基于细胞自动机模型电力网络攻击预测技术

冶莉娟[1]，王亦婷[1]，朱励程[2]
（1. 国网青海省电力公司，青海 西宁 810008；2. 上海柒志科技有限公司，上海 200122）

摘　要：传统电力网络攻击范围预测技术的预测范围不够广，导致电力网络安全性提升效果不明显。为此，提出基于细胞自动机模型的电力网络攻击预测技术。搭建电力细胞自动机模型，将细胞自动机中的细胞看作电力细胞，建立细胞活力值转换规则，将其与攻击者执行攻击概率相结合，预测电力细胞的发展变化。根据中心电力细胞及邻域电力细胞的变化趋势预测电力网络攻击。实验结果表明：在时间因素影响下，提出的基于细胞自动机模型电力网络攻击预测技术的预测攻击节点位置与原始节点基本一致，预测后负荷切除量始终在 100 MW 以下，本文所提技术的有效性更好。

关键词：细胞自动机；电力网络；攻击概率；网络信息；预测模型
中图分类号：TP391
文献标志码：A
doi: 10.11959/j.issn.1000–0801.2023099

Cellular automata model based power network attack prediction technology

YE Lijuan[1], WANG Yiting[1], ZHU Licheng[2]
1. Qinghai Electric Power Company, Xining 810008, China
2. Qizhi Technology Co., Ltd., Shanghai 200122, China

Abstract: The prediction range of the traditional power network attack range prediction technology was not wide enough, resulting in the poor effect of power network security improvement. For this reason, a power network attack prediction technology based on cellular automata model was proposed. A cellular automata model was built, regarding the cells in the cellular automata as power cells, a cell vitality value conversion rule was established and combined with the attack probability of attackers to predict the development and change of power cells. The power network attack was predicted according to the change trend of central power cells and neighboring power cells. The experimental result shows that, under the influence of time factors, the predicted attack node location of the proposed power network attack prediction technology based on cellular automata model is basically consistent with the original node, and the predicted load removal is always below 100 MW, the proposed technology is more effective.

Key words: cellular automata, power network, attack probability, network information, prediction model

收稿日期：2022–08–17；修回日期：2023–04–14

0 引言

智能电网是国家建设、社会发展的关键基础设施之一，但其易遭受各种物理和网络攻击，影响人们生活的正常用电，因此，需要采取一定的技术手段保障电网安全稳定运行。随着网络规模的不断增长，智能电网变得更加复杂，整个基础设施无法完整地受保护，并且随着信息技术在电网中的应用和迭代更新，智能电网出现越来越多的漏洞，易遭受大范围的攻击[1-3]。网络攻击利用监控系统、数据采集等组件的可访问性，远程控制或破坏电力资源，导致设备无法正常工作[4]。这些不断增加的攻击方式严重威胁了电力网络的安全运行。因此，有必要分析电力网络中的安全隐患，预测网络攻击，以及可能产生的影响，并提出针对性的解决方案，保障电力系统的正常运行[5]。

网络攻击类型比较多，攻击手段复杂。现有研究资料显示，国内外在电力网络攻击预测方面的研究有很多，但是较少涉及未知攻击以及攻击能力等级对后续攻击的影响[6]。如文献[7]提出基于溯因推理网络的预测方法，利用假设的理论与经验相对照，以证明对网络攻击预测的准确性，这种预测方法更注重逻辑性，对于后续攻击的影响分析较少，其预测结果的有效性比较差。文献[8]提出基于多尺度卷积神经网络的预测方法，利用仿造生物的视知觉机制构建神经网络，以网络攻击特点作为特征，通过表征学习预测网络攻击，但是在实际应用中有效性也受到一定的限制，还存在进步的空间。文献[9]提出一种容忍阶段性故障的电网级联故障预警方法。明确电网级联故障预警目标，根据其在报警开始的时间点上的观察数据，识别出各类可能的串联故障，并构建相应的预警解集。在此基础上，以动态计算的网络攻击预报误差和阶段故障观察误差为信息物理融合的联合预警准则，研究其在电网串联故障主动防范中的有效性。但是，该方法忽略了对电网级联故障特征数据库的建立，导致故障相关数据较为混乱，影响故障预警效果。文献[10]利用性能时程响应函数评估电力网络毁伤韧性，以此实现电网故障预测。该文以我国某市电力网络为例，利用策略博弈模型求解出纳什均衡状态下电网攻防双方策略，获取不同恢复条件下该电力网络毁伤韧性。但是该方法对于复杂电网结构的处理效果不够理想。因此，本文提出基于细胞自动机模型电力网络攻击预测技术，利用空间相互作用和时间因果关系模拟电力网络攻击，预测网络攻击，解决上述问题。

1 基于细胞自动机模型的电力网络攻击预测

1.1 生成电力网络攻击特征数据库

不同类型的电力网络攻击行为呈现的特征各不相同，其特征变化是预测攻击的根本。能够表示攻击性特征的参数有两类，一类为攻击前与攻击无关的变量，包括负荷水平、惯性时间常数等；另一类为故障信息，包括攻击点、攻击量和攻击类型等。生成电力网络攻击特征数据库的关键要求是速度快、内容丰富、数量大，不仅能够代表大量数据，而且其本身还具有快速生产和传播的属性，能够辅助用户实现有用信息的快速搜索与获取。因此，在生成电力网络攻击特征数据库时，要考虑电力网络的实际运行方式和攻击信息的设定。

使用以往攻击信息数据作为输入，在编程软件中读取数据，并通过一些数据的预处理功能，完成电力网络运行暂态分析批量对象的设置。之后，通过编码程序调用网络接口函数，生成攻击仿真模块，利用预先设定好的网络攻击仿真条件循环调用该模块，自动批量仿真，生成大量数据样本。

调用攻击仿真模块之前，设置仿真条件，包

括运行方式和扰动信息的设置。运行方式的设置包括负荷水平、负荷模型和惯性时间常数[11]。设置的具体分类情况如下。

负荷水平：50%，50.25%，50.5%，…，110%。

攻击模型：100%Z，100%I，40%Z－60%P，35%Z－35%I－30%P，30%Z－40%I－30%P。

其中，Z 表示主动攻击，I 表示被动攻击，P 表示漏洞式攻击。

惯性时间常数：0.2，0.4，0.6，…，2.0。

其中，惯性时间常数以机组原始数值为基准。攻击类型的选择主要考虑单一类型故障，不考虑特殊复型故障，仿真的故障主要设置为数据库 SQL 注入、组件权限许可和访问控制漏洞和远程缓冲区溢出[12]。在仿真条件设置完成后，任意选择一种运行方式和攻击类型，形成不同的攻击仿真场景，经过暂态仿真后得到大量数据样本，汇总其中的攻击特征，生成电力网络攻击特征数据库。

1.2　计算攻击者执行攻击行为概率

电力网络攻击中包含域内攻击和跨域攻击，电力网络中的域分为物理域和信息域。在信息域攻击形式下，攻击者可以通过分布式拒绝服务、窃取等攻击手段达到攻击目的；在物理域攻击形式下，攻击者可以通过切断物理设备之间的连接达到攻击目的[13]。跨域攻击为横跨信息域和物理域的一种攻击形式，攻击主体的不同，攻击者采取的攻击方式也不同。本文以 APT（高级可持续威胁攻击）攻击为例，计算攻击行为概率。通常情况下，攻击者对电力网络的攻击为多路径攻击[14]，因此攻击行为存在“与”和“或”的关系。当默认计算条件为“与”关系时，计算攻击者能够独立执行攻击行为的概率，表示为 $p(a_1)$。计算过程中包含 3 个指标，分别是访问概率、访问复杂度和认证系数。依据通用漏洞评分系统的评分标准，计算攻击者电力网络攻击概率，计算式如下：

$$p(a_1)=2K_{\mathrm{v}}K_{\mathrm{c}}K_{\mathrm{u}} \tag{1}$$

其中，a_1 表示攻击行为，K_{v} 表示访问概率，K_{c} 表示访问复杂度，K_{u} 表示认证系数。当默认计算条件为“或”关系时，攻击者可以成功攻击目标的概率为：

$$p(t_i)=\sum_{i,j=1}^{n}P\left(t_i=T\left|p(t_i)\right.\right)\cdot p(t_j) \tag{2}$$

其中，T 表示攻击者达到目标花费的时间，t_i 和 t_j 均表示电力网络中的节点，n 表示电力网络中节点总数。在计算攻击者执行攻击概率行为后，采用细胞自动机模型预测电力网络攻击。

1.3　预测电力网络攻击

标准的细胞自动机模型是一个四元组，表示为：

$$W=(Q,R,N,F) \tag{3}$$

其中，R 表示细胞空间的维度，Q 表示细胞空间，N 表示一个包含 n 个不同细胞状态的一个空间矢量的组合，n 表示中心细胞的邻居个数，F 表示将 R^n 映射到 R 上的一个局部转换函数。将式（3）给出的细胞自动机中的细胞看作电力细胞，反映电力网络内电力负荷的不同类型和状态，将细胞的变化转换为活力值，利用该值构建电力细胞活力模型[15]。建立细胞活力值推理规则如下：

- 若细胞活力值“大”，则细胞转换概率“小”；
- 若细胞活力值“较大”，则细胞转换的可能性“较小”；
- 若细胞活力值“一般”，则细胞转换的可能性“一般”；
- 若细胞活力值“较小”，则细胞转换的可能性“较大”；
- 若细胞活力值“小”，则细胞转换的可能性“大”。

在细胞自动机模型中电力细胞活力值各取值的模型为：

$$U_{Qij}=U(K_{\mathrm{v}},K_{\mathrm{c}}K_{\mathrm{u}})\cdot p(t_i) \tag{4}$$

其中，U_{Qij} 表示影响因素 i 的第 j 个取值的活力计

算模型，U 表示电力细胞活力值。在建立模型后，通过不确定推理计算区域空间变量对每个电力细胞的概率，将 $t+1$ 时刻电力网络中心距离影响下的电力细胞转换概率记为 $P_{2,k}^{t+1}$，建立 t+1 时刻与电力网络中心距离最近的推理规则，同时考虑邻域电力细胞对中心电力细胞的影响。定义在中心电力细胞的 8 个方向的细胞，将与中心电力细胞有接触的细胞均定义为该中心电力细胞的邻居。则邻域电力细胞影响描述为：

$$G_k^{t+1}=\frac{\sum_{i,j=1}^{n}\mathrm{con}(e_{ij})}{n} \tag{5}$$

其中，n 表示邻居电力细胞的个数，con(·) 是一个条件函数，e_{ij} 表示邻居的发展状况，若 e_{ij} 表示邻居已经发生变化或即将发生变化，则返回 1，否则，返回 0。

在以上转换规则的支持下，即可得到电力细胞发展总概率的模型，进而预测到电力网络攻击。计算式如下：

$$p_k^{t+1}=G_k^{t+1}\times\sum p_{i,k}^{t+1} \tag{6}$$

其中，p_k^{t+1} 表示电力细胞在 $t+1$ 时刻发生转换的总概率，在计算开始之前，设置初始阈值 p_0，计算每个细胞的发展总概率。若计算结果大于设置的初始阈值，说明该电力细胞在网络攻击下发生了改变，以此类推，计算得到电力网络内的所有细胞。待计算完成后，即可预测电力网络攻击。

2 实验研究与结果分析

2.1 实验准备

为验证提出的基于细胞自动机模型电力网络攻击预测技术的实际性能，以电力无接触供电技术（CPS）作为实验背景，使用第三方软件模拟攻击者攻击电力网络的过程。关于实验硬件平台，处理器型号为 Core i7-2350M，内存为 4 GB，软件平台为 Window10 操作系统，使用 MATLAB 作为实验仿真软件，并使用 C++语言编程实现对电力网络攻击的预测。实验拓扑如图 1 所示。

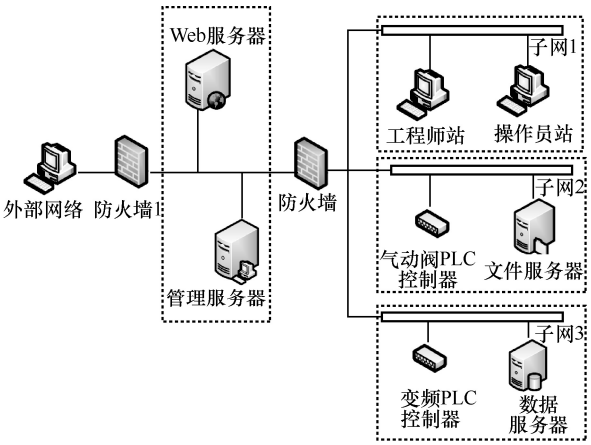


图 1 实验拓扑

图 1 中分为 4 个区域，分别是 DMZ、子网 1、子网 2 和子网 3，每个区域组成各不相同，攻击者可以针对不同的漏洞采取不同的形式攻击电力网络。因此，在每个组件上模拟不同的攻击漏洞。电力 CPS 漏洞信息见表 1。

表 1 电力 CPS 漏洞信息

组件编号	组件信息	CVE 编号	漏洞编号	漏洞说明	漏洞利用攻击编号
Z1	工程师站	CVE-2018-3951	D1	HTML 代码执行	a1
Z2	Web 服务器	CVE-2018-5056	D2	内核中的漏洞允许特权提升	a2
Z3	WinCC 操作员站	CVE-2018-2846	D3	数据库 SQL 注入漏洞	a3
Z4	文件服务器	CVE-2018-4627	D4	组件权限许可和访问控制漏洞	a4
Z5	变频 PLC 控制器	CVE-2018-0671	D5	模块访问安全绕过漏洞	a5
Z6	气动阀 PLC 控制器	CVE-2018-0084	D6	远程缓冲区溢出	a6
Z7	数据服务器	CVE-2018-0076	D7	释放后重用漏洞	a7

当构造基于电力 CPS 的攻击路径时，考虑电力 CPS 中核心保护对象和安全目标，结合以上准备内容，生成如下 4 条攻击路径。

path1 ： $t_0 \to a_1 \to t_1 \to a_3 \to t_5 \to a_7 \to t_6$；

path2 ： $t_0 \to a_1 \to t_1 \to a_4 \to t_2 \to a_6 \to t_5 \to a_9 \to t_6$；

path3 ： $t_0 \to a_1 \to t_1 \to a_5 \to t_3 \to a_6 \to t_7 \to a_7 \to t_6$；

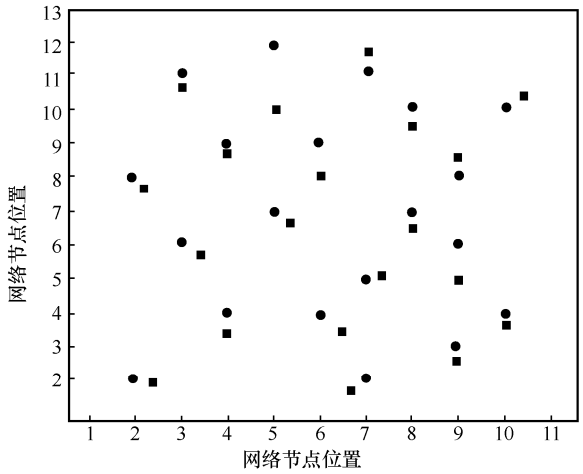
path4 ： $t_0 \to a_1 \to t_1 \to a_5 \to t_3 \to (t_0 \to a_2 \to t_4) \to a_7 \to t_6$。

其中，t 表示时间，参数 a 表示漏洞利用攻击编号，path4 中的括号表示优先对其进行攻击。根据以上内容模拟电力网络遭受攻击时的博弈情形，采用不同的电力网络攻击预测技术预测不同攻击路径下的攻击范围，统计每次攻击预测的节点位置，计算每次攻击后的负荷切除量。负荷切除量越高说明预测方法负载过重，电力网络运行越不流畅；反之，负荷切除量越低，说明预测方法负载小，电力网络运行流畅。

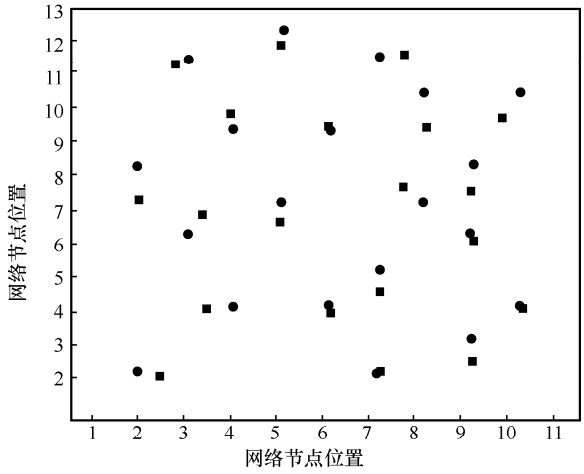
2.2　网络攻击预测节点位置实验结果及分析

实验中以电力 CPS 中各节点为关键点。执行不同的电力网络攻击预测方法，使用第三方软件输出实验结果，判断攻击预测节点位置。不同预测方法的预测攻击节点位置实验结果如图2所示。图 2 中，黑色圆圈表示原始攻击节点位置，黑色方块表示不同方法预测位置。

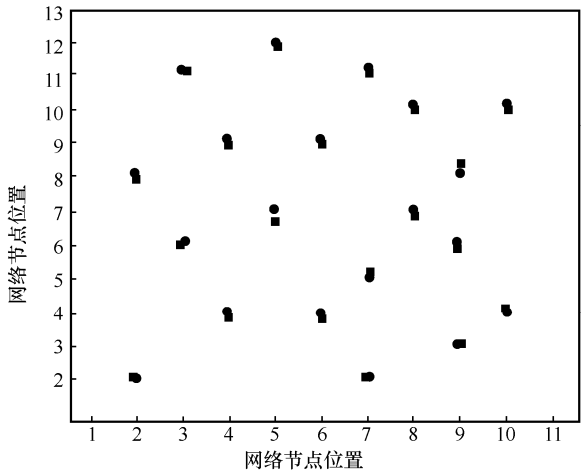
在网格内共有 20 个攻击节点，在相同的实验背景，默认预测结果有效的情况下，从图 2 可以看出，文献[7]方法中实际预测的攻击节点位置与原始的攻击节点位置存在误差，文献[8]方法的实验结果预测的节点位置与文献[7]相比，存在预测结果与原始攻击节点相符的情况。相比之下，在本文提出的基于细胞自动机模型电力网络攻击预测方法的实验结果中，预测的节点位置与原始攻击节点位置基本一致。因此，实验结果说明本文所提方法的预测效果更好。



(a) 文献[7]方法的实验结果



(b) 文献[8]方法的实验结果



(c) 本文所提方法的实验结果

图 2　不同预测方法的预测攻击节点位置实验结果

2.3　负荷切除量实验结果及分析

在负荷切除量实验研究中，以电力 CPS 作为实验背景，在所有攻击形式后，计算每种攻击形式下计算每种电力网络攻击预测方法的负荷切除

量。实验中使用的预测方法是在电力网络预测中比较常见的两种方法。不同攻击预测负荷切除量实验结果见表 2。

表 2　不同攻击预测负荷切除量实验结果

攻击路径种类	文献[7]方法	文献[8]方法	本文所提方法
path1	376 MW	362 MW	72 MW
path2	232 MW	294 MW	56 MW
path3	352 MW	276 MW	97 MW
path4	328 MW	306 MW	54 MW

表 2 中，在不同的攻击路径攻击后，常见的两种传统预测方法负荷切除量非常高，提出的预测方法负荷切除量均在 100 MW 以下，相比之下，本文所提方法负荷量与其相差了 3～4 倍，说明所提方法在使用过程中负载较少，电力网络运行更为流畅。将其与预测节点位置实验结果相结合，可知提出的基于细胞自动机模型电力网络攻击预测方法预测节点位置与原始节点位置基本一致，在预测中负荷切除量少，该预测方法的有效性优于常见的预测方法。

3　结束语

本文围绕着电力网络攻击预测展开研究与讨论，在大量研究资料和文献的支持下，进行了基于细胞自动机模型电力网络攻击预测技术的研究，并在完成预测后，设计了大量对比实验，通过对比实验证明了提出的基于细胞自动机模型电力网络攻击预测技术的可靠性。但是电力网络发展演变受到很多方面因素的影响，针对不同的规划地区，还需要适当调整预测深度，在后续研究中，将从这一方面深入探讨。

参考文献：

[1] 张红, 沈士根, 吴小军, 等. 基于元胞自动机和静态贝叶斯博弈的 WSN 恶意程序传染模型[J]. 电信科学, 2019, 35(6): 60-69.
ZHANG H, SHEN S G, WU X J, et al. WSN malware infection model based on cellular automaton and static Bayesian game[J]. Telecommunications Science, 2019, 35(6): 60-69.

[2] 韩丽芳, 胡博文, 杨军, 等. 基于攻击预测的电力 CPS 安全风险评估[J]. 中国电力, 2019, 52(1): 48-56.
HAN L F, HU B W, YANG J, et al. A new security risk assessment method for cyber physical power system based on attack prediction[J]. Electric Power, 2019, 52(1): 48-56.

[3] 刘巍, 李锰, 李秋燕, 等. 基于改进遗传算法的电网投资组合预测方法[J]. 电力系统保护与控制, 2020, 48(8): 78-85.
LIU W, LI M, LI Q Y, et al. Power grid portfolio forecasting method based on an improved genetic algorithm[J]. Power System Protection and Control, 2020, 48(8): 78-85.

[4] 阳育德, 蓝水岚, 覃智君, 等. 电力信息物理融合系统的网络-物理协同攻击[J]. 电力自动化设备, 2020, 40(2): 97-102.
YANG Y D, LAN S L, QIN Z J, et al. Coordinated cyber-physical attacks of cyber-physical power system[J]. Electric Power Automation Equipment, 2020, 40(2): 97-102.

[5] 陈碧云, 李弘斌, 李滨. 伪量测建模与 AUKF 在配电网虚假数据注入攻击辨识中的应用[J]. 电网技术, 2019, 43(9): 3226-3234.
CHEN B Y, LI H B, LI B. Application research on pseudo measurement modeling and AUKF in FDIAs identification of distribution network[J]. Power System Technology, 2019, 43(9): 3226-3234.

[6] 李昌祖, 牛东晓, 张欣岩, 等. 基于改进的粒子群优化 BP 神经网络浙江电能替代潜力预测模型[J]. 科学技术与工程, 2020, 20(13): 5173-5179.
LI C Z, NIU D X, ZHANG X Y, et al. Zhejiang Province electric power substitution potential prediction model based on improved particle swarm optimization BP neural network[J]. Science Technology and Engineering, 2020, 20(13): 5173-5179.

[7] 刘晓琴, 王大志. 基于溯因推理网络的电网故障预测方法研究[J]. 控制工程, 2019, 26(2): 343-348.
LIU X Q, WANG D Z. Research on power grid fault forecast based on abductive reasoning network[J]. Control Engineering of China, 2019, 26(2): 343-348.

[8] 许言路, 武志锴, 朱赫炎, 等. 基于多尺度卷积神经网络的短期电力负荷预测[J]. 沈阳工业大学学报, 2020, 42(6): 618-623.
XU Y L, WU Z K, ZHU H Y, et al. Short-term load forecasting based on multi-scale convolutional neural network[J]. Journal of Shenyang University of Technology, 2020, 42(6): 618-623.

[9] 王宇飞, 李俊娥, 刘艳丽, 等. 容忍阶段性故障的协同网络攻击引发电网级联故障预警方法[J]. 电力系统自动化, 2021, 45(3): 24-32.
WANG Y F, LI J E, LIU Y L, et al. Staged failure tolerance based early warning method for cascading failures in power grid caused by coordinated cyber attacks[J]. Automation of Electric Power Systems, 2021, 45(3): 24-32.

[10] 韩林, 赵旭东, 陈志龙, 等. 蓄意攻击下城市电力网络毁伤韧性评估[J]. 中国安全科学学报, 2021, 31(6): 161-169.
HAN L, ZHAO X D, CHEN Z L, et al. Research on damage re-

silience assessment of urban power networks under intentional attacks[J]. China Safety Science Journal, 2021, 31(6): 161-169.

[11] 孙平远, 刘科研, 齐冬莲. 基于电力信息物理系统实时仿真平台的网络安全仿真[J]. 电力建设, 2020, 41(2): 40-46.
SUN P Y, LIU K Y, QI D L. Cyber security simulation based on real-time simulation platform of cyber physical power system[J]. Electric Power Construction, 2020, 41(2): 40-46.

[12] 王珂, 田来, 吴俊. 基于区域毁伤的基础设施网络抗毁性评估模型[J]. 系统工程与电子技术, 2020, 42(5): 1102-1108.
WANG K, TIAN L, WU J. Survivability assessing model of infrastructure networks based on regional damages[J]. Systems Engineering and Electronics, 2020, 42(5): 1102-1108.

[13] 李永攀, 彭伟伦, 门锟, 等. 基于多视角低秩分析的电力状态不良数据检测[J]. 电子科技大学学报, 2019, 48(3): 361-365.
LI Y P, PENG W L, MEN K, et al. An approach for detecting band data in smart grid based on low-rank multi-view analysis[J]. Journal of University of Electronic Science and Technology of China, 2019, 48(3): 361-365.

[14] 狄冲, 李桐. 网络未知攻击检测的深度学习方法[J]. 计算机工程与应用, 2020, 56(22): 109-116.
DI C, LI T. Network unknown attack detection with deep learning[J]. Computer Engineering and Applications, 2020, 56(22): 109-116.

[15] 董刚, 余伟, 玄光哲. 高级持续性威胁中攻击特征的分析与检测[J]. 吉林大学学报(理学版), 2019, 57(2): 339-344.
DONG G, YU W, XUAN G Z. Analysis and detection of attack characteristics in advanced persistent threats[J]. Journal of Jilin University (Science Edition), 2019, 57(2): 339-344.

[作者简介]

冶莉娟（1982– ），女，国网青海省电力公司高级工程师，主要研究方向为电力调度自动化技术、电力监控系统网络安全技术等。

王亦婷（1974– ），女，国网青海省电力公司高级工程师，主要研究方向为电力系统及其自动化技术、电网调度技术等。

朱励程（1989– ），男，上海柒志科技有限公司产品研发部工程师，主要研究方向为计算机软件技术应用研究及管理。