面向工业入侵检测的数据增强和检测模型的研究

宗学军 王 震 何 戡 连 莲
(沈阳化工大学信息工程学院 辽宁 沈阳 110142)

摘 要 由于采集到的工业互联网流量数据存在正常流量和攻击流量的样本数目不平衡、样本特征复杂的问题,提出一种使用梯度惩罚的 Wasserstein 生成对抗网络(WGAN-GP)并结合卷积神经网络(CNN)与门控循环单元(GRU)的深度学习入侵检测方法。使用 WGAN-GP 数据增强并使用 CNN 与 GRU 混合模型进行深层特征提取解决上述问题。使用加拿大网络安全研究所公布的 CICIDS2017 数据集对模型进行实验,结果表明,对比不同机器学习算法,采用该方法的入侵检测结果准确率更高。利用密西西比州立大学天然气管道数据集对模型进行验证,结果证明了该模型在工业网络环境下的可行性和有效性。

关键词 生成对抗网络 数据增强算法 卷积神经网络 门控循环单元 工业入侵检测

中图分类号 TP393 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.09.051

DATA ENHANCEMENT AND DETECTION MODEL FOR INDUSTRIAL INTRUSION DETECTION

Zong Xuejun Wang Zhen He Kan Lian Lian
(*College of Information Engineer*, *Shenyang University of Chemical Technology*, *Shenyang 110142*, *Liaoning*, *China*)

Abstract Since the collected industrial Internet traffic data has the problems of imbalance in the number of samples of normal traffic and attack traffic, and complex sample features, a Wasserstein generative adversarial network using gradient penalty (WGAN-GP) is proposed and combined with a convolutional neural network (CNN) deep learning intrusion detection method with gated recurrent unit (GRU). We used WGAN-GP data enhancement and used the CNN and GRU hybrid model for deep feature extraction to solve the above problems. Experiments on the model using the CICIDS2017 data set published by the Canadian Institute of Cybersecurity, the results show that compared with different machine learning algorithms, the intrusion detection results using this method are more accurate. The model is validated with the Mississippi State University natural gas pipeline data set, and the results verify the feasibility and effectiveness of the model in an industrial network environment.

Keywords Generative adversarial networks Data enhancement algorithm Convolutional neural network Gated recurrent unit Industrial intrusion detection

0 引 言

工业控制系统(Industrial Control Systems,ICS)广泛应用于能源、制造、航天、军工的众多国民经济核心产业当中,关系着众多核心产业的命脉,是国民生产生活的重要保障[1]。

目前,工控系统的网络安全深受关注,随着工业 4.0、智能制造 2025、智慧工厂等有关概念的提出,工业控制系统逐步突破枷锁,接入到全球互联网中,每年全球暴露在公网的工控设备多达数十万,涉及众多核心生产制造行业,工业控制系统面临的安全形势越来越严峻[2]。

当今,全球已经进入大数据时代,网络流量数据存

收稿日期:2021 - 04 - 12。2020 年辽宁省重点研发计划项目(2020JH2/10100035);2019 年"辽宁省高等学校创新团队及创新人才支持计划"项目(LT2019010)。**宗学军**,教授,主研领域:工业过程控制,工业信息安全。**王震**,硕士生。**何戡**,副教授。**连莲**,讲师。

在数量多、维度高等特点,并且流量数据存在严重的不平衡性,在进行入侵检测之前,数据的平衡处理显得尤为重要[3]。目前,深度学习应用于网络入侵检测领域的研究备受关注,众多学者对此进行了大量研究。

文献[4]使用 SMOTE 算法对数据集中少数样本进行上采样来解决数据不平衡问题,但是文中使用的 KDD99 数据集相对落后,面对当今复杂网络环境不具有泛化性。文献[5]使用单类 SVM 算法进行 Modbus TCP/IP 协议下的异常入侵检测,但是当数据量增大时传统机器学习算法不足以提取足够特征解决多分类问题。文献[6]提出使用一维卷积神经网络作为分类模型的方法,但是不能很好地将少数类样本分类出来。

通过上述分析,为解决工控网络入侵流量中攻击数据不平衡、特征提取不充分,导致模型对多数样本过拟合和传统单一深度学习算法分类模型的分类精度低的问题,提出一种使用 WGAN-GP 作为数据增强算法,使用 CNN 和 GRU 模型作为入侵检测分类算法的方法来解决上述问题,提高网络入侵检测的效果。

1　基于 WGAN-GP 数据增强和 CNN-GRU 模型的入侵检测算法

为满足神经网络的训练要求,需要对数据进行预处理,使其能够满足深度学习的输入数据的格式要求;将预处理后的数据送入 WGAN-GP 数据增强模块进行处理,处理后的数据送入 CNN-GRU 混合网络进行特征提取,最后由 MLP(Multi-Layer Perceptron)分类器给出分类结果。本文整体模型框架如图 1 所示。

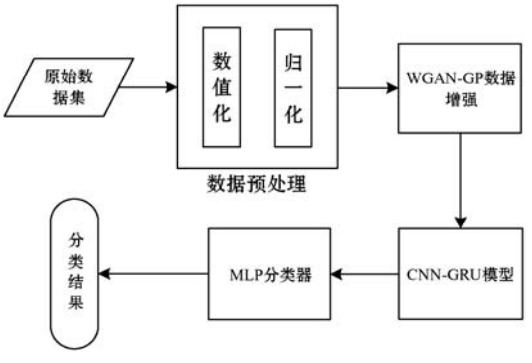

图 1　基于 WGAN-GP 数据增强和 CNN-GRU 模型的入侵检测算法的原理框架

1.1　数据分析及预处理

从网络中采集到的原始数据流量不能直接用于入侵检测的研究当中,需要对数据进行预处理。数据预处理总共分为两大部分:

(1) 数值化。对于原始网络流量样本 $X_{raw}=\{x_1,x_2,\cdots,x_n,y\}$ 每一个样本会包括 n 个连续型特征 x 以及一个数据标签 y,其中,标签 y 是字符型数据,采用 One-Hot 方法将字符型数据转化为数值型数据[7]。

(2) 归一化。将连续型特征 min-max 归一化,映射到[0,1]区间,x_i 表示连续型特征,x_{min}、x_{max} 表示该特征的最小值和最大值[8],x'_i 为归一化后的特征数值,如式(1)所示。

$$x'_i=\frac{x_i-x_{min}}{x_{min}x_{max}} \tag{1}$$

1.2　WGAN-GP 数据增强

由于现实中获取到的网络流量样本数据中,正常网络流量数据的数量远多于非正常的攻击流量数据,严重的数据不平衡问题对神经网络的训练产生很大的负面影响,使神经网络对多数类样本过拟合,对少数类样本欠拟合。本文提出一种基于 WGAN-GP 的数据增强算法,通过 WGAN-GP 生成一定数量的少数类样本,加入原始数据集中,使样本分布更加合理,有效提高入侵检测模型对少数类样本的检出能力。本文的 WGAN-GP 结构如图 2 所示。

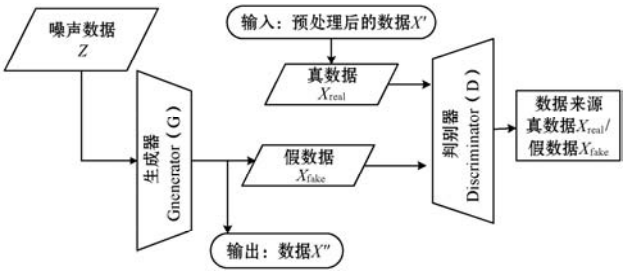

图 2　WGAN-GP 结构

WGAN-GP 的基本网络结构由数据输入层、噪声输入层、生成器网络、判别器网络和输出层构成[9-10]。本文设计的 WGAN-GP 中,生成器的网络和判别器的网络都由 MLP 构成,MLP 包含输入层、隐藏层和输出层,MLP 结构可以快捷地拟合数据并且收敛速度快,可以很好地实现生成器网络和判别器网络的功能。

将随机初始化分布生成的噪声数据 $\boldsymbol{Z}$ 输入到生成器 G 的网络中,生成假数据 $\boldsymbol{X}_{fake}$。在生成器的网络中,输入噪声数据 $\boldsymbol{Z}$ 时:

$$\boldsymbol{h}_1=f_1([\boldsymbol{z}]\cdot\boldsymbol{w}_1+\boldsymbol{b}_1) \tag{2}$$

$$\boldsymbol{h}_2=f_1(\boldsymbol{h}_1\cdot\boldsymbol{w}_2+\boldsymbol{b}_2) \tag{3}$$

$$\boldsymbol{h}_3=f_1(\boldsymbol{h}_2\cdot\boldsymbol{w}_3+\boldsymbol{b}_3) \tag{4}$$

$$\boldsymbol{x}_{fake}=f_1(\boldsymbol{h}_3\cdot\boldsymbol{w}_4+\boldsymbol{b}_4) \tag{5}$$

式中:f_1 是非线性激活函数 ReLU;$\boldsymbol{w}_1$、$\boldsymbol{w}_2$、$\boldsymbol{w}_3$、$\boldsymbol{w}_4$ 为权重矩阵;$\boldsymbol{b}_1$、$\boldsymbol{b}_2$、$\boldsymbol{b}_3$、$\boldsymbol{b}_4$ 为偏置向量。

将真数据 $\boldsymbol{X}_{real}$ 与生成器生成的假数据 $\boldsymbol{X}_{fake}$ 一同输入到判别器 D,判别数据的来源是真还是假(real or fake)。在判别器网络中,输入真数据 $\boldsymbol{X}_{real}$ 时:

$$\boldsymbol{h}_1=f_1(\boldsymbol{X}_{real}\cdot\boldsymbol{w}_1+\boldsymbol{b}_1) \tag{6}$$

$$\boldsymbol{h}_2 = f_1(\boldsymbol{h}_1 \cdot \boldsymbol{w}_2 + \boldsymbol{b}_2) \tag{7}$$

$$\boldsymbol{y}_{\text{real}} = \boldsymbol{h}_1 \cdot \boldsymbol{w}_3 + \boldsymbol{b}_3 \tag{8}$$

输入假数据 $\boldsymbol{X}_{\text{fake}}$ 时：

$$\boldsymbol{h}_1 = f_1(\boldsymbol{X}_{\text{fake}} \cdot \boldsymbol{w}_1 + \boldsymbol{b}_1) \tag{9}$$

$$\boldsymbol{h}_2 = f_1(\boldsymbol{h}_1 \cdot \boldsymbol{w}_2 + \boldsymbol{b}_2) \tag{10}$$

$$\boldsymbol{y}_{\text{fake}} = \boldsymbol{h}_1 \cdot \boldsymbol{w}_3 + \boldsymbol{b}_3 \tag{11}$$

式中：f_1 是非线性激活函数 ReLU；$\boldsymbol{w}_1$、$\boldsymbol{w}_2$、$\boldsymbol{w}_3$ 为权重矩阵；$\boldsymbol{b}_1$、$\boldsymbol{b}_2$、$\boldsymbol{b}_3$ 为偏执向量。

损失函数包含真假数据来源（S）判别损失，式(12)和式(13)，真实分布和生成分布之间的插值数据 $\hat{x}$，式(14)和梯度惩罚项式(15)。

$$L_1 = E[D(S_{\text{fake}})] \tag{12}$$

$$L_2 = E[D(S_{\text{real}})] \tag{13}$$

$$\hat{x} = \varepsilon x_{\text{real}} + (1-\varepsilon)x_{\text{fake}} \tag{14}$$

$$L_3 = \lambda E[(\|\nabla_{\hat{x}} D(\hat{x})\|_2 - 1)^2] \tag{15}$$

式中：ε 是在[0,1]间的随机采样数；λ 是梯度惩罚项的权重因子，用于控制梯度惩罚项的强度。

生成器 G 的损失函数 $L_G = -L_1$，判别器 D 的损失函数 $L_D = L_1 - L_2 + L_3$。

生成器 G 通过对 L_G 的优化不断提高生成假数据的能力，使生成数据的分布不断靠近真实数据的分布。判别器 D 通过对 L_D 的优化不断提高判别真假数据的能力。G 和 D 通过互相博弈对抗，不断调节各自的网络参数，最终生成器和判别器达到一种稳定平衡状态，生成器输出数据 X''。

1.3 CNN-GRU 混合网络模型

CNN 网络和 GRU 网络都是深度学习中常见的网络。与普通的机器学习相比较能够实现数据的逐层递进转换，CNN 网络能够有效地提取数据的深层特征信息，GRU 网络能够有效提取数据的时序信息[11]。

1.3.1 CNN 网络

CNN 是一种主要应用在与图像处理有关的深度学习领域，通过卷积运算，可有效地提取出图片每个像素的特征信息。通常 CNN 的基本结构包括输入层、卷积层、池化层、全连接层和输出层构成。CNN 网络基本结构如图 3 所示。

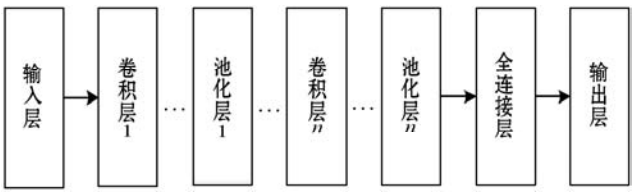

图 3 CNN 网络基本结构

对于第 m 卷积层，其输出为 y_m，那么第 k 个卷积核的输出为 y_k^m，则有：

$$y_k^m = \delta\left(\sum_{y_i^{m-1} \in M_k} y_i^{m-1} \otimes W_{ik}^m + b_k^m\right) \tag{16}$$

式中：δ 为激活函数；M_k 表示上一层特征集合；W_{ik}^m 为卷积核；$\otimes$ 为卷积操作；b_k^m 为偏置量。

池化层通过一定的池化规则对卷积层的输出执行池化运算，保留数据的主要特征，同时可以减少参数数目和计算量，防止过拟合。池化过程可以用式(17)表示：

$$P = pool(y_k^m) \tag{17}$$

式中：P 表示池化层的输出特征图；$pool$ 表示池化规则，例如平均池化、最大池化等。

CNN 的特点是能够提取数据中的隐藏特征，并将其逐层结合，生成抽象的高级特性。然而 CNN 不具备记忆功能，缺乏对时序数据时间相关性的考虑[12-13]。

1.3.2 GRU 网络

Chung 等[14]把 LSTM 网络中的输入门和遗忘门合并为更新门，通过对 LSTM 的改造，构建出了 GRU 网络，GRU 网络作为 LSTM 网络的变体，解决了 LSTM 网络计算复杂、训练难度大等问题。GRU 网络的结构如图 4 所示。

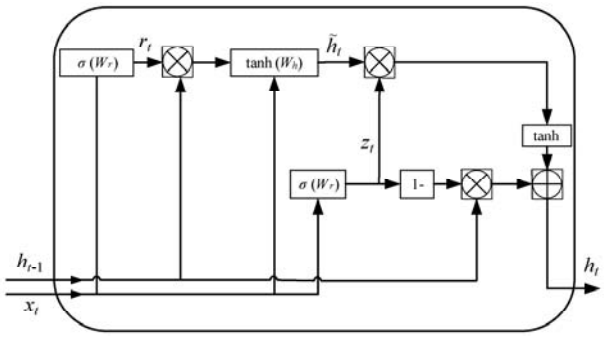

图 4 GRU 网络模型

GRU 神经网络中由两个选通单元，分别为“复位门”r_t 和“更新门”z_t。r_t 用于控制前一时刻的状态 h_{t-1} 对候选状态 $\hat{h}_t$ 的影响程度，z_t 用于决定 h_{t-1} 中有多少信息可以传递到当前状态 h_t 中。GRU 神经网络的更新方式如下：

$$\boldsymbol{r}_t = \sigma(\boldsymbol{x}_t \boldsymbol{W}_{xr} + \boldsymbol{h}_{t-1} \boldsymbol{W}_{hr} + \boldsymbol{b}_r) \tag{18}$$

$$\boldsymbol{z}_t = \sigma(\boldsymbol{x}_t \boldsymbol{W}_{xz} + \boldsymbol{h}_{t-1} \boldsymbol{W}_{hr} + \boldsymbol{b}_z) \tag{19}$$

$$\tilde{\boldsymbol{h}}_t = \tanh(\boldsymbol{x}_t \boldsymbol{W}_{xh} + \boldsymbol{r}_t \odot \boldsymbol{h}_{t-1} \boldsymbol{W}_{hh} + \boldsymbol{b}_h) \tag{20}$$

$$\boldsymbol{h}_t = \boldsymbol{z}_t \odot \boldsymbol{h}_{t-1} + (\boldsymbol{1} - \boldsymbol{z}_t) \odot \tilde{\boldsymbol{h}}_t \tag{21}$$

式中：$\boldsymbol{z}_t$ 表示更新门的状态，决定信息的取舍；$\boldsymbol{r}_t$ 表示重置门的状态，决定忘记信息的程度；σ 是 Sigmoid 函数；tanh 是双曲正切函数；$\boldsymbol{x}_t$ 是 t 时刻的输入；$\boldsymbol{h}_t$ 是 t 时刻的输出；$\boldsymbol{W}_{xr}$、$\boldsymbol{W}_{xz}$、$\boldsymbol{W}_{xh}$ 是输入-状态的权重矩阵；$\boldsymbol{W}_{hr}$、$\boldsymbol{W}_{hz}$ 和 $\boldsymbol{W}_{hh}$ 是状态-状态的权重矩阵；$\boldsymbol{b}_r$、$\boldsymbol{b}_z$、$\boldsymbol{b}_h$ 是偏置量；$\odot$ 是元素乘法。

1.3.3　CNN-GRU 混合网络模型的构成

CNN 通过卷积操作,可以提取出样本数据的高层次特征,降低数据的维度,为提高预测精度奠定基础,但 CNN 缺乏对时序数据相关性的考虑。工业控制系统网络中的流量具有明显的时序特征,GRU 通过门函数控制对历史数据的记忆和遗忘,可以有效地提取出网络流量数据中的时间序列特征,但是面临过大的网络数据流量时,随着计算量的增加,GRU 对远期数据的联系也会逐渐降低,从而导致 GRU 的准确率也随之降低。因此,本文提出 CNN-GRU 混合网络模型,将处理好的数据 X 送入 CNN-GRU 混合网络模型进行高级特征的提取与处理,最后得到输出 P,通过多种网络结构的组合,提取出不同的关键特征信息,可以有效地提高网络入侵检测的准确率。CNN-GRU 混合网络模型如图 5 所示。

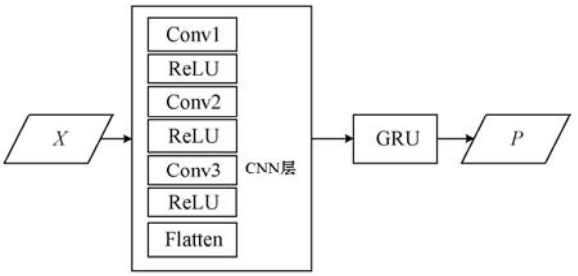

图 5　CNN-GRU 混合网络模型

由于池化层的池化操作是一种有损的降维方法,在计算机算力允许的情况下,为了尽量不丢弃输入数据并尽可能符合网络入侵检测高精度场景的要求,故在本文 CNN 算法中舍弃传统 CNN 结构中的池化层,并且采用补 0 填充的方式使得输出与输入的特征图保持大小一致。

在 CNN-GRU 网络中,CNN 层包含三层卷积,第一层卷积层包含 120 个 3×3 尺寸的卷积核,第二层卷积层包含 60 个 3×3 尺寸的卷积核,第三层卷积层包含 30 个 3×3 尺寸的卷积核,三层卷积层中激活函数均为"ReLU",填充方式均为"SAME"。CNN-GRU 各单元参数设置如表 1 所示。

表 1　CNN-GRU 参数设置

参数	卷积层 1	卷积层 2	卷积层 3	GRU
卷积核数量	120	60	30	—
卷积核尺寸	3×3	3×3	3×3	—
卷积运算步长	1	1	1	—
填充方法	SAME	SAME	SAME	—
激活函数	ReLU	ReLU	ReLU	—
单元数量	—	—	—	64

1.4　MLP 分类器

MLP 分类器是一种全连接神经网络,主要由两部分组成,分别是输入层和输出层。通过 CNN-GRU 混合网络对样本数据进行高级的特征提取,只需要 MLP 这一简单的分类器就可以实现入侵检测的分类任务。首先,处理好的数据分别通过两个全连接层和一个 Dropout 层,最后通过 Softmax 函数输出。CNN-GRU 混合网络的输出结果为 P,MLP 分计算如下:

$$y = f_{\text{dence}}(W_{\text{dence}} \cdot P + b_{\text{dence}}) \tag{22}$$

$$P(y_i) = \frac{e^{y_i}}{\sum_j e^{y_j}} \tag{23}$$

式中:$\boldsymbol{W}_{\text{dence}}$ 为全连接层权重矩阵;$\boldsymbol{b}_{\text{dence}}$ 为偏置向量;f_{dence} 为非线性激活函数 ReLU;y_i 为全连接输出特征的第 i 维;$P(y_i)$ 为预测类别 i 的概率,$0 \leqslant P(y_i) \leqslant 1$。

2　实验与结果

2.1　模型评价标准

入侵检测模型评价指标主要有模型的准确率(Accuracy,ACC)、各个类别的精确率(Precisione,P)、召回率((Recall,R))和 F1 值(F1-measure),计算公式如下:

$$A_{\text{CC}} = \frac{T_{\text{P}} + T_{\text{N}}}{T_{\text{P}} + T_{\text{N}} + F_{\text{P}} + F_{\text{N}}} \tag{24}$$

$$R = \frac{T_{\text{P}}}{T_{\text{P}} + F_{\text{N}}} \tag{25}$$

$$P = \frac{T_{\text{P}}}{T_{\text{P}} + F_{\text{P}}} \tag{26}$$

$$F = \frac{2 \times P \times R}{P + R} \tag{27}$$

$$F_{\text{PR}} = \frac{F_{\text{N}}}{T_{\text{P}} + F_{\text{N}}} \tag{28}$$

$$F_{\text{NR}} = \frac{F_{\text{P}}}{T_{\text{P}} + F_{\text{P}}} \tag{29}$$

式中:T_{P} 表示正确识别的攻击类别数目;F_{N} 表示漏报即未正确识别攻击类别的数目;F_{P} 表示误报即错误识别正常类别的数目;T_{N} 表示正确识别的正常类别数目[15]。

2.2　数据分析及预处理

使用加拿大网络安全研究所公布的 CICIDS2017 数据集进行入侵检测实验,数据集包含 1 种正常数据和 14 种网络攻击数据,每条数据共有 84 个特征属性和 1 个标签。攻击类型包括暴力破解、端口扫描、各类 DoS/DDoS、Web 攻击、渗透等。数据集中的样本分布极度不平衡,最多类别样本可达百万,最少类别样本仅

为 11 个。对 84 个连续型特征进行 min-max 归一化，对数据集样本标签进行 One-Hot 编码，预处理后数据集描述如表 2 所示。

表 2 CICIDS2017 数据集描述

攻击类型	标签编码	数量
BENIGN	0	1 739 643
Bot	1	1 956
DDos	2	128 006
DoS GoledenEye	3	10 288
DoS Hulk	4	229 965
DoS Slowhttptest	5	5 499
DoS slowloris	6	5 796
FTP-Patator	7	7 931
Heartbleed	8	11
Infiltration	9	36
PortScan	10	158 804
SSH-Patator	11	5 897
Web Attack Brute Force	12	1 507
Web Attack Sql Injection	13	21
Web Attack XSS	14	652

2.3 WGAN-GP 数据增强实现

根据表 2 可以看出，该原始数据集存在严重不平衡问题，攻击样本 Heartbleed、Infiltration 等数量远远少于其他样本数量，在这种情况下用于训练分类器模型，模型很大程度会偏向多数类，忽略少数类，导致模型的泛化能力不强。因此本文使用 WGAN-GP 数据增强算法对少数类样本进行过采样，将生成的样本加入原始数据集，生成平衡数据集。

WGAN-GP 参数设置，随机初始化噪声维度 Z-DIM = 128，一次迭代输入模型样本适量 BATCH-SIZE = 4，全部样本训练次数 EPOCHS = 2 400，初始化学习率 LR = 0.005，生成器和判别器的优化函数均使用 Adam，每训练五次鉴别器后训练一次判别器。绘制生成器 G 和判别器 D 的损失函数曲线如图 6 所示。

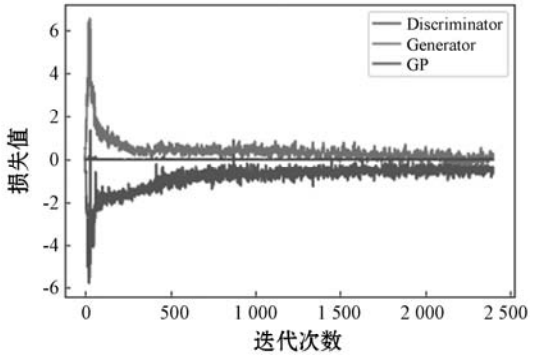

图 6 G 和 D 损失函数

根据图 6 可以看出，生成器 G 和判别器 D 通过互相博弈，达到了一种稳定平衡状态，每种少数类样本分别生成 5 000 条新样本加入数据集，生成的样本数量如表 3 所示。使用 WGAN-GP 生成数据前后的少数类样本数据总量对比如表 4 所示。

表 3 生成样本数量

标签	1	8	9	12	13	14
数目	5 000	5 000	5 000	5 000	5 000	5 000

表 4 WGAN-GP 前后对比

类别	1	8	9	12	13	14
Wgan-gp 前	1 956	11	36	5 000	21	625
Wgan-gp 后	6 956	5011	5 036	6 507	5 021	5 625

在保证数据集样本比例情况下，将 WGAN 前后的数据集划分 8 份作为训练集，2 份作为测试集。

2.4 入侵检测模型实现

2.4.1 WGAN-GP 前后实验结果对比

使用 CNN-GRU 混合网络对 WGAN-GP 前后的数据集进行检测，实验结果对比如表 5 所示。

表 5 实验结果对比(%)

项目	训练集 ACC	测试集 ACC	误报率 FPR	漏报率 FNR
WGAN-GP 前	98.95	98.63	1.07	0.611
WGAN-GP 后	99.61	99.59	0.579	0.599

可以看出，WGAN-GP 后，训练集 ACC 提高 0.66 百分点，测试集 ACC 提高 0.96 百分点；误报率 FPR 降低 0.491 百分点，漏报率 FNR 降低 0.033 百分点，可见 WGAN-GP 对于提高模型的检测精度、降低误报率和漏报率具有明显效果。WGAN-GP 数据增强前后各种样本 F1 值对比如图 7 所示。

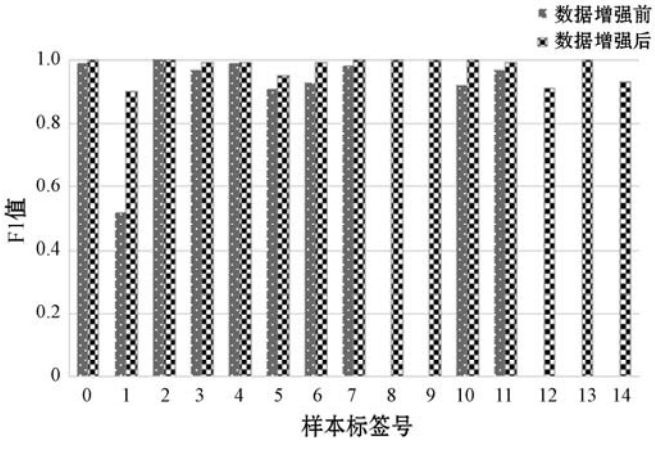

图 7 样本 WGAN-GP 前后 CNN-GRU 模型下各样本 F1 分数比较

可以看出,标签 1、8、9、12、13、14 在 WGAN-GP 后,F1 值均有显著提高,可见 WGAN-GP 对不平衡样本具有数据增强效果。

2.4.2　不同的机器学习入侵检测模型

在入侵检测模型中,比较常用的机器学习算法包括决策树(Decision Tree,DT)、随机森林(Random Forest,RF)、朴素贝叶斯(Naive Bayes,NB)、支持向量机(Support Vector Machine,SVM)、K 最近邻(K-Nearest Neighbor,KNN)。使用这些常用算法建立入侵检测模型,对 CICIDS2017 数据集进行检测,不同机器学习模型检测结果对比如表 6 所示。

表 6　检测结果对比(%)

算法	训练集 ACC	测试集 ACC
DT	92.85	92.92
RF	94.46	94.60
NB	92.84	92.78
SVM	95.38	95.12
KNN	95.98	95.69
CNN-GRU	98.95	98.63
WGAN-GP + CNN-GRU	99.61	99.59

可以看出,传统的机器学习模型在检测结果上面相对本文的深度神经网络模型还略有不足,KNN 表现最好,训练集 ACC 达到 95.98%,测试集 ACC 达到 95.69%。在未进行 WGAN-GP 数据增强的情况下,使用 CNN-GRU 混合网络对数据集进行检测,检测结果相对于表现最好的机器学习 KNN 模型,训练集 ACC 提高 2.97 百分点,测试集 ACC 提高 2.94 百分点,证明 CNN-GRU 混合网络相较于普通机器学习能够显著提高入侵检测模型的检测精度。在 WGAN-GP 数据增强后,使用 CNN-GRU 混合网络训练集 ACC 达到 99.61%,测试集 ACC 达到 99.59%,相较于未进行数据增强,仅使用 CNN-GRU 混合网络检测,训练集 ACC 提高 0.88 百分点,测试集 ACC 提高 0.77 百分点,这足以证明,WGAN-GP 数据增强对于处理不平衡数据、提高入侵检测模型性能具有很好的效果。

2.5　入侵检测模型在工业控制网络环境下的验证

验证实验采用密西西比州立大学天然气管道控制系统数据集进行实验,数据集包含 1 种正常数据和 7 种攻击数据,数据集描述如表 7 所示。

表 7　天然气管道控制系统数据集描述

标签名称	标签编号	数量
Normal	0	61 156
NMRI	1	2 763
CMRI	2	15 466
MSCI	3	782
MPCI	4	7 637
MFCI	5	573
DOS	6	1 837
Recon	7	6 805

数据集包含 1 种正常数据和 7 个攻击数据,相比较 CICIDS2017 数据集,该数据集采集自现实工业控制网络环境,更具有针对工业控制网络进行入侵检测的代表性,并且数据集同样存在严重的数据不平衡问题。

按照本文的入侵检测模型实现步骤,首先对天然气管道控制系统数据集进行分析和预处理,其次采用 WGAN-GP 进行数据增强,然后使用 CNN-GRU 混合网络进行特征提取,最后通过 MLP 网络输出入侵检测结果。

WGAN-GP 数据增强前后数据集对比如表 8 所示。

表 8　WGAN-GP 前后数据集对比

标签	WGAN-GP 前	WGAN-GP 后
Normal	61 156	61 156
NMRI	2 763	2 763
CMRI	15 466	15 466
MSCI	782	1 282
MPCI	7 637	7 637
MFCI	573	1 073
DOS	1 837	1 837
Recon	6 805	6 805

使用 CNN-GRU 混合网络在 WGAN-GP 前后实验结果对比如表 9 所示。

表 9　WGAN-GP 前后结果对比(%)

名称	训练集 ACC	测试集 ACC	误报率 FPR	漏报率 FNR
WGAN-GP 前	97.53	97.38	1.12	0.658
WGAN-GP 后	99.12	99.28	0.601	0.625

可以看出使用 CNN-GRU 混合网络模型在 WGAN-GP 数据增强后,相比较于未使用 WGAN-GP 数据增强,训练集 ACC 提高 1.59 百分点,测试集 ACC 提高 1.9 百分点,误报率 FPR 降低 0.519 百分点,漏报率降

低 0.033 百分点。不难看出 WGAN-GP 数据增强能够明显提高模型的检测能力,证明了该模型在工业网络环境下进行入侵检测的可行性和有效性。

3 结 语

针对日趋严重的工业控制系统网络安全问题,本文提出以 WGAN-GP 作为数据增强手段、CNN-GRU 混合网络作为工业控制网络的入侵检测模型。使用加拿大网络安全研究所 CICIDS2017 数据集进行实验,结果表明,本文模型相对于传统机器学习模型,对网络入侵检测的多种攻击类别的精确率和 F1 值都有提高,而且模型最终准确率更高(99.61%)、误报率更低(0.579%)、漏报率更低(0.599%),符合网络入侵检测的要求。使用美国密西西比州立大学天然气管道控制系统数据集进行验证,多种实验结果表明,在工业控制网络环境下,模型依然能够有着较好的检测能力,证明了该模型在工业网络环境下进行入侵检测的可行性、优越性和有效性。

本文提出的 WGAN-GP 数据增强算法和 CNN-GRU 混合网络入侵检测模型,解决了网络入侵检测数据集存在的样本不平衡、特征提取不充分的问题,较传统机器学习而言,使用深度学习模型大大提高了入侵检测效果,为工业控制系统网络入侵检测技术的发展提供了新的研究思路和技术支持。

参 考 文 献

[1] 黄杰. 工控网络安全浅析[J]. 网络安全技术与应用,2021(2):104 - 105.

[2] 石乐义,朱红强,刘祎豪,等. 基于相关信息熵和 CNN-BiLSTM 的工业控制系统入侵检测[J]. 计算机研究与发展,2019,56(11):2330 - 2338.

[3] 安磊,韩忠华,林硕,等. 面向网络入侵检测的 GAN-SDAE-RF 模型研究[J]. 计算机工程与应用,2021,57(21):155 - 164.

[4] 张阳,张涛,陈锦,等. 基于 SMOTE 和机器学习的网络入侵检测[J]. 北京理工大学学报,2019,39(12):1258 - 1262.

[5] Dong H, Peng D. Research on abnormal detection of Modbus TCP/IP protocol based on one-class SVM[C]//2018 33rd Youth Academic Annual Conference of Chinese Association of Automation (YAC),2018:398 - 403.

[6] 时东阁,章晓庆,毛保磊,等. 一种基于卷积神经网络的入侵检测方法[J]. 计算机应用与软件,2020,37(10):323 - 327,333.

[7] 郑伟发. 基于 CNN-LSTM 混合模型的入侵检测算法研究[J]. 网络安全技术与应用,2020(5):61 - 64.

[8] 赵智阳,夏筱筠. 基于卷积神经网络的电网工控系统入侵检测算法[J]. 计算机系统应用,2020,29(8):179 - 184.

[9] Gulrajani I, Ahmed F, Arjovsky M, et al. Improved training of Wasserstein GANs[EB]. arXiv:1704.00028, 2017.

[10] 闵佳媛. 基于 WGAN-GP 的人脸素描-照片转化研究[D]. 长春:吉林大学,2020.

[11] 党建武,从筱卿. 基于 CNN 和 GRU 的混合股指预测模型研究[J]. 计算机工程与应用,2021,57(16):167 - 174.

[12] 宋宇,李治霖,程超. 基于 CNN-BILSTM 的工业控制系统 ARP 攻击入侵检测方法[J]. 计算机应用研究,2020,37(S2):242 - 244.

[13] 於帮兵,王华忠,颜秉勇. 基于长短时记忆网络的工业控制系统入侵检测[J]. 信息与控制,2018,47(1):54 - 59.

[14] Chung J, Gulcehre C, Cho K H, et al. Empirical evaluation of gated recurrent neural networks on sequence modeling[EB]. arXiv:1412.3555,2014.

[15] 李振. 生成式对抗网络在入侵检测中的研究与应用[D]. 南昌:南昌大学,2020.

(上接第 318 页)

[6] Zhang L Y, Liu L, Zhang L. Research on position correction method for AUV large depth navigation based on ranging positioning[J]. Computer Communications,2020,150:747 - 756.

[7] Zhang X, He B, Li G L. NavNet: AUV navigation through deep sequential learning[J]. IEEE Access,2020,8:59845 - 59861.

[8] Zhang X, Fei X Y, Zhu Y M, et al. Novel improved UKF algorithm and its application in AUV navigation system[C]// IEEE Kobe Techno-Oceans,2018:1 - 4.

[9] Xu B, Li S X, Razzaqi A, et al. Cooperative localization in harsh underwater environment based on the MC-ANFIS[J]. IEEE Access,2019,7:55407 - 55421.

[10] Bin J, Xin M, Cheng Y. High-degree cubature Kalman filter[J]. Automatic,2013,49(2):510 - 518.

[11] Mu X K, Guo J, Song Y, et al. Application of modified EKF algorithm in AUV navigation system[C]//OCEANS,2017:1 - 4.

[12] Liu H M, He B, Feng C, et al. Navigation algorithm based on PSO-BP UKF of autonomous underwater vehicle[C]// IEEE Underwater Technology,2019:1 - 4.

[13] 王婧琦. 浮标型长基线定位算法与软件实现[D]. 哈尔滨:哈尔滨工程大学,2019.

[14] 李翔宇. 长基线高精度定位方法研究与实现[D]. 哈尔滨:哈尔滨工程大学,2017.

[15] 陈菘,卢敏. 几种滤波算法的分析与比较[J]. 电脑知识与技术,2020,16(32):23 - 25.