基于改进径向基函数前馈神经模型的计算机网络入侵检测技术

吴茂雪[1] 徐 杰[1]
WU Maoxue XU Jie

摘 要 为防范局域网面临的 DoS（denial of service）拒绝服务攻击、SQL（structured query language）代码注入攻击、恶意软件攻击、MIMT 中间人攻击、DNS 欺诈等入侵威胁，提出基于径向基函数（radial basis function）前馈神经网络算法，在输入层利用径向基神经元对被测入侵数据集作出异常样本特征检测、分类概率计算，基于竞争神经元作出同一类样本的概率加权累计，同时引入蚁群（ant colony optimization）算法对 RBF 深度神经网络算法的异常数据寻优能力作出优化。实验结果表明，基于改进 ACO-RBF 神经网络模型的入侵攻击检测方案，得到的异常数据包流量检测精度为 98.04%、误报率为 5.36%，相比 LSTM 神经网络算法有着更为良好的网络入侵检测效果。

关键词 改进 ACO-RBF 前馈神经模型；计算机网络；入侵检测；技术

doi：10.3969/j.issn.1672-9528.2024.10.037

0 引言

随着大数据及云计算技术、SDN（software defined network）软件定义网络的快速发展，面向云平台网元化的数据流量传输成为主流，但大数据网络中海量化的数据资源传输、频繁的应用程序调用会产生潜在的网络安全问题。传统基于网络路由防火墙、部署于交换机的入侵检测 IDS（intrusion detection systems）系统进行网络异常流量的监测分析，存在面向远程或非授权攻击行为识别的准确率低、误报率高的问题，在这一背景下引入改进 ACO-RBF 前馈神经网络模型，由径向基神经元、竞争神经元实时捕获网络信道的数据流量，在网络算法模型的隐含层对输入待测网络数据集作出筛选、数值化、归一化处理与分类提取，可实现网络正常数据、异常数据包流量的特征值提取与分类，且改进径向基函数算法具有良好的自适应学习性、迭代训练容错性，能够满足大数据网络海量用户访问、入侵攻击的安全检测需求。

1 网络入侵检测中应用改进 ACO-RBF 神经网络模型的优势

依托复合型防火墙的网络入侵攻击安全检测方式，是针对用户访问的源 IP 地址 / 目的 IP 地址、源端口 / 目的端口、TCP/IP 通信协议等五元组信息，设置“Sip=192.168.x.x/xx and dip=192.168.x.x”“action=permit”等深度包过滤规则，将外部入侵用户的五元组信息、ACL 访问控制列表的包过滤规则作出条件匹配，验证网络数据包流量 IP 地址、“Type-*”字段类型、“length-*”内容描述、“UTC-*”时间戳的合法性，若不合法则代理网关拒绝用户的网络通信连接[1]。

而部署于路由器、交换机的 IDS 入侵检测系统，被称为网络防火墙后的第二道“安全闸门”。IDS 入侵检测系统包括事件探测器、分析器、响应单元等组成结构。面对不同类型的网络入侵攻击，先由 Suricata/Snort 入侵探测器监测入侵用户的 IP 地址、网络通信进程，随后按照“网络数据包流量监测——网关配置下发——访问日志收集——日志流量转发”的入侵数据感知流程，采集网络数据包的数字签名、异常日志信息，并将网络日志与设置的预定义规则列表作出匹配，及时发现入侵安全威胁并发出事件告警，具体的网络入侵检测与安全预警模型[2]如图 1 所示。

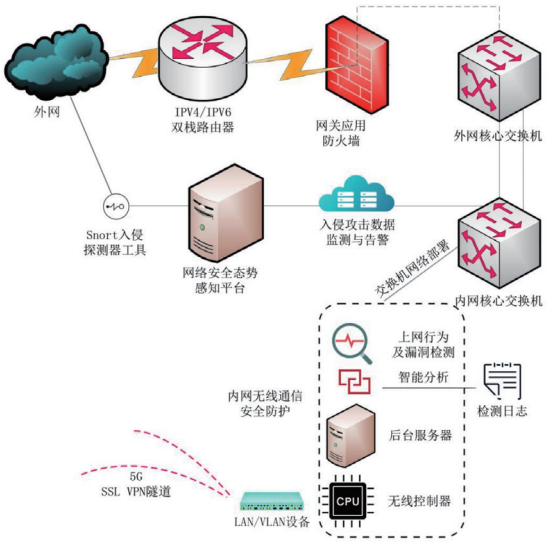

图 1 基于路由器、交换机的 IDS 网络入侵检测与安全预警模型

1. 贵州机电职业技术学院 贵州都匀 558000

由于远程非授权进入（remote to user）、DoS 拒绝服务攻击、U2R（user-to-root）提权攻击、Probe 探测攻击等类型的入侵，会绕过网络防火墙“一次认证与信任服务”的授权验证。因而在此情况下，引入改进 ACO-RBF 前馈神经网络模型的入侵检测方法，基于径向基神经元的自适应学习能力，从待测网络数据集中提取异常的数据样本特征、计算分类概率；运用竞争神经元的竞争机制建立从输入空间、输出空间的非线性映射，将不同攻击类型的入侵数据分配至特定的输出神经元，删除对入侵检测分类决策判定不起作用、冗余的特征数据，使得更新后的网络入侵检测数据更有代表性。

2 计算机网络入侵数据特征的数值化编码、归一化处理

2.1 外部入侵数据特征的数值化编码

当前网络入侵攻击数据包呈现出非数值化，每条数据记录内通常包含 IP 地址、字段类型、网络服务类型、内容描述、flag 标志位和时间戳等特征属性。为统一不同特征属性的数值意义，需要基于独热编码（one-hot encoding）法将每个类别化变量的取值转换为二进制特征向量，使每个类别成为独立的特征；基于标签编码法将每个类别化变量的取值转换为有序整数，保留类别变量之间的序列关系，在完成入侵攻击数据包的非数值化特征编码后，才能作出进一步的归一化处理、分类提取操作 [3]。

例如将网络入侵攻击目标主机的 IP 地址作为待数值化编码的特征属性，创建“encoder_input”二维数组作为 One-Hot 编码器的输入，攻击目标主机 IP 地址拆分为网络 ID（NetID）地址、宿主机 ID（HostID）地址等组成结构，按照“parts = ip_address.split= '129.45.8.22' one_hot_encoded_ip = one_hot_encode_ip(ip_address) print(one_hot_encoded_ip)”的执行代码，将十进制或十六进制的 IP 地址转换为二进制代码，得到的 8 位二进制代码可表示 '10000001 00101101 00001000 00010110'。而后基于标签编码法设置 0 ～ 100 的编码顺序，对入侵工具数据的不同特征属性进行状态编码，如对“http、smtp、finger、domain_u、auth、telnet、ftp、eco_i、ntp_u、ecr_i、other”等网络服务类型，将 0 ～ 10 的编号作为网络服务特征的数值化编码 [4]。

2.2 网络入侵攻击数据特征的归一化处理

在完成入侵数据特征的数值化编码后，需要将不同的输入特征向量作出归一化处理，使特征取值范围映射到特定的变化区间，逐行将每一维特征线性映射到诸如 $[a, b]$ 等的目标范围内，以消除不同特征值的量纲差异，也即若最小特征值映射为 a、最大特征值映射为 b，那么可用计算公式表示网络入侵数据特征向量的归一化处理结果：

$$x^{'} = a + \frac{(x - x_{\min})(b - a)}{x_{\max} - x_{\min}} \tag{1}$$

式中：$x_{\max}$ 和 $x_{\min}$ 分别表示归一化前入侵数据的最大、最小特征值，$[a, b]$ 表示归一化后线性映射的特征范围值。若特征线性转换后的均值映射为 0、标准差映射为 1，也即当 $x = x_{\min}$ 时 $x' = a = 0$，当 $x = x_{\max}$ 时 $x' = b = 1$ 符合标准的正态分布，那么可将网络入侵数据的有序整数特征值、统一归一化处理为 [0,1] 之间的数值，以式（1）的计算公式可转换为：

$$x^{'} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{2}$$

3 基于改进 ACO-RBF 神经网络算法的网络入侵攻击检测策略

径向基函数深度神经网络算法为前馈三层网络，通常涵盖输入层、隐含层、输出层等组成结构（如图 2 所示）。其中，输入层含有 $\{X_1, X_2, \cdots, X_n\}$ 的 n 个径向基神经元，用于向隐含层传输数据特征信号，由输入层到隐含层的非线性变换可表示为 $X_n \rightarrow \boldsymbol{C}_o$；而后在隐含层利用 o 个竞争神经元节点，对输入特征变量作出非线性变换的映射计算，得出输入特征向量 $\boldsymbol{x}'$、神经元的数据中心矢量 $\boldsymbol{C}_j$ 之间的欧几里得距离，将同一类特征样本作出概率加权累计 [5-6]。

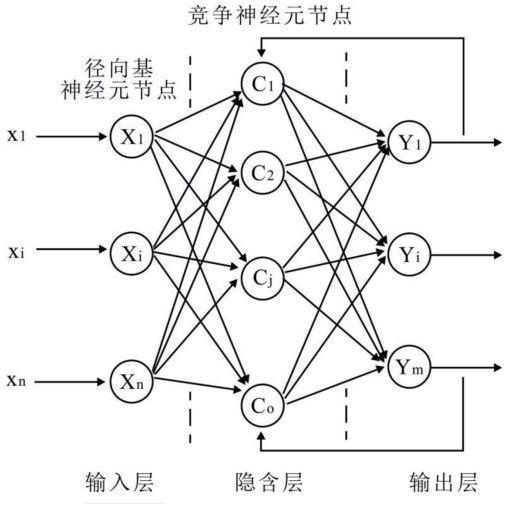

图 2 径向基函数深度神经网络算法结构

3.1 基于 RBF 前馈神经网络算法的网络入侵攻击检测

在 RBF 前馈神经网络结构中，输入初始化处理后的网络入侵数据特征值为 $\{x_1', x_2', \cdots, x_n'\}$，$n$ 个径向基神经元节点用于接收多维的网络入侵特征向量，而后将其传输至隐含层节点并作特征向量、数据中心矢量的欧几里得距离计算，具体公式为：

$$h_j = \exp\left(-\frac{\left\|x_i^{'} - C_j\right\|^2}{2\sigma_j^2}\right) \tag{3}$$

式中：$\boldsymbol{H}=[h_1, h_2, \cdots, h_j, \cdots, h_n]$ 表示径向基函数；$\boldsymbol{\sigma}$ 表示径向基函数的扩展宽度向量且 $\boldsymbol{\sigma}=[\sigma_1, \sigma_2, \cdots, \sigma_j, \cdots, \sigma_n]$；$\{\boldsymbol{C}_1, \boldsymbol{C}_2, \cdots, \boldsymbol{C}_j, \cdots, \boldsymbol{C}_o\}$ 表示神经网络中隐含层节点的中心矢量；‖‖表示欧式范数。若输入层、隐含层间的连接权值为 ω_{ij}，则经隐含层竞争神经元处理后的入侵攻击数据特征向量输出结果可表示为：

$$y_j=\sum_{i=1}^{n}\sum_{j=1}^{m}\omega_{ij}\exp\left(-\frac{\left\|x_i'-C_j\right\|^2}{2\sigma_j^2}\right)\quad \omega_{ij}=\frac{c_{\max}}{\sqrt{2o}} \tag{4}$$

式中：y_j 表示隐含层节点输出的入侵攻击数据特征向量值，$c_{\max}$ 表示不同数据中心矢量监督最大距离，o 表示隐含层的神经元节点数。按照 $[A, B, \cdots, G]$ 等的类别对入侵攻击数据特征属性作出归类，每个竞争神经元计算同类特征属性输出值的加权，估计输出特征向量属于特定入侵攻击类别的概率，计算公式 [7-8] 为：

$$p\left(y_j|C_j(A,B,\ldots,G)\right)=\frac{1}{N(A,B,\ldots,G)\cdot 2\pi^{n/2}\cdot\sigma^n}\sum_{i=1}^{n}\sum_{j=1}^{m}\omega_{ij}\exp\left(-\frac{\left\|x_i'-C_j(A,B,\ldots,G)\right\|^2}{2\sigma_j^2}\right) \tag{5}$$

式中：$N(A, B, \cdots, G)$ 表示特征属性为 $[A, B, \cdots, G]$ 等类别的样本数量。可按照不同分类样本输出的时间序列，对得到的入侵攻击数据结果作出排序。但由于隐含层神经元节点的中心、节点个数设置，会影响算法的入侵攻击数据监测精度、样本泛化能力，因而通过引入蚁群算法优化径向基函数的宽度、连接权值，以便保证隐含层神经元节点中心选择的自适应寻优，使得不同入侵攻击数据特征值被分配到更合理的节点，并作出迭代训练计算 [9]。

3.2 基于 ACO 蚁群寻优算法的 RBF 前馈神经网络优化

蚁群算法为效仿蚂蚁行走路径的节点寻优方法，主要根据路径节点的信息素浓度选择行进的方向，蚂蚁能够选择具有更高信息素浓度的路径作出寻优更新。引申至 RBF 前馈神经网络的节点寻优方面，是在 t 时刻由径向基神经元节点自适应选择特定隐含层节点，通常涵盖偏正态分布参数估计、相似度矩阵计量、蚁群寻优计算等执行流程 [10]。

（1）偏正态分布参数确定。当入侵攻击数据特征向量的输出结果、输出特征向量属于特定入侵攻击类别的概率不发生变化时，也即算法的全局极值固定后可能陷入局部最优解。为解决这一问题，先基于偏正态分布用于衡量入侵攻击数据特征值的分布对称性，根据输入的网络入侵数据特征值 $\{x_1', x_2', \cdots, x_n'\}$，计算数据特征值的均值、中位数及标准差，利用式（6）计算得出入侵数据特征值的偏度系数，用于衡量入侵攻击数据的分布对称情况。若偏度系数 SK 为 0，则表明入侵攻击数据特征的分布对称，否则当偏度系数大于或小于 0 时，表明入侵攻击数据呈现偏上或偏下分布形态。

$$\mathrm{SK}=\frac{\sum_{i=1}^{n}\left(x_i'-\bar{x}'\right)^3}{nS^3} \tag{6}$$

式中：$\bar{x}'$ 表示入侵数据特征属性的平均值，S 表示入侵数据特征属性的标准差值。偏度系数主要按照入侵数据特征值多阶中心距的计算结果，来定义其为正值或负值。偏度系数的绝对值越大，表明入侵攻击数据偏离输入层神经元节点中心位置的程度越大。

（2）关联度矩阵计量。相似度矩阵主要用于量化输入层径向基神经元、隐含层竞争神经元的关联度，基于输入层、隐含层不同节点间的连接权值 ω_{ij}，引入关联系数公式对输入层、隐含层的节点作出关联性度量，具体公式为：

$$\rho\left(X_i, C_j\right)=\frac{\omega_{ij}\operatorname{cov}\left(X_i, C_j\right)}{\sigma\left(X_i\right)} \tag{7}$$

式中：$\rho(X_i, C_j)$ 表示输入层节点、隐含层节点的关联系数，$\operatorname{cov}(X_i, C_j)$ 表示输入层节点 X_i、隐含层节点 C_j 的协方差，$\sigma(X_i)$ 表示径向基函数的宽度向量。

（3）隐含层节点的蚁群寻优计算。将入侵数据特征属性的偏度系数值 SK，以及输入层、隐含层不同节点间的连接权值 ω_{ij} 作为蚁群的信息素挥发因子，执行径向基神经元节点自适应的选择特定隐含层节点的计算流程，在 t 时刻进行隐含层节点蚁群寻优的计算公式 [6] 为：

$$P\left(X_i\mid t\right)=\left\{\begin{array}{ll}\dfrac{\mathrm{SK}\left[\omega_{C_j}(t)\right]^{\alpha}\left[\eta_{C_j}(t)\right]^{\beta}}{\sum_{s\in\text{allowed }X_i}\left[\omega_{C_j}(t)\right]^{\alpha}\left[\eta_{C_j}(t)\right]^{\beta}} & s\in\text{allowed }X_i\\ 0 & \text{else}\end{array}\right\} \tag{8}$$

式中：$P(X_i|t)$ 表示在 t 时刻输入节点 X_i 在隐含层中选择某一节点的概率；$s\in\text{allowed}X_i$ 表示在 t 时刻输入节点 X_i 能够选择的隐含层节点类别；$\omega_{C_j}(t)$ 表示隐含层中不同节点间的连接权值大小；$\eta_{C_j}(t)$ 表示隐含层中不同节点的重要性程度；α 和 β 分别表示蚁群信息素的信息启发因子、期望启发因子，信息启发式因子 α 越大，表明选择重复节点的概率越高，期望启发式因子 β 越大，表明算法的迭代收敛速度越快。

4 仿真实验及结果分析

4.1 实验环境设置

基于 Linux 网络操作系统、MVC（model-view-controller）软件开发框架、Tomcat 云服务器，以及 Intel Pentium® G5400T @3.10 GHz CPU 32 GB 1 TB 网络计算机、XeonE5-260 服务器等软硬件，搭建起面向改进 ACO-RBF 神经网络算法的入

侵攻击监测仿真实验平台。选用 UNSW-NB15 数据集作为入侵检测的实验数据，包含 1000 条的特征属性数据记录，分为正常（normal）数据、远程非授权进入（remote to user）、DoS 拒绝服务攻击、U2R（user-to-root）提权攻击、Probe 探测攻击等数据类型，基于 MATLAB R2022a 仿真软件执行改进 ACO-RBF 神经网络算法的网络安全态势感知环节，使之与 LSTM 长短期记忆神经网络算法的入侵攻击样本检测作出对比分析。

4.2 实验结果分析

根据以上基于 RBF 前馈神经网络算法的网络入侵攻击检测流程，对不同入侵攻击类别数据出现的概率作出特征提取、分类匹配与存储，设定算法最大迭代次数为 100 次，基于 ACO 蚁群寻优算法对 RBF 前馈神经网络的节点寻优选择过程作出优化，提取得到网络信道通信的非法入侵数据量实验结果如表 1、图 3 所示 [11]。

表 1 基于改进 ACO-RBF、LSTM 神经网络算法的网络入侵攻击监测结果

监测算法	准确率（Precision/%）	误报率（False/%）	检出率（DR/%）	攻击监测结果数据量 / 个
改进 ACO-RBF 神经网络算法	98.04	5.36	95.60	Normal:94;DOS:249;PRO:328;R2L:260;U2R:25
LSTM 神经网络算法	87.34	26.87	92.30	Normal:45;DOS:236;PRO:309;R2L:251;U2R:82

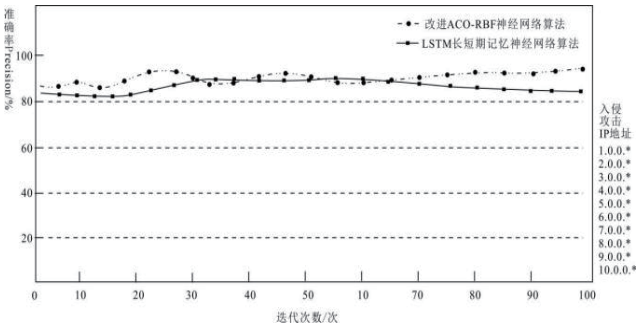

图 3 两种算法的网络入侵攻击监测结果

根据表 1、图 3 的仿真实验结果可得，基于改进 ACO-RBF 神经网络算法的入侵攻击样本数据特征属性分类监测，在检测准确率、误报率、检出率等方面相比 LSTM 神经网络算法都具有明显优势，且改进 ACO-RBF 神经网络算法将入侵攻击数据预测为正常数据的占比更小、检出率精度更高，面向 DOS、PRO、R2L、U2R 等入侵攻击类型的检出率为 95.60%，因而可最大程度满足大数据网络中外网访问的入侵攻击监测需求。

5 结语

采用传统复合型防火墙的 TCP/IP 通信协议、深度包过滤规则、ACL 访问控制列表规则等技术，已难以实现有效的网络安全监测和防御，为此基于改进 ACO-RBF 神经网络模型，设置输入层、隐含层、输出层，根据不同层级的连接权值进行网络入侵检测，由输出层 *m* 个神经元节点接收特征映射，输出分类完成的数据特征结果，所得到的网络入侵检测准确率、误报率相比 LSTM 神经网络算法更优。

参考文献：

[1] 景雯 , 张杰 . 基于区块链技术的无线传感网络入侵检测算法 [J]. 传感技术学报 ,2023(6):978-983.

[2] 陈立家 , 周为 , 许毅 , 等 . 一种基于 SDN 的多约束无人船网络传输路由算法 [J]. 中国舰船研究 ,2022(4):107-113.

[3] 刘拥民 , 杨钰津 , 罗皓懿 , 等 . 基于双向循环生成对抗网络的无线传感网入侵检测方法 [J]. 计算机应用 , 2023(1):160-168.

[4] 唐玺博 , 张立民 , 钟兆根 . 基于 ADASYN 与改进残差网络的入侵流量检测识别 [J]. 系统工程与电子技术 , 2022(12):3850-3862.

[5] 马明艳 , 陈伟 , 吴礼发 . 基于 CNN_BiLSTM 网络的入侵检测方法 [J]. 计算机工程与应用 , 2022(10):116-124.

[6] 陈解元 . 基于 LSTM 的卷积神经网络异常流量检测方法 [J]. 信息技术与网络安全 ,2021(7): 42-46.

[7] 刘珊珊 , 李根 , 管艺博 , 基于混合神经网络模型的低速率网络入侵检测研究 [J]. 成都工业学院学报 , 2024(1):52-56.

[8] 刘金硕 , 詹岱依 , 邓娟 , 等 . 基于深度神经网络和联邦学习的网络入侵检测 [J]. 计算机工程 , 2023,49(1):15-21.

[9] 魏明军 , 张鑫楠 , 刘亚志 , 等 . 一种基于 SSA-BRF 的网络入侵检测方法 [J]. 河北大学学报（自然科学版）, 2022, 42(5): 552-560.

[10]. 郭志民 , 周劼英 , 王丹 , 等 . 基于 Transformer 神经网络模型的网络入侵检测方法 [J]. 重庆大学学报 , 2021, 44(11):81-88.

[11] 宋洪涛 . 基于随机森林的无线通信网络入侵检测方法 [J]. 长江信息通信 , 2024(1):61-63.

【作者简介】

吴茂雪（1992—），女，贵州都匀人，本科，助教，研究方向：计算机软件。

徐杰（1991—），男，贵州都匀人，本科，助教，研究方向：计算机网络。

（收稿日期：2024-07-11）