

文章编号: 1000-5013(2011)02-0175-03

# Email 系统特征交互问题的 $\pi$ -演算检测

李文翔, 潘孝铭

(华侨大学 计算机科学与技术学院, 福建 泉州 362021)

**摘要:** 采用  $\pi$ -演算给出基于客户端-服务器模式的 Email 系统, 以及系统中特征的行为描述; 然后, 利用  $\mu$ -演算描述和分析 Email 系统中存在的特征交互问题. 最后, 利用移动工作台软件工具, 验证基于  $\pi$ -演算描述的移动并发系统.

**关键词:** 特征交互; Email 系统;  $\pi$ -演算;  $\mu$ -演算; 移动工作台

**中图分类号:** TP 311.5

**文献标志码:** A

特征交互问题最早是由美国贝尔通信实验针对电信系统提出的<sup>[1]</sup>. 它主要表现为软件系统中可组合的服务或者特征之间的非预期的相互影响, 而这些影响会导致系统无法向用户提供正常的服务或者影响服务的质量. 2001 年 10 月, Feature Interaction Workshop 国际会议上明确地提出了研究电信领域以外的其他软件系统中存在的特征交互问题<sup>[2]</sup>. 目前, 应用于特征交互问题检测, 主要有软件工程方法, 形式化方法和在线检测方法 3 个方法<sup>[3-4]</sup>. 形式化方法主要在需求规约阶段对基础子系统和特征进行描述, 然后分析和检测特征之间的交互问题. Milner 等<sup>[5-6]</sup>提出以进程间的移动通信为研究重点的并发理论—— $\pi$ -演算. 其主要优点是可以用一个动态通信结构来表示系统, 不仅可以传递变量和值等, 也可以传递通道名, 且将这些实体统称为名字而不作区分.  $\mu$ -演算<sup>[7]</sup>是 HML (Hennessy-Milner Logic) 逻辑的扩展. 它增加了最大不动点和最小不动点的概念, 比 HML 具有更强的表达能力, 可以处理无限状态的进程. 本文采用  $\pi$ -演算对 Email 模型进行行为描述, 利用  $\mu$ -演算对特征交互进行描述分析和检测.

## 1 Email 系统模型的 $\pi$ -演算描述

图 1 为 Email 系统模型. 它包含了一系列的用户 (Client) 和一个服务器 (Mailer). 用户和服务器之间的通信是异步进行的. 每个用户都有一个唯一的地址来标识自己, 用户可以发送和接收邮件; 服务器可以将邮件发送给用户.

用户  $i$  有两个通信通道: 输出动作 network 和输入动作 mailbox. 前者用于用户  $i$  向服务器发送邮件, 后者用于用户  $i$  接收来自服务器的邮件, 即用户  $i$  的收件箱. 在发送邮件前, 用户  $i$  有一个输出动作  $iM$ , 表示发送前的准备工作. 接收到邮件后, 用户  $i$  执行输出动作  $rM$ , 表示接收后的用户  $i$  的一些后续操作. 采用基于 New Jersey SML 语言编辑器的移动工作台 (Mobility Workbench, MWB) 工具<sup>[8-9]</sup>, 分析和验证基于  $\pi$ -演算描述的移动并发系统. 用户 A 的  $\pi$ -演算描述如下:

agent ClientA(msg, agentA, agentB, sender, receiver, network, mailboxA, iAM, rMA) = 'iAM. 'network<msg, agentA, agentB>. ClientA<msg, agentA, agentB, sender, receiver, network, mailboxA, iAM, rMA> + mailboxA (msg, sender, receiver). 'rMA. ClientA<msg, agentA, agentB, sender, receiver, network, mailboxA, iAM, rMA>

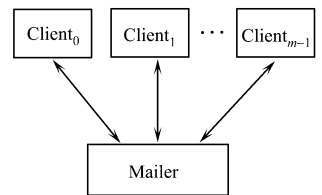


图 1 Email 系统模型

Fig. 1 Email system model

收稿日期: 2009-10-21

通信作者: 潘孝铭(1968-), 男, 副教授, 主要从事形式化技术的研究. E-mail: panxiaom@hqu.edu.cn.

基金项目: 福建省自然科学基金资助项目(A0810013); 华侨大学科研基金资助项目(04BS313)

其中: agentA 和 agentB 分别表示用户 A 和用户 B 的地址; msg 表示所传递的邮件; mailer 在整个模型中只起到分发邮件的作用, 它拥有一个 network 输入动作, 用于接收来自用户的邮件, 以及与多个用户进行通信的通道 mailbox1, mailbox2, ..., mailboxn. 这里, 考虑 2 个用户之间的邮件传递. 因此, mailer 在 MWB 中的  $\pi$ -演算描述如下:

$$\text{agent Mailer}(\text{msg}, \text{agentA}, \text{agentB}, \text{sender}, \text{receiver}, \text{network}, \text{mailboxA}, \text{mailboxB}) = \text{network}(\text{msg}, \text{sender}, \text{receiver}). ([\text{receiver} = \text{agentB}] \text{'mailboxB'}(\text{msg}, \text{sender}, \text{receiver}). \text{Mailer}(\text{msg}, \text{agentA}, \text{agentB}, \text{sender}, \text{receiver}, \text{network}, \text{mailboxA}, \text{mailboxB}) + [\text{receiver} = \text{agentA}] \text{'mailboxA'}(\text{msg}, \text{sender}, \text{receiver}). \text{Mailer}(\text{msg}, \text{agentA}, \text{agentB}, \text{sender}, \text{receiver}, \text{network}, \text{mailboxA}, \text{mailboxB}) + \text{Mailer}(\text{msg}, \text{agentA}, \text{agentB}, \text{sender}, \text{receiver}, \text{network}, \text{mailboxA}, \text{mailboxB}))$$

整个模型可以描述如下:

$$\text{agent Mail}(\text{iAM}, \text{iBM}, \text{rMA}, \text{rMB}) = (\text{'msg'}, \text{agentA}, \text{agentB}, \text{sender}, \text{receiver}, \text{network}, \text{mailboxA}, \text{mailboxB}) (\text{ClientA}(\text{msg}, \text{agentA}, \text{agentB}, \text{sender}, \text{receiver}, \text{network}, \text{mailboxA}, \text{iAM}, \text{rMA}) | \text{ClientB}(\text{msg}, \text{agentA}, \text{agentB}, \text{sender}, \text{receiver}, \text{network}, \text{mailboxB}, \text{iBM}, \text{rMB}) | \text{Mailer}(\text{msg}, \text{agentA}, \text{agentB}, \text{sender}, \text{receiver}, \text{network}, \text{mailboxA}, \text{mailboxB}))$$

根据  $\pi$ -演算的推理规则, 模型存在着一条路径从用户 A 发送邮件给服务器 mailer; 然后, 再由 mailer 转发给用户 B. 即  $\langle \text{'iAM'} \rangle \langle \text{'t'} \rangle \langle \text{'rMB'} \rangle$ . 用 MWB 工具对上述描述进行调试, 证明了  $\text{Mail}(\text{iAM}, \text{iBM}, \text{rMA}, \text{rMB}) | = \langle \text{'iAM'} \rangle \langle \text{'t'} \rangle \langle \text{'rMB'} \rangle \text{TT}$ .

Email 系统模型中,  $\text{Mail}(\text{iAM}, \text{iBM}, \text{rMA}, \text{rMB}) | = \langle \text{'iAM'} \rangle \langle \text{'t'} \rangle \langle \text{'rMB'} \rangle \text{TT}$  的验证结果表明: 用户 A 在向服务器 M 发送邮件之前做了一些准备工作 'iAM', 接着发送邮件到服务器, 即  $A \rightarrow M; \{\text{msg}, \text{agentA}, \text{agentB}\}$ ; 服务器 M 在接收到邮件之后, 根据 A 提供的目标接收者 B, 将邮件转发给用户 B, 即  $M \rightarrow B; \{\text{msg}, \text{agentA}, \text{agentB}\}$ ; 用户 B 在接收到邮件之后, 进行了 'rMB' 动作, 用来表示接收邮件的后继动作. 因此, 整个模型满足了 Email 系统的基本功能, 即 A 向 B 发送邮件.

## 2 Email 系统的特征交互分析

文献[4]给出了 Email 系统中所有的特征. 此处, 只考虑一个最基本的特征, 即自动回复. 用户申请自动回复服务后, 一旦用户接收到邮件, 就会自动发送一封邮件回复给定发送方. 因此, 在上述的模型描述中, 在用户 mailbox 动作后面添加一个输出动作 network. 考虑到后面问题描述的方便, 将这个输出动作添加到输出动作 r 之后. 一个 client 的 MWB 中  $\pi$ -演算的描述如下:

$$\text{agent ClientA}(\text{msg}, \text{agentA}, \text{agentB}, \text{sender}, \text{receiver}, \text{network}, \text{mailboxA}, \text{iAM}, \text{rMA}) = \text{'iAM'}. \text{'network'}(\text{msg}, \text{agentA}, \text{agentB}). \text{ClientA}(\text{msg}, \text{agentA}, \text{agentB}, \text{sender}, \text{receiver}, \text{network}, \text{mailboxA}, \text{iAM}, \text{rMA}) + \text{mailboxA}(\text{msg}, \text{sender}, \text{receiver}). \text{'rMA'}. \text{'network'}(\text{msg}, \text{agentA}, \text{agentB}). \text{ClientA}(\text{msg}, \text{agentA}, \text{agentB}, \text{sender}, \text{receiver}, \text{network}, \text{mailboxA}, \text{iAM}, \text{rMA})$$

当都定制了自动回复功能的用户 A 和 B 进行邮件传递的时候, 模型中就存在着特征交互. 即当用户 B 接收来自用户 A 的邮件后, 就自动发送了回复邮件; 而 A 收到邮件后, A 也向 B 发送回复邮件, B 收到邮件后再次向 A 发送回复邮件.

如此往复, A 和 B 之间就存在着一条循环路径, 且此循环是无条件的. 因此, 在 MWB 中以这样的公式表示:  $\langle \text{'iAM'} \rangle \langle \text{'t'} \rangle \langle \text{'rMB'} \rangle (\text{nuZ}. (\langle \text{'t'} \rangle \langle \text{'t'} \rangle \langle \text{'rMA'} \rangle \langle \text{'t'} \rangle \langle \text{'rMB'} \rangle Z))$ . 然后, 利用 check 命令验证模型 Mail 是否满足上述公式. 若是, 则模型中存在着特征交互.

$\text{Mail}(\text{iAM}, \text{iBM}, \text{rMA}, \text{rMB}) | = \langle \text{'iAM'} \rangle \langle \text{'t'} \rangle \langle \text{'rMB'} \rangle (\text{nuZ}. (\langle \text{'t'} \rangle \langle \text{'t'} \rangle \langle \text{'rMA'} \rangle \langle \text{'t'} \rangle \langle \text{'rMB'} \rangle Z))$  在 MWB 中的验证结果表明: 在用户 B 确认接收到来自用户 A 发出的邮件时, B 在动作 'rMB' 之后做了一个自动回复动作, 即  $B \rightarrow M; \{\text{msg}, \text{agentB}, \text{agentA}\}$ ; 服务器 M 在接收到这个回复邮件时, 根据 B 提供的邮件接收者将邮件通过通道 mailboxA 将邮件转发给用户 A. 此时, 在用户 A 确认接收到邮件时, 由于

自动回复功能, A 发送了回复邮件; 而服务器 M 又将回复邮件转发给 B.

如此往复, 用户 A、服务器 M 和用户 B 这 3 者之间就陷入了不断发送和转发回复邮件的无限循环步骤, 则系统就发生了自动回复特征交互问题.

### 3 结束语

对于 Email 系统的所有特征, 只对自动回复特征进行了描述和分析. 对于消息过滤和自动回复等其他特征交互问题, 未作描述和分析. 同时, 在研究过程中, 出现了状态空间爆炸的问题, 这也是进一步要解决的问题.

#### 参考文献:

[1] CAMERON J E, GRIFFETH N, LIN Y J, et al. A feature interaction benchmark for IN and beyond[J]. IEEE Communications Magazine, 1993, 31(3): 64-69.

[2] PULVERMUELLER E, SPECK A, COPLIEN J, et al. Feature interaction in composed systems[C]//Proceedings of the Workshops on Object-Oriented Technology. London: Springer-Verlag, 2001: 86-97.

[3] KIMBLER K, BOUMA L G. Feature interactions in telecommunications and software systems (V)[M]. Amsterdam: IOS Press, 1998.

[4] CALDER N, MAGILL E. Feature interactions in telecommunications and software systems (VI)[M]. Amsterdam: IOS Press, 2000.

[5] MILNER R. Communicating and mobile systems: The  $\pi$ -calculus[M]. Cambridge: Cambridge University Press, 1999.

[6] MILNER R. The polyadic  $\pi$ -calculus: A tutorial[C]//BAUER F, et al. Logic and Algebra of Specification. Berlin: Springer-Verlag, 1992: 203-246.

[7] BRADFIELD J, STIRLING C. Modal  $\mu$ -calculus[C]//BLACKBURN P, et al. The Handbook of Modal Logic. New York: Elsevier Science Ltd, 2006: 721-756.

[8] VICTOR B. The mobility workbench user's guide: Polyadic version 3. 122[R]. Uppsala: Uppsala University, 1995.

[9] VICTOR B. A verification tool for the polyadic  $\pi$ -calculus[R]. Uppsala: Uppsala University, 1994.

## Detection of Feature Interactions in Email System Based on $\pi$ -Calculus

LI Wen-xiang, PAN Xiao-ming

(College of Computer Science and Technologe, Huaqiao University, Quanzhou 362021, China)

**Abstract:** In this paper, the email system based on client-server and the features are defined in a behavioral description by using  $\pi$ -calculus. Then we use  $\mu$ -calculus to describe and analyze the feature interactions problems in this system. And at last we use a tool called mobility workbench to prove the mobile concurrent system described by  $\pi$ -calculus.

**Keywords:** feature interactions; Email system;  $\pi$ -calculus;  $\mu$ -calculus; mobility workbench

(责任编辑: 陈志贤      英文审校: 吴逢铁)