免疫系统的主组织相容复杂性及其应用

李 军，郝玉洁，刘乃琦，罗大光

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】在模拟免疫系统的主组织相容复杂性的基础上，结合模糊逻辑与扩展阴性选择算法提出了一个基于免疫系统主组织相容复杂性的模糊逻辑综合决策算法，并用该算法构建了一个实际的基于网络的入侵检测系统。该算法应用高效的扩展阴性选择算法作出第一次网络流量检测，当网络数据异常特征明显时，能直接检测出入侵。若其不能准确地识别待分析数据，则利用具有检测结果准确优势的规则匹配算法作出二次检测，最后结合两次检测结论用模糊逻辑决策模型做出综合决策。

关 键 词 主组织相容复杂性; 人工免疫; 模糊逻辑; 入侵检测
中图分类号 TP311 文献标识码 A

Major Histocompatibility Complex of Immune System and Its Application

LI Jun，HAO Yu-jie，LIU Lai-qi，LUO Da-guang

(School of Computer Science and Engineering, Univ. of Electron. Sci. & Tech. of China Chengdu 610054)

Abstract A novel algorithm based on the simulation of the major histocompatibility complex feature of human immune system is proposed. The extended negative selection algorithm makes the first decision to decide whether the network traffic is intrusion. Another algorithm, rule match-based alglrithm, makes the second decision while the first decision failed to identify the intrusion. The proposed algorithm, called major histocompatibility complex feature-based synthetic fuzzy decision-making algorithm, composes the first decision and the second decision to make a synthetic fuzzy decision by taking advantage of fuzzy logic.

Key words major histocompatibility complex; artificial immune system; fuzzy logic; intrusion detection

在计算智能技术领域，自然免疫是一个非常复杂的系统。由于人体免疫系统抵御抗原的方式与计算机入侵检测系统的相似性，许多学者利用人工免疫技术建立了一些基于免疫原理的入侵检测系统。

1 免疫原理及其应用

人体免疫功能由淋巴系统执行，T 细胞和 B 细胞及主组织相容复杂性分子(Major Histocompatibility Complex，MHC)在免疫机制中起重要作用，正是由于 MHC 分子的二次识别，才使免疫系统能有效地辨别抗原和正常体内细胞[1]。文献[2-3]证明了自然免疫系统的基因库进化、阴性选择和无性繁殖(克隆)等 3 个主要特性能建立一个有效的基于网络的入侵检测系统，该系统满足分布性、自组织和轻量级的要求。

文献[1,4,5]开发了一种基于免疫技术的扩展阴性选择算法(eXtended Negative Selection Algorithm,XNSA)来刻画入侵特征。该算法采用 n 维超立方体描述问题空间，取每秒分组、字节或 ICMP 数作为参数 $\boldsymbol{r}$，以向量($\boldsymbol{r}_1$，$\boldsymbol{r}_2$，…，$\boldsymbol{r}_n$)作为超立方体中的点，经过训练，使用从麻省理工大学林肯实验室得到的正常及入侵数据集后得到一个抗体集合，将计算出的实时网络数据在 n 维超立方体中的点的位置与抗体集合中的点相比较。使用由马里兰大学开发的计算 K 维空间树中点的欧几里德距离的函数库，根据欧几里德距离的大小，便可得出实际网络数据是入侵数据的可能性。如图 1 所示，通过精心选择的参数(取欧几里德距离门限值为 0.8)，在某次实际的攻击检验测试中，5 次攻击都被精确地检测到了，如图中的 Back，Portsweep，Satan，Portsweep 和 Neptune。因此，扩展阴性选择算法在入侵数据分析中表现出了良好的性能。并且，由于扩展阴性选择算法检测子的产生是完全随机的[4]，保证了对未知入侵的有效检测。但扩展阴性算法还存在一些问题：(1) 算

收稿日期：2003 – 11 – 25
作者简介：李 军(1976 –)，男，硕士生，主要从事网络与信息安全、计算智能领域方面的研究.

法“异常数据的特征可以被以某种变量为参数的时间序列所刻画”的基本假设，虽然实验证明这个假设较符合实际，但没有获得充分的理论依据；(2) 算法要精心地选择阈值才能准确地检测入侵，在入侵手段变化多端的现代网络中比较困难；(3) 算法要求有很好的网络数据噪声抑制功能。所以需要考虑是否能将传统的规则匹配算法的高准确性与扩展阴性选择算法结合，构造一个具有两者优点的入侵检测系统。

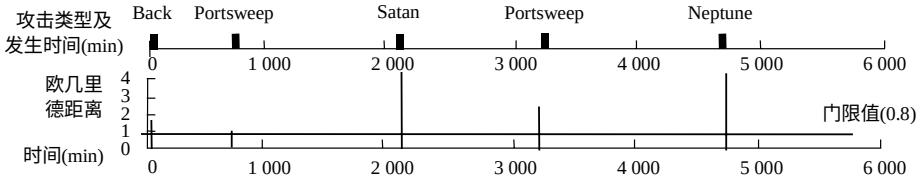

图 1　扩展阴性选择算法的检测结果

2　基于MHC原理的入侵数据检测算法

根据免疫系统的 MHC 特性及文献[1]的研究，本文提出了基于 MHC 特性的模糊逻辑综合决策系统。作为对免疫系统的 B 细胞的模拟，该系统首先以扩展阴性选择算法作为主检测引擎，以发挥其高效、能检测未知入侵的特点。当检测结果 P_1 值高于根据实际情况预先选定(配置)的门限值 P_0 时，系统直接认定这是一个入侵数据。根据文献[1]的结果，当数据表现出较强的攻击特征，即当 P_1 值较大时，说明数据分析结果远高于特征阈值时，此引擎能很好地工作。若数据入侵特征并不明显，判定数据包是否是恶意数据包并不容易。此时，数据分析结果接近特征阈值，即 P_1 值在 P_0 值附近，由 XNSDAE 触发基于规则匹配的数据分析 RDAE 引擎进行二次检测。XNSDAE 对 RDAE 的触发由一个包含可疑数据标识的 IP 数据包(*time_X*，P_1)组成。*Time_X* 表示可疑数据发生的时间段，P_1 表示 XNSDAE 的分析结果。在正常情况下，RDAE 没有收到(*time_X*，P_1)数据包时，只是简单地提取网络数据的规则特征，并将其存储于特征库 DB_Signature 中，并不执行规则匹配算法。当 RDAE 收到(*time_X*，P_1)触发信号时，启动规则匹配算法，将已存储的在时间段 *time_X* 中出现过的网络数据特征值取出，并进行传统的规则匹配算法，得出一个可能是入侵的概率 P_2 值可由匹配时耦合度决定，比如在汉明匹配中的汉明距离的长短。根据 XNSDAE 及 RDAE 的结果，P_1、P_2 运用模糊逻辑综合决策算法得出综合检测结果。

基于MHC原理的入侵数据检测算法如下:

While收到标识为(*time_X*，P_1的包){

从特征数据库DB_signature中提取在时间*time_X*段中发生的网络数据的特征(可能有多个)并存入数组*X*_array[*k*]；

if(*k*=0)　//数据库中没有存储在时间*time_X*段中发生的网络数据

continue；

else{　// 数据库中存储有在时间*time_X*段中发生的网络数据

for(int *I*=0；*I*<*k*；*I*++){

调用规则匹配算法得出本连接是入侵的概率P_2；

根据参数P_1，P_2调用模糊逻辑综合决策算法得出检测结果；

根据结果切断连接或发出警告等；

continue；

}

}

3　模糊逻辑综合决策算法

根据扩展阴性选择算法与规则匹配的结果，结合模糊逻辑理论，做出一个模糊逻辑综合决策是模糊逻辑综合决策系统的重点。为了达到这个目的，先引入一个模糊决策模型描述问题空间如下[6]：

设 $f: X \to Y, x \mapsto f(x)$，则称映射 X to Y：$f: X \to F(Y), x \mapsto f(x) = B \in F(Y)$ 为从*X*到*Y*的点-集映射，*F*(*A*)表示*A*的幂集。

3.1 模糊逻辑综合决策系统的数学模型

(1) 因素集$U=\{u_1,u_2\}$，其中u_1为XNSDAE分析结果，u_2为RDAE分析结果。

(2) 评判集$V=\{v_1,v_2,v_3\}$，其中v_1是入侵；v_2有可能是入侵；v_3不是入侵。且v_1，v_2，$v_3\in[0.0, 1.0]$

(3) 根据XNSDAE及RDAE分析的结果，对每一因素u_i单独做一个评判$f(u_i)$，可以看作是U到V的模糊映射f，即 $f:U\to F(V);u_i\mapsto f(u_i)=\{r_{i1},r_{i2},r_{i3}\}\in F(V)$。

(4) 权重$A=(a_1,a_2)\in F(U)$，a_i为因素u_i的权重，且$\sum a_i=1$。权重的作用是根据不同的情况，对XNSDAE和RDAE采取不同的信任度。

(5) 根据模糊逻辑与上面的数学模型，可以得出一个模糊关系(Zadeh 表达式)[6]：

$$f:U\to F(V),u_i\mapsto f(u_i)=B=\frac{r_{i1}}{y_1}+\frac{r_{i2}}{y_2}+\frac{r_{i3}}{y_3}=(r_{i1},r_{i2},r_{i3})\in F(V)$$

该模糊关系也可以用模糊矩阵表示为：

$$\boldsymbol{R}=\begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \end{bmatrix}$$

由此，(U,V,R)构成了一个模糊综合决策模型。根据该模型取max-min合成运算，即用模型$M(\wedge,\vee)$计算Zadeh表达式可得综合评判结果 $B=A\circ\boldsymbol{R}$。

3.2 模糊逻辑综合决策算法的一个实例

应用这个模型到基于MHC特性的模糊逻辑综合系统便可从XNSDAE与RDAE的分析结果得出一个综合决策用P_1与P_2表示的入侵概率向量(v_{i1},v_{i2},v_{i3})。以下是应用该决策模型到入侵检测系统的一个例子。

(1) 从XNSDAE，可以得到一个以概率表示的分析结果，设u_1(0.7，0.3，0)表示扩展阴性选择算法对某网络数据分析的结果；其中，从RDAE，可以得到应用规则匹配表示的结果，设为u_2(0.5，0.3，0.2)，且其含义同u_1，故模糊矩阵为：

$$\boldsymbol{R}=\begin{bmatrix} 0.7 & 0.3 & 0 \\ 0.5 & 0.3 & 0.2 \end{bmatrix}$$

(2) 依据不同的网络环境和客户需求，可能需要对XNSDAE与RDAE的结果赋予不同的权重$A=\{a_1,a_2\}$，取A_1=(0.7，0.3)表示在做决策时对XNSDAE的分析结果较为重视，可得综合评判：

$$B_1=A\circ\boldsymbol{R}=(0.7,0.3)\begin{bmatrix} 0.7 & 0.3 & 0 \\ 0.5 & 0.3 & 0.2 \end{bmatrix}=(0.64,0.3,0.06)$$

根据最大隶属度原则，在权重A_1下这次分析结果认定连接为入侵。

(3) 为了更方便地显示决策信息及提高灵活性，可以将评判结果所形成的向量归一化。为此将评判集的等级用1分制数量化，再将评判结果进行加权平均，便可得单一的评判结果。取评判集V=[0.8(入侵), 0.6(可能是入侵)，0.4(非入侵)]，并且规定归一化后的分值V_0在0.7以上为入侵，则得归一化结果为 $V_0=(0.64,0.3,0.06)\begin{bmatrix} 0.8 \\ 0.6 \\ 0.4 \end{bmatrix}=0.716$，此次分析结果说明连接为入侵。

如果用户根据环境的变化更重视RDAE的分析结果，可以取权重A_2=(0.3，0.7)，所得到的归一化结果为 $V_0=B_1\circ V=(0.3,0.7)\begin{bmatrix} 0.7 & 0.3 & 0 \\ 0.5 & 0.3 & 0.2 \end{bmatrix}\begin{bmatrix} 0.8 \\ 0.6 \\ 0.4 \end{bmatrix}=0.684$，在权重$A_2$及门限0.7这两个条件下，分析结果表明连接不是入侵。

4 结 论

基于MHC特性的模糊逻辑综合系统利用模糊逻辑综合了XNSDAE和RDAE检测不同入侵的优点，并且由于对权重A、评判集B和门限的不同选择可以体现不同网络环境的特征，因此具有非常好的适应性，可以根据用户环境进行参数调整，从而得出一个最好的检测结果。

参　考　文　献

[1] Gonzalez F, Dasgupta D. An immunogenetic technique to detect anomalies in network traffic[C]// The International Conference Genetic and Evolutionary Computation (GECCO), New York, 1999.
[2] Kim J, Bentley P. The human immune system and network intrusion detection[C]// 7th European Congress on Intelligent Techniques and Soft Computing，Aachen, 1999.
[3] Kim J. The artificial immune system for network intrusion detection[C]// Genetic and Evolutionary Computation Conference，Orlando, 1999.
[4] Dasgupta D，Gonzalez F. An immunity-based technique to characterize intrusions in computer networks[J]. IEEE Transactions on Evolutionary Computation, 2002，6(3): 281-291.
[5] Gonzalez F. Study of artificial immune systems applied to anomaly detection[D]//Nemphis: University of Memphis, 2003.
[6] 谢季坚, 刘承平. 模糊数学方法及其应用[M].武汉: 华中科技大学出版社，2000.

编　辑　熊思亮

(上接第533页)

尽管改进的AC-BM算法能区分大小写，但为了使检测条件与AC-BM算法一致，在测试时，统一为不区分大小写。为避免进程调度带来的干扰，每组测试取10次的平均值，测试结果见表1。从表中可以看出，不同的数据集，测试结果各有差异，但每次测试结果都表明，改进的AC-BM算法比原AC-BM算法要快。

4　结 束 语

字符串匹配是入侵检测、防火墙、内容分析与审计等系统的关键技术之一。本文对AC-BM算法提出改进方案，保留了原算法的优点，但实现更加简单，性能也更好。作为一种新型的算法，AC-BM算法还可进行其他改进，例如，AC-BM算法在预处理时，对规则进行了排序，这种排序有利于提取规则的共同前缀信息，但却改变了规则的命中顺序，从而与部分入侵检测、防火墙系统要求产生矛盾。对AC-BM算法的进一步改进是本文的后续课题。

参　考　文　献

[1] Knuth D, Morris J, Pratt P. Fast pattern matching in strings[J]. SIAM Journal on Computing, 1997, 6(2): 323.
[2] Boyer R S, Moore J S. A fast string searching algorithm[J] Communications of the ACM, 1997, 20(10): 762.
[3] Nigel H R. Practical fast searching in strings[J]. Software Practice and Experience, 1980, 10(6); 501-506.
[4] Aho A, Corasick M. Efficient string matching: An aid to bibliographic search[J]. Communications of the ACM, 1975, 18(6): 333-343
[5] Jason C C, Staniford S, McAlemey J. Towards faster string for intrusion detection or exceeding the sped of snert[J/OL]. http://www.silicondefense.com/sotfware/acbm/speed_of_snort_03_16_2001.padf, 2003-10-06
[6] Fisk M, Varghese G. Fast content-base packet handling for intrusion detection[R]. UCSD Techinal Report: ucsd-tr-cs,2001-0670.
[[7] 王永成, 沈　州, 许一震. 改进的多模式匹配算法[J]. 计算机研究与发展, 2002, 39(1):55-60

编　辑　熊思亮