一种抗阻断攻击的认证组密钥协商协议*)

崔国华 郑明辉 粟 栗

(华中科技大学计算机科学与技术学院 武汉 430074)

摘 要 一个非认证的组密钥协商协议不能对通信参与者和消息进行认证,它必须依赖认证的网络信道或其它的认证方法。分析了 Burmester 等人在认证广播信道下提出的著名组密钥协商协议,指出它不能抵抗内部恶意节点发起的密钥协商阻断攻击,该攻击导致组内其它诚实节点不能正确计算出一致的组密钥。提出了一种改进的认证的组密钥协商协议,在原协议中加入了消息正确性的认证方法,能够对组内恶意节点进行检测,并在随机预言模型下证明了改进的协议能够抵抗密钥协商阻断攻击。

关键词 密钥管理,组密钥协商,离散对数问题,阻断攻击

An Authenticated Group Key Management Protocol Withstand Interrupted Attack

CUI Guo-Hua ZHENG Ming-Hui SU Li

(School of Computer Science, Huazhong University of Science & Technology, Wuhan 430074)

Abstract A non-authenticated group key agreement protocol cannot provide participant and message authentication, thus it must depend on an authenticated network channel or use another scheme to provide authentication. 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 of malicious participants in group. This attack leads that other honest participants will not be able to correctly agree on a group key consistently. In this paper, an improved protocol is proposed. The proposed protocol which joins the message authentication method in original protocol can detect the malicious participant. Under the random oracle model, paper proves the improved protocol can withstand the interrupted attack from malicious participant.

Keywords Key management, Group key agreement, Discrete logarithm problem, Interrupted attack

组播是基于 UDP/IP 协议、面向多接收者的数据传送方式,其重要性随着 Internet 的发展日益突出,在视频会议、网络游戏、远程协作、安全数据复制等面向组的通信领域有着广泛的应用。组密钥管理为参与组播的成员生成、分发和更新组密钥。组密钥是所有参与通信的组成员的共享密钥,该密钥被用来对组成员间传送的组播报文进行加密、解密和认证等操作,以满足组播的基本安全需求。

现有的组密钥管理协议可分为两类[1,2]:组密钥分配协议和组密钥协商协议。组密钥分配协议需要一个中心节点负责生成、分发和更新组密钥,而组密钥协商协议则需要所有的参与成员共同合作生成和更新组密钥。根据是否提供认证功能,又将组密钥协商协议分为非认证的[3,4]和认证的两类[5,6]。一个非认证的组密钥协商协议不能提供对通信参与者及消息的认证功能,它必须依赖认证的网络信道,或使用其它方法为协议提供认证功能。Burmester 和 Desmedt(简称 BD)在文[3]中根据不同的网络环境提出了几个不同的组密钥协商协议,其中的协议 3(简称 BD_3)是一个基于认证广播信道的非认证组密钥协商协议,该协议的优点是密钥协商过程只需 2 轮通信,每个参与方广播的消息数量为常量。由于广播信道是认证的,BD_3 协议可抵抗外部节点的假冒攻击,并能防止被动攻击,即一个敌手通过窃听参与者之间传递的消息来计算组密钥是不可行的。然而,文章分析指出:在 BD_3 协议中,一个组内恶意节点能够通过发送错误消息发起密钥协商阻断攻击,该攻击导致组内其它诚实节点不能够正确协商出组密钥,不能实现组通信的机密性;同时,组内诚实节点也不能确定发起阻断攻击的恶意节点身份。尽管文[3]中的协议 7 使用一种连续证明方法为协议 3 提供了认证功能,但消息传递的轮数正比于参与者的数量,且仅仅只能认证消息是否为参与者发送,并不能认证参与者发送的消息是否正确,即组内其它参与者是否能用该消息计算出正确的组密钥,因此协议 7 没能处理密钥协商阻断攻击问题。为了优化协议 7 中通信的轮效率,文[5,6]提出了相应的认证组密钥协商协议,但也没有考虑组内恶意节点进行密钥协商阻断攻击问题。

本文提出一种改进的 BD_3 组密钥协商协议,该协议在不改变原协议轮效率的前提下,加入了对消息正确性进行认证的机制,该机制利用数字签名技术能够检测出组内恶意节点,并在驱逐恶意节点后重启组密钥协商,解决了原协议中存在的密钥协商阻断攻击问题。

1 BD_3 协议及安全性分析

1.1 BD_3 协议简介

Burmester 等人提出的 BD_3 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。同原协议一样,文章也没有考虑成员动态事件。

*)国家自然科学基金资助,项目编号 60403027;湖北省教育厅优秀中青年基金资助,项目编号 Q200629001。**崔国华** 博士生导师,教授,研究方向:现代密码学、网络安全及算法分析等;**郑明辉** 博士生,研究方向:现代密码学、网络安全等;**粟 栗** 博士生,研究方向:公钥密码、网络安全等。

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。假定 $M=\{M_1,M_2,\cdots,M_n\}$ 表示初始的组成员集，且集合中成员的下标构成一个环，即 M_{n+1} 为 M_1，M_0 为 M_n，依此类推，则组密钥协商步骤为：

Step1. 成员 $M_i(1\leqslant i\leqslant n)$ 选择一个随机数 $r_i\in Z_q$，计算并广播 $y_i=g^{r_i} \bmod q$；

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 计算组密钥：

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

从上面的步骤可以看出，BD_3 协议仅涉及 2 轮通信（Step1 和 Stept2），故轮效率很高。

1.2 BD_3 协议安全性分析

一个没有认证能力的密钥协商协议不能提供通信参与者及消息的认证，它必须依赖已认证的网络信道或使用其它的方法提供认证能力。BD_3 组密钥协商协议在设计过程中使用了认证的广播信道，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，这样，每个参与者能识别其他的参与者和他们发送的消息。文[3]已经指出，在此认证的广播信道模式下，BD_3 协议能够抵制假冒攻击和被动攻击。下面，文章将对 BD_3 组密钥协商协议进行深入分析，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。

从 BD_3 协议的 Step3 可以看出，组成员 M_i 计算出的组密钥 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。假定有一个恶意的内部节点 M_i 试图阻断组内的密钥协商。该恶意节点 M_i 在协议的 Step2 中，并不使用正确的表达式 $z_i=(y_{i+1}/y_{i-1})^{r_i} \bmod p$ 计算 z_i 的值，而是随意选取 $z_i=S\neq(y_{i+1}/y_{i-1})^{r_i} \bmod p$ 并广播该值，或不使用自己的秘密 r_i，另选取 $r'_i\neq r_i$，计算并广播 $z_i=(y_{i+1}/y_{i-1})^{r'_i} \bmod p$，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_i 计算组密钥 k，但发现不能用该组密钥 k 与组内其它成员通信，因为每个诚实组成员计算出的组密钥 k 不同。显而易见，尽管该协议基于一个认证的广播信道，但在密钥协商阻断攻击发生后，其它成员并不能确定谁是发起攻击的内部恶意节点。因此可得如下结论：BD_3 协议不能检测内部恶意节点，不能抵抗恶意节点发起的密钥协商阻断攻击。

2 认证的组密钥协商协议

文章对 BD_3 协议进行改进，提出了一种具有认证功能的组密钥协商协议，该协议同样基于认证的广播信道。提出的协议不仅保持了 BD_3 协议在组密钥协商过程中只需 2 轮通信的优点，还提供了消息正确性的验证机制，能够对发起密钥协商阻断攻击的恶意节点进行检测。改进的协议包括组密钥协商、恶意节点检测、恶意节点驱逐与组密钥协商重启等三个阶段：

(1)组密钥协商阶段

Step1. 每一个成员 $M_i(1\leqslant i\leqslant n)$ 选择一个随机数 $r_i\in Z_q$，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 选择一个随机数 $s_i\in Z_p$，计算并广播 $(z_i,\eta_i,\mu_i,\omega_i)$，其中

$$z_i=(y_{i+1}/y_{i-1})^{r_i} \bmod p$$

$$\eta_i=g^{s_i} \bmod p$$

$$\mu_i=(y_{i+1}/y_{i-1})^{s_i} \bmod p$$

$$\omega_i=s_i+r_iH(z_i\parallel\eta_i\parallel\mu_i) \bmod q。$$

Step3. 接收到所有的 $(z_j,\eta_j,\mu_j,\omega_j)(1\leqslant j\leqslant n, j\neq i)$ 后，成员 M_i 计算组密钥：

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

如果 M_i 能够用计算出的组密钥 k 加密和解密会话消息，则表明没有内部恶意节点发起密钥协商阻断攻击，密钥协商过程完成。否则表明有恶意节点阻断了本次组密钥的协商，需继续执行下面的恶意节点检测操作，找出发起阻断攻击的恶意节点。

(2)恶意节点检测阶段

成员 M_i 在组密钥协商失败后，通过验证下列两个等式是否成立找出发起密钥协商阻断攻击的内部恶意节点：

$$g^{\omega_j}=\eta_jy_j^e \bmod p,$$

$$(y_{j+1}/y_{j-1})^{\omega_j}=\mu_jz_j^e \bmod p$$

其中 $e=H(z_j\parallel\eta_j\parallel\mu_j)$。如果上面的两式成立，则表明 M_j 为诚实节点，否则表明 M_j 为发起密钥协商阻断攻击的恶意节点。

如果每个节点对另外 $n-1$ 个节点在组密钥协商阶段的 Step2 中发送的消息都进行验证操作，其计算开销将会很大。另外，由于出现密钥协商阻断攻击的概率较小，在没有发生阻断攻击的情况下，执行恶意节点检测操作也没有必要，它只会让参与者付出额外的计算开销。因此在改进的协议中，可先进行组密钥协商，如果协商成功，则协议终止；否则进一步执行协议的第二阶段，即只有在阻断攻击发生时才执行恶意节点检测操作，这样处理可以降低每个参与节点的计算开销。

下面证明当成员 M_j 使用正确的表达式计算 z_j 时，上述两个等式成立。

证明：在组密钥协商阶段的 Step2 中，(η_j,μ_j,ω_j) 实质上是对 z_j 的一个特殊签名，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

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

另外

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

□

(3)恶意节点驱逐与组密钥协商重启阶段

一个参与通信的成员 M_j 试图发送一个错误的 z_j 阻断密钥协商被认为是恶意节点，该恶意节点被检测出来了以后，被从通信组中驱逐并重新进行组密钥协商。驱逐恶意节点及重新进行组密钥协商的过程如下：在广播成员 M_j 为恶意节点后，M_j 相应的广播值 $y_j=g^{r_j} \bmod p$ 也被组内所有成员删除，由于恶意节点 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 $z'_{j-1}=(y_{j+1}/y_{j-2})^{r_{j-1}} \bmod p$，

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

组内成员接收到更新的数据后检测其正确性。如果收到的数据检测为正确数据，则回到协议第一阶段的 Step3 计算新的组密钥。假定组内剩下 $m(m<n)$ 个诚实成员，则成员 $M_i(1\leqslant i\leqslant m)$ 计算的组密钥为 $k=y_i^{mr_i}z_i^{m-1}z_{i+1}^{m-2}\cdots z_{i-2} \bmod p=g^{r_1r_2+r_2r_3+\cdots+r_mr_1} \bmod p$。

3 协议的安全性分析

基于离散对数问题(Discrete Logarithm Problem, DLP)，本节先分析改进的认证组密钥协商协议能够抵抗组外敌手的被动攻击。然后在随机预言模型(Random Oracle, RO)[8]下，证明协议能抵抗组内恶意节点发起的密钥协商阻断攻击。

(1)组外敌手的被动攻击

定理 1 组外敌手推导组密钥的困难性等价于求离散对数问题。

证明：考虑组外被动敌手 $\mathcal{A}$ 企图通过窃听组内成员的广播消息来推导组密钥的情形。

从计算组密钥 k 的表达式可知，计算 k 必须要知道组成员 M_i 随$(1\leqslant i\leqslant n)$机选择的秘密 r_i。一个敌手 $\mathcal{A}$ 通过窃听可获取组成员 M_i 发送的消息$(y_i,z_i,\eta_i,\mu_i,\omega_i)$，并试图通过获取的这些消息推导 M_i 的秘密 r_i。敌手如果根据表达式 $y_i=g^{r_i} \bmod p$ 推导 r_i，则要面对求离散对数问题。由于 $z_i=(y_{i+1}/y_{i-1})^{r_i} \bmod p=g^{(r_{i+1}-r_{i-1})r_i}$，如果敌手企图利用该表达式推导 r_i，同样要面对求离散对数问题。最后，敌手如果利用表达式 $\omega_i=s_i+r_iH(z_i\|\eta_i\|\mu_i) \bmod q$ 推导 r_i，则必须求出 M_i 的另一个秘密 s_i，而由 $\eta_i=g^{s_i} \bmod p$ 可知，求 s_i 同样要面对求离散对数问题。故一个被动敌手通过窃听的消息不能获取组成员的秘密而计算出组密钥 k。□

(2)组内恶意参与方的阻断攻击

在提出的协议中，如果恶意节点选取错误的 z_j 并能伪造出一个相应的签名消息$(z_j,\eta_j,\mu_j,\omega_j)$，使之能通过恶意节点检测阶段的两个验证式，则表明改进的协议不能检测恶出意节点，达不到抵抗密钥协商阻断攻击的目的。反之，如果能证明改进协议对 z_j 的签名抗存在性伪造，则表明恶意节点的检测方法是安全可行的。

对改进协议抗存在性伪造攻击的证明可以使用基于随机预言(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[8]提出了一个分叉引理并利用该引理证明了 Schnorr 签名方案[9]抗存在性伪造攻击。该引理使用“预言重放攻击”，即以相同的随机数和不同的预言在多项式时间内重放攻击，将得到关于某一形式的两个有效签名，从而解决公认的困难性问题。

引理 1(分叉引理) 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，改进协议中 z_j 的相当于签名消息 m，(η_j,μ_j)相当于 σ_1，e 相当于 h，ω_j 相当于 σ_2。下面的定理将表明，一个不使用秘密 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 2 在 RO 模型和 DLP 假定下，不使用秘密 r_j 的任意恶意节点 $\mathcal{A}$ 不能生成有效的签名$(z_j,\eta_j,\mu_j,\omega_j)$，因此改进的认证密钥协商协议抗存在性伪造。

证明：用反证法证明该定理。假设恶意节点 $\mathcal{A}$ 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。在 RO 模型下，根据分叉引理可知恶意节点 $\mathcal{A}$ 对 Step2 中特定的信息(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$(z_j,\eta_j,\mu_j,\omega'_j)$，使之分别满足恶意节点检测阶段中的两个验证式：

$g^{\omega_j}=\eta_jy_j^e \bmod p, (y_{j+1}/y_{j-1})^{\omega_j}=\mu_jz_j^e \bmod p$ 及

$g^{\omega'_j}=\eta_jy_j^{e'} \bmod p, (y_{j+1}/y_{i-1})^{\omega'_j}=\mu_jz_j^{e'} \bmod p$，

其中的 e 和 e' 是在 RO 模型下的两个不同的哈希值。恶意节点 $\mathcal{A}$ 根据上面的验证式可以得到：$r_j=\log_g y_j=\log_{(y_{j+1}/y_{j-1})}z_j=(e-e')/(\omega_j-\omega'_j)$，即离散对数被恶意节点求出。该结论与 DLP 假定矛盾，故假设不成立。因此，只有使用秘密 r_j 才能得出有效的签名消息$(z_j,\eta_j,\mu_j,\omega_j)$，提出的改进协议抗存在性伪造。□

由于定理 2 可知，当恶意节点发送错误的 z_j 企图阻断组内诚实节点之间的密钥协商时，并不能伪造其有效的签名，将在恶意节点检测阶段被检测出来，故下面的定理 3 成立。

定理 3 改进的认证组密钥协商协议抗内部恶意节点的密钥协商阻断攻击。

结束语 密钥管理是安全组播得以广泛应用的关键技术之一。本文通过分析指出，Burmester 等人提出的基于认证广播信道的 BD_3 组密钥管理协议中，组内恶意节点可以通过发送错误消息进行密钥协商阻断攻击，该攻击将导致组内诚实节点不能计算出一致的组密钥，通信的机密性被破坏。为了克服此安全缺陷，提出了一种改进的认证组密钥协商协议，改进协议不仅保持了原协议仅需 2 轮通信的优点，另外还提供了消息认证机制，该机制能正确检测出发起攻击的恶意节点，并在随机预言模型下证明了改进的协议能够抵抗内部恶意节点发起的密钥协商阻断攻击。由于改进的协议首先进行组密钥协商，如果协商成功即终止协议，只有在发现协商失败时才执行消息认证、恶意节点检测的操作，故可以最小化因消息认证带来的额外计算开销。

参 考 文 献

1 Sandro R, David H. A Survey of Key Management for Secure Group Communication [J]. ACM Computing Surveys, 2003, 35(3): 309～329

2 Challal Y, Seba H. Group key management protocols: a novel taxonomy [J]. International Journal of Information Technology, 2005, 2(2): 105～118.

3 Burmester M, Desmedt Y. A secure and efficient conference key distribution system [C]. Eurocrypt' 94, Italy, LNCS 950, Springer-Verlag, Berlin, 1994. 275～286

4 Horng G. An efficient and secure protocol for multi-party key establishment [J]. Computer Journal, 2001, 44: 463～470

5 Ateniese G, Steiner M, Tsudik G. New multiparty authentication services and key agreement protocols [J]. IEEE Journal Sel. Area. Comm., 2000, 18: 628～639

6 Boyd C, Nieto G. Round-optimal contributory conference key agreement [C]. In: Proc. Public-Key Cryptography' 03, USA, LNCS 2567, Springer-Verlag, Berlin, 2003. 161～174

7 Bresson E, Chevassut O, Pointcheval D. Dynamic group Diffie-Hellman key exchange under standard assumptions [C]. Advances in Cryptology-Proc. Eurocrypt 2002, Netherlands, LNCS 2332, Springer-Verlag, Berlin, 2002. 321～336

8 Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols [C]. ACM CCS'93, ACM Press, New York, 1993. 62～73

9 Schnorr C P. Efficient signature generation for smart cards [J]. Journal of Cryptology, 1991, 4(3): 161～175