基于免疫的新型入侵防御模型*

刘合安
(湖南城市学院 网络信息中心, 湖南 益阳 413000)

摘 要: 针对真实网络环境动态变化的特点,提出了一种基于免疫的新型入侵防御模型。给出了模型及其检测性能的形式化定义和数学描述;建立了基于动态自体库的多代动态耐受、抗体动态变化的数学模型及变化方程。通过真实网络数据及 KDDCup1999 入侵检测评估数据进行了仿真对比实验。结果表明,本模型具有更高的检测率和更低的虚警率,有效提高了网络安全的防御能力。

关键词: 入侵防御模型; 人工免疫系统; 虚警率; 检测率
中图分类号: TP18; TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)07-2712-03
doi:10.3969/j.issn.1001-3695.2012.07.085

Immune based novel intrusion prevention model

LIU He-an
(*Center of Network Information*, *Hunan City University*, *Yiyang Hunan* 413000, *China*)

Abstract: This paper proposed an immune based novel model for intrusion prevention for dynamic change of real network. It presented the formal definition and mathematical description of the model and its detection performance. Based on dynamic self-sets, it designed the mathematical model and equations of dynamic tolerance and dynamic Ab. The experimental data included the data collected from the actual LANs and KDDCup1999 intrusion detection evaluation data sets. The experimental results prove that the model has higher detection rate and lower false alarm rate. It enhances the security prevention of the network.

Key words: intrusion prevention model; artificial immune system; false alarm rate; detection rate

0 引言

入侵防御是目前网络安全技术发展的主要方向之一。它对所流经的网络流量进行检测与响应,具备主动防御能力[1]。生物免疫系统通过免疫学习、认知、反馈等机制,从而有效清除外来入侵,这与网络入侵防御系统有着极大的相似性,同时也为入侵防御的研究提供了一条新的思路。已有的基于免疫的入侵检测防御模型中[2~4],存在自体库庞大、缺乏自适应机制、缺少定量描述等问题。基于此,本文提出了一种基于免疫的入侵防御新模型,该模型能很好地模拟抗体自身演化过程及对入侵抗原的检测和处理过程。实验结果表明,本文模型具有更低的虚警率和漏检率、更高的检测率,可以有效提高网络安全的防御能力。

1 基本理论基础

1.1 入侵防御模型的形式化描述

基于免疫的入侵防御模型 Σ_{AIPS} 可表示为四元组:$\Sigma_{\text{AIPS}} = (\text{IN}_{\text{AIPS}}, \text{OUT}_{\text{AIPS}}, G_{\text{AIPS}}, D_{\text{AIPS}})$。其中:$\text{IN}_{\text{AIPS}}$ 表示入侵防御模型的输入,一般表现为网络数据包,令 W 表示输入的整个论域,I 表示入侵数据集合,$\bar{I}$ 表示正常数据集合,则 I 与 $\bar{I}$ 互斥,有 $I \cup \bar{I} = W$, $I \cap \bar{I} = \varnothing$, $\text{IN}_{\text{AIPS}} \in W$;$\text{OUT}_{\text{AIPS}}$ 表示入侵防御模型的输出,输出为报警 A 和不报警 $\bar{A}$ 两种状态,报警用 1 表示,不报警用 0 表示;G_{AIDS} 表示输入与输出之间的非线性函数关系,有

$$\text{OUT}_{\text{AIPS}} = G_{\text{AIPS}}(\text{IN}_{\text{AIPS}}) = \begin{cases} 1 & \text{if } \text{IN}_{\text{AIPS}} \in I \\ 0 & \text{if } \text{IN}_{\text{AIPS}} \in \bar{I} \end{cases}$$

D_{AIPS} 表示对检测到的入侵数据进行相应的主动防御处理,如直接丢弃。

1.2 入侵防御模型的检测性能描述

用符号 R_{TP}、R_{MP}、R_{FP} 分别表示入侵防御模型 Σ_{AIPS} 的检测率、漏警率、虚警率,则

$$R_{TP}(\Sigma_{\text{AIPS}}) = P(\text{OUT}_{\text{AIPS}} = 1 / \text{IN}_{\text{AIPS}} \in I)$$
$$R_{MP}(\Sigma_{\text{AIPS}}) = P(\text{OUT}_{\text{AIPS}} = 0 / \text{IN}_{\text{AIPS}} \in I) = 1 - R_{TP}$$
$$R_{FP}(\Sigma_{\text{AIPS}}) = P(\text{OUT}_{\text{AIPS}} = 1 / \text{IN}_{\text{AIPS}} \in \bar{I})$$

如果一个检测系统具有较高的检测率和较低的虚警率,则性能更优。

1.3 生物免疫系统与入侵防御系统的映射关系

基于免疫的入侵防御模型中,生物体类比为网络,生物免疫系统中的淋巴结类比为网络中的主机,免疫系统中的抗原类比为入侵防御中的网络行为,自体抗原、非自体抗原分别被类比为正常网络行为、非法网络行为,抗体(包括成熟抗体和记忆抗体)则被隐喻为入侵防御系统的检测器。生物免疫系统中抗体识别判断抗原是自体/非自体的过程就被类比为检测器检测网络行为是否正常(入侵)的过程[1,5,6]。

本文设计的基于免疫的入侵防御过程如图 1 所示。在模型中,随机生成的检测器将首先经历否定选择(免疫自体耐受),排除与自体匹配的检测器,生成成熟检测器。在克隆选

收稿日期: 2011-11-14; **修回日期**: 2011-12-15 **基金项目**: 湖南省科技厅自然科技基金资助项目(2010CK3030)
作者简介:刘合安(1975-),男,湖南桃江人,讲师,硕士,主要研究方向为计算机网络、信息安全、图形图像等(9571365@qq.com).

择模块中,通过成熟检测器完成对数据包的检测。如果是攻击,则进行相应的入侵响应;同时,在检测过程中动态更新检测器,以提高系统的检测率。

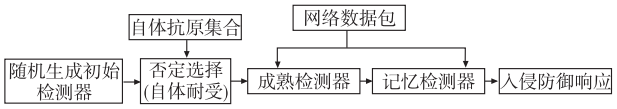

图 1　基于免疫的入侵防御过程

2　模型具体实现

2.1　抗原与抗体的形式化描述

定义所有的网络行为为问题空间 $D=\{0,1\}^l$,抗原集合 $Ag\subset D$,所有正常网络行为称为自体集合 $Self\subset Ag$,所有非法网络行为称为非自体集合 $Nonself\subset Ag$,有 $Self\cup Nonself=Ag$,$Self\cap Nonself=\varnothing$,则检测器和抗原均为相同长度的二进制串。

抗原和抗体的匹配采用 r 匹配算法,定义为

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

其中:1 表示匹配,0 表示不匹配[7]。

2.2　自体的动力学方程

在真实的网络环境中,正常网络行为(自体)和非正常网络行为(非自体)通常是动态变化的。传统的方法为了包含更多的正常行为,自体库往往过于庞大,并且由于成熟检测器的训练代价与自体集合的大小成指数关系,造成计算代价过大[8]。因此,本文提出了一个网络自体(正常活动)随时间动态变化的方程,并保证自体范围大小为 L,以提高训练效率。

定义自体的动力学变化方程为

$$Self(t)=\begin{cases}\{x_1,x_2,\cdots,x_n\} & t=0\\ Self(t-1)-Self_{dead}(t)- & t\geqslant 0\\ Self_{variation}(t)+Self_{new}\end{cases} \tag{2}$$

$$Self_{variation}(t)=\{x\mid x\in Self(t-1),\ \exists y\in B(t-1)\wedge f_{match}(x,y)=1\} \tag{3}$$

式(2)中 $x_i\in D(i\geqslant 1,i\in N)$ 为初始自体集合。$Self_{dead}$ 表示当自体集合超过阈值时,淘汰(死去)一部分自体元素,以保证自体集合的大小保持在一定规模,从而确保免疫耐受工作能够高效进行。$Self_{variation}$ 表示由于环境变化而发生了变异的自体(如由自体变为非自体),这些自体被随时清除,避免了未成熟抗体对发生变异的自体耐受,从而降低了漏警率。$Self_{new}$ 表示新增加的自体元素集合,从而扩大自体的描述范围,降低虚警率。

2.3　未成熟抗体(随机生成检测器)的演化

由于基因能用于描述异常的网络行为,因此,由基因组合、串联生成的检测器对相应的异常网络行为进行检测具有较好的预见性[9]。

定义基因库的动力学方程为

$$Gene(t)=\begin{cases}\{g_1,g_2,\cdots,g_k\} & t=0\\ Gene(t-1)-Gene_{dead}(t)+Gene_{new}(t) & t\geqslant 1\end{cases} \tag{4}$$

为了有效地控制检测器的进化方向,可以采用注射疫苗的方式。注射疫苗就是人工地将一段特有的基因与现有的未成熟检测器进行交叉变异,产生具有特殊基因的未成熟检测器,通过免疫耐受后参与到检测中,以提高入侵防御系统对特定攻击的检测和防御能力,减少系统漏警率。在实际应用中,对各种新出现的入侵手段,可以有效提取并注入相应的疫苗,再利用正选择的方法进行检测,从而提高系统的整体防御性能。

2.4　自体耐受(否定选择)动力学方程

未成熟抗体必须经过自体耐受才能转换为成熟抗体。由于自体 Self 是动态的,因此耐受过程也是动态的[5,10]。

定义自体耐受动力学方程为

$$I_b(t)=\begin{cases}\{x_1,x_2,\cdots,x_\xi\} & t=0\\ I_{tolerance}(t)-I_{maturation}(t)+I_{new}(t) & t\geqslant 1\end{cases} \tag{5}$$

$$I_{toderance}(t)=\{y\mid y\in I_b,y.d=x.d,y.age=x.age+1,\{x\mid x\in(I_b(t-1)-\{x\mid x\in I_b(t-1),\exists y\in Self(t-1)f_{match}(x,y)=1\}\)\} \tag{6}$$

$$I_{maturation}(t)=\{x\mid x\in I_{tolerance}(t),x.age>a\} \tag{7}$$

式(5)模拟免疫细胞自体耐受情况。其中:$x_i\in D(1\leqslant i\leqslant\xi)$ 为初始的未成熟免疫细胞;$I_{tolerance}(t)$ 为上阶段的自体 $Self(t-1)$ 经历耐受后的有效免疫细胞;$I_{maturation}$ 为 t 时刻成熟的免疫抗体(a 模拟耐受期,为大于 1 的常数);$I_{new}(t)$ 为 t 时刻新生成的未成熟免抗体。

动态耐受模型可以高效率地产生成熟细胞,并对经常性的正常网络活动耐受,保证了对突发网络活动的敏感性。这正好与真实网络环境相一致。

2.5　成熟抗体动力学方程

未成熟抗体经过自体耐受进化为成熟抗体。设 T_b 为成熟抗体集合,成熟抗体集合的动力学方程为

$$T_b(t)=\begin{cases}\varnothing & t=0\\ T_b(t-1)+T_{new}(t)-(T_{active}(t)+T_{dead}(t)) & t\geqslant 1\end{cases} \tag{8}$$

$$T_{new}(t)=I_{maturation}(t)+T_{clone}(t) \tag{9}$$

其中:$I_{maturation}(t)$ 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。

$$T_{active}=\{x\mid x\in T_b\wedge x.count\geqslant\theta\wedge x.age\leqslant\lambda\} \tag{10}$$

$$T_{dead}=\{x\mid x\in T_b\wedge x.count<\theta\wedge x.age>\lambda\} \tag{11}$$

其中:T_{active} 表示激活为记忆抗体的成熟抗体,即在生命周期 λ 内,匹配抗原数目达到了激活阈值;T_{dead} 表示删除未达到激活阈值的成熟抗体。

死亡机制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,并能保留最好的免疫细胞。通过克隆选择,淘汰那些对检测入侵没有作用或作用不大的抗体,保留优势抗体使之进化为记忆抗体,当类似入侵再次发生时,能进行更高效的应答和防御[11]。

通过上述理论上的创新,本模型有效地提高了检测率,降低了虚警率,提高了入侵防御系统的检测性能和效率。

3　系统仿真实验与分析

为了有效测试本模型的性能,用实际数据和仿真数据分别进行了两组实验。第一组数据来自于网络实验室局域网收集到的真实数据,第二组数据来源于 KDDCup1999 入侵检测评估数据集[12]。经过反复实验,参数值设置如下:$l=256$,$r=8$,

$N=50,\theta=40,\lambda=7,a=2,p=12,L=2000$。

第一组实验数据来自于网络安全实验室的通信数据,通过数据捕获程序获得。该实验室 40 台计算机参与了实验,这些计算机分别对外提供 WWW、FTP、e-mail 等服务,操作系统为 Windows 2003。收集该网络一周的正常网络数据作为训练数据。利用攻击工具对网络进行 Smurf、Syn flood、Teardrop 等攻击,将攻击产生的网络流量与正常的网络流量一起作为测试数据进行了多次实验。结果表明,系统的检测率平均可以达到 97% 以上,虚警率可以降低到 4% 以内。同时,与 Idid 算法[5] 进行了比较,实验结果如图 2 和 3 所示。

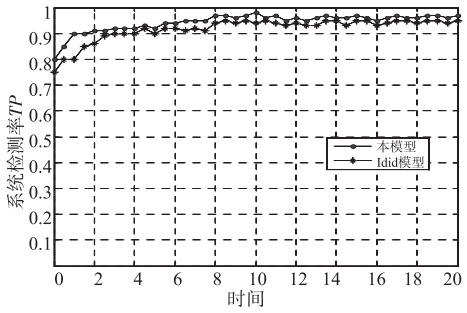

图 2 本模型与 Idid 模型检测率 *TP* 比较

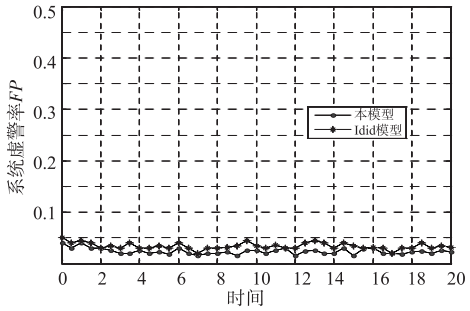

图 3 本模型与 Idid 模型虚警率 *FP* 比较

通过上面的实验数据可以发现,本文系统的检测率较高、虚警率较低,具有较好的检测性能。

第二组实验使用的数据是 KDDCup1999 入侵检测数据集。在样本库的选择上,采用 KDDCUP99 10% 的数据集作为基准数据。测试数据集中包含正常数据和攻击数据。攻击数据分为 DoS(拒绝服务攻击)、Probe(扫描与探查)、U2R(未经授权提升权限)、R2L(远端未经授权的访问)四大类[13]。用五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五次实验。实验结果采用 *TP* 值(检测率)和 *FP* 值(虚警率)对模型进行评估。实验结果表明,本系统平均 *TP* 值可以达到 97.18%,平均 *FP* 值可以降低到 3.13%。

同时,与三个开放源代码的 IDS 系统 Snort、Bro、Prelude IDS 进行了比较,共选用五个不同的测试数据集进行了测试。各系统的检测率如表 1 所示,虚警率如表 2 所示。

表 1 各系统检测率对比

测试集	Snort	Bro	Prelude IDS	本文模型
1	84.22	87.64	90.47	97.32
2	78.96	80.28	88.38	96.86
3	82.68	86.54	91.32	97.50
4	68.96	70.51	85.09	95.58
5	76.82	75.54	89.96	95.62

表 2 各检测器虚警率对比

测试集	Snort	Bro	Prelude IDS	本文模型
1	18.17	10.20	5.45	2.12
2	9.44	8.37	3.90	1.93
3	15.38	10.44	4.53	2.24
4	19.32	12.01	3.42	1.96
5	17.93	10.12	4.26	2.31

从结果可以看出,本模型具有较高的检测率和较低的虚警率,说明本模型具有良好的自学习性和自适应性。

4 结束语

本文提出了一种基于免疫的新型入侵防御模型。该模型与现实网络环境高度吻合,设计了网络攻击的动态进化过程。实验表明,本文提出的模型与已有模型相比,具有更高的检测率和更低的虚警率。同时,经过适当变换,本模型还可以应用于病毒检测及垃圾邮件识别等领域。如何进一步优化检测器以及入侵防御手段的完善是下一步研究的方向。

参考文献:

[1] 刘芳,朱思峰. 新型智能入侵检测模型[J]. 华中科技大学学报,2010,38(1):68-70.

[2] HARMER P K, WILLIAMS P D, GUNSCH G H, *et al*. An artificial immune system architecture for computer security applications[J]. IEEE Trans on Evolutionary Computation, 2002, 6(3): 252-280.

[3] 盛云雷,李永忠. 高速网络入侵防御系统中免疫算法的改进[J]. 微电子学与计算机,2011,28(5):99-102.

[4] 闫巧,江勇,吴建平. 基于免疫机理的网络入侵检测系统的抗体生成与检测组件[J]. 计算机学报,2005,29(9):1515-1522.

[5] 李涛. Idid:一种基于免疫的动态入侵检测模型[J]. 科学通报,2009,50(17):1912-1919.

[6] LIU Sun-jun, LI Tao. Multi-agent network intrusion active defense model based on immune theory[J]. Wuhan University Journal of Natural Sciences, 2007, 12(1): 167-171.

[7] 李涛. 基于免疫的网络监控模型[J]. 计算机学报,2008,29(9):1515-1522.

[8] 何申,罗文坚,王煦法. 一种检测器长度可变的非选择算法[J]. 软件学报,2007,18(6):1361-1368.

[9] TIMMIS J, ANDREWS P, OWENS N, *et al*. An interdisciplinary perspective on artificial immune systems[J]. Evolutionary Intelligence, 2008, 1(1): 5-26.

[10] KIM J, BENTLEY P J, AICKELIN U, *et al*. Immune system approaches to intrusion detection: a review[J]. Natural Computing, 2009, 6(4): 41-66.

[11] 罗文坚,曹先彬,王煦法. 检测器自适应生成算法研究[J]. 自动化学报,2007,31(6):907-916.

[12] University of California. KDDLib[EB/OL]. [2009-03-02]. http://kdd.ics.uci.edu/databases/kddcup99.

[13] KIM J, BENTLEY P J. Immune memory and gene library evolution in dynamical clone selection algorithm[J]. Journal of Genetic Programming and Evolvable Machines, 2004, 5(4): 361-391.

[14] KIM J, BENTLEY P J. Towards an artificial immune system for network intrusion detection: an investigation of dynamic clonal selection [C]//Proc of Congress on Evolutionary Computation. Piscataway: IEEE Press, 2002: 1015-1020.

[15] 刘才铭,张雁. 多级免疫检测器集在分布式入侵检测中的应用[J]. 电子科技大学学报,2007,36(6):1179-1182.

[16] DASGUPTA D. Advances in artificial immune system[J]. IEEE Computational Intelligence Magazine, 2006, 1(4): 4-9.