

基于免疫机理与合同网协议的 多 Agent 入侵检测系统

马 鑫^{1,2}, 梁艳春^{1,2}, 田 野^{1,2}, 于 涛³

(1. 吉林大学计算机科学与技术学院,长春 130012; 2. 吉林大学符号计算与知识工程教育部重点实验室,
长春 130012; 3. 中国科学院长春光学精密机械与物理研究所, 长春 130033)

摘要: 建立了一种基于免疫机理与合同网协议的多 Agent 入侵检测系统 ICNPIDS。在被动免疫抗体 PAb、记忆自动免疫抗体 MANAb 及模糊自动免疫抗体 FANAb 的基础上, 将合同网的协同方法应用到抗体检测中, 提出了联合免疫抗体 UAb 的概念, 并研究了 UAb 抗体的生成、检测和更新过程, 从构造上克服了 Agent 间分析经验难以共享借鉴的问题。通过滥用检测和异常检测技术的使用, 显著提高了系统的检测性能, 增强了系统对于外界负载变换的适应能力。模拟实验结果验证了 ICNPIDS 是一种具有较高检测性能、可自主适应环境变化的入侵检测系统。

关键词: 计算机应用; 网络安全; 入侵检测; 人工免疫; 合同网协议; 联合免疫抗体; Agent

中图分类号: TP393 **文献标志码:** A **文章编号:** 1671-5497(2011)01-0176-06

An immune and contract net protocol-based multi-agent intrusion detection system

MA Xin^{1,2}, LIANG Yan-chun^{1,2}, TIAN Ye^{1,2}, YU Tao³

(1. College of Computer Science and Technology, Jilin University, Changchun 130012, China; 2. Key Laboratory of Symbol Computation and Knowledge Engineering of the Ministry of Education, Jilin University, Changchun 130012, China; 3. Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China)

Abstract: A multi-agent intrusion detection system (ICNPIDS) was proposed based on immune and contract net protocol. Applying the cooperation method of the contract net protocol to intrusion detection, the concept of united immune antibodies was also proposed by analogy with the passive immune antibodies, the memory automatic antibodies, and fuzzy automatic immune antibodies. The generation, detection, and updating of the united immune antibodies were examined, which overcomes the difficulty that the analytic experience can not be shared between agents. The efficiency of the intrusion detection model that uses abusive detection and the analogy detection was improved greatly. Experiment results show that ICNPIDS is a more adaptive and efficient system.

Key words: computer application; network security; intrusion detection; artificial immune; contract net protocol; united immune antibody; Agent

收稿日期: 2010-01-08.

基金项目: “863”国家高技术研究发展计划项目(2009AA02Z307); 国家自然科学基金项目(10872077); 吉林省科技发展计划项目(20080708).

作者简介: 马鑫(1981-), 男, 博士研究生。研究方向: 计算智能, 人工智能, 智能信息处理。E-mail: chairmancit@hotmail.com
通信作者: 梁艳春(1953-), 男, 教授, 博士生导师。研究方向: 计算智能, 生物信息学。E-mail: yeliang@jlu.edu.cn

随着网络规模的日益扩大以及入侵行为的复杂化,传统的集中式入侵检测系统已经越来越不能满足当前社会的需要,因此基于多 Agent 的分布式入侵检测系统作为一种行之有效的方法,已经成为广大学者研究的热点。但目前基于多 Agent 的入侵检测系统却普遍存在着以下不足:①入侵检测技术不够先进,系统的检测率有待提高;②Agent 之间的依赖程度大,系统不够健壮、灵活^[1];③用于系统分析的 Agent 往往缺少一定的合作机制,Agent 间的分析经验难以共享借鉴。本文针对上述问题,提出了一种基于免疫机理与合同网协议的多 Agent 入侵检测系统 ICNPIDS (Immune and contract net protocol-base multi-agent intrusion detection system), 给出了 ICNPIDS 的系统结构,讨论了各 Agent 的工作原理;在被动免疫抗体 PAb、记忆自动免疫抗体 MANAb 及模糊自动免疫抗体 FANAb 的基础上,借鉴合同网协议提出了联合免疫抗体(UAb)的概念,研究了其生成与检测的方法,从构造上克服了 Agent 间分析经验难以共享借鉴的问题;最后对 ICNPIDS 进行了仿真实验,实验表明该系统具有良好的检测性和自适应性。

1 免疫机理与合同网协议

1.1 免疫机理

由于生物免疫系统在抵抗病毒和细菌等病原体的入侵方面与网络入侵检测系统具有惊人的相似性,因此将生物免疫技术引入到网络入侵检测中,解决计算机网络安全问题。根据生物免疫系统原理,获得性免疫主要分为被动免疫和自动免疫两种。被动免疫是婴儿在形成发育过程中由母体的血清抗体(IgG)通过初乳(IgA)、胎盘进入婴儿体内或者通过注入同/异种抗体形成的,这样婴儿就获得了与母体类似或者具有特定抗原的免疫能力^[2]。在自动免疫中,B 淋巴细胞和 T 淋巴细胞分别在骨髓和胸腺经历克隆消除 (clonal deletion) 或阴性选择 (negative selection), 获得对自身的隐含描述,然后进入循环系统和淋巴系统,根据自身的记忆与有害抗原发生不精确的粘合反应,从而区分出自身和非自身^[3-4],因此自动免疫是婴儿依赖 T 淋巴细胞和 B 淋巴细胞对遇到的大量新型复杂抗原的免疫能力。

1.2 合同网协议

合同网协议是 Smith^[5] 在 1980 年研究分布

式求解问题时提出来的,后来被广泛地应用于多 Agent 系统的协调中,它把一个多 Agent 系统看作是一个由多个节点组成的合同网,每个节点是一个 Agent。这些结点可分为管理者、投标者和中标者三类。合同网的具体过程是:管理者把自己负责的任务以招标的方式通知系统中的所有潜在投标者。招标信息中包含任务的具体要求,以及所能承受的代价等。接到招标信息后,投标者按照自己所能提供的处理类型和期望收益,选择收益最大的任务,并向相应的管理者发出投标信息。投标信息中给出了完成任务的具体时间和代价等。收到投标信息后,管理者按照处理要求,选择能满足要求并且代价最小的投标者作为潜在中标者,然后向其发出中标通知信息。得到中标信息后,中标者向管理者发出确认信息。这样,管理者(任务方)和中标者(承包方)就完成了相互选择过程,建立起了合同关系,也即完成了任务的分配。当完成所有招投标过程后,任务调度也就完成了。

2 本文的入侵检测系统

2.1 系统框架结构

ICNPIDS 由数据采集 Agent(DCA)、免疫检测 Agent(MDA)、调度 Agent(SA) 和管理 Agent (MA) 构成。系统的体系结构如图 1 示。DCA 属于资源请求方,负责采集网络数据流,并进行数据包的解析和特征提取统计工作。由于 ICNPIDS 采取的是以太网卡的杂收工作模式,因此 DCA 通过 WINPCAP 抓包库获得经过本网段的所有特征数据 TZData ,并将其提交给 MDA。

MDA 是一种需要注册才可以使用的资源,MDA 负责生成能够检测网络入侵的免疫检测抗体,并利用这些抗体对网络数据包进行检测,区分出攻击数据包。每个 MDA 都会常驻三种免疫抗体:PAb 抗体、MANAb 抗体和 FANAb 抗体,其中 PAb 抗体是利用已知的入侵特征的知识形成规则,将这些规则直接存入滥用检测规则集,发布给入侵检测系统,使得系统在开始工作时就具有基本的免疫能力;MANAb 抗体主要检测一些基本的异常情况,它由学习到的自身正常轮廓库和一些简单的异常检测规则 (MRule) 组成,输出有两种状态,即正常或异常;FANAb 抗体主要检测一些复杂的异常情况,它是由学习到的正常统计特征库与模糊异常检测规则 (FRule) 共同组成的。

一组模糊推理系统,输出表示判断网络数据包是攻击的可能性,它有三种状态,即正常、怀疑和异常。MDA 的结构如图 2 所示。

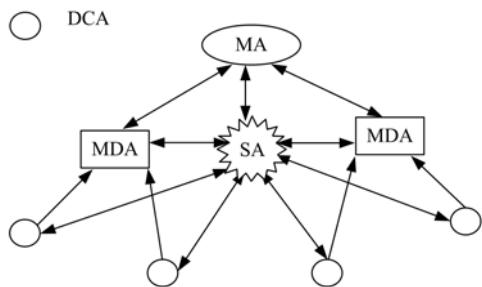


图 1 系统的体系结构图

Fig. 1 Structure of system

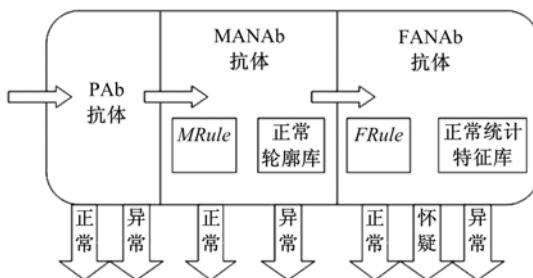


图 2 MDA 的结构

Fig. 2 Structure of MDA

作为资源请求方和资源的中介,SA 的目标是有效利用 MDA 提供的检测服务,完成 DCA 的攻击检测请求,实现资源的合理调度。SA 维护着一个待调度 DCA 注册表和一个可用 MDA 注册表。收到调度指令后,SA 按照一定的调度策略将待调度的 DCA 的 TZData 发送到合适的 MDA 上进行数据处理。MA 负责为用户提供准确的报警信息的监控入侵界面,显示从 MDA 传过来的警报,并人工控制其他 Agent 的启动或停止。

2.2 SA 的调度策略

SA 是多 Agent 入侵检测系统的重要组成部分,整个系统的负载平衡能力通过 SA 来调节。SA 完成的主要任务是收集各 DCA 经过预处理之后的 TZData,根据各 MDA 当前的负载情况和选择策略,将待处理的 TZData 分配给合适的 MDA。

结合系统的实际情况,作者提出了一种改进的资源可用度 U 的调度策略。在系统中,一个待处理的 TZData 是否分配给某个 MDA,由 MDA 上的性能综合指标决定,包括检测准确性 A 和资

源效率 E。因此, $U_i = A_i \times E_i$,其中 U_i 是第 i 个 MDA 的资源可用度, A_i 是第 i 个 MDA 的检测准确性, E_i 是第 i 个 MDA 的工作效率; $A_i = AlarmRate(x) \times w_1 + MisreportRate(x) \times w_2$,其中 $AlarmRate(x)$ 为第 i 个 MDA 在 x 时刻的报警率, $MisreportRate(x)$ 为第 i 个 MDA 在 x 时刻的误报率,这里 w_1, w_2 均为权重系数; $E_i = \frac{Num_{worked}(y)}{Num_{worked}(y) + Num_{deployed}(y)}$,其中 $Num_{worked}(y)$ 为第 i 个 MDA 在 y 时刻已经处理 TZData 的个数, $Num_{deployed}(y)$ 为第 i 个 MDA 在 y 时刻已经排序准备处理 TZData 的个数。SA 按照上面的资源可用度计算方法为各 MDA 计算其资源可用度,决定待处理 TZData 的分配方式。

3 联合免疫抗体(UAb)

3.1 UAb 抗体

定义 1 若抗体彼此孤立存在,并在识别自身以及非自身的过程中独立作用、互不干扰,具有一定的独立性和单一性,则称其为抗体的单体性。

为了跨越抗体单体性的局限,作者提出了一种新型的免疫抗体——联合免疫抗体(UAb)。UAb 抗体主要是检测一些相对 FANAb 抗体检测结果为“怀疑”的 TZData,它能够针对上述 TZData,瞬间集合相关 MDA 所具有的“分析经验”,并依据联合免疫检测函数 Y 最终判定是否发生了入侵攻击,Y 有两种状态,即正常和异常。UAb 抗体是由 UAb 异常检测规则集 URules 和 UAb 关系库 Store_{relation} 构成,URules 主要是收集用于联合免疫检测的 MRule 和 FRule,Store_{relation} 主要是存储用于联合免疫检测的重要计算数据和相关 MDA 的属性信息。MDA 中 UAb 的结构如图 3 所示。

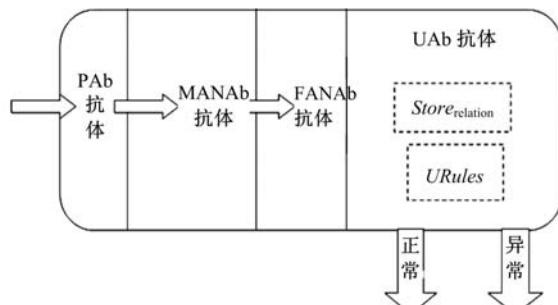


图 3 MDA 中 UAb 的结构图

Fig. 3 Structure of UAb in MDA

3.2 UAb 抗体的生成

对于每个 MDA, 它都需要维护一个联合免疫任务队列 *TaskQueue*, 并且 *TaskQueue* 存储着若干个经 FANAb 抗体检测结果为“怀疑”的 *TZData*。基于合同网协议的分类, 将所有 MDA 区分为管理 MDA、投标 MDA 和中标 MDA 三类。因此 UAb 抗体的具体生成过程如下:

StepA1 将检测结果为“怀疑”的 *TZData* 存储于 *TaskQueue* 中。

StepA2 当 *TZData* 到达队首时, MDA 取出 *TZData*, 并置 MDA 为管理 MDA。

StepA3 管理 MDA 向在 SA 上注册了的系统中的其他活跃着的、能提供联合免疫的 MDA 发送 *TZData* 进行联合免疫招标, 并设定回复时间期限 $T_{time-out}$ 。

StepA4 收到 *TZData* 的投标 MDA, 按照自己的 MANAb 或 FANAb 进行攻击检测, 并将 MANAb 的检测结果或 FANAb 的免疫怀疑度 $D(i)$ 向当前管理 MDA 进行投标。

StepA5: 若在时间 $T_{time-out}$ 内管理 MDA 没有收到任何免疫投标书, 管理 MDA 停止操作, goto StepA7; 否则管理 MDA 根据联合免疫决策函数 F , 选择指定的投标 MDA 作为中标 MDA, 向其发送中标通知, 同时通知其他投标 MDA 投标失败。

StepA6: 一轮 UAb 抗体生成结束。

StepA7: 若管理 MDA 决定进行新一轮 UAb 抗体生成, goto StepA3。

StepA8: UAb 抗体生成结束。

定义 2 管理 MDA 相信投标 MDA 的 FANAb 抗体入侵检测结果的程度称为信任度, 记为 $Tr(i)$, $Tr(i) \in [0, 1]$, $i \in [1, n]$, $n \leq N$, n 为 MDA 的数量。

在 StepA4 中, 投标 MDA 的 MANAb 检测结果向管理 MDA 发送“MDA(i) | MANAb | normability/abnormity | MRule(i)”格式的标书, 即“MANAb 型免疫标书”; FANAb 向管理 MDA 发送格式为“MDA(i) | FANAb | D(i) | Tr(i) | FRule(i)”的标书, 即“FANAb 型免疫标书”。MRule(i) 表示在 MDA(i) 中触发 MANAb 抗体做出 normability/abnormity(正常/异常)结果的异常检测规则; FRule(i) 表示在 MDA(i) 中参与 FANAb 抗体计算免疫怀疑度 $D(i)$ 的模糊异常检测规则。FANAb 抗体在计

算免疫怀疑度 $D(i)$ 时, 模糊蕴含算子采用最小运算: $A \rightarrow B = \min[\mu_A(x), \mu_B(x)]$; 模糊合成算子采用模糊并运算: $\mu_{A \cup B}(x) = \max[\mu_A(x), \mu_B(x)]$; 采用重心法去模糊:

$$D = \frac{\sum_{j=1}^p y_i \cdot \mu(y_i)}{\sum_{j=1}^p \mu(y_i)}$$

总怀疑度为

$$D(i) = \begin{cases} 0, & \forall D < \alpha \\ K, & \forall D > \beta \\ w_1 \times D_{session} + w_2 \times D_{connect} + w_3 \times \\ D_{host} + w_4 \times D_{port} + w_5 \times D_{traffic}, & \text{else} \end{cases}$$

这里初始权重 $w_1 = w_2 = w_3 = w_4 = w_5 = 10$, $K = 50$, $\alpha = 0.35$, $\beta = 076$ 。

对于 StepA5, 管理 MDA 将依据联合免疫决策函数 F 选择特定的投标 MDA 作为中标 Agent, 函数 F 的具体算法如下:

StepB1 统计 MANAb 型标书的数量 a 与 FANAb 型标书的数量 b 。

StepB2 若 $a > 0$ 且 $b = 0$, 则 F 向所有发送 MANAb 型标书的 MDA 发送中标通知, 通知其参与 UAb 抗体的生成。

StepB3 若 $a > 0$ 且 $b > 0$, 则 F 向所有发送 MANAb 型标书的 MDA 发送中标通知, 通知其参与 UAb 抗体的生成; 并通知所有发送 FANAb 型标书的 MDA 投标失败。

StepB4 若 $a = 0$ 且 $b > 0$, 则 F 向所有发送 FANAb 型标书的 MDA 发送中标通知, 通知其参与 UAb 抗体的生成。

StepB5 联合免疫决策结束。

管理 MDA 在收到投标 MDA 的标书后, 它会首先通过联合免疫决策函数 F 选择特定的投标 MDA 作为中标 MDA, 并在其标书上增加一个数据项 FLAG 以作标识。如果中标为 MANAb 型标书, 则以 FLAG1 标识; 如果中标为 FANAb 型标书, 则以 FLAG2 标识; 从而形成“MDA(i) | MANAb | normability/abnormity | MRule(i) | FLAG1”或“MDA(i) | FANAb | D(i) | Tr(i) | FRule(i) | FLAG2”的标书; 然后它将创建一个空间用于存储 UAb 异常检测规则集 URules 和 UAb 关系库 Store_{relation}; 然后将收到中标标书中的 MRule(i) 和 FRule(i) 存储到 URules 中; 最后它将标书中其他数据项映射成

“MDA(*i*) \rightarrow MANAb \rightarrow normability/abnormity”或“MDA(*i*) \rightarrow FANAb \rightarrow D(*i*) \rightarrow Tr(*i*)”的对应关系,并暂存于 Store_{relation} 中。至此 UAb 抗体在管理 MDA 中完成了此次的生成。

3.3 UAb 抗体的检测和更新

由于生成的 UAb 抗体在一定时间内需要处理多个 MDA 的标书信息,瞬间占据的内存资源相当大,因此它的存在也只能是暂时的,它要在较短的时间内释放相应的内存资源,以提高整个系统的检测效率。于是每个 UAb 抗体都是随一种新型入侵攻击的到来而产生,随这种入侵攻击的第一次检测完毕而消亡的。对于每次 UAb 抗体检测的结果,它都将作为一种经验知识,转存固化到相关 MDA 的 PAb 抗体和 MANAb 抗体中去,即以后再出现相同的入侵攻击,它将由本地的 PAb 和 MANAb 抗体检测出来。具体检测更新过程如下:

StepC1 如果 FLAG = FLAG1, 则检测结果为异常,goto StepC3。

StepC2 如果 FLAG = FLAG2, 且联合免疫检测函数 $Y = D(1) \cdot Tr(1) + \dots + D(i) \cdot Tr(i) + \dots + D(n) \cdot Tr(n) \leq K$ (K 为异常阈值; n 为 FANAb 抗体的个数), 则输出结果为正常, 否则输出结果为异常。

StepC3 UAb 抗体将把本次得到的 URules 增量存储到管理 MDA 的 MRule 和 FRule, 并对自身轮廓中的特征进行更新,从而增加对自身改变的耐受能力。

StepC4 UAb 抗体自动将抗体特征整合形成规则,并将此规则作为记忆规则存入所有中标 MDA 的 PAb 中,当相似攻击再次发生时,直接通过 PAb 中的记忆规则进行攻击检测。

StepC5 UAb 抗体检测结束。

在 StepC2 中,对于各 MDA 信任度 Tr(*i*) 的计算,可认为 MDA 的信任主要来自于长时间 SA 对 MDA 执行作业的历史的考察,因此, $Tr(i) = Size_i/T$, 其中 $Size_i$ 是在固定时间内处理完 TZData 的大小(byte); T 是一个固定时间。

4 免疫检测算法

提出了一种改进的免疫检测算法,具体如下:

StepD1 利用 PAb 抗体检测当前流行的已知攻击,若输出异常,goto StepD5。

StepD2 利用 MANAb 抗体检测一些基本的

未知攻击,若输出异常,goto StepD5。

StepD3 利用 FANAb 抗体检测一些复杂的未知攻击,若输出正常,goto StepD6;若输出异常,goto StepD5。

StepD4 建立 UAb 抗体,利用 UAb 抗体检测 FANAb 抗体检测结果为“怀疑”的潜在攻击,并更新相关 MDA 的 PAb 抗体和 MANAb 抗体,若输出正常,goto StepD6。

StepD5 记录数据包信息,向 MA 报警。

StepD6 一轮检测结束。

StepD7 消亡 UAb 抗体。

该算法一方面去掉了阴性选择算法中检测器耐受反应这一步,避免了由于大量的网络数据包使得生成的免疫抗体需要过长时间的缺点;另一方面,由于系统正常超载和异常超载的界线本身就是模糊的,所以经过 FANAb 抗体检测的结果就包含正常、怀疑、异常三种状态。而现实中 FANAb 抗体检测的结果往往大多数是“怀疑”,对于这些数据包,其中不乏存在大量潜在的入侵与攻击,而仅仅就是由于本地 MDA 的“分析经验”不够充分,造成了对它们的误判断。因此系统增加了 UAb 抗体检测方法,这样就促进了 MDA 间经验的彼此借鉴,提高了 MDA 的智能性和对未知分析情况的预警能力。

5 实验结果与分析

用仿真试验数据进行了 2 个实验,以测试 ICNPIDS 的攻击检测能力、健壮性和灵活性。

5.1 实验一

实验一的数据使用的是本文在试验中收集的 1500 条正常连接和 1000 条攻击连接,其中攻击连接包括拒绝服务攻击和探测攻击,并将其第一周数据用作训练数据,第二周数据用作测试数据。实验结果及其比较如表 1 所示。从表 1 中可看出对于新型攻击,ICNPIDS 由于使用联合免疫抗体,具有更高的检测率,较低的误报率。

表 1 实验结果及其比较

Table 1 Experiment results and comparison

	系统	DARPA	AINIDS	ICNPIDS
拒绝服务攻击	检测率/%	23.6	57.6	65.6
	漏警率/%	18.9	12.9	12.1
	虚警率/%	17.2	16.7	13.3
探测攻击	检测率/%	54.1	85.3	89.2
	漏警率/%	20.1	11.4	8.9
	虚警率/%	17.7	13.7	7.4

5.2 实验二

实验二的数据来自某机关机房局域网的网络通信数据。该机房包括 60 台计算机,绝大部分机器的操作系统采用 WINDOWS XP。测试使用了单机入侵检测系统 SIDS、传统分布式入侵检测系统 TDIDS、AINIDS 以及 ICNPIDS 四个入侵检测系统,入侵检测系统的探头个数均为 2。上述四个人侵检测系统的检测结果如图 4 所示。

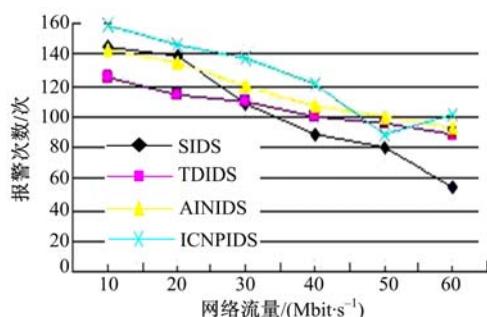


图 4 4 种入侵检测系统的实验结果和比较

Fig. 4 Experiment and comparison for different IDS

从图 4 可知,在网络流量小于 20 Mbit/s 时,上述入侵检测系统的检测性能都很好,并且比较稳定,此时系统抗体的数量与种类的多少就决定了报警数量的多少。当网络流量增至 30 Mbit/s 时,SIDS 明显已经适应不了网速流量的变化,集中式分析处理弊端显现无疑,因此它的检测速度大幅下降。当网络流量继续激增至 50 Mbit/s 时,一方面由于各入侵检测系统的检测分析速度明显延迟于网络流速,导致所有系统的报警数量都有所下调;另一方面 ICNPIDS 在攻击检测的同时,MDA 之间还要进行联合免疫检测,延迟速度更大于其他系统,因此 ICNPIDS 在此时的报警数量跌至谷底。当网络流量持续停留在 50 Mbit/s 以上时,虽然各入侵检测系统的检测分析速度继续下降,报警数量继续走低,但 ICNPIDS 在联合免疫检测以及规则更新后,由于 MDA 间的检测经验得以共享借鉴,自身轮廓以及记忆规则明显增多,因此它的检测性能大幅提升,再加之切实可行的调度策略,它的报警数量又重新恢复至平均水平。总体说来,ICNPIDS 在大部分情况下较其他系统都具有较好的检测性和自适应性。

实验证明:①在记忆自动免疫抗体和模糊自动免疫抗体的基础上,由于改进的免疫检测算法引入了联合免疫抗体,入侵检测系统对新型攻击的检测能力得到了大幅提升;②系统的多 Agent 结构,可以灵活地根据网络的实际运行情况自动调整,充分利用系统的工作能力,使之随时适应变化的网络状态。

6 结束语

提出了一种基于免疫机理与合同网协议的多 Agent 入侵检测系统 ICNPIDS。同时本文在 PAb、MANAb 及 FANAb 的基础上,利用合同网的协同工作原理,提出了联合免疫抗体 UAb 的概念,并建立了 Agent 间的合作机制,共享了分析经验。通过基于滥用检测和异常检测的改进免疫检测算法,以及自适应的调度策略,提高了 ICNPIDS 检测性能,增强了对于外界负载变换的适应能力。实验结果验证了 ICNPIDS 是一种具有较高检测性能、可自主适应环境变化的入侵检测系统。

参考文献:

- [1] 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(11):1934-1939.
Wang Jin, Li De-quan, Feng Deng-guo. An autonomous agent-based adaptive distributed intrusion detection system[J]. Journal of Computer Research and Development, 2005, 42(11):1934-1939.
- [2] 朱吉禹,郑家齐. 病原学与免疫学[M]. 重庆: 重庆大学出版社,1994.
- [3] Forrest S, Hofmeyr S, Somayaji A. Computer immunology[J]. Communications of the ACM, 1997, 40(10): 88-96.
- [4] Hofmeyr A S. An Interpretative Introduction to the Immune System: Design Principles for the Immune System and other Distributed Autonomous Systems [M]. London: Oxford University Press, 2000.
- [5] Smith G R. The contract net protocol high level communication and control in a distributed problem solver[J]. IEEE Transaction on Computers, 1980, 29(12): 1104-1113.