

融合多维标识特征的摄像头身份识别方法

朱容辰¹ 李欣^{1,2} 王晗旭¹ 叶瀚¹ 曹志威³ 樊志杰³

1 中国人民公安大学信息安全学院 北京 100038
2 安全防范技术与风险评估公安部重点实验室 北京 100026
3 公安部第三研究所信息安全技术部 上海 200031
(zhurongchen@stu.ppsuc.edu.cn)

摘要 随着智慧城市、公安大数据的发展,视频监控网络已成为城市治理的重要基础设施。但是,攻击者通过替换或篡改监控摄像头这一重要的前端设备,能够接入内部网络,实现设备劫持、信息窃取、网络瘫痪,威胁个人、社会与国家安全。为了提前识别非法或可疑的摄像头身份,提出了融合多维标识特征的摄像头身份识别方法。通过提取摄像头静态信息与动态流量信息,构建了融合显性、隐性、动态标识符的摄像头身份标识体系。为选择简洁有效的身份标识符,提出了基于自信息量与信息熵的标识符贡献度评估方法,所抽取的标识符特征向量能够为未来的异常摄像头入侵检测奠定基础。实验结果表明,显性标识符自信息量与贡献度最大,但容易被伪造;动态标识符贡献度次之,但流量收集与处理的工作量较大;静态标识符贡献度较低,但仍有一定的身份标识作用。

关键词: 摄像头;标识特征;自信息量;身份识别;入侵检测

中图法分类号 TP309

Camera Identity Recognition Method Fused with Multi-dimensional Identification Features

ZHU Rong-chen¹, LI Xin^{1,2}, WANG Han-xu¹, YE Han¹, CAO Zhi-wei³ and FAN Zhi-jie³
1 School of Information Network Security, People's Public Security University of China, Beijing 100038, China
2 Key Laboratory of Security Prevention Technology and Risk Assessment of the Ministry of Public Security, Beijing 100026, China
3 Department of Information Security Technology, The Third Research Institute of Ministry of Public Security, Shanghai 200031, China

Abstract With the development of smart cities and public security big data, video surveillance networks have become essential infrastructure for urban governance. However, by replacing or tampering with surveillance cameras- the important front-end device, an attacker can access the internal network to achieve device hijacking, information theft, network paralysis, and threatening personal, social, and national security. A camera identity recognition method combining multi-dimensional identification features is proposed to identify illegal camera identities in advance. A camera identification system that integrates explicit, implicit, and dynamic identifiers is constructed by extracting the camera's static information and the dynamic flow information. An evaluation method of identifier contribution based on self-information and information entropy is proposed to select a concise and practical identity identifier. The extracted identifier feature vector can lay the foundation for future abnormal camera intrusion detection. Experimental results show that explicit identifiers have the most considerable amount of self-information and contribution but are easy to be forged; dynamic identifiers have the second-highest contribution, but the workload of traffic collection and processing is enormous; static identifiers have a low contribution but still have a specific role in identification.

Keywords Camera, Identification feature, Self-information amount, Identity recognition, Intrusion detection

近年来,随着公安大数据应用的快速发展,视频监控网络成为了治安管理、犯罪侦查的利器^[1]。公安部门主导建立的视频监控专网,具有视频前端设备规模庞大、地域覆盖广泛、系统应用软件多样、承载业务功能丰富、监控要求严格等特点,它有助于提高公安工作效率、辅助案件侦查^[2]。但是视频监控

系统面临复杂网络安全风险,这种分布于各地的网络容易成为犯罪分子的攻击目标,一旦发生重大网络安全事件将会导致视频监控资源不可用,进而可能威胁到国家、社会、企业和个人安全^[1-3]。工业界和学术界在防范工具和方法的开发上投入了大量资金,通过监测和预警,前移防范屏障,减少潜在的损失。

视频监控摄像头作为视频监控网络(见图 1)的重要前端

基金项目:国家自然科学基金面上项目(62076246);公安部科技强警基础工作专项项目(2020GABJC01);中国人民公安大学拔尖创新人才培养经费支持研究生科研创新项目(2021yjsky016)

This work was supported by the National Natural Science Foundation of China(62076246), Science and Technology Project of the Ministry of Public Security(2020GABJC01) and Top Talent Training Special Funding Graduate Research and Innovation Project of People's Public Security University of China(2021yjsky016).

通信作者:李欣(lixin@ppsuc.edu.cn)

设备,具有数量众多、种类繁杂的特点。如果某摄像头被非法替换,容易发展为整个视频网络的安全风险。但是,由于一部分视频专网摄像头是通过运营商租赁、购买、安装和更换,管理部门往往无法厘清所有前端设备,同时缺乏前端设备的整体安全管理机制,未有一种高效的前端设备身份真实性检测方法。传统的前端摄像头采用类似 MAC 地址、IP 地址等静态标识符的方法对其进行设备标识,容易被伪造和篡改^[4]。因此,即使视频监控摄像头被非法替换,安全管理部门往往难以察觉。

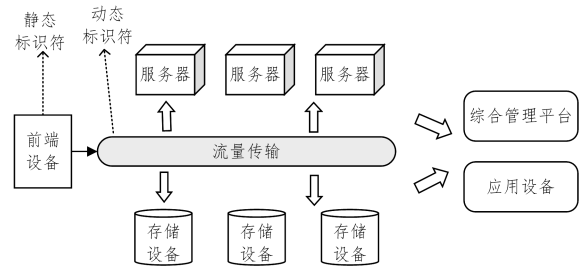


图 1 视频监控网络工作流程

Fig. 1 Video surveillance network workflow

为此,本文提出了一种融合多维标识特征的摄像头身份识别方法。首先收集并提取摄像头的静态标识符,包括显性标识符与隐性标识符。接着从摄像头网络流量的角度入手,提取一系列动态流量特征集。将多维标识符进行融合,分析每个标识符的自信息量。最后根据标识符在标识体系中的贡献量确定摄像头身份识别指标。

1 相关工作

为了加强公安视频专网安全防护的建设,公安部科技信息化局自 2017 年至 2018 年发布了视频监控的文件《关于加强公安视频监控安全管理工作的通知》《关于开展 2018 年度全国公安信息网络安全检查工作的通知》和《关于做好修复视频监控系统摄像机安全漏洞等相关工作的通知》,这些文件在一定程度上加强了公安视频监控的安全管理水平,减少了安全漏洞数量。大量学者也对视频监控网络安全进行了深入的研究,Li 等^[1]构建了面向视频专网的网络安全态势指标体系,并给出了指标量化方法。Duan^[2]使用隐马尔可夫模型等实现了网络安全态势要素提取与评估。上述研究主要关注视频专网宏观安全态势,并没有重点关注前端设备的身份识别安全风险;同时指标的量化基于专家经验,较为粗糙。

基于设备指纹的硬件身份认证技术是网络空间安全的热点问题^[4]。设备指纹是指利用设备的特征信息,来生成独一无二的标识符^[5]。基于设备标识符,用户可以进行设备认证与设备异常检测^[6]。目前,设备指纹认证技术主要有:基于瞬态特征^[7]、基于调制信号^[7-8]和基于内部传感器^[9-10]3 种^[4]。代表性的研究有,Lukas 等^[11]通过传感器图案噪声识别摄像机,并在 9 种不同摄像机的 320 张图像上验证了方法的有效性。Wang 等^[6]从不同设备的特征区分度和相同设备的特征稳定性出发,设计了一种设备指纹特征选择方法,其在 6424 台安卓设备上的实验结果显示了该方法的准确率较高。Zhang 等^[12]为了解决物联网系统的身份认证问题,使用双向认证协议研究 RFID 标签认证技术,实验结果表明该技术能

够快速确认身份信息,保证物联网完全。但是该文是从传统密码学的角度进行双向身份认证,方法难以用于摄像头身份识别领域。

相比安卓设备、平板电脑,视频监控摄像头的功能较为单一,且基于设备指纹,针对视频监控摄像头的身份识别的研究仍然较少。代表性的工作有 Yin 等^[3]提出了使用决策树方法对设备指纹进行分类,继而实现了 IP 视频专网的入网检测。其中设备指纹包括多个维度,如 IP 地址、设备上正在运行的服务、内存使用信息等。但是该研究忽略了摄像头的流量信息。

每个视频监控摄像头的动态的流量特征集能够全面反映前端摄像头的流量特点,是前端网络中摄像头的唯一性标识及后续精准识别和网络入侵检测的基础。如果有人恶意替换摄像头,大部分显性标识符是容易伪造的,公共安全部门很难察觉异常。但是摄像头的流量特征则是难以篡改的,因此可以用作身份识别的重要指标。关于流量特征的研究,Yang 等^[13]提出了基于流量指纹的物联网设备识别方法,该方法具有更好的检测效果与稳定性。Meidan 等^[14]提出使用机器学习方法对物联网设备的网络流量进行分析并完成设备识别,其整体分类精度高达 99%。目前,对视频监控摄像头的流量特征进行摄像头身份识别的研究仍是空白,需要深入的研究。

在视频监控网络中,如果某前端接入设备的标识符与本地数据库中不一致,便可以被认为是异常设备。而设备异常接入入侵检测算法,则更多地使用关联规则、支持向量机^[15]、随机森林^[16]、决策树^[3]等算法在数据集中识别出异常数据^[17]。

通过回顾文献发现:1)针对摄像头身份识别的研究较少,亟需开展面向视频监控前端设备的身份识别研究;2)相关部门仍依靠显性标识符判断设备身份,在身份标识中没有考虑利用隐性标识特征与摄像头流量这一动态特征信息;3)未采用有效的方法评估不同标识符对设备身份识别的贡献程度。

为了解决以上问题,需要采用合适的方法对摄像头特征进行采集、分析、汇聚、融合。为此,本文提出了一种融合多维标识特征的摄像头身份识别方法,为安全管理部门提供有效的前端设备非法接入识别手段。

本文的主要贡献如下:

(1)设计了一个包含静态与动态标识符的摄像头标识体系。从摄像头显性、隐性特征、流量特征出发,实现多维特征采集与抽取。

(2)提出了一种基于自信息量与信息熵的摄像头多维特征分析方法。计算标识符的特征向量,判断特征贡献信息,为代表性指标选取奠定基础。

本文第 2 节详细介绍了融合多维标识特征的摄像头身份识别方法;第 3 节通过实验验证了本文方法的可行性;最后总结全文并展望未来。

2 融合多维标识特征的摄像头身份识别方法

本文拟提出一种融合多维静态与动态标识特征的视频摄像头身份标识方法,主要研究方法如图 2 所示。首先收集视频监控摄像头的的数据,接着提取每个摄像头的静态与动态标识符,并计算不同标识符的自信息量与信息熵,以此评价不同

标识符的贡献度并最终实现摄像头身份识别。

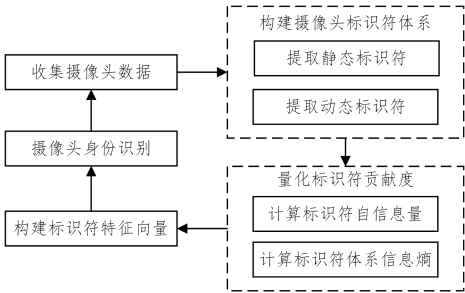


图 2 本文流程图
Fig. 2 Flow chart of our method

我们将原始标识符体系分为静态标识符体系和动态标识符体系。每个体系所包含的标识符如图 3 所示,每个标识符将在后续章节详细叙述。

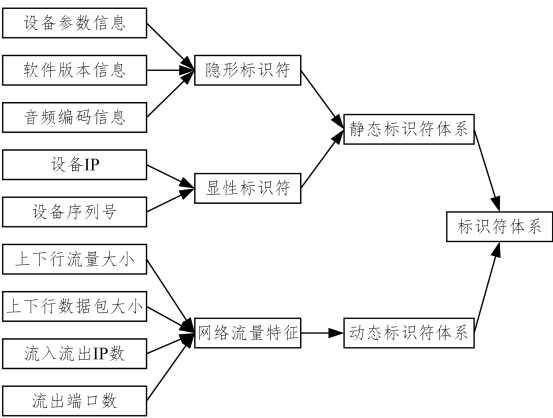


图 3 摄像头标识符体系
Fig. 3 Camera identifier system

2.1 标识符体系的构建

2.1.1 静态标识符体系

静态标识符体系包括显性标识符和隐形标识符两种,在原始标识符体系的基础上对其进行二次提取与融合,生成最终的标识符体系。传统的前端摄像头采用类似显性标识符的方法对其进行唯一标识,容易被伪造和篡改。单独隐性标识符不具备唯一标识的能力,通过组合多个隐形标识符提高标识能力。本文结合二者各自的优缺点,选取显性标识符与隐性标识符相结合的方式构建并生成静态标识符体系。

显性标识符是指明显标识视频监控摄像头的符号。本文对摄像头身份识别采用的显性标识符包括 IP 地址、mac 地址、序列号、设备类型,如表 1 所列。

表 1 部分摄像头的显性标识符举例

设备 IP	设备序列号	MAC 地址	设备类型
192.168.1.65	iDS-2CD6024	28:57:be:29:7b:4a	iDS-2CD6024FWD-A/F
192.168.1.63	FWD-A/F2015	28:57:be:b1:2f:a9	iDS-2DF5220S-D4/JY
192.168.1.61	1114CCCH	28:57:be:59:d6:5c	iDS-2CD6812F-IS/B
192.168.1.62	555848778	28:57:be:39:d7:56	DS-GJZ22G-IS

本文拟提取的 6 类隐性标识符如表 2 所列,分别从参数信息、通道信息、音频编码信息、视频配置信息、软件信息等方面收集摄像头隐性标识符。表 2 标明了每一类标识符所包含的隐性标识符名称。表 3 列出了一部分隐性标识符信息。

表 2 摄像头隐性标识符的类别举例
Table 2 Examples of categories of hidden camera identifiers

隐性标识符类别	说明
设备参数信息	包含设备品牌、设备类型、操作系统等信息
通道信息	包含通道名称、通道大小等
音频编码信息	音频编码类型
视频配置信息	包含视频帧率、位率类型等信息
软件信息	包含主软件版本、DSP 软件版本等信息

表 3 摄像头隐性标识符举例
Table 3 Examples of hidden camera identifiers

操作系统	设备品牌	设备型号	开放服务	音频编码类型
Linux	大华	IPC-HF	554:rtsp	G711_A
OpenWrt	海康威视	DS-2CD	9010:sdr	AAC
Windows	华为	IPC622	20000:dnf	G711_U
Android	丽泽智能	IDS-2CD	8080:http	G711_A

2.1.2 动态标识符体系

在动态标识符体系方面,针对前端摄像头的应用场景特点,本文从摄像头流量特征的角度进行定义和提取。动态的流量特征集是由一系列能全面反映前端摄像头的流量特征的指标构成,是后续精准识别和网络入侵检测的基础。

本文初步构建的视频监控摄像头的动态标识符体系如表 4 所列。网络流量特征主要包括 4 类,分别为上下行流量特征、上下行数据包特征、流入流出 IP 特征、流出目的端口数特征,一共包含 10 个特征。

表 4 摄像头流量特征举例
Table 4 Examples of camera flow characteristics

序号	流量特征名称	示例
1	每小时上行流量	27962327 bytes
2	每小时下行流量	3061933914 bytes
3	每小时总流量	3089896241 bytes
4	每小时上行数据包	687167 个
5	每小时下行数据包	2138965 个
6	每小时总数据包	2826132 个
7	每日流出 ip 数	6 个
8	每日流入 ip 数	6 个
9	每日总连接 ip 数	6 个
10	每日流出目的端口数	2 个

本文对摄像头每天特定时段的内容进行抽取,得到流量大小、数据包大小、IP 特征等信息。这些信息是根据特定摄像头的视频流传输协议所确定的,因此违法者难以对这类特征进行伪造,一旦前端摄像头被恶意更换,这类特征往往会相应改变。如果管理人员能够实时统计并比对设备流量特征,能够察觉到前端摄像头身份是否改变。

2.2 标识符贡献值量化

在静态和动态原始标识符体系初步构建的基础上,需要量化不同标识符的贡献值,以方便用户与管理部门选择并提取适当标识符,同时贡献值也证明了标识符可以辅助摄像头身份识别。本文通过信息论中的自信息量和信息熵来对标识符具有的信息量进行分析与判断,构建最终的标识符特征向量。

基于自信息量的标识符贡献度评估已经在多个领域被有效应用^[18-20]。如图 1 所示,本文首先通过计算标识符体系中不同标识符的自信息量,得到该标识符在该前端摄像头标识符体系中的贡献信息;而对于整体的标识符体系,计算标识符自信息量的期望,得到标识符体系在整体上所代表的信息量。也就是说,自信息量与信息熵分别从个体和整体来量化标识符的信息贡献。

假设每个前端摄像头有 n 个标识符,使用 P_i 表示第 i 个标识符能够正确识别摄像头的概率,事件 X_i 表示第 i 个标识

符能够正确识别摄像头。事件 X_i 的自信息量计算公式为：

$$I(X_i)=-\ln P_i$$

(1)

信息熵^[21]是为了对信息进行量化与度量,从公式来看,信息熵是自信息量的数学期望,即是计算整个标识符体系所带来的信息量大小。如果某标识符体系带来的不确定性大,则认为该标识符体系的信息量大,同时认为其贡献量也相应较大。因此,通过计算信息熵可以得到信息量最大的标识符体系。信息熵的计算公式如下：

$$H(X)=-\sum_{i=1}^n P_i \ln P_i$$

(2)

信息量将作为前端摄像头的最终标识符体系选取的重要指标之一,同时自信息量可以作为设备身份鉴别的初步依据之一,为后续前端摄像头身份的识别算法研究和前端网络的入侵检测奠定研究基础。

2.3 标识符特征向量的提取

在确定所选标识符的基础上,本节对标识符进行特征处理并整合为特征向量,以实现快捷有效的标识符比对。

本文的特征处理借鉴了 Yang 等^[13]与 Miettinen 等^[22]的离散化方法。离散化操作主要分为两步:1)收集各项标识符历史数据;2)利用专家经验对历史数据进行整理与离散。代表性的离散方法包括:1)对于某些标识符包含多个字段,对每个字段分别赋值。例如对不同的软件版本分别赋值[1,2,

3,⋯, n]。2)对于具有相对稳定数值的标识符,基于历史数据的最高、最低记录,设置浮动区间。若现有数据在浮动区间,则赋值为 1,否则赋值为 0。举例来说,某摄像头每日流出 ip 数在[4,5,6,7]间浮动,若某日该摄像头流出 ip 数为 8,则赋值为 0。3)对于包含连续型数值的标识符,可以在不改变数值相对大小的情况下,将数值映射到更小的空间。举例来说,如果某地摄像头流量包的数量在 1 000~90 000 间浮动,可以根据专家经验制定离散规则,将流量包离散为[1,2,3,4,⋯, n]。表 5 列出了代表性的特征变换方法。

表 5 标识符特征变换方法

Table 5 Identifier feature transformation method

标识符名称	特征变换方法
流量包长度	进行离散操作,转化为数字
通道名称	离散为 1~4 的数字
软件版本	不同软件版本对应不同数字
操作系统类别	不同类型系统对应不同数字
每日流出 ip 数	在历史数据区间为 1,否则为 0

基于表 6 所列的视频专网摄像头 21 个静态与 10 个动态标识符的标识符体系,在贡献值量化后决定保留所有标识符,则第 i 个摄像头的特征向量可以表示为：

$$P_i=\{f_{1,i},f_{2,i},f_{3,i},\cdots,f_{31,i}\}$$

(3)

表 6 面向视频专网的摄像头标识符体系

Table 6 Camera identifier system for video network

显性标识符		隐性标识符		动态标识符	
设备 IP	设备品牌	音频编码类型	通道名称	位率上限	每小时上行流量
设备序列号	设备型号	屏幕分辨率设置	码率类型	软件版本	每小时下行流量
MAC 地址	操作系统	解码器地址	视频帧率	DSP 软件版本	每小时总流量
设备类型	开放服务	RS485 速率	位率类型	通道个数	每小时上行数据包
	报警输入数				每小时下行数据包

3 实验与结果

3.1 实验数据与设置

本文采用分段验证的方法,首先提取摄像头厂家 A 和 B 一部分摄像头的显性与隐性标识符,并比较其对摄像头身份识别的贡献效果。

本文使用摄像头参数设置工具获得静态标识符数据。具体方法为:首先接入视频内网,接着打开摄像头参数设置工具并连接摄像头,导出摄像头参数信息,最后进行参数信息的筛选与清洗。本文捕获某地视频专网中的流量数据,并实现摄像头动态标识符的提取,特征举例如表 7 所列。

表 7 实验摄像头特征举例

Table 7 Examples of experimental camera features

标识符名	标识符内容	标识符名	标识符内容
设备 IP	192.168.1.65	设备品牌	海康
	iDS-2CD6024FWD-A/		
序列号	F20151114CCCH	设备型号	31
	555848778		
MAC 地址	28:57:be:29:7b:4a	音频编码类型	G711_A
设备类型	iDS-2CD6024FWD-A/F	屏幕分辨率设置	HD1080i

3.2 实验结果

基于 3.1 节收集的数据样本和 2.3 节的标识符贡献值量化的方法,计算可得标识符贡献排名。对于本文收集的厂家摄像头来说,设备 IP、设备序列号、MAC 地址的自信息量最

高,这是由于这 3 个标识符都是摄像头身份的唯一标识信息,但是这类标识符也容易被伪造或替换。在动态标识符中,每小时上行流量、每小时上行流量包的贡献值较高,每小时流出 ip、流入 ip 的贡献度较低。在隐性标识符中,开放服务、设备型号的自信息量最大,这是因为摄像头的这类信息往往具备一定的独特性。而如屏幕分辨率设置、位率类型等标识符的自信息量较小,这是由于摄像头往往提供了几种屏幕分辨率选项,因而特定选项出现的概率较大,根据式(1)可知,自信息量会较低。

但需要注意的是,不同厂家不同款式的摄像头标识符的贡献度是不同的,例如对于厂家 A 的摄像头来说,隐性标识符中开放端口的贡献度最大,但在厂家 B 的摄像头中开放端口是较为固定的,因此自信息量较低。这提醒了摄像头管理部门,需要根据不同厂家摄像头的特点确定不同的标识符进行身份识别。同时,如果进一步对不同款式摄像头设置不同的标识符识别方法,可以节省计算资源与存储空间。

使用信息熵对不同类别的标识符的贡献度进行分析,我们发现显性标识符在摄像头身份识别上所贡献的信息量是最大的,这是因为显性标识符具有一一对应性,即每个摄像头的显性标识都是不同的,因此其包含的信息量最大。动态标识符的贡献度次之,这是由于几乎每个摄像头的流量信息、流量包数量等都是不同的,因而自信息量较大。而隐性标识符的取值范围有限,会出现相同或者相似的现象,因此这类标识符

所贡献的信息量较低。

结束语 随着智慧城市与公安大数据的发展,视频监控网络必然会实现更高速的发展。在视频监控摄像头被广泛布置在城市角落的同时,也面临着被非法替换与篡改的风险,这类风险一旦蔓延,将会给整个视频网络与公共社会带来严峻挑战。本文提出了一种融合多维标识特征的摄像头身份识别方法,通过提取摄像头的显性与隐性的静态特征与流量动态特征,构建了摄像头标识符指标体系;接着进行标识的融合、筛选,组成特征向量,并利用互信息量与信息熵分析指标贡献水平,为入侵检测与设备识别奠定基础。实验结果表明,显性标识符的自信息量与贡献度最大,但最容易被伪造;动态标识符的贡献量次之,但是流量采集分析的工作量较大;隐性标识符的贡献量较少但仍具有一定的身份标识能力。

未来,首先将提取更多的摄像头动态特征,并进行特征融合,获取更有效的识别特征;其次,基于标识符指标体系与特征向量,通过收集被替换的摄像头数据,实现摄像头入侵异常检测是一个有潜力的方向;最后,我们将利用卷积神经网络与长短时记忆神经网络进行标识数据的特征提取与分类,以提升入侵检测效果。

参 考 文 献

[1] LI X, DUAN Y C, HUANG S H, et al. Construction of network security situation index system for video private network[J]. Journal of Beijing University of Aeronautics and Astronautics, 2020, 46(9): 1625-1634.

[2] DUAN Y C. Extraction and evaluation of network security situation elements for video private network[D]. Beijing: People's Public Security University of China, 2020.

[3] YIN X M, HU Z L, CHEN G L, et al. Research on IP video private network access detection scheme based on device fingerprint decision tree classification[J]. Information Network Security, 2016(12): 68-73.

[4] LUO J Z, YANG M, LING Z, et al. Cyberspace Security System and key technologies[J]. Chinese Science: Information Science, 2016, 46(8): 939-968.

[5] BUJLOW T, CARELA-ESPAÑOL V, SOLÉ-PARETA J, et al. A Survey on Web Tracking: Mechanisms, Implications, and Defenses[J]. Proceedings of the IEEE, 2017, 105(8): 1476-1510.

[6] WANG M, DING Z J. A new method for fingerprint feature selection and model construction of equipment[J]. Computer Science, 2020, 47(7): 257-262.

[7] DANEV B, ZANETTI D, CAPKUN S. On physical-layer identification of wireless devices[J]. ACM Computing Surveys, 2013, 45(1): 1-29.

[8] GERDES R, DANIELS T, PHD M, et al. Device Identification via Analog Signal Fingerprinting: A Matched Filter Approach [C]//Proceedings of the Network and Distributed System Security Symposium. 2006: 1-11.

[9] DEY S, ROY N, XU W, et al. AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable[C]//Network and Distributed System Security Symposium. 2014: 1-16.

[10] LI C T. Source Camera Identification Using Enhanced Sensor

Pattern Noise[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 280-287.

[11] LUKAS J, FRIDRICH J, GOLJAN M. Digital camera identification from sensor pattern noise[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 205-214.

[12] ZHANG Y T, YAN C H. Research on RFID tag authentication technology based on bidirectional authentication protocol[J]. Information Network Security, 2016(1): 64-69.

[13] YANG W C, GUO Y B, LI T, et al. Identification method and security model of Internet of things based on traffic fingerprint [J]. Computer Science, 2020, 47(7): 299-306.

[14] MEIDAN Y, BOHADANA M, SHABTAI A, et al. ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis[C]//Proceedings of the Symposium on Applied Computing. 2017: 506-509.

[15] ZHANG L P, LEI D J, ZENG X H. System call intrusion detection method based on frequency eigenvector[J]. Computer Science, 2013, 40(S1): 330-333, 339.

[16] YAO D, LUO J Y, CHEN W P, et al. Double random forest real-time intrusion detection method based on improved non extensive entropy feature extraction[J]. Computer Science, 2013, 40(12): 192-196, 218.

[17] LIN G Y, HUANG H, ZHANG Y P. Research progress of intrusion detection system[J]. Computer Science, 2008(2): 69-74.

[18] LUO C K, CHEN Y X, HU X, et al. Evaluation method of equipment system contribution rate based on combat ring and self information[J]. Journal of Shanghai Jiaotong University, 2019, 53(6): 741-748.

[19] PENG C G, DING H F, ZHU Y J, et al. Information entropy model and measurement method of privacy protection[J]. Acta Sinica Sinica, 2016, 27(8): 1891-1903.

[20] CHI Y, GAO Z W. Construction of hybrid P2P network based on self information algorithm [J]. Computer Science, 2012, 39(S1): 159-162.

[21] SHANNON C E. A mathematical theory of communication[J]. The Bell System Technical Journal, 1948, 27(3): 379-423.

[22] 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.



ZHU Rong-chen, born in 1996, master. His main research interests include cyber security, video network and machine learning.



LI Xin, born in 1977, Ph. D, associate professor. His main research interests include cyber security and so on.