COTS 软构件测试的信用度量及决策模型*

余金山
(华侨大学 计算机学院,福建 泉州 362011)

摘 要:给出了 COTS 构件可信度度量的概念及构件测试的若干决策模型。该模型可以指导用户在 COTS 构件交易过程中对构件进行何种程度的测试做出选择并对风险管理和控制提供支持,从而帮助用户在能较好地进行风险管理和控制的前提下尽量减少测试的时间和成本。

关键词:软构件;测试;可信度度量;决策模型;COTS 软构件;交易

中图分类号:TP311,TP11 **文献标识码**:A **文章编号**:1674-7720(2012)03-0004-04

Trust metrics and decision-making models for COTS software component testing

Yu Jinshan
(College of Computer Science and Technology, Huaqiao University, Quanzhou 362011, China)

Abstract: This paper firstly introduces a trust metrics of COTS components, and then presents a number of alternative decision-making models for component testing. The model can in the process of COTS components transaction guide the user to make a choice on what kind of degree or extent of testing he or she should do and support risk management and control. Thus help components users to do a better risk management and control and minimize as far as possible the testing efforts and cost.

Key words: software component; testing; trust metrics; decision-making model; COTS software component; transaction

基于 COTS(Commercial Off-The-Shelf)构件的软件开发或称为基于 COTS 软构件的信息技术解决方案,被认为是一种革命性的软件开发新模式,对软件开发有着广泛和深刻的影响,它将开创软件开发的新纪元[1-2]。近几年来不但在软件界产生了巨大的影响,而且还引起了其他一系列产业界的高度重视。基于构件的软件工程已成为软件开发的主流技术,软构件技术已成为软件产业发展的主导力量。因此,构件的使用者如何对拟采用的构件进行测试已成为一个倍受重视的研究热点。

COTS 构件是一种特殊的软件产品,具有许多自身固有的完全不同于传统软件的新特性[1,3],例如:(1)面向大众进行销售、租赁和注册;(2)以赢利为目的;(3)由开发商支持及升级,开发商拥有知识产权;(4)可以有多个拷贝;(5)可能存在众多的可供选择的候选构件;(6)源代码的不可见性;(7)构件的异质(混杂)性;(8)构件版本的可能变更以及不确定性。此外,还有用户使用构件的上下文环境的多样性和不确定性、构件的开发者和构件的使用者的信息脱节等。

软件的测试不但困难,而且费时、费力和高成本。COTS 构件的这些特殊性又给其测试带来了新的问题和挑战。目前虽然对 COTS 构件的测试进行了相当多的研究,但是仍存在很多实质性的问题无法解决[1]。对任何产品的选择、交易和采用,除了微观上的具体检测和验证之外,宏观上对产品的可信度的了解和评估对用户的抉择具有相当大的指导意义。特别是像 COTS 构件这样的产品,这种宏观上的评估(以下简称评估)就更重要和更有价值。例如,参考文献[4]就是针对 COTS 构件测试的困难性和使用的风险问题,对欧洲多个国家中的几百个实际项目的开发过程中开发者是否使用 COTS 构件或使用现成的开源软件资产的决策进行了研究。但该文只是基于调查的实验性研究,仅总结出了开发者直觉的决策过程,没有提出具有普遍意义的决策指南。

针对以上问题,本文首先介绍了 COTS 构件可信度度量的概念,然后给出构件测试决策的若干模型,用以指导用户在 COTS 构件交易过程中对构件进行何种程度的测试

*基金项目:福建省自然科学基金资助项目(A0810013)

做出选择。从而能在较好地进行风险管理和控制的前提下尽量减少测试的时间和成本。从更广的角度，COTS 构件的测试和选用以及成本问题也属于信息安全的经济学范畴，因此，从经济学的角度对此进行研究具有深刻的意义[5]。

1 COTS 构件可信度度量

任何产品的交易达成都依赖于两大方面：微观上的具体检测和验证；宏观上客商之间的信用和对交易历史等信息的了解与评判。例如，客户对生产商、供应者、品牌、产品的返修率、其他人或机构对产品的反馈意见、评价、投诉等。但是，普通商品（包括计算机硬件）都可能由于生产时间、地点、生产批次、所用的原材料等的细微差别，甚至不同的生产线和生产线上的工作人员的不同，而导致同一品牌同一型号的产品本质上的差别。而软件产品却不存在这样的问题，同一版本的软件的功能、性能和其他一切质量指标都是相同的。因而，其交易信息和历史数据的可信度和可用性更高。事实上，几乎所有的软构件库都存储和提供这些数据，例如青鸟构件库、REBOOT、上海构件库等。此外，软件特别是 COTS 构件的测试的困难性也从另一个侧面突出了交易信息和历史数据的作用和依赖性。例如，Voas 提出构件认证策略是：独立认证实验室大量执行构件测试，独立发布测试结果[6]。但是，即使是最权威的第三方测试也无法完全取代用户本身的测试。

COTS 构件可信度度量也是十分复杂、困难的，目前尚无统一的标准。例如，Kunda 突出强调了供应商信誉、用户经验[7]；Ballurio 等人根据供应商的财务能力、市场稳定性、管理能力、研发能力和产品支持能力，从供应商能力的角度，研究降低 COTS 软构件的选择风险[8]；Jaccheri 等人则认为要重点评估 COTS 软构件的获取成本、拥有成本、市场占有量、市场占有率和许可类型[9]。通过对一些已有的有代表性的研究结果和典型的构件库管理标准（如 NATO、青鸟构件库、REBOOT、上海构件库等）的综合研究，本文认为没有任何一个单独的测量单元是足够的，必须使用多个有关的变量来描述和度量，因此 COTS 构件可信度必须包括以下几个方面：

（1）供应商。供应商的信誉、能力等。

（2）交易历史。交易历史与个人信用历史相似，如银行在放贷或放宽信用限制之前会检查个人信用历史。在 COTS 构件交易中，交易历史包含客户与多个商家的交易档案以及商家与多个客户的交易档案。例如，客户的退货、反馈意见、评价、投诉等。

（3）中介、第三方权威机构对构件的认证和测试结果。交易信用级别随着可信任中介对损失做出担保而提高。对于无交易历史的新商家或新客户更是如此：他们可能不会进行昂贵的交易，直到可信任的中介进行担保。中介也可以提供额外的保护措施，以对抗不可控的、昂贵的大笔交易。

（4）其他变量。在风险评估中另外需要考虑的变量是时间（软件退役、供应商不再进行产品支持等；开发商、供应商破产或出局）。

表 1 给出了 COTS 构件可信度度量的相关变量。

表 1 COTS 软构件可信度度量的相关变量

类别	因 素	类别	因 素
供应商	能力成熟度(CMM)	交易历史	构件被检索、察看次数
	市场占有率		构件被复用次数
	市场占有量		问题报告次数
	市场稳定性		退货/返修率
	财务能力		复用者满意度
	管理能力		…
	研发能力	成本	获取成本
	产品支持水平		拥有成本
	信誉	中介	中介担保
	培训		第三方机构认证/测试
	许可类型	其他	时间
	交货时间		…

即使建立了可信度度量的相关变量，对于 COTS 软构件的评估目前仍然没有公认的标准和方法。许多研究者将 COTS 软构件评估看作多准则决策问题 MCDM（Multi-Criterion Decision Making）。对于 COTS 软构件的可信度评估，MCDM 的多属性决策 MADM（Multi-Attributes Decision Making）中的加权评分法（Weighted Score Method）是一种有效的相对可行和易于操作的方法。该方法是：对于每个候选构件采用下面的算式进行评分：

$$\text{Score } A=\sum_{j=1}^{n}(Weight_j \times Score_{ij}) \quad (1)$$

其中，A 代表候选构件，j 代表第 j 个属性，n 是属性总数。

2 基于信用模型的风险分析

一个构件的交易过程的总风险可以设计成一个由交易费用和信用度量值决定的函数。首先，风险是一个货物或服务的费用的函数：谨慎的买家在进行昂贵的采购前，会有更多的考虑。同样地，商家并不担心进行一个孤立的、费用低下的微流程中损失收入，但随着一笔交易金额的提高或者微流程数量的提高，风险也将相应提高，因此商家也会提高对于收入和费用的注意力（包括质量与费用）。就客户而言，对于可信度高的构件的交易，其风险就较低，反之则风险就上升。而对商家来说，他们也可根据客户的信用度对交易风险进行分析。

风险变量一旦确立，交易行为和交易流程就可以根据风险来确定。交易行为可归纳为验证和授权两个方面。

（1）验证：对客户，是质疑由商家给出的账单和产品质量的可信性；对 COTS 构件，客户完成在线交易之前，难以完全测试产品，但又无法相信商家的保证，即保证软件下载后能被成功安装，并包含所有宣称的功能和性能。一个解决方案是：放弃验证小额的交易，或检验随机选定的微流程，特别是对那些值得信任的商家。商家的一般策略是对每一笔消费检查客户的授权信息（包括购买力、支付信息和背景）。如果验证的成本太高，商家也会根据交易费用和客户的信用度选择验证的方式

和方法。

(2)授权:交易费用的多少以及对商家的信用则会在很大程度上影响客户的购买行为,例如,要对拟购买的构件进行级别的测试、是否达成交易等等。对商家而言,则要考虑当客户被授予购买服务和商品的权力后,是否能相信他们不会滥用权力。例如,是否可以相信他们不会侵犯版权、超越使用范围和权限等,常用方法是在给客户授权时限制其权力,信用等级低的客户将受到更大的限制。

3 构件测试的决策模型

3.1 基于布尔逻辑的模型

这是一个最简单的模型。矩阵中,V 表示一个应该被检验的交易流程,无需验证的行为圈入可信区域,区域边界是信用边界。如图 1 所示,交易历史不良的客、商,尽管交易金额/重要性不大,但每个交易流程都需要被验证。交易历史优良的,则只需重点检验大额/重要的交易,也即对交易信用历史记录差的客、商,其每一项流程都必须被检验。而对于交易信用历史记录良好的,检验/测试的强度随着交易金额/重要性的增加而增加。

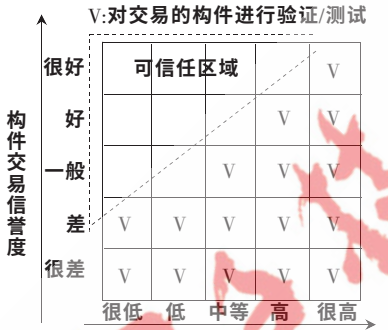

图 1 基于布尔逻辑的决策模型

3.2 基于模糊逻辑的模型

“小额交易”、“优良交易历史”等术语可方便描述度量单元。但是,对于同样程度的检验,即使是检验同样交易额的交易,检验缺乏交易历史的客户比检验具有优良交易历史的客户更有意义。因此,有必要进行加权处理以得到更加精细的、不同的行为度量值。

图 2 描述了在变化的交易历史中,权值对行为级别的影响。例如,交易历史很好的客、商在 50 次交易过程中可以只检验一次(V/50)或其测试强度为 1/50。图 2 中,20 V 表示对交易历史很差的客、商,每次交易都需要检验/测试,而且需要通过各种不同的方法检验/测试,包括对客户与其他商家、可信任中介做彻底的咨询,考察客户之前的交易等,或称其测试强度为 20。

这样的加权体系形成了一个加权信用边界,边界上的最高值是 20V,最低是 V/70。加权信用边界是一个由平滑插值的方式形成的三维边界。图 2 中的虚线划出了加权信用边界。显然,交易价/交易数量越多(如微流程),信用记录越差,检验/测试的要求越高,作用也越显著。

但是,加权决策矩阵中的具体数字不容易确定,而且“20V”这样的说法也不确切。一种可行的方法是用基于模糊逻辑的矩阵来解决,如图 3 所示。模糊逻辑的一个好处是使用语言用词(如“一般”,“很好”,“很差”

图 2 加权决策模型

等),可信任的中介和权威机构能更容易标注矩阵中的实体。语言用词覆盖了值的一个范围,而不是孤立的一个“散”的值,这个优点使其能在知识处理系统(如模糊逻辑专家系统)中得到应用。基于模糊逻辑的专家系统可以由数学函数,例如成员函数来表示语言用词的值。因此,模糊逻辑矩阵能用一组有助于推理的模糊成员函数集替换。

图 3 模糊决策模型

在模糊决策矩阵中,具体的数值由标准化的或中介定义的语义变量替换。例如,交易记录优良且只进行“一般”性交易时的检验/测试强度是低 LV(Low Verification)。

3.3 决策模型的传播

对于 COTS 构件这样的交易,客户通常在联系商家之前,会与若干可信任的中介联系。COTS 构件交易要求供应商、客户和所有中介之间有相互的信用。因此,既有客户与中介之间的信用关系,又有可信任中介 TI(Trusted Intermediary)与经纪人(代理商)之间的关系。这些信用关系的数量随着客户与商家之间可信任中介数量的增加而增加。

客户、中介和商家之间存在不同的信用-行为关系。中介中,有的中介与其他中介之间可能不存在可信任的关系,而是一个默认的关系。要计算客户与商家之间的单一信用-行为值,需要形成一个涵盖他们之间所有流程的总的信用-行为关系。在交易和验证/测试决策时,必须把客户与商家的各种信用-行为关系(称为信用行为-关系链)简化成一个单独的值,这个值可由覆盖所有流程的值构成的所有信用-行为关系的合成得到。

例如,图 4 是一个描述客户与可信任中介之间的决

策矩阵。矩阵中的变量是交易历史和交易数量。图 5 是中介和经纪人之间类似的矩阵。矩阵中每一个值表示一个类似于加权决策模型中的验证级别。

图 4 的矩阵是基于变量是构件交易信誉度和构件交易价/交易数量的决策模型。图 5 是基于满意度指数和构件交易价/交易数量的决策模型。满意度指数表明了一类客户的平均交易历史水平，或是可信任的中介基于其客户提交的满意度报告确定的。在这里，合成操作指的是用图 5 所示的矩阵来调整使用如图 4 所示的矩阵交易风险或者帮助对构件的验证/测试决策。

合成操作可以是减法运算、取最小值运算、取平均值运算，还可以是几种运算的组合。图 6 给出了对图 4 和图 5 执行某些合成运算的部分结果的示例。

图 4 客户与中介的决策矩阵

图 5 中介与经纪人的决策矩阵

图 6 决策矩阵合成操作示例

4 决策过程和应用

本方法已应用于某银行的国际贸易结算系统的构件测试决策中。系统已实现的部分包括基本业务功能构件 29 个，其中自主开发 10 个，委托开发/购买 19 个；系统管理和维护构件 12 个，其中自主开发 4 个，委托开发/购买 8 个。出于对可靠性的特殊要求，以往对委托开发/购买的构件的测试投入的成本相当大。而应用本模型辅助决策，且采取了比文中的模型更加谨慎的措施（把信誉度降低或/把交易价提高），测试代价约减少了 50%。采用对比实验通过测试分析和初步运行的对比研究，没有发现显著差异。其决策和测试过程的大致步骤如下：(1)根据表 1 和式(1)确定交易信誉度；(2)交易价/数量由构件的实际价格、该构件在系统中的比重（价格比重、规模比重、重要性比重等）、公司的规模和财务能力确定；(3) 谨慎度调整（提高或降低交易信誉度和交易价/数量的等级）；(4) 根据选择的测试决策模型确定测试强度（例如本试验应用选取加权模型）；(5)选择合适的构件测试方法[1,10]按确定的测试强度要求进行测试。

本文给出的 COTS 构件可信度度量和测试决策模型，可以指导用户在 COTS 构件交易过程中对构件进行何种程度的测试做出选择并对风险管理和控制提供帮助，从而帮助用户在能较好地进行风险管理和控制的前提下尽量减少测试的时间和成本。COTS 软构件评估和测试的决策也是传统的信息系统理论所无法涵盖的。本文通过对影响构件测试决策复杂的、多变量的抽象，最终以矩阵的方式实现对模型的语义定义。矩阵描述的模型具有易于理解和应用、可操作性强的优点。如何把本模型结合构件安全性和可用性的投入成本的权衡[11]是值得进一步进行研究的。

参考文献

[1] 毛澄映，卢炎.生构件软件测试技术研究进展[J].计算机研究与发展，2006，43(8)：1375-138.
[2] 余金山，万静.一个基于 Internet 的软构件信息系统的研究与实现[J].信息与控制，2002，31(4)：357-362.
[3] 原欣伟，覃正.COTS 软构件评估研究综述[J].计算机应用研究，2006，23(7)：5-7.
[4] Li PJingyue, PREIDAR C, ODD P N., et al.An empirical study on decision making in off-the-shelf component-based development. Proceedings of the 28th international conference on Software engineering[C]. ACM, 2 Penn Plaza, Suite 701 New York NY USA, 2006：897-900.
[5] ROSS A, TYLER M. The economics of information security [J]. Science,2006,314(5799)：610-613.
[6] VOAS J. Developing a usage-based software certification process[J]. IEEE Computer, 2000(8)：32~37.
[7] STACE K D. Social technical approach to COTS software evaluation [J]. Lecture Notes in Computer Science, 2003,2693：64-84.
[8] BALLURIO K, SCALZO B, ROSE L. Risk reduction in COTS software selection with BASIS [J]. Lecture Notes in Computer Science, 2002,2255：31-43.
[9] JACCHERI L, TORCHIANO M. Classifying COTS products[J]. Lecture Notes in Computer Science, 2002,2349：246-255.
[10] 郑成文，韩柯，张海粟. 一种改进的软件自适应随机测试策略[J].计算机工程，2011，37(16)：82-83，100.
[11] IOANNIDIS C, PYM D, WILLIAMS J. Investments and trade-offs in the economics of information security [J]. Lecture Notes in Computer Science, 2009,5628：148-166.

（收稿日期：2011-10-10）

作者简介：
余金山，男，1952 年生，教授，主要研究方向：软件工程，网络计算，人工智能应用等。