

一种面向物联网数据交易的高效PCN路由策略

李敦锋, 肖瑶, 冯勇

引用本文

李敦锋, 肖瑶, 冯勇. 一种面向物联网数据交易的高效PCN路由策略[J]. 计算机科学, 2022, 49(11A): 211100010-5.

LI Dun-feng, XIAO Yao, FENG Yong. [Efficient Routing Strategy for IoT Data Transaction Based on Payment Channel Network](#) [J]. Computer Science, 2022, 49(11A): 211100010-5.

相似文章推荐 (请使用火狐或 IE 浏览器查看文章)

Similar articles recommended (Please use Firefox or IE to view the article)

[基于边缘计算的数据无损压缩方法](#)

Lossless Data Compression Method Based on Edge Computing

计算机科学, 2022, 49(11A): 210500195-6. <https://doi.org/10.11896/jsjcx.210500195>

[边云协同计算中成本感知的物联网数据处理方法](#)

Cost-aware IoT Data Processing in Edge-Cloud Collaborative Computing

计算机科学, 2022, 49(11A): 211000101-7. <https://doi.org/10.11896/jsjcx.211000101>

[基于密码学累加器的电力物联网设备接入管理](#)

Power Internet of Things Device Access Management Based on Cryptographic Accumulator

计算机科学, 2022, 49(11A): 210900218-6. <https://doi.org/10.11896/jsjcx.210900218>

[基于预训练技术和专家知识的重入漏洞检测](#)

Reentrancy Vulnerability Detection Based on Pre-training Technology and Expert Knowledge

计算机科学, 2022, 49(11A): 211200182-8. <https://doi.org/10.11896/jsjcx.211200182>

[支持分片内多轮PBFT验证算法的状态同步方案](#)

State Synchronization Scheme Supporting Multiple Rounds of PBFT VerificationAlgorithm in Sharding

计算机科学, 2022, 49(11A): 211000125-7. <https://doi.org/10.11896/jsjcx.211000125>

一种面向物联网数据交易的高效 PCN 路由策略

李敦锋 肖 瑶 冯 勇

昆明理工大学云南省计算机重点实验室 昆明 650500

(1002213567@qq.com)

摘 要 为了提高物联网数据交易的效率,提出了一种基于付费信道网络(Payment Channel Network,PCN)的高效路由策略。该策略从网关选择和大额交易拆分两个方面入手来完善 PCN 网络的缺陷。通过计算不同网关的支付和接收资金流量比率来选择合适的网关进行交易,以保证网络的平衡,增加了网络的稳定性。为了解决大额交易时信道容量不足的问题,将单笔交易拆分成多个交易单元,并通过多信道均衡算法来进行路径选择,减少了链上交易次数,提高了网络的交易效率。仿真结果表明,该方案拥有较高的交易成功率和更低的交易时延。

关键词: 区块链;物联网;付费信道网络;数据交易;路由均衡

中图法分类号 TP311

Efficient Routing Strategy for IoT Data Transaction Based on Payment Channel Network

LI Dun-feng, XIAO Yao and FENG Yong

Yunnan Key Laboratory of Computer Technology Applications, Kunming University of Science and Technology, Kunming 650500, China

Abstract In order to improve the efficiency of data transactions in Internet of Things, an efficient routing strategy based on payment channel network(PCN) is proposed. This strategy improves the defects of PCN network from two aspects: gateway selection and large-value transaction splitting. By calculating the payment and receiving fund flow ratios of different gateways, the appropriate gateways are selected for transactions to ensure the balance of the network, which increases the stability of the network. In order to solve the problem of insufficient channel capacity in large-value transactions, a single transaction is split into multiple transaction units, and path selection is performed through a multi-channel equalization algorithm, which reduces the number of transactions on the chain and improves the transaction efficiency of the network. Simulation results show that the program has a higher transaction success rate and lower transaction delay.

Keywords Blockchain, Internet of Things, Payment channel network, Data transaction, Routing balance

1 引言

随着物联网设备的普及,物联网数据也具有了商品的价值属性,如何建立一个高效的、安全的数据交易网络成为了一个重要的研究方向。区块链技术具有去中心化、可编程和防伪篡改等特征,这些特征为构建安全可信的分布式交易环境提供了良好的契机^[1-3]。随着物联网设备的普及,如何安全的交易和使用物联网设备产生的数据成为了一个重要的研究方向。本文将区块链技术应用于物联网数据交易。然而,受到共识机制和智能合约的约束,区块链交易的吞吐量和可拓展性都很差^[4]。比特币每秒只能完成 3~7 笔交易,以太坊每秒可以进行最多 15 笔交易,而全球化的如 Visa 等支付提供商每秒可进行上千次的交易,这是目前区块链技术无法企及的^[5]。而在物联网数据交易中,对交易实时性的要求较高、区块链技术可拓展性差和吞吐量低的问题被进一步放大。

付费信道技术可以解决传统区块链技术交易速度慢的问题,这是一种链下支付技术,该方法是在两个用户之间建立付费信道,并在信道中托管一定的资金,将交易从链上转移到

链下,避免了链上共识建立和确认的时延^[6]。只有在建立和关闭支付信道时,才会将交易信息写入区块链,链下的交易可以频繁地执行,不需要上链,从而大大提升了交易效率、吞吐量和可拓展性。连接不同用户的付费信道共同组成了付费信道网络(Payment Channel Network,PCN)^[7]。

将付费信道网络和物联网数据交易结合,提高了交易的安全性和可拓展性。但普通的 PCN 技术容易产生链上资金耗尽的问题。在交易过程中,中间节点的资金会被暂时冻结,如果交易路由选择不当,中间节点的资金会耗尽,该节点将无法发起或者接收任何交易。目前可以通过链上对耗尽资金节点进行资金补充来解决问题,但该过程涉及到复杂的链上共识和签名认证机制,影响链下交易进程和成功率^[8]。

基于以上问题,本文提出了一种基于 PCN 的物联网数据交易的路由策略,在保证交易安全的前提下,能够满足物联网数据交易高效率 and 可持续性的要求。该策略分为两个部分,第一个部分为均衡网关选择算法,第二个部分为多路由均衡算法。本文第 2 节介绍了国内外的相关工作;第 3 节建立了均衡网关选择模型和多路由均衡交易模型;第 4 节为相关策略和

基金项目:国家自然科学基金(62062047,61662042,61962030)

This work was supported by the National Natural Science Foundation of China(62062047,61662042,61962030).

通信作者:冯勇(fybraver@163.com)

模型的实现;第 5 节为仿真实验和分析;最后总结全文。

2 相关工作

目前已经有一些研究将区块链技术运用到物联网中。Li 等^[9]研究了区块链技术在工业物联网能源交易中的应用,提出了一种安全的能源交易系统,该系统采用联盟区块链技术,通过 Stackelberg 博弈定价来确保系统安全高效。Lu 等^[10-11]研究了区块链在车联网中的应用,实现了基于区块链的非对称加密匿名认证方案,解决了匿名认证的扩展性和认证效率问题。Liu 等^[12]提出了基于区块链的物联网数据交易模型,利用边缘计算和云服务器来验证区块链存储和智能合约,并使用 Stein-berg 博弈模型进行定价。

在物联网数据交易方面,目前也有研究者使用链下技术来进行研究和设计,其中包括安全性、支付协议和路由优化。Cao 等^[13]提出了一种迭代的数据交易模式,通过社会最优的方式来协调交易,无需访问个人信息,保护了节点的隐私。Niu 等^[14]通过同态加密和数字身份签名来保证数据的隐私性和真实性。Decker 等^[15]提出了一种双工小额支付通道协议,用于保证端到端的安全性并允许即时交易,奠定了 PSP 网络的基础。Hannon 等^[16]也提出使用支付信道进行物联网设备之间的通信,其交易过程通过区块链进行并且引入了交易外的第三方进行监督。在路由优化方面,Sivaraman 等^[7]提出了 Spider 算法来解决节点资金耗尽问题,同时使用了多路径传输协议来实现高吞吐量。Yu 等^[17]对 PCN 进行了深入研究,提出了一种新型分布式动态路由机制,降低了支付开销并提高了支付成功率。

以上研究对 PCN 技术在物联网数据交易中涉及到的交易通道阻塞问题和单笔交易过大造成的交易延迟问题没有进行详细的讨论。

3 系统模型

本节将描述基于 PCN 的物联网数据交易模型的整体架构以及路由算法模型。

3.1 链下付费信道

传统的区块链技术,例如比特币的平均区块生成时间需要 10 min,而交易时间更是可能达到数十分钟之久,这使得人们在日常交易或者小额的交易中无法使用它。为了解决这个问题,提出了“链下付款信道”的支付机制,该机制使用的是区块链中的智能合约机制。该合约称之为“哈希时间锁定合约”(Hash Time Locked Contract, HTLC),合约流程如图 1 所示。

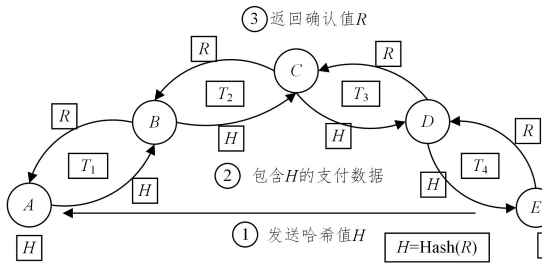


图 1 哈希时间锁定合约

Fig. 1 Hashed time lock contract

如图 1 所示,对于请求 $A \rightarrow E$,接收者 E 生成密钥 R 及其哈希 H ,并将 H 发送给 A 。 A 将 H 和时限 T_1 编码到与 B 的

合约中,这样 B 无法在时限 T_1 内且不向 A 返回密钥 R 的情况下花费锁定资金。之后每个节点类似地转发付款,并采用递减的截止时间,即 $T_1 > T_2 > T_3 > T_4$ 。收到付款后, E 将向 D 提供 R 以确认收到付款,同时解锁 D 的锁定资金,而 D 将对上一个节点执行相同的操作,直到 A 收到 R 。

链下支付的优势在于用户不需要将每笔交易都发布到区块链上,只有在创建和关闭通道时涉及到与区块链通信,使用 HTLC 技术可以很好地保证支付信道的安全性和可靠性。没有了频繁的链上交易后,也不会存在高额的交易费用,这解决了物联网数据交易频繁时,使用比特币等传统技术交易费用过高、交易速度过慢的问题。

3.2 PCN 网络模型

链下付费信道可进一步用于 PCN 网络的创建。如图 2 所示,假设 A 从 D 获取物联网数据并进行交易,在交易过程中经过 B 和 C 两个节点,整个交易过程通过 HTLC 协议来保证交易的安全,在交易过程中可以将网络中的节点分为 3 类。

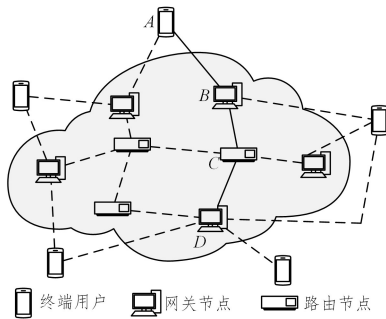


图 2 PCN 网络模型

Fig. 2 Payment channel network model

(1)终端用户,终端用户也可以称之为购买节点,常为购买数据而付款。终端用户连接到网关节点以访问网络的其余部分,并且它必须在其与网关的通道中保持最低数量的资金才能继续进行交易。在交易时该节点会请求打开一个带有网关节点的通道,该通道可以将其连接到其他节点,为了提高效率,最好能够直接与交易的网关连接,也可以通过路由节点和不直接相连的网关进行交易。

(2)网关节点,也可以叫作数据商店节点,这些节点是通常希望收到付款但很少发送付款的物联网节点,也就是物联网数据的提供者。这些节点还帮助终端用户与网络中的其他节点进行交易。网关节点必须与路由节点有良好的连通性。他们的主要目标是以加密货币销售他们的物联网数据,而不是为其他交易赚取转账费。

(3)路由节点,路由节点负责连接网络中的不同网关。每个路由节点都试图拥有大量连接,主要通过收取交易的转账费用获益,并且它们还负责维护整个网络中信道的平衡。这使它们成为支付网络的中心点。

假设存在于 PCN 网络中的节点通过链下付费信道相互连接。两个节点的通道容量代表了这两个节点在多重签名地址中存入的货币量。图 2 所示的网络模拟现金流从客户到网关的真实场景,因此将每个节点区分为终端用户节点、网关节点和路由节点,虽然任何节点都可以扮演这 3 种角色中的任意一个。

4 策略设计与实现

为了提高支付效率和成功率,本文提出了一种高效的

支付路由策略,它由均衡网关选择策略和多信道均衡算法组成,大大减少了链上交易次数,在维护网络稳定性的同时提高了交易的成功率。

4.1 均衡网关选择协议

在 PCN 中,终端用户通过网关节点和路由节点向另一网关节点发起支付,如图 2 中 A 到 D 的支付路径所示。如果通道中资金不足,将无法完成此多跳传输。在现实条件下,支付往往是高度定向的,渠道中的资金将转移到特定的一侧,网关节点极易出现信道资金平衡耗尽。如果一个网关节点将其所有资金用于单向的支付,那么在收到某些付款之前,这个节点将无法继续作为中间节点进行运转,如图 3 所示。

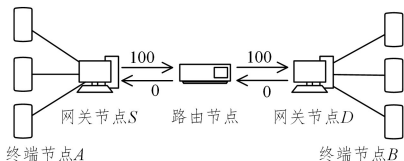


图3 通道资金耗尽导致通道阻塞

Fig. 3 Channel blockage caused by channel funds exhaustion

PCN 中的支付通道为双向通道且共用通道的货币容量,假设信道的货币容量为 100。图 3 给出了 A 区域的终端节点从 D 网关节点购买数据的最短路径,假设 A 区域终端节点在短时间内大量地从 D 节点购买数据,此时耗光了该通道的所有容量,在这些交易完全结束前,交易通道中的资金会被冻结以保证交易的安全。在通道资金冻结时,如果 B 区域的节点想从网关 S 购买数据,该通道同样为最短路径,但此时路径中的资金容量已被单向交易耗尽,因此 B 区域节点只能等待通道释放足够多的交易资金或重新选择交易通道。为了解决这一问题,可以更改发起交易的网关,如果一个网关节点已经进行了大量的单向交易,则应当避开该网关,使用其他的网关进行交易,这样可以保证该通道不会被完全阻塞,保证最短交易路径双向交易的功能随时可用,这样可以更好地保持 PCN 中的网络平衡和交易效率。

交易发起节点确定交易金额,根据路由表确定发起节点所连接的网关节点的当前交易金额,去掉交易金额不足的网关节点;计算满足要求的网关节点之前一段时间的支付和收入金额比率,具体计算方法为 $Ra = out_account / in_account$,其中, Ra 为支付收入比率, $out_account$ 为一段时间内预计用于支出而被锁定的金额, $in_account$ 为一段时间内预计收入而解冻的金额,其中:

$$\begin{cases} in_account = in_total + capacity(v, u) \\ out_account = out_total + capacity(u, v) \end{cases} \quad (1)$$

其中, in_total 为接收付款的交易, in_total 为支出付款的交易, $capacity(v, u)$ 是可以用于支出的通道余额, $capacity(v, u)$ 为可用于接收金额的通道余额,可知当 Ra 越小时,网关节点预期用于支付的资金越多,选用 Ra 最小的网关节点进行支付,并且将网关用于最大支出交易的最大交易金额 MTA ($\max \text{ transaction amount}$) $= 0.8 * (capacity(v, u) + capacity(u, v))$, MTA 为该网关单次可用于支出交易的最大金额,并被用于最大单笔交易划分问题。

算法 1 I/O 比率计算算法

输入:网关节点列表 G,有向连通图 C

输出:最佳路径 Path

1. 初始化最大值 $maximum = 0$

2. for k in G do // 计算所有网关链接的比率

3. $in_total = out_total = 0$

4. for channel(u, v), of gateway k do

5. $in_total = in_total + capacity(v, u)$

6. $out_total = out_total + capacity(u, v)$

7. end for

8. $ratio = in_total / out_total$

9. if $ratio \geq maximum$ then

10. $maximum = ratio$

11. end if

12. end for

13. Path = ShortestPath(C, from = maximum, to = 目标节点)

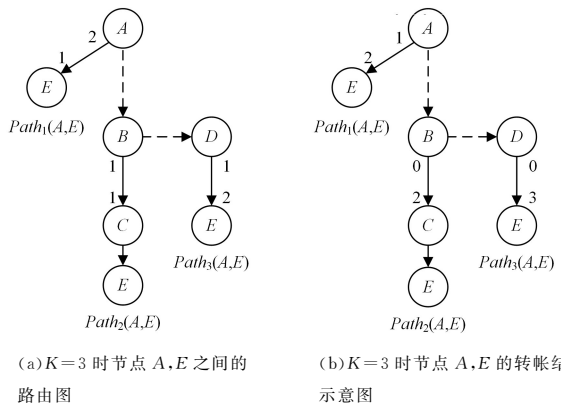
4.2 多路由均衡协议

显然,均衡网关选择算法解决了单个网关节点在进行大量交易时的资金不平衡问题,而在交易过程中,还会遇到单笔交易额过大的问题,如果此时网络中没有单一的交易通道拥有足够的交易能力,那么这个交易就会被搁置。为了解决这个问题,可以利用 K 最短路(K Shortest Paths, KSP)^[18-19]算法的思路,根据均衡网关选择算法设计了适合物联网数据交易的多路由均衡算法。传统的 K 路径算法如图 4 所示。假设一个业务请求的源、目的节点分别为 v_i 和 v_j , K 路径算法可分为两部分:

(1) 利用基础路由算法算出首条路径 $Path_1(v_i, v_j)$, 然后在此基础上求得其他 $K-1$ 条路径。

(2) 在求 $Path_{k+1}(v_i, v_j)$ 时 ($1 < k < K$), 将 $Path_1(v_i, v_j)$ 上的除了目的节点之外的所有节点都视为背离节点, 并根据基础路由算法计算每个背离节点到目的节点的路径, 再与之前 $Path_1(v_i, v_j)$ 上的源节点到背离节点的路径连接, 构成候选路径。

假设 $K=3$, 节点 A 与 E 之间存在 3 个单位的转账请求, 节点 A 与 E 的 K 路径选路结果示例如图 4(a) 所示。其中 $Path_1(A, E)$ 与 $Path_2(A, E)$ 之间的偏离节点为 A, $Path_2(A, E)$ 与 $Path_3(A, E)$ 之间的偏离节点为 B。从图 4(a) 可以看出, 3 条路径的最大可流通资金均无法满足需求, 将转账请求平均分散到 3 条候选路径可转账成功, 结果如图 4(b) 所示。



(a) $K=3$ 时节点 A, E 之间的路由图

(b) $K=3$ 时节点 A, E 的转账结果示意图

图 4 K 最短路算法示意图

Fig. 4 Diagram of K shortest path algorithm

路由均衡算法在交易发起时将交易拆分成一系列独立路由的交易单元, 定义最大的交易金额 MTA 为一个交易单元。交易过程中使用独立的密钥创建每个交易单元, 拆分交易并不会影响交易的安全性。当交易接收方接收并确认交易单元时, 发送方可以选择性地仅显示已确认交易单元的密钥。

交易发送方在交易过程中将收到通知,告知他们已完成了多少交易单元,发送方可以选择取消未完成的交易单元或在区块链上重试。多路径转发算法可简单分为 3 个步骤。

首先,计算交易单元个数,如式(2)所示:

num_{Tun} = Round \cup \left(\frac{m}{MTA} \right) \tag{2}

其中, Round \cup 代表向上取整, MTA 表示最大交易单元大小, m 表示交易金额。

其次,使用 K 路径算法计算交易的转发路径,转发路径的条数如式(3)所示:

NUM_{Path}(trans_i(v_i, v_j, m)) = \min(num_{Tun}, NUM_{path}(v_i, v_j)) \tag{3}

其中, NUM_{Path}(trans_i(v_i, v_j, m)) 为交易选择的路径, NUM_{path}(v_i, v_j) 为 K 最短路径算法找到的所有路径。

最后,每个交易单元根据算法 1 来选择网关路径并将其转发。多路径路由转发算法的流程如算法 2 所示。

算法 2 多路径路由转发算法

输入:交易请求 trans_i(v_i, v_j, m), K 路径算法, MTA

- 1. if (m ≤ MTA) then
- 2. 调用算法 1 选择网关进行交易
- 3. else 计算 v_i 到 v_j 所有可转发路径个数 NUM_{path}(v_i, v_j)
- 4. end if
- 5. 按照式(1)计算交易单元个数 num_{Tun}
- 6. 按照式(2)计算交易需要的转发路径个数 NUM_{Path}(trans_i(v_i, v_j, m))
- 7. if (NUM_{Path}(trans_i(v_i, v_j, m)) ≥ num_{Tun}) then
- 8. 对各个交易单元进行签名
- 9. K = num_{Tun}
- 10. 按照算法 1 选择网关并按照 K 路径算法转发交易单元
- 11. else if (NUM_{Path}(trans_i(v_i, v_j, m)) < num_{Tun}) then
- 12. 对 NUM_{Path}(trans_i(v_i, v_j, m)) 个交易单元进行签名
- 13. K = NUM_{Path}(trans_i(v_i, v_j, m))
- 14. 按照算法 1 选择网关并按照 K 路径算法转发交易单元
- 15. num_{Tun} = NUM_{Path}(trans_i(v_i, v_j, m)), 返回步骤 12
- 16. end if

通过上述两种算法,实现了高效率的物联网数据交易路由由协议。在数据交易单向流动时,通过均衡网关选择算法解决交易节点资金不平衡的问题,基本上,当出站资金容量小于入站资金容量时,其承担更少的支出交易。在有大额交易需求时,通过划分交易单元来提高交易成功率,缩短了交易等待时间。

5 仿真分析

为了验证上文提出的物联网数据交易路由策略,搭建了基于 Kotlin 的 PCN 仿真系统,同时对比了 ERS_PCN^[4] 算法和 RituSindhu^[20] 的实验,并与 AODV-Ext^[21] 路由方案进行了对比。实验参数设置如表 1 所列。

表 1 仿真参数设置

参数	值
节点个数	100
基础路由算法	K 最短路径算法
节点平均度数	3
平均交易金额	6 瑞波币
交易通道容量	20~60 瑞波币
交易次数	120~720

实验构造的网络中终端节点:网关节点:路由节点为 5:4:1。终端节点和网关节点的初始账户余额遵循正态分布,

范围在 20~60 瑞波币之间。同时交易时的单次交易金额也遵循正态分布,平均交易金额为 6 瑞波币。每次交易使用随机算法在账户余额充足的终端节点或网关节点中选择发起节点,而目的节点则是在所有路由节点之外的节点中选择。节点度数代表节点与其他节点直接连接的个数。

实验结果如图 5 所示,随着每秒交易次数的增加,本文提出的物联网数据交易路由由算法的成功率高于 AODV-Ext 路由协议和 ERS_PCN 路由协议,且一直保持着稳定的交易成功率。可以看到,随着交易次数的增加,交易成功率的差值也随之增大。由于 ERS_PCN 算法也采用了多路由交易技术,因此其效率算法与本文算法接近,但是本文提出了均衡网关选择算法,使其在更大数量的交易请求中有更好的表现,交易成功率相比 ERS_PCN 算法提升了约 12%,相比 AODV-Ext 算法提升了 114%。

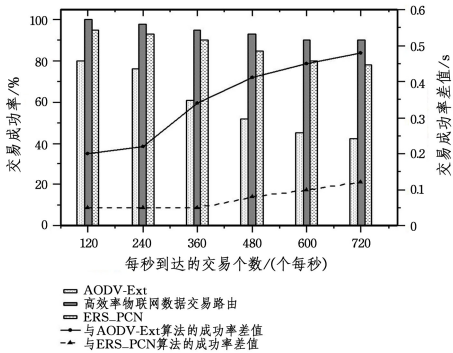


图 5 交易成功率对比

Fig. 5 Comparison of transaction success rate

如图 6 所示,实验对比了在每秒到达交易个数不同的情况下,不同算法之间交易延时的情况,交易延时越小越好。由于实验运行在本地服务器中,因此不考虑传输时延和传输协议,仿真实验的交易延时是交易过程中建立交易通道和使用不同路由协议或交易协议产生的延迟,体现的是不同路由协议之间的效率差别。如图 6 所示,本文算法和 ERS_PCN 算法的延迟远小于 AODV-Ext 算法,该算法没有对交易做任何处理,导致交易次数较高时,交易节点阻塞失效,大大降低了交易的效率。而本文算法将大型交易进行了划分,避免了交易拥堵的状况,使用均衡网关选择算法减轻了网络失衡的问题,这也是本文算法的交易延时比 ERS_PCN 算法更低的原因。相比 AODV-Ext 算法,交易效率提高了约 225%,相比 ERS_PCN 算法,交易效率提高了约 56%。

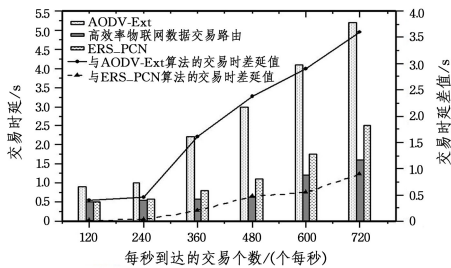


图 6 交易延时对比

Fig. 6 Transaction delay comparison

图 7 模拟了在不同网络规模下本文提出的高效物联网数据交易路由由策略的成功率和交易延迟的变化。可以发现,即使网络规模扩大,交易成功率依旧保持在较高的水平,而交易延时随着网络规模的扩大而提高,但是总体延迟在 1 s 之内。

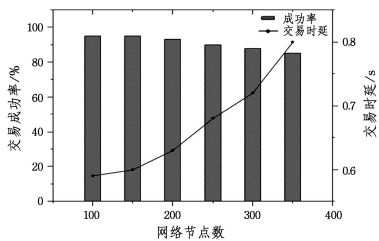


图 7 在不同网络节点规模下算法的表现

Fig. 7 Performance under different network node scales

结束语 本文提出了一种面向物联网数据交易的高效交易策略,该策略基于 PCN 技术,既保留了其轻量化和快速交易的特点,又对其路由建立和交易分发机制进行了改进。通过计算网关节点的支出和收入资金比来选择合适的网关节点进行交易传输,保证了整体网络的平衡。同时,将大笔交易划分成多个交易单元,减少了交易网络的交易容量要求,且满足了物联网数据交易对大规模数据交易和快速交易的需求。相比 ERS_PCN 算法增加了大规模交易分发机制,提高了交易速率;相比使用一般 PCN 技术的 AODV-Ext 算法,本文对 PCN 技术改进后的整体性能有了较大提升。该策略可用数据交易市场^[22]中交易系统的构建,对物联网数据交易方式进行了探索和优化。但研究对交易数据本身的考虑不够全面,没有就大量数据交易对信道产生的影响进行探讨和实验,在之后的研究中,可以针对交易数据量过大时,对如何解决交易信道的占用进行更加深入的探讨。

参 考 文 献

[1] UNDERWOOD S. Blockchain beyond bitcoin[J]. Communications of the ACM, 2016, 59(11): 15-17.

[2] CAO L, LIN L, LI Y, et al. Review of blockchain research [J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition), 2020, 32(1): 1-14.

[3] GAI R, DU X, MA S, et al. A summary of the research on the foundation and application of blockchain technology[C]// Journal of Physics: Conference Series. IOP Publishing, 2020.

[4] HUO R, NI D, LU H, et al. Efficient routing strategy of blockchain-based payment channel network[J]. Journal on Communications, 2021, 42(6): 30-40.

[5] POON J, DRYJA T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments[EB/OL]. (2016-01-14). <https://lightning.network/lightning-network-paper.pdf>.

[6] MALAVOLTA G, MORENO-SANCHEZ P, KATE A, et al. Concurrency and privacy with payment-channel networks[C]// Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017: 455-471.

[7] SIVARAMAN V, VENKATAKRISHNAN S B, RUAN K, et al. High throughput cryptocurrency routing in payment channel networks[C]// 17th {USENIX} Symposium on Networked Systems Design and Implementation({NSDI} 20). 2020: 777-796.

[8] CROMAN K, DECKER C, EYAL I, et al. On scaling decentralized blockchains[C]// International conference on financial cryptography and data security. Berlin: Springer, 2016: 106-125.

[9] LI Z, KANG J, YU R, et al. Consortium blockchain for secure energy trading in industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2017, 14(8): 3690-3700.

[10] LU Z, WANG Q, QU G, et al. Bars: a blockchain-based anonymous reputation system for trust management in vanets[C]//

2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018: 98-103.

[11] ERDIN E, CEBE M, AKKAYA K, et al. Building a private bitcoin-based payment network among electric vehicles and charging stations[C]// 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE, 2018: 1609-1615.

[12] LIU K. Optimal Pricing Mechanism for Data Market in Blockchain-Enhanced Internet of Things[J]. IEEE Internet of Things Journal, 2019, 6(6): 9748-9761.

[13] CAO X, CHEN Y, LIU K J R. Data trading with multiple owners, collectors, and users: An iterative auction mechanism[J]. IEEE Transactions on Signal and Information Processing over Networks, 2017, 3(2): 268-281.

[14] NIU C, ZHENG Z, WU F, et al. Achieving data truthfulness and privacy preservation in data markets[J]. IEEE Transactions on Knowledge and Data Engineering, 2018, 31(1): 105-119.

[15] DECKER C, WATTENHOFFER R. A fast and scalable payment network with bitcoin duplex micropayment channels[C]// Symposium on Self-Stabilizing Systems. Cham: Springer, 2015: 3-18.

[16] HANNON C, JIN D. Bitcoin payment-channels for resource limited IoT devices[C]// Proceedings of the International Conference on Omni-Layer Intelligent Systems. 2019: 50-57.

[17] YU R, XUE G, KILARI V T, et al. Coinexpress: A fast payment routing mechanism in blockchain-based payment channel networks[C]// 2018 27th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2018: 1-9.

[18] GAO S, LU F. The Kth Shortest Path Algorithms: Accuracy and Efficiency Evaluation [J]. Journal of Image and Graphics, 2009, 14(8): 1677-1683.

[19] XU T, DING X L, LI J F. Review on K shortest paths algorithms [J]. Computer Engineering and Design, 2013, 34(11): 3900-3906.

[20] MERCAN S, ERDIN E, AKKAYA K. Improving transaction success rate in cryptocurrency payment channel networks[J]. Computer Communications, 2021, 166: 196-207.

[21] LI D, FENG Y, XIAO Y, et al. A Data Trading Scheme Based on Payment Channel Network for Internet of Things[C]// International Conference on Blockchain and Trustworthy Systems. Singapore: Springer, 2020: 319-332.

[22] ZHANG Y, WEN J T. The IoT electric business model: Using block-chain technology for the internet of things[J]. Peer-to-Peer Networking and Applications, 2017, 10(4): 983-994.



LI Dun-feng, born in 1995, postgraduate. He main research interests include internet of things and blockchain technology.



FENG Yong, born in 1975, professor. His main research interests include Internet of things, blockchain and the application of deep learning in the Internet of things and blockchain.