ISSN 1006－7167
CN 31－1707/T

实验室研究与探索
RESEARCH AND EXPLORATION IN LABORATORY

第41卷 第4期 2022年4月
Vol. 41 No. 4 Apr. 2022

DOI: 10.19927/j.cnki.syyt.2022.04.006

一种无线组网智能家居系统的安全通信方法

王海珍[a]， 廉佐政[a]， 谷文成[b]， 李梦歌[a]
(齐齐哈尔大学 a. 计算机与控制工程学院，b. 网络信息中心，黑龙江 齐齐哈尔 161006)

摘 要: 智能家居面临日益严重的数据安全问题，提出一种无线组网智能家居系统及其安全通信方法，即设计组网方案，采用 WiFi 和 ZigBee 无线技术通信。家居设备节点采用 ZigBee 通信方式，其他设备采用 WiFi 通信方式。结合 MQTT 协议设计安全通信方案，路由器部署为 MQTT 服务器，并进行安全配置; 家居控制设备为 MQTT 客户端，使外网中的控制设备可以采用安全内网穿透方案 ZeroTier 访问内网。同时，提出基于 L-P 混沌系统交叉扩散方法产生 AES 初始轮密钥，并用于 ZigBee 安全通信。实验结果与分析显示，所提通信方法安全，与标准 AES 算法相比，运行时间相似，分别为 0.628、0.633 s 本文方法所需时间更短，具有可用性。

关键词: 无线组网; 智能家居; WiFi 通信方式; ZigBee 通信方式; MQTT 协议; 混沌系统
中图分类号: TP 393.1 **文献标志码:** A **文章编号:** 1006－7167(2022)04－0026－05

A Secure Communication Method for Smart Home System Based on Wireless Networking

WANG Haizhen[a], *LIAN Zuozheng*[a], *GU Wencheng*[b], *LI Mengge*[a]
(a. College of Computer and Control Engineering; b. Network Information Center, Qiqihar University, Qiqihar 161006, Heilongjiang, China)

Abstract: For the increasingly serious data security problems faced by smart home, a wireless networking smart home system and its secure communication method are proposed. Firstly, the networking scheme is designed, based on WiFi and ZigBee wireless technologies, mainly. Among them, the home device nodes adopt ZigBee communication mode, and other devices adopt WiFi communication mode. Then combined with MQTT protocol, a secure communication scheme is designed. The router is deployed as an MQTT server and configured for security. The home control devices are as MQTT clients, so that the control devices in the external network can access the internal network using the secure internal network penetration scheme of ZeroTier. At the same time, the cross diffusions method based on L-P chaotic system is proposed to generate AES initial round key, and achieve ZigBee secure communication. The experimental results and analysis show that the proposed communication method is secure, and compared with the standard AES algorithm, the running time is similar, which is 0.628 s and 0.633 s respectively. The method in this paper Costs less running time, so it is available.

Key words: wireless networking; smart home; WiFi communication mode; ZigBee communication mode; message queuing telemetry transport (MQTT) protocol; chaotic system

收稿日期: 2021-07-26
基金项目: 黑龙江省省属高等学校基本科研业务费科研项目(135209245); 黑龙江省高等教育教学改革研究项目(SJGY20200770, SJGY20190710); 黑龙江省省属高等学校基本科研业务费科研创新平台项目(135409421)

作者简介: 王海珍(1976－)，女，山东临沂人，硕士，副教授，主要研究方向为嵌入式技术、密码分析与设计、网络安全。
Tel.: 13384626702; E-mail: wanghaizhen1976@163.com

0　引　言

基于无线组网方案的智能家居系统,安装、扩展方便,使人们生活更加舒适和智能。大容量、低功耗、低成本是智能家居重要需求[1],Zigbee 技术最多可组成 65 000个节点的网络[2],网络中的节点使用 2 节干电池可支持一个节点工作 6 ~ 24 个月,Zigbee 技术免协议专利费、芯片价格低[3],能够较好满足无线智能家居的应用场景[4]。消息队列遥测传输协议(Message Queuing Telemetry Transport,MQTT)作为一种低开销[5]、低带宽的即时通信协议[6],可为远程设备提供实时可靠的消息服务[7],为实现智能家居设备的远程控制提供了方便[8]。

伴随通信技术引入系统,智能家居也遭到大量网络威胁[9],用户信息在传输过程中容易被窃取、篡改[10],甚至被攻击。现迫切需要解决数据在传输过程中的安全问题[11]。文献[12]中提出物联网智能家居安全设计的必要性,分析了设计过程中存在的问题,如安全标准不统一、没有专门的安全预警机制等。文献[13]中依据智能家居系统的安全需求,采用 SM4 对称密码算法,对传输的数据与接入认证信息进行加密,保证组网内的信息安全传输,但未实现移动端控制。文献[14]中对家居控制用户进行身份认证,并采用标准的 AES 算法对控制指令进行加密,提高了智能家居系统的安全,但系统的稳定性有待提升。综上所述,现阶段智能家居行业标准还不统一,系统资源有限,对复杂运算的处理能力不足,研究一种无线组网智能家居系统的安全方案,尤其重要。本文提出一种新的智能家居系统的无线组网方案,并研究了系统的安全通信方法。

1　系统安全通信方法

1.1　系统组网方案

系统组网方案如图 1 所示,包括内网和外网,内网便于用户在家控制家居设备,外网用于实现远程控制。

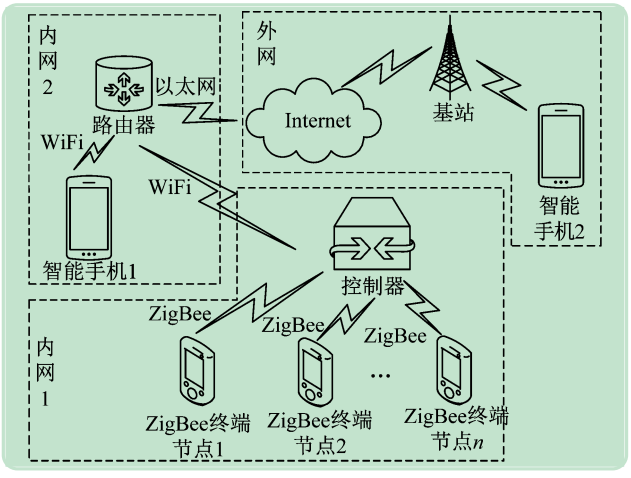

图 1　系统组网方案

内网包括 2 部分,一部分实现家居信息采集、传输,该部分数据量小、传输距离短、节点多,采用 ZigBee 协议通信方式; 另一部分通过 WiFi 通信。外网采用安全的内网穿透方案 ZeroTier[15],并使用 MQTT 协议进行远程控制。路由器作为 MQTT 服务器,智能手机和控制器作为 MQTT 客户端,内网 1 的控制器作为协调器,它和 ZigBee 终端节点都称为 ZigBee 节点,它们组成 ZigBee 网络。ZigBee 终端节点数量可以依据采集信息情况确定,通过传感器采集室内的温度、光照等信息,并通过 ZigBee 协议发送给控制器,控制器通过 WiFi 发送给 MQTT 服务器。智能手机是控制端,可以通过 APP 发送控制信息给 MQTT 服务器,MQTT 服务器再发送给控制器,控制器依据接收的控制信息,控制家居设备,如开启或关闭窗帘、开/关电灯等。由图 1 可知,系统的通信主要包括 MQTT 客户端和服务器之间的通信,ZigBee 网络的通信。

1.2　MQTT 客户端和服务器之间的安全通信方法

本节的安全通信方法如下: MQTT 客户端通过用户名和密码登陆服务器,MQTT 服务器启用 SSL 安全连接,处于外网的智能手机 2 使用内网穿透方案 ZeroTier 与服务器组建虚拟局域网,实现加密的 P2P 安全通信。

(1) 方案设计。设计 MQTT 客户端和服务器的安全通信方案,如图 2 所示。

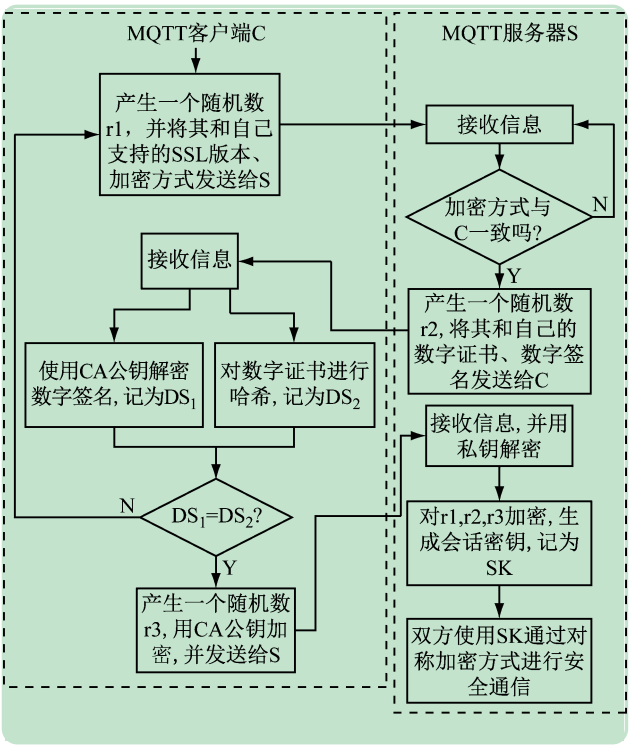

图 2　MQTT 客户端与服务器的安全通信方案

(2) 平台构建。路由器上刷 OpenWrt 系统,安装 MQTT 服务器 mosquitto 软件,设置客户端用户名、密

码，配置 SSL，实现 MQTT 客户端和服务器的安全通信，搭建 ZeroTier 网络，安装 ZeroTier 客户端软件，实现外网智能手机安全访问内网 1 的控制器。主要步骤。

步骤 1 路由器刷 OpenWrt 系统（以 wnr2000v4 型号的路由器为例）。

刷入与路由器型号对应的固件；

在 PC 机上下载路由器型号对应的 Uboot 和 Openwrt（15.05 版本）；

PC 机上要搭建 TFTP 服务器，将 Uboot 和 Openwrt 下载到路由器；

路由器分别刷入 Uboot、OpenWrt 系统。

步骤 2 服务器 mosquito 软件安装及配置。

将路由器连到 Internet，在 PC 机的命令行窗口输入 telnet 命令，telnet 到路由器，然后输入命令：opkg install mosquito，安装 Mosquitto 服务器；

配置 MQTT 客户端登陆的用户名和密码，修改 mosquitto.conf 配置文件内容，不允许匿名用户登录，使用密码文件 password_file、访问权限列表文件 acl_file。

```
allow_anonymous false
password_file /etc/mosquito/pwfile
acl_file /etc/mosquittto/aclfile
```

添加用户名和密码

为 MQTT 客户端智能手机和控制器分别配置用户名和密码，设它们的用户名、密码都为 supass，则配置用户名的命令：

```
mosquito_passwd -c /etc/mosquito/pwfile supass
```

按提示输入密码。

添加用户的主题控制权限

在/etc/mosquito/目录下，新建一个文件 aclfile，添加命令，指定所有 MQTT 用户对所有主题都有读、写权限，以便订阅或发布家居系统的信息。

步骤 3 配置通过 ssl 通信。

安装 openssl；

产生证书文件。

① 产生 CA 的公钥和证书文件

```
openssl req -new -x509 -days 36500 -extensions v3_ca -keyout ca.key -out ca.crt
```

② 为 MQTT 服务器产生一个私钥文件 server.key，并设置加密方式

```
openssl genrsa -out server.key 2048
openssl genrsa -des3 -out server.key 2048
```

③ 为 MQTT 服务器产生一个签发证书的请求文件“server.csr”

```
openssl req -out server.csr -key server.key -new
```

④ 为 mosquitto server 产生一个证书文件

```
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt -days 36500
```

⑤ 重复②～④，为 3 个 MQTT 客户端生成证书文件。

步骤 4 搭建 ZeroTier 网络并测试。

在 ZeroTier 官网注册账号；

分别下载 OpenWrt 系统、智能手机操作系统对应的 ZeroTier 客户端软件版本，并进行安装；

使用在 ZeroTier 官网注册的账号，登录个人账号工作面板，创建网络 ID；

在路由器和智能手机上运行 ZeroTier 客户端软件，加入创建好的网络 ID；

在工作面板上授权各客户端的连接，分配虚拟局域网 IP 地址；

网络连通测试。在路由器上 ping 智能手机 IPv4 地址，若建立起了 P2P 通道，则可以 PING 通。

（3）实现过程。智能手机和控制器都是 MQTT 客户端，且智能手机是控制端，它们之间通过路由器实现通信，智能手机和控制器都需要设计 MQTT 客户端程序。依据 1.2 节通信方案，采用 Android Studio，为 Android 系统的智能手机，设计 MQTT 客户端程序，采用 Arduino 开发环境设计控制器的 MQTT 客户端程序[16]。智能手机 2 采用 ZeroTier 技术分配的虚拟局域网 IP 地址，进行网络连通后，从手机 APP 发布的 MQTT 消息内网穿透后，直接以 P2P 方式传到路由器，路由器上 MQTT 服务器收到这个消息后，转发给控制器，以便控制内网 1 中的 ZigBee 终端节点。

1.3 ZigBee 网络的安全通信方法

依据 1.1 节，控制器和 ZigBee 终端节点组成以协调器为核心的星型网络，通过改进的 Z-Stack 协议栈 AES 加密算法实现它们之间的安全通信。Z-Stack 协议栈中文件 nwk_global.c 定义了默认的初始轮密钥，所有 ZigBee 节点开启 AES 加密算法后，可以设置协调器节点向各个节点发送初始轮密钥，它们之间通过 AES 加密算法通信，提高安全性。但是 AES 加密算法的初始轮密钥不具有随机性，容易破解，因此，本节提出 AES 初始轮密钥的产生方法，如图 3 所示，初始轮密钥由控制器产生，每间隔一定时间，或重启后轮密钥重新设置，由 Logistic、PWLCM 混沌映射交叉扩散生成，为了保证密钥的随机性，Logistic 混沌映射、PWLCM 混沌映射分别迭代若干次。控制器产生轮密钥后，将其通过 MD5 函数生成数字签名，并将轮密钥及其数字签名发送给其它所有 Zigbee 节点，ZigBee 节点接收后，进行数字签名验证，验证无误后，便可将轮密钥作为初始轮密钥进行 AES 加密或解密。其中，初始轮密钥产生的主要步骤如下。

步骤 1 设置混沌系统的参数。

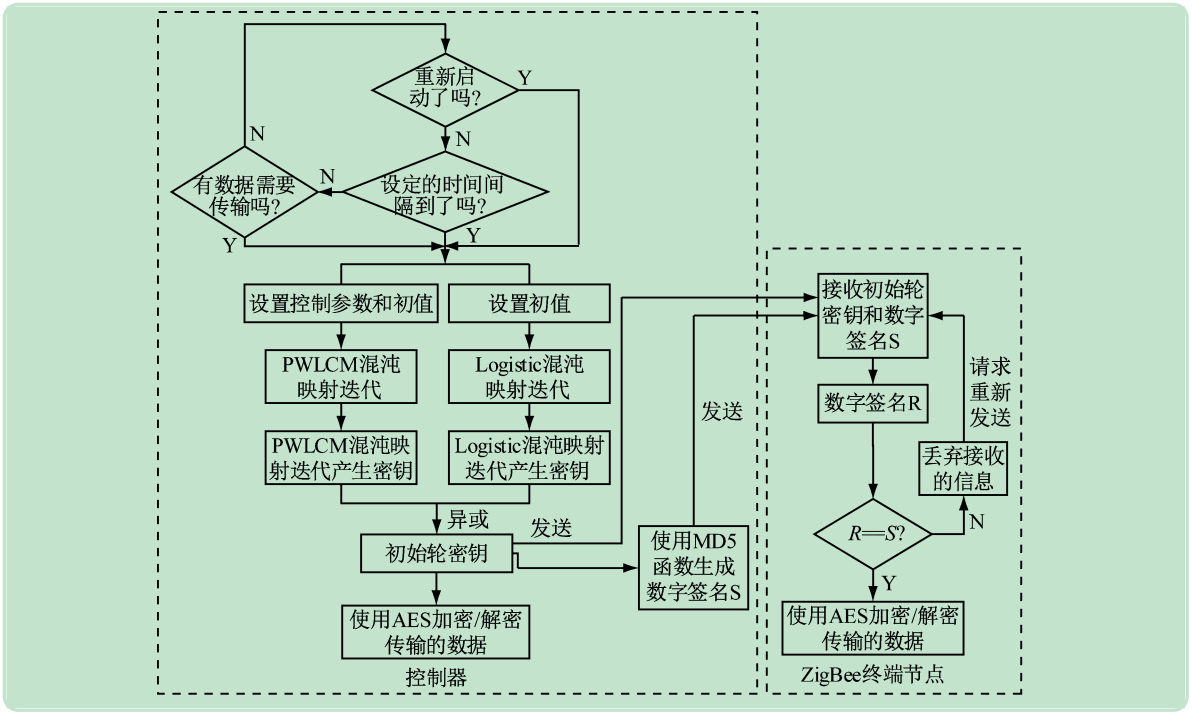

图 3　AES 初始轮密钥产生方法

随机产生一个取值范围为(3.569 945 6,4]的数作为 Logistic 混沌系统的控制参数 μ;

随机产生一个取值范围(0,0.5]之间的数作为 PWLCM 混沌系统的控制参数;

产生两个取值范围为(0,1)之间的随机数,key0、key1,分别作为 Logistic 混沌系统、PWLCM 混沌系统迭代的初值。

步骤 2　混沌系统迭代至混沌状态。

Logistic 混沌系统按步骤 1 设置的参数分别迭代 100 次,消除暂态的影响,处于混沌状态。

步骤 3　产生 AES 初始轮密钥。

在前面 Logistic 混沌映射迭代基础上,再迭代 16 次,将这 16 次 Logistic 映射迭代产生的结果分别保存在 PWLCM(i)中,其中 $i=1,2,\cdots,16$;

在前面 PWLCM 混沌映射迭代基础,再迭代 16 次,将这 16 次 PWLCM 映射迭代产生的结果分别保存在 Logistic(i)中,其中 $i=1,2,\cdots,16$;

将 PWLCM(i)、Logistic(i)转换成整数序列,即乘以 10^8,并对 256 取余;

将整数序列 $y\_PWLCM(i)$、$y\_PLogistic(i)$ 分别转换成 4×4 矩阵 p_mat、l_mat,然后将两个矩阵对应元素进行异或,作为 *AES* 加密的初始轮密钥。

2　实验结果与分析

2.1　MQTT 客户端程序设计

以 Android 手机为例说明 MQTT 客户端程序的设计。在 Windows 环境下构建 Android Studio 软件开发环境,即安装 Java 开发工具包 JDK1.8;配置 JDK 环境变量;安装 Java 集成开发环境 eclipse;安装 Android SDK;为 eclipse 安装 ADT 插件。在 Android Studio 开发环境下设计程序,该程序主要包括登录模块和主界面,实现家居系统中的环境参数信息和非法入侵监测信息的查看,或者向家居系统发送控制指令。登录模块的功能是建立用户和服务器的 SSL 连接,如果连接成功,跳转到客户端主界面;否则返回登录失败信息。主界面如图 4 所示。

图 4　MQTT 客户端程序主界面

2.2　改进的 AES 算法实验结果与分析

采用的实验环境:内存 8 GB,处理器 i7-6700HQ,CPU2.6 GHz,操作系统 Windows 10,仿真软件为 Matlab R2014a。使用标准 AES 算法默认密钥加密解密运行结果如图 5 所示,本文算法产生初始密钥的运

行结果如图6所示。

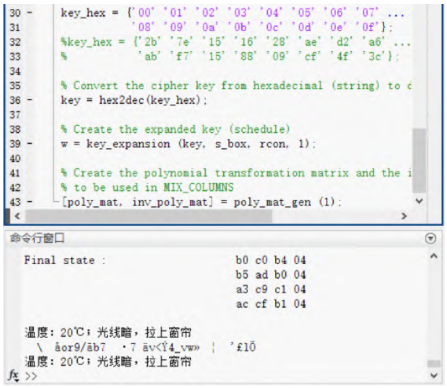

图5 使用标准AES算法默认密钥加密解密运行结果

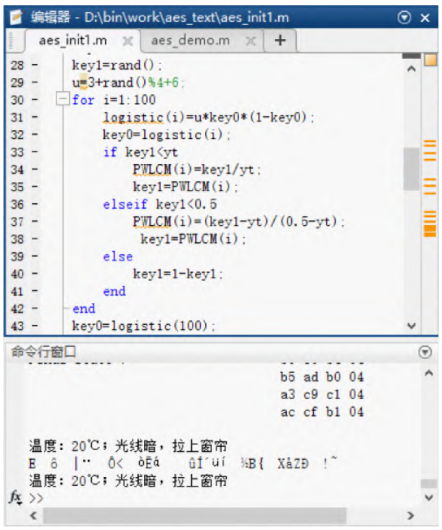

图6 使用本文算法的密钥加密解密运行结果

图5、6中命令窗口最后3行为处理的数据，其中第1行“温度:20 ℃;光线暗,拉上窗帘”为传输的原始数据，第2行为加密后的数据，第3行为解密后的数据。对比2种算法的运行时间，都在0.63 s左右，而本文算法加密时间较短，见表1。

表1 算法运行时间对比

算法	加密时间/s
标准AES	0.628 0
本文算法	0.633 0

3 结 语

针对智能家居面临的数据安全问题，本文提出一种无线组网的智能家居系统，采用WiFi和ZigBee无线技术通信，将路由器部署为MQTT服务器，路由器上配置安全方案，实现MQTT客户端和服务器之间的安全通信，成本低、安全性好。同时基于ZigBee芯片设计的家居设备节点之间通过ZigBee技术进行通信，为了保证其安全性，启用Z-Stack协议栈的AES加密算法，并基于Logistic混沌系统和PWLCM混沌系统进行交叉扩散，产生AES初始轮密钥，改善AES算法的安全性，经过实验分析，相对标准AES算法，改进的加密算法运行时间较短，有可应用性。

参考文献(References):

[1] 鲁玉军，刘 振. ZigBee技术在智能家居系统中的应用[J]. 物联网技术，2017，7(4):40-43.
[2] 闫亚玲，李 博，刘伟杰. 基于ZigBee的实验室防火远程监控系统设计[J]. 实验室研究与探索，2019，38(5):282-285.
[3] 杨蒲菊. 基于ZigBee技术的智能家居系统设计与应用研究[J]. 电脑知识与技术，2019，15(9):96-97.
[4] Jose A C，Malekian R. Improving smart home security: Integrating logical sensing into smart home[J]. IEEE Sensors Journal，2017，17(13):4269-4286.
[5] 卢阿丽，顾德林，张剑书，等. 基于MQTT和ILZ4压缩法的智慧能源云平台[J]. 控制工程，2020，181(1):176-183.
[6] 陈文艺，高 婧，杨 辉. 基于MQTT协议的物联网通信系统设计与实现[J]. 西安邮电大学学报，2020,25(3):30-36.
[7] 李 洋. 基于消息队列遥测传输协议的智能家居消息中间件设计[J]. 计算机应用，2018，38(z1): 162-164,217.
[8] 袁青杰. 智能家居系统扩展及应用服务的技术研究[D]. 西安:西安电子科技大学,2018.
[9] 黄文锋. 基于智能家居的物联网感知层安全威胁及关键技术分析[J]. 西安文理学院学报:自然科学版，2021,24(1):59-64.
[10] 王顺业，杜彦辉，芦天亮. 面向智能家居的音视频文件安全传输方法研究[J]. 现代电子技术，2020，43(12):182-186.
[11] 肖 起. 面向智能家居的物联网隐私保护方法研究与实现[D]. 北京:北京工业大学,2017.
[12] 冯晓林，赵彦乔. 物联网智能家居安全性设计[J]. 智能城市应用，2020，3(3):56-57.
[13] 王亚超. 基于WSN的智能家居系统关键技术研究[D]. 哈尔滨:黑龙江大学，2020.
[14] 江治国. 混沌加密算法在智能家居通信安全系统中的应用[J]. 电脑知识与技术,2018，14(11):42-43,53.
[15] 钱 立. 一种内网穿透控制智能家居设备的方案[J]. 现代信息科技，2020，4(18):169-171.
[16] Saraswathi E，Kumar A，Singh J，*et al*. Arduino based home automation system using MQTT protocol incorporating internet of things (IOT)[J]. Journal of Network Communications and Emerging Technologies (JNCET)，2018，8(5):24-26.