Journal of Computer Applications ISSN 1001-9081 2017-10-10
计算机应用,2017,37(10):2742-2747 CODEN JYIIDU http://www.joca.cn

文章编号:1001-9081(2017)10-2742-06 DOI:10.11772/j.issn.1001-9081.2017.10.2742

基于联盟区块链的智能电网数据安全存储与共享系统

吴振铨[1],梁宇辉[2],康嘉文[1*],余 荣[1],何昭水[1]

(1.广东工业大学 自动化学院,广州 510006; 2.广东电网有限责任公司 珠海供电局,广东 珠海 519000)

(* 通信作者电子邮箱 kangjw@mail2.gdut.edu.cn)

摘 要: 智能电网为了实现电网可靠、安全、高效地运行,需要广泛部署无线传感网络(WSN)监控电网状态,并及时对电网异常情况进行处理。在现有的智能电网中,WSN的感知数据需要上传到可信的中心节点进行存储与共享,但是这种中心化的存储方式容易引起中心节点遭受恶意攻击而发生单点失效、数据被故意篡改等信息安全问题。针对这些信息安全问题,利用新兴的联盟区块链技术在智能电网中选定若干数据采集基站,组成智能电网数据存储联盟链(DSCB)系统。DSCB中节点间数据共享通过智能合约的方式来完成,数据拥有者设定数据共享的约束条件,使用计算机语言代替法律条款来规范数据访问者行为,从而实现以去中心化的方式集体维护一个安全可靠的数据存储数据库。安全分析表明所提数据存储联盟链系统能实现安全、有效的数据存储与共享。

关键词: 智能电网;联盟区块链;数据存储;安全与隐私保护

中图分类号: TP309.2 **文献标志码:** A

Secure data storage and sharing system based on consortium blockchain in smart grid

WU Zhenquan[1], LIANG Yuhui[2], KANG Jiawen[1*], YU Rong[1], HE Zhaoshui[1]

(1. *Faculty of Automation, Guangdong University of Technology, Guangzhou Guangdong* 510006, *China*;
2. *Zhuhai Power Supply Bureau, Guangdong Power Grid Company Limited, Zhuhai Guangdong* 519000, *China*)

Abstract: In order to realize the reliable, safe and efficient power grids, Wireless Sensor Networks (WSNs) are widely deployed in smart grids to monitor power grids and deal with emergencies of power grids in time. In the existing smart grids, sensing data of the WSNs are needed to be uploaded to a trusted central node for storage and sharing. However, this central way suffers from many security problems including single point failure and data tampering. To address these security problems, an emerging technology named consortium blockchain was exploited to form a Data Storage Consortium Blockchain (DSCB), which consists of pre-selected data collection base stations in the smart grid. In DSCB, data sharing was accomplished by smart contracts. The constraints about data sharing were set by data owners, and computer language was used to replace the legal terms to regulate data visitors, thus achieving a decentralized, safe and reliable data storage database. Security analysis shows that DSCB can achieve safe and effective data storage and sharing.

Key words: smart grid; consortium blockchain; data storage; security and privacy protection

0 引言

智能电网整合了信息与通信网络技术,利用先进的传感网络实时采集、监控电网运行,并根据电网工作数据动态调整电网的运行状态。智能电网需要实时、可靠地监控电网数据,及时发现和排除电网故障,从而避免大规模事故发生。为此,用于监控的无线传感网络(Wireless Sensor Network, WSN)由于其具有开销低、部署快、内嵌智能处理等优点被广泛部署于电网中,从而保证电网安全可靠地运行[1-3],最终实现一个完全自动化的电力传输网络,能够监视和控制每个用户和电网节点,保证从电厂到终端用户整个输配电过程中所有节点之间的信息双向流动和电能的按需配送。

在传统的智能电网中,无线传感节点实时监控电网设备运行,并通过邻近数据采集基站将采集的电网数据定期上传到一个可信中心节点进行存储与共享[4]。这种中心化的数据存储方式面临集中式恶意攻击、中心节点单点失效、数据中心的存储数据被恶意篡改等信息安全问题。针对这些安全挑战,迫切需要设计安全可靠的去中心化的数据存储系统来保证智能电网的正常运行。

最近,备受关注的区块链技术被引入到分布式的数据安全存储的研究中[4-6]。区块链是按照时间顺序将数据生成区块,并以顺序相连的方式组合成的一种链式数据结构,是利用密码学方式保证数据不可篡改和不可伪造的分布式账本。区块链技术利用加密链式区块结构来验证与存储数据,利用分布式节点共识算法来生成和更新数据。所谓共识算法是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。现有智能电网系统的感知数据存储方式大多是中心式存储。文献[5]构建了一个基于区块链技术的医疗数据安全存储模

收稿日期:2017-04-17;修回日期:2017-06-28。 基金项目:国家自然科学基金资助项目(61422201,61370159);广东省中国科学院全面战略合作专项(2013B091100014);广州市科技计划项目(201508010007)。

作者简介:吴振铨(1985—),男,广东饶平人,助理研究员,博士研究生,主要研究方向:车联网; 梁宇辉(1989—),男,广东珠海人,助理工程师,主要研究方向:电力系统; 康嘉文(1989—),男,广东茂名人,博士研究生,主要研究方向:物联网、信息安全; 余荣(1979—),男,广东饶平人,教授,博士,主要研究方向:物联网、移动云计算; 何昭水(1978—),男,湖南郴州人,教授,博士,主要研究方向:智能信息处理、机器学习。

型,通过分布式存储及传播机制,创建了一种大规模、安全的端对端信息交互方式; 文献[6]结合传统的区块链技术和数字签名保证电能安全交易与数据安全验证、存储。由于传统区块链技术的共识过程需要全网节点配合开展,导致网络耗能巨大,所以上述方案并不适用于智能电网传感数据的存储。

在智能电网中无线传感节点的能量有限,传统的区块链无法直接部署于无线传感网络,否则其带来的能耗开销将使无线传感网络无法正常工作。为此,本文利用联盟区块链技术来设计针对智能电网的安全数据存储系统,命名为智能电网数据存储联盟链(Data Storage Consortium Blockchain, DSCB)。联盟区块链是特殊的区块链,它建立在一定数目的预选认证节点上。区块链的共识算法由这些预选节点执行,而非全网所有节点,从而能大大减少网络开销。本文的预选节点可由无线传感网络中的数据采集基站充当[7]。本文的 DSCB 建立在部分数据采集基站,并由这些基站公开审计、安全存储数据,DSCB 系统不依赖于全网唯一可信的节点来执行数据存储。传感节点采集的数据经过加密后,发送到附近的数据采集基站,然后由这些基站运行共识算法,把通过审计检验的数据记录到一个公共的"账本"(数据库),从而实现智能电网去中心化的安全可靠的数据存储[8]。

这个公共的账本可通过智能合约的方式设置共享条件、时长和次数等参数,自动执行数据在感知节点间共享、授权 DSCB 系统的节点(传感节点和数据采集基站)进行安全访问。

1　数据存储联盟链的系统组成

在智能电网中,无线传感网络利用传感节点对电网里的配电、输电、发电等设备进行实时监测,采集监控数据,了解其运行状态,进而及时发现故障现象,对故障区做好迅速定位,提升电网质量。无线传感网的传感节点采集网络数据,并把数据整合发送到邻近的数据采集基站,本文定义这些数据采集基站为数据聚合器(data aggregator)。数据聚合器实时分析感知数据,响应电网运行。本文的数据聚合器通过有线网络连接通信[9],从而保证数据聚合器可协同合作分析数据。具体而言,本地数据聚合器分析本地采集的数据,通过有线网络按需获取其他数据采集基站的数据,综合分析电网运行情况,从而保证数据分析的实时性和正确性。

经过初步数据分析后,电网对全网的感知的历史数据通过数据存储联盟链进行安全存储,便于后续进一步深入分析统计。数据存储联盟链是建立在部分数据聚合器上的联盟区块链。在数据存储联盟链中,有一个重要的数据审计阶段——共识过程。传统区块链的共识过程在所有网络节点中执行,但是这样的方式给传感节点带来很大的能量开销。在本文的 DSCB 中,使用联盟链技术在预选的数据聚合器(数据采集基站)上执行共识过程。这些数据聚合器有权控制共识过程并争取获得数据写入资格,从而获得奖励。本文根据经验设定,当全网节点数目 <500 时,预选的数据聚合器数目为全网节点数的 20%; 当全网节点数目 $\geqslant 500$ 时,预选节点数目为 101[10]。

如图 1 所示,数据存储联盟链主要包括以下实体[11]:

1) 感知数据。智能电网的感知数据最终将存储在 DSCB 中,这些感知数据包含传感节点的假名、数据类型、元数据标签、元数据索引库、上传感知数据事件的时间戳等。这些信息通过数据加密和数字签名技术保证可验证和准确性。

2) 数据区块。在 DSCB 中,所有的感知数据都将被数据聚合器审计,并再存储在数据聚合器中,进而在网络节点中进行共享。由于传感节点的计算能力和存储空间有限,本文的传感节点无需直接存储感知数据,而是存储感知数据的索引列表,这个索引列表表明元数据的具体存储位置。数据聚合器收集并管理本地的感知数据。这些感知数据被所有的预选数据聚合器审计通过(即完成共识过程)后,就会被压缩整理成数据区块。每个新产生的区块含有链接到上一个数据区块的加密哈希值,这个哈希值能用于追踪和查验数据区块。

3) 工作量证明(Proof-of-Work, PoW)。工作量证明简单理解就是一份证明,用来确认你做过一定量的工作。类似于比特币,新的数据块在加入区块链前,DSCB 某个时间段内数据的"记账权"需要在预选的数据聚合器之间进行竞争获取。数据聚合器的工作量证明与比特币的工作量证明类似。数据聚合器通过 Merkle 哈希过程计算数据区块的 Merkle Root,然后将求解的随机数 Nonce 代入,计算 Merkle Root 的 SHA256 双哈希值,若该值小于目标哈希值 Bits,则审计通过。每个数据聚合器竞争寻找有效的工作量证明(即,随机数 Nonce),最快找到有效工作量证明的数据聚合器将获得一定量的奖励,负责审计交易记录并把它们组建成数据存储联盟链上新的数据区块。

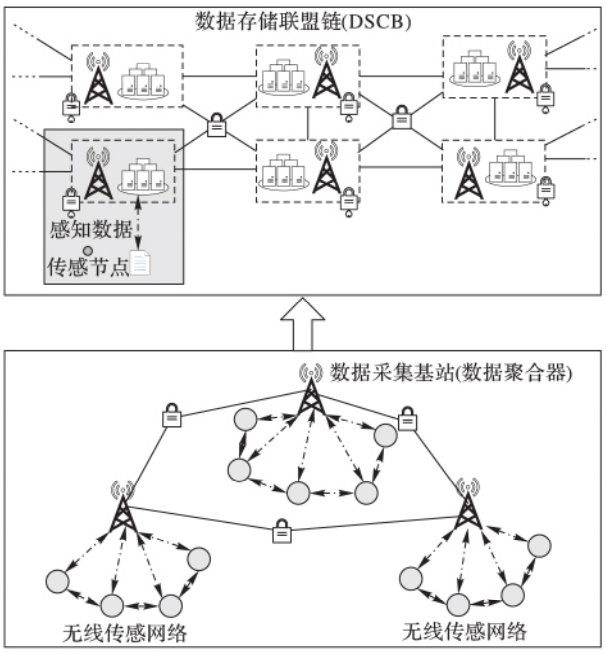

图 1　数据存储联盟链系统框架

Fig. 1　Framework of data storage consortium blockchain

2　数据存储联盟链的系统运行

如图 2 所示,数据存储联盟链中的数据聚合器包含区块数据记录池和本地控制器。区块数据记录池存储联盟链数据。本地控制器整合传感节点上传的感知数据,并负责执行智能合约控制数据的共享访问。这里的智能合约是一套以数字形式定义的承诺,包括合约参与方可以在上面执行这些承诺的协议。从本质上讲,合约协议的工作原理类似于其他计算机程序的 if-then 语句。智能合约只是以这种方式与真实

世界的资产进行交互。当一个预先编好的条件被触发时，智能合约执行相应的合同条款[12]。在本文中，智能合约是一个运行在安全环境下(去中心化的计算机网络)的计算机程序，与共识机制、点对点网络、Merkle 树以及数据库技术构成了区块链这样一种成本低、高度可靠的基础设施。在满足合约执行的促发条件下，智能合约智能化自动执行数据访问和共享请求，依据定义好的约束条件执行数据输出、数据共享等操作。本文所使用符号见表 1。

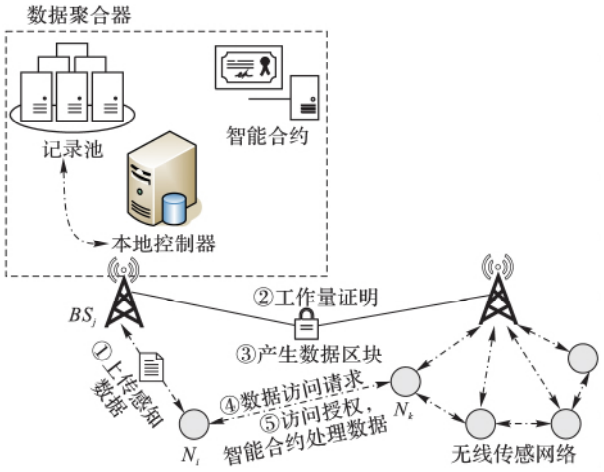

图 2 数据存储联盟链系统运行

Fig. 2 Operations on data storage consortium blockchain

表 1 主要符号及其含义

Tab. 1 Main symbols in this paper

符号	含义
N_i	第 i 个无线传感节点
BS_j	第 j 个数据聚合器(数据采集基站)
PK_i，SK_i，$Cert_i$	实体 i 的公钥，私钥和证书
$\{x\}$	元素 x 的集合
$Timestamp$	时间戳
$i \rightarrow j$	实体 i 发送信息给实体 j
$x \parallel y$	元素 x 连接元素 y
$E_{PK_i}(m)$	使用实体 i 的公钥加密信息 m
$Sign_{SK_i}(m)$	使用实体 i 的私钥对信息 m 进行数字签名
$Hash(m)$	信息 m 的哈希值

数据存储联盟链的运行主要包括感知数据存储和节点间数据共享两方面。

2.1 感知数据存储

1) 系统初始化和密钥生成：本文采用 Boneh-Boyen 短签名技术来执行系统初始化[13]。无线传感节点首先通过系统管理者的身份认证后，成为无线传感网络的合法节点，并获取用于加密数据的假名集合及其证书，表示为 $\{PK_{PID_i^k}, SK_{PID_i^k}, Cert_{PID_i^k}\}_{k=1}^{v}$。当进行系统初始化时，节点从邻近的数据聚合器的记录池中下载当前数据存储联盟链的元数据索引库(即区块数据存储位置索引表)。

2) 上传感知数据：感知节点(例如节点 N_i)先发送上传请求给本地数据聚合器，其中上传请求中包含节点的当前使用的假名证书 $Cert_{PID_i^k}$ 和数字签名 Sig_1，从而保证数据来源可靠性和真实性。本地数据聚合器接收到请求后，验证节点的请求和身份信息，确认其合法性后回应节点的上传请求。感知节点使用当前假名的公钥 $PK_{PID_i^k}$ 加密感知数据 $Data$，并附上加密数据的数字签名，然后使用本地数据聚合器(例如 BS_j)的公钥 PK_{BS_j} 对上传记录进行加密得到最终上传数据 $Record$，上述过程具体表示如下：

$$N_i \rightarrow BS_j: Record = E_{PK_{BS_j}}(Data\_1 \parallel Cert_{PID_i^k} \parallel Sig\_1 \parallel timestamp)$$

其中：

$$Data\_1 = E_{PK_{PID_i^k}}(Data \parallel timestamp)$$

$$Sig\_1 = Sign_{SK_{PID_i^k}}(Data\_1)$$

3) 本地数据聚合器收集上传数据：本地数据聚合器 BS_j 对上传 $Record$ 进行验证，如果数据安全有效，即可存储到本地记录池；如果不是安全有效的数据，则直接忽略。

4) 本地数据聚合器工作量证明：经过一段时间(例如 10 min)后，本地数据聚合器 BS_j 把这段时间内所有收集的有效数据整合成数据集合(表示为 $Data\_set = \{Records \parallel timestamp\}$)，并对数据进行数据签名，保证数据集合的来源合法性和可验证性。数据聚合器竞相寻找有效的工作量证明以争取记录本次数据区块、获得奖励的计划。这里的工作量证明是指数据聚合器依据随机数 x 和上一个区块的哈希值、时间戳、merkel 根值等数值(表示为 P_data)来计算当前区块的哈希值，也即是计算满足 $Hash(x + P\_data) < Difficulty$ 的随机数 x。这里 $Difficulty$ 是系统用于调整数据集合器计算正确 x 值的速度的值。最先计算出特定随机数 x 的数据聚合器(假设是 BS_j)将广播当前数据集合和计算出来的 x 值(即 PoW)给其他数据聚合器，以便审计和校验。如果其他数据聚合器也认可这个最快计算出 x 值的工作量证明，该数据聚合器获得将数据集合整合成新的数据区块，并存储在数据存储联盟链的权利，同时获得相应的系统奖励。后续的工作量证明将在这个新的区块数据上进行后续的计算。此步骤通过 PoW 的方式确定某个时间段内的数据记账管理权限。

5) 数据聚合器间的区块共识过程：最快计算出有效工作量证明的数据聚合器将成为当前共识过程的主节点(不妨设为 BS_j，标记为 Leader)，其余数据聚合器将成为从节点，本文采用拜占庭容错(Practical Byzantine Fault Tolerance，PBFT)共识机制进行区块共识[14]。具体共识过程如下：

步骤 1 如图 3 所示，主节点收集各从节点的数据集合整合成一个新的数据区块，附上主节点的数字签名和新数据区块的哈希值以备审查验证。主节点向各个从节点广播新生成的数据区块以待查验。上述过程具体表述如下：

$$BS_j \rightarrow All: Record = (Data\_sets \parallel Data\_hash \parallel Cert_{BS_j} \parallel Sig_{BS_j} \parallel timestamp)$$

其中：

$$Data\_hash = Hash(Data\_sets \parallel timestamp)$$

$$Sig_{BS_j} = Sign_{SK_{BS_j}}(Data\_sets \parallel Data\_hash)$$

步骤 2 从节点接收到数据区块后，通过主节点发送过来的区块哈希值和数字签名等信息验证数据区块的合法性和正确性，并把它们的审计结果(Result)附上各自的数字签名广播给其他从节点，以实现从节点间的相互监督和共同查验。

步骤 3 从节点(例如 BS_l)接收并汇总其他从节点的审计结果后，与自身的审计结果进行对比，并向主节点发送一个回复(Reply)，这个回复包含从节点自身的审计结果

(my_result) 、收到的所有审计结果($Rece\_results$) 、审计对比的结论($Comparison$) ,以及对应的数字签名。上述过程具体表述如下:

$$BS_l \rightarrow BS_j: Reply = E_{PK_{BS_j}}(Data\_3 \parallel Cert_{BS_l} \parallel Sig_{BS_l} \parallel timestamp)$$

其中:

$$Data\_3 = (my\_result \parallel Rece\_results \parallel Comparison)$$

$$Sig_{BS_l} = Sign_{SK_{BS_l}}(Data\_3)$$

步骤 4　主节点汇总所有来源于从节点的审计回复。如果全部数据集合器都赞同当前数据区块的合法性和正确性,主节点将把该数据区块连同参与审计的从节点的证书集合($\{Cert_{BS}\}$) ,以及对应的数字签名整合后发送给所有从节点。此后,该数据区块将以时间先后的顺序存储在数据存储联盟链中,主节点也从中获得系统的奖励。上述过程具体表述如下:

$$BS_j \rightarrow All: Data\_block = (Data\_4 \parallel Sig_{BS_j} \parallel timestamp)$$

其中:

$$Data\_4 = (Data\_sets \parallel Data\_hash \parallel \{Cert_{BS}\} \parallel timestamp)$$

$$Sig_{BS_j} = Sign_{SK_{BS_j}}(Data\_4)$$

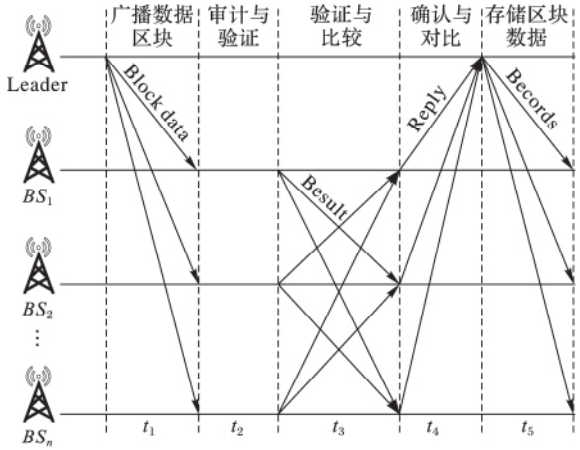

图 3　数据存储联盟链的共识过程

Fig. 3　Consensus process on consortium blockchain

步骤 5　假若有部分数据聚合器不赞同当前的审计结果,主节点将分析和查验这些数据聚合器的审计结果。必要时,主节点重新发送该数据区块给这部分数据聚合器进行第二次审计,如果仍有数据集合器不赞同,将采取少数服从多数的原则,超过一定比例的数据集合器赞同该数据区块,则将该数据区块按步骤 4 所提方式加载到数据存储联盟链中。同时,主节点将进一步分析个别不赞同的数据聚合器的审计结果,判断这些数据聚合器是否有恶意行为,及时对恶意数据聚合器进行处理。此步骤有利于及时发现并剔除非法恶意数据聚合器,从而保证系统的安全稳定运行。

2.2　节点间数据共享

感知节点存储在数据存储联盟链上的数据已被数据真正持有者 —— 感知节点使用不同的假名私钥进行加密,感知节点有权控制并有选择性地公开部分数据,促进智能电网的正常运行。本文的节点间数据共享通过执行智能合约的脚本文件来完成[14]。数据拥有者设定数据共享的范围、时限等约束条件,使用计算机语言代替法律条款来规范数据访问者行为。这些约束条件通过计算机脚本语言在加入联盟链的节点上自动执行,保证数据共享的合法性和公平性。

智能合约的脚本主要包括锁定脚本和解锁脚本[7,14-15]。锁定脚本规定共享数据输出的阻碍条件,解锁脚本定义了数据输出的执行条件。如图 2 所示,一个使用智能合约实施数据共享的场景主要包括以下流程: 当节点 N_m 向节点 N_i 请求共享感知数据时,节点 N_i 首先查验节点 N_m 身份,与 N_m 达成共识后,节点 N_i 制定访问约束条件(例如数据共享范围、时效、次数等) ,然后智能合约根据节点 N_i 提供的私钥将数据解密,并依据约束条件输出对应结果,在输出数据给节点 N_m 之前,使用 N_m 提供的公钥对数据进行加密,N_m 再通过自身私钥进行解密。具体如下:

1) 共享访问请求。节点 N_m 向节点 N_i 发出感知数据共享请求 Req,请求中包含数据访问目的、时间和次数等信息。节点 N_i 查验节点 N_m 身份后,针对节点 N_m 制定访问约束条件 $Constrainsts$(例如数据共享范围、时效、次数等) ,授权访问,并把这些条件和被访问数据块对应的假名私钥 $SK_{PID_i^k}$ 发送给邻近数据集合器 BS_j:

$$N_i \rightarrow N_m: Req = E_{PK_{N_k}}(Request \parallel Cert_{N_m} \parallel timestamp)$$

$$N_m \rightarrow BS_j: Message = E_{PK_{BS_j}}(Constraints \parallel SK_{PID_i^k} \parallel PK_{N_m} \parallel timestamp \parallel Cert_{N_i})$$

2) 智能合约执行。数据集合器 BS_j 验证信息后,开始执行智能合约,根据节点设定的访问约束条件,锁定脚本,并根据提供的对称密钥,解密所共享的数据,使用访问节点的公钥 PK_{N_m} 对共享数据进行非对称加密,输出结果。

3) 共享数据发送。假若数据访问节点 N_m 和被访问节点 N_i 在同一个数据聚合器的覆盖范围内,则数据聚合器直接把数据发送给数据访问节点 N_m; 否则,由当前执行智能合约的节点把加密结果发送到访问节点 N_m 的邻近数据聚合器。上述过程具体表述如下:

$$BS_j \rightarrow BS_{j+1}: Shared\_data = E_{PK_{BS_{j+1}}}(Data\_2 \parallel timestamp \parallel Cert_{BS_j})$$

其中:

$$Data\_2 = E_{PK_{N_m}}(Data \parallel Cert_{N_i} \parallel Cert_{BS_j} \parallel timestamp)$$

4) 访问指定数据。数据访问节点 N_m 收到数据后,通过自身私钥解密数据,并进行数据读取访问。

3　安全性能分析

3.1　基本安全要求

本文所提数据存储联盟链利用标准的对称加密和非对称加密技术,对传统的安全攻击具有良好的抵御能力。例如,通过加密和验证机制,攻击者无法通过短时间的暴力破解打开加密信息; 通过在信息中加入时间戳,攻击者发动的重放攻击也被较好地抵御了; 在通信的过程中,通信节点使用数字签名技术抵御攻击者伪装成合法实体或者伪造虚假信息的攻击; 任何实体在没有签名者的私钥的情况下,无法伪造其他实体的数字签名; 合法实体能通过数字签名技术验证接收信息的发送者以及查验信息是否被更改过。

3.2　区块链相关安全

与一般的信息安全保护不同,本文所提的数据存储联盟链具有以下特点:

1) 无需全局可信的第三方实体。与传统的数据中心化存储不同，本文所提数据存储联盟链采用分布式数据存储方法来保证数据的安全存储，不依赖于全局可信的第三方实体，节点间采用端到端的通信方式，分布式存储数据，从而避免了传统中心化数据存储方法的中心节点容易遭受集中式恶意攻击的风险。这种非中心化的存储系统具有良好的可扩展性和可靠性。

2) 节点身份隐私保护。本文所提数据存储联盟链系统中的节点采用假名保护的方式来进行通信，通信双方无法获知通信节点的真实身份；同时，数据存储过程使用不同的非对称密钥对不同时间采集的数据进行加密，最大可能保证数据安全存储；此外，本文数据存储联盟链采用智能合约的方式执行数据共享，限制预选的数据聚合器随意访问数据的权限，并约束了数据聚合器的访问条件，使得数据的真正拥有者——感知节点能掌握并控制数据的访问权限和开发程度。

3) 数据存储安全验证。利用工作量证明机制，所有的加密感知数据由预选的数据聚合器执行公开审计和验证工作，从而保证数据的合法性和真实有效性。

4) 存储数据防故意篡改。对于普通感知节点而言，即使某一个感知节点串通攻击者来伪造数据存储联盟链部分数据，通过工作量证明和共识机制，这些被攻击的数据也会被其他数据聚合器在审计和查验数据时发现问题。只有攻击者控制超过全网节点50%以上的计算能力才能篡改数据。对于预选的数据聚合器节点而言，预选的数据聚合器节点间采用PBFT共识机制，不妨设全网存在f个恶意预选数据聚合器节点，只需预选数据聚合器数目n满足$n > 3f + 1$，便可抵御f个预选的数据聚合器节点发起的恶意篡改数据攻击，保证数据的合法性与真实性[16-17]。

对于预选数据聚合器发起的恶意篡改数据攻击，举例分析如下：设全网存在100个预选数据聚合器，且预选数据聚合器成为恶意数据聚合器的概率为1/2。根据上述分析内容可知，需要同时存在33个恶意数据聚合器才能成功发起数据篡改攻击。因此在此条件下，恶意数据聚合器篡改数据的成功率仅为$1/2^{33}$。

5) 数据不可伪造。联盟区块链分布式的本质特性联合数字签名技术保证攻击者无法假扮成某个合法实体来干扰无线网络数据存储。存储在联盟链上的元数据是通过节点的密钥加密后才上传到数据聚合器，除非攻击者窃取到感知节点全部的非对称加密密钥，否则无法获取完整的感知数据，进而去伪造这些数据。

3.3 数据存储联盟链能耗分析

在PBFT共识算法中(如图3所示)，系统主要的能耗是包括主从节点间的广播数据区块操作与节点收到数据后的校验操作。不妨设联盟链每10 min执行一次共识算法，n个预选节点间需要进行$n^2 + n - 2$次广播操作以及$n^2 + 2n - 2$次验证操作。其中每个数据区块大小为1 MB，每个节点执行广播操作需要0.9 J能量，验证操作需要0.03 J[17]。100个预选节点每小时执行PBFT共识机制能耗是54 kJ。与电网能量相比，PBFT共识机制能耗数量级不大。即使全网节点数目增加，本系统预选数据聚合器节点数目取值不变，PBFT共识机制的能耗相对固定[18]。

4 结语

随着智能电网无线传感网络的快速发展，中心化的数据存储方式难以应对日益增多的感知数据，数据存放方式开始由集中式转向分布式。区块链技术响应了去中心化的分布式存储，联盟区块链以较小的成本开销实现了数据的分布式安全存储，对智能电网的发展产生深远影响。本文提出的基于联盟区块链的智能电网数据安全存储系统，使得感知数据以非中心化的方式安全存储，解决数据集中式存储的潜在安全风险，在数据存储联盟链中，感知节点通过智能合约设置共享条件、时长和次数等参数，自动执行数据在感知节点间共享，实现数据安全有效的共享访问。安全性能分析表明本文方案安全有效。在未来工作中，为了进一步增强安全性能分析方面的科学性，将考虑采用形式化的方法对所提方案进行更为详细的量化说明与逻辑验证。

参考文献(References)

[1] JARADAT M, JARRAH M, BOUSSELHAM A, et al. The Internet of energy: smart sensor networks and big data management for smart grid [J]. Procedia Computer Science, 2015, 56: 592-597.

[2] FADEL E, GUNGOR V C, NASSEF L, et al. A survey on wireless sensor networks for smart grid [J]. Computer Communications, 2015, 71(C): 22-33.

[3] 张强，孙雨耕，杨挺，等. 无线传感器网络在智能电网中的应用[J]. 中国电力，2010，43(6)：31-36.(ZHANG Q, SUN Y G, YANG T, et al. Applications of wireless sensor networks in smart grid [J]. Electric Power, 2010, 43(6): 31-36.)

[4] 袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报，2016，42(4)：481-494.(YUAN Y, WANG F Y, Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42(4): 481-494.)

[5] 张亚娇，王枞. 区块链技术在医疗数据安全存储中的应用[EB/OL]. 北京：中国科技论文在线[2016-12-27]. http://www.paper.edu.cn/releasepaper/content/201612-553.(ZHANG Y J, WANG C. Application of blockchain in medical data secure storage [EB/OL]. Chinese Science Paper Online [2016-12-27]. http://www.paper.edu.cn/releasepaper/content/201612-553.)

[6] AITZHAN N Z, SVETINOVIC D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams [J]. IEEE Transactions on Dependable and Secure Computing, 2016, PP(99).

[7] 沈鑫，裴庆祺，刘雪峰. 区块链技术综述[J]. 网络与信息安全学报，2016，2(11)：11-20.(SHEN X, FEI Q Q, LIU X F. Survey of block chain [J]. Chinese Journal of Network and Information Security, 2016, 2(11): 11-20.)

[8] 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.(ZHANG N, WANG Y, KANG C Q, et al. Blockchain technique in the energy Internet: preliminary research framework and typical applications [J]. Proceedings of the CSEE, 2016, 36(15): 4011-4022.)

[9] 董慧，张成岩，严斌峰. 区块链技术应用研究与展望[J]. 互联网天地，2016，13(11)：14-19.(DONG H, ZHANG C Y, YAN B F. Research and prospect of block chain technology [J]. China Internet, 2016, 13(11): 14-19.)

[10] 董俐君，张芊，刘宣. 基于SGWM的230 MHz无线宽带通信

技术的用电信息采集系统的通信系统研究[C]// 2014 电力行业信息化年会论文集. 北京: 中国电机工程学会电力信息化专业委员会, 2014. (DONG L J, ZHANG Q, LIU X. Energy information collection system research on SGWM-based 230 MHz wireless bandwidth communication technology [C]// Proceedings of the 2014 Annual Conference Proceedings on Power Industry Information Society. Beijing: China Electrical Engineering Society of Electric Power Information Committee, 2014.)

[11] Lekko 乐扣老师. 区块链共识算法(POW、POS、DPOS、PBFT)介绍和心得[EB/OL]. [2017-01-10]. http://blog.csdn.net/lsttoy/article/details/61624287. (Lekko. Introduction on blockchain consensus algorithm (POW, POS, DPOS, PBFT) [EB/OL]. [2017-01-10]. http://blog.csdn.net/lsttoy/article/details/61624287.)

[12] 黄洁华. 众筹区块链上的智能合约设计[J]. 信息安全研究, 2017, 3(3): 211-219. (HUANG J H. The design of smart contracts on crowd funding private blockchain [J]. Journal of Information Security Research, 2017, 3(3): 211-219.)

[13] BONEH D, BOYEN X. Efficient selective identity-based encryption without random oracles [J]. Journal of Cryptology, 2011, 24(4): 659-693.

[14] 胡凯, 白晓敏, 高灵超, 等. 智能合约的形式化验证方法[J]. 信息安全研究, 2016, 2(12): 1080-1089. (HU K, BAI X M, GAO L C, et al. Formal verification method of smart contract [J]. Journal of Information Security Research, 2016, 2(12): 1080-1089.)

[15] ZYSKIND G, NATHAN O, PENTLAND A. Decentralizing privacy: using blockchain to protect personal data [C]// SPW 2015: Proceedings of the 2015 IEEE Security and Privacy Workshops. Washington, DC: IEEE Computer Society, 2015: 180-184.

[16] CRAIN T, GRAMOLI V, LARREA M, et al. (Leader/randomization/signature) — free byzantine consensus for consortium blockchains [EB/OL]. [2017-01-10]. https://arxiv.org/pdf/1702.03068.pdf.

[17] KANG J, YU R, MAHARJAN S, et al. Toward secure energy harvesting cooperative networks [J]. IEEE Communications Magazine, 2015, 53(8): 114-121.

[18] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains [C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 17-30.

This work is partially supported by the National Natural Science Foundation of China (61422202, 61370159), the Comprehensive Strategic Cooperation Project of Chinese Academy of Sciences and Guangdong Province (2013B091100014), the Guangzhou Technology Program (201508010007).

WU Zhenquan, born in 1985, Ph. D. candidate, research assistant. His research interests include Internet of vehicles.

LIANG Yuhui, born in 1989, junior engineer. His research interests include power system.

KANG Jiawen, born in 1989, Ph. D. candidate. His research interests include Internet of things, information security.

YU Rong, born in 1979, Ph. D., professor. His research interests include Internet of things, mobile cloud computing.

HE Zhaoshui, born in 1978, Ph. D., professor. His research interests include intelligent information processing, machine learning.

(上接第 2741 页)

[9] ZHENG Q, XU C, WU M. A novel MIMO channel model for high speed railway system [C]// Proceedings of the IEEE 14th International Conference on Communication Technology. Piscataway, NJ: IEEE, 2012: 31-35.

[10] GHAZAL A, WANG C, HAAS H, et al. A non-stationary MIMO channel model for high speed train communication systems [C]// Proceedings of the IEEE 75th Vehicular Technology Conference. Piscataway, NJ: IEEE, 2012: 1-5.

[11] GHAZAL A, WANG C, HAAS H, et al. A non-stationary geometry-based stochastic model for MIMO high-speed train channels [C]// Proceedings of the IEEE 12th International Conference on ITS Telecommunications. Piscataway, NJ: IEEE, 2012: 7-11.

[12] GHAZAL A, WANG C, AI B, et al. A nonstationary wideband MIMO channel model for high-mobility intelligent transportation systems [J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(2): 885-897.

[13] CHEN B, ZHONG Z. Geometry-based stochastic modeling for MIMO channel in high-speed mobile scenario [J]. International Journal of Antennas & Propagation, 2012, 2012: Article ID 184682.

[14] LIN S, ZHONG Z, CAI L, et al. Finite state Markov modelling for high speed railway wireless communication channel [C]// Proceedings of the 2012 IEEE Global Communications Conference. Piscataway, NJ: IEEE, 2012: 5421-5426.

[15] XUAN L, CHAO S, AI B, et al. Finite-state Markov modeling of fading channels: a field measurement in high-speed railways [C]// Proceedings of the 2013 IEEE/CIC International Conference on Communications in China. Piscataway, NJ: IEEE, 2013: 577-582.

[16] AI B, HE R, ZHONG Z, et al. Radio wave propagation scene partitioning for high-speed rails [J]. International Journal of Antennas & Propagation, 2012(2012), Article ID 815232.

[17] 邱佳慧, 陶成, 刘留, 等. U 型槽无线信道多径传播特性测量与建模方法的研究[J]. 铁道学报, 2014, 36(1): 40-48. (QIU J H, TAO C, LIU L, et al. Research on measurement and modeling of wireless channel multipath propagation properties for U-shape cutting [J]. Journal of the China Railway Society, 2014, 36(1): 40-48.)

This work is partially supported by the National Natural Science Foundation of China (61501066, 61571069), the Chongqing Frontier and Applied Basic Research Project (cstc2015jcyjA40003), the Fundamental Research Funds for the Central Universities (106112017CDJXY500001, 106112017CDJQJ168817), the Open Fund of the State Key Laboratory of Integrated Services Networks (ISN16-03).

LIAO Yong, born in 1982, Ph. D., associate professor. His research interests include high-speed mobile communication, aerocraft tracking, telemetry & command and communication.

HU Yi, born in 1994, M. S. candidate. Her research interests include channel model and its modeling methods of high-speed mobile communication.