

一种基于MSCPO-BiGRU的智慧水利网络安全态势预测方法

夏卓群¹, 周子豪¹, 邓斌², 康琛³

(1. 长沙理工大学 计算机与通信工程学院; 2. 长沙理工大学 水利与环境工程学院;
3. 湖南省水旱灾害防御事务中心 网信技术部, 湖南 长沙 410000)

摘要: 智慧水利是国家关键信息基础设施的核心行业与关键领域, 对其网络安全态势预测技术进行研究可有效提升行业整体的安全防护能力与风险预警水平。为解决智慧水利网络安全态势预测的复杂性和多变性问题, 提出一种基于双向门控循环单元(BiGRU)与多种群混沌粒子优化算法(MSCPO)的预测方法。首先, 采用MSCPO算法寻优BiGRU的超参数, 包括迭代次数、学习率和隐含层节点数; 其次, 使用优化后的BiGRU单元进行态势预测。在SWaT数据集上的实验结果表明, 所提方法的均方误差为0.002 8, 平均绝对误差为10.97%, 决定系数为0.916 1。与传统算法相比, 所提方法的预测准确性和稳定性更高, 可为智慧水利网络安全建设提供有效支撑。

关键词: 智慧水利; 网络安全态势预测; BiGRU; MSCPO

DOI: 10.11907/rjdk.251033

中图分类号: TP183

文献标识码: A

文章编号: 1672-7800(2026)004-0089-09

扫描二维码阅读全文: 

A Network Security Situation Prediction Method for Intelligent Water Conservancy Based on MSCPO-BiGRU

XIA Zhuoqun¹, ZHOU Zihao¹, DENG Bin², KANG Chen³

(1. School of Computer and Communication Engineering, Changsha University of Technology; 2. School of Hydraulic and Environmental Engineering, Changsha University of Technology; 3. Network Information Technology Department of Hunan Provincial Flood and Drought Disaster Prevention Center, Changsha 410000, China)

Abstract: Intelligent water conservancy serves as the core industry and key field of national key information infrastructure. Research on its network security situation prediction technology can effectively enhance the industry's overall security protection capability and risk early-warning level. To address the complexity and variability in predicting the security situation of intelligent water conservancy networks, a prediction method based on Bidirectional Gated Recurrent Unit (BiGRU) and Multi-Swarm Chaotic Particle Optimization Algorithm (MSCPO) is proposed. This method first employs the MSCPO algorithm to optimize the hyperparameters of BiGRU, including the number of iterations, learning rate, and number of hidden layer nodes. Subsequently, the optimized BiGRU unit is used for situation prediction. Experimental results on the SWaT dataset demonstrate that the proposed method achieves a mean square error of 0.002 8, an average absolute error of 10.97%, and a determination coefficient of 0.916 1. Compared with traditional algorithms, the proposed method exhibits higher prediction accuracy and stability, providing effective support for the construction of intelligent water conservancy network security.

Key Words: intelligent water conservancy; network security situation prediction; BiGRU; MSCPO

0 引言

智慧水利充分依托物联网、云计算、大数据等新兴信

息通信技术, 深度赋能水利规划、工程建设、运行管控以及社会服务等各个环节, 有力推动水利行业整体向智慧化方向迈进。在这一过程中, 水利系统的构成变得极为复杂多样。例如, 一个大型跨区域的水利工程涵盖了众多分布在

收稿日期: 2025-03-11

基金项目: 湖南省水利厅科技基金项目(XSKJ2023059-40)

作者简介: 夏卓群(1977-), 男, 博士, 长沙理工大学计算机与通信工程学院教授, 研究方向为网络安全; 周子豪(1999-), 男, 长沙理工大学计算机与通信工程学院硕士研究生, 研究方向为网络安全。本文通讯作者: 周子豪。

不同地理环境下的子系统,包括山区的水源采集系统、平原地区的输水渠道监控系统以及城市周边的污水处理系统等。山区的水源采集系统由于地处偏远、地形复杂,其网络通信设备可能会因恶劣的自然环境,如暴雨、山体滑坡等导致信号中断或设备损坏,从而引发数据传输安全问题。平原地区的输水渠道监控系统则可能因为线路长、覆盖范围广,容易遭受人为的恶意破坏或非法接入,影响系统的正常运行和数据安全。城市周边的污水处理系统由于靠近人口密集区和工业区域,面临着来自周边网络环境的干扰和攻击风险,如工业电磁干扰可能影响传感器数据的准确性,恶意软件可能通过周边网络入侵控制系统。这些不同子系统的独特安全问题以及它们之间复杂的相互关联,使得整个智慧水利网络安全态势难以准确把握。

智慧水利标志着水利信息化进入全新阶段,是水利现代化的直观呈现^[1]。网络安全作为一项系统工程,在智慧水利建设中处于极为基础且关键的地位,是确保水利信息系统得以安全、稳定运行的重要支撑^[2]。习近平总书记在2016年网络安全和信息化工作座谈会上提到:“全天候全方位感知网络安全态势。知己知彼,才能百战不殆。没有意识到风险是最大的风险……维护网络安全,首先要知道风险在哪里,是什么样的风险,什么时候发生风险,正所谓‘聪者听于无声,明者见于未形’。感知网络安全态势是最基本的工作。”^[3]因此,态势感知技术是发现水利网络安全威胁的有效手段。

1 相关研究

网络安全态势感知领域涉及的研究方法丰富多样。态势评估与预测作为该领域研究的核心,吸引众多学者投身其中。例如,Hu等^[4]将注意力机制融入到BiGRU(Bidirectional Gated Recurrent Unit)算法中,并结合卷积神经网络(Convolutional Neural Network, CNN)网络提出Attention-CNN-BiGRU网络安全态势预测模型。该模型中的BiGRU算法弥补了门控循环单元(Gated Recurrent Unit, GRU)算法忽略后向连接捕获信息的缺陷,注意力机制提升了编码器—解码器性能, CNN网络可以快速分析原始数据,但未能有效解决BiGRU算法最优权重赋值的问题,使其在面对复杂网络安全数据时难以精准地根据数据特征调整权重,从而影响预测的准确性。Yang等^[5]提出基于分解—融合的物联网安全态势预测模型,首先通过整合物联网攻击因素、攻击概率和威胁因素来计算态势值;其次使用VMD(Variational Mode Decomposition)分解原始序列,并基于CNN-BiLSTM-Attention(Convolutional Neural Network-Bidirectional Long Short-Term Memory-Attention)架构预测每个子序列;最后采用BiLSTM融合结果,生成最终预测值。该模型虽然综合考虑了多种因素,但网络结构较为复杂,计

算过程繁琐,计算效率较低。同时,其在参数设置和模型调优方面难度较大,需要大量实验和经验来确定合适的参数,增加了实际应用的难度。曹波等^[6]提出基于时域卷积神经网络(Temporal Convolutional Network, TCN)与GRU的网络安全态势预测方法。该方法首先运用TCN探寻态势数据间的内在联系并引入注意力机制动态调整属性权值;其次借助GRU提取特征获取态势值,同时利用粒子群优化算法进行参数寻优。然而,在对GRU参数进行寻优的过程中,常规的粒子群优化算法(Particle Swarm Optimization, PSO)容易陷入局部最优解,导致最终确定的GRU参数可能并非全局最优,无法充分挖掘数据中的潜在规律,严重限制了模型的预测精准度。Wang等^[7]提出MSCPO-SVM网络安全态势预测模型,使用多种群混沌粒子优化算法(Multi-Swarm Chaotic Particle Optimization, MSCPO)对支持向量机(Support Vector Machines, SVM)进行超参数寻优,用于提升SVM的预测精度。然而,该方法无法全面捕捉数据中的动态变化规律。Chen^[8]提出基于广义径向基函数(Radial Basis Function, RBF)神经网络的态势预测方法,利用K均值聚类算法确定RBF的数据中心和扩展函数,采用最小均方算法调整权值,获取态势值之间的非线性映射关系,实现态势预测。仿真实验结果表明,该方法预测误差较低,但是存在缺乏实际应用验证、未考虑长期趋势等局限。Du等^[9]提出一种基于改良CW-RNN(Clockwork - Recurrent Neural Network)的网络安全态势预测方法,将时钟循环RNN与灰狼算法(Grey Wolf Optimization, GWO)相结合来优化超参数,用于增强模型捕捉态势时间特征与非线性特征的能力。实验结果表明,该方法预测精度良好,时间复杂度较低,实时性表现突出,适用于大规模网络的监测工作。然而,其可解释性欠佳,适应性还有待进一步验证。Hu等^[10]提出基于MR-SVM(MapReduce-SVM)的态势感知预测模型,借助MapReduce实现多路并发来提升SVM的计算能力,进而提高预测能力。然而,该方法过于依赖MapReduce的计算架构,在一些计算资源有限的环境下可能难以有效部署与运行。此外,其并没有从根本上解决SVM的一些固有问题,如对非线性数据的处理能力相对较弱等,因而在面对复杂的网络安全数据时可能会出现预测偏差。曹倩^[11]为帮助管理者快速掌握大型调水工程整体态势并实现跨机构协同指挥,结合大型调水工程运行管理特点和难点,在分析智能运行中心发展现状及趋势的基础上,以“全域态势感知、智能决策分析、协同联动指挥”为切入点,搭建了大型调水工程智能运行中心系统整体架构。

传统机器学习方法在处理具有复杂非线性关系的智慧水利网络安全数据时显得力不从心,难以精准提取关键特征。深度学习方法虽然有所突破,但部分模型存在训练时间长、易过拟合的问题。针对上述问题,本文提出一种

基于 BiGRU 与 MSCPO 的智慧水利网络安全态势预测方法。BiGRU 作为一种深度学习模型, 在处理时间序列数据方面具有独特优势。传统的 GRU 模型仅能单向处理序列信息, 在捕捉序列前后依赖关系时存在局限性。而 BiGRU 可同时从前向和后向两个方向对序列进行处理, 能够更全面地捕捉智慧水利网络安全数据中的时间依赖特征, 无论是早期的安全事件信息, 还是后续的发展趋势, 均能被充分挖掘。在模型参数优化方面, 本文采用 MSCPO 算法。与传统的 PSO 不同, MSCPO 算法利用混沌原理的随机性进行种群初始化。混沌映射具有遍历性、随机性和规律性, 通过混沌映射生成初始粒子群, 能够使粒子在解空间中更均匀地分布, 避免了初始种群的聚集, 增加了算法搜索到全局最优解的可能性。此外, MSCPO 算法通过种群适应度方差判断粒子是否陷入局部收敛。当发现粒子陷入局部

收敛时, 对这些粒子进行混沌处理, 重新初始化它们的位置和速度, 使其能够跳出局部最优区域, 继续探索更优解。这种动态调整机制进一步保证了算法能够为 BiGRU 寻找找到更优的超参数组合, 包括迭代次数、学习率和隐含层节点数等。在 SWaT 数据集上的实验结果表明, 本文方法在均方误差、平均绝对误差和决定系数等指标上表现优异, 相较于传统算法, 其预测准确性和稳定性得到显著提升, 为智慧水利网络安全建设提供了更有力的技术支持。

2 模型构建

基于 MSCPO-BiGRU 的智慧水利网络安全态势预测模型架构见图 1。该模型主要由 3 个模块构成, 分别为输入模块、MSCPO-BiGRU 模块以及态势输出模块。

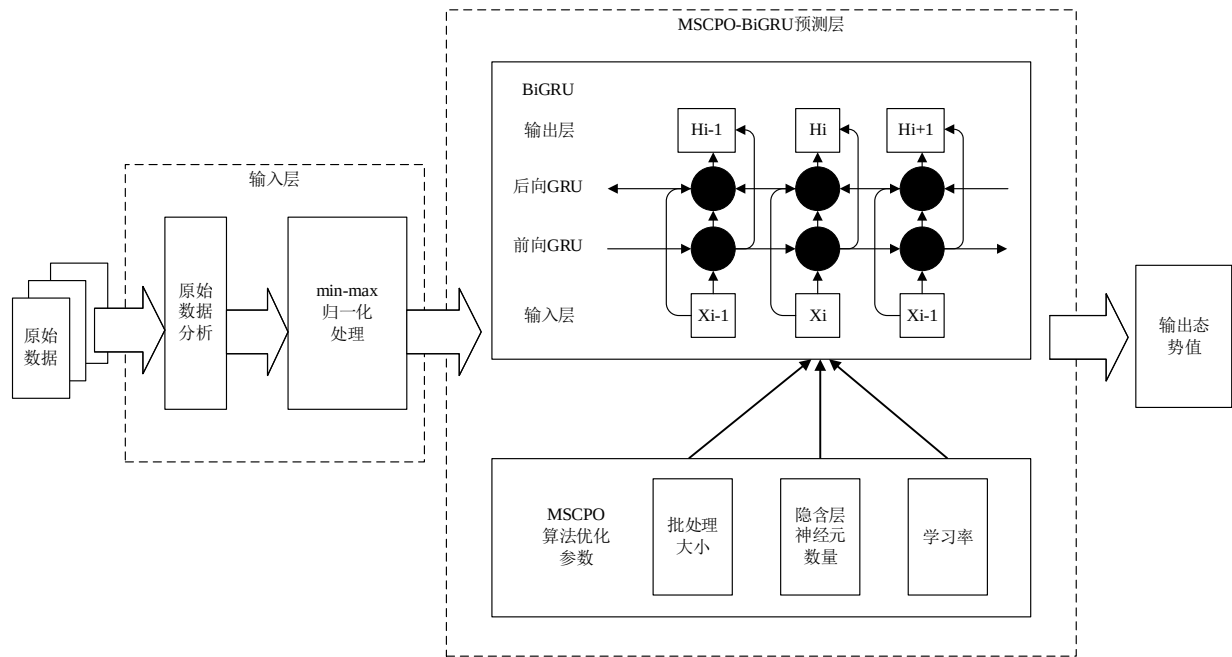


Fig. 1 Situation prediction model structure based on MSCPO-BiGRU

图 1 基于 MSCPO-BiGRU 的态势预测模型架构

MSCPO-BiGRU 预测模型的构建流程如图 2 所示。

基于 MSCPO-BiGRU 的态势预测算法伪代码为：

input: 智慧水利网络安全数据集

output: 网络安全态势预测值

- 1 输入数据集数据 $n = \{n_1, n_2, \dots, n_n\}$ 。
- 2 依据水利系统时间序列数据集特点进行分析。
- 3 构建有效的预测因子, 选定自变量和因变量。
- 4 样本数据归一化处理, 并通过滑动窗口划分训练集以及测试集。
- 5 初始化 MSCPO 算法, 并依据水利数据集特点优化 BiGRU 算法模型。
- 6 利用 MSCPO 算法对 BiGRU 模型的各项参数展开优化调整, 随后借助经过优化的模型针对训练集开展训练操作, 通过这一系列步骤最终确定 MSCPO-BiGRU 预测模型。
- 7 输入测试集, 通过 (5) 中得到的 MSCPO-BiGRU 预测模型得

出态势预测值

End

2.1 BiGRU 结构

GRU 作为 LSTM 网络模型的变体之一, 二者存在一定差异。LSTM 设有输入门、遗忘门以及输出门 3 个门, 而 GRU 则仅有重置门与更新门。其中, 重置门能够对当前时间步的输入信息和上一时间步隐藏状态的混合状况予以调控, 由此确定要保留的旧信息以及需整合的新信息; 更新门则掌控着上一时间步隐藏状态在当前时间步的作用程度, 进而判定是否要将上一时间步的隐藏状态予以摒弃。相较于 LSTM, GRU 的构造更为简易, 参数量也更少。GRU 结构见图 3。

GRU 的核心优势在于其能够更高效地把握长期依赖关系, 这是凭借重置门和更新门两项机制达成的。重置门

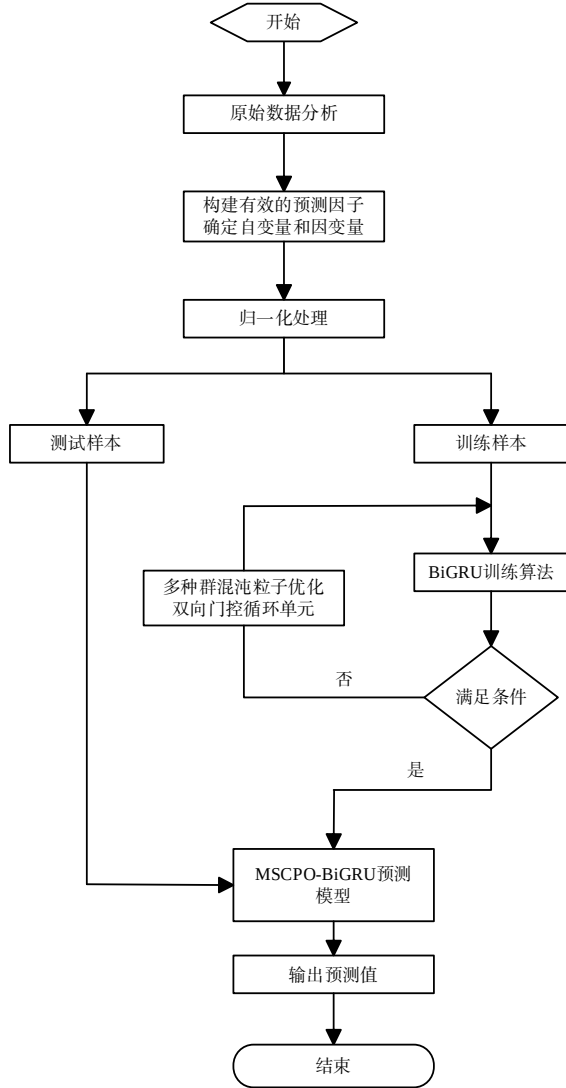


Fig. 2 Construction flow of the MSCPO-BiGRU prediction model
图2 MSCPO-BiGRU预测模型构建流程

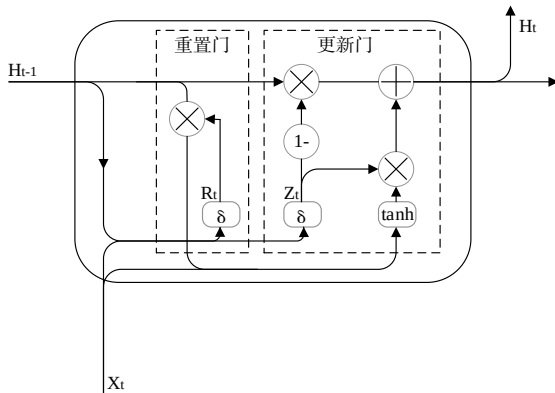


Fig. 3 GRU structure
图3 GRU结构

R_t 的作用在于明确在计算当前候选隐藏状态时需要丢弃多少过往信息。计算公式为:

$$R_t = \delta(W_r \cdot [H_{t-1}, X_t]) \quad (1)$$

式中: R_t 为重置门的激活值; δ 为sigmoid激活函数; W_r

为重置门的权重矩阵; H_{t-1} 为上一个时间步的隐藏状态; X_t 为当前时间步的输入。

更新门 Z_t 的作用在于明确需要保留多少过去的隐藏状态以及新的候选隐藏状态。计算公式为:

$$Z_t = \delta(W_z \cdot [H_{t-1}, X_t]) \quad (2)$$

式中: Z_t 为更新门的激活值; W_z 为更新门的权重矩阵。

候选隐藏状态 $\tilde{H}_t$ 可以视作对隐藏状态进行的临时性更新,其计算过程考虑了重置门带来的影响。计算公式为:

$$\tilde{H}_t = \tanh(W \cdot [R_t \cdot H_{t-1}, X_t]) \quad (3)$$

式中: $\tanh$ 为双曲正切激活函数; $*$ 表示逐元素乘法; W 为权重矩阵。

当前时间步的隐藏状态 H_t 依据更新门的加权平均值进行更新。公式为:

$$H_t = (1 - Z_t) \cdot H_{t-1} + Z_t \cdot \tilde{H}_t \quad (4)$$

式中: H_t 为当前时间步的隐藏状态。

由于水利系统网络安全态势值属于时间序列,BiGRU结构成为理想之选,因为其能够高效捕捉时间序列中的依赖关系。BiGRU本质上是一种双向循环神经网络,由一个正向运行的GRU和一个反向运行的GRU组合而成,最终输出借助前向、后向传播以及拼接操作形成。在输入序列中的模式会受到过去和未来数据影响的情况下,BiGRU这种双向结构能使其在时间序列预测任务中获取更为丰富的上下文信息。结构见图4。

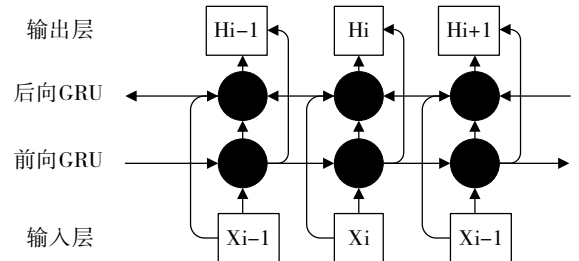


Fig. 4 BiGRU structure
图4 BiGRU结构

2.2 MSCPO算法优化参数

在BiGRU的训练阶段需要对诸多参数进行设定,如GRU隐含层神经元数量、优化器的学习率以及批处理大小等,这些参数会对模型训练结果产生直接影响。运用PSO算法对BiGRU的超参数进行全局寻优不仅能节省人工调参时间,消除其主观依赖性,而且可以获取更优质的网络参数,提升模型预测准确率。PSO由J.Kennedy和R.C.Eberhart提出,是一种借助群体间信息共享且持续迭代的智能算法,能够对各类目标函数进行有效优化^[12]。其将每个函数问题的优化过程想象成鸟群觅食的行为,每个粒子代表一个潜在的解,而最优解就如同鸟群要找寻的食物,需要进行层层搜索。基本PSO算法的伪代码为:

input: 迭代次数 k ;种群规模 X ;空间维度 D ;学习因子: r_1, r_2 ;

加速因子: c_1, c_2

output: 全局最优位置向量 $\mathbf{x}^*(k)$

1 $k \leftarrow 1(\text{initialization});$

2 初始化粒子的位置向量 $x_i^j = x_{\min} + \text{rand}() * (x_{\max} - x_{\min})$

3 初始化粒子的速度向量 $v_i^j = v_{\min} + \text{rand}() * (v_{\max} - v_{\min})$

4 **while** $((f(x(k)^*) \gg \varepsilon) \text{ or } (k \leq T))$ **do**

5 **for** $i = 1$ **to** X **do**

6 $f(x_i(k)) \leftarrow$ 计算粒子的适应度值 $x_i(k)$;

7 更新粒子 i 的局部最优位置 $P_{\text{Best}i}(k)$;

8 更新种群的全局最优位置 $G_{\text{Best}i}(k)$;

9 **for** $i = 1$ **to** X **do**

10 **for** $j = 1$ **to** D **do**

11 更新粒子的速度向量 $V_i(k)$ 和位置向量 $X_i(k)$;

12 $v_i^j(k) \leftarrow v_i^j(k) + c_1 r_1 * (P_i^j(k) - x_i^j(k)) +$

$c_2 r_2 * (G^j(k) - x_i^j(k));$ (5)

13 $x_i^j(k) \leftarrow x_i^j(k) + v_i^j(k);$ (6)

14 $k \leftarrow k + 1$

15 **return** $\mathbf{x}^*(k)$

PSO 算法在运行时可能会出现以下情况: 当某个粒子探测到疑似最优位置时, 其余粒子便即刻向其靠拢。如此以来, 算法极易陷入局部最优, 产生早熟收敛的困境, 导致算法无法在搜索空间中继续探索^[13]。鉴于此, 本文创新性地提出 MSCPO 算法, 利用混沌原理的随机性, 于初始阶段对种群粒子开展初始化工作, 并将粒子分为 3 个种群, 各种群采用不同的更新策略, 借助 3 个种群间的协同合作与实时信息共享来加快算法收敛。该算法通过种群适应度方差这一指标来判断粒子是否陷入局部收敛。若粒子陷入局部收敛, 便对其进行混沌处理, 协助粒子跳出局部收敛点, 以此提升算法性能。

MSCPO 算法的具体步骤为^[14]:

(1) 利用混沌原理的随机性进行种群初始化, 并设定搜寻空间为 $[l_d, u_d]$ 。初始化生成一个 d 维向量: $z_1 = (z_{11}, z_{12}, \dots, z_{1d})$, $z_{1i} \in [0, 1], i = 1, 2, \dots, d$; 经 Logistic 方程得到:

$$z_{i+1,j} = 4z_{ij}(1 - z_{ij}), i = 1, 2, \dots, n-1; j = 1, 2, \dots, d \quad (7)$$

将 z_j 变换到优化问题的搜寻空间中:

$$x_{ij} = l_j + z_{ij}(u_j - l_j), i = 1, 2, \dots, n; j = 1, 2, \dots, d \quad (8)$$

首先, 借助适应度函数计算出所有粒子的适应度值并进行排序; 其次, 从种群中选取较优的 2/5 粒子组成第一种群, 将该种群的惯性权重系数 w 设定为最小值 0.4; 再次, 选取种群中较差的 1/5 粒子构成第二种群, 将该种群的惯性权重系数 w 设为最大值 0.9; 最后, 将占种群 2/5 的中间部分粒子组成第三种群。

(2) 运用式(5)和式(6)对第一种群和第二种群粒子的速度与位置进行更新操作。第三种群采用式(9)和式(10)所代表的自适应更新策略进行更新, 该策略能促进粒子更快朝着最优解的邻域靠近, 进而提升算法的收敛速度。与

此同时, 对惯性权重系数进行动态调整, 使其根据粒子适应度的变化而变化。在算法运行过程中, 以粒子的适应度值与平均适应度值的比较结果作为依据来决定粒子的寻优方式。若粒子的适应度值低于平均适应度值, 此时该粒子会专注于在其当前所处的种群内部展开寻优操作。这种寻优策略可使粒子在局部范围内更深入地挖掘潜在的优质解。反之, 若粒子的适应度值高于平均适应度值, 该粒子则会将寻优范围拓展至全局, 有助于发现全新的、更优的解空间。

$$v_{id}^k = \begin{cases} v_{id}^{k-1}, f^k < f^{k-1} \\ w v_{id}^{k-1} + c_1 r_1 (P_{\text{Best}i} - x_{id}^{k-1}) + c_2 r_2 (G_{\text{Best}i} - x_{id}^{k-1}), f^k \leq \bar{f} \end{cases} \quad (9)$$

$$w = \begin{cases} w_{\min} + \frac{(w_{\max} - w_{\min})(f^k - f_{\min})}{\bar{f} - f_{\min}}, f^k \leq \bar{f} \\ w_{\max}, f^k > \bar{f} \end{cases} \quad (10)$$

式中: f^k, f^{k-1} 分别为粒子当前及上一次的适应度值; $\bar{f}, f_{\min}$ 分别为种群的平均和最小适应度值; $w_{\min}, w_{\max}$ 分别设置为 0.4 和 0.9。

在自适应更新策略中需对学习因子 c_1, c_2 进行动态调整, 在搜索前期快速降低 c_1 值可加快进入局部寻优, 提升收敛速度; 在搜索后期增大 c_2 值可维持种群粒子的多样性, 避免早熟收敛。调整公式为:

$$c_1 = c_{1\varnothing} + \left(1 - \frac{\arccos\left(-\frac{k}{k_{\max}} + 1\right)}{\pi} \right) \times (c_{1\varphi} - c_{1\varnothing}) \quad (11)$$

$$c_2 = c_{2\varnothing} + \left(1 - \frac{\arccos\left(-\frac{k}{k_{\max}} + 1\right)}{\pi} \right) \times (c_{2\varphi} - c_{2\varnothing}) \quad (12)$$

式中: $c_{1\varnothing}=2.75$, 为 c_1 的初始迭代值; $c_{1\varphi}=1.25$, 为 c_1 的终止迭代值; $c_{2\varnothing}=0.5$, 为 c_2 的初始迭代值, $c_{2\varphi}=2.25$, 为 c_2 的终止迭代值。

(3) 利用适应度函数计算出全部粒子的适应度值, 若某粒子的适应度值比其此前所经历过的个体最优位置 $P_{\text{Best}i}$ 对应的适应度值更优, 则将该粒子的个体最优位置更新为当前这个更优的值, 即更新为 $P_{\text{Best}i}$ 。若某粒子的适应度值比种群的全局最优位置 $G_{\text{Best}i}$ 对应的适应度值更优, 则将种群的全局最优位置更新为这个更优的值, 即更新为 $G_{\text{Best}i}$ 。

(4) 对是否符合结束条件(粒子是否达到全局最优位置)进行判断, 若满足该结束条件, 则输出相应的值; 若不满足结束条件, 则按流程继续执行。

(5) 根据种群适应度方差 σ^2 的值来判定粒子是否陷入局部收敛, 计算公式见式(13)。若 σ^2 小于设定阈值, 则按流程继续执行; 若 σ^2 大于等于设定的阈值, 则跳转至步骤(2)进行相应操作。

$$\sigma^2 = \frac{1}{n} \sum_{i=1}^n \left(\frac{f_i - \bar{f}}{f} \right)^2, f = \max[1, \max |f_i - \bar{f}|] \quad (13)$$

式中: $\bar{f}$ 为当前种群的平均适应度值; f_i 为当前粒子 i 的适应度值。

(6) 对粒子进行混沌处理后返回到步骤(2)进行后续流程。混沌处理是指将那些陷入局部收敛状态的粒子位置 x_i 转变为混沌序列:

$$y_i = \frac{x_i - l_i}{u_i - l_i}, (i = 1, 2, \dots) \quad (14)$$

对 y_i 进行变换, 得到下一状态的混沌序列。表示为:

$$y_i^* = 4y_i(1 - y_i), (i = 1, 2, \dots) \quad (15)$$

对 y_i^* 进行逆映射可得到原来搜寻空间的位置。表示为:

$$x_i^* = l_i + y_i^*(u_i - l_i), (i = 1, 2, \dots) \quad (16)$$

MSCPO 算法流程如图 5 所示。

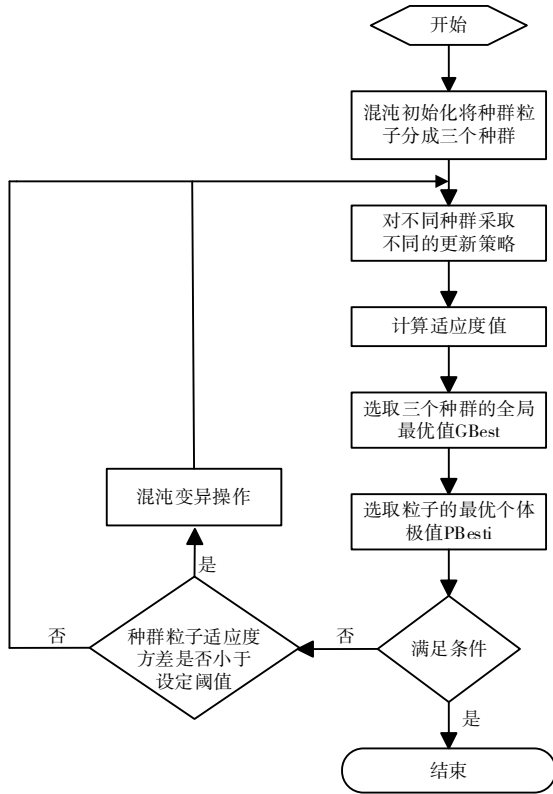


Fig. 5 Flow of MSCPO algorithm

图5 MSCPO 算法流程

3 实验方法与结果分析

3.1 实验环境与参数设置

3.1.1 实验环境

硬件配置为 Intel (R) Core (TM) i7-8750H 处理器、NVIDIA GeForce GTX 1050 Ti 显卡、16 GB 内存。在 Windows 64 位系统上采用 Python3.9 编程, 机器学习库为 TensorFlow2.10, 训练和测试阶段均利用 GPU 加速。

3.1.2 实验参数设置

由于每个时间步只有一个特征, 且仅需要预测下一个时间步的值, 本文设置输入、输出神经元个数均为 1, 以确保模型能够正确处理单变量时间序列数据。

PSO 算法参数设定为: 粒子群数量 $N=50$; 每个粒子维数(寻优的参数个数)为 3; 加速因子 $c_1 = 1.49, c_2 = 1.49$; 学习因子 r_1, r_2 为取值在 $[0, 1)$ 之间的随机数; 惯性权重 $w = 0.7$; 最大迭代次数为 50。

MSCPO 算法参数设定为: 粒子群 $N=20$, 种群数量为 3 个; 最大迭代次数为 20; 每个粒子维数(寻优的参数个数)为 3; 训练轮次为 10; 前两个种群采取标准粒子更新策略, 加速因子 $c_1 = 1.49, c_2 = 1.49$, 第一个种群权重为 0.4, 第二个种群权重为 0.9; 最后一个种群采取自适应更新策略, 权重调整范围为 $w_{min} = 0.4, w_{max} = 0.9$, 学习因子 c_1 动态调整范围为 $c_{10} = 2.75, c_{100} = 1.25$, 学习因子 c_2 动态调整范围为 $c_{20} = 0.5, c_{200} = 2.25$ 。3 个种群的学习因子 r_1, r_2 均为 $[0, 1)$ 之间的随机数。

此外, 为避免粒子进行毫无目的搜索, 进而对收敛速度产生影响, 需要给寻优参数设置相应界限: 学习率取值范围为 $[0.001, 0.1]$; 批处理大小取值范围为 $[16, 64]$; 隐藏层神经元数量范围设定为 $[10, 100]$ 。优化后的超参数设置见表 1。

Table 1 Optimized hyperparameter settings

表 1 优化后的超参数设置

超参数	数值
隐藏层神经元数量	53
学习率	0.042 1
批处理大小	16

选择均方误差 (Mean Squared Error, MSE) 作为主要适应度指标, 其能够直观反映模型预测值与实际值之间的偏离程度。选择平均绝对百分比误差 (Mean Absolute Percentage Error, MAPE) 和决定系数 (Coefficient of Determination, R^2) 作为次要适应度指标, 有助于从更多维度对模型性能展开评估。最终模型在验证集上的适应度值为 $MSE = 0.0028, MAPE = 10.97, R^2 = 0.9161$ 。

3.2 数据集及其预处理

3.2.1 数据集

选择 SWaT (Secure Water Treatment) 数据集进行实验^[15]。其来自新加坡国立大学研究项目中的水处理厂, 虽然不是直接的智慧水利场景, 但与智慧水利系统架构、运行逻辑相似, 且包含丰富的正常和异常数据, 对研究智慧水利网络安全态势有借鉴意义。SWaT 数据集涵盖了水利系统的多个参数, 包含 51 个特征和 6 种攻击所产生的主要异常行为类型^[16]。该数据集来自于 51 个传感器和执行器, 共记录连续 11 天的数据, 其中 7 天为正常操作数据, 4 天阶段性受到攻击, 共遭受 41 次攻击。数据集详情见表 2。

SWaT 数据集中的主要异常行为类型及对应的影响因

Table 2 Detailed information of SWaT dataset	
表 2 SWaT 数据集详情	
指标	数值
所含特征种类	51
攻击次数	41
攻击持续时间/min	2~25
训练大小(均为正常数据)	496 800
测试大小(含攻击数据)	449 919
N_rate/%	88.02

注:N_rate 为正常数据点与测试数据集中所有数据点的比率。

子见表 3。影响因子是衡量不同网络攻击或异常行为对智慧水利系统安全态势影响程度的量化指标。如表 3 所示,在 SWaT 数据集中,化学品加药系统的异常行为影响因子为 0.3。该项行为发生时会使化学物质投加量失控,影响水质处理,干扰水利系统正常运行,因此其影响因子较高。原水存储和转移异常行为的影响因子为 0.1,影响相对较小,但可能导致水源供应不稳定,评估安全态势时同样需要考虑。

Table 3 Abnormal behavior types in the SWaT dataset	
表 3 SWaT 数据集中的异常行为类型	
异常行为类型	影响因子
化学品加药系统异常行为	0.3
原水存储和转移异常行为	0.1
预处理系统异常行为	0.2
膜过滤系统异常行为	0.2
消毒系统异常行为	0.2

3.2.2 预处理方法

SWaT 数据集中的部分特征最大值与最小值差异较大。为使特征处于相同范围且保留数据关系,本文采用最大最小值法归一化处理数据。公式为:

$$x'_{ij} = \frac{x_{ij} - x_{imin}}{x_{imax} - x_{imin}} \tag{17}$$

式中: x_{ij} 为需要归一化处理的数据; x_{imax} 、 x_{imin} 分别为数据中的最大值和最小值; x'_{ij} 为归一化处理后的输出结果,取值范围为 $x'_{ij} \in [0, 1]$ 。

3.2.3 态势值生成

态势值生成对模型预测极为关键。准确的态势值可为模型提供好的训练样本,辅助其学习数据特征、精准预测异常场景,其生成方式还会影响模型的泛化能力。SWaT 数据集中无直接可用的态势值字段。本文参考基于 DS-DAEDNN (Dempster Shafer-Deep Auto Encoder Deep Neural Networks) 的网络安全态势评估模型,结合数据集分析得到的异常行为影响因子见表 3,依据《国家突发公共事件应急预案》对网络安全形势的分类,按照对水利系统的威胁程度分配影响因子,综合计算得出网络安全态势值^[17]。本文从数据集中选取含 608 个样本的时间段(约对应 1.5 天系统网络活动)作为分析基础单位,按照上述方法生成真实态势值,再将所有态势值映射到 $[0, 1]$ 区间。最终,训练集由 59 个时间段构成,测试集由 10 个时间段构成。具体见图 6。

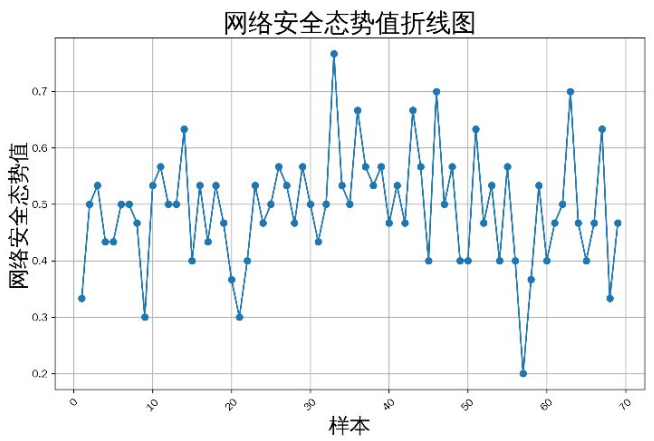


Fig. 6 Line chart of the actual situation values
图 6 真实态势值折线图

3.3 评价标准

为准确评估算法性能,本文选择 MAPE、 R^2 和 MSE 3 个评价指标^[18]。MAPE 主要用于衡量算法的准确性,通过计算实际值与预测值之间的平均百分比误差得到。计算公式为:

$$MAPE = \frac{1}{n} \sum_{i=1}^n \left| \frac{A_i - F_i}{A_i} \right| \times 100\% \tag{18}$$

式中: A_i 为第 i 个观测点的实际值; F_i 为第 i 个观测点的预测值。通常情况下,MAPE 值越小,模型预测准确性越高。

R^2 为模型预测方差在数据总方差中所占的比例,用于评价模型对数据的解释能力。计算公式为:

$$R^2 = 1 - \frac{\sum_{i=1}^n (A_i - F_i)^2}{\sum_{i=1}^n (A_i - \bar{A})^2} \tag{19}$$

式中: $\bar{A}$ 为所有实际观测值的平均数。 R^2 值越接近 1,表明模型对数据的拟合程度越高。

MSE 旨在衡量预测值与实际观测值之间的差异大小。计算公式为:

$$MSE = \frac{1}{n} \sum_{i=1}^n (y_i - \hat{y}_i)^2 \tag{20}$$

式中: y_i 为第 i 个观测点的实际值; $\hat{y}_i$ 为第 i 个观测点的预测值; n 为观测点总数。MSE 值越小,预测值与实际值之间的偏离程度越小。

3.4 实验结果与分析

3.4.1 复杂度分析

不同算法的时间复杂度见表 4。可以看出, MSCPO-BiGRU 算法的时间复杂度为 $O(S \cdot N \cdot I \cdot 2T(DH + H^2))$, 其中 T 为输入序列长度, H 为隐藏层数量, D 为输入特征维度, S 为混沌粒子群算法中的种群数量, N 为每种子群的粒子数量, I 为迭代次数。

3.4.2 预测精度比较

为考察本文模型的预测能力,在相同实验条件下分别采用 GRU、BiGRU、PSO-GRU、PSO-BiGRU、MSCPO-GRU、MSCPO-BiGRU 模型进行预测,得到预测值与真实值的对

Table 4 Comparison of time complexities of different algorithms

表 4 不同算法时间复杂度比较

算法	复杂度
GRU	$O(T(DH + H^2))$
BiGRU	$O(2T(DH + H^2))$
PSO-GRU	$O(N \cdot I \cdot T(DH + H^2))$
PSO-BiGRU	$O(N \cdot I \cdot 2T(DH + H^2))$
MSCPO-GRU	$O(S \cdot N \cdot I \cdot T(DH + H^2))$
MSCPO-BiGRU	$O(S \cdot N \cdot I \cdot 2T(DH + H^2))$

比图,结果如图 7 所示。可以看出,未采用 PSO 算法的 GRU 和 BiGRU 模型的预测效果与实际态势值有一定差距,BiGRU 在精度上略高于 GRU 模型。PSO-GRU 模型会产生部分误差过大的预测值,但整体预测趋势与真实态势值保持一致,整体上比未采用 PSO 算法的 GRU 模型更好。本文所提 MSCPO-BiGRU 模型与 MSCPO-GRU 模型在预测整体趋势方面相差不大,但在预测精度上, MSCPO-BiGRU 略优于 MSCPO-GRU 模型。

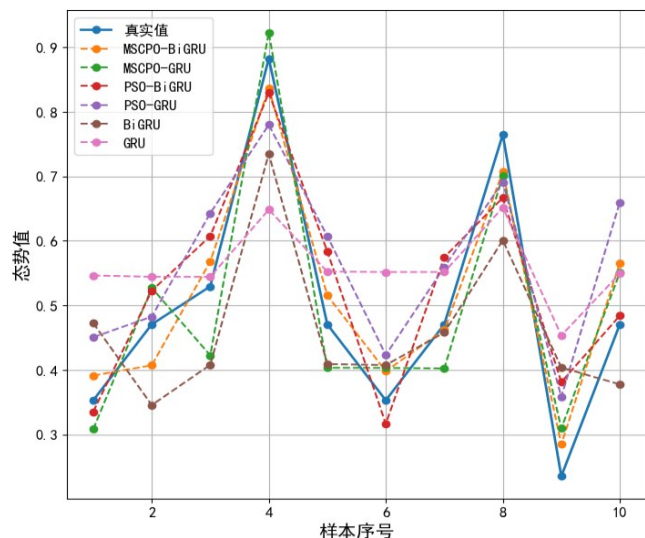


Fig. 7 Comparison of prediction accuracy among different models

图 7 不同模型预测精度比较

不同模型的预测误差指标比较见表 5。可以看出, MSCPO-BiGRU 模型 MSE、MAPE 和 R^2 表现突出,其中 MSE 和 MAPE 为最低, R^2 为最高。相比之下, GRU 和 BiGRU 模型由于未经过有效的参数优化,其 MSE 和 MAPE 值较大, R^2 值较低。PSO-GRU 和 PSO-BiGRU 模型虽然通过粒子群优化有所改进,但由于 PSO 算法易陷入局部最优,在误差控制和拟合效果上不如 MSCPO-BiGRU 模型。MSCPO-GRU 模型虽然在一定程度上利用 MSCPO 算法进行优化,但因未充分发挥 BiGRU 的双向结构优势,在各项指标上也逊于 MSCPO-BiGRU 模型。

4 结语

本文针对现有预测模型在捕捉智慧水利网络安全态势变化时存在局限这一问题,提出基于 MSCPO-BiGRU 的

Table 5 Comparison of prediction error indicators among different models

表 5 不同模型预测误差指标比较

模型	MAPE/%	R^2	MSE
MSCPO-BiGRU	10.97	0.916 1	0.002 8
MSCPO-GRU	14.95	0.862 1	0.004 6
PSO-BiGRU	17.10	0.796 6	0.006 8
PSO-GRU	23.32	0.637 0	0.012 0
BiGRU	24.42	0.588 8	0.013 7
GRU	31.49	0.349 0	0.021 0

预测方法。该方法在超参数优化算法上进行创新,利用 MSCPO 算法独特的种群初始化与更新策略,有效避免陷入局部最优,为 BiGRU 寻得更优的超参数组合;同时,发挥 BiGRU 双向捕捉时间序列依赖关系的结构优势,结合智慧水利系统的历史与未来信息,实现更精准的预测。在 SWaT 数据集上的实验结果表明,该方法的 MSE(0.002 8)、MAPE(10.97%)和 R^2 (0.916 1)等评价指标优于对照方法,展现出更高的准确性和稳定性。

然而,本文研究仍存在一定不足之处:一方面,模型在面对极端复杂且大规模的智慧水利网络数据时计算资源消耗较大,运行效率有待进一步提升;另一方面,尽管 MSCPO 算法在寻优过程中采取多种策略避免局部最优,但对于某些极为特殊的数据分布情况,仍可能无法获取绝对最优参数组合,在一定程度上限制了预测精度的进一步提高。针对以上不足,后续研究可从以下两方面展开:其一,探索高效的模型轻量化技术,如模型剪枝、量化等,减少模型参数冗余,同时结合分布式计算框架,提升模型在大规模数据处理时的运行效率;其二,深入融合多种智能优化算法,或改进现有混沌优化策略,进一步增强算法在复杂数据环境下的全局寻优能力,以获取更理想的模型参数,提高预测精度,为智慧水利网络安全态势预测提供更完善的解决方案。

参考文献:

- [1] ZHANG C, FANG Z G, GUO R. Construction of a network security technology system for smart water conservancy[J]. China Water Resources, 2023(11):41-44.
张潮,房志刚,郭冉.面向智慧水利的网络安全技术体系构建[J].中国水利,2023(11):41-44.
- [2] JIA K, WANG L H, LIU D. Preliminary exploration on the construction of Yangtze river hydrological network security situation awareness system[J]. Express Water Resources & Hydropower Information, 2021, 42(3):79-84.
贾克,王立海,刘迪.长江水文网络安全态势感知系统构建初探[J].水利水电快报,2021,42(3):79-84.
- [3] LI Y J, ZHANG J, YANG X, et al. Discovery of cyber security threats in water conservancy based on situation awareness[C]//Proceedings of the 2020 (8th) China Water Resources Informatization Technology Forum, 2020:328-334.
李元杰,张瑾,杨旭,等.基于态势感知的水利网络安全威胁发现[C]//2020年(第八届)中国水利信息化技术论坛论文集,2020:328-334.

- [4] HU C, LIU G, LI M. A network security situation prediction method based on Attention-CNN-BiGRU[C]//2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design, 2022: 257-262.
- [5] YANG A M, XIE B S, LIU Y K, et al. A network security situation prediction for consumer data in the internet of things using variational mode decomposition (VMD) and fused CNN-BiLSTM-attention[J]. IEEE Transactions on Consumer Electronics, 2024, 70(1): 1122-1133.
- [6] CAO B, LI C H, FAN X S, et al. A network security situation prediction method integrating TCN and GRU[J/OL]. Journal of Small & Microcomputer Systems, 2025-01-13, <https://doi.org/10.20009/j.cnki.21-1106/TP.2022-0027>.
曹波, 李成海, 范晓诗, 等. 融合TCN和GRU的网络安全态势预测方法[J/OL]. 小型微型计算机系统, 2025-01-13, <https://doi.org/10.20009/j.cnki.21-1106/TP.2022-0027>.
- [7] WANG D J, FU Z, WU Y. Information network security situation prediction method based on particle swarm optimization[C]//2023 2nd International Conference on Artificial Intelligence and Autonomous Robot Systems (AIARS), 2023: 135-139.
- [8] CHEN G. Multimedia security situation prediction based on optimization of radial basis function neural network algorithm[EB/OL]. <https://onlinelibrary.wiley.com/doi/10.1155/2022/6314262>.
- [9] DU J, XIU L, TAO F. Network security situation prediction based on optimized clock-cycle recurrent neural network for sensor-enabled networks[J]. Sensors, 2023, 23(13): 6087.
- [10] HU J, MA D, LIU C, et al. Network security situation prediction based on MR-SVM[J]. IEEE Access, 2019(7): 130937-130945.
- [11] CAO Q. Design and application of intelligent operation center system for large-scale water diversion project[J]. Water Resources Informatization, 2022(1): 65-70.
曹倩. 大型调水工程智能运行中心系统设计与应用[J]. 水利信息化, 2022(1): 65-70.
- [12] KENNEDY J, EBERHART R. Particle swarm optimization[C]//Proceedings of IEEE International Conference on Neural Networks, 1995: 1942-1948.
- [13] MOHANDES M A. Modeling global solar radiation using particle swarm optimization (PSO)[J]. Solar Energy, 2012, 86(11): 3137-3145.
- [14] LI Z P. Improvement of particle swarm optimization algorithm and its application in network situation prediction[D]. Lanzhou: Lanzhou University, 2017.
栗志鹏. 粒子群算法改进及在网络态势预测的应用[D]. 兰州: 兰州大学, 2017.
- [15] GOH J, ADEPU S, NAZIR J K, et al. A dataset to support research in the design of secure water treatment systems[C]//International Conference on Critical Information Infrastructures Security, 2016: 88-99.
- [16] ITRUST. Centre for research in cyber security[EB/OL]. <https://itrust.sutd.edu.sg/itrust-labs/datasets/>.
- [17] The State Council. National overall emergency plan for public emergencies[EB/OL]. http://www.gov.cn/jrzq/2006-01/08/content_150878.htm.
国务院. 国家突发公共事件总体应急预案[EB/OL]. http://www.gov.cn/jrzq/2006-01/08/content_150878.htm.
- [18] PENG X W, YUAN L Y. Internet of Things security situation prediction based on ADE-ABiGRU[J]. Network Security and Data Governance, 2023, 42(12): 48-53.
彭兴维, 袁凌云. 基于ADE-ABiGRU的物联网安全态势预测[J]. 网络安全与数据治理, 2023, 42(12): 48-53.

(责任编辑:尹晨茹)