多移动代理系统的路由安全管理方案的研究

王汝传*** 黄海平* 李明远*
*(南京邮电学院计算机科学与技术系 南京 210003)
**(信息安全国家重点实验室 (中国科学院研究生院) 北京 100039)

摘 要：随着电子商务与网管技术的发展，多移动代理系统得到了广泛应用，同时也使得该系统的路由安全管理更具复杂性与灵活性。该文针对多移动代理系统，提出了一种新的路由安全管理方案。该方案基于保护任务代理的警卫 Agent（Proxy agent）的思想，引入了委托信任机制和可信任验证服务器，且对传统的路由表结构进行了改造。方案充分利用了多移动代理协作和交互的优越性，有效提高了路由选择的效率和安全性，同时也保证了最优化。

关键词：多移动代理系统，路由安全，委托信任机制
中图分类号：TP393, TP309 **文献标识码**：A **文章编号**：1009-5896(2005)06-0978-05

The Study on Routing Security Management Scheme in Multi-mobile Agent System

Wang Ru-chuan* ** Huang Hai-ping* Li Ming-yuan*
*(*Dept of Computer Science & Technology, Nanjing University of Posts and Telecom., Nanjing* 210003, *China*)
** (*State Key Laboratory of Information Security(Graduate School of Chinese Academy of Sciences), Beijing* 100039, *China*)

Abstract The rapid development of E-business & network management has been promoting the broad applications on multi-mobile agents system. However, it made routing security management of this system more complex and flexible. Aimed at multi-mobile agents system, this paper proposes a new scheme of routing security management. Based on the idea of Guard Agent (Proxy Agent) whose responsibility is protecting Task Agent, this scheme introduces Trust Mechanism & Verification Server and modifies the structure of traditional routing tables. It makes full use of the advantages of multi-mobile agents' cooperation & interaction, improves the safety and efficiency of routing and ensures optimization.

Key words Multi-mobile agents system , Routing security, Trust mechanism

1 引言

移动代理(Mobile agent)是一系列代码与状态的集合，它能代表源主机在网络上自主地迁移以完成特定的任务。随着电子商务、分布式网管和 Agent 技术的发展，多移动代理系统日益受到重视。多个代理之间可以相互协作、共享有限的资源、分派执行任务，从而使商务交易、网络管理的效率最大化[1]。然而，网络的开放性和不可信任性带来了严峻的安全问题——任何恶意的代码、主机及执行平台都可能对代理进行非法攻击。因此，迫切需要在多移动代理系统中引入安全机制，以保证移动代码的正确性、代理所携带数据的机密性及控制流的完整性。除了常用的几种解决方案例如加密、数字签名、访问控制等，多移动代理的协作与交互也能保护系统免受恶意方的攻击，这也是多代理系统的特殊优点。电子商务中的联合签名机制便是通过多移动代理协作来保障安全的经典方案：多个移动代理在与电子市场交互时可将其标识绑定至一信息块中，从而在利用代理组功能时能提供相应的安全保障[2]。电子投票中的公平匿名性研究也可以借助于多移动代理的协作与交互[3-5]。而本文的重点是构建一个基于动态路由协议、委托信任机制、监测技术和密钥技术的多移动代理路由安全管理方案。

2003-12-25 收到，2004-09-07 改回
国家自然科学基金(60173037 和 70271050), 江苏省自然科学基金(BK2003105 和 BK2004218), 江苏省高技术研究计划(BG2004004)和江苏省计算机信息处理技术重点实验室基金(kjs03061 和 kjs04)资助课题

2 多移动代理系统

2.1 多移动代理的组成结构

多移动代理的组成结构一般有两种模式——对等模式(Peer to Peer Pattern)与主从模式(Master-Slave Pattern)。如图 1 所示，主代理 1 和主代理 2 属于对等模式，从代理 1、从代理 2 和从代理 3 之间也是平等关系，它们从属于主代理 1，

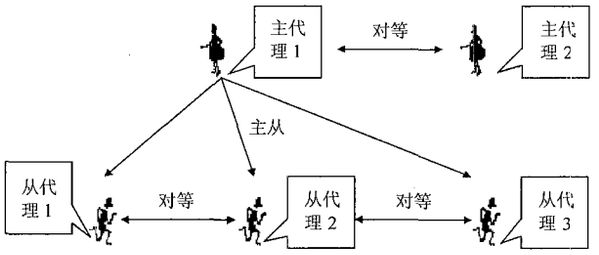

图 1　多移动代理的组成结构

其主从关系主要体现在所分派任务的不同、所携带数据的机密程度不同，而主代理一般具备指挥协同从代理的能力。下文介绍的任务代理和警卫 Agent 之间便是非对等主从模式。

相对于单一代理结构而言，多移动代理系统具有如下优点：任务的分布、快速求解问题、减少通信流量、增加安全性、增加灵活性、增加可靠性等等[6]。

2.2　多移动代理之间的秘密分割与共享

多移动代理之间秘密分割与共享所遵循的原则为：主代理拥有 1 份主秘密，其 n 个从代理各拥有 1 份子秘密(共有 n 份)，只有子秘密的份数大于等于 t ($1 \le t \le n$)时，方能导出主秘密。t 是一个门限值，它的大小代表了不同的安全需求，可以根据秘密的重要程度来确定 t 值的大小。一般而言，t 值越大，安全级别越高。

仍以图 1 为例，譬如主代理 1 拥有主秘密 s，从代理 1、2 和 3 分别拥有子秘密 ss_i (i=1, 2, 3)，且有 $C_3^t[ss_i\ (i=1, 2, 3)]\ (1 \le t \le 3) \Rightarrow s$ 成立，其中 C_n^t 为排列组合取值符号。若 t=1，则 $s \Leftrightarrow ss_i\ (i=1, 2, 3)$；若 t=3，则只有 3 个从代理均到齐时方能推导出 s，安全级别较高。

3　多移动代理的路由安全管理方案

3.1　路由安全管理的一般分析

路由管理是支撑网络传输的关键技术，网络、流量规模的大小和路由选择原则的有效性永远是一对相互矛盾、相互促进的因素[7]。在这一小节中，将对多移动代理系统的路由安全管理进行一般性分析。

如图 2 的网络拓扑结构所示，节点 0 是能产生多个移动代理的源主机。图中标识的移动代理 1 与移动代理 2 接受了源主机所分派的任务，被称之为“任务代理”，它们之间是对等协作关系。它们分别拥有源主机将其秘密 s (例如银行信用卡 ID)分割后的子秘密 ss_1 和 ss_2，并共享一个简单的加解密函数 $f(x)/f^{-1}(x)$。它们还各自配备了一个警卫 Agent，用于检查各网络线路及节点的安全性。警卫 Agent 机制是一种用于保障移动代理执行任务的新的多 Agent 架构，其实质可

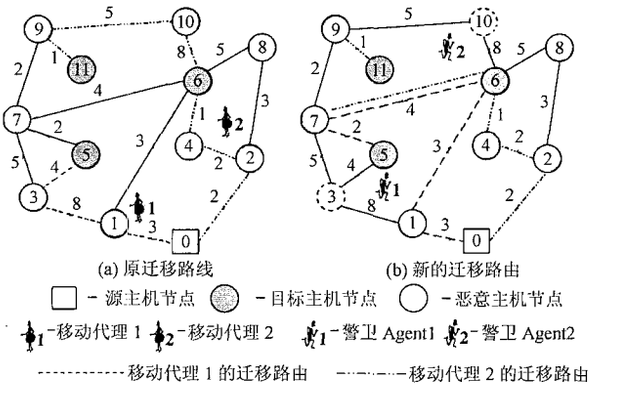

图 2　引入警卫 Agent 之后的网络路由安全分析

以是一种警卫 Agent[8]。它所提供的安全服务是系统级的、库级的或者是对象级的透明安全服务。警卫 Agent 由源主机在创建任务代理时创建且紧密追随任务代理，并可通过扩充以满足更多的需要。此时任务代理的安全便由警卫 Agent 负责，它必须对代理所要访问的主机节点进行验证和监测，通过鉴别任务代理的状态来确保工作流的一致性。警卫 Agent 可采用支持安全性的编程语言（例如 SADL）来开发[8]。

移动代理迁移的原则按优先次序可约定如下：(1) 安全性；(2) 各节点链路允许的最大传输容量以及当前可用带宽；(3) 节点与节点的间距长短。为了便于讨论，先假定各节点链路允许的最大传输容量为 10 单位，每两个节点之间的间距是等长的，且网络各节点的当前可用带宽为该时段的预期平均经验值（如图 2 中数字所标识）。在图 2 中，移动代理 1 携有子秘密 ss_1，它将访问目标节点 5，且要在节点 5 提供源主机完整的机密信息以完成最终的任务；在它到达节点 5 之前必须搜集节点 1 和节点 3(或节点 7)的相关信息。移动代理 2 携有子秘密 ss_2，它先访问目标节点 6，完成目标节点 6 的任务之后再访问目标节点 11，且在到达 11 之前必须搜集节点 9 与节点 10 (或节点 7) 的相关信息。移动代理 1 需要与移动代理 2 协同工作才能最终完成任务，因为移动代理 1 在目标节点 5 需要移动代理 2 在目标节点 11 获取的信息，更为重要的是，只有$[ss_1, ss_2]$才能 $\Rightarrow s$。

移动代理可根据路由表中记录的网络各节点链路的预期可用带宽，事先选择一条负载流量最小的路线作为其迁移路由；同时派遣警卫 Agent 在其迁移至下一节点之前检验该节点和线路的安全性。根据节点选择原则的优先次序，若该节点为不安全节点，则将其从路由表中舍弃。图 2(a)和 2(b)反映了这种情况。移动代理 1 原本的迁移路线如图 2(a)所标识：0－1－3－5，其中节点 5 为目标节点，链路长度为 3，可用带宽总和为 15 单位。但由于警卫 Agent1 监测到节点 3

为不可信任(或有恶意动机)节点，为了避免受到攻击而泄露子秘密 ss_1，移动代理 1 必须改变其迁移路由，于是新的路由如图 2(b)所标识：0－1－6－7－5，链路长度增加了 1，带宽总和减少了 3。由于节点 7 与节点 3 具有可替代性，所以不影响移动代理 1 完成任务。同理，移动代理 2 的警卫 Agent2 监测到节点 10 为不安全节点，其迁移路由也发生了改变，如图 2(b)所示，当然也增加了迁移的代价。

移动代理 1 与移动代理 2 在协作过程中还要防止不同的主机节点达成合谋，因为这种“合谋攻击”的威胁性很大，随着合谋阵营的扩大，警卫 Agent 将很难监测到安全隐患[9]。

当移动代理 1 顺利到达节点 5，且移动代理 2 也顺利到达节点 11 并获取了所有相关信息之后，两个代理将协作完成最终任务。此时移动代理 1 会索要节点主机 5 的签名信息 o，并委派其警卫 Agent1 将 o 传送给移动代理 2 同时监测移动代理 2 是否被攻击；移动代理 2 验证签名信息 o 之后，将子秘密 ss_2 用简单加密函数加密成 $f(ss_2)$，并委派警卫 Agent2 连同所获信息一起传送给代理 1 并监测其是否被攻击；移动代理 1 解密 $f^{-1}(ss_2)$ 得到子秘密 ss_2，再结合 ss_1 推导出完整的机密信息 s。至此，代理 1 与代理 2 已通过协作圆满完成任务，各自选择路由返回源主机。

安全性分析 (1) 秘密的分割使得源主机的机密信息更加安全，攻击其中一个代理得到的子秘密无法推导出完整的信息，若是网络中存在更多移动代理，门限值的设定将大大提高安全级别；(2) 节点主机 5 无法抵赖它与移动代理 1 的交互行为，有其签名信息 o 为证；(3) 代理 2 携有的子秘密 ss_2 只有在节点主机 5 的签名信息有效的前提下才会被传输，且加密之后也提高了安全级别；(4) 双方的警卫 Agent 会监测各网络节点的安全以及对方代理的状态并核查其是否被攻击，若任一环节发现安全隐患，则宣告任务终止。

3.2 路由安全管理的进一步深化

3.2.1 *委托信任机制的引入* 在定义多移动代理系统的委托信任关系之前，首先定义一组相关实体：

$O=\{O_0,O_1,\cdots\}$表示源主机，$VS=\{VS_0,VS_1,\cdots\}$表示网络中的验证服务器（可信任的第三方），$H=\{H_0,H_1,\cdots\}$表示系统内的执行主机节点，$S=\{S_0,S_1,\cdots\}$表示不同的安全级别。

O 是移动代理的发起端，它决定了移动代理的运行路线。VS 验证服务器的作用主要是对网络中的源主机、执行主机和移动代理进行公证仲裁。网络中各种实体间的委托信任关系是根据不同的安全级别来建立的。

以下是网络中 4 类不同实体间的委托信任关系：

(1) 验证服务器 VS 和执行主机 H 之间的委托信任关系：<VS> T <H> with S;

当验证服务器 VS 验证了执行主机 H 递交的身份标识、签名信息及以往的移动代理执行安全报告并确认无误后，二者建立委托信任关系；

(2) 验证服务器 VS 和源主机 O 之间的委托信任关系：<VS> T <O> with S;

当源主机 O 需要验证服务器 VS 来验证移动代理的执行状况时，二者之间会建立起一种验证委托关系。这种信任关系一旦建立，那么 O 将会提供给 VS 必要的相关资源。比如：源主机的身份标识、签名信息、移动代理的初始化信息等等；

(3) 源主机 O 和执行主机 H 之间的委托信任关系[1]：<O> T <H> with S;

由于验证服务器 VS 是系统内唯一具有验证功能的实体，因此 O 和 H 之间无法直接建立信任关系，而只能通过验证服务器来间接建立；

(4) 执行主机 H_1 和执行主机 H_2 之间的委托信任关系：<H_1> T <H_2> with S;

同（3），H_1 和 H_2 之间也无法直接建立委托信任关系，必须以验证服务器为中介。

安全级别 S 取决于两个实体之间的透明度和信任关系的维系周期。一般而言，透明度越高，维系周期越长，则 S 的级别越高。委托信任关系的不可勉强性导致其可由双方中的任何一方取缔。例如源主机 O 和执行主机 H 之间有委托信任关系<O> T <H> with S，若 O 派遣的移动代理被 H 攻击，则 O 会立即取缔这种信任关系，并告知验证服务器 VS；VS 核实后会取缔它与 H 的委托信任关系并对 H 的恶意行为在网络中进行广播。可见这种机制可以限制执行主机的恶意企图，大大提高安全性。

以下是委托信任机制的几个定理：

定理 1 由于委托信任关系是对称的，因而有<A> T <B> with S $\Leftrightarrow$ <B> T <A> with S，且信任关系随任意一方的取缔而消亡，而验证服务器 VS 是绝对可信任的；

定理 2 <A> T <B> with S_1，<B> T <C> with $S_2 \Rightarrow$ <A> T <C> with S_0，其中 $S_0=\min\{S_1, S_2\}$，可见委托信任关系具有传递性；

定理 3 对定理 2 可以扩展至 n 步，即传递的路径可以无限延长；

[1] 证明：若已知<VS> T <O> with S 和<VS> T <H> with S 成立，根据定理 1，可得<O> T <VS> with S，再根据定理 2，则可推出<O> T <H> with S 成立。

定理 4　<A> T <网络中的其它所有主机> with { S_1, S_2,…}，且 min{S_1, S_2,…}已达到 A 所需求的安全级别，则整个网络对于 A 而言是可信任的。

委托信任机制的引入可以提高路由选择的效率和安全级别，延续 3.1 节图 2(b)的讨论，以移动代理 1 为例阐述这种机制所起的作用。如图 3 所示：

可信任的验证服务器与节点 0, 1, 2, 5, 8, 11 建立了委托信任关系：<VS> T <O_0> with S，<VS> T <H_1> with S…，根据定理 1、定理 2 和定理 3，可推出<O_0> T <H_1> with S，<H_1> T <H_2> with S…<O_0> T <H_5> with S 等。移动代理 1 协同其警卫 Agent 到目标节点 5 执行任务，迁移路由如图 3 所标识，警卫 Agent 根据携带的委托信任关系表，仅需对节点主机 6 和主机 7 进行监测，即可保证移动代理 1 的安全，因为路由上的其它节点均为可信任节点。

优点　减轻了警卫 Agent 的负担，节省了系统开销；增加了可信任的验证服务器，提高了安全性能，增加了透明性，使路由选择更加有效。

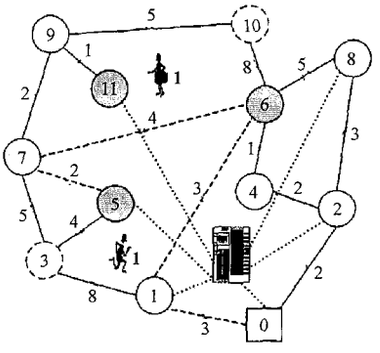

图 3　引入委托信任机制的网络路由安全分析

3.2.2　*路由表结构的改进*　在网络中添加验证服务器建立起委托信任机制之后，可以对移动代理的路由表结构进行改造。在 3.1 节中，各链路的可用带宽是事先根据各网络节点的预测平均经验值来设定的，也没有考虑链路长度，随机性较大，且在实践中的可操作性也较差，因此有必要对其进行改进。

由于任务代理的行程路线可能是根据网络负载动态变化的，改进时要求源主机委派的任务代理携有动态更新的路由表，且能自主产生从代理协助其建立一个从当前节点到其它路由节点的距离统计模型以估算网络的负载流量。携有委托信任关系表的警卫 Agent 仍然负责任务代理的安全。

改进后的路由表 T_k 所包含的数据是不同的目的节点 d 与其每一个不同的相邻节点 n 的选择概率值 P_{nd}，亦即是当目的节点是 d 时选取相邻节点 n 为下一个节点的概率。在保证安全性之后，任务代理将根据 P_{nd} 的值选择下一个行程节点。与传统路由表结构不同的是，依据各相邻节点选择概率的比特值，将能准确估测出网络的负载流量，且不保留明确的网络拓扑结构，以便移动代理能充分利用网络资源。显然，路由表 T_k 的数据存储必须符合式(1)的要求——对应于同一目的节点的所有相邻节点的选择概率值之和等于 1，其中，n 代表此节点的任一相邻节点，共有 N_k 个；d 表示网络中的任意节点，共有 N 个。

$$\sum_{n\in N_k} P_{nd}=1,\quad d\in[1,N],\quad N_k=\{\text{neighbors}(k)\} \tag{1}$$

任务代理在其从代理的协助下，还能在迁移过程中动态建立起一张数据表 $M_k\left(\mu_d,\sigma_d^2,\varpi_d\right)$，以映射某一节点 k 所观察到的全网各个节点距离的简单参数统计模型。该模型是自适应的，通过移动代理所经历的行程时间的反馈来更新得到统计模型的平均值 μ_d 和方差值 σ_d^2，并用 ϖ_d 来保存最近一段时间窗口内最佳的代理行程时间。对于每一个目的节点 d，通过估算的平均值 μ_d 和方差值 σ_d^2 来反映对本地节点、目的节点之间行程的期望时间和此期望时间的稳定性。该数据表可以存储在节点 k 本地，以减轻从代理的负载。

T_k 和 M_k 可以看成是节点 k 对动态网络各方面情况的估计：M_k 包含了从本节点到所有节点的绝对距离和行程时间估计，其主要作用是动态的对 T_k 中各个目的节点与其相邻节点的选择概率进行更新。当节点 k 收到从代理由 k 迁移到目的节点 d 的行程时间之后，将对距离统计表 M_k 进行刷新，可以采用算术、指数和窗口的策略来动态计算该统计模型。而路由表 T_k 中选择概率 P_{nd} 的变化大小依赖于对行程时间 $T_{k\to d}$ 的评价。基于 M_k，可引入行程时间函数 $r=r\left(t,M_k\right)$，$r\in(0,1]$，作为 $T_{k\to d}$ 的衡量标准，并实现对 P_{nd} 的更新。r 的精确定义可通过式(2)来实现：

$$r=c_1\frac{W_{\text{best}}}{t}-c_2\frac{t-\mu}{\sigma} \tag{2}$$

W_{best} 是移动代理向着目的节点 d 前进时在最近的观察窗口 ϖ_d 中的最优行程时间，t 是从本节点到目的节点的行程时间，μ 是统计模型中对行程时间的期望值，σ 指行程时间在期望值附近的偏差。式(2)中的第一个表达式计算了在观察窗口中最佳行程时间与即时所得的行程时间之间的比率，第 2 个表达式计算行程时间 t 与长期观察得来的行程时间平均值 μ 之差和波动范围 σ 的比较，用于校正第 1 个表达式。系数 c_1 和 c_2 用于衡量两个表达式的重要性。第 1 个表达式起主导作用，第 2 个表达式对其进行校正。

r 综合两个因素：已有的行程时间的平均值和它们的变化，来对行程时间 t 进行衡量。在有了对路由移动代理行程时间的客观评价之后，概率 P_{nd} 可通过式(3)进行更新：

$$P_{nd} \leftarrow P_{nd} + r\left(1 - P_{nd}\right) \tag{3}$$

而以 d 为目的节点的其它相邻节点的概率 $P_{n'd}$ 将会减小，可以通过式(4)计算得到

$$P_{n'd} \leftarrow P_{n'd} - rP_{n'd}, \qquad n' \in N_k, \quad n' \neq n \tag{4}$$

可见，$P_{n'd}$ 得到更新的同时也保证了所有以 d 为目的节点的概率之和还是 1。

以上对路由表结构的调整，有效弥补了 3.1 节中对(2)，(3)两点加限制条件讨论的缺憾，用行程时间及其变化来选择路由，减少了选择的随机性，增加了正确性；且主从代理及警卫 Agent 的协同工作也提高了系统效率和安全。

4 结束语

路由选择是移动代理在网络中迁移的关键技术，而安全性、高效性和最优化则成为路由管理的核心问题。本文建议的路由安全管理方案充分利用了多移动代理协作的优越性。负责保护任务代理安全的警卫 Agent（Proxy Agent）的提出是移动代理安全性研究的一个重要创新，它们能排除系统的安全隐患，增加透明度和有效性；而委托信任机制和可信任验证服务器的引入也进一步提高了系统的效率和安全级别；路由表结构的改进则减少了路由选择的随机性，增加了实践的可操作性。这几种机制都依赖于系统中多个移动代理的协作和交互。然而，由于移动代理缺乏统一的国际标准，在“规范化”问题上依旧存在障碍，例如代理平台的多样化、通信机制和接口的兼容性等等，OMG 和 FIPA 正致力于规范化工作的进展[10]。当然，委托信任机制的进一步深入，动态路由表、距离统计模型的数据结构和仿真实验以及传输时延和路由“死锁”问题则是下一步研究工作的重点。

参 考 文 献

[1] Wang X F, Yi X, Lam K Y. Secure information agent for internet trading. 11th Australian Joint Conference on Artificial Intelligence'98. Vol.1, No.544, Brisban, Australia: Springer- Verlag Publishers, 1998: 183 – 194.

[2] Ye Yiming, Yi Xun. Coalition signature scheme in multi-agent system. 11th International World Wide Web Conference, Honolulu, Hawaii, USA, 7 – 11 May, 2002: 96 – 102.

[3] Chaum D, van Heyst E. Group signatures. In D.W.Davies, editor, Proc. of Eurocrypt'91, vol. 547 of LNCS, Springer-Verlag, 1992: 257 – 265.

[4] Bresson E, Stern J, Szydlo M. Threshold ring signature for ad-hoc groups, Advances in Cryptology-Proceedings of CRYPTO'02, Santa Barbara, California, USA. August 18 – 22, 2002: 465 – 480.

[5] 赖溪松，韩亮，张真诚著，张玉清，肖国镇改编. 计算机密码学及其应用. 北京：国防工业出版社，2001：第 21 章，196 – 199.

[6] Roth V. Mutual protection of cooperating agents. In Jan Vitek and Christian Jensen, Editors, Secure Internet Programming: Security Issues for Mobile and Distributed Objects, vol. 1603 of Lecture Notes in Computer Science, 1997: 275 – 285.

[7] Dorigo M, Maniezzo V, Colorni A. The ant system: optimization by a colony of cooperating agents. *IEEE Trans. on Systems, Man, and Cybernetics-PartB*, 1996, 26(1): 29 – 41.

[8] Mitrovic N, Arronategui U. Mobile agent security using proxy-agents and trusted domains. Second International Workshop on Security of Mobile Multi-agent Systems (SEMAS 2002), Bologna, Italy, July 2002: 81 – 83.

[9] Sander T, Tschudin C. Protecting mobile agents against malicious hosts. Mobile Agents and Security, Springer-Verlag, Lecture Notes in Computer Science. No.1419, 1998: 44 – 60.

[10] 张云勇. 移动 Agent 及其应用. 北京：清华大学出版社，2002，第 4 章，28 – 35.

王汝传： 男，1943 年生，教授，博士生导师，主要研究方向为计算机软件、计算机网络、信息安全、移动代理和虚拟现实技术等.

黄海平： 男，1981 年生，硕士生，主要研究方向为计算机网络、计算机软件在通信中的应用和信息安全.

李明远： 男，1979 年生，硕士生，研究方向为计算机网络和信息安全.