文章编号：2095-4980(2020)01-0072-05

基于软件无线电的无线设备指纹识别

张靖志，郑娜娥，田英华

(战略支援部队信息工程大学 数据与目标工程学院，河南 郑州 450001)

摘　要：无线局域网由于其开放的信道环境和传统的密钥身份验证机制，安全问题十分严峻。通过射频指纹识别技术，提取无线设备硬件特征进行身份验证，能够大大提高无线网络安全性。本文基于通用软件无线电外设(USRP)和 GNU Radio 开源平台，提取 IEEE 802.11a/g 信号载波频偏作为指纹，结合神经网络分类器进行识别。首先接收信号并提取每帧信号载波频偏，然后训练神经网络分类器，最后利用此分类器对无线设备进行识别。在办公室和体育馆 2 种典型室内环境进行无线设备个体识别实验，识别率均大于 90%。实验结果说明，基于软件无线电提取信号载波频偏可以识别出不同的无线设备，检测出非法设备接入，能够提高无线网络安全性。

关键词：无线设备；射频指纹识别；载波频偏；软件无线电

中图分类号：TN97　　**文献标志码：**A　　**doi：**10.11805/TKYDA2018202

Radio frequency fingerprinting identification of devices using software radio

ZHANG Jingzhi，ZHENG Na'e，TIAN Yinghua

(School of Data and Target Engineering，Strategic Support Force Information Engineering University，Zhengzhou Henan 450001，China)

Abstract：There are risks in Wireless Local Area Network(WLAN) because of the open channel environment and the traditional key authentication mechanism. Radio frequency fingerprinting identification which extracts hardware features of wireless devices for authentication, could greatly improve the wireless network security. Based on Universal Software Radio Peripheral(USRP) and GNU Radio open source platform, carrier frequency offset of IEEE 802.11a/g signals is extracted as the fingerprint, and the neural network classifier is used for recognition. Firstly, this method collects IEEE 802.11 a/g signals and extracts the carrier frequency offset of each frame, then trains a neural network classifier. Lastly it identifies wireless devices by using the classifier. In two typical indoor environments of the office and the gymnasium, the recognition rate of wireless devices is more than 90%. The experimental results show that wireless devices can be identified by extracting carrier frequency offset of signals based on software radio, and illegal device access can be detected, which could improve the security of wireless network.

Keywords：wireless device；radio frequency fingerprinting identification；frequency offset；software radio

无线局域网(WLAN)是接入互联网的常用方式，由于 WLAN 开放的信道环境、多样的接入设备和组网形式等原因，安全问题十分严峻。传统的身份验证方式主要是密钥身份验证，以及根据接入设备 MAC 地址、IP 地址等信息识别，但这些信息很容易被嗅探、伪装和篡改。此外无线网络安全协议通常存在漏洞，非法用户窃取到密钥可以入侵无线网络。2017 年 10 月，Mathy Vanhoef 公布了针对 WAP2 协议的密钥重装攻击，攻击者可以读取目标无线网络连接上的所有流量[1]。

由于电子元器件的制造容差，以及元器件的退化老化效应等，即使是同一型号同一批次的无线设备的实际硬件参数也存在差异，这种硬件上的差异会反映在通信信号上[2]。就像每个人有不同的指纹，每个无线设备也有不同的指纹——“射频指纹”。通过接收到的射频信号提取无线设备指纹特征，训练出能够标识特定无线设备

收稿日期：2018-09-04；**修回日期：**2018-11-14

基金项目：电子信息系统复杂电磁环境效应国家重点实验室 2018 年度主任基金资助项目(CEMEE20188Z0103B)

作者简介：张靖志(1994–)，男，在读硕士研究生，主要研究方向为辐射源个体识别。email:zjz030721@163.com

的分类器，再利用此分类器将待识别设备分类和识别，采取硬件个体身份验证方式实现无线设备接入控制、识别和追踪等目的，可以辅助和增强传统的无线网络身份验证机制，大大提高无线网络的安全性。

目前，对 IEEE 802.11 信号分析与指纹特征提取多采用矢量信号分析仪、WLAN 综合测试仪等设备[3−4]，提取载波频偏、前导相关、幅度相位误差、误差矢量幅度、I/Q 偏移、I/Q 不平衡等诸多调制域特征，以及信号分形维数、熵特征、时频特征等变换域特征用于识别和分类，取得了较好的效果，但这些设备成本高昂，体积庞大，不适用于实际无线网络安全应用。另一方面，基于 GNU Radio 开源平台和通用软件无线电外设(USRP)的信号处理系统架构灵活，易于重配置，体积小，成本相对低廉，满足实际无线设备指纹提取需求。因此，可以采用软件无线电构建 IEEE 802.11a/g 信号接收系统，选取稳定、易于提取的指纹特征进行识别与分析[5−6]。

1　IEEE 802.11a/g 帧格式

IEEE 802.11a/g 是典型的分组突发传输系统，其 PLCP 协议数据单元(PLCP Protocol Data Unit，PPDU)帧结构如图 1 所示，一帧数据由短训练(short training)序列、长训练(long training)序列、信令段和数据段四部分组成。短训练序列由 10 个重复的符号段($t_0t_1\cdots t_9$)组成，每段符号含有 16 个符号。短训练序列主要用于数据帧开始检测、自动增益控制和粗频率校准。长训练序列由循环前缀(Cyclic Prefix，CP)和 2 个重复的符号段(T_1,T_2)组成，这 2 个重复的符号段每段含有 64 个符号。长训练序列用于信道估计、精频率校准和时间同步。信令段包含数据速率、数据长度和校验位信息。数据段携带有效的数据信息，包括服务字段、PLCP 服务数据单元(PLCP Service Data Unit，PSDU)、尾比特和填充比特[7]。

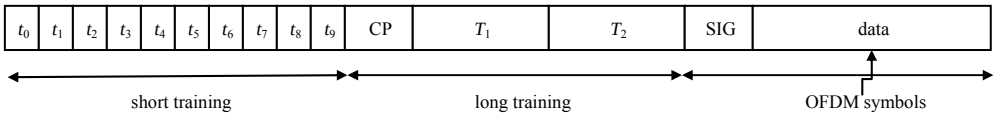

Fig.1 IEEE 802.11a/g frame structure
图 1 IEEE 802.11a/g 帧结构

2　无线设备个体识别方法

指纹特征选取是个体识别的核心问题，选取稳定可靠的特征有利于降低分类器的复杂度，提高分类精确度和识别正确率。一般选取指纹特征需要遵循唯一性、可测性、稳定性原则。唯一性指特征由设备非理想特性唯一决定，与信号调制方式、速率、调制信息等无关；可测性是指该特征可检测提取到，并且精确度满足辐射源个体分类需求；稳定性指特征在一段时间内稳定，不受温度等环境变化发生剧烈变化[8−9]。分类识别包括分类器设计和分类决策两部分。分类器设计指根据训练集求解一最优分界面，使得分类错误率最低或分类错误代价最小；分类决策则是通过分类器判决测试对象所属类别。一般要求分类器类间分类性能好，类内泛化性能高[10]。

2.1 载波频率偏差机理分析

通信系统中，发送端的基带信号上变频为高频带通信号，接收端使用与发送端频率一致的本地载波将带通信号下变频为基带信号。电子元器件制造容差导致的本地振荡器频率差异，以及发送端和接收端相对运动导致的多普勒效应，都会导致载波频率偏差。单载波通信中，载波频偏会导致接收信号幅度衰减和相位旋转[11]。而 IEEE 802.11a/g 是典型的正交频分复用(Orthogonal Frequency Division Multiplexing，OFDM)系统，利用多载波传输数据，对载波频偏十分敏感。载波频偏会在相邻子信道产生干扰，严重影响系统性能。IEEE 802.11 协议规定，5 GHz 频段信号中心频率容限为±20 ppm(0.002%)；2.4 GHz 频段信号中心频率容限为 ± 25 ppm[7]。

指纹特征提取的一个重要挑战是如何尽量降低信道对指纹特征的影响。室内环境下，信号传播时受障碍物影响发生散射、反射、绕射，产生多径效应，接收信号会出现在短时间、短距离内的快速起伏变化和多径时延扩展[12]。室内多径衰落信道不会改变信号频率，并且发送端和接收端相对运动速度较低，多普勒频移效应弱，载波频偏主要由发送端和接收端本地振荡器差异导致。对于同一接收端，提取接收信号的载波频偏可作为不同发射端的指纹特征。

2.2 载波频率偏差估计算法

IEEE 802.11a/g 突发分组式的无线局域网常用数据辅助型频偏估计算法。算法利用接收信号前导训练序列时域相关，在单个训练符号内就可以完成同步和频偏估计，再对有效信息进行补偿。为了提高估计精确度，一

般先将载波频率偏差估计到一个较小的范围，然后再对剩余频偏进一步估计。即利用短训练序列进行粗频偏估计和补偿，再利用长训练序列进行精频偏估计。

对接收信号共轭相关，得到相关峰时，认为接收到了数据[13]。利用短训练序列的后 5 个符号段进行粗频偏估计。

$$\hat{\alpha}_{\mathrm{ST}}=\frac{1}{16}angle\left(\sum_{m=0}^{63}S_m S_{m+16}^{*}\right) \tag{1}$$

式中：$S_m(m=1,2,\cdots,79)$ 为短训练序列后 5 个符号段的符号；$angle(\ )$ 为取相位运算符。

利用 $\hat{\alpha}_{\mathrm{ST}}$ 补偿长训练序列符号后再次进行精频偏估计。

$$S_n^{'}=S_n\mathrm{e}^{-\mathrm{j}m\hat{\alpha}_{\mathrm{ST}}} \tag{2}$$

式中：$S_n(n=0,1,\cdots,127)$ 为长训练序列符号；$S_n^{'}$ 为粗频率补偿后的长训练序列符号。

最后利用长训练序列进行精频偏估计。

$$\hat{\alpha}_{\mathrm{LT}}=\frac{1}{64}angle\left(\sum_{m=0}^{63}S_n^{'}S_{n+64}^{'*}\right) \tag{3}$$

总的频偏估计 $\hat{\alpha}_{\mathrm{T}}=\hat{\alpha}_{\mathrm{ST}}+\hat{\alpha}_{\mathrm{LT}}$。文献[14]推导了利用训练序列估计的归一化载波频率偏差：

$$\hat{\varepsilon}=\frac{N}{2\pi D}angle(\hat{\alpha}) \tag{4}$$

式中：$\hat{\varepsilon}$ 为归一化频率偏差；N 为 OFDM 信号调制的 IFFT 点数；D 为序列相关延时；$\hat{\alpha}$ 为序列相关值。

以 20 MHz 带宽 802.11a/g 信号为例，OFDM 调制的 IFFT 点数为 64，则短训练序列粗频偏估计最大频偏为 625 kHz，长训练序列精频偏估计最大频偏为 156.25 kHz。

2.3 神经网络分类器构建

构建两层神经网络分类器，第一层网络节点数为 10，激活函数为线性函数 logsig，第二层节点数由训练集设备数决定，激活函数为对数 S 形转移函数 purelin。分类器学习规则为梯度下降自适应学习率训练函数。设备接入无线网络后会产生大量的数据帧，故对每个无线设备采集 1 000 帧的频偏信息作为训练集，提取每帧信号 MAC 地址做监督，训练分类器。训练完成后，采集目标无线设备频偏测试分类器性能。

3 实验与分析

3.1 实验平台设计

以 USRP B210 作为信号接收设备，通过 USB 3.0 与主机连接，主机运行 GNU Radio 进行信号处理，提取信号帧频偏，并提取信号 MAC 地址作为每帧信号的标识[6]。为便于实验，设定路由器工作信道为固定的单一信道，实验平台中心频率与路由器工作信道中心频率一致，采样率为 20 MSa/s，将系统采集到的无线设备频偏信息实时显示并存储。无线设备信号指纹提取实验平台处理步骤如下：

步骤 1：对接收信号共轭相关，得到相关峰时，认为接收到了 IEEE 802.11a/g 信号，进行后续处理。

步骤 2：利用短训练序列使帧同步，同时粗估计载波频偏。

步骤 3：利用长训练序列使符号同步，同时精估计载波频偏，步骤 2 和步骤 3 获得最终的载波频偏估计。

步骤 4：在频域估计信道并做均衡。

步骤 5：移除导频和循环前缀，解交织，维特比译码，解扰，获取该帧信号载荷信息，由载荷信息提取出信号的 MAC 地址。

步骤 6：以每帧信号的 MAC 地址作为类标，以载波频偏作为信号指纹，训练神经网络分类器，识别不同的无线设备。

表 1 目标无线网络设备 MAC 地址

Table1 Devices MAC address of target WLAN

wireless devices	MAC address
RTL8811AU_1	e8:4e:06:56:46:db
RTL8811AU_2	e8:4e:06:56:e2:52
RTL8811AU_3	e8:4e:06:56:e2:40
mobile phone	50:8f:4c:ff:53:a0
laptop	34:e6:ad:a0:38:77
router	1a:63:bf:ce:12:6a

3.2 无线设备个体识别实验

目标无线网络接入了 3 个同一型号同一批次的 Realtek RTL8811AU 无线网卡、1 台笔记本电脑和 1 部手机。各接入设备的 MAC 地址如表 1 所示。某一次实验结果如图 3 所示，可以发现不同 MAC 地址，即不同设备的频偏存在差异且稳定在一固定值附近。本文进行了多次实验，一周的时间内在不同设备位置、不同的无线设备行为模式(浏览网页、观看直播、ping 指令等)、不同的天线方向，对无线设备载波频偏进行提取，

发现几乎没有差异。说明在短期内，无线设备载波频率偏差稳定，可作为指纹特征识别无线设备。由于监测的信道中还有其他路由器和网络设备，会提取到一些非目标网络设备的 MAC 地址，如‘5c:e0:c5:1d:c7:2f’，‘da:a1:19:19:13:7b’。

针对同一型号同一批次设备指纹特征提取与个体识别，本文分别在 2 种典型室内信道环境下进行实验：办公室空间较小，有较多障碍物遮挡；体育馆相对较为空旷。办公室与体育馆环境下，3 个无线网卡接入网络并提取载波频偏，结果如图 3、图 4 所示(此处仅显示出 3 个网卡的载波频偏)。从图中可以发现，同信道环境下 3 个网卡载波频偏稳定且存在差异。

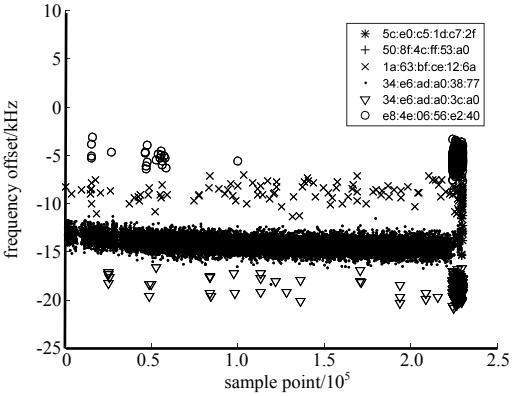

Fig.2 Frequency offset of wireless devices
图 2 无线设备载波频偏

利用采集到的 3 个网卡载波频偏训练神经网络分类器，并进行测试。办公室环境下，分类器总体识别率为 90.6%；体育馆环境下，分类器总体识别率为 93%。实验结果说明该分类器可以实现对目标无线网卡的识别和分类。

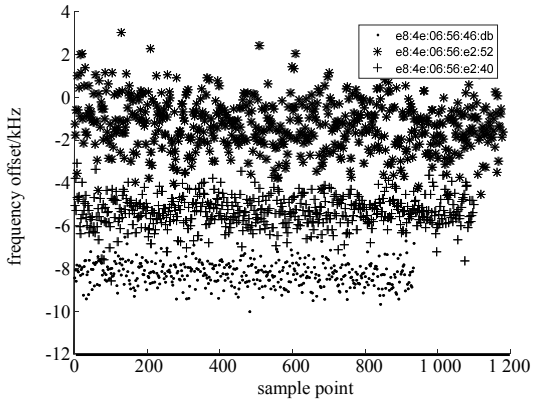

Fig.3 Frequency offset of NICs at office
图 3 办公室环境下无线网卡载波频偏

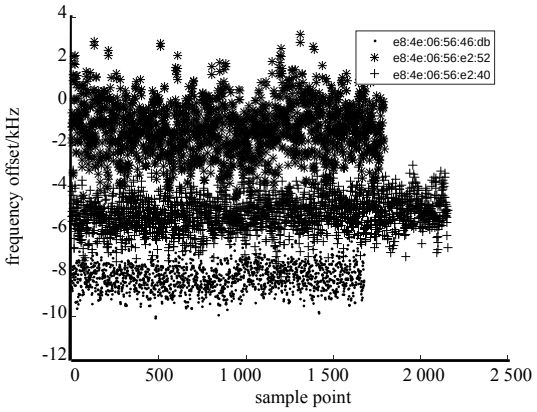

Fig.4 Frequency offset of NICs at gymnasium
图 4 体育馆环境下无线网卡载波频偏

最后，针对典型的 MAC 伪装入侵无线网络[15]的情形，本文修改‘e8:4e:06:56:e2:52’RTL8811AU 无线网卡 MAC 地址为‘e8:4e:06:56:e2:40’，伪装成合法用户接入目标网络。传统的基于密钥的身份验证机制，当非法用户窃取到密钥，伪装合法用户的 IP 与 MAC 地址后，难以被检测出，往往都是被窃取了关键信息后察觉。

当提取无线设备载波频偏作为信号指纹辅助密钥验证机制时，从图 5 中可以看出，‘e8:4e:06:56:e2:40’无线网卡载波频偏稳定在 2 个值附近，此时分类器识别正确率远低于 90.6%，检测到伪装入侵的设备。

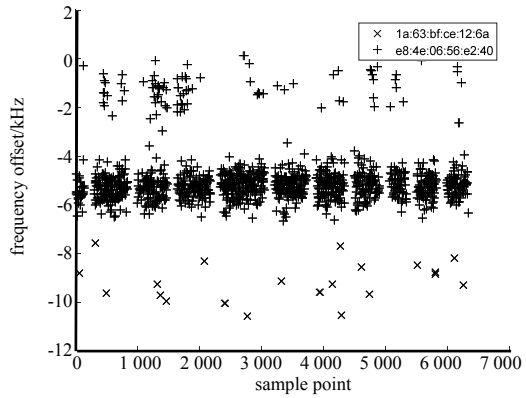

Fig.5 Detection of MAC spoofing
图 5 MAC 伪装检测

在实际无线网络安全应用中，对无线网络设备采集载波频偏，构建合法用户信号指纹集。当无线设备产生流量时，提取其载波频偏并识别。这时可以将分类器视为 MAC 伪装检测器，提取无线网卡信号指纹和 MAC 地址，当分类器识别率低于某一阈值时，认为检测到了伪装入侵的设备。通过设定不同的阈值满足不同的漏警虚警概率。

3.3 实验结果分析

实验说明，不同的无线网络设备频率源存在容差，容差导致信号载波频率存在偏差且在一定时间内稳定，受信道影响小，可以作为设备的指纹特征。通过采集样本训练分类器，能够检测出非法接入的无线设备，辅助传统的密钥身份验证。但该系统存在两点不足：一是软件无线电系统处理当前数据帧时，并发的数据帧无法检测和提取频偏信息，可以通过适当增加监测时间改善；另一个是本系统仅提取单一的频偏特征用于指纹识别，攻击者容易寻找到频偏相近的无线设备伪装入侵，或同样利用软件无线电架构的无线设备入侵网络，需要提取其他指纹特征来提高系统稳健性。

4 结论

本文基于 GNU Radio 和 USRP B210 提取 IEEE 802.11a/g 无线设备载波频率偏差作为指纹特征，通过硬件个体身份验证实现了设备识别和非法用户入侵检测。该方法可以改进和辅助传统的密钥身份验证机制，提高无线网络的安全性。小波系数、时频特征、熵特征等需要大量的样本，而载波频偏作为一种调制域特征，由一帧信号就可以提取出特征。与利用矢量信号分析仪、WLAN 综合测试仪提取指纹特征的系统相比，软件无线电架构简洁，设备体积小，成本相对低廉，易于布设，在无线网络安全有较好的应用前景。同时，新的无线局域网标准 IEEE 802.11n/ac 提供了更高的数据传输速度和用户容量，被广泛使用。协议规定了新的帧格式，结合了多用户 MIMO (Multiple User-Multiple Input Multiple Output，MU-MIMO)技术，除载波频偏外又提供了新的特性。后续将从指纹识别的角度针对 IEEE 802.11n/ac 载波频率偏差和 MIMO 特性继续展开研究。

参考文献：

[1] VANHOEF M,PIESSENS F. Key reinstallation attacks: forcing nonce reuse in WPA2[C]// Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. Dallas,TX,USA:ACM, 2017:1313-1328.

[2] HALL J,BARBEAU M,KRANAKIS E. Detection of transient in radio frequency fingerprinting using signal phase[C]// The Seventh IASTED International Conference on Wireless and Optical Communications. Banff,Canada:International Association of Science and Technology for Development(IASTED), 2003:13-18.

[3] 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):393-397. (LIANG Jianghai,HUANG Zhitao,YUAN Yingjun,et al. A method based on empirical mode decomposition for identifying transmitter individuals[J]. Journal of CAEIT, 2013,8(4):393-397.)

[4] BRIK V,BANERJEE S,GRUTESER M,et al. Wireless device identification with radiometric signatures[C]// Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. San Francisco,California,USA:ACM, 2008: 116-127.

[5] VO-HUU T D,NOUBIR G. Fingerprinting Wi-Fi devices using software defined radios[C]// Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks. New York,USA:ACM, 2016:3-14.

[6] BLOESSL B,SEGATA M,SOMMER C,et al. Demo: decoding IEEE 802.11 a/g/p OFDM in software using GNU radio[C]// Proceedings of the 19th ACM International Conference on Mobile Computing and Networking. Miami,Florida,USA:ACM, 2013:159-162.

[7] WG802.11-Wireless LAN Working Group. IEEE Std 802.11g-2003,part11:wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications:further higher data rate extension in the 2.4 GHz band[S/OL]. IEEE SA, 2003 [2018-11-14]. https://standards.ieee.org/ findstds/standard/802.11g-2003.html.

[8] 许丹. 辐射源指纹机理及识别方法研究[D]. 长沙:国防科学技术大学, 2008. (XU Dan. Research on mechanism and methodology of specific emitter identification[D]. Changsha,Hunan,China:National University of Defense Technology, 2008.)

[9] 俞佳宝,胡爱群,朱长明,等. 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. (YU Jiabao, HU Aiqun,ZHU Changming,et al. RF fingerprinting extraction and identification of wireless communication devices[J]. Journal of Cryptologic Research, 2016,3(5):433-446.)

[10] 周斌. 信号细微特征提取及识别技术研究[D]. 哈尔滨:哈尔滨工业大学, 2011. (ZHOU Bin. Research on signal subtle feature extraction and recognition technologies[D]. Harbin,Heilongjiang,China:Harbin Institute of Technology, 2011.)

[11] HOU W,WANG X,CHOUINARD J Y,et al. Physical layer authentication for mobile systems with time-varying carrier frequency offsets[J]. IEEE Transactions on Communications, 2014,62(5):1658-1667.

[12] ATA O W. An extended-AMATA indoor propagation model for GSM 900/1 800 MHz and Wi-Fi 2.4 GHz frequencies[J]. Wireless Personal Communications, 2017,92(3):993-1009.

[13] LIU C H. On the design of OFDM signal detection algorithms for hardware implementation[C]// IEEE Global Telecommunications Conference. San Francisco,CA,USA:IEEE, 2003:596-599.

[14] 张田静. 面向 IEEE 802.11 ac 射频一致性测试的载波频偏估计算法研究与应用[D]. 南京:东南大学, 2016. (ZHANG Tianjing. Research and application on carrier frequency offset estimation of 802.11ac RF conformance test[D]. Nanjing, Jiangsu,China:Southeast University, 2016.)

[15] BANAKH R,PISKOZUB A,OPIRSKYY I. Detection of MAC spoofing attacks in IEEE 802.11 networks using signal strength from attackers' devices[C]// International Conference on Computer Science, Engineering and Education Applications. Kiev,Ukraine:Springer International Publishing, 2018:468-477.