刘嘉琪, 魏霖静. 基于 SSA-LSTM 的网络安全态势预测研究[J]. 智能计算机与应用,2025,15(11):158-163. DOI:10.20169/j.issn.2095-2163.24032202

基于 SSA-LSTM 的网络安全态势预测研究

刘嘉琪, 魏霖静
(甘肃农业大学 信息科学技术学院, 兰州 730070)

摘 要: 随着互联网应用的发展和普及,网络已从虚拟空间变成了现实社会不可缺少的重要组成部分,网络安全形势也日益严峻复杂。为减少网络安全风险的发生,本文提出一种基于 SSA-LSTM 的网络安全态势预测方法,利用长短期记忆网络的序列建模能力和麻雀搜索算法的全局搜索能力,在网络入侵数据的基础上建立网络安全态势预测模型;使用麻雀搜索算法对 LSTM 模型进行优化调参,相较于优化前的 LSTM 模型与 SVR 模型,优化后的 SSA-LSTM 网络安全态势预测模型拟合效果更好,在 MAE、MSE、RMSE 评价指标上的误差值最小,具有一定的可行性和优越性。

关键词: 网络安全态势; 预测; LSTM; 麻雀搜索算法
中图分类号: TP301.6 **文献标志码**: A **文章编号**: 2095-2163(2025)11-0158-06

Research on SSA-LSTM based network security posture prediction

LIU Jiaqi, WEI Linjing
(College of Information Science and Technology, Gansu Agricultural University, Lanzhou 730070, China)

Abstract: With the development and popularization of Internet applications, the network has turned from a virtual space into an indispensable and important part of the real society, and the network security situation has become increasingly severe and complex. In order to reduce the occurrence of network security risks, a network security posture prediction method based on SSA-LSTM is proposed, which is to establish a network security posture prediction model based on network intrusion data by using the sequence modeling capability of long and short-term memory network and the global search capability of sparrow search algorithm. The method uses the sparrow search algorithm to optimize and adjust the parameters of the LSTM model. Compared with the LSTM model and the SVR model before optimization, the optimized SSA-LSTM network security situation prediction model has a better fitting effect, and the error value in the evaluation indicators of MAE, MSE and RMSE is the smallest, which has certain feasibility and superiorit.

Key words: network security posture; prediction; LSTM; sparrow search algorithm

0 引 言

网络安全态势预测是目前态势感知中最重要的研究内容,网络环境日益复杂严峻,网络设备产生的数据大多无法共享,数量多且分散,因此使用时间序列对其进行研究,模型在预测过程中根据输出值结果与真实值的差值进行改进调整[1]。网络安全态势具有时序性的特点,因此选用长短期记忆神经网络进行处理,可以更好地预测将来一段时间内的网络安全态势值。与其他群智能算法相比,麻雀搜索算法具有较高的全局搜索能力和较快的收敛速度,求解精度高,具有很好的鲁棒性和自适应性,能够根据问题的特点自动调整搜索策略。因此,本文采取麻雀搜索算法对长短期记忆网络的参数进行优化,通过优化算法进行寻优,使其具有更高的准确性和客观性。

1 基于 SSA-LSTM 算法的网络安全态势评估模型

1.1 长短期记忆网络

长短期记忆网络(Long Short-Term Memory, LSTM)是一种特殊的循环神经网络,包括输入层、输

基金项目: 科技部国家外专项目(G2022042005L); 兰州市人才创新创业项目(2021-RC-47)。
作者简介: 刘嘉琪(1999—),女,硕士,主要研究方向:网络与信息安全。
通信作者: 魏霖静(1977—),女,博士,教授,硕士生导师,主要研究方向:智能计算,农业信息化,农业大数据。Email:916277964@qq.com。
收稿日期: 2024-03-22

出层和隐藏层，其中隐藏层中存在遗忘门，可将过去的信息随着时间的推移慢慢遗忘，相比于传统的 RNN ，在处理长序列数据时具有更好的表现[2-3]。LSTM 由多个相同结构的细胞单元格组成，每个细胞单元格又包含细胞单元状态和 3 个门（输入门、遗忘门和输出门）来控制信息的流动，输入门用来控制新信息的输入，决定哪些信息需要被加入到细胞状态中；遗忘门用来控制旧信息的遗忘，决定哪些信息需要从细胞状态中删除；输出门用来控制输出信息的选择，决定哪些信息需要被输出[4-5]。LSTM 模型如图 1 所示。

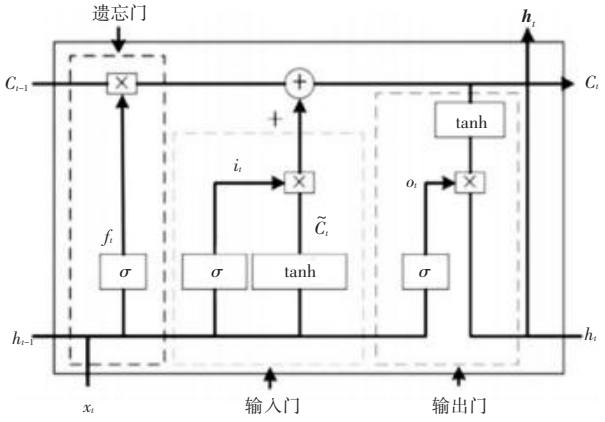

图 1　LSTM 模型示意图

Fig. 1　Schematic diagram of LSTM model

遗忘门根据输入信息的重要程度判断是否增加并长期保留信息状态：

$$f_t = \sigma(W[h_{t-1}, x_t] + b_f) \tag{1}$$

其中，f_t 为记忆衰减系数；σ 是激活函数；W_f 为权重系数；b_f 为偏置。

经过 Sigmoid 激活函数调整，查看 h_{t-1}（前一个输出）和 x_t（当前输入），并为单元格状态 C_{t-1}（上一个状态）中的每个数字在范围［0，1］中赋予输出值，其中“ 1 ”代表“信息完全保留”，“ 0 ”代表“信息完全删除”。输入门用来决定哪些新信息通过加权运算放在细胞状态里，首先经过 tanh 层得到目前信息，经过 Sigmoid 层确定更新哪些值，再与 tanh 层的输出相乘加入到细胞状态中，得到当前时刻细胞状态[6]：

$$i_t = \sigma(W_i \times [h_{t-1}, x_t] + b_i) \tag{2}$$

$$\tilde{C}_t = \tanh(W_c \times [h_{t-1}, x_t] + b_c) \tag{3}$$

$$C_t = f_t \times C_{t-1} + i_t \times \tilde{C}_t \tag{4}$$

其中，i 为输入门；W_i 为输入门权重系数；b_i 为输入门的偏置；C_{t-1} 为上一时刻的记忆；C_t 为 当前时刻的记忆。

输出门决定重要信息对于下层网络的保留程度，即此刻的输出状态。将单元格状态通过 tanh 将值规范化到 -1～1 之间，并将其乘以 Sigmoid 层的输出，即得到当前时刻的状态：

$$o_t = \sigma(W_o \times [h_{t-1}, x_t] + b_o) \tag{5}$$

$$\boldsymbol{h}_t = o_t \times \tanh(C_t) \tag{6}$$

其中，o 为输出门；W_o 为输出门权重系数；b_o 为输出门的偏置；$\boldsymbol{h}_t$ 为单元输出向量。

LSTM 引入门控机制，并且各公式中的加法计算解决了神经网络因子多项相乘带来的梯度爆炸和梯度消失等问题，相对于基础的 RNN 网络来说，LSTM 记忆能力更强，更擅长处理较长的序列信号数据[7-8]。

1.2　麻雀搜索算法

麻雀搜索算法（Sparrow Search Algorithm，SSA）是一种群体智能优化算法，其灵感源自麻雀种群的觅食和反捕食行为，并以发现者-加入者模型为基础，同时融入侦查预警机制[9-10]。为建立麻雀搜索算法的数学模型，可以采用一些基本的数学概念和模型来描述这些规则[11]。以下是对每个规则的抽象描述：

（1）发现者负责觅食，通常具有最多的能量储备，为其他个体提供方向和区域，每只麻雀个体的能量储备可以表示为一个适应度值的函数。这个函数可以是一个简单的映射，将适应度值映射到能量储备上。

（2）每只麻雀个体可以通过一个报警值来表示其发出的报警信号的强度，当报警值超过一定的安全值时，麻雀将采取行动以确保安全，可以建模为一个阈值函数，当报警值超过阈值时，触发一系列的行为，比如移动到安全区域。

（3）麻雀个体的身份可以用一个状态变量表示，这个状态可以根据某些条件来动态改变，比如当一个麻雀发现了更好的食物来源时，其可以成为发现者，而另一个麻雀则成为加入者。

（4）麻雀个体的能量水平可以影响其觅食位置，低能量的个体更有可能飞往其他地方觅食，而高能量的个体可能会停留在当前位置，可以建模为一个能量水平和觅食位置之间的概率分布。

（5）加入者总是能够搜索到提供最好食物的发现者，可以建模为一个概率分布，表示加入者搜索到发现者的概率，可能受到距离和其他因素的影响。

（6）种群中会选择一定比例的麻雀（通常占麻雀种群总数的 10%～20%）进行侦查预警，麻雀在意识到危险时会采取不同的行为，例如向安全区域移动或者随机移动，可以建模为一个行为选择的过程，可能受到危险程度和其他因素的影响。

从数学角度,由 n 只麻雀组成的种群可表示为:

$$X = \begin{bmatrix} x_1^1 & x_1^2 & \cdots & x_1^d \\ x_2^1 & x_2^2 & \cdots & x_2^d \\ \cdots & \cdots & \cdots & \cdots \\ x_n^1 & x_n^2 & \cdots & x_n^d \end{bmatrix} \tag{7}$$

所有麻雀的适应度值可以表示为:

$$F_x = \begin{bmatrix} f([x_1^1 \quad x_1^2 \quad \cdots \quad x_1^d]) \\ f([x_2^1 \quad x_2^2 \quad \cdots \quad x_2^d]) \\ f([\cdots \quad \cdots \quad \cdots \quad \cdots]) \\ f([x_n^1 \quad x_n^2 \quad \cdots \quad x_n^d]) \end{bmatrix} \tag{8}$$

在算法中,发现者具有全局导向的能力,负责为整个种群寻找食物,需要具备更广泛的觅食搜索范围。由此发现者的位置更新表述为:

$$X_{i,j}^{t+1} = \begin{cases} X_{i,j}^t \cdot \exp\left(-\dfrac{i}{\alpha \cdot \text{iter}_{\max}}\right), & \text{if } R_2 < \text{ST} \\ X_{i,j}^t + Q \cdot \boldsymbol{L}, & \text{if } R_2 \geqslant \text{ST} \end{cases} \tag{9}$$

其中,α 和 Q 为随机数,且 $\alpha \in (0,1]$,$\boldsymbol{L}$ 为元素均为1的矩阵,$R_2 \in [0,1]$ 和 $\text{ST} \in [0.5,1]$ 分别表示预警值和安全值。

当 $R_2 < \text{ST}$ 时表示环境安全,发现者可以自由搜索;当 $R_2 \geqslant \text{ST}$ 时表示危险出现,某些麻雀会发出警报提醒种群中其它麻雀,在这种情况下,所有麻雀都会马上离开危险地区,飞往安全区域[12]。

除发现者外的其他所有麻雀均被定义为加入者。加入者的位置更新表述为:

$$X_{i,j}^{t+1} = \begin{cases} Q \cdot \exp\left(\dfrac{X_{\text{worst}}^t - X_{i,j}^t}{i^2}\right), & \text{if } i > \dfrac{n}{2} \\ X_P^{t+1} + \left|X_{i,j}^t - X_P^{t+1}\right| \cdot A^+ \cdot L, & \text{otherwise} \end{cases} \tag{10}$$

其中,X_{worst}^t 为第 t 次迭代中最差的个体,A^+ 公式为:

$$A^+ = A^{\mathrm{T}}(AA^{\mathrm{T}})^{-1} \tag{11}$$

当 $i > \dfrac{n}{2}$ 时,表明第 i 个加入者极度饥饿,即需飞往别处来获取更多食物;当 $i \leqslant \dfrac{n}{2}$ 时,表明在当前最优位置附近随机找到一处位置,且每一维距离最优位置方差较小,值较为稳定[13]。

在麻雀种群中,具备警戒机制的麻雀位置是随机分布的,麻雀种群位置更新为:

$$X_{i,j}^{t+1} = \begin{cases} X_{\text{best}}^t + \beta \cdot \left|X_{i,j}^t - X_{\text{best}}^t\right|, & \text{if } f_i > f_g \\ X_{i,j}^t + K \cdot \left(\dfrac{\left|X_{i,j}^t - X_{\text{worst}}^t\right|}{(f_i - f_w) + \varepsilon}\right), & \text{if } f_i = f_g \end{cases} \tag{12}$$

其中,β 为步长控制参数,$K \in [-1,1]$。

当麻雀个体适应度值大于当前全局最佳适应度值时,表示麻雀正处于种群的边缘,极易成为捕食者的攻击目标;当麻雀个体适应度值等于当前全局最佳适应度值时,表明处于种群中间的麻雀感受到捕食者出现,需要靠近其它麻雀以此尽量减少自身被捕食的风险[14]。

根据上述步骤得到的麻雀搜索算法的伪代码见表1。

表 1 麻雀搜索算法的伪代码流程

Table 1 Pseudo code execution flow of the SSA algorithm

SSA 搜索算法
输入:
G:最大迭代次数
PD:生产者的数量
SD:察觉到危险的麻雀的数量
R_2:告警值
n:麻雀的数量
初始化 n 只麻雀的种群并定义其相关参数。
输出: X_{best}, f_q
1:while ($t < G$)
2:对适应度值进行排序,找出当前最佳个体和当前最差个体;
3: $R_2 = \text{rand}(1)$
4:for $i = 1 : PD$
5: 利用公式(1-9)更新麻雀的位置;
6:end for
7:for $i = (PD + 1) : n$
8: 利用公式(1-10)更新麻雀的位置;
9:end for
10:for $i = 1 : SD$
11: 利用公式(1-12)更新麻雀的位置;
12:end for
13: 获取当前的新位置;
14: ;如果新位置比以前更好,则更新;
15: $t = t + 1$
16:end while
17:return X_{best}, f_q.

1.3 构建基于 SSA-LSTM 的网络安全态势预测模型

由于网络安全数据集生成的态势值具有非线性和随机性的特点,而 LSTM 神经网络又具有较好的时间序列数据处理能力,所以选用 LSTM 神经网络来进行网络安全态势预测。态势预测技术具有极其重要的作用,能够在网络未来的某一时刻之前,准确预知安全状态,使管理员能够预先采取措施,有效防范和化解潜在的安全风险,确保网络的稳定运行,不仅提升了网络管理的效率和准确性,也大幅增强了网络安全防护的主动性和前瞻性。

LSTM 神经网络模型中存在许多超参数，其性能和评估准确性在一定程度上受到超参数的影响，而麻雀搜索算法具有较强的全局搜索能力，可以消除 LSTM 参数选取上的主观性因素，使用麻雀搜索算法对 LSTM 的超参数进行优化，如学习率、迭代次数、dropout 比例、隐藏层节点数等，适应度函数选用均方误差(MSE)。算法通过每轮迭代更新麻雀种群的位置，结合目标函数，即神经网络的精度，并根据一定的策略，如预警者、加入者等进行位置调整，不断搜索最优的超参数组合，直至达到最大迭代次数或满足停止条件为止。此模型的优化过程基本步骤如下：

(1)使用 KDD99 数据集，整理数据集，进行数据预处理，若数据存在缺失值则对其进行填补，之后执行归一化处理，使其值处于(0,1)之间，数据归一化公式如下：

$$x_i^{'} = \frac{x_i - x_{\mathrm{m}}}{x_{\mathrm{M}} - x_{\mathrm{m}}} \tag{13}$$

其中，$x_i^{'}$ 为归一化后的数据值；x_i 为原始数据值；x_{M} 为样本数据的最大值；x_{m} 为样本数据的最小值。

KDD99 数据集共包含 4 种攻击类型的数据，并依照国家互联网应急中心的划分标准对网络安全态势各攻击类型赋予等级，对各等级分别赋予不同权重值，设置的权值与其对网络安全的影响成正比，即权值越小，影响程度越小，网络越安全。各等级的权值见表 2 。

表 2　各等级及权重

Table 2　Levels and weights

等级	优	良	中	差	危
权值	0	0.1	0.2	0.3	0.4

网络安全态势值选择使用加权聚合的方式计算[15]：

$$S = \sum_{n=1}^{k} w_i l_i \tag{14}$$

其中，k 表示计算使用的数据量，w_i 为某一等级的权重，当网络数据等级为优时 l_i 取值为 0 ，当等级为其他 4 种时 l_i 取值为 1 。

得到态势值 S 后，使用下式对其进行归一化处理，使归一化后的态势值 $\mathrm{SA} \in [0,1]$：

$$\mathrm{SA} = y_m + \frac{y_M - y_m}{x_M - x_m}(x_i - x_{\mathrm{m}}) \tag{15}$$

其中，x_i 表示当前的态势值；x_{m} 和 x_{M} 表示态势值的最小值与最大值；y_m 和 y_{M} 表示归一化后区间的最小值与最大值。

将计算出的态势值 SA 区间与 5 种风险等级分别对应，当 $\mathrm{SA} \in [0,0.2]$ 时，态势等级为优；当 $\mathrm{SA} \in [0.21,0.4]$ 时，态势等级为良；当 $\mathrm{SA} \in [0.41,0.75]$ 时，态势等级为中；当 $\mathrm{SA} \in [0.76,0.90]$ 时，态势等级为差；当 $\mathrm{SA} \in (0.9,1]$ 时，态势等级为危。

滑动时间窗口算法(Sliding Time Window Algorithm)是一种用于处理实时数据流的算法[16]。采用滑动时间窗口构造样本集，将网络安全态势数据从一维变成多维，使用过去 5 个时间段的数据来预测第 6 个时间段的数据，多维态势数据集建构见表 3。

表 3　数据集建构

Table 3　Data set construction

数据输入	数据输出
x_1, x_2, x_3, x_4, x_5	x_6
$x_6, x_7, x_8, x_9, x_{10}$	x_{11}
$x_{11}, x_{12}, x_{13}, x_{14}, x_{15}$	x_{16}
…	…
$x_{n-5}, x_{n-4}, x_{n-3}, . x_{n-2}, x_{n-1}$	n

(2)利用参数如种群规模、维度、最大迭代次数等初始化一群虚拟麻雀的个体位置和适应度，选取 LSTM 模型的关键超参数作为优化对象；

(3)对种群中每个麻雀按照适应度值进行排序，找到目前具有最优适应度和最差适应度的个体；使用训练集进行模型训练，在迭代过程中，使用 Adam 和 RMSprop 优化器优化 LSTM 的参数；

(4)根据上述公式(9)~(11)更新 3 种角色的位置，保留每次迭代过程中适应度最高的个体，并更新全局最优适应度值；

(5)重复步骤(3)~(4)，直至满足算法停止条件，保存算法寻找到的最优参数，最终确定网络安全态势评估模型。

构建的 SSA-LSTM 模型流程图如图 2 所示。

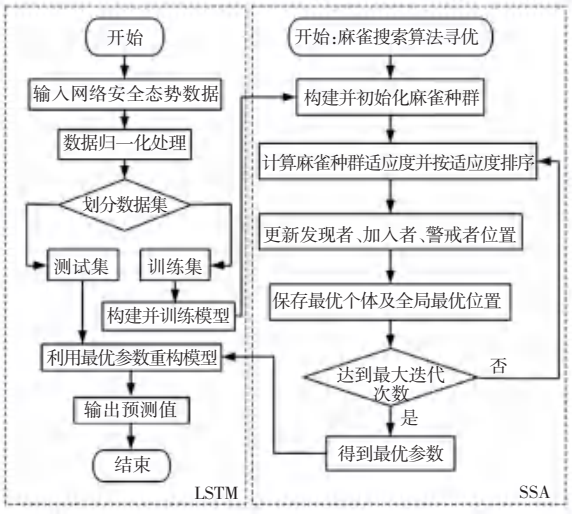

图 2　SSA-LSTM 模型流程图

Fig. 2　Flow chart of SSA-LSTM model

2 实验分析

2.1 实验环境及数据

实验计算机为 Windows 10 操作系统,64 位,8 核 CPU 内存,仿真软件为 pycharm,python3.7 环境搭建。本文采用 KDD99 数据集中的训练子集。KDD99 数据集是一个用来从正常连接中监测非正常连接的公开数据集,具有广泛性和权威性[17-18]。设置使用一定数据量生成一个网络安全态势值,共得到 3 000 个态势值,取其中一部分态势值结果进行可视化,如图 3 所示,数据峰值越大,代表此刻的网络状况越危险。

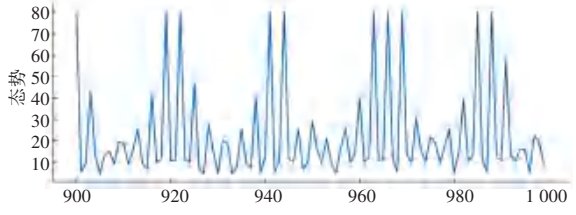

图 3 部分态势值序列

Fig. 3 Part of the status value sequence

2.2 参数设置

使用过去 5 个时间段的数据预测下一个时间段的数据,因此将 LSTM 模型的输入层节点个数设置为 5 ,输出层节点个数设置为 1 ,其他超参数设置见表 4。

表 4 LSTM 神经网络超参数设置

Table 4 LSTM neural network hyperparameter settings

超参数	上界(UP)	下界(DOWN)
Batch_size	32	8
Dropout	0.5	0.05
第一隐藏层节点数	500	350
第二隐藏层节点数	350	200

将经过预处理的数据代入模型中,使用麻雀搜索算法对 LSTM 模型超参数进行优化,其参数设置见表 5。

表 5 SSA 算法参数设置

Table 5 SSA algorithm parameter settings

参数	设置值
多维数组维度(n_dim)	4
种群大小(pop_size)	22
最大迭代次数(Max_iter)	128
下界(lb)	DOWN
上界(ub)	UP

2.3 模型评价指标

为了评价模型的预测能力,本文选取以下 3 种指标对模型预测效果进行定量评价。

(1)平均绝对误差(Mean Absolute Error,MAE):是回归分析中常用的一种拟合优度评价准则,是预测值与实际值之差的绝对值的平均数:

$$\mathrm{MAE} = \frac{1}{n}\sum_{i=1}^{n} | x_i - x_i' | \tag{16}$$

(2)均方误差(Mean Squared Error,MSE):是真实值与预测值的差值的平方和然后求平均:

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n} (x_i - x_i')^2 \tag{17}$$

(3)均方根误差(Root Mean Squared Error,RMSE):又被称为标准误差,衡量预测值与真实值之间的均方根差异:

$$\mathrm{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n} (x_i - x_i')^2} \tag{18}$$

其中,n 为样本个数;x_i 表示真实态势值;x_i' 代表模型预测出的态势值。

与均方误差相比,RMSE 对较大的误差更加敏感,因此当预测中存在异常值时,RMSE 可能会产生较大的波动。

以上评价指标的值越小,说明预测值与真实值之间偏差越小,模型预测精度越高。

2.4 结果分析

由 SSA 算法优化后,得出 LSTM 模型最优化的参数,第一隐藏层 468 个神经元,第二隐藏层 212 个神经元,dropout 比例为 0.24 ,Batch_size 值为 18。为了验证 SSA-LSTM 网络安全态势预测模型的准确性,分别选取 LSTM 模型和支持向量回归(Support Vector Regression,SVR)模型与 SSA-LSTM 模型进行对比试验,一部分预测结果如图 4 所示。

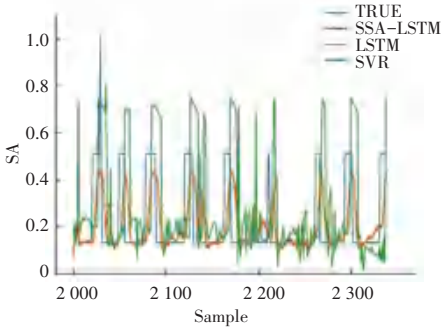

图 4 不同预测模型态势值对比

Fig. 4 Comparison of situation values of different prediction models

通过图中的实验结果对比可知，SSA-LSTM 模型的预测能力优于 LSTM 模型及 SVR 模型，能够准确预测出网络安全态势数据的大致趋势走向，拟合效果较好。

根据 3 种评价指标，计算出 3 种模型预测值与真实值的误差，结果见表 6。

表 6　3 种模型预测误差对比

Table 6　Comparison of prediction errors of the three models

预测模型	MAE	MSE	RMSE
SVR	3.104 9	4.733 9	3.518 2
LSTM	2.794 1	4.429 6	3.366 1
SSA-LSTM	**2.733 4**	**4.392 5**	**3.347 5**

从表 6 中可以看出 SSA-LSTM 模型在 3 种评价指标上的误差值均最小。SSA-LSTM 模型比 LSTM 模型、SVR 模型在 MAE 评价指标上的误差分别降低 2.17%、11.96%；在 MSE 评价指标上的误差分别降低 0.84%、7.21%；在 RMSE 评价指标上的误差分别降低 0.55%、4.85%。由于模型的评价指标值越小，预测效果越好，所以综合评定得出，SSA-LSTM 模型与 LSTM 模型、SVR 模型相比，预测效果相对较好。因此，本文提出的基于 SSA-LSTM 的网络安全态势预测模型具有一定的研究意义和可行性。

3　结束语

网络安全态势预测是目前网络安全重点关注的话题。针对当前国内外网络威胁不断增加这一现状进行分析，本文深入分析了网络安全态势预测中使用的 LSTM 模型，由于预设参数对于实验结果具有显著影响，可能导致模型收敛性较慢、效率低下以及泛化能力弱等问题。为了克服这些不足，本文采用麻雀搜索算法对 LSTM 模型进行优化，通过智能搜索全局最优参数，得到了一个更加准确、收敛性更强的 SSA-LSTM 模型。实验结果表明，本文提出的 SSA-LSTM 模型使用 MAE、MSE、RMSE 评价指标时误差值均最小，相比于 LSTM 模型和 SVR 模型，具有更好的预测能力，证明了 SSA-LSTM 网络安全态势预测模型具有一定可行性和优势，为网络安全态势预测提供了更为可靠的支持。

参考文献

[1] 孙理理. 网络安全治理对策研究[J]. 信息网络安全，2023，23(6)：104-110.

[2] 田园，孙梦觉，周植高，等. 一种基于信息熵的 LSTM 时间序列数据预测模型[J]. 科技创新与应用，2024，14(7)：28-34.

[3] 郑圣彬，谢加良，张东晓. 基于 LSTM-WGAN 的时间序列数据异常检测[J]. 福建师范大学学报(自然科学版)，2024，40(2)：36-45.

[4] 朱江，陈森. 基于 NAWL-ILSTM 的网络安全态势预测方法[J]. 计算机科学，2019，46(10)：161-166.

[5] 唐清苇，向月，代佳琨，等. 基于 CNN - LSTM 的风电场发电功率迁移预测方法[J]. 工程科学与技术，2024，56(2)：91-99.

[6] 苏小玉，董兆伟，孙立辉，等. 基于强化 LSTM 的网络安全态势预测方法[J]. 计算机技术与发展，2021，31(7)：127-133.

[7] 刘微. 基于 LSTM 神经网络的网络安全态势预测的应用研究[D]. 上海：上海应用技术大学，2020.

[8] 李麟，王伟. 基于改进 RNN 多源融合算法的网络异构信息集成管理系统[J]. 西安工程大学学报，2023，37(6)：145-152.

[9] 兰永青，乔元栋，程虹铭，等. 基于 SSA-LSTM 的瓦斯浓度预测模型[J]. 工矿自动化，2024，50(2)：90-97.

[10] 曹还君，李长云. 基于 SSA-LSTM 模型的空气质量预测研究[J]. 现代信息科技，2024，8(4)：142-146.

[11] 李江华，王鹏晖，李伟. 一种混合多策略改进的麻雀搜索算法[J]. 计算机工程与科学，2024，46(2)：303-315.

[12] 欧阳城添，朱东林. 融合 K-means 的多策略改进麻雀搜索算法研究[J]. 电光与控制，2021，28(12)：11-16.

[13] 翁嘉诚，周晓杰，叶蓓蕾，等. 基于改进麻雀搜索算法的 K-means 聚类[J]. 数学的实践与认识，2024，54(2)：152-166.

[14] 王浩，陈婷，陈兴侯，等. 基于改进 SSA-BP 神经网络的复烤水分和温度预测[J]. 农业与技术，2022，42(6)：18-25.

[15] 宋国顺. 基于特征加权聚合的传感网络多模式攻击检测方法[J]. 通化师范学院学报，2023，44(10)：74-80.

[16] 冉华明. 基于滑动时间窗的机载传感器多任务调度算法[J]. 北京航空航天大学学报，2025，51(9)：2968-2978，DOI：10.13700/J.BH.1001-5965 2023.0488.

[17] ELKAN C. Results of the KDD99 classifier learning[J]. ACM SIGK-DD Explorations Newsletter，2000，1(2)：63-64.

[18] 余华鸿，周凤艳，陈毛毛. 基于机器学习的 KDDCUP99 网络入侵检测数据集的分析[J]. 计算机工程与科学，2019，41(S1)：91-97.