第 36 卷 第 5 期
2021 年 10 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol. 36 No. 5
Oct. 2021

DOI:10.13364/j.issn.1672-6510.20200206

面向不完备信息网络的集成神经网络入侵检测方法

张翼英，阮元龙，尚 静
（天津科技大学人工智能学院，天津 300457）

摘 要：常见的基于人工智能的入侵检测算法要求完备的训练数据，否则易因数据类别不均衡、特征不完备等原因导致无法有效识别入侵行为. 针对网络信息的不完备，本文提出一种面向不完备信息的集成神经网络入侵检测方法（intrusion detection with incomplete information based on ensemble neural network，IDII-ENN），解决不完备信息条件下检测准确率低、训练时间长的难题. 首先，针对不完备的数据进行优化处理，提出基于 bootstrap 的采样方法，在保证其特征稳定的情况下实现数据的完备化；然后，构建基于前馈神经网络的入侵检测分类模型，实现轻量级的入侵检测分类；最后，设计基于投票策略的集成学习融合方法，实现对入侵行为的精准识别. 实验结果表明：IDII-ENN 对数据特征的敏感度较低，准确率相较完全基于前馈神经网络的检测模型（simplified feed-forward intrusion detection，SFID）提高了 1%；同时训练效率相较基于稀疏自编码器（sprarse auto-encoder，SAE）的特征提取方法提高了近 1 倍，满足入侵检测实时性的需求.

关键词：不完备信息；集成学习；神经网络；网络入侵检测
中图分类号：TP393.08 **文献标志码**：A **文章编号**：1672-6510（2021）05-0068-07

Intrusion Detection with Incomplete Information Based on Ensemble Neural Network

ZHANG Yiying，RUAN Yuanlong，SHANG Jing
（College of Artificial Intelligence，Tianjin University of Science & Technology，Tianjin 300457，China）

Abstract：The common intrusion detection algorithm based on artificial intelligence requires complete training data，otherwise it is easy to be unable to effectively identify intrusion behavior due to unbalanced data categories，incomplete features and other reasons. Aiming at the incompleteness of network information，in this article we propose intrusion detection with incomplete information based on ensemble neural network（IDII-ENN），which solves the problems of low detection accuracy and long training time under the condition of incomplete information. Firstly，aiming at the incomplete data，we propose a bootstrap based sampling method to complete the data under the condition of feature stability. Secondly，we construct an intrusion detection classification model based on feed-forward neural network to achieve lightweight intrusion detection classification. Finally，we design an ensemble learning fusion method based on voting strategies to achieve accurate identification of intrusions. The experimental results show that the sensitivity of IDII-ENN to data features was low，and the accuracy was 1% higher than that of simplified feed-forward intrusion detection（SFID）. At the same time，the training efficiency of the model was nearly doubled compared with sparse auto-encoder（SAE），which meets the demand of real-time intrusion detection.

Key words：incomplete information；ensemble learning；neural network；network intrusion detection

近年来，随着网络技术的进步，网络安全问题日益严峻，各种各样的入侵方式层出不穷. 根据中国互联网应急中心 2020 年 2 月发布的《网络信息安全与动态周报》[1]的数据显示，境内感染网络病毒的设备

收稿日期：2020-12-07；**修回日期**：2021-04-22
基金项目：国家自然科学基金资助项目（61807024）
作者简介：张翼英（1973—），男，辽宁人，教授，yiyingzhang@tust.edu.cn

数量达到 132 万个[2]. 网络入侵威胁着用户的信息安全，因此入侵检测[3]的重要性日益凸显，建立一套有效的检测机制尤为必要.

随着人工智能的兴起，有学者[3-4]将机器学习引入入侵检测系统. 但是，基于深度学习的入侵检测方法存在 3 个问题：第一，深度学习结构复杂，需要花费大量时间训练参数，检测实时性不好[5]；第二，训练需要大量完备的数据，以增强模型的训练效果[6]；第三，神经网络复杂的结构决定了其强大的拟合能力，但同时容易导致过拟合.

目前，国内外基于深度学习方法的入侵检测研究均取得一定成果. 针对训练效率，Khan 等[7]结合主成分分析方法（principal component analysis，PCA）和贝叶斯网络，基于 PCA 提取数据主要特征，基于贝叶斯网络进行入侵分类，但检测时效性不好. Gurung 等[8]采用基于深度置信网络（deep belief network，DBN）与支持向量机（support vector machine，SVM）相结合的模型，模型的检测准确率高，但在训练时长上存在不足. Lopez-Martin 等[9]采用基于稀疏自编码器（sprarse auto-encoder，SAE）的特征提取方法，并用自学习（self-taught learning，STL）的方式对数据进行有监督的训练，检测准确率在 90% 以上，但训练时间过长. 冯文英等[10]设计了一种完全基于前馈神经网络的检测模型（simplified feed-forward intrusion detection，SFID），模型通过神经元个数逐级递减，消除样本数据中的冗余特征，基于降维后的特征对网络行为进行分类，实现特征抽取和入侵分类，提升了模型整体的训练效率，但检测结果仍有提升空间.

针对信息不完备的处理，池亚平等[11]将 SVM 作为弱分类器，每个 SVM 对应一个特征，一组 SVM 作为所有选取的特征所组成一个基分类器，Adaboost 将多个基分类器组合，利用 SVM 和 Adaboost 的各自优点构建了 SVM-Adaboost 模型. 虽然提升了训练效率，但是并没有考虑数据类别不平衡的问题. Li 等[12]采用半监督算法对未标记的数据进行自动标记，虽然无需人工干预，但缺少对不完备信息数据的处理. Hamid 等[13]构建小波变换和人工神经网络的结合模型，降低了数据不平衡所造成的影响，提高了低频数据类别的检测准确率. Wu 等[14]设计了 SAE 和 Bagging 组合的检测方法，通过对大量高维、无标签原始数据的特征降维，获得原始数据的深层特征. 算法引入了稀疏因子，使得栈式稀疏自编码在检测过程中有更好的泛化性能，检测准确率较高，但对数据特征量要求大. 饶绪黎等[15]设计了数据不完备下的入侵检测方法，方法丢弃了部分特征，仅利用少量特征就获得较好的检测效果.

综上所述，虽然有很多机器学习算法被应用于入侵检测领域，也取得了不错的检测效果，但大多数模型的结构复杂、训练时间长，难以满足真实网络环境下检测实时性的要求，且其中一些模型对数据的特征非常敏感，一旦数据特征量减少，检测准确率会迅速下降.

针对上述问题，本文提出一种面向不完备信息的集成神经网络入侵检测方法（intrusion detection with incomplete information based on ensemble neural network，IDII-ENN），实现了不完备信息下的轻量级网络入侵检测. 模型主要包含了 3 个部分：首先，模型对数据类别不平衡的缺陷进行弥补，避免了因信息不完备导致训练不充分的问题；然后，将采样后的数据送入基于前馈神经网络的分类器，网络的低复杂度可以有效降低模型的训练时间，满足网络入侵检测实时性的要求；最后，采用基于集成学习的方法，对基分类器的分类结果进行融合，强化了模型的分类效果. 模型在满足检测实时性的同时，以较高的准确率实现了不完备信息下的入侵检测.

1　模型设计

在网络传输的过程中，存在数据丢包和网络延迟等问题，以及为了保护隐私对数据进行隐藏的现象. 因此，模型在数据层面，对网络数据进行信息完备化处理，优化各类别的数据量，弥补网络数据自身的缺陷. 模型在算法层面，基于前馈神经网络对数据进行分类，降低神经网络的复杂度，提升训练效率. 模型在分类阶段，设计基于集成学习的结果融合方法，对多个基分类器的结果按照一定策略进行融合，得到最终的检测结果，提高模型检测的准确率. 入侵检测的模型如图 1 所示.

1.1　基于 bootstrap 采样的信息完备化

信息不完备导致了各类别数据的数据量不均衡的问题，为了避免训练数据在各类别上存在较大的差别，避免训练不充分. 模型先对数据进行完备化处理，处理方法基于改进后的 bootstrap 方法.

自助抽样法（bootstrap sampling，BS）是有放回的抽样算法，在给定包含 m 个样本的数据集 D 中，经 m 次有放回的抽样生成一个数据子集. 但在样本训练

集的随机采样中，每个样本被采集到的概率是 $1/m$，不被采集到的概率为 $1-1/m$. 经 m 次采样均没有被采集到的概率是 $(1-1/m)^m$，因此当采样次数足够大时，在每轮的随机采样中，训练集中仍有约 36.8% 的数据无法被采样到.

为了使尽可能多的数据被采样到，对 BS 稍作改进，将原始数据集按照抽取、选取、合并、丢弃这 4 步进行采样，得到一份新的数据子集. 平衡各类别间的数据量，基于 BS 的完备化处理如图 2 所示.

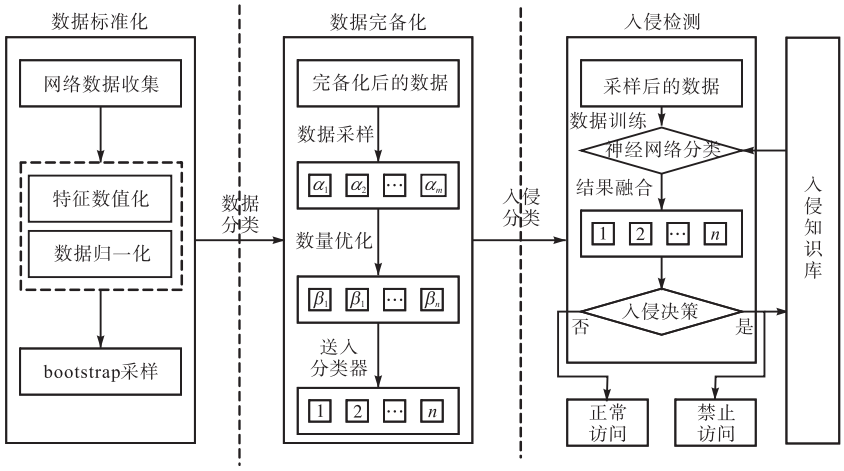

图 1　IDII-ENN 入侵检测模型

Fig. 1　IDII-ENN intrusion detection model

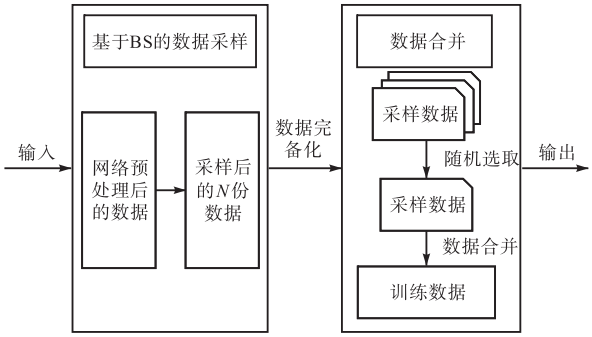

图 2　基于 BS 的完备化处理

Fig. 2　Complete processing based on BS

完备化处理步骤：

(1) 假定分类器的个数为 N 个，为了提升采集到低频样本的概率，使用有放回的 BS 方法对数据进行 N 轮采样，抽取 N 份数据子集 D'，记为 $\alpha_1,\alpha_2,\cdots,\alpha_N$，$\alpha_i$ 中的数据量与原始数据集 D 中的数据量相同，记为 m.

(2) 在抽取出的 $\alpha_1,\alpha_2,\cdots,\alpha_N$ 中随机选取 $\lceil \ln N \rceil$ 份数据，记为 $\beta_1,\beta_2,\cdots,\beta_{\ln N}$.

(3) 将选取出的 $\beta_1,\beta_2,\cdots,\beta_{\ln N}$ 进行合并，得到数据集 β，即 $\beta=\beta_1+\beta_2+\cdots+\beta_{\ln N}$，从而获取较单份采样数据更丰富的样本子集.

(4) 为了平衡样本子集的数据量，对数据集 β 进行数据随机丢弃，丢弃比例按 β 中数据量的 $1-\dfrac{1}{\lceil \ln N \rceil}$ 计，丢弃后得到一份完整的样本数据子集 $\sum_i$，此时 $\sum_i$ 中的数据量为 m.

在获取到一份新的样本数据子集 $\sum_i$ 后，重复 N 次上述的抽样算法，得到基于 BS 有放回采样的 N 份样本数据子集，记为 $\sum_1,\sum_2,\cdots,\sum_N$，以便每个学习器学习. 通过多轮的采集数据，降低了各类别在数据量上的不均衡；通过对数据的随机丢弃，避免了因数据冗余而导致的训练效率低的问题.

1.2　基于前馈神经网络的入侵检测

基于前馈神经网络对入侵行为进行分类，前馈神经网络包含输入层、隐藏层、输出层，其中隐藏层有 3 层，数据由输入层传入，经隐藏层降维，送进输出层，输出层采用 softmax 函数，并完成分类. 前馈神经网络分类器如图 3 所示.

训练数据记为 $X=(x_1^0,x_2^0,\cdots,x_m^0)$，训练数据乘上对应权重 $(\boldsymbol{w})$，再加上神经元的偏置值 $(\boldsymbol{b})$，得到下一层的输入值. 第 $i-1$ 层到第 i 层的权重矩阵记为 $\boldsymbol{w}^i$、偏置向量记为 $\boldsymbol{b}^i$，输入值记为 z^i. 为了便于描述和公式统一，当 $i=0$ 时，将输入层的输入特征 x^i 用 a^i 表示，即 $a^i=X$，因此输入值可以统一表示为 $z^i=\boldsymbol{w}^i a^i+\boldsymbol{b}^i$. 激活函数为 ReLU 函数，表达式为 $f(x)=\max(0,x)$. 第 i 层的激活值为 a^i，$a^i=\mathrm{ReLU}(z^i)$.

计算得到各隐藏层神经元的输出值，并引入 Dropout，随机将 20% 的神经元置零，以增强模型泛化性. 输出层使用 softmax 函数，函数表达式为

$S_i=\dfrac{\mathrm{e}^i}{\sum\limits_{i=1}^{n}\mathrm{e}^i}$. 输出层的输出为 y_i，y_i 的表达式为

$$y_i=\mathrm{softmax}(\boldsymbol{w}^i a^i+\boldsymbol{b}^i) \tag{1}$$

基于正则化后交叉熵损失函数，对样本点为 m、类别为 n 的交叉熵损失函数的表达式为

$$\mathrm{loss}=-\frac{1}{m}\sum_{j=1}^{m}\sum_{i=1}^{n}y_{ji}\log(\hat{y}_{ji})+\frac{\lambda}{2n}\sum_{i=1}^{n}\|\boldsymbol{w}_i\| \tag{2}$$

式中：n 为类别数量；m 为当前 batch 的训练样本数量；y_{ji} 为该样本真实的 one-hot 编码；$\hat{y}_{ji}$ 为 softmax 函数的输出值，$\boldsymbol{w}_i$ 为权重值. loss 函数中加入正则项，预防模型因个别特征的影响产生较大误差.

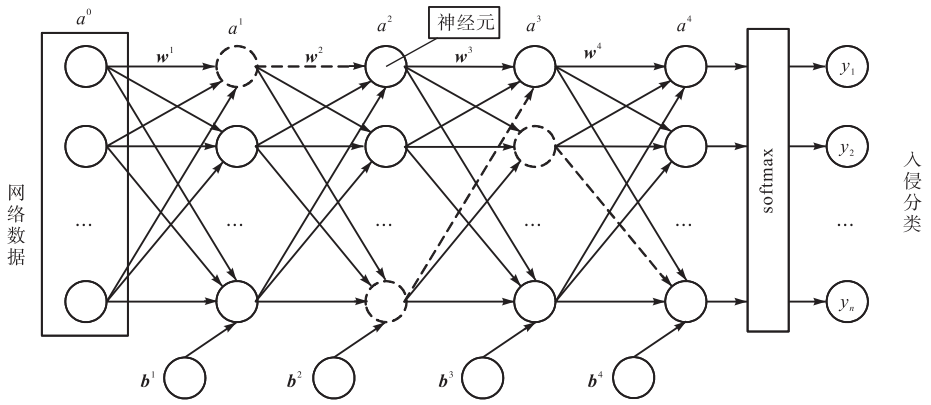

图 3　前馈神经网络分类器

Fig. 3　Feedforward neural network classifier

模型的参数集合为 $\theta=\{\boldsymbol{w}^i,\boldsymbol{b}^i,i=1,2,3,4\}$，基于随机低度下降(stochastic gradient descent，SGD)的方法对参数进行更新. 参数 θ 的更新表达式为式(3)，α 为模型更新的速率.

$$\theta'=\theta-\alpha\frac{\partial\mathrm{loss}}{\partial\theta} \tag{3}$$

1.3　基于 Bagging 集成学习结果融合

集成学习是使用多个学习器共同学习的算法，然后使用一定的策略对多个学习器的结果加以融合，从而获得比单个学习器更好的学习效果. 本文设计了基于 Bagging 算法的结果融合方法. 首先对网络数据按照前文所述方法进行 N 次重复采样，获得 N 份不完全相同的训练数据；然后将每一份数据送入前馈神经网络分类器，并行对其进行入侵检测的判断；最后对多个结果进行融合，得到最终的检测结果. 基于 Bagging 的集成结果融合如图 4 所示.

模型基于集成学习的方法将多个弱分类器组合成一个强分类器，强化模型的分类效果，提升了分类准确率. 通过简化神经网络模型的复杂度缩短了模型训练时间. 经过采样后的数据具有较大差异性，提高了基于集成学习分类方法的检测准确率. 模型基于投票表决法融合了多个分类器的结果，投票公式为

$$f(x)=\arg\max(N_i) \tag{4}$$

式中：N_i 表示类别为 i 的分类器的个数. $f(x)$ 即为入侵检测数据的最终类别.

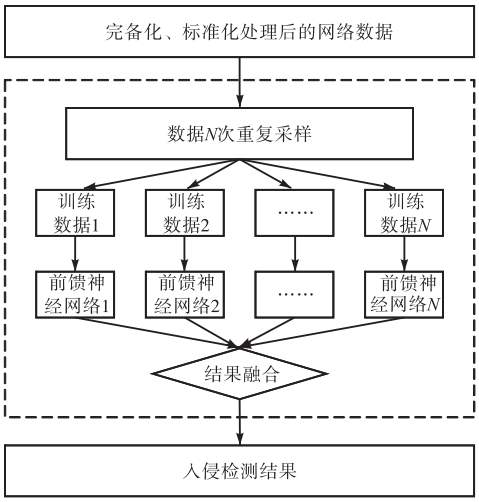

图 4　基于 Bagging 的集成结果融合

Fig. 4　Ensemble result fusion based on Bagging

2　实验设置

KDD Cup 99 数据集是入侵检测的标准数据集. 在入侵检测前，先对数据进行预处理，包括特征数值化和归一化等操作. 在入侵检测模块，基于前馈神经网络对采样后的数据进行分类，并用集成学习将多个弱分类器组成一个强分类器. 本文对每个数据集进行多次实验，并在测试集上验证了模型的有效性.

2.1　实验数据

KDD Cup 99 数据集的每个网络连接被标记为正

常或异常，异常类型包含拒绝服务攻击(denial of service，DOS)、远程主机攻击(remote to local，R2L)、用户到根攻击(user to root，U2R)、端口扫描攻击(Probe)等共 39 种攻击类型，其中 22 种攻击类型出现在训练集中，另有 17 种未知攻击类型出现在测试集中. 数据类型数量分布见表 1.

表 1　数据类型数量分布

Tab. 1　Data type quantity distribution

类型	训练数据(10%)	测试数据
Normal	97 278	60 593
DOS	391 458	229 853
Probe	4 107	4 166
R2L	1 126	16 189
U2R	52	228

2.2　数据预处理

样本特征包含数值型数据和字符型数据(protocol_type，service，flag)，采用 one-hot 编码方式将字符型数据数值化处理. 部分数据存在数值量纲差异大的问题，而过大的量纲差异导致网络收敛慢，故对数据进行归一化，归一化公式为

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{5}$$

式中：x' 为归一化后的特征值；x 为原特征值；$x_{\max}$ 和 $x_{\min}$ 分别为该特征属性中的最大值和最小值. 模型采用 Min-Max 线性归一化方法，把所有特征均映射到[0，1]的区间上.

2.3　评估机制

使用准确率(accuracy，AC)和训练时间对模型的检测效果进行评价. 样例根据其真实类别与分类器的预测类别组合分为真正例(true positive，TP)、假正例(false positive，FP)、真反例(true negative，TN)、假反例(false negative，FN). 准确率的定义表达式为

$$\mathrm{AC} = \frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}} \times 100\% \tag{6}$$

模型的准确率表示预测正确的个数占全部样本的百分比，百分比越大表示模型的检测效果越好.

3　实验及结果评估

为模拟信息不完备的情况，实验中将数据特征量递减，观察 IDII-ENN 准确率的变化.

准确率的实验包括：第一，观察数据特征量对准确率的影响，特征量从 80% 特征开始，以 10% 递减，直至为总特征量的 10%，对比 IDII-ENN、SFID、SAE 各自的准确率；第二，观察分类器个数的差异对准确率的影响，比较 3 种方法在准确率上的表现.

训练时间的实验包括：第一，在分类器个数变化的情况下比较集成算法的耗时；第二，在确定分类器个数的情况下，比较各算法在特征量不同情况下的耗时.

3.1　准确率

在数据预处理后，实验对比了 SFID、SAE、IDII-ENN 算法在信息不完备情况下的检测准确率. 为避免结果的随机性，在相同实验环境下，进行多次实验，取平均准确率为最终结果. IDII-ENN 算法在特征量 40% 时获得了较高的准确率且趋于稳定. 3 种算法实验的准确率如图 5 所示.

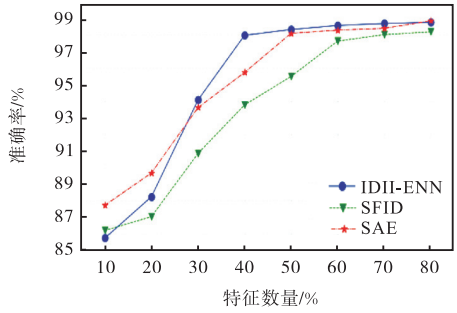

图 5　不同算法的检测准确率

Fig. 5　Detection accuracy of different algorithms

集成学习的分类器数量会对模型的检测准确率产生影响，因此设计了 Bagging-DL 和 SVM-Adaboost 在不同分类器个数下的准确率对比实验. 本文的模型在分类器个数达到 60 个时就获得了较高的准确率，该结果优于对比算法(图 6).

为了验证模型对各数据类型的分类准确率情况，本文设计了 IDII-ENN 模型在不同特征量下对各数据类型的检测实验(图 7). IDII-ENN 对 Normal、DOS、Probe 这 3 类数据检测结果较好，在特征数量达到 50% 时就已经获得了较高的准确率. 3 个类别的检测准确率曲线非常接近，表明在相同条件下数据量对模型检测有着重要影响，训练数据越多，模型的拟合效果越好. 同时，原始数据的数据量对模型的初始训练非常重要，可以使模型快速获得较好的检测效果. 模型对 U2R、R2L 的检测在特征较多时同样可以获得较好的检测准确率. 这说明本文的模型对各数据类型的分类均有良好的表现.

损失函数在不同的神经网络中有不同的效果，实验对比了 Mean Squared Error、Root Mean Square Error、Mean Absolute Error、Cross Entry 等损失函数的

优化效果. 为了验证不同特征数量下损失函数的表现，本文对比了几种损失函数在特征数量为 20%、40%、80% 下的检测准确率(表 2). 通过实验结果可知，Cross Entry 损失函数相比其他损失函数在检测准确率上的表现更好.

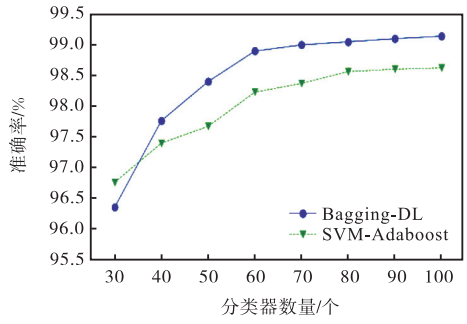

图 6　不同分类器下的检测准确率

Fig. 6　Detection accuracy of different classifiers

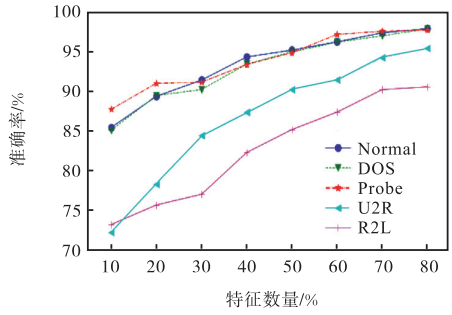

图 7　不同数据类型的检测准确率

Fig. 7　Detection accuracy chart of different data types

表 2　不同特征数量各类损失函数的检测准确率

Tab. 2　Accuracy of various loss functions of different feature quantites

损失函数	准确率/%		
	20%	40%	80%
Cross Entry	88.25	97.97	98.75
Root Mean Square Error	90.68	97.35	98.25
Mean Absolute Error	87.82	97.76	98.98
Mean Squared Error	89.24	96.08	97.67

3.2　训练时间

为了验证模型在检测时间上的表现，对比了 IDII-ENN、SFID、SAE 算法在信息不完全情况下的训练时间. Bagging-DL 和 SVM-Adaboost 都是基于集成学习的分类算法，本文设计了两种算法在不同分类器数量下训练时间的对比实验. 实验中对各算法的运行时间进行记录，在相同实验环境下，多次实验，取平均运行时间作为最终结果. 3 种算法在不同特征数量的训练时间如图 8 所示. Bagging-DL 和 SVM-Adaboost 不同分类器数量的训练时间如图 9 所示.

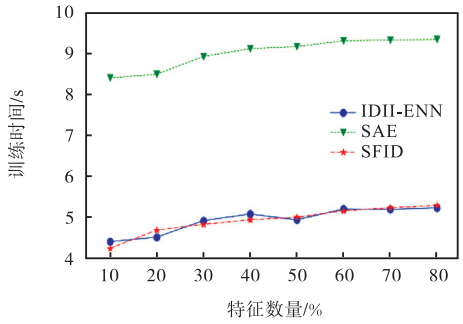

图 8　不同特征数量的训练时间图

Fig. 8　Training time graph of different feature quantities

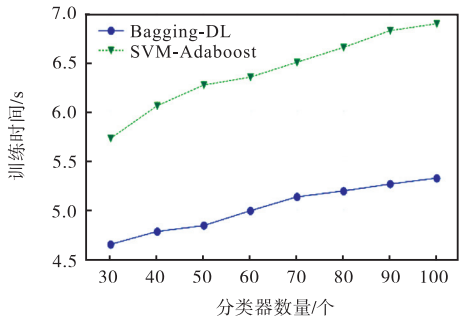

图 9　不同分类器数量的训练时间图

Fig. 9　Training time graph for different number of classifiers

由图 8 和图 9 可知：本文模型和 SFID 模型训练时间相差无几，但本文的算法在训练时间上更平稳，相较之下 SAE 的训练时间略长. 在特征数量减小时，IDII-ENN、SFID、SAE 这 3 种算法的训练时间均有一定的变化，表明数据的特征数量对这 3 种算法的训练时间存在影响. 集成学习分类器个数对训练时间也有影响，随着分类器数量增加，训练时间也随之上升，但是整体来看影响并不大.

4　结　语

针对传统入侵检测方法很难同时满足准确率和实时性的双重要求，同时为了解决不完备信息下入侵检测的问题，本文提出了一种面向不完备信息网络的集成神经网络入侵检测方法. 该方法的检测结果与其他算法的结果在准确率方面不相上下，但在训练时间上缩短了 15%，表明该方法具有可推广性，能够满足网络入侵检测实时性的需求.

参考文献：

[1] CHU A，LAI Y，LIU J，et al. Industrial control intrusion fetection spproach based on multi-classification Google-

Net-LSTM model[EB/OL]. [2020-12-06] https://dblp.org/rec/journals/scn/ChuLL19.html.

[2] 汪盼,宋雪桦,王昌达,等. 基于改进的深度信念网络的入侵检测方法[J]. 计算机工程与应用,2020,56(20):87-92.

[3] AMINANTO M E, CHOI R, TANUWIDJAJA H C, et al. Deep abstraction and weighted feature selection for Wi-Fi impersonation detection[J]. IEEE Transactions on information forensics and security, 2018, 13(3): 621-636.

[4] DIEU-MERCI K K. Network data security for the detection system in the internet of things with deep learning approach[D]. 太原:太原理工大学,2018.

[5] SHONE N, NGOC T N, PHAI V D, et al. A deep learning approach to network intrusion detection[J]. IEEE Transactions on emerging topics in computational intelligence, 2018, 2(1): 41-50.

[6] LIU H, LANG B. Machine learning and deep learning methods for intrusion detection systems: a survey[J]. Applied sciences, 2019, 9(20): 4396.

[7] KHAN K, MEHMOOD A, KHAN S, et al. A survey on intrusion detection and prevention in wireless ad-hoc networks[J]. Journal of systems architecture, 2020, 105: 101701.

[8] GURUNG S, GHOSE M K, SUBEDI A. Deep learning approach on network intrusion detection system using NSL-KDD dataset[J]. International journal of computer network and information security, 2019, 11(3): 8-14.

[9] LOPEZ-MARTIN M, CARRO B, SANCHEZ-ESGUEVILLAS A. Application of deep reinforcement learning to intrusion detection for supervised problems[J]. Expert systems with applications, 2020, 141: 112963.

[10] 冯文英,郭晓博,何原野,等. 基于前馈神经网络的入侵检测模型[J]. 信息网络安全,2019(9):101-105.

[11] 池亚平,凌志婷,王志强,等. 基于支持向量机与Adaboost 的入侵检测系统[J]. 计算机工程,2019,45(10):183-188.

[12] LI W, MENG W, AU M H. Enhancing collaborative intrusion detection via disagreement-based semi-supervised learning in IoT environments[J]. Journal of network and computer applications, 2020, 161: 102631.

[13] HAMID Y, SHAH F A, SUGUMARAN M. Wavelet neural network model for network intrusion detection system[J]. International journal of information technology, 2019, 11(2): 251-263.

[14] WU Z, WANG J, HU L, et al. A network intrusion detection method based on semantic re-encoding and deep learning[J]. Journal of network and computer applications, 2020, 164: 102688.

[15] 饶绪黎,徐彭娜,陈志德,等. 基于不完全信息的深度学习网络入侵检测[J]. 信息网络安全,2019(6):53-60.

责任编辑: 郎婧

(上接第 53 页)

2017, 201: 503-510.

[14] SHAN W J, FENG Z C, LI Z L, et al. Oxidative steam reforming of methanol on $Ce_{0.9}Cu_{0.1}O_Y$ catalysts prepared by deposition-precipitation, coprecipitation, and complexation-combustion methods[J]. Journal of catalysis, 2004, 228: 206-217.

[15] 李桂菊,李弘涛,夏欣,等. 催化臭氧氧化技术深度处理印染废水的研究[J]. 天津科技大学学报,2019,34(2):55-59.

[16] LU X, LIN L, LIU R, et al. Textile wastewater reuse as an alternative water source for dyeing and finishing processes: a case study[J]. Desalination, 2010, 258(1/2/3): 229-232.

[17] QI F, XU B B, ZHAO L, et al. Comparison of the efficiency and mechanism of catalytic ozonation of 2,4,6-trichloroanisole by iron and manganese modified bauxite[J]. Applied catalysis B: environmental, 2012, 121/122: 171-181.

责任编辑: 周建军