异常入侵检测系统虚警率问题研究

柴争义[1,2] 汪宏海[3]

(河南工业大学信息科学与工程学院 郑州 450001)[1] (西安电子科技大学计算机学院 西安 710071)[2]

(赣南教育学院计算机系 赣州 341000)[3]

摘 要 入侵检测系统的虚警率影响检测结果的可信性。通过分析入侵检测系统的可信问题及异常入侵检测系统的虚警率问题,提出了降低虚警率的方法:基于进程检测行为的入侵检测方法、多检测系统协作工作模式。重点描述了基于人工免疫思想,动态构建正常系统轮廓,抑制虚警率的方法,并对其进行了仿真实验。实验表明,本方法可以提高检测效率,有效降低系统虚警率。

关键词 异常入侵检测,虚警率,人工免疫,进程行为

中图法分类号 TP393.08 **文献标识码** A

Study of Anomaly Intrusion Detection System on False Positive Rate

CHAI Zheng-yi[1,2] WANG Hong-hai[3]

(School of Information Science and Engineering, Hennan University of Technology, Zhengzhou 450001, China)[1]

(School of Computer, Xidian University, Xian 710071, China)[2]

(School of Computer Science, Gannan Institute of Education, Ganzhou 341000)[3]

Abstract False positive rate of intrusion detection systems (IDS) affect the detection creditability. Methods to reduce the false positive rate were presented after analyzing creditability of IDS and false positive rate of anomaly IDS. It put methods include the followings: method based on process detection, multi-detection system model. It put emphasis on constructing normal profile dynamically based on artificial immunity to restrain false positive rate, then simulation experiment was done. The results show that the method can improve the detection efficiency and reduce the false positive rate.

Keywords Anomaly intrusion detection, False positive rate, Artificial immunity, Process behaviors

1 引言

目前,入侵检测系统(IDS)正在网络安全防护中发挥着越来越重要的作用,但其检测结果的可信性一直是一个严峻的问题,其中存在的一个主要问题是虚警率。虚警是指把系统的正常行为误判为入侵行为进行报警,入侵检测系统在检测过程中出现虚警的概率即为虚警率。过多的虚警必然造成检测结果的不可信,所以必须尽可能降低系统虚警率,提高检测的可信性。

2 入侵检测系统的可信问题

入侵检测问题可视为一个简单的二值假设检验问题。为便于分析,我们采用数学语言来描述,先给出一系列相关的定义和符号。假设 I 与 $\bar{I}$ 分别表示对目标系统的入侵行为和目标系统的正常行为;A 代表检测系统发出了入侵报警,$\bar{A}$ 表示检测系统没有报警。检测率指受到入侵攻击时检测系统能够正确报警的概率,可表示为 $P(A|I)$。实际使用中,可通过利用已知入侵攻击的实验数据集合来测试入侵检测系统的检测率。虚警率指检测系统在检测时出现虚警的概率 $P(A|\bar{I})$,且有 $P(\bar{A}|I)=1-P(A|I)$,$P(\bar{A}|\bar{I})=1-P(A|\bar{I})$。

对于网络管理员来说,真正关心的是入侵检测系统的可信问题。入侵检测系统的可信度可用两个可信概率来表示:(1)检测系统报警可信概率,由 $P(I|A)$ 给出,即检测系统报警时目标系统实际受到入侵攻击的概率。该参数小于1时,说明检测系统存在虚警现象。(2)检测系统不报警可信概率,由 $P(\bar{A}|\bar{I})$ 给出,即检测系统没有报警时目标系统处于安全状态(没有受到入侵攻击)的概率。该参数小于1时,说明检测系统存在漏警现象。

显然,为了使入侵检测系统更有效,我们希望系统的这两个参数值越大越好。由于入侵检测系统是根据其检测结果,以对入侵行为进行报警的形式通知被监控系统,因此主要关注告警信息的可信度 $P(I/A)$ 与检测系统性能的关系。应用

到稿日期:2008-12-11 返修日期:2009-03-02 本文受国家自然科学基金(60473021),河南省自然科学基金项目(082400440260,2008A180041)资助。

柴争义(1976-),男,博士生,主要研究方向为网络安全、智能计算,E-mail:super_chai@tom.com;汪宏海(1977-),男,讲师,主要研究方向为网络安全、工作流技术。

贝叶斯定理可以求出入侵检测系统可信度的概率为：

$$P(I/A)=\frac{P(I)P(A/I)}{P(I)P(A/I)+P(\bar{I})P(A/\bar{I})}$$

根据上面的分析，针对给定的实验数据或具体环境，可以通过已经获得的数据统计以及系统仿真获得 $P(I)$，$P(\bar{I})$，$P(A/I)$，$P(A/\bar{I})$的先验概率，进而计算出 $P(I/A)$。在一般情况下，入侵行为出现的概率是非常低的，即 $P(I)\leqslant P(\bar{I})$，并且 $P(I)+P(\bar{I})=1$。所以，在计算 $P(I/A)$式子中，分母主要取决于虚警率 $P(A|\bar{I})$的影响。因此，降低虚警率，可以提高告警信息的可信度。

3 异常入侵检测系统的虚警问题

异常检测系统亦称为基于统计行为的入侵检测系统。其方法为：检测系统首先建立被检系统的正常行为轮廓，当检测系统发现被检系统的行为偏离正常轮廓的范围超出某个阈值时，则认为有入侵发生。异常检测分析方式可以检测到未知的和更为复杂的入侵，但其缺点是虚警率高。实际上，入侵活动与异常行为并非总是联系在一起，活动有 4 种可能性，即①非入侵活动且非异常；②入侵且异常；③入侵而非异常；④非入侵而异常。异常检测系统能够正确处理前两种活动。但对第③种情况，比如在建立正常轮廓时误包含了某种入侵活动，或者某个入侵不会导致异常行为或者导致的异常行为偏离正常轮廓的范围很小，未超出检测阈值时，异常检测系统将会产生漏警。而对于第④种情况，异常检测系统将会产生虚警，该情况主要是检测系统建立的正常行为轮廓不完善，不能涵盖所有正常活动所致。比如在建立正常行为轮廓时未能考虑所有的正常行为，或者正常行为是动态变化的（如用户行为或习惯的改变），而正常轮廓的建立是静止的，不能及时跟上这种变化等。由于降低漏警率和降低虚警率是两个研究内容不同的课题，下面重点研究如何降低虚警率，提高报警可信度。

4 降低异常入侵检测系统虚警率的方法

根据前面所讨论的虚警产生的原因和自然免疫机理的启发，主要采用 3 种方法来抑制虚警率，增加入侵检测系统的可信性。

4.1 使用基于进程行为的入侵检测方法

这里使用的基本思想是进程的正常执行轨迹和异常执行轨迹有着不同的行为模式，并且可以用系统调用的短序列来表征。表示入侵行为的异常事件具有时间上的局部集中性，这为利用系统调用短序列判断进程是否受到入侵提供了依据。

具体实现系统短序列正常与否的识别时，采用贝叶斯分类器。它利用概率统计和机器学习理论对这些系统调用短序列进行处理。它通过计算一个待识别的序列属于哪个类的概率最大来确定它的归属，具有一定的预测性。但是，我们需要知道的是被监控的程序是否遭受了入侵。为此，还必须对系统调用短序列模式分类器的输出结果做进一步的分析判断。

由于分类器的不精确性，对系统调用短序列的分类结果也会偶尔出现错误。为了解决这个问题，可以通过分析某一时间段里异常序列的百分比是否达到给定的阈值，来判断系统进程执行迹是否异常。在程序识别器中，采用反映最近事件状况的“漏桶算法”，对进程分类器的结果做进一步的分析，减少误判的可能。漏桶中的水位反映了入侵行为发生时标为“异常”的系统调用短序列的局部集中性，水位越高，说明最近的一段时间里被监控进程遭受入侵的可能性越大。一个被监控进程如果在执行过程中对应“漏桶”水位计数器的值超过了给定阈值，则认为其不是程序识别器所代表的系统程序在运行，或是程序遭受到了入侵。由于漏桶算法对大量具有时间局部相关性的异常操作的集中出现表现得非常敏感，从而在入侵攻击时能够有效地将这些异常操作检测出来，因此，可以通过调整漏桶水位计数器的阈值以及漏桶中漏水的速率，来控制检测系统的虚警率和检测率。在设计入侵检测系统时，采用漏桶算法强调了异常系统调用短序列在时间上的局部相关性，忽略了分散、偶然的异常子序列的影响，从而有效地对分类的结果进行了综合分析，使得检测系统具有较高的检测性能。

4.2 采用多检测系统协同工作模式（数据融合）降低虚警

由于不同的检测机制从不同的角度考虑入侵检测问题，因此可以采用不同的机制检测系统协同工作的模式。基于异常的检测系统由于数据不完备，从而在检测时必然存在虚警。

对采用相同检测机制的检测系统的协作，设检测系统 A，B 以及二者共同工作时的整体检测率分别为 p_{dA}，p_{dB} 及 p_d，且对应的虚警率分别为 p_{fA}，p_{fB} 及 p_f。我们指定判定规则如下：两个检测器都认为正常时，判定为正常；若只有一个检测器认为正常，则进行报警或做进一步分析；两者都认为是异常时，才确定是异常。一个正常的行为，只有两个检测系统都认为是入侵时才出现虚警，所以针对检测系统，虚警率为 $p_f=p_{fA}\times p_{fB}$，并且 $p_f\leqslant p_{fA}$，$p_f\leqslant p_{fB}$。因此，两个异常检测系统的协作可以有效降低系统的虚警率。

基于不同检测机制的入侵检测系统的协作，设系统 A 为基于系统行为特征轮廓的异常检测系统，B 为基于入侵检测知识的检测系统，N 表示被保护系统的正常行为集合。系统 A 把系统特征集合轮廓集合 A 之外的行为 $\bar{A}$ 都看作是异常行为，而系统 B 把已知入侵知识对应的入侵特征集 B 之外的行为 $\bar{B}$ 都看作是正常行为。协作时，假设检测系统 B 能够检测出所有的已知入侵且具有很低的虚警率，那么对于已知的入侵攻击手段，系统 B 可以用来验证系统 A 的检测结果，以降低 A 的虚警率。两个系统的协作分以下几种情况：(1)当检测系统 A 和 B 同时检测到入侵时（$\bar{A}\cap B$），认为系统受到了入侵。(2)当系统 A 检测到入侵，系统 B 认为正常时，则只是给出警告或进一步分析系统表现的特征。(3)系统 A 认为是正常时，不验证。根据上面的规则，系统 A 在验证模式下工作时，只有集合（$\bar{A}\cap B\cap N$）所表示的系统正常行为可能被误判为入侵行为。而集合（$\bar{A}\cap\bar{B}\cap N$）中的系统正常行为，在 A 系统单独工作时，被误判为入侵行为。但当系统 B 对其检测结果进行验证时，只是把它们判为可疑的行为，不把它们作为入侵情况看待，从而降低了系统 A 的检测虚警率。

4.3 构建能够动态改变的正常系统轮廓

早期的异常检测系统主要是通过收集足够长时间、足够多的正常行为建立正常轮廓，以便能够尽量地涵盖所有的正常行为。通过对历史数据分配不同的权值，近期数据分配较大的权重，早期数据分配较小的权重而实时更新轮廓库，可以使正常轮廓动态地跟随正常行为的改变。

受生物免疫系统可以识别未知入侵和免疫学习的启发，这里通过基于人工免疫的思想建立正常行为轮廓。具体来讲，网络对应生物体，网络中的主机对应生物免疫系统中的淋

巴结，免疫系统中的抗原映射成模型中的网络行为。根据免疫学原理，抗原又被分为自体抗原和非自体抗原，因此把自体抗原映射成正常网络行为(S)，非自体抗原(T)映射成非法网络行为。定义论域 $D=\{0,1\}^l$，把整个系统的网络行为抽象为一个由长度为 l 的二进制字符串组成的集合 U，其中 $S\cup T=U, S\cap T=\phi$。

免疫系统中是通过抗体来识别抗原的。在入侵检测系统中，模拟抗体识别抗原的过程，把正常行为轮廓对应于检测器，检测器即类似于抗体集合，通过检测器来识别外来入侵(抗原)。定义抗原集合 $Ag\subset D$。其中 Ag 表示对网络上传输的 IP 包进行特征提取得到的长度为 L 的二进制字符串(类似免疫系统中的抗原提呈)，包括 IP 地址、端口号、协议类型等网络事务特征。定义免疫抗体细胞集合 B，每个抗体为一个四元组，$B=\{\langle d,p,age,count\rangle \mid d\in D\wedge p\in R\wedge age\in N\wedge count\in N\}$，其中 d 为抗体(长度为 l 的二进制字符串)，p 为抗体浓度(被该抗体捕获到的抗原)，age 为抗体年龄，$count$ 为抗体匹配抗原数目(抗体的累计亲和力)，N 为自然数集合。

检测器最主要的是检测元的生成算法，这里采用否定选择算法。算法简单描述如下：(1)将一段时间 T_S 内局域网上的所有正常连接定义为自身集合 S，作为生成有效检测元的训练集；(2)产生有效检测元集合 B。随机产生候选检测元 $I_b=\{\langle d,age\rangle \mid d\in D, age\in N\}$，将产生的候选检测元与自我集中 S 的模式用公式 $f_{tolerance}(I_b)=I_b-\{d \mid d\in I_b\wedge \exists y\in Self\wedge f_{match}(d,y)=1\}$ 进行匹配试验，其中匹配采用 r 为连续匹配实现，即如果 $\exists i,j(x.d_i=y_i, x.d_{i+1}=y_{i+1},\cdots, x.d_j=y_j, j-i\geqslant r, 0<i<j\leqslant l)$，则 x 和 y 匹配成功。若匹配，则丢弃该候选串；否则该候选检测元就是一个有效的检测元，进入 B 集合。重复此过程，直到产生一定数量的检测元为止。通过否定选择算法实现，避免了将自体识别为非自体的误检行为。这些通过否定选择检测的检测元被称为成熟检测元 T_b。

成熟检测元 T_b 通过亲和力累积实现进化。在生命周期 λ 内，每经过单位时间，成熟抗体的年龄 age 增加 1。如果该检测元与入侵匹配成功，则该成熟检测元匹配抗原数目 $count$ 增加 1。成熟检测元在生命周期内匹配抗原数目达到激活阈值 β，则激活为记忆抗体，如下式所示：

$$T_{active}:=\{x \mid x\in T_{Ab}\wedge x.count\geqslant\beta\wedge x.age\leqslant\lambda\}$$

成熟检测元年龄超过生命周期而匹配抗原数目未达到激活阈值，则被删除，如下式所示：

$$T_{dead}:=\{x \mid x\in T_{Ab}\wedge x.count<\beta\wedge x.age>\lambda\}$$

所以，抗体集合 $B=M_b\cup T_b$，其中 $M_b=\{x \mid x\in B, x.count>\beta\}$ 为记忆免疫抗体集合，β 为匹配阈值，T_b 为成熟免疫抗体集合。成熟抗体激活成为记忆抗体，并进行克隆扩增时，产生大量类似的检测器，以抵御更多抗原的入侵。

综合上面的分析，B 也就是传统入侵检测系统中的正常轮廓。通过延长否定选择时间 α，可以使检测器集合识别更多自身连接。成熟的检测器集合 B 中的检测器具有一定的生命周期，经过一段时间后会死亡或者变成记忆检测器 M_b。同时随机检测器集合不断生成，并接受否定选择，从而使得检测器集合 B 保持动态变化，确保了检测器的多样性。记忆检测器具有更长的生命周期，甚至无限长。记忆检测器总数超过上限后，可以转变为成熟检测器(如使用 LRU 算法来淘汰)。记忆检测器再次匹配抗原(外来入侵行为)后，就会被再次激活并克隆自己，克隆生成的新检测器加入检测器集合。一部分符合条件的记忆检测器还能进行变异，以使系统具有学习进化的能力，能够根据自身集合的变化而作出相应的调整。所以，检测系统的正常轮廓(检测器集合 B)具有多样性，并具有学习、自适应能力，可以识别更多的入侵源，提高检测性能，降低虚警率。

5 系统仿真实验与分析

我们对第三种方法进行了模拟实现。实验在网络安全实验室进行，以单台主机为观察对象，多主机参加了实验。在 Windows 2003 Server 之上搭建 IIS，FTP，DNS 等服务器(用端口号进行区分)，另外有一些扫描软件和攻击软件。取 32 位源、目的 IP 地址、16 位端口以及 16 位协议标志等构成 $L=96$ 的二进制串提呈抗原，检测针对各种网络服务的攻击。采用 r 连续位匹配方法计算亲和力($r=8$)，选取初始自体集合大小为 40。每次从网上捕获 100 个 IP 包，对 IP 包进行预处理，将其变换为检测统处理的抗原格式。模拟对网络进行 syn flood，smurf 等多种攻击，其中所发包中非自体串和自体串的比例为 9:1，也就是说攻击程序所发 10 个包中夹杂一个自体包。系统的虚警率记为 p_f。

在 p_f 值的对比实验中，采取的方法是每 100 个数据包中夹杂 40 个自体，其中 20 个自体为新近定义，即以前这 20 个 IP 包被认为是不正常的网络行为，但现在被认为它们是正常的(比如有 20 个网络端口刚被打开以提供服务)，以观察 p_f 值。由于系统参数对结果影响很大，经过反复地比较实验，最终选定了一组参数：$\beta=40$，$\lambda=7$d，$\alpha=48$h。这组参数组合在保证了较高检测率的前提下，p_f 尽可能地低，可以达到 6.25%左右，且系统表现稳定。

对于传统的异常检测方法，由于正常轮廓集合不能实时调整，因此将这些服务作为异常事件进行了报警。对于采用免疫算法的入侵检测系统，由于自体集合具有学习、自适应能力，经过一段时间的学习后，可以对其进行识别，以大大降低虚警率。

结束语 分析了当前入侵检测系统存在的可信问题以及基于异常检测的入侵系统的虚警率问题。给出了通过基于进程行为的入侵检测和采用多检测系统协同工作的模式降低虚警的方法，重点讨论了使用人工免疫思想，动态构建正常行为轮廓，降低虚警率的方法，并通过实验进行了验证。如何进一步融合各种技术，更好地降低入侵检测系统的报警率，还有待进一步研究。

参 考 文 献

[1] 闫巧，喻建平，谢维信. 入侵检测系统的可信问题[J]. 计算机研究与发展，2003，40(8)：1203-1208

[2] 苏璞睿，冯登国. 基于进程行为的异常检测模型[J]. 电子学报，2006，36(10)：1809-1811

[3] Tinnagonsutibout C，Watanapongse P. A novel approach to process-based intrusion detection system using read sequence finite state automata with inbound byte proler[A]// ICEP2003[C]. 2003

[4] 傅涛，孙文静，孙亚民，等. 基于免疫学原理的混合入侵检测系统的设计与实现[J]. 计算机科学，2008，35(6)：63-66

[5] 杨义先，钮心忻. 入侵检测理论与技术[M]. 北京：高等教育出版社，2006

[6] 李涛. 计算机免疫学[M]. 北京：电子工业出版社，2004