文章编号:1009-3087(2016)01-0106-05 DOI:10.15961/j.jsuese.2016.01.016

基于隐马尔可夫模型的入侵检测方法

赵 婧[1],魏 彬[2],罗 鹏[2],杨晓元[2]
(1.西京学院 控制工程学院,陕西 西安 710123;2.武警工程大学 电子技术系,陕西 西安 710086)

摘 要:针对当前网络安全事件频发以及异常检测方法大多集中在对系统调用数据的建模研究上等问题,提出一种基于隐马尔可夫模型的入侵检测方法。该算法基于系统调用和函数返回地址链的联合信息来建立主机进程的隐马尔可夫模型。此外,针对常用训练方法存在的不足,设计了一种快速算法用以训练模型的各个参数。实验结果表明:基于系统调用和函数返回地址链的联合信息的引入能够有效区分进程的正常行为和异常行为,大幅度降低训练时间,取得了良好的运算效果。

关键词:入侵检测;隐马尔可夫模型;系统调用序列
中图分类号:TP393.08;TP183 **文献标志码**:A

Intrusion Detection Method Based on Hidden Markov Model

ZHAO Jing[1], *WEI Bin*[2], *LUO Peng*[2], *YANG Xiaoyuan*[2]
(1. School of Control Eng., Xijing Univ., Xi'an 710123, China; 2. Eng. Univ. of CAPF, Xi'an 710086, China)

Abstract: In order to solve the problem that network security incidents occurred frequently and anomaly detection methods are mostly focused on the modeling of the system call data, an intrusion detection method based on hidden Markov model was proposed. Joint information of system calls and function return address chain was used to establish the host process of hidden Markov model. In addition, a fast algorithm was designed to train the parameters of the model. The experimental results showed that the introduction of joint information of system calls and function return address chain could effectively distinguish between normal behavior and abnormal behavior of the process, and significantly reduce the operation time.

Key words: intrusion detection; hidden Markov model; system call sequence

入侵检测作为一种网络安全防卫技术,可以有效地发现来自外部或内部的非法入侵[1],因此针对入侵检测算法的研究具有重要的理论和很强的实际应用价值[2]。

基于动态调用序列对系统的入侵行为进行发掘是入侵检测领域主要的检测方法之一。自 Forrest 在 1996 年首次提出使用系统调用进行异常检测的思路和方法以来,有很多基于此的改进算法被提出。文献[3]提出一种基于频率特征向量的系统调用入侵检测方法,将正常系统调用序列抽取出的子序列的频率特征转换为频率特征向量。文献[4]提出基于枚举序列、隐马尔科夫 2 种方法建立系统行为的层次化模型。然而,这类方法在误报率以及漏报率方面仍与实际需求有着一定的差距。

此外,由于隐马尔可夫模型(hidden markov model,HMM)是一种描述离散时间内观察数据非常强大的统计工具[5],因此在基于主机的入侵检测研究中,HMM 方法是目前重要的研究方向之一[6]。美国新墨西哥大学的 Warrender 等[7]首次于 1999 年在 IEEE Symposium on Security and Privacy 会议上提出将 HMM 应用于基于系统调用的入侵检测中。2002年,Qiao等[8]提出使用HMM对系统调用序列

收稿日期:2015-09-22
基金项目:陕西省教育厅科研计划资助项目(15JK2187);西京学院科研基金资助项目(XJ140115);武警工程大学基础研究基金资助项目(WJY201518)
作者简介:赵 婧(1983—),女,博士生,讲师. 研究方向:数据挖掘;模式识别. E-mail:zhaojing.83@163.com
网络出版时间:2015-12-24 15:05:59 **网络出版地址**:http://www.cnki.net/kcms/detail/51.1596.T.20151224.1505.002.html

进行建模,利用 TIDE 方法划分状态序列的短序列,建立正常数据的状态短序列库来进行检测。2003 年,Cho 等[9]提出用 HMM 对关键的系统调用序列进行建模。文献[10]设计了一种双层 HMM 模型进行入侵检测,而其中所用到的训练方法存在局部最优以及时间效率较低等问题限制了其在实际中的应用。文献[11]依据在网络数据包中发现的频繁情节,设计了基于 HMM 的误用检测模型。文献[12]设计了一种基于节点生长马氏距离 K 均值和 HMM 的网络入侵检测方法。近些年,针对此方面的研究热度依然不减[6,13-14]。然而,从目前的研究情况看,虽然基于隐马尔可夫模型的入侵检测技术能取得较好的检测效果,但是也存在着如下几个问题:1)基于 HMM 的入侵检测技术主要集中在对主机的命令序列或者系统调用序列进行建模,单一的数据源提供的信息较少,因此检测效果仍然不够理想。2)在线学习问题,隐马尔可夫模型的建立需要消耗大量的时间和空间对参数进行调整学习,这导致了 HMM 难以得到有效的利用。综上所述,为克服现有模型算法所存在的问题,提出一种新的基于系统调用和进程堆栈信息的 HMM 入侵检测方法,该方法的主要思想是将系统调用和函数返回地址信息作为检测数据源,并利用 HMM 来构建主机特权进程的正常行为模型。其次,针对经典模型训练法存在局部最优且算法的复杂度较高等问题,设计一个更为简单的训练算法来计算 HMM 的参数,进而提升算法效率。最后,设计了附加观察值和附加状态等参数,用以消除非完备的数据以及零概率对模型的影响。

1　隐马尔可夫模型

马尔可夫模型中的每个状态都与一个具体的观察事件相互对应,但实际问题可能会比 Markov 链模型所描述的情况更复杂,人们所能观察到的事件一般情况下并不是与状态完全一致对应的,而是通过概率相联系,这样的模型称为 HMM[15]。

HMM[6]是由马尔可夫过程扩充改变而形成的一种随机模型算法,它的基本理论是由数学家 Baum 在 20 世纪 60 年代后期建立起来的。该方法最早在 20 世纪 70 年代应用于语音处理领域,而在 20 世纪 80 年代逐渐广泛应用于文本处理等各个领域中。20 世纪 90 年代初以来,HMM 及其各种推广形式开始被用于图像信号处理以及视频信号处理等领域。

HMM 的状态不能够直接观察到,而是可以通过观测向量序列得到,每个观测向量都是由概率密度分布表现为不同的状态,因此其是具有一定状态数的隐马尔科夫链和显示随机函数集。而其在应用过程中需要解决 3 个基本问题:对于给定的一个观察序列 $O = \{O_1, O_2, \cdots, O_T\}$ 和一个 HMM 参数 $\lambda = (\boldsymbol{\pi}, A, B)$,有:

1)评估问题,

2)解码问题,

3)训练问题。

2　基于 HMM 入侵检测方法

2.1　模型的参数定义

系统调用和函数返回地址反映了程序执行时系统内核层的服务行为。系统调用信息是进程对资源的请求,它从一定程度上反映了进程行为的变化过程。而层层嵌套的函数返回地址则反映了系统调用对内核资源请求的过程。把函数返回地址的序列称为函数调用链,它代表了一个系统调用产生时完整的函数调用的路径。假设函数 $f()$ 是函数 main() 的一个子函数且被 main() 调用,且函数 $f()$ 直接调用某个系统调用,则该调用对应的一条函数链为 $A = \{a_1, a_2\}$,其中,a_1 为函数 main() 的返回地址,a_2 为函数 $f()$ 的返回地址。系统调用与函数调用链的联合信息能够比仅仅使用系统调用信息更加有效、精确地描述进程的行为,因此,采用系统调用和函数调用链来构建正常进程的隐马尔可夫模型。

HMM 是一种双重随机过程,能够有效地刻画离散事件之间的转移特性。传统的基于 HMM 的入侵检测方法中,系统调用是 HMM 的观察符号,HMM 的观察序列是程序运行时的系统调用序列,而隐状态是不可见的。隐状态在模型中没有具体的意义,一般选择不同类型系统调用的个数作为 HMM 中隐状态的个数。

在提出的 HMM 方法中,系统调用作为 HMM 的隐状态,而系统调用产生时对应的函数调用链作为 HMM 的观察值。那么,隐马尔可夫模型的参数可以定义如下:

1)N,模型的隐状态个数。定义隐状态集合为 $S = \{S_1, S_2, \cdots, S_N\}$,$q_t$ 为 t 时刻 HMM 所处的状态。对于某个特权进程,模型的隐状态集合即为进程所有可能出现的不同类型的系统调用组成的集合,该集合中系统调用的个数即为隐状态的个数。

2)M,模型的观察值个数。定义观察值集合为 $V = \{v_1, v_2, \cdots, v_M\}$,$O_t$ 为 t 时刻 HMM 输出的观察值。对于

某个特权进程,模型的观察值集合即为进程所有可能出现的不同的函数调用链组成的集合,该集合中函数链的个数即为观察值个数。

3) 状态转移概率矩阵 $\boldsymbol{A} = \{a_{ij}\}$,其中,$a_{ij} = P(q_{t+1} = S_j \mid q_t = S_i)$,$1 \le i,j \le N$,表示当前状态(系统调用)为 S_j 且下一个状态(系统调用)为 S_i 的概率值。该状态转移矩阵描述了系统调用之间的一步转移概率。

4) 输出概率矩阵 $\boldsymbol{B} = \{b_j(k)\}$,其中,$b_j(k) = P(O_t = v_k \mid q_t = S_j)$,$1 \le j \le N$,$1 \le k \le M$,表示当前状态(系调用)为 S_j 时,对应的观察值(函数调用链)为 v_k 的概率值。如果概率值为0,则表示进程执行时,进程不可能通过执行函数路径 v_k 得到当前系统调用 S_j。

5) 初始概率矩阵 $\boldsymbol{\pi} = \{\pi_i\}$,其中,$\pi_i = P(q_1 = S_i)$,$1 \le i \le N$,表示在初始时刻处于状态(系统调用)$S_i$ 的概率值。

根据上面的参数定义,可以得到关于进程系统调用和堆栈信息的隐马尔可夫模型 $\lambda = (\boldsymbol{\pi}, A, B)$。

2.2 模型的训练

隐马尔可夫模型的训练算法是基于 HMM 的入侵检测应用的关键问题。经典的训练方法 Baum-Welch 算法是一种迭代算法,它利用前向后向概率来解决参数估计问题。但是 BW 算法是一种局部最优算法而且算法的复杂度较高,需要消耗大量的时间进行训练,这些缺点影响了 HMM 的检测效果和实用性。在提出的方法中,系统调用是作为模型的状态出现的,它对于整个模型是可见的。因此,可以利用一个更为简单的训练算法来计算 HMM 的参数。

给定某个特权进程的一条系统调用序列和相应的函数调用链序列对 HMM 进行训练。假设进程的函数调用链序列为 $O = \{O_1, O_2, \cdots, O_T\}$,系统调用序列为 $Q = \{q_1, q_2, \cdots q_T\}$,其中,$O_t$ 为进程执行系统调用 q_t 时对应执行的函数调用链。HMM 模型 $\lambda = (\boldsymbol{\pi}, A, B)$ 的各参数可由如下公式计算得到:

$$a_{ij} = \frac{N_{ij}}{N_{i*}} \tag{1}$$

$$\pi_i = \frac{N_i}{N_{to}} \tag{2}$$

$$b_j(k) = \frac{M_{jk}}{M_{j*}} \tag{3}$$

其中:N_{ij} 为训练进程中当前时刻 t 的状态 q_t 为 S_i,下一时刻 $t+1$ 的状态 q_{t+1} 为 S_j 的个数;N_{i*} 为训练进程中当前时刻的 t 状态 q_t 为 S_i,下一时刻 $t+1$ 的状态 q_{t+1} 为 $S = \{S_1, S_2, \cdots, S_N\}$ 中任一系统调用的个数;N_i 为训练进程中当前时刻 t 的状态 q_t 为系统调用 S_i 的个数;N_{to} 为训练进程中系统调用的总个数;M_{jk} 为训练进程中当前时刻 t 的状态 q_t 为系统调用 S_j 时,观察符号 O_t 为函数调用链 V_k 的个数;M_{j*} 为训练进程中当前时刻 t 的状态 q_t 为系统调用 S_j 时,观察符号 O_t 为 $V = \{v_1, v_2, \cdots, v_M\}$ 中任一函数调用链的个数。

由于完备的训练数据是很难获得的,因此在实际检测中有可能出现之前在训练数据集中未曾学习到的系统调用或者函数调用链;另外当服务进程遭受入侵时,也会产生一系列未曾在训练数据中出现过的系统调用或函数调用链。考虑到以上因素,引入一个附加观察值 v_{M+1} 和附加状态 S_{N+1} 来表示这些没有出现过的观察值和状态。在隐马尔可夫模型中,参数定义如下:$\pi_{S_{N+1}} = 10^{-6}$,$a_{S_{N+1}S_j} = a_{S_iS_{N+1}} = 10^{-6}$,$b_j(V_{M+1}) = 10^{-6}$,$1 \le i \le N$,$1 \le j \le M$。为了避免检测时出现概率值为零的情况,在状态转移矩阵 $\boldsymbol{A}$ 和初始概率分布 $\boldsymbol{\pi}$ 中为零者,也赋予一个固定的小概率值10^{-6}。

2.3 异常检测

基于正常程序行为的 HMM 训练完成以后,在实验中,以每个进程作为研究对象,检测某个进程是否正常。因此,给定一组包含系统调用和函数调用链的数据,首先按照进程号对它们进行分组,然后将每个进程产生的系统调用和函数调用链作为一组进行检测。在实际的异常检测中,长度为 L 的滑动窗用以对上述数据进行分割,其中步距为1。

利用正常数据训练得到的 HMM 参数模型 $\lambda = (\boldsymbol{\pi}, A, B)$,对于给定的一条函数调用链序列 $X = \{O_{t-L+1}, \cdots, O_t\}$(该函数链对应的系统调用序列为 $Y = \{q_{t-L+1}, \cdots, q_t\}$),可以按如下公式计算它出现的概率:

$$P(X \mid \lambda) = \pi_{q_{t-L+1}} b_{q_{t-L+1}}(O_{t-L+1}) \prod_{i=t-L+1}^{t-1} a_{q_i\, q_{i+1}} b_{q_{i+1}}(O_{i+1}) \tag{4}$$

此外,文中将异常度 δ 定义为如下的形式:

$$\delta = \frac{N_{NC}}{N_{TS}} \tag{5}$$

其中:N_{NC} 为不匹配短序列数,定义为输出概率小于初始设定阈值数目;N_{TS} 为测试进程中的总的短序列数。在实验中将求得的异常度与实验中不断调整得到的阈值 δ_h 进行比较,如果异常度大于该阈值,

就认为产生此测试序列的进程可能为异常;否则认为是正常。

3　实验结果与分析

3.1　实验数据

实验数据由在 Redhat Linux 7.2 上跟踪 Ftp 和 SambaHttpd 特权进程所获得,并将其分为训练以及测试 2 个部分。其中,训练数据是部分正常数据,而测试数据则由其余正常数据以及异常数据构成。正常数据由模拟用户各种正常行为获得,而异常数据则是对进程进行模拟攻击得到。

3.2　实验结果

每一个正常数据轨迹都是正常状态下,一个特权从开始产生到最后结束的系统调用和函数调用链序列。每一个异常数据轨迹都是特权进程从开始被攻击到最后进程结束的系统调用和函数调用链序列。

能够有效区分进程的正常状态和异常状态是评价一个入侵检测方法好坏的重要标准。进程的正常序列和进程的异常序列之间的异常度差异越大,则越容易发现针对系统的入侵行为。实验结果如表 1 所示,可见正常进程和异常进程的平均异常度差异非常明显,因此可以作为正常与异常的区分。

表 1　Ftp 和 Samba 进程正常序列和异常序列的平均异常度

Tab. 1　Ftp and Samba process the average abnormal degree of normal and abnormal sequences

L	测试特权进程	平均异常度		测试序列数		参数选择
		正常序列	异常序列	正常序列	异常序列	ε
3	Ftp	3.25	25.34	74	20	$7.582\,6\times10^{-10}$
	Samba	0.96	32.73	6	4	$1.131\,2\times10^{-10}$
6	Ftp	5.34	29.56	74	20	$4.248\,4\times10^{-18}$
	Samba	1.60	35.83	6	4	$8.658\,9\times10^{-17}$

误报率和漏报率是评价入侵检测方法有效性的一个重要标准。实验中将 Warrender 提出的经典 HMM 入侵检测方法和提出的 HMM 入侵检测方法进行比较。2 种方法都采用异常度作为判定进程是否异常的指标,同时滑动窗口的长度均选择为 $L=6$。实验采用的数据为 Ftp 和 Samba 这 2 种特权进程的正常序列和异常序列。由于 Warrender 的方法是基于系统调用来对进程的隐马尔可夫模型建模的,因此该方法只使用实验数据中各进程的系统调用序列进行训练和测试。

2 组数据的误报率和漏报率分别为表 2 和 3 所示。

表 2　FTP 进程的误报率和漏报率实验结果

Tab. 2　FTP process experimental results in rate of false positives and false negatives rates

算法	正常序列个数	异常序列个数	误报个数	漏报个数	误报率/%	漏报率/%
HMM	74	20	3	0	4.054	0
提出的方法	74	20	2	0	2.703	0

表 3　Samba 进程的误报率和漏报率实验结果

Tab. 3　Samba process experimental results in rate of false positives and false negatives rates

算法	正常序列个数	异常序列个数	误报个数	漏报个数	误报率/%	漏报率/%
HMM	6	4	0	0	0	0
提出的方法	6	4	0	0	0	0

为了评估提出的入侵检测方法的实时性,在实验中,对 2 种方法的训练时间进行了比较。实验所用计算机配置为 CPU Pengtium IV 2.6 GHz,512 MB DDR 内存,进程 FTP 训练和检测的统计结果如表 4 所示。

表 4　进程 FTP 数据的训练时间

Tab. 4　The FTP data training time for the process

算法	用作训练的系统调用数	训练时间/s
HMM	823 123	79 835.4
提出的方法	823 123	2 154.2

3.3　实验结果的分析与讨论

从上述结果可以看出:

1)所提出的基于系统调用和进程堆栈信息的 HMM 入侵检测方法是有效的。无论是 Ftp 数据还是 Samba 数据,异常序列的异常度比正常序列的异常度明显要高得多。因此,使用所提出的方法能够很容易地将程序的正常行为和异常行为区分出来,从而给检测系统提供一个较大的阈值范围选择。

2)提出的方法与 Warrender 的方法都能够检测出所有的异常进程,2 个方法对于测试数据的漏报率相同,在误报率方面提出的方法要比 Warrender 方法略好。可见,提出的方法可以保持在一个较低误报率的情况下,有效且准确地检测出针对系统的攻击行为。

3)提出的方法对正常行为模型的训练的时间消耗要远远少于 Warrender 方法。例如,训练近 83 万条系统调用需耗时约 36 min 左右,而经典的 HMM 方法则需要耗时约 22 h。

4 总 结

首先介绍了隐马尔可夫模型的基本概念,隐马尔可夫模型的3个基本问题及相关算法。然后根据隐马尔可夫模型的结构特点,提出一种利用系统调用和函数调用链2方面信息来联合构建特权进程的正常行为模型的方法,将系统调用作为隐马尔可夫模型的隐状态,函数调用链作为隐马尔可夫模型的观察符号,利用一种更为简单的训练算法来得到模型的各个参数。检测时,根据一段函数调用链的序列连续出现的概率和异常度来检测整条序列是否异常。实验结果表明:提出的方法能够有效区分进程的正常行为和异常行为;与经典HMM方法相比,该方法的训练时间消耗要小得多,因此具有更好的实时性以及实用性,即可作为一种实时有效的在线入侵检测方法。

参考文献:

[1] Wang Jian, Feng Weisen. Key technology research for content supervision based on KAD network[J]. Journal of Sichuan University: Engineering Science Edition, 2013, 45(1):133-137. [王建,冯伟森. 基于KAD网络内容监督的关键技术研究[J]. 四川大学学报:工程科学版,2013,45(1):133-137.]

[2] Zhao Jianhua, Li Weihua. Intrusion detection based on improved SOM with optimized GA[J]. Journal of Computers, 2013, 8(6):1456-1463.

[3] Zhang Liping, Lei Dajiang, Zeng Xianhua. System calls based intrusion detection method with frequency feature vector[J]. Computer Science, 2013, 6(6):330-334. [张莉萍,雷大江,曾宪华. 基于频率特征向量的系统调用入侵检测方法[J]. 计算机科学,2013,6(6):330-334.]

[4] Dong Ling, Zhang Hongli, Ye Lin. A new study of the system call sequence analysis method[J]. Intelligent Computer and Applications, 2014, 4(4):13-16. [董玲,张宏莉,叶麟. 基于系统调用序列分析入侵检测的层次化模型[J]. 智能计算机与应用,2014,4(4):13-16.]

[5] Gao Yan, Liu Wenfen. A dynamic trust evaluation model based on optimized hidden Markov process[J]. Journal of Sichuan University: Engineering Science Edition, 2015, 47(3):101-107. [郜燕,刘文芬. 基于隐Markov过程的网络信任评估模型[J]. 四川大学学报:工程科学版,2015,47(3):101-107.]

[6] Xie Yi, Tang S, Xiang Y, et al. Resisting web proxy-based HTTP attacks by temporal and spatial locality behavior[J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(7):1401-1410.

[7] Warrender C, Forresr S, Pearlmutter B. Detecting intrusions using system calls: Alternative data models[C]//Gong L, Reiter M K. Proceedings of the 1999 IEEE Symposium on Security and Privacy. Oakland, CA: IEEE, 1999:133-145.

[8] Qiao Y, Xin X W, Bin Y, et al. Anomaly intrusion detection method based on HMM[J]. Electronics Letters, 2002, 38(13):663-664.

[9] Cho S B, Park H J. Efficient anomaly detection by modeling privilege flows using Hidden Markov Model[J]. Computers & Security, 2003, 22(1):45-55.

[10] Zhou Xing, Peng Qinke, Wang Jingbo. Intrusion detection method based on two-layer HMM[J]. Application Research of Computers, 2008, 25(3):912-915. [周星,彭勤科,王静波. 基于两层隐马尔可夫模型的入侵检测方法[J]. 计算机应用研究,2008,25(3):912-915.]

[11] Li Cong. Research on network intrusion detection based on hidden Markov model computer & digital engineering[J]. Computer & Digital Engineering, 2012, 40(12):123-125. [李丛. 基于HMM的网络入侵检测研究[J]. 计算机与数字工程,2012,40(12):123-125.]

[12] Chu Zenan, Li Shiyang. Design of network intrusion detection method based on node grow Mahahanobis distance *K*-means and HMM[J]. Computer Measurement & Control, 2014, 22(10):3406-3409. [储泽楠,李世扬. 基于节点生长马氏距离*K*均值和HMM的网络入侵检测方法设计[J]. 计算机测量与控制,2014,22(10):3406-3409.]

[13] Zheng Ruijuan, Zhang Mingchuan, Wu Qingtao, et al. Analysis and application of bio-inspired multi-net security model[J]. International Journal of Information Security, 2010, 9(1):1-17.

[14] Huang Jenyan, Liao Ien, Chung Yufang, et al. Shielding wireless sensor network using Markovian intrusion detection system with attack pattern mining[J]. Information Sciences, 2013, 231:32-44.

[15] Zhang Lei, Li Mengshi, Chen Li, et al. Features and opinions classification of Chinese product reviews based on two-level HHMMs[J]. Journal of Sichuan University: Engineering Science Edition, 2013, 45(2):94-102. [张磊,李梦诗,陈黎,等. 基于双层HHMM的产品评论特征和情感分类[J]. 四川大学学报:工程科学版,2013,45(2):94-102.]

(编辑 杨 蓓)