文章编号:2095-476X(2015)3/4-0094-04

对 Tasi 群密钥协商协议的改进及安全分析

霍丽娟[1], 李朝阳[2], 孙垒[3]

(1. 河南理工大学 计算机科学与技术学院, 河南 焦作 454003;
2. 郑州轻工业学院 数学与信息科学学院, 河南 郑州 450002;
3. 河南理工大学 数学与信息科学学院, 河南 焦作 454003)

摘要:针对 J. L. Tsai 等人提出的移动环境下群密钥协商协议存在的安全缺陷,利用数字签名技术,对其进行了改进:在数字签名中加入序列号,用以标记签名和将要生成的群密钥的次序,并将序列号作为数字签名公开验证信息之一,从而实现对移动用户或者具有较强计算能力的节点所发送消息的及时验证. 由安全分析可知,改进后的协议不仅具有原来的安全特性,而且可以抵抗重放攻击或冒充攻击.

关键词:群密钥协商协议;双线性对;移动通信;数字签名
中图分类号:TP309 **文献标志码**:A **DOI**:10.3969/j.issn.2095-476X.2015.3/4.021

Improvement and security analysis on Tasi's group key agreement

HUO Li-juan[1], LI Zhao-yang[2], SUN Lei[3]

(1. *College of Computer Science and Technology, He'nan Polytechnic University, Jiaozuo* 454003, *China*;
2. *College of Mathematics and Information Science, Zhengzhou University of Light Industry, Zhengzhou* 450002, *China*;
3. *College of Mathematics and Information Science, He'nan Polytechnic University, Jiaozuo* 454003, *China*)

Abstract: Aimed at the security defect of group key agreement protocol for mobile environment proposed by J. L. Tsai, the protocol was improved by using the digital signature technology. That is, some serial numbers were inserted in the digital signatures so as to identify the signatures and the order of the group keys to be generated, and the serial numbers were used as part of public information to verify the digital signatures. So the freshness of messages sent by the mobile users or the powerful node could be checked. According to the security analysis, it is found that the improved protocol not only had the old security properties, but also could resist against impersonation attack or forgery attack.

Key words: group key agreement protocol; bilinear pairing; mobile communication; digital signature

0 引言

群密钥协商协议[1]是一种非常重要的群体通信协议,群成员共同参与,通过协商和共同计算,形成一个群体共享的密钥. 同时,群体成员通过这个共享密钥对群成员之间的通信内容进行加密和解密,以实现群体成员之间的安全通信. 移动环境下群密钥协商协议是安全通信重要的研究内容.

收稿日期:2015-01-01
基金项目:国家自然科学基金项目(61272525);河南省教育厅科学技术研究项目(14A110003)
作者简介:霍丽娟(1978—),女,河南省临颍县人,河南理工大学助教,主要研究方向为计算机网络安全.

早期移动环境下的群密钥协商协议[2-4]计算量大,其计算耗费随着移动用户的增加而线性增加,因此这些协议在移动环境下的应用受到了限制. 为此,J. Nam 等[5]提出了一种计算轮数固定、计算量小且具有前向安全性的密钥协商协议,但该协议无法证明移动用户都具有同样的群密钥计算贡献. Y. M. Tseng[6]给出一种非平衡无线网络下的群密钥协商协议,以保证群密钥协商中所有移动用户在生成群密钥时提供相同的密钥贡献. 随后, C. C. Lee 等[7]证明了文献[6]中群密钥协商协议存在的安全缺陷,即该协议是非认证的,并且提出一种新的认证群密钥协商协议. 2011 年, J. L. Tsai 等[8]分析了文献[7]的群密钥协商协议,指出该协议不能抵抗冒充攻击,并给出了一种改进的协议(以下简称 Tsai 协议). 然而,通过本文分析,发现 Tasi 协议仍然存在安全缺陷,即该协议不能抵抗重放或冒充攻击. 事实上,对于文献[2-8]所给出的群密钥协商协议,都可以归结为基于公钥证书的群密钥协商协议. 最近几年,为简化公钥证书管理,一些学者也相继提出了基于身份的群密钥协商协议[9-11]. 然而,这些群密钥协商协议都需要一个绝对可信的密钥生成机构为用户生成私钥,所有用户都必须绝对信任这些密钥生成机构,这使得这些协议的使用范围受到了限制,即其只能用于封闭的机构(如一个企业或单位的内部). 同基于身份的群密钥协商协议相比,基于公钥证书的群密钥协商协议仍然具有自己的优势,即这种协议不需要可信的密钥生成机构为用户生成私钥,从而避免了密钥托管. 因此,本文将研究重点放在基于公钥证书的群密钥协商协议的安全构造上,在分析 Tsai 协议基础上对其进行改进,以使改进后的协议不仅具有原来的安全特性,而且可以抵抗重放或冒充攻击.

1　Tasi 协议分析

Tasi 协议中需要用到的参数如表 1 所示.

假设 $U_1, U_2, \cdots, U_{n-1}$ 为计算能力较弱的移动用户,而 U_n 为具有较强计算能力的节点,Tasi 协议实现步骤如下.

步骤 1　每个 $U_i(1 \leqslant i \leqslant n-1)$ 分别计算 $A_i = a_i P(a_i \in_R Z_q^*)$ 和 $S_i = \frac{1}{H(A_i) + X_i} P$,并将 (U_i, A_i, S_i) 发送给 U_n.

表 1　Tasi 协议中的部分符号描述

符号	符号描述
p, q	分别为一个素数和椭圆曲线的阶数
G_1, G_2	分别为阶数为 q 的加法循环群和乘法循环群
P	G_1 中公开选取的一个点
n	参与密钥协商的用户个数
$H(\cdot)$	单向 Hash 函数,$H: \{0,1\}^* \rightarrow G_1$
X_i	移动用户或者具有较强计算能力的节点的私钥
Y_i	移动用户或者具有较强计算能力的节点的公钥
$a_i \in_R Z_q^*$	a_i 为在 Z_q^* 中随机选取的一个数

步骤 2　收到 (U_i, A_i, S_i) 后,U_n 验证双线性映射[12] $e(H(A_i)P + Y_i, S_i) = e(P, P)$ 是否成立. 若成立,U_n 计算 $x_i = a_n A_i$,其中 $a_n \in_R Z_q^*$. 然后,U_n 计算 $B = H(U_n, x_1, x_2, \cdots, x_{n-1})$ 和其签名 $S_n = \frac{1}{B + X_n} P$,以及群密钥 $K = H(a_n P, x_1, x_2, \cdots, x_{n-1}, S_n)$. U_n 向 U_i 广播 $(U_n, x_1, x_2, \cdots, x_{n-1}, S_n)$.

步骤 3　收到广播后,每个 U_i 计算 $B = H(U_n, x_1, x_2, \cdots, x_{n-1})$ 并验证 $e(BP + Y_n, S_n) = e(P, P)$ 是否成立. 若成立,每个 U_i 计算群密钥 $K = H(a_i^{-1} x_i, x_1, x_2, \cdots, x_{n-1}, S_n) = H(a_n P, a_n a_1 P, a_n a_2 P, \cdots, a_n a_{n-1} P, S_n)$.

虽然文献[8]证明了其所提出 Tasi 协议的安全性,但事实上,在上述步骤 1 中,是利用短签名方案[12]对数据 A_i 进行签名的,并将签名 (U_i, A_i, S_i) 发给 U_n,而这个签名并不能抵抗重放或冒充攻击. 由于 (U_i, A_i, S_i) 是公开的,任何人都可以窃听或截获这个签名. 当恶意的攻击者 Alice 截获 (U_i, A_i, S_i) 后,可以保存这些旧数据. 当移动用户发动下一次的群密钥协商时,Alice 可以冒充任何一个 U_i,并将该 U_i 相应的旧 (U_i, A_i, S_i) 重新发送给 U_n. 由于 (U_i, A_i, S_i) 是 U_i 合法的签名,其必然能通过 U_n 的验证. 这种重放攻击使得 Alice 能够冒充 U_i 参与群密钥协商,从而干扰了 U_i 参与群密钥协商的行为,破坏了群密钥协商的协作性.

另外,当移动用户发动下一次的群密钥协商时,在这种重放攻击下,Alice 还可以计算出新的群密钥. 事实上,$A_i = a_i P$ 中的 a_i 作为临时使用的数据,有可能遭到泄露. 而一旦 a_i 遭到泄露,攻击者可以冒充 U_i 获得下次的群密钥协商所产生的群密钥 K. 比如,假定在某次群密钥协商中,攻击者 Alice 获得了某个 U_i 的有效 (U_i, A_i, S_i),并且掌握了 a_i. Alice可以通过以下步骤冒充 U_i 参与以后的群密钥协商,并计算出新的群密钥.

步骤 1 每个 $U_j(1\leqslant j\leqslant n-1, j\neq i)$ 分别计算 $A'_j = a'_j P(a'_j \in_R Z_q^*)$ 和 $S'_j = \frac{1}{H(A'_j)+X_j}P$, 并将 (U_j, A'_j, S'_j) 发送给 U_n. 而 Alice 冒充 U_i 将以前所保存的旧 (U_i, A_i, S_i) 发送给 U_n.

步骤 2 收到 (U_j, A'_j, S'_j) 和 (U_i, A_i, S_i) 后, U_n 验证双线性映射 $e(H(A'_j)P+Y_j, S'_j) = e(P,P)$ 和 $e(H(A_i)P+Y_i, S_i) = e(P,P)$ 是否成立. 若成立, U_n 计算 $x'_j = a'_n A'_j$ 和 $x'_i = a'_n A_i$, 其中 $a'_n \in_R Z_q^*$. 然后, U_n 计算 $B' = H(U_n, x'_1, x'_2, \cdots x'_{n-1})$ 和其签名 $S'_n = \frac{1}{B'+X_n}P$, 以及群密钥 $K' = H(a'_n P, x'_1, x'_2, \cdots, x'_{n-1}, S'_n)$. U_n 向 U_j 广播 $(U_n, x'_1, x'_2, \cdots, x'_{n-1}, S'_n)$.

步骤 3 收到广播后, 每个 U_j 计算 $B' = H(U_n, x'_1, x'_2, \cdots, x'_{n-1})$ 并验证 $e(B'P+Y_n, S'_n) = e(P,P)$ 是否成立. 若成立, 每个 U_j 能够计算群密钥

$$K' = H(a'^{-1}_j x'_j, x'_1, x'_2, \cdots, x'_{i-1}, x'_i, x'_{i+1}, \cdots, x'_{n-1}, S'_n) = H(a'_n P, a'_n a'_1 P, a'_n a'_2 P, \cdots, a'_n a'_{i-1} P, a'_n a_i P, a'_n a'_{i+1} P, \cdots, a'_n a'_{n-1} P, S'_n)$$

同时, 攻击者 Alice 也可以计算群密钥

$$K' = H(a_i^{-1} x'_i, x'_1, x'_2, \cdots, x'_{i-1}, x'_i, x'_{i+1}, \cdots, x'_{n-1}, S'_n) = H(a'_n P, a'_n a'_1 P, a'_n a'_2 P, \cdots, a'_n a'_{i-1} P, a'_n a_i P, a'_n a'_{i+1} P, \cdots, a'_n a'_{n-1} P, S'_n)$$

2 Tasi 协议的改进及安全分析

由以上分析可知, Tasi 协议的主要问题在于步骤 1 中 U_i 仅仅对随机数 A_i 进行了签名 (U_i, A_i, S_i), 其作用缺乏时效性. 为保证签名的时效性, 防止 Alice进行重放或冒充攻击, 可以改变签名的内容, 即在签名中加入序列号, 序列号是本次将要生成群密钥次序的唯一标记. 为此, 对协议进行如下改进.

步骤 1 每个 $U_i(1\leqslant i\leqslant n-1)$ 分别计算 $A_i = a_i P(a_i \in_R Z_q^*)$ 和 $S_i = \frac{1}{H(A_i \| T)+T_i}P$, 并将 (U_i, A_i, T, S_i) 发送给 U_n, 其中, T 为当前序列号, 标记为本次将要生成的群密钥的次序.

步骤 2 收到 (U_i, A_i, T, S_i) 后, U_n 验证 $e(H(A_i \| T)P+Y_i, S_i) = e(P,P)$ ("‖"表示二进制串的连接) 是否成立. 若成立, 并且序列号 T 符合本次将要生成的群密钥的次序, 则 U_n 计算 $x_i = a_n A_i$, 其中 $a_n \in_R Z_q^*$. 然后, U_n 计算 $B = H(U_n, x_1, x_2, \cdots, x_{n-1}, T)$ 和其签名 $S_n = \frac{1}{B+X_n}P$, 以及群密钥 $K = H(a_n P, x_1, x_2, \cdots, x_n, S_n, T)$. U_n 向 U_i 广播 $(U_n, x_1, x_2, \cdots, x_{n-1}, T, S_n)$.

步骤 3 收到广播后, 每个 $U_i(1\leqslant i\leqslant n-1)$ 计算 $B = H(U_n, x_1, x_2, \cdots, x_{n-1}, T)$ 并验证 $e(BP+Y_n, S_n) = e(P,P)$ 是否成立. 若成立, 并且 T 符合规定的群密钥的次序, 则每个 U_i 能够计算群密钥

$$K = H(a_i^{-1} x_i, x_1, x_2, \cdots, x_{n-1}, S_n) = H(a_n P, a_n a_1 P, a_n a_2 P, \cdots, a_n a_{n-1} P, S_n)$$

定理 1 在改进的协议中, 敌手通过窃听或截获所有 $U_i(1\leqslant i\leqslant n-1)$ 和 U_n 之间的通信内容, 无法获得群密钥.

证明 敌手通过窃听或截获所有 $U_i(1\leqslant i\leqslant n-1)$ 和 U_n 之间的通信内容, 可以获得 (U_i, A_i, T, S_i) 和 $(U_n, x_1, x_2, \cdots, x_{n-1}, T, S_n)$. 在离散对数问题假设下[12], 敌手由 A_i 计算出 a_i 是困难的. 而群密钥 $K = H(a_n P, a_n a_1 P, a_n a_2 P, \cdots, a_n a_{n-1} P, S_n)$, 故敌手若想计算出 K, 就必须先计算出 $a_n P$. 但是, 在不知道 a_i 的条件下, 利用椭圆曲线下的计算 Diffie-Hellman 问题和离散对数问题假设[13], 可知敌手无法由 $a_n a_1 P, a_n a_2 P, \cdots, a_n a_{n-1} P$ 计算出 $a_n P$. 因此, 敌手无法获得群密钥 K.

定理 2 改进的协议可以抵抗冒充攻击.

证明 假定一个敌手想冒充合法的用户 $U_i(1\leqslant i\leqslant n-1)$ 和 U_n 进行通信, 希望能够计算出群密钥 K. 若想冒充 U_i, 敌手需要计算出短签名 $S_i = \frac{1}{H(A_i \| T)+X_i}P$. 若敌手想冒充 U_n 和 U_i 进行通信, 其也必须计算出短签名 $S_n = \frac{1}{B+X_n}P$. 然而, 短签名是不可伪造的[12], 即非法用户无法计算出这些短签名, 故敌手无法成功冒充用户 U_i 和 U_n. 因此, 改进的协议可以抵抗冒充攻击.

然而, 需要进一步考虑的是, Alice 能否重放旧 (U_i, A_i, T, S_i) 得到新的群密钥. 事实上, 在改进的协议中使用序列号 T 对每次通信的 (U_i, A_i, T, S_i) 和 $(U_n, x_1, x_2, \cdots, x_{n-1}, T, S_n)$ 进行标记, 即本次将要生成的群密钥的次序. 一旦Alice重新将某个旧 (U_i, A_i, T, S_i) 发送给 U_n, U_n 可以通过检查序列号 T 是否符合本次群密钥的生成次序. 若 T 已经使用过, 则可以检测出 Alice 重放 (U_i, A_i, T, S_i) 或冒充 U_i. 类似地, 在 S_n 中也加入序列号 T, U_i 可以通过检查序列号 T 来检测出 Alice 重放旧数据 $(U_n, x_1, x_2, \cdots, x_{n-1}, T, S_n)$ 或冒充 U_n. 从而, Alice 无法利用旧 (U_i, A_i, T, S_i) 计算新的群密钥.

同时, 由于所使用的文献[12]的短签名可证明

是安全的,故在改进的协议中,(U_i, A_i, T, S_i)和$(U_n, x_1, x_2, \cdots, x_{n-1}, T, S_n)$仍具有不可伪造性,所使用的序列号保证了这些数据的新鲜性,进而保证协议可以检测出敌手的重放攻击或冒充攻击.

3　结语

本文对 J. L. Tsai 等提出的移动环境下群密钥协商协议存在的安全缺陷,作出了改进:通过在移动用户 U_i 和节点 U_n 所发送或广播的数据中加入序列号,并将这些数据和相应的序列号绑定后再利用短签名方案对其签名,以保证用户之间通信内容的认证性和新鲜性,使得改进后的群密钥协商协议可以抵抗重放或冒充攻击. 同时,改进的协议具备 Tasi 协议的其他安全特性.

参考文献:

[1] Asokan N, Ginzboorg P. Key agreement in ad hoc networks [J]. Computer Communications, 2000, 23(17): 1627.

[2] Burmester M, Desmedt Y. Advances in Cryptology—EUROCRYPT94 [M]. Berlin: Springer Berlin Heidelberg, 1994: 275 – 286.

[3] Bresson E, Catalano D. Public Key Cryptography—PKC 2004 [M]. Berlin: Springer Berlin Heidelberg, 2004: 115 – 129.

[4] Katz J, Yung M. Scalable protocol for authenticated group key exchange [J]. Journal of Cryptology, 2007, 20(1): 85.

[5] Nam J, Lee J, Kim S, et al. DDH-based group key agreement in a mobile environment [J]. Journal of Systems and Software, 2005, 78(1): 73.

[6] Tseng Y M. A resource-constrained group key agreement protocol for imbalanced wireless networks [J]. Computer & Security, 2007, 26(4): 331.

[7] Lee C C, Lin T H, Tsai C S. A new authenticated group key agreement in a mobile environment [J]. Annals of Telecommunications, 2009, 64(11 – 12): 735.

[8] Tsai J L. A novel authenticated group key agreement protocol for mobile environment [J]. Annals of Telecommunications, 2011, 66(11 – 12): 663.

[9] Teng J, Wu C K, Tang C. An ID-based authenticated dynamic group keyagreement with optimal round [J]. Science China Information Sciences, 2012, 55(11): 2542.

[10] Konstantinou E. Network and System Security [M]. Berlin: Springer Berlin Heidelberg, 2013: 563 – 574.

[11] Hu K W, Xue J F, Hu C Z, et al. An improved id-based group key agreement protocol [J]. Tsinghua Science and Technology, 2014, 19(5): 421.

[12] Zhang F G, Safavi-Naini R, Susilo W. Public Key Cryptography—PKC 2004 [M]. Berlin: Springer Berlin Heidelberg, 2004: 277 – 290.

[13] Zhang J H, Yang Y X, Niu X X. Advances in Neural Networks—ISNN 2009 [M]. Berlin: Springer Berlin Heidelberg, 2009: 318 – 327.