计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20180073
55(7):1462-1478,2018

基于区块链的分布式物联网信任管理方法研究

任彦冰[1] 李兴华[1] 刘 海[1] 程庆丰[2] 马建峰[1]
[1](西安电子科技大学网络与信息安全学院 西安 710071)
[2](数学工程与先进计算国家重点实验室(解放军信息工程大学) 郑州 450001)
(yanbing_ren@foxmail.com)

Blockchain-Based Trust Management Framework for Distributed Internet of Things

Ren Yanbing[1], Li Xinghua[1], Liu Hai[1], Cheng Qingfeng[2], and Ma Jianfeng[1]
[1](*School of Cyber Engineering, Xidian University, Xi'an* 710071)
[2](*State Key Laboratory of Mathematical Engineering and Advanced Computing (PLA Information Engineering University), Zhengzhou* 450001)

Abstract With the development of the Internet of things (IoT) technology, a new scenario emerges among various IoT networks in which different IoT networks form a large-scale, heterogeneous and dynamic distributed IoT environment. There is a need for various cooperations among devices and IoT authorities, for which it is necessary to establish a trust mechanism to promote cooperation. However, the existing researches on trust mechanism are mostly separated from the IoT environment, and do not consider the resource limitations of IoT devices as well as great differences among them in computing and storage capabilities, which results in the study of abstract trust mechanisms can not be directly applied to IoT. On the other hand, the existing researches on the issues of IoT trust rely on additional trusted third-party or inter-domain trust assumption, which is hard to be achieved in practice. In order to solve the above problems, we propose a trust management method which is suitable for distributed IoT with the help of blockchain and risk theory. Specifically, we embody the abstract concept of trust as an examination of expected credit and risk, and enable effective sharing of trust data using blockchain. Experimental simulation and analysis show that our method can quantify the trust effectively, protect the data from being tampered and have lower storage cost.

Key words trust management; distributed systems; Internet of things (IoT); risk; blockchain

摘 要 随着物联网(Internet of things, IoT)技术的发展,在不同的物联网之间逐渐形成了大规模、异构化、动态化的分布式物联网环境.分布式物联网内的设备间与物联网管理机构间存在着广泛的合作需求,为此需要在其中建立信任机制以促进合作.然而,现有的信任机制研究大部分脱离于物联网环境,没有考虑物联网设备计算与存储能力有限且差异较大这一特点,造成抽象信任机制研究无法直接应用于物联网中;另一方面,现有的物联网信任问题研究都依赖于额外的可信第三方或域间信任假设,这在实际中是难以实现的.为了解决上述问题,借助区块链与风险理论,提出一种适用于分布式物联网的信任

收稿日期:2018-01-31;**修回日期**:2018-05-02
基金项目:国家自然科学基金项目(U1708262,U1736203,U1405255);国家重点研发计划项目(2017YFB0801805)
This work was supported by the National Natural Science Foundation of China (U1708262, U1736203, U1405255) and the National Key Research and Development Program of China (2017YFB0801805).
通信作者:李兴华(xhli1@mail.xidian.edu.cn)

管理方法.具体地,将信任量化为对期望信用与风险的考察,并借助区块链实现信任数据的有效共享与安全性.实验与分析表明:该方案能够有效量化信任,保护数据不被篡改,且能够以较低的存储开销维护系统的正常运行.

关键词 信任管理;分布式系统;物联网;风险;区块链

中图法分类号 TP399

随着物联网(Internet of things, IoT)技术的发展,在不同的物联网之间逐渐形成了大规模、异构化、动态化的分布式物联网环境.其中每个物联网作为一个独立的管理域都拥有大量的物联网设备,独立的域内通信协议与管理方式.物联网中的设备存在着合作、交互与资源调度的需求(后文将此过程统称为合作),设备间的合作可能在管理域内进行,也可能在管理域间进行;另一方面,物联网管理机构间也存在着业务往来、信息共享等各种形式的合作.由于物联网内设备众多,异构物联网之间在域内组织与管理机制等方面存在较大差异,分布式物联网中的合作问题尚未得到有效解决.

解决合作问题的前提是在物联网设备间以及机构间建立信任机制,然而物联网应用种类众多,不同机构的业务属性与信任特征各异,各种物联网设备在计算与存储能力上存在较大差异,使得现有的抽象信任机制研究无法直接应用在分布式物联网环境中.另一方面,现有的物联网信任研究大部分属于对管理域内信任问题的研究,对于管理域间信任问题的研究依然较少且无法应用于不依赖可信第三方与额外信任假设的完全分布式物联网环境中.

对此本文借助区块链与风险理论,提出了一种适用于分布式物联网的信任管理方法,具体地,我们将"信任"这一主观抽象的概念[1]具体化为对期望信用(expected credit)与风险(risk)的考察,并借助区块链实现信任数据的有效共享、不可篡改、公开可查.本文的主要贡献有3个方面:

1)针对分布式物联网内管理机构业务属性与信任特征各异,难以建立通用的信任管理方法,提出了机构间信任建立与管理,信任数据共享的方法.所提方法不依赖任何可信第三方与先验域间信任假设,信任建立与管理完全依赖各机构自行实施与维护.

2)针对物联网设备的域间信任需求,提出了分布式物联网内的设备间信任管理方法;根据物联网设备计算与存储能力差异较大的特点,为具有不同计算与存储能力的设备提供了差异化的信任管理选项.

3)实验模拟与分析表明,所提方案能够有效量化与衡量系统内实体的信任程度,且能够在保护历史信任数据不被恶意篡改的同时以较低的存储开销维护系统正常运行.

1 相关工作

信任作为一个主观抽象的概念[1],其定义涉及到不同研究领域的主体、客体、上下文环境等各种因素[2],没有一种模型能够将不同领域与不同上下文环境的信任概念有效完备地表达.目前存在着两种不同的信任机制研究:基于策略制定的机制与基于信誉的机制.基于策略制定的机制[3]采用类似于公钥基础设施的方式进行严格的授权管理,结点是否可信由数字证书严格定义,并通过逻辑程序设计限定结点权限,通常要求系统中存在可信的权威机构,不适用于分布式环境;基于信誉的机制[4-6]通过结点间的直接交互与其他结点对目标实体的建议与评价来计算与更新信任,理论上可以不依赖权威机构,但会产生大量的结点间通信.无论是基于策略制定的机制还是基于信誉的机制都是在抽象的网络层面对信任问题的研究,物联网设备的计算,存储与通信能力差异化程度高,异构物联网的域内通信与管理方式存在差异,使得以抽象网络环境为背景的信任研究无法直接应用在分布式物联网中.

现有的物联网信任研究大部分关注于解决单个物联网中的信任问题[7-12].Chen等人[7]借助模糊理论对物联网环境下的信任进行了建模,在提高物联网中路由效率的同时对其中的节点行为进行检测.Lize等人[8]将物联网信任分为传感器层、网络层与应用层,利用模糊集理论将多层的信息进行融合,计算出一个对象的全局声誉.Saied等人[9]尝试用多个函数对不同设备服务进行信任评价,提出了一种基于环境感知的信任管理系统.该方案从节点在过去的不同合作类型中的表现导出面对新任务时获得的信任值,这一过程依赖可信的信任管理机构完成.由于分布式物联网中的设备隶属与不同的所有者且不同所有者之间存在不完全可信的关系,而单个物联

网只有一个所有者且是完全可信的,因此为单个物联网设计的信任管理方法不能直接应用于分布式物联网中,否则会造成信任数据不收敛导致方案失效的情况.

部分学者对多物联网环境下的信任问题进行了研究. Liu 等人[13]提出了一种可验证的缓存前次交互摘要方法,构建了"现象可信-行为可信-节点可信-机构可信-授权可信"的环流,目的是解决物联网系统层次化的信任问题. 但是,该方案主要研究机构与阅读器之间的信任问题,对阅读器之间的信任问题未做详细讨论;另外,文章令不同的机构隶属于同一个信任管理机构,实际是在不同的域外建立了额外的可信第三方,这在现实中是难以实现的. Chen 等人[14]设计了一种自适应的社交物联网信任管理协议,一个具有社交属性的物联网设备可以自适应地选择最佳参数设置以适应设备所有者社交关系的变化. 然而,该方案对设备所有者之间的信任关系假设依然是独立于方案设计,先验进行的. 这实际是对域间的信任关系做了前提假设,忽略了跨域信任管理中的域间信任问题. Benkerrou 等人[15]提出了一种基于信用与诚实的物联网信任评估方法,文章将合作的双方称为服务请求者与合作者,服务请求者向域内的主节点发送服务请求,域内主节点选择潜在的合作者提供服务. 其中使用信用值描述合作者的受信任程度,诚实值描述请求者的受信任程度,通过将信用值与诚实值演算为统一的信任值,实现对物联网中对象信任的管理. 但是该方案重点关注了域内的信任问题,虽然提到了域间信任,但是却假设所有的域内主节点都是完全可信的,然而事实上很难在现实中找到符合这一假设的情况. 另外,该方案只给出了信任评价的逻辑表达式,却没有讨论具体的实现机制. Rafey 等人[16]提出了一种基于上下文的物联网社交信任模型,在信任计算过程中考虑到物联网节点之间的社会关系与交互的上下文环境. 每个节点基于直接交互和其他节点的推荐来计算目标节点的可信度. 然而,该方案依然假设域管理者之间的信任关系是方案开始前便存在的,并没有对这一信任关系进行深入研究;且方案中的每个节点维护一个对其他节点的认识,容易导致节点内存储的信任值随节点数量呈指数增长,使得节点信任不能有效传播,一个恶意节点可能依次对其他节点进行欺诈而不被察觉.

可见,现有的物联网信任问题研究部分因为只适用于单个物联网而无法应用于分布式物联网中,部分在解决分布式物联网信任问题时引入了权威第三方或域间信任假设,这实际上依然使得分布式物联网位于同一个逻辑域内,属于抽象意义上的域内信任问题. 然而,目前尚没有既不引入额外的可信第三方也不引入先验域间信任假设的分布式物联网信任管理机制研究,本文便为解决这一问题而展开.

2 系统架构与信任模型

2.1 系统架构

考虑一个去中心化的分布式物联网架构,在网络中,存在着许多的物联网设备(或称结点),结点之间通过覆盖网络协议(overlay network protocols)或底层网络协议(underlying network protocols)进行通信[14]. 每一个结点隶属于一个唯一的物联网管理者,每一个物联网管理者拥有许多不同的物联网设备. 物联网管理者与其所有的下属设备构成一个管理域. 设备可以在管理域内或管理域间进行合作以实现特定需求,域管理者可以在彼此之间进行合作. 为此,域管理者需要建立、评估与更新彼此间的信任关系;网络中的设备也需要动态地调整和更新与其他设备间的信任关系. 分布式物联网体系架构如图 1 所示.

图 1 中,$H(x)$表示域管理者服务器,$D(x,y)$表示 $H(x)$管理下的设备,$A(x)$表示管理域,$\varepsilon(x)$表示 $A(x)$内设备数量的最大编号. 形式化地,我们有 $x\in\{\mu\in N^*\mid 1\leqslant\mu\leqslant\alpha,\alpha\in N^*\}$,$y\in\{\omega\in N^*\mid 1\leqslant\omega\leqslant\varepsilon(x),\varepsilon(x)\in N^*\}$,其中 α 表示网络中管理域的个数. 图 1 中,$1\leqslant c_1\leqslant\alpha$,$1\leqslant c_2\leqslant\alpha$,$1\leqslant c_3\leqslant\alpha$;并省略了除 $A(c_1)$,$A(c_2)$,$A(c_3)$以外的其他管理域.

在系统架构中,我们假设域管理者与其下属的物联网设备间存在安全稳定的通信链路,由管理域各自选择协议与通信机制实现. 对于不同管理者的可信性及它们之间的信任关系,本文不作先验假设.

2.2 期望信用-风险模型

信任作为一个抽象的概念,不同研究对于这一概念有不同的体现方式. 本文采用期望信用(expected credit)与风险(risk)对一个实体的可信程度进行描述. 其中期望信用反映特定实体在某时间点被其他实体期望拥有的履行信用的能力,风险反映特定实体在过去的一段时间内信用表现的稳定性. 具体定义如下.

定义 1. $A(x)$的期望信用. 在不考虑历史信用数据的情况下,能够唯一标识 $A(x)$在某个特定时

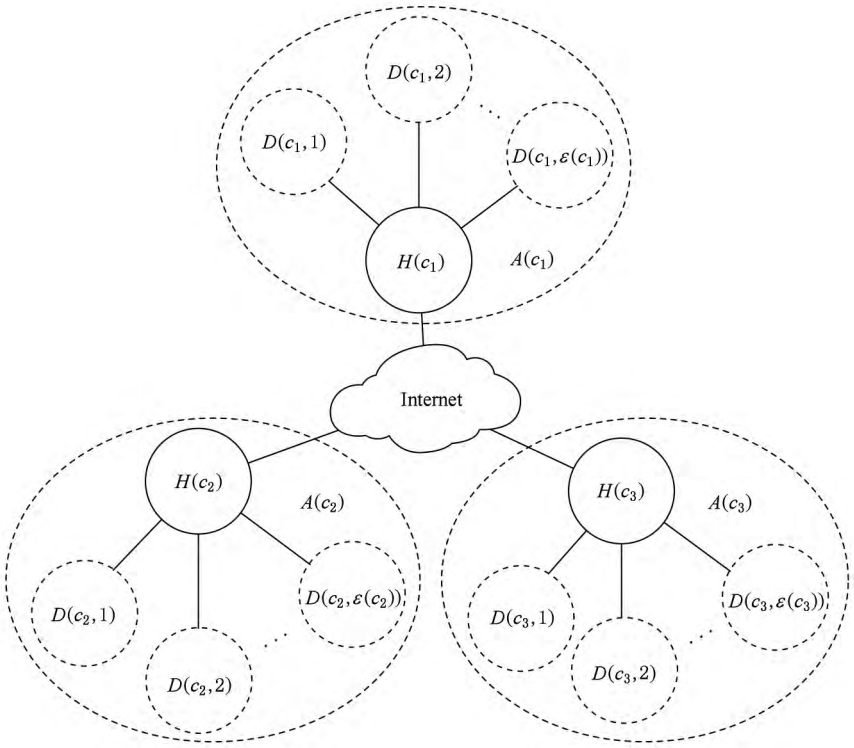


Fig. 1 Architecture of distributed Internet of things

图 1 分布式物联网系统架构

间点受其他实体 $A(x')$ 期望的能提供有效服务与合作的程度或概率,记为 $C_a(x,k)$;其中 $x,x'\in\{\mu\in N^*\mid 1\leqslant\mu\leqslant\alpha,\alpha\in N^*\}$,$k\in N^*$,且有 $x\neq x'$.

定义 2. $C_a(x,k)$ 的信用秤值 $S_a(x,k)$. 由一常数值 $I_a(x)$ 初始确定,并受到 $A(x')$ 的输出参数 $\delta(x,i)$ 调节的变量值,且满足:

$$S_a(x,k)=I_a(x)+\sum_{i=1}^{k-1}\delta(x,i),\tag{1}$$

$$C_a(x,k)=f(S_a(x,k)),\tag{2}$$

其中,f 为从 $\{S_a(x,k)\}$ 到 $\{C_a(x,k)\}$ 的映射函数;$x,x'\in\{\mu\in N^*\mid 1\leqslant\mu\leqslant\alpha,\alpha\in N^*\}$,$k\in N^*$,且有 $x\neq x'$;$\delta(x,i)\in\{-1,0,1\}$,表示对 $S_a(x,k)$ 的调节因子;$i\in N^*$.

定义 3. $D(x,y)$ 的信用值. 在不考虑历史信用数据的情况下,能够唯一标识 $D(x,y)$ 在某个特定时间点上的受 $D(x',y')$ 信任程度的值,记为 $C_d(x,y,k)$. 其中,$x,x'\in\{\mu\in N^*\mid 1\leqslant\mu\leqslant\alpha,\alpha\in N^*\}$,$y\in\{\omega\in N^*\mid 1\leqslant\omega\leqslant\varepsilon(x),\varepsilon(x)\in N^*\}$,$y'\in\{\omega\in N^*\mid 1\leqslant\omega\leqslant\varepsilon(x'),\varepsilon(x')\in N^*\}$,$k\in N^*$,且有 $\{x,y\}\neq\{x',y'\}$.

定义 4. $C_d(x,y,k)$ 的信用秤值 $S_d(x,y,k)$. 由一常数值 $I_d(x,y)$ 初始确定,并受到 $D(x',y')$ 的输出参数 $\delta(x,y,i)$ 调节的变量值,且满足:

$$S_d(x,y,k)=I_d(x,y)+\sum_{\lambda=1}^{k-1}\sum_{i=1}^{\tau(\lambda)}\delta(x,y,i),\tag{3}$$

$$C_d(x,y,k)=f(S_d(x,y,k)),\tag{4}$$

其中,f 为从 $\{S_d(x,y,k)\}$ 到 $\{C_d(x,y,k)\}$ 的映射函数;$\tau(\lambda)$ 为在某特定时间段内,一个特定的区域 $A(x_\lambda)$ 内所存在的 $D(x_\lambda,y_\lambda)$ 向其管理者服务器 $H(x_\lambda)$ 提交的对 $D(x,y)$ 的信用评价调节因子 $\delta(x,y,i)$ 的个数. 此处"特定时间段与特定区域"在第 3 节记账权选择问题中进行更详细的介绍;$x,x_\lambda\in\{\mu\in N^*\mid 1\leqslant\mu\leqslant\alpha,\alpha\in N^*\}$,$y\in\{\omega\in N^*\mid 1\leqslant\omega\leqslant\varepsilon(x),\varepsilon(x)\in N^*\}$,$y_\lambda\in\{\omega\in N^*\mid 1\leqslant\omega\leqslant\varepsilon(x_\lambda),\varepsilon(x_\lambda)\in N^*\}$,$k\in N^*$,且有 $\{x,y\}\neq\{x_\lambda,y_\lambda\}$;$\delta(x,y,i)\in\{-1,0,1\}$,表示对 $S_d(x,y,k)$ 的调节因子,$i\in N^*$,$\tau\in N^*$,$\lambda\in N^*$.

记 $C_a(x,\hat{k})$ 与 $C_d(x,y,\hat{k})$ 为在查询时刻系统能够提供的 $A(x)$ 与 $D(x,y)$ 的最新期望信用值,其中 $\hat{k}\in N^*$,但其表现力是有限的. 举例来说,如果存在一个实体,其期望信用 C 总是处在不断上升与下降的连续变化之中,那么尽管其在查询时刻的最新 C 值可能较高,但是翻看其期望信用历史记录就会对其是否具有当前 C 值所呈现的信用履行能力产生怀疑,故给出对参与者风险值的定义.

定义 5. $A(x)$ 的风险值. 能够衡量 $A(x)$ 在过去

一段信用记录历史中信用表现稳定性的度量. 将 $A(x)$ 的截止 $C_a(x,\hat{k})$ 的 r 个期望信用值纳入考虑所得到的风险值记为 $R_a(x,\hat{k},r)$:

$$R_a(x,\hat{k},r)=\sqrt{\frac{\sum_{k=\hat{k}-r+1}^{k}\left[C_a(x,k)-\overline{C_a(\hat{k},r)}\right]^2}{r-1}},\tag{5}$$

其中,$\hat{k}\in N^*$,表示纳入风险考察的期望信用 $C_a(x,k)$ 的截止序号;$r\in N^*$,表示纳入风险考察的 $C_a(x,k)$ 的数量;且:

$$\overline{C_a(\hat{k},r)}=\frac{\sum_{k=\hat{k}-r+1}^{k}C_a(x,k)}{r}.\tag{6}$$

定义 6. $D(x,y)$ 的风险值. 能够衡量 $D(x,y)$ 在过去一段信用记录历史中信用表现稳定性的度量. 将 $D(x,y)$ 的截止 $C_d(x,y,\hat{k})$ 的 r 个期望信用值纳入考虑得到的风险值记为 $R_d(x,y,\hat{k},r)$:

$$R_d(x,y,\hat{k},r)=\sqrt{\frac{\sum_{k=\hat{k}-r+1}^{k}\left[C_d(x,y,k)-\overline{C_d(\hat{k},r)}\right]^2}{r-1}},\tag{7}$$

其中 $\hat{k}\in N^*$,表示纳入风险考察的期望信用 $C_d(x,y,k)$ 的截止序号;$r\in N^*$,表示纳入风险考察的 $C_d(x,y,k)$ 的数量;且:

$$\overline{C_d(\hat{k},r)}=\frac{\sum_{k=\hat{k}-r+1}^{k}C_d(x,y,k)}{r}.\tag{8}$$

定义 5 与定义 6 将风险值看做是每个纳入风险考察的期望信用 C 与其均值的偏差的算数平均数,它反映了 $A(x')$ 在与 $A(x)$ 的合作过程中因为 $A(x)$ 的违约而导致损失的可能性. 风险值越高,表示在过去一段时间中该实体的信用表现越不稳定,意味着在将来的合作中该实体可能出现与其当前的期望信用 C 所呈现的信用水平相悖离的行为.

3 分布式物联网信任管理方法

3.1 信任管理载体

为了在跨管理域的参与者之间进行信任管理,采用区块链来实现分布式物联网中信任数据的共享与同步. 区块链技术是由 Nakamoto[17] 提出的能够在纯分布式环境中实现可信地数据共享与状态共识的分布式存储机制. 按照部署与应用场景的不同,区块链可分为 3 种:公有链、联盟链和私有链.

1) 公有链指区块链部署与运行在公网上,所有互联网用户只要下载软件或配置本地环境就能够接入的区块链系统;

2) 联盟链指区块链部署与运行在几个或多个不同机构或管理域之间,为不同机构或管理域的跨平台数据共享提供信任,属于受限准入型区块链;

3) 私有链指区块链部署与运行在单个机构或企业的内网中,只能由该机构内特定的服务器产生与维护,其他用户可以存储与查询的区块链. 私有链中的"单个机构或企业"可以是地理上的,也可以是逻辑上的.

本文采用联盟链实现分布式物联网中信任数据的共享与维护,主要利用区块链的分布式信任,不可篡改与公开透明特性. 其中分布式信任确保 $A(x)$ 之间对区块链副本唯一性与正确性的共识,不可篡改性确保已经写入区块链的数据不能被恶意伪造或修改,公开透明性确保区块链上的信息是开放的,所有参与者随时可查. 联盟链的优势在于能够在不同的 $A(x)$ 间进行信任管理并共享数据,而不需要可信第三方进行仲裁.

3.2 区块链结构

一个区块链可以表示为 $\{B_i\mid i\in N^*\}$,且对任何 $t\in\{\sigma\in N^*\mid 1\leqslant\sigma\leqslant i\}$,有 $B_t\supseteq\{\mathrm{Hash}(B_{t-1}),A(x_1),A(x_2),S_a(x_2,k-1),\delta(x_2,k-1),k,MR,TrI,\sigma(x_2),\mathrm{PK}(x_1),\sigma(x_1),C_d\{\cdot\}\}$,其中 $\mathrm{Hash}(B_{t-1})$ 表示对 B_t 在区块链中的上一个区块求 Hash 的值;$A(x_1)$ 表示区块生成者的唯一标识;$A(x_2)$ 表示受评域管理者的唯一标识;$S_a(x_2,k-1)=S_a(x_2,k-2)+\delta(x_2,k-2)$;$\delta(x_2,k-1)$ 为 $A(x_1)$ 对 $A(x_2)$ 给出的信用评价调节因子;k 为本次评价的 S_a 序号,在每次对 $A(x_2)$ 的评价中递进增长;MR 为 Merkle 树根;TrI 为一次商业交易行为中的交易信息,包含价格、交易时间等市场因素;$\sigma(x_2)=\mathrm{Sig}_{A(x_2)}(\mathrm{Hash}(TrI))$,$\mathrm{Sig}_{A(x_2)}(\cdot)$ 表示 $A(x_2)$ 的签名;$\mathrm{PK}(x_1)$ 表示 $A(x_1)$ 的公钥;$\sigma(x_1)=\mathrm{Sig}_{A(x_1)}(\mathrm{Hash}(\mathrm{Hash}(B_{t-1}),A(x_1),C_a(x_2,k),k,MR,TrI,\mathrm{PK}(x_1)))$;$C_d\{\cdot\}$ 表示 $D(x_1,y_i)$ 对与其合作的 $D(x',y')$ 进行信用评价调节之后的 $C_d(x',y',k')$ 构成的集合,其中 $D(x_1,y_i)\in\{D(x_1,y_i)\mid x_1,y_i,i\in N^*,1\leqslant x_1\leqslant\alpha,1\leqslant y_i\leqslant\varepsilon(x_1)\}$,$D(x',y')\in\{D(x',y')\mid x',y'\in N^*,1\leqslant x'\leqslant\alpha,1\leqslant y'\leqslant\varepsilon(x')\}$;$k'\in N^*$.

定义 $Head(B_t)\subseteq B_t$,$B_t-Head(B_t)=\{C_d\{\cdot\}\}$,称 $Head(B_t)$ 为区块头,$\{C_d\{\cdot\}\}$ 为区块体. 将 $C_d\{\cdot\}$ 组织成 Merkle 树[18-19] 的方式,Merkle 树根在区块

头中.举例来说,假设 $C_d\{\cdot\}=\{A,B,C,D,E\}$,其 Merkle 树上的 Hash 配对关系可表示为图 2 所示:

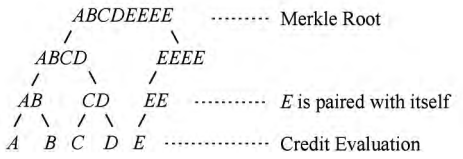


Fig. 2 Structure of Merkle Tree

图 2 Merkle 树构造

图 2 中,$A=C_d\{l_1,m_1,k_1\}$,$B=C_d\{l_2,m_2,k_2\}$,$C=C_d\{l_3,m_3,k_3\}$,$D=C_d\{l_4,m_4,k_4\}$,$E=C_d\{l_5,m_5,k_5\}$.$l_i\in\{l\in N^*\mid 1\leqslant l\leqslant\alpha\}$,$m_i\in\{m\in N^*\mid 1\leqslant m\leqslant\varepsilon(l)\}$,$k_i\in N^*$,$\{l_i,m_i\}\neq\{l_j,m_j\}$,$i,j\in\{\nu\in N^*\mid 1\leqslant\nu\leqslant 5\}$且 $i\neq j$.

应当指出,上述对 B_t 的描述只给出了其上与本文主旨有关的重要字段,为了在不影响关键信息描述的情况下简化表达,对于如 B_t 在区块链中的高度 t 值、时间戳等字段则不作赘述.

3.3 记账权选择

在区块链技术中,共识机制问题指如何在系统中不同节点上维护其历史数据与状态一致性;记账权选择问题要求提供一种机制,确定区块的发布权,即确定哪个节点可以打包并发布现有区块链中的下一区块.公有链中,由于总是通过记账权选择的竞争实现共识机制,二者之间存在很强的关联性,甚至在很大程度上可以被视为同一个问题,故现有成熟的公有链共识机制常依赖于记账权选择策略的设计[17,20].联盟链与私有链中,由于参与节点较公有链中少很多,一些在区块链这一概念提出前便已存在的共识机制研究[21-27]可直接应用,因此将记账权选择与共识机制分别讨论.联盟链中记账权的选择具有较大的自主性,一般可根据应用场景与实际需求设计与选择合适的方法来确定记账权.

本文中对管理域在语义层面的属性与功能不作特定的假设.事实上,管理域可能是拥有大量传感器与智能设备,需要在战场上彼此合作的军事单位;或是供应链中拥有大量智能工业与物流设备,期望提高合作效率,维护商业信誉的企业.在第 4 节实验模拟与分析部分,我们将采用供应链作为场景去考察本文所提信任管理方法的效果.此处对记账权选择机制给出抽象的,一般性的设计描述.

情形 1. 定义函数

$$f(A(x_i),A(x_j))=\begin{cases}0, & \neg\ \exists\Gamma_{i,j}\\ 1, & \exists\Gamma_{i,j}\end{cases},$$

规定当且仅当 $f(A(x_i),A(x_j))=1$ 时,$H(x_i)$ 获得且仅获得一次产生一个新区块 B_c 并将其添加到区块链末尾的权利,其中现有区块链为 $\{B_1,B_2,\cdots,B_{c-1}\}$.$\Gamma_{i,j}$ 表示 $H(x_i)$ 与 $H(x_j)$ 之间的某一合作过程且满足 $\Gamma_{i,j}\neq\Gamma_{j,i}$.

情形 2. 在特定的场景与环境下,系统中任何 $H(x_i)$ 与 $H(x_j)$ 之间较长时间没有合作 $\Gamma_{i,j}$ 出现时,就会导致 $D(x_i,y_m)$ 提交的信用数据在 $H(x_i)$ 中大量积存,无法共享到 $H(x_j)$,使存在信用请求需求的 $D(x_j,y_n)$ 无法获得最新的信用评价,同时造成 $H(x_i)$ 内存资源的消耗,对服务器的可用性造成潜在的影响.

为此,令每个 $H(x_i)$ 维护一个固定大小的内存空间,记为 $Pool(x_i)$.$H(x_i)$ 在区块链上查询 $C_d(x_j,y_n,\hat{k})$ 并计算:$S_d(x_j,y_n,\hat{k})=f^{-1}(C_d(x_j,y_n,\hat{k}))$.随后,$H(x_i)$ 不断接收其下属设备 $D(x_i,y_m)$ 的信用评价调节请求 $\delta(x_j,y_n,l)$ 来更新 $S_d(x_j,y_n,\tilde{k})$,其中 $\tilde{k}=\hat{k}+1$,$S_d(x_j,y_n,\tilde{k})=S_d(x_j,y_n,\hat{k})+\sum_{l=1}^{\tau(i)}\delta(x_j,y_n,l)$.$H(x_i)$ 将 $S_d(x_j,y_n,\tilde{k})$ 缓存在 $Pool(x_i)$ 中,我们记 $Pool(x_i)$ 中能够容纳的最大 $S_d(x_j,y_n,\tilde{k})$ 的个数为 $Max(Pool(x_i))$,并要求所有 $H(x_i)$ 维护相同的 $Max(Pool(x_i))$ 以确保公平.当 $Pool(x_i)$ 满足 $\theta\leqslant\frac{Available(Pool(x_i))}{Max(Pool(x_i))}\leqslant 1$ 时,$H(x_i)$ 选择随机时间打包并发布包含 $\{C_d(x_j^1,y_n^1,\tilde{k}),C_d(x_j^2,y_n^2,\tilde{k}),\cdots,C_d(x_j^z,y_n^z,\tilde{k})\}$ 的新区块.其中 $Available(Pool(x_i))$ 表示当前 $H(x_i)$ 已经接收的 $S_d(x_j,y_n,\tilde{k})$ 的个数,$\theta\in\{\lambda_1\in\mathrm{R}\mid 0<\lambda_1\leqslant 1\}$,$\tau(x_i)\in\{\lambda_2\in N^*\mid 0\leqslant\lambda_2\leqslant Max(Pool(x_i))\}$,$l=Available(Pool(x_i))$;$\{C_d(x_j^1,y_n^1,\tilde{k}),C_d(x_j^2,y_n^2,\tilde{k}),\cdots,C_d(x_j^c,y_n^c,\tilde{k})\}$ 为待发布的 $C_d(x_j,y_n,\tilde{k})$ 构成的集合,其中 $\tilde{k}_i=\hat{k}_i+1$,$z\in\{\lambda_3\in N^*\mid 1\leqslant\lambda_3\leqslant\sum_{m=1}^{\alpha}\varepsilon(m)\}$.

3.4 区块发布与接收

假设 $H(x_i)$ 在特定时间满足 3.3 节中指出的条件,需要打包并发布区块 B_t,此时,对于 3.3 节中情形 1 与情形 2,$Head(B_t)$ 的填写将有差异.此节中情形 1 与情形 2 分别对应 3.3 节中情形 1 与情形 2.

情形 1. $f(A(x_i),A(x_j))=1$ 时,$A(x_i)$ 需要对 $A(x_j)$ 在合作 $\Gamma_{i,j}$ 中的信用表现作出评价,即给出 $\delta(x_j,k-1)$,并通过查询区块链计算 $S_a(x_j,k-1)$,其中 $S_a(x_j,k-1)=S_a(x_j,k-2)+\delta(x_j,k-2)$.然后将与这一过程有关的字段,具体包括 $A(x_j)$,

$S_a(x_j,k-1)$,$\delta(x_j,k-1)$,k,TrI,$\sigma(x_j)$,填入 $Head(B_t)$中.其中 $\sigma(x_j)$由 $A(x_j)$提供,本文不对这一过程作出假设.

情形 2. 此时没有合作 $\Gamma_{i,j}$发生,当 $Pool(x_i)$满足 $\theta\leqslant\frac{Available(Pool(x_i))}{Max(Pool(x_i))}\leqslant 1$ 时,$A(x_i)$随机选择时间打包并发布 B_t,并将与 $\Gamma_{i,j}$有关的字段$A(x_j)$,$S_a(x_j,k-1)$,$\delta(x_j,k-1)$,k,TrI,$\sigma(x_j)$全部置为 ρ,一般可取 $\rho=0$.

由于 $H(x_i)$与 $H(x_j)$之间通过因特网通信,因此在区块数据的发布过程中,可能会遇到网络环境不稳定导致的数据包丢失等问题,这被称作区块链中的节点发生了拜占庭故障.拜占庭故障可以理解为试图达成特定共识的网络节点当中存在的个别节点因为任意原因篡改或隐藏真实信息的行为,发生拜占庭故障的节点也被称为拜占庭节点.自从 Lamport 提出拜占庭将军问题以来[21],对于这一问题的研究不断深入[28],已经产生了一些被广泛接受与应用的分布式一致性算法[22-27].基于此,本文对于区块链上新区块的发布过程采用模块化的设计,允许采用 Paxos[22-24],PBFT[25],Raft[27] 等算法实现.这种模块化的方式使得对于节点间共识机制与算法的研究与在区块链上进行顶层设计的研究相互独立,也是当前联盟链中常见的设计模式[29].

一旦 $H(x_i)$通过模块化的共识机制成功发布了区块 B_t,网络上的其他所有 $H(x_k)$接收 B_t 并将其添加进 $\{B_1,B_2,\cdots,B_{t-1}\}$,随后 $\{B_1,B_2,\cdots,B_{t-1},B_t\}$便成为系统中受非拜占庭节点认可的区块链.

3.5 信任评价

3.5.1 域管理者间评价

$A(x_i)$与 $A(x_j)$之间通过区块链进行信用评价,假设过程 $\Gamma_{i,j}$发生,则 $H(x_i)$在区块链上查询并获取 $S_a(x_j,k-2)$,$\delta(x_j,k-2)$与 $k-1$ 值,计算 $S_a(x_j,k-1)=S_a(x_j,k-2)+\delta(x_j,k-2)$.随后 $H(x_i)$接收由域管理者给出的信用评价调节因子 $\delta(x_j,k-1)$,并将 $S_a(x_j,k-1)$与 $\delta(x_j,k-1)$一起写进 $Head(B_t)$完成信用评价.

在 $Head(B_t)$中包括了 TrI 与 $\sigma(x_j)$字段以对历史进行背书并提供审查需求.TrI 描述了 $\Gamma_{i,j}$过程中的必要语义信息以及为什么对本次过程给出 $\delta(x_j,k-1)$的评价因子的描述信息等;$\sigma(x_j)=Sig_{A(x_j)}(\mathrm{Hash}(TrI))$,是由 $A(x_i)$向 $A(x_j)$出示并展示 TrI 后,经 $A(x_j)$确认并提供的对 TrI 的数字签名.提供 $\sigma(x_j)$后,$A(x_j)$将无法否认 $\Gamma_{i,j}$及其中的必要信息.

假设过程 $\Gamma_{i,j}$ 发生,$A(x_i)$对 $A(x_j)$进行评价,评价过程中 $H(x_i)$上的操作可表为算法 1 所示.

算法 1. 域管理者间评价.

执行者:$H(x_i)$;

输入:TrI,$\delta(x_j,k-1)$;

输出:B_t.

① 接收到 $\Gamma_{i,j}$发生的信息;

② 接收到与 $\Gamma_{i,j}$有关,$Head(B_t)$中要求的信息;

③ 在 $\{B_c\mid c\in N^*,t\in N^*,1\leqslant c\leqslant t-1\}$上查询并获取 $S_a(x_j,k-2)$,$\delta(x_j,k-2)$,与 $k-1$ 值;

④ $S_a(x_j,k-1)\leftarrow S_a(x_j,k-2)+\delta(x_j,k-2)$;

⑤ 接收 $\delta(x_j,k-1)$;

⑥ 将 $S_a(x_j,k-1)$与 $\delta(x_j,k-1)$写进 $Head(B_t)$;

⑦ 获取或计算 $Head(B_t)$中其他字段值,写进 $Head(B_t)$;

⑧ 将 $\{Head(B_t),C_d\{\cdot\}\}$作为新区块 B_t,借助模块化的共识算法发布 B_t,算法结束.

算法 1 的时间复杂度为 $O(t)$,空间复杂度为 $O(1)$,按照既定步骤执行后产生唯一输出 B_t,作为最新的区块添加到区块链上.

3.5.2 设备间评价

$D(x_i,y_m)$与 $D(x_j,y_n)$进行通信合作之后,$D(x_i,y_m)$与 $D(x_j,y_n)$可以选择对彼此在合作中的表现进行评价.假设 $D(x_i,y_m)$选择对 $D(x_j,y_n)$进行评价,它只需要作出自己的评价决定,并将信用评价调节因子 $\delta(x_j,y_n,i)$发送到 $H(x_i)$.$H(x_i)$在收到 $\delta(x_j,y_n,l)$后首先在 $Pool(x_i)$查询 $S_d(x_j,y_n,\tilde{k})$,如果找到则将其值更新为 $S_d(x_j,y_n,\tilde{k})+\delta(x_j,y_n,i)$;如果无法在 $Pool(x_i)$中查询到 $S_d(x_j,y_n,\tilde{k})$,则在 $\{B_c\mid c\in N^*,t\in N^*,1\leqslant c\leqslant t-1\}$上查询 $S_d(x_j,y_n,\hat{k})$,并计算 $S_d(x_j,y_n,\tilde{k})=S_d(x_j,y_n,\hat{k})+\delta(x_j,y_n,i)$,然后将 $S_d(x_j,y_n,\tilde{k})$存入 $Pool(x_i)$中;如果无法在 $Pool(x_i)$与 $\{B_c\mid c\in N^*,t\in N^*,1\leqslant c\leqslant t-1\}$中查询得到 $S_d(x_j,y_n,\tilde{k})$或 $S_d(x_j,y_n,\hat{k})$,则产生 $S_d(x_j,y_n,1)=I_d(x,y)+\delta(x_j,y_n,i)$,然后将 $S_d(x_j,y_n,1)$ 存入 $Pool(x_i)$中.信用评价过程中$D(x_i,y_m)$所作的操作可由算法 2 描述.

算法 2. $D(x_i,y_m)$进行信任评价($D(x_i,y_m)$方面).

执行者:$D(x_i,y_m)$;

输入:无;

输出:$\delta(x_j,y_n,i)$.

① 向 $D(x_j,y_n)$发出合作请求;

② 若未得到响应或请求被拒绝,转③;否则,转⑥;

③ 若选择进行评价,转④;否则,转⑫;

④ 生成 $\delta(x_j,y_n,i)$;

⑤ 将 $\delta(x_j,y_n,i)$发送到 $H(x_i)$,转⑫;

⑥ 与 $D(x_j,y_n)$进行合作;

⑦ 合作过程;

⑧ 合作结束;

⑨ 选择是否进行评价,若是,转⑩;若否,转⑫;

⑩ 生成 $\delta(x_j,y_n,i)$;

⑪ 将 $\delta(x_j,y_n,i)$发送到 $H(x_i)$;

⑫ 算法结束.

算法 2 的时间复杂度为 $O(1)$,空间复杂度为 $O(1)$,按照既定步骤执行后产生唯一输出 $\delta(x_j,y_n,i)$. 通过将 $\delta(x_j,y_n,i)$发送到 $H(x_i)$完成信任评价.

服务器 $H(x_i)$在此过程中所做的工作可由算法 3 描述.

算法 3. $D(x_i,y_m)$进行信任评价($H(x_i)$方面).

执行者:$H(x_i)$;

输入:$\delta(x_j,y_n,j)$;

输出:$S_d(x_j,y_n,\tilde{k})$.

① 在存储空间中维护 $Pool(x_i)$与$\{B_c\mid c\in N^*,t\in N^*,1\leqslant c\leqslant t-1\}$;

② 收到 $D(x_i,y_m)$发送的 $\delta(x_j,y_n,j)$;

③ 在$Pool(x_i)$中查询 $S_d(x_j,y_n,\tilde{k})$,若成功,转④;否则,转⑤;

④ $S_d(x_j,y_n,\tilde{k})\leftarrow S_d(x_j,y_n,\tilde{k})+\delta(x_j,y_n,j)$,转⑨;

⑤ 在$\{B_c\mid c\in N^*,t\in N^*,1\leqslant c\leqslant t-1\}$上查询 $S_d(x_j,y_n,\hat{k})$,若成功,转⑥;否则,转⑦;

⑥ $S_d(x_j,y_n,\tilde{k})\leftarrow S_d(x_j,y_n,\hat{k})+\delta(x_j,y_n,j)$,转⑨;

⑦ $S_d(x_j,y_n,1)\leftarrow I_d(x,y)+\delta(x_j,y_n,j)$;

⑧ $S_d(x_j,y_n,\tilde{k})\leftarrow S_d(x_j,y_n,1)$;

⑨ 将$S_d(x_j,y_n,\tilde{k})$放入 $Pool(x_i)$中;

⑩ 算法结束.

算法 3 的时间复杂度为 $O(t)$,空间复杂度为 $O(1)$,按照既定步骤执行后产生唯一输出 $S_d(x_j,y_n,\tilde{k})$,并将其存入缓冲区 $Pool(x_i)$中等待发布.

需要指出的是,$D(x_i,y_m)$与 $D(x_j,y_n)$进行合作时,$D(x_i,y_m)$属于 $A(x_i)$而与 $H(x_i)$通信,$D(x_j,y_n)$属于 $A(x_j)$而与 $H(x_j)$通信,且$\{x_i,y_m\}\neq\{x_j,y_n\}$是可能的. 即属于不同管理域的设备有可能在地理上接近而产生合作,同一管理域的设备也有可能在地理上远离而无法合作;设备之间的合作可能在管理域之间进行.

设有服务器 $H(x_i)$,它所参与到的域间信任评价、设备间信任评价以及区块的生成与打包过程可以综合表示为算法 4 所示.

算法 4. $H(x_i)$的工作流程.

执行者:$H(x_i)$;

输入:$TrI,\delta(x_j,k-1),\delta(x_j,y_n,j)$;

输出:B_t.

① 在存储空间中维护 $Pool(x_i)$与$\{B_c\mid c\in N^*,t\in N^*,1\leqslant c\leqslant t-1\}$;

② 等待并接收 $D(x_i,y_m)$发送的 $\delta(x_j,y_n,j)$;

③ 对收到的 $\delta(x_j,y_n,j)$,使用算法 3 计算 $S_d(x_j,y_n,\tilde{k})$,并放入 $Pool(x_i)$中;

④ 检查是否收到 $\Gamma_{i,j}$发生指令,若是,转⑤;若否,转⑥;

⑤ 使用算法 1 的过程输出 B_t,转⑩;

⑥ 检查 $Pool(x_i)$是否满足

$$\theta\leqslant\frac{Available(Pool(x_i))}{Max(Pool(x_i))}\leqslant 1,$$

若是,转⑦;若否,转②;

⑦ 选择是否打包并发布 B_t,若是,转⑧;若否,转②;

⑧ 对$Pool(x_i)$中 $S_d(x_j,y_n,\tilde{k})$计算 $C_d(x_j,y_n,\tilde{k})=f(S_d(x_j,y_n,\tilde{k}))$,并将 $C_d(x_j,y_n,\tilde{k})$以 Merkle 树的形式组织成 MR 与 $C_d\{\cdot\}$. 按 3.4 节情形 2 所述填写 $Head(B_t)$中的各字段,打包为 B_t;

⑨ 按第 3.4 节所述发布 B_t;

⑩ 算法结束.

算法 4 的时间复杂度为 $O(t\times Max(Pool(x_i)))$,空间复杂度为 $O(1)$,按照既定步骤执行后产生唯一输出 B_t,作为新区块发布到区块链上.

3.6 信任评估

3.6.1 域管理者间评估

假设 $A(x_i)$试图寻找合作伙伴,$\Phi_1=\{A(x_j)\mid 1\leqslant x_j\leqslant\alpha,x_j\in N^*,j\in N^*\}$为候选集合. $A(x_i)$将在 Φ_1 中选择期望信用最高,合作风险最低的域作为合作伙伴.

此时 $A(x_i)$查询$\{B_c\mid c\in N^*,t\in N^*,1\leqslant c\leqslant t-1\}$,获取到 $\Phi_2=\{S_a(x_j,\mu),\delta(x_j,\mu)\mid A(x_j)\in\Phi_1,t-r-1\leqslant\mu\leqslant t-2,\mu\in N^*\}$并计算:

$$\hat{k}=k-1, \tag{9}$$

$$S_a(x_j,\hat{k})=S_a(x_j,k-2)+\delta(x_j,k-2), \tag{10}$$

$$C_a(x_j,\hat{k})=f(S_a(x_j,\hat{k})). \tag{11}$$

求出每一个合作伙伴当前最新的信用值 C_a.

对每一个 $A(x_j)$,根据式(5)计算其在参数 r 下的风险值 $R_a(x_j,\hat{k},r)$,然后计算:

$$\frac{1}{E_a(x_j,\hat{k},r)}=\frac{1}{C_a(x_j,\hat{k})}+R_a(x_j,\hat{k},r), \quad (12)$$

$$E_a(x_j,\hat{k},r)=\frac{C_a(x_j,\hat{k})}{1+C_a(x_j,\hat{k})\times R_a(x_j,\hat{k},r)}. \quad (13)$$

将 $E_a(x_j,\hat{k},r)$ 作为对 $A(x_j)$ 进行信任评价的综合打分. 从式(12)与式(13)可以看出,E_a 等于 C_a 与 $1/R_a$ 的调和平均值. 与算数平均和几何平均相比,调和平均更重视较小值[30]. 由于 $C_a\leqslant 1/R_a$,因此采用调和平均的方法计算 E_a,对于 C_a 的重视度更高.

随后 $A(x_i)$ 选择 $A(x_j)$ 作为合作伙伴,其中 $E_a(x_j,\hat{k},r)=\max(\{E_a(x_j,\hat{k},r)\mid A(x_j)\in\Phi_1,\hat{k}\in N^*,r\in N^*\})$.

3.6.2 设备间评估

由于物联网设备种类广泛,我们对不同的设备按照其自身特点与任务属性设计不同的查询方式,分别列为选项 1 与选项 2.

选项 1. 对于计算能力较弱的设备或低功耗设备以及重要性较低的任务,为了节省设备的计算开销,可令其不考虑设备风险 R_d,仅考虑期望信用 C_d. 设 $D(x_i,y_m)$ 试图寻找合作设备,$\Phi_3=\{D(x_j,y_n)\mid 1\leqslant x_j\leqslant\alpha,1\leqslant y_n\leqslant\varepsilon(x_j),x_j\in N^*,y_n\in N^*\}$ 为候选集合,$D(x_i,y_m)$ 选择信用值 C_d 最高的设备作为合作伙伴. 此时,$D(x_i,y_m)$ 查询 $\{B_c\mid c\in N^*,t\in N^*,1\leqslant c\leqslant t-1\}$,获得 $\Phi_4=\{C_d(x_j,y_n,\hat{k})\mid D(x_j,y_n)\in\Phi_3\}$,并令:

$$E_d(x_j,y_n,\hat{k})=C_d(x_j,y_n,\hat{k}) \quad (14)$$

即可. 随后 $D(x_i,y_m)$ 选择具有最大 $E_d(x_j,y_n,\hat{k})$ 的 $D(x_j,y_n)$ 作为合作伙伴.

选项 2. 大部分物联网设备能够完成一定规模的数学运算,具有较强的计算与存储能力. 此时应当以选项 2 作为信任值 E_d 的产生方式.

假设 $D(x_i,y_m)$ 试图寻找合作伙伴,Φ_3 为候选集合,$D(x_i,y_m)$ 在 Φ_3 中选择期望信用最高,合作风险最低的设备作为合作设备.

$D(x_i,y_m)$ 查询 $\{B_c\mid c\in N^*,t\in N^*,1\leqslant c\leqslant t-1\}$,获得 $\Phi_5=\{C_d(x_j,y_n,\mu)\mid D(x_j,y_n)\in\Phi_3,t-r-1\leqslant\mu\leqslant t-2,\mu\in N^*\}$,并根据式(7)计算 $R_d(x_j,y_n,\hat{k},r)$.

随后计算:

$$\frac{1}{E_d(x_j,y_n,\hat{k},r)}=\frac{1}{C_d(x_j,y_n,\hat{k})}+R_d(x_j,y_n,\hat{k},r), \quad (15)$$

$$E_d(x_j,y_n,\hat{k},r)=\frac{C_d(x_j,y_n,\hat{k})}{1+C_d(x_j,y_n,\hat{k})\times R_d(x_j,y_n,\hat{k},r)}. \quad (16)$$

将 $E_d(x_j,y_n,\hat{k},r)$ 作为对 $D(x_j,y_n)$ 进行信任评价的综合打分. 与 E_a 相类似,E_d 为 C_d 与 $1/R_d$ 的调和均值,以在评估中对 C_d 给予更高程度的重视.

随后 $D(x_i,y_m)$ 选择 $D(x_j,y_n)$ 作为合作伙伴,其中 $E_d(x_j,y_n,\hat{k},r)=\max(\{E_d(x_j,y_n,\hat{k},r)\mid D(x_j,y_n)\in\Phi_3,\hat{k}\in N^*,r\in N^*\})$.

需要指出的是 $D(x_i,y_m)$ 查询 $\{B_c\mid c\in N^*,t\in N^*,1\leqslant c\leqslant t-1\}$ 的过程可以通过询问服务器直接获得 Φ_4,也可以先将 $\{B_c\mid c\in N^*,t\in N^*,1\leqslant c\leqslant t-1\}$ 存储在本地,然后查询获得 Φ_4. 前者适用于设备存储空间较小的情况,后者适用于设备的存储空间较大的情况.

4 实验模拟与分析

为了检验所提方案的有效性与实用性,本文从期望信用-风险表现、共识机制安全性、存储开销、信任评估效果 4 个方面进行了实验与分析. 本文实验均采用 MATLAB 编程模拟,实验平台为 3.4 GHz Intel Core i7-6700 CPU,8 GB RAM,操作系统为 Windows 7-64 位.

4.1 期望信用-风险表现

在 2.2 节中提出了信任管理的期望信用-风险模型,并指出如果只考虑 $H(x)$ 与 $D(x,y)$ 在查询时刻的期望信用 $C_a(x,\hat{k})$ 与 $C_d(x,y,\hat{k})$. 将无法消除选择与之合作后受到损失的风险,因此需要引入对风险的考虑. 假设实体 A 与实体 B 作为我们的候选合作伙伴,A 在一段信任评价历史中的期望信用变异度较小;B 在同样长度的评价历史中的期望信用变异度较大. 那么若 A 与 B 在当前时刻的期望信用大致相同,作为理性的参与者,我们应该选择 A 作为合作伙伴,因为我们更有理由相信 A 会像它的期望信用所表现的那样参与合作.

上述例子中 A 对应低风险参与者,B 对应高风险参与者. 我们利用 MATLAB 产生了 200 次信用评价数据,分别模拟在进行 100 次评价的情况下,一个具有较低风险的参与者 $H(x_1)$ 与一个具有较高风险的参与者 $H(x_2)$ 的信用表现,实验中选取 $f(S_a(x,k))=\frac{1}{1+e^{-S_a(x,k)}}$,即使得 C_a 对于 S_a 的变化

具有一定的容忍度,通过分配合适的 I_a,使得在持续调节 S_a 的过程中满足 C_a 在收到 δ 较少时变化幅度较小,随着收到 δ 数量的增大,变化幅度逐渐增大,如果 S_a 继续在相同方向上调节,C_a 受 δ 的影响将重新变小且能够持续保持;实验中令 $I_a(x_1)=0$,$I_a(x_2)=0$.

$H(x_1)$与 $H(x_2)$的信用秤值、信用评价调节因子值、期望信用值以及风险值如图 3、图 4 所示:

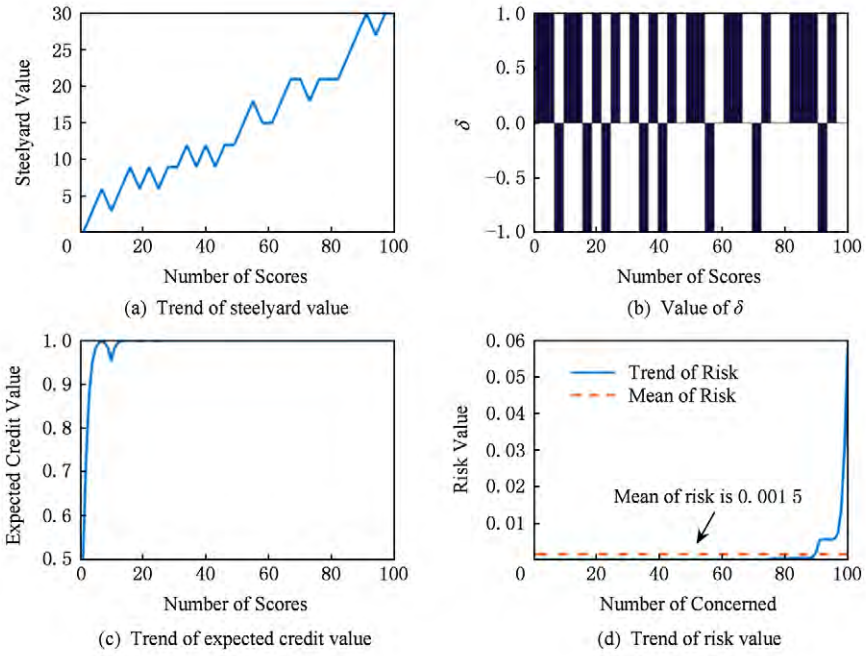


Fig. 3 Performance of participant with Low-Risk

图 3 低风险参与者期望信用-风险表现

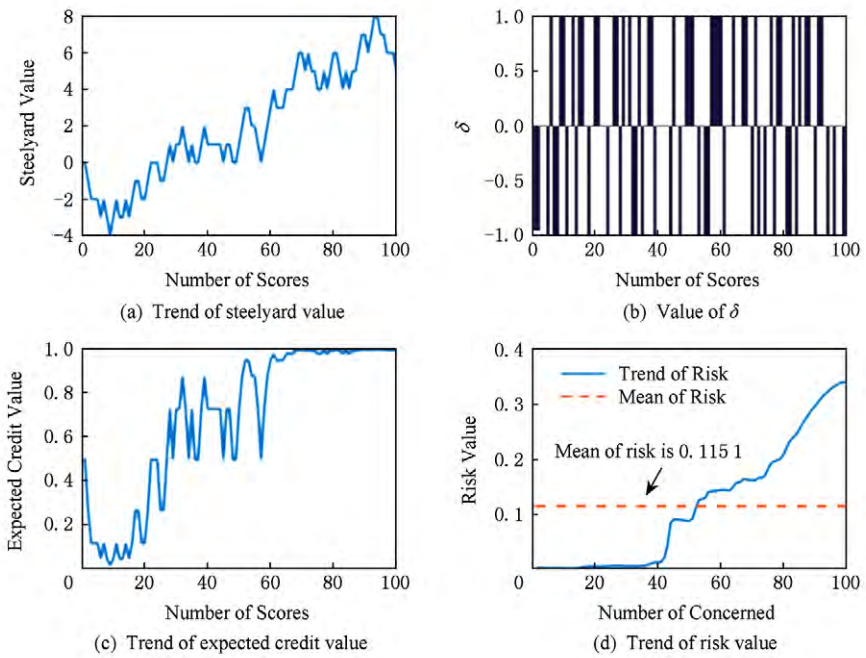


Fig. 4 Performance of participant with High-Risk

图 4 高风险参与者期望信用-风险表现

从图 3 与图 4 中可以看出,尽管当 $\hat{k}=100$ 时,$C_a(x_1,\hat{k})$与 $C_a(x_2,\hat{k})$十分接近,都大致为 1,但它们的风险值 $R_a(x_1,\hat{k},r)$,$R_a(x_2,\hat{k},r)$的均值在当 $r\in\{\nu\,|\,2\leqslant\nu\leqslant100\}$时相差了 76.8 倍. 图 3 中,$H(x_1)$的风险值在当 $r>90$ 以后有了显著的提升,这是因为当纳入风险考虑的信用值逐渐变多之后,$H(x_1)$在加

入系统早期期望信用快速增长的影响在风险中反映了出来. 尽管如此,当 $r=100$ 时,$H(x_1)$的风险值依然非常低的,只有 0.058;而当 $r=100$ 时,$H(x_2)$的风险值则为 0.340.

另外,$H(x_1)$的期望信用变化趋势较为稳定,其风险值在 r 的不同取值下的均值很低;而 $H(x_2)$的期望信用变化趋势则波动较大,其风险值的均值也较大. 低风险与高风险参与者期望信用变化趋势与风险均值的对比图如图 5 所示:

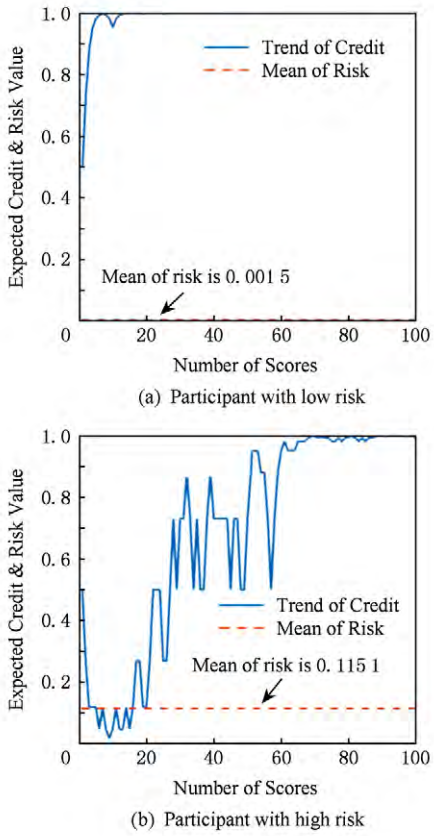


Fig. 5 Comparison between participants with high and low risk

图 5 高低风险参与者对比

以上是对 $H(x_1)$与 $H(x_2)$所作的讨论,对于设备之间的信用风险表现,情形是类似的.

4.2 记账权选择与共识机制安全性

我们在 3.3 节中描述了本方案的记账权选择策略,与当前区块链中最常用的 PoW 共识机制采用的记账权选择方式(竞争破解 Hash 值[17])相比,我们的方案在分布式物联网中更加安全也更加高效. 众所周知,PoW 机制面临 51%攻击[31]问题,这一缺陷使得 PoW 机制只适用于公有链的场景. 因为 PoW 的安全性基于网络中没有节点或组织能够获得超过全网 50%的总算力. 在公有链中,由于节点众多,全网总算力十分庞大,这一假设是合理的;而在联盟链中,参与记账的服务器数量相比公有链中节点数量少很多,且分布式物联网中的不同机构完全可能在所部署服务器的算力上存在较大差异. 因此当联盟链中有机构部署的服务器算力远超其他机构服务器,或是少数机构间形成 Cartel 组织时,将可能出现个别几台,甚至单台服务器的计算能力超过网络算力 50%的情况,这会造成 PoW 区块链的信任基础遭到破坏. 图 6 中我们模拟了如果在分布式物联网的联盟链中使用 PoW 机制,系统内的恶意域管理者为了篡改信任历史数据所发起的 51%攻击的大致过程.

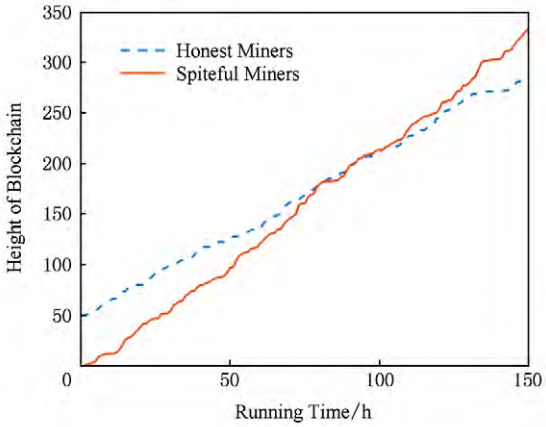


Fig. 6 Example of 51% attack

图 6 51%攻击示例

图 6 中,我们采用了比特币区块链所遵循的大约每 10 min 产生一个新区块的策略,并为攻击者分配了全网 60%的算力,诚实的用户则占据了剩下 40%的算力. 从图 6 中可以看出,当诚实的用户具有初始 50 个区块的优势时,占据全网 60%算力的攻击者可以在大约 60 h 内追赶上诚实用户,并在随后产生比诚实用户所维护的更长的链以欺骗其他用户. 因此,在联盟链中,PoW 机制是不应该被采用的.

本文采用的记账权选择方式是当某一特定过程发生或符合某一特定条件时由指定的域管理者服务器借助模块化的共识机制产生新区块,区块链的不可篡改性由模块化共识机制维护. 事实上,由于 PoW 采用长链共识,而 PBFT,RAFT 等可替换模块化共识机制采用最终共识,即服务器在区块链初次写入后不会因外部条件改变而修改原有数据,因此保证了区块链的不可伪造与篡改.

4.3 存储开销

与传统的比特币区块链相比,本文提出的记账权选择策略具有更小的存储开销,使得系统中的服

务器能够以更低的成本在更长一段时间内维护系统的正常运行.根据3.2节区块结构,可为$Head(B_t)$分配字段长度如表1所示:

Table 1 The Length of Fields in a Block

表1 区块字段长度

Field	Field Length/B
$\mathrm{Hash}(B_{t-1})$	32
$A(x_1)$	4
$A(x_2)$	4
$S_a(x_2,k-1)$	4
$\delta(x_2,k-1)$	1
k	4
MR	32
TrI	256
$\sigma(x_2)$	32
$PK(x_1)$	256
$\sigma(x_1)$	32
Total	657

令每个C_d占4 B,则区块中的$C_d\{\cdot\}$最多可占$4\times Max(Pool(x))$字节.假设$Max(Pool(x))=100$且$\theta=1$,则$C_d\{\cdot\}$最多可占存储空间为400 B.区块B_t所占存储空间最大为1 057 B,只比1 KB稍微多一点.本文方案中区块最大存储开销与$Max(Pool(x))$之间的对应关系如表2所示:

Table 2 Maximum Storage Overhead of a Block

表2 区块最大存储开销

$Max(Pool(x))$	Maximum Block Size/B
100	1 057
500	2 657
1000	4 657
2000	8 657
3000	12 657
10000	40 657
50000	200 657
100000	400 657

从表2中可以看出,当$Max(Pool(x))=100\,000$时,区块B_t的最大存储开销是0.38 MB.而比特币系统中每个区块最大为1 MB,远大于我们方案中单个区块的存储开销.

考察本文方案与比特币在区块产生速率上的差异.由于本方案中区块产生条件与3.3节记账权选择机制相关,其中的$\Gamma_{i,j}$在不同的语境下可定义为不同语义.本文以供应链场景作为实验模拟的语境,即将供应链中的企业看作管理域,企业内选出唯一的域管理者,企业部署与运维的物联网与智能设备作为域内节点.同时,考虑到"供应链中的企业存在稳定的经济联系,且这种经济联系是以存在商业信用为前提的,商业信用有其严格的方向性,在供应链中只能由上游产品企业向下游产品企业提供信用[32]",我们将$\Gamma_{i,j}$具象化为$A(x_i)\xrightarrow{Value}A(x_j)$以辅助$A(x_i)$提供商业信用的能力.其中$A(x_i)$代表公有链中某一上游企业,$A(x_j)$代表一个下游企业,$A(x_i)\xrightarrow{Value}A(x_j)$表示商品或服务及其价值由$A(x_i)$流向$A(x_j)$的过程.

此时,令实验中所有$A(x)\in\Phi_1$且$|\Phi_1|=10$,$Max(Pool(x))=1\,000$且$\theta=1$,模拟结果如图7所示:

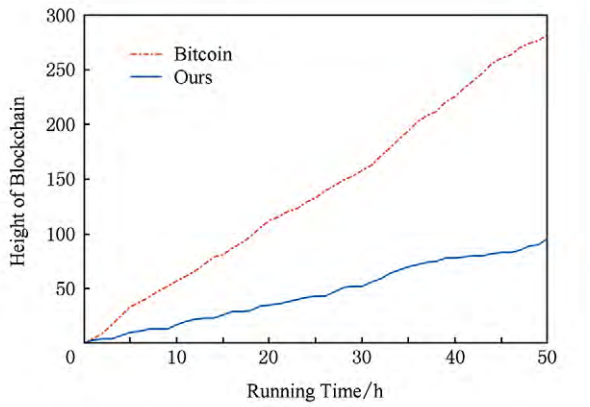


Fig. 7 Trend of Blockchain Growing

图7 区块链增长趋势

从图7中趋势可以看出,当$Max(Pool(x))=1\,000$且$\theta=1$时,本文方案的出块速率显著慢于比特币出块速率.又因为本文方案中单个区块比比特币区块要小,因此在实验语境中,本文方案比比特币区块链更加节省存储空间.

实验模拟中涉及到的$\Gamma_{i,j}$次数与设备间合作次数的频数分布直方图如图8所示.

此外,出块速率与区块链存储开销与$Max(Pool(x))$是密不可分的,本文考察了当$Max(Pool(x))$的取值不断变大时的区块产生情况,如图9所示.

从图9中可以看出,$Pool$值越大,区块产生速率越小.在相同的供应链经济表现($\Gamma_{i,j}$次数,设备间合作次数)下,$Pool$值增大的过程中区块产生速率下降的幅度会越来越小,这是因为当$Pool$值较小时,

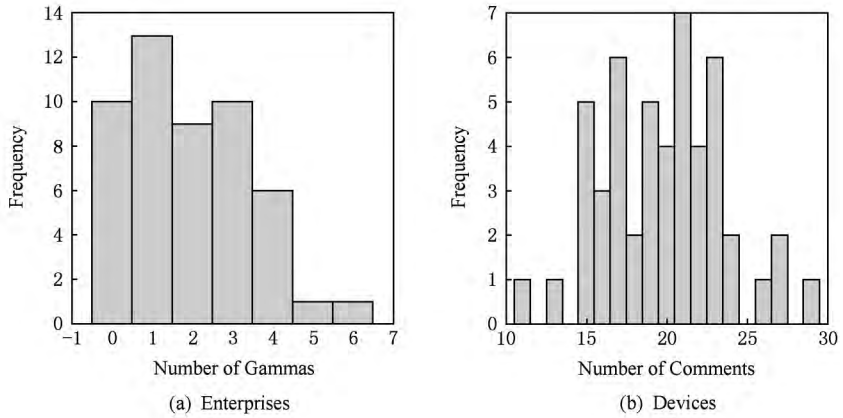


Fig. 8 The external environment related to the generation of blocks in the experiment

图 8 实验中与新区块产生有关的外部环境

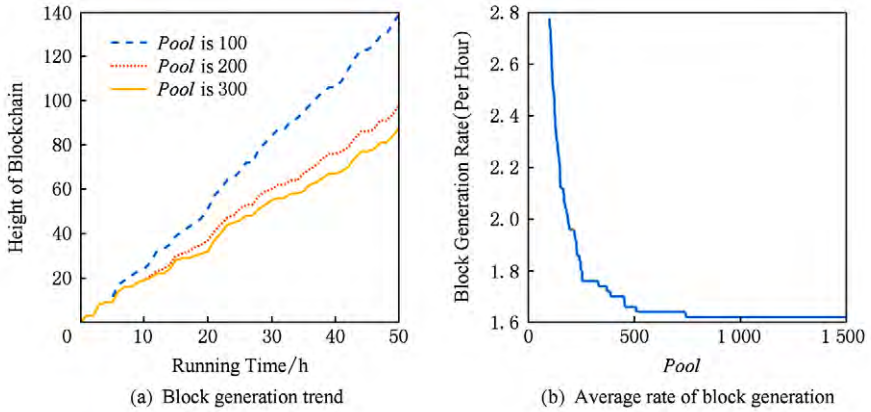


Fig. 9 Relationship between size of pool and block generation rate

图 9 *Pool* 大小与区块产生速率的关系

3.3 节所述情形 2 是区块产生速率的主要影响因素，此时新区块的产生主要由设备间评价影响；而当 *Pool* 值不断增大到能够使服务器较为轻易地容纳设备在较长时间内产生的期望信用评价数据时，影响区块产生速率的主要因素就变换为 3.3 节所述情形 1，此时企业间合作与评价占据新区块产生的主要方面，区块产生速率对 *Pool* 值的依赖性降低.

图 9 所示实验中的其他因素为，$A(x)\in\Phi_1$，$|\Phi_1|=10$ 且 $\theta=1$. 代表实验中外部环境的数据如下直方图所示.

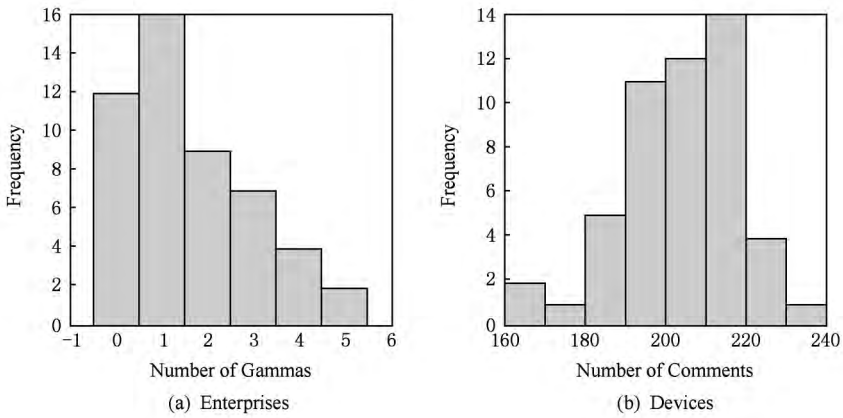


Fig. 10 The external environment related to the Fig. 9

图 10 与图 9 实验关联的外部环境

4.4 评估值 E_a,E_d 效果

在 3.6 节中,我们介绍了使用 E_a 与 E_d 作为域管理者与域内设备信任综合评价的结果.并说明了在本文方案中,E_a 与 E_d 的设计原则是使 C 受到比 R 相对较高的重视,这样当 C 与 R 同时很高或同时很低的情况时,能够对综合值给出更倾向于 C 值的结果.由于参与者试图选出期望信用最高,风险最低的实体作为合作伙伴,且信用值 C 与风险值 R 的取值都处于[0,1]区间内,选取简单归一化方法 $E_1=C/(C+R)$ 与 $E_2=C/\sqrt{C^2+R^2}$ 作为基准方法用来参照,并考察我们的计算方法与基准方法在评价性能上的差异.如图 11 与图 12 所示:

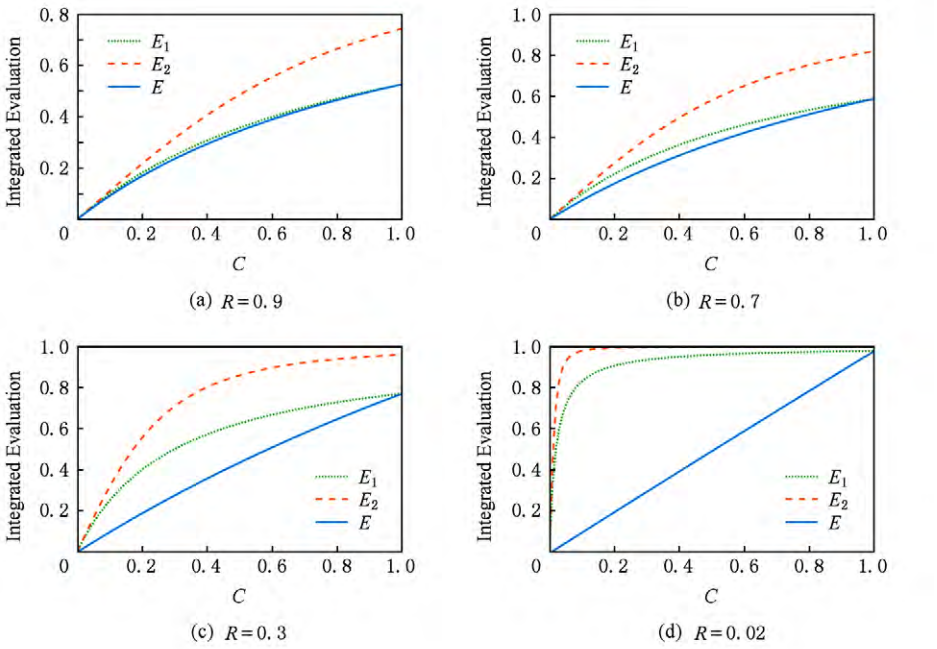


Fig. 11 Integrated evaluation with C changes

图 11 综合评价值随 C 的变化

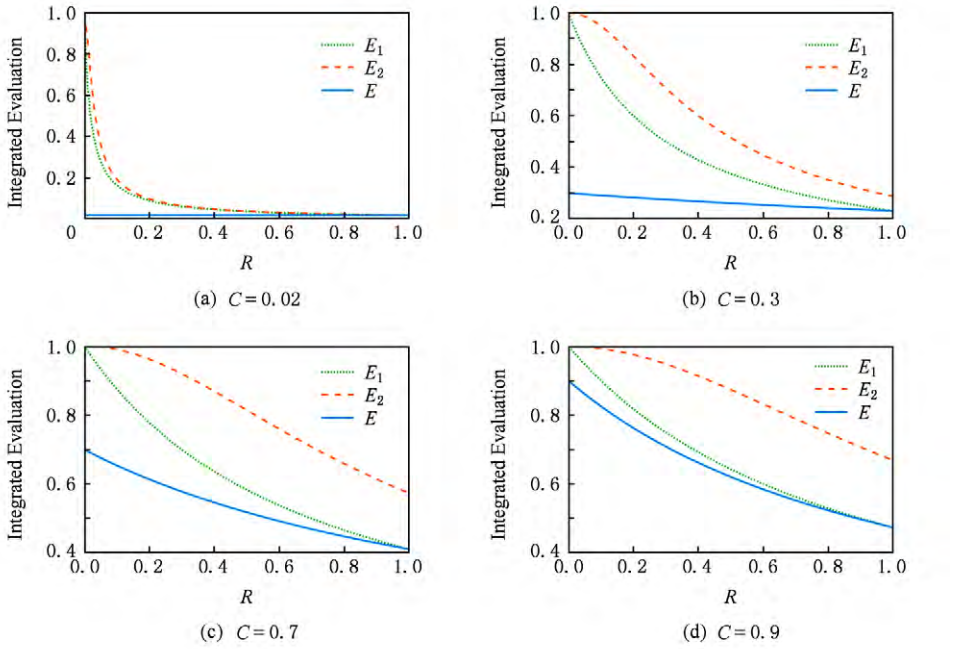


Fig. 12 Integrated evaluation with R changes

图 12 综合评价值随 R 的变化

从图 11 与图 12 中可以看出，当 C 逐渐变大时，E_1，E_2 与 E 都有逐渐变大的趋势，但是 E_1 与 E_2 更易受到单个变量变化的影响. 具体地，E_1 与 E_2 更易受到一个极低的风险或是极高的期望信用的影响，而忽略对另一个值的合理考虑，而 E 则在打分中显得更加得谨慎与保守.

图 13 示出了当 $C=R$ 时 E_1，E_2，E 的评价方式.

可以看出，当 C 与 R 相等时，E_1，E_2 都没有能够对 C 与 R 的数值变化做出反应，这使得信用与风险都十分低的实体与二者都十分高的实体分数完全一样；而 E 则对不同的期望信用-风险取值做出了不同的信任评价，使得当期望信用与风险同时很低或很高时，重点考虑期望信用的影响.

E_1，E_2 与 E 在 C 与 R 同时变化时的取值情况如图 14 所示.

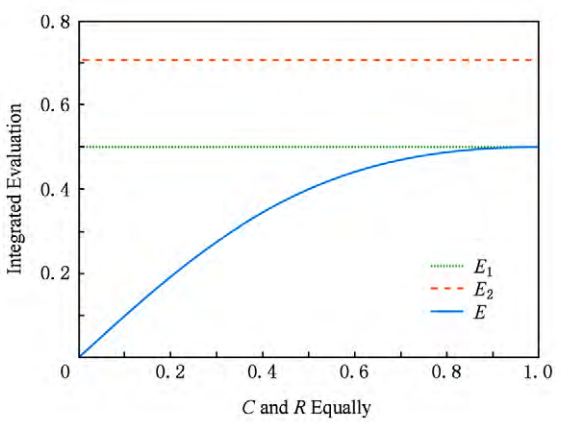


Fig. 13 Integrated evaluation with the case of $C=R$

图 13 $C=R$ 时综合评价值变化情况

可见，相比 E_1 与 E_2，E 的取值曲面更加地平滑，意味着不会因单个变量的小范围变化造成信任值的剧烈波动.

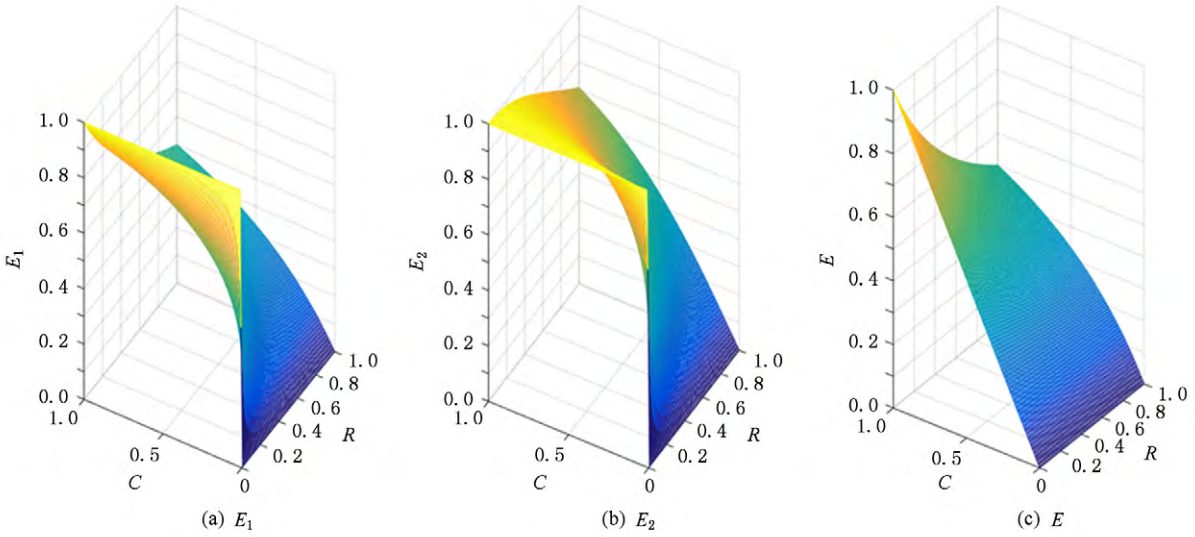


Fig. 14 Integrated evaluation with C and R changes

图 14 E_1，E_2 与 E 随 C 和 R 变化的取值图

5 总结与展望

本文提出了一种分布式物联网的信任管理方法，针对不依赖可信第三方与额外信任假设难以在纯分布式物联网中进行信任管理与后续合作的问题，借助区块链与风险理论设计了适用于域管理者与域内设备进行信任评价与评估的方法，以实现对分布式物联网内实体的信任管理. 实验模拟与分析表明本方案在信任管理与度量上的有效性，采用基于区块链的联盟链的最终共识防止信任数据被伪造与篡改，同时具有较低的存储开销.

随着物联网设备的成本下降与智能化程度的提升，分布式物联网的现实场景将更加广泛与多样化，使得这一环境下的信任管理问题面临着日益严峻的挑战. 未来对这一问题的研究可从 3 个方面进行：

1) 本文对设备之间的合作形式与交互方式未做假设，因为设备间的合作可能是复杂多样的，包括数据共享、资源调度等各种形式. 后续的研究可以关注于特定设备间对特定合作过程的交互协议设计.

2) 本文引入对风险的考察，但只用到了较为基础的风险理论. 我们使用了风险度量理论的创始人 Markowitz 在文献[33]中所提出的风险度量思想.

后续的研究可以关注于风险量化模型的比较,探索更加适合分布式物联网的风险量化模型.

3) 在分布式物联网中域管理者与设备都需要在合作中表现良好,才不会被合作伙伴给予负向信任评价;同样地,它们也需要为自己的评价负责,以避免存在参与者不负责任地对其他合作者作出大量正向或负向评价.对于域管理者间信用评价,本文方案提供了可追溯性;但对于设备,本文尚未对这一问题作详细讨论.简单的解决办法是使设备在向管理者服务器提交调节因子时携带数字签名,或者由服务器负责记录每次评价发起的设备并与评价结果一并记录在区块链上,并通过审计途径使得系统内参与者为其评价负责.后续研究可以关注于分布式物联网信任管理系统中的审计方法.如何实现自动化审计、审计主体的粒度、发现不负责任的评价者后的惩罚措施等问题都值得未来进一步研究.

参 考 文 献

[1] McKnight D H, Chervany N L. What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology [J]. International Journal of Electronic Commerce, 2001, 6(2): 35-59

[2] Mui L. Computational models of trust and reputation: Agents, evolutionary games, and social networks [D]. Cambridge, MA: Massachusetts Institute of Technology, 2002

[3] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management [C] //Proc of the 1996 IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 1996: 164-173

[4] Resnick P, Zechauser R, Friedman E, et al. Reputation systems: Facilitating trust in Internet interactions [J]. Communications of the ACM, 2000, 43(12): 45-48

[5] Sun Y L, Yu Wei, Han Zhu, et al. Information theoretic framework of trust modeling and evaluation for ad hoc networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 305-317

[6] Gupta M, Judge P, Ammar M. A reputation system for peer-to-peer networks [C] //Proc of the 13th Int Workshop on Network and Operating Systems Support for Digital Audio and Video. New York: ACM, 2003: 144-152

[7] Chen Dong, Chang Guiran, Sun Dawei, et al. TRM-IoT: A trust management model based on fuzzy reputation for Internet of things [J]. Computer Science and Information Systems, 2011, 8(4): 1207-1228

[8] Lize G, Jingpei W, Bin S. Trust management mechanism for Internet of things [J]. China Communications, 2014, 11(2): 148-156

[9] Saied Y B, Olivereau A, Zeghlache D, et al. Trust management system design for the Internet of things: A context-aware and multi-service approach [J]. Computers & Security, 2013, 39: 351-365

[10] Xiao Hannan, Sidhu N, Christianson B. Guarantor and reputation based trust model for social Internet of things [C] //Proc of Int Wireless Communications and Mobile Computing Conf 2015 (IWCMC'15). Piscataway, NJ: IEEE, 2015: 600-605

[11] Nitti M, Girau R, Atzori L. Trustworthiness management in the social Internet of things [J]. IEEE Trans on Knowledge and Data Engineering, 2014, 26(5): 1253-1266

[12] Duan Junqi, Gao Deyun, Yang Dong, et al. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications [J]. IEEE Internet of Things Journal, 2014, 1(1): 58-69

[13] Liu Wenmao, Yin Lihua, Fang Binxing, et al. A hierarchical trust model for the Internet of things [J]. Chinese Journal of Computers, 2012, 35(5): 846-855 (in Chinese)
(刘文懋, 殷丽华, 方滨兴, 等. 物联网环境下的信任机制研究[J]. 计算机学报, 2012, 35(5): 846-855)

[14] Chen I-R, Bao Fenye, Guo Jia. Trust-based service management for social Internet of things systems [J]. IEEE Trans on Dependable and Secure Computing, 2016, 13(6): 684-696

[15] Benkerrou H, Heddad S, Omar M. Credit and honesty-based trust assessment for hierarchical collaborative IoT systems [C] //Proc of 2017 Int Conf on. Information and Digital Technologies (IDT). Piscataway, NJ: IEEE, 2017: 295-299

[16] Rafey S E A, Abdel-Hamid A, El-Nasr M A. CBSTM-IoT: Context-based social trust model for the Internet of things [C] //Proc of the 2016 Int Conf on Selected Topics in Mobile & Wireless Networking (MoWNeT'16). Piscataway, NJ: IEEE, 2016: 1-8

[17] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [OL]. [2018-01-01]. https://bitcoin.org/bitcoin.pdf

[18] Merkle R C. Method of providing digital signatures: USA Patent 4,309,569 [P]. 1982-01-05

[19] Merkle R C. A certified digital signature [C] //Proc of CRYPTO89. Berlin: Springer, 1989: 218-238

[20] King S, Nadal S. PPCoin: Peer-to-peer crypto-currency with proof-of-stake [OL]. [2014]. http://ppcoin.org/static/ppcoin-paper.pdf

[21] Lamport L, Shostak R, Pease M. The Byzantine generals problem [J]. ACM Trans on Programming Languages and Systems, 1982, 4(3): 382-401

[22] Lamport L. The part-time parliament [J]. ACM Trans on Computer Systems, 1998, 16(2): 133-169

[23] Lamport L. Paxos made simple [J]. ACM Sigact News, 2001, 32(4): 18-25

[24] Lamport L. Fast paxos [J]. Distributed Computing, 2006, 19(2): 79-103

[25] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery [J]. ACM Trans on Computer Systems, 2002, 20(4): 398-461

[26] Alchieri E A P, Bessani A N, da Silva Fraga J, et al. Byzantine consensus with unknown participants [C] //Proc of the 12th Int Conf on Principles of Distributed Systems (OPODIS 2008). Berlin: Springer, 2008: 22-40

[27] Ongaro D, Ousterhout J K. In search of an understandable consensus algorithm [C] //Proc of 2014 USENIX Annual Technical Conf. Berkeley, CA: USENIX Association. 2014: 305-319

[28] Fischer M J, Lynch N A, Paterson M S. Impossibility of distributed consensus with one faulty process [J]. Journal of the ACM, 1985, 32(2): 374-382

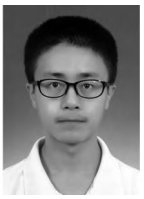
[29] Cachin C. Architecture of the Hyperledger blockchain fabric [C] //Proc of the 1st Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL 2016). New York: ACM, 2016.

[30] Xia Dafeng, Xu Senlin, Qi Feng. A proof of the arithmetic mean-geometric mean-harmonic mean inequalities [J]. RGMIA Research Report Collection, 1999, 2(1): 99-102

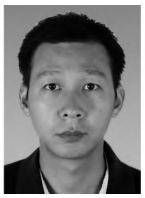
[31] Bastiaan M. Preventing the 51%-attack: A stochastic analysis of two phase proof of work in bitcoin [OL]. [2018-01-01]. http://pdfs.semanticscholar.org/0336/6d1fda3b24651c71ec6ce21bb88f34872e40.pdf

[32] Petersen M A, Rajan R G. Trade credit: Theories and evidence [J]. The Review of Financial Studies, 1997, 10(3): 661-691

[33] Markowitz H. Portfolio selection [J]. The Journal of Finance, 1952, 7(1): 77-91



Ren Yanbing, born in 1993. Master candidate. His main research interests include distributed systems, privacy preserving and networks & information security.



Li Xinghua, born in 1978. PhD, professor, PhD supervisor. Member of CCF. His main research interests include wireless networks security, privacy preserving and networks & information security.

Liu Hai, born in 1984. PhD candidate. His main research interests include privacy preserving and rational cryptographic protocols.

Cheng Qingfeng, born in 1979. PhD, associate professor in Information Engineering University. His main research interests include cryptography and information security.

Ma Jianfeng, born in 1963. PhD, professor, PhD supervisor. Fellow of CCF and Senior member of IEEE. His main research interests include distributed systems, wireless and mobile computing systems, computer networks & information security.