利用半监督学习提升室内多径环境下的射频指纹识别性能

Mohamed K. M. Fadul，Donald R. Reising†，Lakmali P. Weerasena，T. Daniel Loveless，Mina Sartipi，Joshua H. Tyler*田纳西大学查塔努加分校，美国田纳西州查塔努加，邮编37403 电子邮箱：{mohammed-fadul, donald-reising†, lakmali-weerasena, daniel-loveless, mina-sartipi}@utc.edu, ygm111@mocs.utc.edu*

arXiv:2304.00648v1 [eess.SP] 2 Apr 2023

摘要——**预计到2025年，物联网部署数量将达到754亿。约70%的物联网设备使用弱加密或完全不加密，因此这些设备及其互联基础设施面临遭受攻击的风险，攻击者可能使用未经正确身份认证或完全未经身份认证的设备。物理层安全方法——称为特定发射器识别（SEI）——已被提出，并正在作为一种可行的物联网安全机制加以研究。SEI的优势在于它是一种被动技术，利用物联网设备射频（RF）前端在信号形成和传输过程中无意引入信号中的固有且独特的特征。SEI对无意信号特征的被动利用，无需修改物联网设备，因此非常适用于现有及未来的物联网部署。尽管已开展大量SEI研究，但要使SEI成为可行的物联网安全方法，仍有一些挑战亟待解决。其中一项挑战是从多径衰落条件下采集的信号中提取特定发射机识别特征。多径会破坏用于区分不同物联网设备的固有SEI特征，从而降低身份认证性能并增加遭受攻击的可能性。本文提出两种半监督深度学习（DL）均衡方法，并将其性能与当前最先进水平进行比较。这两种方法分别为条件生成对抗网络（CGAN）和联合卷积自编码器与卷积神经网络（JCAECNN）。这两种方法均通过学习信道分布来实现多径校正，同时保留SEI所利用的信号特征。本文在瑞利衰落信道下，针对逐渐降低的信噪比、最多32台物联网设备以及两个公开可用的信号数据集，对CGAN和JCAECNN的性能进行了评估。JCAECNN使特定发射机识别性能比当前最先进水平提高了10%。**

索引词—**深度学习、特定发射器识别（SEI）、物联网（IoT）、安全**

I. 引言

It 据估计，到 2025 [1]，联网物联网（IoT）设备的数量将达到754亿。令人担忧的是，约70%的物联网设备采用了较弱的加密方式，或完全没有加密，这主要是由于设备板载资源有限（如内存、计算能力等）、制造成本过高而无法采用加密，或密钥管理及规模化实施存在困难 [2]–[4]。缺乏或加密不足会造成安全漏洞，使单个物联网设备及其对应基础设施容易遭受恶意行为者的攻击 [5]–[12]。基于这一现状及相关攻击，迫切需要一种有效的物联网安全解决方案。

物联网部署遵循开放系统互连（OSI）模型。该模型指出，物理（PHY）层负责完成点对点比特流通信，并被视为最低且最先的一层 [13]。按照设计，传统安全技术部署在较高的 OSI 层（例如数据链路层或网络层）；因此，尽管攻击者必须经过 PHY 层才能实施攻击，这些技术仍未将其纳入考虑 [14]。特定发射器识别（SEI）已被提出作为一种 PHY 层物联网安全解决方案 [15]–[17]。研究表明，SEI 能够利用信号在形成和传输过程中所带有的不可变、非故意着色，实现序列号判别。这种着色源于构成发射机射频（RF）前端的各个组件、子系统和系统中存在的、可容许的制造偏差 [14], [18]–[38]。SEI 的优势在于，它提供了一种被动认证机制，无需修改终端设备（即着色是在正常运行过程中产生的），因此特别适用于物联网应用，因为识别设备无需额外消耗资源。然而，自近三十年前问世以来，SEI 在多径等复杂运行条件下的性能几乎未受到关注。SEI 作为物联网安全解决方案的可行性，取决于其在运行条件恶化时能否继续保持有效。

射频独特固有属性（RF-DNA）指纹识别是一种特定发射机识别（SEI）实现方式，它从发射信号中对应于固定且已知符号序列的部分提取可利用特征，例如 IEEE 802.11a 无线保真（Wi-Fi）前导码。以往的射频指纹识别研究采用依赖专家知识和人工设计特征的监督学习和无监督学习算法，以促进物联网设备判别 [14], [17], [21], [23]–[26], [34]–[41]。这些算法可能产生次优模型，从而限制射频指纹识别的性能，尤其是在

†– 通讯作者。本研究得到查塔努加大学（UC）基金会的部分资助。

表 I 符号
说明。

N_D	本研究使用的发射器数量	N_B	每个发射机的采集信号数量 发射机	A，B	独立同分布随机变量
σ^2	方差	L	瑞利衰落信道长度	T_r	时延的均方根 扩展
T_s	采样周期	α_k	k^{th} 瑞利衰落系数 入射路径	τ_k	.....的延迟 k^{th} 瑞利衰落 path
$x(t)$	采集到的 IEEE 802.11a 信号	$r(t)$	多径接收信号	$n(t)$	复高斯白噪声
$h(t)$	时延线信道冲激响应	$\hat{x}(m)$	发射信号的估计值 $x(m)$	γ	信噪比（SNR）
I_A	与.....维度匹配的单位矩阵 维度为 A	β	神经网络激活函数	W	卷积核权重
$\mathcal{F}$	一组射频 DNA 指纹及其 类别标签	b	神经网络偏 置	θ	神经网络可训练参数
$J(\theta)$	神经网络损失函数	$D(x)$	判别器对输入 x的输出	$G(z)$	生成器对输入 z的输出
$P_d(x)$	训练数据的分布 x	$P_z(z)$	G的输入 z的先验概率	$r_{\mathscr{R}}(n)$	接收信号同相分量
$r_{\mathscr{I}}(n)$	接收信号正交分量- nent	ρ_r	接收信号的幅度	θ_r	接收信号的相位角
N_R	每个发射机的训练信号数量 ter	N_T	每个发射机的测试信号数量	$\tilde{x}[n]$	输入对应的加性高斯白噪声信道输出 $x[n]$
y	与该信号对应的真实标签 发射信号 $x[n]$	$\tilde{X}_e$	IQ+NL 的有标签表示 $\tilde{x}[n]$	$\mathbf{R}_e$	IQ+NL 的有标签表示 $r[n]$
$\hat{X}_e$	G 对输入$\mathbf{R}_e$的输出	$\tilde{y}_c$	JCAECNN 给出的估计标签 分类器	C_k	该信号的延迟和缩放版本 发射信号 $x[n]$
N_z	噪声实现次数	z	条件生成对抗网络生成器的输入，G		

时间变化信道或较低信噪比（SNR）信道等退化工作条件下。在过去五年中，特定发射机识别研究群体因深度学习（DL）在频谱管理[42]，[43]，、调制和发射机识别 [44]–[46]，、系统设计 [44], [47]–[50], 中的成功应用，以及其能够在信息量不断增加的情况下保持良好性能并消除对人工设计特征的需求 [35]，[46]，[51]–[85]，一直致力于研究深度学习（DL）。基于这些已发表的深度学习研究成果，本文所 प्रस्तुत的工作表明，深度学习能够提供一种有效的射频指纹识别流程，在退化工作条件下实现物联网设备序列号判别。具体而言，我们证明，在室内多径信道环境中，最多 32 个仅序列号不同的物联网设备可以被成功地区分。

本文其余部分的组织结构如下。第 II 节总结了与本研究最相关的现有文献，并更详细地阐述了本研究的贡献。第 III 节介绍目标信号、信号采集与检测过程、多径信道建模、Nelder-Mead（N-M）信道估计器和最小均方误差（MMSE）均衡器，以及本文所采用的深度学习架构。第 IV 节介绍所提出的、由深度学习驱动的室内多径环境射频 DNA 指纹识别方法。第 V 节展示实验结果，第 VI 节总结全文。

II. 相关工作与贡献

基于深度学习的特定发射机识别已被证明能够提供一种最优的端到端解决方案，并取得卓越的性能，然而大多数已发表的研究并未使用经历时变衰落的射频信号进行特定发射机识别。事实上，只有少数基于深度学习的特定发射机识别研究评估了其在多径条件下的性能，而且其中大多数使用的信道可归为以下两类：(i) 静态信道（即信道系数或特性始终不变） [35]，，或 (ii) 时变信道，但环境的具体特性（例如反射体数量、是否存在视距传播、衰落类型等）未知、未说明或未由作者披露 [35], [46], [53], [62], [63], [74], [76], [81]。无论如何，大多数基于深度学习的特定发射机识别研究都假设，所选用、修改或开发的算法能够直接从接收信号中学习判别性特征；因此，在射频信号分类前无需进行信道估计和校正。事实上，多径衰落信道的时变特性会妨碍或严重阻碍深度学习算法学习对多径衰落具有不变性的判别性信号特征。

[41] 中的研究是这一趋势的例外，因为作者：（i）采用 IEEE 802.11a Wi-Fi 室内信道模型，并说明了用于配置该模型的具体参数值 [86]；（ii）在使用卷积自编码器（CAE）初始化的卷积神经网络（CNN）进行特定发射机识别之前，先采用传统（即非基于深度学习的）多径信道估计与校正方法。由于信道系数估计误差，以及对已知信道统计特性的依赖，作者采用传统估计与校正方法导致特定发射机识别性能未达最优。最后，作者仅使用四个发射器评估其 CAE-CNN 特定发射机识别方法，这与通常包含数十至数百台设备的物联网部署情况不符。

本文其余部分将详细介绍我们的工作。我们的工作通过以下贡献推动了基于深度学习的特定发射机识别当前最先进水平的发展：

1) 将标签嵌入与条件生成对抗网络（CGAN）相结合，以高效学习每个发射机的条件特征分布。

2) 通过采用直角坐标和极坐标信号表示 [87]，增强判别特征学习。 3) 介绍并评估两种半监督学习均衡方法，以在瑞利衰落和信噪比下降条件下提升基于卷积神经网络的特定发射机识别性能。 4) 介绍并评估一种可扩展的半监督学习架构，该架构联合构建基于卷积自编码器的生成模型和基于卷积神经网络的判别模型，以校正瑞利衰落，同时保留特定发射机识别的判别特征。该联合架构在此称为 JCAECNN ； 在进行 CNN 分类之前，它将多径信号分解为原始发射信号的多个独立缩放和延迟版本。

5) 通过采用指数衰减损失函数权重，提升我们的 JCAECNN 的特定发射机识别性能。
6) 评估 CGAN 和 JCAECNN 架构在四个、八个、十六个或三十二个发射机通过瑞利衰落信道通信时的特定发射机识别性能。 7) 使用由 [88], [89] 的作者生成的公开信号数据集，评估 JCAECNN 的特定发射机识别性能。这些结果可作为基准，以便与当前及未来的研究成果进行比较。
8) 将 CGAN 和 JCAECNN 架构的特定发射机识别性能与我们在 [38], [41] 中的先前工作直接进行比较。

这些贡献使平均分类正确率达到 94.35% 或更高；这一表现适用于信噪比不低于 9 dB、包含五个反射/路径的瑞利衰落信道，以及由十六台设备组成的物联网部署。

III. 背景

A. 目标信号

本研究使用通过 IEEE 802.11a Wi-Fi 协议进行通信的物联网发射器。选择 IEEE 802.11a 协议作为信号子层的原因如下： （i）802.11a 基于正交频分复用（OFDM）信号，该信号应用于多种无线通信标准，例如 802.11ac、802.11ad、802.11ax、长期演进（LTE）和微波接入全球互通（ WiMAX） [90], ； （ii）特定发射机识别领域的多项研究已证明，使用 802.11a 信号能够取得良好效果 [18], [21], [24], [27], [33], [34],[36]–[39], [46], [56], [85], [87], [91],； （iii）可获取我们先前发表成果中使用的同一数据集 [36]–[38],[41], [85], [87]，便于开展比较评估； 以及（iv）802.11a Wi-Fi 已被采用为物联网通信协议 [92]。与我们先前发表的成果一致，本研究通过从 IEEE 802.11a 无线保真前导码中提取射频 DNA 指纹来进行特定发射机识别。该前导码包含每次传输的前 16 μ 个符号。使用 802.11a 前导码是理想的，因为接收机正是利用信号的这一部分进行信道均衡。802.11a 前导码由十个短训练符号（STS） t_1 至 t_{10}、一个保护间隔（GI），以及两个长训练符号（LTS）组成；图 1 [93] 中将这两个长训练符号分别标记为 T_1 和 T_2。

B. 信号采集与检测

本研究使用的主要数据集由 $N_D = 4$ Cisco AIR-CB21G-A-K9 Wi-Fi 发射器发射的 802.11a Wi-Fi 信号组成，并使用基于 Agilent E3238S 的频谱分析仪进行采集。该频谱分析仪的信号采样率最高可达每秒 95 兆样本（ Msps），工作频率范围为 20 MHz 至 6 GHz，射频带宽为 36 MHz，并配有 12 位模数转换器 [94]。采集完成后，使用基于幅度方差轨迹的检测方法，为每个 $N_D = 4$ 发射器选取总计 $N_B = 2,$ 000 个信号 [23]。随后，使用截止频率为 7.7 MHz 的四阶巴特沃斯低通滤波器对每个信号进行滤波。滤波后，通过校正载波频率偏移对信号进行后处理，并将其降采样至 20 MHz [39]。

C. 多径信道建模

多径是室内环境中通信系统面临的主要问题之一。它会限制接收机正确恢复传输消息的能力，从而降低系统性能。这种性能下降是由于与不同延迟和衰减值相关联的发射信号多个副本在接收机天线处相互发生破坏性干涉所致。这些副本是发射信号在传播环境 [86] 中各处物体上反射形成的。接收机处这些反射副本的叠加会随机改变发射机与接收机之间的载波频率，并在短时间间隔内改变信号强度 [86]。本文所述研究出于两个原因，使用瑞利分布对室内多径信道进行建模：(i) IEEE 802.11 工作组使用该分布评估 Wi-Fi 调制性能 [86], ； (ii) 先前关于特定发射机识别的研究曾使用相同分布或据此评估系统性能 [36]–[38], [41], [53],[74], [76], [81]。

在多径衰落中，单次反射（又称路径）通过系数及其对应的时延（称为时延扩展） [86]来量化。对于瑞利衰落，

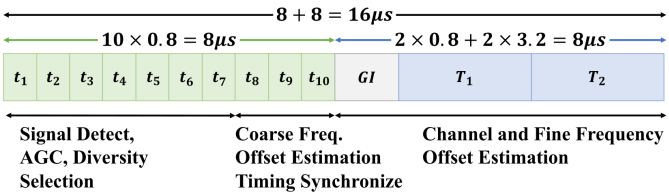


图 1. 每个 IEEE 802.11a Wi-Fi 帧开头处的 16 μs 时长前导码结构 [93]。

使用抽头延迟线（TDL）对信道进行数学描述。在抽头延迟线中，每个“抽头”代表一个系数和时延。对于每条路径 k，系数用圆对称复高斯随机变量表示，

$$\alpha_k = A + jB, \tag{1}$$

其中，$k=1$、.....、L 表示组成信道的路径总数为 L，而 σ^2 是零均值、独立同分布高斯随机变量 A和 B [86]的方差。若时延扩展的均方根（RMS）为 T_{r}，采样周期为 T_s，则方差可定义为:

$$\sigma^2 = \frac{\sigma_k^2}{2} = \frac{1}{2}\left\{\left[1-\exp\left(\frac{-T_s}{T_{\mathrm{r}}}\right)\right]\exp\left(\frac{-kT_s}{T_{\mathrm{r}}}\right)\right\}. \tag{2}$$

最后，对于由 L条反射路径组成的多径环境，其抽头延迟线（TDL）为:

$$h(t) = \sum_{k=1}^{L} \alpha_k \delta(t-\tau_k T_s), \tag{3}$$

其中，α_k 和 τ_k 分别是与 k^{th} 路径 [86], [95]相关联的系数和时延扩展。具有多径的接收信号可表示为:

$$r(t) = x(t) * h(t) + n(t), \tag{4}$$

其中，$x(t)$是采集到的 802.11a Wi-Fi信号，$h(t)$是式（3）中的抽头延迟线（TDL），$n(t)$是复高斯白噪声，$*$ 表示卷积操作。噪声 $n(t)$经过滤波和缩放后，与 $x(t) * h(t)$的结果相加，从而生成信噪比值为 9 dB 至 30 dB、相邻取值间隔为 3 dB 的多径信号。

D. 传统信道估计与均衡

本节介绍内尔德-米德（N-M）估计器和 MMSE均衡器，用于便于比较我们在第 V 节中的结果与已发表工作 [41]中的结果。

1) 内尔德-米德信道估计器：N-M 估计器采用 N-M 单纯形算法构建，该算法使用直接搜索方法求解无约束优化问题 [96]。N-M 单纯形算法通过迭代，仅利用函数值和四种定义的操作，确定一个 d 变量非线性函数的最小解 [97]。N-M 单纯形算法计算效率较高，因为它不需要计算函数导数 [97]。在每次迭代 j开始时，定义一个包含 $d+1$ 个顶点的单纯形，并执行反射、扩张、收缩和缩减四种操作中的一种或多种，以计算一个或多个新点，再利用新点计算函数值。如果由 x_1 至 $xd+1$ 给出的顶点处计算所得函数值满足特定条件，则新点将替换单纯形中标记为 x_{d+1} [96]、 [97] 的最差点。如果前三种操作的条件均不满足，则使用缩减操作，按照以下公式计算一组新的点，即 $v2$ 至 $vd+1$，计算时使用缩减操作及以下公式 [97],

$$v_i = x_i + \varphi(x_i - x_1), \tag{5}$$

其中 $1<i\le d+1$，下一次迭代的新单纯形为（x_1，v_2，$\cdots v_{d+1}$） [97]。当计算得到的函数值——在第 j 次迭代时——满足一个或多个终止条件时，N-M 单纯形算法即停止。用于估计瑞利衰落信道系数的终止条件与 [36]–[38]，中使用的条件相同，具体公式如下:

$$\frac{1}{d}\sum_{i=1}^{d+1}[f(x_i)-\bar{f}]^2 < \epsilon_1, \tag{6}$$

$$\frac{1}{d}\sum_{i=1}^{d}\left\|x_i^j - x_i^{j+1}\right\|^2 < \epsilon_2, \tag{7}$$

其中 $\bar{f}$ 是函数值 $f(x_i)$ 的平均值，$\|\bullet\|$ 是l_2范数，ϵ_1 和 ϵ_2 分别是基于函数值 $f(x_i)$ 和点 x_i 的容差。每次迭代结束时都会检查这两个条件。需要最小化的函数为:

$$f(h) = \sum_{m\in T}\left|r(m) - \sum_{k=1}^{L} x(m-\tau_k)\alpha_k\right|^2. \tag{8}$$

函数 $f(h)$ 可描述为接收信号与发射信号 $x(m)$ 的加权延迟副本 [37] 之间的平方误差函数。由于 $r(m)$ 和 $x(m)$ 是复值，而 N-M 单纯形算法求解的是实值函数 [96], [97], 因此将方程 (8) 分为两部分进行最小化。将复值信号分解为实部和虚部，即可得到两个实值平方误差函数 [36]。分别对这两个函数应用 N-M 单纯形算法以计算系数值 α_k, 并通过取两个平方误差函数所得估计值的平均值作为最终系数估计值，从而降低估计误差 [36]。与 [36]–[38], [41], 一样，从每个 $N_D = 4$ IEEE 802.11a 发射器的信号集中随机选取五个“候选”前导码，以表示发射信号 $x(m)$。对每个候选前导码使用 N-M 单纯形算法求解方程 (8)，共得到 $N_C = 20$ 个信道冲激响应估计值。残差功率公式如下： [25],

$$\hat{h}(m) = \arg\min_{c}\left\{\sum_{m}\left|r(m) - \hat{h}_c(m) * x_c(m)\right|^2\right\}, \tag{9}$$

$\hat{}$，并用于选择最佳信道估计值。其中，$h_c(m)$ 是与候选前导码 $x_c(m)$ 对应的估计信道冲激响应，且 $1\le c\le N_C$ [37]。

*2) MMSE*信道均衡器：使用N-M估计器估计信道冲激响应后，采用MMSE算法校正多径信道效应。MMSE均衡器结合噪声功率等信道统计特性以及估计的多径信道系数 [36]，尝试从接收信号中重建发射信号。MMSE 在均衡过程中纳入信道统计特性，使其在信噪比条件恶化时具有更强的鲁棒性。MMSE均衡器旨在减小估计的发射信号 $\hat{x}(m)$ 与原始发射信号 $x(m)$ 之间的平方误差，如下所示，

$$\hat{x}(m) = \arg\min_{\hat{x}(m)} E\left[(x(m) - \hat{x}(m))^2\right]. \tag{10}$$

如果已知噪声功率或信道信噪比，则 MMSE 通过求解以下问题来估计发射信号，

$$\hat{\mathbf{x}}_M = \mathbf{A}^H \left(\mathbf{A}\mathbf{A}^H + \gamma^{-1}\mathbf{I}_A\right)^{-1} r \tag{11}$$

其中 $\mathbf{A}$ 是表示估计信道冲激响应的二维矩阵，γ 是信噪比，I_A 是与$\mathbf{A}$ [98]维度相匹配的单位矩阵。

E. 深度学习架构

本节简要介绍用于生成第 V 节结果的各类深度学习架构和算法。

1) 卷积神经网络：卷积神经网络（CNN）是一类基于多层感知机（MLP）的监督式神经网络（NN），旨在处理网格架构中的多维数据。它可用于处理一维向量（例如时间间隔数据）、二维和三维像素网格（例如图像）[99]。CNN 使用反向传播算法学习参数 θ，通过最小化损失函数来估计判别模型的映射函数。损失函数计算模型预测值与真实值之间的误差。

卷积神经网络由一个多层感知机以及前置的卷积层和池化层组成。卷积层由多个按网格排列的神经元构成，每个神经元都对应于一个多维卷积核（亦称滤波器）与输入中一个和卷积核大小相同区域之间的逐元素乘积。卷积核的元素称为权重，所有神经元共享这些权重 [100]。在卷积神经网络中，卷积层用于检测并提取输入数据多个区域中的特征，以生成特征图。卷积层中的每个神经元都通过激活函数对特征图中的对应元素进行非线性变换 [56]，[100]。池化层通常位于卷积层之后，通过计算相邻输出的统计摘要（例如最大值、最小值和平均值）来降低激活后特征图的维度 [99]。最大池化是卷积神经网络中最常用的池化层。本研究采用最大池化，在激活后的特征图矩形区域内提取最大值特征。经过一个或多个卷积与池化层阶段后，使用全连接层（亦称稠密层）检测高级特征，并将其传递至输出层 [46]。输出层的作用是预测提取出的特征所属的标签。本研究采用卷积神经网络，利用 IEEE 802.11a Wi-Fi 前导码实现射频指纹DNA 指纹分类；这些前导码经过瑞利衰落信道，且信噪比不断降低。

2) 自编码器：自编码器（AE）是一种基于多层感知机的神经网络，它尝试在输出端尽可能准确地重建多维输入 [101], [102]。AE 是一种基于无监督学习的架构，用于学习输入数据的分布并获取高效表示。从逻辑上讲，AE 由两个主要部分组成：编码器和解码器。通常，编码器尝试估计一个映射函数，以输出中间隐藏表示$\mathbf{h} = f(\mathbf{x})$。解码器旨在通过应用另一个映射函数$g(\mathbf{h})$，从隐藏表示重建输入，使得最终输出 $\mathbf{r} = g(\mathbf{h}(\mathbf{x}))$ 尽可能接近输入 $\mathbf{x}$ [99]。在训练过程中，AE 的损失函数会惩罚解码器输出与$\mathbf{x}$之间的差异。本研究对所有 AE 均使用均方误差（MSE）作为损失函数。当编码器由卷积层和池化层构成时，该 AE 称为卷积自编码器（CAE）。如果 CAE 输入端的多维数据（即张量）为$\mathbf{x}$，则对应于该 i^{th} 张量的隐藏表示为：

$$h_i = \beta(x_i * W + b), \tag{12}$$

其中，W 是卷积核的元素（也称为权重），b 是偏置，$*$ 表示卷积操作，β 是激活函数 [102]。解码器对 h_i 的输出r_i 为：

$$r_i = \beta(h_i * \tilde{W} + \tilde{b}), \tag{13}$$

其中，$\tilde{W}$ 是反卷积核的权重，$\tilde{b}$ 是解码器的偏置 [102]。训练期间，通过反向传播调整 CAE 参数$\tilde{\theta}$，包括 W、$\tilde{W}$、b和 $\tilde{b}$，以最小化以下损失函数：

$$J(\theta) = \sum_{i=1}^{m} (x_i - r_i)^2, \tag{14}$$

其中，m是训练样本的数量。

3）生成对抗网络：生成对抗网络（GAN）是一种基于深度学习的架构，通过对两个深度网络模型同时进行对抗训练，旨在估计生成模型。GAN 可用于估计多种应用所需的生成模型，包括图像编辑、风格迁移和图像合成 [103]。GAN 由两个模型组成，分别称为生成器 G 和判别器 D。G 是一个生成网络，它学习训练数据分布，从而能够生成具有相同分布的新样本。D 是一个判别网络，负责判断输入样本属于训练数据集，还是由

由 G生成。GAN 训练可视为一种极小极大双人博弈： G 尝试学习训练数据分布，并估计能够生成新样本的映射函数，以提高 D做出错误判定的概率；而 D 则试图最大限度地提高其做出正确判定的概率（即区分训练样本与生成样本） [99], [104]。当 D的输出处处均匀分布且概率为二分之一时，训练将达到唯一解。

当多层感知机网络同时用于 G 和 D网络时，可以使用反向传播训练整个系统：其中，表示 G 的神经网络无需访问训练数据即可恢复数据分布，而 D 则最大化作出正确二元判决的概率 [103]，[104]。如果 G 输入$\mathbf{z}$ 的先验概率为 $P_{\mathbf{z}}(z)$，则生成器映射函数可表示为 $G(\mathbf{z};\ \theta_g)$，其中θ_g 是 G的多层感知机参数。 D 函数表示为 $D(\mathbf{x};\ \theta_d)$，其输入为$\mathbf{x}$ ，单一输出为 $D(\mathbf{x})$，表示$\mathbf{x}$ 来自训练数据而非 G [104]的概率。在生成对抗网络训练过程中， G 网络旨在学习训练数据$\mathbf{X}$上的分布 P_g ，方法是同时最大化正确判决概率$D(\mathbf{x})$，并最小化与 G 网络对应的项（ $1 - D(G(\mathbf{z}))$） [104]。生成对抗网络极小极大优化问题可由以下目标函数描述：

$$\min_G \max_D V(D,G) = E_{x\sim P_{\mathrm{d}}(x)}\{\log[D(x)]\} + E_{z\sim P_z(z)}\{\log[1-D(G(z))]\}, \quad (15)$$

其中， E 为期望值。当 G 能够完美恢复训练数据分布（即 $P_g = P_{data}$）时，便达到最优点 [99], [104]。

IV. 方法

本节介绍一种非传统的预处理方法，该方法利用半监督深度学习来校正多径信道效应，同时保留用于特定发射机识别的射频 DNA 指纹。具体而言，本文研究了两种基于半监督学习的信道均衡方法。第一种方法利用生成对抗网络架构的对抗关系训练 G ，使其学习多径信道效应以及信号的射频 DNA 指纹分布，从而构建能够估计并校正多径信道效应的映射函数。第二种方法联合训练卷积自编码器与卷积神经网络架构（本文将其称为 JCAECNN），以校正多径信道效应，同时提升系统提取更具判别性的特定发射机识别特征的能力。

对每个采集到的同相正交前导码应用由 L 条路径组成的瑞利衰落信道，以模拟多径环境。采用各种半监督学习方法对生成的多径前导码集进行均衡，旨在最大限度地提升特定发射机识别性能。受 [87], 中结果的启发，半监督学习采用原始 IQ 前导码样本及其自然对数（NL）表示进行。原始 IQ 样本的自然对数定义如下：

$$\begin{aligned}\tilde{r}(n) &= \ln[r_{\mathscr{R}}(n) + jr_{\mathscr{I}}(n)] = \ln\left[\rho_r \exp(j\phi_r)\right] \\ &= \ln[\rho_r] + j\phi_r = \tilde{\rho}_r + j\phi_r, \end{aligned} \quad (16)$$

其中， $r_{\mathscr{R}}$ 是信号的实部（同相）分量， $r_{\mathscr{I}}$ 是虚部（正交）分量， ρ_r 是幅度， ϕ_r 是相位角 [87]。 i^{th}均衡后前导码的增强表示——此处记为 IQ+NL——是，

$$R^i(m,n) = \begin{bmatrix} r^i_{\mathscr{R}}(1,1) & r^i_{\mathscr{R}}(1,2) & \cdots & r^i_{\mathscr{R}}(1,320) \\ r^i_{\mathscr{I}}(2,1) & r^i_{\mathscr{I}}(2,2) & \cdots & r^i_{\mathscr{I}}(2,320) \\ \tilde{\rho}^i_r(3,1) & \tilde{\rho}^i_r(3,2) & \cdots & \tilde{\rho}^i_r(3,320) \\ \phi^i_r(4,1) & \phi^i_r(4,1) & \cdots & \phi^i_r(4,320) \end{bmatrix}, \quad (17)$$

其中， $i = 1, 2, \ldots, N_B$，总计 N_B个前导码，$m = 1, 2, \ldots, N_D$，以及 $n = 1, 2, \ldots, 320$，适用于以 20 MHz 采样的 IEEE 802.11a Wi-Fi 前导码。将由 ϕ_r 捕获的前导码相位特性与 IQ特征相结合，可提供一种计算效率高的机制，在信噪比条件恶化时提升特定发射机识别性能 [87]。本节其余部分将详细介绍两种半监督学习方法，这些方法能够利用在瑞利衰落和信噪比条件恶化情况下采集的信号进行特定发射机识别。

A. 使用条件生成对抗网络进行多径均衡

在生成射频设备指纹之前，所有信号都通过条件生成对抗网络（CGAN）进行信道均衡；该网络由 [105] 的作者提出。CGAN 使用 CAE 和 CNN 分别构建 G 和 D。半监督训练使模型能够估计生成函数 $G(z|y)$，从而重建不受瑞利衰落影响的 Wi-Fi 前导码，即使输入到 G 的前导码中存在这些衰落影响。图 2 展示了为生成第 V 节所述结果而开发的 CGAN 训练和射频信号均衡流程。表 II 列出了用于构建 CGAN 的 G和 D 的配置和参数。

通过使用唯一的 TDL（由公式 (3) 给定）对每个采集到的前导码进行滤波，来引入多径信道效应；该 TDL 配置为表示由 $L = 5$ 条反射路径组成的瑞利衰落信道。随后，向每个前导码添加一组独特的、经过缩放且采用相同滤波方式处理的加性白高斯噪声（AWGN），使信噪比达到 9 dB 至 30 dB，步长为 3 dB。对于每个信噪比，共生成十组独特的 AWGN 实现，以扩充数据集并便于进行蒙特卡洛分析。所得接收信号 $r[n]$（如公式 (4) 所示）采用 IQ+NL 表示，并使用最小-最大归一化将每个特征重新缩放至 [0, 1] 范围内。随后，将归一化后的 N_B 个前导码随机分配到训练集或测试集。训练集包含 $N_R = 1800$ 个前导码（即在所选信噪比和噪声实现下可用总数的 90%），测试集包含 $N_T = 200$ 个前导码（即在所选信噪比和噪声实现下可用总数的 10%），其中 $N_T = N_B - N_R$。

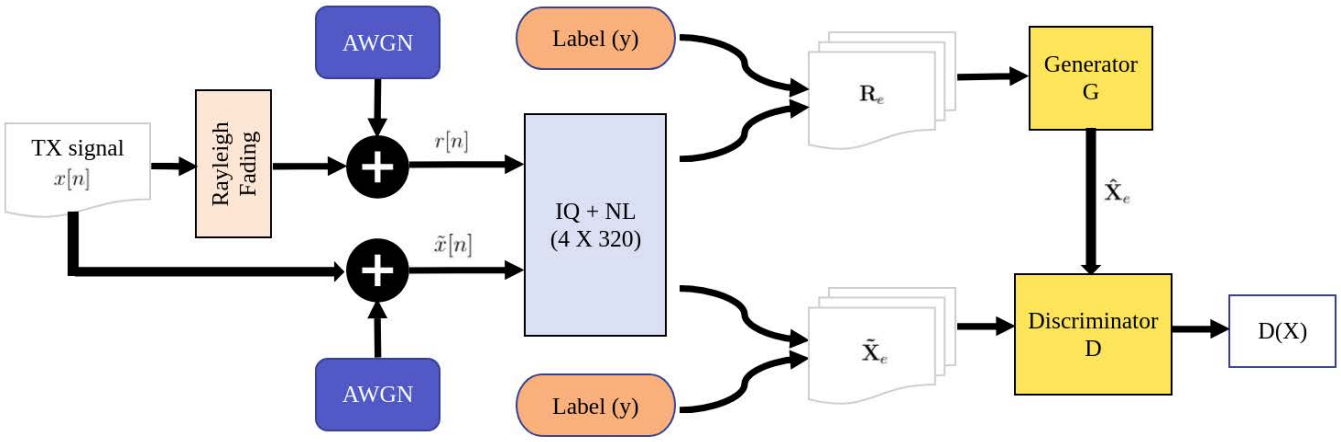


图 2. 条件生成对抗网络训练：展示用于训练 G 的流程图，以实现信道均衡，同时保留所利用的发射机特定的SEI特征。

条件生成对抗网络（CGAN）最早在 [105] 中提出，是对 [104] 中介绍的传统生成对抗网络（GAN）的扩展。在 CGAN 中，图 2 所示的 G和 D 网络接受类别标签 y 作为额外输入；因此，两个映射函数 G（z）和D（X）均以变量 y 为条件，传统 GAN 的极小极大优化方程则改写为 [105],

$$\min_G \max_D V(D,G) = E_{x\sim P_d(x)}\{\log[D(x|y)]\} + E_{z\sim P_z(z)}\{\log[1-D(G(z|y))]\}, \quad (18)$$

其中， $P_d(x)$是由 G学习到的训练数据分布。在本研究中，类别标签与输入一同输入到G和 D，并通过隐藏表示使 GAN能够估计以y 为条件的一对多生成函数，而非传统的一对一映射。隐藏表示由嵌入层生成，该层将每个发射机的类别标签映射为长度为五十的向量。需要注意的是，向量长度是根据 [106]通过经验确定的。标签向量的长度通过全连接层扩展至1,280，并重塑为 4×320 张量，以匹配其对应前导码的维度。将 4×320标签附加到相应发射机经归一化的 IQ+NL 前导码表示上，形成带有 4×320×2 标签的前导码表示，记为$\mathbf{R}_e$。

在 CGAN 训练过程中， G的输入是前导码 $\mathbf{R}_e$~，而 D 的输入是一组仅含加性高斯白噪声的前导码 $\mathbf{X}_e$ （即这组信号中不存在多径效应）。 G 尝试学习受多径影响的前导码的分布，并估计函数 $G(z)$，将其映射为 ˆ ˆ$\mathbf{X}_e$ ，使 $\mathbf{X}_e$ 的分布与~所关联的、用于训练 D的仅含加性高斯白噪声的前导码 $\mathbf{X}_e$ 的分布相匹配。 D 输出一个单值 $D(x)$，表示输入 x 来自训练数据$\mathbf{X}^e$ˆ而非$\mathbf{X}_e$的~概率。CGAN 使用反向传播进行训练，小批量大小为 256 个张量，训练 10,000 轮，并采用交替方案：根据给定的 G，对 D 训练 S 步。训练 S 步可得到最佳版本的 D。 [104] 的作者将 S 视为超参数

其中， $S = 1$ 的计算复杂度最低；因此，在第 V 节所呈现的结果中，S 设为 1。D 通过前向传播和反向传播进行训练，目标是最大化 $V(D,G)$，以获得最高的正确决策概率。经过 $S = 1$ 步后，使用随机梯度下降（SGD）训练 G，以最小化 $V(D,G)$，从而降低 D做出正确决策的能力。此训练过程持续进行，直到 $D(x) = 0.5$ 处处成立，或训练迭代总次数达到经验选定的 10,000 次。

表 II 用于 CGAN 均衡射频指纹识别的生成器 G、判别器 D 和 RF-DNA 指纹分类器对应的神经网络配置。

Model	Layer	Dimension	Activation
Generator (G)	Input	4 X 320 X 2	none
	Convolution 2D	3 X 3 X 64	relu
	Max Pooling 2D	2 X 2	none
	Convolution 2D	3 X 3 X 32	relu
	Max Pooling 2D	1 X 2	none
	Convolution 2D	2 X 3 X 8	relu
	De-Convolution 2D	2 X 3 X 16	relu
	UP-Sampling	1 X 2	none
	De-Convolution 2D	2 X 3 X 16	relu
	UP-Sampling	2 X 2	none
	De-Convolution 2D	2 X 3 X 8	relu
	Dropout 2D	0.5	none
	De-Convolution 2D	1 X 3 X 2	linear
Discriminator (D)	Input	4 X 320 X 2	none
	Convolution 2D	3 X 3 X 64	relu
	Max Pooling 2D	2 X 2	none
	Convolution 2D	3 X 3 X 32	relu
	Max Pooling 2D	1 X 2	none
	Convolution 2D	3 X 3 X 8	relu
	Flatten	none	none
	Dropout	0.5	none
	Dense	128	relu
	Dense	1	sigmoid
Fingerprinting Classifier	Input	4 X 320 X 2	none
	Convolution 2D	3 X 3 X 64	relu
	Max Pooling 2D	2 X 2	none
	Convolution 2D	3 X 3 X 32	relu
	Max Pooling 2D	1 X 2	none
	Convolution 2D	3 X 3 X 8	relu
	Flatten	none	none
	Dropout	0.5	none
	Dense	128	relu
	Dense	4	softmax

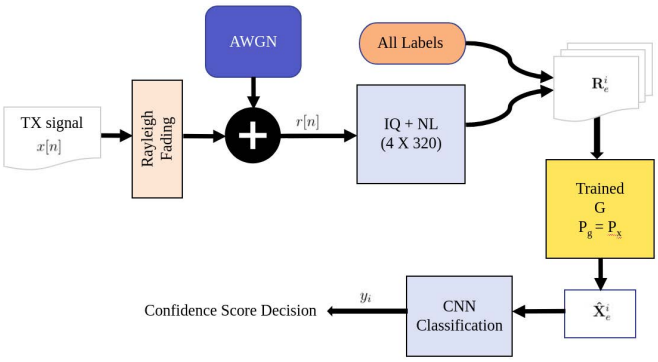


图 3. SEI过程示意图：利用训练好的条件生成对抗网络的 G 网络执行多径信道均衡，同时保留CNN分类前所利用的发射机特定RF-DNA指纹识别特征。

CGAN 训练完成后，将所得的 G（它提供映射函数 $G(z|y,\theta_g)$）与 D断开，并用于均衡由构成 $x[n]$测试集的 N_T 前导码生成的多径前导码 $r[n]$ 。使用本节前面所述的隐藏表示，将每个测试前导码 $r[n]$ 分别与 $N_D = 4$个标签组合，从而生成总计四个带标签的前导码 $\mathbf{R}_e^i$，其中 $i = 1,2,3,4$。训练好的 G 会生成与每个带标签前导码 $\mathbf{R}_e^i$对应的均衡输出 $\hat{}\mathbf{X}_e^i$。最后，在使用训练好的卷积神经网络进行分类之前，从 G的输出 $\hat{}\mathbf{X}_e^i$ 中移除第二个信道（又称隐藏表示标签）。该过程如图 3 所示。

CNN使用以下方法进行训练：(i) 4×320 张量，这些张量由利用仅含加性高斯白噪声 训练集 $\tilde{x}[n]$生成的 IQ+NL 前导码表示构成；(ii) 反向传播；(iii) 使用随机梯度下降最小化分类交叉熵损失函数；(iv)l_2-范数正则化以减少过拟合；以及 (v) 使用 Adam优化调整网络权重 [107]。CNN的输出层使用 Softmax 判决，为i^{th} 均衡后的表示 $\hat{}\mathbf{X}_e^i$ 分配标签 y_i ，依据如下，

$$y_i = \max_j (Q_{ij}), \tag{19}$$

其中， Q_{ij}是针对 i^{th}均衡后表示输入 $\hat{}\mathbf{X}_e^i$的 j^{th}CNN输出，$j = [1,2,3,4]$ 是 Softmax层输出的索引， $i = [1,2,3,4]$ 是给定接收前导码$r[n]$时的值。最后，使用置信度评分决策为接收的多径前导码 $r[n]$ 分配满足以下条件的标签 $\hat{}y$ ，

$$\hat{y} = \max_i (y_i) = \max_i \max_j (Q_{ij}). \tag{20}$$

通过在低于测试集信噪比的条件下训练卷积神经网络，可以获得最佳的特定发射机识别性能。通过网格搜索确定卷积神经网络的最佳训练信噪比，从而在所有信噪比下获得最高的特定发射机识别性能。例如，使用在 12 dB 信噪比下采集的前导码训练卷积神经网络；训练完成后，该网络对信噪比范围为 9 dB 至 30 dB、相邻信噪比值间隔为 3 dB 时采集的前导码进行分类。“最佳”训练信噪比是指其对应的已训练卷积神经网络在所有信噪比下取得最高平均分类正确率的信噪比。条件生成对抗网络的特定发射机识别过程可通过以下算法概述：

B. 使用 *JCAECNN* 进行多径均衡

该均衡方法采用联合卷积自编码器与卷积神经网络（CAE 和 CNN，亦称 JCAECNN）架构，与 [61] 中使用的架构类似；不过，此处所述方法与 [61] 中的方法不同，其卷积自编码器架构由多个解码器头组成，而非单个解码器头。解码器头将经历瑞利衰落的接收前导码分解为发射信号 $x[n]$ 的 L 个加权延迟副本。如图 4 所示，JCAECNN 均衡过程基于单输入多输出（SIMO）系统构建，该系统包括：信号采集与检测（第 III-A 节）、多径衰落与加性高斯白噪声缩放（第 III-C 节），以及在均衡与分类之前按照我们此前的工作 [87] 进行的信号预处理。

均衡通过卷积自编码器实现，该自编码器由一个编码器和 L 个解码器头组成（即瑞利衰落信道中每条路径对应一个解码器头），输入为所选信噪比下前导码的 IQ+NL 表示。受 [108], 中所述结果的启发，我们采用密集连接卷积网络（DenseNet）来实现图 4 所示的“共享”编码器。DenseNet 由多个密集块组成，每个密集块通过将每个卷积层连接到同尺寸的所有前序卷积层而构建。这些密集连接使每个卷积层都能访问此前生成的所有特征图，从而实现特征复用。本研究使用两个密集连接块构建编码器。DenseNet 编码器生成压缩表示 h（$\mathbf{R}[m,n]$），并将其作为输入共享给以下各神经网络架构： L 解码器头和分类器。由此得到的 JCAECNN 架构基于方程 (8) 的平方误差函数构建。其优化目标是最小化接收信号 r（m）与利用方程 (3) 中的抽头延迟线生成的延迟缩放副本 $C_k = \alpha_k x$（$m - \tau_k$）之间的误差。每个解码器头的目标是重建一个对应于瑞利衰落信道中 k^{th} 路径的副本 C_k。除解码器头外，还使用卷积神经网络分类器（CNN_I），通过 Softmax 判决将压缩表示 h（$\mathbf{R}[m,n]$）分配给 $N_D = 4$ 个发射器中的任意一个。共享编码器、解码器头和 CNN_I 分类器的神经网络配置见表 III。

JCAECNN 通过迭代训练来联合优化给定的组合损失函数，

$$F(\theta) = \sum_{k=1}^{L} \left[\lambda_k \times M(m,\tau_k) + \lambda_c \times C(y_c, \tilde{y_c})\right], \tag{21}$$

其中， λ_k 是 k^{th} 解码器头针对每条瑞利衰落路径的损失权重，λ_c 是卷积神经网络的损失权重，M（m，τ_k）是均方误差损失，其定义如下：

$$M(m,\tau_k) = \frac{1}{N_s} \sum_{m=1}^{N_s} (x(m-\tau_k) - \hat{x}(m-\tau_k))^2 \tag{22}$$

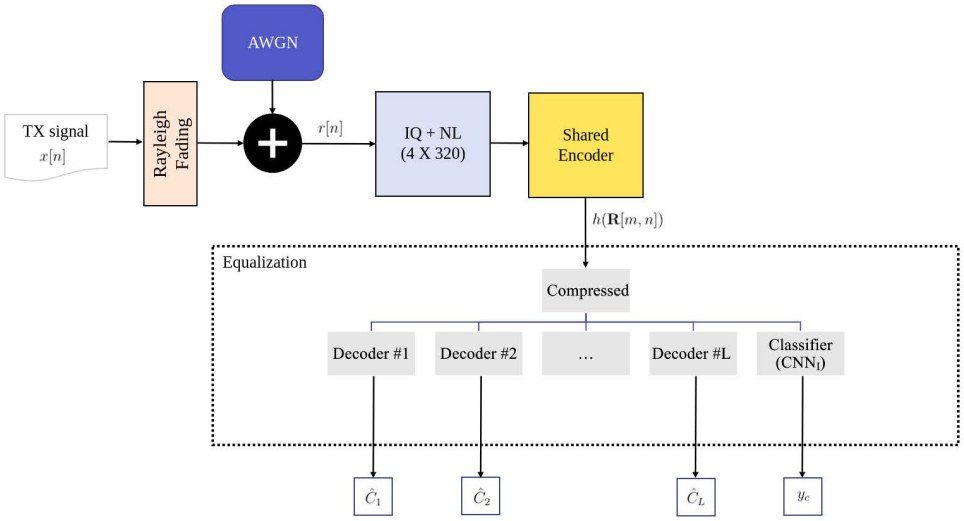


图 4. *JCAECNN* 训练：展示信号预处理和联合 CAE 多径均衡的流程图。

其中，$\hat{x}(m-\tau_k) = \hat{C}_k$ 是解码器针对 k^{th} 路径的输出，而 $C(y_c, \hat{y}_c)$ 是卷积神经网络分类器用于计算真实标签 y_c 与估计标签$\hat{y}_c$之间差异的类别交叉熵函数。如果真实标签采用独热编码，其中$y_c = [y_{c,1}, y_{c,2}, \ldots, y_{c,N_D}]$，则类别交叉熵可按以下公式计算：

$$C(y_c, \hat{y}_c) = -\sum_{l=1}^{N_D} (y_{c,l} \times \log(\hat{y}_{c,l})) \tag{23}$$

其中，l 是独热编码真实值和分类器 [109] 输出层中的类别索引。通过更新分配给所选衰落路径的共享编码器和解码器头的权重，优化单条衰落路径的均方误差损失。

解码器头训练使共享编码器能够学习

表 III JCAECNN 射频指纹识别中共享 DenseNet 编码器、解码器头和 RF-DNA 指纹分类器所关联的神经网络配置

Model	Layer	Dimension	Activation
Shared Encoder (DenseNet)	Input	4 X 320 X 1	none
	Convolution 2D	3 X 3 X 64	relu
	Convolution 2D	3 X 3 X 64	relu
	Convolution 2D	3 X 3 X 64	relu
	Max Pooling 2D	2 X 2	none
	Convolution 2D	2 X 3 X 16	relu
	Convolution 2D	2 X 3 X 16	relu
	Convolution 2D	2 X 3 X 16	relu
Decoder Head	De-Convolution 2D	2 X 3 X 16	relu
	UP-Sampling	2 X 2	none
	De-Convolution 2D	3 X 3 X 32	relu
	Dropout 2D	none	none
	De-Convolution 2D	2 X 3 X 8	relu
	De-Convolution 2D	1 X 3 X 1	linear
Fingerprinting Classifier Head	Convolution 2D	2 X 3 X 8	relu
	Max Pooling 2D	1 X 2	none
	Flatten	none	none
	Dropout	0.5	none
	Dense	128	relu
	Dense	4	softmax

压缩且时延不变的 SEI 特征。训练 CNN 分类器头，以最小化真实标签 y_c 与估计标签 $\tilde{y}_c$之间的 C 损失，从而使共享编码器学到的 SEI 特征比训练解码器头时学到的特征更具判别力。

如图 5 所示，训练后的 JCAECNN 将均衡后的前导码 C_k– $k = 1, 2, \cdots, L$–以及针对每个归一化 IQ+NL 前导码表示$\mathbf{R}[m,n]$ 的 CNN_I 决策 $\tilde{y}_c$ 提供给判别 CNN，该网络记作 CNN_D。CNN_D 为所有 k 分配 C_k 类别标签 y_k，并根据 y_k和 y_c中的最高投票结果，判断接收前导码是由哪个类别标签对应的发射机发送的。CNN_D 的架构与表 II 所示的 RF-DNA 指纹分类器架构相似，并使用与仅含加性高斯白噪声的 JCAECNN 相同的数据集进行训练（即信号集中不存在多径效应）。

V. 结果

本节介绍并分析基于 RF-DNA 指纹的特定发射机识别实验结果，研究对象为信号经过瑞利衰落信道且信噪比不断降低的 IEEE 802.11a Wi-Fi 发射器；实验采用 CGAN 和 JCAECNN 方-

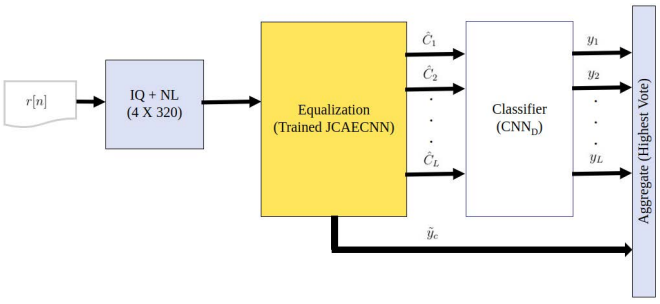


图 5. *JCAECNN* 测试：流程图展示了使用经过训练的 JCAECNN 系统进行射频指纹DNA识别的过程，该系统执行信道均衡并提供 CNN_I 判决，以形成汇总 CNN 分类判决。

法，分别如第 IV-A 节和第 IV-B 节所述。下文将展示以下实验的结果。

1) 实验 *#1*：在 [38], [41] 中发表的瑞利衰落条件下发射机射频指纹识别研究基础上，对比评估 CGAN、JCAECNN 两种方法与我们的方法。

2) 实验 *#2*：对 CGAN 和 JCAECNN 方法进行可扩展性分析。本实验使用由以下数量的商用发射机采集的信号构成的数据集，评估这两种方法的特定发射机识别性能：4、8、16 和 32 个，以代表规模更大的物联网设备部署。

3) 实验*3*：使用实验 #2 的 16 个发射机信号集，以及与 [88], [89] 中所呈现已发表结果相关的公开数据集，评估 JCAECNN 的特定发射机识别性能。本实验评估 JCAECNN架构从多径信号中学习特定发射机识别判别特征的有效性；这些信号的发射机在制造商、型号或尺寸、重量和功耗成本（SWaP-C）方面与 III-B 节所述发射机不同。此外，本实验结果还可作为基准，以便评估未来的研究工作。

4) 实验 *#4*：本实验使用一种损失函数评估 JCAECNN 的特定发射机识别性能，该损失函数的权重根据瑞利衰落信道的路径方差进行选择。本实验优化均方误差损失权重，以最大化 JCAECNN 的性能。

数据集、训练和测试方法的具体细节将在各实验对应的章节中说明。

A. 实验 *#1* 的结果

本实验使用的 IEEE 802.11a Wi-Fi 信号集由从四个 Cisco AIR- CB21G-A-K9 Wi-Fi发射器中提取的前导码组成，这些发射器在第 III-B 节中进行了描述，并用于生成我们先前出版物 [38], [41] 中所呈现的结果。四个发射器中的每一个均提取 2,000 个前导码，并将其划分为训练集和测试集，其中每个发射器分别包含 $N_R = 1{,}800$ 个和 $N_T = 200$ 个随机选取的前导码。训练集被复制，以便创建一个仅含加性高斯白噪声的 数据集——该数据集用于 CGAN 的训练——以及一个瑞利衰落加加性高斯白噪声数据集。测试集仅包含受到瑞利衰落加加性高斯白噪声影响的前导码。需要注意的是，瑞利衰落信道由 $L = 5$ 条路径组成，按照第 III-C 节所述生成并应用于每个信号，并且每个前导码对应的信道都是唯一的（即每次传输时信道系数都会发生变化）。通过向每个前导码添加经过缩放且采用相同滤波器处理的加性高斯白噪声来实现特定的信噪比，并将该过程重复十次，以便进行蒙特卡洛仿真。特定发射机识别性能通过评估信噪比为 9 dB 至 30 dB、相邻取值之间步长为 3 dB 时的平均分类正确率来衡量。

CGAN 和 JCAECNN 方法的训练分别按照第 IV-A 节和第 IV-B 节进行。请注意，通过使用低于测试集所包含信噪比值的数据训练 CGAN，可使其特定发射机识别性能达到最大。

表 IV：在信噪比为 SNR_T 时对测试集前导码进行分类，能够最大限度提升条件生成对抗网络的特定发射机识别性能的训练信噪比，记作 SNR_R。所有信噪比值均以分贝为单位。

SNR_T	SNR_R
9	9
12	9
15	9
18	12
21	15
24	15
27	15
30	18

网格搜索的结果（如第 IV-A 节所述）列于表 IV，其中 SNR_R 表示用于训练 CGAN 的前导码的信噪比，SNR_T 表示由在 SNR_R下训练的 CGAN 分类的前导码的信噪比。JCAECNN 方法的“最佳”训练信噪比采用与 CGAN 相同的方法确定；对于所有 SNR_T 值，得到的 SNR_R 均为 9 dB。 [41] 提出的分区时域射频指纹识别（PTRFF）方法和 [38] 提出的传统时频特征工程射频指纹识别（TFRFF）方法，均使用第 III-D1 节和第 III-D2 节所述的 N-M 信道估计器和 MMSE信道均衡器进行信道校正。PTRFF 方法使用预训练的一维卷积神经网络对分区后的时域 IQ 前导码进行分类。通过使用长度为 $N_w = 64$ 的滑动窗口切分每个均衡前导码的 IQ 样本，生成时域分区。TFRFF 方法从根据前导码 IQ 样本计算出的归一化伽博系数中提取特征，并使用多重判别分析/最大似然（MDA/ML）分类器进行分类。关于 PTRFF 和 TFRFF 方法的具体方法、结果、分析和结论，请分别参阅 [41]和 [38]。

CGAN、JCAECNN、PTRFF 和 TFRFF 特定发射机识别方法的平均分类正确率如图 6 所示。每个数据点对应 $N_T \times N_z \times N_D = 8{,}000$ 次单独的分类决策。通过将 λ_k 和λ_c 设为 1，得到 JCAECNN 的结果。与 PTRFF 和 TFRFF 方法相比，图 6 的结果表明，当信噪比为 18 dB 或更低时，CGAN 和 JCAECNN 方法的平均分类正确率更高。对于所有信噪比值，CGAN 方法的平均分类正确率均为最佳；在信噪比为 30 dB 时最高可达 99.85%，在信噪比为 9 dB 时最低为 95%。根据图 6 的结果，第 IV 节所介绍的半监督学习方法所采用的基于深度学习的均衡，能够更好地补偿多径信道效应，同时保留特定发射机识别特征。

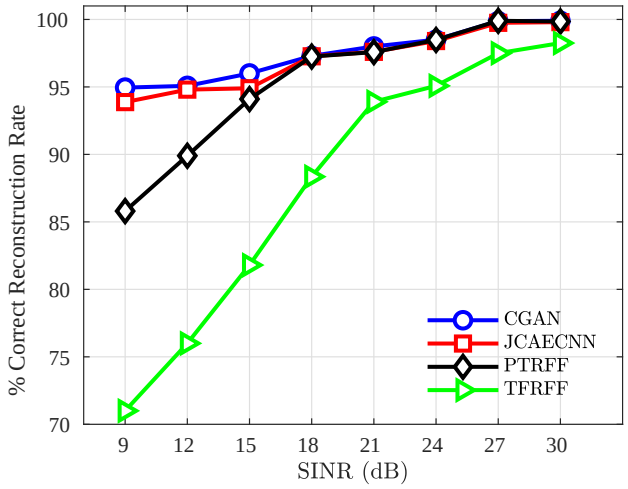


图 6. 实验 *#1* 结果：使用 CGAN、JCAECNN、PTRFF 和 TFRFF 方法，在信噪比∈[9, 30] dB（步长为 3 dB）条件下，对 $N_D = 4$ 个 IEEE 802.11a Wi-Fi 发射器进行分类的平均正确率。

B. 实验 *#2* 的结果

为反映更大规模的物联网设备部署，我们在发射器数量增加的情况下评估 CGAN 和 JCAECNN 均衡与分类方法。待识别发射器的数量为： $N_D = [4, 8, 16, 32]$。这项补充评估使用从 32 个 TP-Link AC1300 USB Wi-Fi 适配器发射的信号中提取的前导码进行。评估涵盖以下四种场景。

- 场景 *#1*： N_B = 10,000 个前导码，从发射器 #1 到发射器 #4 传输的信号中提取。
- 场景 *#2*： N_B = 10,000 个前导码，从发射器 #1 到发射器 #8 传输的信号中提取。
- 场景 *#3*： N_B = 10,000 个前导码，从发射器 #1 到发射器 #16 传输的信号中提取。
- 场景 *#4*： N_B = 10,000 个前导码，从发射器 #1 到发射器 #32 传输的信号中提取。

对于每种场景，在添加经缩放且采用相同滤波方式的加性高斯白噪声之前，先将一个独特的 $L = 5$ 瑞利衰落信道与每个采集到的前导码进行卷积，使信噪比达到 9 dB 至 30 dB，相邻信噪比取值间隔为 3 dB，并且每个信噪比对应十种噪声实现。CGAN 和 JCAECNN 方法按照本节前文所述的相同流程，对每种场景的前导码进行均衡和分类；但对于每个信噪比、噪声实 $N_R = 8,\ 000$ 和 $N_T = 2,\ 000$，以及每个发射机，均采用上述设置。四种场景下 CGAN 和 JCAECNN 方法的平均分类正确率如图 7 所示，其中 CGAN_i 和 JCAECNN_i分别表示 CGAN 和 JCAECNN 在i^{th} 场景中的性能结果。

图 7 展示了实验 #2 的全部四种场景下的平均分类正确率结果。在区分四个发射器时，两种方法的表现与图 6 所示相近，其中 CGAN 方法在所有信噪比下均取得了更高的平均分类正确率。随着待识别的发射器数量增加，JCAECNN 方法的表现开始超过 CGAN 方法。当使用总共十六个发射器时（即场景 #3），JCAECNN 在所有信噪比下的表现至少比 CGAN 方法高 1%。当使用全部三十二个发射器时（即场景 #4），JCAECNN 在所有信噪比下的表现均超过 CGAN 方法。提升幅度最小为信噪比 18 dB 时的 5%，最大为信噪比 9 dB 时的 11%。

图 7 显示，随着待识别发射器数量从 4 个增加到 32 个，JCAECNN 的性能下降较少；因此，该方法更适用于规模更大的物联网部署。CGAN 方法性能较差，原因在于发射器数量从 4 个增至 32 个时， G 需要学习的条件分布数量随之增加，这一问题又因隐藏标签表示效率降低而加剧。从决策复杂度来看，对于每个接收前导码 $r[n]$，JCAECNN 总共进行 $L + 1$ 次 CNN 决策，分别对应重构后的 C_k 和 CNN 分类器的输出 $\hat{}y_c$。JCAECNN 的分类次数不取决于发射器（即标签）的数量，而 CGAN 并非如此。在 CGAN 方法中，将前导码 $r[n]$ 分配给标签 y，需要由 G 执行总计 N_D 次均衡操作，随后再进行 N_D 次顺序分类。这是因为发射机的身份未知，因此必须将前导码与每个已知发射机的类别进行比较。因此，随着发射器数量线性增加， G 所学习的条件分布数量，以及 CGAN 均衡和分类决策的数量也会随之增加。

C. 实验*3*结果

基于第五节B部分所呈现的结果，本节中的结果仅使用JCAECNN方法生成。图8显示了平均分类正确率，每

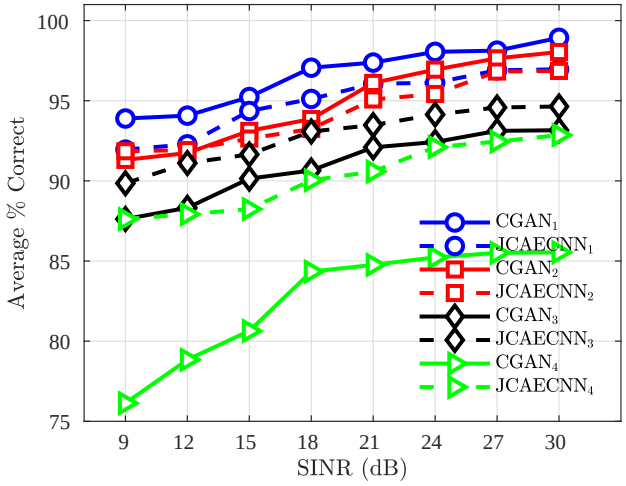


图 7. 实验 *#2* 结果：采用 CGAN 方法 JCAECNN 时，针对信噪比为∈[9, 30] dB（以 3 dB 为步长），最多 $N_D = 32$ 个 IEEE 802.11a TP-Link 适配器的平均分类正确率表现。请注意，下标表示场景编号。

个数据集均包含从至少十六个符合IEEE802.11a Wi-Fi标准的发射器采集的信号，展示了JCAECNN方法在以下三个不同数据集上的性能。

- 数据集 *#1*：该数据集由用于生成图 7 所示并在第 V-C 节中说明的场景 #3 结果的 IEEE 802.11a Wi-Fi 前导码组成。该数据集的结果标记为“TP-Link”。

- 数据集 *#2*：该数据集由 [88] 的作者收集，用于评估基于卷积神经网络的优化无线电分类（ORACLE）方法。该数据集包含使用一台固定的 Ettus Research USRP B210 软件定义无线电（SDR）作为接收机，从 16 台 USRP X310 软件定义无线电（SDR）采集的 IEEE 802.11a Wi-Fi 信号。需要注意的是，B210 接收机的采样率设为 5 MHz，低于此前用于生成所示结果的所采集信号的 20 MHz 采样率。该数据集的结果标记为“ORACLE”。

- 数据集 *#3*：该数据集由 [89] 的作者采集，并命名为 WiFi Signal (WiSig) 数据集。WiSig 数据集包含为期四天采集的 IEEE 802.11a Wi-Fi 信号，共来自 174 个发射器，包括 USRP B210、X310 和 N210 软件定义无线电，并由 41 台 USRP 接收机接收。为与另外两个数据集及本文其余结果保持一致，仅使用 WiSig 信号中单日、单台接收机采集的数据。所选 WiSig 信号通过对前导码的 STS 部分进行自相关检测，然后重采样至 20 MHz。该数据集的结果标记为“WiSig”。

与场景 #3 中的 TP-Link 数据类似，在添加经过缩放且采用相同滤波方式的加性高斯白噪声之前，Oracle 和 WiSig 数据集中的每个信号都会先经过一个独立的$L = 5$ 瑞利衰落信道处理，以实现 9 dB 至 30 dB 的信噪比，相邻信噪比之间间隔 3 dB，且每个信噪比对应十种噪声实现。之后，JCAECNN 方法按照本节前文所述进行均衡和分类。为保持一致，从 WiSig 数据集中随机选取 16 个发射器，使其与 TP-Link 和 ORACLE 数据集所含的发射器数量一致。对于 TP-Link 和 Oracle 数据集，$N_R = 8,000$ 和 $N_T = 2,000$。对于 WiSig 数据中单日、单台接收机采集的数据，每个发射器采集的信号总数为 1,000；因此，

$N_R = 800$ 和 $N_T = 200$，以提供与另外两个数据集一致的比例。图8所示的平均分类正确率结果表明，尽管训练样本数量有限，JCAECNN对WiSig前导码进行均衡和分类的性能仍优于ORACLE数据在所有信噪比下的表现。这可能归因于采集ORACLE数据时使用的采样率较低，仅为TP-Link和ORACLE数据采样率的25%。此外，WiSig数据集包含多种型号的USRP，而ORACLE信号均由同一型号的USRP发射。后者

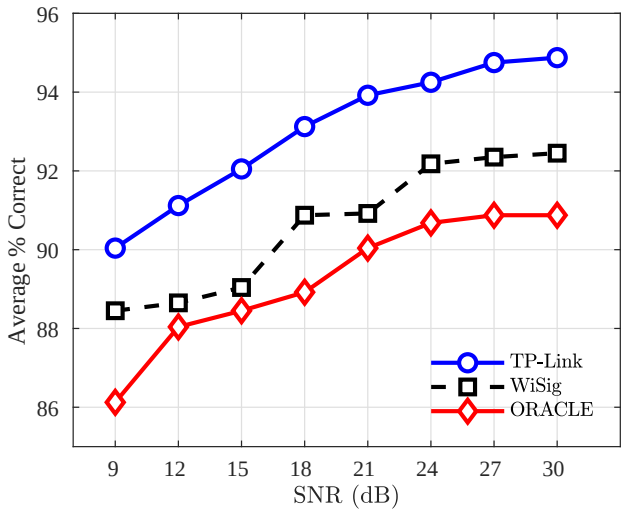


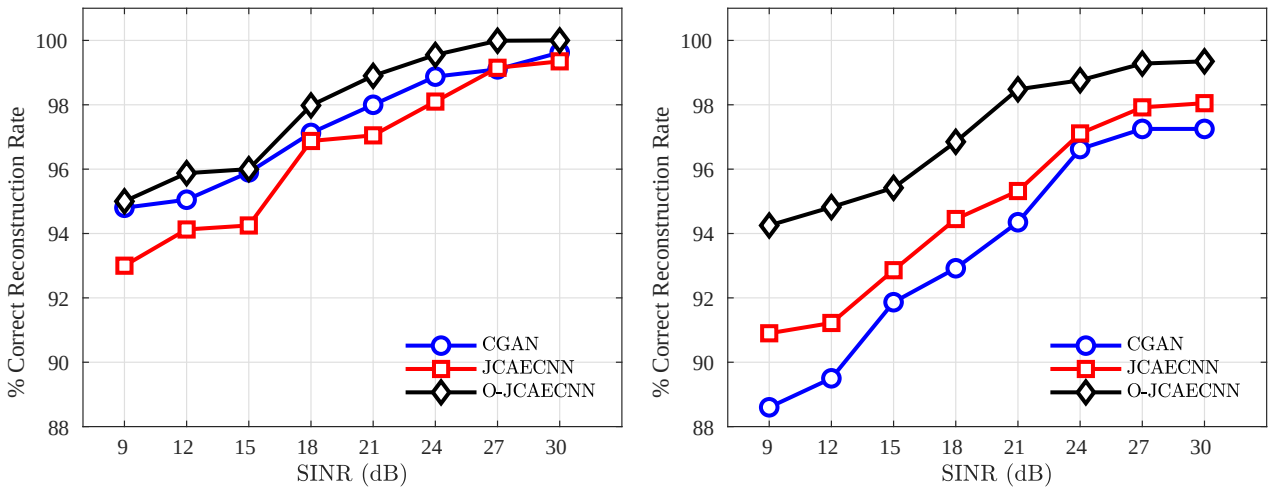
图8。实验*3*结果：采用 JCAECNN 方法，在相邻信噪比取值间隔为 3 dB 的条件下，针对信噪比为∈[9, 30] dB时，TP-Link、WiSig 和 ORACLE 数据集的平均分类正确率表现。这些数据集均包含从 $N_D = 16$ IEEE 80d2.11a Wi-Fi 发射器采集的信号。

是序列号判别，这是最具挑战性的特定发射机识别情形。此外，ORACLE的USRP X310是一款售价8,500美元的高性能软件定义无线电，采用低差异性组件，这意味着不同软件定义无线电之间的特征差异较小，使特定发射机识别更困难 [88]。

D. 实验 *#4* 的结果

到目前为止，JCAECNN 方法生成的所有结果中，λ_k 和 λ_c 均设为 1。为优化 $L = 5$瑞利衰落信道均衡和分类性能，$k = [1, 2, 3, 4, 5]$ 和λ_c 对应的损失函数权重 λ_k 分别设为 32、16、8、4、2 和 32。这些值的选择依据是：方程（2）中给出的相应瑞利信道路径的方差随 k呈指数衰减。图9展示了采用衰减损失权重的 JCAECNN 方法的平均分类正确率，记为 O-JCAECNN，其中“O”表示“优化”。比较评估采用以下结果：(i) 损失权重相同（即均设为 1）的 JCAECNN 实现结果；(ii) 图 6 所示的 CGAN 结果。

使用 O-JCAECNN 方法，在所有信噪比值为 9 dB 至 30 dB（相邻值间隔 3 dB）时，均可获得更高的平均分类正确率。它是唯一一种在 $N_D = 4$ 情况下实现 100% 平均分类正确率的特定发射机识别方法，该情况出现在信噪比为 27 dB 和 30 dB 时。图 10 是与图 9(b) 所示 9 dB O-JCAECNN 结果相对应的混淆矩阵，旨在展示 $N_D = 16$ 个发射器中每个发射器的分类正确率。可以看出，16 个发射器中有 11 个对应深蓝色对角线条目，表明其分类正确率至少为 95%。



(a) $N_D = 4$ 个发射器。 (b) $N_D = 16$ 个发射器。

图 9. 实验 *#4* 结果：使用 CGAN、JCAECNN 和 O-JCAECNN 方法，对 N_D 个 IEEE 802.11a Wi-Fi TP-Link 适配器在信噪比为 ∈[9, 30] dB、步长为 3 dB 时的平均分类正确率。

例外的是发射器 #3、发射器 #4、发射器 #5、发射器 #6 和发射器 #12，其中只有发射器 #4 的分类正确率未达到 90%。

结果表明，JCAECNN 型号的性能主要受以下因素影响：(i) 方程 (21) 中对应于前几个瑞利衰落路径的损失权重，以及 (ii) 对应于卷积神经网络 $_I$ 分类器头的损失权重 λ_c。这表明，通过优化 JCAECNN 损失函数中前几个且占主导地位的权重，可以实现信道不变射频指纹识别。

VI. 结论与未来工作

本文提出并分析了两种半监督深度学习方法，分别称为 CGAN 和 JCAECNN，旨在瑞利衰落和信噪比不断降低的条件下通过特定发射机识别提升物联网安全。这些方法能够从信号中提取具有判别力的射频指纹DNA特征

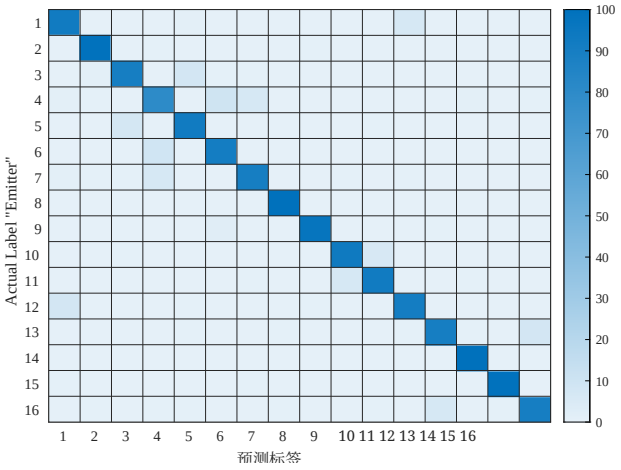


图 10. 实验 *#4*结果：混淆矩阵，显示场景 #3（第五节B部分）中提供的 $N_D = 16$ 个 IEEE 802.11a Wi-Fi TP-Link 适配器各自的分类正确率百分比，采用 JCAECNN 方法，信噪比为 $= 9$ dB。平均分类正确率为 94.25%。

这些信号由最多三十二个 IEEE 802.11a Wi-Fi 发射器发射，并经过 $L = 5$ 瑞利衰落信道传播。这两种架构都能够从接收的多径失真版本中重建所发射的前导码，同时借助具有信噪比鲁棒性的 IQ+NL 前导码表示保留特定发射机识别的判别特征。本文将这两种半监督学习方法与传统的射频指纹DNA方法进行了比较，结果见 [38], [41]。随着发射器数量从 $N_D = 4$ 增加到 $N_D = 32$, JCAECNN 方法表现出更好的可扩展性；而 CGAN 方法则不然，因为前导码重建和分类决策的数量会随发射器数量线性增加。在信噪比为 9 dB 及以上时，对于十六个 IEEE 802.11a Wi-Fi 发射器，O-JCAECNN 的平均正确分类率超过 94%，表现更优。

未来研究将通过修改条件生成对抗网络和 JCAECNN 架构，提升基于特定发射机识别的物联网安全的可行性，以实现：（i）检测训练信号集中未包含的发射机；（ii）整合 [110] 中提出的协作学习方案，以利用同步训练。[111] Goldsmith，A.（2005年）。《无线通信》。剑桥：剑桥大学出版社。doi:10.1017/CBO9780511841224

参考文献

[1] Maayan, G.，《2020年物联网概览：统计数据、风险与解决方案》，https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for-2020.aspx，2020年1月。[2] Rawlinson, K.，《惠普研究揭示70%的物联网设备易受攻击》，2014年7月。 [在线]。网址：https://www
8 =1744676 .
[3]
hp.com/us/en/hp-news/press-release.html?id Ray, I.、D. Kar、J. Peterson 和 S. Goeringer，《物联网领域中放弃密码学的设备身份与信任》，载于国际协作与互联网计算会议（*CIC*），2019年。[4] Neshenko, N.、E. Bou-Harb、J. Crichigno、G. Kaddoum 和 N. Ghani，《揭开物联网安全的神秘面纱：物联网漏洞详尽综述及对互联网规模物联网攻击的首次实证考察》，*IEEE*通信调查与教程，第21卷，第3期，页码2702–2733，2019年。

[5] Larsen, S.，《一只智能鱼缸让赌场暴露于黑客攻击风险之下》，网站：https://money.cnn.com/2017/07/19/technology/fish-tank-hack-darktrace/index.html，2017年7月。[6] Wright, J. 和 J. Cache，《无线黑客揭秘：无线安全秘诀与解决方案》，第3版。McGraw-Hill，2015年。[7] Stanislav, M. 和 T. Beardsley，《物联网黑客：婴儿监护暴露风险与漏洞案例研究》，Rapid7，页码1–17，2015年。[8] Wright, J.，《KillerBee：实用的ZigBee漏洞利用框架，或“无线黑客与动能世界”》，页码1–39。 [在线]。网址：https://www.inguardians.com/works/ [9] Simon, S.，《“物联网”黑客攻击导致多个热门网站大范围中断》，美国国家公共广播电台，2016年10月。 [在线]。网址：
h
t
t
p
s://
w
w
w.
w
b
u
r.
o
r
g/
n
p
r/
4
9
8
9
5
4
197/internet-outage-update-internet-of-things-hacking-attack-led-to-outage-of-popular. [10] Shipley, P.，《Insteon：虚假安全与误导性文档》，DEFCON 23，2014年。 [在线]。网址：https://www.youtube.com/watch?v=dy1LTQLmPtM [11] ——。《Insteon射频工具》。2015年。 [在线]。网址：https: //github.com/evilpete/insteonrf [12] Brook, C.，《Mirai物联网僵尸网络共同作者认罪》，Digital Guardian，2017年。 [在线]。网址：https://digitalguardian.com/blog/mirai-iot-botnet-co-authors-plead-guilty/ [13] Li, Y.、D. Li、W. Cui 和 R. Zhang，《基于OSI模型的研究》，载于《2011年IEEE第三届国际通信软件与网络会议》，2011年，页码554–557。[14] Reising, D.，《利用射频指纹DNA进行设备分类与验证：基于GRLVQI的处理》，博士论文，美国空军理工学院，2012年12月。[15] Talbot, C.、M. Temple、T. Carbino 和 J. Betances，《检测商用Insteon家庭自动化系统中的伪装攻击》，《计算机与安全》，第74卷，页码296–307，2017年10月。[16] Sa, K.、D. Lang、C. Wang 和 Y. Bai，《物联网特定发射机识别技术》，IEEE Access，第8卷，页码1644–1652，2019年。[17] Reising, D.、J. Cancelleri、T. D. Loveless、F. Kandah 和 A. Skjellum，《使用射频指纹DNA和支持向量机进行基于无线电身份验证的物联网安全》，IEEE《物联网学报》，第8卷，第10期，2020年。[18] Pang, J.、B. Greenstein、R. Gummadi、S. Seshan 和 D. Wetherall，《802.11用户指纹识别》，载于第13届ACM移动计算与网络年度国际会议论文集，系列：MobiCom ’07。美国纽约：计算机协会，2007年，页码99–110。[19] Dudczyk J.、J. Matuszewski 和 M. Wnuk，《将辐射发射应用于特定发射机识别》，载于《国际微波、雷达与无线通信会议》（IEEE目录号04EX824），第2卷，2004年，页码431–434。[20] Brik, V.、S. Banerjee、M. Gruteser 和 S. Oh，《利用辐射测量特征进行无线设备识别》，载于第14届ACM移动计算与网络国际会议论文集，系列：MobiCom ’08。美国纽约：计算机协会，2008年，页码116–127。[21] Suski W.、M. Temple、M. Mendenhall 和 R. Mills，《通过射频指纹识别商用通信设备以增强电子安全》，《电子安全与数字取证国际期刊》，第1卷，第3期，页码301–322，2008年10月。[22] Danev B. 和 S. Kapkun，《基于瞬态特征的无线传感器节点识别》，载于ACM传感器网络信息处理国际会议，2009年4月，页码25–36。[23] Klein R.、M. Temple、M. Mendenfhall 和 D. Reising，《突发信号检测与射频指纹分类性能的灵敏度分析》，载于IEEE国际通信会议，2009年6月，页码1–5。[24] Liu, M. 和 J. Doherty，《多径信道中特定发射机识别的非线性估计》，《IEEE信息取证与安全汇刊》，第6卷，第3期，页码1076–1085，2011年9月。[25] Kennedy, I. 和 A. Kuzminskiy，《无线多径信道中的射频指纹检测》，载于第七届无线通信系统国际研讨会，2010年9月，页码820–823。[26] Williams M.、S. Munns、M. Temple 和 M. Mendenhall，《用于机场WiMAX通信安全的射频指纹DNA识别》，载于第四届网络与系统安全国际会议，2010年9月，页码32–39。[27] Takahashi, D.、Y. Xiaoa、Y. Zhang、P. Chatzimisios 和 H. Chend，《IEEE 802.11用户指纹识别及其在入侵检测，”*Computers and Math with Applications*，第60卷，第2期，第307–318页，2010年7月。[28] Tekbas, O., O. Ureten 和 N. Serinken，“低信噪比瞬态信号发射机识别系统的改进”，*IEE Electronics Letters*，第40卷，第3期，第182–183页，2004年。[29] Ellis K. 和 N. Serinken，“无线电发射机指纹的特征”，*Radio Science*，第36卷，第4期，第585–597页，2001年。[30] Soliman, S. 和 S-Z. Hsue，“利用统计矩进行信号分类”，*IEEE Transactions on Communications*，第40卷，第5期，第908–916页，1992年。[31] Defence R& D Canada - Ottawa，“用于特定发射机识别与测向的干涉式脉内雷达接收机”，*Fact Sheet REW 224*，2007年6月。[32] Azzouz E. 和 A. Nandi，通信信号的自动调制识别。Springer Science & Business Media，2013年。[33] Reising D.、M. Temple 和 J. Jackson，“利用降维 RF-DNA 指纹对授权与 rogue 设备进行判别”，*IEEE Transactions on Information Forensics and Security*，第10卷，第6期，第1180–1192页，2015年。[34] Wheeler C. 和 D. Reising，“评估载波频率偏移对 RF-DNA 指纹分类性能的影响”，载于*InternationalConference on Computing, Networking and Communications*，2017年1月，第110–114页。[35] Pan, Y.、S. Yang、H. Peng、T. Li 和 W. Wang，“基于深度残差网络的特定发射机识别”，*IEEE Access*，2019年。[36] Fadul, M.、D. Reising、T. D. Loveless 和 A. Ofoli，“利用 RF-DNA 指纹在瑞利衰落条件下对 OFDM 发射机进行分类”，*IEEE Transactions on InformationForensics and Security*，审稿中 - 可查阅：https://arxiv.org/abs/2005.04184，2020年。[37] Fadul M.、D. Reising、D. Loveless 和 A. Ofoli，“利用瑞利衰落信道模型对 OFDM 信号进行 RF-DNA 指纹分类 ”，载于 *IEEEWireless Communications and Networking Conference (WCNC)*，2019年4月，第1–7页。[38] Fadul, M.、J. Willis、D. Reising 和 T. Loveless，“瑞利衰落条件下优化特定发射机识别的过程参数分析”，载于*Global IoT Summit (GIoTS)*，2022年6月（已录用）。[39] Fadul, M，“瑞利衰落信道效应对 RF-DNA 指纹识别过程的影响”，硕士论文，University of Tennessee - Chattanooga，2018年8月。[40] Kandah, F.、J. Cancelleri、D. Reising、A. Altarawneh 和 A. Skjellum，“面向大规模物联网/信息物理系统的身份、信任与韧性的软硬件协同设计方法”，载于*International ConferenceonInternetofThings (iThings)andIEEEGreen Computing andCommunications (GreenCom)andIEEE Cyber,Physical andSocialComputing (CPSCom) and IEEE Smart Data (SmartData)*，2019年7月，第1125–1134页。[41] Fadul, Mohamed K.、Reising, Donald R. 和 Sartipi, Mina，“利用 RF-DNA 和深度学习在瑞利衰落条件下识别基于 OFDM 的无线电设备”，*IEEE Access*，第9卷，第17 100–17 113页，2021年。[42] Defense Advances Research Projects Agency (DARPA)，“频谱协作挑战——利用人工智能释放射频频谱的真正潜力”，https://archive.darpa.mil/sc2/，2017年。[43] Yu, Yiding、Wang, Taotao 和 Liew, Soung Chang，“面向异构无线网络的深度强化学习多址接入”，载于*2018 IEEEInternational Conference onCommunications (ICC)*，2018年，第1–7页。[44] O’Shea T. 和 J. Hoydis，“物理层深度学习导论”，*IEEE*认知通信与网络汇刊，第3卷，第4期，2017年12月。[45]Defense Advances Research Projects Agency (DARPA)，“射频机器学习系统”，
h
t
t
p
s://
www.darpa.mil/program/radio-frequency-machine-learning-systems，2019年。[46] Restuccia, F.、S. D’Oro、Salvatore、A. Al-Shawabka、M. Belgiovine、L. Angioloni、S. Ioannidis、Stratis、K. Chowdhury 和 T. Melodia，“DeepRadioID：深度学习无线电指纹算法的实时抗信道优化”，载于*ACM*移动自组织网络与计算国际研讨会，系列：Mobihoc，2019年。[47] Restuccia, Francesco 和 Melodia, Tommaso，“Polymorf：通过物理层深度学习实现多态无线接收机”，载于第二十一届移动网络理论、算法基础与协议设计国际研讨会论文集

与移动计算，系列：Mobihoc '20。美国纽约州纽约市：计算机协会，2020年，第271–280页。 [在线]。可访问：https://doi.org/10 1145 3397166 3409132 。/。Qin, Zhijin、Ye, Hao、Li, Geoffrey Ye 和 Juang, Biing-Hwang Fred，“物理层通信中的深度学习”，IEEE无线通信，第26卷，第2期，第93–99页，2019年。[49] Downey, Joe、Hilburn, Ben、O'Shea, Tim 和 West, Nathan，“未来，设计无线信号的将是人工智能，而非人类”，IEEE Spectrum杂志，2020年4月。[50] Fadul, Mohamed K.、Reising, Donald R.、Arasu, K. T. 和 Clark, Michael R.，“用于增强扩频通信的对抗机器学习”，载于 MILCOM 2021 - 2021 IEEE军事通信会议 (MILCOM)，2021年，第783–788页。[51] Baldini, G. 和 R. Giuliani，“利用时频表示和卷积神经网络评估无线干扰对物联网发射机识别的影响”，载于全球物联网峰会 (GIoTS)，2019年6月，第1–6页。[52] Baldini, G.、C. Gentile、R. Giuliani 和 G. Steri，“基于深度卷积神经网络的辐射特征识别技术比较”，IET电子快报，第55卷，92，2019年2，90第。–页。[53] O'Shea, T.、T. Roy 和 T. Clancy，“基于空口深度学习的无线电信号分类”，IEEE信号处理精选主题期刊，第12卷，第1期，第168–179页，2018年2月。[54] Wong, L.、W. Headley、S. Andrews、R. Gerdes 和 A. Michaels，“对用于发射机识别的原始I/Q数据所提取的卷积神经网络特征进行聚类”，载于 IEEE军事通信会议 (MILCOM)，2018年10月，第26–33页。[55] Mendis, G.、J. Wei 和 A. Madanayake，“结合硬件设计的基于深度学习的无线电信号识别”，IEEE 航空航天与电子系统汇刊，第55卷，第5期，第2516–2531页，2019年10月。[56] Riyaz, S.、K. Sankhe、S. Ioannidis 和 K. Chowdhury，“用于无线电识别的深度学习卷积神经网络”，IEEE通信杂志，第56卷，第9期，第146–152页，2018年9月。[57] Merchant, K.、S. Revay、G. Stantchev 和 B. Nousain，“认知通信网络中用于射频设备指纹识别的深度学习”，IEEE信号处理精选主题期刊，第12卷，第1期，第160–167页，2018年2月。[58] Jafari, H.、O. Omotere、D. Adesina、H. Wu 和 L. Qian，“利用深度学习进行物联网设备指纹识别”，载于 IEEE军事通信会议 (MILCOM)，2018年10月，第1–9页。[59] Guyue, L.、Y. Jiabao、Y. Xing 和 A. Hu，“面向 WiFi 设备的位置无关物理层识别方法”，IEEE Access，第7卷，第06 974–106 986页，2019年8月。[60] Youssef, K.、L. Bouchard、K. Haigh、J. Silovsky、B. Thapa 和 C. Valk，“射频发射机识别的机器学习方法”，IEEE射频识别期刊，第2卷，第4期，第197–205页，2018年12月。[61] Yu, J.、A. Hu、F. Zhou、Y. Xing、Y. Yu、G. Li 和 L. Peng，“基于去噪自编码器的射频指纹识别”，载于2019年无线与移动计算、网络和通信国际会议 (WiMob)。IEEE，2019年，第1–6页。[62] Jian, T.、B. Rendon、E. Ojuba、N. Soltani、Z. Wang、K. Sankhe、A. Gritsenko、J. Dy、K. Chowdhury 和 S. Ioannidis，“射频指纹识别深度学习：大规模实验研究”，IEEE物联网杂志，第3卷，第1期，第50–57页，2020年。[63] Robinson, J.、S. Kuzdeba、J. Stankowicz 和 J. Carmack，“用于射频指纹识别的扩张因果卷积模型”，载于2020年第十届年度计算与通信研讨会暨会议 (CCWC)，2020年，第0157–0162页。[64] Ding, Lida、Wang, Shilian、Wang, Fanggang 和 Zhang, Wei，“基于卷积神经网络的特定发射机识别”，IEEE通信快报，第22卷，第12期，第2591–2594页，2018年。[65] Chen, Peibo、Guo, Yulan、Li, Gang、Wang, Ling 和 Wan, Jianwei，“用于特定发射机识别的判别式对抗网络”，电子快报，第56卷，02，2020年。[66] Peng, Linning、Zhang, Junqing、Liu, Ming 和 Hu, Aiqun，“利用差分星座轨迹图进行基于深度学习的射频指纹识别”，IEEE车辆技术汇刊，第69卷，第1期，第1091–1095页，2020年。[67] Yang, Ning、Zhang, Bangning、Ding, Guoru、Wei, Yimin、Wei, Guofeng、Wang, Jian 和 Guo, Daoxing，“有限样本条件下的特定发射机识别：一种模型无关元学习方法”，IEEE通信快报，第1–1页，2021年。[68] Morin, Cyrille and Cardoso, Leonardo S. and Hoydis, Jakob and Gorce, Jean-Marie and Vial, Thibaud”，编辑=”Kliks, Adrian and Kryszkiewicz, Paweł and Bader, Faouzi and Triantafyllopoulou, Dionysia and Caicedo, Carlos E. and Sezgin, Aydin and Dimitriou, Nikos and Sybis, Michał，“采用监督式深度学习的发射机分类”，载于 认知无线电导向的无线网络。Cham：施普林格国际出版公司，2019年，第73–86页。[69] Behura, Sambit and Kedia, Subham and Hiremath, Shrishail M. and Patra, Sarat Kumar，“Wist id——基于深度学习的大规模无线标准技术识别”，*IEEE Transactions on Cognitive Communications and Networking*，第6卷，第4期，第1365–1377页，2020年。[70] McGinthy, Jason M. and Wong, Lauren J. and Michaels, Alan J.，“基于神经网络的物联网特定发射机识别认证基础”，*IEEE*《物联网学报》，第6卷，第4期，第6429–6440页，2019年。[71] Tang, Peng and Xu, Yitao and Wei, Guofeng and Yang, Yang and Yue, Chao，“基于深度残差收缩网络的物联网设备特定发射机识别”，《中国通信》，第18卷，第12期，第81–93页，2021年。[72] Liu, Yongxin and Wang, Jian and Li, Ji anqiang and Song, Houbing and Yang, Thomas and Niu, Shuteng and Ming, Zhong，“用于准确识别物联网（iot）设备的零偏置深度学习”，*IEEE*《物联网学报》，第8卷，第4期，第2627–2634页，2021年。[73] Zha, Xiong and Chen, Huai and Li, Tianyun and Qiu, Zhaoyang and Feng, Yiwei，“基于复数傅里叶神经网络的特定发射机识别”，*IEEE*通信快报，第1–1页，2021年。[74] Gong, Jialiang and Xu, Xiaodong and Qin, Yufeng and Dong, Weijie，“一种基于生成对抗网络的特定发射机表征与识别框架”，载于 *2019*年第*11*届无线通信与信号处理国际会议（*WCSP*），2019年，第1–6页。[75] Ji, Hao and Wan, Tao and Xiong, Wanan and Liao, Jingyi，“一种基于环线双谱和卷积神经网络的特定发射机识别方法”，载于 *2020 IEEE*第*3*届自动化、电子与电气工程国际会议（*AUTEEE*），2020年，第328–332页。[76] Gong, Jialiang and Xu, Xiaodong and Lei, Yingke，“使用嵌入射频指纹的InfoGAN进行无监督特定发射机识别的方法”，*IEEE Transactions on Information Forensics and Security*，第15卷，第2898–2913页，2020年。[77] Li, Rundong and Hu, Jianhao and Li, Shaoqian and Ai, Weiwei，“基于多域特征学习的特定发射机识别”，载于 *2021 IEEE*人工智能与工业设计国际会议（*AIID*），2021年，第178–183页。[78] Wang, Yu and Gui, Guan and Gacanin, Haris and Ohtsuki, Tomoaki and Dobre, Octavia A. and Poor, H. Vincent，“一种基于复值神经网络和网络压缩的高效特定发射机识别方法”，*IEEE Journal on Selected Areas in Communi- cations*，第39卷，第8期，第2305–2317页，2021年。[79] Qu, Ling-Zhi and Liu, Hui and Huang, Ke-Ju and Yang, Jun-An，“基于多域特征融合和集成学习的特定发射机识别”，《*Symmetry*》，第13卷，第8期，2021年。 [在线]。可获取于：https://www.mdpi.com/2073-8994/13/8/1481[80] Bassey, Joshua and Adesina, Damilola and Li, Xiangfang and Qian, Lijun and Aved, Alexander and Kroecker, Timothy，“使用深度学习进行基于射频指纹识别的物联网设备入侵检测”，载于 *2019*年第*4*届雾计算与移动边缘计算国际会议（*FMEC*），2019年，第98–104页。[81] Wang, Jian and Zhang, Bangning and Zhang, Jie and Yang, Ning and Wei, Guofeng and Guo, Daoxing，“基于深度对抗域适应的特定发射机识别”，载于 *2021*年第*4*届信息通信与信号处理国际会议（*ICICSP*），2021年，第104–109页。[82] Cun, Chentao and Li, Tianyun and Zhu, Jiawei，“基于眼图的特定发射机识别”，载于 *2021 IEEE*第*21*届通信技术国际会议（*ICCT*），2021年，第1261–1265页。[83] Peng, Yinan and Zhou, Yuan，“频域中通过挤压激励神经网络进行特定发射机识别”，载于 *2021*年第*40*2021年，8310 8314届中国控制会议（*CCC*），第–页。[84] Shen, Weiguo and Wang, Wei，“基于卷积神经网络的无线网络节点识别”，载于 *2018*年第*14*届计算智能与安全国际会议（*CIS*），2018年，第238–241页。

[85] Tyler, J., M. Fadul, D. Reising, and F. Kandah，“信号能量影响及其对基于深度学习的特定发射机识别威胁的分析”，载于 *IEEE*国际通信会议（*ICC*），2022年6月。[86] O’Hara, B. and A. Petrick，*IEEE 802.11*手册：设计人员指南。*Standard Information Network*。IEEE出版社，2005年。[87] Tyler, J., M. Fadul, D. Reising, and E. Kaplanoglu，“基于前导码的波形的鲁棒特定发射机识别简化去噪”，载于 *IEEE*全球通信会议，2021年12月。[88] Sankhe, Kunal and Belgiovine, Mauro and Zhou, Fan and Riyaz, Shamnaz and Ioannidis, Stratis and Chowdhury, Kaushik，“ ORACLE：基于卷积神经网络的优化无线电分类”，载于 *IEEE INFOCOM 2019 - IEEE*计算机通信会议，2019年，第370–378页。[89] Hanna, Samer and Karunartne, Samurdhi and Cabric, Danijela，“WiSig：一个用于与接收机和信道无关的射频指纹识别的大规模Wi-Fi 信号数据集”，*IEEE Access*，第10卷，第22 808–22 818页，2022年。[90] Lajos, H., A. Yosef, W. Li, and J. Ming，面向*LTE*、*Wi-Fi*和*WiMAX*的*MIMO-OFDM*。John Wiley and Sons, Ltd.，2011年。[91] Liu, M. and J. Doherty，“使用非线性设备估计的特定发射机识别”，载于 *IEEE Sarnoff*研讨会，2009年3月，第1–5页。[92] WiSilica，“六大物联网通信协议”，https://wisilica.com/company/top-6-iot-communication-protocols/，2020年8月。[93] *IEEE*标准*802.11-2007*，局域网和城域网，第*11*部分：无线局域网介质访问控制（*MAC*）和物理层（*PHY*）规范，IEEE，2007年6月。[94] *Agilent E3238*信号截获与采集解决方案：系列概览，Agilent Technology Inc.，美国，出版物5989-1274EN，2004年7月。[95]Hijazi, H. and L. Ros，“OFDM系统中采用载波间干扰抑制的时变多径增益多项式估计”，*IEEE*车辆技术汇刊，第58卷，第1期，2009年1月。[96] Nelder, J. and R. Mead，“用于函数最小化的单纯形法”，*TheComputerJournal*，第7卷，第4期，第308–313页，1965年。[97] Lagarias, J., J. Reeds, M. Wright, and P. Wright，“低维空间中Nelder–Mead单纯形法的收敛性质”，*SIAM J. on Optimization*，第9卷，第1期，2006年1月。[98] Rugini, L., P. Banelli, and G. Leus，“OFDM时变信道的简单均衡”，*IEEE Comms Letters*，第9卷，第7期，第619–621页，2005年7月。[99] Goodfellow, I., Y. Bengio and A. Courville，深度学习。MIT出版社，2016年，http://www.deeplearningbook.org。[100] Patterson, J. 和 A. Gibson，深度学习：实践者指南。O’Reilly Media，2017年。[101] Masci, J.、U. Meier、D. Cires¸an 和 J. Schmidhuber，“用于层次特征提取的堆叠卷积自编码器”，载于人工神经网络与机器学习——*ICANN 2011*，T. Honkela、W. Duch、M. Girolami 和 S. Kaski 编。柏林，海德堡：Springer Berlin Heidelberg，2011年，第52–59页。[102] Seyfio˘glu, M.、A. ¨Ozbayo˘glu 和 S. G¨urb¨uz，“基于雷达的相似辅助与非辅助人类活动分类的深度卷积自编码器”，*IEEE* 航空航天与电子系统汇刊，第54卷，第4期，第1709–1723页，2018年8月。[103] Creswell, A.、T. White、V. Dumoulin、K. Arulkumaran、B. Sengupta 和 A. A. Bharath，“生成对抗网络：综述”，*IEEE* 信号处理杂志，第35卷，第1期，第53–65页，2018年。[104] Goodfellow, Ian、Pouget-Abadie, Jean、Mirza, Mehdi、Xu, Bing、Warde-Farley, David、Ozair, Sherjil、Courville, Aaron 和 Bengio, Yoshua，“生成对抗网络”，载于神经信息处理系统进展，第27卷。Curran Associates, Inc.，2014年。[105] Mirza, M. 和 S. Osindero，“条件生成对抗网络”，*arXiv*，2014年。 [在线]。获取地址：https://www.inguardians.com/works/[106] Bogale Gereme, Fantahun 和 Zhu, William，“ 利用深度学习打击虚假新闻：预训练词嵌入与嵌入层研究 ”，载于*2020*年第三届国际计算智能与智能系统会议，丛书：CIIS 2020。美国纽约：计算机协会，2020年，第 24 29 [ ] 10 1145 3440840 3440847 –页。[107] 在线。获取地址：https://doi.org/。/。Kignma, D. 和 J. Ba，“Adam：一种随机优化方法”，*arXiv*，2015年。 [在线]。获取地址：https://arxiv.org/pdf/1412.6980.pdf[108] Huang, Gao、Liu, Zhuang、van der Maaten, Laurens 和 Weinberger, Kilian Q.，“密集连接卷积网络”，载于*IEEE* 计算机视觉与模式识别会议论文集（*CVPR*），2017年7月。[109] Polat, G¨orkem、ergenc¸, Ilkay、Kani, Haluk、Alahdab, Yesim、Atug, Ozlen 和 Temizel, Alptekin，“用于溃疡性结肠炎严重程度估计的类别距离加权交叉熵损失”，*arXiv*预印本 *arXiv:2202.05167*，2022年。[110] Guocong, Song 和 Wei Chai，“深度神经网络的协同学习”，2018年。[111] R. S. Sutton 和 A. G. Barto，强化学习：导论。MIT出版社，2018年。