文章编号: 1000-5641(2018)05-0135-09

基于区块链的智能电表身份认证方案

田福粮, 田秀霞, 陈 希

(上海电力学院 计算机科学与技术学院, 上海 200090)

摘要: 能源互联网是未来发展的趋势, 能够实现电力资源在用户和能源系统中的双向流通. 智能电表作为连接用户和能源系统的关键点, 具有用户身份信息和大量有效的电力交易数据, 而这些信息会造成用户隐私泄露. 为保护用户隐私, 提出了基于区块链的智能电表身份认证方案, 利用 Merkle 树原理对智能电表身份信息进行处理并存储在区块链中, 实现智能电表身份有效认证的同时, 使智能电表身份信息具有不可篡改性, 并破坏了用户身份和电力数据之间的可关联性, 能够有效抵御内部和外部攻击者获取用户隐私. 通过利用区块链的自身特性, 保证了交易数据的完整性和有效性.

关键词: 区块链; 智能电表; 身份认证; 信誉共识机制

中图分类号: TM933.4 **文献标志码**: A **DOI:** 10.3969/j.issn.1000-5641.2018.05.011

Blockchain-based smart meter authentication scheme

TIAN Fu-liang, TIAN Xiu-xia, CHEN Xi

(*College of Computer Science and Technology, Shanghai University of Electric Power, Shanghai* 200090, *China*)

Abstract: The development of power networks is a trend of the future. These networks allow the two-way flow of power resources between users and power systems. As the key node for connecting users and energy systems, smart meters contain a large volume of user's power transaction data and identity information, which leaves the potential for a breach of private user data. To protect the privacy of the user, an identity authentication scheme for smart meters, based on blockchain technology, is proposed. The smart meter's identity information is processed using the Merkle-tree principle and stored in the blockchain; with this, the authentication of the smart meter's identity is realized and the identity information cannot be modified. Additionally, it breaks the connection between the user's identity and their power data, preventing internal and external hackers from obtaining private user data. The integrity and validity of the transaction data are guaranteed by using the characteristics of blockchain technology.

Keywords: blockchain; smart meter; identity authentication; reputation consensus

收稿日期: 2018-07-04

基金项目: 国家自然科学基金(61772327, 61532021); 上海市科委资助项目(15110500700)

第一作者: 田福粮, 男, 硕士研究生, 研究方向为隐私保护. E-mail: tianflxs@163.com.

通信作者: 田秀霞, 女, 博士, 教授, 研究方向为数据库安全、隐私保护与机器学习.
E-mail: xxtian@shiep.edu.cn.

0 引 言

随着太阳能和风力发电技术的不断发展, 其应用成本也在不断降低, 使得太阳能和风力发电以分布式能源的形式广泛应用于社区和家庭[1]. 传统的电能消费者开始具备了供电能力, 同时售电市场的改革使各种分布式电源等主体参与电力市场竞争成为未来发展的趋势. 智能电表作为用户和电力系统的连接点, 在电力系统中属于终端设备, 具有身份属性, 不仅能够完成用户的身份认证和记录用户的实时用电量, 而且要能够根据用户的实时电量信息进行电能的双向传输, 实现用户和能源系统的有效交易.

而现有的传统电力系统是以大型发电厂为中心, 采用中心式管理和数据集中储存的运行模式, 电力公司具有最高权限. 在交易过程中电力公司知晓用户的真实身份, 同时具有用户细粒度的实时用电数据, 攻击者通过获取这些数据, 可以将用户的身份和实时用电数据进行关联, 进而分析出用户的日常用电习惯, 对用户造成一定的潜在危险. 除此之外, 现有的中心式能源网络中, 所有数据被集中存储和管理, 一旦遭受攻击, 容易造成数据被篡改或丢失的后果, 不能保证数据的真实性、完整性和有效性.

因此, 本文提出了基于区块链的智能电表身份认证方案, 利用 Merkle 树原理将用户身份信息进行处理并存储在区块链中, 使用户在身份认证过程中身份信息不被篡改, 同时破坏了用户身份信息和实时电量数据之间的关联性, 在一定程度上解决了目前智能电表隐私保护所面临的问题. 区块链通过数据加密、数据链式钩稽、多副本存储和分布式共识等机制, 实现去中心化的分布式数据管理技术[2], 具有信息不可篡改等特点, 解决了传统中心化机构的高成本、低效率和数据存储不安全的问题[3]. 将区块链技术运用到能源系统中不仅能够提高交易的可信程度, 还能建立一套完整的可追溯交易体系, 对发生的交易进行监管, 避免传统电力市场中存在的假账和错账问题.

1 相关工作

针对智能电表的隐私保护, 研究人员根据不同的应用场景提出了很多解决方案, 目前主要通过身份匿名和数据聚合两种方式实现.

Cheung 等[4]采用盲签名的方法, 通过使签名者不知道签名内容而生成认证凭证的方式实现身份认证. Afrin 等[5]提出了匿名单元, 建立了不依赖于第三方的电力消费数据匿名机制. Yu 等[6]利用环签名实现智能电表的身份认证和用户的隐私保护, 但计算复杂性和通信开销较大. Lee 等[7]提出的证书验证方案, 采用可信第三方给智能电表颁发证书的方式进行身份验证, 但不能实现智能电表和电力公司之间的认证. Fan 等[8]提出了保护用户隐私的电力数据聚合方案, 能够抵御电网的内部攻击. Li 等[9]提出了基于同态加密的数据聚合方案, 利用同态加密的方法保护用户的电力数据隐私. 张少敏等[10]利用改进的无证书环签密方案, 使用户身份和电力数据不能关联来达到保护隐私的目的.

Li 等人[11]基于 Merkle 哈希树提出了一种认证和隐私保护方案, 将电量信息划分为若干部分作为 Merkle 树的叶节点, 内部节点值是从它们的子节点派生的, 最后获得根节点的值, 通过记录关联节点的值来验证节点信息的完整性. Liu 等人[12]提出了一种轻量级通信方案, 使用 Lagrange 多项式公式进行消息发送者认证, 相比Li等人的方案具有更好的性能. 但是这两个方案并没有解决一些安全问题. Abbasinezhad 等人[13]提出了一个非常轻量级的通信方案, 可以有效地应用于智能电表和临近网关之间的安全双向通信. Saxena 等[14]提出了一种

基于轻量级云信任权限的集中分布式认证协议, 以分布式方式在智能电网实体之间提供相互认证.

学术界关于区块链应用在能源领域的研究还处于初级阶段, 主要是对其可行性进行了研究[15]. 张宁等[16]探讨了区块链在能源互联网中的研究框架及可行应用. 曹寅[17]介绍了区块链和能源互联网之间的特性匹配情况, 并提出了一些典型的应用场景. 李彬等[18]提出了弱中心化管理电力交易的方法, 利用区块链技术, 以智能合约的形式自动执行资金转移和交易信息存储. 国内外也有一些企业在尝试将区块链技术应用到能源领域. 美国能源公司 LO3 Energy 与比特币开发公司 Consensus Systems 在布鲁克林街区为一些用户建立了一个基于区块链技术的可交互电网平台, 具有新能源发电设备的用户在满足自身电力需求的同时, 可以将剩余的电能在平台上进行交易, 而不依赖任何第三方中介[19]. 欧盟 Scanergy 项目旨在基于区块链系统实现用户绿色能源的直接交易, 该项目设想在交易系统中每隔一段时间检测一次网络的生产与消费状态, 并向能源的供应者提供一种电子货币作为奖励, 该项目尚未投入实际运行[20].

2　方案设计

本节首先介绍了智能电表工作的系统结构, 然后对系统初始化过程中的密钥分配和智能电表身份注册进行了说明, 最后详细介绍了智能电表的身份认证方法和交易过程.

2.1　系统结构

随着能源互联网的发展和相关技术的应用, 以家庭或社区形式出现的分布式能源将会大量接入到能源系统中, 从而实现能源的双向流通, 这就使得传统的中心式电力系统结构很难适用. 因此, 根据现有能源系统的特点和发展趋势, 本方案将系统分为三部分: 注册机构(Registration Agencies, RA), 区域管理器(Regional Manager, RM)和智能电表(Smart Meter, SM). 系统结构如图 1 所示, 注册机构负责对区域管理器和智能电表进行身份注册, 提供智能电表身份认证凭证, 但不参与交易和认证过程. 智能电表是用户端的电量记录和控制设备, 一般安装在具有产消电能能力的家庭或社区内, 可以根据用户的发电和用电情况向区域管理器发出购电或售电请求. 区域管理器是某个地区的电能管理中心, 可以验证智能电表的身份信息, 并对智能电表的请求进行响应, 也可以根据本地区的电量需求与其他区域管理器进行电量交易.

根据智能电表计算和存储能力差的特点, 智能电表在整个系统中被视为一般结点, 只记录自身和区域管理器之间的交易信息和数据, 并存储在区块链中. 而区域管理器具有较强的计算和存储能力, 能够与其他区域管理器和本区域内所有的智能电表进行通信和电量交易, 因此在系统中将其视为特殊结点, 所有区域管理器组成联盟链, 记录全网的交易信息.

2.2　系统初始化

系统初始化包括注册机构对区域管理器的认证和联盟链的组成, 以及对智能电表身份的注册. 这里主要考虑智能电表的身份注册和认证, 对区域管理器的身份认证和联盟链的组成过程不进行讨论.

2.2.1　密钥分配

注册机构负责密钥的分发工作, 当区域管理器和智能电表提出注册申请时, 注册机构为其分发主密钥对, 区域管理器和智能电表根据主密钥对计算自身的公钥和私钥, 通过这种方

式可以避免密钥的泄露, 具体步骤如下.

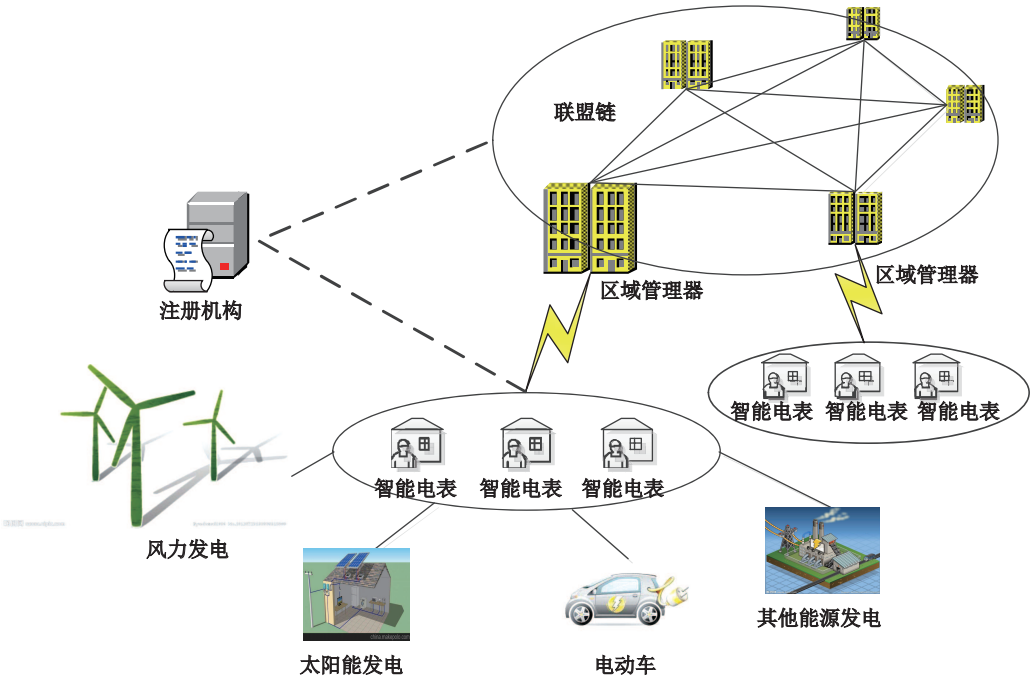

图 1 系统结构

Fig. 1 System model

区域管理器提出身份认证请求, 注册机构向其发送主密钥对(MPU_1, MPR_1), 区域管理器选择随机数 λ 并结合主密钥对(MPU_1, MPR_1)生成自身公钥$PU_{RM} = f(MPU_1, \lambda)$和私钥 $PR_{RM} = f(MPR_1, \lambda)$.

智能电表提出注册申请, 注册机构向其发送主密钥对(MPU_2, MPR_2). 智能电表选择一个随机数 r 并结合主密钥对(MPU_2, MPR_2)生成自身的公钥 $PU_{SM} = f(MPU_2, r)$ 和私钥 $PR_{SM} = f(MPR_2, r)$.

2.2.2 智能电表身份注册

为保护用户隐私, 并保证智能电表身份信息在认证过程中的有效性, 我们利用 Merkle 树[21]原理对智能电表的注册信息和认证信息进行了处理. Merkle 树的主要思想是建立基于单向加密哈希函数的树, 通过相关路径结点的信息可以验证每个叶节点的数据完整性, 下面通过一个例子对 Merkle 树的原理进行说明.

如图 2 所示, 将信息 D_i 的哈希值 $H_i = h(D_i)(i = 1, \cdots, 8)$ 作为 Merkle 树的叶节点, 内部结点的值是其两个子结点的哈希值, 例如 $H_{12} = h(H_1, H_2)$. 依次计算, 最后生成根结点 $H_{18} = h(H_{14}, H_{58})$. 通过构建的 Merkle 树, 每个叶结点数据的完整性都可以通过根节点和相关结点进行验证. 当要验证 D_1 时, 只需获得根节点 H_{18} 和结点 (H_2, H_{34}, H_{58}) 的值, 并依次计算 $H_1 = h(D_1)$, $H_{12} = h(H_1, H_2)$, $H_{14} = h(H_{12}, H_{34})$, $H'_{18} = h(H_{14}, H_{58})$, 最后验证计算得到的 H'_{18} 和原存的根哈希值 H_{18} 是否相同, 只有相同时才能说明数据是正确的. 由于只进行哈希计算, 所以验证的成本非常低.

智能电表身份注册过程如图 3 所示, 智能电表将真实合法的身份信息用注册机构的公钥加密, 比如用户姓名, 身份证号码, 家庭住址, 手机号等信息, 获得密文 ϕ_1 =

$E_{PU_{RA}}(name, ID, address, number)$. 然后智能电表在所有的身份信息中选择某一单一元素用自身公钥进行加密, 比如姓名, 获得密文 $\phi_2 = E_{PU_{SM}}(name)$. 智能电表将密文 $\{\phi_1, \phi_2\}$ 发送给注册机构.

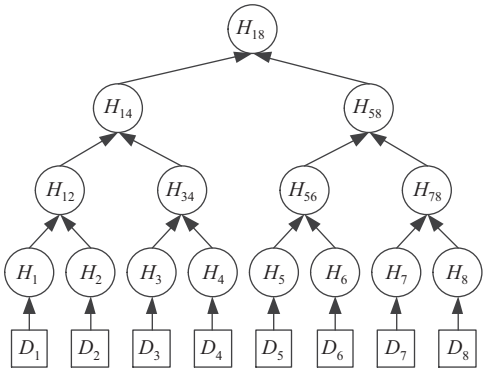

图 2　Merkle 树

Fig. 2　Merkle-tree

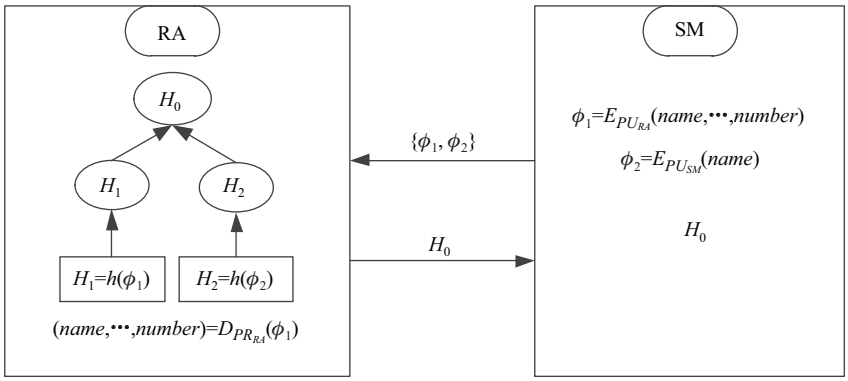

图 3　智能电表身份注册

Fig. 3　The registration of SM

因为 ϕ_2 是智能电表用自身公钥加密得到的密文, 所以只有智能电表的私钥才能进行解密. 注册机构接收到信息 $\{\phi_1, \phi_2\}$ 后, 只能用自身私钥 PR_{RA} 对 ϕ_1 进行解密, 得到用户的详细身份信息 $(name, ID, address, number) = D_{PR_{RA}}(\phi_1)$.

注册机构验证智能电表的注册信息, 如果合法, 则分别计算 ϕ_1, ϕ_2 的哈希值 $H_1 = h(\phi_1)$, $H_2 = h(\phi_2)$. 将 (H_1, H_2) 作为叶子结点, 计算得到根哈希值 $H_0 = h(H_1, H_2)$. 根据 Merkle树原理, 获得 (H_0, H_1, H_2) 中的根哈希值和叶节点中的任意一个值, 就可以验证另一个数据的完整性和有效性. 注册机构将 H_0 返回给智能电表, 并将 (H_0, H_1) 在区域管理器的联盟链中进行广播, 记录在区块链中.

例如, 用户 Bob 需要进行智能电表身份注册, Bob 将详细的身份信息用注册机构的公钥加密 $\phi_1 = E_{PU_{RA}}(Bob, 12345678, China, 3)$, 并选择姓名 Bob 用自身公钥加密作为认证信息 $\phi_2 = E_{PU_{SM}}(Bob)$. 智能电表将密文 $\{\phi_1, \phi_2\}$ 发送给注册机构. 注册机构对 Bob 的注册信息进行解密 $(Bob, 12345678, China, 3) = D_{PR_{RA}}(\phi_1)$, 验证注册信息的合法性. 若合法, 则分别计算 (ϕ_1, ϕ_2) 的哈希值 $H_1 = h(\phi_1) =$ "$E0789A1498A220AD828E54A5491BF8D6$", $H_2 =$

$h(\phi_2)$ = "$B47F40C3269FD01F8FA402E4EFDC3BD0$". 将 (H_1, H_2) 作为叶子结点, 计算得到根哈希值 $H_0 = h(H_1, H_2)$ = "$DF73C66D2B5977A4F33469C648D7A97F$". 注册机构将 H_0 返回给智能电表, 并将 (H_0, H_1) 在区域管理器的联盟链中进行广播, 记录在区块链中.

2.3 智能电表身份认证

智能电表在和区域管理器进行交易前, 需要进行身份认证, 如图 4 所示. 当智能电表向区域管理器发出交易请求时, 首先将自己选取的单一身份认证信息用公钥 PU_{SM} 进行加密 $\phi_2' = E_{PU_{SM}}(name)$, 然后将交易信息 $\{\phi_2', H_0, T, R\}$ 用区域管理器的公钥 PU_{RM} 进行加密得到密文 $MSG_{SM} = E_{PU_{RM}}(\phi_2', H_0, T, R)$. 智能电表将密文 MSG_{SM} 发送给区域管理器, 其中 T 是系统时间戳, R 是交易请求内容. 只有在有效时间内的请求才会被响应, 通过添加时间戳可以防止重放攻击.

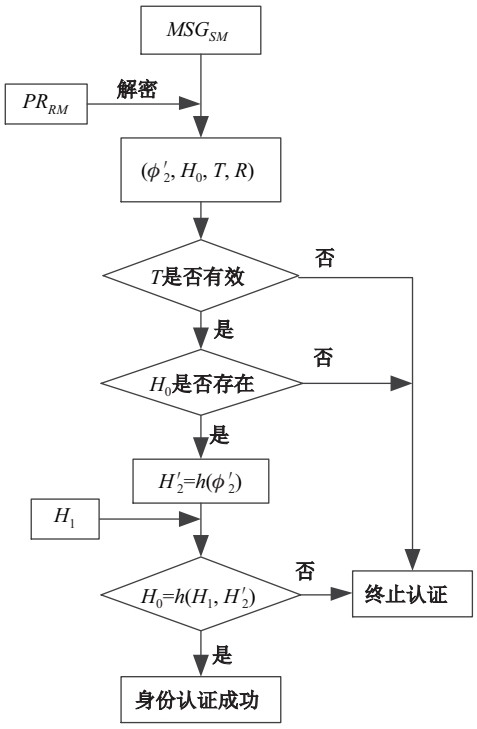

图 4 智能电表身份认证

Fig. 4 Authentication of SM

区域管理器接收到信息 MSG_{SM} 之后, 用自身私钥 PR_{RM} 进行解密获得信息 $(\phi_2', H_0, T, R) = D_{PR_{RM}}(MSG_{SM})$. 区域管理器首先验证 T 是否有效以避免重放攻击. 若有效, 则区域管理器在区块链中查找 H_0, 若区块链中不存在 H_0, 说明该智能电表身份没有进行注册. 若存在, 则获取与 H_0 对应的 H_1. 然后, 区域管理器对 ϕ_2' 进行哈希值计算得到$H_2' = h(\phi_2')$, 验证 $H_0 = h(H_1, H_2')$ 是否成立. 如果成立, 则表明智能电表身份合法, 进而进行能源交易, 否则认证失败.

同样以 Bob 为例, Bob 将自己选取的认证信息用公钥 PU_{SM} 进行加密 $\phi_2' = E_{PU_{SM}}(Bob)$, 然后将 (ϕ_2', H_0) 添加在信息中, 用区域管理器的公钥 PU_{RM} 加密后发送给区域管理器, 其中 H_0 = "$DF73C66D2B5977A4F33469C648D7A97F$". 区域管理

器对密文解密后, 先验证信息的时效性, 然后在区块链中根据 H_0 找到与之对应的 $H_1 = h(\phi_1) =$ "$E0789A1498A220AD828E54A5491BF8D6$", 然后计算 ϕ_2' 的哈希值 $H_2' = h(\phi_2') =$ "$B47F40C3269FD01F8FA402E4EFDC3BD0$". 根据 (H_1, H_2') 计算得到根哈希值$H_0' = h(H_1, H_2') =$ "$DF73C66D2B5977A4F33469C648D7A97F$", 因为计算得到的根哈希值 H_0' 和 H_0 相同, 所以智能电表身份认证成功.

2.4　交易过程

智能电表身份认证完成后能够和区域管理器进行能源交易, 可以出售剩余的电量, 也可以向区域管理器购买电量. 以往的能源交易中, 用户和电力公司的交易数据由电力公司记录并集中保存, 用户对自己的交易数据没有掌控权, 使得交易过程存在不公平性. 并且数据集中存储, 很容易受到攻击或被篡改. 在本方案中, 智能电表身份认证之后, 和区域管理器的每次交易都由区域管理器在联盟链中进行全网广播, 其他区域管理器将交易记录保存在自己的缓存区块中, 等待获得记账权限后对数据进行验证并生成区块链.

区域管理器不仅能够和智能电表进行能源交易, 不同的区域管理器之间同样能够进行能源交易, 因此, 找到一种合适的共识机制非常重要. 比特币中采用的是工作量证明 (Proof of Work, PoW) 的机制, 通过"挖矿"来获得记账权, 并保证区块链的正确性[22]. 为了避免 PoW 带来的算力消耗和能量消耗, 提出了 PoS(Proof of Stake, PoS) 共识机制, 验证结点随机产生, 并由其生成区块, 通过奖励机制鼓励参与结点成为验证结点.

而在本方案中, 区域管理器组成联盟链, 结点相对较少, 各结点的可信度较高, 因此我们提出采用信誉值的方式获得记账权限. 若规定区域管理器联盟链的记账周期为 10 分钟, 则在一个记账周期内, 由当前信誉值最高的区域管理器获得记账权. 区域管理器的当前信誉值由以往信誉值和本周期信誉值计算得出.

每个区域管理器注册之后都具有相同的初始信誉值 C_0. 区域管理器每次和智能电表进行交易后, 智能电表需对本次交易进行评价, 评价结果会用于区域管理器的信誉值计算. 若智能电表对该次交易持认可态度, 则返回的评价结果 $C_{approval}$ 为正值, 智能电表用自身私钥对评价结果进行加密, 并添加系统时间戳 T, 然后将密文 $E_{PR_{SM}}(C_{approval}, T)$ 发送给区域管理器, 区域管理器将密文和交易记录一起进行全网广播. 若智能电表对某次交易结果不认可, 则返回的评价结果 C_{blam} 为负值, 智能电表用自身私钥对评价结果进行加密, 并添加系统时间戳 T, 然后将密文 $E_{PR_{SM}}(C_{blam}, T)$ 发送给区域管理器, 区域管理器将密文和交易记录一起进行全网广播. 智能电表将评价用私钥加密, 使区域管理器不能伪造评价, 添加的时间戳可以防止区域管理器利用过期的评价来代替当前评价.

当一个记账周期到来时, 区域管理器对本周期内的所有评价进行解密, 并根据下式计算本周期所获得的总评价D.

$$D = \frac{1}{n}(k \cdot C_{approval} + (n-k) \cdot C_{blam}), \quad k \in \{0, 1, \cdots, n\}. \tag{1}$$

其中: n为交易次数; k为获得的评价结果为$C_{approval}$的次数. 这种取平均值的计算方式使信誉值的计算不受区域内智能电表数量的影响, 适用于不同地区的区域管理器.

设第i个记账周期时区域管理器的信誉值为C_i, 则当前第t个周期的信誉值可由公式(2)计算得出.

$$C_t = \sum_{i=0}^{t-1} C_i \mathrm{e}^{-(t-i)} + D, \tag{2}$$

其中公式(2)的第一项为往期信誉值对当前信誉值的影响值. 根据现实生活的规律, 时间越早的事件对当前事件的影响越小, 因此为了减少以往行为对当前信誉值的影响, 我们需要引入一个递减函数, 使得以往信誉值的权重随时间的变化而降低, 比如e^{-x}. 因此,以往信誉值对当前信誉值的影响值由公式(3)计算得出.

$$\sum_{i=0}^{t-1} C_i \mathrm{e}^{-(t-i)}. \tag{3}$$

区域管理器在联盟链中广播自己的当前信誉值, 并对获得最高信誉值的区域管理器的信誉值进行验证. 验证通过后, 具有最高信誉值的区域管理器获得本次记账权限, 完成本周期内交易区块的生成, 并能得到一定的奖励. 若发现区域管理器的信誉值出现伪造行为, 则取消该结点的记账权.

3 安全性分析

首先, 基于区块链的系统结构, 智能电表拥有了更多的主动权, 同时每笔交易数据被记录在区块链中, 并分布存储在各个结点上, 使数据不能被篡改, 提高了数据的安全性和可靠性.

在用户身份隐私方面, 用户的注册信息被注册机构公钥加密后储存 $\phi_1 = E_{PU_{RA}}(name, ID, address, number)$, 只有注册机构用自身私钥才能解密, 外部攻击者不可能获得用户的详细身份信息. 智能电表在交易过程中的认证信息 $\phi_2 = E_{PU_{SM}}(name)$ 不同于注册信息, 是注册信息中的单一元素, 并用自身公钥进行加密, 即使被攻击者获取, 也很难精准地对用户进行定位, 有效保护了用户的身份信息. 根据 Merkle 树原理, 注册机构对智能电表的注册信息和智能电表的认证信息进行哈希计算获得根哈希值 $H_0 = h(H_1, H_2)$, 并将 (H_0, H_1) 记录在区块链中, 使得任何一方都不能对智能电表的身份进行修改, 确保了智能电表身份信息的有效性, 使认证过程更加安全可靠.

在身份认证过程中, 若单纯采用密钥进行身份认证, 认证者需要获得信息发送者的真实身份和密钥的对应关系才能完成认证, 这无形中就会使密文内容和发送者的真实身份进行了关联. 通过 Merkle 树对智能电表身份信息进行处理, 认证者不需要获得发送者的任何真实身份信息即可完成认证过程, 避免了信息内容和身份信息之间关联的可能性,更有效地保护了用户的隐私.

在交易过程中, 注册机构只负责用户身份的注册和存储, 并不参与电能的交易, 不能得到用户的详细用电信息. 区域管理器在和智能电表进行电能交易时, 虽然具有相关的电量信息, 但获取的身份认证信息是用户某一单一信息的密文和相关哈希值. 因此, 系统中的任何一方都不能将智能电表的有效身份与电量信息进行关联, 有效抵御了内部和外部攻击, 确保用户隐私不被泄露.

区域管理器将每笔交易都在区块链中进行广播, 由信誉值较高的结点进行验证并生成区块, 使交易数据不能被篡改, 同时具有可追溯性, 解决了传统电力系统中数据不安全的问题. 采用信誉值共识机制避免了因结点挖矿而造成的资源浪费, 而且区域管理器的信誉值由往期信誉值和当前周期参与交易的智能电表共同决定, 其他结点也能够对每个结点的当前信誉值进行验证, 这增加了结点伪造区块的难度, 保证了区块链的正确性.

智能电表在发送的信息中添加了系统时间戳 T, 区域管理器接受到信息后首先验证时间戳的有效性, 只有在有效时间内的请求才会被响应, 避免了重放攻击的发生.

本文提出的智能电表身份认证方案和其他方案的安全性对比如表 1 所示, 本文提出的智能电表身份认证方案能够抵御电力公司等内部参与者泄露用户隐私, 具有更好的安全性. 表中“yes”表示能够抵御此类攻击, “no”表示不能抵御该种攻击.

表 1　安全性对比

Tab. 1　Security comparison

方案	恶意用户	电力公司	中间人	第三方	重放攻击
Lee等[7]	no	no	yes	no	yes
Li等[11]	yes	no	yes	yes	yes
Liu等[12]	yes	no	yes	yes	yes
Saxena等[14]	yes	no	no	yes	no
本方案	yes	yes	yes	yes	yes

4　结　　论

根据能源系统的发展趋势, 智能电表将具有大量用户隐私数据, 基于区块链的智能电表身份认证方案, 使用户身份信息得到了有效保护, 使内部和外部攻击者不能将用户身份信息和实时电力数据关联. 区块链技术的应用使交易过程更加公平和安全, 同时数据分布式存储, 提高了系统的安全性和可靠性. 提出的信誉值共识机制有效避免了区块链结点因“挖矿”造成的资源浪费, 使系统能够更加清洁高效地运行.

[参　考　文　献]

[1] SIOSHANSI F. Smart Grid: Integrating Renewable, Distributed And Efficient Energy [M]. New York: Academic Press, 2012.

[2] 钱卫宁, 邵奇峰, 朱燕超, 等. 区块链与可信数据管理: 问题与方法 [J]. 软件学报, 2018, 29(1): 150-159.

[3] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system [R]. 2008.

[4] CHEUNG J C L, CHIM T W, YIU S M, et al. Credential-based privacy-preserving power request scheme for smart grid network[C]// Global Tele-communications Conference. IEEE, 2011: 1-5.

[5] AFRIN S, MISHRA S. An anonymized authentication framework for smart metering data privacy[C]// Innovative Smart Grid Technologies Conference. IEEE, 2016: 1-5.

[6] YU C M, CHEN C Y, KUOS Y, et al. Privacy preserving power request in smart grid nerworks [J]. IEEE Systems Journal, 2014, 8(2): 441-449.

[7] LEE S, BONG J, SHIN S, et al. A security mechanism of Smart Grid AMI network through smart device mutual authentication[C]// International Conference on Information Networking. IEEE, 2014: 592-595.

[8] FAN C I, HUANG S Y, LAI Y L. Privacy-enhanced data aggregation scheme against internal attackers in smart grid [J]. IEEE Transactions on Indus-trial Informatics, 2013, 10(1): 666-675.

[9] LI F, LUO B, LIU P. Secure information aggregation for smart grids using homomorphic encryption[C]// First IEEE International Conference on Smart Grid Communications. IEEE, 2010: 327-332.

[10] 张少敏, 赵乙桥, 王保义. 智能电网下保护用户隐私的无证书环签密方案 [J]. 电力系统自动化, 2018(3): 118-123.

[11] LI H, LU R, ZHOU L, et al. An efficient merkle-tree-based authentication scheme for smart grid [J]. IEEE Systems Journal, 2014, 8(2): 655-663.

[12] LIU Y, CHENG C, GU T, et al. A light weight authenticated communication scheme for smart grid [J]. IEEE Sensors Journal, 2016, 16(3): 836-842.

[13] ABBASINEZHAD-MOOD D, NIKOOGHADAM M. An ultra-lightweight and secure scheme for communications of smart meters and neighborhood gateways by utilization of an ARM Cortex-M microcontroller [J]. IEEE Transactions on Smart Grid, 2017(99): 1-11.

[14] SAXENA N, CHOI B J. Integrated distributed authentication protocol for smart grid communications [J]. IEEE Systems Journal, 2016(99): 1-12.

[15] MIHAYLOV M, JURADO S, AVELLANA N, et al. NRGcoin: Virtual currency for trading of re-newable energy in smart grids[C]// 2014 11th International Conference on the European Energy Market (EEM). IEEE, 2014: 1-6.

(下转第 171 页)

[6] BRADLEY P S, BENNETT K P, DEMIRIZ A. Constrained k-means clustering [J]. Microsoft Research Redmond, 2000, 59(1): 1-34.

[7] KUHN H W. The Hungarian method for the assignment problem [J]. Naval Research Logistics, 2005, 52(1): 7-21.

[8] WU B, ZHOU Y, YUAN P, et al. Semstore: A semantic-preserving distributed rdf triple store [C]// Proceedings of the 23rd ACM International Conference on Conference on Information and Knowledge Management. NY: ACM, 2014: 509-518.

[9] BANERJEE A, GHOSH J. On scaling up balanced clustering algorithms [C]// Proceedings of the 2002 SIAM International Conference on Data Mining. PA: Society for Industrial and Applied Mathematics, 2002: 333-349.

[10] BANERJEE A, GHOSH J. Frequency-sensitive competitive learning for scalable balanced clustering on high-dimensional hyperspheres [J]. IEEE Transactions on Neural Networks, 2004, 15(3): 702-719.

[11] NG A Y, JORDAN M I, WEISS Y. On spectral clustering: Analysis and an algorithm [C]// Proceedings of the neural information processing systems. Massachusetts: MIT Press, 2002: 849-856.

[12] CAI D, HE X, HAN J. Document clustering using locality preserving indexing [J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 17(12): 1624-1637.

[13] STREHL A, CHOSH J. Knowledge reuse framework for combining multiple partitions [J]. Journal of Machine learning Research, 2002, 33(3): 583-617.

(责任编辑: 李万会)

(上接第 143 页)

[16] 张宁, 王毅, 康重庆, 等. 能源互联网中的区块链技术: 研究框架与典型应用初探 [J]. 中国电机工程学报, 2016, 36(15): 4011-4022.

[17] 曹寅. 能源区块链与能源互联网 [J]. 风能, 2016(5): 14-15.

[18] 李彬, 张洁, 祁兵, 等. 区块链: 需求侧资源参与电网互动的支撑技术 [J]. 电力建设, 2017, 38(3): 1-8.

[19] LINDA. 区块链能源应用后续: 美国布鲁克林微电网如何运作与交易 [EB/OL]. (2017-04-21) [2018-05-20]. https://www.jinse.com/news/blockchain/17041.html.

[20] PRISCO C. An energy blockchain for European prosumers [EB/OL]. (2016-05-02) [2018-05-20]. https://bitcoinmagazine.com/articles/an-energy-blockchain-for-european-prosumers-1462218142/.

[21] MERKLE R C. A digital signature based on a conventional encryption function [C]// Conference on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1987: 369-378.

[22] GARAY J, KIAYIAS A, LEONARDOS N. The bitcoin backbone protocol: Analysis and applications [C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2015: 281-310.

(责任编辑: 林　磊)