新南威尔士大学电气工程学院电讯专业

**用蓝牙访问控制**

**致谢**

我们论文组的每一个成员要项在整个项目的持续时间内向我们提供热心帮助和支持的几个人表示感谢。首先，我们要感谢我们的论文导师，蒂姆·摩尔博士，他不仅认真回答我们组在论文中所面临的问题，而且也尽了最大努力为我们提供所需的一切资源和后勤保障，同时，我们还要感谢约瑟夫·杨，蓝牙实验室的实验室技术员主管，为我们提供了我们所需要的必需后勤保障，其中包括提供给我们在开发软件合用的电脑，并且还计算机坏掉时提供维修，还有很多帮助。

**摘要**

本文提出的项目是用蓝牙访问控制的方法。目前访问控制方法需要物理上连接到一个装置，例如一个划卡。蓝牙是一种无线技术，它可以用来代替这样的应用，并且提供了便利的无线接入控制。本文的目的是证明这样的概念是可行的，通过实施这样的一个应用程序。本文所开发的应用程序需要实现切断铃声即让手机静音。这个设计方针是通过蓝牙创建一个静音的接入点。接入点就会发出一个“信标”信号到手机，通过蓝牙，告诉它关闭其铃声。这个论文的另一个焦点是确保此过程的安全性。在本文的设计中，两个移动电话和接入点将会开展的认证过程。伴随此论文的成功，这样的概念可以扩展到其它形式的访问控制应用。

**1. 介绍**

**1.1 背景**

蓝牙标准和技术的建立之初是源于爱立信移动通讯进行了一项关于在其移动电话及其配件间找到一个低能耗并且低成本的无线接口的研究。研究表明，短距离无线链路解决方案是可行的。为了开发该技术，并获得广泛的市场支持，爱立信，加上英特尔，IBM，东芝和诺基亚移动电话在1998年形成了一个特殊的兴趣小组（SIG），该组形成是为了建立无线接口标准和控制它的软件，如要实现不同的设备之间的相互操作来自不同生产商。 [1]

**1.2动机**

本论文的动机是展示在访问控制应用中使用蓝牙技术。一个特定的应用是在进入报告厅时在支持蓝牙的手机上控制关闭手机铃声，应为作为能够响铃的移动电话是不能出现在这种场景的。

目前，大部分的访问控制解决方案是通过使用常规的实施的技术，如条形码刷卡，并获得pin码号码。使用较新的支持蓝牙的移动设备，能够使用蓝牙技术开发的应用程序替代旧访问控制技术，允许以无线方式输送访问控制命令。

因为蓝牙是一种相对较新的技术，还没有很多的蓝牙应用被创建出来。。因此，写一个蓝牙软件系统将是我们的最后一年的论文一个具有挑战性的，但有趣的经历。

**2.蓝牙功能**

**2.1 优势**

下表比较蓝牙无线电无线LAN和红外线。这些三种技术在许多当今的无线应用是最常用的。他们每个人都有自己的优点和缺点，这使得它们每个都适合于某些应用程序。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 蓝牙 | 无线LAN | 红外 |
| 范围 | 中等10m | 长100m | 短1m |
| 可见 | 不可见 | 不可见 | 可见 |
| 带宽 | 1 Mbps的共享 | 11Mbps的共享 | 115kbps&4Mbps的专用 |
| 干扰 | 其他射频设备 | 其他射频设备 | 无 |
| 安全性 | 安全性小与红外 | 不安全的，除非 | 非常安全的，由于 |
| 使用linklayer | 保护。例如WEP | 短距离和可见要求 |
| 认证。 | ＆WPA加密 |  |
| 仍然需要应用层 |  |  |
| 安全性。 |  |  |
|  |  |  |
| 耗电量 | 高，需要保持连接 | 非常高，需要保持连接 | 低，不需要保持连接，像无线电台 |
| 组件成本 | 约20美元，有望下降到5美元 | 约25美元 | 低于2美元 |

**表 1**:通过蓝牙，无限LAN，红外三种技术的比较，蓝牙的主要特点，使得他在如下应用中适用：

* 最小的硬件尺寸。
* 低价蓝牙组件。
* 低功耗蓝牙连接。
* 固有的安全特性（节所述）。
* 中程。

低成本小尺寸的蓝牙无线电意味着它可以集成到许多便携式设备。这些例如移动电话，PDA等SIG中的公司生产的产品，为蓝牙器件及其应用创造了巨大的市场潜力。

低功率消耗在这个项目中特别重要，因为软件系统要求在所有的时间移动电话上的蓝牙无线电都被接通 。这有助于延长电池寿命，这是在移动电话中很重要的需求。

固有的安全特性和蓝牙的中程范围使得蓝牙是相对安全的，因为相对于其他无线电，如无线局域网。安全功能使得它很难监听数据传输。中程意味着黑客为了监听它的访问流量将必须靠近蓝牙无线电的物理范围内。所有这些都是重要的，因为该项目涉及访问控制，其中安全起着非常重要的作用。但是请注意，蓝牙安全对于这种应用是不够的，因为它从不因为其它蓝牙设备系统的“攻击”而停止系统。一个附加的应用层认证过程，将对这些恶意的蓝牙用户进行过滤，如第6.5.6所述。

蓝牙相对较低的数据传输效率在本项目中不是问题，因为项目中将只涉及到较少的数据

**2.2营销环节**

在过去的几十年中，消费产品，如个人电脑，笔记本电脑，个人数字助理，手机等已经更加受欢迎。这是基于这些设备的连续的成本的降低和尺寸的减少。设备之江的信息传输因为需要电缆而受到阻碍。蓝牙为省去电缆提过了一种解决方案 。它也提供了用于彼此之间的多点连接，例如建立多种蓝牙设备间的个人小型区域网络。

**2.3无线频谱**

蓝牙工作在2.4 GHz频谱是可以不经过许可的。这意味着该频谱是向公众开放，而不需要许可证，只要它们满足由FCC指定的要求。此外，蓝牙应用都是针对做了很多旅行的消费者。因此在蓝牙操作上的频谱必须是全球统一的。 2.4 GHz频谱是免费的，因此在世界上大多数国家符合这一标准

这个频谱的使用说明介绍了很多的蓝牙无线电传输的干扰源。干扰的一个来源是高功率的发射机，发送在2.4GHz频带的装置如微波炉的照明装置。干扰的另一来源是来自其他蓝牙用户的用户干扰。

抗干扰可通过干扰抑制或避免来获得。然而，这些技术将不会在本报告中进行讨论。

**2.4点对点无线连接**

蓝牙无线电系统从其他无线电系统中脱颖而出，是由于其自组织连接。大多数目前使用的无线电系统是基于蜂窝式无线电架构。移动网络是建立在有线骨干网的基础设施，以及由位于不同位置中的一个或多个基站来提供蜂窝覆盖。移动终端然后访问在网络中的这些覆盖区域。故有基站和这种系统的终端之间的明确分离。与此相反，在蓝牙系统中没有显着的基站或终端，也没有无线电单元之间的任何差别。没有有线基础设施来支持连接，并且不存在预定义的用于单位依靠用于制造互连的中央控制器。

这意味着系统的实施过程中，我们就不必担心关于所得到的网络的体系结构。这也是重要的，因为蓝牙功能的设备将不断上移，导致网络不断变化。没有基础设施意味着网络有很强的适应性。

**2.5 网络拓扑结构**

蓝牙设备可以组织成二至八个设备的组，它们共同形成一个微微网。每个微网将包含至少一个主单元，所有其他的参与微微网的单位将是奴隶。一个微微网的主单元控制微微网内的通信。

单位在一个微微网的数量是故意限制为八个（一个主，七从站），以保持所有单元之间的高容量链路。它也限制了开销所需的寻址。请注意，主/从角色只持续了持续时间的微微网。一旦微微网被取消，这些角色也被取消。任何单位可以成为主机或从机。根据定义，建立微微网的单位成为主单位。

两个或更多个微微网可以相互连接以形成一个散射网。两个微网之间的连接点是蓝牙装置，既微微网的成员。一台设备可以是在一个微微网上的一个主机，而在另一个是从机。设备也可以是一个以上微微网的从机，但它不能是一个以上微微网的主机，因为这将意味着这两个实际上是一个微微网（具有单个主）。

**图 1**: 示出了包括三个微微网一个散射网。两个微网通过俩网的一个节点连接。

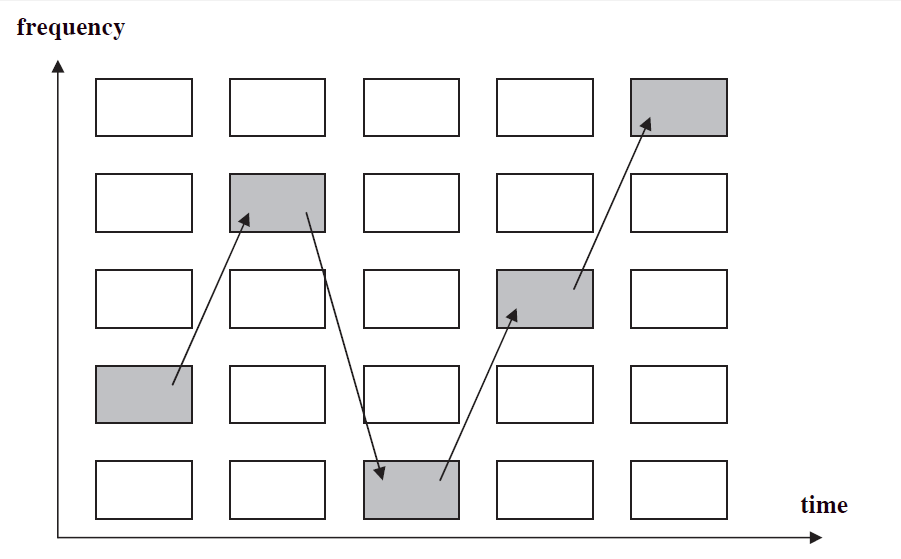
**2.6蓝牙安全性**

以下三种途径提供了蓝牙安全性:

1. 伪随机跳频。

2.认证

3.加密

跳频是一种扩频技术的目的是为噪声回弹性这一点。但是它也是一个很好的方式，以防止窃听[5]，因为窃听者以跟踪发送的通过蓝牙网络的频率变化是非常难的。下图显示了一个蓝牙信道的频率可以随时间改变。

**图 2**: 一个蓝牙信道的频率伪随机地改变。

认证允许用户限制到指定设备的连接。加密是数据只有授权设备/方可见，从而防止窃听。所有支持蓝牙的设备实施通用的访问配置文件，它定义了安全模式，包括三种安全模式：

1.不安全的模式。没有运行安全程序。

2.服务级强制安全。没有安全程序进行之前，建立信道。

3.链路级的安全。安全程序开始之前，建立完整的链路。

内置的用于处理访问控制的安全措施对本项目是很重要的。然而，这些固有的安全措施不足以应对未来的应用

**2.7蓝牙功耗和工作模式**

蓝牙支持四种为了节省能源，减小能耗的活动模型，这四种活动模型是：

1.活动模式

2.发觉模式

3.保持模式

4.暂停模式

在本文中，我们主要关注的是活动模式和保持模式，因为他们与手机的主要过程对应。在活动模式中，主设备和从设备彼此在相同的信道进行通信。这显然很耗电。这种模式用于当主机和从机之间的数据通信存在时。

在保持模式，主从之间没有积极的沟通。从设备仅仅侦听到信道，以确定它是否应该退出该模式。在这段时间内，从设备能够扫描，标记或查询在同一地区的设备。这种模式下消耗功率显著小于活动模式，如下表中所述。

|  |  |  |
| --- | --- | --- |
| 活动的模式 | | |
| 产品 | 在暂停模式功耗 | 在活动模式功耗 |
| CSR蓝芯01 | 0.3 mW | 0.6 – 135 mW |

**表 2:** 在活动的两种模式中进行功耗的差异比较。（从表中采取和提取）

**2.8蓝牙查询和连接建立**

****

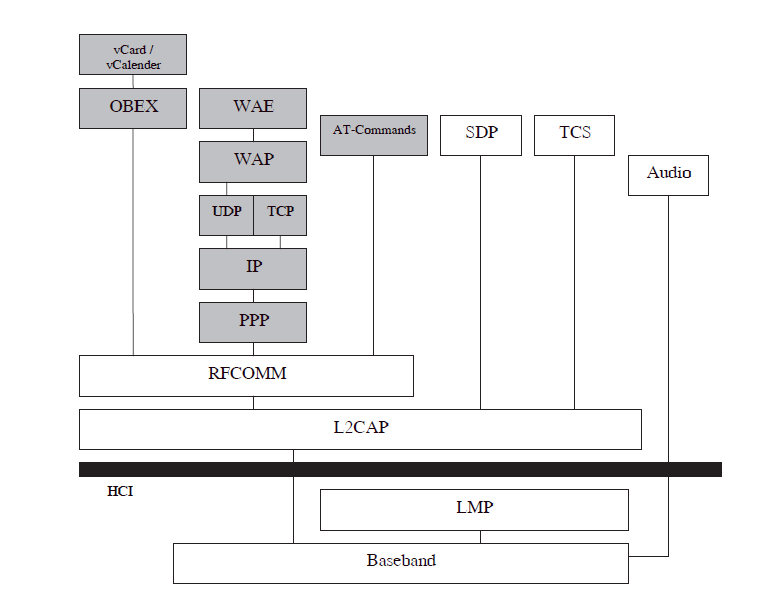
**图 3:**典型蓝牙连接过程。

查询程序是蓝牙的重要组成部分。这是一个过程，其中一个蓝牙设备试图找到所有相邻蓝牙设备。正试图扫描其它设备的设备被认为是处于“调查模式”。设备正在侦听查询请求是“查询扫描模式”。这种“查询扫描模式”通常是设定在一个设定为“发现”的蓝牙设备上。

当启动调查，该设备进入“查询模式”，并加速其跳频频率。另一方面，该设备在“查询扫描模式”降低了它的跳频频率。该算法将允许在“查询扫描模式”时查询设备赶上发射频率设备。这是因为，频率的跳频算法是蓝牙使用中较为重要的算法。当频率一致时，扫描设备将充当从设备，发送其掌握的地址和时钟信息。 [8]调查结束后，查询设备将能够发起连接到所查询设备。因为由查询设备发起连接，它将作为主设备。此初始连接被称为分页。寻呼可能从频率插槽由主设备完成发送寻呼请求。这个频率间隙计算从蓝牙地址来的和在接受调查的时钟信息。

在连接建立时，从机将同步其时间到了主机的时间。整个连接，主从不改变其跳频序列或相位（电流跳槽，由主时钟确定）。与此相反，从机将与主时钟同步所有的时间。

**2.9蓝牙软件堆栈**

蓝牙可以被定义为一个包括电缆替代协议，电话协议，所采用的协议，核心协议在内的分层协议结构。该层为了增加抽象性并适应其他蓝牙技术现有的协议而被指定。 **图 4:**蓝牙协议栈

核心协议是四个协议层包括[1，9]:

* **基带处理。**指定了空中接口的细节，包括频率，利用跳频，调制方式，以及发送功率。还指定微微网中连接的建立协议，寻址，数据包格式，为了传输，时序，功率控制和信道编码。
* **链路管理协议 (LMP).** 负责蓝牙之间链路的建立设备和正在进行的链路管理如加密和安全性。该范围内，当检测到其他蓝牙设备时允许发现服务。
* **逻辑链路控制和适配协议(L2CAP).** 适应上层协议的基带层。它也负责了上层多路复用数据。这是通过指定一个特定的PSM（多路复用数）来完成。
* **服务发现协议(SDP).** 查询可能可用的设备。不要求进连接。

我们感兴趣的是三个特定的层，因为它们是我们有可能实现的系统中的通信层，这些层是[1,9，10]。：

* **HCI** (主机控制器接口) 处于在L2CAP和LMP之间。它是程序员和协议之间的第一接口，允许了硬件访问功能。它也负责该多路复用数据到上层。
* **L2CAP** 层, 如上所述充当至上层的适应层，但是它也允许无连接数据传输。
* **RFCOMM** 层是电缆通信协议，旨在模拟串行端口。

我们决定在L2CAP层计划，因为RFCOMM只提供一到一连接，同时L2CAP允许数据的复用通过PSM数。这意味着两个蓝牙设备可具有多个连接到彼此，从而使不同的蓝牙程序同时运行。这可能不会是我们当前的实现重点，但它可能是为未来的实现是有用的。

**3. 蓝牙应用**

当下所用的大多数蓝牙应用可大致归为几个类别, 它们是：

1. 办公应用

2. 特设网络

3. 访问控制应用

办公应用往往关于建立无线工作环境。举个例子, 电脑的键盘和鼠标通过蓝牙连接到该电脑，或者连接多个计算机到支持蓝牙的显示器。这也涉及到电脑间的同步。举例说， 一个商人浏览并在自己的PDA上写了很多信息。当他下班回到家里, 他想把这些信息放到自己的笔记本电脑上。如果他的笔记本电脑和PDA支持蓝牙，这将变得很容易。

特设联网涉及范围内的多个设备，当它们被需要联系起来时，它们就形成了形成了网络社区（个人区域网）。目前应用包括电子名片用户之间的交流。

蓝牙设备可以在访问控制应用中使用。一个应用是，它可以进行移动支付，如信用卡。蓝牙设备，如蓝牙功能的手机可以与支持蓝牙功能的电影院售票机沟通，例如，允许用户购买一张票不用排队，然后为他的电话账单计费。或者，每个蓝牙设备可以包含一个唯一的代码，用来识别一个特定的用户，从而连接他在他的信用账户有多少信贷。蓝牙也可以用来作为房卡。用户可以进入一个建筑，或某些资源的控制区，通过他们的存在，可以在没有卡机的情况下刷卡。

**4. 硬件和开发**

**4.1 移动电话**

手机将运行手机版本的ZoneIT软件。如果手机检测到附近的接入点，该软件将会把手机的铃声音量调低。

用于移动电话的最低要求是：

1.可编程。

2.支持蓝牙的。

3. API必须能够访问蓝牙功能。

为了让蓝牙可编程，蓝牙协议（软件）堆栈是必需的。此协议栈在前面第2.9解释，并且它通常是在实施SDK。该SDK可以被看作是一个简单的库，允许程序员控制蓝牙设备。

我们的团队不得不考虑并决定在系统中用哪款手机。以下是备选手机。

**4.1.1 诺基亚 6310i**



**Figure 5:**诺基亚 6310i.

这款蓝牙功能的手机是我们的大学导师，博士蒂姆·摩尔提供给我们的团队。最初的计划是用java编程，按照我们采访到的诺基亚的代表的说法，这是编程这款手机的唯一方法。然而，诺基亚代表还提到，蓝牙的功能，功能不是提供给程序员。因此，这块手机不适合我们的项目。

**4.1.2 索尼爱立信 P800**



**图 6:** 索尼爱立信 P800.

这款手机是通过碰巧拥有手机的我们团队的阿古斯获得。对这样的手机做了一些研究之后，我们的团队发现，在手机跑在Symbian操作系统，这部移动电话为蓝牙功能提供了一个API。这使得手机的可开发。Symbian操作系统是一种用于移动设备如PDA和移动电话的流行的操作系统。这意味着，移植我们的电话代码在这些移动设备上是方便的。

**4.2 接入点**

接入点被用来控制周围的移动电话的铃声音量运行ZoneIT软件。它作为智能航标，以验证自身使用ZoneIT软件的手机。

接入点最低要求是：

1.蓝牙功能。

2.可编程，支持蓝牙发现和数据通信。

3.能够存储和处理蓝牙地址。

作为与移动电话，还需要一个蓝牙协议栈。我们有多种选择，以使有关平台部署接入点，并且接入点会在操作系统在其上进行操作。

1.支持蓝牙的IPAQ PDA（个人数字助理）。

2. Windows和Casira CSR蓝牙设备。

3. Windows和USB加密狗。

4. Linux和USB加密狗。

**4.2.1 IPAQ和Microsoft Windows CE**

IPAQ PDA有很多乐趣。它体积小，相当强大，运行在Windows CE操作系统上。主要的缺点是，它作为一个典型的PDA但花费超过1000美元，这意味着使用IPAQ作为接入点在涉及到部署不会极具成本效益。

即便如此，我们的团队被它的简洁和优雅吸引到。我们决定尝试在IPAQ上开发接入点。经过反复研究，我们发现该SDK（软件开发工具包）的Pocket PC免费分发。不幸的是，该SDK需要Microsoft的eMbedded Visual C ++开发，或使用Microsoft嵌入式Visual Basic开发。这些编程环境（IDE）将花费数千美元，因此我们决定不使用IPAQ。

**4.2.2微软Windows & Casira**

****

**图 7:** Carisa 核心控制器

Casira微控制器在BlueCore芯片上运行一个完整的蓝牙协议栈。它是所谓的BlueCore的微控制器和蓝牙无线电设备的组合无线电模块。使用Casira是有吸引力的，因为它可以作为一个独立的装置。但是它的主要缺点是，微控制器板限制内存。这可能需要我们对代码的长度加以限制。此外还有其他学生在蓝牙实验室与我们有冲突的使用这些模块。因此，我们决定去其他办法。

**4.2.3微软Windows和USB加密狗**

微软Windows平台加上蓝牙USB设备（加密狗）是另一个用来实现系统的吸引人的组合。这所大学在演讲厅拥有运行Microsoft Windows系统的多台计算机。加入蓝牙加密狗和访问控制软件，我们可以在我们的大学教室实现系统。经过研究，我们发现，从微软获得的SDK是免费的。不幸的是，在两个不同的计算机测试后，我们发现SDK的蓝牙堆没有正常工作，因为我们无法访问蓝牙堆栈功能。这可能是因为蓝牙USB适配器不支持我们使用。我们还在互联网上发现各种类似关于这个问题的言论论坛。

**4.2.4 Linux and USB 加密狗**

类似于在以前第4.2.3的情况，这个选项有吸引力是因为电脑在大学广泛应用。另外，在Linux操作系统是一部分GNU，所以它是开放的，并且可以从互联网下载。 GNU软件被允许公开分发，使用和修改。经过一番研究，我们发现了一个Linux蓝牙堆栈称为BlueZ。当时，Bluez已经成为官方的Linux版本蓝牙堆栈。并且在Linux中，Bluez也是GNU软件。

**4.2.5选择的平台和操作系统**

经过多次评估和测试这些选项，权衡的利弊后，最终，我们终于决定在Linux上使用USB加密狗实施接入点的程序，详见第4.2.4节。

在Linux上使用USB加密狗的优势在于：

* 蓝牙加密狗的花销确实低 (大约 $60)。
* Linux操作系统和 Bluez 蓝牙堆栈是免费的。使用Linux自带的C编程语言工具进行开发，如 GCC 或者 CC。
* Bluez实现堆栈中的很多层例如 SDP, RFCOMM, L2CAP, HCI层。
* 支持多种蓝牙设备，包括我们使用的是MSI加密狗。我们使用Mandrake Linux的9.1版与Bluez。装置的Bluez在Linux上将在附录中进行描述。

**4.3编程工具和SDKs**

本节应描述编程工具和软件开发工具包（SDK）这是在我们的软件系统的开发中使用。由于这两种手机和接入点是不同的平台上，每个人都有自己的一套工具和SDK。在使用这些工具和SDK时讨论一些优势。

**4.3.1 移动电话**

**4.3.1.1 Symbian 操作系统和它的蓝牙堆栈**

Symbian操作系统是多尼爱立信P800运行的操作系统。 Symbian 有几个变种。例如， 60系列手机上运行的Series 60的Symbian操作系统， 而索尼爱立信 P800运行UIQ Symbian操作系统。所有的这些操作系统都是相似的， 并且所有的代码都在Symbian 操作系统上实现并可以方便的移植到其他Symbian 操作系统上。

Symbian操作系统提供蓝牙堆栈的所有基本功能并定义蓝牙版本为v1.1。此外，它在有限的程度允许程序员访问RFCOMM，L2CAP，SDP，HCI层。因为我们的团队是在L2CAP层编程，这款蓝牙协议栈是足够满足我们的需求。

**4.3.1.2在 Symbian操作系统上编程**

Symbian的编程是简单，除了一个事实，即代码在任何测试可以做之前必须是编译和部署在手机上。在这种情况下，仿真器的电话将是理想的。索尼爱立信提供这样一个仿真器，但需花费高额费用。然而，即使我们愿意支付仿真器的成本，直接在仿真器上策是我们所有的蓝牙代码是不可能的，因为仿真器无法识别外接蓝牙设备。

开始了编程所需的现有代码的研究。我们的团队所使用的代码是“HelloWorld”的例子。我们的团队修改这个代码，并形成了我们的软件系统的应用框架。由于该项目的重点是蓝牙开发，我们不想花太多时间在用户界面上。索尼爱立信提供了一个在线论坛，它只是提供技术援助。最的时候，它并没有帮助。但是有一些由Symbian程序员建立的几个网站。虽然这些网站大多不注重的Symbian UIQ编程，但它们是有很大帮助，因为之前提到的，大部分的Symbian代码可以很容易移植跨越Symbian操作系统的变种。大多数时候我们需要的手机资料上的文档，这是与Symbian SDK一起打包。这些信息是非常有用的，是移动电话软件的成功。然而，有一些问题在文档。例如，有在实施代码的错误，以及几个功能并没有在文件中很好的说明。

**4.3.2 接入点**

**4.3.2.1 Linux 和 Bluez**

Linux是在GPL下发布一个众所周知的开源操作系统（GNU公共许可证）。这意味着，它是免费使用或分发。近日，Bluez一直做出正式的Linux蓝牙协议栈。因此，最近的Linux发行版2.4.6或更高版本将包括Bluez包。这也表明，Bluez是相对于其他的Linux蓝牙栈被确认为可靠的堆栈，并且将在未来该开源社区得到更多的关注和改进。Bluez最初是由高通公司开发的。

其他知名的蓝牙堆栈是OpenBT和Affix。两者都开源.OpenBT已经在有些方面有了静态的更新和改进，而Affix是由移动电话公司诺基亚开发新的堆栈。使用Linux和Bluez的理由最初是由于经济原因，其他蓝牙协议栈和操作系统的组合都是昂贵的。但随着项目的进行，我们发现Bluez了许多积极的方面。Bluez实现几乎所有由蓝牙限定的可用的栈标准。

从bluez官方网站采取执行堆栈的名单是：

* 蓝牙核心 - HCI设备和连接管理器。
* HCI USB，UART，PCMCIA和VHCI（虚拟HCI）的驱动程序。
* L2CAP-可靠的数据报协议。
* RFCOMM - 串行端口仿真。可靠的面向连接的流协议。
* BNEP - 以太网仿真。
* SCO - 同步连接（音）。

bluez的支持链路层的安全，和多个连接。这些都是我们项目的关键。在这些之上，它也允许多个蓝牙设备，可能需要对于未来的本文扩展。例如，我们可以使用多个设备创建单一的“虚拟”的接入点。这扩大了服务的覆盖区域。

**4.3.2.2 Bluez 编程**

Bluez的是一个开源项目。因此，没有太多的支持给予使用堆栈的程序员。API（应用程序编程接口）提供给程序员参考的功能。不幸的是，在Bluez中不存在一个API。因此，为了使程序员使用Bluez堆栈编程，他们给出的示例文件，也尽量筛选Bluez邮件列表的任何主题相关的程序的开发。

从包中给出的文件是C（源）文件和H（头）文件的形式。但是很少有，或者没有文件作出关于所用的功能文件。因此，它作为我们开始编程方面接入点是很难的。但是，邮件列表和FAQ（常见问题解答）的帮助源代码为理解接入点程序提供了依据。

幸运的是，Bluez L2CAP是一个使用标准UNIX C套接字编程的基于编码的套接字。因此，我们能够很容易从其他来源理解我们的基本需求内容。

**4.3.3.3 可移植性**

正如本报告前面提到的，Bluez使用Unix的C，以及它也使用标准套接字编程。这是Bluez的网站中提到的，上面写着，“添加Bluez支持到任何现有的基于socket的程序是很容易的。例如，你可以使用AF\_BLUETOOTH而不是AF\_INET（IP），当你进行了一个套接字调用。你会使用sockaddr\_l2代替SOCKADDR\_IN，使用SOCK\_SEQ\_PACKET代替SOCK\_STREAM等。只介绍了少数的新数据结构和常数“。

这意味着，它很容易将其他C套接字程序移植为C蓝牙套接字程序。它还意味着，我们可以很容易的将C套接字移植到Bluez，到另一个栈或是另一个平台。在接入点的变成后，我们的团队认为应用秉承了通讯模块，它采用L2CAP基于编程的套接字。但同样也不能说它使用的HCI层扫描模块是仅仅特定于蓝牙的。

**5. 论文方案**

**5.1问题陈述**

目前，大部分的访问控制解决方案已通过使用常规的技术做了出来，如条形码刷卡，和插入针号。随着配有蓝牙的较新的移动设备的引入，使用蓝牙技术代替旧的访问控制技术成为可能。蓝牙允许无线接入控制应用程序的开发。我们的论文试图展示在门禁应用中使用蓝牙技术。我们的团队已经选择了一个特定的应用程序，这将在下面说明。

手机的铃声经常中断会议，如正在开展的演讲。这通常是由于移动电话用户在他们的会谈前忘记关闭手机。这不仅惹恼了在会议中的其他各方，同时也中断了正在进行的会议。

**5.2提出的解决方案**

如果可能的话，一种实用的解决这个问题的办法是当它们进入一指定为“无声”区，如在会议区域时自动关闭这些移动电话。这样一来，即使在手机的业主忘记手动将其关闭，有一个来电，手机铃声也不会打断会议时。

这个概念以后可以扩展到其他访问控制应用，例如使用蓝牙功能的手机，以进入一个房间，这是由一个支持蓝牙的锁实现。另一个例子是，创建一个应用程序，可以提供一个博物馆的导游，例如，为区域内的访问者是文本，音频和图象。

* 1. **需求**

我们的项目团队想提案，设计和实施一个系统解决上述的问题。以下给出了顶层描述来描述系统应该如何的表现

* 一个用户带着移动电话进入指定的“沉默”区。一个定义了的接入点区域覆盖了该区域。
* 当用户进入的“沉默”区域时，用户的移动电话将能够检测接入点的存在。
* 移动电话应当能与该接入点区域对话并确定这是静默区域，然后它会自己调低自己的音量。
* 手机只要在临近接入点的覆盖区域就会保持它的铃声音量调低。如果它退出的覆盖区域，手机音量将恢复以前的状态。
* 该系统必须是弹性的能够以拒绝服务策略应对俩种形式的攻击。

- 恶意蓝牙设备应不能关闭移动电话的铃音

-接入点应该是健壮的，以使得攻击者不能

打倒它所提供的服务。

系统的需求应该松散的定义，比如可以允许不同的方法来解决问题。接下来的章节会介绍一些可能符合需求的方法。

**5.4 可能的方法**

以下是我们的团队提出的解决这个问题三种可能的途径的剪接陈述。每个解决方案都有自己的优点和缺点。

**5.4.1方法一：被动扫描**

这里在移动电话和接入点之间将没有实际的数据通信。该接入点系统的蓝牙地址将被硬编码到移动电话的软件，或经由在移动电话中的数据库访问。当移动电话不周期性查询并检测附近的蓝牙设备，它将比较这些设备的蓝牙地址与那些在数据库中的蓝牙地址。如果存在匹配，则移动电话将会知道它处于一个“无声”区并会关闭它的铃声。

这种解决方案的优点是，它易于实施，因为我们将不用做任何形式的socket编程，我们也不用在接入点上做任何形式编程。另一个优点是该系统的可扩展性，因为每个手机负责自行关闭。接入点仅作为类似灯塔的存在而没有任何处理要求。

这种方法的缺点是没有办法来实现的任何形式的应用层认证，这意味着该系统将是容易受到拒绝服务攻击（参见6.5.6）。如果恶意用户使用假的欺骗性的蓝牙地址冒充一个真正的接入点的蓝牙地址，那么他将可以非法关闭手机的铃音。此外，该手机需要知道之前所有接入点的蓝牙地址，这意味着该在移动电话中的数据库可能经常需要被更新。这使得部署和维护这种系统十分困难。

**5.4.2方法二：数据通信和被动扫描**

移动电话将作为服务器运行，所述接入点将作为客户端运行。接入点会定期扫描附近的蓝牙设备。一旦它找到一个蓝牙设备（手机），它试图建立一个沟通渠道（通过套接字）与电话，并用它进行认证。一旦认证完成后，手机关闭了呼入音，并记录该接入点的蓝牙地址。然后，它继续查询附近的蓝牙设备，使用记录的蓝牙地址查询是否还在接入点覆盖范围内。

这种方法的优点在于，它能够不管蓝牙地址而验证接入点。因此，没有必要对所有可能的接入点的进行蓝牙地址硬编码，或存储所有数据库中的地址。此办法还享有可扩展性。接入点只需要验证每个移动手机一次，而忽略它的其他时间。手机将自己确定是否仍然是在接入点的覆盖区域。

这种方法缺点是，它仍然可能是欺骗性的接入点蓝牙地址，允许恶意用户使用软件来欺骗电话，以为这是静止接入点的覆盖范围内，而它实际上不是在此范围内（即，在认证阶段之后）。

**5.4.3方法三：定期轮询**

这种方法类似于第二个方法（5.4.2）。然而，接入点会在每一个预定周期（需要一个定时器）试图建立与电话的通信信道，代替之前的信道。手机也不会对附近的蓝牙设备做任何查找。只要在接入点管理通信手机在时间间隔内，手机铃声依然关闭。否则，该手机会认为它是“沉默”区外，并恢复它的铃声。

这种方法的优点是，它比其他两种方法更安全。这是因为该接入点以规则的间隔被认证。恶意用户仍然可以欺骗接入点的蓝牙地址，但不能够让与移动电话进行本身验证。此外，在这种方法中，所有的处理负荷从移动电话传送到接入点。由于移动电话具有比所述接入点少的处理能力（接入点是一台PC），这可能是一个值得考虑的重要因素。

这种方法的一个显著的缺点是该系统的可扩展性。如果太许多用户试图同时使用系统，接入点可能会遇到应对这些用户的麻烦，因为它会在一定的时间间隔，再次验证他们。接入点可能在认证用户列表中，而当用户的下一个清单到达，从而导致用户的积压从而迫使它必须重新验证。另一缺点是能量需求。这种定期轮询会需要定期的数据通信（主动模式），这将消耗手机电池的大量电源，如第2.7节所述。

**5.5 方法的选择**

我们的团队已决定使用第二种方法，如第5.4.2所述。这是因为我们的系统需要部署在一个有大量用户的环境，如在演讲厅。这意味着，该系统大规模大数量的用户，因此在节5.4.3中描述的第三种方法无法实施 。此外，因为我们希望我们的系统是安全的，我们不能使用在第5.4.1描述的方法。虽然第二种方法是容易受到欺骗，但我们的团队认为这是做法1和3之间一个很好的互补，因此我们决定采取这种做法。

能够允许用户在移动电话的软件系统中在三种方法之间进行选择，因为这三种方法可以被编程为该系统的独立组件。但是我们的团队已经决定不这样做，由于缺少时间，并将他它作为一个在今后的工作中的可能的扩展。

**5.6 规范**

从上面的要求和做法中，我们的团队已经建立出了一套规范，为了提供所需的功能，我们的系统必须坚持这个规范。

**5.6.1 移动电话/接入点接口**

* 移动电话和接入点必须通过蓝牙v1.1版本规范进行通信。
* 使用大多数通信系统使用的的客户机 - 服务器关系的模型，移动电话将作为一个服务器，而接入点会充当客户端。接入点就可以访问移动电话。

**5.6.2移动电话**

* 一旦启动，该软件将运行服务器模块，监听传入的​​蓝牙连接。
* 如果启动传入连接时，移动电话将必须确保传入连接的所有者属于一个值得信赖的接入点。如果不是，它将关闭连接，继续侦听新的连接。
* 认证之后，移动电话推断，这是在一个“无声”区域，并且自动关闭了它的铃声音量。然后关闭蓝牙连接。
* 在此期间，手机需要周期性询问指向，以确保它仍然是在接入点的覆盖区域内。
* 因为蓝牙是一种无线通信标准，它经常经历信号减弱，这种“询问”程序在移动电话判定它是不是在接入点的覆盖区域时将收到多次查询失败。如果失败的次数太多了，本软件停止“查询”程序，并恢复铃音音量。
* 一旦离开了覆盖区，该软件重新启动的服务器模块来监听新传入的连接。

**5.6.3 接入点**

* 接入点扫描其覆盖区域内和附近的所有的蓝牙设备。接入点将保存所有形式的蓝牙地址，蓝牙地址是所有蓝牙设备的唯一标识符。
* 接入点随后将尝试与所有的移动设备进行通信，并关闭那些安装有ZoneIT软件手机的铃声。
* 在通信过程中，接入点将要求移动设备验证自己。这个认证用于确保接入点被授权能够关闭的移动电话的铃声。
* 接入点必须是有效的，能够同时连接到多个移动电话。
* 最后，接入点不应当与之前已经连接过的手机重新连接，因为这样做是多余的。