融合自适应 SSAE 与神经网络算法的网络安全模型研究

林金妹[1] 韦冰东[1]
LIN Jinmei WEI Bingdong

摘 要 为提升网络安全防护的智能化与精准度，利用自适应 SSAE 与神经网络融合算法，优化设计网络安全模型。采用网络爬虫算法，采集网络运行数据以此作为模型输入值。从防护时间、风险容忍度等方面设置模型约束条件。以自适应堆叠稀疏自编码器和神经网络构建与融合，通过算法的学习迭代提取网络运行特征，根据提取特征与网络异常标准特征的匹配度，确定网络的异常状态与类型。根据网络异常检测结果，通过异常节点隔离、安全加固、访问控制 3 个步骤，实现模型的安全防御功能。通过模型测试实验得出结论：与传统模型相比，优化设计模型的网络攻击误检率和漏检率分别下降 4.25% 和 3.55%，在模型作用下网络丢包率降低 1.28%。

关键词 自适应 SSAE 算法；神经网络算法；融合算法；网络安全；模型设计

doi：10.3969/j.issn.1672-9528.2025.02.033

0 引言

网络安全是指保护网络系统中的硬件、软件及数据免受恶意攻击、破坏、泄露或非法使用的综合措施与技术。涵盖多个层面，包括信息完整性、保密性、可用性和真实性等关键要素[1]。为提升防护能力、保障业务连续性，本文提出了一种网络安全模型。网络安全模型是一种框架或体系结构，旨在描述、分析和解决网络安全问题，通过定义一系列安全策略、原则、组件和操作过程，确保网络系统的机密性、完整性和可用性。目前发展较为成熟的网络安全模型具体包括：文献 [2] 提出的基于 SecOC 的网络通信安全模型、文献 [3] 提出的基于 PDST-EEF 机制的网络安全模型以及文献 [4] 提出的基于模型的网络安全模型，然而上述模型在运行过程中由于无法精准检测网络安全问题，导致模型运行存在明显的执行不力问题，为此引入自适应 SSAE 与神经网络算法。自适应 SSAE 算法即自适应堆叠稀疏自编码器算法，是一种基于深度学习的数据表示方法，通过多层非线性变换，将数据从原始高维空间映射到低维特征空间，同时保持数据的关键信息。

1 网络安全模型设计

1.1 确定网络安全模型输入值

采用网络爬虫程序对网络运行数据进行采集，以此作为模型输入值。以用户行为数据为例，爬虫首先访问目标网站，模拟用户浏览、点击等行为，通过分析网页结构，识别并提取用户行为相关的数据元素，用户行为数据的采集结果为：

$$x_{c-b}=\kappa_p\cdot x_b \tag{1}$$

式中：x_b 和 $x_{c\text{-}b}$ 分别表示网络用户行为数据的实际值和采集值；κ_p 为网络爬虫采集系数，归一化处理过程为：

$$x_{\mathrm{cg}}=\frac{x_c-x_{\min}}{x_{\max}-x_{\min}} \tag{2}$$

式中：x_c 为初始输入的网络数据；$x_{\max}$ 和 $x_{\min}$ 分别为网络运行数据的最大值和最小值。在实际的模型工作过程中，将归一化处理完成的网络数据输入到模型中。

1.2 设定网络安全模型约束条件

为降低网络安全模型运行对实际网络产生的影响，从防护时间、风险容忍度、资源消耗量等方面设置约束条件。防护时间是指模型启动防护措施到网络攻击成功绕过防护措施所需的时间，具体约束条件的设定情况为：

$$y_t=T_f-T_a\geq 0 \tag{3}$$

式中：T_f 和 T_a 分别表示防护措施的执行时间和攻击者绕过防护措施的消耗时间。风险容忍度表示网络安全模型对潜在风险的接受程度，该约束条件的设置结果为：

$$y_r=\frac{1}{1+e^{(r-\delta_r)}}\geq 0.5 \tag{4}$$

表示当前风险水平 r 始终高于网络安全模型的风险容忍阈值 δ_r[5]。按照上述方式可以得出所有约束条件的量化设计结果，并保证优化设计网络安全模型的运行满足设定约束条件。

1.3 融合自适应 SSAE 与神经网络算法检测网络异常

以输入网络安全模型的网络运行数据为处理对象，通过

1. 广西理工职业技术学院 广西崇左 532200

自适应 SSAE 与神经网络融合算法的学习与迭代，判断当前网络是否存在入侵或运行异常，由此实现对网络安全态势的评估。

1.3.1 构建自适应堆叠稀疏自编码器和神经网络

为得出自适应 SSAE 与神经网络融合算法，分别构建自适应堆叠稀疏自编码器和神经网络，构建结构如图 1 所示。

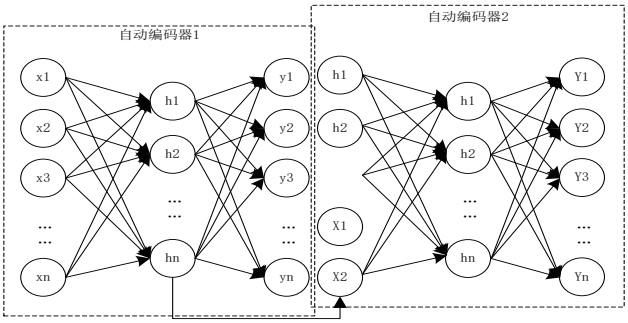


图 1 自适应堆叠稀疏自编码器结构图

从图 1 中可以看出，构建的自适应堆叠稀疏自编码器由输入层、堆叠的稀疏自编码器层、输出层等部分组成。其中输入层用来接收输入数据。堆叠的稀疏自编码器层包含多个稀疏自编码器层，每一层都包含编码器和解码器两部分，编码器部分将输入数据转换为稀疏表示，即大部分神经元被抑制，只有少数神经元被激活。解码器部分则尝试从稀疏表示中重建输入数据，以最小化重建误差 [6]。自适应 SSAE 与神经网络融合算法的运行可分为前向传播和反向传播两个部分，在前向传播阶段 [7]，将输入值代入到输入层中，对于每一层稀疏自编码器，隐藏层的激活值的计算结果为：

$$h_j = g\left(\varpi_j x + b_j\right) \tag{5}$$

式中：x 为融合算法中的输入值；$g()$ 为激活函数；ϖ_j和 b_j 分别为第 j 层的权重和偏置 [8]。隐藏层神经元的平均激活度为：

$$\lambda_j = \frac{1}{n_x}\sum_{i=1}^{n_x} h_j\left(x_i\right) \tag{6}$$

式中：n_x 为输入融合算法中的样本数据量。平均激活度与稀疏性参数之间的差异为：

$$C = \varphi \lg\frac{\varphi}{\lambda_j} + (1-\varphi)\lg\frac{1-\varphi}{1-\lambda_j} \tag{7}$$

式中：φ 为稀疏性参数。由此可以得出融合算法的输出结果为：

$$h_{\text{out}} = \sum_{j=1}^{n_s} h(j) \tag{8}$$

式中：变量 n_s 表示是融合算法中包含的神经元数量 [9]。在反向传播过程中，计算损失函数关于网络参数的梯度，使用梯度下降法更新网络参数，以最小化总损失函数。以权重系数为例，其更新过程可以量化表示为：

$$\varpi_j(t) = \alpha\left(\varpi_j(t-1) - \sigma\cdot C\right) \tag{9}$$

式中：$\varpi_j(t-1)$和$\varpi_j(t)$分别为第 t-1 和 t 次迭代中的第 j 层权重值；σ 为稀疏性惩罚项的权重；α 为学习率。将参数更新结果代入到前向传播中，重复执行上述操作，直至算法运行满足终止条件，即达到最大迭代次数。由于自适应机制的引用，根据梯度的变化动态调整学习率参数，由此得出自适应 SSAE 与神经网络融合算法的学习迭代结果。

1.3.2 利用融合算法提取网络运行特征

将确定的网络安全模型输入值代入到自适应 SSAE 与神经网络融合算法中，通过算法的学习迭代，得出网络运行特征的提取结果 [10]。以网络流量运行特征为例，其特征向量包括流量大小、平均包长、流量速率等，上述特征分量的提取结果为：

$$\begin{cases} \tau_d = h_{\text{out}}\sum n_b \\ \tau_l = \dfrac{\tau_d}{n_b} \\ \tau_v = \dfrac{\tau_d}{t_c} \end{cases} \tag{10}$$

式中：τ_d 表示流量值；τ_l 表示平均包长；τ_v 表示流量速率；n_b 为各个数据包的大小值；t_c 为网络数据的传输时间。按照上述方式可以得出其他网络流量、用户行为等数据的提取结果，通过融合算法中的输出层进行输出，并对提取的所有特征分量进行融合处理，处理结果记为 τ。

1.3.3 判定网络异常状态与类型

采用特征匹配的方式，计算当前网络运行特征与不同网络异常状态下的标准运行特征之间的匹配度，由此判断当前网络的异常状态。特征匹配度计算公式为：

$$s = \frac{\tau\cdot\tau_B(i)}{\|\tau\|\cdot\|\tau_B(i)\|} \tag{11}$$

式中：$\tau_B(i)$ 为 i 类异常状态下网络的标准运行特征，若计算结果高于阈值 s_0，证明当前网络处于异常状态，异常状态类型为 i，否则进行下一标准特征的匹配，直至得出满足阈值条件的匹配结果。若均不满足阈值条件，则说明当前网络处于正常运行状态。

1.4 实现网络安全防御控制功能

针对检测存在异常的网络，对网络中的异常节点进行隔离处理，并对网络安全进行加固。在网络安全模型运行过程中，对申请接入网络的节点进行信誉度量，通过对用户行为风险的评估，实现对其接入进程的控制，最大程度保证网络的运行安全。

1.4.1 隔离网络异常节点

对于检测处于异常状态的网络，需对网络中所有节点的

异常概率进行求解，确定异常节点位置，作为网络异常隔离目标。网络中任意节点的异常概率求解公式为：

$$P_{ab}(i)=\frac{n_{\tau(s)}(i)}{n_{\tau}(i)}\times\frac{\eta(i)}{\overline{\eta}}\times\omega \tag{12}$$

式中：$n_{\tau(s)}$ 和 n_{τ} 分别表示网络节点 i 的异常行为特征数量以及总行为特征数量；$\eta(i)$ 和$\overline{\eta}$为节点 i 的丢包率及网络所有节点丢包率的平均值；ω 为权重因子，选择异常概率求解最大的节点作为网络的异常节点，将其作为隔离处理对象 [11]。

1.4.2 网络接入访问控制

综合考虑申请访问网络用户的行为特征，计算用户的信誉度，由此生成访问控制决策指令，进而执行网络接入访问控制任务。首先根据输入模型中的用户行为数据，计算用户信誉度，计算公式为：

$$\psi(i)=\varsigma\cdot\Sigma\left(\psi_{\mathrm{com}}(i)\times\frac{\phi(i)}{\omega_{\vartheta}(i)}\right) \tag{13}$$

式中：ζ 为衰减因子；$\psi_{\mathrm{com}}(i)$、$\phi(i)$ 和 $\omega_{\vartheta}(i)$ 分别表示网络节点 i 的交互信誉度、交易信誉度和信誉度量权重 [12]。在得到用户信誉度后，可以根据信誉度值生成访问控制决策指令，访问决策结果为：

$$\begin{cases}\psi(i)\geq\psi_0, i\in U_{\mathrm{visit}}\\ \psi(i)<\psi_0, i\notin U_{\mathrm{visit}}\end{cases} \tag{14}$$

式中：ψ_0 为信誉度阈值；U_{visit} 为网络允许访问用户集合。从式中可以看出，通过信誉度阈值的设置，当用户的信誉度高于该阈值时，允许其访问网络资源；当用户的信誉度低于该阈值时，则拒绝其访问请求。网络访问控制任务的执行涉及配置防火墙 [13-14]、路由器 [15-16] 等网络设备，以允许或拒绝特定用户的网络访问请求。

2 模型测试实验分析

2.1 配置网络环境

为保证优化设计网络安全模型能够成功调用自适应 SSAE 与神经网络融合算法，需要对自适应堆叠稀疏自编码器和神经网络算法的相关运行参数进行设定 [17]。自适应 SSAE 与神经网络算法的激活函数均设定为 ReLU 函数，稀疏性参数为 0.05，学习率为 0.1，最大迭代次数为 80。输入、隐含 / 稀疏自编码器、输出层包含的节点数量分别为 10、50 和 20，初始权值为 0.2。优化设计网络模型选择 Nemesis 作为开发工具，该工具支持自适应 SSAE 框架的集成，包括安全策略的动态调整、网络流量的实时监控与分析等，同时满足神经网络的运行条件 [18]。将配置的静态和移动网络接入到优化设计的网络安全模型中，得出模型的运行结果。

2.2 设置模型测试指标

根据模型工作内容，分别从安全检测和安全防御两个方面设置测试指标，其中安全检测测试指标为误检率和漏检率，测试结果为：

$$\begin{cases}\eta_{\mathrm{err}}=\dfrac{N_{\mathrm{err}}}{N_L}\times100\%\\ \eta_{\mathrm{loss}}=\dfrac{N_w}{N_L}\times100\%\end{cases} \tag{15}$$

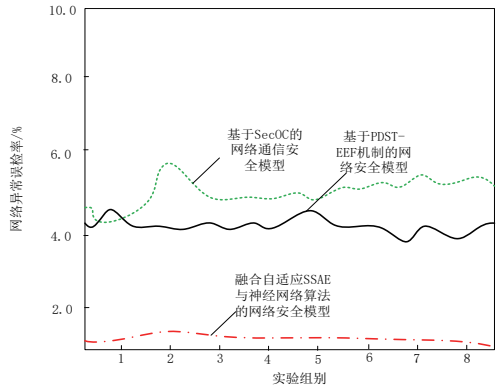
式中：N_{err}、N_w 和 N_L 分别表示错误识别为入侵攻击的正常连接数量、未被检测出的入侵攻击数量和入侵攻击总数量。计算得出误检率和漏检率取值越小，证明对应模型的安全检测性能越优。模型安全防御性能的测试指标为丢包率，该指标测试结果为：

$$\eta=\left(\frac{N_{\mathrm{se}}-N_{\mathrm{re}}}{N_{\mathrm{se}}}\right)\times100\% \tag{16}$$

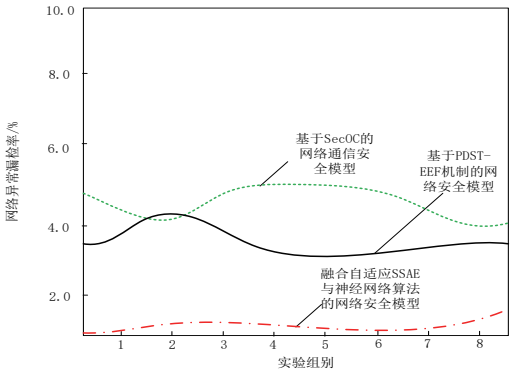
式中：N_{se} 和 N_{re} 分别表示实际发送和接收的网络传输数据量。计算得出丢包率取值越大，证明模型安全防御性能越差。

2.3 模型测试实验结果与分析

综合考虑网络静态和动态两个运行状态，通过相关参数的统计与式（15）的计算，得出不同模型作用下网络入侵检测误检率和漏检率的测试结果，如图 2 所示。



（a）误检率



（b）漏检率

图 2 网络安全模型入侵检测性能测试结果

从实验结果中可以看出，3 种网络安全模型的误检率平均值分别为5.4%、3.9%和0.4%，漏检率的平均值分别为4.7%、

3.6% 和 0.6%，由此证明优化设计模型具有更优的攻击检测性能。另外，在优化设计模型作用下，网络丢包率的测试结果如表 1 所示。

表 1 网络安全模型作用下网络丢包率测试数据表

单位：MB

实验组别	发送数据量	基于 SecOC 的网络通信安全模型下接收数据量	基于 PDST-EEF 机制的网络安全模型下接收数据量	融合自适应 SSAE 与神经网络算法的网络安全模型下接收数据量
1	489	474	482	485
2	623	611	620	622
3	581	565	577	580
4	714	703	710	714
5	569	560	564	568
6	384	375	380	384
7	625	613	621	623
8	724	705	718	722

将表 1 中的数据代入到式（16）中，即可得出 3 种模型作用下网络丢包率分别为 2.22%、0.82% 和 0.24%。由此证明优化设计模型具有更优的安全防御性能。

3 结语

网络安全模型能有效应对日益复杂的网络威胁，提升网络系统的防护能力，通过实时监测与预警，模型能及时发现并阻断潜在的安全风险，保障用户数据与隐私的安全。为提升模型的作用效果，融合自适应 SSAE 与神经网络算法对模型进行优化设计，通过利用 SSAE 在特征提取与数据降维方面的优势，结合神经网络在复杂模式识别上的强大能力，使网络安全模型能够自动学习网络流量数据的深层特征，并准确识别出潜在的网络攻击行为，最大程度的保证网络的运行安全。

参考文献：

[1] 章熙 , 段金长 , 刘晓放 , 等 . 基于 PKI 公钥体系的电力监控网络安全接入机制 [J]. 沈阳工业大学学报 ,2024,46(1):115-120.

[2] 章意 , 李飞 , 张森葳 . 基于 SecOC 的车载网络通信安全模型研究 [J]. 计算机应用研究 ,2022,39(8):2474-2478.

[3] 熊洪樟 , 程杰 , 刘岩 , 等 . 基于 PDST-EEF 机制的智能电网网络安全框架研究 [J]. 高电压技术 ,2023,49(S1):135-140.

[4] 蒋宁 , 范纯龙 , 张睿航 , 等 . 基于模型的零信任网络安全架构 [J]. 小型微型计算机系统 ,2023,44(8):1819-1826.

[5] 徐勇军 , 曹奇 , 万杨亮 , 等 . 基于硬件损伤的异构网络鲁棒安全资源分配算法 [J]. 电子与信息学报 , 2023, 45(1): 243-253.

[6] 韦磊 , 徐江涛 , 郭雅娟 , 等 . 基于信任机制的电力无线传感网络安全簇头选举算法 [J]. 中国电力 ,2023,56(8):61-67.

[7] 陈何雄 , 罗宇薇 , 韦云凯 , 等 . 基于区块链的软件定义网络数据帧安全验证机制 [J]. 计算机应用 ,2022,42(10):3074-3083.

[8] 程雨芊 , 程中鼎 . 基于 LSSVM 的传感器网络安全风险预测与控制 [J]. 沈阳工业大学学报 ,2022,44(5):558-564.

[9] 刘晋州 , 唐雪琴 , 韩宝安 , 等 . 基于 IFS-FOA-ELM 的网络安全态势预测方法 [J]. 火力与指挥控制 ,2024,49(5):184-190.

[10] 田世林 , 李焕洲 , 唐彰国 , 等 . 基于堆叠稀疏去噪自编码器的混合入侵检测方法 [J]. 四川师范大学学报 (自然科学版),2024,47(4):517-527.

[11] 李江坤 , 黄海燕 . 互信息深度稀疏自编码融合 DLSTM 预测网络 [J]. 计算机工程与应用 ,2022,58(20):277-285.

[12] 颜蔚 . 基于卷积神经网络的无线网络安全风险评估及控制 [J]. 沈阳工业大学学报 ,2022,44(5):565-569.

[13] 赵一 , 刘行 , 明洋 , 等 . 完备的 IBE 密码学逆向防火墙构造方法 [J]. 软件学报 , 2024, 35(7):3482-3496.

[14] 曹子雯 , 贺霖卿 . 兼顾“高联通性”和“低传染性”的金融机构关联网络优化路径研究 [J]. 金融理论与实践 , 2024(7): 71-81.

[15] 王晨磊 , 解大 , 顾承红 . 基于复杂网络理论的能源路由器物理层模型及配置策略 [J]. 中国电机工程学报 , 2023, 43(7): 2666-2676.

[16] 杨鹏飞 , 蔡瑞杰 , 郭世臣 , 等 . 一种基于容器的 Cisco IOS-XE 系统入侵检测方法 [J]. 计算机科学 , 2023, 50(4): 298-307.

[17] 何静 , 唐润忠 , 张昌凡 , 等 . 基于 Adaline 神经网络参数辨识的 PMSM 鲁棒电流预测控制 [J]. 电机与控制学报 , 2023, 27(4):127-139.

[18] 马燕峰 , 李鑫 , 赵书强 . 考虑储能约束的神经网络 VSG 参数自适应控制策略 [J]. 华北电力大学学报 (自然科学版), 2024, 51(4):57-68.

【作者简介】

林金妹（1996—），女，广西梧州人，本科，研究方向：网络安全。

韦冰东（1997—），男，广西南宁人，本科，研究方向：网络安全。

（收稿日期：2024-10-23）