



基于 eUICC 的智能家居认证方案

黎艳, 卢燕青, 张荣, 郭茂文

(中国电信股份有限公司广州研究院, 广东 广州 510630)

摘要: 分析了当前智能家居的各种主要安全隐患。针对隐患原因, 提出智能家居认证关键点及基于 eUICC 的认证方案, 包括总体架构、主要模块交互及关键流程等, 最后, 对 eUICC 在智能家居领域的应用进行了前景展望。

关键词: eUICC; 智能家居; 用户卡认证; 设备安全

中图分类号: TN918.91

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018040

Authentication scheme of smart home based on eUICC

LI Yan, LU Yanqing, ZHANG Rong, GUO Maowen

Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

Abstract: The main existing security risks in smart home services was analyzed. For the reason of these risks, the key points of smart home security and also the authentication scheme based on eUICC were put forward, including the overall architecture, main module interactions, key processes, etc. Finally, the application of eUICC in the field of smart home was prospected.

Key words: eUICC, smart home, user card authentication, device security

1 引言

互联网技术的高速发展使人们对家居生活安全和便利的需求日益提高。随着智能家居和物联网各种技术的涌现, 智慧家庭设备、云端控制中心和用户之间可以进行有效的信息交互^[1]。用户在获得更多家庭内部信息的同时, 对认证的安全要求也越来越高。

传统的认证大多使用业务账号和密码或短信验证码, 其存在密码泄露、短信被截获等风险。

目前, 已经暴露了很多设备安全事件, 比如, 摄像头被非法访问、物联网设备被非法平台操控等。同时, 用户授权机制的完善也有待考虑。如何实现终端设备与认证平台之间的高强度双向认证, 并且与用户授权相结合, 是物联网时代智能家居面临的一大挑战。

2 智能家居安全隐患

2.1 访问认证漏洞

智能家居设备收集了用户大量的隐私数据,



首要的安全问题就是数据访问漏洞。目前,大多数智能家居设备的访问都是使用简单的用户名和密码,并没有严谨的安全控制策略。2016年10月,黑客攻破大量物联网智能设备,集中向美国最主要的DNS服务商Dyn服务器发起史上最严重的DDoS攻击,导致数百家网站无法访问。2017年6月,中央电视台(以下简称央视)调查曝光大量摄像头被入侵,通过IP地址扫描,大量弱口令摄像头被破解,用户隐私视频曝光。数据访问控制问题亟待解决。

主要的访问认证安全隐患包括以下几个方面。

(1) 用户名和密码强度弱

目前,大多数家庭设备都是使用用户名和密码的方式登录和管理设备,但普遍对用户名和密码的强度没有要求,甚至直接使用弱口令,很多终端设备更是直接在终端设备表面印刷默认的用户名和密码,而用户也很少会更改密码。密码强度不足及密码管理不严导致了用户名和密码存在容易泄露、被扫描、被暴力破解和被劫持的风险。

(2) 访问授权缺失

绝大部分智能家居设备访问无需额外授权,设备被攻破并非法访问时,设备所有者并不知情,导致设备轻易被操控,用户隐私无形之中被暴露无遗。

(3) IP地址暴露

通过扫描器,使用弱口令暗码(如user、admin)做大规模的IP地址和端口扫描就可以获取家居智能设备(如摄像头)的IP地址,一旦IP地址暴露且弱口令匹配,即可直接获取数据资源。除了智能家居设备存在此安全隐患,很多公共户外网络设备同样有被破解的风险。

2.2 设备侧漏洞

由于智能家居设备承担着数据收集、数据上报、指令执行等重要职责^[2],智能设备的身份保护尤其重要。

设备侧安全隐患主要有以下几方面。

(1) 设备伪造

设备关键信息被非法读取之后,伪造者利用关键信息进行设备伪造,如伪造设备号、伪造设备MAC地址等。用伪造的身份冒充原设备侵入系统,并且在交互过程利用伪造的身份欺骗服务器。这种情况多出现在使用弱身份标识或身份凭证存储失当的智能家居系统中。

(2) 隐私数据被窃取

智能家居设备采集的用户隐私数据如果没有高强度的安全存储、加密或者读取鉴权,就极易被窃取。隐私数据除了设备所存储的安全凭证和设备所采集的用户数据之外,也包括设备与服务器或App之间的业务逻辑等。

(3) 指令伪造

通过逆向工程获知通信逻辑,继而伪造App或者服务器,向智能家居设备下发恶意消息序列或非法指令。通过指令伪造,达到恶意控制设备的目的,如联网的烤箱被恶意控制干烧或联网洗衣机被恶意控制空转等。如果智能家居设备对指令来源并未做任何认证,而只是盲目执行,则极易被非法用户恶意控制。

2.3 数据交互(传输)安全

智能家居设备与App或者云端服务器之间的通信涉及各种指令的传输、关键数据的同步、采集数据的上传,这些数据的安全保障也是至关重要的。

常见的数据安全隐患如下。

(1) 数据侦听截获

利用传输过程开放协议的漏洞,侦听并截获设备与应用、设备与云端服务器的交互数据;通过对交互数据的进一步解析,破解相关通信逻辑或非法获取当中的关键隐私数据。

(2) 数据被篡改

在截获传输的交互数据之后,对当中的关键数据进行篡改,如用户的计费账号信息、指令的类别和内容等。如果设备侧、应用侧或云端服务器侧没有对数据的完整性和可靠性进行校验,很

容易带来家居安全隐患。

(3) 伪造数据造成阻塞

通过非法伪造数据造成设备或云端阻塞不可用,如模拟平台向同一台终端设备下发大量指令,超出设备处理能力导致设备发生故障。抑或模拟设备向平台发送大量请求,从而占用过多的服务资源使服务器超负荷,导致合法设备无法得到服务响应。

(4) 数据重放攻击

不需了解分析通信协议,在身份认证过程,直接将窃听到的通信数据原封不动重新发送给接收方,从而达到欺骗系统的目的。

3 智能家居安全认证思路和总体设计

针对目前智慧家庭应用中账号/密码认证强度弱、设备ID容易被篡改和远程配置管理弱的情况,提出了基于eUICC实现设备侧和云端的双向认证,主要优势如下。

- 硬件级认证的引入。实现高安全等级的身份认证和访问控制,保障家庭设备的信息安全,可以作为电信智慧家庭业务(如机顶盒家悦业务、家庭视频监控)的一大卖点。
- 实现设备认证与eUICC之间的通信之后,可以应用到物联网其他设备,利用eUICC内卡应用的安全加解密能力,实现设备与应用平台的双向认证。目前已有类似行业应用需求。
- eUICC基于Java平台,支持PKI非对称计算能力,软硬件能力比普通SIM卡强,能够兼容各种卡认证的能力需求^[3]。
- 现有家庭网络设备基于线路绑定和用户密码绑定的方式实现认证,使应用的物理空间和认证方式都有所限制。eUICC的引入可以突破这些局限性,应用上更加灵活。设备认证思路具体如下。

(1) 为每台设备配置高强度的唯一身份。

(2) 设备的身份认证需使用安全加密算法,如对称的OCRA动态口令或更高安全的PKI非对称密钥体系。

(3) 设备侧与云端服务器侧实行双向认证,可在设备侧和云端分别存储对方的非对称密钥对的公钥,基于PKI实现双向身份认证^[4]。

(4) 数据传输需经过安全加密,安全加密密钥的协商可以使用数字信封技术。

访问认证(授权)思路具体如下。

(1) 用户手机侧使用SIM卡认证实现设备访问的控制、授权,目前,国内三大运营商基本上已经在用户卡上实现了快捷认证和数字证书认证,可以通过应用安全需求选择合适的认证方式。

(2) 由云端服务端或者认证平台管理和维护设备与授权手机的关系^[5],并通过空口SCP80协议向授权手机下发授权请求。

以下是智能家居安全认证总体的架构如图1所示,各模块具体介绍如下。

(1) eUICC

eUICC内装载认证卡应用,负责设备侧各加密密钥的生成、数据的加/解密等认证相关数据的处理。

(2) 家庭中心设备(或使用其他承载网络如NB-IoT的设备)

管理家庭其他设备的接入,通过ISO 7816或SPI协议与eUICC内装载的认证卡应用进行通信,从而获取相关加密认证数据,并向认证服务器上设备信息及提交访问授权请求。

(3) 认证服务器

验证设备上传的认证数据,管理设备与用户手机之间的关联关系,并根据设备—手机的对应关系向相应的管理手机下发授权请求数据短信。

(4) 用户手机卡

用户手机卡内装载认证卡应用,实现快捷认证(免账号/密码登录)及数字证书认证,使用卡应用进行身份认证的基础上用户可以接收并处理

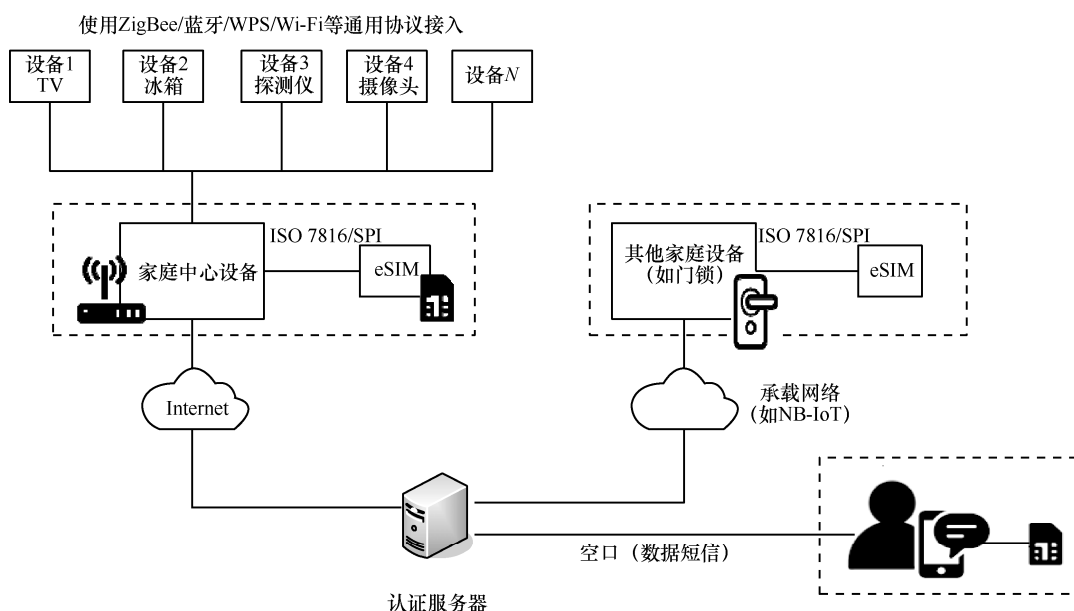


图1 智能家居认证系统总体架构

认证服务器的授权请求。

4 智能家居认证方案

基于设备双向认证和用户卡认证授权的思路，本方案利用 eUICC 的物理和安全特性，为智能家居设备实现高强度的身份认证。之所以使用 eUICC 作为处理认证安全数据的关键，是因为 eUICC 具有如下特性：

- eUICC 芯片达到 EAL5+，通过国家商用密码安全认证；
- 相对普通 SIM 卡有更强的处理能力，具有 DES/AES/RSA/SM（国密算法）的硬件协处理器；
- eUICC 与设备之间是机卡一体并强绑定的，其 EID 可以作为设备的唯一识别码；
- eUICC 支持 FOTA（firmware over the air），可以很方便地进行云端升级，实现系统修复和优化，如卡应用的升级等^[6]；
- eUICC 与其他 SIM 一样，一卡一密，通过空中加密通道下发的数据短信只有唯一对应的 eUICC 才能解密获取相关数据。

智能家居设备与 eUICC 之间的通信如图 2 所示，各模块具体介绍如下。

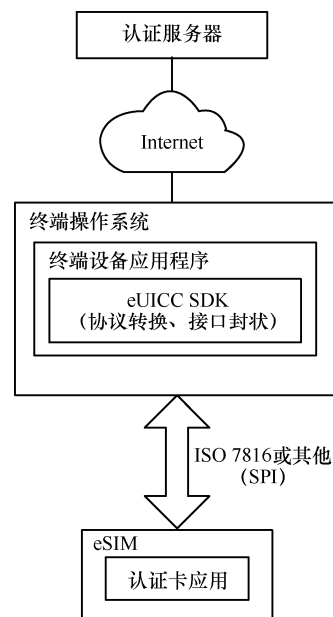


图2 智能家居设备与 eUICC 之间的通信示意

(1) eUICC 认证卡应用

负责认证数据的加/解密，包括密钥生成、存储及同步，对称加/解密（DES/3DES/AES/SM4）和非对称加/解密（RSA1024/RSA2048/SM2）。

(2) eUICC SDK

负责终端设备协议转换、APDU 指令封装以及向终端应用程序开放 eUICC 认证卡应用的相关接口, SDK 向终端设备应用程序提供并集成。

(3) 终端设备应用程序与 eUICC 之间的通信通道

通过在终端侧进行协议转换, 终端设备可以通过 ISO 7816 协议或 SPI 协议与 eUICC 进行通信。

4.1 设备接入认证流程

假设终端设备绑定的 eUICC EID 在 CRM 侧已经与用户、管理、手机信息进行绑定并同步到认证服务器, 具体的设备接入及绑定认证流程如图 3 所示, 具体介绍如下。

(1) 终端设备上电并接入网络。

(2) 设备检测设备绑定标识, 若已绑定, 则结束设备接入认证流程; 若未绑定, 则继续检查

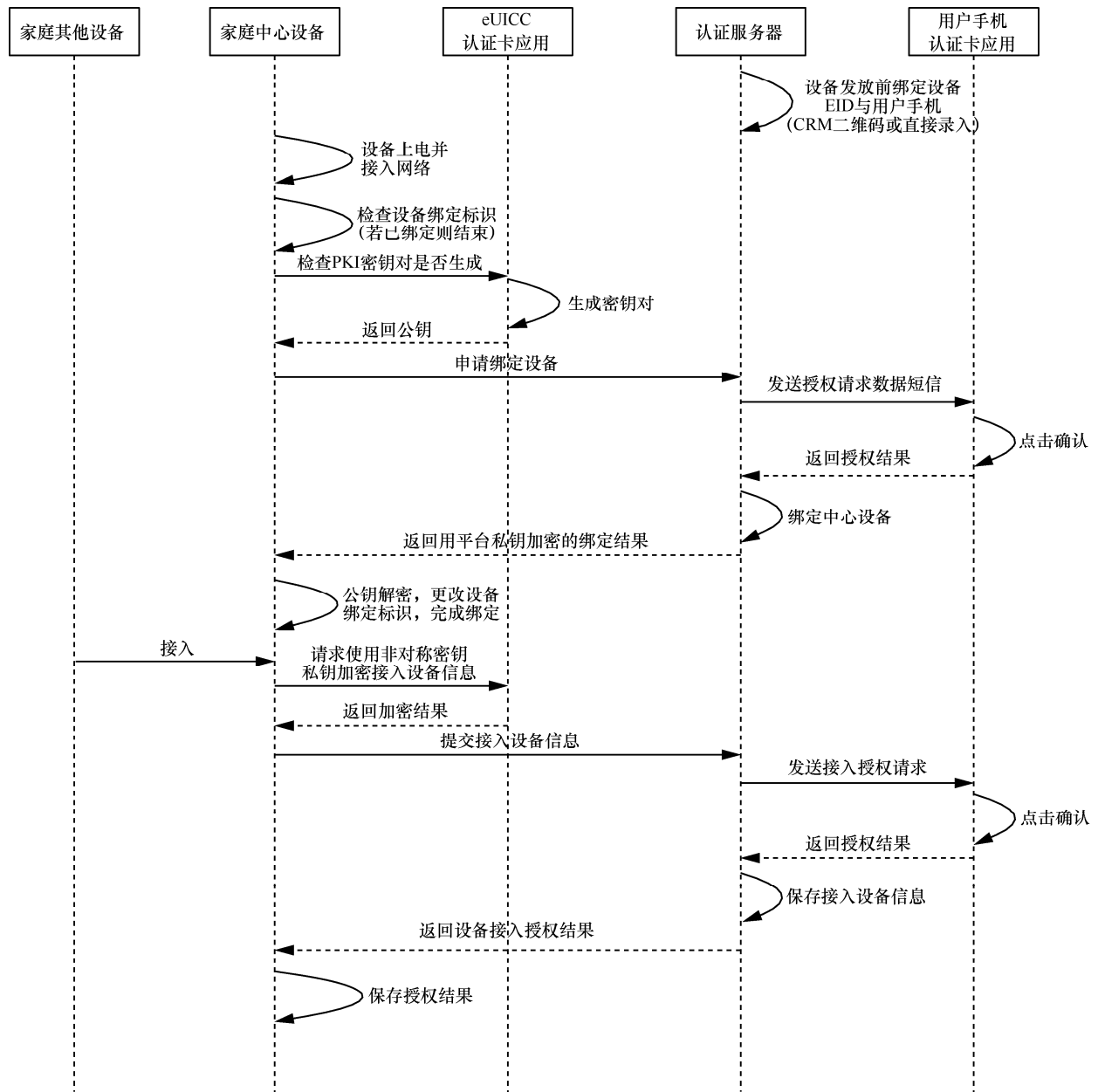


图3 设备接入及绑定认证流程



密钥对生成标识。

(3) 若密钥对已生成，则将密钥对公钥上传到认证服务器进行绑定。

(4) 认证服务器将接入绑定请求数据短信下发到用户的管理手机，请求授权。

(5) 用户确认之后，认证服务器返回绑定结果（使用认证服务器私钥加密）。

(6) 终端设备使用认证服务器公钥对返回的绑定结果进行解密，完成绑定。

(7) 中心终端设备完成绑定认证之后，一旦有其他设备接入中心设备，中心设备会使用自己的非对称密钥对私钥对接入的设备信息进行加

密，提交到认证服务器。

4.2 访问认证流程

以摄像头访问为例，当外部连接需要访问网络摄像头的视频内容时，摄像头会向摄像头云端服务器发送视频数据，使用如图 4 所示访问认证方案可以对此动作进行放行或阻拦。

假设中心终端设备（通常是网关、机顶盒、路由器等中心控制设备）已经完成设备接入绑定流程，具体访问认证流程如下。

(1) 家庭中心设备检测到设备向外的数据分组。

(2) 家庭中心设备调用 eUICC 签名接口，使用 eUICC 私钥对事件描述进行签名，发送到认证

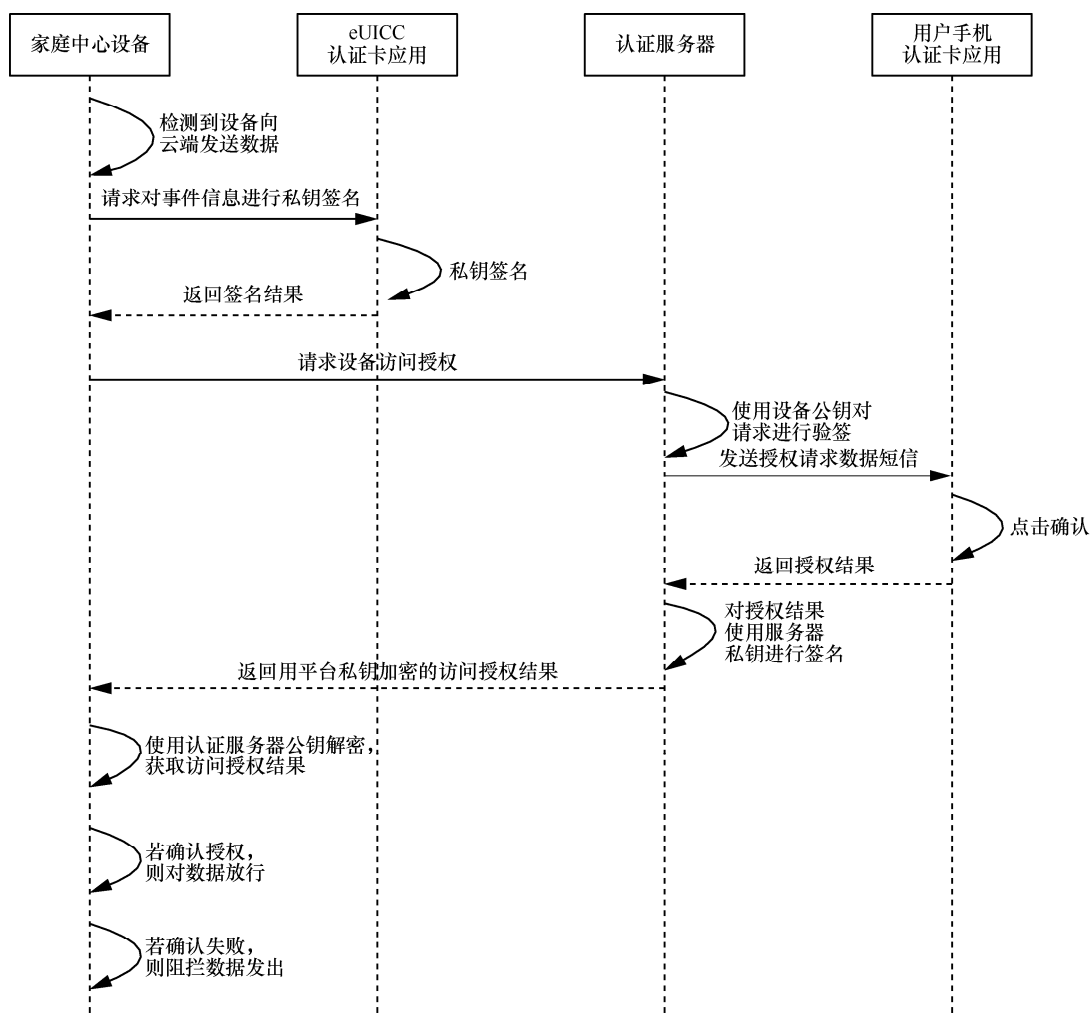


图 4 设备访问认证及授权流程

服务器。

(3) 认证服务器验签, 对设备身份进行认证。

(4) 完成认证之后, 认证服务器向用户管理手机下发授权请求数据短信。

(5) 用户卡完成授权之后, 认证服务器使用服务器私钥对授权结果进行加密。

(6) 家庭中心设备使用认证服务公钥进行解密, 对认证服务器身份进行认证。

(7) 家庭中心设备根据授权结果对数据进行放行或阻拦。

5 结束语

本文首先分析了当前智能家居的各种主要安全隐患。针对隐患原因, 提出智能家居安全认证思路及基于 eUICC 的总体设计方案。通过使用具有物理及安全特性的 eUICC 实现设备与服务器端的双向认证, 可以有效避免设备伪造、设备非法控制、非法指令下发、数据窃听篡改等智能家居安全隐患。而运营商使用 eUICC 进行智能家居安全认证部署, 可以把统一认证扩展到智慧家庭领域, 开拓一片新的价值蓝海。

参考文献:

- [1] 朱敏玲, 李宁. 智能家居发展现状及未来浅析[J]. 电视技术, 2015, 39(4): 82-96.
ZHU M L, LI N. State of art and trend of smart home in China[J]. Video Engineering, 2015, 39(4): 82-96.
- [2] 韩建亭. 可运营智慧家庭系统的构建[J]. 电信科学, 2015, 3(11): 109-115.
HAN J T. Construction of smart home system architecture for operating[J]. Telecommunications Science, 2015, 3(11): 109-115.
- [3] 杨红梅. eUICC 的关键技术及相关标准[J]. 电信网技术, 2015(6): 58-62.
YANG H M. Key technologies and related standards of eUICC[J]. Telecommunications Network Technology, 2015(6): 58-62.
- [4] 刘丽萍. 基于智能卡和密码保护的 WSN 远程用户安全认证方案[J]. 电信科学, 2015, 31(12): 105-110.

LIU L P. A remote user security authentication scheme using smart card and password protection for WSN [J]. Telecommunications Science, 2015, 31(12): 105-110.

- [5] 王斌, 杨晓玲, 肖冬娣. 基于云服务实现智能家居应用控制的方案[J]. 电信科学, 2015, 31(11): 140-145.
WANG B, YANG X L, XIAO D D. Scheme of smart home application control based on cloud service[J]. Telecommunications Science, 2015, 31(11): 140-145.
- [6] 杨剑, 戴国华, 李培煜. 电信运营商 eUICC 发展关键问题分析及建议[J]. 移动通信, 2015(12): 158-165.
YANG J, DAI G H, LI P Y. Analysis and suggestions on key problems of eUICC development in telecom operators[J]. Mobile Communications, 2015(12): 158-165.

[作者简介]



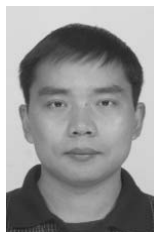
黎艳 (1981-), 女, 中国电信股份有限公司广州研究院工程师, 主要研究方向为移动互联网安全技术与产品开发。



卢燕青 (1973-), 男, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为互联网网络技术和应用研发、移动互联网核心业务。



张荣 (1973-), 女, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为移动互联网新技术与业务、智能管道。



郭茂文 (1973-), 男, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为移动互联网技术与业务、互联网应用安全。