文章编号：2095-4980(2025)02-0175-07

电力物联网终端漏洞关联挖掘优化算法设计

王　健，付志博，农彩勤，刘家豪，许伟杰

(南方电网数字电网集团信息通信科技有限公司，广东 广州 510670)

摘　要：受电力物联网(IoT)复杂性与终端漏洞隐蔽性的共同作用，现阶段采用的传统漏洞关联挖掘方法在关联特征参量上存在局部偏差，造成整体挖掘尺度不足，算法全局寻优效率偏低，严重影响电力IoT终端正常运行。为解决上述问题，从IoT结构特点入手，引入黑盒遗传算法，通过电力IoT终端状态感知、终端漏洞关联挖掘规则生成、黑盒遗传算法参量引入、终端漏洞关联挖掘4部分完成整体挖掘方法全局参量的重构优化，提升挖掘精确度与尺度。仿真测试表明，所提方法的挖掘曲线数值较大，且均值偏差指标差异为0.1，说明黑盒遗传算法在电力IoT终端安全漏洞挖掘中具有较高的可行性和有效性，且挖掘稳定性足以满足现阶段终端漏洞挖掘任务需求。

关键词：黑盒遗传算法；电力物联网；终端漏洞；关联挖掘

中图分类号：TP301.6　　**文献标志码：**A　　**doi：**10.11805/TKYDA2023276

Design of optimization algorithm for vulnerability correlation mining of power Internet of Things terminals

WANG Jian，FU Zhibo，NONG Caiqin，LIU Jiahao，XU Weijie

(Information and Communication Technology Co.，LTD.，China Southern Power Grid Digital Grid Group，Guangzhou Guangdong 510670，China)

Abstract：Affected by the complexity of the power Internet of Things(IoT) and the stealth of terminal vulnerabilities, the traditional vulnerability correlation mining methods currently in use exhibit local biases in correlation feature parameters. This leads to insufficient overall mining scale and low global optimization efficiency of the algorithms, which severely impacts the normal operation of power IoT terminals. To address the aforementioned issues, starting from the structural characteristics of IoT, a black-box genetic algorithm is introduced. By completing the global parameter reconstruction and optimization of the overall mining method through four parts: power IoT terminal status perception, terminal vulnerability correlation mining rule generation, introduction of black-box genetic algorithm parameters, and terminal vulnerability correlation mining, the accuracy and scale of mining are enhanced. Simulation tests indicate that the mining curve values of the proposed method are relatively large, and the mean deviation index difference is 0.1. This demonstrates that the black-box genetic algorithm has high feasibility and effectiveness in the mining of security vulnerabilities in power IoT terminals, and the mining stability is sufficient to meet the current terminal vulnerability mining task requirements.

Keywords：black box genetic algorithm；power Internet of Things；terminal vulnerability；association mining

近年来，我国在智能电网领域取得了一定的成就，智能电网的建设越来越广泛，对电力物联网(IoT)终端的安全防护要求也越来越高。智能电网的安全建设关系到我国社会经济的可持续发展，而电力IoT终端是智能电网中一个重要组成部分，其安全防护是保障智能电网安全运行的基础。由于电力IoT终端种类繁多，且存在不同程度的漏洞[1]，因此部分学者针对漏洞挖掘和检测展开了相应的研究。

陈泽等[2]主要关注基于知识图谱的电力网络安全漏洞挖掘系统的设计与实现，该系统能够实现电力网络安全

收稿日期：2023-09-22；修回日期：2023-11-30

漏洞的挖掘，并具有高效率和高准确率。王勇等[3]主要关注基于弱监督学习的电力信息动态漏洞挖掘系统的设计与实现，该系统能够更好地解决现存的漏洞信息错误挖掘问题。Pavaskar M等[4]提出了一种基于线性网格网络的单源可靠广播算法，该算法适用于移动自组织网络中，确保消息能够传递到网络中的所有节点。通过该算法，只有一部分节点进行广播传输，并且每个节点只发送一次，以实现可靠的广播。

黑盒遗传算法作为一种优化算法，通过模拟生物进化过程，在不依赖事先定义的适应度函数的情况下，从复杂的、无法直接获取或定义适应度值的问题中寻找最优解。将黑盒遗传算法用于电力物联网终端漏洞关联挖掘中，能够通过优化搜索和智能学习的方式，发现潜在的漏洞关联和异常行为。为此，本文提出一种基于黑盒遗传算法的电力IoT终端漏洞挖掘方法，并对其进行了仿真实验和性能分析，验证该方法在电力IoT终端安全漏洞挖掘中的可行性和有效性。

1 电力通信网络态势感知网络模型

为更好地识别漏洞特征，辅助优化挖掘尺度，对电力IoT终端状态感知进行计算。电力IoT结构中，网络主机与客户端、服务器之间信息交互均需通过交换机完成，因此可得到电力IoT数据交互网络结构，如图1所示。

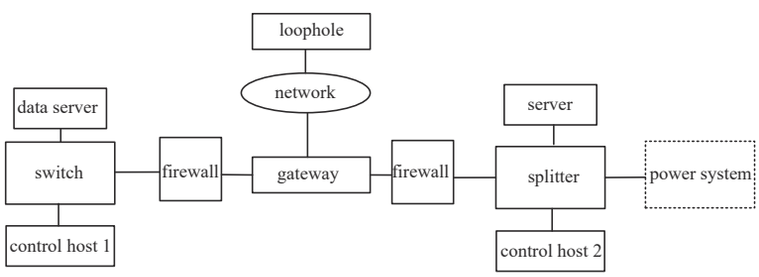

Fig.1 Data interaction network structure of power IoT
图1 电力物联网数据交互网络结构

当物联网中交互客户端信息存在漏洞异常风险时，在网络防火墙的机制作用下，会首先对客户端用户进行身份判别，同时对漏洞位置的数据状态进行感知分析。在获得客户端最高级别控制权限状态下，通过数据反向注入，可快速感知漏洞数据攻击位置。

2 黑盒遗传算法的引入与具体优化计算

2.1 电力物联网终端状态感知

通过电力通信网络态势感知网络模型，能够快速执行上述反向注入感知操作，配合物联网拓扑网络结果，完成全局接口的感知扫描，进一步获得精准的电力IoT态势感知状态转移示意图，如图2所示。由图2可知，电力IoT终端状态经历了5次转化后完成了与终端控制器文件的信息连通，5次状态依次标记为S_1~S_5。

以上述结构中2号主机感知的漏洞攻击状态为例进行计算分析，其感知态势对应系数计算过程为：

1) 对全局物联网信息交互状态进行安全态势威胁概率计算。以2次攻击状态出现概率为指标，计算其态势关联程度：

$$R(x,y)=\frac{\sum_{j=1}^{d}\lambda_j\gamma_j(x,y)}{\sum_{j=1}^{d}\lambda_j} \tag{1}$$

式中：λ_j为漏洞位置所对应第j个节点信息的攻击加权系数；γ_j为漏洞攻击特征的关联系数；d为节点数量。

2) 根据攻击关联系数对IoT终端态势进行威胁概率感知计算。

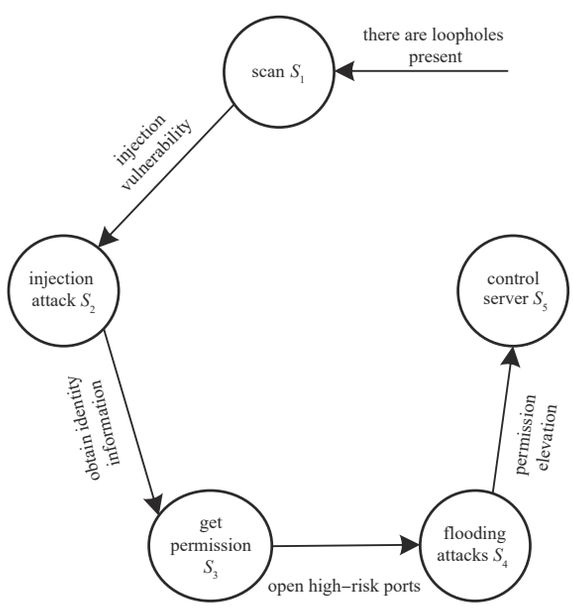

Fig.2 Schematic diagram of situational awareness state transfer in power IoT network
图2 电力物联网络态势感知状态转移示意图

3) 基于计算所得的网络攻击损失与威胁态势关联概率，可完成终端漏洞感知评分。为确保评分的精准，引入漏洞评分体系[5-6]对感知结果予以赋值。

4) 通过式(2)计算电力IoT终端状态感知输出结果：

$$W=\sum_{i=1}^{d}Aw_i D \tag{2}$$

式中：w_i为终端信息对应感知权重；A为全局物联网此刻的终端安全态势；D为终端信息。

2.2 终端漏洞关联挖掘规则生成

通过对上述感知信息的分析发现，感知信息以集合的形式构成频繁项集，因此可对构成的频繁项集之间关联性与依赖关系[7]进行感知规则的生成，找出电力物联网络中终端漏洞之间的潜在联系与模式，快速感知漏洞及其潜在威胁，增强电力物联网终端漏洞关联挖掘能力。

传统算法中采用的关联规则生成算法普遍基于神经网络的粒子传递特性，因此会受到网络漏洞中粒子属性差异的限制。为更准确地生成关联规则，本文提出黑盒遗传算法，利用其Sigmoid关系属性函数[8]对网络空间的粒子速度进行存在率计算，进而将问题由粒子关联属性问题转化为粒子属性的空间存在问题[9-10]，并通过概率选择粒子的存在形式为0或1，降低粒子优化过程的计算难度。在此基础上，利用黑盒遗传算法下粒子遗传聚类属性，对网络空间下的数据节点进行多类型划分，获得多个子类型数据库，以此提升数据区域挖掘的精准度。在此过程中可通过各个子类数据库得到其对应的频繁数据集，通过合并操作可进一步完成与之对应的终端漏洞特征关联，获得更为精准的挖掘规则。上述过程的流程如图3所示。

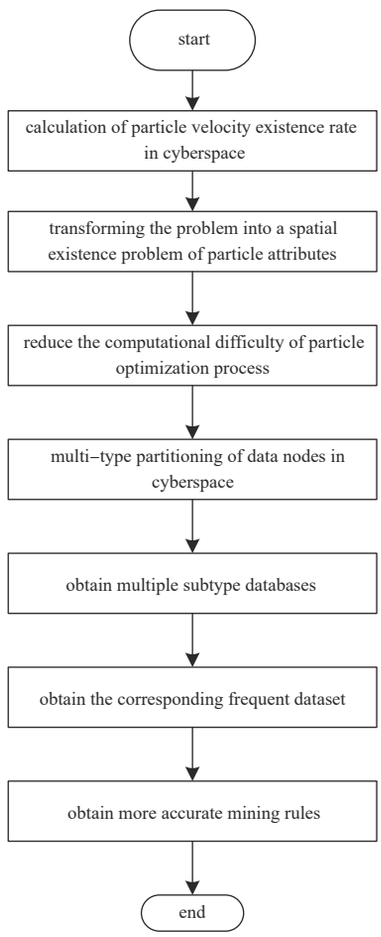

Fig.3 Process of mining rule generation
图3 挖掘规则生成流程

将网络漏洞特征数据节点所对应的数据库关联规则组成集合，其中，终端漏洞特征信息的聚类中心系数为M；粒子最优解为$m_{\max}$；动态无序化初始处理后的数据关联群体为s，其对应终端漏洞的特征关联集合的支持度与置信度分别满足$sup_{\min}$、$conf_{\min}$所对应的关联规则。

若在组成的关联集合中存在频繁项集A，将其划分为2个非空集合K与L，令其满足当前置信度所需的所有要求。通过计算其此时的置信度可得到关联输出特征节点组成的局部频繁项集，将其标记为X。同时，在关联模式下，通过遗传信息的属性划分，可将X划分为$\{X_1,X_2,\cdots,X_{s1}\}$，最后将所得子数据库$\{X_1,X_2,\cdots,X_{s1}\}$下的所有频繁数据集进行合并，生成关联规则。

2.3 黑盒遗传算法参量引入

通过上述分析可知，已获得的关联规则下，终端漏洞所对应的数据集在黑盒遗传算法的作用下可视其为一个模糊测试用例。当算法参量所得执行结果为0时，说明其关联规则下的源地址(fd)、目的地址(cmd)、缓冲字节长度(arg)参数均有效，漏洞挖掘尺度只需调整arg对应参数值使其满足变异要求即可。

黑盒遗传算法引入后，各个子数据集之间的关联函数发生变化，在遗传变异机制的作用下可得

$$\begin{cases} x_{i+1}=\mathrm{cmd}_i+\mathrm{arg}_{i+1}, & \mathrm{result}=0 \\ x_{i+1}=g\left(\mathrm{cmd}_i\right)+f\left(\mathrm{arg}_{i+1}\right), & \mathrm{result}=-1 \end{cases} \tag{3}$$

式中：f为按照变异要求配置arg概率函数；g为按照变异要求配置cmd概率函数；x_i为当前关联节点的个体状态；x_{i+1}为下一代关联节点的个体状态。

2.4 终端漏洞关联挖掘

按照上述关联规则及算法引入后的参量函数配置情况开展终端漏洞的关联挖掘。通过上述多项配置优化后可以发现，计算过程中挖掘特征参量组成的集合中存在一定的干扰影响信息，使挖掘过程在决策环节中部分配

置参量出现尺度异常情况，需进行关联修正。通过黑盒遗传关联修正方法对决策配置信息进行挖掘特征尺度配置信息的关联修正操作，从导入数据源头节点开始，用生成决策配置信息的训练样本进行关联修正[11-12]。

关联修正过程需在一个特征节点位置完成关联量的汇总，设定样本为B。若电力IoT终端漏洞数为N，在子类数据库中存在的关联修正特征节点数为Y个。关联修正过程的具体计算公式为：

$$P=\frac{\sum_{y=1}^{Y}N_y+0.3B}{B} \tag{4}$$

$$E_{\text{before}}=B\times P \tag{5}$$

$$\text{std}(g)=\sqrt{B\times P\times(1-P)} \tag{6}$$

$$MJ_{\text{up}}=E_{\text{before}}+\text{std}(g) \tag{7}$$

$$E_{\text{after}}=c+0.3 \tag{8}$$

式中：P为关联修正前挖掘关联特征分量的修正误差；E_{before}为对目标挖掘关联特征分量进行关联修正前的电力IoT终端漏洞总数误判阈值；$\text{std}(g)$为关联修正前误差标准量；MJ_{up}为对目标挖掘关联特征分量进行关联修正前的网络漏洞信息误判上限；E_{after}为对目标挖掘关联特征分量进行关联修正后的电力IoT终端漏洞总数误判阈值；c为关联因子。

若$E_{\text{after}}<MJ_{\text{up}}$，说明存在需要关联修正的偏差节点；若不满足上述关系，则不存在需要关联修正的偏差节点，此时自动生成决策配置信息。

挖掘过程中，对应配置规则下的支持度与置信度为挖掘精准与准确度的关键参量。因此，关联二者的参量条件包括挖掘加权系数Q、关联因子c_1及关联因子c_2的遗传速度。通过调整关联因子c_2的更新速度，优化漏洞挖掘特征信息对应的粒子群种类的丰富性。加权系数Q取值越大，说明黑盒遗传算法的全局挖掘能力越强。

若挖掘粒子性能发生线性下降，根据挖掘线性属性的整体适应度变化情况[13]，说明在电力IoT终端漏洞挖掘信息中存在一处梯度变化。该位置信息的挖掘过程可描述为：

$$\text{grad}(x_0,y_0)=\left[\frac{\partial f(x_0,y_0)}{\partial x},\frac{\partial f(x_0,y_0)}{\partial y}\right] \tag{9}$$

式中$f(x_0,y_0)$为电力物联网终端漏洞挖掘信息中梯度变化位置的函数关系。

挖掘关联修正前关联因子为C_1，挖掘关联修正后关联因子为C_2。关联修正效率所对应C_1位置上的状态系数不断减少，与之相应位置上的C_2状态系数不断增加，且允许规则节点在全局网络空间下进行挖掘。由此可得到挖掘关联修正特征节点速度v_i的计算公式为：

$$v_i=Qv_i+C_1r_1(p_i-x_i)+C_2r_2(p_j-x_j) \tag{10}$$

式中：r_1与r_2均为随机变量，取值范围为$[0,1]$；p_i为位于第i个关联修正节点位置上已搜索的最优修正系数下对应节点个体极值；p_j为位于第j个关联修正节点位置上已搜索的最优修正系数下对应节点个体极值；x_i为第i个修正关联节点；x_j为第j个修正关联节点；i与j均满足$0<i<j<M$，其中M为关联特征总数。

关联修正过程中扰动粒子t所在位置的适应度函数为：

$$X(t)=lF(t)+nT(t) \tag{11}$$

式中：l与n均为支持度与置信度参量指标所指向节点位置上的适应度函数的约束条件，在$0\leqslant l\leqslant 1$，$0\leqslant n\leqslant 1$时同时满足$l+n=1$；$F(t)$为支持度；$T(t)$为置信度。

将上述2个指标量与关联规则相结合，可进一步提升挖掘效果，尤其在漏洞特征搜索寻优速率方面，能够在不断提升更新粒子位置的同时，完成最优解或次优解的寻找。

将挖掘优化粒子的遗传种群数量设定为K，挖掘寻优粒子速度为r，则最终优化后的终端漏洞挖掘效率E_{f}为：

$$E_{\text{f}}=\frac{h_{\max}}{\sum_{i=0}^{K}h(r_i)} \tag{12}$$

式中：$h_{\max}$为漏洞挖掘所能达到的最大效率值；$h(r_i)$为第i个修正关联节点寻优粒子速度为r时，实际达到的漏洞挖掘效率。

3　应用测试

对上述方法的应用性能进行数据仿真，在仿真中通过多样本指标对比的方法验证所提方法的有效性与稳定性。用于对比的参照组为3种不同的挖掘算法，分别为：基于大数据的分析算法(参照A方法)、神经遗传算法(参照B方法)以及自适应神经差异特征分析算法(参照C方法)。为便于仿真过程描述，将本文所提方法命名为仿真样本。在相同的条件配置下，完成测试指标采集与分析。

3.1 仿真参数配置

为真实还原电力IoT运行环境，采用深圳市电力系统网络数据作为基础样本。在不考虑硬件服务器对测试数据结果影响的前提下，对其网络配置中的终端漏洞类型及数量进行配置，如表1所示。其中，数据运行方式采用Python IDE辅助优化运行，同时配合仿真测试工具Matlab与Net Framework模拟器一同完成数据仿真。

表1 仿真漏洞样本配置

Table1 Configuration of simulation vulnerability samples

number	types of vulnerabilities	number of samples
1	upload type	2 500
2	download type	2 500
3	injection type	2 500
4	Cross Site Request Forgery(CSRF) type	2 500

3.2 挖掘尺度测试

从各个漏洞类型中分别抽取500组，组成2 000组混合测试样本，设定挖掘基础指标值为1.0，采用4种挖掘方法对其进行关联挖掘。挖掘尺度计算公式为：

$$\delta=\sum_{x=1}^{X}\gamma_x T(t) \tag{13}$$

式中γ_x为节点关联度。

计算不同方法在不同漏洞下的挖掘尺度，生成曲线图，如图4~7所示。通过对比图4~7可以发现，4组不同的挖掘方法针对4组不同漏洞类型所表现出的挖掘性能各不相同，且不同算法与不同漏洞之间的性能差异较大。逐一对其进行分析。

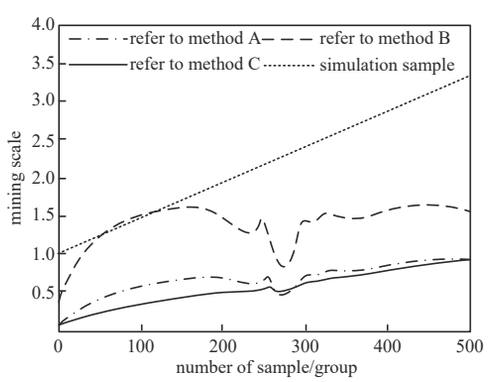

Fig.4 Mining scale of downloadable vulnerability samples

图4 下载型漏洞样本挖掘尺度

参照A方法的整体挖掘效果并不理想，其挖掘尺度均值经过计算为0.89，未满足基础指标值1.0，且对应4种不同漏洞的挖掘过程波动变化较大，因此整体挖掘尺度无法满足测试要求。

参照B方法相较参照A方法，整体尺度指标有所增长。除上传型漏洞挖掘曲线指标偏低外，其他3种类型漏洞的指标均值均超过基础指标值1.0。但结合曲线波动情况看，参照B方法的挖掘尺度控制效果较差，扰动影响范围较大，且影响变化频繁。综合上述指标分析，其效果很难满足测试要求。

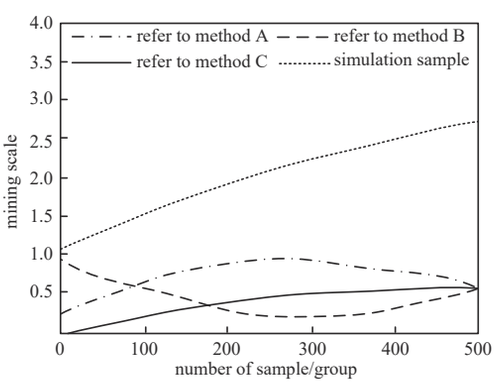

Fig.5 Mining scale of uploaded vulnerability samples

图5 上传型漏洞样本挖掘尺度

参照C方法的挖掘曲线稳定性明显优于上述2种参照方法，且曲线控制一致性表现优秀。但从指标值看，参照C方法的指标值整体偏小，均值尺度仅为0.45，因此该方法的漏洞挖掘尺度不能满足测试要求。

仿真样本的挖掘尺度整体性较好，且尺度控制效果与参照C方法相同，表现优秀。但不同的是，仿真样本所得挖掘曲线数值较大，且均值指标为参测方法中最大，整体表现最佳。

综合上述分析，可以判定仿真样本的漏洞挖掘尺度符合设计预期，满足测试相关指标要求。

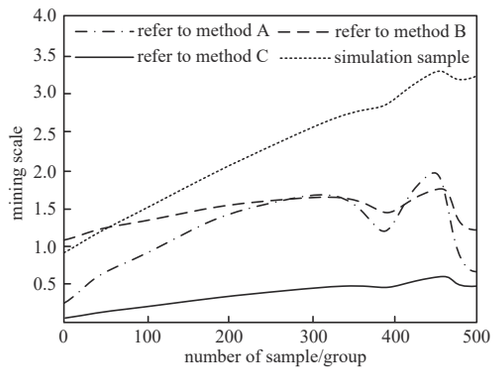

Fig.6 Mining scale of injected vulnerability samples
图6 注入型漏洞样本挖掘尺度

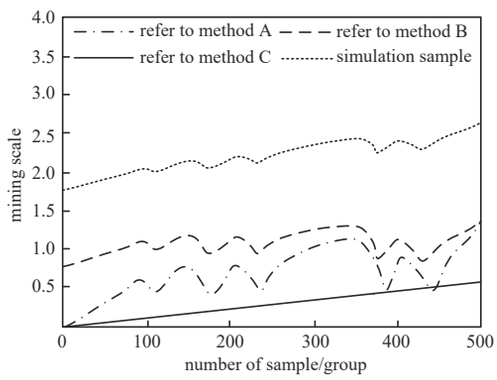

Fig.7 Mining scale of CSRF vulnerability samples
图7 CSRF 型漏洞样本挖掘尺度

3.3 挖掘偏差测试

测试漏洞样本全局参与测试，每种漏洞测试结果划分为5组计算均值偏差，由此得到4种漏洞的20组挖掘均值偏差统计，如表2所示。由表2数据的观察对比分析可以发现，4组挖掘方法在不同漏洞连续挖掘状态下，均值偏差指标差异较大，从数值大小与数值变化情况看，仿真样本所得指标最佳，参照A方法所得指标最差，参照C方法所得指标优于参照B方法，由此按照指标表现性能由高到低的顺序，4组挖掘方法的稳定性排列为仿真样本–参照C方法–参照B方法–参照A方法。

表2 针对4种漏洞不同算法所得挖掘均值的偏差统计

Table2 Statistics of mining mean deviation of four different vulnerability algorithms

serial number	mean deviation of upload type vulnerability mining			
	simulation sample	refer to method A	refer to method B	refer to method C
1	0.1	6.4	3.7	2.4
2	0.1	5.2	4.1	2.0
3	0.1	5.4	3.3	2.4
4	0.1	5.1	3.5	2.4
5	0.1	5.4	3.6	2.0
serial number	mean deviation of download type based vulnerability mining			
	simulation sample	refer to method A	refer to method B	refer to method C
1	0.1	4.3	3.1	2.4
2	0.1	4.2	3.3	2.0
3	0.2	4.2	3.5	2.0
4	0.2	4.7	3.6	2.0
5	0.2	4.3	3.5	2.0
serial number	mean deviation of injection type vulnerability mining			
	simulation sample	refer to method A	refer to method B	refer to method C
1	0.1	4.4	2.7	2.4
2	0.2	4.0	3.5	2.4
3	0.1	5.7	2.6	2.0
4	0.1	5.6	2.4	2.0
5	0.1	4.0	2.8	2.0
serial number	mean deviation of CSRF type vulnerability mining			
	simulation sample	refer to method A	refer to method B	refer to method C
1	0.2	4.6	3.2	2.4
2	0.1	5.7	3.0	2.0
3	0.3	5.6	3.1	2.4
4	0.1	5.8	3.0	2.0
5	0.1	4.7	3.6	2.0

4 结论

基于电力物联网络终端分布特点与黑盒遗传算法的特性，对其漏洞挖掘参量进行针对性优化，通过重构挖掘关联规则，量化不同漏洞挖掘参量及其特征尺度，从而获得最佳的挖掘效果，为漏洞挖掘研究提供了新的解决方案。但是，从数据仿真单元可以看出，提出方法在局部数据控制方面还存在不足，结合网络环境的实际变化，在现阶段还无法有效预测网络不确定性因素的分布范围与变化，因此需要较长的一段时间去总结积累方法在实际应用中的数据，通过数据的累积作用，配合多样性训练算法，不断提升挖掘特征样本精确度，将挖掘方法调整至最佳状态。

参考文献：

[1] 樊志强,王洪宇,刘日昇. 命令行接口模糊测试漏洞挖掘研究及应用[J]. 网络安全与数据治理, 2023,42(7):61-66,78. (FAN Zhiqiang,WANG Hongyu,LIU Risheng.Research and application of CLI vulnerability mining by fuzz testing[J]. Cyber Security and Data Governance, 2023,42(7):61-66,78.) doi:10.19358/j.issn.2097-1788.2023.07.010.

[2] 陈泽,邬桐,左晓军,等. 基于知识图谱的电力网络安全漏洞挖掘系统设计[J]. 制造业自动化, 2023,45(7):100-105,110. (CHEN Ze,WU Tong,ZUO Xiaojun, et al. Design of power network security vulnerability mining system based on knowledge graph[J]. Manufacturing Automation, 2023,45(7):100-105,110.) doi:10.3969/j.issn.1009-0134.2023.07.021.

[3] 王勇,裘建开,严钰君,等. 基于弱监督学习的电力信息动态漏洞挖掘系统[J]. 电子设计工程, 2023,31(13):114-117,122. (WANG Yong, QIU Jiankai, YAN Yujun, et al. Power information dynamic vulnerability mining system based on weakly supervised learning[J]. Electronic Design Engineering, 2023,31(13):114-117,122.) doi:10.14022/j.issn1674-6236.2023.13.024.

[4] PAVASKAR M,KAKADE S,GOND S,et al. Security and intrusion detection in mobile ad hoc network[J]. Journal of Mechanics and MEMS, 2020,12(1):27-32.

[5] 余入丽,吴涤,马先平,等. 基于数据挖掘的电力无线通信网络漏洞检测[J]. 电子设计工程, 2023,31(13):163-166,172. (YU Ruli,WU Di,MA Xianping,et al. Vulnerability detection of power wireless communication network based on data mining[J]. Electronic Design Engineering, 2023,31(13):163-166,172.) doi:10.14022/j.issn1674-6236.2023.13.034.

[6] 顾守珂,陈文. 基于增强 AST 的图神经网络函数级代码漏洞检测方法[J]. 计算机科学, 2023,50(6):283-290. (GU Shouke, CHEN Wen. Function level code vulnerability detection method of graph neural network based on extended AST[J]. Computer Science, 2023,50(6):283-290.) doi:10.11896/jsjkx.220600131.

[7] 李爽,刘海鹏,郭兰图. 基于电磁环境数据的信息挖掘与关联分析[J]. 太赫兹科学与电子信息学报, 2022,20(1):8-15. (LI Shuang,LIU Haipeng,GUO Lantu. Information mining and association analysis based on electromagnetic environment data[J]. Journal of Terahertz Science and Electronic Information Technology, 2022,20(1):8-15.) doi:10.11805/TKYDA2021168.

[8] 苏东禹,姜宇,谢景海,等. 电力通信系统安全漏洞自动挖掘方法[J] .信息技术, 2023,47(3):128-132,138. (SU Dongyu,JIANG Yu, XIE Jinghai, et al. Automatic mining method of security vulnerabilities in power communication system[J]. Information Technology, 2023,47(3):128-132,138.) doi:10.13274/j.cnki.hdzj.2023.03.024.

[9] 程亚维,王东霞. 基于网络爬虫技术的网页SQL注入漏洞检测方法[J]. 信息与电脑(理论版), 2023,35(4):236-238. (CHENG Yawei, WANG Dongxia. Web page SQL injection vulnerability detection method based on Web crawler technology[J]. China Computer & Communication(Theory Edition), 2023,35(4):236-238.) doi:10.3969/j.issn.1003-9767.2023.04.068.

[10] 佘庚达,付才,岑泽威,等. 基于适应度和输入约束模型的内核驱动漏洞挖掘[J]. 计算机应用研究, 2023,40(7):2151-2156. (SHE Gengda,FU Cai,CEN Zewei, et al. Kernel driver vulnerability mining based on fitness and input constraint model[J]. Application Research of Computers, 2023,40(7):2151-2156.) doi:10.19734/j.issn.1001-3695.2022.11.0772.

[11] 吕国曙,鞠磊. 基于数据挖掘的电力系统网络安全漏洞识别方法[J]. 电工技术, 2023(2):49-51. (LYU Guoshu, JU Lei. Network security vulnerability identification method for power system based on data mining[J]. Electric Engineering, 2023(2):49-51.) doi:10.19768/j.cnki.dgjs.2023.02.014.

[12] 吕乐乐,董伟,赵云飞,等. 基于Q算法的认证协议漏洞挖掘技术研究[J]. 电子技术应用, 2022,48(10):63-68. (LYU Lele, DONG Wei,ZHAO Yunfei,et al. Research on the vulnerability mining technology of authentication protocol based on Q-learning [J]. Application of Electronic Technique, 2022,48(10):63-68.) doi:10.16157/j.issn.0258-7998.222641.

[13] 于英涛,吴明虎. 欺骗攻击环境下网络信息安全漏洞深度挖掘方法[J]. 自动化技术与应用, 2022,41(7):91-93,141. (YU Yingtao, WU Minghu. Deep mining method of network information security vulnerability in spoofing attack environment[J]. Techniques of Automation and Applications, 2022,41(7):91-93,141.) doi:10.20033/j.1003-7241(2022)07-0091-04.

作者简介：

王　健(1978-)，男，硕士，高级工程师，主要研究方向为网络安全、通信工程.email:LlIOo0175a@126.com.

付志博(1990-)，男，本科，工程师，主要研究方向为信息安全.

农彩勤(1990-)，女，硕士，工程师，主要研究方向为云计算安全、信息安全.

刘家豪(1984-)，男，本科，工程师，主要研究方向为网络安全运营.

许伟杰(1993-)，男，本科，工程师，主要研究方向为网络安全攻防.