一种改进的移动 Agent 通信模型①

黄成伟 贾宇波 蔡 浩 (浙江理工大学 信电学院 浙江 杭州 310018)

摘 要： 移动 Agent 系统的通信问题是阻碍其广泛应用于实践的最重要的因素之一。通过对已有的移动 Agent 系统通信机制的研究与分析，提出了一种改进的移动 Agent 通信参考模型。该参考模型分别从移动 Agent 命名与定位、移动 Agent 通信安全和移动 Agent 通信失效三个方面进行分析，在某种程度上解决了移动 Agent 的通信问题，并提高了移动 Agent 通信安全性。最后，对未来的工作做了展望。

关键词： 移动 Agent；通信机制；PED；通信失效

An Improved Communication Model for Mobile Agent

HUANG Cheng-Wei, JIA Yu-Bo, CAI Hao

(School of Information and Electronics, Zhejiang Sci-Tech University, Hangzhou 310018, China)

Abstract: Communication is one of the biggest obstacles for the application of mobile agent system. After analyzing the communication problems, this paper presents an improved communication model for mobile agent. It is performed based on the framework concerning three major areas: the naming and locating scheme of mobile agent, the security of mobile agent communication and the communication failure of mobile agent. The proposed model solves communication problems in some degree, and improves the safety of mobile agent. At last, future work is discussed.

Keywords: mobile agent; communication mechanism; PED; communication failure

自 19 世纪 80 年代以来，多 Agent 系统[1]已经成为最活跃的研究领域之一,Agent 技术被广泛应用于许多领域诸如网格计算、普适计算、语义 Web 和电子商务等。随着网络技术与分布式技术的不断发展，可以让智能 Agent 在 Internet 上自主移动并执行,以完成用户指定的任务,这就是移动 Agent 的最初构想。可以说移动 Agent 是 Agent 技术与分布式技术相结合的产物，它是 Internet 发展的必然趋势。

移动 Agent 的概念是 20 世纪 90 年代初由 General Magic 公开发中心在推出商业系统 Telescript[2]时提出的。简单地说，移动 Agent 是一个能够在运行过程中自主的从一台主机迁移到另一台主机，并可与其它 Agent 或资源交互的程序[3]。与传统的分布式技术相比，它具有很多优点，移动 Agent 技术通过将服务请求 Agent 动态地移到服务器端执行，使得此 Agent 较少依赖网络传输这一中间环节而直接面对要访问的服务器资源，从而避免了大量数据的网络传送，降低了系统对网络带宽的依赖，克服网络延迟。移动 Agent 不需要统一调度，由用户创建的 Agent 可以异步地在不同节点上运行，等任务完成后再将结果传送给用户[4]。移动 Agent 具有动态自适应性，它可以感知运行环境，并且对变化自主、快速地做出反应，使整个系统始终保持在最优状态。此外它还具有自治性、健壮性和容错性等特性。

由于移动 Agent 的众多优点，其理论已经被应用于电子商务、分布式计算、信息检索等领域。然而，随着移动 Agent 技术的推广，移动 Agent 通信机制显得日益重要，它是限制移动 Agent 技术广泛应用于

① 基金项目:国家自然科学基金(60702081)
收稿时间:2009-07-08

实际的主要因素之一。由于现有通信机制还不够完善，因此，提出一种完善的通信模型具有重要的现实意义。

本文的第 1 节阐述了移动 Agent 通信常见的解决方案及其缺点和不足，并介绍了最近国内外的一些相关的研究工作，第 2、3 和 4 节分别针对第 1 节中分析的三个问题提出了相应的解决方案，从而形成了一个改进的通信模型，最后，第 5 节给出本文的结论和对未来作了展望。

1　问题分析与相关工作

1.1 问题分析

在传统的分布式计算环境中，计算实体一旦被创建，它们的位置便固定下来，发送方只需得到接收方的当前位置即可始终与之通信。但是在基于移动 Agent 的系统中，由于移动 Agent 的移动性，移动 Agent 的位置经常改变，因此移动 Agent 之间进行通信需要考虑的问题有：

(1) 移动 Agent 的命名与定位问题。在分布式环境下移动 Agent 命名的一致性，如何才能让其它移动 Agent 知道这一变化，实现移动 Agent 按名寻址。

(2) 移动 Agent 的通信安全问题。当移动 Agent 之间传输数据时，如何保证通信数据的安全性。

(3) 移动 Agent 的通信失效问题[5]。当移动 Agent 迁移时，如何处理正在发送给移动 Agent 的消息。

1.2 相关工作

针对移动 Agent 通信问题，现有的通信机制实现方法主要有广播机制[6]、消息转发机制[7]、基于 HOME 的寻址机制[8]和基于邮箱的通信机制[9]。广播机制基本思想是消息从根节点开始发送，按照某种规则遍历网络中的所有结点。 Murphy[6] 曾论证过，仅仅通过简单的广播是无法实现 Agent 消息的可靠传输的。消息转发机制实现起来也较简单，并支持消息的发送和 Agent 迁移的异步运行，可以在一定程度上加强消息发送的可靠性，但若移动 Agent 迁移很频繁，就会存在消息追击现象。基于 Home 的寻址机制的基本思想是消息先发送到 Home 主机上，Home 主机根据其记录的移动 Agent 的当前所在主机地址将消息转发目标 Agent，这种机制实现简单，且迁移和消息发送的开销不大，缺点在于对 Home 有依赖性、不支持消息发送和 Agent 迁移的异步运行、Home 瓶颈问题和消息的不可靠传输问题。基于邮箱的通信机制，由于邮箱是根据需要而决定是否随其 Agent 迁移，使得这种机制较为灵活，另外信箱的迁移率相对 Agent 的迁移率小得多,但同时也增加了系统的额外负担。

此外，文献[10]中提出了一种基于消息重发的可靠通信机制来解决因 Agent 迁移或网络故障产生的消息丢失问题，算法采用类似于 TCP 协议中的滑动窗口机制，当消息得不到确认时进行重发，重发几次后仍得不到确认则认为目标 Agent 已经迁移，将消息交给服务器转发。但是，算法仍无法避免多次重发和转发的可能，没有从根本上解决消息发送和Agent迁移之间的矛盾。

通过对现有移动 Agent 通信机制的缺点与不足的研究，本文在原有的算法和思想的基础之上，提出了一种改进的移动 Agent 通信模型，该模型分别从移动 Agent 的命名与定位问题、移动 Agent 的通信安全问题和移动Agent的通信失效问题三个方面进行了阐述。

2　移动Agent的命名与定位

对于移动 Agent 命名问题，最简单的方法是提供基于主机的的 IP 地址和端口号的名字解析机制来对 Agent 进行命名，然后使用域名解析系统来实现名字的解析,这种命名方式对静态对象的命名和名字解析非常有效。然而，对于移动 Agent，它的位置在不断的发生变化，因此，名字需要同步的改变以反映其最新的位置，这就使对 Agent 定位变得非常复杂，此外，把所有的名字解析工作交给一部分主机来完成，容易造成瓶颈，一旦名字解析服务器发生崩溃，那么所有的通信将无法进行。因此，采用全局的、与位置无关的命名方法移动对 Agent 进行统一命名。

在参考 Mogent 系统[5]的命名方式的基础上，本文提出了一种改进的移动 Agent 命名机制，有效的保证了移动 Agent 在迁移过程中与位置无关。其数据结构如表 1 所示：

表 1　移动 Agent 数据结构

源主机 ID	AgentID	源主机 Agent 系统类型
目标主机 ID	ID	目标主机 Agent 系统类型

该数据结构采用两层命名规范，第一层为逻辑层，移动 Agent 的源主机 ID(移动 Agent 产生地)可由源主机 IP 地址和端口号组成，AgentID 是源主机为移动 Agent 分配的一个标识 ID，源主机 ID 和 AgentID 联合组成全球唯一，源主机 Agent 系统类型为其使用的 Agent 系统类型及版本，以保证其兼容性和可扩展性。

第二层为物理层，目标主机 ID(移动 Agent 迁移地)可由目标主机 IP 地址和端口号组成，ID 是由目标主机为移动 Agent 分配的标识 ID，目标主机的 Agent 系统类型字段保存了目标主机上的 Agent 系统类型及版本，每当移动 Agent 迁移到一个目标主机时，其物理层的各字段都需要发生相应的变化。

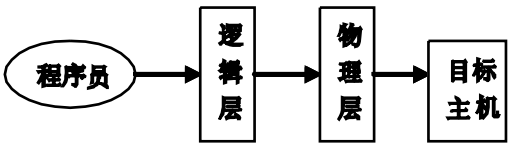

图 1　移动 Agent 寻址

移动Agent命名的逻辑层在整个生命周期中始终保持不变，保证了移动Agent 位置的透明性，程序员只需要知道移动 Agent 的逻辑名，然后根据逻辑名影射到其物理名，从而可以解析出当前移动 Agent 的所在位置。

3　移动Agent的通信安全

为了保证移动 Agent 在通信过程中数据和运行状态安全，需要一种高效的并行加密算法，该模型采用 PED 加密算法，保证移动 Agent 在通信过程中的安全性，并证实了该加密算法的可行性。

3.1 PED 算法简介

PED 算法[11]可以防止未经授权的主机窃听信道上迁移的移动 Agent 数据和运行状态，PED 可以分配 52 个随机字母(26 个小写和 26 个大写)，并提供了 8.07×10^{67} 种不同的符号，其通用的加密和解密模式通常由四元组表示，M={T，C，K，I},其中 T 表示明文，C 表示密文，K 表示键值，I 表示级别。

2.1.1 加密

定义 1.　假设源数据文件 T 表示为 T=Z90，其中 Z 是指包含 90 个元素的域空间，$t_i\in T$，其中 t_i 表示可能由 26 个大写字母或小写字母，0–9 的 10 个数字和 28 个特殊字符(包括空格)组成的明文。

定义 2.　假设键值空间表示为：$K=P\binom{52}{52}$，$\pi_i\in K$,表示键值是根据 Pseudo 随机数函数 $\pi_i=Rnd(s_i)$ 得到的。

定义 3.　密文 C 是由 52 个元素组成($C=Z_{52}$)，且 c_i 是 C 中的元素，即 $c_i\in C$，基于这个定义，那么初始的信息文本可以表示为：

$$c_i=\begin{cases}[e^{l_i}_{\pi_i}(t_i)]\wedge[e^{l_i}_{\pi_i}(t_{i+1})]\wedge[e^{l_i}_{\pi_i}(l_{i+1})] & (i>0)\\ PK(\pi_i+l_i) & (i=0)\end{cases} \quad (1)$$

其中 l_i 表示级数，PK 表示公钥，$e^{l_i}_{\pi_i}(x)$ 表示加密函数，它可以表示成如下：

$$e^{l_i}_{\pi_i}(t_i)=\{a^{l}(\pi_i(a^{l-1}(\pi_i(\cdots a^{1}(\pi_i(t_i))))))\} \quad (2)$$

2.1.2 解密

根据上一节的加密算法(1–3 的表达式)，密文的解密过程可以表示为如下：

$$t_i=\begin{cases}d^{l_i}_{\pi_i}(c_i) & (i>0)\\ PK^{-1}(s_i) & (i=0)\end{cases} \quad (3)$$

其中 $d^{l_i}_{\pi_i}(x)$ 是解码函数，它可表示为：

$$d^{l_i}_{\pi_i}(c_i)=\{\pi_i^{-1}(a^{1}(\pi_i^{-1}(a^{2}(\cdots\pi_i^{-1}(a^{l}(c_i)))))\} \quad (4)$$

在解密函数中，同时也要用到表达式(3)中的赋值表。此外，PED 加密函数能够把密文分解中若干个数据报文，从而可以抵制频繁的分析攻击。

3.2 通信安全

移动 Agent 在迁移和通信过程中最大的安全威胁在于保护其代码和状态被篡改。为了提高通信中的安全性，通常使用加密机制和认证机制，该模型使用 PED 算法实现加密机制和认证机制，大量提高了 Agent 在迁移和运行过程中的可靠性。

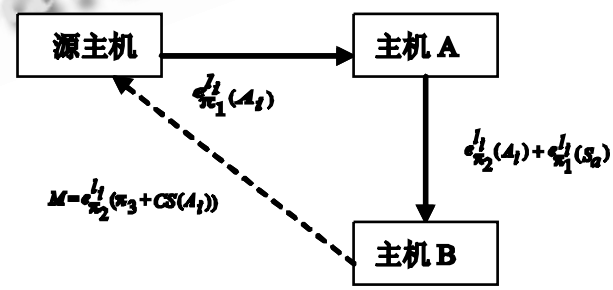

图 2　移动 Agent 迁移加密与认证机制

从上图中可以知道，首先由源主机根据 Pseudo 随机数函数生成的键值 π_1，使用 PED $e^{l_i}_{\pi_1}(A_i)$ 函数加密创建好的移动 Agent，同时第一个键值 π_1 发送到主机 A 上，获取认证后，移动 Agent 迁移到主机 A 上，主机 A 根据接收的键值通过公钥管理函数 PK_A 解密，解

密成功后移动 Agent 执行相关操作。

当移动 Agent 在主机 A 上执行完相关操作后，它需要迁移到主机 B 上运行，因此，主机 A 则会根据Pseudo 随机数函数生成的键值π_2，并发送到主机 B 上，分别使用π_1和π_2来加密当前移动 Agent 的状态和代码，同时，把键值π_2发送到主机 B 上，主机 B 获得认证后，通过主机 A 加密后的移动 Agent 迁移到主机 B。由于主机 B 并不知道的π_1值，所以他并不能解密移动Agent，因此，主机 B 会发送校验和函数 CS(A_i)和π_2的值到源主机(为了提高安全性，发送前使用主机 B 生成的键值π_3进行加密传输，生成报文M)。源主机接收到报文 M 后，把它与初始的报文进行比较，如果相同，则表示认证通过，便把π_1的值发送给主机 B，授权其可以运行，如果不相同，则可能是移动 Agent 在传输过程中受到攻击或是受到来自主机 A 的恶意攻击。

4　移动Agent的通信失效问题

通信失效问题是指在特定条件约束下的信件不能或不能及时到达接收者的一种现象。通信失效从本质上来看是因为在路由信件和实际信件传输过程中，目标 Agent 发生了物理位置的变化，而这种变化是随机的、不可预料的。基于 Home 的转发机制[8]具有较好的健壮性和可扩展性，而且实现了分布式处理，但在移动 Agent 生命周期内必须保证 Home 的长久连接，而且每次迁移和定位移动 Agent 都要与 Home 通信，延迟较大，此外，当 Home 向 Agent 发送信息时，Agent 正好移动到其他节点，这时就会发生通信失效，因而它也不能保证消息能够正确发送给目标 Agent。本文提出了一种改进的基于 Home 通信机制，在传统的算法上构建了一个消息转发组件，有效地防止了通信失效问题。

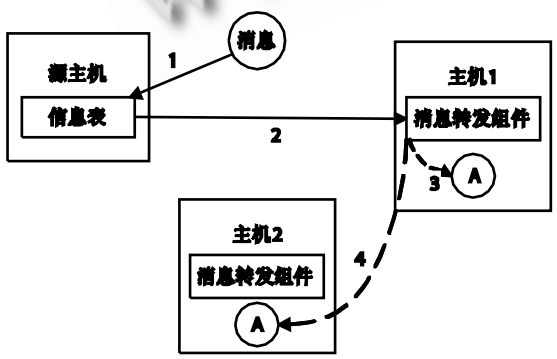

图 3　改进的 Home 通信机制

如图 3 所示，首先把需要发送的消息发送给源主机，源主机根据信息表查找出当前移动 Agent 的所在主机位置(主机 1)，然后，消息通过 2 发送到主机 1 中的消息转发组件，如果 Agent 还在主机 1 上，则把消息发送给 Agent 处理，如果 Agent 已经迁移到其他主机上(主机 2)，则通过消息转发组件把消息发送上主机 2 上给 Agent 处理，从而有效地防止了通信失效问题。

5　总结与展望

移动 Agent 的通信问题一直是限制移动 Agent 系统被广泛应用的主要因素之一，现有移动 Agent 的通信机制理论体系还不够成熟，仍然有许多问题需要进一步的研究。本文在分析移动 Agent 的命名与定位、移动 Agent 通信安全和移动 Agent 通信失效的各自的特点的基础上，提出了一个改进的移动 Agent 通信参考模型，在某种程度解决了移动 Agent 通信问题，提高了移动 Agent 之间通信的安全性。但仍然在某些方面存在不足之处，比如，移动 Agent 的命名时增加物理层数据段和架构一个消息转发组件会给系统带来额外的负担，随着新一代硬件技术的不断改进，特别是芯片处理速度的不断提升，资源消耗问题能够得以解决。

在基于 Home 通信机制上增加消息转发组件在某种程度上防止了通信失效问题,在本文设计的移动 Agent 的两层命名规范的特性的基础上，详细设计消息转发组件的数据结构并实现具有重要的意义，这是下一步的研究工作。此外，移动 Agent 安全性问题[12]也是需要进一步研究。随着移动 Agent 理论体系的不断完善，其应用会得到更广泛的推广。

参考文献

1 Wooldridage M. An Introduction to MultiAgent Systems. Chichester, England: Published by John Wiley, 2002.

2 White JE. Telescript technology: the foundation for the electronic market place. White Paper, General Magic Inc, Mountatin View, CA, 1994.

3 周龙骧,刘添添.移动 agent 综述.计算机应用与软件, 2003,20(11):21－25.

4 张云勇,刘锦德.移动 agent 技术.北京:清华大学出版社, 2003:63－68.

(下转第 141 页)

(上接第 90 页)

5 陶先平,冯新宇,李新,等.Mogent 系统的通信机制.软件学报, 2000,11(8):1060－1065.

6 Murphy A, Picco GP. Reliable communication for highly mobile agents. Proc. Agent Systems and Architectures/Mobile Agents (ASA/MA)'99,CA,USA, 1999.141－150.

7 Belle WV, Verelst K. D'Hondt T. Location transparent routing in mobile Agent systems merging name lookups with routing. Proc. the 7th IEEE Workshop on Future Trends of Distributed Computing Systems. 1999.207－212.

8 Milojicic D, Breugst M, Busse I. MASIF: The OMG mobile Agent system interoperability facility. Rothernet K, Hohl F, eds. Proc. of the MA'98.LNCS1477, Berlin: Springer-Verleg, 1998.50－67.

9 Feng XY, Cao JN, Lu J, et al. An Efficient Mailbox-based Algorithm for Message Delivery in Mobile Agent Systems. Proc. of the MA'01, Berlin, Germany: Springer-Verlag, 2001.

10 Ranganathan M, Bednarek M, Montgomery D. A reliable message delivery protocol for mobile Agents. Kotz David et al eds. Agent Systems. Mobile Agents. and Applications. Lecture Notes in Computer Science.1882. Berlin: Springer-Verlag. 2000.206－220.

11 Duan JJ, Hurd J, et al. Functional Correctness Proofs of Encryption Algorithms. Springer Berlin, Heidelberg. 2005.519－533.

12 KunY, Xin G, Dayou L. Security in mobile agent system: Problems and approaches. ACM SIGOPS Operating Systems Review, 2000,34(1):21－28.