云环境下基于改进 BP 算法的入侵检测模型

何文河[1],李陶深[1,2],黄汝维[1,2]
(1. 广西大学 计算机与电子信息学院,广西 南宁 530004;
2. 广西高校并行与分布式计算技术重点实验室,广西 南宁 530004)

摘 要:随着云计算技术的发展,商业云资源的使用成本越来越低,恶意用户可能利用云平台资源对同驻的虚拟机或者其他云平台实施入侵攻击。针对云服务的入侵攻击主要包括对虚拟机或监视器的攻击和后门通道攻击。针对现有云入侵检测系统仅能检测已知的攻击、对不同虚拟网络模型的兼容性较低、对攻击的变种的检测精度较低等问题,在分析 KVM 网络模型的基础上,提出一种云环境下基于改进 BP 算法的入侵检测模型(MBPCIDM)。该模型结合了 PSO 算法的全局寻优能力和 BP 算法的梯度下降局部搜索等特点,将 PSO 算法引入到 BP 的初始权值与阈值的优化,融入了动量项与自适应学习速率方法,使得 BP 网络更快收敛,且有效避免了算法陷入局部最优。实验结果表明,所提出的模型平均检出率较高,能为云环境提供入侵检测服务。

关键词:云安全;入侵检测;内核虚拟机;反向传播神经网络;粒子群优化算法
中图分类号:TP391 **文献标识码**:A **文章编号**:1673-629X(2016)02-0087-04
doi:10.3969/j.issn.1673-629X.2016.02.020

Intrusion Detection Model Based on Improved BP Algorithm in Cloud Environment

HE Wen-he[1],LI Tao-shen[1,2],HUANG Ru-wei[1,2]
(1. School of Computer,Electronics and Information,Guangxi University,Nanning 530004,China;
2. Key Laboratory of Parallel and Distributed Computing Technology of Guangxi Colleges and Universities,
Nanning 530004,China)

Abstract:With the development of cloud computing technology,the cost of commercial cloud resources is lower and lower,a malicious user could use the cloud resources in the same virtual machine or other cloud platform to implement intrusion attack. The intrusion attack for cloud service mainly includes the virtual machine or monitor attack and back channel attack. The existing cloud intrusion detection systems can only detect known attacks,cannot be applied to a virtualized environment that has different network models,and the detection accuracy of variant of attack is lower. Based on the analysis of the KVM network structures,an improved intrusion detection model based on BP algorithm in the cloud environment (MBPCIDM) was proposed. It combines the ability of searching global optimal solution of PSO algorithm and the feature of the gradient descent in local search of BP algorithm. To make the BP network convergence faster and prevent it from falling into local optimum,the momentum and adaptive learning rate method was also used in this paper. The experimental results show that the average detection rate of the proposed model is higher,it can provide intrusion detection services for cloud environments.

Key words:cloud security;intrusion detection;KVM;BP neural network;PSO algorithm

0 引 言

随着云资源的租金越来越低,恶意用户可以用较少的费用来租用虚拟硬件资源对同驻的虚拟机或者其他云平台实施入侵攻击,这对云平台的其他合法用户造成安全威胁。当前,云系统所面临的入侵攻击主要包括内部攻击、洪泛攻击、U2R 攻击、端口扫描、对虚拟机或监视器的攻击和后门通道攻击等[1]。目前,多数已有的云计算环境下的入侵检测系统仅能检测已知

收稿日期:2015-03-02 **修回日期**:2015-07-06 **网络出版时间**:2016-01-26
基金项目:国家自然科学基金资助项目(61363067);广西自然科学基金资助项目(2012GXNSFAA053226)
作者简介:何文河(1989-),男,硕士研究生,研究方向为云安全;李陶深,教授,博导,博士,研究方向为无线 Mesh 网络、分布式数据库、云计算等;黄汝维,副教授,硕导,博士,研究方向为云计算、云安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20160126.1517.004.html

的攻击,对已知攻击的变种的检测精度较低,难以兼容于 KVM(Kernel-based Virtual Machine,基于内核的虚拟机)环境下的不同网络模型。当前云计算环境中尚缺少一种实时高效的入侵检测模型。

1 相关研究

当前云环境中主流的网络安全技术主要包括加密、防火墙、入侵检测系统等[1]。文献[2]提出了一种新的虚拟化自检系统,以保护 KVM 环境下的虚拟机不受恶意攻击,但是此系统受限于所建立的规则,并且它的误检率和漏检率较高。文献[3]提出了一种为入侵检测系统建立一个高效模型从而获取最优特征数量的方法,该方法能降低检测攻击所需的计算机资源(存储和 CPU 时间),但是实时性和效率较低。为了在云端处理大量的网络访问流并管理控制数据与应用,文献[4]提出了一种新的多线程分布式云入侵检测模型,通过将知识与行为分析整合到入侵检测中,实现对大量数据流进行处理,分析并生成报告,但是模型实现较复杂,检测效率较低。文献[5]在开源云—Eucalyptus 上部署了基于 Snort[6] 的误用检测器,提出了一种快速且高效的方案,仅能检测已知攻击。文献[7]将入侵检测功能作为云平台的一种服务,以服务的形式给每个云用户配置一个 Snort 组件,只能检测网络层上的已知攻击。

当前多数研究所提出的入侵检测系统与虚拟化环境的网络模式的兼容性较低;多数系统仅能检测已知攻击,对未知攻击的检测率较低;多数研究仅涉及入侵检测,对于相应的防御模块未加讨论。

针对上述问题,文中在分析 KVM 网络模型的基础上,结合基于 PSO 的带动量因子与自适应速率的 BP 算法(MLPSO-BP),提出了一种云环境下基于改进 BP 神经网络的入侵检测模型(MBPCIDM),可以为云环境提供入侵检测服务。

2 KVM 下基于改进 BP 算法的入侵检测系统

2.1 基于软计算方法的入侵检测

软计算方法是入侵检测的常用方法,主要包括 BP 算法、PSO 算法。

(1)BP 算法的改进。

BP 网络对初始的权值很敏感,若设置不当会引起震荡影响与慢收敛速度,文献[8]将 PSO 用于优化 BP 的初始权值与阈值,用该算法构造出的入侵检测系统具有较高检测率。文中使用 PSO 来搜寻 BP 网络的最优初始权值与阈值。

(2)PSO 算法。

PSO 算法计算简单、鲁棒性较好,它在多维连续空间、神经网络训练、组合优化等优化问题上具有较好的性能[9]。基本的粒子群算法的位置与速度的更新公式如式(1)和式(2)所示:

$$v_i(t+1) = \omega(t)v_i(t) + c_1r_1(\mathrm{pBest}_i(t) - x_i(t)) + c_2r_2(\mathrm{gBest}(t) - x_i(t)) \quad (1)$$

$$x_i(t+1) = x_i(t) + v_i(t+1) \quad (2)$$

其中,v 为速度项;x 为位置项;i 为当前粒子编号;t 为当前迭代次数;c_1、c_2 为学习因子;r_1、r_2 为分布在[0,1]内的随机数;pBest 为单个粒子本身找到个体极值;gBest 为整个粒子群当前找到的全局极值。

(3)动量因子与自适应速率。

由文献[10]的分析可知,动量因子算法能够加快收敛速度,自适应速率算法能够避免陷入局部极小,两者从不同的方面解决了 BP 网络算法的不足。文中将其应用于 BP 网络中,以提高系统性能。

2.2 基于改进 BP 算法的入侵检测算法

2.2.1 算法设计思想

当前多数研究所提出的入侵检测系统仅能检测已知攻击,对已知攻击的变种的检测率较低;多数研究仅涉及入侵检测模块,而对于云环境下的相应防御模块未加讨论。

针对上述问题,文中设计了一个云环境下的入侵检测算法(MLPSO-BP),此算法采用了基于 PSO 的带动量因子与自适应速率的 BP 算法。

2.2.2 MLPSO-BP 算法设计

MLPSO-BP 算法描述如下:

步骤 1:初始化 BP 神经网络的初始参数,设置各层的节点数等等。

步骤 2:初始化 MPSO 参数,计算粒子的维度,初始化集群并生成粒子的参数,如初始位置和速度等。

步骤 3:依据式(3)计算各个粒子的适应度值,与当前最好的适应度值 pBest 进行比较,若该值更好,则更新 pBest,否则保持 pBest;比较 pBest 与全局最优值 gBest,若该值更好,用 pBest 更新 gBest,否则保持 gBest。

$$\mathrm{fitness} = 1/(1 + \frac{1}{2}\sum_{i=1}^{N}(y_i^d - y_i)^2) \quad (3)$$

其中,N 是 PSO-BP 的训练样本数;y_i^d 是第 i 个期望输出;y_i 是第 i 个实际输出。

步骤 4:更新惯性权重,再依据式(1)和式(2)调整粒子的位置与速度。

步骤 5:若当前迭代达到最大次数或者误差已经在给定的范围中则结束迭代过程,则当前的全局极值 gBest 视为 BP 神经网络的初始权值与阈值,寻优过程

结束,转步骤 5;否则,转步骤 3。

步骤 6:基于所得的初始权值与阈值和动量因子与自适应速率对 BP 网络进行训练与测试,据此建立入侵检测模型。

2.3　基于改进 BP 的入侵检测模型

为了使所设计算法兼容于 KVM 的不同网络模型,文中在结合已有研究的基础上,提出了一种新的云环境入侵检测模型。

2.3.1　KVM 网络模型研究

KVM 提供了两种基本的网络连接模式[11-12]:即 Ethernet-Tap 模式和用户模式。文献[13]基于 NAT 技术和网桥技术设计了一种新的网络连接模式:NAT+网桥模式。

(1)用户模式。

在用户模式下,用户发出的数据包由 QEMU 进程完成。利用所截获的客户发送或接收的数据包,无法识别攻击者的位置,因为这些数据包的源地址就是主机地址。此时,无法直接利用所提出的方法来进行入侵检测,需要通过动态迁移技术将发包系统调用超过特定次数的可疑虚拟机的用户模式改为独立的 NAT+网桥模式,依据 MLPSO-BP 算法,检测可疑虚拟机以判断入侵者的虚拟机。用户模式的网络结构见图 1。

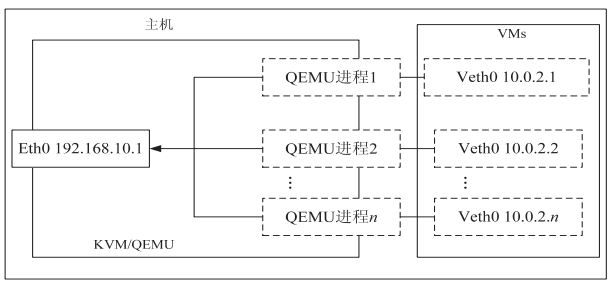

图 1　用户模式网络结构

(2)NAT+网桥模式。

在 NAT+网桥网络模式下,可以根据数据包的路径来确定数据包的发出者。通过主机端相同的令牌,可以利用 Tap 设备来截获相应客户发送或接收的数据包,然后依据 MLPSO-BP 算法来进行入侵检测。NAT+网桥模式如图 2 所示。

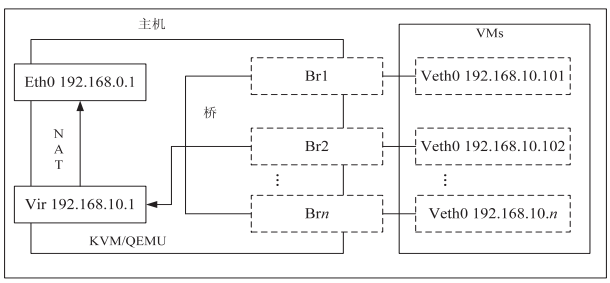

图 2　NAT+网桥模式网络结构

2.3.2　MBPCIDM 模型研究

为了将 MLPSO-BP 算法应用于云环境,此检测算法应当兼容于不同虚拟化网络模型。文中结合 KVM 下的 NAT+网桥模式网络结构,将所提出的 MLPSO-BP 算法应用于云入侵检测模型 MBPCIDM 中,见图 3。

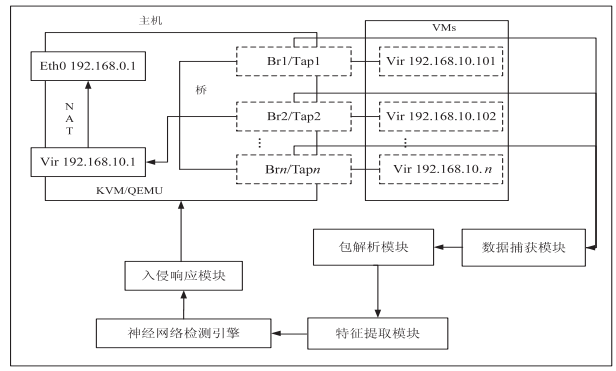

图 3　MBPCIDM 模型

模型中包含的模块介绍如下:

(1)数据捕获模块:依据虚拟化环境的网络模式(Ethernet-Tap 模式/用户模式/NAT+网桥模式)设置数据捕获方式,将所捕获数据提交给数据包解析模块。

(2)数据包解析模块:依据网络协议对所捕获的数据包进行解析,将解析结果提交给特征提取模块。

(3)特征提取模块:根据入侵检测系统所需的检测特征,从数据中提取出特定特征,将编码后的数据提交给神经网络检测引擎。

(4)神经网络检测引擎:依据改进的 BP 神经网络所构建的检测引擎,判断数据是否是入侵数据,将检测结果提交给入侵响应模块。

(5)入侵响应模块:根据检测结果,对可疑的恶意虚拟机进行相应的管理操作,如迁移、挂起、关闭和撤销等。

3　算法实验与性能分析

3.1　实验数据与指标

实验中所采用的入侵检测数据集是 KDD Cup 99[14],此数据集是较常用的入侵检测算法训练与测试数据。文中选取了其中 12 个特征作为输入样本,从数据集中挑出了 1 322 个记录,其中的 611 个样本用于检测算法的训练,其余样本用于测试。为了检验所提算法的性能,将实验结果与 PSO-BP 算法、BP 算法的实验结果进行对比。实验涉及的指标有:检测率、误检率和检测率。其中:

检测率=被正确检测的样本数/总样本数

漏检率=误检的入侵样本数/总样本数

误检率=被误检的正常数据数/总样本数

3.2　实验分析

为了分析系统性能,文中进行了 10 次实验,结果如图 4~6 所示。

由图 4 的检测率曲线的分布可知,MLPSO-BP 算

法的检测率要略高于单纯的 PSO-BP 算法,传统的 BP 算法的检测率低于前面两者。其原因在于:

(1)动量因子与自适应速率算法在加速 BP 算法收敛速度与避免陷入局部最小这两方面所起的作用;

(2)PSO 算法在全局寻优方面的优势。

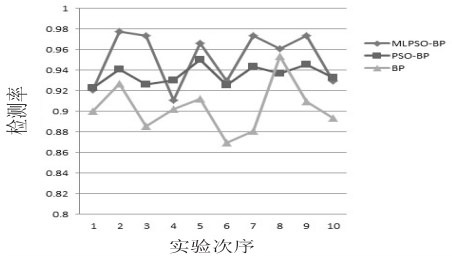

图 4 检测率对比

在图 5 中,MLPSO-BP 算法的误检率略低于 PSO-BP 算法。在图 6 中,MLPSO-BP 算法的漏检率略好于 PSO-BP 算法。由此可知,MLPSO-BP 算法与 PSO-BP 算法在误检和漏检方面各有优势。

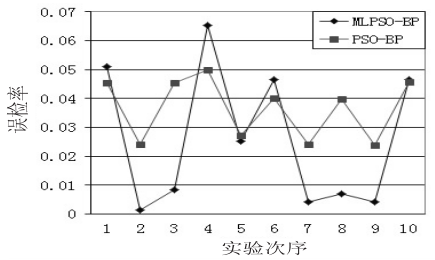

图 5 误检率对比

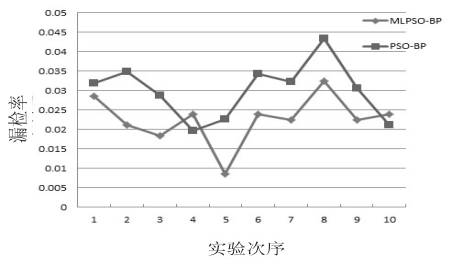

图 6 漏检率对比

综上所述,文中所提出的算法的整体检测性能较高,可以为云计算虚拟化环境提供入侵检测服务。

4 结束语

文中首先分析了 KVM 的网络结构,在此基础上结合粒子群优化算法和动量项与自适应学习速率算法,对传统 BP 算法进行了改进,提出了 MLPSO-BP 算法。

实验结果表明,文中所提算法的检测率较高。将此算法应用于虚拟化环境下的入侵检测系统中,构建了一个云环境下基于改进 BP 算法的入侵检测模型-MBPCIDM 模型。此模型兼容了虚拟化环境的不同网络模式,能够为云环境提供入侵检测服务。

在未来的研究中,需提高系统的实时性检测能力,并结合其他软计算方法,构建具有较高实用性系统。

参考文献:

[1] Modi C, Patel D, Borisaniya B, et al. A survey of intrusion detection techniques in cloud[J]. Journal of Network and Computer Applications, 2013, 36(1): 42-57.

[2] Lee S W, Yu F. Securing KVM-based cloud systems via virtualization introspection[C]//Proc of 47th Hawaii international conference on system sciences. Hawaii: IEEE, 2014: 5028-5037.

[3] Mahmood Z, Agrawal C, Hasan S S, et al. Intrusion detection in cloud computing environment using neural network[J]. International Journal of Research in Computer Engineering & Electronics, 2012, 1(1): 19-22.

[4] Shelke M P K, Sontakke M S, Gawande A D. Intrusion detection system for cloud computing[J]. International Journal of Scientific & Technology Research, 2012, 1(4): 67-71.

[5] Mazzariello C, Bifulco R, Canonico R. Integrating a network ids into an open source cloud computing environment[C]//Proc of sixth international conference on information assurance and security. Atlanta, GA: IEEE, 2010: 265-270.

[6] Roesch M. Snort homepage[EB/OL]. (1998-08-16)[1998-10-04]. http://www.snort.org/.

[7] Hamad H, Al-Hoby M. Managing intrusion detection as a service in cloud networks[J]. International Journal of Computer Applications, 2012, 41(1): 35-40.

[8] Yi X, Wu P, Dai D, et al. Intrusion detection using BP optimized by PSO[J]. International Journal of Advancements in Computing Technology, 2012, 4(2): 268-274.

[9] Pant M, Thangaraj R, Abraham A. Particle swarm optimization using adaptive mutation[C]//Proc of 19th international workshop on database and expert systems application. Turin: IEEE, 2008: 519-523.

[10] 马 锐. 人工神经网络原理[M]. 北京: 机械工业出版社, 2010: 74-76.

[11] Zhuang Wei, Guo Xiaolin, Huang Ruiwei, et al. TCP DDOS attack detection on the host in the KVM virtual machine environment[C]//Proc of IEEE/ACIS 11th international conference on computer and information science. Shanghai: IEEE, 2012: 62-67.

[12] Zeng S, Hao Q. Network I/O path analysis in the kernel-based virtual machine environment through tracing[C]//Proc of 1st international conference on information science and engineering. [s. l.]: IEEE, 2009: 2658-2661.

[13] Miao Q G, Ruo H L, Zhang X G, et al. Developing a virtual network environment for analyzing malicious network behavior [C]//Proc of international conference on educational and network technology. [s. l.]: IEEE, 2010: 271-275.

[14] Lippmann R P, Fried D J, Graf I, et al. Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation[C]//Proc of DISCEX'00. [s. l.]: IEEE, 2000: 12-26.

云环境下基于改进BP算法的入侵检测模型

作者： 何文河， 李陶深， 黄汝维， HE Wen-he， LI Tao-shen， HUANG Ru-wei

作者单位： 何文河,HE Wen-he(广西大学 计算机与电子信息学院,广西 南宁,530004)， 李陶深,黄汝维,LI Tao-shen,HUANG Ru-wei(广西大学 计算机与电子信息学院，广西 南宁 530004；广西高校并行与分布式计算技术重点实验室，广西 南宁 530004)

刊名： 计算机技术与发展 ISTIC

英文刊名：

年，卷(期)： 2016(2)