软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, 2022,33(7):2699−2715 [doi: 10.13328/j.cnki.jos.006288]

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

面向智能家居的区块链轻量级认证机制*

张珠君[1,2], 范 伟[1], 朱大立[1]

[1](中国科学院 信息工程研究所, 北京 100093)

[2](中国科学院大学 网络空间安全学院, 北京 100049)

通信作者: 范伟, E-mail: fanwei@iie.ac.cn

摘 要: 5G 技术为智能家居行业开拓了更大的发展空间, 但安全问题也日益突出, 用户身份认证作为信息安全防护的第一道关卡备受关注. 智能家居系统传统的认证方法存在中心化信任挑战, 且资源开销大. 区块链技术因其去中心化、不可篡改等优势成为研究热点, 为实现分布式智能家居系统安全认证提供了新思路. 但无中心认证面临着用户与多个分布式终端认证的效率问题和用户隐私泄露问题两个方面的挑战. 提出了一种基于区块链的动态可信轻量级认证机制(dynamic trusted lightweight authentication mechanism, DTL). DTL 机制采用联盟链构建区块链系统, 既保证了仅授权的智能家居传感器节点可加入网络, 又满足分布式高效认证和安全访问需求. DTL 具有以下优点: (1) 针对认证效率问题, 通过改进共识算法建立面向智能家居的动态可信传感设备组(DT sensor group, DTSG)认证机制, 避免了传统的用户端与传感终端或者网关节点之间一对一的频繁认证引起的接入效率低和用户访问速率低问题, 实现了轻量级认证; (2) 针对用户隐私保护问题, 创新性地设计了 DTSG 机制和零知识证明结合的认证方案, 在不泄露用户隐私情况下, 实现了用户身份的认证. 对 DTL 的安全特性进行了定性分析, 并通过大量仿真实验对 DTL 的实用性和轻量级进行了验证.

关键词: 智能家居; 区块链; 动态可信轻量级认证; 零知识证明

中图法分类号: TP309

中文引用格式: 张珠君, 范伟, 朱大立. 面向智能家居的区块链轻量级认证机制. 软件学报, 2022, 33(7): 2699–2715. http://www.jos.org.cn/1000-9825/6288.htm

英文引用格式: Zhang ZJ, Fan W, Zhu DL. Lightweight Blockchain Authentication Mechanism for Smart Home. Ruan Jian Xue Bao/Journal of Software, 2022, 33(7): 2699−2715 (in Chinese). http://www.jos.org.cn/1000-9825/6288.htm

Lightweight Blockchain Authentication Mechanism for Smart Home

ZHANG Zhu-Jun[1,2], FAN Wei[1], ZHU Da-Li[1]

[1](Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

[2](School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: The promotion of 5G provides new opportunities for the rapid development of the smart home industry, while the authentication issue of smart home systems has become a concern. The traditional centralized management and authentication methods adopted by smart home systems face centralized trust issues, and have the disadvantages of high performance overhead. Blockchain technology has become a research hotspot due to its advantages of decentralized and non-tampering features, providing new ideas for the realization of security certification for distributed smart home. Nevertheless, it also faces two challenges: the efficiency of user authentication with multiple distributed terminals and the leakage of user privacy. This study proposes a dynamic trusted lightweight authentication mechanism (DTL) based on blockchain. DTL uses consortium blockchain to build a blockchain system, which not only ensures that only authorized smart home sensor nodes can join the network, but also meets the needs of distributed security and scalability. DTL can achieve the following two advantages. (1) Aiming at the issue of authentication efficiency, by improving the consensus algorithm, a dynamic trusted sensor group (DTSG) authentication mechanism for smart homes is established, which avoids low access efficiency and low user access rate

* 收稿时间: 2020-05-14; 修改时间: 2020-07-16, 2020-10-20, 2020-11-30; 采用时间: 2020-12-20

caused by one-to-one frequent authentication between the user and sensor terminal or gateway node. DTL has realized lightweight authentication. (2) For addressing the problem of user privacy protection, an authentication scheme combining DTSG mechanism and zero-knowledge proof is innovatively designed, which realizes user identity authentication without leaking user privacy. These security features are demonstrated by carrying out security analysis. Meanwhile, extensive simulations are conducted to validate the practicality and lightweight of DTL.

Key words: smart home; blockchain; dynamic trusted lightweight authentication; zero-knowledge proof

物联网(Internet of Things, IOT)在日常生活中连接数量众多的智能设备, 例如各类传感终端以及摄像头、空调、电灯等智能家电[1]. 近年来, 5G 的兴起推动了 IOT 领域智能家居行业的发展. 用户可通过手机等方式灵活方便地控制智能家居设备. 智能家居系统存储和处理的信息大多涉及用户隐私和设备运行数据, 身份认证作为智能家居系统安全防护的第一道关卡, 成为研究热点.

在智能家居领域, 身份认证的瓶颈主要体现在性能和安全两个方面: (1) 低计算能力、低能源的传感器设备组成了智能家居系统[2], 这类设备将大量资源用于应用业务[3], 其投入安全防护的资源十分有限, 必须寻求在受限的硬件资源条件下实现智能家居安全认证的方案; (2) 传统的智能家居网络大多采用中心化的体系架构, 由一个高性能中心节点(比如服务器)来存储和处理终端设备信息, 网络中所有节点都需要与中心节点进行通信[4]. 这种架构适用于高资源集群系统, 但是在资源受限的智能家居中应用, 会存在中心节点流量拥塞导致较大网络延迟的性能问题. 另外, 中心化的管理方式普遍面临中心信任的安全问题, 中心节点遭受攻击会引发整个系统信息泄露.

分析智能家居系统存在的性能问题和安全风险, 安全可行的认证机制需要满足以下需求: (1) 分布式认证模式替代中心化认证模式, 以解决中心化信任问题; (2) 不泄露身份信息; (3) 接入系统中的智能家居设备安全可信; (4) 少量终端设备被攻击不影响整个系统安全运转; (5) 时延低, 不影响用户体验; (6) 认证机制是轻量级的, 适用于资源受限的智能家居环境.

区块链是一个去中心认证的、由保存有同样信息的大量网络节点组成的分布式系统[5], 可解决中心化管理方式带来的性能问题和安全问题, 提高系统可靠性和健壮性[6], 为智能家居设备和用户的身份认证提供了一个可行的解决方案.

本文考虑的是包含多个住宅分布式部署的智能家居系统环境[7]. 区块链的分布式架构可以满足智能家居系统分布式认证需求, 避免中心化系统架构带来的性能和安全问题; 区块链应用的密码学技术支持用户匿名通信, 不会暴露用户隐私; 加密机制保护通信数据的安全和不可篡改; 基于共识的信任机制可保证网络节点认证的一致性, 且具有一定的容错性能, 少量虚假节点不会影响整个网络的决策. 区块链的技术特性天然符合智能家居环境安全认证需求.

虽然传统区块链的安全特性可满足智能家居系统安全认证的部分需求, 但共识机制及密码算法的运行仍需消耗大量存储资源、计算资源和网络资源, 超出了智能家居设备的能力. 同时, 区块链的安全机制会引起较大网络时延, 用户体验差, 不能满足智能家居系统的实时性要求. 经典的区块链安全机制仍无法完美契合智能家居系统的安全认证需求.

针对以上难题, 本文提出了基于区块链的动态可信轻量级安全认证 DTL 机制, 尽可能地在系统安全和设备性能开销之间取得平衡, 以适应智能家居身份认证的需求, 并通过定性分析和仿真验证的方式证明 DTL 的安全性和实用性.

本文的主要贡献是:

(1) 基于联盟链的系统架构. 将联盟链引入智能家居系统, 保证仅授权的智能家居传感器节点可加入网络, 满足分布式认证效率和安全需求.

(2) 轻量级共识算法. 优化共识机制, 提出了 DTSG-PBFT 高效共识算法, 将无中心的传感网组织成安全可信组 DTSG, 利用可信组 DTSG 的认证结果和定向信任传播机制, 将用户与可信组成员间的认证结果在 DTSG 内进行信任传递, 实现 DTSG 成员共享认证结果, 使可信组内的成员均识别该合法

用户, 减少用户在 DTSG 间的频繁认证开销, 提高访问效率和用户体验.

(3) 基于零知识证明的认证. 采用一种 DTSG 机制和零知识证明[8]结合的身份认证方案, 在不泄露用户隐私条件下进行认证.

1 相关工作

智能家居身份认证机制在区块链技术兴起之前便有许多研究成果. 因此, 本节相关工作描述主要从传统的智能家居安全认证机制以及基于区块链技术的智能家居身份认证两方面展开.

1.1 传统的智能家居身份认证机制

智能家居是物联网(IoT)的新兴应用, 智能家居的身份认证问题一直是学术界关注的热点. 在区块链技术兴起之前, 在该方向很多研究已经涌现. Gross 等人提出了基于 IPsec 的认证方案[9], 但超出了大多数智能家居设备计算能力. Skarmeta 等人设计了一种用户访问控制分布式架构[10], 但该方法未充分考虑计算开销和网络延迟因素, 不满足智能家居实时性需求, 并有可能泄露用户隐私. Fakroon 等人提出一种有效的匿名身份验证方案以保证智能家居环境中用户和设备安全的通信, 但是该方案仅考虑用户的身份认证, 未考虑智能家居设备安全接入的认证[11]. 姜怡等人设计了结合中国余数定理和椭圆曲线 Diffie-Hellman(ECDH)的密钥协议[12], 提高了系统安全性; 同时, 通过单向哈希认证而不是双向认证来实现算法的轻量级. 该方法不适用于安全性要求较高的应用场合. Sahraoui 等人设计了一种点到点的认证机制[13], 该方法通过修改网络协议报头来减少网络开销, 不适合通用的应用场合. Soumya 等人提出一种基于 Internet 安全协议和应用程序的自动验证的智能家居匿名认证方案[14], 但其通信开销较大, 不满足智能家居低耗能要求.

综上, 传统的智能家居身份认证方案具有较强的应用局限, 主要表现在以下 3 个方面.

(1) 认证算法复杂度高, 对计算资源和存储资源要求较高, 不适用于资源受限的智能家居设备.

(2) 大多采用中心化的网络设计, 面临管理节点流量过大引起拥塞延迟的性能问题, 以及单点攻击整个网络受影响的安全问题.

(3) 一些安全认证算法是通过修改通用协议以实现认证的轻量级, 适于特定应用, 不具备普适性.

1.2 基于区块链的智能家居身份认证

近几年, 随着区块链技术的发展, 不少专家学者进行了将区块链应用于智能家居身份认证的探索. Rahim 等人搭建了基于私有链的智能家居系统, 并采用物理不可克隆技术提高身份认证的安全强度. 但是该方案仍面临私有链管理服务器的中心化信任问题[15]. Singh 等人提出一种基于云计算和区块链技术的安全高效的物联网智能家居体系结构[16], 身份认证通过策略控制和共享密钥来实现. 该方案实现的前提是所有设备连接上云, 对计算能力有限的智能家居设备而言是一个挑战. Dang 等人应用区块链的智能合约技术保护智能家居的数据[17], 该方案需要较高的计算资源, 对资源十分有限的智能家居设备应用场景未提出解决思路. 梅晨等人结合区块链设计了一种分布式的物联网平台[18], 并在该平台上运用区块链的智能合约实现对设备的接入认证功能; 同时, 采用区块链账本对认证结果进行备份, 保证其不被篡改. 该方案实现了智能家居安全认证, 但未针对轻量级计算需求提出解决思路. 王泽远等人针对智能家居信息安全设计了区块链分层方案[19], 降低了能源消耗和时延, 但设计方案中未考虑本地设备中心管理器受攻击的情况.

综上, 尽管区块链技术去中心化、不可篡改等诸多特性[20]在智能家居身份认证方面有良好的应用场景, 但两者成熟融合应用还有待进一步探索. 目前存在的主要问题如下.

(1) 传统的区块链分布式共识需要消耗大量的计算资源, 且具有较高时延.

(2) 区块链采用的一些计算密集型认证算法, 超过了大多数智能家居设备的处理能力.

(3) 采用私有链进行智能家居设备安全认证的方案, 仍存在中心服务器受攻击带来的安全威胁.

因此, 在充分利用区块链诸多安全特性保证的同时, 要充分结合智能家居设备资源和能力受限的因素, 这也是本文的研究重点.

2 背景知识

2.1 区块链与共识机制

区块链实质上是记账各方共同维护的分布式账本[21], 通过数学算法选取记账节点, 其他成员跟随该节点实现一致的账本[22]. 节点选取所依赖的机制就是共识机制. 每次记账的节点都会根据网络环境和共识算法结果的不同而变化, 进而保证系统不会因某一节点的故障和信任问题而崩溃[23].

不同共识算法适应不同的应用环境. 例如, PoW 算法能源消耗大, 易遭受算力攻击, 共识达成周期较长等不适用于时延要求高的通信系统[24].

智能家居系统对网络和设备的响应效率有较高的要求, 基于区块链的认证机制需要重点解决高效响应问题. 另外, 传统 PBFT 算法假设的前提是参与共识的节点相对固定, 而 DTSG 是跟随用户端移动和访问需求的改变动态变化的. 为了提升算法效率和 DTSG 的适应性, 本文充分考虑 DTSG 动态变化的特性, 基于 PBFT 共识机制优化算法设计.

2.2 零知识身份认证

本文采用的认证方案基于 Feige-Fiat-Shamir 零知识身份证明和 DH 密钥交换算法[25], 保证用户和设备可以通过区块链账本中的公开参数信息来验证其合法身份, 不会泄露隐私数据. 认证方案的安全基于以下两个方面.

- 一是 Feige-Fiat-Shamir 零知识身份证明协议. 证明者 P 有 k 组公私密钥对$(v_1,v_1,\ldots,v_k)$与$(s_1,s_1,\ldots,s_k)$, P 欺骗验证者 V 一次的概率为 $1/2^k$, 欺骗 t 次的概率为 $1/2^{kt}$.
- 二是离散对数问题(DLP). $b=a^i \bmod q$ $(0\leqslant i\leqslant q-1)$. 基于 b 计算 i 具有指数级计算复杂度.

3 以用户为中心的 DTSG 架构

本文方案基于多个智能家居系统共同构建区块链的场景. 智能家居系统中, 未授权的终端设备和用户不可加入区块链, 因此公有链的架构不适用于智能家居环境. 本文使用联盟链构建面向智能家居应用的区块链系统, 不同住宅的智能家居传感网系统互通构成联盟链.

3.1 设计目标

一个实用的认证方案必须综合考虑可用性、安全性和效率, 因此本节从方案具备的安全属性、认证性能两个方面提出设计目标. 对于分布式智能家居系统, DTL 应该实现如下设计目标来保证安全和性能.

(1) 安全性

参考 Wang 等人[26]所提出的认证机制安全要求, 结合本文基于区块链的安全认证模型 DTL 自身的应用特点, 提出以下 9 类安全属性以评估方案的安全性.

S1. 密码存储安全: 密码不会被超级管理员获取.

S2. 抗攻击性: 可抵抗认证机制面临的 6 种典型攻击类型, 包括重放攻击、假冒攻击、传感器节点捕获攻击、中间人攻击、女巫攻击、设备注入攻击.

S3. 错误及时告警: 如果用户输入密码等认证信息错误, 可快速向用户反应告警.

S4. 双向认证: 服务器和客户端之间进行双向认证.

S5. 匿名性: 用户身份隐私数据不被泄漏.

S6. 前向安全性: 认证机制具有前向保密性.

S7. 正确性: 保证信息不被篡改, 一致完整.

S8. 保密性: 保证信息不可非法解密.

S9. 不可抵赖: 当一个非法用户被举报, 其不良行为不可抵赖.

(2) 性能

智能家居环境下对用户请求响应的实时性要求较高, 同时, 应考虑多用户访问下的认证效率不会明显降低, 因此提出以下性能要求.

- 可扩展性: 系统性能不受网络节点数目增大而降低.
- 轻量级: 计算和通信开销低, 能够适应计算能力和网络资源受限的智能家居设备.

3.2 以用户为中心的DTSG架构

本文所设计的 DTL 方案基于分布式的智能家居环境, 如图 1 所示. 区块链网络由系统中的所有实体设备组成. 设备类型包括 3 类: (1) 汇聚节点(sink node, SN), 智能家居设备的管理控制节点, 通常是服务器、计算机或网关等设备; (2) 传感终端(sensor terminal, ST), 智能家居传感设备, 可通过 WiFi, ZigBee 或有线网络与汇聚节点连接; (3) 用户设备(user device, U), 用户的手机、平板电脑等访问控制智能家居的设备. 各设备间可以相互通信. SN 和 ST 是区块链共识的主体. 用户设备作为客体向区块链提出访问请求. 当一个新的用户请求访问控制 ST 时, 需要向区块链进行注册, 区块中存储的注册信息同步更新.

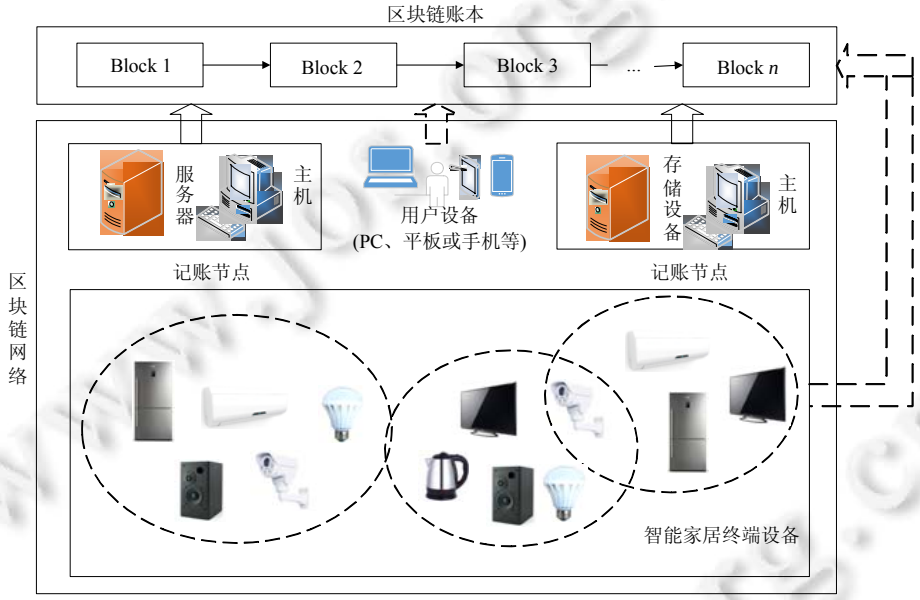


图 1 智能家居网络架构

智能家居网络中包含大量节点, 为了确保用户访问认证的高效以及网络的可扩展, 本文设定联盟链分组管理, 即按 DTSG 管理, 如图 2 所示. 在分布式网络中, 用户访问智能家居终端时需要频繁与不同的终端设备进行认证, 认证开销大, 影响用户体验. 因此, 建立可信的智能家居传感设备组 DTSG, 为用户提供认证访问服务. 用户只需与 DTSG 内终端进行一次认证, 可在组内所有终端设备间认证通行. 由于网络中的终端设备可能存在假冒或恶意节点, 对认证效率要求较高, 因此, 本文通过对高效且支持拜占庭容错的 PBFT 共识机制进行改进, 提出了 DTSG-PBFT 算法, 选取可信的终端设备组成一个可信设备组 DTSG. 可信设备组内所有终端节点信息以区块方式存储到区块链中. 当用户访问需求发生变化时, 参与共识的节点随之变化, DTSG 成员同步更新.

DTSG 架构的安全性体现在智能家居终端设备安全和用户认证数据安全两个方面.

- 终端设备安全方面, 只要保证划分到DTSG的设备成员是安全的, 就可以在设备访问层面保证用户访问的安全性, 而无需要求网络中所有设备终端都必须是合法可信的, 从而缩小了设备终端安全保证的范围和难度[27]. 由于 DTSG 的组成是动态的和无中心化的, 因此用户要进行安全可信的访问, 在用

户周围形成一个安全可信的 DTSG 是必不可少的前提.

- 用户隐私保护方面, 采用零知识证明协议保证了用户认证过程中隐私数据的安全.

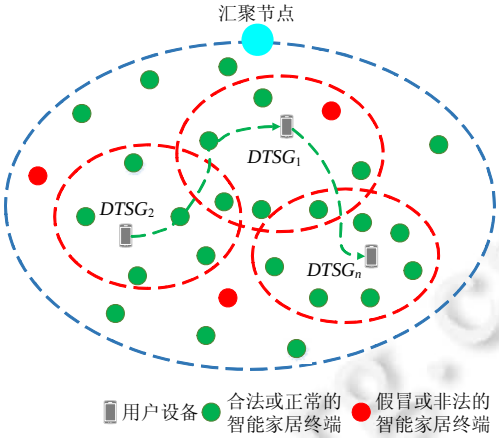


图 2 以用户为中心的 DTSG 架构

在性能方面: (1) 该方案采用了基于 DTSG 的分组认证机制, 网络中的基本任务都由 SN 执行, 更能适应大规模的区块链网络环境, 比传统区块链具有更好的扩展性; (2) 基于 DTSG 可信组的认证机制, 大大减少了用户认证次数和计算开销.

3.3 区块数据结构设计

区块数据结构设计是整个认证架构的基础. 区块链账本中存储 SN, ST 和 U 用于身份认证和密钥协商的公开信息, 包括交易类型、设备节点的身份 ID、DTSG 可信组 ID、零知识证明和 DH 密钥交换算法的相关公开信息、时间戳等. 区块数据结构如图 3 所示.

- Type: 智能家居设备交易类型.
- Identity: 设备 ID, 设备注册时分配.
- DTSG id: 设备所属的可信设备组 ID, 若设备不属于任何可新设备组, 则该值为空.
- ZKP info: 零知识证明需要的公开参数信息.
- DH info: DH 密钥交换算法需要的公开参数信息.
- Timestamp: 提交交易的时间.

Type	Identity	DTSG id	ZKP info	DH info	Timestamp

图 3 区块数据结构

4 DTL 机制描述

DTL 机制在 DTSG 建立的基础上运行. 为实现 DTSG 的容错和快速生成, 本文提出了一种基于 PBFT 共识机制改进的 DTSG 生成算法 DTSG-PBFT, 并在该 DTSG-PBFT 算法的基础上提出了基于零知识证明的身份认证方案. 因此, 本节首先介绍 DTL 机制运行原理, 然后分别对改进的共识算法以及认证算法进行详细描述.

4.1 DTL运行原理

本节通过 6 个部分逐步描述 DTL, 分别是节点注册、DTSG 初始化申请、基于共识的可信 ST 选取、DTSG 生成、U 与 DTSG 成员的双向认证、U 认证结果的 DTSG 定向传递, 如图 4 所示. 这里, U 代表用户, SN 代表汇聚节点.

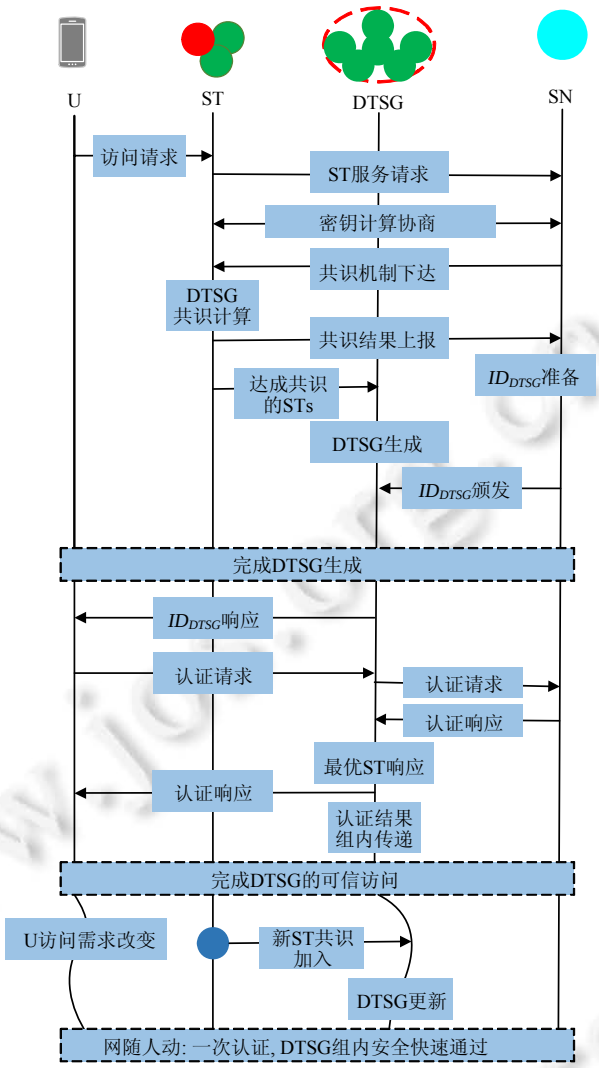


图 4 DTL 运行原理

步骤 1: 节点注册. 所有 U 和 ST 节点在加入网络时, 必须首先进行注册, 获取 ID. 注册信息写入区块链, 用于用户身份认证. 本文采用零知识证明协议验证身份, 利用 DH 算法交换密钥. 注册流程在第 4.3 节进行了详细描述.

步骤 2: DTSG 初始化申请. U 发起初始接入请求, 请求范围内(设定数量为 n)的所有 $ST[n]$接收并转发 U 的请求信息, 并向 SN 申请服务. SN 接到请求后, 准备 DTSG 的唯一标识信息 ID_{DTSG} 和密钥, 同时向 $ST[n]$发送进行共识的消息. 本文方案采用基于 PBFT 的进行优化的算法共识机制运行.

步骤 3: 基于共识的 ST 选取. 网络中的终端设备节点可能存在虚假或非法节点, 那么如何通过共识算法选出可信安全的 ST 进行记账是核心问题. 经典的 PBFT 共识运算获得的结果, 决定了所有网络节点达成一致性的账本, 但无法保证记录账本的节点的安全性和可靠性. 本文在 PBFT 基础上提出的 DTSG-PBFT 算法, 对终端节点增加了标记为 $ST[n]$, 区分节点接收和发出的共识计算结果. 当共识计算完成, 通过二分法查找发出的共识结果与最终形成的一致性共识结果一样的节点 $ST[i]$, 即为本轮共识运算中提供正确共识消息的可信终端节点.

为提高选取的 ST 认证的可靠性, 本文引入了基于信誉度的节点激励机制. 在信誉度评价中, 复杂且难以

衡量的节点信誉度问题被分解为对多个可收集、可测量和可计算指标的评估. 我们采用层次分析法 AHP 算法[28]对节点信誉度进行量化评估, 选取节点安全性和可用性作为第 1 级指标描述属性. 安全性描述了诚实合作和节点不欺诈的特征, 包括异常数据比率、误码率和身份欺诈比率. 可用性是根据节点自身的通信功能、存储功能和处理能力(包括传输成功率、可用存储容量比率和处理器利用率)来描述的. 这 6 个属性作为第 2 级指标属性. 这些指标的定量评估数据是通过硬件和软件测试获得的, 并标准化并转换为[0,1]范围内的值. 依据这些指标进行 AHP 运算, 最终确定各个 ST 节点的信誉度评分 s_r. 优先在信誉度处于较高评分阈值范围的节点集合内进行共识运算, 选取可信 ST.

当用户访问节点的需求发生了变化, 或者有新的节点加入和旧的节点退出时, 需要重新进行共识运算, 重新选举 $ST[i]$. 本文第 4.2 节对 DTSG-PBFT 共识算法进行了详细描述.

步骤 4: DTSG 构建. 通过 DTSG-PBFT 选取出所有发出正确共识消息的节点 $ST[i]$集合, 构成 DTSG 可信设备组. 节点 $ST[i]$集合作为区块 $ST[j](j=[1,...,m],m\leqslant n)$构成基于 DTSG 的区块链结构体. SN 将步骤 1 准备的 ID_{DTSG} 分配给新生成的 DTSG, 组成 DTSG 中的所有成员 ST 都是可信的, 组成可信传感设备组为用户提供服务, 共享 DTSG 的标识 ID_{DTSG}. 其他未被选取的 ST 节点被认为不可靠节点被丢弃. 需要说明的是, DTSG 可信组是逻辑上的, 是没有顺序和方向的, 即无中心的.

步骤 5: U 与 DTSG 成员的双向认证. DTSG 生成后, 其中选取一个成员 $ST[j]$对用户 U 进行 Feige-Fiat-Shamir 零知识身份认证. 若认证通过, 则该节点 $ST[j]$将获得相应的认证结果. 本文第 4.3 节对认证算法进行了详细描述.

考虑到用户 U 的移动性和访问请求的变化, 共识重新运算, DTSG 成员不断更新, 可能有的 ST 多次被选中. 为提升用户体验, 可以对与 U 进行双向认证的 DTSG 中成员 $ST[j]$的选取进行优化. 本文对 DTSG 中的成员增加选取次数记录, 由于它已在 DTSG 中, 只标记该节点 $ST[j]$被选中的次数, 不做其他处理. 被选中次数最多的接入节点作为优选节点.

步骤 6: U 认证结果的 DTSG 定向传递. U 认证结果通过区块链传播机制在具有相同 DTSG 标识 ID_{DTSG} 的节点 STs 之间传播, 即 DTSG 定向传播. 所有收到定向广播的接入节点 $ST[j](j=[1,...,m],m\leqslant n)$将保存 U 的认证结果. 当 U 移动到该节点 $ST[j]$的覆盖范围内时, U 直接出示认证并与接入节点 $ST[j]$中保存的认证结果进行快速校验(无须重复完整的双向认证过程). 校验通过, 则提供数据访问服务, 用户将无感知地接入到下一个 ST 节点中, 即永远处于一个 DTSG 的无缝覆盖服务范围内.

随着 U 访问请求的变化, 重复第 2 步、第 3 步和 DTSG 更新, 使用户获得最好的体验和高效认证的支撑.

4.2 DTSG-PBFT共识算法

在智能家居环境中, SN 是所有传感设备 STs 的管理节点, 且在实际应用中大多为经过认证的设备, 可信度较高. 本文根据实际应用条件, 选取信誉度评分较高的 ST 集合, 在该集合内为每个 ST 进行编号, 并指定 SN 为主节点且编号为 0, 其他节点 STs 从 1 开始. 其中, f 为可容忍的拜占庭节点数即不可信节点数. 设定当前网络中有 n 个节点参与运算, 共识计算推选出共识节点 $ST[i]$并构建 DTSG. 随着用户访问需求的变化, 当节点数量发生变动时, 重新计算共识和构建 DTSG.

SN 收到 U 的请求, 开始下达指令后, 各节点开始计算共识. 共识开始时, SN 作为身份验证的主节点, 在 pre-prepare 阶段广播消息$\langle b,n,i,d,s\rangle$,其中 b 是新区块,n 是出块序号,i 是节点序号,d 是区块 b 的摘要,s 是摘要的签名.当其余作为副节点的 ST 收到广播消息验证合法后,进入 prepare 阶段,副节点向全网广播消息$\langle b,n,i,d,s\rangle$.当每个节点累计收到 $2f+1$ 条不同节点的相同 prepare 阶段广播的消息后,进入 commit 阶段,对身份信息进行认证,广播 commit 消息$\langle b,n,i,d,s\rangle$. 每个节点收到超过 $2f+1$ 条不同节点在 commit 阶段广播的信息后, 对该区块达成共识, 并回应用户. 由于在 prepare 阶段和 commit 阶段只要收到 $2f+1$ 条相同的广播信息即可完成共识, 网络中可能存在假冒或恶意节点, 这些节点广播的信息与共识结果并不相同, 因此在一轮共识完成后, SN 根据开始设定的 ST 编号选择与共识结果计算一致的 ST 节点作为可信节点, 所有的可信节点组成可信设备组 DTSG 为用户提供服务.

DTSG-PBFT 关键算法流程如下.

DTSG-PBFT Algorithm.

SN.*Accept*(*block*,ST_0);

ST.*filter*($s_h \leqslant s_\tau \leqslant 1$); //选取信誉度较高的节点集合进行共识

ST_0.*Broadcast*⟨*b*,*n*,*i*,*d*,*s*⟩;

While (2×*f*+1)<*n*

  For *i*=1 to *n*

    ST_i.*Receive*(*block*,*j*++);

    ST_i.*Prepare*⟨*b*,*n*,*i*,*d*,*s*⟩;

    ST_i.*Commit*⟨*b*,*n*,*i*,*d*,*s*⟩;

    If *j*>(2×*f*) **Then**

      ST_i.*addMark*⟨*input*,*output*,*k*⟩;

      ST_i.*Broadcast*⟨*b*,*n*,*i*,*d*,*s*⟩;

    End if

  End for

  ST_0.*Receive*(ST_i.*block*,*i*);

End while

ST_0.*Reply*(*block*,*U*);

ST_0.*Lookup*(ST_i,*i*++,*k*);

DTSG=*fun*(ID_{DTSG},ST_1,ST_2,…,ST_k);

If *p*(ST_k,ST_0)=true **Then**

  addChain(ID_{DTSG},*block*,ST_k);

Else

  Skip;

End if

在 DTSG-PBFT 算法实现中, 选取计算能力和可信度都较高的设备作为 SN 管理节点, 缩减了 PBFT 中管理节点计算筛选的步骤; *Commit* 阶段对终端节点设置唯一标识, *Reply* 阶段结合节点编号, 通过二分法查找选择出共识计算一致的可信节点, 高效构建 DTSG.

4.3 基于零知识证明协议和DH算法的认证方案

本文采用基于零知识证明协议和 DH 算法的认证方案. Feige-Fiat-Shamir 方案使用公钥密码机制, 它的优点是只需要很少的模块化操作, 因此它与其他公钥算法(比如 RSA)相比更快, 可以在智能传感终端中嵌入的弱微处理器上实现, 这很符合智能家居设备计算能力有限的场景, 因此本文选择 FFS 零知识证明的协议为用户身份隐私信息不被泄露提供一定保证; 在密钥协商机制选择上, 采用 DH 密钥交换算法, 算法涉及模幂运算, 计算复杂度较高, 但认证一次产生的时间消耗不会对用户体验产生太大影响, 对密钥的可靠传输也可提供更可靠的保证. 所有 U 和 ST 在加入区块链前需进行注册, 获取零知识证明协议和 DH 算法所需的公开参数信息. 注册流程如下.

(1) 设置一个系统安全参数 X_i.

(2) 计算 DH 算法交互参数 $Y_i = a^{X_i} \bmod q$, 其中, a, q 为系统预置参数.

(3) 生成一系列本地参数, 包括随机数 r、随机符号数 s(s 赋值为−1 或 1)、$s_1,s_2,\ldots,s_k$.

(4) 设置大整数 m, 计算 $v_i = s_i^2 \bmod m$, 用于组成零知识证明的公开参数信息.

(5) 组装注册信息 $reg=\{id,(v_1,v_2,\ldots,v_k),Y_i\}$向区块链网络广播, id 为节点标识信息.

用户 U 和终端节点 $ST[j]$的双向认证过程如下.

(1) 用户 U 向 DTSG 发送请求信息, 查询获取 $ST[j]$注册的公开参数信息, 即绑定节点 $ST[j]$的 id_j 生成的零知识证明公开参数 $s_1,s_2,\ldots,s_k$ 和 DH 算法参数 Y_j, 向 $ST[j]$发送用户标识 id_u、时间戳 t_1 和随机序列值 N_1.

(2) 节点 $ST[j]$收到用户 U 发来的消息后, 随机生成二进制数串 $a_1,a_2,\ldots,a_k$, a_k 为 0 或 1, 向用户 U 发送该数串、节点自身 id_j、时间戳 t_2 和序号 $N_2(N_2=N_1+1)$.

(3) 节点 $ST[j]$请求获取用户 U 的注册信息.

(4) 用户 U 获取到节点 $ST[j]$发送的二进制数串 $a_1,a_2,\ldots,a_k$ 后, 依据其注册信息随机数 r 和 $s_1,s_2,\ldots,s_k$ 计算零知识证明参数信息, 并将该信息同当前时间戳 t_3、序列值 $N_3(N_3=N_2+1)$发送给节点 $ST[j]$.

(5) 用户 U 依据 DH 算法计算公共密钥 $K=(Y_j)^{X_U} \bmod q$, 然后用 K 加密信息并发送给 $ST[j]$.

(6) 节点 $ST[j]$收到 U 发送的信息后, 根据零知识证明协议对 U 身份进行验证, 若验证通过, 则说明用户 U 身份正确. 节点 $ST[j]$根据区块链获取的用户 U 的注册信息计算公钥 $K=(Y_U)^{X_j} \bmod q$, 解密 U 的消息, 并用 K 加密信息发送给用户 U. 认证结束, K 即为数据交换时的会话密钥.

5 安全性分析

为验证方案是否实现了第 3.1 节设定的安全目标,本节分析 DTL 方案的安全性,包括认证机制的抗攻击性和 DTSG-PBFT 的安全性两方面.

5.1 抗攻击性分析

(1) 攻击模型

参考传感网络身份认证的抗攻击安全需求[29], 提出了基于区块链系统的认证机制面临的 6 种典型攻击类型, 建立了基于区块链的认证方案的攻击模型, 如图 5 所示.

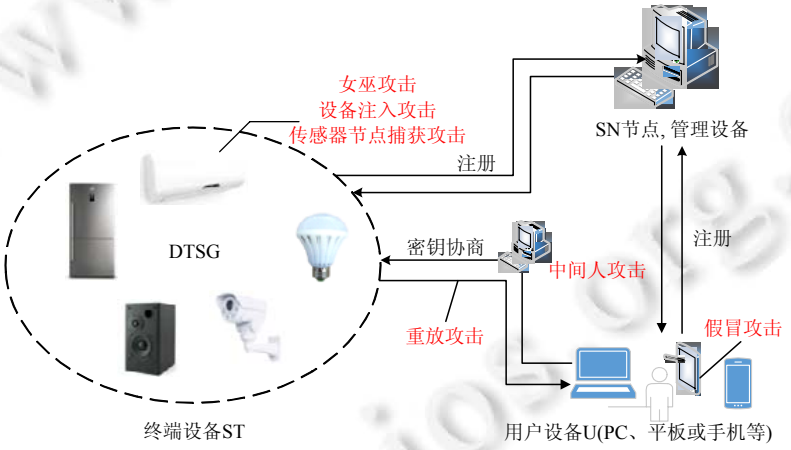


图 5 攻击模型

- 重放攻击: 攻击者窃听网络中的认证数据, 然后重复多次发给验证者, 以获取非法服务或利益.
- 假冒攻击: 攻击者截获网络中传播的合法用户身份信息, 利用身份信息假冒用户实施欺骗行为.
- 传感器节点捕获攻击: 攻击者有足够的计算能力和手段窃听并获取到网络中部分合法传感节点的私密信息, 进而攻陷网络中更多的通信链路.
- 中间人攻击: 攻击者通过技术手段拦截两个设备间的通信数据, 在双方无感知情况下, 进行数据篡改等操作.
- 女巫攻击: 网络中少量攻击节点模仿多种身份, 以达到控制网络中大部分节点的攻击. 针对区块链这

种通过多个节点保存的冗余数据保证网络数据安全和不可篡改的特性, 女巫攻击通过控制大多数节点, 削弱冗余备份的安全作用.

- 设备注入攻击: 攻击者将虚假或恶意设备接入智能家居系统中, 以窃取用户注册的隐私信息.

(2) 抗攻击能力分析

具体分析本方案如何防御上述 6 种攻击, 如表 1 所示. 通过分析可知, DTL 机制可以有效抵抗基于区块链身份认证方案的常用攻击, 满足设计目标.

- 抵抗重放攻击: DTL 机制中, 用户 U 和智能家居设备 ST 的每一次认证交互信息都包含时间戳 t、序列值 N、随机数 r、随机符号数 s, 每一次会话, 上述信息都会变化, 攻击者重新发放数据包的恶意行为很容易被发现, 重放攻击几乎不可能发生.
- 抵抗假冒攻击: 本文通过 DH 算法计算得到会话密钥 $K=(Y_j)^{X_U} \bmod q$, 模幂运算复杂度高, 攻击者难以通过窃听的公钥信息来计算出节点的私钥, 从而难以假冒用户 U. 基于零知识证明的认证协议保证虚假节点无法验证通过.
- 抵抗传感器节点捕获攻击: 假设攻击者已获取某些设备节点 ST 的私密信息, 但是每个 ST 节点和用户节点的会话密钥都包含随机数 r、随机符号数 s 等信息, 用户 U 与每个传感节点 ST 的会话密钥都不同, 且每次认证会话密钥都会更新. 攻击者很难通过捕获的少量传感节点私密信息攻陷整个网络.
- 抵抗中间人攻击: 本文采用 FFS 零知识证明协议, 即使中间人获得了用户 U 与传感设备 ST 的通信信息, 也不会从截获信息中获得用户私密信息.
- 抵抗女巫攻击: 设备节点 ST 在注册时要验证其合法 ID, 验证不通过的节点注册信息无法生效, 节点不可能伪造多重身份信息加入区块链中.
- 抵抗设备注入攻击: 注入的恶意设备 ST 在共识机制中无法提供正确的共识结果, 不会被纳入 DTSG 可信组, 会被抛弃不参加认证, 进而不会获取用户隐私信息.

表 1 列出了本文所提出的 DTL 方案与其他认证方案, 包括基于区块链技术的认证机制(文献[15,20,30])和传统非区块链的认证机制(文献[11,31]), 在抵抗上述典型网络攻击能力上的对比. 与其他认证方案相比, DTL 可以更有效、全面地抵抗上述 6 种典型攻击.

表 1 抗攻击能力对比

攻击类型	DTL 机制	文献[15]	文献[20]	文献[30]	文献[11]	文献[31]
重放攻击	√	√	√	√	√	√
假冒攻击	√	√	√	√	√	√
传感节点捕获攻击	√	√	×	√	√	√
中间人攻击	√	√	√	√	√	√
女巫攻击	√	√	×	√	√	√
设备注入攻击	√	×	√	√	/	/

5.2 DTSG-PBFT安全性分析

DTSG-PBFT 算法在保持 PBFT 容错性条件下, 确定非拜占庭节点共识计算的一致性, 并且通过二分法查找发出的共识结果与最终形成的共识结果一致的节点形成 DTSG 可信组. 因此, DTSG-PBFT 的安全性体现在:

(1) 共识不会分叉. 在 PBFT 机制中, 若超过全网 2/3 的节点计算得到一致性结果, 则形成对一组计算数据的共识. 在一轮共识中不会出现两个不同的共识结果.

(2) 基于节点信誉度的共识组成的 DTSG 的设备 ST 为可靠节点, 可为用户提供服务.

5.2.1 共识不会分叉.

设定网络节点总数 $N=3f+1$, 则网络中最多有 f 个拜占庭节点. 假设节点 ST1 和 ST2 接收到了两个不同的共识结果, 则超过全网 2/3 的节点即至少 $2f+1$ 个节点计算达成了共识结果 1, 至少 $2f+1$ 各节点计算达成了共识结果 2. 因此,至少 $2f+1+2f+1-3f-1=f+1$ 有个节点发出了两个共识结果. 这样的节点为拜占庭节点, 与设定条件网络中最多有 f 个拜占庭节点矛盾. 因此假设不成立, 不会出现超过全网 2/3 的节点计算得出两个不同共识

结果的情况.

5.2.2 共识选取的 ST 节点的可靠性.

DTSG-PBFT 对参与共识的节点进行编号. 用户提出访问请求后启动共识计算. 在形成共识后, 根据编号查找发出共识结果与最终形成的共识结果一致的节点, 这些节点为非拜占庭节点, 可为用户提供本次访问请求的可靠服务. 随着用户访问需求的变化, 会重新启动共识计算和可信节点 ST 的选举, 以保证每次交易中服务于用户的 ST 的可靠性.

6 性能分析

DTL 的轻量级主要依赖于改进的共识算法和基于 DTSG 的认证机制, 因此, 为了说明 DTL 机制的性能优势, 本节首先单独计算并仿真分析改进的共识算法 DTSG-PBFT 在效率和评分值上的改善; 然后计算认证的时间开销, 并仿真认证流程, 从认证响应时间的角度说明本文提出的认证方案是可行并且是轻量级的.

6.1 DTSG-PBFT共识算法仿真与分析

为了提高效率, 首先分析了区块链技术对智能家居环境的适应性. 智能家居场景不需要永久可信的账本, 但在有多个不可信终端节点加入的条件下能高效地达成共识一致, 及时响应用户需求. 因此, DTSG-PBFT 中通过高效建立 DTSG, 为用户提供快速认证对象群, 并指定特定 SN 作为管理节点, 进一步提高共识效率.

为了量化评估共识算法的性能, 提出如下评价公式:

$$Efficiency=\sum_{ST}\frac{tps}{delay} \tag{1}$$

其中, tps 为每秒交易量, 定义为 $tps=\sum transactions/\Delta t$ 表示; $delay$ 为共识消耗时间; ST 为网络节点.

为模拟 DTSG-PBFT 性能, 基于 python 语言和 flask 架构编写仿真系统. 设定网络中节点数目分别为 35, 40, 45, 50, 对共识算法进行有效性观测.

系统仿真后观测到的相关结果与 PBFT 算法比较如图 6–图 8 所示.

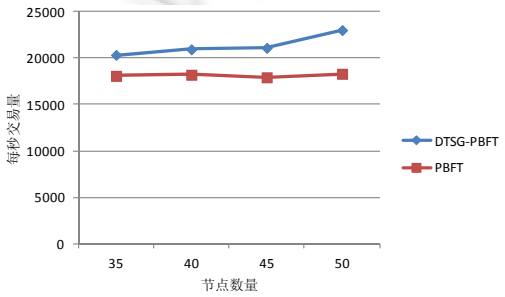


图 6 节点数变化情况下的每秒交易量比较

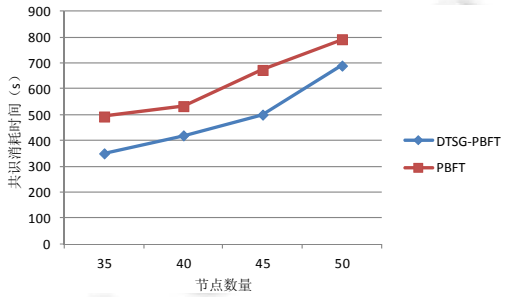


图 7 节点数变化情况下的共识消耗时间比较

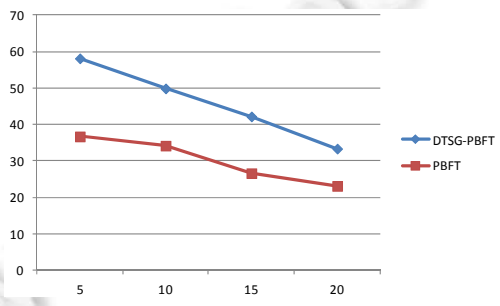


图 8 节点数变化情况下的评分值比较

从以上仿真可知, 在不同节点数量条件下, DTSG-PBFT 比 PBFT 具有更高的交易量和更低的时间延迟, 共识效率更高.

6.2 认证性能评估

6.2.1 认证开销

一个用户 U 需负责发送环境上下文信息给 ST 进行认证. 用户认证通过后, ST 将认证消息在 DTSG 内定向传递. 为了衡量认证阶段产生的时延, 本文采用了两台电脑分别作为 U, SN, 电脑配置为 Intel(R) Core(TM) i7CPU, 8 GB 内存; 选用 z1 mote 传感器作为智能家居终端设备 ST.

本文应用协议 IEEE 802.15.4, 将信息大小设为 24 字节. 在此设置条件下, 模拟用户 U 与已共识选取产生的 ST 进行认证, 记录在认证阶段 FFS 和 DH 算法运算产生的时间消耗. 当 ST 接收到消息后进行认证, 主要操作需要进行大数幂乘运算, 在 JAVA 运行环境下运算对应的时间见表 2. 为了更准确地衡量算法消耗,实验设置认证算法分别执行 100 次、200 次、300 次和 400 次,再计算平均时间消耗.

表 2 与 ST 的认证时间消耗

认证算法执行次数	时间消耗(ms)
100	136
200	282
300	403
400	536

由表 2 数据计算可得出, 平均一次算法运行时间消耗为 1.357 ms. 根据 DTL 工作流程, U 与优选的 ST 认证通过后, 在 ST 所在的 DTSG 内定向传播认证结果, 以保证整个 DTSG 内节点可提供给 U 合法服务. 服务定向传播阶段, 时间消耗主要由于信息传播和数据搜索产生. 信息传播时间为 1.928 ms. 本文采用的数据搜索方法是快速搜索算法, 如哈希搜索算法. DTSG 内节点数目 k 不同, 搜索时间不同.

从 U 与 ST 开始认证, 到 DTSG 内节点成员可提供给 U 合法服务, 所需总时间消耗 $overhead$=3.285+$T(k)$, 见表 3.

表 3 DTSG 认证时间消耗

DTSG 内节点数量	时间消耗(ms)
5	4.082
6	4.301
7	4.496
8	4.691

6.2.2 认证机制对比

为了分析 DTL 机制的优越性, 本节选取了基于区块链技术的认证机制[20]和传统非区块链的认证机制[11]作为比较对象, 从可用性、安全性和效率等方面综合评价.

在安全性评价方面, 依据第 3.1 节提出的 9 项安全属性要求, 分析 DTL 与文献[11,20]提出的认证机制的安全性.

在性能评价方面, 考虑到智能家居系统快速响应的需求, 本文选取认证耗时为评价指标. 从 U 与 ST 开始认证, 到 DTSG 内节点所有成员可提供给 U 合法服务所消耗时间, 包括模幂运算耗时、信息广播耗时、哈希算法耗时. 在上述第 6.2.1 节认证开销所描述的环境中, 各部分计算的时间开销见表 4.

表 4 计算时间开销

操作类型	时间消耗(ms)
模幂运算 $T_{\exp}$	1.357
哈希运算 T_h	0.176
信息广播 T_t	1.928
非对称加密/解密 $T_{e/d}$	0.932

设定 DTSG 内节点数量为 8, DTL 与文献[11,20]提出的认证机制在安全性、性能方面的对比见表 5.

表 5 认证的安全性与效率对比

认证机制	计算耗时	仿真耗时(ms)	S1	S2	S3	S4	S5	S6	S7	S8	S9
DTL 机制	$T_{exp}+T_t+8T_h$	1.928	√	√	√	√	√	√	√	√	√
文献[20]	$8\times2T_{e/d}$	14.91	√	×	×	√	√	√	√	√	√
文献[11]	$8\times10T_h$	14.08	×	×	√	√	√	√	√	√	×

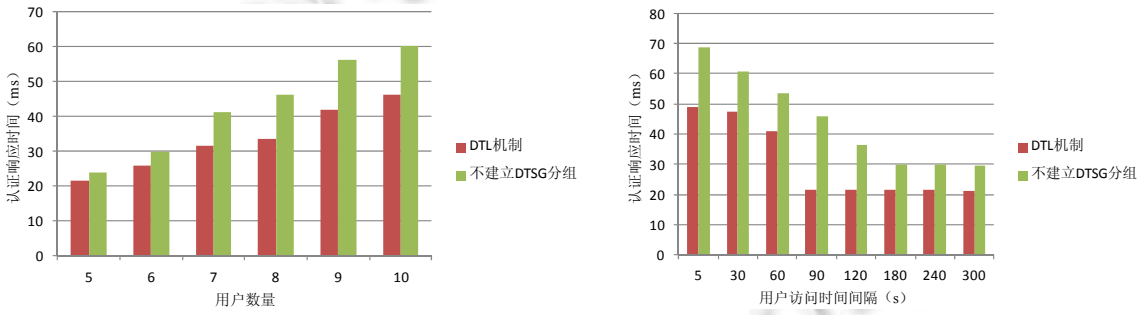
从表 5 可看出, DTL 满足第 3.1 节提出的 9 项安全要求, 而另外两种方案并不能完全抵抗 S2 所列的所有攻击; 此外, 文献[20]提出的认证方案缺少用户密码错误及时检测特性, 文献[11]提出的认证方案在密码存储安全、不可抵赖等方面安全性也比较弱; 在认证效率方面, 虽然 DTL 涉及模幂运算, 比较耗时, 但由于用户 U 与优选节点 ST 认证一次, 认证结果即可在 DTSG 内所有 ST 间传递, 不需再重新认证, 认证效率高于其他认证方案. 通过以上分析可得: DTL 在具备较高安全性的同时, 也具有较高的运行效率, 安全性和性能皆优于文献[11,20]提出的认证机制.

6.2.3 仿 真

为了对比分析达成共识条件下 DTL 认证开销, 本文模拟了不采用 DTSG 分组认证的场景, 其他条件与 DTL 机制相同, 将其作为 DTL 比较的对象.

本文假设每个 DTSG 包含采用 ST 数目相同, 都为 5 个, 共存在 4 个 DTSG.设置如下: (a) 在每一个 DTSG 范围内有 m 个 U, 并且用户请求遵循泊松分布, 用户成批提出访问认证请求, 系数为 λ_i; (b) 用户的转发时间为 1.928 ms 乘以用户的数量; (c) 一批用户的认证时间为 $overhead$=3.285+$T(k)$乘以用户的数量. 基于这些设置, 本文进行如下仿真.

在第 1 组仿真中, 设置参数如下: (a) $m\in$[5,10]; (b) $1/\lambda_i$=1 s. 结果如图 9(a)所示. 第 2 次仿真设置参数如下: (a) m=5; (b) $1/\lambda_i$=[5,300] s. 其他参数同第 1 次设置. 结果如图 9(b)所示.



(a) 随着 U 数量增加, 响应时间的变化 (b) 随着 U 认证请求间隔时间增加, 响应时间的变化

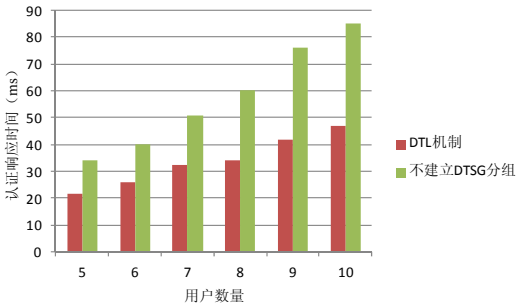
图 9 每个 DTSG 包含 5 个 ST 时, 响应时间的变化

第 2 组仿真和第 3 组仿真, 本文分别设每一个 DTSG 节点数量为 6 和 8, 其他参数同第 1 组设置. 结果分别如图 10、图 11 所示.

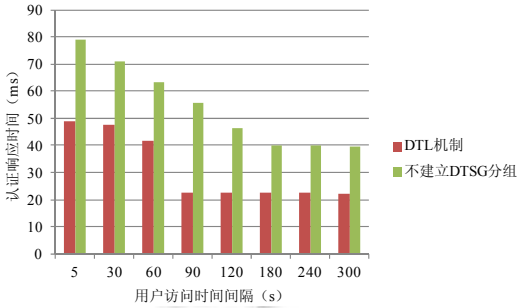
从图 9(a)、图 10(a)、图 11(a), 本文观察到: DTL 机制下, 随着 U 数目的增加, 认证的平均响应时间增加. 原因是 U 数目越多, 等待时间越长. 然而, 随着 DTSG 包含 ST 数目的增加, 认证响应一个请求的平均时间几乎没有变化. 而不采用 DTSG 分组认证的场景, 平均响应时间消耗皆大于 DTL; 并且随着 ST 数目的增多, 平均响应时间也越来越长. 原因是: 基于 DTSG 的认证, 用户仅需要与分组内优选的一个 ST 进行一次认证, 之后在分组内广播认证结果, ST 的变化对认证时间影响不大; 而不采用 DTSG 的认证场景, 随着 ST 数量增多, 用户认证次数增多, 认证时间随之增加.

从图 9(b)、图 10(b)、图 11(b), 本文观察到: DTL 机制下, 随着认证请求时间间隔的增加, 平均认证响应时间开始时下降, 在第 1 分钟时突然下降, 之后保持平衡. 原因是随着请求间隔增加, 等待认证时间越来越

短, 因此平均响应时间逐步减小. 当时间间隔达到 1 分钟时, 由于没有等待时间了, 响应时间急剧下滑. 而不采用 DTSG 分组认证的场景, 平均响应时间消耗皆大于 DTL, 当到 2 分钟以后, 认证时间才保持平衡.

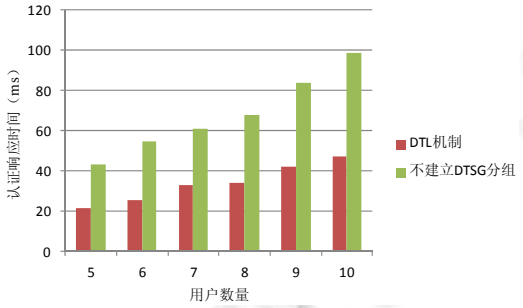


(a) 随着 U 数量增加, 响应时间的变化

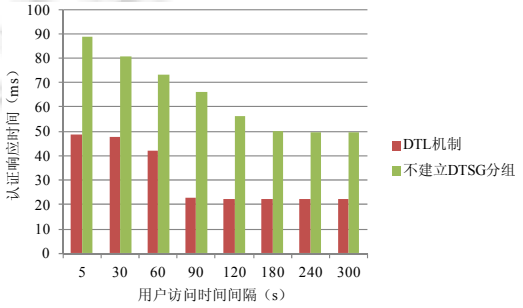


(b) 随着 U 认证请求间隔时间增加, 响应时间的变化

图 10 每个 DTSG 包含 6 个 ST 时, 响应时间的变化



(a) 随着 U 数量增加, 响应时间的变化



(b) 随着 U 认证请求间隔时间增加, 响应时间的变化

图 11 每个 DTSG 包含 8 个 ST 时, 响应时间的变化

仿真结果表明, 提出的 DTL 机制在单用户和多用户访问下的认证响应时间都是毫秒级, 应用上是可行的. 并且与不采用 DTSG 分组认证的场景对比, 时间消耗更低, 因此 DTL 机制是轻量级的, 适合于资源能力受限且对实时性要求较高的智能家居应用.

7 结束语

随着 5G 和物联网技术的发展, 智能家居系统中部署的终端传感设备和用户访问数量更加密集, 智能家居终端传感设备之间相互独立且平等, 所有终端设备相互对等构成一个无中心的网络. 如何保证用户安全高效地访问可信的智能家居网络, 这对未来 5G 网络下物联网系统架构和安全机制提出了新的挑战. 现有的认证与密钥协商算法不能满足用户快速而安全访问一个无中心的动态变化的智能家居系统的需求. 本文针对智能家居设备资源受限问题, 提出了基于区块链的轻量级认证方案 DTL, 并验证其改善的能力. DTL 机制通过 DTSG-PBFT 共识算法及反向筛选机制, 在智能家居环境中实现动态生成可信任的 DTSG, 并将用户认证结果在 DTSG 组成员中进行信任传递和共享, 使得可信链上的成员均能够认证该用户, 减少了用户在 DTSG 成员间的频繁认证, 实现了用户平滑接入与安全访问, 提高了用户体验. 通过对共识算法的仿真分析表明, DTSG-PBFT 算法提升了共识算法的效率, 这对保障未来 5G 环境下物联网系统的可靠安全性具有重要的参考价值.

References:

[1] Ukil A, Bandyopadhyay S, Pal A. IoT-privacy: To be private or not to be private. In: Proc. of the 2014 IEEE Conf. on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2014. 123−124.

[2] Sun RL, Gong JB, Wang R, Zhang L, Cui L. Vehicle identification approach based on DSMT in WSN. Journal of Computer Research and Development, 2010, 47(S2): 246−250 (in Chinese with English abstract).

[3] Zhong X. The era of smart media: Privacy, security and ethics of smart homes—Taking EU GDPR and e-PrivacyDirective legislation as examples. TV Research, 2018, 340(3): 94−96 (in Chinese with English abstract).

[4] Sun JG, Wang JX, Yin GS, Wu XL. Overview of network situation awareness technology. Secrecy Science and Technology, 2016, 67(4): 17−19 (in Chinese with English abstract).

[5] Zhao K, Xing YH. Security survey of Internet of things driven by blockchain technology. Netinfo Security, 2017, 17(5): 1−6.

[6] Shen X, Pei QQ, Liu XF. Overview of blockchain technology. Journal of Network and Information Security, 2016, 2(11): 11−20 (in Chinese with English abstract).

[7] Brambilla G, Picone M, Amoretti M, Zanichelli F. An adaptive peer-to-peer overlay scheme for location-based services. Network Computing and Applications (NCA), 2014, 2(1): 181−188.

[8] Wang Y , Han GG, Li HZ. Provable security mobile user key exchange protocol for wireless communications. Netinfo Security, 2015, 15(3): 54−58.

[9] Gross H, Hölbl M, Slamanig D. Privacy-aware authentication in the Internet of things. In: Proc. of the Int'l Conf. on Cryptology and Network Security. Cham: Springer, 2015. 32−39.

[10] Skarmeta AF, Hernández-Ramos JL, Moreno MV. A decentralized approach for security and privacy challenges in the Internet of things. In: Proc. of the 2014 IEEE World Forum on Internet of Things (WF-IoT). IEEE, 2014. 67−72.

[11] Fakroon M, Alshahrani M, Gebali F, Traore I. Secure remote anonymous user authentication scheme for smart home environment. IEEE Internet of Things Journal, 2020, 9(1): 1−20.

[12] Jiang Y, Shen Y, Zhu QY. A lightweight key agreement protocol based on Chinese remainder theorem and ECDH for smart homes. Sensors, 2020, 20(5): 1357−1368.

[13] Sahraoui S, Bilami A. Compressed and distributed host identity protocol for end-to-end security in the IoT. In: Proc. of the 2014 Int'l Conf. on Next Generation Networks and Services (NGNS). IEEE, 2014. 295−301.

[14] Banerjee S, Odelu V. An efficient, anonymous and robust authentication scheme for smart home environments. Sensors, 2020, 20(4): 1215−1233.

[15] Rahim K, Tahir H, Ikram N. Sensor based PUF IoT authentication model for a smart home with private blockchain. In: Proc. of the Int'l Conf. on Applied and Engineering Mathematics. 2018. 102−108.

[16] Singh S, Ra I, Meng WZ. SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. Int'l Journal of Distributed Sensor Networks, 2019, 15(4): 867−879.

[17] Dang TLN, Nguyen MS. An approach to data privacy in smart home using blockchain technology. In: Proc. of the Int'l Conf. on Advanced Computing and Applications (ACOMP). 2018. 58−64.

[18] Mei C. Design and implementation of IoT security platform based on blockchain [MS. Thesis]. Beijing: Beijing University of Posts and Telecommunications, 2018 (in Chinese with English abstract).

[19] Wang ZY. Research on blockchain technology applied to smart home information security [MS. Thesis]. Wuhan: Huazhong University of Science and Technology, 2019 (in Chinese with English abstract).

[20] Yao YY, Chang XL, Zhen P. Decentralized identity authentication and key management scheme based on blockchain. Cyberspace Security, 2019, 6(10): 36−39 (in Chinese with English abstract).

[21] Wu QH. Crypto technology shoulders the important mission of ensuring the healthy development of the blockchain. China Information Security, 2018, 5(1): 99−102 (in Chinese with English abstract).

[22] Kiayias A, Russell A, David B. Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Proc. of the Annual Int'l Cryptology Conf. 2017. 357−388.

[23] Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. In: Proc. of the 2017 Int'l Congress on Big Data (BigData Congress). IEEE, 2017. 557−564. [doi: 10.1109/BigDataCongress.2017.85]

[24] Yao YY, Chang XL, Mišić J, Mišić VB, Li L. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet of Things Journal, 2019, 6(1): 734−743.

[25] Duan QQ, Xiang DH, Shi HZ. Design on the blockchain-based authentication for smart objects. Netinfo Security, 2018, 18(9): 95−101 (in Chinese with English abstract).

[26] Wang D, Wang P. Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Trans. on Dependable and Secure Computing, 2018, 15(4): 708−722.

[27] Chen ZL. Research on security key technologies of user-centric ultra-dense networks [Ph.D. Thesis]. Beijing: Beijing University of Posts and Telecommunications, 2019 (in Chinese with English abstract).

[28] Jiao L. Research of blockchain data communication performance optimization considering trust degree and weight [Ph.D. Thesis]. Xi'an: Northwestern Polytechnical University, 2017 (in Chinese with English abstract).

[29] Wang D, Li WT, Wang P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor worrks. IEEE Trans. on Industrial Informatics, 2018, 14(9): 4081−4092.

[30] Lin C, He DB, Kumar N, Huang XY, Vijayakumar P. HomeChain: A blockchain-based secure mutual authentication system for smart homes. IIEEE Internet of Things Journal, 2020, 7(2): 818−829.

[31] Wang D, Wang P, Wang CY. Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs. ACM Trans. on Cyber-physical Systems, 2020, 4(3): 1−26.

附中文参考文献:

[2] 孙荣丽, 宫继兵, 王睿, 张磊, 崔莉. WSN 中基于 DSmT 的车辆识别方法研究. 计算机研究与发展, 2010, 47(S2): 246−250.

[3] 仲心. 智媒时代: 智能家居的隐私安全和伦理道德——以欧盟 GDPR 和 e-Privacy Directive 立法为例. 电视研究, 2018, 340(3): 94−96.

[4] 孙建国, 王稼祥, 印桂生, 吴晓鲁. 网络态势感知技术综述. 保密科学技术, 2016, 67(4): 17−19.

[6] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述. 网络与信息安全学报, 2016, 2(11): 11−20.

[18] 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.

[19] 王泽远. 应用于智能家居信息安全的区块链技术研究 [硕士学位论文]. 武汉: 华中科技大学, 2019.

[20] 姚莹莹, 常晓林, 甄平. 基于区块链的去中心化身份认证及密钥管理方案. 网络空间安全, 2019, 6(10): 36−39.

[21] 伍前红. 密码技术肩负着保障区块链健康发展的重要使命. 中国信息安全, 2018, 5(1): 99−102.

[25] 段琼琼, 项定华, 史红周. 基于区块链的智能物件认证技术方案设计. 信息网络安全, 2018, 18(9): 95−101.

[27] 陈中林. 以用户为中心的超密集网络安全关键技术研究 [博士学位论文]. 北京: 北京邮电大学, 2019.

[28] 李皎. 考虑信任度和权值的区块链数据通信性能优化研究 [博士学位论文]. 西安: 西北工业大学, 2017.

张珠君(1987－), 女, 博士, 工程师, 主要研究领域为区块链技术, 物联网安全.

朱大立(1972－), 男, 博士, 正研级高级工程师, 博士生导师, 主要研究领域为移动互联网安全.

范伟(1984－), 男, 博士, 高级工程师, 主要研究领域为云计算技术,云计算安全, 区块链技术.