导读：在数字化浪潮席卷全球的今天，工业互联网作为新一代信息技术与制造业深度融合的产物，正深刻改变着传统工业的生产方式和产业格局。随着工业互联网、5G、人工智能等技术的深度融合，工控系统正面临日益复杂的网络安全威胁，如何构建自主安全、智能弹性、全生命周期覆盖的工业安全体系，已成为学术界与工业界亟待攻克的重大课题。为促进我国工业互联网领域的科技创新和学术交流，《网络安全与数据治理》在2025年第9期推出“工业互联网安全”主题专栏，以期为工业互联网安全领域的研究与发展提供有益借鉴。

专栏主编：

洪晟，北京航空航天大学副教授，博士生导师，北京市安全学科带头人，北京市科委技术专家，北京航空航天大学“青年拔尖人才”。主持和参与973/863课题、国家重点研发课题、技术基础课题、国家自然科学基金等课题30余项；担任国内外多个期刊和会议的编委，发表论文70余篇，其中SCI检索30余篇，全球前1% ESI高被引论文1篇；授权国家发明专利20项，获国防科技进步一等奖1项，北京市科学技术进步二等奖1项。

一种融合多维信息的电力物联网设备指纹识别技术*

卢列文[1]，刘佳烨[2]，杨盛明[1]

（1. 工业和信息化部电子第五研究所，广东 广州 511300；2. 中国人民解放军93131部队，北京 100068）

摘 要：针对电力物联网无算力设备面临的恶意篡改、非法接入等安全问题，以及现有设备指纹技术在复杂环境下适应性不足，提出一种融合多维信息的设备指纹识别技术，提升设备识别安全性与准确性。方法上，融合硬件标识、通信协议特征及运行状态数据，通过自适应哈希编码、注意力增强编码、窗口算法等构建动态指纹模型，并与主流算法对比验证。研究结果表明，该技术在正常及异常网络环境和电力运行状态下，准确率、召回率和*F*1值均较高，适配无算力设备，且能适应一定程度的环境变化。该技术为电力物联网无算力设备的精准识别和安全管理提供了有效方案，未来可结合新技术进一步优化，以适应更多新场景。

关键词：电力物联网；无算力设备；设备指纹；识别技术；建模；实验仿真

中图分类号：TP309.2　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.09.001

引用格式：卢列文，刘佳烨，杨盛明. 一种融合多维信息的电力物联网设备指纹识别技术［J］. 网络安全与数据治理，2025，44(9)：1-7.

A fingerprint recognition technology for power IoT devices integrating multidimensional information

Lu Liewen[1], Liu Jiaye[2], Yang Shengming[1]

(1. China Electronic Product Reliability and Environmental Testing Research Institute, Guangzhou 511300, China;
2. 93131 Troops of the Chinese People's Liberation Army, Beijing 100068, China)

Abstract: To address security issues such as malicious tampering and illegal access faced by computing-power-free devices in the power Internet of Things (IoT), and existing device fingerprint technology lacks adaptability in complex environments, this paper proposes a device fingerprint recognition technology that integrates multi-dimensional information to enhance the security and accuracy of device recognition. Methodologically, it combines hardware identifiers, communication protocol characteristics, and operational status data to construct a dynamic fingerprint model through adaptive hashing, attention-enhanced encoding, window algorithms, and other techniques, and verifies its performance through comparison with mainstream algorithms. The research results show that this technology achieves high accuracy, recall rate, and *F*1 score in both normal and abnormal network environments and

power operation states. It is suitable for computing-power-free devices and can adapt to a certain degree of environmental changes. This technology provides an effective solution for accurate identification and security management of computing-power-free devices in the power IoT. In the future, it can be further optimized by combining new technologies to adapt to more new scenarios.

Key words: power Internet of Things; computing-power-free device; device fingerprint; identification technology; modeling; experimental simulation

0 引言

电力物联网作为智能电网发展的关键支撑，正逐渐改变着传统电力系统的运营模式[1]。在电力物联网架构中，无算力设备（通常是指不具备或仅具有极弱数据处理、计算能力的设备），如电表、数据终端单元（Data Terminal Unit，DTU）、馈线终端单元（Feeder Terminal Unit，FTU）、配电变压器监测终端（Transformer Terminal Unit，TTU）等，这类设备数量庞大且分布广泛，它们负责采集、传输电力数据，是电力物联网实现智能化的基础。然而，随着电力物联网的规模不断扩大，这些设备面临着严峻的安全挑战，如设备被恶意篡改、非法接入等问题，严重威胁电力系统的安全稳定运行。

设备指纹识别技术作为一种有效的设备管理和安全防护手段，能够为每台设备生成独一无二的身份信息，实现对设备的精准识别和追踪。通过准确识别无算力设备指纹，对于及时发现非法设备接入，提高设备管理的精细化程度，构建电力物联网安全防御体系具有重要意义。

1 研究现状

1.1 国外研究现状

国外在设备指纹识别技术上起步早，早期研究聚焦硬件物理特征识别，如文献［2］基于射频指纹分析设备射频信号细微特征实现识别，但该技术受硬件和环境影响大；文献［3－4］基于网络流量特征研究，借助机器学习，利用深度学习算法自动提取数据包长度分布等特征构建设备指纹，部分结合主动探测增强准确性，但存在干扰和隐私风险。近年研究注重多维信息融合，整合硬件、网络流量、软件行为等特征，如文献［5］采用集成学习和深度学习端到端模型提升识别准确率，在电力物联网场景中，研究轻量级模型、抗干扰算法及基于密码学的安全技术以满足实时性、抗干扰和安全性需求。

1.2 国内研究现状

国内物联网设备指纹识别技术起步晚，但发展快，早期借鉴国外硬件指纹技术，后结合国内电力网络特点进行创新。文献［6－7］在网络流量分析上，针对电力专用协议设计特征提取模块，运用深度学习处理时空特征提升识别率。文献［8－10］提出多维信息融合算法，包括融合电力参数、环境感知信息及时序动态特征，具有创新性。文献［11］采用动态指纹模型适应设备状态变化。同时，研究注重与电力物联网安全体系整合，用于接入控制、异常检测，推动国产化技术替代，如国产密码算法的指纹加密技术。

1.3 国内外技术总结分析

通过研究国内外研究现状，现有设备指纹识别技术普遍存在三大不足：（1）多维特征融合停留在浅层拼接，未构建动态关联模型；（2）对电力设备运行中的参数漂移（如老化、负荷变化）缺乏自适应更新机制；（3）复杂模型难以部署于无算力传感器等边缘设备。而电力无算力设备（如智能电表、传感器）占比超 70%，其低功耗、无 CPU 的特性导致传统指纹技术难以适用，亟需轻量级、抗噪的指纹生成算法。这类设备作为电力物联网末梢节点，其身份识别是保障电网安全的基础，若缺乏有效指纹技术，易成为恶意入侵的突破口，因此研究适配电力物联网无算力设备的指纹识别技术，对构建安全可信的电力物联网具有重要意义。

2 设备指纹识别技术研究

2.1 设备指纹信息维度确定

（1）硬件标识信息

电力物联网无算力设备的硬件标识是设备的重要身份特征[12－13]。以电表为例，其表号通常由生产厂家在制造过程中根据特定编码规则赋予，具有唯一性；DTU、FTU、TTU 等设备的序列号同样如此。这些硬件标识犹如设备的“身份证”，是构建设备指纹的基础元素。

本文电力物联网无算力设备的硬件物理特征为硬件标识信息，如图 1 所示。

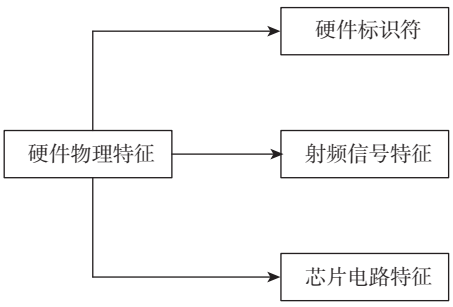


图 1 硬件物理特征信息

* 基金项目：广州市重点研发计划项目（2023B01J0002）

（2）通信协议特征

电力物联网中广泛使用多种通信协议，如 Modbus、IEC-61850（MMS、GOOSE、SV）、IEC-60870（IEC-101、102、103、104）、DLT645-2007 等[14]。这些协议在数据帧格式、功能码使用以及通信频率等方面具有独特规范。以 Modbus 协议为例，其数据帧包含设备地址、功能码、数据内容及 CRC 校验码等字段。不同设备在使用 Modbus 协议进行通信时，其功能码的使用模式、数据长度变化规律以及 CRC 校验码的生成方式等都存在差异。通过长期监测设备通信过程中的这些协议特征，能够提取出具有设备特异性的通信协议指纹。

本研究以网络流量特征为通信协议标识信息，如图 2 所示。

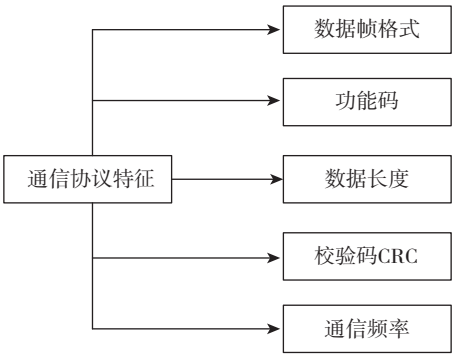


图 2　网络流量特征

（3）运行状态数据

运行状态数据反映无算力设备在实际运行中的工作状况[15-16]。对于电表，其电量数据的变化趋势、尖峰平谷时段的用电量分布等都是重要的运行特征。对于 DTU、FTU 和 TTU 等设备，电压、电流、功率因数、变压器油温等数据的实时值和变化规律，包含着设备的运行状态信息。通过对这些运行状态数据进行长时间的采集和分析，发现设备特有的运行模式和数据变化规律。

本研究以电力运行参数为电力物联网无算力设备的运行状态标识信息，如图 3 所示。

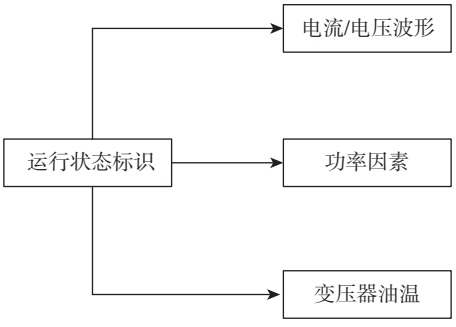


图 3　电力运行参数

2.2　设备指纹建模

设备指纹建模的核心是将多维度原始信息转化为具有唯一性、稳定性和抗干扰性的指纹向量。本文采用自适应编码机制和动态特征融合的方式实现建模，具体过程如下。

2.2.1　硬件标识自适应哈希编码

硬件标识（如序列号、设备 ID）是设备身份的基础，但长期运行中可能因硬件老化（如芯片温度漂移）导致物理特征细微变化，传统固定哈希编码（如 SHA－256）无法捕捉此类变化，易产生指纹偏差。为此设计基线哈希修正的双阶段哈希编码，对电力物联网无算力设备进行硬件标识。

（1）基线哈希生成

以设备出厂硬件标识为基准，将其记为 ID_{base}，采用 SHA-256 生成初始哈希值，作为身份基准：

$$\boldsymbol{H}_{base}=\text{SHA-256}(ID_{base}) \tag{1}$$

其中，$\boldsymbol{H}_{base}$ 为 256 位二进制向量，确保硬件标识的原始唯一性。

（2）动态修正因子计算

实时采集硬件运行辅助特征（如芯片工作温度 T、供电电压 V），通过轻量化函数生成修正因子 δ，量化硬件当前状态与出厂状态的偏差：

$$\delta=\frac{1}{2}\left(\frac{T-T_{base}}{T_{max}-T_{base}}+\frac{V-V_{base}}{V_{max}-V_{base}}\right) \tag{2}$$

其中，T_{base}、V_{base} 为设备正常工作时温度和电压的基准值，T_{max}、V_{max} 为设备允许的最大偏差阈值。δ 取值范围为 $[0,1]$，$\delta=0$ 表示无偏差，δ 越大表示硬件状态偏离出厂状态越明显。

（3）自适应哈希编码生成

将基线哈希与修正因子融合，生成最终硬件标识编码：

$$\boldsymbol{H}_{hardware}=\boldsymbol{H}_{base}\oplus\text{Binary}(\delta\cdot 2^{256}) \tag{3}$$

其中，$\oplus$ 为异或运算，Binary（·）将 δ 映射为 256 位二进制向量（值越大，修正位越多）。该编码既保留 $\boldsymbol{H}_{base}$ 的基础唯一性，又通过 δ 动态适配硬件状态变化。

2.2.2　通信协议特征注意力增强编码

通信协议特征（如 Modbus 功能码、IEC-61850 数据帧结构）是设备身份的动态标识，但不同特征对设备识别存在差异性，如 Modbus 功能码 0x03（读数据）的调用频率具有设备特异性，而 CRC 校验码受噪声影响更大。传统独热编码对所有特征赋予均匀权重，易放大噪声特征的干扰。为此设计特征重要性加权独热编码。

（1）关键特征提取

以 Modbus 协议为例，从通信数据帧中提取 3 类核心

特征：功能码 f（取值范围 0x01 ~ 0x10）、数据长度 L（取值范围 1 ~ 255 字节）、CRC 校验码 C（16 位二进制），构成特征集 $F = \{f, L, C\}$。

（2）特征重要性评分

通过信息增益量化特征对设备身份的区分能力。设设备集合为 $D = \{d_1, d_2, \cdots, d_N\}$，特征 x 的信息增益 IG（x）定义为：

$$\mathrm{IG}(x) = H(D) - H(D \mid x) \tag{4}$$

其中，$H(D)$ 为设备集合的信息熵，$H(D \mid x)$ 为已知特征 x 时的条件熵。IG(x) 越大，说明特征 x 对设备身份的区分能力越强。

（3）注意力加权独热编码

对特征集 F 进行独热编码后，按信息增益分配权重：

①独热编码：对 f、L、C 分别生成独热向量 $\boldsymbol{O}_f$（长度 16）、$\boldsymbol{O}_L$（长度 255）、$\boldsymbol{O}_C$（长度 65 536）；

②权重分配：计算 IG(f)、IG(L)、IG(C)，归一化后得到权重

$$w_f = \frac{\mathrm{IG}(f)}{\mathrm{IG}(f) + \mathrm{IG}(L) + \mathrm{IG}(C)} \tag{5}$$

w_L、w_C 计算同理。

③加权编码：通信协议特征编码为：

$$\boldsymbol{H}_{\text{protocol}} = w_f \cdot \boldsymbol{O}_f + w_L \cdot \boldsymbol{O}_L + w_C \cdot \boldsymbol{O}_C \tag{6}$$

该编码通过注意力机制放大高区分度特征的影响，抑制低区分度特征的干扰，解决了传统独热编码特征权重均等化的缺陷。

2.2.3 运行状态数据动态窗口特征提取

运行状态数据（如电压、油温）具有强时序性和周期性，传统固定窗口算法无法适配不同设备的周期差异，易丢失关键特征，为此设计周期感知动态窗口算法。

（1）周期特征识别

对运行状态时序数据 $S = \{s_1, s_2, \cdots, s_T\}$（$T$ 为采样点数）进行频谱分析，通过快速傅里叶变换（FFT）提取主周期 T_p：

$$\mathrm{FFT}(S) = \sum_{t=1}^{T} s_t \cdot \mathrm{e}^{-\mathrm{j}2\pi ft} \tag{7}$$

其中，f 为频率，取 FFT（S）中幅值最大的频率 f_p，对应主周期 $T_p = 1/f_p$。

（2）动态窗口划分

根据主周期 T_p 自适应设置窗口大小 W 和滑动步长 Step：

$$W = T_p / k \tag{8}$$

$$\mathrm{Step} = W/2 \tag{9}$$

其中，k 为周期内窗口数量。

（3）特征向量提取

在每个窗口内计算 3 类鲁棒特征：

①稳健均值（抑制瞬时脉冲干扰）：

$$\mu = \frac{1}{W-2} \sum_{i=2}^{W-1} s_i \tag{10}$$

②变异系数（归一化离散度）：

$$\mathrm{CV} = \frac{\sigma}{\mu} \quad (\mu \neq 0) \tag{11}$$

其中，σ 为窗口内数据标准差，消除量纲影响。

③趋势斜率（反映状态变化方向）：

$$k = \frac{W\sum_{i=1}^{W} i \cdot s_i - \sum_{i=1}^{W} i \sum_{i=1}^{W} s_i}{W\sum_{i=1}^{W} i^2 - \left(\sum_{i=1}^{W} i\right)^2} \tag{12}$$

（4）特征量化

将上述特征 $\{\mu, \mathrm{CV}, k\}$ 映射到 [0, 1] 区间（消除设备间参数差异）：

$$\mu' = \frac{\mu - \mu_{\min}}{\mu_{\max} - \mu_{\min}} \tag{13}$$

其中，$\mu_{\min}$、$\mu_{\max}$ 为历史数据中 μ 的最小值、最大值。CV、k 量化方式同理，最终形成运行状态特征向量 $\boldsymbol{H}_{\text{status}}$。

2.2.4 动态权重特征融合

传统融合方法采用固定权重拼接，未考虑各维度特征在实时环境中的可靠性，为此设计实时可靠性驱动的动态融合。

（1）特征可靠性评估

为每个维度特征定义可靠性系数：

①硬件特征可靠性 r_h：基于硬件温度偏差 $\Delta T = |T - T_{\text{base}}|$，$r_h = 1 - \min(\Delta T/T_{\max}, 1)$（$T_{\max}$ 为允许最大温差）；

②通信特征可靠性 r_p：基于通信丢包率 P_{loss}，$r_p = 1 - P_{\text{loss}}$；

③运行特征可靠性 r_s：基于数据波动幅度 $\Delta S = |\sigma - \sigma_{\text{base}}|$，$r_s = 1 - \min(\Delta S/\sigma_{\max}, 1)$（$\sigma_{\text{base}}$ 为正常波动标准差）。

（2）动态权重计算

将可靠性系数归一化后作为融合权重：

$$\begin{cases} w_h = \dfrac{r_h}{r_h + r_p + r_s} \\ w_p = \dfrac{r_p}{r_h + r_p + r_s} \\ w_s = \dfrac{r_s}{r_h + r_p + r_s} \end{cases} \tag{14}$$

（3）生成最终指纹

通过加权拼接融合三维特征，得到设备指纹 $\boldsymbol{F}$：

$$\boldsymbol{F} = w_h \cdot \boldsymbol{H}_{\text{hardware}} \oplus w_p \cdot \boldsymbol{H}_{\text{protocol}} \oplus w_s \cdot \boldsymbol{H}_{\text{status}} \tag{15}$$

其中⊕为向量拼接运算；权重 w_h，w_p，w_s 随实时可靠性动态调整，如网络丢包率升高时，r_p 下降，w_p 减小，降

低通信特征的干扰。

3 实验仿真验证

3.1 实验环境搭建

搭建包含 20 台电力物联网无算力设备的实验平台，该实验平台还配置数据采集服务器（支持 1 Hz 通信数据、10 Hz 运行数据同步采集）、环境模拟器（可模拟0 ~ 100 ms 延迟、0 ~ 10% 丢包及设备过载等状态）。硬件采用工业级交换机搭建局域网，软件部署数据预处理模块（异常值清洗、标准化）及算法测试框架，确保数据采集、场景模拟及算法对比的稳定性。

设备类型及参数如表 1 所示，覆盖电力系统常见物联网感知设备。

3.1.1 硬件与网络环境

网络环境通过工业以太网与无线通信（LoRa）搭建，配备网络模拟器（支持延迟、丢包模拟）和电力系统仿真软件（支持正常、过载、短路状态模拟），模拟实际电力物联网的复杂场景。

3.1.2 对比算法设置

选取电力物联网设备识别领域 4 类主流算法作为对照组，确保对比公平性，如表 2 所示。

3.2 实验数据采集

3.2.1 数据来源与类型

通过以下方式采集实验数据，覆盖 20 台设备连续 30 天的运行记录（本实验数据是基于我司智能制造装备安全研究课题项目，未公开）。

硬件标识数据：设备出厂序列号、芯片 ID（每日采集 1 次，共 600 条）；

通信协议数据：Modbus/IEC 帧结构（功能码、数据长度等，采集频率 1 Hz，共约 5.2×10^6 条）；

运行状态数据：电压、电流、油温等（采集频率 10 Hz，共约 5.2×10^7 条）；

环境干扰数据：网络延迟（0 ~ 100 ms）、丢包率（0 ~ 10%）、电力状态（正常/过载/短路）的模拟记录。

3.2.2 数据预处理

清洗：剔除异常值（如电压 > 380 V ± 20%）、重复数据（通信帧重传记录）；

标准化：将运行状态数据归一化至［0，1］，通信协议特征编码为数值型（如功能码映射为 0 ~ 15）；

时序格式化：为 LSTM 生成时序样本（24 个时间步/样本），为 CNN 生成通信帧特征矩阵（10 × 10 维度）。

3.3 实验步骤

（1）指纹库构建

对 20 台设备的前 20 天数据，按各算法要求生成基准指纹：

①本文算法：生成动态指纹向量（硬件 + 通信 + 运行特征融合）；

②RF/CNN/LSTM：训练分类模型（输入特征，输出设备 ID）；

表 1 物联网无算力设备清单

设备类型	厂家	型号	数量/台	硬件标识	通信协议	运行状态监测参数
智能电表	威胜集团	DTSD341 9Q	5	VS202405010001-005	DLT645-2007	电压、电流、用电量
数据终端单元（DTU）	厦门四信	F2C16	4	SX-F2C16-0013-0016	Modbus	通信信号强度、数据传输时延
馈线终端单元（FTU）	许继电气	WJ-801F	5	XJFTU202403150001-005	IEC-60870	线路电流、故障信号
变压器监测终端（TTU）	南瑞	NRD-800T	6	NR-TTU202402100001-006	IEC-61850	变压器油温、负荷率

表 2 对比算法设置清单

算法类型	核心原理	适配场景	参数设置
本文算法	动态特征融合 + 自适应相似度度量	多维特征动态变化场景	动态窗口 $k=6$，权重更新周期 5 min，相似度阈值 0.85
随机森林（RF）	集成决策树提取特征重要性	多维静态特征分类	决策树数量 50，最大深度 10，节点分裂标准 Gini
卷积神经网络（CNN）	卷积层提取局部特征 + 全连接分类	通信协议帧结构等局部特征场景	2 层卷积（3 × 3 核），1 层全连接（128 神经元），ReLU 激活
长短期记忆网络（LSTM）	时序依赖建模 + 门控机制抑制噪声	运行状态周期性时序特征场景	2 层隐藏层（64 神经元/层），时间步长 24，Dropout = 0.2
传统指纹算法（Baseline）	固定编码 + 固定权重 + 余弦相似度	简单静态环境	固定窗口 5 min，权重（硬件 0.4，通信 0.3，运行 0.3）

③Baseline：生成固定指纹向量（固定编码 + 固定权重）。

（2）识别测试

用后 10 天数据模拟未知设备接入、测试。

输入：测试设备的实时硬件、通信、运行数据。

处理：各算法生成实时指纹或分类结果。

比对：本文算法、Baseline 计算与指纹库的相似度；RF、CNN、LSTM 直接输出分类标签。

判断：相似度 ≥ 0.85（本文算法/Baseline）或分类置信度 ≥ 0.8（RF/CNN/LSTM）为识别成功。

（3）性能评估

计算各算法在不同场景下的核心指标：

①准确率（Accuracy）：正确识别样本/总样本；

②召回率（Recall）：正确识别的目标设备样本/实际目标设备样本；

③*F*1 值：准确率与召回率的调和平均（平衡两者）；

④耗时：单设备单次识别的平均计算时间（ms）。

3.4 实验结果与分析

3.4.1 不同场景下的性能对比

不同场景下，各算法的横向对比实验结果如表 3 所示。

表 3 横向对比算法实验结果

网络环境	电力运行状态	评估指标	本文算法	RF	CNN	LSTM	Baseline
正常网络	正常用电	准确率	0.99	0.97	0.96	0.95	0.99
		召回率	0.98	0.96	0.95	0.94	0.98
		*F*1 值	0.98	0.96	0.95	0.94	0.98
		耗时/ms	8.2	12.5	29.3	36.1	7.8
	过载	准确率	0.96	0.92	0.9	0.91	0.95
		召回率	0.95	0.9	0.88	0.89	0.93
		*F*1 值	0.95	0.91	0.89	0.9	0.94
		耗时/ms	8.5	12.8	29.7	36.5	8
网络丢包 10%	正常用电	准确率	0.9	0.82	0.78	0.8	0.85
		召回率	0.89	0.8	0.76	0.78	0.83
		*F*1 值	0.89	0.81	0.77	0.79	0.84
		耗时/ms	9.1	13.2	30.2	37.3	8.2
网络延迟 100 ms	正常用电	准确率	0.88	0.8	0.76	0.79	0.83
		召回率	0.86	0.78	0.74	0.77	0.81
		*F*1 值	0.87	0.79	0.75	0.78	0.82
		耗时/ms	8.9	13	29.9	37	8.1

3.4.2 结果分析

（1）性能优势

正常场景下，所有算法均保持高准确率（≥0.95），但本文算法在动态适应性方面优势明显（如正常用电时 *F*1 值与 Baseline 持平，略高于 RF/CNN/LSTM）。

异常场景（过载、10% 丢包、100 ms 延迟）下，本文算法的 *F*1 值显著领先：

①对比 RF：高 4% ~8%（因 RF 依赖静态特征重要性，无法适配过载时硬件特征漂移）；

②对比 CNN/LSTM：高 10% ~12%（因 CNN 对通信延迟导致的帧结构变形敏感，LSTM 对丢包导致的时序断裂鲁棒性不足）；

③对比 Baseline：高 5%（因 Baseline 固定权重无法降低不可靠特征的干扰，如丢包时通信特征权重仍占 0.3）。

（2）效率优势

本文算法单设备识别耗时（8.2 ~9.1 ms）仅略高于 Baseline（7.8 ~8.2 ms），但远低于 RF（12.5 ~13.2 ms）、CNN（29.3 ~30.2 ms）、LSTM（36.1 ~37.3 ms）。动态特征融合基于轻量化公式，无需神经网络的反向传播计算；自适应权重调整避免了 RF 的决策树集成计算开销，更适配无算力设备的低功耗需求。

（3）局限性与优化方向

本文算法在硬件老化 + 10% 丢包复合异常下 *F*1 值降至 0.85，主要因硬件、通信特征同时失真。后续可增加特征可靠性分级机制：当某维度可靠性 < 0.5 时，自动剔除该维度特征，仅保留高可靠性特征参与融合。

3.5 实验结论

实验表明，本文所提设备指纹识别技术在正常与异常场景下均保持高识别性能，且计算效率适配无算力设备需求。与主流算法对比，其核心优势在于动态特征适配与轻量化设计的结合。本文研究验证了多维信息融合框架下自适应建模的有效性，为电力物联网无算力设备识别提供了兼具准确性和工程实用性的方案。

4 结论

本文针对电力物联网无算力设备的特点，提出一种基于多维度信息融合的设备指纹识别技术。通过确定硬件标识、通信协议特征和运行状态数据等信息维度，建立设备指纹模型，经过多轮实验仿真验证，该技术在不同网络环境和设备运行状态下，都能取得较好的识别效果，为电力物联网无算力设备的精准识别和安全管理提供有效的解决方案。

未来研究可结合联邦学习实现分布式指纹更新，适配无算力设备迭代；引入图神经网络建模设备关联特征，提升大规模网络识别效率；探索量子加密增强指纹抗篡改性。

参考文献

[1] Omdia. 2024 物联网趋势预测报告 [EB/OL]. (2024 - 02 - xx) [2025 - 06 - 01]. https://iot.telenor.com/wp-content/uploads/2024/02/Telenor-IoT-Prediction-Report-2024_ CHS.pdf.

[2] GEYER R C, KLEIN T, NABI M. Differentially private federated learning: a client level perspective [J]. arXiv: 1712.07557, 2017.

[3] YANG Q, LIU Y, CHEN T. Federated machine learning: concept and applications [J]. ACM Transactions on Intelligent Systems and Technology, 2019, 10 (2): 1 - 19.

[4] FAN L N, LI C L, WU Y C, et al. Survey on IoT device identification and anomaly detection [J]. Ruan Jian Xue Bao/Journal of Software (in Chinese), 2024, 35 (1): 288 - 308.

[5] JMILA H, BLANC G, SHAHID M, et al. A survey of smart home IoT device classification using machine learning-based network traffic analysis [J]. IEEE Access, 2020 (10): 97117 - 97141.

[6] 卢徐霖. 面向网络流量的物联网设备识别关键技术研究 [D]. 无锡：江南大学，2024.

[7] 祝博宇，陈霄，沙乐天，等. 基于流量和文本指纹的两层物联网设备分类识别模型 [J]. 计算机科学，2023，50 (8)：304 - 313.

[8] 石佳琪，王瑞敏，张媛媛，等. 基于多重检验特征选择的物联网设备识别 [J]. 信息工程大学学报，2023，24 (5)：579 - 585.

[9] 彭敢. 基于设备指纹的物联网安全接入技术研究 [D]. 镇江：江苏科技大学，2024.

[10] 黄强. 基于设备指纹和行为可信的物联网访问控制系统 [D]. 南京：东南大学，2019.

[11] 王萌，丁志军. 一种新的设备指纹特征选择及模型构建方法 [J]. 计算机科学，2020，47 (7)：257 - 262.

[12] 宋宇波，祁欣妤，黄强，等. 基于二阶段多分类的物联网设备识别算法 [J]. 清华大学学报 (自然科学版)，2020，60 (5)：365 - 370.

[13] 张彦杰，庞振江，王晖南，等. 基于特征标识及密码技术的设备指纹提取方法 [J]. 太原理工大学学报，2022，53 (4)：707 - 712.

[14] 卢文迪，李晓辉，汪涵. 基于设备指纹的物联网设备安全接入方法研究与实现 [J]. 电子设计工程，2019，27 (3)：136 - 141.

[15] 刘芹，史桢港，崔竞松. 基于行为指纹的网络设备识别方法 [J]. 武汉科技大学学报，2023，46 (1)：64 - 74.

[16] 杨威超，郭渊博，李涛，等. 基于流量指纹的物联网设备识别方法和物联网安全模型 [J]. 计算机科学，2020，47 (7)：299 - 306.

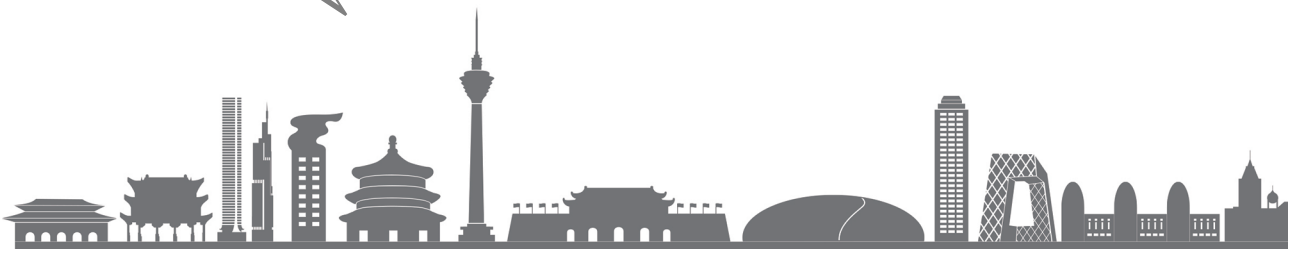
(收稿日期：2025 - 07 - 06)

作者简介：

卢列文 (1975 -)，男，硕士，高级工程师，主要研究方向：信息系统网络安全、工业控制系统安全、无人机安全、网络空间对抗。

刘佳烨 (1997 -)，男，本科，助理工程师，主要研究方向：装备试验鉴定、网络空间对抗。

杨盛明 (1985 -)，男，硕士，高级工程师，主要研究方向：信息系统网络安全、工业控制系统安全、无人机安全、网络空间对抗。



版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部