

融合注意力机制和 BSRU 的工业互联网安全态势预测方法

胡向东, 田正国

(重庆邮电大学自动化学院/工业互联网学院, 重庆 400065)

摘要: 安全态势预测对确保工业互联网平稳可靠运行至关重要。传统的预测模型在面对工业生产过程中产生的海量、高维和时间序列数据时, 难以准确、高效地对网络安全态势进行预测, 因此提出一种融合注意力机制和双向简单循环单元 (BSRU, bi-directional simple recurrent unit) 的工业互联网安全态势预测方法, 以满足工业生产的实时性和准确性要求。对各安全要素进行分析和处理, 使其能反映当前网络状态, 便于态势值的求取。使用一维卷积网络提取各安全要素之间的空间维度特征, 保留特征间的时间相关性。利用 BSRU 网络提取信息之间的时间维度特征, 减少历史信息的丢失, 同时借助 SRU 网络强大的并行能力, 减少模型的训练时间。引入注意力机制优化 BSRU 隐含状态中的相关性权重, 以突出强相关性因素, 减少弱相关性因素的影响, 实现融合注意力机制和 BSRU 的工业互联网安全态势预测。对比实验结果显示, 该模型较使用双向长短期记忆网络和双向门控循环单元的预测模型, 在训练时间和训练误差上分别减少了 13.1% 和 28.5%; 相比于没有使用注意力机制的卷积和 BSRU 网络融合模型, 训练时间虽增加了 2%, 但预测误差降低了 28.8%; 在不同预测时长下该模型的预测效果优于其他模型, 实现了在时间性能上的优化, 使用注意力机制在增加少量时间成本的前提下, 提升了模型的预测精度, 能够较好地拟合网络安全态势发展, 且模型在多步预测上存在一定的优势。

关键词: 工业互联网; 注意力机制; 简单循环单元; 安全态势

中图分类号: TP391

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2021092

Methods of security situation prediction for industrial internet fused attention mechanism and BSRU

HU Xiangdong, TIAN Zhengguo

College of Automation/Industrial Internet Institute, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: The security situation prediction plays an important role in balanced and reliable work for industrial internet. In the face of massive, high-dimensional and time-series data generated in the industrial production process, traditional prediction models are difficult to accurately and efficiently predict the network security situation.

收稿日期: 2021-05-17; 修回日期: 2021-06-24

通信作者: 胡向东, huxd@cqupt.edu.cn

基金项目: 教育部-中国移动科研基金 (MCM20150202, MCM20180404)

Foundation Item: The Joint Research Foundation of the Ministry of Education of the People's Republic of China and China Mobile (MCM20150202, MCM20180404)

引用格式: 胡向东, 田正国. 融合注意力机制和 BSRU 的工业互联网安全态势预测方法[J]. 网络与信息安全学报, 2022, 8(1): 41-51.

Citation Format: HU X D, TIAN Z G. Methods of security situation prediction for industrial internet fused attention mechanism and BSRU[J]. Chinese Journal of Network and Information Security, 2022, 8(1): 41-51.

Therefore, the methods of security situation prediction for industrial internet fused attention mechanism and bi-directional simple recurrent unit (BSRU) were proposed to meet the real-time and accuracy requirements of industrial production. Each security element was analyzed and processed, so that it could reflect the current network state and facilitate the calculation of the situation value. One-dimensional convolutional network was used to extract the spatial dimension features between each security element and preserve the temporal correlation between features. The BSRU network was used to extract the time dimension features between the data information and reduced the loss of historical information. Meanwhile, with the powerful parallel capability of SRU network, the training time of model was reduced. Attention mechanism was introduced to optimize the correlation weight of BSRU hidden state to highlight strong correlation factors, reduced the influence of weak correlation factors, and realized the prediction of industrial internet security situation combining attention mechanism and BSRU. The comparative experimental results show that the model reduces the training time and training error by 13.1% and 28.5% than the model using bidirectional long short-term memory network and bidirectional gated recurrent unit. Compared with the convolutional and BSRU network fusion model without attention mechanism, the prediction error is reduced by 28.8% despite the training time increased by 2%. The prediction effect under different prediction time is better than other models. Compared with other prediction network models, this model achieves the optimization of time performance and uses the attention mechanism to improve the prediction accuracy of the model under the premise of increasing a small amount of time cost. The proposed model can well fit the trend of network security situation, meanwhile, it has some advantages in multistep prediction.

Keywords: industrial internet, attention mechanism, simple recurrent unit, security situation

0 引言

随着一些低时延、高可靠的新型网络基础设施在工业领域的应用,互联网在工业领域迅速普及。高速、智能的工业互联网给企业带来便利的同时使原本与互联网隔离的工控系统面临复杂的网络安全问题。因此,为了提前感知危险,及时做出应对措施,高效率、高稳定、高智能的感知预测模型变得越来越重要。网络安全态势感知(NSSA, network security situation awareness)^[1-2]技术可以用于收集工业互联网环境下网络安全威胁要素,进行合理分析与评估,管理者基于获得的安全态势值判断可能发生的网络安全风险,做出安全决策,保证工控网络的安全。

在工业互联网领域,每天都会产生大量具有非线性和时变性的数据,传统的预测方法,如基于隐马尔可夫链^[3]、支持向量机(SVM, support vector machine)^[4]和反向传播网络(BP, back propagation)^[5]等模型,由于容错性、自学能力较差,已经不适应当前网络环境对安全态势的预测。寻找一种泛化能力强、善于处理非线性问题的模

型,正成为研究者促进工业与互联网安全态势预测的研究重点。Zhang等^[6]针对网络安全威胁事件的不确定性和突发性,提出了一种优化的前馈神经网络预测模型。该模型通过动态模糊聚类 and 消除机制改进后的遗传算法优化网络参数,不仅提高了模型的收敛效率,同时预测精度得到了提升。Xiao等^[7]针对网络安全态势数据具有的非线性、时间性等特点,提出一种基于改进BP的网络安全态势预测算法。该算法通过思维进化算法优化BP网络参数,提升了预测的准确度和效率,但是对历史数据的处理不够完善。杨宏宇等^[8]针对时间序列数据,提出一种基于自修正系数的预测模型,使用熵关联度将数据信息转换为时间样本序列,采用时变加权马尔可夫链对预测结果进行修正,提高对时间序列数据的预测精度,但对线性数据的处理不够完善。

虽然上述方法在预测精度和收敛速度等方面都取得了很好的效果,但只考虑了网络安全态势值,忽略了多属性网络安全态势要素的重要性,参考因素相对片面,精确预测方面存在不足。为了改善这个问题,张任川等^[9]针对网络安全态势要素和态势值等问题,提出一种改进的卷积神经

网络(CNN, convolution neural network)。通过改进卷积结构,降低了模型的优化难度,但没有充分利用卷积网络在特征提取上的优势,预测精度略有不足。Li等^[10]针对训练时间长、各要素间存在时间相关性等问题,采用简单循环单元与注意力机制相结合的方式,对影响要素进行选择学习,提高了预测精度,缩短了训练时间。

为了区分不同工业互联网网络安全态势要素对安全态势值的影响,同时避免模型产生较大的计算代价,本文提出了一种融合注意力机制和BSRU的工业互联网安全态势预测方法(Attention-BSRU),通过CNN和BSRU处理不同网络安全态势要素对未来网络安全态势值的影响,挖掘各要素之间的时间相关性;利用BSRU强大的并行能力,提高训练时间性能,满足工控系统对实时性的要求;引入Attention机制^[11]融合多属性网络安全数据,加强重要因素对安全态势值的影响,从而达到提高预测精度和预测效率的目的。

1 工业互联网安全态势预测模型

采用Attention-BSRU模型对态势值进行预测的思路是先将获取到的数据进行预处理并经过滑动窗口重构后作为模型的输入,利用CNN和BSRU提取各要素间的局部特征,捕获时间相关性,利用注意力机制调整输入特征的权重,使用Sigmoid函数对态势值进行预测。预测模型的流程如图1所示。

1.1 数据预处理

1.1.1 工业互联网安全态势指标选取

工业互联网安全区别于通用信息网络安全特殊性主要表现为业务数据含义的不同及其影响程度的差异,指令数据错误不仅可能导致业务逻辑出错,还可能造成物理上的财物损坏甚至人身安全事故发生;工业互联网安全数据包含生产设备的详细情况及运行规律,也包含大量市场、客户等信息,连接种类和数量更多,场景更复杂;为了满足工业生产的需求,要求工业互联网的性能更可靠和安全,因此对数据的真实性、完整性、时效性等要求更高;工业环境中的行业标准多,评价标准不一,选取不同的数据结果会不同;工

业互联网数据具有更强的时间相关性,实时性要求更高。因此,工业互联网安全影响更大,实效性要求更高,指标选取和性能评估要考虑的因素更多。

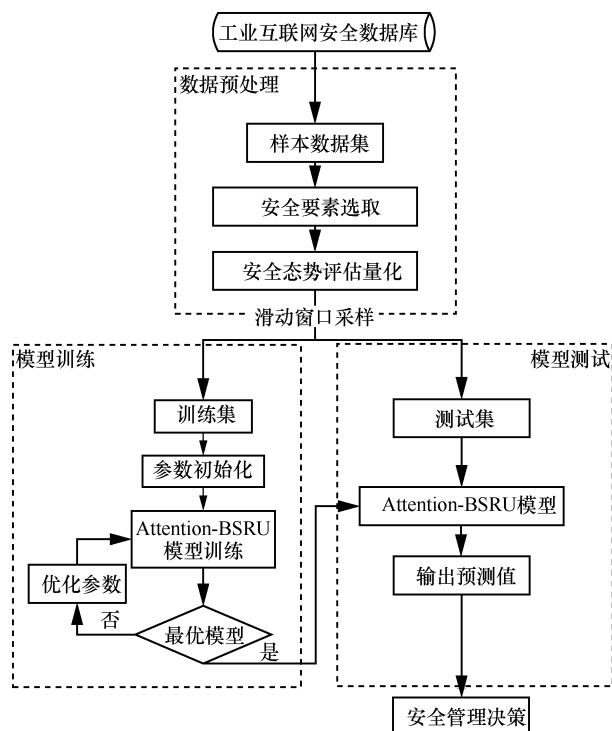


图1 预测模型的流程
Figure 1 Flow of prediction model

由于工业互联网中数据种类繁多,在工业互联网安全风险评估、识别可能的安全威胁和评估潜在损失的过程中,不能使用单一的指标判断网络运行状态。参考文献[12-13]对分层模型的研究并结合网络信息安全风险评估规范 GB/T 20984-2007,从威胁性、脆弱性、资产价值3个方面进行要素选取。工业互联网安全态势评估指标如表1所示。

根据漏洞类型、漏洞危害等级、网络设备资产、攻击数量和通用安全漏洞评分系统评分等构造工业互联网漏洞数据库。本文参考文献[14-15]对评估方法的研究,考虑以下要素评估安全态势值。

1) 脆弱性指数 V : 指对工控系统漏洞信息、设备补丁信息和设备安全漏洞等进行量化评估后,能反映工控系统在遭受攻击入侵时防御失败的可能性,系统越脆弱,该指数越高。 V 的计算

式如(1)所示。

$$V = \sum_{i=1}^m g(E_i) \cdot \omega_i \quad (1)$$

其中, E_i 为安全要素 e_i 的数值, $g(E_i)$ 为 E_i 的归一化值, m 为安全要素个数, ω_i 为各安全要素对应的权重, 满足归一化约束, 如式(2)所示。

$$\sum_{i=1}^m \omega_i = 1, \omega_i \geq 0, i = 1, 2, \dots, m \quad (2)$$

表 1 工业互联网安全态势评估指标
Table 1 Industrial internet security situation assessment indicators

一级指标	二级指标
威胁性	攻击事件的数量
	攻击事件的等级
	攻击事件发生频率
脆弱性	系统安全漏洞数量、级别
	设备安全漏洞数量、级别
	是否存在补丁
资产价值	受攻击设备数量
	设备提供的服务、运行信息
	系统信息资产的评估价值

2) 威胁性指数 T : 指利用脆弱性导致的攻击事件, 通过关联分析得到的评估指数, 反映工控系统受到威胁的程度, 该指数越高表示威胁越大。 T 的计算如式(3)所示。

$$T = \sum_{i \in m} P(s_i) \cdot L(s_i) \quad (3)$$

其中, s_i 指攻击事件, $P(s_i)$ 指事件 s_i 发生的概率, $L(s_i)$ 指安全事件 s_i 造成的损失。

3) 资产安全风险指数 R : 指对工控系统中设备和网络资产信息等进行量化评估后, 得到能够反映网络中资产价值的数值。资产价值越大, 受到攻击后, 损失越大。 R 的计算如式(4)所示。

$$R = \sum_{i=1}^m \sum_{j=1}^k A_{e_i}^j \cdot P(A_{e_i}^j) \quad (4)$$

其中, $A_{e_i}^j$ 表示安全要素 e_i 涉及的资产 j (包括信息、财产、人员等 k 种资产) 的价值, $P(A_{e_i}^j)$ 表示资产 $A_{e_i}^j$ 被破坏的概率。

4) 网络安全态势值 $\bar{S}$: 指在一定时间内对工控网络安全造成影响的各种安全要素 (主要依赖于威胁性指数 T 、脆弱性指数 V 、资产安全风险指数 R) 进行量化评估后, 得到能够反映工控系统总体网络安全态势的数值。网络安全态势值过大, 则表明系统受到严重攻击, 会造成重大损失。为了提前预警, 避免损失, 将红色警报的临界值设为 0.75, 同时对 [0.4, 0.75] 的态势数据进行了细化, 以便及时应对网络威胁。 $\bar{S}$ 的计算如式(5)所示。网络安全态势等级对照如表 2 所示。

$$\bar{S} = g(T + V + R) \quad (5)$$

其中, $g(\cdot)$ 为归一化函数。

表 2 网络安全态势等级对照
Table 2 Network security situation level comparison

态势值	危险级别	说明
(0, 0.2]	1 (安全)	运行正常, 网络中没有严重的安全威胁
(0.2, 0.4]	2 (轻度危险)	受轻微影响, 安全威胁增加, 损失较小
(0.4, 0.5]	3 (危险)	受较大影响, 出现重大故障的可能性较高
(0.5, 0.6]	4 (中度危险)	受到攻击比较严重, 关键基础设施受影响
(0.6, 0.75]	5 (高度危险)	存在大量网络威胁, 会导致重大危险
(0.75, 1.0]	6 (红色警报)	威胁危险等级高, 数量多, 会导致严重事件

1.1.2 数据归一化

由于工业互联网环境的复杂性和不确定性、收集数据之间的量纲存在差异性问题, 同时为了满足本文所用神经网络的激活函数对于 [-1, 1] 的数据效果有较好的需求, 将单位或量级指标不同的数据进行加权, 从而提高态势预测的准确性, 本文按如下方式对数据进行标准化处理。

$$x_i' = \frac{x_i - \text{mean}(x_i)}{\max(x_i) - \min(x_i)} \quad (6)$$

其中, x_i 、 x_i' 为样本处理前、后的数据, 安全要素个数 $i = 1, 2, \dots, 5$, $\text{mean}(x_i)$ 、 $\max(x_i)$ 、 $\min(x_i)$ 分别为各列数据的平均值、最大值和最小值。

1.1.3 数据重构

预处理后得到的网络安全态势值存在时间序列特征, 以如图 2 所示滑动窗口的方式将数据处理成适合训练的结构: 窗口大小 $\otimes$ 输入维度, 预测标签为 N 时刻之后的网络安全态势值 $\bar{S}$, 窗口大小为 W_{size} , 滑动步长为 Step 。数据重构算法如算法 1 所示。

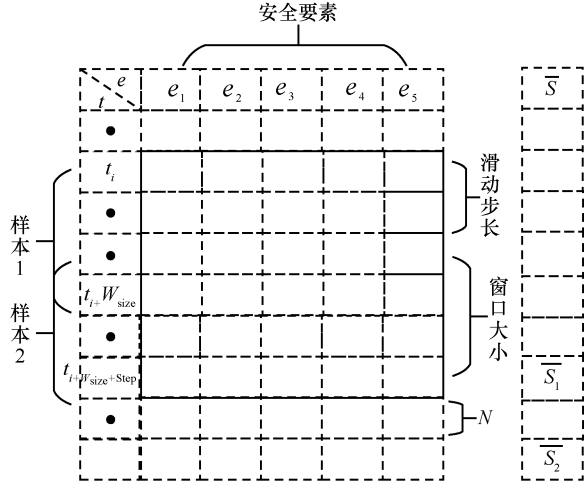


图2 样本构造方法
Figure 2 Sample construction method

算法1 数据重构算法

输入 原始数据集 S , 窗口大小 W_{size} , 特征列 f , 目标列 $target$, 预测时长 N 。

输出 重构数据集 S_N

- 1) 初始化 $S, W_{size}, f, target, N$ 。
- 2) 利用滑动窗口将 t 时刻的 f 和 $target$ 进行数据重构, 生成新的特征和目标集合 $X_t^f = S[t:t+W_{size}, f]$, $Y_t^f = S[t+N-1, target]$ 。
- 3) 使用 reshape 函数对 X_t^f, Y_t^f 进行重塑, 得到 $R_X_t^f, R_Y_t^f$ 。
- 4) 将前 m 个特征列 f 生成的 $R_X_t^f$ 通过 concatenate 函数进行拼接, 形成输入数据 $X_t = [R_X_t^1, R_X_t^2, R_X_t^3, \dots, R_X_t^m]$ 。
- 5) 选取一定的比例分割数据集, 得到重构数据集 S_N 。

1.2 Attention-BSRU 预测方法

针对工业互联网安全态势的影响因素多、具有时序性等特点, 本文使用 BSRU 为基础架构, 利用 CNN 提取多属性安全要素中的重要信息, 引入注意力机制赋予各属性不同的权重。Attention-BSRU 预测模型结构如图3所示。

1.2.1 卷积层

考虑到网络安全数据是具有时间性的多元变量, 且不同特征之间存在耦合性, 本文采取一维卷积神经网络, 提取输入样本数据 S_N 的局部特征, 将抽象数据特征进行融合, 得到新的特征, 作为双向 SRU 层的输入。

卷积层的输入为 X_t 。根据式(7)对 X_t 进行卷积操作。

$$J = f(W_d \otimes X_t + b_d) \quad (7)$$

其中, $f(\cdot)$ 为激活函数, 选取 Tanh 函数, 还可选用 Sigmoid、Relu 等, W_d 为权重矩阵, d 为卷积核大小, b_d 为偏置, $\otimes$ 为卷积运算。通过卷积后, 得到新的特征 $J = [c_1, c_2, \dots, c_{n-d+1}]$, 作为双向 SRU 层的输入序列。

1.2.2 双向 SRU 层

双向 SRU 层根据卷积层提取的数据捕获数据间的时间相关特性, 从正反两个方向处理数据, 提高预测的准确度, 通过并行化计算, 提高训练时间性能。

为了加速循环神经网络 (RNN, recurrent neural network) 的训练, 本文选用 SRU 单元结构。SRU 是 Lei 等^[16]为了解决 RNN 训练时间长的问

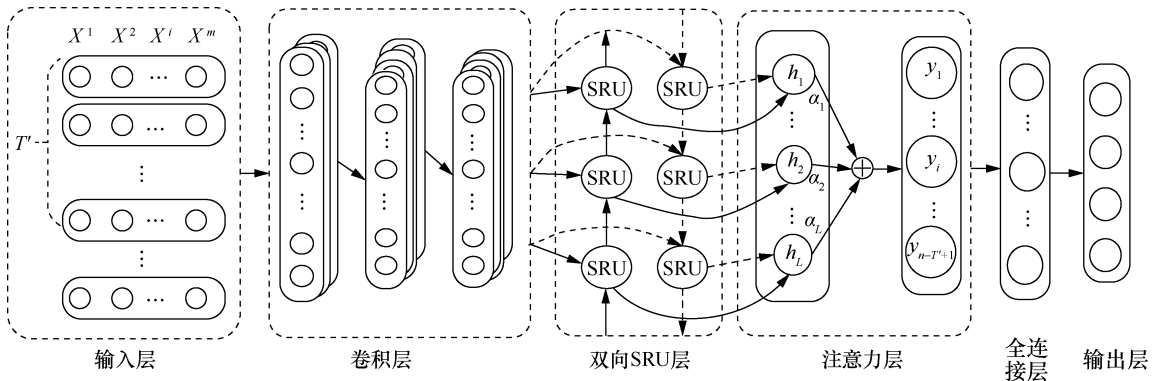


图3 Attention-BSRU 预测模型结构
Figure 3 The structure of the Attention-BSRU prediction model

网，基于长短期记忆（LSTM，long short-term memory）网络提出的一种变体结构。SRU 单元丢弃了原有循环结构中数据间的依赖关系，实现了并行化计算，减小了计算成本。SRU 的结构如图 4 所示。

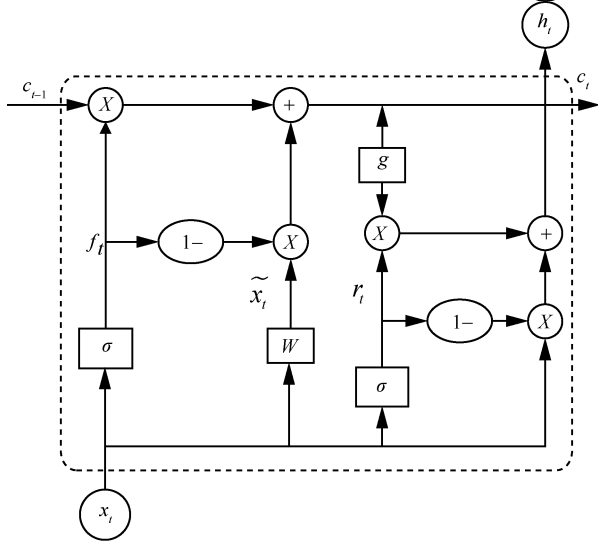


图 4 SRU 结构
Figure 4 SRU structure

单层 SRU 的计算可分为两部分：轻度循环和高速网络。计算过程如下。

$$\tilde{x}_t = Wx_t \quad (8)$$

$$f_t = \sigma(W_f x_t + v_f \odot c_{t-1} + b_f) \quad (9)$$

$$c_t = f_t \odot c_{t-1} + (1 - f_t) \odot \tilde{x}_t \quad (10)$$

$$r_t = \sigma(W_r x_t + v_r \odot c_{t-1} + b_r) \quad (11)$$

$$h_t = r_t \odot g(c_t) + (1 - r_t) \odot x_t \quad (12)$$

其中， W 、 W_f 和 W_r 为对应输入的权重矩阵； v_f 、 v_r 、 b_f 和 b_r 为参数向量； x_t 为 t 时刻的输入向量， $\tilde{x}_t$ 表示线性运算； r_t 为重置门，用于计算输出状态 h_t ； c_{t-1} 表示 $t-1$ 时刻 SRU 单元的状态向量，但是 c_{t-1} 却记录了 $t-k$ 到 $t-1$ 时刻对 t 时刻输出的影响； $\odot$ 为逐元素相乘， $(1-r_t) \odot x_t$ 是跳跃连接，可改善伸缩性，允许梯度直接传播到上一层^[17]； σ 为 Sigmoid 函数， $g(\cdot)$ 为输出状态 h_t 的激活函数——Tanh 函数。

轻度循环(式(8)~式(10))读取输入数据 x_t 并捕获顺序状态 c_t 的序列，获取序列信息。高速网

络(式(11)~式(12))促进了基于梯度的深层网络的训练，生成最终的输出状态。

相较于 LSTM、GRU 等循环单元，本文使用 SRU，主要是因为 SRU 的门运算和输入转换仅取决于循环的当前输入，删除 h_{t-1} 的影响，使用逐点乘积来进行并行化运算，同时记忆单元 c_t 仍然依赖上一时间步 c_{t-1} ，既保留了时间相关性，又减小了计算代价。

双向 SRU 层由正向 SRU 和反向 SRU 组成，若 t 时刻正向 SRU 输出的隐藏状态为 $\bar{h}_t$ ，反向 SRU 输出的隐藏状态为 $\bar{h}_t$ ，则双向 SRU 层输出的隐藏状态 h_t 如下。

$$h_t = \bar{h}_t \oplus \bar{h}_t \quad (13)$$

将卷积层的输出向量 J 输入双向 SRU 层，经正向 SRU 和反向 SRU 的遗忘门 f_t 和复位门 r_t 对 J 的特征信息进行提取，最终输出 $h_t = [\bar{h}_t, \bar{h}_t]$ 。双向 SRU 层不仅实现了数据的长期记忆，还能同时从过去和未来两个方向处理数据，挖掘更多时间序列中的特征，提高预测的准确度。

1.2.3 注意力层

由于输入是多属性的安全要素，且不同安全要素间的重要性差异不同。本文通过注意力层调整输入特征的权重，获取序列的完整特征表示，计算预测数值。

Attention 机制可以看作一个关键特征提取器，主要进行加权求和操作，通过调整输入特征的权重，改变不同特征对输出的影响程度，提高预测能力。

将双向 SRU 层的输出 h_t 输入注意力层，然后通过对不同特征向量的权值分配，更新权重参数矩阵，得到最优矩阵，输出融合后的安全态势值 y_t 。计算步骤如下。

1) 计算双向 SRU 层隐藏状态值与不同特征属性之间的相似性得分 $\text{score}(h_t)$ ，用于评估对输出的影响程度。

$$\text{score}(h_t) = u_t^T \tanh(h_t) \quad (14)$$

其中， u_t^T 为权重矩阵， h_t 表示双向 SRU 隐藏状态值。

2) 通过 Softmax 函数归一化，生成所有元素

权重之和为 1 的概率向量 β_t ，得到最终的注意力权重系数。

$$\beta_t = \frac{\exp(\text{score}(h_t))}{\sum_{i=1}^m \exp(\text{score}(h_i))} \quad (15)$$

3) 将生成的注意力权重与输入数据进行加权计算，得到 t 时刻网络安全态势值 y_t 。

$$y_t = \sum_{i=1}^m \beta_i h_i \quad (16)$$

4) 将得到的网络安全态势值送入全连接层，使用 Sigmoid 函数进行预测。

2 实验仿真

2.1 实验环境

国家互联网应急中心 (CNCERT) 发布的每周态势报告依托公共互联网网络安全监测平台对安全事件自主监测，其实验拓扑结构如图 5 所示。

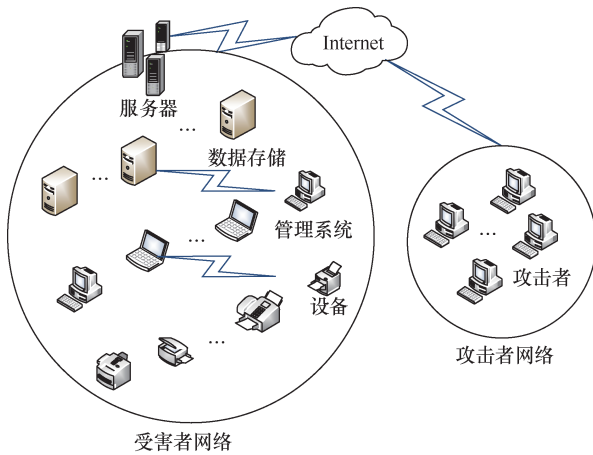


图 5 实验拓扑结构
Figure 5 Experimental topological structure

网络结构被分为两部分：攻击者网络和受害者网络，收集的数据中包含了典型的植入后门、网页仿冒、恶意程序等网络威胁的数量。

实验选取 2017 年第 32 期到 2020 年第 41 期共 167 期的每周态势报告^[18]作为实验数据，选取其中的 5 个安全要素：受感染主机数量、被篡改网站数量、被植入后门网站数量、仿冒页面数量和新增安全漏洞数量，按照工业互联网安全态势评价指标和相关性分析结果赋予安全要素不同的安全等级和权重指数，用于评估网络安全态势值。

由于数据集中没有明确的资产信息，本文将数据中收录的安全产品、操作系统、网络设备、Web 应用和应用程序 5 种受安全漏洞影响的对象作为资产模拟对象，将漏洞、恶意程序和网页仿冒 3 种攻击事件模拟威胁性，然后按式(3)~式(4)计算出威胁性指数和资产安全风险指数，最后通过式(5)得到 167 周的网络安全态势值。具体网络安全态势值量化模型如图 6 所示。

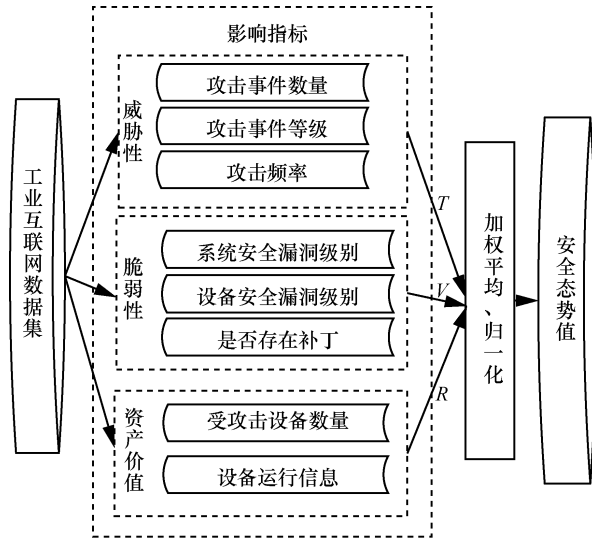


图 6 态势值量化模型
Figure 6 Quantification model of situation value

2.2 参数设置

按 9:1 的比例将经过重构的数据集分为训练集和测试集，在本文预测模型中，为保证数据在时间上的连续性，选取滑动步长 $\text{Step}=1$ ，窗口大小 $W_{\text{size}}=4$ ，特征数 $\text{features}=5$ ，归一化在 $[-1,1]$ 的样本集，后文为了验证模型在多步预测上的优势，分别选取预测时长 $N=1,5,10,15$ ，得到数据集 S_1, S_5, S_{10}, S_{15} 。卷积层的卷积核数目依次设置为 32, 64... 卷积窗口都是 2，激活函数选取 Tanh 函数，如果增加卷积网络，其卷积核依次以 2 的倍数增加。因为训练样本的输入维度较小，不宜使用较大的网络结构，本文采用单层的 BSRU，其中神经节点数为 16，激活函数采用 Tanh 函数，将卷积层提取的抽象特征进行回归预测，为了防止过拟合，添加 L2 正则化，惩罚系数 $\lambda=0.001$ 。输出层使用 Sigmoid 函数作为激活函数。

采用 Adam 优化算法^[19]来训练该模型，学习率 $\text{lr}=0.001$ ，衰减因子为默认参数。通过不断更

新模型参数, 加快模型的收敛速度, 使用均方误差函数(式(17))作为损失函数, batch_size=1 进行在线学习, 训练次数 epoch=1 000。本文实验基于 Keras 深度学习框架, 仿真平台为 Intel Xeon CPU E3-1231 v3 3.40 GHz, 24 GB 内存, Windows10 64 位操作系统, 不采用 GPU 加速。网络结构的参数根据数据集通过实验微调所得。

$$MSE = \frac{1}{n} \sum_{i=1}^n (y_i - y'_i)^2 \quad (17)$$

其中, y_i 和 y'_i 为第 i 个安全态势值的真实值和预测值, n 为预测样本个数。

2.3 评价指标

为了能够准确地评估不同预测模型的性能, 参考文献[20-21]的研究, 采用平均绝对误差(MAE, mean absolute error)、平均绝对百分比误差(MAPE, mean absolute percentage error)和均方根误差(RMSE, root mean square error)作为评价指标, 分别表示如下。

$$MAE = \frac{1}{n} \sum_{i=1}^n |y_i - y'_i| \quad (18)$$

$$RMSE = \sqrt{\frac{1}{n} \sum_{i=1}^n (y_i - y'_i)^2} \quad (19)$$

$$MAPE = \frac{1}{n} \sum_{i=1}^n \frac{|y_i - y'_i|}{y_i} \quad (20)$$

其中的参数与式(17)一致, 在安全态势预测中, 以上指标的值越小, 表明预测越准确, 模型越好。

2.4 与单一网络预测模型对比

为了验证融合网络的优越性, 本文模型同单一的 CNN、SRU、SVM、BP 等传统预测网络模型进行对比实验。考虑到神经网络权重初始化的随机性会导致实验结果与真实结果存在一定偏差, 实验过程中对所有预测模型进行多次训练取平均值, 以减小误差。本文数据选取 10 次实验数据的平均值作为比较数据, 同时使用本文提出的评价指标和迭代时间作为性能评价标准, 预测时长 $N=10$ 。结果如表 3 所示, 相比单独使用 CNN、SRU 的预测模型, 本文所构造的模型将预测误差降低了 43%、40.8%。

表 3 单一网络预测模型的预测结果
Table 3 The results of a single network prediction model

预测模型	MAE	RMSE	MAPE
Attention-BSRU	0.018 3	0.022 1	3.780 1%
CNN	0.032 1	0.036 3	6.524 8%
SRU	0.030 9	0.033 2	6.376 6%
BLSTM	0.028 9	0.034 9	6.108 6%
BP	0.033 8	0.039 3	6.978 5%
SVM	0.058 3	0.072 4	12.895 5%

各预测模型的预测危险级别与真实危险级别的对比如图 7 所示, 可以看出 SRU 网络不能很好地预测网络危险级别, 如第 13 周就将危险级别 4 误报为危险级别 3, 而增加了 CNN 对特征提取后的融合网络, 减小了误报率。但是在第 10 个预测点处存在误差, 实际的危险级别属于 5, 而预测出的结果对应的危险级别是 4, 管理者采取的措施在面对大量网络威胁时, 防范不足, 会导致重大危险。比较所有预测模型, 在该位置的预测都存在误差, 可能是评估模型在临界点处存在误差或者该点为异常点所致。

各预测模型的态势值对比如图 8 所示, 从整体趋势上分析, 本文方法所得结果的拟合度最高, SVM 预测模型的效果最差, 只能预测大概的变化趋势, 而其余预测网络可以很好地预测数据的变化趋势, 但拟合效果稍逊于融合网络模型, 这表明融合 CNN 和 BSRU 的网络模型通过对多属性安全要素来预测态势值的有效性, 既可以解决历史数据的长期依赖问题, 也可以更好地提取数据特征, 提高了预测的准确度。

时间序列预测的评判标准不仅要考虑预测的准确度, 还要考虑不同预测时长下的准确度。本文针对不同预测模型在不同预测时长下的预测误差进行对比, 取预测时长 $N=1, 5, 10, 15$, 结果如图 9 所示。

从图 9 可以看出, 在相同的预测时长下, 本文网络模型比其他单一网络预测模型具有更好的预测效果, 而随着预测时长的增加, 预测效果有所改变, 总体而言, 本文模型在多步预测时优于单步预测, 预测效果优于其他预测模型。但是预测时长过短或过长都会导致预测效果变差, 所以模型的鲁棒性略差。

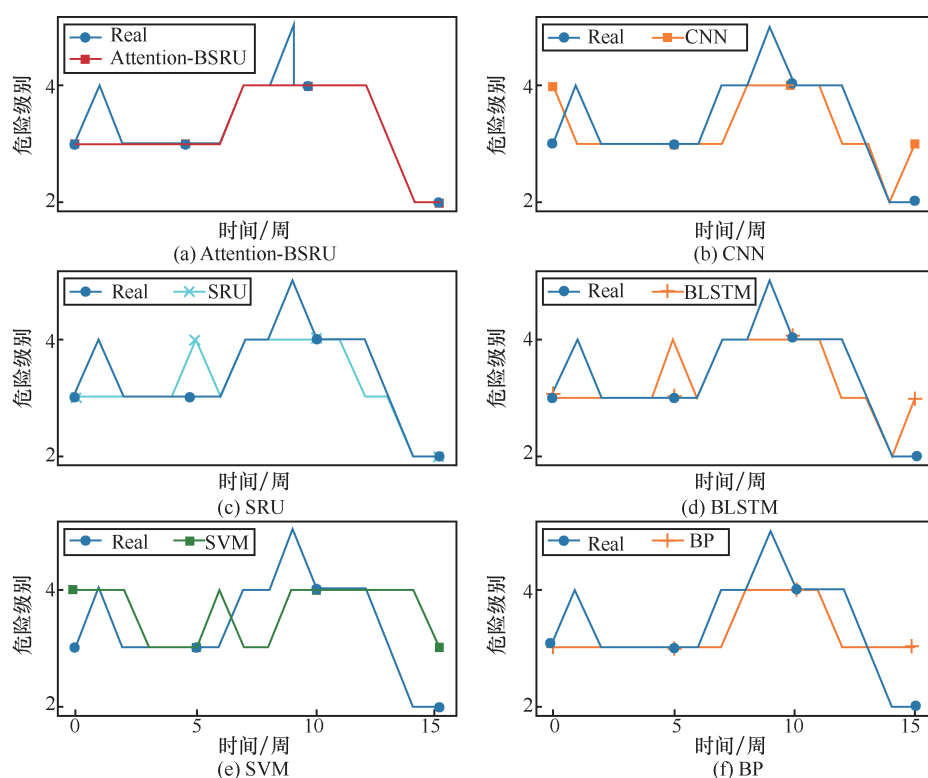


图 7 预测危险级别与真实危险级别对比
Figure 7 Comparison of prediction level and danger level

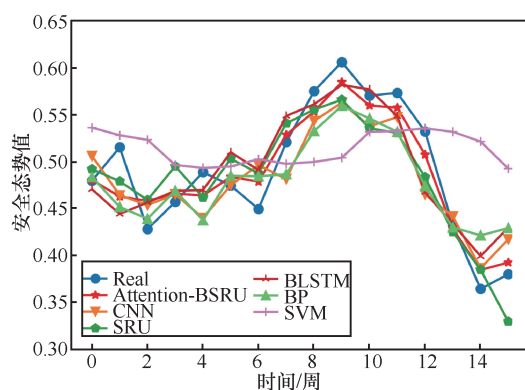


图 8 预测模型的态势值对比
Figure 8 Comparison of situation values of the prediction model

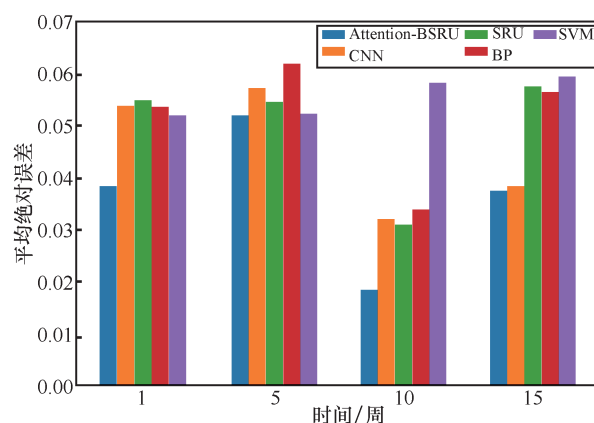


图 9 不同预测时长下的平均绝对误差对比
Figure 9 Comparison of MAE under different prediction duration

2.5 融合网络预测模型对比

为了验证本文所使用的 SRU 单元在时间序列数据处理效率上的优越性, 将 Attention-BSRU 模型中的 SRU 单元替换为 LSTM、GRU 单元, 其他参数不改变, 得到 Attention-BGRU 和 Attention-BLSTM 模型并进行对比实验, 同时与不加注意力机制的 CNN-BSRU 模型和基于注意力机制的 AIS-LSTM^[22]模型预测值进行对比实验。结果如表 4 所示, 反映了 Attention-BSRU 模型相比其他融合网络模型的突出优势。

表 4 融合网络预测模型的预测结果

Table 4 The prediction results of the fusion network prediction model

预测模型	MAE	RMSE	MAPE	时间/s
Attention-BLSTM	0.026 6	0.030 2	5.610 3%	510.913 6
Attention-BGRU	0.025 6	0.030 2	5.354 9%	462.312
Attention-BSRU	0.018 3	0.022 1	3.780 1%	401.663 7
CNN-BSRU	0.025 7	0.032 7	5.185 3%	393.638 9
AIS-LSTM	0.037 8	0.044 6	7.553 3%	864.448 2

相比 Attention-BLSTM、Attention-BGRU 模型, 本文将误差分别降低了 31.2%和 28.5%, 训练时间分别提高了 21.4%和 13.1%, 表明 SRU 单元比 LSTM、GRU 单元在预测的准确度和训练时间上都有较大提升; 相比 CNN-BSRU 模型, 本文模型的训练时间增加了 2%, 误差降低了 28.8%, 这表明使用注意力机制可以降低模型的预测误差, 因此可以在损失少量时间的前提下, 使用注意力机制提升预测的准确度; AIS-LSTM 模型的训练时间、预测绝对误差都不及本文模型。

图 10 反映了不同融合网络预测模型训练损失随迭代次数的变化规律, 其中 AIS-LSTM 的损失下降速度最慢, Attention-BGRU 的损失下降速度最快, Attention-BSRU 的下降速度稍慢于 Attention-BGRU 模型; 各模型都有一定限度的振荡, 但最后都趋于平稳, 表明各模型的收敛性、稳定性相似; 但是 Attention-BSRU 的初始损失值比其他模型的初始损失值都大。从稳定性、收敛性和学习速率来看, Attention-BGRU 表现最好, Attention-BSRU 次之, AIS-LSTM 最差。

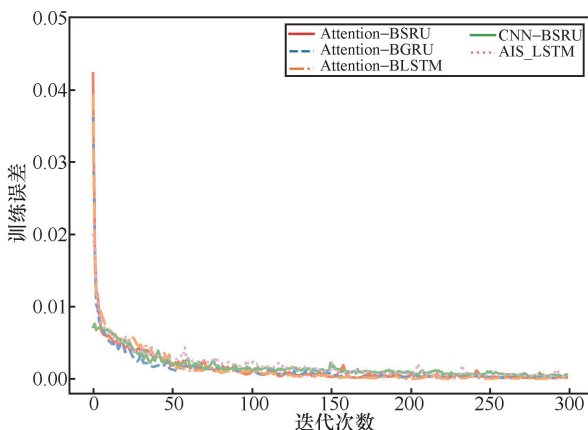


图 10 融合网络预测模型的训练损失曲线
Figure 10 Training loss curve of fusion network prediction mode

图 11 反映了不同融合网络预测模型的预测态势值与实际值的对比情况, 从图中可以看出 Attention-BSRU 的拟合效果较好, AIS-LSTM 的拟合效果较差。综合分析, 在牺牲少量稳定性、收敛性和学习速率的代价下, 可以换取训练时间性能和拟合效果的提升, 在对时间要求较高的工控领域, 本文所提的模型优于其他模型。

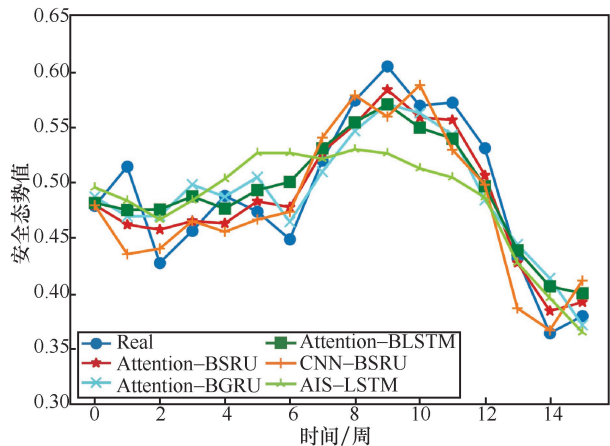


图 11 融合网络预测模型的预测态势值与实际值对比
Figure 11 Comparison of predicted situation value and actual value of the fusion network prediction model

3 结束语

针对存在时间相关性的工业互联网安全态势值受多种网络安全态势要素的影响, 且广泛应用于时间序列处理的 LSTM、GRU 循环单元计算代价较大问题, 本文提出一种融合注意力机制和 BSRU 的工业互联网安全态势值预测方法。该方法利用 CNN 提取网络安全态势要素, 使用 BSRU 保存历史信息, 充分挖掘安全态势要素之间的相互依赖关系, 避免对评估态势值的依赖, 利用注意力机制调整输入特征的权重, 提高对重要特征的关注度, 使预测更准确。本文模型使用的 SRU 单元相比其他循环单元具有更好的预测效果, 还能减少计算代价, 时效性更好。相比传统的单一网络预测模型, 该模型预测效果更好, 在多步预测时优势更明显, 同时在相同预测时长下, 本文预测模型略微优于其他预测模型。通过实验数据和仿真验证了本文模型预测的准确性和高效性。但是该方法还存在一些需要改进的地方, 下一步的研究方向为: 构建更加完善的工业互联网安全态势评估模型, 使临界点处的网络安全态势值具有很好的辨识度; 采用一些优化算法优化网络参数, 进一步提高模型的预测准确度。

参考文献:

- [1] LIU X, YU J, LV W, et al. Network security situation: from awareness to awareness-control[J]. Journal of Network and Computer Applications, 2019, 139: 15-30.
- [2] WU J, OTA K, DONG M, et al. Big data analysis-based security

- situational awareness for smart grid[J]. IEEE Transactions on Big Data, 2016, 4(3): 408-417.
- [3] LIANG W, LONG J, CHEN Z, et al. A security situation prediction algorithm based on HMM in mobile network[J]. Wireless Communications & Mobile Computing, 2018, 2018: 1-11.
- [4] HU J, Ma D, LIU C, et al. Network security situation prediction based on MR-SVM[J]. IEEE Access, 2019, 7: 130937-130945.
- [5] 谢丽霞, 王亚超, 于巾博. 基于神经网络的网络安全态势感知[J]. 清华大学学报(自然科学版), 2013, 53(12): 1750-1760.
- XIE L X, WANG Y C, YU J B. Network security situation awareness based on neural networks[J]. Journal of Tsinghua University(Science and Technology), 2013, 53(12): 1750-1760.
- [6] ZHANG H, HUANG Q, LI F, et al. A network security situation prediction model based on wavelet neural network with optimized parameters[J]. Digital Communications and Networks, 2016, 2(3): 139-144.
- [7] XIAO P, XIAN M, WANG H. Network security situation prediction method based on MEA-BP[C]//2017 3rd International Conference on Computational Intelligence & Communication Technology (CICIT). IEEE, 2017: 1-5.
- [8] 杨宏宇, 张旭高. 基于自修正系数修匀法的网络安全态势预测[J]. 通信学报, 2020, 41(5): 196-204.
- YANG H Y, ZHANG X G. Self-corrected coefficient smoothing method based network security situation prediction[J]. Journal on Communications, 2020, 41(5): 196-204.
- [9] 张任川, 张玉臣, 刘璟, 等. 应用改进卷积神经网络的网络安全态势预测方法[J]. 计算机工程与应用, 2019, 55(6): 86-93.
- ZHANG R C, ZHANG Y C, LIU J, et al. Network security situation prediction method using improved convolution neural network[J]. Computer Engineering and Applications, 2019, 55(6): 86-93.
- [10] LI Y, LIU B, ZHANG L, et al. Fast trajectory prediction method with attention enhanced SRU[J]. IEEE Access, 2020, 8: 206614-206621.
- [11] LUONG M T, PHAM H, MANNING C D. Effective approaches to attention-based neural machine translation[J]. arXiv preprint arXiv:1508.04025, 2015.
- [12] 丁华东, 许华虎, 段然, 等. 基于贝叶斯方法的网络安全态势感知模型[J]. 计算机工程, 2020, 46(6): 130-135.
- DING H D, XU H H, DUAN R, et al. Network security situation awareness model based on bayesian method[J]. Computer Engineering, 2020, 46(6): 130-135.
- [13] 程家根. 基于机器学习的网络安全态势感知模型研究与实现[D]. 南京邮电大学, 2020.
- CHENG J G. Research and implementation of network security situation awareness model based on machine learning[D]. Nanjing: Nanjing University of Posts and Telecommunications, 2020.
- [14] CHERDANTSEVA Y, BURNAP P, BLYTH A, et al. A review of cyber security risk assessment methods for SCADA systems[J]. Computers & security, 2016, 56: 1-27.
- [15] HUANG K, ZHOU C, TIAN Y C, et al. Assessing the physical impact of cyberattacks on industrial cyber-physical systems[J]. IEEE Transactions on Industrial Electronics, 2018, 65(10): 8153-8162.
- [16] LEI T, ZHANG Y, WANG S I, et al. Simple recurrent units for highly parallelizable recurrence[J]. arXiv preprint arXiv:1709.02755, 2017.
- [17] ZILLY J G, SRIVASTAVA R K, KOUTNIK J, et al. Recurrent highway networks[C]//International Conference on Machine Learning. 2017: 4189-4198.
- [18] CNCERT. 2017年至2020年网络安全信息与动态周报[EB]. CNCERT. Network security information and trends weekly report from 2017 to 2020[EB].
- [19] BOCK S, WEIB M. A proof of local convergence for the Adam optimizer[C]//2019 International Joint Conference on Neural Networks (IJCNN). IEEE, 2019: 1-8.
- [20] KHWAJA A, ZHANG X, ANPALAGAN A, et al. Boosted neural networks for improved short-term electric load forecasting[J]. Electric Power Systems Research, 2017, 143: 431-437.
- [21] ZENG L, REN W, SHAN L J N. Attention-based bidirectional gated recurrent unit neural networks for well logs prediction and lithology identification[J]. Neuro Computing, 2020, 414: 153-171.
- [22] MUNKHDALAI L, MUNKHDALAI T, PARK K H, et al. An end-to-end adaptive input selection with dynamic weights for forecasting multivariate time series[J]. IEEE Access, 2019, 7: 99099-99114.

[作者简介]



胡向东(1971—),男,四川广安人,博士,重庆邮电大学教授、博士生导师,主要研究方向为物联网安全智能理论与技术、智能感知、网络化测量与工业大数据安全、复杂系统建模仿真与优化。



田正国(1995—),男,江苏徐州人,重庆邮电大学硕士生,主要研究方向为工业互联网安全。