文章编号：1007-2322(2023)00-0001-08 文献标志码：A 中图分类号：TM71

基于边缘节点技术的电力系统入侵安全防护

李金[1]，高红亮[1]，刘科孟[1]，谢虎[2]
（1. 中国南方电网电力调度控制中心, 广东省 广州市 510630；2. 南方电网数字电网研究院有限公司, 广东省 广州市 510663）

Intrusion Security Protection of Power System Based on Edge Node Technology

LI Jin[1]，GAO Hongliang[1]，LIU Kemeng[1]，XIE Hu[2]
（1. China Southern Power Grid Power Dispatching Control Center, Guangzhou510630, Guangdong Province, China；2. Digital Grid Research Institute, China Southern Power Grid, Guangzhou 510663, Guangdong Province, China）

摘要：在电力系统安全防护中，为解决防护不全面问题，设计了基于边缘节点技术的电力系统安全防护方法。首先，基于边缘节点技术，建立边缘多址接入计算模型，对电力系统实施数据迁移，实现数据分布式部署。其次，设计数据传输加密算法，并基于 GCForest，建立电力系统网络入侵检测模型，模型由样本输入层、多粒度扫描层以及训练层构成，实施系统入侵检测。测试结果表明：该方法的平均服务时延最低仅为 456.32ms，网络健壮性没有较大波动，入侵检测的最高误检率和漏检率分别为 0.13% 和 0.14%。

关键词：边缘节点技术；数据迁移；分布式部署；电力系统；入侵检测；安全防护

Abstract：To solve the problem of incomplete protection in power system security protection, a power system security protection method based on edge node technology was designed. Firstly, based on the edge node technology, the edge multi-access computing model was established to implement data migration for the power system and realize distributed data deployment. Secondly, the data transmission encryption algorithm was designed. And based on the GCForest, the power system network intrusion detection model, which was composed of a sample input layer, multi-granularity scanning layer, and training layer, was established to implement system intrusion detection. The test results show that the average service delay of the proposed method is only 456.32ms, the network robustness has no significant fluctuations, and the maximum false detection rate and missed detection rate of intrusion detection are 0.13% and 0.14%, respectively.

Keywords： edge node technology；data migration；distributed deployment；power system；intrusion detection；safety protection

DOI：10.19725/j.cnki.1007-2322.2022.0422

0 引言

电网作为一种重要的国家基础设施，其发展一直备受国民瞩目。近年来，我国一直致力于以双碳为目标发展综合能源的新型电力系统。在新型电力系统的发展中，安全问题很容易受到忽视，因此必须高度重视其安全防护问题[1]。我国工信部也提出要求，阐明有关国有企业、有关部门以及各地区都需要提高新型电力系统的安全防护意识，切实加强其安防管理，以更好地保障国家经济稳定、工业生产安全以及人民的财产、生命安全[2]。

在“双碳”目标下，“终端能耗电动化+电力系统脱碳”是主要减排路径。能源生产加快向清洁发展，能源消费高度电动化，能源配置越来越扁平化，能源利用越来越高效，给电力系统各环节带来深刻变革。新型电力系统承担着准实时或实时对电网进行管理与控制的任务，具体功能包括对厂站端与主站系统进行遥视、遥信等，因此系统数据量巨大，与电网安全有着直接的关系[3]。一旦遭受攻击，后果可能极其严重[4]。同时在连接其他系统时，往往会出现各系统安全级

基金项目：国家重点研发计划资（2020YFB0906000）；南方电网公司重点科技项目（0000002021030101XT00045）
Project Supported by National Key R&D Program Funding (2020YFB0906000); Key Technology Projects of China Southern Power Grid Corporation (000002021030101XT00045)

别不同的情况，安全隐患很多，更加凸显了新型电力系统安全防护问题的重要性[5]。基于该背景对电力系统安全防护问题进行深入研究。文献 [6] 提出了基于智能仿生算法和深度信念神经网络的智能电网网络入侵检测模型。利用智能仿生算法和深度信念神经网络，构建智能电网网络入侵检测模型，将智能仿生算法和深度信念神经网络融合，对该构建的模型进行求解，实现电网网络入侵检测；文献 [7] 提出了电力系统智能终端信息安全防护技术研究框架。依据电力系统智能终端安全互联和现场移动作业需求，分析电力系统智能终端安全防护挑战及防护技术框架。建立覆盖芯片层、终端层和交互层，实现对芯片电路级的可证明安全防护和内核故障的自动修复。对可信计算和业务安全的异构终端主动免疫进行融合，实现电力系统智能终端的信息安全防护。但上述方法的入侵检测误检率、漏检率和服务时延较高，网络波动较大，安全防护功能较差。

基于上述研究成果，在电力系统安全防护中，攻击手段也在不断演变。为了解决保护不足的问题，本文设计了一种基于边缘节点技术的电力系统安全防护方法，采用边缘节点技术，将重点放在边缘、数据处理、应用操作甚至一些功能服务的实现上。将中心服务器分散到网络边缘节点，加快了数据处理速度，减少了延迟，改善了客户体验。有研究表明，边缘计算可以将云计算的处理速度提高 30 倍。边缘节点技术最重要的是减少时延。借助边缘计算，对实时决策至关重要的数据可以进行现场处理，从而加快决策速度。离场景中处理的数据越近，响应时间就越快。

1 基于边缘节点技术的电力系统入侵安全防护方法设计

1.1 基于边缘节点技术的数据分布式部署

基于边缘节点技术设计一种边缘多址接入计算模型对电力系统实施数据迁移，实现数据的分布式部署[8-10]。

设计的边缘多址接入计算模型由 3 部分构成，如图 1 所示。

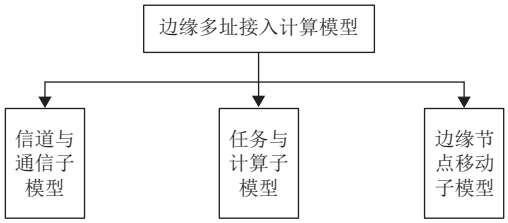

图 1 边缘多址接入计算模型

Fig. 1 Edge multiple access computing model

第 1 个部分是信道与通信子模型。首先对该子模型进行设计，具体如式 (1) 所示

$$\begin{cases} g_{ij}(t)=\dfrac{2h_{ij}(t)}{\vartheta_{ij}\times d_{ij}(t)} \\ S_{ij}(t)=\dfrac{2p_{ij}g_{ij}(t)}{\sum\limits_{n=1,n\neq i}^{N}p_{ij}g_{ij}(t)+2\sigma_{ij}(t)} \\ \forall i\in D,\ \forall j\in C \end{cases} \tag{1}$$

式中：$g_{ij}(t)$指的是电力系统网络节点与边缘节点之间的信道增益；$h_{ij}(t)$是指电力系统网络节点与边缘节点之间存在的小尺度衰落；ϑ_{ij}指的是二者之间的路径损失；$d_{ij}(t)$是指二者之间的距离；D指的是计算迁移周期中有数据传输任务的电力系统网络节点索引集；C是指边缘节点索引集；$S_{ij}(t)$指的是边缘节点j与电力系统网络节点i之间的信干噪比；p_{ij}是指边缘节点j与电力系统网络节点i之间的上行链路传输功率；N指的是边缘节点数量；n是指电力系统网络节点数量；$\sigma_{ij}(t)$指的是 2 种节点之间的信道功率增益[11-13]。

第 2 个部分是任务与计算子模型，构建的模型如式 (2) 所示

$$\begin{cases} F=\{1,2,\cdots f\} \\ f_a=\left[f_a{}^1,f_a{}^2,f_a{}^3\right] \\ t=\dfrac{U_C{}^2}{\varphi_{ij}(t)} \end{cases} \tag{2}$$

式中：F指的是电力系统数据业务类型的对应索引集合；f是指第f种电力系统数据业务类型；f_a指的是电力系统网络节点数据任务类型对应的属性集合；$f_a{}^1$是指电力系统数据业务类型对应的优先级；$f_a{}^2$指的是业务类型的实际大小；$f_a{}^3$是指任务处理时延；t指的是处理单位 bit 电力系统数据所需的时间；U_C是指处理单位 bit 电力系统数据所需的计算周期；$\varphi_{ij}(t)$指的是节点j向节点i分配的计算资源[14-16]。

第 3 部分是边缘节点移动子模型，具体如下式所示

$$p_q=\begin{cases} 0, u\leqslant 5 \\ 1, u>5 \end{cases} \tag{3}$$

式中：p_q指的是边缘节点移动概率；u是指该区域中现有的边缘节点数[17-19]。

通过 3 个边缘多址接入计算模型对数据进行分布式部署。

1.2　数据传输加密

本文设计一种数据传输加密算法（如图 2 所示），实施电力系统的数据传输加密。设计的数据传输加密算法由 3 部分构成，分别为解密算法、加密算法以及子密匙生成算法。

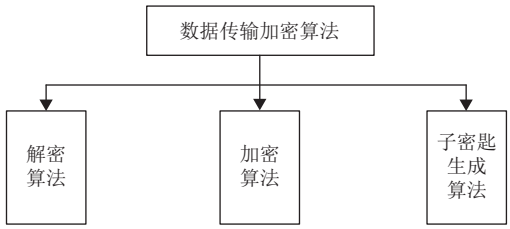

图 2　数据传输加密构成

Fig. 2　Data transmission encryption composition

数据传输加密算法在运行中共进行 8 次加密，因此首先需要对 8 个子密匙进行生成，并将其存储在子密匙集$Ks[0,1,\cdots 7]$中。生成 8 个子密匙的具体过程如下：边缘节点通过随机数生成器生成一个随机数，用 C 来表示。通过 C 对生成子密匙时的移位情况进行控制，混合基站发送的密匙与初始密匙的对应生成标识后共同进行运算，完成运算后取末尾的 8 个元素当作子密匙[20-22]。

因此子密匙生成算法的步骤设计具体如图 3 所示：

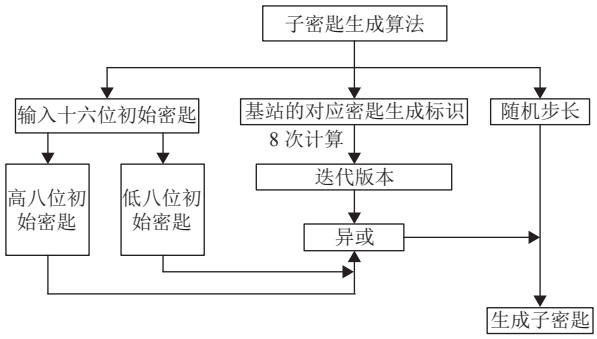

图 3　子密匙生成算法流程图

Fig. 3　Flowchart of sub key generation algorithm

1）输入初始密匙、随机步长 C 以及基站的对应密匙生成标识S；

2）对 16 位初始密匙进行划分，将其划分为 2 个 8 位的部分，其中低 8 位写入K_{or}中，高 8 位写入K_{ol}中，具体如下式

$$K_{16} \Rightarrow K_{(ol)},\ K_{(or)} \tag{4}$$

式中：K_{16}指的是 16 位初始密匙。

3）对基站的对应密匙生成标识 S 实施运算，获取其下一代迭代版本；

4）将写入K_{or}中的高 8 位密匙当作下一次迭代密码中的低 8 位部分；

5）对于写入K_{or}中低 8 位密匙，将其与基站的对应密匙生成标识S进行异或，接着与写入K_{or}中的高 8 位密匙进行异或，并实施移位，获取下一代迭代版本中的高 8 位；

6）经过 4 次初始加密运算与 8 次计算后获取子密匙集$Ks[0,1,\cdots 7]$，由K_6、K_7、K_8、K_9、K_{10}、K_{11}、K_{12}、K_{13}这 8 个元素构成。

在加密与解密中，算法使用 32 位明文密文，加密时实施 16 位运算，解密时需要使用 2 个寄存器，分别用 A 和 B 来表示[23-25]。将明文分为 2 个 16 位的部分分别存储在 A、B 中，通过以下流程实施明文的加密：

1）输入 32 位明文 M、随机步长 C 以及子密匙集$Ks[0,1,\cdots 7]$；

2）边缘节点在对信息进行感知时会产生很多数据，通过高位补 0 的方式对数据进行扩展，使其成为 32 的整数倍；

3）以 32 为基准对数据进行划分，获取 M 个数据片段；

4）通过L_0对 M 中的高 16 位进行存储，通过R_0对 M>中的低 16 位进行存储，具体如下式所示

$$M \Rightarrow L_0,\ R_0 \tag{5}$$

5）通过随机步长C与子密匙集$Ks[0,1,\cdots 7]$不断进行迭代，用L_{i+1}、R_{i+1}表示L_0、R_0在迭代中的中间过程；

6）8 次迭代后获取L_8、R_8，通过L_8对存储密文X中的高 8 位进行存储；通过R_8对存储密文X中的低 8 位进行存储；

7）将L_8、R_8合并，获取 32 位的存储密文 X。

解密步骤与加密相反，具体如下：

1）输入 32 位密文 X、随机步长 C 以及子密匙集$Ks[0,1,\cdots 7]$；

2）由于在算法中使用了密匙预存储技术，各边缘节点中存储着各节点的对应初始密匙。基站首先要通过子密匙生成算法对节点的对应初始密匙实施迭代；

3）通过随机步长C与子密匙集$Ks[0,1,\cdots 7]$继续进行迭代；

4）将迭代获取的密文分为L_8、$R_8 2$部分；

5）保留迭代中的R_i作为前一次迭代中的L_{i-1}；

6）使迭代中的R_i被密匙K_i作用；

7）对作用结果与循环右移C位的L_{i-1}实施减法运算，获取前一次迭代中的L_{i-2}；

8）不断循环，最终获取L_0、R_0；

9）组合L_0、R_0获取明文M。

1.3 网络入侵检测

基于 GCForest 设计一种电力系统网络入侵检测模型，实施系统的入侵检测。设计的电力系统网络入侵检测模型由 3 部分构成，第 1 部分是样本输入层，在该层中需要对输入样本实施预处理；第 2 部分是多粒度扫描层，负责对样本数据进行重构，并将其输入至森林层，接着对输出的预测概率向量进行拼接，将其作为训练层的输入向量；第 3 部分是由多层森林构成的训练层。在该层中，输入向量会分别通过各层森林。通过每层森林后，对输入向量进行添加，添加的向量会与该层输出的对应预测概率向量进行拼接，拼接结果即为下一层森林的输入，通过多层森林后，会得到样本的入侵概率预测结果[26-28]。在整体训练过程中，通过交叉验证可以对模型是否收敛进行判断，从而决定该层设置的森林层总数。

在样本输入层，实施的样本预处理步骤为数据尺度缩放与主成分分析处理。

其中数据尺度缩放处理使用的公式具体如下：

$$\begin{cases} f_{\text{std}}^{i}=\dfrac{f_i-\mu_x}{2\sigma_f} \\ \mu_x=\dfrac{1}{2}\displaystyle\sum_{i=1}^{n}f_i \\ \sigma_f=\sqrt{\dfrac{1}{2}\displaystyle\sum_{i=1}^{n}(f_i-\mu_x)^2} \end{cases} \tag{6}$$

式中：f_{std}^{i}指的是数据标准化处理结果；f_i是指第i组特征数据；μ_x指的是一组特征数据的对应均值；σ_f是指一组特征数据的对应标准差。

接着通过 PCA 算法实施主成分分析，经过主成分分析后，原始一维样本X的长度会变为d。对使用宽度为(a,b,c)的窗口实施特征扫描，扫描中的步长为(s_a,s_b,s_c)，将样本目标类型数用W来表示，则经过多粒度扫描层后，获得的特征数据X_{mgs}的长度具体如下式所示：

$$L=\left[\frac{(a-b)}{s_a}\right]^2+\left[\frac{(b-d)}{s_b}\right]^2+\left[\frac{(c-d)}{s_c}\right]^2 \tag{7}$$

在训练层中输入X_{mgs}，获取样本的入侵概率预测结果，完成电力系统安全防护设计。

2 实验测试

2.1 实验电力系统数据

为验证提出的基于边缘节点技术的电力系统安全防护方法的有效性，对其性能进行实验测试。在测试中，选择某地区构建的新型电力系统，该电力系统的网架结构如图 4 所示。

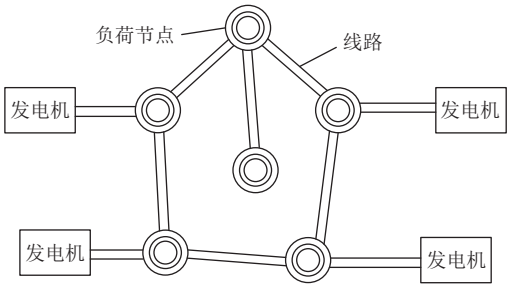

图 4 电力系统的网架结构示意图

Fig. 4 Schematic diagram of the grid structure of the power system

利用设计方法对其进行安全防护，测试该方法的各种安全防护性能，证明设计方法的有效性。

实验电力系统有 10 条线路、6 个负荷节点以及四台发电机。其中 10 条线路的参数如表 1 所示。

表 1 电力系统 10 条线路的参数

Table 1 Parameters of 10 power system lines

线路	始节点	末节点	电功率最大值/ MW	电抗参数
L1	1	2	48	0.25
L2	1	4	62	0.25
L3	1	5	58	0.31
L4	2	3	59	0.26
L5	2	4	88	0.13
L6	2	5	46	0.36
L7	2	6	58	0.22
3	5	5	48	0.24
L9	3	6	82	0.13
L10	4	5	45	0.45

实验电力系统的整体负荷达到 320 MW。由

于该电力系统线路较多、规模较大，因此经常遭受攻击，对其实施安全防护很有必要。

在测试时布设 2 台 PC 机，用于运行设计方法中的算法。实验环境具体如图 5 所示。

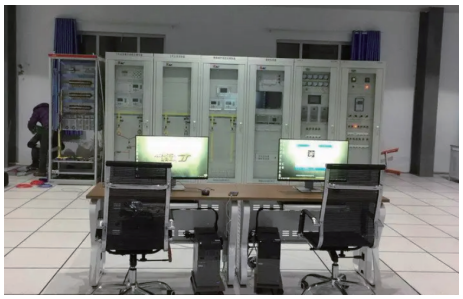

图 5　实验环境

Fig. 5　Experimental environment

在实验环境下对设计方法的性能进行测试。

2.2　数据分布式部署的服务时延测试

首先测试设计方法的数据分布式部署的服务时延，测试采用的边缘节点设备的内存为 256 MB，CPU 为 1 核，硬盘为 1 GB，OS 为 x86_64 架构。测试结果具体如表 2 所示。

表 2　数据分布式部署服务时延测试结果

Table 2　Test results of the data distributed deployment service delay

边缘节点数量/个	最高服务时延/ms	最低服务时延/ms	平均服务时延/ms
50	543.69	352.21	456.32
55	593.20	345.30	498.52
60	652.14	412.26	501.24
65	698.25	444.68	557.24
70	764.20	425.69	596.32
75	812.20	501.24	608.25
80	882.54	524.85	625.57
85	925.32	712.54	752.25
90	965.85	765.25	789.25

根据表 2 的数据分布式部署的服务时延测试数据，设计方法在边缘节点数量不断增加的过程中，数据分布式部署的服务时延也有一定增加，但整体增幅较小，说明设计方法的数据分布式部署的服务时延整体较低，其中平均服务时延最低仅为 456.32 ms，表明设计方法的数据分布式部署较快，有利于提高电力系统的安全性。

2.3　网络健壮性波动测试

接着测试设计方法在数据传输中的数据加密性能，具体来说，主要是测试在攻击节点增加的情况下，实验电力系统的网络健壮性是否有较大波动。具体测试结果如图 6 所示。

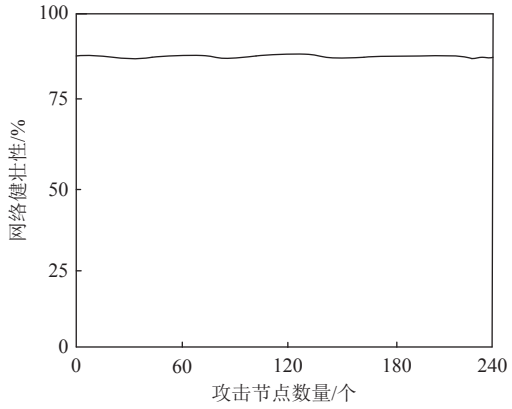

图 6　网络健壮性波动测试结果

Fig. 6　Test results of the network robustness fluctuation

根据图 6 的网络健壮性波动测试结果可以发现，在攻击节点数量增加后，实验电力系统的网络健壮性没有很大波动，整体比较平稳，数值也没有下降，说明设计方法的加密效果较好，攻击节点无法破解。

2.4　网络入侵检测误检率测试

测试设计方法在不同攻击节点数量下的网络入侵检测误检率，测试结果具体如图 7 所示。

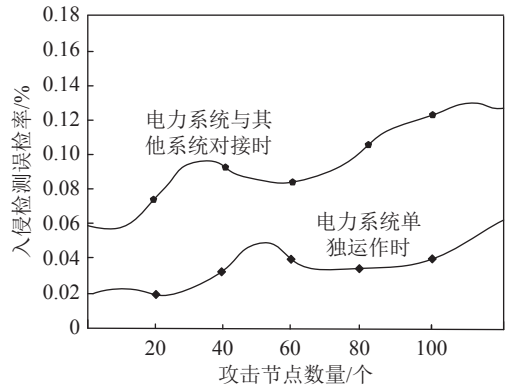

图 7　网络入侵检测误检率测试结果

Fig. 7　Test results of the network intrusion detection misdetection rate

根据图 7 的网络入侵检测误检率测试数据，在攻击节点数量不断增加的情况下，设计方法的网络入侵检测误检率有一定增加，但增幅较低。同时虽然在电力系统与其他系统对接时，入侵检测误检率高于系统单独运作时的误检率，但对接时的入侵检测误检率最高仅为 0.13%，说明设计方法的网络入侵检测误检率整体较低，证明了其

安全防护性能较好。

2.5 网络入侵检测漏检率测试

最后测试设计方法在不同攻击节点数量下的网络入侵检测漏检率，测试结果如图 8 所示。

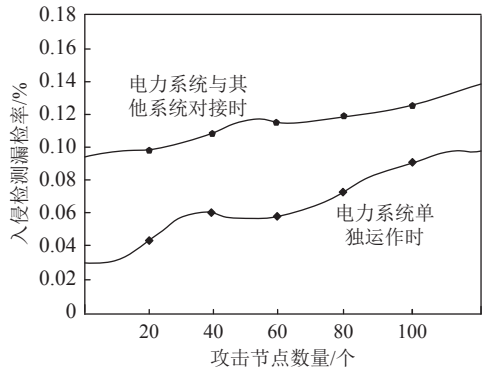

图 8 网络入侵检测漏检率测试结果

Fig. 8 Test results of the network intrusion detection misdetection rate

根据图 8 可知，随着攻击节点数量的增加，设计方法的网络入侵检测的漏检率也随之上升。同时虽然在电力系统与其他系统对接时，入侵检测漏检率高于系统单独运作时的漏检率，但对接时的入侵检测漏检率最高仅为 0.14%，证明设计方法的安全防护性能好。

2.6 网络入侵检测准确率测试

在此基础上，测试设计方法在不同攻击节点数量下的网络入侵检测准确率，测试结果如表 3 所示。

表 3 不同方法的网络入侵检测准确率测试结果对比

Table 3 Comparison of the accuracy test results of the network intrusion detection using different methods

攻击节点数量/个	所提方法/%	文献[6]方法/%	文献[7]方法/%
20	93.6	85.2	89.3
40	95.2	87.3	88.5
60	94.4	82.6	85.4
80	96.5	84.8	87.2
100	96.2	85.6	86.3

根据表 3 可知，当攻击节点数量达到 100 个时，文献 [6] 方法和文献 [7] 方法的平均网络入侵检测准确率分别为 85.1% 和 87.3%，而所提方法的平均网络入侵检测准确率高达 95.2%。由此可知，所提方法的网络入侵检测准确率较高。

3 结论

1) 本文设计方法的平均服务时延仅为 456.32 ms，表明设计方法的数据分布式部署较快，有利于提高电力系统的安全性。

2) 本文设计方法在攻击节点数量增加后，网络健壮性波动较小，整体较为平稳，说明设计方法的加密效果较好，攻击节点无法破解。

3）本文设计方法的网络入侵检测误检率有一定增加，但增幅较低。对接时的入侵检测误检率最高仅为 0.13%，说明设计方法的网络入侵检测误检率较低，证明了其安全防护性能较好。

4）本文设计方法的网络入侵检测漏检率有所上升，但对接时的入侵检测漏检率最高仅为 0.14%，证明设计方法的安全防护性能好。

5）本文设计方法的平均网络入侵检测准确率高达 95.2%，表明设计方法的网络入侵检测准确率较高。

参考文献

[1] 魏勇, 崔俊彬, 刘辛彤, 等. 基于改进动态故障树的电力系统广域保护通信系统可靠性分析方法 [J]. 电力系统保护与控制, 2021, 49(23): 171−177.
WEI Yong, CUI Junbin, LIU Xintong, *et al*. A reliability analysis method power system wide area protection communication system based on an improved dynamic fault tree [J] . Power System Protection and Control, 2021, 49 (23): 171−177.

[2] 王小虎, 王超, 李群, 等. 基于黑盒遗传算法的电力系统网络安全漏洞挖掘方法 [J]. 沈阳工业大学学报, 2021, 43(5): 500−504.
WANG Xiaohu, WANG Chao, LI Qun, *et al*. Network security vulnerability mining method for power system based on black box genetic algorithm [J]. Journal of Shenyang University of Technology, 2021, 43 (5): 500−504.

[3] 于杨, 姚浩, 习伟, 等. 具有主动免疫能力的电力终端内嵌入式组件解决方案 [J]. 南方电网技术, 2020, 14(1): 65−73.
YU Yang, YAO Hao, XI Wei, *et al*. Solution scheme of embedded component with active immunity for electric power terminals [J]. Southern Power System Technology, 2020, 14 (1): 65−73.

[4] 李雪, 孙霆锴, 侯恺, 等. 极端天气下电力系统大范围随机设备故障的 N-k 安全分析及筛选方法 [J]. 中国电机工程学报, 2020, 40(16): 5113−5125, 5.
LI Xue, SUN Tingkai, HOU Kai, *et al*. N-k Security assessment and screening for large-scale random equipment faults

in bulk power grid under extreme weather [J]. Proceedings of the CSEE, 2020, 40 (16): 5113−5125.

[5] 朱炳铨, 郭逸豪, 郭创新, 等. 信息失效威胁下的电力信息物理系统安全评估与防御研究综述 [J]. 电力系统保护与控制, 2021, 49(1): 178−187.
ZHU Bingquan, GUO Yihao, GUO Chuangxin, *et al*. A survey of the security assessment and security defense of a cyber physical power system under cyber failure threat [J]. Power System Protection and Control, 2021, 49 (1): 178−187.

[6] NAYAK M S, KUMAR M A. An intelligent CSO-DBNN based cyber intrusion detection model for smart grid power system[J]. International Journal of Engineering Trends and Technology, 2020, 68(6): 50−57.

[7] 张涛, 赵东艳, 薛峰, 等. 电力系统智能终端信息安全防护技术研究框架 [J]. 电力系统自动化, 2019, 43(19): 1-8, 67.
ZHANG Tao, ZHAO Dongyan, XUE Feng, *et al*. Research framework of cyber-security protection technologies for smart terminals in power system [J]. Automation of Electric Power Systems, 2019, 43(19): 1-8, 67.

[8] 于群, 刘启林. 基于 L2 范数的电力系统运行安全态势三维可视化评估 [J]. 科学技术与工程, 2020, 20(19): 7704−7710.
YU Qun, LIU Qilin. Three dimensional visualization evaluation of power system operation security situation based on L2 Norm [J]. Science Technology and Engineering, 2020, 20 (19): 7704−7710.

[9] 皇甫成, 邱婷, 梁吉, 等. 一种考虑电力系统频率安全的新能源并网限值评估方法 [J]. 电网与清洁能源, 2021, 37(2): 85-90, 98.
HUANG Fucheng, QIU Ting, LIANG Ji, *et al*. A sustainable energy penetration limit evaluation method considering power system frequency security [J]. Power System and Clean Energy, 2021, 37 (2): 85-90, 98.

[10] 杨天琦, 王琦, 叶志浩. 基于迁移支持向量机的舰船综合电力系统继电保护方法研究 [J]. 电力系统保护与控制, 2020, 48(23): 124−132.
YANG Tianqi, WANG Qi, YE Zhihao. Research on relay protection of ship integrated power system based on transfer support vector machine [J]. Power System Protection and Control, 2020, 48 (23): 124−132.

[11] 李满礼, 倪明, 颜云松, 等. 面向恶意攻击的安全稳定控制系统信息物理协调防御方法 [J]. 电力系统自动化, 2021, 45(18): 113−121.
LI Manli, NI Ming, YAN Yunsong, *et al*. Cyber-physical coordinated defense method against malicious attacks for security and stability control system [J]. Automation of Electric Power Systems, 2021, 45 (18): 113−121.

[12] 孙国强, 张恪, 卫志农, 等. 基于深度学习的含统一潮流控制器的电力系统快速安全校正 [J]. 电力系统自动化, 2020, 44(19): 119−127.
SUN Guoqiang, ZHANG Ke, WEI Zhinong, *et al*. Deep learning based fast security correction of power system with unified power flow controller [J]. Automation of Electric Power Systems, 2020, 44 (19): 119−127.

[13] 梁汉东, 高毓群, 侯婷, 等. 柔性直流配电系统负荷波动对系统过电压及过电流影响研究 [J]. 电力系统保护与控制, 2020, 48(13): 56−62.
LIANG Handong, GAO Yuqun, HOU Ting, *et al*. Study on the influence of load fluctuation on overvoltage and overcurrent of a VSC-DC distribution system [J]. Power System Protection and Control, 2020, 48 (13): 56−62.

[14] 林恒先, 侯凯元, 陈磊, 等. 高比例风电电力系统考虑频率安全约束的机组组合 [J]. 电网技术, 2021, 45(1): 1−9.
LIN Hengxian, HOU Kaiyuan, CHEN Lei, *et al*. Unit commitment of power system with high proportion of wind power considering frequency safety constraints [J]. Power System Technology, 2021, 45 (1): 1−9.

[15] 王罡, 刘敬文, 李国鹏, 等. 基于多源异构数据融合的综合管廊电力舱系统保护 [J]. 电力系统保护与控制, 2021, 49(7): 103−109.
WANG Gang, LIU Jingwen, LI Guopeng, *et al*. System protection of a pipe corridor power cabin based on multi-source heterogeneous data fusion [J]. Power System Protection and Control, 2021, 49 (7): 103−109.

[16] 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 of demand-side resource utilization for power systems dominated by renewable energy [J] . Automation of Electric Power Systems, 2021, 45 (16): 37−48.

[17] 张程铭, 柳璐, 程浩忠, 等. 考虑频率安全的电力系统规划与运行优化研究综述与展望 [J]. 电网技术, 2022, 46(1): 250-264, 13.
ZHANG Chengming, LIU Lu, CHENG Haozhong, *et al*. Review and prospects of planning and operation optimization for electrical power systems considering frequency security [J]. Power System Technology, 2022, 46 (1): 250-264, 13.

[18] 邓勇, 彭敏放, 刘靖雯. 电力信息物理系统建模和信息攻击机制分析 [J]. 电力系统及其自动化学报, 2021, 33(10):

10−17.
DENG Yong, PENG Minfang, LIU Jingwen. Modeling of cyber power physical system and analysis of information attack mechanism [J]. Proceedings of the CSU-EPSA, 2021, 33 (10): 10−17.

[19] 杨瑞, 和敬涵, 许寅, 等. 考虑安控措施的交直流电力系统动态等值边界确定方法 [J]. 电力自动化设备, 2020, 40(4): 56−62.
YANG Rui, HE Jinghan, XU Yin, *et al*. Determination method of dynamic equivalent boundary for AC-DC power system considering security control actions [J]. Electric Power Automation Equipment, 2020, 40 (4): 56−62.

[20] 武卫东, 沈文, 徐丙凤. 集成防危性与安全性的电力 CPS 风险分析研究综述 [J]. 电测与仪表, 2020, 57(20): 51−59.
WU Weidong, SHEN Wen, XU Bingfeng. A survey review on integrated safety and security risk analysis of power cyber-physical system [J]. Electrical Measurement & Instrumentation, 2020, 57 (20): 51−59.

[21] 林银鸿, 王彬, 葛怀畅, 等. 电网在线暂态电压安全分析的降维方法 [J]. 电力系统自动化, 2021, 45(12): 109−118.
LIN Yinhong, WANG Bin, GE Huaichang, *et al*. Dimension reduction method for online transient voltage security analysis of power grid [J]. Automation of Electric Power Systems, 2021, 45 (12): 109−118.

[22] 宋晓芳, 周海强, 薛峰, 等. 计及源荷不确定性及频率安全的电力系统区间优化调度方法 [J]. 电力自动化设备, 2022, 44(3), 1−13.
SONG Xiaofang, ZHOU Haiqiang, XUE Feng, *et al*. Interval optimal dispatching method of power system considering source-load uncertainty and frequency security [J]. Electric Power Automation Equipment, 2022, 44(3), 1−13.

[23] 王华昕, 刘健, 邹龙, 等. 新型电力系统下低压直流配网的接地故障保护方法 [J]. 电测与仪表, 2022, 59(18), 1−9.
WANG Huaxin, LIU Jian, ZOU Long, *et al*. Ground fault protection method of low-voltage DC distribution network under new power system[J]. Electrical Measurement & Instrumentation, 2022, 59 (18): 1−9.

[24] 闫炯程, 李常刚, 刘玉田. 计及源荷不确定性的交直流大电网动态安全分级滚动预警 [J]. 电力系统自动化, 46(12), 61-69.
YAN Jiongcheng, LI Changgang, LIU Yutian. Graded rolling early warning of dynamic security for large-scale AC/DC power grid considering uncertainties on source and load sides[J]. Automation of Electric Power Systems, 2020, 46 (12): 61-69.

[25] 解鹏, 刘双峰, 张金华, 等. 基于区块链技术的电力系统光传输网络异常节点入侵检测 [J]. 自动化仪表, 2021, 42(4): 95−99.
XIE Peng, LIU Shuangfeng, ZHANG Jinhua, *et al*. Intrusion Detection of Abnormal Nodes in Optical Transmission Network of Power System Based on Blockchain Technology[J]. Process Automation Instrumentation, 2021, 42(4): 95−99.

[26] 杨杰, 郭逸豪, 郭创新, 等. 考虑模型与数据双重驱动的电力信息物理系统动态安全防护研究综述 [J]. 电力系统保护与控制, 2022, 50(7): 176−187.
YANG Jie, GUO Yihao, GUO Chuangxin, *et al*. A review of dynamic security protection on a cyber physical power system considering model and data driving[J]. Power System Protection and Control, 2022, 50(7): 176−187.

[27] 李大虎, 袁志军, 黄文涛, 等. 电网安全风险闭环管控体系构建方法设计 [J]. 电力系统保护与控制, 2021, 49(22): 161−170.
LI Dahu, YUAN Zhijun, HUANG Wentao, *et al*. Construction method design of a power grid security risk closed-loop management and control system[J]. Power System Protection and Control, 2021, 49(22): 161−170.

[28] 黄冬梅, 何立昂, 孙锦中, 等. 基于边缘计算的电网假数据攻击分布式检测方法 [J]. 电力系统保护与控制, 2021, 49(13): 1−9.
HUANG Dongmei, HE Li'ang, SUN Jinzhong, *et al*. Distributed detection method for a false data attack in a power grid based on edge computing[J]. Power System Protection and Control, 2021, 49(13): 1−9.

收稿日期：2022−10−27

作者简介：
李金 (1979)，男，硕士，教授级高级工程师，主要研究方向为电力系统自动化， E-mail：lijin790502@163.com；
高红亮 (1982)，男，硕士，高级工程师，主要研究方向为电力系统自动化；
刘科孟 (1995)，男，硕士，工程师，主要研究方向为调度自动化、大数据应用；
谢虎 (1986)，男，硕士，工程师，主要研究方向为调度自动化、新能源发电。