

无可信 PKG 的基于身份的指定接收者群签密方案*

王娟, 王晓峰, 王尚平, 林婷婷, 向新银

(西安理工大学 密码理论与网络安全研究室, 西安 710054)

摘要: 利用签密的思想, 对基于身份的群签名方案进行改进, 提出无可信 PKG(私钥生成中心)的基于身份的指定接收者群签密方案。在提出的方案中, 只有指定接收者可以从群签密密文恢复出被群签密消息的明文来验证群签密的有效性; 并可以通过指定接收者进一步公开相关信息, 转换为不泄露消息明文但可以被公开验证的群签名。该方案能够同时保证消息的机密性、可认证性和不可否认性。此外, 群公钥的大小和群签密的长度独立于群成员的个数。

关键词: 基于身份的密码体制; 私钥生成中心; 双线性对; 指定接收者; 群签密

中图分类号: TP309 文献标志码: A 文章编号: 1001-3695(2007)12-0158-04

ID-based designated recipient group signcryption scheme without trusted PKG

WANG Juan, WANG Xiao-feng, WANG Shang-ping, LIN Ting-ting, XIANG Xin-yin

(Laboratory of Cryptography & Network Security, Xi'an University of Technology, Xi'an 710054, China)

Abstract: Based on the idea of signcryption, an ID-based designated recipient group signcryption scheme without trusted PKG (private key generator) was proposed by improving an ID-based group signature scheme. In the proposed scheme, only the designated recipient could recover the group signcrypted plain message from the ciphertext to verify the validity of the group signcryption. The proposed scheme could be converted into a group signature scheme with public verifiability by using the relevant information published by the designated recipient, which did not disclose the plain message. Moreover, the confidentiality, authenticity and non-repudiation of message were guaranteed simultaneously. The size of the group public key and the length of the group signcryption were independent on the size of the group.

Key words: ID-based cryptosystems; PKG; bilinear pairings; designated recipient; group signcryption

0 引言

群签名的概念首先由 Chaum 等人^[1]在 1991 年提出。它允许每一个群成员代表群对消息匿名地签名。同时, 验证者可以使用群公钥验证签名是否是群的有效签名, 但不能确定该签名由哪个群成员所签, 也不能确定两个不同的群签名是否由同一个签名者所签。在以后发生纠纷时, 群主管可以打开该签名并揭露签名者的真实身份。群签名在电子货币、电子选举等领域得到了广泛的应用。

最初的群签名方案^[2]均建立在基于证书的公钥密码系统下。该系统需要有系统公认的证书认证权威, 参与者在用一个用户的公钥之前必须先验证其证书的有效性。因此, 系统需要大量的存储空间和计算开销去管理用户的公钥证书。近年来, 在基于身份的公钥密码系统下, 用户的公钥可以很容易地由能够标志用户身份的信息(如 e-mail 地址或 IP 地址等)计算得到, 因而它成为基于证书的公钥密码系统很好的替代品, 并在现实中具有广泛的应用。

基于身份的公钥密码体制首先由 Shamir^[3]在 1984 年提出, 直到 2001 年才由 Boneh 等人^[4]提出了一个实用的基于身

份的公钥密码系统; 之后又提出了一些基于身份的群签名方案^[5], 但是这些方案均存在一个致命的弱点, 即系统必须有一个公共可信任的私钥生成中心(PKG)。PKG 可以计算系统内任意用户的私钥, 所以可以伪造任何用户的“有效”签名, 而且验证者无法判断 PKG 是否有欺骗行为。由此可见, 无条件地信任 PKG 大大限制了基于身份的群签名方案的广泛应用。2003 年, Chen 等人^[6]提出了一个新的无可信 PKG 的基于身份的系统从而解决了上述问题。

在现实生活中, 有时存在这样的实际应用场景: 一组技术人员联合绘制了某种零件的加工图纸, 他们需要对图纸群签名并加密后发送给加工者, 只有加工者可以恢复出图纸的明文并验证群签名的有效性。必要时, 加工者可以在不泄露图纸秘密的情况下使公众均可以验证群签名的有效性。考虑到以上的现实需求, 以及现有的基于身份的群签名方案没有考虑对被群签名消息的机密性, 笔者将签密的概念应用其中。签密的概念首先由 Zheng^[7]在 1997 年提出, 其主要思想是把加密和签名的功能结合起来, 在一个逻辑步骤内同时完成加密和签名。结合签密和群签名, 2000 年由 Mu 等人^[8]提出了群签密的概念, 其主要思想是群 A 中的任何成员能够代表群 A 对消息群签

收稿日期: 2006-09-21; 修返日期: 2006-12-03 基金项目: 国家自然科学基金资助项目(60273089); 陕西省教育厅专项科学研究计划资助项目(06JK213); 陕西省自然科学基金基础研究计划资助项目(2005F02); 西安理工大学科技创新基金资助项目(108210402)

作者简介: 王娟(1982-), 女, 江苏高邮人, 硕士研究生, 主要研究方向为密码理论与网络安全(wangjuan718@hotmail.com); 王晓峰(1966-), 女, 副教授, 硕导, 主要研究方向为密码理论与网络安全; 王尚平(1963-), 男, 教授, 硕导, 主要研究方向为密码理论与网络安全; 林婷婷(1981-), 女, 硕士研究生, 主要研究方向为密码理论与网络安全; 向新银(1979-), 男, 硕士研究生, 主要研究方向为密码理论与网络安全。

密, 然后将该群签密发送给群 A 指定的接收群 B, 群 B 中的任何成员可以恢复消息并对群签名验证。

基于双线性对, 本文提出了一个无可信 PKG 的基于身份的指定接收者群签密方案。与上述群签密方案所不同的是, 本方案中群签密的指定接收者是一个指定的用户而不是一个指定的群。该方案除了满足群签名的要求外, 还具有以下特性: a) 基于身份的特性, 但系统中的 PKG 不必是可信的, 它可以解决密钥的托管问题。b) 群签密的特性, 能够将群签名和加密的功能结合起来, 一次性完成群签名和加密, 同时达到了消息的机密性和可认证性。c) 指定接收者恢复消息的特性, 即只能由指定接收者才可以恢复消息的明文以保持消息的机密性。在恢复出消息后, 必要时指定接收者可以公开消息的 hash 值等相关信息, 使得任何人可以验证群签密的有效性, 这样可以大大缩小消息的扩散范围, 为一些需要保密的消息(如个人隐私)提供了很好的解决途径。

1 预备知识

1.1 双线性对

令 G_1 是一个由 P 生成的循环加法群, 阶为素数 q , G_2 是一个阶为素数 q 的循环乘法群。令 $a, b \in \mathbb{Z}_q^*$, 假设群 G_1 和 G_2 中的离散对数问题是困难的。双线性对是一个映射 $e: G_1 \times G_1 \rightarrow G_2$, 具有下面的性质:

- 双线性。 $e(aP, bQ) = e(P, Q)^{ab}$, 其中 $P, Q \in G_1$ 。
- 非退化性。存在 $P, Q \in G_1$, 使得 $e(P, Q) = 1$ 。
- 可计算性。对于 $P, Q \in G_1$, 存在一个有效的算法可以计算 $e(P, Q)$ 。

1.2 Gap Diffie-Hellman 群

令 G_1 是一个循环加法群, 阶为素数 q , 生成元为 P 。假设在群 G_1 中的加法和求逆可以被有效地计算。首先描述三个数学问题:

- 离散对数问题(DLP)。给定两个群元素 P 和 Q , 寻找一个整数 $n \in \mathbb{Z}_q^*$, 使得 $Q = nP$ 。
- 判定性 Diffie-Hellman 问题(DDHP)。对于 $a, b, c \in \mathbb{Z}_q^*$, 给定 P, aP, bP, cP , 判定是否 $c = ab \pmod{q}$ 。如果上式成立, (P, aP, bP, cP) 称为一个有效的 Diffie-Hellman 四元组。
- 计算性 Diffie-Hellman 问题(CDHP)。对于 $a, b \in \mathbb{Z}_q^*$, 给定 P, aP, bP , 计算 abP 。

在群 G_1 中, 如果 DDHP 能在多项式时间内得到有效解决, 但是不存在多项式时间算法能以不可忽略的概率解决 CDHP, 这样的问题称为 Gap Diffie-Hellman 问题(GDHP), 称群 G_1 为 Gap Diffie-Hellman 群。这样的群可以在有限域上的超奇异椭圆曲线或超椭圆曲线中找到, 并且双线性对可以从 Weil 或 Tate 对推导得到^[4]。

2 无可信 PKG 的基于身份的指定接收者群签密方案

假定系统中存在一个由用户 u_1, u_2, \dots, u_n 组成的群, 其对应的身份为 ID_1, ID_2, \dots, ID_n 。设用户 $u_j(j=1, 2, \dots, n)$ 代表该群对消息群签密, 用户 B 是群签密的指定接收者, 他能够恢复出被群签密消息的明文。只有当该指定接收者恢复消息并公

开相关信息后, 其他人才可以公开地对群签密验证。该方案由以下六个部分组成: 系统的建立、密钥的提取、群成员的加入、群签密、消息恢复并验证、群签密的打开。在该系统中, 存在 PKG 但它不必是一个可信实体。为了简便, 在此只需考虑群主管是 PKG 的情况^[6]。

2.1 系统的建立

G_1, G_2 和 e 如 1.1 节所述。设 $H_1, H_2, H_3, H_4, H_5, H_6$ 为六个公开的抗碰撞的密码学单向 hash 函数, 定义为 $H_1: \{0, 1\}^* \times G_1 \rightarrow G_1, H_2: \{0, 1\}^* \times G_1 \rightarrow G_1, H_3: \{0, 1\}^n \times G_1 \rightarrow G_1, H_4: \{0, 1\}^* \times \{0, 1\}^n \rightarrow G_2, H_5: G_2 \times \{0, 1\}^* \rightarrow G_2, H_6: \{0, 1\}^* \times G_2 \rightarrow G_1$ 。PKG 选择随机数 $s \in \mathbb{Z}_q^*$ 作为主密钥, 计算 $P_{pub} = sP$ 作为 PKG 的公钥。公开一个能够代表上述群身份的值 $L = ID_1 \parallel ID_2 \parallel \dots \parallel ID_n$ 。系统的公开参数 $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3, H_4, H_5, H_6, L\}$ 。

2.2 密钥的提取

在提出的方案中, 任何一个用户 $u_i(i=1, 2, \dots, n)$ 在加入群之前均必须先向 PKG 申请用于其普通签名的私钥, 借鉴文献[6]的方法解决密钥托管问题。方法如下:

- 用户 u_i 首先选择随机数 $r_i \in \mathbb{Z}_q^*$ 作为其私钥, 计算 r_iP ; 然后将 (ID_i, r_i, P, T_i) 发送给 PKG。其中: ID_i 是用户 u_i 的身份信息; T_i 是 r_i 的使用期限。
- PKG 计算 $Q_{ID_i} = H_1(ID_i \parallel T_i, r_iP)$ 和 $S_{D_i} = sQ_{ID_i} = sH_1(ID_i \parallel T_i, r_iP)$, 把 S_{D_i} 通过安全信道发送给用户 u_i 。用户 u_i 的公钥是 Q_{ID_i} , 私钥是 (r_i, D_{ID_i}) 。在经过周期 T_i 后, 用户 u_i 应当更新其公私钥对。为了简单起见, 在此不讨论这个问题。

由于 PKG 不是可信的, PKG 有可能假冒用户 u_i 对消息签名。PKG 可以选择随机数 $r_i \in \mathbb{Z}_q^*$ 生成一个新的密钥 $S_{D_i} = sH_1(ID_i \parallel T_i, r_iP)$ 去伪造签名。如果伪造的签名能够通过验证, 用户 u_i 能够提供证据证明该签名是由 PKG 伪造的, 他可以向仲裁者提供一个知识证明来证明其知道 $S_{D_i} = sH_1(ID_i \parallel T_i, r_iP)$ 。方法如下:

- 用户 u_i 首先将 r_iP 发送给仲裁者, 然后仲裁者随机选择一个秘密的整数 $k \in \mathbb{Z}_q^*$ 并计算 kP , 将 kP 通过安全信道发送给用户 u_i 。
- 用户 u_i 计算 $e(S_{D_i}, kP)$, 仲裁者计算 $e(H_1(ID_i \parallel T_i, r_iP), P_{pub})^k$ 。如果等式 $e(S_{D_i}, kP) = e(H_1(ID_i \parallel T_i, r_iP), P_{pub})^k$ 成立, 说明用户 u_i 知道 S_{D_i} 并且他的 ID_i 在同一周期 T_i 内与 r_iP 和 r_iP 都对应, 此时仲裁者就推断出 PKG 是不诚实的, 因为主密钥 s 只有 PKG 知道。

2.3 群成员的加入

当已经提取了私钥的用户 $u_j(j=1, 2, \dots, n)$ 要加入群时, 他与群主管(即 PKG)执行以下协议:

- 用户 u_j 首先选择随机数 $x_j \in \mathbb{Z}_q^*$, 计算 x_jP 和 r_jx_jP , 然后将 $\{r_jx_jP, x_jP, S_{D_j}\}$ 发送给 PKG。
- 如果 $S_{D_j} = sH_1(ID_j \parallel T_j, r_jx_jP)$ 成立(即 PKG 确信用户 u_j 知道 S_{D_j}) 并且 $e(r_jx_jP, P) = e(x_jP, r_jP)$ 成立, 那么 PKG 向用户 u_j 秘密地发送 $S_{D_j} = sH_1(ID_j \parallel T_j, r_jx_jP)$, 表明用户 u_j 已经加入到群中。此时, 用户 u_j 的成员证书是 (S_{D_j}, r_jx_jP) , 用户 u_j 的秘密钥是 x_j 和 r_jx_j 。如果上述两式不成立, PKG 就拒绝用户 u_j 的加入。

c) 当用户 u_j 加入该群后, PKG 将 $\{r_j x_j P, x_j P, r_j P, ID_j, T_j\}$ 添加到成员列表并秘密保存。

2.4 群签密

在群成员 u_j 对消息群签密之前, 指定接收者 B 首先选择随机数 $r_B \in \mathbb{Z}_q^*$ 并计算 $R_B = r_B P$, 然后将 R_B 向该群广播, 用于群成员 u_j 对消息群签密。在此不讨论指定接收者 B 如何广播 R_B 给群。指定接收者 B 还要计算 $R_B = r_B H_2(ID_B)$ 并保密 R_B , 用于从群签密中恢复消息。其中 ID_B 是指定接收者 B 的身份信息。对于待群签密的消息 m , 群成员 $u_j (j=1, 2, \dots, n)$ 计算如下:

$$U_j = r_j x_j P + r_j x_j^2 P, \text{ 其中 } r_j, x_j \in \mathbb{Z}_q^*$$

$$V_j = a_j H_1(ID_j, T_j, r_j x_j P), \text{ 其中 } a_j \in \mathbb{Z}_q^*$$

$$W_j = r_j x_j H_1(ID_B, m, U_j)$$

$$h_j = H_3(H_4(m), U_j + V_j + W_j)$$

$$R_j = (r_j x_j + r_j x_j^2) h_j + a_j S_{ID_j}$$

$$Z_j = t_j P, \text{ 其中 } t_j \in \mathbb{Z}_q^*$$

$$X_j = e(H_2(ID_B), t_j R_B)$$

$$c_j = H_5(X_j) \oplus (m \parallel D)$$

$$c_j = H_6(L, X_j) \oplus W_j$$

$$c_j = H_6(L, X_j) \oplus R_j$$

消息 m 的群签密为 $(Z_j, U_j, V_j, c_j, c_j, c_j)$ 。最后, 群组将 $(Z_j, U_j, V_j, c_j, c_j, c_j)$ 发送给指定接收者 B。

2.5 消息恢复并验证

1) 消息恢复

指定接收者 B 收到群签密后, 按照下列步骤恢复消息:

a) 计算 $X_j = e(R_B, Z_j)$ 并计算 $H_5(X_j)$ 。因为 $X_j = e(H_2(ID_B), t_j R_B) = e(H_2(ID_B), t_j r_B P) = e(r_B H_2(ID_B), t_j P) = e(R_B, Z_j)$ 。

b) 计算 $c_j \oplus H_5(X_j) = m \parallel L$ 。因为已知 L , 由此可得 m 。

c) 计算 $H_4(m)$ 和 $H_6(L, X_j)$, 必要时可公开, 便于其他验证者公开验证群签密。

2) 公开验证

群签密的验证者在得到 $(Z_j, U_j, V_j, c_j, c_j, c_j)$ 、 $H_4(m)$ 和 $H_6(L, X_j)$ 后就可以验证群签密的有效性。方法如下:

a) 计算 $c_j \oplus H_6(L, X_j) = W_j$ 和 $c_j \oplus H_6(L, X_j) = R_j$ 。

b) 计算 $h_j = H_3(H_4(m), U_j + V_j + W_j)$ 。

c) 检验 $e(R_j, P) = e(h_j, U_j) \times e(V_j, P_{pub})$ 是否成立。若成立说明群签密 $(Z_j, U_j, V_j, c_j, c_j, c_j)$ 有效; 否则, 该群签密无效。

2.6 群签密的打开

给定一个有效的群签密, PKG 能够很容易地识别出群签密者的身份。由于 PKG 知道 $(r_j x_j P, x_j P, r_j P, ID_j, T_j)$, 他可以根据一个有效的群签密 $(Z_j, U_j, V_j, c_j, c_j, c_j)$ 来逐个验证 $e(U_j, P) = e(r_j x_j P, P) = e(r_j x_j P, x_j P)$, 使得等式成立的 U_j 对应的群成员 u_j 即为群签密者。

群签密者不能够否认他的群签密, 因为 PKG 能够提供以下证据证明该群签密确实属于该群签密者:

$$e(U_j, P) = e(r_j x_j P, P) = e(r_j x_j P, x_j P)$$

$$e(S_{ID_j}, P) = e(H_1(ID_j, T_j, r_j x_j P), P_{pub})$$

$$e(S_{ID_j}, P) = e(H_1(ID_j, T_j, r_j P), P_{pub})$$

同样, PKG 也不能把一个群签密陷害给该群签密者, 除非 PKG 能够解决计算性 Diffie-Hellman 问题的逆问题, 即给定 P 、

aP 、 rP , 计算满足 $a = rb \pmod q$ 的 bP 。该问题与 G_1 中的计算性 Diffie-Hellman 问题是等价的, 证明参见文献[6]。

对于群成员的删除问题可作如下考虑: 若群主管想要删除群成员 $u_j (j=1, 2, \dots, n)$, 他可通过群成员 u_j 的身份 ID_j 从成员列表中找到与其相关的这组值 $\{r_j x_j P, x_j P, r_j P, ID_j, T_j\}$, 然后将这组值从成员列表中删除并向外界公布这组值已被删除。

3 方案的安全性分析

3.1 满足群签名方案的安全性

基于计算性 Diffie-Hellman 问题是困难的假设下, 本文对该方案进行安全性分析, 该方案满足群签名方案的安全性。

a) 正确性。如果群签密 $(Z_j, U_j, V_j, c_j, c_j, c_j)$ 是群成员 u_j 所签, 那么通过使用指定接收者 B 在消息恢复时计算的值 $H_4(m)$ 和 $H_6(L, X_j)$ 就可以验证群签密 $(Z_j, U_j, V_j, c_j, c_j, c_j)$, 并且该群签密一定能够通过验证。因为 $e(R_j, P) = e((r_j x_j + r_j x_j^2) h_j + a_j S_{ID_j}, P) = e((r_j x_j + r_j x_j^2) h_j, P) \times e(a_j S_{ID_j}, P) = e(h_j, U_j) \times e(a_j H_1(ID_j, T_j, r_j x_j P), P) = e(h_j, U_j) \times e(V_j, P_{pub})$ 是成立的, 所以该群签密可以通过验证, 从而满足正确性。

b) 不可伪造性。在本方案中, 虽然 PKG 知道用户 u_j 的成员证书, 但是由于群成员在对消息 m 群签密时加入了自己的秘密钥 x_j 和 $r_j x_j$, 使得 PKG 要对群签密伪造是不可能的。因为从 $x_j P$ 求解 x_j 和从 $r_j x_j P$ 求解 $r_j x_j$ 是求解群 G_1 中的离散对数问题, 而求解该问题是困难的, 所以群签密不能够伪造。PKG 伪造群签密是困难的, 其他人要伪造群签密就更加困难, 因为 PKG 要比其他人能够得到更多群签密时所需用到的值。

c) 匿名性。给定一个有效的群签密, 除群主管外, 任何人确定群签密者的身份在计算上是困难的。因为群签密者在群签密时加入了随机数, 所以群主管以外的任何人从群签密的结果不能够得到关于任何群签密者的信息。给定一个有效的群签密, 只有群主管可以使用这组值 $\{r_j x_j P, x_j P, r_j P, ID_j, T_j\}$ 通过打开算法识别出群签密者的身份。

d) 不可链接性。对于两个不同的群签密 $(Z_j, U_j, V_j, c_j, c_j, c_j)$ 和 $(\hat{Z}_j, \hat{U}_j, \hat{V}_j, \hat{c}_j, \hat{c}_j, \hat{c}_j)$, 由于群签密者在群签密时选择了随机数, 所以每次的群签密均不同。同时 $(Z_j, U_j, V_j, c_j, c_j, c_j)$ 和 $(\hat{Z}_j, \hat{U}_j, \hat{V}_j, \hat{c}_j, \hat{c}_j, \hat{c}_j)$ 是完全独立的, 所以不可能从两个不同的群签密来确定是否是由同一个群签密者所签。

e) 可追踪性。群主管使用打开算法能够打开任何一个有效的群签密来确定群签密者的身份, 因为群主管能够提供零知识证明来说明群签密者确实生成了该群签密。

f) 开脱性。群成员和群主管均不能代表其他群成员群签密。即使群主管与一些群成员勾结起来也不能把一个有效的群签密陷害给某个群成员, 这是因为在同一使用期限 T_j 内, 一个身份 ID_j 只能对应一个 $r_j P$, 所以开脱性是满足的。

g) 抗联合攻击。对于群成员来说, 要想伪造一个群主管不能打开的有效群签密, 就要成功地伪造群成员证书。如果能够成功地伪造群成员证书, 就意味着能够解决 G_1 中的 CDHP, 但这是困难问题的, 所以群成员证书是不能够伪造的, 即群成员联合起来 (即使是整个群) 也不能生成一个群主管不能打开的有效群签密。

3.2 只有指定接收者才可以恢复消息

从消息恢复并验证的过程可以看出, 攻击者若想恢复消息

就必须知道指定接收者 B 的秘密值 R_B 。因为 $R_B = r_B H_2(\text{ID}_B)$, 所以要知道 R_B 就是要知道 r_B , 即从 $R_B = r_B H_2(\text{ID}_B)$ 中计算 r_B , 这是一个离散对数问题。因此, 攻击者无法恢复消息, 只有指定接收者 B 才可以恢复消息。

3.3 消息的秘密性

在指定接收者 B 恢复消息后, 他没有直接将恢复出来的消息给其他验证者, 只是给了他们消息 m 的 hash 值, 这样可以避免在其他验证者验证群签密时知道消息的明文。消息的明文只有群签密者和指定接收者 B 知道。如果指定接收者 B 改动了消息, 在其他验证者验证群签密的有效性时, 验证式 $e(R_j, P) = e(h_j, U_j) \times e(V_j, P_{\text{pub}})$ 无法成立。从其他验证者的角度看, 他们不能够判断出是本身要验证的群签密无效, 还是指定接收者 B 对消息篡改后使得验证式不成立。在此认定指定接收者 B 不会改动恢复出来的消息, 即他是可信的。

4 结束语

本文基于 GDH 问题, 提出了一个无可信 PKG 的基于身份的指定接收者群签密方案, 并对其安全性作了简要分析。在该方案中, 群签密者代表由 n 个成员组成的群对消息群签密, 所以适合群成员的个数是有限的群, 因此该方案更加具有实际意义。该方案的优点是将消息的机密性、可认证性和不可否认性结合起来, 同时在指定接收者恢复消息后, 其他验证者在验证时不能够看到消息的明文, 避免了消息的广泛公开; 缺点是由于同时需要满足的要求比较多, 导致多次使用 hash 函数, 使方案比较复杂。如何将该方案简化是笔者下一步将要研究的问题。

(上接第 157 页) 本文提出的推荐信任模型性能是令人满意的。

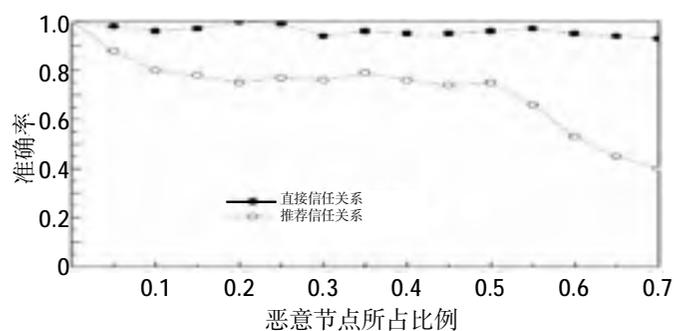


图 4 恶意节点对模型性能的影响

5 结束语

本文在总结现有典型推荐信任模型的基础上, 讨论了信任的含义和性质, 深入研究了推荐信任关系中推荐信任的传递与合成问题以及推荐信任网的形成过程, 提出了推荐信任的合成方法, 给出了总体信任值的评价公式。此外, 设置了 α 、 β 、 depthLimit 和 maxDepth 等参数, 使推荐机制更加灵活, 反映了不同实体进行信任评估时所具有的个性特点; 同时选择推荐深度较小且是独立的推荐信任路径使推荐具有更高的可信性。这些措施有效地防止了恶意推荐等问题, 使得推荐信任关系的合成更符合实际情况。最后建立仿真环境, 实验结果表明, 本文提出的推荐信任模型可以作为一种有效的工具, 为开放分布式环境中的主体信任决策提供有效支持。

参考文献:

[1] ASMUSSON L, JANSSON S. Simulated social control for secure In-

参考文献:

- [1] HAUM D, HEYST E V. Group signatures[C] // Proc of Advances in Cryptology-EUROCRYPT '91, LNCS 547. Berlin: Springer-Verlag, 1991: 257-265.
- [2] CAMENISCH J, STADLER M. Efficient group signatures schemes for large groups[C] // Proc of Advances in Cryptology-CRYPTO '97, LNCS 1294. Berlin: Springer-Verlag, 1997: 410-424.
- [3] SHAMIR A. Identity-based cryptosystems and signature schemes [C] // Proc of Advances in Cryptology-CRYPTO '84, LNCS 196. Berlin: Springer-Verlag, 1984: 47-53.
- [4] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairings[C] // Proc of Advances in Cryptology-CRYPTO 2001, LNCS 2139. Berlin: Springer-Verlag, 2001: 213-229.
- [5] TSENG Y, JAN J. A novel ID-based group signature[C] // Proc of International Computer Symposium, Workshop on Cryptology and Information Security. Tainan: [s. n.], 1998: 159-164.
- [6] CHEN Xiao-feng, ZHANG Fang-guo, LIM K. A new ID-based group signature scheme from bilinear pairings[EB/OL]. [2003]. http://eprint.iacr.org/2003/116.
- [7] ZHENG Yu-liang. Digital signcryption or how to achieve $\text{cost}(\text{signature} \& \text{encryption}) \ll \text{cost}(\text{signature}) + \text{cost}(\text{encryption})$ [C] // Proc of Advances in Cryptology-CRYPTO '97, LNCS 1294. Berlin: Springer-Verlag, 1997: 165-179.
- [8] MU Yi, VARADHARAJAN V. Distributed signcryption[C] // Proc of the 1st International Conference on Progress in Cryptology. London: Springer-Verlag, 2000: 155-164.
- [9] TAN Zuo-wen, LIU Zhuo-jun. A novel identity-based group signature scheme from bilinear maps[EB/OL]. [2003]. http://www.mmrc.iss.ac.cn/pub/mm22.pdf/17.pdf.
- [10] WATTS D J, STROGATZ S H. Collective dynamics of small-world networks[M]. London: Nature, 1998: 440-442.
- [1] ternet commerce[C] // Proc of the 1996 Workshop on New Security Paradigms. New York: ACM Press, 1996: 18-25.
- [2] BETH T, BORCHERDING M, KLEIN B. Valuation of trust in open networks[C] // GOLLMANN D. Proc of the 3rd European Symposium on Research in Computer Security. Brighton: Springer-Verlag, 1994: 3-18.
- [3] ABDUL-RAHMAN A, HAILES S. A distributed trust model[C] // Proc of the 1997 Workshop on New Security Paradigms. New York: ACM Press, 1998: 48-60.
- [4] J SANG A. A subjective metric of authentication [C] // QUISQUATER J. Proc of the 5th European Symposium on Research in Computer Security. London: Springer-Verlag, 1998: 329-444.
- [5] WANG Yao, VASSILEVA J. Bayesian network-based trust model [C] // Proc of the IEEE Computer Society / WIC International Conference on Web Intelligence. Washington D C: IEEE Computer Society, 2003: 372-378.
- [6] GUHA R, KUMAR R, RAGHAVAN P, et al. Propagation of trust and distrust[C] // Proc of the 13th International Conference on World Wide Web. New York: ACM Press, 2004: 17-22.
- [7] YU Bin, SINGH M P. An evidential model of distributed reputation management[C] // Proc of the 1st International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1. New York: ACM Press, 2002: 294-301.
- [8] YAN Sun, WEI Yu, ZHU Han, et al. Trust modeling and evaluation in Ad hoc networks[C] // Proc of Global Telecommunications Conference. Washington D C: IEEE Computer Society, 2005: 1862-1867.
- [9] 王莉苹, 杨寿保. 网格环境中的一种信任模型[J]. 计算机工程与应用, 2004, 40(23): 50-53.