软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2024,35(1):288−308 [doi: 10.13328/j.cnki.jos.006818]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

# 物联网设备识别及异常检测研究综述*

樊琳娜[1,2,3], 李城龙[1], 吴毅超[1,2], 段晨鑫[1,2], 王之梁[1,2], 林 海[1,2], 杨家海[1,2]

[1](清华大学 网络科学与网络空间研究院, 北京 100084)

[2](北京信息科学与技术国家研究中心, 北京 100084)

[3](国防科技大学 信息通信学院, 湖北 武汉 430019)

通信作者: 李城龙, E-mail: lichenglong@tsinghua.edu.cn; 杨家海, E-mail: yang@cernet.edu.cn

**摘 要**: 随着物联网技术的发展, 物联网设备广泛应用于生产和生活的各个领域, 但也为设备资产管理和安全管理带来了严峻的挑战. 首先, 由于物联网设备类型和接入方式的多样性, 网络管理员通常难以得知网络中的物联网设备类型及运行状态. 其次, 物联网设备由于其计算、存储资源有限, 难以部署传统防御措施, 正逐渐成为网络攻击的焦点. 因此, 通过设备识别了解网络中的物联网设备并基于设备识别结果进行异常检测, 以保证其正常运行尤为重要. 近几年来, 学术界围绕上述问题开展了大量的研究. 系统地梳理物联网设备识别和异常检测方面的相关工作. 在设备识别方面, 根据是否向网络中发送数据包, 现有研究可分为被动识别方法和主动识别方法. 针对被动识别方法按照识别方法、识别粒度和应用场景进行进一步的调研, 针对主动识别方法按照识别方法、识别粒度和探测粒度进行进一步的调研. 在异常检测方面, 按照基于机器学习算法的检测方法和基于行为规范的规则匹配方法进行梳理. 在此基础上, 总结物联网设备识别和异常检测领域的研究挑战并展望其未来发展方向.

**关键词**: 物联网; 设备识别; 异常检测

**中图法分类号**: TP393

中文引用格式: 樊琳娜, 李城龙, 吴毅超, 段晨鑫, 王之梁, 林海, 杨家海. 物联网设备识别及异常检测研究综述. 软件学报, 2024, 35(1): 288–308. http://www.jos.org.cn/1000-9825/6818.htm

英文引用格式: Fan LN, Li CL, Wu YC, Duan CX, Wang ZL, Lin H, Yang JH. Survey on IoT Device Identification and Anomaly Detection. Ruan Jian Xue Bao/Journal of Software, 2024, 35(1): 288–308 (in Chinese). http://www.jos.org.cn/1000-9825/6818.htm

## Survey on IoT Device Identification and Anomaly Detection

FAN Lin-Na[1,2,3], LI Cheng-Long[1], WU Yi-Chao[1,2], DUAN Chen-Xin[1,2], WANG Zhi-Liang[1,2], LIN Hai[1,2], YANG Jia-Hai[1,2]

[1](Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China)

[2](Beijing National Research Center for Information Science and Technology, Beijing 100084, China)

[3](College of Information and Communication, National University of Defense Technology, Wuhan 430019, China)

**Abstract**: With the development of Internet of Things (IoT) technology, IoT devices are widely applied in many areas of production and life. However, IoT devices also bring severe challenges to equipment asset management and security management. Firstly, Due to the diversity of IoT device types and access modes, it is often difficult for network administrators to know the IoT device types and operating status in the network. Secondly, IoT devices are becoming the focus of cyber attacks due to their limited computing and storage resources, which makes it difficult to deploy traditional defense measures. Therefore, it is important to acknowledge the IoT devices in the network through device identification and detect anomalies based on the device identification results, so as to ensure the normal operation of IoT devices. In recent years, academia has carried out a lot of research on the above issues. This study systematically reviews the work related to IoT device identification and anomaly detection. In terms of device identification, existing research can be divided into passive

* 基金项目: 国家自然科学基金 (62172251); 国家重点研发计划 (2018YFB1800204)
收稿时间: 2021-11-11; 修改时间: 2022-02-20, 2022-07-18; 采用时间: 2022-08-15; jos 在线出版时间: 2023-01-13
CNKI 网络首发时间: 2023-05-26

identification methods and active identification methods according to whether data packets are sent to the network. The passive identification methods are further investigated according to the identification method, identification granularity, and application scenarios. The study also investigates the active identification methods according to the identification method, identification granularity, and detection granularity. In terms of anomaly detection, the existing work can be divided into detection methods based on machine learning algorithms and rule-matching methods based on behavioral norms. On this basis, challenges in IoT device identification and anomaly detection are summarized, and the future development direction is proposed.

**Key words**: Internet of Things (IoT); device identification; anomaly detection

互联网作为当代信息社会的基础载体, 将人与人连接起来, 而信息化社会对通信的要求不只局限于人与人之间, 物联网 (Internet of Things, IoT) 技术的发展将通信拓展到了人与物、物与物之间. 物联网设备指的是能够互相通信, 且不需要人类直接参与的设备[1], 如智能插座、智能电灯、摄像头、温度/湿度传感器等. 非物联网设备包括计算机、笔记本电脑、平板电脑、手机等. 物联网技术的发展可以节约生产成本并提高经济效益, 已成为继计算机、互联网之后信息科技产业的第 3 次革命. 据 IDC (international data corporation) 预测, 物联网技术的产值在 2022 年将会超过 1.2 万亿美元[2]. 然而, 物联网的发展也为设备资产管理和安全管理带来了严峻的挑战.

设备资产管理随着物联网设备的增多变得困难. 网络管理员通常需要对网络中的传感器、控制器等进行定期安装、配置、监控、诊断、更新和维护, 网络中众多的物联网设备对网络管理员提出了很高的要求. 此外, 某些设备处于远离企业主要设施的偏远位置, 通过物理的方式对每个设备进行管理需要耗费大量的人力、物力. 同时, 网络接入也变得更加不可控, 新的物联网设备通过各种形态的无线方式接入, 管理员需要及时发现新接入的设备以及判定新接入的设备是否属于违规接入设备. 因此, 需要通过技术手段达到设备的自动识别和监控.

物联网技术的发展为安全管理带来了严峻的挑战. 物联网技术的发展造成的网络安全问题层出不穷且危害巨大. Mirai 正是一种由被攻陷的物联网设备所组成的一个大型僵尸网络, 其在 2016 年所发动的大规模分布式拒绝服务攻击使美国东海岸的重要通信基础设施陷入瘫痪, 带来了巨大的经济损失[3]. 而这种主要由物联网设备构成的僵尸网络愈演愈烈, 变得越来越顽强[4], 甚至有研究表明, 由大功率物联网设备所构成的僵尸网络具备破坏一个地区的电力能源系统的能力[5]. 物联网设备易受攻击的原因来自 3 个方面. 首先, 物联网设备的计算和存储资源通常比较有限, 导致其难以部署如防病毒软件、防火墙等传统的防御措施; 其次, 物联网设备的硬件、软件多样性较强, 导致其暴露的攻击面大, 并且难以部署统一的防御措施; 最后, 物联网设备制造商在设备生产时也缺乏安全性考虑的动力. 而物联网设备一旦被攻击后造成的影响也较大. 首先, 物联网设备受攻击后其自身的功能会受到影响; 其次, 受攻击的物联网设备可能会成为攻击者的跳板从而进一步攻击其他设备; 最后, 受攻击的物联网设备也可以被攻击者利用进行 DDoS 攻击, 导致网络瘫痪. 因此, 需要通过物联网设备异常检测, 及时发现网络中的攻击行为, 提升安全管理能力.

综上, 研究物联网设备识别和异常检测对于设备资产管理和安全管理具有重要意义. 同时, 物联网设备识别也是安全管理的基础. 从应用角度来看, 异常检测模型应建立在设备识别的基础上, 这主要包含两方面的原因. 首先, 在物联网设备与通用联网设备并存的网络环境中, 对两类设备采用统一的混合式监控和异常检测通常会面临检测粒度粗糙和正常行为与异常行为边界模糊的问题, 难以取得较好的检测性能. 其次, 各种不同的物联网设备彼此之间的功能和通信模式上也存在较大的差异, 例如一个联网监控摄像头会持续产生视频流量输出, 而一个智能插座的流量产生多数是由用户操作驱动的. 已有的异常检测技术几乎都缺少基于这些差异的定制化的设计和实现, 难以对网络中的各种物联网设备实现细粒度的监控与高精度的异常检测. 所以, 基于设备类型充分挖掘各种物联网设备所独有的通信模式, 并定制化的设计专用异常检测算法, 对于未来存在大量物联网设备的真实网络环境中的网络管理至关重要. 因此, 物联网设备识别工作应作为异常检测的基础, 二者密不可分. 此外, 在技术原理上, 二者也有相通之处, 即设备识别和异常检测都可以转化为分类问题, 其原理可以表示为图 1 所示的过程. 首先需要进行数据采集, 设备识别采集的是被动的网络流量或者通过主动探测得到的目标设备的响应数据包, 异常检测采集的是正常流量数据或特定异常类型的流量数据、日志或应用的源代码等; 然后对采集得到的数据进行预处理, 设备识别可以从数据中提取规则构成规则库从而用于设备识别, 异常检测可以构建设备的正常行为规范, 从而将不符合行为规范的设备判断为异常. 除了规则匹配, 它们也可以利用预处理后的数据得到原始特征, 构建机器学习模

型, 用于设备识别或异常检测. 从分类结果来看, 设备识别分类的结果是设备类别, 而异常检测的分类结果是正常/异常或者具体的异常类型. 由于设备识别和异常检测均可归结为分类问题, 因此通常可采用准确率 (Accuracy)、精确率 (Precision)、召回率 (Recall) 和 $F1$ 分数值来进行评估. 异常检测还可以使用误报率 (false alarm rate)、漏报率 (false negative rate) 来评测.


图 1 IoT 设备识别和异常检测原理

近年来物联网设备识别和异常检测工作成为研究热点, 但现有的综述相对较少, 已有的综述也各有侧重, 缺乏对该领域的全面梳理. 文献 [6] 总结了 IoT 设备识别和异常检测的相关工作, 但缺乏对最新的被动识别方法的总结和梳理. 文献 [7] 重点关注的是基于机器学习的设备识别方法, 缺乏对设备识别方法的全面梳理. 文献 [8] 中的异常检测工作只关注基于 MUD (manufacturer usage description) 的方法. 并且以上的综述文献都缺少对 IoT 设备主动识别方法的梳理. 为了解决以上问题, 本文系统地梳理了 IoT 设备识别和异常检测的相关工作以及数据集, 如图 2 所示.

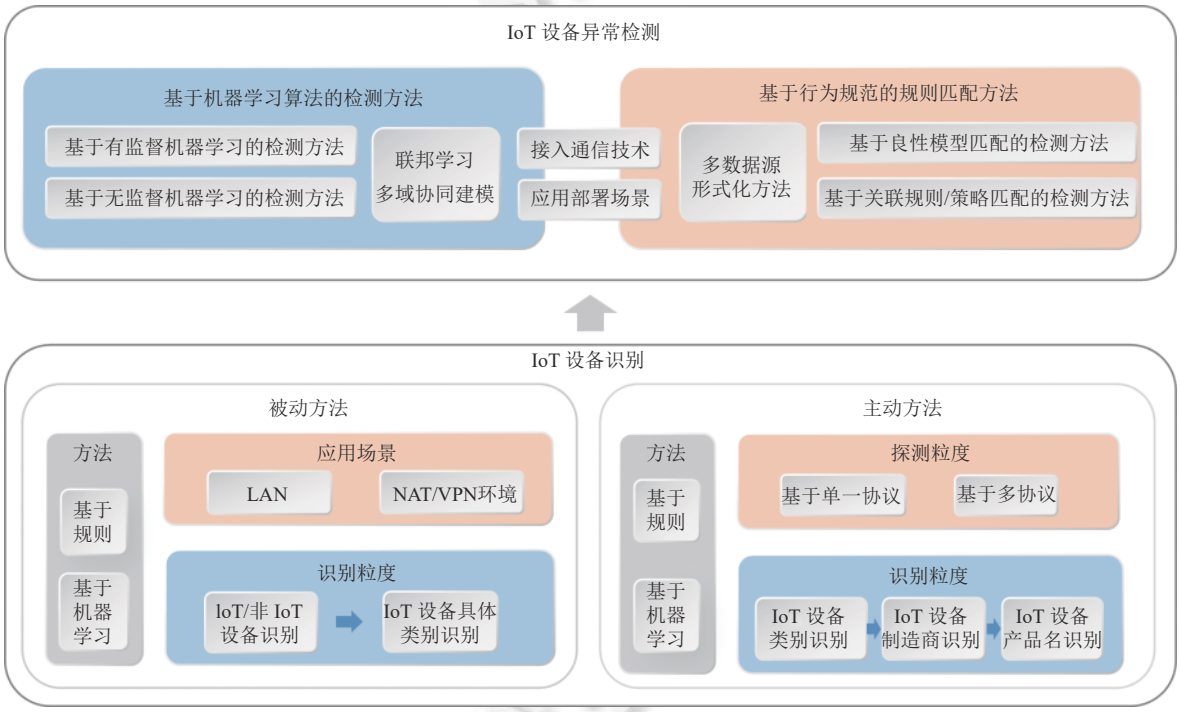


图 2 IoT 设备识别及异常检测工作梳理

在 IoT 设备识别方面, 根据是否向网络中发送数据包, 现有研究可分为被动识别方法和主动识别方法.

被动识别方法对网络造成的影响较小, 现有的工作可以从不同的维度进行划分. 从方法层面, 现有工作可分为基于规则的方法和基于机器学习的方法. 从识别粒度方面, 可分为 IoT 和非 IoT 设备的识别和 IoT 具体类别的识别. 从应用场景上, 大多数方法只能应用于局域网 (local area network, LAN) 环境, 部分方法可应用于更为复杂的网络环境, 如有 NAT (network address translation) 或有 VPN (virtual private network) 存在的环境.

主动识别方法中, 需要确定好待识别目标, 然后主动向目标发送探测包并接受其返回数据, 因此会对网络造成一定的影响, 影响的大小主要取决于待识别目标的范围以及探测包的发送速率. 现有的在主动场景下的设备识别工作同样可以从不同维度进行划分. 从方法层面, 可分为基于机器学习和基于规则两大类. 从识别粒度层面, 可分为 IoT 设备类型识别、设备制造商识别和设备产品名识别. 从探测粒度层面, 可分为基于单一协议的设备识别和基于多协议的设备识别.

为了确保各类物联网设备能够持续稳定地正常运转, 及时准确地发现物联网设备上发生的异常现象尤为重要, 这就需要面向物联网设备的异常检测系统. 与通用的网络异常检测系统相似, 面向物联网设备的异常检测系统也可以分为基于机器学习算法的检测方法和基于行为规范的规则匹配方法. 这两类方法都需要根据目标物联网设备所采用的接入通信技术和其应用部署场景进行定制化的设计. 在已有的基于机器学习算法的检测方法中, 通常利用有监督算法来识别已知的异常类型, 利用无监督算法构建出设备的正常行为轮廓从而检测未知的异常. 除此之外, 基于联邦学习技术的应用场景与同类型物联网设备大量分布式部署的特点, 一些研究者提出协同构建异常检测系统, 共享安全威胁情报和设备软件固件升级等信息. 已有的基于行为规范的规则匹配方法尝试通过多种不同的数据源, 如源代码、界面描述和日志等, 提取出描述物联网设备工作逻辑的行为规范, 其中既有对单个物联网设备的通信行为进行描述的算法, 也有对多个物联网设备之间的协作关系进行建模和规则提取的算法. 这类方法中形式化验证技术被广泛应用, 以检测出潜在的攻击向量.

本文在 IoT 设备识别方面分别梳理了被动识别方法和基于主动探测的方法, 然后总结了 IoT 异常检测的相关工作. 基于对这些工作系统地梳理, 总结了 IoT 设备识别和异常检测面临的挑战并展望了未来发展趋势.

## 1 基于被动方法的物联网设备识别

基于被动方法的 IoT 设备识别是指通过流量中含有的一些与设备有关的特征或信息来识别设备, 该类方法对网络造成的影响较小. 从方法上, 现有工作可分为基于规则和基于机器学习的方法. 从设备识别的粒度, 现有工作可分为 IoT/非 IoT 设备的识别和 IoT 具体类别的识别. 根据应用场景的不同, 现有工作可分为局域网环境下的设备识别和 NAT/VPN 环境下的设备识别.

### 1.1 识别方法

基于被动方法的 IoT 设备识别包括规则匹配和机器学习方法, 如图 3 所示. 规则匹配首先根据已知设备的流量特征建立规则库, 然后通过这些规则来识别相同类型设备. 基于机器学习的方法可以从部分有标签设备的流量中进行特征提取, 然后利用这些特征训练传统有监督机器学习模型或深度学习模型, 对于待识别设备同样进行特征提取并根据模型输出判断所属类别. 此外, 也可以不需要已知设备的标签信息, 直接对待识别设备进行特征提取, 然后通过聚类结果判断哪些设备属于一类.

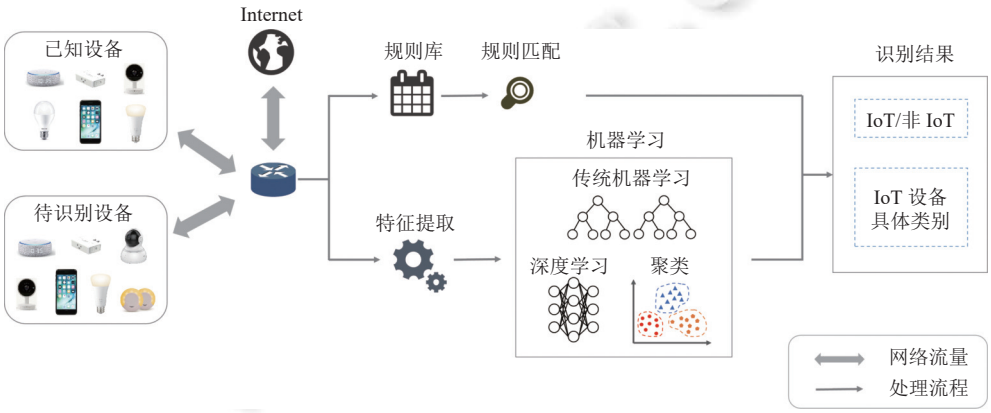


图 3 基于被动方法的 IoT 设备识别模型

1.1.1 基于规则的方法

基于规则的方法指通过收集已知设备的相关信息, 如 user-agent、MAC OUI (media access control organizationally unique identifier)[9]、DHCP (dynamic host configuration protocol) 中的主机名或者与 IoT 设备通信的云服务器的目的 IP 地址、通信端口号、DNS (domain name system) 请求中的域名等构建规则, 然后根据这些规则在流量中识别设备. 这类方法的依据是 IoT 设备的某些特征, 如 MAC OUI, DHCP 主机名或者与其通信的云服务器的目的 IP 地址、产生的域名等具有独特性, 因此通过这些信息构建规则, 从而用于设备识别.

早期的 IoT 设备识别方法利用了设备在通信过程中携带的信息, 如 HTTP (hyper text transfer protocol) 请求中的 user-agent 字段, MAC OUI 或者 DHCP 协商过程中的主机名 (host name) 信息来进行识别. 基于 user-agent 的设备识别方法无法应用于加密流量、仅有部分设备以明文传输该信息, 并且该方法具有较高的时间延迟, 因此不具备普适性[10,11]. MAC OUI 虽然对设备识别有帮助, 但识别粒度过粗[12]. DHCP 中的主机名虽然能够提供一定的设备类型信息, 但许多 IoT 设备在 DHCP 请求中不设置主机名或通过设置的主机名无法得到有用信息[13,14]. 此外, DHCP 主机名也容易被篡改.

由于早期方法存在的局限性, 有学者提出通过与 IoT 设备通信的云服务器的目的 IP 地址、通信端口号、DNS 请求中的域名等构建规则并进行设备识别, 如 Guo 等人[15]和 Hu 等人[16]. Saidi 等人[17]针对 ISP 流量很大的问题, 提出了一种通过稀疏采样进行设备识别的方法, 通过云服务器的 IP 地址、域名和端口号等来识别 ISP 和 IXP (Internet exchange point) 流量中的相同设备. Mazhar 等人[18]从 SSDP (simple service discovery protocol), DHCP, UPnP (universal plug and play) 数据包中抽取特征进行设备识别, 但由于 SSDP, DHCP 的流量可能会来自相同的网络组件, 如无线芯片, 因此该方法可能会失效.

基于规则的方法也具有其局限性. User-agent、MAC OUI、DHCP 中的主机名通常识别效果有限. 对于利用与 IoT 相关的云服务器的特征进行设备识别的方法来说, 如果远端服务器部署在公有云上, 它们对应的 IP 地址可能会动态变化[19]. 此外, 不同的 IoT 设备对应的服务器可能会部署在相同的云上, 导致它们的服务器 IP 地址相同, 并且随着 CDN (content delivery network) 的广泛部署, 通过远端服务器的 IP 地址进行识别将更不可靠[19]. 最后, 由于许多同一厂商的不同设备依赖于相同的远端服务器, 因此基于规则的方法无法对设备进行精确识别.

1.1.2 基于机器学习的方法

基于机器学习的方法已成为近年来的研究热点, 其通过设备流量提取相应的特征, 然后训练机器学习分类器以进行设备识别. 用于分类的特征通常包括时间间隔特征、流量特征、协议特征等. 现有的基于机器学习的方法包括随机森林 (random forests)、adaptive boosting (AdaBoost)、决策树 (decision tree)、朴素贝叶斯 (naive Bayesian) 和支持向量机 (support vector machine, SVM) 等传统有监督机器学习方法, 或卷积神经网络 (convolutional neural network, CNN)、循环神经网络 (recurrent neural network, RNN) 等深度学习方法以及 K 近邻 (K-nearest neighbors, KNN) 等聚类算法. 根据使用标签数量可分为有监督学习、半监督学习和无监督学习.

● 基于有监督学习的设备识别方法. 现有的工作大多数属于有监督学习方法. 使用有监督机器学习的理论依据是不同设备流量特征具有不同的概率分布, 可以基于此确定不同类别之间的分类边界, 对于待识别设备可以根据有监督模型判断它大概率属于哪个类别. 文献 [14,20−28] 基于传统有监督学习进行设备识别, 它们采用的模型包括 AdaBoost、KNN、决策树、随机森林、朴素贝叶斯和 SVM 等, 提取的特征也可归纳为时间间隔特征、流量特征和协议特征.

此外, 还有些工作[29−32]为每类设备构建二分类器来识别设备属于该类或不属于该类, 分类器采用的模型有随机森林、XGBoost、GBM (gradient boosting machine) 等. 采用的特征包括流量特征, 网络层、传输层和应用层的协议特征、域名等. 构建二分类器的缺点是每类设备均需建立一个分类器, 会耗费较多的计算、存储资源.

由于深度学习的飞速发展和强大的表征能力, 部分工作提出使用卷积神经网络、循环神经网络等进行设备识别. 文献 [33,34] 从流量中提取特征并使用 CNN 和长短期记忆 (long short-term memory, LSTM) 神经网络进行设备识别. 文献 [35] 构建多层感知机来达到设备识别的目的.

在以上方法中, 文献 [21−23,25,30,33] 是基于流提取特征的. 文献 [29,31] 需要捕获设备启动阶段的流量进行

设备识别, 缺点是一旦设备运行后将无法提取特征并建立模型.

● 基于半监督学习的设备识别方法. 考虑到有监督学习需要大量的有标注数据, 耗费较大的人力和时间, 因此文献 [36,37] 提出使用少量标签进行设备识别. 半监督学习只依据少量的有标签数据判断不同类别之间的决策边界. 文献 [36] 通过少量标签初始化聚类中心, 然后再使用 K-means 进行设备识别. 文献 [37] 训练了一个 CNN 分类器, 并在模型的损失中加入了 CCLP (compact clustering via label propagation) 损失[38], 即相同类设备的实例能够通过减小该损失形成一个紧凑的簇, 以利于后续的全连接层得到最终分类结果.

● 基于无监督学习的设备识别方法. 为进一步减少对标签的依赖, 部分工作提出使用无监督学习进行设备识别. 无监督学习方法的理论依据是相同类型的设备其流量具有相似性, 因而在聚类时相同类型设备其类内距离更小. Marchal 等人提出了 AuDI[39], 使用 KNN 算法进行聚类来完成设备识别, 该方法在训练过程中由于使用了傅里叶变换, 因此会耗费较长的运行时间, 难以满足实时性要求. 文献 [40] 通对每个设备分别使用 PCA (principal component analysis) 进行特征降维并使用 K-means 进行聚类. 在设备识别时, 根据待检测设备和这些聚类中心的距离以及聚类边界判断其所属类别. 文献 [41] 通过变分自编码器 (variational autoencoder, VAE) 进行特征降维, 然后使用 K-means 进行聚类. 无监督学习方法虽然不依赖于标签, 但通过在公开数据集上的实验发现无监督学习方法的识别精度低于有监督和半监督学习方法[37].

### 1.2 识别粒度

根据识别粒度的不同, 现有工作可分为 IoT/非 IoT 设备识别和 IoT 设备具体类别识别, 即首先从流量中区分哪些流量属于 IoT, 哪些属于非 IoT, 然后在 IoT 流量中区分具体设备类型. 现有的部分工作将每类非 IoT 设备也视为不同的设备, 这些做法虽然也能一定程度区分 IoT 与非 IoT 设备, 但在流量较大情况下识别每一种非 IoT 设备会耗费大量的资源和降低实时性, 因此在真实场景下首先区分 IoT 和非 IoT 设备是必要的步骤.

#### 1.2.1 IoT/非 IoT 设备识别

文献 [42] 结合 SDN (software defined network) 和机器学习提出了一种基于网络流量的 IoT 设备管理系统. 将流规则写入到 SDN 的交换机中, 然后对于流规则收集到的流量计算其统计特征并通过随机森林进行 IoT 和非 IoT 设备的分类.

DeviceMien[43]是一种基于神经网络的设备识别方法, 能够用于区分具体设备类别以及 IoT 和非 IoT 设备, 该方法从 TCP 流的载荷中提取信息, 然后通过降维和采样为每个设备得到多项式分布. 当要识别设备时, 通过对比多项式分布确定是否为同一类设备. 当判断待检测设备不属于已知类别时, 再通过 one class SVM 判断该设备是 IoT 还是非 IoT 设备. 该方法的优点是它考虑了新设备加入情况下判断 IoT 还是非 IoT, 但由于使用载荷训练神经网络, 因此会耗费大量的存储和计算资源, 且通过实验发现该方法耗费较长的时间.

文献 [11] 提出了新设备加入情况下的 IoT 和非 IoT 设备识别, 使用的分类器包括 3 种, 分别为逻辑回归分类器、根据 DHCP 信息建立的决策树以及这两种方法的结合. 在通过 DHCP 信息构建决策树过程中, 为了获取 DHCP 信息, 需要主动切断设备并使设备重新与 DHCP 服务器协商, 因此会对设备正常工作状态造成一定影响.

#### 1.2.2 IoT 设备具体类型识别

在区分设备属于 IoT 还是非 IoT 后, 对于 IoT 设备还需要进一步识别其具体类型, 如 Belkin Wemo Motion Sensor, Amazon Echo 等. 第 1.1 节中总结的方法, 包括基于规则的方法和基于机器学习的方法均可用于 IoT 设备具体类型的识别, 在此不再赘述. 本节重点阐述 IoT 设备具体类型识别中一个较为重要的问题, 即新类型设备的识别. 现有的大多数工作基于网络封闭的假设, 即网络中设备类型不再变化. 但真实的网络环境是一个开放的环境, 新的设备会不断加入, 这些新加入的设备可能属于已知设备类型, 也有可能是从未出现过的新类型, 只有实现新类型设备的识别并不断更新模型, IoT 设备识别才能应用到真实的网络环境中.

文献 [27] 为了识别新类型设备, 训练了一种结合有监督学习和无监督学习的混合模型. 首先为每个设备训练一个基于随机森林的二分类器, 用于判断待检测设备属于该类或不属于该类. 当待检测设备无法与已知类型匹配时, 认为它可能是一个新类型设备. 文献 [36] 使用 seeded K-means 进行设备识别, 即通过少量标签初始化聚类中

心, 然后再使用 K-means 进行设备识别. 当待检测设备的向量偏离聚类中心距离较大时, 认为它属于新类别, 然后利用新类别的特征更新模型参数. DeviceMien[43]也能够区分新类型设备, 它通过 LSTM-Autoencoder 学习到设备的低维向量表征, 然后通过聚类得到的伪标签为每类设备生成多个多项式分布, 通过多项式分布之间的 KS 检验判断待检测设备属于哪一类, 如果待检测设备不属于已知类别中的任何一种, 则认为它属于一种新类别.

现有的 IoT 设备识别中关于新类型设备识别的工作相对较少, 以上 3 篇文献 (文献 [27,36,43]) 能够一定程度上识别新设备, 但它们的实验都是基于新设备类别数固定且较少的情况, 当新设备类型数较多时, 模型对新设备的识别, 以及判断新类别的种类数和根据新设备流量更新模型都是值得研究的问题.

### 1.3 应用场景

以上的 IoT 设备识别方法适用于不同的网络环境, 有的方法只能局限于局域网 (LAN) 环境, 有的可以适用于更复杂的网络环境, 如 NAT、VPN 存在的环境.

#### 1.3.1 LAN 中的设备识别

LAN 网络环境下, IoT 设备识别系统通常可以部署于局域网的网关, 因此可以根据 MAC 地址或静态 IP 区分每个设备的流量, 在基于规则的方法中, 通过 MAC OUI 和 DHCP 主机名进行设备识别的方法只能用于 LAN 环境中, 而使用 HTTP 请求中 user-agent 的方法可以应用在更广泛的网络环境中. 利用与 IoT 设备相关的云服务器的特征进行设备识别的方法可以在更复杂网络环境中进行设备识别, 如 NAT 存在的网络环境. 基于机器学习的方法要从每个设备流量中提取特征, 因此现有方法大多只能应用于局域网环境.

#### 1.3.2 更加复杂网络环境下的设备识别

除了局域网环境之外, IoT 设备识别系统还可能部署在更为复杂的网络环境中, 如有 NAT 或 VPN 存在的环境中. 当有 NAT 存在时, 将无法区分其中不同设备的流量. 基于规则的方法由于仅使用与 IoT 设备通信的云服务器的信息, 因此不受影响, 但这时某个 IP 后的流量可能是多种设备流量的混合, 因此判断出的结果可能是某个 IP 后存在多种 IoT 设备.

Ma 等人[19]是从 ISP 的角度去识别 IoT 设备, 针对每个设备分别训练了两个 CNN 分类器, 用于识别设备类型和估算设备数量. Dong 等人[44]提出了一种在 NAPT 和 VPN 环境下识别 IoT 设备的方法, 通过双向 LSTM 分类器用于设备识别. 实验发现, 在 VPN 环境下, 设备识别精度下降, 因为此时特征中的目的端口、协议和包长等特征均因 VPN 流量的加密而受到影响.

综上所述, 对于较为复杂的网络环境下的 IoT 设备精确识别研究较少, 虽然基于规则的方法能够一定程度上识别设备, 但公有云及 CDN 的部署会使特征中的目的 IP 地址受到影响, 从而降低设备识别精度. 文献 [19] 和文献 [44] 虽然能在 NAT 和 VPN 环境下一定程度上识别 IoT 设备, 但是实验规模都较小, 在真实环境中的识别精度和识别效率有待验证. 基于被动方法的 IoT 设备识别工作如表 1 所示.

表 1 基于被动方法的 IoT 设备识别

| 大类 | 细分类别 | | 识别粒度 | 应用场景 | 数据集 | 识别效果(%) |
|---|---|---|---|---|---|---|
| 基于规则 | | User-agent[10] | Δ | LAN和NAT | 智能手机流量 | Acc: 100 |
| | | MAC OUI[12] | Δ | LAN | 试验床网络流量 | Acc: 80–90 |
| | | DHCP主机名[11] | Δ | LAN | 试验床网络流量 | *F*1: 96 |
| | | 云服务器的特征[15–19] | Δ | LAN和NAT | IXP/校园网流量 | Acc: 29–78 |
| 基于机器学习 | 有监督学习 | 传统有监督机器学习[11,14,20–32] | ○ /Δ/□ | LAN | 试验床网络流量/UNSW数据集[14] | Acc: 81–99 |
| | | 深度学习[19,33–35,43,44] | ○ /Δ/□ | LAN/NAT/VPN | 试验床网络流量 | Acc: 74–99 |
| | 半监督学习 | 基于部分标签聚类[36] | Δ/□ | LAN | 试验床网络流量 | Acc: 97 |
| | | 深度学习[37] | ○ /Δ | LAN | UNSW数据集[14] | Acc: 99 |
| | 无监督学习 | 聚类[39–41] | Δ | LAN | 试验床网络流量 | Acc: 94–98 |

注: 识别粒度列中, ○表示IoT/非IoT设备识别, Δ表示IoT具体设备识别, □表示新设备识别. Acc表示准确率Accuracy

### 1.4 数据集

公开数据集对于评估基于被动的 IoT 设备识别方法具有至关重要的作用. UNSW 数据集[14]和 Yourthings 数据集[45]就是用来评估设备类型识别的数据集. UNSW 数据集是为识别 IoT 设备类型而在新南威尔士大学的一个智能环境的网关处中采集的网络流量, 数据集中总共有 21 种不同的 IoT 设备共 20 天的流量, 此外, 还有一些非 IoT 设备的流量, 如笔记本电脑、移动电话等. 这些流量均是设备正常工作状态下收集的流量. Yourthings 数据集是为了评估 IoT 设备安全性而采集的流量, 其中含有 45 种 IoT 设备和若干非 IoT 设备的流量, 由于对这些设备的评估分为设备评估和网络评估, 因此流量也包括 3 天的设备评估产生的流量和 10 天的网络评估产生的流量. 由于在网络中使用了多种安全评估工具, 如扫描器等, 因此会对设备正常工作流量造成影响.

## 2 基于主动探测的物联网设备识别

基于主动探测的 IoT 设备识别是指主动向目标网段和端口发送探测包, 并收集返回的应用层协议数据以进行 IoT 设备的识别. 现有的工作可以从不同维度进行划分, 如前文图 1 所示. 从设备识别方法上考虑, 可分为基于规则和基于机器学习两大类. 从设备识别粒度上考虑, 可分为 IoT 设备类型识别、IoT 设备制造商识别、IoT 设备产品名称识别. 从探测粒度上可分为单一协议设备识别和多协议设备识别.

### 2.1 识别方法

基于主动探测的 IoT 设备识别方法同样包括基于机器学习和基于规则匹配的方法, 如图 4 所示. 扫描器进行网络扫描后, 获取到的设备返回数据将作为各种方法的原始输入. 规则匹配的方法利用已有的规则库对原始数据进行设备识别, 该规则库是事先利用人工或自动化的方法生成的. 基于机器学习的方法主要利用文本分析从原始数据中提取特征, 然后利用有监督机器学习算法或深度学习构建分类器并进行模型训练和测试.

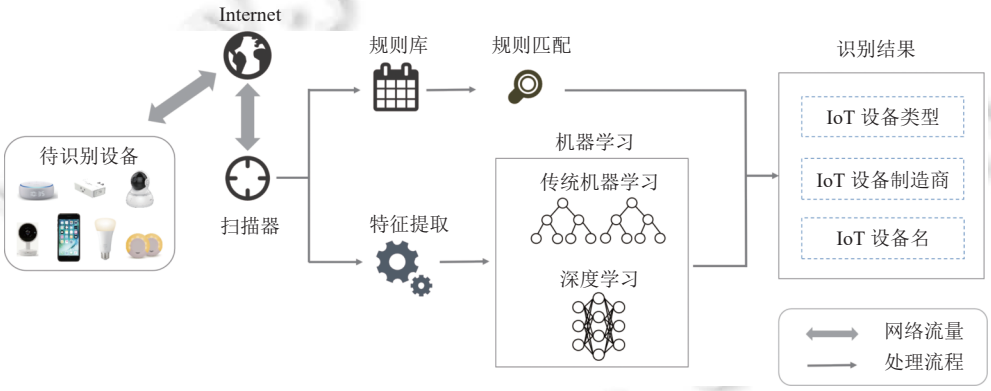


图 4 基于主动探测的 IoT 设备识别方法

#### 2.1.1 基于机器学习的方法

基于机器学习的方法的基本思路是首先从应用层返回数据中提取一定量的特征作为设备指纹, 再通过基于机器学习的方法根据已标注的数据训练出分类模型, 并利用该模型进行设备识别. 因此, 特征的选择和提取、数据的标注方法、模型的选择和训练都是研究的热点问题.

一些工作[15,46−50]致力于用一个模型解决多类 IoT 设备的分类问题. Cheng 等人[46]发现一些 IoT 设备暴露出来的 Web 页面中包含丰富的信息, 因此提取 HTML 页面中 server 等字段的长度, 包含的 CSS 数量等统计值作为特征向量, 并使用随机森林等机器学习方法训练模型来识别具体的 IoT 设备类型. 该方法的缺点是只适用于有 Web 页面的 IoT 设备识别. Yang 等人[47]提出将网络层和传输层的协议特征与应用层协议特征融合作为设备指纹. 并使用全连接网络作为多分类器. 此方法虽然能识别多种 IoT 设备, 且准确率较高, 但设备识别粒度较为粗糙.

还有些工作[51,52]致力于特定类型的 IoT 设备的识别. Song 等人[51]对网络摄像头设备类型及制造商进行更细

粒度的识别. 首先将完整的 HTTP 数据包作为设备指纹训练出一个二分类器, 区分是否为网络摄像头设备. 然后对设备指纹进行聚类和人工类别标注即可识别出不同设备的制造商. 此方法存在的问题是聚类时难以确定类别的数量, 且最后需要大量的人工标注. Yan 等人[52]致力于打印机的识别. 此工作将设备返回的不同协议的文本信息都作为用于设备识别的原始数据. 作者对原始数据进行预处理和词嵌入 (word embedding), 提取出文本特征作为设备指纹, 并使用 LSTM 训练了 3 个分类器, 分别用于判断设备类型 (是否为打印机)、设备制造商以及设备名. 此方法有高精度、细粒度的优点, 缺点是只适用于单一类型的设备识别且训练和识别时使用的 3 个 LSTM 网络开销较大, 数据量大时会存在一些性能问题.

这些工作本质上都是利用不同的方法从设备返回的原始数据中提取设备特征, 再根据所提取特征的特点构建机器学习分类模型, 并利用设备特征去训练这些模型. 受限于有监督学习的缺陷, 这些方法的不足之处也是类似的, 如训练集的获取, 新设备的识别等.

#### 2.1.2 基于规则的方法

基于规则的方法的基本思路是: 通过人工编写或自动化的方式来生成设备识别规则, 这些规则通常是由正则表达式和对应的设备信息所组成的二元组. 在进行设备识别时, 如果设备的应用层返回数据中的子串能与规则中的正则表达式匹配, 则利用该规则中的设备信息对设备进行标注[53]. 目前国内外已有的大型主动探测平台 (如 Censys, Shodan, ZoomEye 等) 几乎都是利用人工编写的规则库来进行设备识别. 然而, 人工编写标注规则过于繁琐, 且要求标注人员有较强的领域知识. 此外, 随着已有规则的不断增加, 大型规则库的维护与更新也是一大难题. 因此自动化的规则生成是当前研究的一大热点.

Feng 等人提出 ARE (acquisitional rule-based engine)[54], 开创性地提出了一套自动化的规则生成框架. 首先是数据收集与预处理, 通过主动发送探测包, 收集待测目标的应用层数据并提取关键词, 然后调用搜索引擎 API 来对这些关键词进行搜索和爬取, 获取设备关键词与搜索引擎返回的 Web 页面的映射. 其次在规则生成阶段, 利用 DER (device entity recognition, 设备实体识别) 从 Web 页面中提取设备注释 (类型、制造商和产品名) 并生成一系列关键词与设备注释的映射 (事务), 之后利用 Apriori 算法来学习和更新可用于设备标注的事务 (规则). ARE 在实际应用中仍存在许多问题, 例如: 如果 IoT 设备应用层数据中不存在有关类型、制造商、产品名等关键词, 则无法提取并用于搜索引擎识别; 如果 IoT 设备过于老旧, 搜索引擎可能无法返回搜索结果, 也可能搜索结果已经不是该设备的设备描述, 就无法继续进行下一步的规则生成, 或者会生成错误的标注规则.

Wang 等人提出 IoTTracker [55]来进一步识别 ARE 无法识别的设备. 在特征提取阶段, IoTTracker 将设备的应用层数据分为半结构数据 (如 HTML 文本等) 和无结构数据 (文本数据), 并分别提取其结构和类型特征, 内容和顺序特征. 在设备识别阶段, 需要打上标签的设备数据库, 并计算未知设备和已知设备的特征相似度, 如果相似度超过某一阈值, 则可用已知设备的标签来标记未知设备. 该方法局限性是, 能识别的设备数量依赖于标签集的完备程度; 但随着标签数据集的不断扩大, 识别时遍历的开销就越大, 造成设备识别的性能下降.

上述工作本质上是从不同的角度挖掘设备返回数据中与设备信息有关的文本模式, 然后将文本模式与设备信息一起构建标注规则, 虽然设备信息的获取可能是通过人工撰写的、自动化方式获取的或是依赖已有的数据集, 但最后规则的呈现方式都是相似的. 因此在实际应用中, 此类方法可以结合使用, 如 ARE 与 IoTTracker 结合能让生成的识别规则所覆盖的设备范围更广, 以达到更好的设备识别能力.

### 2.2 识别粒度

#### 2.2.1 多种设备信息识别

现有的基于主动探测的 IoT 设备识别方法几乎都是在设备信息量允许的前提下, 尽可能地进行细粒度的设备识别, 即识别出设备类型、设备制造商和设备产品名.

在基于规则的方法中, 通常是检查设备的原始数据中是否有能匹配规则中的正则表达式的子字符串, 若有, 则给该设备打上对应的设备信息标签. 注意, 这里的标签可能只含有单一设备信息 (如设备类型), 也可能含多种设备信息. 若原始数据匹配了多个标注规则, 则该设备被标注的设备信息通常也会更多. 不过当规则库非常庞大复杂,

设备信息也十分丰富时, 可能会因为误匹配而产生一些误标, 这也是基于规则的方法的缺陷之一. 在基于设备指纹的方法中, 通常将识别粒度划分为 3 个等级, 即仅识别设备类型、识别设备类型和制造商、或识别全部的 3 种设备信息. 识别设备类型作为最基本的识别粒度, 类别数较少, 且设备数据中有关类型的特征和信息量较多, 利用机器学习可以训练出性能良好的分类器. 对于第 2 等级的设备信息识别, 由于设备制造商数量繁多, 而且考虑到不同的设备制造商可能会使用相似的应用层协议实现, 会导致分类模型性能的显著下降. 而对于第 3 等级的设备信息识别, 由于设备名数量更多, 几乎无法针对所有 IoT 设备训练识别模型, 所以目前常用的方法主要有两种: 一种是对不同类型的 IoT 设备分别训练模型, 每个模型只负责对应类型设备的识别; 另一种是借鉴基于规则的方法, 即使用正则表达式来匹配设备名.

#### 2.2.2 单一设备信息识别

除了上述工作, 也有工作仅识别单一设备信息[56−58]. Holland 等人提出了主动识别网络设备制造商的通用方法[56]. 该方法结合了无监督和有监督两种机器学习方法. 在训练阶段, 使用基于文本的全新聚类方法生成一系列的类集, 对于每个类集, 通过人工查询 Google, Censys, Shodan 等, 为其打上标签并用于模型训练; 预测时先对数据进行特征提取, 然后使用训练好的模型来预测其制造商. 此方法在一定程度上解决了训练集的标注问题, 且同时保证了识别精度. 然而文中的总样本数仅为 16 万, 所包含的设备制造商数量也相对较少. 当样本规模扩大, 设备制造商数量也会随之增大, 不仅聚类的精度无法保证, 人工标注的工作量也会大大增加.

### 2.3 探测粒度

#### 2.3.1 基于单一协议的设备识别

上述提到的大部分工作都是基于单一协议的[46,51−56,59], 即对于某个待识别的设备, 仅使用了从该设备某一开放端口探测到的应用层数据来进行设备识别, 识别对象精确到 IP 地址+端口. 通常的做法是: 对于某一 IP 的某个端口, 探测其对应的应用层协议数据, 再利用基于设备指纹或者基于规则的方法进行设备识别. 这样做的优势在于: 首先, 对于大范围的网络仅需要针对单端口的一次探测, 就可以根据返回数据, 识别出大量的 IoT 设备; 其次, 部分设备可能是通过路由器端口映射来与外界进行通信, 精确到 IP 地址+端口的识别对象可以保证识别的有效性. 劣势在于: 基于单一协议信息有时候并不能有效进行设备识别, 例如, 对于某一设备, 其完整设备信息可能分散在多个不同端口的不同应用层协议下, 仅利用某一端口的信息无法进行有效的设备识别.

#### 2.3.2 基于多协议的设备识别

为了解决基于单一协议的设备识别方法的不足, 一些工作提出了基于多协议的设备识别方法[57,60]. Wang 等人提出了 FDI[57], 通过聚合多个不同的分类器, 以一种迭代的方式来融合多个端口的信息取代直接整合的方法来进行更高精度的识别. 具体地, FDI 的数据收集器针对一个端口进行设备原始数据收集, 然后交付给对应的端口数据分类器, 分类器将结果传输给决策器, 如果某些设备的分类可信度没有超过既定阈值, 决策器将调度数据收集器收集这些设备下一个端口的原始数据, 并与上一分类器的输出合并传递给下一个端口数据分类器, 迭代直至分类可信度超过阈值或者扫描完既定端口列表. 该方法存在的问题是, 预先设定的端口列表在一定程度上直接决定了 FDI 对于服务开放在非常用端口上的 IoT 设备没有识别能力, 而如果 FDI 需要扩展到非常用端口, 则需要考虑这些端口开放的不同协议问题. 虽然 Yu 等人提出利用强化学习的方法来训练并获得待扫描的端口列表[60]解决了上述的端口列表设置问题, 但依然存在非常用端口的协议多样性问题.

综上所述, 基于机器学习的方法性能大部分要略好于基于规则的方法. 然而数据集的获取, 新设备的识别等问题需要未来更多的研究工作. 基于多协议的设备识别方法相对于基于单一协议的方法有识别准确度高、可信度高等优势[61]. 然而仍存在许多待解决的问题, 如多协议数据的融合方式、端口探测的方案、非常用端口对应的应用层协议识别等, 都需要更深入的研究和探索. 基于主动探测的 IoT 设备识别工作的总结如后文表 2 所示.

### 2.4 数据集

考虑到主动探测场景的特殊性, 目前为研究人员提供的公开数据集只有 Censys[59]的研究者数据集. 该数据集包含了每天 IPv4 全网大量端口的服务数据以及少量的 IoT 设备标签, 并且在持续更新. 数据集包含的 IoT 设备数

量大概在 340 万左右, 标注粒度为设备类型、设备制造商和设备名. 该数据集的标注由 Censys 提供的专家规则生成, 虽然对大部分 IoT 设备的标注都较为准确, 但在少数情况下, 对于同一个 IP, Censys 会将其打上完全不同的设备标签. 在使用设备标签时, 需要按需进行数据清洗. 不过总体来说, Censys 还是为广大研究人员, 特别是资源有限无法进行大范围主动探测的研究人员提供了非常宝贵的主动探测数据和较为准确的设备标签.

表 2 基于主动方法的 IoT 设备识别

| 大类 | 细分类别 | 识别粒度 | 探测粒度 | 数据集 | 识别效果 (Acc) (%) |
|---|---|---|---|---|---|
| 基于规则 | 基于正则表达式匹配[53] | ○ /Δ/ □ | 单协议 | — | — |
| | 基于外部数据的自动化规则生成[54] | ○ /Δ/ □ | 单协议 | Censys[59], 自探测数据 | 95–98 |
| | 基于相似度计算[55] | ○ /Δ/ □ | 单协议 | 自探测数据, ARE标注[54] | 93–98 |
| 基于机器学习 | 基于二分类模型[51,52] | ○ /Δ | 单协议 | Censys[59], Shodan, 自探测数据 | 96–99 |
| | 基于多分类模型[15,46−50,56,57,60] | ○ /Δ | 单协议/多协议 | Censys[59], CCZ DNS 数据集, 自探测数据 | 92–99 |

注: 识别粒度列中, ○表示IoT设备类型, Δ表示IoT设备制造商, □表示IoT设备名. Acc表示准确率Accuracy

## 3 物联网设备异常检测

面向物联网设备的异常检测技术可以分为基于机器学习算法的检测方法和基于行为规范的规则匹配方法, 其总体分类结构如图 5 所示. 在通用方法的基础上, 面向物联网设备的流量异常检测方法结合物联网设备独有的通信特点, 对所采用的技术体系和部署场景进行定制化的设计. 随着机器学习技术的快速发展, 传统的有监督机器学习、深度学习等各种机器学习技术被广泛应用于物联网设备的异常检测中. 在基于行为规范的规则匹配方法中, 已有的工作采用不同数据源提取物联网设备的正常行为规范的描述, 且形式化验证方法被广泛应用.

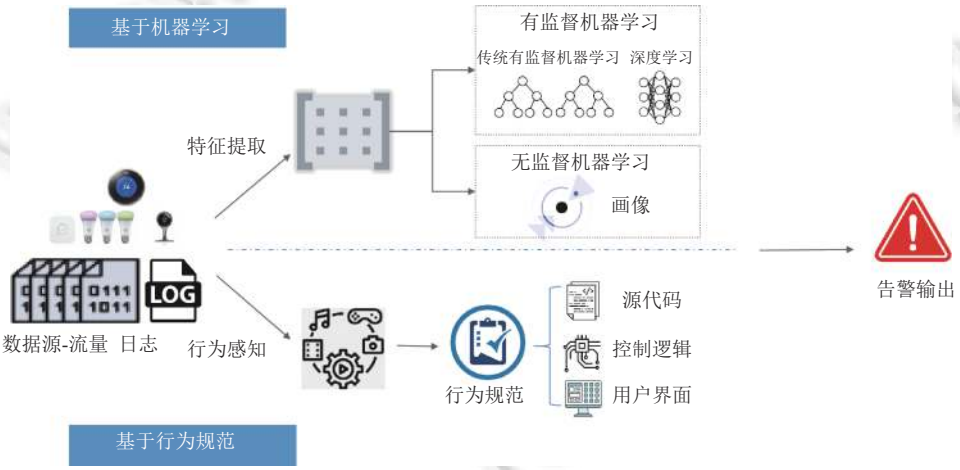


图 5 物联网设备异常检测技术

### 3.1 基于机器学习算法的检测方法

基于机器学习的异常检测算法根据是否依赖于有标签数据可以分为有监督学习和无监督学习算法, 根据检测的目标异常类型, 面向不同的场景通常采用不同的机器学习模型.

#### 3.1.1 基于有监督机器学习的检测方法

针对已知的特定单一异常的检测系统主要基于有监督机器学习算法, 即将异常检测视作分类问题, 收集某种特定的异常情况下所产生的流量样本和正常流量样本构成有标注的数据集来训练机器学习分类器. 有监督机器学

习算法的理论依据在于设备正常流量和由恶意行为产生的异常流量在流量统计特征上会有不同的概率分布, 对于一组流量样本, 可以根据特征判断其具有更高概率所属的类别, 机器学习算法能够基于一定的模型假设拟合出样本属于不同类别的决策边界, 从而根据样本与决策边界的关系判断类别.

在有监督的机器学习算法中, 常常将基于统计的机器学习算法应用到异常检测[62−64], 如 Birnbach 等人设计了名为 Peeves 的系统, 专门用于对传感器设备所报告的物理事件的真实性进行验证[62], 攻击者可以产生虚假的物理事件报告让设备做出错误的响应. Peeves 系统以智能家居应用中各传感器的实时数据为输入, 采用 SVM 来判断触发系统响应的物理事件的真实性. Bhatt 等人设计了名为 HADS 的混合机器学习方式的检测系统, 其中基于有监督的机器学习模型采用高斯混合模型和孤立森林, 对物联网设备产生的具有不同特点的时间序列进行异常检测[63]. IoTArgos[64]采用了两阶段异常检测算法, 其中一阶段采用 5 种计算量小的机器学习分类算法来检测和过滤一个攻击子集, 以平衡入侵检测性能和系统消耗, 如资源有限的家庭路由器的 CPU 和内存成本.

与传统的机器学习算法相比, 基于有监督的深度学习方法凭借其对数据特征的强大提取能力, 往往能够实现更高的检测准确率. DÏoT[65]针对每个设备的流量模型分别进行建模, 对其报文进行特征提取和处理. 然后采用 RNN 预测下一个报文的出现概率, 根据概率阈值决定是否产生异常告警. 这种建模方式能够充分地利用单个物联网设备功能单一、通信模式简单的特点, 取得更好的检测性能, 且具备多域协同建模的功能, 以应对设备软件固件更新带来的检测效果下降的问题. 这种多域协同的异常检测算法正受到越来越多的关注, 具有相似工作环境的设备可以共享威胁情报, 同时也能增加用于模型训练所需的数据规模[66,67]. Alaiz-Moreton 等人针对物联网常用协议 MQTT 设计了基于多分类的攻击流量检测算法[68], 该工作采集了物联网设备的正常流量以及 DDoS 等 3 种攻击流量, 并使用 XGBoost 及 4 种循环神经网络对流量样本进行分类, 从而实现对攻击流量的检测.

3.1.2 基于无监督机器学习的检测方法

物联网设备所面临的攻击平面较为广泛, 为了降低部署和维护的开销, 人们希望构建出通用且能够检测出多种异常以及未知异常的系统. 考虑到物联网设备的功能通常十分简单, 一些已有的方法尝试采用无监督机器学习算法, 仅使用设备产生的正常流量数据集进行零正例训练, 构建出描述物联网设备的正常通信行为的模型, 并将所有偏离了正常画像的网络流量视为异常. 这类方法不针对检测特定的异常类型, 从而不需要获取有标注的各类异常数据的样本, 也能够检测出未知的异常. 这种方法的理论依据在于物联网设备由于其功能和使用方式的限制, 其正常流量在各类特征上仅占数值空间的小部分区域, 而区域的边界可以通过机器学习算法来拟合.

同样的, 无监督的机器学习算法中常常应用传统的基于统计的机器学习算法如聚类和离群点检测算法. Hamza 等人[69]在 SDN 场景下基于物联网设备的 MUD 规范文档设计了用于检测洪泛式拒绝服务攻击的算法, 该算法主要考虑每条通信流的报文数量和总的流量规模特征, 对流量样本进行聚类, 并基于时序关系和马尔科夫模型构建聚类簇之间的转移关系, 将离群点和转移失败的序列作为异常. Santos 等人[70]设计了针对基于 5G 低功耗广域网的智慧城市应用的异常检测系统, 采用离群点检测和隔离森林的无监督机器学习算法来检测 IoT 设备的应用数据. IoTArgos[64]则是在异常检测的第 2 阶段采用了无监督的离群点检测算法, 将与已知的正常通信模式不同的流量视作新的网络攻击类型, 用于在网关处部署的针对整个网络内的所有流量进行异常检测.

还有一些研究[71−73]将深度学习模型应用到了异常检测算法中. 如 Li 等人[71]针对拥有大量网络传感器和执行器的复杂网络物理系统 (CPS), 使用 LSTM-RNN 捕捉其正常的多变量时间序列, 并提出一种基于对抗生成网络 (GAN) 的异常检测方法来区分一个复杂的 6 级安全水处理 (SWaT) 系统的异常攻击情况和正常工作条件. Kitsune[72]则是一个基于深度神经网络的通用入侵检测系统, 它提取报文的一些基本特征和统计量, 利用多个层叠的自编码器模型对映射之后的特征向量进行重建, 并告警那些重建误差超过一定阈值的报文. Meidan 等人则是提取了流量的多维时空统计特征, 并采用深度自编码器模型来检测物联网设备发出的僵尸网络流量[73].

已有的基于机器学习方法通常在实验室评估环境下能够取得卓越的效果. 然而, 现有的不少研究工作对所设计的异常检测系统进行评估时都只涵盖了部分较为常见的异常现象, 在真实场景下的检测性能还有待评估. 另一方面, 很多机器学习算法都依赖于输入数据与预测目标在训练阶段和预测阶段遵从独立同分布的假设. 目前已有的基于机器学习算法的物联网设备异常检测技术, 其训练过程和检测验证过程都是基于在一段较短的时间范围内

收集的数据集, 以此得到的评估结果并不能充分证明这些异常检测系统在长时间的持续运行中能够始终保持较高的检测性能[74]. 已有的针对物联网设备而设计的异常检测系统对物联网设备所独有的行为演进特点和长时间尺度下的性能评估都还关注不够, 有待进一步的研究工作进行探索.

### 3.2 基于行为规范的规则匹配方法

物联网设备通常功能较为单一, 运行逻辑较为简单, 因此可以通过精细化构建设备的通信行为规范, 将设备的正常运行逻辑表示为一系列规则, 以此为基准进行规则匹配, 这类方法的理论依据在于可以通过逻辑和语义规则来描述物联网设备的运行逻辑, 这些规则能够从不同数据源中获得, 并用于和实时观测到的物联网设备行为进行比对. 在进行规则匹配时, 系统需要实时感知物联网设备的工作状态及其变更情况, 目前已有的研究工作中尝试从多种不同的数据源中来完成对设备状态的监控, 包括设备控制逻辑、源代码、用户界面描述和日志等.

#### 3.2.1 基于良性模型匹配的检测方法

这类方法将设备的规范行为抽象为设备在正常状态之间动态地运行. 具体地来说, 通过状态转移机, 交互图等模型来刻画设备正常的行为顺序, 结合动态运行环境, 用户部署策略等其他信息, 构造良性模型来刻画设备的规范行为模式. 在真实环境下, 采集设备通信流量并对其特征分析, 获取对应的事件或命令发生顺序, 从良性模型的初始状态开始进行匹配, 判断是否符合设备的正常运行逻辑.

Orpheus 设计工业控制场景下针对物联网设备面向数据的攻击的检测和防御方法[75]. 其通过分析设备的控制程序构建事件感知的有限状态自动机来表示设备的行为规范, 并使用事件检查来发现物理事件是否符合模型所描述的规范, 对异常的事件产生告警. Yu 等人提出对物联网设备的行为进行细粒度建模和策略验证的方法, 其也采用自动机模型表示和协议相关的设备行为和状态变迁的规范[76]. 此外还有不少工作关注多设备之间的协作关系, 如应用定义的跨设备触发响应规则. HoMonit[77]和 IoTGaze[78]是两个十分相似的系统, 它们都是针对三星的 SmartThings 平台所设计. 这两个系统首先都对 SmartApp 源代码或 UI 界面进行静态分析, 之后根据结果构建 DFA 模型来拟合设备的行为规范. 这两个系统能够有效检测出设备工作环境的上下文相关的异常, 如事件欺骗、设备越权、命令失效、设备故障等. 最后还有一类工作采用形式化验证的方法来检测部署策略中潜在的风险和攻击向量. IoTSafe 关注联动的物联网设备通过物理信道产生的交互风险, 基于交互图设计了策略规划表示和检查的算法, 并在三星 SmartThings 平台上进行了原型系统实现和验证[79].

#### 3.2.2 基于关联规则/策略匹配的检测方法

这类方法根据触发事件和响应动作之间的因果关系, 将设备的行为规范抽象成语义规则或执行策略, 并且通过语义求解器或语义分析方法如自然语言处理, 分析设备的真实场景下的行为是否符合关联规则.

Wang 等人采用形式化验证的方法对物联网平台中所设置的触发响应规则进行分析, 检查不同规则之间是否存在冲突或可能造成安全风险的情况[80]. IoTC$^2$[81]和 IoTSAT[82]具有类似功能的系统. 这些工作基于策略分析处理器与可满足理论求解器验证现有的设备配置不会产生潜在的冲突或风险. HAWatcher 基于应用化的智能家居设备的事件日志和语义信息来检测智能家居系统中的事件流中的上下文异常和因果关系异常[83]. 总之, 现有的工作已经探索了通过不同数据源面向不同的安全风险提取和验证设备行为规范的算法.

对于基于设备行为规范提取的异常检测算法能对设备的工作过程进行有效的监控. 然而, 目前的很多研究工作是针对特定的物联网平台而设计的规则提取算法, 例如三星的 SmartThings 智能家居平台常用于原型系统验证[77−79]. 这些基于规则的检测算法尽管从方法论的角度来说具有在不同平台之间的可迁移性, 但是这种迁移通常也会引入较大的开销. 以 SmartThings 平台为例, 对于 APP 和 UI 界面的静态分析会因为不同平台的异构性如不同的描述语言和平台框架而失效, 而适配跨平台的差异意味着较大的研发投入.

综上所述, 基于机器学习算法的异常检测方法结合物联网设备独有的通信特点、所采用的技术体系和部署场景进行定制化的设计. 而基于行为规范的规则匹配方法通过提取物联网设备的正常行为规范来检测异常, 各种方法的总结如表 3 所示.

表 3 物联网设备异常检测

| 大类 | 细分类别 | | 检测方法 | 数据源 | 检测效果 (Acc) (%) |
|---|---|---|---|---|---|
| 基于机器学习 | 有监督机器学习 | 传统有监督机器学习 | 线性支持向量机[62] | 网络流量 | 99 |
| | | | 高斯混合模型, 孤立森林等[63] | 网络流量 | 96–98 |
| | | | K近邻, 逻辑回归, 朴素贝叶斯, 随机森林等[64] | 网络流量 | 78–89 |
| | | 神经网络 | RNN, LSTM, GRU[68] | 网络流量 | 93–96 |
| | | | GRU[65] | 网络流量 | 95 |
| | 无监督机器学习 | 传统机器学习方法 | 高斯混合模型等[69] | 网络流量 | 94–97 |
| | | | 离群点检测, 隔离森林等[64,70] | 应用数据[70], 网络流量[64] | 92–98 |
| | | 神经网络 | 自编码器[72,73] | 网络流量 | 98–99 |
| | | | 生成对抗网络[71] | 网络流量 | 90–94 |
| 基于行为规范 | 基于良性模型匹配的检测方法 | | 有限状态自动机[75−78] | 源代码或UI界面 | 98–99 |
| | | | 交互图[79] | 日志, 用户管理配置 | 96 |
| | 基于关联规则/策略匹配的检测方法 | | 策略分析和处理器[80,81]<br>可满足性理论(SMT)求解器[82] | IoT设备的设置 | 82–97 |
| | | | 影子执行引擎[83] | 事件日志 | 77–100 |

### 3.3 数据集

评估物联网设备异常检测系统的性能需要具有代表性的数据集. 当前研究社区中已经存在一定的公开数据集. Meidan 等人发布了他们针对正常物联网设备流量和僵尸网络流量所提取的多维流量特征数据集[73]. Hamza 等人发布了包含多种洪泛式拒绝服务攻击和设备正常流量的原始流量数据集, 并提供了报文级别的标注[69]. Alaiz-Moreton 等人公开了一组采用 MQTT 协议的物联网设备的正常流量数据和攻击流量数据集, 攻击数据集包含拒绝服务攻击、中间人攻击和网络入侵 3 种类型的攻击[68]. Kitsune 的作者为了评估其所构建的通用入侵检测系统的性能搭建了一个真实的物联网环境, 并公布其中采集的正常设备流量和注入的多种攻击流量, 包括扫描类、洪泛类、中间人攻击和僵尸网络流量等[72]. 除了这些流量数据集外, 对物联网设备构成的大型僵尸网络进行测量的工作也会公布其所采集的针对物联网设备的恶意软件样本, 如 Mirai[3]和 Hajime[4]. Alrawi 等人对物联网设备恶意软件生态的大规模测量也公布了一系列针对物联网设备的恶意软件样本[84].

## 4 研究展望

随着 IoT 设备的广泛应用, IoT 设备管理和异常检测受到了越来越多的关注, 虽然 IoT 设备识别和异常检测取得了一定的研究成果, 但在真实场景中应用还存在许多挑战. 通过前文对当前物联网设备识别和异常检测主要工作的分析, 本节对该领域的现存问题和未来研究趋势加以阐述.

### 4.1 物联网设备识别应用于真实网络环境的挑战

虽然现有的基于被动方法的物联网设备识别方案能到达较高的识别精度, 但应用在真实场景中还存在很多挑战, 这是因为真实的网络是一个动态开放的环境. 其动态性体现在随着时间的推移, 新的 IoT 设备会不断加入, 模型应具备识别新类型设备并不断更新的能力, 而现有的大多数解决方案未考虑到新类型设备加入的问题. 开放性体现在网络中会有各种干扰流量如扫描流量的存在, 这些干扰流量会对设备正常工作的流量造成一定影响, 从而影响设备识别精度. 因此, 针对这些问题, 在设计 IoT 设备识别方案时应充分考虑新类型设备加入的情况以及模型更新的机制, 并对有干扰流量影响下模型识别精度进行评估. 此外, 现有的大多数被动识别方法是针对局域网环境设计的, 对更为复杂网络环境, 如 NAT 或 VPN 环境下如何准确识别 IoT 设备的研究还相对较少, 这一问题相对于局域网环境下的 IoT 设备识别难度更大, 值得研究.

对于基于主动方法的物联网设备识别方案来说, 其可靠性和全面性还存在一定问题. 对于可靠性, 基于主动探

测获取的设备数据十分庞杂, 现有的方法大都是基于单一协议的识别方法, 在数据质量较低, 噪声较多时, 其设备识别的可靠性无法保证, 如何有效去除噪声数据或者结合多协议信息来保证识别的可靠性是值得研究的问题. 另外, 在设备识别的全面性上, 现有方法几乎都是基于常用端口和协议来进行 IoT 设备等发现与识别. 然而, 相当一部分设备的应用层服务开放在非常用端口上[61]. 因此, 如何高效地发现只开放了非常用端口的 IoT 设备也是目前研究工作的挑战之一. 此外, 在 IPv6 网络下, 我们无法通过暴力扫描来遍历整个地址空间并进行设备发现, 高效地进行设备发现是主动方法的基础, 也是目前在 IPv6 网络空间下进行设备识别的主要挑战.

此外, 主被动的 IoT 设备识别方法部署于真实网络环境时, 还存在着设备识别时间和数据收集的挑战. 为每种设备单独建立一个二分类器通常会耗费更多的设备识别时间. 相比之下, 为所有设备类型建立统一的模型能够直接根据待识别设备的特征得到预测结果, 花费较少的设备识别时间. 对于数据收集来说, 现有的基于机器学习的物联网设备识别方法大多为有监督机器学习, 需要大量的有标签数据训练模型, 而收集标签通常会耗费较多的人力和时间. 因此, 如何基于半监督和无监督学习的方法降低人工开销并提高识别精度是值得研究的问题.

主被动的设备识别方案有各自的优点和缺点, 在真实的网络环境中可以相互配合、互为补充. 被动的设备识别方法不会对网络造成较大影响, 但应用在 NAT、VPN 或广域网等更为复杂的网络环境中时, 由于某个地址对应的流量可能是多种设备流量的混合, 因此进行设备精确识别会面临更大的挑战. 而主动方法能够应用的范围不仅局限于局域网, 还可以在广域网中进行设备识别, 因此适用范围更广, 但主动方法会对网络造成额外的负担, 尤其是需要进行新设备识别时, 需要重新对网络进行扫描, 会带来较大开销. 因此, 主被动的设备识别方法可配合使用, 发挥各自的优点, 在扩大识别范围的同时减小对网络带来的开销.

### 4.2 物联网设备异常检测在通用性、可扩展性和可维护性方面的挑战

虽然 IoT 设备异常检测引起了更多的关注并涌现出一系列的研究成果, 但在通用性、可扩展性和可维护性方面仍存在许多挑战.

通用性的挑战体现在很多工作都基于人工提取的流量特征和机器学习模型来训练异常检测系统, 其中很多流量特征都和特定的协议或通信技术相关. 应用于不同领域的物联网设备通常会采用不同的通信协议和技术. 已有的物联网设备流量异常检测系统都基于某一种特定的通信技术 (如 TCP/IP 协议栈和低功耗无线个域网协议 ZigBee) 所设计, 难以被直接迁移到使用其他不同通信技术体系的物联网设备. 但与此同时, 物联网设备功能单一和通信行为存在较为固定的重复模式的特征为设计和实现通用的或可迁移的异常检测算法提供了可能. 异常检测算法可以尝试基于通用的流量固有特征进行分析建模, 例如所有的分组交换通信技术产生的通信流量都会存在单个报文长度的体量特征, 连续的报文序列之间能够提取出时序特征. 一些进行设备级指纹和事件级指纹的研究工作已经证明了这些简单的固有流量特征所具备的强大的表征能力[85−87]. 未来的工作可以探索基于具有可迁移性的简单固有特征建立精细化的流量模型, 使得所设计出的异常检测系统具有通用性.

在可扩展性和可维护性方面, 异常检测系统在运行过程中难免会出现误报和漏检的案例. 当误报和漏检的案例被证实时, 网络管理员通常希望系统能够从这些案例中学习, 进一步提升系统的检测性能, 避免相同的错误再次出现. 已有的方法对系统在完成训练投入部署运行之后的优化和维护缺少关注, 在实际运行过程中可能会不断产生重复的错误告警或漏检, 给网络管理员造成困扰. 另外, 现有的 IoT 异常检测模型也缺少长时间尺度下模型更新的考虑, 物联网设备的使用场景通常与人们的生产和生活行为密切相关, 其自身的通信行为也会随着用户习惯及物理环境 (如温度、天气和季节等) 的变化而发生迁移, 这就要求异常检测系统能够及时感知并适应这些变化, 更新自身对正常行为与异常行为的判断标准, 在长期的运行过程中始终保持较高的检测性能. 然而, 已有的异常检测系统几乎都是在一段较短的时间内所采集的数据集上进行训练和测试, 没有充分考量物联网设备在使用过程中的行为演进对异常检测系统的影响, 也缺少对系统在较长的时间尺度下持续运行的检测性能的评估. 未来研究可考虑终生检测目标, 目前国内外已有的工作中在这方面都还缺乏较为深入的研究, 未来的研究工作可以尝试从机器学习领域应对概念漂移问题借鉴相关思想应用到物联网设备的异常检测系统中, 进一步提升系统的可用性和长时间尺度下的性能. 最后, 考虑到真实网络环境中新的 IoT 设备会不断加入, 应将 IoT 设备识别和异常检测技术相结

合, 从设备识别得到的结果作为异常检测系统的输入, 如果发现新的 IoT 设备, 需要针对其构建异常检测模型, 以保证 IoT 异常检测系统能够覆盖到网络中新的 IoT 设备.

### 4.3 物联网设备识别和异常检测的可解释性的挑战

现有的很多物联网设备识别和异常检测工作都使用了机器学习模型, 该类方法也是目前的研究热点. 机器学习模型能够构建输入到输出的复杂映射, 因而具有很强的数据拟合能力, 具有识别精度高的优点, 在各个领域都得到了广泛应用. 但这些模型的可解释性却存在一定问题, 人们无法理解机器学习模型的决策过程以及输出结果的判断依据. 对于设备识别来说, 管理员无法得知设备被划分到某一类的原因. 而在异常检测的问题中, 异常检测系统输出的告警通常还需要网络管理员进行进一步的验证和响应, 已有的基于机器学习模型的异常检测系统通常会提取大量高度集成的统计流量特征, 当系统产生告警时, 网络管理员无从得知系统将流量判定为异常的依据, 从而难以对其进行验证和采取相应的响应措施. 研究 IoT 设备识别和异常检测模型的可解释性有助于判别并减轻模型引起的偏差、增进人类对模型的信任和发现新的领域知识. 此外, 由于很多机器学习模型, 如随机森林、深度学习等方法相当于一个“黑盒子”, 因此管理员无法理解模型根据输入得到相应预测值的原因, 这样会大大降低管理员对模型的信任度, 不利用基于机器学习的模型在设备识别和异常检测领域的广泛应用和部署. 因此, 对于 IoT 设备识别和异常检测的可解释性的研究是非常必要的.

在 IoT 设备识别和异常检测模型的数据集中可能会存在偏差, 这是因为用于训练的数据规模有限, 不能代表所有数据, 或者数据收集过程会引入潜在的偏差. 此时, 进行可解释性的研究、分析设备错分的原因或者异常检测判断错误的原因有助于发现数据或模型中潜在的问题, 对提取的特征或模型进行调整.

通过可解释性分析各种因素之间的相关性, 还有助于发现新的知识. 比如在异常检测领域, 可以通过深度学习模型发现未知异常, 并通过对异常的解释发现异常样本和正常流量样本之间的偏差, 从而发现新的攻击方式.

### 4.4 数据集带来的挑战

数据集对于评估设备识别和异常检测方法尤为重要, 有助于公平对比模型和发现模型存在的问题.

对于 IoT 设备识别来说, 当前 IoT 设备识别的数据集相对较小, UNSW 数据集含有 20 多种 IoT 设备, Yourthings 数据集含有 40 多种 IoT 设备, 建立更大规模的数据集有利于对设备识别方法进行更有效的评估. 更大规模一方面体现在 IoT 设备数量上, 另一方面是 IoT 设备类型具有多样性, 应包含多种厂商的设备以及同厂商不同功能的设备或同厂商相似功能不同型号的设备. 对于同厂商相同型号的设备, 还应包含不同配置下采集的设备流量, 以评估不同配置对于设备识别带来的影响. 此外, 考虑到真实网络环境下会有干扰流量, 如扫描流量存在, 应收集较长时间内设备流量或在设备流量采集过程中人为注入干扰流量以模拟真实网络环境. 除了 IoT 设备, 真实网络环境中还具有大量的非 IoT 设备, 因此数据集中的非 IoT 设备数量和类型数应达到一定量级, 非 IoT 设备应包含多种厂商、多种型号、多种操作系统和应用软件的台式计算机、笔记本电脑、平板电脑和手机等. 局域网中收集的流量可以用于局域网环境下设备识别的评估, 除了局域网环境, 构建更为复杂的网络环境, 比如 NAT 环境或 VPN 环境中的数据集有助于研究 IoT 被动识别方法应用于更大范围的网络环境. 在这种情况下, 如何对设备经过 NAT 或 VPN 后的流量进行标注显得尤为重要, 因为设备流量经过 VPN 后由于被加密难以从协议上进行区分.

对于 IoT 异常检测的数据集来说, 正如目前的研究工作的局限性一样, 已有的流量数据集多是在一段较短的时间内采集的, 其中的攻击流量与设备异常行为多为人为注入. 为了衡量异常检测系统, 尤其是物联网设备流量异常检测系统在长时间尺度下的性能, 需要采集设备在真实用户的日常使用中产生的流量. 除此之外, 设备的配置不同和软件固件更新对设备所产生的流量带来的影响目前也缺少对真实数据的采集和分析. 未来的工作也可以尝试从构建包含这些因素在内的数据集来对社区做出贡献.

## 5 总 结

物联网技术的飞速发展使其广泛应用于智能家居、智慧城市、车联网和工业互联网等生产和生活的各个领域, 但物联网设备种类和接入方式的多样性也带来了设备资产管理和安全管理方面的问题, 因此物联网设备识别

和异常检测成为研究的热点. 本文系统地梳理了被动和主动的物联网设备识别方法以及异常检测方面的相关工作, 阐明了其面临的挑战和未来发展方向, 期望能够对未来该领域相关研究工作提供参考和指引帮助.

**References:**


[1] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2347–2376. [doi: 10.1109/COMST.2015.2444095]

[2] Torchia M, Shirer M. IDC forecasts worldwide technology spending on the Internet of Things to reach $1.2 trillion in 2022. 2018. https://apnews.com/press-release/pr-businesswire/da5501b627d14cc4bd8b2090b266e8e5

[3] Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, Durumeric Z, Halderman JA, Invernizzi L, Kallitsis M, Kumar D, Lever C, Ma ZE, Mason J, Menscher D, Seaman C, Sullivan N, Thomas K, Zhou Y. Understanding the Mirai Botnet. In: Proc. of the 26th USENIX Conf. on Security Symp. Vancouver: USENIX Association, 2017. 1093–1110.

[4] Herwig S, Harvey K, Hughey G, Roberts R, Levin D. Measurement and analysis of Hajime, a peer-to-peer IoT Botnet. In: Proc. of the 2019 Network and Distributed Systems Security Symp. San Diego: ISOC, 2019. 1–15. [doi: 10.14722/ndss.2019.23488]

[5] Soltan S, Mittal P, Poor HV. BlackIoT: IoT Botnet of high wattage devices can disrupt the power grid. In: Proc. of the 27th USENIX Conf. on Security Symp. Baltimore: USENIX Association, 2018. 15–32.

[6] Tahaei H, Afifi F, Asemi A, Zaki F, Anuar NB. The rise of traffic classification in IoT networks: A survey. Journal of Network and Computer Applications, 2020, 154: 102538. [doi: 10.1016/j.jnca.2020.102538]

[7] Liu YX, Wang J, Li JQ, Niu ST, Song HB. Machine learning for the detection and identification of Internet of Things devices: A survey. IEEE Internet of Things Journal, 2022, 9(1): 298–320. [doi: 10.1109/jiot.2021.3099028]

[8] Mazhar N, Salleh R, Zeeshan M, Hameed MM. Role of device identification and manufacturer usage description in IoT security: A survey. IEEE Access, 2021, 9: 41757–41786. [doi: 10.1109/access.2021.3065123]

[9] Lear E, Droms R, Romascanu D. Manufacturer usage description specification. 2019. https://www.rfc-editor.org/rfc/rfc8520.html

[10] Meidan Y, Bohadana M, Shabtai A, Guarnizo JD, Ochoa M, Tippenhauer NO, Elovici Y. ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis. In: Proc. of the 2017 Symp. on Applied Computing. Marrakech: ACM, 2017. 506–509. [doi: 10.1145/3019612.3019878]

[11] Bremler-Barr A, Levy H, Yakhini Z. IoT or not: Identifying IoT devices in a short time scale. In: Proc. of the 2020 IEEE/IFIP Network Operations and Management Symp. Budapest: IEEE, 2020. 1–9. [doi: 10.1109/noms47738.2020.9110451]

[12] Martin J, Rye E, Beverly R. Decomposition of MAC address structure for granular device inference. In: Proc. of the 32nd Annual Conf. on Computer Security Applications. Los Angeles: ACM, 2016. 78–88. [doi: 10.1145/2991079.2991098]

[13] Alexander S, Droms R. DHCP options and BOOTP vendor extensions. 1997. https://tools.ietf.org/rfc/rfc2132.txt [doi: 10.17487/rfc1533]

[14] Sivanathan A, Gharakheili HH, Loi F, Radford A, Wijenayake C, Vishwanath A, Sivaraman V. Classifying IoT devices in smart environments using network traffic characteristics. IEEE Trans. on Mobile Computing, 2019, 18(8): 1745–1759. [doi: 10.1109/tmc.2018.2866249]

[15] Guo H, Heidemann J. Detecting IoT devices in the Internet. IEEE/ACM Trans. on Networking, 2020, 28(5): 2323–2336. [doi: 10.1109/tnet.2020.3009425]

[16] Hu GN, Fukuda K. Toward detecting IoT device traffic in transit networks. In: Proc. of the 2020 Int'l Conf. on Artificial Intelligence in Information and Communication. Fukuoka: IEEE, 2020. 525–530. [doi: 10.1109/icaiic48513.2020.9065229]

[17] Saidi SJ, Mandalari AM, Kolcun R, Haddadi H, Dubois DJ, Choffnes D, Smaragdakis G, Feldmann A. A haystack full of needles: Scalable detection of IoT devices in the wild. In: Proc. of the 2020 ACM Internet Measurement Conf. ACM, 2020. 87–100. [doi: 10.1145/3419394.3423650]

[18] Mazhar MH, Shafiq Z. Characterizing smart home IoT traffic in the wild. In: Proc. of the 5th IEEE/ACM Int'l Conf. on Internet-of-Things Design and Implementation (IoTDI). Sydney: IEEE, 2020. 203–215. [doi: 10.1109/iotdi49375.2020.00027]

[19] Ma XB, Qu J, Li JF, Lui JCS, Li ZH, Guan XH. Pinpointing hidden IoT devices via spatial-temporal traffic fingerprinting. In: Proc. of the 2020 IEEE Int'l Conf. on Computer Communications (INFOCOM). Toronto: IEEE, 2020: 894–903. [doi: 10.1109/infocom41043.2020.9155346]

[20] Sivanathan A, Sherratt D, Gharakheili HH, Radford A, Wijenayake C, Vishwanath A, Sivaraman V. Characterizing and classifying IoT traffic in smart cities and campuses. In: Proc. of the 2017 IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS). Atlanta: IEEE, 2017. 559–564. [doi: 10.1109/infcomw.2017.8116438]

[21] Bezawada B, Bachani M, Peterson J, Shirazi H, Ray I, Ray I. IotSense: Behavioral fingerprinting of IoT devices. arXiv:1804.03852,

2018.

[22] Hamad SA, Zhang WE, Sheng QZ, Nepal S. IoT device identification via network-flow based fingerprinting and learning. In: Proc. of the 18th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications/the 13th IEEE Int'l Conf. on Big Data Science and Engineering. Rotorua: IEEE, 2019. 103–111. [doi: 10.1109/trustcom/bigdatase.2019.00023]

[23] Msadek N, Soua R, Engel T. IoT device fingerprinting: Machine learning based encrypted traffic analysis. In: Proc. of the 2019 IEEE Wireless Communications and Networking Conf. Marrakesh: IEEE, 2019. 1–8. [doi: 10.1109/wcnc.2019.8885429]

[24] Skowron M, Janicki A, Mazurczyk W. Traffic fingerprinting attacks on Internet of Things using machine learning. IEEE Access, 2020, 8: 20386–20400. [doi: 10.1109/access.2020.2969015]

[25] Shahid MR, Blanc G, Zhang ZH, Debar H. IoT devices recognition through network traffic analysis. In: Proc. of the 2018 IEEE Int'l Conf. on Big Data (Big Data). Seattle: IEEE, 2018. 5187–5192. [doi: 10.1109/bigdata.2018.8622243]

[26] Aksoy A, Gunes MH. Automated IoT device identification using network traffic. In: Proc. of the 2019 IEEE Int'l Conf. on Communications (ICC). Shanghai: IEEE, 2019. 1–7. [doi: 10.1109/icc.2019.8761559]

[27] Bao JQ, Hamdaoui B, Wong WK. IoT device type identification using hybrid deep learning approach for increased IoT security. In: Proc. of the 2020 Int'l Wireless Communications and Mobile Computing (IWCMC). Limassol: IEEE, 2020. 565–570. [doi: 10.1109/iwcmc48107.2020.9148110]

[28] Acar A, Fereidooni H, Abera T, Sikder AK, Miettinen M, Aksu H, Conti M, Sadeghi AR, Uluagac S. Peek-a-boo: I see your smart home activities, even encrypted! In: Proc. of the 13th ACM Conf. on Security and Privacy in Wireless and Mobile Networks (WiSec). Linz: ACM, 2020. 207–218. [doi: 10.1145/3395351.3399421]

[29] Miettinen M, Marchal S, Hafeez I, Asokan N, Sadeghi AR, Tarkoma S. IoT SENTINEL: Automated device-type identification for security enforcement in IoT. In: Proc. of the 37th IEEE Int'l Conf. on Distributed Computing Systems (ICDCS). Atlanta: IEEE, 2017. 2177–2184. [doi: 10.1109/icdcs.2017.283]

[30] Meidan Y, Bohadana M, Shabtai A, Ochoa M, Tippenhauer NO, Guarnizo JD, Elovici Y. Detection of unauthorized IoT devices using machine learning techniques. arXiv:1709.04647, 2017.

[31] Song YB, Huang Q, Yang JJ, Fan M, Hu AQ, Jiang Y. IoT device fingerprinting for relieving pressure in the access control. In: Proc. of the 2019 ACM Turing Celebration Conf. Chengdu: ACM, 2019. 1–8. [doi: 10.1145/3321408.3326671]

[32] Perdisci R, Papastergiou T, Alrawi O, Antonakakis M. IoTFinder: Efficient large-scale identification of IoT devices via passive DNS traffic analysis. In: Proc. of the 2020 IEEE European Symp. on Security and Privacy (EuroS&P). Genoa: IEEE, 2020. 474–489. [doi: 10.1109/eurosp48549.2020.00037]

[33] Lopez-Martin M, Carro B, Sanchez-Esguevillas A, Lloret J. Network traffic classifier with convolutional and recurrent neural networks for Internet of Things. IEEE Access, 2017, 5: 18042–18050. [doi: 10.1109/ACCESS.2017.2747560]

[34] Bai L, Yao LN, Kanhere SS, Wang XZ, Yang Z. Automatic device classification from network traffic streams of Internet of Things. In: Proc. of the 43rd IEEE Conf. on Local Computer Networks (LCN). Chicago: IEEE, 2018. 1–9. [doi: 10.1109/lcn.2018.8638232]

[35] Sun JH, Sun K, Shenefiel C. Automated IoT device fingerprinting through encrypted stream classification. In: Proc. of the 15th EAI Int'l Conf. on Security and Privacy in Communication Networks. Orlando: Springer, 2019. 147–167. [doi: 10.1007/978-3-030-37228-6_8]

[36] Thangavelu V, Divakaran DM, Sairam R, Bhunia SS, Gurusamy M. DEFT: A distributed IoT fingerprinting technique. IEEE Internet of Things Journal, 2019, 6(1): 940–952. [doi: 10.1109/jiot.2018.2865604]

[37] Fan LN, Zhang SZ, Wu YC, Wang ZL, Duan CX, Li J, Yang JH. An IoT device identification method based on semi-supervised learning. In: Proc. of the 16th Int'l Conf. on Network and Service Management (CNSM). Izmir: IEEE, 2020. 1–7. [doi: 10.23919/cnsm50824.2020.9269044]

[38] Kamnitsas K, de Castro DC, Le Folgoc L, Walker I, Tanno R, Rueckert D, Glocker B, Criminisi A, Nori AV. Semi-supervised learning via compact latent space clustering. In: Proc. of the 35th Int'l Conf. on Machine Learning. Stockholm: MLResearch Press, 2018. 2464–2473.

[39] Marchal S, Miettinen M, Nguyen TD, Sadeghi AR, Asokan N. AuDI: Toward autonomous IoT device-type identification using periodic communication. IEEE Journal on Selected Areas in Communications, 2019, 37(6): 1402–1412. [doi: 10.1109/jsac.2019.2904364]

[40] Sivanathan A, Gharakheili HH, Sivaraman V. Inferring IoT device types from network behavior using unsupervised clustering. In: Proc. of the 44th IEEE Conf. on Local Computer Networks (LCN). Osnabrueck: IEEE, 2019. 230–233. [doi: 10.1109/LCN44214.2019.8990797]

[41] Zhang SZ, Wang ZL, Yang JH, Bai DB, Li FL, Li ZM, Liu XR. Unsupervised IoT fingerprinting method via variational auto-encoder and K-means. In: Proc. of the 2021 IEEE Int'l Conf. on Communications (ICC). Montreal: IEEE, 2021. 1–6. [doi: 10.1109/icc42927.2021.9500301]

[42] Sivanathan A, Gharakheili HH, Sivaraman V. Managing IoT cyber-security using programmable telemetry and machine learning. IEEE Trans. on Network and Service Management, 2020, 17(1): 60–74. [doi: 10.1109/tnsm.2020.2971213]

[43] Ortiz J, Crawford C, Le F. DeviceMien: Network device behavior modeling for identifying unknown IoT devices. In: Proc. of the 2019 Int'l Conf. on Internet of Things Design and Implementation (IoTDI). Montreal: ACM, 2019. 106–117. [doi: 10.1145/3302505.3310073]

[44] Dong SK, Li Z, Tang D, Chen JY, Sun MH, Zhang KH. Your smart home can't keep a secret: Towards automated fingerprinting of IoT traffic. In: Proc. of the 15th ACM Asia Conf. on Computer and Communications Security (ASIA CCS). Taipei: ACM, 2020. 47–59. [doi: 10.1145/3320269.3384732]

[45] Alrawi O, Lever C, Antonakakis M, Monrose F. SoK: Security evaluation of home-based IoT deployments. In: Proc. of the 2019 IEEE Symp. on Security and Privacy (SP). San Francisco: IEEE, 2019. 1362–1380. [doi: 10.1109/sp.2019.00013]

[46] Cheng H, Dong WY, Zheng Y, Lv B. Identify IoT devices through Web interface characteristics. In: Proc. of the 6th Int'l Conf. on Computer and Communication Systems (ICCCS). Chengdu: IEEE, 2021. 405–410. [doi: 10.1109/ICCCS52626.2021.9449258]

[47] Yang KT, Li Q, Sun LM. Towards automatic fingerprinting of IoT devices in the cyberspace. Computer Networks, 2019, 148: 318–327. [doi: 10.1016/j.comnet.2018.11.013]

[48] Lavrenovs A, Visky G. Investigating HTTP response headers for the classification of devices on the Internet. In: Proc. of the 7th IEEE Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE). Liepaja: IEEE, 2019. 1–6. [doi: 10.1109/AIEEE48629.2019.8977115]

[49] Lavrenovs A, Visky G. Exploring features of HTTP responses for the classification of devices on the Internet. In: Proc. of the 27th Telecommunications Forum (TELFOR). Belgrade: IEEE, 2019. 1–4. [doi: 10.1109/TELFOR48224.2019.8971100]

[50] Venkataraman S, Caballero J, Poosankam P, Kang MG, Song DX. FiG: Automatic fingerprint generation. In: Proc. of the 2007 Network and Distributed System Security Symp. (NDSS). San Diego: ISOC, 2007. 1–16.

[51] Song JK, Li Q, Wang HN, Sun LM. Under the concealing surface: Detecting and understanding live webcams in the wild. In: Proc. of the 2020 SIGMETRICS/Performance Joint Int'l Conf. on Measurement and Modeling of Computer Systems. New York: Association for Computing Machinery, 2020. 77–78. [doi: 10.1145/3393691.3394220]

[52] Yan ZT, Lv SC, Zhang YY, Zhu HS, Sun LM. Remote fingerprinting on Internet-wide printers based on neural network. In: Proc. of the 2019 IEEE Global Communications Conf. Waikoloa: IEEE, 2019. 1–6. [doi: 10.1109/GLOBECOM38437.2019.9014144]

[53] ZTag. Tagging and annotation framework for scan data. 2019. https://github.com/zmap/ztag

[54] Feng X, Li Q, Wang HN, Sun LM. Acquisitional rule-based engine for discovering internet-of-thing devices. In: Proc. of the 27th USENIX Conf. on Security Symp. Baltimore: USENIX Association, 2018. 327–341.

[55] Wang X, Wang YC, Feng X, Zhu HS, Sun LM, Zou YC. IoTTracker: An enhanced engine for discovering Internet-of-Thing devices. In: Proc. of the 20th IEEE Int'l Symp. on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM). Washington: IEEE, 2019. 1–9. [doi: 10.1109/WoWMoM.2019.8793012]

[56] Holland J, Teixeira R, Schmitt P, Borgolte K, Rexford J, Feamster N, Mayer J. Classifying network vendors at Internet scale. arXiv:2006.13086, 2020.

[57] Wang XW, Huang J, Qi CY. FDI: A fast IoT device identification approach. In: Proc. of the 2020 Int'l Conf. on Cyberspace Innovation of Advanced Technologies. Guangzhou: ACM, 2020. 277–282. [doi: 10.1145/3444370.3444585]

[58] Li Q, Feng X, Wang RN, Li Z, Sun LM. Towards fine-grained fingerprinting of firmware in online embedded devices. In: Proc. of the 2018 IEEE Conf. on Computer Communications (INFOCOM). Honolulu: IEEE, 2018. 2537–2545. [doi: 10.1109/INFOCOM.2018.8486326]

[59] Durumeric Z, Adrian D, Mirian A, Bailey M, Halderman JA. A search engine backed by Internet-wide scanning. In: Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security (CCS). Denver: ACM, 2015. 542–553. [doi: 10.1145/2810103.2813703]

[60] Yu D, Li PY, Chen YL, Ma Y, Chen JJ. A time-efficient multi-protocol probe scheme for fine-grain IoT device identification. Sensors, 2020, 20(7): 1863. [doi: 10.3390/s20071863]

[61] Izhikevich L, Teixeira R, Durumeric Z. LZR: Identifying unexpected Internet services. In: Proc. of the 30th USENIX Security Symp. Vancouver: USENIX Association, 2021. 3111–3128.

[62] Birnbach S, Eberz S, Martinovic I. Peeves: Physical event verification in smart homes. In: Proc. of the 2019 ACM SIGSAC Conf. on Computer and Communications Security (CCS). London: ACM, 2019. 1455–1467. [doi: 10.1145/3319535.3354254]

[63] Bhatt P, Morais A. HADS: Hybrid anomaly detection system for IoT environments. In: Proc. of the 2018 Int'l Conf. on Internet of Things, Embedded Systems and Communications (IINTEC). Hamammet: IEEE, 2018. 191–196. [doi: 10.1109/IINTEC.2018.8695303]

[64] Wan YX, Xu K, Xue GL, Wang F. IoTArgos: A multi-layer security monitoring system for Internet-of-Things in smart homes. In: Proc.

of the 2020 IEEE Conf. on Computer Communications (INFOCOM). Toronto: IEEE, 2020. 874–883. [doi: 10.1109/INFOCOM41043.2020.9155424]

[65] Nguyen TD, Marchal S, Miettinen M, Fereidooni H, Asokan N, Sadeghi AR. DÏoT: A federated self-learning anomaly detection system for IoT. In: Proc. of the 39th IEEE Int'l Conf. on Distributed Computing Systems (ICDCS). Dallas: IEEE, 2019. 756–767. [doi: 10.1109/ICDCS.2019.00080]

[66] Weinger B, Kim J, Sim A, Nakashima M, Moustafa N, Wu KJ. Enhancing IoT anomaly detection performance for federated learning. Digital Communications and Networks, 2022, 8(3): 314–323. [doi: 10.1016/j.dcan.2022.02.007]

[67] Fan YL, Li Y, Zhan MQ, Cui HJ, Zhang Y. IoTDefender: A federated transfer learning intrusion detection framework for 5G IoT. In: Proc. of the 14th IEEE Int'l Conf. on Big Data Science and Engineering (BigDataSE). Guangzhou: IEEE, 2020. 88–95. [doi: 10.1109/BigDataSE50710.2020.00020]

[68] Alaiz-Moreton H, Aveleira-Mata J, Ondicol-Garcia J, Muñoz-Castañeda AL, García I, Benavides C. Multiclass classification procedure for detecting attacks on MQTT-IoT protocol. Complexity, 2019, 2019: 6516253. [doi: 10.1155/2019/6516253]

[69] Hamza A, Gharakheili HH, Benson TA, Sivaraman V. Detecting volumetric attacks on loT devices via SDN-based monitoring of MUD activity. In: Proc. of the 2019 ACM Symp. on SDN Research. San Jose: ACM, 2019. 36–48. [doi: 10.1145/3314148.3314352]

[70] Santos J, Leroux P, Wauters T, Volckaert B, De Turck F. Anomaly detection for smart city applications over 5G low power wide area networks. In: Proc. of the 2018 IEEE/IFIP Network Operations and Management Symp. Taipei: IEEE, 2018. 1–9. [doi: 10.1109/NOMS.2018.8406257]

[71] Li D, Chen DC, Goh J, Ng SK. Anomaly detection with generative adversarial networks for multivariate time series. arXiv:1809.04758, 2018.

[72] Mirsky Y, Doitshman T, Elovici Y, Shabtai A. Kitsune: An ensemble of autoencoders for online network intrusion detection. In: Proc. of the 2018 Network and Distributed System Security Symp (NDSS). San Diego: ISOC, 2018. 1–15. [doi: 10.14722/ndss.2018.23204]

[73] Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shabtai A, Breitenbacher D, Elovici Y. N-BaIoT—Network-based detection of IoT Botnet attacks using deep autoencoders. IEEE Pervasive Computing, 2018, 17(3): 12–22. [doi: 10.1109/MPRV.2018.03367731]

[74] Duan CX, Li J, Han DQ, Fan LN, Zhang SZ, Yang JH, Wang ZL. Towards the adaptability of traffic-based IoT security management systems to the device behavior evolutions. In: Proc. of the 1st EAI Int 'l Conf. on Applied Cryptography in Computer and Communications. Springer, 2021. 88–95. [doi: 10.1007/978-3-030-80851-8_15]

[75] Cheng L, Tian K, Yao DF. Orpheus: Enforcing cyber-physical execution semantics to defend against data-oriented attacks. In: Proc. of the 33rd Annual Computer Security Applications Conf. Orlando: ACM, 2017. 315–326. [doi: 10.1145/3134600.3134640]

[76] Yu TL. Securing Internet-of-Things via fine-grained network detection and prevention [Ph.D. Thesis]. Pittsburgh: Carnegie Mellon University, 2020.

[77] Zhang W, Meng Y, Liu YG, Zhang XK, Zhang YQ, Zhu HJ. HoMonit: Monitoring smart home apps from encrypted traffic. In: Proc. of the 2018 ACM SIGSAC Conf. on Computer and Communications Security (CCS). Toronto: ACM, 2018. 1074–1088.

[78] Gu TB, Fang Z, Abhishek A, Fu H, Hu PF, Mohapatra P. IoTGaze: IoT security enforcement via wireless context analysis. In: Proc. of the 2020 IEEE Conf. on Computer Communications (INFOCOM). Toronto: IEEE, 2020. 884–893. [doi: 10.1109/INFOCOM41043.2020.9155459]

[79] Ding WB, Hu HX, Cheng L. IoTSafe: Enforcing safety and security policy with real IoT physical interaction discovery. In: Proc. of the 2021 Network and Distributed System Security Symp. (NDSS). ISOC, 2021. 1–18. [doi: 10.14722/ndss.2021.24368]

[80] Wang Q, Datta P, Yang W, Liu S, Bates A, Gunter CA. Charting the attack surface of trigger-action IoT platforms. In: Proc. of the 2019 ACM SIGSAC Conf. on Computer and Communications Security (CCS). London: ACM, 2019. 1439–1453. [doi: 10.1145/3319535.3345662]

[81] Al Farooq A, Al-Shaer E, Moyer T, Kant K. IoTC$^2$: A formal method approach for detecting conflicts in large scale IoT systems. In: Proc. of the 2019 IFIP/IEEE Symp. on Integrated Network and Service Management (IM). Arlington: IEEE, 2019. 442–447.

[82] Mohsin M, Anwar Z, Husari G, Al-Shaer E, Rahman MA. IoTSAT: A formal framework for security analysis of the Internet of Things (IoT). In: Proc. of the 2016 IEEE Conf. on Communications and Network Security (CNS). Philadelphia: IEEE, 2016. 180–188. [doi: 10.1109/CNS.2016.7860484]

[83] Fu CL, Zeng Q, Du XJ. Hawatcher: Semantics-aware anomaly detection for appified smart homes. In: Proc. of the 30th USENIX Security Symp. USENIX Association, 2021. 4223–4240.

[84] Alrawi O, Lever C, Valakuzhy K, Court R, Snow KZ, Monrose F, Antonakakis M. The circle of life: A large-scale study of the IoT malware lifecycle. In: Proc. of the 30th USENIX Security Symp. USENIX Association, 2021. 3505–3522.

[85] Pinheiro AJ, de M Bezerra J, Burgardt CAP, Campelo DR. Identifying IoT devices and events based on packet length from encrypted

traffic. Computer Communications, 2019, 144: 8–17. [doi: 10.1016/j.comcom.2019.05.012]

[86] Junges PM, François J, Festor O. Passive inference of user actions through iot gateway encrypted traffic analysis. In: Proc. of the 2019 IFIP/IEEE Symp. on Integrated Network and Service Management (IM). Arlington: IEEE, 2019. 7–12.

[87] Trimananda R, Varmarken J, Markopoulou A, Demsky B. Packet-level signatures for smart home devices. In: Proc. of the 2020 Network and Distributed System Security Symp. (NDSS). San Diego: ISOC, 2020. 1–18. [doi: 10.14722/ndss.2020.24097]

**樊琳娜**(1987－), 女, 讲师, 主要研究领域为物联网, 机器学习.

**王之梁**(1978－), 男, 副教授, 主要研究领域为计算机网络体系结构, 网络形式化验证和测试, 网络测量.

**李城龙**(1985－), 男, 博士, 副研究员, CCF 专业会员, 主要研究领域为网络空间测绘, 网络信息安全.

**林海**(2000－), 男, 博士生, 主要研究领域为机器学习, 知识图谱, 物联网.

**吴毅超**(1997－), 男, 硕士生, 主要研究领域为网络测量, 网络路由优化.

**杨家海**(1966－), 男, 博士, 教授, 博士生导师, CCF 高级会员, 主要研究领域为计算机网络体系结构, 网络管理与测量, 网络空间安全与测绘, 云计算.

**段晨鑫**(1996－), 男, 硕士生, 主要研究领域为网络测量, 网络安全.