ISSN 1004-9037,CODEN SCYCE4
Journal of Data Acquisition and Processing Vol. 35,No. 6,Nov. 2020,pp. 1125－1133
DOI:10. 16337/j. 1004-9037. 2020. 06. 012

http://sjcj. nuaa. edu. cn
E-mail:sjcj@nuaa. edu. cn
Tel/Fax:＋86-025-84892742

LTE伪基站的软件无线电识别技术

钟文华[1,3]，王红光[2]，刘成国[1,3]

(1. 武汉理工大学理学院,武汉，430070;2. 中国电波传播研究所,青岛，266107;3. 湖北省射频微波应用工程技术研究中心,武汉，430070)

摘　要：相比全球移动通讯系统(Global system for mobile communications，GSM)网络,长期演进(Long term evolution，LTE)中增加了双向鉴权机制,伪基站的防治得到了改善,但受传统硬件设施的桎梏,检测和跟踪代价昂贵、灵活性也有所不足。不仅如此,随着通信技术的升级,伪基站更加偏向于智能化和小型化,难以被侦测。针对以上问题,本文基于软件无线电技术,对相关伪基站识别算法进行改进,提出了一种新的LTE伪基站识别方案。通过搭建软件无线电平台和建立LTE下行广播信息接收链路获取基站的关键小区相关信息,并基于信息一致识别算法对基站进行判别。该方案选择了两个测试场景,正确地检测到了合法基站,也检测到了伪基站的信息,验证了本文识别方法的可行性。结合软件无线电自身的优点,本文形成的技术具有系统升级效率高、成本低的优势。

关键词：软件无线电;LTE伪基站;识别

中图分类号：TN918.91　　**文献标志码：**A

Software Radio Recognition Technology for LTE Pseudo Base Station

ZHONG Wenhua[1,3]，WANG Hongguang[2]，LIU Chengguo[1,3]

(1. School of Science，Wuhan University of Technology，Wuhan，430070，China; 2. China Research Institute of Radiowave Propagation,Qingdao，266107,China;3. Hubei Engineering Research Center of RF-Microwave Technology and Application,Wuhan，430070,China)

Abstract：Compared with the GSM network，the two-way authentication mechanism has been added to LTE，and the prevention and control of pseudo base stations are improved. However，due to the shackles of traditional hardware facilities，detection and tracking are expensive and the flexibility is insufficient. Not only that，with the upgrade of communication technology，pseudo base stations are more inclined to be intelligent and miniaturized，which is difficult to detect. In response to the above problems，based on the software radio technology，this paper improves the related pseudo base station identification algorithm and proposes a new LTE pseudo base station identification scheme：Acquiring a key cell of the base station by building a software radio platform and establishing an LTE downlink broadcast information receiving link Relevant information，and the base stationis is distinguished based on the consistent information recognition algorithm. The scheme selected two test scenarios，correctly detected the legal base station，and also detected the information of the pseudo base station，which verified the feasibility of the identification

基金项目：电波环境特性及模化技术重点实验室基金(A161703014)资助项目;国家自然科学基金国际合作重大(61320106004)资助项目;湖北省技术创新项目重大专项(2016AAA007)资助项目。
收稿日期：2020-01-15;**修订日期：**2020-05-21

method in this paper. Combined with the advantages of software radio itself, the technology formed in this paper has the advantages of high system upgrade efficiency and cost reduction.

Key words: software radio; LTE pseudo base station; identification

引　　言

2G时代,伪基站利用全球移动通讯系统(Global system for mobile communications, GSM)单向认证缺陷实现诈骗。早期主要通过安装拦截软件、改用安全性更高的手机以及即时留意手机信号等来达到预防伪基站的目的,但明显效率低下[1]。相比之下,长期演进(Long term evolution, LTE)增加了双向鉴权机制,伪基站的防治得到改善,但国内外检测系统的硬件架构体积庞大,便携性也有所不足[2-3]。不仅如此,面对通信系统的更新换代以及各种新式伪基站的层出不穷,大部分检测系统由于传统硬件的桎梏,升级更新缓慢,代价高昂,检测效率也难以提升。相应地,伪基站硬件系统下主要有5种应用识别算法。基于接收信号强度指示(Received signal strength indicator, RSSI)信号接收强度的识别算法,提供信号地图的可视化界面,交互性好但对现实环境中的信道干扰较为敏感,需要根据多变的信道环境采取不同的检测算法,复杂度高且依赖移动终端对于信号强度的检测,随着手机端硬件等设施的差异,判定结果也有所差异,识别准确率较低。基于临近小区信息列表识别算法,与第1种算法相似,依赖移动终端获取小区信息列表,受限较大,但不受信道环境所干扰因此性能消耗最小,用户体验也不错。基于静默短信攻击的识别算法,该算法较为特殊,需要对终端无线通信的相关消息缓冲区字节流进行解码,识别率很高,但性能消耗过多且复杂度较高,同样该算法依赖终端侧的辅助。基于跟踪区域码(Tracking area code, TAC)/小区识别号(Cell identity, CID)位置更新的识别算法和基于基站信息一致性识别算法,两种算法本质相同,都采用信息对比方式进行判定。前者利用伪基站工作时,手机会切断与正常基站的连接进而被伪基站捕获,导致TAC、CID等参数发生变化从而进行识别,识别率理论上最高,用户体验也很不错但依然需要外部设备的辅助。后者因为也是跟本地数据对比,准确率较高但依赖基站信息数据库,若缺乏某地域的数据,检测将无法进行,所以用户体验一般[4]。

综上所述,伪基站识别系统受传统硬件的桎梏存在诸多缺点,灵活性差,升级效率也低,并且现有识别算法的复杂度、交互性、准确率以及依赖性等都相互制约,难以权衡。而相比之下,软件无线电具有可重配置能力,升级更新灵活、运维成本低廉,还能适应移动通信网络多制式模式[5-6]。

虽然将软件无线电技术运用在LTE伪基站识别方面少有,但已有研究表明,将其运用在2G伪基站系统中,能够在相同的硬件基础上通过软件更新的方式来达到功能的升级,有效提高系统升级的效率[7-8]。除此之外,伪基站5种识别算法当中,大部分算法都需要借用移动终端获取相关辅助信息,灵活性太差,而将软件无线电技术运用在LTE信号的接收处理当中刚好可以辅助获取相关信息。不仅如此,后期面对新式伪基站或者不同的信道环境,只需借助软件无线电技术对其中的相应模块进行技术上的升级即可实现系统性能的提高,大大提高了整个识别系统的升级效率。因此,为了形成LTE伪基站软件无线电识别技术原型,本文开展将软件无线电技术用于LTE伪基站检测的研究。

1　原理分析

1.1　伪基站工作机制

伪基站的实施机制主要分为两种:固定式,一般藏匿于钟点房内、快捷酒店等不易被人察觉的地方;流动式,布置在拉杆箱或者小型汽车内便于流动作案。通常情况下,LTE伪基站在获取到附近基站的系统消息相关参数后会设置假冒的参数构建新的eNodeB基站。其中,一个伪基站eNodeB用于干扰移动终端使其脱离当前驻留的4G网络,称作eNodeB_jammer。另一个伪基站叫做eNodeB_Collector,

它通过设置更高的发射功率或高的频点优先级,强制LTE终端用户通过小区重选机制接入伪基站的网络,取代合法运营商服务。不过,eNodeB_Collector虽然把移动设备网络代码(Mobile network code, MNC)和移动设备国家代码(Mobile country code, MCC)设置为当前运营商的合法基站参数值,但是其TAC通常设置为与正常基站相异的值,只有这样eNodeB_Collector才能伪装成正常的基站并诱使移动终端在脱网后发起重连TAU_REQUEST[9-10]。不仅如此,eNodeB_Collector的EARFCN由于被人为的设置为4G网络区域内的最高优先级,因此,LTE终端用户在重新进行小区搜索时就会直接落入LTE伪基站的网络区域当中,从而面临诈骗危险。

1.2 伪基站识别算法

伪基站识别算法中,基于信息一致性识别和基于TAC/CID位置更新的识别由于利用基站的小区相关信息中TAC和CID参数进行识别,准确率最高但依赖移动终端获取相关信息,灵活性太差。与此同时,伪基站系统受限于传统硬件拥有诸多缺点效率低下,若能借用软件无线电技术代替传统硬件的同时还能通过某种手段获取TAC和CID参数,那么这两种算法的优势将得到进一步提升。

(1) 基于TAC/CID位置更新的识别算法

LTE中,TAC用于标识移动通信网络中一定范围的区域,且每个TAC标识的区域内,基站的TAC值都相同。图1为蜂窝小区示意图,左边为正常基站蜂窝小区,右边为存在伪基站时的蜂窝小区。由图1可知,移动终端与正常基站(TAC-2020,CID-202 020)已连接,伪基站eNodeB_jammer干扰移动终端使其脱离当前驻留的4G网络(灰色虚线)。接着eNodeB_Collector设置了与正常基站相同的TAC和CID参数:TAC-2020,CID-202 020,并设置更高的发射功率或高的频点优先级迫使移动终端与其进行连接(蓝色虚线)。最后eNodeB_Collector更改TAC值为2021(见图1中标橙区域),从而触发移动终端发起位置更新请求获取用户真实信息。因此,只要不断获取基站的TAC和CID等信息,并判断该基站的TAC是否发生更新便能判断其是否为伪基站。

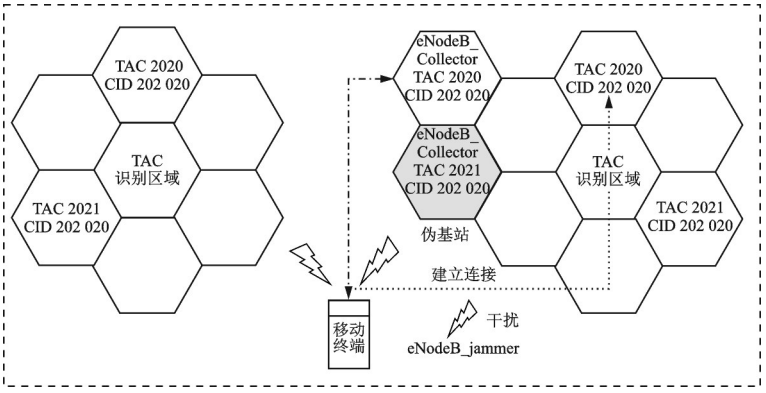

图1 伪基站工作时TAC变化示意图

Fig.1 Schematic diagram of TAC changes when the pseudo base station works

(2) 基于信息一致性识别算法

如图2所示,该算法对当前移动终端接入基站的CID和TAC进行检测,与基于TAC/CID位置更新的识别算法不同的是,它在于检测最终的TAC值与CID的联合信息。首先终端侧联网后依靠底层接口获取TAC和CID信息,然后将该信息与运营商自建数据或者第3方开源基站信息数据库进行对比,若当前接入的基站信息与数据库有一定差异,则基本可以判定该基站为伪基站。该识别方法可离线侦测,成本低廉且准确率极高。其中,第3方开源基站信息数据库可通过开源平台如OpenCellID.org

提供,且本文后续章节中为了提高识别效率选取该算法并使用基于移动位置服务系统(Location based service,LBS)中的运营商数据对基站进行判别。

2 系统方案和实现

LTE伪基站劫持移动终端时,其部分小区相关信息参数设置为与正常基站相异的值。若能实时获取到附近基站的TAC,再结合基站参数CID,便能基于基站信息一致性识别算法在LBS系统中利用本地运营商数据库作对比,找出参数异常的基站,从而识别出LTE伪基站。因此本文提出在不借用移动终端的情况下,利用LTE伪基站部分小区相关信息参数设置为与正常基站值相异的特点,实现伪基站识别的新方案。

如图3所示,该方案包括硬件采集模块、软件解码模块以及识别验证模块。硬件采集模块通过搭建软件无线电平台对4G信号进行采集;软件解调解码模块通过建立LTE下行系统广播信息接收链路解码系统信息块(System information blocks 1,SIB1)获取TAC和CID;识别验证模块利用LBS系统来判别基站的合法性。

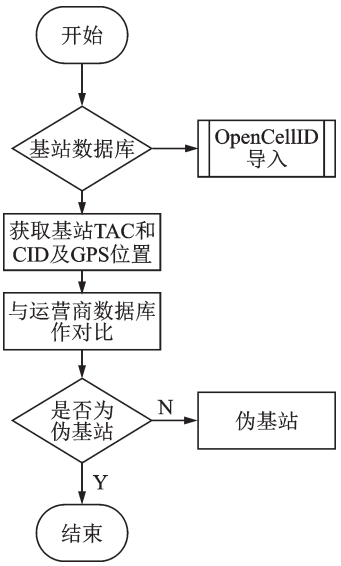

图2 基于信息一致识别算法流程

Fig.2 Recognition algorithm flow based on consistent information

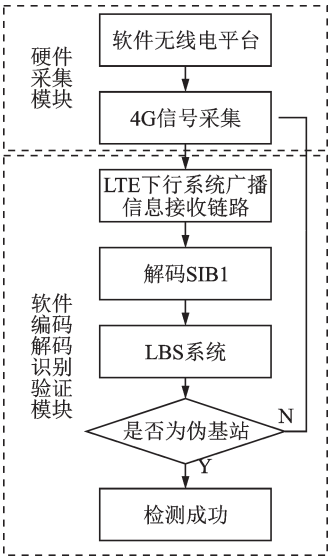

图3 LTE伪基站识别系统框图

Fig.3 LTE pseudo base station identification system block diagram

2.1 硬件采集模块实现

本文分析了中国移动、电信和联通的LTE技术标准和主要软件无线电硬件平台产品的技术性能。选用通信设备HackRF One作为开发支持的硬件,主要进行信号的收发、滤波、混频以及采样等前端处理[11-12]。其最大频率为6 GHz,覆盖了LTE的整个频段且带宽20 MHz刚好为LTE的最大带宽,AD采样率最大为20 Msps也可通过变采样理论变换到LTE标准采样率30.72 Msps,因此满足本研究的需求。

在Ubuntu18.04 LTS系统上结合HackRF搭建软件无线电平台,开发实现对4G信号的检测和采集的控制程序。HackRF实时采集固定频率和时段的数字IQ信号,通过搭建HackRF环境生成库文件以及hackrf_transfer可执行程序实现。对LTE所有频段进行扫描和跟踪通过开发LTE扫描程序实现。搜索到的LTE小区信息结合hackrf_transfer程序实现对相应频率的LTE信号采集并保存为二进制格

式的IQ数据,实现图3所示的硬件采集模块功能,为信息鉴别程序的解调解码提供数据。

2.2 软件解码模块实现

软件部分利用Matlab建立下行系统广播信息接收链路对SIB1解码,主要包括LTE信号预处理、小区搜索、信道估计以及下行物理信道解码等过程(见图4)。

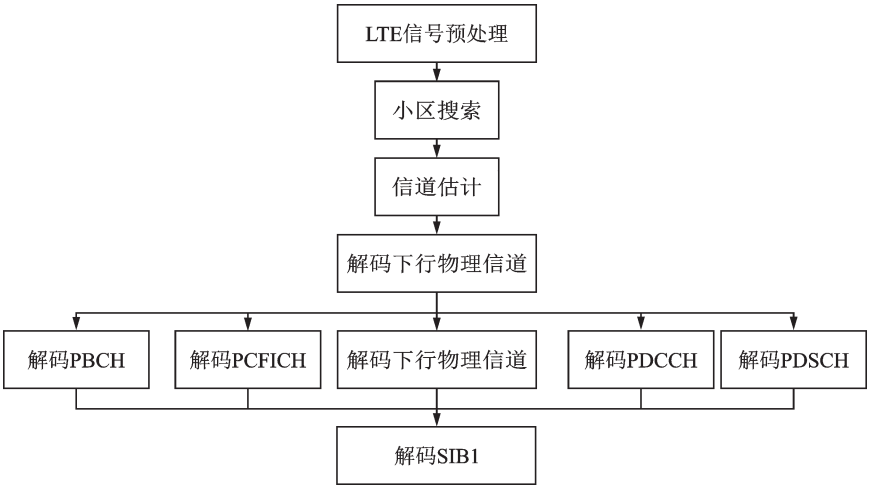

图4 LTE下行系统广播信息接收链路

Fig.4 LTE downlink system broadcast information receiving link

LTE信号预处理中,将HackRF采集到的8帧数字IQ信号转化为Matlab可识别的矩阵文件格式然后减去均值除去直流。由于数据采样率设置为19.2 Msps,利用变采样理论,在Matlab中通过一个8倍上升采样低通滤波器再每隔5个数据进行抽取,得到完整的20 MHz带宽且采样率为30.72 Msps的LTE信号。如图5所示,其中$I=8$,$D=5$。

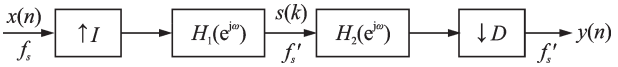

图5 变采样变换

Fig.5 Variable sampling transformation

小区搜索中通过检测主同步信号(Primary synchronization signal, PSS)N_{ID}^2和辅同步信号(Secondary synchronization signal, SSS)N_{ID}^1信号以及解码下行物理信道PBCH完成,由于同步信号具有良好的自相关特性,便于接收端专门用来下行同步[13-14]。本文采用基于时域的互相关算法对PSS信号进行检测,该算法对频率偏移敏感,为了确保检测的正确性和有效性,将本地PSS序列加上频率偏移,然后找到每个相应的频率偏移即时域上的时间偏移和各个PSS根指数相关的峰值,从而确定N_{ID}^2。将8帧的PBCH数据与之前生成并且添加过频率偏移的本地PSS序列进行滑动相关,检测到的相关峰值则是PSS所在位置的索引,计算公式为

$$Y[u]=\sum_{0}^{N-1}y[n]\,x_{f\mathrm{PBCH}}^{*}[n] \tag{1}$$

式中,$y[n]=h[n]\otimes x_{f\mathrm{PBCH}}+w[n]$,$h[n]$为离散的信道响应,$x_{f\mathrm{PBCH}}$为添加频偏后的本地PBCH离散数字IQ数据,$w[n]$为加性高斯白噪声。

由相关检测得到的峰值可以由式(2)推算出N_{ID}^2

$$N_{\mathrm{ID}}^2=\arg\max\left|Y[u]\right| \tag{2}$$

SSS信号则根据式(3—7)生成公式,采用逆向解扰获得N_{ID}^1。

$$q_p = \text{floor}(N_{\text{ID}}^{(l)}/30) \tag{3}$$

$$q = \text{floor}((N_{\text{ID}}^{(l)} + q_p \times (q_p + 1)/2)/30 \tag{4}$$

$$m_p = N_{\text{ID}}^{(l)} + q \times (q + 1)/2 \tag{5}$$

$$m_0 = \text{mod}(m_p, 31) \tag{6}$$

$$m_1 = \text{mod}(m_0 + \text{floor}(m_p/31) + 1 \tag{7}$$

式中，m_0和m_1为m序列的索引值，且(m_0,m_1)与N_{ID}^1值相对应，mod为取余操作，floor为向下取整函数。

后续利用PSS和SSS信号完成PBCH的解码。如表2所示，主信息块(Master information block，MIB)以40 ms为周期在PBCH上传输(同BCH)并重复传输4次，每次传输都携带相同的码块(Coded bit)。因此，在信道质量足够好的情况下，只接收这40 ms内的其中一个就能成功解码出MIB，为了确保其能够解码，前面已截取8帧信号。

图6展示了MIB如何由信道BCH和PBCH将bit级信息进行处理。MIB的bit位信息为20，经BCH，首先添加16位循环冗余校验(Cyclic redundancy check，CRC)；进行编码和速率匹配，使得其等于PBCH信道上40 ms内能够提供的空间，接着码块分段等分成片段，并分别添加CRC、信道编码以及速率匹配。最后进行码块重组形成码本送给PBCH处理。在PBCH处理链中，将码本进行加扰、调制、层映射、预编码和资源网格映射等过程，最终由快速傅里叶逆变换(Inverse fast Fourier transform，IFFT)形成正交频分复用(Orthogonal frequency division multiplexing，OFDM)符号[15]。在Matlab中根据协议中的规定细节设计相应模块即可逆向解码得到MIB信息。

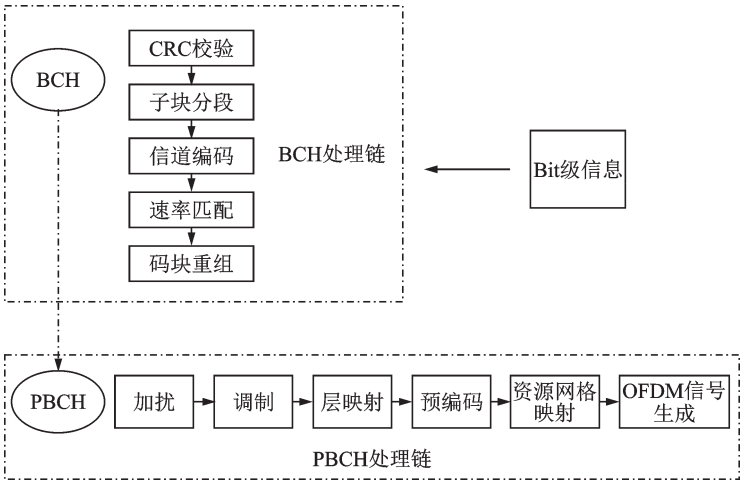

图6 BCH-PBCH处理链

Fig.6 BCH-PBCH chain processing

整个搜索过程的具体流程如图7所示。小区搜索获取到下行系统带宽后便可以对整个带宽信号进行信道估计以消除信道的干扰，从而减弱宽带通信时的多径时延带来的码间串扰问题。在Matlab中采用频域信道估计算法可降低复杂度，首先利用最大似然估计法计算信道传递函数(Channel transfer function，CTF)，然后经过时频域的转换得到信道的冲激响应[16-17]，由此得到信道估计值对CRS的信道估计$\boldsymbol{H}_n$。

$$\boldsymbol{H}_n = \boldsymbol{F}_n \boldsymbol{h} + Z_n \tag{8}$$

式中，n为CRS的数量，$\boldsymbol{h}$为信道的冲激响应且为向量，$\boldsymbol{F}_n$为对应参考序列的离散傅里叶变换矩阵，Z_n为白噪声功率。

最后仿照PBCH信道的解码过程，进行其他下行物理信道的解码获取SIB1信息。LTE中，LTE-

RRC协议都是ASN.1文法描述,并且是PER编码。为了更好地解码SIB1,本研究在Ubuntu18.04系统下构建LTE-RRC协议编解码器程序。利用36.331系列协议文档生成LTE-RRC的ASN.1描述文件,安装编译lameditor,生成36331-ac0.asn描述文件,然后生成LTE-RRC.ASN1解码程序。程序根目录下,Progname为LTE-RRC执行程序,sib_info.per为PER编码的SIB1信息文件,-p命令选项指示执行程序要运行的文件类型为BCCH-DL-SCH-Message,即下行共享信道中传播的系统广播信息SIBs。在Matlab中调用程序即可解码SIB1获取TAC和CID参数。

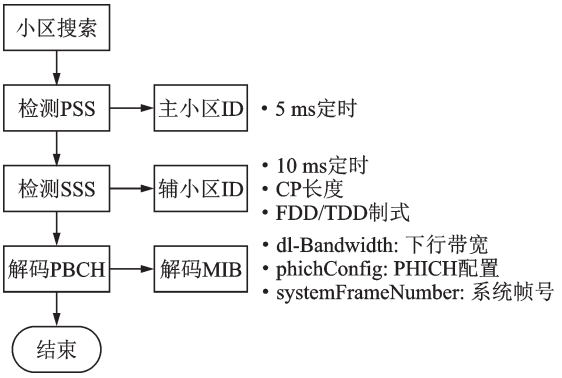

图7 小区搜索过程

Fig.7 Cell search process

3 实测验证

3.1 实测情况

数据采集平台和下行接收链路都搭建成功后,本研究分别对青岛的城市区域(测试点1)和海岸区域(测试点2)展开测试,以此验证提取技术的性能。测试1位于青岛市城阳区,将系统置于楼顶;测试2在小麦岛的海洋观测站放置系统,保证测试系统四周空旷无遮挡物,无干扰设施,测试环境良好。整个测试环境如表1所示。

表1 测试环境

Table 1 Measured environment

试验设备	测试环境
计算机操作系统	Ununtu18.04 LTS
软件无线电硬件外设	HackRF One
编程软件平台	Matlab
测试频段	LTE全频段
测试点1	山东省青岛市城阳区景康路城区附近
测试点2	山东省青岛市崂山区麦岛路郊区附近

首先利用CellSearch命令对LTE的所有频段进行扫描并将跟踪到的LTE信号利用hackrf_transfer程序将其8帧完整信号数据进行保存;然后在Matlab上利用下行系统广播信息接收链路对保存下来的数据进行处理,解码出系统信息块SIB1;最后将得到的TAC和CID参数利用LBS系统本地数据库进行校验,完成基站的定位和识别。

3.2 测试结果

2019年7月20日和2019年8月6日在测试点1和测试点2依照实测方案对附近LTE基站分别进行了验证测试。系统成功地实现基站信息解码。表2给出了测试点1得到的SIB1的解码信息。说明该测试点给出的5个基站的TAC和CID的二进制编码,形成了转化为十进制系统信息的基本数据。在测试点2的测量中,检测到2个基站,也得到了它们的TAC和CID的二进制编码。

将TAC和CID二进制参数转化为十进制输入到LBS系统中进行本地数据的对比,基于信息一致识别算法对基站进行鉴定,其中测试点1和测试点2的结果如表3所示。

由表1,测试点1所在城区测试地点为山东省青岛市城阳区景康路附近,测试点2所在的小麦岛郊区测试地点为山东省青岛市崂山区麦岛路附近。因此,实际检测到的基站坐标理论上应该一致。从表3的测试结果可知,基站1,2,5所显示的地理坐标与理论上的地理坐标一致,显然是合法基站;基站3的地理坐标在LBS本地数据库中未查询到,基本可以确定它是伪基站,如果再结合现有的伪基站定位算法便可以对其进行侦测和验证;基站4所显示的地点为福建省厦门市思明区,居然与基站的理论坐标相差几个省市的距离,明显存在异常。所以,该基站一定是伪基站。表3的结果表明对于小麦岛郊区基站6,7检测到的基站位置与理论上地理坐标一致所以为合法基站。

表2 测试点1中SIB1解码信息

Table 2 SIB1 decoding information in test point 1

LTE基站编号	SIB1具体参数	二进制
1	TAC(1)	101010000001001
	CID(1)	10111110110010100010001100
2	TAC(2)	11010001001100
	CID(2)	11010000000000010000110001
3	TAC(3)	11100100001010
	CID(3)	1110110001111110
4	TAC(4)	1000100100111
	CID(4)	10100100001101100000000001
5	TAC(5)	11010001001100
	CID(5)	11010000000000010000000011

表3 两个测试点中基站的识别结果

Table 3 Identification results of base stations in two test points

LTE基站编号	经纬度	对应地点
1	(36.242 418,120.415 734)	山东省青岛市城阳区景康路
2	(36.243 028,120.415 292)	山东省青岛市城阳区仙山东路
3	未查询到	未查询到
4	(24.440 627,118.070 43)	福建省厦门市思明区安海路44号
5	(36.242 955,120.410 323)	山东省青岛市城阳区同特物流园
6	(36.062 436,120.425 994)	山东省青岛市崂山区麦岛路1号
7	(36.062 297,120.427 997)	山东省青岛市崂山区东海东路1号

4 结束语

本文针对当前扰乱通信安全的伪基站问题,形成了用软件无线电技术提取基站信息的思路,提出了构建识别系统的一个新技术。论文设计了一个基于该技术的伪基站识别系统。系统用HackRF硬件设备搭建软件无线电平台实现对LTE信号的采集,通过软件Matlab建立下行系统广播信息接收链路对采集的信号进行解调解码。实测验证中分别对青岛城区和郊区两个试验点进行了测试。测试表明系统成功获取到SIB1参数中的CID和TAC,并基于信息一致识别算法验证检测到的基站是否为伪基站。试验表明将软件无线电技术应用在LTE伪基站识别中是可行的,为后续建立低成本灵活的新型伪基站检测系统研究提供基础。

参考文献:

[1] 刘泽忠.一种基于伪基站的GSM用户分选系统实现方案[J].通信技术,2013, 46(6): 127-129.
LIU Zezhong. An implementation scheme of GSM user sorting system based on pseudo base station [J]. Communication Technology, 2013, 46(6): 127-129.

[2] 姚景朋,张立志,何旭萌.基于三维联合检测法的伪基站检测系统方案设计[J].电子设计工程,2016, 24(14): 52-55.
YAO Jingpeng, ZHANG Lizhi, HE Xumeng. Scheme design of pseudo base station detection system based on three-dimensional joint detection method [J]. Electronic Design Engineering, 2016, 24(14): 52-55.

[3] 叶林刚.4G伪基站快速识别与定位分析[J].数字技术与应用, 2018, 36(7): 22, 24.

YE Lingang. Fast identification and positioning analysis of 4G pseudo base station [J]. Digital Technology and Application, 2018, 36 (7): 22, 24.

[4] 江浩. 基于移动端的伪基站识别与定位技术[D]. 武汉:华中科技大学, 2016.
JIANG Hao. Pseudo base station identification and positioning technology based on mobile terminal [D]. Wuhan: Huazhong University of Science and Technology, 2016.

[5] BALAKRISHNAN M, MEERJA K A, GUNDUGONTI K K, et al. Design of interfaces between high speed data converters and high performance FPGAs for software defined radio applications[J]. Telecommunication Systems, 2019, 71(4): 601-614.

[6] CHAUDHURI R B, BARMAN A D, BOGONI A. Design and analysis of photonic radio frequency multiband generation using transfer function approach in advanced design system software[J]. Optik, 2019, 182: 571-579.

[7] 孟俊伟. 基于软件无线电的GSM伪基站检测与定位[D]. 兰州: 兰州交通大学, 2016.
MENG Junwei. GSM pseudo base station detection and location based on software radio [D]. Lanzhou: Lanzhou Jiaotong University, 2016.

[8] 李国建, 郝恒. 基于GNURadio和USRP的未知信号检测技术研究[J]. 通信技术, 2017, 50(11): 2610-2616.
LI Guojian, HAO Heng. Unknown signal detection technology based on GNURadio and USRP[J]. Communication Technology, 2017, 50(11): 2610-2616.

[9] ZHANG H, TANG X, LI C, et al. PBSVis: A visual system for studying behavior patterns of pseudo base stations[C]// Proceedings of International Conference of Pioneering Computer Scientists, Engineers and Educators. Singapore: Springer, 2018: 599-610.

[10] YU F. An interactive visual system for generating striking pseudo base stations decisions[J]. Journal of Physics: Conference Series, 2019, 1237(5): 19.

[11] 王刚, 吴健健. 基于Gnuradio与Hackrf的无线通信收发系统实现[J]. 电脑知识与技术, 2016, 12(5): 34-36.
WANG Gang, WU Jianjian. Implementation of wireless communication transceiver system based on Gnuradio and Hackrf[J]. Computer Knowledge and Technology, 2016, 12(5): 34-36.

[12] 王晓丽, 赵树波, 王锐, 等. 基于GNU Radio与HackRF的无线通信系统实现[J]. 国外电子测量技术, 2018, 37(3): 13-17.
WANG Xiaoli, ZHAO Shubo, WANG Rui, et al. Implementation of wireless communication system based on GNU radio and HackRF[J]. Foreign Electronic Measurement Technology, 2018, 37(3): 13-17.

[13] SRIHARSHA M R, DAMA S, KUCHI K. A complete cell search and synchronization in LTE[J]. EURASIP Journal on Wireless Communications and Networking, 2017, 2017(1): 1-14.

[14] DEMEL J, KOSLOWSKI S, JONDRAL F K. A LTE receiver framework using GNU radio[J]. Journal of Signal Processing Systems, 2015, 78(3): 313-320.

[15] 刘映君, 舒睿俊, 刘立刚, 等. 基于SDR的智能电网系统PBCH加扰实现与优化[J]. 电子设计工程, 2018, 26(6): 81-85.
LIU Yingjun, SHU Ruijun, LIU Ligang, et al. Implementation and optimization of SDR-based smart grid system PBCH scrambling [J]. Electronic Design Engineering, 2018, 26 (6): 81-85.

[16] 李慧敏, 张治中, 李琳潇. LTE-A系统中基于小区参考信号的信道估计算法[J]. 计算机应用, 2018, 38(7): 2009-2014.
LI Huimin, ZHANG Zhizhong, LI Linxiao. Channel estimation algorithm based on cell reference signal in LTE-A system[J]. Journal of Computer Applications, 2018, 38(7): 2009-2014.

[17] 胡杨, 胡蝶. 一种LTE多小区干扰环境下的信道估计方法[J]. 太赫兹科学与电子信息学报, 2018, 16(4): 609-613.
HU Yang, HU Die. A channel estimation method in LTE multi-cell interference environment[J]. Journal of Terahertz Science and Electronics, 2018, 16(4): 609-613.

作者简介:

钟文华(1994-),男,硕士研究生,研究方向:无线电物理和软件无线电信号处理相关理论,E-mail:1260932133@qq.com。

王红光(1980-),男,高工,博士,研究方向:大气波导等电波环境和电波传播特性及其在无线电系统中的应用。

刘成国(1966-),男,博士,研究方向:电磁波理论与应用、电波传播与天线、射频与微波技术。

(编辑:陈珺)