

P2P 下基于 RSA 密码机制和门限秘密共享的信誉管理方案

孙 华, 于 炯, 廖 彬, 杨兴耀

(新疆大学 软件学院, 新疆 乌鲁木齐 830008)

摘 要: 在 P2P 网络环境下, 利用 RSA 密码机制和门限秘密共享进行信誉管理是一个非常有效的方案. 利用秘密共享原理将信誉信息分成 n 个秘密份额, 其中的任意 $t(t < n)$ 个合法的秘密共享参与者均可以重新构造信誉信息. 为了有效地防止网络中的恶意实体进行欺诈, 方案中还配备了与每个秘密份额相对应的验证份额分发给相应的参与实体, 任何非法参与实体冒称拥有秘密份额或者参与实体提供虚假的秘密份额, 只有攻破了 RSA 密码才能不被识别出来, 因此方案是安全有效的.

关键词: P2P; 信誉; RSA; 门限秘密共享

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2013)09-0098-04

A Scheme of Reputation Management Base on RSA and Threshold Secret Sharing in P2P Networks

SUN Hua, YU Jiong, LIAO Bin, YANG Xin-yao

(School of Software, Xinjiang University, Urumqi 830008, China)

Abstract: A scheme based on RSA and threshold secret sharing is proposed, and it can manage reputation information in P2P networks. This scheme uses theory of threshold secret sharing to protect reputation information, and information will be divided into n secret shadows and distributed to different participants, who act as rightful ones. Reputation information which was divided can be reconstructed by any of t or more participants, but any fewer participants can't do this according to the theory. In order to protect reputation information, a validation shadow will also be sent with secret shadow to the participant. Any participant will be recognized at once if he is unlawful participant or offers false secret shadow, unless he can break through RSA cryptography, so this scheme can be proved secure enough.

Key words: Peer-to-Peer; reputation; RSA; threshold secret sharing

1 引言

随着各种复杂的应用在 P2P 网络中发展, P2P 网络的优越性越来越突出. 但是, P2P 网络的匿名、动态特性也使它成为恶意实体攻击的目标, 在面对 P2P 网络中各种各样的欺诈行为时, 网络中各实体的信任和信誉^[1]已经被引入到网络中作为可信程度的一种有效的评判依据. 尤其是在分布式的网络环境中, 当相互陌生的实体之间需要发生交互前, 双方可以查看对方的信誉来评判对方的可信程度. 信誉

是其它的实体对目标实体的可信程度作出的评价. 通过对评价信息进行综合分析可以得出目标实体是否可信, 从而决定是否与之进行交互. 因此, 评价信息对信誉的有效评判起到至关重要的作用.

秘密共享是信息安全的一个重要研究分支, 自 1979 年门限秘密共享方案被提出以来, 已经取得了很多研究成果^[2, 3]. 本文中所使用的 (t, n) 门限秘密共享方案是指, 将一个秘密信息分割成 n 份, 并将他们分别发送给 n 个参与实体, 任意 $t(t < n)$ 个秘密份额可以重新构造出秘密信息. 基于秘密共享的研究

收稿日期: 2012-11-20; **修回日期:** 2012-12-22

基金项目: 国家自然科学基金项目(61063042, 61262088); 新疆大学博士启动基金项目(BS120134)

工作已经在很多方面展开了研究,包括多重秘密共享^[4]和基于 RSA 密码体制的秘密共享^[5]等。

基于 RSA 的门限秘密共享方案具备抵抗欺诈行为的能力,而且对于合法的参与者或者非法的参与者提供虚假的信息时,系统能够进行有效的识别并进行验证。秘密信息的分发者是与目标实体交互后产生的评价信息,然后将这些评价信息分割成若干个份额后再分别发送给其它的参与实体。当某个实体需要查询目标实体的信誉时,只需要由 t 个拥有秘密份额的参与者就可以重构评价信息。为了防止恶意实体的欺诈行为,评价者在分发秘密份额时还会分发相应的验证份额,任何参与者提供的虚假份额都可以通过验证份额验证后被发现,除非可以攻破 RSA 密码体制。因此,本文所提出的方案可以保证信息的完整性。

2 相关研究工作

基于 Girault 密钥交换协议结合基于身份(ID)的公钥密码技术^[6],提出了秘密共享方案用于解决目前的秘密份额分发过程中的安全问题。因为方案中是把用户的私钥当作秘密份额,由于私钥的机密性不能进行分发,但是任何实体都可以在验证过程中利用参与实体的公钥实施验证,甚至是在离线的环境下也可以进行。

面向服务的计算^[7]也可以采用秘密共享方案,根据各个服务的性能、历史的状态、消费者的反馈意见以及服务者的信誉等进行服务的选择,然后再完成相应的任务,信息是通过扩展 UDDI 标准并以及秘密共享来实现安全性的,并采取 Hash 函数的方法验证信息,验证结束后对哈希值进行删除,因此,只能验证一次。

TrustMe^[8]是由 Aameek Singh 等提出来的信息的匿名管理系统。方案中设计了一个匿名的信任管理协议,匿名的处理主要是针对查询信誉的实现和响应实体。由系统引导服务器指定每个实体的信息的保存地址,而且被指定的地址可能在若干个实体中,在指定的实体与被指定的实体之间也需要实行匿名管理,以防止信息被恶意篡改、破坏以及可能的攻击。引导服务器在系统中处于完全信任的地位,这在 P2P 等完全分布式的网络环境中很难实现。文献^[9]中,采用无须加密的信誉共享协议保证评价信息的完整性,而且可以有效阻止中间人攻击。

在具有超级节点的网络下,信任管理结构可以采用文献^[10]的方式。一些族处于超级节点网络中,

而每个族中又包含一个超级节点、一些普通节点以及一个存储节点,其中存储节点的主要任务是存储其它各节点的评价信息。

3 基于 RSA 密码机制的门限秘密共享方案

3.1 基于 RSA 密码机制的门限秘密共享

利用 RSA 密码机制和 (t, n) 门限秘密共享机制,实现密码信息的共享需要做如下处理。对外公开的信息包括:

(1) 一个大素数,假设为 r , 其中, $r > n$;

(2) β , 作为有限域 $GF(r)$ 的本原元素;

保密信息为 m , 是两个互异的大素数的乘积, 即 $m = pq$ 。

3.2 产生秘密份额和验证份额

设秘密共享的 n 个参与者分别为 $P_1, P_2, \dots, P_n$, 秘密信息为 $k \in GF(r)$, 则秘密信息被分割成若干个秘密份额的算法如下:

(1) 由秘密的拥有者秘密选择一个多项式 $f(x)$, 并且 $f(x) = b_{t-1}x^{t-1} + b_{t-2}x^{t-2} + \dots + b_1x + k \pmod{r}$, 其中多项式中的各个系数 $b_{t-1}, b_{t-2}, \dots, b_1$ 以及 $f(x)$ 均属于 $GF(r)$;

(2) 任意选择两个整数 e_1 和 e_2 , 并对外公开, 其中 e_1 和 e_2 与欧拉函数 $\varphi(m)$ 互素;

(3) 计算 $d_1 = e_1^{-1} \pmod{\varphi(m)}$, $d_2 = e_2^{-1} \pmod{\varphi(m)}$;

(4) 给每一个秘密参与者分发秘密份额 S_i (其中 $i = 1, 2, \dots, n$) 和验证份额 W_i (其中 $i = 1, 2, \dots, n$), 其中 $S_i = f(\beta^i)$, $W_i = S_i^{e_2 d_1} \pmod{m}$ 。

3.3 秘密信息的重新构造

秘密信息被分割以后分别被分发给 n 个参考实体, 当需要重构秘密信息时, 只需从中任意选择 t 个即可。假设 $P_1, P_2, \dots, P_t$ 分别是 t 个参与实体, 利用 t 个秘密份额得到 t 个插值点, 分别为: $(b_1, S_1), (b_2, S_2), \dots, (b_t, S_t)$, 使用 Lagrange 插值法可以重新构造一个满足 $S_i = f(\beta^i)$ 的 $t-1$ 次多项式, 计算可以得出 $k = f(0)$, 即:

$$k = \sum_{i=1}^t S_i \prod_{j=1, j \neq i}^t \frac{-\beta^j}{\beta^i - \beta^j} \pmod{r}$$

3.4 防欺诈验证

方案的验证过程如图 1 所示。对于参与秘密共享的任意一个实体 P_i ($1 \leq i \leq n$), 假设 S_i 和 W_i 分别是它拥有的秘密份额和验证份额, 其它的实体可以通过验证等式 $W_i \stackrel{?}{=} S_i^{e_2} \pmod{m}$ 是否成立。

如果 P_i 提供虚假信息, 为了不被发现, 他必须

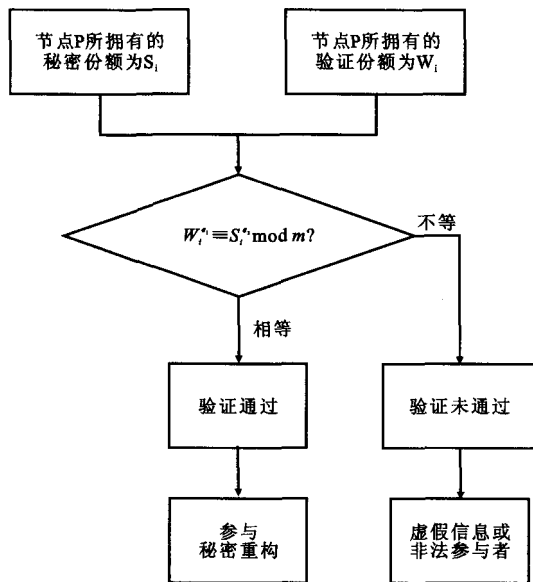


图1 秘密份额的验证过程

破解 RSA 加解密算法才能实现。假设 S_i^* 和 W_i^* 分别是它所提供的秘密份额以及与之相对应的验证份额,为了通过验证,等式 $W_i^* \equiv S_i^* \bmod m$ 必须成立,因为只拥有 e_1 ,在 d_1 未知的情况下,为了使等式 $e_1 d_1 \equiv 1 \bmod \varphi(m)$ 成立,相当于攻破 RSA 密码体制,由于计算能力上的不可行性,因此欺诈行为不被识破的前提条件不成立。

4 基于 RSA 机制的门限秘密共享方案的信誉管理方案

为了实现秘密信息的重构目标,需要 t 个以上的参与者。当网络中的两个实体需要进行交互时,假设分别为实体 Q 和实体 O,当实体 Q 查询实体 O 的信誉信息,实体 Q 首先发送查询信誉的请求信息,若能收到 t 个以上的实体反馈回来的秘密份额以及验证份额,实体 Q 通过验证来确定收到的秘密份额是否有效,然后再根据所获得的各个秘密份额重新构造秘密信息;否则存在欺诈行为。实体 O 需要用同样的方式查询实体 Q 的信誉信息。具体过程如图 2 所示。

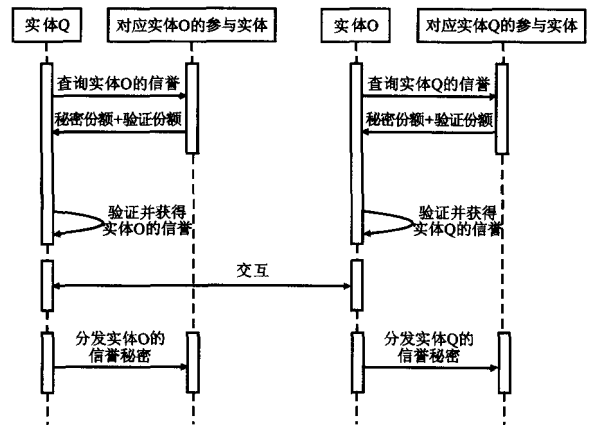


图2 信誉管理过程

5 方案的性能分析和对比

5.1 方案性能分析

(1)本方案可以防止信息被篡改

本文所提出的方案是根据 RSA 密码机制和 Shamir 的秘密共享体制实现的,任何少于 t 个参与者不能恢复秘密信息,而且任何一个实体提供虚假的被篡改的信息不能恢复秘密信息,而且这些是可以通过验证被发现的,因此秘密信息是安全的。

(2)本方案可以保证信息的完整性

在 P2P 网络环境下,系统中不存在完全可以信赖的实体。在本文的方案中,根据 RSA 密码体制和门限秘密共享体制,可以保证信息的完整性,而且并不要求所有的参与实体在线提供秘密份额,只要能够达到门限即可。

(3)本方案能够防止实体的欺诈行为

如果网络中的恶意实体冒称拥有秘密份额参与秘密重构,或者合法的参与者使用虚假的信息冒称真实的秘密份额,可以通过相应的验证份额对秘密份额进行验证。因为任何欺诈行为不被识别的前提是可以攻破 RSA 密码体制。

(4)参与者可以同时拥有多个秘密份额

网络中的实体可以同时作为多个秘密份额的拥有者,当秘密信息重构时,用对应的秘密份额再重

表1 各方案对比

	中心服务器	通信	安全方面	防内部欺诈	完整性验证方法	验证内容	验证次数
文献[7]	需要(UDDI)	大	存储安全	是	哈希函数	整体评价信息完整性	只能一次
文献[9]	不需要	小	递安全	否	信誉共享协议	整体评价信息完整性	只需要一次
本文方案	不需要	小	存储、传递安全	是	门限秘密共享	各秘密份额的完整性	不限次

新构造不同的秘密信息时,并不会影响整个系统的安全性。网络中的各个实体可以共享多个秘密,这对于整个系统而言,系统的安全性不会受到影响。

5.2 对比

将本文的方案与以前的研究方案分别从以下几个方面做对比,结果如表1所示。

6 结束语

文中方案利用 RSA 密码体制和门限秘密共享机制实现信誉的管理时,只要大于门限个数的实体就可以重构密码信息;而且任何一个实体存在欺诈行为,妄图利用虚假的秘密份额阻止信誉信息的生成都是可以通过验证被发现,因此,可以有效地对信誉信息进行管理。

参考文献:

- [1] Li, Huaizhi, Mukesh Singhal. Trust management in distributed systems [J]. Computer, 2007, 40(2): 45-53.
- [2] Tan K J, Zhu H W, Gu S J. Cheater identification in (t, n) threshold scheme [J]. Computer Communications, 1999, 22(8): 762-765.
- [3] Tassa T. Hierarchical threshold secret sharing [J]. Journal of Cryptology, 2007, 20(2): 237-264.
- [4] Dehkordi M H, Mashhadi S. New efficient and practical verifiable multi-secret sharing schemes [J]. Information Sciences, 2008, 178(9): 2262-2274.
- [5] 费如纯,王丽娜. 基于 RSA 和单向函数防欺诈的秘密共享体制[J]. 软件学报, 2003, 14(1): 146-150.
- [6] 裴庆祺,马建峰,庞辽军,等. 基于身份自证实的秘密共享方案[J]. 计算机学报, 2010, 33(1): 152-156.
- [7] Namin A S, et al. Applying secret sharing schemes to service reputation [C]//Proceedings of the Ninth International Conference on Computer Supported Cooperative Work in Design. Priory Street; Coventry Univ, 2005.
- [8] Singh Aameek, Ling Liu. TrustMe: anonymous management of trust relationships in decentralized P2P systems [C]// Third International Conference on Peer-to-Peer Computing (P2P'03). Los Alamitos,

California; IEEE, 2003: 142-149.

- [9] Ma Xin-Xin, Qin Zhi-Guang. Partition and multi-path transmission: an encryption-free reputation sharing protocol in gnutella-like peer-to-peer network [J]. Computer Communications, 2008, 31: 3059-3063.
- [10] Dimitriou Tassos, Ghassan Karame, Ioannis Christou. Supertrust-a secure and efficient framework for handling trust in super peer networks [C]// ICDCN. Berlin Heidelberg; Springer-Verlag, 2008: 350-362.

作者简介:

孙 华 女,(1977—),博士,讲师.研究方向为信息安全和信誉管理。



于 炯 男,(1964—),教授,博士生导师.研究方向为网络安全、网络与分布式计算。



廖 彬 男,(1986—),博士研究生.研究方向为网络与云计算、数据库与数据挖掘和绿色计算。



杨兴耀 男,(1984—),博士研究生.研究方向为推荐系统、网络和可信计算。

