物联网的家庭私有应用

摘要

物联网（Internet of Things，IOT）就是把传感器装备到电网、铁路、桥梁、隧道、公路、建筑、供水系统、大坝、油气管道以及家用电器等各种真实物体上，通过互联网联接起来，进而运行特定的程序，达到远程控制或者实现物与物的直接通信。物联网，即通过装置在各类物体上的射频识别(RFID)、传感器、二维码等，经过接口与无线网络相连，从而给物体赋予“智能”，可实现人与物体的沟通和对话，也可以实现物体与物体互相间的沟通和对话，这种将物体联接起来的网络被称为“物联网”。

物联网给我们生活带来便利，提高工作效率和生活质量。物联网是依赖于Internet网络以一种P2P的通讯方式，发送指令和信息的网络。这就需要保证网络通讯的高度安全性。在这个项目中我使用了先阶段比较常用的几个加密方式公开密钥密码体制（RSA），高级加密标准（Advanced Encryption Standard，AES）和动态口令来保证了信息的安全和真实。P2P的通讯方式要求在互联网上有唯一识别的标示（IPv6），以便控制终端能准确的定位到被控制端。物联网的家庭应用是用户利用Internet远程控制及监控家中的电器。家用电器会分布在房中的各个角落，这给指令的发送和接受带来了障碍。但只要有电器就会存在电源，就会有电力网，物联网在家中的通讯可以使用电力网通讯来解决。

关键字：通讯加密技术，IPv6，电力线通信技术

目 录

第一章 绪论1

1.1引言2

1.2物联网2

键入章标题(第 3 级)3

键入章标题(第 1 级)4

键入章标题(第 2 级)5

键入章标题(第 3 级)6

**第一章 绪论**

1.1 引言

在网络技术高速发展的今天，互联网已经与我们的生活息息相关。互联网可以给我们最新的资讯，未知的学识和实时的通讯。而物联网能给人类的生活与工作带来更高的质量和效率。如今的社会，上班族的工作压力越来越大。同时分配给自己休息和享受生活的时间逐渐减少。这些人因为工作的关系，没空自己做饭就出去吃快餐，没空洗衣服就把衣服送去洗衣房，没空打扫房间就干脆不打扫了。这样的生活应该不是每个人想要的。那么如果有一种方法可以我们只需要操纵下手机、平板电脑或是计算机，就能远程查看和控制家中的任何电器。使其在主人回家之前就已经完成了相应的工作，而不是等到主人回家。这样就能充分利用起宝贵的时间。

试想一下，如果每天出门前把淘好的米放进电饭煲，脏衣服扔进洗衣机。上班时就能利用电脑或手机监控家中的图像，操作电器开始煮饭、洗衣服、打扫卫生等。回到家后衣服已经洗干净, 热腾腾香喷喷的米饭已经煮好，还有打扫干净的屋子。我们就有跟过的时间来休息，学习和陪伴家人。如果再公司突然发现有重要的文件落在家中的电脑里，也可以使用物联网远程启动并操纵家中的电脑读取文件。

我曾经玩过一个非常热门的网络游戏（魔兽世界）。因为当时玩这款游戏的人太多，游戏服务器承受不了这么多人数的压力。所以玩这款游戏好需要排队，每次排队没有个把小时是进不去游戏的。我每次回家总需要等很长一段时间玩上这个游戏。当时我想，如果有一个工具能让我远程控制家中的电脑提早开始游戏排队就好了。从此我就产生了制作这个项目的想法。

1.2 物联网介绍

物联网是新一代信息技术的重要组成部分。其英文名称是“The Internet of things”。由此，顾名思义，“物联网就是物物相连的互联网”。这有两层意思：第一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；第二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信。因此，物联网的定义是通过射频识别（RFID）、红外感应器、全球定位系统、激光扫描器等信息传感设备，按约定的协议，把任何物品与互联网相连接，进行信息交换和通信，以实现对物品的智能化识别、定位、跟踪、监控和管理的一种网络。物联网存在以下结果特征：

首先，物联网的每个终端有多存在侦测其状态的传感器。用户可以用控制端查看被控终端的状态信息。

其次，物联网是依托于互联网的特殊网络通讯。控制终端的信息会在互联网上海量的传输。这就要求网络信息的准确性和及时性。

还有，物联网不但存在状态检测的功能，还需要与智能操控相结合。利用云计算机，模式识别等技术。对用户的操作进行正确的响应和执行。

“物”的涵义：

有数据传输通路

有数据存储功能

有中央处理器（CPU）

有操作系统

有专门的引用程序

遵循物联网的通讯协议

在世界网络中又可被唯一识别的编号

1.2 物联网历史

1. 1990年，施乐公司（xerox）使用了第一台网络可乐贩售机——Networked Coke Machine。
2. 1999年，美国召开的移动计算和网络国际会议上由MIT Auto-ID中心的Ashton教授首先提出物联网这个概念。
3. 2003年，美国的《技术评论》提出传感网络技术将是未来改变人们生活的十大技术之首。
4. 2005年，在突尼斯的信息社会世界峰会（WSIS）上，国际电信联盟（ITU）发布《ITU互联网报告2005：物联网》，指出物联网的覆盖范围正逐渐扩大。
5. 2008年，在中国北京大学举行的第二届中国移动政务研讨会“知识社会与创新2.0”提出移动技术、物联网技术的发展代表着新一代信息技术的形成。
6. 2009年，2009IBM论坛上，IBM大中华区CEO钱大群，公布了名为“智慧的地球”的最新策略。同年温家宝总理在视察中科院无锡物联网产业研究所时，对于物联网应用也提出了一些看法和要求。自温总理提出“感知中国”以来，物联网被正式列为国家五大新兴战略性产业之一，写入“政府工作报告”。

1.3 物联网发展优势

同时，一些其他技术的成熟也促进了物联网的发展。

1.3.1 IPv6的推广

物联网的“物”的涵义中，“在互联网中有唯一识别的编号”是物的特征之一。这个值得就是IP地址。现阶段IPv4的数量已开始满足不了迅猛发展的互联网的需求。IPv4由4组0～255的数字组成，也就是2的32次方个IP地址，约42亿个IP地址。1999年全球人数已经达到了60亿，平均下来每个人连一个IP地址都拿不到。为了解决IP地址不足的问题，IPv6诞生了。

IPv6(Internet Protocol Version 6)是用来替换IPv4的新的互联网协议。IPv6由8组16进制数组成，每组两字节。这样IPv6的地址空间就有了2的128次方，相当于42沟（东汉时代《数术记遗》中记载，表示10的32次方的数词）个IP地址。如果充分的使用IP地址，那么地球上的每一粒沙子都可以被分配到一个IPv6的地址。

1.3.2 射频识别RFID

射频识别即RFID（Radio Frequency IDentification）技术，又称电子标签、无线射频识别，是一种通信技术，可通过无线电讯号识别特定目标并读写相关数据，而无需识别系统与特定目标之间建立机械或光学接触。常用的有低频（125k~134.2K）、高频（13.56Mhz）、超高频，无源等技术。RFID读写器也分移动式的和固定式的，目前RFID技术应用很广，如：图书馆，门禁系统，食品安全溯源等。

1.3.3 电力线通信技术

电力线通信技术（Power Line Communication）简称PLC，是利用电力线传输数据和话音信号的一种通信方式。该技术是把载有信息的高频信号加载于电流，然后用电线传输，接受信息的调制解调器再把高频从电流中分离出来，并传送到计算机或电话，以实现信息传递。目前在多种场合使用的低速（1200bps以下）电力载波已很普遍。利用输电线路作为信号的传输媒介，人们利用电力线可以传输电话、电报、远动、数据和远方保护信号等。由于电力线机械强度高，可靠性好，不需要线路的基础建设投资和日常的维护费用，因此PLC具有较高的经济性和可靠性，在电力系统的调度通信、生产指挥、行政业务通信以及各种信息传输方面发挥了重要作用。

**第二章 项目介绍**

2.1项目结构

这个项目是物联网在家庭中的私有应用。功能是在互联网中使用控制终端（手机或电脑）监控和启动家中的电脑。

项目分为以下几部分：

2.1.1 密钥生成者

密钥生成者有Visual Basic .NET编写，其工作前，用户必须告知密钥的有效期限和一个Visual Basic的项目工具（devenv.exe）路径。执行生成操作以后产生3个文件：Generate.log密钥日志文件，记录此次生成的创建时间，密钥生效时间和密钥失效时间；Key文件，是提供给服务器查询的口令库；Key.exe文件，是提供给用户查询口令的工具。口令库由N组6位数字组成，每组密钥有效时间两分钟。当控制终端与物联网服务器连接时，核对动态口令以确保操作权限。

2.1.2 物联网服务器

2.1.3 便携控制端

2.2通讯流程

2,3模块详细介绍

2.3.1 Database数据库模块

2.3.2 Logger日志记录者模块

2.3.3 Terminal Manager终端管理者模块

2.3.4 Packager打包者模块

数据包头结构：

1.包长2Byte

2.识别码2Byte

3.指令码2Byte

4.包编号2Byte

流量计算：

1.公钥包结构 0x0001

-IP头(20B)/TCP头(20B)/TCP内容(160B)

2.口令包结构 0x0002

-IP头(20B)/TCP头(20B)/TCP内容(12B)

3.普通回应包结构 0x0003

-IP头(20B)/TCP头(20B)/TCP内容(8B)

4.连接断开包结构 0x0004

-IP头(20B)/TCP头(20B)/TCP内容(8B)

5.远程唤醒或关闭数据包结构 0x0005

-IP头(20B)/TCP头(20B)/TCP内容(9B)

-中国移动5元/月，30MB=31457280B

-远程唤醒数据包，49B

-GPRS 5元套餐可以远程唤醒641985次。平均每次唤醒花费0.008厘钱。每天可以唤醒或关闭电脑21399次。

6.状态查看数据包结构(详细) 0x0006

-IP头(20B)/TCP头(20B)/TCP内容(n\*4B)

7.状态查看数据包结构 0x0007

-IP头(20B)/TCP头(20B)/TCP内容(nB)

2.3.5 Listener监听者模块

2.3.6 Securer守护者模块

1.RSA

密钥生成：由Crypto.PublicKey.RSA函数完成

密钥空间： 私钥 256607= 607字节

公钥 256162= 162字节

2.aes

密钥生成：随机数装换得到（用struct.pack转成字符串）

密钥空间： AES key 25616= 16字节

IV（随机生成） 25616= 16字节

3.my key

密钥生成：AuthManager工程生成

密钥空间：106（密码生命周期：2分钟）

加密知识：

1.非对称密钥是用来换取一个对称密钥的

2.公钥加密，私钥解密；私钥加密，公钥解密（检查回包的正确性，以确定回包的是私钥持有者）

加密协商步骤描述：

-socket连接ServiceCenter,ServiceCenter生成公私密钥，将公钥发送给手机终端（之后称“公钥持有者”）。则ServiceCenter持有私钥（之后称“私钥持有者”）  
-公钥持有者生成超长密钥（在一段时间内无法用穷举法算出）作为对称密钥，外加动态口令用公钥加密后发送给私钥持有者。

-私钥持有者用私钥解密后验证动态口令的真确性，来确定对称密钥的可信性。私钥持有者用私钥加密返回确认对称密钥信息发送至公钥持有者。

-公钥持有者收到对称密钥确认消息后，用对称密码对数据包加密。

注意：其中任何一步出现问题一律断开socket重新协商

疑问：

为什么要用对称密钥加密？

1.对称密钥加密后网络第三方攻击者就无法得知用户进行的操作

2.动态口令过短，且全为数字，非常容易被破解。所以需要使用对称密钥在增加密钥空间。

为什么要用非对称密钥来换取对称密钥？

-非对称密钥，存在公钥这一特性。公钥即公开，谁都可以得掉。且谁都可以伪造数据包。

如果用公钥加密对称密钥：

1.只有私钥持有者才能得知对称密钥

2.只要设计足够长的对称密钥，使用穷举法是无法在短时间内破解对称密钥

3.对称密钥只会在网络上传输一次

既然有了公钥和私钥，为什么还要用动态口令？

-动态口令是用来判断，是否有权限设定对称密钥的。

参考文献

[1] [http://zh.wikipedia.org/](http://zh.wikipedia.org/wiki/%E7%89%A9%E8%81%94%E7%BD%91) 维基百科 2012

[2] [http://baike.baidu.com/](http://baike.baidu.com/view/1136308.htm) 百度百科 2012

[3]

开发内容：

1.路由器运行python服务（曾经开发过类似的程序，但没有试过在路由上执行）

市面上有些路由器经过破解后可以执行python脚本，但是这个python解释器是不是可以执行所有的python函数，需要验证。

备用方案：如果路由器上的python解释器无法执行我编写的python服务，我直接用家中废弃的主机作为家庭网关。网关上装完整的linux系统。

2.手机控制端（没有接触过objective-c，但现学应该不麻烦）

用objective-c开发一个简单的手机控制端，使用socket通讯

备用方案：架设web服务，手机用web形式访问路由

3.手机控制端与路由服务端的通讯加密

打算使用动态令牌的加密手段，然后给每个数据包添加信息摘要（md5）验证

论文提纲：

1.为什么要建立物联网

a.概念介绍

b.历史

c.优势（IPv6推广，RFID，电力线网络的成熟）

2.项目技术介绍

a.路由部分

b.手机终端部分

c.通讯加密部分

3.项目计划（只是计划部分，论文中只是提出概念，不予实现）

a.控制除电脑以外的其他电器，从电器的开关电源开始。（因为牵涉到硬件论文中只是提出一个概念）

b.从开关电源开始，慢慢与家电厂商合作。拓展对家电控制的功能。

c.对路由的功能进行拓展，使路由成为下载服务器（外挂硬盘），打印机服务器，文件管理服务器等等。

d.对硬件外观进行美化，对用户体验进行改良。这样可以卖硬件卖服务。