一种基于免疫学的园区网入侵检测模型

孙美凤　龚俭
(msun、jgong)@njnet.edu.cn

Abstract： 现有的基于网络的入侵检测系统在许多方面有缺陷，其中的两个主要问题是高误报率和缺乏自适应性。在各种基于免疫学的入侵检测模型中，Hofmeyr 提出的自适应免疫系统模型具有显著特性：分布性、自组织性、轻量级，但不能直接应用于园区网。本文首先简单介绍了 Hofmeyr 的自适应免疫系统模型，然后分析了园区网的流量特征，描述了一个可用于园区网的入侵检测系统模型。新的模型保留了 Hofmeyr 模型的优点，并具有更强的能力，可望为园区网提供全局性的检测和保护。
Keywords：入侵检测、人体免疫系统，检测器

An Immunity-Based Model for Intrusion Detection Applicable on Intranet

Sun Meifeng　　Gong jian
(msun、jgong)@njnet.edu.cn

Abstract : Existing network-based Intrusion detection System have drawbacks in many aspects, among of which the two outstanding problems are high radio of false alarms and the lack of self-adaptation. The Adaptive Immune System Model offered by Hofmeyr had salient features compared with variants of immunology-based network intrusion system, which are distributed、self-organization、lightweight. In this paper, Hofmeyr's model was introduced briefly fistly, then the features of Intranet traffic were analized. Based on these, a new model was proposed. This new model can be expected to detect and to protect the overall Intranet from attacts with the advantages of Hofmeyr's Model.
Keywords: intrusion detection、the human immune system、detector

1 背景

基于网络的入侵检测系统（NIDS）与基于主机的入侵检测系统（HIDS）相比，具有许多特点：较低的造价、能够检测 HIDS 不可检测的活动、入侵者很难销毁证据、实时的检测和响应、可以检测到未成功的入侵活动和恶意的攻击企图、独立于操作系统。正因为 NIDS 具备上述 HIDS 不可比拟的优点，IDS 的研究热点正逐溅转向 NIDS[1]。

因为网络行为很难把握，现有的 NIDS 都采用了 Denning 提出的滥用检测模型。NIDS 的体系通常由数据采集、分析、管理三个层次组成，数据采集层抓取网络报文，分析层基于知识进行决策推理，并将结果报送管理层，管理层在安全管理员的参与下作出响应[2]。该模型在许多方面有缺陷，其中的两个主要问题是高误报率和缺乏自适应性。巨大的网络流量，限制了规则的复杂性和精确性，从而导致高误报率。高误报率占用了管理员的大量时间，消耗大量的系统资源，甚至导致灾难的自动响应后果。缺乏自适应性意味着 IDS 不能自动检测新出现的攻击或已知攻击的变种，从而要求系统构造者调整或修改检测规则，这样的工作浪费了大量的时间。新的攻击不断出现，缺乏自适应正成为 NIDS 的严重问题[3]。

Kim 和 Bently[4]研究了基于网络的入侵检测系统的基本要求，并得出结论：一个有效的 NIDS 应满足三大设计目标：分布性、自组织、轻量级。人体免疫系统通过否定选择、克隆选择、自学习等机制很好的满足了上述目标，吸引了计算机安全领域研究者的关注。在 NIDS 方面，[5]给出的基于免疫学的 NIDS 的模型强调三个进化过程（基因库进化、否定选择、和克隆选择）的有机集合，但缺少 self 集的定义和基因（攻击规则）的有效表达方法。

[6]给出了基于免疫学的各种计算机安全体系，这些体系都仅仅建立了人体免疫系统与计算机安全系统的映射关系。[7、8]中 Hofmeyr 提出了一个通用的自适应免疫系统模型，该模型满足 Kim 和 Bently 提出的 NIDS 设计目标，但不能直接应用于园区网。

Internet 连接着数以百万计的园区网，为园区网提供有效的检测措施是整个 Internet 入侵检测的基础。

本文在简单介绍了 Hofmeyr 模型之后，针对园区网的流量特征提出对该模型的改进，新的模型保留了 Hofmeyr 模型的优点，具有更强的能力，可望为园区网提供全局的检测和保护。

本文的第 2 部分介绍了 Hofmeyr 模型并分析了它的特性；第 3 部分分析了园区网的流量特征，建议了一种新的 NIDS 模型；最后是结束语。

2 Hofmeyr 的 AIS 模型

Hofmeyr 在引文[7、8]中给出了一个通用 AIS 模型，该模型定义问题域是长度为 L 的二进制串全集。U 被分成两个不相交的子集 S（self）、N（non-self）。检测器是同样长度的二进制串。因此检测问题是：对任意的 u∈U，判定 u∈S 或∈N。

2.1 检测器的生命周期

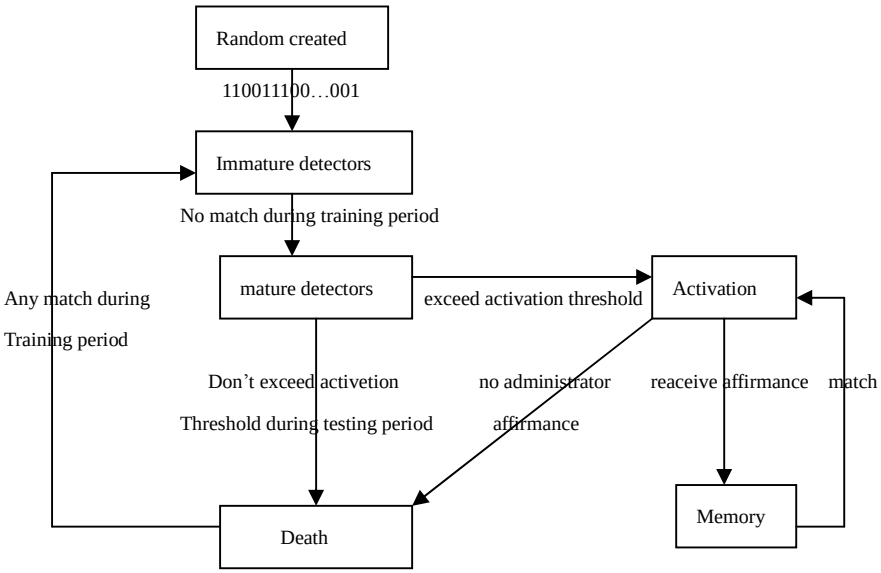

图 1 检测器的生命周器

人体免疫系统具有检测和响应功能。响应过程非常复杂，现有的理论和实验都没能够揭示人体免疫系统的响应机理。Hofmeyr 的 AIS 模型只模拟了人体免疫系统的检测能力，模型中的检测器综合了各类免疫细胞和分子的功能，具有新生、成熟、激活三种状态。首先，AIS 随机生成检测器，新生态的检测器可能匹配 self 集出现误报（在人体中会引起自体免疫系统紊乱），因此新生态检测器必须经过培训才能进入成熟态。培训是一个否定选择的过程，在此期间新生检测器大量接触 self 集，与 self 集匹配的检测器被视为无用而删除，否则成长为成熟的检测器。

成熟检测器有两种类型：通用型和记忆型。通用性检测器有较短的生命期，在存活期间如匹配足够次数（阀值）的异常，则进入激活态，否则死亡。类似于淋巴细胞，激活后的检

测器需等待确认（人体免疫系统称其为 comestication，进一步防止了误报），得到确认的激活检测器转化为记忆型检测器（人体免疫系统将进入克隆过程，大量杀死外来有害抗原，同时学习抗原特征转化为记忆型淋巴细胞）。记忆型检测器有较低的阀值和较长的生命期，能够迅速检测曾经见过的异常。检测器的生命周期如图 1 所示。

2.2 不完备的 self 集

模型中检测器自学习 self 信息。自学习得到的 self 集具有不完备性，存在两种可能影响检测结果：（1） self 集是不完全的，使得一个与 self 串匹配的检测器生存下来，从而将正常误报为异常。对此，模型规定了一个激活阀值，仅当检测器匹配阀值以上的异常时才被激活，并且激活以后还需要等待后台系统的确认，Hofmeyr 模型的后台系统指安全管理员，他对正常和异常有更深刻的理解。得到确认的检测器转化为记忆型检测器，否则被删除。激活阀值和后台确认大大降低了误报的可能性。（2）self 集包含躁声。躁声使得异常检测器被视为正常，从而不能通过否定选择。然而对一个现实的系统，我们总能假定：异常出现的概率远远小于正常出现的概率，异常最终总能够被检测到。

2．3　Hofmeyr 模型在入侵检测领域的应用

Hofmeyr 的 AIS 模型是通用模型，具有分布性、自组织性和轻量级的特点，满足 Kim 和 Bendly 提出的 NIDS 模型的三大要求[7,8]。该模型可方便的映射到基于网络的入侵检测领域。定义问题域是网络所有的 TCP/IP 连接，Self 是正常连接，nonself 是恶意的异常连接。每个连接可用原地址、目的地址、端口号和协议类型表示，并可方便地映射成唯一的二进制串。检测器是同样长度的二进制串，并使用近似匹配规则识别 nonself。

3 基于免疫学的园区网 NIDS 模型

3.1 园区网的流量行为特征[1]

如图 2 所示，一个典型的园区网由若干部门子网互连而成。部门子网通常具有相同的物理结构，包括若干服务器/工作站，支持部门内部业务，同时子网内也许配有 web、email 等服务器，用于内外的交流。园区网通常包括一个公共服务子网，配置 web、ftp、email、proxy 等服务器，代表整个园区与外界联系。

园区网的物理结构及其应用背景决定了园区网流量行为具有局部性，不同的部门子网因为其用户流量行为的不同，呈现不同的总体流量行为特征。考察单一的部门子网流量，它包括内部流量（子网内部两台计算机的交互）和进出流量。内部流量具有相对的稳定性，可用（源地址、目的地址、端口号）表示。进出流量是各种 ftp、Web、email 流量，这些流量具有不确定的源和目的地，显然不能用内部流量同样的方法刻画正常和异常。过滤掉出流量（从不确定的源到不确定的目的地，且我们更关心别人对我们发起的攻击），正常的入流量应是到达子网对外提供服务的主机和端口，可用（目的地址，端口号）表示。

综上所述，园区网流量的特点：（1）各子网的流量行为是不同的；（2）各子网的流量包含两类：内部流量和入流量，其行为特征需要不同的表示方法。

[1] 注：本文建议的模型检测网络 TCP/IP 连接。因为习惯性，第 3 部分统称其为流量，实为连接。

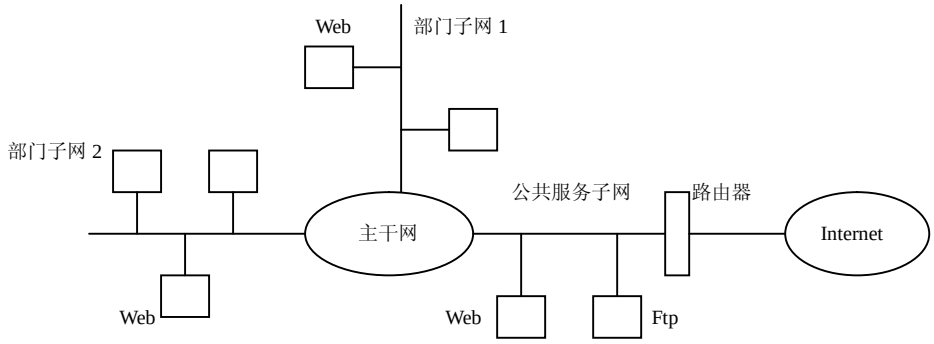

图 2 园区网的物理结构

3．2 园区网的 NIDS 模型

由于园区网流量行为的特征，单一的 Hofmeyr 模型显然不适合。我们不能完全模拟人体免疫系统在一个点（骨髓和胸腺）生成和培训检测器集，因为任何子网的流量行为特征不能代表其它子网，所以园区网 NIDS 模型要求在每个子网配置一个或多个检测代理，代理的数量是代价和性能的均衡。每个检测代理就是一个完整的 Hofmeyr 的 AIS 系统，与其中的检测器在概念上是不等同的。

Hofmeyr 模型中若干检测器在表示形式和工作方式上是一致的。而正如 2.1 中的分析，园区网的每个子网至少需要两种类型的检测器，分别检测内部流量的异常和入流量的异常。因为使用（目的地址、端口号）定义的入流量具有稳定和少量的正常模式，我们采取与人体免疫系统相反的培训和检测方法，在培训阶段检测到的流量生成成熟的检测器，在检测阶段与所有成熟检测器不匹配的流量视为异常，在正常模式很少的情况下，具有更高的效率。因此园区网模型中检测器的不同类型既是不同的表示，也是不同的匹配规则。

观察人体免疫系统，淋巴细胞的生成并非完全随机，而是在骨髓和胸腺的基因库的参与下生成的，基因库是人体免疫系统有效性的基础，促使淋巴细胞向着有效检测抗原的方向进化。为此，园区网 NIDS 模型引入基因库的功能，它是有效的检测规则的集合，决定了各子网检测代理的工作方式。当前系统只使用了两条检测规则分别用于内部流量和入流量异常地检测。

综上所述，园区网的 NIDS 模型包括两部分：主系统和检测代理。主系统是一个安全管理员参与的专家系统，它维护包括网络拓扑、服务器分布、检测代理分布、攻击事实信息的网络事实库，在此基础上完成两部分功能：生成基因库并发布、负责异常确认。检测代理的工作过程如 Hofmeyr 的 AIS 模型。

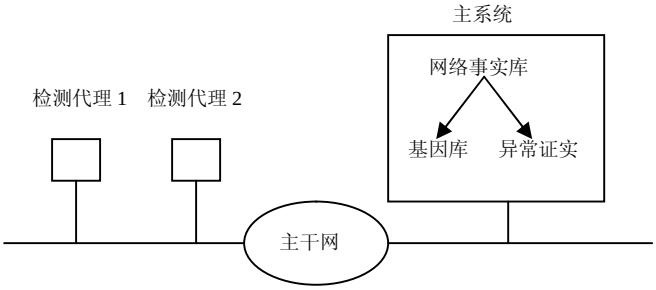

图 3 园区网 NIDS 模型

3．3 园区网 NIDS 模型分析

模型由主系统和若干分布的检测代理组成。每个检测代理都按照 Hofmeyr 模型的方式独立工作，因此园区网的 NIDS 模型继承了 Hofmeyr 模型的分布性、自组织性和轻量级的优点；模型引入了基因库的功能，允许多种类型的检测器存在，具有更好的扩展性和更强大的检测能力；同时主系统是在全面分析网络事实的基础上生成基因库并负责异常证实，使得系统决策更全面和科学，而网络事实库包含的信息不需要经常变更，不会带来维护的负担。

4 结束语

本文在 Hofmeyr 通用 AIS 模型的基础上，建议了一种可用于园区网的 NIDS 模型。该模型能够检测用 TCP/IP 连接头刻画的攻击，例如扫描攻击（在一定时间内同一源多次试图连接不同的目的地址和端口）和 DOS 攻击（在同一时间内大量的源试图连接相同的目的地）；而对用报文内容刻画的攻击无能为力，例如各种特洛伊木马攻击以报文中具有某个子串为攻击特征。因为大量的攻击以扫描为前奏，所以该模型可望对园区网提供强有力的保护，同时又能够克服现有的 NIDS 系统的高误报率和缺乏自适应性的缺点。

参考文献

[1]陈鹏、吕卫峰等，“基于网络的入侵检测方法研究”，*计算机工程与应用*，2001

[2]龚俭、董庆、陆晟，“面向入侵检测的网络安全检测模型”，*小型微型计算机系统*，2001

[3]Zhang Yanchao. Et al.,”An Immunity-Based Model for Network Intrusion Detection” **, *2001 International Conferences* on , vol.5 ,Page(s): 24 –29,2001.**

[4]J.Kim, P.Bently,“The Human Immune System and Network Intrusion Detection” ，*7th European Conference on Intelligent Techniques and Soft Computing(EUFIT’99)*，Aachen Germany,1999.

[5]J.Kim,P.Bently，“An Articial Immune Model for Network Intrusion Detection”，*7th European Conference on Intelligent Techniques and soft Computing(EUFIT’99)*,Aachen,Germany,1999.

[6]Somayaji,A. Et al,“Principles of a Computer Immune System”,*Proceeding of New Security Paradigms Workshop*,Langdale,Cumbria,Page(s)：75-82,1997.

[7]S.Hofmeyr,S.Forrest, “Architecture for an Artificial Immune System”,*Evolutionary Computation*,vol.7,No.1,Page(s)：45-68,2000.

[8]S.Hofmeyr,S.Forrest,“Immunity by Design: An Artificial Immune System”, *Proc. of GECCO'99*, 1289-1296,1999.