一个新的广播信道会议密钥协商协议

毛 剑,高虎明,王育民
(西安电子科技大学 ISN 国家重点实验室,陕西西安 710071)

摘 要: 群组用户试图在开放式网络上进行安全通信时,需运行一个会议密钥协议来支持一个共同的会议密钥 K.本文中,利用基于 MDS 码(Maximum Distance Code,极大最小距离可分码)的秘密共享方案作为基本构件,提出了一个新颖高效、可证明安全的广播信道下会议密钥协商协议.该协议在广义的 Diffie-Hellman Problem(DHP)困难假设下,被动攻击者得不到任何有关诚实参与者协商出的会议密钥的信息;且无论存在多少恶意参与者,诚实参与者一定能够协商出一共同的会议密钥.

关键词: MDS 码; 秘密共享; 广播信道; 会议密钥协商; 数字签名
中图分类号: TP198 **文献标识码**: A **文章编号**: 0372-2112 (2004) 04-0642-03

A New Conference-Key Agreement Protocol Under the Broadcast Channel

MAO Jane, GAO Hu-ming, WANG Yu-min
(*National Key Lab. of ISN, Xidian Univ., Xian, Shaanxi* 710071, *China*)

Abstract: When a group of people want to communicate securely over an open network, they need to run a conference-key establishment protocol to establish a common conference key K such that all their communication thereafter are encrypted with the key K. By using the secret sharing scheme based on the MDS code as the basic component in this paper, we propose a new provably secure conference-key agreement protocol under the broadcast channel. In the protocol, a passive adversary gets no information about the conference-key established by the honest participants under the assumption of general Diffie-Hellman problem; and the honest participants can agree on a common conference-key no matter how many participants are malicious.

Key words: MDS code; secret sharing; broadcast channel; conference-key agreement; digital sigature

1 引言

在开放式网络进行群组通信时,通常需采用会议密钥建立协议来建立一密钥 K,以便通信群体能够进行高效的秘密通信.会议密钥建立有两类:(1)由可信赖中心(TA)选择一个会议密钥,然后分发给通信群体中的各个成员,这种方式通常被称为会议密钥分发;(2)无需 TA,由通信群体中成员一起计算出共同的会议密钥 K,这种方式通常被称为会议密钥协商.其中,会议密钥协商更适合应用于分布式环境.

广播信道下的会议密钥协商协议有如下特点:(1)参与者间不存在秘密信道;(2)恶意参与者的目的是阻止诚信的参与者协商出共同的会议密钥;(3)一旦发现恶意参与者,恶意参与者将被从会议群体中删除,其秘密信息作废,而不会影响会议密钥的生成.

目前,针对会议密钥建立协议已经有了很多深入的研究,如会议密钥分发协议[1,2];会议密钥协商协议[3,4].大多数协议致力于会议密钥的保密以及对于不同网络连接的信息效率.然而这些协议均无法防止恶意用户对会议密钥的协商所进行的破坏.

本文中,我们给出一个新颖高效的广播信道下会议密钥协商协议.通常协议将面对主动、被动两种攻击:主动攻击者意图阻止诚实参与者建立会议密钥;被动攻击者意图通过窃听参与者间的通信来获得会议密钥.我们将证明,在本方案中:基于广义 Diffie-Hellman problem 困难假设下,被动攻击者将得不到有关诚信参与者协商出的会议密钥的任何信息;且无论存在多少的恶意参与者(主动攻击者),所有诚信参与者亦能够协商出一共同的会议密钥.

2 方案模型

系统中用户为一概率多项式时间图灵机.每个用户 U_i 拥有一秘密信息 x_i 及相应的公开信息 y_i.系统中建立一公共目录用以存放系统、用户的公开信息,且可被任意访问.所有用户均连接在认证的广播信道之上,即网络中所有传送的消息均被确认且不会被替换、阻塞或迟延.用户之间不存在秘密信道.意欲协商密钥的一组用户被称为参与者集合,其中可能存在恶意参与者.

收稿日期:2002-06-12;修回日期:2002-10-19
基金项目:国家自然科学基金(No.60073052)

存在的两类攻击者均为概率多项式时间图灵机.被动攻击者本身并非参与者,其对广播信道进行侦听以求获得诚实参与者所协商出的会议密钥.主动攻击者是协议参与者,意图阻止诚信参与者协商出共同的会议密钥.主动攻击者主要通过广播恶意消息以愚弄诚实参与者,使诚实参与者相信他也在遵守协议进行会议密钥的协商,进一步对会议密钥协商的破坏,使得会议无法及时进行;而本协议具有鲁棒性,即使有多个恶意参与者合谋,对本协议亦不构成威胁,诚实用户总能够按照协议协商出一个公共的会议密钥,以保证会议顺利进行.一个会议密钥协商协议是安全的,意味着它能够抗主动被动攻击:(1)抗被动攻击,单个敌手通过监听信道,得不到任何有关会议密钥的信息;(2)抗主动攻击,敌手不论以何种方式违反协议,其成功破坏诚实参与者协商会议密钥的概率可以忽略不计.

3　方案设计

本协议的设计思想基于所谓的 Democratic Shared Control Scheme[6],其核心概念是:(1)每个参与者输入其自己的 contributor 来一起确定一个 secret(即,会议密钥).每个参与者的 contributor 对 secret 值的确定具有同等的重要性(这里的 contributor 相当于子密钥);(2)每个参与者将其 contributor 的信息与其他参与者部分共享,使得其他参与者能够利用所知以及共享信息恢复出该参与者的 contributor;(3)这样,所有的参与者即可计算出一共同的 secret.若有恶意参与者,意图发送恶意信息(如,给出错误共享信息;或声称他人所给的共享信息有误)以对密钥协商进行破坏,则其他用户便会将其从参与者集合中删除,而后重新启动协议,进行会议密钥的协商.在我们的方案中,采用 MDS 码作为秘密共享的基本构件[6].

3.1　准备工作——注册

每个需要参与会议的用户,需进行注册,由系统对用户进行编号后,系统将所有参与者集合列表 $\overline{U}=(U_1,U_2,\cdots,U_n)$ 公布于公开目录中.

3.2　具体协议

3.2.1　参数设定　系统公开参数:$\overline{U}:(U_1,U_2,\cdots,U_n)$为初始参与者集合;$p$ 为大素数,且 $p=2q+1$,其中 q 亦为一大素数,$q+2\geq n$;H 为 $Z_q\to Z_q$ 的哈希函数;g 为 $G_q=\{i^2\mid i\in Z_p^*\}$ 的生成元;G 为 $GF(q)$上的$(2n,n)$-MDS 码的生成距阵.

用户参数:秘密参数:$x_i\in Z_q^*$;公开参数:$y_i=g^{x_i}\bmod p$

3.2.2　协议执行　初始化:每个用户初始化其参与者集 $\overline{U}_i=\overline{U}=\{U_1,U_2,\cdots,U_n\}$.

step1　秘密分享与承诺　每个参与者 $U_i(1\leq i\leq n)$执行:

(a)随机选择 $R_i,K_i\in Z_q,S_i\in Z_q^*$;

(b)计算 $d_{i,j}=\begin{cases}y_j^{R_i}\bmod p\bmod q, & j\in\{j\mid U_j\in\overline{U}_i\},j\neq i;\\ 0, & j\in\{j\mid U_j\notin\overline{U}_i,U_j\in\overline{U}\},\end{cases}$由 $K_i,d_{i,j}(1\leq j\leq n,i\neq j)$构成 n 维向量:$D_i=(d_{i,1},\cdots,d_{i,i-1},K_i,d_{i,i+1},\cdots,d_{i,n})$;

(c)计算 $B_i=D_i\cdot G=(d_{i,1},\cdots,d_{i,i-1},K_i,d_{i,i+1},\cdots,d_{i,n},b_{i,1},\cdots,b_{i,n})$,(根据系统码定义,码字的前 n 位仍保持信息位不变,后 n 位则为校验位);

(d)公布 $\boldsymbol{b}_i=((b_{i,j},j))_{1\times(|\{j\mid U_j\in\overline{U}_i\}|-1)},j\in\{j\mid U_j\in\overline{U}_i\},j\neq i$;

(e)计算并分布 $\alpha_i=g^{R_i}\bmod p;\gamma_i=g^{S_i}\bmod p;\delta_i=S_i^{-1}(H(K_i)-\gamma_i x_i)\bmod q$.

Step2　子密钥计算与验证　当 $j\neq i$ 时,U_i 执行:

(a)收到 $\boldsymbol{b}_j,\alpha_j$,计算　$d_{j,i}=\gamma_j^{R_j}\bmod p\bmod q=\alpha_j^{x_i}\bmod q$;

(b)由广播消息　U_i 可知:

$$\begin{cases}d_{j,i}=\alpha_j^{x_i}\bmod q\\ d_{j,l}=0, & l\in\{l\mid U_l\notin\overline{U}_i,U_l\in\overline{U}\}\ (1),\\ \boldsymbol{b}_j=((b_{j,l},l))_{1\times(|\{l\mid U_l\in\overline{U}_j\}|-1)}, & l\in\{l\mid U_l\in\overline{U}_i\},l\neq j\end{cases}$$

若$|\{l\mid U_l\in\overline{U}_i\}|\neq|\boldsymbol{b}_j|+1$,则广播 $V_{ij}=$"failure",且视 U_j 为恶意参与者,结束 step2;否则根据$(2n,n)$-MDS 码的定义,由式(1)可知 D_j 相应 n 位的值,既而计算恢复出码字 D_j;

(c)取 D_j 的第 j 位分量 K'_j(此处用 K'_j 表示仍待验证的子密钥);

(d)验证　$g^{H(K'_j)}\bmod p=\gamma_j^{\gamma_j}\gamma_j^{\delta_j}\bmod p$ 是否成立;若成立,则广播　$V_{ij}=$"success";否则,广播　$V_{ij}=$"failure",且视 U_j 为恶意参与者.

Step3　错误探测　当 $j\neq i$ 时,U_i 执行:

(a)接收以某些 U_j 发出的 $V_{ij}=$"failure"时(即,有参与者声称 U_i 欺诈):U_i 输出 R_i,K_i,S_i,作为其错误探测信息,以待其他参与者验证;

(b)接收到 $U_{jm}=$"failure"时(即,U_j 声称 $U_m(m\neq i)$欺诈):(1)等待接收 U_m 的错误探测信息:R_m,K_m,S_m;(2)若一直未接收到 U_m 的错误探测信息,则确定 U_m 为恶意参与者;(3)若接收到 U_m 的错误探测信息(R_m,K_m,S_m),则验证 $\boldsymbol{b}_m,\alpha_m,\gamma_m,\delta_m$ 是否正确,即验证:(1)$|\{l\mid U_l\in\overline{U}_i\}|=|\boldsymbol{b}_m|+1$ 是否成立;(2)$\alpha_m=g^{R_m}\bmod p$ 是否成立;(3)是否 $\exists B_m$,有 $B_m=D_m\cdot G$;(4)$\boldsymbol{b}_m=((b_{m,l},l))_{1\times(|\{l\mid U_l\in\overline{U}_m\}|-1)},l\in\{l\mid U_l\in\overline{U}_m\},l\neq m$ 是否成立;(5)(α_m,γ_m)是否是 U_m 对 $H(K'_m)$的 ELGAMAL 签字;若通过所有验证,则证明 U_j 为恶意参与者;否则 U_m 即是恶意参与者;

(c)将恶意参与者从自己的参与者集中删除,然后重启协议,直到探测无误。

Step4　会议密钥计算

探测无误后,每个参与者 U_i 计算会议密钥:

$$K=\sum_{l\in\{l\mid U_l\in\overline{U}_i\}}K_l\bmod q.$$

4　安全性分析

本节对协议的正确性,鲁棒性(抗主动攻击),以及抗被动攻击安全性加以分析.

4.1　正确性及鲁棒性

定理 1(正确性)　如果所有参与者均遵守协议,则他们一定能够计算出一个共同的会议密钥.

证明　由 U_j 广播的消息,U_i 能够计算出码字 B_j 的 n 个分量,由$(2n,n)$-MDS 码的定义可知,U_i 能够唯一确定出码字

B_j,取出 B_j 的第 j 位即为 K_j.通过 $H(K_j)$的签字 γ_j,δ_j,即可验证出 K_j 的正确性.因此,所有参与者均可计算出 K_j,进而计算出统一的会议密钥 $K = K_1 + K_2 + \cdots + K_n \bmod q$. [证毕].

通过对协议的分析,很容易得到如下结论:结论(1)所有试图欺骗诚实参与者接受错误 K_j 的参与者 U_j,一定会被所有诚实参与者从各自的参与者集中删除;结论(2)任何诚实参与者均不会被其他诚实参与者从参与者集中删除.

定理 2(鲁棒性) 无论存在多少恶意参与者,所有诚实参与者拥有同样的参与者集,且能够计算出统一的会议密钥.

4.2 抗被动攻击安全性

被动攻击者会试图通过监听广播信道中消息,来获得有关会议密钥的信息.在我们的方案中,基于广义 Diffie-Hellman 问题困难假设下(DHP),攻击者仅仅从监听所得视图($\boldsymbol{b}_i$,α_i,γ_i,δ_i),得不到任何有关用户 U_i 子密钥 K_i 的信息.

由广义 Diffie-Hellman Problem(DHP)[6]知循环群 G,g 为 G 的生成元,且已知 g^a、g^b 为 G 中元素,求 g^{ab} 的问题为广义 Diffie-Hellman 问题.

假设:设 G_q 上,广义 Diffie-Hellman Problem 困难.

结论(3)在 DHP 困难假设下,被动攻击者得不到任何有关 $y_j^{\beta_i} \bmod p \bmod q (1 \le j \le n)$的信息.

根据$(2n, n)$-MDS 码的特性,被动攻击者在仅知码字 n-1 位分量的情形下,得不到任何有关码字其他位的信息.

结论(4)被动攻击者由 $\boldsymbol{b}_i$ 得不到任何有关码字其他位的信息.

由结论(3)、(4),有下面的定理.

定理 3 被动攻击者得不到任何有关用户 U_i 子密钥 K_i 的信息.

定理 4 被动攻击者得不到任何有关会议密钥 K 的信息.

5 结论

在本文中,给出了一个新颖高效的广播信道下会议密钥协商协议.在广义 Diffie-Hellman problem 困难假设下,协议对于主、被动攻击是计算上安全的.协议非常实用有效,在探测出所有恶意参与者后,只需两轮计算,诚实参与者即可得到一个共同的会议密钥.不过,每个参与者广播的消息大小与参与者人数成正比.因此,如何设计一个在轮数和消息长度方面均高效的协议仍有待于进一步研究.

参考文献:

[1] C C Chang, C H Lin. How to converse securely in a conference [A]. proc. IEEE 3th Ann. Int'l Carnahan Conf [C]. Lexingto, Kentucky, 1996.42 - 45.

[2] C Blundo, A D Santis. Perfectly-secure key distribution for dynamic conference [A]. Proc. Advances in Cryptology-Crypto'92 [C]. Santa Barbara, California, Springer-Verlag, 1993.471 - 486.

[3] D Steer, L Strawczynski. A secure audio teleconference system [A]. Proc. Advances in Cryptology-Crypto'88 [C]. Santa Barbara, California, Springer-Verlag, 1990.520 - 528.

[4] T C Wu. Conference key distribution system with user anonymity based on algebraic approach [J]. IEE Proc. Computers and Digital Techniques, 1997, 144(2): 145 - 148.

[5] Ingemarsson I. A protocol to set up shared secret schemes without the assistance of a mutually trusted party [A]. Proc. Advances in Cryptology-Eurocrypt'90 [C]. Aarhus, Denmark, Springer-Verlag, 1991.266 - 282.

[6] D Boneh, R Venkatesan. Hardness of computing the most significant bits of secret keys in diffie-hellman and related problems [A]. Proc. Advances in Crytology-Crypto'96 [C]. Santa Barbara, California, Springer-Verlag, 1996.129 - 142.

作者简介:

毛 剑 女,1978 年 2 月生于宁夏银川市,西安电子科技大学博士生,主要研究方向:密码学及其应用,电子商务和网络安全.E-mail: maoxiaojane@hotmail.com

高虎明 男,1963 年 1 月生于山西,西安电子科技大学博士生,副教授,主要研究方向:密码学及其应用,电子商务和网络安全.

王育民 男,1936 年生于北京,西安电子科技大学教授,博士生导师,研究领域为信息理论,编码及密码理论.