基于区块链的用能数据完整性保护框架

韦 涛[1],周治平[1,2]
(1. 江南大学 物联网工程学院,江苏 无锡 214122;
2. 江南大学 物联网技术应用教育部工程研究中心,江苏 无锡 214122)

摘要:终端设备的分布式拓扑结构和节点有限的计算资源给区块链和用能信息采集系统集成带来很大阻碍,为此,提出基于区块链的多层互连数据保护框架(HBDF),用于能源互联网下的用能数据安全采集。HBDF以分散方式对终端设备进行身份认证来克服单点故障问题以及提高系统的可扩展性。利用基于截断式哈希消息认证码(HMAC)的承诺方案构建轻量级数据完整性验证方案,该方案利用反向哈希链表对验证密钥进行更新来减轻受限节点的计算负担。对框架安全性的分析表明,其可对通信实体和内容进行有效认证。实验验证了该框架的可行性。

关键词:区块链;智能电网;用能数据保护;终端身份认证;完整性验证
中图分类号:TP 73;TP 393 **文献标志码**:A DOI:10.16081/j.epae.202108010

0 引言

随着智能电网SG(Smart Grid)的不断建设,各种数据采集设备和信息管理系统被集成[1],在能源消费环节中,建设用能单位在线监测系统是其中的重点[2]。能源计量设备会生成大量用能数据,这些数据的完整性关系到设备和在线监测系统的安全性,对上层能耗监测和数据分析应用的影响较大,因此,用能数据的完整性愈发受到关注。用能数据完整性需求包括:通信完整性,指使通信接收方可确保发送方身份的真实有效性;信息完整性,指使通信接收方能对发送信息进行有效验证,保证信息在通信过程中未被修改、删除或重放;系统完整性,指对智能电网基础平台、控制采集系统、数据存储和业务系统进行防护,使数据具有不被篡改及可审计的特性。

Deswarte等人最早提出数据完整性验证概念[3],其通过计算和比较消息认证码MAC(Message Authentication Code)值,提出2种解决方案来确定远程节点上的数据是否完整,但这些方案的通信开销及计算成本较大。文献[4]减少签名过程中哈希函数的计算开销,并使用随机掩码技术保护数据隐私。考虑到图形数据库的特殊性和复杂性,文献[5]提出2个基于哈希消息认证码HMAC(Hash Message Authentication Code)的安全性概念,用于验证图形数据完整性和查询结果。但传统方法通常依赖于受信任的第三方审计员TPA(Third Party Auditor)来执行审计任务,然而TPA并不完全值得信赖,尤其是在多个利益体联合管理的智能电网场景[6]。

区块链最初是用于加密货币的底层技术[7],是在不依赖可信第三方的情况下解决各节点间建立信任的问题,这与传统密码学相辅相成,为解决智能电网用能数据安全采集问题提供了新方法。区块链在智能电网下各场景的应用及其商业价值已被广泛讨论和发掘[8]。文献[2]结合能耗采集的业务需求和业务难点分析区块链技术的价值。现有利用区块链技术进行用能数据保护的研究主要集中在保护数据存储安全方面[9-10],而较少涉及与授权有关的远程保护智能电网中的用能数据资源,在运行环境越来越复杂的情况下,将数据上传到区块链之前保证数据的完整性对确保基于区块链系统的功能实现至关重要。文献[11]将以太坊作为智能电网实体间通信的基础设施,并以智能合约(SC)进行通信实体身份管理,安全且私密地对能耗数据进行采集,但其方案的可扩展性和成本都受到很大限制。文献[12]致力于电力数据精准读取和安全存储,将所读数据的加密哈希值存储在区块链网络中,尽管其实现了目标,但并未考虑基础分散账本的可扩展性,并且忽略了终端设备的计算/功率限制,例如在8~50 MHz、4~32 KB RAM和32~512 KB闪存的智能电表下,任何新的安全层都可能增加操作任务的复杂性[13]。

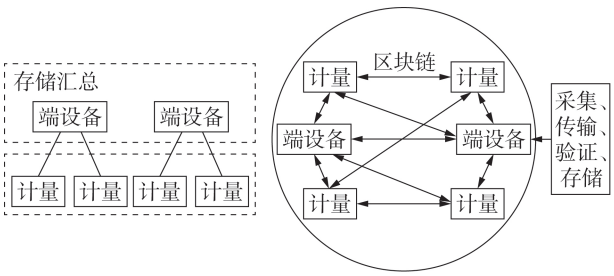
上述文献大多关注区块链在智能电网业务和数据存储中的应用,而没有考虑区块链视角下受限设备的身份管理以及频繁用能信息采集带来的终端设备计算负担问题。为此,本文提出一种基于区块链的多层互连数据保护框架HBDF(Hierarchical Blockchain Data Framework),利用区块链网络组织边缘多个智能体并管理分散的终端设备子集,利用截断式HMAC构建的承诺方案保护数据传输的完整性,并结合反向哈希列表更新密钥,最大限度地减少资源受限设备节点昂贵的密钥加密操作的使用次数。

1 能耗采集区块链框架概述

传统的中心化认证方式大多遵循策略决策点

收稿日期:2020-09-27;**修回日期**:2021-06-02

（PDP）和策略执行点（PEP）方案[14]，其将资源受限的PEP连接到PDP通过获取授权令牌进行访问控制。HBDF在传统PDP代理授权的框架上引入新的安全措施，通过区块链给分散的PDP提供可信任的执行环境，并提供系统的透明性和数据可追溯性。传统模式和区块链模式下能耗采集系统拓扑对比见图1。



（a）传统模式　　（b）区块链模式

图1　2种模式下能耗采集系统拓扑对比

Fig.1　Topological comparison of energy consumption collection system between two modes

通过边缘PDP节点为受限的计量设备PEP节点提供授权服务，该体系结构能够分散每个域的身份管理权限。与访问相关的大量数据集中在几个边缘PDP节点上，利用联盟链组织管理边缘节点。用能数据完整性保护框架如图2所示。

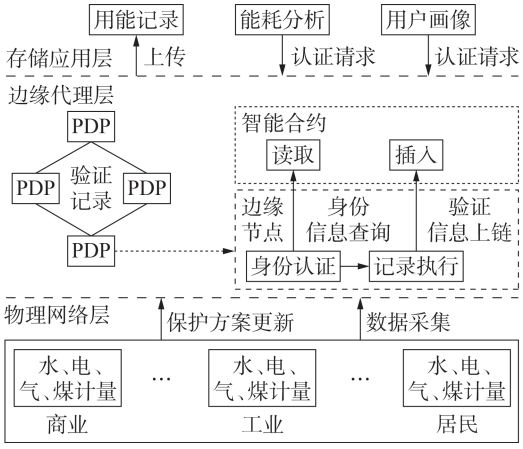


图2　用能数据完整性保护框架

Fig.2　Framework of energy consumption data integrity protection

1）物理网络层。在该层有多个相互独立的域，其包含大量能源计量器，包括水、电、气、煤等各种能源的消耗数据以及关联的采集设备信息[2]。设备部署在不同的用能单位和区域中进行感应，这些计量设备集合可按功能和系统的不同分类为不同管理域，每个域中PEP节点关联在几个高性能PDP节点上。

2）边缘代理层。该层包含一个启用了联盟链的PDP节点网络，将这些节点设置为代理节点，每个代理节点管理资源受限的PEP节点，代理节点相互通信同步身份验证、授权关联和完整性保护方案的相关信息，以实现事务的资源访问请求和系统数据完整性的验证。

3）存储应用层。云端、数据应用商和国家管理机构可合作存储大量用能数据，并协助边缘层进行能耗监测、节能管理以及提供数据服务。但云端和数据应用商不受完全信任，对手可能更改终端采集的用能数据，当发生这类事件时，边缘层区块链中的验证信息可以帮助最终用户检测到修改。

2　框架详细设计

2.1　终端可信认证

用能数据采集终端的可信认证是其数据完整性的基础，利用PDP节点为所在管理域中受限设备节点生成认证凭证来提供身份验证和委托授权的服务，并将注册信息和授权日志记录在联盟链中。

2.1.1　认证凭证生成

PDP节点的身份安全管理是计量终端设备安全认证的前提，因此在身份授权之前首先要将PDP节点通过平台管理员加入联盟链网络中，平台管理员为每个PDP节点生成唯一的ID（A_{ID}），该ID可由单位名称和启用了区块链的PDP节点的最后5个哈希数字组成。PDP节点利用私钥A_{IK}签名节点ID生成新证书$A_{IK}(A_{ID})$并创建事务将其分布在所有代理节点之间，且在全局部署PDP节点的认证管理合约SC-PDP，防止双重注册和PDP节点身份权限管理。同时为了更好地管理后续相关联的PEP设备，为每个PDP节点创建一个管理合约SC-PEP。用能单位下属的计量终端会通过平台管理员收到其注册后的PDP节点的证书，并且平台管理员将计量终端的公共地址列表与PDP节点共享，以防止添加任何恶意设备。

当PDP节点加入区块链后，其各个管理域中终端开始向收到的证书所对应的PDP节点注册和申请认证凭证。首先终端利用自身相关标识符生成一个注册令牌reg_token=$D_{IK}(D_{ID}, D_{IP}, A_{ID})$，其中包括终端设备编号（$D_{ID}$）、设备公共地址（$D_{IP}$）和被分配的PDP节点的ID（$A_{ID}$），并将生成的reg_token和管理员分发的$A_{IK}(A_{ID})$发给PDP节点申请身份凭证。如果提供的证书合法并且A_{ID}存在区块链中，则智能合约将验证区块链中是否存在用于验证reg_token的公钥，验证该公用地址与平台管理员之前保存的公用地址是否相同。在确认之后，PDP节点生成认证凭证auth_token=$A_{IK}(D_{ID}, D_{IP}, A_{ID})$，在各PDP节点达成共识后写入区块链中。最后，PDP节点向注册的设备提供名为auth_token的凭证，设备节点可用该凭证进行身份验证，其流程图如附录A图A1所示。

2.1.2　设备身份认证

在用能数据上传阶段，PDP节点需要对其管理的终端设备身份进行认证。PDP节点利用管理的终

端设备公钥D_{Pk}来验证数据包的合法性，并利用自身的公钥提取auth_token中的相关信息。然后区块链网络进行以下验证。

步骤1 通过SC-PDP合约检测提供管理域ID是否存在于区块链中。

步骤2 如果A_{ID}存在，则通过SC-PEP合约审计其提供的终端ID是否存在以及是否相关联。

步骤3 如果D_{ID}与A_{ID}相关联，则进一步检查提供的设备地址是否对应。

步骤4 通过SC-PEP合约检查给定的映射(D_{ID}，D_{IP}，A_{ID})是否有效。

若上述步骤均有效，则终端设备通过身份验证。该验证过程由智能合约自动执行，保证了验证流程的安全合法性。通过2.2节定制的数据完整性保护方案可减少SC-PEP合约执行次数。

2.2 能耗数据完整性保护

尽管数字签名可保护通信数据完整性，但大多能耗采集终端的计算和电源资源受限，不能承受计算密集型的非对称加密操作，尤其是高频计量设备和依赖电池供能的计量设备[13]。因此，本文在HBDF下定制轻量级的数据完整性保护方案，并利用区块链的不可篡改特性保证能耗数据后向安全性。

2.2.1 数据完整性保护方案

考虑到终端设备节点和通信数据特点，利用截断式HMAC构建承诺方案对消息进行完整性保护[15]。使用承诺方案延迟密钥信息的披露而不是利用加密来隐藏密钥，并对SHA-1加密哈希函数构建HMAC进行截断处理，将160 bit长度的消息认证码值截断至80 bit。同时为了减轻节点的计算负担，使用反向哈希链表对密钥进行更新来降低公共密钥加密的操作成本。该方案包括如下5个字段。

1)发送方。设备节点的认证凭证auth_token用于确认发送方的身份。

2)消息认证码长度。截断后的消息认证码长度为$\lambda(2s<\lambda<l)$。其中，s为抗碰撞强度；l为哈希函数输出消息认证码的长度。

3)密钥信息。其是指所选数据完整性机制中使用的密钥信息，设备节点可以选择HMAC或基于密码的消息认证码(CMAC)。

4)密钥更新频率。密钥更新频率f用来确定验证密钥使用的次数，当密钥用于一定时间的数据单元后，密钥从k_{i-1}更新为k_i，并停止使用k_{i-1}以确保新数据单元的完整性。

5)方案寿命。该字段是一个正整数n，用于确定更新验证密钥的最大次数，$N=nf$为方案保护的最大数据段数。

用能数据大多按固定的时间段间隔采集，因此采用以时间为基准的密钥更新手段来构建数据完整性保护方案。首先，设备节点会确定寿命字段n，并选择一个随机消息认证码密钥k_n。然后，设备计算$k_{n-1}\leftarrow H\left(k_n\|n-1\right)$、$\cdots$、$k_1\leftarrow H\left(k_2\|1\right)$，其中$H(\cdot)$为有足够输出大小的哈希函数(例如SHA-1)。密钥信息字段在创建时会向公众隐藏，以防止对手为假数据生成有效的消息认证码，但会在后续需要时进行公开，以允许他人使用密钥信息字段验证发件人生成的消息认证码。最后，节点确定密钥更新频率字段f，该字段还会影响验证数据完整性的等待时间，因为只有在密钥更新后之前的密钥才会被披露以进行数据完整性验证，新密钥才会被用来保护下一段数据。

在方案构建成功后，设备节点将数据段d_i在固定时段进行传输。设备节点在t_1时刻将k_1作为第一段的数据身份验证密钥，并将k_1计算截断后的MAC值m_1附加在元数据中发送到边缘区块链网络，同时在另一个信道传输分段的加密数据，其过程如图3所示。设备节点会在必要时将消息认证码密钥从$k_{i-1}(2\leqslant i\leqslant n)$更新为$k_i$。

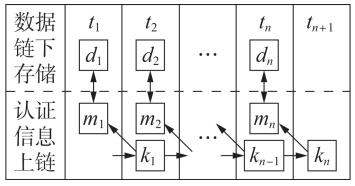


图3 终端发送数据过程

Fig.3 Terminal sending data process

2.2.2 数据完整性验证

终端设备在一段时间内产生的用能数据发送到云服务器存储，而边缘区块链节点负责管理和验证完整性信息。当云服务器接收并存储数据段m_i时，其完整性无法立即验证。数据应用方只有在t_{i+1}时刻设备节点提供了保护密钥k_i才能验证m_i是否完整，在该时刻其PDP节点验证等式(1)、(2)是否成立，如果均成立则数据段完整。

$$m_i=T(\mathrm{HMAC}(d_i,k_i))_\lambda \tag{1}$$

$$H\left(k_i\|i-1\right)=k_{i-1} \tag{2}$$

式中：函数HMAC$(\cdot)$用于消息认证码的计算；函数$T(\cdot)$用于对消息认证码进行截断处理。截断后λ=80 bit，HMAC抗碰撞强度即为$\lambda/2$=40(bit)，即使对HMAC进行截断降低了消息认证的强度，也仍可以满足实际工业控制系统数据完整性的需要[15]，这是由于对于高频用能数据的采集，其能耗数据主要用于智能预测模块的输入，而不用于计费功能，其与工业控制中数据采集的用途类似，且智能电网属于工业4.0的分支。密钥更新频率f的选择可根据数据实时性要求确定，对于实时性要求不高的数据应用方，可以降低密钥更新频率以节省受限设备计算资源，而对于实时性要求较高的数据应用方，可以提高

密钥更新频率以缩短验证等待时间。

3　实验与分析

3.1　完整性需求分析

3.1.1　通信完整性

本节采用有限状态机FSM(Finite State Machine)分析框架内终端身份管理的安全性，通过证明系统的初始状态和所有状态的转化函数安全，来证明整个身份管理系统安全。

首先定义相关的状态变量，模型的有限状态机系统定义为一个四元组模型$M=(V, I, O, F)$。其中，V为系统的有限状态集合；I为系统的输入集合；O为系统的输出集合；$F: V\times I\rightarrow V$为状态转换函数，表示在输入的驱动下从某个状态转换到另一个状态。根据以上定义的状态变量，身份认证状态的设置见表1。

表1　终端身份管理状态设置

Table 1　State setting of terminal identity management

集合	元素	含义
V	V_0	初始状态
	V_1	交易发送
	V_2	节点关联认证成功
	V_3	终端身份认证成功
	V_4	终端身份认证失败
	V_5	认证结束
I	I_0	PEP生成事件
	I_1	从SC-PEP调用判断函数
	I_2	从SC-PDP调用判断函数
	I_3	允许事件生成上链
	I_4	不满足认证条件
	I_5	身份认证结束
O	O_0	发送交易和调用函数
	O_1	获取关联设备信息判断结果
	O_2	获取设备认证结果
	O_3	接受交易
	O_4	拒绝接受交易
	O_5	结束身份认证整个流程

根据定义的状态变量，整个流程的状态转换函数包括如下5个子函数。

1）$F_1: V_0I_0\rightarrow V_1$。该函数表示PEP设备生成事件请求，包括数据完整性方案的上传、能耗数据上传和消息认证码密钥更新。

2）$F_2: V_1I_1\rightarrow V_2/V_4$。该函数表示调用SC-PEP中的函数对设备关联属性进行判断。

3）$F_3: V_2I_2\rightarrow V_3/V_4$。该函数表示调用SC-PDP中的函数对PDP设备身份进行认证，并对PDP节点身份权限进行决策。

4）$F_4: V_3I_3\rightarrow V_5$。该函数表示监听事件返回结果，如果对终端设备认证成功，则允许交易上链。

5）$F_5: V_4I_4\rightarrow V_5$。该函数表示监听事件返回结果，如果对终端设备认证失败，则拒绝处理交易。

状态转化示意图如图4所示。

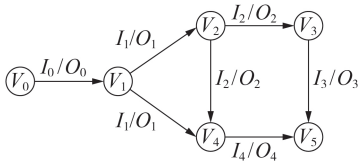


图4　状态转化示意图

Fig.4　Schematic diagram of state transition

在初始状态V_0没有任何交易，合约仅被部署而没有被调用，系统没有任何操作，其初始状态是安全的。假设PEP终端发起一个安全的交易请求，当前系统状态V_1安全。在区块链环境中智能合约可自动执行指定操作，若PEP终端拥有正确认证凭证满足认证条件，则系统输出为设备终端已被关联；同理，所关联的PDP节点身份信息会被审核，且事务请求操作是可溯源、防篡改的，因此状态V_2、V_3安全。当合约的输出是认证失败时，系统不会有任何操作，能够保持系统的安全性，因此状态V_4安全。根据分析可知，若系统初始状态V_0和状态转化函数F安全，则对终端身份的管理是安全的。

3.1.2　信息完整性

本文利用定制数据完整性保护方案替代传统数字签名。在该方案中，哈希承诺方案的绑定功能可确保在生成和发布承诺后任何人都无法修改承诺的值，因此对手想要破坏数据段d_i的完整性就必须在m_i值上链前生成一个有效的消息认证码，根据式(1)，对手需学习到未使用的保护密钥。本文将SHA-1作为$H(\cdot)$，当$H(\cdot)$的输入与输出大小相同时，密钥k_i由多次哈希运算$H(\cdot)$组成，其生成过程等效于$n-i$次哈希迭代，这不会影响其原像抵抗功能。因此，只要底层的密码哈希函数有原像抗性且原始输入大小等于哈希函数的输出大小，并且保证密钥k_n的机密性，对手就几乎无法学习到未使用的身份验证密钥。在密钥k_n披露前，代理节点收到经身份认证后节点发来的承诺并将其存储在区块链中，且节点承诺对密钥保密，承诺方案的隐藏功能可确保护密钥k_n的机密性。

3.1.3　系统完整性

本文数据完整性保护框架基于区块链平台，提供多方联合管理的可信的执行环境，同时区块链保证了上链数据不可篡改特性，即使对手拥有一个完整性保护方案内所有消息的认证码密钥，也不能破坏历史数据。

3.2　性能分析与比较

3.2.1　实验环境

为测试本文基于区块链的数据完整性验证框架的性能和可操作性，本节采用IBM的Hyperledger Fabric 1.4网络搭建边缘联盟区块链验证环境。通过将数据生成终端应用程序单独打包成Docker容器模拟采集终端，利用3.3 / GHz速度CPU、16 GB内存、256 GB

SSD、Ubuntu18.04操作系统的PC机作为服务器。

3.2.2 性能分析

HBDF使用数据完整性保护方案来保护能耗数据的完整性。对于终端采集设备，它生成使用完整性保护方案来保护一个时间段内数据的完整性，然后更新方案密钥信息生成新的方案。本节分析和对比新增数据完整性保护方案和现有文献方案对完整性保护的计算和通信成本。

生成数据完整性保护方案是本文框架新增的阶段，终端设备需通过生成数字签名向边缘区块链节点提交数据完整性验证方案。终端设备的计算成本仅来自生成一次数字签名，而通信成本来自传输一次数字签名和方案。数据完整性保护方案主要由消息认证码密钥和消息认证码生成，终端设备需预先计算反向的哈希链表，哈希计算的次数由寿命字段n确定。为提交第i个数据段，若节点不存储任何中间结果，则在原始消息认证码密钥上计算$n-i$个哈希生成密钥k_i及其消息认证码值。因此，当节点没有缓存任何之前的计算结果时，计算复杂度为$O(n^2)$次哈希计算和生成每段数据的消息认证码，其与给定方案保护的数据量成正比，通信成本来自传输N次哈希值及其对应的消息认证码。数据验证信息上链主要是节点数据生成的消息认证码值和消息认证码密钥插入区块链中，某时刻验证信息虽有m_i和k_{i-1}两段，但其大小为240 bit，而文献[12]中以数据哈希值为验证信息的大小为256 bit。完整性保护方案的加入会带来额外的验证延迟，除了区块链操作的固有延迟外，密钥的更新频率f也影响完整性验证的时效性。

当方案寿命为n时，在一个周期内该方案终端设备上的计算量为单次签名操作、n^2次哈希计算和N次消息认证码操作。文献[11-12]在数据完整性保护中均利用数字签名保证每段数据传输的完整性，并将每段数据哈希值与存储索引生成交易存储在区块链上以供完整性验证，其在N段数据段完整性保护上需要进行N次签名和哈希操作，同时数据完整性保护方案的增加，在区块链网络中的通信次数仅增加了1次完整性保护方案的提交。

3.2.3 性能比较

为证明HBDF的有效性，本文选择文献[12]和文献[16]方案进行比较分析，其中文献[12]方案直接将数据的哈希结果存储到区块链网络，文献[16]构建一个用于完整性验证的默克尔树结构，结果对比见图5。每个数据段大小固定(1 KB)，数据段数量越多，HBDF越具有优势，并且完整性方案寿命对应的N(其中n=10)越大，完整性验证的开销越低，这主要是由于数据完整性验证方案减少了椭圆曲线数字签名(ECDSA)操作次数，且在资源受限的场景计算开销的差异更加明显。例如在ARM Cortex-M3处理器下，ECDSA大约需要486 ms来生成签名，而计算1 KB数据的SHA-256仅需要0.6 ms[17]。文献[16]在计算根节点时会受到Merkle树结构影响，Merkle层数越多，其验证成本就越高。

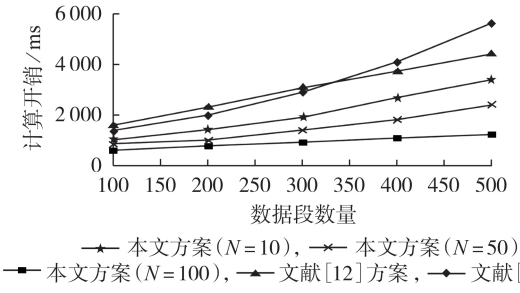


图5 不同数据段数量下的计算开销

Fig.5 Computational overhead for different numbers of data section

通信空间开销指在数据完整性保护和验证过程中在各部分间进行数据传输产生的数据量，各方案间通信空间开销的对比见图6。随着数据段(1 KB)数量的增加，通信空间开销呈线性增加。虽然HBDF新增了完整性验证方案字段，但额外通信空间开销较少，且其额外的通信次数仅为M/N次，其中M为数据总段数。同时虽然HBDF中有2段完整性验证信息，但仍比文献[12]中直接将数据的哈希值作为验证信息的开销低，而文献[16]中进行验证时需携带辅助的位置信息，因此其需更多的通信空间开销。

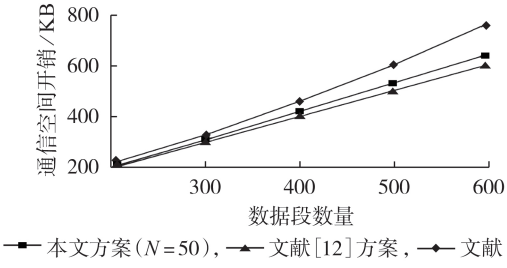


图6 通信空间开销对比

Fig.6 Comparison of communication space overhead

4 结论

本文研究了区块链视角下计算资源受限的用能采集终端身份认证和数据完整性保护方案，旨在解决终端设备进行频繁用能数据采集所带来的计算负担问题，同时保证用能数据的完整性。基于此，利用定制的完整性保护方案来减少终端数字签名次数，同时利用区块链保护验证信息的后向安全性，满足用能数据完整性的需求。

由于本文框架是基于区块链技术实现的，在实际拥有海量采集终端的智能电网环境下，区块链的共识算法会限制系统运行的实时性，因此未来工作将围绕研究和改进适合能源互联网的共识算法来提高框架的可行性。

附录见本刊网络版(http://www.epae.cn)。

参考文献:

[1] 翟峰,杨挺,曹永峰,等. 基于区块链与*K*-means算法的智能电表密钥管理方法[J]. 电力自动化设备,2020,40(8):38-46.
ZHAI Feng,YANG Ting,CAO Yongfeng,et al. Key management method of smart meter based on blockchain and *K*-means algorithm[J]. Electric Power Automation Equipment,2020,40(8):38-46.

[2] 曾隽芳,刘禹. 能耗监测中的区块链终端信任管理[J]. 电力自动化设备,2020,40(8):31-37.
ZENG Junfang,LIU Yu. Trust management of blockchain terminals in energy consumption monitoring[J]. Electric Power Automation Equipment,2020,40(8):31-37.

[3] DESWARTE Y,QUISQUATER J J,SAIDANE A. Remote integrity checking[C]//Working Conference on Integrity and Internal Control Information Systems. Boston,USA:Springer,2003:1-11.

[4] ZHU H L,YUAN Y,CHEN Y L,et al. A secure and efficient data integrity verification scheme for cloud-IoT based on short signature[J]. IEEE Access,2019,7:90036-90044.

[5] ARSHAD M U,KUNDU A,BERTINO E,et al. Efficient and scalable integrity verification of data and query results for graph databases[J]. IEEE Transactions on Knowledge and Data Engineering,2018,30(5):866-879.

[6] 朱西平,付迁,文红,等. 区块链视角下多能源主体储能优化配置模型[J]. 电力自动化设备,2020,40(8):47-56.
ZHU Xiping,FU Qian,WEN Hong,et al. Optimal allocation model of multi-energy entity energy storage from perspective of blockchain[J]. Electric Power Automation Equipment,2020,40(8):47-56.

[7] 袁勇,王飞跃. 平行区块链:概念、方法与内涵解析[J]. 自动化学报,2017,43(10):1703-1712.
YUAN Yong,WANG Feiyue. Parallel blockchain:concept,methods and issues[J]. Acta Automatica Sinica,2017,43(10):1703-1712.

[8] 王胜寒,郭创新,冯斌,等. 区块链技术在电力系统中的应用:前景与思路[J]. 电力系统自动化,2020,44(11):10-24.
WANG Shenghan,GUO Chuangxin,FENG Bin,et al. Application of blockchain technology in power systems:prospects and ideas[J]. Automation of Electric Power Systems,2020,44(11):10-24.

[9] YIN H,GUO D C,WANG K,et al. Hyperconnected network:adecentralized trusted computing and networking paradigm[J]. IEEE Network,2018,32(1):112-117.

[10] MUSLEH A S,YAO G,MUYEEN S M. Blockchain applications in smart grid-review and frameworks[J]. IEEE Access,2019,7:86746-86757.

[11] AKHRAS R,EL-HAJJ W,MAJDALANI M,et al. Securing smart grid communication using ethereumsmart contracts[C]//2020 International Wireless Communications and Mobile Computing(IWCMC). Limassol,Cyprus:IEEE,2020:1672-1678.

[12] CAO S,ZOU J C,DU X J,et al. A successive framework:enabling accurate identification and secure storage for data in smart grid[C]//ICC 2020-2020 IEEE International Conference on Communications(ICC). Dublin,Ireland:IEEE,2020:1-6.

[13] RUBIO J E,ROMAN R,ALCARAZ C,et al. Tracking APTs in industrial ecosystems:a proof of concept[J]. Journal of Computer Security,2019,27(5):521-546.

[14] ALCARAZ C,LOPEZ J,WOLTHUSEN S. Policy enforcement system for secure interoperable control in distributed smart grid systems[J]. Journal of Network and Computer Applications,2016,59:301-314.

[15] JIANG N,LIN H,YIN Z Y,et al. Performance research on industrial demilitarized zone in defense-in-depth architecture[C]//2018 IEEE International Conference on Information and Automation(ICIA). Wuyishan,China:IEEE,2018:534-537.

[16] YUE D D,LI R X,ZHANG Y,et al. Blockchain based data integrity verification in P2P cloud storage[C]//2018 IEEE 24th International Conference on Parallel And Distributed Systems(ICPADS). Singapore:IEEE,2018:561-568.

[17] TSCHOFEN H,PEGOURIE-GONNARD M. Performance of state-of-the-art cryptography on arm-based microprocessors[C]//NISTLightweight Cryptography Workshop. Gaithersburg,USA:[s.n.],2015:1-40.

作者简介:

韦　涛

韦　涛(1994—),男,江苏盐城人,硕士研究生,主要研究方向为区块链、物联网安全、网络安全(**E-mail**:6181913038@stu.jiangnan.edu.cn);

周治平(1962—),男,江苏无锡人,教授,博士,主要研究方向为工业网络信息安全(**E-mail**:zzp@jiangnan.edu.cn)。

(**编辑**　王锦秀)

Integrity protection framework for energy consumption data based on blockchain

WEI Tao[1],ZHOU Zhiping[1,2]

(1. School of Internet of Things Engineering,Jiangnan University,Wuxi 214122,China;
2. Engineering Research Center of Internet of Things Technology Applications Ministry of Education,Jiangnan University,Wuxi 214122,China)

Abstract:The distributed topological structure of terminal equipment and limited computational resource of nodes bring major obstacle to the integration of blockchain and energy consumption information collection system,for which,the HBDF(Hierarchical Blockchain Data Framework) is proposed for energy consumption data security collection under energy internet. The HBDF adopts a distributed mode to authenticate the terminal equipment to overcome the single-point failure and improve the scalability of system. A lightweight data integrity verification scheme is constructed by a commitment scheme based on truncated HMAC(Hash Message Authentication Code),which uses reverse hash linked list to update the verification key to reduce the computational burden of restricted nodes. The analysis of framework security shows that it can effectively authenticate the communication contents and entities. The experiment verifies the effectiveness of the framework.

Key words:blockchain;smart grid;energy consumption data protection;terminal identity authentication;integrity verification

附录A：

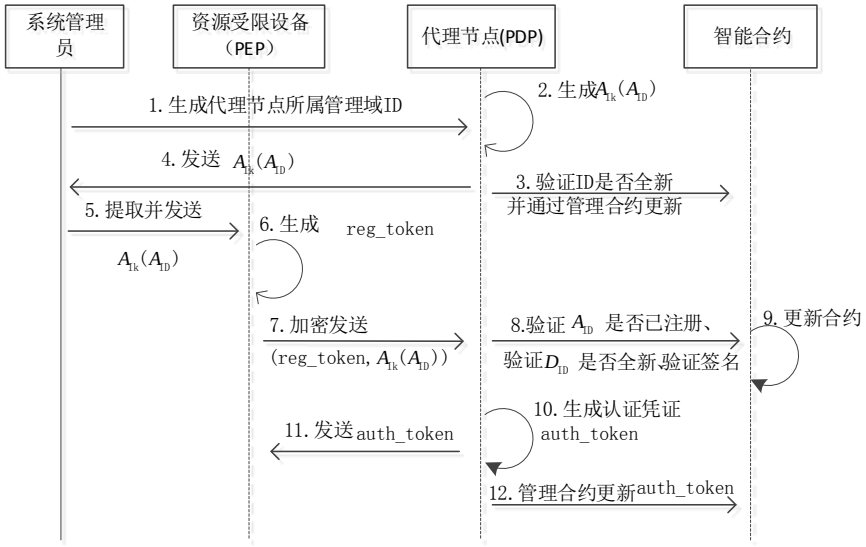


图 A1 认证凭证申请流程

Fig.A1 Authentication certificate application process