支持拜占庭容错的分布式物联网访问控制机制

柴蓉[1,2]，艾莉萍[1,2]，杨泞渝[1,2]，梁承超[1,2]
（1.重庆邮电大学通信与信息工程学院，重庆 400065；2.重庆市移动通信技术重点实验室，重庆 400065）

摘　要：随着物联网的广泛应用，物联网设备承载的数据量迅速增长，数据访问需求显著增加。然而，物联网应用场景复杂多样、设备异构高混杂以及数据高度敏感等特性，给数据的高效管理与安全访问带来了严峻挑战。针对存在拜占庭节点的物联网场景，研究物联网访问控制技术，提出了一种分层区块链网络架构，包括一个主集群及多个子集群。综合考虑物联网设备的算力及通信速率，定义节点性能度量以确定主集群节点，并基于系统吞吐量优化确定节点关联策略。基于所构建的分层区块链网络架构，设计数据访问控制智能合约，精确刻画访问控制策略的定义、更新、部署和撤销函数。为实现数据访问控制的高效可靠共识，综合考虑系统共识性能与复杂度，提出了一种改进的 Paxos-Hotstuff 分层共识算法，由主集群节点执行改进式 Paxos 算法，子集群节点执行 Hotstuff 算法。仿真结果验证了所提算法的有效性。

关键词：物联网；访问控制；区块链；共识算法；拜占庭容错；智能合约
中图分类号：TP309
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025068

Byzantine fault-tolerant distributed access control mechanism for the Internet of things

CHAI Rong[1,2], AI Liping[1,2], YANG Ningyu[1,2], LIANG Chengchao[1,2]
1. School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. Chongqing Key Laboratory of Mobile Communication Technology, Chongqing 400065, China

Abstract: With the widespread adoption of the Internet of things (IoT), the data volume handled by IoT devices has been growing rapidly, leading to a significant increase in data access demands. However, the wide geographic distribution of IoT devices, their heterogeneous networks, and the highly sensitive nature of the data pose severe challenges to efficient data management and secure access. Addresses IoT scenarios involving Byzantine nodes by investigating IoT access control technologies, a hierarchical blockchain network architecture was proposed which comprised a main cluster and multiple sub-clusters. Based on the computational power and communication rate of IoT devices, a node performance metric was defined to identify main cluster nodes and determine node association strategies to optimize system throughput. Within the constructed hierarchical blockchain network architecture, smart contracts were deployed to manage access control policies, including their definition, updates, deployment, and revocation. To enable IoT access control in scenarios with Byzantine nodes, an improved Paxos-Hotstuff hierarchical consensus algorithm was proposed, which comprehensively considered system consensus performance and complexity. In the proposed algorithm, the main cluster nodes execute an improved Paxos algorithm, while the sub-cluster nodes execute the Hotstuff algorithm. Simulation results validate the effectiveness of the proposed algorithm.

Keywords: Internet of things, access control, blockchain, consensus algorithm, Byzantine fault tolerance, smart contract

收稿日期：2024–12–31；修回日期：2025–03–29
通信作者：柴蓉，chairong@cqupt.edu.cn
基金项目：国家自然科学基金资助项目（No.62271097）
Foundation Item：The National Natural Science Foundation of China (No.62271097)

0　引言

当今由无线通信技术和智能设备驱动的数字化时代，物联网已成为连接物理世界与数字世界的桥梁，其应用范畴从智能家居延伸至工业控制、智慧城市乃至医疗健康等多个关键领域，实现了前所未有的万物互联[1]。随着物联网的广泛应用，物联网设备所承载的数据量快速增长，设备的数据访问需求也相应显著增加，然而，物联网设备的地理分散性、网络异构性以及数据的高度敏感性均对数据的高效管理与安全访问提出了严峻挑战[2]。因此，亟须研究物联网设备访问控制技术，设计高效可靠的数据访问控制策略，以保障物联网系统安全稳健运行。

近年来，已有文献研究物联网的访问控制问题[3-15]。文献[3]针对智能家居场景，将基于角色及基于属性的访问控制机制相结合，实现用户设备的访问授权。文献[4]针对云辅助物联网提出一种访问控制方案，使用基于属性的可穿刺加密技术保护数据安全及隐私，并引入去中心化密钥生成和密钥更新方法实现数据的安全访问。文献[5]提出一种基于用户声誉评估策略的物联网跨域访问控制方案，以激励用户规范访问网络数据。文献[6]针对工业物联网中实时数据交互的异常行为，提出了一种多级哈希认证方法，以识别和阻止未经授权的数据访问。文献[7]提出了一种安全隐私保护双边访问控制方案，利用细粒度访问控制和匹配加密技术，确保用户健康数据的安全可靠访问。文献[8]提出一种基于云的物联网数据管理方案，支持可外包解密和密钥可追溯性，保证密钥泄露情况下的物联网数据安全。

文献[3-8]提出的物联网访问控制方案采用集中式架构评估设备访问权限，并设计相应访问控制策略，存在单点故障、可扩展性差、动态性管理不足等问题，为解决这一问题，研究人员提出基于区块链的物联网访问控制方案。文献[9-10]使用区块链技术记录物联网设备属性的分布，并设计基于属性的访问控制策略，实现去中心化、细粒度及动态物联网访问控制。文献[11-12]基于区块链的访问记录进行跟踪或动态信任评估，对恶意行为有效检测，防止恶意节点非法创建策略。文献[13-15]通过设计区块链智能合约或使用加密技术构建可信的数据共享环境，实现物联网数据安全及细粒度访问控制。文献[16-17]设计不同区块链共识机制存储物联网访问控制策略，以实现访问策略管理。

针对物联网访问控制问题，现有研究设计基于属性的访问控制策略[9-10]，采用区块链网络的动态信任评估机制[11-12]、智能合约及加密技术[13-15]和共识算法[16-17]实现访问策略管理及访问授权。然而，上述方案未充分考虑物联网大量异构节点共存场景，导致算法可扩展性受限，难以适用于大规模物联网场景。此外，现有研究较少考虑存在拜占庭节点的访问控制问题，导致所提方案难以实现拜占庭容错。

本文针对存在拜占庭节点的大规模物联网场景，研究物联网设备数据访问控制问题。首先提出了一种分层区块链访问控制架构，根据节点性能度量确定主集群节点，并确定节点之间的关联策略以实现系统吞吐量优化；基于所构建的分层架构，进而设计数据安全访问控制方案，提出了基于非对称加密的物联网数据安全访问控制机制及拜占庭容错的分层 Paxos-Hotstuff 算法，实现大规模物联网设备的可靠高效数据访问。

1　系统模型及访问控制架构

1.1　系统模型

本文考虑一个由 M 个物联网设备及 N 个网关设备组成的物联网系统，其中物联网设备执行数据采集任务，并存储所收集的数据。令网络中设备集合为 $\Phi=\{D_1,D_2,\cdots,D_{M+N}\}$，其中 D_n 表示第 n 个网络设备，$1\leqslant n\leqslant M+N$。若 $1\leqslant n\leqslant M$，D_n 表示第 n 个物联网设备；若 $M+1\leqslant n\leqslant M+N$，$D_n$ 表示第 $n-M$ 个网关设备。

假设物联网设备之间可基于访问控制策略实现数据共享。若某个物联网设备（称为请求设备）需获取另一物联网设备（目标设备）的数据，为访问目标设备资源，请求设备通过网关设备向目标设备发送访问请求。网关设备对请求消息进行验证，若请求设备身份合法，网关设备发送确认消息至目标设备，目标设备将所需数据发送至请求设备。不失一般性，假设物联网设备与网关设备均具有无线通信能力，可与邻近设备进行通信。此外，假设网关设备的通信及计算能力强于物联网设备。

本文假设所考虑的物联网场景中存在部分拜占庭设备，令 f 为系统中拜占庭节点的数目。拜占庭

设备因故障或受到攻击而无法正常工作，在接收到来自其他设备的消息后，可能会拒绝响应、延迟响应或进行恶意响应。如何在存在拜占庭设备的大规模物联网中实现可靠数据访问成为亟待解决的问题。系统模型如图1所示。

1.2　基于区块链的物联网分层访问控制架构

为实现可靠的物联网数据访问与共享，本文提出了一种基于区块链的物联网分层访问控制架构，由一个主集群及多个子集群组成。本节首先对所提架构进行概述，进而提出主集群节点确定方案及主集群节点与子集群节点间的关联策略。

1.2.1　架构概述

本节构建基于区块链的物联网分层访问控制架构。该架构利用区块链技术的去中心化和防篡改特性，确保设备之间的通信和数据共享的安全性和可靠性。所提架构中的主集群节点由所有网关设备或部分高性能物联网设备组成，子集群节点由剩余物联网设备组成。每个子集群与一个主集群节点关联，子集群节点仅可与所关联的主集群节点通信，而子集群内的各节点可相互通信；主集群节点间相互可通信，且每个主集群节点仅可与其所关联的子集群节点进行信息交互。基于区块链的分层访问控制架构如图2所示。

1.2.2　基于节点性能度量确定主集群节点

本文基于节点性能度量确定主集群节点。令K表示主集群节点数量，不失一般性，假设$K > N$，也即主集群节点数量大于网关数目，因此，除所有网关设备外，还需选择$K - N$个物联网设备作为主

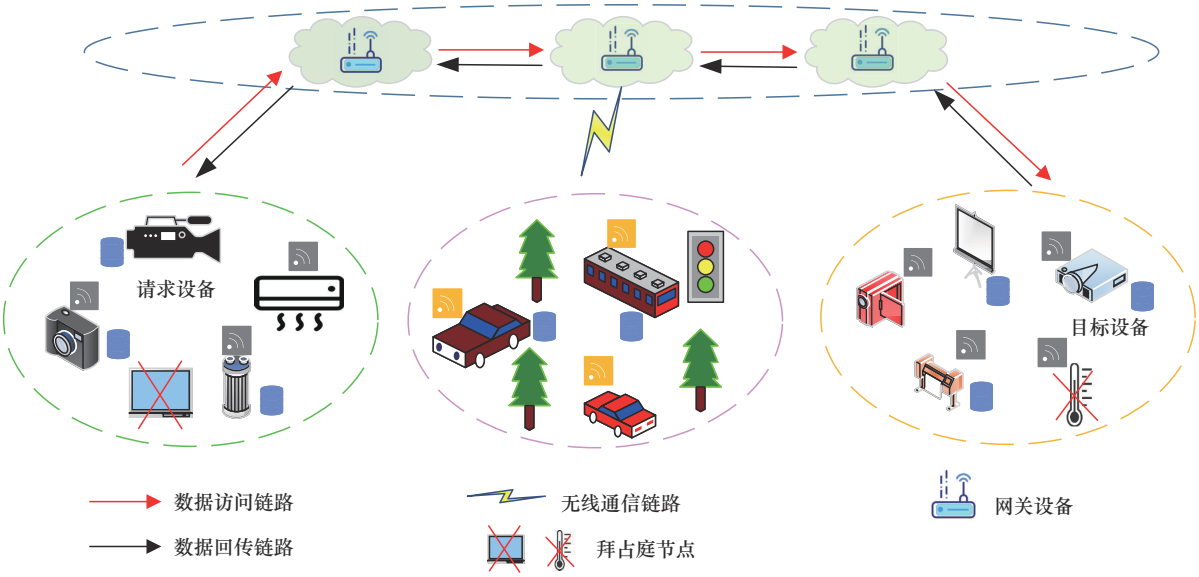


图1　系统模型

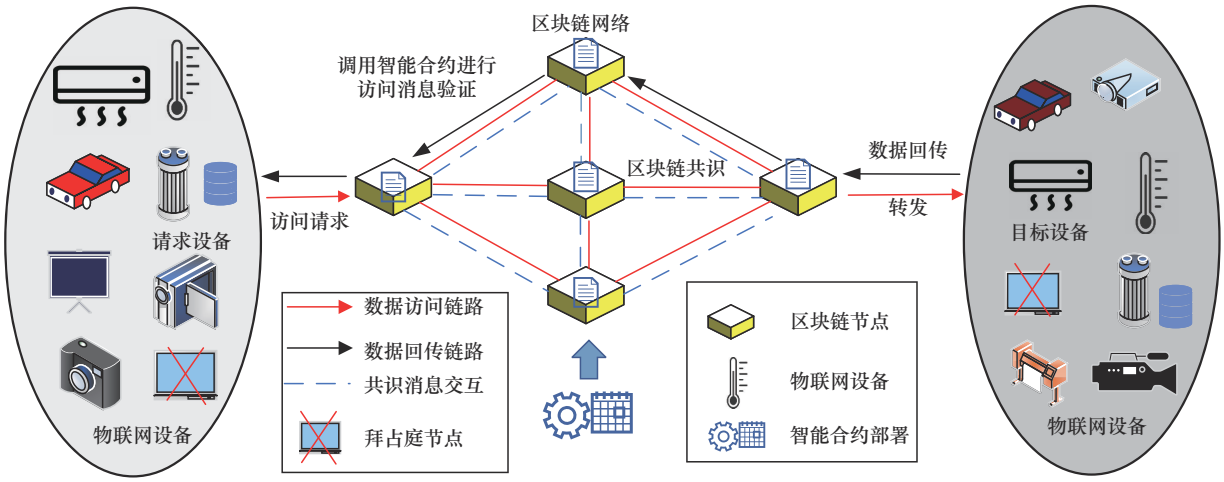


图2　基于区块链的分层访问控制架构

集群节点。

本文基于计算能力及通信能力定义物联网设备性能度量，进而选择性能度量较优的物联网设备作为主集群节点。令μ_n表示物联网设备D_n的算力值，$1 \leqslant n \leqslant M$。考虑网络设备之间的通信性能，将物联网设备的通信能力定义为该设备与所有其他网络设备的通信速率之和。令R_n表示网络设备D_n的通信能力，建模为$R_n = \sum\limits_{\substack{n'=1 \\ n' \neq n}}^{M+N} R_{n,n'}$，$1 \leqslant n \leqslant M+N$，其中，$R_{n,n'}$表示网络设备$D_n$与$D_{n'}$间的通信速率，建模为

$$R_{n,n'} = B_n \mathrm{lb}\left(1 + \frac{P_n h_{n,n'}}{N_0 B_n}\right) \tag{1}$$

其中，B_n为设备D_n的链路可用带宽；P_n为设备D_n的发送功率；$h_{n,n'}$为设备D_n与$D_{n'}$之间链路的信道增益，建模为$h_{n,n'} = \dfrac{\rho}{\left|\boldsymbol{q}_n - \boldsymbol{q}_{n'}\right|^2}$，$\boldsymbol{q}_n$与$\boldsymbol{q}_{n'}$分别为网络设备$D_n$与$D_{n'}$的坐标，$\rho$为单位距离下的信道损耗系数；$N_0$为噪声功率谱密度。

令η_n表示物联网设备D_n的性能度量值，定义为该设备计算能力及通信能力的线性加权，即

$$\eta_n = \omega_1 \mu_n + \omega_2 R_n, 1 \leqslant n \leqslant M \tag{2}$$

其中，ω_1和ω_2分别为节点算力值和通信速率对应的权重。

对物联网设备性能度量值进行降序排列，若$\eta_{n_1} \geqslant \eta_{n_2} \geqslant \cdots \geqslant \eta_{n_M}$，选择物联网设备$D_{n_1}$至$D_{n_{K-N}}$作为主集群节点。令主集群节点集合为$\boldsymbol{\Phi}_\mathrm{p}$，可得$\boldsymbol{\Phi}_\mathrm{p} = \left\{D_{n_1}, D_{n_2}, \cdots, D_{n_{K-N}}, D_{M+1}, \cdots, D_{M+N}\right\}$，其余物联网设备组成子集群节点集合$\boldsymbol{\Phi}_\mathrm{s}$，即$\boldsymbol{\Phi}_\mathrm{s} = \boldsymbol{\Phi} \backslash \boldsymbol{\Phi}_\mathrm{p}$。

1.2.3　基于系统吞吐量优化的节点关联算法

本节基于系统吞吐量优化设计主集群节点与子集群节点之间的关联策略。令R表示系统吞吐量，定义为主集群节点与其所关联子集群节点间的速率和，即

$$R = \sum_{D_k \in \boldsymbol{\Phi}_\mathrm{p}} \sum_{D_i \in \boldsymbol{\Phi}_\mathrm{s}} x_{k,i} R_{k,i} \tag{3}$$

其中，$x_{k,i}$表示主集群节点D_k与子集群节点D_i之间的关联策略，若主集群节点D_k与子集群节点D_i关联，$x_{k,i} = 1$，否则，$x_{k,i} = 0$。将主集群与子集群节点值之间的关联问题建模为系统吞吐量最大化问题，即

$$\begin{aligned}
&\max_{x_{k,i}} \quad R \\
&\text{s.t.} \quad x_{k,i} \in \{0,1\} \\
&\quad \sum_{D_k \in \boldsymbol{\Phi}_\mathrm{p}} x_{k,i} = 1, \forall D_i \in \boldsymbol{\Phi}_\mathrm{s} \\
&\quad \sum_{D_i \in \boldsymbol{\Phi}_\mathrm{s}} x_{k,i} \geqslant 1, \forall D_k \in \boldsymbol{\Phi}_\mathrm{p} \\
&\quad R_{k,i} \geqslant x_{k,i} R_{\min}, \forall D_i \in \boldsymbol{\Phi}_\mathrm{s}, \forall D_k \in \boldsymbol{\Phi}_\mathrm{p}
\end{aligned} \tag{4}$$

其中，$R_{\min}$为网络设备间通信速率的最小值。

由于上述优化问题为主集群节点与子集群节点间的一对多匹配问题，难以采用传统一对一匹配算法进行求解。针对这一问题，本节对主集群节点进行虚拟化，将每个主集群节点虚拟化为L个虚拟节点，其中，$L = \left\lceil \dfrac{N}{K} \right\rceil$；令$D_{k,l}$表示主集群节点$D_k$的第$l$个虚拟节点，令$x_{k,l,i}$表示主集群虚拟节点$D_{k,l}$与子集群节点$D_i$的关联变量，若$D_{k,l}$与$D_i$关联，则$x_{k,l,i} = 1$，否则，$x_{k,l,i} = 0$。令$\boldsymbol{\Phi}'_\mathrm{p} = \left\{D_{k,l} | D_k \in \boldsymbol{\Phi}_\mathrm{p}, 1 \leqslant l \leqslant L\right\}$表示主集群虚拟节点集合，$R_{k,l,i}$表示$D_{k,l}$与$D_i$之间的关联效用值，可得$R_{k,l,i} = R_{k,i}$，$\forall l$，可将系统吞吐量$R$改写为

$$R = \sum_{D_k \in \boldsymbol{\Phi}_\mathrm{p}} \sum_{l=1}^{L} \sum_{D_i \in \boldsymbol{\Phi}_\mathrm{s}} x_{k,l,i} R_{k,l,i} \tag{5}$$

式(4)中所建模的优化问题可转换为主集群虚拟节点$D_{k,l}$与子集群节点D_i之间的一对一关联问题，即

$$\begin{aligned}
&\max_{x_{k,l,i}} \quad R \\
&\text{s.t.} \quad x_{k,l,i} \in \{0,1\} \\
&\quad \sum_{D_k \in \boldsymbol{\Phi}_\mathrm{p}} \sum_{l=1}^{L} x_{k,l,i} = 1, \forall D_i \in \boldsymbol{\Phi}_\mathrm{s} \\
&\quad \sum_{D_i \in \boldsymbol{\Phi}_\mathrm{s}} x_{k,l,i} \leqslant 1, \forall D_k \in \boldsymbol{\Phi}_\mathrm{p}, \forall 1 \leqslant l \leqslant L \\
&\quad \sum_{l=1}^{L} \sum_{D_i \in \boldsymbol{\Phi}_\mathrm{s}} x_{k,l,i} \geqslant 1, \forall D_k \in \boldsymbol{\Phi}_\mathrm{p} \\
&\quad R_{k,l,i} \geqslant x_{k,l,i} R_{\min}, \forall D_k \in \boldsymbol{\Phi}_\mathrm{p}, \forall 1 \leqslant l \leqslant L, \forall D_i \in \boldsymbol{\Phi}_\mathrm{s}
\end{aligned} \tag{6}$$

优化问题式(6)可视为带权完全二部图匹配问题，可采用K-M算法求解，以确定主集群节点与子集群节点的关联策略。将优化问题式(6)映射为带权完全二部图$G = \left(\boldsymbol{\Phi}'_p, \boldsymbol{\Phi}_s, E, W\right)$，其中，$E = \left\{e(D_{k,l}, D_i)\right\}$表示连接主集群虚拟节点与子集群节点

的边的集合，$e\left(D_{k,l},D_i\right)$表示连接主集群虚拟节点$D_{k,l}$与子集群节点$D_i$的边，$W=\left\{w\left(D_{k,l},D_i\right)\right\}$表示边权值集合，$w\left(D_{k,l},D_i\right)$表示$e\left(D_{k,l},D_i\right)$的权值，建模为$w\left(D_{k,l},D_i\right)=R_{k,l,i}$。

基于K-M算法可确定对应系统吞吐量优化的主集群虚拟节点与子集群节点的关联策略。令$x_{k,l,i}^*$表示最优关联策略，若对于任意k,l，$\sum_{l=1}^{L}x_{k,l,i}^*=1$，则$x_{k,i}^*=1$，否则$x_{k,i}^*=0$。

1.3 访问控制策略管理

基于所确定的主集群节点及节点关联算法构建分层区块链网络架构，部署智能合约，以实现对物联网设备访问控制策略的管理，包括访问控制策略的定义、部署、更新及撤销。

令D表示已注册物联网设备集合，$D=\left\{D_1,D_2,\cdots,D_M\right\}$。令$\Psi$表示系统中所有设备访问控制策略的集合，$\Psi=\left\{\Psi_{n,n'},1\leqslant n\neq n'\leqslant M\right\}$，其中，$\Psi_{n,n'}$表示物联网设备$D_n$对物联网设备$D_{n'}$的访问控制策略，定义为$\Psi_{n,n'}=\left(D_n,D_{n'},p_{n,n'}\right)$，$p_{n,n'}$表示物联网设备$D_n$对$D_{n'}$的访问权限，$p_{n,n'}\in\{r,w\}$，$r$、$w$分别表示访问权限为可读、可写。为实现对物联网设备的访问控制管理，在所搭建的区块链架构中定义如下智能合约。

1) 物联网设备注册合约：区块链节点与此合约交互完成物联网设备的注册。若需实现对物联网设备D_n的注册，执行物联网设备注册合约，已注册物联网设备集合更新为$D\leftarrow D\cup\left\{D_n\right\}$。

2) 物联网设备注销合约：区块链节点与此合约交互完成物联网设备的注销。若需完成对物联网设备D_n的注销，执行物联网设备注销合约，已注册物联网设备集合更新为$D\leftarrow D\backslash\left\{D_n\right\}$。

3) 设备访问控制权限增加合约：区块链节点与此合约交互完成物联网设备访问控制权限的增加。若需增加物联网设备D_n对$D_{n'}$的访问权限，执行设备访问控制权限增加合约，在访问控制策略集合中添加$\Psi_{n,n'}$，即$\Psi\leftarrow\Psi\cup\left\{\Psi_{n,n'}\right\}$。

4) 设备访问控制权限撤销合约：区块链节点与此合约交互完成物联网设备访问控制权限的撤销。若需撤销物联网设备D_n对$D_{n'}$的访问权限，执行设备访问控制权限撤销合约，在访问控制策略集合中删除$\Psi_{n,n'}$，即$\Psi\leftarrow\Psi\backslash\left\{\Psi_{n,n'}\right\}$。

5) 物联网设备访问控制策略查询合约：区块链节点与此合约交互完成对物联网设备访问策略的查询，并返回该设备的策略。

6) 物联网设备认证合约：区块链节点与此合约交互完成对物联网设备注册信息的查询。

1.4 基于非对称加密的物联网访问控制流程

基于所构建的物联网访问控制架构及所部署的智能合约，可实现对物联网设备的访问控制。本节对物联网设备访问控制流程进行概述。为实现数据的安全访问，区块链网络为各物联网设备分配公钥及私钥对。令PK_n及SK_n分别表示物联网设备D_n的公钥及私钥，$1\leqslant n\leqslant M$；Enc和Dec分别表示公钥加密和解密算法。为确认访问请求设备的身份，防止物联网设备伪造身份进行数据访问，采用数字签名技术确保数据访问交易的完整性及真实性。令Sig和Ver分别表示数字签名算法和签名验证算法。

不失一般性，假设物联网设备D_n需访问$D_{n'}$的数据资源，且D_n及$D_{n'}$均为子集群节点。基于区块链的物联网访问控制流程简述如下。

1) 请求设备发送访问请求消息

请求设备生成目标数据传输的会话密钥$\varepsilon_{n,n'}$，并采用加密算法对ε进行加密。令$C_{n,n'}$表示请求设备D_n访问目标设备$D_{n'}$加密后的会话密钥，可得$C_{n,n'}=\mathrm{Enc}\left(\varepsilon_{n,n'},\mathrm{PK}_n\right)$。令$T_{n,n'}$表示请求设备访问目标设备的消息类型，其中$T_{n,n'}\in\left\{T_{\mathrm{r}},T_{\mathrm{v}}\right\}$，$T_{\mathrm{r}}$和$T_{\mathrm{v}}$分别表示消息类型为请求消息类型和验证消息类型。请求设备生成访问请求消息，签名后发送至主集群节点。访问请求消息中包含访问消息类型、请求设备公钥标识、目标设备公钥标识、访问权限、加密会话密钥及当前时间戳等信息，可表示为$\mathrm{req}_{n,n'}=\left\langle T_{n,n'},\mathrm{PK}_n,\mathrm{PK}_{n'},p_{n,n'},C_{n,n'},t\right\rangle_{\sigma}$，其中，$\sigma$为请求设备的签名。

2) 主集群节点对请求设备进行认证

主集群节点接收来自请求设备D_n的访问请求消息后，调用物联网设备认证合约对请求设备进行认证。若认证失败，主集群节点拒绝请求设备的访问请求，否则，转至步骤3)。

3) 主集群节点验证访问请求消息

主集群节点采用哈希函数计算访问请求消息

$\mathrm{req}_{n,n'}$的哈希值，并基于数字签名验证算法验证该消息的有效性。令$H\left(\mathrm{req}_{n,n'}\right)$表示该请求消息的哈希值，$\mathrm{Ver}\left(\sigma,\mathrm{PK}_n,H\left(\mathrm{req}_{n,n'}\right)\right)$表示数字签名算法的验证结果。若$\mathrm{Ver}\left(\sigma,\mathrm{PK}_n,H\left(\mathrm{req}_{n,n'}\right)\right)$为真，则确认访问请求消息来自合法请求设备，且在传输过程中未被篡改，转至步骤4)；否则，该访问请求消息不合法，拒绝请求设备的访问请求。

4) 生成访问交易并验证

主集群节点根据验证后的访问请求消息生成访问交易。将该交易表示为$\mathrm{Tx}_{n,n'}=\left\langle\mathrm{TxID},\mathrm{req}_{n,n'}\right\rangle$，其中，TxID为交易$\mathrm{Tx}_{n,n'}$的标识。主集群节点将访问交易$\mathrm{Tx}_{n,n'}$发送至请求设备。请求设备确认该交易是否符合自身访问控制请求，若是，则对访问交易信息进行哈希操作，签名后发送至主集群节点。令τ表示请求设备对交易信息的签名，可得$\tau=\mathrm{Sig}\left(H\left(\mathrm{Tx}_{n,n'}\right),\mathrm{SK}_n\right)$。主集群节点通过验证请求者的签名$\tau$判断访问交易的真实性，若$\mathrm{Ver}\left(\tau,\mathrm{PK}_n,H\left(\mathrm{Tx}_{n,n'}\right)\right)$输出为真，则验证通过，转至步骤5)；否则，访问交易验证不通过，主集群节点拒绝提交该访问交易，请求设备访问目标设备资源失败。

5) 区块链网络对访问交易达成共识

区块链网络对验证后的访问交易执行Paxos-Hotstuff算法（第2节详述）。若达成共识，则允许请求设备对目标设备进行数据访问，转至步骤6)；否则，拒绝请求设备的访问请求。

6) 获取目标设备资源

主集群节点将访问请求发送至目标设备，目标设备使用其私钥对加密后的会话密钥$C_{n,n'}$解密，获取会话密钥ε，即$\varepsilon=\mathrm{Dec}\left(C_{n,n'},\mathrm{SK}_{n'}\right)$。目标设备通过会话密钥$\varepsilon$对数据资源加密后发送至对应主集群节点，主集群节点转发数据资源至请求设备，请求设备使用会话密钥解密以获取目标设备的数据资源。

2　基于Paxos-Hotstuff的分层共识算法

本文基于区块链的分层网络架构中，主集群及子集群节点针对物联网请求设备的访问交易执行共识算法，若达成共识，则允许请求设备访问目标设备的数据。本文综合考虑系统共识性能及复杂度，提出基于Paxos-Hotstuff的分层共识算法，由主集群节点执行改进式Paxos算法，子集群节点执行Hotstuff算法，主集群节点作为对应子集群Hotstuff算法的领导者节点。本节分别介绍基于改进式Paxos算法的主集群共识机制及基于Hotstuff算法的子集群共识机制，Paxos-Hotstuff 算法流程如图3所示。

2.1　基于改进式Paxos算法的主集群共识机制

2.1.1　算法概述

传统Paxos算法将节点分为提案者、投票者和学习者3类角色。算法流程概述如下。1)提案者选择一个提案编号N，并向所有投票者发送准备请求消息；投票者接收到准备请求消息回复承诺消息，表明不再接受编号小于N的提案。2)提案者在收到来自大多数投票者的承诺消息后，发送提案请求消息，其中包含对应提案及其编号N。3)投票者接收提案请求消息后，若确认提案编号有效，则发送接受消息。4)若提案者收到来自大多数投票者的接受消息，则发送提案共识确认消息，表明该提案已达成共识；学习者收到提案共识确认消息后存储该

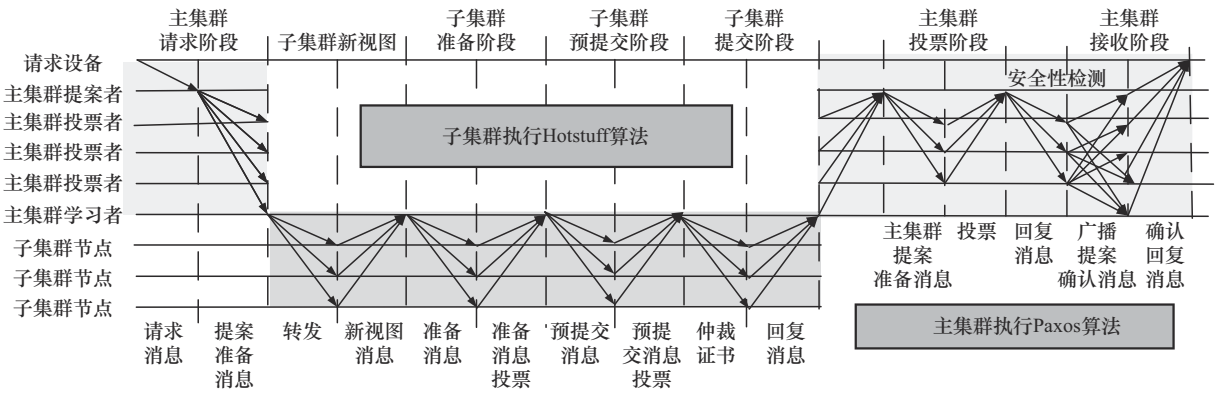


图3　本文Paxos-Hotstuff 算法流程

提案。

传统Paxos算法具有算法流程较为简单、计算开销小、执行效率高等优点，然而，传统Paxos算法采用单提案设计，每轮操作仅针对单个提案达成共识，无法实现多提案共识的并行执行。此外，传统Paxos算法仅考虑节点可能崩溃或超时，并设计超时机制和重新选举机制恢复共识进程。若拜占庭节点恶意篡改或伪造消息，Paxos算法无法检测该行为，故难以实现拜占庭容错，无法用于存在拜占庭节点的物联网场景中。针对传统Paxos算法存在的问题，本文提出改进式Paxos算法，采用流水线及安全检测等机制提升算法性能。流水线机制允许不同提案在不同阶段同时进行，从而实现多个提案的并行处理；安全检测机制保证系统中存在拜占庭节点时可达成共识。

2.1.2 安全检测及流水线机制

传统Paxos算法无法解决恶意节点发送错误投票的问题，导致算法在拜占庭故障场景中失效。针对这一问题，本文引入安全检测机制实现共识算法的拜占庭容错，安全性检测机制包含2个规则，即安全性规则及活跃性规则。

投票者在对其他投票者的签名进行聚合后，针对聚合签名，进行安全性规则验证，确保投票者及聚合签名的真实性和一致性。安全性规则检测所对应的投票者是否为聚合签名后仲裁证书的直接子节点，若是，说明各节点间的待提交交易都是同步的；若不是，进一步确定安全性检测不一致的投票者数量。若一半以上投票者检测不一致，则终止该提案共识；否则，安全性检测通过。使用安全性检测机制可以保证即使系统存在部分节点出现故障或恶意行为时，仍然能够保持系统的稳定性和安全性。

传统Paxos算法主要用于单个提案达成共识，对于存在多个提案并行的情况，可能导致提案冲突，最终无法达成共识。针对这一问题，本文设计流水线机制，允许多个提案同时处于不同的共识阶段。定义活跃性检测规则用于检测系统是否能够在合理时间内达成共识，并判断是否存在网络分区或节点失效等问题，避免系统停滞不前或无法在有效时间内达成一致。首先，投票者对接收到的提案者视图编号进行检测，选取所收到的最大视图编号并进行锁定，防止当前提案共识期间其他提案提出影响最终共识结果。其次，判断锁定的视图编号是否小于仲裁证书的视图编号，若是，表明该投票者在对一个已达成共识的视图进行验证，也即存在提案冲突，则需进行视图切换，由提案者生成新的视图编号，直至达成共识；否则，继续当前提案的共识。

2.1.3 算法流程

本节提出的改进式Paxos算法的具体流程包括请求阶段、投票阶段及接收阶段。

1) 请求阶段

若请求设备拟获取目标设备的数据资源，请求设备将请求消息发送至所关联的主集群节点。主集群节点验证请求消息合法性，若通过验证，则生成提案请求消息，并将该消息发送至提案者。提案者接收到提案请求消息后，添加提案准备消息标识符、提案索引、提案编号N、成功共识的最大提案编号$N_{\max}$，生成提案准备消息，并将其发送给所有主集群节点。主集群节点接收提案准备消息，广播至对应的子集群。子集群节点收到提案准备消息后，执行Hotstuff算法以达成共识。

若子集群共识成功，领导者发送对应共识结果至主集群提案者。提案者判断子集群共识成功消息数量是否超过主集群数量的一半，若否，共识失败，生成确认回复消息，其中，确认回复消息包含各子集群共识失败消息及提案者签名；否则，主集群节点基于改进式Paxos算法执行共识。

2) 投票阶段

主集群提案者将子集群共识成功消息添加至主集群提案准备消息中，并发送至投票者。投票者基于提案准备消息对提案进行投票，将投票结果进行聚合，生成聚合签名，添加至回复消息中并发送至提案者。提案者对回复消息进行安全性检测，若检测通过且提案者收到半数以上投票者的回复结果，则生成提案确认消息，其中包含提案准备消息标识符、提案索引、当前提案编号N及时间戳；若未通过安全性检测或提案者收到的投票者的回复少于半数，则生成提案拒绝消息，并发送至其他主集群节点。

3) 接收阶段

主集群投票者接收提案确认消息，广播该消息。学习者监听提案消息并执行对应提案，将最大提案编号更新为$N_{\max}=N$。主集群节点生成确认回

复消息，发送至请求设备，此次提案共识成功。

2.2　基于 Hotstuff 算法的子集群共识机制

本文分层架构中，子集群节点执行 Hotstuff 算法实现访问请求的共识。本节对 Hotstuff 算法进行概述，并对共识流程进行阐述。

2.2.1　算法概述

Hotstuff 算法采用领导者驱动及流水线机制，由领导者负责提议新的提案，并以广播方式发送至所有副本节点。副本节点验证提案的正确性，并向领导者发送投票。领导者接收到至少 $2f+1$ 个投票后，生成仲裁证书，并将其传播至副本节点。每个提案达成共识需要经历 3 个阶段，即准备阶段、预提交阶段、提交阶段，每个阶段的完成均依赖于上一阶段生成的仲裁证书作为状态确认的证明。副本节点在连续完成 3 个提案的验证后，提交区块到区块链中，从而实现高效、安全且容错性强的共识。

Hotstuff 结合拜占庭容错机制的核心思想与流水线机制，实现了高效拜占庭容错。然而，Hotstuff 算法性能与领导者节点的性能密切相关，若领导者出现故障或网络延迟，可能导致系统共识性能下降。针对这一问题，本文所选择的主集群节点，即子集群领导者节点为网关或性能较优的物联网设备，从而可有效保障子集群共识性能。此外，本文分层架构能够有效实现多个领导者及子集群的同步共识，从而提升系统的并行性和可扩展性。

2.2.2　算法流程

子集群节点接收到主集群节点的提案准备消息后，基于 Hotstuff 算法执行子集群共识。该算法具体步骤包括准备阶段、预提交阶段、提交阶段、决定阶段。

1) 准备阶段

子集群节点收到提案准备消息后，生成视图编号，启动新一轮的视图，并将视图编号添加至提案准备消息中生成新视图消息，发送至领导者。领导者收集子集群节点发送的新视图消息，若新视图消息超过 $2f+1$，领导者在所收集的新视图消息中选取具有最高视图编号的消息进行聚合签名后生成准备仲裁证书，并将准备仲裁证书封装至准备消息中，广播准备消息。

2) 预提交阶段

子集群节点接收准备消息，对提案进行投票，并将投票结果发送至对应子集群的领导者。若领导者收集到超过 $2f+1$ 个节点的投票后，对投票结果进行阈值签名操作，生成预提交仲裁证书并将其添加至生成的预提交消息中，预提交消息中包含视图编号、预提交仲裁证书、时间戳、提案索引、当前提案编号 N。

3) 提交阶段

领导者将预提交消息广播至子集群节点，子集群收到预提交消息后，对该消息进行投票。若投票通过，则对预提交消息添加签名，并将签名后的消息发送至领导者。若领导者节点至少收集到 $2f+1$ 个关于预提交消息的签名，则进行签名聚合操作，将聚合签名作为提交仲裁证书，并生成提交消息。该消息中包含视图编号、预提交仲裁证书、提交仲裁证书、时间戳、提案索引、提案编号 N。领导者广播提交消息至子集群节点，子集群节点收到提交消息后，对该消息进行验证，若验证通过，返回验证通过消息至对应领导者。

4) 决定阶段

拜占庭容错的物联网访问控制方案如图 4 所示。若领导者收到不少于 $2f+1$ 个验证通过消息，则生成回复证书及决定消息，其中决定消息包含视图编号、预提交仲裁证书、提交仲裁证书、时间戳、提案索引、提案编号 N、回复证书。领导者将决定消息广播至子集群节点，实现子集群节点的共识。

2.3　共识算法安全性证明

本文分层 Paxos-Hotstuff 共识算法的安全性证明包括一致性证明和不可逆性证明。一致性是指在存在拜占庭节点的情况下，所有诚实节点仍可对提案达成一致，即在相同的视图中不同节点提交的提案一致，不会出现多个不同提案。不可逆性是指若某个区块已被提交，后续不会出现与之冲突的区块。

2.3.1　算法一致性证明

1) 主集群一致性证明

本文改进的 Paxos-Hotstuff 分层共识算法中，主集群基于 Paxos 算法达成共识。主集群一致性是指对于存在 2 个或多个节点生成的仲裁证书，若对应的共识阶段（类型）相同，且节点提交的提案相互冲突，则对应仲裁证书应不同。

根据本文 Paxos 算法的安全性机制，若节点投票生成仲裁证书，则投票的诚实节点数量不少于

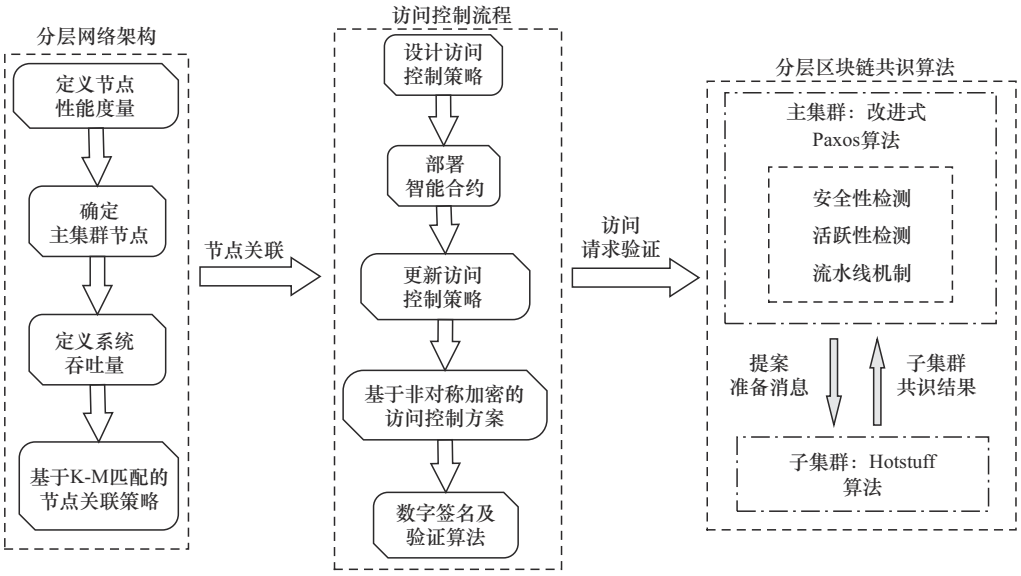


图4　拜占庭容错的物联网访问控制方案

$2f+1$。若节点1在编号为qc_1.viewNumber的视图中提交仲裁证书qc_1，说明节点1至少获得了$2f+1$个投票。类似地，若节点2在编号为qc_2.viewNumber的视图中生成仲裁证书qc_2，也需收到$2f+1$个投票。由于系统节点总数为$3f+1$，其中，拜占庭节点数量最多为f个，诚实节点数量不少于$2f+1$，因此，2个仲裁证书间至少有$2f+1$个共同节点。若2个提案相互冲突，诚实节点在同一视图下无法对这2个提案同时进行投票，因此无法生成2个有效的仲裁证书，从而严格保证了算法一致性。

2) 子集群一致性证明

子集群基于Hotstuff算法达成共识，在共识准备阶段、预准备阶段和提交阶段，若节点至少收到$2f+1$个投票，则生成对应阶段的仲裁证书。证明Hotstuff算法的一致性，即需证明在同一个视图及共识相同阶段，不存在2个不同的有效仲裁证书。

以下对算法一致性进行说明。若在同一个视图，节点1及节点2分别生成视图qc_1及qc_2，则说明节点1及节点2均至少获得$2f+1$个投票。由于系统节点总数为$3f+1$，其中，诚实节点数量不少于$2f+1$，且任何一个诚实节点在一个视图只能投票一次，因此，一个诚实节点不可能同时支持qc_1和qc_2。若qc_1和qc_2不同，则其对应的投票集合至少部分不相交，即意味着部分诚实节点同时支持qc_1及qc_2，与诚实节点在每个视图的相同阶段只能投票一次的投票规则相矛盾，因此可得出结论：在相同视图的相同阶段，不可能存在2个不同的qc，从而保证了共识协议的一致性。

2.3.2　*算法不可逆性证明*

证明子集群所采用的Hotstuff算法满足不可逆性，即需证明：若节点1及节点2为相互冲突的节点，则2个节点所对应的提案不可能均被提交。不失一般性，假设节点1及节点2均在提交阶段生成2个有效的qc，即qc_1.type = commit，qc_2.type = commit。令v_1和v_2分别表示qc_1和qc_2的视图编号，根据一致性可知，$v_1 \neq v_2$，假设$v_1 < v_2$。由于qc_2是提交阶段的仲裁证书，意味着在v_2之前的某个视图v_s中，必然存在一个准备阶段的有效qc，该qc与节点1的提案冲突，且qc_s满足最小性，也即qc_s为节点1与节点2发生冲突前最早的准备阶段的qc。

由于节点1及节点2生成qc_1和qc_2均需要至少$2f+1$个投票，而系统总节点数量为$3f+1$，因此至少存在多个诚实节点同时对qc_1及qc_s进行投票。若某个诚实节点，如诚实节点3在视图v_1时，对节点1的提案进行了投票，并锁定了当前投票，由于qc_s与节点1的提案qc相冲突，且qc_s的视图号大于v_1，诚实节点3只有在qc_s形成之前对节点1的提案解锁，才能投票给qc_s。这与qc_s的最小性矛盾。由于在qc_s之前不存在另一个与节点1的提案冲突的准备qc，因此qc_s不可能被创建，与假设相矛盾。因而，可证明冲突节点所支持的区块不可能都被提

交，即已提交区块不可能被回滚，证明了算法的不可逆性。采用类似方法可证明主集群所采用的Paxos算法也满足不可逆性。

3　仿真分析

对本文基于区块链的物联网访问控制算法的性能进行仿真评估，所考虑的仿真场景由多个物联网设备及网关节点组成，仿真区域大小为2 000 m×2 000 m，网关设备及物联网设备随机分布。仿真参数设置如表1所示[18-19]，所有仿真结果为多次实验的平均值。

表1　　仿真参数设置

仿真参数	数值
物联网设备发送功率P_n/ W	0.1
噪声功率谱密度N_0/(dBm·Hz^{-1})	−174
链路带宽B_n/MHz	1
单位距离下的信道损耗系数ρ	0.01
预准备阶段阈值签名生成时间/ms	100
准备阶段阈值签名生成时间/ms	100
提交阶段阈值签名生成时间/ms	100

共识时延与节点数量关系如图5所示。由图5可知，随着系统节点数量增加，各算法对应的系统平均共识时延均逐渐增大。这是因为节点数量的增加导致节点间进行同步所发送和接收的数据量也随之增加，从而导致共识时延的增加。对比不同共识算法性能可知，本文算法达成共识所需时延低于文献[9]、文献[16]及文献[18]所提算法，略高于单层Hotstuff。原因是文献[9]所使用的PBFT算法采用3阶段共识，各阶段所有节点均需与其他节点进行信息交互，且视图切换过程较为复杂，导致算法通信及计算开销较大，共识时延较高。文献[16]采用单层Paxos算法，对于较大规模物联网场景，算法投票者及学习者数量显著增加，领导者及投票者消息验证所需时延较长，导致共识时延相应增加。文献[18]所提分层共识算法采用“两步聚类”方法构建双层区块链架构，并将混合阈值代理签名与PBFT算法相结合。由于文献[18]所提算法采用双层PBFT算法，共识阶段多节点复杂交互方式导致共识时延较长。本文改进的Paxos-Hotstuff分层共识算法兼具分层架构、Paxos及Hotstuff算法的性能优势，与文献[9]、文献[16]及文献[18]所提算法相比，共识时延短且算法复杂度低。需说明的是，本文算法为实现大规模物联网设备的访问控制请求共识，构建了分层区块链网络架构，增加了多轮验证阶段，同时增加了对提案消息的投票及验证过程，从而导致共识时延略高于单层Hotstuff算法。

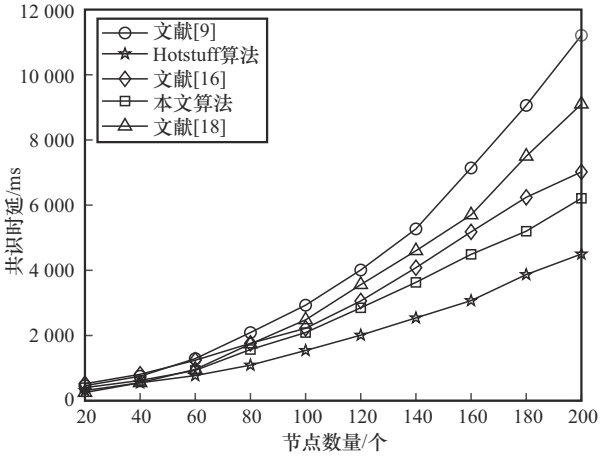


图5　共识时延与节点数量关系

吞吐量与节点数量关系如图6所示。由图6可知，随着系统节点数量增加，系统吞吐量呈现下降趋势。这是因为随着节点数量的增加，每个节点需要与其他节点交互的数据量也显著增加，占用大量系统通信资源，从而导致吞吐量的下降。对比不同共识算法的系统吞吐量可知，本文算法在节点数量较大时对应的吞吐量高于其他4种算法，原因是本文算法的分层架构使得系统资源分配更加灵活，各集群内部共识可并行执行，从而显著提升系统吞吐量。此外，本文改进的Paxos-Hotstuff分层共识算法兼具改进Paxos算法的低复杂度、高可靠性、拜占庭容错，以及Hotstuff算法支持并行共识、复杂度低及扩展性强的性能优势。文献[9]及文献[18]所提算法中采用PBFT算法，节点间信息交互复杂，导致算法通信及计算开销较大，吞吐量较低。文献[16]所采用的单层Paxos算法，在算法投票者及学习者数量较多时，消息验证所需时延较长，导致吞吐量较低。视图变更开销也会进一步降低系统的整体吞吐量。Hotstuff算法采用单层架构，在节点数量较大时，节点间状态同步、仲裁证书交互及视图切换的通信开销均相应增加，导致系统吞吐量降低。

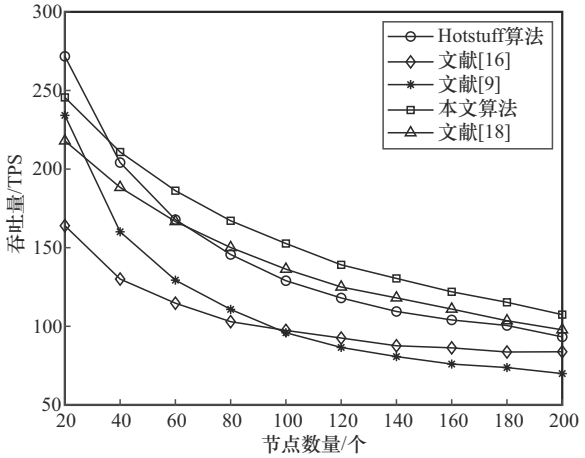


图6　吞吐量与节点数量关系

共识时延与集群数量关系如图7所示。由图7可知，共识时延随着集群数量的增加呈现先减后增的趋势。这是因为增加集群数量减少了子集群内部达成共识所需的通信次数，子集群内部共识时延及系统共识时延相应减少；随着集群数量的持续增加，主集群节点间通信更为频繁，导致共识时延逐渐增加。对比不同节点数量的共识时延可以看出，随着节点数量的增加，共识时延相应增加。

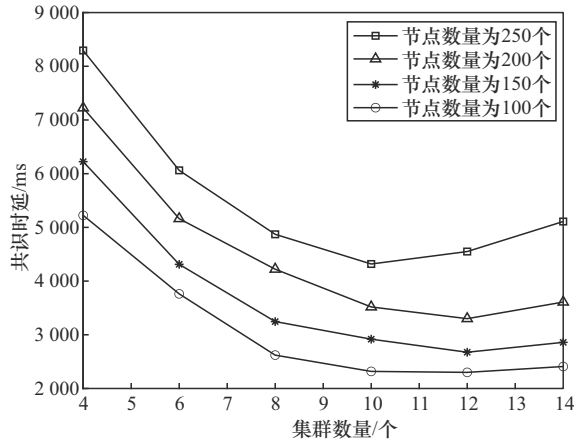


图7　共识时延与集群数量关系

吞吐量与集群数量关系如图8所示。由图8可知，随着集群数量的增加，系统吞吐量相应增加。这是因为节点数量一定时，随着集群数量的增加，子集群内节点数量相应减少，节点达成共识所需时延较小，吞吐量相应增加。对比不同节点数量的吞吐量可以看出，随着节点数量的增加，吞吐量相应增加。

通信开销与节点数量的关系如图9所示。由图9可知，随着节点数量的增加，各算法的通信开销均相应增加。这是因为随着节点数量的增加，节点之间的交互数量显著增加，导致通信开销增加。对比不同共识算法对应的通信开销可知，本文算法的通信开销较小。文献[9]所采用的PBFT算法涉及复杂的节点间交互，导致通信开销较大。文献[16]采用的单层Paxos算法在节点数量较多时，算法投票者及学习者数量显著增加，节点间通信量快速增加，导致通信开销相应增加。本文基于Paxos-Hotstuff算法采用双层架构及低复杂度的Hotstuff算法，可实现较低的通信开销。

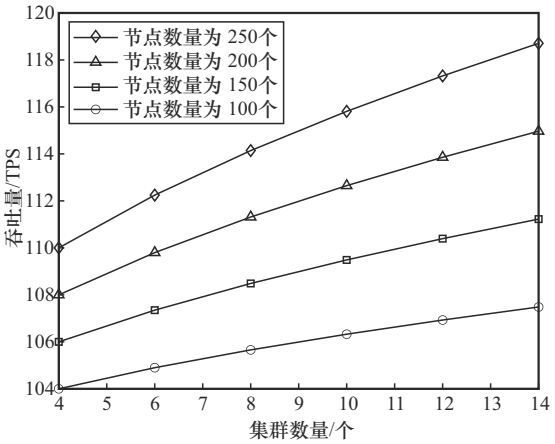


图8　吞吐量与集群数量关系

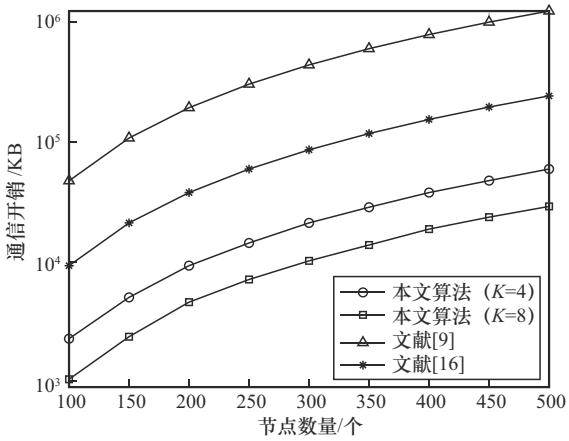


图9　通信开销与节点数量关系

吞吐量与故障节点比例关系如图10所示。由图10可知，随着故障节点比例增加，系统吞吐量呈现下降趋势，且下降趋势随故障节点比例增加而增大。这是由于故障节点比例较小时，共识成功率较高，节点故障对共识结果影响较小。随着故障节点比例不断增大，导致集群间共识失败数目增多，共识成功率降低，系统吞吐量相应降低。

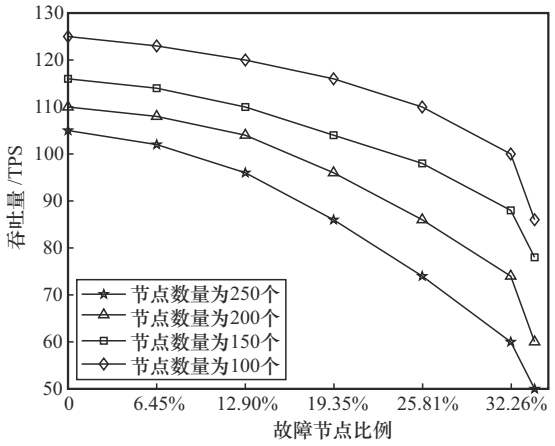


图10　吞吐量与故障节点比例关系

4　结束语

针对大规模物联网场景的访问控制问题，本文研究基于区块链的可扩展访问控制架构及可靠的访问控制共识机制。首先，构建分层区块链网络架构，包括主集群及子集群，进而基于节点性能度量确定主集群节点，并提出基于系统吞吐量优化设计主集群节点与子集群节点之间的关联策略。其次，为实现网络设备间的高效共识，设计基于 Paxos-Hotstuff 共识机制的物联网访问控制算法。最后，分析本文算法的共识时延、系统吞吐量。仿真结果表明，本文算法在不同节点数量、不同集群数量、不同故障节点比例下的平均时延和系统吞吐量有着较为优异的表现，适用于大规模物联网场景下网络设备达成共识，具备良好的实用性。

参考文献：

[1] CHETTRI L, BERA R. A comprehensive survey on Internet of things (IoT) toward 5G wireless systems[J]. IEEE Internet of Things Journal, 2020, 7(1): 16-32.

[2] QIU J, TIAN Z H, DU C L, et al. A survey on access control in the age of Internet of things[J]. IEEE Internet of Things Journal, 2020, 7(6): 4682-4696.

[3] AMEER S, BENSON J, SANDHU R. Hybrid approaches (ABAC and RBAC) toward secure access control in smart home IoT[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(5): 4032-4051.

[4] DENG H, YIN H, QIN Z, et al. Toward fine-grained and forward-secure access control in cloud-assisted IoT[J]. IEEE Internet of Things Journal, 2024, 11(22): 36569-36580.

[5] HE Q W, LIN H, HU J, et al. A novel cross-domain access control protocol in mobile edge computing[C]//Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE Press, 2021: 1-6.

[6] WANG J P, ZHU M, LI M H, et al. An access control method against unauthorized and noncompliant behaviors of real-time data in industrial IoT[J]. IEEE Internet of Things Journal, 2024, 11(1): 708-727.

[7] SUN J F, YUAN Y, TANG M J, et al. Privacy-preserving bilateral fine-grained access control for cloud-enabled industrial IoT healthcare[J]. IEEE Transactions on Industrial Informatics, 2022, 18(9): 6483-6493.

[8] HAHN C, KIM J, KWON H, et al. Efficient IoT management with resilience to unauthorized access to cloud storage[J]. IEEE Transactions on Cloud Computing, 2022, 10(2): 1008-1020.

[9] DING S, CAO J, LI C, et al. A novel attribute-based access control scheme using blockchain for IoT[J]. IEEE Access, 2019, 7: 38431-38441.

[10] LIU H, HAN D Z, LI D. Fabric-IoT: a blockchain-based access control system in IoT[J]. IEEE Access, 2020, 8: 18207-18218.

[11] HAN D Z, ZHU Y J, LI D, et al. A blockchain-based auditable access control system for private data in service-centric IoT environments[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 3530-3540.

[12] FENG L B, LIN J Y, QIU F, et al. SDAC-BBPP: a secure dynamic access control scheme with blockchain-based privacy protection for IIoT[J]. IEEE Transactions on Network and Service Management, 2024, 21(3): 3179-3193.

[13] MERLEC M M, IN H P. SC-CAAC: a smart-contract-based context-taware access control scheme for blockchain-enabled IoT systems[J]. IEEE Internet of Things Journal, 2024, 11(11): 19866-19881.

[14] SAHA R, KUMAR G, CONTI M, et al. DHACS: smart contract-based decentralized hybrid access control for industrial Internet-of-things[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 3452-3461.

[15] CHENG G J, WANG Y W, DENG S G, et al. A lightweight authentication-driven trusted management framework for IoT collaboration[J]. IEEE Transactions on Services Computing, 2024, 17(3): 747-760.

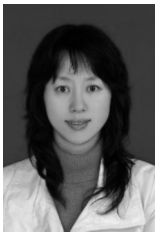
[16] FENG Y M, ZHANG W Z, LUO X P, et al. A consortium blockchain-based access control framework with dynamic orderer node selection for 5G-enabled industrial IoT[J]. IEEE Transactions on Industrial Informatics, 2022, 18(4): 2840-2848.

[17] HAO X H, REN W, FEI Y Y, et al. A blockchain-based cross-domain and autonomous access control scheme for Internet of Things[J]. IEEE Transactions on Services Computing, 2023, 16(2): 773-786.

[18] TANG F, XU T X, PENG J L, et al. TP-PBFT: a scalable PBFT based on threshold proxy signature for IoT-blockchain applications[J]. IEEE Internet of Things Journal, 2024, 11(9): 15434-15449.

[19] 3GPP. User equipment (UE) radio transmission and reception (release 10): TS 25.101[S]. 2022.

[作者简介]



柴蓉（1974– ），女，陕西西安人，博士，重庆邮电大学教授，主要研究方向为空天体一体化网络架构及关键技术、无线资源管理及移动性管理技术、区块链等。

艾莉萍（2001– ），女，江西赣州人，重庆邮电大学硕士生，主要研究方向为区块链共识、访问控制架构、网络安全及密码学原理等。

杨泞渝（2000– ），男，重庆人，重庆邮电大学硕士生，主要研究方向为区块链共识、访问控制架构、网络安全等。

梁承超（1988– ），男，贵州贵阳人，重庆邮电大学教授，主要研究方向为移动通信、无线网络、卫星互联网及优化理论等。