一种故障容忍的可证安全组密钥协商协议

郑明辉[1,2], 周慧华[1], 崔国华[1], 韩兰胜[1]
(1. 华中科技大学计算机科学与技术学院, 湖北武汉 430074; 2. 湖北民族学院信息工程学院, 湖北恩施 445000)

摘 要: 对 Burmester 等人提出的非认证组密钥协商协议的安全性进行了深入分析, 指出该协议不能抵抗内部恶意节点发起的密钥协商阻断攻击和密钥控制攻击. 提出了一种故障容忍的组密钥协商(FT-GKA)协议, FT-GKA 协议在密钥协商过程中加入了消息正确性的认证机制, 该机制利用数字签名技术检测组内恶意节点, 并在驱逐恶意节点后保证组内诚实节点能计算出正确的会话密钥, 解决了 Burmester 等人提出协议中存在的内部恶意节点攻击问题. 并证明提出的协议在 DDH 假设下能抵抗敌手的被动攻击, 在 DL 假设和随机预言模型下能够抵抗内部恶意节点发起的密钥协商阻断攻击和密钥控制攻击. 理论分析与实验测试表明, 提出的协议具有较高的通信轮效率和较低的计算开销.

关键词: 组密钥协商; 阻断攻击; 密钥控制攻击; 故障容忍; 随机预言模型
中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2009) 11-2396-07

A Provable Secure Group Key Agreement Protocol with Fault-Tolerant

ZHENG Ming-hui[1,2], ZHOU Hui-hua[1], CUI Guo-hua[1], HAN Lan-sheng[1]
(1. *School of Computer Science, Huazhong University of Science & Technology, Wuhan, Hubei 430074, China;*
2. *School of Information Engineering, Hubei Institute for Nationalities, Enshi, Hubei 445000, China*)

Abstract: This paper indicates that Burmester et al.'s group key agreement protocol which based on the authenticated broadcast channel is unable to withstand the disruption attack and key-control attack of malicious participants in group. These two attacks lead that other honest participants will compute different session key and other honest participants compute the fixed session key which is determined previously by malicious participants, respectively. In this paper, a fault-tolerant group key agreement (FT-GKA) protocol is proposed. Even if there are malicious participants trying to attack the establishment of a session key, all other honest participants following the proposed protocol are still able to compute the correct session key using the digital signature technology. Paper proves the protocol can withstand the passive attack of adversary under the DDH assumption, and the protocol can withstand the interrupted attack and key-control attack from malicious participants under the DL assumption and the random oracle model. Furthermore, the proposed protocol possesses both constant number of rounds and lower computation overhead.

Key words: group key agreement; interrupted attack; key-control attack; fault tolerant; random oracle model

1 引言

组密钥协商协议为参与组播[1]的所有成员建立一个共享会话密钥, 该密钥用来对组成员间传送的消息进行加密、解密和认证等操作, 实现在不可信网络上的安全通信. 组密钥协商协议需要所有的参与成员共同协作才能有效生成会话密钥, 没有一个或部分成员能预先决定或计算出会话密钥[2,3]. 根据是否提供认证功能, 组密钥协商协议可分为非认证的[4,5]和可认证的两大类[6~8].

Burmester 和 Desmedt 在文献[4]中提出了一个著名的非认证组密钥协商协议(简称 BD 协议), 该协议的优点是密钥协商过程只需 2 轮通信. 由于基于认证广播信道, BD 协议可防止被动攻击, 即一个组外敌手通过窃听节点之间传递的消息来计算会话密钥是不可行的, 并能抵抗组外节点的假冒攻击, 该安全结论在 2005 年又被 Burmester 和 Desmedt 进一步形式化地进行了证明[9]. 然而 BD 协议并未考虑内部恶意节点的攻击问题, Pieprayk 和 Wang 提出了一种针对 BD 协议的密钥控制攻击[10], 指出两个位置相邻的内部恶意节点通过广播错误消息, 让组内其它诚实节点毫无觉察地生成它们预先设置好的会话密钥, 以达到控制会话密钥的目的. Katz 和 Yung 也提出了一种类似的攻击方法[11], 但他们均未给出抵抗该类攻击的安全解决方案. 另外, 我们也将提出一种针对 BD 协议的密钥协商阻断攻击[12], 指出一个组内恶意节点通过广播错误消息导致组内其它诚实节点协商出的会话密钥各不相同. Desmedt 等人近期对 Katz 和

收稿日期: 2008-09-28; 修回日期: 2009-07-11
基金项目: 国家自然科学基金(No. 60703048); 湖北教育厅重点项目(No. D20092O3)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

Yung 的工作进行扩展, 利用可验证秘密共享技术提出了一种能抵抗内部恶意节点攻击的组密钥协商协议[13], 但其通信和计算复杂度均正比于组成员数量.

故障容忍是组密钥协商协议的一个重要安全特性[14~16], 其目标是密钥协商过程中即使有少数内部恶意节点发起了攻击, 但组内其它诚实节点能发现攻击, 并在驱逐恶意节点后协商出正确的会话密钥. 在 BD 协议的基础上, 提出了一种故障容忍的组密钥协商(Group Key Agreement with Fault-Tolerant, FT-GKA)协议. FT-GKA 协议在密钥协商过程中加入了消息正确性的认证机制, 该机制能够检测出组内恶意节点, 并在驱逐恶意节点后保证组内诚实节点能计算出正确的会话密钥, 解决了原协议中存在的密钥协商阻断攻击、密钥控制攻击等问题.

2　BD 协议及安全性分析

2.1　BD 协议简介

Burmester 等人提出的 BD 协议是一种非认证的组密钥协商协议, 该协议的详细描述如下.

假设 p、q 分别为大素数, 且满足 $p=2q+1$, G_q 为循环群 Z_p^* 中的一个二次剩余子群, 即 $G_q=\{i^2 \mid i\in Z_p^*\}$, g 为 G_q 的生成元, H 为安全 hash 函数, 符号 $\in_R$ 表示随机选取. 假定 $M=\{M_1, M_2, \cdots, M_n\}$ 表示初始的组成员集, 集合中成员的下标构成一个虚拟的环, 即 M_{n+1} 为 M_1, M_0 为 M_n, 依此类推, 且每个成员知道其它成员在环中的相对位置. 则会话密钥的协商过程为:

Step1　成员 $M_i(1\leqslant i\leqslant n)$ 选择 $r_i\in_R Z_q$, 计算并广播 $y_i=g^{r_i}\bmod p$;

Step2　接收到所有的 $y_j(1\leqslant j\leqslant n, j\neq i)$ 后, 成员 M_i 计算并广播 $z_i=(y_{i+1}/y_{i-1})^{r_i}\bmod p$;

Step3　接收到所有的 $z_j(1\leqslant j\leqslant n, j\neq i)$ 后, 成员 M_i 计算会话密钥:

$$k_i=y_{i-1}^{nr_i}z_i^{n-1}z_{i+1}^{n-2}\cdots z_{i-2}\bmod p=g^{r_1r_2+r_2r_3+\cdots+r_nr_1}\bmod p$$

若记 $k=g^{r_1r_2+r_2r_3+\cdots+r_nr_1}\bmod p$, 则有 $k=k_1=k_2=\cdots=k_n$, 即所有组内成员计算出相同的会话密钥. 从上面的步骤可以看出, 由于每步中的成员都同步操作, 故 BD 协议仅涉及 2 轮通信(Step1 和 Stept2), 具有很高的通信轮效率.

2.2　BD 协议安全性分析

BD 组密钥协商协议本身并不具备认证功能, 其设计基于认证的广播信道, 它满足接收者能够确认每个特定参与者通过该广播信道发送的消息, 每个参与者能识别其它的参与者和它们发送的消息, 但是不能识别参与者发送的消息是否正确. 文献[4, 8]已经指出, 在认证的广播信道模式下, BD 协议能够抵制外部敌手的假冒攻击和被动攻击. 从 BD 协议的 Step3 可以看出, 组成员 M_i 计算出的会话密钥 k 正确与否依赖于其接收到的所有 $z_j(1\leqslant j\leqslant n, j\neq i)$ 是否使用正确的表达式 $z_j=(y_{j+1}/y_{j-1})^{r_j}\bmod p$ 计算得出. 但在协议的 Step2 中, 接收成员 M_i 并不能验证发送成员 M_j 广播的 z_j 是否利用正确的表达式计算得出, 下面对 BD 协议进行深入分析, 指出组内恶意节点可以利用该缺陷在协议的 Step2 中通过广播错误的 z_j 发起密钥控制攻击或密钥协商阻断攻击.

(1)密钥控制攻击

两个合谋的相邻内部恶意节点 M_{j-1}、M_j 能通过下面的方法发起密钥控制攻击, 其目的是让组内诚实节点计算出的会话密钥为它们预先设置好的密钥并毫无觉察, 从而控制密钥协商的结果. 在 BD 协议的 Step2 中, 恶意节点 M_{j-1} 和 M_j 首先相互交换 $z_{j-1}=(y_j/y_{j-2})^{r_{j-1}}$ 和 $z_j=(y_{j+1}/y_{j-1})^{r_j}$ 但不向组内其它节点广播该值, 在收到其它所有节点 $M_i(i\neq j-1, j)$ 广播的 $z_i=(y_{i+1}/y_{i-1})^{r_i}\bmod p$ 后, 计算它们在诚实的情况下进行密钥协商得到的会话密钥 k, 然后再分别广播 $z'_{j-1}=(k'/k)z_{j-1}$ 和 $z'_j=(k/k')z_j$, 其中的 k' 为 M_{j-1} 和 M_j 事先设置好的密钥, z_{j-1} 和 z_j 分别为它们在诚实的情况下应该广播的值. 则组内诚实节点 $M_i(i\neq j-1, j)$ 根据 Step3 计算的会话密钥为:

$$\begin{aligned}k_i&=y_{i-1}^{nr_i}z_i^{n-1}\cdots(z'_{j-1})^{n-j+i}(z'_j)^{n-j+i-1}\cdots z_{i-2}\bmod p\\&=y_{i-1}^{nr_i}\cdots(k'/k)^{n-j+i}z_{j-1}^{n-j+i}(k/k')^{n-j+i-1}z_j^{n-j+i-1}\cdots z_{i-2}\bmod p\\&=(k'/k)y_{i-1}^{nr_i}z_i^{n-1}\cdots z_{j-1}^{n-j+i}z_j^{n-j+i-1}\cdots z_{i-2}\bmod p=k'\end{aligned}$$

即组内诚实节点计算出的会话密钥均为合谋节点 M_{j-1} 和 M_j 事先确定的会话密钥 k', 恶意节点的密钥控制攻击成功.

(2)密钥协商阻断攻击

下面指出一个内部恶意节点 M_j 能通过广播错误消息进行密钥协商阻断攻击. 恶意节点 M_j 在协议的 Step2 中并不使用正确的表达式 $z_j=(y_{j+1}/y_{j-1})^{r_j}\bmod p$ 计算 z_j 的值, 而是随意选取 $z'_j\neq(y_{j+1}/y_{j-1})^{r_j}\bmod p$ 并广播该值, 或另选取 $r'_j\neq r_j$, 计算并广播 $z'_j=(y_{j+1}/y_{j-1})^{r'_j}\bmod p$, 可分析这两种方法实质等价. 组内的其它诚实参与者利用收到的错误 z'_j 根据 Step3 计算会话密钥, 假设 M_d、$M_l(d\neq l)$ 为组内任意两个合法成员, 他们计算的会话密钥分别为:

$$\begin{aligned}k_d&=y_{d-1}^{nr_d}z_d^{n-1}\cdots(z'_j)^{n-j+d-1}\cdots z_{d-2}\bmod p\\&=k(z'_j/z_j)^{n-j+d-1}\bmod p,\\k_l&=y_{l-1}^{nr_l}z_l^{n-1}\cdots(z'_j)^{n-j+l-1}\cdots z_{l-2}\bmod p\\&=k(z'_j/z_j)^{n-j+l-1}\bmod p,\end{aligned}$$

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

其中 k 为 M_j 在诚实的情况下使用 $z_j=(y_{j+1}/y_{j-1})^{r_j}\bmod p$ 得到的正确会话密钥. 比较上面的式子, 由于 $d\neq l$, 则 $k_d\neq k_l$, 即 M_d 与 M_l 计算出不同的会话密钥. 因此每个诚实组成员计算出的会话密钥各不相同, 组内秘密通信被中断.

3 故障容忍的组密钥协商(FT-GKA)协议

3.1 FT-GKA 协议描述

文章对 BD 协议进行改进, 通过增加消息认证功能, 提出了一种 FT-GKA 协议, 该协议不仅保持了 BD 协议在会话密钥协商过程中只需 2 轮通信的优点, 还能够对发起密钥控制攻击、密钥协商阻断攻击的恶意节点进行检测和驱逐, 确保组内诚实节点能计算出正确的会话密钥. FT-GKA 协议详细描述如下:

Step1 每个成员 $M_i(1\leqslant i\leqslant n)$ 选择 $r_i\in_R Z_q$, 计算并广播 $y_i=g^{r_i}\bmod p$;

Step2 接收到所有的 $y_j(1\leqslant j\leqslant n, j\neq i)$ 后, M_i 选择 $s_i\in_R Z_q$, 计算并广播 $(z_i, \eta_i, \mu_i, \omega_i)$, 其中

$$z_i=(y_{i+1}/y_{i-1})^{r_i}\bmod p,$$
$$\eta_i=g^{s_i}\bmod p,$$
$$\mu_i=(y_{i+1}/y_{i-1})^{s_i}\bmod p,$$
$$\omega_i=s_i+r_iH(z_i\|\eta_i\|\mu_i)\bmod q.$$

Step3 接收到所有的 $(z_j, \eta_j, \mu_j, \omega_j)(1\leqslant j\leqslant n, j\neq i)$ 后, M_i 通过验证下列两个式子检测故障:

$$g^{\omega_j}\stackrel{?}{=}\eta_j y_j^{e_j}\bmod p,$$
$$(y_{j+1}/y_{j-1})^{\omega_j}\stackrel{?}{=}\mu_j z_j^{e_j}\bmod p,$$

其中 $e_j=H(z_j\|\eta_j\|\mu_j)$. 如果两式成立, 则表明 M_j 为诚实节点, 否则表明 M_j 为恶意节点.

Step4 如果检测出故障, 即存在内部恶意节点攻击, 则执行下面的恶意节点驱逐过程, 否则直接执行 Step5, 计算会话密钥.

先考虑发生阻断攻击的情况. 一个参与通信的成员 M_j 广播错误的 z_j 发起阻断攻击被检测出来后, 通过以下方法驱逐出通信组: 广播 M_j 为恶意节点后, M_j 相应的值 $y_j=g^{r_j}\bmod p$ 被组内所有成员删除, 由于 M_j 的前一个邻近成员 M_{j-1} 计算的消息 $(z_{j-1}, \eta_{j-1}, \mu_{j-1}, \omega_{j-1})$ 和后一个成员邻近 M_{j+1} 计算的消息 $(z_{j+1}, \eta_{j+1}, \mu_{j+1}, \omega_{j+1})$ 都与恶意节点广播的 $y_j=g^{r_j}\bmod p$ 相关, 故邻近成员 M_{j-1} 和 M_{j+1} 必须分别将上面的两组值分别更新为 $(z'_{j-1}, \eta'_{j-1}, \mu'_{j-1}, \omega'_{j-1})$ 和 $(z'_{j+1}, \eta'_{j+1}, \mu'_{j+1}, \omega'_{j+1})$ 并广播给组内其它成员, 其中

$$z'_{j-1}=(y_{j+1}/y_{j-2})^{r_{j-1}}\bmod p$$
$$\eta'_{j-1}=g^{s_{j-1}}\bmod p$$
$$\mu'_{j-1}=(y_{j+1}/y_{j-2})^{s_{j-1}}\bmod p$$
$$\omega'_{j-1}=s_{j-1}+r_{j-1}H(z'_{j-1}\|\eta'_{j-1}\|\mu'_{j-1})\bmod q$$
$$z'_{j+1}=(y_{j+2}/y_{j-1})^{r_{j+1}}\bmod p$$
$$\eta'_{j+1}=g^{s_{j+1}}\bmod p$$
$$\mu'_{j+1}=(y_{j+2}/y_{j-1})^{s_{j+1}}\bmod p$$
$$\omega'_{j+1}=s_{j+1}+r_{j+1}H(z'_{j+1}\|\eta'_{j+1}\|\mu'_{j+1})\bmod q.$$

然后利用 Step3 中的式子验证这两组更新消息的正确性.

再考虑密钥控制攻击的情况. 如果检测出两个相邻的合谋成员 M_{j-1}、M_j 发起了密钥控制攻击, 其驱逐过程与发生阻断攻击时的方法类似, 只需在 Step2 中将恶意节点的邻近成员 M_{j-2}、M_{j+1} 的广播值分别更新为 $(z'_{j-2}, \eta'_{j-2}, \mu'_{j-2}, \omega'_{j-2})$ 和 $(z'_{j+1}, \eta'_{j+1}, \mu'_{j+1}, \omega'_{j+1})$ 即可, 更新方法同上. 然后利用 Step3 中的式子验证这两组更新消息的正确性.

Step5 假定组内剩下 $m(m\leqslant n)$ 个诚实成员, 则 $M_i(1\leqslant i\leqslant m)$ 计算共享会话密钥:

$$k_i=y_{i-1}^{mr_i}z_i^{m-1}z_{i+1}^{m-2}\cdots z_{i-2}\bmod p=g^{r_1r_2+r_2r_3+\cdots+r_mr_1}\bmod p.$$

3.2 降低协议的计算开销

由于参与通信的所有节点组成一个虚拟的环, 在 Step3 中的进行故障检测时, 为了提高验证的效率, 减少因验证带来的额外计算开销, 每个节点 M_i 可从与自己相邻的下一个节点 M_{i+1} 开始往后验证, 如果存在内部攻击的话, 这样操作可能只需一次验证就能找出内部恶意节点.

另外, 在 Step5 中, 为降低的计算开销, 成员利用下面的方法计算会话密钥: M_i 首先计算

$$h_{i-1}=y_{i-1}^{r_i}\bmod p,\ h_i=h_{i-1}z_i\bmod p,\ h_{i+1}=h_iz_{i+1}\bmod p,\ \cdots,$$

然后再用下列表达式计算会话密钥

$$k_i=h_{i-1}h_ih_{i+1}\cdots h_{i-2}\bmod p=g^{r_1r_2+r_2r_3+\cdots+r_mr_1}\bmod p.$$

这样每个成员在 Step5 中计算会话密钥时只需 1 次幂运算和 $2(m-1)$ 次乘运算.

3.3 故障检测的正确性证明

下面的定理证明了 FT-GKA 协议的故障检测过程是正确的.

定理 1 若成员 M_j 使用正确的表达式计算 z_j, 则 Step3 中两个验证式成立.

证明 在 Step3 中, $(\eta_j, \mu_j, \omega_j)$ 实质上是对 z_j 的一个非交互式的数字签名, 组内其它成员通过验证该签名结果来检测 z_j 是否根据正确的表达式 $z_j=(y_{j+1}/y_{j-1})^{r_j}\bmod p$ 计算得出. 假定成员 M_j 使用表达式计算 z_j, 则有

$$g^{\omega_j}=g^{s_j+r_jH(z_j\|\eta_j\|\mu_j)}\bmod p$$
$$=\eta_j(g^{r_j})^{H(z_j\|\eta_j\|\mu_j)}\bmod p=\eta_jy_j^{e_j}\bmod p$$

另外

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

$$(y_{j+1}/y_{j-1})^{\omega_j}=(y_{j+1}/y_{j-1})^{s_j+r_jH(z_j\|\eta_j\|\mu_j)}\bmod p$$
$$=(y_{j+1}/y_{j-1})^{s_j}(y_{j+1}/y_{j-1})^{r_jH(z_j\|\eta_j\|\mu_j)}\bmod p$$
$$=\mu_j z_j^{e_j}\bmod p$$

4 协议安全性证明

4.1 计算复杂性假设

假设$\mathcal{IG}$是个实例生成器,输入为1^l,l为安全参数,在l的多项式时间内输出一个实例(D_G,g),其中的D_G是关于一个乘法群G的描述,g为群G的q阶生成元,$|q|=l$.

离散对数(DL)假设　如果$(D_G,g)\leftarrow\mathcal{IG}(1^l)$,给定$y\in Z_q^*$,求解唯一整数$r\in Z_q$使之满足$y=g^r \bmod q$称为离散对数问题(DLP),则成功求解DLP在计算上是难的(Intractable),即不存在一个的概率多项式时间算法$\mathcal{A}$满足:

$$\Pr[r\leftarrow\mathcal{A}(D_G,g,y)]>\varepsilon,$$

其中$\varepsilon>0$是一个关于l的可忽略量.

判定 Diffie-Hellman(DDH)假设　如果$(D_G,g)\leftarrow\mathcal{IG}(1^l)$,给定$y_a=g^{r_a}\bmod q$,$y_b=g^{r_b}\bmod q$,$r_a,r_b,\varphi\in_R Z_q$,则$(g,y_a,y_b,g^{r_ar_b})$和$(g,y_a,y_b,\varphi)$是计算不可区分的(Indistinguishable),即不存在一个有效算法$\mathcal{A}$满足:

$$|\Pr[\mathcal{A}(g,y_a,y_b,g^{r_ar_b})=1]-\Pr[\mathcal{A}(g,y_a,y_b,\varphi)=1]|>\varepsilon$$

其中$\varepsilon>0$是一个关于l的可忽略量.

4.2 组外敌手的被动攻击

组密钥协商协议能抵抗被动攻击是指敌手不能通过窃听广播信道上通信节点间传递的消息来推导出会话密钥.在提出的FT-GKA协议中,一个组外敌手通过窃听可以得到信息$(y_i,z_i,\eta_i,\mu_i,\omega_i)$,故只需证明$(g,y_i,z_i,\eta_i,\mu_i,\omega_i,k)$与$(g,y_i,z_i,\eta_i,\mu_i,\omega_i,\varphi)$是计算不可区分的,就可证明提出的协议能抵抗组外敌手的被动攻击,其中$\varphi\in_R G_q$,$k=g^{r_1r_2+r_2r_3+\cdots+r_nr_1}\bmod p$为组成员计算出的会话密钥.

在Step2中,协议使用非交互式的数字签名技术用成员的私钥r_i对消息进行签名,从签名表达式易知,若从信息(η_i,μ_i,ω_i)中推导出成员私钥r_i将面对求解离散对数问题.对满足等式$\log_g\eta_i'=\log_{(y_{i+1}/y_{i-1})}\mu_i'$的$\omega_i'\in Z_q$,$\eta_i'\in G_q\setminus\{1\}$和$\mu_i'\in G_q\setminus\{1\}$,可得到如下的概率:

$$\Pr[\omega_i=\omega_i',\eta_i=\eta_i',\mu_i=\mu_i']=1/(q(q-1)),$$

其中$1\leqslant i\leqslant n$.由于对确定的η_i',μ_i'和ω_i',随机变量(η_i,μ_i,ω_i)也相应确定,因此只需考虑以下两个条件概率即可:

$$\Pr[(g,y_i,z_i,k)\mid\eta_i=\eta_i',\mu_i=\mu_i',\omega_i=\omega_i'],$$
$$\Pr[(g,y_i,z_i,\varphi)\mid\eta_i=\eta_i',\mu_i=\mu_i',\omega_i=\omega_i'],$$

其中$1\leqslant i\leqslant n$.根据上面的分析,可将$(g,y_i,z_i,\eta_i,\mu_i,\omega_i,k)$与$(g,y_i,z_i,\eta_i,\mu_i,\omega_i,\varphi)$计算不可区分的讨论简化为$(g,y_i,z_i,k)$与$(g,y_i,z_i,\varphi)$计算不可区分的讨论.

定理2　在DDH假定下,(g,y_i,z_i,k)与(g,y_i,z_i,φ)计算不可区分,其中k为会话密钥,$\varphi\in_R G_q$,$1\leqslant i\leqslant n$.

证明　一个被动敌手通过窃听可以得到(y_i,z_i),其中$y_i=g^{r_i}\bmod p$,$z_i=(y_{i+1}/y_{i-1})^{r_i}\bmod p$,$1\leqslant i\leqslant n$.在DDH假设下,下面将用反证法来证明$(g,y_i,z_i,k)$和$(g,y_i,z_i,\varphi)$是计算不可区分的,其中$k=y_{i-1}^{nr_i}z_i^{n-1}z_{i+1}^{n-2}\cdots z_{i-2}\bmod p$为会话密钥,$\varphi$为群$G_q$中的随机值.

假设存在一个算法$\mathcal{A}$能有效区分(g,y_i,z_i,k)和(g,y_i,z_i,φ),其中$1\leqslant i\leqslant n$,则能利用该算法$\mathcal{A}$构造另一个算法$\mathcal{A}'$有效区分$(g,y_a,y_b,g^{r_ar_b})$和(g,y_a,y_b,φ),从而推翻DDH假定,其中$y_a=g^{r_a}\bmod p$,$y_b=g^{r_b}\bmod p$,$r_a,r_b\in Z_q^*$.下面构造算法$\mathcal{A}'$:(y_a,y_b,φ)为算法$\mathcal{A}'$的输入,首先令$y_1=y_a$,$y_n=y_b$,随机选择$t_2,t_3,\cdots,t_{n-1}\in Z_q$,并计算:

$$y_2=g^{t_2}\bmod p,$$
$$y_3=g^{t_3}\bmod p,$$
$$y_{n-1}=g^{t_{n-1}}\bmod p.$$

然后计算:$z_i=(y_{i+1}/y_{i-1})^{t_i}\bmod p$,$2\leqslant i\leqslant n-1$.

由于$z_1=(y_2/y_n)^{r_a}\bmod p=g^{t_2r_a}/y_b^{r_a}\bmod p=y_a^{t_2}/g^{r_ar_b}\bmod p$,$z_n=(y_1/y_{n-1})^{r_b}\bmod p=y_1^{r_b}/y_{n-1}^{r_b}\bmod p=g^{r_ar_b}/g^{t_{n-1}r_b}\bmod p=g^{r_ar_b}/y_{\beta}^{t_{\beta-1}}\bmod p$,用"测试"值$\varphi$代替其中的$g^{r_ar_b}$,可得到:

$$z_1=y_a^{t_2}/\varphi\bmod p\text{ 和 }z_2=\varphi/y_{\beta}^{t_{\beta-1}}\bmod p.$$

这样,算法$\mathcal{A}'$根据上面的过程构造出了所有的(y_i,z_i),$1\leqslant i\leqslant n$,并计算$\varphi y_a^{(n-1)t_2}\prod_{j=2}^{n-1}z_j^{n-j}\bmod p$,然后$\mathcal{A}'$用这些值调用算法$\mathcal{A}$.由于算法$\mathcal{A}$能有效区分$(g,y_i,z_i,k)$和$(g,y_i,z_i,\varphi)$,因此,如果$k=\varphi y_a^{(n-1)t_2}\prod_{j=2}^{n-1}z_j^{n-j}\bmod p$成立,则有$g^{r_ar_b}\bmod p=\varphi$,即算法$\mathcal{A}'$能够利用算法$\mathcal{A}$有效区分$(g,y_a,y_b,g^{r_ar_b})$和$(g,y_a,y_b,\varphi)$,该结论与DDH假设矛盾.故定理2成立.

4.3 组内恶意节点的阻断攻击和密钥控制攻击

根据前面的分析可知,在BD协议中,内部恶意节点通过广播错误的z_j发动阻断攻击或密钥控制攻击.*FT-GKA*协议使用签名技术来防止恶意节点发动攻击,但是,如果恶意节点能够选取一个错误的z_j并能伪造出相应的签名消息$(z_j,\eta_j,\mu_j,\omega_j)$,使之能通过Step3中的两个验证式,则说明FT-GKA协议不能检测出恶意节点,达不到抵抗上述两种攻击的目的.反之,如果能证明FT-GKA协议对z_j的签名抗存在性伪造,则表明提出的恶意节点检测方法是可行的.

对FT-GKA协议抗存在性伪造攻击的证明可以使用

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

基于随机预言(Random Oracle,RO)模型的归约技术给出,该证明由"归约为矛盾"得到:一个成功的伪造将导致离散对数问题可解.文献[17]提出了一个分叉引理并利用该引理证明了 Schnorr 签名方案抗存在性伪造攻击.

引理 1 假设$\mathcal{M}$是一个概率多项式图灵机,以给定的公开数据作为输入,如果$\mathcal{M}$能以不可忽略的概率得到一个有效的签名(m,σ_1,h,σ_2),则以相同的随机数和不同的预言重放图灵机,$\mathcal{M}$将以不可忽略的概率得到另一个有效的签名$(m,\sigma_1,h',\sigma_2')$,其中 $h\neq h'$.

对照 Schnorr 签名方案,提出协议中的 z_j 相当于签名消息 m,(η_j,μ_j)相当于 σ_1,e_j 相当于 h,ω_j 相当于 σ_2.下面的定理将表明,一个不使用私钥 r_j 计算 z_j 的恶意节点,不能生成有效的签名消息$(z_j,\eta_j,\mu_j,\omega_j)$.

定理 3 在 RO 模型和 DL 假定下,不使用私钥 r_j 的恶意节点 M_j 不能生成有效的签名$(z_j,\eta_j,\mu_j,\omega_j)$,因此 FT-GKA 协议抗存在性伪造.

证明 假设恶意节点 M_j 在不使用秘密 r_j 的情况下,能以不可忽略的概率 ε 生成y_{j+1}/y_{j-1}的有效签名.那么在 *RO* 模型下,根据引理 1 可知恶意节点 M_j 对 Step2 中的消息(y_{j+1},y_{j-1},s_j)能以至少 $\varepsilon/2$ 的概率生成两个有效的签名$(z_j,\eta_j,\mu_j,\omega_j)$和$(z_j,\eta_j,\mu_j,\omega_j')$,使之分别满足 Step3 中的两个验证式:

$$g^{\omega_j}=\eta_j y_j^{e_j}\bmod p,(y_{j+1}/y_{j-1})^{\omega_j}=\mu_j z_j^{e_j}\bmod p \text{ 及}$$

$$g^{\omega_j'}=\eta_j y_j^{e_j'}\bmod p,(y_{j+1}y_{j-1})^{\omega_j'}=\mu_j z_j^{e_j'}\bmod p,$$

其中的 e_j 和 e_j' 是在 RO 模型下的两个不同的哈希值.恶意节点 M_j 根据上面的验证式可以得到:

$$r_j=\log_g y_j=\log_{(y_{j+1}/y_{j-1})}z_j=\frac{e_j-e_j'}{\omega_j-w_j'}$$

即离散对数问题被恶意节点求解.该结论与 DL 假定矛盾,故假设不成立.由于节点 M_j 只有在利用秘密 r_j 正确计算 $z_j=(y_{j+1}/y_{j-1})^{r_j}$的情况下,才能得到有效的签名消息$(z_j,\eta_j,\mu_j,\omega_j)$,故 FT-GKA 协议抗签名的存在性伪造.

根据定理 3 可知,当某个内部恶意节点广播错误的 z_j 发起阻断攻击时,由于不能伪造其有效签名,将在 Step3 中被组内诚实节点检测出来,故下面的定理 4 成立.

定理 4 FT-GKA 协商协议能抵抗内部恶意节点的密钥协商阻断攻击.

同理,根据定理 3 可知下面的定理 5 亦成立.

定理 5 FT-GKA 协议能抵抗内部恶意节点的密钥控制攻击.

5 性能分析与比较

5.1 理论分析

设计一个组密钥协商协议时,需考虑其通信轮数、通信开销和计算开销.通信轮数用所有参与成员异步发送消息的次数来度量;通信开销用每个参与成员发送的消息总长度来度量;计算开销用每个参与成员进行的幂运算、逆运算、乘运算和哈希运算的次数来度量.下面分析 FT-GKA 协议在这三方面的性能,并与 BD 等协议进行比较.

在没有内部恶意节点攻击时,FT-GKA 协议与 BD 协议一样仅需 2 轮通信.当有恶意节点攻击时,检测出恶意节点的成员需额外增加 1 轮通信用来广播恶意节点的身份,另外,在驱逐恶意节点时,恶意节点前后两个邻近成员也需额外增加 1 轮通信用来广播更新后的消息,故通信轮数增加到 4 轮.

若用$|X|$表示消息 X 的比特位数,在 FT-GKA 协议中,每个成员在 Step1 和 Step2 中分别广播 y_j 和$(z_i,\eta_i,\mu_i,\omega_i)$,它们的总长度为$4|p|+|q|$.当有恶意节点攻击时,由于更新消息导致恶意节点前后两个邻近成员广播的消息总长度增加到$7|p|+2|q|$.

每个成员在 Step1 中需 1 次幂运算;在 Step2 中需 3 次幂运算、1 次求逆运算、1 次乘运算和 1 次哈希运算;在故障检测的 Step3 中,每个成员在最好情况下仅需 4 次幂运算和 1 次求逆运算,而在最差情况下却需 $4(n-1)$次幂运算和 $n-1$ 次求逆运算;如果存在恶意节点攻击,恶意节点前后两个邻近成员在 Step4 中额外增加的计算开销与 Step2 中的相同;在 Step5 中,每个成员计算会话密钥只需 1 次幂运算和 $2(m-1)$次乘运算.由于幂运算和逆运算的耗时远远大于乘运算和哈希运算,故只考虑前面的两种运算,而 1 次逆运算的耗时几乎等价于 1 次幂运算,故 FT-GKA 协议中每个成员的幂运算开销为 $O(n)$.

表 1 列出了 BD 协议、KY 协议(Katz 和 Yung 的协议[11])、DPSW 协议(Desmedt 和 Pieprzyk 等人的协议[13])与提出的 FT-GKA 协议的性能比较.假设 KY 协议与 DPSW 协议均使用 RSA 公钥密码体制[18],t 为可验证秘密共享技术中的门限值.通过表 1 可以看出,FT-GKA 协议具有较优的通信轮效率和通信开销,且具有故障容忍功能.

表 1 协议性能比较

	BD 协议	KY 协议	DPSW 协议	FT-GKA 协议	
				无攻击	有攻击
故障容忍	No	No	Yes	Yes	Yes
通信轮数	2	3	7	2	4
成员通信开销	$2\|p\|$	$2\|q\|+5\|p\|$	$(3tn+5)\|p\|$	$4\|p\|+\|q\|$	$7\|p\|+2\|q\|$
成员幂运算开销	$O(n)$	$O(n)$	$O(n)$	$O(n)$	

5.2 实验测试

本小节将通过实验对 BD 协议、DPSW 协议和提出的 FT-GKA 协议进行性能测试与比较,测试目标为组密钥协商时延和 FT-GKA 协议的故障容忍能力.组密钥协商时延是指从启动协议到在所有的成员间成功协商出一

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

个共享的会话密钥所花费的平均时间. 下面先介绍支持测试所需的组通信系统、密码算法库、测试床和相关的测试参数.

(1) 组通信系统

实验测试首先需要一个支持组通信的平台——组通信系统(Group communication systems, GCS). 目前, 常用的组通信系统有 Spread 系统[19]、TOTEM 系统[20] 等. 我们选择源代码开放的 Spread 系统为测试工作提供组通信服务. 关于 Spread 的详细介绍可参见文献[19] 和"Spread 使用手册[21]".

(2) 密码算法库

为了确保各协议的实验结果具有更好的可比性, 在实现组密钥协商协议时, 尽量让参与测试的组密钥协商协议具有较多的共性, 如相同的数据结构, 相同的密码算法等. 我们采用了 OpenSSL 密码算法库中的分组密码算法 DES、数字签名算法 RSA、哈希函数 SHA-1.

(3) 测试床与测试参数

在局域网(LAN) 环境中对组密钥协商协议进行性能的测试. 实验测试床为 6 台运行 Windows XP 系统的 PC 机, 每台 PC 的 CPU 主频为 1.5GHz、RAM 为 512MB, 每台 PC 上都安装一个组通信系统 Spread, 通过修改 Spread 的配置可以实现将组成员平均分布到 6 台 PC 上, 其具体配置方法见文献[21].

使用的 DH 参数为 p = 1024- bit 和 q = 160- bit. 在组建的测试系统中, 一次模幂运算的时延为 5.9mm (Msec). 使用 1024- bit、公开指数为 3 的 RSA 数字签名方案对 BD 协议的消息源和数据进行认证, 其签名和验证过程的时延分别为 4.9mm 和 0.3mm. 使用分组长度为 500- byte 的 DES 加密算法, 时延为 0.1mm. 测试结果还表明, 当组成员数量从 6 开始以 3 为步长逐渐增加到 300 时, 发送一个组播消息的时延从 0.7ms 逐渐增加到 0.93mm; 每个组成员广播一个消息并接收到其它剩下组成员发送的 n- 1 个消息的时延(即一轮消息的时延) 为从 4mm 逐渐上升到 31mm.

(4) 实验结果与分析

在测试过程中, 对 FT-GKA 协议在组规模 n = 72, 132, 216 和 276 时加入内部恶意节点攻击(即组密钥协商阻断攻击和密钥控制攻击), 对其故障容忍功能进行测试, 实验结果如图 1 所示. 从实验结果可以看出, 由于 FT-GKA 协议在 Step2 中增加了签名计算, 故比 BD 协议在整体上具有更大的时延. 尤其在存在恶意节点攻击时, 对恶意节点的检测和驱逐导致了更大的时延. 但与另一个具有故障容忍功能的 DPSW 协议相比, 提出的协议具有较低的密钥协商时延.

测试还考虑了对 FT-GKA 协议的连续攻击, 如图 2 所示. 当组规模分别为 n= 60, 36 时, 各进行了 100 次的组密钥协商时延测试. 在第 20~ 40 次测试之间, 连续增加密钥控制攻击; 在第 60~ 80 次测试之间, 连续同时增加密钥控制攻击和密钥协商阻断攻击. 图中的实验结果表明, 在攻击发生后, 组成员都能协商出正确的会话密钥, 即协议具备故障容忍功能, 但导致了组成员密钥协商时延的增加.

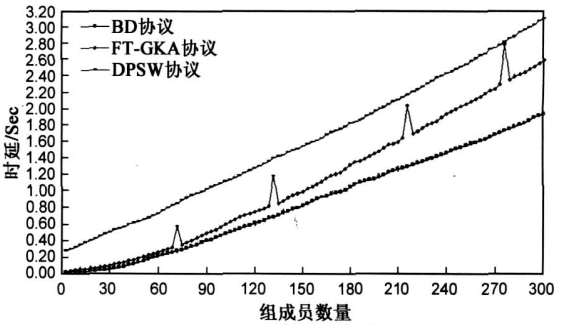

图1　组密钥协商时延开销比较

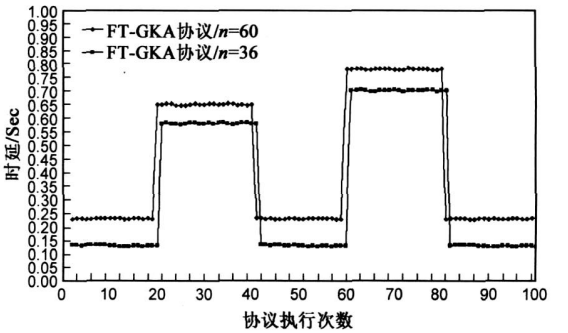

图2　FT-GKA协议在不同组规模下的时延

6　结束语

本文分析指出, 在 Burmester 等人提出的 BD 组密钥管理协议中, 组内恶意节点可以通过广播错误消息发起密钥协商阻断攻击和密钥控制攻击. 为解决内部恶意节点的攻击问题, 提出了一种故障容忍的 FT-GKA 协议, 该协议不仅保持了通信轮效率较高的优点, 还提供了消息正确性认证机制, 能正确检测出发起攻击的恶意节点, 并在驱逐恶意节点后保障组内诚实节点能计算出正确的会话密钥. 并证明了 FT-GKA 协议在 DDH 假设下能抵抗敌手的被动攻击, 在 DL 假设和随机预言模型下能够抵抗内部恶意节点发起的密钥协商阻断攻击和密钥控制攻击.

参考文献:

[1] Quinn B, Almeroth K. IP Multicast Applications: Challenges and Solutions[S]. IEFT RFC3170, 2001.

[2] Challal Y, Seba H. Group key management protocols: a novel taxonomy[J]. International Journal of Information Technology, 2006, 2(2): 105- 118.

[3] Sandro R, David H. A survey of key management for secure

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

group communication[J]. ACM Computing Surveys. 2003, 35(3): 309- 329.
[4] Burmester M, Desmedt Y. A secure and efficient conference key distribution system [A]. Eurocrypt' 94 [C]. Berlin: Springer-Verlag, 1994. 275- 286.
[5] Horng G. An efficient and secure protocol for multi- party key establishment[J]. Computer Journal, 2001, 44: 463- 470.
[6] Ateniese G, Steiner M, Tsudik G. New multiparty authentication services and key agreement protocols[J]. IEEE Journal Sel Area Comm, 2000, 18: 628- 639.
[7] Boyd C, Nieto G. Round-optimal contributory conference key agreement[A]. In Proc Public-Key Cryptography' 03[C]. Berlin: Springer-Verlag, 2003. 161- 174.
[8] Zheng M H, Zhou H H, Li J et al. Efficient and provably security password-based group key agreement protocol[J]. Computer Standards & Interfaces, 2009, 31(5): 948- 953.
[9] Burmester M, Desmedt Y. A secure and scalable group key exchange system[J]. Information Processing Letters, 2005, 94: 137- 143.
[10] Pieprayk J, Wang H. Key control in multi-party key agreement protocols[A]. In workshop on Coding, Cryptography and Combinatories(CCS' 03)[C]. Berlin: Springer-Verlag. 2003. 86- 105.
[11] Katz J, Yung M. Scalable protocols for authenticated group key exchange[A]. In CRYPTO' 03[C]. Berlin: Spring-Verlag. 2003, 110- 125.
[12] 郑明辉, 崔国华, 祝建华. 一种抗阻断攻击的多方密钥协商协议[J]. 电子学报, 2008, 36(7): 1368- 1372.
Zheng Ming-hui, Cui Guo-hua, Zhu Jian-hua. A multi-party key agreement protocol withstands interrupted attack[J]. Acta Electronica Sinica, 2004, 32(4): 635- 638. (in Chinese)
[13] Desmedt Y, Pieprzyk J, Steinfeld R, Wang H. A non-malleable group key exchange protocol robust against active insiders [A]. ISC' 06[C]. Berlin: Springer-Verlag, 2006. 459- 475.
[14] Tseng W G. A secure fault- tolerant conference-key agreement protocol[J]. IEEE Transactions on Computers, 2002, 51(4): 373- 379.
[15] Tseng Y M. A communication-efficient and fault- tolerant conference-key agreement protocol with forward secrecy[J]. Journal of Systems and Software, 2007, 80: 1091- 1101.
[16] Tang Q, Mitchell C J. Security properties of two authenticated conference key agreement protocols[A]. In the 7th Conference of Information and Communications Security [C]. Berlin: Springer-Verlag, 2005. 304- 314.
[17] Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols[A]. ACM CCS' 93 [C]. New York: ACM Press, 1993. 62- 73.
[18] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack[A]. Advances in Cryptology-CRYPTO' 98[C]. Berlin: Springer-Verlag, 1998. 13- 25.
[19] Amir Y, Nita-Rotaru C, Stanton J. Secure spread: an integrated architecture for secure group communication[J]. IEEE Transactions on Dependable and Secure Computing, 2005, 2(3): 248- 261.
[20] Moser L, Melliar-Smith P, Agarwal D et al. Totem: a fault-tolerant multicast group communication system[J]. Communications of the ACM, 1996, 39(4): 54- 63.
[21] Stanton J. A users guide to Spread: Version 0. 11[EB/OL]. November 2002. http: // www. spread. org/ docspread. html.

作者简介:

郑明辉 男, 1972 年生于湖北嘉鱼, 博士, 副教授, 主要研究方向为现代密码学、网络安全等.
E-mail: mhzheng@ smail. hust. edu. cn

周慧华 女, 1973 年生于湖北鹤峰, 博士研究生, 副教授. 主要研究方向为密码理论与技术、信息隐藏等.

崔国华 男, 1947 年生于湖北武汉, 博士生导师, 教授, 主要研究方向为现代密码学、网络安全及算法分析等. 通信作者
E-mail: cuil9@sina. com

韩兰胜 男, 1969 年生于湖北武汉, 博士, 副教授, 主要研究方向为公钥密码、网络安全等.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net