密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2016,3(5):433–446

E-mail: jcr@cacrnet.org.cn
http:. In: www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-81033101

无线通信设备的射频指纹提取与识别方法*

俞佳宝[1], 胡爱群[1], 朱长明[2], 彭林宁[1], 姜 禹[1]

1. 东南大学 信息科学与工程学院, 南京 210096
2. 中国运载火箭技术研究院研发中心, 北京 100076
通讯作者: 胡爱群, E-mail: aqhu@seu.edu.cn

摘 要: 通过分析无线设备的通信信号来提取设备的射频指纹进行设备识别是一种保护通信系统安全的物理层方法. 射频指纹是无线通信设备的物理层本质特征, 很难被篡改. 就像不同的人有不同的指纹, 不同的无线设备也拥有不同的射频指纹, 可用于无线设备的身份识别和接入认证. 本文主要回顾了过去二十年国内外射频指纹技术的研究进展. 根据射频指纹提取与识别的典型流程, 首先分析了射频指纹的产生机理及众多可识别的设备类型, 反应出射频指纹拥有广阔的应用前景. 然后, 本文将可识别信号主要分成了瞬态信号和稳态信号两类, 并简述了检测和截取可识别信号的方法. 随后, 本文对射频指纹特征做了简单分类, 归纳分析了射频指纹应该具备的五大特点, 即通用性、唯一性、短时不变性、独立性以及稳健性. 本文还从瞬态信号射频指纹技术和稳态信号射频指纹技术两个方面总结了该领域的研究现状. 此外, 本文对于如何评估射频指纹系统的性能也做了一定的论述. 最后, 本文指出了该领域进一步的研究方向和可能面临的技术难题.

关键词: 射频指纹; 设备识别; 物理层安全; 特征提取
中图法分类号: TP309.7 **文献标识码**: A DOI: 10.13868/j.cnki.jcr.000141

中文引用格式: 俞佳宝, 胡爱群, 朱长明, 彭林宁, 姜禹. 无线通信设备的射频指纹提取与识别方法[J]. 密码学报, 2016, 3(5): 433–446.
英文引用格式: YU J B, HU A Q, ZHU C M, PENG L N, JIANG Y. RF fingerprinting extraction and identification of wireless communication devices[J]. Journal of Cryptologic Research, 2016, 3(5): 433–446.

RF Fingerprinting Extraction and Identification of Wireless Communication Devices

YU Jia-Bao[1], HU Ai-Qun[1], ZHU Chang-Ming[2], PENG Lin-Ning[1], JIANG Yu[1]

1. School of Information Science and Engineering, Southeast University, Nanjing 210096, China
2. Research Center of China Academy of Launch Vehicle Technology, Beijing 100076, China
Corresponding author: Hu Ai-Qun, E-mail: aqhu@seu.edu.cn

Abstract: Wireless device identification via radio frequency (RF) fingerprinting extracted from communication signals is a physical layer approach for communication system security. In physical layer, RF fingerprinting is an inherent characteristic of wireless communication devices themselves, which can hardly be tampered. Just as people have unique fingerprints, different wireless devices exhibit different RF fingerprints which can be used for

* 基金项目: 国家重点基础研究发展项目(973 计划)(2013CB338003); 国家自然科学基金项目(61571110); 江苏省六大人才高峰项目; 航天 CALT 基金项目
收稿日期: 2015-12-03 定稿日期: 2016-10-05

identification and authentication. This paper mainly provides a review of the research and development in RF fingerprinting extraction and identification in the past twenty years. According to the procedure of RF fingerprinting extraction and identification, we first analyze the generation mechanism of RF fingerprinting and the corresponding identification devices, which reflect the broad applications of the RF fingerprinting. Then, the identification signals are divided into transient signal and steady-state signal, and a method to detect and extract such signals are described. This paper further classifies the RF fingerprinting and summaries their five features, i.e., universality, uniqueness, short-time invariance, independence and robustness. This paper also summarizes the state of art on the procedure of transient and steady-state based techniques. It also describes how to evaluate the performance of RF fingerprinting identification systems. Finally, some potential research directions and challenges in this area are pointed out.

Key words: Radio frequency (RF) fingerprinting; device identification; physical layer security; feature extraction

1 引言

随着移动通信设备的不断普及和物联网技术的蓬勃发展, 无线通信在军事和民用两方面都发挥着不可替代的作用, 已成为现代社会不可或缺的一部分. 然而, 无线网络由于其开放性, 相比于传统的有线网络更容易受到大规模的恶意攻击, 其安全问题不容忽视. 传统的保护无线网络安全的方法通常是基于比特层面的(即 OSI 七层模型中物理层以上的层次), 通过设计基于密码机制的安全协议来实现对数据完整性和机密性的保护以及提供通信双方身份的认证. 然而, 实际的无线网络安全协议通常会存在漏洞[1]. 例如, IEEE 820.11 无线局域网(WLAN)最初的有线等效加密(WEP)协议易受统计分析攻击[2], 虽然此后升级为 WPA 和 WPA2, 但其口令句可以被恢复, 仍然存在着各种各样的安全问题[3]. 此外, 一旦密钥泄露, 现有的安全机制无法实现身份认证. 因此, 人们急需寻找一种新型的安全机制有效识别授权用户和非授权用户, 从而降低来自恶意用户的潜在威胁.

在过去的十几年里, 无线通信设备的射频指纹提取和识别方法得到了国内外广泛的关注. 这种方法通过分析无线设备的通信信号来提取设备的“射频指纹(Radio Frequency Fingerprinting, RFF)”[4–13]. 就像每个人有不同的指纹, 每个无线设备也有不同的射频指纹——即硬件的差异, 这种硬件上的差异会反映在通信信号中, 通过分析接收到的射频信号就可以提取出该特征. 这种根据通信信号提取设备硬件特征的方法被称为“射频指纹提取”, 而利用射频指纹对不同的无线设备进行识别的方法则称为“射频指纹识别”. 无线通信设备的射频指纹提取和识别方法工作在物理层, 因此其既能够单独运作, 也可以辅助和增强传统的无线网络识别机制, 从而为无线网络提供更高的安全性能.

“射频指纹”这一概念最早是在 2003 年由加拿大的 Hall 等人在文献[14]中提出的, 通过提取蓝牙通信信号中的射频指纹进行蓝牙通信设备的识别. 但这种基于通信信号来进行设备识别的方法其实早在 1995 年就已经由 Choe 等人和 Toonstra 等人分别在文献[15]和文献[16]中提出, 其中 Toonstra 等人更是明确提出利用无线发射机的瞬态信号产生独特的“指纹”进行设备识别. 在随后的十年里, 人们围绕瞬态信号展开研究. 直到 2008 年, Kennedy 等人首次提出了基于稳态信号的射频指纹研究[17]. 近几年来, 基于稳态信号的射频指纹提取和识别技术得到了越来越多的重视, 也取得了一定的成果.

然而, 随着国外对于射频指纹技术的愈发重视, 国内对于这一领域的关注却不是很多. 本文主要通过回顾和总结过去二十年射频指纹提取和识别的研究进展, 旨在使大家对射频指纹提取和识别技术有进一步的了解. 本文的第 2 节首先提出了射频指纹提取和识别的工作流程, 随后在 2.2 节分析了射频指纹的产生机理, 在 2.3 节归纳了可进行识别的无线通信设备类型, 在 2.4 节将用来提取设备特征的信号段定义为“可识别信号”, 将其分为瞬态信号和稳态信号两类, 并简述了检测和截取可识别信号的方法. 然后, 在 2.5 节对提取的射频指纹特征做了简单分类, 在 2.6 节归纳了射频指纹应该具备的特点, 在 2.7 节则简单提及了

分类的步骤. 本文的第 3 节从瞬态信号射频指纹技术和稳态信号射频指纹技术两个方面总结了该领域的研究现状. 本文的第 4 节则对如何评估射频指纹系统的性能做了一定的论述. 最后, 我们在第 5 节指出了该领域潜在的研究方向和可能面临的难题, 并对全文做了总结.

2 射频指纹提取与识别流程

2.1 基本模型

无线通信设备射频指纹提取与识别过程如图 1 所示: 无线通信设备发送射频信号, 射频指纹提取与识别系统采集该信号. 采集到的射频信号与发送信号相比, 受到了多径信道的影响, 因此根据接收信号提取的特征可以分成两部分: 基于信道的特征和基于发射机的特征. 其中, 基于信道的特征表征了无线信道响应以及周围环境影响, 被称为信道指纹; 而基于发射机的特征则主要代表了发射机模拟电路的射频特征, 被称为设备指纹, 本文研究的主要是后者.

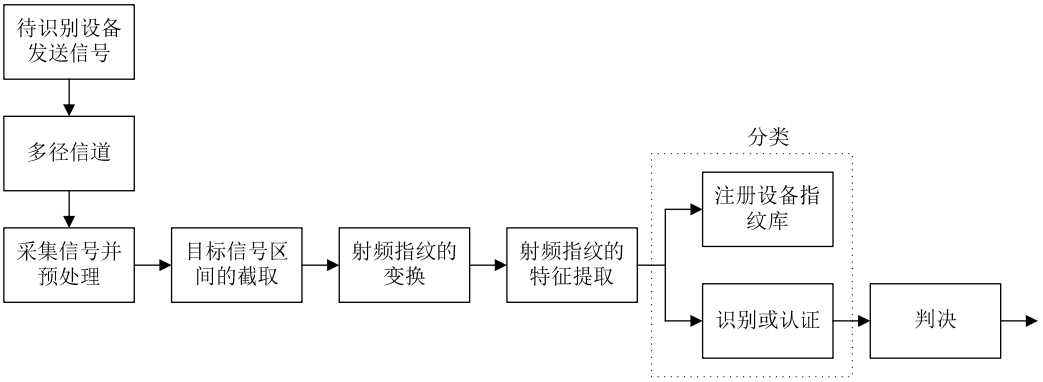


图 1 射频指纹提取与识别的流程

Figure 1 The procedure of RF fingerprinting extraction and identification

系统采集信号后, 根据后续的射频指纹提取要求, 要对信号先进行下变频、相位补偿、能量归一化、丢弃不合格信号等预处理. 在信号的预处理阶段, 要求尽可能少引入噪声. 因此, 信号采集和预处理一般要求使用高端仪器设备, 大部分文献也都是采用示波器等高精度设备进行信号的采集和预处理的. 然而, 考虑到实际应用场景, 近些年的文献中开始研究采用通用软件无线电外设(Universal Software Radio Peripheral, USRP)等中低端接收设备进行设备的射频指纹提取和识别[18–20]. 文献[20]还比较了分别采用高端设备和低端设备进行信号采集预处理的识别性能, 实验结果显示采用高端设备的识别性能比采用低端设备高 10%左右.

在进行预处理后, 识别系统检测和截取可识别信号, 将这段信号进行射频指纹变换, 变换到时域、频域或小波域提取设备相关的特征, 构成一个特征向量作为设备的射频指纹, 具体可提取的特征在 2.5 节做了详细的论述.

最后则是一个典型的模式分类问题, 主要分成训练和识别两个步骤. 在训练阶段, 对面向的所有设备进行信号的采集与存储, 提取每个设备的射频指纹, 登记入库, 与对应设备的 ID 号链接在一起构建成射频指纹库. 在识别阶段, 通过采集待识别设备的通信信号提取其对应射频指纹, 与指纹库中的对照指纹进行比较获得结果. 通常识别可分成两种: 一种是 1 对 N 的识别, 即判断待识别设备是库中哪个已登记设备; 另一种则是 1 对 1 的认证, 将提取的待识别设备射频指纹与其声称设备的对照指纹进行对照, 判断其是否身份匹配. 分类的判决结果一般是和具体应用相关的, 不同的应用要求结果不同, 但一般都是一个确定性的判决结果,例如允许或者不允许设备接入.

2.2 射频指纹产生机理

图 2 所示是一种典型的数字无线电发射机的系统框图. 基带信号经过数字信号处理后进入到灰色标示的模拟电路部分, 这部分模拟器件的容差是发射机射频指纹的主要来源. 无论是集成电路还是非集成电路, 其本质都是由电子元器件构成的, 电子元器件的容差导致最终的器件存在容差效应.

电子元器件的容差可以分成制造容差和漂移容差两部分. 其中, 制造容差是指在元件生产过程中, 由于设备的材料和加工工艺误差等原因, 导致电子元器件的电参数与标称值存在一定的容差, 常用的容差有±1%、±5%、±10%等, 容差值越小, 生产成本也就越高. 而漂移容差主要是指由于时间积累引起的器件参数的退化老化效应, 此外, 还包括由于设备工作环境的变化, 如温度、湿度等因素的变化导致设备工作过程中元件参数值的变化. 除了集成电路与非集成电路内部的元件存在的容差之外, 引起射频指纹的容差因素还包括印制电路板的材质、走线等, 这些统称为电路的容差效应. 容差效应导致即使是同一厂家同一型号同一系列甚至是同一批次的无线通信设备的实际硬件参数也会存在差异, 包括振荡器的频偏、相位噪声、调制器的调制误差、功放的非线性失真、功率 ramp-up 的失真以及包括中频、射频滤波器等滤波器的失真——这些硬件容差就是产生射频指纹的物质基础. 虽然通过提高生产精度可以减小硬件容差, 但其成本会显著提升. 此外, 通常的技术标准例如 IEEE 802.11 和 IEEE 802.15.4 等设备要求能够容忍接收信号较大的波动. 因此, 这些硬件容差可以用来构建发射机的独特身份[1].

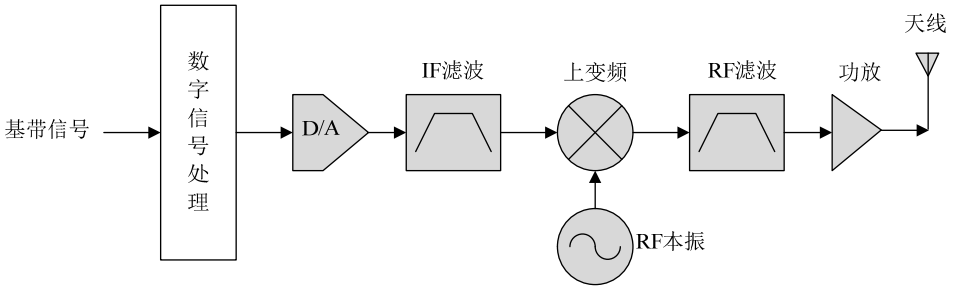


图 2 典型的数字无线电发射机结构
Figure 2 The typical structure of digital radio transmitter

2.3 可识别设备类型

射频指纹识别通过分析无线通信设备的通信信号提取射频指纹来进行设备识别. 因此, 理论上所有无线通信设备都可以通过提取射频指纹进行识别. 至今为止, 已经有各种各样的无线设备被用来进行射频指纹的研究, 包括最早开始研究的 VHF FM 发射机[21–26], 随后的蓝牙设备[14], GSM 设备[27,28], IEEE 802.16WiMax 设备[29], 通用移动通信系统(UMTS)设备[30], LTE 设备[31,32], 认知无线电网络(CRN)设备[33], RFID 设备[34], 以及研究最多的 IEEE 802.11 WiFi 设备[35]和 IEEE 802.15.4 Zigbee 设备[36,37].

上一节我们已经指出这些服从不同标准的无线通信设备的射频指纹主要来源于其模拟电路部分的容差, 然而具体是哪一部分器件引入了主要的容差并没有得到充分的研究. 文献[21]提出 VHF 发射机的射频指纹主要来源于频率综合器的偏差, 并依此提取了射频指纹进行设备识别. 文献[38]建议利用 RFID 的天线和电荷泵引入的容差来提取指纹识别 RFID 设备. 然而, LTE 设备等相对复杂的无线通信设备难以抽离出特定的器件容差, 一般利用整体的电路容差作为射频指纹. 如果对于这些相对复杂的设备, 也能够确定哪一部分器件是整体差异的主要来源, 不管是对于攻击还是防护, 都将会发挥巨大的作用, 这也是该领域未来可研究的方向之一.

2.4 可识别信号的检测与截取

无线通信设备的通信信号遵从各种不同的标准, 可以通过截取一段信号来进行射频指纹的提取, 这段目标信号被定义为“可识别信号”. 如图 3 所示是一个典型的 WiFi 无线通信信号, 主要包括三部分: 信道噪

声段、瞬态信号段和稳态信号段. 其中,“信道噪声段”是指接收机未采集到通信信号的信号段, 主要由信道噪声和设备噪声构成. “瞬态信号段”是指接收到的发射机功率从零到达额定功率时发送的信号段, 这段信号不包含任何数据信息, 只与设备的硬件特征相关, 因此具有可比性, 可以用作“可识别信号”来提取射频指纹区分不同的发射机. “稳态信号段”是指无线发射机在功率稳定下发送的信号部分, 这部分信号是具体符号数据的调制波形. 若接收机已知部分先验的符号信息, 可以通过比较不同发射机的频偏、前导、调制特征等信息来区分信号, 因此具有一定先验信息的稳态信号段也可以作为可识别信号.

系统需要精确检测可识别信号的起始与结束, 才能截取可识别信号用作后续的射频指纹变换、特征提取与分类识别. 当射频指纹不具备时间平移不变性时, 可识别信号的检测与截取精度将直接影响最后的分类识别性能. 文献[39]就瞬态检测误差对最终分类性能的影响做了详细的分析, 结果显示检测精度对分类结果有着极大的影响. 因此, 可识别信号的检测与截取是射频指纹提取与识别系统中至关重要的一个环节, 早期的许多工作也都围绕着可识别信号的检测展开.

早在 1997 年, Shaw 等人[40]提出了基于信号幅度的门限检测方法, 该门限方法对于噪声十分敏感, 并且需要预先设定门限值, 在信噪比较低时精度较低. 1999 年, Ureten 等人[24]提出了基于信号幅度变化的 Bayesian 阶跃变点检测方法, 与门限检测方法不同, Bayesian 阶跃变点检测方法不需要设定门限, 仅利用信号的变化特征进行检测, 对于阶跃信号的检测效果较好. 然而, 由于 WiFi 等信号在设计时为了防止设备开关时功率扩散到相邻信道, 一般采用功率渐升的方法达到额定功率, 并在功率未升至额定功率时就开始前导的发送, 该方法针对这类信号效果较差. 因此, 2005 年, Ureten 等人[41]又提出了 Bayesian 渐升变点检测方法来检测功率渐升的瞬态信号. 2008 年, Suski 等人[42]提出了利用信号的瞬时幅度、瞬时相位的方差轨迹(variance trajectory, VT)来进行可识别信号的检测, 实验结果显示基于幅度的方差轨迹检测更加有效. 2009 年, Klein 等人提出了 Fractal-Bayesian 阶跃检测, 这种方法先对信号进行分形维数的计算, 再对分形维数进行 Bayesian 阶跃变点检测[43]. 此后, 对于可识别信号的检测研究渐少, 大部分文献中的检测方法也都是基于上述几种方法实现的. 直到 2015 年, 国防科大的袁英俊等人又提出了一种新型的检测方法. 由于排列熵(permutation entropy, PE)能够度量时间序列的复杂性, 该方法基于信号序列与噪声序列的排列熵的差异, 用广义似然比检验来检测捕获信号的信号起始点. 该方法即避免了阈值的设置, 又能同时应用于阶跃信号和功率渐升信号, 实验结果显示, 该方法在低信噪比下仍然能有效工作[44].

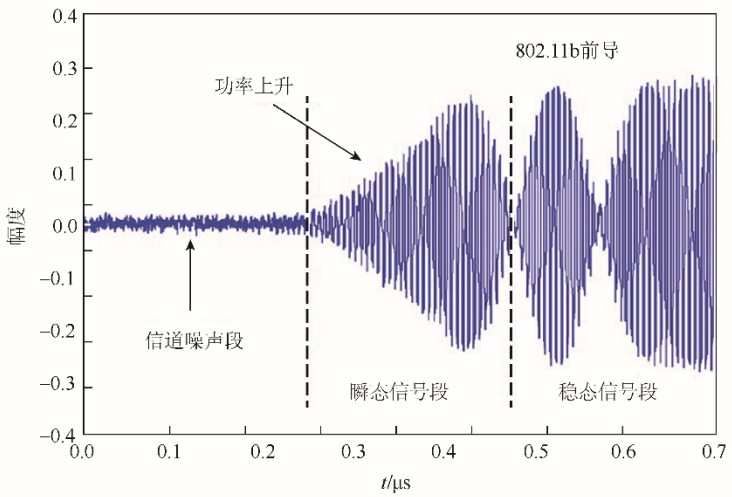


图 3 典型的 WiFi 波形[45]

Figure 3 Typical WiFi waveform

瞬态信号通常持续时间极短, 一般在纳秒级或亚微秒级, 如图 3 所示的瞬态信号持续时间约为 220 ns. 因此基于瞬态信号的射频指纹提取和识别方法对于可识别信号的检测精度要求极高, 从而导致检测成本较高. 而稳态信号的持续时间相对较长, 一般都在微秒级以上, 检测精度相对要求较低.

2.5 可识别信号的特征提取

可识别信号本身就是一种射频指纹, 但这种指纹包含的冗余信息过多, 维数太大, 识别阶段计算量巨大, 导致识别效率不足. 因此, 需要先去除可识别信号中无关和冗余信息, 尽可能多的保留设备特征, 这本质上就是一个信号降维的过程.

针对可识别信号, 可以根据其时域波形直接提取特征. 例如文献[14]提出将信号波形的分形维数作为特征. 文献[46]更是将开启瞬态信号的持续时间这样简单的一维特征作为设备的指纹. 文献[47]根据时间同步函数时间戳来计算 AP 的频偏作为特征.

此外, 也可以对可识别信号先进行变换域的处理然后再提取特征. 如文献[37]和文献[48]提出对可识别信号先做 Hilbert 变换, 计算其瞬时幅度、瞬时相位和瞬时频率, 再提取标准差、方差、峰态系数和偏态系数等统计特征作为射频指纹. 文献[49]提出对可识别信号进行 Fourier 变换提取频谱特征, 文献[29]中计算信号的功率谱密度作为射频指纹也是同样的思想. 文献[23]和文献[50]将可识别信号变换到小波域, 再提取小波系数作为射频指纹. 文献[51]更是考虑到离散小波变换没有时移不变性, 若可识别信号的检测误差稍大, 小波系数会发生巨大变化, 故提出利用几乎时间平移不变的双树复小波变换(DT-CWT)的小波系数作为设备指纹. 文献[52]提出将信号变换到调制域, 进行调制域星座点参数的提取, 如 I/Q 原点偏移等特征. 如图 4 所示总结了可识别信号可以提取的部分特征.

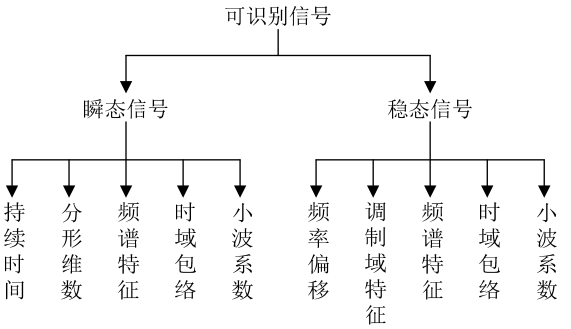


图 4 可识别信号特征分类
Figure 4 Features of identification signals

2.6 射频指纹特点

无线通信设备的射频指纹是针对可识别信号提取的一个或多个特征的集合, 用来识别发射源. 在实际应用时, 射频指纹应具备如下特点:

(1) 射频指纹的通用性. 通用性包括两个方面: 首先是指射频指纹对于发射机的通用性, 即面向的同一类设备均能用这种方法提取出要求的射频指纹; 另一方面则是指接收机的通用性, 即射频指纹不随射频指纹系统中接收机的改变而改变, 射频指纹仅最大限度地包含与待识别无线发射机相关的特征. 射频指纹具备通用性是射频指纹能够广泛应用的前提.

(2) 射频指纹的唯一性. 正如“世界上没有两片完全相同的树叶”, 不同无线设备发送的射频信号也是不同的. 尽管数字化接收过程中的采样和量化一定程度上模糊了接收信号间的差异, 然而我们根据可识别信号提取出的射频指纹仍应该具备唯一性, 这样设备才能进行准确的区分. 其中, 如何识别同一型号同一系列的无线发射机是一个难点. 这类设备之间的差异相对较小, 信号间的细微差别很容易被噪声淹没, 如

何保证提取的射频指纹具有唯一性是一个至关重要的问题.

(3) 射频指纹的短时不变性. 由于设备存在器件老化问题, 长时间的积累会引起器件参数的退化老化效应, 从而导致实时提取的射频指纹与一开始登记入库的射频指纹存在差异, 但射频指纹至少应该保持短时不变性. 文献[52]显示, 五个月时间内, 该文献中针对 WLAN 网卡提取的射频指纹仍然保持一致性, 设备的分类识别性能保持稳定. 至于更长时间以及针对不同设备的射频指纹是否仍具有时不变性还有待进一步的研究.

(4) 射频指纹的独立性. 所谓的独立性是指从承载数据的稳态信号段提取出的射频指纹应与承载的数字信息无关, 只与设备的硬件特征有关. 针对发送不同数据的信号, 提取出来的设备指纹应该是相同的.

(5) 射频指纹的稳健性. 文献[49]的实验结果表明: 发射机和接收机的距离变化、电压和温度的变化、天线的极化方向变化等因素会对提取的射频指纹产生影响, 最终影响识别性能. 射频指纹的稳健性是指射频指纹在对抗时变无线多径信道、收发机距离改变、天线极化方向变化、电压变化、温度变化、功率变化、噪声及干扰等保持的一致性. 简而言之, 就是提取的设备射频指纹应该与通信环境的改变及设备工作环境的变化无关, 稳健的射频指纹能使射频指纹识别系统更加可靠.

2.7 射频指纹分类

射频指纹的分类过程主要分为登记和识别两个过程. 首先, 将目标网络内的所有设备进行射频指纹的提取, 登记入库, 与对应的设备 ID 号链接在一起, 构成一个设备对照射频指纹库. 然后, 识别系统通过匹配待识别设备的射频指纹和库中对照指纹, 根据具体应用的具体要求, 给出一个允许/不允许接入的认证结果, 或者给出一个与库中所有对照指纹相似度的一个识别结果, 具体的判决可人为完成. 具体识别的算法可以采用简单的距离度量或者更加复杂的模式识别算法, 例如神经网络、支持向量机(SVM)等. 具体的分类识别算法依据具体信号提取的射频指纹和具体应用的要求而定, 本文不做详细的展开, 可以参考文献[53]和文献[54].

3 射频指纹提取和识别研究现状

与大多数技术相同, 射频指纹提取与识别技术也是来源于军用技术, 最早可以追溯到二战时期的敌我雷达识别[55], 主要通过直接比较接收信号的波形图和我方雷达已经登记的波形图来进行敌我判断. 然而, 随着设备的增多和生产工艺的提升, 直接比较信号波形这种方法已经不切实际. 早在 1995 年左右, Choe 等人和 Toonstra 等人开始研究提取设备通信信号的特征来识别和检测非法操作的 VHF FM 发射机[15,21]. 随后, 大量的射频指纹技术开始得到研究, 涌现出各种各样的射频指纹提取和识别方法. 本节总结了现有的一些射频指纹提取和识别方法, 根据可识别信号的分类, 分成瞬态信号射频指纹技术和稳态信号射频指纹技术两个部分进行论述.

3.1 瞬态信号射频指纹技术

瞬态信号射频指纹技术是指根据开启/关闭瞬态信号提取设备射频指纹, 主要是利用开启瞬态信号, 即发射机功率从零到达额定功率时发送的信号部分. 这部分信号不承载任何数据信息, 只与发射机硬件特征相关, 具有数据独立性. 其持续时间极为短暂, 一般在纳秒级, 在射频指纹提取前, 要对信号进行极为精确的起始点检测与瞬态信号截取[39].

最早的射频指纹技术就是 1995 年 Toonstra 和 Kinsner 提出的基于瞬态信号的特征提取方法, 早期的研究也都围绕瞬态信号射频指纹技术展开. Toonstra 等人在文献[21]中提出对捕获的 VHF FM 瞬态信号进行多分辨率小波分析, 用小波系数来刻画瞬态信号的特征, 作为发射机的射频指纹, 然后用遗传算法和神经网络对设备进行分类. 通过加入模拟的高斯噪声来调节信噪比, 实验结果显示在 20dB 信噪比以上时, 该方法能有效识别来自于四个厂家的 7 个不同的 VHF FM 发射机.

同年, Choe 等人在文献[15]中提出了一种自动、快速的设备识别方法, 该方法将瞬态信号变换到小波

域提取多分辨率的特征(包括统计特征和能量特征)作为射频指纹, 利用人工神经网络(ANN)进行分类器的设计, 实现了对三个射频发射机的有效分类.

1997 年, Shaw 等人在文献[40]中首次提出了采用瞬态信号的多重分形轨迹作为射频指纹, 利用基于信号幅度的多重分段分形维数的门限检测方法来检测瞬态信号的开始并进行信号的分离, 用概率神经网络(PNN)来进行分类, 获得了 92.5%的分类准确率.

2001 年, Ellis 等人在文献[56]中研究了 28 个 VHF FM 发射机发送的瞬态信号的特点, 根据瞬态信号的复包络, 分析了信号的瞬时幅度、瞬时相位和瞬时频率, 讨论了特征的唯一性、时不变性和通用性. 其通过人眼观察, 发现同一厂家同一型号的设备的波形特征比较相似, 人眼很难区分. 同时, 作者提出需要进一步量化环境因素的影响, 例如多普勒频移、多径衰落、工作温度等因素.

2004 年, Tekbaş 等人在文献[25]中就环境的影响做了一定的研究. 通过改变设备供电电压(从 9V 到 15V)和改变房间温度(从-10℃到 20℃)研究了 10 个 VHF FM 发射机的瞬态信号射频指纹变化. 该文章采用信号的幅度特征和相位特征作为射频指纹. 实验结果表明, 射频指纹会随着供电电压和工作环境温度的变化而变化. 该文献采用概率神经网络(PNN)进行射频指纹的分类, 实验结果显示需要在不同温度和不同工作供电电压下进行训练, 才能达到较好的识别性能, 平均分类误差在 5%左右. 同时, 该文的作者在同年的文献[26]中指出可以通过在训练阶段估计信噪比和进行信噪比的修正达到更好的分类效果.

除了早期研究的 VHF FM 发射机, 2003 年开始, Hall 等人开始关注蓝牙设备和 IEEE 802.11b 设备的射频指纹识别[14,57-59], 提出用高精度的频谱仪在近距离(10cm)采集来自 6 个不同厂家的 30 个 IEEE 802.11b 设备的瞬态信号, 提取瞬态信号的幅度、相位、同相分量、正交分量、功率以及离散小波变换(DWT)系数等特征. 第一次提出采用组合多个不同类型的特征作为设备的指纹, 最终达到了 8%的平均错误率. 同样的方法也被作者用于提取 10 个蓝牙设备的射频指纹和分类, 最终的性能也近乎相同. 此外, 考虑到设备的射频指纹可能会随工作环境的变化而变化, 作者首次提出定时更新设备对照射频指纹库.

2007 年, Rasmussen 等人在文献[46]中提出将射频指纹技术应用于无线传感网节点, 选用了工作在 433MHz 频段的同一厂家同一型号的 Chipcon 1000 无线设备进行研究. 选择瞬态信号持续时间、归一化幅度方差、载波信号的峰值数、抽取的第一段信号的离散小波变换系数以及归一化幅度的均值和最大值之差作为射频指纹. 在近距离进行瞬态信号的采集, 最终的平均分类误差却高达 30%, 显示出同一型号设备的分类难度大大增加.

2009 年, Danev 等人在文献[38]和文献[49]中对多跳无线传感网络中节点的射频指纹提取和识别做了进一步研究. 选择 50 个同一厂家同一型号的服从 IEEE 802.15.4 标准的 CC2420 作为待识别无线设备, 实验采用高精度的示波器进行瞬态信号采集, 待识别设备距离示波器 40 米. 选择提取瞬态信号的统计滤波 FFT 谱作为射频指纹, 利用马氏距离作为指纹相似性的度量, 最后的设备识别性能 EER 低达 0.0024(0.24%). 然而, 这么好的性能是在固定距离、固定天线极化方向、电压可变的情况下获得的, 一旦变化设备的位置和天线方向, 性能就会急剧下降, 这也反应了多径信道对提取设备指纹的影响. 因此根据采集信号提取出的射频指纹包含了信道指纹和设备指纹, 如何通过估计信道去除信道指纹提高设备指纹的稳定性是值得研究的一个问题.

总的来说, 瞬态信号射频指纹识别技术需要高精度的设备采集瞬态信号, 其中瞬态信号起始点的检测是关键研究点, 可以用来提取的特征主要有瞬态信号持续时间、频谱特征、小波域特征、分形维数以及包络特征等. 此外, 基于瞬态信号提取的指纹易受信道变化的影响, 相对稳态信号射频指纹更加脆弱.

3.2 稳态信号射频指纹技术

所有的通信信号都具有瞬态信号部分, 却不一定包含前导部分, 其稳态信号部分可能会发生变化, 并不一定能从每个信号都抽取出相同的可识别稳态信号. 因此, 早期射频指纹研究领域主要关注基于瞬态信号的射频指纹提取和识别技术. 然而, 相比于稳态信号, 瞬态信号由于其相对较短的持续时间, 瞬态检测

及可识别信号的截取需要较高的采样速率[17]. 因此, 基于瞬态信号的射频指纹技术如果要做到实时工作, 面临着许多困难. 另一方面, 随着技术的不断发展, 几乎所有的数字通信系统都在数据段之前加入了前导序列, 以便简化接收机的设计[30]. 稳定的前导提供了一个稳定的可识别稳态信号, 因此, 该领域的研究重心开始转向稳态信号射频指纹提取和识别技术.

2008 年, Kennedy 等人首次进行了基于稳态信号的射频指纹提取和识别研究. 将通用移动通信系统(Universal Mobile Telecommunications System, UMTS) 的前导信号变换为频谱作为射频指纹, 用于 UMTS 用户设备的识别. 实验室环境下, 当 SNR 为 15dB 时, 七个不同型号的 UMTS 用户设备能获得 91%的正确识别率; 而包含 10 个同一型号设备的共 20 个 UMTS 用户设备作为待识别对象时, 识别率为 85%[17].

2008 年, Suski 等人在文献[35]中提出用 OFDM 802.11a/g 设备前导信号的瞬时幅度和瞬时相位的方差轨迹来进行前导信号起始点检测, 抽取前导信号的功率谱密度(PSD)作为射频指纹, 用谱相关的方法来进行设备分类. 实验结果显示基于幅度的前导起始检测更有效. 其分类是针对三个设备进行的, 分类精度在 SNR 大于 6dB 时达到了 80%, 在低 SNR 时性能一般.

稳态信号的射频指纹主要是由发射机在信号调制阶段引入的特征构成的. 2008 年, Brik 等人设计了一个被动的射频设备识别系统(Passive RAdiometric Device Identification System, PARADIS)用来识别 IEEE 802.11b 设备, 主要是提取硬件容差引起的调制误差作为射频指纹来识别设备. 选用了调制信号的五个特征: 频偏、前导相关、I/Q 偏移、幅度误差和相位误差作为设备射频指纹. 系统测试了 138 个同一型号的无线网卡, 信号从 3 到 15 米的不同距离进行采集, 用 K 最近邻算法进行分类时分类误差为 3%, 用支持向量机进行分类时分类误差仅为 0.34%. 并且该文献声称对噪声、天线间距改变及硬件老化具备稳健性[52].

2011 年, Shi 等人采取了和 Brik 相似的方法提取射频指纹, 选用数据段信号的误差矢量幅度、载波中心频率偏差、OFDM 导频的相位偏差、符号时钟偏差、I/Q 偏移、I/Q 相位旋转、I/Q 增益不平衡以及前导相关等诸多调制域特征作为设备的射频指纹. 文中还比较了 MIMO 设备和 SISO 设备的识别性能, 发现 MIMO 设备的识别性能显著提升. 此外, 文中第一次提出用信息论的方法来研究哪些特征在区分设备时最有效[60].

2014 年, Peng 等人提出利用调制域的 I/Q 不平衡作为设备射频指纹进行协同中继系统的中继认证和识别, 采用双参数假设检验和似然比检验的方法进行认证, 最后用数值仿真进行了验证, 结果显示认证性能有显著提升[61].

2015 年, Knox 等人利用 Ettus Labs USRP1 软线无线电平台作为接收设备, 以 4M 的采样速率对来自同一厂家的五个 SiLabs IEEE 802.15.4 2.4GHz 的射频设备进行信号采集和解调. 为了减小噪声的影响, 该文首先将采集的信号用一个噪声滤波器进行了筛选, 然后提取解调后基带信号的相位信息作为射频指纹. 实验研究了这种射频指纹在不同温度、不同信道环境下长时的分类性能. 结果显示, 在短距离的实际信道环境下, 平均分类准确率为 99.6%; 在中距离信道下, 平均分类准确率为 95.3%; 在远距离信道下, 平均分类准确率为 81.9%. 实验结果还指出在固定信道下, 分类性能在 12 小时时间内的变化总是小于 8%(通常小于 2%)[62].

2015 年, 袁英俊等人提出将发射机建模成非线性动力系统, 利用相空间重构的方法选取重构相空间的两类特征共 30 个特征作为 RFF, 利用主成分分析方法和支持向量机分类器对四个无线网卡进行识别, 每个网卡 100 个信号, 1:1 进行训练测试, 实验结果显示在信噪比 10dB 以上时, 正确率达到 94%以上[63].

总之, 由于基于稳态信号的射频指纹携带无线设备发射机的更多硬件信息, 因而取得了更好的识别性能. 然而, 上述文献声称的识别性能都是在一定的实验条件下获得的, 这些实验条件离真正的应用还有距离, 并且还有许多影响射频指纹稳定性的因素没有得到深入的研究. 因此, 无线通信设备的射频指纹提取和识别仍然是一个困难的问题.

4 系统性能评估方法

构建射频指纹提取和识别系统后, 如何评估系统性能是一个重要议题, 具体的性能指标更是系统设计时需要考虑的重要因素之一. 射频指纹系统最主要的系统指标就是系统的识别准确度, 其不能通过理论计算获得, 需要通过设备的大量测试信号来统计估计具体数值. 此外, 由于射频指纹系统和传统的生物指纹识别系统本质上是相同的, 因此可以采用现有的一些准确度指标来进行度量.

首先, 用来评估系统性能最简单的系数就是分类准确率. 故名思议, 就是正确识别的概率, 与之相反的指标则是平均错误率(Average error rate), 就是指错误分类的样本数占总样本数的比例. 这是对识别系统总体分类性能的一个粗略评估, 但其不会区分下面将要介绍的两个评估指纹识别系统的主要参数——拒真率 FRR(False Rejection Rate)和认假率 FAR(False Acceptance Rate).

拒真率 FRR 指的是“把应该相互匹配成功的指纹当成不能匹配的指纹”的概率, 也就是已经登记的设备自己和自己比不认可的概率. 例如, 用同一个已登记设备的 100 个采样信号提取设备射频指纹进行匹配. 由于即使是同一设备发出的相同规格的信号也会受周围环境和电压纹波等内部因素略有变化, 其实时提取的射频指纹也会略有不同. 如果将匹配的阈值设定为 90%, 即如果有 90 个信号提取出的射频指纹与该设备的库中对照指纹相似度足够, 则认为是同一个设备. 那么, 假设这里有 10 次比较, 7 次大于 90%, 3 次小于 90%, 就是说有 3 次匹配不成功, 那么 FRR 就是 3/10=30%. 拒真率与设定的匹配门限相关.

认假率 FAR 也叫误判率,是用来评估指纹识别算法性能的最重要参数, 指的是“把不应该匹配的指纹当成匹配的指纹”的概率, 通常是指其他设备被误认为已登记设备 A 的概率, 这里的其他设备可以是其他已经登记的设备, 也可以是未登记的设备. FAR 与 FRR 比较而言, FRR 是自己和自己比, 而 FAR 则是其他设备和自己比. 沿用上面的例子, 假设总共有 100 个设备, 每个设备有 100 个采样信号, 其余 99 个设备的每个采样信号提取的射频指纹都要依次和设备 A 的库内对照射频指纹进行匹配. 匹配阈值仍设为 90%, 每个设备比较 100 次, 于是是否匹配的比较次数为 100*99=9900 次. 如果有 99 次成功匹配, 则认为设备 A 的认假率 FAR 为 99/9900=1%. 同理可求整体识别系统的平均认假率.

在同一个指纹库中, 对同一个算法来讲, 需要设定一个阈值, 作为判定相似的标准. 当相似度大于这个阈值时, 表示匹配成功, 否则表示匹配失败. FRR 是随阈值增大而增大的, 即判定相似的门槛值越高, 则授权设备被认定是非授权设备的几率越大. 反之, FAR 是随阈值增大而减小的, 即随着判定相似度的门槛值越高, 把非授权设判定为授权设备的概率会越小.

EER(Equal Error Rate)是相等错误率的意思, 主要用于评价指纹算法整体效能. 也就是把 FAR、FRR 两个参数统一为一个参数, 来衡量指纹算法的整体性能. 将 FAR 和 FRR 两个评估参数放在同一个坐标中, 构成一个 ROC(Receiver Operating Characteristic)曲线. 其中, FAR 是随阈值增大而减小的, FRR 是随阈值增大而增大的, 两者之间有一个交点. 这个点是在某个阈值下的 FAR 与 FRR 等值的点, 通常用这一点 EER 的值来衡量算法的综合性能. 把 FAR 和 FRR 曲线都向下平移, 则相交点 EER 也向下平移. 因此, EER 值越小表示系统的整体识别性能越高.

此外, 为了保证不会过度学习, 通常采用 k-折交叉验证(k-fold cross-validation)来进行上述性能评估参数的获得. 即将测试信号集分成 k 个不相交的子集, 一个作为训练, 其余 $k-1$ 个作为测试, 这样做 k 次评估, 从而保证不会过度学习.

另外, 由于我们采用的接收设备可能是示波器等高精度设备, 而不是普通的接收设备, 应该要先丢弃一些普通接收设备会丢弃的已不符合标准的数据帧(可能已经在传输过程中过度失真), 再进行待识别设备的射频指纹识别, 从而提高评估性能的合理性[41]. 我们除了考虑到系统对于此类异常情况的处理, 在具体评估时还应该综合考虑系统的构建成本、指纹的提取与匹配速度等因素.

5 总结与展望

随着无线网络的不断发展和安全威胁的与日俱增, 基于射频指纹的物理层安全增强方法得到了越来越多的重视. 射频指纹技术可以应用于大多数现存无线通信设备的识别和认证阶段, 拥有着广阔的应用场景. 然而, 无线通信设备的射频指纹提取和识别技术虽然在过去的十几年里得到了越来越多的关注和研究, 但在实际应用中还存在许多问题和挑战:

(1) 不同设备射频指纹的产生机理有待深入研究. 通过对不同设备进行详细的建模分析, 分析设备内哪些器件引入了容差、容差的具体大小、对射频指纹的影响程度等因素. 通过进一步的深入分析, 能更加针对性地提取特征, 从理论上指导特征加权系数的分配, 而不单单是依靠具体实验的调整.

(2) 克服无线多径信道对射频指纹的不利影响. 系统采集信号后进行预处理, 尽可能地还原发送信号, 以便提取发射机的设备指纹. 然而, 最终提取的指纹中还是不可避免的包含了信道指纹. 由于无线多径信道具有时变性, 这就会导致提取的设备指纹缺乏稳定性. 如何消除或减弱信道指纹仍是需要研究的问题.

(3) 射频指纹的提取问题. 根据同一设备发射的通信信号, 可以选择不同的信号段作为可识别信号. 可以从不同的视角, 进行可识别信号的域变换. 针对变换后的射频指纹, 还可以采用不同的特征提取方法. 采用何种变换和特征提取方法提取设备射频指纹能够尽可能多的包含待识别发射机的硬件信息, 也是需要进一步研究的问题.

(4) 射频指纹的稳健性. 设备器件老化等问题会导致射频指纹的长期稳定性不足. 同时, 设备工作环境的变化如设备所在位置的变化、电压和温度的变化、天线的极化方向变化等也可能会导致设备射频指纹的变化. 如何解决这些问题, 提高设备指纹的稳健性也有待研究. 此外, 能否利用射频指纹变化来进行设备的远程监控也是值得研究的环节. 当然, 如何对射频指纹不可避免的老化进行管理也有待进一步探讨.

(5) MIMO 设备的射频指纹的研究. 随着多天线设备的发展, 如何从多天线设备的通信信号中提取更多的设备信息作为设备指纹也有待研究.

(6) 设备识别的安全和隐私问题. 随着射频指纹识别技术的不断发展, 针对该技术的攻击方法也开始有了初步的研究. 现有的射频指纹技术主要对重放攻击和中间人攻击较为脆弱, 如何抵抗这些攻击也是需要进一步研究的. 另外, 射频指纹技术可能存在用户隐私侵犯的问题. 例如, 如果在手机卖给用户前提前进行设备射频指纹的提取, 利用射频指纹对用户进行定位和追踪, 这也是可能存在的隐私侵犯问题. 随着射频指纹技术的不断发展, 如何保护隐私也值得更深入的研究.

总而言之, 本文详细综述了无线通信设备的射频指纹提取和识别方法, 回顾了射频指纹技术过去二十年的发展, 归纳了基于通信信号提取射频指纹进行设备识别的典型流程. 随后, 本文对射频指纹的产生机理、可识别设备的类型以及识别系统的各个流程依次做了介绍, 并对射频指纹的特点做了一定的归纳. 本文还总结了现有的基于瞬态信号和稳态信号的射频指纹技术的典型研究, 简单分析了两种技术的不同之处. 此外, 本文对于如何评估射频指纹识别系统的性能也做了一定的论述. 最后, 本文指出了射频指纹的提取和识别技术中存在的一些急需解决和有待研究的问题.

References

[1] YUAN H L. Research on physical-layer authentication of wireless network based on RF fingerprinting[D]. Southeast University, 2011.
袁红林. 基于射频指纹的无线网络物理层认证关键技术研究[D]. 东南大学,2011.
[2] CHAABOUNI R. Break wep faster with statistical analysis[R]. 2006.
[3] MAVRIDIS I P, ANDROULAKISA I E, HALKIAS A B, et al. Real-life paradigms of wireless network security attacks[C]. In: 15th Panhellenic Conference on Informatics (PCI), 2011. IEEE, 2011: 112–116.
[4] FRANKLIN J, MCCOY D, TABRIZ P, et al. Passive data link layer 802.11 wireless device driver fingerprinting[C]. In: Usenix Security. 2006.

[5] BRATUS S, CORNELIUS C, KOTZ D, et al. Active behavioral fingerprinting of wireless devices[C]. In: Proceedings of the First ACM Conference on Wireless Network Security. ACM, 2008: 56–61.
[6] DESMOND L C C, YUAN C C, PHENG T C, et al. Identifying unique devices through wireless fingerprinting[C]. In: Proceedings of the First ACM Conference on Wireless Network Security. ACM, 2008: 46–55.
[7] GAO K, CORBETT C, BEYAH R. A passive approach to wireless device fingerprinting[C]. In: IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2010. IEEE, 2010: 383–392.
[8] NGUYEN N T, ZHENG G, HAN Z, et al. Device fingerprinting to enhance wireless security using nonparametric Bayesian method[C]. In: INFOCOM, 2011 Proceedings IEEE. IEEE, 2011: 1404–1412.
[9] POLAK A C, GOECKEL D L. Wireless device identification based on RF oscillator imperfections[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2492–2501.
[10] REISING D R, TEMPLE M A, JACKSON J A. Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(6): 1180–1192.
[11] POLAK A C, GOECKEL D L. Identification of wireless devices of users who actively fake their RF fingerprints with artificial data distortion[J]. IEEE Transactions on Wireless Communications, 2015, 14(11): 5889–5899.
[12] WANG W, SUN Z, PIAO S, et al. Wireless physical-layer identification: modeling and validation[J]. IEEE Transactions on Information Forensics & Security, 2015, 11(9): 2091–2106.
[13] GUNGOR O, KOKSAL C E. On the basic limits of RF-fingerprint-based authentication[J]. IEEE Transactions on Information Theory, 2016, 62(8): 1–1.
[14] HALL J, BARBEAU M, KRANAKIS E. Detection of transient in radio frequency fingerprinting using signal phase[J]. Wireless and Optical Communications, 2003: 13–18.
[15] CHOE H C, POOLE C E, ANDREA M Y, et al. Novel identification of intercepted signals from unknown radio transmitters[C]. In: SPIE's 1995 Symposium on OE/Aerospace Sensing and Dual Use Photonics. International Society for Optics and Photonics, 1995: 504–517.
[16] NEUMANN C, HEEN O, ONNO S. An empirical study of passive 802.11 device fingerprinting[C]. In: 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), 2012. IEEE, 2012: 593–602.
[17] KENNEDY I O, SCANLON P, MULLANY F J, et al. Radio transmitter fingerprinting: A steady state frequency domain approach[C] In: 68th Vehicular Technology Conference, 2008. IEEE, 2008: 1–5.
[18] REHMAN S U, SOWERBY K, COGHILL C, et al. The analysis of RF fingerprinting for low-end wireless receivers with application to IEEE 802.11 a[C]. In: 2012 International Conference on Selected Topics in Mobile and Wireless Networking (iCOST). IEEE, 2012: 24–29.
[19] REHMAN S U, ALAM S, ARDEKANI I T. An overview of radio frequency fingerprinting for low-end devices[J]. International Journal of Mobile Computing and Multimedia Communications (IJMCMC), 2014, 6(3): 1–21.
[20] PATEL H, TEMPLE M, RAMSEY B W. Comparison of high-end and low-end receivers for RF-DNA fingerprinting[C]. In: IEEE Military Communications Conference (MILCOM), IEEE, 2014: 24–29.
[21] TOONSTRA J, KINSNER W. Transient analysis and genetic algorithms for classification[C]. In: IEEE WESCANEX 95. Communications, Power, and Computing. IEEE, 1995: 432–437.
[22] TOONSTRA J, KINSNER W. A radio transmitter fingerprinting system ODO-1[C]. In: Canadian Conference on Electrical and Computer Engineering, 1996. IEEE, 1996, 1: 60–63.
[23] HIPPENSTIEL R D, PAYAL Y. Wavelet based transmitter identification[C]. In: Fourth International Symposium on Signal Processing and Its Applications, 1996. IEEE, 1996, 2: 740–742.
[24] URETEN O, SERINKEN N. Detection of radio transmitter turn-on transients[J]. Electronics Letters, 1999, 35(23): 1996–1997.
[25] TEKBAŞ Ö H, SERINKEN N, ÜRETEN O. An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions[J]. Canadian Journal of Electrical and Computer Engineering, 2004, 29(3): 203–209.
[26] TEKBAŞ Ö H, ÜRETEN O, SERINKEN N. Improvement of transmitter identification system for low SNR transients[J]. Electronics Letters, 2004, 40(3): 182–183.
[27] REISING D R, TEMPLE M A, MENDENHALL M J. Improving intra-cellular security using air monitoring with RF fingerprints[C]. In: IEEE Wireless Communications and Networking Conference (WCNC), 2010. IEEE, 2010: 1–6.
[28] WILLIAMS M K D, TEMPLE M A, REISING D R. Augmenting bit-level network security using physical layer RF-DNA fingerprinting[C]. In: IEEE Global Telecommunications Conference (GLOBECOM), 2010. IEEE, 2010: 1–6.
[29] WILLIAMS M K D, MUNNS S, TEMPLE M A, et al. RF-DNA fingerprinting for airport WiMax communications security[C]. In: 4th International Conference on Network and System Security (NSS), 2010. IEEE, 2010: 32–39.
[30] SCANLON P, KENNEDY I O, LIU Y. Feature extraction approaches to RF fingerprinting for device identification in femtocells[J]. Bell Labs Technical Journal, 2010, 15(3): 141–151.

[31] DEMERS F, ST-HILAIRE M. Radiometric identification of LTE transmitters[C]. In: IEEE Global Communications Conference (GLOBECOM), 2013. IEEE, 2013: 4116–4121.
[32] MONDAL R, TURKKA J, RISTANIEMI T, et al. Performance evaluation of MDT assisted LTE RF fingerprint framework[C]. In: Seventh International Conference on Mobile Computing and Ubiquitous Networking (ICMU), 2014. IEEE, 2014: 33–37.
[33] KIM K, SPOONER C M, AKBAR I, et al. Specific emitter identification for cognitive radio with application to IEEE 802.11[C]. In: IEEE Global Telecommunications Conference, 2008. IEEE, 2008: 1–5.
[34] ZANETTI D, DANEV B. Physical-layer identification of UHF RFID tags[C]. In: Proceedings of the 16th Annual International Conference on Mobile Computing and Networking. ACM, 2010: 353–364.
[35] SUSKI W C, TEMPLE M A, MENDENHALL M J, et al. Using spectral fingerprints to improve wireless network security[C]. In: IEEE Global Telecommunications Conference, 2008. IEEE, 2008: 1–5.
[36] DUBENDORFER C K, RAMSEY B W, TEMPLE M. An RF-DNA verification process for ZigBee networks[C]. In: Military Communications Conference, 2012. IEEE, 2012: 1–6.
[37] PATEL H J, TEMPLE M, BALDWIN R O. Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting[J]. IEEE Transactions on Reliability, 2015, 64(1): 221–233.
[38] DANEV B, HEYDT-BENJAMIN T S, CAPKUN S. Physical-layer identification of RFID devices[C]. In: Usenix Security Symposium. 2009: 199–214.
[39] KLEIN R W, TEMPLE M A, MENDENHALL M J, et al. Sensitivity analysis of burst detection and RF fingerprinting classification performance[C]. In: IEEE International Conference on Communications, 2009. IEEE, 2009: 1–5.
[40] SHAW D, KINSNER W. Multifractal modelling of radio transmitter transients for classification[C]. In: IEEE WESCANEX 97: Communications, Power and Computing. IEEE, 1997: 306–312.
[41] URETEN O, SERINKEN N. Bayesian detection of Wi-Fi transmitter RF fingerprints[J]. Electronics Letters, 2005, 41(6): 373–374.
[42] SUSKI W C, TEMPLE M A, MENDENHALL M J, et al. Using spectral fingerprints to improve wireless network security[C]. In: IEEE Global Telecommunications Conference, 2008. IEEE, 2008: 1–5.
[43] KLEIN R W, TEMPLE M A, MENDENHALL M J, et al. Sensitivity analysis of burst detection and RF fingerprinting classification performance[C]. In: IEEE International Conference on Communications, 2009. IEEE, 2009: 1–5.
[44] YUAN Y J, WANG X, HUANG Z T, et al. Detection of radio transient signal based on permutation entropy and GLRT[J]. Wireless Personal Communications, 2015, 82(2): 1047–1057.
[45] URETEN O, SERINKEN N. Wireless security through RF fingerprinting[J]. Canadian Journal of Electrical and Computer Engineering, 2007, 32(1): 27–33
[46] RASMUSSEN K B, CAPKUN S. Implications of radio fingerprinting on the security of sensor networks[C]. In: Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007. IEEE, 2007: 331–340.
[47] JANA S, KASERA S K. On fast and accurate detection of unauthorized wireless access points using clock skews[J]. IEEE Transactions on Mobile Computing, 2010, 9(3): 449–462.
[48] REISING D R, TEMPLE M, JACKSON J. Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(6): 1180–1192.
[49] DANEV B, CAPKUN S. Transient-based identification of wireless sensor nodes[C]. In: Proceedings of the 2009 International Conference on Information Processing in Sensor Networks. IEEE, 2009: 25–36.
[50] BERTONCINI C, RUDD K, NOUSAIN B, et al. Wavelet fingerprinting of radio-frequency identification (RFID) tags[J]. IEEE Transactions on Industrial Electronics, 2012, 59(12): 4843–4850.
[51] KLEIN R W, TEMPLE M A, MENDENHALL M J. Application of wavelet denoising to improve OFDM-based signal detection and classification[J]. Security and Communication Networks, 2010, 3(1): 71–82.
[52] BRIK V, BANERJEE S, GRUTESER M, et al. Wireless device identification with radiometric signatures[C]. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. ACM, 2008: 116–127.
[53] DUDA R O, HART P E, STORK D G. Pattern Classification[M]. John Wiley & Sons, 2012.
[54] BISHOP C M. Pattern Recognition and Machine Learning[M]. Springer, 2006.
[55] DANEV B, ZANETTI D, CAPKUN S. On physical-layer identification of wireless devices[J]. ACM Computing Surveys, 2012, 45(1): 1–29.
[56] ELLIS K, SERINKEN N. Characteristics of radio transmitter fingerprints[J]. Radio Science, 2001, 36(4): 585–597.
[57] HALL J, BARBEAU M, KRANAKIS E. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting[C]. In: Communications, Internet, and Information Technology. 2004: 201–206.

[58] BARBEAU M, HALL J, KRANAKIS E. Detection of rogue devices in bluetooth networks using radio frequency fingerprinting[C]. In: Proceedings of the 3rd IASTED International Conference on Communications and Computer Networks, CCN. 2006: 4–6.

[59] HALL J, BARBEAU M, KRANAKIS E. Radio frequency fingerprinting for intrusion detection in wireless networks[J]. IEEE transactions on defendable and secure computing, 2005.

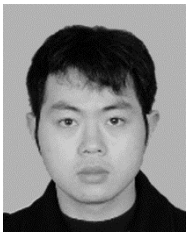
[60] SHI Y, JENSEN M. Improved radiometric identification of wireless devices using mimo transmission[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(4): 1346–1354.

[61] PENG H, XIANBIN W, BEHNAD A. Relay authentication by exploiting I/Q imbalance in amplify-and-forward system[C] In: IEEE Global Communications Conference (GLOBECOM), 2014. IEEE, 2014: 613–618.

[62] KNOX D A, KUNZ T. Wireless fingerprints inside a wireless sensor network[J]. ACM Transactions on Sensor Networks, 2015, 11(2): 1–30.

[63] YUAN Y, HUANG Z, WANG F, et al. Radio Specific Emitter Identification based on nonlinear characteristics of signal[C]. In: IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2015. IEEE, 2015: 77–81.

作者信息



俞佳宝(1992–), 浙江绍兴人, 2014年东南大学信息科学与工程学院攻读工学博士学位. 主要研究领域为物理层安全.
E-mail: yujiabao@seu.edu.cn

朱长明(1980–), 河南焦作人, 博士, 高工. 主要研究领域为信息安全.
E-mail:zhuchangming2003@126.com

姜禹(1981–), 江苏南京人, 博士, 讲师. 主要研究领域为无线网络安全.
E-mail: jiangyu@seu.edu.cn

胡爱群(1964–), 江苏人, 博士, 教授. 主要研究领域为无线通信安全.
E-mail: aqhu@seu.edu.cn

彭林宁(1984-), 江苏苏州人, 博士, 副研究员. 主要研究领域为物理层安全.
E-mail: pengln@seu.edu.cn