

文章编号:1001-9081(2007)06-1360-03

## 基于模糊滑窗隐马尔可夫模型的入侵检测研究

成科扬

(江苏大学 计算机学院, 江苏 镇江 212013)

(1982cky@sina.com)

**摘要:**针对传统基于隐马尔可夫模型(HMM)入侵检测中普遍存在误报与漏报过高的问题,提出了一种基于模糊窗口隐马尔可夫模型(FWHMM)的入侵检测新方法。该方法通过运用状态转移依赖滑窗的设置提高了系统的检测精度,通过将状态的随机转移转变为模糊随机转移,提高了系统的鲁棒性和自适应性。实验结果表明,使用本文方法的检测效果要明显优于基于经典HMM的方法。

**关键词:**入侵检测;模糊滑窗隐马尔可夫模型

**中图分类号:** TP309    **文献标识码:**A

## Research of intrusion detection based on fuzzy window hidden Markov model

CHENG Ke-yang

(Department of Computer, Jiangsu University, Zhenjiang Jiangsu 212013, China)

**Abstract:** To improve detection accuracy, a new intrusion detection method with high efficiency was presented, which was based on Fuzzy Window Hidden Markov Model (FWHMM). The method improves detection accuracy by setting window of dependence between states and increases the self-adjustability and becomes lustier by changing the probability into the fuzzy random variable value. Experimental results show that the proposed method improves the detection accuracy more than the traditional HMM based method.

**Key words:** intrusion detection; Fuzzy Window Hidden Markov Model (FWHMM)

### 0 引言

入侵检测系统(IDS)作为一种重要的网络安全防卫系统,近年来已经成为计算机与网络安全研究的热点。目前,大部分基于主机的IDS,都是通过使用不同的方法,以系统调用作为研究对象来建立正常的程序行为模型,从而实现入侵检测的。这些方法包括短序列匹配、数据挖掘、非负矩阵分解、主成分分析等。隐马尔可夫模型(HMM)可以跟踪系统调用中隐含的状态转移特性,因此利用它会有较好的检测效果。但是,传统的基于HMM的入侵检测方法中由于判断依据只是测试序列的一阶马尔可夫链转移概率值的匹配程度,与历史和时间均无关,因而,极易造成误判与漏判。本文提出的基于模糊窗口隐马尔可夫模型(Fuzzy Window Hidden Markov Model, FWHMM)的入侵检测方法,引入模糊随机变量,将状态的随机转移扩展为模糊随机转移,解决了由于信息缺乏而造成的难以求得转移概率的问题;另一方面,模型将一阶马尔可夫链中t时刻的状态转移仅依赖于t-1时刻的状态扩展为其对[t-m,t-1]各时刻状态的联合依赖,从而增加了待测序列的状态上下文相关性,进而增加了模型的鲁棒性,减少了误判与漏判的概率。

### 1 模糊滑窗隐马尔可夫模型

由于传统经典HMM存在三个重要假设:

1) 马尔可夫假设(状态构成一阶马尔可夫链):

$p(w(t) | w(t-1), \dots, w(1)) = p(w(t) | w(t-1))$

2) 不动性假设(状态与具体时间无关):

$p(w_j(m) | w_i(m)) = p(w_j(n) | w_i(n))$ , 对任意  $m, n$  成立

3) 输出独立性假设(输出仅与当前状态有关):

$p(v(1), \dots, v(T) | w(1), \dots, w(T)) = \prod p(v(t) | w(t))$

三个假设一方面简化了模型的复杂性,节省了运算时间,推动了模型的应用;另一方面,由于以上模型假设的存在,导致了模型精度下降,限制了模型的应用领域。

模糊滑窗隐马尔可夫模型首先针对HMM假设一,定义  $P_{ss}^w$  为  $[t-m, t-1]$  时间段内任意时刻系统处于状态  $i$  转移到  $t$  时刻系统处于状态  $j$  的概率,其中  $m$  为滑窗的大小<sup>[1]</sup>,则系统的状态转移矩阵为:

$$P_{ss}^w = \begin{bmatrix} P_{s_1 s_1}^w & P_{s_1 s_2}^w & \cdots & P_{s_1 s_n}^w \\ P_{s_2 s_1}^w & P_{s_2 s_2}^w & \cdots & P_{s_2 s_n}^w \\ \vdots & & & \vdots \\ P_{s_n s_1}^w & P_{s_n s_2}^w & \cdots & P_{s_n s_n}^w \end{bmatrix}$$

同理,针对HMM假设三的改进,定义  $P_{sv}^w$  为  $[t-m, t-1]$  时间段内任意时刻系统处于状态  $j$ ,  $t$  时刻输出观察量  $k$  的概率,则系统观察值对状态的依赖矩阵为:

$$P_{sv}^w = \begin{bmatrix} P_{s_1 v_1}^w & P_{s_1 v_2}^w & \cdots & P_{s_1 v_n}^w \\ P_{s_2 v_1}^w & P_{s_2 v_2}^w & \cdots & P_{s_2 v_n}^w \\ \vdots & & & \vdots \\ P_{s_n v_1}^w & P_{s_n v_2}^w & \cdots & P_{s_n v_n}^w \end{bmatrix}$$

对于HMM假设二,即不动性假设(状态与具体时间无

关): $p(w_j(m) | w_i(m)) = p(w_j(n) | w_i(n))$ ,对任意 $m, n$ 成立,实质上由于系统的动态变化,包括检测者对系统观察值信息的增加, $p(w_j(m) | w_i(m)) \neq p(w_j(n) | w_i(n))$ ,也就是说 $p(w_j | w_i)$ 是一个动态变化的值,而不是一个一成不变的概率值。由此,我们引入了模糊随机变量来代替状态转移概率值。

从信息论的角度,有随机性和模糊性两种不确定性。用随机变量来描述随机性,用模糊集来描述模糊性。当所考虑的事件模糊性和随机性共存时,用模糊随机变量可以同时刻画这两种不确定性。模糊随机变量最早是由文献[3]在1978年引入。

**定义** 记 $F(U) = \{A | A: U \rightarrow [0,1]\}$ ,给定概率测度空间 $(\Omega, F, P)$ ,如果满足:

1) 对 $\forall a \in [0,1]$ , $\mu_a^-(\omega), \mu_a^+(\omega)$ ,其中:

$$\mu_a^-(\omega) = \inf\{x \in U | \mu(\omega)(x) \geq a\}$$

$$\mu_a^+(\omega) = \sup\{x \in U | \mu(\omega)(x) \geq a\}$$

2) 对 $\forall a \in [0,1]$ , $\mu_a^-(\omega), \mu_a^+(\omega)$ 均为 $(\Omega, F, P)$ 上随机变量,其中 $\mu(\omega)(x)$ 为 $\mu(\omega)$ 的隶属函数。

则称:映射 $X: \Omega \rightarrow F(U) | \omega \rightarrow \mu(\omega)$ 为模糊随机变量<sup>[3]</sup>。

这里, $a$ 为模糊集的置信水平, $\mu_a^-(\omega), \mu_a^+(\omega)$ 是迭代过程中以置信水平 $a$ 消除模糊性后返回截集的下限和上限。本文中提出按照最大隶属度消除模糊性就是以某个置信水平的上限为判据来实现的。事实上,还有很多其他消除模糊性的方法<sup>[4]</sup>:

a) 最大平均去模糊化发

$$x^* = \sum_{i=1}^l x_i / l$$

b) 重心或面积中心去模糊化法:

$$\text{对于连续域: } x^* = [\int_{\omega} \mu(\omega)(x) dx] / \int_{\omega} \mu(\omega)(x) dx;$$

$$\text{对于离散域: } x^* = [\sum_{i=1}^l x_i \mu(\omega)(x_i)] / \sum_{i=1}^l \mu(\omega)(x_i)$$

c) 面积均分去模糊化法

$$\int_{\min}^{x^*} \mu(\omega)(x) dx = \int_{x^*}^{\max} \mu(\omega)(x) dx \Rightarrow x^*$$

因此,由模糊随机变量值代替随机变量值的状态转移矩阵为:

$$\boldsymbol{\mu}_{ss}^w = \begin{bmatrix} \mu_{s_1 s_1}^w & \mu_{s_1 s_2}^w & \cdots & \mu_{s_1 s_n}^w \\ \mu_{s_2 s_1}^w & \mu_{s_2 s_2}^w & \cdots & \mu_{s_2 s_n}^w \\ \vdots & & & \vdots \\ \mu_{s_n s_1}^w & \mu_{s_n s_2}^w & \cdots & \mu_{s_n s_n}^w \end{bmatrix}$$

同理,各状态输出各观察值的依赖矩阵为:

$$\boldsymbol{\mu}_{sv}^w = \begin{bmatrix} \mu_{s_1 v_1}^w & \mu_{s_1 v_2}^w & \cdots & \mu_{s_1 v_n}^w \\ \mu_{s_2 v_1}^w & \mu_{s_2 v_2}^w & \cdots & \mu_{s_2 v_n}^w \\ \vdots & & & \vdots \\ \mu_{s_n v_1}^w & \mu_{s_n v_2}^w & \cdots & \mu_{s_n v_n}^w \end{bmatrix}$$

至此,模糊滑窗隐马尔可夫模型中观察值的输出模糊随机值为: $\mu(V^T) = \bigvee_{r=1}^{t_{\max}} \bigwedge_{t=1}^T \mu_{s_r v_t}^w(t) \mu_{ss}^w(t-1)$  (1)

基于HMM的入侵检测实质是当观察到一个新事件,而根据先前的状态和迁移检测矩阵判断出得到该新的事件的似

然概率较低时,则表明出现异常入侵情况<sup>[5]</sup>。这是要求系统通过学习、训练,得出状态转移矩阵,在经典HMM中有Baum-Welch算法可以解决这一问题。本文所建立的FWHMM要进行入侵检测应用,就必须对Baum-Welch算法进行改进:

前向公式:

$$\alpha_i(t) = \begin{cases} 0 & t = 0 \text{ 且 } \varpi_j(t) \neq \varpi_0 \\ 1 & t = 0 \text{ 且 } \varpi_j(t) = \varpi_0 \\ \bigvee_{i=1}^N \alpha_i(t-1) \mu_{s_i s_j}^w(t) \bigwedge_{k=t-1}^t \mu_{s_j s_k}^w(t), & \text{其他} \end{cases}$$

后向公式:

$$\beta_i(t) = \begin{cases} 0 & t = T \text{ 且 } \varpi_j(t) \neq \varpi_0 \\ 1 & t = T \text{ 且 } \varpi_j(t) = \varpi_0 \\ \bigvee_{i=1}^N \beta_i(t+1) \mu_{s_i s_j}^w(t) \bigwedge_{k=t+1}^T \mu_{s_j s_k}^w(t), & \text{其他} \end{cases}$$

令:

$$\xi_{ij}(t) = \frac{\alpha_i(t) \mu_{s_i s_j}^w(t) \mu_{s_j s_k}^w(t) \beta_j(t+1)}{\bigvee_{i=1}^N \bigvee_{j=1}^N \alpha_i(t) \mu_{s_i s_j}^w(t) \mu_{s_j s_k}^w(t) \beta_j(t+1)}$$

$$\gamma_i(t) = \bigvee_{j=1}^N \xi_{ij}(t)$$

参数重估公式:

$$\hat{\mu}_{s_i s_j}^w(t) = \frac{\bigvee_{t=1}^{t-1} \xi_{ij}(t)}{\bigvee_{t=1}^{t-1} \gamma_i(t)}, \hat{\mu}_{s_j s_k}^w(t) = \frac{\bigvee_{t=1}^T \gamma_j(t)}{\bigvee_{t=1}^T \gamma_j(t)}$$

改进后的 Baum-Welch 算法如下:

Initialize  $\mu_{s_i s_j}^w(t), \mu_{s_j s_k}^w(t), t: 0$ , 训练序列  $V^T$ , 收敛判据  $\theta$

for  $t: t + 1$

计算  $\hat{\mu}_{s_i s_j}^w(t), \hat{\mu}_{s_j s_k}^w(t)$

until  $\max[\hat{\mu}_{s_i s_j}^w(t) - \mu_{s_i s_j}^w(t), \hat{\mu}_{s_j s_k}^w(t) - \mu_{s_j s_k}^w(t)] < \theta$  (达到收敛)

$\mu_{s_i s_j}^w(t) = \hat{\mu}_{s_i s_j}^w(t), \mu_{s_j s_k}^w(t) = \hat{\mu}_{s_j s_k}^w(t)$

$\mu_{s_i s_j}^w(t), \mu_{s_j s_k}^w(t)$  去模糊化为:  $p_{s_i s_j}^w(t), p_{s_j s_k}^w(t)$

end

## 2 基于FWHMM的入侵检测系统构建

### 2.1 基于FWHMM入侵检测系统状态及观察值的设定

每个计算机用户在操作程序时总是处于某种状态的,而这种状态总是与其当前的意图相一致的。在这些不同的用户操作中,用户总是会发出不同的通信命令或行为。这些主要命令或行为的类型是因不同程序操作而异的,由此就可将这些状态作为入侵检测系统Markov链的状态。而这些具体的命令及操作即为状态所对应的观察值。因此,不难通过调查研究,得出在模糊滑窗隐马尔可夫模型中如何将普通用户的操作划分为若干状态。

这里,需要重点说明一下的是用户登陆和超级用户这两个特殊状态,由于这两个状态的特殊性,其往往作为模糊滑窗隐马尔可夫模型的起始状态,从而无法通过模型自身根据状态转移分析其合法性,因而需要通过其他检测方法加以辅助判定<sup>[6]</sup>。

另外,实质上当用户将要进行下一步操作时,其状态的转移总是与其业已完成的一系列操作相关的,而不是仅仅与其当前操作有关,这里,模糊滑窗隐马尔可夫模型中滑窗的设置恰能很好地处理这一问题。

## 2.2 基于 FWHMM 入侵检测系统参数的设定

要使模糊滑窗隐马尔可夫模型能在入侵检测系统中发挥功用,就必须首先求出状态转移矩阵  $\mu_{ss}^w$  及状态输出观察值依赖矩阵  $\mu_{sv}^w$ 。由于模糊滑窗隐马尔可夫模型是一个动态自适应模型,因此,模型参数的设定,分为系统使用前的静态训练和系统使用中的动态训练两部分。在静态训练部分,设立正常访问操作样集并结合改进后的 Baum-Welch 算法进行  $\mu_{ss}^w, \mu_{sv}^w$  参数静态重估。在系统动态运行中,通过对已判断的入侵检测结果与用户的实际反馈进行检测结论校验,并将校验结果反馈至模型分类器,从而对模糊随机变量  $\mu_{ss}^w, \mu_{sv}^w$  中概率值隶属度做出调整,如图 1 所示。

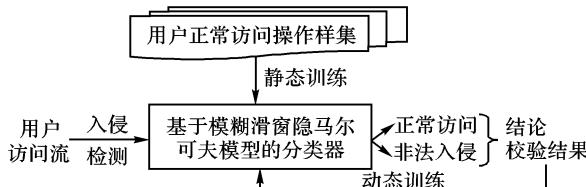


图 1 基于 FWHMM 入侵检测系统运行流程

另外,在模糊滑窗隐马尔可夫模型应用到入侵检测系统中,滑窗值  $m$  的大小也是一个十分重要的参量,其关系到模型的精度和运算量。在实际应用中,应当由待检测访问流的类型、检测的实时性要求、待访问数据库的重要性及系统开销的容度等几方面的平衡点来决定。

## 2.3 基于 FWHMM 入侵检测系统检测结论判定过程

### 1) 求出观察值序列的似然概率

对待测的若干个观察值序列根据(1)式求出  $\mu(V^T)$  并去模糊化后得  $P(V^T)$ ,为了突出概率值的差异可取  $\lg P(V^T)$ 。

### 2) 判定各子观察序列的异常倾向

系统设定一异常倾向阈值  $\varepsilon$ ,并将  $\lg P(V^T)$  与  $\varepsilon$  比较,若  $\lg P(V^T) < \varepsilon$ ,则判定该子序列有异常倾向。

### 3) 确定系统入侵检测结果

设  $C_{sum}$  为异常倾向子序列总数,  $C_{max}$  为所有子序列的总数,定义系统异常度  $\delta = \frac{C_{sum}}{C_{max}}$ ,将系统异常度  $\delta$  与系统设定的异常阈值  $\lambda$  比较,若  $\delta > \lambda$ ,则系统判定系统发生非法入侵。

## 3 系统实验及结果分析

### 3.1 实验数据

为了便于比较实验结果,本文使用美国新墨西哥大学(UNM)采集到的 sendmail 守护进程在正常运行时产生的系统调用数据和入侵进程产生的数据作为实验数据源(<http://www.cs.unm.edu/~immsec/datasets.htm>),该数据描述如表 1 所示。

表 1 实验数据描述

	数据名称	T	进程数
静态训练数据	sendmail	24 075	117
正常测试数据	sendmail	37 596	47
	local 1	1 516	6
	local 2	1 574	6
异常测试数据	remote 1	1 861	7
	remote 2	1 553	4
	sm565a	275	3
	sm5x	1 537	8

训练时,首先选取模型中的状态数  $N$ ,本文所使用的训练数据共有 53 个不同的系统调用,因此可确定模型中状态数  $N = 53$ 。

## 3.2 实验结果

表 2 异常度实验结果描述

		系统入侵检测异常度 $\delta$					
		基于传统HMM	基于FWHMM	m=1	m=3	m=6	m=10
正常测试数据	sendmail	0.63	0.55	0.43	0.35		
异常测试数据	local 1	6.10	7.46	14.97	16.72		
	local 2	8.00	8.46	13.96	19.23		
	remote 1	11.50	14.42	21.01	25.59		
	remote 2	8.40	13.41	18.28	21.70		
	sm565a	8.10	13.19	19.63	27.74		
	sm5x	8.21	10.88	19.45	28.08		

表 3 识别率实验结果描述

	滑窗大小	识别率/%	误、漏报率/%
基于 HMM	$m = 1$	80.59	19.41
	$m = 3$	83.19	16.81
基于 FWHMM	$m = 6$	85.78	14.22
	$m = 10$	86.57	13.43

从表 2、表 3 可以得出以下结果:

1) 异常测试数据的异常度比正常测试数据的异常度明显大得多,因此使用本文方法很容易准确地将程序的正常行为与异常行为区分出来。

2) 使用本文方法得到的异常测试数据的  $\delta$  比基于传统 HMM 的方法大得多,这说明利用本文方法可以更有效、更准确地将异常行为检测出来,且随着  $m$  的增大,检测效果越好。

3) 本文方法较之于基于传统 HMM 的方法,入侵检测的误报率、漏报率显著降低。

## 4 结语

本文提出了一种基于模糊滑窗隐马尔可夫模型的入侵检测新方法。系统通过运用状态转移依赖滑窗的设置提高了系统的检测精度,通过将状态的随机转移转变为模糊随机转移,提高了系统的鲁棒性和自适应性。实验结果表明,使用本文方法的检测效果要明显优于基于 HMM 的经典方法。

### 参考文献:

- [1] XU ZJ, SUN JZ, LI WJ. Intrusion Detection Using Fuzzy Window Markov Model[J]. Proc. IEEE, 2004: 645 - 648.
- [2] 冯前进,陈武凡.模糊马尔可夫场模型与图像分割新算法[J].南方医科大学学报,2006,26(5):579 - 583.
- [3] KWAKENAAK H. Fuzzy random variables I: Definitions and theorems[J]. Information Sciences 1978, 15: 1 - 29.
- [4] GRABISCH M, MUROFUSHI T, SUGENO M. Fuzzy measures and integrals: theory and applications[M]. New York: Springer, 2000.
- [5] 张响亮,王伟,管晓宏.基于隐马尔可夫模型的程序行为异常检测[J].西安交通大学学报,2005,39(10):56 - 59.
- [6] LEE W, STOLFO S. Data mining approaches for intrusion detection [A]. In: Proceedings of the 7th USENIX Security Symposium, San Antonio, TX, 1998. 26 - 40.