高技术通讯 2010 年 第 20 卷 第 10 期:1027 ~ 1032

doi:10.3772/j.issn.1002-0470.2010.10.007

基于免疫抗体浓度的网络入侵风险定量评估①

柴争义②* ** 郑丽萍* 朱思峰**

(* 河南工业大学信息科学与工程学院 郑州 450001)

(** 西安电子科技大学计算机学院 西安 710071)

摘 要 借鉴免疫危险理论,利用抗体浓度,提出了一种网络入侵风险检测和定量评估方法。首先,为了更准确地检测出入侵,建立了抗原、各类抗体(未成熟抗体、成熟抗体、记忆抗体)的动态演化方程;其次,为了正确评估入侵风险,建立了每类攻击的抗体浓度的定量表示方法;依据每类攻击的危害性以及每台主机的重要性不同,给出了某个主机以及整个网络面临攻击时的风险值计算方程;最后进行了仿真和对比实验。实验结果表明,该方法可以高效检测出网络入侵,并能正确评估每一台主机和网络整体面临任何一类攻击及全部攻击时的风险。

关键词 人工免疫,危险理论,抗体浓度,网络入侵,风险评估

0 引 言

随着网络的广泛应用,网络安全问题也日益突出。目前所有的安全防御手段都无法保证网络的绝对安全。因此,对网络当前的安全风险进行检测和评估,进而采取相应的安全防范措施,以提升网络的生存能力,就显得非常重要。目前,已有的网络风险感知模型中,CRAMM,COBRA,OCTAVE 等属于静态方法[1],它们可以对网络长期所处的风险状态进行粗略评估,但无法实时检测网络正在遭受的攻击,缺少自适应性。文献[2]提出了一种介于静态评估和实时评估的网络安全风险检测方法,但无法正确识别网络面临攻击但还未被攻破时的风险;文献[3-6]分别使用概率统计、层次分析法、模糊集理论、隐马尔可夫模型(hidden Markov model,HMM)等方法对网络的风险进行实时评估,这些方法具有动态和直观的优点,但缺乏对未知攻击的辨别能力;文献[7]提出了基于人工免疫理论的实时风险检测方法,但由于是建立在传统的自体与非自体区别上,导致风险检测虚警率较高;文献[8]给出了基于危险信号的网络风险评估模型,但较为粗糙,缺少危险信号的定量计算。基于此,本文提出了一种基于危险理论和抗体浓度的实时、定量检测和评估网络安全风险的模型。理论分析和实验结果表明,该模型可以高效检测出网络入侵,并能正确评估主机及网络面临的各种风险,从而能为采取适当的防御手段提供有力依据。同时,该模型对各种异常检测,如病毒检测、垃圾邮件识别等,均有一定的参考价值。

1 免疫危险理论基础和网络安全风险检测评估模型设计思想

生物免疫系统通过分布在全身的抗体(免疫细胞)识别和清除侵入生物体的抗原(自体和非自体)。当抗体识别超过一定数量的抗原后,将会克隆增扩,该抗体浓度急剧增加;当抗原消除后抗体将会受到抑制,抗体浓度降低,使免疫系统趋于稳定[9]。正常的情况下,生物体的各种抗体的浓度应该基本上是不变的,因此可以通过测量各种类型抗体的浓度来判断生物体是否得病及病的严重程度。将此机制引入到网络安全领域,通过适当的映射关系和问题描述,就可以通过抗体浓度来评价网络的安全风险。

危险理论[10]认为并不是所有外来抗原都会引起免疫响应,免疫系统只对危险的非自体反应。同样,在网络安全中,并非所有的入侵都会对网络造成危险。比如有些针对主机某些固定端口的攻击,从自体、非自体的角度看,属于网络攻击行为(非自

① 国家自然科学基金(70701013),陕西省"13115"科技创新工程重大科技专项(2008ZDKG-37)和河南省自然科学基金(2009A52008)资助项目。

② 男,1976 年生,博士,讲师;研究方向:人工免疫,网络与信息安全;联系人,E-mail: super_chai@tom.com; chaizhengyi@haut.edu.cn

(收稿日期:2009-07-10)

体),但实际上,如果主机并没有开放此端口的话,对主机就是安全的,可以不必进行响应。因此,基于危险信号进行响应,更能真实体现网络面临的安全风险。

依据危险理论的解释,抗原死亡有两种方式[11]:凋亡(apoptosis)与坏死(necrosis)。在本文的入侵检测中,网络行为正常结束隐喻为抗原凋亡,网络行为的非正常结束隐喻为抗原坏死。相应地,抗原凋亡产生抑制信号抑制抗体产生,而抗原坏死产生增强信号激励抗体产生。因此,通过对抗体克隆和危险信号的分析可知,抗体浓度的大小可以表示网络的风险强弱和危险程度。

本文提出的网络安全风险检测和评估模型的任务可描述为:如何保证网络免受入侵及准确检测出入侵行为;当受到入侵后如何评价主机及网络所面临的安全风险。具体工作流程是:对网络入侵行为进行检测并对攻击进行分类,然后按照危险理论,根据抗体浓度和攻击强度的对应关系,计算出主机面临每种攻击的危险的程度以及主机面临所有攻击的危险的程度,进而给出网络面临每一种攻击及所有攻击的风险的等级。

本模型由入侵检测和风险评估两部分组成。

2 网络入侵检测的具体实现

入侵检测模型中检测网络行为是正常行为还是网络攻击的过程隐喻为生物免疫中抗体识别并判断抗原是自体/非自体的过程。为了更客观和准确地评估网络风险,检测子系统应具有高的检测率和低的虚警率。在真实环境中,正常网络行为(自体)往往是动态变化的,因此相应的自体耐受、抗体检测过程都是动态的。下面分别给出抗原(自体,非自体)和抗体(未成熟抗体、成熟抗体、记忆抗体)的形式化描述和动力学方程。

2.1 抗原形式化描述及变化方程

定义抗原集合 $Ag \subset D, D = \{0,1\}^l (l > 0)$,其中 Ag 表示对网络上传输的 IP 包进行特征提取得到的长度为 l 的二进制字符串。定义自体集合 $Self \subset Ag$,非自体集合 $Nonself \subset Ag$,则有 $Self \cup Nonself = Ag$, $Self \cap Nonself = \phi$。$Self$ 集为正常网络行为,$Nonself$ 集为网络攻击行为。

定义自体的动力学方程为

$$Self(t) = Self(t-1) - Self_{dead}(t) - Self_{variation}(t) + Self_{new}(t) \quad (1)$$

其中,$Self_{variation}$ 表示发生了变异的自体(由自体变为非自体);$Self_{new}$ 表示新增加的自体元素;$Self_{dead}$ 表示当自体集合大小超过阈值 L 时淘汰掉的一部分自体元素。本文中,设置 L 主要是确保自体耐受高效进行,淘汰可按 LRU(最久未使用)的原则。

2.2 抗体形式化描述及变化

定义抗体集合 B 为一个四元组:

$$B = \{< d, \rho, age, count > \mid d \in D \wedge \rho \in R \wedge age \in N \wedge count \in N\} \quad (2)$$

其中 d 为抗体(长度为 l 的二进制字符串),ρ 为抗体浓度,age 为抗体年龄,$count$ 为抗体的累计亲和力数目,R 为实数集合,N 为自然数集合。

抗体分为未成熟抗体、成熟抗体、记忆抗体,分别用 I_b、T_b、M_b 表示。免疫检测抗体集合 $B = M_b \cup T_b$。

定义 $I_b = \{< d, age > \mid d \in D,\ age \in N\}$ (3)

定义 T_b 由在一定时间内(age)经过自体耐受的未成熟免疫抗体 I_b 组成。定义自体耐受过程如下:

$$f_{tolerance}(I_b) = I_b - \{x \mid x \in I_b \wedge \exists y \in Self \wedge f_{match}(x,y) = 1\} \quad (4)$$

其中,f_{match} 函数的定义如公式

$$f_{match}(x,y) = \begin{cases} 1, & \text{iff} \exists i,j (x.d_i = y_i, x.d_{i+1} = y_{i+1}, \cdots, x.d_j = y_j, \\ & j - i \geqslant r, 0 < i < j \leqslant l, i,j,r \in N) \\ 0, & \text{otherwise} \end{cases} \quad (5)$$

所示,1 表示匹配,0 表示不匹配。如果有连续的 r 位相同,则认为匹配,否则,认为不匹配。本文采用了一种可变阈值模糊 r 匹配算法[11],通过调整匹配阈值,大幅度降低了黑洞数量,减小了检测器的时间耗费,提高了检测率和性能。

定义记忆抗体 M_b 由成熟抗体 T_b 在生命周期 λ 内累积亲和力超过阈值 β 进化而来,如式

$$M_b = \{x \mid x \in B \wedge x.count \geqslant \theta \wedge x.age \leqslant \lambda\} \quad (6)$$

所示。

2.3 未成熟抗体的动力学方程

在已有相关算法中[7-9],未成熟抗体的生成采用随机产生。这样虽然保证了抗体的多样性,但存在较多冗余,效率也不高。本文中,未成熟抗体的生成采用一部分完全随机产生,确保抗体的多样性,另一部分由基因库组合、串联生成的方法生成,提高了其

成为成熟检测器的可能性和生成效率,并具有检测入侵变种的能力。

未成熟抗体的生成方程为

$$I_{new}(t) = Random(Ag) + Random(Gene(t)) \tag{7}$$

定义基因库的动力学方程为

$$Gene(t) = Gene(t-1) - Gene_{dead}(t) + Gene_{new}(t) \tag{8}$$

$Gene_{dead}(t)$ 为 t 时刻发生错误肯定(虚警)的记忆细胞基因。定义 $Gene_{new}(t)$ 为 t 时刻抗体初次应答时抗体克隆体的基因。

在实际应用中,对于各种新出现的入侵手段,提取相关疫苗[12],可更好地控制检测器的进化方向,提高系统的整体检测和防御性能。

未成熟抗体经过自体耐受进化为成熟抗体。由于自体 Self 是动态的,因此耐受过程也是动态的。定义自体耐受动力学方程为

$$I_b(t) = I_{tolerance}(t) - I_{maturation}(t) + I_{new}(t) \tag{9}$$

其中,$I_{tolerance}(t)$ 为上一阶段的自体 $self(t-1)$ 经历一次耐受后剩下的免疫细胞;$I_{maturation}(t)$ 为 t 时刻已经成熟的免疫抗体;$I_{new}(t)$ 为 t 时刻新生成的未成熟的免疫抗体。

2.4 成熟抗体动力学方程

成熟抗体集合 T_b 的动力学方程为

$$T_b(t) = T_b(t-1) + T_{new}(t) - (T_{active}(t) + T_{dead}(t)) \tag{10}$$

其中

$$T_{new}(t) = I_{maturation}(t) + T_{clone}(t) \tag{11}$$

$$T_{active} = \{x \mid x \in T_b \wedge x.count \geqslant \theta \wedge x.age \leqslant \lambda\} \tag{12}$$

$$T_{dead} = \{x \mid x \in T_b \wedge x.count < \theta \wedge x.age > \lambda\} \tag{13}$$

$T_{new}(t)$ 为 t 时刻新生成的抗体,$I_{maturation}(t)$ 为 t 时刻新进化产生的成熟抗体,$T_{clone}(t)$ 为细胞克隆新产生出的免疫抗体,对抗原进行初次应答;成熟抗体的克隆变异采用随机变异,保证免疫系统的多样性[13]。T_{active} 为激活为记忆抗体的成熟抗体,T_{dead} 表示年龄超过生命周期而匹配抗原数目未达到激活阈值的成熟抗体。

2.5 记忆抗体动力学方程

记忆抗体集合 M_b 动力学方程定义为

$$M_b(t) = M_b(t-1) + M_{new}(t) + M_{other}(t) - M_{dead}(t) \tag{14}$$

其中

$$M_{new}(t) = T_{active}(t) + M_{clone}(t) \tag{15}$$

$$M_{clone}(t) = \{x \mid x \in T_b(t-1), \exists y \in Ag(t-1) f_{match}(x,y) = 1\} \tag{16}$$

即 $M_{new}(t)$ 由成熟抗体进化而来和克隆选择产生;$M_{death}(t)$ 是匹配了自体的记忆细胞;$M_{other}(t)$ 指从其它主机接受的免疫记忆抗体,类似于疫苗接种过程,对抗原进行二次应答。本文中,记忆抗体的克隆变异采用可控变异[14],保证对网络当前流行入侵的快速识别能力。

2.6 入侵检测性能分析

本文的入侵检测子系统有如下优点:

(1)定义了自体的动态变化方程,很好地满足了真实网络环境下正常网络行为和入侵行为往往是动态变化这一情况,有效降低了漏警率和虚警率。

(2)动态耐受过程中,通过设定自体集合大小,保证了耐受工作高效进行。

(3)在未成熟抗体的生成中,采用了随机生成和抗体基因库结合的生成方法,既保证了抗体的多样性,又提高了其成为成熟检测器的可能性和生成效率。

(4)成熟抗体和记忆抗体的死亡确保了免疫细胞的多样性,保证了其对抗原空间的持续搜索能力,淘汰机制进一步降低了系统虚警率和漏警率。

(5)疫苗接种和分发机制提高了网络主动检测类似抗原攻击的能力及检测的准确性和预见性;记忆抗体的克隆变异采用可控变异,保证对网络当前流行入侵的快速识别能力。

(6)抗原抗体的匹配采用可变阈值模糊 r 匹配算法,大幅度降低了黑洞数量,减小了检测器的时间耗费,提高了检测率和性能。

3 网络风险评估的具体实现

3.1 抗体浓度计算

对检测到的攻击行为,按照血亲分类[15]。攻击的种类以血亲类为标志,把抗原攻击集合划分为 $A = \{A_1, A_2, A_3, \cdots, A_n\}$,每个子集 $A_i(1 \leqslant i \leqslant n)$ 刺激产生相应抗体。各子集 A_i 的组成定义如下

$$A_i(t) = A_i\_new(t) + A_i\_necro(t) - A_i\_apopt(t) \tag{17}$$

其中,$A_i\_new(t)$ 是在 t 时刻新加入的抗原;$A_i\_necro(t)$ 是在 t 时刻以坏死方式死亡的抗原,它对

抗体浓度产生增强作用；$A_i\_apopt(t)$ 是在 t 时刻以凋亡方式死亡的抗原，它将对抗体浓度产生抑制作用。

能检测出第 A_i 类攻击(抗原)的抗体 Ab_i 的浓度 $\rho_{\mathrm{Abi}}(t)$ 定义如下

$$\rho_{\mathrm{Abi}}(t) = k_1\sum_{i=1}^{n_1} new(t) + k_2\sum_{i=1}^{n_2} necro(t) - k_3\sum_{i=1}^{n_3} apopt(t) \tag{18}$$

其中，$\sum_{i=1}^{n_1} new(t)$，$\sum_{i=1}^{n_2} necro(t)$，$\sum_{i=1}^{n_3} apopt(t)$ 分别表示 n_1 个 $A_i\_new(t)$、n_2 个 $A_i\_necro(t)$、n_3 个 $A_i\_apopt(t)$ 对抗体浓度的影响值；k_1、k_2、k_3 分别为影响因子。

定义抗体 Ab_i 激活后被克隆的数目为 $N_{\mathrm{clonc}}(Ab_i) = \lceil K(1-\frac{Num}{|B_{(t-1)}|})\rceil$，其中 K 为比例系数，Num 为与抗体 Ab_i 具有相同基因的抗体的数目(血亲分类)；$B_{(t-1)} = T_b(t-1)\cup M_b(t-1)$。

3.2 风险定量计算

设网络中共有 n 台计算机，由于不同类型的攻击其危害性不相同，同时每台主机在网络中的重要性也有所不同。因此，在评估主机 $j(1\leqslant j\leqslant n)$ 具体面临的风险时，必须综合考虑每类攻击的危害性以及每台主机的重要性。

设主机 j 在 t 时刻所面临的危险风险为 $dr_j(t)$(*Degree of risk*)$(0\leqslant dr_j(t)\leqslant 1)$，其值越大，表明主机面临的风险越高。根据前面的分析可知，$dr_j(t)$ 的计算可以通过 $\rho_{\mathrm{Abi}}(t)$ 得到。设 cr_i(*coeffcient of risk*) 表示主机 j 遭受到攻击 A_i 的危险系数。

定义主机 j 在 t 时刻面临第 A_i 类攻击的安全风险 $dr^i_{j(t)}$ 为

$$dr^i_{j(t)} = \left(1-\frac{1}{1+e^{-cr_i\cdot\rho_{\mathrm{Abi}}(t)}}\right) \tag{19}$$

定义主机 j 在 t 时刻面临的整体安全风险为

$$dr_{j(t)} = \left(1-\frac{1}{1+e^{-\sum_{i=1}^{n} cr_i\cdot\rho_{\mathrm{Abi}}(t)}}\right) \tag{20}$$

设 $\phi_j(0\leqslant\phi_j\leqslant 1)$ 为主机 j 在网络中的重要性。设网络 t 时刻面临攻击 A_i 的危险风险记为 $NR_{i(t)}$(*Network Risk*)，定义

$$NR_{i(t)} = \left(1-\frac{1}{1+e^{(-cr_i\cdot\rho_{\mathrm{Abi}}(t)\cdot\sum_{j=1}^{n}\phi_j)}}\right) \tag{21}$$

定义整个网络系统的整体安全风险为

$$NR_{(t)} = \left(1-\frac{1}{1+e^{\sum_{j=1}^{n}\phi_j\cdot(-\sum_{i=1}^{n}(-cr_i\cdot\rho_{\mathrm{Abi}}(t)))}}\right) \tag{22}$$

4 系统仿真实验与分析

实验在网络实验室进行，利用本模型对网络中的20台主机进行监控并评估。被监控网络分别对外提供WWW，FTP，E-mail等服务，操作系统为Windows2003。入侵实验使用的数据是KDDCup99入侵检测数据集kddcup.data-10-per-cent[16]。我们采用了不包括任何攻击的数据作为训练数据，测试数据集中包含有小部分训练集中未出现的样本。用5个不同的测试数据集(包含攻击类型不同，如land、spy、perl等)对系统进行了测试，同样的数据重复进行5次实验。实验结果采用TP值(检测率)和FP值(虚警率)对模型进行评估。由于系统参数对结果影响很大，经过反复的比较实验，在系统表现稳定的情况下，最终选定了一组参数：r 可变阈值范围从13到20，$l=128$，$\theta=40$，$\lambda=7$ 天，$L=2000$，克隆选择系数 $k=1$，抗体浓度的影响因子 k_1、k_2、k_3 分别设为0.8，1.2，0.5。实验结果表明，本系统平均TP值(检测率)可以达到96.58%，FP值(虚警率)平均可以降低到2.13%，具有很好的检测性能。

在检测出攻击后，对主机及网络所面临的风险进行评估。在实验中，对WEB服务器、FTP服务器、E-Mail等3台服务器进行监控并评估，其对应的重要性分别为0.9、0.7、0.5；实验中采用了flood、land、teardrop等多种攻击，其危险性分别设为0.8、0.6、0.4。

为了验证本模型的性能，把本模型与insre模型[7]进行了对比实验。insre模型是基于免疫实现的网络风险评估的典型代表，具有较高的性能。对比实验中，参数的选取完全相同。对风险的检测结果如图1和图2所示。图1分别表示FTP服务器遭受综合攻击时，攻击强度实际变化曲线与风险检测模型检测计算到的风险变化曲线对比图；图2表示整个网络面临综合攻击时的实际攻击强度与风险模型检测的风险变化对比图。

从图1和图2可以看出，两个模型均能较好地反映出网络遭受攻击时的风险强度。随着网络攻击强度的增强，其相应的安全风险也迅速跟着上升；当攻击强度下降时，其相应的安全风险也降低，但下降的斜率相对攻击强度下降的斜率要小。这表明当某

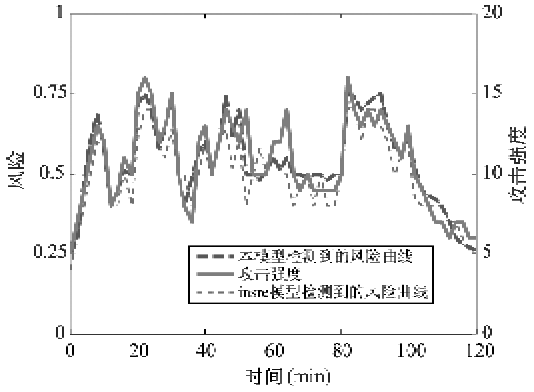

图 1　主机遭受攻击时的风险图

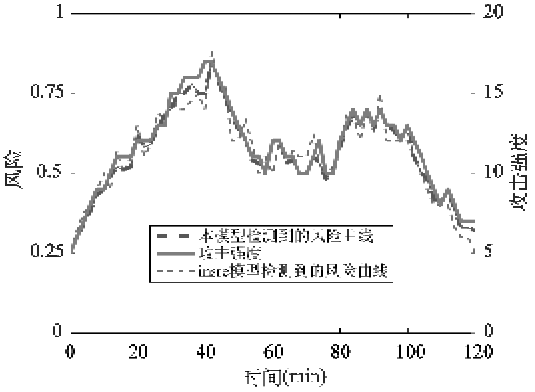

图 2　网络遭受全部攻击时的风险图

一攻击在短时间内再次发生时,网络仍可保持较高的敏感度。这恰好与真实网络环境一致。

同时,从图 1 和图 2 也可以看出,相比较而言,本文模型更能精确检测和判断网络遭受攻击时面临的安全风险。这主要在于,与传统基于免疫的网络安全风险检测方法 insre 相比[7],本模型引入了危险信号,排除了一些对网络无危险的攻击,因此,评估结果更贴近实际,合理可信。

5　结　论

本文借鉴免疫危险理论,利用抗体浓度,设计了一种网络安全风险实时检测系统,为主动积极地调整当前网络安全防御策略提供了直接的技术支持。文中模拟真实网络环境中的自体动态变化,给出了自体、抗体的动态演化机制,风险检测和评估的定量计算;提出了随机生成和基因库相结合的未成熟抗体的生成机制,并引入了可控变异、疫苗接种和分发机制,提高了网络主动检测能力。相比传统模型,该模型可以高效检测出网络攻击,并能实时、定量地计算和评估网络以及网络中主机面临每一类网络攻击的风险及整体综合风险,并能检测出未知攻击。本模型能准确地评判网络面临攻击但还未被攻破时的风险情况,为避免严重的攻击事件发生提供了充分和可靠的依据。

同时,该模型经过适当变换,还可以应用于病毒检测及垃圾邮件识别等相关领域。如何进一步优化抗体浓度表示及风险计算中的各个参数,是本文下一步继续研究的方向。

参考文献

[1] Visintine V. An introduction to information risk assessment. *SANS institute Journal*, 2003, 8(5): 101-118

[2] Chu C K, Chu M. An integrated framework for the assessment of network operations, reliability, and security. *Bell Labs Technical Journal*, 2004, 8(4): 133-152

[3] 陈秀真,郑庆华,管晓宏等. 层次化网络安全威胁态势量化评估方法. 软件学报,2006,17(4):885-89

[4] 张永铮,方滨兴,迟悦. 用于评估网络信息系统的风险传播模型. 软件学报,2007,18(1):137-145

[5] 韦勇,连一峰. 基于日志审计与性能修正算法的网络安全态势评估模型. 计算机学报,2009,32(4):763-772

[6] 李伟明,雷杰,董静等. 一种优化的实时网络安全风险量化方法. 计算机学报, 2009,32(4): 793-804

[7] Li Tao. An immunity based network security risk assessment. *Science China Information Sciences* (*Science in China Series F*), 2005,48(5):557-578

[8] 彭凌西,陈月峰. 基于危险理论的网络风险评估模型. 电子科技大学学报,2007,36(6):1998-2001

[9] Glickman M, Balthrop J, Forrest S. A machine learning evaluation of an artificial immune system. *Evolutionary Computation*, 2008, 13(2): 179-212

[10] Matzinger P. The danger model: a renewed sense of self. *Science*, 2004, 296(5566): 301-30

[11] 张衡,吴礼发,张毓森. 一种 r 可变阴性选择算法及其仿真分析. 计算机学报,2007,28(10):1614-1619

[12] 严宣辉. 应用疫苗接种策略的免疫入侵检测模型. 电子学报,2009,37(4):780-785

[13] Ji Z, Dasgupta D. Revisiting negative selection algorithm. *Evolutionary Computation*, 2007, 15(2): 123-139

[14] Dasgupta D. Advances in artificial immune system. *IEEE Computational Intelligence Magazine*, 2008, 11(4): 4-9

[15] 李涛. 基于免疫的计算机病毒动态检测模型. 中国科学 F 辑:信息科学,2009,39(4):422-430

[16] University of California. KDDLib[EB/OL]. [2009-3-2]. http://kdd.ics.uci.edu/databases/kddcup99.html

Quantitative assessment of network intrusion risk based on immune antibody concentration

Chai Zhengyi[*,**], Zheng Liping[*], Zhu Sifeng[**]
([*] School of Information Science and Engineering, Henan University of Technology, Zhengzhou 450001)
([**] School of Computer Science and Technology, Xidian University, Xi'an 710071)

Abstract

An immune antibody concentration based method was proposed for detection and quantitative assessment of network intrusion risk. First, in order to detect the intrusion accurately, the dynamic evolution equations of Ag and various Abs (immature Ab, mature Ab and memory Ab) were designed. Second, the quantitative equations of Ab concentration were established for each type of attack in order to assess the intrusion risk. Based on different dangers of each attack and the importance of each host, the risk equations for a given host and the whole network were presented. Finally, the simulation and comparison experiments were done to test the method. The experimental results prove that using the method, the intrusion attacks can be dected effectively, and the risk that the host and network will bear when they face each attack and the whole attacks can be also evaluated.

Key words: artificial immune, danger theory, antibody concentration, network intrusion, risk assessment