

# 基于 Agent-Based 模型和群智能算法的 供电信息通信监控中心威胁感知方法

陶程栋<sup>1†</sup>, 梅峰<sup>1</sup>, 王强强<sup>2</sup>

(1. 国网浙江省电力有限公司信息通信分公司, 浙江 杭州 310016; 2. 浙江大有实业有限公司钱塘分公司, 浙江 杭州 310000)

**摘 要:**针对采样结果泛化程度较差导致感知粒子覆盖率较低、监控中心威胁样本召回率较低的问题, 设计了基于 Agent-Based 模型和群智能算法的供电信息通信监控中心威胁感知方法。首先, 对供电信息通信监控中心数据进行采样和分析, 并对采样结果进行泛化处理和归约计算; 然后, 基于 Agent-Based 模型构建供电信息通信监控中心威胁本体溯源函数, 并计算 Agent 的感知能力; 最后, 采用群智能算法对构建威胁本体溯源函数的感知结果进行优化处理, 实现对供电信息通信监控中心威胁的精确感知; 最终完成供电信息通信监控中心威胁感知方法设计。实验结果表明, 该方法在实际应用中, 召回率更高, 感知效果更好。

**关键词:** Agent-Based 模型; 群智能算法; 供电信息; 通信监控中心; 感知方法; 方法设计

中图分类号: G642

文献标识码: A

## A Threat Perception Method for Power Supply Information Communication Monitoring Center Based on Agent-Based Model and Group Intelligence Algorithm

TAO Chengdong<sup>1†</sup>, MEI Feng<sup>1</sup>, WANG Qiangqiang<sup>2</sup>

(1. Information & Telecommunication Branch, State Grid Zhejiang Electric Power Co., Ltd., Hangzhou, Zhejiang 310016, China;

2. Qiantang Branch of Zhejiang Dayou Industrial Co., Ltd., Hangzhou, Zhejiang 310000, China)

**Abstract:** In response to the problem of poor generalization of sampling results resulting in low coverage of perceived particles and low recall rate of threat samples in monitoring centers, a threat perception method for power supply information communication monitoring centers based on the Agent-Based model and swarm intelligence algorithm was designed. After considering the actual situation of the power supply information communication monitoring center, it is sampled and analyzed, and the sampling results are generalized and reduced. Based on the Agent-Based model, the threat ontology traceability function of the power supply information communication monitoring center is constructed, and the perception ability of the agent is calculated. Under the action of swarm intelligence algorithms, the perception results of the threat ontology traceability function are optimized, realize accurate perception of threats to power supply information communication monitoring centers. Through the above design, the design of the threat perception method for the power supply information communication monitoring center is completed. The experimental results show that this method has a higher recall rate and better perception effect in practical applications.

**Key words:** Agent-Based model; swarm intelligence algorithm; power supply information; communication monitoring center; perception methods; method design

供电信息通信监控中心是电力系统的重要组成部分,它负责监控电力设备的运行状态、控制电力系统的运行参数以及保障电力系统的稳定运行。然而,随着信息技术的不断发展,针对供电信息通信监控中心的威胁行为越来越多,如网络攻击、病毒入侵、恶意软件等。这些威胁行为不仅会对供电信息通信监控中心的正常运行造成影响,还会对整个电力系统的稳定运行带来极大的安全隐患。因此,开展供电信息通信监控中心威胁感知方法的研究对于保障电力系统的安全稳定运行具有重要的意义。现有的感知方法由于技术的限制,无法实现对威胁行为的快速感知与预警,也难以确定威胁行为的类型和来源,导致感知效率较低,感知效果较差。在上述背景下,不少研究学者针对感知方法展开了研究,并提出了自己的想法。

文献[1]采集网络空间安全领域的多源数据,并提取数据中的关键信息,建立网络空间安全领域的知识库,在知识图谱的作用下,对提取的关键信息进行分类和聚类分析,构建相应的威胁感知模型,对异常行为和潜在威胁进行快速感知,并制订相应的应对措施,但该方法的感知效果较差。文献[2]收集网络运行状态信息,提取有效的网络运行特征,在多信息融合的作用下,提取融合信息的关键特征的模式,由此感知光纤网络中的威胁。实验结果表明,该方法的感知时间较长。文献[3]采集施工现场危险区域和关键位置的视频数据,利用图像处理技术对采集的视频数据进行分析,利用感知的目标特征构建联合交集模型,确定不同特征之间的关联情况,实时感知可能出现的侵入行为,但该方法的感知成本较高。

在以往研究的基础上,本文设计了基于 Agent-Based 模型和群智能算法的供电信息通信监控中心威胁感知方法。根据供电信息通信监控中心的实际情况,对其进行数据采样,在 Agent-Based 模型的作用下,构建供电信息通信监控威胁本体溯源函数,利用群智能算法对供电信息通信监控中心出现的威胁进行快速感知。本文设计的方法能够实现供电信息通信监控中心威胁行为的实时监测和预警,提高供电信息通信监控中心的安全性和稳定性<sup>[4-5]</sup>。同时,本文深入研究了供电信息通信监控中心面临的威胁类型和攻击手段,为防范和应对威胁提供理论支持,对于保障国家和社会稳定具有重要意义。

## 1 供电信息通信监控中心威胁感知方法设计

### 1.1 供电信息通信监控中心数据采样及归约

供电信息通信监控中心的数据采样主要是从实时数据流中按照一定的规则和频率提取样本数据。这些数据包括网络流量、系统日志、设备状态等信息。通过对这些数据进行采样和分析,可以及时发现异常行为和潜在威胁,保障供电信息通信系统的安全和稳定运行<sup>[6]</sup>。其具体的采样结果如下所示:

$$N(t) = \alpha_1 \text{Net}(t) + \alpha_2 \text{Log}(t) + \alpha_3 \text{Set}(t) \quad (1)$$

式中,  $N(t)$  表示供电信息通信监控中心数据采样结果,  $\text{Net}(t)$  表示采样的网络流量数据,  $\alpha_1$  表示网络流量数据所占的比例,  $\text{Log}(t)$  表示采样的系统日志数据,  $\alpha_2$  表示系统日志数据所占比例,  $\text{Set}(t)$  表示采样的设备状态数据,  $\alpha_3$  表示设备状态数据所占的比例。通过上述公式,完成对数据的采样处理。在上式基础上,为保证采样数据的质量,需要对数据进行优化处理,包括对数据进行数据泛化和数据归约处理。其中,数据泛化处理能够将具体的数据实例归纳为更抽象、更高级别的概念或类别,使数据更加简洁、易于理解和分析<sup>[7]</sup>。数据泛化处理的具体过程如下所示:

$$N(t)' = \frac{N(t) - N(t)_{\min}}{N(t)_{\max} - N(t)_{\min}} \times [N(t)'_{\max} - N(t)'_{\min}] + N(t)_{\min} \quad (2)$$

式中,  $N(t)'$  表示数据泛化处理的结果,  $N(t)_{\max}$  表示采样数据的最大值,  $N(t)_{\min}$  表示采样数据的最小值,  $N(t)'_{\max}$  表示数据泛化处理的最大值,  $N(t)'_{\min}$  表示数据泛化处理的最小值。通过上述公式,完成对数据的数据泛化处理。数据归约处理能够减小数据集的大小,删除数据冗余的不必要信息,并尽可能地保留其原始信息,降低数据的维度和复杂性,从而提高数据处理效率和准确性,为后续感知供电信息通信监控中心威胁提供可靠的数据支持<sup>[8]</sup>。数据归约的具体计算过程如下所示:

$$I = H[N(t)] - H[N(t)|A] \quad (3)$$

式中,  $I$  表示数据归约处理的结果,  $H[N(t)]$  表示数据采样结果的熵值,  $H[N(t)|A]$  表示在属性  $A$  下数据采样结果的熵值。通过上述公式,完成对数据的归约处理。在上述过程中,通过对数据的数据泛化和归约处理,提高了数据的质量,完成了数据优化处理,为后续构建威胁本体溯源函数奠定基础。

1.2 供电信息通信监控中心威胁本体溯源函数

在上述设计的基础上,利用供电信息通信监控中心的采样结果,在 Agent-Based 模型的作用下,构建供电信息通信监控中心威胁本体溯源函数。其中,Agent-Based 模型是一种建模方法,能够将复杂系统中的个体视为具有自主意识、行为和相互作用的 Agent,在构建威胁本体溯源函数时,利用 Agent-Based 模型将威胁类型定义为一种行为模式,通过模拟该行为模式对威胁类型进行溯源和分析<sup>[9]</sup>。威胁本体溯源函数构建流程具体如图 1 所示。

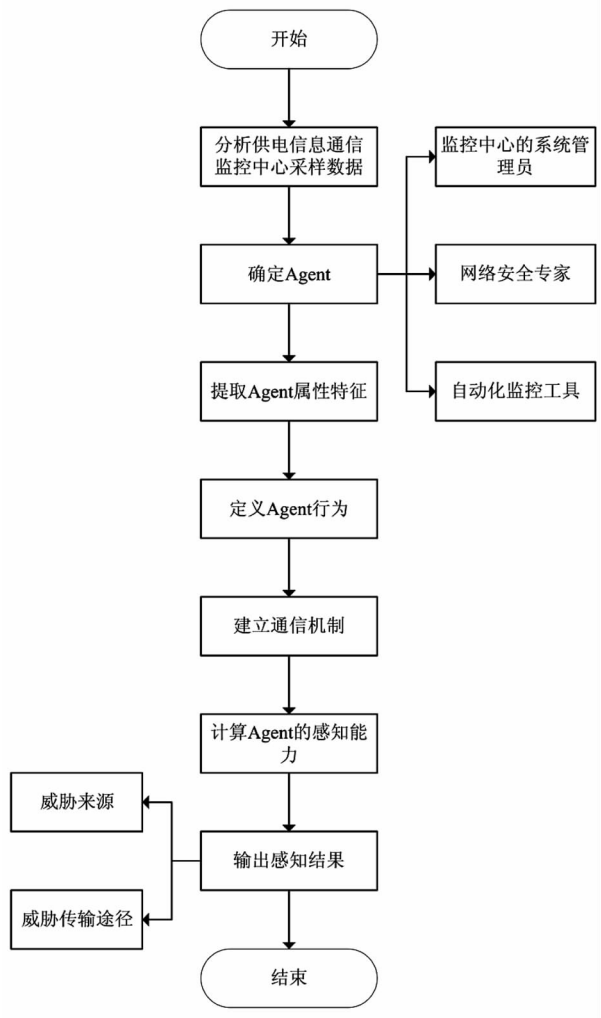


图 1 威胁本体溯源函数构建流程

如图 1 所示,利用 Agent-Based 模型,先对供电信息通信监控中心进行分析,确定相应的 Agent,如监控中心的系统管理员、网络安全专家或自动化监控工具等都可以成为 Agent。根据 Agent 的属性,提取其自身的特征,并根据其所处的环境定义其自身的行为,由此建立相应的通信机

制,并通过该通信机制进行信息传递,防止潜在威胁对模型的干扰<sup>[10]</sup>。在此基础上,通过计算 Agent 对网络威胁的感知能力,生成对应的威胁本体溯源函数,对供电信息通信监控中心威胁的来源、传输途径进行描述。基于 Agent-Based 模型构建的威胁本体溯源函数如下所示:

$$M = f \left[ \begin{matrix} \text{Agents}, \text{Agent1}, \text{Agent2}, \\ \text{Agent3}, \text{Threat}, \text{Sources} \end{matrix} \right] \quad (4)$$

式中,  $M$  表示威胁本体溯源函数,  $\text{Agents}$  表示确定的 Agent 实体,  $\text{Agent1}$  表示 Agent 的属性,  $\text{Agent2}$  表示 Agent 的行为模式,  $\text{Agent3}$  表示 Agent 之间的通信机制,  $\text{Threat}$  表示监控中心出现的威胁来源,  $\text{Sources}$  表示对威胁的响应结果。通过上述公式,完成对供电信息通信监控中心威胁本体溯源函数的构建。

为保证威胁本体溯源函数的性能,需要对 Agent 的感知能力进行计算。在计算过程中,针对供电信息通信监控中心的数据进行特征提取,再利用 Agent 提取其中较为有用的特征,并与已有的数据集进行匹配,从而感知到其中威胁<sup>[11]</sup>。Agent 的感知能力计算过程如下所示:

$$R = f \left[ \begin{matrix} \text{Features}, \text{Agent4}, \text{Data1}, \text{Data2}, \\ \text{Agent5}, \text{Evaluation} \end{matrix} \right] \quad (5)$$

式中,  $R$  表示 Agent 的感知能力,  $\text{Features}$  表示供电信息通信监控中心数据的特征,  $\text{Agent4}$  表示 Agent 的能力,  $\text{Data1}$  表示供电信息通信监控中心数据集的质量,  $\text{Data2}$  表示供电信息通信监控中心数据集的大小,  $\text{Agent5}$  表示 Agent 的感知过程,  $\text{Evaluation}$  表示影响 Agent 感知的影响因素。通过上述公式,计算出 Agent 的感知能力,提高构建的供电信息通信监控中心威胁本体溯源函数的性能,为后续更为精准地感知供电信息通信监控中心的威胁奠定基础<sup>[12]</sup>。

1.3 供电信息通信监控中心威胁感知

将构建的威胁本体溯源函数作为基础,利用群智能感知算法对供电信息通信监控中心的威胁进行感知。群智能算法是一种基于群体智能的优化和搜索算法,它利用群体中个体的协作和信息共享来寻找复杂问题的最优解或可行解。在本文的设计中,利用群智能算法,对构建的威胁本体溯源函数进行处理,能够优化威胁感知的结果,进一步提高感知效果<sup>[13]</sup>。其具体感知流程如图 2 所示。

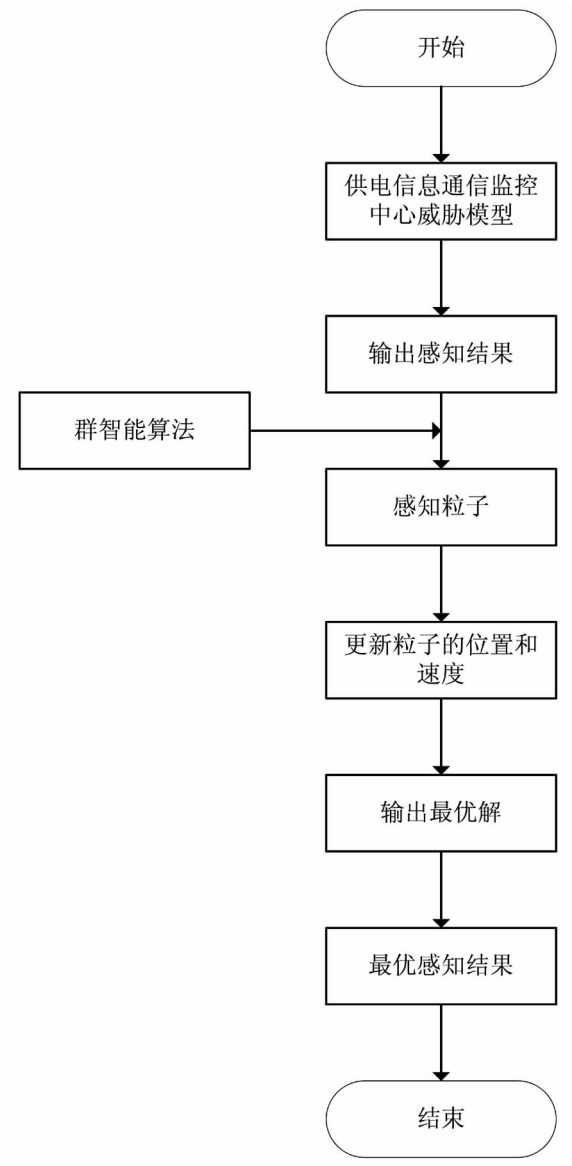


图 2 基于群智能算法的供电信息通信监控中心威胁感知流程

如图 2 所示,在上述感知流程中,利用威胁本体溯源函数,对供电信息通信监控中心的威胁进行溯源,输出相应的感知结果,在群智能算法的作用下,将该感知结果看作一种粒子,对粒子的速度和位置进行更新,从而得到最优解<sup>[14]</sup>。上述更新过程,也是对感知结果的多次优化,从而得到最为精确的感知结果,保证感知的效果。在群智能算法的作用下,粒子的更新速度和位置如下所示:

$$\begin{cases} v_{ij} = w \times v_{ij} + c_1 \times \text{rand}() \times (p_{ij} - x_{ij}) + c_2 \times \text{rand}() \times (g_{ij} - x_{ij}) \\ x_{ij} = x_{ij} + v_{ij} \end{cases} \quad (6)$$

式中,  $v_{ij}$  表示粒子更新后的速度,  $v_{ij}$  表示粒子的初始速度,  $w$  表示粒子的惯性权重值,  $c_1$ 、 $c_2$  表

示粒子在运行过程中的感知因子,  $p_{ij}$  表示筛选过程中的个体最优解,  $g_{ij}$  表示全局最优解,  $x_{ij}$  表示粒子更新后的位置,  $x_{ij}'$  表示粒子的初始位置。通过上述公式,对粒子的速度和位置进行更新<sup>[15]</sup>,以此为基础,实现对感知结果的优化。

2 实验测试

为提高实验结果的可靠性,设置对照实验。其中,本文设计的基于 Agent-Based 模型和群智能算法的供电信息通信监控中心威胁感知方法为方法 1,基于特征熵值和关联规则的供电信息通信监控中心威胁感知方法为方法 2,基于多信息融合和知识图谱的供电信息通信监控中心威胁感知方法为方法 3。

2.1 实验准备

为验证本文设计的基于 Agent-Based 模型和群智能算法的供电信息通信监控中心威胁感知方法在实际应用中的效果,进行实验测试。实验中,以某供电信息通信监控中心为实验对象,构建相应的实验环境。具体的实验环境如图 3 所示。



图 3 实验环境

如图 3 所示,在上述实验环境中,传感器和监控设备用于实时监控某供电信息通信监控中心的实时状况,利用数据采集仪从传感器上采集相关数据信息,每分钟需要采集 10% 的某供电信息通信监控中心的实时数据,采集的数据分别为监控中心的网络流量数据、系统日志和事件响应记录数据等。将采集的数据传输到计算机上,利用计算机对采集的数据进行优化处理。实验使用的计算机参数为:主频 Intel Xeon421R 2.4 GHz,12 核处理器,128 GB 的内存,64 TB 的硬盘,RTX3090 GPU 显卡。利用本文设计的方法对采集的数据进行优化处理,其优化处理的效果如图 4 所示。

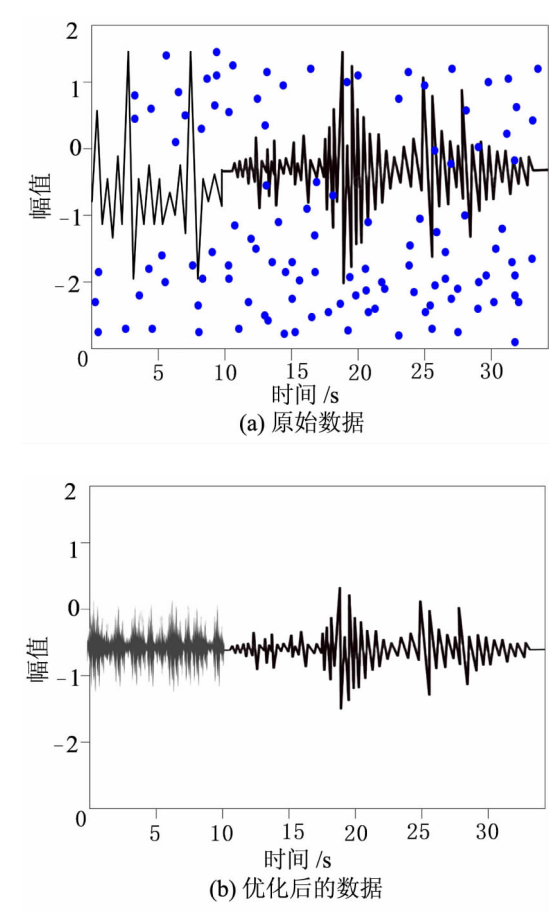


图 4 实验数据归约处理结果

如图 4 所示,在上述处理结果中,采集的实验数据不仅波动幅度较大,存在很大的不稳定性,还存在大量的离散数据点,会对感知结果造成一定的干扰,利用本文设计的方法对其进行处理,减小了数据的波动幅度,并将数据中的离散数据点全部去除,减少了外在因素的干扰,提高了实验结果的可靠性。

2.2 实验结果讨论

为对比上述三种方法在实际应用中的效果,实验以召回率为评价指标,对比三种方法的性能。实验中,利用三种方法对实验数据集进行感知,统计其感知到的威胁,并计算方法的召回率。具体统计结果如表 1 所示。

如表 1 所示,在上述实验结果中,通过多次实验可知,方法 1 的召回率数值远高于其他两种方法,召回率平均值为 97.89%,感知效果较好。在实际应用中,方法 1 对供电信息通信监控中心威胁的感知效果更好,能够准确感知到监控中心面临的威胁,减少相应的损失。

表 1 三种方法的感知结果

| 实验次数 | 三种方法的召回率/% |       |       |
|------|------------|-------|-------|
|      | 方法 1       | 方法 2  | 方法 3  |
| 1    | 99.62      | 82.13 | 71.56 |
| 2    | 97.46      | 83.14 | 70.36 |
| 3    | 98.12      | 85.65 | 71.35 |
| 4    | 96.69      | 86.32 | 70.69 |
| 5    | 96.84      | 86.57 | 71.25 |
| 6    | 98.32      | 88.23 | 72.58 |
| 7    | 99.14      | 86.15 | 71.26 |
| 8    | 97.68      | 84.39 | 72.69 |
| 9    | 98.54      | 86.12 | 72.55 |
| 10   | 98.65      | 84.59 | 72.39 |

为进一步验证上述三种方法在实际应用中的效果,以方法的感知粒子覆盖率为评价指标,进行实验测试。覆盖率是指不同方法能够感知到的数据数量与数据集的总量的比例,感知粒子覆盖率越高,说明方法对数据集的感知效果更好,能够减少对供电信息通信监控中心的错误感知或感知遗漏,保证感知结果的准确性。感知粒子覆盖率的具体统计结果如图 5 所示。

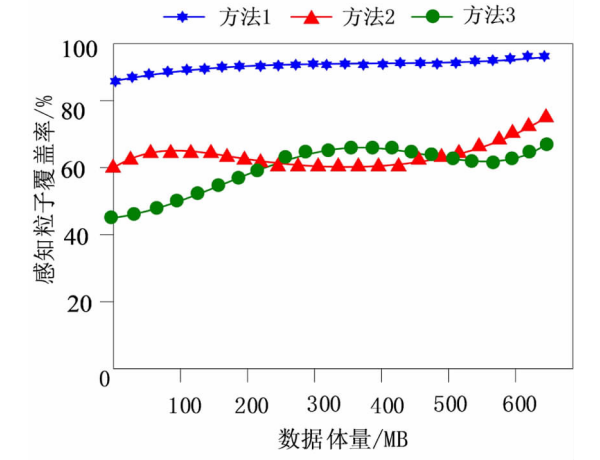


图 5 三种方法的感知粒子覆盖率

如图 5 所示,在不同数据体量下,方法 1 的感知粒子覆盖率随着数据体量上升而不断上升,且覆盖率一直处于较高水平,方法 2 和方法 3 的覆盖率水平则相对较差,且波动幅度较大。在实际应用中,方法 1 由于覆盖率较高,出现的感知遗漏情况减少,能够保证供电信息通信监控中心的稳定性,减少其在运行过程中受到的威胁。

综上所述,本文设计的基于 Agent-Based 模型和群智能算法的供电信息通信监控中心威胁感知

方法在实际应用中的召回率、覆盖率较高,实际应用效果较好。

### 3 结 论

在面对复杂的供电信息通信系统时,监控中心需要对潜在的威胁进行快速、准确的感知和响应。本文提出了一种基于 Agent-Based 模型和群智能算法的威胁感知方法,旨在提高监控中心的威胁感知能力。该方法利用 Agent-Based 模型的自组织和适应性,能够有效地感知和识别供电信息通信系统中的异常和威胁。同时,通过群智能算法的协作和信息共享机制,能够提高威胁感知的准确性和效率,具有广泛的应用前景和重要的研究价值。在未来的研究中,可以进一步探讨如何将该方法与其他安全技术和防护措施相结合,以提供更加全面和高效的供电信息通信安全保障。

### 参考文献

[1] 石波,于然,朱健. 基于知识图谱的网络空间安全威胁感知技术研究[J]. 信息安全研究,2022,8(8):845—853.

[2] 李秀峰,王崇霞. 基于多信息融合的光纤网络威胁智能感知方法[J]. 激光杂志,2021,42(10):138—142.

[3] 刘泽锋,韩豫,李文涛,等. 视觉联合交集下施工危险区域侵入行为动态感知方法[J]. 安全与环境工程,2023,30(4):18—25.

[4] 马翔,钱肖,吕磊炎等. 基于机器视觉和动态阈值的电气设备

运行异常关联感知方法[J]. 微型电脑应用,2023,39(6):62—65.

[5] 赵丽军,邢作霞,刘洋等. 基于数据分析的风电机组偏航机构异常感知方法研究[J]. 太阳能学报,2022,43(1):108—115.

[6] 王珂. 基于用电信息采集系统的末端负荷态势感知方法研究[J]. 山东电力高等专科学校学报,2021,24(5):20—22.

[7] 张启雷,孙斌. 改进 Laplace 先验下的复数域多任务贝叶斯压缩感知方法[J]. 国防科技大学学报,2023,45(5):150—156.

[8] 林立鑫,涂剑峰,喻燕华,等. 基于改进决策树的通信网络安全态势感知方法[J]. 信息与电脑(理论版),2023,35(9):223—225.

[9] 边泽英,赵鸿铎,彭科迪,等. 基于分布式振动传感的车辆轴载感知方法[J]. 同济大学学报(自然科学版),2023,51(8):1157—1167.

[10] 李茜瑶,李宏海,黄烨然,等. 基于多源数据的微观路段交通状态感知方法[J]. 公路交通科技,2022,39(S1):77—83.

[11] 魏伟. 基于改进 K-means 算法的校园网络环境安全态势感知方法[J]. 信息与电脑(理论版),2023,35(12):96—98.

[12] 李明杰,刘小飞. 基于毫米波传感器与激光雷达信号融合的自动驾驶障碍物感知方法[J]. 激光杂志,2023,44(6):199—203.

[13] 孟祥艳,张欣,张峰,等. 融合迁移特征学习的生物启发网络用于可见光成像室内位置感知方法[J]. 中国激光,2023,50(10):176—183.

[14] 刘凯,宫旻,李晓峰,等. 基于无线传感器网络的智能配电网安全态势感知方法[J]. 电子设计工程,2023,31(12):142—146.

[15] 陈宗汉,徐永海,陶顺,等. 面向负荷管理过程的工业用户安全用电风险态势感知方法[J]. 高电压技术,2023,49(7):2796—2805.