基于分级属性的软件监控点可信行为模型

李 珍* 田俊峰 赵鹏远
(河北大学数学与计算机学院 保定 071002)

摘 要：为了准确判断软件的可信性，针对软件预期行为轨迹中的软件监控点，该文提出了一个基于分级属性的软件监控点可信行为模型。首先，依据软件监控点各属性在可信评价中的作用范围将属性分级，构建各级属性的可信行为模型。其次，针对场景级属性，对同一监控点的训练样本进行区分，提出了一个基于高斯核函数的场景级属性聚类算法；针对单类训练样本，提出了基于单类样本的场景级属性权重分配策略。最后，实验分析表明：基于分级属性的软件监控点可信行为模型能够准确地对监控点的可信性进行评价；对于场景级属性可信模型，采用基于高斯核函数的场景级属性聚类算法具有更低的分类错误率，基于单类样本的场景级属性权重分配策略具有更优的可信性评价效果。

关键词：软件行为；监控点；可信性评价；聚类；属性权重
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2012)06-1445-07
DOI: 10.3724/SP.J.1146.2011.01060

A Trustworthy Behavior Model for Software Monitoring Point Based on Classification Attributes

Li Zhen Tian Jun-feng Zhao Peng-yuan
(*College of Mathematics and Computer*, *Hebei University*, *Baoding* 071002, *China*)

Abstract: In order to estimate the software trustworthiness accurately, a trustworthy behavior model for software monitoring point based on classification attributes is proposed for the software monitoring point in the expected behavior trace of software. Firstly, the attributes of software monitoring point are classified according to the sphere of action during the trustworthiness evaluation and the trustworthy behavior model of each attribute level is constructed. Secondly, for scene level attributes, a clustering algorithm of scene level attributes based on Gaussian kernel function is presented considering the distinction of training samples of one monitoring point, and a weight distribution strategy for scene level attributes based on one-class samples is proposed for one-class training samples. Finally, experiments and analyses show that: the model can evaluate software monitoring point accurately; For trustworthy behavior model of scene level attributes, the clustering algorithm has lower classification error rate than other clustering algorithms, and the weight distribution strategy has better effect of trustworthiness evaluation than other methods of weight distribution for one-class samples.

Key words: Software behavior; Monitoring point; Trustworthiness evaluation; Clustering; Attribute weight

1 引言

随着软件在敏感领域如金融、军事及经济等应用的不断深化，对软件可信性需求愈加急迫。如果在软件执行过程中，软件行为符合软件预期行为描述集中的相关规则，则认为软件是可信的[1]。软件的预期行为轨迹通常由一系列有序的软件监控点及监控点间的转移事件构成。监控点设置的粒度越细，则软件检查的粒度越细，软件可信的程度越高，但对软件运行效率的影响也就越大，在实际应用中需要根据对可信程度和运行效率的要求进行设置。常用的细粒度监控点有系统调用，粗粒度监控点有功能模块、构件等。构建软件监控点的可信行为模型为实现软件的可信性评价提供了重要的依据。

通过软件监控点来刻画软件预期行为轨迹，出现了一系列描述软件行为轨迹的模型。例如，静态分析源代码建立的 FSA 和 PDA 模型[2]，静态分析与动态学习结合的 HPDA 模型[3]，上下文敏感的 Dyck 模型[4]，静态分析-动态绑定的混杂模型

2011-10-13 收到，2012-01-06 改回
国家自然科学基金(60873203, 61170254)，空天信息安全与可信计算教育部重点实验室开放基金(AISTC2009_03)，河北省杰出青年基金 (F2010000317) 和河北省自然科学基金 (F2010000319, F2011201039)资助课题
*通信作者：李珍 lizhen_hbu@126.com

HFA[5] ，支持运行监控的可信软件构造模型[6]，基于运行路径的构件软件模型[7]等。上述模型能够刻画软件的运行轨迹，部分模型针对软件监控点引入了一些属性，如参数策略、上下文等，来实现对软件控制流和数据流的监控，但涉及的软件监控点的属性信息有限，一些研究者对此进行了扩充。例如，Pu 等人[8]引入了时间间距属性；李小勇等人[9]从可用性、可靠性和安全性等方面对多个属性进行监控；文献[10]在软件可信性评价时引入了监控点功能、参数策略、上下文、时间戳、内存占用率、CPU 占用率等属性。然而上述模型对属性的特点及在软件监控点可信性评价中的作用没有加以区分；而且在训练阶段，通过软件的多次运行，将捕获的同一监控点全部样本的属性值作为一个训练集来构建软件监控点的可信行为模型。由于软件运行时，从上一监控点到当前监控点经过的路径可能不同，使得同一监控点的同一属性的正常值可能出现明显的差距，因此上述方法建立的软件监控点可信行为模型不准确，从而影响了软件的可信性评价。

针对上述问题，本文依据软件监控点各属性在可信评价中的作用范围，将属性分级，提出了一个基于分级属性的软件监控点可信行为模型。针对场景级属性，对同一监控点的训练样本进行区分，提出了基于高斯核函数的场景级属性聚类算法，建立了场景级属性可信模型，并提出了一种基于单类样本的场景级属性权重分配策略，从而达到更好的可信性评价效果。

2 基于分级属性的软件监控点可信行为模型概述

软件监控点的行为通过监控点的多个属性来描述，依据各属性的特点及在可信评价中的作用范围，将属性分为以下三级：

(1)控制流级　该级属性用来决定软件是否按照正确的路径运行，如监控点功能，上下文属性等。上下文可以表示为当前监控点的调用堆栈信息，即若两个监控点的调用堆栈相同，则这两个监控点的上下文是相同的，否则是不同的。

(2)访问控制级　该级属性用来描述对资源的访问控制信息，如参数策略属性。参数策略是在监控点上下文下允许访问的参数值的限制，主要包括一元关系和二元关系。一元关系是关于单一参数的关系，例如采用枚举方式列出允许或不允许出现的参数值；二元关系是关于两个监控点参数或一监控点参数和另一监控点返回值之间的关系，例如等于关系，两个监控点参数或参数与返回值之间相等，用 equal 表示。

(3)场景级　该级属性用来描述监控点的场景级信息，这些属性的可信取值无法用准确的数字表示，允许存在一定范围的误差，如时间间距、CPU 改变量、内存改变量等，分别用来表示当前监控点与上一监控点起始时间、CPU 占用率及内存占用率差的绝对值。

控制流级属性和访问控制级属性对软件监控点可信性评价是确定的，一旦偏离正常值，则能直接决定该监控点不可信。而场景级属性无法用准确的数字表示，允许存在一定范围的误差，具有一定的模糊性。基于分级属性的软件监控点可信行为模型及可信评价过程如图 1 所示。左侧部分是一个由若干软件监控点及监控点间转移形成的软件预期行为轨迹示意图，其中带有阴影的监控点及加粗的箭头描述了软件运行的某一实例经过的监控点及其转移过程。对于任一软件监控点 mp_i，其可信行为模型如图 1 右侧部分所示，由控制流级属性可信模型、访问控制级属性可信模型和场景级属性可信模型 3 部分组成。mp_i 的可信评价过程如下：

步骤 1　依据控制流级属性可信模型，进行控制流级属性的可信评价。控制流级属性如监控点功能、上下文等属性的可信取值建模方法详见文献[11]。当 mp_i 的控制流级属性均为正常值，则其控制流级属性的可信度 $d_c=1$；否则若任一控制流级属性偏离正常值，则 $d_c=0$，转步骤 4。

步骤 2　依据访问控制级属性可信模型，进行

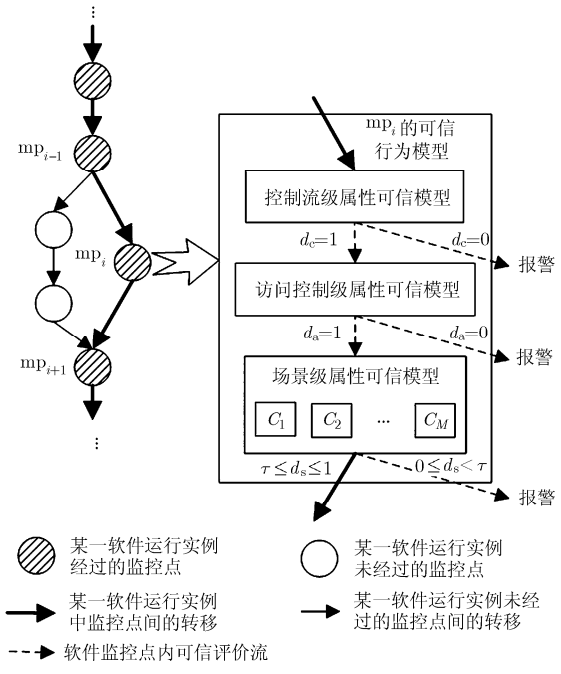

图 1 软件监控点的可信行为模型及可信评价流程

访问控制级属性的可信评价。可信的参数策略详见文献[11]。当 mp_i 的访问控制级属性均为正常值，则其访问控制级属性的可信度 $d_{\mathrm{a}}=1$；否则 $d_{\mathrm{a}}=0$，转步骤 4。

步骤 3　依据场景级属性可信模型，进行场景级属性的可信评价。场景级属性的可信模型详见第 3 节。mp_i 的场景级属性的可信度 d_{s} 取值为[0,1]。

步骤 4　mp_i 的可信度 d 表示为

$$d=\begin{cases}0, & d_{\mathrm{c}}=0\text{或}d_{\mathrm{a}}=0\\ d_{\mathrm{s}}, & \text{其它}\end{cases} \tag{1}$$

通过对已知可信性的大量软件监控点进行实验，可以给出可信的软件监控点可信度的取值范围，从而设置合适的软件监控点可信度阈值 τ ($\tau\in(0,1)$)。若 $d\in[\tau,1]$，则 mp_i 可信，软件继续运行至下一监控点 mp_{i+1}，重新从步骤 1 开始 mp_{i+1} 的可信评价；否则报警 mp_i 不可信，软件停止运行。

3　软件监控点场景级属性可信模型

3.1 场景级属性的训练样本聚类

训练阶段，在给定环境下经过软件的多次运行得到每一监控点各属性的多个样本。由于软件运行时，从上一监控点到当前监控点经过的路径可能不同，因此同一监控点的同一场景级属性的正常值可能出现明显的差距，致使依据未加区分的样本值训练得到的可信模型不准确。因此需要对这些样本进行聚类。

很多传统的聚类算法不能自动选择聚类数，目前虽然有一些算法能够自动选择聚类数，但还存在一些不足。比如，ISODATA 算法[12]不适用于类重叠或各类协方差不同的情况；COLRM 算法[13]采用 K 均值算法得到初始的符合高斯分布的类，也不适用于各类协方差不同的情况。考虑到除去环境影响后，每一监控点的场景级属性的频数基本呈高斯混合分布[14]，本文采用基于高斯核函数的场景级属性聚类算法把近似符合高斯混合分布的样本数据划分为符合高斯分布的类，该算法对类重叠及各类协方差不同的情况均适用，具体描述如下：

设软件监控点 mp 有 n 个样本 $\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_n$，每个样本是一个 m 维的随机向量，由 m 个场景级属性 $A_1,A_2,\cdots,A_m$ 组成，用样本矩阵 $\boldsymbol{X}=(x_{ij})_{n\times m}$ $(1\le i\le n,1\le j\le m)$表示。

(1)输入初始聚类数 M_{init}，重叠度阈值 δ，令每次迭代的聚类数 $M_{\mathrm{e}}=M_{\mathrm{init}}$。

(2)令聚类数 $M=M_{\mathrm{e}}$，则样本的类别表示为 $C_1,C_2,\cdots,C_M$，采用以样本的统计估计值为参数的高斯函数作为核函数，第 t $(1\le t\le M)$ 类样本的核函数 $K_t(\boldsymbol{X}_i,V_t)$ 表示为

$$K_t(\boldsymbol{X}_i,V_t)=\frac{1}{(2\pi)^{m/2}\,|\,\boldsymbol{\Sigma}_t\,|^{1/2}}\cdot\exp\left\{-\frac{1}{2}(\boldsymbol{X}_i-\boldsymbol{\mu}_t)^{\mathrm{T}}\boldsymbol{\Sigma}_t^{-1}(\boldsymbol{X}_i-\boldsymbol{\mu}_t)\right\} \tag{2}$$

这里的参数集 $V_t=\{\boldsymbol{\mu}_t,\boldsymbol{\Sigma}_t\}$，其中，$\boldsymbol{\mu}_t$ 为样本均值向量，$\boldsymbol{\Sigma}_t$ 为样本协方差矩阵。

(3)采用高斯分布的贝叶斯决策规则，定义样本 $\boldsymbol{X}_i$ 与第 t 类样本的相似性度量 $\Delta(\boldsymbol{X}_i,K_t)$，表示为

$$\Delta(\boldsymbol{X}_i,K_t)=\frac{1}{2}(\boldsymbol{X}_i-\boldsymbol{\mu}_t)^{\mathrm{T}}\boldsymbol{\Sigma}_t^{-1}(\boldsymbol{X}_i-\boldsymbol{\mu}_t)+\frac{1}{2}\lg|\,\boldsymbol{\Sigma}_t\,| \tag{3}$$

按照以下规则将每个样本分到相应的类中去。

若 $\Delta(\boldsymbol{X}_i,K_t)=\min\limits_{k}\Delta(\boldsymbol{X}_i,K_k)$，$k=1,2,\cdots,M$，则 $\boldsymbol{X}_i$ 属于 C_t 类。

(4)采用文献[13]中提出的计算高斯混合模型的两个组成成分重叠度的方法，计算每两个类的重叠度 OLR_{pq} $(1\le p<q\le M)$，若 C_p 和 C_q 类满足

$$\mathrm{OLR}_{pq}>\delta\text{ 并且 }\mathrm{OLR}_{pq}=\max_{r\ge q,s\le p}\{\mathrm{OLR}_{p,r},\mathrm{OLR}_{s,q}\} \tag{4}$$

则合并 C_p 和 C_q 两类，形成一个新的类。

(5)更新聚类数 M，若 M 改变并且满足 $M>1$，则转第(2)步；否则算法结束。

上述算法所得结果就是所要聚类的结果，记为 $C_1,C_2,\cdots,C_M$ (M 为类数)。初始聚类数 M_{init} 和重叠度阈值 δ 的选取可通过大量实验得到经验值。

3.2 场景级属性可信模型的建立

对于聚类后的 $C_q(1\le q\le M)$ 类训练样本 $\boldsymbol{Y}_1^q,\boldsymbol{Y}_2^q,\cdots,\boldsymbol{Y}_{n'}^q$，令 $y_{1j}^q,y_{2j}^q,\cdots,y_{n'j}^q$ 表示软件监控点 mp 在场景级属性 A_j 上的 n' 个样本值。由于除去环境影响后，场景级属性的频数基本呈高斯分布，每个场景级属性的正常值都在均值附近波动，因此依据偏离均值的程度来确定场景级属性的可信度。C_q 类训练样本的均值 μ_j^q 表示为

$$\mu_j^q=\left(\sum_{i=1}^{n'}y_{ij}^q\right)\Big/n' \tag{5}$$

软件实际运行时，在 mp 处捕获的测试样本 $\boldsymbol{Z}$，令 $z_1,z_2,\cdots,z_m$ 表示 m 个场景级属性的值。样本 $\boldsymbol{Z}$ 在场景级属性 A_j 对于 C_q 类的可信度 $d_{\mathrm{s}j}^q$ 表示为

$$d_{\mathrm{s}j}^q=\begin{cases}z_j/\mu_j^q, & z_j\in[y\min_j^q,\mu_j^q]\\ 1+\dfrac{\mu_j^q}{y\max_j^q}-\dfrac{z_j}{y\max_j^q}, & z_j\in[\mu_j^q,y\max_j^q]\\ 0, & \text{其它}\end{cases} \tag{6}$$

其中 $y\min_j^q=\min\limits_{1\le i\le n'}\{y_{ij}^q\}$，$y\max_j^q=\max\limits_{1\le i\le n'}\{y_{ij}^q\}$，$j=1,2,\cdots,m$。

测试样本 $\boldsymbol{Z}$ 对于 C_q 类的可信度 d_{s}^q 为：$d_{\mathrm{s}}^q=\sum_{j=1}^m w_j^q d_{\mathrm{s}j}^q$。对于 mp，软件实际运行时捕获的测试样本 $\boldsymbol{Z}$ 的可信度 d_{s} 为对于各类的可信度的最大值，即 $d_{\mathrm{s}}=\max\limits_{1\le q\le M}\{d_{\mathrm{s}}^q\}$。$d_{\mathrm{s}}$ 偏离 1 的程度越大，表示可信的程度越低。

3.3 基于单类样本的场景级属性权重分配策略

在控制流级属性和访问控制级属性可信的前提下，软件监控点的可信性取决于场景级属性，而场景级属性的权重分配直接决定了软件监控点可信评价的准确度，进而决定了软件的可信性。

由于软件监控点场景级属性的权重凭主观经验较难判断，本文考虑客观赋权方法。目前采用客观方法进行属性权重分配的大部分文献获取属性权重的样本要么是多类数据的训练样本[9]，要么每个样本作为多属性决策排序的一个备选方案[15]。而对于一个软件监控点，用于权重分配的训练样本属于同类。因此这些文献中的方法均无法用于解决依据单类样本获取属性的权重问题。依据单类样本的属性权重分配方法目前为止研究较少，信息熵[16,17]是一种解决方法，它的思想是计算一类样本中各属性的信息熵，属性熵值越小说明数据越规则，建立的模型准确性越好，赋予较大的权重；反之赋予较小权重。然而信息熵方法仅考虑了单个属性值的分散程度，没有考虑属性之间的相互影响。由于多个场景级属性间是线性相关的，我们将属性间的相关性引入权重计算过程，并采用线性相关系数来度量属性间的相关性。对适用于多属性决策的 CCSD (Correlation Coefficient and Standard Deviation)方法[15]进行改进，从属性值的分散程度以及属性间的相互关系出发确定场景级属性的权重，给出一个基于单类样本的场景级属性权重分配策略——改进 CCSD 算法。具体描述如下：

(1)计算标准差　对于聚类后的 C_q 类训练样本 $\boldsymbol{Y}_1^q,\boldsymbol{Y}_2^q,\cdots,\boldsymbol{Y}_{n'}^q$，训练样本 $\boldsymbol{Y}_i^q\ (1\le i\le n')$ 在场景级属性 A_j 上的标准差 σ_j^q 为

$$\sigma_j^q=\sqrt{\left[\sum_{i=1}^{n'}(y_{ij}^q-\mu_j^q)^2\right]\Big/(n'-1)} \tag{7}$$

若标准差 σ_j^q 越小，说明取值越集中，刻画正常行为的能力越强，应分配给 A_j 大权重；反之说明取值越分散，刻画正常行为的能力越弱，应分配给 A_j 小权重。

(2)计算相关系数　训练样本 $\boldsymbol{Y}_i^q$ 在 A_j 的可信度 $d_{\mathrm{s}ij}^q$ 表示为

$$d_{\mathrm{s}ij}^q=\begin{cases}y_{ij}^q/\mu_j^q, & y_{ij}^q\in[y\min_j^q,\mu_j^q]\\ 1+\dfrac{\mu_j^q}{y\max_j^q}-\dfrac{y_{ij}^q}{y\max_j^q}, & y_{ij}^q\in[\mu_j^q,y\max_j^q]\end{cases} \tag{8}$$

其中 $y\min_j^q=\min\limits_{1\le i\le n'}\{y_{ij}^q\}$，$y\max_j^q=\max\limits_{1\le i\le n'}\{y_{ij}^q\}$，$j=1,2,\cdots,m$。

可见，$d_{\mathrm{s}ij}^q\in[0,1]$。对于软件监控点 mp，$C_q$ 类样本 $\boldsymbol{Y}_i^q$ 的可信度 $d_{\mathrm{s}i}^q$ 为：$d_{\mathrm{s}i}^q=\sum_{j=1}^m w_j^q d_{\mathrm{s}ij}^q$。$w_j^q$ 为 C_q 类样本 A_j 的权重。

当去掉 A_j 后，样本 $\boldsymbol{Y}_i^q$ 的可信度 $d_{\mathrm{s}i}^{\bar{q}j}$ 为：$d_{\mathrm{s}i}^{\bar{q}j}=\sum_{k=1,k\ne j}^m w_k^q d_{\mathrm{s}ik}^q$。$A_j$ 的可信度 $d_{\mathrm{s}ij}^q$ 与样本 $\boldsymbol{Y}_i^q$ 的可信度 $d_{\mathrm{s}i}^q$ 的相关系数 R_j^q 表示为

$$R_j^q=\frac{\sum\limits_{i=1}^{n'}(d_{\mathrm{s}ij}^q-\bar{d}_{\mathrm{s}j}^q)(d_{\mathrm{s}i}^{\bar{q}j}-\bar{d}_{\mathrm{s}}^{\bar{q}j})}{\sqrt{\sum\limits_{i=1}^{n'}(d_{\mathrm{s}ij}^q-\bar{d}_{\mathrm{s}j}^q)^2\cdot\sum\limits_{i=1}^{n'}(d_{\mathrm{s}i}^{\bar{q}j}-\bar{d}_{\mathrm{s}}^{\bar{q}j})^2}} \tag{9}$$

其中 $\bar{d}_{\mathrm{s}j}^q=\dfrac{1}{n'}\sum\limits_{i=1}^{n'}d_{\mathrm{s}ij}^q$，$\bar{d}_{\mathrm{s}}^{\bar{q}j}=\dfrac{1}{n'}\sum\limits_{i=1}^{n'}d_{\mathrm{s}i}^{\bar{q}j}$。

A_j 与其他场景级属性的相关系数 R_j^q 若很大，接近 1，说明 A_j 对整体判断影响很小，则应分配给 A_j 小权重；反之若 R_j^q 很小，接近-1，说明 A_j 对整体判断影响很大，则应分配给 A_j 大权重。

(3)综合上述标准差和相关系数，计算场景级属性的权重　场景级属性权重分配公式如下：

$$w_j^q=\frac{\sqrt{1-R_j^q}\,\Big/\sigma_j^q}{\sum\limits_{k=1}^{m}\sqrt{1-R_k^q}\,\Big/\sigma_k^q} \tag{10}$$

式(10)包含 m 个公式，唯一确定了 m 个权重变量。将其转化为求解下述非线性最优模型，即已知 $\sum_{j=1}^m w_j^q=1$，$w_j^q\ge 0$，最小化式(11)。

$$J=\sum_{j=1}^{m}\left(w_j^q-\frac{\sqrt{1-R_j^q}\,\Big/\sigma_j^q}{\sum\limits_{k=1}^{m}\sqrt{1-R_k^q}\,\Big/\sigma_k^q}\right)^2 \tag{11}$$

通过 LINGO 软件即可解出各场景级属性的权重值。

4 实验与分析

本文在 CPU 为 Intel(R)Core (TM)2 Duo E7500 2.93 GHz，内存为 2 GB 的主机上进行了实验，Linux 内核为 2.4.20。软件监控点的设置粒度为系统调用，通过可加载内核模块 LKM 截获每个系统调用，并进行相应的修改，捕获系统调用的多个属性值。针对 Red Hat 9 Linux 下的编辑器软件 vi6.1 进行了实验，以访问控制级属性和场景级属性为例进行分析。令软件监控点的可信度阈值 $\tau=0.85$。

4.1 访问控制级属性的可信评价

软件 vi6.1 存在 TOCTTOU(Time Of Check To

Time Of Use)漏洞。当 root 用户使用 vi6.1 编辑所有者为普通用户的文件时，该普通用户可能成为敏感文件如/etc/passwd 的所有者。该漏洞涉及到 fileio.c 文件中的脆弱性窗口<open, chown32>系统调用对。

进行如下攻击测试：循环检测 wfname 文件的所有者是否已变为 root，一旦发生，就将 wfname 文件符号链接到敏感文件/etc/passwd。之后 vi6.1 把/etc/passwd 的所有者改为攻击者。

当攻击成功时，vi6.1 运行到系统调用 chown32 时，通过控制流级属性可信评价，d_c=1。在访问控制级属性可信评价时，检测到不满足 chown32 的访问控制级的如下参数策略属性：chown32(wfname) equal open(wfname)。访问控制级可信度 d_a=0，则 chown32 的可信度 $d<\tau$，因此该监控点不可信，软件停止运行。该攻击被成功检测出。有关引入系统调用作为软件监控点后增加的时间开销详见文献[10]。

4.2 场景级属性的可信评价

选取软件 vi6.1 中一个 3 条路径汇合处的系统调用监控点，在干净的环境下沿各路径运行时分别捕获到 50 个场景级属性样本(含时间间距、内存改变量、CPU 改变量 3 个场景级属性)。图 2 分别用 3 个类表示沿 3 条路径捕获的场景级属性样本数据。其中，类 1 样本属性值与其他两类属性值差异较大，而类 2 与类 3 样本的属性值差异较小，存在部分重叠，且各类协方差矩阵相差较大。当该监控点控制流级属性的可信度 d_c 和访问控制级属性的可信度 d_a 均为 1 时，监控点的可信度 d 取决于场景级属性的可信度 d_s。

(1)基于高斯核函数的场景级属性聚类算法测试　基于高斯核函数的场景级属性聚类算法需要设置初始聚类数 M_{init}，如果初始聚类数太大，会增加反复迭代的次数。给定聚类数 M，由该算法可以得出需迭代的次数，图 3 给出了当聚类数 M 为 2,3,4 时初始聚类数与迭代次数的关系。可以看出，对于

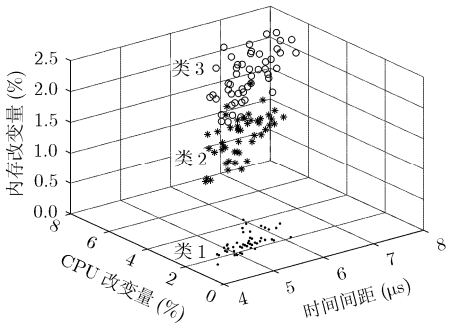

图 2 场景级属性样本数据

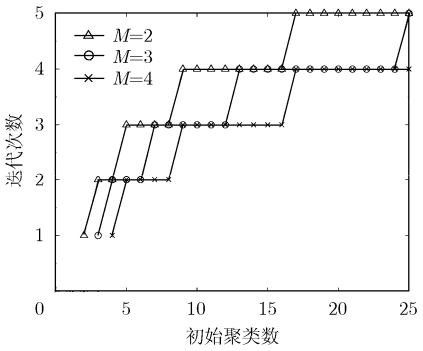

图 3 初始聚类数与迭代次数的关系

给定初始聚类数，M 的值越小，通常迭代的次数越多；反之迭代的次数越少。考虑到软件监控点处分支不会太多，通常不会超过 5 个，即聚类数 M 通常不超过 5 个，设置初始聚类数为 5–15 之间较为合适。

为了评估本文聚类算法的效果，定义分类错误率如下：

$$\text{分类错误率}=\left(\sum_{i=1}^{M}\left|\text{第}i\text{类实际样本数}-\text{第}i\text{类正确样本数}\right|\right)/\text{总样本数}\times 100\%$$

其中 M 为聚类数。令重叠度阈值 δ=0.7，采用本文算法与 ISODATA 算法[12]和 COLRM 算法[13]得到的聚类数和分类错误率如表 1 所示。由于 ISODATA 算法不适用于类重叠的情况，因此对具有类重叠的图 2 样本数据的聚类数进行了误判；COLRM 算法虽然能够处理类重叠，但不适用于各类协方差不同的情况，因此对各类协方差矩阵相差较大的图 2 样本数据的分类效果也欠佳。可以看出本文算法的聚类数准确，且分类错误率低于 ISODATA 和 COLRM 算法，能够更准确地划分数据。

表 1 聚类算法的比较

聚类算法	聚类数	分类错误率(%)
ISODATA	2	66.7
COLRM	3	9.3
本文算法	3	5.3

(2)改进 CCSD 算法测试　实验以图 2 中类 1 和类 2 样本为例，各类任取 45 个样本为训练样本，剩余的 5 个样本作为测试样本，通过训练样本来构建场景级属性可信模型。分别对两类中训练样本采用 4 种方法(等权，CCSD[15]，信息熵[17]，改进 CCSD)得到各属性的权重，如图 4 和图 5 所示。对于类 1，改进 CCSD 算法计算得到的各属性的相关系数差距较小，因此属性权重基本取决于属性值的分散程度，

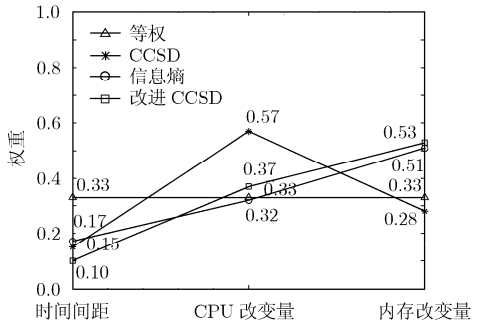

图 4 类 1 属性权重

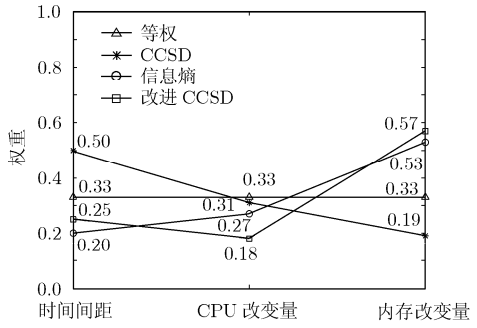

图 5 类 2 属性权重

与信息熵方法得到的权重相差不大；对于类 2，改进 CCSD 算法计算得到的各属性的相关系数差距较大，因此与信息熵方法得到的权重相差较大。

实验 1 将类 1 训练样本作为可信数据，其他类样本作为不可信数据。由于类 1 与其他两类属性值差别较大，因此对 4 种权重分配方法，类 1 测试样本均被判为可信，误报率为 0；类 2 和类 3 全部样本均被判为不可信，漏报率为 0。

实验 2 将类 2 训练样本作为可信数据，其他类样本作为不可信数据。采用 4 种权重分配方法的测试结果如表 2 所示。对于类 2 测试样本，4 种权重分配方法的误报率均为 0，且可信度均值相同。对于类 1 和类 3 全部样本，改进 CCSD 算法样本漏报率最小，其次是信息熵方法，而对于适用于多属性决策的 CCSD 方法由于认为具有较大标准偏差的属性比较小标准偏差的属性有更大权重，直接用于场景级属性权重的效果最差；而且 4 种方法中采用改进 CCSD 算法得到的可信度均值最小，即得出的不可信程度最大。可见，本文提出的改进 CCSD 算法的可信性评价效果优于其他方法。

(3)聚类对场景级属性可信评价的影响 下面将未经过聚类以及经过基于高斯核函数的场景级属性聚类形成的场景级属性可信模型的准确性进行比较。测试时，分别捕获了软件 vi6.1 运行的若干条正常轨迹和异常轨迹在该监控点的场景级属性值。其中异常轨迹是在该软件监控点与上一监控点间增加部分代码实现的。下面以表 3 所示的两条正常轨迹

表 2 实验 2 测试结果

权重分配方法	可信度均值		误报率 (%)	漏报率 (%)
	类 2 测试样本	类 1 和类 3 全部样本		
等权	0.94	0.61	0	15
CCSD	0.94	0.68	0	22
信息熵	0.94	0.56	0	8
改进 CCSD	0.94	0.48	0	4

表 3 测试样本的属性值

测试样本	时间间距(μs)	CPU 改变量 (%)	内存改变量 (%)
Normal1	5.0	1.4	0.2
Normal2	6.2	4.3	1.3
Abnormal1	5.5	3.7	0.9
Abnormal2	11.7	6.6	3.0

(Normal1 和 Normal2)和两条异常轨迹(Abnormal1 和 Abnormal2)为例进行说明。

我们采用改进 CCSD 算法获取场景级属性权重，测试样本在未聚类以及基于高斯混合分布的场景级属性聚类后对各类的可信度如表 4 所示。未聚类时，Normal1 的可信度为 $0.51<\tau$，误判为不可信；Abnormal1 的可信度为 $0.87>\tau$，误判为可信；Normal2 和 Abnormal2 的可信性判断准确。聚类后，测试样本的可信度为各类可信度中的最大值，Normal1 和 Normal2 的可信度分别为 0.95 和 0.98，均大于 τ，准确地判为可信；Abnormal1 和 Abonormal2 的可信度分别为 0.39 和 0.22，均小于 τ，准确地判为不可信。可见，经过基于高斯核函数的场景级属性聚类后训练形成的场景级属性可信模型准确性更高。

5 结束语

本文提出了一个基于分级属性的软件监控点可信行为模型。依据软件监控点各属性在可信判断中的作用范围，将属性分级，对监控点行为进行更全

表 4 测试样本的可信度

测试样本	可信度			
	未聚类	类 1	类 2	类 3
Normal1	0.51	0.95	0.21	0.17
Normal2	0.95	0	0.98	0.21
Abnormal1	0.87	0.09	0.39	0.18
Abnormal2	0.11	0	0	0.22

面准确的建模。针对场景级属性，对同一监控点的训练样本进行区分，提出了基于高斯核函数的场景级属性聚类算法，建立了场景级属性可信模型，并提出了一种适用于软件监控点的场景级属性权重分配策略。本文提出的聚类算法适用于任何符合高斯混合分布的模糊多维属性的聚类，提出的权重分配算法适用于任何依据单类样本来确定模糊属性权重的场合，具有广泛的推广价值。下一步的工作是考虑软件监控点各级属性的选择，以期达到更好的软件行为可信评价效果。

参 考 文 献

[1] 沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展[J]. 中国科学: 信息科学, 2010, 40(2): 139–166.
Shen Chang-xiang, Zhang Huan-guo, Wang Huai-min, *et al*.. The research and development of trusted computing[J]. *Science China*: *Information Science*, 2010, 40(2): 139–166.

[2] Wagner D and Dean D. Intrusion detection via static analysis[C]. Proceedings of the IEEE Symposium on Security and Privacy, Oakland, USA, 2001: 156–169.

[3] Liu Z, Bridges S M, and Vaughn R B. Combining static analysis and dynamic learning to build accurate intrusion detection models[C]. Proceedings of the 3rd IEEE Int'1 Workshop on Information Assurance, College Park, Maryland, March 23–24, 2005: 164–177.

[4] Giffin J, Jha S, and Miller B. Efficient context-sensitive intrusion detection[C]. Proceedings of the 11th Network and Distributed System Security Symposium, San Diego, USA, 2004: 1–15.

[5] 李闻, 戴英侠, 连一峰, 等. 基于混杂模型的上下文相关主机入侵检测系统[J]. 软件学报, 2009, 20(1): 138–151.
Li Wen, Dai Ying-xia, Lian Yi-feng, *et al*.. Context sensitive host-based IDS using hybrid automaton[J]. *Journal of Software*, 2009, 20(1): 138–151.

[6] 李仁杰. 基于监控的可信软件构造技术研究与实现[D]. [博士论文], 长沙, 国防科学技术大学, 2007.
Li Ren-jie. Research and implementation of the trusted software constitution based on monitoring[D]. [Ph. D. dissertation], Changsha, National University of Defense Technology, 2007.

[7] Hsu C J and Huang C Y. An adaptive reliability analysis using path testing for complex component-based software systems[J]. *IEEE Transactions on Reliability*, 2011, 60(1): 158–170.

[8] Pu S and Lang B. An intrusion detection method based on system call temporal serial analysis[C]. Proceedings of the 3rd International Conference on Intelligent Computing, Qingdao, China, August 21–24, 2007: 656–666.

[9] 李小勇, 桂小林, 毛倩, 等. 基于行为监控的自适应动态信任度测模型[J]. 计算机学报, 2009, 32(4): 664–674.
Li Xiao-yong, Gui Xiao-lin, Mao Qian, *et al*.. Adaptive dynamic trust measurement and prediction model based on behavior monitoring[J]. *Chinese Journal of Computers*, 2009, 32(4): 664–674.

[10] 田俊峰, 李珍, 刘玉玲. 一种可信软件设计方法及可信性评价[J]. 计算机研究与发展, 2011, 48(8): 1447–1454.
Tian Jun-feng, Li Zhen, and Liu Yu-ling. A design approach of trustworthy software and its trustworthiness evaluation[J]. *Journal of Computer Research and Development*, 2011, 48(8): 1447–1454.

[11] Li Z and Tian J F. A software behavior automaton model based on system call and context[J]. *Journal of Computers*, 2011, 6(5): 889–896.

[12] 边肇祺, 张学工. 模式识别[M]. 北京: 清华大学出版社, 2002: 230–243.
Bian Zhao-qi and Zhang Xue-gong. Pattern Recognition[M]. Beijing: Tsinghua University Press, 2002: 230–243.

[13] Wang S and Sun H. Mesuring overlap-rate for cluster merging in a hierarchical approach to color image segmentation[J]. *International Journal of Fuzzy Systems*, 2004, 6(3): 147–156.

[14] Larsen R J and Marx M L. An Introduction to Mathematical Statistics and Its Applications[M]. 4th Ed., Upper Saddle River, New Jersey 07458: Pearson Prentice Hall, 2006: 292–316.

[15] Wang Y M and Luo Y. Integration of correlations with standard deviations for determining attribute weights in multiple attribute decision making[J]. *Mathematical and Computer Modeling*, 2010, 51(1-2): 1–12.

[16] 徐菲菲, 苗夺谦, 魏莱, 等. 基于互信息的模糊粗糙集属性约简[J]. 电子与信息学报, 2008, 30(6): 1372–1375.
Xu Fei-fei, Miao Duo-qian, Wei Lai, *et al*.. Mutual information-based algorithm for fuzzy-rough attribute reduction[J]. *Journal of Electronics & Information Technology*, 2008, 30(6): 1372–1375.

[17] Tian J F and Zhu Y. Trusted shell based constitution model of trusted software[J]. *China Communications*, 2011, 8(4): 11–22.

李　珍：　女，1981 年生，讲师，研究方向为信息安全、可信软件.

田俊峰：　男，1965 年生，教授，研究方向为信息安全、分布计算、网络技术.

赵鹏远：　男，1979 年生，讲师，研究方向为信息安全、可信计算.