装 订 线

浙江大学

本科实验报告

姓名： 潘盛琪

学院： 电气工程学院

专业： 自动化

学号： 3170105737

指导教师： 冀晓宇 陆铃霞

2019 年 12 月 2 日

实验名称：海豚音攻击最小系统实现 姓名：潘盛琪 学号：3170105737

专业：自 动 化
姓名：潘盛琪
学号：3170105737
日期：2019 年 12 月 2 日
地点：玉 泉 教 2

浙江大学实验报告

课程名称：物联网安全 指导老师：冀晓宇 陆铃霞 成绩：

实验名称：海豚音攻击最小系统实现 实验类型：探究性实验 同组学生姓名：毕铁锴

一、实验目的

1. 本实验要求学生结合理论课程中物联网**终端传感器安全**核心技术，结合信号分析和处理技术，基于矢量信号发生器、频谱分析仪、示波器、超声波发生器等设备，观察麦克风非线性作用；针对智能语音系统，实现基于器件非线性作用的安全攻击，并进行防护机制设计。

二、实验原理

1. 常见的语音指令系统主要包括两个模块：语音信号获取及语音识别，如 Figure 1 所示。

语音信号获取模块首先获得语音信号，然后进行放大、滤波和 AD 转换；然后，语音识别模块再对原始捕获的数字信号进行预处理，以去除超出声音范围的频率，并丢弃无法识别的信号段，然后识别处理后的信号的内容。

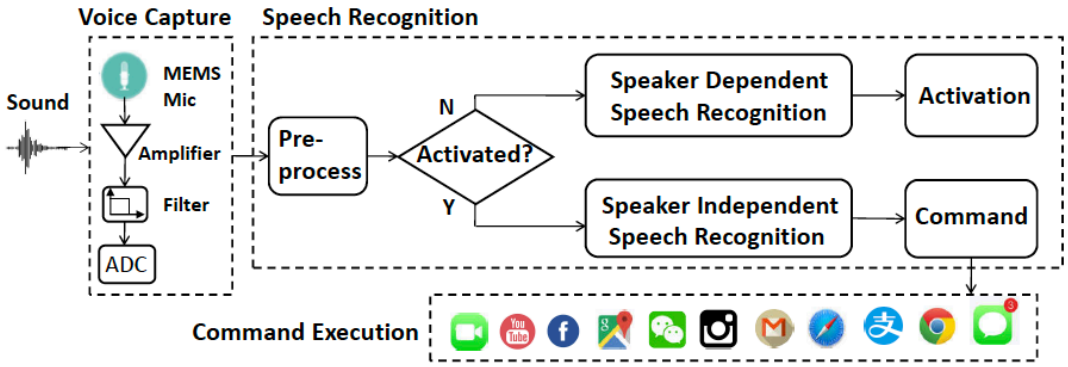


Figure 1 **常见的语音指令系统**

2. 非线性影响模型

麦克风可以被视为输入/输出信号传输特性中具有平方非线性的组件，放大器可以产生低频范围内的解调信号。这里我们研究麦克风的非线性，其模型一般如公式 1 所示。假设输入信号为 Sin（t），则输出信号 Sout（t）为：

$$s_{out}(t) = As_{in}(t) + Bs_{in}^2(t) \qquad \text{(公式 1)}$$

实验名称：海豚音攻击最小系统实现 姓名：潘盛琪 学号：3170105737

其中 A 是输入信号的增益，B 是二次项的增益。线性分量采用正弦输入频率为 f 的信号并输出具有相同频率 f 的正弦信号。相比之下，电气设备的非线性会产生谐波和叉积。这些非线性特征会带来不希望有的失真，产生新的频率，但通过精心设计的输入信号，这些新的频率可以恢复出基带信号。

假设所需的语音控制信号为 m（t），我们选择中心频率为 fc 的载波上的调制信号为

$$s_{in}(t) = m(t)\cos(2\pi f_c t) + \cos(2\pi f_c t) \quad \text{（公式 2）}$$

即使用幅度调制（注意：所以实验中信号发生器要设置为外调制模式下的 AM 模式，与此处对应）。可令 m（t）为 m（t）= cos（2πfmt），计算得到 S_{in}，即传送给麦克风的输入信号，联立上面两方程，得到 S_{out}，并进行傅立叶变换，可以得到麦克风输出信号包含预期的频率分量 fm 以及 S_{in} 的基本频率分量（即 fc-fm，fc + fm 和 fc），谐波和其他交叉乘积（即 fm，2（fc -fm），2（fc + fm），2fc，2fc + fm 和 2fc - fm）。经过低通滤波器后，所有高频成分将被滤掉，而 fm 频率成分将保留下来，如 Figure 2 所示：

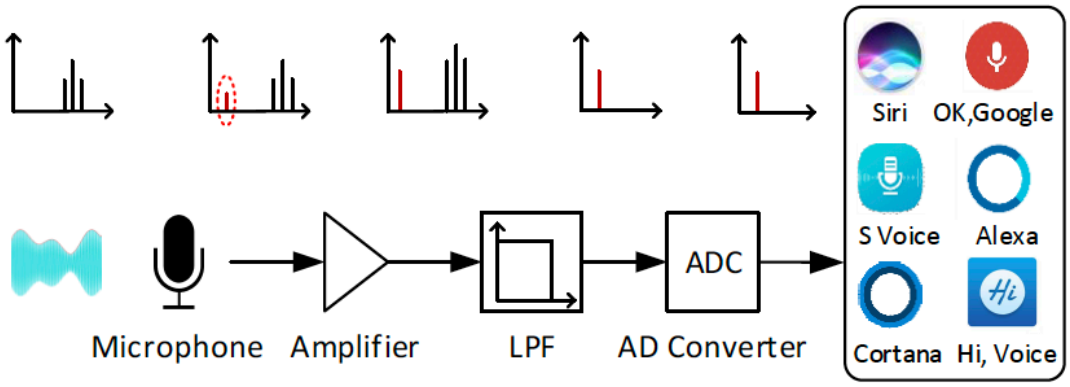


Figure 2 被攻击过程中的语音信号分析与处理过程

三、主要仪器设备

1. 信号发生器（调制）、超声波模块、示波器、音频连接线

四、实验过程

“海豚音”攻击重现，基于单超声波探头，实现对手机或者电脑等设备的攻击，具体步骤如下：

1) 下载 TTS（Text To Speech）APP 工具，运行该软件，并输入相关的文本备用，如图 3 所示：

装 订 线

实验名称：海豚音攻击最小系统实现 姓名：潘盛琪 学号：3170105737

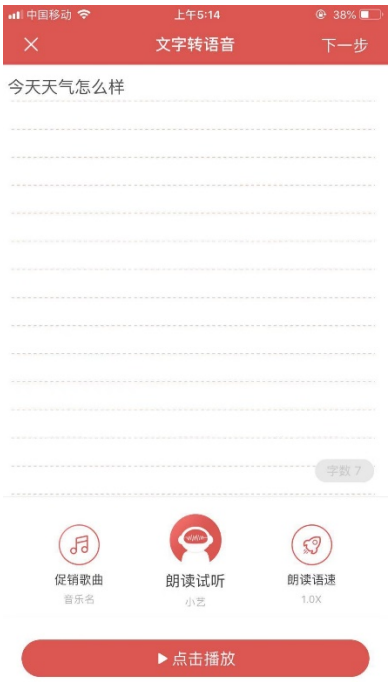


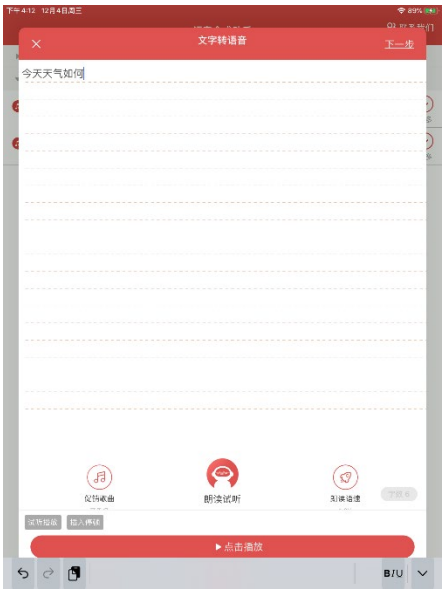
图 3 TTS APP 工具

2) 通过 3.5 公头耳机插头转 BNC 公头接口线将手机连接至信号发生器的 Modulation in 接口；
3) 调试信号发生器参数，使用外调制功能，设置为 AM 模式，输出载波为 25kHz-40kHz 正弦波，本次实验建议设置载波为 25kHz，Vpp 设置为 15V 的正弦波；
4) 使用双鳄鱼夹 BNC 连接线，将示波器 Chanel1 通道与超声波模块探头连接（注意超声波模块标记黑圈的引脚接信号发生器的正端，同时要避免两个鳄鱼夹短路，还有实验室信号发生器的 Chanel1 在右下角靠下面的接口，而不是上面的，此处很容易弄错，务必注意信号输出通道的正确连接，可通过示波器观察输出载波波形确认信号是否正确）；
5) 一位同学将超声波模块对准被攻击手机的麦克风，另外一位同学在主动攻击的手机上通过 TTS APP 软件播放攻击声音（注意：超声波模块要对准麦克风，距离不要太远，可将被攻击手机平放在桌子上以方便对焦，本次实验中，被攻击同学的手机要将相应的语音助手处于激活状态，如图 1 中要处于 Activated 的 yes 状态。同时为提高实验的成功率，建议使用 iPhone 的 Sari 或手机自带的语音助手）；
6) 在被攻击手机上观察是否成功；

五、实验结果

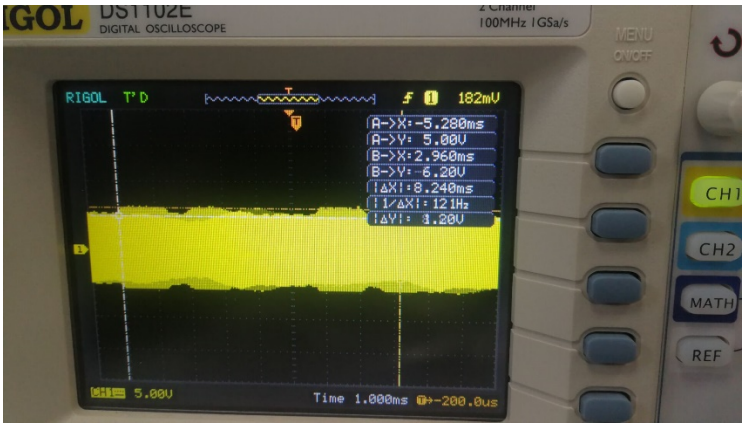
如下图，用 tts 将“今天天气如何”的指令转换为语音输出

实验名称：海豚音攻击最小系统实现 姓名：潘盛琪 学号：3170105737



观察在基带信号未输入时，示波器的波形如下图：

在播放 tts 输出的音频后，示波器的波形如下图，可以看到基带信号被成功调制



将信号发生器的鳄鱼夹接到超声波发生器，并将超声波发生器对准手机的副麦克风，将手机的语音助手唤醒后对其进行攻击，结果如下：

实验名称：海豚音攻击最小系统实现 姓名：潘盛琪 学号：3170105737

装 订 线

六、思考题

1. 结果显示示波器波形中调制波形不明显，如何使示波器波形中调制波形更明显？不限制设备器材。

- 可以增大载波幅度
- 可以增加 tts 的输出音量

2. 有些语音助手可以被攻击，有些语音助手不可以，从语音系统的组成和信号流上来看，可能的原因有哪些？如果直接录音后播放，人耳可以听清楚里面的内容吗？

可能的原因

- 首先，从输入的角度来看，可能不同的麦克风设备的线性作用不同，部分麦克风的非线性作用会导致分解出的基带信号出现混叠，导致无法识别。
- 从语音助手的原理来看，攻击部分语音助手不可以被攻击可能是由于 ai 算法的脆弱性。如我们在实验中，在保持其他条件不变的情况下，换用另一语音助手，“今天天气如何”会被识别为“嘿嘿嘿嘿嘿嘿”。

由于录音时也会经过麦克风的非线性作用，所录到的内容和语音助手所接收到的内容是一样的，都包含被还原的基带信号，因此录音后直接播放人耳也可以听清楚里面的内容，但音量会比较低。进过实验测试，结果确实如此。

3. 可能的防护方法有哪些？

- 硬件层面：在麦克风前加低通滤波器

实验名称：海豚音攻击最小系统实现 姓名：潘盛琪 学号：3170105737

- 软件层面：利用两个系数 a 相同 b 不同的麦克风，分别测试经过处理后信号，若幅值相同则未被攻击，若幅值不同则说明被攻击。

七、心得体会

本次实验实现了海豚音攻击的最小系统，虽然实验过程较为简单，通过本次实验我还是收获了不少。我最初听说海豚音攻击时，认为海豚音攻击非常高深，对于从未接触过科研的我而言无法理解。有一次突然想到为什么不直接加个滤波器就能防止了？突然又觉得好简单。当然这些都发生在上物联网安全这门课之前。上了课我才弄明白了“为什么超声波可以攻击麦克风”“为什么不能加滤波器将超声滤去”等问题。科研不像我想象的那么复杂，但科研对于“逻辑严密”有很高的要求，必须把原理弄透，实验成功率才会比较高。