基于 SVDD 的网络安全审计模型研究

罗 隽,潘志松,胡谷雨
(解放军理工大学 指挥自动化学院,江苏 南京 210007)

摘 要:审计是入侵检测的基础,为入侵检测提供必要的分析数据.在传统的网络安全审计与入侵检测系统中,需要由人工来定义攻击特征以发现异常活动.但攻击特征数据难以获取,能够预知的往往只是正常用户正常使用的审计信息.提出并进一步分析了一种基于支持向量描述(SVDD)的安全审计模型,使用正常数据训练分类器,使偏离正常模式的活动都被认为是潜在的入侵.通过国际标准数据集 MIT LPR 的优化处理,只利用少量的训练样本,试验获得了对异常样本 100 %的检测率,而平均虚警率接近为 0.

关键词:网络安全审计;入侵检测;支持向量描述;单类分类器
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-4785(2007)04-0069-05

A network security audit system based on support vector data description algorithm

LUO Jun, PAN Zhi-song, HU Gu-yu
(Institute of Command Automation, PLA University of Science and Technology, Nanjing 210007, China)

Abstract: Security audit, which is the basis of intrusion detection, provides the necessary data for intrusion detection analysis. In traditional security audit and intrusion detection system, the characteristics of an attack need to be defined by experts for the system to be able to successfully identify anomalous activities. Due to the difficulty in predicting attack data, in most cases administrators only get normal sequences of system calls. In this paper, a security audit system based on SVDD algorithm was designed to resolve the one-class problem in anomalous activity detection. All activities deviating from normal patterns were classified as potential intrusions. In experiments using the international standard data set MIT LPR, the one-class classifier achieved a 100 % detection rate and a zero false alarm rate for sequences of system calls based on a small training dataset. The proposed algorithms can be trained for anomalous activity detection simply by using normal samples and the algorithm also enables the security audit system to detect new types of anomalous behavior.

Keywords: network security audit; intrusion detection; support vector data description, one-class classifier

在网络安全体系中,对于 C2 及其以上安全级别的计算机系统来讲,审计功能是其必备的安全机制,是其他安全机制的有力补充,同时,审计还是人们研究入侵检测系统的前提[1].由于审计跟踪审查是基于每个目标或每个用户的访问模式,必然导致有海量数据产生,特别是网络攻击带来的海量的安全审计信息难以处理,如何利用人工智能技术解决入侵检测和安全审计中"数据爆炸、知识贫乏"的问题,成为当前网络安全研究中的难点和热点.自动的知识发现是网络安全检测和安全审计处理的重要研究方向[2].传统的入侵检测由于依赖已知攻击数据进行训练,不能做到自动更新规则库和检测新的入侵也无法检测新的攻击行为.

审计跟踪作为一种安全机制,其信息包含了很多方面的内容,本文中主要关注的是网络安全审计中的系统调用执行迹[3-4].1996 年,墨西哥大学的 Forrest 等人提出了在异常检测中通过分析程序执

收稿日期:2006-10-13.
基金项目:江苏省自然科学基金资助项目(BK2005009);中国博士后基金资助项目(2004036405);江苏博士后基金资助项目(0401064B).

行过程产生的系统调用序列(称为系统调用执行迹, sequences system calls, SSC)来构建特征轮廓的方法,并用实验证明了程序执行轨迹的局部模式(系统调用的短序列)可以完全刻画程序行为的特征[1].这种基于程序行为的分析方法可以大大减少由用户行为的不可测性带来的系统虚警(误报)率. Forrest 对短序列采用的是统计的方法,较为经典的是 Tide (time-delay embedding)和 Stide(sequence time-delay embedding) 2 种方法[4]. Tide 方法存储所有唯一的短序列来构成特征数据库,检测时比较并记录被测轨迹的短序列与数据库中记录的不匹配,以此作为检测标准. Stide 是在 Tide 方法的基础上通过求序列的局部不匹配率来判断异常,这种方法认为局部区域的不匹配数目能够更好地表征异常行为.虽然采用了树状存储,但这些算法仍需要较大的空间来存储特征数据库,且缺少对偶然事件和入侵变异的识别能力,很容易产生虚报. 在后来的研究中, LEE 等人用数据挖掘的方法研究系统调用数据的采样,使用一个称为 RIPPER(repeated incremental pruning to produce error reduction)的程序[5],用一个较小的规则集合来描述正常数据的模式特征,在检测时,违反这些特征的序列被视为异常. 同时在神经网络领域中,Anupk Ghosh 等人提出了一种用神经网络对程序行为特征进行分析的方法[6].

这些理论研究证明了系统调用序列检测方法是高效、准确的,但是作为现有的网络入侵检测系统,缺乏良好的实时效应,以及特征数据库的训练依赖于特定的网络环境,因而迟迟未得到实际应用.

本文提出了基于支持向量描述(SVDD)的安全审计模型,利用 SVDD 算法构建了系统正常状态模式,对偏离该模式的行为进行异常检测. 在对安全审计中的系统调用序列数据预处理中,对大量的短序列样本进行数据规约. 减少 SVDD 的训练样本,降低 SVDD 训练的复杂度. 利用不完备的数据集,实现基于 SVDD 的安全审计模型,通过对短序列切分大小的调整,对 SVDD 模型在 MIT lpr 数据集上的异常检测效果进行了验证. 基于前期短序列的切分长度对 SVDD 的分类效果的影响,进一步讨论了不同的核参数以及数据发生频率等约束对于结果的不同影响,并作了比较.

1 系统调用序列的数据预处理

系统调用序列的数据采集方法比较简单,通过对系统的审计系统进行配置,就可使审计系统根据用户的要求监控相关程序的执行过程[3]. 预处理的主要目的就是要得到执行迹的系统调用短序列. 由于执行迹中系统调用的次序关系是描述该程序行为的重要特征,分析这种次序关系的最简单方法就是利用长度为 K 的滑动窗口(sliding window)技术构造系统调用短序列. 基于前期的研究和对比,本实验选取短序列的长度 K 为 7.

对滑动窗口进行切分后,得到大量的短序列样本,存入安全审计数据库中. 由于各个用户在使用过程中常常使用类似的系统调用序列,这样会产生大量冗余的数据. 经过对短序列的数据规约,得到了有代表性的少量样本. 这些样本将用来训练基于支持向量描述的单类分类器. 选择原始样本2 912 133个,训练样本 604 个。

可见,经过适当的数据预处理,利用少量的训练样本来训练 SVDD,大大减少了运算量,保证了实验的高效、顺利进行,同时也符合支持向量描述算法的思想.

2 基于 SVDD 的审计模型

D. M. J Tax 建立了支持向量数据描述(SVDD)利用高斯核函数把样本空间映射到核空间,在核空间找到一个能够包含所有训练数据的一个球体. 当判别时,如果测试样本位于这个高维球体中,那么就认为正常,否则就认为异常. 其基本思想是:首先通过核函数将输入空间映射到一个高维空间,在这个高维空间构造一个包含所有训练样本点的球体;在球面上的样本点即为 SVDD 所求得的支持向量. 由于支持向量的个数是稀疏的,因此计算量相应减少.

假设模型 $f(x; w)$ 表示一类紧密的有界数据集,因此可以借助一个超球体去包含并描述它. 这个球体可以用中心 a 和半径 R 表示,而且使训练集 X^{tr} 的所有样本都落在此球体内. 这就表示经验风险等于 0,因此,类比于 SVM[7],定义一个结构误差:

$$\varepsilon_{\mathrm{struct}}(R, a) = R^2. \tag{1}$$

在如下的约束下对它最小化:

$$\| x_i - a \|^2 \leq R^2, \ \forall i. \tag{2}$$

由于训练样本中一般含有噪声或野值(也叫新颖值),因此上述优化结果对噪声或野值敏感,缺少鲁棒性. 为提高结果的鲁棒性,仿照 SVM 为每个样本引入松弛变量 $\xi_i \geq 0, \ \forall i$,以控制野值对解的影响. 意即对于远离球心的样本点实施惩罚,因此,最小化问题变为如下形式:

$$e_{\mathrm{struct}}(R, a, x) = R^2 + C\sum a_i x_i, \tag{3}$$

其约束条件为

$$\| x_i - a \|^2 \leq R^2 + \xi_i, \xi_i \geq 0, \ \forall i, \tag{4}$$

参数 C 类似于 SVM 中的控制变量.

利用 Lagrange 函数求解上述约束下的最小化问题,其约束条件不变.

Lagrange 函数为

$$L(R,a,x,a,g) = R^2 + C\mathring{a}_i x_i - \mathring{a}_i a_i\{R^2 + x_i - (x_i \times x_i 2a \times x_i a \times a)\} - \mathring{a}_i g_i x_i. \quad (5)$$

令 L 分别对 a、R、γ 求偏导,并令偏导为 0,可得

$$L = \sum_i a_i (x_i \cdot x_i) - \sum_{i,j} a_i a_j (x_i \cdot x_j), \quad (6)$$

约束为:1) $\sum_i a_i = 1$;　2) $0 \leq a_i \leq C, \forall i$.

对上述问题相对求 α 最大,可以用标准的二次规划算法来解决. 这样就可以求得 α 的最优值,对于 $0 \leq a_i \leq C$,其对应的样本点是支持向量,位于球面上;而 $a_i = 0$ 则表示对应的样本点位于球体内. 在这里并没有显式表出 a 和 R,它们可以用 α 隐含表出.

假设 z 为测试样本,那么当如下公式满足,即判别 z 是正常类,否则为异常类. 相当于 z 落在该超球体内部.

$$\| z - a \|^2 = (z \cdot z) - 2\sum_i a_i (z \cdot x_i) + \sum_{i,j} a_i a_j (x_i \cdot x_j) \leq R^2. \quad (7)$$

式中:R 是任意一个支持向量 x_k 到球心 a 的距离:

$$R^2 = (x_k \cdot x_k) - 2\sum_i a_i (x_i \cdot x_k) + \sum_{i,j} a_i a_j (x_i \cdot x_j). \quad (8)$$

当输入空间的样本点不满足球状分布时,可以通过核技巧把输入空间先映射到高维空间,然后在映射后的高维空间内求解. 也就是将上述公式中的内积形式都变换成核函数形式:

$$x_i \cdot x_j \rightarrow \phi(x_i) \cdot \phi(x_j) = K(x_i, x_j). \quad (9)$$

式中:ϕ 为非线性映射,对于某些核函数可以显式地求出 ϕ,而绝大多数则难以表出.

选择一个适当的核函数也是比较重要的,如果选取的核函数能够将输入空间正好映射成高维空间的一个球体分布,那么所求得的分类器也会比较吻合实际的分布情况. 常用的的核函数有

1) 多项式核函数:

$$L(x,y) = (1 + x \cdot y)^d. \quad (10)$$

2) Gaussian RBF 核函数:

$$K(x,y) = \exp\left[-\frac{\| x - y \|^2}{256\sigma^2}\right]. \quad (11)$$

3) Sigmoid 核函数:

$$K(x,y) = \tanh[b(x \cdot y) - c]. \quad (12)$$

引入核函数后,原来的公式变成了如下形式:

$$L = \sum_i a_i K(x_i, x_i) - \sum_{i,j} a_i a_j K(x_i, x_j), \quad (13)$$

约束不变,而决策函数变为

$$f_{\mathrm{SVDD}}(z;a,R) = I(\| \phi(z) - \phi(a) \|^2 \leq R^2) = I(K(z,z) - 2\sum_i a_i K(z, x_i) + \sum_{i,j} a_i a_j K(x_i, x_j) \leq R^2). \quad (14)$$

这里判别函数 I 定义为

$$I(A) = \begin{cases} 1, & \text{if } A \text{ is true}, \\ 0, & \text{otherwise}. \end{cases} \quad (15)$$

3　小样本 SVDD 的系统调用序列分类器仿真实验

为了检测单类分类器在安全审计记录上的效果,利用 MIT LPR 程序的相关数据来对该模型的异常检测能力进行评估. 试验将少量的正常程序执行迹作为训练样本. 在测试数据集中正常的执行迹为 2 704 个,而异常执行迹为 1 001 个.

首先对训练集中的系统执行迹进行预处理,获得的长度为 K 的系统调用短序列集作为训练样本输入 SVDD 单类分类器,训练后的分类器就可以实现对在线样本的异常检测. 在测试阶段,将测试的程序执行迹进行预处理,得到的一系列的短序列输入单类分类器,根据式(14),当 $f_{\mathrm{SVDD}}(z;a,R)$ 输出为 +1 时,判断为正常的短系列;当 SVDD 输出为 -1 时,可以认为对应的短序列偏离了正常模式,判断为异常短序列. 为了更加正确地判断整个系统执行迹的异常状态,需设置相应的规则来提高整个检测系统的性能. 针对监控状态下整个系统调用执行迹,选定一个阈值 α,当该执行迹中的短序列被判断为异常的数目超过 α,则判定该系统调用执行迹为异常.

在本实验中,当给定的系统执行迹中短序列输出为 -1(即异常样本)的个数超过 α 时,即整个用户系统调用执行迹为异常;否则,判断为正常.

通过前期的研究与实验[13],当序列长度 K 取 9～12 时,系统的检测率和误报率(即虚警率,将正常误报为异常的比率)非常理想. 但在 K 取值为 6～8 的时候,系统的误报率比较高. 如图 1 所示.

但序列长度的增加意味着训练样本数目和训练时间的增加,为了更好地满足检测的实时性需要,必须把序列长度控制在一个较小的范围内,因此选取合适的核参数是很关键的,为了验证核参数的调整对实验结果的影响,选取比较典型的 $K = 7$ 的样例进行调整,具体实验步骤以及使用的参数为

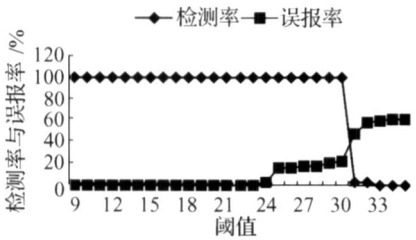

图 1 K 取 7 时系统检测率与误报率

Fig. 1 Detecting rate & error rate when $K = 7$

1) 通过计算, SVDD 中选用的核函数为 RBF 核, $\sigma = 20$, $C = 1$, $K = 7$.

2) 为了验证核参数 kernel param (KP) 的取值对整个检测结果的影响, 选取 3 个范围的 KP 即 5～9、10～14、15～20, 分别取各个范围的检测率和误报率的平均值, 以观察不同的核参数对应于整个系统的检测结果.

3) 根据不同阈值 (本实验取值为 9～35), 对切分好的攻击数据和正常数据进行检测, 从图 2～4 可以看到 KP 取不同值时的异常检测系统的检测率和误报率.

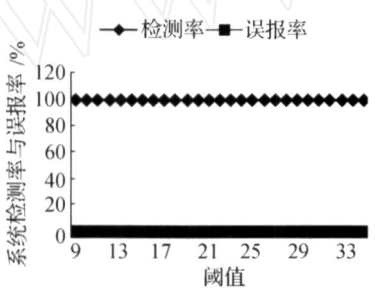

图 2 KP 取 5～9 时平均系统检测率与误报率

Fig. 2 Average detecting rate & error rate when KP = 5～9

由图 2 所示, 在 KP 取 5～9 时, 对于测试的所有阈值, 系统获得了对异常样本接近 100 % 的检测率, 误报率在 0～0.6 %, 而当 KP 取 10～14、15～20 时, 平均最高误报警率则分别达到了 42.31 % 和 98.54 % (图 3, 图 4), 远大于前次取值所获得的误报率.

根据实验结果, 当 KP 取 5～9 时, 系统在阈值调整的整个坐标系内, 检测率和误报警率一直维持在一个 100 % 和平均接近于 0 的范围, 说明通过核参数的调整, 在序列长度维持不变的情况下, 改善系统性能也是可行的, 从另一个方面证明了文中设计的系统是鲁棒的; 正常数据和攻击数据可以被完全得到区分, 同时也说明不同的核参数选择对于检测结果的影响是较大的. KP = 5～9 的情况下系统性

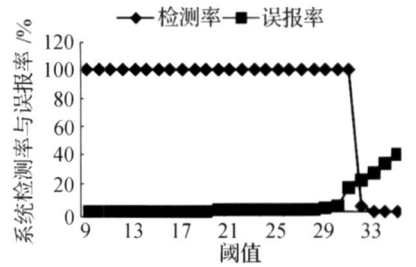

图 3 KP 取 10～14 时平均系统检测率与误报率

Fig. 3 Average detecting rate & error rate when KP = 10～14

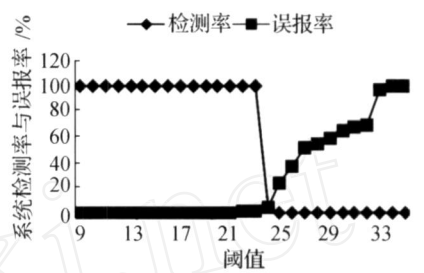

图 4 KP 取 15～20 时平均系统检测率与误报率

Fig. 4 Average detecting rate & error rate when KP = 15～20

能达到了最优, 完全将 MIT LPR 中的异常样本分开. 当 KP > 10 时, 系统的误警率有了较大回升.

通过实验可以看出, 基于 SVDD 的单类分类器的入侵检测模型具有以下特点:

1) 它不需要为系统提供异常的信息, 避免了大规模的短序列匹配过程, 减少了预处理时间.

2) 可以从较少的正常执行迹中学习正常的模式, 并能取得比较理想的检测效果.

3) 该方法由于不需要入侵的先验知识, 利用正常的样本建立正常的工作模式, 所以该方法能够检测新的攻击和攻击的变种.

4) 由于检测部分只需要简单的计算, 能够满足入侵检测实时性的要求.

4 结束语

绝对安全无缺陷的系统是不存在的, 因此入侵防护系统已成为系统安全防护中最重要的组成部分, 传统基于网络的防护系统由于数据采集方式的不足, 对非授权获得超级用户权限攻击 (user to root, U2R) 和远程用户到本地的非授权访问 (remote to local, R2L) 对这 2 类模仿正常的用户行为的攻击的识别效果很不好, 本文利用主机系统调用安全审计信息为数据源, 同时引入 SVDD 单类分类

器,避免了对入侵知识进行大规模匹配和提取的复杂工作,解决了安全审计中的异常检测问题.本文提出了基于 SVDD 单类分类器的安全审计异常检测模型,其检测性能在国际标准数据集上得到了较好的效果.需要在真实的应用环境中进一步验证这一结论,并同时深入研究实施该技术的方法和系统结构等问题,同时还要对系统调用的分类做进一步的研究,以确定一个更为合适的划分方法,从而构造能力更强、效率更高的防护系统.

参考文献:

[1]BISHOP M. A standard audit trail format [A]. Proceeding of the 18th National Information Systems Security Conference [C]. Baltimore, l995.

[2]FORREST S, HOFMEYR S A. Computer immunology [J]. Communications of the ACM, 1997,40(10):88 - 96.

[3]WARRENDER C, FORREST S, PEARLMUTTER B. Detecting intrusion using system calls: alternative data models [EB/OL]. http://www.cs.unm.edu/～forrest/publications/ Oakland-with-cite.pdf, 2000.

[4]FORREST S, HOFMEYR S A, LONGSTAFF T A. A sense of self for unix processes[A]. IEEE Computer Society Press[C]. Los Alamitos, 1996.

[5]LEE W, STOLFO S J, MOK K W. A data mining framework for building intrusion detection models [A]. Proc the 1999 IEEE Symposium on Security and Privacy [C]. Berkely, USA, 1999.

[6]HAYKIN S. Neural networks-a comprehensive foundation[M] 2nd. Beijing: Tsinghua University Press, 2001.

[7]CRISTIANINI N, TAYLOR J S. An introduction to SVMs and other kernel-based learning methods [M]. Cambridge Univ Press, 2000.

[8]DAVID M J T. One-class classification [D]. Dissertation: ICT Group Delft Netherland,1999.

[9]MANEVITZ L M, YOUSEF M. One-class SVMs for document classification [J]. Journal of Machine Learning Research, 2001(2):139 - 154.

[10]RTSCH G, SCHLKOPF B, MIKA S M, et al. SVM and boosting: one class [R]. Berlin, Germany: GMD FIRST Kekuié t, 2000.

[11]CHEN Y Q, ZHOU X, ET A L. One-class SVM for learning in image retrieval [A]. IEEE Intl Conf on Image Proc (ICIP2001) [C]. Thessaloniki, Greece, 2001.

[12]COLIN C, KRISTIN P. A linear programming approach to novelty detection[J]. Advances in Neural Information Processing System, 2001,13:25 - 28.

[13]潘志松,罗　隽. 基于支持向量描述的人工免疫检测算法[J]. 哈尔滨工程大学学报,2006,27(增刊):302 - 306.

PAN Zhisong, LUO Jun. An immune detector algorithm based suppert vector data description[J]. Journal of Harbin Enqineering University, 2006, 27 (supl): 302 - 306.

作者简介:

罗　隽,男,1981 年生,讲师,主要研究方向为网络安全、模式识别.

E-mail:zyqs1981 @hotmail.com.

潘志松,男,1973 年生,副教授,主要研究方向为网络安全、模式识别.

E-mail:hotpzs @hotmail.com.

胡谷雨,男,1963 年生,教授,博士生导师,主要研究方向为网络安全、网络管理.

E-mail:huguyu @vip.163.com.