DOI:10.19651/j.cnki.emt.2210509

基于 WiFi 嗅探的室内人员定位系统*

杨啸鹏 华国环
(南京信息工程大学长望学院 南京 210044)

摘 要：为了获知行人在楼宇中的位置信息,设计了一个基于 WiFi 嗅探的室内人员定位系统。使用 WiFi 指纹法来实现定位功能,并在指纹法中引入信道特征,来分析不同信道对信号强度的影响。本设计的主控芯片选用了国产安路公司的 FPGA 芯片,使用 FPGA 芯片进行指纹库的匹配,同时依靠 FPGA 丰富的拓展接口,本设计开发了局域网网站以及基于串口屏的显示界面来进行人机交互。以南京信息工程大学文德楼 3 楼北区为实验地点,在 2 m 宽的走廊里,本系统对 14 个房间的定位准确度均可以达到 90%,响应时间小于 6 s。本设计所有器件均为国产,推广性较好,应用范围较广。

关键词：WiFi 嗅探;指纹法;国产 FPGA;局域网;串口屏
中图分类号：TP806.1 **文献标识码**：A **国家标准学科分类代码**：510.4050

Indoor positioning system based on WiFi sniffing

Yang Xiaopeng Hua Guohuan
(Changwang School of Honors, Nanjing University of Information Science & Technology, Nanjing 210044, China)

Abstract: In order to get the location information of pedestrians in buildings, an indoor personnel location system based on WiFi sniffing is designed. The WiFi fingerprint method is used to realize the positioning function, and the channel characteristics are introduced into the fingerprint method to analyze the influence of different channels on the signal strength. The main control chip of this design selects the FPGA chip of the domestic Anlu company, and uses the FPGA chip to match the fingerprint library. At the same time, relying on the rich expansion interface of FPGA, this design has developed a LAN website and a display interface based on the serial port screen for human-computer interaction. Taking the north area of the third floor of Wende building of NUIST as the experimental site, in the 2 m wide corridor, the positioning accuracy of the system for 14 rooms can reach 90%, and the response time is less than 6 s. All devices in this design are made in China with good popularization and wide application range.

Keywords: WiFi sniffing;fingerprint method;domestic FPGA;LAN;serial screen

0 引 言

在定位领域,随着 GPS 等卫星导航技术的发展,室外定位技术发展已经很成熟,但民用 GPS 定位精度只有 2 m 且室内无法接收卫星信号,因此室内定位技术具有极高的研究价值。同时,室内定位技术也具有很好的市场价值[1-2],2022 年室内定位市场规模预计可以达到 409.9 亿美元。

目前室内定位的技术研究也比较多,有 A-GPS,超声波,红外线,地磁,RFID,蓝牙、WiFi 等[3-4]。其中 WiFi 技术通过接收信号强度(即 RSSI)等方式实现复杂环境下的定位[5]。虽然在室内环境中 WiFi 信号传输容易受到多径效应和环境影响,但其不需要额外部署设备,可以依托现有的 WiFi 设备,所以是目前室内定位技术研究热点。

本文设计的基于 WiFi 嗅探的室内人员定位系统,是以国产 FPGA 芯片 EG4S20BG25617 为主控芯片,使用 AP851-US 探针、ESP8266 与串口屏的定位系统。该系统具有定位较快、实用性强、国产化、应用范围广的特点。

1 工作原理与总体方案设计

1.1 工作原理

现阶段,因为室内环境错综复杂,通过接收到的室内 WiFi 信号强度来计算信号的衰减进而计算距离是很困难的。WiFi 指纹法因为绕开了复杂的计算,在 WiFi 定位领

收稿日期:2022-06-28
* 基金项目:国家自然科学基金(12074192)项目资助

域得到了广泛应用[6]。指纹法定位可分为两部分，在线阶段与离线阶段[7]，如图 1 所示。

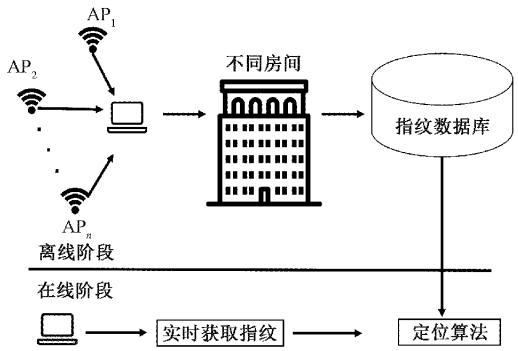

图 1　指纹法原理

离线阶段：在离线阶段需要实地采集各个房间的 WiFi 数据。该 WiFi 数据是路由器信号经过衰减、多径效应之后的信号，记录其特征与房间的对应关系，可以避免计算无线信号的衰减[8]。通过筛选 WiFi 数据，可以构成一张路由器 MAC 地址与房间的对应关系，即指纹库。指纹库如表 1、2 所示。

表 1　房间与路由器

房间	MAC_1	MAC_2	…	MAC_N
$room_1$	RSS_1^1	RSS_1^2	…	RSS_1^N
$room_2$	RSS_2^1	RSS_2^2	…	RSS_2^N
⋮	⋮	⋮	⋱	⋮
$room_M$	RSS_M^1	RSS_M^2	…	RSS_M^N

表 2　不同信道的 RSS 强度

channel	1	2	3	…	13
rss	rss_1	rss_2	rss_3	…	rss_{13}

在以往指纹库的研究中指纹库的构建以表 1 为主，极少考虑 WiFi 信道对 RSS 的影响，本设计引入信道类型作为指纹库构建的指标[9]。其中 $room_i(i=1,2,\cdots,M)$ 为采样点，RSS_i^j 是第 i 个房间中第 j 个路由的信号数据集。在 IEEE 802.11 b/g 2.4 GHz 标准中，将工作频段划分为 13 个信道，不同信道在楼宇中的衰减也不相同。在表 2 中每个信道有不同的信号强度 $rss_k(k=1,2,\cdots,13)$，rss_k 是多次采样之后的平均值。

在线阶段：在线阶段主要是将实时获取到的房间的 WiFi 信息与数据库进行匹配，从而获得相应的位置信息。有时会配合聚类、滤波算法提高匹配精度[10-11]。

1.2　总体方案设计

基于 WiFi 嗅探的室内人员定位系统的总体设计包括定位系统硬件设计、局域网系统设计、FPGA 定位算法设计。系统框架如图 2 所示。

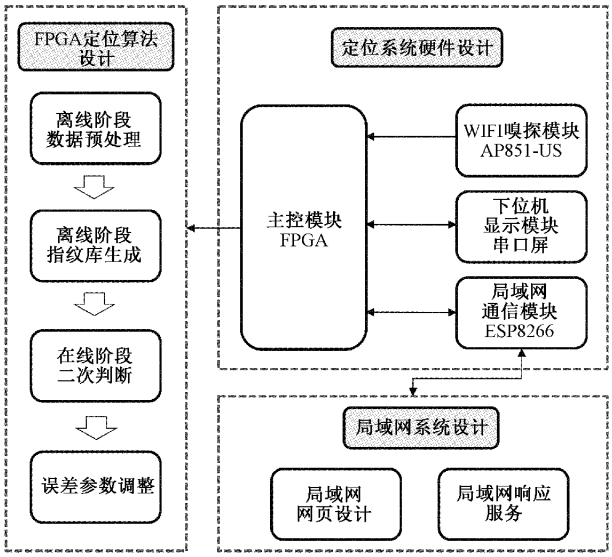

图 2　系统框图

2　定位系统硬件设计

硬部分主要包括主控模块、WiFi 嗅探模块、下位机显示模块、局域网通信模块。

2.1　主控模块

主控芯片使用的是中国安路公司的 EG4S20BG25617 芯片。该芯片有 23 520 个四输入查找表，最大 156.8 K 容量的分布式 RAM，64 个 9 kB 嵌入式 ram，最高 200 MHz 工作频率 64 Mbit 的 SDRAM，3 个 PLL，1MSPS12-bitSAR 型 ADC。该国产芯片搭配了自研的 EDA 工具 TD，可以满足对 FPGA 硬件逻辑设计的需求，同时 FPGA 是并行逻辑，定位算法与跟外设通信可同步进行，可以缩短响应时间[12]。

2.2　WiFi 嗅探模块

WiFi 嗅探模块使用的是 WiFi 探针 AP851-US。该模块采用串口通信协议进行传输，体积较小，功耗较低，便于携带和户外使用。该模块能接收到的信号种类众多，不仅包含手机系统和电脑系统，同时可以接收路由器 SSID/MAC 以及关联设备的信息。其发送的数据格式如表 3 所示。

表 3　AP851-US 的数据格式

数据段	数据格式	数据段	数据格式
1	探针 MAC	5	信号强度
2	捕获 MAC	6	网关类型
3	捕获类型	7	密钥算法
4	信道类型	8	未知 MAC

2.3　局域网通信模块

本系统的使用场景是在室内，而在室内环境中有着丰富的 WiFi 资源，所以上位机与下位机的通信过程使用局域

网通信是对资源极好的利用。本部分选用了中国乐鑫公司的 ESP8266 通信模块。

ESP8266 使用无线终端模式,该模式下,ESP8266 可以当作客户端,与手机、电脑等终端设备一致,通过 WiFi 连接上无线路由器[13],如图 3 所示。

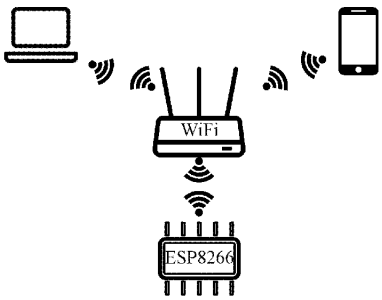

图 3 ESP8266 工作模式

ESP8266 连接入局域网需要提前将 WiFi 名称与密码写入。当位置信息确定之后上位机就可使用 IP 地址通过局域网对 ESP8266 进行访问。

2.4 下位机显示模块

每次局域网分配的 IP 是未知的,所以需要通过下位机显示模块显示连接的 WiFi 名称以及 IP 地址。下位机显示模块使用了中国淘晶驰公司的串口屏,型号为 TJC4024T032_01。在具体使用中,串口屏也可作为与用户的交互界面,显示当前的位置信息[14]。串口屏界面设计如图 4 所示。

图 4 串口屏界面设计

如上所述,设计了 WiFi 名称与 IP 以及房间信息界面,同时该界面左下角增加了“开始定位”触控按钮,用于人机交互。硬件实物如图 5 所示。

3 FPGA 定位算法设计

3.1 指纹法离线阶段

本次设计选择了南京信息工程大学文德楼 3 楼北区作为实验地点。该楼层是环形结构,每一间教室都配有路由器。地图如图 6 所示。

指纹库的构建首先需要在各个房间搜集 WiFi 信息。为了避免偶然性,提高指纹库的准确性,共进行了 3 轮数据搜集。

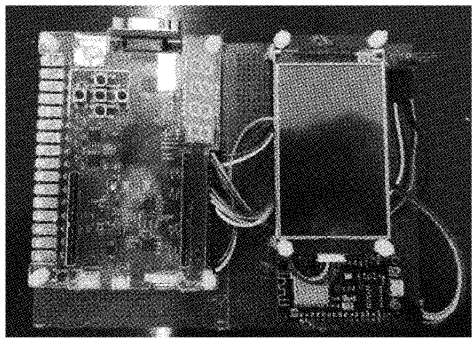

图 5 基于 WiFi 嗅探的室内人员定位系统实物

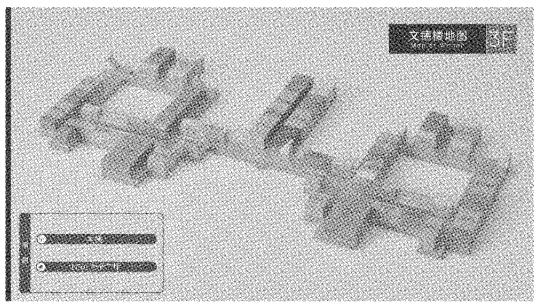

图 6 南京信息工程大学文德楼三楼

各个房间的 WiFi 信号数据是原始数据,其中不仅包含了指纹库建立所需的路由器 MAC 地址、路由器信号强度等有用信息,还包含了诸如探针 MAC 地址、网管类型、密钥算法等无用信息。所以需要在原始数据中剔除无用信息,并且根据一定的指标(如信号方差、信号出现频率)筛选数据,本阶段设立了如下 5 个筛选流程以及筛选标准[15]。

1)选出 3 个数据库中,每一轮都出现的路由器的 MAC 地址。在这一步中只保留探针返回的捕获类型是“ap”与“client”的数据,将对应非路由器设备的“unknown”捕获类型数据删去。

2)针对第一轮选出的路由器,将其 MAC 地址作为索引依据,在 3 个数据库中将同一个路由器的不同信道的数据记录下来。

3)针对每个路由器,记录不同信道的出现次数并求解该信道的平均信号强度以及方差。

4)设定阈值。筛选出出现次数大于 20 次,方差小于 15 的信道数据。

5)若有在不同房间同时出现并且信道相同,信号强度相近的数据,删去其中一个房间的数据。

由此,通过层层筛选得到了在 3 个数据库中都频繁出现且信号强度稳定的 WiFi 数据集合。该集合就是 WiFi 指纹库,包含路由器 MAC、信道、信号强度。

以房间 N301 为例,在完成上述的数据筛选之后,得到了如表 4 所示的指纹库信息。

表 4　N301 数据库展示(部分)

路由器 MAC	信道	次数	均值/dBm	方差
a4560273bc47	11	91	74.53	14.18
28d127b3b963	2	55	82.12	4.12
600b03552fa1	6	41	74.97	2.97
600b03546430	1	39	85.87	4.19
600b03546430	6	27	72.91	3.42

表 4 所示，第 4 和第 5 条指纹数据是来自同一个路由器的不同信道。信道类型的引入提高了指纹库的识别精度，细化了路由器不同的工作状态。

表 4 第 1 条记录中的方差与其他数据相差较大，考虑是该路由器的该信道数据量较大，共探测到 91 次，其中存在个别异常值，从而增加了方差。经过测试，方差小于 15 的数据可以满足定位需求。

3.2　指纹法在线阶段

Chen 等[15]在指纹法匹配过程中使用了决策树的方式来减少索引次数[16]。但是决策树增加了前期开发时间，需要因地制宜地设计决策分支，不利于项目普及。FPGA 因其并行逻辑，可以在与外设通信过程中进行指纹法的匹配过程，所以在合理利用时序的情况下，使用遍历的方法也可以适用于容量较大的指纹库的匹配任务，有利于普及。如图 7 所示。

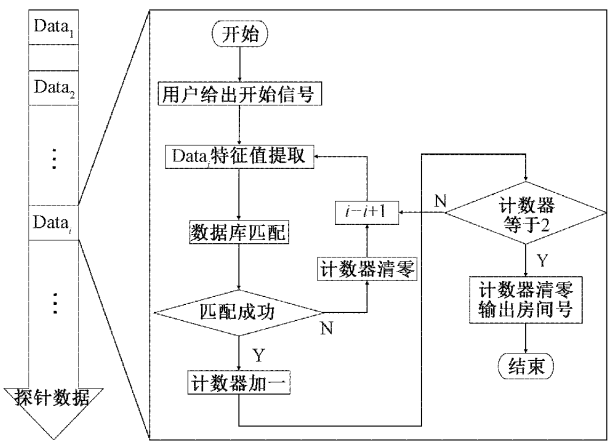

图 7　在线阶段流程

在流程中增加了二次判断用于解决到达两房间信号强度相近的情况，如图 8 所示。当实际信号与指纹库中的信号强度之差小于设定的误差参数就可以认为是匹配成功。

在数据筛选阶段对于图 8 情况是删去了其中一个房间数据，在实际操作的时候两个房间信号可能会在指纹库中匹配失误，使用二次判断可减少出错的几率。

在现阶段实测数据如表 5 所示。

上表呈现了房间 N302 和 N308 在现阶段的数据。两个房间的定位时间均值分别为 4.4 与 5.3 s，考虑是 N308 房间可探测到的 WiFi 信号数量大于 N302 房间，所以在现

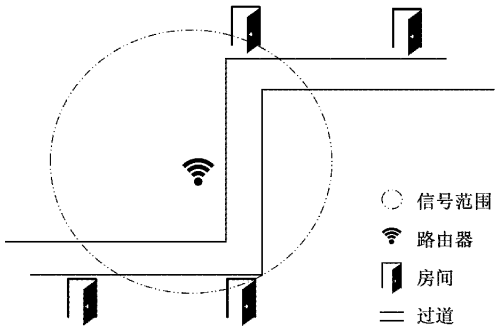

图 8　WiFi 信号强度相近情况

表 5　指纹法在现阶段数据(部分)

编号	房间号	路由器 MAC	信道	用时/s	结果
1	N302	08b3af1f36a7	6	2.4	N302
2	N302	005a13478f74	8	5.2	N302
3	N302	005a13478f74	8	5.1	N302
4	N302	fcd7339a888a	3	5.6	N302
5	N302	9c9d7e54c7c3	4	4.3	N302
6	N302	9c9d7e54c7c3	4	3.9	N302
7	N302	040e3c816b3d	4	3.2	N302
8	N302	ec888f7f031c	6	4.9	N303
9	N302	600b0339acb8	6	4.2	N302
10	N302	600b0339acb9	6	5.1	N302
11	N308	040e3c816b3d	6	6.2	N308
12	N308	060e3c81eb3d	6	4.8	N308
13	N308	005a13478f74	9	4.6	N308
14	N308	005a13478f74	10	3.4	N308
15	N308	005a13478f74	11	5.7	N308
16	N308	80ea07507036	5	6.7	N308
17	N308	80ea07507036	5	5.4	N308
18	N308	08b3af1f36a7	5	4.2	N308
19	N308	86454bcce8cc	6	5.6	N308
20	N308	060e3c7358e8	10	6.7	N309

阶段检索的时间更长。同时，两个房间在 10 次的测试中，都存在一次定位错误，编号为 8 与 20，并且都是该房间与相邻房间的误判，考虑是由于两个相邻房间距离较近，数据库中存在两个指纹相似的情况，信号在传播过程中受到扰动，从而造成了判断错误。这两个房间的定位准确度都能保持在 90%左右。

3.3　FPGA 程序总体框架

除了构建匹配算法，也需要实现与各个模块的通信与数据提取[17]。FPGA 程序总体框架如图 9 所示。

4　局域网系统设计

系统中的局域网增加了通信距离，也符合室内定位的楼宇环境。为了方便用户使用，放弃了 AT 指令的操作方式，而是设计了相配套的局域网网页来显示时间与位置信息。

网页设计的界面如图 10 所示。

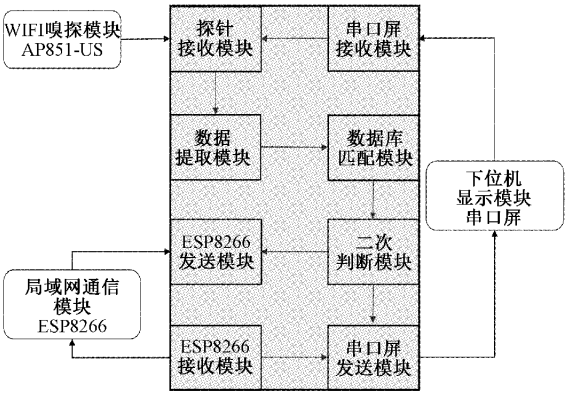

图 9　FPGA 程序总体框架

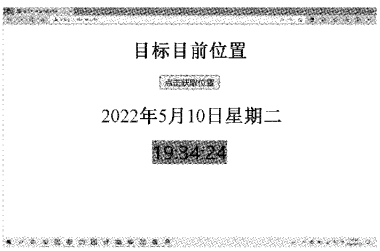

图 10　网页设计界面

该网页的运行流程如图 11 所示。

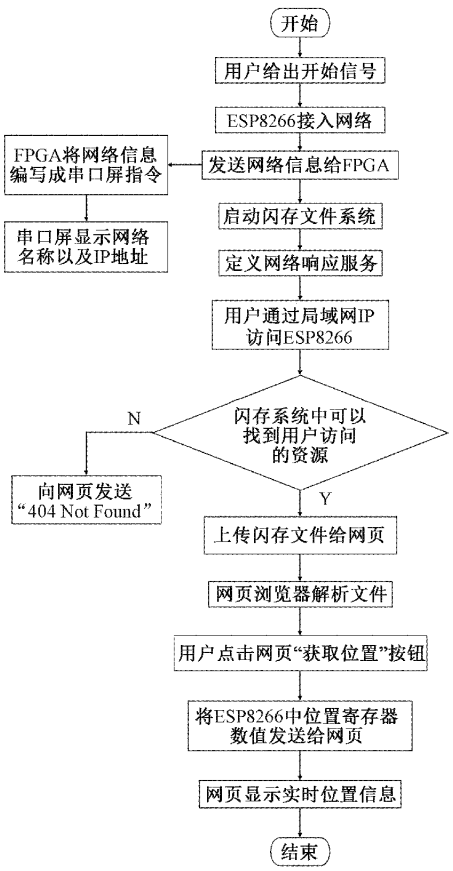

图 11　网页响应流程

5　实测与分析

本系统需要先让上位机与定位系统连接入同一个局域网,在定位系统定位成功之后,上位机可通过浏览器访问定位系统。图 12 以房间 N301 为例。

图 12　N301 定位结果

由图 12 可知,实际定位点显示的房间号码与上位机端是一致的,其余房间类似。通过改变设定的误差参数可以调整定位的精度,通过实际测试,本设计中误差参数设定为 3 dBm,定位精度两米,即在采样点距离两米的范围内定位可以兼顾定位准确性与响应时间。各个房间的定位时间与定位准确度如表 6 所示。

表 6　二次判断实测结果(部分)

房间	定位时间/s	定位准确度/%
N301	5.3	80
N302	4.4	90
N303	5.4	100
N304	5.7	100
N305	5.3	100
N306	5.8	80
N307	5.4	90
N308	5.3	90
N309	6.0	100
N310	6.1	90
N311	5.2	90
N312	5.8	80
N313	5.9	90
N314	4.3	90

在引入二次判断之后,一次判断与二次判断的时间消耗与准确率对比如表 7 所示。

可以看到在进行二次判断之后,在时间增加了 68.75%情况下,可以较大提高准确率。在 2 m 宽的走廊内,均可以实现 90%的定位准确度。

表 7　一次判断与二次判断对比

参数	结果
一次判断平均时间/s	3.2
二次判断平均时间/s	5.4
一次判断准确率/%	70
二次判断准确率/%	90

6　结　　论

本文介绍了一种基于 WiFi 嗅探的室内人员定位系统。系统主要包括 WiFi 嗅探模块、下位机显示模块、局域网通信模块。系统定位时间总体小于 6 s，准确率均在 90%。在常用指纹法基础上使用信道作为指纹特征，针对楼宇的使用场景设计了局域网网页，并且使用 FPGA 加快了指纹匹配速度。本系统主要可用于医院指定病房送药、大型饭店指定包厢送餐等需要楼宇内定位以及通信的场景，应用范围较广。同时本系统所使用模块均为国产，推广性较好。

参考文献

[1] Indoor Atlas. The rise of indoor positioning-a 2016 global research report on indoor positioning market[R]. 2016.

[2] 万潇阳，孙耀华，王则予. 6 G 室内定位技术原理与展望[J]. 电信科学，2021，37(6)：91-104.

[3] 廖文光. 物联网室内定位技术对比分析[J]. 中国有线电视，2021(1)：48-51.

[4] 马亚松. 基于无线传感器网络的远程室内人员定位系统设计[D]. 太原：中北大学，2017.

[5] 刘夫玉. 基于地磁场和智能手机的粒子滤波室内定位算法[D]. 南京：南京邮电大学，2017.

[6] KHALAJMEHRABADI A，GATSIS N，AKOPIAN D. Modern WLAN fingerprinting indoor positioning methods and deployment challenges [J]. IEEE Communications Surveys & Tutorials，2017，19(3)：1974-2002.

[7] 乐燕芬，许远航，施伟斌. 基于 DPC 指纹子空间匹配的室内 WiFi 定位方法[J]. 仪器仪表学报，2021，42(11)：106-114.

[8] 郑学伟. 基于权值参数的 WiFi 定位算法研究[J]. 国外电子测量技术，2014，33(3)：35-37，50.

[9] 杨敏，刘思怡. 一种基于先验信息的 WiFi 室内定位方法[J]. 电子测量与仪器学报，2020，34(6)：163-168.

[10] 王阳，叶芝慧，冯奇，等. 基于 Android 的室内 WiFi 定位系统设计与实现[J]. 电子测量技术，2016，39(9)：16-19.

[11] 卿怀军. 基于机器学习的数字信号调制识别及 FPGA 设计与实现[D]. 北京：北京交通大学，2021.

[12] 马媛. 基于 ESP8266 的无线通信系统设计[J]. 电子测试，2022，36(5)：44-46.

[13] 李梁京，张雪芹，刘华波. 基于 USART-HMI 智能串口屏的节能恒温控制系统设计[J]. 制造业自动化，2021，43(9)：140-143.

[14] 崔雯雯. 基于 CNN 的 WLAN 室内定位系统设计与实现[D]. 银川：宁夏大学，2021.

[15] CHEN Y Q，YANG Q，YIN J，et al. Power-efficient access-point selection for indoor location estimation[J]. IEEE Transactions on Knowledge and Data Engineering，2016，18(7)：877-888.

[16] 杨洋，和蕾，王旭，等. 基于 FPGA 的 UART 串行通信参数自适应设计与实现[J]. 电子设计工程，2021，29(16)：21-25.

[17] 夏宇闻. Verilog 数字系统设计教程[M]. 北京：北京航空航天大学出版社，2008.

作者简介

杨啸鹏，本科，主要研究方向为传感器信号采集系统。

E-mail：1810480975@qq.com

华国环，博士，讲师，主要研究方向为传感器技术和数模混合集成电路。

E-mail：hgh20010@163.com