Computer Science and Application 计算机科学与应用, 2021, 11(5), 1411-1418
Published Online May 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.115144

Hans汉斯

基于改进LSTM方法的安全态势感知模型研究

于春光[1]，孙远航[2]，李光耀[2*]，田春岐[2]

[1]中国航发上海商用航空发动机制造有限责任公司，上海
[2]同济大学电子与信息工程学院，上海
Email: *lgy423@126.com

收稿日期：2021年4月24日；录用日期：2021年5月19日；发布日期：2021年5月26日

摘　要

网络环境中的各种网络攻击行为给网络带来了很多挑战，导致网络故障和负载增加等突发网络安全事件发生的概率变大，网络安全预警的前提是安全态势。因此，针对网络安全态势的不确定性、波动性等特点，提出了改进的长短期记忆(LSTM)网络的安全态势感知模型。首先，针对神经网络训练过程中速度较慢和数据维度过高的问题，采用卷积神经网络进行降维，然后利用改进的循环神经网络进行预测态势值，最后通过计算均方根误差来评价模型的优势。通过仿真对比实验验证了改进的LSTM模型大大降低了模型预测误差，能够更加高效、准确地实现对网络态势的评估和预测。

关键词

态势感知，深度学习，卷积神经网络，LSTM，RNN

Research on Security Situation Awareness Model Based on Improved LSTM Method

Chunguang Yu[1], Yuanhang Sun[2], Guangyao Li[2*], Chunqi Tian[2]

[1]China Shanghai Commercial Aircraft Engine Manufacturing Co. Ltd. (AECC CAEM), Shanghai
[2]College of Electronics and Information Engineering, Tongji University, Shanghai
Email: *lgy423@126.com

Received: Apr. 24th, 2021; accepted: May 19th, 2021; published: May 26th, 2021

Abstract

Various network attack behaviors in the network environment have brought many challenges to

*通讯作者。

文章引用: 于春光, 孙远航, 李光耀, 田春岐. 基于改进 LSTM 方法的安全态势感知模型研究[J]. 计算机科学与应用, 2021, 11(5): 1411-1418. DOI: 10.12677/csa.2021.115144

the network, leading to increased probability of sudden network security incidents such as network failures and load increases. The prerequisite for network security early warning is the security situation. Therefore, in view of the uncertainty and volatility of the network security situation, an improved long short-term memory (LSTM) network security situation awareness model is proposed. First of all, in view of the slow speed and high dimensionality of the neural network training process, the convolutional neural network is used to reduce the dimension, then the improved recurrent neural network is used to predict the situation value, and finally the root mean square error is calculated to evaluate the model advantages. Simulation and comparison experiments verify that the improved LSTM model greatly reduces the model prediction error, and can more efficiently and accurately realize the evaluation and prediction of the network situation.

Keywords

Situational Awareness, Deep Learning, Convolutional Neural Network, LSTM, RNN

1. 引言

随着互联网的飞速发展和规模的不断扩大，各种各样的网络威胁攻击带来的风险也在不断上升。而现有的入侵检测、漏洞检测等安全技术只能对已发生的威胁攻击进行保护防御行为，缺少在宏观情况下了解网络安全态势的能力。由于网络数据具有动态、非线性和高噪声等特点，网络安全态势感知(Network Security Situation Awareness, NSSA)模型不仅要及时地感知网络态势的变化，还要对将来的网络态势进行推测，因此成为一项非常具有挑战性的工作。

随着机器学习算法的普遍应用，很多科研人员提出了安全态势感知模型，如贝叶斯方法、马尔可夫方法、神经网络等。但是，目前国内外对于网络安全态势感知的研究缺少权威的科学依据，也都还只是针对某一部分的内容进行研究，没有形成一个比较统一的标准，缺少整体化的研究思路，所以仍然需要进一步地研究探索。文献[1]提出基于贝叶斯方法的网络安全态势感知混合模型，通过分级模型的态势指标数据逐层融合进而得到安全态势指标，但是模型考虑的参数较少，容易产生数据误差。文献[2]构建了一种基于神经网络的安全态势感知模型，并采用自适应遗传算法对参数进行优化并感知网络态势，但该文的方法是否适合大规模的复杂网络仍有待研究。文献[3]提出了利用 D-S 证据理论构建网络安全态势感知模型，利用知识发现的方法实现网络安全图的自动生成，但缺少支持大规模网络安全态势感知的能力。

近几年的研究和发展，一方面深度学习在许多领域得到了广泛的应用，另一方面学者对于网络安全态势感知也有了比较明确的认识，并逐步将深度学习技术使用在网络安全态势评估与预测中。与传统的学习模型相比，深度神经网络可以通过分层特征分析复杂的非线性关系，具备更强大的学习能力，适合处理网络数据这种多因素影响、复杂的非线性问题。循环神经网络(Recurrent Neural Network, RNN)是一种建立在过去记忆基础上的特殊神经网络，其最大的优势在于网络可以记忆过去的内容。然而，由于 RNN 难以处理“梯度消失”问题，因此不适合用 RNN 去处理长序列数据。因此，Hochreiter 等人通过改进 RNN 网络单元结构进而提出了长短期记忆(Long Short-Term Memory, LSTM)模型[4]。针对态势要素提取不足，导致多源数据难以找出主要因素等问题，本文构建一种基于 LSTM 的安全态势感知模型，结合卷积神经网络(Convolutional Neural Networks, CNN)网络优化算法，提高了收敛速度，并且减少了模型训练的成本。

通过将典型的预测模型与改进的 LSTM 预测模型进行比较，验证了本文模型具有更好的预测精度。

2. 网络安全态势感知模型

网络安全态势感知目的是感知网络在安全运行、承担相应功能、提供服务过程中系统的安全状况，是一种多维度的安全防护手段。Tim Bass 等人最早提出了网络安全态势感知的初步模型，帮助管理者迅速发现、评估和定位网络攻击行为，并应用多传感器数据融合的网络空间态势感知框架[5]。目前学术界对网络安全态势感知模型大多从网络的不同角度、层面进行研究，采集到的数据如入侵检测系统(intrusion detection system, IDS)、漏洞信息后对数据信息进行糅合得出安全态势。

虽然网络安全态势感知的系统模型一直在改进变化，但是依然存在核心的三个层级。模型如图 1 所示，首先是态势感知层，主要是获取数据并进行融合；其次是态势状况层，主要是根据融合后的数据去建立态势感知模型，从而对当前网络安全的态势进行理解和评估；最后是态势预测层，主要是根据当前和历史时刻的网络安全态势，对未来的网络安全态势进行预测。

Figure 1. Schematic diagram of network security situation awareness model
图 1. 网络安全态势感知模型示意图

3. 基于改进的循环神经网络

为了验证本模型的可行性和优势，我们使用东北大学的 NEU-DET 数据集进行实验。

3.1. 循环神经网络

在传统的神经网络模型中，是从输入层到隐含层最后到输出层，相邻层之间的节点完全连接，而同一层的节点没有任何联系，由于节点之间需要相互交互，导致这种类型的网络模型在处理时间序列预测问题上性能欠佳。循环神经网络[6]利用带自反馈的神经元，用于处理序列数据的神经网络。RNN 中的隐藏单元可以接收到先前状态对当前状态的反馈。图 2 展示了一个基本的 RNN 架构。

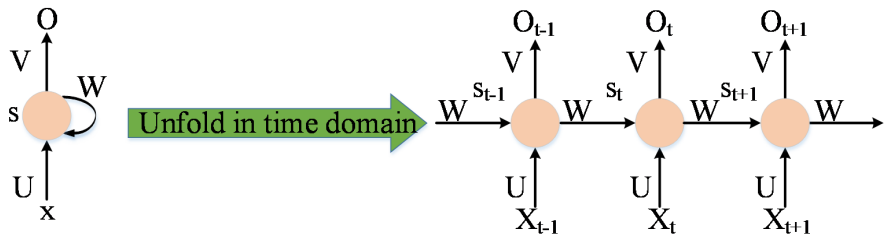

Figure 2. Structure of RNN
图 2. RNN 架构图

在这种结构中，输入向量逐次送入 RNN 中，而不像传统神经网络一样采用固定数量的输入方式，同时能够根据实际情况确定 RNN 的深度。最终的输出结果不仅受当前输入值的影响，还受先前隐藏层输出结果的影响。以下用数学模型表示：

$$\begin{aligned} t_i &= W_{hx}x_i + W_{hh}x_{i-1} + b_h \\ h_i &= \sigma(t_i) \\ s_i &= w_{oh}h_i + b_y \\ s_i &= w_{oh}h_i + b_y \end{aligned} \tag{1}$$

公式中 x_i 表示输入变量，W_{hx}、W_{hh} 和 W_{oh} 为权重矩阵，b_h 和 b_y 是偏差向量，σ 和 g 为 Sigmoid 函数，t_i、h_i 和 s_i 为临时变量，$\hat{o}$ 为输出变量。损失函数如下：

$$f = \sum_i \left(\left\| \hat{o}_i - o_i \right\| / 2 \right) \tag{2}$$

其中 o_i 表示真实输出。$t+1$ 处的输出由 $t+1$ 处的输入和历史数据共同决定。由于梯度的问题，RNN 模型的精度随时间的推移下降，最终导致输出误差较大。

但是随着时间的不断扩大会导致 RNN 的历史信息会逐渐递减，所以为了解决后面的时间节点对于前面时间节点感知力下降这个问题，引入了 LSTM [7]。

3.2. LSTM 模型

长短期记忆模型是 RNN 模型的一种变体，RNN 因为梯度消失的原因导致只有短期记忆，而 LSTM 模型通过将隐藏层作为记忆单元，通过门控制能够解决短期和长期时间序列的相关性问题。图 3 给出记忆单元的结构图，存储单元位于整个记忆单元的核心处，用红色圆圈表示。输入为已知数据，而输出则是预测的结果。在记忆单元中存在三个门，分别为输入门、遗忘门、输出门，通过绿色圆圈在图中标识。每个单元的状态用表示，每个门的输入由预处理数据和先前状态组成。蓝色点代表汇聚点，虚线是前一状态函数。以记忆单元中信息的流动为基础，状态的更新和输出可以归纳为公式(3)：

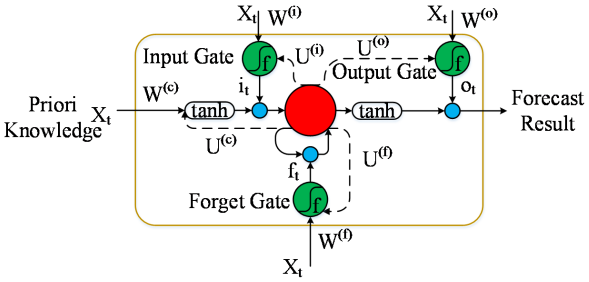

Figure 3. Design of the memory unit of LSTM
图 3. LSTM 记忆单元设计

$$\begin{aligned} i_t &= \sigma\left(W^{(i)}X_t + U^{(i)}S_{t-1}\right) \\ f_t &= \sigma\left(W^{(f)}X_t + U^{(f)}S_{t-1}\right) \\ o_t &= \sigma\left(W^{(o)}X_t + U^{(o)}S_{t-1}\right) \\ \tilde{S}_t &= \tanh\left(W^{(c)}X_t + U^{(c)}S_{t-1}\right) \\ S_t &= f_t \circ S_{t-1} + i_t \circ \tilde{S}_t \\ O_t &= o_t \circ \tanh(S_t) \end{aligned} \tag{3}$$

公式中的∘表示 Hadamard 乘积，i_t、f_t 和 o_t 表示三种不同的门，$\tilde{S}_t$ 为新状态的记忆单元，S_t 为最终状态的记忆单元，O_t 是最终输出的存储单元。$W^{(i)}$、$W^{(f)}$、$W^{(o)}$、$W^{(c)}$、$U^{(i)}$、$U^{(o)}$、$U^{(o)}$ 和 $U^{(c)}$ 为系数矩阵。

经由不同功能门后，LSTM 记忆单元可以捕获短期和长期时间序列中复杂的相关特性，相比 RNN 模型性能明显提高。

3.3. 基于改进的 LSTM 方法的 NSSA 模型

实该模型首先根据攻击影响提出一种态势指标评估因子，构建出网络安全态势评估指标体系，同时将改进的 LSTM 方法引入到网络安全态势评估之中，通过最终得到的影响指标对当前的网络安全态势进行态势评估，能够准确、高效地对网络当前状态进行评估。

3.3.1. 态势评估指标

对态势进行评估和预测的基础是构建科学合理的评估指标体系。在进行指标体系的构建要选择比较适中的指标因素，若选取的指标数量过大会使得评估模型结构复杂化，会降低整个评估过程的实时性和准确性；若选取的指标过少又反过来会加大评估结果的偶然性与随机性。本文根据以下原则来选取态势影响指标：

1) 层次性。层次性指的是所选取的指标能反应网络整体结构以及运行状况，各设备之间、传输数据信息所反映的信息有一定的差异性，要求尽可能地选取多层次、多方面的指标数据进行分析；

2) 系统性。系统性指的是所选取的指标能尽可能有一定的代表性与典型性等指标，网络安全的各个因素之间同时是相互关联、相互影响的，所以能够系统、全面的反应整个网络安全的整体状况；

3) 相似性。相似性指的是指标中会有功能近似并且相互之间会有影响的因素存在，会影响到网络安全的整体态势状态，这个因素也是在进行指标选取时候值得考虑的。

然后建立网络的层次性、系统性和相似性相结合的一级指标，并通过二级指标中的影响因素进行具体描述，具体的网络态势指标体系如下表 1 所示：

Table 1. Classification of situation indexes
表 1. 态势指标分类

一级指标	二级指标
层次性	cpu 占用率、网内流量变化率、带宽使用率、服务类型
系统性	主机操作系统、网络带宽、设备本身的版本、存储介质情况
相似性	网络漏洞等级、漏洞数目、攻击产生的后果

3.3.2. 态势评估等级划分

在构建态势评估指标体系后，通过结合国标 GB/T20984-2007 以及国家突发公共事件总体应急预案，本文将整体网络态势定义为 4 个评估类别，即安全、轻度危险、中度危险、重度危险四个等级。为了直观分析网络安全态势评估的结果，在[0,1]范围内对安全态势值进行量化。

Table 2. Network security situation level
表 2. 网络安全态势等级

安全系数	安全等级	网络运行状况
[0,0.2]	安全	正常
[0.2,0.5]	轻度危险	轻微影响
[0.5,0.8]	中度危险	较大影响
[0.8,1.0]	重度危险	严重事故

本文所用到的改进的循环神经网络[8] (C-LSTM)模型用于对网络安全态势值变化趋势的预测，C-LSTM 是由卷积神经网络和循环神经网络以线性结构串联组成的。由于 CNN 在提取空间特征上具有优势，因而通过它构建的滤波器能够通过对输入数据进行逐层卷积和池化操作来提取数据之间隐藏的特征。

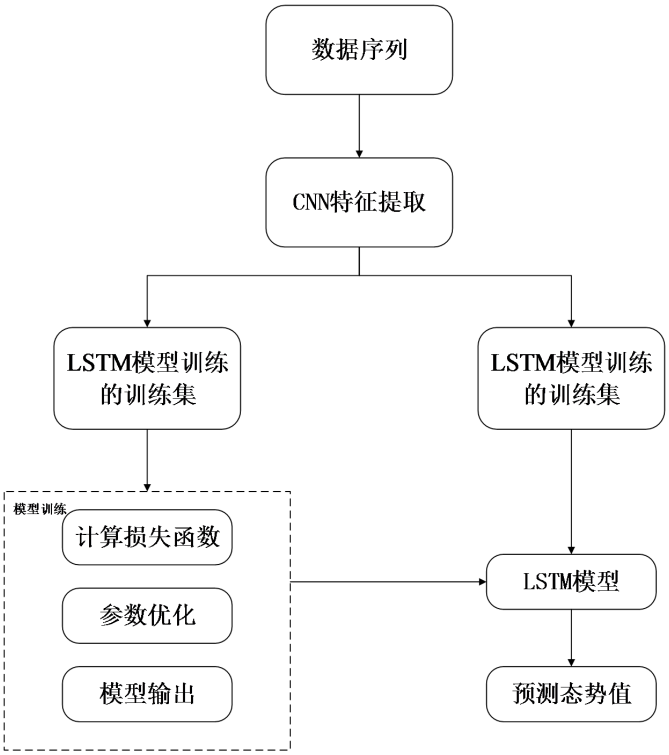

Figure 4. Situational awareness framework based on improved LSTM
图 4. 基于改进 LSTM 的态势感知框架

本文采用 LSTM 网络实现对态势值的预测，基于改进 LSTM 方法的网络安全态势感知模型构建的框架如图 4 所示。首先通过卷次神经网络来提取数据序列的特征，然后通过层次化安全态势评估量化方法进行量化计算得到安全态势值，并将其进行归一化，然后得到新的样本集当作 LSTM 网络的输入。在训练过程中，可以调节循环神经网络隐层节点的个数和时间序列的长度对模型的预测正确率进行调节，最后计算真实数据和预测数据的均方根误差判断模型的好坏。

Table 3. Identification types of KDD cup99
表 3. KDD Cup99 标识类型

威胁等级	攻击类型	网络运行状况
低	DoS	teardrop smurf pod. neptune land. back
较低	U2R	perl, loadmodule, buffer overflow, rootkit
中等	R2L	guess passwd, warezmaster, ftp write, imap，
较高	/	phf, multihop, warezclient, spy
高	Probing	Ipsweep, nmap, portsweep, satan

构建准确合理的网络安全评估指标体系是对态势进行感知的基础，所以在进行安全态势感知之前需要对网络安全态势之进行一定的量化。虽然态势指标的确定是模糊并且是一个逐渐改变的进程，本文创

新性的采用定性类别分析法来描述网络安全态势，赋予其有了可以具体量化的值，能够用于态势计算。根据网络的行为判断其受到的攻击类型以及所处的安全等级类别，在网络受到的攻击越大时，网络安全态势值相应就越高，因而通常情况网络威胁程度的判定是由主机权限以及网络攻击对通信性能的损害程度来决定的[9]。KDD Cup99 中的威胁等级及攻击类型如表 3 所示。

KDD Cup99 数据集的网络攻击主要包括 4 类，并对攻击类型进行威胁定值，在检测到该类网络攻击时，则对网络的攻击赋予相应的量化值，如表 4 所示。

Table 4. Quantified value of attack event
表 4. 攻击事件量化值

攻击类型	威胁值	事件
Normal	0	无
Proble	0.2	端口监测、扫描
R2L	0.4	非法尝试登陆主机
DoS	0.6	进行拒绝服务攻击
U2L	0.8	非法获取主机或管理员权限

在进行实验训练数据时，根据不同攻击类型确定网络威胁值，判断其存在于某个网络安全等级类别，则取表 2 中各类别的中间值作为网络安全态势值[10]。在数据集中提取出 100 条网络入侵检测数据，以“天”作为态势预测的时间尺度，得到 100 个归一化后的原始安全态势值作为样本集，用此样本集考察模型在时序上态势值的走势情况。首先将数据样本分为训练集和测试集，将前 74 个数据点成为训练集，用于构建模型和方法训练；后 26 个称为测试集，用于将预测结果和实际结果作对比。

本文采用的预测模型预测结果与原始安全态势值相比，如下图 5 所示：

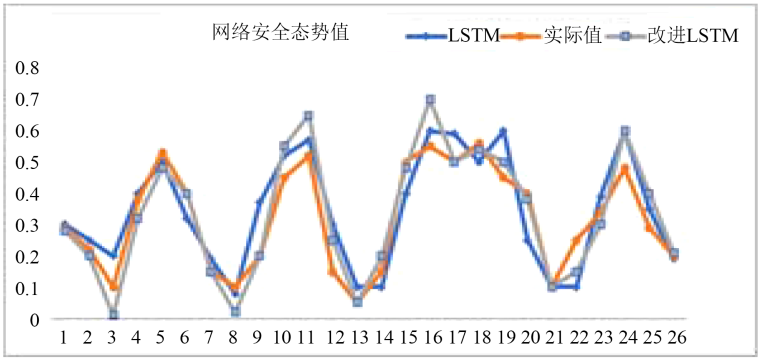

Figure 5. Situation value comparison
图 5. 安全态势值对比

为了更加直观的表现本文算法的可行性，采用平均相对误差(MRE)和均方根误差(RMSE)对预测结果进行评价：

$$\mathrm{MRE}=\frac{1}{N}\sum_{i=1}^{n}\left(\frac{\left|y_i'-y_i\right|}{y_i}\times 100\%\right) \tag{4}$$

$$\mathrm{RMSE}=\sqrt{\frac{\sum_{i=1}^{N}\left(y_i'-y_i\right)^2}{N}} \tag{5}$$

上式中，N 表示样本个数，y_i 表示预测态势值，y_i 表示实际态势值。在对模型精确度进行评价时，误差越小，则表示模型的精确度越好。结果如下表 5 所示：

Table 5. Error comparison of the prediction results of the two models
表 5. 两种模型预测结果的误差对比

模型名称	平均相对误差	均方根误差	样本数
本文模型	0.3082	0.7074	26
LSTM	0.4924	0.7351	26

4. 总结

本文以“天”作为态势预测的时间尺度，通过对网络安全状态进行分析，构建态势指标评估因子，实现对网络安全等级的分类，使用改进后的 LSTM 模型进行态势值的预测。实验表明相较于统计模型和其他预测模型，该方法能够更好地处理长时间序列不确定性的问题，为网络安全防范措施的调整、网络风险的预估等工作提供了一定的决策支持。该数据集虽然能够对提出的改进方法进行验证，但是不能很好地代表网络更加真实的环境数据。在未来的工作中，将构建更加完备的网络场景进行实验，验证本文所提出方法的稳定性。

基金项目

上海市工业互联网资助项目(2018-GYHLW-02043)；国家自然科学基金资助项目(61771346, 61772372)；上海市信息化发展专项资金(新一代信息基础设施建设)项目(201901010)。

参考文献

[1] 丁华东, 许华虎, 段然, 陈帆. 基于贝叶斯方法的网络安全态势感知模型[J]. 计算机工程, 2020, 46(6): 130-135.

[2] 谢丽霞, 王亚超, 于巾博. 基于神经网络的网络安全态势感知[J]. 清华大学学报(自然科学版), 2013, 53(12): 1750-1760.

[3] 王春雷, 方兰, 王东霞, 戴一奇. 基于知识发现的网络安全态势感知系统[J]. 计算机科学, 2012, 39(7): 11-17+24.

[4] Hochreiter, S. and Schmidhuber, J. (1997) Long Short-Term Memory. *Neural Computation*, **9**, 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735

[5] Bass, T. (2000) Intrusion Detection Systems and Multisensor Data Fusion: Create Cyberspace Situation Awareness. *Communications of the ACM*, **43**, 99-105. https://doi.org/10.1145/332051.332079

[6] Graves, A., Mohamed, A.R. and Hinton, G. (2003) Speech Recognition with Deep Recurrent Neural Networks. 2013 *IEEE International Conference on Acoustics, Speech and Signal Processing*, **38**, 6645-6649. .

[7] Graves, A. (2012) Long Short-Term Memory. Supervised Sequence Labelling with Recurrent Neural Networks. Springer Berlin Heidelberg, 1735-1780. https://doi.org/10.1007/978-3-642-24797-2_4

[8] Kim, T.Y. and Cho, S.B. (2018) Web Traffic Anomaly Detection Using C-LSTM Neural Networks. *Expert Systems with Applications*, **106**, 66-76. https://doi.org/10.1016/j.eswa.2018.04.004

[9] 王一村. 网络安全态势分析与预测方法研究[D]: [硕士学位论文]. 北京: 北京交通大学, 2015.

[10] 赵燕伟. 基于网络行为特征的网络安全态势研究[D]: [硕士学位论文]. 哈尔滨: 黑龙江大学, 2018.