第35卷 第18期 计 算 机 工 程 2009年9月
Vol.35 No.18 Computer Engineering September 2009
·安全技术· 文章编号：1000—3428(2009)18—0142—03 文献标识码：A 中图分类号：N945

基于分层代理的P2P网络信誉管理模型

刘 浩[1,2]，张连明[1]，彭利民[1]
(1. 华南理工大学计算机科学与工程学院，广州 510640；2. 湖南人文科技学院计算机科学技术系，娄底 417000)

摘 要：针对大多数信誉管理机制忽略节点的匿名性和其中的信息洪泛现象，构造一种基于分层信誉代理的P2P网络信誉管理模型HARMM。该模型采用多个公/私钥组合使用和洋葱路由等方法，通过理论分析及仿真实验证明该模型能较好地保证节点匿名性和数据可信性，有效抵抗一些典型的安全攻击。

关键词：P2P网络；信誉管理；信誉代理；洋葱路由

Reputation Management Model of P2P Network Based on Hierarchical Agents

LIU Hao[1,2], ZHANG Lian-ming[1], PENG Li-min[1]
(1. School of Computer Science & Engineering, South China University of Technology, Guangzhou 510640;
2. Department of Computer Science and Technology, Hunan Institute of Humanities, Science and Technology, Loudi 417000)

【Abstract】 Due to the neglect of peer anonymity and information flooding in most reputatioin management mechanisms, this paper proposes a reputation management model of P2P network based on hierarchical Agents named HARMM(Hierarchical-Agents-based Reputation Managerial Model), which uses several public/private key pairs, onion routing and other methods. Analysis and simulation tests prove that the model is capable of guaranteeing peer anonymity and data authenticity, and effectively restrains several typical security attacks.

【Key words】 P2P network; reputatioin managemnet; reputation Agent; onion routing

1 概述

P2P网络因其开放性导致了大量不良数据的快速传播，于是人们引入信誉管理模型来保证数据的可信性。一般认为，信任是一种主观信念，可理解成一个实体评价其他实体行为的主观可能性程度[1]。而信誉是一个来自某团体所有成员的全局量，即所有其他成员对某一成员评价结果的综合。因此，在P2P网络中建立性能良好的信誉管理机制十分必要。目前大多数信誉管理机制是通过牺牲匿名性和洪泛机制实现的，如Eigenrep[2]，这给P2P网络安全带来了新的问题。基于分布式哈希表(DHT)的网络信任机制的固有缺陷使其无法适用于大规模P2P网络。对于非结构化P2P网络，如果采用完全分布式机制，容易导致信息洪泛现象，但若使用依赖于中心节点的信誉管理服务器，将带来通信瓶颈和单点失效等问题。而采用层次结构的信誉管理系统既可以获得两者的优点，又可避免它们的缺陷。本文提出的基于分层代理的P2P网络信誉管理模型 HARMM(Hierarchical-Agents-based Reputation Managerial Model)能很好地保证节点匿名性和数据可信性。

2 HARMM

2.1 洋葱路由

洋葱路由方案采用了实时双向隐藏路径的实现方法，它在请求站点的代理服务器与目标主机之间进行匿名连接，其数据流经过若干中间洋葱路由器后抵达目的站点从而形成一条隐藏路径。源节点处理数据从后向前逐层采用不同的加密密钥加密信息包，收到该数据包的中间节点只能解密最外层，整个包的格式如同多层的洋葱[3]。由于每个中间站点只能解密数据包的最外层，中间站点不可能得知有关信息，因此可达到信息隐匿的目的。

对于任意节点，给出如下定义：

定义1 称二元组(AP, AR)为匿名密钥对，用于保证消息的匿名性。

定义2 称二元组(SP, SR)为签名密钥对，用于保证消息的真实性。

定义3 设W为任意节点，则分别称AP_W, AR_W, SP_W, SR_W为节点W的匿名公钥、匿名私钥、签名公钥、签名私钥。

定义4 设*nodeID*为节点的身份标识，*nodeID*为采用约定哈希函数对*SP*进行哈希得到的哈希值。

用户通过身份标识*nodeID*构建自己的信誉，该信誉值只与其公共签名密钥相关，与真实世界中的身份无关。但节点的匿名密钥对和它的IP地址相关联。

定义5 设*nounce*为时间戳，用于防止消息重放攻击。

一次路由中继获取匿名公钥的协议如图1所示。由于节点P知道节点K的IP地址，因此选择K作为它的洋葱路由中继。协议如下：

(1)P直接发送一个路由中继请求(R_o, SP_p, IP_p)到K，将自己的SP_p和IP_p告知K，R_o表示路由中继请求。

(2)K发回一个应答消息给P，消息格式为$SP_p(AP_k, IP_k, nounce)$，其中用SP_p进行加密。

(3)收到来自K的应答后，P用SR_P签名的消息$SR_P(AP_p, IP_p, nounce)$发送给K。

基金项目：中国博士后科学基金资助项目(20070420782)
作者简介：刘 浩(1977－)，男，博士研究生，主研方向：P2P网络及其安全；张连明，副教授、博士后；彭利民，讲师、博士研究生
收稿日期：2009-01-10 **E-mail：**lhkd0407@126.com

(4)K 接收到这条消息后，用 SP_P 对其进行解密，并送回一条密钥确认消息 $SP_p(confirmed,\ IP_k,\ nounce)$，如果 P 没有收到这条确认消息，那么它就知道 AP_k 是非法的。

重复上述协议过程，从所有洋葱路由中继获得了匿名密钥后，P 就定义了一条到达自己的匿名路径，从而可以构造自己的洋葱包。其格式如下：

$$(((((((fakeOnion)AP_p)IP_p)AP_1)IP_1)\cdots AP_k)IP_k, sq)SR_p$$

其中，AP_i 是第 i 个节点的匿名公钥；sq 是非减性序号，表明洋葱包的年龄；P 用 SR_p 签名洋葱包保证整个包的真实性。

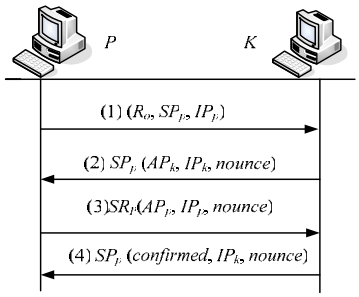

图 1　一次路由中继获取匿名公钥协议过程

定义 6 设 $Onion_{(P,Q)}$ 为一条由节点 P 到达节点 Q 的洋葱路由路径。

2.2　信誉代理社团

任何节点都可以申明自己作为信誉代理，但是只有信誉良好、高性能的节点才被选择作为可信信誉代理，所有的可信信誉代理共同组成信誉代理社团。

2.2.1　可信信誉代理的列表请求

任意节点 P 都在本地保存并维护一张对自身来说可信的信誉代理列表。该列表中每一个条目的格式如下：

$$\{weight,\ nodeID_{agent}, Onion_{(P,agent)}, SP_{agent}\}$$

其中，$Weight$ 为该信誉代理的权重；$agent$ 代表信誉代理节点。

当某节点首次加入这个 P2P 系统中，或者该节点想参考其他节点的推荐以收集一些信誉良好的可信代理时，它将发出一个可信代理列表请求到它的邻居节点，这个列表请求消息的格式为：$\{R_{al}, token, TTL\}$，其中，R_{al} 是一个可信代理列表请求；令牌数目 $token$ 与该节点想要收集的可信代理列表的数目相同，只有当一个节点返回它的可信代理列表给请求者时，才会消耗一个令牌；生存周期 TTL 限制了消息在网络中的流通时间，以防止发生洪泛现象。

2.2.2　代理排位与选择

请求者收到来自其他节点的可信代理列表后，将对每一个可信的信誉代理进行评估排位，假设请求者想要收集 n 个信誉代理，排位规则如下：

(1)评估权重最高的信誉代理的排位值为 n，评估权重次高的信誉代理的排位值为 n-1，依此类推。

(2)如果收到的可信代理列表中的信誉代理数目 m 大于请求者的需求数目 n，则剩余的 n-m 个信誉代理排位值将被评估为 0。

(3)如果同一个信誉代理出现在获得的多个不同代理列表中，选择其最高的权重值作为其排位的依据。

排位结束后，请求者根据最终的排位选择它的可信信誉代理，组成本地可信代理列表。

2.2.3　可信信誉代理的更新

当请求者组织好它的本地可信代理列表后，将每一个代理的权重值初始化为 0，并且在每一次服务后对其权重值进行更新。假设代理 E 的权重值为 A_p，而在当前服务中的评估值为 A_c，那么当前服务完成后代理 E 的权重值就更新为

$$A_p = \alpha A_c + (1-\alpha)A_p,\ \alpha \in (0,1) \tag{1}$$

其中，A_c 取值为(-1,0,1)。当本次服务的质量与该信誉代理提供的评估值严重不符时 A_c 取值-1，基本符合时评估值取 0，很符时评估值取 1。

2.3　信任值分布式处理

信任值分布式处理过程应能同时保证选举者的匿名性及信任值的真实性。选举者包括可信信誉代理和向各自的可信代理报告服务评价结果的节点。

可信信誉代理要保存并维护一张节点的签名公钥列表，该列表的格式如下：

$$\{nodeID_1, SP_1; nodeID_2, SP_2; \cdots; nodeID_n, SP_n\}$$

其中，SP_i 是选择该信誉代理作为自己可信代理节点的签名公钥。信任值分布式处理包括信任值请求、信任值应答和评价结果处理 3 个子过程：

(1)当节点 P 需要从它的可信代理 E 获得某特定节点的信任值时，首先查询本地可信代理列表，获得通向 E 的一条洋葱路由，经由这条洋葱路由向 E 发出信任值请求消息，其格式如下：$\{SP_E(R), SP_p, Onion_{(E,P)}\}$，其中，$R$ 是信任值请求消息，其格式为：$\{request, nounce\}$，$request$ 是请求内容，包含要请求的节点身份信息等关键信息。此处要使用 SP_E 进行加密，以防泄露。

(2)当 E 收到来自 P 的信任值请求消息后，通过约定的哈希函数对 SP_p 哈希可得其身份信息 $nodeID$。若 P 的 $nodeID$ 不在本地节点列表中，表明 P 是一个新节点，就将 P 的 $nodeID$ 和 SP_p 加入本地的节点签名公钥列表中。然后 E 用 SR_E 对消息解密，获知请求消息的具体内容，参照该消息从本地的信任值数据库中提取出特定节点的信任值及相关信息 T，最后将 T 封装后发回一条应答消息给 P，其格式为：$\{SP_p(T),\ SP_E,\ Onion_{(P,E)}\}$，其中，$T$ 是信任值应带消息，格式为：$\{trust\ value,\ nounce\}$，$trust\ value$ 是应答的节点信任值，其他说明与请求消息相同。

(3)服务结束后，P 要将本次服务的评价结果通过应答消息中节点 E 确定的洋葱路由 $Onion_{(P,E)}$ 报告给 E，以更新 E 保存的节点信任值。评价结果报告消息的格式如下：$\{SR_p(result, nounce),\ nodeID_p\}$，其中使用 SR_p 进行签名以保证其真实性。

收到报告后，E 参照消息中的 $nodeID_p$ 可以在本地节点签名公钥列表中查知解密用的 SP_p，并解密获得本次服务评价结果报告。

每次信誉代理收到来自资源请求者的评价结果报告后，将根据这个反馈报告对本地存储的节点信誉度进行更新。节点 m 的信誉度计算模型为

$$T(m) = \frac{\sum_{i}^{NT(m)} E(m,i)\times W(p(m,i))}{NT(m)} \tag{2}$$

其中，$NT(m)$ 为节点 m 的总服务次数；$T(m)$ 代表节点 m 的当前信誉度；$E(m,i)$ 代表与节点 m 进行第 i 次服务后的服务结果反馈值，可为(-1,0,+1)，分别代表不满意、一般和满意；$p(m,i)$ 为与节点 m 进行第 i 次服务的服务参与方，也是给出

反馈值的节点；$W(p(m,i))$ 是节点 $p(m,i)$ 的反馈值权重，即反馈的可信度。

3 安全性能分析

3.1 夸大或诋毁

(1)恶意节点试图影响其他节点选择信誉良好的可信代理。

当恶意节点试图给高性能信誉代理多倍的恶意推荐时，由于每个节点对某信誉代理的排位评估是根据该信誉代理所有权重中最高的权重值，而节点总能收到正确的权重值评价，因此来自攻击者的恶意推荐权重会自动忽略。当恶意节点试图给低性能信誉代理多倍的赞誉推荐时，由于多倍的赞誉推荐仍然相当于单一的高评价，因此不会影响其权重值。

(2)敌手试图通过影响信誉评估的过程影响其他节点的信誉值更新[4]。

通过签名可以保证发给信誉代理的评价结果报告的真实性，在处理这些真实评价结果后，信誉代理使用式(2)更新本地的节点信任值数据库。因为可信信誉代理总能收到大量的信息来进行信任计算，所以最终信任值的可靠性和准确性会很高。

3.2 冒名

冒名是指敌手通过使用其他节点的身份信息，伪装成其他节点[4]。因为所有的信任值和评价结果都经由发送者的签名密钥进行了签名，并且与发送者唯一的身份信息联系在一起，理论上敌手不可能获得其他节点的密钥对而伪装成其他节点。

3.3 DoS 攻击

DoS 攻击可能使高性能的信誉代理节点服务不可用，为了达到该目的，敌手先要区分出高性能的信誉代理。由于通信信息总是在随机选择的洋葱路由中继和大量的信誉代理之间传播，因此很难分析这种情况下的通信信息流，更难以分析其中的信任值请求包或应答包，从而几乎不可能确定高性能信誉代理。

4 计算机仿真

对该模型进行仿真，代码使用 VC++编写。因为在单机仿真环境中，节点间的洋葱路由很难也没必要实现，所以本文认为在所采用的密码体制是安全的前提下，节点之间路由是安全和匿名的。

4.1 仿真环境说明

(1)设想的仿真应用场景为文件共享应用，假设网络中一共有以下几类节点：

1)Good Peers：这类节点行为良好，无论是提供的服务还是对其他节点的评价都是真实的。称这类节点为 G 类。

2)Bad Peers：这类节点行为恶意，称这类节点为 B 类。为了更好地检测模型的安全性能，该类节点分为以下 3 个子类：①单纯的恶意节点，这类节点只提供不真实的服务，称这类节点为 BE 类。②试图影响其他节点选择信誉良好的可信代理节点，称这类节点为 BK 类。③试图通过影响信誉评估来影响其他节点信誉值的节点，称这类节点为 BS 类。

(2)网络由 1 000 个节点构成。每个节点同时作为服务节点和下载请求节点，每个节点发出 100 次下载请求。网络中发生的下载请求共有 100 000 次。每个节点保留一个可信信誉代理列表，其数目为 10，每个节点都可能被别的节点选为信誉代理节点。网络中共有 10 000 个文件供下载，这些文件被随机分配到所有 1 000 个节点，并保证每个文件至少被一个 G 类节点拥有。

(3)用户的目标是下载其所需的文件，假定下载请求节点能找到所需文件及其所在节点。下载请求节点根据其信誉代理节点提供的信任值最大服务节点进行下载。下载文件的真实性是判断本次交易成功与否的唯一标准。在网络中全部是 G 类节点的理想情况下，交易成功次数为下载请求总次数，即 100 000 次。

(4)节点的初始 *Trust* 值取为 0，每次服务完成后，其 *Trust* 将根据式(2)进行计算修正。每个信誉代理节点权重初始值为 0，同时本次服务的信誉代理节点权重值也将按式(1)进行修正。任何节点每交易 100 次后，更新自己的信誉代理节点。

(5)通过多个仿真实验检测模型的性能，在实验 1 中，G 类节点在网络中所占的比例为 60%，BE 类节点所占的比例为 40%，在初始状态下，2 类节点在信誉代理团中的比重也按相同的比例。该实验主要考察随着交易次数的增加，2 类节点在信誉代理团中比重和平均信任值的变化情况。实验 2 主要考察随着 B 类节点在网络中所占比例的不同，整个网络交易成功次数的变化；由于 B 类节点有 3 个子类，因此该实验要做 3 次。

4.2 仿真结果与分析

实验 1 的仿真结果如表 1 所示。实验 2 的仿真结果如表 2 所示。

表 1 实验 1 的仿真结果

交易次数	在信誉代理团中的比例/(%)		平均信任值	
	G 类节点	B 类节点	G 类节点	B 类节点
0	60.0	40.0	0.00	0.00
10^2	64.8	35.2	0.18	-0.12
10^3	70.9	29.1	0.32	-0.23
10^4	78.5	21.5	0.56	-0.41
5×10^4	87.9	12.1	0.75	-0.58
10^5	92.4	7.6	0.87	-0.69

表 2 实验 2 的仿真结果

B 类节点所占比例/(%)	成功次数与理想情况比值		
	BE 类	BK 类	BS 类
5	0.978	0.993	0.982
10	0.954	0.975	0.961
15	0.932	0.948	0.939
20	0.896	0.926	0.902
25	0.859	0.885	0.867
30	0.792	0.847	0.805
35	0.776	0.820	0.787
40	0.754	0.804	0.768

结果分析如下：

(1)在实验 1 中，随着交易次数的增加，信誉代理中 G 类节点的比重急剧增加，BE 类节点的比重快速减小。同时，G 类节点的平均信任值急剧增大，BE 类节点的平均信任值快速减小。

(2)在实验 2 中，如果没有信誉模型对网络进行管理，随着 3 种 B 类节点在网络中所占比例的增大，整个网络的成功交易次数应该同比例地减少。仿真实验结果表明在该模型的监管下，整个网络成功交易次数的减少平缓得多。

由此可见，本模型能够有效保护信誉良好的节点和抑制恶意节点，对夸大和诋毁等安全攻击有一定的抵制功能。

5 结束语

本文针对已有模型的若干局限性，构造了一种基于分层信誉代理的 P2P 网络信誉管理模型。通过分析和仿真证明本模型在多个性能指标上具有较大的提高。未来研究的工作包括如何建立一套完整的激励机制和惩罚机制等。

(下转第 147 页)