文章编号:1673-0062(2009)03-0039-04

基于人工免疫原理的免疫检测技术研究

虞宏霄,谭敏生

(南华大学 计算机科学与技术学院,湖南 衡阳 421001)

摘 要:针对人工免疫原理在计算机安全领域中的研究现状,对人工免疫系统及其计算模型进行了详细的介绍与分析.同时结合人体免疫理论,重点研究了B、T细胞检测器的生成算法.最后通过实验对检测器进行了测试,并对免疫检测技术未来的研究方向提出了展望.

关键词:人工免疫系统;主动防御;计算机安全

中图分类号:TP393 **文献标识码**:A

A Survey of Artificial Immune Theory - based Computer Defense Technology

YU Hong-xiao, TAN Min-sheng

(School of Computer Science and Technology, University of South China, Hengyang, Hunan 421001, China)

Abstract: According to the research status of the Artificial Immune Theory being applied in the field of computer security, this paper mainly introduced the Artificial Immune System and its computational models. Then combined with Artificial Immune principle, a training algorithm of B cell detector and T cell detector has been presented. At last the detector was tested by experiment and the future research direction was pointed out.

Key words: artificial immune system; proactive defense; computer security

1 人体免疫机制概述

自上世纪六十年代,Bagley和Rosenberg等先驱成功地将生命科学领域的研究成果应用于工程科学领域后[1],基于生物进化规律的生命科学与工程科学的交叉学科受到了各国学者的广泛重视.人体免疫系统属于层次型结构防御系统,其结构如图1所示[2]:第一层是皮肤和黏膜,皮肤通过其致密的角化层阻挡病原体的侵入,而黏膜则通过分泌酸和酶等化学物质杀死进入人体的外界病原;第二层是吞噬细胞和巨吞噬细胞,当少数病原体突破第一层防线进入人体后,吞噬细胞和巨吞噬细胞会迅速向病原体集中、包围,并通过释放溶解酶将其消化;第三层是特异性免疫,极少数病原

收稿日期:2009-04-03

基金项目:湖南省自然科学基金资助项目(09JJ5042)

作者简介:虞宏霄(1976-),男,河北秦皇岛人,南华大学计算机科学与技术学院助教,硕士.主要研究方向:计算机网络与信息安全.

体突破前两层防线进入人体会生长繁殖并引起感染,特异性免疫将针对某种病原体(抗原)进行识别并分泌抗体予以消灭.

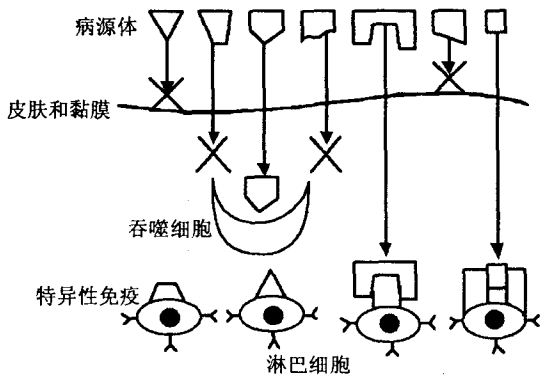

图 1 人体免疫系统层次结构

Fig. 1 The architecture of artificial immune system

2 人工免疫原理及其计算模型

免疫网络理论最早由丹麦学者 N. K. Jerne 在 1974 年提出[3],由此奠定了免疫计算的理论基础. Jerne 的免疫理论主要阐述的是免疫记忆的产生以及 B 细胞之间的相互作用,这种相互作用包括相互刺激(Stimulation)和相互抑制(Suppression),同时产生免疫抗体. 根据 Jerne 的免疫理论,抗体识别抗原主要依靠的是抗体表面的受体与抗原表面的决定基之间化学健的绑定结合. 免疫记忆,即 B 细胞的自"学习"能力,其"水平"高低主要是通过一个亲合力值(Affinity)来进行判断. 基于人体免疫理论的免疫网络数学建模过程及其描述描述如下[4]:

1)首先定义抗原集合为 A,初始 B 细胞集合为 B;

2)然后 B 细胞将针对某种特定的抗原进行识别:$f^{A}_{\text{sitmulation}}: A \times B \rightarrow R$

3)再对 B 细胞与抗原之间的亲合力(affinity)进行判断:

$$f^{A}_{\text{sitmulation}}(a,b): g(f_{\text{affinity}}(a,b))\ (a \in A, b \in B)$$

4)由于 B 细胞之间存在相互刺激(Stimulation)和相互抑制(Suppression)作用:

$$f^{B}_{\text{sitmulation}}: B \times B \rightarrow R; f^{B}_{\text{suppression}}: B \times B \rightarrow R$$

5)所以,B 细胞对抗原的识别及其之间相互作用的总公式为:

$$F(b) = \sum_{a \in A} f^{A}_{\text{sitmulation}}(a,b) \sum_{b' \in B, b' \neq b} f^{B}_{\text{sitmulation}}(b',b) \sum_{b' \in B, b' \neq b} f^{B}_{\text{suppression}}(b',b)$$

免疫检测技术是将异常网络连接定义为"抗原","B 细胞检测器"是由经验数据集(training data)和计算机脆弱点、漏洞列表结合生成的一个规则集. 克隆选择过程首先是选择一个亲合力函数阀值 λ_0,然后分别将规则集中的每条规则以亲合力函数阀值同正常数据 Ndata 做比较,如果匹配则将其从规则集中删除,再将其他亲合力值较高的新规则加入到规则集中. 不断重复以上过程,反复比较,直至生成较为成熟的 B 细胞检测器集合.

3 免疫检测器研究

由于传统的入侵检测系统普遍存在着误报、漏报及缺乏自适应性等缺陷,因此将人工免疫原理应用于入侵检测领域成为当前研究的新热点. 基于人工免疫原理的入侵检测技术主要解决的是检测器的生成问题,1994 年美国学者 Forrest、Perelson 根据 T 细胞在人体胸腺中的成熟过程提出了"否定选择算法"[5]用于生成检测器并完成了检测器的耐受训练过程.

3.1 协同检测机制

在人体中,对于外来抗原的识别主要依靠 B 细胞对其绑定,但当 B 细胞绑定的抗原数量达到一定阀值却未能激活并分泌抗体时,极有可能发生自免疫现象,即将 self 当作 non - self 进行绑定并分泌抗体予以消灭. 这种误识别是不允许的,因此要求 T 细胞对 B 细胞绑定的抗原进行确认.

采用 B、T 检测器协同工作方式的优势在于可以通过分别设定叉反应域的 r_b 和 r_t 取值,弥补单一检测器在检测过程中如果交叉反应域 r 值选取过高,可能会出现某些"非我串"不被检测器匹配(漏报);如果交叉反应域 r 值选取过低,又可能会出现某些"自我串"被误判为"非我串"(误报)的缺陷.

3.2 B、T 细胞检测器的生成算法研究

在人体中,B 细胞是通过细胞膜表面的抗原表位层来识别抗原,而 T 细胞是通过细胞膜表面的抗原肽链层来识别抗原. 在入侵检测中,网络数据包的包头信息类似于自适应免疫系统中的抗原表位,而连接的 ID、连接状态、连接统计情况等类似于抗原肽链. 因此,可以将所有的网络连接依照其模式映射成固定长度的二进制字符串,并定义 r 个连续位为亲合力,分别对其进行部分匹配的 B、T 检测. 若连续匹配成功的位数大于等于 r,则认为改连接为入侵连接.

在研究过程中,根据 Forrest 所提出的否定选

择算法,结合人体免疫机制中 B、T 细胞的协同工作原理,提出了一个 B、T 检测器的生成算法,具体描述如下[6]:

1)收集已知的 self 和 non - self 集合;

2)将所有的 self 与 non - self 映射成二进制字符串,并随机产生同样长度的字符串作为检测器(该检测器是非成熟的,需要经过一段时间的训练);

3)将单个检测器分别与 self 集合中的每个元素进行匹配,若检测器串 d 与 self 串 s 的连续匹配位数大于等于 r,则认为匹配成功;

4)定义两个阀值 r_1、r_2,并令 $r_2 > r_1$;

B 检测器的训练生成过程:

①令 $r = r_2$;

②将检测器与 self 集合中的每个元素进行匹配,一旦出现匹配成功,则该检测器被删除,由新的随机产生的识别串替代;

③最多与 self 有 $r_2 - 1$ 个连续位相匹配位的字符串集组成 B 检测器;

T 检测器的训练生成过程:

①令 $r = r_1$;

②将检测器与 self 集合中的每个元素进行匹配,一旦出现匹配成功,则该检测器被删除,由新的随机产生的识别串替代;

③最多与 self 有 $r_1 - 1$ 个连续位相匹配位的字符串集组成 T 检测器集;

④再将已知的 non - self 串也加入 T 检测器集中,共同组成 T 检测器;

由于 $r_2 > r_1$,因此经训练生成 T 检测器基本不会与 self 串匹配,能够与其进行匹配的几乎都是异常连接. 但 B 检测器极有可能同 self 相绑定,所以需要 T 检测器的协同检测. 当某个 B 检测器识别到的抗原不能与 T 检测器相匹配时,则该 B 检测器将从 B 检测器集合中被删除;反之,说明该 B 检测器与抗原的亲合度较高,则将其从 B 检测器集合中提取出来,成为记忆检测器,用以加快识别速度.

4　检测器的设计与实现

在 B、T 检测器进行训练生成实验之前,首先需要采集正常数据并生成初始正常数据集合. 本文是利用 JPcap 工具收集日常上网的常见数据包并将其作为初始的正常数据集,该初始数据集合共 100 万个包. 然后按照规定的特征映射编码模型将收集初始数据集进行编码并存入数据库中用于耐受体的训练. 生成好的初始正常数据集如图 2 所示.

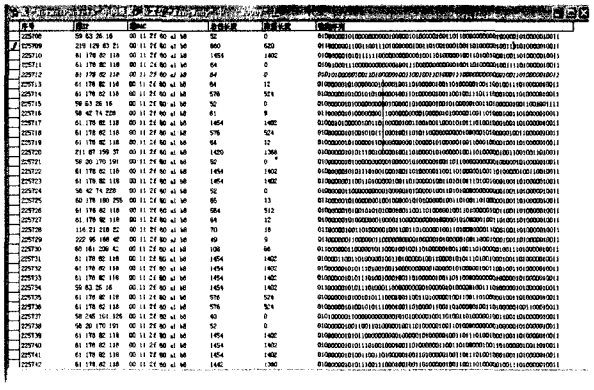

图 2　正常数据集合

Fig. 2　The set of normal data

4.1　检测器的生成

检测器生成过程中所选用的数据集是麻省理工学院林肯实验室提供的 KDDCUP 网络链接记录集,共包含 9 个星期的网络流量数据. 由于原始数据量较大,在实验中抽取了前五周的部分数据进行测试. 其中:第一周和第三周的数据为正常数据,不包含任何攻击信息;第二周的数据中含有 18 种攻击类别,43 个攻击行为数据;第四、五周的数据中共含有 58 种攻击类别,201 个攻击行为数据. 然后,随机生成 30 万个与正常数据集合规定长度一致的二进制字符串集合作为耐受体集合,将耐受体集合中的每个元素(即每个二进制字符串)按照第 3.2 节给出的 B、T 检测器生成算法,分别与正常数据集进行 r - 连续位匹配. 检测器的生成过程如图 3 所示.

生成好的 B、T 细胞检测器被存入 SQLServer2005 设计的数据库中,如图 4 所示.

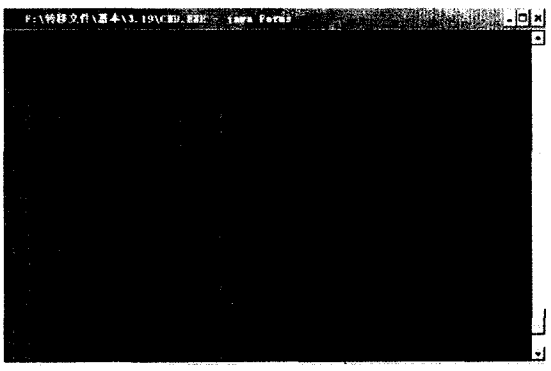

图 3　检测器的生成过程

Fig. 3　The training process of detector

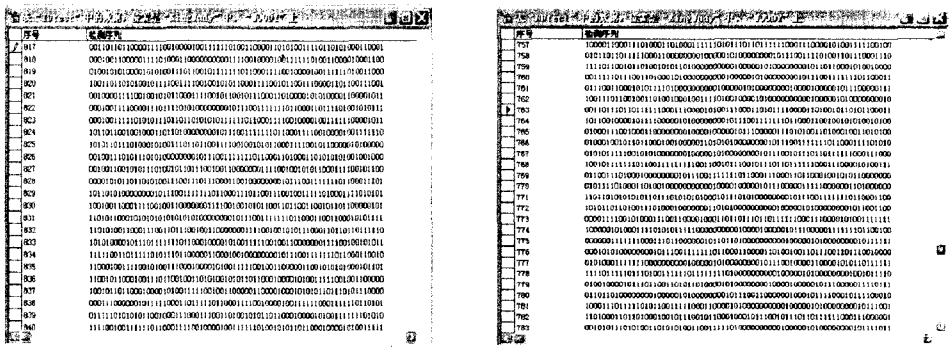

图 4 B 细胞检测器与 T 细胞检测器

Fig. 4 The B - cell and T - cell detector

4.2 检测器的实际运行实验

在检测器的实际运行试验过程中,从 KDD-CUP 网络链接记录集第一周正常数据中随机选取了 200 条,并从第二、四、五周的攻击数据中共抽取了的 76 种典型的攻击行为,其中包括:DoS(拒绝服务攻击)、U - L(本地非法访问攻击)、R - L(远程非法访问攻击)、Probing(非法扫描与探测攻击)、Data(非法泄密攻击)5 个大类.

将所有的攻击行为数据和正常数据混合后,按照规定的特征映射编码模型进行编码,并存储到数据库中,作为测试数据集合.然后将生成好的 B、T 细胞检测器装入实验主机,对测试数据进行检测,检测器的实际运行效果如图 5 所示:

从实验可以看出,生成的 B、T 细胞检测器能够针对正常数据和非法数据进行有效地区分,可以保护主机的正常运行.

5 结束语

本文的主要研究工作在于借鉴人工免疫原理,提出了一个免疫检测器的生成算法,并对其进行了设计与实现.但通过实验发现,否定选择算法最大的时间复杂度呈指数级增长,当问题空间太大时其可行性下降,而且在检测器的生成过程中资源消耗较大.在今后的研究过程中,将结合神经网络、遗传算法以及数据挖掘技术在入侵检测领域中已有的研究成果,对人工免疫原理以及人工免疫系统(AIS)进行理论丰富,寻找更加完善的耐受体训练算法以提高检测器的检测精度.

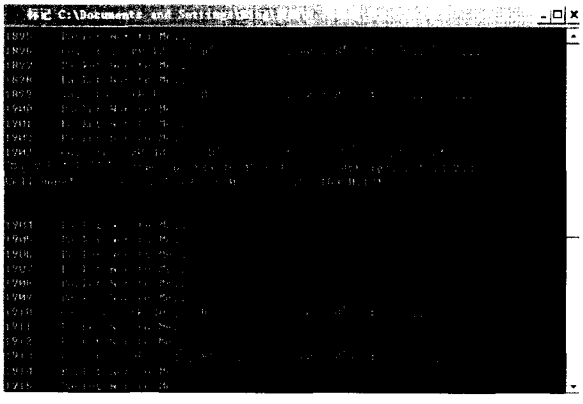

图 5 检测器的运行效果

Fig. 5 The operating result of detector

参考文献:

[1] Bagley J D. The behavior of adaptive systems which employ genetic and correlation algorithms[J]. Dissertation Abstracts International,1968,8(12):218 - 226.

[2] 李 涛. 计算机免疫学[M]. 北京:电子工业出版社,2004.

[3] Jerne N K. Towards a network theory of the immune system[J]. Annual Immunology,1974(125):373 - 389.

[4] Juan Carlos Galeano, Angélica Veloza - Suan, Fabio A. González. A Comparative analysis of artificial immune network models[C]//Proceedings of the 2005 Conference on Genetic and Evolutionary Computation, Washington D C, USA, 2005:361 - 368.

[5] Forrest S, Perelson A S, Allen L, et al. Self - nonself discrimination in a computer[C]//Proc. of the IEEE Symposium on Research in Security and Privacy, Oakland, 1994:251 - 257.

[6] 李征难,梁意文,董红斌. 人工免疫中 B 细胞和 T 细胞的协同演化方法[J]. 计算机工程与应用,2004(36):69 - 72.

[7] 莫宏伟,金鸿章. 免疫算法原理与应用[J]. 航空计算技术,2002,32(4):49 - 51.

[8] 刘克胜,曹先彬,郑浩然. 基于免疫算法的 TSP 问题求解[J]. 计算机工程,2000(26):53 - 56.