一种基于身份的分布式会议密钥分发方案*)

杨宗凯[1,2] 谢海涛[1] 程文青[1] 谭运猛[1]

(华中科技大学电子与信息工程系 武汉 430074)[1] (华中师范大学 武汉 430071)[2]

摘 要 基于身份的密码体制和(t,n)门限共享,提出了一种分布式可容错的会议密钥分发方案,与传统的秘密共享方案不同的是,秘密分片由服务器的私钥产生,而不是由会议发起者产生并分配给这些服务器;通过收集这些秘密分片,构造多项式函数;任何被邀请参加会议的成员,都可向这些服务器申请秘密分片并恢复会议密钥。在会议密钥的分发和重构过程中,各个成员的身份可以方便地进行验证,避免了各类欺诈行为的发生。

关键词 基于身份的认证,秘密共享,会议密钥分发

An Identity-based Distributed Conference Key Distribution Scheme

YANG Zong-Kai[1,2] XIE Hai-Tao[1,2] CHENG Wen-Qing[1] TANG Yun-Meng[1]

(Department of Electronic and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074)[1]

(Huazhong Normal University, Wuhan 430071)[2]

Abstract A distributed fault-tolerant conference key distribution and restitution scheme based on mechanism of identity-based cryptography and (t,n)threshold secret sharing is proposed in this paper. The new scheme is much different to traditional scheme, its secret shadows are not brought from the sponsor of conference, but from each server's private key signature. By getting together these n secret shadows, the sponsor can construct polynomial. Any of conferees invited by the sponsor can request these secret shadows from t of these n servers, and then restitute conference key by them. In all courses of conference key distribution and restitution, every member's identity can be easily validated, so it can be prevented from all kinds of cheat.

Keywords ID-based cryptography, Secret sharing, Conference key distribution

1 引言

随着互联网技术的迅速发展,网络会议正成为 Internet 的最重要应用之一,由于网络的开放性和不确定性等特点,其安全性成为人们研究的焦点。通信安全的基本手段是加密体制,而加密体制中最关键的问题是密钥的分发和管理,因此,如何有效、安全地分配会议密钥是保证网络会议安全性的首要问题。总的来看,会议密钥分发的方式有两种:(1)集中式的会议密钥分配[1~3],由一个可信的密钥分配服务器为各会议用户生成并发送会议密钥。这种方式的特点是协议设计简单,信息交互量少,但一旦这个密钥分配服务器受到攻击或失效,则会危及到整个密钥系统;(2)协商式会议密钥分配[4~7],会议密钥由参加会议的各方共同协商产生,避免了前一种方式中单一失败点的问题,然而由于会议密钥需要所有成员完成交互才能产生,协议的设计一般相当复杂,且所需交互量很大。

到目前为止,大多数的会议密钥分发方案都不具有容错能力,因此不能抵抗来自系统内部的主动攻击。Tzeng[4]提出了一种容错的会议密钥协商方案,但该方案不能抵抗来自不同子网的不同密钥攻击;Xu[5]则提出了一种基于身份的容错的会议密钥协商方案,该方案利用会议桥来收集来自会议各方的密钥请求并协商出会议密钥,与 Tzeng 的方案相比,在通信开销和计算开销方面都有改善,但其会议桥会成为系统的单一失败点,给系统带来安全隐患。

近年来,基于身份的公钥密码体制开始引起密码研究者的关注,正在身份认证和密钥管理等方面得到了越来越广泛的应用,成为密码学的一个新方向。基于身份的公钥密码体制最先是由 Shamir[8]提出的,以后又有多种基于身份的加密方案和签名方案陆续出现。在这种体制下,每个人的公钥是由唯一标识其身份的相关信息而不是由随机选择的字符串所确定的。

本文提出了一种基于身份的分布式可容错的会议密钥分发方案:网络中的每个成员都拥有基于身份的公私密钥对;会议由发起者自行产生会议密钥,通过收集信任集中的 n 个成员的签名,由 Shamir 秘密共享方案[9]构造会议密钥的密钥分片;任何会议成员想加入会议,只需向这 n 个成员中的任意 t 个成员提出申请,通过计算这 t 个伪秘密分片,可以正确恢复出会话密钥,少于 t 个伪秘密分片,则不能恢复会话密钥。

2 基于身份的密码体制

实际应用中,可以利用超奇异椭圆曲线上修正的 Weil 对[10]构造有效的双线性映射,进而构造安全高效的基于身份的密码体制。

*)基金项目:国家自然科学基金资助项目(90104033)。杨宗凯 教授,博士生导师,研究方向为电子商务、远程教育和网络安全。谢海涛 博士研究生,研究方向为信息安全和无线网络;程文青 教授,研究方向为网络安全和下一代互联网;谭运猛 博士,副教授,研究方向为网络安全、信息安全和应用密码学。

2.1 修正的 Weil 对

设 q 为大素数，G_1 和 G_2 分别为 q 阶的加法和乘法循环群。修正的 *Weil* 对定义为 G_1、G_2 之间的映射：$\hat{e}: G_1 \times G_1 \mapsto G_2$，具有以下性质：

(1)双线性：对于任意 $P,Q,R \in G_1$，$a,b \in {}_UZ_q^*$：

$\hat{e}(P,Q+R)=\hat{e}(P,Q)\hat{e}(P,R)$

$\hat{e}(P+Q,R)=\hat{e}(P,R)\hat{e}(Q,R)$

$\hat{e}(aP,bQ)=\hat{e}(abP,Q)=\hat{e}(P,abQ)=\hat{e}(P,Q)^{ab}$

(2)对称性：对于任意 $P,Q \in G_1$：$\hat{e}(P,Q)=\hat{e}(Q,P)$

(3)非退化性：存在 $P \in G_1$，使得 $\hat{e}(P,P) \neq 1$。

(4)可计算性：给定 $P,Q \in G_1$，存在一个高效的算法，能够计算 $\hat{e}(P,Q)$。

2.2 基于身份的密码体制

Boneh 和 Franklin 基于身份的密码体制[11]包括系统参数创建和用户密钥生成两个阶段。

系统参数创建：密钥生成中心(KGC)生成阶数为素数 q 的两个群 $(G_1,+)$ 和 $(G_2,\cdot)$，一个修正的 Weil 对映射：$\hat{e}: (G_1,+)^2 \mapsto (G_2,\cdot)$，任意选择一个生成元 $P \in G_1$。选择单向散列函数 $H: \{0,1\}^* \mapsto G_1^* = G_1 - \{O\}$。选取 $s \in {}_UZ_q^*$，并令 $P_{pub}=sP$。KGC 将 s 作为系统的私钥秘密保存，并公开系统参数和它们的描述 $\{G_1,G_2,\hat{e},P,P_{pub},H\}$。

用户密钥生成：假设 ID_i 表示用户 U_i 的唯一可识别的身份。对 U_i 进行物理鉴定以确信 ID_i 具有唯一性。KGC 计算 U_i 的公钥为 $Q_i=H(ID_i)$。然后利用 s 计算 U_i 的私钥：$D_i=sQ_i$，并将 S_i 通过安全的信道传输给 U_i 保存。

用户 U_i 完成以上两个阶段后，拥有自己的公私密钥对 (Q_i,D_i)，以后就可以通过它来完成加/脱密、签名/验证等安全服务。

3 会议密钥的分发和重构算法

3.1 网络初始状态和系统成员

网络的初始状态：网络中任意合法成员 U_i 都完成由 KGC 提供的密钥生成服务并拥有可验证的公私密钥对 (Q_i,D_i)。

系统成员和参数：会议的发起者为 U_d，会议密钥 K 由 U_d 产生，K 的生存期为 T_d；设 $U=\{U_1,\cdots,U_m\}$ 是受到 U_d 邀请参加会议的合法用户集，$S=\{U_1,U_2,\cdots,U_n\}$ 是为 U 提供会议密钥服务的服务集，S 由 U_d 从网络中一些链路状态稳定并能长期提供服务的成员中选择产生。令 q 是一个随机选取且大于 n 的大素数。会议密钥的分发过程如下：

3.2 会议密钥的分发

Step1：U_d 产生随机数 $r \in {}_UZ_q^*$，设当前时间为 T_0，则会议密钥 K 的有效期为 T_0+T_d(即当系统时间 T 满足：$T \leqslant T_0+T_d$ 时 K 有效)。令 $N=(U_d,U,T_0+T_d)$，分别选择两个单向散列函数 $h_1: G_2 \mapsto \{0,1\}^{|N|}$(其中 $|N|$ 代表 N 的二进制长度)和 $h_2: G_1 | Z_q^* = Z_q - \{0\}$，对所有 $1 \leqslant i \leqslant n$ 计算：

$R=rP$

$R_i=\hat{e}(Q_i,rP_{pub}) \in G_2$

$C_i=N \oplus h_1(R_i)$

$V_d=\hat{e}((rP_{pub}+h_2(R)D_d),P)$

将 $\{R,h_1,h_2,V_d\}$ 公开，并将 C_i 传给 $U_i \in S$。

Step2：U_i 接收到 C_i 以及公开信息 (R,h_1,h_2,V_d) 后，首先利用 V_d 验证 U_d 的合法性：$V_d \stackrel{?}{=} \hat{e}((R+h_2(R)Q_d),P_{pub})$。然后解密 C_i 得到 $N=C_i \oplus h_1(\hat{e}(D_i,R))$。由 N 可以获知密钥 K 的有效期以及参加会议的成员 U 的信息。

U_i 返回 $h_2(R)D_i$ 给 U_d。

Step3：U_d 收到 U_i 的消息后，验证 $\hat{e}(h_2(R)D_i,Q_d) \stackrel{?}{=} \hat{e}(h_2(R)Q_i,D_d)$，若成立，说明 U_i 给出了正确的私钥。所有的 $U_i \in S$ 通过验证后，U_d 通过点 $(i,\hat{e}(h_2(R)D_i,D_d))$，$1 \leqslant i \leqslant n$ 以及 $(0,K)$ 构造 n 次多项式 $y \equiv f(x) \equiv K+a_1x+\cdots+a_nx^n \pmod q$。

Step4：计算：$w_j=f(n+j) \pmod q$，$1 \leqslant j \leqslant n-t+1$

公开 $\{S,h_2(R)D_d,w_j\}$，$1 \leqslant j \leqslant n-t+1$，并向所有 $U_j \in U$ 其发出会议邀请。

3.3 会议密钥的重构

为了重构会议密钥 K，任意合法的用户 $U_j \in U$ 至少需要个服务集成员合作。不失一般性，设这 t 个服务集为 $S_t=\{U_1,U_2,\cdots,U_t\}$，特别地，当 $U_j \in S$ 时，只需要向另外 $(t-1)$ 个服务器 $S_{t-1}=\{U_1,\cdots,U_{j-1},U_{j+1},\cdots,U_t\}$ 提出申请。

Step1：U_j 收到 U_d 的邀请后，先确认是否属于 S，如果是，则计算 $w'_i=\hat{e}(h_2(R)D_d,D_j)$，然后向另外 S_{t-1} 提出申请，否则需要向 S_t 提出申请。计算

$V_j=\hat{e}((h_2(R)D_d+h_2(R)D_j),P)$

向 $U_i \in S$ 发送 $\{h_2(R)D_d,V_j\}$。

Step2：任意 $U_i \in S$ 收到申请后，首先确定 U_j 属于 U，且当前正处于有效期，否则拒绝该申请。验证 $V_j \stackrel{?}{=} e(h_2(R)(Q_d+Q_j),P_{pub})$，通过验证后，计算

$w'_i=\hat{e}(h_2(R)D_d,D_i)$

$V_i=\hat{e}((h_2(R)D_d+h_2(R)D_i),P)$

发送 $\{W'_i,V_i\}$ 给 U_j。

Step3：U_j 收到消息，验证 $V_i \stackrel{?}{=} e(h_2(R)(Q_d+Q_i),P_{pub})$，所有 $U_i \in S_t$ 通过验证后，U_j 通过 (i,w'_i)，$1 \leqslant i \leqslant t$ 以及 (j,w_j)，$1 \leqslant j \leqslant n-t+1$ 这 $n+1$ 个点重构 n 次多项式 $y \equiv f(x) \pmod q$，计算会议密钥：$K=f(0)$。

4 分析和讨论

本方案的安全性是建立在基于身份的密码体制和 Shamir 秘密共享方案的安全性之上的。

4.1 正确性和容错性分析

定理 4.1(正确性) 所有被邀请的合法用户得到 S_t 的服务后都能恢复正确的会议密钥。

证明：任意用户 $U_j \in U$ 收到 S_t 的服务后，将会得到这样 $n+1$ 个点：(i,w'_i)，$1 \leqslant i \leqslant t$ 和 (j,w_j)，$1 \leqslant j \leqslant n-t+1$。通过这 $n+1$ 个点可以唯一地构造有限域 n 次多项式为 $y \equiv f'(x) \pmod q$。由修正 Weil 对的性质，有 $w'_i=\hat{e}(h_2(R)D_d,D_i)=e(h_2(R)D_i,D_d)$，则对所有 (i,w'_i)，$1 \leqslant i \leqslant t$ 同时满足方程 $y \equiv f(x) \equiv K+a_1x+\cdots+a_nx^n \pmod q$。因此，$f'(x) \equiv f(x) \equiv K+a_1x+\cdots+a_nx^n \pmod q$，这样，可以计算正确的会议密钥 $K=f(0)$。

定理 4.2(容错性) 如果满足 $t<n<2t$，则在 n 个服务器中最多有 $(n-t)$ 个不诚实服务器时，依然能得到正确的会议密钥。

证明：由 Shamir 秘密共享方案，会议密钥 K 的 n 个秘密分片分别为 (i,w'_i)，$1 \leqslant i \leqslant n$，每一个服务器 $U_i \in S$ 都拥有一个秘密分片。在完成会议密钥的分发后，假使这 n 个服务器

(下转第 143 页)

PI"控制律作用下，系统对运动目标进行视觉跟踪的仿真结果如图5所示。

分析图4与图5知：当目标匀速运动或作缓慢变速平动时，在受限"P+模糊自调节PI"控制律的作用下，目标深度和目标质心在图像上的投影位置可快速收敛至理想值附近，即目标深度收敛至理想深度500mm附近，目标质心投影位置收敛至图像中心$[0,0]^T$附近。并且由于模糊调节器的在线调节功能，控制系统具有较好的动态特征。

结束语 本文阐述了一种能跟踪匀速平动或者缓慢变速平动目标的视觉伺服控制结构和PI参数模糊自调节的视觉跟踪控制算法。在该控制结构和控制算法的作用下，目标始终保持在图像中央且目标深度满足给定值。此外，本文所选择的图像特征集实际上为二值目标图像矩特征的一个子集。采用图像矩作为图像特征的好处是：①无需特征匹配，简化图像处理过程；②对图像噪声具有较强的鲁棒性。

参考文献

1 Hutchinson S. A Tutorial on Visual Servo Control. IEEE Transactions on Robotics and Automation, 1996,12:651～670

2 Benameur K, Belanger P R. Grasping of a moving target with a robotic hand-eye system. In: Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems, 1998. 304～310

3 林靖，陈辉堂，王月娟，等. 基于图像矩的运动目标3D平动视觉跟踪. 机器人，2000,22:218～223

4 SHEN Xiao-Jing. A Simple Adaptive Control for Visual Servoing, 2003 International Conference on Machine Learning and Cybernetics, November 2003,2: 976～979

5 Hong Hyeong-Pyo, Park Suk-Joon, Cho Kyeong-Young. A design of auto-tuning PID controller using fuzzy logic. In: Proceeding of the 1992 International Conference on Industrial Electronics, Control, Instrumentation and Automation, Nov. 1994, 2: 971～976

(上接第116页)

中$(n-t)$的个服务器被攻占或失效，任意用户$U_j \in U$都可向剩余的t个服务器提出请求，同样可以获得t个秘密分片从而恢复会议密钥K。同时，被攻占的$(n-t)$个服务器因为少于t个，所以无法重构多项式$y \equiv f(x) \pmod q$，从而无法获得K的任何信息。

4.2 抗欺诈性分析

本方案可抵抗网络内外的各种欺诈行为：(1)假冒发起者的欺诈：任何非法用户(即没有建立公私钥对的用户)想假冒合法用户发起会议。由于没有正确的私钥D_d，将不能通过验证：$\hat{e}(h_2(R)D_i, Q_d) \stackrel{?}{=} \hat{e}(h_2(R)Q_i, D_d)$，因此任何$U_i \in S$将发现这种欺骗。(2)假冒服务器的欺诈：任何$U_s \notin S$想假冒服务器成员，他可在密钥分发中计算$h_2(R)D_i$，或者在密钥重构中计算$\hat{e}(h_2(R)D_d, D_i)$时欺骗，但是由于$h_2(R)$和$h_2(R)D_d$都是公开信息，任何成员都可以利用$U_i$的公钥$Q_i$进行验证，发现其欺诈行为。(3)假冒会议成员的欺诈：由于每一个服务器成员都秘密地拥有被邀请成员的信息U，任何$U_i \notin U$想假冒会议成员来非法获得会议密钥，都不能通过服务器的检验。(4)不诚实服务器的攻击：如果服务器提供不正确的私钥来生成签名或解密，和(2)一样，将不能通过验证。

另外，由于每个服务器都保存有会议密钥的有效期(T_0+T_d)，当会议过期时，每个服务器都会拒绝为任何成员提供重构会议密钥的服务，这样，就实现了会议密钥的撤消。

4.3 网络性能分析

本方案具有可扩展性的优点，与Tzeng和Xu的方案相比，更适合应用于分布式的环境中。主要表现在这几个方面：(1)会议密钥的秘密分片由服务器自身的私钥产生，在密钥的分发过程中，每个服务器的私钥不会被任何其它成员计算出来，当有多个会议密钥需要共享时，每个会议密钥在这个服务器上的秘密分片只由会议发起者产生的随机数和其本身的私钥决定，不能互相计算得到。这样，任意合法成员都可发起会话，也可在各自指定的服务器集中共享多个会议密钥，同时不需要专门的服务器来存储其秘密分片。(2)服务集S可由会议发起者指定，一般根据选择那些能稳定地提供网络服务的成员作为服务器。服务集的规模n根据它们与会议发起者之间的链路状态来选定，而t值则由会议发起者通过综合考虑网络的运行效率和会议的安全性给出。

结论 本文利用基于身份的密码体制和Shamir秘密共享方案，提出了一种分布式会议密钥分发方案。与传统的秘密共享方案不同的是，秘密分片由服务器的私钥产生，通过收集这些秘密分片，构造多项式函数。这样不需要由会议发起者分发秘密分片，并且在会议密钥的分发和重构过程中，各个成员的身份可以方便地进行验证，避免了各类欺诈行为的发生。与传统的集中式会议密钥分配方案相比，避免了其单一失败点的问题，同时，比协商式会议密钥分配方案具有更少的通信开销和更好的可扩展性，更适合应用于分布式网络。

参考文献

1 Hwang M S. Dynamic Participation in A Secure Conference Scheme For Mobile Communications. IEEE Trans. Vehicular Technology, 1999, 48(5): 1469～1474

2 Xu Y, Siew C K, Tan C H. A Secure and Efficient Conference Scheme for Mobile Communications. IEEE Trans. Vehicular Technology, 2003, 52(4): 784～793

3 Chang C C, Wu T C, Chen C P. The Design of a Conference Key Distribution System. In: Proc. Advances in Cryptology-Auscrypt'92, 1992. 459～466

4 Steiner M, Tsudik G, Waidrer M. Diffie-Hellman key distribution extended to groups. In: ACM Conference Computer and Communication Security, California, 1996, 3: 31～37

5 Kim Y, Perrig A, Tsudik G. Group Key Agreement Efficient in Communication. IEEE Trans. Computers, 2004, 53(7): 905～921

6 Tzeng W G. A Secure Fault-tolerant Conference-key Agreement Protocol. IEEE Trans. Computers, 2002, 51(4): 373～379

7 Xu Y. Identity-Based Fault-Tolerant Conference Key Agreement. IEEE Trans. Dependable and Secure Computing, 2004, 1(3): 170～178

8 Shamir A. Identity-based Cryptosystems and Signature Schemes. In: Proceedings of Crypto 1984, Providence, USA: Springer-Verlag, 1984. 47～53

9 Shamir A. How to Share a Secret. Comm. ACM, 1979, 22(11): 656～715

10 Verheul E R. Evidence That XTR Is More Secure Than Supersingular Elliptic Curve Cryptosystems. Advances in Cryptology-Proceedings of EUROCRYPT'01, Spring-Verlag, 2001. 195～210

11 Boneh D, Franklin M. Identity Based Encryption From The Weil Pairing. Advances in Cryptology-Proceedings of CRYPTO'01, Spring-Verlag, 2001. 213～229