基于免疫机理的入侵检测系统的数学描述

闫 巧
(深圳大学信息工程学院 深圳 518060)

摘 要 入侵检测问题可以看作是一种模式分类问题,但由于该问题具有一些固有特点如高维特征空间、模式之间的线性不可分性、正常和异常数据的严重不均匀性,使得直接使用传统的模式识别方法进行攻击检测时比较困难。自然免疫系统实际上是一个分布的具有自适应性和自学习能力的分类器,它通过学习、记忆和联想提取来解决识别和分类任务,基于自然免疫机理设计了一个入侵检测系统,并给出了它的性能指标的数学描述。重点是基于免疫机理设计了具有多层次性、多样性、独特性、异常检测能力、抑制虚警能力、健壮性、自适应性和动态防护性的入侵检测系统 AIIDS。

关键词 入侵检测,免疫机理,模式分类
中图法分类号 TP393 **文献标识码** A

Mathematic Description of Intrusion Detection System Based on Immune Mechanism

YAN Qiao
(Information Engineering School, Shenzhen University, Shenzhen 518060, China)

Abstract Intrusion detection can be looked as a problem of pattern classification. Since intrusion detection has some intrinsic characteristic such as high dimensional feature spaces, linearity non-differentiation, severe unevenness of normal pattern and anomaly pattern, it is very difficult to detect intrusion by using classical pattern recognition method directly. Nature immune system is a self-adaptive and self-learning classifier, which can accomplish recognition and classification by learning, remembrance and association. In this paper first we used four-tuple to define nature immune system and intrusion detection system, and then we gave the mathematic formalization description of performance index of intrusion detection system. Finally we put emphasis on designing an intrusion detection system based on immune mechanism, named AIIDS, which has many good features such as multiple layers, distributablility, diversity, uniqueness, anomaly detection, restraining false positive alarm, robustness, adaptability, dynamic defensive.

Keywords Intrusion detection, Immune mechanism, Pattern classification

1 引言

入侵检测问题可以看作是一种模式分类问题,如果仅要求将当前活动分成正常和异常的话,入侵检测问题就可以看作是一种两类的模式分类问题,对于分类问题,模式识别技术已经做了深入研究,但是由于入侵检测问题存在下面一些特点,这些特点是:

·为了判别当前活动的正常和异常,提取的特征往往是高维的,而传统的模式识别方法在应用于高维特征时会存在一定困难。

·由于入侵模式和正常模式并不遵从一定的分布,而且不是线性可分的,因此使用各种统计分类方法如贝叶斯方法、线性分类器或简单的非线性分类器方法进行分类存在很多困难。如使用贝叶斯分类方法,需要估计类间概率密度,而正常类或异常类的类间概率密度是随时间随机变化的,难以估计。

·虽然分类正常或异常仅仅是简单的两类问题。但这两类是非常不均匀的,入侵数据分散在广泛的正常记录的背景噪声中,而正常记录的数据量特别巨大,入侵与正常数据的比一般为 $10^{-5}\sim2\times10^{-5}$ 或更低[1],为此常常将入侵检测问题说成是海里捞针问题,这种问题既对应海量样本的数据集,又需要模式识别算法具有良好的鲁棒性,即算法性能不应以假设模型有小的偏离而受到显著的影响,并且不会因噪声或孤立点的影响而显著恶化。

正是由于入侵检测问题具有上述的一些固有特点,使得直接使用传统的模式识别方法进行攻击分类时比较困难,而自然免疫系统面临着与入侵检测类似的问题,比如"自身"与"有害的非自身"也不是线性可分的,区分"自身"与"有害的非自身"也需要采用高维特征,并且"自身"蛋白质的量非常巨大,而少量的"非自身"毫无规律地分布在"自身"蛋白质中。但是自然免疫系统利用不同类型的防御细胞的共同努力,能够高效地用最短的响应时间、最大限度地利用有限的资源来区分"自身"与"有害的非自身",保证生物体的存活和正常生

到稿日期:2008-07-24 返修日期:2008-10-13 本文受国家"973"重点基础研究发展规划基金项目(2003CB314805),国家自然基金-广东省联合基金(U0675001),深圳大学青年科学基金(200875)资助。

闫 巧(1972-),女,博士,副研究员,CCF会员,主要研究领域为网络安全和人工免疫系统,E-mail:yanq@szu.edu.cn。

理活动的进行。从计算角度来看，自然免疫系统实际等同于一个分布的、具有自适应性和自学习能力的分类器，它通过学习、记忆和联想等方法较圆满地完成了识别和分类任务。所以本文将根据免疫机理的启发来设计一个入侵检测系统，以更好地完成检测入侵的任务。

2 定义

首先我们用一个四元组来描述自然免疫系统 Σ_{NIS}。

$$\Sigma_{NIS}=(X_{NIS},\Omega_{NIS},\Upsilon_{NIS},G_{NIS}) \tag{1}$$

其中 X_{NIS} 为自然免疫系统的输入。它可能为各种类型的抗原，该抗原可能是自身蛋白，也可能是某种病原体，若令 E 表示抗原全体，则整个抗原全体包括两个互斥的集合即自身蛋白集合和病原体集合，若用 S 表示自身蛋白集合，NS 表示病原体集合则有：

$$S\cup NS=E,S\cap NS=\phi \tag{2}$$

Y_{NIS} 为自然免疫系统的输出，这里仅考虑免疫系统对病原体的识别而忽略免疫效应（即免疫系统消灭病原体的反应），则 Y_{NIS} 可以取 0 或 1，分别表示自然免疫系统判别输入是自身或非自身。

G_{NIS} 表示自然免疫系统输入与输出之间的非线性关系函数，有

$$Y_{NIS}=G_{NIS}(X_{NIS})=\begin{cases}1 & \text{若判别 } X_{NIS}\in NS\\ 0 & \text{若判别 } X_{NIS}\in S\end{cases} \tag{3}$$

Ω_{NIS} 为自然免疫系统的内部组成，从不同的角度看，Ω_{NIS} 可能有不同的组成部分。

同理定义入侵检测系统为 Σ_{IDS}

$$\Sigma_{IDS}=(X_{IDS},\Omega_{IDS},Y_{IDS},G_{IDS}) \tag{4}$$

其中 X_{IDS} 为入侵检测系统的输入，它可能是操作系统日志记录或网络数据包。令 W 表示输入的整个论域，则整个论域可以划分成为两个互斥的集合即入侵集合，表示为 I 和正常集合表示为 $\neg I$，则有：

$$I\cup\neg I=W \quad I\cap\neg I=\phi \tag{5}$$

$$\text{输入 } X_{IDS}\in W \tag{6}$$

Y_{IDS} 为入侵检测系统的输出，这里入侵检测系统具有报警 A 和不报警 $\neg A$ 两种状态，报警用 1 来表示，不报警用 0 来表示。

G_{IDS} 表示输入与输出之间的非线形函数关系，有

$$Y_{IDS}=G_{IDS}(X_{IDS})=\begin{cases}1 & \text{若判别 } X_{IDS}\in I\\ 0 & \text{若判别 } X_{IDS}\in \neg I\end{cases} \tag{7}$$

Ω_{IDS} 为入侵检测系统的内部组成。不同类型的入侵检测系统，一般具有不同的 Ω_{IDS}，从而产生不同的 G_{IDS} 将输入向量映射到输出的两类中。对于一个入侵检测系统我们最关心的是它的检测性能、健壮性、自适应性和动态防护性，下面给出这些指标的数学描述。

我们用符号 R_{TD} 表示检测率，则入侵检测系统 Σ_{IDS} 的检测率可以表示为 $R_{TD}(\Sigma_{IDS})$，根据检测率的定义有：

$$R_{TD}(\Sigma_{IDS})=P(Y_{IDS}=1/X_{IDS}\in I) \tag{8}$$

用符号 R_{MD} 表示漏警率，则根据漏警率的定义有：

$$R_{MD}(\Sigma_{IDS})=P(Y_{IDS}=0/X_{IDS}\in I)=1-R_{TD}(\Sigma_{IDS}) \tag{9}$$

用符号 R_{FD} 表示虚警率，根据虚警率的定义有：

$$R_{FD}(\Sigma_{IDS})=P(Y_{IDS}=1/X_{IDS}\in \neg I) \tag{10}$$

定义 1（入侵检测系统的检测性能） 我们用符号 DA 表示检测性能，则入侵检测系统 Σ_{IDS} 的检测性能可以表示为 $DA(\Sigma_{IDS})$。衡量入侵检测系统的性能可以从很多方面考虑，因此也可以制订许多相应指标，我们在此处采用错误概率作为检测性能的指标，定义：

$$DA(\Sigma_{IDS})=\omega_{MD}\cdot R_{MD}(\Sigma_{IDS})+\omega_{FD}\cdot R_{FD}(\Sigma_{IDS}) \tag{11}$$

其中 ω_{MD} 和 ω_{FD} 为权值，可根据具体情况下检测性能中对漏警或虚警的侧重不同而赋值，且有：

$$0\leqslant\omega_{MD}\leqslant 1,0\leqslant\omega_{FD}\leqslant 1,0\leqslant\omega_{MD}+\omega_{FD}\leqslant 1 \tag{12}$$

所以有 $DA(\Sigma_{IDS})\in[0,+1]$，且该值越小，说明检测性能越好，理想的入侵检测系统的 DA 为 0。

定义 2（入侵检测系统的健壮性） 设有入侵检测系统 Σ_{IDS} 的内部组成 $\Omega_{IDS}=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$，其中 $\alpha_i(1\leqslant i\leqslant n)$ 为检测代理或子系统，n 为检测代理或子系统的个数。若有任意 k $(k<n)$ 个检测代理或子系统失效，即原入侵检测系统 Σ_{IDS} 变成新的入侵检测系统 $\breve{\Sigma}_{IDS}$，$\breve{\Sigma}_{IDS}$ 的 $\breve{\Omega}_{IDS}=\{\alpha_1,\alpha_2,\cdots,\alpha_{n-k}\}$。如果满足：

$$\frac{DA(\breve{\Sigma}_{IDS})-DA(\Sigma_{IDS})}{DA(\Sigma_{IDS})}\leqslant\Gamma \tag{13}$$

其中 Γ 为规定的指标，则称原系统具有 k 级健壮性。

定义 3（入侵检测系统的自适应性） 设有入侵检测系统 Σ_{IDS} 的内部组成 $\Omega_{IDS}=\{\bigcup_{i=1}^{n}\beta_i\}$，其中 $\beta_i(1\leqslant i\leqslant n)$ 为检测代理或子系统或检测规则，n 为检测代理或子系统或规则的个数，若经过一段时间 T，随着入侵的变化，原系统变成 $\dot{\Sigma}_{IDS}$，并且 $\dot{\Sigma}_{IDS}$ 的 $\dot{\Omega}_{IDS}=\{\bigcup_{i=1}^{m}\dot{\beta}_i\}$，其中 $\dot{\beta}_i(1\leqslant i\leqslant m)$ 为新系统的检测代理或子系统或检测规则，m 为检测代理或子系统或检测规则的个数。如果满足以下任意一个条件，则称原系统具有自适应性。

①$DA(\dot{\Sigma}_{IDS})<DA(\Sigma_{IDS})$；

②$\dot{\Sigma}_{IDS}$ 检测到入侵所用的时间 $\dot{t}$ 比 Σ_{IDS} 检测到入侵所用的时间 t 少；

③$\dot{\Sigma}_{IDS}$ 检测到入侵所用的资源 $\dot{r}$ 比 Σ_{IDS} 检测到入侵所用的资源 r 少。

定义 4（入侵检测系统的动态防护性） 设入侵检测系统 Σ_{IDS} 的内部组成 Ω_{IDS} 在一段时间 T 内所可能包括的全部检测代理或检测规则的集合为 A_{all}

$A_{all}=\{a_1,a_2,\cdots,a_n$，其中 n 为代理或规则个数$\}$

以 f 为采样频率可以得到时间段 T 内的 k 个均匀时间采样点 $t_1,t_2,t_3,\cdots,t_k$，其中 $k=\lfloor fT\rfloor$，设在任意时刻 $t_i(1\leqslant i\leqslant k)$，$\Omega_{IDS}$ 所包括的检测代理或规则集合为 A_{t_i}，若同时满足下列条件：

①动态性：$A_{t_i}\subseteq A_{all}$，且存在 i,j，其中 $1\leqslant i\leqslant k,1\leqslant j\leqslant k$，满足当 $i\neq j$ 时有 $A_{t_i}\neq A_{t_j}$；

②完备性：f_0 使得当 $f\geqslant f_0$ 时，有 $A_{all}=\bigcup_{i=1}^{k}A_{t_i}$，则称 Σ_{IDS} 具有动态防护性。

3 自然免疫系统的启发

自然免疫系统 Σ_{NIS} 实际上是一个复杂的模式识别系统，它能够比较圆满地完成检测任务，从而保证生物个体的存活和种族的延续。

3.1 检测性能

自然免疫系统具有非常优异的检测性能，即高的检测率和低的虚警率。比如人的免疫系统能够检测到大约 10^{16} 种抗原，包括许多未知的抗原，而染上自免疫疾病的可能性却很低[2]。自然免疫系统之所以具有这样好的检测性能，是因为自然免疫系统具有多层次性、多样性、独特性、异常检测能力、协同性等多种良好特性。

3.1.1 多层次性

从防护层次来看

$$\Omega_{NIS}=\{L_1,L_2,L_3,L_4\} \tag{14}$$

其中，L_1 为皮肤与黏膜，L_2 为生理屏障，L_3 为先天性免疫系统，L_4 为自适应免疫系统。每一个 L_i 对不同的病原体有不同的检测能力，各个 L_i 之间呈现一种并联互补模式，从而增加自然免疫系统 Σ_{NIS} 的检测能力。

3.1.2 多样性

从细胞粒度来看，自然免疫系统 Ω_{NIS} 可表示为：

$$\Omega_{NIS}=\left\{\bigcup_{\substack{i=1\sim m\\ j=1\sim k_i}} C_{ij},\ \begin{array}{l}\text{其中 } m \text{ 为淋巴细胞的种类个数，}\\ k_i \text{ 为第 } i \text{ 种淋巴的个数}\end{array}\right\} \tag{15}$$

自然免疫系统 Σ_{NIS} 包含着种类繁多的免疫细胞如 T 淋巴细胞、B 淋巴细胞、噬菌细胞、中性粒细胞等等。每一种免疫细胞都包括多个个体分散到体内不同的淋巴节点，每一个免疫细胞 C_{ij} 擅长检测一种或几种病原体，从而使得整个自然免疫系统 Σ_{NIS} 能够检测多种类型的病原体。

3.1.3 独特性

独特性是指：若有

$$\Omega_{NIS}=\{\bigcup_{\substack{i=1\sim m\\ j=1\sim k_i}} C_{ij}\}\neq\Omega_{NIS}'=\{\bigcup_{\substack{i=1\sim m\\ j=1\sim k_i}} C'_{ij}\} \tag{16}$$

则必然 $\exists C_{ij}\neq C'_{ij}$ (17)

即不同的自然免疫系统 Σ_{NIS} 所包含的免疫细胞集合是不完全相同的，所以每个个体所能防御的病原体种类也不同，这总体提高了种群的免疫能力，因为同一种病毒不能对所有个体起作用。

3.1.4 阴性选择

所谓阴性选择(negative selection)是指在胸腺中遍布着人体的自身细胞，只有在一段时间内与这些细胞不发生反应的 T 淋巴细胞才能发育成熟，而那些与自身细胞发生反应的 T 淋巴细胞会发生程序死亡而没有机会成熟[2,3]。成熟的 T 淋巴细胞离开产生它的特定区域进入循环系统和淋巴系统。自然免疫系统 Σ_{NIS} 的自适应免疫系统主要通过阴性选择获得对自身的隐含描述，采用一种异常检测的方法检测病原体，从而使得自然免疫系统 Σ_{NIS} 能够检测到它以前从未见过的新的病原体。

正是由于自然免疫系统多层次性、多样性、独特性以及阴性选择机理才使它能够可靠检测多如牛毛的各种病原体，具有很高检测率。

3.2 动态防护性

自然免疫系统 Σ_{NIS} 可以利用相对比较少的资源来完成复杂的检测任务。人体大约有 10^8 个淋巴检测器，但有约 10^{16} 种病原体要识别，自然免疫系统采用的方法是动态防护[3]，在任一时刻，体内的淋巴检测器只能检测病原体的一个子集，但淋巴检测器每天都会更新，所以每天检测的病原体子集不同，大约每 10 天左右淋巴细胞会全部更换一次，以适应当前的待检物质。动态防护性实际上是以一定的时间作为代价来换取一定的空间。

3.3 健壮性

自然免疫系统采用了高度分布式的体系结构，大量自治的淋巴细胞随血液和淋巴系统在体内循环，遍布全身，少量淋巴细胞的失效甚至死亡都不会对整个系统造成致命的影响，所以自然免疫系统具有很强的健壮性。

3.4 自适应性

自然免疫系统 Σ_{NIS} 具有良好的自适应性，这主要体现在初次响应阶段中 B 淋巴细胞的克隆选择(clone selection)过程[3]，克隆选择过程使得与当前抗原亲合度高的 B 淋巴细胞不断被克隆增生，且通过超变异产生具有更高亲合度的新的 B 淋巴细胞，并消除与抗原亲合度低于某个阈值的 B 淋巴细胞，从而使得整个 B 淋巴细胞集合更加适合当前的病原体。自然免疫系统 Σ_{NIS} 有两种响应方式，分别叫做初次响应和二次响应，由于记忆细胞的存在，当自然免疫系统再次遇到类似抗原时，会产生潜伏期缩短而强度提高的二次响应[3,4]。

4 基于免疫机理的入侵检测系统的设计

基于自然免疫系统的工作机理，我们建立一个基于免疫机理的入侵检测系统 Σ_{AIIDS}

$$\Sigma_{AIIDS}=(X_{AIIDS},\Omega_{AIIDS},Y_{AIIDS},G_{AIIDS}) \tag{18}$$

其体系架构如图 1 所示，包括 4 个子系统：基于免疫机理的主机入侵检测子系统、基于免疫机理的网络入侵检测子系统、基于免疫机理的网络节点入侵检测子系统和控制台[5]。

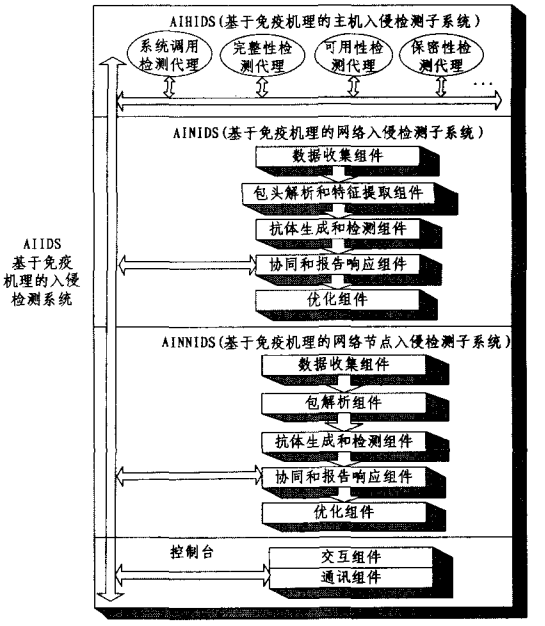

图 1 基于免疫机理的入侵检测系统的体系架构

4.1 检测性能

首先从防护层次的角度，Ω_{AIIDS} 包括多层防护，即

$$\Omega_{AIIDS}=\{L_a,L_b,L_c\} \tag{19}$$

L_a 主要检测网络包层：检测以太网中同一冲突域的所有进出的网络通讯数据包的包头，及时发现畸形的数据包头、网络流量的异常以及已知的各种攻击特征。

L_b 主要检测网络应用层：检测进出网络节点处的网络通讯数据包。对数据包进行与主机操作系统协议栈完全一致的解码和分析。根据数据包端口的不同调用不同的代理，检测

各种基于应用层的攻击。

L_c 主要检测主机层：根据操作系统的审计日志完成对网络系统的关键主机的检测。检测内容包括特权进程的系统调用轨迹、CPU 使用峰值、可用内存量和磁盘空间量、关键文件的改变以及登录事件异常等等。

从具体的检测代理的角度来看，Ω_{AIIDS} 包括多个代理，即

$$\Omega_{AIIDS}=\left\{\bigcup_{\substack{i=1\sim m\\ j=1\sim k_i}} a_{ij},\ \begin{array}{l}\text{其中 } m \text{ 检测代理种类的个数，}\\ k_i \text{ 为第 } i \text{ 种检测代理的个数}\end{array}\right\} \tag{20}$$

检测代理包括很多种类如系统调用检测代理、完整性检测代理、可用性检测代理、HTTP 检测代理、FTP 检测代理等等，分别检测不同的特征，每一种代理都有若干个，分布到网络的不同位置。各个代理既能够独立地完成各自的检测任务，又能够通过少量的通讯进行一定程度的合作。

$$\text{且对于 } \Omega_{AIIDS}=\{\bigcup_{\substack{i=1\sim m\\ j=1\sim k_i}} a_{ij}\}\neq\Omega_{AIIDS}'=\{\bigcup_{\substack{i=1\sim m\\ j=1\sim k_i}} a_{ij}'\} \tag{21}$$

$$\text{则必然 } \exists a_{ij}\neq a'_{ij} \tag{22}$$

即对于不同的 Ω_{AIIDS}，它所包括的检测代理集合不会完全相同。而且各种检测代理进行检测时常常采用基于规则的检测方法，规则可以从学习中得到。因此经过一段时间，即使是同一种类型的检测代理，若所处的位置不同，则其所利用的规则集合就不会完全相同，使得同一种类型的检测代理具有不同的检测性能。因此基于免疫机理的入侵检测系统 Σ_{AIIDS} 具有系统意义和代理意义两种层次的独特性，使得不同节点的代理或不同的系统能够检测到的入侵是不相同的。这种独特性从整体上增加了网络系统的抗攻击能力。目前许多站点运行着相同的软件，并有着类似的防护系统。一旦一个弱点被发现，所有这些站点都可能会被成功入侵。但若具有 AIIDS 所具有的独特性，就能够大大减少某一种攻击对一大批系统所构成的威胁。

同时基于免疫机理的入侵检测系统广泛采用异常检测技术，从而能够检测到新型的攻击。但是异常检测技术常常会因“自身轮廓”不完备等原因引起高的虚警，自然免疫系统 Σ_{NIS} 如何克服自免疫的发生呢？自免疫的克服主要依赖一种叫做 T 协助细胞的 T 淋巴细胞（T help cells）提供的协同信号（costimulation），从而使得自免疫疾病非常罕见[4]。

类比自然免疫系统 Σ_{NIS} 的协同信号机理，基于免疫机理的入侵检测系统 Σ_{AIIDS} 为了降低虚警，也引入了协同信号。考虑到入侵是指任何试图危害资源的保密性、完整性、可用性的活动集合，所以 Σ_{AIIDS} 将提供给检测器一个说明系统可能受损（从保密性、完整性、可用性等几个方面来描述系统可能受损的情况）的信号作为协同信号。只有当 L_a 或 L_b 产生异常怀疑，并同时收到来自 L_c 的协同信号时，Σ_{AIIDS} 才报警。

结论 1 由于 Σ_{AIIDS} 采用了多层次防护和协同机制，因此 Σ_{AIIDS} 具有比只采用单层防护且不采用协同信号的传统入侵检测系统有更好的检测性能。

具体证明如下：

因为 Σ_{AIIDS} 的 $\Omega_{AIIDS}=\{L_a,L_b,L_c\}$，对于不同防护层次有：

$R_{TD}(L_v)=P(Y_{L_v}=1/X_{AIIDS}\in I)$ 其中 $v\in\{a,b,c\}$

$R_{FD}(L_v)=P(Y_{L_v}=1/X_{AIIDS}\in\neg I_v)$ 其中 $v\in\{a,b,c\}$

因为各个层次在检测入侵时并联互补

$R_{TD}(\Sigma_{AIIDS})=P(Y_{AIIDS}=1/X_{AIIDS}\in I)=P(\{Y_{L_a}=1\}\cup\{Y_{L_b}=1\}\cup\{Y_{L_c}=1\}/X_{AIIDS}\in I)$ 且 $\{Y_{L_v}=1\}\subset(\{Y_{L_a}=1\}\cup\{Y_{L_b}=1\}\cup\{Y_{L_c}=1\})$，其中 $v\in\{a,b,c\}$

所以 $R_{TD}(\Sigma_{AIIDS})>R_{TD}(L_v)$ 其中 $v\in\{a,b,c\}$

因为不同层次在检测入侵时进行彼此协同，只有当 L_a 或 L_b 产生异常怀疑，并同时收到来自 L_c 的协同信号时，Σ_{AIIDS} 才报警。

$R_{FD}(\Sigma_{AIIDS})=P(Y_{AIIDS}=1/X_{AIIDS}\in\neg I)=P(\{Y_{L_a}=1\}\cap\{Y_{L_c}=1\}/X_{AIIDS}\in I)$

或者 $R_{FD}(\Sigma_{AIIDS})=P(Y_{AIIDS}=1/X_{AIIDS}\in\neg I)=P(\{Y_{L_b}=1\}\cap\{Y_{L_c}=1\}/X_{AIIDS}\in I)$

且 $(\{Y_{L_a}=1\}\cap\{(Y_{L_c}=1)\})\subset\{Y_{L_o}=1\}$

其中 $o\in\{a,c\}$

$(\{Y_{L_b}=1\}\cap\{(Y_{L_c}=1)\})\subset\{Y_{L_w}=1\}$

其中 $w\in\{b,c\}$

所以 $R_{FD}(\Sigma_{AIIDS})<R_{FD}(L_v)$

其中 $v\in\{a,b,c\}$

所以 $DA(\Sigma_{AIIDS})=\omega_{MD}\cdot(1-R_{TD}(\Sigma_{AIIDS}))+\omega_{FD}\cdot R_{FD}(\Sigma_{AIIDS})<\omega_{MD}\cdot(1-R_{TD}(L_v))+\omega_{FD}\cdot R_{FD}(L_v)=DA(\Sigma_{L_v})$

其中 $v\in\{a,b,c\}$

证毕。

4.2 动态防护性

在 Σ_{AIIDS} 中某一时刻只包括能够检测所有入侵的一个子集的必要的检测代理或规则集合，但该检测代理或规则集合能随时间动态变化，在一段时间范围 T 内可以完成对所有可能的入侵的检测，时间范围 T 和每个时刻激活的代理或规则数目可以根据具体的检测情况进行调节，这使得用户可以根据自己的需要在检测性能和资源消耗之间进行折中。具体体现在基于免疫机理的主机入侵检测子系统 AIHIDS 中，为了减少资源消耗，该子系统在正常工作时，设置所包含的代理异步串行工作，即每个代理工作一段时间后暂时停止工作并激活下一个代理开始检测，经过一段时间，所有代理全部激活一次，以得到检测的完备性。而在基于免疫机理的网络入侵检测子系统 AINIDS 以及基于免疫机理的网络节点入侵检测子系统 AINNIDS 中，都具有两个记忆规则库，即当前记忆规则库和不常用记忆规则库，在检测时以更低的频率匹配不常用记忆规则库以节省检测所需要的资源和时间。

4.3 健壮性

基于免疫机理的入侵检测系统 Σ_{AIIDS} 包含多个子系统和大量遍布整个系统的轻型有效的自治检测代理，每个子系统或每个检测代理本身仅能检测某一类或某几类入侵，多个子系统或大量检测器的集合能以很高的概率检测到绝大多数入侵，若少量几个代理失效则仅使几种攻击的检测能力受到影响，而不会使得整个系统的检测能力显著下降。具体到 AIIDS 中包括大量多种代理如系统调用检测代理、可用性检测代理、HTTP 检测代理、FTP 检测代理等等，各个代理能够独立地检测某一类入侵，并且各代理的检测能力之间具有一定的冗余。若某个节点的某个检测代理如 HTTP 检测代理突然失效，只有针对某个节点的 HTTP 协议的一类攻击无法检测到，而对于其它攻击如针对该节点的 FTP 协议的攻击的检测将不会受到影响，对于针对其它节点的 HTTP 攻击的检测

（下转第 84 页）

由于 $f(x)$ 是 t-弹性函数，则 $F(f)=0$，因此 $\Lambda<2^{n-k}-1$，也就是，$\Lambda\leqslant 2^{n-k}-2$。所以存在满足 $2^{2n-2(t+2+\varepsilon)}=\sum_{j=1}^{c}\lambda_i j^2\leqslant\Lambda i^2\leqslant i^2(2^{n-k}-2)$ 的整数 i。

因此，可以定义 l 为满足 $2^{2n-2(t+2+\varepsilon)}\leqslant i^2(2^{n-k}-2)$ 的最小 i。这时能保证对某个 $\alpha\in U_f$ 使得 $|F(f+\varphi_\alpha)|\geqslant l2^{t+2+\varepsilon}$。所以就证明了沃什谱的绝对值最小值为 $l2^{t+2+\varepsilon}$，等价于，$N_f\leqslant 2^{n-1}-l\cdot 2^{t+2+\varepsilon}$。

2)利用 1)的方法就能得到 2)的结果。

结束语 文中得到了具有线性结构的布尔函数的一些性质。找到了此类函数的一个事实：若 V 是布尔函数的线性结构，则 $f(x)$ 的沃什谱值在 $F_2^n\backslash V^\perp$ 或者 $V^\perp$ 上为零。同时得到布尔函数没有 $k(k\geqslant 0)$ 线性结构的充分条件，最后给出了具有线性结构的弹性函数的非线性度的新上界。这些结果将为以后设计性质良好的弹性函数提供依据。

参 考 文 献

[1] Yan Matsui M. Linear cryptanalysis method for DES cipher[C] // Advances in Cryptology-Eurocrypt'93, LNCS. 1994, 765: 386-397

[2] Siegenthaler T. Decrypting a class of stream ciphers using ciphertexts only[J]. IEEE Transactions on Computers, 1985, 34 (1): 81-85

[3] Sarkar P, Maitra M. Nonlinearity bounds and constructions of resilient Boolean functions[C] // Advances in cryptology Eurocrypt'2000, LNCS. Springer-Verlag, 2000, 1809: 515-532

[4] Charpin P, Pasalic E. On propagation characteristics of resilient functions[C] // Advances in Cryptology-SAC' 2002, LNCS. Springer-Verlag, 2003, 2595: 175-195

[5] Canteaut A, Carlet C, Charpin P, et al. On cryptographic properties of the cosets of R(1, m)[J]. IEEE Transactions on Information Theory, 2001, 47: 1494-1513

[6] Pasalic E. Maiorana - McFarland class : degree optimization and algebraic properties[J]. IEEE Transactions on Information Theory, 2006, 52(10): 4581-4594

[7] Charpin P, Psaslic E. Highly nonlinear resilient functions th - rough disjoint codes in projective spaces[J]. Designs, Codes and Cryptology, 2005, 37(2): 319-346

[8] Xiao Guozhen, Massey J L. A spectral characterization of correlation immune combining function[J]. IEEE Transactions on Information Theory, 1988, 34(5): 569-571

[9] Tarannikov Y. On resilient Boolean functions with maximal possible nonlinearity[C] // Proceedings of Indocrypt 2000, LNCS. Spring- Verlag, 2000, 1977: 19-30

[10] Carlet C. On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions[C] // Sequences and their Applications-SETA 2001(Discrete Mathematics and Theoretical Compute Science). Berlin: Springer-Verlag, 2001: 131-144

[11] 温巧燕，钮心忻，杨义先. 现代密码学中的布尔函数[M]. 北京：科学出版社，2000: 13-14

(上接第 81 页)

也不会受到影响。而且由于有些针对 HTTP 的攻击会导致系统的可用性严重偏离系统正常使用时的状态，很可能会被其它代理如可用性检测代理检测到，所以在少量检测代理失效时，增加的漏警率会很小，即：$\omega_{MD}R_{MD}(\breve{\Sigma}_{AIIDS})-\omega_{MD}R_{MD}(\breve{\Sigma}_{AIIDS})$ 很小；而当少量检测代理失效时，由它们所引起的虚警会消失，同时它们产生的抑制虚警的能力也会消失，两种作用相抵消，使得增加的虚警率比较小，即：$\omega_{FD}R_{FD}(\breve{\Sigma}_{AIIDS})-\omega_{FD}R_{FD}(\Sigma_{AIIDS})$ 比较小，因此能够满足：

$$\frac{DA(\breve{\Sigma}_{AIIDS})-DA(\Sigma_{AIIDS})}{DA(\Sigma_{AIIDS})}$$

$$=\frac{\omega_{MD}R_{MD}(\breve{\Sigma}_{AIIDS})+\omega_{FD}R_{FD}(\breve{\Sigma}_{AIIDS})-\omega_{MD}R_{MD}(\Sigma_{AIIDS})-\omega_{FD}R_{FD}(\Sigma_{AIIDS})}{\omega_{MD}R_{MD}(\Sigma_{AIIDS})+\omega_{FD}R_{FD}(\Sigma_{AIIDS})}\leqslant\Gamma$$

所以 Σ_{AIIDS} 具有健壮性。

4.4 自适应性

基于自然免疫系统克隆选择的启发，在 Σ_{AIIDS} 利用规则优化组件使得检测器的规则集合能够根据当前的入侵自动调节，经常能够检测到攻击的规则具有更高的适应度，而在一定时间范围内，很少或根本没有检测到入侵的规则具有更低的适应度，最终将会被移出常用规则库，这样就会使得当前规则库中的规则能够更好地适应它所经常遇到的攻击。基于免疫机理的入侵检测系统 Σ_{AIIDS} 大量采用异常检测方法检测攻击，而规则优化组件对通过异常检测检测到的攻击能够提取其特征形成新的滥用检测规则，从而当这些入侵再次出现时能够直接通过规则匹配来检测到。由于优化组件提取已知入侵的特征形成新的滥用检测规则，当相同入侵再次出现时，Σ_{AIIDS} 能够直接通过滥用检测规则检测到，从而减少了异常检测所需的时间和资源，因此满足入侵检测系统的自适应性的第二和第三个条件。由于经过一段时间，规则库中的规则都是具有较高适应度的，使得此时的检测系统比原系统有更强的检测能力，因此满足入侵检测系统的自适应性的第一个条件。因此可以得出 Σ_{AIIDS} 具有自适应性的结论。

结束语 本文用四元组定义了自然免疫系统和入侵检测系统的数学模型，并给出了入侵检测系统检测性能、健壮性、自适应性以及动态防护性等概念的数学描述，基于自然免疫系统的多层次性、多样性、独特性、协同性、动态性、分布性和克隆选择等机理提出基于免疫机理的入侵检测系统 AIIDS 的总体设计。我们已经根据该设计用 c 语言实现了 AIIDS 的原型，并对一些标准入侵检测数据以及自己收集到的数据进行了实验，实验结果[5]证实了 AIIDS 检测的有效性。

参 考 文 献

[1] Axelsson S. The Base-Rate Fallacy and the Difficulty of Intrusion Detection[J]. ACM Transactions on Information and System Security, 2000, 3(3): 186-205

[2] Hofmeyr S A. An Interpretative Introduction to the Immune System[M] // I. Cohen, L. Segel, eds. Design Principles for the Immune System and other Distributed Autonomous Systems. Oxford University Press, 2000

[3] Forrest S, Hofmeyr S, Somayaji A. Computer Immunology[J]. Communications of the ACM, 1997, 40(10): 88-96

[4] Hofmeyr S A. A Immunological Model of Distributed Detection and its Application to Computer Security[D]. Department of Computer Sciences, University of New Mexico, Albuquerque, NM, April 1999.

[5] 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, 28(10): 1601-1607