西安电子科技大学学报
Journal of Xidian University
ISSN 1001-2400,CN 61-1076/TN

《西安电子科技大学学报》网络首发论文

题目：一种深度学习的网络安全态势评估方法
作者：杨宏宇，曾仁韵
收稿日期：2020-08-16
网络首发日期：2020-10-20
引用格式：杨宏宇，曾仁韵．一种深度学习的网络安全态势评估方法．西安电子科技大学学报. https://kns.cnki.net/kcms/detail/61.1076.TN.20201020.1419.002.html

一种深度学习的网络安全态势评估方法

杨宏宇[1]，曾仁韵[1]

(1. 中国民航大学 计算机科学与技术学院，天津 300300)

摘要：由于传统的网络安全态势评估方法依赖于人工的标注和评估，在面对大量数据时，存在效率低、灵活性差等问题。针对这些问题，提出一种深度学习的网络安全态势评估方法。首先，建立深度自编码模型，对网络中受到的各种攻击进行识别；然后，为了提高模型对拥有少量训练样本的类型的检测率，设计了欠过采样加权算法；最后进行模型测试并计算攻击概率，确定每种攻击的影响得分并计算网络安全态势值。实验结果表明，提出的深度自编码模型的准确率和召回率都优于对比的模型，这使得评估结果更加准确有效。

关键词：网络安全态势评估；网络攻击；深度学习；深度自编码器；数据重采样

中图分类号：TP309　　**文献标识码**：A

Method for assessment of network security situation with deep learning

YANG Hongyu[1], *ZENG Renyun*[1]

(1. School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China)

Abstract: The traditional methods for assessment of network security situation rely on manual label and evaluation. When faced with a large amount of data, there appearsome problems such as low efficiency and poor flexibility. First, we propose a Deep Autoencoder-Deep Neural Network (DAEDNN) model to identify all kinds of attacks on the network. Then, the Under-Over Sampling Weighted (UOSW) algorithm is designed to improve the detection rate of the model on categories with a few training samples. Finally, we conduct model testing and calculate the attack probability. Besides, we determine the impact score of each type of attack and calculate the network security situation value. Experimental results show that the precision and recall of the proposed model are better than those of the compared models, and that the proposed model has a better performance in accuracy and efficiency.

Key Words: network security situation assessment; network attacks; deep learning; deep autoencoder; data resampling

收稿日期：2020-08-16
基金项目：国家自然科学基金民航联合研究项目（U1833107）
作者简介：杨宏宇(1969—)，男，教授，博士 E-mail：yhyxlx@hotmail.com

近年来，随着互联网的快速发展，通过互联网进行的攻击问题越来越频繁，带来的危害也越来越严重。我国互联网态势报告[1]中指出，在 2019 上半年，我国网络遭受了大量的、多样的威胁攻击，并针对此情况开展了网络安全威胁治理工作，采用的一个重要手段就是网络安全态势评估。网络安全态势评估是一种常用的、有效的解决方案，它综合了影响网络安全的指标，为网络管理人员提供决策意见，从最大程度上降低网络攻击威胁产生的危害[2]。

ZHAO 等[3]提出了基于层次分析法和灰色关联分析的多维系统安全评价方法，以系统安全评价模型构建原则为指导，构建了环境安全、网络安全、脆弱性安全的多维系统安全评价模型。Alali 等[4]将互联网受到的网络威胁作为态势评估的重要指标，利用模糊逻辑推理系统改进网络安全威胁评估模型。然而，上述方式在面对新型的网络威胁攻击时不能做出及时反应。

随着神经网络、机器学习等信息技术在许多领域的成功应用，在信息安全领域开始尝试将这些技术融入网络威胁态势评估。DONG 等[5]引入动量因子，对搜索算法进行了优化，提出了一种改进反向传播神经网络的网络安全态势定量评估方法。WEN 等[6]提出了结合朴素贝叶斯分类器的网络安全态势评估方法，从整体动态上展示网络当前安全状况。HU[7]结合支持向量机，并改良了布谷鸟算法预测网络安全态势，该方法在 KDD 数据集上的性能达到了较高的精度。上述方法可以动态评估网络安全态势，但是面对如今的大量网络威胁数据，已经不能满足实时、直观的评估需求。

在大数据背景下，结合深度神经网络的算法已经应用于海量威胁攻击数据检测。HODO 等[8]通过实验表明，相对于传统的浅层网络方法，深层网络在检测网络威胁攻击方面更加准确和有效。ALTHUBITI 等[9]应用长短期记忆网络（Long-Short-Term Memory，LSTM）在 CIDDS-001 数据集上进行训练和测试。尽管实验结果取得较高的准确率，但是文中选择的测试集是训练集的一部分，因此没有表现出模型的泛化性。JAVAID 等[10]将自我学习（Self-taught Learning，STL）与稀疏自动编码器（Sparse Autoencoder，SAE）相结合，对 NSL-KDD 数据集的检测准确率有很大的提升。然而，该方法在训练过程中抑制了某些神经元的传播而且易出现不同数量的样本检测结果不平衡的现象。

针对上述方法的不足，笔者提出基于深度学习的网络安全态势评估方法。为了解决数据集中不同类型攻击的分类结果极度不平衡问题，提出一种欠过采样加权（Under-Over Sampling Weighted，UOSW）算法对数据集进行处理，结合深度自动编码器（Deep Autoencoder，DAE）对网络攻击进行分类。在得到网络攻击分类后，对每种攻击类型进行影响评估，并对网络安全状况进行量化评估。通过实验证明本文方法可实现对网络安全状况的实时评估，评估效果更加高效、直观，性能指标优于其他模型。

1 网络安全态势评估模型

笔者设计的网络安全态势评估模型包括态势获取、态势分析和态势评估 3 个部分。网络安全态势评估模型的结构如图 1 所示。

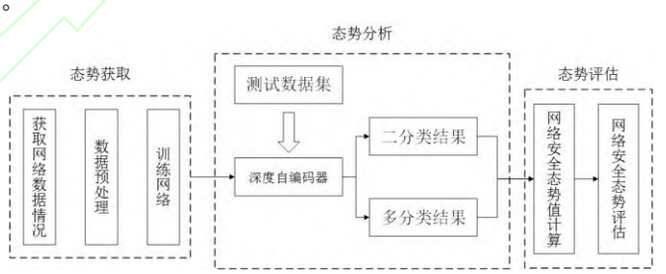

图 1 网络安全态势评估模型

（1） 态势获取

在此阶段，获取网络中的流量数据。为了模拟网络处理海量流量数据的情况，本文选取上述 NSL-KDD 数据集作为网络流量。数据预处理后，输入深度自编码器进行训练。

（2） 态势分析

将测试数据集输入训练后的模型，记录结果输出的二分类结果和多分类结果，用于计算网络安全态势量化值。

（3）　态势评估

根据测试的攻击分类结果，计算网络攻击概率和各种网络攻击的影响值。另外，计算网络安全态势值并对网络安全态势进行评估。详细计算方法将在接下来的章节展示。

2　深度自编码器

2.1　深度自编码器设计

2.1.1　模型结构

自动编码器（Autoencoder，AE）由编码器和解码器组成，主要被应用于数据降维和特征学习。输入数据通过编码器被映射到解码器，解码器可以用更精简的特征描述原始数据。深度自动编码器（Deep Autoencoder，DAE）是一种改进的自动编码器模型。HINTON 等人[11]深化了原有自动编码器的网络结构，生成了 DAE 网络。因为含有隐藏层更多，DAE 的学习能力得到了提高，这使得它更有利于特征学习。

深度神经网络（Deep Neural Network，DNN）由于其准确性和高效性，在入侵检测中得到了广泛的应用。由于 DNN 包含了多个隐藏层，使得它的学习能力显著提高。与传统的机器学习分类器相比，DNN 可以在更短的时间内获得更准确的分类结果，因此，选择 DNN 作为网络攻击数据的分类器，所提出的深度自编码器模型(Deep Autoencoder Deep Neural Network，DAEDNN)如图 2 所示。

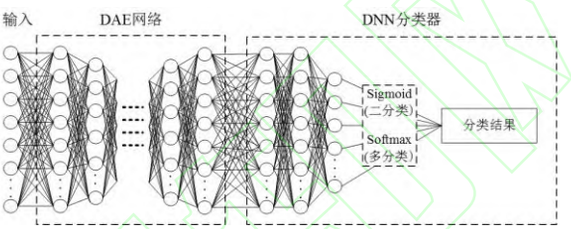

图 2 DAEDNN 模型

由图 2 可见，模型接收输入数据后，先通过 DAE 网络进行特征学习并记录学习结果，根据学习结果和 DNN 分类器，将输入数据进行分类，而后将其分类结果应用于后续的网络安全态势量化评估过程。

DAEDNN 模型不仅可以进行二分类，也可以进行多分类。在进行二分类任务时，模型的激活函数为 sigmoid 函数，sigmoid 函数将模型输出值映射到 0 和 1 区间，其中，数值越靠近 1，则越容易被判定为异常流量。Sigmoid 函数（F_{sgm}）的计算公式如下：

$$F_{sgm}(x) = \left(1 + e^{-x}\right)^{-1} \tag{1}$$

当模型进行多分类任务时，模型的激活函数为 softmax 函数，softmax 也是将输出映射到 0 和 1 区间，但是与 sigmoid 函数不同的是，各个类别的输出值相加的值等于 1，模型选择输出值最大的类别为预测的类别。Softmax 函数（F_{sfm}）的计算公式如下所示：

$$F_{sfm}(z_i) = e^{z_i} \Big/ \sum_{j=1}^{K} e^{z_j} \tag{2}$$

其中，$z = (z_1, z_2, ..., z_k)$，K 表示输出可以被分为 K 个类，z_i 表示每一类所取得的值。

2.1.2　模型训练

在 DAEDNN 模型中，DAE 模型进行特征学习，为了让 DNN 分类器充分学习 DAE 的特征提取结果和提高模型性能，减少模型过拟合的风险，分次训练 DAEDNN 模型。

模型训练分为三个步骤：（1）将训练数据输入至 DAE 网络，进行特征学习，记录训练完成的权重值。（2）DAE 模型训练结束后，组合 DAE 模型和 DNN 模型为 DAEDNN 模型，一起训练这两个网络。为了获取 DAE 模型的训练结果，将 DAEDNN 模型中的 DAE 网络的权重值设置为（1）保留的权重值，并把 DAE 层的参数设置为不可训练，与 DNN 网络一起进行训练，此时网络只会更新 DNN 网络的参数。（3）将 DAE 层的参数设置为可训练，更新 DAE 网络和 DNN 网络的参数。训练过程中更新训练参数，不仅可

以获取 DAE 层的特征学习结果，也提高了模型对数据的表征能力。

2.2 欠过采样加权数据重采样算法

2.2.1 数据集描述

选择网络安全领域相对权威的入侵检测数据集 NSL-KDD 作为评估的数据源。NSL-KDD 数据集改良于 KDD99 数据集，它删除了重复的网络流量数据记录，这有助于分类器产生无偏差的结果[12]。NSL-KDD 数据集包含 41 个特征和 5 种主要攻击类型。文中使用的数据集信息如表 1 所示。

表 1 KDD-NSL 数据集信息

数据集	Normal	DoS	Probe	R2L	U2R	Total
KDDTrain+	67,343	45,927	11,656	995	52	125,973
KDDTest+	9710	7456	2421	2754	202	22,543

2.2.2 数据预处理

为了更方便、准确地训练网络模型，需要将数据集中的分类特征转换为数字特征，并进行数值归一化。

1） 特征数值化

NSL-KDD 数据集有 3 个分类特征“protocol_type”、“service”和“flag”，分别包括 3、64 和 10 个类别。通过独热编码技术，将这 3 种分类特征转化为只表示 0 和 1 的数据。对这 3 个分类特征进行处理之后，数据集由 41 个特征维度变为 116 个特征维度。

2） 数值归一化

数据集中某些特征的最小值与最大值之间存在显著差异。为了减少不同数值水平对模型的负面影响，本文采用对数标度法对特征值进行标度，使其归一化到同一区间。数值归一化的过程可以表示为：

$$x_{norm} = (x - x_{min}) / (x_{max} - x_{min}) \tag{3}$$

其中，x 表示特征原本的值，x_{max} 和 x_{min} 为特征所取得的最大值和最小值。

2.2.3 欠过采样加权数据重采样算法

由表 1 可见，在训练数据集中，五类攻击的数据量非常不均匀，其中数据量最大的 Nomal 类有 67343 条数据，而 DoS 和 U2R 这两种类型只包含 52 和 995 条数据。在训练深度学习模型的过程中，训练数据较少会导致模型无法充分学习数据的特征，而训练数据过多又可能导致模型过拟合，即模型学习到了数据本身以外的特征。因此，极不平衡的数据会导致模型的学习效果不佳，导致数据量大的类别的识别准确度较高，反之较小。

数据分析中的过采样和欠采样是用来调整数据集类分布的技术，也称为数据重采样。欠采样通常是删除数据量过大的类别的些许样本，而过采样增加了数据中少数样本的数据量，以达到数据平衡。为解决数据量分布不平衡的问题，提高模型检测少数类的精度，笔者提出一种过采样、欠采样和加权相结合的欠过采样加权（Under-Over Sampling Weighted，UOSW）算法。该算法步骤设计如下：

设原始数据集为 Set_1，输出的数据集为 Set^2，需要进行重采样处理的数据类型为 $type_i$，其原始数据集和样本数量为 Set_i 和 x_i。

步骤 1 计算数据集中每种类型的权重 w_i。在网络训练中，当训练集中每个类别的数据量非常接近（达到平均值，以下用 *average* 代替）时，网络的识别准确率会很高。因此，本文计算每种类型的实际样本量与理想样本量之间的差值作为权重，以达到每种类型的均衡值。

$$w_i = \sum_i^n x_i \Big/ (x_i \times n) \tag{4}$$

其中，n 表示数据集包含 n 种类别。

步骤 2 数据欠采样。对于数据量过大的类型，进行数据欠采样，使处理后的数据样本接近平均值(*average*)。使用 Python 中 sklearn 库的“train_test_split”方法将数据集 Set_i 分为两个数据集 S_{i_train}, S_{i_remain}。将 S_{i_train} 作为训练集，并加入 Set^2，其中，S_{i_train} 的数据量大小 $size_i = x_i \times w_i$；S_{i_remain} 用于接下来的数据过采样操作，将其加入数据集 Set_{remain}。

步骤 3 数据过采样。应用过采样算法 SMOTE[13]处理数据量很少的类别的样本，SMOTE 的核心是在

现有少数类样本的基础上生成新的同类样本。由于 SMOTE 算法最初是针对二分类问题，而本文研究中存在多分类问题，因此对算法进行了以下改进：

1） 合并其他类型数据。将步骤 2 中经过欠采样处理的数据集 Set_{remain} 和原始数据集中的少量类型的数据集合并，表示为 Set_{union}。

2） 改变标签。经过步骤 1），Set_{union} 中包含与 n 种类别的数据，由于 SMOTE 算法只针对于二分类，因此要将需要进行过采样的类型与其他类型区分开来。将数据集 Set_{union} 的标签更改为同一类型，但不同于 $type_i$。

3） 确定数据量大小。为了平衡数据集，需要对少数类样本进行扩展，设扩展后的数据量大小为 $size_i$ 其中 $size_i = x_i \times w_i$，w_i 是数据类型 $type_i$ 的权重。

4） 数据过采样。使用 Python 中 imblearn 库的 SMOTE 方法，结合其他类型的数据生成所需的数据，将其加入 Set^2。

重复（1）~（4），直到数据量少于平均值的类型全部完成过采样操作。

3　网络安全态势评估

3.1　网络攻击影响值

NSL-KDD 数据集包括 5 种类型的网络数据：Normal、DoS、U2R、R2L 和 Probe。上述攻击的基本信息如表 2 所示。

表 2　5 种攻击类型的基本情况

攻击类型	描述
拒绝服务(Denial of Service , DoS)	这种攻击会使计算机或网络停止服务，使其目标用户无法访问。DoS攻击通过向目标发送大量流量或信息来实现这一点。
获取权限(User to Root, U2R)	这种攻击通过非法手段，尝试获取根帐户的权限。
远程入侵(Remote to Local, R2L)	这种攻击使入侵者能够访问原本没有账户的本地计算机。
探测攻击(Probe)	这种攻击收集网络信息，这些信息是发起其他攻击之前所必需的。
正常流量(Normal)	正常的网络流量

基于通用漏洞评分系统（CVSS）制定了攻击影响值评定表[14]。机密性（C）、完整性（I）和可用性（A）得分如表 3 所示。

表 3 攻击影响值评定表

指标	影响程度	影响值
机密性(C)	无(N)/低(L)/高(H)	0/0.22/0.56
完整性(I)	无(N)/低(L)/高(H)	0/0.22/0.56
可用性(A)	无(N)/低(L)/高(H)	0/0.22/0.56

每种攻击类型的影响值（I_i）计算公式如下：

$$I_i = C_i + I_i + A_i \tag{5}$$

3.2 网络安全态势量化

量化网络安全态势，可以更直观地分析网络整体状况。本文的网络安全态势量化评估过程主要包括 4 个部分:攻击分析、计算攻击的影响、计算网络安全态势值和网络安全态势定量评估。每个部分的处理过程设计如下：

（1）　攻击分析

从测试数据集中随机选取若干组数据，并将其输入到 DAEDNN 模型中，对其进行二进制和多分类，记二分类中检测到的攻击比例记为攻击概率（attack probability，p）。

（2）　计算攻击的影响值

结合表 2、表 3 确定每一类攻击类型的 C、I、A 值，并根据公式（5）确定综合的攻击影响值。

（3）　计算网络安全态势值

网络安全态势值综合考虑了网络受到的全部攻击和每种攻击会对网络造成的危害程度，设网络安全态势值为 T：

$$T = \left(p \times \sum_{i}^{n-1} I_i \times t_i \right) \Big/ N - t_n \tag{6}$$

其中，p 为（1）中所得出的攻击概率，n 和 N 表示一共有 n 种类型的数据和 N 个样本，I_i 表示每种攻击类型的影响值，t_i 表示每种攻击的出现次数。t_n 为 Normal 类型出现的次数，由于 Normal 类型是正常的网络数据流，对网络的机密性、完整性和可用性不会有影响，因此它的影响分数为 0，只需要计算 n-1 种攻击类型的影响分值即可。

（4） 网络安全态势定量评估

参考《国家突发公共事件应急预案》[15]对网络安全形势进行分类。根据网络安全态势值 0.00~0.20、0.21~0.40、0.41~0.60、0.61~0.80 和 0.81~1.00 的 5 个区间，将网络安全态势严重程度划分为安全、低风险、中等风险、高风险和超风险等 5 个级别。

4 实验结果与分析

实验的硬件环境为：Intel(R) Xeon(R) Silver 处理器，显卡为 NVIDIA Quadro P2000，内存为 32GB。训练和测试实验均在 Windows 64 位操作系统上进行，使用的编程语言和机器学习库为 Python3.5 和 TensorFlow2.0，模型的训练和测试均使用 GPU 加速。

4.1 评价指标

文中所用的评价指标如下所示：

真阳性（True Positive，*TP*）：表示被模型预测为攻击样本而实际也是攻击样本的次数。假阳性（False Positive，*FP*）：表示被模型预测为正常样本而实际是攻击样本的次数。真阴性（True Negative，*TN*）：表示被模型预测为正常样本而实际也是正常样本的次数。假阴性（False Negative，*FN*）：表示被模型预测为攻击样本而实际是正常样本的次数。下列公式中 P_T，P_F，N_T 和 N_F 分别表示 *TP*，*FP*，*TN* 和 *FN*。

准确率（Precision，*P*）：表示模型预测正确的攻击样本频率。准确率越高，误报率越低。它可以表示为

$$P = \left(P_T \Big/ P_T + P_F \right) \tag{7}$$

召回率（Recall，*R*）：表示被模型正确分类的攻击样本与实际攻击样本的百分比。它可以表示为

$$R = \left(P_T \Big/ P_T + N_F \right) \tag{8}$$

F1 值（F1-score，*F*）：表示综合考虑了模型的准确率和召回率。它可以表示为

$$F = 2 \times P \times R \Big/ \left(P + R \right) \tag{9}$$

4.2 模型二分类结果

在二分类任务时，选择 ROC 曲线和 AUC 面积来反映分类模型的性能。ROC 曲线表示不同阈值设置下分类模型的性能，AUC 面积为 ROC 曲线下的面积，面积越大，表示模型的性能越好，通过面积可以直观地对比各个模型。

在二值分类任务中，模型只需要区分数据是攻击数据还是正常数据。为了检验本文模型的有效性，将笔者提出的 DAEDNN 与决策树（Decision Tree，DT）[8]、支持向量机（Support Vector Machine，SVM）[8] 和长短期记忆网络（Long Short-Term Memory，LSTM）[9] 等模型进行了比较。为了验证本文模型的泛化性，使用 KDDTrain+ 80%的数据进行训练，分别对剩下的 20%和 KDDTest+进行测试。4 种模型的二分类结果如图 3 所示。

从图 3(a)可以看出，在使用 20% KDDTrain+对 4 种模型进行测试时，4 种模型均表现出较好的准确性和泛化能力。这是由于训练集和测试集来源于同一集合，模型学习到的特征可以完全应用于测试数据集，

所以能得到理想的结果。然而，从图 3(b)可见，如果使用 KDDTest+数据集作为测试数据集，4 个模型的准确性则会降低。这是因为测试训练集中存在一些与训练数据集数据格式不同的样本，这种情况与真实的网络情况一致，即模型面临众多未知攻击类型。从图 3(b)可见，在使用 KDDTest+数据集进行模型测试的情况下，DAEDNN 模型的准确率明显优于其他 3 个模型，分别比 DT、SVM 和 LSTM 高出近 13.35%、16.17%和 2.72%，说明 DAEDNN 模型的学习能力更强，具有较好的泛化性。

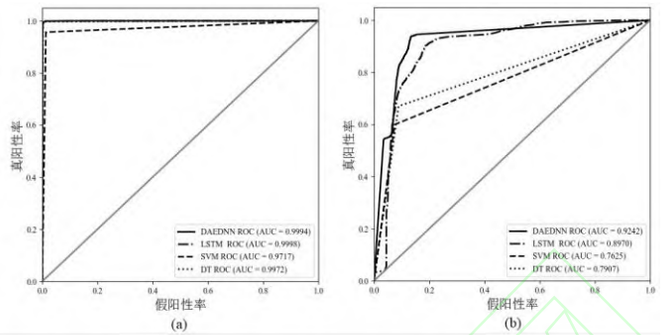

图 3 4 种模型二分类结果

4.3 模型五分类结果

使用 KDDTest+数据集对 DT、SVM、LSTM、DAEDNN 和应用 UOSW 算法的 DAENDD 这 5 种模型进行检验，并选取准确率、召回率和 F1 值作为评价指标，对各种模型进行比较分析。不同模型的指标得分如图 4 所示，图中的纵坐标表示评价指标的百分数，数值越高，模型性能越好。

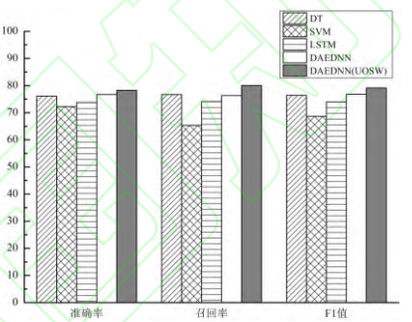

图 4　不同模型的各类指标得分

从图 4 可见，DAEDNN(UOSW)模型在准确率、召回率和 F1 值等方面都优于其他 4 种模型。实验结果表明，DAEDNN(UOSW)提高了少数训练数据样本的攻击类型的召回率和准确率，而对拥有大量训练样本的攻击检测性能并没有降低。

值得注意的是，结合文中的 UOSW 算法后，DAEDNN 的准确率和召回率更高，泛化能力更强。与 DT、SVM 和 LSTM 模型相比，DAEDNN(UOSW)的 F1 值分别提高了 2.77%、10.5%和 5.2%。

4.4 网络安全态势量化评估

从测试数据集中随机选取相同数量的测试样本，对网络安全状况进行了量化评估，并对于分别用不同的模型计算网络安全态势值，其中 20 组测试的网络安全态势值如图 5 所示。

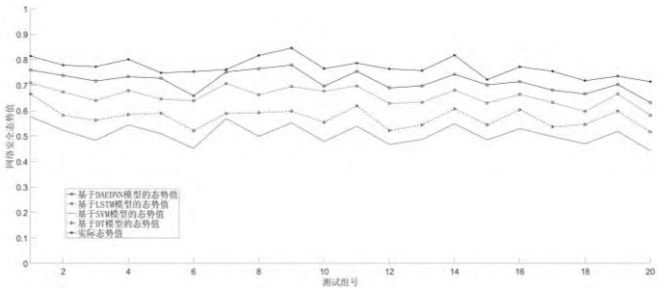

图 5 20 组测试的网络安全态势值

由图5可见，基于DAEDNN模型计算出的网络安全态势值最贴合样本的实际安全态势值，相比于SVM和DT这两类传统的机器学习模型，DAEDNN和LSTM这两类深度学习的方法更能表示数据的真实情况。其他三种模型的态势值与实际态势值相差较大的原因是，训练样本中存在样本量极少的攻击类型，导致模型无法充分学习到这类攻击的特征。而DAEDNN模型应用了UOSW算法，提高了模型检测少样本攻击类型的准确率。所提出模型计算出的态势值与实际态势值之间存在些许差异，但大多数态势值都落在了相同的区域内，根据4.2节定义的网络安全态势严重程度和实际情况相符。

5 结 论

针对传统网络安全态势评估方法在处理大量网络数据时效率低的缺点，提出一种深度学习的网络安全态势评估方法。该方法首先结合了自动编码器和深度神经网络组成DAEDNN模型，用于对网络攻击进行识别。根据识别的结果，计算攻击概率和攻击影响值，从而得出网络安全态势量化值。通过安全态势量化值，可以更直观地反映网络安全态势。实验结果表明，笔者提出的模型在二分类和多分类的攻击检测方面优于其他模型。此外，在进行多种攻击类型检测时，结合所提出的UOSW算法，可以提高模型对拥有少量训练样本的攻击的检测准确率，从而可以更准确地评估网络安全态势。

参考文献：

[1] 国家互联网应急中心. 2019年上半年我国互联网网络安全态势 [EB]. 2020年8月14日. http://www.cac.gov.cn/2019-08/13/c_1124871484.htm.
National Internet Emergency Response Center. The situation of Internet network security in the first half of 2019 [EB]. last accessed 2020/08/14. http://www.cac.gov.cn/2019-08/13/c_1124871484.htm.

[2] YAO Jiayu, FAN Xiani, CAO Ning. Survey of Network Security Situational Awareness [C]// International Symposium on Cyberspace Safety and Security. Cham, Springer, 2019: 34-44.

[3] ZHAO Xiaolin, XU Hao, WANG Ting, et al. Research on Multidimensional System Security Assessment Based on AHP and Gray Correlation [C]// Chinese Conference on Trusted Computing and Information Security. Singapore, Springer, 2019: 177-192.

[4] ALALI M, ALMOGREN A, HASSAN M M, et al. Improving risk assessment model of cyber security using fuzzy logic inference system [J]. Computers & Security, 2018, 74:323-339.

[5] DONG Gangsong, LI Wencui, WANG Shiwen, et al. The Assessment Method of Network Security Situation Based on Improved BP Neural Network [C]// International Conference on Computer Engineering and Networks. Cham, Springe, 2018:67-76.

[6] WEN Zhicheng, CAO Chunli, ZHOU Hao. Network security situation assessment method based on Naive Bayes classifier [J]. Journal of Computer Applications, 2015, 8: 12.

[7] HU Jingjing, MA Dongyan, LIU Chen, et al. Network Security Situation Prediction Based on MR-SVM [J]. IEEE Access, 2019, 7: 130937-130945.

[8] HODO E, BELLEKENS X, HAMILTON A, et al. Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey [J]. arXiv preprint arXiv, 2017, 1701.02145.

[9] ALTHUBITI S A, JONES E M, ROY K. LSTM for Anomaly-Based Network Intrusion Detection [C]// 2018 28th International Telecommunication Networks and Applications Conference. ITNAC, 2018: 1-3.

[10] JAVAID A, NIYAZ Q, SUN Weiqing, et al. A deep learning approach for network intrusion detection system [C]// 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), 2016: 21-26.

[11] HINTON G E, SALAKHUTDINOV R R. Reducing the dimensionality of data with neural networks [J]. science, 2006, 313.5786: 504-507.

[12] BALA R. A REVIEW ON KDD CUP99 AND NSL-KDD DATASET [J]. International Journal of Advanced Research in Computer Science.2019, 10(2): 64.

[13] CHAWLA N V, BOWYER K W, HALL L O, et al. SMOTE: Synthetic Minority Over-sampling Technique [J]. Journal of Artificial Intelligence Research, 2002, 16(1): 321-357.

[14] Common Vulnerability Scoring System v3.0: Specification Document, last accessed 2020/06/22. https://www.first.org/cvss/specification-document.

[15] 国务院. 国家突发公共事件总体应急预案[M]. 北京: 中国法制出版社, 2006.
State Council: The State Council of the People's Republic of China. Overall Emergency Plans for National Sudden Public Incidents. China Lesgal Press, Beijing (2006).