基于深度径向智能的拒绝服务攻击检测

袁明兰[1] 李 林[2] 何守亮[3]

[1](重庆商务职业学院商贸管理系 重庆 401331)

[2](电子科技大学信息与软件工程学院 四川 成都 610054)

[3](重庆旅游职业学院智能制造与旅游交通系 重庆 409099)

摘 要 为了解决基于机器学习的攻击检测系统梯度消失和陷入局部最小值的问题,提出一种基于深度径向智能(Deep Radial Intelligence, DeeRaI)的拒绝服务检测系统。使用从具有不同抽象级别的径向基函数中提取的智能信息来训练 DeeRaI 网络,得到训练样本特征之间的相关性;使用积累化身(Cumulative Incarnation, CuI)算法优化 DeeRaI 网络权重,生成最佳权重。实验结果表明,DeeRaI 拒绝服务攻击检测系统学习收敛速度更快,并且在检测率、准确率、误报率和误差率性能方面优于现有其他方法。

关键词 DoS 攻击 局部最小值 深度径向智能 累积化身

中图分类号 TP393 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.12.050

DENIAL OF SERVICE ATTACK DETECTION BASED ON DEEP RADIAL INTELLIGENCE

Yuan Minglan[1] Li Lin[2] He Shouliang[3]

[1](*Department of Commerce and Trade Management, Chongqing Business Vocational College, Chongqing 401331, China*)

[2](*School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, Sichuan, China*)

[3](*Department of Intelligent Manufacturing and Tourism Transportation, Chongqing Vocational Institute of Tourism, Chongqing 409099, China*)

Abstract In order to solve the problem of gradient disappearance and getting stuck in the local minimum of attack detection system based on machine learning, this paper proposes a denial of service attack detection based on deep radial intelligence (DeeRaI). It used the intelligent information extracted from the radial basis function with different abstract levels to train the DeeRaI network and obtained the correlation between the features of the training samples. The cumulative incarnation (CuI) algorithm was used to optimize the DeeRaI network weights to generate the optimal weight. The experimental results show that the DeeRaI-based denial of service attack detection can learns faster, and is superior to other existing methods in detection rate, accuracy, false positive rate and error rate.

Keywords DoS attacks Local minimum Deep radial intelligence Cumulative incarnation

0 引 言

拒绝服务(Denial of Service, DoS)攻击利用当今的云基础架构来攻击关键 Web 服务[1],其目的是使计算机或网络无法提供正常的服务。DoS 攻击破坏性大,危害广,发生的频率高,攻击手段复杂,已经成为当今互联网最主要威胁之一[2]。目前基于异常的 DoS 攻击检测方法主要有统计、机器学习和数据挖掘。这些方法包括两个阶段,即培训和测试。培训阶段使模型通过识别特征和类来从训练数据中学习;测试阶段使用训练的模型对未知数据(没有类标签的输入数据)进行分类。机器学习方法主要分析数据中提取的关系,它分为监督学习、无监督学习、半监督学习和强

收稿日期:2019-07-18。重庆市教育委员会科学技术研究项目(KJQN201805301)。**袁明兰**,副教授,主研领域:计算机网络与软件技术。**李林**,副教授。**何守亮**,副教授。

化学习[3]。在本文中,使用监督学习作为训练样本已知的类标签。

径向基函数(Radial Basis Function,RBF)神经网络是具有单隐层的三层前向网络,第一层输入层接收输入的数据,第二层隐藏层负责将输入空间映射到隐藏空间,第三层输出层是对输入模式作出的响应[4]。隐藏层中包含高斯函数,输出响应随着输入数据中心位置的变化而变化,距离中心越近响应越大[5],反之亦然。在本文中,RBF 用于提取特征数据中隐藏的智能信息。

提取隐藏的特征信息和权值优化是 DoS 攻击检测系统需要解决的关键问题。近年来,有关 DoS 攻击检测系统的研究已取得若干成果。文献[6]提出了一种基于熵和粒度计算的拒绝服务攻击特征选择算法,该算法利用熵计算每个属性的权重来识别 DoS 攻击,利用 NSL-KDD 数据集给出基于用户自定义选择粒度的潜在属性选择方法。文献[7]提出了一种基于模拟退火特征选择方法的拒绝服务攻击检测系统,该系统利用模拟退火算法选择最优特征来识别拒绝服务攻击。文献[8]提出了一种建模网络流量统计分布的方法,用于特定目的异常网络(分布式拒绝服务攻击)检测,该方法充分利用了原始极限学习机的良好性能和计算时间比,但是其需要有简单的更新规则,使模型随着新流量和主机的进入而及时更新。

在研究了现有 DoS 攻击检测系统的基础上,为了使学习快速收敛且不陷入局部最小值,本文提出一个新的 DoS 攻击检测系统,即基于深度径向智能(DeeRaI)分析的拒绝服务攻击检测系统,并将积累化身(Cumulative Incarnation, CuI)算法应用于 DeeRaI 网络的学习。该方法从具有不同抽象级别的 RBF 中提取隐藏的智能信息,逐层计算训练样本特征之间的相关性,为了增强学习过程,将 CuI 算法应用于 DeeRaI 网络,以此生成最佳拟合权重。该方法缩短了学习时间,并且在不陷入局部极小值的情况下逐渐收敛。

1　具有累积化身优化的深度径向智能

DeeRaI 从第一个隐藏层中提取的 RBF 神经网络的智能信息训练网络,用 CuI 算法优化 DeeRaI 网络权重,生成最佳拟合权重。具有 CuI 优化的 DeeRaI 的方框示意图如图 1 所示,该方法包括 2 个阶段,即培训和测试,其中:训练阶段表示用实线表示;测试阶段用虚线表示。

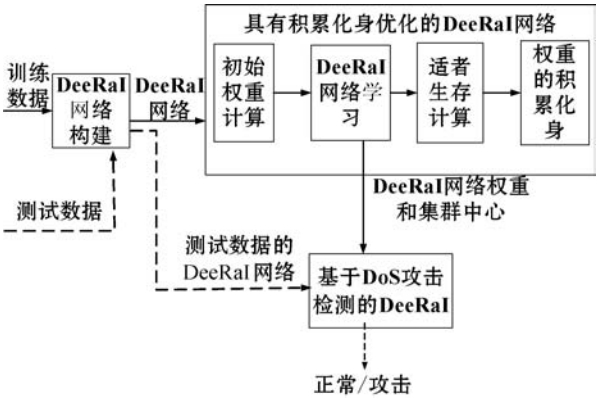

图 1　具有 CuI 优化的 DeeRaI 的方框示意图

1.1　DeeRaI 网络设计

DeeRaI 网络是 RBF 和 DL 神经网络的混合,它采用了 s-5-4-3-2-1 结构,输入层由 s 个节点组成,由输入要素的数量决定;隐藏层共有四层,第一个、第二个、第三个和第四个隐藏层中分别有 5、4、3 和 2 个节点;输出层只有 1 个节点。第一个隐藏层用于形成输入值的非线性映射,由于径向智能的中心计算要求,本文在第一个隐藏层中选择 5 个节点,使用 k 均值聚类法[9]计算中心;从第二个隐藏层到最后一个隐藏层是基于试错法设计的,使用带有激活函数整流线性单元(Rectified Linear Unit, ReLU)的 DL 方法[10],采用4-3-2 结构以循序渐进的方式逐层地学习提取的智能信息。

具有 s-5-4-3-2-1 结构的 DeeRaI 网络如图 2 所示。归一化特征 $F_1,F_2,\cdots,F_S$作为输入传递到输入层,输入层的输入神经元 $I_1,I_2,\cdots,I_S$保存并传递输入的值。从第一个隐藏层开始计算,隐藏的神经元表示为 $H_{ef}(1\leqslant e\leqslant 4,1\leqslant f\leqslant 5)$,其中:$e$ 表示隐藏层数;f 表示隐藏层中神经元的位置。O_1 表示输出层的神经元,C_{out} 表示DeeRaI网络的计算输出。

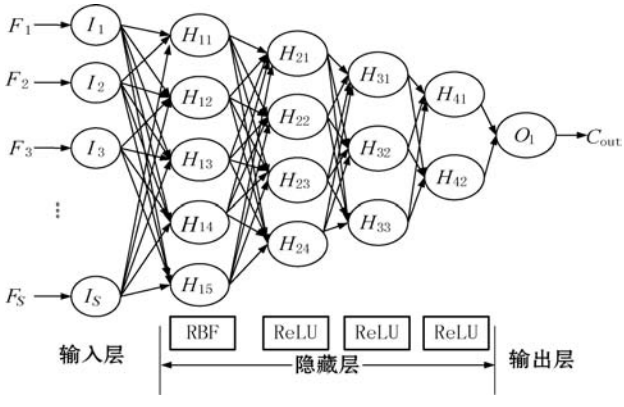

图 2　DeeRaI 网络

1.2　初始权重计算

神经网络的学习是通过权重进行的,因此神经网络中的初始权重对检测精度有着重要的作用,为了使网络快速学习,既需要正权重,也需要负权重。本文所

设计的权重计算过程是通过基于特征信息的最高有效位的面值为权重指定正负符号。初始权重计算模块中的术语基于遗传术语，所有生成解决方案的集合称为人口，每个群体由许多称为染色体的个体组成，染色体由基因组成，权重来自基因，通过计算 DeeRaI 网络所需的权重数来生成初始权重空间。

对于第一个隐藏层到第 e 个隐藏层所需的权重数量 $Wei_{\mathrm{H1}e}$ 的计算如式(1)所示，第 e 个隐藏层到输出层所需的权重数量 Wei_{Heo} 的计算如式(2)所示，DeeRaI 网络所需的权重总数如式(3)所示。

$$Wei_{\mathrm{H1e}} = N_{\mathrm{H1}} \times N_{\mathrm{He}} \tag{1}$$

$$Wei_{\mathrm{Heo}} = N_{\mathrm{He}} \times N_{\mathrm{O1}} \tag{2}$$

$$WeiTot = Wei_{\mathrm{H1}e} + Wei_{\mathrm{Heo}} \tag{3}$$

式中：N_{H1} 是第一隐藏层中的节点数；N_{He} 是第 e 个隐藏层中的节点数；N_{O1} 是输出层中的节点数。

图 3 为本文设计权重的提取过程，初始种群的第 i 个染色体表示为 $s_0, s_1, \cdots, s_{n-1}$。染色体的大小取决于学习所需的权重大小，假设染色体被分为 $WeiTot$ 个基因，权重的大小为 w，其中第一个数字决定权重的符号，剩余的数字位于小数点之后。因此，群体中个体的染色体大小计算如式(4)所示，基因 G_i 中提取重量 W_i 的数学表达式如式(5)所示。

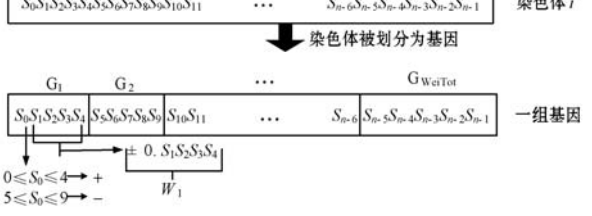

图 3 权重提取过程

$$C_{\mathrm{size}} = WeiTot \times w \tag{4}$$

$$W_i = \begin{cases} +\left(\begin{matrix} S_{wi-4}10^{-1} + S_{wi-3}10^{-2} + \\ S_{wi-2}10^{-3} + S_{wi-1}10^{-4} \end{matrix}\right) & 0 \leqslant S_{w(i-1)} \leqslant 4 \\ -\left(\begin{matrix} S_{wi-4}10^{-1} + S_{wi-3}10^{-2} + \\ S_{wi-2}10^{-3} + S_{wi-1}10^{-4} \end{matrix}\right) & 5 \leqslant S_{w(i-1)} \leqslant 9 \end{cases} \tag{5}$$

1.3 DeeRaI 网络学习

DeeRaI 网络学习被定义为能够使用从 RBF 中提取的智能信息来训练样本的 DL 网络，即通过对网络进行样本和权值训练，在更短的时间内找到特征数据之间的相关性。DeeRaI 网络学习特点是减少了学习时间，并通过克服消失的梯度问题来更快地检测到异常。

DeeRaI 网络学习将归一化的训练数据、五个聚类中心和初始权重作为输入，将学习的权重作为输出，最后将获得的学习权重用于攻击检测。输入层神经元的输出按式(6)计算；第一个隐藏层的输入为从 RBF 提取的输入特征的智能信息，其输出按式(7)计算；第二个隐藏层的输入是通过将相应的权重乘以第一个隐藏层的输出来计算的，如式(8)所示；第二个隐藏层的输出使用激活函数 ReLU 计算，如式(9)所示；与第二隐藏层算法相同，第三和第四隐藏层的输入和输出分别采用式(8)和式(9)计算，并使用相应的隐藏层输出和权重；输出层通过将相应的权重与最后一个隐藏层的输出相乘，计算 DeeRaI 网络的输出 C_{out}，并按式(10)添加偏移，偏置项将输出推送到适当的类。

$$O_q^1 = r_{sq} \tag{6}$$

$$H1_r = \exp^{-\| O_q^1 - C_k \|^2} \tag{7}$$

$$I_t^{H2} = \sum_{r=1}^{f} H1_r \times W_{ef}^{H1} \tag{8}$$

$$f(I_t^{H2}) = \max(I_t^{H2}, 0) \tag{9}$$

$$C_{\mathrm{out}} = \sum_{r=1}^{f} H3_r \times W_{ef}^{H3} + Bias \tag{10}$$

式中：r_{sq} 是具有 s 特征的第 q 个记录；O_q^1 为输入层的输出；$H1_r$ 为第一隐藏层的输出；C_k 是 k 均值聚类的结果，k 的取值范围是 1 到 5；I_t^{H2} 为第二隐藏层的输入；$f(I_t^{H2})$ 为第二隐藏层的输出；C_{out} 为 DeeRaI 网络输出；$Bias$ 为偏置项，本文偏置项取 1。

1.4 适者生存

适者生存(Survival of Fittest，SoF)函数可以量化解决方案的最优性，它是将特定的解决方案与其他所有解决方案进行排序，每个解决方案的适应度取决于它与问题最佳解决方案的接近程度。SoF 函数首先计算数据集里每个记录的误差，然后计算群体中每个个体的均方根误差(Root Mean Square Error，RMSE)，以此计算当前代中每个个体的 SoF 值。RMSE 是根据 DeeRaI 学习的输出和类标签来计算的，如式(11)所示，每个个体的 SoF 值按式(12)计算，种群中的个体根据 SoF 值进行排序，并将前 50% 的个体保留给下一代使用。

$$RMSE_{pj} = \sqrt{\sum_{t=1}^{n_t} \frac{(T_t - C_{\mathrm{out}})^2}{n_t}} \tag{11}$$

$$SoF_{pj} = \frac{1}{RMSE_{pj}} \tag{12}$$

式中：T_t 是数据集里每条记录的目标类；C_{out} 是计算输出；n_t 是训练记录的数量。

1.5 积累化身

神经网络的权重在训练过程中起主要作用，每代权重的随机生成导致 DeeRaI 学习不能很快收敛，因此需要对 DeeRaI 网络进行权重优化。现有的遗传算法

(Genetic Algorithm, GA)和差分进化(Differential Evolution, DE)算法均以随机方式产生新的权重。为了克服因权重的随机选择而导致局部极小值的问题,本文应用积累化身(CuI)算法来生成最佳权重,即通过计算最优拟合权重的累积和来生成新的权重实例。"累积化身"一词是指新的权重实例是根据前一代精英主义的最佳拟合权重计算出来的。

权重生成累积化身的过程如下:每个个体的权重根据当前 SoF 值排列,在上一代中排名前 50% 的权重(R1 至 R50)被选为下一代的精英,后 50% 的权重是根据最佳拟合权重 R1 – R50 计算的。第 51 个权重是 R1 和 R2 的平均值,第 52 个权重是 R1、R2 和 R3 的平均值,第 53 个权重是 R1、R2、R3 和 R4 的平均值,以此类推,第 99 个权重是 R1、R2、…、R49 和 R50 的平均值,第 100 个权重是 51 到 99 的平均值。因为新的权重群体是从前一代的最佳拟合权重生成的,所以这种权重优化方法可以产生更好的结果。

1.6　基于 DeeRaI 的 DoS 攻击检测

本文设计的基于 DeeRaI 的 DoS 攻击检测系统如图 4 所示。DoS 攻击检测系统的输入是训练阶段使用的聚类中心、学习训练数据后提取的权重,以及测试数据。针对给定的测试数据,构建 DeeRaI 网络,并利用聚类中心从第一个隐藏层提取径向智能信息,为所有层分配学习的权重,使用式(6)到式(10)逐层计算相应隐藏层的输入和输出。然后将计算的输出作为输入传递给检测函数(Detection Function, DetFun),如式(13)所示,如果 DetFun 的输出为 0,则给定的测试数据被归类为正常数据,否则将其归类为攻击。

$$DetFun = \begin{cases} 0 & C_{out} < 1 \\ 1 & 其他 \end{cases} \tag{13}$$

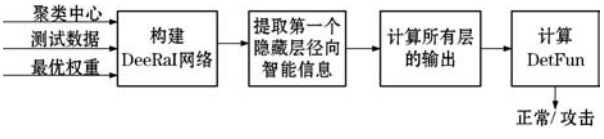

图 4　DeeRaI 的 DoS 攻击检测

2　实　验

为评估本文设计的系统,定义了下列性能指标:真阳性(True Positive, TP)是正确分类为攻击的攻击流量记录数;真阴性(True Negative, TN)是正确分类为正常流量的流量记录数;假阳性(False Positive, FP)是错误分类为攻击的正常流量记录数;假阴性(False Negative, FN)是错误分类为正常的攻击记录数。检测率(Ture Positive Rate, TPR)是指在所有攻击中检测到的攻击所占的比例,用式(14)计算;误报率(False Positive Rate, FPR)是指检测系统错误分类的网络流量的百分比,用式(15)计算;准确率(Accuracy, Acc)是攻击检测系统准确分类的数据比例,用式(16)计算;误差率(Error Rate, ER)是攻击检测系统错误分类的数据比例,用式(17)计算。

$$TPR = \frac{TP}{TP + FN} \times 100 \tag{14}$$

$$FPR = \frac{FP}{FP + TN} \times 100 \tag{15}$$

$$Acc = \frac{TP + TN}{TP + FP + TN + FN} \times 100 \tag{16}$$

$$ER = \frac{FN + FP}{TP + TN + FN + FP} \times 100 \tag{17}$$

2.1　代数与绩效指标

DeeRaI 网络学习速度与收敛的代数有关,收敛的代数越少,DeeRaI 网络学习速度越快。实验在 MATLAB R2016B 上采用 NSL-KDD 数据集,分别利用 GA、DE 算法和 CuI 算法对 DeeRaI 网络进行优化,测试训练数据。

图 5 到图 8 描绘了本文方法在不同代数下的性能指标。可以看出,采用 CuI 算法的 DeeRaI 大约在第 350 代收敛,采用 DE 算法的 DeeRaI 网络接近第 500 代收敛,采用 GA 的 DeeRaI 网络接近第 450 代收敛。需要注意的是,收敛的代数越少,DeeRaI 网络学习速度越快。因此,与利用 GA 和 DE 算法的 DeeRaI 相比,利用 CuI 算法的 DeeRaI 学习训练数据花费的时间更少并且没有陷入局部最小值,并且与现有方法相比,本文方法收敛得更快。

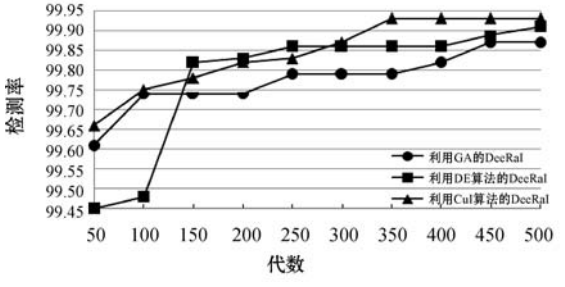

图 5　不同代数下的检测率

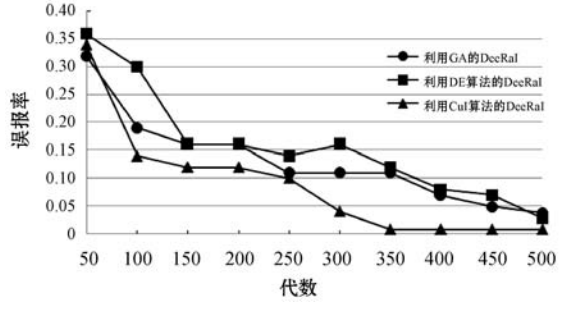

图 6　不同代数下的误报率

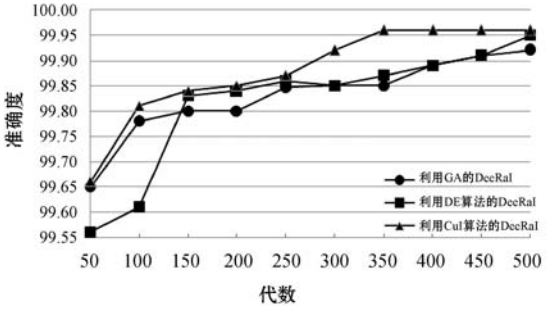

图 7 不同代数下的准确率

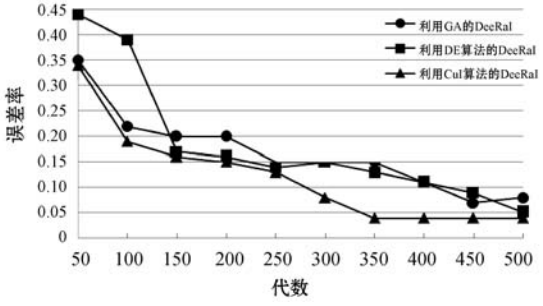

图 8 不同代数下的误差率

2.2 学习方法与绩效指标

实验在 MATLAB R2016B 上采用 NSL-KDD 数据集,将三种学习方法,即 RBF、DL 和 DeeRaI,分别使用 GA、DE 算法和 CuI 算法进行优化,并将其测试数据与未优化的学习方法测试数据进行比较。

图 9 到图 12 描绘了不同学习方法的性能指标,可以看出,与现有的学习方法和权重优化方法相比,使用 CuI 算法的 DeeRaI 具有更高的检测率和准确率,更低误报率和误差率。使用 CuI 算法的 RBF 性能不佳的原因是隐层节点的数量较少,使用 CuI 算法的 DL 性能不佳的原因是 DL 中没有智能提取组件,使用 CuI 算法的 DeeRaI 性能在权重优化和特征提取方面实现了改进。

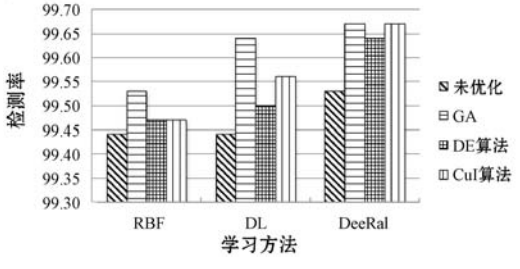

图 9 不同学习方法下的检测率

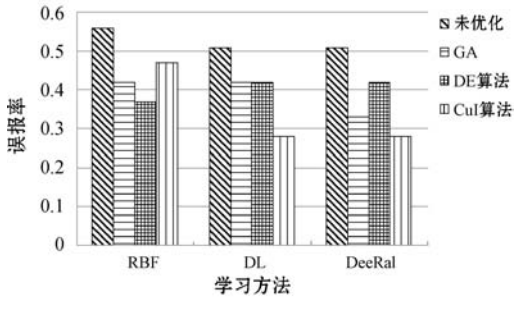

图 10 不同学习方法下的误报率

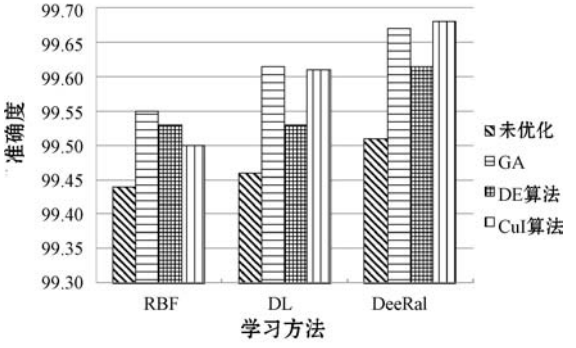

图 11 不同学习方法下的准确率

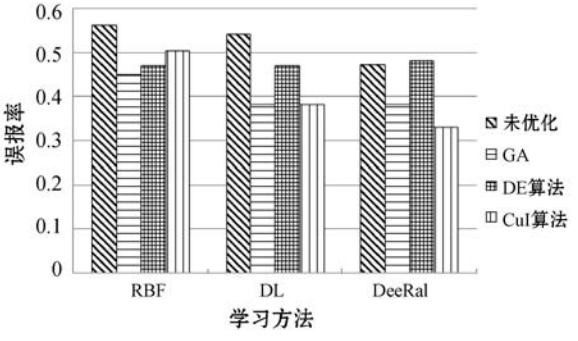

图 12 不同学习方法下的误差率

2.3 实验平台搭建与结果验证

为了验证所提算法在真实物理环境下的性能,本文用 5 个正常用户、1 个路由器、1 个 100 Mbit/s 网关、文件传输协议(File Transfer Protocol, FTP)服务器和黑客攻击端搭建了一个 DoS 攻击系统,实验环境的网络拓扑结构如图 13 所示。网络间的速率均为 100 Mbit/s,黑客随机发动 100 次攻击,随机选择每次攻击的时间起点。

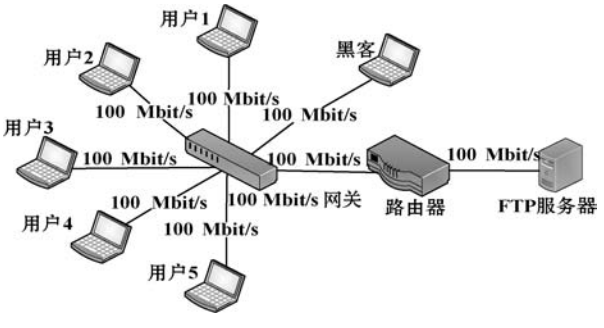

图 13 实验环境的网络拓扑结构

表 1 为本文算法与现有攻击检测系统中半监督机器学习方法[3]和基于自动编码器的特征学习方法[11]的准确率和误报率。

表 1 不同算法的检测结果比较 %

方法	准确率	误报率
半监督学习	83.34	30
自动编码器学习	98.23	33
本文算法	99.69	28

可见,本文算法在准确率和误报率方面都优于现有方法。本文通过使用激活函数 ReLU 从 RBF 网络中提取的智能信息进行学习,利用 CuI 算法获得了学习的权重,因此本文 DeeRaI 花费较少的学习时间,以较高的准确率实现拒绝服务检测。

3 结　语

为了克服机器学习法梯度的消失和由于随机选择权重陷入局部最小值等问题,本文提出一种 DeeRaI 学习网络拒绝服务(DoS)检测系统。从第一隐藏层中提取 RBF 神经网络的智能信息,将其用来训练 DeeRaI 网络,使用本文设计的方法提取 DeeRaI 网络的初始权重,使用积累化身(CuI)的算法生成最佳权重,获得的权重用于区分正常流量和 DoS 攻击流量。实验表明,本文方法在检测率、准确性、误报率和误差率性能方面均优于现有的其他方法,并且比现有的权重优化方法收敛得更快。未来的工作是考虑在多个入侵检测数据集上进行实验,从而更全面地验证所提算法的效果。

参　考　文　献

[1] Somani G, Gaur M S, Sanghi D, et al. DDoS attacks in cloud computing: Issues, taxonomy, and future directions [J]. Computer Communications, 2017, 107: 30 – 48.

[2] 陈超,曹晓梅. SDN 场景中基于双向流量特征的 DDoS 攻击检测方法[J]. 计算机应用研究, 2019,36(7):2148 – 2153.

[3] Idhammad M, Afdel K, Belouch M. Semi-supervised machine learning approach for DDoS detection[J]. Applied Intelligence, 2018, 48(10): 3193 – 3208.

[4] Agrawal S, Agrawal J, Kaur S, et al. A comparative study of fuzzy PSO and fuzzy SVD-based RBF neural network for multi-label classification[J]. Neural Computing and Applications, 2018, 29(1): 245 – 256.

[5] 孙玉杰,贺思艳,徐小龙,等. 神经网络补偿算法在基于 MEMS 的姿态检测中的应用[J]. 计算机应用研究,2019,36(9):2696 – 2699.

[6] Khan S, Gani A, Wahab A W A, et al. Feature selection of denial-of-service attacks using entropy and granular computing[J]. Arabian Journal for Science and Engineering, 2018, 43(2): 499 – 508.

[7] Jeong I S, Kim H K, Kim T H, et al. A feature selection approach based on simulated annealing for detecting various denial of service attacks[J]. Software Networking, 2018, 2016(1): 173 – 190.

[8] Kalliola A, Miche Y, Oliver I, et al. Learning flow characteristics distributions with ELM for distributed denial of service detection and mitigation [M]//Proceedings of ELM-2016. Springer, 2018: 129 – 143.

[9] Aljarah I, Faris H, Mirjalili S. Optimizing connection weights in neural networks using the whale optimization algorithm[J]. Soft Computing, 2018, 22(1): 1 – 15.

[10] Jiang X, Pang Y, Li X, et al. Deep neural networks with elastic rectified linear units for object recognition[J]. Neurocomputing, 2018, 275: 1132 – 1139.

[11] Yousefi-Azar M, Varadharajan V, Hamey L, et al. Autoencoder-based feature learning for cyber security applications [C]//2017 International Joint Conference on Neural Networks (IJCNN), 2017.

(上接第 265 页)

[14] 孙婷,向新,孙晔,等. 基于 Q-学习自适应蚁群算法的 CR 电频谱分配[J]. 电视技术,2014,38(19):72 – 75,84.

[15] 陈善学,张佳佳,朱江,等. 认知无线电网络遗传-蚁群联合优化路由算法[J]. 计算机工程与设计,2015,36(4):886 – 891.

(上接第 284 页)

[3] Gong Z, Long Y, Hong X, et al. Two certificateless aggregate signatures from bilinear maps [C]//Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. IEEE, 2007:188 – 193.

[4] Xiong H, Guan Z, Chen Z, et al. An efficient certificateless aggregate signature with constant pairing computations[J]. Information Science, 2013, 219:225 – 235.

[5] He D B, Tian M M, Chen J H. Insecurity of an efficient certificateless aggregate signature with constant pairing computations[J]. Information Sciences, 2014, 268:458 – 462.

[6] 侯红霞,张雪锋,董晓丽. 改进的无证书聚合签名方案[J]. 山东大学学报(理学版),2013,48(9):29 – 34.

[7] 王大星,滕济凯. 车载网中可证安全的无证书聚合签名算法[J]. 电子与信息学报,2018,40(1):11 – 17.

[8] 袁峰,程朝辉. SM9 标识密码算法综述[J]. 信息安全研究,2016,2(11):1008 – 1027.

[9] 赵楠,章国安,谷晓会. VANET 中隐私保护的无证书聚合签名方案[J]. 计算机工程,2020,46(1):114 – 120,128.

[10] 王大星,滕济凯. 车载传感网中基于聚合签名的认证方案[J]. 吉林大学学报(理学版),2018,56(3):657 – 662.

[11] 刘二根,王露,易传佳,等. 基于聚合签名的变电终端数据安全传输[J]. 计算机工程与设计,2019,40(7):1809 – 1815.

[12] Kilinc H H, Yanik T. A survey of SIP authentication and key agreement schemes [J]. IEEE Communications Surveys & Tutorials, 2014, 16(2):1005 – 1023.