摘 要

随着网络和通信技术的发展，移动终端身份认证的需求已经成为众多安全要素中需要着重考虑的一环。基于音频的认证系统相比现有的认证手段，是一种解决了现存方法中的一部分弊端的手段。课题核心要求为：设计一套基于音频的安全D2D通信系统。

认证系统基于移动设备，得以具有良好的普适性，并要求系统本身具有足够的可靠性和稳定性。且因为移动设备几乎都具备麦克风和扬声器，得以保证系统的门槛足够低，能够广泛应用，且不同型号的设备之间存在差异，使得系统能够实现认证功能。

课题的主要内容为：

①设计基于音频硬件物理指纹设备认证应用软件

②设计基于音频硬件的安全信息传输的应用软件

③完成基于音频的安全D2D通信系统

其中，根据学期不同，本学期主要完成的目标为第一项。基于硬件和软件的需求，我们需要在移动设备上开发一款使用音频硬件物理指纹来实现设备认证的应用。

这款应用应当实现的功能，有：生成随机认证音频、学习认证音频并提取指纹、基于已有指纹验证新的认证音频。其中，生成随机认证音频部分考虑如何产生适当的音频，考虑功能性；学习认证音频需要考虑如何从收到的音频中排除干扰，提取出指纹，并且防止可能的攻击伪装；认证部分同样需要有相关考虑。

本课题同时会使用跨平台开发语言Flutter和Dart，使最终作品能在不同手机系统上运行而无需分别编写完整原生应用。

**关键词：音频物理指纹，应用软件设计，功能实现，跨平台，Flutter**

# 目 录

第一章 复杂工程问题归纳与实施方案可行性研究 1

1.1 需求分析与建模 1

1.2 复杂工程问题归纳 1

1.3 实施方案与可行性研究 1

第二章 存在问题与解决方案 2

2.1 存在的主要问题 2

2.2 解决方案 2

第三章 执行情况与完成度 3

第四章 分工协作与交流情况 4

参考文献 5

致谢 6

# 第一章 复杂工程问题归纳与实施方案可行性研究

## 需求分析与建模

对于开发这款应用软件，我们依据本学期所软件工程知识的内容实现了软件生命周期内从问题定义到软件详细设计的部分，给出了一个可交付的应用软件界面。由于前期需求明确，我们采用了改进的瀑布模型的开发方式，完成了需求分析，软件设计和一部分的软件测试。

需求分析部分通过需求获取、需求提炼、需求描述，我们撰写了一个基本的软件规格需求说明书，

发送端：

(1)、建立连接，获取接收端ID；

(2)、产生混频信号；

(3)、在不同距离多次发送信号。

接收端：

(1)、建立连接，发送本机ID，获取对方ID；

(2)、接收信号；

(3)、对接收的信号进行FFT变换以及对数处理；

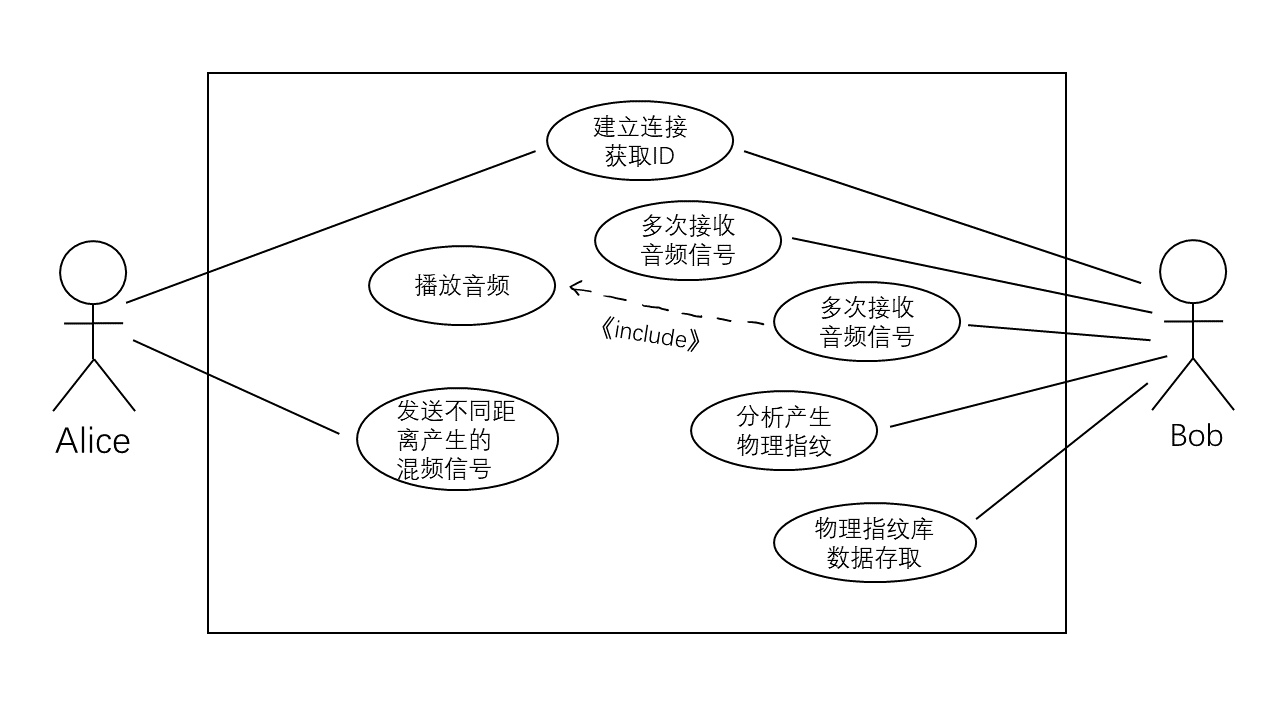
(4)、判断是学习或认证。若是认证，跳转到步骤5，若是学习，则保存学习文件；

(5)、读取对方的多次学习数据，通过比较，得出与认证信号最接近的一组学习值；

(6)、利用步骤5得到的学习值，通过带宽分析法得出认证值；

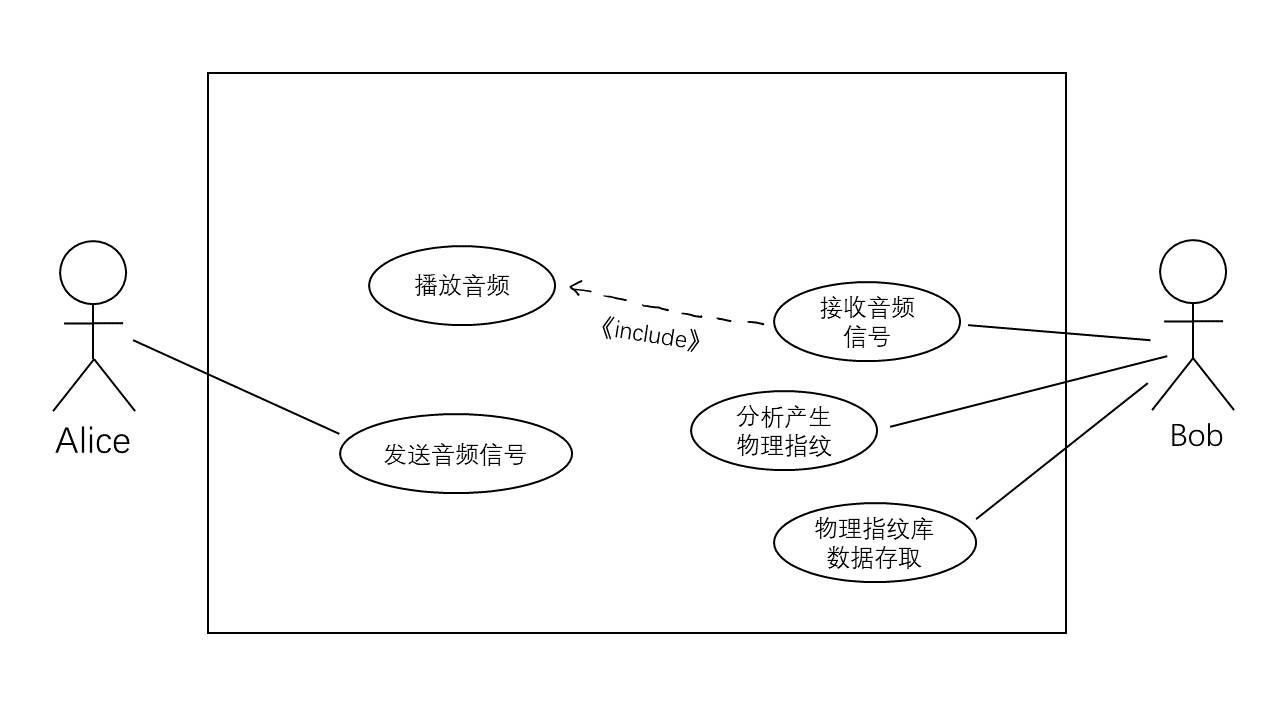
(7)、将认证值与阈值进行比较，判断是否认证成功。

由于前期需求明确，类数目少，类间关系简单，故直接基于说明书，从面向过程和面向对象两方面进行了功能模型的建模，软件主要实现两个方面的功能，即学习和认证，学习是认证的基础，学习部分的顺利多次完成与认证成功率呈明显正相关。对于发送端和接收端，又需要实现独享和共享的不同功能，如建立连接、播放音频、发送音频、分析音频指纹等。以对象为核心，学习部分实现所需要的功能和性能的功能模型如下，其中Alice为发送端，Bob为接收端，也即学习的一方，功能要求包括建立连接、发送与接收音频信号、指纹提取等：

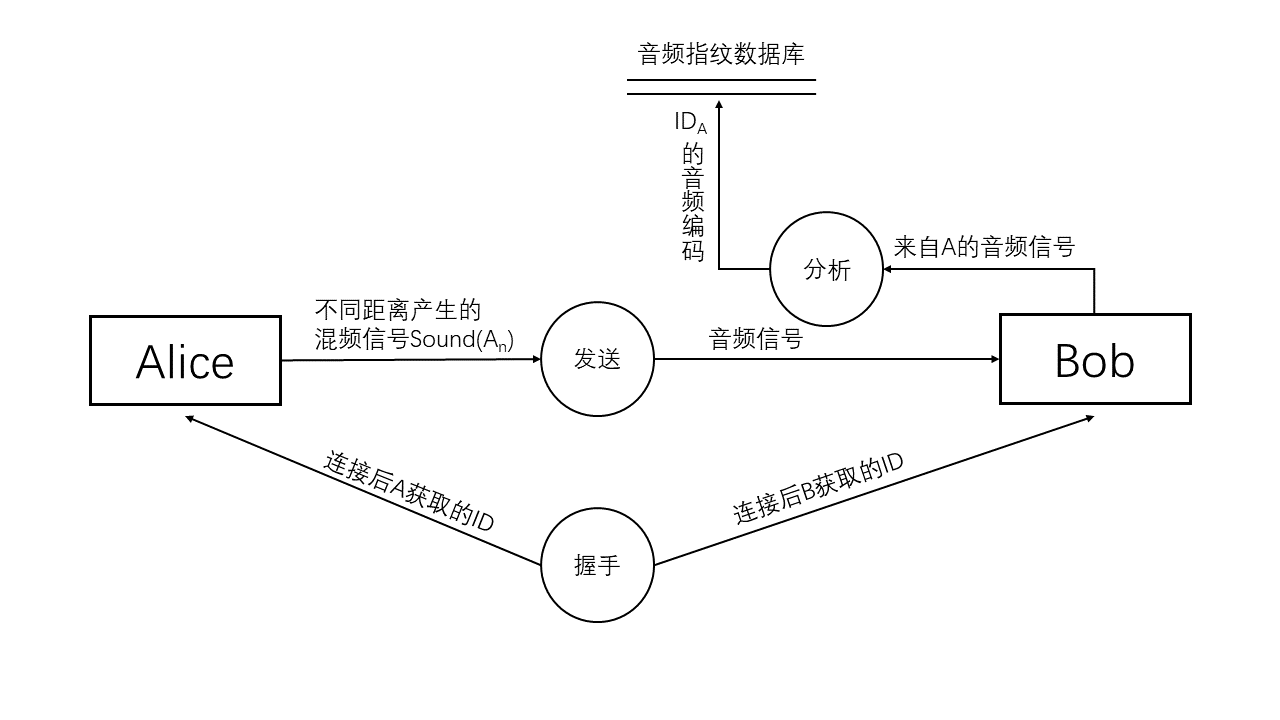


接下来进行认证部分的建模。

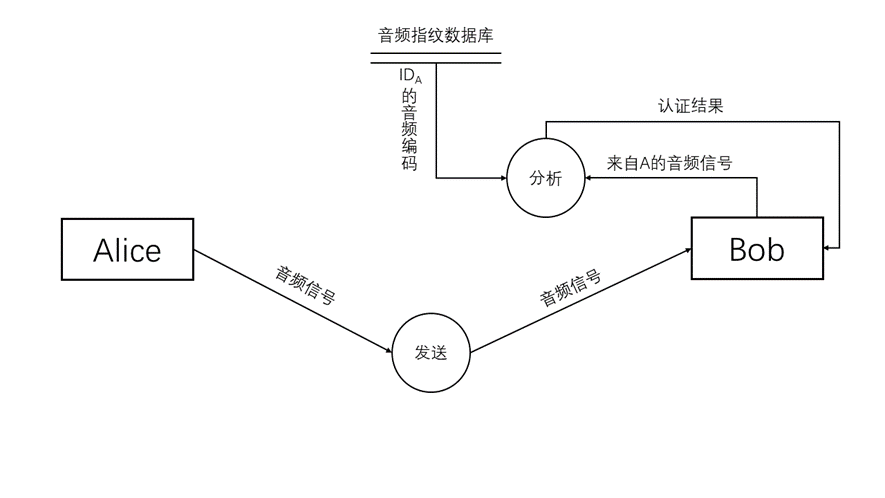
由于学习部分与认证部分从用例图中无法准确识别数据流向的数据操作的详细区别，故我们又采用了双角度的方式，面向过程进行了数据流的建模。通过分离学习和认证角度，分别准确展示出他们所进行的不同流程以及所需要的功能、其中的数据走向，如图所示：



学习部分的功能模型，如图所示：

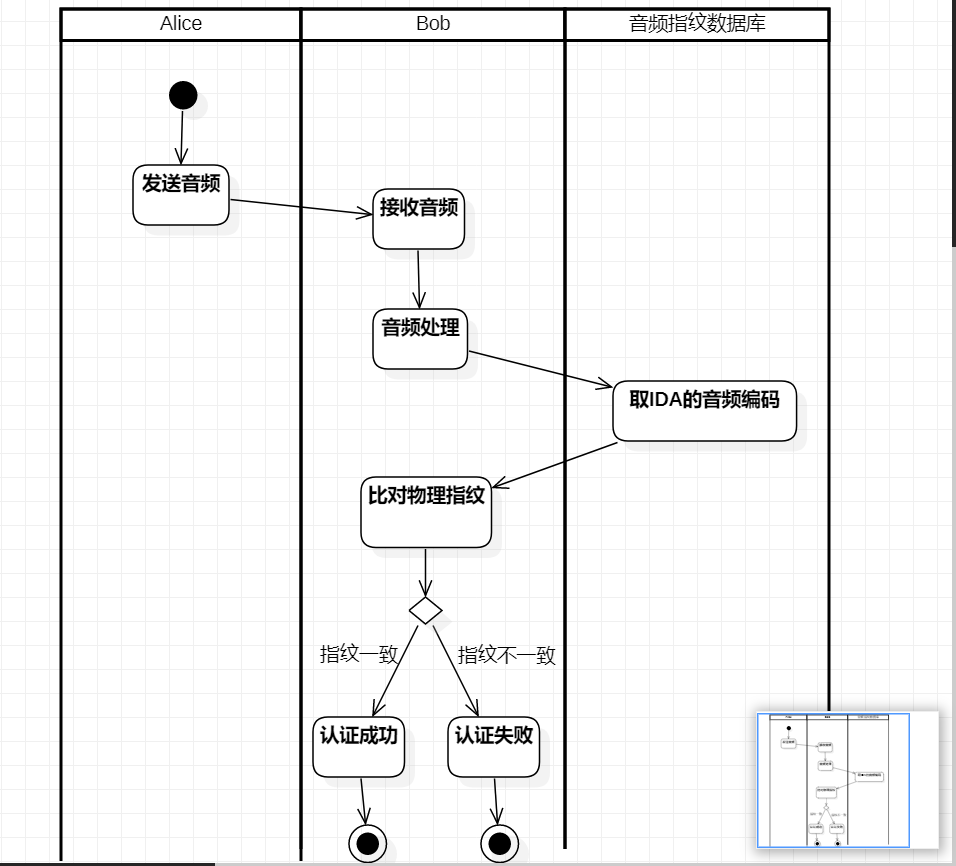


认证部分的功能模型，如图所示：



通过这样对项目建模，数据传输和操作一目了然。

接下来，便可以很轻松地根据用例图和数据流图进行每个用例的细化，下面给出认证的活动图。活动图采用带泳道绘制，分别标注发送端、接收端以及相应的音频指纹数据库，UML格式：



通过建立完善的模型和图表，我们对于项目的结构和需要实现的功能已经有了大致的框架。至此，需求分析与建模方面的工作暂时告一段落。

## 复杂工程问题归纳

在需求分析中，我们有较多的功能需要进行相应开发，由此也产生了诸多的复杂工程问题。

譬如，如何设计算法，产生我们需要的音频信号；如何设计使用FFT算法，对产生的音频信号进行分析、提取指纹；如何管理物理指纹库；使用什么方法对软件进行开发等等。

其中，生成音频信号方面，我们需要考虑对相应的频点如何附加要传送的信息。考虑到嘈杂环境中，需要对于噪声、环境音等干扰音源进行处理，且需要利用算法对于音频的特征进行分析，在满足相对较高的认证成功率时，降低被攻击的可能性，特别是可能出现的相同硬件型号攻击等成功可能性较高的攻击手段。如何改进音频生成、认证使用的相关频点，是一大难点。

而对于FFT算法，我们需要更加深入的研究，通过合理地运用FFT算法实现能达成我们作品所要求的特性的认证算法，是我们需要重点解决的另一难题。

开发软件方面，移动端有两大操作系统：Android和iOS可选。考虑到两系统不互通，且Android开发比较贴近我们的所学内容，应当主要考虑以Android作为开发方向。

## 实施方案与可行性研究

开发软件，我们决定选用能够跨平台的编程解决方案Flutter。其使用Dart作为编程语言，并且支持跨Android、iOS等平台开发软件。考虑到移动端平台整体特性十分接近，硬件属性差别不大，Flutter提供的跨平台特性应该足以让我们完成软件的开发工作，并且比较方便地实现同时在Android和iOS两大平台上运行，做到真正的低门槛、易用。

为了防止跨平台开发存在的潜在风险，我们同时也在推进纯Android的软件开发。Android平台上已有众多成熟的库和包，可以用于实现项目所需的各种功能，以作为Flutter暂无法实现时的后备方案。

算法方面，我们通过对以往相关研究论文的学习，考虑使用“带状匹配算法”时可以有效匹配音频硬件物理指纹。我们决定使用该算法进行相关的匹配，同时对算法进行必要的改进，使之能达成课题的开发目标。

# 第二章 存在问题与解决方案

## 2.1 存在的主要问题

在app的界面开发中，我们遇到的主要的问题是：为了实现app界面的简洁和美观，需要自定义底部导航栏和顶部导航栏。我们使用的跨平台开发解决方案Flutter带有自己的底部导航栏组件（BottomNavigationBar）和顶部导航栏组件（Tabbar），底部导航栏的图标一般来说是通过自带的Icon组件实现的，且Icon组件自带选中和未选中的显示形式，顶部导航栏则只能在tabs变量里面添加多个组件来实现图标的显示，于是如何使用自己的图片实现Icon组件的替换便成了第一个问题。

另外，由于app中包含了多个页面，如发送、握手、接收等页面，放在一个文件中会显得复杂，不便于阅读修改。于是把不同的页面写在不同文件中进行封装，那么如何在主页面内通过点击导航栏、左右滑动等方式实现页面的切换也是一个问题。

除此之外，Flutter提供各类构件和开源库，通过引用这些组件，可以实现代码重用，减少我们的工作量。但是，如何合理利用其中有用的组件来设计实现音频认证需要的各种算法，使其能在不同平台上正常工作，也是我们面临的一个挑战。

Android开发方面，界面我们使用Material Design的底栏切换页面实现不同功能页面的切换。如何给这些功能页做跳转，以及相关的布局设计是要解决的问题。

## 2.2 解决方案

首先是底部导航栏。通过BottomNavigationBarItem组件中的icon和activeicon组件变量，我们将图片放在本地并在pubspec.yaml中进行配置，将对应的未选中和选中时的底部导航栏图片赋给icon和activeicon，从而实现底部导航栏的使用图片替换Icon组件。

而顶部导航栏，由于没有自带的icon和activeicon属性，要略微复杂。

首先创建一个组件数组，将6种Image组件图片放进去，然后定义一个tabController，再使用tabController来实现页面的切换。每次切换时，使用tabController.addListener进行监听，通过setState函数切换顶部导航栏的状态，更改相应的变量，最后在顶部导航栏的tabs里通过 组件数组[变量] 的方式添加组件，即可实现顶部导航栏图片的切换。

而页面的切换，也是通过类似的组件数组和当前索引值（currentIndex）这一变量，在切换页面时更新当前索引值，在Scaffold的body中用 组件数组[变量] 的方式添加页面组件来实现。

Android方面，我们使用fragment实现不同页面，以及NavigationView来切换不同的页面。同时，使用menu的方式作为底栏的provider，实现底栏简单切换不同页面。

# 第三章 执行情况与完成度

软件开发方面，目前Flutter的界面设计已经基本完成，接下来是和算法以及软件功能进行对接，使用Dart语言实现所需要的带状匹配算法，并且实现相应的各种功能，完成软件开发工作。

Android方面，其开发功能基本完整，目前界面以及一些代码需要更新，作为目前的第二选择具有较强的健壮性。

# 第四章 分工协作与交流情况

课题在组内的分工如下：

冉江皓：统筹开发进度，开发Android作为后备选择；

邓亚辉、官宏：开发Android作为后备选择；

罗驰宇、冯一凡：开发Flutter方向作为主要开发方向。

因为Android方向和Flutter方向也有一定程度重合，组内信息共享交流比较活跃，目前保持开发进度稳定前推，预期可以顺利完成目标。

# 参考文献

1. 无

# 致谢

本报告的工作是在我们的指导教师陈大江老师的悉心指导下完成的，而这份报告的诞生离不开所有组员的一起努力，包括主力开发Flutter的冯一凡和罗驰宇、主力开发Android的邓亚辉、官宏和冉江皓。除此之外，我们还想感谢众多开源文档的贡献者。没有你们创造的自由的平台，就没有我们今天开发的软件。

诚挚地表示感谢！