

[智能家居系统]

智能家居系统中的网络安全问题研究

文/彭楠¹ 蔺国强¹ 蔺河琿² 李丙辰³ 刘文捷³ 梁士瞳³

1. 中铁置业集团有限公司; 2. 北京邮电大学世纪学院; 3. 中建研科技股份有限公司

由于智能家居系统的组成及构架以网络通信系统协议为底层基础, 物理结构以计算机应用模块来控制末端需用设备以满足人们对日常生活的需求, 因此网络安全引起人们的关注, 怎样保护好个人隐私、家庭安全提上了日程。围绕智能家居的定义和组成、网络安全存在问题、家庭安全分析和家庭网络安全解决方案等方面进行论述, 并对未来进行展望。

随着人民生活水平的日益提高和科学技术的快速发展, 智能家居系统如雨后春笋植入了千家万户。大到空调彩电, 小到一个摄像头或传感器, 几个简单的设备就能组成一套智能家居系统, 极大地方便了人们的日常生活。调查报告显示, 未来5年中国配备智能家居系统的家庭可能会超过5亿户。随着智能家居系统的不断普及, 其网络安全性也备受大众关注, 如果网络信息安全问题得不到解决, 不仅会对现有的智能家居系统用户造成不确定的损失, 还会阻碍未来智能家居产品的普及。解决智能家居系统的网络安全问题是当务之急, 以便让智能家居系统更好地为人们服务。

智能家居系统的定义和组成

智能家居系统是利用计算机网络技术、有线或无线网络通信技术、计算机软硬件技术、安全防范技术、自动控制技术和音/视频多媒体技术等, 以家庭住宅为服务平台, 将与家居生活相关的设施嵌入集成, 构建高效优质的住宅生活设施与家庭日程事务的信息化管理系统, 大大提高家居安全性、便利性、舒适性和艺术性, 同时实现低碳节能的居住环境。

基础的智能家居系统由终端控制器(如智能手

机、iPad等)、IoT设备(如各类传感器、智能家电等)和网络三部分共同组成。用户使用终端控制器, 通过网络发送相应命令给IoT设备, 从而实现互联网和软件自动控制或远程控制等功能。智能家居系统架构如图1所示。

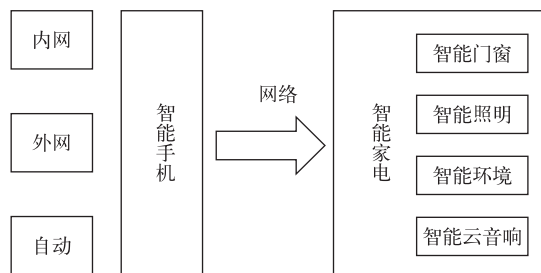


图1 智能家居系统架构

用户控制智能家居系统通常有三种方式:

- 1) 当终端控制器和IoT设备处于同一局域网时, 整个智能家居系统为全封闭状态, 用户通过内部局域网控制智能家居设备。
- 2) 当终端控制器和IoT设备不在同一局域网时, 即终端控制器处于广域网内, 用户需通过网关或路由器远程控制内部局域网中的智能家居设备。
- 3) 用户事先设定好程序, 当触发某一条件时, 智能家居系统自动运行, 例如用户设定好开关灯的

时间或者条件，智能开关根据时间或触发该条件时进行相关操作。

智能家居系统存在的网络安全问题

智能家居系统的网络安全问题主要有以下几点。

1. 设备的假身份

大多数智能家居设备都有一些特定形式的字段名称，也就是作为唯一ID或证书的设备标识符。但是，如果攻击者了解设备标识符是如何生成的，那么他们就可以计算出并克隆唯一的标识符，而這些标识符没有密码保护。鉴于唯一的标识符可以在未经许可的情况下被克隆，攻击者可以立即访问网络，并在克隆设备的帮助下部署下一阶段的攻击。比如盗取关键信息、滥用网络带宽及注入恶意程序、代码和病毒等。另一方面，验证服务器标识也是必不可少的。如果智能家居设备与恶意服务器连接，恶意服务器不仅会窃取用户的关键数据，还会导致整个家庭网络受损，甚至瘫痪。

2. 数据窃听

智能家居系统大多选择基于无线通信技术的通信接口（如蓝牙、ZigBee、WiFi等），虽然大部分无线通信技术都有相应的安全防护机制，但考虑到选择案例的局限性，稳定性并不高。例如蓝牙可能会产生借助通信接口窃听用户关键和敏感数据的风险，因为蓝牙往往依赖简单的密码进行配对。在选择加密密钥加密通信数据的同时，对通信数据的保密性和完整性有一定的保护作用。因此，保护加密密钥不被盗取、不被盗用是必不可少的。

3. 数据操作

除了存在被窃听的风险外，关键数据也会遭到恶意攻击或更改，因此智能家居系统安全的另一个关键问题是数据的完整性保护。计费信息、敏感配置数据或资源使用等重要信息不能作为操作值进行通信和存储。

4. 恶意软件感染

当攻击者进入网络后，大部分情况下都会安装恶意程序，从而使被感染的智能终端装置成为下一等级攻击的源头。此前出现在一些重大电信网络上的案例就是采用这种攻击网络的方式。只要智能家居设备受到攻击者安装的恶意程序的危害，这些设备自然会被添加到僵尸局域网连接中，并且发出分布式拒绝服

务（DDoS）攻击。不只是计算机，很多智能家居设备都将是DDoS攻击的潜在源头。如智能摄像机、家庭路由器等智能家居设备的数量要比联网计算机多得多，所以僵尸网络DDoS攻击会造成更大规模的破坏，相对来说速度要快得多。

智能家居系统安全需求分析

1. 智能家居系统安全体系结构

参考物联网技术，可以将智能家居系统的网络安全体系结构分为感知层、网络层和应用层，如图2所示。

2. 感知层的安全需求分析

智能家居系统感知层的主要作用是对外界信息进行感知和采集，类似于人的感觉器官，采集设备包括传感器和图像采集设备等，甚至是可以作为采集信息使用的GPS信息或时间信息。采集设备根据用户需求对相关数据信息进行采集。比如门窗传感器的开关信息，控制家中空调器等智能设备的开关，家庭中监控用的安防摄像头或智能窗帘在某一时段的展开和收放等。然而，在设备收集信息的过程中，也会出现监控画面被不法分子利用、监控，甚至控制用户生活、泄露个人隐私等各种安全问题，而且这种事件随着智能家居的普及将会有增无减。

智能家居系统的感知层在当前的安全挑战主要有以下六点。

- 1) 感知层的网络节点被蓄意控制（安全性全部丢失）。
- 2) 感知节点所感知的信息泄露。
- 3) 感知层的普通节点被蓄意控制（攻击者获得密钥）。
- 4) 感知层的普通节点被非法入侵（无密钥，不能被控制）。
- 5) 感知层的节点受到拒绝服务（DoS）的攻击。
- 6) 接入物联网中的海量感知节点的标记、识别、认证和控制问题。

智能家居系统中相当一部分的安全问题出现在感知层中，所以在其感知信息的过程中对信息安全的保护十分重要，关键取决于感知设备的能力。如果对感知信息的安全保护不当，攻击者就很容易获

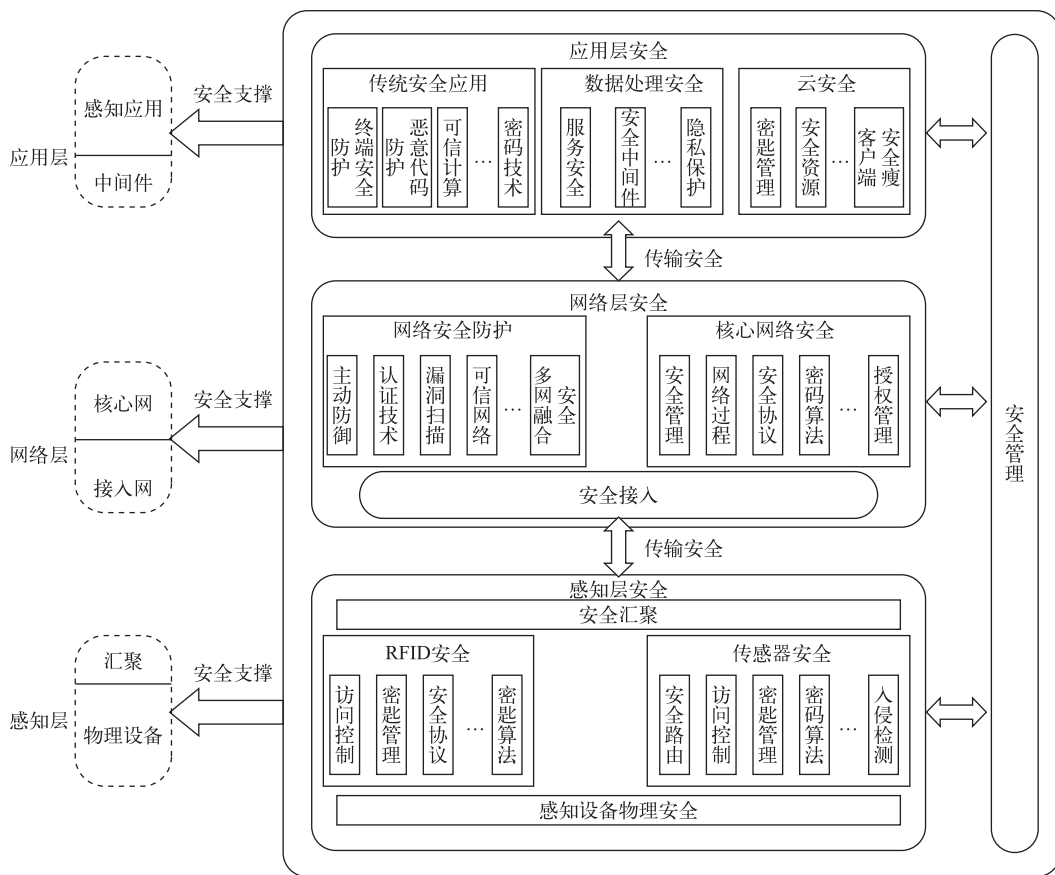


图2 智能家居系统的安全体系结构

取这些信息，因而可能造成巨大的安全隐患和威胁。由于很难获取节点密钥，攻击者一般只能入侵节点但无法控制节点，只能阻止信息的发送，系统极易察觉到。若攻击者通过某种方式得到了节点的共享密钥，便可轻松通过该密钥截获节点的信息并控制节点。攻击者通过控制节点以获取节点中的相关信息，并向系统发送错误数据。同时，有些攻击者攻击感知层的节点是为了分析确定节点的类型和用途，方便进行下一步的攻击。

结合以上分析，对感知层的安全需求分析如下：

- 1) 对于普通节点，尽量避免使用共享密钥，加强完善认证和对于密钥的管理。
- 2) 在数据通信之间采用密钥协商的形式，加强传输中数据的保护。
- 3) 当节点接入感知层时，需进行身份认证，以此避免非法节点的接入。
- 4) 使用相对高级的安全路由技术，可以保障感知层与节点和节点与节点间的安全通信。

3. 网络层的安全需求分析

作为感知层与应用层之间的直接联系，网络层将感知层接收到的信息根据需求精确地传递到应用层所需的地点。各种通信网构成了网络层的基础，保障其安全认证对于沟通不同类型的网络至关重要。由于通信网络的节点数量巨大，网络安全问题很多，如大量设备短时间内访问导致网络堵塞，攻击者可能会在此期间使用DDoS等攻击手段攻击服务器；能否在接入大量设备的情况下进行安全认证，决定着违规接入是否给网络层带来安全隐患；通过代理人攻击的方式阻止设备与网络连接，然后假装将访问请求发送给设备，这时网络就会判断错误，从而让攻击者进入到网络中。简单概括，对于网络层而言，网络安全挑战主要分为网络设备的非法访问、代理人攻击或DDoS攻击以及对传输信息进行修改、拦截和控制等。信息交换是异构网络中的网络层安全的致命点，特别是在认证方面，免不了遭受异步或合谋攻击等各种非法网络攻击，需要更加有效的安全防护措施，才能避免此类网络攻击。

的发生。不法攻击者在信息传递过程中，极有可能对相关信息进行截取甚至篡改，因此对信息采取加密防护非常关键。

网络层的安全需求：

1) 数据机密性。保证数据传输过程中不被攻击者盗取。

2) 数据完整性。保证数据传输过程中不被攻击者篡改。

3) 数据流机密性。保证数据传输过程中数据流量信息不被攻击者盗取。

4) 恶意攻击的检测。常见的攻击手段是DoS攻击，网络层需要迅速检测出DoS攻击，防止对网络造成进一步的破坏。

4. 应用层安全需求

应用层涉及的信息问题直接面对智能家居系统用户，其作用在于满足智能家居系统具体功能的需求，与其他层级的区别显而易见。因为智能家居涉及众多的设备和用户，所以应用层中需要处理大量的数据，相对来说安全性存在很多问题，例如如何保证用户数据的隐私性、完整性等。除此之外，应用层的安全还关乎位置安全、云安全等。

应用层的安全挑战：

- 1) 大量节点设备的身份认证问题。
- 2) 大量节点数据存储的安全问题。
- 3) 大量用户数据的隐私保护问题。
- 4) 系统的可控性。
- 5) 系统对恶意攻击的防御性。

此外，智能家居系统网络中还有大量节点设备产生的数据，保证这些数据隐私安全的最有效的方法就是随数据进行加密。但是目前网络层面临的挑战是如何处理这些大量的加密数据。总结来说，应用层安全的需求主要在于大量节点设备需要高效率的安全接入、大量数据的安全保存以及用户的隐私保护问题。

智能家居系统网络安全方案设计

1. 智能家居系统的网络结构

智能家居系统的网络结构主要分为和家庭网关相连并和上位机进行交互的公用网络和由受控设备组网形成的家庭内部网络，如图3所示。

从图3中可知，在智能家居系统中可能有两个关

节存在网络安全问题：其一是用户通过外部Internet网络方式登录网关，因为登录通道是互联网的非安全通道，所以用户的身份和隐私信息易遭到网络攻击，其带来的安全威胁难以预料；其二是对于家庭内部局域网来说，被控设备通过无线方式与网关相连，信号在无线信道的传输中可能被拦截、窃听甚至控制。因此，加密需传输的控制指令便可保证数据传输中的安全。

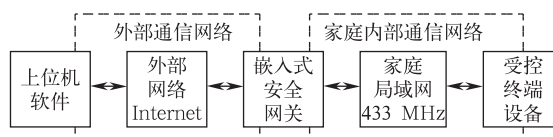


图3 智能家居系统网络结构

2. 智能家居系统网络安全软件架构

智能家居系统网络安全问题存在于外部网络通信和家庭局域网内网通信两个环节。基于此，可采用一次口令身份认证系统解决外部网络通信安全问题，采用AES-128加密算法解决家庭局域网内网通信安全问题，如图4所示。

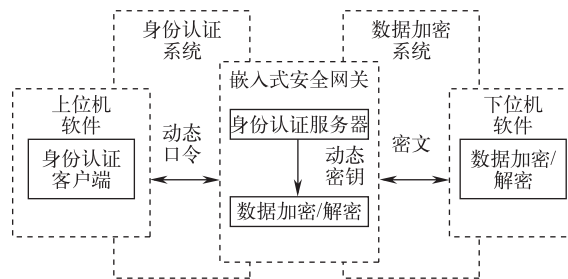


图4 智能家居网络安全软件架构

3. 一次口令身份认证系统

采用一次口令身份认证系统解决外部网络通信安全问题，包括客户端认证模块、服务器认证模块和动态密钥模块。客户端和服务端需要相互认证，只有在服务器和用户都合法认证的情况下，才可以完成认证工作。之后，系统随机生成128位的动态密钥，成为种子密钥，供后续加密系统使用。系统架构如图5所示。

4. 身份认证系统软件架构

在一次口令身份认证系统中，系统需要进行客户端和认证服务器交互的工作，包括三个方面：提出认证请求、验证服务器是否合法以及应答请求。下面介绍客户端所完成的工作。

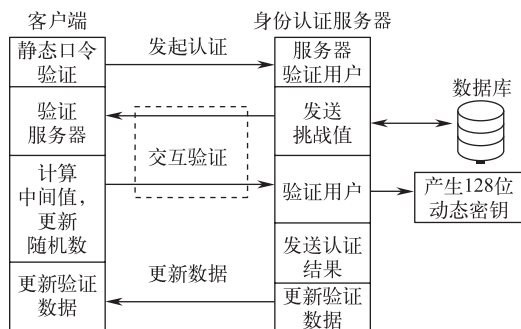


图5 一次口令身份认证系统架构

(1) 请求工作

用户向服务器申请认证时，客户端先验证用户名和响应静态口令是否对应。完成认证后，客户端产生随机数并将通过MD5哈希函数产生的值发送到服务器端。算法流程如图6所示。

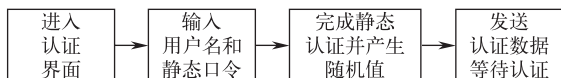


图6 请求工作算法流程

(2) 验证工作

在客户端发起认证请求后，服务器反馈数据对其合法性进行验证，之后服务器将挑战值发送给客户端，客户端通过相应算法计算出待验证值并与数据库中的值比对，从而对服务器的合法性进行判断。算法流程如图7所示。



图7 验证工作算法流程

(3) 应答工作

在客户端完成了对服务器合法性的检测之后，服务器需要对客户端的合法性进行核实。客户端更新随机数待验证信息，认证服务器通过计算确定客户端是否合法，通过网络将相应的验证信息发送给认证服务器。算法流程如图8所示。

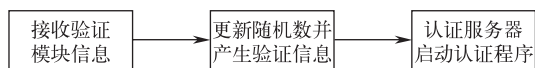


图8 应答工作算法流程

5. 嵌入式安全网关架构

嵌入式安全网关（以下简称“网关”）是智能家居系统的核心控制系统，也是智能家居系统网络

安全的密钥生成器和认证服务器。网关的应用程序基于Redhat Enterprise 6版本的Linux系统的应用层开发，结合Linux系统架构，嵌入式网关的软件架构如图9所示。



图9 嵌入式网关软件架构

网关软件开发工作的重点和难点在于身份验证服务器的开发及与数据加密系统的融合。除与网络安全通信相关的模块外，网关也包含协议转换模块和资源调度模块。前者是将由互联网传送的IP数据包转换成局域网设备的可识别的命令，同时将从串口获取的数据上传至上位机进行存储或动态显示。架构中的U-Boot就像Windows系统中的基本输入输出系统（BIOS），将操作系统文件拷贝到RAM中并提供系统程序的执行入口。U-Boot之上是Linux系统内核，作用是调用控制存储器、文件系统以及各种外设等资源。内核之上是YAFFS文件系统，用来对文件进行存储管理。

6. 数据加密系统

数据加密系统需要完成局域网内数据的加密与解密。为了和身份认证系统的128位动态密钥匹配，数据加密系统需满足以下三个条件。

(1) 密钥长度需匹配

一次口令身份认证系统可以产生128位的动态密钥，加密算法的密钥必须是128位。

(2) 模块间需实现强隔离

在实际使用过程中，若完成了一次身份验证，

家庭局域网传送指令的过程中很有可能发生密钥被窃取的情况；如果不能实现强隔离，入侵者便可以通过种子密钥反推出用户的登录口令，导致用户的静态口令丢失。例如采用MD5哈希函数，根据其性质可知从哈希值反推原相是不可行的。

(3) 对硬件平台的要求

以AES-128加密算法为例，对硬件平台的要求详见表1。可以选用STM8L101系列单片机，Flash大小为8 K，RAM大小为1.5 K，结合表1数据可知，该系列单片机可满足需求。

表1 AES-128加密算法对硬件平台要求

项目	加密算法	解密算法
时钟周期	~6 600	~8 400
Flash (byte)	1 839	2 423
RAM (byte)	80	80

7. 身份认证系统和数据加密系统的融合

家庭网关在实际使用过程中，当用户有登录需求时，身份认证系统与数据加密系统的融合才能启动。网关通过加密用户利用算法发出的指令，在与服务器顺利完成相互验证后完成相应的控制。其流程图如图10所示。

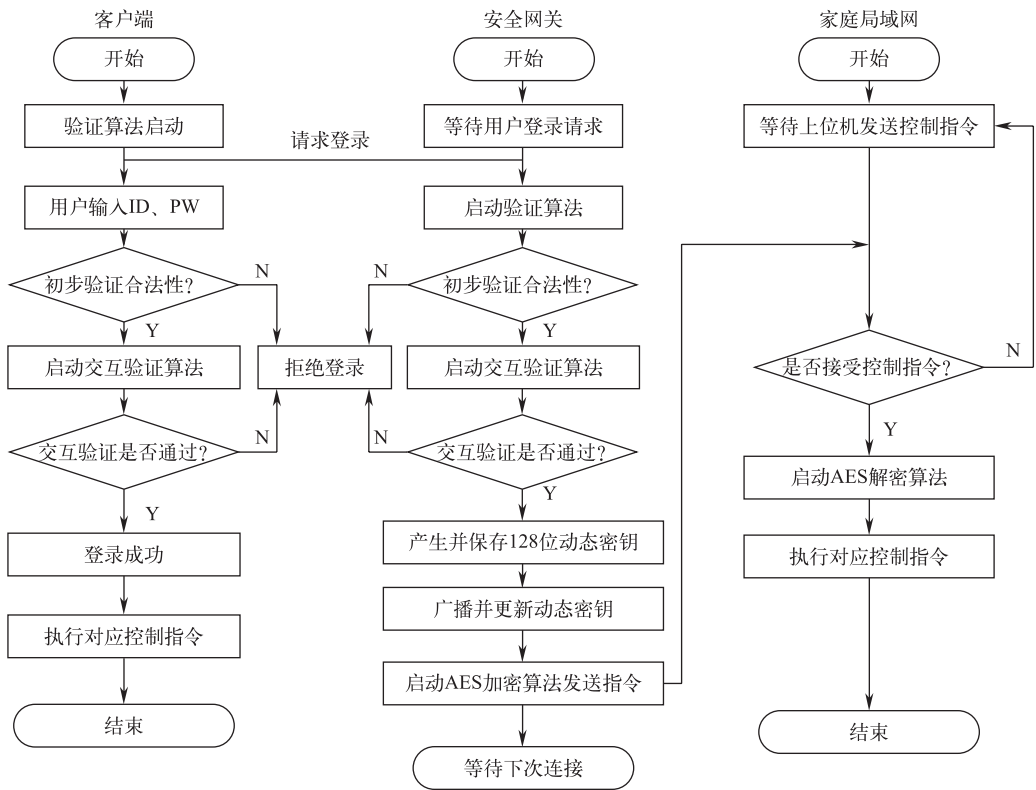


图10 身份认证系统和数据加密系统的融合算法流程图

总结与展望

随着大数据、机器学习、云计算及物联网等新兴技术的蓬勃发展，出现了很多安全问题，将数据安全技术与接入安全技术相结合，使智能家居系统网络的信息安全得到保障，是智能家居系统网络安全管理的基础。分析多种密码技术的优劣，结合智能家居系统的安全和高效需求，选择AES-128加密算法作为系统的密码算法，在数据加密和接入认证方面，有效提升了整体网络系统的安全性，提高了

效率。

随着时代的发展，智能家居技术也在不断更新，外延也在不断扩大，但各种潜在的风险和问题也在不断增加，通过更严密的安全防护措施，在保证用户隐私安全的同时，也需要相关技术水平的进一步提升，通过制定更好的标准，为用户提供信息，最终实现智能家居的安全环保体验。EA

(收稿日期：2023-05-08)