

基于粒子群优化和免疫 Agent 的入侵检测算法研究

李正洁, 李永忠, 徐 磊

(江苏科技大学 计算机科学与工程学院, 江苏 镇江 212003)

摘 要: 为解决传统入侵检测系统检测速度慢和误检率高的问题, 结合量子粒子群优化算法、免疫原理和移动 Agent 技术, 提出了基于粒子群优化算法和免疫 Agent 的入侵检测模型. 介绍了系统模型与体系结构, 并对系统性能进行仿真实验. 实验结果对比表明, 系统能提高传统入侵检测系统的检测速度和降低误检率.

关键词: 量子粒子群; 免疫原理; 移动 Agent; 入侵检测

中图分类号: TP393.8

文献标识码: A

文章编号: 1000-7180(2011)10-0094-04

Research of Intrusion Detection Algorithm Based on Particle Swarm Optimization and Immune Agent

LI Zheng-jie, LI Yong-zhong, XU Lei

(School of Computer Science and Engineering, Jiangsu University of Science and Technology, Zhenjiang 212003, China)

Abstract: Aiming at resolving the problem of low detecting speed and high false positive rate of traditional intrusion detection system, Quantum-behaved particle swarm optimization, immune principle and mobile agent are combined in this thesis. An intrusion detection model based on particle swarm optimization and immune agent is proposed. System model and systematic construction is introduced, and system performance is tested. The experiment results indicate that the system can improve the low detecting speed and high false positive rate of traditional intrusion detection system.

Key words: quantum-behaved particle swarm optimization; immune principle; mobile agent; intrusion detection

1 引言

与传统的预防性安全机制相比, 入侵检测(Intrusion Detection, ID)技术具有智能监控、实时探测、动态响应、易于配置等特点. 它能够运用一些自治和智能的工具, 实现对系统或网络资源的实时保护, 具有积极主动性^[1]. 当前的入侵检测技术^[2]存在的缺陷主要是速度瓶颈问题和误报漏报问题. 文中在 Kim 和 Bentley 提出的克隆选择算法^[3]的基础上, 提出将改进的动态克隆算法和移动 Agent 技术结合起来, 建立入侵/异常检测和响应的通用框架结构, 改进检测方法, 使系统具有自我学习, 感知外界环境的变化并能做出相应的反应的能力, 以提高系

统的检测速度, 减少误报漏报. 高质量的入侵特征库是 IDS 高效运行的必要条件, 为获得更优的检测规则库, 文中将量子粒子群算法运用在分类器中, 使特征匹配的分类更加准确, 以降低检测系统的误报率^[4].

2 量子粒子群优化算法和免疫 Agent

2.1 量子粒子群优化算法

量子粒子群算法^[4](Quantum-behaved Particle Swarm Optimization, QPSO), 由微粒群算法(PSO 算法)改进形成, 对 PSO 更新粒子位置的进化方法进行改进. 在该算法中, 重点考虑各个粒子位置更新时, 当前局部最优位置信息和全局最优位置信息.

收稿日期: 2011-04-10; 修回日期: 2011-06-29

基金项目: 江苏省高校自然科学基金资助项目(05KJD52006); 江苏科技大学科研资助项目(2005DX006J); 江苏科技大学研究生科技创新计划项目

2.2 免疫 Agent 原理

2.2.1 移动 Agent 和人工免疫技术

移动代理(MA)作为自治程序,能够自主地从网络中的一个结点移动到另一个结点,其运行场地不再局限在某一个特定位置.其获得的数据也更全面和更有针对性^[1].人工免疫技术^[3]采用模拟生物免疫系统消灭外来病原体入侵的机制,具有个体检测多样性、自组织、免疫记忆等优点.将这两种技术应用到 IDS 系统中,系统中的各个实体具有智能决策的知识,能进行相互交流和协作,使系统具有自我学习、感知外界环境的变化并能做出相应的反应能力,从而改进检测方法,提高检测速度,减少系统误报漏报^[5].

2.2.2 动态克隆选择算法

动态克隆选择算法于 2002 年由 Kim 和 Bentley 在 Hofmer 提出的 CIS 的概念的基础上提出,但该算法存在不能及时更新自我抗原,记忆检测器的生命周期过长,以及对外部系统的仲裁请求过多等不足.针对这些缺陷,本文对记忆检测器和成熟检测器做了改进^[6].将改进的动态克隆选择算法运用到检测模块中,如图 1 所示,成熟检测器和记忆检测器由系统通过改进动态克隆选择算法生成,当有抗原进入时,先将其与记忆检测器进行匹配,如若发现该抗原与记忆检测器集中记忆检测器匹配,不再直接删除该抗原,而是将当前的 self 子集与该抗原进行匹配,判断该抗原是否属于自我抗原,若当前子集不与之匹配,则认为发现非我抗原,确认入侵;若当前 self 集中的自我抗原与该抗原发生匹配,则认为该记忆检测器检测到了自我抗原,删除该记忆检测器,并把该抗原放入到 self 集中.

3 系统体系结构

该 IDS 系统中存在很多 Agent,这些 Agent 一般都是动态 Agent,这种免疫 Agent 有不同的类型,执行不同种类的检测任务,相当于生物系统中针对不同种类抗原的不同抗体.这些 Agent 是将量子粒子群优化算法、免疫的机理以及 Agent 技术融合在一起^[6],构造出的基于量子粒子群优化算法并具有免疫特征的 Agent 单元——免疫 Agent.所有这些免疫 Agent 分布在网络的各个节点上,动态检测网络安全情况,一旦发现异常立即协作处理,完成复杂任务^[7-8].

图 2 描述了基于量子粒子群优化和免疫 Agent 的 IDS 系统体系结构.

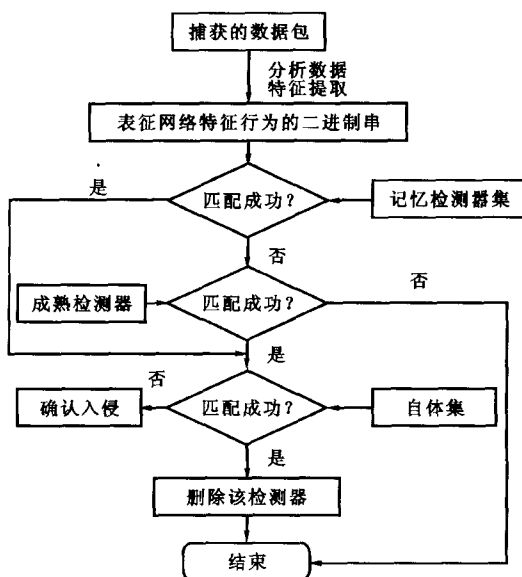


图 1 改进后的检测流程图

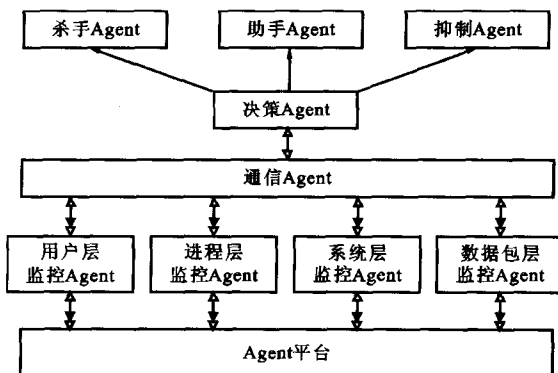


图 2 量子粒子群优化的免疫 Agent IDS 体系结构

将 IDS 系统^[1]分为四个模块,通信模块、检测模块、管理模块和响应模块,其中通信模块负责系统中信息的交流和传递;检测模块负责收集数据、检测入侵并做出决策;管理模块负责协调和管理各 agent 的运行状态;响应模块根据检测模块传送来的信息做出相应反应.

3.1 通信模块

通信模块由通信 Agent 构成,通信 Agent 是具有指定能力的谈判代表,或是通信联络其他 Agent 的消息邮员,该模块能实现抗体培育中心和更新的入侵规则库与各 Agent 的交流,以及各 Agent 之间信息的交流,以使系统中各个组件相互协作完成入侵检测任务.

3.2 检测模块

检测模块^[6]是系统检测入侵的主要部分,包括监控 Agent 和决策 Agent.其中监控 Agent 根据提取网络上传输的数据包,运行基于量子粒子群的免疫算法以获得攻击类型,而后将攻击类型传送给决

策 Agent; 决策 Agent 根据监控 Agent 传送来的抗原与抗体进行匹配, 来确定是否有抗体被激活, 若检测到入侵则作出相应的决策并通知响应代理进行处理. 入侵的性质和严重程度, 由决策 Agent 综合分析多个监控 Agent 的信息来判断, 然后激活相应的响应 Agent.

3.3 管理模块

管理模块主要用于管理用户接口、响应机制及发布攻击通告, 是入侵检测模块中与外界交流的重要部分. 它根据各个 Agent 收集的系统和控制中心的指令, 协调和管理 Agent 的运行状态, 同时管理模块运用量子粒子群优化算法不断更新检测基因库, 并根据人工免疫原理, 自动生成检测模型.

3.4 响应模块

响应模块是系统根据入侵的特性与强度激活一个适当的反应 Agent 集合, 它包括杀手 Agent、助手 Agent、抑制 Agent 三种响应 Agent.

杀手 Agent 由多个决策 Agent 通过通信 Agent 激活, 能在真实的入侵与恶意活动发生时采取中断行为. 助手 Agent 由决策 Agent 通过通信 Agent 激活, 被激活后, 它们将当前的环境状态报告给终端用户或显示决策报告, 然后由系统管理员或用户决定对入侵行为采取进一步的行动. 抑制 Agent 能够在入侵检测反应过程的后期防止系统对假阳性错误采取其他行动, 抑制 Agent 被激活后, 它们会干扰其他决策 Agent 采取更进一步的行为.

大部分时间内监控 Agent 都漫游在网络中, 监视网络状态. 监控 Agent 能区别恶意和正常的行为, 具备全面的分析系统或者通信能力. 如果网络某个部分出现异常情况, 若被监控 Agent 发现, 它试图理解所发生的事件, 并做出相应的决策. 在有些场合下, Agent 会咨询周围的其他 Agent 而后作出决策, 这相当于免疫反应中协同刺激的第二信号, 作出决策之后, 由通信 Agent 通知决策 Agent, 采取特定的行动. 在 IDS 系统中, 若检测和识别出可疑行为, 决策 Agent 会自动阻止恶意代码进入安全区域或者阻止恶意代码的执行^[8].

4 系统测试与结果分析

在基于 Java 的移动 agent 平台 IBM Aglets 上构建实验检测系统, 建立移动 agent 系统的仿真环境, 通过执行 agent 代码获取它的基本数据, 并对在各种环境下仿真实现的移动 agent 性能作出评价.

本文使用 4 台主机在实验室内部环境下进行测

试. 实验中, 一台主机作为攻击主机使用, 产生攻击数据, 另外 3 台主机产生正常的网络流量数据, 将采集的网络数据包数据存储为文本格式.

实验使用 KDD99 数据集^[9], 评价量子粒子群算法和免疫 Agent 在入侵检测上的应用效果, 其中包括训练集(kddcup. data. gz)和测试集(corrected. gz). 实验中采用 10 % 的数据子集(kddcup. data _ 10 _ percent. gz) 中 20 % 的数据作为训练数据, 采用带有 corrected 标记的数据子集(corrected. gz) 中 20 % 的数据作为测试数据. 表 1 中列出了各种类型的样本数据在训练集和测试集中的分布情况.

表 1 训练数据和测试数据
中的各样本分布

连接类型	样本数	
	训练数据集	测试数据集
Normal	19 455	12 118
Dos	78 291	45 970
Probing	824	833
U2R	10	45
R2L	225	3 237

设置系数 $\beta=0.7$, 匹配方法中的 r 参数为 6, 未成熟检测器的耐受期 T 为 10, 成熟检测器的生命周期 L 为 20, 成熟检测器的激活阈值 A 为 15, 对系统性能进行测试, 表 2 中列出了优化后的实验结果与文献[10]中结果之间的比较. 本文提出的方法在参数优化后, 在 Normal、Dos 和 Probing 三种类型的检测中, 检测效果较好, U2R 攻击类型的检测率并不十分理想. 在对 R2L 攻击类型的检测中, 性能较差.

表 2 各攻击类型的检测结果比较

连接类型	检测结果/%	文献[10]的结果/%
Normal(12 118)	96.52	96.2
Dos(45 970)	97.89	96.6
Probing(833)	91.81	80.9
U2R(45)	73.68	9.6
R2L(3 237)	4.17	0.1

主要原因是: 在训练数据中, 相对于 Normal、Dos 和 Probing 类型的样本量来说, U2R 和 R2L 两类攻击的样本数量明显偏少, 无法有效形成稳定的知识, 从而多数被误判为正常行为. 而在测试数据中, U2R 类攻击的测试数据量相对较小, R2L 类攻击的测试数据量相对较多, 如表 1 所示, 最终导致

R2L 攻击类型的检测率特别低,因此,如何改善对 R2L 和 U2R 两种攻击类型的检测,是下一步的工作目标。

5 结束语

本文结合免疫学原理、多 Agent 技术和量子粒子群优化算法三种技术,融合三者优势并将其应用到入侵检测系统中,提高了系统的检测速度并降低了误检率。另与文献[10]中结果做出比较,证明本系统使用的检测方法取得一定的良好效果。但该系统还存在一些不足,如改善对 R2L 和 U2R 两种攻击类型的检测,引入量子行为的粒子群算法还存在陷入局部最优解的问题,等等,这些都是下一步展开的工作。

参考文献:

- [1] 李永忠,罗军生,孙彦. 基于移动 Agent 的智能化入侵检测系统结构研究[J]. 计算机研究与发展, 2006, 43(1): 296—301.
- [2] 毕战科,许胜礼. 入侵检测技术的研究现状及其发展[J]. 软件导刊, 2010 11(9): 152—155.
- [3] Jungwon Kim, Peter Bentley. Immune memory and gene library evolution in the dynamic clonal selection algorithm[J]. Genetic Programming and Evolvable Machines, 2004, 5(4): 361—391.
- [4] Sun J, Xu W B. A global search strategy of quantum-behaved particle swarm optimization[C]// Proceedings of IEEE Conference on Cybernetics and Intelligent Systems, USA: IEEE, 2004: 111—116.
- [5] 倪建成,李志蜀. 基于免疫原理的多代理网格入侵检测系统体系结构研究[J]. 计算机应用研究, 2009, 26(2): 705—708.
- [6] 段富,苏同芬. 免疫粒子群算法的改进及应用[J]. 计算机应用, 2010(7): 1883—1884.
- [7] 王汝山,李永忠. 基于半监督学习的入侵检测算法研究[J]. 微电子学与计算机, 2009, 26(10): 25—29.
- [8] Dasgupta D, Majumdar N S. MILA—multilevel immune learning algorithm[C]// Proc of the Genetic and Evolutionary Computation, USA, Memphis, 2006: 183—194.
- [9] KDD Cup 1999 Data. Irvine, CA(USA). Information and computer science[M]. California: University of California, 1999.
- [10] 刘衍珩,田大新,余雪岗,等. 基于分布式学习的大规模网络入侵检测算法[J]. 软件学报, 2008, 19(4): 993—1003.

作者简介:

- 李正洁** 女, (1987—), 硕士研究生. 研究方向为网络与信息安全;
- 李永忠** 男, (1961—), 教授, 硕士生导师. 研究方向为网络安全、计算机应用、藏文信息处理;
- 徐磊** 男, (1986—), 硕士研究生. 研究方向为计算智能.

作者简介:

- 张文娟** 女, (1978—), 硕士, 讲师. 研究方向为图像处理与模式识别.
- 康家银** 男, (1974—), 博士, 讲师. 研究方向为图像处理、模式识别、机器学习.

(上接第 93 页)

- [3] Chua L O, Yang L. Cellular neural networks: theory and applications[J]. IEEE trans. circuits and system, 1988(35): 1257—1290.
- [4] Chua L O. CNN: a vision of complex[J]. Int. J. bifurcation and chaos, 1997, 7(10): 2219—2425.
- [5] Chua L O, Roska T. Cellular neural networks and visual computing[M]. London: Cambridge Press, 2002: 52—66.
- [6] Cai H, Min L Q. A kind of two-input CNN with application[J]. International Journal of Bifurcation and Chaos, 2005, 15(12): 4007—4011.

- [7] Yang X H, Jiao L C. Fusion algorithm for remote sensing images based on nonsubsampling contour transform[J]. ACTA Automatic Sinica, 2008(34): 274—281.
- [8] 邢素霞,吴静珠,陈天华. 图像融合质量评价方法研究[J]. 微电子学与计算机, 2010, 27(6): 157—159.