文章编号:1671-4598(2025)02-0063-08 DOI:10.16526/j.cnki.11-4762/tp.2025.02.009 中图分类号:TP393 文献标识码:A

基于改进 LSTM 的网络入侵检测方法

黄 亮,陶 达,王秀木,刘静闻,刘也凡
(辽宁省地震局,沈阳 110031)

摘要:随着网络数据的增加,以及黑客技术的不断发展,网络入侵检测技术的精度以及效率需要进一步提升;针对此问题,提出一种基于逃避网络数据和改进长短时记忆网络的网络入侵检测模型;该模型将黑客入侵过程中产生的异常数据作为训练集和测试集;之后利用麻雀优化算法改进长短时记忆网络模型,并将其与卷积神经网络结合,通过强化学习进一步提升模型的检测精度;实验结果表明,基于改进长短时记忆网络的入侵检测模型的检测准确率达到了 98.51%,且响应时间仅为 0.84 s,漏报率和误报率分别为 1.23%和 0.36%;该网络入侵检测模型能够实现高效的网络入侵检测,实时保障网络安全,实现网络入侵防御,为网络安全提供可靠的技术支持;该方法在网络攻防领域具有积极意义,为相关领域研究提供了新的思路。

关键词:逃避行为;网络入侵;检测;LSTM;SSA 算法;CNN;强化学习

Network Intrusion Detection Method Based on Improved LSTM

HUANG Liang, TAO Da, WANG Xiumu, LIU Jingwen, LIU Yefan
(Seismological Bureau of Liaoning Province, Shenyang 110031, China)

Abstract: With the increase of network data and the continuous development of hacker technology, network intrusion detection technology needs to further improve its accuracy and efficiency. To address this issue, a network intrusion detection model based on evading network data and improving long short-term memory (LSTM) network is proposed. This model uses the abnormal data generated during the hacker intrusion process as the training and testing sets. Afterwards, sparrow optimization algorithm (SSA) is used to improve the LSTM network model, which is combined with convolutional neural network (CNN) to further enhance the detection accuracy of the model through reinforcement learning. Experimental results show that the detection accuracy of the intrusion detection model based on the improved LSTM network reaches up to 98.51%, the response time is only 0.84s, and the missed and false alarm rates are 1.23% and 0.36%, respectively. This network intrusion detection model can effectively detects network intrusions, ensure real-time network security, realize network intrusion defense, and provide a reliable technical support for network security, which is of great significance in the field of network attack and defense, providing new ideas for research in related fields.

Keywords: avoidance behavior; network intrusion; detection; LSTM; SSA algorithm; CNN; reinforcement learning

0 引言

随着网络技术的不断发展,网络安全问题变得越来越重要。网络入侵检测作为保护网络不受攻击的重要手段,其性能直接影响到整个网络的安全性[1]。网络入侵检测技术自诞生以来,经历了从基于规则的检测到基于异常的检测,再到基于机器学习的检测等多个阶段。基于规则的检测方法依赖于专家系统,通过定义一系列的入侵规则来识别攻击行为。然而,这种方法在面对复杂多变的网络环境时,往往显得力不从心。基于异常的检测方法通过建立正常行为的模型,将不符合模型的行为视为异常。这种方法虽然能够检测到未知的攻击,但误报率较高。近年来,随着机器学习技术的发展,基于机器学习的网络入侵检测方法逐渐成为研究热点。通过训练数据集,机器学习模型能够自动学习和识别攻击行为,提高了检测的准确性和效率[2]。文献[3]为了提高网络入侵检测的准确度提出了一种基于菌群优化深度学习的网络入侵检测模型。该模型利用菌群优化算法寻找深度置信网络的最佳参数,并利用优化后的深度置信网络进行入侵检测。结果表明,该方法的检测准确率达到了 90%以上。在文献[4]中,作者提出了一种基于判别条件变分自编码与密度峰值聚类算法的网络入侵检

收稿日期:2024-09-05; **修回日期**:2024-10-17。
作者简介:黄 亮(1979-),男,大学本科,高级工程师。
引用格式:黄 亮,陶 达,王秀木,等.基于改进 LSTM 的网络入侵检测方法[J].计算机测量与控制,2025,33(2):63-70.

测模型。该模型通过判别条件变分自编码器对网络流量进行编码，然后利用密度峰值聚类算法对编码后的数据进行聚类分析，从而识别出异常流量。该方法的优点在于能够有效识别复杂的网络攻击模式，尤其是对于那些位置攻击的识别率较高。然而，该方法在处理大规模网络数据时，模型的训练和聚类过程可能会消耗较多的计算资源和时间。在文献［5］中，作者提出了一种交叉评价模型，旨在解决基于监督机器学习的网络入侵检测系统在训练过程中需要大量明确标记样本数据的问题。该模型通过交叉验证和评价机制，能够从少量标记数据中提取更多的信息，从而构建更加准确和全面的数据集。这种方法的优点在于能够减少人工标注的工作量，同时提高模型的泛化能力。然而，交叉评价模型可能在某些情况下无法充分捕捉到数据中的所有特征，这可能会导致模型的检测性能受到影响。综合来看，文献［4］和文献［5］提出的算法各有优缺点，适用于不同的网络入侵检测场景。判别条件变分自编码与密度峰值聚类算法适合于需要高识别率的场景，尤其是在处理位置攻击时表现出色。而交叉评价模型则更适合于资源受限或需要减少人工标注工作量的场景，通过更高效地利用有限的标记数据来提升检测性能。

网络数据逃避行为是指攻击者通过各种手段，如数据包分割、加密、伪装等，来规避入侵检测系统的检测。这种行为给网络入侵检测带来了极大的挑战。传统的检测方法往往难以应对这些逃避行为，导致检测率下降。因此，研究如何有效识别和应对网络数据逃避行为，成为提高网络入侵检测性能的关键。在网络攻防技术不断发展的背景下，黑客们的逃避行为也在不断进化。为了应对这些挑战，研究人员开始探索更加智能和高效的网络入侵检测方法[6]。文献［7］为提高网络安全防护的效果，在建立入侵检测模型前，考虑了对抗逃避攻击的安全度量，设计了过滤式的对抗特征筛选方法。此外，其基于多目标演化子集选择算法进一步提高特征选择的相关性。结果表明，应用该方法的入侵模型的检测准确率得到了明显提高。其主要优点在于可以筛选出对逃避攻击更为敏感的特征，从而增强模型的检测性能。此外，其模型复杂度更低，检测速度更快。该方法的缺点在于需要额外的计算资源来处理对抗特征筛选和演化算法，这可能会增加系统的计算负担。文献［8］发现黑客在攻击网络过程中会产生较多的逃避行为以及攻击路径，其从这两个方面考虑提出了一种基于分层任务网络的攻击路径发现方法。通过该方法进一步提高网络攻防的有效性。结果表明，该方法的执行效率相较于普通方法明显更高。其优势在于能够通过将攻击路径发现任务分解为多个子任务，提高执行效率，快速响应网络攻击事件。然而，该方法的局限性在于可能需要大量的历史攻击数据来训练模型，这在实际应用中可能难以获得。文献［7］的方法更适合于需要高度准确性和对逃避行为敏感的网络环境，而文献［8］的方法则更适合于需要快速识别攻击路径的场景。长短时记忆网络（LSTM，long short-time memory network）是一种特殊的循环神经网络（RNN，recurrent neural network），在处理和预测时间序列数据方面表现出色[9]。此外，文献［10］发现多元时间序列数据的时序特征并不符合一般规律，为提高对这类序列异常情况的预测精度，其提出了一种基于生成对抗网络和 LSTM 的序列异常检测方法。该方法以迭代的方式重构正常数据，并利用检测方法捕获时间特性，放大异常特征。结果表明，该方法的检测准确率提升了 10％以上。然而，传统的 LSTM 在处理网络入侵检测任务时，仍存在一些局限性，如难以捕捉长期依赖关系和容易过拟合等[11-12]。为了提高网络入侵检测系统的性能，研究提出了一种基于网络数据逃避和改进 LSTM 的网络入侵检测方法。研究旨在提升网络入侵检测的准确性，保障网络安全。研究的创新性在于考虑了黑客入侵网络过程中的逃避数据，将其作为入侵检测的重要基础。此外，研究将卷积神经网络和 LSTM 引入到强化学习框架中，进一步提高神经网络的分类精度，实现更为准确的网络入侵检测。

1 逃避行为研究

逃避行为作为网络攻击者常用的手段，其目的是绕过现有的安全防护措施。逃避行为的研究对于提高网络入侵检测系统的性能至关重要。逃避行为的种类繁多，包括但不限于数据包分割、加密、伪装、流量混淆、协议异常等。这些手段使得攻击者能够隐藏其真实意图，从而避开传统的入侵检测系统的检测。这种逃避行为通常会产生一些异常数据，这些数据在正常网络流量中并不常见。大多数的逃避都是叠加在正常的传输控制协议（TCP，transmission control protocol）流的基础上的，故研究选择采集 TCP 数据的网络数据流的逃避行为进行网络入侵检测。逃避行为主要包含日志逃避、IDS 逃避、取证逃避共 3 种[13-15]。IDS 逃避是最常见的一种逃避行为，攻击者通过修改数据包的特征，使得入侵检测系统难以识别其真实意图。而取证逃避是攻击者通过修改日志文件、系统文件等，使得事后取证变得困难。日志逃避则主要针对系统日志进行操作，使得攻击者的行为难以被追踪。为了采集逃避网络数据，研究搭建了一个专门的网络环境，模拟正常和异常的网络流量。通过在该环境中部署各种网络设备和安全工具，可以实时监控和记录网络数据流。入侵者常用的日志逃避策略如图 1 所示。

如图 1 所示，入侵者主要可通过 IP 欺骗、账户伪

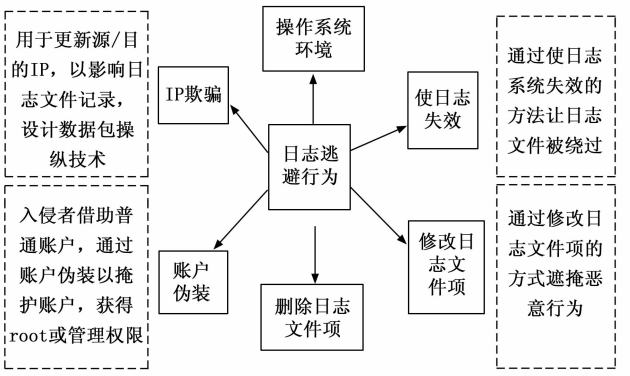

图 1　入侵者常用的日志逃避策略

装、提出日志文件项、修改日志文件项、提出日志文件等操作，绕过日志文件控制。为了有效采集网络中的逃避行为数据，研究通过模拟网络环境，并在该环境中模拟黑客的逃避行为，之后将模拟过程中产生的网络数据流收集，作为之后训练及测试的数据集。在提取得到各类网络逃避数据之后，筛选出数据流的多个不同的特征，建立特征序列。特征序列中的特征共计 17 个，分别为源 IP 地址、目的 IP 地址、源端口号、目的端口号、传输协议类型、包长度、包间隔时间、数据包载荷大小、数据包载荷内容、数据包载荷特征、数据包载荷变化率、数据包载荷熵值、数据包载荷的哈希值、数据包载荷的异常检测得分、数据包载荷的流量特征、数据包载荷的协议异常检测得分以及数据包载荷的签名匹配得分。采集完成后的数据并不能直接应用到模型中，这是因为数据中可能包含噪声、缺失值以及不一致性等问题。为了确保数据质量，研究通过数据清洗、数据标准化操作对其进行预处理。此外，网络数据流很可能存在数据不平衡的情况，为此，研究采用边界线合成少数类过采样技术（Borderline-SMOTE，synthetic minority over-sampling technique with borderline selection）算法，对数据进行过采样处理。其计算方法如式（1）所示：

$$x_{\text{new}} = x_i + rand * (x_i - \widetilde{x_i}) \tag{1}$$

式中，x_i 为选中的少数类样本，$\widetilde{x_i}$ 为 x_i 的近邻，x_{new} 为新生成的样本。研究利用 Borderline-SMOTE 方法通过计算少数类样本和多数类样本之间的距离，识别出边界区域的少数类样本。然后通过在边界区域的少数类样本中选择合适的近邻，生成新的合成样本，以此来平衡数据集中的类别分布。综合上述内容，研究通过模拟网络环境，实时监控和记录网络数据，由此采集得到合适的网络逃避数据。并利用 Borderline-SMOTE 技术对数据进行预处理，进一步降低数据的不平衡度，为后续网络入侵检测提供可靠的数据支撑。

2　入侵检测模型建立

2.1　基于 SSA 优化的改进 LSTM 模型

在提取得到合适的逃避网络数据之后，研究将其应用到入侵检测模型的训练和检验当中。为了构建一个高效的网络入侵检测系统，研究决定采用 LSTM 作为基础模型。LSTM 是一种特殊的 RNN，它能够学习长期依赖信息，非常适合处理和预测时间序列数据中的重要事件[16-17]。若仅靠不断测试人工微调网络参数将非常耗时且难以达到最优效果。因此，研究采用了一种基于自动微调的优化方法，即利用麻雀优化算法（SSA，sparrow search algorithm）对 LSTM 网络的超参数进行自动调整。研究提出的 SSA-LSTM 网络结构如图 2 所示。

如图 2 所示，研究将麻雀优化算法应用到训练过程中，不断更新网络的学习率、迭代次数以及隐藏层节点等参数。在通过 SSA 算法优化参数之后，就可以训练 LSTM 网络，并将其应用于网络入侵检测当中。LSTM 中包括遗忘门、输入门、输出门和细胞状态，这些门控机制使得 LSTM 能够有效地捕捉长期依赖关系，同时避免了传统 RNN 中的梯度消失问题。遗忘门通过计算保留权重决定哪些信息需要从细胞状态中丢弃，其输出如式（2）所示：

$$f_t = \sigma[\boldsymbol{W}_f \cdot (h_{t-1}, x_t) + b_f] \tag{2}$$

式中，b_f 为遗忘门偏置，f_t 为通过遗忘筛选后的输出，σ 为 Sigmoid 函数，x_t 为输入数据，$\boldsymbol{W}_f$ 为遗忘门的权重系数矩阵，h_{t-1} 为上一个时间步的隐藏状态。经过遗忘门筛选后传送到输入门中，输入门决定哪些新信息需要被添加到细胞状态中，输入门和遗忘门中更新的信息法如

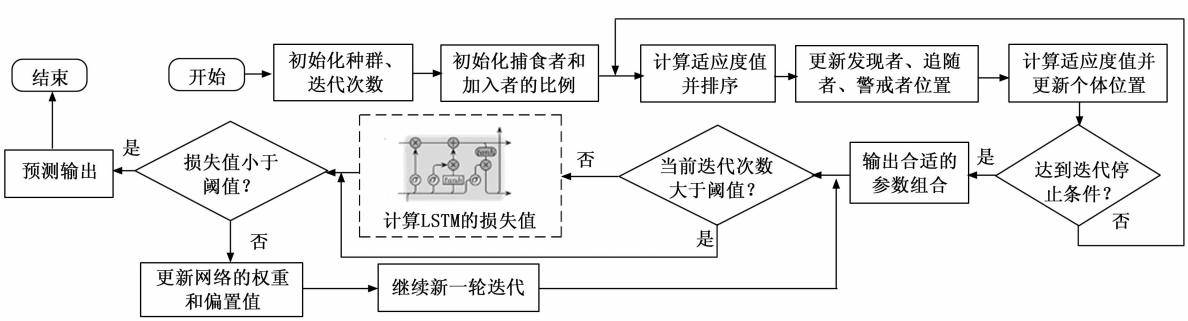

图 2　研究提出的 SSA-LSTM 网络结构

式（3）所示：

$$\begin{cases}\tilde{a}_t = \sigma[\boldsymbol{W}_a \cdot (h_{t-1}, x_t) + b_a] \\ \tilde{c}_t = \tanh[\boldsymbol{W}_c \cdot (h_{t-1}, x_t) + b_c]\end{cases} \tag{3}$$

式中，tanh(·) 为双曲正切函数，b_a 为 Sigmoid 激活层的偏置，$\boldsymbol{W}_a$ 为该层的权重矩阵，$\tilde{a}_t$ 为该层的新信息，b_c 为 tanh 激活层的偏置，$\boldsymbol{W}_c$ 为该层的权重矩阵，$\tilde{c}_t$ 为该层的新信息。在计算得到 $\tilde{a}_t$ 和 $\tilde{c}_t$ 之后，研究将其合并，并根据合并得到的信息对细胞状态进行更新，过程如式（4）所示：

$$C_t = f_t \cdot C_{t-1} + \tilde{a}_t \cdot \tilde{c}_t \tag{4}$$

式中，C_t 为 t 时刻的细胞状态，C_{t-1} 为前一时刻的细胞状态。而输出门则负责决定下一个隐藏状态的输出值，输出得到最终的网络预测值，具体如式（5）所示：

$$o_t = \sigma[\boldsymbol{W}_o \cdot (h_{t-1}, x_t) + b_o] \tag{5}$$

式中，b_o 为输出门的偏置，$\boldsymbol{W}_o$ 为其权重矩阵，o_t 为输出门的输出。SSA 算法中包括了 3 种不同类型的群体，这 3 种群体分别为开拓者、加入者以及警惕者[18-20]。开拓者通过随机探索新的参数空间，以寻找更优的网络配置。加入者则根据开拓者的成功经验进行学习，并在现有参数基础上进行微调。警惕者则负责监视环境，确保算法在搜索过程中不会陷入局部最优解，从而提高全局搜索能力。在 SSA 算法中，每个麻雀个体都有一个适应度值，用于评估其解的质量。3 种群体类型根据适应度值进行角色切换，以确保算法的高效运行。当一个麻雀个体在探索过程中发现一个更优的解时，它将转变为开拓者角色，以引导其他个体向该方向搜索。加入者则根据开拓者的指引，对已发现的优秀解进行细致的局部搜索，以进一步优化解的质量。警惕者则在搜索过程中不断评估当前解的优劣，若发现算法陷入局部最优，则会采取措施引导其他个体跳出局部最优，从而提高算法的全局搜索能力。开拓者的位置更新过程如式（6）所示：

$$X_{id}^{t+1} = \begin{cases} X_{id}^{t} \cdot \exp\left(-\dfrac{i}{\alpha T}\right), R_2 < S_T \\ X_{id}^{t} + \Gamma \cdot \boldsymbol{L}, R_2 \geqslant S_T \end{cases} \tag{6}$$

式中，X_{id}^{t+1} 和 X_{id}^{t} 分别为种群第 $t+1$ 代和第 t 代中第 i 只麻雀的位置，S_T 为安全值，其取值范围为 [0.5, 1.0]，Γ 为服从标准正态分布的随机数，$\boldsymbol{L}$ 为表示元素维度为 d，数值全为 1 的矩阵，R_2 为预警值，取值范围为 [0, 1]，α 为随机数，T 为最大迭代次数。加入者位置更新公式如式（7）所示：

$$X_{id}^{t+1} = \begin{cases} \Gamma \cdot \exp\left(\dfrac{X_{wd}^{t} - X_{id}^{t}}{i^2}\right), & i > \dfrac{n}{2} \\ X_{pd}^{t+1} + \left| X_{id}^{t} - X_{pd}^{t+1} \right| \boldsymbol{A}^{+} \cdot \boldsymbol{L}, & \text{otherwise} \end{cases} \tag{7}$$

式中，X_{pd}^{t+1} 和 X_{wd}^{t} 分别为第 $t+1$ 次迭代的最优位置和第 t 次迭代的最差位置，$\boldsymbol{A}+$ 为元素为 1 或 −1 的矩阵，n 为麻雀种群麻雀的数量，X'^{t+1}_{id} 为加入者的更新位置。警惕者的位置更新公式如式（8）所示：

$$X''^{t+1}_{id} = \begin{cases} X_{bd}^{t} + \beta(X_{id}^{t} - X_{bd}^{t}), f_i \neq f_g \\ X_{id}^{t} + K \dfrac{X_{id}^{t} - X_{wd}^{t}}{|f_i - f_w| + \delta}, f_i = f_g \end{cases} \tag{8}$$

式中，f_i 和 f_g 分别为第 i 只麻雀的适应值和当前麻雀种群的最优适应值，β 为步长参数，f_w 为最差适应值，δ 为随机数，其符合正态分布，X_{bd}^{t} 为当前全局最优，K 的取值范围为 [−1, 1]。研究首先初始化 LSTM 网络的超参数，包括学习率、迭代次数和隐藏层节点数。然后，利用麻雀优化算法对这些超参数进行优化。在每次迭代中，开拓者负责探索新的超参数组合，加入者则在已有的优秀解附近进行局部搜索，而警惕者则负责评估当前解的质量并引导算法跳出局部最优。通过这样的协同工作，找到更优的超参数，从而提高 LSTM 网络的性能。综合上述内容，研究利用 SSA 算法对 LSTM 的网络参数进行优化，进一步提高网络入侵检测的准确率。

2.2 基于 SSA-LSTM-CNN 和 DQNN 的入侵检测模型

在利用网络逃避数据和 SSA-LSTM 建立网络入侵检测模型之后，研究发现，该模型在学习过程中对样本标签具有较强的依赖性，且流量数据特征提取并不够充分，这导致其检测精度还不够理想，为此研究对其进行优化处理。研究将双重深度 Q 网络（DDQN，double deep q-network）应用到分类模型的学习当中，以期提高其自主决策能力。DDQN 通过结合深度学习和强化学习的优势，能够更好地处理高维状态空间问题。在 DDQN 中，两个深度神经网络分别用于评估和目标策略，从而减少过估计问题，提高学习的稳定性。此外，为了充分利用逃避网络数据的特征，研究将卷积神经网络（CNN，convolutional neural networks）和改进后的 LSTM 相结合，以提取更完备的时空融合特征。CNN 负责提取网络流量数据的空间特征，而改进后的 LSTM 则负责捕捉时间序列特征。通过这种结合，模型能够更好地捕捉到网络流量数据中的时空相关性，从而提取出更加完备的特征。模型的输入输出分别为网络流量数据和入侵检测结果。网络流量数据作为模型的输入，通过预处理步骤，如数据清洗、特征提取等，转换为适合模型处理的格式。在模型的输出端，入侵检测结果被生成，它包括了对网络流量是否包含入侵行为的判断，以及相应的分类标签。LSTM-CNN 模型流程和 DDQN 框架下的入侵检测流程如图 3 所示。

如图 3（a）所示，研究提出的 LSTM-CNN 混合模型通过卷积层、池化层、归一层、LSTM 层对输入数据

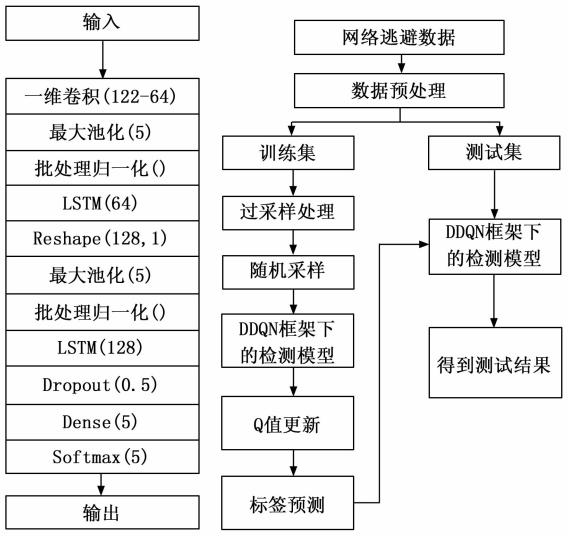

图 3　入侵检测模型的入侵具体流程示意图

进行处理，并给出分类结果。如图 3（b）所示，研究在对数据进行预处理之后将其分为 60％的训练集和 40％的测试集，然后训练集通过采样技术缓解不平衡情况，并输入到 DDQN 强化学习训练的强分类器中，通过 Q 值更新得到最优参数。研究将双重深度 Q 网络（DDQN，double deep q-network）应用到 SSA-LSTM-CNN 的学习当中，以期提高其自主决策能力。首先，研究初始化 DDQN 网络的超参数，包括学习率、折扣因子、探索率和目标网络更新频率。然后，通过与环境的交互，DDQN 网络开始学习如何在不同的网络流量场景下做出最优决策。在每个时间步，DDQN 网络根据当前的状态选择一个动作，并接收环境的反馈，包括下一个状态和即时奖励。通过这种方式，DDQN 网络不断更新其策略，以最大化预期的累积奖励。由此，对 SSA-LSTM-CNN 的输出检测结果进行不断优化，进一步提升检测精度。研究采集的逃避数据是一种时空特征序列，为完善提取的特征，进一步提高检测精度，研究将其的时间及空间特征皆进行提取。在结合改进 LSTM 和 CNN 网络结构时，研究发现两种结构都具有较高的复杂性，若直接结合使用将进一步加重模型的计算负担。针对此问题，研究使用一维卷积神经网络（1D-CNN）来降低计算复杂度。1D-CNN 专注于时间序列数据的特征提取，能够有效减少参数数量，同时保留关键信息。在 1D-CNN 层之后加入最大池化层和批处理归一层，通过此将特征维度进一步降低，从而提高模型的运算效率。此后，加入 LSTM 层，对时间特征进行提取[21-23]。之后研究将设计的混合模型引入到 DDQN 架构中，进行进一步的优化和训练。传统的深度 Q 网络（DQN，deep q-network）使用贪婪算法寻找使 Q 值最大的动作，虽然这种方法可以快速逼近优化目标，但会带来最大化偏差，使动作估计的 Q 值大于真实值，从而产生过估计的情况。

DDQN 在 DQN 的基础上引入了目标网络的概念，目标网络用于生成目标 Q 值，以减少训练过程中的最大化偏差。目标网络的参数与训练网络的参数不同步更新，而是每隔一定步数进行一次参数复制，从而使得目标网络的参数变化更加平滑，有助于提高模型的稳定性和收敛速度。因此，研究选择 DDQN 来优化分类器。DDQN 的回报估计值代表了在当前状态下采取某一动作后获得的期望回报。在训练过程中，DDQN 通过经验回放机制来缓解样本之间的相关性，提高训练的稳定性。具体来说，经验回放机制将训练样本存储在回放缓冲区中，并在训练时随机抽取一批样本进行学习，从而避免了样本之间的相关性问题。DDQN 的回报估计值计算方法如式（9）所示：

$$Qt_t = R + \gamma Q(S_{t+1}, \text{argmax}Q(s_{t+1}, a; \omega); \omega') \tag{9}$$

式中，R 为回报函数，γ 为折扣因子，ω 和 ω' 分别为评估网络和目标网络的权重参数，$Q(s,a;\omega)$ 为状态－动作值函数，s_{t+1} 为 $t+1$ 时刻的状态，a 为当前动作。DDQN 定义了状态－动作值函数与状态值函数的差值，并将其应用到状态－动作值函数 $Q(s,a;\omega)$ 的计算当中。最终 $Q(s,a;\omega)$ 的计算方法如式（10）所示：

$$Q(s,a;\omega) = V(s;\omega) + A(s,a;\omega) \tag{10}$$

式中，$A(s,a;\omega)$ 和 $V(s;\omega)$ 分别为优势指函数和状态值函数。为解决同一个状态－动作函数的分解有无穷多种的问题，研究在其后面加上优势函数的平均值。通过这种方式，研究能够有效地估计每个动作的期望回报，并在训练过程中不断调整网络参数以最小化误差。为了进一步提高模型的泛化能力，研究引入了正则化技术。正则化技术通过在损失函数中添加一个惩罚项来防止模型过拟合，从而提高模型在未知数据上的表现。研究采用了 L2 正则化，它通过在损失函数中添加权重平方的和来限制模型参数的大小。最终的状态－动作函数如式（11）所示：

$$Q'(s,a;\omega) = V(s;\omega) + A(s,a;\omega) - \frac{1}{|A|}\sum_{a\in A} A(s,a;\omega) \tag{11}$$

式中，A 为优势函数的集合。由于动作和状态函数无关，DDQN 的状态更新时，也同时对状态－动作值函数的平均值进行了调整，进而一次性调整了在该状态下的所有动作值，进一步提高了算法效率。综合上述内容，研究利用逃避网络数据作为模型的训练集和测试集，进一步训练网络入侵检测模型。在建立网络入侵检测模型时，研究利用 SSA 算法对 LSTM 的网络参数进行优化，进一步提高网络入侵检测的准确率。之后将改

进后的 LSTM 和 CNN 混合，进一步提高模型的特征提取能力。最后采用 DDQN 对混合模型进行强化学习，进一步提高入侵检测模型的检测效率。由此，构建了一个基于逃避网络数据和改进 LSTM 的网络入侵检测模型。考虑到模型规模及参数变量的复杂性增加会导致训练和实际应用工作量加大，研究对模型结构进行轻量化改进：研究采用深度可分离卷积技术来替代传统的卷积操作。将标准卷积分解为深度卷积和逐点卷积两个步骤，以减少了模型参数的数量。此外，研究将输入特征图分成若干组，每组分别进行卷积操作，进一步降低了计算复杂度。在模型训练过程中，研究还采用了早停策略来防止过拟合。此外，研究还使用了批量归一化技术来加速训练过程并提高模型的泛化能力。

3 实验与分析

研究基于逃避网络数据和改进 LSTM 建立了一个新的网络入侵检测模型。为检验所提出的模型的性能，研究开展了一系列实验对其性能进行对比分析。研究在仿真软件上进行了实验，实验环境配置如下：操作系统为 Ubuntu 18.04，CPU 为 Intel Core i7-9700K，内存为 64 GB，显卡为 NVIDIA GeForce RTX 2080 Ti。实验中的测试数据集包括 NSL-KDD、UNSW-NB15 两个数据集。NSL-KDD 数据集是 KDD Cup 99 的一个改进版本，解决了原始数据集中的重复记录问题，并且更加注重于分类的准确性。UNSW-NB15 数据集是相对较新的数据集，其模拟了现代网络环境下的攻击行为，提供了更加全面和复杂的网络流量数据。为检验研究提出的基于强化学习和 SSA-LSTM-CNN 模型的训练效果，研究将其与单一的 LSTM、CNN 以及 LSTM-CNN 模型在相同环境中进行训练，并记录训练过程中的损失值以及训练模型的检测精度的变化情况。具体结果如图 4 所示。

如图 4（a）所示，随着训练次数的加大，各个模型的损失值逐渐下降，且趋于平稳。其中 SSA-LSTM-CNN 的收敛时间相较于另外 3 个模型明显更快，其在迭代至 23 次即开始收敛，且收敛损失值相较于单一的 LSTM 和 CNN 更低。这是因为 LSTM 和 CNN 混合之后提取得到的特征更加全面，而 SSA 算法对网络参数的优化进一步提高了模型的收敛速度和精度。从图 4（b）中可以看出，SSA-LSTM-CNN 模型在检测精度方面也表现出了明显的优势。在迭代至 78 次时，该模型的检测精度已经超过了 98%，而单一的 LSTM 和 CNN 模型的检测精度分别只有 92%和 94%。这说明混合模型在特征提取和检测能力方面具有显著的优势。综合图 4 结果可知，研究利用 SSA 算法改进的 LSTM-CNN 混合模型能够在保持计算效率的同时具有较高的检测精度。

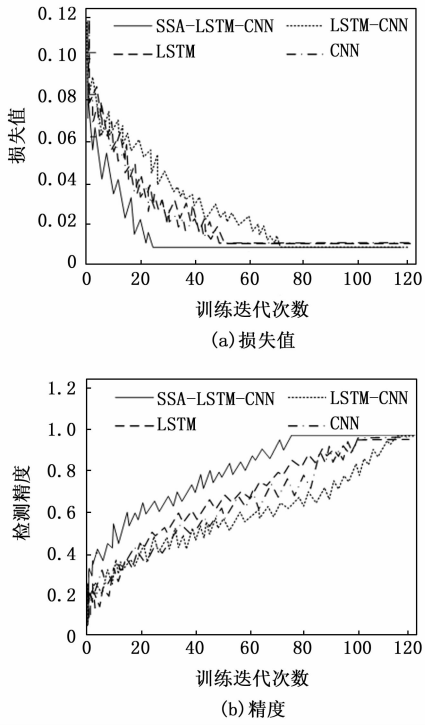

图 4 训练过程中的损失值以及训练模型的检测精度的变化情况

为验证研究提出的 DDQN 强化学习的合理性，研究将其与传统的强化学习算法进行比较。对比方法包括 Q 学习（Q-learning）、时序差分学习算法（SARSA，state-action-reward-state-action）和 DQN。对比指标包括检测准确率、召回率、F_1 分数和响应时间。在这 4 种框架下的检测模型的分类性能比较结果如图 5 所示。

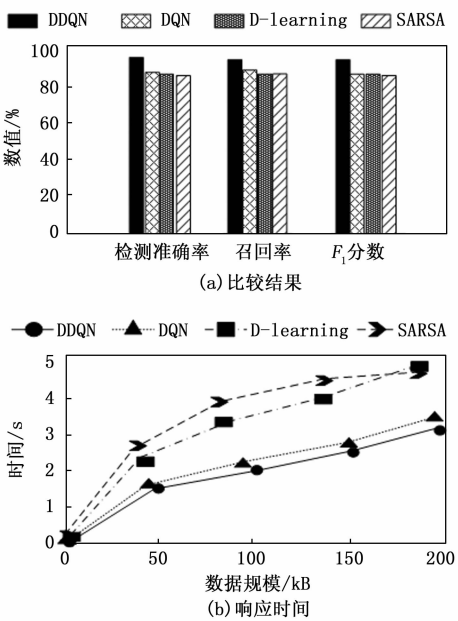

图 5 4 种强化学习框架下的检测模型的分类性能比较结果

如图 5（a）所示，DDQN 的检测准确率、召回率以及 F_1 分数解高于另外 3 个强化学习方法。具体来说，DDQN 的 3 个评价指标的数值分别为 0.98、0.97 和 0.97，而 Q-learning、SARSA 和 DQN 的检测准确率分别为 91%、90%和 92%，召回率分别为 91%、92%和 93%，F_1 分数分别为 91%、91%和 92%。这表明 DDQN 在处理网络入侵检测问题时，能够更有效地学习到最优策略，从而提高检测的准确性和效率。如图 5（b）所示，随着检测数据量的增加，各个检测模型的检测时间逐渐增加，但 DDQN 框架下的模型的检测时间增长幅度相对较小，在数据规模为 500 kB 时，其计算时间为 1.84 s。这说明 DDQN 在处理大规模数据时，仍能保持较高的检测效率，具有良好的可扩展性。综合图 5 结果可知，DDQN 在性能上优于其他 3 种强化学习方法，不仅在准确率和效率上表现出色，而且在处理大规模数据时仍能保持较高的性能。

为检验研究提出的网络入侵检测模型（模型 1）的性能，研究将其与目前较为先进的网络入侵检测模型进行对比实验。对比过程中采用研究建立的正常流量以及逃避行为数据集作为测试集。对比模型包括文献［24］中的网络入侵检测模型（模型 2）、文献［25］中的网络入侵检测模型（模型 3）、文献［26］中的网络入侵检测模型（模型 4）。对比指标包括检测准确率、响应时间、漏报率、误报率。对比结果如表 1 所示。

表 1　网络入侵检测模型性能对比结果

模型	检测准确率/%	响应时间/s	漏报率/%	误报率/%
模型 1	98.51	0.84	1.23	0.36
模型 2	90.57	2.00	7.87	1.54
模型 3	92.48	1.65	5.14	0.90
模型 4	89.88	2.54	10.33	2.84

如表 1 所示，模型 1 在检测准确率方面显著优于其他对比模型，达到了 98.51%，而模型 2、模型 3 和模型 4 的检测准确率分别为 90.57、92.48 和 89.88%。这表明模型 1 在识别网络入侵行为方面具有更高的准确性和可靠性。响应时间方面，模型 1 仅需 0.84 s 即可完成检测，远低于其他模型，这说明模型 1 在实时性方面表现优异，能够快速响应网络入侵事件。漏报率和误报率是衡量网络入侵检测系统性能的两个重要指标，漏报率高意味着系统可能遗漏真正的入侵行为，而误报率高则会导致过多的正常行为被错误地判定为入侵。模型 1 的漏报率为 1.23%，误报率为 0.36%，均低于其他对比模型，这表明模型 1 在减少漏报和误报方面具有明显优势。综上所述，基于逃避网络数据和改进 LSTM 的网络入侵检测模型能够有效应对网络入侵检测的挑战，提高检测的准确性和效率。

4　结束语

作为网络安全的重要防护手段，目前的入侵检测技术仍然存在精度低，实时性差的问题。针对此，研究提出了一种结合网络逃避数据的新的网络入侵检测模型。该模型将网络逃避数据应用到模型的训练学习当中，并将 LSTM 和 CNN 作为入侵检测的基础模型。在此基础上，研究引入强化学习和 SSA 算法对模型进行优化。实验结果表明，研究提出的 SSA-LSTM-CNN 模型的训练效果明显优于另外两个单一模型和 LSTM-CNN 模型。其分别训练至 23 次和 78 次达到最佳的损失值和检测精度。相较于其他模型具有较好的收敛性。研究提出的强化学习框架 DDQN 下的检测模型的检测准确率、召回率以及 F_1 分数明显高于另外几个强化学习方法。其数值分别为 0.98、0.97 和 0.97。且该强化学习方法的检测时间也在理想范围内，在数据规模为 500 kB 时，其计算时间为 1.84 s。在与目前较为流行的入侵检测模型进行对比的实验中，模型 1 的检测准确率，响应时间分别为 98.51%和 0.84 s，其能够有效检测出网络入侵中的逃避行为。此外，模型 1 的漏报率和误报率分别为 1.23%和 0.36%，其在减少漏报和误报方面具有明显优势。综合上述内容可知，研究提出的检测模型能够在网络运行过程中及时检测出网络入侵，为网络安全提供可靠保障。在之后的工作中，可考虑采用轻量化方法进一步简化模型结构，提升检测效率。

参考文献：

［1］田小芳. 基于人工蜂群算法的计算机网络 DDoS 攻击检测方法［J］. 计算机测量与控制，2023，31（12）：28－33.

［2］ABDULGANIYU O H，AIT TCHAKOUCHT T，SAHEED Y K. A systematic literature review for network intrusion detection system（IDS）［J］. International Journal of Information Security，2023，22（5）：1125－1162.

［3］白文荣，马琳娟，巩　政. 基于菌群优化深度学习的网络入侵检测模型［J］. 南京理工大学学报，2023，47（5）：636－642.

［4］李登辉，葛丽娜，王　哲，等. DCVAE 与 DPC 融合的网络入侵检测模型研究［J］. 小型微型计算机系统，2024，45（4）：998－1006.

［5］APRUZZESE G，PAJOLA L，CONTI M. The cross-evaluation of machine learning-based network intrusion detection systems［J］. IEEE Transactions on Network and Service Management，2022，19（4）：5152－5169.

［6］MOHY-EDDINE M，GUEZZAZ A，BENKIRANE S，et al. An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection［J］.

Multimedia Tools and Applications, 2023, 82 (15): 23615 - 23633.
[7] 黄启萌, 吴苗苗, 李 云. 对抗逃避攻击的过滤式对抗特征选择研究 [J]. 电信科学, 2023, 39 (7): 46 - 58.
[8] 王子博, 张耀方, 陈翊璐, 等. 基于分层任务网络的攻击路径发现方法 [J]. 计算机科学, 2023, 50 (9): 35 - 43.
[9] APRUZZESE G, ANDREOLINI M, FERRETTI L, et al. Modeling realistic adversarial attacks against network intrusion detection systems [J]. Digital Threats: Research and Practice (DTRAP), 2022, 3 (3): 1 - 19.
[10] 陈世伟, 李 静, 玄佳兴, 等. LSTM-GAN: 融合 GAN 和 Bi-LSTM 的无监督时间序列异常检测 [J]. 小型微型计算机系统, 2024, 45 (1): 123 - 131.
[11] 白万荣, 魏 峰, 郑广远, 等. 基于 TCN-BiLSTM 的入侵检测算法研究 [J]. 计算机科学, 2023, 50 (2): 929 - 936.
[12] WANG N, CHEN Y, XIAO Y, et al. Manda: on adversarial example detection for network intrusion detection system [J]. IEEE Transactions on Dependable and Secure Computing, 2022, 20 (2): 1139 - 1153.
[13] AL-TURAIKI I, ALTWAIJRY N. A convolutional neural network for improved anomaly-based network intrusion detection [J]. Big Data, 2021, 9 (3): 233 - 252.
[14] RASHID M, KAMRUZZAMAN J, IMAM T, et al. A tree-based stacking ensemble technique with feature selection for network intrusion detection [J]. Applied Intelligence, 2022, 52 (9): 9768 - 9781.
[15] ABDELKHALEK A, MASHALY M. Addressing the class imbalance problem in network intrusion detection systems using data resampling and deep learning [J]. The Journal of Supercomputing, 2023, 79 (10): 10611 - 10644.
[16] THOCKCHOM N, SINGH M M, NANDI U. A novel ensemble learning-based model for network intrusion detection [J]. Complex & Intelligent Systems, 2023, 9 (5): 5693 - 5714.
[17] MERZOUK M A, CUPPENS F, BOULAHIA-CUPPENS N, et al. Investigating the practicality of adversarial evasion attacks on network intrusion detection [J]. Annals of Telecommunications, 2022, 77 (11): 763 - 775.
[18] SIVAMOHAN S, SRIDHAR S S. An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework [J]. Neural Computing and Applications, 2023, 35 (15): 11459 - 11475.
[19] GAD A G, SALLAM K M, CHAKRABORTTY R K, et al. An improved binary sparrow search algorithm for feature selection in data classification [J]. Neural Computing and Applications, 2022, 34 (18): 15705 - 15752.
[20] GYAMFI E, JURCUT A D. Novel online network intrusion detection system for industrial IoT based on OI-SVDD and AS-ELM [J]. IEEE Internet of Things Journal, 2022, 10 (5): 3827 - 3839.
[21] RANI M, GAGANDEEP. Effective network intrusion detection by addressing class imbalance with deep neural networks multimedia tools and applications [J]. Multimedia Tools and Applications, 2022, 81 (6): 8499 - 8518.
[22] UDAS P B, KARIM M E, ROY K S. SPIDER: A shallow PCA based network intrusion detection system with enhanced recurrent neural networks [J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34 (10): 10246 - 10272.
[23] ILYAS M U, ALHARBI S A. Machine learning approaches to network intrusion detection for contemporary internet traffic [J]. Computing, 2022, 104 (5): 1061 - 1076.
[24] 周湘贞, 李 帅, 隋 栋. 线性判别分析优化孪生支持向量机的网络入侵检测 [J]. 济南大学学报: 自然科学版, 2023, 37 (4): 466 - 471.
[25] 万 壮, 赵 云, 陆 川, 等. 基于 multi-CNN 的专用网络入侵检测模型设计与仿真 [J]. 现代电子技术, 2023, 46 (2): 80 - 84.
[26] 于继江. 基于机器学习与 DBN 网络的网络入侵检测方法研究 [J]. 微型电脑应用, 2024, 40 (1): 184 - 187.

(上接第 30 页)

[15] 何 彧, 宋克臣, 张德富, 等. 融合多层级特征的弱监督钢板表面缺陷检测算法 [J]. 东北大学学报 (自然科学版), 2021, 42 (5): 687 - 692.
[16] 徐志祥, 关守岩, 杨 帆, 等. 一种基于 2D-CNN 的激光超声表面缺陷检测方法 [J]. 应用光学, 2021, 42 (1): 149 - 156.
[17] 简川霞, 王华明, 徐进军, 等. OLED 显示屏表面缺陷自动检测方法 [J]. 包装工程, 2021, 42 (13): 280 - 287.
[18] 明五一, 贾豪杰, 何文斌, 等. 透明件表面缺陷的机器视觉检测综述 [J]. 机械科学与技术, 2021, 40 (1): 116 - 124.
[19] 郭井宽, 张 森, 张延松. 管屏拼焊焊缝表面缺陷的激光视觉检测方法 [J]. 焊接, 2022 (12): 30 - 35.
[20] 刘文芳, 韩 军, 刘艳锋, 等. 基于机器学习的金属近表面缺陷超声检测方法 [J]. 中国测试, 2022, 48 (1): 46 - 52.