编号

**南京航空航天大学**

**毕业设计**

|  |  |
| --- | --- |
| 题 目 | 无线热点扫描器的设计与实现 |

|  |  |
| --- | --- |
| 学生姓名 | 肖端桂 |
| 学 号 | 161220329 |
| 学 院 | 计算机科学与技术学院 |
| 专 业 | 信息安全 |
| 班 级 | 1612203 |
| 指导教师 | 陈兵 教授 |

二〇一六年六月

**本科毕业设计（论文）诚信承诺书**

本人郑重声明：所呈交的毕业设计（论文）（题目：无线热点扫描器的设计与实现）是本人在导师的指导下独立进行研究所取得的成果。尽本人所知，除了毕业设计（论文）中特别加以标注引用的内容外，本毕业设计（论文）不包含任何其他个人或集体已经发表或撰写的成果作品。

作者签名： 肖端桂 2016年 6月1 日

（学号）：161220329

无线热点扫描器的设计与实现

摘 要

无线网络因为它的成本低廉、方便快捷、灵活运用等优势越来越得到有效的开发和利用。尤其在当环境复杂、地理布线困难的地方，无线网络的优势显得更为明显,无线网络越来越受到用户的青睐。无线网络目前已经运用到各行各业，企业生产、政府办公、家庭生活、个人学习等。但目前无线网络也存在不足，无线网络在使用过程中存在着除有线网已知的安全威胁外，还存在众多安全问题，而扫描发现无线热点作为后续查找安全问题的第一步尤其显得重要。本文首先简要描述了无线网络的发展情况，研究对比无线网与有线网的优劣；其次，在此基础上设计并实现了一款无线热点扫描器，扫描区域内无线热点信号，并显示无线热点信号强度的变化情况；最后，实验结果表明，使用本文设计并实现的无线热点扫描器能够正确扫描到无线热点，并显示无线信号强度变化情况。

关键词**：无线局域网、无线热点、无线热点扫描器、信号**

Design and implementation of wireless hot spot scanner

Abstract

Because of its low cost, convenient and flexible use of the advantages of the wireless network, it is more and more effective to be developed and utilized . Especially when the environment is complex and the geographical wiring is difficult, the advantage of the wireless network is more obvious, so it is more and more popular. Wireless network has been applied to all works of life, business production, government office, family life, personal learning, etc.. But the wireless network is also insufficient, in addition to the wired network known security threats, there are still many security problems in the process of and scanning found wireless hotspot as a follow-up to find security problems the first step is especially important. This paper begins with a brief description of the development of the wireless network, the pros and cons of the comparative study of wireless network and wired network; secondly, on the basis of this is designed and implemented a wireless hotspot scanner, scan area wireless hotspot signal and show hot wireless signal intensity change situation; finally, the final results of the experiments show that, used in this paper is the design and implementation of a wireless hotspot scanner to detect wireless signal can reach the expected goal.

Key Words**：**WLAN, Wireless hotspot, Wireless hots pot scanner, signal

目录

[摘 要 i](#_Toc453352266)

[Abstract ii](#_Toc453352267)

[第一章 引 言 - 1 -](#_Toc453352268)

[第二章 无线热点扫描器概述 - 4 -](#_Toc453352269)

[2.1无线热点扫描器简介 - 4 -](#_Toc453352270)

[2.2无线热点扫描器的发展方向 - 4 -](#_Toc453352271)

[2.3无线热点扫描器的应用领域 - 4 -](#_Toc453352272)

[2.4几种常用的无线热点扫描器 - 5 -](#_Toc453352273)

[2.5开发环境 - 6 -](#_Toc453352274)

[第三章 无线热点扫描器软件设计与实现 - 7 -](#_Toc453352275)

[3.1软件功能需求分析 - 7 -](#_Toc453352276)

[3.2无线热点扫描器的软件结构 - 9 -](#_Toc453352277)

[3.3 各模块流程图及功能介绍 - 12 -](#_Toc453352278)

[第四章 测试结果 - 23 -](#_Toc453352279)

[4.1 热点清单信息测试结果 - 23 -](#_Toc453352280)

[4.2 热点场强变化测试结果 - 23 -](#_Toc453352281)

[4.3 信道使用信息测试结果 - 24 -](#_Toc453352282)

[第五章 总结和展望 - 25 -](#_Toc453352283)

[5.1本文工作 - 25 -](#_Toc453352284)

[5.2下一步工作 - 25 -](#_Toc453352285)

[参考文献 - 26 -](#_Toc453352286)

# 引 言

随着研究人员对无线局域网的研究的深入，已经发现了很多无线网的使用技巧，在网络使用领域中无线网存在的优势。但是，也发现了很多无线网自身存在的不足。本章将浅显的描述无线局域网对比有线网的优势，同时分析它存在的主要安全威胁，及无线局域网的研究现状。

**1.1研究的背景及意义**

随着计算机硬件设备技术提高，产品价格下降，计算机领域的不断扩展，以及现代电子信息技术的迅猛发展，无线网络因为它的成本低廉、方便快捷、灵活运用等优势越来越得到有效的开发和利用。尤其在当地环境复杂、地理布线困难的地方，无线网络的优势显得更为明显。无线局域网通过电磁波在空气中发送和传播信息，具有移动性、兼容强、扩充性高和功率低、成本低廉、效率高效等诸多优点。

无线通信和计算机的迅速发展，无线网络充分结合他们的优势，渐渐的开始应用于企业办公、政府各个部门、个人家庭生活等领域。无线局域网随着技术的成熟，设备成本不断下降，部署难度越来越低，在企事业单位、政府部门及个人家庭得到普及，给人们的工作、学习和生活带来便利，提高了人们的工作效率，改善了人们的生活质量。随着科学技术的高速发展和无线网络的广泛运用，我们必须不断发挥其优势，以给我们的生活、学习、工作带来便利。同时需要不断研究如何改进无线局域网的结构，探索无线局域网的安全设置以便让它更加安全可靠，充分发挥无线网络在现代经济发展的作用。

但由于无线局域网的传输介质是无线电波，这决定了它不但具有有线网络的安全威胁，同时还有其他的安全威胁。在访问控制、认证等安全技术方面与传统的以电缆为传输介质的局域网有较大区别，不仅无线信道容易被窃听和干扰，引发信息泄露、无线钓鱼等安全问题，还容易遭受冒充、篡改、欺骗等形式的攻击。其中非法“无线接入点”（Access Point，AP）的问题尤其突出。非法AP的问题是随着无线局域网的出现而显现的，它影响着国家的安全、内网的安全、个人的隐私、社会稳定和经济安全。非法AP对社会网络的威胁主要表现在以下三个方面：（1）不法用户实验测试mdk2等软件工具。用无线网卡建立虚假的AP信号，占用正常运行的信道，干扰无线信道的正常；（2）截获无线网络通信数据，入侵个人计算机，泄露个人信息；（3）在企事业单位内部网络上随意搭建非法的AP，严重威胁到内网安全，增加内网被入侵的风险。因此，影响无线局域网安全的非法AP问题已经成为的主要安全问题之一，但同时又因为它能够轻松搭建，搭建手段不断改变，造成了解决它的安全威胁变得困难，解决方法需要经常更新。因此，无线热点扫描器可以帮助用户发现存在的AP，并为下一步操作提供了基础。

**1.2研究现状**

2010年，陈潮、勒慧云[1]关于网络中非法AP的定位问题的研究详细阐述非法AP的定义，分析非法AP的危害并给出清除非法AP的方法。他们指出清除非法AP关键是检测定位AP的位置，在研究和分析前人有关AP定位技术的基础上，总结出三种定位非法AP的方法，并对三种方法优缺点进行了详细的分析和比较。

2014年，赵方、罗海勇、耿皓、孙启金[3]提出一种基于RSSI梯度的AP定位算法，并与其他几种定位算法进行了详细的分析、对比，同时说明它的应用对象和前景。

同年，江苏省宿迁广播电视大学的于万清[4]发表了自己对于无线网络的研究的成果，对无线网络的结构，优缺点，安全设置进行了分析，同时给出简单的解决方案。

2007年，文献[12]在802.11无线局域网的安全基础上，深入研究了它面临的安全威胁和仍未解决的安全漏洞，以及可能存在未知的安全威胁，提出了自己的增强方案，同时对目前认为比较先进的网络安全协议进行深入分析，并给出自己的意见和建议。

**1.3 本文研究内容**

上述研究并没有说明如何判定一个AP是否合法，同时他们给出解决非法AP的定位方法过于复杂，技术要求比较高，这在一定程度上很难普及。因此，在上述的研究基础上，本文将进行以下研究：

（1）研究现有扫描器的功能。

（2）参考**wireless MON**软件进行无线热点扫描器的设计，包括热点清单功能、热点场强变化功能、无线访问探测功能，并在Windows平台下进行具体实现。

（3）在windows平台下实现无线热点的扫描，能够正确显示当前能够查询到的无线热点，并能够实时显示选定无线热点的场强变化情况。

**1.4 论文章节安排**

本文共分为五章，每章内容如下：

第一章，绪论。首先介绍了课题背景、目的及主要任务。阐述无线网的发展背景、发展现状。

第二章，无线热点扫描器概述。对常用的无线热点扫描器进行介绍。

第三章，无线热点扫描器软件设计。Windows平台下无线热点扫描器的设计和实现方面，提出需要解决的主要技术难点，给出解决方案，并详细描述主要模块的设计与实现。

第四章，测试结果。列出了在搭建的验证平台上对无线热点扫描器验证实验，并对实验结果进行了分析。

第五章是对本文所做工作的总结。

最后是参考文献和致谢。

# 无线热点扫描器概述

## 2.1无线热点扫描器简介

无线网络是一种采用电磁波来实现数据传输的网络。它能够让用户自主建立随意距离的无线连接的语音通信和数据网络，随着无线网络的发展，无线网络应用也越来越广泛；同时，无线网络安全问题也日益突出，而对于无线热点的信息分析也变得尤为重要。至此，无线热点扫描器开始得到广泛应用，它能扫描并获得无线信号的大量信息，并能试图找出无线信号可能存在的漏洞，以及对用户设置的陷阱。

无线热点扫描器能扫描区域中的无线网络，并显示大量信息，其中包括：机主的网络名称、机主的MAC地址、所用的PHY类型、RSSI、搜索到的信号质量、工作频率、通道数量、最大传输速度、适配器厂商名称、路由器型号和名称等。

## 2.2无线热点扫描器的发展方向

无线热点扫描器的发展趋势将向智能化、高效化、便携化、功能多样化、结构简单化等几个方面发展。

1. 智能化：主要指在扫描时能根据需求自主选择需要扫描的目标，并详细显示重要的信息。
2. 高效化：扫描可以快速的找到用户需要的目标。节约时间成本、减少资源消耗、实现高效快捷。
3. 便携化：无线扫描器的发展应更上时代的潮流，更够随时随地的使用。
4. 功能多样化：随着无线网络的全面发展与功能的多样化，无线热点扫描器也应该相应的更上发展的步伐。
5. 结构简单化：无线热点扫描器发展方向应是结构简单，同时能实现主要的功能。
6. 低价格化：在这个市场竞争激烈的环境下，同样的功能，更低廉的价格的产品将会更好的获得消费者认可。

## 2.3无线热点扫描器的应用领域

无线通信技术和计算机技术的迅速发展，无线网络技术充分结合两者的优势，开始应用于企业生产、政府办公、个人家庭生活等领域。可分为下面几种：

1. 在计算机网络传输领域和电子通信领域中的应用；
2. 企业办公领域的应用；
3. 政府工作部门的应用；
4. 家庭生活领域的应用；
5. 个人领域的应用。

## 2.4几种常用的无线热点扫描器

（1）Kismet

Kismet是一款工作在802.11协议第二层的无线网络检测、嗅探、干扰工具。可以工作在支持raw监控模式的所有无线网卡上。可以用Kismet对802.11b、802.11a和802.11g在内的协议包进行网络探测。

Kismet是一个在Linux上运行的无线网络扫描软件。这是一个相当方便的工具，通过测量周围的无线信号来找到目标WLAN。除扫描无线信号之外，Kismet还可以抓获网络中的数据包到存放到一个指定的文件中以方便今后分析使用。

当Kismet开始运行时，它会显示这个区域内它找到的所有的无线局域网。甚至当目标计算机已关闭时，Kismet也正可从目标AP中检测到数据包，这是因为目标AP在不停地向外界发出信号，它能够提醒拥有无线网卡的PC有一个AP在它们范围内。

（2）Wireless Mon

Wireless Mon是一款允许使用者监控无线适配器和聚集的状态，显示周边无线AP或BS实时信息的软件，能列出PC与BS间的信号强度，实时的监测无线热点的传输速度，便于让用户了解热点的传输速度和稳定性。

（3）Vistumbler

Vistumbler算是一款较新的开源扫描程序，Vistumbler能搜寻到附近所有的无线网络，并且在上面附加信息，如：活跃、MAC地址、SSID、信号、频道、认证、加密和网络类型。它可显示基本的AP信息，包括精确的认证和加密方式，甚至可显示SSID和RSSI。Vistumbler还支持GPS设备，与当地不同的Wi-Fi网络连接，输出其他格式的数据。

（4）Wifi Analyzer

Wifi Analyzer是一款免费的Android应用工具，可以在Android平台的移动终端上寻找AP。它能将2.4GHz信道的AP所有详细信息都一一列出，也支持5GHz信道的其他设备。用户还可以将AP详细信息以XML格式输出到文本并通过电子邮件或者其他应用程序、屏幕截取等形式共享。它能根据信号的信道强度，使用频率、信号的来源地远近以图形的方式表达出来。

## 2.5开发环境

本项目的开发环境是在Window8平台下，采用Blend工具来进行软件界面的设计，通过Visual Studio 2015来编写逻辑功能代码。

Blend for Visual Studio 2015是微软提供的一款为HTML和XAML应用程序设计用户界面的工具。开发人员可以用VS开发应用程序，这些程序可以用Blend for Visual Studio 2015打开，并且，在blend内有设计人员添加动画或者美工。

Blend是一款功能齐全的专业设计工具，可制作出精美复杂的应用程序用户界面。新版Blend拥有圆滑的黑色界面，这也与VS 2015的整体风格十分搭配。除此之外，Blend For Visual Studio 2015还带来了XAML智能感知、基础调试能力、团队资源浏览器以及可管理NuGet包，更好的可用性等诸多改进。

# 无线热点扫描器软件设计与实现

## 3.1软件功能需求分析

无线热点扫描器系统包括热点清单功能、热点场强变化功能和无线访问探测功能，同时能对单一的信号进行追踪，并在使用者需要的时候能够对某个指定的信号进行访问探测。

1. **热点清单**

热点清单能够详细的显示热点的主机名、MAC地址、SSID、信道、网路类型等信息。具体说明如下：

1. 主机名

主机名，就是建立无线热点的计算机或者其他能够建立无线热点的设备的名字。

1. MAC地址

MAC地址，媒体访问控制，或称为物理地址、硬件地址。在OSI模型中，第三层网络层负责IP地址，第二层数据链路层则负责MAC地址。因此一个主机会有一个MAC地址，而每个网络位置有一个专属于的IP地址。这个功能用来定义网络设备的位置。

1. SSID

SSID，意思是：服务集标识。SSID技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入本网络。

1. 信道

通信的通道，是信号传输的媒介。

1. 信号强度

能够直观的表达每个信号的强度信息。

1. 加密类型

它能显示无线热点是否加密，用的哪种加密方式。

1. 网络类型

从不同的角度对网络有不同的分类方法，每种网络名称都有特殊的含意。几种名称的组合或名称加参数更可以看出网络的特征。

1. 速度

数据传输能达到的最大速度。

1. 首次搜索时间

无线扫描器首次搜索到热点的时间。

1. 最后搜索时间

无线扫描器当前或最后搜索到热点的时间。

1. 位置

热点的大概位置，通过GPS定位实现。

1. **热点强度变化**

无线扫描器软件界面能显示热点强度随时间、距离的变化曲线。对单个热点的变化曲线进行跟踪显示，这个属性能体现热点是否稳定可靠。一个稳定的热点信号，强度变化曲线的上下波动不会很大，即使它的最大传输速度不高。反之，一个波动频率高，起伏幅度大的信号，即使最大传输速度很大，也不会是一个理想的选择。

1. **热点访问探测**

在需要的时候，能够对某个指定的热点进行访问。一些热点在建立时没有设置加密，用户能通过这些热点实现Internet访问。但是大多数热点在建立时会进行加密，用户在不知道密码的情况下想通过这些热点访问Internet就变得不可能。这个功能的作用是尝试找出并分析热点的弱点，然后分析可能的击破方式，再对密码进行相应的攻击，如暴力穷举、密码心理学、绕过破解、网络钓鱼、利用系统漏洞等方式，最后进行Internet访问。

（1）暴力穷举

密码破解技术中最基本的就是暴力破解，也叫密码穷举。如果黑客事先知道了账户号码，如邮件帐号、QQ用户帐号、网上银行账号等，而用户的密码又设置的十分简单，比如用简单的数字组合，黑客使用暴力破解工具很快就可以破解出密码来。因此用户要尽量将密码设置的复杂一些。

（2）密码心理学

不需要工具而破解密码的骗局称为社交工程攻击。很多著名的黑客破解密码并非用的什么尖端的技术，而只是用到了密码心理学，从用户的心理入手，从细微入手分析用户的信息，分析用户的心理，从而更快的破解出密码。其实，获得信息还有很多途径的，密码心理学如果掌握的好，可以非常快速破解获得用户信息。

（3）绕过破解

绕过式密码破解原理非常简单，其实就是绕过密码的认证机制，绕过的方法有很多种，有些取决于系统本身，有些和用户的习惯有关，例如用户如果使用了多个系统，黑客可以通过先破解较为简单的系统的用户密码，然后用已经破解的密码推算出其他系统的用户密码，而很多用户对于所有系统都使用相同的密码。

（4）网络钓鱼

“网络钓鱼”攻击利用欺骗性的电子邮件和伪造的网站登陆站点来进行诈骗活动，受骗者往往会泄露自己的敏感信息（如用户名、口令、帐号、PIN码或信用卡详细信息），网络钓鱼主要通过发送电子邮件引诱用户登录假冒的网上银行、网上证券网站，骗取用户帐号密码实施盗窃。

（5）系统漏洞

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。许多系统都有这样那样的安全漏洞，其中某些是操作系统或应用软件本身具有的，这些漏洞在补丁未被开发出来之前一般很难防御黑客的破坏，还有一些漏洞是由于系统管理员配置错误引起的。这都会给黑客带来可乘之机，应及时加以修正。利用系统漏洞的攻击手段所以能够存在，根本原因是系统中有安全漏洞的存在以及人类在使用中所犯的错误所致。因为很难保证系统的实现和使用中不发生错误，所以从理论上说无法从根本上解决系统攻击问题。

## 3.2无线热点扫描器的软件结构

无线扫描器整体结构、扫描模块功能设计图、热点清单模块功能设计图、WIFI管理模块功能设计和GPS模块功能设计图。如图3.1所示。



图3.1（1） 无线扫描器软件结构图



图3.1（2） 扫描模块功能设计图

图3.1（3） 热点清单模块功能设计图



图3.1（4） WIFI管理模块功能设计图



图3.1（5） GPS模块功能设计图

软件基于无线网络管理来实现。通过调用网卡接口，根据接口收集到的热点信息，来实现一系列操作和功能。软件同时能进行主动扫描与被动扫描。

被动扫描是通过无线网卡监听由接点广播的Beacon（信标）帧，然后对数据进行抓包分析，从中取出SSID等信息。

主动扫描是用无线网卡主动广播出Probe Request（探测请求）帧，并且等待接入点回复的Probe Response（探测回复）帧，分析返回帧，从中取出SSID等信息。

## 3.3 各模块流程图及功能介绍

**3.3.1 扫描模块**

扫描模块是软件的最基本功能模块，它能主动从无线网卡处获得热点的详细信息，用申请的存储空间对得到数据进行存储，并且能对信息进行初步分类，然后把数据发送给WIFI管理模块。扫描模块流程图如下：

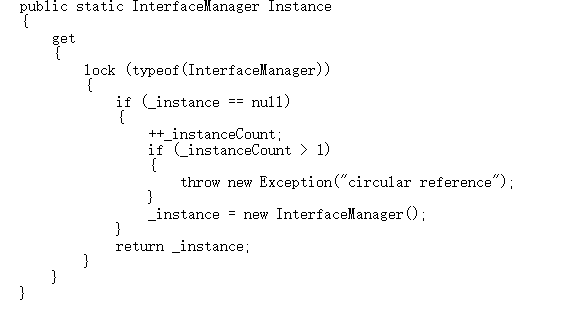


图3.2 扫描模块流程图

扫描模块的细化功能模块包括网络接口管理模块、网络数据缓存模块、网络扫描器模块、数据处理模块、扫描控制器模块、扫描界面模块、扫描界面管理模块。

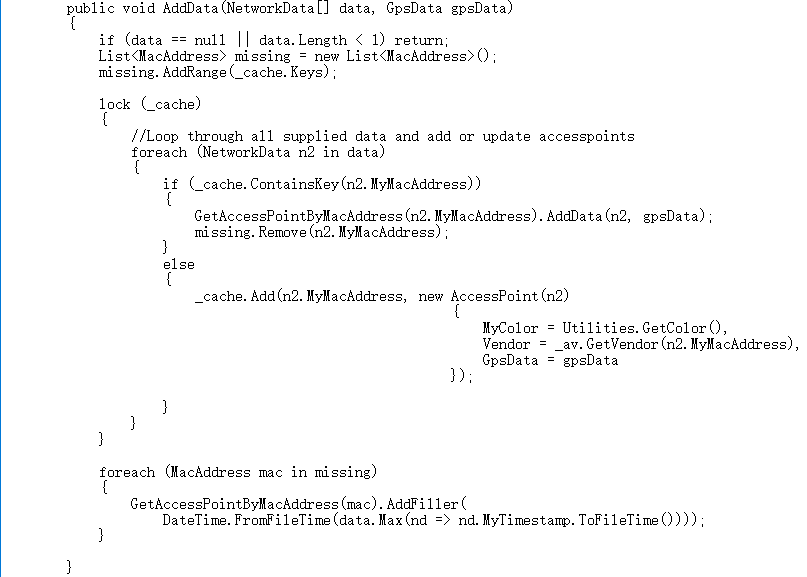
1. 网络接口管理模块

在扫描器工作时通过网络扫描模块调用网卡接口，得到无线信号，分析信号的信息，然后把信息发给数据完整度模块分析，并传输到扫描器界面模块，在扫描器界面模块对数据信息进行处理并在扫描器界面显示出来。核心代码如下：



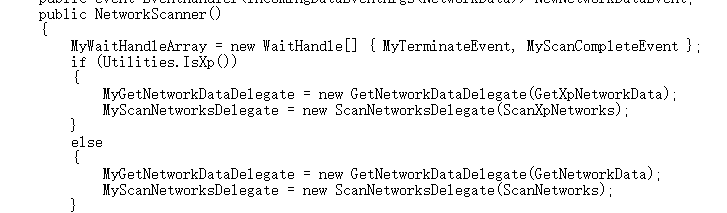
1. 网络数据缓存模块

通过向内存申请内存空间，分类存储扫描到的数据信息。比如用户之前获得的各种信息，并且在需要的时候能够快速的读取到想要的信息。核心代码如下：



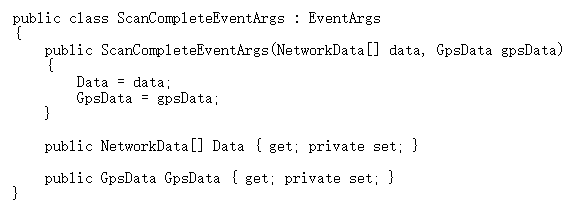
1. 网络扫描器模块

在扫描器工作时调用网卡接口，获得常规热点信息，然后传输给网络接口管理模块。每一个无线热点扫描器都会有网络扫描器这个细化模块，它能够扫描区域内所有的无线信号，并反馈到数据管理模块上，让用户知道区域内有什么信号，然后进行下一步操作。构造代码如下：



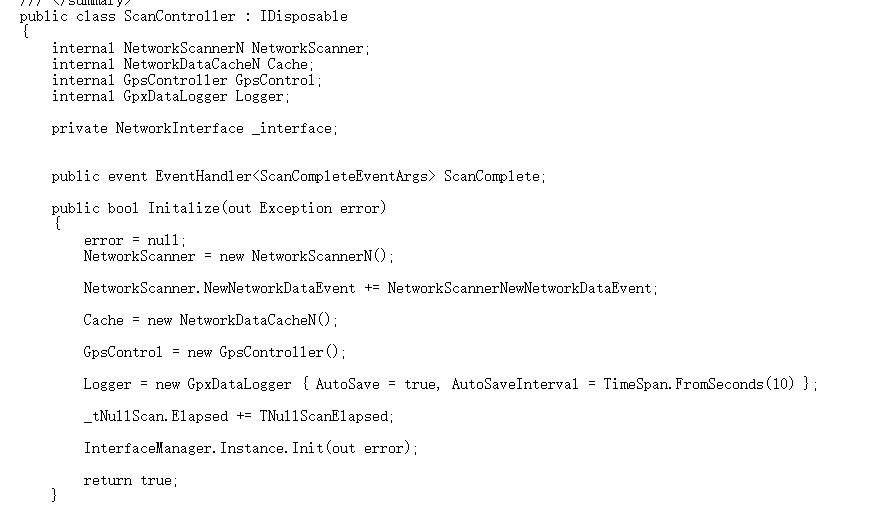
1. 数据完整度信息模块

这个模块能够完整的收集到关于一个信号的目前已知的所有信息。这个模块能够把收集的信息准确完整地分类送给不同需求的模块；同时由于各个模块只需要自己需求的信息，如果没有这个模块对数据进行分类的话，所有的数据都对各个模块走一遍，这样会产生很多的垃圾数据，这些垃圾数据同样会占用系统或者软件申请的内存空间，内存就会因为越来越多的数据堆积起来。然后软件就很容易因为数据堆积而出现问题，从而出现软件崩溃的危险，所以这个模块在对数据处理的时候非常有用，同样在对数据完整性也很重要。核心代码如下：

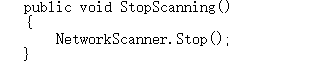
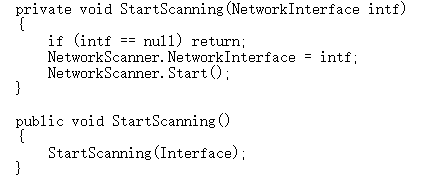


1. 扫描器管理模块

用于用户对扫描器进行各种需要施行的操作。没有操作功能的扫描器只能简单的扫描信号、给出数据，而无法进行深入操作的软件是无法满足用户需求的，同时它也达不到用户的体验要求。构造代码如下：

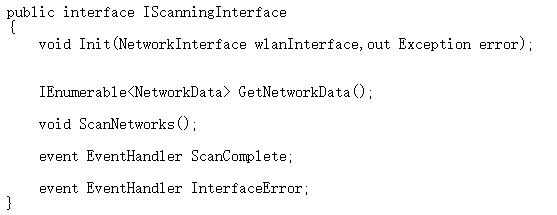


启动扫描器，停止扫描器核心代码如下：



1. 扫描器界面

用于显示热点清单，热点场强变化等。构造代码如下：



**3.3.2 热点清单模块**

热点清单模块流程图如下：

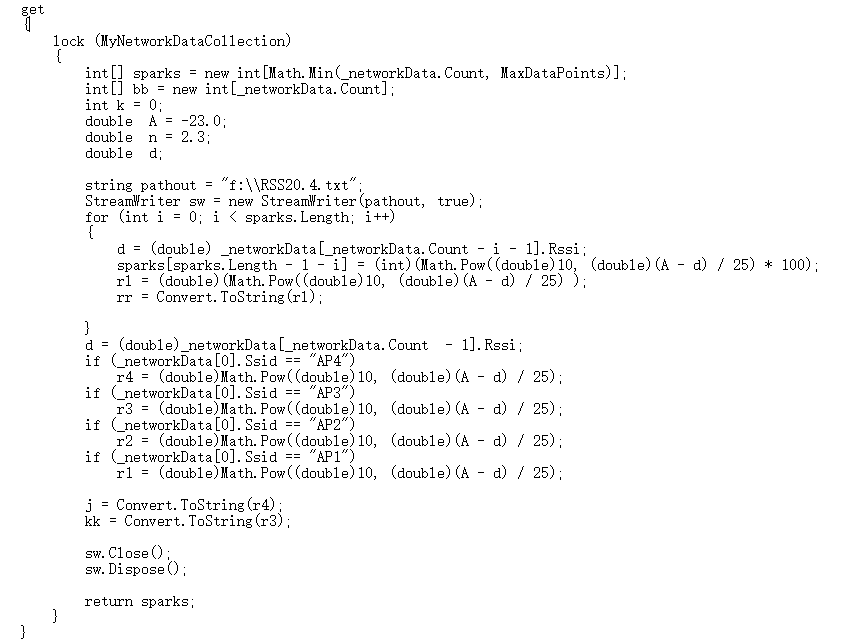


图3.3 热点清单模块流程图

这个模块是具体的实现热点清单功能的模块，它能详细的在扫描器界面把热点的所有清单显示出来，如MAC地址、SSID、信道、信号强度、加密类型、网络类型、最大速度、首次搜索时间、最后搜索时间、AP位置等等。它能对热点的数据进行分析、处理，然后输出到扫描器界面上。

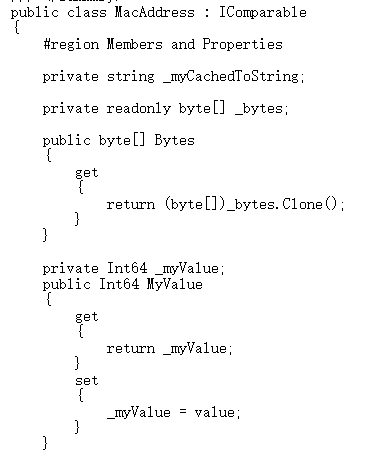
1）热点信息

对热点数据信息进行分析，然后建立清单。核心代码如下：



2）MAC地址信息

MAC地址是固定的，它由网卡控制着。MAC地址又称物理地址、硬件地址或访问地址。在OSI模型中，第二层数据链路层辅助MAC地址，所以每个网卡会有一个MAC地址。它用来表示网络上每一个站点的标识符，用十六进制数来表示，一共有六个字节，共四十八位。前面三个字节由IEEE的RA给商家分配。后面三个字节由厂家自己指派给适配器接口的生产商来决定。MAC地址对应于OSI参考模型的第二层数据链路层，交换机工作在数据链路层维护计算机MAC地址和数据库安全，交换机能够按照收到的数据帧中的目标MAC地址来转发数据帧。构造代码如下：

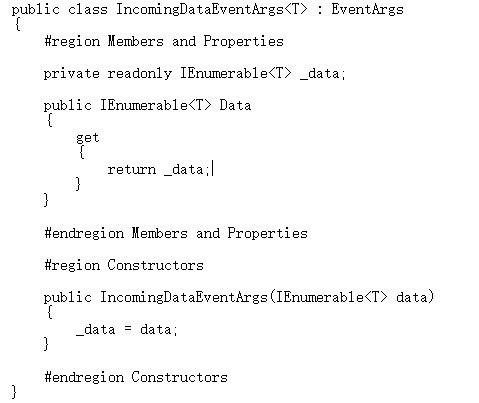


3）信号占用通道

这个模块能够检测信号当前信道使用情况，是2.4GHz还是5GHz等。如果这种信道类的热点数量比较少，那么这个热点的信号受到干扰的可能性就会降低，因而这个信号会比较稳定。

4）输入数据的参数

在清单中输入热点的数据信息，对数据进行实时更新，并显示时间变化及场强变化。构造代码如下：



5）一些其他信息

在其他小模块当中，增加一个函数调用，来实现他的功能。这些细化的信息对于信号的信息处理起到辅助作用，能够帮助用户增进对信号的理解。如网络数据、滤波。

**3.3.3 WIFI管理模块**

WIFI管理模块流程图如下：

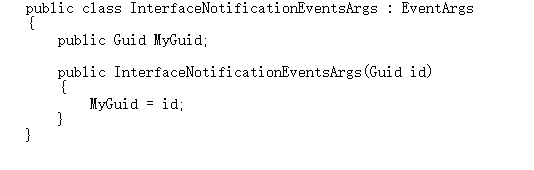


图3.4 WIFI管理模块流程图

这个模块能对收集的信号进行管理。比如：WLAN，WLAN清单、WLAN的网络接口、装配信息、IE分析器及接口的参数通知等。这个模块是对热点清单模块的一个补充，它能够完善热点清单模块缺少的功能，同时增加一些附加功能，方便用户的使用。它在一定程度上能够完善软件的完整度，降低软件出错率、减少软件运行错误等。

1）热点网络接口

用来分析热点的网络接口信息。构造代码如下：



**3.3.4 GPS管理模块**

GPS管理模块通过分析位置数据是否符合GPS NMEA协议来实现对AP的定位，流程图如下：



图3.5 GPS管理模块

该模块能够调用设备的GPS信息，通过GPS管理器加以管理，然后对AP进行对位。这个模块的作用是在结合设备的定位系统来实现对热点信号进行定位。目前，非法AP已经越来越使用频繁，而它的危害也在慢慢的体现出来，它在一定程度上增加网络管理员对于网络管理的难度，增加管理员查询网络情况的难度。GPS在当下的各种移动的或非移动的设备中已经运用的越来越广泛。

**3.3.5辅助功能模块**

辅助模块实现对软件功能的完善。辅助功能模块是由很多小的数据结构整合而成，实现对各个大模块功能的辅助。如2.4GHz/5.0GHz频段、UI设计、软件扩展功能、软件联网功能、适配器信息等。

# 测试结果

测试结果与预期一样，实验达到了预期的目的。能够扫描到区域内的设备能够接收到的所有的无线热点信号。

## 4.1 热点清单信息测试结果

信号的清单能清晰明了显示出来。如图4.1。



图4.1 热点扫描清单

图4.1显示了热点清单信息。从图上可以看出，扫描器实现了热点清单功能的要求。扫描器显示界面详细罗列出热点的所有基本信息。

## 4.2 热点场强变化测试结果

如图4.2所示，扫描器能显示热点信号强度随时间变化的曲线。

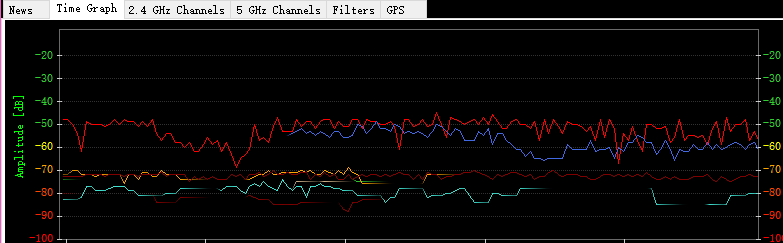


图4.2 热点信号强度随时间变化曲线图

## 4.3 信道使用信息测试结果

如图4.3（1）所示，扫描器能显示2.4GHz频段上信道的使用信息，为用户选择AP的时候能够提供参考。

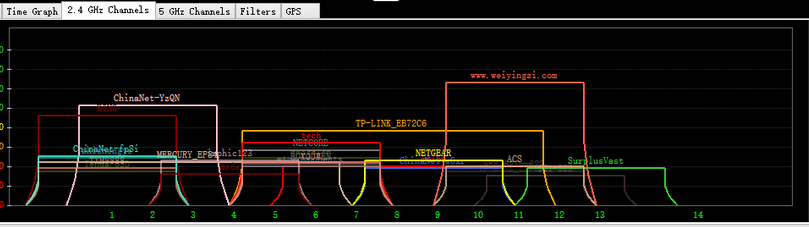


图4.3（1） 热点2.4GHz信道使用情况

如图4.3（2）所示，扫描器能显示5.0GHz频段上信号的使用信息。鉴于目前大多数信号使用2.4GHz频段，5.0GHz频段上此次测试没有信号使用。



图4.3（2）热点5.0GHz频段使用情况

# 总结和展望

本课题的目的是开发在Windows平台下的无线热点扫描器，通过对比参照以往有的无线热点扫描软件，设计并实现包括热点清单功能、热点场强变化功能、无线访问探测功能。本课题的研究达到预期的目的。

## 5.1本文工作

本文以介绍分析无线局域网的优势和劣势开始，进一步探讨无线局域网的改进机制和安全威胁的解决办法，包括无线热点的便利性、安全性、使用漏洞等问题，进而提及无线热点扫描器的设计和实现。

首先讨论了该软件使用重要技术，然后按照软件工程的思路从需求分析，设计思想，数据结构设计，功能设计，系统实现来介绍了整个软件从设计到实现的完整过程。对于系统的各个功能模块，都给出了详细的算法和实现流程。重点介绍了各个模块的功能设计、工作流程、实现算法和作用。最后用实验验证软件已经实现的各个功能并且达到预期的目的。

## 5.2下一步工作

由于对访问探测这一块知识的匮乏，使得软件在访问探测无法实现。同时由于实验设备的GPS无法正常工作，使得软件的GPS功能无法测试。

下一步工作将会是完善该无线热点扫描器的功能，并继续加以改进，使之实现访问探测功能，进行无线热点漏洞扫描，同时使用能支持GPS的实验设备，测试并完善软件的GPS功能。

# 参考文献

[1] 陈潮，靳慧云. 无线局域网中非法AP的定位问题研究.[J].信息网络安全，2010（10）：72-73.

[2] 夏英，王磊，刘兆宏. 基于无线局域网接收信号强度分析的混合室内定位方法[J].重庆邮电大学学报：自然科学版，2012,24（2）.

[3] 赵方，罗海勇，耿皓，孙启金.基于RSSI梯度的AP定位算法[J].中国通信，2014（2）.

[4] 于万清.无线局域网技术浅析[J].读与写：教育教学刊，2014,11（5）：85-85.

[5] 郭峰，曾兴雯，刘乃安，马义广．无线局域网[M]．北京：电子工业出版社，1996，3-7l.

[6] 尹桂杰，卢建川，邓洁．无线局域网关键技术及发展综述[J]．电讯技术，2002，4：36-40.

[7] 姜驶，杨莘元．无线局域网的发展与应用[J]．信息技术，2002，4：63-67.

[8] Jim Geier著．无线局域网(王群，礼馥娟，叶清扬译)[M]．北京：人民邮电出版社，200l，15．47.

[9] 范平志，赵其刚．无线局域网及其关键技术[J]．计算机应用，1998，9：21-25.

[10] 杨嵩山，秦春燕．无线局域网技术及应用[J]．邮电设计技术，2002，4：14-16.

[11] 凌畅宇．部署安全的无线局域网[D]．西安：西安电子科技大学，2003.

[12] 王文胜.无线局域网安全技术研究[D].成都：电子科技大学，2007.

[13] 聂武超，张彦兴．802．1x认证技术分析[R]．华为技术报，2002，2：45-51.

[14] 王蔚．宽带无线Ⅲ系统中AP软件的设计与实现[D]．西安：西安电子科技大学，2002.

[15] 唐瑀. 基于无线局域网的室内定位技术[j].南京邮电大学，2015.

[16] 段希文.基于无线局域网的室内定位技术的研究[J].山东科技大学，2014.

[17] 李翔.基于无线局域网的位置指纹室内定位技术研究[J].湖南大学，2015.

[18] 严蔚敏，吴伟民.数据结构（C语言版）[M].北京：清华大学出版社，2007.

[19] L Yunxiao，Q Sujuan. An Improved Indoor Positioning Method Based on Received Signal Strengths[C]. International Conference on Intelligent Transportation，2015：90-93.

[20] J Zhuang，J Zhang，D Zhou，H Pang，W Huang.An Improved Wi-Fi Indoor Positioning Method via Signal Strength Order Invariance[C]. IEEE International Conference on Computer & Information Technology，2014:3-6.

[21] MS Rahman Sakib，MA Quyum，K Andersson，K Synnes，U Korner. Improving Wi-Fi based indoor positioning using Particle Filter based on signal strength[C]. IEEE Ninth International Conference on Intelligent Sensors，2014:1-6.

**致 谢**

这次毕业设计能够圆满完成归功于指导导师、同学和亲人朋友的大力帮助。在此，我要感谢：

第一：指导老师陈兵教授的指导和帮助，他实时关注我的研究进度，并对我研究存在的困难和不足加以指导，提出改进和解决办法，使我的研究能够顺利进行，进度能够按时完成。

第二：宿舍和班级同学在我研究遇到瓶颈时，给我分享了他们各种的研究经验，同时给出意见和建议，这对我的研究非常有帮助。同时，我在研究期间存在的小难题都在他们那儿得到解决。这使我的研究进度能够顺利进行。

第三：感谢亲人朋友在我研究期间给予我的精神上和物质上的帮助和鼓励，让我的研究不会因为外界干扰或者物质原因而中断、落下进度甚至无法完成。

在此，我衷心的感谢那些帮助我的人，谢谢你们。