基于瞬态强度的射频指纹识别方法*

田金鹏 刘燕平 刘小娟
(上海大学 特种光纤与光接入网省部共建重点实验室 上海 200072)

摘 要：射频指纹识别是指无线通信中的发射机识别，用于加强无线安全，其难点在于有效的特征提取，特征提取方法主要分为瞬态和稳态分析，考虑到瞬态波形的差异性，将平均功率与幅度峰值之比定义为瞬态强度，并将其作为指纹特征来识别发射机。实验仿真中，采集了不同类型笔记本无线网卡和同一类型不同系列的波形进行分类性能估计，结果表明，相较于时频域的希尔伯特黄变换和短时傅里叶变换幅值特征，瞬态强度的指纹特征，使射频指纹识别有更高的识别准确率和更短的分类时间。

关键词：射频指纹识别；瞬态分析；瞬态强度
中图分类号：TN918 **文献标识码**：A **国家标准学科分类代码**：510.4030

RF fingerprinting method based on transient intensity

Tian Jinpeng Liu Yanping Liu Xiaojuan
(Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai 200072, China)

Abstract: Radio Frequency fingerprinting is the transmitters identification in wireless communication process, applying in wireless security, whose difficulty is the effective feature extraction. The feature extraction approaches for RF fingerprinting can broadly be divided into transient and steady-state analysis. Considering the difference of transient waveforms, we use transient intensity as the fingerprint feature to identity transmitters, which is defined as the ratio of signals' mean power and peak magnitude. The classification performance of notebook wireless network adapts in different models and USB wireless network adapts in different series have been evaluated from experimental simulation, combined with features of the magnitude of Hilbert-Huang Transform and the Short Time Fourier Transform in time-frequency domain. It is demonstrated that the feature of transient intensity has some advantages, such as high accuracy and short time of classification.

Keywords: radio frequency fingerprinting; transient analysis; transient intensity

1 引 言

射频指纹(radio frequency fingerprint, RFF)是指无线发射机的瞬态或稳态信号部分，射频指纹识别是指在无线通信过程中，通过提取特定的射频指纹来识别无线发射机[1]。

大数据时代，无线网络安全越来越受到重视，各种识别技术[2]也应运而生，射频指纹识别常用于加强无线网络安全。如军事及民用的频谱资源管理、通信流量分析及射频干扰源定位[3]，认知无线电安全认证与伪用户检测[4]，无线传感网的节点认证[5]等。

无线发射机的电子元件容差是形成RFF主要原因，电子元件包括印刷线路板走线、集成电路内部元件与走线、天线等无线发射机的所有构成成分。电子元件容差分为制造容差和漂移容差，制造容差是在元件制造过程中，由于生产精度导致的元件出厂时的实际值与标称值之间的差值，漂移容差是无线发射机工作过程中，由于温度、湿度、压力、阳光、装配、老化、灰尘等因素导致的元件值的变化，一般来说，漂移容差会大于制造容差。对于不同的无线发射机，由于电子元件容差的存在，即使输入相同，其输出也会不同[6]。

射频指纹识别系统包括4个阶段，信号预处理阶段、瞬态或稳态信号起始点检测阶段、特征提取阶段和分类阶段。射频指纹识别的重点和难点在于选取无线发射机有效的指纹特征。

收稿日期：2015-08
*基金项目：该项目获上海市重点学科项目(S30108)、国家自然科学基金重点项目(61132003)、面上项目(61171086)、上海大学创新基金(sdcx2012041)

2 实验系统建立与数据采集

无线网卡(WLNA)是无线通信中常用的发射机,实验提取了16个无线网卡的多个波形,包括7个笔记本无线网卡和9个USB无线网卡,其中7个笔记本无线网卡来自不同类型,USB无线网卡来自于同一类型两个系列,6个来自系列一,其余3个来自系列二。

图1是数据采集系统,用于采集工作于2.4 GHz频段的无线网卡信号波形,其中射频示波器作为模数转换器,来获得波形的时域信息,型号为Agilent DSO80604B,示波器采样率设置为10 GSa/s,路由器(Router)型号为TL-WR842N,USB无线网卡型号为TL-WN722N,采用IEEE802.11n协议,笔记本无线网卡则来自于不同的类型,也是采用IEEE802.11n协议。

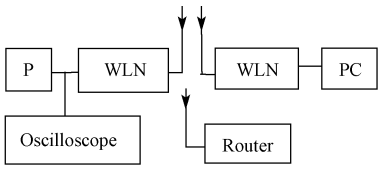

图1 数据采集系统

共采集了16个无线网卡的1650个波形,其中250个波形用于训练,其余用于测试分类。用MATLAB及其工具箱进行仿真识别。在预处理阶段,将信号进行幅值归一化来滤除传输过程中的幅度偏差,将归一化后的信号进行希尔伯特变换来获得近似包络,最后用低通滤波器来滤除信号低频部分,以平滑波形。

起始点检测是为了获得信号的瞬态部分,该文用贝叶斯步进检测法,其模型为

$$x_i=\begin{cases}\mu_1+n_i, 1\leqslant i<s\\ \mu_2+n_i, s\leqslant i\leqslant N\end{cases} \tag{1}$$

式中:x_i是i点信号的归一化包络,μ_1和μ_2起始点前后的包络均值,n_i是均值为0,方差为σ的白高斯过程,N是抽样点数,s是瞬态信号的起始点。

3 特征提取

在特征提取方面,很多学者提出了不同的算法,为了减少特征向量的维度和分类时间,有人提出将幅度信息结合主成分分析方法。文献[7]将短时傅立叶变换中得到的能量包络作为特征指纹,实现了低采样率时较高的识别正确率。文献[8]用高斯函数和正弦函数拟合小波变换得到瞬态包络,将拟合系数作为特征向量用于识别无线发射机。

文献[9]利用经验模态分解(EMD)方法,提取稳态信号杂散成分的频域特征,实现了低信噪比情况下的高识别正确率。文献[10]将无源RFID标签信号的对数谱作为特征指纹,把指纹集成到读写器应用层协议,实现了标签与读写器之间信息的控制。文献[11]结合主成分分析法和局部最小二乘递归法来缩短分类时间。文献[12]提出利用希尔伯特黄变换得到瞬态信号的时频域能量分布来识别无线发射机。

关于射频指纹识别,已经有很多的特征提取方法,其中一部分算法的复杂度较高,一部分算法需要较长的分类时间,还有一部分可能没有对各种不同的无线发射机进行实验仿真,识别相同类型和相同系列的无线发射机还是非常困难。

相比于稳态信号,不同发射机的瞬态信号具有更大的差异性,因此该文提取的是其瞬态信号部分。无线发射机的瞬态过程一般在十分之一微秒到几十毫秒之间,这里选择1024个采样点来进行特征提取。

该文提出将信号平均功率和幅度峰值的比值作为指纹特征,用模式识别中常用的径向基概率神经网络分类器,对不同类型的笔记本无线网卡和相同类型不同系列及同一系列的USB无线网卡进行实验仿真分类。再将瞬态强度的指纹特征,与时频域的希尔伯特黄变换和短时傅里叶变换的幅值特征进行了比较。

3.1 希尔伯特黄变换

希尔伯特黄变换(HHT)[13]是一种时频域分析方法,主要步骤是将信号进行经验模态分解[14],分解为多个本征模态函数,然后对每个本征模态函数进行希尔伯特变换来获得瞬时频率。

本征模态函数的条件:

1)在整个信号序列中,极值点个数和零点个数必须相等,或最多相差一个。

2)在任意抽样点上,信号的局部极大值和局部极小值定义的包络平均值为0。

经验模态分解过程:

1)找到信号$x(n)$的所有极大值点和极小值点,用插值函数生成上包络线$x_u(n)$和下包络线$x_l(n)$。

2)计算上、下包络线的均值$m(n)$

$$m(n)=(x_u(n)+x_l(n))/2 \tag{2}$$

3)计算原信号序列与该均值的差值

$$h(n)=x(n)-m(n) \tag{3}$$

4)若$h(n)$满足本征模态函数的条件,则$h(n)$即为第一个本征模态函数$c(n)$,若$h(n)$不满足本征模态函数条件,则将$h(n)$代替原信号$x(n)$,多次重复(1)~(3),直至其满足本征模态函数条件。

5)用信号序列$x(n)$减去第一个本征模态函数,得到剩余值

$$r(n)=x(n)-c(n) \tag{4}$$

6)对$r(n)$进行经验模态分解,直至剩余值为单调函数,或小于一个非常小的值,所以信号$x(n)$可表示为

$$x(n)=\sum_{j=1}^{m} IMF_j(n)+r_n(n) \tag{5}$$

对每个本征模态函数进行希尔伯特变换,并将其幅值

作为指纹特征，即

$$RFF = abs(hilbert(IMF_1(n))) \tag{6}$$

3.2　短时傅里叶变换

短时傅里叶变换（STFT）是用窗函数来截断时域信号，然后对截断信号进行傅里叶变换得到的局部频谱，其计算公式如下：

$$|STFT((x(n)))| = \left|\sum_{-\infty}^{\infty} x(n)w(n-m)e^{-jwm}\right| \tag{7}$$

式中：$w(n)$ 是滑动窗函数，$x(n)$ 是被传输的信号。

3.3　瞬态强度

我们将瞬态强度定义为信号的平均功率与幅度峰值之比，其提取过程如下：

1）选择一小波函数，对信号进行小波变换，得到其细节（高频）部分，即瞬态信号的主要成分，这里为一级 Haar 小波[15]。

$$x_h = Haar(x) \tag{8}$$

2）对信号进行分段处理，每段有 L 个抽样点。考虑到时间分辨率和复杂度，设置 $L = 8$ 。

3）计算每一段的平均功率

$$P_m(k) = \frac{1}{L}\left(\sum_{n=1}^{L} x_k^2(n)\right) \tag{9}$$

4）计算每一段的幅度峰值

$$P_p(k) = \max\{|x_k(n)|\} \tag{10}$$

5）计算瞬态强度

$$TI(k) = P_m(k+1)/P_p(k)\ \ 1 \leqslant k \leqslant L-1 \tag{11}$$

图 2～4 是来自 USB 无线网卡同一波形的特征波形，图 2 是希尔伯特黄变换的幅值特征，图 3 是短时傅里叶变换的幅频特性，图 4 是信号的瞬时强度特征。

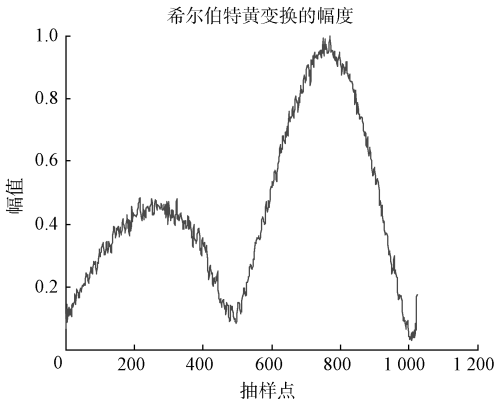

图 2　希尔伯特黄变换的幅值

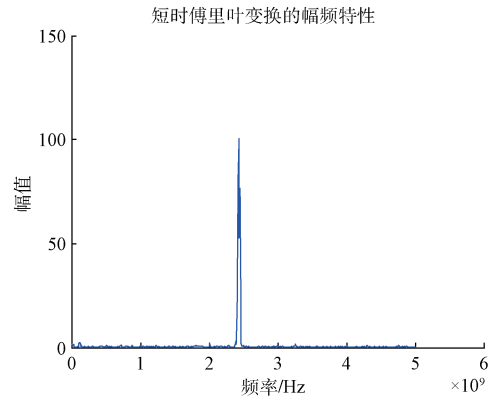

图 3　短时傅里叶变换的幅频特性

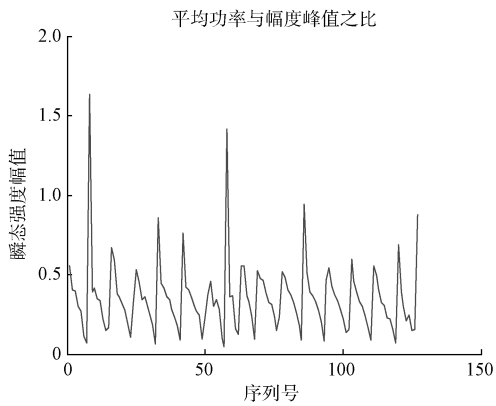

图 4　信号的瞬态强度

4　分类性能分析

径向基概率神经网络分类器结合了径向基函数网络与概率神经网络的优点，减少了网络连接权值的训练时间与网络隐单元的数目。该文用径向基概率神经网络分类器对指纹特征进行分类。

图 5～7 是文中第 3 部分阐述的 3 种指纹特征算法的分类结果图，表 1 对比了 3 种算法的分类误差和分类时间。

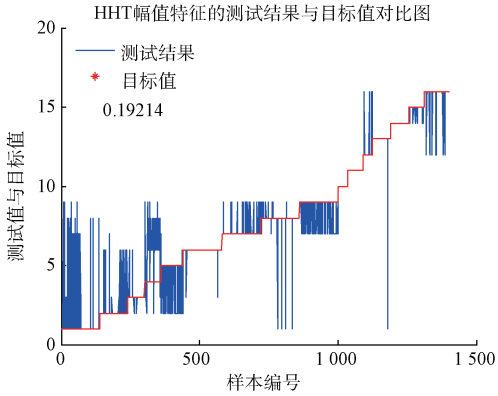

图 5　HHT 幅值特征的分类误差

由图 5～7 和表 1 可知，相较于信号的希尔伯特黄变换和短时傅里叶变换幅值特征，从信号平均功率与幅度峰值比值得到的瞬态强度特征，具有较低的分类误差和较短的分类时间，就分类性能上，该文提出的瞬态强度指纹特征算法具有较大的改进。在图 5～7 中，纵坐标 1～6 代表

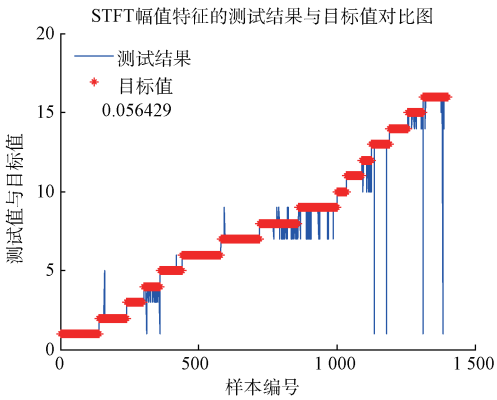

图 6 STFT 幅值特征的分类误差

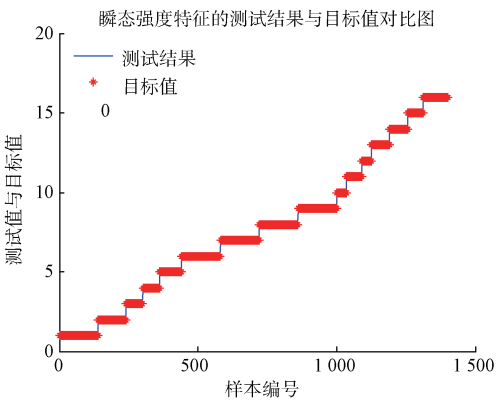

图 7 瞬态强度特征的分类误差

表 1 分类误差和分类时间

指纹特征	分类误差	分类时间/s
HHT 幅值	19%	302
STFT 幅值	5.6%	217
瞬态强度	0	192

来自系列一的 USB 无线网卡,7～9 代表来自系列二的 USB 无线网卡,10～16 代表来自不同类型的笔记本无线网卡,由图可知,相比于不同类型的无线网卡,相同类型的无线网卡识别会难一些,相同类型同一系列的则会更难一些,但可以通过不断地改进算法和找到更适合的指纹特征,使分类性能得到进一步提高。

5 结 论

针对射频指纹识别技术,该文提出用信号平均功率与幅度峰值之比定义的瞬态强度作特征指纹,用径向基概率神经网络分类器对瞬态强度特征进行分类,与希尔伯特黄变换和短时傅里叶变换幅值特征相比,该算法具有分类准确率高和分类时间短的优点。

由于射频指纹识别可以在接收端识别发射机,这将有助于控制非法接入和检测信息来源的可靠性。为了进一步加强无线网络安全领域,接下来将会扩大发射机和接收机之间的距离以及增加更多的发射机设备。

参考文献

[1] 袁红林,胡爱群. 射频指纹的产生机理与唯一性[J]. 东南大学学报:自然科学版,2009,39(2):230-233.

[2] 赵锦瑾,秦红磊. 射频标签自动测试系统[J]. 电子测量技术,2013,36(4):1-7.

[3] LAKAFOSIS V, TRAILLE A, LEE H, et al. RF fingerprinting physical objects for anticounterfeiting applications[J]. IEEE Transactions on Microwave Theory and Techniques, 2011, 59(2): 504-514.

[4] HARMER P K, REISING D R, TEMPLE M A. Classifier selection for physical layer security augmentation in cognitive radio networks[C]//2013 IEEE International Conference on Communications (ICC). IEEE, 2013: 2846-2851.

[5] NORMAN J, JOSEPH P. Secure neighbour authentication in wireless sensor networks[C]// 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), IEEE, 2011: 1-4.

[6] 袁红林, 胡爱群, 陈开志. 射频指纹的唯一性研究[J]. 应用科学学报, 2009, 27(1): 1-5.

[7] REHMAN S U, SOWERBY K, COGHILL C. RF fingerprint extraction from the energy envelope of an instantaneous transient signal[C]//Communications Theory Workshop (AusCTW), 2012 Australian. IEEE, 2012: 90-95.

[8] HUANG L, WU X, ZHAO C, et al. Identification of radio transmitters fingerprint based on curve fitting [C]//2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC). IEEE, 2013: 1-5.

[9] 梁江海,黄知涛,袁英俊,等. 一种基于经验模态分解的通信辐射源个体识别方法[J]. 中国电子科学研究院学报,2013,8(4):393-398.

[10] 袁红林,包志华,严燕. 基于对数谱射频指纹的 RFID 系统信息监测方法[J]. 通信学报,2014, 35(7): 86-93.

[11] PADILLA J L, PADILLA P, VALENZUELA-VALDéS J F, et al. RF fingerprint measurements for the identification of devices in wireless communication networks based on feature reduction and subspace transformation [J]. Measurement, 2014 (58): 468-475.

(下转第 65 页)