文章编号:1671-4598(2020)02-0058-05 DOI:10.16526/j.cnki.11—4762/tp.2020.02.012 中图分类号:TP393.0 文献标识码:A

基于 Adam—BNDNN 的网络入侵检测模型

何梦乙，覃仁超，刘建兰，熊 健，唐风扬
(西南科技大学 计算机科学与技术学院，四川 绵阳 621010)

摘要：针对传统入侵检测算法检测精度低、误报率高等问题，提出了一种融合批量规范化和深度神经网络的网络入侵检测模型；该模型首先在深度神经网络隐藏层添加批量规范化层，优化隐藏层的输出结果，然后采用 Adam 自适应梯度下降优化算法对 BNDNN 参数进行自动优化，提高模型检测能力；并使用 NSL—KDD 数据集进行仿真实验，结果表明该模型的检测效果优于 SNN、KNN、DNN 等检测方法；整体检测率可达 99.41%，整体误报率为 0.59%，证明了模型的可行性。

关键词：入侵检测；深度神经网络；批量规范化；NSL 数据集

Network intrusion Detection Model Based on Adam—BNDNN

He Mengyi，Qin Renchao，Liu Jianlan，Xiong Jian，Tang Fengyang
(School of Computer Science and Technology，Southwest University of Science and Technology，Mianyang 621010，China)

Abstract：Aiming at the problems of low detection accuracy and high false alarm rate of traditional intrusion detection algorithm，a network intrusion detection model combining batch normalization and deep neural network is proposed. Firstly，a batch normalization layer is added to the hidden layer of the deep neural network to optimize the output of the hidden layer，and then the adaptive gradient descent optimization algorithm of Adam is used to optimize the parameters of BNDNN automatically to improve the detection ability of the model. The simulation experiment with NSL—KDD data set shows that the detection effect of the model is better than shallow neural network (SNN)，k—Nearest Neighbor (KNN)，deep neural network (DNN) and other detection methods；The overall detection rate is 99.41%，and the overall false alarm rate is 0.59%，which proves the feasibility of the model.

Keywords：intrusion detection；deep neural network；batch normalization；NSL—kdd dataset

0 引言

入侵检测系统（intrusion detection system，IDS）是计算机网络中一种主动防御的成果，它为人类工作和生活提供安全保护。此前，许多学者提出了一些典型的 IDS；文献[1]结合改进的 KNN 和 Kmeans 实现 I2K 用于入侵检测，结果表明该算法具备良好的检测率和新攻击识别能力，但检测速度仍有待提升；文献[2]提出一种结合多目标优化理论的克隆选择算法，其能有效改善种群进化效率，增加种群多样性，进而提高检测率，但对于样本容量较大时，检测效率仍然比较低；文献[3]先用信息增益（IG）对网络数据进行特征提取，再用主成分分析（PCA）进行数据降维，最后用 Naive Bayes 来完成入侵分类检测，该方法虽然检测率高于 KPCA、FPCA、PCA—LDA，但并未提高对各攻击的检测率。文献[4]使用自适应 SSO 的分组过滤方法来完成入侵检测，虽然在不降低网络安全性的前提下，能有效减轻基于签名的入侵检测系统的负担，但在黑名单分组过滤签名匹配时还是消耗了较多时间。

随着大数据时代到来，网络数据的数量增多、格式多变、网络入侵行为多样化等，传统网络入侵检测模型面临着检测精度低、误报率高等问题。而近年来深度学习的兴起，基于深度学习的 IDS 也慢慢开始得到应用。文献[5]利用独热编码对网络包进行编码形成二维数据，再用 GoogLeNet 进行特征提取并训练 Softmax 分类器，其在检测精度、漏检率和误检率等都有很大提升；文献[6]结合深度学习理论和神经网络的极限学习机，提出一种自编码器—极限学习机入侵检测模型；用 MODBUS 数据集进行仿真实验，结果表明其优于 SVM、ELM、DBN、MLP、K—Means，符合网络入侵检测“高精度，低误报率”的检测要求。而本文结合 DNN 优异的特征学习能力、BN 的规范化数据处理和 Adam 自适应梯度优化方法，提出了一种基于 Adam—BNDNN 的入侵检测模型。

1 DNN 概述

深层神经网络（deep neural network，DNN）属第三代人工神经网络，它具有 1 个输入层，1 个输出层和 n 个隐含层，结构如图 1 所示，在数据量大的情况下可以计算得更快，花费更少的代价[7]。

DNN 同样和分为前向和后向。首先对权值 W 和阈值 b 进行初始化，前向时数据通过预处理后从输入层经 n 个隐

收稿日期:2019-11-29； **修回日期**:2019-12-19。
基金项目:国防基础科研计划项目(JCKY2017404C004)；四川省教育厅(17zd1119)；四川省教育厅(18sxb022)；四川省组织部(17sjjg02)。

作者简介:何梦乙(1995-)，女，四川珙县人，硕士研究生，主要从事信息安全相关方向的研究。
覃仁超(1978-)，男，四川武胜人，博士，副教授，主要从事网络安全技术及应用、计算智能相关方向的研究。

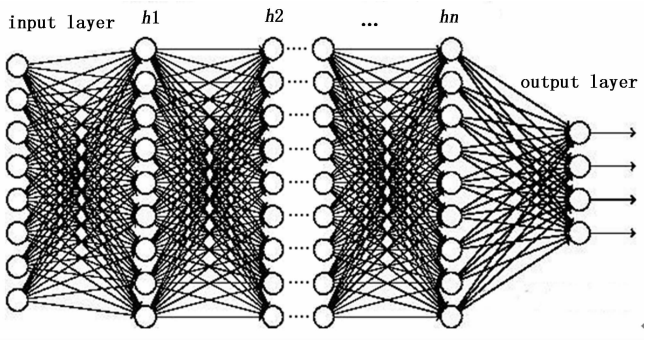

图 1　DNN 网络结构图

含层计算后传入输出层，输出层激活后的输出结果与期望结果进行对比得到误差，误差再以梯度下降的方式从输出层经隐含层回传至输入层，以此便完成了一轮神经网络的训练。

1.1　He 初始化权值

初始化时一般将阈值 b 初始化为 0，传统神经网络权值初始化常用初始化为 0 和随机初始化，但 W 初始化为 0 会出现每一层的学习能力相同，因而整个网络的学习能力也有限；而随机初始化实质上是一个均值为 0 方差为 1 高斯分布，若神经网络层数增加，则会出现后面层激活函数的输出值接近 0，进而可能产生梯度消失。

而现在常用的权值初始化有 Xavier 初始化、He 初始化等。Xavier 初始化中输入和输出都被控制在一定范围内，激活函数的值都尽量远离 0，则不会出现梯度过小的问题，公式如式（1）：

$$W_{ij} = U[-\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}] \tag{1}$$

但是 Xavier 对于激活函数 ReLU 不太适合，在更深层的 ReLU 中，激活函数的输出明显接近 0，所以 Xavier 一般用于 Sigmiod 和 Tanh。

而 He 初始化的出现解决了 ReLU 的问题，此方法基本思想是正向传播时，激活值方差不产生变化，回传时，激活值梯度方差不产生变化；对于 ReLU 和 Leaky ReLU 有不同的初始化方法，ReLU 适用于公式（2），Leaky ReLU 适用于公式（3），本文采用的便是基于 ReLU 的 He 初始化方法。

$$W = N\left[0, \sqrt{\frac{2}{n_i}}\right] \tag{2}$$

$$W = N\left[0, \sqrt{\frac{2}{(1+a^2)\, n_i}}\right] \tag{3}$$

1.2　ReLU 和 Softmax 激活函数

激活函数的选择会对模型收敛速度、训练时间产生非常大的影响。之前常用的激活函数有 Sigmoid 以及 Tanh，Sigmoid 将输出结果规约到 0～1 之间，Tanh 规约到－1～1 之间，在隐层中相较而言 Tanh 要优于 Sigmoid，因为 Tanh 的均值为 0，关于原点对称，具有对称性；但两者在训练时都容易造成两端饱和使得导数趋于零，以致权重无法更新最终造成梯度消失；而 RuLU 左边是抑制的，右边是有梯度的，一般不会造成梯度消失，因为神经网络的输入数据一般都大于 0；且 RuLU 具有更快的计算速度和收敛速度，因此隐藏层使用 RuLU 比前两者更好。3 种激活函数的输出图像如图 2 所示。

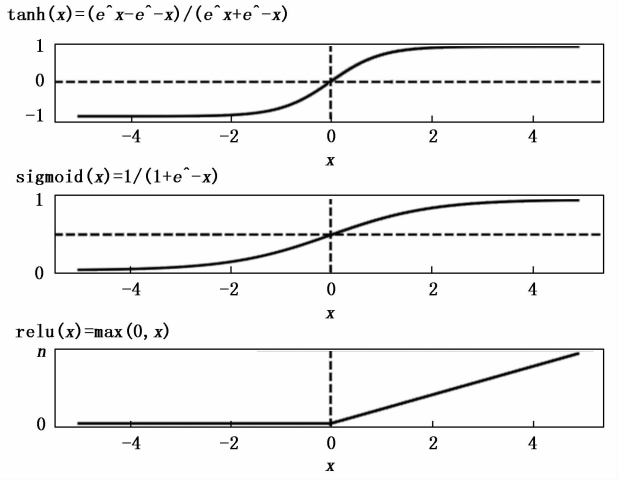

图 2　Sigmoid－Tanh－Softmax 函数图像

输出层通常采用 Sigmoid 函数或 Softmax 函数将输出层的输出结果归约到 0～1 之间，如公式（4）和（5）：

$$f(x) = \frac{L}{1+e^{-k(x-x_0)}} \tag{4}$$

$$\sigma(z)_j = \frac{e^{zj}}{\sum_{k=1}^{K} e^z k} \tag{5}$$

其中，Sigmoid 将输出层每一个输出节点的结果归约到 0～1 之间，故输出节点间的输出结果相互是独立的，且总和可能为 1 可能不为 1；而 Softmax 输出层中每一个输出节点的结果是相互紧密关联的，其概率的总和永远为 1。由于本模型采用 One－hot 来编码分类结果，在输出层时选用 Softmax 分类器较为方便。

1.3　Mini－batch 梯度下降

神经网络以梯度下降的方式来更新参数。在参数更新中，若使用整个数据集进行梯度下降，W 和 b 每次更新都在整个数据集一次训练完以后，这样可能不利于鲁棒性收敛，有可能造成局部最优；如果一次只用 1 个样本进行训练，W 和 b 更新太频繁，整个训练的过程也会很长。

而介于两者之间的 Mini－batch，把整个数据集随机分为 Mini－batch 的 Size 大小，W 和 b 更新是在每个小批量后，且每次小批量训练的数据更具有随机性，这样可以使得模型梯度下降参数更新更快，避免局部最优，同时加速模型的训练。

2　模型设计

2.1　Adam－BNDNN 的检测模型

本文检测模型主要分 3 个模块，结构如图 3 所示。

数据获取和预处理模块：获取网络数据集，并对其进行特征提取、数值转换、数据归一化等预处理操作，使其

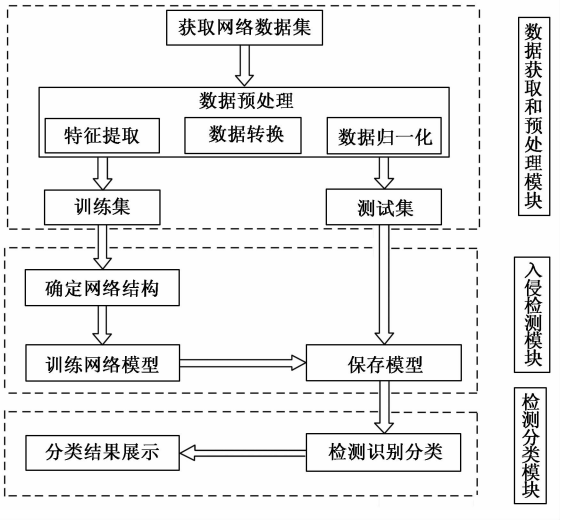

图 3 基于 Adam－BNDNN 的入侵检测模型

满足输入数据的要求；并将其分为训练集和测试集，分别用于模型训练和模型测试。

入侵检测模块：结合预处理后数据的维度确定 Adam－BNDNN 网络的输入输出节点，再根据隐层和其他参数从而确定整个网络结构和训练参数，用训练集对模型进行训练，完成训练后保存模型用于测试。

检测分类模块：测试集使用保存的模型进行测试，并将检测分类结果展示给用户。

2.2 BN 批量规范化优化

Batch Normalization[8]（BN）是近些年以来深度学习的一个重要发现，其应用在隐藏层，经常同 Mini－batch 一起使用。主要将每个隐层的输出结果进行归一化处理再进入下一个隐层，但并不是简单的归一化，而是进行变换重构，引入 λ、β 这 2 个可学习的参数，如公式（6）：

$$y^{(k)} = \gamma^{(k)x(k)} + \beta^{(k)} \tag{6}$$

引入参数后，网络即可学习出原始网络所需的特征信息；BN 操作如图 4 所示。

批量规范化（BN）操作流程：

1）数据先从输入层输入，经隐含层激活计算后得到激活值。

2）对隐含层激活值做批量规范化可以理解成在隐层后加入了一个 BN 操作层，这个操作先让激活值变成了均值为 0，方差为 1 的正态分布，即将其归约到 0～1 之间，最后用 γ 和 β 进行尺度变换和偏移得到网络的特征信息。

3）数据完成 BN 后再进入下一隐层。

BN 的使用降低了初始化要求，可使用较大学习率，也使神经网络的隐含层增强了相互间的独立性，同时增大了反向传播的梯度，进而避免了梯度消失的问题；且和 Dropout 一样具有防过拟合的正则化效果。

2.3 Adam 梯度下降优化

神经网络传统的随机梯度下降（SGD）缺点是很难选择一个比较合适的学习率，同时收敛速度也很慢，且容易

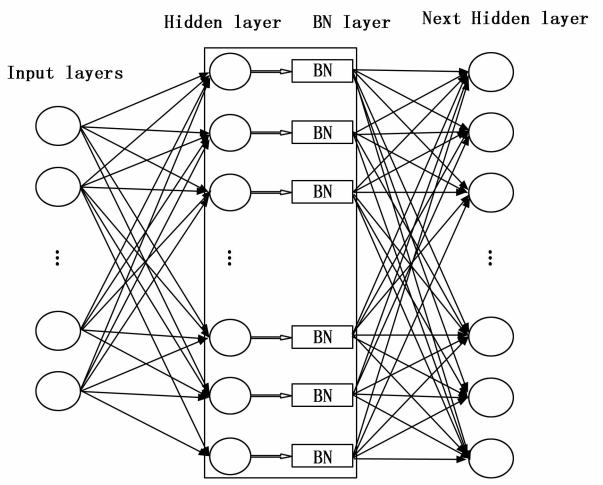

图 4 BN 操作结构图

达到局部最优。而以梯度下降为基础的 Adam 优化算法[9]，结合了 RMSProp 优化算法和 Momentum 优化算法。

RMSProp 中神经网络在训练时可自动调整学习率，不用过多的人为调整；而 Momentum 则是调整梯度方向，使得在训练时加速梯度下降的速度，从而加快训练过程。参数更新如公式（7）：

$$w_t = w_{t-1} - \alpha * \frac{\hat{m}_t}{\sqrt{\hat{v}_t} + \varepsilon} \tag{7}$$

式中，$\hat{m}_t$ 和 $\hat{v}_t$ 分别是动量 m_t 和速度 v_t 的更新，如公式（8）：

$$\hat{m}_t = \frac{m_t}{1-\beta_1^t}$$

$$\hat{v}_t = \frac{v_t}{1-\beta_2^t} \tag{8}$$

其中：α、β_1、β_2、ε 都有缺省值，也可以自行调整。

2.4 L2 正则化

在网络的训练过程中若数据过少或者训练过度则可能会产生过拟合现象，而正则化可以在学习中降低模型的复杂度，从而避免过拟合。正则化实质在损失函数中添加了正则项，对损失函数的参数做一些限制；一般有 L1 和 L2 正则化，本文选用 L2 正则化，L2 正则化对 b 更新无影响，对 w 更新有影响；拿逻辑回归为例，公式如（9）所示：

$$l = l_0 + \frac{\lambda}{2m}\sum_w w^2 \tag{9}$$

其中：l_0 为原始代价，m 为样本总数，系数 $\frac{1}{2}$ 是为了与求导产生的 2 相乘为整数而设置，λ 为正则参数，w^2 为权值的平方，$\frac{\lambda}{2m}\sum_w w^2$ 整体就是正则化。L2 正则化后 w 变小，模型的复杂度变低，使得抗干扰能力增强，进而在一定程度上避免过拟合。

3 数据集选取和处理

3.1 实验数据集选取

实验选取的是 NSL _ KDD 数据集[10]，它是 KDD CUP

数据的浓缩版，其在 KDD CUP 数据集的基础上进行的改进有：

1）KDD 中冗余数据的去除：使分类结果不会偏向更频繁的记录。

2）KDD 中重复数据的去除：使检测更加准确。

3）数据集大小更合理：KDD 共有 500 万左右条数据，数据总量多且冗余、重复数据多，可能会造成检测结果不理想以及训练时间过长。而 NSL 数据集总量 125973 条，正常和各异常数据占比也符合真实网络情况，用于训练的时间也不会太长。

NSL 一共有 41 维属性特征和 1 维标志特征，具体信息如表 1 所示。

表 1　NSL 数据的属性信息

属性号	属性名称
1－9	网络连接基本特征
10－22	网络连接的内容特征
23－31	基于时间的流量特征
32－41	基于主机的流量特征
42	标志特征

3.2　数据预处理

3.2.1　特征提取

在 NSL 数据集的 41 维属性特征中，每一维属性特征对结果的影响都是不一样的，为了合理选取网络数据的属性参数，文献[11]选取了 12 个属性特征，文献[12]选取了 14 个属性特征；文献[13]选取了 15 个属性特征；本文结合 2 种特征选取技术综合考量后最终选择 21 个最优特征属性，如表 2 所示。

表 2　NSL 数据集 21 个属性选取

特征选取	特征属性号
基于一致性评价	1,2,3,5,6,12,23,24,29,30,32,33,34,35,36,37,38,39,40
基于滤波	4,5,6,12,26,29,30,37
最终子集	1,2,3,4,5,6,12,23,24,26,29,30,32,33,34,35,36,37,38,39,40

3.2.2　数值化

21 维属性特征选取完以后，其中 Protocol type、Service、Flag 和 Label 是离散型数据，对离散型数据首先应数值化；

在 Protocol type 中，共有 Tcp、Udp、Icmp 三种协议类型，分别用数字 1、2、3 代替；

Service 中共有 70 种服务名称，分别用数字 1～70 代替；

Flag 中共有 11 种网络连接状态，分别用数字 1～11 代替；

最后是 Label 标志的数值化，Label 共有 5 种，分别标识 Nor、Pro、Dos、U2r、R2l，为了便于后面检测的分类工作，在数值化时使用 One－hot 进行编码，如 Normal 编码为 10000。

3.2.3　归一化

NSL 数据经数值化后，有些数值区间较大，各特征间差异也大，若不经处理就做输入数据，可能会使训练结果偏向更大的数，继而对训练速度和精度也会有一定的影响。为了避免上述情况发生，一般使用公式（10）将其归一化到 0～1 之间，

$$x_i^* = \frac{x_i - x_{\min}}{x_{\max} - x_{\min}} \tag{10}$$

归一化后一方面能提升模型收敛速度，另一方面提升模型的精度。

3.3　训练集和测试集的划分

NSL 数据进行预处理以后，随机取其 2/3 做训练集，剩下 1/3 做测试集，如表 3 所示。检测评价标准是 2 分类检测结果和 5 分类检测结果的准确率以及误报率。

表 3　训练集和测试集划分

数据集	Nor	Pro	Dos	U2r	R2l
训练集	44895	7771	30618	35	663
测试集	22448	3885	15309	17	332

4　实验与对比分析

4.1　实验参数选取

在数据预处理中选择 21 维属性特征，5 维 One－hot 编码标志特征，则 Adam－BNDNN 对应的输入为 21 个节点，输出为 5 个节点。

为了选择模型训练合适的 Epoch，以 3 隐层 Adam－BNDNN 网络 21－50－30－20－5 为例，选取总迭代次数 200 次，迭代 Epoch 和对应的代价 Loss 如图 5 所示。

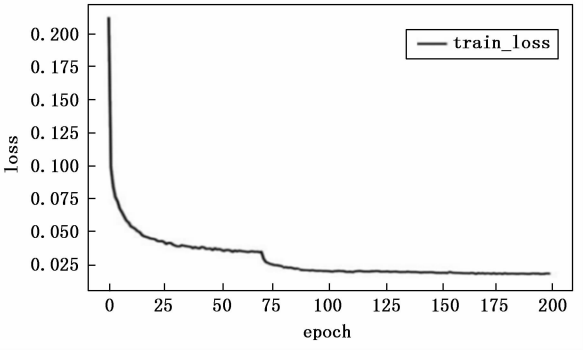

图 5　迭代 Epoch 和代价 Loss 曲线图

结果显示：在迭代 100 次以后，网络的训练代价趋于平缓。在迭代次数选取时，若迭代次数过少，则会造成训练不足，若迭代次数过多也有可能会造成过拟合。因此，在模型训练中，选取的迭代 Epoch 为 100 次。

接着是神经网络隐层数选择。为了选择合适的隐层数量，分别选取隐层数为 1～5 的 5 种不同网络结构 5 分类的平均准确率，网络结构如表 4 所示。

表 4 Adam－BNDNN 网络的不同隐层数结构

网络隐层数	网络结构
1	21－25－5
2	21－50－30－5
3	21－50－50－15－5
4	21－50－45－35－15－5
5	21－50－45－30－25－15－5

经实验得出，隐层数为 3 和 4 时整体检测率差不多，但 4 隐层时 U2r 和 R2l 的检测率低于 3 隐层，隐层数为 5 时精度大幅度下降，综合考量则最合适的隐层数为 3。

确定了网络的 Epoch 和网络结构后，Adam－BNDNN 所有参数设置如表 5 所示。

表 5 Adam－BNDNN 参数

参数名称	参数值
网络结构	21－50－50－15－5
初始化参数	权值:He 初始化,阈值:0
激活函数	Relu、Softmax
梯度下降	Mini－batch
正则化	Adam,BN,l2
学习率	0.001
学习率衰减	0.1
Mini－batch Size	64
Epoch	100 次

4.2 实验结果及分析

用 NSL－KDD 数据集仿真实验后，分别使用 2 分类检测结果和 5 分类检测结果的准确率以及误报率来评估模型的检测性能，结果如表 6 所示。

为了验证模型的检测效果，分别用浅层神经网络（SNN），K 最近邻（KNN），深层神经网络（DNN）、Alpha－OSELM[13]与本文做对比，2 分类结果如表 7 所示，5 分类结果如表 8 所示。

表 6 Adam－BNDNN 模型检测的分类结果 %

IDS	总检测率	正常检测率	异常检测				总误报率
			Pro 检测率	Dos 检测率	U2r 检测率	R2l 检测率	
2 分类	99.46	99.50	99.41				0.54
5 分类	99.41	99.50	99.05	99.63	35.29	90.06	0.59

表 7 各 IDS 的 2 分类结果 %

IDS	总检测率	正常检测率	异常检测率	总误报率
SNN	93.36	97.25	89.19	4.01
Alpha－OSELM	96.83	98.87	96.99	3.02
KNN	98.08	98.90	97.14	1.92
DNN	98.80	98.88	98.71	1.20
本文	99.46	99.50	99.41	0.54

表 8 各 IDS 的 5 分类结果 %

IDS	总检测率	正常检测率	Pro 检测率	Dos 检测率	U2r 检测率	R2l 检测率	总误报率
SNN	92.14	97.25	66.46	97.13	0.00	72.15	4.83
Alpha－OSELM	96.83	98.87	90.35	99.14	56.75	78.10	3.05
KNN	98.03	98.90	96.19	97.88	29.41	71.69	1.97
DNN	98.64	98.88	98.64	98.97	23.53	70.18	1.36
本文	99.41	99.50	99.05	99.63	35.29	90.06	0.59

从表 6 可以看出，2 分类的整体检测率要比 5 分类高，整体误报率要比 5 分类低。因为在 2 分类检测中，若类型为 R2l 的攻击误检为 U2l，对于 2 分类检测结果是正确的，但在 5 分类检测中则是错误的。

从表 7，表 8 可以看出本文检测模型的整体检测率要优于其他 IDS，整体误报率要低于其他 IDS。但 5 分类中 U2r 的检测结果并不是很好，主要因为在 125973 条样本数据中 U2r 只有 52 条，数据总量过于少，检测率没有其他 4 类高也是可以理解的；总体上证明了检测模型的可行性。

5 总结

针对传统入侵检测算法对网络入侵检测能力不足的问题，本文结合网络流量数据的特性，提出一个基于 Adam－BNDNN 的网络入侵检测模型，用属性简约后的 NSL－KDD 数据集来仿真实验，并与其他算法进行了对比分析，从而证明本模型的可行性。下一步工作将搭建真实网络环境，采集实时数据进行网络入侵检测。

参考文献：

[1] 张若楠，李红辉，张骏温. 一种融合改进 Kmeans 和 KNN 的网络入侵检测方法 [A]. 中国计算机用户协会网络应用分会，2018 年第二十二届网络新技术与应用年会 [C]. 2018.

[2] 范学林. 多目标免疫入侵检测策略研究 [D]. 哈尔滨：哈尔滨理工大学，2017.

[3] 王旭仁，马慧珍，冯安然，等. 基于信息增益与主成分分析的网络入侵检测方法 [J]. 计算机工程，2019 (6)：175－180.

[4] 陈惠娟，冯月春，赵雪青. 利用 SSO 的自适应黑名单分组过滤器网络入侵检测方法 [J]. 控制工程，2018 (10)：1940－1945.

[5] 梁 杰，陈嘉豪，张雪芹，等. 基于独热编码和卷积神经网络的异常检测 [J]. 清华大学学报：自然科学版，2019 (7)：523－529.

[6] 李 熠，李永忠. 基于自编码器和极限学习机的工业控制网络入侵检测算法 [J]. 南京理工大学学报（自然科学版），2019，43 (4)：408－413.

[7] 胡 越，罗东阳，花 奎，等. 关于深度学习的综述与讨论 [J]. 智能系统学报，2019，14 (1)：1－19.

[8] Ioffe S，Szegedy C. Batch normalization：accelerating deep network training by reducing internal covariate shift [A]. International Conference on International Conference on Machine Learning [C]. JMLR.org，2015.

(下转第 81 页)