控制理论与应用
Control Theory & Applications
ISSN 1000-8152,CN 44-1240/TP

《控制理论与应用》网络首发论文

题目：基于半同态加密体制的安全分布式经济调度
作者：杨飞生，刘佳明，丁瑞森，姬毓明，潘泉
收稿日期：2023-02-25
网络首发日期：2024-04-18
引用格式：杨飞生，刘佳明，丁瑞森，姬毓明，潘泉．基于半同态加密体制的安全分布式经济调度[J/OL]．控制理论与应用．
https://link.cnki.net/urlid/44.1240.TP.20240416.0935.022

基于半同态加密体制的安全分布式经济调度

杨飞生[1,2†]， 刘佳明[1,2]， 丁瑞森[1,2]， 姬毓明[1,2]， 潘　泉[2]

(1. 西北工业大学深圳研究院, 广东 深圳 518000;

2. 西北工业大学 自动化学院, 陕西 西安 710129)

摘要: 经济调度是电力系统运行中一个基本而又重要的问题, 主要涉及到如何精准调配和管理发电资源，以满足负载需求，同时尽可能地降低整体发电成本. 本文从一致性协议出发, 给出了一种基于分布式优化的经济调度算法, 以实现电力系统发电成本的最小化. 然后基于半同态加密的Paillier密码系统, 制定了隐私保护方案, 既可以保证通过网络传输的信息不被恶意攻击者获得, 又保证了每个节点的隐私数据不被其他节点获取. 最后, 通过构造Lyapunov能量泛函分析了加密解密等行为诱导的时变时延对经济调度模型的影响, 导出了兼顾保守性与复杂度的算法收敛条件, 进而通过仿真比较验证了方法的有效性和优越性.

关键词: 分布式经济调度; 隐私保护; 半同态加密; 时变时延

引用格式: 杨飞生, 刘佳明, 丁瑞森, 姬毓明, 潘泉. 基于半同态加密体制的安全分布式经济调度. 控制理论与应用, 2024, 41(x): 1– 10

DOI: 10.7641/CTA.2023.30084

Secure distributed economic dispatch based on semi-homomorphic encryption

YANG Feisheng[1,2†], LIU Jiaming[1,2], DING Ruisen[1,2], JI Yuming[1,2], PAN Quan[2]

(1. Research & Development Institute of Northwestern Polytechnical University in Shenzhen, Guangdong 518000, China;
2. School of Automation, Northwestern Polytechnical University, Xi'an Shaanxi 710129, China)

Abstract: Economic dispatch (ED) is a basic and important problem in power system operation which mainly involves how to accurately allocate and manage power generation resources to meet the load demand, while reducing the overall cost of power generation as much as possible. This paper proposes an economic dispatch algorithm based on distributed optimization from the point of view of consensus protocol to minimize the generation cost of power system. At the same time, a privacy preservation scheme is developed based on Paillier cryptosystem with semi-homomorphic encryption. This scheme can not only ensure that the information transmitted by the network is not obtained by malicious attackers, but also the privacy information of each node is not obtained by other nodes. The Lyapunov energy functional is constructed to analyze the effect of the time-varying delay induced by encryption and decryption on the economic dispatch model, and the convergence condition that makes a tradeoff between conservatism and complexity is derived. The effectiveness and superiority of the method are illustrated by simulation comparison.

Key words: distributed economic dispatch; privacy preservation; semi-homomorphic encryption; time-varying delay

Citation: YANG Feisheng, LIU Jiaming, DING Ruisen, JI Yuming, PAN Quan. Secure distributed economic dispatch based on semi-homomorphic encryption. *Control Theory & Applications*, 2024, 41(x): 1 – 10

1　引言

经济调度是电力系统运行和控制的关键问题, 其目的是满足系统约束的前提下, 协调各发电机组的发电量, 实现供电成本的最小化. 与传统的集中式经济调度相比, 分布式方案因其灵活、高效、可扩展性强等优点获得了越来越多的关注. 分布式经济调度强调参与调度的单元进行独立决策. 每个单元根据预设协议通过网络与邻居交换信息, 对比调整己方输出, 协

收稿日期: 2023−02−25; 录用日期: 2023−12−27.

†通信作者. E-mail: yangfeisheng@nwpu.edu.cn;

本文责任编委: 邹云

广东省基础与应用基础研究基金(2023A1515011220), 国家自然科学基金(62073269), 陕西省重点研发计划(2022GY-244), 航空科学基金(2020Z034053002), 重庆市自然科学基金(CSTB2022NSCQ-MSX0963)资助.

Supported by the Guangdong Basic and Applied Basic Research Foundation (2023A1515011220), National Natural Science Foundation of China (62073269), Key Research and Development Program of Shaanxi (2022GY-244) , Aeronautical Science Foundation of China (2020Z034053002), and Natural Science Foundation of Chongqing, China (CSTB2022NSCQ-MSX0963).

同最小化电力系统的发电成本. 分布式模式利用稀疏通信结构实现了各单元的分散协作, 具有较好的鲁棒性[1] 与灵活性[2]. 文献[3]提出了一种基于推送的、可应用于时变有向拓扑的分布式经济调度策略. 文献[4]提出了一种考虑通信时滞的分布式经济调度算法, 采用时滞分割的方法, 得到了算法收敛的充分条件. 文献[5]提出了一种解决多目标经济调度问题的多层分布式一致性算法, 实现了大规模多区域互联电力系统中经济调度问题的快速求解. 文献[6]提出了一种分布式双牛顿下降算法, 加快了收敛速度. 文献[7]考虑了通信延迟和噪声梯度观测, 提出了一种解决有向网络上经济调度问题的全分布式算法. 文献[8]提出了基于梯度下降和一致性的算法, 仅需在互连母线间交换局部信息就可以实现电力的供需平衡. 文献[9]基于交替方向乘子法提出了一种完全分布式的跨区域电力系统动态经济调度方法.

然而, 为实现成本最小化的目标, 发电机组通常会将重要且敏感的信息传递给邻居进行分布式计算, 因此一旦有攻击者侵入通信链路, 就能轻易窃取传输信息, 对系统安全造成威胁. 除此之外, 邻居的一些不当行为也有可能造成隐私信息的泄露. 研究人员针对上述安全问题提出了各种方法, 比较流行的有基于噪声的数据混淆[10–13]、基于区块链的安全保护[14–15] 以及基于密码学的加密方法[16–17]. 文献[10]提出了一种基于秘密函数的保护算法, 每个节点向原始数据添加仅相邻节点可知的指数衰减噪声进行通信. 文献[11]定义了(α,β)-数据隐私, 并开发了一种添加均匀分布的噪声来实现最高(α,β)-数据隐私的算法. 文献[12]通过注入噪声来掩盖传输信息, 同时建立了节点行为监测机制和基于声誉的异常单元隔离方案. 文献[13]使用差分隐私来保护传输信息, 还研究了收敛性、准确性和差分隐私之间的权衡. 文献[14]中通过使用区块链技术、多重签名和匿名加密消息流保证分布式能源交易的信息安全, 使各节点能够匿名协商能源价格并安全地执行交易. 文献[15]利用区块链组建协调中心实现了分布式系统进行经济调度成员间的平衡, 还开发了无协调中心情况下使用的分层安全约束算法. 文献[16]针对分布式原始-对偶次梯度算法, 设计了近似数算法的全同态加密方案来保护分布式能量管理系统的用户隐私. 文献[17]针对分布式投影梯度算法的安全问题, 提出了可以实现安全多方计算的的私钥全同态加密方案, 该方案可以保护每个参与者不受任何其他参与者的影响.

基于公钥和私钥的一致性算法可以分为非对称加密方法与对称加密方法. 非对称加密方法多使用Paillier 加密体制. 基于公钥和私钥文献[18]提出了一种基于半同态加密机制的隐私保护一致性算法. 文献[19]采用了非对称Paillier 加密方法来实现平均一致性的信息传输安全. 文献[16]也采用了Paillier加密机制来确保能源管理算法中的信息安全. 文献[20]研究了一种基于Paillier加密的二阶动态网络系统的平均一致性算法. 文献[21]在Paillier 加密机制的基础上设计了一个辅助变量来保证容错一致性控制方案的安全性. 文献[22]使用了对称加密的方式将估计的状态加密成一系列有限级码字, 然后通过有向拓扑传输给其他智能体. 与上述工作不同的是, 以上文章中的安全一致性算法没有考虑到加密解密过程计算量增大对信息传输实时性的影响, 本文首次将加密解密、处理数据以及信息传输的过程对算法运行的影响建模并加以处理.

本文基于Paillier密码体制提出了分布式经济调度的隐私保护方案, 主要创新点有两个方面. (1) 针对含灵活负载与光伏发电的电力系统经济调度问题, 设计合适的分布式优化算法, 进而引入Paillier 加密体制[23], 围绕算法的信息交换提出一套隐私保护方案, 能够在确保信息传输安全、节点隐私性好的前提下实现最优分布式经济调度. (2) 考虑到使用Paillier密码体制在加密解密时需要比较大的计算量, 这会影响信息传输的实时性, 本文将这种影响建模成更具有现实意义的时变时延. 针对受时延影响的经济调度算法, 通过构造多重求和的能量泛函, 求取差分并放缩, 获得了兼顾保守性与复杂性的时滞依赖算法收敛判据, 证明了所提算法在时延影响下依然收敛, 发电机的最优发电量可以被求出, 同时实现了发电成本的最小化.

2 预备知识与问题描述

2.1 Paillier密码系统重要性质

Paillier密码系统[18,23]具有半同态加密的性质, 适用于开放和动态的网络, 不需要在第三方协助下进行密钥的管理. 该密码系统使用一个私钥和一个可以分发的公钥, 获得公钥的个体可以使用公钥加密信息, 但经过加密的信息只能由持有私钥的个体解密. 加性同态是Paillier密码体制最重要的性质, 信息t_1+t_2的密文$\Psi(t_1+t_2)$可以通过$\Psi(t_1)$ 和$\Psi(t_2)$计算而得到:

$$\psi(t_1+t_2)=\psi(t_1)\times\psi(t_2). \tag{1}$$

将该性质做进一步推导, 可以得到在f为正整数的前提下, 有:

$$\psi(t)^f=\prod_{i=1}^{f}\psi(t)=\psi(\sum_{i=1}^{f}t)=\psi(ft), \tag{2}$$

其中$i=1,2,3,\cdots,f$.

2.2 问题描述

考虑一个由N个节点组成的电力系统, 每个节点包含独立的发电机组与负载, 发电机组是由地理位置相近、性质相同的多台发电机共同组成的一个集群.

每个节点均含火力发电机组, 部分节点还含有新能源发电机组, 负载包括固定负载与灵活负载, 后者反映了用户侧电力需求的实时性. 火力发电机组的发电成本函数可近似描述为[12–13, 15]:

$$C_i(p_i) = \alpha_i + \beta_i p_i + \gamma_i p_i^2, i = 1, 2, ..., N. \quad (3)$$

其中, $C_i(p_i)$代表节点i所含火力发电机组的发电成本, p_i代表其发电量, α_i, β_i, γ_i 是拟合的成本系数. 新能源发电考虑光伏发电, 其电力输出相比其他清洁能源发电方式更具稳定性. 对于光伏发电, 假设其运营成本可以忽略不计[24]. 电力系统中经济调度的目标是通过调整可控发电机组的发电量, 在满足电力供需平衡的基础上, 实现发电成本的最小化, 该过程通常还要考虑发电机组的发电约束, 所以分布式经济调度问题可以表述为:

$$\begin{aligned} &\min \textstyle\sum_{i=1}^{N} C_i(p_i) \quad (4)\\ s.t. \quad &\textstyle\sum_{i=1}^{N} p_i + \sum_{j\in\mathcal{M}} p_j = P_d + \sum_{k\in\mathcal{N}} p_k,\\ &p_i^{\min} \le p_i \le p_i^{\max}, i = 1, 2, ..., N.\\ &0 \le p_k \le p_k^{\max}, k \in \mathcal{N}. \end{aligned}$$

其中, P_d是电力系统恒定负载的总用电需求, $p_i^{\min}$和$p_i^{\max}$分别是第i 个节点所含火力发电机组的功率输出下限和上限, p_i 是第i 个节点所含火力发电机组的功率输出. $\mathcal{M}$是所有含有光伏发电机组节点的集合, p_j表示第j个节点所含光伏发电机组的功率, $\mathcal{N}$为所有含有灵活负载节点的集合, p_k 表示第k个节点所含灵活负载的需求值. $\sum_{k\in\mathcal{N}} p_k^{\max}$是灵活负载需求的最大值. 供电时优先消耗光伏发电机组产生的电力, 调控对象仅为可控的火力发电机组, 因此接下来的描述中发电机组i均指节点i所含的火力发电机组. 为经济调度不失一般性, 有如下假设:

假设 1　优化问题(4) 存在可行解, 满足:
$\sum_{i=1}^{N} p_i^{\min} \le P_d + \sum_{k\in\mathcal{N}} p_k^{\max} \le \sum_{i=1}^{N} p_i^{\max}$.

假设 2　分布式电力系统的通信拓扑为无向连通图.

3　信息传输与隐私保护方案

3.1　分布式经济调度方法

在经济调度中, $\lambda_i(k)$代表k时刻火力发电机组i的增量成本, a_{ij} 表示节点i 和j间的权重, 火力发电机组依据$\lambda_i(k)$ 调整发电量$p(k)$:

$$p(k+1) = B\lambda(k+1) - [\sigma_1, \sigma_2, ..., \sigma_i]^T, \quad (5)$$

其中B=$diag(1/2\gamma_i)$, σ_i=$\beta_i/2\gamma_i$. 因为火力发电机组存在功率输出约束, 所以当$p_i(k+1) \ge p_i^{max}$时, 令$p_i(k+1) = p_i^{max}$, 当$p_i(k+1) \le p_i^{min}$时, 令$p_i(k+1) = p_i^{min}$.

需要建立一个分布式电力系统的状态迭代算法来实现成本最小化, 多智能体系统中常用下述规则进行迭代:

$$\lambda_i(k+1) = \lambda_i(k) + \epsilon_1 \sum_{j\in N_i} a_{ij}[\lambda_j(k) - \lambda_i(k)], \quad (6)$$

其中, N_i表示节点i的邻居集合, ϵ_1是恒定的学习增益, 假设系统通信拓扑图Laplace矩阵的最大特征值为p, 则$\epsilon_1 \le 1/p$.

但式(6)仅能实现系统增量成本的一致性, 无法保证系统中电力供给与用电需求相匹配, 只适用于初始时刻供需相匹配的电力系统. 因此引入函数$m(k) = col\{m_1(k), m_2(k), ...m_N(k)\}$表示局部的电力供需失配, $m(k)$定义如下:

$$m(k+1) = m(k) - \epsilon_2 Lm(k) - [p(k+1) - p(k)], \quad (7)$$

L为系统通信拓扑图的Laplace矩阵, ϵ_2 也是恒定的学习增益, 也需满足$\epsilon_2 \le 1/p$. 将$m(k)$引入式(6) 作为调整火力发电总输出的反馈可得:

$$\lambda(k+1) = \lambda(k) - \epsilon_1 L\lambda(k) + \iota m(k), \quad (8)$$

其中ι为反馈系数, 是一个较小的正常数. 将式(6)-(8)进行联立得到增广的分布式经济调度状态空间描述:

$$\begin{bmatrix} \lambda(k+1) \\ m(k+1) \end{bmatrix} = \begin{bmatrix} I - \epsilon_1 L & \iota I \\ \epsilon_1 BL & I - \epsilon_2 L - \iota B \end{bmatrix} \begin{bmatrix} \lambda(k) \\ m(k) \end{bmatrix}. \quad (9)$$

注 1　首先建立Lagrange函数

$$\mathcal{L} = \sum_{i=1}^{N} C_i(p_i) + \lambda \left(\sum_{i\in\mathcal{M}} p_j + \sum_{i\in\mathcal{N}} p_k - \sum_{i=1}^{N} p_i \right).$$

根据KKT条件$\begin{cases} \frac{\partial \mathcal{L}}{\partial p_i} = 0 \\ \frac{\partial \mathcal{L}}{\partial \lambda} = 0 \end{cases}$ 可以得到

$$\begin{cases} P_d + \sum_{k\in\mathcal{N}} p_k - \sum_{j\in\mathcal{M}} p_j - \sum_{i=1}^{N} p_i^* = 0 \\ 2\gamma_i p_i^* + \beta_i - \lambda^* = 0 \end{cases},$$

进一步可以得到

$$\begin{cases} \lambda^* = \frac{P_d + \sum_{k\in\mathcal{N}} p_k - \sum_{j\in\mathcal{M}} p_j + \sum_{i=1}^{N} \frac{\beta_i}{2\gamma_i}}{\sum_{i=1}^{N} \frac{1}{2\gamma_i}} \\ p_i^* = \frac{\lambda - \beta_i}{2\gamma_i} \end{cases}.$$

可以看出Lagrange乘子λ达成一致性时, 发电供需达到平衡, 所以采用一致性算法(6), 由于$2\gamma_i p_i^* + \beta_i - \lambda^* = 0$, 所以有式(5). 将$m(k)$引入式(6)作为调整火力发电总输出的反馈得到(7).

3.2　隐私保护方案

为保证电力系统分布式经济调度时信息传输的安全性, 结合文献[18]中的方法, 本文提出一种基于Paillier密码系统的新型隐私保护方案. 针对权重平衡的分布式发电系统, 具体方案设计分为以下几个步

骤:

1) 传输准备:

根据电力系统中各发电机组的特点与距离, 获得分布式电力系统的无向加权图. 将图中每条边的权重都拆分为两个正整数因子, 与这条边相关的发电机组仅可获得其中的一个因子. 例如, 对于节点i和j之间的权重a_{ij}, 首先将其拆分为a_{i-j}和a_{j-i}, $a_{ij}=a_{i-j}\times a_{j-i}$, i仅可获得a_{i-j}的数值, j仅可获得a_{j-i}的数值. 完成权重分解与分配后, 各节点生成密钥并将其中的公钥分享给邻居.

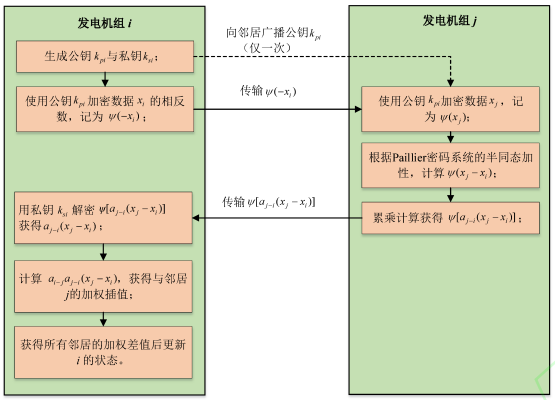

图 1 发电机组间信息传递方案

Fig. 1 Information transmission scheme among generator units

2) 数据传输:

下面将以节点i为例描述与其邻居j的一次信息传递的过程, 记i的公钥为k_{pi}, 私钥为k_{si}:

(a) 节点i使用k_{pi}加密己方状态信息x_i的相反数, 记为$\Psi(-x_i)$, 然后传送给j;

(b) 节点j用k_{pi}加密己方信息x_j, 收到$\Psi(-x_i)$后, 根据式(1)计算$\Psi(x_j)\times\Psi(-x_i)$得到$\Psi(x_j-x_i)$;

(c) 节点j根据式(2), 将$\Psi(x_j-x_i)$累乘a_{j-i}次得到$\Psi[a_{j-i}(x_j-x_i)]$, 并将该值传回i;

(d) 节点i在收到回传数据后, 使用k_{si}解密可得$a_{j-i}(x_j-x_i)$, 乘以a_{i-j}得到与j的状态信息加权差.

图1展示了节点i如何在不造成信息外泄的前提下, 获得与邻居j的加权差值. 发电机组每次状态更新都需要将上述交换过程进行(邻居个数*状态个数)次, 但这些交换可以并行进行.

3) 公钥更新:

公钥的分享发生在传输准备阶段, 所有节点以明文的方式向邻居分享自己的公钥, 在这以后数据仅以密文的形式进行交互.

设置公钥更新标志位, 根据实际情况对公钥进行更新, 新公钥$k_p(k+1)$的获取依赖于原有公钥$k_p(k)$, 描述为$k_p(k+1)=\mathcal{Z}(k_p(k))$, 其中$\mathcal{Z}(k_p(k))$表示对$k_p(k)$进行基础运算, 这种更新方式不会侵害到其他发电机组的隐私. 其他有更新必要的信息, 如对节点间权重的调整, 也按照这种方式进行.

注 2 本方案通过加密的方式保护数据隐私, 通过特殊的信息交换机制使得节点在不直接获得邻居信息的情况下也能正常经济调度, 有效的提高了信息的安全性与隐私性. 在该方案实施过程中, 信息的加密使外部攻击者无法获知发电机组的具体状态; 因为密钥的存在, 攻击者也无法伪造出可以欺骗发电机组的错误数据, 使得分布式发电系统在一定程度上免疫欺骗攻击.

4 考虑时间延迟的分布式经济调度

上一节设计的基于Paillier密码系统的隐私保护方案可实施性强, 并且对于数据安全具有很高的价值, 但是加密传输会给系统带来时间延迟[25]. 从图1中也可以看出, 相较于明文传输, 该方案获得一次加权差值需要经过加解密、密文运算等一系列行为.

本节将隐私保护方案对数据实时性的影响建模为时间延迟, 分析时延对经济调度算法收敛性造成的影响. 文献[26]开展了类似的工作, 但该文献只分析了固定时延的影响, 考虑到复杂的工作环境, 本节针对在工程应用中具有更大的实际意义的时变时延展开研究.

4.1 分布式优化模型更新

通过前述安全方案保护分布式电力系统的传输信息, 将其带给算法的影响建模为时变时延$d(k)$, $0<\underline{d}\le d(k)\le\overline{d}$. 对发电机组$i$来说, 状态$\lambda_i(k)$与$m_i(k)$依靠自身信息以及邻居间状态的加权差值进行迭代, 后者需要通过交互获得. 经济调度模型(9)中状态的加权差值均与矩阵L 相关, 因此使用隐私保护方案后需要将模型做如下调整:

$$\begin{bmatrix}\lambda(k+1)\\ m(k+1)\end{bmatrix}=\begin{bmatrix}I & \iota I\\ 0 & I-\iota B\end{bmatrix}\begin{bmatrix}\lambda(k)\\ m(k)\end{bmatrix}+\begin{bmatrix}-\epsilon_1 L & 0\\ \epsilon_1 BL & -\epsilon_2 L\end{bmatrix}\begin{bmatrix}\lambda(k-d(k))\\ m(k-d(k))\end{bmatrix}. \tag{10}$$

根据模型(10)可知节点的状态更新参考了若干周期以前的邻居信息, 这不可避免地会造成误差, 影响一致性的实现, 如果时延超出允许范围, 则会使得算法震荡甚至发散, 因此需要对时延影响下的经济调度开展性能分析. 为了便于下一步分析, 将式(10)简化为:

$$x(k+1)=Ax(k)+A_d x(k-d(k)), \tag{11}$$

其中

$$x(k)=\begin{bmatrix}\lambda(k)\\ m(k)\end{bmatrix},A=\begin{bmatrix}I & \iota I\\ 0 & I-\iota B\end{bmatrix},$$

$$A_d=\begin{bmatrix}-\epsilon_1 L & 0\\ \epsilon_1 BL & -\epsilon_2 L\end{bmatrix},$$

系统的初始状态定义为: $x(k)=\varphi(k)$, $-\overline{d}\le k\le 0$.

注 3　节点间每一条传输的信息都会被加密, 这种加密解密的过程被建模成了时延, 所以时延存在于所有需要交换信息的节点之间. 由于传输的信息都需要加密解密, 其带来的计算量增加不可避免, 那么时延也是一个不可避免的现象, 所以本文设置了时延下界.

4.2　收敛性与最优性分析

使用$\mathbb{R}^{p\times q}$表示的所有$p\times q$实矩阵的集合, $\mathbb{S}_+^p$表示$\mathbb{R}^{p\times p}$中所有对称正定实矩阵的集合. 为方便推导过程中的书写, 首先定义:

$$\xi(k)=[\xi_1^T(k)\quad \xi_2^T(k)\quad \xi_3^T(k)\quad \xi_4^T(k)]^T,$$

$$\xi_1(k)=\begin{bmatrix}x(k)\\ x(k-\underline{d})\\ x(k-d(k))\\ x(k-\overline{d})\end{bmatrix},$$

$$\xi_2(k)=\begin{bmatrix}\frac{1}{\underline{d}+1}\sum_{s=k-\underline{d}}^{k}x(s)\\ \frac{1}{d_1+1}\sum_{s=k-d(k)}^{k-\underline{d}}x(s)\\ \frac{1}{d_2+1}\sum_{s=k-\overline{d}}^{k-d(k)}x(s)\end{bmatrix},$$

$$\xi_3(k)=\begin{bmatrix}\frac{2}{(\underline{d}+2)(\underline{d}+1)}\sum_{s=-\underline{d}}^{0}\sum_{u=k+s}^{k}x(u)\\ \frac{2}{(d_1+2)(d_1+1)}\sum_{s=-d(k)}^{-\underline{d}}\sum_{u=k+s}^{k-\underline{d}}x(u)\\ \frac{2}{(d_2+2)(d_2+1)}\sum_{s=-\overline{d}}^{-d(k)}\sum_{u=k+s}^{k-d(k)}x(u)\end{bmatrix},$$

$$\xi_4(k)=\begin{bmatrix}\frac{6}{\prod_{i=1}^{3}(\underline{d}+i)}\sum_{j=-\underline{d}}^{0}\sum_{s=j}^{0}\sum_{u=k+s}^{k}x(u)\\ \frac{6}{\prod_{i=1}^{3}(d_1+i)}\sum_{j=-d(k)}^{-\underline{d}}\sum_{s=j}^{-\underline{d}}\sum_{u=k+s}^{k-\underline{d}}x(u)\\ \frac{6}{\prod_{i=1}^{3}(d_2+i)}\sum_{j=-\overline{d}}^{-d(k)}\sum_{s=j}^{-d(k)}\sum_{u=k+s}^{k-d(k)}x(u)\end{bmatrix},$$

$d_1=d(k)-\underline{d}$, $d_2=\overline{d}-d(k)$.

定理 1　在假设1、2成立的前提下, 对于存在时变时延$d(k)$, $\underline{d}\le d(k)\le\overline{d}$的分布式经济调度模型(11), 如果存在$\underline{d}$, $\overline{d}$, 与矩阵$P\in\mathbb{S}_+^{3w}$, $Q_1,Q_2,R_1,R_2,Z_1,Z_2,Z_3,Z_4\in\mathbb{S}_+^{w}$, $S\in\mathbb{R}^{3w\times 3w}$, 使得$d(k)=\overline{d}$与$d(k)=\underline{d}$时线性矩阵不等式(12), (13)同时成立, 则分布式经济调度算法收敛, 其中w为系统矩阵A 的阶数.

$$\Omega_1+\Omega_2-\Gamma<0, \tag{12}$$

$$\begin{bmatrix}\overline{R}_2+\overline{Z}_3 & S\\ S^T & \overline{R}_2+\overline{Z}_4\end{bmatrix}\ge 0, \tag{13}$$

其中

$$\begin{aligned}\Omega_1=&(\Pi_1-\Pi_2)^TPF(d(k))\\ &+F(d(k))^TP(\Pi_1-\Pi_2),\\ \Omega_2=&-M_1^T\overline{R}_1M_1-M_4^T\widetilde{Z}_1M_4-M_5^T\widetilde{Z}_2M_5\\ &-M_6^T\widetilde{Z}_3M_6-M_7^T\widetilde{Z}_3M_7-M_8^T\widetilde{Z}_4M_8\\ &-M_9^T\widetilde{Z}_4M_9+e_1^TQ_1e_1-e_2^TQ_1e_2\\ &+e_2^TQ_2e_2-e_4^TQ_2e_4+\Pi_1^TP\Pi_1-\Pi_2^TP\Pi_2\\ &+(e_0-e_1)^T[\underline{d}^2R_1+\frac{\underline{d}(\underline{d}+1)}{2}(Z_1+Z_2)\\ &+\frac{(\overline{d}-\underline{d})(\overline{d}-\underline{d}+1)}{2}(Z_3+Z_4)\\ &+(\overline{d}-\underline{d})^2R_2](e_0-e_1)+d_2(d_1+1)e_6\\ &-d_2e_2+(d(k)-\underline{d})(d_2+1)e_7-\\ &(d(k)-\underline{d})e_3,\end{aligned}$$

$$\Gamma=\begin{bmatrix}M_2\\ M_3\end{bmatrix}^T\begin{bmatrix}\overline{R}_2 & S\\ S^T & \overline{R}_2\end{bmatrix}\begin{bmatrix}M_2\\ M_3\end{bmatrix},$$

$$\Pi_1=col\{e_0,(\underline{d}+1)e_5-e_2,-e_4-e_3\},$$

$$\Pi_2=col\{e_1,(\underline{d}+1)e_5-e_1,-e_3-e_2\},$$

$$\begin{aligned}M_1=col\{&e_1-e_2,e_1+e_2-2e_5,\\ &e_1-e_2+6e_5-6e_8\},\end{aligned}$$

$$\begin{aligned}M_2=col\{&e_2-e_3,e_2+e_3-2e_6,\\ &e_2-e_3+6e_6-6e_9\},\end{aligned}$$

$$\begin{aligned}M_3=col\{&e_3-e_4,e_3+e_4-2e_7,\\ &e_3-e_4+6e_7-6e_{10}\},\end{aligned}$$

$$\begin{aligned}M_4=col\{&e_1-e_5+\frac{1}{\underline{d}+1}e_1,\\ &e_1+2e_5-\frac{2}{\underline{d}+1}e_1-3e_8,\\ &e_1-3e_5+\frac{3}{\underline{d}+1}e_1+12e_8-10e_{11}\},\end{aligned}$$

$$\begin{aligned}M_5=col\{&-e_2+e_5-\frac{1}{\underline{d}+1}e_1,\\ &e_2-4e_5+\frac{4}{\underline{d}+1}e_1+3e_8,\\ &-e_2+9e_5-\frac{9}{\underline{d}+1}e_1-18e_8+10e_{11}\},\end{aligned}$$

$$\begin{aligned}M_6=col\{&e_2-e_6+\frac{1}{d_1+1}e_2,\\ &e_2+2e_6-\frac{2}{d_1+1}e_2-3e_9,\\ &e_2-3e_6+\frac{3}{d_1+1}e_2+12e_9-10e_{12}\},\end{aligned}$$

$$\begin{aligned}M_7=col\{&e_3-e_7+\frac{1}{d_2+1}e_3,\\ &e_3+2e_7-\frac{2}{d_2+1}e_3-3e_{10},\\ &e_3-3e_7+\frac{3}{d_2+1}e_3+12e_{10}-10e_{13}\},\end{aligned}$$

$$M_8=col\{-e_3+e_6-\frac{1}{d_1+1}e_2,$$

$$e_3-4e_6+\frac{4}{d_1+1}e_2+3e_9,$$
$$-e_3+9e_6-\frac{9}{d_1+1}e_2-18e_9+10e_{12}\},$$
$$M_9=col\{-e_4+e_7-\frac{1}{d_2+1}e_3,$$
$$e_4-4e_7+\frac{4}{d_2+1}e_3+3e_{10},$$
$$-e_4+9e_7-\frac{9}{d_2+1}e_3-18e_{10}+10e_{13}\},$$
$$F(\,d(\,k))=col\{0_{13w\times w},0_{13w\times w},$$
$$(d_1+1)e_6+(d_2+1)e_7\},$$
$$e_i=[0_{w\times[w\times(i-1)]},I_w,0_{w\times[w\times(13-i)]}]^T,$$
$$i=1,2,...,13,$$
$$e_0=Ae_1+A_de_3,$$
$$\overline{R_i}=diag\{R_i,3R_i,5R_i\},i=1,2,$$
$$\overline{Z_i}=diag\{Z_i,3Z_i,5Z_i\},i=3,4,$$
$$\widetilde{Z_i}=diag\{2Z_i,4Z_i,6Z_i\},i=1,2,3,4.$$

证 构建Lyapunov-Krasovskii泛函如下:

$$V(k)=\sum_{i=1}^{5}V_i(k),$$

其中

$$V_1(k)=\zeta^T(k)P\zeta(k),$$
$$\zeta(k)=col\{x(k),\sum_{s=k-\underline{d}}^{k-1}x(s),\sum_{s=k-\overline{d}}^{k-\underline{d}-1}x(s)\},$$
$$V_2(k)=\sum_{s=k-\underline{d}}^{k-1}x^T(s)Q_1x(s)+\sum_{s=k-\overline{d}}^{k-\underline{d}-1}x^T(s)Q_2x(s),$$
$$V_3(k)=\underline{d}\sum_{s=-\underline{d}}^{-1}\sum_{v=k+s}^{k-1}y^T(v)R_1y(v)+(\overline{d}-\underline{d})\sum_{s=-\overline{d}}^{-\underline{d}-1}\sum_{v=k+s}^{k-1}y^T(v)R_2y(v),$$
$$V_4(k)=\sum_{s=-\underline{d}}^{-1}\sum_{u=s}^{-1}\sum_{v=k+u}^{k-1}y^T(v)Z_1y(v)+\sum_{s=-\underline{d}}^{-1}\sum_{u=-\underline{d}}^{s}\sum_{v=k+u}^{k-1}y^T(v)Z_2y(v),$$
$$V_5(k)=\sum_{s=-\overline{d}}^{-\underline{d}-1}\sum_{u=s}^{-\underline{d}-1}\sum_{v=k+u}^{k-1}y^T(v)Z_3y(v)+\sum_{s=-\overline{d}}^{-\underline{d}-1}\sum_{u=-\overline{d}}^{s}\sum_{v=k+u}^{k-1}y^T(v)Z_4y(v).$$

其中$y(k):=x(k+1)-x(k)$, 对$V(k)$计算前向差分可以得到:

$$\Delta V_1=\zeta^T(k+1)P\zeta(k+1)-\zeta^T(k)P\zeta(k),$$
$$\Delta V_2=x^T(k)Q_1x(k)-x^T(k-\underline{d})Q_1x(k-\underline{d})+x^T(k-\underline{d})Q_2x(k-\underline{d})-x^T(k-\overline{d})Q_2x(k-\overline{d}),$$
$$\Delta V_3=\underline{d}^2y^T(k)R_1y(k)-\underline{d}\sum_{u=k-\underline{d}}^{k-1}y^T(u)R_1y(u)+(\overline{d}-\underline{d})^2y^T(k)R_2y(k)-(\overline{d}-\underline{d})\sum_{u=k-\overline{d}}^{k-\underline{d}-1}y^T(u)R_2y(u),$$
$$\Delta V_4=\frac{\underline{d}(\underline{d}+1)}{2}y^T(k)(Z_1+Z_2)y(k)-\sum_{s=-\underline{d}}^{-1}\sum_{u=k+s}^{k-1}y^T(u)Z_1y(u)-\sum_{s=-\underline{d}}^{-1}\sum_{u=k-\underline{d}}^{k+s}y^T(u)Z_2y(u),$$
$$\Delta V_5=\frac{(\overline{d}-\underline{d})(\overline{d}-\underline{d}+1)}{2}y^T(k)(Z_3+Z_4)y(k)-\sum_{s=-\overline{d}}^{-\underline{d}-1}\sum_{u=k+s}^{k-\underline{d}-1}y^T(u)Z_3y(u)-\sum_{s=-\overline{d}}^{-\underline{d}-1}\sum_{u=k-\overline{d}}^{k+s}y^T(u)Z_4y(u).$$

根据 [27]与倒数凸组合引理[28] 对ΔV 中的相关项(或相关项的变形)进行处理, 即可得到如下不等式关系:

$$\Delta V\le\xi^T(k)(\Omega_1+\Omega_2-\Gamma)\xi(k).$$

根据Lyapunov稳定性理论, 当$\Delta V<0$, 即存在矩阵$(\Omega_1+\Omega_2-\Gamma)$负定时, 系统渐进稳定, 亦即分布式经济调度算法收敛, 定理1得证. □

定理 2 在算法收敛的前提下, 本文所提出的分布式经济调度算法可以实现增量成本的一致性, 并且可以保证系统总发电量等于总负载需求, 算法收敛至优化问题(4)的最优解.

证 因为灵活负载的需求以及光伏发电的出力在一段时间内都维持在一个相对固定的值, 所以假设火力发电需要满足的负载需求为: $D_p=P_d+\sum_{k\in\mathcal{N}}p_k-\sum_{i\in\mathcal{M}}p_i$. 使用Lagrange乘子法可得优化问题(4)的最优解$\lambda^*=[D_p+\sum_{i=1}^{N}(\beta_i/2\gamma_i)]/\sum_{i=1}^{N}(1/2\gamma_i)$. 分布式经济调度模型(11)达到平衡状态时有$\overline{\lambda}(k+1)=\overline{\lambda}(k)=\overline{\lambda}(k-d(k))$, 由此可以得

到$\epsilon_1 L\lambda(k)=\iota m(k)$, 通过使用Laplace矩阵性质$1_N^T L=0$可以推出此时局部电力失配$m(k)=0$, 电力供需已经实现了平衡. 将式(5)左乘$1_N^T$可以获得总发电量(总负载需求)与$\sum_{i=1}^{N}\lambda_i$间的关系, 因为在算法收敛时各节点的增量成本具有一致性, 进而可知此时增量成本等于λ^*, 即算法收敛于优化问题(4) 的最优解. □

5　仿真验证

考虑由12个节点构成的分布式电力系统, 每个节点表示发电机组与负载, 其中第3、4、6、9、10、12节点除火力发电机组外还集成了光伏发电机组, 第1、2、6、7、8、12 节点含有灵活负载. 表1给出了各节点所含火力发电机组的成本函数拟合参数与发电限制. 节点的初始电力情况如表2所示. 将本文所提经济调度算法应用于上述系统, 算法所需参数设置如下: $\iota=8.0\times10^{-4}$, $\epsilon_1=1/150$, $\epsilon_2=1/150$, 采样间隔设置为0.1s. 为验证本文方法的有效性, 使用定理1和文献[27]、[29]中的结论分别计算了$\underline{d}=1$的情况下分布式经济调度模型可以承受的时延最大允许上界(maximum allowable upper bounds, MAUBs). 表3展示了数值结果, 包括决策变量数. 系统通信拓扑的邻接矩阵如下述矩阵A所示.

$A=[0\,2\,1\,0\,0\,1\,3\,0\,0\,3\,1\,0;\ 2\,0\,3\,0\,1\,0\,2\,2\,2\,2\,0\,3;\ 1\,3\,0\,3\,1\,2\,0\,0\,0\,2\,2\,1;\ 0\,0\,3\,0\,2\,2\,0\,0\,2\,1\,1\,2;\ 0\,1\,1\,2\,0\,1\,2\,2\,0\,3\,1\,0;\ 1\,0\,2\,2\,1\,0\,3\,3\,2\,1\,0\,1;\ 3\,2\,0\,0\,2\,3\,0\,1\,1\,0\,2\,0;\ 0\,2\,0\,0\,2\,3\,1\,0\,3\,1\,2\,2;\ 0\,2\,0\,2\,0\,2\,1\,3\,0\,1\,2\,1;\ 3\,2\,2\,1\,3\,1\,0\,1\,1\,0\,2\,2;\ 1\,0\,2\,1\,1\,0\,2\,2\,2\,2\,0\,1;\ 0\,3\,1\,2\,0\,1\,0\,2\,1\,2\,1\,0]$.

表 1　发电机组成本计算参数及发电限制

Table 1　Generator cost calculation parameters and generation limits

节点	γ_i	β_i	α_i	$p_i^{\min}$(MW)	$p_i^{\max}$(MW)
1	0.0142	7.20	510	380	510
2	0.0145	7.00	600	360	480
3	0.0143	6.60	570	360	470
4	0.0147	6.80	500	380	425
5	0.0145	6.60	620	385	465
6	0.0142	7.00	550	355	450
7	0.0148	7.20	550	380	510
8	0.0147	7.00	600	360	480
9	0.0146	6.60	570	360	470
10	0.0145	6.80	500	380	425
11	0.0144	6.60	620	385	465
12	0.0142	7.00	550	355	450

表 2　节点的初始电力情况

Table 2　Initial power condition

节点	1	2	3	4	5	6
火力输出(MW)	500	450	370	400	460	420
光伏输出(MW)	0	0	100	50	0	40
固定负载(MW)	310	300	550	380	420	430
灵活负载(MW)	70	100	0	0	0	60
节点	7	8	9	10	11	12
火力输出(MW)	500	450	370	400	460	420
光伏输出(MW)	0	0	100	50	0	40
固定负载(MW)	310	300	550	380	420	430
灵活负载(MW)	70	100	0	0	0	60

表 3　$\underline{d}=1$情况下MAUBs及决策变量数

Table 3　MAUBs and number of decision variables when $\underline{d}=1$

方法	MAUBs	决策变量数
[27]	7	$32.5w^2+6.5w$
[29]	7	$29.5w^2+8.5w$
定理1	7	$17.5w^2+5.5w$

可以看到, 三种方法在$\underline{d}=1$的情况下都得到了相同的时延最大允许上界, 但定理1 所求决策变量数小于其他文献, 计算复杂度低于其他结果. 接下来验证时延影响下经济调度算法的最优性, 使用Lagrange乘子法可以获得分布式电力系统增量成本的最优值为18.63$/MWh. 首先验证固定时延的情况, 依据表3计算结果, 将安全传输方案造成的时延设定为所允许的最大值7 步.

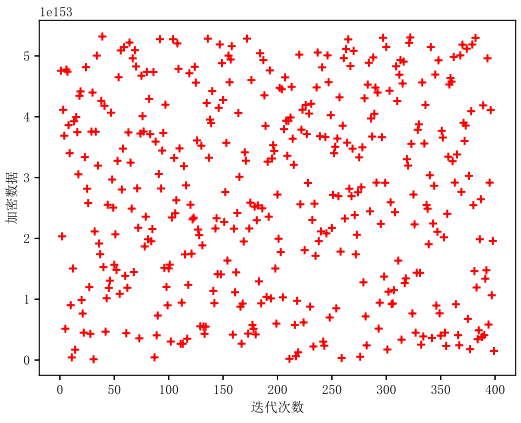

图 2　加密数据散点图

Fig. 2　Scatter Chart of Encrypted Data

我们使用Python中的Paillier库[30]进行加密仿真验证, 密钥长度设置为64 位, 在一台含2.39 GHz Intel Core i7-5500U和12.0 GB内存的笔记本电脑中, 测试了隐私保护方案的加密部分. 图2 给出了节点1增量成本负值的加密数据散点图, 可以看到数据经过加密后不再具有关联性, 因为加密随机数的存在, 相同的

明文经过加密以后也不同, 因此该方法具备良好的安全性.

图3和图4分别给出了$d(k)=7$时分布式电力系统的局部电力失配以及增量成本的变化轨迹图, m_i表示节点i的局部电力失配, IC_i表示增量成本. 从图3 中可以看到各节点的局部电力失配最终趋于0, 即满足了分布式电力系统所有的用电需求. 图4则显示了各节点的火力发电的增量成本最终实现了一致性, 收敛于18.63$/MWh.

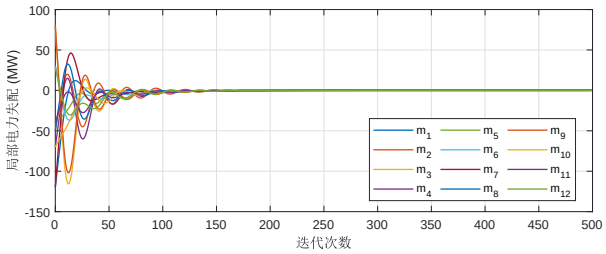

图 3 固定时延情况下局部电力失配变化图

Fig. 3 Local power mismatch change with fixed delay

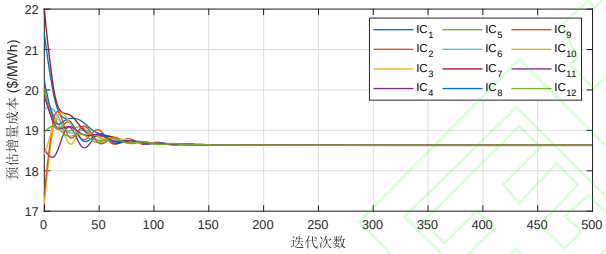

图 4 固定时延情况下增量成本变化图

Fig. 4 Incremental cost change with fixed delay

考 虑 时 变 时 延 的 情 况, 设置$d(k)=randi(7,1,1)$, 其中$randi(7,1,1)$ 函数可以产生1-7 之间的伪随机整数, m_i表示节点i的局部电力失配, IC_i表示增量成本.

图5展示了局部电力失配的变化, 图6为增量成本变化图, 可以看到在时变时延的影响下算法依然收敛到了最优值18.63$/MWh, 说明本文所提安全分布式经济调度方案可以实现增量成本的最优, 完成了发电成本最小化的目标.

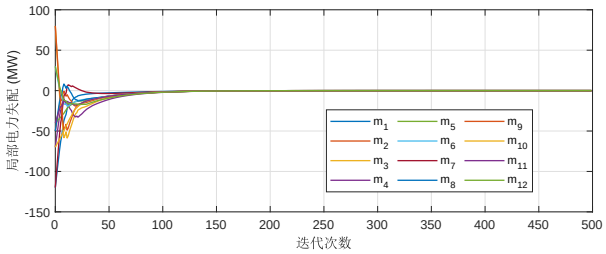

图 5 时变时延情况下局部电力失配变化图

Fig. 5 Local power mismatch change with time-varying delay

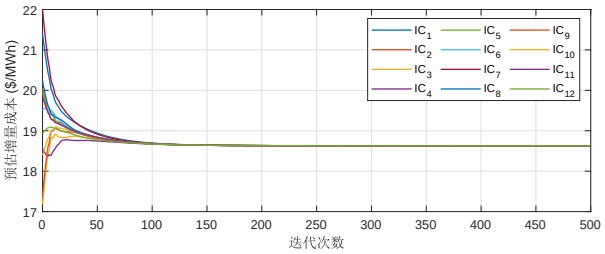

图 6 时变时延情况下增量成本变化图

Fig. 6 Incremental cost change with time-varying delay

最后考虑动态场景下的经济调度实现, 在迭代次数为1000时, 第3、4、6、9、10、12节点的光伏发电机组的电力输出分别减小20MW、30MW、20MW、20MW、30MW、20MW. 在迭代次数为2000时, 第1、2、6、7、8、12节点含有灵活负载需求分别增加80MW、10MW、40MW、80MW、10MW、40MW.

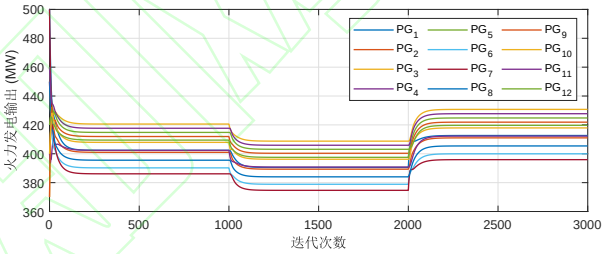

图 7 动态场景下火力发电机组电力变化图

Fig. 7 Thermal power generation output change under dynamic conditions

图7给出了火力发电机组的各节点输出的变化情况. 综上可得本文所提经济调度方案在动态场景下依然可行.

6 结论

本文针对含灵活负载与光伏发电的电力系统, 首先给出了基于一致性的经济调度算法, 然后围绕算法的信息交换制定了基于Paillier密码体制的隐私保护方案, 提高了节点的隐私性与传输信息的安全性. 进而将安全方案对经济调度的影响建模为时变时延, 基于Lyapunov稳定性理论导出了算法收敛的条件, 证明了所提算法可以在安全方案的保护下实现电力供需平衡, 并且收敛于优化问题的最优解. 最后, 本文仅通过数字仿真验证了所提出的经济调度算法的有效性与优越性.

参考文献:

[1] LI Y, ZHANG H, LIANG X, et al. Event-triggered-based distributed cooperative energy management for multienergy systems.*IEEE Transactions on Industrial Informatics*, 2019, 15(4): 2008 – 2022.

[2] HAN R, MENG L, GUERRERO J M, et al. Distributed nonlinear control with event-triggered communication to achieve current-sharing and voltage regulation in DC microgrids. *IEEE Transactions on Power Electronics*, 2018, 33: 6416 – 6433.

[3] WANG Z, WANG D, WEN C, et al. Push-based distributed economic dispatch in smart grids over time-varying unbalanced directed graphs. *IEEE Transactions on Smart Grid*, 2021, 12(4): 3185 – 3199.

[4] SUN Miaoping, JIANG Bo. Design of distributed power economic dispatch algorithm considering communication delay. *Control Theory & Applications*, 2020, 37(11): 2303 – 2311.
(孙妙平, 姜波. 考虑通信时滞的分布式电力经济调度算法设计. 控制理论与应用, 2020, 37(11): 2303 – 2311.)

[5] YIN L, SUN Z. Multi-layer distributed multi-objective consensus algorithm for multi-objective economic dispatch of large-scale multi-area interconnected power systems. *Applied Energy*, 2021, 300(Oct.15):117391.1 – 117391.17.

[6] LI Y, GAO D W, GAO W, et al. A distributed double-newton descent algorithm for cooperative energy management of multiple energy bodies in energy internet. *IEEE Transactions on Industrial Informatics*, 2021, 17(9): 5993 – 6003.

[7] LI H, WANG Z, CHEN G, et al. Distributed robust algorithm for economic dispatch in smart grids over general unbalanced directed networks. *IEEE Transactions on Industrial Informatics*, 2020, 16(7): 4322 – 4332.

[8] MA Kai, YU Yangqing, ZHU Shanying, et al. Distributed algorithm for economic dispatch based on gradient descent and consensus in power grid. *Sci Sin Inform*, 2018, 48(10): 1364 – 1380.
(马锴,于洋庆,朱善迎,等.基于梯度下降和一致性的电网分布式经济调度算法.中国科学:信息科学, 2018, 48(10): 1364 – 1380.)

[9] YANG Qingrun, LI Cheng, DING Tao, et al. Fully distributed dynamic economical dispatching method for power system based on alternating direction multiplier method. *Control Theory & Applications*, 2018, 35(5): 709 – 716.
(杨青润, 李澄, 丁涛, 等. 基于交替方向乘子法的电力系统完全分布式动态经济调度方法. 控制理论与应用, 2018, 35(5): 709 – 716)

[10] ZHAO C, CHEN J, HE J, et al. Privacy-preserving consensus-based energy management in smart grids. *IEEE Transactions on Signal Processing*, 2018, 66(23): 6162 – 6176.

[11] HE J, CAI L, ZHAO C, et al. Privacy preserving average consensus: Privacy analysis and algorithm design. *IEEE Transactions on Signal and Information Processing over Networks*, 2019, 5(1): 127 – 138.

[12] HUANG B, LI Y, ZHAN F, et al. A distributed robust economic dispatch strategy for integrated energy system considering cyber-attacks. *IEEE Transactions on Industrial Informatics*, 2022, 18(2): 880 – 890.

[13] YAN L, CHEN X, CHEN Y. A consensus-based privacy-preserving energy management strategy for microgrids with event-triggered scheme. *International Journal of Electrical Power and Energy Systems*, 2022, 141: 108198.

[14] AITZHAN N Z, SVETINOVIC D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, 2018, 15(5): 840 – 852.

[15] CHEN S, ZHANG L, YAN Z, et al. A distributed and robust security-constrained economic dispatch algorithm based on blockchain. *IEEE Transactions on Power Systems*, 2022, 37(1): 691 – 700.

[16] CHENG Zheyuan, YE Feng, CAO Xianghui, et al. A homomorphic encryption-based private collaborative distributed energy management system. *IEEE Transactions on Smart Grid*, 2021, 12(6): 5233 – 5243.

[17] LU Y, ZHU M. Privacy preserving distributed optimization using homomorphic encryption. *Automatica*, 2018, 96: 314 – 325.

[18] RUAN M, GAO H, WANG Y. Secure and privacy-preserving consensus. *IEEE Transactions on Automatic Control*, 2019, 64(10): 4035 – 4049.

[19] C. N. Hadjicostis, A. D. Domínguez-García. Privacy-Preserving distributed averaging via homomorphically encrypted ratio consensus. *IEEE Transactions on Automatic Control*, 2020, 65(9): 3887–3894.

[20] Fang W, M Zamani, Chen Z. Secure and privacy preserving consensus for second-order systems based on Paillier *encryption,Systems & Control Letters*. 2021, 148, 104869.

[21] Gao C, Wang Z, He X, Dong H. Encryption – decryption-based consensus control for multi-agent systems: Handling actuator faults, *Automatica*, 134,2021,109908.

[22] Gao C, Wang Z, He X, Dong H. Fault-Tolerant Consensus Control for Multiagent Systems: An Encryption-Decryption Scheme. *IEEE Transactions on Automatic Control*, 2022, 67(5):2560-2567.

[23] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes. *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques*. Prague, Czech Republic, 1999: 223 – 238.

[24] LI J, YE Y, PAPADASKALOPOULOS Dimitrios, et al. Distributed consensus-based coordination of flexible demand and energy storage resources. *IEEE Transactions on Power Systems*, 2021, 36(4): 3053 – 3069.

[25] Wei M, Wang W. Safety can be dangerous: secure communications impair smart grid stability under emergencies. *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA: IEEE, 2015, 1 – 6.

[26] LIANG Yao, FENG Dongqin, XU Shanshan, et al. Feasibility analysis of encrypted transmission on security of industrial control systems. *Acta Automatica Sinica*, 2018, 44(3): 434 – 442.
(梁耀,冯冬芹,徐珊珊,等.加密传输在工控系统安全中的可行性研究.自动化学报, 2018, 44(3): 434 – 442.)

[27] CHEN J, XU S, MA Q, et al. Two novel general summation inequalities to discrete-time systems with time-varying delay. *Journal of the Franklin Institute*, 2017, 354(13): 5537 – 5558.

[28] PARK P, KO J W, JEONG C. Reciprocally convex approach to stability of systems with time-varying delays. *Automatica*, 2011, 47(1): 235 – 238.

[29] NAM P T, TRINH H, PATHIRANA P N. Discrete inequalities based on multiple auxiliary functions and their applications to stability analysis of time-delay systems. *Journal of the Franklin Institute*, 2015, 352: 5810 – 5831.

[30] https://python-paillier.readthedocs.io/en/latest/usage.html

作者简介:

杨飞生 博士, 副教授, 博士生导师, 目前主要研究方向为网络化控制与分布式优化、电力系统与无人系统、信息物理系统控制与安全等, E-mail: yangfeisheng@nwpu.edu.cn;

刘佳明 硕士研究生, 目前主要研究方向为电力系统分布式优化、事件触发机制、隐私保护, E-mail: npuljm@mail.nwpu.edu.cn;

丁瑞森 硕士研究生, 目前主要研究方向为电力系统的负荷频率控制、事件触发控制、数据的加密传输, E-mail: ruisending@mail.nwpu.edu.cn;

姬毓明 硕士研究生, 目前主要研究方向为电力系统经济调度、隐私保护, E-mail: jiyuming@mail.nwpu.edu.cn;

潘 泉 博士, 教授, 博士生导师, 目前主要研究方向为信息融合理论及应用、工业控制系统信息安全、商业密码应用与和现代保密技术, E-mail: quanpan@nwpu.edu.cn.