DOI:10.19651/j.cnki.emt.2107058

基于ZigBee的智能家居系统安全通信研究*

王海珍[1] 廉佐政[1] 谷文成[2] 崔志青[1]
(1.齐齐哈尔大学 计算机与控制工程学院 齐齐哈尔 161006;2.齐齐哈尔大学 网络信息中心 齐齐哈尔 161006)

摘 要: 目前基于无线技术的智能家居系统给人们带来了舒适和便利,但系统容易遭受攻击,有较多的隐私数据需要保护。针对无线通信中数据安全问题,设计了一种智能家居系统及其安全通信方法,即设计了系统的组网结构,规划了外网和内网。内网的家居设备节点采集信息并采用ZigBee通信方式,其他设备采用WiFi通信方式。路由器部署为MQTT服务器、手机等控制设备为MQTT客户端,并在服务器上进行SSL通信相关的配置、设计客户端程序。每次外部网络的MQTT客户端访问服务器时,先采用安全的内网穿透方案ZeroTier连接到内部网络,再通过SSL协议产生公钥和证书,进行安全通信。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。实验结果为外网MQTT客户端和服务器可以连接到一个ZeroTier网络,并通过SSL协议安全通信;ZigBee通信方式达到了加密效果,相对标准AES算法,加密时间短、平均端到端通信延迟小,分别降低了3.77%和28.5%,且能量消耗少,节点平均剩余能量提高了30.22%。因此,实验结果表明,所提出的通信方法安全,且具有应用性。

关键词: 智能家居;WiFi通信方式;ZigBee通信方式;MQTT服务器;混沌系统
中图分类号: TP393 **文献标识码:** A **国家标准学科分类代码:** 520.6050

Research on the secure communication of smart home system based on ZigBee

Wang Haizhen[1] Lian Zuozheng[1] Gu Wencheng[2] Cui Zhiqing[1]
(1. College of Computer and Control Engineering, Qiqihar University, Qiqihar 161006, China;
2. Network Information Center, Qiqihar University, Qiqihar 161006, China)

Abstract: At present, the smart home system based on wireless technology has brought comfort and convenience to people, but the system is vulnerable to attack, and there are more private data to be protected. For the data security problem in wireless communication, a kind of smart home system and its secure communication method is designed, namely, the networking structure of the system is designed, external network and internal network are planned. The home device nodes in internal collect information and apply ZigBee to communicate mode, while other devices apply WiFi to communicate. The router is deployed as MQTT server, mobile phones and other control devices are MQTT clients, and SSL communication is configured on server, client program is designed. While the MQTT client in the external network accesses the server, it uses first secure intranet penetration scheme of ZeroTier to connect to the internal network, and then generates public keys and certificates by SSL protocol for secure communication. The cross diffusions method of L-P chaotic system is proposed to generate AES initial round key, and applied to ZigBee secure communication. The experimental results are that MQTT client in internet and server can connect to a ZeroTier network and communicate securely through SSL protocol can communicate securely. ZigBee communication mode achieves the encryption effect, compared with the standard AES algorithm, it is shorter encryption time and shorter communication delay, which are reduced by 3.77%, and 28.5% respectively, and less energy consumption, the average residual energy of nodes is increased by 30.22%. Therefore, the experimental results show that the communication method proposed is secure and applicable.

Keywords: smart home; WiFi communication; ZigBee communication; message queuing telemetry transport server; chaotic system

0 引 言

基于无线组网的智能家居系统,便于安装、扩展,使人们生活更加便利和智能。大容量、低功耗、低成本是智能家居的重要需求[1],ZigBee技术最多可组成65 000个节点的网络,节点使用两节干电池可工作0.5~2年,ZigBee芯片

收稿日期:2021-06-24
*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(135309470)、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)资助

价格较低[2],因此,ZigBee 技术能很好地满足智能家居的应用场景[3]。此外,消息队列遥测传输协议(MQTT)是一种低开销[4]、低带宽的即时通信协议[5],可以为远程设备提供实时可靠的消息服务[6],易于实现智能家居设备的远程控制[7]。

伴随通信技术的引入,智能家居也遭到了大量的网络威胁,用户信息在传输过程中容易被窃取和篡改,迫切需要解决数据在传输过程中的安全问题[8]。文献[9]提出了一种内网穿透控制智能家居设备的方案,手机 APP 和家庭路由器之间采用 ZeroTier 方案进行 P2P 内网穿透的通信,保证了安全性,提高了远程控制响应速度,但未涉及家居设备间的安全通信方法。文献[10]以智能终端远程控制的智能家居系统为模型,分析了智能家居的安全风险问题,并提出了相应的防护手段,重点给出了认证、加密、安全传输协议的应用分析,但未进行应用相关的实验。文献[11]将智能家居的安全问题划分为平台安全、设备安全、通信安全,分析了他们的研究现状,并提出了未来的研究方向。文献[12]提出了融合身份认证和 AES 算法的智能家居通信安全系统,系统的外部网络通信,采用一次口令认证登录,内部网络通信通过动态生成 128 位密钥的 AES 算法加密,提高了系统保密性,保证系统中数据传输更加安全,有效解决了智能家居的安全通信问题,但输入数据量增加,系统运行时间会增加,系统的稳定性及有效性有待提高。文献[13]实时提取、处理人体脉搏特征数据,生成 128 位密钥,然后使用 ECC 加密密钥、AES 算法加密原始数据,时空开销低,可以适应健康智能家居系统数据处理要求,但密钥的随机性有待改进。因此,考虑到 Logistic 混沌映射产生的变量具有较强的遍历性[14]、较好的随机性[15],如文献[16]改进了标准 Logistic 混沌映射,提高了种群多样性,改善了教育学优化算法的精度和效率。综合分析以上文献 本文设计了一种基于 ZigBee 智能家居系统,提出了系统的安全通信方法。首先给出了系统的组网结构,部署了系统的 MQTT 服务器和客户端,并设计了他们之间的安全通信方案。然后,提出基于 L-P 混沌系统交叉扩散方法产生 AES 初始轮密钥,并用于家居设备之间的 ZigBee 安全通信。

1 系统组网结构及安全通信方法研究

1.1 系统组网结构设计

设计的系统结构如图 1 所示。系统包括内部网络和外部互联网,内部网络便于用户在家控制家居设备,外部网络用于实现远程控制,内部网络传输的数据量小、传输距离短、节点多,采用 ZigBee 协议通信方式,外部网络采用安全的内网穿透方案 ZeroTier,并基于 MQTT 协议进行远程控制。路由器作为 MQTT 服务器,Android 手机和 Z-W 控制器作为 MQTT 客户端,内部网络的 ZigBee 终端节点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 Z-W 控制器,Z-W 控制器再通过 WiFi 发送给 MQTT 服务器。Android 手机是控制设备,可以发送控制信息给 MQTT 服务器,MQTT 服务器再发送给 Z-W 控制器,Z-W 控制器依据接收的控制信息,控制家居设备进行相应动作,如开启或关闭窗帘、开/关电灯等。

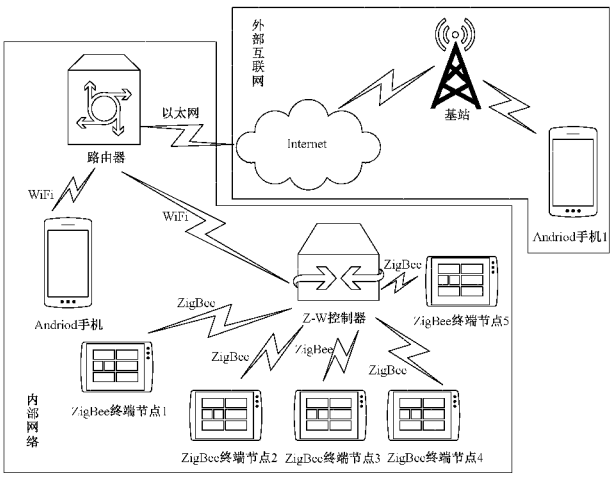

图 1 系统组网结构

因此,系统主要包括 MQTT 客户端和服务器之间的通信、ZigBee 节点之间的通信,下面分别介绍它们之间的安全通信方法。

1.2 MQTT 客户端和服务器之间的安全通信

Andriod 手机和 Z-W 控制器之间使用 MQTT 协议通信,需要研究 MQTT 协议的安全性。本文的安全通信体现在 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,处于非家居内网的 Andriod 手机 1 使用内网穿透方案 ZeroTier,实现在加密安全的全球点对点(P2P)对等网上进行分布式的管理。

1)安全通信方案设计

设计 MQTT 客户端和服务器的通信方案如图 2 所示。

2)通信平台构建

路由器上刷 OpenWrt 系统,以小米路由器 mini 为例,刷 OpenWrt 18.06,安装 MQTT 服务器 mosquitto 软件,并客户端用户名、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,实现外网的 Andriod 手机安全访问内网的 Z-W 控制器。主要步骤:

步骤 1:路由器刷 OpenWrt 系统。

(1)刷入与路由器型号对应的开发版系统。

(2)获取 SSH 工具。

(3)获取路由器的 root 权限。

(4)刷入 OpenWrt 系统。

步骤 2:服务器 mosquito 软件安装及配置。

(1)通过 putty 软件,使用 SSH 协议登陆到路由器,通过如下命令安装 mosquitto 服务器软件。

opkg install mosquito

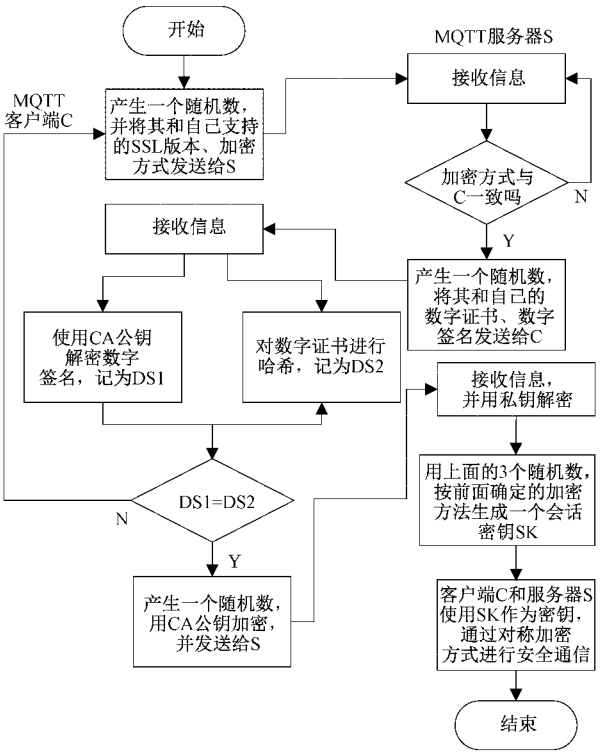

图 2　MQTT 客户端与服务器的安全通信方案

(2)配置 MQTT 客户端登陆的用户名和密码。

第 1 步：修改 mosquitto.conf 配置文件内容，禁止匿名用户登陆，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

第 2 步：添加用户名和密码。

为 MQTT 客户端 Andriod 手机和 Z-W 控制器分别设置用户名、密码，假设 Andriod 手机的用户名、密码都为 samqtt，则配置用户名的命令如下：

mosquito_passwd-c/etc/mosquito/pwfilc samqtt

按提示输入 2 次密码即可。

第 3 步：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。

首先，安装 openssl。

然后，按如下步骤产生证书文件。

第 1 步：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

第 2 步：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

第 3 步：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

第 4 步：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

第 5 步：重复第 1～4 步，为 3 个 MQTT 客户端生成证书文件。

步骤 4：搭建 ZeroTier 网络。

(1)在 ZeroTier 官网先注册账号。

(2)下载 OpenWrt 系统、Android 系统的 ZeroTier 客户端软件，并分别安装到路由器、Android 手机 1 上。

(3)网页登录个人账号工作面板，创建网络 ID。

(4)在使用环境中运行 ZeroTierOne 软件，加入创建好的网络 ID。

(5)在工作面板上授权各客户端的连接，分配虚拟局域网 IP。

(6)网络连通测试。由路由器向手机 IPv4 地址发送 PING 包，若建立起了 P2P 通道，则可 PING 通。

3)安全通信方案实现方法

Android 手机和 Z-W 控制器都是 MQTT 客户端，而且 Android 手机是控制端，它们之间通过路由器实现通信，因此，Android 手机和 Z-W 控制器都需要设计 MQTT 客户端程序，基于图 2 所示的通信方案，本文使用 Android Studio 设计 Android 手机 MQTT 客户端程序，采用 Arduino 开发环境设计 Z-W 控制器的 MQTT 客户端程序。设计完成后，Android 手机 1 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 Z-W 控制模块从而控制家居设备，从而控制 ZigBee 终端节点。

1.3　ZigBee 网络的安全通信

由系统的网络结构可知，Z-W 控制器既包括 WiFi 模块，也包括 ZigBee 协调器模块，后者和 ZigBee 终端节点统称 ZigBee 节点，组成了 ZigBee 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 给出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，本文提出了 AES 初始轮密钥的产生方法，如图 3 所示。

初始轮密钥的产生步骤如下：

1) 设置混沌系统的参数

(1)随机产生一个取值范围为(3.569 945 6,4]的数作

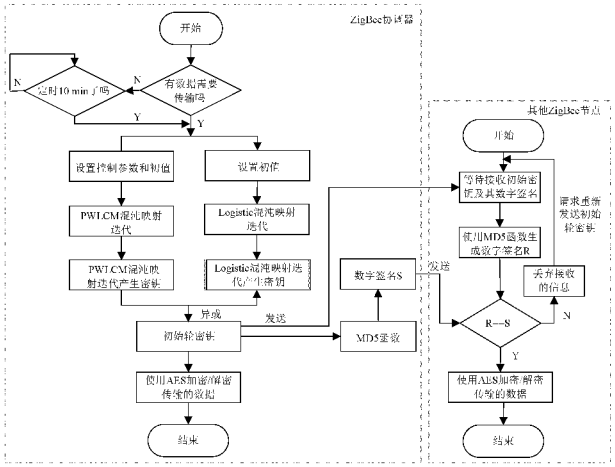

图 3 AES 初始轮密钥产生方法

为 Logistic 混沌系统的控制参数 μ。

(2)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 η。

(3)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。

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。

3) 产生 AES 初始轮密钥

(1)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 $i=1,\cdots,16$。

(2)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 $i=1,\cdots,16$。

(3)将 $PWLCM(i)$、$Logistic(i)$ 转换成整数序列,即乘以 108,并对 256 取余。

(4)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。

初始轮密钥由 ZigBee 协调器产生,每隔 10 min,或重启后轮密钥都重新设置,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 混沌映射先分别迭代若干次。ZigBee 协调器产生轮密钥后,将其通过 MD5 函数生数字签名,并将轮密钥及其数字签名发送给其他所有 ZigBee 节点,ZigBee 节点接收后,进行数字签名验证,验证无误后,再将轮密钥作为初始轮密钥进行 AES 加密或解密。

2 实验与分析

针对前面所述 MQTT 客户端和服务器、ZigBee 节点的安全通信方法,本节进行了实验。

2.1 MQTT 客户端和服务器的通信方法实验

按 1.2 节所述构建通信平台,将路由器部署为 MQTT 服务器,建立 ZeroTier 网络,使外网的 MQTT 客户端以 P2P 方式和 MQTT 服务器同在一个局域网中,然后通过 mosquitto 的 SSL 产生公钥和证书,进行安全通信。

1)ZeroTier 网络建立及测试

登录 ZeroTier 官网,先注册,然后创建 ZeroTier 网络,依据获得的网络 ID 和名称,将 Andriod 手机 1(MQTT 客户端)和路由器(MQTT 服务器)加入到网络,如图 4 所示,此时,点击 Login,按前面 1.2 节中 mosquito 配置时设置的用户名和密码登录即可。

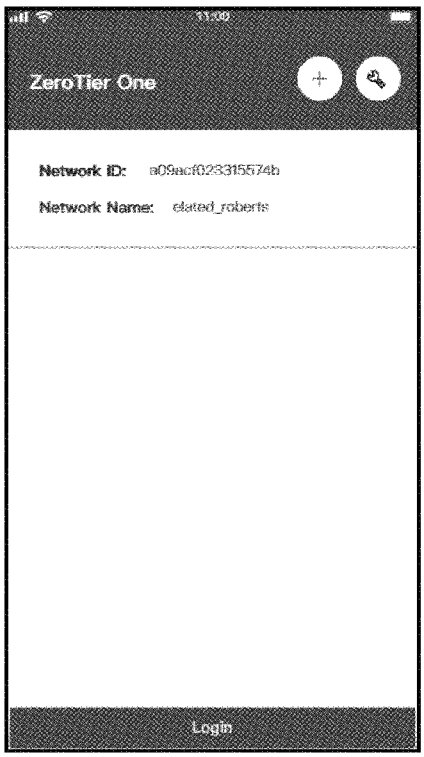

图 4 Andriod 手机 1 接入 ZeroTier 网络

2)MQTT 客户端和服务器的 SSL 通信

(1)MQTT 客户端程序设计

采用 Android 手机为 MQTT 客户端,需要设计 MQTT 客户端程序。即在 Windows 环境下构建 Android Studio 软件开发环境,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。然后在 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模块,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。登录模块的功能如图 4 的 Login,如果登录成功,跳转到客户端主界面;否则返回登录失败信息。主界面模块如图 5 所示。

图 5　MQTT 客户端程序主界面

(2)SSL 通信实验

Android 手机 MQTT 客户端成功登录后，可以点击“消息”，与 MQTT 服务器进行安全通信，这可以通过获取 MQTT 客户端和服务器之间通信的数据包来分析。考虑到 PC 机上捕获数据包比较方便，PC 机上安装抓包软件 Wireshark，将路由器的 LAN 接口和 PC 机通过网线连接，Android 手机 MQTT 客户端给路由器通发送“hello”时，使用抓包软件捕获的数据包如图 6 所示。其中，192.168.190.164、192.168.190.188 分别 MQTT 客户端、路由器的 IP 地址，他们之间通信时使用的是 SSL 协议，可以实现通信的安全性。

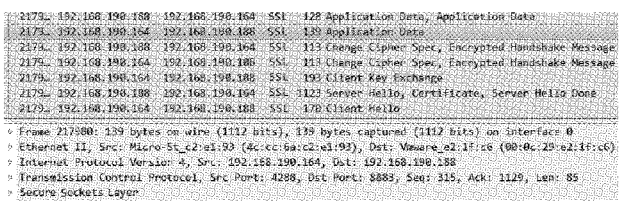

图 6　SSL 协议分析

2.2　ZigBee 节点通信方法实验

1)算法效果实验

为了分析本文改进的 AES 算法在 ZigBee 节点之间的安全通信效果，采用的实验环境如下：内存 8 GB，处理器 i7-6700HQ，CPU2.6 GHz，Win 10 操作系统，仿真软件是 MATLAB R2014a。使用标准 AES 默认密钥加密解密运行结果如图 7 所示，本文算法产生初始密钥的运行结果如图 8 所示。图 7 中命令窗口最后 4 行为处理的数据，其中第 1 行“温度：22 ℃；光线明亮”为传输的原始数据，第 2～3 行为加密后的数据，第 4 行为解密后的数据。图 8 中编辑器窗口显示的是部分源代码，命令窗口最后 3 行是处理的数据，其中，第 1 行为传输的原始数据，第 2 行为加密后的数据，第 3 行为解密后的数据。对比它们的运行时间，都在 0.7 s 左右，本文算法加密时间较短，降低了 3.77%，如表 1 所示。

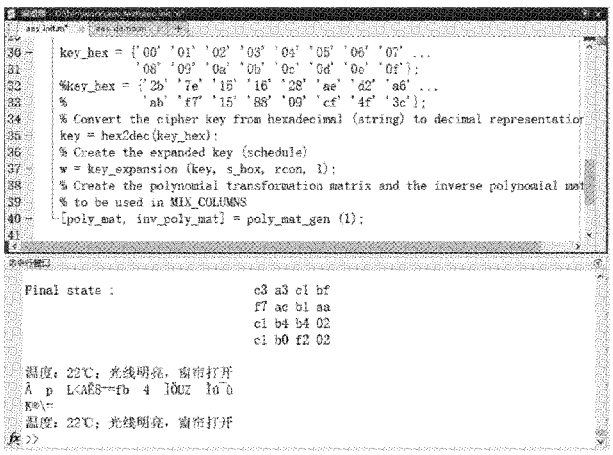

图 7　使用标准 AES 默认密钥加密解密运行结果

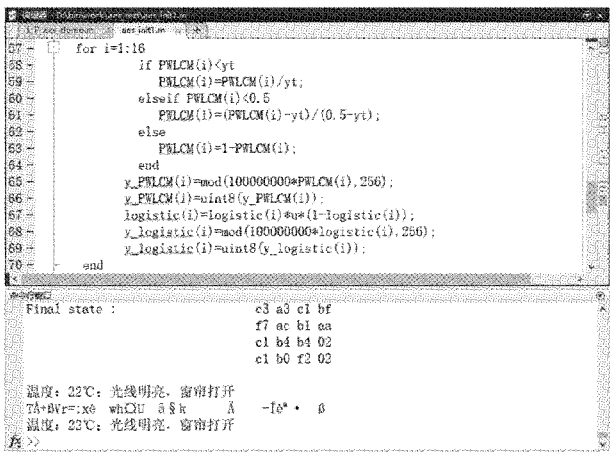

图 8　使用本文算法的密钥加密解密运行结果

表 1　算法运行时间对比

算法	加密时间/s
标准 AES 算法	0.742 0
本文算法	0.714 0

2)算法性能实验

为了分析本文改进 AES 算法的能耗和通信延迟等性能，本文采用 Omnet＋＋网络仿真软件进行实验，即基于 Win 10 操作系统，安装 Omnet＋＋4.5，并导入传感网仿真框架 mixim2.3，建立的拓扑如图 9 所示。

在图 9 中，controller 代表 Z-W 控制器，充当协调器的

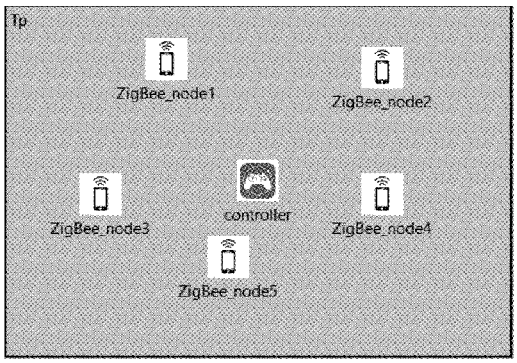

图 9 网络拓扑图

功能,位于仿真区域的中心。其他设备代表 ZigBee 终端节点,表示智能家居设备,他们随机部署在仿真区域。

依据 AES 算法及其改进算法设计程序,初始参数如表 2 所示,调试运行程序,对比分析算法的能耗和通信延迟,运行结果如图 10、11 所示。

表 2 初始参数设置

参数名称	初始值
分布区域	300×300
节点初始能量/mJ	2 500
ZigBee 终端节点数量	5
发射功率/mW	1
消息长度/B	250

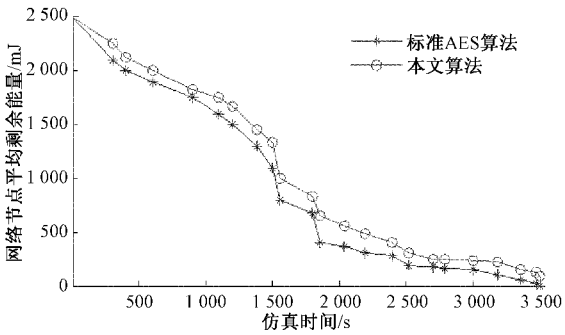

图 10 能量消耗比较

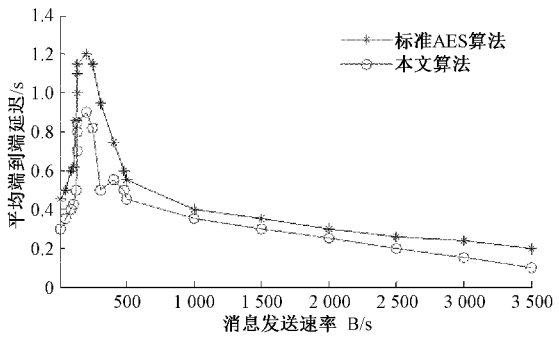

图 11 平均端到端延迟比较

图 10 显示了 ZigBee 网络中,节点平均剩余的能量,初始能量为 2 500 mJ,随着仿真时间的增加,节点间发送、接收数据,剩余能量逐渐减少。通过分析,相对标准 AES 算法,本文算法的剩余能量提高了 30.22%,从而能量消耗小。图 11 显示,初始平均端到端延迟较大,随着发送速率的提高,端到端延迟逐渐降低,并趋于平稳。这是由于 ZigBee 终端通信时,由协调器转发,网络运行一段时间后,协调器存放了相关的转发数据,缩短了数据传输时间。通过分析,相对标准 AES,本文改进的 AES 算法平均端到端通信延迟降低了 28.5%。

3 结 论

针对智能家居目前的安全问题,本文设计了一种新的智能家居组网结构,采用 WiFi 和 ZigBee 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 客户端和服务器安全通信,既节约了成本又提高了安全性。同时家居设备通过 ZigBee 技术进行通信,为了提高安全性,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,来提升 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,能耗和通信延迟小,具有应用性。

参考文献

[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] 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.

[3] JOSE A C, MALEKIAN R. Improving smart home security: Integrating logical sensing into smart home[J]. IEEE Sensors Journal, 2017, 17(13):4269-4286.

[4] 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.

[5] 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.

[6] 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.

[7] 于海飞, 张爱军. 基于 MQTT 的多协议物联网网关设计与实现[J]. 国外电子测量技术, 2019, 38(11):45-51.

[8] 陈亚科. 基于大数据的信息传输过程中数据安全性的研究[J]. 电子测量技术, 2020, 43(7):119-123.

[9] 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):177-179.

[10] 苏治中. 基于物联网的智能家居安全问题分析[J]. 广州广播电视大学学报, 2020, 20(2):27-30.

[11] 王基策, 李意莲, 贾岩,等. 智能家居安全综述[J]. 计

算机研究与发展，2018，55(10)：2111-2124.

[12] 江治国. AES 算法在智能家居通信安全系统中的应用[J]. 吉首大学学报(自然科学版)，2018，139(3)：30-35.

[13] 陈思伟，高翠云，沈庆伟，等. 面向智能家居的生理参数密钥加密方法研究[J]. 电子测量与仪器学报，2020，35(3)：173-180.

[14] WANG X Y，LI Y P. Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence[J]. Optics and Lasers in Engineering，2021，137(11)：393-408.

[15] 王尔申，贾超颖，曲萍萍，等. 基于混沌粒子群优化的北斗/GPS 组合导航选星算法[J]. 北京航空航天大学学报，2019，45(2)：259-265.

[16] 孙凤山，范孟豹，曹丙花，等. 基于混沌映射与差分进化自适应教与学优化算法的太赫兹图像增强模型[J]. 仪器仪表学报，2021，42(4)：92-101.

作者简介

王海珍，副教授，主要研究方向为嵌入式技术、密码分析与设计、网络安全等。

E-mail：wanghaizhen1976@163.com

廉佐政，副教授，主要研究方向为机器学习、Web 安全等。

E-mail：lianzuozheng@163.com

谷文成，高级工程师，主要研究方向为计算机应用技术。

E-mail：421324660@qq.com

崔志青，在读硕士，主要研究方向为计算机网络与信息安全。

E-mail：1713794596@qq.com