（k-NN）判别分类器的输入。PARADIS [7] 使用 SVM 和 k-NN 算法，根据帧中特定的调制误差对 802.11 设备进行指纹识别，准确率高达 99%。文献[8]提出了一种利用人工神经网络进行物理设备和设备类型分类的技术，称为 GTID，该技术利用了设备的时钟偏移和硬件组成的差异。然而，由于使用了多种不同的特征，选择正确的特征集是一项挑战。当存在大量设备时，这还会造成可扩展性问题，导致训练计算复杂度增加。

*2) 深度学习*深度学习为复杂函数的学习提供了一个强大的框架，利用了大型数据集，并大大增加了层数和层内神经元的数量。O'Shea 和 Corgan [2] 以及 O'Shea 和 Hoydis [11] 将深度学习应用于物理层，特别侧重于使用 IQ 样本和卷积神经网络进行调制识别。他们对 11 种不同的调制方案进行了分类。不过，这种方法无法识别像 ORACLE 这样的设备，只能识别发射器使用的调制类型。在我们最初的工作[12]中，我们使用原始 IQ 样本和 CNN 来识别低端 SDR 无线电设备。

据我们所知，ORACLE 是第一个
可训练 CNN 进行比特相似设备识别

这样，同一个分类器就可以在未知/动态信道条件下工作，而无需进行新的试验。

III. 进一步了解设备签名

在本节中，我们首先研究射频硬件损伤，这些损伤会导致 IQ 样本的变化，从而形成每个设备的独特*特征*。我们将重点放在 IQ 不平衡和直流偏移上，这两种损伤 (i) 与环境无关，(ii) 不仅仅适用于特定的发射器-接收器对（与相对相位偏移等不同）。然后，我们将介绍一种在接收器上使用 GNU Radio UHD API 引入受控损伤的方法。随后，我们将解释用于跟踪数据收集的实验测试平台设置。

A.射频损伤

由于篇幅有限，我们的方法也可以扩展到其他方面。

- **IQ 不平衡：**正交混频器通常会因射频链中处理 I 信号路径和 Q 信号路径的并行部分之间的增益和相位失配而受损。增益不匹配会导致振幅不平衡，而相位不匹配则会导致 IQ 不平衡。

正交信号的相位偏离 90°，结果是
相位失衡。IQ 不平衡只随频率变化

由于低通滤波器与频率有关，因此它带有该频率发射机的独特特征。

- **直流偏移：**由于混频器的本地振荡器（LO）和射频端口之间的隔离度有限，LO 信号的直接馈入往往会耦合到输出端，因此会在正交混频器内部产生直流偏移。

B.基于软件的损伤控制

我们首先解释如何使用 Ettus 提供的自校准实用程序，利用 GNU 无线电功能在发射机链中设置 IQ 不平衡和直流偏移。

- ***IQ 失衡补偿*:** 设 $s(t) \in \mathbb{C}$ 为 t 时未受 IQ 不平衡失真影响的发送基带复信号。那么，时域中失真基带信号为

$$s_d(t) = \mu_t\, s(t) + \nu\, s_t^*(t)\text{、} \tag{1}$$

其中，失真参数 μ_t 和 ν_t 与发射机链中正交混频器 I 路和 Q 路的振幅和相位不平衡有关。

这些失真参数的简化模型可以写成： $\mu_t = \cos\theta_t/2$ $\alpha_t \cos\theta_t/2$ 和 $\theta_t \neq 2$ ，其中 α_t 和 θ_t 是振幅。

利用 MATLAB 通信系统工具箱，我们模拟了一个典型的无线通信处理链

和发射器 I 信号路径与 Q 信号路径之间的相位失衡。相位失衡是指与理想的 90° 相位的任何偏差。振幅不平衡为定义为$\frac{\alpha_I - \alpha_Q}{}$，其中 α_I 和 α_Q 分别是增益在 I 和 Q 路径上的振幅。

IQ 不平衡会在镜像频率上产生图像，从而对信号造成干扰。如图 2 所示，通过测量图像相对于所需信号的功(见图 1，接收到的复值 IQ 样本有偏移），然后修改理想运算模块，引入实际硬件实施中常见的射频损伤。这样，我们就能单独研究 IQ 不平衡、直流偏移、相位噪声、载波频率偏移和功率放大器的非线性失真。在本文中，我们将重点研究两种损耗（IQ 失衡和直流偏移）。

率（也称为图像抑制比 (IMRR) ）来量化这种干扰。IMRR 的计算方法是发送复正弦波 e^{jwt}，并计算图像频率（-w）和期望频率（w）的信号功率之比。因此，振幅不平衡 α_t 和相位差 θ_t 时的 IMMR 由以下公式给出：

$$IMRR = \frac{\gamma_t^2 + 1 - 2\gamma_t \cos\theta_t}{\gamma^2{}_t + 1 + 2\gamma_t \cos\theta_t}, \quad (2)$$

其中 $\gamma_t = \alpha_t + 1$。

虽然许多理论上的时域和频 域方法都可以补偿 IQ 不平衡，但我们使用的是埃图斯提供的 UHD 校准实用程序 `uhd_cal_tx_iq_balance`。它在一定频率范围内执行校准扫描，检查传输路径信号泄漏到接收路径的情况。

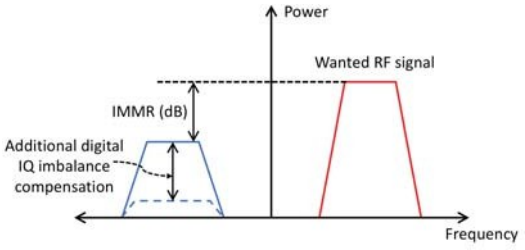


图 2：通过 IMRR 量化智商失衡的影响。

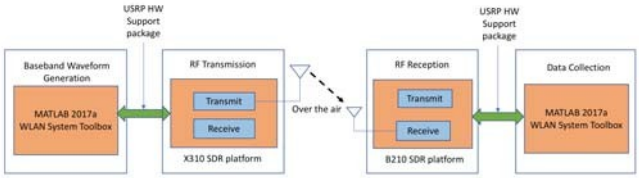


图 3：使用 SDR 收集数据的实验装置。表 II：使用 SDR 记录的 IMMR IQ 不平衡水平快照

`uhd_cal_tx_iq_balance` 实用程序

更正真实	修正图像。	主音的力量	的力量图像色调	IMMR （分贝）
-0.272	-0.636	-49.036	-66.138	-17.102
-0.636	-0.636	-48.852	-66.306	-17.454
-0.454	-0.0909	-49.091	-67.326	-18.235

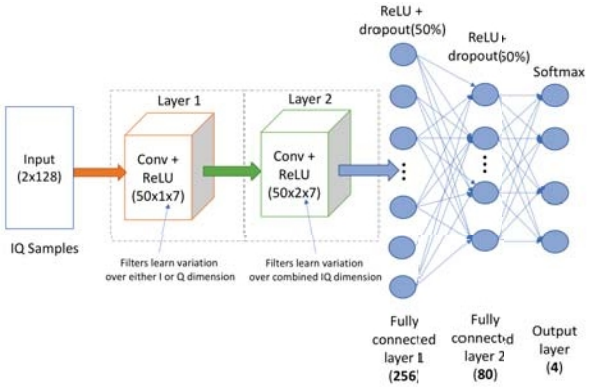
在运行时，UHD 软件会自动对射频子板的发射链进行校正，通常是一个单一的复合因子。在给定校正因子值的情况下，传输单频音调，并测量所需音调和图像音调的功率，以计算 IMMR。

我们修改了该实用程序，以记录校正系数和相应的 IMMR。表 II 显示了 USRP X310 无线电在 2.45 GHz 中心频率下记录的 IMMR 水平快照。

- ***直流偏移补偿***：直流偏移会导致频谱中心出现较大的尖峰。通过测量直流频率下主音的功率，我们可以确定直流偏移量。UHD 校准实用程序 `uhd_cal_tx_dc_offset` 使用一个单一的复合因子来校正直流偏移电平。它能找到最佳校正系数，使直流音 频 的功率最小。同样，通过修改实用程序，我们可以记录校正因子的直流偏移水平。

我们使用开源的 GNU Radio companion (GRC) 通过 SDR 传输符合标准的 IEEE 802.11a WiFi 包。利用 GRC 中的 `set_iq_balance` 和 `set_dc_offset` 函数，可以设置这两个独立的复杂校正因子，从而有意识地在无线电中引入所需的损伤水平。

C.痕迹数据收集的实验装置



我们使用从 USRP SDR 实验装置收集的 IQ 样本研究了 CNN 的性能，如图 3 所示，接收器为固定的 USRP B210。所有

图 4：我们提出的 CNN 架构包含两个卷积层和两个全连接层。

发射器是位类似的 USRP X310 无线电设备，可发射通过 MATLAB WLAN 系统工具箱生成的符合 IEEE 802.11a 标准的帧。生成的数据帧包含随机有效载荷，但具有相同的地址字段，然后流式传输到选定的 SDR，进行空中无线传输。接收器 SDR 以 5 MS/s 的采样率对输入信号进行采样，WiFi 的中心频率为 2.45 GHz。收集到的复杂 IQ 样本被划分为子序列。在实验研究中，我们将子序列长度固定为 128，即每次用于训练和分类的连续采样长度。总体而言，我们为每个无线电收集了 2000 多万个样本，随后将其分为训练集、验证集和测试集。

IV. 静态频道的 cnn 架构

A. 分类器架构

对于静态信道，我们设计了一种 CNN 架构，使用从 16 节点 USRP X310 SDR 测试平台和由 140 个 COTS WiFi 设备组成的外部数据库生成的原始时间序列 IQ 样本。我们提出的 CNN 架构如图 4 所示，部分灵感来自 AlexNet [13]。这是一种深度 CNN 架构，专门用于将 ImageNet 数据集中的 120 万张高分辨率图像分为 1000 个不同的类别。与由 8 层（5 个卷积层和 3 个全连接层）组成的 AlexNet 不同，我们的 CNN 架构由 4 层组成，其中包括 2 个卷积层和 2 个全连接层（或密集层）。CNN 的输入是长度为 128 的原始 IQ 样本窗口序列。我们选择了一种*滑动窗口*方法来分割训练样本，以增强 CNN 所学特征的移位不变性。每个复数值都用二维实数值表示（即 I 和 Q 是两个实数值流），这使得我们的输入数据维度增加到 2 × 128。然后，这些数据被输送到第一个卷积层。卷积层由一组空间滤波器（也称为*内核*）组成，对输入数据进行卷积运算以提取特征。第一个卷积层由 50 个滤波器组成，每个滤波器的大小为 1 × 7，其中每个滤波器在 I 或 Q 维上分别学习 7 个样本的时间变化，从而在 I 或 Q 维上生成 50 个不同的特征图。

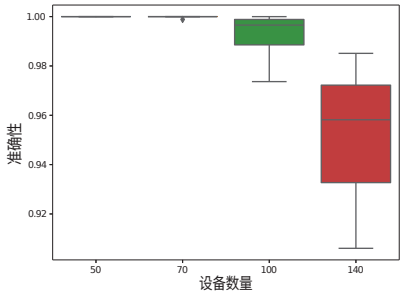


图 5：使用 CNN 对 WiFi 设备进行分类的方框图。

完整的输入样本。同样，第二卷积层有 50 个滤波器，每个滤波器的大小为 2 × 7，每个滤波器学习 I 和 Q 的变化，同样是 7 个激活值。

第一个卷积层之后得到的 50 维激活体积的维数。每个卷积层之后都有一个整流线性单元（ReLU）激活，对卷积输出的每个元素进行预先确定的非线性变换。

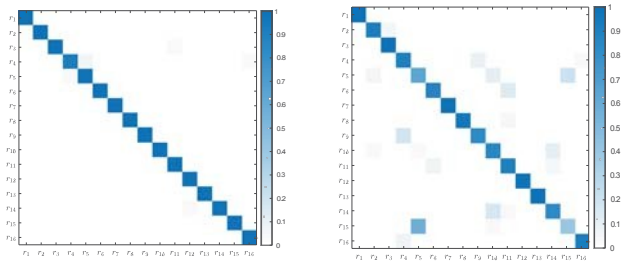
然后，将第二卷积层的输出作为第一全连接层的输入，该层有 256 个神经元。第二个全连接层有 80 个神经元，用于提取更高层次的非线性组合。

从前面各层提取的特征最终被传递到分类器层。最后一层使用*软最大*分类器输出每个样本输入 CNN 的概率。超参数的选择，如滤波器的大小、卷积层中滤波器的 数量以及 CNN 的深度，对于确保 CNN 模型具有良好的泛化能力非常重要。这些参数都是通过交叉验证精心选择的。为了克服过度拟合，我们将密集层的丢弃率设置为 50%。我们还使用了一个 l_2 正则化参数 $\lambda = 0.0001$。我们使用学习率为 $lr = 0.0001$ 的亚当优化器训练网络权重。我们使用分类交叉熵作为分类器输出计算的损失函数，通过反向传播使预测误差最小化。我们使用 Keras 实现了 CNN 架构，该架构在配备 8 个英伟达 Cuda Tesla K80m GPU 的系统上运行于 TensorFlow 之上。

B. 初步结果

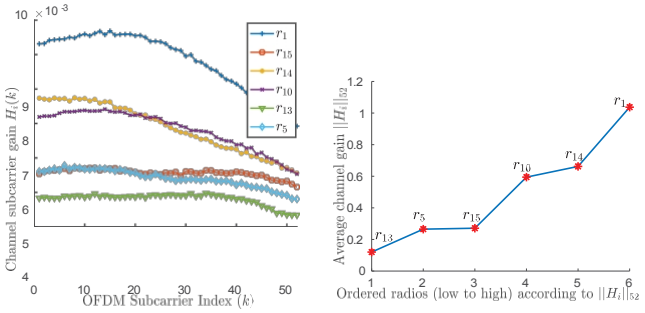
我们的初步评估旨在证明 ORACLE 的 CNN 架构在静态条件下对无线电进行分类的准确性，同时也激发了利用第 III-B 节所述技术对动态信道进行接收器反馈驱动修改的需求。

*1）静态信道条件下的准确性：*首先，我们使用外部数据库验证了我们提出的 CNN 在对 COTS WiFi 设备进行分类



(a) (b)

图 6：使用相同设备和不同位置进行的两次实验的混淆矩阵：(a) 整体准确率为 98.60%；(b) 整体准确率为 87.13%。



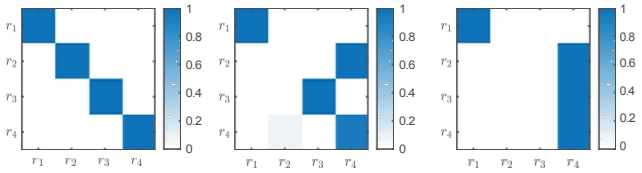
(a) (b)

时的性能，该数据库包含从 122 家制造商的 140 种设备（手机/平板电脑/笔记本电脑/无人机）中收集的标注 IQ 样本。对于每个设备，我们根据数据库中的可用样本，使用 4.5K 个加窗示例作为训练集，1K 个示例作为测试集。在每个训练时程中，每个设备都会使用由 300 个示例组成的验证集，以监测其性能。

图 7：(a) 每个无线电 $ri \in R$ 的 k^{th} 子载波的估计信道增益 $H_i(k)$ (b) 所有无线电 $ri \in R$ 的估计信道增益$\|H_i\|^2$（从低到高排序）。

如果连续 10 个训练历元的验证准确率没有提高，则停止训练过程。本实验使用全部 140 台设备的训练时间≈ *15* 分钟。图 5 显示了 ORACLE 的性能，以及每个数据集的最低准确率、第一四分位数、中位数、第三四分位数和最高准确率。图中， X 轴代表随机选择的设备数量，Y 轴表示分类准确率。在多达 100 个不同设备的情况下，我们获得的中位准确率为 99%，而在 140 个设备的情况下为 96% 。我们注意到，虽然无线电的数量很大，但这些设备的比特并不相似。因此，我们使用从 16 个高端 X310 USRP SDR 收集到的 IQ 样本对分类器进行了 "压力测试"，这些 SDR 具有较窄的损伤范围，并使用相同的 B210 无线电作为接收器。本实验的训练集包括每个无线电的 200K 窗口训练示例和 10K 验证示例。我们使用每个设备的另外 *50K 个*示例来测试训练模型的性能。以我们目前的设置，训练 16 个无线电设备的 模型需要 ≈ *30* 分钟。同样在这种设置下，我们在测试集上获得了 98.6% 的准确率，如图 6a 所示。

*2) 动态信道中原始 IQ 样本的局限性：*多径反射和衰减对接收到的 IQ 样本有相当大的影响，有时会使样本失真，分类器无法再正确识别无线电。通常情况下，信道的影响会通过信道定时和均衡技术得到补偿，以正确检索空中传输的数据。因此，正如我们接下来所展示的，分类



(a) (b) (c)

图 8：(a) 在时间 $_{t1}$ 测试的 4 台设备的分类准确率和位置 l_1；（b）时间 t_2 和相同位置 l_1；（c）时间 t_3 和不同的位置 $_{l3}$.

当 (i) 分类器在给定信道下根据原始 IQ 样本进行训练，然后

或 (ii) 发射机的信道条件非常相似。

图 6a 显示了 16 个 X310 无线电设备的分类准确性，所有设备的分类结果接近完美。然而，图 6b 显示的是在不同位置的相同设置，如混淆矩阵所示，存在几个异常值，如无线电对（5,15）、（10,14）。原因是*某些发射机对所经历的无线信道的相似性主导了微妙的硬件变化*。给定一组 R 个无线电对、

$_{H\sim i}(k)$ 表示th 子载波中的平均信道增益

$_i \in R$，根据属于训练数据集的 WiFi 数据包估算。

图 7a 和 7b 揭示了信道估计差异较小的发射机的接收样本在测试过程中更容易被 ORACLE 错误分类。这表明，无线信道状态对接收器捕获的复杂符号的分布有不可忽视的影响，因此*当分类器使用原始 IQ 样本进行训练时，*无线信道状态会*成为一个判别因素*。如果我们尝试使用

如果将预先训练好的模型用于对从相同设备但在不同时间或地点采集的样本进行分类，分类结果将难以预测。见图 8a、8b 和 8c

的分类结果，显示了训练有素的分类器在时间和地点上的依赖性。

V. 带反馈的 ORACLE 动态通道

本节将介绍 ORACLE 的增强功能，使其能够在未知环境中稳健地对发射机进行分类。这里的两个主要假设是(i) ORACLE 使用解调符号代替原始 IQ 样本，并且

(ii) 在部署前阶段，接收机向发射机提供反馈，以纳入受控损伤。

A. 损伤对解调符号的影响

ORACLE 修改了 SDR 的发射机链，使其各自的解调符

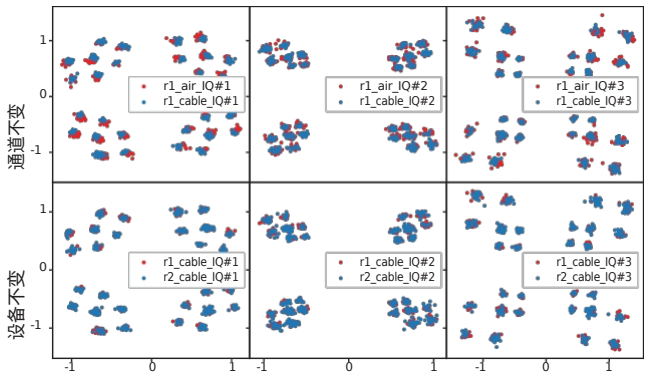


图 9：在 2 种信道条件下，2 种设备上的 3 种损伤所产生的模式。第一行和第二行分别显示了模式的信道不变性和设备不变性。

IQ 不平衡水平。第一行显示的是同一发射机的信道完全改变（即从空中到电缆）时解调样本的 细微差别。在第二行中，当保持相同信道但发射机本身不同时，添加相同水平的 IQ 不平衡会导致每种情况下的模式几乎相同，从而确保了可重复性和鲁棒性。

我们还利用 "地球移动距离"（EMD）定量分析了模式的信道和设备不变性属性。"地球移动距离 "是一种广泛用于衡量两个多维分布之间相似性的指标。更确切地说，假设 R^2 中有两组点。让 $A \subset R^2$ 和 $B \subset R^2$ 是两个大小相等的子集，即 $|A| = |B|$。让 F 是所有可能的从 A 到 B 的双射（1 - 1 和到映射）的集合：

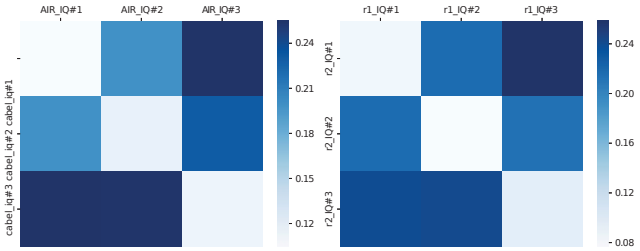
$$EMD(A, B) = \min_{f \in F} \sum_{x \in A} \|x - f(x)\|_{\circ} \qquad (3)$$

号获得独特的特性，从而使 CNN 对信道变化具有鲁棒性，即使发射机硬件*主导*信道引起的变化。我们首先验证了一个假设，即特定的损伤组合会导致分类结果的可重复性。为了证明这一点，我们考虑了从两个 X310 无线电设备接收到的解调符号，如图 9 所示，它们通过有线和空中信道，在三种不同的情况下

换句话说，EMD 是在所有可能的有效投射 f : A → B 中，A 和 B 中各点之间欧氏距离之和的最小值。图 10 (a)和(b)分别显示了图 9 中在不同信道条件和设备上产生的模式的 EMD 矩阵，它们具有相同的损伤集。我们可以看到，矩阵对角线上计算的 EMD（代表由相同损伤产生的模式）远远低于由不同损伤产生的模式的 EMD。我们进一步评估了在 3 种不同信道条件下收集的解调信号的 EMD，4 种设备，32 种不同程度的损伤。我们发现，尽管信道条件会造成变化，但相同和不同程度的损伤所产生的模式的平均 EMD 分别保持在 0.1 和 0.2 左右。这一结果与图 10 非常吻合，验证了我们的直觉。

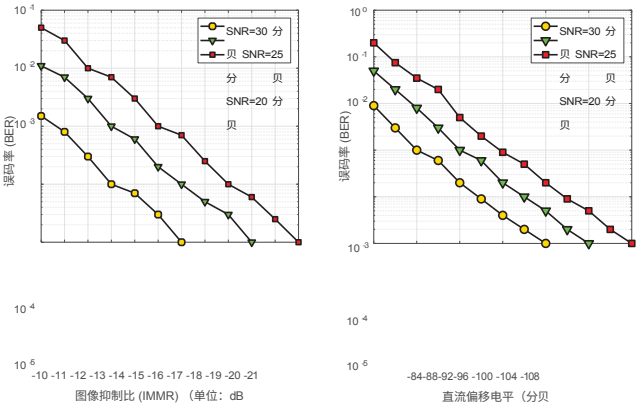
B. 确定可行的损伤

在训练 CNN 之前引入随机损伤组合的天真方法存在三个问题：



(a) (b)

图 10：在不同信道条件下生成的图案的 EMD 矩阵（a）；（b）在不同设备上生成的图案。



(a) (b)

图 11：(a) 误码率与 IQ 不平衡的 IMMR 值的关系；(b) 不同信噪比时误码率与 DC 偏移水平的关系。

1) *可扩展性：*如果网络中引入一个新的发射器，我们就必须重新训练整个 CNN，这是一个耗时耗力的过程。
2) *准确性：由于*在 IQ 平面上的位置发生变化，来自两个不同发射机的解调样本（以前很容易区分）现在可能会集中在一起。这可能会降低分类器的性能。
3) *通信影响：*增加损伤自然会增加误码率。因此，需要明智、可控地添加干扰，以限制对误码率的不利影响。

为解决这些问题，ORACLE 会自动选择可产生 IQ 样本星座点的功能损伤，这些损伤点之间存在显著差异，但对发射机误码率的影响最小。这一步骤允许 ORACLE 在虚拟无线电发射链（在 GNU Radio 中构建）上进行预训练，因然后，发射机通过电缆向 B210 USRP 接收机发送已知数据流。然后，发射机通过电缆向 B210 USRP 接收机发送已知数据流，由接收机检查误码率。在实验中，我们考虑了 80 种不同程度的 IQ 不平衡，IMMR 值从 -9 dB 到 -44 dB 和 120 级直流偏移，范围从 -82 dB 到 -140dB。不同信噪比水平下 的误码率图如图 11a 和图 11b 所示，我们将其简明地称为损伤图 M，并在后面的第 V-D 章中使用。损伤的 界限取决于无线电的工作信噪比。例如，我们实验室的本底噪声为 -70 dBm，在这种情况下我们假设平均信噪比水平为 30 dB，误码率限制为 10^{-4}。因此，我们选择上限为 -13 dB

在 IMMR 上的 IQ 不平衡和-94 dB 的直流偏移电平。接下来，我们将解释如何从满足误码率约束条件的所有损伤组合中找出可行集 S。具体来说，让 $[c_1, c_2, \cdots, c_{max}]$成为不同 IQ 不平衡水平的向量，从而产生一个有序的相关集。对应的误码率，即 $误码率[c_i] < 误_{i+1}]$.因此，$c_{最大码率}[c$ 是我们在不超过误码率限制的情况下所能增加的最大 IQ 不平衡。请注意，10^{-4} 的误码率限制是在*理想*信噪比水平（40 dB）下评估的。我们从 c_1，因为它对通信的影响最小，所以会越来越多地将 c_2 添加到 c_{max} 的集合 S 中。

为损伤会主导由自身硬件和无线信道引入的其他变化。因此，ORACLE 会学习损伤模式，我们在图 9 中已经证明了这种模式与设备和信道无关，也就是说，在相同损伤下，两个不同的无线电会在接收器处产生类似的解调 IQ 模式。这种方法大大提高了 ORACLE 的灵活性：如果增加了新的发射机，我们只需将其分配给可行的、未承诺的损伤之一，而无需重新训练 CNN。

我们使用的是通用的 X310 USRP 无线电设备，它在环路中运行，同时通过实用程序 `uhd_cal_tx_iq_balance` 和 `uhd_cal_tx_dc_offset` 自动为其硬件增加 IQ 不平衡和直流偏移的损伤、

只有当 c_i 生成的模式与 S 中任何现有 c_k 生成的模式之间的 EMD 差值大于阈值 T *时，*才有资格添加新的 c_i 。正如我们在第 V-A 章中看到的，$T = 0.15$ 允许在评估给定 IQ 模式与另一模式的接近程度时使用可接受的缓冲区。在达到 c_{max} 之后，我们将无线电配置为不同类型的损伤，直到 S||| > N，其中 N 是比特相似无线电的数量。

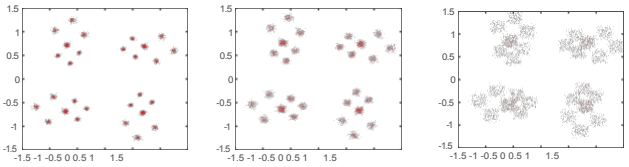
C. 利用发射端损伤的CNN 分类器

在本节中，我们将讨论如 何 训练模式分类器（见第五章 B 节）。我们重复使用与第四节所述相同的 CNN 架构和输入数据格式。请注意，所有用于训练的 IQ 样本都是通过电缆收集的，也就是说，我们消除了无线信道的影响，这样 CNN 就能捕捉到仅由硬件损伤产生的模式。ORACLE 故意通过修改原始数据来引入随机噪音，以增加分类器输入前初始数据集的数量和可变性，这是深度学习中常用的一种技术。由于接收样本的信噪比较低，导致 IQ 平面内理想星座点位置周围出现散射，因此噪声被建模为高斯变量。我们注意到，噪声可能会导致解调后的 IQ 样本模式与原始模 式 不同，如图 12 所示。为了精细控制可能出现的变化，我们在添加噪声*后将* EMD 保持在 0.1 以下，因为达到这一水平的两个样本模式仍然彼此相似（见第 V-A 章）。因此，添加小于 σ^2 = -13 dB 的噪声功率可确保两个样本之间的 EMD 值保持在 0.1 以下。原始模式和更改模式的比例低于这一临界值。

n

D. 将特定发射机分配给损伤

增加损耗的主要挑战是会 增加误码率，降低服务质量。在



(a) (b) (c)

图 12：使用 (a) 原始（解调）数据生成的图案；(b) 添加 -17 dB 噪声后的数据，EMD（a）：0.07；(c) 添加 -9 dB 噪声后的数据，EMD（a）：0.18。

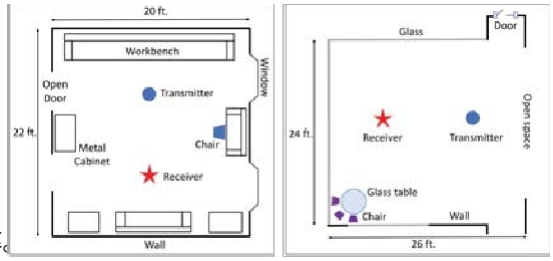
此外，在不同信噪比水平下，无线电的衰减情况也不同（如图 11 所示）。信噪比越低，为了确保所需的误码率，我们可以在无线电中添加的损伤越少。我们将在本节讨论如何解决这一问题，假设接收端的信噪比测量在持续时间 T 内是准静态的，允许在每个时隙内平均信噪比水平。

问题的提出：给定 K 个无线电 $[r_1, r_2, \cdots, r_K]$，这些无线电的平均 SNR 水平为 $[snr_1, snr_2, \cdots, snr_k]$。我们需要根据接收器的平均信噪比水平，选择 K 种能使每个发射机误码率最小的损伤。

我们使用贪婪启发式来解决这个问题，该启发式与我们在第 V-A 章中用于生成独特模式的启发式类似。在不失一般性的前提下，考虑 IQ 不平衡，$[c, c_{12}, \cdots, c_n]$为所选 IMMR 水平集，M 为不同 SNR 水平到最大 IQ 不平衡的映射，以保持最低误码率（见第 V-B 节）。然后，对于每个无线电 r_i，我们选择 c^i，其中 $c^i = M[max(Q)]$，Q 是 M 中 SNR 的集合，$q < snr_i$，$\forall q \in Q$。

在此步骤之后，我们按照 c^i 对无线电 $[r_1, r_2, \cdots, r_i]$进行最终排序，使得 $c^i \leq c^{i+1}$，即按照可增加的最大 IQ 不平衡度对无线电进行排序。然后，我们创建两个空集 R_1 和 R_2，分别表示可分类和不可分类的无线电。然后，只要 $c_i \leq c^i$，我们就开始将$[c_1, c_2, \cdots, c_n]$迭代分配给从 r_1 到 r_k 的无线电，并将给定的无线电置于可分类集 R_1 中。否则，如果 $c_i > c^i$，则意味着在不超过误码率限制的情况下，无法向无线电 i 添加可行的 IQ 不平衡。因此，我们将该无线电放入不可分类集 R_2 中。在探索完所有无线电后，如果 R_2 不为空，我们将用第二种类型的损伤（如直流偏移）重复上述过程，直到所有无线电都被放入可分类集。

总之，从低到高分配损耗可确保我们最大限度地降低误码率。



VI. 绩效评估

在本节中，我们将展示 ORACLE 的性能：(1) 它提高了比特相似无线电的分类准确性，而且准确性不受无线信道条件变化的影响（VI-A 节）；(2) 它在不牺牲分类性能的情况下，最大限度地减少了硬件损伤引起的误码率变化（VI-B 节）。

实验设置：我们首先确定一组 S，共 32 项损伤，如第 V-B 节所述，这些损伤会产生独特的模式。

结果。

(a) (b)

图 13：两种不同的实验环境：(a) 封闭的实验室区域（位置 1）；(b) 反射更少的开放休闲区域（位置 2）。

接下来，我们通过 GNU 无线电应用程序接口（GNU Radio API）引入这些损伤后，从单个无线电通过电缆传输的 WiFi 数据包中收集解调数据。我们通过添加随机高斯噪声来复制和增强解调数据。我们将噪声的功率限制在 -13 dB 以下，以确保从原始数据和改变后的数据生成的模式之间的 EMD 低于 0.1 的阈值。最后，我们使用与第四部分所述相同的 CNN 架构，使用增强数据集训练分类器。

A. 不同信道条件下的分类精度

我们用 16 个 X310 无线电设备测试了训练有素的 CNN 分类器的性能。为此，我们首先通过电缆收集这些无线电的样本。根据第 V-D 章中描述的方法，所有无线电都配置了从集合 S 中选择的 16 种损伤之一。如图 14a 所示，ORACLE 可以轻松区分故意引入所选损伤的比特相似无线电，分类准确率高达 99.76%。这表明我们预先训练的分类器能够准确识别比特相似无线电。

接下来，我们利用通过无线信道收集的数据对 ORACLE 的性能进行评估。为了显示对信道条件变化的鲁棒性，我们在两个不同的地点进行了实验：(1) 我们的实验室，这是一个典型的室内环境（图 13a）；(2) 一个更开阔的休闲区，这里反射较少（图 13b）。分类准确率的融合矩阵分别如图 14b 和图 14c 所示。总的来说，在这两种环境中，ORACLE 的准确率都能达到 99.5%以上，这证明即使在随机噪声的情况下，也能检测到由损伤产生的独特模式。

相比之下，用这 16 个 X310 设备训练相同的分类器，而不人为引入任何类型的硬件损伤，结果分类性能很差。如图 14d 所示，这些比特相似无线电的分类准确率仅为 35.96%，这说明了精心的损伤分配过程的 好处。

B. 启发式损伤选择降低误码率

我们使用所有发射机的平均误码率总和作为衡量标准，并比较了 i) 随机分配和 ii) 使用算法贪婪地分配误码率的

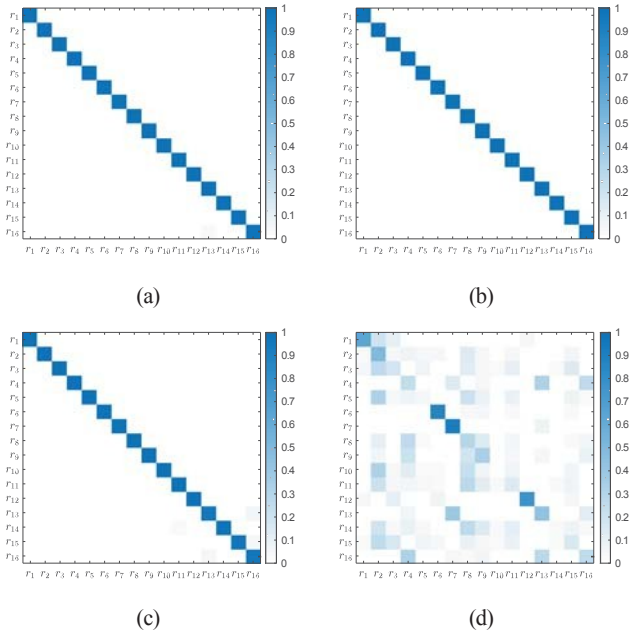


图 14：分类准确度 (a) 通过电缆；(b) 位置 1 的 空气（图 13a）；(c) 位置 2 的空气（ 图 13b）。(d)显示的是未使用 ORACLE 时的准确度（在位置 2 收集的数据）。

将在第 V-D 章中介绍。我们认为 $R = 4$、8、12、16 个区域的平均信噪比值是从以下四个区域中随机选择的 {20,25,30} dB。让 IQ 不平衡成为唯一增加的损伤，它以 IMMR 值 -13.5 dB 为界。不过，我们考虑了 16 个可用的损伤等级，其范围从 IMMR 的 -13.5 到 -21 dB，间隔为 0.5 dB。每次选择时，我们都要确保 CNN 根据这些损伤等级分类的准确率*大于*99%。

在随机分配方法下，*R 个*无线电随机分配所选的 16 个损伤级别中的一个。另一方面，我们的贪婪启发式算法会迭代地为平均信噪比最小的无线电分配最低的可用损伤级别。图 11a 显示了不同 SNR 水平下每个无线电的误码率值。我们进行了 1000 次迭代，其中每个无线电随机分配一个 SNR 水平。在每次迭代中，使用随机分配策略为每个无线电随机分配一个唯一的损伤等级。我们重复 500 次，计算出在给定信噪比分配下，所有无线电在 500 次迭代中的平均误码率总和。然后再计算 1000 次 SNR 分配的平均值。类似地，我们计算使用贪婪启发式算法获得的所有无线电设备的误码率总和，在 1000 次 SNR 分配中取平均值。表 III 显示了所有无线电的误码率，证实 ORACLE 的损伤分配方法始终优于随机分配。

表 III：随机和贪婪启发式损伤分配的误码率性能比较。

无线电数量	误码率平均总和	
	随机	贪婪启发式
$R = 4$	1.28×10^{-3}	1.81×10^{-5}
$R = 8$	2.62×10^{-3}	7.82×10^{-5}
$R = 12$	3.90×10^{-3}	2.49×10^{-4}
$R = 16$	5.20×10^{-3}	8.13×10^{-4}

在静态环境中，我们对 > 100 多个 COTS WiFi 设备和 16 个 X310 USRP 无线电设备进行了采样。为了进一步提高动态环境下的分类准确性，我们展示了反馈驱动的发射机侧修改如何提高比特相似设备的可区分性。其关键创新在于 " 一次培训，随处部署 "的特点。我们在实验中证明，无论信道条件和无线传输环境如何不同，比特相似的 X310 无线电设备的准确率*大于*99%。

鸣谢

这项工作得到了美国国防部高级研究计划局 RFMLS 计划合同 N00164-18-R-WQ80 的支持。我们感谢 Paul Tilgh-

VII. 结论

我们介绍了 ORACLE，这是一种基于发射机链内以硬件为中心的特征来识别特定无线电的指纹识别技术。我们的研究表明，我们的 CNN 分类器使用原始 IQ

DARPA 的项目经理 Man 和 Esko Jaska 提出了 富有见地的意见和建议。

参考资料

[1] Q.Xu、R. Zheng、W. Saad 和 Z. Han，"少线网络中的设备指纹识别：挑战与机遇》，《*IEEE 通信概览教程*》，第 18 卷，第 1 期，第 94-104 页，2016 年第一季度。

[2] T.J. O'Shea 和 J. Corgan，"卷积无线电调制识别网络"，2016 年。[Online].Available: http://arxiv.org/abs/1602.04105

[3] A.Selim, F. Paisana, J. A. Arokkiam, Y. Zhang, L. Doyle, and L. A. DaSilva, "Spectrum monitoring for radar bands using deep convolutional neural networks," in *IEEE GLOBECOM 2017*.

[4] J.Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. Van Randwyk, and D.Sicker：《被动数据链路层 802.11 无线设备驱动程序指 纹 识别》，*ACM USENIX 安全研讨会 - 第 15 卷*，2006 年。

[5] K.Gao, C. Corbett, and R. Beyah, "A passive approach to wireless device fingerprinting," in *IEEE DSN 2010*, June 2010, pp.

[6] I.I. O. Kennedy、P. Scanlon、F. J. Mullany、M. M. Buddhikot、K. E. Nolan 和 T. W. Rondeau，"无线电发射机指纹：A steady state f r e q u e n c y d o m a i n approach," in *IEEE VTC, Sept* 2008, pp.

[7] V.Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *ACM MOBICOM 2008*.

[8] S.V. Radhakrishnan、A. S. Uluagac 和 R. Beyah，"Gtid：物理设备和设备类型指纹识别技术》，《*电气与 电子工程师学会可依赖与安全计算交互》*，2015 年 9 月。

[9] F.Chen, Q. Yan, C. Shahriar, C. Lu, W. Lou, and T. C. Clancy, "On passive wireless device fingerprinting using infinite hidden markov random field," *submitted for publication*.

[10] N.N. T. Nguyen、G. Zheng、Z. Han 和 R. Zheng，"使用非参数贝叶斯方法增强无线安全的设备指纹"，*IEEE INFOCOM*，2011 年 4 月，第 1404-1412 页。

[11] T.J. O'Shea 和 J. Hoydis，"机器学习通信系统简介"，2017 年。[Online].Available: http://arxiv.org/abs/1702.00832

[12] S.Riyaz, K. Sankhe, S. Ioannidis, and K. Chowdhury, "Deep learning convolutional neural networks for radio identification," *IEEE Communi- cations Magazine, vol.* 56, no. 9, pp.

[13] A.Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," in *NIPS 2012*.