装

订

线

山东农业大学

毕 业 论 文

题目：基于云计算的智能家居安全解决方案

院　　部　信息科学与工程学院

专业班级　网络 11-1

届　　次　2015 届

学生姓名　高宇昊

学　　号　20115147

指导教师　张亮 副教授

二 O 一 五 年 六 月 一 日

基于云计算的智能家居安全解决方案

A Safe Solution of Smart Home Based on Cloud Computing

专业 Speciality	网络工程 Network Engineering
学生 Undergraduate	高宇昊 Gao Yuhao
指导教师 Supervisor	张亮 Zhang Liang

山东农业大学

二〇一五年六月

Shandong Agricultural University

June, 2015

目　录

Contents

基于云计算的智能家居安全解决方案

2011 级网络工程 1 班　高宇昊
指导教师　张亮

【摘　要】随着网络技术的突飞猛进与“互联网+”概念的提出，物联网技术已经成为网络研究的前沿热点领域，智能家居作为其代表性应用之一，开始逐步走入大众的日常生活。然而由于智能家居系统与用户个人隐私信息息息相关，受到了攻击者的极大关注，安全形势日益严峻。

为解决智能家居领域所存在的各类安全问题，本方案对其所面临的安全威胁进行了分析，提出了一套基于私有云技术的智能家居安全解决方案。方案所提出的智能家居系统具有独特的体系结构和加强的安全特性，以及为保证安全通信而设计的节点通信协议，实现了整个系统的安全高效，同时其对二次扩展开发友好，可推广至物联网技术的各类其它应用中。

本文详细介绍了上述方案的完整设计以及方案中所述系统的实现过程与运行情况，并对该方案的创新性进行了总结，对其未来前景进行了展望。

【关键词】物联网；智能家居；云计算；网络安全；通信协议

A Safe Solution of Smart Home Based on Cloud Computing

Gao Yuhao
Zhang Liang

【Abstract】With the rapid development of network technology and the initiative of the concept "Internet +", the Internet of Things technology has become a hot area of network research. The smart home technology, as one of its typical applications, began to gradually into the public's daily life. However, the smart home system, which is closely related to user privacy information, has been a great concern of the attacker. The security situation of the smart home system is increasingly grim.

In order to solve all kinds of security problems that exist in the field of smart home, this solution analyzed various security threats and put forward a safe solution of intelligent home based on proprietary cloud technology. This smart home system has a unique architecture and enhanced security features, and special node communication protocol to guarantee secure communications. They achieve the security and efficiency of the entire system, while it is friendly to extension development and can be extended to all kinds of other applications. This paper describes the design and implementation of the above-mentioned system , and its future prospects were discussed.

【Key words】Internet of things; Smart home; Cloud Computing; Network Security; Communication Protocol

1 引言

1.1研究背景

物联网是新一代信息技术的重要组成部分，是计算机网络与互联网下一步最为热门的研究领域之一，也是目前以及今后一段时间内业界最为引人注目的热点技术之一。物联网的英文名为“the Internet of Things”，即“物与物相连的互联网”，缩写为 IOT。当下随着“互联网+”浪潮的不断发展，物联网的应用领域日益广泛，其中较为典型的应用方向就包括与每个人日常生活息息相关的智能家居。

智能家居为物联网技术在家居生活中的具体应用，即使用物联网相关技术将日常家居中的各种通常意义上智能化、非智能化的设备、家电如音视频系统、灯光系统、空调系统等连接到一起，借助微处理器或是家庭私人服务器，通过一体化与智能化的控制、反馈与交互技术，实现对于居住者而言更为方便、智能、舒适的居家体验。

然而随着互联网技术的飞速发展,与之伴随而来的是日益增加的网络安全威胁,如网络入侵、隐私窃取、网络诈骗等网络安全问题层出不穷，而作为新兴技术的物联网智能家居不仅尚处于技术萌芽阶段，各项安全标准尚未制定完善，同时由于其部署在用户家中能够直接获取极为敏感用户信息的特点，逐渐成为了安全领域各方所关注的焦点。窃取用户私人信息、控制用户家中各类设备、入侵远程摄像头窥探用户隐私乃至破解智能门禁从而破门而入等安全问题已经成为摆在智能家居发展道路上的严峻挑战，安全问题已经成为智能家居发展道路上必须解决的重大问题，保护用户隐私、提高系统安全性迫在眉睫。

云计算是一种新型的、基于互联网的服务交付模式，其整合了传统意义上的分布式计算、网络存储、虚拟化等技术，对于云计算服务的使用者而言，当其使用云计算服务时不需要在私有设备上存储任何数据，只需通过互联网连接至云计算服务提供商即可享受便捷的云计算服务。而私有云则是为一个客户而单独构建的专有云服务，其基础设施为客户单独定制、部署，其服务也仅为唯一客户提供，往往通过部署在私有防火墙之后或者使用 VPN 加密通信等诸多手段,相较于向大量客户提供服务的公有云服务相比，私有云服务能够为客户提供极高的安全性与可用性。

1.2 研究现状

目前已有的各类智能家居产品主要包括单品与整合产品两大类。其中，单品产品往往直接接入互联网，并在同一物理设备内实现了环境信息的采集、受控设备的控制、web 服务的提供等，多种功能均混合在一起，使得设备既要做终端节点，又要承担对外服务器的角色，不仅安全性难以得到保证，同时也缺乏与其他设备联网的能力，而且使用简单单片机所开发的产品往往无法实现数

据的持久化保存。而整合产品目前多是采用已有的各类互联网通信解决方案进行节点间通信，如直接使用 802.11 无线协议进行 wifi 传输或是蓝牙传输等，内容也往往是明文传输，构架上则不具有分层的理念，各个节点与核心节点间往往是出厂前已经配对的，系统扩展性差，且核心节点所能支持的终端节点数量极为有限。

1.3 工作内容

为了解决目前在各类智能家居产品中所存在安全缺陷与不足，本方案首先分析了现有的物联网智能家居产品中所存在的重点安全隐患和可能发生的各类安全问题，如用户直接对智能家居设备数据的访问，数据传输中不进行加密，跨越互联网的明文数据传输，访问控制环节薄弱，缺少客户端与服务端的双向认证措施等，并进一步探讨了现有产品在体系结构中的不足，如传感器直接提供面向互联网的 web 访问服务，数据分析的不足或缺失，各个传感器与控制器节点间无法互联互通，用户无法从统一平台对整个系统进行有效控制等问题。

在对以上问题进行梳理、总结、归纳的基础上，本方案又对典型的智能家居应用场景进行了全面的分析与梳理，针对最为典型的数据采集与设备控制这一应用方式，从体系结构与系统构架入手，对智能家居的整个系统从部署方式到运行模式都进行了重新设计，全新设计了一整套的安全智能家居体系结构，并针对上述问题，在该体系结构的基础上着重强化了其安全性，采用了 VPN、双向认证、加密通信、访问控制等技术，并根据物联网智能家居的通信特点设计了一套适用于物联网智能家居各个设备节点间安全通信的安全通信协议，之后在总结现有各类智能家居产品的基础上，将该体系划分为三大部分，并借助私有云设施，进一步提出了完善的高安全性、高可靠性、可扩展的智能家居安全解决方案。

根据上述设计的解决方案，本作品进一步以目前较为流行的树莓派嵌入式开发平台为依托，使用温湿度传感器、摄像头，借助部分开源的库程序，实现了较为简易的物联网传感控制节点程序，基于开源 Linux 平台以及部分库程序实现了较为简易的私有云核心节点服务端程序，采用命名管道与核心节点进行通信的方式利用 PHP 语言借助 MySQL 数据库编写了一套 web 服务提供程序，最终实现了能够进行简易概念演示的智能家居安全系统。

1.4 创新点

本作品的创新之处在于将传统的单一化智能家居设备如网络摄像头和无加密的智能家居中控系统重新规划，设计出基于私有云的物联网智能家居系统，并对系统中各个安全薄弱环节进行了强化，为节点间的通信设计了一套安全通信协议。

针对现有智能家居系统在体系结构方面的不足，本作品将智能家居系统划分为三个部分，包括感知控制节点、私有云核心节点以及安全云服务。

其中感知控制节点包括传感器与设备控制器，负责对环境数据进行感知与

采集以及对于家居设备的控制，其与私有云核心节点直接进行加密通信，将获取到的环境数据进行上行传送，同时接收私有云核心节点下发的控制指令，实现对家居设备的控制以及对传感器数据采集模式的调整等。私有云核心节点则负责接收汇总各个感知控制节点所传送的数据，对其进行分析处理，选择性地存入数据库、转发至终端用户或是丢弃，并根据终端用户的选择以及系统设定随时对各个节点下发控制指令，保证整个系统的有序运行。同时私有云核心节点提供 API 接口供安全云服务提供程序进行调用，使终端用户可以方便地对系统进行操控。安全云服务则是以 web 服务的形式通过虚拟专用网（VPN）向终端用户所提供的最终的系统接口，用户通过 VPN 连接至安全云服务后即可访问相应的 web 服务，以方便简洁地形式查看整个智能家居系统的所有实时感知数据、历史感知数据、控制家居设备并通过数据分析实现其他功能。

系统的三部分各自独立又能够通过网络通信有机的进行交互与数据传输，极大地提高了智能家居系统的可扩展性和稳定性。同时通过一致的通信协议，系统能够极为方便的进行部署与设备的增加。

针对现有智能家居系统在安全性方面的不足，本系统重点强化了自身的安全特性。系统各个节点在直接通信前均进行双向认证，保证其真实可信，在通信时对内容进行加密与签名，保证通信内容的安全隐秘、可靠和不可抵赖。各节点之间跨越互联网通信时借助 VPN 技术构建安全的通信隧道。终端用户访问系统时使用 VPN 保证数据的安全可靠，同时对终端用户与系统内部节点之间进行隔离，保证系统对外安全边界的可控。而对于系统中最为重要的通信链路即核心节点与感知节点间的通信，专门设计了一套满足其效率要求的同时兼顾安全性的通信协议以保证其通信的安全可靠。

1.5 应用前景

本作品创新性地做到了智能家居系统方便易用性与安全性二者兼顾，从体系结构和通信协议的角度对物联网智能家居系统中存在和可能出现的各类问题进行了防范，并对智能家居各个节点间的互联互通和有序结合进行了规划与设计，具有极高的可扩展性。故本系统在未来智能家居的应用中将具有极为广阔的前景，借助系统易于部署、易于使用、安全可靠的特点，必将在消费领域受到青睐。而其节点程序的通用性与安全性，则使该系统可在除智能家居之外的多种其他场景中进行使用，如工业物联网、农业物联网、医疗物联网等不同领域，其安全性保证了该系统可以被应用于对信息安全具有高要求的敏感行业和领域。同时由于其清晰的结构特征和明确的工作原理，该系统也可以作为各类物联网产品进行二次开发的基础，二次开发人员可以在本系统的基础上，通过修改核心节点与感知控制节点的程序功能，实现更为丰富的各类系统特性，以满足各类用户不同的特殊要求，进一步推广到各类不同的细分市场。

1.6 本文的组织结构

本文主要对于目前物联网智能家居的各种典型应用中所存在的安全问题

进行了分析，在此基础上提出了一套基于云计算的智能家居安全解决方案，对其设计进行了详细介绍，着重介绍了该方案中对于系统安全通信问题的解决方式，之后提出了该方案的一种简单实现，最后分析了该方案的创新性并进行了总结与展望。

全文结构如下：

第一章介绍了物联网智能家居的研究背景与研究现状，简要对本文所做工作进行了概述，并简要概括了整个方案的创新点，最后介绍了本方案的应用前景以及本文的组织结构。

第二章对整个解决方案的设计进行了详细介绍，首先对系统的整体结构进行了概述，之后分别对系统各个组成部分的设计进行了描述。

第三章介绍了本方案中系统各部分之间安全通信所使用的解决方案，包括云服务与用户间通信时和云内部各个节点之间通信时所使用的安全解决方案，着重介绍了云节点间通信时所使用的专门设计的安全通信协议，包括该协议的包结构、时序等。

第四章介绍了本方案的一种简单实现，首先对方案的整体实现进行了概述，之后分别对系统不同部分的实现分别进行了介绍。

第五章着重介绍了本方案的创新之处。

第六章对本方案进行了总结，并对于该方案未来的进一步研发工作与前景进行了展望。

2 系统结构设计

2.1 系统结构概述

基于云计算的智能家居系统主要包括三大部分：感知控制节点、私有云核心节点及安全云服务（如图 2.1），以及系统周边设施如受控设备、安全边界控制等。

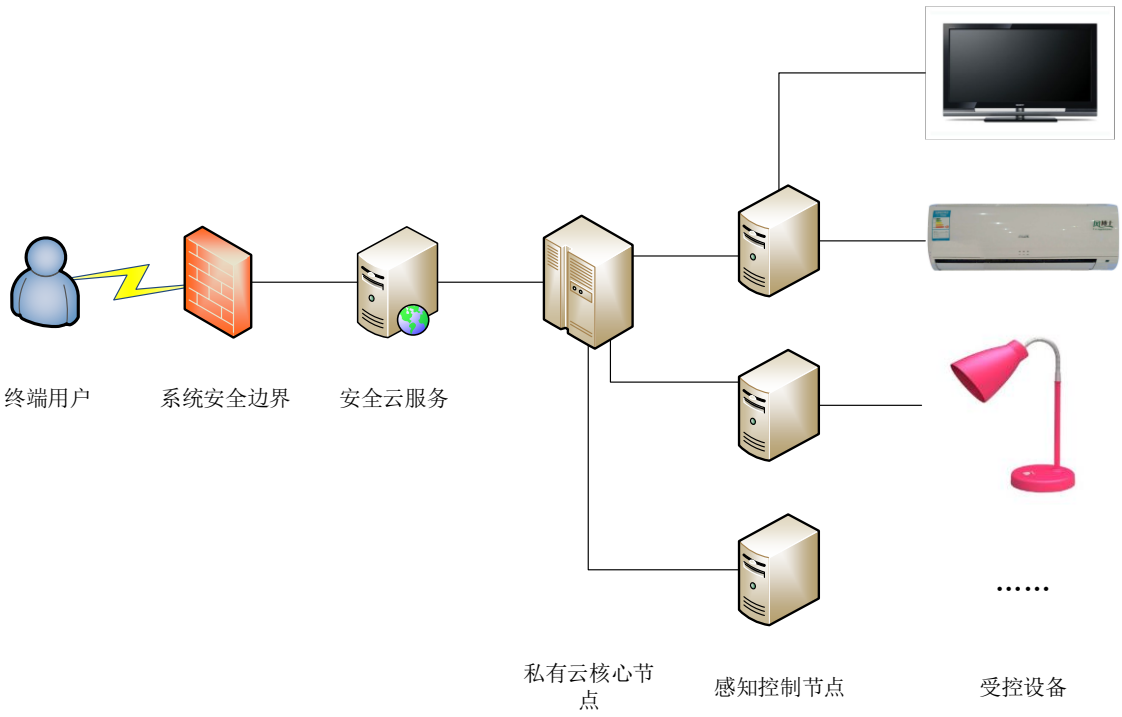

图 2.1 智能家居系统结构图

受控设备即智能家居系统所能控制的普通家用电器，或者是负责进行环境信息采集的传感器等，通过连接至感知控制节点进入本系统，并通过该节点实现数据的上行传送和控制指令的接收。对于提供智能化控制接口的受控设备，可以直接以数字化接口的方式接入系统，传统的家居电器可以通过对感知控制节点增加外围电路的方式实现其数字化控制，进而接入系统。

感知控制节点在系统中作为基本节点，直接与外围受控设备进行交互，节点数量根据整个系统需要连接受控设备的多少可以进行灵活调整。感知控制节点下行连接受控设备，上行连接私有云核心节点。每个感知控制节点负责连接 1-2 个受控设备或是环境信息传感器，所有的节点统一连接到私有云核心节点。各感知控制节点之间独立运行，互相不影响。通过本节点，系统可以实现对受控设备的操作与数据获取。一个感知控制节点物理设备可以运行多个实例程序，通过使用不同的端口与私有云核心节点进行通信从而实现设备的复用与系统部署成本的压缩。

私有云核心节点是系统的中枢控制节点，下行连接感知控制节点，上行连

接安全云服务，整个系统的配置信息和运行数据均保存在该节点中。系统中所有的感知控制节点均连接至本节点，同时本节点向安全云服务节点提供 API 接口。在系统运行过程中，本节点负责对系统中所包含的各个感知控制节点根据系统配置与用户控制信息发送不同的控制指令，并实时采集其上传的感知数据与运行状态数据，对数据进行分类处理、存储、展示等。

安全云服务为系统向用户所提供的一组基于认证授权的 web 访问服务，通过该 web 服务用户可以直接通过互联网连接至本系统，方便地使用浏览器对系统的运行情况和各个传感器获取的环境信息进行实时查看、调取数据库中存储的历史数据、对系统运行发出控制指令。该服务要求用户通过 VPN 连接至本系统，保证了数据在跨越互联网传输过程中的安全可靠，通过使用用户认证与授权以及根据用户角色进行不同的权限划分，保证了系统各级别隐私数据的安全不被窃取。

系统安全边界即系统内部与外部网络环境之间的数据控制，主要包括智能感知节点与私有云核心节点之间进行数据通信时使用私有网络或是在必须跨越互联网进行数据传输时使用安全的 VPN 技术组建虚拟专用网，保证节点全部位于安全边界之内，且其通信过程使用本系统所特有的专用安全通信协议来进行；私有云核心节点与安全云服务通常部署在同一私有网络范围内，通过防火墙进行隔离，保证 web 服务器只能访问核心节点，不得访问私有网络中的其他节点特别是智能感知节点，或是私有云核心节点与安全云服务部署在同一物理服务器中，其互联网链路接口部署防火墙进行安全防护，对互联网流量进行严格过滤。

2.2 智能感知控制节点与受控设备

智能感知控制节点是整个智能家居系统中最为基本的组成节点，其核心作用即实现家居设备与整个系统的连接与整合。

智能感知控制节点对于设备的连接与控制包括两种形式，即对于提供数字化控制接口如蓝牙、USB、网络通信协议的设备直接采用其所提供的接口与数据通信规范进行通信，对于不提供数字化控制接口的传统家用设备，采用连接外围电路、增加控制转换中间硬件等间接连接的方式获取数据。

外围受控设备通过非网络连接方式连接智能感知控制节点并唯一的接入智能家居系统，除与之相连接的控制节点外系统内的其他节点、设备以及系统以外的任何其他设备均不能直接获取其上传的数据或是对其进行控制。

为了保证节点运行的稳定性与程序控制、通信的接口统一性，在智能感知控制节点内部，划分为三层工作系统：硬件接入层、设备驱动层、节点服务实例。结构如图 2.2 所示。

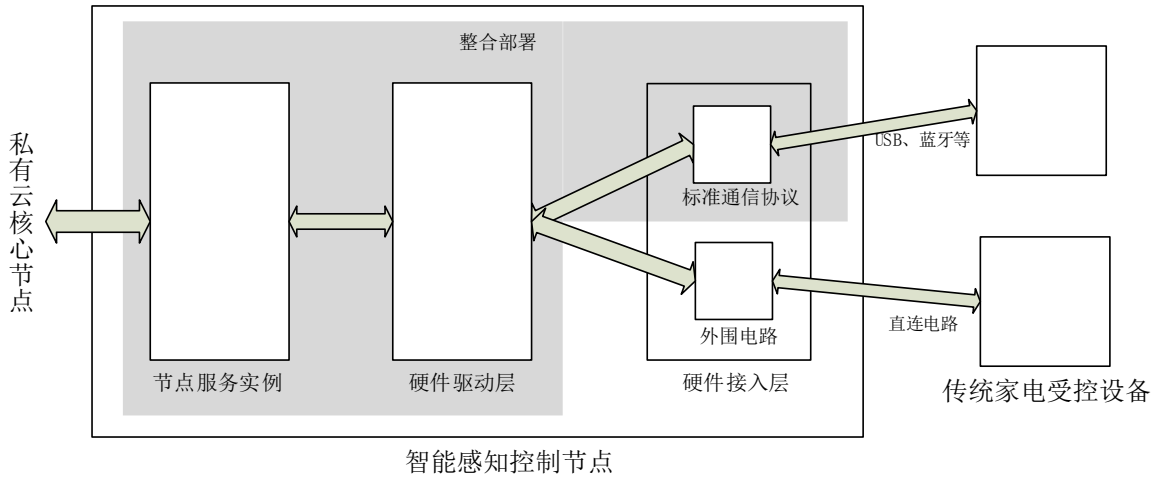

图 2.2 智能感知控制节点结构图

硬件接入层主要实现节点与受控设备的连接，为硬件设备、电路或是已有通信协议的某种实现，向下通过不同的方式与受控设备相连接，向上为硬件驱动层提供可用的软件接口以进行受控设备的控制。针对不同的受控设备，可以采用不同的接入方式。对于提供数字接口的受控设备，使用已有的标准通信协议进行接入，在本层中则退化为调用相关的标准通信协议即可实现设备与节点之间的连接通信，不需要额外的硬件或设备；对于不提供数字接口的传统家电受控设备，在本层中则需要提供适合其硬件特性的控制方式并向硬件驱动层暴露一定的硬件可操作接口，如使用自制的外围电路并借助单片机进行控制，或是采用已有的控制解决方案如 Arduino 等，使用 GPIO 接口实现节点与受控设备间的连接。

硬件驱动层主要实现对于不同方式接入节点的设备分别选择不同的通信方式对其进行控制与驱动，并在本层隐藏与受控设备之间的通信细节，屏蔽这种不同，向上层即节点服务实例提供统一的控制与通讯接口。对于提供数字化接口的受控设备，在本层直接调用相应的通信协议直接与设备进行通信，对于不提供数字化接口的传统设备，本层次调用相应的 GPIO 接口控制程序或是中间控制设备提供的通信接口，间接实现与受控设备的通信。在实现屏蔽通信细节的基础上，本层针对不同的受控设备封装并实现一组特定的操作指令，如面向室内灯光提供开关灯指令，面向环境信息传感器提供捕获数据指令等，从而方便上层对设备的操作。对于向上层所提供的统一通信接口，可以选择仅限本地访问的网络端口或者是管道通信等方式。

节点服务实例主要实现与核心节点的通信，控制本节点的运行，向核心节点传送本节点所采集的数据以及接收核心节点的控制指令并根据指令执行相应操作。节点服务实例在开始运行后首先启动本节点的硬件驱动层软件，检测相关硬件状态并进行启动，进入待机状态，然后主动向核心节点发起连接，连接成功后与核心节点进行证书交换、双向认证、协商会话通信密钥，之后进入命令等待状态，监听端口等待核心节点的指令，当收到指令后根据指令内容执行相应的操作如对设备进行控制、向核心节点发送数据等。

在进行感知控制节点的部署时，节点服务实例、硬件驱动层、以及硬件接入层的标准通信协议类型通信部分往往可以共同部署到同一硬件设备上，同时多个感知控制节点也可以部署在同一硬件设备上，通过运行不同的节点实例程序、复用不同端口进行通信的形式充分利用有限的硬件资源。

2.3 私有云核心节点

私有云核心节点作为智能家居系统的中枢控制部分，是整个系统构架中最为核心的部分，该节点的主要功能包括与各个感知控制节点建立连接、维护各个节点的状态信息、根据系统配置与用户指令向各个节点发送控制指令、接收各个节点上传的数据与状态信息、提供可供调用与访问的接口。

私有云核心节点在结构上分为四部分，即节点通信实例、节点状态维护模块、访问接口模块、数据存储与转发模块，如图 2.3 所示。

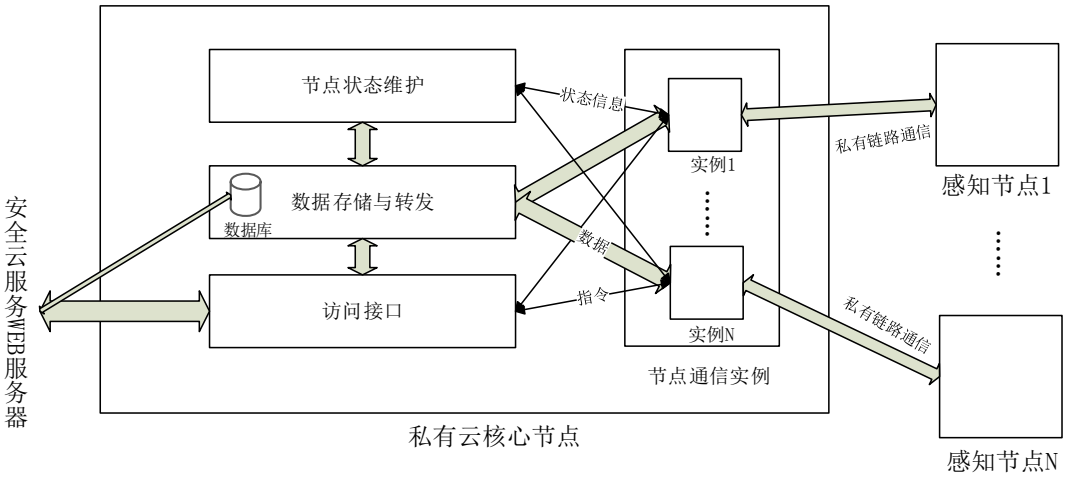

图 2.3 私有云核心节点结构图

节点通信实例负责与感知控制节点进行实际的通信交互，当核心节点启动之后，每次有感知节点连入核心节点时，核心节点自动开启一个新的节点通信实例与之进行专门的通信交互：首先通信实例开始与感知节点进行认证，通过验证节点证书进行节点可信认证，通过认证之后会话正式建立，进入数据接收等待和指令发送等待状态。每个节点通信实例只负责一个感知节点的通信工作，其功能包括定期询问感知节点的工作状态，以保证感知节点的在线与正常工作，并将节点状态信息传送给节点状态维护部分；根据配置将感知节点传回的数据以正确的格式写入数据库、写入文件系统或丢弃；接收访问接口所发来的用户指令，并根据指令向相应的感知节点下达特定的指令。

节点状态维护模块负责实时维护连接到私有云核心节点的各感知节点的工作状态，动态维护一张包含各个节点状态的表格。具体来说当每个新的节点通信实例创建以后向本模块发送信息，提示新的感知节点开始与核心节点进行连接，本模块将向所维护的节点状态表中插入新行，节点状态被初始化为发起连接，当节点通信实例与感知节点认证结束并正式建立连接时再次向本模块发

送信息报告连接建立的完成，本模块将更新状态表中对应节点信息的状态为已连接，之后每次节点通信实例定时向感知节点进行状态询问后都将自动向本模块发送信息报告节点的最新状态，当一个感知节点被报告离线后，本模块将从所维护的节点状态信息表中删除相应节点的数据行。

数据存储与转发模块包括存储转发模块以及数据库，负责对各个感知节点所发送的数据进行汇总处理，根据配置情况以及用户的指令，分别对不同的数据进行入库存储以及直接转发等不同的处理。对于各个节点采集到的环境感知数据，一般根据系统配置，本模块会选择加入节点标记与时间戳后直接存入数据库，对于根据用户指令获得的特殊数据如摄像头图片采集数据，则在数据库记录后写入文件系统，并将存储路径返回到用户接口，对于根据用户指令进行采集的实时视频数据，本模块将直接对原始视频数据进行可选的编码后开启一个新端口直接传输数据到相应的用户接口中。同时，本模块中的数据库除存储相关数据外，还可以直接供安全云服务 web 服务器通过只读帐号直接进行数据的读取，方便了 web 服务的开发。

访问接口模块主要向用户提供一组可供操作的接口，以实现对于感知节点的控制。具体来说本模块以管道或是本地端口的形式建立访问接口，并提供一组可选的操作指令，当用户通过上述接口调用特定的操作指令时，本模块将自动将指令转换为各个感知控制节点所提供的控制接口指令并通过相应的节点通信实例向节点发送指令，实现对节点的控制。

2.4 安全云服务

安全云服务在本系统中是由 web 服务器向用户提供的一组服务，用户需要通过使用虚拟专用网（VPN）连接到本系统后才可以访问相应服务，由此保证了数据传输的安全性与可靠性。

本组服务主要包括用户认证与授权、数据读取、指令下发三大部分。

用户认证与授权部分主要提供对用户身份的验证，用户使用用户名和密码登录系统后，系统为用户自动分配会话 ID 并存储用户的身份信息以及用户类型，在之后的服务访问过程中，特定服务将会使用保存在会话中的用户授权信息判断用户是否有足够权限使用该服务。

数据读取部分主要提供面向用户的对各感知控制节点实时采集的环境信息数据的查看以及对在数据库中所保存的历史数据的访问以及汇总展示。不同权限的用户根据系统配置所能查看到的信息数量和类型将会有所区别。同时该部分也提供对于类似视频监控数据的实时查看功能，用户可以通过嵌入式的 web 网页视频播放器查看实时视频数据。

指令下发部分主要向用户提供对于各个节点的控制功能，当用户通过 web 服务向相应节点下发指令后，系统将会自动以管道方式或是本地端口 socket 通信的方式向私有云核心节点下发相应指令，核心节点再向指定的感知控制节点下达具体的操作指令，感知控制节点收到指令后作出相应动作，最终实现用户所需要的功能。

3 系统安全通信设计

3.1 系统通信结构概述

本系统的通信结构从宏观上来说分为私有云内部与外部两大部分，其中私有云外部是系统的终端使用者从互联网链路连接至云端进行云服务访问的部分，即从终端用户连入系统安全云服务部分的通信链路，而云内部的通信则主要是云端各节点之间的通信，即私有云核心节点与感知控制节点之间的通信链路。其通信结构示意如图 3.1 所示。

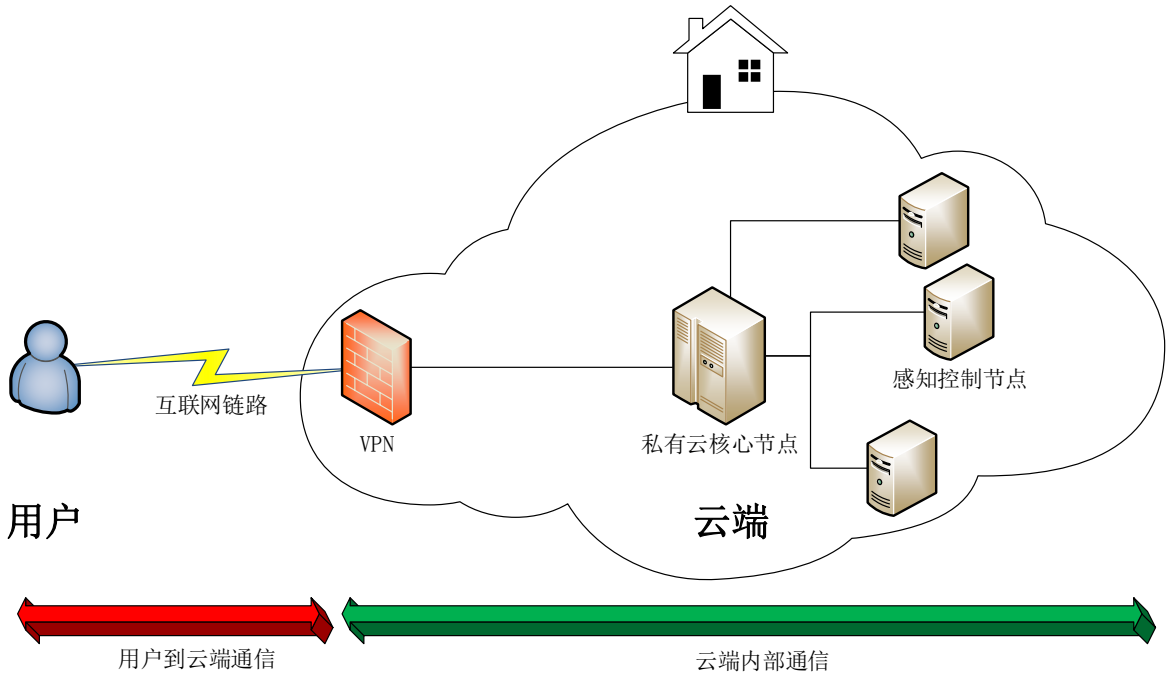

图 3.1 系统通信结构示意图

从系统结构来看，系统两大部分的通信链路所处环境是有较大差别的。由于在多数情况下系统的终端用户通过互联网接入云端并使用云端所提供服务，故其中用户到云端的通信链路通常情况下是需要跨越互联网的，而云端各节点包括私有云核心节点与感知控制节点，通常情况下则是部署在可信的局域网环境中比如使用者的家居环境中，该私有网络环境一般需要通过路由器与互联网相连接，从网络拓扑的角度已经实现了一层网络的分割，同时由于家用局域网一般使用私有地址进行网络规划与部署，对于互联网访问者来说其内部细节是不可见的，天然的形成了一定的隔离。而局域网内部的各个节点则通过局域网链路进行连接，除安全云服务需要以web服务的形式向互联网暴露访问接口外，

其他各个节点均不对外开放。

3.2 系统安全通信方案概述

针对本系统所涉及的用户到云端通信、云端各节点间通信两种不同的通信形式，本方案对其二者的通信链路特点、通信所需实现的目标和适用方案分别进行了分析,并选择了不同的方案进行实现，如图 3.2 所示。

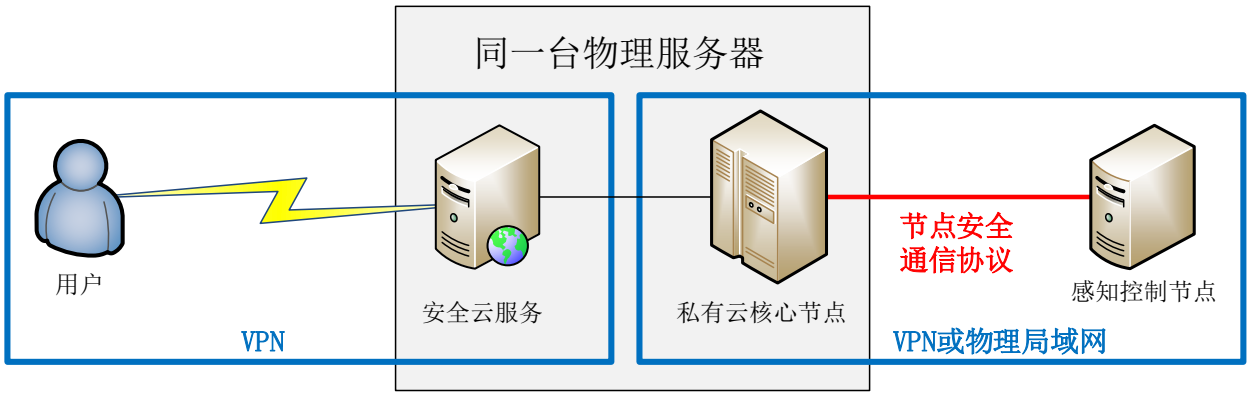

图 3.2 系统安全通信示意图

其中用户到云端的通信跨越了互联网链路，而通常意义上互联网链路是不可信的，具有被攻击的极大可能，为保证链路的安全，该部分的安全通信方案采用了使用加密链路进行通信的方式。由于链路整体的不可靠特性，在跨越互联网进行安全通信时较为安全的做法是使用 VPN 即虚拟专用网技术，建立从客户到云端跨越互联网的安全通信链路，故而在此处使用 VPN 技术方案保证通信的安全性。

而云端内部的通信情况要根据网络的部署方式分为两种情况进行讨论。当云端各个节点直接部署在同一局域网内部时，其通信链路不须跨越互联网，可以认为是部分可靠的，不会受到外部的直接攻击，而当云端各个节点是各自直接接入互联网进行通信时，由于互联网网络链路的不可靠，首先需要通过部署 VPN 并将各个节点全部接入到同一 VPN 中来保证通信的安全可靠,同时通过 VPN 技术各个节点在接入统一 VPN 后可以认为其处在同一局域网内。当云端内部节点通过 VPN 形成局域网或是直接部署在同一物理局域网络内部时，为了保证节点间的通信不会受到来自局域网内部的攻击，其通信不应使用明文进行，而考虑到物联网节点性能的局限性、单次通信数据的数据量小但通信频繁等特点，故而不适合使用已有的大型通信协议，在本方案中，为解决云端内部节点间的通信安全问题，专门设计了适合其进行通信的安全通信协议，用以保证其通信的安全可靠。

3.3 用户到云端的安全通信

3.3.1 技术背景

1)虚拟专用网 VPN

虚拟专用网（Virtual Private Network，简称 VPN），是一种常用于连接中、大型企业或团体与团体间的私人网络的通讯方法。虚拟私人网络的信息通过公用的网络架构（如互联网等）来传送局域网的网络信息。它利用已加密的通道协议（Tunneling Protocol）来达到保密、发送端认证、消息准确性等私有信息安全效果。这种技术可以用不安全的网络（例如：互联网）来发送可靠、安全的消息。需要注意的是，加密消息与否是可以控制的。没有加密的虚拟专用网消息依然有被窃取的危险。

2)点对点隧道协议 PPTP

点对点隧道协议（英语：Point to Point Tunneling Protocol，缩写为 PPTP）是实现虚拟专用网（VPN）的方式之一。PPTP 使用传输控制协议（TCP）创建控制通道来发送控制命令，以及利用通用路由封装（GRE）通道来封装点对点协议（PPP）数据包以发送数据。这个协议最早由微软等厂商主导开发，但因为它的加密方式容易被破解，微软已经不再建议使用这个协议。

PPTP 的协议规范本身并未描述加密或身份验证的部分,它依靠点对点协议（PPP）来实现这些安全性功能。因为 PPTP 协议内置在微软视窗系统家族的各个产品中，在微软点对点协议（PPP）协议堆栈中，提供了各种标准的身份验证与加密机制来支持 PPTP 。 在微软视窗系统中，它可以搭配 PAP、CHAP、MS-CHAP v1/v2 或 EAP-TLS 来进行身份验证。通常也可以搭配微软点对点加密（MPPE）或 IPSec 的加密机制来提高安全性。

3.3.2 通信方案介绍

本系统在用户到云端的通信过程中选择使用由 PPTP 协议实现的 VPN 技术来保证用户跨越互联网访问云端时的通信安全。

具体来说，当用户需要从互联网中的某个节点通过公网链路接入云端服务时，需要首先与云端建立一条加密的 PPTP VPN 链路，在用户与云端之间形成一条加密的通信链路，实现避免来自公网攻击的目的。由于云端向用户所提供的是 web 服务，用户在通过 VPN 接入云端后实际上通过 VPN 与 web 服务器进入了同一虚拟局域网内部，此时用户不需要其他配置即可如访问本地网内服务器一样安全的访问云端 web 服务。

此处需要着重注意的是用户接入云端的 VPN 连接只包含用户与 web 服务器,与私有云核心节点在网络上是不能直接连接的,若云端节点间也是通过 VPN 跨越互联网进行连接的，此 VPN 与云端节点之间所使用的 VPN 是两个相互隔离的网段，不能互通，保证来自用户的任何访问或攻击不能到达云内部。特别是当系统部署为 web 服务器与云核心节点在同一物理服务器上时，需要通过设置使 web 容器与核心节点分别处在两个不同且隔离的局域网中，二者的通信方式

只能是借助由系统提供的命名管道来进行有限的数据交互，以保证云端的安全可靠。

3.4 云端各节点间的安全通信

3.4.1 技术背景

1) 良好隐私密码法 PGP

良好隐私密码法（Pretty Good Privacy，缩写为 PGP），一套用于信息加密、验证的应用程序，采用 IDEA 的散列算法作为加密与验证之用。

PGP 的主要开发者是菲尔·齐默尔曼（Phil Zimmermann）。齐默曼于 1991 年将 PGP 在互联网上免费发布。PGP 本身是商业应用程序；开源并具有同类功能的工具名为 GPG（GnuPG）。PGP 及其同类产品均遵守 OpenPGP 数据加解密标准(RFC 4880)。

PGP 加密由一系列散列、数据压缩、对称密钥加密，以及公钥加密的算法组合而成。每个步骤支持几种算法，可以选择一个使用。每个公钥均绑定唯一的用户名和/或者 E-mail 地址。这个系统的第一个版本通常称为可信 Web 或 X.509 系统；X.509 系统使用的是基于数字证书认证机构的分层方案，该方案后来被加入到 PGP 的实现中。当前的 PGP 加密版本通过一个自动密钥管理服务器来进行密钥的可靠存放。

PGP 可以用来发送机密消息。这是通过对称的一组密钥-公钥组合来实现的。消息采用对称加密算法加密，采用一组对称密钥。每个对称密钥只使用一次，所以也叫做会话密钥。会话密钥通过接收方的公钥来加密保护，因此只需确保仅接收方能解密会话密钥即可。加密的消息和加密的会话密钥一起发送给接收方。

PGP 支持消息认证和完整性检测。完整性检测被用来检查消息在传输过程中是否变更过（即验证消息完整性），而消息认证则是被用来决定消息是否确由某特定的人或实体发出（即数字签名验证）。在 PGP 中，这些特性默认是和消息加密同时开启的,而且同样可以被应用到明文的验证。发送者只需使用 PGP 为消息建立一个数字签名（签名算法采用 RSA 或 DSA）。具体步骤为：PGP 以数据或信息建立一个散列，然后使用发送者的私钥利用散列生成数字签名。

2) 传输层安全协议 SSL

传输层安全协议（Transport Layer Security，缩写为 TLS），及其前身安全套接层（Secure Sockets Layer，SSL）是一种安全协议，目的是为互联网通信，提供安全及数据完整性保障。在网景公司（Netscape）推出首版 Web 浏览器的同时提出 SSL，IETF 将 SSL 进行标准化，1999 年公布了 TLS 标准文件。

SSL 包含记录层（Record Layer）和传输层，记录层协议确定了传输层数据的封装格式。传输层安全协议使用 X.509 认证，之后利用非对称加密演算来对通信方做身份认证，之后交换对称密钥作为会谈密钥（Session key）。这个会谈密钥是用来将通信两方交换的数据做加密，保证两个应用间通信的保密性

和可靠性，使客户与服务器应用之间的通信不被攻击者窃听。

SSL 在服务器和客户机两端可同时被支持，目前已成为互联网上保密通讯的工业标准。现行的 Web 浏览器亦普遍将 HTTP 和 SSL 相结合，从而实现安全通信。

3.4.2 通信方案介绍

云端内部的通信是系统中最为核心的数据通信链路，根据不同的部署方式，云端各个节点之间分为部署在同一物理网络中与通过互联网进行连接两种情况。

当云端各个节点部署在同一物理网络中时，只需保证该物理网络与外界完全隔离即可，保证网络中只有本系统私有云核心节点与感知控制节点的存在，且通信仅限于二者之间进行，所有节点不得向外提供直接的网络访问接口。

若云端各个节点是部署在不同的物理网络中并通过互联网相连接，则为了保证节点间通信的可靠，首先需要部署 VPN 虚拟网络，通过 VPN 将各个节点连接到一起，组成虚拟局域网，该 VPN 内需要仅存在核心节点与感知节点，不允许除此之外的网络节点存在，同时通信仅限于该二者，不允许任何节点向外部提供直接的网络接口。

在云端通过物理部署或借助 VPN 技术搭建的局域网内部，感知控制节点与私有云核心节点共同构成了智能家居系统云服务部分的基础设施，这两大部分的通信效率与安全性是整个系统安全高效运行的重要保障，同时也是本系统整个安全体系中最为重要的一环，为保证其通信的安全高效，本系统在感知控制节点与私有云核心节点的通信过程中除借助局域网作出限制外，进一步地使用了专门设计的专用安全通信协议，以避免包括冒充、截获等安全问题。该协议是基于 UDP 通信协议的传输层通信协议，使用非对称加密协议进行通信各方的可信认证、通信密钥交换与数字签名，之后使用对称加密保证通信过程的安全可靠，并通过维护虚会话来监控系统中各个节点的运行状态与连接情况，能够保证通信过程的安全高效。

3.5 节点间安全通信协议

3.5.1 协议概述

节点间的安全通信协议是本方案为保证云端各个节点之间的通信安全而专门设计的一套通信方案，该方案参考了现有的 PGP、SSL 等安全解决方案，基于无连接的 UDP 协议，并在参考其他安全解决方案的基础上根据物联网网络节点通信的特点进行设计，使得该协议能够适用于物联网节点性能有限、单次通信数据少、数据通信频繁且需要随时感知节点状态信息等特点。

在该通信协议中，涉及到的各方包括虚拟的 CA 认证中心、感知控制节点与私有云核心节点，涉及的证书包括虚拟 CA 根证书、通信各方所使用的节点通信证书，涉及到的概念包括虚拟 CA 的公私密钥对、各个通信节点的公私密钥对、虚会话、会话通信密钥。

3.5.2 CA

虚拟的 CA 认证中心是本通信系统中可信任关系的起点，在本系统中的所有各方均需无条件的承认该 CA 的可信性。该 CA 在物理上是不存在的，实际上在整个系统中该 CA 仅包括一组预先生成的非对称加密公私密钥对，该组密钥由系统的开发与部署人员所掌控。

虚拟 CA 的功能包括生成根证书与向各个节点颁发通信证书。

3.5.3 根证书

CA 根证书由虚拟 CA 密钥中的公钥来制作，并在系统部署前需将其预置入各个感知控制节点以及私有云核心节点中，各节点无条件将其作为已知的可信关系起点。除了发布根证书外，该 CA 也负责为各个节点颁发其在通信过程中需要使用的通信证书,CA 密钥对中的私钥便用于对向各个节点颁发的通信证书进行签名，签名分发后该证书便可供各个节点在通信中用来进行可靠性验证、通信会话密钥的交换以及数字签名。

3.5.4 通信节点

通信中私有云核心节点与感知控制节点的地位是对等的，在节点部署完成之后由 CA 负责给各节点生成一个唯一的节点 ID 以及一对公私密钥，并利用该密钥对中的公钥生成其通信证书，然后使用 CA 私钥对证书进行签名。各节点通信证书的完整内容包括该节点的唯一 ID 字符串（该 ID 也用作该证书的序列号）、节点类型、节点非对称加密公钥、由利用其私钥对该证书进行的签名。节点通信证书和由 CA 颁发的根证书需要在节点进行部署时一同置入节点的服务程序实例中。在各个节点间进行通信时需要首先进行通信证书交换并互相使用其自身内置的根证书验证对方通信证书的有效性，通过验证后双方才可以建立并开启此次会话，之后共商会话通信密钥，在本次会话中后续的通信均通过此密钥完成，直至节点离线宣告会话结束。

为了保证通信的高效性，同时考虑到各个感知控制节点在性能上的限制性、各个节点在能耗方面的要求、通信网络扩大后节点间通信数据的增大对网络的负载要求以及单个核心节点所能支持感知控制节点的数量，在该安全通信协议中，各个节点的通信均使用 UDP 协议进行，同时为了保证节点之间会话的延续性以及核心节点对各个节点状态的监控，由各个节点通过会话通信密钥维护一个虚会话，核心节点通过定期对与其建立会话的感知控制节点进行状态查询保证能够实时得到节点的活动状态。

3.5.5 节点证书的生成与结构

在本协议中，每个通信节点必须具有其独一无二的节点通信证书，该证书既用于节点身份的认证，也用于通信中部分数据的加密和数字签名。

节点的通信证书由虚拟 CA 在整套系统进行部署之前在技术人员的操作下为每个节点生成，再由部署人员将每个节点的证书置入节点设备中，完成各个

节点证书的部署。

虚拟 CA 在整个系统部署之前进行初始化，其包括一对用于 RSA 加密使用的非对称加密密钥对，密钥长度在此处选择 1024 位。

每个节点的通信证书由节点 ID、节点类型、节点的非对称加密密钥对、CA 对该证书的数字签名、CA 的公钥构成，证书使用文本文件保存，字符的编码方式均为 ASCII 码。各个部分的具体说明如下：

1) 节点 ID：节点 ID 是由小写英文字母和数字组成的一串随机字符串，长度为 16 个字符，用于唯一的标识一个节点，同时该 ID 也是节点通信证书的证书 ID。
2) 节点类型：节点类型使用一位数字进行表示，0 代表核心节点，1 代表感知节点。
3) 节点的非对称加密密钥对：一组在生成证书时由 CA 生成的一对用于 RSA 加密算法运算所使用的非对称密钥对，长度为 1024 位。
4) 数字签名：由 CA 对该证书进行的签名，即使用 CA 的私钥对该证书中前三个字段进行加密后得到的密文结果。
5) CA 的公钥：即 CA 的公钥，用于本节点对其他节点证书的校验。

3.5.6 包结构

由于本通信协议基于 UDP 协议，并由于 UDP 协议依赖于 IP 协议，故本协议的包结构均在 UDP 数据报的基础上进行设计，封装在 UDP 数据报中，并进一步的包含在 IP 数据包和帧中。本协议的数据包位置在整个网络通信体系数据的封装结构中位置如图 3.3 所示。

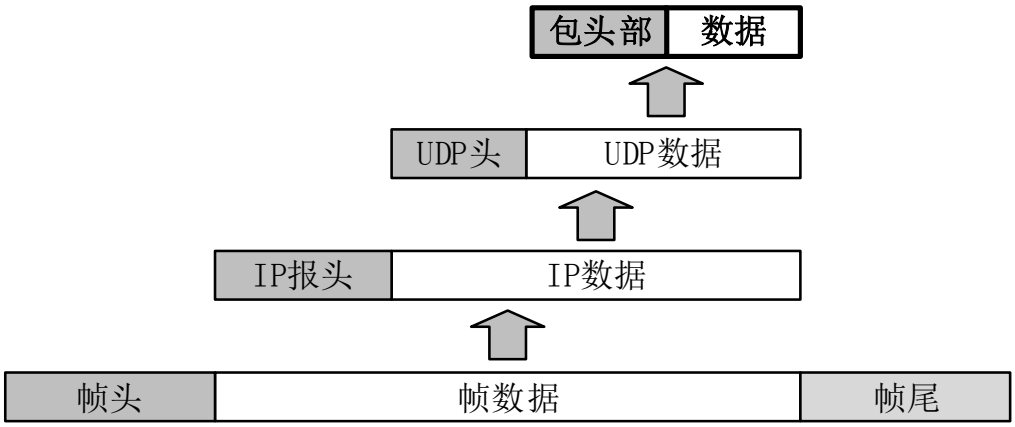

图 3.3 节点间安全通信协议数据包层次示意图

本协议的数据包基础结构分为包头部与正文数据两大部分，其中头部数据属于描述性元数据，主要对本次通信所产生的数据包结构、功能进行说明与描述。而消息正文数据部分则为本次通信所使用的具体通信数据,包结构如图 3.4 所示。

<table>
<tr><td rowspan="2">消息头部</td><td>标志位(4)</td><td>会话ID(16)</td><td>通信方向(1)</td><td>源ID(16)</td><td>时间戳(10)</td><td>数据长度/密钥长度(6)</td></tr>
<tr><td>加密方式(1)</td><td colspan="4">消息验证码(16)</td><td>空白填充(10)</td></tr>
<tr><td rowspan="3">消息正文</td><td colspan="6">加密内容片段(1024)</td></tr>
<tr><td colspan="6">……</td></tr>
<tr><td colspan="6">加密内容片段(1024)</td></tr>
</table>

图 3.4 数据包结构示意图

数据包的头部数据又包括了以下 8 个字段，各个字段的内容如表 3.1 所示。

表 3.1 数据包头部字段描述表

字段名	字段描述
协议标志位	用于标记本协议及数据包起始位置
会话 ID	用于通信双方识别本次会话
方向	用于说明数据包的发送方向
源节点 ID	用于标记源节点
时间戳	用于标记数据包的发送时间
数据长度	用于描述数据的内容长度
加密方式	用于描述数据的加密方式
消息验证码	用于对消息进行完整性校验和数字签名

数据包头部各字段的具体取值和说明如下：

1) 协议标志位：协议标志位用于标记本协议，以方便与其他协议进行区分，其取值为固定值。同时该协议标志位标志着数据包的起始，如果通信节点收到的数据包中该标志位错误或无该标志位，则认为该数据包不合法，予以抛弃。

2) 会话 ID：会话 ID 为由核心节点所生成的一组数字 ID，用于标记和识别一个会话。

3) 方向：用于标记数据包的发送方向，包括由核心节点发送到感知节点（值为 0）、从感知节点发送到核心节点（值为 1）两种。

4) 源节点 ID：用于识别源节点，该字段由数据包的发送方将自身的节点 ID 附加到此处，用于标记发送方节点的身份，会话双方通过对比此 ID

以保证对对方的身份识别。

5) 时间戳：用于记录数据包的发送时间，以避免重放攻击。

6) 数据长度：用于记录消息正文的数据长度。

7) 加密方式：用于描述数据的加密方式，包括块加密（值为 0）和流加密（值为 1）两种类型，在终止会话时充当标志位，置为-1。

8) 消息验证码：对消息时间戳和正文进行散列计算后使用节点私钥进行加密，以保证数据的完整性并作为数字签名保证对发送方的认证。

3.5.7 会话的建立

会话过程的流程如图 3.5 所示，重点描述了建立会话、终止会话的情况。

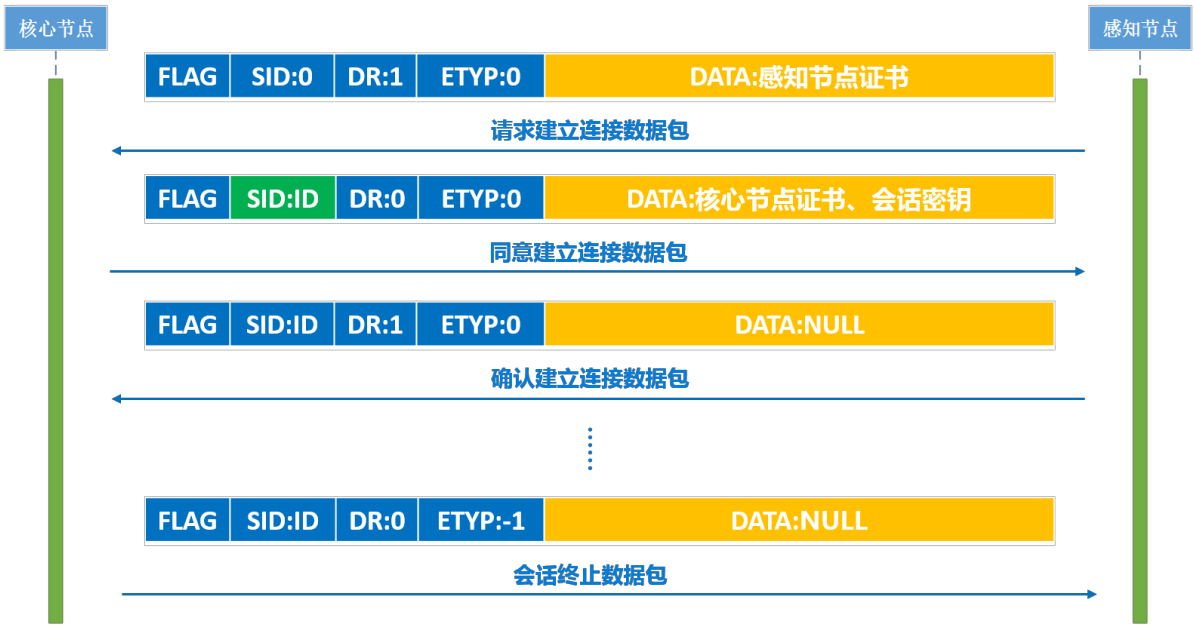

图 3.5 会话流程图

1) 会话建立的流程

建立一个新会话的过程由感知节点发起，当感知节点开始运行之后，会自动根据配置文件查找其所配置的核心节点参数，向其发起会话建立请求，然后由核心节点验证后接受请求并通知感知节点，而后感知节点再次确认，会话建立成功。整个会话的建立流程如图 3.6 所示。

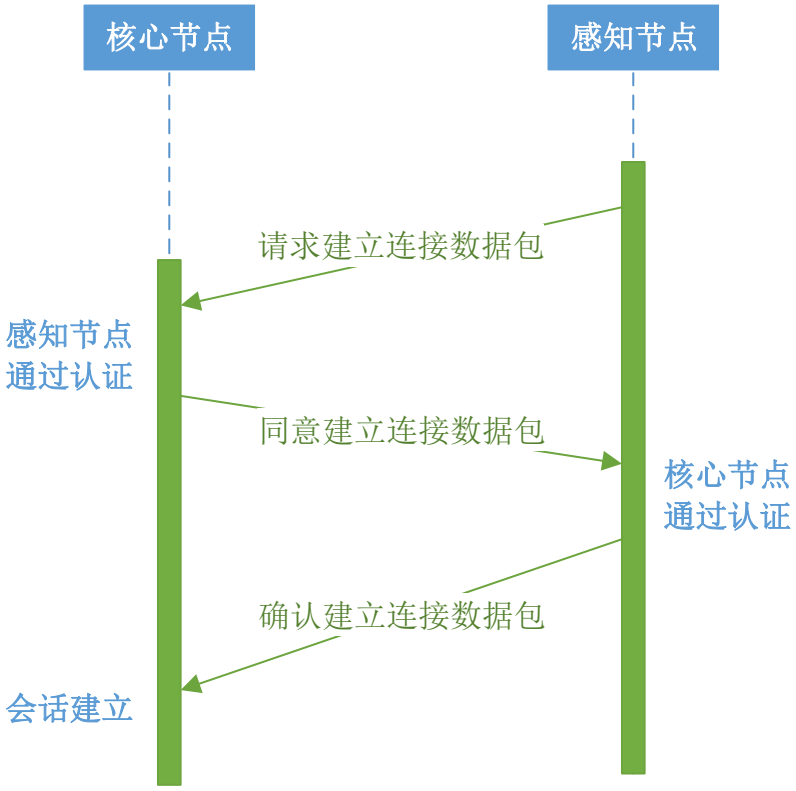

图 3.6 会话的建立流程图

具体来说建立会话包括下列步骤：

第一步：感知节点向核心节点发送会话建立请求数据包，传送其节点通信证书到核心节点。

第二步：核心节点收到会话建立请求，提取其中的感知节点通信证书进行认证，如果通过认证，进入第三步，否则向该节点发送强制终止会话数据包，会话建立失败，如图 3.7 所示。

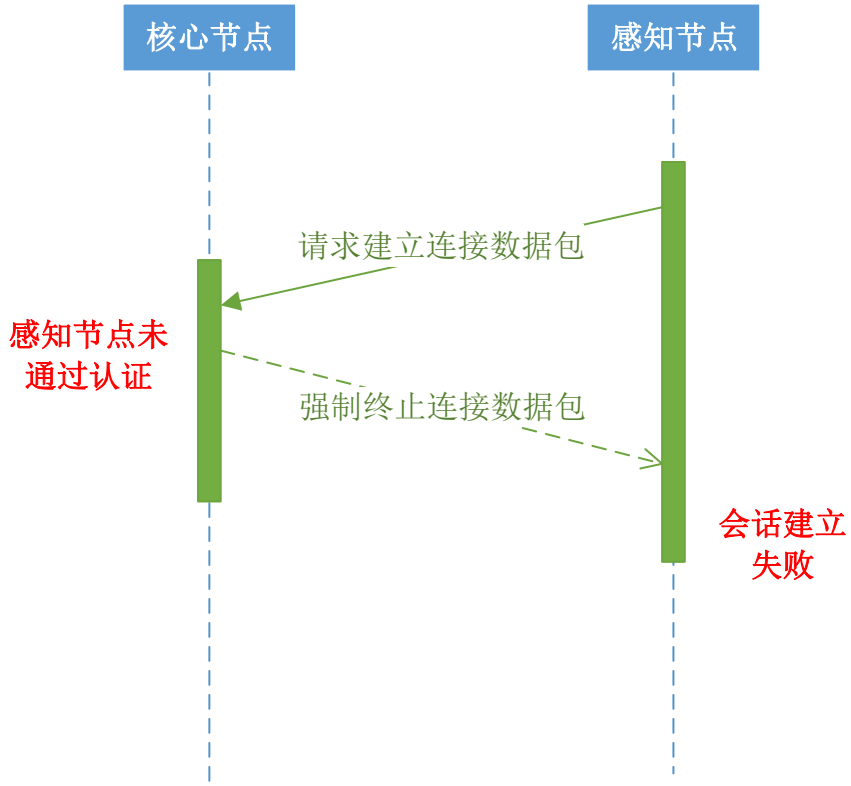

图 3.7 感知节点无法通过认证而会话建立失败示意图

第三步：核心节点记录感知节点的节点信息，生成会话 ID，生成会话密钥，并向其发送同意建立会话数据包，其中包含核心节点的通信证书、会话 ID、会话密钥。

第四步：感知节点收到核心节点发出的同意建立会话数据包，对其通信证书进行认证，如果通过认证，进入第五步，否则向该节点发送强制终止会话数据包，会话建立失败，如图 3.8 所示。

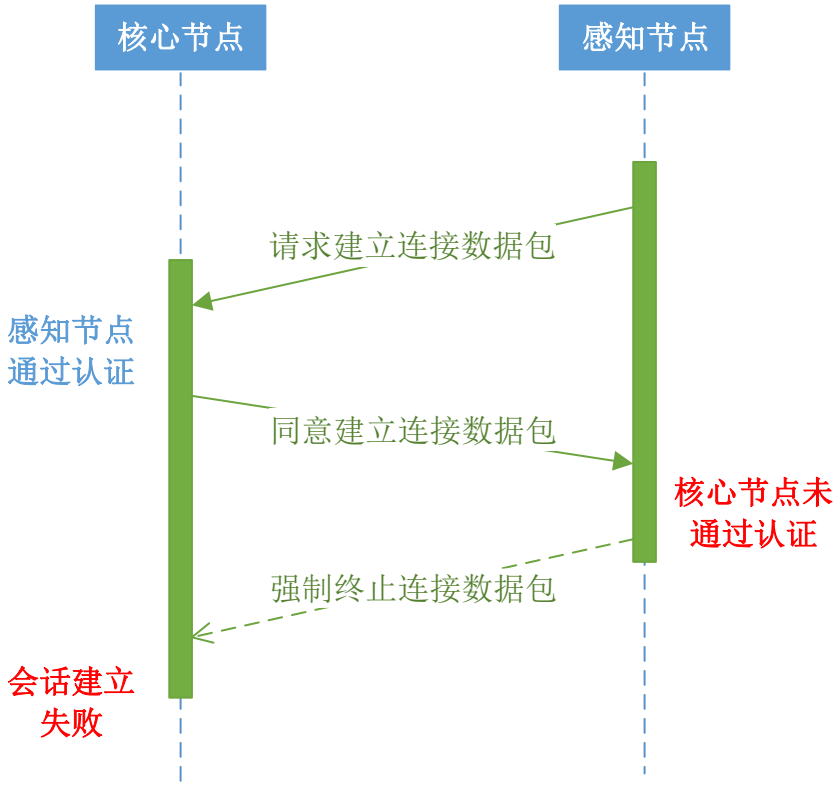

图 3.8 核心节点无法通过认证而会话建立失败示意图

第五步：感知节点向核心节点发送确认建立连接数据包，会话建立完成，如图 3.6 所示。

2) 会话建立使用的数据包结构

请求建立连接数据包：包格式如前所述，头部数据部分会话 ID 为 0，方向字段为 1，加密方式字段值为 0，数据部分包括感知节点的节点通信证书。

同意建立连接数据包：包格式如前所述，头部数据部分会话 ID 为生成的会话 ID，方向字段为 0，加密方式字段值为 0，数据部分包括核心节点的节点通信证书、会话密钥。

确认建立连接数据包：包格式如前所述，头部数据部分会话 ID 为本次会话 ID，方向字段为 1，加密方式字段值为 0，数据部分为空。

强制终止会话数据包：即会话终止数据包，见 3.5.6 会话的终止。

3) 节点的认证

核心节点与感知节点所使用的验证逻辑相同，即提取接收到的对方通信证书中的数字签名部分，使用 CA 公钥进行解密后与通过证书直接进行散列计算得到的结果进行比较，若相同，则通过认证，不同，则认证失败。

3.5.8 会话的进行

1) 会话进行的流程

会话进行中可以由任何一方向对方发送数据包，包结构中头部数据的会话

ID 为本次会话 ID，方向根据具体情况进行填充，加密方式根据具体方式进行填充。

2)会话数据的块加密

当发送普通的有格式文件或信息时，根据文件或信息的长度分块进行发送，块大小可以根据系统设置灵活调整，此时选用块加密，使用 DES 方式进行数据加密与解密。

3)会话数据的流加密

当发送流媒体音视频等流格式信息时，选用流加密方式进行数据加密，使用 RC 加密算法对数据进行加密和解密。

3.5.9 会话的终止

1)会话终止的流程

会话的终止分为两种情况：超时终止和主动终止。

在会话建立后核心节点所维护的节点状态表中记录了每个与核心节点已经建立连接的感知节点信息，且通信实例进程对其所负责的节点进行定期的询问以保证其存活。当核心节点向某个感知节点发出普通数据包或询问数据包时，若该节点在系统配置的超时时间内无应答，则核心节点认为其离线，会话终止，同时向其发送会话终止数据包，但不关心其后续回应，会话已经结束，并销毁核心节点所维护的相关节点信息。当感知节点在系统设置的询问超时时间内未收到核心节点发出的询问数据包时，认为核心节点或节点自身离线，会话终止，同时向核心节点发送会话终止数据包，且不关心其后续回应，感知节点服务进程终止或根据配置重新启动。

当通信双方某方需要主动终止会话时，可以直接向另一方发送会话终止数据包，同时直接终止会话，不关心对方的回应，收到数据包的一方立即终止会话，且向发送方回应一个终止会话数据包。主动终止会话的流程如图 3.9 所示。

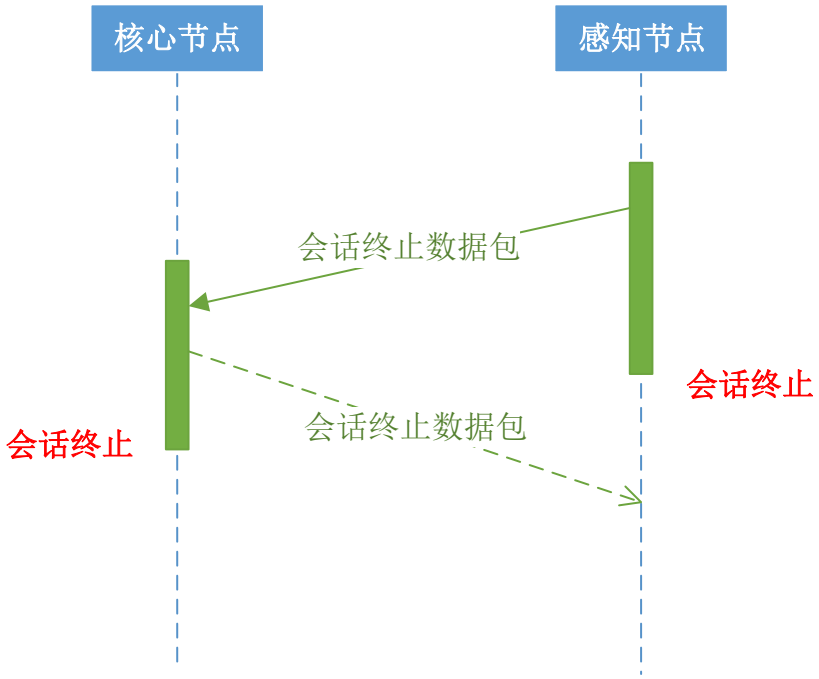

图 3.9 主动终止会话流程示意图

2) 会话终止的数据包结构

会话终止数据包即强制终止会话数据包，其结构如前描述，其中头部数据均照常填写，但加密字段值置为-1，标志会话的结束，同时包数据内容为空。

4 系统实现

4.1 系统整体实现概述

为简单实现前述的智能家居系统作为案例，本作品选取了符合前述设计的智能家居特定场景与特定设备，对系统细节作出了适当的调整与简化，借助一定设备，完成了一套基于前述设计的智能家居系统概念作品，该作品包括前述设计中的所有模块，能够正常运行并向用户提供服务。

4.2 感知控制节点与受控设备的实现

作为系统最基础部分的感知控制节点，是系统中负责与受控设备直接进行通信的重要部分，起到承上启下的作用，在本系统中，感知控制节点与受控设备的硬件部分选用目前较为流行的树莓派开发板以及部分传感器作为感知控制节点和受控设备，选用锂电池进行供电，保证不间断电源供应以及电压的稳定，整个节点如图 4.1。

图 4.1 感知控制节点与受控设备实物图

本节点核心硬件所选用的树莓派为树莓派二代产品 Raspberry Pi 2，其 CPU 为四核心的 Broadcom BCM2836 处理器，配备 1GB RAM 存储，原生带有 40pin 扩展的 GPIO 接口，支持 SD 卡读取，并且板载 4 个标准 USB 接口，以及 CSI 摄像头接口、视频、音频输入输出接口等，采用 MicroUSB 端口进行供电，电压 5v。基于以上特性，且由于其低廉的产品售价，强大的性能以及拥有其官方移

植的 Debian 系统 Raspbian 作为操作系统，该开发板非常适合作为本系统中的感知控制节点。

对于受控设备，出于简化实现的目的，系统选择了温湿度传感器和摄像头作为典型的受控设备代表来进行演示。

受控设备中的温度传感器选用了 DHT11 温湿度模块，该传感器体积小、价格低廉、精确度可以达到日常使用的要求，而且封装之后采用三针脚的结构，包括 VCC、GND、DATA 三脚，可以十分方便的接入树莓派板载的 GPIO 接口，实现对其进行直接控制与数据读取，无需额外的转换设备。

受控设备中的摄像头选用了树莓派同厂商出品的 Raspberry Pi Camera Module 模块，其感光芯片采用的是 OmniVision 公司生产的 1/4 英寸 OV5647 芯片，接口为 CSI 通讯接口，可通过软排线直接与树莓派板载的 CSI 控制接口连接。其配备的 500 万像素的图像传感器支持录制每秒 30 帧的 1080p 全高清视频，也可拍摄 2592x1944 分辨率的图片。

该节点的供电部分选用锂聚合物电池，规格为 5v 电压下容量 20AH，最大输出电流 2A，可以为节点提供长时间的稳定供电。

感知控制节点与核心节点的连接为保证稳定性，选择了有线连接，即使用五类双绞线进行网络连接。

感知控制节点的软件部分分为操作系统、节点软件两大部分。

为保证节点运行的稳定可靠，节点选择了树莓派开发板官方移植的 Debian 操作系统树莓派平台版本即 Raspbian 系统。

系统内核信息为：

Linux version 3.18.7-v7+ (dc4@dc4-XPS13-9333) (gcc version 4.8.3 20140303 (prerelease) (crosstool-NG linaro-1.13.1+bzr2650 - Linaro GCC 2014.03))

系统发行版本信息为：Raspbian GNU/Linux 7

节点软件则主要包括驱动部分与节点服务实例。

由于本节点通过使用温湿度传感器与摄像头来模拟受控设备，两种设备均不提供标准的通信协议接口，所以需要为其分别编写不同的驱动程序来满足节点服务实例的数据获取需求。其中 DHT11 温湿度传感模块通过 GPIO 针脚直接与节点开发版相连，其驱动借助树莓派 GPIO 操作库 wiringPi 可以直接进行操作，而 CSI 摄像头模块通过板载的 CSI 接口连接，其驱动借助 Raspbian 系统所提供的实用程序 raspivid 和 raspistill 分别进行视频捕获以及静态图像的捕获。

节点服务实例则选择 C++语言进行开发，由于树莓派开发板为 ARM 平台，其运行的机器码与 PC 平台机器不同，故在 PC 机所编译的可执行文件无法直接移植，本方案采用了直接在树莓派平台进行编译的方式保证其可运行。运行效果如图 4.2 所示。

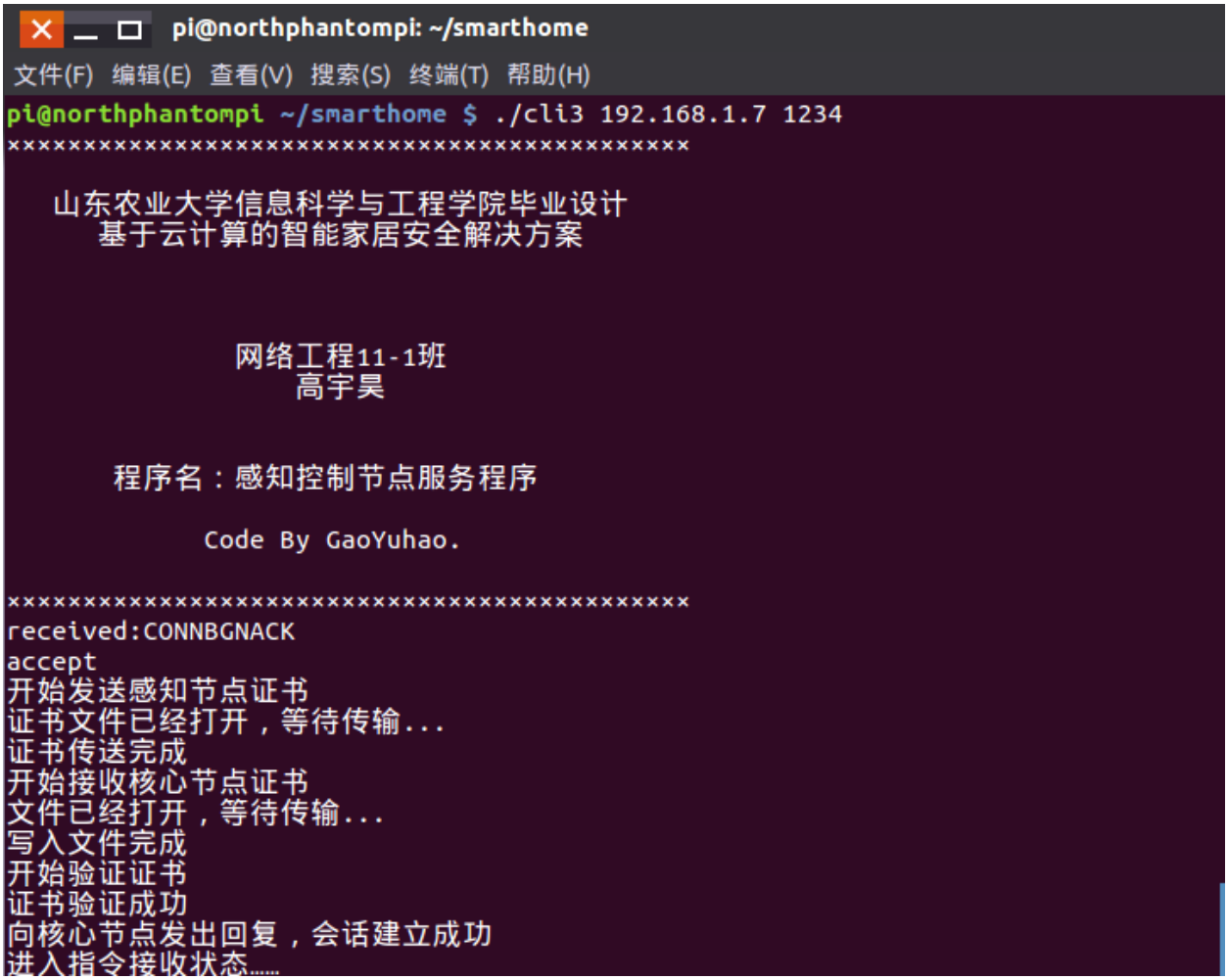

图 4.2 感知控制节点运行截图

4.3 私有云核心节点的实现

私有云核心节点作为整个系统的核心控制部分，其对于硬件设备性能有着一定的要求，故选择 PC 机作为其硬件承载，同时为保证其性能和稳定性，采用了 Linux 系统作为该节点的操作系统，采用的发行版为 Ubuntu Kylin 15.04。考虑到网络布置的需求，为保证系统部署的方便，私有云核心节点被选择部署在虚拟机当中，选用的虚拟机为 VMware Workstation 10.0.0。

操作系统的内核信息：Linux version 3.19.0-15-generic (buildd@tipua) (gcc version 4.9.2 (Ubuntu 4.9.2-10ubuntu13))

操作系统的发行版信息：Ubuntu 15.04

虚拟机配置信息：单核心 Intel i7-3770CPU，4GB 内存

核心节点的服务器软件部分由 C++语言开发，采用多进程的工作模式，对于每个通信实例开启单独的工作进程，节点状态维护模块、数据存储转发模块、接口模块均采用单独的进程进行工作。提供的对外控制接口采用命名管道的方式供用户程序（在本作品中即安全云服务模块的 web 服务器相应程序）进行操作。程序运行截图如图 4.3 所示。

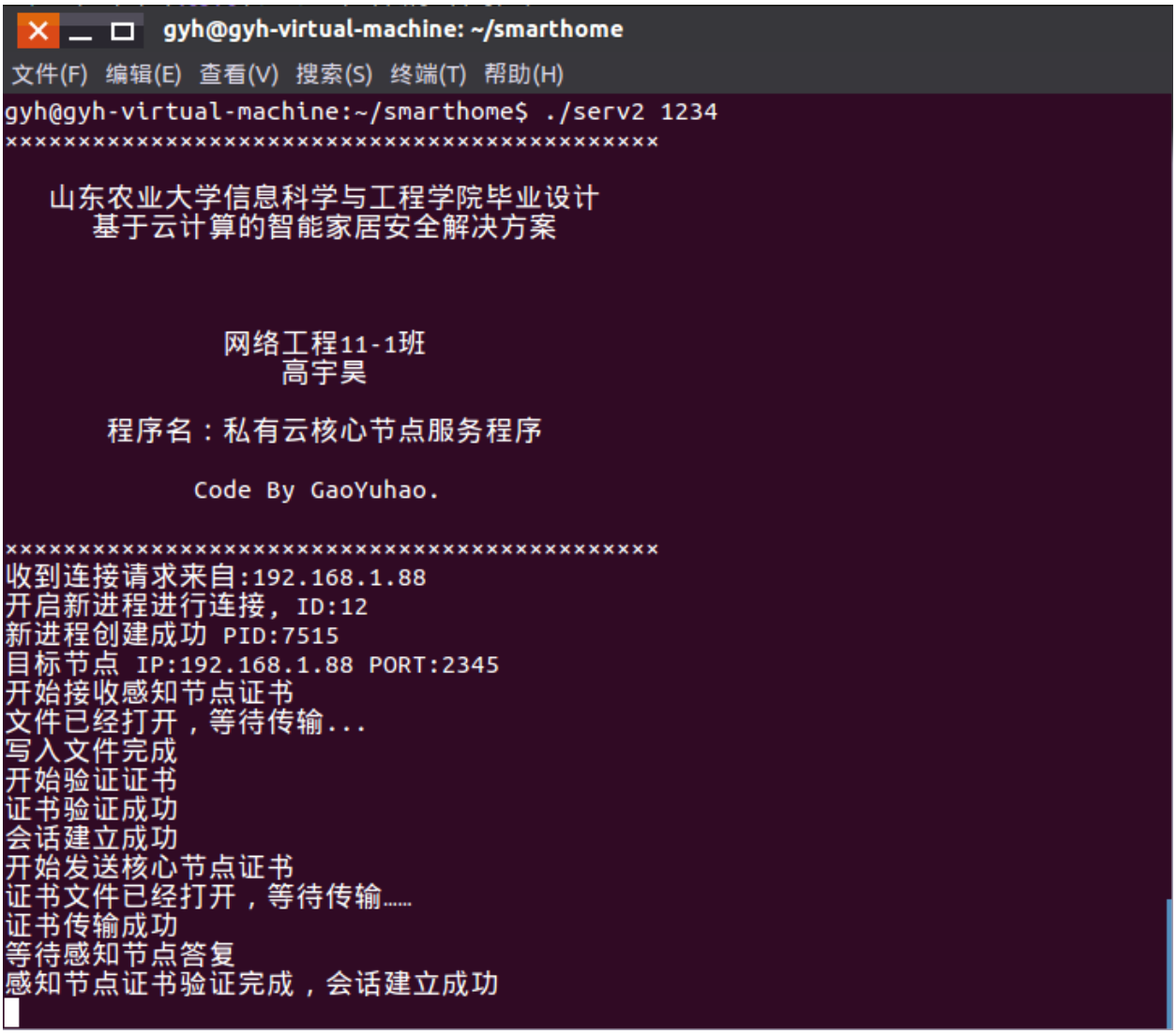

图 4.3 私有云核心节点运行截图

核心节点的数据库选择了较为流行的开源数据库 MySQL，其开源、易用、性能效率较高的特性满足作为核心节点数据库的要求。

数据库设计单一的写权限用户，只有核心节点服务器端程序具有写数据库的权限，其他客户端程序只可以根据权限读取不同表的数据。

存储数据的表结构如表 4.1 所示。

表 4.1 私有云核心节点数据存储结构表

#	字段名	类型	额外	备注
1	id	int(10)	AI	数据 ID
2	time	datetime		数据生成时间
3	node_id	text		节点 ID
4	node_ip	varchar(40)		节点 IP
5	data	text		数据内容

其中 node_ip 列考虑到未来对于 IPv6 协议大规模应用的支持，其存储空间预留为 40 个字符长度，可以保证 ipv6 协议地址 32 位 16 进制字符以及 7 位分隔符的存储需求，多余一个字符用作缓冲。

4.4 安全云服务的实现

安全云服务指的是系统通过 web 服务器以及 VPN 安全连接向用户提供的一组 web 服务，通过访问该服务，用户可以使用本系统所提供的各类功能，如查阅系统中所保存的历史数据、实时查看系统当前状态以及各个节点所采集的环境数据等。

为保证服务部署的简便快捷以及一定的性能，本系统选择流行的 Nginx 服务器作为安全云服务的 web 服务器。Nginx 是 Linux 平台上极为流行的一款 web 服务器，其以出色的性能和简便的配置方式获得诸多用户的青睐。

Web 服务器端脚本语言选择了 PHP 语言，其灵活易用且易于部署的特点非常适合本系统使用，结合 Nginx 服务器的可以快速完成安全云服务的部署与上线。同时 PHP 语言还支持用户使用 C/C++语言编写自定义的 PHP 扩展，可以方便的实现扩展语言本身所不具有的特性，对于本系统后续的升级改造、功能扩展提供了便利。

云服务数据库选用 MySQL 数据库，在本作品中由于安全云服务与可以方便的与核心节点数据库部署在同一台物理设备上，故其 MySQL 数据库可以共用同一实例，通过划分不同的数据库、配置不同的用户与权限实现访问区域的分离。

云服务与核心节点的通信在此处由于部署在同一物理服务器上，可以选择较为方便的系统命名管道通信方式，使用通信管道方式进行进程间通信可以十分方便的交换数据，其读写效率较 socket 通信方式有较大的优势，同时由于其使用标准的文件读写接口，也对于程序的开发部署和权限配置、调试等带来了极大的方便。

云服务前端页面采用标准的 html、css 语言编写，保证在各个浏览器中页面样式的兼容性，提高终端用户的使用体验。

云服务的数据用户表结构如表 4.2 所示。

表 4.2 云服务用户表存储结构表

#	名字	类型	属性	额外	备注
1	uid	int(6)	UNSIGNED	AI	用户 ID
2	user	varchar(30)			用户名
3	psw	varchar(32)			密码
4	salt	varchar(10)			盐
5	type	tinyint(1)			用户类型

其中用户密码存储字段采用 32 位 MD5 加密的方式进行存储，同时为了抵御彩虹表暴力攻击，在进行 MD5 密码加密运算时每用户进行 10 位加盐运算，

即当添加新用户时，系统随机生成十位长度的字符串作为该用户的盐值，然后利用此盐值进行密码的计算，密码生成函数为：

$$P = MD5(M + Salt) \quad （公式 4.1）$$

其中，M 表示用户输入的原始密码明文，Salt 为系统生成的 10 位随机字符串盐值，MD5 为散列函数，P 为加密后生成的密码密文。

当用户设定密码时，按照此公式计算出密码密文并存入数据库，当用户之后访问系统并申请进行认证时，系统将用户输入的密码带入验证函数进行计算，验证函数为：

$$P' = MD5(M' + Salt) \quad （公式 4.2）$$

其中 M' 为用户输入的待验证密码，P'为验证函数生成的待验证密文，系统将 P'与数据库中所保存的原始密文 P 进行比较，若相同，则用户通过验证，并根据用户类型进行相应的授权，若不符，则验证失败。

4.5 硬件结构

4.5.1 系统硬件结构概述

系统中各个硬件的连接方式如图 4.4 所示。

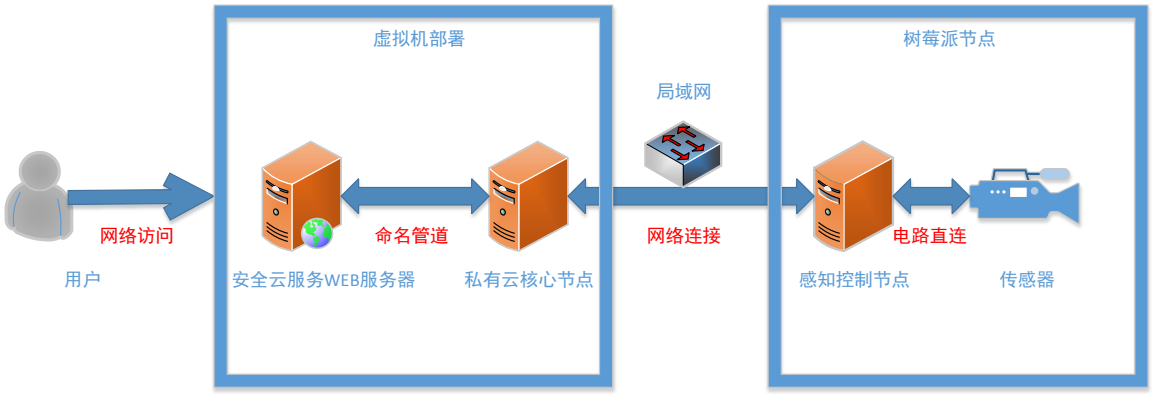

图 4.4 系统连接结构

其中，感知控制节点与摄像头之间采用 CSI 连线直接相连，与 DHT11 温湿度传感器之间采用电路连线直接相连。感知控制节点与私有云核心节点直接通过网线接入同一局域网内。私有云核心节点与 web 服务器部署在同一虚拟机内，二者之间直接采用命名管道的通信方式进行连接。终端用户则可以直接通过网络访问 web 服务器所提供的 web 服务。

4.5.2 感知控制节点与受控设备硬件结构

感知控制节点与 DHT11 温湿度传感器和 CSI 摄像头的电路连接方式如图 4.5 所示。

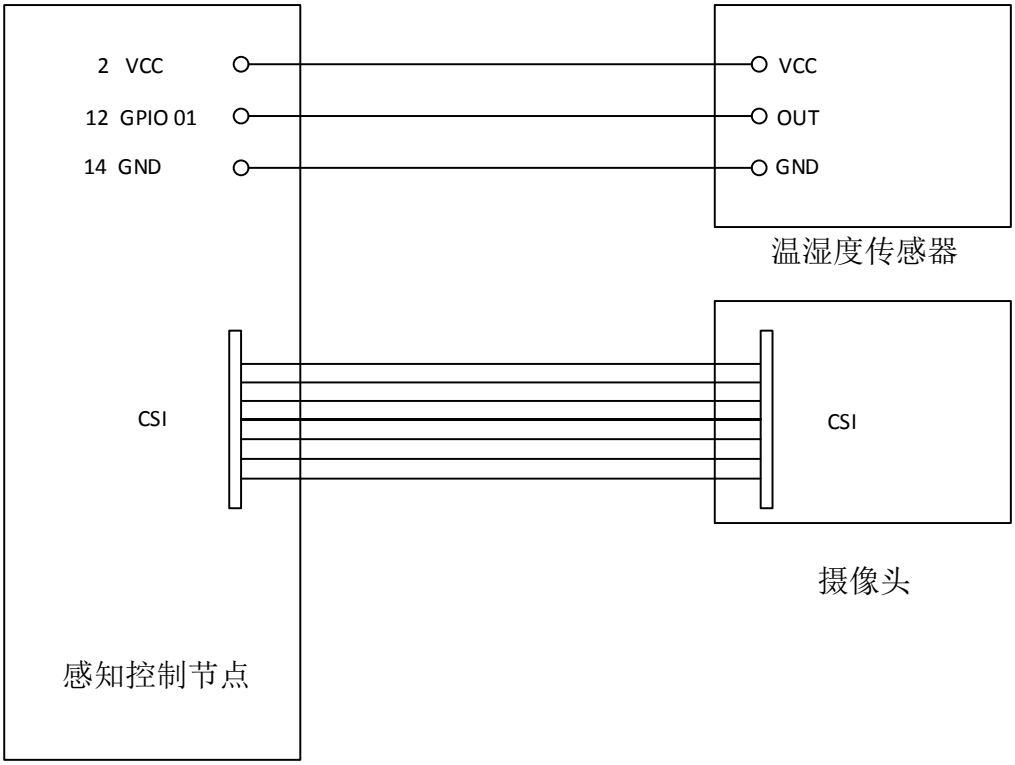

图 4.5 感知控制节点与受控设备硬件连接结构图

4.6 软件运行流程

4.6.1 感知控制节点运行流程

感知控制节点的程序实例运行情况采用活动图表示，如图 4.6 所示。

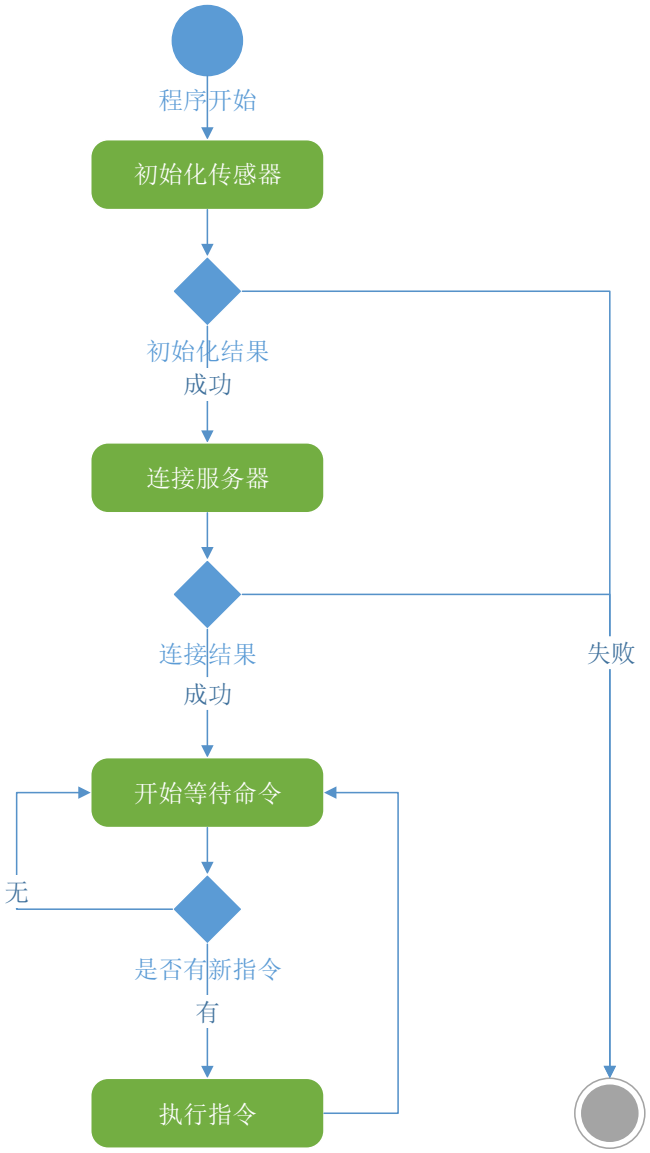

图 4.6 感知控制节点程序活动图

程序开始运行之后首先进行传感器的初始化工作，进行测试性的数据读取，传感器初始化成功后开始尝试连接服务器，连接核心节点并进行双向认证成功后开启加密通信信道，然后进入监听等待状态，等待核心节点的指令，当接到核心节点指令后则执行相应的操作。

4.6.2 核心节点软件运行流程

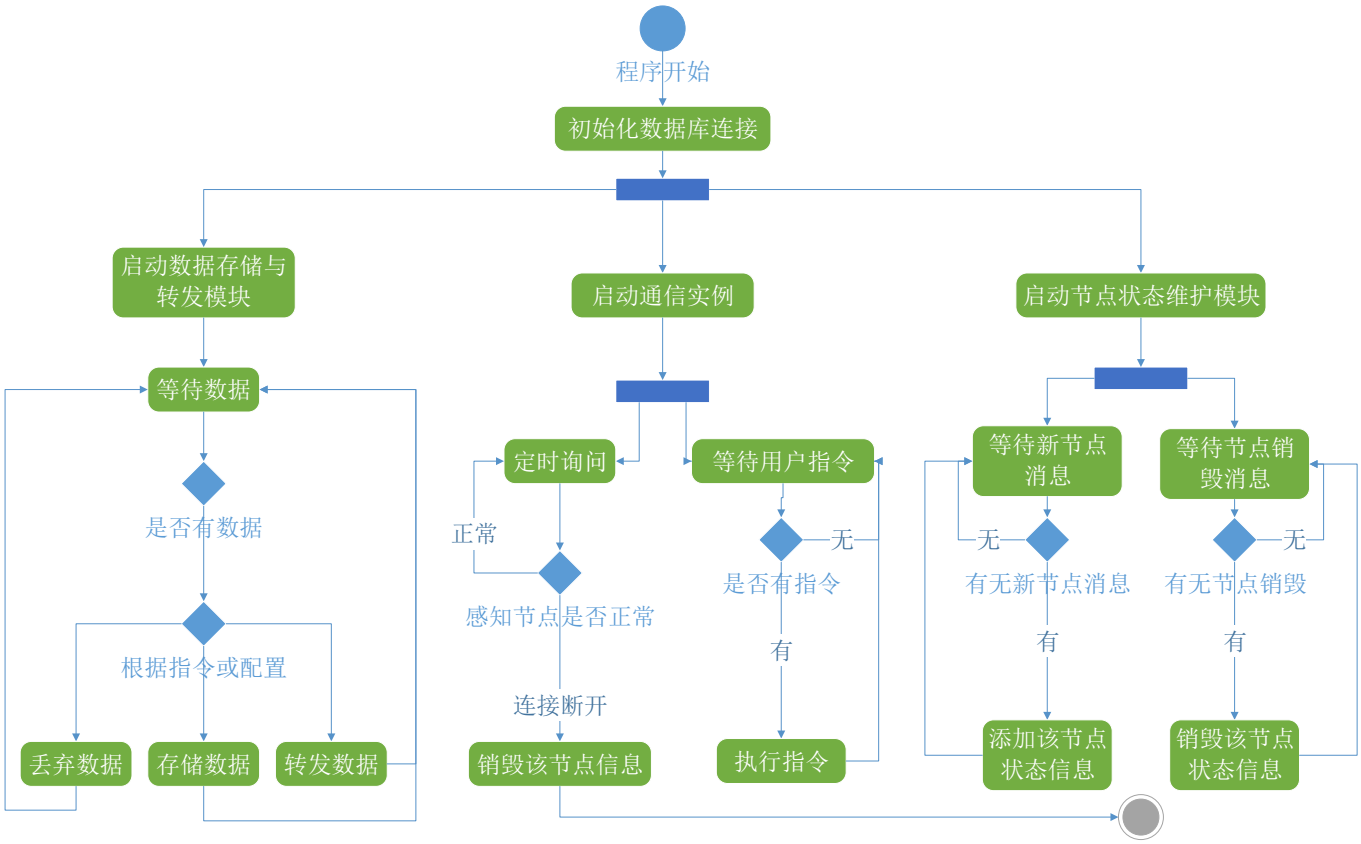

图 4.7 核心节点程序活动图

核心节点服务启动后自动开启三个进程，数据存储转发进程负责接收数据，然后根据配置或者用户指令决定将数据进行存储、转发或丢弃；通信实例当每次有新节点连入后都会新建进程，该进程定期询问节点是否正常，若出现不正常或者节点离线，则调用相关操作，终止该进程实例，该进程也随时等待用户指令，并根据指令向节点下达指令；节点状态维护进程负责维护活动节点列表，当有新节点连入消息时向表中插入新行，当有节点销毁时删除表中相应行。

4.6.3 安全云服务用户操作流程

安全云服务为 web 服务，其运行为根据用户请求进行触发，此处仅以典型的用户访问服务操作流程绘制用户登录系统后的操作，其具体流程如图 4.8 所示。

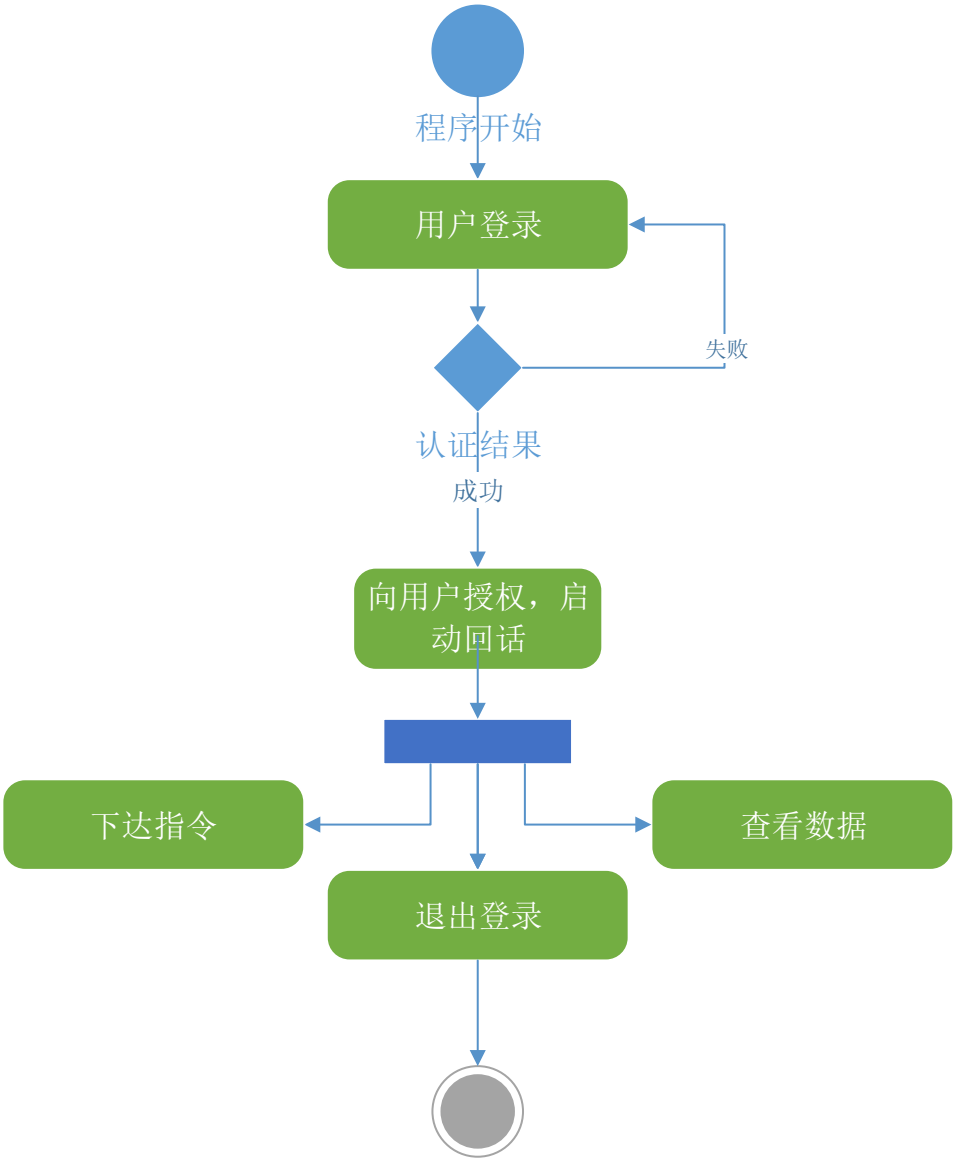

图 4.8 安全云服务用户操作

当用户试图访问 web 服务时，首先进行用户身份的认证，若认证失败，不允许访问系统其他功能，退回认证页面，若用户身份认证成功，则系统启动该会话，在会话中保存该用户的用户信息以及授权信息。同时成功登录后，用户可以访问系统所提供的各项操作，包括向连入系统的各个感知控制节点发送指令、查看当前系统状态与传感器采集到的实时环境信息、查看系统数据库中所保存的历史数据，其中查看实时远程监控视频的系统运行截图如图 4.9 所示。

图 4.9 实时视频监控运行截图

5 创新性分析

5.1 系统构架创新

系统构架的创新性主要体现在系统独特的三层结构与专门为物联网智能家居中各个节点间通信所设计的安全通信协议。

目前已有的各类智能家居产品主要包括单品与整合产品两大类。其中，单品产品往往直接接入互联网，并在同一物理设备内实现了环境信息的采集、受控设备的控制、web 服务的提供等，多种功能均混合在一起，使得设备既要做终端节点，又要承担对外服务器的角色，不仅安全性难以得到保证，同时也缺乏与其他设备联网的能力，而且使用简单单片机所开发的产品往往无法实现数据的持久化保存。而整合产品目前多是采用已有的各类互联网通信解决方案进行节点间通信，如直接使用 802.11 无线协议进行 wifi 传输或是蓝牙传输等，内容也往往是明文传输，构架上也则不具有分层的理念，各个节点与核心节点间往往是出厂前已经配对的，系统扩展性差，且核心节点所能支持的终端节点数量极为有限。

针对当前智能家居系统中存在的以上问题，本系统提出了三层构架的体系结构解决方案，对以上问题进行了改进。在三层构架中，不同的节点担任不同角色，感知节点、核心节点、安全云服务均有各自不同的工作方式和工作任务，相互之间不会形成干扰，各节点工作的单一性提高了系统整体的稳定性，同时间接提高了各个节点的性能。而采用核心节点与感知节点分离和使用无状态协议则使得系统具备了极大的可扩展性，凡是符合系统规范和通信协议的节点都可以通过获取通信证书、根证书的方式接入已有的系统，实现系统的轻松扩展。

5.2 安全特性创新

系统安全特性的创新主要体现在针对系统各个环节所可能出现的各类安全问题而采取的各类安全措施与特殊设计。

针对系统整体的安全，系统选择了使用云构架的模式来保证，具体来说，系统选择了私有云的部署模式，以核心节点和感知节点以及云服务所共同组成的整体来作为系统所提供云服务的基础设施，当用户需要使用系统时，只需通过 VPN 连入安全云服务并以 web 访问的方式就可以轻松简便的使用系统所提供的各类服务，而无需考虑系统内各个节点的技术细节，不需要直接操作各个节点。保证了用户对于系统的有限访问，同时访问借助 VPN 链接则保护了用户的访问过程安全可靠。

针对系统内部的节点间安全通信，系统使用了专门设计的安全通信协议，借助第三方证书认证的方式进行节点可靠性的检验，通过使用对称、非对称加密算法保证了节点间通信全过程的安全可信以及通信数据的私密性。

针对用户与系统的访问安全，系统通过借助用户访问时所使用的 VPN 协议

来保证用户跨越互联网对系统的访问实现安全可靠，而用户在访问 web 服务的过程中，则通过用户认证与授权和用户角色的划分来实现用户间的权限管理以及系统各类敏感数据不被非法读取。

与现有产品所存在的不进行用户身份认证、无法保证跨越互联网的通信安全性、节点间通信容易被嗅探伪造乃至可通过突破核心节点进而控制整个网络等各类安全隐患相比，以上方案较为完善的解决了各类智能家居应用中所能遇到的各类安全性问题，为保证系统的安全运行和保护用户隐私不被窃取提供了有力的支撑。

6 总结与展望

随着计算机、网络技术的突飞猛进，伴随“互联网+”概念的提出，物联网作为网络研究的前沿热点领域，受到了业界越来越多的关注，而智能家居作为物联网技术的代表性应用之一，已经开始逐步走入大众的日常生活中，智能家电、室内环境传感器、家居网络摄像头等应用层出不穷。然而由于智能家居技术仍处在发展成熟期，业界也尚未形成公认可靠的行业标准，在当今严峻的网络安全形势下，由于其部署在用户家中这一敏感环境，包含大量个人隐私信息且能够极大影响用户生活，受到了攻击者的极大关注。

为解决智能家居领域目前所存在的各类安全问题，本作品对当前较为典型的智能家居应用环境、目前常见的智能家居产品以及所面临的安全威胁进行了分析，提出了一套基于私有云技术的智能家居安全解决方案。该方案主要包括一套完善的物联网智能家居应用系统，其体系结构系针对智能家居所专门设计的三层体系结构，包括感知控制节点、私有云核心节点、安全云服务，其安全性方面则针对目前常见的安全问题进行了重点强化，同时为保证节点间通信的安全可靠，专门设计了专用的安全通信协议，对节点间的认证、通信提供了更为完善的保证，进一步提高了整个系统的安全性。

本系统由于其专门设计的体系结构及安全特性，具有易于部署、易于使用、易于扩展、安全高效的特点，适合于智能家居应用的各类场景，同时开发者可以对其进行二次扩展与开发，使其可以推广至物联网技术的各类其它应用中。

本作品包括基于私有云的智能家居系统设计方案以及一套方案的简单实现，该系统以典型的智能家居应用场景为蓝本，设计了包括温湿度传感器与摄像头的一套智能家居系统，实现了温湿度的实时监控与历史数据查看，摄像头实时拍照与实时视频监控等功能，并且依托于专用的安全通信协议和系统的体系结构，该应用具有较高的安全性与稳定性。以实例的方式展示了上述设计方案的先进性和实用性。

本系统目前对智能家居应用的使用与安全问题均进行了初步的完善，在后期的工作中可在现有系统的基础上，针对不同的需求和行业特点，进一步对本系统加以完善和修改，以满足更为广泛的使用场景。

针对智能家居消费市场的使用特点，可以进一步加强系统部署和使用的简易度，通过对通信认证协议添加自发现、自识别、联网验证等模块，力求实现设备的自动化安装部署，消费者购买相关产品后可以做到开机即用。同时可以编写内置 VPN 安全通信协议的专用 iOS 与 Android 客户端供消费者使用。

针对大规模部署的工业、农业物联网网络，本系统可以在现有基础上进一步调整系统构架，将网络通信方式由各个传感节点直接与核心节点通信的星型模式改进为节点自组织网络的通信模式，加强网络稳定性、降低网络功耗，同时改进通信协议使其适合于大量节点的快速部署。

参考文献

[1] ITU Internet Report 2005: The Internet Of Things [R].Geneva, Switzerland: ITU, 2005.

[2] Luigi Atzori, Antonio Iera, Giacomo Morabito. The Internet of Things: A survey . Computer Networks. 2010.

[3] 吴振强,周彦伟,马建峰 物联网安全传输模型[J]. 计算机学报. 2011(08)

[4] 李力行,金芝,李戈 基于时间自动机的物联网服务建模和验证[J]. 计算机学报. 2011(08)

[5] 刘洪涛,程良伦 基于 DHT 的物联网命名服务体系结构研究[J]. 计算机应用研究. 2011(06)

[6] 孙利民,沈杰,朱红松 从云计算到海计算:论物联网的体系结构[J]. 中兴通讯技术. 2011(01)

[7] 邹俊伟,吴岳辛,张晓莹 异构物联网的开放式架构研究(英文)[J]. 中国通信. 2011(01)

[8] 沈苏彬,毛燕琴,范曲立,宗平,黄维 物联网概念模型与体系结构[J]. 南京邮电大学学报(自然科学版). 2010(04)

[9] 胡向东,韩恺敏,许宏如 智能家居物联网的安全性设计与验证[J] 重庆邮电大学学报(自然科学版) 2014(02)

[10] 顾新建,代风,陈茂熙,杨青海,祁国宁. 智慧制造与智慧城市的关系研究[J]. 计算机集成制造系统. 2013(05)

[11] 崔铁良,卢许,陈援非. 基于云服务的家庭物联网智能消防系统[J]. 中国安全生产科学技术. 2012(12)

[12] 杨金翠,方滨兴,翟立东,张方娇. 面向物联网的通用控制系统安全模型研究[J]. 通信学报. 2012(11)

[13] 邓彬伟,李超. 时间序列加密智能家居安全控制系统的设计与实现[J]. 电子产品世界. 2012(09)

[14] 陈帅,钟先信,刘积学,李晓毅,邵小良. 基于 GPRS 的智能家居安全监控[J]. 计算机测量与控制. 2011(02)

[15] 宁焕生,徐群玉. 全球物联网发展及中国物联网建设若干思考[J]. 电子学报. 2010(11)

致谢

历经几个月的努力，这篇论文从零起步，经过不断地设计、规划、调整，代码的编写、调试，硬件的规划、设计，通信协议的设计、修改，到最后论文文本的撰写完成，得到了我的论文指导老师张亮教授的大量指导与帮助，他严谨的治学态度、科学的思维方式、平易近人的教学风范都给我留下了深刻印象，在这里向张亮老师表达衷心的感谢，感谢他对我本人毕业论文的悉心指导以及在过去的几年中对于信息安全团队建设的大力支持。同时感谢在论文的撰写中给予我帮助的信安团队韩晓东、孙艳涛同学，他们的耐心和友好令我受益良多。

感谢于群老师、柳平增教授，在智慧农业实验室的学习经历让我获益匪浅，两位老师在学术、生活上给予了我极大的帮助与关怀，让我的学术能力和各方面水平均有了极大的提高。感谢费玉奎教授，费老在 ACM 比赛中对我的严格要求和耐心指导令我对计算机科学的认识有了进一步的提高，费老师严谨的治学态度、刻苦认真的毅力令我肃然起敬。

此外感谢在大学四年中陪伴我一起学习生活的各位宿舍舍友、大学同学和朋友们，愿友谊天长地久。

最后，感谢我的父母一直以来对我无私的关心与支持，正是有你们作为我坚强的后盾才让我能够有今天的优越条件能够努力学习。

感谢参加评审与答辩的各位老师辛勤的工作，谢谢！