Computer Science and Application 计算机科学与应用, 2016, 6(8), 505-513
Published Online August 2016 in Hans. http://www.hanspub.org/journal/csa
http://dx.doi.org/10.12677/csa.2016.68063

Hans汉斯

Research on Intrusion Detection Method Based on SOM Neural Network in Cloud Environment

Jin Zhao[1], Youchan Zhu[2]

[1]School of Control and Computer Engineering, North China Electric Power University, Baoding Hebei
[2]Information and Network Management Center, North China Electric Power University, Baoding Hebei
Email: du.lululu@163.com, zyc_hd@sina.com

Received: Jul. 30th, 2016; accepted: Aug. 15th, 2016; published: Aug. 23rd, 2016

Abstract

Cloud security has become an important challenge in the development of cloud computing. The intrusion detection system based on cloud computing will be an important part of the cloud security system. According to the characteristics and security requirements of cloud computing, an intrusion detection system model is designed for the cloud environment, and the SOM self-organizing feature map neural network algorithm is introduced into the intrusion detection algorithm. The random initialization of SOM network connection weights may lead to the failure of the training, so the particle swarm optimization algorithm based on simulated annealing is used to optimize the SOM neural network algorithm. The simulation experiment results show that the optimization algorithm can effectively improve the performance of intrusion detection.

Keywords

Intrusion Detection, SOM Neural Network, Particle Swarm Optimization Algorithm, Simulated Annealing Algorithm

云环境下基于SOM神经网络的入侵检测方法研究

赵　津[1]，朱有产[2]

文章引用: 赵津, 朱有产. 云环境下基于 SOM 神经网络的入侵检测方法研究[J]. 计算机科学与应用, 2016, 6(8): 505-513. http://dx.doi.org/10.12677/csa.2016.68063

[1]华北电力大学控制与计算机工程学院，河北 保定
[2]华北电力大学信息与网络管理中心，河北 保定
Email: du.lululu@163.com, zyc_hd@sina.com

收稿日期：2016年7月30日；录用日期：2016年8月15日；发布日期：2016年8月23日

摘 要

云安全已成为云计算发展过程中面临的重要挑战，基于云计算的入侵检测系统将成为云安全体系的重要组成部分。根据云计算特点和安全需求，设计了一种适合云环境的入侵检测系统模型，在入侵检测算法中引入SOM自组织特征映射神经网络算法，对SOM网络连接权值随机初始化可能导致的训练失败问题，采用基于模拟退火的微粒群算法对其进行优化，通过仿真实验验证优化算法可有效提高入侵检测性能。

关键词

入侵检测，SOM神经网络，微粒群算法，模拟退火算法

1. 引言

随着云计算服务在社会各领域的广泛应用，云环境下计算机系统和网络资源的安全性已成为云计算发展过程中面临的重要挑战。为了应对云环境的安全危机，基于云计算的入侵检测系统将成为云安全体系重要的组成部分[1]。入侵检测系统(Intrusion Detection System)通过分析流经网络的数据包、用户的行为、系统的安全记录、相关数据以及计算机系统某些关键点的信息，来判断是否发生了入侵行为。

传统的入侵检测系统在处理海量检测数据问题上难以满足实时性和有效性的要求，云计算强大的计算能力可以解决此瓶颈问题[2]。同时，神经网络具有的优势使其非常适合云环境下的入侵检测，目前专家学者的研究大多关注 BP 神经网络，对 SOM 网络的研究相对较少。根据云计算的特点和安全需求，设计出一种适合云环境的入侵检测系统模型。在核心检测分析模块的入侵检测算法部分，引入 SOM 自组织特征映射神经网络算法。在此基础上，针对 SOM 神经网络连接权值随机初始化可能导致的训练失败问题，使用微粒群算法和模拟退火算法相结合对其进行优化，提高入侵检测效率。

2. 云环境下的入侵检测系统模型

考虑到云环境的计算特点和安全需求[3]，设计的入侵检测系统模型如图 1 所示。每台云服务器安装入侵检测子系统，负责各自的入侵检测，每组云服务器集群设置一台入侵检测管理服务器，以自动检测和人工管理结合的方式对入侵检测系统进行管理，减少误报和漏报的概率。

在云服务器的入侵检测系统中，数据采集模块负责数据包的监听和捕获，数据预处理模块对捕获到的数据包进行协议解析、特征提取、数字标准化和归一化处理，并传送给检测分析模块。检测分析模块采取一定的入侵检测算法，根据入侵规则库对数据包进行分析，判断是否发生了入侵行为，若存在异常行为，则发送至响应模块并发出报警信息。

入侵检测管理服务器通过通信模块与云服务器通讯协作。容侵模块[4]对云服务器中的检测分析模块状态进行监控，当发现某个分析模块性能严重下降时，通知资源调度模块为该任务分配新的分析模块。资源调度模块收到检测请求后根据一定的调度算法分配新的检测分析模块。系统管理模块为管理员提供

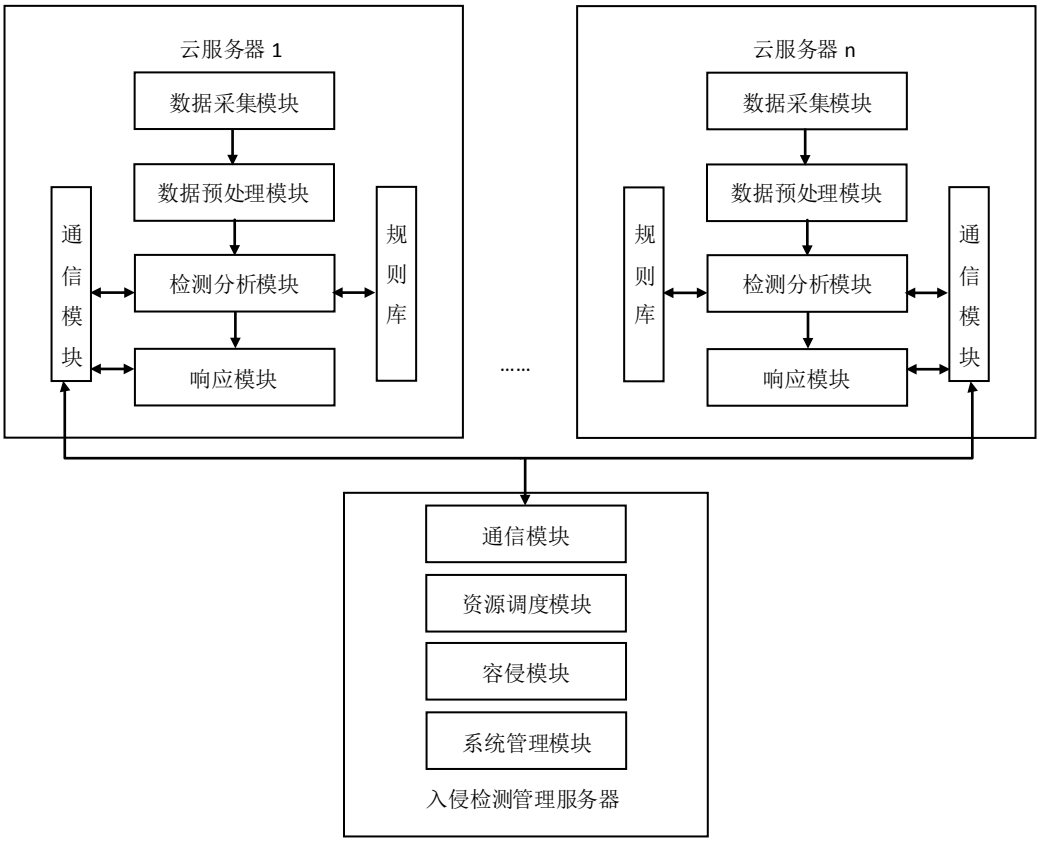

Figure 1. Intrusion detection system model
图 1. 入侵检测系统模型

了管理所有云服务器的系统平台，管理员可以查看云服务器中相关的系统日志，并根据系统运行状况对相关参数进行配置，以降低误报率和漏报率。

3. 基于 SOM 的入侵检测原理

3.1. SOM 概述

自组织特征映射神经网络(Self Organizing Map, SOM)是一种无导师学习的神经网络，通过自动寻找样本中内在规律和本质属性，自组织、自适应地改变网络参数与结构，并对具有共同特征的事物进行正确聚类[5]。

典型的 SOM 网络拓扑结构如图 2 所示，由输入层和输出层(竞争层)组成，输入层神经元与输出层神经元之间为全相连的权值向量，输出层之间实行侧向连接。输入层神经元个数由输入模式的特征数决定，通过权向量将外界信息汇集到输出层各神经元。

在 SOM 网络的训练阶段，输出层的神经元通过竞争学习的方式来获取对输入模式的响应，与输入模式最为相似的神经元为获胜神经元，获胜神经元及其优胜邻域内的所有神经元的权值向量均向输入模式方向作不同程度的调整。

经过训练后，输出层各神经元对特定模式类敏感，通过权值向量将相似的输入样本聚类，映射到某个神经元周围的样本属于同一类。当输入一个向量时，输出层与该模式类匹配的特定神经元将产生最大响应，从而将该输入向量自动归类。

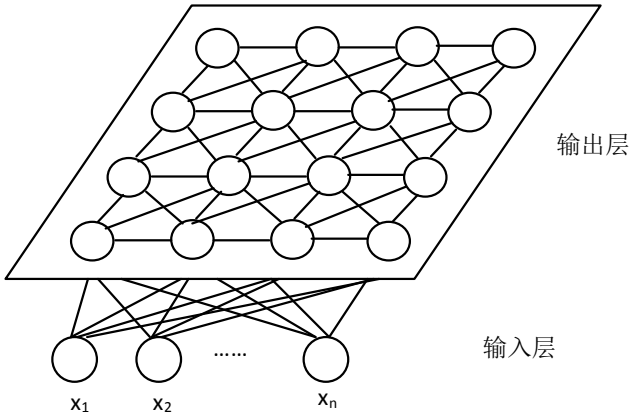

Figure 2. SOM neural network architecture
图 2. SOM 神经网络结构

3.2. SOM 神经网络算法

对应于上述运行原理，SOM 网络采用的学习算法按如下步骤进行。

假设训练样本维数为 n，则输入层神经元个数为 n，输出层神经元个数为 m，连接权向量为 $w_{ij}\left(i=1,2,\cdots,n;\ j=1,2,\cdots,m\right)$，每个训练样本输入向量为 $X=\left(x_1,x_2,\cdots,x_n\right)^{\mathrm{T}}$，令 $W_j=\left(w_{1j},w_{2j},\cdots,w_{nj}\right)^{\mathrm{T}}$ 为每个输出层神经元的连接权向量。

1) SOM 神经网络初始化：对连接权向量 $w_{ij}\left(i=1,2,\cdots,n;\ j=1,2,\cdots,m\right)$ 赋[0,1]区间内的随机小数，定义优胜邻域 $N_{j^*}(t)$ 的初始值 $N_{j^*}(0)$ 和学习率函数 $\eta(t)$ 的初始值 $\eta(0)$，定义最大学习次数 T。

2) 接收训练样本：从训练集中随机选取一个输入向量 $X=\left(x_1,x_2,\cdots,x_n\right)^{\mathrm{T}}$。

3) 寻找获胜神经元：计算各神经元的权值向量 W_j 和输入向量 X 的欧氏距离 d_j，找出所有 d_j 中的最小值 d_{j^*}，与 d_{j^*} 对应的神经元 j^* 即为获胜神经元。

$$d_j=\left\|X-W_j\right\|=\sqrt{\sum_{i=1}^{n}\left(x_i-w_{ij}\right)^2},\left(j=1,2,\cdots,m\right) \tag{1}$$

$$d_{j^*}=\min_{j\in\{1,2,\cdots,m\}}d_j \tag{2}$$

4) 调整权值：对优胜邻域 $N_{j^*}(t)$ 内的所有神经元调整权值：

$$w_{ij}(t+1)=w_{ij}(t)+\eta(t)\left[x_i-w_{ij}(t)\right],i=1,2,\cdots,n,\ j\in N_{j^*}(t) \tag{3}$$

5) 更新优胜邻域 $N_{j^*}(t)$ 和学习率 $\eta(t)$：确定 t 时刻的权值调整域和学习率，以获胜神经元 j^* 为中心，初始邻域 $N_{j^*}(0)$ 和学习率 $\eta(0)$ 较大，训练过程中 $N_{j^*}(t)$ 和 $\eta(t)$ 逐渐收缩。

$$\eta(t)=\eta(0)*\left(1-\frac{t}{T}\right),\ T\text{ 是最大学习次数} \tag{4}$$

$$N_{j^*}(t)=INT\left(N_{j^*}(0)*\left(1-\frac{t}{T}\right)+1\right),\ INT\text{ 为取整操作} \tag{5}$$

6) 判断训练是否结束：学习次数加 1，检查算法是否达到最大学习次数，或者学习率是否衰减至某个预定的正小数，是则训练结束；否则转到步骤 2 继续训练。

3.3. SOM 应用于入侵检测

SOM 神经网络中的各个神经元经过训练后，能将模式相近的输入样本聚类在拓扑结构相邻的区域中，

从而能够在数据类别未知的情况下对不同数据实行分类。入侵检测主要目标是要通过区分异常数据和正常数据，检测出异常行为。如果采用足够多的正常数据和异常数据对 SOM 网络进行训练，则训练后的 SOM 网络就可以有效识别异常行为。

4. SOM 神经网络算法的优化

4.1. 基本思想

常规 SOM 网络算法中，初始连接权向量是随机生成的，若选取不当，不仅会影响到网络训练的速度，而且还会直接地影响到网络的分类精度，甚至导致训练失败。为解决这一问题，本文提出微粒群算法对 SOM 算法进行优化，用微粒群算法来选取最优的 SOM 网络初始连接权值，利用微粒群算法参数少寻优能力强的优点，将算法迭代得到的最优解作为初始连接权向量。

然而，微粒群算法最大的局限性就是容易陷入局部极值点，导致得不到全局最优解[6]。模拟退火算法是一种有效的全局优化算法，在迭代过程中可以接受较差解，增加了搜索过程的灵活性，扩大了搜索范围，跳出局部极值点得到全局最优解的能力较强。因而将模拟退火思想引入到微粒群算法中，利用基于模拟退火的微粒群算法寻找 SOM 网络最优初始连接权向量，可以提高算法的收敛速度和分类精度。

4.2. 微粒群算法

微粒群优化算法(Particle Swarm Optimization, PSO)是一种基于群体智能的随机优化技术。PSO 算法将待优化问题的每个可能解表述为种群中的一个微粒，每个微粒有自己的位置向量、速度向量和一个由目标函数决定的适应度。所有微粒在搜索空间中以一定的速度飞行，通过追随当前搜索到的最优解来寻找全局最优解。

假设在 D 维搜索空间中，有一个规模为 m 的微粒群，第 i 个微粒的位置表示为 $X_i=(x_{i1},x_{i2},\cdots,x_{iD})$，其飞行速度为 $V_i=(v_{i1},v_{i2},\cdots,v_{iD})$，它经历过的最好位置即个体极值点为 $P_i=(p_{i1},p_{i2},\cdots,p_{iD})$，对应的适应值即为个体极值 Pbest，种群中所有微粒经历过的最好位置即全局极值点为 $P_g=(p_{g1},p_{g2},\cdots,p_{gD})$，对应的适应值即为全局最优解 Gbest。在每次迭代中，微粒通过跟踪个体极值和全局最优解来更新自己的速度和位置：

$$v_{id}(t+1)=w(t)v_{id}(t)+c_1r_1(p_{id}-x_{id}(t))+c_2r_2(p_{gd}-x_{id}(t)) \tag{6}$$

$$x_{id}(t+1)=x_{id}(t)+v_{id}(t+1) \tag{7}$$

其中，t 表示当前迭代次数，$v_{id}(t)$ 表示第 i 个微粒在第 d 维的速度，$x_{id}(t)$ 表示第 i 个微粒在第 d 维的位置，p_{id} 表示第 i 个微粒的个体极值在第 d 维的分量，p_{gd} 表示全局最优解在第 d 维的分量；C_1 和 C_2 是学习因子，通常取值为 2，r_1 和 r_2 是[0,1]之间的随机数；$w(t)$ 是惯性权重，应随着迭代次数增加而线性减少，采用较多的是 Shi 建议的线性递减权值策略[7] [8]，T 是最大迭代次数：

$$w(t)=0.9-\frac{t}{T}*0.5 \tag{8}$$

4.3. 基于模拟退火的微粒群算法

模拟退火算法(Simulated Annealing, SA)来源于物理中固体物质退火过程与组合优化问题之间的相似性，具有渐进收敛性，在理论上已被证明以概率 1 收敛于全局最优解。SA 算法在进行优化时采用 Metropolis 接受准则。首先设定一个足够高的初始温度，随机选择一个初始状态并得到该状态的目标函数值，对当前状态附加一个小扰动，计算新状态的目标函数值，以概率 1 接受目标值较优点，以线性递减概率

$p=\exp\left(-\Delta f/T\left(k\right)\right)>random\left(0,1\right)$ 接受较差点作为当前点，伴随着温度不断下降迭代寻优，最终得到问题的全局最优解[9]。

本文将模拟退火算法思想引入微粒群优化算法，在微粒位置速度迭代更新过程中加入模拟退火概率机制，对微粒更新后的适应值按接受准则接受优化解的同时，也以适当的概率接受恶化解，从而使算法从可能的局部极值中跳出，最终收敛至全局最优解。

基于模拟退火的微粒群算法描述为：

1) 假设种群中包含 m 个微粒，随机初始化各个微粒的位置 X_i 与速度 V_i；初始化学习因子 C_1 和 C_2；初始化迭代次数 t 为 0，最大迭代次数为 $t_{\max}$；设置足够大的退火起始温度 $T(0)$、退火速度 α。

2) 将各个微粒初始位置设为个体极值点 P_i，计算每个微粒的适应值 $f\left(X_i\left(t\right)\right)$ 作为个体极值 Pbest，选择适应度最优的微粒位置设为全局极值点 P_g，对应的适应值设为 Gbest。

3) 根据公式(6)和(7)更新各微粒的位置和速度。

4) 计算每个微粒位置更新前后所引起的适应值的变化量 $\Delta f=f\left(X_i\left(t+1\right)\right)-f\left(X_i\left(t\right)\right)$，如果 $\Delta f<0$ 则接受新位置和新速度为当前位置和当前速度，否则如果 $p=\exp\left(-\Delta f/T\left(t\right)\right)>random\left(0,1\right)$ 成立，也同样接受。否则仍以更新前的位置和速度作为当前位置和当前速度。

5) 计算每个微粒的适应值，如果优于个体极值 Pbest，则设置当前位置为个体极值点 P_i，并用当前位置的适应值替换 Pbest。根据每个微粒的 Pbest 确定全局极值点 P_g 和 Gbest。

6) 迭代次数 $t=t+1$，根据公式(8)更新惯性权重，根据 $T\left(t+1\right)=\alpha*T\left(t\right)$ 更新退火温度。

7) 如果达到最大迭代次数或最优解达到收敛，则终止迭代，输出全局极值点和全局最优解，否则返回步骤 3 继续迭代。

4.4. 模拟退火微粒群算法优化 SOM 神经网络

使用模拟退火微粒群算法优化 SOM 神经网络，实质就是采用模拟退火微粒群算法训练 SOM 网络的最优初始连接权值，然后使用 SOM 网络来对数据进行分类。

4.4.1. 微粒的搜索维度

使用基于模拟退火的微粒群算法寻优目的是得到 SOM 神经网络的最优初始连接权向量，寻优结果得到的全局最优解的位置即为初始连接权值，因而微粒群中每个微粒的维度分量都应该对应 SOM 神经网络中的一个连接权值。假设 SOM 网络输入层由 n 个神经元组成，输出层由 m 个神经元组成，则连接权值个数为 $m\times n$，那么微粒的搜索维度也是 $m\times n$，令 $D=m\times n$，则每个微粒在搜索空间中的位置及飞行速度都是 D 维矢量。

4.4.2. 适应度函数

在模拟退火微粒群算法优化过程中，需要通过一定的适应度函数来评估微粒的优劣，进而迭代得到最优解。SOM 神经网络不同于 BP 神经网络，它是无监督自组织的神经网络，无法利用输出层的误差作为评估准则。因而利用输入样本向量与微粒作为连接权向量时的相似程度作为评估准则[10]，数学描述如下。

假设 SOM 网络输入层神经元个数为 n，输出层神经元个数为 m，某个样本输入向量为 $X_i=\left(x_1,x_2,\cdots,x_n\right)^{\mathrm{T}}$，样本集中包含 N 个样本，表示为 $X=\left(X_1,X_2,\cdots,X_N\right)$；微粒群中每个微粒向量维度为 $D=m\times n$，位置表示为 $P_k=\left(p_1,p_2,\cdots,p_D\right)^{\mathrm{T}}$，每个维度分量对应 SOM 网络中的一个连接权向量。

当以微粒 P_k 作为连接权向量时，对于输入向量 X_i，根据公式(1)和(2)找到其对应的输出层获胜神经元 $j*$，定义 C 为 $j*$ 的连接权向量。

则适应度函数定义为：

$$f\left(P_k\right)=sqrt\left(\sum_{i=1}^{N}\left\|X_i-C\right\|^2\right) \tag{9}$$

4.4.3. 模拟退火微粒群优化 SOM 算法流程

1) 确定 SOM 神经网络结构，初始化网络相关参数，包括输入层和输出层神经元个数、优胜邻域函数及初值、学习率函数及初值。

2) 提供一组样本输入向量，按照 4.3 基于模拟退火的微粒群算法步骤执行算法迭代，其中适应度函数如式(9)。

3) 以得到的全局极值点作为 SOM 网络的初始连接权值，输入样本，训练 SOM 网络。

4) 利用训练收敛后的 SOM 网络实现数据的聚类。

5. 仿真实验与结果分析

为验证模拟退火微粒群优化 SOM 算法应用于入侵检测系统的高效性，分别对基本 SOM 算法、基于微粒群的 SOM 算法以及模拟退火微粒群 SOM 算法进行仿真对比实验。

5.1. 数据准备

实验采用 MIT 林肯实验室的 KDD CUP99 标准入侵检测数据集[11]，包含约 500 万条的训练数据和约 200 万条的测试数据。除正常数据类型 Normal 外，主要分为 DOS (拒绝服务)、Probe (探测攻击)、R2L (远程攻击)、U2R (本地非法提升权限)四大类攻击。

由于 KDD CUP99 数据集样本数量巨大，本次实验从中选择部分数据作为样本，具体样本分布见表 1。

数据集中每个样本都有 41 个特征属性和 1 个类标记，41 维的特征值中有数值型、离散型、字符型，为了便于 SOM 神经网络处理数据，需要对样本数据进行预处理，进行数值化、归一化操作。

5.2. 环境准备

实验主机配置为 Intel(R) Core(TM) i5-5200U CPU@2.20GHz，4GB RAM。操作系统为 Windows XP，编程工具为 MATLAB 7.0 以及 SOM 神经网络工具箱[12]。

SOM 神经网络参数设置：样本作为输入向量有 41 个特征值，因而输入层神经元有 41 个；输出层采用 5 × 5 二维平面阵；学习率初值设定为 0.9。模拟退火微粒群参数设置：微粒种群规模 $m = 50$，学习因子 $C_1 = C_2 = 2$，最大迭代次数 $t_{max} = 1000$；退火起始温度 $T(0) = 10000$，退火速度 $\alpha = 0.85$。

5.3. 结果分析

评价入侵检测算法时常采用三个性能指标：检测率、误报率、漏报率[13]。

Table 1. Sample set distribution
表 1. 样本集分布情况

数据类别	训练样本集	测试样本集
Normal	1500	900
DOS	600	350
Probe	250	150
R2L	150	50
U2R	50	30

检测率 = 检测出的攻击样本数/攻击样本总数 × 100%

误报率 = 被误报为攻击的正常样本数/正常样本总数 × 100%

漏报率 = 未检测出的攻击样本数/攻击样本总数 × 100%

针对基本 SOM 算法、基于微粒群的 SOM 算法以及模拟退火微粒群 SOM 算法三种算法进行入侵检测实验，分别统计其入侵检测率、误报率和漏报率，得到实验结果如下。

表 2 对比出三种算法的入侵检测率，检测率越高，说明入侵检测效果越好。使用基本 SOM 神经网络算法进行入侵检测时，检测率相对较低，经过微粒群算法优化后，检测率有所提高，再结合模拟退火算法的优势后，检测率显著提高，证明入侵检测效率提高。

表 3 和表 4 对比三种算法的误报率和漏报率，与检测率相反，二者的值越低，入侵检测效果越好。经过模拟退火和微粒群算法优化后，误报率和漏报率明显降低，同样证明入侵检测效率提高。

实验结果表明，相对于传统的 SOM 神经网络算法和基于微粒群的 SOM 算法，本文提出的模拟退火微粒群 SOM 算法具有较高的检测率，较低的误报率及漏报率，并且对常见的攻击类型都能够有效检测。这说明，模拟退火微粒群 SOM 算法针对传统 SOM 算法及微粒群算法存在的问题，起到优化作用，入侵检测性能更高。

Table 2. Comparison of intrusion detection algorithm detection rate
表 2. 入侵检测算法检测率对比

攻击类型	检测率 (%)		
	模拟退火微粒群 SOM 算法	微粒群 SOM 算法	SOM 算法
DOS	98.27	89.34	81.56
Probe	97.95	90.41	79.83
R2L	99.15	92.88	86.54
U2R	98.74	92.61	83.71

Table 3. Comparison of intrusion detection algorithm false positive rate
表 3. 入侵检测算法误报率对比

攻击类型	误报率 (%)		
	模拟退火微粒群 SOM 算法	微粒群 SOM 算法	SOM 算法
DOS	1.29	1.56	2.13
Probe	0.97	1.78	2.65
R2L	1.35	2.49	3.77
U2R	1.41	2.01	2.87

Table 4. Comparison of intrusion detection algorithm false negative rate
表 4. 入侵检测算法漏报率对比

攻击类型	漏报率 (%)		
	模拟退火微粒群 SOM 算法	微粒群 SOM 算法	SOM 算法
DOS	1.73	10.66	18.44
Probe	2.05	9.59	20.17
R2L	0.85	7.12	13.46
U2R	1.26	7.39	16.29

6. 小结

针对云安全问题，设计入侵检测系统模型，并介绍了关键模块的功能。在检测分析模块中，利用 SOM 神经网络算法无监督自组织的特性实现入侵检测功能。针对 SOM 算法的不足，提出基于模拟退火微粒群算法优化的 SOM 算法，并通过仿真实验验证了优化算法的高效性，提高入侵检测性能。

参考文献 (References)

[1] 冯登国, 张敏, 张妍, 徐震. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83.

[2] 刘伉伉. 云计算环境下入侵检测技术的研究[D]: [硕士学位论文]. 济南: 山东师范大学, 2015.

[3] 刘鹏. 云计算[M]. 第二版. 北京: 电子工业出版社, 2011.

[4] Mazzariello, C., Bifulco, R. and Canonico, R. (2010) Integrating a Network IDS into an Open Source Cloud Computing Environment. 2010 *Sixth International Conference on Information Assurance and Security* (*IAS*), Atlanta, 23-25 August 2010, 265-270.

[5] 谭秀辉. 自组织神经网络在信息处理中的应用研究[D]: [博士学位论文]. 太原: 中北大学, 2015.

[6] 王芳. 粒子群模拟退火融合算法及其在物流配送问题中的应用[D]: [硕士学位论文]. 上海: 华东理工大学, 2010.

[7] Shi, Y. and Eberhart, R.C. (1998) A Modified Particle Swarm Optimizer. *The* 1998 *IEEE International Conference on Evolutionary Computation Proceedings*, Anchorage, 4-9 May 1998, 69-73. http://dx.doi.org/10.1109/icec.1998.699146

[8] Shi, Y. and Eberhart, R.C. (1999) Empirical Study of Particle Swarm Optimization. *Proceedings of the* 1999 *Congress on Evolutionary Computation*, Washington DC, 6-9 July 1999, 1945-1950. http://dx.doi.org/10.1109/CEC.1999.785511

[9] 吴剑, 冯国瑞. 基于模拟退火和半监督聚类的入侵检测方法[J]. 计算机与现代化, 2014(11): 27-30.

[10] 涂晓芝, 颜学峰, 钱锋. PSO-SOM 分类判别研究及其应用[J]. 高技术通讯, 2006, 16(10): 1014-1018.

[11] KDD Cup 1999 Data Set (1999). http://archive.ics.uci.edu/ml/databases/kddcup99/kddcup99.html

[12] 飞思科技产品研发中心. MATLAB6.5 辅助神经网络分析与设计[M]. 北京: 电子工业出版社, 2003.

[13] 侯梅菊. 计算智能技术在入侵检测系统中的应用研究[D]: [硕士学位论文]. 重庆: 重庆大学, 2012.