移动 Agent 的一种支持安全与容错的迁移机制

王 勇[1]，王忠群[1]，韦良芬[2]

（1. 安徽工程科技学院 计算机系，安徽 芜湖 241000；
2. 三联职业技术学院 计算机系，安徽 合肥 231000）

摘 要：移动 Agent 计算模式将成为未来网络计算的主流模式。移动 Agent 的迁移机制是其技术核心之一，受到了广泛的关注。为了提高移动 Agent 迁移的可靠性和安全性，提出一种支持安全与容错的迁移机制。该机制利用结构化迁移机制寻址，并引入分布式事务、可靠认证与加密等机制，使得移动 Agent 在迁移过程中能有效保护主机与移动 Agent 的安全性，并提供容错支持。

关键词：移动 Agent；迁移；分布式事务；安全；容错

中图分类号：TP393.08；TP302.8　　**文献标识码**：A　　**文章编号**：1673－629X(2007)03－0169－03

A Migration Mechanism of Mobile Agent System Supporting Security and Fault－Tolerance

WANG Yong[1], WANG Zhong-qun[1], WEI Liang-fen[2]

(1. Department of Computer Science, Anhui University of Technology and Science, Wuhu 241000, China;
2. Department of Computer Science, Sanlian Vocational Institute of Technology, Hefei 231000, China)

Abstract: Mobile agent will be one of the major modes of network computing in the future. The migration mechanism, the core technology of mobile agent, catches widely attention from both industry and academy. In order to improve the dependability and security of mobile agent system, a migration mechanism supported for security and fault－tolerance is proposed. On the basis of structured migration mechanism, achieving the reliability and security by means of distributed transaction, reliable authentication and encryption mechanism, this mechanism can effectively protect the host and the mobile agent, and provide support for fault－tolerance.

Key words: mobile agent; migration; distributed transactions; security; fault－tolerance

0 引 言

移动 Agent 是一个能够在异构网络中自主地从网络中的一台主机迁移到另一台主机，并可与其他 Agent 和资源交互的程序。如图 1 所示，其中 a 表示 Agent，(p0，p1，p2，p3，p4)表示移动 Agent 运行的基本环境，移动 Agent 能够在具有运行环境的服务器(Server)上自主移动，以完成特定的功能。移动 Agent 是 Agent 技术与分布式计算技术的结合体，具有移动性和自主性等特点。移动 Agent 计算模式将成为未来网络计算的主流模式。

作为移动 Agent 核心技术之一的迁移机制一直受到广泛关注。文献[1,2]提出一种结构化迁移机制，将移动 Agent 的旅行计划划分成七元组(迁移模式，旅行步控制，目标节点，人口方法 G/M，旅行计划更新方法，名字说明)，很好地解决了任务级迁移的旅行规程问题。但未提供一种有效的安全与容错支持的迁移机制。另一方面，安全性与容错问题一直是影响 Agent 系统应用与扩展的主要瓶颈问题。

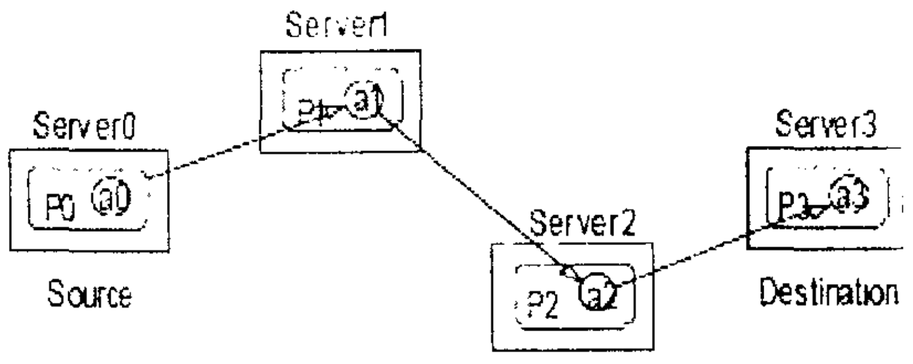

图 1 移动 Agent 的执行

1 移动 Agent 的安全性与容错问题

1.1 安全性问题

移动 Agent 系统是由移动 Agent 和多个为移动 Agent 提供服务的主机组成的，并不能保证整个系统中

收稿日期：2006－05－28

基金项目：安徽教育厅自然科学基金重点项目(2006KJ016A)

作者简介：王 勇(1979－)，男，安徽舒城人，硕士研究生，研究方向为分布式计算、软件工程、容错技术等；王忠群，教授，研究方向为软件工程、分布式计算、工作流技术等。

每个主机都是完全可靠的,其中有可能存在一些恶意主机,这些恶意主机试图攻击移动 Agent,窃取移动 Agent 的重要信息,更为严重的是,对 Agent 的信息进行篡改,使之产生不正确的结果[3]。因此,当存在潜在的恶意环境时,移动 Agent 的保护问题尤为重要。对移动 Agent 的保护,具体到移动 Agent 所包含的数据来说,主要是保护移动 Agent 数据的机密性和完整性。

目前,研究最多的数据保护方法是基于检测的保护措施与主动的保护措施[3]。基于检测的保护措施是根据对运行环境进行检测,判断其是否安全,以及对移动 Agent 进行检测来判断其是否受到了攻击并遭受破坏。主动的保护措施是让移动 Agent 在安全环境上运行,要让移动 Agent 在不信任主机上完全地安全运行。

1.2 容错问题

移动 Agent 在迁移过程中,可能因为网络状态的动态变化、网络节点的崩溃或离线、链路故障或拥塞、传输延迟等引起移动 Agent 不能正确迁移。因此,随着研究深入,必须要保证系统可靠的容错支持。

在系统中,可以通过复制的方法来支持容错[4~6]。但采用复制的方法可能会引起在 Agent 的多个副本在网络中运行,从而破坏移动 Agent 执行的"exactly－once"语义,并且管理多个 Agent 副本会加重系统的负荷。文中在文献[1,2,7]提供的结构化迁移机制的基础上,提出一种支持安全与容错的迁移机制。该机制保证了迁移的"exactly－once"语义、保护 Agent 与主机的安全并提供对用户透明的容错支持。

2 移动 Agent 的迁移机制框架

2.1 结构化迁移机制概述

Agent 的移动类似于人的旅行。人的旅行一般有两种方式:一种是随意旅行,等旅行完一个地方后再决定下一个目的地;另一种是事先定好一个计划,然后按照计划旅行。同样,Agent 的移动方式也类似地有这样两种,分别称之为命令方式和计划方式。在命令方式下,Agent 系统提供一条移动命令,Agent 通过调用这条命令,并附以适当的参数如目的地地址,可以随时移动到任何目的地。结构化迁移机制主要针对计划方式,旅行计划由旅行模式和若干个旅行步组成,一个旅行步说明了一站旅行要求,旅行模式是对这若干个旅行步的解释方法。结构的方式主要来描述一个旅行步,同时对旅行步的解释也按照固定的规程进行,一旦旅行计划制定完成后,就不可以随意进行修改,只能在旅行计划全部解释完之后才能修改和调整原来的旅行计划。一个旅行步包含了 Agent 一次移动所需的所有信息,包括目标节点地址、在目标节点上应该完成的任务等等。采用图 2 所示的结构来描述旅行步信息。具体参考文献[1,2],在此不再赘述。

旅行步控制	目标节点	入口方法		旅行计划更新方法	名字说明
P	H	G	M	T	Name

图 2 旅行步结构

2.2 分布式事务概述

事务是指对特定共享资源的一组不可分割的操作,具有原子性、一致性、隔离性、持续性(即 ACID)等特征。原子性是指事务的发生是不可分割的;一致性指事务不能破坏系统的恒定性;隔离性指并发的事务不能相互干扰;持续性指一旦事务得到提交,改变将是永远存在的。

在分布式环境中,如果事务执行在同一物理位置执行,该事务称为本地事务;如果一个事务访问多个分布在不同地方的独立资源,称这种事务为分布式事务,分布式事务同样具有 ACID 特征。

分布式事务的要么不做、要么全做的特性能够很好地解决分布式环境下数据一致性问题。在事务的提交协议中,可以采用 2PC 提交协议。在两阶段提交协议的第一阶段,协调者询问所有的参与者是否准备好提交;在第二个阶段,协调者通知他们提交(或放弃)事务。如图 3 所示。

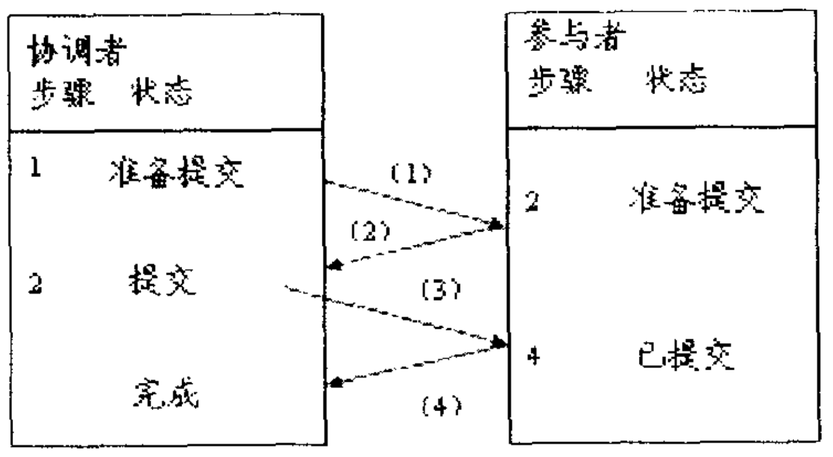

图 3 两阶段提交协议

2PC 提交协议具体算法如下:

第一阶段:(1)、(2);第二阶段:(3)、(4)。

(1)协调者向事务所有者发送"能否提交?"请求。

(2)当参与者收到"能否提交?"请求后,他将向协调者应答它的投票(Yes 或 No)。在投 Yes 票之前,他持久存储所有对象;如果投 No 票,参与者立即放弃。

(3)协调者收集所有的投票(包括它自己的投票)。

a. 如果不存在的故障并且所有的投票均是 Yes 时,协调者决定提交事务并向所有参与者发送"提交"请求。b. 否则,协调者决定放弃事务,并向所有投 Yes 票的参与者发送"放弃"请求。

(4)投 Yes 票的参与者等待协调者发的"提交"或者"放弃"请求。一旦参与者接收到任何一种请求消息,它根据该请求放弃或者提交时务。如果请求是提交事务,那么他还要向协调者发送一个"已提交"来确

认事务已经提交。

2.3　移动 Agent 安全认证与加密方法概述

移动 Agent 运行在 Internet 上,有可能遭到外来恶意 Agent 的攻击,网络中的节点也有可能遭受到非法 Agent 的侵扰而引起服务失效、系统崩溃等严重后果。因此,本机制采用信任站点服务来认证注册的合法用户的移动 Agent,并通过登记日志的方法,提供间接安全(当发生故障时可跟踪日志,找到谁该为故障负责)。

本机制在移动 Agent 中传送中,采用先将移动 Agent 加密,再将加密后的移动 Agent 传送到目标站点。只有目标站点拥有解码的密钥,在目标站点利用密钥解码,这样防止移动 Agent 遭受恶意站点的篡改。

2.4　机制描述

如图 4 所示,信任服务(Trust service)负责移动 Agent 的认证与授权。通过对移动 Agent 的认证与授权机制来确认合法的 Agent,以防止站点被恶意 Agent 破坏。可以在信任站点安排 Backup1 与 Backup2 为信任服务的复制,当信任服务失效时,可以通过选举算法[8]选出其中一个备份作为信任服务。迁移路径服务(travel service)为移动 Agent 寻找合适的目标主机(迁移路径服务器采用的迁移路径选择算法,具体参考文献[1,2,9])。H_i 为需要迁移 Agent 的节点。H_{i+1} 为迁移的目标节点。

下面就移动 Agent 的传送周期加以分析:

(1)源节点首先并向信任节点申请产生一个新 Agent,信任服务产生一个与注册的合法用户相关的一个身份标识(ID),并送回标识给该移动 Agent。

(2)当该移动 Agent 需要传送时,首先通过信任站点的迁移路径服务寻找合适的目标站点。

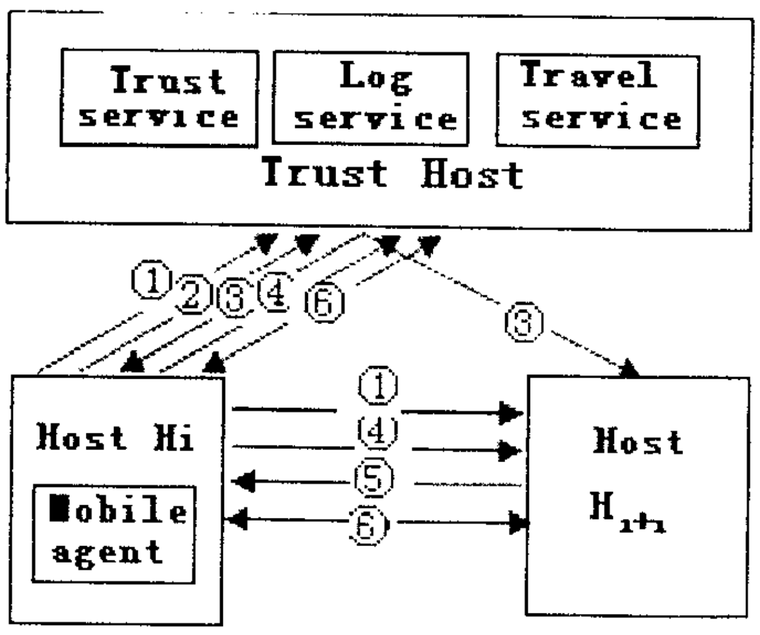

图 4　移动 Agent 的迁移过程

(3)当目标站点与移动 Agent 协商后,一个移动 Agent 的副本被传送到目标站点。笔者采用分布式事务与加密机制获得安全机制。分布式事务保证 Agent 迁移一致性,加密机制保护移动 Agent 免受攻击。

(4)当移动 Agent 迁移成功后,将删除源点的 Agent 副本,并使密钥非法等操作。若迁移出错则放弃迁移,重新开始下一次迁移转到步骤(2)。

(5)如此循环直到 Agent 完成任务。

具体算法如下:

1)Host H_i 开始分布式事务,目标主机 H_{i+1} 与信任节点被包含在该分布式事务中。

2)Host H_i 请求迁移 Agent 到 Host H_{i+1} 的认证。

3)信任节点产生一个密匙并将其复制,传送到 H_i 与 H_{i+1}。

4)在 H_i 节点利用密钥对 Agent 的复制进行加密,并将其传送到目标站点 H_{i+1}。

5)在目标节点利用密钥对传送来的复制进行解码,并在目标主机 H_{i+1} 中初始化 Agent 的拷贝以及确认接受。

6)H_i 开始启动 2PC 协议提交事务。若成功提交事务则提示结束,删除老的 Agent 副本,更新信任站点并使密钥非法。否则放弃事务。

在此算法中,可能产生的故障有:目标站点失效;Trust service 失效;移动 Agent 迁移通信故障;目标主机对移动 Agent 初始化与原 Agent 的不一致性。利用分布式事务的两阶段提交协议(2PC)的原子提交特性,事务要么全做,要么全不做。若事务提交成功,则 Agent 被成功迁移,若事务放弃,则 Agent 重新启动一个新事务,选择新的目标出口继续迁徙。

3　机制分析

3.1　移动 Agent 可靠迁移及容错

当 Agent 在迁移时发生故障,常见的方法是使用复制的方法[4]。但复制可能会引起多个复制在网络中同时运行,并且维护多个复制会加重系统开销。在本机制中,通过使用分布式事务可以提供容错从而避免使用复制的方法。在 Agent 迁移的过程中,发生故障,采用 2PC 提交协议可以保护移动 Agent 的一致性;在任何情况下发生的 Agent 出错,利用分布式事务的事务回滚机制,相当于移动 Agent 什么也没有做。可以让系统再次选择另一个目标主机开始下一个迁移。

3.2　保护主机

系统采用安全认证、授权机制,使得只有信任用户(trusted user)的移动 Agent 才能在信任主机中迁移。可以登记所有访问的移动 Agent 的相关信息(如移动 Agent 的拥有者、移动 Agent 的行为),一旦发生严重问题,可以查看登记的信息,了解情况。通过这种途径,也给系统提供间接的安全保护。

3.3　保护移动 Agent

保证移动 Agent 安全性包括各种方面。通过加密

(下转第 175 页)

3　反病毒传染分析

从上面的随机感染模型和实验可以看出,一旦计算机内有病毒并且获得运行机会,在很短的时间内会感染大量的用户资源,因此,如何控制病毒传染,或者病毒进行有限次传染后及时进行清除是反病毒领域面临的重要课题。对于已知病毒,病毒进行传染前能被反毒软件监测并清除。对于未知病毒,抑制病毒传染和及时检测出病毒相当困难,当前处于反病毒前沿广泛运用的技术,如虚拟机技术、启发式扫描、行为检测技术等等[4],也不能很好地解决对未知病毒的及时发现和清除问题。

消极传染性病毒传染的一般的方式是驻留内存、待机感染,这种病毒具备一定的隐蔽性,由于它对文件的感染主要取决外界程序的行为,相比积极性病毒传染,感染一定数目的文件时间较长。及时对内存扫描、检测和清除是对付这种病毒的主要手段[5]。这种病毒在目前的平台已经很少,取而代之的是驻留内存后采用积极传染的方式进行感染。相比消极传染,积极性传染的效率极高。由前面的结论可知,在当前计算机系统下,未知病毒的微观传染在用户态具备不可控性,反病毒传染需要向更微观的方向发展。未来的反病毒传染技术可以考虑建立在操作系统级,由操作系统监控程序运行,一旦发现程序对其他文件的自我复制行为,进行特征标记,当程序自动对其他文件的写操作超过一定数目时,由判断此程序可能为病毒,并做出相应措施,或交给用户处理,或由操作系统自身处理。

近年出现的内建 CPU 反病毒技术如 INTEL 的 EDB 和 AMD 的 EVP,能够对各种程序进行监视,阻止病毒在受保护的内存位置运行有害代码,是反病毒技术向更微观层次转变的趋势。

4　结束语

抑制传染是反病毒的主要手段之一,随着网络给计算机病毒传播带来的巨大便利,今后计算机系统面临更多病毒入侵的挑战。在保持现行计算机体系结构的前提下,深入分析计算机病毒的规律和发展趋势,克服操作系统的脆弱性,研究软硬件结合的反病毒技术,对反病毒领域的发展将起到重大的推动作用。

参考文献:

[1] Cohen F. Computational aspects of computer viruses[J]. Computers & Security, 1989,8(4):325－344.

[2] 傅建明,彭国军,张焕国. 计算机病毒分析与对抗[M]. 武汉:武汉大学出版社,2004.

[3] 张　波,张景肖. 应用随机过程[M]. 北京:清华大学出版社,2004.

[4] Szor P. The art of computer virus research and defense[M]. [s.l.]:Addison Wesley Professional,2005.

[5] Ford R. The future of virus detection[J]. Information Security Technical Report, 2004,9(2):19－26.

(上接第 171 页)

的方法,保证除了信任站点之外没有其他实例存取移动 Agent。因此,没有不信任的第三方能复制、改变、销毁移动 Agent。如果其中的某个信任站点攻击了 Agent,则登记的日志信息可以跟踪违反的主机,并确认责任。

4　结束语

移动 Agent 的可靠性与安全性问题是移动 Agent 研究的重要内容。文中从移动 Agent 迁移的角度,提出利用信任站点、基于分布式事务等机制的移动 Agent 迁移机制。该机制能很好解决由于网络的不可靠性等因素造成移动 Agent 在迁移过程中可能产生的失效等问题,提供了安全性与透明容错支持。

参考文献:

[1] 陶先平,吕　建,张冠群,等. 一种移动 Agent 结构化迁移机制的设计和实现[J]. 软件学报,2001,11(7):918－923.

[2] 张冠群, 陶先平,李　新,等. Mogent 系统迁移机制的设计与实现[J]. 计算机研究与发展,2001,38(9):1035－1041.

[3] 黄少寅,尹长青,高传善,等. 移动代码加密理论研究[J]. 计算机研究与发展,2003,40(11):1626－1634.

[4] Pleisch S, Schiper A. Approaches to Fault and Transactional Mobile Agent Execution－An Algorithmic View[J]. ACM Computing Surveys,2004,36(3):219－262.

[5] Roth V. Programming satan's Agents[C]// In Proc of the 1st Int Workshop on Secure Mobile Multi－Agent Systems. Montreal, Canada:[s.n.], 2001.

[6] Pleisch S, Schiper A. Modeling fault－tolerant mobile Agent execution as a sequence of agreement problems[C]// In Proc. of 19th IEEE Symposium on Reliable Distributed Systems (SRDS'00). Nuremberg, Germany:[s.n.],2000:11－20.

[7] 吕　建,陶先平,马晓星,等. Mogent 系统的设计、实现与应用研究[C]//全国软件与应用学术会议论文集. 南京:南京大学出版社,2005.

[8] 赵　靖,程　欣,崔　刚,等. 容错的移动代理框架及执行[J]. 计算机工程与应用,2005(1):144－147

[9] 李唯唯. 基于移动 Agent 的电子商务交易协商方案[C]// 全国软件与应用学术会议论文集. 南京:南京大学出版社. 2005.