面向云边协同安全防护的边缘侧通算资源自适应调配方法

陆珊珊[1]，李莉[1]，李林[2]，孙海波[1]，吴润泽[2]
（1.国网冀北电力有限公司经济技术研究院，北京 100038；
2.华北电力大学 电气与电子工程学院，北京 102206）

摘要：近年来，分布式电源、电动汽车、柔性负荷调控等海量新型配电业务大规模接入，致使电力云主站预期运行压力骤增，合理发掘边缘侧通信及算力资源效用可显著缓解云主站预期运行压力。为此，提出一种面向云边协同安全防护的边缘侧通算资源自适应调配方法。首先，考虑多边缘子站可用通算资源构建云边协同接力式业务安全防护模型；再以最小化最大云主站的预期运行压力为目标建立对应线性规划问题，最后利用KKT进行快速求解。仿真结果表明，所提方法通过合理发掘边缘侧通算资源潜力有效降低云主站预期运行压力，在安全防护方面提升系统运行效率。

关键词：云边协同；安全防护；资源调配；新型配电系统
中图分类号：TM28 **文献标识码**：A **DOI**：10.19457/j.1001-2095.dqcd26316

Adaptive Allocation Strategy of Edge-side Communication-computing Resource for Cloud-edge Collaborative Security Protection

LU Shanshan[1]，LI Li[1]，LI Lin[2]，SUN Haibo[1]，WU Runze[2]
（1.*State Grid Jibei Electric Power Co.，Ltd. Economic and Technical Research Institute*，*Beijing* 100038，*China*；
2.*School of Electrical and Electronic Engineering*，*North China Electric Power University*，*Beijing* 102206，*China*）

Abstract：In recent years，the large-scale access of a large number of new power distribution services such as distributed power generation，electric vehicles，and flexible load control has led to a sharp increase in the operating pressure of the power cloud master station. To this end，an adaptive resource allocation method for edge-side general computing resources for cloud-edge collaborative security protection was proposed. Firstly，considering the computing resources available to multiple edge substations，a cloud-edge collaborative relay business security protection model was constructed. Then，with the goal of minimizing the operating pressure of the maximum cloud master，the corresponding linear programming problem was established，and finally the Karush-Kuhn-Tucker（KKT）was used to solve it quickly. The simulation results show that the proposed method can effectively reduce the operation pressure of the cloud master station and improve the operation efficiency of the system in terms of security protection by reasonably exploring the potential of edge computing resources.

Key words：cloud-edge collaboration；security protection；resource allocation；new power distribution system

2024年2月，国家发改委、国家能源局在联合印发的《关于新形势下配电网高质量发展的指导意见》中指出：到2030年，基本完成配电网柔性化、智能化、数字化转型[1-2]。然而，作为其核心业务枢纽，云主站支撑着极大比例的新型配电业务安全防护需求，但随着大量电力电子设备并入电网，产生了大量用电负荷控制问题[3]。在多域、多终端和多任务的复杂应用场景下，云主站预期运行压力骤增，因此如何降低云主站预期运行压力已成为现阶段研究热点之一[4-7]。

针对新型配电业务云主站预期运行压力轻量化问题，王晨晖等[8]从管理和技术两个方面考

基金项目：国网冀北电力有限公司项目(SGJBJY00GPJS2310015)
作者简介：陆珊珊（1998—），女，硕士，助理工程师，主要研究方向为电力通信网规划，Email:1765391876@qq.com
通讯作者：李林（2001—），女，硕士研究生在读，主要研究方向为无线传感网高能效数据采集，Email：2624891913@qq.com

虑，构建了一个新型安全电力系统保护体系。李杰等[9]根据电力网络化下令系统的工作原理，设计集中化信息识别算法，实现合理的集中化信息云调度。邹振万等[10]结合电力物联网的架构，根据智能终端面临的安全风险提出相应的安全防护对策。然而，上述工作仍旧缺乏云边协同视角下的资源调度灵活性，导致边缘设备中存在一部分算力资源未得到充分利用。

以云主站预期运行压力疏解为目标，在边缘算力发掘方面[11]，文献[12-13]提出可将容器化应用扩展到边缘的节点和设备，利用部分边缘侧设备资源进行安全防护。文献[14-16]提出一些云边协同系统安全防护架构和技术以满足数据安全处理需求，形成了较为完善的电力系统安全保护体系。上述方法可在一定程度上轻量化业务云主站预期运行压力，但现阶段边缘子站往往同时支撑多个业务云主站，未能充分考虑其分布式协同对各云主站预期运行压力均衡性的影响。

为解决上述问题，可以参考文献[17]中分布式资源潜能的主-配-微一体化协同控制策略，提出一种面向云边协同安全防护的边缘侧通算资源自适应调配方法（adaptive allocation strategy of edge-side communication-computing resource for cloud-edge collaborative security protection，A2S-EC2R）。首先，结合各边缘子站可用算力资源，构建面向边缘子站及业务云主站的多阶段接力式业务安全防护模型；其次，考虑多边缘子站分布式协同，以最小化最大业务云主站预期运行压力为目标构建对应线性规划问题，最后，利用Karush-Kuhn-Tucker（KKT）对问题进行快速求解。仿真结果表明所提A2S-EC2R算法可通过充分发掘多域边缘子站算力资源显著降低并最小化最大业务云主站预期运行压力。

1　云边协同计算框架及调度模型

1.1　云边协同计算架构

新型电力系统云边协同计算框架分为云、边、端三层结构，示意图如图1所示。其中，终端设备通过各类传感器执行数据采集任务，随后将采集的海量数据上发至边缘子站；边缘子站作为数据链路中的中转节点和实时处理中心，利用其本地资源完成边缘数据的初步处理，只将处理结果发送至云主站，为云主站分担部分计算任务；云主站将节省的计算资源分配到数据分析和任务调度工作中，以实现更快更高效的智能决策。

海量终端异构设备的接入使得配电网数据量骤增，各业务不同的时延要求大大增加了云主站的预期运行压力，从图1中的安全服务和调度管理的角度出发，可设计一多阶段接力式业务安全将防护模型以轻量化云主站预期运行压力。

图1　云边协同计算框架

Fig.1　Cloud-edge collaborative computing framework

1.2　系统模型

所述多阶段接力式业务安全将防护模型包括边缘子站安全防护、业务数据和安防进程上传以及云主站安全防护三个部分。可用有向图$G(B,E,C)$进行建模，$b_i \in B$表示一种业务，每个业务对应一个业务云主站；$e_i \in E$表示一个包含多种业务的边缘子站；$c_i \in C$表示一个业务云主站。云-边安防接力协同策略示意图如图2所示，边缘子站率先将自身可用算力资源分配至各业务，在满足时延约束的情况下，各业务在边缘子站处完成尽可能多的安全防护环节；随后，边缘子站将已处理过的业务传输至其所属云主站；各云主站

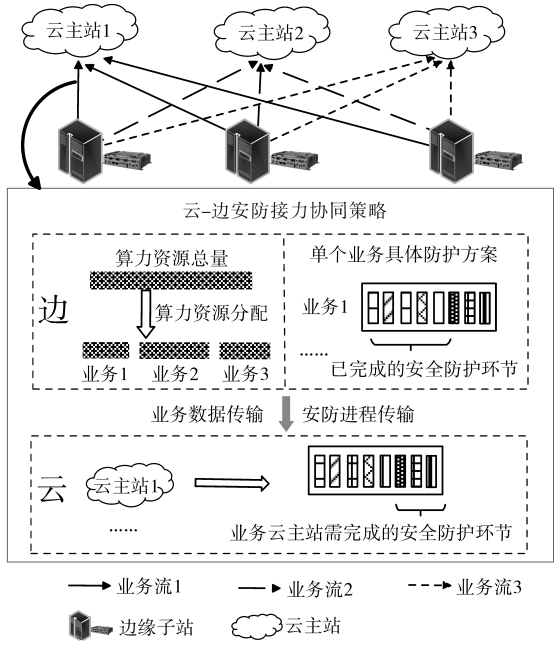

图2　云-边安防接力协同策略示意图

Fig.2　Schematic diagram of cloud-edge security relay coordination strategy

接收到数据后,判断下一步需完成的安全防护环节并完成数据的所有安全防护工作。在边缘子站处采用算力资源自适应分配策略对防护过程进行优化,以便能降低并最小化最大业务云主站预期运行压力。

2 算力资源分配策略

2.1 边缘子站算力资源分配

边缘子站可用于数据安防的算力资源是时刻发生变化的,因此需要将有限的算力资源合理分配给各个业务,以单个边缘子站为例,分配给各业务的算力资源需满足:

$$\sum_{i=1}^{i=\eta} f_i^{e_t} \leqslant f_{\max}^{e_t} \tag{1}$$

式中:η为各边缘子站中包含的业务类型总数;$f_i^{e_t}$为t时刻边缘子站分配给业务的算力资源;$f_{\max}^{e_t}$为t时刻边缘子站用于数据安防的算力资源总量。

考虑各业务的时延约束与边缘子站的算力资源约束,确定各业务在各边缘子站层面需要完成的安防环节数ξ。以业务i为例,时延约束如下:

$$T_{i,\mathrm{e}} + T_{i,\mathrm{tr}} + T_{i,\mathrm{c}} \leqslant T_{i,\mathrm{tot}} \tag{2}$$

其中

$$T_{i,\mathrm{e}} = T_{s_i,\mathrm{e}} + T_{i,\mathrm{p}}$$

$$T_{s_i,\mathrm{e}} = \sum_{k=1}^{k=\xi} T_{s_i,\mathrm{e}}^{k} \tag{3}$$

$$T_{s_i,\mathrm{e}}^{k} = D_i \cdot \frac{\varepsilon_{i,k}}{f_i^{e_t}} \tag{4}$$

式中:$T_{i,\mathrm{e}}$为业务i在边缘子站处的总时延;$T_{i,\mathrm{tr}}$为业务i在边缘子站和其对应业务云主站之间的传输时延;$T_{i,\mathrm{c}}$为业务i在对应云主站处的时延;$T_{i,\mathrm{tot}}$为业务i的时延约束;$T_{s_i,\mathrm{e}}$为业务i在边缘子站处完成数据安防产生的时延;$T_{i,\mathrm{p}}$为业务i的加密解密时延;ξ为业务i需在边缘子站处完成的前ξ个安防环节;$T_{s_i,\mathrm{e}}^{k}$为业务i完成数据安防环节k所消耗的时间;D_i为业务i的数据量大小;$\varepsilon_{i,k}$为安防环节k处理单位比特数据所需算力资源;$f_i^{e_t}$为上述边缘子站在t时刻分配给业务i的算力资源。

2.2 云主站算力资源计算

当业务数据从边缘子站传输至业务云主站时,业务云主站首先判断后续还需进行哪几个安防环节,如若该业务已经完成了所有安防工作,此时其所属业务云主站所需算力资源记为0。反之,计算所属云主站所需算力资源,以业务i为例,方法如下:首先,根据业务时延约束计算业务云主站的安防时间$T_{s_i,\mathrm{c}}$:

$$T_{s_i,\mathrm{c}} = T_{i,\mathrm{c}} - T_{i,\mathrm{p}} \tag{5}$$

式中:$T_{i,\mathrm{c}}$为留给业务云主站的总时间;$T_{i,\mathrm{p}}$为业务i的加密解密时延。

然后,根据$T_{s_i,\mathrm{c}}$便可计算出业务云主站所需算力资源f_i^{c},表示如下:

$$f_i^{\mathrm{c}} = \sum_{j=1}^{j=m} f_{i,j}^{\mathrm{c}} \tag{6}$$

其中

$$f_{i,j}^{\mathrm{c}} = \frac{\sum_{k=\xi+1}^{k=\kappa} \varepsilon_{i,k} \cdot D_i}{T_{s_i,\mathrm{c}}} \tag{7}$$

式中:m为边缘子站的总数量;$f_{i,j}^{\mathrm{c}}$为由边缘子站j发送至业务i所属云主站的数据完成安防所需算力资源。

根据上述所得算力资源,便可计算出各业务云主站预期运行压力。将业务云主站预期运行压力∂定义为在符合时延约束的情况下,其完成全部数据安防工作所需要的工作频率与其最大工作频率之比,以业务i为例,所属云主站预期运行压力∂_i计算方法如下:

$$\partial_i = (f_i^{\mathrm{c}} + f_{i,\mathrm{other}}^{\mathrm{c}}) / f_{i,\mathrm{c}}^{\max} \tag{8}$$

式中:$f_{i,\mathrm{other}}^{\mathrm{c}}$为$t$时刻业务$i$所属云主站中除安全防护外其余工作占用的算力资源;$f_{i,\mathrm{c}}^{\max}$为其最大工作频率。

2.3 问题提出

基于多阶段接力式业务安全防护模型,旨在通过多域边缘子站分布式协同降低并最小化最大业务云主站预期运行压力。面向包含n个业务云主站和m个边缘子站的模型中,构建优化问题,优化目标即为最小化最大业务云主站预期运行压力,表示形式如下:

$$\begin{cases} \min\limits_{f} \max\{\partial_i\} \quad i = 1,2,\cdots,n \\ \text{s.t.} \begin{cases} \mathrm{C1}: \sum_{i=1}^{i=n} f_i^{e_t} \leqslant f_{\max}^{e_t} \\ \mathrm{C2}: 0 \leqslant f_i^{e_t} \leqslant f_{\max}^{e_t} \\ \mathrm{C3}: T_{i,\mathrm{e}} + T_{i,\mathrm{tr}} + T_{i,\mathrm{c}} \leqslant T_{i,\mathrm{tot}} \end{cases} \end{cases} \tag{9}$$

其中,约束C1为算力资源约束,即边缘子站分配给各业务的算力资源之和不能超过其总算力;约束C2为各业务分配到的算力资源非负且不能大于总算力资源;约束C3为时延约束,各业务的传输时延和安全防护时延之和需满足时延要求。

3 问题求解

3.1 求解过程

为便于进行问题求解,假设各边缘子站和云主站拥有足够多的算力资源,能在各业务时延要

求内完成全部安全防护工作,因此在求解过程中将约束C3作为一判定条件即可。在算力资源分配方面,可将上述优化问题转化为如下形式:

$$\begin{cases}\min\limits_{f}\sum\limits_{i=1}^{n}\partial_i \\ \text{s.t.}\begin{cases}\text{C1:}\sum\limits_{i=1}^{i=n}f_i^{e_t}\leqslant f_{\max}^{e_t} \\ \text{C2:}0\leqslant f_i^{e_t}\leqslant f_{\max}^{e_t}\end{cases}\end{cases} \tag{10}$$

上述线性规划问题对于变量$f_i^{e_t}$是严格凹的,因此存在唯一极值点,满足KKT条件,相应的拉格朗日函数如下所示:

$$g(\hat{f})=\sum_{i=1}^{n}\partial_i(f_i^{e_t})+\sum_{i=1}^{n}\alpha_i(f_{\max}^{e_t}-f_i^{e_t})+\sum_{i=1}^{n}\beta_i f_i^{e_t}+\chi_k(f_{\max}^{e_t}-\sum_{i=1}^{i=n}f_i^{e_t}) \tag{11}$$

其中,α_i,β_i和χ分别对应于$f_{\max}^{e_t}\geqslant f_i^{e_t}$,$f_i^{e_t}\geqslant 0$和$f_{\max}^{e_t}\geqslant\sum_{i=1}^{i=n}f_i^{e_t}$的拉格朗日乘子。以业务$i$所属云主站为例,其KKT条件如下:

$$\begin{cases}\partial_i'(f_i^{e_t})-\dot{\chi}_k-\dot{\alpha}_i+\dot{\beta}_i=0 \\ \dot{\alpha}_i(f_{\max}^{e_t}-\dot{f}_i^{e_t})=0 \\ \dot{\beta}_i\dot{f}_i^{e_t}=0 \\ \dot{\chi}_k(f_{\max}^{e_t}-\sum_{i=1}^{i=n}\dot{f}_i^{e_t})=0 \\ \dot{\chi}_k\geqslant 0,\dot{\alpha}_i\geqslant 0,\dot{\beta}_i\geqslant 0\end{cases} \tag{12}$$

$\partial_i'(f_i^{e_t})$是$\partial_i(f_i^{e_t})$的一阶导数,$\dot{f}_i^{e_t}$为业务i对应云主站算力分配的最优解,$\dot{\alpha}_i$,$\dot{\beta}_i$和$\dot{\chi}$是α_i,β_i和χ对应的最优解。相应地,最优解的性质总结如下:

1)当$\dot{\alpha}_i>0$时,$\dot{f}_i^{e_t}=f_{\max}^{e_t}$,同时$\dot{\beta}_i=0$且$\partial_i'(f_i^{e_t})-\dot{\chi}_k=\dot{\alpha}_i$;

2)当$\dot{\alpha}_i=0$且$\dot{\beta}_i=0$时,$0\leqslant\dot{f}_i^{e_t}\leqslant f_{\max}^{e_t}$,此时$\partial_i'(f_i^{e_t})=\dot{\chi}_k$;

3)当$\dot{\beta}_i>0$时,$\dot{f}_i^{e_t}=0$,$\dot{\alpha}_i=0$且$\partial_i'(f_i^{e_t})-\dot{\chi}_k=-\dot{\beta}_i$。

根据上述性质可以发现$\dot{f}_i^{e_t}$和$\partial_i'(f_i^{e_t})-\dot{\chi}_k$之间存在着一些相关性,$\partial_i'(f_i^{e_t})$会随着$\dot{f}_i^{e_t}$的增加而单调递减,通过对$\dot{\chi}_k$迭代,可根据$\dot{\chi}_k$,$\partial_i'(0)$和$\partial_i'(f_{\max}^{e_t})$之间的关系计算出最优解$\dot{f}_i^{e_t}$。

具体来说,当$\dot{\chi}_k<\partial_i'(f_{\max}^{e_t})$时,满足性质1),此时$\dot{f}_i^{e_t}=f_{\max}^{e_t}$;当$\dot{\chi}_k>\partial_i'(0)$时,性质满足3),此时$\dot{f}_i^{e_t}=0$;当$\partial_i'(f_i^{e_t})=\dot{\chi}_{ki}$且$\partial_i'^{-1}(f_i^{e_t})=\dot{f}_i^{e_t}$时,满足性质2),通过迭代$\dot{\chi}_k$,直至$\sum_{i=1}^{i=n}\dot{f}_i^{e_t}$逼近$f_{\max}^{e_t}$时便可得到最优算力资源分配方案。

3.2 算法设计及复杂度分析

基于上述对问题的分解于局部凸近似处理,进行全局迭代优化,完成云边算力资源自适应调度的具体迭代过程伪代码如图3所示。

算法1:面向云边协同安全防护的边缘侧通算资源自适应调配方法

输入:各业务时延要求、边缘子站总算力资源、云主站总算力资源、各边缘子站包含的业务
输出:各云主站预期运行压力

```
1: 计算各边缘子站处的可用算力资源
2: for i=1,2,...,m do
3:    边缘子站根据3.1节所述方法自适应分配算力资源
4:    for j=1,2,...,n do
5:       for k=1,2,...,κ do
            if T_{i,e}+T_{i,tr}+T_{i,c}≤T_{i,tol} // 根据时延约束确定边缘子站处各业务可完成的安全防护进程
            else 安全防护进程 k-1
6:    各边缘子站将业务传输至对应云主站并完成其余安全防护工作
7:    根据式(8)计算各云主站预期运行压力
8: return 各云主站预期运行压力 ∂_i
```

图3 伪代码

Fig.3 Pseudocode

此算法的复杂度主要来自两个方面:第一,边缘子站CPU频率分配的计算;第二,边缘子站和云主站处数据安防进程的计算。设边缘子站数量为N,云主站的数量为M,安防进程数为K。由于KKT的迭代过程是借助二分法完成,则一个边缘子站处完成算力资源分配的复杂度可以用$o(\log_2 M)$表示,由于每个云主站需综合考虑来自各个边缘子站的业务及其安防进程,因此算法1的总复杂度为$o(NK\log_2 M)$,且其复杂度随着边缘子站数量和云主站数量的增加呈单调递增。

4 实验结果与分析

采用Matlab R2020a对所提出的面向云边协同安全防护的边缘侧通算资源自适应调配方法与其相关算法进行仿真,以验证A2S-EC2R的有效性,系统仿真环境参数设置如表1所示。

表1 仿真参数

Tab.1 Simulation parameters

参数	数值
边缘子站CPU最大工作频率/GHz	3
防护环节总数	5
各边缘子站传输的数据总量/k	300
边缘子站数量	5
业务云主站的数量	3
业务云主站CPU最大工作频率/GHz	5
各业务时延要求/s	[0.8,2,2.2]
业务传输带宽/bps	1 000
单位比特各业务所需频率周期数	[420,1 000,2 200]

在现实场景中,由于各边缘子站所处地理环

境不同,其包含的业务种类也不尽相同,为验证所提算法的有效性,在仿真过程中设置边缘子站包含随机业务和全部业务两种场景进行对比实验,边缘子站业务类型设置具体情况如表2所示。

表2　边缘子站业务类型设置

Tab.2　Service type setting of the edge substations

边缘子站号	随机业务	全部业务
1	业务1	业务1~业务3
2	业务2	业务1~业务3
3	业务1,业务2	业务1~业务3
4	业务2,业务3	业务1~业务3
5	业务1~业务3	业务1~业务3

为验证A2S-EC2R的性能,将其同未利用边缘子站可用算力资源(not using the available computing resources of the edge substations,NACR)和平均分配边缘子站可用算力资源(evenly distribute the available computing resources of edge substations,EDACR)进行对比,重点分析各业务云主站的预期运行压力,在包含5个边缘子站和3个云主站的系统模型中,图4和图5分别对应随机业务和全业务预期运行压力仿真结果。

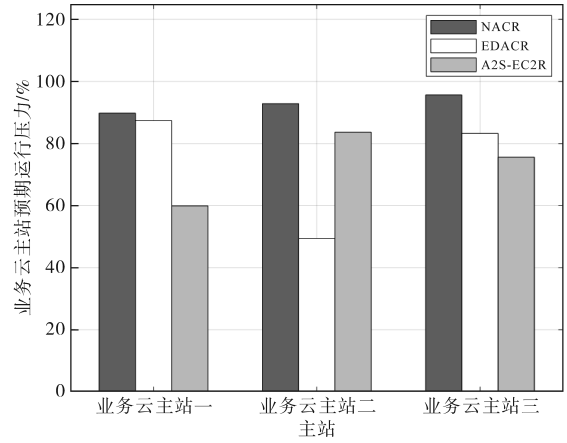

图4　随机业务预期运行压力仿真结果

Fig.4　Simulation result of random business expected operating pressure

由图4可知,与NACR相比,通过发掘边缘子站可用算力资源,EDACR和A2S-EC2R均可有效降低各业务云主站预期运行压力。但通过对比EDACR和A2S-EC2R的结果可知,A2S-EC2R在最小化最大云主站预期运行压力方面效果更优,云主站最大预期运行压力从EDACR的91.39%下降至83.64%。图5为相同条件下,各边缘子站全业务预期运行压力仿真结果,边缘子站处业务类型的增加导致网络中数据总量增加,因此与图4相比,图5中各云主站的预期运行压力整体增大,

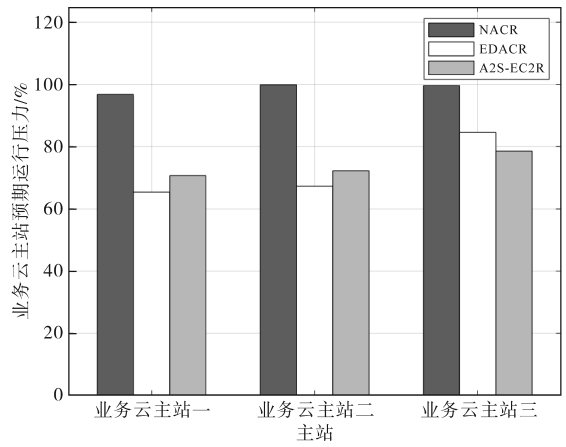

图5　全业务预期运行压力仿真结果

Fig.5　Simulation result of full-service expected operating pressure

但就仿真结果可知,A2S-EC2R在最小化最大云主站预期运行压力方面效果更优,图4所示云主站最大预期运行压力从EDACR的87.38%下降至83.64%,图5所示云主站最大预期运行压力从EDACR的84.54%下降至78.53%。

图6和图7分别是包含10个边缘子站和5个业务云主站的系统模型对应的仿真结果,在算力资源分配方法方面其对比结果与上述图4和图5得出的结论相同,即A2S-EC2R算法在最小化最大云主站预期运行压力方面效果更优。但由于边缘子站数量的增加会导致各业务数据总量增加,因此与图4和图5相比,图6和图7所示在未利用边缘子站可用算力资源的情况下各业务云主站的预期运行压力骤增,甚至超过了云主站性能上限,故而压力超过100%。相应地,相比图6,图7所示后续增加的业务会影响在边缘子站处算力资源的分配情况,并且业务类型的增加会导致业务数据量增加,加大云主站的预期运行压力。

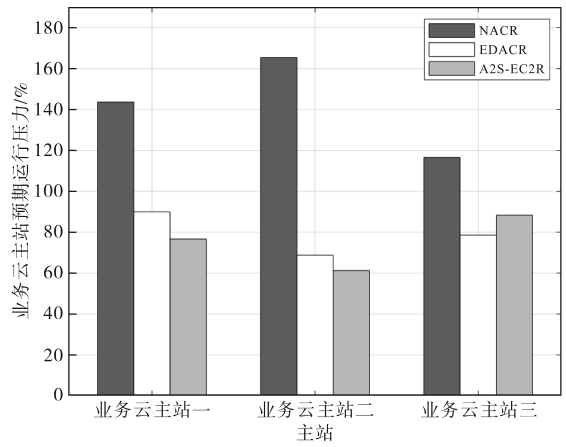

图6　10边缘子站下随机业务预期运行压力仿真结果

Fig.6　Simulation result of random service expected operation pressure under 10 edge substations

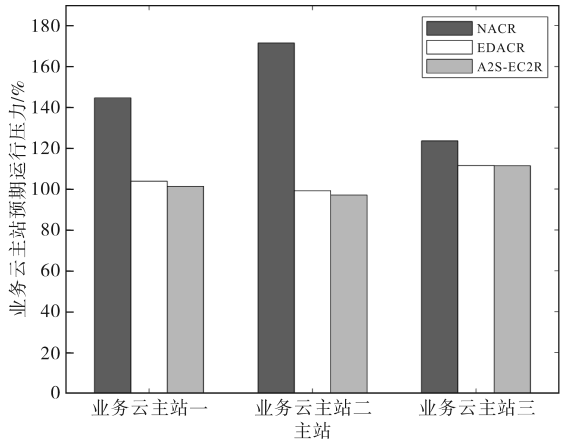

图7　10边缘子站下全业务预期运行压力仿真结果

Fig.7　Simulation result of full-service expected operation pressure under 10 edge substations

因此，EDSCR和A2S-EC2R所对应的各业务云主站预期运行压力与图6结果相比较大。此外，A2S-EC2R算法在最小化最大云主站预期运行压力方面效果更优，图6所示云主站最大预期运行压力从EDACR的89.96%下降至88.37%，图7所示云主站最大预期运行压力从EDACR的111.54%下降至111.37%。

图8和图9所示为边缘子站算力4 GHz下随机业务和全业务预期运行压力仿真结果，在边缘子站算力资源增大的情况下，可分配至各业务的可用算力资源相应增大，各云主站的预期运行压力会相应减少。通过图8与图4，图9和图5的对比结果可知，借助边缘子站进行分布式协同安全防护时，其可用算力资源增加会降低云主站的预期运行压力。此外，A2S-EC2R算法在最小化最大云主站预期运行压力方面效果更优，图8所示

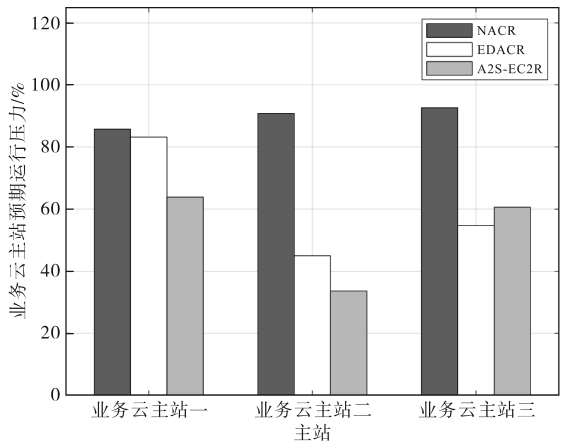

图8　边缘子站算力4 GHz下随机业务预期运行压力仿真结果

Fig.8　Simulation result of random service expected operation pressure under the computing power of 4 GHz of edge substations

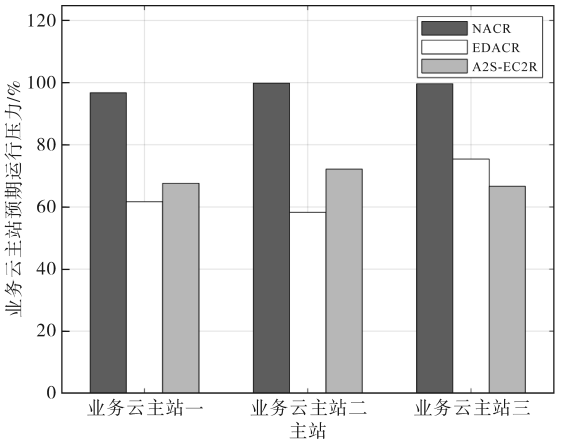

图9　边缘子站算力4 GHz下全业务预期运行压力仿真结果

Fig.9　Simulation result of full-service expected operation pressure under the computing power of 4 GHz of edge substations

云主站最大预期运行压力从EDACR的83.22%下降至66.89%，图9所示云主站最大预期运行压力从EDACR的75.42%下降至72.18%。

图10和图11分别为云主站算力5 GHz下随

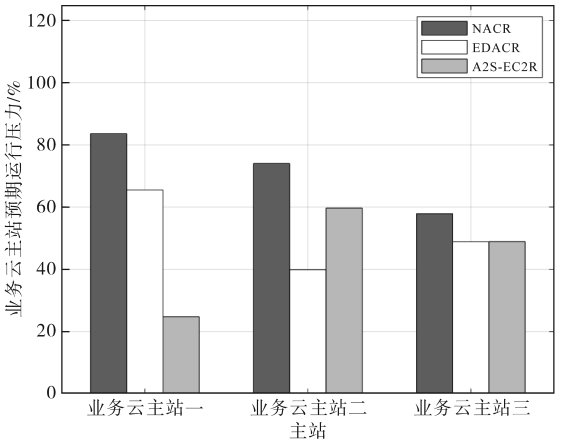

图10　云主站算力5 GHz下随机业务预期运行压力仿真结果

Fig.10　Simulation result of random service expected operation pressure under the computing power of 5 GHz of cloud master stations

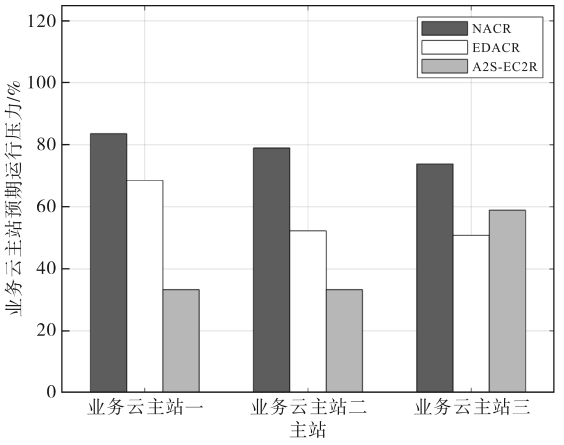

图11　云主站算力5 GHz下全业务预期运行压力仿真结果

Fig.11　Simulation result of full-service expected operation pressure under the computing power of 5 GHz of cloud master stations

机业务和全业务预期运行压力仿真结果。通过图10与图4，图11和图5的对比结果可知，借助边缘子站进行分布式协同安全防护时，云主站算力资源增大可显著降低其预期运行压力。此外，仿真结果显示A2S-EC2R算法在最小化最大云主站预期运行压力方面效果更优，图10所示云主站最大预期运行压力从EDACR的65.52%下降至5 963%，图11所示云主站最大预期运行压力从EDACR的68.52%下降至33.33%。

5　结论

面向新型配电系统，提出了一种基于云-边安防接力协同的新型配电通算资源自适应调度方法，通过多阶段接力式业务安全将防护模型，实现面向各边缘子站可用算力资源的分布式协同调度，显著降低并最小化最大业务云主站预期运行压力。通过提升配电系统多域异质资源联合调度灵活性，助力其柔性化、智能化、数字化转型。

参考文献

[1] 王俊娜，高新平. 电力系统计算机网络信息安全防护研究[J]. 工业控制计算机，2024，37(7)：137-138，160.
WANG Junna，GAO Xinping. Research on computer network information security protection of power system[J]. Industrial Control Computer，2024，37(7)：137-138，160.

[2] 邓嘉浩，林凌雪，朱林，等. 多阶段多属性配电网规划项目优选模型及求解[J]. 电气传动，2024，54(4)：67-74.
DENG Jiahao，LIN Lingxue，ZHU Lin，et al. Multi-stage and multi-attribute distribution network planning project optimal selection model and its solution[J]. Electric Drive，2024，54 (4)：67-74.

[3] 李顺昕，赵轩，赵一男，等. 基于"源-荷"不确定性的配电网用电负荷分布式协同控制[J]. 电气传动，2024，54 (12)：54-60.
LI Shunxin，ZHAO Xuan，ZHAO Yinan，et al. Distributed collaborative control of electricity load in distribution networks based on source-load uncertainty[J]. Electric Drive，2024，54 (12)：54-60.

[4] 曹翔，姜敏. 基于业务关联模型的变电站网络安全风险评估方法[J]. 电力信息与通信技术，2022，20(11)：57-64.
CAO Xiang，JIANG Min. Substation cyber security risk assessment method based on business association model[J]. Electric Power Information and Communication Technology，2022，20 (11)：57-64.

[5] MANIA H，ABDURACHMAN E，GAOL F L，et al. Survey on threats and risks in the cloud computing environment[J]. Procedia Computer Science，2019，161：1325-1332.

[6] HUANG Z Y，XIA G M，WANG Z H，et al. Survey on edge computing security[C]//Proceedings of the 2020 International Conference on Big Data，Artificial Inteligence and Internet of Things Engineering (lCBAlE)，Piscataway：IEEE Press，2020：96-105.

[7] 李鹏，刘念，胡秦然，等. "新型电力系统数字化关键技术综述"专辑评述[J]. 电力系统自动化，2024，48(6)：1-12.
LI Peng，LIU Nian，HU Qinran，et al. Commentary on special issue of reviews on key technologies for digitalization of new power system[J]. Automation of Electric Power Systems，2024，48 (6)：1-12.

[8] 王晨晖，乔耀逵，方文顺. 新型电力系统安全保护系统的研究[J]. 电气技术与经济，2024 (7)：31-34.
WANG Chenhui，QIAO Yaokui，FANG Wenshun. Research on new power system security protection system[J]. Electrical Technology and Economics，2024(7)：31-34.

[9] 李杰，王卫，金广厚，等. 电力网络化下令系统集中化信息云调度方法[J]. 信息技术，2023 (6)：129-133.
LI Jie，WANG Wei，JIN Guanghou，et al. Centralized information cloud dispatching method for power network command system[J]. Information Technology，2023 (6)：129-133.

[10] ZOU Z，LI F，HOU Y. Research on security protection technology of intelligent terminal of electricity internet of things[C]// 2021 IEEE 5th Information Technology，Networking，Electronic and Automation Control Conference (ITNEC)，Xi'an，China，2021：1467-1470.

[11] 王彩霞，时智勇，梁志峰，等. 新能源为主体电力系统的需求侧资源利用关键技术及展望[J]. 电力系统自动化，2021，45 (16)：37-48.
WANG Caixia，SHI Zhiyong，LIANG Zhifeng，et al. Key technologies and prospects for demand-side resources utilization for power systems dominated by renewable energy[J]. Automation of Electric Power Systems，2021，45 (16)：37-48.

[12] 阮正平，余文魁，李凯，等. 基于KubeEdge架构的边缘智能设备管理研究[J]. 电力信息与通信技术，2020，18(2)：63-68.
RUAN Zhengping，YU Wenkui，LI Kai，et al. Research of the edge intelligent device management method based on KubeEdge [J]. Electric Power Information and Communication，2020，18 (2)：63-68.

[13] 赵航，刘胜，罗坤，等. 面向KubeEdge边缘计算系统应用研究[J]. 智能科学与技术学报，2022，4(1)：118-128.
ZHAO Hang，LIU Sheng，LUO Kun，et al. Research on the application of KubeEdge edge computing system[J]. Chinese Journal of Intelligent Science and Technology，2022，4 (1)：118-128.

[14] CHATTOPADHYAY A，MITRA U. Security against false data-injection attack in cyber-physicalsystems[J]. IEEE Transcations on Control of Network Systems，2019，7(2)：1015-1027.

[15] SEYEDI Y，KELLER J，GRIJALVA S，et al. A research testbed for protection，automation，and cyber-security of digital substations[C]//South East Conference 2024，Atlanta，GA，USA，2024：

（下转第57页）

WANG Qingyuan, CUI Li, WANG Mingshen, et al. Peak load regulation pricing strategy of electric vehicle considering fast and slow charging characteristics[J]. Electric Power Engineering Technology, 2023, 42(4): 31-40.

[13] 王琼，邹晴，李乐，等. 基于多智能体强化学习的电动汽车充放电调控算法[J]. 供用电，2023，40(9)：83-90.
WANG Qiong, ZOU Qing, LI Le, et al. Multi-agent reinforcement learning algorithm for charging/discharging control of electric vehicles[J]. Distribution & Utilization, 2023, 40 (9): 83-90.

[14] ZHAO Zhonghao, LEE Carman K M. Dynamic pricing for EV charging stations: a deep reinforcement learning approach[J]. IEEE Transactions on Transportation Electrification, 2022, 8(2): 2456-2468.

[15] 王子昊，王旭，蒋传文，等. 基于近端策略优化算法的灾后配电网韧性提升方法[J]. 电力系统自动化，2022，46(21)：62-70.
WANG Zihao, WANG Xu, JIANG Chuanwen, et al. Resilience improvement method for post-disaster distribution network based on proximal policy optimization algorithm[J]. Automation of Electric Power Systems, 2022, 46(21): 62-70.

[16] 杨志学，任洲洋，孙志媛，等. 基于近端策略优化算法的新能源电力系统安全约束经济调度方法[J]. 电网技术，2023，47(3)：988-998.
ZHU Zhixue, REN Zhouyang, SUN Zhiyuan, et al. Security-constrained economic dispatch of renewable energy integrated power systems based on proximal policy optimization algorithm[J]. Power System Technology, 2023, 47(3): 988-998.

[17] 马涛，李津，曹晓波，等. 计及用户行为差异性和配电网潮流的电采暖负荷群优化调度策略研究[J]. 电力科学与技术学报，2023，38(1)：77-87.
MA Tao, LI Jin, CAO Xiaobo, et al. Research on optimal dispatch strategy of electric heating load groups considering user behavior difference and distribution network power flow[J]. Journal of Electric Power Science and Technology, 2023, 38(1): 77-87.

[18] 薛贵挺，汪柳君，刘哲，等. 考虑碳排放的光储充一体站日前运行策略[J]. 电力系统保护与控制，2022，50(7)：103-110.
XUE Guiting, WANG Liujun, LIU Zhe, et al. Day-ahead operation strategy of an integrated photovoltaic storage and charging station considering carbon emissions[J]. Power System Protection and Control, 2022, 50(7): 103-110.

收稿日期：2024-10-07
修改稿日期：2024-11-17

（上接第49页）

1306-1310.

[16] 唐亚东，刘寅杨，杨维永. 基于等级保护网络安全体系的新型电力系统风险分析与防范[J]. 网络安全技术与应用，2023(12)：130-133.
TANG Yadong, LIU Yinyang, YANG Weiyong. Risk analysis and prevention of new power system based on hierarchical protection network security system[J]. Network Security Technology and Application, 2023(12): 130-133.

[17] 潘小辉，罗兴，穆煜，等. 挖掘分布式资源潜能的主-配-微一体化协同控制[J]. 电力大数据，2024，27(5)：1-8.
PAN Xiaohui, LUO Xing, MU Yu, et al. Coordinated optimization control for main-distribution-microgrid interconnection utilizing the potential of massive distributed resources[J]. Power Systems and Big Data, 2024, 27(5): 1-8.

收稿日期：2024-11-13
修改稿日期：2024-12-30