Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Research
Smart Grid and Energy Internet—Article

双区块链辅助的安全与匿名数据聚合研究

陈思光[a,b,*]，杨丽[a,b]，赵传信[c]，Vijayakumar Varadarajan[d]，王堃[e]

[a] Jiangsu Key Lab of Broadband Wireless Communication and Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[b] Jiangsu Engineering Research Center of Communication and Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[c] Anhui Provincial Key Laboratory of Network and Information Security, Anhui Normal University, Wuhu 241000, China
[d] School of Computer Science and Engineering, Vellore Institute of Technology, Chennai 600127, India
[e] Department of Electrical and Computer Engineering, University of California, Los Angeles, CA 90095, USA

ARTICLE INFO

Article history:
Received 20 August 2019
Revised 11 May 2020
Accepted 27 June 2020
Available online 11 August 2020

关键词
区块链
雾计算
同态加密
智能电网
匿名性

摘要

作为未来典型的能源系统，智能电网旨在提高传统电力系统的效率，同时提供更稳定可靠的服务。但是，这种高效、可靠的服务依赖于频繁收集和分析用户的用电数据，将引发各种安全和隐私威胁。为了应对这些挑战，本文在雾计算使能智能电网场景下提出了一种双区块链辅助的安全与匿名数据聚合（double-blockchain assisted secure and anonymous data aggregation, DA-SADA）方案。具体地，本文通过融合雾计算和区块链技术设计了一种三层架构的数据聚合框架，该框架为实现智能电网中安全高效的数据收集提供了有力支撑；其次，通过融合 Paillier 同态加密、批量聚合签名和匿名身份验证机制，提出了一种低计算开销、安全且匿名的数据聚合机制。特别地，该方案通过设计的双区块链和二级数据聚合框架，实现了细粒度的数据聚合，并为电力调度和动态定价提供了有效的支撑。最后，通过一系列的安全性和计算成本分析说明了该方案的优越性。

1. 引言

作为下一代电力网络，智能电网通过融合先进的信息处理技术和通信技术[1–2]，提供更加高效、智能的电力和信息交换，以提高能源利用率，满足现代需求。例如，用户家中的智能电表可以实时感知家用电器的用电信息，控制中心可以通过收集和分析这些数据了解用户的用电行为，从而提供动态定价和灵活的电力调度策略[3–5]。然而，由于智能电表数量的爆炸式增长，如今的智能电网面临着巨大的通信和计算负担[6–7]。除此之外，收集的智能电表功耗数据的暴露会增加隐私泄漏风险，这些用电数据可能会被用于推断用户的生活习惯，甚至可以获知其经济情况[8]。与此同时，篡改和伪造攻击也将对智能电网的稳定性产生巨大威胁[9–10]。例如，2015 年，来自网络攻击者的虚假数据注入攻击造成了震惊世界的乌克兰停电事故[11]。因此，为了应对智能电网中关于性能、隐私和安全性等诸多挑战，国内外研究者已经提出了许多方案，其中最典型的代表即安全高效的数据聚合机制，因其显著优势而引起了广泛关注。当前，智能电网中的隐私数据聚合方案可以大致分为以下三类。

* Corresponding author.
E-mail address: sgchen@njupt.edu.cn (S. Chen).

英文原文：Engineering 2022, 8(1): 159–169
引用本文：Siguang Chen, Li Yang, Chuanxin Zhao, Vijayakumar Varadarajan, Kun Wang. Double-Blockchain Assisted Secure and Anonymous Data Aggregation for Fog-Enabled Smart Grid. *Engineering*, https://doi.org/10.1016/j.eng.2020.06.018

第一类主要是基于传统网络体系结构的数据聚合方案。例如，在文献[12]中提出了一种高效的隐私保护数据聚合机制，将超递增序列、同态Paillier加密算法和批量验证算法相结合，实现了高效的多维数据聚合，同时保护了安全和隐私。此外，在文献[13]中，通过联合使用同态加密算法、陷门哈希函数和同态身份验证器构建了一个安全增强的数据聚合方案，然而，在保密性和完整性得到保障的情况下，工作的计算和通信成本将会增加。从动态定价和服务支持的角度出发，文献[14]构建了一种隐私友好的轻量级数据聚合机制，它在提供动态计费的前提下实现了强大的隐私保护，更适于计算资源有限的智能电网设备。在无需可信赖第三方支持的前提下，Liu等[15]提出了一种有效实用的隐私保护数据聚合方案，该方案将受信任的用户连接起来以形成一个虚拟的聚合区域，并将聚合的结果用于数据分析，从而保护了用户的个人隐私并提高系统的稳健性。而文献[16]则从细粒度聚合的角度出发，实现了一种隐私保护的多子集数据聚合方案，该方案可以聚合不同范围内的电力消耗数据，实现多子集聚合并提供细粒度的数据服务；同时，该方案的计算成本较低。尽管以上文献中提出的方案实现了有效且安全的数据聚合，但是由于所采用的是传统的网络体系结构，在减少数据处理延迟和通信开销方面仍然存在一定的进步空间。

幸运的是，雾计算作为一种十分具有前景的计算模式，为其提供了新的解决方法。基于雾计算的网络结构克服了传统网络架构的弱点，尤其是与云计算的结合使用，可以显著减少系统延迟和通信开销[17]。因此，第二类解决方案设计了具有边缘/雾计算体系结构的数据聚合机制。例如，文献[18]通过结合Paillier加密算法、单向哈希链和中国余数定理，构建了雾辅助隐私保护数据聚合方案。该方案具有将异构的物联网（Internet of Things, IoT）设备的数据聚合为一的特性，并能够过滤虚假数据。在文献[19]中使用了基于雾计算的选择性数据聚合方案，该方案可以分别聚合不同类型的数据，以供不同的应用程序使用，同时还考虑了可靠性和隐私保护等问题。为了进一步增强上述方法的隐私保护效果，文献[20]提出了一种基于雾计算的差分隐私保护数据聚合方案，该方案实现了统计数据的差分隐私，并能够确保来自聚合器数据的机密性。考虑到边缘计算系统的资源有限，Zhang等[21]提出了一种高效的隐私保护数据聚合方案，该方案通过将耗时的签名操作转移至离线阶段，从而有效地减轻了在线计算的负担。而文献[22]致力于研究基于雾计算的智能电网系统中的匿名认证，通过采用Paillier密码系统和盲签名构造了一种匿名的数据聚合方案，该方案以较低的计算和通信成本为系统提供了强大的隐私保护。尽管上述解决方案显著减少了系统延迟和通信开销，并在一定程度上提供了隐私和安全保护，但是这类方案仍然面临安全性和中心化的问题。例如，当用户的私人信息被发送至雾节点，并且恶意攻击者成功拦截了该信道并窃取了秘钥时，用户的隐私很难得到保证。而且所有用户的数据都集中在雾层或云层中，这将不可避免地带来中心化的问题。

而区块链技术[23]的出现为解决上述问题提供了新的视角，由于其去中心化和不可篡改的特性，当前有一些研究已将区块链应用于智能电网。例如，文献[24]研究了基于区块链的智能电网数据保护方案，并证明了区块链可以有效地提高系统抵御网络攻击的能力。因此，第三类解决方案主要涉及区块链技术和数据聚合的结合。具体地，文献[25]通过将联盟区块链集成到智能电网中，研究了一种用于智能功率调节的安全数据聚合机制，该机制提出了一种用于收集多维数据的多接收器模型，并基于智能合约建立了灵活的功率监控和管理机制来增强智能电网的安全性。文献[26]研究了智能电网中区块链辅助的匿名数据聚合方案，与其他解决方案相比，它可以增强系统安全性，改善系统性能。然而，用户的用电数据以明文形式成组传输，这将不可避免地面临一些安全隐患。尽管上述基于区块链的隐私保护数据聚合方案有效地增强了智能电网的安全性，并解决了集中化和单点故障的问题，但都没有考虑基于边缘计算的网络架构，无法对本地资源进行有效利用，系统效率存在很大的改进空间。相应地，文献[27-28]通过结合区块链和边缘计算来抵御网络攻击，可提高系统性能，但并未提供具体的可执行解决方案。

上述方案在不同程度上解决了智能电网中的一些问题，但仍然存在许多不足。与现有解决方案不同，本文通过融合区块链技术、Paillier密码系统、批量聚合验证和匿名身份验证机制，为雾计算场景下的智能电网提出了一种双区块链辅助的安全和匿名数据聚合（double-blockchain assisted secure and anonymous data aggregation, DA-SADA）方案。具体来说，该方案的主要贡献如下：

（1）通过融合雾计算和区块链技术，设计了一种基于三层体系结构的数据聚合框架，在增强安全性的同时，有效利用本地资源，为在智能电网中实现高效、安全的数据收集提供了有力支撑。

（2）提出了一种安全且匿名的数据聚合机制，该机制通过联合利用Paillier加密算法、批量聚合签名和匿名身份验证机制，可以有效降低计算开销；同时抵御各种安全威胁（如窃听、篡改和重放攻击），并提供多重隐私保护。

（3）实现了细粒度的隐私数据同态聚合，并通过设计

的双区块链机制和二级数据聚合框架为电力调度和动态定价提供了有效的支撑。此外，该设计进一步强化了系统的安全性和稳健性。

本文的其余部分组织如下：第2部分描述了相关的预备知识；第3部分详细介绍了构建的网络模型；第4部分介绍了本文提出的方案；第5部分进行了安全性和性能评估；第6部分总结全文。

2. 预备知识

2.1. 区块链

区块链可以被认为是一个点对点（peer-to-peer, P2P）的分布式数据库，它按时间顺序创建块和链接[29]，旨在为广泛的物联网和工业物联网（Industrial Internet of Things, IIoT）应用提供去中心化和分布式的解决方案。区块链的主要组成部分包括交易、区块、智能合约、共识机制、密码学和P2P网络[30]。具体地，在区块链网络中，参与者充当协同保护和维护交易共享记录的分布式节点，它不需要任何可信赖的第三方监督管理机构。所有节点负责共享、封装、验证和存储在区块链网络中生成的新交易。因此，在分布式场景下，它可以在互不信任的参与实体之间建立信任。它还具有去中心化、不可篡改性和安全性等特点。

去中心化：区块链的分布式结构保证了去中心化的特性。此外，区块链不需要第三方维护管理，网络中的节点基于激励机制完全自治。

不可篡改性：不可篡改性是指交易数据一旦记录在区块链中就无法被成功篡改或删除。

安全性：写入区块链的数据需要集体验证，这意味着想要成功篡改交易数据至少需要全网51%的算力，这在实际中通常是不可能的。

2.2. Paillier加密

Paillier同态加密算法被广泛应用于隐私保护领域。它可以直接对密文进行操作，从而有效保护数据隐私。具体来说，Paillier加密是一种加法同态加密，由密钥生成、加密操作和解密操作组成。

密钥生成：给定安全参数κ，随机选择两个大素数p和q，满足$|p|=|q|=\kappa$（这项操作用于计算p和q的长度，它们的长度都等于κ比特），且$\gcd[pq,(p-1)(q-1)]=1$，然后计算出$N=pq$、$\lambda=\mathrm{lcm}(p-1,q-1)$。选择一个生成元$g\in Z_{N^2}^*$，同时需要保证存在$\mu=[L(g^\lambda \bmod N^2 \bmod N)]^{-1}$。其中将函数$L$定义为$L(u)=(u-1)/N$。最终，得到Paillier加密算法的公钥$(N,g)$和私钥$(\lambda,\mu)$。

加密操作：对于任意的明文$m\in Z_N$，选择随机数$r=Z_N^*$，则加密后的密文为$C=g^m r^N \bmod N^2$。

解密操作：根据密文C，计算明文$m=L(C^\lambda \bmod N^2)/L(g^\lambda \bmod N^2)\bmod N$。

2.3. 布隆过滤器

布隆过滤器由一个长二元向量和一系列随机映射函数组成，具有计算复杂度低、空间利用率高、查询效率高等优点，能够快速回答“某个元素是否在一个集合内”的问题。

具体地，假设存在k个哈希函数$\{h_1,h_2,\ldots,h_k\}$和一组元素$\{x_1,x_2,\ldots,x_\omega\}$，通过这$k$个哈希函数将这一组元素映射到布隆过滤器中，并将对应位置设为1，具体操作如图1所示。

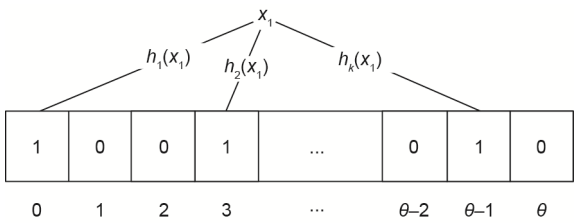

图1. 布隆过滤器的生成。

元素的添加：如图1所示，将元素组中的元素x_1经过k次哈希得到k个哈希值$\{h_1(x_1),h_2(x_1),\ldots,h_k(x_1)\}$，然后根据这些值找到对应位置，并将相应位置设为1。

元素的查询：为了查询x_1是否已经存在于布隆过滤器中，首先，按照相同的方式计算元素x_1的k个哈希值，并将其表示为$\{h_1(x_1),h_2(x_1),\ldots,h_k(x_1)\}$，随后找到相应位置并检查该位置是否已经全部设为1。如果其中有0存在，则说明该元素不曾被添加到布隆过滤器中；否则，可以证明x_1已被存储在布隆过滤器中。

误报率：布隆过滤器存在误报的情况，即意味着元素x_1不存在于布隆过滤器中，但相应位置$\mathrm{BF}[h_i(x)](1\le i\le k)$皆为1。假设元素在布隆过滤器中被设置为1的概率为$p=1-(1-1/\theta)^{kn}$，根据文献[31]的结果可以得到误判率的上限为$\varepsilon=p^k\left\{1+o\left[k/p\sqrt{\ln(\theta)k\ln(p)/\theta}\right]\right\}$，其中$\theta$表示布隆过滤器中元素的数量。

3. 网络模型和威胁

3.1. 网络模型

在本文构建的网络模型中，一个基于雾计算的数据聚

合智能电网主要由4个实体[智能电表、雾节点、云服务器和可信机构（trust authority, TA）]组成，如图2所示。具体来说，首先假设智能电网覆盖区域被划分为m个子区域，每个子区域部署n个智能电表以检测用户的功耗信息，所有$m \times n$个智能电表形成用户层。因此，每个子区域都部署一个雾节点以收集和聚合来自其自身子区域的数据，所有m个雾节点形成雾层，雾层位于网络边缘，处于用户层和服务支撑层之间。在服务支撑层，云服务器将处理从雾层上传的数据并生成实时决策。TA负责整个系统参数的生成。下面将对各层进行详细阐述。

用户层：用户层主要由大量的智能电表组成。例如，在子区域j的第i个智能电表SM_{ij}会收集用户的实时功耗信息，然后对这些功耗数据进行加密和签名，并将这些加密数据发送至位于用户层的聚合节点。聚合节点则对通过验证的密文进行聚合以生成一级聚合密文，然后将相关信息封装到一个区块中。同时，新生成的区块通过共识机制之后被添加到用户聚合区块链[(user aggregation, UA)-blockchain]中。在上述操作过程中，SM_{ij}（即用户）的身份始终以假名的形式存在。最后，将生成的UA-blockchain发送到雾节点fog_j等待进一步处理。

雾层：雾层位于用户层和服务支撑层之间的中间层，通过在雾层对加密数据进行二级聚合能够显著减少通信开销。具体来说，当fog_j从由用户层中的聚合节点发送的UA-blockchain中读取到一级聚合密文时，将对该聚合密文进行签名，并将其发送到雾层的聚合节点以进行二次聚合。随后聚合节点同样将相关信息封装到一个新区块中，然后通过共识机制将新生成的区块添加到雾聚合区块链[(fog aggregation, FA)-blockchain]中。最后，将生成的FA-blockchain发送到云服务器。

服务支撑层：在该层，云服务器可以实时记录、分析、存储和管理用户的用电信息，整个过程不需要人工干预，由智能合约自动执行，借此提高系统效率，同时增强隐私数据的安全性。具体地，当云服务器收到从雾层处的聚合节点发送的FA-blockchain时，首先读取链中的二级聚合密文，以进行解密操作，从而恢复二级聚合明文，然后利用霍纳规则得到细粒度的聚合明文。粗粒度和细粒度聚合的结合为有效的电力调度管理提供了各种数据支持。

TA：TA主要负责为系统中的实体生成和管理所有公共参数和密钥。同时，通过收集用户的假名为每个子区域的智能电表生成布隆过滤器，并将生成的布隆过滤器发送

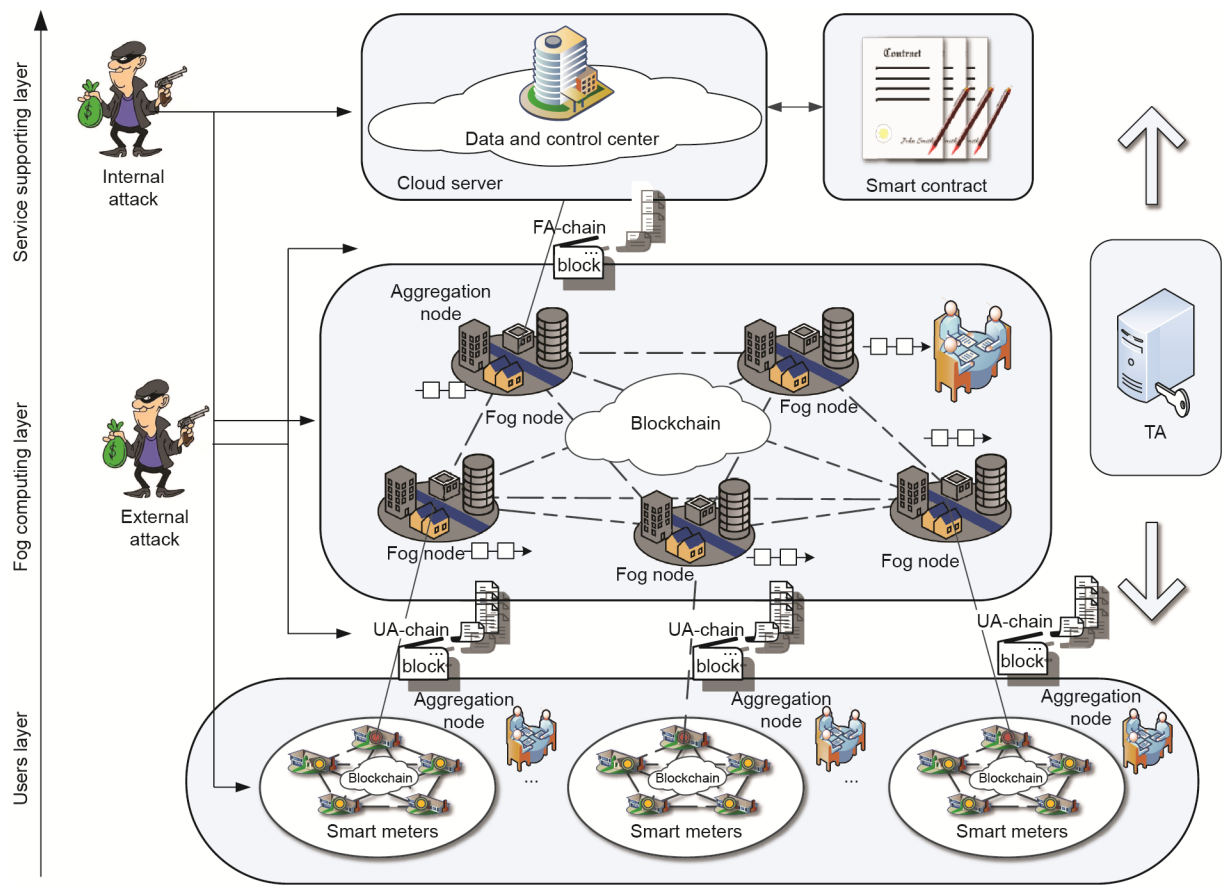

图2. 网络结构。

给相应的用户，在雾层也将进行类似的操作。

3.2. 威胁模型

在智能电网场景中，可能存在窃听者为了窥探用户的隐私而窃听智能电表与雾节点之间的通信链路。同时，主动攻击者可能会篡改传输信息，并发起重放攻击以威胁智能电网的安全。本文的威胁模型将网络中可能发生的威胁分为两种：内部攻击和外部攻击。

内部攻击：内部攻击也可分为两种。第一类由恶意节点攻击组成，恶意节点攻击主要发生在用户层和雾层中的区块链生成期间。例如，在区块链的生成过程中，恶意节点冒充网络中的合法节点，通过发起一些主动攻击（如篡改、伪造、重放等），以损害用户身份以及私人数据的真实性和完整性。因此，所提出的网络系统应具有在共识过程中识别节点身份合法性的能力。第二类内部攻击主要是源于雾节点和云节点的“好奇心”。例如，雾节点可能会受到未被检测到的恶意软件的影响，恶意软件会窃听设备中的数据，因此必须确保在整个过程中雾节点无法观察到用户的隐私数据。同样地，系统应保证云服务器也不能获知用户的隐私数据。

外部攻击：攻击者可以窃听和篡改通信链路中传输的数据；除此之外，攻击者也可以主动发起重放攻击。因此，系统必须确保攻击者无法通过攻击通信链路成功获取隐私信息并且能够免疫主动攻击。

4. 双区块链辅助的安全与匿名数据聚合方案

本节通过融合区块链技术、Paillier密码系统、批量聚合验证技术和匿名身份验证机制，为雾计算使能的智能电网提出一种双块链辅助的安全与匿名数据聚合方案，包括4个步骤：系统初始化、UA-blockchain的生成、FA-blockchain的生成及服务支撑。

4.1. 系统初始化

在构建的网络场景中，TA负责系统初始化。在此系统初始化过程中，TA需要执行三个步骤，即系统参数的生成、系统参数的分发和布隆过滤器的生成。

系统参数的生成：在系统参数的生成阶段，TA首先选择系统安全性参数κ，生成两个安全的大素数$|p|=|q|=\kappa$。随后计算$N=pq$作为公钥，计算$\lambda=\mathrm{lcm}(p-1,q-1)$作为相应私钥。同时系统将随机选择$r\in Z_N^*$，计算$s=r^N \bmod N^2$，令$g=N+1$，定义函数

$$L(u)=\frac{u-1}{N} \tag{1}$$

此外，为了保证身份的匿名性，智能电表SM_{ij}选择一个随机素数X_{ij}作为公钥，计算其密钥$Y_{ij}=X_{ij}^{-1} \bmod N^2$；该公钥$X_{ij}$同样用于计算智能电表的假名$\mathrm{Pseu}_{ij}=X_{ij} \bmod N^2$。同样地，雾节点$\mathrm{fog}_j$选择一个随机素数$X_j$作为其公钥，并计算其私钥$Y_j=X_j^{-1} \bmod N^2$，同样得到雾设备的假名$\mathrm{Pseu}_j=X_j \bmod N^2$。最后，TA选择安全密码散列函数$H:\{0,1\}^* \to Z_N^*$。

系统参数的分发：随着所有系统参数$(\lambda,N,s,H,X_{ij},X_j,Y_{ij},Y_j)$的生成，TA发布公共参数$(N,H)$，随后分配其余参数给相应实体。具体地，分别将密钥$(X_{ij},Y_{ij},s)$、$(X_j,Y_j)$和$\lambda$通过秘密信道分配给智能电表$\mathrm{SM}_{ij}$、雾节点$\mathrm{fog}_j$和云服务器。

布隆过滤器的生成：TA收集智能电表的假名，为每个子区域创建布隆过滤器。同样地，TA收集雾设备的假名，以便在雾层创建布隆过滤器。具体来说，在用户层中，TA设置一个θ位的数组，然后使用哈希函数来计算同一区域中所有假名的哈希值。当索引值等于$H(\mathrm{Pseu}_{ij}) \bmod \theta$时，将该位元素值设置为1。最后，TA将布隆过滤器发送到相应区域中的智能电表，类似的操作也将在雾层执行。

4.2. UA-blockchain的生成

考虑到对用电数据的分析所带来的隐私泄漏风险以及篡改威胁，感知设备（即智能电表）需要对用户的用电数据进行加密，并且需要对相关信息进行签名以确保隐私数据的完整性，这个过程被称为事务的生成。随后，聚合节点将聚合来自感知设备的加密数据并将相应信息记录到相关块中。最后，聚合节点通过共识机制生成UA-blockchain。具体生成过程如图3所示。

4.2.1. 事务的生成

功耗数据密文的生成：每个子区域j有n个智能电表，在一个特定的时隙t_s，可以得到该区域第i个智能电表SM_{ij}的功耗数据d_{ij}，从而可以计算出该智能电表的功耗数据密文C_{ij}。

$$\begin{aligned} C_{ij} &= g^{d_{ij}} \cdot r^N \bmod N^2 \\ &= (N+1)^{d_{ij}} \cdot r^N \bmod N^2 \\ &= (1+d_{ij}N) \cdot s \end{aligned} \tag{2}$$

式中，$1\le i\le n$，$1\le j\le m$。根据模数的性质$(1+N)^m \equiv (1+mN) \bmod N^2$，可以通过计算$g=N+1$，获得$c=(1+mN)r^N \bmod N^2$形式的扩展的Paillier加密算法，该形式的算法主要是通过避免加解密操作中繁琐的指数计算，以减少计算开销。

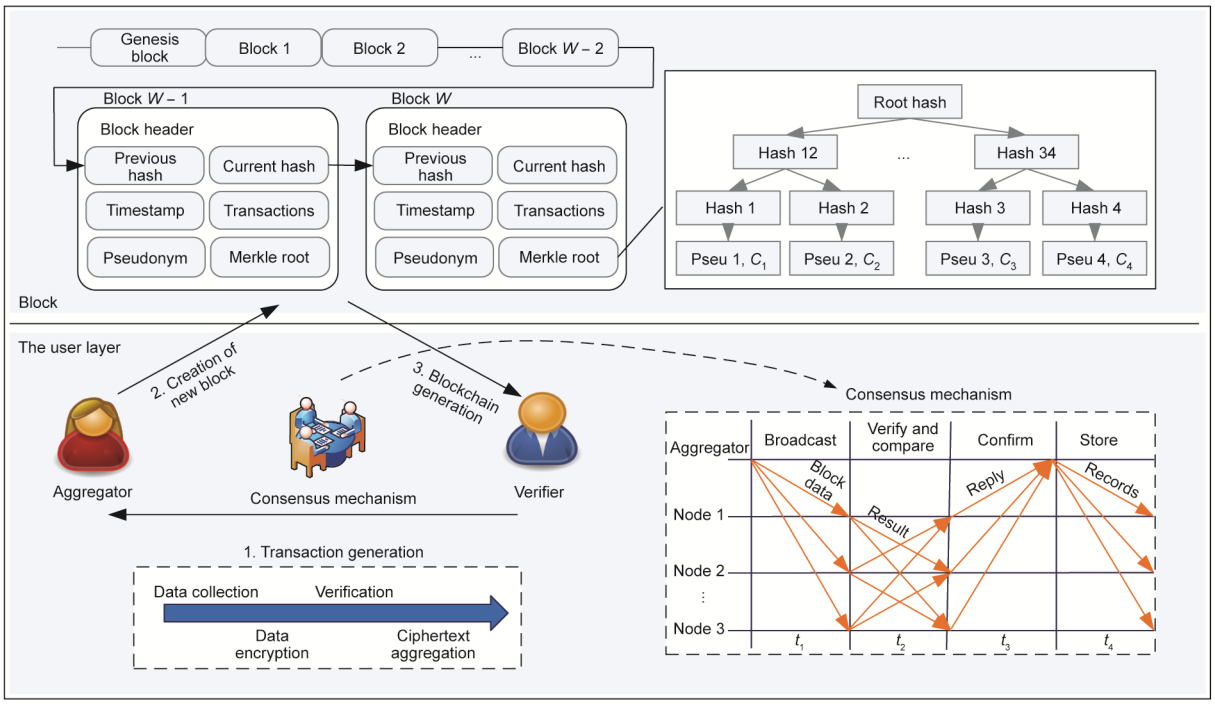

图3. UA-blockchain的生成。这个过程包括三个步骤——事务的生成、新区块的创建和区块链的生成。

签名的生成：可以得到签名σ_{ij}。

$$u_{ij}=H(C_{ij}\|t_s) \tag{3}$$

$$\sigma_{ij}=H(u_{ij}\|\mathrm{Pseu}_{ij})^{Y_{ij}} \tag{4}$$

随后，智能电表发送报告$(\sigma_{ij}\|C_{ij}\|t_s\|\mathrm{Pseu}_{ij})$至相应的用户层聚合节点，此处通过选择剩余计算资源最大的智能电表作为用户层的聚合节点。

签名验证和密文聚合：每个子区域内的聚合节点从该区域智能电表处收到报告后，聚合节点首先会通过布隆过滤器检查用户假名的有效性。然后检查时间戳以确认报告的有效性。最后，使用批量聚合验证算法来验证签名的真实性，具体表达式为：

$$\prod_{i=1}^{n}\sigma_{ij}^{X_{ij}}=\prod_{i=1}^{n}H\left[H\left(C_{ij}\|t_s\right)\|\mathrm{Pseu}_{ij}\right]\bmod N^2 \tag{5}$$

公式（5）是通过聚合操作和公私钥的具体值得出的，详细表达式为

$$\begin{aligned}\prod_{i=1}^{n}\sigma_{ij}^{X_{ij}}&=\prod_{i=1}^{n}H\left(u_{ij}\|\mathrm{Pseu}_{ij}\right)^{Y_{ij}X_{ij}}\bmod N^2\\&=\prod_{i=1}^{n}H\left[H\left(C_{ij}\|t_s\right)\|\mathrm{Pseu}_{ij}\right]^{Y_{ij}X_{ij}}\bmod N^2\\&=\prod_{i=1}^{n}H\left[H\left(C_{ij}\|t_s\right)\|\mathrm{Pseu}_{ij}\right]\bmod N^2\end{aligned} \tag{6}$$

智能电表的签名验证通过后，聚合节点将执行聚合操作，以获取子区域j的聚合密文C_j：

$$C_j=\prod_{i=1}^{n}C_{ij}\bmod N^2 \tag{7}$$

最终，聚合密文C_j与其他相关信息汇合生成事务$T_x=(C_j,\mathrm{Pseu}_{ij},t_s)$。

4.2.2. 新区块的创建

聚合节点将生成的事务$T_x=(C_j,\mathrm{Pseu}_{ij},t_s)$记录在一个新的区块中，并在子区域$j$中广播新区块以进行信息认证。除事务记录之外，该新区块还包含其他三个元素，即Merkle根、前一区块的哈希值和当前区块哈希值。具体地，Merkle根的值是通过对Merkle树中的功耗密文数据C_j和相关用户假名进行哈希处理得到的，具体过程如图3所示。当前区块的哈希值可按以下公式计算：

$$\begin{aligned}H_{\mathrm{curr-block}}=\mathrm{SHA256}\,(&\mathrm{index}+H_{\mathrm{prev-block}}+\mathrm{Pseu}_{ij}+\mathrm{timestamp}+\\&C_j+\sum_{ij}\mathrm{transactions}_{ij}\,)\end{aligned} \tag{8}$$

这种计算过程意味着一旦将新区块添加到链中，该区块中的内容很难被成功篡改，因为当前块哈希值的计算总涉及前一个块的哈希值。

4.2.3. 区块链的生成

聚合节点创建新区块之后，新的区块将在此子区域中进行广播。该子区域中的其他普通节点将验证该新区块中的记录，且每个节点仅验证与其自身有关的数据，以满足智能电网中对于实时调度的要求。如果与原始数据一致，则新区块通过验证，验证结果将广播到用户层的其他节点。在收集了其他$2n/3+1$个或更多节点发送的正确性确

认消息后，该新区块被视为有效区块，同时将其添加到UA-blockchain中。假设在形成区块链网络中，可以允许的恶意节点的数量少于或等于网络节点总数的1/3。由于本文定义一个新的区块只有在通过其他$2n/3+1$个节点或更多节点的验证后才能添加到区块链中，因此出于安全性考虑，设置了上述阈值。同时，这也说明攻击者只有捕获到网络中2/3以上的节点才能够成功篡改区块中的信息。具体的共识过程如图3所示。

4.3. FA-blockchain的生成

与用户层UA-blockchain的生成过程类似，雾层FA-blockchain的生成同样包括事务的生成、新区块的创建和区块链的生成。

4.3.1. 事务的生成

雾层事务的生成与用户层类似。首先，当雾节点j从接收的UA-blcokchain读取加密数据后，雾节点j将对这些数据进行签名以确保该信息的完整性。随后，选择雾层的聚合节点将对该区域内所有雾节点的功耗密文$C_j, j\in\{1,2,\ldots,m\}$执行聚合操作，以获得二级聚合密文。同样地，具有最大剩余计算资源的雾节点将会被选中作为聚合节点。

签名的生成：当雾节点fog_j读取到相应子区域内的聚合功耗密文C_j后，首先需要计算签名σ_j。

$$u_j=H(C_j\|t_s) \tag{9}$$

$$\sigma_j=H(u_j\|\mathrm{Pseu}_j)^{Y_j} \tag{10}$$

随后，该雾节点发送报告$(\sigma_j\|C_j\|t_s\|\mathrm{Pseu}_j)$至该层相关聚合节点。

签名验证和密文聚合：雾层聚合节点从该层其他雾节点处收到报告后，聚合节点首先会通过布隆过滤器检查雾节点假名的有效性；随后检查时间戳以确认报告的有效性；最后，使用批量验证算法来验证签名的真实性，具体表达式为

$$\prod_{j=1}^{m}\sigma_j^{X_j}=\prod_{j=1}^{m}H(u_j\|\mathrm{Pseu}_j)\bmod N^2 \tag{11}$$

公式（11）是通过聚合操作和公私钥的具体值得出的，详细表达式为

$$\begin{aligned}\prod_{j=1}^{m}\sigma_j^{X_j}&=\prod_{j=1}^{m}H(H(C_j\|t_s)\|\mathrm{Pseu}_j)^{Y_jX_j}\bmod N^2\\&=\prod_{j=1}^{m}H(u_j\|\mathrm{Pseu}_j)^{Y_jX_j}\bmod N^2\\&=\prod_{j=1}^{m}H(u_j\|\mathrm{Pseu}_j)\bmod N^2\end{aligned} \tag{12}$$

智能电表的签名验证通过后，聚合节点将执行聚合操作，以获取所有子区域的二级聚合密文C_{AS}。

$$C_{\mathrm{AS}}=\prod_{j=1}^{m}C_j\bmod N^2 \tag{13}$$

最终，聚合密文与其他相关信息汇合生成事务$T_x'=(C_{\mathrm{AS}},\mathrm{Pseu}_j,t_s)$。

4.3.2. 新区块的创建

雾层的聚合节点将交易$T_x'=(C_{\mathrm{AS}},\mathrm{Pseu}_j,t_s)$记录在一个新的区块中，并将该新区块广播至其他雾节点以进行信息认证。与在用户层中创建新区块类似，雾层新区块的创建主要包含事务、Merkle根、前一区块的哈希值和当前区块的哈希值。当前区块的哈希值按以下公式计算：

$$\begin{aligned}H'_{\mathrm{curr-block}}=\mathrm{SHA\ 256}\,(&\mathrm{index}+H_{\mathrm{prev-block}}+\mathrm{Pseu}_j+\mathrm{timestamp}+\\&C_{\mathrm{AS}}+\sum_j\mathrm{transactions}_j\,)\end{aligned} \tag{14}$$

4.3.3. 区块链的生成

聚合节点在雾层中创建新区块之后，将该新区块广播至其他雾节点，并通过共识机制添加到FA-blockchain中。雾层的共识机制类似于用户层的共识机制。首先，雾层中除聚合节点之外的普通节点将验证该新块中的记录，且每个节点仅验证与其自身相关的数据。如果与原始数据一致，则通过验证并将验证结果广播到雾层中的其他节点。收集到其他$2m/3+1$个或更多的雾节点发送的正确性得到确认的消息后，该区块被认为有效并将其添加至FA-blockchain中。

4.4. 服务支撑

当云服务器接收到来自雾层的FA-blockchain时，首先会读取二级聚合密文，并使用Paillier解密算法对该聚合密文进行解密。为了有效利用Paillier解密算法，接下来进一步分析公式（13），并得到以下公式：

$$\begin{aligned}C_{\mathrm{AS}}&=\prod_{j=1}^{m}C_j\bmod N^2=\prod_{j=1}^{m}\left(\prod_{i=1}^{n}C_{ij}\bmod N^2\right)\\&=\prod_{j=1}^{m}\left(\prod_{i=1}^{n}g^{d_{ij}}\cdot r_j^N\bmod N^2\right)\\&=\prod_{i=1}^{n}\left(\prod_{j=1}^{m}g^{d_{ij}}\cdot r_j^N\bmod N^2\right)\\&=\prod_{i=1}^{n}\left(g^{d_{i1}}\cdot g^{d_{i2}}\cdots g^{d_{im}}\bmod N^2\right)\left(\prod_{j=1}^{m}r_j\right)^N\bmod N^2\\&=g^{a_1\sum_{i=1}^{n}d_{i1}}\cdot g^{a_2\sum_{i=1}^{n}d_{i2}}\cdots g^{a_m\sum_{i=1}^{n}d_{im}}\left(\prod_{j=1}^{m}r_j\right)^N\bmod N^2\\&=g^{a_1\sum_{i=1}^{n}d_{i1}+a_2\sum_{i=1}^{n}d_{i2}+\cdots+a_m\sum_{i=1}^{n}d_{im}}\left(\prod_{j=1}^{m}r_j\right)^N\bmod N^2\end{aligned} \tag{15}$$

同时，分别将符号M和R定义为

$$M=a_1\sum_{i=1}^{n}d_{i1}+a_2\sum_{i=1}^{n}d_{i2}+\cdots+a_m\sum_{i=1}^{n}d_{im} \tag{16}$$

$$R=\prod_{j=1}^{m}r_j \tag{17}$$

因此，云服务器可以将密文C_{AS}写为公式（18）的形式，该形式与Paillier加密算法的密文形式一致。

$$C=g^M\cdot R^N \bmod N^2 \tag{18}$$

随后云服务器可以使用Paillier解密算法直接对上述形式的聚合密文进行解密，并获得聚合明文M。

$$\begin{aligned}M&=\frac{L\left(C^\lambda \bmod N^2\right)}{L\left(g^\lambda \bmod N^2\right)}\\&=\frac{L\left(C^\lambda \bmod N^2\right)}{L\left[(1+N)^\lambda \bmod N^2\right]}\\&=L\left(C^\lambda \bmod N^2\right)\cdot\lambda^{-1}\end{aligned} \tag{19}$$

最后，利用霍纳规则对聚合明文进行高速解析并获得细粒度的聚合结果；具体求解过程如算法1所示。在算法1中，系数表示某子区域j的总功耗，并且定义为：

$$UA_j=\sum_{i=1}^{n}d_{ij} \tag{20}$$

Algorithm 1. Horner rule−based analytical algorithm

Input:

M and R.

Output:

Total power consumption UA_j in each subarea $j, j=1,2,\ldots,m$.

1: **Begin**

2: $x_0\leftarrow M/R, a_1=R^1, a_2=R^2,\ldots, a_m=R^m; x_0=\mathrm{UA}_1+R^1\mathrm{UA}_2+\ldots+R^{m-1}\mathrm{UA}_m$;

3: **For** $j\leftarrow 1$ to m do

4: $UA_j\leftarrow x_{j-1} \bmod R$;

5: $x_j\leftarrow x_{j-1} \bmod R$;

6: **End for**

7: Obtain $(\mathrm{UA}_1,\mathrm{UA}_2,\ldots,\mathrm{UA}_m)$.

8: **End**

根据这些系数的值，可以成功获得细粒度聚合明文。换言之，不仅可以获取整个网络的整体功耗，还可以恢复不同子区域的功耗数据。

一旦云服务器通过上述操作获得每个子区域的功耗数据，便可以根据这些细粒度的用电数据推测每个子区域的用电趋势，为接下来的电力调度和价格的动态调整提供决策支持。此外，智能合约使这些决策能够自动执行，同时可依据时间制定动态的定价反馈策略，以鼓励用户调整其用电习惯，从而减轻电网负担并提高用电效率。

另一方面，随着数据的积累，区块链共享账本将越来越大，这种情况通常被称为区块链膨胀。例如，在过去的9年中，比特币系统账本的大小已达到153.1 GB [32]。因为这些账本主要用于计算账户余额，所以比特币的所有历史交易项目都需要保存很长时间。但对于本文提出的聚合机制，智能电表生成新的数据项并不依赖于其之前的账本数据，因此无需将所有账本数据长期保存在每个节点上。在本文中，建议定期清除过期的账本数据并释放相关节点中的存储空间，以此解决区块链膨胀问题。

5. 安全与性能分析

本节将详细讨论所提出方案的安全性和匿名性，并根据计算成本分析所提出算法在性能上的提升。特别地，本节还对攻击者在不同情况下成功发动篡改攻击的概率进行了定量分析，再次证明了该方案的高安全性。此外，本节还详细分析了身份认证和整个系统的计算成本，表明所提出的方案是轻量级的，更适合于对实时性有需求的智能电网系统。

5.1. 安全分析

数据机密性：在定义的威胁模型中，用户的功耗数据容易在通信链路处受到窃听攻击，同时雾节点和云服务器又是和“诚实”而充满“好奇心”的。因此为了保证用户隐私数据的机密性，Paillier加密算法被用于对这些用电数据进行加密，得到加密之后的功耗数据$C_{ij}=g^{d_{ij}}\cdot r^N \bmod N^2$。这意味着即使窃听者监测了所有的用户隐私数据并获知了加密算法，它们也很难在没有私钥的情况下破解密文以获取用户的隐私信息，因为Paillier加密的密文在语义上不受选择性明文攻击的影响[33]。同样地，雾节点和云服务器执行聚合的对象都是加密后的数据，若没有相应私钥，雾节点也无法获取用户的真实功耗数据。尽管云服务器可以通过使用Paillier算法的加法同态性来恢复每个子区域的聚合明文，即$\mathrm{UA}_j=\sum_{i=1}^{n}d_{ij}$，但是它仍然无法推断出每个用户的原始仪表数据。因此，本文所提出的方案为用户的功耗数据提供了高度的机密性，有效地保护了用户的隐私信息。

数据的完整性和有效性：为了抵御恶意攻击者对智能电表数据发起的主动攻击（如篡改、伪造、重放等），用户在发送密文C_{ij}和时间戳t_s到网络上层之前，需通过使用批量聚合签名方法对其进行签名，即$\sigma_{ij}=H\left[H\left(C_{ij}\|t_s\right)\|\mathrm{Pseu}_{ij}\right]^{Y_{ij}}$。

仅当$\prod_{i=1}^{n}\sigma_{ij}^{X_{ij}}=\prod_{i=1}^{n}H\left[H\left(C_{ij}\|t_s\right)\|\mathrm{Pseu}_{ij}\right]\bmod N^2$时，接收器能确认接收到的信息未被篡改。显然，一旦数据$(\sigma_{ij}\|C_{ij}\|t_s\|\mathrm{Pseu}_{ij})$被篡改，该等式就不会成立。换言之，即使攻击者成功修改了信息或发起了重放攻击，接收器也可以有效地检测到这些威胁。因此，该方案可确保隐私数据的完整性和有效性。类似地，在雾层也能提供相同的安全保护。

身份的匿名性和真实性：用户的身份通常与隐私信息相关联，用户身份信息的泄露将会导致一系列危害。在本方案中，智能电表和雾设备的身份始终以假名的形式存在，即分别为$\mathrm{Pseu}_{ij}=X_{ij}\bmod N^2$和$\mathrm{Pseu}_j=X_j\bmod N^2$，其中用户和雾设备分别随机选择公钥$X_{ij}$和$X_j$，通过上述方式随机生成假名，并且假名与用户和雾设备的真实身份无关。即使恶意攻击者成功解密了用户的电表数据，攻击仍然是无效的，因为攻击者无法获得用户的真实身份，从而实现了用户身份的匿名性。同时，也可能存在非法节点恶意冒充合法用户身份的行为，本方案的身份真实性认证机制可以有效识别这种身份欺诈行为，从而保证用户身份信息的安全性（因为已经预先收集了所有合法假名并将其映射到布隆过滤器中）。通过简单的查询操作，可以快速确定该节点的假名是否在布隆过滤器中，即确定该节点是否合法。

5.2. 攻击成功概率分析

根据第3节定义的威胁模型，本部分将分析两种典型的攻击来评估其对聚合结果的影响，即在节点和链路上发起的篡改攻击。为了证明所提出的解决方案的优势，下面将比较分析在不同解决方案下篡改攻击的成功概率。

5.2.1. 节点上的篡改攻击

在定义的威胁模型中，假设攻击者想要成功发起篡改攻击所需俘获智能电表的总数为w，而攻击者俘获雾节点所需的总数为f。为了便于理解，本节中假设每个智能电表被成功俘获的概率是独立的，并将其表示为α_i $(i=1,2,\ldots,w,\ldots,nm,0\le\alpha_i\le1)$。同样地，雾节点和云服务器的被俘概率分别由$\beta_j$ $(j=1,2,\ldots,f,\ldots,m,0\le\beta_j\le1)$和$\gamma$表示。同时，假设恶意节点成功拦截智能电表密钥的概率是独立的，并将其设置为∂_i $(i=1,2,\ldots,w,\ldots,nm,\ 0\le\partial_i\le1)$。

因此，传统安全方案下篡改攻击的成功概率是独立的，且可以表示为：

$$P_{\mathrm{node}}=\frac{1}{3}\left[\left(\prod_{i=1}^{w}\alpha_i\right)\left(\prod_{i=1}^{w}\partial_i\right)+\left(\prod_{j=1}^{f}\beta_j\right)\left(\prod_{i=1}^{fn}\partial_i\right)+\gamma\right]\quad(21)$$

式中，设置权重为1/3，表示攻击者选择攻击三种节点的概率是相等的。这种传统的安全方案是指数据在节点间传输而不考虑区块链，但其具有与本文提出的方案相同的其他安全机制。

对于提出的DA-SADA方案，由于共识机制的存在，基于区块链的安全方案可以容忍少于1/3的被俘节点。基于此结论，本节定义了每个子区域的阈值为$\psi=\mathrm{ceil}[(2/3)(n-1)+1]$，其中函数ceil( )用以返回大于或等于括号内指定表达式的值的最小整数；在雾层，相应阈值为$\psi'=\mathrm{ceil}[(2/3)(m-1)+1]$。因此，可以获知在本文所提出的方案下，篡改攻击的成功概率是独立的且可以表示为：

$$P'_{\mathrm{node}}=\frac{1}{3}\left[\left(\prod_{i=1}^{m\psi}\alpha_i\right)\left(\prod_{i=1}^{m\psi}\partial_i\right)+\left(\prod_{j=1}^{\psi'}\beta_j\right)\left(\prod_{i=1}^{n\psi'}\partial_i\right)+\gamma\right]\quad(22)$$

5.2.2. 通信链路上的篡改攻击

在这一部分将考虑通过通信链路来截获或篡改数据包的攻击。

对于传统的安全方案，攻击者可以在雾节点或云服务器接收数据之前发起攻击，以篡改用户功耗数据，这种类型的攻击往往需要成功侵入通信信道并获取发送方节点的私钥，才能成功修改数据。因此用η_i $(i=1,2,\ldots,w,\ldots,nm,\ 0\le\eta_i\le1)$表示在智能电表与雾节点之间通信链路成功发起截获攻击的概率，并将$\bar{\eta}_j$ $(j=1,2,\ldots,f,\ldots m,\ 0\le\bar{\eta}_j\le1)$表示为在雾节点与云服务器之间通信链路成功发起截获攻击的概率。因此，这种篡改攻击的成功概率是独立的且可表示为：

$$P_{\mathrm{link}}=\frac{1}{2}\left[\left(\prod_{i=1}^{w}\eta_i\right)\left(\prod_{i=1}^{w}\partial_i\right)+\left(\prod_{j=1}^{f}\bar{\eta}_j\right)\left(\prod_{i=1}^{fn}\partial_i\ \right)\right]\quad(23)$$

式中，设置权重为1/2，表示攻击者选择攻击这两种通信链路的概率是相等的。

对于本文提出的方案，考虑隐私数据被封装至区块中，用户层与雾层以及雾层与云服务器之间的通信链路在传输时，均以区块的形式存在。而一般来说，区块链中的数据是不可篡改的，因此不必考虑恶意攻击者在用户层、雾层和云服务器之间的通信链路中成功发动篡改攻击的可能性。但是，在区块链形成之前需要执行共识过程，共识过程中用户层的节点需要彼此通信以形成内部通信网络，在该通信网络中用户层可能会面临通信链路上的篡改攻击。同样地，该威胁也存在于雾层。因此，接下来将针对这两个内部通信链路网络成功发动篡改攻击的概率进行分析。首先，假设在用户层中存在通信链路$x_{\mathrm{uc}}=m\cdot\mathrm{ceil}[\psi(\psi-1)/2]$个，且在用户层中成功截获该通信链路的概率可表示为$\eta_{x_{\mathrm{uc}}}(x_{\mathrm{uc}}=1,2,\ldots,l,\ldots L,\ 0\le\eta_{x_{\mathrm{uc}}}\le1)$。与此同时，

假设在雾层中存在通信链路$x_{\mathrm{fc}}=\mathrm{ceil}[\psi'(\psi'-1)/2]$个，且在雾层成功截获该通信链路的概率可表示为$\bar{\eta}_{x_{\mathrm{fc}}}(x_{\mathrm{fc}}=1,2,\ldots,\mathcal{K},\ldots,K,0\le\bar{\eta}_{x_{\mathrm{fc}}}\le1)$。因此，在提出的双区块链网络中成功篡改数据的成功概率是独立的且可以表示为：

$$P'_{\mathrm{link}}=\frac{1}{2}\left[\left(\prod_{x_{\mathrm{uc}}=1}^{l}\eta_{x_{\mathrm{uc}}}\right)\left(\prod_{i=1}^{m\psi}\partial_i\right)+\left(\prod_{x_{\mathrm{fc}}=1}^{\mathcal{K}}\bar{\eta}_{x_{\mathrm{fc}}}\right)\left(\prod_{i=1}^{n\psi'}\partial_i\right)\right] \quad (24)$$

最后，假设在节点和通信链路上成功发动篡改攻击也是互相独立的，并且攻击者发动这两种攻击的概率也是相等的。因此，在传统的方案和本文提出的方案中，成功发动篡改攻击的总概率分别为：

$$P_{\mathrm{tradition}}=\frac{1}{2}(P_{\mathrm{node}}+P_{\mathrm{link}}) \quad (25)$$

$$P_{\mathrm{proposed}}=\frac{1}{2}(P'_{\mathrm{node}}+P'_{\mathrm{link}}) \quad (26)$$

式中，设置权重为1/2，表示攻击者发起这两种攻击的成功概率是独立且相等的。

5.2.3. 成功概率

前两部分从理论角度分析了传统方案和DA-SADA方案被成功篡改的可能性。为了更直观地显示分析结果，本部分使用Monte Carlo模拟方法对成功概率进行了进一步分析。在建立的模拟场景中，首先假设每个子区域内有20个智能电表，服务支撑层有1个云服务器，并且雾节点的数量为50。然后，假设攻击者需要操纵智能电表的概率是10%~100%，因此w在整个网络中的变化范围是100~1000。同时，本部分定义变量α、β、∂、η，$\bar{\eta}$的取值范围是0.9~1，设置γ的范围为[0,0.1]。每次试验，变量α、β、∂、η、$\bar{\eta}$的值在设置范围内随机选择，取执行1000次实验后结果的平均值以评估方案的安全性。实验在Intel Core i5-7200U CPU @ 2.50 GHZ、8.00GB RAM的笔记本电脑上运行。

图4描述了成功攻击概率与攻击者需要操纵的智能电表总数之间的相互关系。值得注意的是，随着被操纵智能电表数量的增加，攻击者成功攻击概率呈现持续下降的趋势，并且容易看出DA-SADA方案在削弱安全威胁方面有显著优势。特别地，当攻击者需要操纵的智能电表总数超过500时，DA-SADA方案中成功攻击概率接近0。之所以产生这个结果，主要归因于DA-SADA方案在生成UA-blockchain和FA-blockchain的过程中经历了两个共识机制，而共识机制需要群体验证。因此，双区块链的使用显著增强了系统的稳健性。

5.3. 计算成本分析

本节将分析身份认证的成本和整个系统的计算成本。

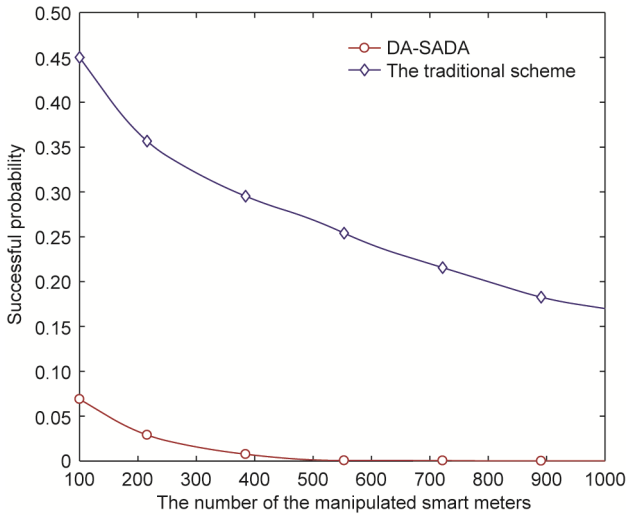

图4. 不同方案下的成功攻击概率。

在该仿真场景下，假设雾节点的数量在5~50之间变化，布隆过滤器的误判率设置为0.01，并将RSA模数N和参数p分别定义为1024位和160位。尽管基于内容的布隆过滤器通常存在冲突，但冲突概率往往非常小。例如，在使用7个不同哈希函数的情况下，要使用2 MB大小的位串，总的误判率是小于0.01的；因此，将布隆过滤器的误判率设置为0.01是合理的。为了便于说明，本节分别将T_{E1}、T_{E2}、T_{M}、T_{P}分别表示为$Z^*_{N^2}$中的指数运算，G中的指数运算、乘法运算和G中的双线性配对。使用基于配对的密码学（pairing-based cryptography, PBC）库来实现这些操作。仿真数据集来自爱尔兰能源监管委员会（Commission for Energy Regulation Ireland） [34]。表1列出了评估过程中的操作符号及其时间成本。

表1 操作符号与时间成本

Notation	Description	Time cost (ms)
T_{E1}	Exponentiation operation in $Z^*_{N^2}$	1.60
T_{E2}	Exponentiation operation in G	1.62
T_{M}	Multiplication operation	0.06
T_{P}	Pairing operation	17.70

图5显示了在使用和不使用布隆过滤器情况下身份认证的时间成本。从该图可以看出，随着智能电表数量的增加，不使用布隆滤波器的传统方案的时间成本急剧增加，但DA-SADA方案的时间成本增长范围有限，且远低于传统方案。这是因为布隆过滤器可以使用多个哈希函数来提高空间利用率，从而大大提高身份验证过程中的查询效率。

接下来为了全面分析系统的计算成本，将提出的DA-SADA方案与其他两种方案进行了比较，即安全增强数据聚合（security-enhanced data aggregation, SEDA）[13]和边

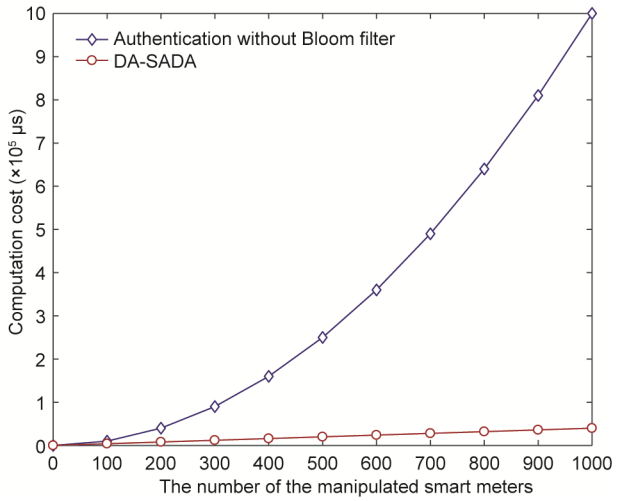

图5. 身份认证的时间成本。

缘计算中的轻量级隐私数据聚合（lightweight privacy-preserving data aggregation for edge computing, LPDA-EC）[21]。由于哈希运算的计算成本与乘幂运算和乘法运算相比可以忽略不计，因此在整个评估过程中不必考虑哈希运算的成本。

具体地，在用户层中，密文 $C_{ij}=(1+d_{ij}N)\cdot s$ 和签名 $\sigma_{ij}=H(u_{ij}\|\mathrm{Pseu}_{ij})^{Y_{ij}}$ 的生成分别需要两个乘法运算 T_{M} 和一个指数运算 T_{E1}。在每个子区域内，当用户层中的聚合节点从 n 个智能电表接收到报告 $(\sigma_{ij}\|C_{ij}\|t_s\|\mathrm{Pseu}_{ij})$ 后，首先要通过批量验证，确保接收后的数据的有效性和完整性。验证算法包括 n 个乘法运算 T_{M} 和一个指数运算 T_{E1}。接下来，用户数据的聚合运算需要 n 个乘法运算 T_{M}。最后，聚合节点将报告发送至雾层。在雾层中，生成签名 σ_j 需要一个指数运算 T_{E1}，随后雾节点将报告 $(\sigma_j\|C_j\|t_s\|\mathrm{Pseu}_j)$ 发送到雾层中的聚合节点，聚合节点首先通过对接收到的数据进行批量验证，包括 m 个乘法运算 T_{M} 和一个指数运算 T_{E1}。验证通过后，聚合节点再次对一级聚合密文 C_j（$j=1,2,\ldots,m$）进行聚合，此过程需要 m 个乘法运算 T_{M}。然后，雾节点将聚合报告继续发送至上层。当云服务器从雾节点接收到报告时，云服务器首先要对聚合报告进行解密操作，该操作包括一个指数运算 T_{E1} 和一个乘法运算 T_{M}。通过以上分析，DA-SADA 方案的整个计算过程包括操作 $(4mn+2m+1)T_{\mathrm{M}}+(mn+2m+2)T_{\mathrm{E1}}$。同样地，也可以得到其他方案的计算成本，如表2所示。

由图6可以看出，与身份认证的计算成本相类似，系统的总计算成本与智能电表的数量成正比。同时，与SEDA和LPDA-EC相比，提出的DA-SADA方案可显著降低总计算成本。例如当智能电表的数量为500时，DA-SADA方案的总计算成本为 10^3 ms，与SEDA和LPDA-EC相比，

表2 时间成本

Scheme	Operation
DA-SADA	$(4mn+2m+1)T_{\mathrm{M}}+(mn+2m+2)T_{\mathrm{E1}}$
SEDA	$2T_{\mathrm{P}}+4T_{\mathrm{E1}}+(6nm+3)T_{\mathrm{E2}}+(2nm+1)T_{\mathrm{M}}$
LPDA-EC	$2T_{\mathrm{P}}+4T_{\mathrm{E1}}+(3nm+3)T_{\mathrm{E2}}+(2nm+1)T_{\mathrm{M}}$

DA-SADA方案的总计算成本分别降低了80%、60%。而随着智能电表数量的增加，计算成本的降低将更加明显。这主要是因为双线性配对所需的时间比其他操作大得多，SEDA和LPDA-EC在验证过程中都包含昂贵的双线性配对操作。而DA-SADA方案则有效避免了使用配对计算，大大降低了计算成本。

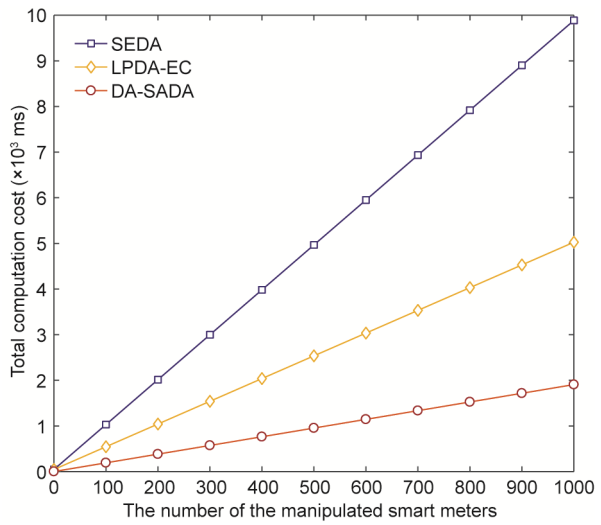

图6. 系统总计算成本。

从以上安全性和性能分析结果可看出，DA-SADA方案在提供强大的安全性和匿名性的同时，显著降低了系统的计算成本，更适合具有实时高频数据采集和聚合要求的智能电网系统。

6. 总结

智能电网可以通过收集和分析用户的用电数据来提供可靠和稳定的服务，但这些操作往往会威胁到用户的安全和隐私，为了应对这些挑战，本文提出了DA-SADA。具体来说，DA-SADA通过结合雾计算和区块链技术构建了安全性增强的三层网络体系结构，同时实现了对本地资源的有效利用。此外，提出了一种轻量级的安全聚合机制，来确保用户隐私数据的机密性、完整性和真实性。特别地，为了实现电力的灵活调控，设计的双区块链可以收集细粒度的用户功耗数据，双区块链形成过程中的双重共识

机制又进一步增强了系统的安全性。最后，详细的安全性分析可以证实DA-SADA方案的高安全性，而随后对整个系统的计算成本的比较分析，则进一步验证了所提出方案的性能优势，证明该方案更适合于对实时性有需求的智能电网系统。虽然所提出的方案为智能电网提供了一种高效、安全的数据收集机制，但仍然缺乏一种高效、智能的聚合节点选择方法。因此，在未来的工作中，拟研究一种动态的、智能的聚合节点选择机制，通过集成机器学习方法来提高所提出方案在真实网络场景中的适用性。

致谢

本研究得到了国家自然科学基金项目（61971235、61871412、61771258）、江苏省“六大人才高峰”高层次人才项目（XYDXXJS-044）、中国博士后科学基金项目（2018M630590）、江苏省“333高层次人才培养工程”、南京邮电大学“1311”人才计划、江苏省通信与网络技术工程研究中心开放课题重点项目（JSGCZX17011）、南京邮电大学科学研究基金项目（NY218058）和网络与信息安全安徽省重点实验室开放课题（AHNIS2020001）的大力支持。

Compliance with ethics guidelines

Siguang Chen, Li Yang, Chuanxin Zhao, Vijayakumar Varadarajan and Kun Wang declare that they have no conflict of interest or financial conflicts to disclose.

References

[1] Ketter W, Collins J, Saar-Tsechansky M, Marom O. Information systems for a smart electricity grid: emerging challenges and opportunities. ACM Trans Manage Inf Syst 2018;9(3):1−22.
[2] Chen S, Wen H, Wu J, Lei W, Hou W, Liu W, et al. Internet of things based smart grids supported by intelligent edge computing. IEEE Access 2019;7(1):74089−102.
[3] Asghar MR, Dán G, Miorandi D, Chlamtac I. Smart meter data privacy: a survey. IEEE Commun Surv Tutorials 2017;19(4):2820−35.
[4] Wang Y, Chen Q, Hong T, Kang C. Review of smart meter data analytics: applications, methodologies, and challenges. IEEE Trans Smart Grid 2019;10(3):3125−48.
[5] Abdallah A, Shen XS. A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. IEEE Trans Smart Grid 2018;9(1):396−405.
[6] Chen S, Wang K, Zhao C, Zhang H, Sun Y. Accelerated distributed optimization design for reconstruction of big sensory data. IEEE Internet Things J 2017;4(5):1716−25.
[7] Chen S, Wang Z, Zhang H, Yang G, Wang K. Fog-based optimized Kronecker-supported compression design for industrial IoT. IEEE Trans Sustainable Comput 2020;5(1):95−106.
[8] Yan Y, Qian Y, Sharif H, Tipper D. A survey on cyber security for smart grid communications. IEEE Commun Surv Tutorials 2012;14(4):998−1010.
[9] Chen Y, Martínez-Ortega J, Castillejo P, López L. A homomorphic-based multiple data aggregation scheme for smart grid. IEEE Sens J 2019;19(10):3921−9.
[10] Gai K, Wu Y, Zhu L, Qiu M, Shen M. Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Trans Ind Inf 2019;15(6):3548−58.
[11] Liang G, Weller SR, Zhao J, Luo F, Dong ZY. The 2015 Ukraine blackout: implications for false data injection attacks. IEEE Trans Power Syst 2017;32(4):3317−8.
[12] Lu R, Liang X, Li X, Lin X, Shen X. EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Trans Parallel Distrib Syst 2012;23(9):1621−31.
[13] Ni J, Alharbi K, Lin X, Shen X. Security-enhanced data aggregation against malicious gateways in smart grid. In: Proceedings of the 2015 IEEE Global Communications Conference; 2015 Dec 6–10; San Diego, CA, USA; 2015.
[14] Gope P, Sikdar B. An efficient data aggregation scheme for privacy-friendly dynamic pricing-based billing and demand-response management in smart grids. IEEE Internet Things J 2018;5(4):3126−35.
[15] Liu Y, Guo W, Fan C, Chang L, Cheng C. A practical privacy-preserving data aggregation (3PDA) scheme for smart grid. IEEE Trans Ind Inf 2019;15(3):1767−74.
[16] Li S, Xue K, Yang Q, Hong P. PPMA: privacy-preserving multisubset data aggregation in smart grid. IEEE Trans Ind Inf 2018;14(2):462−71.
[17] Peng L, Dhaini AR, Ho P. Toward integrated cloud-fog networks for efficient IoT provisioning: key challenges and solutions. Future Gener Comput Syst 2018;88:606−13.
[18] Lu R, Heung K, Lashkari AH, Ghorbani AA. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. IEEE Access 2017;5:3302−12.
[19] Huang C, Liu D, Ni J, Lu R, Shen X. Reliable and privacy-preserving selective data aggregation for fog-based IoT. In: Proceedings of the 2018 IEEE International Conference on Communications; 2018 May 20−24; Kansas City, MO, USA; 2018.
[20] Lyu L, Nandakumar K, Rubinstein B, Jin J, Bedo J, Palaniswami M. PPFA: privacy preserving fog-enabled aggregation in smart grid. IEEE Trans Ind Inf 2018;14(8):3733−44.
[21] Zhang J, Zhao Y, Wu J, Chen B. LPDA-EC: a lightweight privacy-preserving data aggregation scheme for edge computing. In: Proceedings of the 2018 IEEE 15th International Conference on Mobile Ad Hoc Sensor Systems; 2018 Oct 9−12; Chengdu, China; 2018.
[22] Zhu L, Li M, Zhang Z, Xu C, Zhang R, Du X, Guizani N. Privacy-preserving authentication and data aggregation for fog-based smart grid. IEEE Commun Mag 2019;57(6):80−5.
[23] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [Internet]. Bitcoin; 2018 [cited 2019 Aug 21]. Available from: https://bitcoin.org/bitcoin.pdf.
[24] Liang G, Weller SR, Luo F, Zhao J, Dong ZY. Distributed blockchain-based data protection framework for modern power systems against cyber attacks. IEEE Trans Smart Grid 2019;10(3):3162−73.
[25] Fan M, Zhang X. Consortium blockchain based data aggregation and regulation mechanism for smart grid. IEEE Access 2019;7:35929−40.
[26] Guan Z, Si G, Zhang X, Wu L, Guizani N, Du X, et al. Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. IEEE Commun Mag 2018;56(7):82−8.
[27] Yang R, Yu FR, Si P, Yang Z, Zhang Y. Integrated blockchain and edge computing systems: a survey, some research issues and challenges. IEEE Commun Surv Tutorials 2019;21(2):1508−32.
[28] Xiong Z, Zhang Y, Niyato D, Wang P, Han Z. When mobile blockchain meets edge computing. IEEE Commun Mag 2018;56(8):33−9.
[29] Wood G. Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj Yellow Pap 2014;151:1−32.
[30] Hassan MU, Rehmani MH, Chen J. Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions. Future Gener Comput Syst 2019;97:512−29.
[31] Bose P, Guo H, Kranakis E, Maheshwari A, Morin P, Morrison J, et al. On the false-positive rate of Bloom filters. Inf Process Lett 2008;108(4):210−3.
[32] Bitcoin.com. Blockchain size [Internet]. Saint Bitts LLC; 2018 [cited 2019 Aug 21]. Available from: https://charts.bitcoin.com/chart/blockchainsize.
[33] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Proceedings of the 1999 Annual International Conference on the Theory and Applications of Cryptographic Techniques; 1999 May 2−6; Prague, Czech Republic; 1999. p. 223−38.
[34] Commission for Energy Regulation. Smart metering trial data publication [Internet]. Commission for Energy Regulation; 2013 [cited 2019 Aug 21]. Available from: http://www.cer.ie/en/information-centre-reportsandpublications.aspx?article=5dd4bce4-ebd8-475e-b78d-da24e4ff7339.