无线设备射频指纹识别方法研究

Research on Radio Frequency Fingerprint Identification Method for Wireless Devices

李英　韩鹏蕊

Ying Li　Pengrui Han

国家无线电监测中心检测中心　中国·北京 100041

The State Radio_monitoring_center Testing Center, Beijing, 100041, China

摘　要：在通信传输过程中，每一台无线设备的自身硬件特征都是独特的，不同设备的硬件差异会形成无线设备的独有指纹，并附加在传输的无线电信号上。射频指纹识别是指对于辐射源设备发出的无线信号进行特征提取，提取出可以作为辐射源设备唯一性的指纹特征，从而实现辐射源个体识别。射频指纹识别技术在通信领域中表现出了很大潜力，论文对射频指纹识别技术的研究现状进行了概述，并对无线设备射频指纹识别方法进行了归纳分类，最后讨论了射频指纹识别技术目前所面临的困难以及未来可能的研究方向，以期对射频指纹识别的研究与应用有所帮助。

Abstract: In the process of communication transmission, the hardware characteristics of each wireless device are unique. The hardware differences of different devices will form the unique fingerprint of the wireless device, and be attached to the transmitted radio signal. RF fingerprint identification refers to the feature extraction of the wireless signal issued by the radiation source equipment, and extracting the fingerprint features that can be used as the uniqueness of the radiation source equipment, so as to realize the individual identification of the radiation source. RF fingerprint identification technology in the great potential in communication, this paper summarizes the research situation of radio frequency fingerprint identification technology, and the wireless equipment radio frequency fingerprint identification method is classified, finally discusses the RF fingerprint identification technology currently facing difficulties and possible future research direction, in order to help the research and application of radio frequency fingerprint identification.

关键词：射频指纹识别；辐射源识别；硬件差异

Keywords: radio frequency fingerprint identification; radiation source identification; hardware difference

DOI: 10.12346/csai.v1i4.8164

1 引言

射频指纹识别技术在近年来广泛受到人们关注，由于不同设备之间存在硬件差异，可以从传输的信号中提取这种差异用于无线设备的识别。利用无线信号识别不同设备的方法最早应用于 1995 年 [1]，而“射频指纹”的概念是 2003 年由 Hall 等人提出 [2]，将这种通信设备硬件所产生的差异称为“射频指纹”。由于不同设备间的硬件差异属于物理层的本质特征，很难被修改，因此，射频指纹识别技术可以有效提高通信网络安全性。

射频指纹识别技术无论是在军事上还是民用上都有着非常广泛的应用。在军事上，变幻莫测的战场环境不仅为正常通信传输造成一定困扰，同时也使我们无法及时获取准确的战场情况。射频指纹识别技术的兴起可以让我们能够在敌我双方作战时快速准确地识别到敌方设备和传输信号，从而精准掌握敌方动态，有助于破解敌方战略部署，通过跟踪监视敌方设备有利于我方在战场上及时做出战略调整，从而在复杂的战场环境下掌握军事行动的主动权。

在民用中，射频指纹识别技术在很多领域都承担着不可忽视的作用，可以应用于工业中及时诊断出设备故障，提高生产效率。尤其是在通信网络的安全领域中发挥的作用更

【作者简介】李英（1995-），女，中国黑龙江大庆人，硕士，从事移动通信设备全球GCF、北美PTCRB一致性认证及运营商入库测试相关的项目管理研究。

大。近年来物联网发展迅猛，每一年的联网设备数量都急速增长。由于通信网络的开放性，无线网络安全问题也随之变得越来越严重。传统的提高互联网安全性能的方式通常是基于物理层之上的认证实现，比如在 MAC 层通过设置密码进行加密的方式进行设备身份认证。但是认证密码很容易通过软件被伪造，还存在密码泄露的风险，一旦密码泄露会造成更加严重的网络恶意攻击问题。而射频指纹是设备物理层固有属性，不易被篡改，对解决无线网络安全问题提高网络环境安全性具有重要意义。

2 射频指纹识别系统框架

通用的射频指纹识别系统框架如图 1 所示，主要包括信号采集、信号预处理、对采集的信号进行特征提取、特征降维以及最后的分类识别几部分。

①信号采集模块是指对辐射源发出的无线电信号进行收集，可进行信号采集的辐射源设备多种多样，例如通信传输中常见的商用 ZigBee 模块、Wi-Fi 设备、蓝牙设备，USRP 等。常用的采集装置有高端的示波器、频谱仪，以及低端的 USRP 等设备。

②信号预处理模块是对采集到的信号进行起始点检测和截取等操作，将信号截取成瞬态和稳态两部分，用于后续信号的特征提取。

③特征提取模块主要是对预处理之后的信号进行特征提取。特征提取的方法非常多，但总体上是根据信号类型分为基于瞬态信号和基于稳态信号的特征提取方法。

④特征降维模块主要是对提取的特征进行降维，以减轻对分类器造成的负担，加快识别速度。常用的降维方法是主成分分析方法（PCA），原理是找到一个超平面，使得所有数据点到该超平面的距离最近，以及所有数据点在该超平面上的投影尽量分散。

⑤分类识别模块是对特征提取和降维之后的特征进行识别和验证的过程，分为训练和测试两个阶段。训练阶段通过对已知的大量辐射源传输信号进行特征提取，构建射频指纹特征数据库，并与每个辐射源设备的类别进行关联。测试阶段则是对待检设备的信号进行相同步骤的特征提取，将提取的特征与射频指纹特征库中的样本进行匹配。最后通过特征距离测度等评估指标给出待检设备的真是类别。一般分类识别的结果可以表示为 1 对多的识别和 1 对 1 的验证。1 对多的识别问题是指对于某个待测设备，判别该设备属于指纹特征样本库中的哪一类设备，输出结果是该设备的类别。而 1 对 1 的验证则是对该设备声称的身份信息进行验证，从而判断出该设备是否是在射频指纹特征库中已登记的设备，最后给出允许接入或拒绝接入的判决结果。

3 射频指纹识别方法概述

射频指纹识别技术在近 30 年来经过了快速发展的阶段，目前已经逐渐成熟。在射频指纹识别过程中最重要的一步就是特征提取，目前普遍研究的特征提取方法包括基于瞬态信号的特征提取方法、基于稳态信号的特征提取方法和基于发射机非线性模型的特征提取方法。如图 2 所示。

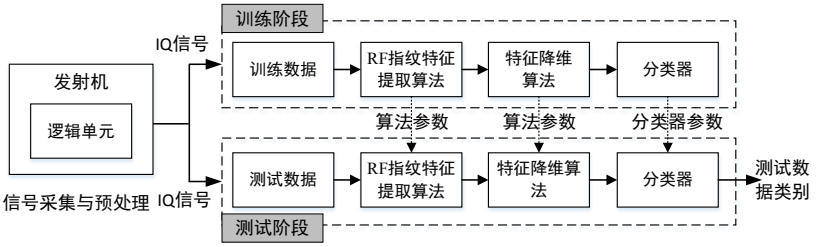

图 1 射频指纹识别系统框架

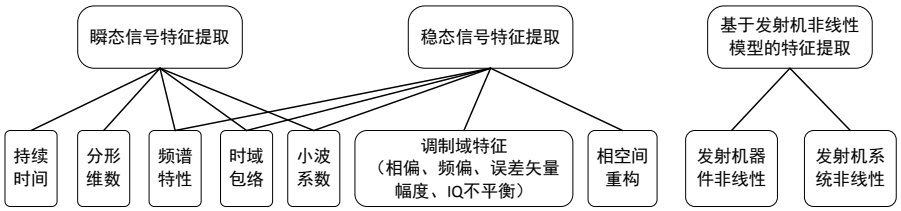

图 2 射频指纹特征提取方法

3.1 瞬态信号特征提取方法

瞬态信号是指辐射源设备从关机到开机状态的转换过程中产生的信号，所有的辐射源设备都具有瞬态信号段。在实际的通信传输过程中，瞬态信号是在实际数据包传输之前就已出现，在瞬态信号段中不包含传输的调制信号内容，也就不受信号数据部分的影响，因此瞬态信号段具有数据独立性。瞬态信号只与发射机内部硬件结构和设计有关，不同发射机产生的瞬态信号不同，由此可见瞬态信号可以用来表征发射机硬件特性，可以用在设备识别和故障诊断等领域 [3]。对瞬态信号提取特征通常从几个方面出发，包括直接以瞬态信号持续时间作为指纹特征、提取信号分形维数、从波形中提取时域包络特征 [4]、谱特征 [5]、小波特征 [6] 等。

除此之外，信号稀疏表示方法也是一种常用的分类识别方法，尤其是在文献中，作者提出了一种基于稀疏表示的分类方案，采集了发射机从开机到进行数据通信到关机的整个突发信号，并将其分为上升瞬态信号段、稳态信号段、下降瞬态信号三个区域。实验结果表明，使用多组信号段作为射频指纹的识别性能明显优于只使用一个信号段的结果。这篇文章具有启发性的一点是首次使用下降瞬态信号段作为射频指纹，该段区域信号此前从未被研究过。

基于瞬态信号的识别是建立在高精度信号采集装置以及精确的信号检测基础上，虽然不受传输数据的影响，但也对信道的鲁棒性较差。

3.2 基于稳态信号的特征提取方法

目前几乎所有投入使用的通信系统都会在数据包传输开始之前加入一段前同步码，也叫前导码，用来提醒接收机准备接收信号以及进行同步，这样能够很大程度上简化接收机的结构设计。由于稳态信号中承载着传输的调制信号，因此基于稳态信号的特征提取方法主要是基于前导码以及基于数据部分的特征提取。基于稳态信号的特征提取最早是在 2008 年由 Kennedy 等人提 Irwin O. </author><author>Scanlon, Patricia </author><author>Mullany, Francis J. </author><author>Buddhikot, Milind M. </author><author>Rondeau, Thomas W.</author></authors></contributors><titles><title>Radio transmitter fingerprinting: A steady state frequency domain approach</title><secondary-title>2008 IEEE 68th Vehicular Technology Conference</secondary-title></titles><pages>1-5</pages><dates><year>2008</year></dates><urls></urls></record></Cite></EndNote>，经过不断的发展，目前常用的稳态信号特征包括载波频偏、相偏、误差矢量幅度、I/Q 不平衡、基于星座图的特征、熵特征等，也可以通过域变换的方式提取信号在其他域的特征，或者基于相空间重构的方法提取发射机特征。

以前的研究中通常将整个前同步码都视为稳态信号，而将前同步码进一步分为半稳态部分和稳态部分，其中半稳态部分是前导的前几个符号，通过这种新型方式可以达到非常高的识别精度。

发射器之间的微弱差异是由发射器硬件的非线性引起的杂散调制，这些信号分量大多数是非平稳的和非高斯的，很难通过时域和频域方法进行准确分析。可以采用域变换的方法提取射频指纹特征，常用的有变分模式分解（VMD）和固有时间分解（ITD）等，可以将接收到的信号分解成各种时间和频谱模式。

基于瞬态信号和基于稳态信号的特征提取方法都需要采集信号并进行预处理，而现阶段比较流行的深度学习方法则可以省略预处理这一步，直接将完整的信号投入分类器中即可得到分类结果。虽然不需要单独进行预处理、特征提取和分类识别这几个步骤，但是深度学习由于模型较为复杂，进行特征提取和分类识别的时间也是相对较长。而且通过深度学习的方法提取的特征并没有具体的数学模型或原理可以进行清晰的解释，且网络运行的时间花销也非常大，因此在实际应用中也具有一定的局限性。

3.3 基于发射机非线性模型的特征提取方法

基于瞬态信号和稳态信号的特征提取方法需要对传输信号进行预处理操作，而基于深度学习的方法无法明确解释所提取的特征。目前对于射频指纹识别方法的研究大多数都集中在通过对传输信号直接提取已知特征达到设备识别的目的，对于辐射源硬件特征机理分析的研究却很少。

辐射源设备内部硬件缺陷导致了不同设备个体具有独特的非线性特性，因此对于辐射源硬件非线性的研究可以分为基于发射机器件的非线性和基于发射机整体的非线性。图 3 是一个典型的无线数字发射机结构设计，其中标明了射频指纹的来源。

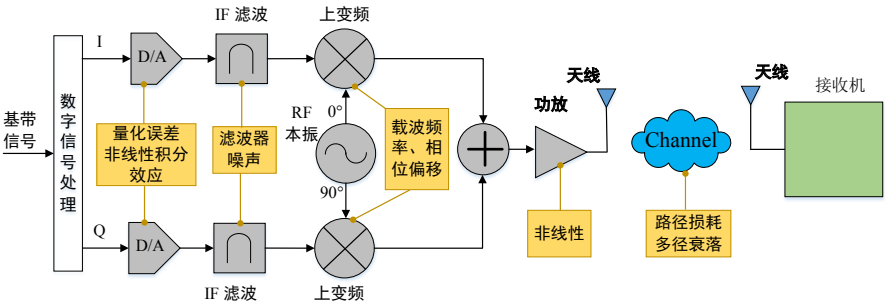

图 3 典型的无线数字发射机结构

无线设备在生产制造以及使用过程中会受到多种因素的共同影响，例如电路板材质、走线、所用的材料、加工工艺、封装工艺、器件老化、工作环境变化等影响，使得即使是生产流程相同的多个设备，也没有两个是完全相同的。不同发射机内的各器件具有一定的器件容差，即“硬件缺陷”。这种缺陷是由于发射机器件的物理特性发生正常改变而存在的，也可以称之为损伤。硬件损伤会使得无线设备实际发射的信号与理想情况下的输出有所不同。可用的硬件特征包括时钟抖动、DAC 采样误差、混频器频率偏移、功率放大器非线性及调制器子电路等。具体体现在辐射源的射频信号中。

4 结语

射频指纹识别技术作为提高无线设备安全性能的重要发展方向之一，已经在近年来得到广泛的研究。但目前在射频指纹识别领域仍然有一些需要解决的问题。第一，是缺少一份公开、规范、准确且齐全的数据集，使得目前出现的各种识别方法无法在相同数据集上统一进行比较，也就没办法衡量不同方法的优缺点；第二，是虽然目前对于无线设备射频指纹产生的机理有所研究，但是缺少射频指纹产生机理的正向数学推导模型，使得很多研究没办法找到理论支撑；第三，是由于通信传输环境日趋复杂，以及传输信道的不确定性，导致射频指纹的稳定性无法恒久保持，对于识别结果的准确度会造成很大的影响，也是一个未来的研究方向。

参考文献

[1] 张长森,赵秋实,吴君.基于Infogram的重复瞬态特征提取与旋转机械故障诊断[J].测控技术,2018,37(7):64-68.

[2] 王欢欢,张涛.结合时域分析和改进双谱的通信信号特征提取算法[J].信号处理,2017,33(6):864-871.

[3] 余沁,程伟,李敬文.利用小波变换特征提取的通信辐射源个体识别方法[J].信号处理,2018,34(9):1076-1085.

[4] 刘传波.一种基于稀疏表示的雷达辐射源识别方法[J].舰船电子工程,2020,40(10):72-75.

[5] 张靖志,郑娜娥,田英华.基于软件无线电的无线设备指纹识别[J].太赫兹科学与电子信息学报,2020,18(1):72-76.

[6] 任东方,张涛,韩洁,等.基于ITD与纹理分析的特定辐射源识别方法[J].通信学报,2017,38(12):160-168.