基于区块链与*K*-means算法的智能电表密钥管理方法

翟　峰[1,2]，杨　挺[1]，曹永峰[2]，李双全[3]
（1. 天津大学 智能电网教育部重点实验室，天津 300072；
2. 中国电力科学研究院有限公司 计量研究所，北京 100192；
3. 杭州海兴电力科技股份有限公司，浙江 杭州 310011）

摘要：随着电力物联网建设的推进，电力系统高级计量体系逐渐形成了由海量智能电表、边缘计算装置和云端主站构成的“云-边-端”三层架构体系。在此背景下，针对传统集中式智能电表密钥管理机制存在主站依赖度高、密钥存储效率差、响应速度慢的问题，提出一种基于区块链与*K*-means算法的智能电表分布式密钥管理方法。考虑到传统区块链建链过程中区块节点数量对建链时效性影响较大以及未考虑到节点通信传输资源有限的问题，首先利用*K*-means算法对智能电表集群按空间位置进行聚类，并提出采用图中央点算法确定边缘计算装置的位置，从而降低区块链规模；然后，提出计及智能电表通信带宽的按需传输机制，以最小化边缘计算装置的负载均衡度为目标规划区块链节点中的传输路径，从而提升传输时效性；最后，基于Hyperledger Fabric平台的智能电表密钥管理算例结果表明，与传统的不考虑节点规模与信道带宽的区块链建链方法相比，当区块链节点数量增大时，所提方法的建链时间增长速率减少了8.18%以上，而负载均衡度增长速率降低了42.16%以上；所提智能电表密钥管理方法具有更快的建链速度以及更优的网络性能，因而具备更好的可行性。

关键词：智能电表；密钥管理；区块链；*K*-means算法；电力物联网；负载均衡
中图分类号：TP 391；TN 918.4；TM 933.4　　**文献标志码**：A　　DOI：10.16081/j.epae.202006019

0　引言

电力物联网是在电力系统中引入高效的物联网双向通信网络，并采用先进的多维感知、机器学习与云边协同控制等技术，实现电网的智能化管理[1]。对用户用电信息的计量是电力物联网的一项重要功能，近年来随着云计算、物联网技术的兴起，以及电力物联网建设的推进，诸多边缘计算装置（如国网公司提出的台区融合终端、具备边缘计算能力的集中器）以及海量智能电表开始广泛部署，对高级计量体系AMI（Advanced Metering Infrastructure）的安全防护提出了更高的要求。AMI是一个绵延数千米的复杂网络，攻击者往往试图从某一节点发起攻击，篡改用电数据，观察用户行为，甚至获取对电力物联网各个组件的控制权。为了提高AMI系统的可靠性，用电数据都采用密钥加密的方式进行传输。传统的集中式密钥管理体系存在着主站依赖度高、密钥存储效率差、响应速度慢的缺点，一旦主站系统受到攻击，可能引起AMI系统整个密钥管理的瘫痪，从而降低计量系统的可靠性。因此，如何实现AMI系统中智能电表密钥的可靠、高效管理，成为了一个亟需解决的热点问题[2]。

AMI系统中海量智能电表与集中器、主站的双向通信容易受到捕获与恶意篡改等攻击，为了确保用电数据等信息能安全地进行传输，已有大量研究工作聚焦密钥管理系统可靠性的提升[3]。例如：文献[4]提出了一种智能电表网关SMGW（Smart Meter GateWay）设计方法，该网关与两阶段身份验证机制和密钥管理方案相关联，以建立主站与网关的连接，通过放置SMGW可以降低智能电表的设计复杂度并增强安全性，但是并未考虑密钥系统自身的安全性与抗攻击性；文献[5]提出了一种用于AMI系统中智能电表的安全密钥更新方案，密钥每一固定周期更新一次，即使密钥在前一周期中遭到破坏，更新后的安全性仍可得到保障，但是该方案需要频繁更新密钥系统，当智能电表数量规模很大时，十分浪费网络资源；文献[6]使用基于身份认证的密码学作为密钥分发机制的基本模块，以非交互方式在相邻智能电表之间生成密钥，并提出一种利用多播网络功能的轻量级密钥传递机制，然而，多播网络对于软硬件系统都有一定的要求，并不适用于现阶段的AMI系统；文献[7]利用基于身份的签名方案和加密方案，提出了一种新的智能电表匿名密钥分发方案，该方案中智能电表无需身份验证过程，即可使用一个私钥匿名访问服务，但是基于身份的密钥系统需要可

收稿日期：2019-12-30；**修回日期**：2020-04-22
基金项目：国家重点研发计划项目（2017YFE0132100）；国家自然科学基金资助项目（61571324）；国家电网公司科技项目（1100-201919158A-0-0-00）
Project supported by the National Key R&D Program of China（2017YFE0132100），the National Natural Science Foundation of China（61571324） and the Science and Technology Program of SGCC（1100-201919158A-0-0-00）

信的第三方利用用户身份和所选的主密钥为该用户生成相应的私钥，执行过程非常复杂。

随着比特币概念的提出，其核心技术——区块链的运用开始慢慢渗透到各个技术领域[8]，将区块链的分布式、去中心化特性与AMI系统的密钥管理系统相结合，可以大幅提升密钥体系的可靠性和高效性。近年来，区块链技术在电力系统中的应用也受到了众多学者的关注，例如：文献[9]探讨了区块链技术在电力物联网中的建设方案，但是未对其中的技术细节进行深入的研究；文献[10]提出了基于联盟区块链技术的电力交易平台构建方法，重点探讨了区域数据中心区块链节点的分布式存储框架，但该方案中并未考虑到网络负载对区块链响应速度的影响；文献[11]基于联盟区块链技术构建了以一对多能源节点账户匹配机制为核心的能源互联网交易平台。上述方案中直接采用了传统的以SHA256算法为核心的共识机制，每隔10 min进行区块创建操作。然而，在电力物联网的背景下，智能电表除了具备交易结算的功能外，还将参与需求响应、大数据挖掘、用户用电行为分析以及安全加密等其他业务[12]。因此，AMI系统中的区块链建链必须考虑时间约束。传统的区块链共识机制中认为边缘节点的负载能力以及节点之间的物理信道是理想的。而在实际应用过程中，除了需对共识机制进行针对性的裁剪外，还需要对边缘计算装置数据的传输路径进行优化设计[13]。这是因为在区块链建链过程中需要向全网广播，并且密钥信息的增加、更改与删除也需要其他区块链节点的确认。如果不考虑通信资源的约束进行数据的传输，会造成区块链链路上负载不均衡，进而导致堵塞以及数据传输延时变大甚至数据丢失等问题。

因此，本文提出基于区块链与*K*-means算法的智能电表分布式密钥管理方法，主要创新点如下。

（1）基于电力物联网AMI系统“云-边-端”框架，采用*K*-means算法对智能电表进行以边缘计算装置为核心的聚类，形成动态智能电表集群。与传统的不考虑聚类的区块链建链方法相比，本文所提方法能够使区块链具有更小的规模，从而提升区块链的构建速度。

（2）摒弃了集中式密钥管理体系统存在的缺陷，采用基于边缘计算装置的分布式区块链技术，建立密钥的去中心化管理机制。考虑到边缘计算装置的计算资源有限以及数据重传丢包影响，为了提高智能电表密钥更新的时效性以及区块链节点上密钥操作记录的同步问题，提出基于排队论的按需传输机制。与传统的不考虑信道带宽的区块链建链方法相比，所提按需传输机制能够自适应地选择负载最低的链路作为传输路径，从而提升了数据传输的时效性。

1　电力物联网“云-边-端”AMI系统架构

电力物联网中包含海量智能电表，这些电表分布在各个用户单元，承担着电网信息计量与监测的重要作用。智能电表端节点需要与云化营销主站（智能电表数据管理系统）进行双向通信，进行数据的汇集、处理以及控制指令的下发。云化营销主站与智能电表之间的远距离通信以及高峰时刻的海量数据量吞吐对通信网络提出了挑战。通过在云化营销主站与智能电表之间引入边缘计算装置（例如台区融合终端或者具备边缘计算能力的集中器），形成电力物联网“云-边-端”AMI系统，对绝大部分数据采用本地边缘计算装置进行实时快速处理，可有效缓解通信网络和主站的压力，提升数据传输与计量效率。

电力物联网“云-边-端”AMI系统架构如图1所示。其中，通信网络与云化营销主站之间进行双向通信。该通信网络是一个混合分层网络，边缘计算装置之间以及边缘计算装置与云化营销主站之间均采用广域网，边缘计算装置与智能电表之间采用邻域网。边缘计算装置定期收集、存储和传输大量来自智能电表的数据包，优先进行本地化处理，并将处理后的结果或者超出计算能力的数据传输到云化营销主站。

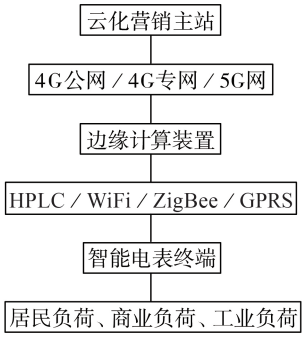

图1　电力物联网“云-边-端”AMI系统架构

Fig.1　“Cloud-edge-end” AMI system architecture in power internet of things

从更广泛的角度来看，电力物联网“云-边-端”AMI系统涵盖了从各类用电负荷到云化营销主站的所有内容，形成了一个全面的网络架构。该架构包含以下主要的子组件。

（1）各类用电负荷。

用电负荷包括居民、商业和工业中所有的耗电设备，耗电量按照电力物联网的计量标准计算，智能电表先对用电数据进行测量、校准、收集，再进行上传。

(2)智能电表。

智能电表构成AMI系统的主干,是“云-边-端”结构中的端节点,负责测量与收集用户的消费信息,进行短暂的存储与简单处理后,以加密数据包的形式通过邻域网将其汇集至边缘计算装置。建筑物内的家用电器、商业用电设备、工业用电设备与智能电表之间形成的小网络称为建筑物内部网络。

(3)邻域网。

除了包括建筑物内部网络外,还有一个覆盖范围更大的网络,其由一个区域内的各种智能电表(存量电表配置采集器)至边缘计算装置之间的通信网络组成。一般可用高速电力线载波HPLC(High speed Power Line Communication)技术,HPLC主要采用正交频分复用OFDM(Orthogonal Frequency Division Multiplexing)技术,与传统的低速窄带电力线载波技术相比,HPLC技术具有带宽大、传输速率高的优势。也可采用小无线(WiFi、ZigBee、GPRS等)网络进行通信。

(4)边缘计算装置。

边缘计算装置是“云-边-端”AMI系统结构中的边缘节点,旨在帮助用户实现从云到端节点的平滑、低延迟的服务交付。边缘计算装置可以对智能电表进行身份验证,管理区域内智能电表的密钥系统,定期更新密钥库。边缘计算装置主要是台区融合终端或者具备边缘计算能力的集中器,采用物联网容器设计方式,实现硬件平台化、软件APP化,具备一定的边缘计算与数据处理能力。

(5)广域网。

广域网连接边缘计算装置之间以及边缘计算装置与云化营销主站之间的通信网络,一般采用无线4G公网,有条件的地方可采用无线4G专网或者5G网。

(6)云化营销主站。

云化营销主站包含数据中台、业务中台和各类型微服务微应用,通过从边缘计算装置接收到的密钥验证邻域网数据的真实性。

传统的密钥管理方式一般采用中心化的结构,由主站集中管理各个端节点的密钥信息。这种中心化的管理方式的可靠性比较低,一旦云端受到攻击或者密钥系统出现故障,整个AMI系统将会瘫痪,导致灾难性的后果。而AMI系统是一个庞大的网络,包含海量的终端设备,常有新电表的加入与旧电表的剔除,对密钥系统的更改较为频繁,给主站造成了较大的压力,也为攻击者提供了潜在的进攻机会。而新型“云-边-端”AMI系统架构为分布式密钥管理提供了较好的支撑,边缘计算装置可以管理一定范围内的智能电表密钥,可以对智能电表进行身份验证,管理区域内智能电表的密钥系统,定期更新密钥库。边缘计算装置之间通过邻域网交换密钥信息,并且通过广域网与主站进行交互,云化营销主站通过从边缘计算装置接收到的密钥验证邻域网数据的真实性。因此在新型“云-边-端”AMI系统架构下,本文提出一种基于区块链的分布式密钥管理方法,并采用基于*K*-means算法的智能电表身份认证方法提高AMI系统中智能电表密钥管理的可靠性与安全性。

2 基于区块链与*K*-means算法的密钥管理方法

云化营销主站请求智能电表数据时首先需要获取相应的密钥,为了克服传统集中式存储方法面临的可靠性低、存储效率差、硬件依赖度高的缺点,本文提出了基于区块链与*K*-means算法的密钥管理方案,包含如下2个步骤。

(1)基于*K*-means算法对智能电表进行空间聚类,并基于图中央点方法确定边缘计算装置的布置位置,形成不同的智能电表集群。智能电表的密钥信息按最邻近原则存储于边缘计算装置中。

(2)为了克服传统的集中式密钥管理体系对单点故障的脆弱性,提出了基于分布式区块链技术的密钥管理方法,即密钥的更新、注销等操作的确认需要得到由边缘计算装置组成的区块链中50%以上成员的确认方可进行。为了提升智能电表加入、密钥更新、密钥注销等密钥请求的时效性以及区块链节点间密钥相关操作的同步记录问题,提出了一种基于排队论的按需传输机制。

2.1 基于无监督学习*K*-means的智能电表聚类算法

由于智能电表的空间位置一般是已经确定的,因此本节主要考虑边缘计算装置的布置问题。依据最邻近传输原则,智能电表应当选择距离最邻近的边缘计算装置获取密钥。因此,本文首先采用无监督学习*K*-means聚类算法对智能电表进行聚类划分,然后采用图中央点方法选择边缘计算装置的布置位置。

设(X_i, Y_i)为边缘计算装置的空间坐标,其中$i=1,2,\cdots,N$为边缘计算装置的编号,N为边缘计算装置的数量;(x_j, y_j)为智能电表的空间坐标,且为了实现区块链功能,智能电表与边缘计算装置之间能够进行双向数据交换。需要指出的是,N的数值主要与边缘计算装置的最大电表承载数量成反比,而与智能电表数量成正比,实际应用时可以粗略确定N的取值下限。

在无监督学习*K*-means聚类算法中,采用欧几里得距离作为不同智能电表之间的聚类标准,计算

式如式(1)所示。

$$D_{\text{dis}}(S_m, S_n)=\sqrt{(x_m-x_n)^2+(y_m-y_n)^2} \tag{1}$$

其中，$S_m=(x_m, y_m)$和$S_n=(x_n, y_n)$分别为智能电表m和智能电表n的空间坐标。显然，2个智能电表之间的距离越近，则二者应具有越大的可能性属于同一类别。

利用无监督学习K-means聚类算法对待分类的智能电表集合$S=\{S_j\}$进行分类，基本算法步骤如下。

步骤1：初始化边缘计算装置的设置，在智能电表空间范围内随机选择N个点布置边缘计算装置。每个智能电表与边缘装置之间构建全网唯一的一对一映射关系，从而获取所有智能电表的空间位置信息。

步骤2：在获取智能电表集合的坐标集合$\{(x_j, y_j)\}$的基础上，建立智能电表的无向图模型，如式(2)所示。

$$G=(S, E) \tag{2}$$

其中，E为智能电表之间的通信链路集合。

步骤3：基于无监督学习K-means聚类算法对智能电表集合进行聚类划分，其中聚类数量即为边缘计算装置的数量，即聚类数量为N，对于智能电表j，根据式(1)计算其与每一个质心C_i之间的距离$D_{\text{dis}}(C_i, S_j)$，并按照最邻近原则重新将其划分至空间距离最近的质心所属的集合，从而得到的智能电表子集合数量为N。

步骤4：重新计算步骤2聚类后的集合的质心，选择图的中央点作为边缘计算装置可行的部署位置，并采用图中央点方法求取其中央点，即$C_i'=(X_i', Y_i')$。其中，图中央点的选取要求是使得该点到聚类的智能电表的距离总和最小时所对应的位置，其数学表述为：

$$\min \sum_{i=1}^{L_i} D_{\text{dis}}(C_i', S_i) \tag{3}$$

其中，L_i为聚类i中的智能电表的数量。

步骤5：按照式(1)计算步骤4中求取的图中央点与原始随机选择的质心之间的距离$D_{\text{dis}}(C_i, C_i')$，若其满足式(4)，则说明重新计算的质心已经趋于稳定而不再变化，终止迭代，同时选择质心作为边缘计算装置的最终布置位置，并实现智能电表信息数据的迁移；否则，重复步骤2—4。

$$D_{\text{dis}}(C_i, C_i')\leqslant\varepsilon \tag{4}$$

其中，ε为充分小正数，即迭代精度。

需要指出的是，在实际工程中由于存在未知新电表的加入操作，因此边缘计算装置需要预留一定的资源空间。当资源空间不再满足新增需求时，只需要根据步骤1—4重新确定新接入的边缘计算装置即可，即重新建立智能电表与边缘计算装置之间的映射关系，这个过程的时间复杂度即为K-means算法的时间复杂度$O(N)$，可见在智能电表数量规模庞大时仍然具备较高的计算效率。而对于映射关系发生变动的智能电表，其本质上是对电表密钥信息的存储位置进行变动，属于数据迁移操作，该操作与智能电表密钥更新、注销等其他操作一样，需要得到由边缘计算装置组成的区块链上半数以上节点的确认方可进行，从而确保了智能电表加入／退出的安全性。

2.2　基于区块链技术的智能电表密钥管理机制与按需传输算法

2.2.1　基于区块链技术的智能电表密钥管理机制

区块链是一种衍生自比特币的分布式账本技术，其结构如图2所示。每个数据区块包括区块头、区块体2个部分，前者包含了数据区块中大量的验证信息，如版本号、根据默克尔(Merkle)树哈希计算得到的前一区块哈希值、时间戳、随机数、当前区块Merkle根(根据Merkle树哈希计算得到)；后者主要为交易数据，即边缘计算装置对聚类集合内智能电表密钥信息的数字签名，而智能电表密钥则按最邻近原则存放于本地边缘计算装置中，该方案的优势在于以下两方面。

(1)密钥本身不直接与其他边缘计算装置进行交互，可以避免其他边缘计算装置遭受攻击时导致的密钥泄露，从而保证了安全性。

(2)交易数据仅包含了数字签名，本质上减少了区块链中的数据传输量，从而可以缩短建立区块链的时间，确保了时效性。

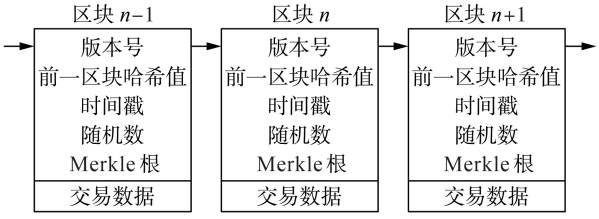

图2　区块链的结构

Fig.2　Structure of blockchain

区块链的特征之一是其分散的网络使它能够在分散的系统节点之间建立信任关系，而无需第三方的信任。区块链内所有节点应当对链式结构达成共识，即所有节点都同意区块的顺序，并且所有节点都存储着相同的区块链信息，当需要在区块链尾部增加新的数据区块时，需要向全网广播并经过所有节点的认证。区块链的分布式存储系统与去中心化的特征保障了在单一节点发生故障时，其数据区块链不受影响。

利用区块链分布式、去中心化的特征，在AMI系统的“云–边–端”架构中，将所有边缘计算装置视为区块链节点，将各个智能电表的密钥信息作为区块链的交易信息，实现基于区块链的密钥系统的可靠管理，避免了中心化密钥管理系统在单节点发生故障情况下可靠性差的问题。当来自外界的攻击试图篡改密钥系统时，需要同时攻击大量的边缘计算装置，难度将急剧上升。基于区块链技术的智能电表密钥管理模型如图3所示，其主要包含以下4个步骤。

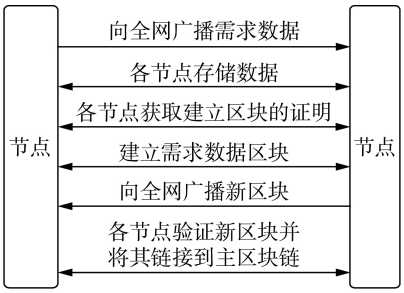

图3 基于区块链技术的智能电表密钥管理模型

Fig.3 Key management model of smart meter based on blockchain technology

(1)密钥生成。

新的智能电表接入AMI系统后，首先生成其唯一有效的密钥，边缘计算装置对密钥信息进行数字签名，生成初始区块，并将密钥的数字签名向全网广播。初始区块包含图2中的所有信息。为了构成区块链以增加密钥存储的安全性以及抗篡改性，区块链采取工作量证明PoW(Proof of Work)机制，首先设置难度系数可变的数学题，而每个边缘计算装置通过求解数学题(即算力展示)的方式竞争密钥数字签名的存储权。当某一边缘计算装置最先获得存储权时，便立即向全网广播，其余节点便停止该密钥存储权的竞争，转而竞争下一个智能电表密钥的存储权，至此完整的区块链形成。新形成的区块链同样按照图2所示结构进行创建。

(2)密钥查询。

当智能电表需要对用电数据进行加密处理时，首先向当前边缘计算装置查询密钥信息，节点会在本地进行搜索，从区块链末端开始，依次向前确认每个区块是否包含对应的密钥数据，当查询到有效的区块时，停止搜索。如果有效区块的区块体存储在本地，则当前边缘计算装置直接将密钥信息下发给智能电表；否则，节点向区块链网络中的其余节点发起请求。各个边缘计算装置在验证请求的有效性之后，发起本地查询，如果该有效区块体存储在本地，则节点会返回该区块的所有信息至当前边缘计算装置，再由当前边缘计算装置将密钥信息转发到智能电表。

(3)密钥更新。

当智能电表的密钥发生变更时，需要对区块链进行更新，智能电表首先生成新的密钥，使用旧密钥对新的密钥进行信息签名，并将其发送给边缘计算装置。区块链系统会采用密钥生成的方式生成一个新的区块添加到区块链链尾，当智能电表向节点发起密钥查询时，节点由区块链链尾向前搜索，检索到最新密钥区块后即停止搜索，因此旧密钥区块不会被检索到，从而自动失效。若失效的密钥区块处于区块链链首，则该区块会被节点自动忽视，不再对其进行维护管理。

(4)密钥注销。

当智能电表数据不再使用密钥加密，或者密钥被恶意篡改、窃取时，可以向节点申请密钥注销。此时智能电表可以生成一个空密钥，采用密钥更新的方式将其上传至边缘计算装置，边缘计算装置在区块链链尾添加包含这一信息的区块，当节点再次检测到该区块时，自动识别为密钥已注销。

2.2.2 基于排队论的智能电表密钥按需传输机制

由图3可以看出，影响区块链建链时间的因素主要包括以下2个方面：①PoW共识机制中求解数学题所耗费的时间；②构建过程中2次全网广播操作的传输延时。对于前者，在后续仿真实验中仅将难度系数设定为较小的数值；而本文主要关注后者，即尽可能地缩短传输延时。这是因为传统区块链中的建链时间间隔一般在10 min以上，因此无需过多关注数据传输算法的优化设计。但是在智能电表密钥管理中应用区块链技术时，由于智能电表的数量庞大，而边缘计算装置的通信资源有限且数据传输过程中存在数据丢失、重传现象，从而影响智能电表密钥维护的时效性。因此，通过借鉴通信网络中的路由算法设计思想，本文提出一种基于排队论的按需传输机制。与传统的不考虑信道带宽的区块链构建方法相比，本文所提方法能够自适应地选择负载最低的链路作为传输路径，从而提升了数据传输的时效性。

可将数据请求事件视为一泊松事件[13]，其平均到达率为λ；而各边缘计算装置则按照先到先服务FCFS(First Come First Served)的方式转发数据，其转发率为μ。从而节点的转发强度ρ可定义为：

$$\rho=\frac{\lambda}{\mu} \tag{5}$$

设各边缘计算装置的通信缓存资源容量配置为M，从而边缘计算装置对数据的处理过程可建模为M/M/1的排队模型。根据排队论相关知识，整个边缘计算装置区块链的丢包率P_{loss}和节点排队等待时间τ_{delay}如式(6)所示。

$$\begin{cases} P_{\text{loss}} = \dfrac{1-\rho}{1-\rho^{M+1}}\rho^{M} \\ \tau_{\text{delay}} = \dfrac{L_{\text{s}}}{\bar{\rho}} = \dfrac{\dfrac{\rho}{1-\rho} - \dfrac{(M+1)\rho^{M+1}}{1-\rho^{M+1}}}{\lambda(1-P_{\text{loss}})} \end{cases} \tag{6}$$

其中，L_{s}和$\bar{\rho}$分别为节点的平均排队长度和平均服务强度。而对于一个需要r个转发节点的区块链而言，其数据包长度、物理传输时间均固定，因此影响建链时间的主要因素即为排队总时长τ_{Σ}，如式(7)所示。

$$\tau_{\Sigma} = \sum_{j=1}^{r} (\tau_{\text{delay\_}j} + P_{\text{loss}} t_{wj}^{r}) \tag{7}$$

其中，$\tau_{\text{delay_}j}$为节点j的排队等待时间；t_{wj}^{r}为节点j数据包因丢失而重传的等待时间，一般为定值。此外，为了衡量区块链的网络性能，本文提出以负载均衡度作为性能指标，如式(8)所示。

$$L_{\text{load}} = \sqrt{\frac{(B_j - \overline{B})^2}{N_{\text{Num}}}} \tag{8}$$

其中，L_{load}为区块链的负载均值；B_j为区块链节点j到其余节点路径上的空闲带宽；$\overline{B}$为所有路径上空闲带宽均值；N_{Num}为链路数量。

进一步地，本文所提按需传输机制可转化为带约束的负载均衡度优化问题，如式(9)所示。

$$\begin{cases} \min\ L_{\text{load}} \\ \text{s.t.}\quad \tau_{\text{delay}} \leqslant T_{\max} \\ \qquad B_j \geqslant 0 \\ \qquad h \leqslant H_{\max} \end{cases} \tag{9}$$

其中，$T_{\max}$为区块链节点的延时约束；$H_{\max}$为区块链节点跳数h的约束。对于上述问题，可采用基于贪心策略的方法进行转发路径求解，具体求解思路本文不再赘述。

此外，需要指出的是，上述机制对新智能电表的加入具有良好的可扩展性。对于一个新的智能电表而言，在采用2.1节中所述*K*-means聚类算法对其进行分类后，由于并未对区块链的共识、合约等机制进行修改，故只需要更新执行按需传输机制确定数据转发路径即可。

3　实验仿真分析

为了验证本文所提方法的有效性与可行性，实验采取NS2半实物仿真的形式进行，边缘计算装置采用海兴电力PL系列配变终端装置，配置Huawei Hi-Grid T1主控板，硬件配置选择为CPU 700 MHz双核工业级，内存512 MB，Flash 1 GB，软件则选择Golang语言进行区块链中椭圆曲线签名、智能合约验证、PoW等关键算法的编写，并通过Hyperledger Fabric 1.4版本搭建智能电表密钥存储与管理系统，将其部署于边缘计算装置上，以保证所有边缘计算装置采用统一的版本协议进行区块链创建，从而避免了区块链分叉问题。考虑到边缘计算装置的算力有限并且电力业务场景有时效性要求，PoW共识机制中的难度系数值设定为8位二进制数00000100（对应于十进制数8），按照文献[14]中所提算法流程进行编写。智能电表与边缘计算装置之间以及边缘计算装置与边缘计算装置之间的通信网络采用NS2环境中的虚拟网络进行仿真，代替真实的HPLC和微功率无线网络。智能电表采用面向对象协议，在NS2中使用数据包大小为360 Byte的源节点进行等效，其与边缘计算装置之间的通信速率为25~128 KByte / s。智能电表请求数据的平均到达率λ为50~200 packet / s，边缘计算装置的转发速率μ=25 Mbit / s。

3.1　基于*K*-means算法的智能电表聚类效果分析

本节首先进行所提无监督学习*K*-means算法（配置方案1）的聚类性能分析。图4(a)给出了在3.5 km×4 km网格内300个智能电表的空间分布位置。仿真时设每个边缘计算装置最多可以承载25个智能电表同时发起数据请求，并考虑一定的计算裕量，从而边缘计算装置的配置数量确定为N=13。对比方法选择为文献[15]中所提的基于Voronoi图的空间区域划分算法，其时间复杂度为$O(N\lg N)$，每次迭代过程中均采用图中央点作为边缘计算装置的配置点（配置方案2）；但与*K*-means聚类算法的不同点在于，其使用三角剖分方法将空间上的点集划分到预设的边缘计算装置集合中。由于*K*-means算法的时间复杂度为$O(N)$[16]，因此从时间复杂度而言，本文所提算法具有更高的执行效率。另外，本文同样考虑了以1 km×1 km网格进行简单无聚类的边缘计算装置布置，选择图中央点为边缘计算装置的配置点（配置方案3）。图4(b)—(d)给出了3种配置方案下边缘计算装置的分布。对图4(b)—(d)所示布置方案中的边缘计算装置分别按照从左到右、从上到下的顺序进行编号，图5给出了配置这3种方案中每个边缘计算装置下智能电表的数量，对应的方差分别为18.74、25.74、158.58。由图4和图5可知，由于基于*K*-means算法的配置方案下智能电表的数量方差比基于Voronoi图的配置方案和简单无聚类网格的配置方案分别低27.20%、88.18%，这表明本文所提方案能够使智能电表的划分更加均衡，结合*K*-means算法在时间复杂度上的优势，从而验证了本文所提方法的有效性。

进一步地，本节讨论了智能电表规模对区块链建链的影响。当智能电表规模较大时，由于更新、加入或退出更为频繁，因此体现在智能电表的平均到

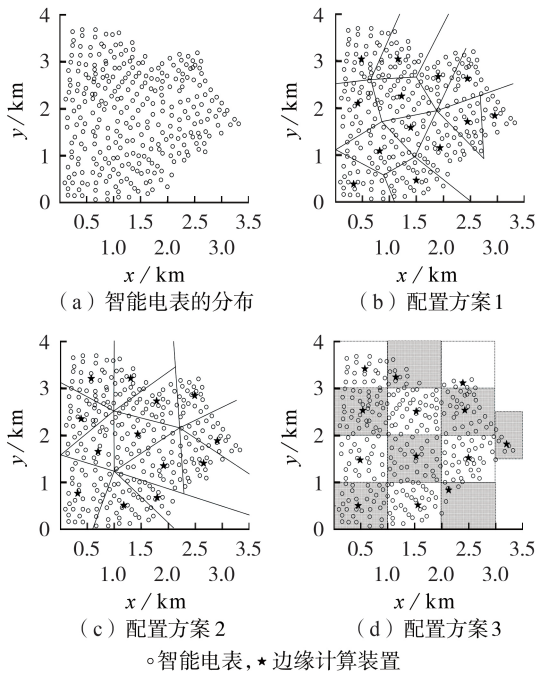

图4 3种配置方案下的边缘计算装置分布

Fig.4 Distribution of edge computing devices under three configuration schemes

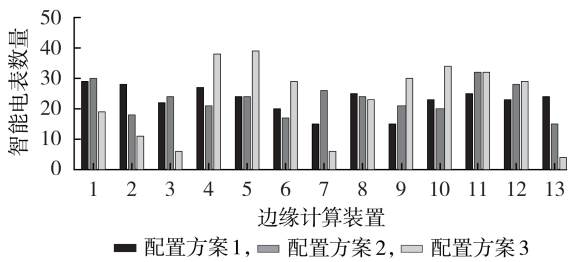

图5 3种配置方案中边缘计算装置下的智能电表数量

Fig.5 Number of smart meters in edge computing devices under three configuration schemes

达率将更高。表1给出了λ为50~200 packet/s、步长为50 packet/s时区块链的建链时间与边缘计算装置的负载均衡度。从表1中可知，随着智能电表规模的扩大，边缘计算装置的区块链建链时间与负载均衡度均有所上升，但建链时间的数量级仍为毫秒级，能够满足诸如需求响应、交易结算、大数据分析挖掘等场景。

表1 建链时间与负载均衡度随到达率的变化关系

Table 1 Change relationship between chain establishment time and load balancing degree with arrival rate

λ/(packet·s^{-1})	建链时间/ms	负载均衡度	λ/(packet·s^{-1})	建链时间/ms	负载均衡度
50	61.23	67.0	150	200.79	197.5
100	120.58	130.7	200	280.64	270.3

3.2 基于按需传输机制的边缘计算装置区块链建链时间分析

本节讨论了不同的传输算法对区块链建链时间的影响。对比算法选择为文献[17]中所提边缘计算装置最短路径传输算法、文献[18]中所提基于节点通信可靠性标度的数据传输算法以及文献[19]中所提计及链路剩余容量的数据传输算法。图6和图7分别给出了不同数据传输算法下边缘计算装置的数量从1增加到20时的建链时间与负载均衡度的变化情况。从图中可以看出，所有算法的建链时间和负载均衡度都随着区块链中节点数量的增加而增大。然而，相比于传统建链算法，采用本文所提按需传输机制的建链时间和负载均衡度均有所减小。此外，当节点数量从1变化到10时，采用本文所提按需传输机制的建链时间的增长幅度比文献[17]中最短路径传输算法、文献[18]中链路可靠性标度传输算法、文献[19]中链路剩余容量传输算法分别小19.83%、8.18%、14.40%，而相应的负载均衡度增长幅度则比3种传统建链算法分别小73.05%、49.94%、42.16%。这是因为本文所提算法优化了数据在不同区块链节点之间的传输机制，通过选择使整个区块链网络负载均衡度最小的传输路径来实现数据的优化传输。

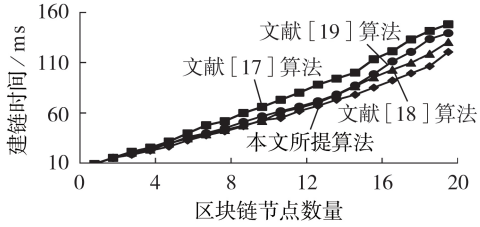

图6 建链时间随区块链节点数量的变化关系

Fig.6 Relationship between chain establishment time and number of blockchain nodes

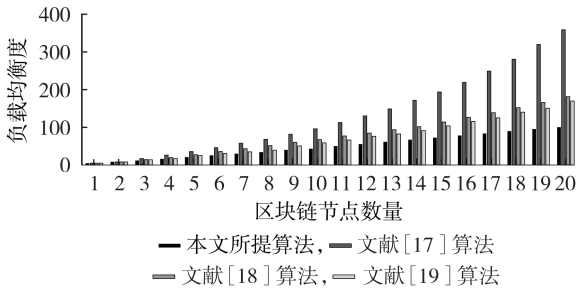

图7 负载均衡度随区块链节点数量的变化关系

Fig.7 Relationship between load balance degree and number of blockchain nodes

4 结论

本文提出了一种基于区块链与*K*-means聚类算法相结合的智能电表密钥管理方法。针对传统区块链构建过程中存在区块链节点过多从而影响建链时间的缺点，采用*K*-means聚类算法和基于排队论的按需传输机制进行改进，算例实验结果表明所提方法具有更短的建链时间和更好的负载均衡度，从而

表明相较于传统的区块链算法，本文所提算法具备更优的可实现性。由于所提方法中仍延续采用传统的共识算法进行智能电表身份的认证，故未来的研究工作将着眼于对共识算法的改进，以进一步提升其时效性与算法的实用性。此外，未来还将进一步研究新的边缘节点布置算法以克服*K*-means算法对智能电表加入或退出敏感的缺点。

参考文献：

[1] 余贻鑫. 智能电网实施的紧迫性和长期性[J]. 电力系统保护与控制，2019，47(17)：1-5.
YU Yixin. Urgency and long-term nature of smart grid implementation[J]. Power System Protection and Control，2019，47(17)：1-5.

[2] BENMALEK M，CHALLAL Y. MK-AMI：efficient multi-group key management scheme for secure communications in AMI systems[C]//2016 IEEE Wireless Communications and Networking Conference. Doha，Qatar：IEEE，2016：1-6.

[3] BENMALEK M，CHALLAL Y，BOUABDALLAH A. Scalable multi-group key management for advanced metering infrastructure[C]//2015 IEEE International Conference on Computer and Information Technology；Ubiquitous Computing and Communications；Dependable，Autonomic and Secure Computing；Pervasive Intelligence and Computing. Liverpool，UK：IEEE，2015：183-190.

[4] CHANG S H，WILLIAM T，WU W Z，et al. Design of an authentication and key management system for a smart meter gateway in AMI[C]//2017 IEEE 6th Global Conference on Consumer Electronics(GCCE). Nagoya，Japan：IEEE，2017：1-2.

[5] HSIAO C Y，CHEN W J. Secure key update scheme for smart meters[C]//2016 3rd International Conference on Green Technology and Sustainable Development(GTSD). Kaohsiung，China：IEEE，2016：170.

[6] SEFERIAN V，KANJ R，CHEHAB A，et al. Identity based key distribution framework for link layer security of AMI networks[J]. IEEE Transactions on Smart Grid，2018，9(4)：3166-3179.

[7] TSAI J L，LO N W. Secure anonymous key distribution scheme for smart grid[J]. IEEE Transactions on Smart Grid，2016，7(2)：906-914.

[8] 马天男，彭丽霖，杜英，等. 区块链技术下局域多微电网市场竞争博弈模型及求解算法[J]. 电力自动化设备，2018，38(5)：191-203.
MA Tiannan，PENG Lilin，DU Ying，et al. Competition game model for local multi-microgrid market based on block chain technology and its solution algorithm[J]. Electric Power Automation Equipment，2018，38(5)：191-203.

[9] 江秀臣，罗林根，余钟民，等. 区块链在电力设备泛在物联网应用的关键技术及方案[J]. 高电压技术，2019，45(11)：3393-3400.
JIANG Xiuchen，LUO Lingen，YU Zhongmin，et al. Technologies and solutions of blockchain application in power equipment Ubiquitous Internet of Things[J]. High Voltage Engineering，2019，45(11)：3393-3400

[10] 黄虹，文康珍，刘璇，等. 泛在电力物联网背景下基于联盟区块链的电力交易方法[J]. 电力系统保护与控制，2020，48(3)：22-28.
HUANG Hong，WEN Kangzhen，LIU Xuan，et al. Power trading method based on consortium blockchain under Ubiquitous Power Internet of Things[J]. Power System Protection and Control，2020，48(3)：22-28.

[11] 龙洋洋，陈玉玲，辛阳，等. 基于联盟区块链的安全能源交易方案[J/OL]. 计算机应用.(2020-01-09)[2020-03-18]. http://kns.cnki.net/kcms/detail/51.1307.TP.20200109.1438.028.html.

[12] 黄怀东，薛冰，李伟华，等. 基于AMI的需求侧响应方法设计与系统实现[J]. 电工技术，2017(10)：41-42.

[13] 杨挺，赵俊杰，张卫欣，等. 电力信息物理融合系统数据区块链生成算法[J]. 电力自动化设备，2018，38(10)：74-80.
YANG Ting，ZHAO Junjie，ZHANG Weixin，et al. Data blockchain generation algorithm of cyber physical power system[J]. Electric Power Automation Equipment，2018，38(10)：74-80.

[14] 钱斌，蔡梓文，肖勇，等. 基于边缘计算的电表计量系统数据协同检测方案[J]. 中国电力，2019，52(11)：145-152.
QIAN Bin，CAI Ziwen，XIAO Yong，et al. Data collaborative detection scheme of electric metering system based on edge computing[J]. Electric Power，2019，52(11)：145-152.

[15] 冯瑛敏，赵新，任国岐，等. 城市集中型充电站规划方法[J]. 电力系统及其自动化学报，2018，30(8)：58-61，67.
FENG Yingmin，ZHAO Xin，REN Guoqi，et al. Planning method for urban centralized charging stations[J]. Proceedings of the CSU-EPSA，2018，30(8)：58-61，67.

[16] 张朝，郭秀娟，张坤鹏. *K*-means算法聚类中心选取[J]. 吉林大学学报(信息科学版)，2019，37(4)：437-441.
ZHANG Zhao，GUO Xiujuan，ZHANG Kunpeng. Clustering center selection on *K*-means clustering algorithm[J]. Journal of Jilin University(Information Science Edition)，2019，37(4)：437-441.

[17] 王建平，王梦彪，王金玲，等. 智能配电网通信实时性与可靠性QoS路由机制研究[J]. 电子测量与仪器学报，2013，27(3)：187-193.
WANG Jianping，WANG Mengbiao，WANG Jinling，et al. Research on real-time and reliability of intelligent distribution networks QoS routing mechanism[J]. Journal of Electronic Measurement and Instrument，2013，27(3)：187-193.

[18] 王文华，贾晓纯，陈兴渝. 基于平衡树的智能电网数据采集路由算法[J]. 北京邮电大学学报，2015，38(增刊1)：41-44.
WANG Wenhua，JIA Xiaochun，CHEN Xingyu. Balanced tree based routing algorithm for smart grid data collection[J]. Journal of Beijing University of Posts and Telecommunications，2015，38(Supplement 1)：41-44.

[19] 薛俏，丁慧霞，张庚，等. 基于Q Learning算法的电力通信业务路由规划[J]. 光学与光电技术，2019，17(4)：51-56.
XUE Qiao，DING Huixia，ZHANG Geng，et al. Routing method for power communication network based on Q Learning[J]. Optics & Optoelectronic Technology，2019，17(4)：51-56.

作者简介：


翟　峰

翟　峰(1979—)，男，山东济南人，高级工程师，博士研究生，主要研究方向为电气工程、智能用电与网络安全等(**E-mail**：epri_zhaifeng2019@163.com)；

杨　挺(1979—)，男，天津人，教授，博士研究生导师，主要研究方向为电力信息物理系统、区块链；

曹永峰(1987—)，男，河北辛集人，工程师，硕士，主要研究方向为信息安全、智能用电等；

李双全(1986—)，男，湖南常德人，工程师，研究方向为电能计量、信息安全、智能用电等。

(**编辑**　陆丹)

Key management method of smart meter based on blockchain and *K*-means algorithm

ZHAI Feng[1,2], YANG Ting[1], CAO Yongfeng[2], LI Shuangquan[3]

(1. Key Laboratory of Smart Grid of Ministry of Education, Tianjin University, Tianjin 300072, China;
2. Institute of Metrology, China Electric Power Research Institute, Beijing 100192, China;
3. Hexing Electrical Co., Ltd., Hangzhou 310011, China)

Abstract: With the development of power internet of things, the advanced metering infrastructure of power systems has gradually formed a "cloud-edge-end" three-tier architecture consisting of many intelligent meters, edge computing devices and cloud master stations. In this context, the traditional centralized smart meter key management mechanism has the problems of high dependence on the master station, poor key storage efficiency and slow response speed. Therefore, a distributed key management method of smart meter is proposed based on blockchain and *K*-means algorithm. Considering that the number of block nodes in the process of building a traditional blockchain has a great impact on the timeliness of building a chain, and the problem of limited communication and transmission resources of nodes is not considered, firstly, the *K*-means algorithm is used to cluster the smart meters by spatial distribution. The central point algorithm is used to determine the location of edge computing devices, so as to reduce the blockchain size. Then, the on-demand transmission mechanism that takes into account the communication bandwidth of smart meters is proposed. The transmission path in the blockchain node is planned with the goal of minimizing the load balance of edge computing devices, so as to improve the transmission timeliness. Finally, the example results of smart meter key management based on the Hyperledger Fabric platform show that, compared with the traditional blockchain building algorithm without considering the node size and channel bandwidth, when the number of blockchain nodes increases, the chain building time growth rate of the proposed algorithm is reduced by more than 8.18%, while the load balance growth rate is reduced by more than 42.16%. The proposed smart meter key management method has faster chain building speed and better network performance, so it has better feasibility.

Key words: smart meter; key management; blockchain; *K*-means algorithm; power internet of things; load balance