文章编号：2096-5125 (2020) 06-0552-08 中图分类号：TM73；TP309 文献标志码：A
DOI：10.19705/j.cnki.issn2096-5125.2020.06.002

信息能源系统的边缘节点可信评估及控制策略

任汝飞，胡旌伟，孙秋野 *
（东北大学信息科学与工程学院，辽宁省 沈阳市 110819）

Edge-node Reliability Assessment and Control Strategy in Cyber Energy Systems

REN Rufei, HU Jingwei, SUN Qiuye*
(College of Information Science and Engineering, Northeastern University, Shenyang 110819, Liaoning Province, China)

Abstract: With the continuous development of distributed computing technologies, the energy industry is demonstrating a tendency to adopt multi-integration of energy Internet. Although distributed computing can help overcome the disadvantages of traditional centralized-computing network congestion and low computing capacity, it is inefficient from the viewpoint of privacy protection and edge-device reliability. Based on energy Internet and edge-device characteristics, a cyber energy edge service system (CEESS) is presented in this paper. The main features of CEESS include edge computing, distributed control, and availability of an intelligent terminal. CEESS facilitates the storage and safe transmission of edge information while guaranteeing the network-information flux. Reliability-perception strategies pertaining to the edge equipment and energy are proposed in the zero-trust model. Finally, based on the edge-service system, this paper proposes event-triggering edge control under reliability as well as a node-self-healing method in the event of a network collapse. This guarantees the safe operation of equipment as well as reliability control of cyber energy systems.

Keywords: cyber energy system; edge calculation; privacy protection; safety assessment; reliability control

摘 要：能源行业新兴分布式技术不断发展，分布式计算虽然能弥补传统集中式计算网络拥堵、计算能力低的缺点，但对边缘设备隐私安全和可信感知存在不足。首先根据能源互联网和边缘设备特性，依托边缘计算、分布式控制和智能终端建立了信息能源边缘服务系统（cyber energy edge service system, CEESS），保证网络信息流通量的同时，实现了边缘信息存储和安全传输。在零信任模型下，针对边缘设备和能源信息分别提出相应的信任感知策略。最后提出数据可信下的事件触发边缘控制，以及网络崩溃情况下的节点自愈方法，保障了信息能源系统的设备安全运行和可信性控制。

关键词：信息能源系统；边缘计算；隐私保护；安全评估；可信控制

0 引言

随着新基建及能源互联网的发展，利用信息技术满足能源高效运行的需求日益增长[1-2]。信息能源系统（cyber energy system，CES）是能源互联网发展的新阶段和应用的新形态，隶属于信息物理系统（cyber physical systems，CPS），更注重能源信息的调控与处理。CES深度耦合信息网与能源网，可有效提升基础能源网络的区域协调性、控制实时性与边缘协同性，满足能源用户产销快速转换的多元化市场需求[3-6]。

中国工程院院士柴天佑教授指出，针对信息物理系统的分布式协同优化理论和应用已经成为当代控制科学与工程的重要发展方向之一[7]；美国国家工程院院士G. T. Heydt教授也发文指出“如何将这些控制作为协同智能体在智能能源管理中的多个微处理器上进行划分和分配是关键的挑战”[8]。以云计算为核心的大数据处理系统计算能力低、必要网络带宽大、延时严重，且传统分布式控制存在边缘设备隐私安全性低、数据传输能耗大、通信节点故障率高等缺点[9]，已无法满足边缘设备的需求。

在云端大数据处理难以保证海量信息和边缘设备隐私安全的情况下，提升CES边缘数据降维后的安全感知和数据信任下的控制策略尤为重要[10]。为避免海量数据中的无关信息泛滥影响安全感知和系统控制，

基金项目：国家重点研发计划项目（2018YFA0702200）；国家自然科学基金重点项目（61433004）；国家自然科学基金（61573094）。

National Key Research and Development Program of China (2018YFA0702200); Key Program of National Natural Science Foundation of China (61433004); National Natural Science Foundation of China (61573094).

可利用最小误差极大极小概率[11]、基于互信息的双向选择算法[12]、K临近图加权线性叠加[13]等方式进行数据降维，也可利用构建径向基神经网络[14]、不完备信息的动态神经网络[15]、半监督学习[16]等人工智能方法对不完备信息分类感知。随着隐私保护意识的逐渐提升，零信任模型[17]和可信计算[18]得到了发展，保证在任何情况下的数据都是不受信任的，仅在得到特定的可信授权情况下，数据才可使用[19]。在网络攻击和节点随机损坏的情况下，将差异隐私概念带入多智能体系统[20]，或使用弹性共识一致性策略[21]，保证了网络的收敛和鲁棒性。

本文从边缘节点出发，首先构建了信息能源边缘服务系统（cyber energy edge service system, CEESS），第2章研究了边缘节点的隐私保护和数据降维策略，第3章提出零信任模型下的可信感知，为信息网络的安全隐私保护提供新的解决方法。最后在受信情况下，提出信息网络的可信事件触发边缘控制，以及能源网络瘫痪后的边缘节点自愈控制。

1　信息能源边缘服务系统

CES通过大量的智能节点实现分布式控制、区域协同、资源调配等多元数字化策略，但产能侧、网侧、负荷侧的参数和运行信息都会发送至云端服务器，考虑到仅有少量必需信息参与调度和控制，大量数据流通给计算中心带来沉重负担，同时考虑通信堵塞带来的时滞、丢包，甚至网络攻击，海量边缘信息会对CES带来极大的信息网络冲击[22-23]。

边缘计算可以利用网络边缘的原始数据执行模型计算，实现信息网络的数据降维、隐私保护、调度控制以及能源网络崩溃时的自愈控制。本文提出的CEESS框架如图1所示。系统依托边缘计算、分布式控制和智能终端的模型把控，以智能通信设备的形式对各个负荷、能源路由器和基础产能的核心器件设置边缘节点，将终端设备的存储、计算等任务迁移至边缘节点，例如产能设备、基站、无线接入点、负载设备等。同时以通信服务器的形式建立边缘终端，作为边缘节点和云端服务器的中间节点，在统筹底层边缘节点控制策略的同时，也可作为边云协同的中转控制器，加强网络的稳定性和安全性。

边缘服务框架的基础在于边缘的划分。对于单一边缘节点，细化到每台核心设备都有智能数据处理的功能，通过自身算法或终端下派控制模型，自主筛选必要信息，极大程度包含设备原始数据。对于能源网络，可按源–储–网–荷分别划分，每级均包括所有内部组织的所有节点，形成边缘节点族群，在保证族群信息归纳和交互的同时，实现边缘对端内进行纵向电–热–气能源互补，横向隐私保护和数据降维，形成

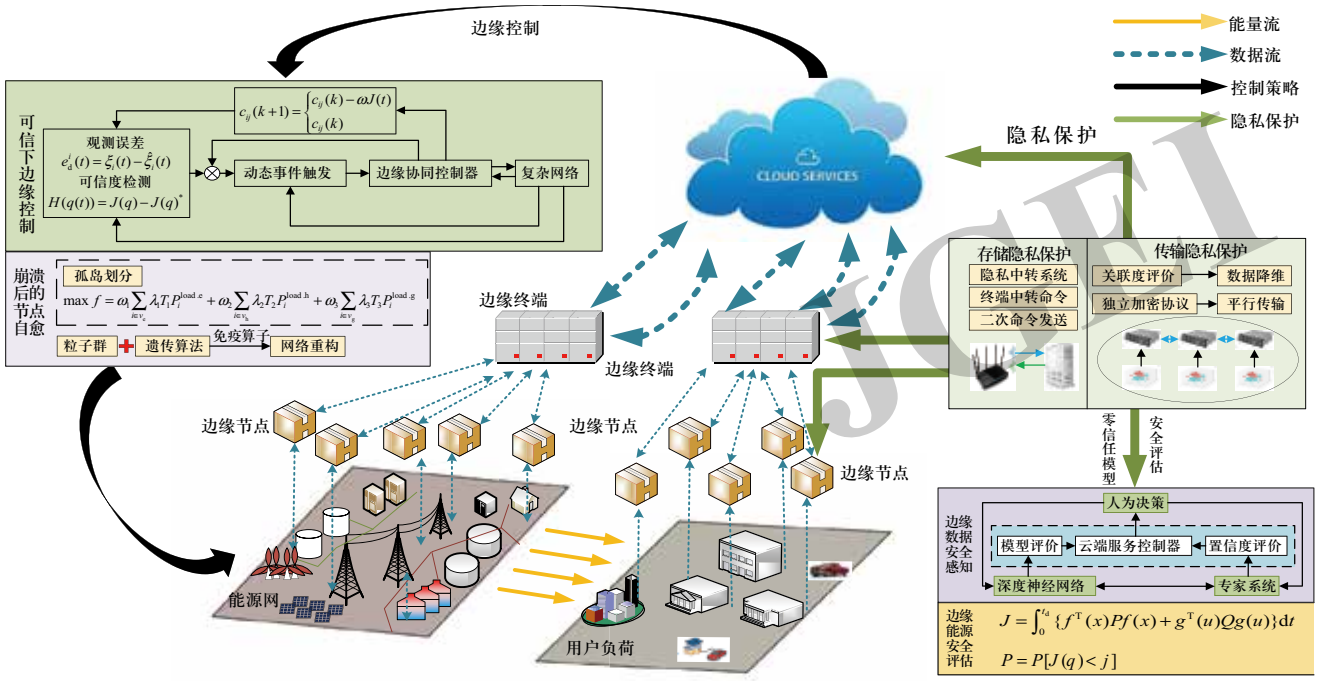

图 1　信息能源边缘服务系统运行框架图

Fig. 1　Operating frame of CEESS (cyber energy edge service system)

按需调整的边缘节点动态划分。各级边缘节点不仅存在物理上的拓扑关系，还具备相互之间的信息通信，将传统复杂系统集中调控的辨识、感知、控制、优化等大部分功能转移到边缘终端，借助物理和通信网络，通过边缘、边边、云边等多级控制协同，保证复杂系统的自适应安全、高效运行。

大量的边缘设备原始数据就地存储，仅将对系统有帮助的控制、优化、交易等必要信息上传，随着数据维度降低，其准确性和可靠性也受到了影响，上层边缘节点或云端服务器则通过零信任模型决策、高信息密度测量数据和可解释知识模型联合互补，实现高效的多维数据安全边缘感知。本文分析了边缘信息的隐私安全保护策略，对存储类信息实时保护，对传输类信息进行数据降维和中转传输，可在边缘数据量指数增长的情况下，使系统有能力抵抗节点损坏和网络攻击造成的扰动。一旦确定边缘节点受到攻击或信息安全性降低，则系统实施多阶段运行警戒策略，通过分析边缘扰动对网络状态的影响，实现故障隔离与网络重构，以及边缘节点的自我感知、诊断、决策和恢复。

在实现节点实时、快速数据分析与本地决策，边缘信息降维和数据安全感知的基础上，可进行边边安全博弈和云边协同控制，更好提升终端业务处理能力。边边安全博弈可解决节点计算的资源需求与边缘设备资源受限之间的矛盾，平衡信息质量和隐私保护，也可将云端计算负担分摊至边缘设备，实现对延迟敏感设备的协同处理。而云边协同不仅可实现多智能体一致性控制，云端也可将机器学习的任务模型按需分配至边缘节点，实现“就地采集、就地学习”，保证学习模型的适用范围与准确度。

根据云边节点的联通属性，存在2种协同模式。①云导向的边云协同。边缘节点主要负责收集数据，将关键信息上传至云端服务器，云端服务器接收到数据后并不会统一计算最终控制结果，根据数据分析，设计、训练和更新控制模型，将中间结果发送至边缘节点，由边缘节点计算最终值。该方法可重新调配云端与边端的计算量与管理权限。②边缘导向的协同。在此模式中，云端只负责将数据反馈分析，更新系统控制模型，边端实时更新控制模型的同时，自行调配控制参数。

2 边缘信息隐私安全

边缘节点的产用能数据、运行数据与用户和企业的工作生产情况密切相关，若这些信息遭到泄露会带来重大的安全隐患。在智能电网系统中，大多隐私保护采用数据掩蔽和噪声添加等匿名化方法[24]，首先将用户标识信息删除，然后添加不改变信息完整性的用户身份K-Anonymity，但K-Anonymity易遭受同质攻击及背景攻击。或使用基于缩放扰动数据掩蔽的隐私保护方案[25]，在一定的采集周期里，生成一个均匀分布的随机数作为噪声干扰，但噪声易被主成分分析等方法去除，难以用于保护隐私。

在CEESS的信息网络隐私保护中，主要由边缘设备、边缘节点、边缘终端和云端服务器构成。基于边缘节点的数据交换方式和隐私数据类型，可将隐私数据分为2类：存储类隐私数据和传输类隐私数据。

2.1 存储类隐私保护

存储类隐私数据一般指节点间或与终端通信之后产生的历史记录，以及节点内部存储的原始数据和计算策略。

这类隐私数据的安全保护，主要针对边缘节点存储数据的存储权、更改权和传输权的把控。这类数据包含大量的设备生产运行原始数据、通信和计算协议，一旦被任意盗取，易造成设备运行信息丢失或分布式计算故障。边缘终端作为设备必要信息的传输者和网络安全的监测者，把控云端服务器发出的上传请求，同时对云端服务器下载的命令文件进行安全监测，从而降低节点数据被暴露的风险。本文提出在边缘终端系统中建立一套隐私数据中转系统，如图2所示，当云端服务器向边缘节点发起数据调用时，首先通过边缘终端进行命令中转，之后向节点发送二次调用命令，才允许将边缘节点的原始数据调用至云端

图 2 存储类隐私数据保护示意图

Fig. 2 Schematic diagram of privacy data protection in terms of storage

服务器；当边缘节点发起云数据下载需求时，也需边缘终端的中转接收和下载允许，才可以实现数据传输。

边缘节点和边缘终端均分担了一部分云端服务器的绝对权限，确保云端无法直接调取边缘设备信息，边缘设备也无法随意发送信息或下载模型，降低了隐私数据被盗取和篡改的风险。

2.2　传输类隐私保护

传输类隐私数据一般指边缘节点与边缘终端通信过程中产生的隐私数据，例如节点向终端发送的生产必需信息，终端下派边缘节点的分布式控制模型等。

为了减少数据传输量，减轻网络通信负担，边缘节点必然起到数据降维的作用，如图3所示。首先将云端服务器初步筛选的数据按照来源及关联度准则分发至各个边缘节点，在边缘节点侧根据已有的数据类型及数量，利用主成分分析、独立成分分析投影寻踪等方法对线性数据降维；利用核方法、多维尺度、等距离映射等方法对非线性数据降维。最终选出函数值高的数据作为关键数据，在保留原始数据重要特征的前提下，实现数据可解释降维[26]。

传统通信方式是将数据发送至上层通信网络（信号基站），再由上层网络传输至指定设备。而边缘服务框架可利用节点设备搭建的局域通信网络，利用边缘节点的智能性、可控性，使同一网络下的终端设备

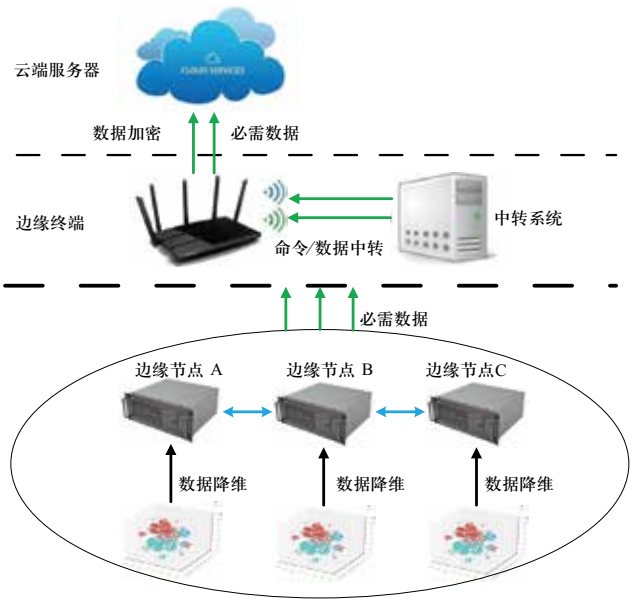

图 3　传输类隐私数据保护示意图

Fig. 3　Schematic diagram of privacy data protection in terms of transmission

IP与边缘设备点对点连接，与自主选择的目标形成私密连接。数据不再通过上层通信网络转发，只在边缘设备之间平行传输。在边缘节点与边缘终端、或与云服务器的交互中，可也利用节点的独立性创建设备独立加密协议，即使在设备遭受信息攻击时，也可将损失降到最小。利用点对点通信和设备独立加密协议，缓解了云端服务器的通信压力，保证了传输类隐私数据的信息安全。

3　边缘节点信任策略

信息能源网络中海量数据涌现，考虑边缘网络可能存在数据攻击/混淆和边缘节点信息失真的非完全可信环境，如何设计边缘信息信任检测策略，有效避免数据丢失、系统入侵、网络攻击，达到消除网络/边缘节点信息失真隐患的目的，实现异常征兆下系统安全可信运行成为了边缘服务系统参与CES协同控制的核心问题。

在CES中，一旦边缘节点的信息网络受到攻击，其检测和表现形式均为通信数据故障。本章首先建立零信任系统框架模型，默认一切数据均是不可信、不可用的；其次，在该框架下研究边缘通信数据信任感知和能源数据的可信评估。

3.1　零信任模型

边缘节点实施了设备隐私安全保护和边缘信息降维，仅将系统的控制、优化、交易等必需信息上传，边缘终端或云端服务器无法接收底层原始数据，使信息检验和事后追溯变得异常困难。

零信任安全模型由John Forrester在2010年首次提出[27]，其基于设备状态评估和用户信息认证，集成持续分析和信任检测功能，以确保网络没有受到入侵和攻击。其框架主要概括为：网络安全不依赖于属性划分；所有设备、用户、节点、网络均享受认证和权限；访问和更改控制策略应动态调用全局设备和信息进行计算评估。

CES的零信任安全防护系统如图4所示，可从边缘节点安全服务、边缘终端管理、动态权限管理、统一身份认证4个方面建立。与传统静态访问的控制规则不同，防护系统持续监测访问设备的身份安全，按需求动态调整权限制度和访问规则。这种安全管理模式在受控的前提下，满足主动性与动态性，降低控制终端权限，增大了网络融合度。

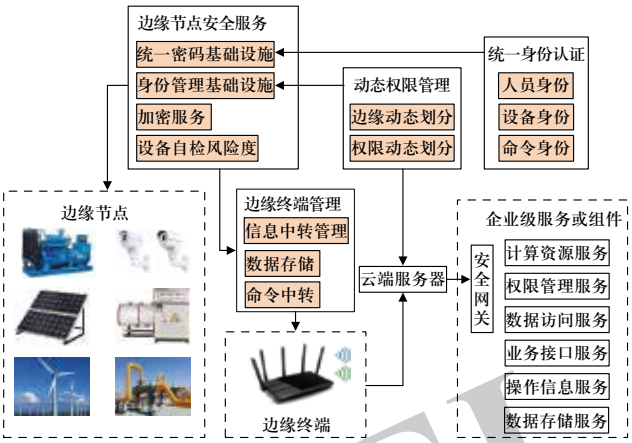

图 4 零信任安全防护系统

Fig. 4 Zero trust security protection system

3.2 边缘通信信任感知

多维边缘信任感知的主要目的是寻找CES在一个特定多维参数空间中所有安全运行点的集合并计算其边界，是实现系统可信运行的基础。依托高信息密度量测数据和可解释知识模型联合互补信息分析，通过扰动评估和工况特征辨识，探明安全域的几何学和动力学性质，并研究多维安全域的在线计算与近似方法，为实现可信运行和智能运维提供支撑。

随着人工智能和机器学习的发展，多维数据计算和运行状态感知得到了极大提升。在CEESS中，边缘节点引入智能优化算法和长短时记忆单元，首先确立边缘数据的安全域，考虑扰动变量在不同测度下，如欧氏距离、相对率、信息熵和信息贡献度等，其表现形式和呈现度均不同。根据系统动态阈值的自适应选择算法实现不同尺度下扰动向量的精确提取与度量。根据概率性能指标及工业控制系统实际需要，定义概率的扰动估计误差性能指标。

云端服务器构建交叉熵的损失函数，可采用多任务联合训练的方法，实现深度网络训练。建立三级安全裕度综合评价方法，如图5所示，对深度学习、专家系统和人为决策的结果，进行分等级安全裕度评价。由于云端服务控制器存在大量人机交互操作，在关键问题处理上，可基于人在运行过程中的操作，增加柔性逻辑推理和规则之间的相容性和关联性分析，利用决策反馈的方式优化专家规则库和深度神经网络。基于工况变化产生的新数据，研究参数更新方法，并基于历史数据和新数据，采用自适应滤波等技术研究参数的在线更新方法，实现深度神经网络的在线增强和参数的实时递归更新。

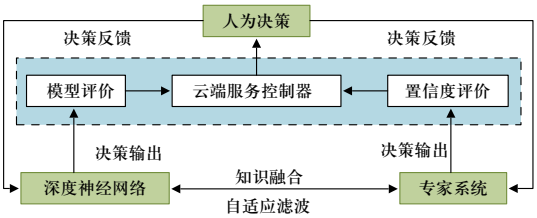

图 5 边缘数据信任感知过程

Fig. 5 Edge data trust perception process

3.3 能源数据信任评估

当CES的能源控制器故障或该控制器的边缘节点受到信息网络攻击时，均可认为该节点是不受信任的。结合边缘控制特征，CES边缘节点的被控状态x所采取的边缘控制器u，其二次型的表征形式能更好地与系统能量函数结合，以分析系统的稳定性能。可针对能源网络构建可信的二次性能指标：

$$J=\int_0^{t_d}\{f^{\mathrm{T}}(x)Pf(x)+g^{\mathrm{T}}(u)Qg(u)\}\mathrm{d}t \tag{1}$$

式中：$f(x)$、$g(u)$分别表示x和u的相关函数；t_d为控制器施加时系统达到稳定的时间；P和Q均为正定的加权矩阵，通过能量函数的方法，定性分析节点控制系统的渐进稳定性和可信性。以分布式能源系统为例，$f(x)$需要涵盖电压、频率、压强、温度等重要信息，$g(u)$需要涵盖各节点的控制器形式及设备可信情况，冗余控制量即为每个节点所能承受的最大负荷量。

设$G(q)$为节点控制系统，q为系统$G(q)$的数据参数向量且在给定参数域中有界；控制系统的可信二次性能指标为$J(q)$；对于可信水平j，$J(q)<j$时该节点的能量控制器是可信的。使用蒙特卡洛方法依照q的概率密度$f(q)$对参数向量q进行N次抽样；仿真生成N组性能指标$J(q)$*；绘制$J(q)$*的累计频率曲线并计算统计量；给定系统的可信水平j，对应累计频率曲线上的点即为可信性能可接受概率$P[J(q)\leqslant j]$的估计值，计算样本可接受概率均值μ和样本标准差S。将样本均值μ作为节点的可信度输出，即可实现对边缘节点数据的实时可信性评估。

4 信任下的边缘控制

4.1 数据可信下的事件触发边缘控制

CEESS中存在大量低成本、高性能、高度互联的边缘节点，系统控制设计方法从集中式转变为分布式，再到边缘式的过程中，边缘节点无法避免地可能出现故障或受到攻击。在控制理论中将边缘节点和边

缘终端均看作一个多智能体，采用基于可信度的事件触发边缘控制策略，可动态调整每一个节点的动作权重。将周期性的可信度检测纳入系统事件触发控制结构，若发现某一节点存在故障或可疑，按信任度调整信息网络中该边缘节点信息流的动作权重，逐渐降低该智能终端数据对整体通信网络的影响，从而逐渐隔离该节点。其控制策略设计如下：

1）基于图论定义的$G=(V, E, A)$加权有向图，$A=[a_{ij}]$为图G的邻接矩阵，建立半正定的拉普拉斯矩阵$L=[L_{ij}]\in \mathrm{R}^{N\times N}$，定义当$i\neq j$时，$l_{ij}=-a_{ij}$；当$i=j$时，$l_{ii}=\sum_{i\neq j}a_{ij}$。

2）定义观测误差$e_{\mathrm{d}}^{i}(t)=\xi_i(t)-\hat{\xi}_i(t)$，根据二次可信性能指标$J(q)$建立可信度触发器

$$H(q(t))=J(q)-J(q)^{*} \tag{2}$$

式中：$J(q)^{*}$为标准二次性能指标；$H(q(t))$为可信阈值，当$H(q(t))<0$时，认为该节点是不可信的。将周期性的信任性能指标触发嵌入事件触发协议中，调整触发时间

$$t_{k+1}^{i}=\max(t_k^i, t_{k+1}^{i\,*}, t_{\mathrm{h}}) \tag{3}$$

式中：t_{h}为设备可信情况低于标准可信度的时刻；$t_{k+1}^{i\,*}$为事件触发通信时刻。

3）对每一个边缘节点建立本地可信权重控制器$c_{ij}(k)$，设置初始值$c_{ij}(0)$后，定义可信权重控制器的更新法则

$$c_{ij}(k+1)=\begin{cases}c_{ij}(k)-\omega\mu & \text{if } j \text{ is suspicious}\\ c_{ij}(k) & \text{otherwise}\end{cases} \tag{4}$$

式中：ω为可信增益；μ为t时刻的节点二次性能指标$J(t)$的概率均值，即该时刻数据的可信度。重新计算邻接矩阵，调整不可信节点权重，逐渐将其边缘化：

$$a_{ij}(k)=\frac{[c_{ij}(k)]_{\bar{c}_{ij}}^{+}}{\sum_{l\in N_i^-}[c_{ij}(k)]_{\bar{c}_{ij}}^{+}} \tag{5}$$

式中：$\bar{c}_{ij}$为$c_{ij}(k)$的最低可信阈值。随着节点在系统中的权重逐渐降低，其所起的控制作用也越来越小，一旦超过最低可信阈值，则彻底切除该节点。公式$[x]_y^{+}$的计算方法如下：

$$[x]_y^{+}=\begin{cases}x & \text{if } x\geqslant y\\ 0 & \text{otherwise}\end{cases} \tag{6}$$

4）引入系统的动态变量，通过嵌入系统状态变量的动态特征以降低系统的通信带宽和控制器更新频率，实现系统在可信度下的事件触发边缘控制。

4.2　能源网络崩溃下的边缘节点自愈控制

边缘设备具有严重的分散性、间歇性等特点，一旦能源网络受到极大破坏，网络稳定下的控制策略将无法保证收敛，需及时实施边缘节点自愈控制。自愈控制的原则是在保证供能可靠性的前提下，将损失降至最低，并尽快消除运行故障，可以使用网络重构与计划孤岛相结合的故障恢复方法，通过融合孤岛方案匹配、恢复网络连通与边缘节点并网、网络重构以及切除节点寻优这4个阶段，实现配电网孤岛划分与网络重构恢复相结合。

4.2.1　孤岛划分

孤岛划分运行是当CES发生故障后，通过最大化网络功能，可仅对关键边缘节点实施隔离保护，避免因关键节点暂态振荡引起的网络二次故障。网络故障时，不同等级的负荷造成的损失不同，首先将负荷根据电源运行条件、功率供需平衡、可控负荷比例等约束划分等级。

$$\begin{aligned}\max f=&\omega_1\sum_{i\in v_{\mathrm{e}}}\lambda_1T_1P_i^{\mathrm{load.e}}+\\ &\omega_2\sum_{i\in v_{\mathrm{h}}}\lambda_2T_2P_i^{\mathrm{load.h}}+\omega_3\sum_{i\in v_{\mathrm{g}}}\lambda_3T_3P_i^{\mathrm{load.g}}\end{aligned} \tag{7}$$

式中：ω_1、ω_2、ω_3为负荷权重；λ_1、λ_2、λ_3为节点功率恢复比例；T_1、T_2、T_3为不同能源节点的脆弱度；$P_i^{\mathrm{load.e}}$、$P_i^{\mathrm{load.h}}$、$P_i^{\mathrm{load.g}}$分别为电负荷、热负荷、气负荷的功率。

其次，采用领地竞争互斥萤火虫优化算法，将所有节点归类为萤火虫集合W，将低等级负荷节点归为雄性集合$X=\{X_i\}_{i=1}^{M}$，高等级负荷节点归为雌性集合$Y=\{Y_i\}_{i=1}^{N}$。在雌雄相互吸引的过程中，保证每个群体都有雌性节点，以保证网络整体的安全运行。建立萤火虫之间的吸引力β：

$$\beta(X_m,Y_n)=\beta_0\mathrm{e}^{-\gamma\times r_{mn}} \tag{8}$$

迭代萤火虫种群的位置：

$$X_m(t)=X_m(t-1)+\beta(X_m(t-1)-Y_n(t-1))+\alpha \tag{9}$$

孤岛划分为0-1规则问题，且萤火虫（节点）位置无法真实移动，所以利用Sigmoid函数对萤火虫位移归一化，解出某一节点划分入某一孤岛的概率S。

$$S(v_{ki}(t))=\frac{1}{1+\mathrm{e}^{-v_{ki}(t)}} \tag{10}$$

式中：$v_{ki}(t)$为t时刻该萤火虫个体在解空间中的位移量。

4.2.2 网络重构

能源系统网络重构技术由Merlin在20世纪70年代提出，目前已在配电网领域趋向成熟，主要分为运行优化重构和供电恢复重构两方面。运行优化重构通过馈线和变电站之间的负荷转移，寻求最佳的网络结构；供电恢复重构是当相邻节点中断时，通过分段开关隔离故障线路，为非故障点寻求新的供电线路。

能源系统网络重构属于混合整数非线性规划问题，存在NP难问题。已有传统优化方法涵盖数学优化理论、最优潮流求解、数理统计等，目前遗传算法和粒子群等人工智能方法也体现出了巨大优势。

遗传算法处理网络重构问题易陷入早熟收敛，可在基因中加入免疫选择算子来提升种群多样性，有利于后续优良基因提取，提升重构搜索效率。

4.2.3 网络自愈

CES的网络自愈流程大体与传统电网自愈流程类似，边缘计算提高了网络数据计算速度，扩大了节点覆盖范围，更有利于实现网络自愈。主要分为以下几个步骤。

1）确定非故障失电区域的恢复方式，若不能通过网络重构恢复但可以通过计划孤岛恢复，则生成故障运行方案，进入计划孤岛恢复过程。若可以网络重构，则通过恢复网络连通与分布式电源并网、网络重构以及切负荷寻优3个阶段实现故障恢复。

2）若使用孤岛划分策略，首先确定孤岛形成过程中分布式电源与负荷的动作序列，根据CES运行状态，辨识出对系统稳定性具有较大影响的边缘节点或边缘终端，重点监测的同时也可为剩余节点提供暂态特征依据。

3）考虑节点的重要性和能源类型，可依据能源容量和负载位置进行孤岛划分，也可依据边缘节点类型，直接对节点上层的边缘终端划分。

4）划分后，孤岛内部的正常边缘节点和故障节点可视为一种多能微网。根据微网内分布式能源配置，选定主能源路由器，保证对微网内的电、热、气、信的稳态控制，再由内部边缘终端进一步校验故障节点位置与故障恢复。

5 总结与展望

本文提出基于智能通信设备的CEESS框架，将大量集中式计算任务分散至边缘侧，利用边缘信息隐私保护方法和节点信任策略，为解决CES边缘数据海量剧增和信息网络攻击提供了新思路。利用边缘计算的特点，引入信任下的边缘控制方法，为系统的安全高效运行提供了新的解决方案。

CES自身的多能源融合、能信耦合、用户身份多频转换等需求，导致信息能源系统在耦合信息网络与能源网络过程中存在多目标冲突与约束、多元指标差异等系统机理问题。未来可研究具体的边缘控制算法，进一步增强数据可信下的系统边缘控制策略，提升基础能源网络的区域协调性、控制实时性与边缘协同性，满足能源用户产销定位快速转换的多元化市场需求。

参考文献

[1] 刘艳红，黄雪涛，石博涵. 中国“新基建”：概念、现状与问题[J]. 北京工业大学学报（社会科学版），2020，20(6)：1-12.
LIU Yanhong, HUANG Xuetao, SHI Bohan. China’s new infrastructure construction: concepts, current situations and problems[J]. Journal of Beijing University of Technology (Social Sciences Edition), 2020, 20(6): 1-12(in Chinese).

[2] 沈沉，贾孟硕，陈颖，等. 能源互联网数字孪生及其应用[J]. 全球能源互联网，2020，3(1)：1-13.
SHEN Chen, JIA Mengshuo, CHEN Ying, et al. Digital twin of the energy Internet and its application[J]. Journal of Global Energy Interconnection, 2020, 3(1): 1-13(in Chinese).

[3] 连祥龙，张文浩，钱瞳，等. 考虑信息节点失效的电力信息物理系统脆弱性评估方法[J]. 全球能源互联网，2019，2(6)：523-529.
LIAN Xianglong, ZHANG Wenhao, QIAN Tong, et al. Vulnerability assessment of cyber physical power system considering cyber nodes failure[J]. Journal of Global Energy Interconnection, 2019, 2(6): 523-529(in Chinese).

[4] 贾宏杰，王丹，徐宪东，等. 区域综合能源系统若干问题研究[J]. 电力系统自动化，2015，39(7)：198-207.
JIA Hongjie, WANG Dan, XU Xiandong, et al. Research on some key problems related to integrated energy systems[J]. Automation of Electric Power Systems, 2015, 39(7): 198-207(in Chinese).

[5] 孙秋野，胡旌伟，张化光. 能源互联网中自能源的建模与应用[J]. 中国科学：信息科学，2018，48(10)：1409-1429.
SUN Qiuye, HU Jingwei, ZHANG Huaguang. Modeling and application of we-energy in energy Internet[J]. Scientia Sinica (Informationis), 2018, 48(10): 1409-1429(in Chinese).

[6] 胡杰，孙秋野，胡旌伟，等. 信息能源系统自–互–群立体协同优化方法[J]. 全球能源互联网，2019，2(5)：457-465.
HU Jie, SUN Qiuye, HU Jingwei, et al. Three-dimensional self-mutual-group collaborative optimization method for Information-energy systems[J]. Journal of Global Energy Interconnection, 2019, 2(5): 457-465(in Chinese).

[7] 杨涛，柴天佑.分布式协同优化的研究现状与展望[J/OL]. 中国科学：技术科学：1-12[2020-10-13].http://kns.cnki.net/kcms/detail/11.5844.TH.20200424.1730.002.html.

[8] HUANG A Q, CROW M L, HEYDT G T, et al. The future renewable electric energy delivery and management (FREEDM) system: the energy Internet[J]. Proceedings of the

IEEE, 2011, 99(1): 133-148.

[9] 施巍松，孙辉，曹杰，等. 边缘计算：万物互联时代新型计算模型[J]. 计算机研究与发展，2017，54(5)：907-924.
SHI Weisong, SUN Hui, CAO Jie, et al. Edge computing: an emerging computing model for the Internet of everything era[J]. Journal of Computer Research and Development, 2017, 54(5): 907-924(in Chinese).

[10] 张佳乐，赵彦超，陈兵，等. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报，2018，39(3)：1-21.
ZHANG Jiale, ZHAO Yanchao, CHEN Bing, et al. Survey on data security and privacy-preserving for the research of edge computing[J]. Journal on Communications, 2018, 39(3): 1-21(in Chinese).

[11] SONG S J, GONG Y S, ZHANG Y L, et al. Dimension reduction by minimum error minimax probability machine[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2017, 47(1): 58-69.

[12] 赵彦涛，单泽宇，常跃进，等. 基于MI-LSSVM的水泥生料细度软测量建模[J]. 仪器仪表学报，2017，38(2)：487-496.
ZHAO Yantao, SHAN Zeyu, CHANG Yuejin, et al. Soft sensor modeling for cement fineness based on least squares support vector machine and mutual information[J]. Chinese Journal of Scientific Instrument, 2017, 38(2): 487-496(in Chinese).

[13] 王君言，张春梅，张云斌，等. 基于DL1图和KNN图叠加图的高光谱图像半监督分类算法[J]. 中国科学：信息科学，2017，47(12)：1662-1673.
WANG Junyan, ZHANG Chunmei, ZHANG Yunbin, et al. Semi-supervised classification algorithm of hyperspectral image based on DL1 graph and KNN superposition graph[J]. Scientia Sinica (Informationis), 2017, 47(12): 1662-1673(in Chinese).

[14] 安剑奇，彭凯，曹卫华，等. 基于动态神经网络的高炉炉壁不完备温度检测信息软测量方法[J]. 化工学报，2016，67(3)：903-911.
AN Jianqi, PENG Kai, CAO Weihua, et al. A soft-sensing method for missing temperature information based on dynamic neural network on BF wall[J]. CIESC Journal, 2016, 67(3): 903-911(in Chinese).

[15] 蒙西，乔俊飞，韩红桂. 基于类脑模块化神经网络的污水处理过程关键出水参数软测量[J]. 自动化学报，2019，45(5)：906-919.
MENG Xi, QIAO Junfei, HAN Honggui. Soft measurement of key effluent parameters in wastewater treatment process using brain-like modular neural networks[J]. Acta Automatica Sinica, 2019, 45(5): 906-919(in Chinese).

[16] SHAO W M, GE Z Q, SONG Z H. Soft-sensor development for processes with multiple operating modes based on semisupervised Gaussian mixture regression[J]. IEEE Transactions on Control Systems Technology, 2019, 27(5): 2169-2181.

[17] 靳起朝，任超. 基于零信任架构的边缘计算接入安全体系研究[J]. 网络安全技术与应用，2018(12): 26-27.

[18] 冯登国，刘敬彬，秦宇，等. 创新发展中的可信计算理论与技术[J]. 中国科学：信息科学，2020，50(8)：1127-1147.
FENG Dengguo, LIU Jingbin, QIN Yu, et al. Trusted computing theory and technology in innovation-driven development[J]. Scientia Sinica (Informationis), 2020, 50(8): 1127-1147(in Chinese).

[19] 魏小强. 基于零信任的远程办公系统安全模型研究与实现[J]. 信息安全研究，2020，6(4)：289-295.
WEI Xiaoqiang. Research and implementation of security model of telecommuting system based on zero trust[J]. Journal of Information Security Research, 2020, 6(4): 289-295(in Chinese).

[20] MONTEIL J, RUSSO G. On the design of nonlinear distributed control protocols for platooning systems[J]. IEEE Control Systems Letters, 2017, 1(1): 140-145.

[21] DE FIORE D, RUSSO G. Resilient consensus for multi-agent systems subject to differential privacy requirements[J]. Automatica, 2019, 106: 18-26.

[22] MAO Y, YOU C S, ZHANG J, et al. A survey on mobile edge computing: the communication perspective[J]. IEEE Communications Surveys & Tutorials, 2017, 19(4): 2322-2358.

[23] 白昱阳，黄彦浩，陈思远，等. 云边智能：电力系统运行控制的边缘计算方法及其应用现状与展望[J]. 自动化学报，2020，46(3)：397-410.
BAI Yuyang, HUANG Yanhao, CHEN Siyuan, et al. Cloud-edge intelligence: status quo and future prospective of edge computing approaches and applications in power system operation and control[J]. Acta Automatica Sinica, 2020, 46(3): 397-410(in Chinese).

[24] WANG S L, ZHOU J W, LIU J K, et al. An efficient file hierarchy attribute-based encryption scheme in cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(6): 1265-1277.

[25] REN X B, YANG X Y, LIN J, et al. On scaling perturbation based privacy-preserving schemes in smart metering systems[C]//2013 22nd International Conference on Computer Communication and Networks (ICCCN). July 30 - August 2, 2013, Nassau, Bahamas. IEEE, 2013: 1-7.

[26] 谭璐. 高维数据的降维理论及应用[D]. 长沙：国防科学技术大学，2005.

[27] ROSE S, BORCHERT O, MITCHELL S, et al. Zero trust architecture[R]. National Institute of Standards and Technology, 2020.

收稿日期：2020–07–07；修回日期：2020–10–09。

作者简介：


任汝飞

任汝飞（1993），男，博士研究生，主要研究方向为信息能源系统分布式控制、能源互联网、边缘计算等，E-mail：rrf_neu@foxmail.com。

胡旌伟（1990），男，博士研究生，主要研究方向为能源市场、博弈论、系统建模及优化控制，E-mail：hjw_neu@outlook.com。

孙秋野（1977），男，博士，教授，主要研究方向为能源互联网的建模与优化运行、多能源综合互补优化、分布式发电系统的网络控制等。通信作者，E-mail：sunqiuye@mail.neu.edu.cn。

（责任编辑　张宇）