

基于DBN-BiLSTM-Attention的工控网络入侵检测算法

邢温豪, 郑梦策

(浙江万里学院 信息与智能工程学院, 浙江 宁波 315100)

摘要: 当前工业控制网络面临的攻击日益复杂多样, 网络环境中的数据展现出显著的海量性、高维性及强时序性等特点, 给传统的入侵检测技术带来了诸多挑战, 包括特征提取复杂性增加、检测精度低下以及模型泛化受限等。为此, 提出一种融合深度信念网络、BiLSTM与注意力机制的工控网络入侵检测算法。首先, 利用深度信念网络和BiLSTM分别对非线性特征和长距离时间依赖信息进行深度特征提取; 其次, 引入注意力机制, 使模型能专注于识别网络流量数据中与工控网络被攻击时刻相邻的特征变化模式; 最后, 利用softmax分类器进行分类。实验结果表明, 该算法在天然气管道网络数据集上的检测准确率达到98.81%, 多项指标优于当前领先的算法模型。

关键词: 工控网络; 入侵检测; 深度信念网络; BiLSTM

DOI: 10.11907/rjdk.241943

中图分类号: TP183

文献标识码: A

文章编号: 1672-7800(2025)012-0176-07

扫描二维码阅读全文:



Industrial Control Network Intrusion Detection Algorithm Based on DBN-BiLSTM-Attention

XING Wenhao, ZHENG Mengce

(School of Information and Intelligent Engineering, Zhejiang Wanli University, Ningbo 315100, China)

Abstract: The attacks faced by current industrial control networks are becoming increasingly complex and diverse. The data in the network environment exhibits significant characteristics such as massive, high-dimensional, and strong temporal nature, which brings many challenges to traditional intrusion detection techniques, including increased complexity in feature extraction, low detection accuracy, and limited model generalization. Therefore, a intrusion detection algorithm for industrial control networks is proposed, which integrates deep belief networks, BiLSTM, and attention mechanisms. The algorithm first utilizes deep belief networks and BiLSTM to extract deep features from nonlinear features and long-range time-dependent information, respectively; Secondly, an attention mechanism is introduced to enable the model to focus on identifying feature change patterns in network traffic data that are adjacent to the time when the industrial control network is attacked; Finally, use the Softmax classifier for classification. The experimental results show that the detection accuracy of this algorithm on the natural gas pipeline network dataset reaches 98.81%, and multiple indicators are superior to the current leading algorithm models.

Key Words: industrial control network; intrusion detection; deep belief networks; BiLSTM

0 引言

工业控制网络融合了互联网与自动化控制技术, 但其开放性特点却削弱了传统工业系统的物理安全屏障, 使得互联网安全威胁能够渗透至工业控制领域^[1]。近年来, 工

业控制网络频遭网络攻击, 工控安全因此成为网络安全领域的紧迫议题。

深度学习因其卓越的海量数据特征提取能力, 在工控网络入侵检测领域得到了广泛应用。例如, Zhang等^[2]提出基于深度信念网络(Deep Belief Network, DBN)与长短期记忆网络(Long Short-Term Memory, LSTM)的电力工控流

收稿日期: 2024-11-06

基金项目: 国家自然科学基金项目(62002335)

作者简介: 邢温豪(2002-), 男, 浙江万里学院信息与智能工程学院学生, 研究方向为网络空间安全; 郑梦策(1990-), 男, 博士, 浙江万里学院信息与智能工程学院副教授, 研究方向为信息安全与密码学。

量异常检测模型,利用 DBN 提取数据的非线性特征,可以在一定程度上提高检测效率;同时利用 LSTM 提高传统浅层机器学习的表示能力。实验结果表明,该模型的准确率达到 97.3%,AUC 达到 0.927。Lu 等^[3]提出基于种群极值优化 DBN 的工控网络入侵检测方法,使用种群极值优化算法来确定 DBN 的参数,包括隐藏单元数量、小批量大小和学习率,有效提高了检测效率。Wei 等^[4]提出一种新的联合优化算法来优化工控入侵检测模型中 DBN 的网络结构。首先,设计一种基于自适应惯性权重与学习因子的粒子群算法;其次,利用鱼群的聚类、觅食等行为对粒子群算法进行优化,寻找初始优化解;最后,在获取初始优化解的基础上,算法进一步采用自调整交叉概率和变异概率的遗传算子对粒子群算法进行优化,以搜索全局最优解。实验结果表明,该算法显著优化了模型性能,使平均分类精确度至少提升了 1.3%,且平均检测时长至少缩减了 24.69%。Monfared 等^[5]基于深度神经网络(Deep Neural Network, DNN)开发了一种精确的工控入侵检测算法,使用卷积网络来检测数据包的空间,通过 LSTM 检测数据包之间的时间依赖性,有效缩短了检测时间,提高了检测精度。

尽管深度学习技术在工控网络入侵检测领域展现出的性能显著超越了传统机器学习方法,但在应对复杂的网络入侵场景时仍具有一些局限性。具体而言,在特征提取环节,DBN 凭借其强大的非线性处理能力,在海量数据环境下能有效抽取复杂特征,但并不直接支持时序序列特征相关性的学习,这在一定程度上限制了其在需要时间序列分析场景下的应用效能。LSTM 虽然擅长捕捉时序序列中的依赖关系,为入侵检测模型提供了动态分析的能力,但其仅能单向提取时序特征,未全面考虑特征间的前后双向影响,这可能影响检测的全面性和准确性。此外,LSTM 模型在处理复杂网络数据时还可能伴随较高的误报率。针对上述问题,本文提出一种融合 DBN、双向长短期记忆网络(Bidirectional Long Short-Term Memory, BiLSTM)和注意力机制(Attention Mechanism)的工控网络入侵检测算法。BiLSTM 网络包含记忆单元和门控机制,能够有效识别序列中的长距离依赖关系,对于网络流量中隐含的时空特性提供了强大的建模能力。通过分析每个特征,BiLSTM 网络将最后一个网络单元的正向输出与反向输出进行串联,形成一个具有时空特性的网络流量表示。这种级联结构有助于综合考虑过去和未来的信息,使模型更加全面地理解序列数据的时序特性。引入的注意力机制使模型能专注于识别数据中与工控网络被攻击时刻相邻的特征变化模式,进一步提升检测效率。

本文具体创新点为:①通过 DBN 和 BiLSTM 进行流量特征提取。DBN 进行纵向工控网络流量深度特征提取,堆叠 3 层,逐层提取特征能够帮助模型从低级到高级逐渐学习数据的层次化特征,使其既可以捕捉到简单模式,又能

处理复杂的攻击模式。BiLSTM 进一步结合横向工控网络流量的时序信息,堆叠 2 层,第一层通过较少的神经元捕捉简单的时序模式,第二层通过更多神经元进一步加强模型对复杂时序依赖关系的学习能力,与 DBN 层提取的数据特征进行时序互补。这种从粗略到细致地逐步加深网络层次的结构设计模仿了人类的学习方式,即首先掌握基本概念,然后深入理解细节和复杂关系,尤其适用于分析复杂、高维和时序性强的工控网络数据流量;②引入了注意力机制。在工业控制网络中,攻击行为往往伴随着流量的剧烈变化,但这些变化可能只出现在特定时刻,且变化的模式相对较小。传统方法可能无法有效捕捉到这些突发变化,而注意力机制使得模型能够聚焦于攻击发生时的关键特征,提升对局部特征的敏感性,增强了模型对细微变化的响应能力,从而提高了检测准确性。

1 理论基础

1.1 DBN

DBN 是一种由多层无监督的受限玻尔兹曼机(Restricted Boltzmann Machine, RBM)和一层有监督的反向传播(Back Propagation, BP)网络构成的深度生成神经网络模型^[6-7]。结构见图 1。RBM 通过最小化其能量函数来学习特征。能量函数定义了输入层与隐藏层之间的交互,通过调整权重和偏置项来优化,使 RBM 能够学习到最能代表输入数据的特征。每层 RBM 包含 1 个可见层(输入层)和 1 个隐藏层,以上一层的隐藏层输出作为下一层的输入。DBN 的训练包括逐层预训练和微调两个阶段。在逐层预训练中,RBM 采用无监督学习方法。首先,由 RBM1 对原始输入数据进行训练,学习其特征表示;其次,将 RBM1 的隐藏层输出作为 RBM2 的输入继续训练,以此类推,逐层提取数据的高层次特征。预训练完成后,通过 BP 算法对整个网络进行有监督的微调,以优化权重参数,使模型更好地适应目标任务。BP 算法通过计算误差梯度,将误差信号反向传播至每一层的权重进行更新。各层间的输入与输出相互依赖,逐层构建数据的深度表示,而最上层的输出用于实际任务,如分类概率的输出。逐层预训练不仅有助于避免梯度消失,而且能显著提高 DBN 的训练效率。通过逐层优化,DBN 能够在更短的时间内达到更好的训练效果,且能捕获数据中的高层次抽象特征。对于复杂的工控网络数据,DBN 能够揭示其间的深层次联系与规律,提取其本质特征,将高维的网络数据映射到低维空间,从而简化问题,提高入侵检测效率与准确性。

1.2 BiLSTM

BiLSTM 是 LSTM 的变体,用于处理序列数据,如自然语言文本或时间序列^[8]。在工控网络流量分析中,数据包在攻击发生时刻的时序属性往往包含有用的特征信息,因

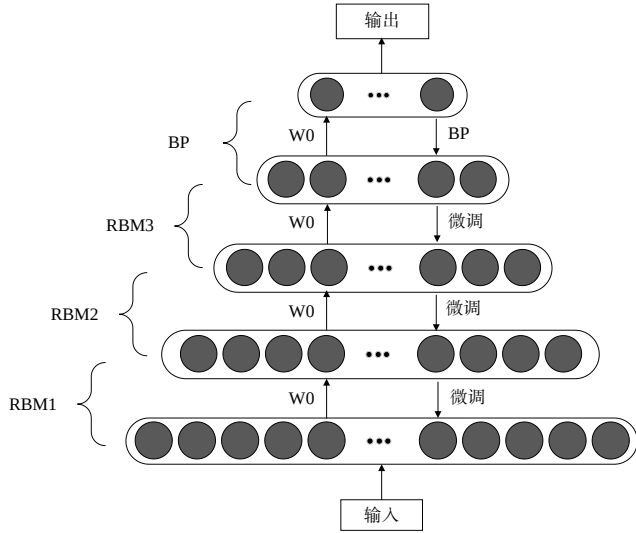


Fig. 1 Structure of DBN model

图1 DBN模型结构

此需要在正反两个方向上进行特征提取。BiLSTM通过引入前向和后向两个方向的隐藏层状态,对输入序列同时进行正向和反向分析,能够有效捕获序列内的双向上下文关联特征,从而更好地理解与建模时序关系。其最大的优点在于能够同时在正向和反向两个方向提取序列数据的时序特征,其中正向隐藏层负责捕捉当前时刻之前的信息,反向隐藏层负责捕捉当前时刻之后的信息,最终输出为正向与反向隐藏状态的连接,提供了全局的上下文信息。BiLSTM模型结构见图2^[9]。

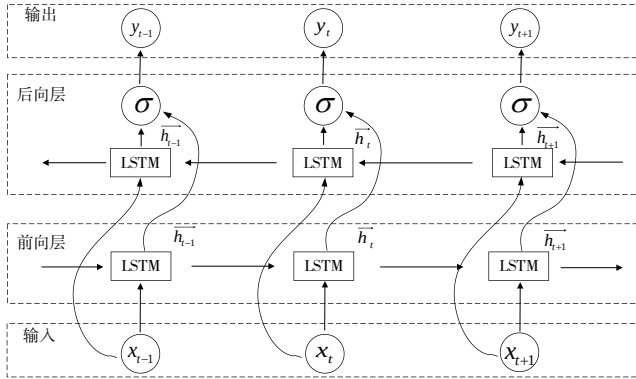


Fig. 2 BiLSTM model structure

图2 BiLSTM模型结构

BiLSTM的运算过程为:

$$\begin{cases} \vec{h}_t = \text{LSTM}(x_t, \vec{h}_{t-1}) \\ \overleftarrow{h}_t = \text{LSTM}(x_t, \overleftarrow{h}_{t+1}) \\ y_t = \sigma(W_y \cdot [\vec{h}_t, \overleftarrow{h}_t] + b_y) \end{cases} \quad (1)$$

式中: $\vec{h}_t$ 表示当前时间步 t 的正向隐藏层状态; $\overleftarrow{h}_t$ 表示反向隐藏层状态; W_y 、 b_y 分别为权重矩阵和偏执项; x 、 y 分别为模型的输入与输出值。

在时间步 t 上,反向LSTM特征提取的计算过程为:

$$\begin{cases} f_t = \sigma(W_f \cdot [h_{t+1}, x_t] + b_f) \\ i_t = \sigma(W_i \cdot [h_{t+1}, x_t] + b_i) \\ C_t = \tanh(W_c \cdot [h_{t+1}, x_t] + b_c) \\ C_t = f_t \otimes C_{t-1} \oplus i_t \otimes C_t \\ O_t = \sigma(W_o \cdot [h_{t+1}, x_t] + b_o) \\ h_t = O_t \otimes \tanh(C_t) \end{cases} \quad (2)$$

式中: h_t 表示当前时刻的输出,可传递到下一个时刻或作为最终输出; f_t 、 i_t 、 o_t 分别为遗忘门、输入门和输出门,用于控制信息的更新和输出; x_t 、 h_{t-1} 分别为当前输入和上一时刻的隐藏状态,用于计算各个门的激活值; W_f 、 W_i 、 W_c 、 W_o 为各个门的权重矩阵,用于学习时序数据的权重分配; C 为当前时刻的单元状态; b 为每个门的偏置项,是模型的可学习参数之一,用于调整每个门激活函数的输出。

1.3 注意力机制

注意力机制是一种高效的聚焦机制,允许模型在处理序列数据时聚焦于输入序列的不同部分,赋予不同位置信息不同的权重,使得模型在生成输出的每一步都能有针对性地关注输入序列的特定区域,而非一概而论地处理整个序列^[10]。图3为Attention值的计算过程。

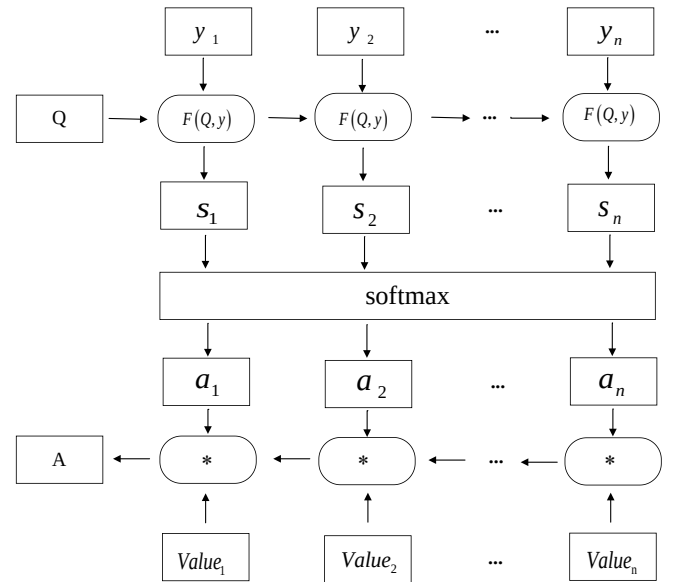


Fig. 3 Attention value calculation process

图3 Attention值计算过程

首先,对输入的键序列 $y = [y_1, y_2, \dots, y_n]$ 进行编码,得到一组查询向量 Q 。通过打分函数评估键与查询向量之间的相似度 s 。计算公式为:

$$s_i = F(Q, y_i) = V^T \tanh(W y_i + U Q) \quad (3)$$

式中: V 、 W 、 U 均为参数在训练过程中待学习的矩阵。

其次,运用softmax函数来标准化每一组的相似度向量,最终计算出每组输入向量的权重 a_i 。计算公式为:

$$a_i = \text{softmax}(F(Q, y_i)) = \frac{\exp(F(Q, y_i))}{\sum_{i=1}^n \exp(F(Q, y_i))} \quad (4)$$

最后,通过加权求和公式,对权重 a_i 及相应键值 $Value_i$ 的值向量进行计算,得到最终经过注意力机制优化的待分类特征 A 。计算公式为:

$$A = \sum_{i=1}^n a_i \quad (5)$$

2 算法构建

基于 DBN-BiLSTM-Attention 的工控网络入侵检测算法由包含 3 层 RBM 的 DBN 模块、2 个双向 LSTM 层构成的 BiLSTM 模块、注意力机制层及 Softmax 分类层构成。整体框架如图 4 所示。

2.1 数据预处理

在数据预处理阶段,删除缺失率超过 70% 的特征,以减少冗余并节约资源,并降低过拟合和不稳定性风险。高缺失率特征信息量极低,可能引入噪声或因填充假设不当而造成偏差,从而干扰模型学习。此外,删除这些特征可以简化模型结构,进一步提升训练效率。移除掉具有唯一价值的数据,同时采用标准化处理来减少数据变异造成的错误,保持特征值归一化在 $[0, 1]$ 区域,最终生成了特征向量并应用了独热编码。

2.2 训练模型堆叠

通过堆叠 3 层 DBN 来逐层提取多层次特征。第一层 RBM(256 个神经元)为浅层,负责从输入数据中提取基础特征。由于工控网络流量数据可能包含低级的时序和频率特征,较少的神经元有助于捕捉简单的特征模式,如流量的基本统计特征、协议类型等。第二层 RBM(512 个神经元)为中层,在第一层特征的基础上提取更复杂的组合特征。该层能够捕捉到不同流量模式之间的关系,如正常流量与攻击流量之间的差异,或网络流量中的潜在模式,如扫描行为、拒绝服务等。第三层 RBM(1 024 个神经元)为深层,进一步对上层特征进行抽象,提取更高阶、具有更强区分能力的特征。在工控网络中,攻击模式往往较为复杂,深层网络可以帮助模型识别更复杂的攻击类型,如高

级持续性攻击和新型攻击模式。较少的 256 个神经元有助于避免模型在第一层便过度拟合,而较多的 1 024 个神经元则能确保网络具有足够的表达能力来捕捉复杂的特征关系。工控网络流量数据往往具有较高的维度和时序性,逐层增加神经元数量有助于模型灵活地适应这些数据的特性,提高训练稳定性。此外,工控网络中的流量模式和攻击模式往往是动态变化的,合理的神经元分布可以根据不同的攻击模式和数据特性调整特征学习策略,保证模型的计算效率,避免不必要的计算开销。

在激活函数作用下,节点 h 的生成值用 φ_h 表示。节点 k 向节点 h 传递的权值由 W_{kh} 表示;学习步长由 η 表示,节点 i 的输出由 Q_i 表示,节点 j 在递归过程中的梯度损失由 φ_j 表示;输出节点的序列由 P 表示,数据 M 在节点 P 上的真实输出由 Q_{MP} 表示,数据 M 在节点 P 上的预期输出由 d_{MP} 表示,整体的数据训练序列由 M 表示。DBN 特征提取算法的伪代码为:

输入:原始数据 $A = \{a_1, a_2, a_3, \dots, a_n\}$,模型迭代次数 N ,偏置值 d ,权重值 W ;

步骤 1: 初始化, $d = 0, W = 0$;

步骤 2: 模型训练,for $n = 1$ to N :

2.1 计算输出模块的梯度差异

for a_i in A :

$$\varphi_h = a'_i(1 - a'_i) \sum_h W_{kh} \varphi_h$$

2.2 计算隐藏层的损失梯度值

for 每个隐藏层节点 k :

$$\varphi_h = a'_i(1 - a'_i) \sum_h W_{kh} \varphi_h$$

2.3 更新权重值

for 每个权重 W_{ij} :

$$W_{ij} = W_{ij} + \Delta W_{ij}, W_{ij} = \eta Q_i \varphi_j$$

2.4 更新所有训练样本的权值

for 每个训练样本:

根据更新后的权值计算新的权值

检查输出误差的方差

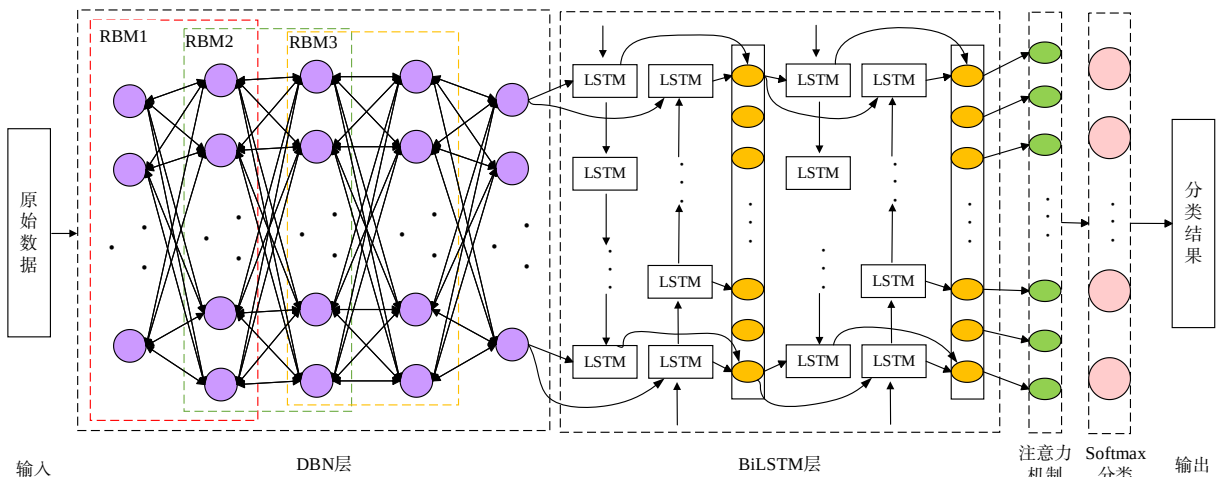


Fig. 4 Overall frame of the DBN-BiLSTM-Attention model

图 4 DBN-BiLSTM-Attention 模型整体框架

$$R = \sum_M (\sum_P (d_{MP} - Q_{MP}))^2$$

if $R \leq \varepsilon$:

break

步骤3: 输出结果,使用更新后的偏置 d 和权重 W ,输出最终的低维表征。

2.3 模型轮转训练

两个 BiLSTM 网络层的配置使得在每一轮训练过程中,其内部结构的核大小都会增加一倍,这种递增设计的初衷是为了逐步增强模型的表达能力。最初的 BiLSTM 网络由 64 个神经元构成,负责捕获数据中的基础特征和全局模式。在此基础上紧接一个拥有 128 个神经元的 BiLSTM 层,能够结合第一层的输出学习到更复杂的时间序列模式,有助于捕捉到隐藏的攻击特征,对初级特征进行更为深入的处理,捕获更加复杂的模式和细节。这种从粗略到细致的结构设计是为了有效处理长距离依赖关系,这在时间序列数据中尤为重要。随着网络层次的加深,模型能够捕捉到数据中更深层次的时间依赖性,有助于更好地理解特征之间的关联。这种层次化特征提取方法还能加快模型收敛速度,缩短训练周期。

2.4 注意力机制优化

采用 Attention 机制对 BiLSTM 层输出的每个时间步的隐藏状态进行加权求和,生成最终的带时间属性的上下文向量。如此一来,模型可以更有效地聚焦于在网络攻击发生时刻及其附近的关键特征变化,而不会忽略或平均化这些重要信息,增强了对关键时刻的感知能力。Attention 机制使模型在处理长时间序列数据时能够保留更为丰富且有针对性的上下文信息,从而提高检测和分类准确性。

2.5 样本分类

将提取完成的特征样本输入到 Softmax 分类器中,通过计算每个类别对应的概率分布来确定特征样本最有可能属于的类别。首先,Softmax 函数会将输入的特征向量映射到一个概率空间,使得所有类别的概率和为 1;其次,分类器根据这些概率分布对样本进行分类,选择概率最高的类别作为最终结果。

3 实验方法与结果分析

3.1 实验环境与参数设置

实验操作系统为 Window11,搭载 8 块 GPU,具体型号为 GV100GL。代码测试环境中,Python 版本为 3.9.6,Tensorflow 及 Keras 版本分别为 2.4.2 及 2.6.6。具体实验配置见表 1 所示。

3.2 数据集

采用 2014 年由密西西比州立大学发布的天然气管道领域的标准工业数据集。具体分布如表 2 所示。该数据集综合了常规网络流量数据与 7 类攻击数据,共有 97 019 条记录,其中正常网络流量数据有 61 156 条,各类攻击情境下的数据有 35 863 条,每个数据样本均包含 26 个特征

Table 1 Experimental environment configuration

表 1 实验环境配置

实验环境与参数	具体配置
实验操作系统	Windows11
Tensorflow 版本	2.4.2
Keras 版本	2.6.6
Python 版本	3.9.6
GPU 型号及其配置	GV100GL [Tesla V100S PCIe 32GB]
第一层 RBM 神经元个数	256
第二层 RBM 神经元个数	512
第三层 RBM 神经元个数	1 024
RBM 循环迭代次数	10 次/层
RBM 每轮迭代样本个数	32
RBM 初始学习率	0.1
第一层 BiLSTM	64 单元
第二层 BiLSTM	128

维度及 1 个类别标签^[11]。数据集被划分为 3 个子集,其中训练集占 70%,验证集占 10%,测试集占 20%。该数据集从基于 Modbus-TCP 通信协议的天然气管道 ICS 中收集,下载地址为 <https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets>。

Table 2 Specific distribution of dataset

表 2 数据集具体分布

标签编码	数据类型	样本数量	所占比例/%
0	Normal	61 156	63.04
1	NMRI	2 763	2.85
2	CMRI	15 466	15.94
3	MSCI	782	0.81
4	MPCI	7 637	7.87
5	MFCI	573	0.59
6	DOS	1 837	1.89
7	RECO	6 805	7.01

3.3 对照模型与评估指标

为验证本文算法的性能优势,将其与目前领先的算法模型进行比较,包括基于 ISSA-LightGBM 的工控入侵检测算法^[11]、基于改进 CGAN 算法的工控网络入侵检测算法 WCGAN-SVM^[12]、基于改进帝王蝶算法的工业入侵检测方法 MBO-LPO^[13]以及基于 XGBoost-DNN 的工业控制系统入侵检测算法^[14]。

采用以下指标评估模型性能:①误报率(False Positive Rate, FPR)^[15]。表示正常流量被误检测为攻击的比率,反映了模型的误警告水平;②准确率(Accuracy, ACC)^[16]。表示正确分类样本占总样本的比率,反映了模型的整体性能;③检出度(Detection Rate, DR)^[17]。表示攻击流量被正确检测的比率,反映了模型发现攻击的能力;④精确率(Precision Rate, PR)^[18]。表示检测为攻击的样本中实际为攻击的比率,反映了模型的结果可信度;⑤F1 分数(F1-score, F1)^[19]。表示综合考虑 PR 和 DR 的加权调和平均,反映了模型的稳定性。以上指标的计算公式为:

$$FPR = \frac{FP}{TN + FP} \quad (6)$$

$$ACC = \frac{TP + TN}{TP + FP + TN + FN} \tag{7}$$
$$DR = \frac{TP}{TP + FN} \tag{8}$$
$$PR = \frac{TP}{TP + FP} \tag{9}$$
$$F1 = \frac{TP}{TP + \frac{FN + FP}{2}} \tag{10}$$

式中:TP表示恶意网络行为被正确划分的数量;FP表示正常网络行为被错误划分的数量;TN表示正常网络行为被正确划分的数量;FN表示恶意网络行为被错误划分的数量^[20]。

3.4 实验结果与分析

使用包含 19 408 个样本的测试数据集对 DBN-BiLSTM-Attention 模型的性能进行测试,将模型预测结果与实际分类结果进行比较,得到如图 5 所示的混淆矩阵。其中,水平轴表示模型预测的流量类别,垂直轴表示真实的流量类别。结果显示,模型成功准确分类了 19 178 个数据点,整体准确率为 98.81%。

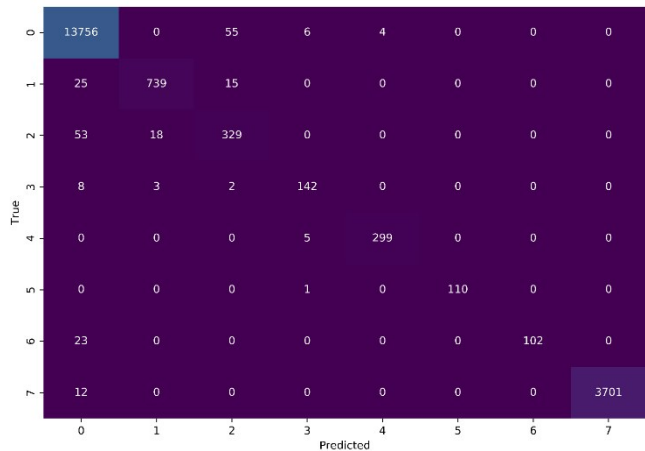


Fig. 5 Confusion matrix of DBN-BiLSTM-Attention model

图5 DBN-BiLSTM-Attention模型的混淆矩阵

表 3 为不同模型的实验结果比较。可以看出,本文模型的各项性能指标均处于领先水平。相比之下,ISSA-LightGBM 虽然准确率接近最优(ACC=0.987 8),但误报率较高(FPR=0.041 7),检出度和精确率也稍逊。WCGAN-SVM 与 MBO-LPO 性能相近,但误报率和 F1 分数上不及前两者。XGBoost-DNN 整体表现最弱,特别是准确率和 F1 分数明显落后。

图 6 为不同算法对各类样本的检测准确率雷达图。

Table 3 Experimental results comparison of different models

表 3 不同模型实验结果比较					
算法模型	ACC	FPR	F1	DR	PR
DBN-BiLSTM-Attention	0.988 1	0.038 2	0.986 5	0.971 3	0.987 3
ISSA-LightGBM	0.987 8	0.041 7	0.973 8	0.933 6	0.949 2
WCGAN-SVM	0.985 2	0.050 4	0.964 9	0.947 5	0.963 1
MBO-LPO	0.986 8	0.049 6	0.965 1	0.932 5	0.972 8
XGBoost-DNN	0.973 2	0.052 7	0.943 7	0.953 7	0.952 9

可以看出,DBN-BiLSTM-Attention 模型在识别不同样本类别时均表现优异,特别是在 MFCI、MPCI、MSCI 和 DOS 样本类型的识别中表现突出,表明其对这些攻击的检测能力较强。相比之下,ISSA-LightGBM 的整体表现也较为优秀,但对 MFCI 和 NMRI 的检测能力略逊色。WCGAN-SVM 和 MBO-LPO 的表现较弱,尤其是对 RECO 和 DOS 的检测能力与其他算法差距较大。XGBoost-DNN 则表现最为薄弱,对各种类别的检测能力均较为逊色。总体而言,DBN-BiLSTM-Attention 的表现最为优异,尤其是对复杂攻击模式的检测精度优于其他算法,在识别正常流量时也拥有最低的误报率,具有较高的准确性和可靠性。

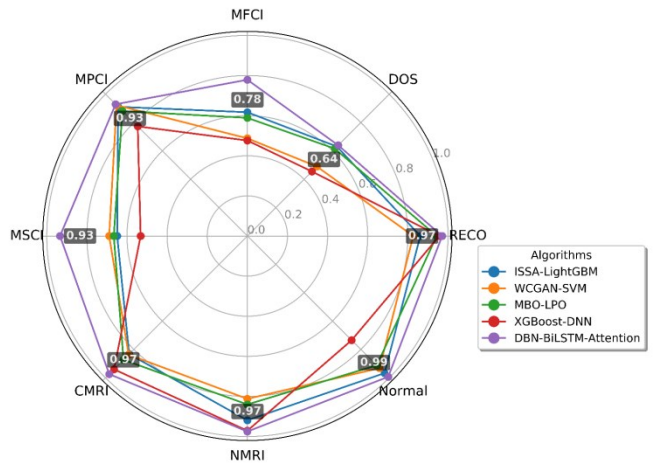


Fig. 6 Radar chart of detection accuracy for various algorithms on different types of samples

图6 不同算法对各类样本的检测准确率雷达图

图 7 为不同算法的 ROC 曲线。可以看出,DBN-BiLSTM-Attention 模型的 ROC 曲线表现十分突出,几乎贴近理想模型的左上角位置,AUC 值达到 0.973,显示出其在分类任务中的优越性。紧随其后的为 MBO-LPO (AUC=0.969)和 WCGAN-SVM (AUC=0.967),这两者也表现出色,但略逊色于 DBN-BiLSTM-Attention。ISSA-LightGBM 的 AUC 值为 0.956,性能较好,但不如前三者。XGBoost-DNN 的 AUC 值最低(0.932)。DBN-BiLSTM-Attention 模型的高 AUC 值表明其在不同阈值下均能平衡真活率率和假活率率,确保入侵检测系统既能准确识别真实威胁,又能将误报率控制在较低水平。

4 结语

针对工控网络面临的复杂攻击行为检测难题,本文提出基于 DBN-BiLSTM-Attention 的工控网络入侵检测算法。该算法结合了 DBN 强大的非线性特征提取能力、BiLSTM 对长距离时间依赖性的捕捉,以及注意力机制对关键信息的聚焦能力。具体来说,DBN 首先执行垂直方向的特征提取过程,其输出结果随后被用作 BiLSTM 的输入数据,以便更深入地挖掘并提取样本内的时间序列相关性特征。随

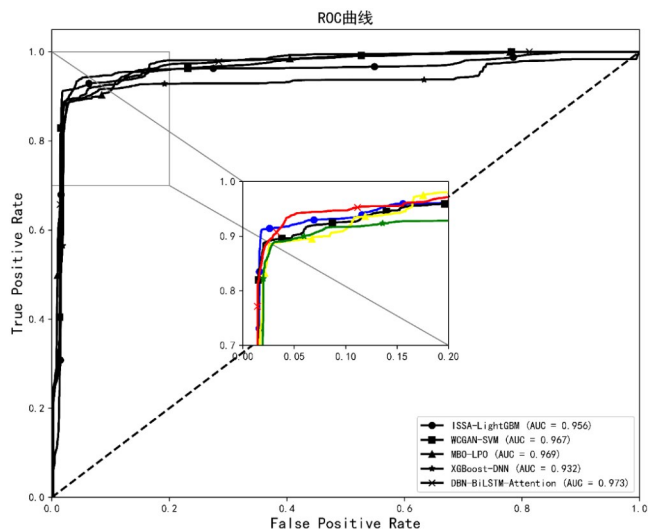


Fig. 7 ROC curves of different algorithms

图7 不同算法的ROC曲线

后,注意力机制的引入使模型能够更精准地聚焦于工控网络受攻击时的关键网络流量数据。经过多重比较实验证实,DBN-BiLSTM-Attention模型在工控网络入侵检测中表现出较高的可靠性和准确性。然而,DBN的多层结构要求逐层预训练,在每一层之间学习复杂的参数和特征。这些层级的复杂性使得模型在训练过程中需要大量计算资源,并且每一层的学习都可能受到先前层输出质量的影响,导致网络的训练变得更加复杂。同时,BiLSTM需要通过反向传播计算梯度和更新权重,尤其是在处理较长的时间序列时计算量和内存消耗会显著增加。此外,BiLSTM还包含多个隐状态单元和门控机制,进一步增加了模型的复杂性,未来可采用混合精度训练或知识蒸馏的方法来进行进一步降低模型的复杂程度。

参考文献:

- [1] GALLOWAY B, HANCKE G P. Introduction to industrial control networks [J]. IEEE Communications Surveys & Tutorials, 2012, 15(2): 860-880.
- [2] ZHANG S, LAI J, YAO Q. Traffic anomaly detection model of electric power industrial control based on DBN-LSTM [C]//2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys), 2021: 1902-1907.
- [3] LU K D, ZENG G Q, LUO X, et al. Evolutionary deep belief network for cyber-attack detection in industrial automation and control system [J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7618-7627.
- [4] WEI P, LI Y, ZHANG Z, et al. An optimization method for intrusion detection classification model based on deep belief network [J]. IEEE Access, 2019, 7: 87593-87605.
- [5] MONFARED M R, FAKHRAHMAD S M. Development of intrusion detection in industrial control systems based on deep learning [J]. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 2022, 46(3): 641-651.
- [6] HU X D, SHENG S L. Industrial Internet intrusion detection method integrating DBN and BiLSTM [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science), 2022, 34(1): 134-146.
胡向东, 盛顺利. 融合DBN和BiLSTM的工业互联网入侵检测方法[J]. 重庆邮电大学学报(自然科学版), 2022, 34(1): 134-146.
- [7] ZOU M, CONZEN S D. A new dynamic Bayesian network (DBN) approach for identifying gene regulatory networks from time course microarray data [J]. Bioinformatics, 2005, 21(1): 71-79.
- [8] NIU Z, ZHONG G, YU H. A review on the attention mechanism of deep learning [J]. Neurocomputing, 2021, 452: 48-62.
- [9] GUO M H, XU T X, LIU J J, et al. Attention mechanisms in computer vision: a survey [J]. Computational Visual Media, 2022, 8(3): 331-368.
- [10] ZHANG Z S, SHI J Z, GAO Q P. Bearing fault diagnosis model based on multi-scale CNN and BiLSTM-Attention [J]. Journal of Zhejiang Normal University (Natural Science Edition), 2024, 47(3): 281-289.
张昭胜, 史久正, 高清平. 基于多尺度卷积神经网络和双向长短期记忆—注意力机制的轴承故障诊断模型[J]. 浙江大学学报(自然科学版), 2024, 47(3): 281-289.
- [11] ZHAO Z D, WANG H Z. Research on industrial control system intrusion detection based on ISSA-LightGBM [J]. Journal of East China University of Science and Technology (Natural Science Edition), 2023, 49(5): 735-743.
赵志达, 王华忠. 基于ISSA-LightGBM的工控入侵检测研究[J]. 华东理工大学学报(自然科学版), 2023, 49(5): 735-743.
- [12] GU H, LAI Y, WANG Y, et al. DEIDS: a novel intrusion detection system for industrial control systems [J]. Neural Computing and Applications, 2022, 34: 9793-9811.
- [13] ALWESHAH M, KHALAILEH S A, GUPTA B B, et al. The monarch butterfly optimization algorithm for solving feature selection problems [J]. Neural Computing and Applications, 2022, 34: 11267-11281.
- [14] DEVAN P, KHARE N. An efficient XGBoost-DNN-based classification model for network intrusion detection system [J]. Neural Computing and Applications, 2020, 32: 12499-12514.
- [15] RICHARD D Y, BOULAY F, WANG J M, et al. International union of basic and clinical pharmacology. LXXIII. nomenclature for the formyl peptide receptor (FPR) family [J]. Pharmacological Reviews, 2009, 61(2): 119-161.
- [16] PENROSE D M, GLICK B R. Methods for isolating and characterizing ACC deaminase-containing plant growth-promoting rhizobacteria [J]. Physiologia Plantarum, 2003, 118(1): 10-15.
- [17] FADLULLAH Z M, NISHIYAMA H, KATO N, et al. Intrusion detection system (IDS) for combating attacks against cognitive radio networks [J]. IEEE Network, 2013, 27(3): 51-56.
- [18] OTOUM Y, NAYAK A. As-ids: anomaly and signature based ids for the Internet of Things [J]. Journal of Network and Systems Management, 2021, 29(3): 23.
- [19] WU Q R, HUANG S C. Intrusion detection algorithm combining convolutional neural network and three-branch decision [J]. Computer Engineering and Applications, 2022, 58(13): 119-127.
吴启睿, 黄树成. 结合卷积神经网络和三支决策的入侵检测算法[J]. 计算机工程与应用, 2022, 58(13): 119-127.
- [20] SIAMI-NAMINI S, TAVAKOLI N, NAMIN A S. The performance of LSTM and BiLSTM in forecasting time series [C]//2019 IEEE International Conference on Big Data, 2019: 3285-3292.

(责任编辑:尹晨茹)