

## 基于声誉的 P2P 信任系统

李健利, 高 勇, 霍光磊, 刘 博

(哈尔滨工程大学 计算机科学与技术学院, 哈尔滨 150001)

(lijianli@hrbeu.edu.cn)

**摘 要:** 针对增强型声誉系统中资源访问的“热点”问题, 提出一种实现资源均衡访问机制的 P2P 声誉系统, 并加入自动信任协商来改善该系统的信任推理机制, 提高该系统的协商效率。仿真结果表明使用 P2P 声誉系统解决了节点间提供服务的瓶颈问题, 资源请求节点和资源提供节点间交互成功率显著提高。

**关键词:** 增强型声誉系统; 资源均衡; 自动信任协商; 对等网络

**中图分类号:** TP393.08 **文献标志码:** A

## Reputation-based P2P trust system

LI Jian-li, GAO Yong, HUO Guang-lei, LIU Bo

(College of Computer Science and Technology, Harbin Engineering University, Harbin Heilongjiang 150001, China)

**Abstract:** Concerning the "hot spots" problem of resource access in the enhanced-reputation system, the P2P reputation system of resource balance access mechanism was proposed, and automated trust negotiation was joined to improve the system reason mechanism of confidence and negotiation efficiency. The simulation results show that P2P reputation system solves the bottleneck problem providing services of among nodes, and the success rate of interaction between requesting and providing resource nodes has been significantly improved.

**Key words:** enhanced-reputation system; resource balance; automated trust negotiation; Peer-to-Peer (P2P) network

### 0 引言

P2P 网络是指一些以非集中的方式来充分利用一些分散资源完成某些功能的系统与应用<sup>[1]</sup>。P2P 网络中现存的声誉系统普遍存在资源访问“热点”和交互成功率比较低的问题, 如何解决这两个问题仍然是声誉系统中亟待解决的问题。

EBay<sup>[2]</sup> 将所有信息都保存在一个中心服务器上, 中心服务器可能存在访问的“热点”问题, 且执行效率不能满足 P2P 网络的要求。增强型声誉系统<sup>[3]</sup> 的节点总是选择从信任值最高的节点处请求服务, 这样有可能会造成声誉好的节点负荷过重, 产生拥塞。

针对现存声誉系统存在的问题, 本文在增强型声誉系统基础上提出一种改进的 P2P 声誉系统, 该系统有效地解决了现有声誉系统中资源访问的“热点”问题, 并在此系统的基础上结合自动信任协商解决 P2P 网络中节点间交互成功率比较低的问题。

### 1 P2P 声誉系统

#### 1.1 系统设计思想

在增强型声誉系统中, 由于节点总是选择从综合信任值最高的节点处提供请求服务, 这样可能会导致这些节点负荷过重, 产生拥塞。本文的解决方法是在信任值评估中加入资源的信任值, 以文件内容的散列值为其 ID, 只要提供服务的节点的确是声誉好的节点所推荐, 那么可以从声誉稍差一些的节点处下载, 因为它们的内容是相同的。

#### 1.2 P2P 声誉系统模型

本文设计的 P2P 声誉系统模型如图 1 所示。

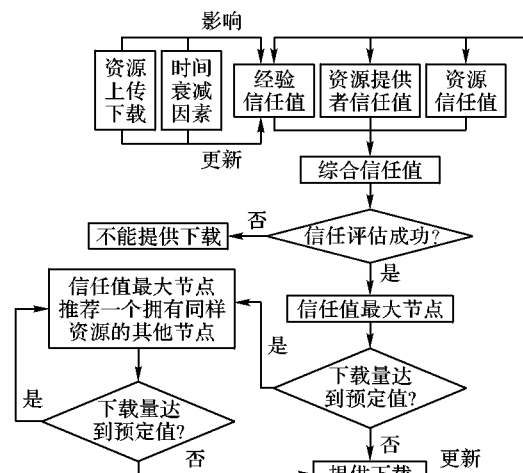


图1 P2P 声誉系统模型

**经验信任值** 请求资源下载的节点对提供资源下载的节点的信任值。

**资源提供者信任值** 网络中其他节点对该节点提供下载服务的推荐信任值。

**资源信任值** 网络中的每个节点都会存储一张资源质量表, 其中, 资源 ID 对应的项即为节点对该资源的资源信任值。

**资源上传下载** 网络中的节点上传资源和下载资源的数量。

**时间衰减因素** 该节点和其他节点进行交流合作的时间。

从图 1 可以看出, 一个节点的信任值由经验信任值、资源提供者信任值和资源信任值三部分组成。其中经验信任值要考虑两个影响因素: 一是该节点上传和下载资源的情况, 本文

收稿日期: 2010-06-07; 修回日期: 2010-07-06。 **基金项目:** 国家自然科学基金资助项目(61073042)。

**作者简介:** 李健利(1963-), 男, 黑龙江哈尔滨人, 副教授, 主要研究方向: 信息安全、人机交互; 高勇(1985-), 男, 黑龙江海倫人, 硕士研究生, 主要研究方向: 信息安全; 霍光磊(1982-), 男, 黑龙江哈尔滨人, 硕士研究生, 主要研究方向: 信息安全; 刘博(1986-), 男, 内蒙古满洲里人, 硕士研究生, 主要研究方向: 信息安全。

认为节点上传的资源越多,其信任值越高;二是时间衰减因素,如果长时间没有和别人通信,其信任值会下降。通过这三个信任值的综合,得到能够提供下载服务的节点总的信任值。

根据这个总的信任值进行评估,如果评估失败(网络中未找到提供该资源下载的节点),显示不能提供资源下载请求。如果评估成功(本文中的评估成功指请求服务的节点能够找到网络中提供资源下载的并且信任值最大的节点),则查看该节点提供资源的下载量,如果未达到节点下载该资源的预定数量(这个值依据系统中节点数量自行确定),那么该节点可以提供资源下载服务,并更新模型图中的三个信任值。否则,由信任值最大的节点推荐一个拥有和自己同样资源的其他节点提供服务,同样,该节点若未达到资源下载预定数量,就可以执行下载要求,并更新模型图中的三个信任值。如果该节点也已经达到资源下载的最大数量,则信任值最大的节点继续进行推荐。

系统执行流程如下。

1) 资源搜索。该系统通过广播向邻近的节点发送查询某个资源的请求,返回符合搜索关键字的节点数量、包含文件名相关信息的查询结果(ResultSet)、提供者标识(Server\_Id)、提供者的IP地址和端口号、资源文件的散列值。

2) 资源选取和推荐。节点从搜索到的结果中选取一个符合自己要求的资源,并向周围其他节点发出推荐请求,请求包括对资源的推荐和对资源提供者的推荐。收到请求后,节点根据自己的资源质量表和资源提供者表来进行推荐,并把推荐者的IP地址、端口号和推荐结果通过用请求者公钥进行加密的方式返回给资源请求者。

3) 计算提供资源请求服务的节点最终信任值。根据本地节点的经验信任值,其他节点推荐的提供者信任值和资源信任值,综合算出该节点最终信任值,其计算方式后文将详细讲述。

4) 选择最优下载节点。决定下载该资源后,还需要考虑从哪个提供节点处下载。如果总是选择综合信任值最大的节点处下载资源,可能会导致该节点出现瓶颈问题。所以,本文采取的方法是从该节点处确认一下该资源的确是它拥有的,然后可以选择从别的提供节点处下载。

5) 资源下载。请求下载资源的节点直接向所选中的提供节点处发送下载请求,当资源下载完毕后,节点再次对资源进行验证,如不符合则丢弃。最后,根据资源和该资源提供者的表现,节点更新模型图中三个信任值。

### 1.3 资源提供者信任值

信任是分等级表示的,既可以用离散值表示也可以用连续值表示,本文选择用连续值(0,1)表示,其中0代表完全不信任,1代表完全信任。对于资源提供者信任值的计算,本文采用的计算公式如式(1)和式(2)所示:

$$tw_1(A, F) = \frac{trv(A, B) + trv(B, E)}{2} \times tfv(E, F) \quad (1)$$

$$tw(A, F) = \sum_{i=1}^n w_i \times tw_i(A, F) \quad (2)$$

其中:本文假设在构造搜索信任链时,间接信任链的长度不超过2;trv(A, B)表示A对B间接推荐信任值;tfv(E, F)表示E对F的直接推荐信任值;tw<sub>i</sub>(A, F)为A到F的第i条信任链上A对F的信任值;tw(A, F)为A到F的所有信任链的综合信任值 $\sum_{i=1}^n w_i = 1$ , w<sub>i</sub>表示第i条信任链在所有信任链中所占的权重。

### 1.4 综合信任值

将文中的经验信任值、推荐信任值和资源信任值加权平均得到节点总的信任值如式(3)所示:

$$T(A, F) = \alpha \cdot Ev(A, F) + \beta \cdot Rv(A, F) + \gamma \cdot Rt(A, F) \quad (3)$$

其中:T(A, F)为节点A对节点F的综合信任值;Ev(A, F)为节点A对节点F的经验信任值;Rv(A, F)为网络中的节点对节点F的推荐信任值(即资源提供者信任值);Rt(A, F)为节点A对节点F的资源信任值; $\alpha, \beta, \gamma$ 为比例系数, $0 \leq \alpha \leq 1$ ,  $0 \leq \beta \leq 1$ ,  $0 \leq \gamma \leq 1$ ,  $\alpha + \beta + \gamma = 1$ 。

### 1.5 更新信任值计算

1) 时间衰减因素的影响。在现实P2P网络中,如果节点长时间没有和其他节点交互,那么它本身的信任值会有所下降。本文采用的计算公式如式(4)所示:

$$T_{new} = \frac{1}{\lambda \cdot \Delta t + 1} T_{old} \quad (4)$$

其中:T<sub>old</sub>为更新前的信任值;T<sub>new</sub>为更新后的信任值; $\Delta t$ 为两次信任值更新时间之差; $\lambda$ 为参数,且 $0 \leq \lambda \leq 1$ 。

2) 服务的利用与供给。为了防止P2P网络中的节点只是一味索取,不提供服务,因此,该系统要考虑服务的利用与供给因素,采用的公式如式(5)所示:

$$T_{new} = \frac{1}{\mu \cdot Da/Ua + 1} T_{old} \quad (5)$$

其中:T<sub>old</sub>为更新前的信任值;T<sub>new</sub>为更新后的信任值;Da为节点利用网络中服务的量;Ua为节点提供服务的量; $\mu$ 为参数,且 $0 \leq \mu \leq 1$ 。

3) 反馈评价计算。更新操作是请求资源下载者对提供资源的质量、提供人和经验信任值的评估,根据提供资源的质量可以采用以下的计算方式进行计算:

$$T_{new} = T_{old} \pm \beta \quad (6)$$

其中:T<sub>old</sub>为更新前的信任值;T<sub>new</sub>为更新后的信任值; $\beta$ 为更新的参数,且 $0 \leq \beta \leq 1$ 。当提供优质的资源时,就采用加的操作;当提供的资源不满意时,采用减的操作。如果更新后的信任值比0小或者比1大,则将信任值分别取0和1。

### 1.6 模型图中三个信任值的存储

网络中的每个节点会保存有关资源质量的信息、提供服务节点的经验信息和资源提供者的推荐信息,为了方便存储和管理,本模型中要求每个节点维持三个表:资源质量表、资源提供者推荐表和推荐信任值表。其中,资源质量表中给出资源ID及其对应的资源质量值,资源质量值用0和1表示,0代表不好,1代表好。资源提供者推荐表中给出资源提供者ID和提供者信任值。经验信任值表中给出提供资源节点的ID号以及对提供服务者的经验信任值。

### 1.7 系统效率问题

由于本文是在增强型声誉系统的基础上进行的改进,而增强型声誉系统采用了加密技术,因而推荐信任值在网络中传输时,一定会多花费一些时间,在计算信任值时也会有相应的时间延迟。本文采用定期计算的方式来解决此问题,每个节点都定期更新自己的本地数据库,当使用者想要了解某一节点信任值时,可不经计算,直接从本地数据库中取出信任值。

## 2 混合系统

本文前面提出的声誉系统模型主要解决资源提供者的信任问题,而自动信任协商主要解决资源请求者的可信问题。

现存的P2P声誉系统中缺乏信任推理机制,且执行效率比较低,使得网络中节点交互成功率受到影响。因此,本文在该系统的基础上加入自动信任协商机制,通过使用加密信任凭证和访问控制策略来防止敏感信息泄露,从而提高网络中节点间交互成功率。

### 2.1 混合系统中的协商策略

在一次资源请求的交互过程中,是否需要自动信任协商将取决于资源提供者的策略,当资源请求者向资源提供者发送下载请求时,资源提供者会根据本地的策略来决策,决策结果有三种情况:允许、拒绝和信任协商。

1) 公开资源可以为任何节点提供服务,请求这类资源时一律返回“允许”。

2) 对资源进行服务控制的请求,请求节点的信任值高于某个设定值时“允许”,低于其值时要求“信任协商”。

3) 对于服务严格控制的请求,要进行“信任协商”。

4) 对私有服务进行资源请求时,统一返回“拒绝”。

### 2.2 混合系统中的信任证和访问控制策略

数字证书<sup>[4]</sup>是用来携带用户身份/属性等相关特征的数字化工具。本文使用的加密信任证技术为 Hidden Credentials<sup>[5]</sup>。

访问控制策略<sup>[6]</sup>是用来保护资源不被合法用户的非授权访问,从而规范合法用户对资源的操作。它决定在自动信任协商(Automated Trust Negotiation, ATN)中暴露哪些证书以及这些证书暴露的先后顺序。本文使用的访问控制策略是 OSBE<sup>[7]</sup>策略。

策略语言<sup>[6]</sup>是用来描述 ATN 中的访问控制策略和信任凭证的,它是 ATN 中的重要工具。在混合系统中使用的策略语言是 ATNL<sup>[8]</sup>。

### 2.3 混合系统的实用性方案

#### 2.3.1 应用背景

P2P 文件共享系统要求该系统具有搜索和下载网络中资源的功能。用户首先进行资源搜索,可以利用本文提出的 P2P 声誉系统给出每个搜索结果的量化信任值,并提供给请求者一个节点进行下载。

#### 2.3.2 设计思想

针对 P2P 声誉系统缺乏信任推理机制和执行效率低下的问题,本文在第1章提出的改进型声誉系统的基础上加入了自动信任协商技术。声誉系统是从量化的角度来解决网络中节点间提供请求服务的问题,而自动信任协商是从逻辑推理角度来实现信任的可靠建立。因此,可以将两种技术结合起来建立一个更加可靠、高效的混合系统。当请求者想要访问一些非敏感资源时,他可能更倾向于使用声誉系统给出的量化信任值来指导信任的建立;当用户访问一些敏感资源时,或者是请求者本身的一些信息敏感时,就需要使用自动信任协商来解决。

#### 2.3.3 混合系统结构

混合系统的结构如图2所示。图2中箭头表示信息流的方向,实线表示依赖关系,虚线表示需要穿越网络。

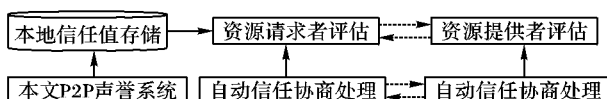


图2 混合系统应用结构

本地信任值存储 保存本地节点对其他节点的信任值,由本文提出的 P2P 声誉系统负责。

本地信任评估 根据声誉系统和自动信任协商模块来决定是否信任目标节点。

资源提供者评估 根据自动信任协商给出三种凭估结果:允许、拒绝和继续信任协商。

自动信任协商处理 完成信任协商的建立。

### 2.4 混合系统执行流程

本文设计的混合系统执行流程如图3所示。

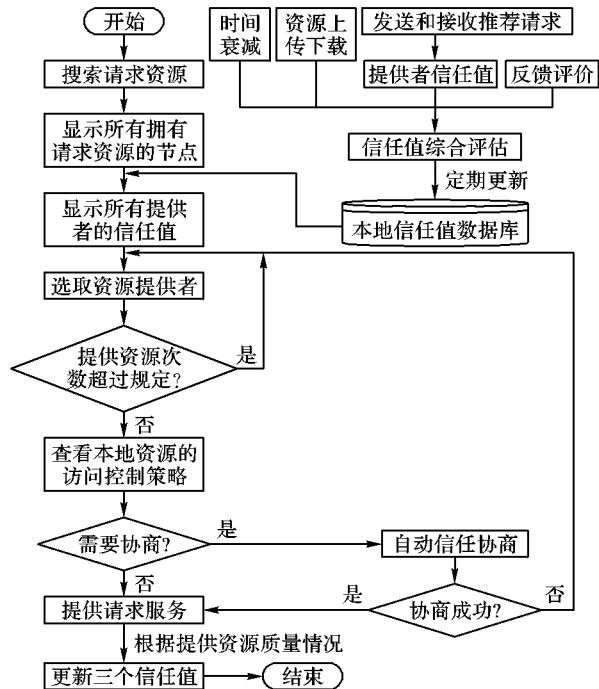


图3 混合系统的执行流程

### 2.5 系统执行流程说明

1) P2P 网络中想要请求服务的节点对网络进行搜索,找到拥有相应资源的节点。

2) 请求服务的节点向所有邻近节点发送推荐提供服务节点的请求,对搜索到的节点算出提供服务节点的信任值。

3) 把模型图中三个信任值进行综合,算出每个拥有资源的节点的最终信任值。

4) 从提供资源的所有节点中选择信任值最高的节点请求服务,发送服务请求。

5) 信任值最高的节点对本地存储的该资源提供服务的次数进行检查,如果没有超过指定值,则执行步骤6);否则,查询本地存储的资源信任值,找到能够提供服务请求的比自己信任值低的其他节点推荐给服务请求者节点。

6) 提供服务的节点查看本地的资源的访问控制策略,如果本身没有提供访问控制策略,则可以直接提供服务,转到步骤8)执行。

7) 提供服务的节点需要进行协商,在 P2P 声誉系统中进行自动信任协商,如果协商没有成功,转到步骤5)执行。

8) 提供服务的节点提供相应的请求服务。

9) 请求服务的节点根据请求资源的质量更新模型图中三个信任值。

## 3 系统模拟

仿真实验中使用的系统仿真环境有:硬件环境,P4 3.0 GHz,512 MB 内存;运行环境,Windows XP Professional 2002,仿真平台,JXTA 2.4.1;开发语言,Java。仿真参数为

$\alpha = 0.7, \beta = 0.2, \gamma = 0.1$ , 交互次数 500, 节点总数 1000, 节点提供服务次数 200, 下载要求的信任值为 0.6, 反馈计算的变量值为 0.1。

在仿真中没有考虑系统后续更新信任值的操作, 只是针对本文解决的问题进行实验模拟, 并没有真正建立一个完善的 P2P 声誉系统。在实验中忽略的因素有: 未能考虑信任值的传输, 没有考虑节点的上传和下载因素, 所有实验节点没有中途退出的可能性, 一直模拟到实验结束。

#### 1) 声誉系统中提供服务均衡性仿真实验。

为了验证本文提出的 P2P 声誉系统解决 P2P 网络中资源访问“热点”问题的效果, 本文在 JXTA 平台下使用 Java 语言编写了模拟程序, 在实验模拟中, 随机生成 1000 个节点, 其中规定节点序号是 200, 400, 600, 800 的节点可以提供网络中其他节点的请求下载服务其信任值根据本文提出的式(3)计算得出的关系为 200 号节点的信任值 > 400 号节点的信任值 > 600 号节点的信任值 > 800 号节点的信任值, 其余节点均没有相应的请求服务。本次实验一共进行了 500 次, 每次实验时规定请求服务的节点向网络中的其他节点请求 600 次服务, 并记录提供服务的节点提供的次数。最终, 对每个节点提供服务的次数取平均值。

绘制的图形如图 4 所示。图 4 中 A 代表增强型声誉系统, B 代表本文提出的 P2P 声誉系统。由实验可知, 增强型声誉系统在选择节点提供服务时总是选择信任值最高的节点, 因此很容易造成该节点拥塞, 而本文提出的 P2P 声誉系统会优先考虑信任值最高的节点提供服务, 但当服务次数到规定值 200 次时, 就选择其他节点提供服务, 不会造成资源访问“热点”问题。

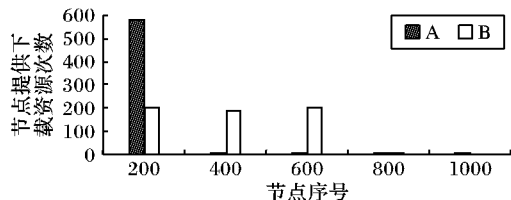


图4 声誉系统中提供服务均衡性仿真实验

#### 2) 混合系统和增强型声誉系统交互成功率仿真。

在仿真过程中的恶意节点包括提供虚假的资源下载服务和带有病毒的节点。在实验中交互了 500 次, 对每次实验结果取平均值, 仿真图形如图 5 所示。

仿真刚开始时, 由于网络中恶意节点比较少, 其需要自动信任协商中访问控制策略的节点不多, 加入自动信任协商使协商成功率受到影响。由于执行自动信任协商比较费时, 影响了节点间交互的效率。但是, 随着恶意节点数的增多, 采用

访问控制策略相应增多的情况下, 增强型声誉系统中节点间交互成功率明显下降, 而本文提出的混合系统节点间交互成功率比增强型声誉系统有较大的提高, 这充分体现出本文提出的混合系统的价值。

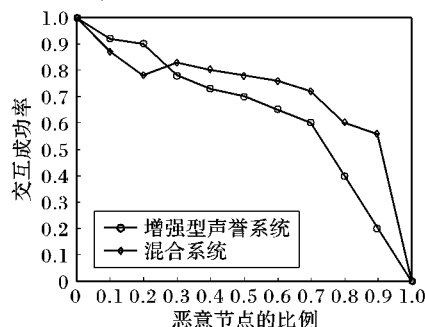


图5 交互成功率仿真实验

## 4 结语

本文在增强型声誉系统的基础上进行改进, 提出一种改进的 P2P 声誉系统, 该系统解决了 P2P 网络中节点提供服务的“热点”问题, 并在该系统基础上, 引入了自动信任协商机制, 进一步解决了 P2P 网络中的敏感信息泄露问题, 随着恶意节点的数量增多, 混合系统的优势得以充分体现。

#### 参考文献:

- [1] 冯真, 张红旗, 刘育楠. 自动信任协商在 P2P 系统中的应用[J]. 计算机工程, 2007, 33(6): 132-133, 136.
- [2] EBay [EB/OL]. [2010-04-13]. <http://www.ebay.com>.
- [3] 冯真. P2P 环境下文件共享的声誉系统研究[D]. 郑州: 信息工程大学, 2006.
- [4] 廖振松, 金海, 李赤松, 等. 自动信任协商及其发展趋势[J]. 软件学报, 2006, 17(9): 1933-1948.
- [5] HOLT J E, BRANDSHAW R W, SEAMONS K E, et al. Hidden credentials[C]// WPES'03. New York: ACM, 2003 [2010-03-22]. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.2.5797&rep=rep1&type=pdf>.
- [6] 李建欣, 怀进鹏, 李先贤. 自动信任协商研究[J]. 软件学报, 2006, 17(1): 124-133.
- [7] LI JIANGTAO, LI NINGHUI. OACerts: Oblivious attribute certificates[J]. IEEE Transactions on Dependable and Secure Computing, 2006, 3(4): 340-352.
- [8] LI JIANGTAO, LI NINGHUI, WINSBOROUGH W H. Automated trust negotiation using cryptographic credentials[C]// ACM Conference on Computer and Communications Security. New York: ACM, 2005: 100-108.
- [9] 冯真, 张红旗, 刘育楠. 自动信任协商在 P2P 系统中的应用[J]. 计算机工程, 2007, 33(6): 132-133, 136.
- [10] EBay [EB/OL]. [2010-04-13]. <http://www.ebay.com>.
- [11] 冯真. P2P 环境下文件共享的声誉系统研究[D]. 郑州: 信息工程大学, 2006.
- [12] 廖振松, 金海, 李赤松, 等. 自动信任协商及其发展趋势[J]. 软件学报, 2006, 17(9): 1933-1948.
- [13] HOLT J E, BRANDSHAW R W, SEAMONS K E, et al. Hidden credentials[C]// WPES'03. New York: ACM, 2003 [2010-03-22]. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.2.5797&rep=rep1&type=pdf>.
- [14] 李建欣, 怀进鹏, 李先贤. 自动信任协商研究[J]. 软件学报, 2006, 17(1): 124-133.
- [15] LI JIANGTAO, LI NINGHUI. OACerts: Oblivious attribute certificates[J]. IEEE Transactions on Dependable and Secure Computing, 2006, 3(4): 340-352.
- [16] LI JIANGTAO, LI NINGHUI, WINSBOROUGH W H. Automated trust negotiation using cryptographic credentials[C]// ACM Conference on Computer and Communications Security. New York: ACM, 2005: 100-108.
- [17] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.
- [18] MAO YINIAN, SUN YAN, WU MIN, et al. JET: Dynamic join-exit-tree amortization and scheduling for contributory key management[J]. IEEE/ACM Transactions on Networking, 2006, 14(5): 1128-1140.
- [19] ZHENG SHANYU, MANZ D, ALVES-FOSS J. A communication-computation efficient group key algorithm for large and dynamic groups[J]. Computer Networks, 2007, 51(1): 69-93.
- [20] ALVES-FOSS J. An efficient secure authenticated group key exchange algorithm for large and dynamic groups[EB/OL]. [2010-02-10]. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.1326>.
- [21] BECKER K, WILLE U. Communication complexity of group key distribution [C]// Proceedings of 5th ACM Conference on Computer and Communications Security. New York: ACM, 1998: 1-6.
- [22] TRAPPE W, WANG Y, LIU K J R. Resource-aware conference key establishment for heterogeneous networks[J]. IEEE/ACM Transactions on Networking, 2005, 13(2): 134-146.
- [23] AGARWAL D A, CHEVASSUTY O, THOMPSON M R, et al. An integrated solution for secure group communication in wide-area networks[C]// Proceedings of the 6th IEEE Symposium on Computers and Communications. New York: IEEE, 2001: 22.

(上接第 146 页)