第33卷 第18期 计 算 机 工 程 2007年9月
Vol.33 No.18 Computer Engineering September 2007
·博士论文· 文章编号：1000—3428(2007)18—0020—02 文献标识码：A 中图分类号：TP393

P2P系统中的一种信任关系管理协议

林怀清[1,2]，李之棠[1]，黄庆凤[1]
(1. 华中科技大学计算机学院，武汉 430074；2. 海军工程大学电子工程学院，武汉 430033)

摘 要：信任关系管理是Peer-to-Peer信任模型的重要部分，在分布式环境中，如何安全存放和访问信任值是一个难以解决的问题。本协议采用可验证的、无可信中心的(k, n)门限密码系统产生系统的公/私密钥，征集k个管理者为系统中的用户生成证书，管理协议为用户提供信任值的匿名存储和访问服务。分析显示协议能极好地抵御各种攻击。

关键词：信任管理；对等网络；门限密码系统；匿名性

Management Protocol of Trust Relationships in P2P System

LIN Huai-qing[1,2], LI Zhi-tang[1], HUANG Qing-feng[1]
(1. College of Computer, Huazhong University of Science & Technology, Wuhan 430074;
2. College of Electronic Engineering, Naval University of Engineering, Wuhan 430033)

【Abstract】Managing trust relationships are important part of trust model. An important challenge in managing such trust relationships is to design a protocol to secure the placement and access of these trust ratings. In this protocol, a verifiable threshold cryptosystem without a trusted center is applied to generate system public/private keys. K managers can generate certification for peer. The protocol provides an anonymous server for peer. The security analysis shows that the protocol has desirable features of anonymity, reliability, accountability and is secure in the presence of a variety of possible attacks.

【Key words】trust management; Peer-to-Peer; threshold cryptosystem; anonymity

自Peer-to-Peer网络出现后，它受到越来越多的关注。它将现在主流的Internet服务模式——客户/服务，回归到end-to-end的原则当中。P2P并不严格地区分服务提供者和消费者，参与的实体(Peer)之间都是平等的，每一个实体既可提供服务也可使用服务，P2P计算体系结构目前已广泛应用于对等协作、资源共享、知识管理等领域。

但是，P2P的开放特性也给系统的安全性带来影响，阻碍了P2P网络的进一步发展。其中存在大量欺诈行为和不可靠的服务质量等问题。一种可行方案是采用信任模型对各用户进行等级评定，进行交易时优先选择信任等级高的用户。文献[1]提出的信任管理体系结构分为3部分：信任管理，数据管理，传输管理。而现有的研究大多集中在信任管理和数据管理，对信任的安全传输的文献并不多。文献[2]提出的TrustMe协议是基于公钥密码体系的信任关系管理协议，它通过引导程序生成系统的公/私密钥，为所有的用户生成公/私密钥，并为用户选择信任值的存放点，该协议的所有安全基础都依赖引导程序，这极可能成为网络性能的瓶颈和安全隐患。本文通过采用可验证的部分认证系统，提出一种信任关系管理方案。

1 密钥生成协议

如何在分布式环境中安全有效地分发公/私密钥是本协议首要考虑的问题。Shamir利用有限域中的多项式方程$f(x)$来构造秘密共享的(k,n)门限方案[3]。如果$f(x)$的最高次数为k-1，则在n个参与者中，征集k个成员即可利用Lagrange插值恢复共享的秘密。在该方案中需要一个可信的秘密分发者，这是笔者所不希望的，Pedersen在文献[4]中提出一种无需可信秘密分发者的可验证秘密分享方案。为便于描述，定义以下符号：p、q是大素数，E是椭圆曲线，G是椭圆曲线的基点。这里p，q，E和G是公开的，Z_q是有限域，$H_i(i=1,2,\ldots,n)$是n个参与秘密分享的用户，k是门限方案的阈值，d是要分享的秘密。Pedersen的可验证秘密分享协议如下。

分发协议：

Step 1 每个H_i随机选择一个d_i，并将d_iG广播给所有的参与者。

Step 2 每个H_i按以下方法分发d_i：H_i随机选择一个Z_q上的k-1次多项式：

$$f_i(x) = f_{i,0} + f_{i,1}x + f_{i,2}x^2 + \ldots + f_{i,k-1}x^{k-1} \quad (1)$$

令$f_{i,0}=d_i$，即$f_i(0) = d_i$，然后将$f_i(j)$安全地传送给H_j，并将$f_{i,j}G$广播到所有的n个参与者。

Step 3 每个H_i执行验证协议。

Step 4 若所有的H_i都通过验证，则执行Step 5，否则停止协议。

Step 5 每个H_i计算

$$t_i = \sum_{j=1}^{n} f_j(i) \quad (2)$$

并保密。

Step 6 每个H_i计算

$$Q = \sum_{i=1}^{n} d_iG\ ,\quad Q_i = t_iG \quad (3)$$

基金项目：国家自然科学基金资助项目“P2P网络的关键安全问题研究”(160573120)
作者简介：林怀清(1973－)，男，讲师、博士研究生，主研方向：P2P网络安全，计算机网络及安全；李之棠，教授、博士、博士生导师；黄庆凤，讲师、博士研究生
收稿日期：2006-09-25 **E-mail：**lhqzyh@hust.edu.cn

并广播这些值。

在该协议中，要为每个用户产生一个证书，用以表明其合法身份。系统的密钥是 $d=\sum_{i=1}^{n} d_i$，每个H_i保存一个影子：

$$s_i=t_i \bmod n \tag{4}$$

则通过 Lagrange 插值，k 个参与者可求出 d：

$$d=\sum_{i=1}^{k} s_i \cdot l_{vi}(0) \bmod n \tag{5}$$

这里，$l_{vi}(x)$是Lagrange系数，$v_i(i=1,2,\ldots,k)$为k个参与者的节点标识，由于

$$l_{vi}(x)=\prod_{\substack{j\neq i\\ j=1}}^{k}\frac{x-v_j}{v_i-v_j} \tag{6}$$

因此，$l_{vi}(0)=\prod_{\substack{j\neq i\\ j=1}}^{k}\frac{v_j}{v_j-v_i}$，令 $SK_i=s_i\cdot l_{vi}(0)$，则有 $d=\sum_{i=1}^{k} SK_i \bmod n$。K个参与者中的每一个可以通过持有的秘密分享$s_i$计算其相应的部分签名的密钥$SK_i$，对某个信息$X$的部分签名为 X^{SK_i}，当用户持有k个部分签名时，即可通过计算获得系统的完整签名：

$$X^{SK_1}\cdot X^{SK_2}\ldots X^{SK_K}=X^{SK_1+SK_2+\ldots+SK_K}=X^{d} \tag{7}$$

这时即可通过系统的公钥 Q 对其进行解密运算获得 X。在发放证书期间，系统私人密钥没有显式出现，无需可信密钥分发者，提高了安全性。

2 管理协议

管理协议中使用的符号定义如下：

THA peers(trust-holding agent peers)代表信任值存储节点；公开密钥算法中的公开密钥用B表示，私人密钥用P表示；SB、SP表示特殊公/私密钥，在信任查询时用于表明THA的合法性以及安全传输；TV(trust value)表示信任值；TS(time stamp)表示时间戳；ID表示节点标识；Cert_i表示系统为peer i发放的证书；K(M)表示用密钥K对消息M加密。

协议分以下几个部分：

2.1 系统初始化

此阶段用于系统的公/私密钥的产生。利用密钥产生协议，n 个系统管理者协作产生一组公/私密钥。

每个H_i执行密钥生成协议，计算系统的公开密钥 $Q=\sum_{i=1}^{n} d_iG$，系统的私人密钥由n个管理者分享s_i，k个管理者可恢复密钥以及签发证书。

2.2 用户登录

Peer i 向其中 k 个管理者申请加入，认证成功后，管理者完成以下任务：

(1)为 peer i 产生两对密钥 $\langle P_i,B_i\rangle$ 和 $\langle P_i',B_i'\rangle$，前一对密钥在 peer i 提供或接受服务时使用，后一对在 peer i 作为其他用户的 THA 时使用。

(2)管理者为用户随机选择一组用户作为peer i的THA，并产生一对特殊密钥 $\langle SP_i,SB_i\rangle$，之所以称其为特殊，是因为peer i并不知道SP_i，而只有peer i的THA才知道。这对特殊密钥的主要作用有两个：一是用于THA的身份验证，用SP_i加密的消息肯定是来自peer i的THA；二是用于信任安全传输，用SB_i加密的消息只有THA能打开。k个管理者分别对以下消息产生部分签名：

$X_j = s_j(ID_i \mid B_i \mid SP_i \mid SB_i)$　　$(j=1,2,\ldots,k)$

并将这些签名消息传送给 peer i 的所有 THA。这样，每个 THA 都可以计算完整的签名：

$$X=\prod_{j=1}^{k} X_j = d(ID_i \mid B_i \mid SP_i \mid SB_i) \tag{8}$$

并通过系统公开密钥 Q 得到

$(ID_i \mid B_i \mid SP_i \mid SB_i)$

(3)为 peer i 产生证书。k 个管理者(称其为 peer j)分别产生部分证书：

$Cert_{j,\,I} = s_j(B_i' \mid TS_{end})$

将这些部分证书传送给 peer i，则在 peer i 端可计算得到完整证书：

$$Cert_i=\prod_{j=1}^{k} Cert_{j,i}(B_i' \mid TS_{end}) = d(B_i' \mid TS_{end}) \tag{9}$$

peer i保存$Cert_i$。$Cert_i$用于向其他用户表明合法身份而不暴露他的ID，因此可在提供服务时保持匿名性。TS_{end}是证书的失效时间，证书在失效前，用户若还需要使用应向管理者申请延长。证书的失效有两种情况，失效时间到时自动失效；另一种是密码丢失时，系统将证书加入到失效证书队列。

2.3 信任值查询

任何需要查询信任值的 peer j 可广播查询消息，消息中包含需要查询的节点 ID，若需要查询多个 peer 的信任值时，可将它们的 ID 联接：

$Q(j, (i_1, i_2, \ldots, i_n)) = \text{"query"}|ID_{i1} \mid ID_{i2} \mid \ldots \mid ID_{in}$

2.4 查询应答

当 peer i 的 THA(称其为 peer j)收到对 peer i 的信任查询时，THA 产生应答消息并返回查询应答，消息格式如下：

$R(x, i) = ID_i \mid SB_i \mid SP_i(TV \mid TS \mid B_i \mid Cert_j \mid P_j'(TS))$

式中，用SP_i加密消息，确保消息来自peer i的THA；时间戳TS用于防止重放攻击；B_i用于稍后与peer i通信时使用；$Cert_j$确保应答节点是有效节点，同时$Cert_j$中的B_j'可确保在需要时定位该THA，例如，可通过$Cert_j$查找提供虚假信任值的THA，然后将其加入到黑名单；$P_j'(TS)$和$Cert_j$中的B_j'可防止其他peer使用$Cert_j$来伪装peer j。

2.5 收集交互证据

两个 peers，peer i 和 peer j 完成交互后，需对本次的交互进行评估，更新双方的信任值，为防止产生虚假评估，应同时提交交互证据，确保双方确实发生过交互。双方交换交互证据过程如图 1 所示。

图 1　交互证据的收集原理

其他peer无法产生这些消息，因为它们不知道这两个peers的私人密钥；TS用于防止重放攻击；B_j和ID_j用于防止交互证据的冒用，例如，如果没有B_j和ID_j，peer j可用交互证据$P_i(TS)$冒充peer i与其他peer交互。

2.6 提交评估报告

两个 peers，peer i 和 peer j 完成交互后，双方对本次的交互进行评估，peer j 对 peer i 的评估报告格式如下：

$ID_i \mid SB_i(\text{"Report"} \mid V \mid B_j \mid P_j(P_i(TS \mid B_j \mid ID_j)))$

式中，SB_i确保只有peer i的THA才能读到消息；V是评估值；交互证据被加密是为了防止产生假报告，外面的B_j和被加密的B_j可确保报告来自peer j。

(下转第 25 页)