计算机科学
COMPUTER SCIENCE

基于联盟链的能源交易数据隐私保护方案

时坤，周勇，张启亮，姜顺荣

引用本文

时坤，周勇，张启亮，姜顺荣. 基于联盟链的能源交易数据隐私保护方案[J]. 计算机科学, 2022, 49(11): 335-344.

SHI Kun, ZHOU Yong, ZHANG Qi-liang, JIANG Shun-rong. Privacy-preserving Scheme of Energy Trading Data Based on Consortium Blockchain[J]. Computer Science, 2022, 49(11): 335-344.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220300138

基于联盟链的能源交易数据隐私保护方案

时 坤[1] 周 勇[1] 张启亮[2] 姜顺荣[1]
1 中国矿业大学计算机科学与技术学院 江苏 徐州 221116
2 徐工汉云技术股份有限公司 江苏 徐州 221001
(shikunss123@163.com)

摘 要 区块链技术可以有效地解决分布式能源交易系统中的信任缺失、恶意篡改和虚假交易等问题,但区块链开放、透明的特性使得基于区块链的能源交易系统极易受到攻击,导致用户隐私泄露。为此,提出了一种基于差分隐私算法和账户映射技术的隐私保护方案BLDP-AM(Blockchain Local Differential Privacy-Account Mapping),用于保护交易数据的隐私。该方案重新设计了本地差分隐私算法的数据扰动机制使之适用于区块链技术,并基于该扰动机制构造了BLDP(Blockchain Local Differential Privacy)算法来保护交易数据的隐私。同时,为了保证交易正确性以及隐藏交易曲线特征,该方案首先通过账户映射(Account Mapping,AM)技术实现用户与多个账户关联,然后采用指数平滑预测(Exponential Smoothing Prediction,ESP)算法计算各账户的交易预测值,最后使用BLDP算法扰动交易预测值来获得真实交易值并进行交易。通过隐私分析证明了该方案在保护数据隐私方面的可行性,且实验分析表明该方案具有较好的性能。

关键词:能源交易系统;区块链;本地差分隐私;账户映射;指数平滑预测
中图法分类号 TP399

Privacy-preserving Scheme of Energy Trading Data Based on Consortium Blockchain

SHI Kun[1],ZHOU Yong[1],ZHANG Qi-liang[2] and JIANG Shun-rong[1]
1 College of Computer Science and Technology,China University of Mining and Technology,Xuzhou,Jiangsu 221116,China
2 XcmgHanyun Technologies Co.,Ltd.,Xuzhou,Jiangsu 221001,China

Abstract Blockchain technology could effectively solve the problems of lack of trust,malicious tampering and false transactions. However,the open and transparent characteristics of the blockchain make the distributed energy trading model based on the blockchain extremely vulnerable to be attacked,leading to the disclosure of user's privacy. Therefore,a privacy-preserving scheme BLDP-AM based on differential privacy algorithm and account mapping technology is proposed to protect the privacy information of trading data. Our scheme redesigns the data perturbation mechanism of the local differential privacy algorithm to make it applicable to blockchain technology,and constructs the BLDP algorithm based on this perturbation mechanism to protect the privacy of transaction data. At the same time,in order to ensure the correctness of trading and hide the characteristics of the trading curve,our scheme first associates users with multiple accounts through account mapping technology,then uses the exponential smoothing prediction algorithm to calculate the trading prediction value of each account,and finally uses the BLDP algorithm to perturb the trading prediction value to obtain the real trading value and conduct trading. Our scheme not only guarantee the correctness of transactions but also achieve the purpose of protecting the privacy of trading data. The privacy analysis proves the feasibility of the scheme in protecting user privacy,and the experimental analysis shows that the scheme has better performance.

Keywords Energy trading systerm,Blockchain,Local differential privacy,Account mapping,Exponential smoothing prediction

1 引言

随着光伏、风力发电技术的不断发展,此类新能源技术的发电成本不断降低且产能急剧增加,因此被广泛应用于社区和家庭自主发电[1],能源交易模式逐渐由集中式向分布式演化。分布式能源交易模式具有参与主体多、交易机制复杂和交易管理困难等特点[2],会产生信任缺失、恶意篡改和虚假交易等问题,而区块链技术可以有效解决上述问题。因此,本文

到稿日期:2022-03-14 返修日期:2022-06-07
基金项目:中央高校基本科研业务费专项资金(2020ZDPY0306);徐州市科技计划项目(KC21044)
This work was supported by the Fundamental Research Funds for the Central Universities of Ministry of Education of China(2020ZDPY0306)and Xuzhou Science and Technology Program(KC21044).
通信作者:姜顺荣(jsywow@163.com)

提出了基于区块链的能源交易系统概念。图 1 为将区块链技术与现有智能电网结合的架构图，其中用户通过安装的光伏或风力发电设施发电，并将多余的电量传输给智能电站，同时智能电站通知管理中心转账；当附近电力短缺的用户向管理中心发送交易请求时，管理中心会通知智能电站输电。智能电站调度电力，管理中心管理转账交易数据，彼此协作完成交易。此外，还可以通过大型传统发电站向智能电网输电的方式，来解决系统中存在的电力缺失和负载不均的问题。总体来说，基于区块链的能源交易系统作为智能电网的一部分，可以提供更低廉、更环保的能源。

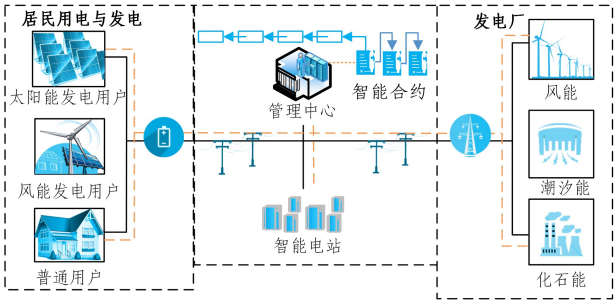


图 1 基于区块链的智能电网架构图

Fig. 1 Diagram of blockchain-based smart grid architecture

通过区块链技术实现可信分布式能源交易也存在各式各样的挑战，因为链上交易数据是公开透明的、可追溯的[3]，攻击者可以根据某用户的交易数据，使用连接攻击[4]、差分攻击[5]或数据挖掘[6]等方法来分析推测出此用户的隐私信息（家用电器使用情况、生活习惯、出行规律等），甚至危及到用户的生命财产安全。因此，迫切需要为其设计一种安全高效的隐私保护方案。

根据数据处理方式的不同，能源交易数据的隐私保护方案主要可以分成两类：基于限制发布和基于密码学[7]。基于限制发布的方法主要包括数据隔离和链下存储[8-9]，其通过公开部分数据或向部分人公开数据的方式来达到保护隐私的目的。但是，如何验证未公布数据，保证数据未被篡改是亟待解决的问题。基于密码学的方法主要包括数据加密和数据失真。数据加密是利用密码学算法将交易数据加密以实现只有权限用户才能查看数据的目的[10]。例如，使用零知识证明命题代替公开透明的交易数据，来解决交易数据泄露隐私的问题，同时使用 zk-SNARKs 算法来验证交易[11]，但该方案的查询和验证效率极低。数据失真是在保证交易数据可用性的同时向交易数据中添加噪声来保护隐私。例如，Hassan 等[12]为基于区块链的微电网系统设计了满足差分隐私的能源拍卖算法，使能源拍卖更加安全和私密。该类方案既能保证区块链的公开透明和不可篡改性，又有较高的查询和验证效率。但中心差分隐私需要一个可信的第三方来处理数据，存在对第三方进行攻击导致隐私泄露的风险。此外，可以通过账户映射技术生成虚拟账户/关联账户，并将其作为账户噪声来掩盖用户的交易趋势和交易记录的特征，预防连接攻击[13-14]。但该方案产生的账户会出现分布不均的情况，导致账户资源的浪费。

本文使用本地差分隐私算法来保护交易数据的隐私。为了隐藏公开能源交易数据的交易特征，使用 AM 技术映射多个关联账户分割数据，接着对多个关联账户使用 BLDP 算法，在保证交易正确的同时使交易数据失真，最终达到保护能源交易数据隐私信息的目的。本文工作的主要贡献在于：

(1)为 BLDP 算法重新设计了本地用户数据扰动机制，满足了交易数据查询与验证操作的隐私要求以及区块链不可篡改、公开透明的特性，并结合 AM 技术保证了交易的正确性。

(2)通过在各关联账户中使用 ESP 算法确定交易数据的方式来抑制交易曲线波动，以达到隐藏交易数据特征的目的。

(3)结合 BLDP 算法、AM 技术和 ESP 算法设计了 BLDP-AM 方案，并将其应用到基于联盟链的能源交易系统中，既保护了能源交易数据的隐私又具有较高的数据查询与验证效率。

(4)证明了 BLDP 算法满足ε-差分隐私，并采用真实数据集，通过实验验证了 BLDP-AM 方案具有较高的可行性和较好的性能。

2 相关工作

在基于区块链的能源交易系统中，为了保护通信和交易过程中的隐私信息，Dorri 等[15]提出了一种使用可行性高的节点形成骨干网络，同时将公钥作为骨干网络通信标识符的方法。该方法通过多个骨干网络节点的公钥来保证普通节点的匿名性。Samuel 等[16]通过联盟链保证信息透明，以解决生产者之间存在争议的滞期费问题，同时使用加法同态加密技术保护生产者交易数据的隐私。Laszka 等[17]提出了一种混合服务机制，将生产的能源随机转移到生产者随机生成的多个匿名地址中，使得攻击者无法通过混合的资产数据追溯到原始的生产者信息。Garg 等[18]设计了一种基于区块链的椭圆曲线加密分层认证方案，可以实现在能源交易时不同实体之间的相互匿名认证。Guan 等[19]为了保护小组内部的用户隐私，允许每个用户使用不同的假名提交自己的能耗数据，并使用 Bloom 过滤器进行快速认证。

上述方案虽然可以有效解决因交易数据被窃取或篡改而导致的隐私泄露问题，但是攻击者仍然可以针对公开交易数据使用交易特征分析或数据挖掘等方法获得相关隐私信息。为了保护能源交易数据中的隐私信息，可以使用访问控制技术控制数据访问权限，Lu 等[20]采用 CP-ABE 构建了一种基于区块链的隐私保护能源交易方案 PP-BCTS，该方案通过密文形式的交易仲裁来实现细粒度的访问控制。此外，也可以使用差分隐私技术在保证数据可用性的同时使交易数据失真，Barbosa 等[12]使用差分隐私算法来保护能够反映某用户电器具体使用情况的智能电表隐私数据。Gai 等[13]通过账户映射技术生成虚拟账户以产生噪声，并通过加入的账户噪声掩盖用户的交易趋势和交易特征。Hassan 等[21]提出了一种基于区块链的微电网能源拍卖策略，并使用差分隐私保护个人的出价及交易数据隐私。Ou 等[22]将奇异频谱分析应用于本地差分隐私，针对智能电表的时间序列数据的隐私问题提出了 SSA-LDP 隐私保护方案。Li 等[23]提出了一种基于差分隐私的在线双重拍卖方案，并将其应用于电动汽车充电拍卖市场。该方案可以在拍卖过程中保护参与者的敏感信息。

3　预备知识

3.1　Fabric 联盟链

联盟链是多个机构共同参与管理的区块链，适用于具有多个交易实体的联盟。Fabric 联盟链具有诸多优点：1）Fabric 是许可链，参与者彼此了解，并不是完全匿名或完全不信任的关系，这在一定程度上缓解了信任缺失的情况；2）Fabric 使用通道技术实现不同组织共享不同的分布式账本，交易方必须通过验证才能与账本进行交互，一定程度上保证了账本的隐私。

3.2　差分隐私

差分隐私是一种数据隐私保护方法，通过在数据中添加噪声的方式，尽可能地在保证数据准确性的同时保护数据的隐私[24]。目前，差分隐私算法主要应用于频率估计、均值估计和 Top-k 等方面[25-27]，且根据添加噪声的位置，可以分成中心差分隐私和本地差分隐私[28]。如图 2 所示，中心差分隐私通过可信的第三方数据收集者对数据分析结果进行隐私化处理；本地差分隐私技术使每个用户能够独立地对个体数据进行隐私化处理，因此不再要求第三方可信，避免了针对第三方的隐私攻击。差分隐私算法涉及的定义与定理的描述如下。

定义 1（邻近数据集）　如果存在两个数据集 D 和 D'，它们相差的元素数目 Δ 可以由式(1)计算得到：

$$\Delta=|D\oplus D'| \tag{1}$$

当且仅当 $\Delta=1$ 时集合 D 与集合 D' 为邻近数据集。

定义 2（ε-差分隐私）　对于邻近数据集 D 与 D'，当且仅当操作函数 f 的任意输出 $O\in Range(f)$ 满足式(2)时，函数 f 满足 ε-差分隐私。

$$Pr[f(D)=O]\leqslant \exp(\varepsilon)\cdot Pr[f(D')=O] \tag{2}$$

其中，$Pr[\cdot]$ 表示 $f(D)=O$ 的概率；ε 表示隐私预算。如果 f 的输出是连续的，那么概率函数将替换为概率密度函数。

定义 3（全局敏感度）　对于函数 $f:D\rightarrow R^k$ 的全局敏感度 Δf 的定义如式(3)所示：

$$\Delta f=\max_{D\sim D'}\| f(D)-f(D')\|_1 \tag{3}$$

其中，$\|\cdot\|$ 为 L_1 范式。

定义 4（拉普拉斯机制）　对于函数 $G:D\rightarrow R^n$，拉普拉斯机制通过式(4)实现(ε，0)-差分隐私。

$$F(D)=G(D)+\eta \tag{4}$$

其中，η 为随机向量且各元素服从拉普拉斯分布，即 $\eta_i\sim Lap(\Delta f/\varepsilon)$。

定理 1（并行组合原理）　$f_1(D_1)$，$f_2(D_2)$，…，$f_m(D_m)$ 分别表示输入数据集为 D_1，D_2，…，D_m 的一系列满足 ε-差分隐私的算法，且任意两种算法的随机过程相互独立，则这些算法的组合算法也满足 ε-差分隐私。

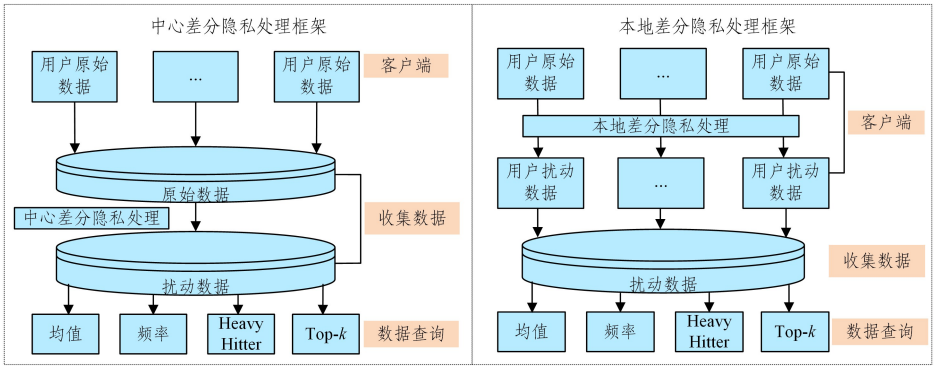


图 2　中心和本地差分隐私数据处理框架

Fig. 2　Central and local differential data processing framwork

4　系统模型与攻击模型

本文方案使用的符号描述如表 1 所列。

表 1　方案中使用的符号

Table 1　Symbols used in our scheme

符号	含义
S/B	某个出售电力的用户/购买电力的用户
M/E	管理中心/智能电站(管理交易/调度电力)
SA/BA	S/B 的映射关联账户集合
SAE^i/SAR^i	S 的各账户的预测值/真实值集合
SAEi a/SAEi in	活跃账户/不活跃账户的预测值集合
←	为账户赋值
↔	等价即两边符号代指同一事物
⊕	异或
→	传输数据或输送电量

4.1　系统模型

首先根据区域将用户分成不同的组织，每个组织都有一个管理中心和智能电站，如图 3 所示。

邻近能源交易模式可以保证交易用户属于同一个组织，是比较可信的，这可以大幅减少恶意交易的发生。本文设计的系统模型实体主要包括监管中心、管理中心、智能电站和交易用户 4 个部分。

(1)监管中心具有颁发证书、设置权限、监管交易、发行代币等功能，并且监管着各节点的交易行为，若发现违规操作，则会通过终止授权的方式，将违规节点从交易网络中剔除。监管中心同时具有发行代币的功能，通过监管能源交易市场决定发行代币的数量，维持代币的价值。

(2)管理中心 M 和智能电站 E 属于同一个组织，它们彼此协同，根据智能合约与用户进行交易。每次交易中，管理中心都会运行 BLDP-AM 方案来保护原始交易数据的隐私。此外，它们具有从大型集中发电站调度电量实现系统负载均衡的功能。

(3)交易用户可以分成卖家 S 和买家 B，它们都是交易用户的一种身份，同一用户可以根据自己的需求选择一种身份

出售或购买电力。售电：S 向 E 发出售电请求并向 E 输电，E 收到请求与电力后，M 转账给 S。购电：B 向 M 发送买电请求并向 M 转账，M 收到请求与转账后，E 向 B 输电。

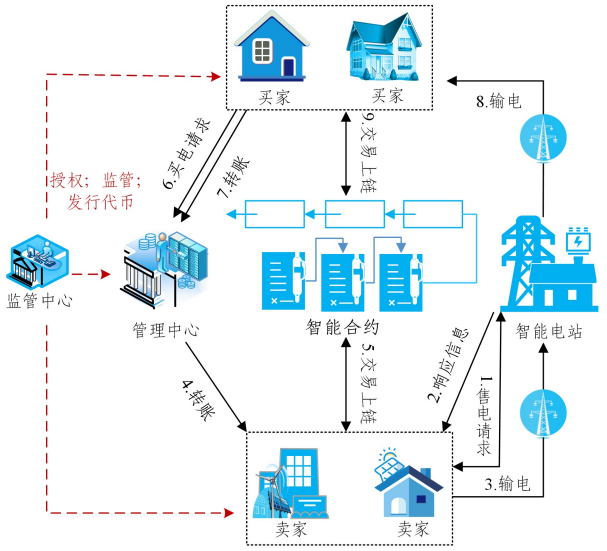


图 3 基于联盟链的能源交易系统流程图

Fig. 3 Flow chart of energy trading system based on consortium blockchain

4.2 攻击模型

由于链上能源交易数据公开透明的特性，受到连接攻击、差分攻击或数据挖掘攻击时，极易泄露用户的隐私信息。

(1)对于连接攻击，假设攻击者拥有多个数据源，例如链上交易数据和链下能源分配数据等，攻击者可以通过特征分析法分析出各数据源的数据特征，然后根据这些特征利用连接攻击理论分析发现各数据源与目标数据之间的关系，最终获得数据源背后隐藏的隐私信息。

(2)对于差分攻击，假设攻击者知道交易系统中某个区域所有用户的基本信息，以及部分用户的能源交易数据，虽然该区域的用户是匿名交易的，通过加密算法隔离了交易数据与匿名用户之间的关系，但由于所有的交易数据都是公开透明且可以被追溯的，因此攻击者仍然可以通过比较匿名的交易数据与已知的部分用户能源交易数据，来分析其中的差异性，最终得到用户的隐私信息。

(3)对于数据挖掘，随着交易的进行，交易数据量会逐渐增多，假设交易数据量达到了可以创建数据挖掘模型的程度，攻击者就可以通过数据挖掘算法，如 C4.5 决策树算法、朴素贝叶斯算法等，从大量的交易数据中分析推断出用户的隐私信息。

5 BLDP 算法

本地差分隐私算法的主要思想是在用户数据收集阶段扰动数据，其数据扰动机制大多基于随机响应实现，每次查询都要重新响应数据并消耗隐私预算，从而避免发生用户通过多次查询获得结果的概率分布，进而导致泄露数据隐私的情况。

在基于区块链的能源交易系统中，我们将区块链抽象成第三方，各用户能源交易数据上链等价于第三方收集数据，所有扰动后的能源交易数据构成了扰动数据集 D'。用户对公开能源交易数据的主要操作为查询或验证某个用户的具体数据，即 $Q(D')$。

然而，区块链交易数据具有不可篡改的特性，因此无法使用随机响应的方式扰动上链的用户能源交易数据；同时，区块链具有公开透明的特性，无法通过隐私预算限制用户的查询次数，因此需要重新设计满足区块链需求的本地差分隐私算法，即 BLDP 算法。

5.1 本地用户数据扰动机制

本地差分隐私算法最重要的部分是设计合适的本地用户数据扰动机制。我们假设本地用户响应数据 x 是可分的，分成 n 份，此时 x 可以看作一个含有 n 个元素的数据集 X，那么根据定义 1，可以得到 X 的邻近数据集 X'。在数据集上的操作函数 f 为求和函数，即 $f(X)=\sum_{i=0}^{n}X[i]=x$，$f(X')=\sum_{i=0}^{n}X'[i]=x'$。根据定义 3 可知，全局敏感度为：

$$\Delta f=\max_{X\sim X'}\| f(X)-f(X')\|_1 \tag{5}$$

考虑极限情况，即集合 X 中的某个元素 $X[i]=x$，其余元素的值为 0，并且集合 X' 和 X 相差的元素为 $X[i]$，根据式(5)可知 $\Delta f=x$。根据定义 4，我们针对 $f(X)\leftrightarrow x$ 加入服从拉普拉斯分布的噪声实现对本地用户数据的扰动，即：

$$x'=x-(x/\varepsilon)*\mathrm{sign}(\alpha)*\ln(1-2|\alpha|) \tag{6}$$

其中，α 服从标准均匀分布。

5.2 隐私分析

本节通过隐私分析来证明 BLDP 算法满足差分隐私。首先证明本地用户数据扰动机制满足差分隐私，根据定义 4 可知：

$$\forall y\in Range(f),\frac{Pr(f(X)=y)}{Pr(f(X')=y)}=\frac{pdf(y-f(X))}{pdf(y-f(X'))}$$

其中，$pdf(\cdot)$ 是服从拉普拉斯分布的概率密度函数。因为 $f(X)=x$ 且 $f(X')=x'$，所以：

$$\begin{aligned}\frac{pdf(y-f(X))}{pdf(y-f(X'))}&=\frac{pdf(y-x)}{pdf(y-x')}\\&=\frac{(1/2b)*\exp((-|y-x|)/b)}{(1/2b)*\exp((-|y-x'|)/b)}\\&=\exp(\frac{|y-x'|-|y-x|}{b})\\&\leqslant\exp(\frac{|x-x'|}{b})\end{aligned}$$

由定义 3 可知：

$$\begin{aligned}\Delta f&=\max_{X\sim X'}\| f(X)-f(X')\|_1\\&=\max_{x\sim x'}\| x-x'\|_1\\&=\max_{x\sim x'}|x-x'|\\&\geqslant|x-x'|\end{aligned}$$

又因为 $b=\Delta f/\varepsilon$，所以：

$$\frac{Pr(f(X)=y)}{Pr(f(X')=y)}\leqslant\exp(\frac{|x-x'|}{b})\leqslant\exp(\frac{\Delta f}{b})=\exp(\varepsilon)$$

根据定义 2 可知，本地用户数据扰动机制满足式(2)，满足 ε-差分隐私。

接着证明 $Q(D')$ 查询或验证操作结果满足差分隐私。由于集合 $D'=\{X_1',X_2',\cdots,X_m'\}$，因此对集合 D' 的查询或

验证操作 $Q(D')=\{f(X_1'),f(X_2'),\cdots,f(X_m')\}$，由定理 1 的差分隐私组合定理可知，$Q(D')$ 满足 ε-差分隐私。

最后，证明 BLDP 算法满足区块链需求。BLDP 算法使用本地用户数据扰动机制对数据加噪后上链公开，用户每次查询都会得到相同的扰动数据，多次查询不会导致隐私预算增加。因此，BLDP 算法既可以满足区块链不可篡改的特性，又不会破坏区块链公开透明的特性。

6　能源交易流程及 BLDP-AM 方案

本节将介绍基于联盟链的能源交易系统的交易流程及 BLDP-AM 隐私保护方案，具体可以分成以下 3 个部分。

6.1　初始化

初始化基于联盟链的能源交易系统的步骤如下：

(1)监管中心联合不同区域的管理中心和智能电站构成的组织，并根据配置文件生成通道和创世区块。

(2)监管中心为各组织成员生成符合 X.509 标准的证书文件，其中包括使用椭圆曲线加密算法生成的公私钥，然后将各个组织加入到通道中构成交易网络。M 的信息标记为 $Id(cert_M(pk_M,sk_M),adr_M)$，$E$ 的信息标记为 $Id(cert_E(pk_E,sk_E),adr_E)$，其中 $cert_i$ 代表实体 i 证书文件，pk_i 代表实体 i 公钥，sk_i 代表实体 i 私钥，adr_i 代表实体 i 地址。

(3)用户向某组织提交注册请求，该组织同意后向监管中心发送消息，监管中心收到消息后使用椭圆曲线加密算法为其生成一组公私钥，同时为用户生成符合 X.509 标准的证书文件。卖家 S 的信息标记为 $Id(cert_S(pk_S,sk_S),adr_S)$，买家 B 的信息标记为 $Id(cert_B(pk_B,sk_B),adr_B)$。最后将 Id 信息返回给用户。

6.2　交易流程

如图 3 所示，以售电交易流程为例。

(1)S 向 E 发送交易请求 $req(adr_s,msg_s)$，并用 E 的公钥加密，即：

$$S\rightarrow E:En(pk_E,req(adr_s,msg_s)) \tag{7}$$

(2)在 E 收到信息后用私钥 sk_E 解密，如果 E 同意请求，则会根据 msg_s 中交易电量 V_S、电力与代币间汇率 r 等因素计算出需要转账的代币量 T。E 将响应信息发送给 S，响应信息包括交易许可、代币量等。具体过程如式(8)所示：

$$\begin{aligned}&De(sk_E,En(pk_E,req(adr_s,msg_s)))\\&T=Cal(V_s,r)\\&E\rightarrow S:En(pk_s,(T,1))\end{aligned} \tag{8}$$

其中，$Cal(\cdot)$ 为电力和代币转换函数，1 代表同意交易信号。

(4)S 接收到 E 的同意交易的响应信息后，如果同意交易方案，则向 E 传输电力，即 $S\rightarrow E:V_s$。

(5)E 收到 S 的电力后，通知 M 向 S 转账。在转账时 M 将使用 BLDP-AM 方案保护交易数据的隐私。

6.3　使用 BLDP-AM 方案保护交易数据隐私

若将 M 向 S 或 B 向 M 转账的原始交易数据直接公开，攻击者则可根据原始交易数据轻易得到交易趋势、发电量和用电量等隐私信息，因此不能直接将原始交易数据公开上链。

6.3.1　保护卖方 S 的交易数据隐私

图 4 给出了在管理中心 M 向卖方 S 转账过程中使用 BLDP-AM 方案保护数据隐私的流程，具体描述如下。

(1)M 使用 S 的公钥加密转账数据，包括代币量 T^i、M 地址 adr_M 等，并将加密数据发送给 S，其中 i 表示交易编号。

(2)S 接收到加密数据后使用私钥解密得到转账数据，并使用 BLDP-AM 方案处理转账数据。

1)根据联盟链的性质，用户 S 可以拥有多个关联账户，用集合 SA 表示，且可以通过监管中心申请或撤销账户。本文使用 AM 技术将多个关联账户的转账权限映射成组合键，以便用户操作。

2)为了抑制交易曲线波动，隐藏交易数据特征，本文根据历史交易数据采用一次指数平滑预测算法，来预测 SA 中的每个账户的交易预测值 SE_k^i，并构成集合 $SAE^i=\{SA_1:SE_1^i,SA_2:SE_2^i,\cdots,SA_k:SE_k^i,\cdots\}$，其中 k 为账户编号。由于通过一次指数平滑预测算法得到的预测值无明显变化趋势，因此如果用户 S 的各账户根据预测值进行交易，则可以隐藏交易数据的部分特征。ESP 算法的计算式如下：

$$SE_k^i=\theta*SE_k^{i-1}+(1-\theta)*SR_k^{i-1} \tag{9}$$

其中，$\theta\in(0,1)$ 为常数，SR_k^{i-1} 为真实交易值。

3)当 S 的各账户依据集合 SAE^i 进行交易时，会导致 SE_k^i 的值不变，攻击者可能依此分析出关联账户间的关系，从而泄露用户隐私；同时，指数平滑预测算法是有迹可寻的，攻击者可以使用差分攻击或数据挖掘方法来获得用户隐私信息。为此，本文使用 BLDP 算法扰动集合 SAE^i 中的各账户交易预测值 SE_k^i，得到交易真实值 SR_k^i，并构成真实交易值集合 $SAR^i=\{SA_1:SR_1^i,SA_2:SR_2^i,\cdots,SA_k:SR_k^i,\cdots\}$。

(3)使用 M 公钥加密新的转账数据 SAR^i 并发送给 M。M 收到加密数据后使用私钥解密并验证新的转账数据的合法性(交易数据是否正确)，如果合法则进行交易，否则向 S 响应错误信息。S 收到错误信息响应后重新使用 BLDP-AM 方案处理转账信息，直到交易成功。

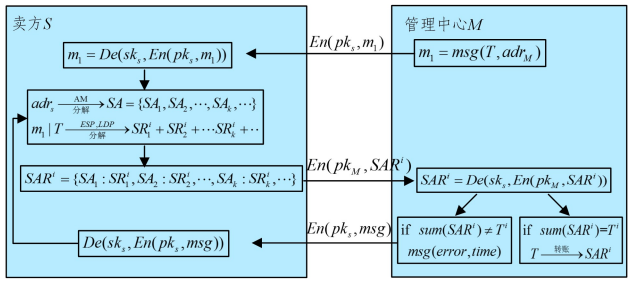


图 4　M 向 S 的转账流程图

Fig. 4　Flow chart of transfer from M to S

6.3.2　BLDP-AM 方案的实现细节

图 5 给出了 BLDP-AM 方案实现的具体流程，详细描述如下。

(1)根据交易预测值 SE_k^i 对 SAE^i 进行降序排序。

(2)遍历 SAE^i，根据交易预测值从大到小选取元素 $SA_k:SE_k^i$，令 $v=SE_k^i$，并重复执行以下步骤：

1)对 v 进行本地差分隐私处理，得到：

$$BLDP(v)=v+Laplace(v/\varepsilon) \tag{10}$$

2)如果 $T^i\geqslant BLDP(v)$，则：

$$T^i = T^i - BLDP(v)$$
$$SR_k^i = BLDP(v) \tag{11}$$
$$SA_k \leftarrow GetState(SA_k) + SR_k^i$$

(3)如果 $T^i < \mathrm{BLDP}(v)$,则:

$$SR_k^i = T^i, SR_{other}^i = 0 \tag{12}$$

(4)所有的 $SA_k : SR_k^i[\cdot]$ 值构成集合 SAR^i。

但上述分配方法存在两个问题:1)账户较多时,T^i 不能分配到所有账户;2)账户较少时,所有账户分配完后,T^i 还有盈余。

针对问题 1),将 SAE^i 分成活跃账户集合和不活跃账户集合,分别标记为 $SAE_a^i = \{\cdots, SA_m : SE_{a,m}^i, \cdots\}$ 和 $SAE_{in}^i = \{\cdots, SA_n : SE_{in,n}^i, \cdots\}$,即 $SAE^i = SAE_a^i \cup SAE_{in}^i$。如果 $SR_k^i = 0 \&\& SR_k^{i-1} = 0$,则 $SA_k : SE_k^i \in SAE_{in}^i$;如果 $SR_k^i > 0$,则 $SA_k : SE_k^i \in SAE_a^i$。在转账 T^i 代币时,只考虑集合 SAE_a^i,即在步骤(1)中用 SAE_a^i 替代 SAE^i。该方法有两个优点:1)集合变小,可以减小计算开销,提高交易效率;2)交易系统中含有活跃度较低的用户,集合 SAE_{in}^i 中的不活跃账户可以保护系统中活跃度较低的用户的隐私。

针对问题 2),在集合 SAE_a^i 中所有活跃账户分配完毕后,如果 $T^i > 0$,则检查 SAE_{in}^i 是否为 $\emptyset$。如果 $SAE_{in}^i \neq \emptyset$,则从 SAE_{in}^i 中随机选取一个账户并到 SAE_a^i,并将剩余代币 T^i 转给该账户,即:

$$SR_n^i = T^i, SE_{in,n}^i \in SAE_a^i$$
$$SA_n \leftarrow GetState(SA_n) + T^i \tag{13}$$

如果 $SAE_{in}^i = \emptyset$,则生成新账户并使用 AM 技术将新账户的转账权限映射到用户组合键,同时将新账户并到 SAE_a^i,并将剩余代币 T^i 转给新账户,即:

$$SR_{\mathrm{new}}^i = T^i, SE_{\mathrm{new}}^i \in SAE_a^i$$
$$SA_{\mathrm{new}} \leftarrow T^i \tag{14}$$

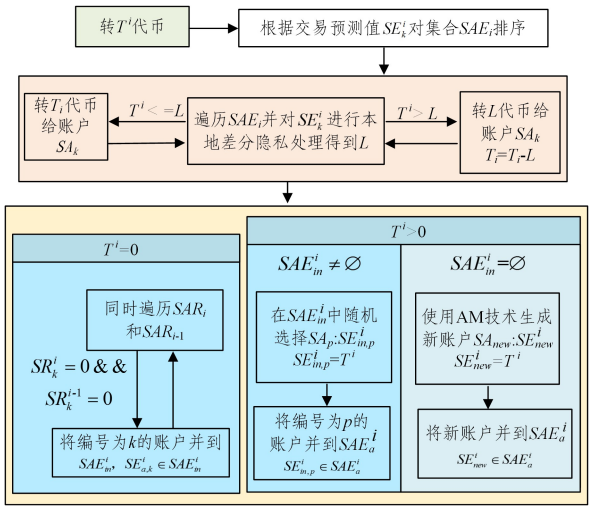


图 5 BLDP-AM 方案的实现流程图

Fig. 5 Realization flow chart of BLDP-AM scheme

6.3.3 保护买方 B 的交易数据隐私

在基于联盟链的能源交易系统中,S 购买能源时身份将转为 B,即集合 $SA \leftrightarrow BA$,在 B 向 M 转账 T^i 代币时,流程如下。

(1)遍历集合 SAE_m^i,选取账户 SA_k 作为支付账户。如果 $T^i > GetState(SA_k)$,则:

$$T^i = T^i - GetState(SA_k), SA_k \leftarrow 0 \tag{15}$$

(2)如果 $T^i > 0$,则从集合 SAE_a^i 中选取账户进行支付,交易完成后撤销集合 SAE_{in}^i 中所有的零账户,即 $GetState(SA_k) = 0$ 的账户。

算法 1 账户交易值预测 ESP 算法

输入:(v, T^1, θ)

输出:(v_i^e)

1. 初始化:$v_1^e \leftarrow v, v_1^r \leftarrow T^1$ /* v_1^e 为第 1 笔交易预测值;v 为用户所在区域每笔交易平均值;T^1 为用户的第 1 笔交易值;v_1^r 为第 1 笔交易真实值 */;
2. for j←2 to i
3. $\quad v_j^e = \theta * v_{j-1}^e + (1-\theta) * v_{i-1}^r$ /* 参数 $\theta \in (0,1)$ */;
4. $\quad$ j++;
5. end for
6. return v_i^e /* 第 i 笔交易预测值 */.

算法 2 BLDP 本地数据扰动算法

输入:(v_i^e, ε)

输出:$(L(v_i^e))$

1. 将 v_i^e 随机分成 n 份,构成数据集 X / * v_i^e 为用户的第 i 笔交易预测值 */;
2. 根据 $|X \oplus X'| = 1$ 得到 X 的邻近数据集 X';
3. 计算全局敏感度 $\Delta f = \max_{X \sim X'} \| f(X) - f(X') \|_1$ /* f 为求和函数 */;
4. $\alpha = \mathrm{Random}()$ /* 随机 */;
5. $L(v_i^e) = v_i^e - (\Delta f/\varepsilon) * \mathrm{sign}(\alpha) * \ln(1 - 2|\alpha|)$;
6. return $L(v_i^e)$ /* 扰动后的本地数据 */.

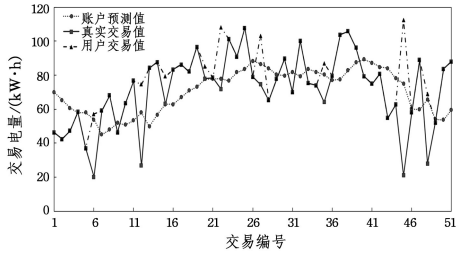
7 实验分析

本文使用真实数据集对所提方案的可行性和性能进行评估。该实验在 Hyperledger Fabric 2.0 上实现并运行,实验环境是 AMD Ryzen 5 3 400 GB with Radeon Vega Graphics 3.70 GHz, 16.0 GB RAM, Ubuntu18.04 系统。进行实验的能源交易系统具有两个组织,每个组织有两个 peer 节点和一个 ca 节点,同时系统具有 1 个 order 节点。实验使用的数据来自 Ausgrid 电网中随机选取的 300 位客户在 2012 年 7 月 1 日至 2013 年 6 月 30 日期间,每天通过太阳能发电系统产生电量构成的数据集,包括用户编号、日期、总发电量等属性。

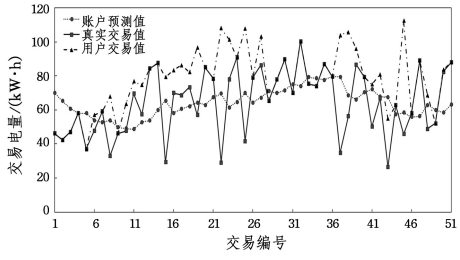
7.1 ε 对隐私强度的影响

本文使用了 BLDP 算法,在进行实验之前,需要选取合适的隐私预算 ε。如图 6 所示,横坐标表示该用户的交易编号;纵坐标表示交易的电量。其中账户预测值是该用户关联映射账户使用 ESP 算法根据历史交易数据预测得到的交易值。图中的账户预测值曲线没有较大波动,可以有效地隐藏该账户的交易特征。真实交易值是 BLDP 算法对账户预测值扰动后的数据,也是最终上链的交易数据。用户交易值代表该用户交易总值等价于其所有关联账户真实交易值之和。如图 6 所示,当 $\varepsilon = 0.1$ 时,账户交易值曲线与用户交易值曲线重合较多,攻击者可以根据真实交易值曲线推断出用户交易特征,

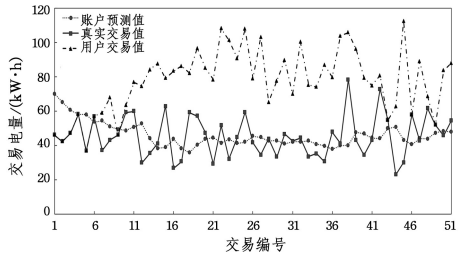
影响隐私保护强度，因此 ε 值不能过小。当 ε 过大时，隐私保护强度也会减弱，例如当 ε＝2.0 时，真实交易值曲线在账户预测值曲线附近波动，波动幅度较小，隐私保护强度较低。当 ε＝1.0 时，真实交易值曲线有较大的波动幅度且与用户交易值曲线重合较少，因此具有较高的隐私保护强度。大量实验结果表明，当 ε∈(0.5，1.5)时，BLDP-AM 方案的隐私保护效果最好，本文实验的隐私预算 ε＝1.0。



(a)隐私预算 ε＝0.1



(b)隐私预算 ε＝1.0



(c)隐私预算 ε＝2.0

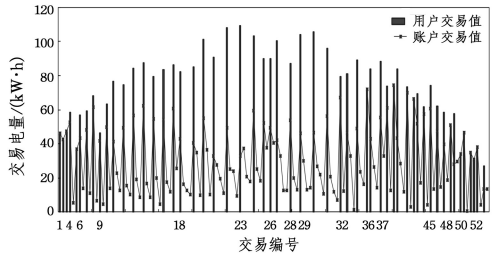
图 6　隐私预算 ε 对隐私保护强度的影响

Fig. 6　Impact of privacy budget ε on privacy-preserving strength

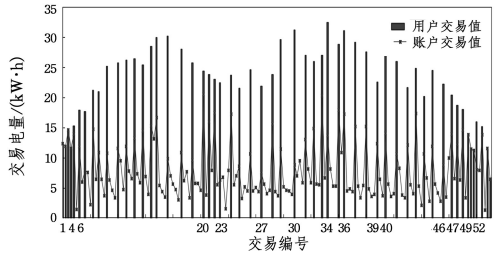
7.2　可行性评估

本节首先根据某用户的账户值变化情况，分析并评估了 BLDP-AM 方案在隐私保护方面的可行性。接着将该方案与 PBT 方案[13]对比，从多用户的账户分布情况和隐私保护强度方面评估了该方案的隐私保护可行性。最后将 BLDP-AM 方案与多个隐私保护方案进行比较，从是否可以隐藏交易特征、是否可以预防各种外部攻击等方面来评估 BLDP-AM 方案的安全可行性。

选取交易数据特征不同的两个用户进行实验，实验结果如图 7 所示。图 7 中，横坐标代表用户交易编号，纵坐标代表每笔交易的电量。用户交易值是原始数据，包含大量的用户隐私信息；而账户交易值是最终上链数据。用户交易值柱状图之间的账户是该用户的活跃账户。如柱状图所示，用户 1 的交易值曲线只有一个峰，而用户 2 的交易值曲线有两个峰和一个谷。当使用 BLDP-AM 方案时，最终公布的交易数据如折线图所示，账户交易值曲线并没有明显的峰谷特征或其他可能泄露用户隐私的特征。因此，BLDP-AM 方案将账户交易值上链，从根本上隐藏了用户交易值的特征，进而保护了原始数据中的隐私信息。



(a)用户 1



(b)用户 2

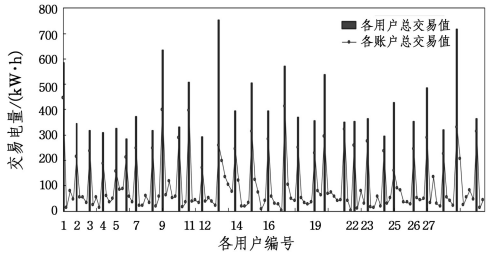
图 7　两个用户的账户交易数据的变化情况

Fig. 7　Changes in account trading data of two users

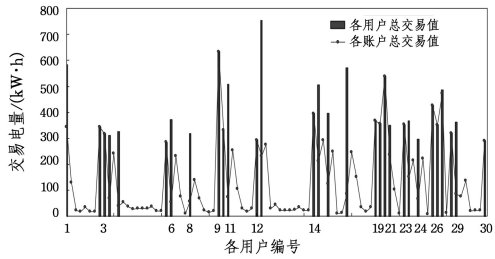
其次，以 3 个月为周期选择 30 组用户进行实验并与 PBT 方案进行比较，根据各用户总交易值与各账户总交易值的分布情况和隐私保护强度，来评估两个方案的隐私保护可行性。如图 8 所示，横坐标代表各用户编号，纵坐标代表 3 个月内交易的电量，柱状图之间的账户就是用户的关联映射账户。如图 8(a)所示，各用户的总交易数据与经过 BLDP-AM 方案处理后得到的各账户的总交易数据之间没有明显关系，攻击者通过上链的交易数据很难得到各用户交易数据中的隐私信息。为了保证交易的准确性，用户的总交易值与其所有账户的总交易值之和相等，这是用户交易数据和账户交易数据之间的唯一联系。然而，在众多账户中找到某用户的所有账户是困难的，甚至是不可能的，因此该方案的隐私保护强度较高。如图 8(b)所示，能源交易系统使用 PBT 方案可以隐藏各用户的交易特征以及交易数据中的部分隐私信息，但根据实验结果可知，该方案并不能完全隐藏各用户的交易特征，如图中编号为 2，3，4 的用户交易特征没有被完全隐藏。此外，PBT 算法的账户映射机制不够完善，如图中编号为 5 的用户映射了 11 个新账户，而编号为 6 的用户没有映射新账户。账户分布不均会导致某些用户的隐私保护强度过高，而某些用户的隐私保护强度过低，在增加账户开销的同时没有达到相应的隐私保护效果，降低了方案的可行性。BLDP-AM 方案的账户映射机制较为完善，各用户的账户分布均衡，实现了用户隐私和开销之间的平衡，有较高的可行性。

最后通过比较 BLDP-AM 方案与其他隐私保护方案的安全性来评估其安全可行性，结果如表 2 所列。我们主要从是否隐藏了交易特征、是否可以预防基于理论的连接攻击和基于语义的连接攻击、是否可以预防差分攻击和数据挖掘方面来比较各个方案的安全性。根据实验结果可知，本文方案

可以有效防御上述所有攻击，安全可行性较高，而其他方案只能防御部分攻击，安全可行性较低。表 2 中，“√”代表可以防御，“×”代表不可防御。BLDP-AM 方案可以有效防御表中所有假设攻击的主要原因为：1）最终上链的不是原始交易数据，并且该方案没有使用任何语义技术连接原始交易数据和公布的交易数据，因此连接攻击不可能得到原始交易数据中隐藏的隐私信息；2）使用 BLDP 算法处理交易数据，可以有效预防差分攻击；3）BLDP 算法处理数据的结果具有随机性，且由于区块链技术的交易数据具有不可篡改的特性，本文差分隐私算法的扰动结果也不会随着查询而改变，因此可防止发生通过多次查询得到数据分布从而泄露隐私的情况，进而可以有效地预防数据挖掘。



(a)BLDP-AM 方案 30 组用户



(b)PBT 方案 30 组用户

图 8 BLDP-AM 和 PBT 方案的多组用户的账户分布情况

Fig. 8 Account distribution of multiple groups of users in BLDP-AM and PBT schemes

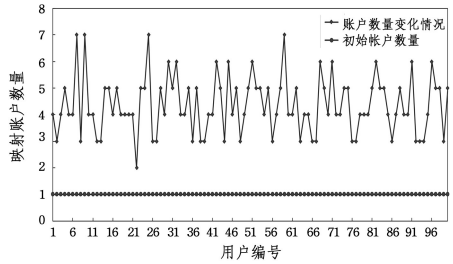
表 2 BLDP-AM 方案与其他隐私保护方案的比较

Table 2 Comparison of BLDP-AM scheme with other privacy-preserving schemes

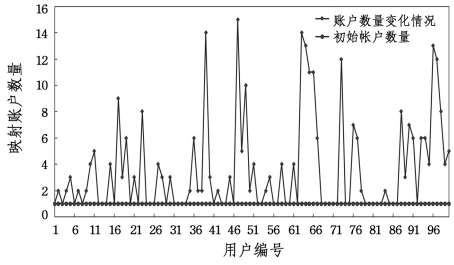
方案	交易特征	基于理论的连接攻击	基于语义的连接攻击	差分攻击	数据挖掘
BLDP-AM	√	√	√	√	√
Barbosa[12]	×	×	×	√	√
Gai[13]	√	√	√	×	×
Hassan[21]	×	√	×	√	×
Ou[22]	×	×	×	√	√
Li[23]	×	√	√	√	×

7.3 性能评估

本节从账户资源利用率、时间开销和每秒处理交易数(Transactions Per Second，TPS)3 个方面评估了 BLDP-AM 和 PBT 方案的性能。图 9(a)给出了使用 BLDP-AM 方案的 100 组用户 3 个月内的账户数量变化情况。从图中可知，用户的账户数量平均为 4.36 个，且分布较为均匀，同时 BLDP-AM 方案具有账户回收机制，可以实现账户数量的动态平衡，充分利用账户资源，提高 BLDP-AM 方案的性能。图 9(b)给出了使用PBT方案的100组用户3个月内的账户数量变化情况。从图中可知，各用户的账户数量变化情况有很大差异，有些用户的账户数量很多，但有些用户的账户数量没有变化，随着交易的进行可能出现某些用户拥有过多的账户而某些用户还只有一个账户的情况，使得账户分布严重不均，导致账户资源浪费，降低账户资源的使用效率，影响 PBT 方案的性能。



(a)BLDP-AM 方案账户数量变化



(b)PBT 方案账户数量变化

图 9 BLDP-AM 和 PBT 方案的账户数量变化情况

Fig. 9 Changes in number of accounts for BLDP-AM and PBT schemes

基于联盟链的能源交易时间开销如图 10 所示，其展示了在能源交易系统拥有不同用户数量时，使用 BLDP-AM 和 PBT 方案进行交易的时间开销情况。横坐标代表用户数量，测试数据在[10，100]之间并以 10 为间隔，纵坐标是交易时间开销。从图中可知，BLDP-AM 方案的时间开销比 PBT 方案的时间开销低且更加稳定，但两个方案的交易时间开销与系统用户数量都没有直接关系，能源交易系统的交易时间开销受到了 Hyperledger Fabric 2.0 平台自身的通信效率的影响。

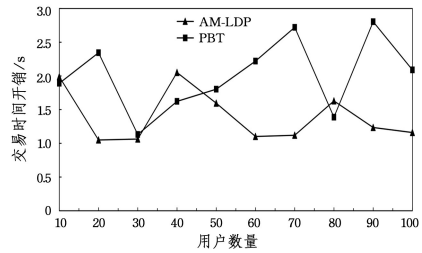


图 10 BLDP-AM 和 PBT 方案的交易时间开销

Fig. 10 Transaction time overhead of BLDP-AM and PBT schemes

图 11 给出了使用 BLDP-AM 方案保护交易数据隐私的能源交易系统的 TPS。首先确定出块的基本参数即最长出块间隔 BachTimeout=2 s，区块最大交易数量 MaxMessageCount=10，区块交易数据大小 PreferredMaxBytes=512 kB，区块交易数据的绝对大小 AbsoluteMaxBytes=10 MB。接着

确定测试 TPS 的并发数，图中横坐标轴代表并发数，10 代表客户端和 peer 节点之间创建的 grpc 连接数量为 10，X 代表每个连接用于向每个 peer 节点发送提案的客户端数量，因此 $10*X$ 代表每个连接用于向每个 peer 节点发送提案的客户端数量。由图中的平均 TPS 曲线和最大 TPS 曲线可知，在并发量小于 700 时，TPS 随着交易并发量增多而增加；在[700，1 400]并发量之间，平均 TPS 稳定在 265 左右，最佳 TPS 为 290.62；在并发量大于 1 400 后能源交易系统的平均 TPS 在 280 左右起伏，受网络波动影响，该部分曲线波动比较大，最佳 TPS 为 294.36。基于联盟链的能源交易系统的 TPS 可以达到 294，这说明 BLDP-AM 隐私保护方案具有良好的性能。

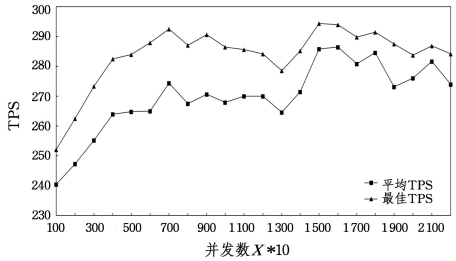


图 11　使用了 BLDP-AM 方案的能源交易系统的 TPS

Fig. 11　TPS of energy trading system using BLDP-AM scheme

结束语　本文研究了基于联盟链的能源交易系统的交易数据隐私保护问题，并提出了一种安全高效的隐私保护方案 BLDP-AM。该方案首先通过用户具有多关联账户的特性以及 ESP 算法抑制账户交易曲线波动的特性，抵御了连接攻击。其次为 BLDP 算法设计了新的本地用户数据扰动机制来满足查询与验证的隐私要求，使其可以有效预防差分攻击。同时，由于该方案具有处理后的链上交易数据与原始交易数据不相关的特性以及 BLDP 算法具有的随机特性，因此可以有效预防数据挖掘。本文方案主要解决了链上一维数值型交易数据的隐私保护问题，但无法处理高维复杂数据。因此，未来的主要研究内容是适用于区块链的高维数据差分隐私算法，目的是将本文隐私保护方案拓展到高维交易数据领域，在保证查询与验证效率的同时保护高维交易数据的隐私。此外，如何将本文的隐私保护方案从能源交易领域迁移到其他应用领域，也是未来的一个研究方向。

参 考 文 献

[1] WANG N，ZHOU X，LU X，et al. When energy trading meets blockchain in electrical power system：the state of the art[J]. Applied Sciences，2019，9(8)：1561.

[2] MORSTYN T，FARRELL N，DARBY S J，et al. Using peer-to-peer energy-trading platforms to incentivize prosumers to form federated power plants[J]. Nature Energy，2018，3(2)：94-101.

[3] GUO S T，WANG J R，ZHANG F L. Summary of Principle and Application of Blockchain[J]. Computer Science，2021，48(2)：271-281.

[4] SERJANTOV A，SEWELL P. Passive Attack Analysis for Connection-Based Anonymity Systems[C]// European Symposium on Research in Computer Security. Berlin：Springer，2003：116-131.

[5] NYBERG K，KNUDSEN L R. Provable security against a differential attack[J]. Journal of Cryptology，1995，8(1)：27-37.

[6] CHUNG H M，GRAY P. Data mining[J]. Journal of management information systems，1999，16(1)：11-16.

[7] ZHANG A，BAI X Y. Survey of Research and Practices on Blockchain Privacy Protection[J]. Journal of Software，2020，31(5)：1406-1434.

[8] YU G，NIE T Z，LI X H，et al. The Challenge and Prospect of Distributed Data Management Techniques in Blockchain Systems[J]. Journal of Computer，2021，44(1)：28-53.

[9] JIANG P P，WANG Q，CHEN Y J，et al. Securing Guarantee of the Blockchain Network：Attacks and Countermeasures[J]. Journal of Communications，2021，42(1)：151-162.

[10] LIU M D，CHEN Z N，SHI Y J，el al. Research Progress of Blockchain in Data Security[J]. Journal of Computer，2021，44(1)：1-27.

[11] POP C D，ANTAL M，CIOARA T，et al. Blockchain and demand response：Zero- knowledge proofs for energy transactions privacy[J]. Sensors，2020，20(19)：5678.

[12] HASSAN M U，REHMANI M H，CHEN J. DEAL：Differentially private auction for blockchain-based microgrids energy trading[J]. IEEE Transactions on Services Computing，2019，13(2)：263-275.

[13] GAI K，WU Y，ZHU L，et al. Privacy-preserving energy trading using consortium blockchain in smart grid[J]. IEEE Transactions on Industrial Informatics，2019，15(6)：3548-3558.

[14] ZHANG X，JIANG S，LIU Y，et al. Privacy-Preserving Scheme with Account- Mapping and Noise-Adding for Energy Trading Based on Consortium Blockchain[J]. IEEE Transactions on Network and Service Management，2021，19(1)：569-581.

[15] DORRI A，HILL A，KANHERE S，et al. Peer-to-Peer Energytrade：A Distributed Private Energy Trading Platform[C]// 2019 IEEE International Conference on Blockchain and Cryptocurrency. IEEE，2019：61-64.

[16] SAMUEL O，JAVAID N. A secure blockchain -based demurrage mechanism for energy trading in smart communities[J]. International Journal of Energy Research，2021，45(1)：297-315.

[17] LASZKA A，DUBEY A，WALKER M，et al. Providing Privacy，Safety，and Security in IoT- Based Transactive Energy Systems Using Distributed Ledgers[C]// Proceedings of the Seventh International Conference on the Internet of Things. 2017：1-8.

[18] GARG S，KAUR K，KADDOUM G，et al. An Efficient Blockchain-Based Hierarchical Authen tication Mechanism for Energy Trading in V2G Environment[C]// 2019 IEEE International Conference on Communications Workshops. IEEE，2019：1-6.

[19] GUAN Z，SI G，ZHANG X，et al. Privacy- preserving and efficient aggregation based on blockchain for power grid communications in smart communities[J]. IEEE Communications Magazine，2018，56(7)：82-88.

[20] LU X，GUAN Z，ZHOU X，et al. An Efficient and Privacy-Pre-

serving Energy Trading Scheme Based on Blockchain[C]// 2019 IEEE Global Communications Conference. IEEE, 2019: 1-6.
[21] HASSAN M U, REHMANI M H, CHEN J. DEAL: Differentially private auction for blockchain-based microgrids energy trading[J]. IEEE Transactions on Services Computing, 2019, 13(2): 263-275.
[22] OU L, QIN Z, LIAO S, et al. Singular spectrum analysis for local differential privacy of classifications in the smart grid[J]. IEEE Internet of Things Journal, 2020, 7(6): 5246-5255.
[23] LI D, YANG Q, YU W, et al. Towards differential privacy-based online double auction for smart grid[J]. IEEE Transactions on Information Forensics and Security, 2019, 15: 971-986.
[24] DWORK C, MCSHERRY F, NISSIM K, et al. Calibrating Noise to Sensitivity in Private Data Analysis[C]// Theory of cryptography conference. Berlin: Springer, 2006: 265-284.
[25] ERLINGSSON Ú, PIHUR V, KOROLOVA A. Rappor: Randomized Aggregatable Privacy- Preserving Ordinal Response [C]// Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014: 1054-1067.
[26] GENG Q, KAIROUZ P, OH S, et al. The staircase mechanism in differential privacy[J]. IEEE Journal of Selected Topics in Signal Processing, 2015, 9(7): 1176-1184.
[27] WANG N, XIAO X, YANG Y, et al. Collecting and Analyzing Multidimensional Data With Local Differential Privacy[C]// 2019 IEEE 35th International Conference on Data Engineering. IEEE, 2019: 638-649.
[28] YE Q Q, MENG X F, ZHU M J, et al. Survey on Local Differential Privacy[J]. Journal of Software, 2018, 29(7): 1981-2005.

SHI Kun, born in 1996, postgraduate, is a member of China Computer Federation. His main research interests include blockchain and data security.

JIANG Shun-rong, born in 1986, Ph.D, associate professor, is a member of China Computer Federation. His main research interests include Internet of vehicles, cloud computing, blockchain and data security.

（责任编辑：何杨）