基于移动 Agent 的免疫入侵检测模型及算法

陈仲民[1,3],王 宇[2]
CHEN Zhong-min[1,3],WANG Yu[2]

1.华中农业大学 计算机科学系,武汉 430070
2.桂林工学院 电子计算机系,广西 桂林 541004
3.东南大学 计算机科学与工程系,南京 210096
1.Department of Computer Science,Huazhong Agriculture University,Wuhan 430070,China
2.Department of Computer Science,Guilin Industry College,Guilin,Guangxi 541004,China
3.Department of Computer Science and Engineering,Southeast University,Nanjing 210096,China
E-mail:chenzm@mail.hzau.edu.cn

CHEN Zhong-min,WANG Yu.Model of intrusion detection based on mobile Agent & immune principle and algorithm. Computer Engineering and Applications,2008,44(8):131-134.

Abstract: A model of intrusion detection based on the mobile agent technology and immune principle,called MAgentIDS,is presented from the aspects of the practical application,which utilizes the mobile agent technology and immune principle to solve the problems on the intrusion detection in the network security area.The immune tolerant model in the IDS is analyzed in especially, and the algorithm of negative selection used in the agent for analyzing is improved.The prototyping system is developed,and the emulational detection is accomplished by simulating the typical intrusions in the LAN.The experimental result indicates that the model is more adaptive than the original one.

Key words: intrusion detection;the mobile agent;immune principle;negative-selection algorithm

摘 要:结合移动 agent 技术和免疫系统的特性,从实际应用的角度出发,将两者的优势引入网络入侵检测系统的设计,提出了一个基于移动 agent 的免疫入侵检测系统 MAgentIDS 模型,并对其做了较为深入的研究。重点分析了用于入侵检测系统的免疫耐受模型,改进了检测分析 agent 采用的否定选择核心算法。开发了原型系统并模拟一些典型入侵行为,完成入侵检测系统的检测任务,实验结果表明该模型较原有的方法具有更好的适应性。

关键词:入侵检测;移动 agent;免疫原理;否定选择算法
文章编号:1002-8331(2008)08-0131-04 **文献标识码:**A **中图分类号:**TP393.08;TP311.52

1 引言

现有的基于移动 agent 的入侵检测系统研究多停留在防火墙中集成较为初级的入侵检测模块阶段。此外,大部分系统是基于规则库的,只有少数系统具有智能检测能力,检验率较低但网速要求较高[4]。再者,真正将移动 agent 与入侵检测结合起来的并不多,多数情况是分派数据收集 agent 采集数据。大部分系统主要是针对 agent 的自主性研究,在移动性方面研究较少。

本文在现有入侵检测系统基础上,将移动 agent 技术与入侵检测系统数据采集部分和数据检测分析部分的设计相结合,并在检测分析部分的设计中借鉴了人工免疫的思想,提出了基于移动 agent 的免疫入侵检测系统 MAgentIDS, 充分发挥了移动 agent 技术和人工免疫原理运用于入侵检测系统设计的优势。

2 MAgentIDS 体系结构的设计

在系统的体系结构设计中选用了综合分层和网状体系结构最佳特征的混合模型,如图 1 所示。

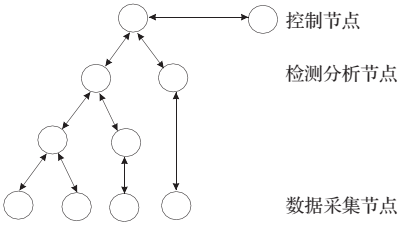

图 1 MAgentIDS 的系统体系结构

在该体系结构的最下层数据采集叶节点负责数据的采集,并根据安全策略对大量数据进行过滤,以减轻上层检测分析节

基金项目:国家自然科学基金(the National Natural Science Foundation of China under Grant No.60373066,No.60425206,No.90412003);高等院校博士学科点专项科研基金(the China Specialized Research Fund for the Doctoral Program of Higher Education under Grant No. 20020286004)。

作者简介:陈仲民(1964-),男,副教授,研究方向:并行与分布式计算,软件工程;王宇(1981-),女,硕士,研究方向:并行与分布式计算。

收稿日期:2007-10-11 **修回日期:**2008-01-09

点的处理压力，有利于检测分析节点专注于识别判断入侵行为，提高检测效率。必要时节点间可以相互协作，以保证更全面、准确的判断。

该体系结构由分布在各受控主机上的移动 agent 组成，各相邻agent 关系平等、连结松散、可彼此独立进行操作。这样设计的入侵检测系统更具容错性，且更容易关联数据和检测分布式攻击。移动 agent 的引入使数据采集节点、检测分析节点和控制节点并不总是驻留在一台物理主机上，即移动 agent 可以作为检测分析节点移动到最合适的物理位置。

3 基于免疫原理的检测算法设计

主要利用匹配的方式模拟免疫系统抗体间，以及抗体和抗原间的反应特征。通过字符串间的不完全匹配仿真实现入侵检测系统 MAgentIDS 中检测分析 agent。

3.1 抗体、抗原的编码

产生的初始抗体集合对应着问题的一个随机解。定义抗原集合为原始网络数据包进行特征提取后得到的长度为 Length 的二进制字符串集合。抗原的判断结果对应识别入侵行为问题的解。

由于主要关注 TCP、UDP、ICMP 协议类型的数据包，因此重点提取对这些协议分析影响较大的字段，遵循抗体、抗原均由多个基因片断连接组合而成的原则，根据“自我”和“非我”的定义，将相应的抗体(Antibody，Ab)和抗原(Antigen，Ag)集合通过协议类型、源 IP 地址、目的 IP 地址、源端口号和目的端口号五个基因片断表达，每个基因片断都是包含各自特征的特征区间，其基因型表达如表 1 所示。

表 1 抗体、抗原的编码方式

协议类型	目的 IP 地址最后一个字节	源主机 IP 地址	目的端口	源端口号

由于否定选择算法中候选检测器的数量将随二进制字符串的长度呈指数级增长，因此在编码部分需要对端口号做些处理。

3.2 抗体、抗原(含抗体间)的亲和力计算

抗体和抗原之间的亲和力基于它们之间的相似性。直接采用免疫系统中抗体和抗原间的互补特性将导致较多的误报率，因此我们考虑采用匹配度来度量抗体和抗原之间的亲和力。如果两个等长字符串中每一个对应位置上的字符都相同，称这种匹配为完整匹配。

在免疫系统中更多的是局部匹配。借鉴 Forrest 和 Hofmeyr 提出的 γ—连续位匹配规则(γ—continuous bits)计算抗体、抗原间以及抗体间的亲和力。假设两个字符串 x 和 y，如果至少存在连续的 γ 位相同，就称它们是 γ—连续位匹配的。如果 γ=4，对于至少连续 4 位相同的两个字符串，它们是匹配的(如图 2)，否则它们就不匹配(如图 3)。

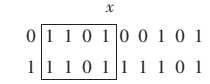

图 2 γ—连续位匹配(γ=4)

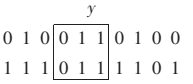

图 3 γ—连续位不匹配(γ=3)

其数学表述为：

$$\text{Affinity}(x,y,\gamma)=\begin{cases}1, i,j,j-i\geqslant\gamma, x_k=y_k, i\leqslant k\leqslant j\\ 0, \text{其它}\end{cases} \quad (1)$$

3.3 检测器的构造和算法思想的改进

(1)检测器的构造

构造检测器首先需要尽可能多地收集网络数据包信息。系统模型的构建借鉴了图论的思想，用图 $G=(V,E)$表示分布式环境，v 表示该网络环境中的一台主机，即一个检测节点，它是局域网环境中所有节点集合 V 的子集，有 $v\in V$；边 e 表示各网络节点之间的连接，代表检测器在节点间的移动，有 $e\in E$。需要注意的是，检测器只能在同一个检测节点和其他检测器交互。

免疫系统中的自体耐受是对自体抗原不产生应答的一种免疫耐受。检测器的构造主要模拟了实现 T 细胞、B 细胞的自体耐受过程。通过以下步骤构造检测器，如图 4 所示。

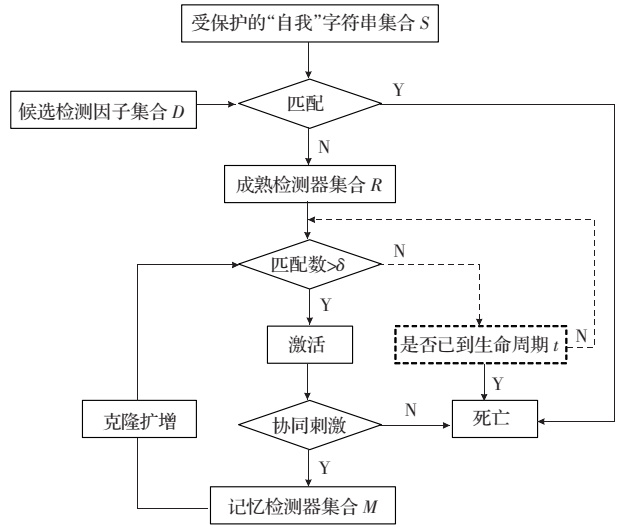

图 4 构造检测器流程图

(2)算法思想的改进

检测过程中会产生两种错误——检测误报率(false positive)和检测漏报率(false negative)。前者将“自我”字符串认为是异常的“非我”，后者将“非我”字符串认为是正常的“自我”[2]。

由于在构造模型的训练数据时可能存在将不可接受行为认为是可接受的，产生漏警的情况，不利于系统检测入侵行为，因此就需要进一步处理否定选择算法分析的数据，尽可能减少这种情况的发生。

深入研究 Forrest 提出的否定选择算法后发现，候选检测器的数量将随着“自我”集合中二进制编码长度的增加成指数级增长，并且该算法没有对检测器的冗余情况进行检查。尽管在她之后也提出了一些改进方法，如线性算法、贪婪算法、二进制模块算法，但都没有很好地解决上述问题。

这部分主要考虑在 Ayara 提出的带变异的否定选择算法[1]基础上做一定改进，增加了对检测器冗余的判断，并且当候选检测器中的字符串和“自我”集合 S 中的字符串匹配时，对候选检测器中的元素做有导向的变异，使其远离“自我”集合 S 中的字符串。

①检测器冗余的判断

在 Forrest 提出的算法中，经否定选择的检测器没有进行冗余检查就直接将其作为成熟检测器中的一个元素进入到协同刺激环节，这可能导致成熟检测器集合 R 中的数据冗余，因此我们考虑增加否定选择后产生的检测器和成熟检测器集合 R 中的检测器的对比环节，判断检测器是否有冗余。如果存在冗余就删除该检测器；否则就将该检测器添加到成熟检测器集合R 中。

②否定选择算法的改进

Forrest 给出如下所示四个公式[2]，利用概率分析的方法估算系统对“非我”集合为满足一定的可靠性（识别率为某一固定值）所应有的检测器数目。

$$P_M \approx m^{-r}\left[\frac{(l-r)(m-1)}{m}+1\right] \tag{2}$$

$$N_R=\frac{-\ln P_f}{P_M} \tag{3}$$

$$N_D=\frac{-\ln P_f}{P_M\times(1-P_M)^{N_S}} \tag{4}$$

$$P_M \approx \frac{1}{N_S} \tag{5}$$

根据公式（2）计算检测出“非我”的概率 P_M；之后根据公式（3）计算经过否定选择算法生成的成熟检测器集合 R 中二进制字符串的数量 N_R；接着根据公式（5）变形得 $N_S \approx \frac{1}{P_M}$，计算所需“自我”集合 S 中二进制字符串的数量 N_S；最后根据公式（4）计算所需候选检测器集合 D 中二进制字符串的数量 N_D。N_T 为测试数据集合的二进制字符串的数量。通过设置不同的匹配阈值 γ（$1<\gamma<$Length）得到 P_{RM}、N_R、N_S、N_D 的取值的差异，如表 2 所示。

表 2　否定选择算法相关参数值比较表

γ	P_M	N_R	N_S	N_D
4	1.688	–	–	–
5	0.828	3	1	17
6	0.406	6	2	17
7	0.199	12	5	36
8	0.098	23	10	65
9	0.048	48	20	128
10	0.023	100	43	272

由表 2 可以看出，当 $\gamma<5$ 时，由于现有的候选检测器都匹配了“自我”数据集合 S 中的元素，将不能产生所需的候选检测器集合 D。因此我们需要对与“自我”数据集合 S 中匹配的候选检测器做有导向的变异，使其远离“自我”集合中的字符串。

在 Ayara 提出的算法里面，以正确分类器（correct classfication）正确分类率最大化和错误分类器（incorrect classfication）错误分类率最小化来设置匹配阈值 γ 的值。由于 γ 的值决定了数据的“自我”和“非我”集合空间的划分，因此选择一个合适的 γ 值对改进的否定选择算法至关重要。

在改进算法的实现过程中，首先产生“自我”数据集合 S；之后产生一个随机候选检测器；接着需要设置匹配阈值 γ 以便进入下一步的免疫耐受过程。在这里，考虑借鉴免疫中 B 细胞对抗原亲和力变异的机理，通过带权值的亲和力的计算来确定匹配阈值 γ，根据自我和候选检测器之间的亲和力自适应地调节变异。变异发生在与“自我”集合元素相匹配的部分。达到“非我”集合空间覆盖率最大，“自我”集合空间覆盖率最小的要求。

在编码中，抗体和抗原集合都用五个基因片断表达，除第一个基因片段与确定协议类型相关，要求编码完全匹配，便于将格式化后的数据交由到不同的协议 agent 处理外，其他的基因片断亲和力计算不单纯依靠字符匹配处理，而是根据检测的实际需要为不同的基因片断设置不同的权值。通过下面的公式（6）：

$$March\_Value=\sum_{i=2}^{m}\alpha_i Matching(I_i) \tag{6}$$

来计算匹配度。其中，$March\_Value$ 表示匹配度，m 表示基因片断的个数，在本系统中根据编码方式，$m=5$，I 表示基因片断，α_i 表示第 i 个基因片断的权值，$Marching(I_i)$ 表示第 i 个基因片断的匹配度。

变异的概率 P_{Mu} 决定了二进制字符串的一个 bit 位置是否发生变异，它的大小和匹配度成正比。也就是说，匹配度越大，变异概率越大。变异主要修改权值较大的基因片断。由于时间复杂度与产生随机检测器并和“自我”集合 S 中的二进制串匹配的时间有关，因此引入限制变异次数的变异控制器 T_{Mu}，严格控制随机检测器的变异过程，这样有利于减少生成随机候选检测器的数量，可以通过更少的检测器达到相同的检测目的。

3.4　细胞及其集合的定义

细胞分为记忆免疫细胞、成熟免疫细胞和未成熟免疫细胞三类。记忆免疫细胞是经过了自体耐受且被抗原激活的成熟免疫细胞。成熟免疫细胞是指经过了自体耐受但未被抗原激活的免疫细胞。未成熟免疫细胞是指尚未经过自体耐受的免疫细胞。

对记忆免疫细胞、成熟免疫细胞和未成熟免疫细胞及其各自集合的定义如下：约定免疫细胞集合 B，$B=\{<d,age,count>|d\in D,age\in N,count\in N\}$，其中 d 为抗体，age 为抗体生命周期，$count$ 为与抗原匹配数，D 为长度为 Length 的二进制字符串集合，N 为自然数集合，有 $B=M_b\cup U_b$[3]。

（1）定义记忆免疫细胞集合 R_b：$R_b=\{x|x\in B,x.count\geqslant\beta\}$，其中 β 为匹配数阈值。记忆细胞的检测过程模拟了免疫系统中记忆细胞自动提取抗原签名，当再次检测到相同或相似抗原时，迅速活化，产生大量具有抗原特异的抗体快速免疫应答的免疫机理。该部分在入侵检测系统 MAgentIDS 中起着快速检测入侵行为，提高系统的检测效率和准确率的作用。

（2）定义成熟免疫细胞集合 M_b。它由经过自体耐受并且与抗原匹配数小于匹配数阈值的免疫细胞组成。成熟细胞的检测过程模拟了成熟免疫细胞（成熟 B 细胞和成熟 T 细胞）的免疫机理，成熟 B 细胞和成熟 T 细胞共同作用，检测病原体且协助清除病原体。它是入侵检测系统 MAgentIDS 的主要检测部分，起着检测抗原的作用，它的完备性将影响检测的准确率。

（3）定义未成熟免疫细胞集合 U_b：$U_b=\{<d,age>|d\in D,age\in N\}$，并有 $|M_b|+|U_b|=\xi$，其中 ξ 为常数。未成熟细胞的耐受过程模拟了骨髓中产生未成熟 B 细胞和胸腺中产生未成熟 T 细胞的免疫机理，未成熟 B 细胞和 T 细胞经过自体耐受发展为成熟免疫细胞。该部分在入侵检测系统 MAgentIDS 中能检测出已知攻击的变种和未知攻击，不断更新检测分析 agent 集合，使 MAgentIDS 具有动态性和自适应性。

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，建立了移动 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。

在具有 4 台主机的实验室内部环境下进行测试。其中，1 台主机作为服务器，安装 Windows 2000 Server 操作系统，其余主机统一安装 Windows XP Professional 操作系统，每台主机上

都分别安装有 JDK1.5.0_02、移动 agent 平台 Aglets-2.0.2 和 MS SQL Server 2000 数据库,采用 10 M 以太网卡。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。

(1)配置性能测试

这部分主要针对 agent 的分派进行测试:在配置管理 agent 上生成新的 Aglet,将其派遣到指定的地址(以"atp://Sarah:500"的形式定义地址)。在对应地址的 Aglets 服务器 Tahiti 上能接收并运行该 Aglet,在远端主机的 Aglets 服务器 Tahiti 上可召回指定的 Aglet。

测试结果说明移动 agent 平台设计合理可行,可在局域网环境下正常工作。

(2)否定选择算法的测试

这部分主要测试改进的否定选择算法的正确性,以及各参数对该算法的影响。

通过对实验结果的分析,得出当两个随机字符串至少 γ—连续位匹配的概率 P_m 很小的情况下,N_s 就很大。当 m 增大到 128 的情况下,$P_m \approx 0$;γ 增大的情况下,P_m 减小;Length 增大的情况下,P_m 增加。经过多次实验,推荐了检测未知攻击的检测分析 agent 中所涉及参数的取值,如表 3 所示。

表 3 检测分析 agent 的参数值

参数	说明	建议取值
m		2
γ	匹配阈值	9
Length	二进制字符串的长度	74
p	活化阈值	20

(3)其它测试

分别进行了 SYN Flood 攻击测试,Land 攻击测试,Smurf 攻击测试、Ping of death 攻击测试,测试结果说明该系统能够检测到以上攻击。

实验数据表明该系统模型设计合理,可完成到目的主机的迁移,检测分析 agent 能较准确地检测出入侵事件,改进的否定选择算法的检测效果较现有方法有明显的改善。

5 结语

本文在分析现有移动 agent 平台的优劣基础上,提出了一种基于移动 agent 的免疫入侵检测系统 MAgentIDS。在 MAgentIDS 体系结构设计上采用了混合模型结构,有效综合了分层和网状体系结构的最佳特征,并对基于免疫原理的检测算法做了详细阐述。在系统进一步完善方面还有大量的工作要做,包括:进一步提高入侵检测系统中的 agent 在高速、低延迟、连接可靠的网络环境和中间数据传输量较小情况下的执行效率,需要进一步完善在网络故障、目标主机关机、源主机长时间无响应等异常情况下的容错机制。

参考文献:

[1] Ayara M,Timmis J,de Lemos R,et al.Negative selection:how to generate detectors[C]//the 1st International Conference on Artificial Immune Systems,2002.

[2] Hofmeyr S A,Forrest S.Architecture for an artificial immune system[J].Evolutionary Computation Journal,2000,8:443-473.

[3] Kim J,Bentley P J.A model of gene library evolution in the dynamic clonal selection algorithm[C]//Proceedings of the First International Conference on Artificial Immune System,Canterbury,2002:57-65.

[4] 王晋,李德全,冯登国.一种基于 Agent 的自适应的分布式入侵检测系统[J].计算机研究与发展,2005,42:1934-1939.

(上接 100 页)

场拓扑简化方法,并通过对漏油数据集的实验验证了方法的可行性。

本文算法的核心是对三维标量场的拓扑简化,不同于网格简化方法,本文结合 Morse 理论,对函数构造 Morse-Smale 复形并且通过反复删除持久性低的临界点对来逐渐简化函数拓扑结构。为了提高简化效率,设计更好的多分辨率数据结构是关键,也是下一步的研究重点;并且通过进一步完善争取将该算法运用到更多的复杂流场中,比如数据分割和特征提取,对医学图像或模拟流场数据跟踪等。

参考文献:

[1] Bajaj C L,Pascucci V.Visualization of scalar topology for structural enhancement[C]//Proceedings of IEEE Visualization'98,Oct 1998.

[2] Tang C K,Medioni G.Extremal feature extraction from 3-D and noisy scalar fields[C]//Proceedings of IEEE Visualization'98,Oct 1998.

[3] Trichoche X,Scheuermann G,Hangen H.Continuous topology simplification of planarvector fields[C]//Proceedings of IEEE Visualization'2001,Oct 2001.

[4] Xavier Tricoche,Gerik Scherermann,Hang Hagen.A topology simplification method for 2Dvector fields[C]//Proceedings of IEEE Visualization'2000,Oct 2000.

[5] Heckel B,Weber G,Hamann B.Construction of vector field hierarchies[C]//Proceedings of IEEE Visualization'99,Oct 1999.

[6] 吴克勤,杨冠杰,尚海霞.与物理特征相关的平面向量场的拓扑简化及压缩[J].计算机辅助设计与图形学报,2006,18(5):656-660.

[7] Floriani L D,Mesmoudi M M,Danovaro E.A smale-like decomposition for discrete scalar fields[C]//Proceedings of ICPR'2002,2002.

[8] Gyulassy A,Natarajan V,Pascucci V,et al.A topological approach to simplification of three-dimensional scalar functions[C]//Proceedings of IEEE Vis'2006,2006.

[9] Bremer P T,Edelsbrunner H,Hamam B,et al.Topological hierarchy for functions on triangulated surfaces[J].IEEE TVCG,2004,10(4):385-396.

[10] Milnor J.Morse theory[M].[S.l.]:Princeton University Press,1963.

[11] Edelsbrunner H,Harer J,Natarajan V,et al.Morse-smale complexes for piecewise linear 3-manifolds[C]//Proc 19th Ann Sympos Comput Geom,2003:361-370.

[12] Bremer P T,Edelsbrunner H,Hamam B,et al.Topological hierarchy for functions on triangulated surfaces[J].IEEE TVCG,2004,10(4):385-396.