基于循环神经网络的无线网络入侵检测分类模型构建与优化研究

陈红松*①② 陈京九①

①(北京科技大学计算机与通信工程学院 北京 100083)

②(材料领域知识工程北京市重点实验室 北京 100083)

摘 要：为提高无线网络入侵检测模型的综合性能，该文将循环神经网络(RNN)算法用于构建无线网络入侵检测分类模型。针对无线网络入侵检测训练数据样本分布不均衡导致分类模型出现过拟合的问题，在对原始数据进行清洗、转换、特征选择等预处理基础上，提出基于窗口的实例选择算法精简训练数据集。对攻击分类模型的网络结构、激活函数和可复用性进行综合优化实验，得到最终优化模型，分类准确率达到98.6699%，综合优化后的运行时间为9.13 s。与其他机器学习算法结果比较，该优化方法在分类准确率和执行效率两个方面取得了很好的效果，综合性能优于传统的入侵检测分类模型。

关键词：入侵检测；循环神经网络；实例选择；模型优化；实验验证

中图分类号：TP393.08; TP183 **文献标识码**：A **文章编号**：1009-5896(2019)06-1427-07

DOI: 10.11999/JEIT180691

Recurrent Neural Networks Based Wireless Network Intrusion Detection and Classification Model Construction and Optimization

CHEN Hongsong①② CHEN Jingjiu①

①(*School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing* 100083, *China*)

②(*Beijing Key Laboratory of Knowledge Engineering for Materials Science, Beijing*, 100083, *China*)

Abstract: In order to improve the comprehensive performance of the wireless network intrusion detection model, Recurrent Neural Network (RNN) algorithm is used to build a wireless network intrusion detection classification model. For the over-fitting problem of the classification model caused by the imbalance of training data samples distribution in wireless network intrusion detection, based on the pre-treatment of raw data cleaning, transformation, feature selection, etc., an instance selection algorithm based on window is proposed to refine the train data-set. The network structure, activation function and re-usability of the attack classification model are optimized experimentally, so the optimization model is obtained finally. The classification accuracy of the optimization model is 98.6699%, and the running time after the model reuse optimization is 9.13 s. Compared to other machine learning algorithms, the proposed approach achieves good results in classification accuracy and execution efficiency. The comprehensive performances of the proposed model are better than those of traditional intrusion detection model.

Key words: Intrusion detection; Recurrent Neural Network (RNN); Instance selection; Model optimization; experimental verification

1 引言

随着互联网的飞速发展，网络已经成为日常生活不可分割的一部分。互联网的使用改变了人们的生产生活方式。尤其是物联网在智能交通、智慧城市等方面的广泛应用，在极大方便生活的同时，使得各种安全威胁变得越来越严重。如何识别各种针对IEEE802.11协议[1]的网络攻击，对保证物联网安全具有十分重要的意义。入侵检测系统(Intrusion Detection System, IDS)是使用最广泛的用于识别各种类型攻击的工具，它可以识别正在发生的或者已经发生了的入侵。事实上，可将对无线网络的入

收稿日期：2018-07-10；改回日期：2019-01-07；网络出版：2019-01-18

*通信作者： 陈红松 chenhs@ustb.edu.cn

基金项目：国家重点研发计划(2018YFB0803400, 2018YFB0803403)，国家社科基金(18BGJ071)

Foundation Items: The National Key Research Development Program (2018YFB0803400, 2018YFB0803403), The National Social Science Foundation of China (18BGJ071)

侵检测转化成一个2分类或多分类问题，即识别网络流量是正常还是异常，或者识别网络流量是正常还是其它攻击中的一种。

Kolias等人[2]研发的爱琴海无线入侵数据集(Aegean WIFI Intrusion Dataset, AWID)是一种公开可用的易于分发的数据集，包含正常和入侵802.11无线网络的实际流量记录，目前国际上共有342家研究机构在使用该数据集[3]。著名的KDD'99为针对有线环境的数据集，该数据集主要用于传统的互联网安全研究，但该数据集发布距今已接近20年，不能反映最新的无线网络攻击技术。AWID数据集从专用WEP保护的802.11无线网络的实际使用中提取，利用metasploit, MDK3等工具，对网络进行了分片攻击(fragmentation)、断续攻击(chopchop)、解认证攻击(deauthenticaton)等15种攻击实验，并将其分为洪泛攻击(flooding)、伪装攻击(impersonation)和注入攻击(injection)3大类。洪泛攻击会造成每单位时间管理帧的突然增加，这种类型的攻击可能会导致服务不可用，也就是拒绝服务(Denial of Service, DoS)攻击。此类攻击通常针对特定客户端，或者试图耗尽网络资源(例如Access Point, AP)导致其中所有客户端的服务不可用。伪装攻击在邻域中引入额外的AP，广播预先存在的有效网络的信标帧，经常与短暂的解除认证帧相结合，以便攻击者可以强制受害者连接到自己的非法AP。这种类型的攻击可能会导致中间人攻击(man-in-the-middle)或密钥流(keystream)猜测攻击。注入攻击通常会导致大量小规模有效加密数据帧的泛滥。攻击者倾向于在很长一段时间内传输大量小数据帧，希望能够唤起网络的适当响应，用以对密钥或密钥流进行猜测攻击。

根据不同攻击的网络流量特征，可将该流量通过入侵检测模型进行分类。因此，针对入侵检测分类模型性能优化问题可转换为如何提高网络流量分类的准确率。近年来机器学习的流行使其被广泛用于识别各种类型的攻击，机器学习方法在一定程度上可以帮助网络管理员采取相应的措施来防止入侵。然而，大多数传统的机器学习方法属于浅层学习，不能有效地解决真实网络环境中出现大量入侵数据的分类问题。随着数据集的动态增长，多个分类任务的准确率也随之下降。相比之下，深度学习可从数据中提取不同特征的内在联系以创建更好的模型[4]，对数据序列的前后关联信息进行挖掘，实现序列数据的有效地处理。

Kolias等人利用AdaBoost, J48, Naive Bayes, Random Forest等机器学习算法对AWID数据集进行建模测试，其准确率为90%～96%，表现最佳的J48算法达到了96.2574%的准确率，花费时间568.92 s。Alotaibi和Elleithy[5]针对AWID数据集构建了一个基于误用的无线局域网入侵检测系统(Wireless Intrusion Detection System, WIDS)，测试了几种机器学习算法并利用多数投票技术将其组合起来，最终达到了96.32%的准确率，花费时间390 s，但也无法准确识别伪装攻击。Thing[6]针对AWID数据集利用栈式自动编码机深度学习方法提出了基于异常检测和分类的解决方案，通过调整激励函数来对网络进行优化，并最终获得了98.6688%的准确率，花费时间并未说明，虽然取得了较高的准确率，但实验过程并未提及所用的深度学习软件框架以及详细实验参数和步骤，所以其他研究人员很难重现其结果。Yin等人[7]对KDD'99有线网络攻击数据集提出了一种使用循环神经网络的入侵检测深度学习方法(RNN-IDS)并研究了模型在2元分类和多类分类中的表现，以及神经元的数量和不同学习速率对该模型性能的影响，为入侵检测提供了一种新的研究方法并获得了81.29%的准确率，花费时间11444 s，但是只针对有线网络建立检测模型，并未对无线网络入侵模型进行优化。陈红松等人[8]通过软件工程方法实现了用于内网用户异常行为分类的朴素贝叶斯算法。

通过对现状分析可知，深度学习有可能从数据中提取更好的特征表示以创建更好的模型。本文受循环神经网络启发，在隐含层引入了反馈机制，对时间序列数据的前后时间关联信息进行学习，实现时间序列数据的有效处理，本文提出一种基于循环神经网络的针对IEEE802.11无线网络环境的入侵检测分类模型，并通过实验进行验证和优化。

2 基于RNN的无线网络入侵检测预实验及问题描述

2.1 无线网络入侵检测数据预处理

通过对AWID数据集分析发现该数据集存在缺失、乱码和重复等问题，无法直接用于无线网络入侵检测模型的构建。为构建基于循环神经网络的IEEE802.11无线网络入侵检测系统，需对原始数据集进行数据清洗、数据变换、特征选择等预处理步骤。由于“脏数据”扭曲了原始数据信息内在的相关联系，严重影响数据分析和处理的运行效果。因此数据清洗时，需要利用自定义的清洗规则，手工或自动地将脏数据转换成满足数据质量要求的数据。数据清洗面对的主要问题是空缺值、错误数据、孤立点和噪声，解决方案是利用相同的常数填

补数据集缺失，将存在的特殊符号及乱码进行清空或替换处理。由于AWID数据集存在的154个特征中，既有数值数据，也有字符数据，而RNN的输入值应该是一个数值化矩阵，所以需要将数据标准化，数据变换时，对非数值化特征如“wlan.ra”、“wlan.da”等转化为数值形式。

由于一些特征字段不一定能够用于区分合法用户和攻击者的痕迹，一些信息可能会阻碍分类任务，特别是在由许多不同特征字段组成的分类问题中，提取重要特征在降低开销的同时甚至可以提高分类器的准确度，因此特征选择对于提高分类器精度和效率都是十分必要的。本文采用基于机器学习模型的特征选择算法，对AWID数据集中的154个特征及类别标签建立预测模型并利用extra tree算法从中选取20维重要特征，包括frame.len, wlan.sa, wep.iv, wlan.ta等重要特征，如表1所示。将处理后的训练集作为训练样本构造RNN-IDS入侵检测模型，并用测试集进行测试。

表 1　最重要的20维特征重要性得分

特征名	特征重要性得分	特征名	特征重要性得分
frame.len	0.8671	RA	0.6850
SA	0.7897	Subtype	0.6506
wep.iv	0.7764	type_sub	0.6373
TA	0.7587	reason_c	0.6327
wep.icv	0.7458	wep.key	0.6161
DA	0.7365	bssid	0.5971
DS	0.7283	Pwrmgt	0.5872
Duration	0.7135	type.cck	0.5866
RSS	0.7112	Protected	0.5865
Seq	0.7100	Datarate	0.5860

2.2　基于RNN的无线网络入侵检测分类模型预实验及问题描述

本文利用TensorFlow开源机器学习软件框架进行预实验，构造基于RNN的无线网络入侵检测分类模型，所设置参数包括输入层、中间层、输出层3层，神经元使用基本RNN单元，网络结构参数包括输入层节点20个、输出层节点4个、中间层节点20个，学习率0.001，采用该RNN分类模型对AWID训练集进行训练，得到无线网络入侵检测分类模型。使用训练得到的RNN模型对测试集进行测试，得到分类准确率为92.17%，并且随循环轮次的增加分类准确率无法继续提高。经过对原始测试集和预测结果统计发现，原始测试集中正常标签样本数，洪泛攻击标签样本数，伪装攻击标签样本数和注入攻击标签样本数分别为530785, 8097, 20079和16682，经模型预测输出交叉矩阵，发现分类器将所有测试样本的类别标签全部预测为正常，即分类器无法识别任何攻击类别。

经分析发现，产生上述问题的原因是AWID训练集中存在数据类别不均衡的问题，经统计正常标签样本与攻击标签样本数量的比值接近10:1，训练集中数据类别不均衡问题会导致分类器对正常标签类别产生过拟合，而对其他攻击标签类别产生欠拟合。在实际网络环境中，会出现持续的正常流量和异常流量，然而正常流量的比例会明显大于异常流量，此时若不对正常流量进行欠采样操作，训练集数据类别不均衡问题会导致分类器产生过拟合现象，从而使攻击检测失效。因此需要对训练数据集样本进行实例选择，通过欠采样操作适度减少正常标签样本的数量，消除训练集中数据类别的不均衡问题。

3　基于RNN的无线网络入侵检测模型的构建与优化

针对RNN模型对攻击类型无法有效识别、原始训练集样本类别不均衡等问题，本文提出无线网络入侵检测分类模型的构建与优化流程，如图1所示。

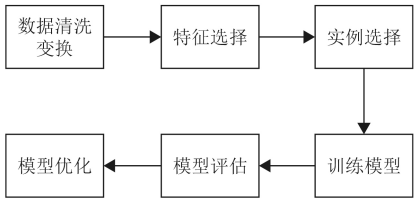

图 1 无线网络入侵检测分类模型的构建与优化流程

由图1可知，经过对AWID原始数据集进行数据清洗变换，特征选择等预处理，需要继续进行3.1节—3.4节的优化及处理。

3.1　实例选择

AWID-CLS-R-Trn训练集共包含1795575条记录，其中1633190条记录为正常流量，162385条为攻击流量。该数据集采集了无线网络1 h的数据，前45 min是没有攻击的，只有后15 min包含攻击。因此数据集的前部分大量出现了正常样本，从而导致RNN分类器对正常样本过拟合，无法识别后续样本的标签。而且对于RNN来讲，类别不均衡问题会导致分类器性能显著下降甚至完全丧失分类能力。因此需要对AWID训练数据集进行实例选择，从而有效抑制训练数据样本分布不均衡问题。本文针对AWID训练数据集中正常样本过多导致分类器过拟合问题，具体采用的方法是对于正常样本进行

欠采样操作。由于训练数据集是时间序列样本，采集的正常样本遍布整个采集周期，本文采用窗口的思想对数据进行欠采样。设样本空间$T=\{T_1, T_2, \cdots, T_n\}$，当前样本为$T_t$，正常样本为normal，基于窗口的实例选择算法SamSelect的伪代码如表2所示。

表 2 SamSelect伪代码

算法1 基于窗口的实例选择算法 SamSelect(D_A, w)

输入：AWID训练集D_A，窗口大小w

输出：采样后训练集D_B

(1) 初始化 正常样本计数器c=0
(2) for t=1 to $|D_A|$ do:
(3) If T_t = normal then:
(4) $c = c+1$
(5) if $c \le w$ then:
(6) 将当前样本放入D_B
(7) end if
(8) end if
(9) if $T_t \ne$ normal then:
(10) c=0
(11) 将当前样本放入D_B
(12) end if
(13) end for
(14) return D_B

窗口阈值与采样数据分布关系如表3所示，将在后续模型评估中通过实验进行选择合适的窗口阈值。

表 3 窗口阈值大小与采样数据分布表

样本标签数量	窗口阈值为5	窗口阈值为2
正常标签样本数量	368038	201007
攻击标签样本数量	162385	162385

3.2 训练模型

循环神经网络(Recurrent Neural Network, RNN)是一种随时间运行的神经网络[9]，适用于处理序列数据。RNN隐藏层之间的节点具有反馈机制，其输入不仅包括输入层的输入还包括上一时刻隐藏层的输出，实现上下文信息的传递，使得RNN具有处理序列数据的能力。展开的循环神经网络如图2所示。

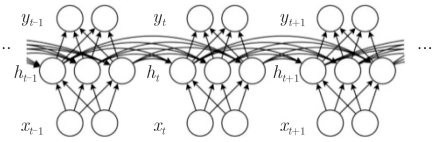

图 2 展开的循环神经网络

RNN神经元中的节点通过有向环和相应的权值连接，$\boldsymbol{x}$, $\boldsymbol{s}$, $\boldsymbol{o}$都是向量，分别代表输入层，隐藏层和输出层的值；$\boldsymbol{U}$, $\boldsymbol{V}$分别是输入层到隐藏层和隐藏层到输出层矩阵，$\boldsymbol{W}$是隐藏层上一时刻的值作为此时刻输入的权重矩阵。循环神经网络参数计算如图3所示。

网络在t时刻接收到输入x_t后，隐藏层的值是s_t，输出值是o_t。此时s_t的值由本时刻输入x_t和上一时刻隐藏层值s_{t-1}决定。计算方法为

$$o_t = g(\boldsymbol{V}s_t) \tag{1}$$

$$s_t = f(\boldsymbol{U}x_t + \boldsymbol{W}s_{t-1}) \tag{2}$$

其中g, f是激活函数。如果将式(2)反复代入式(1)中，可以得到式(3)

$$\begin{aligned} o_t &= g(\boldsymbol{V}s_t) \\ &= g(\boldsymbol{V}f(\boldsymbol{U}x_t + \boldsymbol{W}s_{t-1})) \\ &= g(\boldsymbol{V}f(\boldsymbol{U}x_t + \boldsymbol{W}f(\boldsymbol{U}x_{t-1} + \boldsymbol{W}s_{t-2}))) \\ &= g(\boldsymbol{V}f(\boldsymbol{U}x_t + \boldsymbol{W}f(\boldsymbol{U}x_{t-1} + \boldsymbol{W}f(\boldsymbol{U}x_{t-2} + \boldsymbol{W}s_{t-3})))) \\ &= g(\boldsymbol{V}f(\boldsymbol{U}x_t + \boldsymbol{W}f(\boldsymbol{U}x_{t-1} + \boldsymbol{W}f(\boldsymbol{U}x_{t-2} + \boldsymbol{W}f(\boldsymbol{U}x_{t-3} + \cdots))))) \end{aligned} \tag{3}$$

从上述推导可见RNN任意时刻输出，与之前时刻的输入均有关，这使得循环神经网络具有处理时序数据的能力。但RNN隐含层的输入会随时间的递推覆盖原有数据信息，导致上下文信息的缺失，产生梯度消失问题。

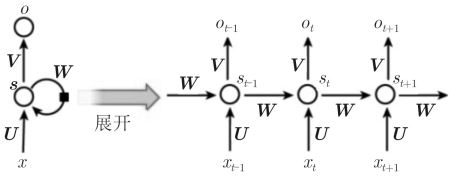

图 3 循环神经网络参数计算

本文采用TensorFlow开源机器学习框架[10]，利用前述约减后的数据集构造基于循环神经网络的无线网络入侵检测模型，使用基本RNN单元，网络参数为20个输入节点，4个输出节点，中间隐藏层1层，隐藏层节点20个，学习率0.001。本文训练模型核心代码如图4所示。

3.3 模型评估

本文实验网络结构参数为20个输入节点，4个输出节点，中间隐藏层节点为20个，学习率设置为0.001，循环轮次设置为300。分别测试了在实例选

择窗口大小分别为5, 2时的分类实验结果，如表4、表5所示。

AWID-CLS-R-Tst测试集共有575643条样本，其中正常标签流量样本530785条，洪泛攻击标签流量样本8097条，伪装攻击标签流量样本20079条，注入攻击标签流量样本16682条。其中伪装攻击标签流量包含咖啡拿铁攻击(Caffe Latte)、牧羊人攻击(Hirte)、邪恶双胞胎攻击(Evil Twin)、蜜罐(Honeypot)等小类攻击，而训练集中没有牧羊人攻击的样本，因此测试集属于牧羊人攻击的样本对于RNN分类器来讲属于新类，所以对其不具有识别能力，可以解释RNN分类器伪装攻击标签流量识别的召回率和准确率均较低的现象。

由表3、表4可见，窗口大小变小时，训练集正常标签流量样本数量变少，因此RNN对于正常标签流量的召回率有些许降低，但准确率有微弱提升；对于洪泛攻击标签流量的召回率有所提高，但准确率有轻微下降；对于伪装攻击标签流量的召回率有大幅提高，在窗口为5和2时均对其具有了一定的识别能力。而窗口大小对于注入攻击标签流量的识别基本没有影响。在时间方面，窗口为5, 2的RNN分类器进行300次循环消耗的时间分别是553.7 s和437.7 s。可见实例选择窗口为2时，RNN分类器能够在训练时间显著减少的同时保持分类能力，甚至可以提高对于伪装攻击标签流量样本的识别效果，因此窗口选为2。

```
n_inputs = 20
n_neurons = 20
n_outputs = 4
basic_cell = tf.contrib.rnn.BasicRNNCell(num_
units=n_neurons)
#隐藏层单元利用基本RNN单元，数量为20个
outputs, states = tf.nn.dynamic_rnn(basic_cell, X,
dtype=tf.float32)
#对隐藏层单元进行动态展开
logits = tf.layers.dense(states,n_outputs,name=
" softmax " )
xentropy = tf.nn.sparse_softmax_cross_
entropy_with_logits(labels=y, logits=logits)
loss = tf.reduce_mean(xentropy)
#计算预测值与真实值之间误差
optimizer = tf.train.AdamOptimizer(learning_
rate=learning_rate)
training_op = optimizer.minimize(loss)
#定义优化器，训练过程减小预测值与真实值之间的
误差
sess.run(training_op,feed_dict={X: X_batch, y:
y_batch})
#将训练集分批次进行训练
```

图 4 训练模型核心代码

表 4　窗口大小为5时的RNN分类预测实验结果报告

类别	精确率(%)	召回率(%)	*F*度量(%)	样本数
正常流量	95.93	99.11	97.49	530785
洪泛攻击流量	74.16	61.47	67.22	8097
伪装攻击流量	22.63	4.34	7.28	20079
注入攻击流量	99.80	99.99	99.90	16682

表 5　窗口大小为2时的RNN分类预测实验结果报告

类别	精确率(%)	召回率(%)	*F*度量(%)	样本数
正常流量	96.04	98.27	97.14	530785
洪泛攻击流量	69.31	66.26	67.75	8097
伪装攻击流量	15.95	6.40	9.14	20079
注入攻击流量	99.63	99.99	99.81	16682

3.4　模型优化

3.4.1　网络单元结构优化

长短时记忆网络(Long Short-Term Momery, LSTM)[11]是一种特殊的RNN类型，其区别于普通RNN的地方，主要就在于它在算法中放置了3扇门，分别叫做输入门(input gates)、遗忘门(forget gates)和输出门(output gates)，通过门结构的设计来避免梯度消失问题。门结构的存在可以让LSTM单元保存和获取长时间周期的上下文信息，LSTM单元内部结构如图5所示。

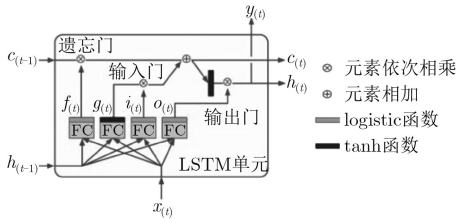

图 5 LSTM单元内部结构

门控循环单元(Gate Recurrent Unit, GRU)[12]可以视为LSTM的一种变体，GRU的结构更为简单，计算量也相对较小。GRU将LSTM中的遗忘门和输入门整合为一个更新门(update gates)，也就是将原来由3个门组成的细胞结构优化成两个门组成的细胞结构。重置门(reset gates)决定了如何将新的输入信息与前面的记忆相结合，更新门定义了前面记忆保存到当前时间步的量。如果将重置门设置为1，更新门设置为0，那么就得到标准RNN模型。

为达到更高的识别准确率，花费更少的时间，需对模型进行优化。网络结构优化效果对比如表6所示。

长短时记忆单元特有的门结构解决了传统循环神经网络时间维度的梯度消失问题，实现较大范围的上下文信息的保存与传输，提高了LSTM单元对具有长时间间隔相关性特点的序列信息的处理能力。由上述实验可知，LSTM在隐藏层数为两层，

表 6 网络单元结构优化效果对比

网络单元结构	隐藏层数	隐藏层节点	学习率	迭代轮数	时间(s)	准确率(%)
RNN	1	20	0.001	429	649.81	95.01
GRU	1	20	0.001	286	681.05	95.19
LSTM	1	20	0.001	277	663.50	95.19
LSTM	2	20	0.001	141	526.65	95.21
LSTM	3	20	0.001	145	545.47	95.14
LSTM	2	10	0.001	186	454.61	95.06
LSTM	2	30	0.001	175	988.17	95.00
LSTM	2	10	0.010	64	165.58	95.22
LSTM	2	10	0.020	86	205.83	95.27
LSTM	2	10	0.005	53	129.61	95.07

隐藏层节点为10个，学习率为0.005时，在不影响分类器准确率的同时达到了效率的提升。

3.4.2 激活函数选择

激活函数(activation function)是在人工神经网络的神经元上运行的函数，负责将神经元的输入映射到输出端。激活函数的主要作用是提供网络的非线性建模能力。每一种激活函数都有各自的优缺点，需通过实验选择最适合当前模型的激活函数。常见的激活函数有修正线性单元(Recitified Linear Unit, ReLU)函数、sigmoid函数、tanh函数和softmax函数等。在网络优化结构基础上，采用网络参数为LSTM神经元，隐藏层2层，隐藏层节点10个，学习率0.005。通过实验发现，ReLU获得了最高的准确率95.73%，且其时间也最低767.84 s。实验证明ReLU激活函数对于该数据集具有更好的拟合效果。

3.4.3 优化模型的复用

由于训练一个模型需要较长时间，且模型并不一定能每次都达到最为拟合数据的情况，因此tensorflow针对这一需求提供了Saver类，利用tensorflow中的Saver类对于本轮训练中的相关模型参数保存至checkpoints文件中。利用restore方法可以将保存的模型恢复，再对数据集进行测试，可达最优效果。为模型的迁移复用提供了便利。利用上述网络结构参数，对数据集进行了1000轮的学习测试，发现第579轮循环时得到了最优的模型结果，准确率达98.6699%，共耗时1717.00 s。将其模型保存后，利用restore方法读取并对测试集进行预测，准确率依然是98.6699%，但其所耗费的时间为9.13 s，大大提高了模型运行效率。

4 模型比较

本文利用处理后的数据集对于目前主流机器学习方法进行了训练测试，最后得到结果是K近邻(KNN)算法获得了最高的准确率95.87%，耗时528.84 s，而AdaBoost算法准确率最低为87.43%，耗时66.97 s。其余的算法如朴素贝叶斯(Naive Bayes, NB)、支持向量机(Support Vector Machine, SVM)、随机森林(Random Forest Classifier, RFC)、决策树(Decesion Tree, DT)、梯度提升(Gradient Boosting, GB)，分别获得了92.49%到95.14%之间不等的准确率，耗费时间跨度也从4.41 s到6757.97 s。与以上方法对比，本文所提RNN-LSTM算法获得了98.67%的准确率，时间为1717.00 s。但利用保存好的模型，时间可以缩短到10 s以内，效果好于传统机器学习模型。分类模型效果对比如表7、表8所示。

表 7 分类模型实验对比效果

算法名称	准确率(%)	时间(s)
KNN	95.87	528.84
SVM	94.92	6757.97
NB	92.49	4.41
RFC	93.27	7.93
DT	93.19	6.43
AdaBoost	87.43	66.97
GB	95.14	53.13
RNN-LSTM	98.67	1717.00
RNN-LSTM(复用优化)	98.67	9.13

表 8 与其他研究工作比较

文献	算法	准确率(%)	花费时间(s)	发表时间(年)
文献[2]	J48	96.26	568.92	2016
文献[5]	Voting	96.32	390	2016
文献[6]	SAE+PRelu	98.67	/	2017
文献[7]	RNN	81.29	11444	2017
本文	RNN-LSTM	98.67	9.13	2018

5　结论

针对无线网络AWID训练数据集样本不均衡所导致的分类器无法识别攻击类别问题，本文提出基于窗口的实例选择算法，适度减少训练集中正常标签样本数量，提升攻击标签样本比例，使训练数据集中各标签样本分布较均衡，解决训练数据集样本不均衡问题，使训练出的分类模型可有效识别攻击类别。通过进一步优化循环神经网络结构、激活函数、复用分类模型，使优化后的分类模型在提高准确率的同时提高分类器执行效率。采用AWID测试数据集对优化后的分类模型进行测试，模型分类预测的准确率达到了98.67%，花费时间9.13 s，综合性能优于其他分类模型。本文所提实例选择算法、网络结构优化、激活函数选择、模型复用等优化方法对基于循环神经网络的入侵检测分类模型构建及优化具有一定参考价值。

参 考 文 献

[1] CHEN Dong. A survey of IEEE 802.11 protocols: Comparison and prospective[C]. Proceedings of the 2017 5th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering, Chongqing, China, 2017: 589–598. doi: 10.2991/icmmcce-17.2017.106.

[2] KOLIAS C, KAMBOURAKIS G, STAVROU A, *et al*. Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset[J]. *IEEE Communications Surveys & Tutorials*, 2016, 18(1): 184–208. doi: 10.1109/COMST.2015.2402161.

[3] KOLIAS C and KAMBOURAKIS G. Organizations requested the dataset[EB/OL]. http://icsdweb.aegean.gr/awid/download.html, 2018.

[4] 白琮, 黄玲, 陈佳楠, 等. 面向大规模图像分类的深度卷积神经网络优化[J]. 软件学报, 2018, 29(4): 1029–1038. doi: 10.13328/j.cnki.jos.005404.

BAI Cong, HUANG Ling, CHEN Jianan, *et al*. Optimization of deep convolutional neural network for large scale image classification[J]. *Journal of Software*, 2018, 29(4): 1029–1038. doi: 10.13328/j.cnki.jos.005404.

[5] ALOTAIBI B and ELLEITHY K. A majority voting technique for wireless intrusion detection systems[C]. Proceedings of 2016 IEEE Long Island Systems, Applications and Technology Conference, New York, USA, 2016: 1–6. doi: 10.1109/LISAT.2016.7494133.

[6] THING V L L. IEEE 802.11 network anomaly detection and attack classification: a deep learning approach[C]. Proceedings of 2017 IEEE Wireless Communications and Networking Conference, San Francisco, USA, 2017: 1–6. doi: 10.1109/WCNC.2017.7925567.

[7] YIN Chuanlong, ZHU Yuefei, FEI Jinlong, *et al*. A deep learning approach for intrusion detection using recurrent neural networks[J]. *IEEE Access*, 2017, 5: 21954–21961. doi: 10.1109/ACCESS.2017.2762418.

[8] 陈红松, 王钢, 宋建林. 基于云计算入侵检测数据集的内网用户异常行为分类算法研究[J]. 信息网络安全, 2018, 18(3): 1–7. doi: 10.3969/j.issn.1671-1122.2018.03.001.

CHEN Hongsong, WANG Gang, and SONG Jianlin. Research on anomaly behavior classification algorithm of internal network user based on cloud computing intrusion detection data set[J]. *Netinfo Security*, 2018, 18(3): 1–7. doi: 10.3969/j.issn.1671-1122.2018.03.001.

[9] MARTENS J and SUTSKEVER I. Learning recurrent neural networks with hessian-free optimization[C]. Proceedings of the 20th International Conference on Machine Learning, Washington, USA, 2011: 1033–1040.

[10] ABADI M, BARHAM P, CHEN Zhifeng, *et al*. Tensorflow: a system for large-scale machine learning[C]. Proceedings of the 12th USENIX conference on Operating Systems Design and Implementation, Savannah, USA, 2016: 265–283.

[11] KIM J, KIM J, LE THI THU H, *et al*. Long short term memory recurrent neural network classifier for intrusion detection[C]. Proceedings of 2016 International Conference on Platform Technology and Service, Jeju, South Korea, 2016: 1–5. doi: 10.1109/PlatCon.2016.7456805.

[12] ZHOU Guobing, WU Jianxin, ZHANG Chenlin, *et al*. Minimal gated unit for recurrent neural networks[J]. *International Journal of Automation and Computing*, 2016, 13(3): 226–234. doi: 10.1007/s11633-016-1006-2.

陈红松：男，1977年生，副教授，研究方向为网络空间安全、大数据与机器学习算法应用、云计算与物联网安全.

陈京九：男，1994年生，硕士生，研究方向为网络空间安全.