软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.006033]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于联盟链的物联网跨域认证*

魏 欣[1], 王心妍[2], 于 卓[3], 郭少勇[1], 邱雪松[1]

[1](北京邮电大学网络与交换技术国家重点实验室 北京 100876)

[2](国网河南省电力公司 郑州 450000)

[3](北京中电普华信息技术有限公司 北京 100192)

通讯作者: 郭少勇,E-mail: syguo@bupt.edu.cn

摘 要: 针对物联网场景下跨信任域的信息交换需求,本文结合区块链与边缘计算思想,构建了一种适应于物联网认证的架构.首先基于联盟链技术,设计了适应于物联网跨域认证的架构及流程,构建了安全的跨域信息交互环境;随后,引入边缘网关以屏蔽物联网的底层异构性,并设计了基于网关的跨域认证流程,增强了物联网认证中的隐私保护;此外,本文针对设计协议的安全性进行了分析,确认其具备符合物联网需求的抗攻击能力;最后设计了实验,对本文设计的认证方案与传统方案做了对比.实验证明本文设计的方案较传统方案有更好的性能,具备实用价值.

关键词: 区块链;物联网;联盟链;多信任域;认证

中图法分类号: TP311

中文引用格式: 魏欣,王心妍,于卓,郭少勇,邱雪松.基于联盟链的物联网跨域认证.软件学报. http://www.jos.org.cn/1000-9825/6033.htm

英文引用格式: Wei X, Wang XY, Guo SY, Qiu XS. Cross Domain Authentication for IoT Based on Permissioned Blockchain. Ruan Jian Xue Bao/Journal of Software, (in Chinese). http://www.jos.org.cn/1000-9825/6033.htm

Cross Domain Authentication for IoT Based on Permissioned Blockchain

WEI Xin[1], WANG Xin-Yan[2], YU Zhuo[2], GUO Shao-Yong[1], QIU Xue-Song[3]

[1](State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)

[2](State Grid Henan Electric Power Company, Zhengzhou 450000, China)

[3](Beijing China-Power Information Technology Co.Ltd., Beijing 100192,China)

Abstract: Aiming at information exchange requirements of cross-trust domains under Internet of Things(IoT) scenario, the paper constructs an authentication architecture which suits for IoT with blockchain and edge computing. Firstly, based on permissioned chain, the paper designs architecture and process for authentication in IoT, which aims to provide a secure cross-domain environment for information interaction. In addition, edge gateway is introduced to shield heterogeneity and sensitive information of things. Then, the paper designs edge gateway based authentication protocol for cross-trust domain authentication. Performance analysis proves that the design could resist common attacks, and simulation results proves it has better performance than traditional way in both computating consumption and communication consumption.

Key words: blockchain; Internet of Things; permissioned blockchain; Cross-trust domain; Authentication

随着网络技术的高速发展和低成本智能设备的大规模部署,物联网取得了飞速的发展,对跨系统之间的信息交互提出了需求.传统物联网采用封闭建设模式,不同系统之间存在认证模式不同、证书形式不同等差异,从

* 基金项目: 国家重点研发计划(2019YFB2102302); 国家自然科学基金(61702048)

Foundation item: National Key Research and Development Program of China (2019YFB2102302); National Natural Science Foundation of China (61702048);.

收稿时间: 2019-11-12; 修改时间: 2020-01-06, 2020-02-26; 采用时间: 2020-03-16; jos 在线出版时间: 2021-04-20

而造成了显著的隔离,形成了多个信任域.由于同一信任域内的资源已经不能满足用户和设备的需求,高效简洁的跨域访问流程设计成为当下的研究重点.

传统的跨域访问流程分为两类:一类采取实时授权的方式,在这种情况下,双方信任域的认证 CA 交互授权提供短期跨域访问凭证,这种方式交互复杂,时延较高;另一类采取长期授权的方式,一方 CA 将另一方 CA 提供的标准化信息作为登录信息长期存储,该类情况下常有更新不及时导致的信息过期等问题.以上跨域方式都难以适应物联网的低时延高可信的需求,究其根本原因在于 CA 之间无法快速达成信任.

区块链作为一种近年来取得广泛关注的分布式信任环境,可为多 CA 之间的合作提供标准化的可信任机制,进而实现不同信任域之间的快速认证.但区块链因其公开透明的特性,在打通多 CA 之间信任的同时也增加了隐私泄露的风险,本文针对该问题设计了隐私保护的认证方式,增强了跨域交互过程中的信息保护.

本文所做的贡献如下:

1) 本文设计了一种适用于物联网跨域认证的架构.通过引入边缘网关实现对物联网设备的接入及管理,提高物联网的管理效率,屏蔽底层异构性问题.在物联网的不同 CA 之间部署联盟链,利用多 CA 共识简化多信任域之间的认证流程,为物联网构建了可信的跨域信息交互环境.通过边缘网关实现物的描述及接口上链,访问者可通过调用智能合约对物进行操作,增强了物联网的连通性.
2) 本文针对区块链引入的隐私问题,设计了一种隐私保护的跨域认证.首先通过预处理设置全局参数完成全部 CA 的导入,而后对边缘网关及访问者执行接入认证.访问者通过边缘网关生成匿名身份,使用匿名身份完成校验.收到访问请求的边缘网关可基于区块链完成对身份的核验.经过证明,本文设计的跨域认证流程可提供安全高效且保护隐私的认证环境.

本文第 1 节对基于区块链的物联网跨域交互方案进行了总结,第 2 节介绍了物、网关、CA、区块链之间的整体架构, 第 3 节提供了对系统的整体描述以及跨域访问的流程设计.第 4 节对本文设计的跨域认证流程进行了正确性及安全性的证明,第 5 节对提出的方法进行了仿真实现并完成了评估.第 6 节总结全文,并对未来值得关注的研究方向进行初步探讨.

1 相关工作

区块链是一种中本聪提出的分布式账本技术[1],糅合了 P2P 网络、加密散列技术、数字签名等技术,可用于分布式环境下的数据可信读写.在区块链环境下,互相不信任的节点可达成合作并形成可信的数据.通常来讲区块链中的活动可以概括为:用户通过一堆非对称加密密钥获得身份并以此签署交易.网络中的节点收集交易并打包成区块链接到前一个区块.通过共识,网络中所有节点维护着完全相同的交易历史.智能合约是一种特殊的数据,当被调用时将在区块链上自动且独立地执行对应的脚本.由于记录在区块链上的数据由全网共享,因此无法进行篡改,可确保数据的真实可信.由此,区块链的可信在互联网资源分配中逐渐引起了广泛重视,如针对 IP 及域名资源的分配及管理等[2][3].2014 年,麻省理工的 Conner 团队[4]提出了首个基于区块链的身份认证系统,通过区块链对用户的身份证书进行管理.考虑到隐私性问题,Axon 等人[5]通过节点权限分级的方式实现了隐私保护的身份认证系统.

考虑到物联网与互联网的相似性,同样具备着大量互不信任的节点高效达成信任的需求,引入区块链以解决物联网的可信问题成为一大研究方向.Christidis K 等人[6]分析了区块链在物联网中的适用性,指出区块链可以为物联网提供可信任、可审计的环境,智能合约可以整合工作流,节约成本及时间.Kshetri N 等人[7]指出,区块链的分布式处理及可信审计特性,为物联网的身份管理及接入控制带来了巨大便利,可以提高物联网的安全性.Lewis 等人[8]指出区块链部署于物联网中存在异构性、可扩展性、可监管性等风险挑战.

在分析区块链如何用于物联网的同时,大量基于区块链的物联网架构设计涌现.Huh S 等人[9]及 Alphand 等人[10]利用区块链对物联网身份进行管理、授权,从而驱动物与物之间的数据共享.Sharma P K 等人[1] 指出中心化的云架构无法实时对海量数据进行处理,难以用于未来的物联网,而区块链可以推进分布式可信运行,进而为雾计算提供支撑.Novo 等人[12]提出了由管理网关将 WSN 网络汇聚到区块链,管理节点定义智能合约并实现共

识.在该设计中,管理网关用于突破物联网设备的限制,实现接口转换,完成物与智能合约的交互.宋文斌[13]、贺毅[14]、梅晨[15]等人在各自的学位论文中设计并实现了基于区块链的物联网身份认证支撑系统.但以上设计并未考虑到针对物联网中的多信任域造成的连通性问题.

万雨薇[16]对物联网下的跨域认证做了细致的流程分析及设计.Wang W 等人[17]设计了跨域场景下的区块链扩展方案及认证流程.针对基于区块链的跨异构域认证,周致成等人[18]与马晓婷等人[19]提出了链模型,证书格式,实现了跨异构域的认证.Lei A 等人[20]针对车联网中移动性带来的认证域变化,提出了基于区块链的动态密钥管理方法.但以上方法采用直接将设备信息公开到区块链,缺乏对隐私的保护机制.Thomas H 等人[21]提出了基于联盟链的匿名身份及访问控制,但该设计中对于每次跨域请求均上链,带来了巨大的访问开销,难以满足物联网的实时性需求.Ma M 等人[22]构建了基于多链的密钥管理框架,在物联网设备注册时即将权限控制策略发布上链,实现对内容的权限访问,通过主链协调跨域的访问请求.Cha S C 等人[23]针对蓝牙低功耗设备设计了网关的工作流程,并设计了隐私保护设定,当且仅当用户与发布到链上的设置吻合时可以对设备进行访问,该设计对身份信息不作保护.Yao Y 等人[24]通过引入第三方来构建区块链,并针对车联网场景研究了面向车联网的跨域隐私认证方法,但未能说明第三方提供认证服务的动机.

在以上工作的基础上,本文设计了适用于物联网的区块链部署架构,引入原有物联网 CA 作为区块链共识节点,边缘网关作为区块链客户端,为人和物提供服务.在交互过程中,通过边缘网关完成身份匿名情况下的校验,减少跨域认证过程中不必要的隐私泄露.

本文设计的架构较传统架构有以下优势:

1）整合了多 CA 的认证资源,为更丰富的物联网服务提供了可能性.相比较传统 CA 之间互通困难造成的信任孤岛,本文设计的结构打通了认证域之间的隔离,促使不同的物联网之间打通隔离.

2）缩短了不同 CA 的跨域流程,为现有的物联网服务提高了效率.传统 CA 之间互相多次重定向并签密延长了跨域认证所需的时间,本文设计的结构通过智能合约加速了跨域之间的认证,提高了效率.

2 系统设计

如图所示,本文设计的物联网跨域认证总体架构与传统架构对比如图 1.

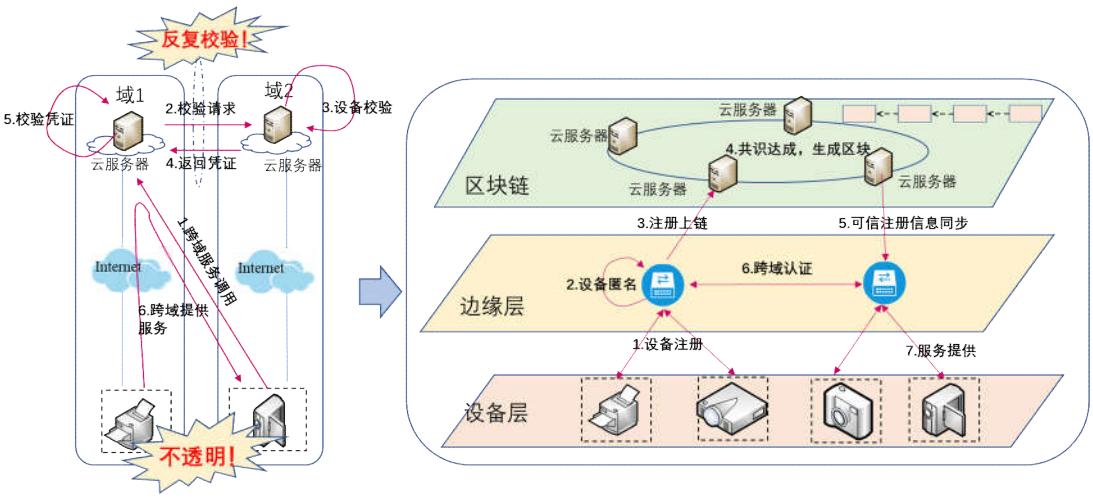

Fig.1 Architecture in IoT

图 1 物联网架构

在传统架构中,物联网不同场景设备通过网络汇聚到各自位于云端的服务器,云服务器为所在信任域的设备提供信任背书,并对外提供接口提供服务.当需要调用其余信任域的设备以实现物联网服务时,云服务器之间

将展开密切的‘请求-校验-重定向-认证-背书-校验’合作过程以确保各方信任域内的设备的可信.但是,由于服务通过云服务器提供的接口实现调用,在设备到云服务器之间可能发生其余云服务器无法察觉的不可信行为.此外,在跨域的合作中,多个服务器为了确保彼此可信的合作将带来大量的通信开销及时延.因此,传统架构难以满足物联网的高效及可信需求.

本文设计的架构如图 1,在传统基础上,做了以下改造:

1） 在云服务器与物联网设备之间增加边缘层,引入边缘网关对设备进行汇聚处理并屏蔽隐私信息,与设备进行最直接的交互.由于跨域认证的计算在边缘执行,对云服务器的依赖性降低,从而降低了认证所需的时延,并减少了对云服务器造成的压力.通过在接入时对设备进行匿名化处理等操作,设备关键信息仅暴露给边缘网关,降低了隐私泄露风险.

2） 引入联盟链技术,实现云服务器之间的认证信息透明可信共享.云服务器可为自身信任域的设备及网关提供注册、更新及注销等服务.通过查询区块链,可获取设备及网关的信息,进而提高跨域认证的效率及可信,从而支撑物联网的各项服务.

对于本架构的详细解释如下:

设备指代是物联网中的各类设备,是物联网中业务的实际执行者,具有迥异的通信接口和隐私保护需求.打通物联网首先需要屏蔽其接口底层的异构特性实现管控,同时对其隐私进行保护.本文关注重点在于设备的身份隐私及行为隐私,即通过匿名化处理避免显式的身份信息暴露上链,同时通过更新设备身份信息避免对设备行为的持续追溯分析.

边缘层部署网关对设备进行汇聚,屏蔽底层异构特性.根据 Byungseok 等人 [25]提出的 IoT 网关概念,IoT 网关支持各种设备之间的多种通信协议和数据类型,可以实现各种设备之间通信的数据格式转换,并以统一的数据格式上传.同时,可将收到的获取或控制命令映射为生成满足特定设备通信协议的消息.网关仅作为逻辑概念,可部署于某些能力较强的设备上.

区块链层由传统架构中的云服务器组成联盟链.作为 CA 角色,为自身可操控的设备身份及能力提供信任背书,作为区块链完整节点,对发布到链上的信息进行共识,提供认证信息的实时共享,从而避免不同 CA 之间反复重定向带来的流程冗余及失效等问题.区块链提供基础的查询及写入功能,节点之间通过协商发布智能合约,并通过调用合约实现复杂功能.

在本文的设计中,边缘网关对设备进行接入后,根据隐私需求对设备进行匿名化处理,真实身份与匿名身份的映射关系仅保存在本地,将匿名身份及公钥签名后通过智能合约发布到区块链完成注册,从而避免了设备的真实身份泄露.云服务器之间达成共识后,设备的信息可通过智能合约进行查询及同步.在服务过程中,当网关收到跨域的调用请求后,查询区块链对请求进行校验,校验通过后执行相应操作并返回结果.为了避免设备的状态及偏好被分析,网关可随时更新设备的公私钥对,以新的身份参与跨域交互.详细流程将在下一节展开介绍.

3 跨域认证机制

本节首先对系统的运行流程进行设计,包括联盟链及网关的初始化、设备的写入、跨域的访问过程等.而后对流程中涉及到的交互协议进行设计,包括网关写入到联盟链的物信息注册、更新、注销;网关从联盟链读取的信息查询;网关与网关之间的跨域访问请求.

3.1 机制描述

本文设计的跨域认证流程与传统流程相比对比如图 2,红线框出的部分即为认证阶段.为了方便描述,本文将区块链的节点配置作为联盟链初始化部分,网关配置作为网关初始化部分;注册部分将设备接入到网关并发布上链,认证部分完成设备的跨域交互.

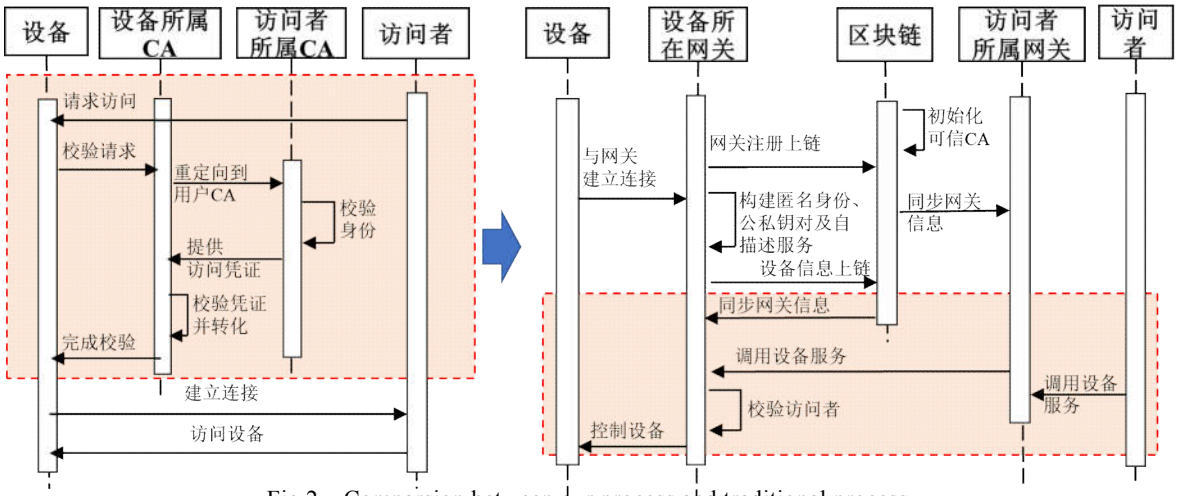

Fig.2 Comparsion between our process and traditional process

图 2 本文跨域访问流程与传统流程的对比

1. 联盟链初始化:

在构建基于联盟链的服务之前,首先对联盟链进行配置.不同于公有链,联盟链中存在至少一个管理节点为参与共识的云服务器发放证书并配置网络,但管理节点本身不参与链上的业务.完成配置后,参与共识的各云服务器的身份信息及对应权限、采用的共识算法、区块大小等将写入创世区块,同步到每一个云服务器.此时,云服务器可作为 CA 对外提供认证服务.由于联盟链的多中心特性,单个 CA 瘫痪后,其余 CA 仍可完成共识,提供服务.此外,创世区块中公布的是共识节点的初始集群,系统的使用过程中节点可按照创世区块中配置的策略加入或退出集群,更新将在链上留下记录.如 CA 退出,其之前签发的网关及设备仍在链上可查,不影响继续使用,但更新需要重新注册.如部分 CA 根据自身的风险感知,认为某 CA 为大量恶意节点颁发了证书或不再具备提供验证服务的能力,则采用对“该节点不可信任”达成共识的形式,迫使其退出.与 CA 主动退出集群的区别在于,该情况需对该 CA 自不可信起发布的全部证书做过期处理.在联盟链上发生的业务将打包成块链接到前一个区块,最终可追溯到创世区块.

具体流程如下:

1) 多个 CA 协商生成大素数 q,并利用 q 生成椭圆曲线群 G 及生成元 P.

2) 定义哈希函数如下:

其中 H_0 根据二进制序列和椭圆曲线上的两个点生成一个不大于 q 的素数,其余类似.

$$H_0(\{0,1\}^*,G,G)\to Z_q^*$$
$$H_1(G,\{0,1\}^*,\{0,1\}^*)\to Z_q^*$$
$$H_2(G)\to\{0,1\}^*$$

3) 选择 $SK_a\in Z_q^*$ 作为该 A 自身的私钥,计算 $PK_1=SK_1\cdot P$ 作为该 CA 的公钥.

4) 公布 q,P,G .类似地,其余 CA 按照相同方法生成各自的密钥对,以四个节点为例,其余三个节点的公钥为 PK_2,PK_3,PK_4 .

5) 公布系统参数 及各 CA 的公钥列表到创世区块.同时部署合约支持对 CA 公钥列表进行查询.后续 CA 的加入按照创世区块中指定的原则完成:如开放有加入接口,则新的 CA 调用注册获取到身份及权限对应证书后,后将现有区块链同步到本地,参与到后续的认证服务;如未开放接口,则需要管理节点

实现对新 CA 的添加及部署.

2. 网关初始化

网关注册的过程如下:

1) 网关 i 选择一个不大于 q 的整数 $SK_{gw_i}^1$ 作为自己的私钥.并计算出 $PK_{gw_i}^1 = SK_{gw_i}^1 \cdot P$,并向某位可验证该网关身份的 CA(以 CA1 为例),发送其身份与公钥,并利用 CA1 的公钥对其进行加密 $EN_{PK_1}(PK_{gw_i}^1 \| ID_{gw_i})$.在这一步的操作中,网关向 CA 提交了仅该 CA 可见的身份,请求验证.

2) CA1 收到消息后,对其进行解密,并校验网关的身份.校验通过后选择不大于 q 的整数 d_i,并计算 $PK_{gw_i}^2 = d_i \cdot P$, $SK_{gw_i}^2 = d_i + SK_1 \cdot H_0(ID_{gw_i}, PK_{gw_i}^2, PK_{gw_i}^1)$,而后利用网关的公钥对其进行加密 $EN_{PK_{gw_i}^1}(SK_{gw_i}^2 \| PK_{gw_i}^2)$,并发送回网关.在这一步的操作中,CA1 以密文方式回复给该网关完整的跨域交互所需公私钥对.

3) 网关解密该消息之后,得到自身的完整密钥对 $SK_{gw_i} = (SK_{gw_i}^1, SK_{gw_i}^2)$, $PK_{gw_i} = (PK_{gw_i}^1, PK_{gw_i}^2)$,同时网关对该私钥进行验证.令 $h_i = H_0(ID_{gw_i}, PK_{gw_i}^2, PK_{gw_i}^1)$,若 $PK_{gw_i}^2 + h_i \cdot PK_1 = SK_{gw_i}^2 \cdot P$,则证明密钥可信.此时向 CA1 发布 $EN_{PK_{gw_i}}(ACK)$,CA1 将 $ID_{gw_i}, PK_{gw_i}^2, PK_{gw_i}^1, PR_{gw_i}$ 发布到链上.其中 PR_{gw_i} 指该域的授权模式.在这一步中,网关对自身获取到的身份进行了确认,且 CA 将其发布到链上,与其余 CA 进行了共享.

3. 设备注册到网关

由于部分哑设备不具备远距离通信及自主密钥的管理,网关协助 CA 对设备身份进行管理.鉴于设备与用户的行为直接相关,隐私敏感,本文分析如下.

1) 网关用于扩展设备的安全及通信能力,与设备直接连接,获取到的是设备的明文信息.

2) 设备的身份及行为与用户密切相关,有必要对链上其余 CA 及网关保密.

3) 设备本身具有移动性,应确保即使其更换所属网关,仍可继续使用.

在此基础上,本文为设备设计流程如下:

1) 网关与设备建立连接,获取到设备的能力 $f_j = \{method : type\}$ 并配置设备的权限管理策略 PRT_j.

2) 网关对设备实施匿名化:生成随机数 w 后计算 pid_j=hash(w + id_j),在本地建立身份映射.

3) 生成设备 j 的本地密钥对 PKT_j^1 并用网关的域内私钥签名,完成域内注册.此时该网关域内的设备可对该新注册的设备进行访问.

4) 网关向自己所属的 CA 发出注册请求,该请求中包含有设备的匿名身份、功能列表、权限;

5) CA 校验了网关的签名后,为设备生成 PKT_j^2,得到网关的确认消息及设备信息后,使用设备注册合约将设备信息如功能描述、设备公钥、密钥版本、密钥有效期等发布上链.

6) 网关注销后,由于设备信息仍可在链上查到,仍可通过校验,但由于更新设备信息需要该网关签名,因此如之前注册设备时使用的网关注销,而需要更新权限规则或功能列表等信息,需重新注册到其他网关.

7) 设备如需更新,网关可对更新信息进行签名并发布上链.注销是一种特殊的更新:将该设备状态更新为不可用.为了避免设备行为被持续的分析挖掘,可通过对设备进行重新注册后注销原 ID 进行隐蔽.

4. 跨域通信

考虑以下两种情况:1)设备自身即具备与外部通信的能力,向非自身所在域的网关请求调用其他设备.2)通过网关向其余网关请求对应设备的服务.

对于第一种情形,当 gw_m 域的设备 pid_j 访问 gw_i 的资源的时候,执行如下操作:

1)设备利用自己的域内私钥及跨域私钥并结合随机数完成签名并加密,而后利用网关 gw_i 的公钥对随机数进行加密.由 j 随机选取两个不大于 q 的整数 r_1, r_2,计算 $T = r_1 \cdot P$, $h = H_1(T + PKT_j^1, pid_j)$, $s = \dfrac{(r_1 + SKT_j^1)}{(SKT_j^1 + h \cdot SKT_j^2)}$.而后计算 $R = r_2 \cdot P$, $C = H_2(R) \oplus (pid_j \| s)$,计算 $Y_i = r_2 \cdot (PK_{gw_i}^1 + PK_{gw_i}^2 + h_i \cdot PK_1)$. 而后,发出密文 $\delta = (Y_i, T, C)$.该信息不含明文,仅有目标所在网关可恢复携带信息.

2）网关收到后,首先利用自身身份解密,获取到设备的签名及身份.而后对设备的身份展开校验.

解密过程:

$R' = (SK_{gw_i}^1 + SK_{gw_i}^2)^{-1} Y_i'$

根据 R' 恢复原始信息,设备身份 pid_j 及 s :

$pid_j \| s = H_2(R') \oplus C$

计算哈希值以完成校验:

$h_{i'} = H_0(ID_{gw_i}, PK_{gw_i}^2, PK_{gw_i}^1)$

$h' = H_1(T + PKT_j^1, PKT_j^2, pid_j)$

若 $h' = H_1(s \cdot (PKT_j^1 + h' \cdot (PKT_j^2 + h_{i'} \cdot PK_1)), pid_j)$,可确认设备身份.如该设备身份符合访问控制,则与其协商本次会话密钥展开通信.

第二种情形与第一种类似,但以网关的身份对设备进行调用.此时 $C = H_2(R) \oplus s$.验证网关身份后,根据访问控制策略决定是否执行来自该网关的指令.

假定 m 域的设备 pid_j 访问 n 域内的 pid_i ,跨域访问流程如下:

Algorithm **1** Cross-domain Procedure

算法 1 跨域访问流程

Algorithm1:m 域的设备 pid_j 访问 n 域内的 pid_i

1: 获取 pid_i 权限配置

pid_j 通过 gw_m 调用合约,获取到 gw_n ,及为 gw_n 签发身份的 CA

2: gw_m 校验 pid_i

if PRT_i 存在（即 $PR_{gw_n} = public$ ）//设备 i 的权限策略可查

gw_m 校验本地是否存在 pid_i 对 pid_j 的授权

若无权限,执行第三步

若有权限,则按照 pid_j 的参数发起调用并返回结果

else if $PR_{gw_n} = protect$ //设备 i 的权限需向 n 域的网关申请

gw_m 查询是否有 gw_n 的权限

若无权限,执行第四步

若有权限,按照 gw_m 的参数调用 pid_i

else(即 $PR_{gw_n} = private$) //设备 i 的权限需向设备 i 申请

执行第三步

3: gw_m 以 pid_j 身份向 gw_n 申请 pid_i 权限

生成 $r_1, r_2 \in Z_q^*$, $s = (r_1 + SKT_j^1) / (SKT_j^1 + h \cdot SKT_j^2)$

$T = r_1 \cdot P$, $h = H_1(T + PKT_j^1, PKT_j^2, pid_j)$

$R = r_2 \cdot P$, $C = H_2(R) \oplus (pid_j \| s)$

$Y_i = r_2 \cdot (PKT_i^1 + PKT_i^2 + h \cdot PK_{gw_n}^1)$,

发送 δ=(Y_i,T,C) 到 gw_n 进入第五步

4: gw_m 向 gw_n 申请授权

发送 gw_m 签名的授权请求

生成 $r_1 \in Z_q^*$

$s = (r_1 + SK_{gw_i}^1) / (SK_{gw_i}^1 + h \cdot SK_{gw_i}^2)$

$h_m = H_0(ID_{gw_m}, PK^2_{gw_m}, PK^1_{gw_m})$

$R = r_2 \cdot P$, $C = H_2(R) \oplus s$

$Y_i = r_2 \cdot (PK^1_{gw_n} + PK^2_{gw_n} + h_m \cdot PK_2)$（假定 gw_n 由 CA2 签署）

发送 $\delta = (Y, C)$ 到 gw_n 进入第五步

5: gw_n 校验身份

$h_i' = H_0(ID_{gw_i}, PK^2_{gw_i}, PK^1_{gw_i})$

$R' = (SK^1_{gw_i} + SK^2_{gw_i})^{-1} Y_i'$

$s = H_2(R') \oplus C$

if 请求来自设备 pid_j

$h' = H_1(T + PKT^1_j, PKT^2_j, pid_j)$

若 $h' = H_1(s \cdot (PKT^1_j + h' \cdot (PKT^2_j + h_i' \cdot PK^1_{gw_m})), pid_j)$,校验通过

if 请求来自网关

$h_m' = H_0(ID_{gw_m}, PK^2_{gw_m}, PK^1_{gw_m})$

若 $h' = H_1(s \cdot (PK^1_{gw_m} + h' \cdot (PK^2_{gw_m} + h_m' \cdot PK_2)))$,校验通过

3.2 消息协议设计

设备接入到网关的底层通信协议根据设备的不同有所不同,但写入到网关的上层数据格式可进行统一如下.

设备的信息按照 json 格式列出如下:

Device {

“Type”:devicetype,//设备类型

“ID”:deviceID,//设备 ID

“GID”:Gateway ID,//所属网关

“Version”:key version//密钥版本

“Pubkey”:public key,//设备公钥

“keyvalue”: [

Key:protected key//私钥或加密后的私钥

Keytype:key//密钥生成算法

Validate:validate,//密钥有效期

]

“Permission”:permissioned type,//权限许可类型 PRT

“Privacy”:[//隐私描述

“Period”: key period, //密钥更新周期

“Signdate”:Sign date,//当前密钥签发时间

]

“Deviceswitch”:switch,//设备开关

“devicefunction”:[

“func1”:value 1,//设备功能 1 的值

“func 2”:value 2, //设备功能 2 的值

“func n”:value n, //设备功能 n 的值

]

}

其中,当设备密钥由设备自身生成时填写加密后的私钥,由网关生成则直接填充密钥.

权限许可类型分为三类:public,protected,private 三类,对于 public 设备可直接发起调用,protected 需获取到本地网关的许可,private 情形下需获取到设备自身的许可.privacy 部分填充密钥更新的频率.此字段为空时说明无需更换.

网关与 CA 及联盟链之间的交互主要包括以下几项:设备的注册、更新、以及查询.

网关向 CA 发起的请求格式如下:

```
Request {
    “gateway”:gatewayID,//网关 ID
    “CA”:CAid,//为该网关签发许可的 CA 公钥
    “commandtype”:command,//请求类型,包括写入、更新、查询.
    “DeviceID”:Public key,//对应的设备公钥
    “Description”:[
        “Attribute1”:value1,//属性 1
        “Attribute2”:value2,//属性 2
    ],//对于写入及更新的请求,需要更新的信息封装为 json 字段
}
```

查询请求的 description 字段为空,合约为其返回对应设备的信息.注册请求需提供设备描述及权限许可等属性信息.更新请求的 description 字段只包括需要更新的信息.

网关向网关发出的跨域认证请求如下:

```
Authenticate{
    “gateway”:gatewayID,//网关 ID
    “CA”:CAid,//为发起请求的网关签发许可的 CA 公钥
    “message1”:Y,
    “message1”:T,
    “message1”:C,//Y,T,C 为网关为设备跨域访问生成的加密字段
    “time”:timestamp;
}
```

当收到请求的网关完成验证,交换会话密钥后,网关向网关发出的跨域访问请求如下.

```
Access{
     “gateway”:gatewayID,//网关 ID
    “CA”:CAid,//为发起请求的网关签发许可的 CA 公钥
    “DeviceID”:Public key,//需控制的设备公钥
    “Deviceswitch”:switch,//设备开关
    “commandtype”:[
        “func1”:value 1,//设备功能 1 的值
        “func 2”:value 2, //设备功能 2 的值
        “func n”:value n, //设备功能 n 的值
    ]
    “time”:timestamp;
}
```

此时收到请求的网关校验权限允许之后,执行 conmandtype 中的函数.

4 认证机制分析

4.1 正确性证明

在 3.1 的机制设计中,提出了认证时使用的数据,被请求的网关校验通过后证明该请求来自于合法的网关或设备.其中为证明校验的正确性,证明如下:

根据设计的协议,需要证明以下两处: $R'=R$,即网关根据自身密钥恢复出的数据确为加密前的原始数据. $h'=h$,即在数据未经过篡改的情况下,恢复出的哈希值 h' 与原数据的哈希相同.

对设备与网关的 R 与 h 计算及校验过程类似,以对设备的校验为例进行证明:

$$
\begin{aligned}
R' &= (SK_{gw_i}^1 + SK_{gw_i}^2)^{-1} Y_i' \\
&= (SK_{gw_i}^1 + SK_{gw_i}^2)^{-1} \cdot r_2 \cdot (PK_{gw_i}^1 + PK_{gw_i}^2 + h_i \cdot PK_1) \\
&= r_2 \cdot (SK_{gw_i}^1 + SK_{gw_i}^2)^{-1} (P \cdot SK_{gw_i}^1 + PK_{gw_i}^2 + h_i \cdot SK1) \\
&= r_2 \cdot (SK_{gw_i}^1 + SK_{gw_i}^2)^{-1} \cdot (P \cdot SK_{gw_i}^1 + P \cdot SK_{gw_i}^2) \\
&= r_2 \cdot P = R
\end{aligned}
$$

对 h 的证明如下:

$$
\begin{aligned}
h' &= H_1(s \cdot (PKT_j^1 + h' \cdot (PKT_j^2 + h_{i'} \cdot PK_{gw_m}^1)), pid_j) \\
&= H_1(\frac{(r_1 + SKT_j^1)}{(SKT_j^1 + h \cdot SKT_j^2)} \cdot (P \cdot SKT_j^1 + h' \cdot (SKT_j^2 \cdot P)), pid_j) \\
&= H_1(P \cdot (r_1 + SKT_j^1), pid_j) \\
&= H_1(T_1 + PKT_j^1, pid_j) \\
&= h
\end{aligned}
$$

4.2 安全性证明

针对网关的安全性分析:在本文设计的架构中,设备的隐私保护与跨域访问校验均通过网关完成,因此系统整体安全依赖于网关.网关的职能在于对单个物理域或信任域内的设备进行统一的汇聚及管理,可部署于用户的个人终端或小型服务器.考虑到用户通过网关对设备进行直接操控,攻击者如攻击网关绕过本系统架构直接获取权限,可认为该网关已被攻破,注销该网关即可.

以下为常见攻击的分析.

拒绝服务攻击:本文设计的架构中,利用多 CA 构建基于区块链的认证服务机制.攻击单个 CA 之后,仍可在其余 CA 维护的区块链上查询到正确的网关及设备信息,抗 DDoS 攻击能力显著增强.

伪造攻击:本处讨论对设备的伪造和对网关的伪造.为了通过伪造攻击,攻击者需要伪造一个能够通过认证的请求信息 δ .对于伪造设备,其无法获得 SKT_j^1 和 SKT_j^2 ,因此无法生成 s ,进而无法生成 C ,无法通过校验;同理,对于伪造网关,无法获得 $SK_{gw_i}^1$ 和 $SK_{gw_i}^2$,同样无法通过校验.由于无法获得密钥,即使盗取设备或网关也无法实施智能卡丢失攻击.

内部攻击:由于网关提交到区块链的身份,以及跨域交互所需的身份仅为设备的公钥 PKT^1,PKT^2 ,仅能证明设备合法,无从确认设备的真实身份 pid ,无法形成内部攻击.仅有直接与设备连接的本地网关可完成设备公钥到设备身份的映射.此外,设备可要求网关对设备的密钥进行更新,以避免被追踪.

服务欺骗攻击:伪造被访问的资源需要 $SK_{gw_n}^1, SK_{gw_n}^2$ 对信息 R 进行解密,伪造服务解密该信息需解决离散对数问题,代价巨大.

重放攻击:发布到链上的信息带有时间戳,网关之间的交互协议均带有时间戳,保证消息新鲜.此外,随机数部分保证每次发布的消息均不同.

中间人攻击:由于中间人无法实施伪造攻击将自己伪装为用户或网关,也无法实施服务欺骗攻击提供服务,

因而无法实施中间人攻击窃取信息.

4.3 隐私分析

本文针对的隐私保护在于CA之间数据共享造成的跨云服务器之间的数据共享,考虑到物联网直面用户的特性,主要隐私涵盖以下两处:设备的身份与设备的行为.

设备的身份隐私:设备的真实身份在网关处做了匿名化的处理,防止透露个人信息.如网关 i 操控的设备中涵盖了一盏灯,在屏蔽其真实 ID 信息进行归一化处理之后,无法从中推测灯的型号等信息,其余网关或设备仅知道在获取相应权限之后可对其进行状态查询及开关操作,不存在[10-14]中身份明文上链带来的隐私问题.

设备的行为隐私:行为泄露来源于两方面,由于设备仅有必要的描述信息发布在链上,因此规避了[15]中每次访问请求均上链导致的行为泄露.在交互过程中全程采用密文传输,交互行为仅双方网关知晓,避免了明文调用带来的危险.

4.4 开销分析

本文与[18]和[19]的方案进行对比.在该两种方案中,CA 多方完成校验之后,将签署本轮访问的凭证上链,凭证内容为在某有效期内,允许外域的某身份访问本域.此处针对从 A 域的身份 i 发起请求至获取到本次访问所需凭证的计算及通信进行比对如下表 1 及表 2.其中其他计算指代本文在 3.1 节中构造的加解密计算.

Table 1 Communication consumption

表 1 通信开销对比

名称	某 CA-其他 CA	网关-区块链或 CA	本地-其他网关	共识
[18]	0	2	5	1
[19]	3	2	1	0
本方案	0	1	1	0

根据表 1 的通信开销对比,本文设计的方案在 CA 之间、网关之间、网关到区块链之间的通信次数都显著低于[18][19]提出的方案,在通信开销上具有显著优势.

Table 2 Computing consumption

表 2 计算开销对比

方案	公钥加密次数		私钥解密次数		签名次数		验证次数		哈希运算		共识次数	其他运算
	本地网关	CA	本地或网关	CA	本地或网关	CA	本地或网关	CA	本地或网关	CA		
[18]	0	0	0	0	1	0	1	1	1	1	1	
[19]	3	3	3	3	2	2	3	1	0	0	0	
本方案	1	0	1	0	1	0	1	0	4	0	0	2

表 2 的计算开销显示,由于通信次数少,本文的公私钥加解密次数较[19]显著偏少,但高于[18],而执行哈希运算次数显著高于[18][19].此外,本方案中涉及到的计算均在网关展开,认证过程不占用 CA 资源.

详细的计算开销及通信开销将在 5.2 认证阶段的实验中展开比对.

5 实验设计及分析

在本文中,考虑到网关与设备距离极近,不考虑网关到设备之间的传输时延.同时,假定网关-网关之间、网关-CA 之间的传输时延均为 T.

联盟链实验环境为部署于金山云上的 1 核 2G 服务器,Ubuntu 16.04 系统.联盟链采用 Hyperledger Fabric 1.4.0,并利用 docker 容器部署联盟链节点,智能合约采用 JavaScript 进行编写.网关及 CA 实验环境为 Windows10 系统,CPU 主频 1.6 GHz,内存 4GB.跨域认证流程采用 Python3.8 模拟实现,实验数据均为运行 50 次的平均值.

5.1 注册阶段

在本文中,定义注册所需的时间为设备请求到设备信息可在链上查询到的时间.分为四部分:

t_1为网关为设备生成密钥的时间,t_2为网关调用合约的时间,t_3为 CA 之间达成共识的时间,t_4为网关查询到合约所需的时间.其中t_1不考虑网关到设备之间的传输时延,t_4仅考虑网关到 CA 之间的传输时延.

由于t_1阶段与传统流程无差别,以及传统流程同样需要写入及查询的时间.因此本节的实验模拟仅考虑采用本架构后增加的时延$t_2+t_3+t_4$,即从请求发布到链,到共识结束.

对于t_2阶段,对注册及更新信息进行打包发布上链.测试结果表明,对于每个注册请求,网关对数据进行打包并提交交易的时间约为2060ms,记作t_S,并随着注册请求个数呈现线性增长.假设网关以固定的时间间隔T进行信息发布,注册及更新信息分布服从参数为λ泊松分布,则每个周期内产生的注册请求个数为λT.

假设网关收集注册请求的时段为[t,t+T],某个设备的请求在$t+t_0$到来,且$\lambda t_0 \cdot t_s < T_0$则存在以下两种可能性:

$$\begin{cases} t_0+t_s \le T_0, \text{则该请求在本轮被提交，} t_2=T_0-t_0 \\ t_0+_s > T_0, \text{则该请求在下一轮被提交，} t_2=2T_0-t_0 \end{cases}$$

则t_2的期望值如下:

$$\begin{aligned} E(t_2)&=\mathrm{E}((T_0-t_0)\cdot\frac{T-t_s}{T}+(2T_0-t_0)\cdot\frac{t_s}{T}) \\ &=E((T_0-t_0)+t_s) \\ &=T_0/2+t_s \\ &\ge 3t_s/2 \end{aligned}$$

考虑到每个收集间隔至少应能打包一份请求,因此存在$T_0 \ge t_s$.由此可知t_2的期望值约为 3090ms.

Table 3 Consensus delay

表 3 共识时延

节点数目	平均运行时延（ms）
4	72
6	74
8	76

对于t_3+t_4阶段,即数据提交上链到结束共识的时间,本文分别对 4,6,8 个 CA 的情形进行模拟,取平均值如表 3.实验结果证明,本文设计的模式下,注册从提交到生效仅增加约 3.17s 的时延.考虑到注册环节对时延的要求不高,且随着 CA 性能提升,该阶段的时延可以迅速下降,本文设计的模式仍然具备实用性.

5.2 认证阶段

本节对本文及[18][19]所设计的跨域认证方案在不同椭圆曲线下进行了模拟.[18]设计的方案中,将各信任域的认证服务器作为区块链节点,域间跨域认证通过查询验证对方域的根 CA 证书服务发布在链上的无签名证书实现.但[18]的设计中大量采用明文通信,隐私泄露风险极大.[19]的设计中基于 SM9 国密算法改进了证书的设计,每次完成认证后将本次认证密钥写入区块链,证书有效期超出之前均可凭借该证书访问.[19]的设计意味链上存储的是实体之间的交互许可.考虑到区块链可增可查不可删改的特性,随着用户的增长,将带来巨大的查询压力.本文在[18]的设计理念基础之上增加了签名校验及加解密计算,在高效同时提高了安全性.实验结果证明,本文方案的时延损耗在常用的椭圆加密曲线下具有优势.

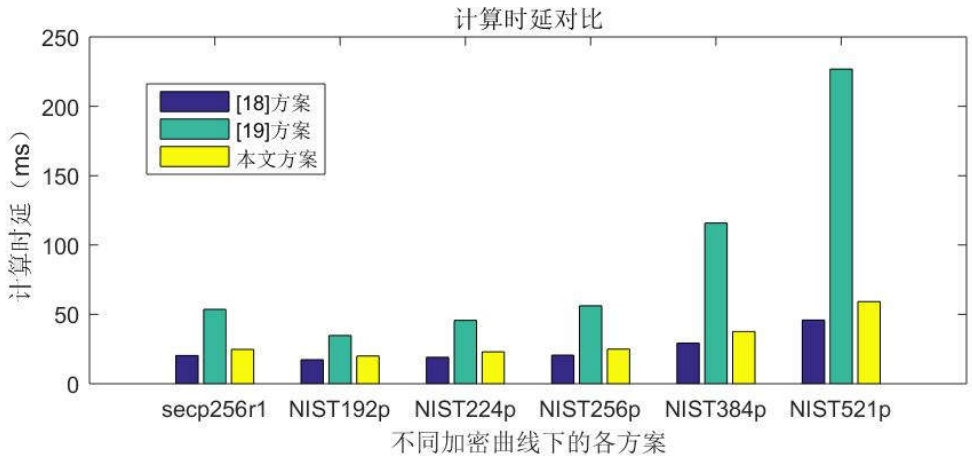

Fig.3 Time delay comparsions between our method and traditional method

图 3　本文认证时延与传统时延对比

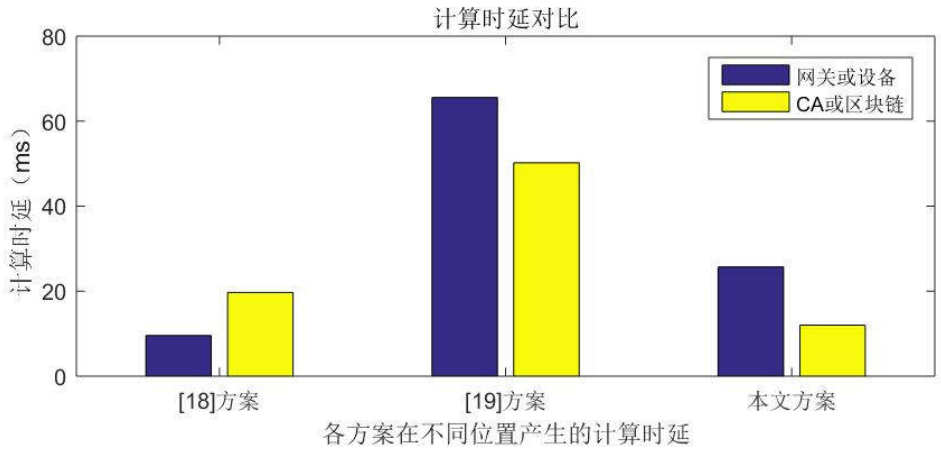

Fig.4 Time delay of different sides in different ways

图 4　不同方法下不同侧的时延

如图 3 所示,在每种加密曲线中,[19]均带来最高的时延,[18]产生的时延最小,本文设计产生的时延接近于[18].随着采用的加密曲线更加复杂,三者之间差距更加明显.考虑到 CA 及区块链部署于云服务器上,计算性能较强,而网关及设备能力计算能力较弱,按照 4.4 的计算开销分析再次展开详细分析.鉴于不同加密曲线下呈现出相同的趋势,以 NIST384p 为例对用户侧的网关及设备、服务器侧的 CA 及区块链计算时延进行分析.

如图 4 所示,[18][19]的方案中大部分计算在服务器端完成,通过提高服务器端性能可大幅降低计算时延迟.但由于大量计算部署在服务器端,给网络带来了较大的通信开销.结合 4.4 中表 1 的通信开销分析,以 NIST384p 为例,其身份信息为 48 字节,签名长度为 104 字节.参照[18]的设定,消息平均长度为 24 字节.按照[19]的假设,证书长度为定长 16 字节,随机数长度为 24 字节.则各端通信量分别分析如下:

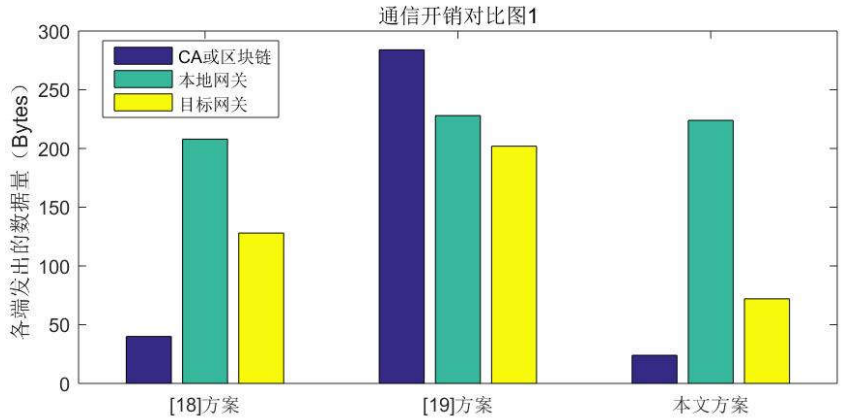

Fig.5 Outgoing data of different sides in different ways

图 5 不同方法下不同侧发出的数据量

图 5 计算各端发出的数据量,据图可观察到以下现象:

1）[19]的 CA 或区块链发出的数据量最多,本文最少.原因在于[18]和[19]均需要反复从 CA 或链上获取到证书信息,而本文仅查询一次网关或设备的信息.

2）本地网关发出的数据三者接近,[19]略高于本文,[18]最低.因此在请求时未造成网关的额外负担.

3）对于目标网关,[19]发出的数据量最多,[18]次之,本文最少.原因在于本文的目标网关确认访问者的身份后,在本地决策是否授权,此外网关之间直接通信,减少了通过 CA 进行中转及转换的环节.由此可知,收到请求的网关同样未给网络带来额外压力.

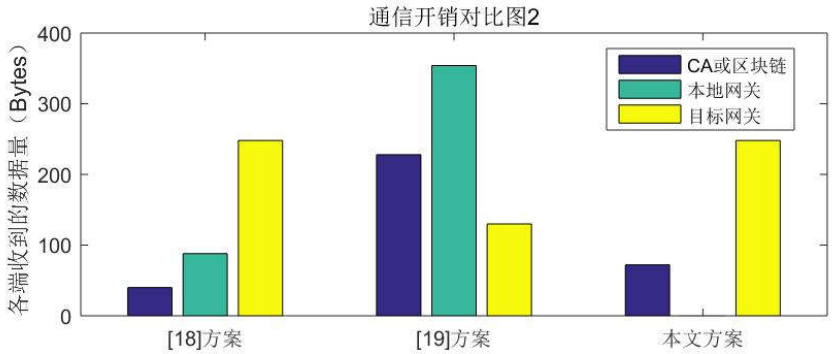

Fig.6 Incoming data of different sides in different ways

图 6 不同方法下各端收到的数据量对比

图 6 计算各端收到的数据量,据图可观察到以下现象:

1） [19]的 CA 或区块链收到的数据量最多,本文其次,[18]最少.这一点符合常识:认证过程主要从服务器请求判断凭证而非上传新的数据.[19]中不同 CA 互相确认身份的流程较为复杂,因此交互数据量较大.[18]由于认证包含的信息简单且交互次数较少,数据量最少.本文在简化认证流程的基础上增加了用于确保信息安全的操作,数据量略高于[18].

2） 对于本地网关,[19]收到的数据量最多,[18]次之,而本文发出请求并签名后仅等待对方提供服务不再确认,因此本地网关的认证过程不再收到消息.而对于目标网关,[18]收到的数据量最多与本文收到的

数据量持平,[19]最少.

3） 对于目标网关,本文与[18]收到的数据量持平,而[19]最少.[18]及本文均需携带认证信息访问目标网关,而[19]仅需获取用户身份,决定通过校验后将证书写入区块链.

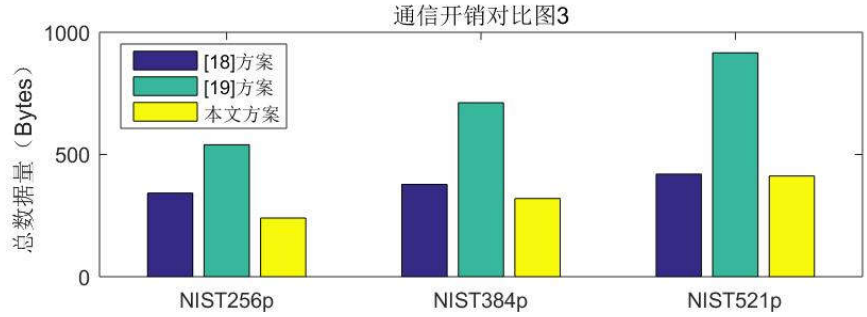

Fig.7 data colume in different curves

图 7 不同方法下总的数据量对比

总体的通信量对比如图 7.可以看到由于签名和加解密的环节极少,更换加密曲线对[18]几乎不造成影响;反之由于签名和加解密环节较多,[19]的开销随着加密曲线的复杂迅速上升.本文由于网关之间直接进行信息交换,仅调用一次区块链进行查询,因此步骤简洁,开销较少.

根据以上的仿真结果及分析,本文设计的认证方法在时延和通信量上均具有较好的性能.

6 结语

本文针对物联网建设封闭导致的认证复杂,提出了基于区块链构建多 CA 合作认证的思想,进而提出了基于联盟链的跨域物联网信任.其核心内容是:部署边缘网关对兼容物联网的多种接入协议,同时利用多 CA 实现网关可信接入、设备可信校验,从而大幅度缩减传统认证模式导致的互操作困难、认证流程复杂、认证系统冗余建设等问题.在提出系统架构、部署方式、运行流程的基础上,设计适用于物联网的跨域认证协议,并对其进行了正确性、安全性及开销的分析.

但区块链应用于物联网中仍存在大量的风险及挑战:首先,多中心备份的服务方式在促进可信合作的同时,作为完整节点参与到区块链需对链上全部信息进行存储,成本显著上升;其次,区块链本身增量不可删除的特性,也导致其数据不断增长,规模化实施之后查询效率难以保证;此外,在匿名化保证隐私和身份可认证确保可信之间存在微妙的平衡,在实际部署中更要参考相关法律法规的指导;物联网的环境错综复杂,完整节点难以到达‘最后一公里’确保数据可信发布,而设备常以微弱的计算及安全性能暴露在大量攻击下,难以保证上链的数据确实可信.下一步工作将针对网关及设备的信任评估及权限控制进行展开,进一步提高网络的安全性.

References:

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. In: Consulted. 2008

[2] Hari, A. and T.V. Lakshman, "The Internet Blockchain: A Distributed, Tamper-Resistant Transaction Framework for the Internet," *Proc. ACM Workshop on Hot Topics in Networks*. 2016. 204 - 210.

[3] Muneeb Ali, Jude Nelson, Ryan Shea, and Michael Freedman. "Blockstack: A Global Naming and Storage System Secured by Blockchains" *Proc. USENIX Annual Technical Conference (USENIX ATC 16)*, 2016. 181-194.

Conner Fromknecht, Dragos Velicanu, Sophia Yakoubov. A decentralized public key infrastructure with identity retention. Technical Report, 803, MassachusettsInstitute of Technology, 2014.

[4] Axon L, Goldsmith M. PB-PKI: A privacy-aware blockchain-based PKI. In: Proc. of the Int'l Conf. on Security and Cryptography.

2017. 311–318. [doi: 10.5220/0006419203110318]

[5] Christidis K, Devetsikiotis M. Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 2016, 4:2292-2303.[doi: 10.1109/access.2016.2566339]

[6] Kshetri N. Can Blockchain Strengthen the Internet of Things?. IT Professional, 2017, 19(4):68-72.[doi: 10.1109/MITP.2017.3051335]

[7] Lewis Tseng, Liwen Wong, Safa Otoum, Moayad Aloqaily, and Jalel Ben Othman. Blockchain for Managing Heterogeneous Internet of Things: A Perspective Architecture. IEEE NETWORK, 2020,34(1):16-23.[doi: 10.1109/MNET.001.1900103]

[8] Huh S, Cho S , Kim S . Managing IoT devices using blockchain platform,2017 19th International Conference on Advanced Communication Technology (ICACT). IEEE, 2017. [doi: 10.23919/ICACT.2017.7890132]

[9] Olivier Alphand,Michele Amoretti,Timothy Claeys,Simone Dall'Asta ,Andrzej Duda,Gianluigi Ferrari ,Franck Rousseau,Bernard Tourancheau,Luca Veltri,Francesco Zanichelli, IoTChain: A blockchain security architecture for the Internet of Things. 2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2018. [doi:10.1109/WCNC.2018.8377385]

[10] Sharma P K , Chen M Y , Park J H . A Software Defined Fog Node based Distributed Blockchain Cloud Architecture for IoT. IEEE Access, 2017:1-1.[doi: 10.1109/ACCESS.2017.2757955]

[11] Novo, Oscar. Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT. IEEE Internet of Things Journal, 2018:1-1.[doi: 10.1109/JIOT.2018.2812239]

[12] Song W, The System of IoT Identity Authentication Based on Blockchain.[M.S.Thesis].Xidian University.2018. (in Chinese with English abstract)

[13] He Y, The research and design of blockchain support platform for the Internet of things applications.[M.S.Thesis].Beijing University of Posts and Telecommunications.2018. (in Chinese with English abstract)

[14] Mei C, The design and implementation of IoT security platform based on blockchain. [M.S.Thesis].Beijing University of Posts and Telecommunications.2018. (in Chinese with English abstract)

[15] Wan Y, Research on the cross-domain authentication under the environment of the Internet of things. [M.S.Thesis].Beijing University of Posts and Telecommunications.2018.(in Chinese with English abstract)

[16] Wang W , Hu N , Liu X . BlockCAM: A Blockchain-Based Cross-Domain Authentication Model, 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). IEEE, 2018.[doi: 10.1109/DSC.2018.00143]

[17] Zhou Z,Li L, Li Z, Efficient cross-domain authentication scheme based on blockchain technology, Journal of Computer Applications,2018,38(2) : 316 － 320,3262018 (in Chinese with English abstract) . [doi: 10.11772/j.issn.1001-9081.2017082170]

[18] Ma X, Ma W, Liu X,A cross domain authentication scheme based on blockchain Technology, Acta electronica sinica,2018,46(11) : 2571－2579,2018 (in Chinese with English abstract) . [doi: 10.3969/j.issn.0372-2112.2018.11.002]

[19] Ao Lei, Haitham Cruickshank , Yue Cao, Philip Asuquo, Chibueze P. Anyigor Ogah, and Zhili Sun. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. IEEE Internet of Things Journal, 2017, PP(99):1-1.[doi: 10.1109/JIOT.2017.2740569]

[20] Thomas H, Alex P, Verifiable anonymous identities and access control in permissioned blockchains. Technical Report, Massachusetts Institute of Technology, 2016. https://arxiv.org/pdf/1903.04584.pdf

[21] Ma M, Shi G, Li F. Privacy-Oriented Blockchain-based Distributed Key Management Architecture for Hierarchical Access Control in the IoT Scenario. IEEE Access, 2019, 7: 34045-34059.[doi: 10.1109/ACCESS.2019.2904042]

[22] Shicho cha, Jyunfu Chen, Chunhua Su, and Kuohui Yeh. A Blockchain Connected Gateway for BLE-based Devices in the Internet of Things. IEEE Access, 2018:1-1.[doi: 10.1109/ACCESS.2018.2799942]

[23] Yingying Yao, Xiaolin Chang, Jelena Miši´,Vojislav B. Miši´ c, and Lin Li. BLA:Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services. IEEE Internet of Things Journal, 2019:1-1.[doi: 10.1109/JIOT.2019.2892009]

[24] Byungseok Kang, Daecheon Kim, and Hyunseung Choo. Internet of Everything: A Large-Scale Autonomic IoT Gateway. IEEE Transactions on Multi-Scale Computing Systems, 2017,(3):206-214.[doi: 10.1109/TMSCS.2017.2705683]

附中文参考文献:

[13]宋文斌. 基于区块链的物联网身份认证系统[硕士学位论文].西安:西安电子科技大学,2018.
[14]贺毅. 面向物联网应用的区块链支撑平台的研究与设计[硕士学位论文]北京:北京邮电大学, 2018.
[15]梅晨. 基于区块链的物联网安全平台的设计与实现[硕士学位论文]北京:北京邮电大学, 2018.
[16]万雨薇.物联网环境下的跨域认证机制研究[硕士学位论文]南昌:南昌大学, 2018.
[18]周致成,李立新,李作辉.基于区块链技术的高效跨域认证方案.计算机应用,2018.[doi: 10.11772/j.issn.1001-9081.2017082170]
[19]马晓婷,马文平,刘小雪. 基于区块链技术的跨域认证方案. 电子学报, 2018, 46(11):2571-2579. [doi: 10.3969/j.issn.0372-2112. 2018. 11.002]