# 树莓派项目（进度汇报）

－2016/7/2

## 项目简介

使用python代码编写一个可抗密钥丢失的点对点通信协议

## 已完成工作

1. 已完成点对点中的stop-wait协议实现，并针对其在windows主机进行了测试。
2. 设计并实现了基于滑动窗口下的协议状态机（GBN模式），详情见附录。
3. 针对点对点协议测试，设计并实现了netsim仿真代码。

## 下一步工作

1. 解决实现GBN时的密钥迭代问题，即若滑动窗口大小为10，而输入包量只有8，那么需要如何迭代包。＝＝＝》目前方向：查看TCP协议栈或者看一下其他的一些基于UDP实现TCP的协议是如何处理的。
2. 如何解决平滑过渡问题，具体见状态机
3. 如何在单个进程中解决收发的并行操作＝》》》基于事件编程
4. 思考在GBN协议下，包失序将会严重降低性能，我们需要如何优化。
5. 在树莓派上，进行多对多网络测试

## 项目成员与分工

由于我们现在人员都分布在不同的城市，后期我们将采取skype进行线上沟通，希望大家能在实习的空闲时间花些功夫在这个有趣的项目上。希望9月份的时候，我们能够在本项目上取得较好的进展。

下一次的项目会议暂定为7月9日。请大家在这几天完成以下任务：

李旭： 学习并测试树莓派的点对点组网通信，多对多通信。另外若还有时间，请尝试稍微看一下TCP栈的协议实现。

沈凯文：这几天抓紧看一下TCP栈实现，争取把封包问题解决好。

吴文俊：学习下当下的文档与状态机相关资料，审计与尝试优化整个项目的解决方案及对应代码。

## 项目文档目录

项目目录结构：

.

├── appRec.py 🡨--外部应用文件（接收者）

├── appSend.py 🡨--外部应用文件（发送者）

├── doc 🡨--项目文档文件夹

├── netSim.py 🡨--网络仿真测试文件

├── netsocket 🡨--项目核心代码文件夹

│   ├── Setdefault.py 🡨--恢复到默认状态

│   ├── \_\_init\_\_.py 🡨--init文件

│   ├── comlib 🡨--通用函数库

│   │   ├── Common.py 🡨--常见函数（包切分、序列迭代类）

│   │   ├── Cryption.py 🡨--加解密库

│   │   ├── File.py 🡨--文件操作函数

│   │   ├── \_\_init\_\_.py

│   ├── communication.py 🡨--定义了发送类和接受类

│   ├── file 🡨--配置与备份文件夹

│   ├── test 🡨--测试文件夹（暂时没有用到）

│   ├── test\_time.py 🡨--运行时间测试函数

├── state 🡨--状态机文件夹

│   ├── Rec.pdf 🡨--S-W下接收者状态机

│   ├── Rec2.pdf 🡨--滑动窗口接受者状态机

│   ├── send.pdf 🡨--S-W发送者状态机

│   └── send2.pdf 🡨--滑动窗口发送者状态机

└── testSnd.py 🡨--测试文件，暂时无用

使用方法

1，第一次运行时运行Setdefault.py重置文件信息。

2. 接下来，运行appRec.py 监听端口

3. 然后，运行appSend.py 发送数据

4. 若上述配置，正确就能正常运行

## 状态机

S-W下状态机：



图1:发送者状态机



图2:接受者状态机

**滑动窗口下状态机：**

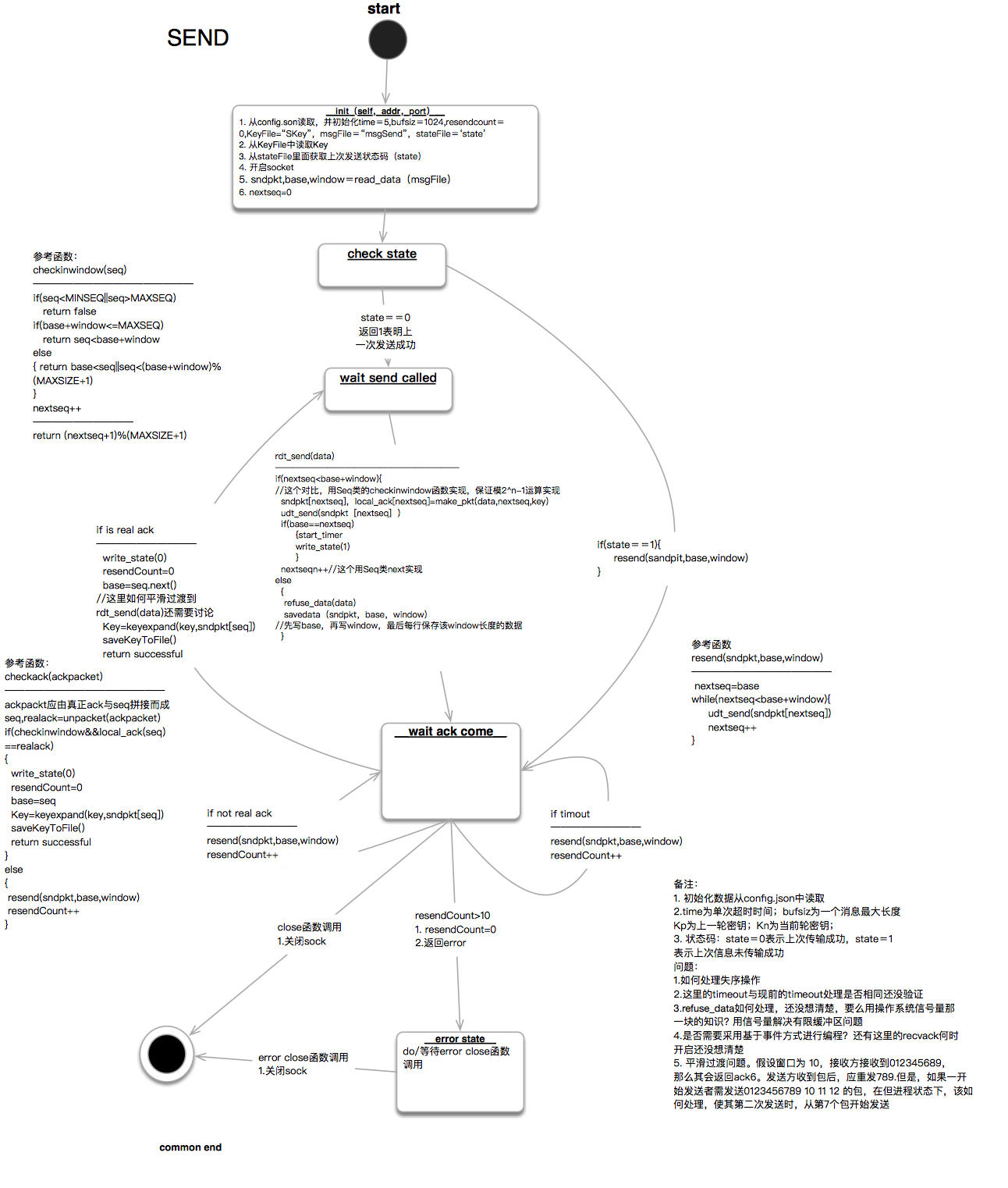
****

图1:发送者状态机

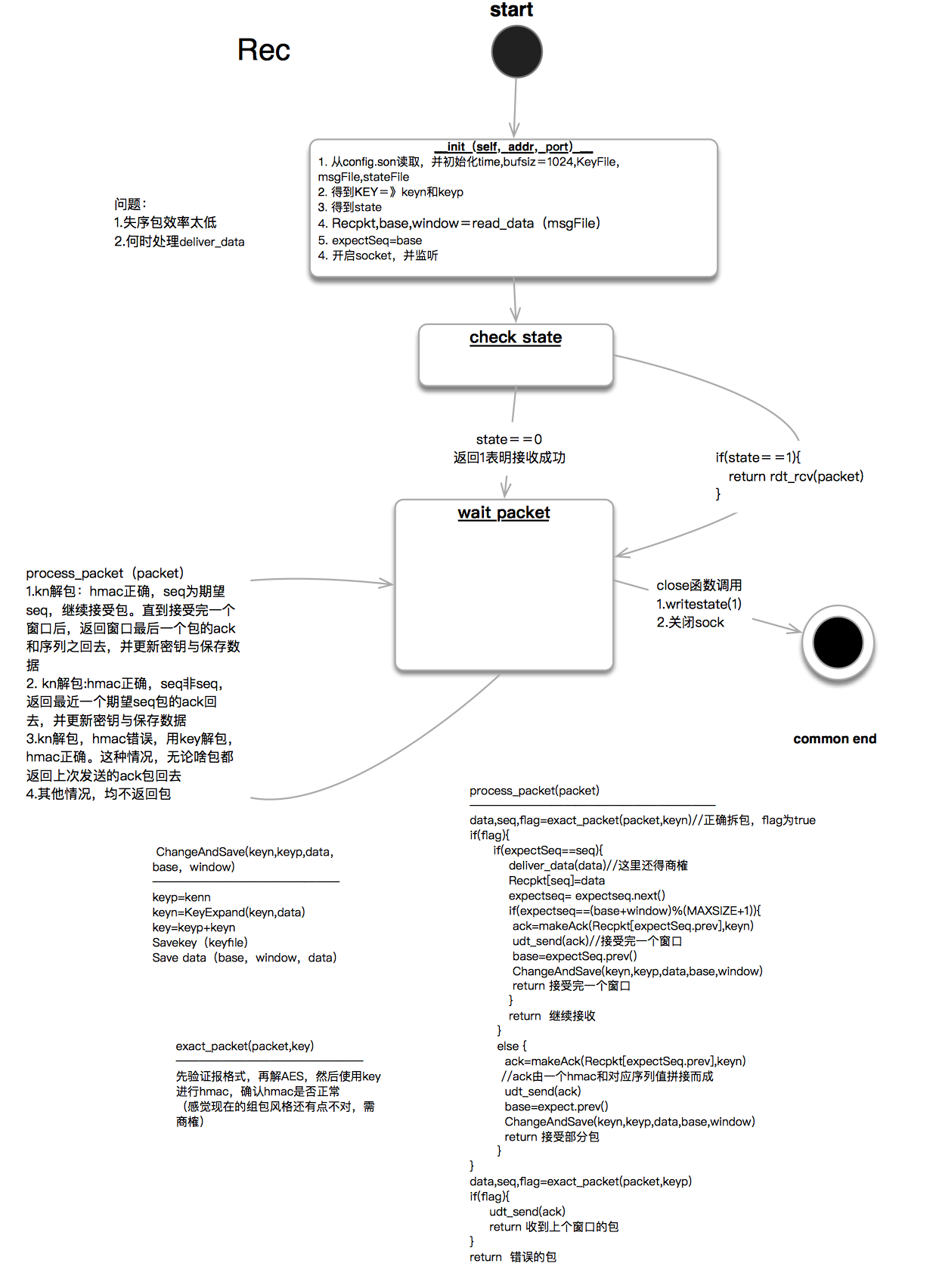
****

图2:接受者状态机

## 打包过程

第一步

message

message

Rand

Len8

Seq8

AESOUT

HMAC（32）

PACKET(992位)

包填充

AES加密

中1/3key

HAMC

前1/3key

打包

exchangge

ACK

data1

第二步

data2

HAMC

后1/3key

data3

HMAC（32）

第一步：

消息message已经打包生成data1，data1前8为储存序列seq，接下来8位储存message长度，接下来是message，最后随机填充长度为0-256位的字符串。

第二步：

AES处理date1使用中1/3key加密生成AESOUT，HMAC 处理date1使用前1/3key生成HMAC。使用AESOUT和HMAC生成date2。

使用exchangge函数处理date2，交换了date2前后部分，HMAC 处理交换后的部分得到ACK。

最后date2已经打包处理成1024的供发送的数据包date3。