ISSN 1002-4956
CN11-2034/T

实 验 技 术 与 管 理
Experimental Technology and Management

第 36 卷 第 2 期 2019 年 2 月
Vol. 36 No. 2 Feb. 2019

DOI:10.16791/j.cnki.sjg.2019.02.040

基于 Wi－Fi 嗅探技术的实验室管理系统设计

高 军[1]，王仲逸[1]，汪砚铖[1]，高泽坤[2]

（1. 东北大学秦皇岛分校 计算机与通信工程学院，河北 秦皇岛 066004；
2. 浙江大学 海洋学院，浙江 舟山 316021）

摘 要：为加强开放实验室的管理，设计了一种基于 Wi-Fi 嗅探技术的人员管理系统。该系统使用基于 ESP8266 芯片的 ESP-WROOM-02 模块解析智能手机的 MAC 地址，在服务器端将该地址与系统存储的数据进行匹配，实现实验人员实时签到功能，并统计出使用实验室的人数和使用情况。通过部署多个 Wi-Fi 嗅探器，可进行实验人员的实时定位和现场安全监测等。利用上述信息，可以实现开放实验室的优化管理。

关键词：Wi-Fi 嗅探；实验室管理；实时定位

中图分类号：TP311.52；G647 **文献标识码**：A **文章编号**：1002－4956(2019)02－0165－03

Design of laboratory management system based on Wi－Fi sniffing technology

GAO Jun[1], WANG Zhongyi[1], WANG Yancheng[1], GAO Zekun[2]

(1. School of Computer and Communication Engineering, Northeastern University at Qinhuangdao, Qinhuangdao 066004, China; 2. Ocean College, Zhejiang University, Zhoushan 316021, China)

Abstract: In order to strengthen the management of open laboratories, a personnel management system based on Wi-Fi sniffing technology is designed. This system uses the ESP-WROOM-02 module based on the ESP8266 chip to analyze the MAC address of the smartphone, matches the address with the data stored in the system on the server side, realizes the real-time check-in function of the experimenter, and counts the number and use of the laboratory. By deploying multiple Wi-Fi sniffers, the real-time positioning, on-site safety monitoring of experimental personnel, etc., can be carried out. Based on the above information, the optimal management of open laboratories can be realized.

Key words: Wi-Fi sniffing; laboratory management; real-time positioning

在高校开放实验室，会采用指纹签到[1-2]、打卡（门禁）[3-4]等考勤方式记录学生进出和使用实验室的信息。这些传统考勤方式不能实时统计实验室内人数，而且考勤过程烦琐，当同时进入实验室的人数较多时容易造成拥挤。本文提出一种基于 Wi-Fi 嗅探技术的开放实验室人员统计管理系统。当学生携带的智能手机 Wi-Fi 处于唤醒状态时，会被该系统的 Wi-Fi 嗅探器捕获。该学生在实验室的时间、位置将被实时记录。相比于传统考勤方式，不但有效地提高了签到效率，还可以提供各个时段学生名单、人数以及实验室使用率等数据信息，辅助实验室的优化管理。

收稿日期：2018-08-28

基金项目：河北省高等学校创新创业教育教学改革研究与实践项目（2017CXCY137）

作者简介：高军（1971—），男，河北昌黎，硕士，副教授，主要研究方向为无线传感器网络.

E-mail：gaojun@neuq.edu.cn

1 系统结构

1.1 Wi-Fi 嗅探原理

在 IEEE 802.11 协议中，移动设备接入 Wi-Fi 的过程有扫描（scanning）、认证（authentication）和关联（association）。

在扫描阶段，移动终端发现 AP 有两种方式：（1）被动扫描，扫描过程中不需要传送任何关联信号；（2）主动扫描，移动终端以主动的方式在每个信道上发出探测请求帧（probe request），请求某个无线网络回应。若某个信道收到帧，则可以进行探测。

在认证阶段，AP 进行身份验证，通过验证后，移动终端才能进行访问。

在关联阶段，AP 返回认证相应信息，认证通过后可以进行关联，然后成功接入并可以使用无线网[5-8]。

移动终端向外广播的探测请求帧正是嗅探器需要

捕获的。捕获探测请求帧数据包后，通过地址解析协议(ARP)，将移动终端的IP地址转换为对应的物理地址(即MAC地址)[9]。MAC地址是每台移动设备独有的6字节、十六进制地址，前3个字节由IEEE的注册管理机构分配给厂家。MAC地址被写入网络适配器中，具有全球唯一性[10]。

1.2 系统结构

基于Wi-Fi嗅探技术的实验室管理系统的结构如图1所示。智能终端是智能手机等可连入Wi-Fi的移动设备。

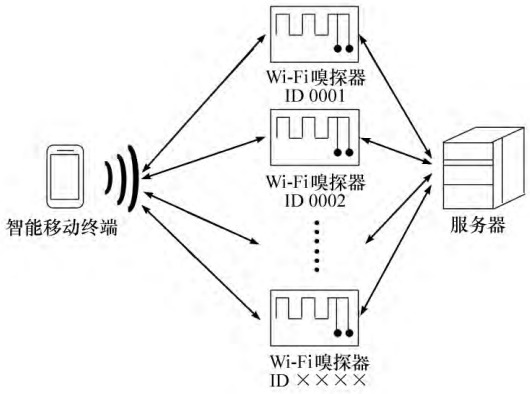

图1 系统结构

嗅探模块包括天线、ESP8266芯片和GPRS模块MGTC-1030。ESP8266芯片完成对移动终端主动发送的IEEE 802.11探测请求帧数据包的捕获，该芯片嵌入超低功耗32位RISC处理器，支持实时操作系统和Wi-Fi协议栈，使本系统能够快速存储和处理数据。芯片内的SRAM提供了数据存储空间，利于程序的稳定和提高处理效率，并且支持I^2C、UART、SPI等类型的接口，实现本系统与PC的数据交换。

天线用于无线数据包的获取和信号的发送。

GPRS模块实现模块和服务器之间的数据传输。在学校里，Wi-Fi、以太网会受校园网的安全限制，而GPRS通过允许现有Internet和新的GPRS网络互通，完全实现移动Internet功能[11]。因此，选择GPRS用以传输会更方便。嗅探模块组成如图2所示。

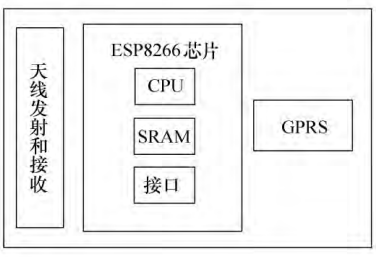

图2 嗅探模块组成图

系统采用B/S架构，客户端计算压力较小，客户端大大简化[12]，在浏览器页面即可读取数据信息。Wi-Fi嗅探器将数据以设定的格式通过GPRS传输到服务器，服务器架设在云空间，采用MySQL数据库，其特点是体积小，速度快，开发成本低。MySQL数据库集群架构能够满足云平台下存储扩展的要求，保证在云平台安全稳定地运行[13]。

2 数据格式

嗅探模块每分钟发送一次数据。上行的数据包长$4+9n$个字节，n为探测到的接入Wi-Fi的移动终端数量。上行的数据格式为：帧头(1字节)＋探针ID(1字节)＋分隔符(1字节)＋MAC地址(6字节)＋信号强度(2字节)＋分隔符(1字节)＋MAC地址(6字节)＋信号强度(2字节)＋分隔符(1字节)＋MAC地址(6字节)＋信号强度(2字节)＋…＋校验(1字节)＋帧尾(1字节)。

传输过程数据为16进制，在传输时探针编号转换为16进制。分隔符和信号强度用转义符，校验码在去掉帧头、帧尾和分隔符之后按位与，取最后一个字节，应该等于探针编号。

每个实验室可以有多个探针，因此需要设置探针编号(ID)，以分辨数据的来源。在得知来源实验室和具体探针之后，即知道了数据的来源。分隔符的作用是方便上位机(PC端)处理数据。MAC地址和信号强度为实时探测到的移动终端信息。校验码若有错，则丢弃该包。帧的最后以帧尾标识一次传送的结束。数据格式示例如图3所示。

帧头	探针编号	分隔符	MAC地址	信号强度	……	校验	帧尾
0xFF	0x01	\1	C472954D5D23	\x55		0x01	0xFE

图3 数据格式示例

PC端对数据处理时，通过分隔符将数据分开，然后将每组MAC地址和对应信号强度进行存储、分类和显示。

3 系统功能

系统中预先录入人员移动终端的MAC地址，利用探针获得的信息对MAC地址进行统计和分析，可实现人员分布的实时监测。系统功能主要包括定位分析模块和考勤统计模块。

3.1 定位分析

为了监控多个实验室的人员信息，在每个实验室都安放1个或者多个探针，并且在服务器中把探针的ID和实验室名称进行绑定(见图4)。由于信号强度的

不稳定，可能存在某一区域被多个探针覆盖的情况。例如某学生携带的手机除了会被他所在的大数据实验室中的 1 号探针探测到，也可能被邻近的其他 3 个探针探测到。但因为距离不同，这 4 个探针得到的 RSSI 会不同。通过对比每个探针接收到的某移动终端信号的 RSSI 值大小，可知该移动设备离 1 号探针最近，系统对其定位在大数据实验室。

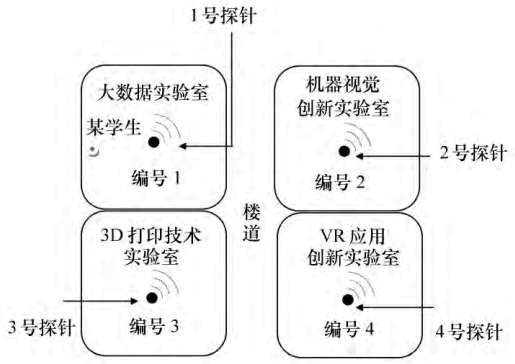

图 4　多实验室探针配置情况

3.2　考勤统计

由于系统可以通过探针获取智能终端的首次探测时间、最后探测时间等信息，只需要将捕获的 MAC 地址和预先录入系统的 MAC 地址相匹配，即可获得对应人员的出勤时间。首次探测时间可以作为第一次打卡，最后探测时间可作为最后离开实验室时间（见表 1）。

表 1　探针探测信息

姓名	MAC 地址	首次探测时间	最后探测时间
王某某	C472＊＊＊＊5D23	04-17 08:53	04-17 16:35
张某某	6896＊＊＊＊CD47	04-17 09:26	04-17 13:18
李某某	9CF3＊＊＊＊79C5	04-17 14:20	04-17 18:20
滕某某	0026＊＊＊＊7890	04-17 10:11	04-11 17:44

系统可以统计某段时间学生进入实验室的天数及累计时长（见表 2）。掌握这些时间数据，可以知道各个实验室的使用时段、时长、人数和频率等信息，可用于实验室资源的合理规划。

表 2　一周出勤时长统计

姓名	工作天数/d	实到天数/d	累计时长/h
王某某	7	6	35
张某某	7	7	37
李某某	7	6	30
滕某某	7	3	12

4　结语

基于 Wi-Fi 嗅探技术的开放实验室管理系统实用性很强。利用 Wi-Fi 嗅探技术收集到的实验室使用频率和使用人数等信息，可以判断哪些实验室需要优先扩大空间和更新设备等，以满足更多学生的需求。目前，该项目已经获得东北大学秦皇岛重点实验室项目资金的支持。在进行 1 年的测试中，该系统体现出方便使用、成本较低、可靠性高等优点。该系统的投入使用，提高了实验室的管理效率，给学院领导决策提供了有价值的参考数据，具有很好的推广前景。

参考文献(References)

[1] 刘欢，方华. 基于指纹识别的实验室门禁管理系统设计[J]. 微型机与应用，2016，35(23)：93-95，99.

[2] 许晓琳，吴向荣. 现场指纹录入常见问题及解决方法[J]. 海峡科学，2014(11)：50-51.

[3] 郭峰，陈晨，郭建平. 基于门禁的实验教学中心智能管理系统研究[J]. 现代商贸工业，2017(14)：180-181.

[4] 黄芳，柏亚妹，蒋斌，等. 基于门禁的开放式护理实践教学管理系统设计与实践[J]. 无线互联科技，2017(20)：64-66，80.

[5] CUNCHE M，KAAFAR M A，BORELI R. Linking wireless devices using information contained in Wi-Fi probe requests[J]. Pervasive and Mobile Computing，2014，11：56-69. DOI：10.1016/j.pmcj.2013.04.001.

[6] BARBERA M V，EPASTO A，MEI A，et al. Signals from the crowd：uncovering social relationships through smartphone probes[C]// Proceedings of the 2013 conference on Internet measurement conference . 2013. DOI：10.1145/2504730.2504742.

[7] FREUDIGER J. How talkative is your mobile device ?：an experimental study of WiFi probe requests[C]//Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks. New York，USA：ACM，2015：8-14.

[8] 赵飞飞，金彦亮，熊勇. 基于 WiFi 嗅探的感知系统研究[J]. 电子测量技术，2016，39(10)：108-113.

[9] 陈浩. ARP 地址解析协议应用[J]. 科技资讯，2009(1)：16.

[10] IEEE Standard Association. 802.11TM-2012. IEEE Standard for Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY)[S].

[11] 于宝堃，许国，胡瑜，等. 基于 GPRS 的实验室监测系统[J]. 电子设计工程，2010，18(2)：7-8，11.

[12] 苏东震，陈明，史忠植. 基于 B/S 架构的数据挖掘原型系统的设计与实现[J]. 微电子学与计算机，2008，25(12)：131-133.

[13] 康文杰，王勇，俸皓. 云平台中 MySQL 数据库高可用性的设计与实现[J]. 计算机工程与设计，2018，39(1)：296-301.