第 33 卷 第 6 期 计 算 机 工 程 2007 年 3 月
Vol.33 No.6 Computer Engineering March 2007
·安全技术· 文章编号：1000—3428(2007)06—0104—03 文献标识码：A 中图分类号：TP309.7

基于密码技术的 Mobile Agent 系统安全解决方案

解迎刚[1]，王志良[1]，永井正武[2]，党会建[1]，张 琴[1]
(1. 北京科技大学信息工程学院，北京 100083；2. 日本帝京大学科学工程学院情报学科)

摘 要：Agent 技术很好地解决了网络间任务分配及合作的问题，但 Agent 系统实际应用时的安全问题一直没有得到很好的解决。该文设计了一个可实际应用的 Mobile Agent 系统安全问题解决方案，该方案可以有效解决实际运行中 Agent 系统的安全认证及安全通信问题。介绍了该方案在个性化 E-learning 系统中的实际应用情况。

关键词：移动代理；Agent 技术；安全通信；E-learning 系统

Solution of Mobile Agent System Security Problem Based on Cryptographic Technique

XIE Yinggang[1], WANG Zhiliang[1], Masatake Nagai[2], DANG Huijian[1], ZHANG Qing[1]
(1. School of Information Engineering, Beijing University of Science & Technology, Beijing 100083;
2. Department of Information Sciences, School of Science and Engineering, Teikyo University)

【Abstract】The agent technology solves the problem of task assigning and cooperation between network while the security problem in the mobile agent system restricts its application. An agent system security solution is presented based on cryptographic technique, which solves the problem of security authentication and secure communication in mobile agent system. The realization is introduced that the solution is applied to the individuality E-learning system.

【Key words】Mobile agent; Agent technique; Secure communication; E-learning system

Agent技术的研究起源于人工智能领域，目前在很多领域得到应用，并被赋予了不同的含义。由于Agent具有自治性、智能性、反应性、主动性等优点，越来越受到人们的重视，并被广泛应用到网络技术与分布式计算中，为网络技术、分布式计算与Internet应用带来了新的思想和优秀特性[1]。

本文介绍了 Mobile Agent 的概念、特点，着重分析 Mobile Agent 的安全性问题，在分析了现有针对 Mobile Agent 系统安全性的常用解决方案后，提出了一种基于 MD5 以及 RAS 密码技术的 Mobile Agent 安全策略以及实现方案，最后介绍了将该方案应用于个性化 E-learning 系统中的实现情况，突出了该方案的现实意义。

1 Mobile Agent 的简要概述

Mobile Agent的一般定义如下：它是一个能在异构网络中自主地从一台主机迁移到另外一台主机并与其它Agent或资源交互的程序[1]。它代表某个用户，按照一定的规程，在异质网络里各计算机间自主迁移，寻找到合适的计算资源、信息资源和软件资源，通过对这些资源的处理和利用，完成特定的任务。通过Mobile Agent可以有效地改善C/S方式下客户机和服务器之间大量中间计算结果浪费网络带宽的 情况。

由 Mobile Agent 的性质决定它有如下 3 个优点：

(1)减少网络带宽和时延。

(2)Mobile Agent 能根据环境、负载的变化动态迁移，以达到一个理想的计算效果。

(3)在分布式环境下，Mobile Agent 系统能实现较好的并行性。

2 Mobile agent 系统的安全性问题

Mobile Agent因其程序的自由迁移和应用的灵活性而产生许多安全性问题[3]。可以归纳为以下 2 个方面:

(1)恶意 Agent 对目标主机的威胁：当一个非可靠 Mobile Agent 迁移到一台主机后，对主机系统的资源可能会进行非法操作。

(2)恶意的目标主机对 Mobile Agent 的威胁：当 Mobile Agent 迁移到一个非可靠主机后，恶意主机可能会对 Mobile Agent 进行非法操作。

从以上分析可知，Mobile Agent 的安全保护问题包括两个方面：

(1)保护运行 Mobile Agent 的主机或实体不受恶意 Agent 的攻击。

(2)保护 Mobile Agent 不受恶意的运行环境以及不协作或者有敌意的其它 Agent 的攻击。

为了解决上述问题，目前已经提出的解决措施有 Sandboxing、认证、授权、Proof-carrying code、付费检查等。

基金项目：北京市“现代信息科学与网络技术”重点实验室开放基金资助项目“多模人机交互技术中的情感计算方法研究”(TDXX0503)；北京科技大学重点基金资助项目“NBIC 会聚技术研究”;国家自然科学基金资助项目“基于状态空间描述的人工情绪理论和方法研究”(60573059)

作者简介：解迎刚(1978－)，男，博士生，主研方向：普适计算，Agent 系统应用与研究，E-learning 系统，人工心理，情感计算；王志良、永井正武，教授、博导；党会建、张 琴，硕士生

收稿日期：2006-03-07 **E-mail：**yinggangxie@163.com

3 系统中 Agent 安全性的实现

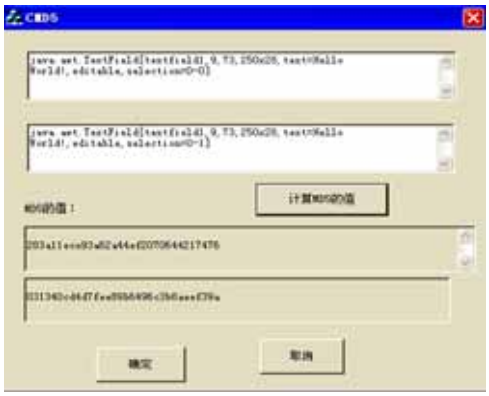
结合现有的 Agent 安全性解决措施的思想和本课题个性化 E-learning 系统的特点，在本系统中重点解决的是恶意 Agent 对目标主机的威胁，对于恶意主机对 Agent 的安全性问题不作为本课题 E-learning 系统中 Agent 应用研究的重点，故不在这里进行讨论。在这里采用密码技术实现系统 Agent 的安全性问题，主要分为 2 部分：通过密码校验技术对认证信息进行加密，实现身份认证的安全。对通信内容和数据信息进行加密，实现通信信息的安全。

(1)Mobile Agent 的身份认证机制

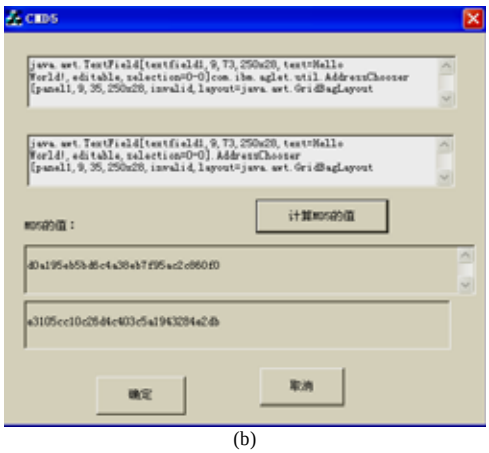
在 Mobile Agent 系统中，如果主机和 Agent 能够推断双方的合法身份，则彼此可以放心地授予对方更多权利。身份认证就是通过标识和鉴别用户的身份，防止攻击者假冒合法用户获取访问权限。目前存在很多身份认证机制，主要有 3 种:请求/应答，公钥加密算法，密码校验和。其中密码校验和(Cryptographic Checksum)方法为：单向散列函数用于为文件产生一个唯一的“指印”，为每一个授权的 Mobile Agent 产生一个密码校验和，即唯一的标记。Mobile Agent 执行之前，主机对它的校验和进行重计算，将结果与信任的校验和比较，如果匹配，则表示验证通过，Mobile Agent 得到授权。

这里着重考虑安全性问题，故采用安全度较高 MD5 校验算法。

下面通过数据进行验证，这里是 2 段 Agent 系统运行中部分 Agent 代码，取了差别非常小的两段代码进行 MD5 校验，校验结果差别非常大(见图 1)。这说明该算法对校验内容变化的高度敏感性，算法达到了扩散、置乱和混淆的效果。



(a)



(b)

图 1 MD5 校验比较

(2)Mobile Agent 的通信安全机制

除了对 Agent 进行校验确认其身份，在通信过程中，同时采用加密算法来确保通信的安全性，考虑到个性化 E-learning 系统的特点，以及其对系统安全性的要求和加解密算法的可操作性，采用基于 RAS 算法的加密机制。该加密机制可以分为下面 3 部分：

1)密钥对的产生:指定公用密钥和私用密钥的长度，接着选择一较大的素数 p，再选择 2 个非负的随机整数 g，x，二者均小于 p，并计算 Y=g mod p，则其公钥为 Y，g 和 p，私钥为 x，g 和 p，可由一组用户共享。

2)加密：将消息分成与密钥长度相同的块。加密时，选择一个随机数 k，k 与 p-1 互质，接着计算整数 a 和 b，a=g mod p，b=y mod p，则(a，b)称为密文。

3)解密: 给定一个密文数对(a，b)，求得相应的整数 M 的值，即解密。M =b/a` mod p，获得 M 后，将每个 M 转化为相应的纯文本数组或文本串，即原来的消息。

通过在身份验证和信息通信过程中的加密通信方式，可以保证该 Agent 系统在通信中的数据保密性，同时通过对通信模式的再构建，共同实现了本系统的安全问题解决方案。对于加解密的效果以及其对整个 Agent 系统延时的影响，笔者做了简单的测试验证。如图 2 所示。

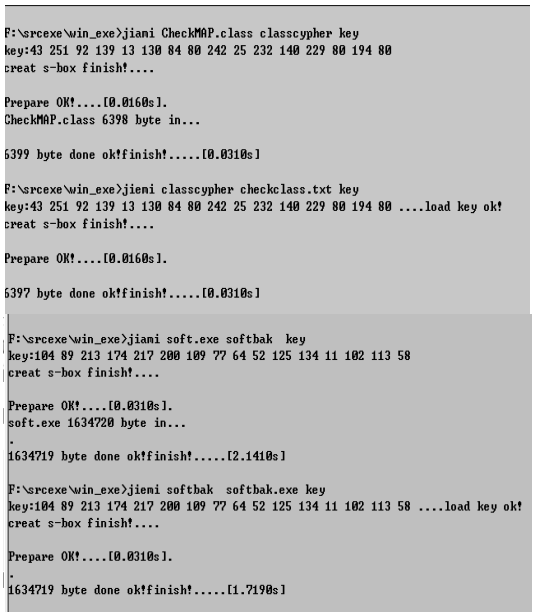


图 2 信息加密比较

从图中数据可以看到，在一般的 Agent 通信过程中，对于迁移的 Agent，加解密的时间均在毫秒级，或几十毫秒。当数据量比较大（1MB 以上）时，加解密的时间会上升到秒级（1~2s）。对于本系统而言，相对较高的通信安全性来说，这样的延时是可以允许的。

4 通信模式的具体实现

下面对该安全解决方案的具体实现进行阐述

在进行阐述前针对本系统的特点以及其对安全性的要求，进行以下 2 点说明：(1)引入密钥中心(cryptographic key Center)，用其保存本机密钥，以及其它系统内主机的公钥。(2)定义中心服务器是安全的，则由其创建的 Agent 也是安全的，同时假定系统内主机是无恶意的，则在实现时，可以暂时不考虑恶意主机对 Agent 的威胁。

为详细阐述通信过程(见图 3)，进行如下定义：密钥中心的加密算法为 R，源主机为 RH(Recourse Host)，目的主机为 DH（Destination Host），迁移前的 Agent 记为 Agent(A)，经过加密和 MD5 算法补充后的 R（Agent(A)）记为 Agent(A)’。

目的主机的访问密码为 PW_B，利用 DH 密钥的解密算法为 JR，目标主机密钥为 SKD，Agent(A)由 RH 创建。

当 Agent(A)要迁移到 DH 之前，先向 cryptographic Center 发出请求，获取系统内 MD5 密钥以及远端 Agent Host 的公钥，然后利用此密钥对认证信息和通信信息用 MD5 算法计算出 MD5 值，由 cryptographic Center 利用目标主机的密钥(SKD)，处理得到 agent(A')

R(Agent(A))→ Agent(A')

这里将 Agent(A)的内容简单描述为

Agent(A)=ID(A)+ PW_B +Message(A)，则

Agent(A')=R(Agent(A))=ID(A)+R(MD5(PW_B))+R(Message(A))+R(MD5

(Message(A)));

Agent(A')迁移到 DH 后，记为 Agent(B)，先由 DH 的验证中心进行身份验证，

If R(MD5(PW_B))正确 then 通过校验。

通过验证后，则按照系统已经定义的协议对信息内容进行解析。

然后对 R(Message(A))进行解密运算，

JR (R(Message(A)))→ Message(A);

再对得到的 Message(A)进行基于 R 密钥的 MD5 计算得到结果 DHR'。

If DHR'==R(MD5(Message(A))) then 通过校验。

通过验证去除 Agent(B) 中的冗余信息，形成 Agent(B')，即有 Agent(B')=Agent(A)，则可以给 Agent(B')充分的授权，使其可以在本平台运行，执行任务。

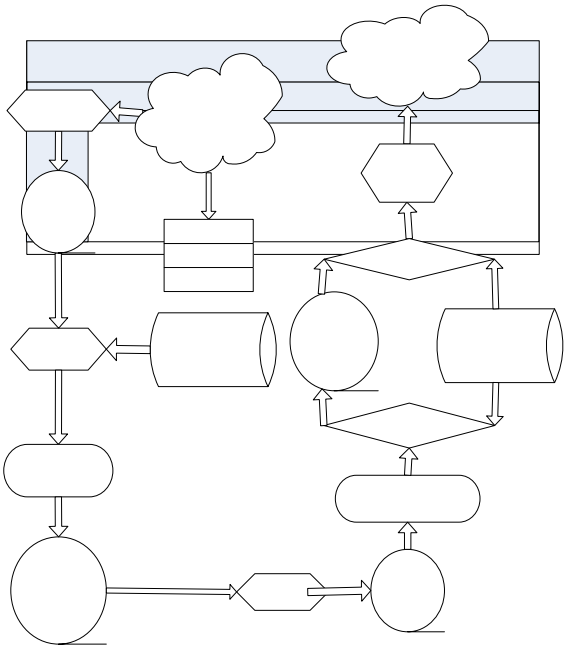


图 3 系统中 Agent 通信过程

在这个验证过程中，Agent 迁移到远程主机后，Agent Host 对 Agent 的身份进行认证，利用认证信息检查该 Agent 来自哪个平台，同时使用自己的密钥对认证信息进行校验，如果校验不通过，则说明在 Agent 迁移过程中，Agent 受到了攻击或破坏，Agent 内容被改动，或者该 Agent 是恶意的，则平台销毁该 Agent，并向 Agent 源主机发送错误信息；如果校验通过，则对 Agent 的信息内容进行解密，并使用自己密钥对信息内容用 MD5 算法计算出 MD5 值，将自己得到的 MD5 值同 Agent 所含信息项的 MD5 值进行校验比较。如果校验不通过，则说明 Agent 在迁移过程中受到破坏，则销毁该 Agent，并向 Agent 源主机发送错误信息；如果校验通过，则容许该 Agent 执行其任务。

由前面的 MD5 理论以及认证过程，可以看到，该通信模式的设计，可以避免恶意 Agent 引起的安全性问题。在 Agent 迁移过程中，如果 Agent 受到攻击，被篡改，根据系统验证模式和 MD5 校验算法，则最后在 DH 处的校验必然无法通过。在 Agent 通信模式中通过密码处理，可以防止 Agent 在传输过程中数据被窃听，从而在一定程度上保证了 Agent 系统的安全性。

5 方案应用

本文提出的基于 MD5 以及 RAS 密码技术的 Mobile Agent 安全策略以及实现方案，其重要意义在于方案的可操作性。

整个个性化 E-learning 系统的实现采用 Aglet、Java 语言和 JSP 技术；数据库采用 SQL Server；在教学过程中，由学生通过人机接口申请学习登录，生成学生 Agent。系统得到学生的相关信息后，由位于服务器端的管理 Agent 进行学生信息分析和教学策略分析，并在非同步教学中通过对学生学习状态、学习情绪、学习日志的分析，并结合单元测试情况，形成针对学生的个性化教学方案。在同步教学过程中，启用电子白板进行辅助教学，并由学生 Agent 对学生端学习状态进行智能管理。在教学过程中，利用智能 Agent 对学生的学习状态进行判断，并在必要的时候由智能 Agent 助手给教师以人性化的提示。系统结构如图 4 所示。

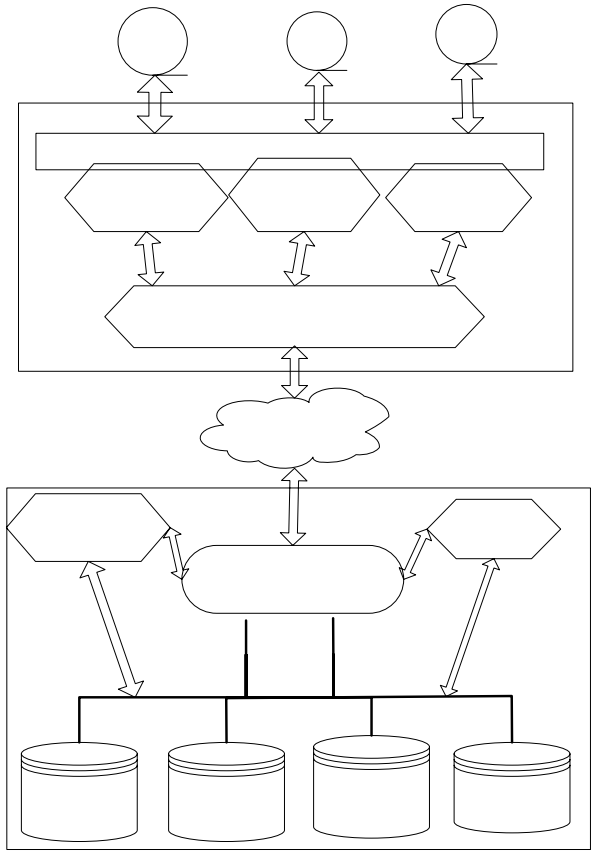


图 4 E-learning 系统结构

整个系统采用 B/S 系统结构，利用 Mobile Agent 实现消息的传递。其中 Message Agent 负责系统间的消息传递，Management Agent 和 Interaction Agent 内部实现了如图 3 所示

(下转第 155 页)

Destination Host

<进程名称>

Agent system

Resource system