基于免疫危险理论的网络安全态势评估

陈妍伶 汤光明 孙怡峰
(解放军信息工程大学 郑州 450001)

摘 要 为实时定量评估网络安全态势,提出了一种基于免疫危险理论的网络安全态势评估方法。通过研究免疫运行机制,定义了网络安全问题中的抗原、抗体和免疫细胞,描述了危险信号的判断规则,准确识别出了抗原。在分析免疫应答机制和免疫平衡机制中抗体浓度变化原因的基础上,给出了抗体浓度的计算方法。最后,结合抗体浓度与危险程度的关系,建立了基于抗体浓度的危险感知模型以实时定量评估网络安全态势。仿真实验表明,所提方法计算出的抗体浓度准确地反映了系统面临的危险程度,能够为网络管理提供有效的决策支持。

关键词 危险理论,人工免疫,抗体浓度,网络安全,态势评估
中图法分类号 TP393.08 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.6.036

Assessment of Network Security Situation Based on Immune Danger Theory

CHEN Yan-ling TANG Guang-ming SUN Yi-feng
(PLA Information Engineering University, Zhengzhou 450001, China)

Abstract In order to assess network security situation in real-time and quantification, an assessment method based on immune danger theory was proposed. Through studying the immune operation mechanism, antigen, antibody and immune cell in the problem of network security were defined. On the premise of describing the judgment rules of danger signal, the antigen is recognized accurately. Based on the changes of antibody density in the immune response and immune balance mechanisms, the calculation method of antibody density was given. Finally, by analyzing the relationship between antibody density and danger level, a danger awareness model based on antibody density was built to assess network security situation in real-time and quantification. The simulation results show that antibody density calculated by using the proposed method accurately reflects the danger level that the system faces, which can provide effective decision-making support for network management.

Keywords Danger theory, Artificial immune, Antibody density, Network security, Situation evaluation

互联网在以前所未有的速度不断发展的同时,还必须应对源自内部的漏洞、来自外部的攻击等可能面临的各种威胁以保证网络在相对稳定和安全的状态下正常运行。在错综复杂的网络环境中,各种攻击手段层出不穷,而传统的防护措施(如防火墙、入侵检测、病毒检测、脆弱性扫描、脆弱性评估等)之间缺少关联性,因此无法提供宏观角度的网络安全性评估。为应对被动、单一的网络管理局面,实现积极防御、主动管理的安全目标,网络安全态势感知(Network Security Situation Awareness, NSSA)成为近几年来网络安全领域的研究热点。

网络安全态势感知是在大规模网络环境中,对能够引起网络态势发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势[1]。其中,态势要素作为网络安全态势的基本描述,对其的获取和理解是进行态势感知的前提。不同的应用需求对网络安全态势的定义和要求存在较大差异,Wang和Jajodia等[2]通过采集网络的脆弱性信息,Ning等[3]通过采集网络的警报信息,分别获得了网络的脆弱性和威胁性态势。不同应用背景下的安全态势针对性更明确,也更易发现问题、方便管理。在态势评估方法上,前人进行了大量探索和尝试。郑黎明等[4]建立了层次化的指标体系,对各个属性采用不同的量化方法,对网络安全态势进行评估。网络数据一定程度上是不完整、不精确,甚至是矛盾的,层次量化的评估方法虽直观明了,但方法模型的建立缺少确定的数据源。张勇等[5]提出一种基于Markov博弈分析的网络安全态势感知方法,动态评估系统的安全态势并给出了安全加固方案。该方法分析了威胁、管理员和普通用户行为的关系,考虑全面、综合性强,但需要较大的存储量和运算量,容易造成维数爆炸,实时性难以保证。卓莹等[6]从网络态势的特点和需求出发,建立了基于粗集分析的网络安全态势评估模型,基本满足了态势评估的需要。然而,在海量网络数据中找到有用的特征以构造决策表较为复杂且难以得到定量的评估结果。Feng等[7]利用反正切函数和修正函数来设计D-S证据理论中的经验函数,建立了态势评估模型。该方法不需要精确的概率分布,但计算复杂度高且准确性易受到冲突证据的影响。为实时定量评估网络安全态势,本文提出了一种基于免疫危险理

到稿日期:2014-07-01 返修日期:2014-09-16 本文受河南省科技攻关计划(122102210047)资助。
陈妍伶(1990—),女,硕士生,主要研究方向为网络安全、人工免疫,E-mail:chylscholar@163.com;汤光明(1963—),女,教授,博士生导师,主要研究方向为信息安全、体系对抗;孙怡峰(1976—),男,博士,副教授,主要研究方向为信息安全、机器视觉。

论的网络安全态势评估方法，计算出的抗体浓度准确地反映了网络当前面临的危险程度，从而为积极防御和主动管理提供了有效的决策支持。

1 基于免疫危险理论的网络安全态势评估

免疫危险理论(Immune Danger Theory，IDT)认为，危险信号是免疫应答的决定性因素，可用于解决传统人工免疫中自体与非自体动态变化且难以区分这一难题。免疫危险理论是生物免疫学领域的最新成果之一[8]，在模式识别、故障诊断、异常检测等领域有良好的应用前景[9]。它仿生并继承了生物免疫相关运行机制，具有自学习、自分类、分布式、自适应和自组织的特性，在抗体种群大小有限的条件下，利用这些特性，免疫系统通过分析所处环境和所受伤害，基于抗体间的通讯协作和不断进化更新，识别出相应抗原并保存免疫记忆，以达到动态平衡稳定的状态。在免疫危险理论中，免疫系统根据感受到的危险信号决定刺激还是抑制抗体产生，使人体免受伤害。抗体浓度随着危险信号的强弱不断变化[10]。同时，为维持抗体种群的多样性，抗体浓度的高低与选择概率的大小呈负相关性，从而保证系统可应对更多威胁并搜索到最优抗体。

对网络安全态势进行评估，要根据当前网络环境下通信过程中呈现的事务属性，在已有的安全防护和检测条件下，识别出未知的危险种类并评估其危险程度，全面把握网络安全状态。可见，其评估过程与免疫危险理论的思想一致，可以将免疫危险理论用于评估网络安全态势。

基于免疫危险理论的网络安全态势评估模型如图 1 所示。

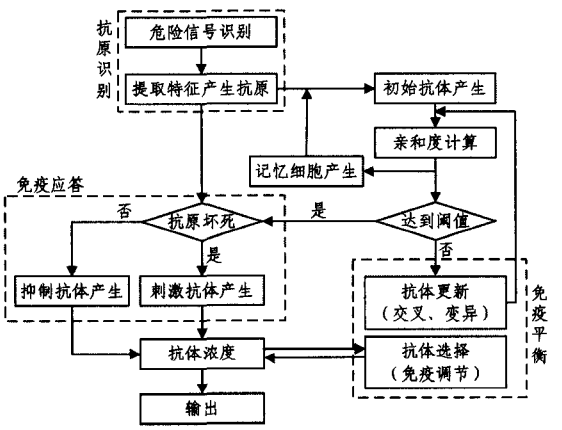

图 1 模型框架

表 1 给出了网络安全态势评估与免疫危险理论的对应关系。

表 1 网络安全态势评估与免疫危险理论对应关系

网络安全态势评估	网络事务	网络事务属性	亲和度匹配器	匹配器产生、减少、更新	匹配器数量	危险程度
免疫危险理论	危险信号	抗原/抗体成分	免疫细胞	免疫应答机制 免疫平衡机制	抗体种群大小	抗体浓度

由模型可知，基于免疫危险理论的网络安全态势评估主要分为 3 个阶段：抗原识别、免疫应答和免疫平衡。

1.1 概念描述

抗原、抗体是免疫危险理论相关机制运行的基础，下面给出在网络安全态势评估中相关概念的定义。

设网络通信过程的状态空间为 $S\in R^L$，$|S|=L$，$S=\{\langle S\_initial, S\_finish\rangle\}$，其中，$S\_initial$ 为通信过程开始所具有的网络事务属性，如源/目的地址 src_IP/dst_IP、协议类型 $protocol\_type$、服务类型 $service$、连接状态 $flag$ 等。S_finish 为通信过程结束所具有的网络事务属性，如登陆是否成功 $logged\_in$、通过的字节数 $bytes$、连接长度 $duration$ 等[11]。$S\_initial$ 由两部分组成，即正确操作 $S\_initial\_right(|S\_initial\_right|=m)$ 与错误操作 $S\_initial\_false(|S\_initial\_false|=n)$，且

$$\begin{aligned} &S\_initial\_right\cup S\_initial\_false=S\_initial\\ &S\_initial\_right\cap S\_initial\_false=\varnothing \end{aligned} \tag{1}$$

同理，有

$$\begin{aligned} &S\_finish\_right\cup S\_finish\_false=S\_finish\\ &S\_finish\_right\cap S\_finish\_false=\varnothing \end{aligned} \tag{2}$$

定义 1 抗原 Ag 是对危险信号 DS 进行特征提呈(antigen presenting)后的抗原决定基(antigenic determinant)组合。决定基组合的特征空间为 $\psi\subset S$。

定义 2 抗体 Ab 是特征空间 ψ 中抗原 Ag 的解。

判断抗体 Ab_i 是否是抗原 Ag_j 的解可采用判断函数 $f_{ij}=\begin{cases}0, & affinity(ij)<\xi\\ 1, & affinity(ij)\geqslant\xi\end{cases}$，$affinity(\cdot)$为亲和度匹配函数。

$$affinity(\cdot)=1-D_{ij} \tag{3}$$

式中

$$D_{ij}=\frac{\|Ab_i-Ag_j\|}{l} \tag{4}$$

$$\|Ab_i-Ag_j\|=\sqrt{\sum_{k=1}^{l}(Ab_{ik}-Ag_{jk})^2}$$

其中，$i=1,2,\cdots,M;j=1,2,\cdots,N;k=1,2,\cdots,l$

Ab_{ik} 和 Ag_{jk} 分别表示 Ab_i 和 Ag_j 的第 k 个分量(特征)。式(4)中 $\|Ab_i-Ag_j\|$ 为形态空间 ψ 中抗体 Ab_i 和抗原 Ag_j 的欧几里德距离。

定义 3 免疫细胞集合 B：

$$B=\{\langle Ab,CT\rangle|Ab\in\psi,CT\in R\} \tag{5}$$

其中，CT 为抗体种群浓度。抗体种群浓度 CT_i 定义为免疫细胞集合中与第 i 个个体亲和度相近的抗体所占的比率，即

$$CT_i=\frac{\sum_{j}(|affinity(j)-affinity(i)|\leqslant\varepsilon)}{N} \tag{6}$$

其中，$\varepsilon\in(0,1)$，N 为抗体种群总数。

1.2 网络安全态势评估

1.2.1 抗原识别

网络状态是网络中所有设备通信、交互的综合表现。网络事务属性记录了通信全过程相应设备的特征。网络事务属性特征空间为 S，$\forall x=\{\langle a,b\rangle\}\in S$，

$$x=\begin{cases}DS^{ap}, & \text{if } x.a\in S\_initial\_right\\ & \quad\wedge x.b\in S\_finish\_right\\ DS^{pe}, & \text{if } x.a\in S\_initial\_false\\ & \quad\wedge x.b\in S\_finish\_false\end{cases} \tag{7}$$

网络行为正常结束对应于细胞凋亡，反之则对应于细胞坏死，DS^{ap} 为细胞凋亡产生的危险信号，DS^{pe} 为细胞坏死产生的危险信号。对 DS 进行特征提取，得到抗原 Ag。即

$$Ag=f_{APC}(DS) \tag{8}$$

f_{APC} 为特征提取函数，$Ag\in\psi$。提取的特征应尽可能全

面地反映通信交互的特点。

由免疫危险理论可知，抗体浓度受两方面影响：1)抗原的作用，分为凋亡和坏死；2)抗体与抗体之间的相互作用，分为刺激与抑制。不妨设某种危险信号 DS_i 相对应的抗体浓度为 $ds_i(t)$，下面分情况进行讨论。

1.2.2 免疫应答

免疫应答是引起抗体浓度变化的主要原因，是抗原对抗体的直接作用。只有达到亲和力匹配阈值，初始抗体才能被保留，进而参与到免疫应答过程；未达到阈值的抗体将不断交叉、变异，进入到下一次的匹配选择。

抗原凋亡代表该网络行为正常结束，网络状况良好，此时应抑制抗体的产生，用 $\omega ds_i^{ap}(t-1)$ 表示，$\omega=-1$ 为影响因子。抗原坏死代表该网络行为非正常结束，网络可能遭遇危险，此时应刺激抗体的产生，用 $\eta ds_i^{re}(t-1)$ 表示，$\eta>0$ 为影响因子。其中，

$$ds_i^{ap}=\sum_j Ab_i,\ \forall Ab_i\in B\wedge affinity(Ab_i,f_{APC}(DS_i^{ap}))\geqslant\xi$$
$$ds_i^{re}=\sum_j Ab_i,\ \forall Ab_i\in B\wedge affinity(Ab_i,f_{APC}(DS_i^{re}))\geqslant\xi \tag{9}$$

1.2.3 免疫平衡

抗体与抗体之间的相互作用主要体现为免疫平衡算子对抗体浓度的调节，用 ds_i^{new} 表示。免疫平衡算子以选择概率 P 对浓度低的抗体产生促进作用；反之，对浓度高的抗体产生抑制作用。P 由亲和度概率 P_t 和浓度概率 P_d 两部分组成。其中

$$ds_i^{new}=\sum_j Ab_i,\ \forall Ab_i\in B\wedge affinity(Ab_i,f_{APC}(DS_i^{new}))\geqslant\xi$$
$$ds_i^{old}=\sum_j Ab_i,\ \forall Ab_i\in B\wedge affinity(Ab_i,f_{APC}(DS_i^{old}))\geqslant\xi \tag{10}$$

ξ 为亲和度评价因子。

$$P=\begin{cases}\theta\cdot P_t+(1-\theta)\cdot P_{d(k)}, & CT_i\geqslant\rho\wedge CT_i\cdot N=k\\ & \wedge P_{d(k)}=\dfrac{1}{N}(1-\dfrac{k}{N})\\ \theta\cdot P_t+(1-\theta)\cdot P_{d(N-k)}, & CT_i<\rho\wedge CT_i\cdot N=N-k\\ & \wedge P_{d(N-k)}=\dfrac{1}{N}(1+\dfrac{k}{N}\cdot\dfrac{k}{N-k})\end{cases} \tag{11}$$

其中，$0\leqslant\theta\leqslant1$，$0<P_t,P_d<1$，$\rho$ 为抗体种群浓度阈值。可见，全部抗体的浓度概率之和为 1，抗体时刻处于选择进化克隆的动态变化之中。

1.2.4 危险程度评估

由前文，抗体浓度可表示如下：

$$ds_i(t)=\begin{cases}ds_i(0), & t=0\\ ds_i(t-1)+\omega ds_i^{ap}(t-1)+\eta ds_i^{re}(t-1)+\\ \quad ds_i^{new}(t-1)-ds_i^{old}(t-1), & \text{else}\end{cases} \tag{12}$$

由式(12)可以得出抗体浓度随时间的变化趋势。

定理 1 若某种抗原长时间(足够长)凋亡，则其相应的抗体浓度将以不高于 $p(0<p<1)$ 的速度衰减为 0。

证明：式(12)可表示为：

$$f(t)=\begin{cases}f(0), & t=0\\ f(t-1)+f_1(t-1)+f_2(t-1)+\\ \quad f_3(t-1)+f_4(t-1), & \text{else}\end{cases} \tag{13}$$

长时间凋亡即 $f_2=0,f_4=0$ 且 $f+f_1=0$，因此，可简化为 $f(t)=\begin{cases}f(0), & t=0\\ f_3(t-1), & \text{else}\end{cases}$。由式(11)知 $\exists p,0<P\leqslant p<1$，故 $f=P\cdot f_3\leqslant p\cdot f_3$。

若从 $t=0$ 开始凋亡，有 $f(t)\leqslant p\cdot f(t-1)\leqslant p^2\cdot f(t-2)\leqslant\cdots\leqslant p^t\cdot f(0)$，$\lim\limits_{t\to\infty}p^t\cdot f(0)=0$，故 $f(t)\to0$。

若从 $t=k$ 开始凋亡，有 $f(t)\leqslant p\cdot f(t-1)\leqslant p^2\cdot f(t-2)\leqslant\cdots\leqslant p^{t-k}\cdot f(k)$，$\lim\limits_{t-k\to\infty}p^{t-k}\cdot f(k)=0$，故 $f(t)\to0$。

定理 2 若某种抗原长时间(足够长)坏死，则相应的抗体浓度将趋于 $\dfrac{\eta_0}{1-\eta'}$。

证明：抗原坏死，即 $f_1=0,f_3=0$，且 $f_2=\eta\cdot f,f_4=-P'\cdot f$，$\exists p',0<p'\leqslant P'<1$，令 $\eta'=\eta-p'$。设 $f(0)=\eta_0$，不失一般性，设 $t=0$ 时抗原开始坏死，在经历 t 个时刻后，由式(13)可得

$$\begin{aligned}f(t)&=\eta_0+f_2(t-1)+f_4(t-1)\leqslant\eta_0+\eta\cdot f(t-1)-p'\cdot f(t-1)\\&=\eta_0+\eta'\cdot f(t-1)\leqslant\eta_0+\eta'\cdot(\eta_0+\eta'\cdot f(t-2))\\&=\eta_0+\eta_0\cdot\eta'+\eta_0\cdot\eta'^2\cdot f(t-2)\\&\cdots\\&\leqslant\eta_0+\eta_0\cdot\eta'+\eta_0\cdot\eta'^2+\eta_0\cdot\eta'^3+\cdots+\eta_0\cdot\eta'^t\\&=\eta_0\cdot\sum_{i=0}^{i=t}\eta'=\eta_0\cdot\frac{1-\eta'^{t+1}}{1-\eta'}\end{aligned}$$

由于 t 充分大，且 $\exists\eta,p'$ 使得 $0<\eta'<1$ 成立，因此抗体浓度将趋于 $\dfrac{\eta_0}{1-\eta'}$。

式(12)表明抗体浓度能够实时定量反映危险程度的大小。由定理 1，若长时间未检测到危险信号，则抗体浓度衰减至 0，表明该抗体表达的警报解除；由定理 2，若长时间连续检测到同类危险信号，抗体浓度将持续增加，浓度最大值表明系统可以承受的最大危险程度。

对于网络 M，设有 m 台主机(包括服务器)，每台设备在网络中的地位有所不同，对于主机 H_i，其重要性为 w_i，且 $\sum\limits_{i=1}^{m}w_i=1$。同时，不同类型的危险信号其危害性也不相同，设危险信号 DS_j 的危害性为 r_j，网络中共有 n 种危险。对主机 H_i，其抗体浓度为：

$$Ab_{Hi}=\frac{1}{n}\sum_{j=1}^{n}r_j ds_j \tag{14}$$

中心主机对来自各个主机的态势进行融合评估，可以得到整个的网络抗体浓度：

$$Ab_N=\frac{1}{m\cdot n}\sum_{i=1}^{m}\sum_{j=1}^{n}w_i r_j ds_j \tag{15}$$

可见，$0<Ab_N<1$，Ab_H 越接近 1，说明网络中抗体浓度越高，危险程度越大。

2 实验及分析

为验证所提方法的有效性，本文进行了仿真实验。实验网络由 1 个中心主机 MC、1 台服务器 Ser 和 4 台主机 H_i $(1\leqslant i\leqslant4)$ 组成。对 Ser 和 H_i 实施 syn flood、land、IP spoofing 攻击，$w(Ser)=0.4$，$w(H_1)=0.2$，$w(H_2)=w(H_3)=0.15$，$w(H_4)=0.1$，攻击的危害性分别为 0.8、0.7 和 0.5，危险信号为 $DS\in S$。抗原是对危险进行特征提呈后得到的二

进制串，如前所述，抗原包含源/目的地址 *src_IP/dst_IP*、端口号 *port*、协议类型 *protocol_type*、服务 *service*、连接状态 *flag*、登陆是否成功 *logged_in*。通过的字节数 *bytes*、连接长度 *duration* 等字段，$l=240$。模型其它参数主要有抗原凋亡影响因子 $\omega=-1$、抗原坏死影响因子 $\eta=0.98$、抗体种群浓度阈值 $\rho=0.75$、选择因子 $\theta=0.5$、种群大小 $N=200$、亲和度评价因子 $\xi=0.85$、迭代次数为 60000 次等。

考虑到不同危险强度条件下，主机或网络所受影响程度不同，为保证实验得以进行，交叉使用 syn flood、land、IP spoofing 攻击服务器和各主机(对每台设备，攻击顺序和强度可能不同)。图 2 给出了在服务器端 *Ser* 实施的攻击强度/危险程度(每秒的攻击包数目)和感知到的抗体浓度对比图，图 3 给出了中心主机进行融合分析后的整个网络的攻击强度/危险程度和抗体浓度对比图。

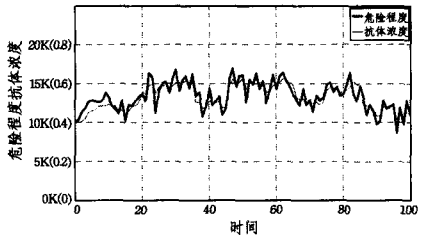

图 2　服务器 *Ser* 的危险程度和抗体浓度变化曲线

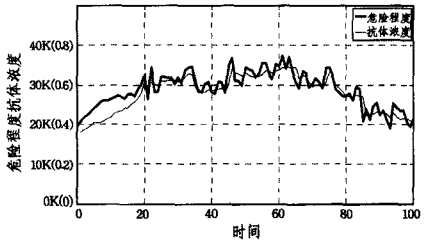

图 3　整个网络的危险程度和抗体浓度变化曲线

从图 2 和图 3 可以看出，当危险发生时，在时刻 0－10，模型经过免疫学习后，抗体浓度将随着相应危险程度的变化而变化。当危险程度降低时，如图 2 中的时刻 21 和图 2 中的时刻 46，相应抗体浓度下降缓慢，这对防止未来短时间内再次发生类似的危险有重要作用。当危险持续不断变化时，如图 1 中的时刻 24－34 和图 3 中的 43－63，抗体始终保持相对较高的浓度，说明系统对连续的变化保持较高的警惕，符合实际网络环境的要求。

由实验结果可知，模型计算出的抗体浓度与主机和网络所面临的危险程度有很好的一致性，即模型可实现对网络安全态势实时定量的评估。

结束语　针对传统人工免疫在入侵检测中自体与非自体动态变化且难以清晰界定的问题，基于网络安全问题与人体免疫问题的相似性，本文提出了基于免疫危险理论的网络安全态势评估方法；给出了危险信号、抗原、抗体和免疫细胞的形式化定义；通过研究抗原与抗体、抗体与抗体浓度之间的作用以及相关免疫选择机制，给出了抗体浓度的计算方法及其与危险程度的关系；最后得到整个网络的安全态势评估。仿真实验表明，本文提出的模型准确反映了系统面临的攻击大小/危险程度，能实时定量地对网络安全态势进行评估。完成面向多态势要素的感知和大型网络安全态势的评估是下一步工作的研究内容。

参 考 文 献

[1] Bass T, Arbor A. Multi-sensor data fusion for next generation distributed intrusion detection systems[C]//Proceeding of IRIS National Symposium on Sensor and Data Fusion. Laurel, MD: [s. n.], 1999: 24-27

[2] Wang Ling-yu, Singhal A, Jajodia S. Measuring network security using attack graphs[C]//Proceedings of the 2007 ACM Workshop on Quality of Protection. New York: ACM Press, 2007: 49-54

[3] Ning Peng, Cui Yun, Reeves D S, et al. Techniques and tools for analyzing intrusion alerts[J]. ACM Transactions on Information and System Security, 2004, 7(2): 274-318

[4] 郑黎明，邹鹏，张建锋，等. 面向大规模网络的安全态势实时量化感知模型[J]. 计算机科学，2011，38(10)：30-35
Zheng Li-ming, Zou Peng, Zhang Jian-feng, et al. Real time situational awareness model for large-scale networks[J]. Computer Science, 2011, 38(10): 30-35

[5] 张勇，谭小彬，崔孝林，等. 基于 Markov 博弈模型的网络安全态势感知方法 [J]. 软件学报，2011，22(3)：495-508
Zhang Yong, Tan Xiao-bin, Cui Xiao-lin, et al. Network Security Situation Awareness Approach Based on Markov Game Model [J]. Journal of Software, 2011, 22(3): 495-508

[6] 卓莹，何明，龚正虎. 网络态势评估的粗集分析模型[J]. 计算机工程与科学，2012，34(3)：1-5
Zhuo Ying, He Ming, Gong Zheng-hu. A Rough Set Analysis Model of Network Situation Awareness[J]. Computer Engineering & Science, 2012, 34(3): 1-5

[7] Feng Xue-wei, Wang Dong-xia, et al. Security Situation Assessment Based on the DS Theory[C]//Proceedings of the 2nd International Workshop on Education Technology and Computer Science. Wuhan, China: IEEE Comput. Soc, 2010: 352-356

[8] Matzinger P. The Danger Model: a Renewed Sense of Self[J]. Science, 2002(12): 301-305

[9] Dasgupta D, Yu S, Nino F. Recent Advances in Artificial Immune Systems: Models and Applications[J]. Applied Soft Computing, 2011(11): 1574-1587

[10] Yin Meng-jia, Zhang Tao, Shu Yuan. An Artificial Immune Model with Danger Theory Based on Changes[C]//Proceedings of 2011 IEEE International Conference on Information Theory and Information Security. Wuhan: Wuhan University, 2012: 672-676

[11] 张永铮，云晓春. 网络运行安全指数多维属性分类模型[J]. 计算机学报，2012，35(8)：1666-1678
Zhang Yong-zheng, Yun Xiao-chun. Network Operation Security Index Classification Model with Multidimensional Attributes [J]. Chinese Journal of Computers, 2012, 35(8): 1666-1678