基于双模态融合的 ZigBee 设备识别方法

李　荣，赖怡聪，李乐言
（中国电子产品可靠性与环境试验研究所，广东　广州　510610）

摘　要：智能家居为人们日常生活带来便利的同时，也带来了隐私安全风险，智能传感器能够不断收集周围环境的信息，并通过无线通信远程传输数据。为了保护用户的隐私安全，提出了一种基于双模态融合的 ZigBee 设备识别方法。首先，通过空中接口被动捕获智能家居设备 ZigBee 流量数据；然后，对设备流量进行分片处理，在文本模态下提取加密流量的时序、长度等特征信息，在图像模态下提取流量图像的高维特征；最后，融合加密流量的文本特征和图像特征，构建基于双模态融合的设备类型识别模型。通过对 5 个厂家 15 个设备的实验结果表明，即使设备的无线流量被加密保护，该方法在 ZigBee 设备识别准确率上达到 99% 左右，能够有效地识别用户身边的智能传感器，保护用户的隐私安全。

关键词：隐私安全；ZigBee；深度学习；智能家居
中图分类号：TN918；TP309　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.02.003
引用格式：李荣，赖怡聪，李乐言. 基于双模态融合的 ZigBee 设备识别方法[J]. 网络安全与数据治理，2025，44(2)：17-25.

A dual-modal fusion approach for ZigBee device identification

Li Rong, Lai Yicong, Li Leyan
(China Electronic Product Reliability and Environmental Testing Research Institute, Guangzhou 510610, China)

Abstract: Smart homes bring convenience to daily life but also introduce privacy and security risks. Smart sensors continuously collect information about their surroundings and transmit data remotely via wireless communication. To protect user privacy, this paper proposes a ZigBee device identification method based on dual-mode fusion. Firstly, ZigBee traffic data from smart home devices is passively captured through the air interface. Then, the device traffic is fragmented: in the text modality, features such as timing and length of encrypted traffic are extracted, while in the image modality, high-dimensional features of traffic images are obtained. Finally, the textual and image features of the encrypted traffic are fused to construct a device type recognition model based on bimodal fusion. Experimental results involving 15 devices from 5 manufacturers show that, even with encrypted wireless traffic, this method achieves an identification accuracy of approximately 99% for ZigBee devices, which can effectively identify nearby smart sensors and protect user privacy.

Key words: privacy security; ZigBee; deep learning; smart home

0　引言

据亿欧发布的 2024 智能家居研究报告显示[1]，2023 年中国智能家居市场规模达到 7 558.1 亿元，预计 2025 年市场规模达到 10 170.2 亿元，物联网、云计算、人工智能等技术的融入，推动智能家居产业繁荣发展。为了实现智能家居自动化，许多智能设备都配备了嵌入式传感器，能够持续地收集周围的环境数据，并根据用户设置执行相应的策略，实现设备之间的智能联动。同时，智能家居设备可以通过无线网络与云端服务器通信，用户通过 APP 可远程查看设备的状态信息。常见的短距离无线通信协议有 Wi-Fi、BLE 和 ZigBee 协议。ZigBee 协议作为低成本、低功耗的无线通信协议，被广泛地应用于小型智能传感器中。

大量智能传感器设备的使用，在方便人们生活的同时，也带来信息安全风险。智能传感器设备持续收集、传输、处理环境中的用户行为信息。一旦入侵者在房间附近部署小型传感器，即可远程收集用户的个人隐私数据。例如，入侵者可以在用户周围部署门磁传感器，通

过其状态的变化来分析用户的出行规律，或者在房间附近部署人体传感器，通过人体传感器的状态分析来推断家中是否有人，严重侵犯了用户的个人隐私安全。

为保护用户隐私安全，可以通过分析设备的无线流量识别周围存在的智能传感器，消除潜在的安全威胁。现有研究大多基于从家用无线路由器获取设备流量，在互联网上捕获设备间或者设备与云服务间的 IP 流量来识别智能家居内的设备信息，对用户而言这种场景有一定局限性，用户可能无法接入攻击者所部署的无线网络中。同时，智能网关在接收智能设备流量后会进一步处理流量数据，在无线路由器中收集到的设备流量数据可能会丢失一些重要的设备数据特征。此外，现有的 ZigBee 设备识别研究依赖设备流量的应用层和链路层特征，由于不同厂商在同类产品上的运行逻辑类似，在多设备分类场景下的性能不足。

为此，本文提出了一种基于双模态融合的 ZigBee 设备识别方法。首先，设计了一种新的智能家居隐私安全防护场景，针对 ZigBee 协议的智能传感器，通过无线嗅探收集环境周围的 ZigBee 流量数据。然后，通过分析智能设备独特的运行模式，从完整 ZigBee 网络流量中提取单个设备的流量，并利用数据的时序关系对流量进行切分。最后，分别在文本模态和图像模态下提取流量的多维特征，融合双模态构建 ZigBee 设备识别模型。实验表明，即使 ZigBee 流量进行了加密，识别模型也能有效地区分出多个厂家的不同智能家居设备，设备识别的准确率达到 99% 左右。

1　相关工作

近年来，随着物联网技术的不断发展，越来越多的研究人员关注物联网设备的隐私与安全[2]。Ramon Saura 等人[3]利用数据挖掘技术研究智能家居环境中的主要安全问题，指出恶意软件、网络安全攻击、数据存储漏洞是智能家居中个人隐私安全的主要威胁。针对 ZigBee 智能家居，Akestoridis 等人[4]开发了一个安全分析工具 Zigator，通过对 ZigBee 流量分析检查可以识别某些加密的 NWK 命令，并且设计了一些选择性干扰和欺骗攻击，以迫使用户对目标设备进行出厂重置，并最终暴露网络密钥。

为了实现对智能设备的统一安全管理，以及实现对智能设备进行访问控制，降低设备的安全风险，研究人员建立了设备指纹识别模型，以准确识别设备类型。对收集的设备数据类型进行划分，可分为应用数据与射频数据。应用数据为无线设备发送的具体报文数据，可以直观地观察数据流向和内容，Miettinen 等人[5]设计了一个用于设备指纹识别和保护 IoT 网络的 IoT Sentinel 框架，收集设备第一次在网络上注册时的设备指纹，并使用机器学习方法对其进行指纹识别，能够自动识别连接到 IoT 网络的设备，并且能够强制执行规则来限制易受攻击设备的通信，从而最大限度地减少危害。为了进一步描述设备行为并处理加密流量，Bezawada 等人[6]提出了一种可用于设备类型识别的设备指纹识别方法。射频数据为无线设备所发送的射频信号，需要依赖较为复杂的特征提取方法，Xie 等人[7]对射频指纹识别进行了总结，涵盖了从信号预处理、射频指纹特征提取到进一步处理和射频指纹识别各个环节，并研究了相关的最新方法，包括基于传统机器学习、深度学习和生成模型的方法。周樨等人[8]针对直接序列扩频的 ZigBee 信号，设计了一种基于扩频还原的射频指纹提取方法，能够高效地识别 60 台智能设备信息，并基于设备指纹信息可构建入侵防护系统，有效地抵抗外部攻击。为了克服数据样本的不足，Liu 等人[9]提出了一种基于自监督学习和对抗性增强的小样本射频指纹识别方法，能够提取更具辨识度的射频指纹特征，并在小样本射频指纹识别中获得更高的识别性能。

数据收集以途径进行划分，可以分为有线收集与无线收集。有线收集通过物理线路收集无线设备所发送的流量数据，可以获取到更为准确的数据。Mirsky 等人[10]提出了一个即插即用的网络入侵检测系统，该系统使用神经网络在无监督的情况下检测本地网络上的攻击。针对在复杂网络环境中的设备管理，Dong 等人[11]假设网关可能启用标准的阻碍性流量分析配置，并提出了一个基于序列学习技术的流量分析框架，用于设备指纹识别。无线收集通过无线嗅探的方式获取设备的无线网络流量，具有更高的自由度。袁杨鑫[12]设计了一种基于概率投票算法的三重卷积神经网络，在室内近距离、室内远距离、室外近距离、室外远距离和非视距信道环境下，利用设备的射频指纹来进行分类识别。Acar 等人[13]提出了一种在智能环境中的多阶段隐私攻击，通过被动嗅探获取智能家居设备的 Wi-Fi、BLE 和 ZigBee 网络流量，并使用机器学习方法来检测家庭内的用户活动。本文将采用无线收集的方式获取设备的应用数据，具有更高的自由度，无需复杂的设备识别算法即可有效地识别无线设备类型。

2　威胁场景

针对常规的智能家居环境，本文设计了图 1 所示识别场景，展示用户如何在未知环境中识别周围存在的智能传感器。

图 1　设备探测识别场景

在构建的设备识别场景中，假设入侵者可临时拥有房间的使用权，隐藏了多个智能传感器于房间内，如门磁传感器、动静贴、人体传感器等。这些智能传感器能够实时监测房间的环境信息，并使用 ZigBee 协议将数据传输至智能网关中，智能网关通过 Wi-Fi 路由器与厂家云服务器进行数据传输，可通过手机 APP 来远程查看房间的环境信息。入侵者通过查看智能传感器的数据可远程获取房间中的环境信息，窃取用户隐私。

根据 ZigBee 协议定义，其工作在 868 MHz、915 MHz、2.4 GHz 频段中，并将频段分为 27 个信道。用户在进入一个陌生的房间时，需要使用 ZigBee 流量嗅探器循环扫描每个 ZigBee 信道，确认 ZigBee 设备工作的信道，确定周围是否存在 ZigBee 设备流量。在获取到设备通信流量之后，用户可将设备流量输入到提前训练好的智能设备识别模型中，进而推断出周围存在的智能传感器类型，保护个人的隐私安全。

3　方法设计

3.1　方法框架

针对上述威胁场景，本文研究了一种基于双模态融合的 ZigBee 设备识别方法，并建立设备识别模型框架，保护用户的隐私安全。具体模型框架如图 2 所示。

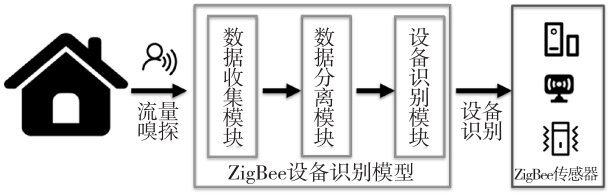

图 2　ZigBee 设备识别模型框架

本文设计的 ZigBee 设备识别模型框架可以分为 3 个模块：数据收集模块、数据分离模块和设备识别模块。其中数据收集模块主要负责收集环境周围存在的 ZigBee 流量，为后续训练设备识别模型提供数据；数据分离模块主要负责对 ZigBee 流量进行预处理，根据协议的特征将单个设备的流量从完整的网络流量中分离，并按时序特征将流量进行分割，构建设备流量矩阵，便于后续流量特征的提取；设备识别模块主要负责提取设备不同模态下的特征，并搭建深度学习模型融合双模态特征，通过多轮训练生成 ZigBee 设备识别模型。

用户在进入陌生环境后，尝试在不同的位置移动，尽可能地触发隐藏在房间中的智能传感器，同时使用 ZigBee 流量嗅探设备收集一段时间内的设备流量，将设备流量输入到 ZigBee 设备识别模型中，能够对环境中存在的智能传感器进行有效识别。

3.2　数据收集模块

为了展示设备识别模型在多个相似设备上的识别性能，本文挑选了一些与用户行为相关的智能家居设备类别，如人体传感器、门磁传感器等，为了应对现实生活中的复杂环境，避免设备识别模型过拟合，同时也挑选了一些不与用户交互的智能传感器，如烟雾报警器等。根据市场销售情况，选取了一些主流的智能家居品牌和功能相似的 ZigBee 智能传感器，总共包含了 5 个厂商的 15 个设备，具体如表 1 所示。

表 1　各厂商 ZigBee 智能传感器

厂商	智能传感器类别			
京东	无线智能插座	人体传感器	无线开关	门磁传感器
小米	烟雾报警器	人体传感器	天然气报警器	
Aqara	门磁传感器	人体传感器	动静贴	
海曼	门磁传感器	人体传感器		
华为	门磁传感器	人体传感器	温湿度传感器	

在捕获设备流量之前，需要对每个 ZigBee 信道进行扫描，确定智能传感器具体的工作信道。本文使用 CC2531 USB 适配器来捕获设备流量，并收集上述 5 个制造商的 15 种不同智能设备的网络流量。为了收集每个智能设备更全面的数据流，展示每个智能设备的独特操作特性，本文将数据收集分为两个部分：第一部分是在真实环境中部署智能设备 1 ~ 2 天，以模拟用户真实生活行为，尽可能收集接近真实环境下的流量数据；第二部分为手动触发智能设备，并重复步骤 20 次以上，以捕获更多设备触发流量数据。

3.3　数据分离模块

在 ZigBee 智能家居网络中，不同制造商的设备可能通过不同的 ZigBee 信道进行通信。一个 ZigBee 信道可能

包含多个由智能网关生成的个人区域网络（Personal Area Network，PAN），每个网络都拥有一个网络 ID，以此来与相同信道中的其他网络进行区分。在每个 ZigBee 网络中，拥有一个智能网关和多个智能设备，每个设备都拥有一个短地址，通过短地址来进行设备间通信，拓扑结构如图 3 所示。在 ZigBee 网络中，智能网关负责网络的管理和协调，并汇总智能设备收集到的数据上传至云端，智能设备则负责收集环境中的信息，并根据用户设置的规则执行自动化操作。

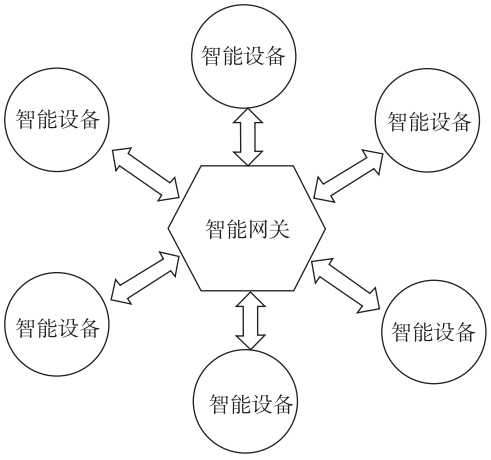

图 3　ZigBee 网络拓扑结构

本文根据设备的短地址对数据进行分离，将整体 ZigBee 网络流量包划分为各个设备的独立流量，并按照时间顺序切分为多个子序列，构建设备流量矩阵，具体流程如图 4 所示。

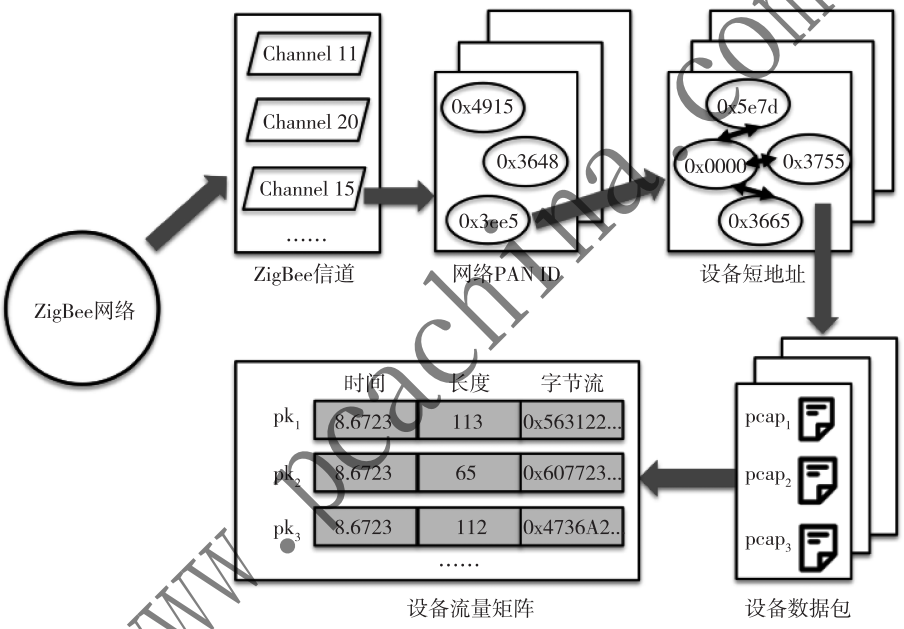

图 4　ZigBee 数据分离流程

由于 ZigBee 设备不具备调频通信能力，设备正常工作时不会切换信道。在进行数据收集之后，本文首先根据 ZigBee 信道将流量划分为多个信道流量，然后，针对每个信道提取各个网络 PAN ID，分别代表各个智能网关搭建的 ZigBee 子网络。在每个网络 PAN ID 中，拥有一个智能网关和多个智能传感器设备，每个设备都具有一个唯一的设备短地址，由于智能网关的短地址通常为 0x0000，在识别智能网关流量时较为容易，故在后续的数据处理中去除智能网关的流量，根据各个子设备的短地址对每个设备的流量进行分离。最终从整个 ZigBee 网络中分离出每个设备的网络流量，并将其以 pcap 格式保存。

为了方便后续设备流量的特征处理，将每个网络流量看作为通信双方实体按时间顺序排列构建的数据包序列。尽管 ZigBee 协议使用高级加密标准（Advanced Encryption Standard，AES）算法加密其有效载荷，但是数据加密并不能掩盖通信流量的基本特征，如数据包的发送时间、长度等，本文将每个数据包处理成特定结构，具体如式（1）所示：

$$pk_i = (time,\ len,\ data) \tag{1}$$

其中，pk_i 代表收集到的第 i 个数据包，time 表示数据包的时间戳，len 表示数据包的长度，data 表示数据包的字节流数据。将所有的数据流量包都处理成上述格式，构建一个具有三列的矩阵，以便后续的数据包特征处理工作。

3.4　设备识别模块

将 ZigBee 设备流量分离之后，为了有效地识别设备类型信息，需要从设备的数据矩阵中提取设备特征，建立深度学习网络搭建设备识别模块，具体如图 5 所示。

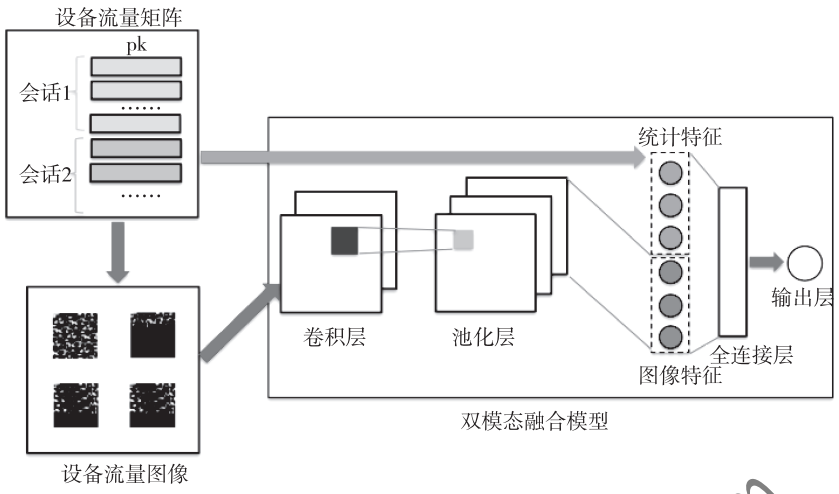

图 5　双模态融合设备识别模型

在双模态融合设备识别模型中，首先需要对设备的数据矩阵切分数据集。常见的流量切分有多种方式，不同的流量切分方式会得到不一样的数据集，如以会话、服务、数据流、TCP 连接等方式进行切分[14]。在 ZigBee 设备流量中，设备监测环境的活动流量是 ZigBee 网络的主体流量，也是不同设备间的主要差异。此外，通过实验观察发现，一个完整的用户触发智能设备的过程通常包含以下三步：用户触发智能设备，智能设备发送数据包至网关，以及网关返回确认包给智能设备。因此，本文使用以会话的方式进行流量划分，将数据流量包看作一个连续的过程，设置时间窗口为 5 s，尽可能包含一个完整的智能设备交互过程，以每 5 s 的流量数据作为一个样本。

为了提高设备识别的准确率，本文设计了一种双模态融合方法，分别提取设备流量的统计特征和图像特征，在构建识别模型时融合两个模态的特征并进行设备分类识别，能够有效地融合两种特征的优点。针对设备流量的统计特征，通过对不同设备产生的流量数据分析发现，不同类型的设备在一个交互过程中产生的流量包数量存在差异，触发数据包的大小也存在一定的差异，即使 ZigBee 流量经过了加密处理，依然无法掩盖流量的基本特征。故本文选取一个时间窗口内的数据包平均包长、数据包包长的标准差、数据包数量以及平均返回时间作为设备类型统计特征。针对设备的图像特征，需要将会话内的设备流量转化为流量图像，本文采用文献［15］流量处理的方式，能够有效地降低模型算法的复杂度。对于每一个流量会话，提取会话中前 784 个字节长度的数据，若会话的数据长度超过 784 字节，则多余的字节去除，若会话的数据长度小于 784 字节，则将在会话数据的末尾补充 0x00 字节，直到会话的大小为 784 字节。然后将会话流量转化为相同大小的灰度图，流量中的每个字节代表灰度图中的一个像素，其中 0xFF 代表白色，0x00 代表黑色，其他数值使用不同深浅的灰色代替，最终每个设备会话均转化为相应的灰度图。

图像的特征采用卷积神经网络（Convolutional Neural Networks，CNN）模型进行提取，在设计的双模态融合设备识别模型中，存在两层卷积层、两层池化层和两层全连接层，其中卷积层用于提取图像的局部特征，池化层用于降低特征图的空间维度，减少参数数量，提高计算效率，第一层全连接层用于进一步抽象特征，学习高级特征组合，第二层全连接层作为最终的分类器，将特征映射到类别空间，两个全连接层中增加 dropout 层以防止模型的过拟合。流量图像在通过卷积层和池化层后，得到相应图像的特征矩阵，同时与相对应的统计特征相融合，将其共同输入至全连接层中进一步学习流量的高维特征，并利用 ReLU 激活函数增强模型的表达能力，最终输出预测的设备类别。通过提取流量文本的统计特征和流量图像的高维特征，并在模型中融合流量数据在不同模态下的数据特征，能够有效地弥补单一模态下数据特征的不足，具有更好的设备识别性能。

4　实验评估

4.1　实验设计

本文收集了来自 5 个厂商的 15 个不同 ZigBee 设备的运行流量，以此作为双模态融合模型的训练数据和测试数据，并以 8 ∶ 2 的比例随机对训练数据和测试数据进行划分。为了突出基于双模态融合识别模型的性能，本文将实验分为两个部分。第一部分实验采用以往研究中常用的方法，使用 ZigBee 流量中的统计特征作为设备的识

别特征，并使用多个多分类模型来测试设备识别的有效性。第二部分实验将融合设备流量的统计特征和图像特征作为设备的识别特征，使用双模态融合模型进行设备分类，并与第一部分的实验结果进行比对，以体现双模态融合模型的设备识别效果。

为了有效地验证不同模型的优劣，本文使用准确率（Accuracy）、精确率（Precision）、召回率（Recall）和 $F1$ 分数（$F1$-score）来评估模型的性能，公式如下所示：

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} \tag{2}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{3}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{4}$$

$$F1 = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{5}$$

其中，TP 代表实际正类且被模型预测为正类的样本数，TN 代表实际负类且被模型预测为负类的样本数，FP 代表实际为负类但被模型错误预测为正类的样本数，FN 代表实际为正类但被模型错误预测为负类的样本数。本文的实验均是在 Windows 平台和 Python 语言环境下完成，具体的实验环境配置信息如表 2 所示。

表 2　实验环境配置

环境配置	版本
操作系统	Windows 11
显卡	NVIDIA 3070
Python	3. 11. 7
Scapy	2. 5. 0
PyTorch	2. 3. 1
Scikit-learn	1. 2. 2

4. 2　实验结果及分析

在第一部分实验中，使用设备流量中的统计特征作为设备分类特征，将其输入 8 个常见的多分类模型中进行训练，其中包含 Random Forest、Support Vector Machine（SVM）、K-Nearest Neighbors、Decision Tree、Multilayer Perceptron（MLP）、Logistic Regression、XGBoost、AdaBoost 模型。同时使用 5 折交叉验证法计算每个机器学习模型的设备识别准确率，避免由于数据集划分不合理而导致出现问题。各模型的平均准确率如图 6 所示。

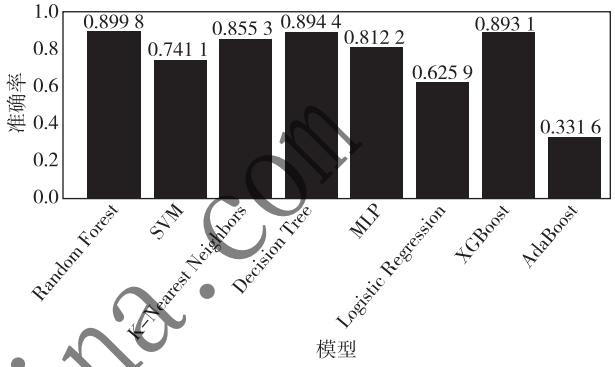

图 6　各分类模型识别性能

从图 6 可以看到，Random Forest、Decision Tree 和 XGBoost 模型拥有较好的设备分类性能，平均准确率均超过了 89%，其中 Random Forest 模型的设备分类准确率最高，达到 89. 98%。与此同时，为了验证分类模型在多折交叉验证下的稳定度，计算模型在不同轮次中的准确率误差，具体结果如图 7 所示。

从图 7 箱线图中可以看到每个模型在交叉验证中的准确率分布。随机数据划分没有给模型带来巨大的性能波动，其中平均准确率最高的 Random Forest 模型同样拥有较小的性能误差。因此，本文选取 Random Forest 模型

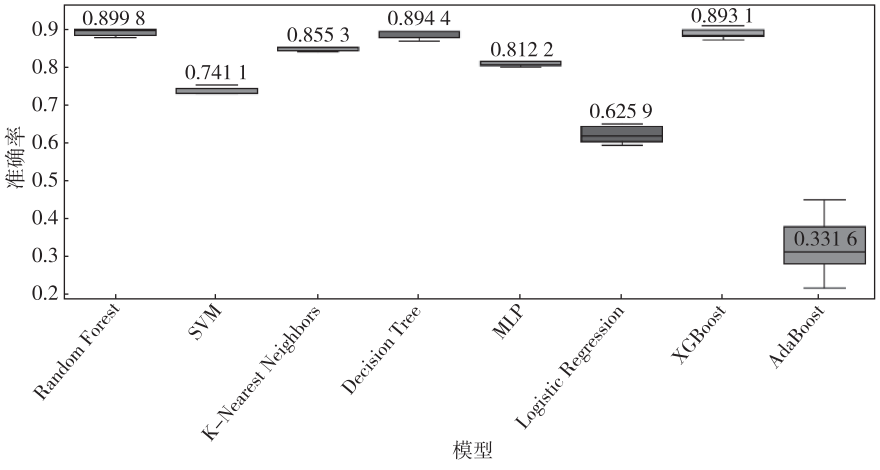

图 7　各分类模型识别准确率分布

作为基于统计特征的基准模型，并进一步展示分类模型在每个设备类型下的识别性能，具体如表 3 所示。

表 3　基于统计特征的设备识别模型性能

设备类型	精确率	召回率	*F*1 分数
Aqara-人体传感器	0.97	1.00	0.99
Aqara-动静贴	0.99	0.96	0.97
Aqara-门磁传感器	0.68	0.75	0.71
京东-人体传感器	0.92	0.92	0.92
京东-无线开关	0.97	1.00	0.99
京东-无线智能插座	0.92	0.93	0.93
京东-门磁传感器	0.89	1.00	0.94
华为-人体传感器	0.88	0.94	0.91
华为-温湿度传感器	0.95	0.68	0.79
华为-门磁传感器	0.73	0.75	0.74
小米-人体传感器	0.88	0.88	0.88
小米-天然气报警器	0.84	0.84	0.84
小米-烟雾报警器	1.00	1.00	1.00
海曼-人体传感器	0.95	0.95	0.95
海曼-门磁传感器	0.69	0.61	0.65

从表 2 可以看到模型对部分设备的识别性能较好，如 Aqara-人体传感器、小米 - 烟雾报警器、京东 - 无线开关等，其中小米 - 烟雾报警器的识别率达到了 100%。与此同时，部分设备的识别性能较差，如海曼 - 门磁传感器的精确率仅为 69%，召回率仅为 61%，*F*1 分数仅为 65%。由于部分设备的通信逻辑类型，仅依赖流量的统计特征搭建的设备识别模型无法很好地处理具有相似功能的多设备分类任务，在识别这类设备时出现错误较多，比如在门磁传感器类别中，Aqara、京东、华为、海曼均拥有该类设备，其设备识别性能较差，模型识别的 *F*1 分数分别仅有 71%、94%、74%、65%。

为了解决传统的基于流量统计特征的设备识别模型性能的不足，本文设计了一种基于双模态融合的设备识别模型，将流量的统计特征与图像特征融合在一起，有效地识别设备类型信息。在第二部分实验中，结合流量的统计特征与图像特征搭建 CNN 模型。训练模型时使用 CrossEntropyLoss 损失函数评估模型在区分不同类别上的性能，使用 Adam 优化器自动调整每个参数的学习率，将初始学习率设为 0.001，模型的训练轮次设为 20。基于双模态融合的 ZigBee 设备识别模型训练过程如图 8 所示，其中（a）为模型训练过程中的损失趋势，（b）为模型每轮次在测试集上的准确率趋势。

当基于双模态融合识别模型经过 20 轮训练后，最终的模型损失趋向稳定，在测试集上达到了良好的设备识别效果，最终轮次的设备识别准确率达到了 99.37%。基于双模态融合识别模型的混淆矩阵如图 9 所示，从图中可以看出，模型在每个设备类别上均拥有良好的设备识别性能。

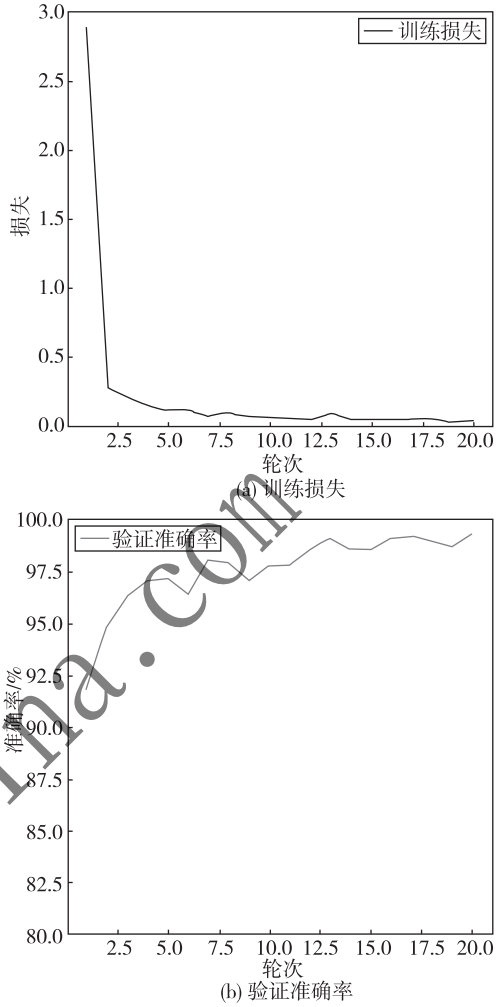

图 8　基于双模态融合识别模型训练过程

为了比较基于统计特征的设备识别模型与基于双模态融合的设备识别模型之间的性能优劣，将每个设备在两个模型中的 *F*1 分数进行比对，具体如图 10 所示，其中模型 -1 代表基于双模态融合的设备识别模型，模型 -2 代表基于统计特征的设备识别模型。从图中可以看到，基于双模态融合的设备识别模型在各设备类别的识别性能均优于基于统计特征的设备识别模型，在大部分设备类别上的 *F*1 分数接近 1，部分设备的 *F*1 分数获得极大的提高，如海曼 - 门磁传感器的 *F*1 分数从 0.65 提高到 0.94，Aqara - 门磁传感器的 *F*1 分数从 0.71 提高到 1。实验证明，基于双模态融合的 ZigBee 设备识别模型能够有效地识别设备类型信息，平均设备识别准确率达到 99.37%，能够有效地保护用户的隐私安全。

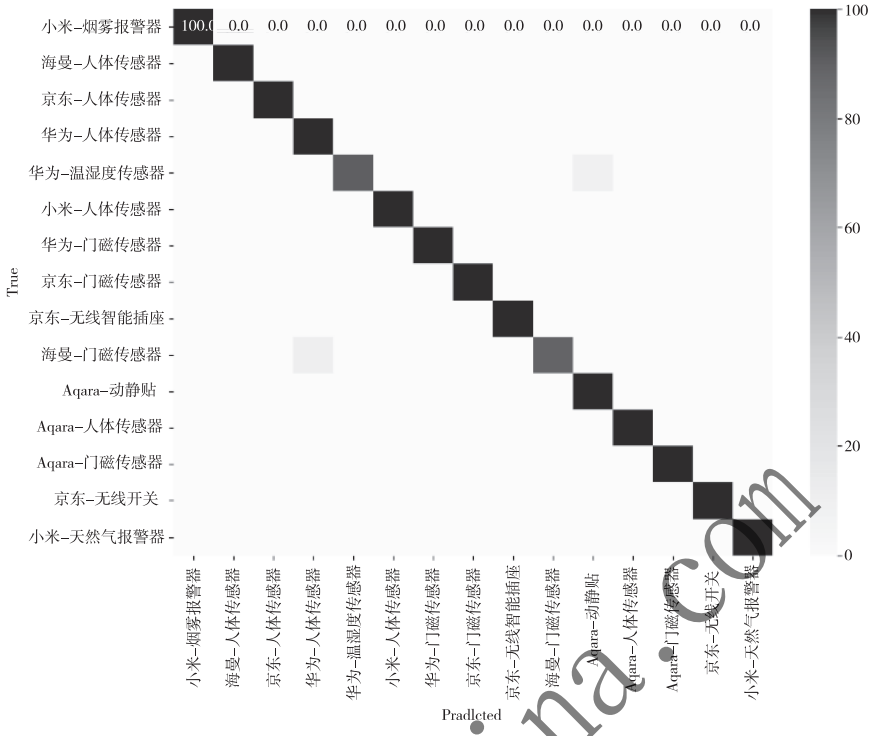

图 9　基于双模态融合识别模型混淆矩阵

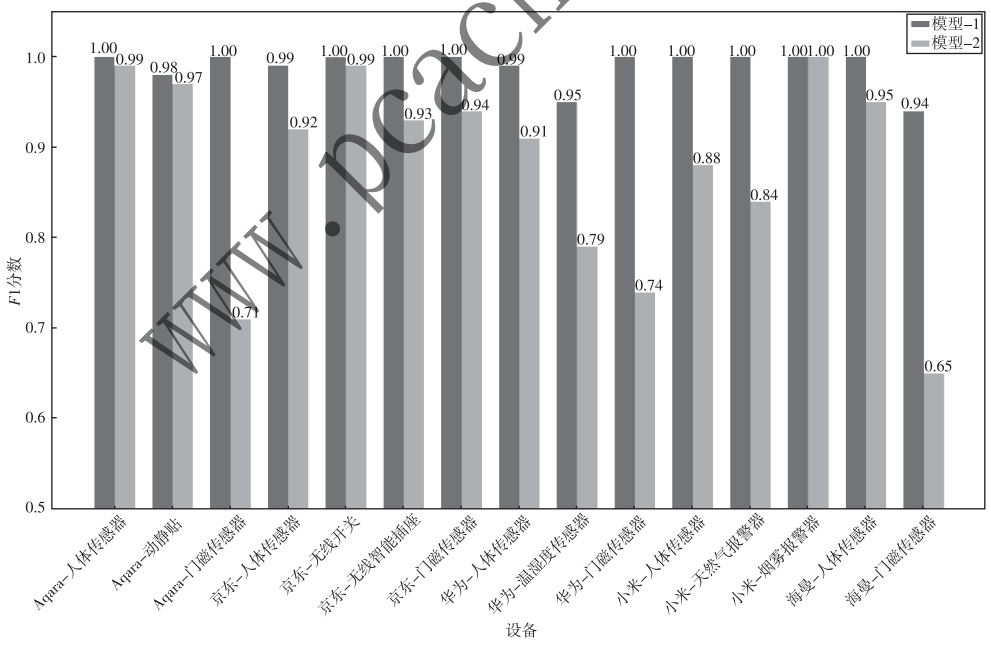

图 10　不同模型下各设备 *F*1 分数比对

5　结论

针对用户隐私信息泄露的威胁场景，本文设计了一种基于双模态融合的 ZigBee 设备识别方法，通过空中抓取环境周围的 ZigBee 流量数据，提取流量在不同模态下的设备特征，构建基于双模态融合的设备识别模型，能够有效地提高设备识别模型性能，在 Zigbee 设备识别准确率上达到 99% 左右。随着智能家居行业的快速发展，大量物联网设备应用于人们的日常生活中，在方便人们日常生活的同时，也带来了隐私泄露风险，如何更好地平衡产品的智联能力和隐私保护设计，依然是未来研究的重点。

参考文献

[1] 亿欧智库. 2024 智能家居行业创新发展与前景展望研究报告[EB/OL]. (2024-03-07)[2024-06-15]. https://www.iyiou.com/research/202403071311.

[2] SCHUSTER F, HABIBIPOUR A. Users' privacy and security concerns that affect IoT adoption in the home domain [J]. International Journal of Human-Computer Interaction, 2024, 40 (7): 1632-1643.

[3] RAMON SAURA J, PALACIOS-MARQUES D, RIBEIRO-SORIANO D. Using data mining techniques to explore security issues in smart living environments in Twitter [J]. Computer Communications, 2021, 179 (C): 285-295.

[4] AKESTORIDIS D G, HARISHANKAR M, WEBER M, et al. Zigator: analyzing the security of Zigbee-enabled smart homes [C]// Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2020: 77-88.

[5] MIETTINEN M, MARCHAL S, HAFEEZ I, et al. IoT sentinel: automated device-type identification for security enforcement in IoT [C]//2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017: 2177-2184.

[6] BEZAWADA B, RAY I, RAY I. Behavioral fingerprinting of Internet-of-Things devices [J]. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 2021, 11 (1): e1337.

[7] XIE L N, PENG L N, ZHANG J Q, et al. Radio frequency fingerprint identification for Internet of Things: a survey [J]. Security and Safety, 2024, 3 (1): 104-135.

[8] 周樨, 唐丹红, 蔡阳, 等. 用于无线设备身份识别的射频指纹提取方法 [J]. 集成电路与嵌入式系统, 2024, 24 (1): 69-72.

[9] LIU C, FU X, WANG Y, et al. Overcoming data limitations: a few-shot specific emitter identification method usingself-supervised learning and adversarial augmentation [J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 500-513.

[10] MIRSKY Y, DOITSHMAN T, ELOVICI Y, et al. Kitsune: an ensemble of autoencoders for online network intrusion detection [J]. arXiv preprint arXiv: 1802.09089, 2018.

[11] DONG S K, LI Z, TANG D, et al. Your smart home can't keep a secret: towards automated fingerprinting of IoT traffic [C]// Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, 2020: 47-59.

[12] 袁杨鑫. 基于深度学习的无线设备射频指纹识别技术研究 [D]. 南京: 东南大学, 2021.

[13] ACAR A, FEREIDOONI H, ABERA T, et al. Peek-a-boo: I see your smart home activities, even encrypted! [C]//Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2020: 207-218.

[14] DAINOTTI A, PESCAPE A, CLAFFY K C. Issues and future directions in traffic classification [J]. IEEE Network, 2012, 26 (1): 35-40.

[15] 胡永进, 郭渊博, 马骏, 等. 基于对抗样本的网络欺骗流量生成方法 [J]. 通信学报, 2020, 41 (9): 59-70.

(收稿日期: 2024-12-20)

作者简介:

李荣 (1998-), 男, 硕士, 助理工程师, 主要研究方向: 物联网安全、车联网安全、AI 安全。

赖怡聪 (1995-), 男, 本科, 助理工程师, 主要研究方向: 智能产品及汽车信息安全。

李乐言 (1993-), 通信作者, 男, 本科, 工程师, 主要研究方向: 信息安全攻防技术和质量评价技术、智能产品及汽车信息安全。E-mali: liyueyan@ceprei.biz。

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