结合先天和适应性免疫的蠕虫检测免疫模型

张俊敏 梁意文
(武汉大学计算机学院 武汉 430079)

摘 要 现有的蠕虫检测方法大多通过关闭不安全的端口,切断感染主机与未感染主机之间通信等方法延缓蠕虫传播而达到将损害减少到最低程度的目的。实际上在实施这些方法时往往有许多障碍需要克服,其中的最大障碍就是存在错误检测率高的问题。现将免疫危险理论中的DCs(树突状细胞,Dendritic Cells)-T细胞协同机制用于蠕虫检测,其中DCs属于先天免疫系统细胞,T细胞属于适应性免疫系统细胞。本模型将蠕虫进程触发的系统调用序列当作抗原,将感染蠕虫导致的主机和网络异常当作危险信号。在该模型中,DCs负责危险信号的收集检测并提呈与该危险信号关联的抗原给T细胞检测器进行抗原结构检测。理论分析说明,这样的双重检测方法可以降低伪肯定率和伪否定率,并且记忆T细胞检测器的采用能使系统对类似蠕虫的再次感染反应更加迅速。

关键词 危险理论,反向选择,免疫记忆,树突状细胞,T细胞,蠕虫检测
中图法分类号 TP309 **文献标识码** A

Worm Detection Immune Model Integrating Innate and Adaptive Immunity

ZHANG Jun-min LIANG Yi-wen
(School of Computer, Wuhan University, Wuhan 430079, China)

Abstract As most of existing worm detection methods have a number of significant hurdles to overcome in order to employ such actions as blocking unsecure ports, breaking communication between infected and non-infected hosts to slow down worm propagation and minimize potential damage. The most noteworthy obstacle is the high false positive rate problem. A recently developed hypothesis in immunology, the Danger Theory, states that our immune system responds to the presence of intruders through sensing molecules belonging to those invaders, plus signals generated by the host indicating danger and damage. Inspired by the theory, the paper proposed an artificial immune model for worm detection. The model considers the cooperation of Dendritic Cells (DCs) in the innate immune system and T cells in the adaptive immune system, in which system calls comprising a process generated can be viewed as antigens and the corresponding behavioral information of the system and network can be viewed as signals. The theory analysis shows that the dual detection method of DCs detecting the behavioral information caused by antigens and T cells detecting antigens can decrease false positive rate, and the model also has a fast secondary response to the reinfection by the same or similar worm.

Keywords Danger theory, Negative selection, Immune memory, Dendritic cells (DCs), T cells, Worm detection

蠕虫是一种可以在网络中自动传播的程序,利用常见服务的安全漏洞或策略缺陷,通过网络进行传播。与传统的计算机病毒相比,蠕虫具有更强的繁殖能力和破坏能力,一台感染蠕虫的计算机可以在瞬间感染成千上万的目标系统,导致大规模的网络阻塞甚至网络瘫痪。比如,2001年7月19日,Code Red蠕虫爆发,9小时攻击主机达25万台之多,造成20亿美元的损失。

正因为如此,现在越来越多的研究人员对蠕虫检测方法的研究投入了大量的精力。比如John W. Lockwood等人提出了一种采用可编程逻辑设备对抗网络蠕虫的防范系统[1]。该系统将网络中的数据报文内容和已掌握的网络蠕虫的特征码或规则表达式进行匹配,根据匹配的结果来确定蠕虫是否存在。Malan等人则通过分析对等的两个操作系统上的系统调用序列是否存在相似性来判断蠕虫的活动情况[2]。CHEUNG S等通过建立和分析节点间的行为图(activity graph),再通过与预定义的行为模式进行匹配来检测网络蠕虫是否存在[3]。G. BAKOS等提出了一种通过分析和收集网络中的ICMP-T3数据包来检测蠕虫的方法[4]。基于经典的Kermack-Mckendrick模型,文献[5]提出了一个采用动态隔离策略、动态传染率和恢复率的蠕虫传播模型。但是由于未知蠕虫多样性、攻击模式的不确定性以及这些方法本身的不足,导致这些方法大多存在错误检测率高、时效性差等问题。

本文的目标在于借鉴机体免疫原理来建立一个用于蠕虫检测的人工免疫模型。在先前的研究中,借鉴传统机体免疫

到稿日期:2009-01-22 返修日期:2009-05-11
张俊敏(1981-),男,博士生,主要研究方向为人工免疫学等,E-mail:zhangjm81@sohu.com;梁意文(1962-),男,教授,博士生导师,主要研究方向为计算智能、信息安全。

原理的人工免疫系统(比如反向选择算法、克隆选择算法)已经用于计算机安全中,旨在检测未知的入侵和异常的网络流量模式、异常的系统调用序列等异常活动[6,7]。该类算法借鉴传统免疫理论中机体免疫系统仅对不属于自身的所谓"非我"做出响应的特点,采用的是预定义自我集并通过反向选择产生检测器集进行检测的方法,虽然可以有效检测未知的入侵和异常行为,但同样存在错误检测率过高的问题[6,7]。

1994 年 Polly Matzinger[8] 提出新的机体免疫学理论——危险理论。该理论跳出经典机体免疫学中"自我-非我"的划分概念,强调触发免疫反应的是"危险",而不是所谓的"非我"。该理论认为,机体免疫系统收集危险信号及产生这些危险的相应抗原,并触发适当的免疫反应。Uwe Aickelin 等[9]首次将危险理论引入到人工免疫系统(AIS)中,期待解决原有 AIS 存在的问题[6,7]。2005 年 Jungwon Kim 等[10]借鉴该理论提出了一个基于 T 细胞免疫与耐受的蠕虫协同检测算法,该算法给出了一个大致的框架,但对"危险"的界定及 T 细胞的定义没有做更多的阐述。

本文在前人工作的基础上,借鉴危险理论,并以如何判定是否对系统产生"危险"征兆为重点,结合反向选择、免疫记忆,提出了一个用于蠕虫检测的人工免疫模型。本模型考虑了 DCs-T 细胞的协同,其中 DCs 负责检测危险信号,T 细胞负责检测与之相关的抗原结构。该模型的目的在于在感染早期就能探测到蠕虫的存在,使双重检测的错误检测率较低。

1 背景知识

1.1 危险理论

针对传统机体免疫理论中的"自我-非我"划分模式无法解释机体免疫中的诸多现象,比如无法解释自身免疫疾病、成功的器官移植等,Polly Matzinger 于 1994 年提出危险理论[8]。该理论消除了传统免疫学中自身与异己的界线,认为无论是自身抗原还是异己抗原,只要它们损伤了机体内的细胞,就会由这些受损细胞发出危险信号,从而激活免疫系统,发挥其特异性免疫应答功能。

机体免疫系统通常被分为两个截然不同而又相互联系的子系统:先天免疫系统和适应性免疫系统[11]。先天免疫系统通常扮演 3 个角色:在感染早期阶段非特异性识别病原体以保护机体,诱导适应性免疫发生,决定适应性免疫类型;而适应性免疫系统则通过特异性识别病原体。

树突状细胞(Dendritic cells,DCs),作为先天免疫系统的一部分,同时也是专职的抗原提呈细胞,能与来自宿主细胞的抗原相互反应并控制适应性免疫细胞的状态。

DCs 的初始状态为不成熟,不成熟的 DCs 从细胞外空间摄取抗原并进行内部处理。在处理过程中,抗原被分解并绑定在主要组织相容性复合体(MHC)分子上,然后将"MHC-抗原"复合体在一定条件下提呈到 DCs 表面。除了从周围环境中摄取抗原外,DCs 也有受体,能对它们周围的一系列信号分子做出响应。某些分子,比如脂多糖,统称为病原相关分子蛋白(pathogen-associated molecular proteins,PAMPs),是所有病原体都具备的。该类分子能与 DCs 表面的 toll-like 受体(TLRs)绑定。

有一类分子,称为危险信号,比如热休克蛋白,是与宿主细胞受到损伤以及与不正常细胞坏死相关联的。还有一类分子,称为安全信号,是与炎症、正常的细胞凋亡相关的。这两类分子都能与 DCs 表面的受体绑定。DCs 当前的成熟状态是由这些复杂的信号网络来决定的。DCs 本身也能分泌称为因子的输出信号分子来控制其它类型细胞的状态。而 DCs 信号分子输出的数量和强度又依赖于它当前的成熟状态。DCs 存在 3 种状态:不成熟、半成熟、成熟,而这些状态又决定了其具体功能。如果不成熟的 DCs 暴露在 PAMPs 和危险信号占优势的环境中,DCs 便分化为成熟的 DCs,并产生成熟 DCs 的输出信号分子 IL-12,其能激活与提呈抗原绑定的 T 细胞;相反,如果不成熟的 DCs 暴露在安全信号占优势的环境中,DCs 就分化成半成熟的 DCs,并产生半成熟 DCs 的输出信号分子 IL-10,该类分子不激活与抗原发生绑定的 T 细胞。两种情况 DCs 都会从组织中移出并迁移到本地淋巴结中。在淋巴结中,DCs 通过其 MHC 提呈抗原给 T 细胞。图 1 是不成熟 DCs 的分化过程。

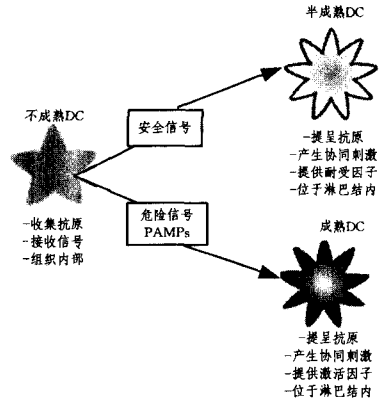

图 1 不成熟 DCs 的分化过程

作为适应性免疫系统成员的成熟 T 细胞是在胸腺中经历了反向选择过程而发育成功的:一个不成熟 T 细胞若与胸腺中任何一个自我抗原匹配,将会自动死亡,而存活下来的 T 细胞是成熟的。成熟 T 细胞从胸腺中迁移出并在血液和淋巴器官之间循环以捕获 DCs 提呈的抗原。成熟 T 细胞的最终激活是由 DCs 所提呈的抗原和 DCs 的输出信号分子决定的。激活后的 T 细胞获得增殖的能力,并且它们的克隆开始分化为辅助 T 细胞(Th cells)或效应 T 细胞(CTLs)。当 Th cells 受体绑定 DCs 所提呈抗原并且收到 DCs 所释放的信号分子(即协同刺激信号)IL-12 时,其被激活,如果 Th cells 所收到的信号分子是 IL-10,则意味着所检测到的抗原可能是自我抗原,其对该 T 细胞是耐受的,因此应删除该 T 细胞。激活的 Th 细胞能释放辅助因子去激活效应 T 细胞(CTLs)。在这些抗原被 CTLs 受体所识别,Th 细胞释放的因子辅助刺激该识别的情况下,该 CTLs 被激活,最终导致免疫反应发生。完成该工作后,大部分 CTLs 死亡,剩余部分变为记忆 CTLs。记忆 CTLs 存活时间更长,能对相似病原体再次入侵响应得更快,并且不需要 Th 细胞的协同刺激就能再次被激活。

1.2 相关概念的对应

程序运行都会触发一系列的系统调用,以提供应用、操作系统和硬件之间的互动。蠕虫由于也是可执行文件,同样不会例外。在这里可以将此系统调用看作是抗原。由于在蠕虫爆发时往往会带来主机和网络的异常,在主机级表现为 CPU 和内存占用率偏高并且波动很大;在网路级表现为带宽耗尽,

收发数据包异常，本地主机的发出连接请求偏高等，这些可以统称之为危险信号。反之，如果这些参数是正常的，则称之为安全信号。

2 系统结构模型

每次蠕虫爆发，往往会造成大面积的网络瘫痪，而且蠕虫传播的速度越来越快，留给安全人员的响应时间也越来越短。在蠕虫爆发的初始阶段就探测到它的存在，便显得尤为重要。在这种情况下，本文借鉴机体免疫中的危险理论原理，提出了一个用于蠕虫检测的人工免疫模型。由于生物系统和计算机系统的不完全一致性，本文提出的人工免疫模型和机体免疫系统也同样具有不完全的一致性。

2.1 总体框架

系统的总体架构和各模块间的关系如图 2 所示。主要包括先天免疫层和适应性免疫层两大块，其中先天免疫层主要负责信号采集和评估、抗原的提取和提呈，适应性免疫层主要负责检测器的生成和抗原结构的检测。

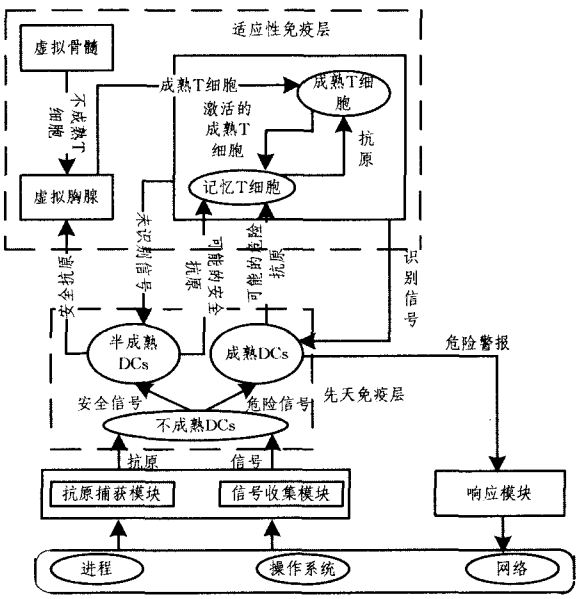

图 2 模型的总体架构图

2.2 抗原捕获模块和信号收集模块

抗原捕获模块负责捕获抗原数据。由于蠕虫运行产生的进程会触发一系列的系统调用，因此，抗原可以看作是这一系列系统调用的子集，对系统调用序列的捕获可以使用工具 systrace。在经过一个延迟时间 Δt 后，该模块才会将所捕获的抗原序列传给随后的不成熟 DCs 进行处理。这样做的目的是让相应的信号收集模块收集到足够的与该进程相关的系统和网络信息。

信号收集模块包括进程信号收集 Agent 和网络信号收集 Agent。蠕虫在运行时一般都会表现出一些特征，因此一个蠕虫在发作的时候，一般在主机级表现为系统运行速度变慢，CPU 占用率偏高甚至达到 100%，内存占用过高等；在网络级的表现通常为：网络流量偏大，本地主机连接数过高，收发数据包异常，局域网时断时续，网络效率很低。该模块主要负责收集相应抗原所引起的系统和网络资源的这些变化信息并提交给不成熟 DCs 做进一步处理。

进程信号收集 Agent 负责收集由于蠕虫的运行所引起的系统资源的变化，记为 $S_{process}=\{C,M,\cdots\}$。其中，$C$ 为 CPU 的负载情况，M 为内存的占用情况等。

网络信号收集 Agent 负责收集由于蠕虫的运行所引起的网络资源的变化，记为 $S_{networking}=\{L,F,\cdots\}$。其中，$L$ 为本地主机连接数，F 为流量参数等。

对于连续变化的参数，在延迟时间 Δt 内按照固定的采样周期采集参数值。设从时间 t_0 开始采集参数值，以 T 为周期对不同时刻的参数值进行采集，每类参数分别获取 $(1+\Delta t/T)$ 个不同的参数值：

CPU 负载情况 C 采样：$C_{t_0 1}, C_{t_0 2}, \cdots, C_{t_0 (1+\Delta t/T)}$；

内存占用情况 M 采样：$M_{t_0 1}, M_{t_0 2}, \cdots, M_{t_0 (1+\Delta t/T)}$；

网络流量情况 F 采样：$F_{t_0 1}, F_{t_0 2}, \cdots, F_{t_0 (1+\Delta t/T)}$；

……

对于非连续变化的参数，比如本地主机的连接数参数 L，我们知道，感染蠕虫的主机在单位时间内发出的连接数远大于其在正常情况下单位时间发出的连接数。比如 Code Red 在传播过程中，平均每秒向 100 个不同的 IP 地址进行扫描，远远大于一般正常主机的网络行为。因此在延迟时间 Δt 内记录了本地主机发出的连接请求数 n。

2.3 DCs 的成熟与分化

该模块主要实施两大功能：多信号处理功能和抗原提呈功能。

该模块对信号收集模块采集的系统和网络资源信号进行处理后产生一个输出信号 $output$，其中 $output\in\{0,1\}$。“1”代表“危险”，则将同期捕获的相关抗原认定为“可能的危险抗原”，并交由记忆 T 细胞检测器进行首次抗原结构快速识别；“0”代表“安全”，则将相应的抗原数据认定为“可能的安全抗原”，并通过 T 细胞检测器返回的协同刺激信号（未识别信号）协同而交由虚拟胸腺（成熟 T 细胞检测器生成模块）进行耐受处理。

如果不成熟 DCs 所处理的参数是连续变化的参数，则将系统在安全状态下采集到的参数序列均值作为比较的基准点。以 CPU 的使用情况 C 为例，$\bar{C}$ 为安全状态下 CPU 使用情况的均值，将延迟时间 Δt 内采集的每个参数值 $C_{t_0 i}$ 和 $\bar{C}$ 进行差分运算，$\Delta C=|C_{t_0 i}-\bar{C}|$。如果 $\Delta C\leqslant\delta(\delta\geqslant 0)$，$\delta$ 是偏离常数，则认为该参数在 t_0+iT 时刻是正常的；反之是异常的。如果在 Δt 时间段内采集的参数值异常数目超过阈值 $Threshold_C$，则该参数“危险”，$Signal_C=1$；否则“安全”，$Signal_C=0$。

如果信号处理 Agent 处理的是非连续变化的参数，比如本地主机的连接数参数 L，则随机抽取正常主机在多个时段在时间间隔 Δt 内的平均连接数 $\bar{N}$ 作为基准。由于在相同时间间隔内，感染网络蠕虫的主机所产生的不同连接数目远大于正常主机的不同连接数目，因此为了提高正确的检测率，设定系数 $\ell(\ell>1)$，如果监控到的主机连接数目 $n>\ell N$，则认定参数 L 是“危险”的，$Signal_L=1$；否则认定该参数 L 是“安全”的。

蠕虫爆发往往带来上述多个参数是“危险”的，但凭一个参数“危险”往往难以确定是否感染蠕虫，如文件下载也会带来大流量。因此，根据每个参数的重要程度，为其设置了合适的权重。比如 $C,M,F,L,\cdots$，其权重分别设置为 $w_C, w_M, w_F, w_L, \cdots$。计算 $cav=Signal_C w_C+Signal_M w_M+Signal_F w_F+Signal_L w_L+\cdots$。

如果 cav 高于一定的阈值 $Threshold_{cav}$，则输出信号 $output=1$，代表对这些系统和网络资源信号进行综合评估后，认定它们预示着“危险”，则 DCs 由不成熟状态转为成熟状态并提呈相应的可能的危险抗原给 T 细胞检测器进行结构检测。如果有 T 细胞检测器和该抗原匹配，T 细胞检测器块会返回一个识别信号（协同刺激信号）给成熟 DCs，收到识别信号后成熟 DCs 会向响应模块发出危险警报；否则 $output=0$，认为该抗原可能是正常的程序所引起的，比如是新安装的新程序，DCs 由不成熟状态转为半成熟状态并提呈相应抗原给 T 细胞检测器进行结构检测，如果该抗原和所有的 T 细胞检测器都不匹配，T 细胞检测器块会返回一个未识别信号（协同刺激信号）给半成熟的 DCs，在收到未识别信号后，半成熟的 DCs 将该抗原提呈给虚拟胸腺实施耐受。

2.4 虚拟骨髓（不成熟 T 细胞检测器生成模块）

该模块本质是不成熟 T 细胞检测器生成模块，负责随机生成不同组合的系统调用序列，得到不成熟 T 细胞检测器 $Ab=b_1b_2\cdots b_u$（$0<u<v$），并将其传给虚拟胸腺。

2.5 虚拟胸腺（成熟 T 细胞检测器生成模块）

该模块用于成熟 T 细胞检测器的生成，并持续性接收由半成熟 DCs 所提呈的抗原（正常程序所触发的系统调用序列）。

训练阶段可以在一个真实的环境中进行，此阶段中成熟 DCs 向 T 细胞检测器提呈抗原功能是暂时关闭的。由于此阶段处理的都是正常程序所触发的系统调用序列，即安全抗原，它们所触发的系统和网络资源信号经过综合评估是“安全”的，自然这些系统调用序列组成了一个初始的自我集，进入虚拟胸腺进行耐受处理。由于该自我集的存在，所有进入该模块的不成熟 T 细胞检测器都要与该“自我”集进行一个反向选择过程：如果不成熟 T 细胞检测器和安全抗原集中的某抗原发生匹配，则删除该不成熟 T 细胞检测器；否则将该不成熟 T 细胞检测器转为成熟 T 细胞检测器并传给成熟 T 细胞检测器检测块。匹配算法采用海明距离，定义如下：

$$\text{海明距离}\quad A_i=\sum_{j=1}^{u}m_{ij},\begin{cases}m_{ij}=1,b_j=g_{i+j-1}\\ m_{ij}=0,\text{otherwise}\end{cases}$$

$$1\leqslant i\leqslant v-u+1,1\leqslant j\leqslant u$$

$$\text{亲和力}\quad F_{affinity}(u,v)=\max(A_1,A_2,\cdots,A_{v-u+1})$$

$$\text{匹配度}\quad F_r(u,v)=\begin{cases}1,F_{affinity}(u,v)/u\geqslant\lambda_r\\ 0,\text{otherwise}\end{cases}$$

由于系统资源限制，设定自我集中安全抗原的数量是常数 N_{self}，一旦其数量超过 N_{self}，系统将转入到检测阶段，成熟 DCs 向 T 细胞检测器提呈抗原功能自动开启。这里为每个进入该模块的安全抗原设置记录其进入该模块的时间属性。

在检测阶段，可能由于新安装程序触发新的系统调用序列，还会有新“安全抗原”陆续进入到该模块，则该“安全抗原”仅和新产生的不成熟 T 细胞检测器进行匹配，而不需和那些经历过反向选择的 T 细胞检测器进行匹配；而同时由于某些程序的卸载，则可将相应的“安全抗原”从“自我”集中删除。

2.6 成熟检测器检测模块

同样由于系统资源限制，成熟 T 细胞检测器数量设为常数 N_d，并且每个检测器都有计时器 C_i，初始 $C_i=0$。状态属性 $State\in\{0,1\}$，“0”表示成熟 T 细胞检测器未被激活；“1”代表成熟 T 细胞检测器被激活。如果成熟 T 细胞检测器与成熟 DCs 提呈的“可能的危险抗原”匹配，则表明该成熟 T 细胞检测器被预激活一次，其预激活计数器 $Count_{preaction}$（初始 $Count_{preaction}=0$）自动加 1，预示着一次低等级危险发生，可能是感染了蠕虫，但不会立刻向成熟 DCs 返回识别信号（协同刺激信号）。与用户行为习惯的变化或错误操作引起的低等级危险不同，蠕虫造成的异常则集中且连续出现，导致这样低等级危险连续出现。当 $Count_{preaction}$ 大于激活阈值 $Threshold$ 时，预示高等级警报发生，表明感染了蠕虫，成熟 T 细胞检测器被激活（状态 $State=1$），并返回识别信号（协同刺激信号）给成熟 DCs。同时该检测器转为记忆 T 细胞检测器，$Count_{preaction}$ 重新置 0，计时器 C_i 重新置 0，并传给记忆 T 细胞检测器块。匹配计算同第 2.5 节中方法。

如果成熟 T 细胞检测器数量低于上限值 N_d，新成熟 T 细胞检测器会继续通过虚拟胸腺中的反向选择产生并加入；如果成熟 T 细胞检测器数量高于 N_d 时，删除 $Count_{preaction}$ 最小的一个。在出现多个 T 细胞检测器预激活数相等情况下，按计时器 C_i，采用“最旧未使用”删除成熟 T 细胞检测器。

2.7 记忆 T 细胞检测器检测模块

记忆 T 细胞检测器由于其激活阈值 $Threshold'$ 小于成熟 T 细胞检测器激活阈值 $Threshold$，与成熟 T 细胞检测器相比，能对经历过的蠕虫进行更快的响应，在初始阶段就探测到它的存在。记忆 T 细胞检测器会先对抗原首次快速识别，如成功识别则返回识别信号（协同刺激信号）给成熟 DCs；若失败，则交由成熟 T 细胞检测器继续识别。

记忆 T 细胞检测器数量为常数值 N_m，并保证每个记忆 T 细胞检测器的唯一性。对于不具备唯一性的，保留最新的一个。如果没有与该新记忆 T 细胞检测器类似的旧检测器，在检测器数量超过上限值 N_m 时，按照“最旧未使用策略”删除其中最久未被激活的记忆 T 细胞检测器。

2.8 响应模块

响应模块包括报警和阻断两种响应方式。报警方式是以电子邮件等途径将结果及时报告网络管理人员，使网络人员能及时对异常数据包进行分析。阻断方式可以控制蠕虫扫描传播的数据包从而降低蠕虫可能造成的损失程度。

当发现感染了蠕虫的主机时，响应模块将通过以下的测量达到对蠕虫控制的目的：

1）报警：产生报警，通知网络管理员。通知存在漏洞的主机下载补丁进行漏洞修复，防止蠕虫进一步传播，并启动相关的杀毒软件对感染了蠕虫的主机进行蠕虫的删除工作。

2）防火墙互动：通过利用防火墙提供的接口，对防火墙规则进行修改，防止外网的蠕虫数据包感染局域网内的主机。

当发现内网主机被蠕虫感染时，能在真实入侵时采取中断行为，如丢弃一个可疑的数据包，关闭相关的进程，切断已感染的子网同局域网内其它子网的通信，防止蠕虫在局域网中大肆传播，同时可以控制因为蠕虫发作而产生的大量的网络流量。

3 模型特性分析

本系统可以部署在网络中需要重点保护的服务器或节点主机上，同时通过协作通道，各节点之间可以实现交流。当一种新的蠕虫被其中任一节点检测到时，该节点会迅速通过协作通道迅速通知其它部署了该系统的节点更新记忆 T 细胞

检测器库，以保证其它节点同样具有快速检测该蠕虫的能力。

本文所提出的蠕虫检测免疫模型与其它蠕虫检测方法相比在很多方面具有优势，下面对这些优势加以分析。

首先，本模型具有较好的开放度。相比传统反向选择、克隆选择算法中训练阶段是在受保护的环境中进行，本文模型由于在训练阶段记忆检测器模块关闭，该阶段可以在开放的环境中完成。

其次，本模型采用 DCs 检测抗原的系统和网络信息、T 细胞检测器识别抗原结构的双重识别方法降低了系统的错误检测率。在危险信号存在的情况下，如果成熟 T 细胞检测器和记忆 T 细胞检测器都不匹配与此危险信号相关的所谓的"危险"抗原，或者有匹配发生，但是在规定时间内二者之间匹配次数达不到检测器的激活阈值，都说明该危险信号不是真正的"危险"，该"危险"抗原有可能是"安全"抗原；如果安全信号存在且不成熟 DCs 提呈可能的安全抗原给 T 细胞检测器，即便有识别信号产生，不成熟 DCs 也不会将该抗原交给虚拟胸腺进行耐受处理。两种情况下系统都不会做出任何响应，降低了错误检测率。

此外该模型通过"危险与否"实现虚拟胸腺中"自我"集的更新，从而使模型具备了很好的自适应性。如果 DCs 的输出信号是"安全"的，则同期采集到的相应抗原是"安全"的，将其加入到虚拟胸腺中的"自我"集中，最终导致成熟 T 细胞检测器集的更新。

最后，由于记忆 T 细胞检测器的引入，记忆检测器激活阈值更低，可以保证模型对经历过的攻击进行快速响应，提高了系统的执行效率。

结束语 本文详细描述了危险理论中先天免疫系统(DCs)和适应性免疫系统(T cells)的协同，在此基础上提出用于蠕虫检测的人工免疫模型，并对主要功能模块的实施进行了详细的描述，最后从理论上对模型的性能进行了分析。在该模型中，以分析蠕虫引起的系统和网络资源的变化信息是否预示"危险"为中心，同时结合了适应性免疫中的反向选择、免疫记忆原理。本模型应具有如下优势：1)采用双重检测：在 DCs 处理模块完成对蠕虫引起的系统和网络"危险"的初步检测后，呈捕获的相应抗原由记忆 T 细胞检测器或者成熟 T 细胞检测器完成下一步检测，这样降低了错误检测率；2)同时，记忆 T 细胞检测器的引入，可以保证对感染过的蠕虫进行快速响应，提高时效性，阻止蠕虫进一步蔓延；3)由于采用双重识别，如果仅仅检测到危险，而相应的匹配没有发生，则说明不是真正的"危险"，可以忽略；4)由于模型以"危险"与否确定蠕虫身份，不再完全依赖于蠕虫特征码的提取，这样对于多态蠕虫具有较好的检测效果。这些都对建立一个更加健壮的蠕虫检测系统具有重要的意义。

接下来仍然有许多的工作要做。以下几点将是未来工作的重点：开发出实验系统，以更好地验证本文所提出模型所具备的种种优势；大量参数值的合理设置如何获取；将机体免疫学中的其它机理引入到本模型中，比如 T 细胞的克隆增殖等等。

参 考 文 献

[1] Lockwood J W, Moscola J, Kulig M. Internet worm and virus protection in dynamically reconfigurable hardware[J]. WORM, 2003

[2] Malan D J, Smith M D. Host-Based detection of worms through peer-to-peer cooperation[C]// Keromytis AD, ed. Proc. of the 2005 ACM Workshop on Rapid Malcode. 2005: 72-80

[3] Cheung S, Hoagland J, Levitt K. The Design of GrIDS: A graph-based intrusion detection system[R]. CSE- 99- 2, U. C. Davis Computer Science Department, 1999

[4] Bakos G, Berk V. Early detection of Internet worm activity by metering ICMP destination unreachable activity[C]// The SPIE conference on Sensors, and Command, Control, Communications and Intelligence. 2002

[5] 张运凯，王方伟，马建峰，等. 基于隔离策略的蠕虫传播模型及分析[J]. 计算机科学，2005，32(3)：62-65

[6] Aickelin U, Greensmith J, Twycross J. Immune system approaches to intrusion detection-a review[C]// Proceedings of ICARIS'04. September 2004: 316-329

[7] Kim J. Integrating Artificial Immune Algorithms for Intrusion Detection[D]. Department of Computer Science, University College London, 2002

[8] Tolerance M P. Danger and the Extended Family[J]. Annual Review in Immunology, 1994, 12: 991-1045

[9] Aickelin U, Cayzer S. The Danger Theory and Its Application to AIS[C]// 1st International Conference on AIS. 2002: 141-148

[10] Kim J, Wilson W, Aickelin U, et al. Cooperative Automated Worm Response and Detection Immune Algorithm (CARDINAL) inspired by T-cell Immunity and Tolerance[C]// The 3rd Int. Conf. on AIS (ICARIS-05). 2005: 168-181

[11] Twycross J. Integrated Innate and Adaptive Artificial Immune Systems Applied to Process Anomaly Detection[D]. University of Nottingham, 2007

(上接第 72 页)

参 考 文 献

[1] Denning D. Reflectons on cyberweapons controls[J]. Computer Security Journal, 2000, 16(4): 3-53

[2] Gordon L A, Loeb M P, Lucyshyn W, et al. CSI/FBI Computer Crime and Security Survey[M]. Computer Security Institute, 2005

[3] Geer D, Soo Hoo K, Jaquith A. Information security: Why the future belongs to the quants[J]. IEEE Security and Privacy, 2003, 1(4): 24-32

[4] 陈天平，乔向东，郑连清，等. 图论在网络安全威胁态势分析中的应用[J]. 北京邮电大学学报，2009，32(1)

[5] 陈光. 信息系统信息安全风险管理方法研究[D]. 长沙：国防科学技术大学，2006：146-153

[6] 彭俊好，徐国爱，杨义先，等. 基于效用的安全风险度量模型[J]. 北京邮电大学学报，2006，29(2)

[7] Menoncin F. Optimal portfolio and background risk: An exact and an approximate solution[J]. Insurance Mathematics and Economics, 2002, 31(2): 249-265

[8] Huang C D, et al. An economic analysis of the optimal information security investment in the case of a risk-averse firm[J]. Production Economics, 2008, 114: 793-804

[9] Kaas R, Gavaerts M, Phaene J, et al. Modern actuarial risk theory [M]. Boston, MA: Kluwer Academic Publishers, 2001