第 34 卷 第 5 期 计 算 机 工 程 2008 年 3 月
Vol.34 No.5 Computer Engineering March 2008
·安全技术· 文章编号：1000—3428(2008)05—0155—03 文献标识码：A 中图分类号：TP309

基于广播加密的会话密钥分配新方案

赖 霞，何明星
(西华大学数学与计算机学院，成都 610039)

摘 要：广播加密方案是一种应用广泛的群组安全通信方案，在付费电视、视频会议和无线传感网络等场合具有良好的应用前景。该文针对许多基于二叉树结构的方案在中心控制密钥量 $O(n)$ 上作了一些改进，提出了一个安全的基于广播加密的会话密钥分配方案。新方案在中心密钥存储量上有明显的优势，同时能安全有效地完成密钥的分发、用户添加以及加密密钥更新等功能。

关键词：广播加密；密钥分配；伪随机函数；预留节点

Secure Session Key Distribution Scheme Based on Broadcast Encryption

LAI Xia, HE Ming-xing
(School of Mathematics and Computer Engineering, Xihua University, Chengdu 610039)

【Abstract】 Broadcast encryption scheme is wildly used in group communications, such as pay-TV, video-conferencing, wireless and sensor networks etc. In many hierarchical binary tree-based schemes, Group Center (GC) needs $O(n)$ spaces to store all related keys. This paper presents a secure session key distribution scheme based on broadcast encryption. The scheme reduces the key storage requirement of GC to a constant size, which is far better than that of the previously proposed schemes and can securely distribute key, join new users and renew encryption-keys successfully.

【Key words】 broadcast encryption; key distribution; pseudo-random function; preserved nodes

1 概述

广播加密方案最早由Fiat和Naor在 1993 年提出[1]。所谓广播加密，就是在每一次会话中，中心都必须加密会话密钥，并在不安全的信道上分发给动态群用户，只有拥有特权的合法用户才能解密秘密信息。本文研究在无状态接收者(stateless receiver)[2]场景下，运用广播加密技术对群组用户进行会话密钥分配。所谓无状态接收者是指接收者不能改变接收节点的状态(例如修改用户密钥)，仅按照初始设置(密钥)处理接收到的广播数据。文献[3]中提出了基于逻辑树的方案，该方案可使用户密钥存储复杂度减少到 $O(\log n)$，但中心需要 $O(n)$ 空间来存储所有相关密钥；文献[4]中的Mihaljevic方案是Mihaljevic于 2003 年提出的可重构的密钥管理方案，该方案可以在传输成本和存储成本之间找到一个平衡点，但即使在最佳状态下，中心也需要复杂度为 $O(n)$ 空间来存储所有相关密钥。并且上述方案缺乏用户扩展能力，即基于这些方案的广播加密系统不能在运行期间注册新用户，如果要注册新用户，必须重建二叉树，其代价是更新全部用户的密钥，而且更新操作通常需要离线操作。本文提出的方案在基于二叉树的广播加密方案中作了一些改进，中心构建一个a叉树 T_a，使用了一个Tseng[4]提出的伪随机函数(Pseudo Random Function, PRF)，引入一种节点预留方法[5]。所谓节点预留，指的是构建 T_a 时用预留节点来代表潜在的用户，注册新用户时，中心将预留节点分配给该用户；选择恰当的预留节点数，能在较长时间内满足用户扩展要求。本文提出的方案在中心控制密钥存储上有显著的优势，能保持为一个常数 $O(1)$，而用户密钥存储量不高于其他方案的存储量；并且很容易扩展为多对多群组通信方案。在引入节点预留方法后，笔者对预留节点采用完全子树进行分组[5]，既能注册新用户，又能安全有效地完成密钥的分发、用户添加以及加密密钥更新等功能。

2 密钥分配新方案

2.1 初始化阶段

首先定义几个参数，注册用户集合用 N 来表示，设 $N=\{U_1,U_2,\cdots,U_n\}$，R 是退出用户集合，假定其元素个数 $|R|=r$，$r\in[0,n]$。中心对剩余用户 $N\backslash R$ 作一划分，这里的划分是基于子集覆盖的思想，定义了一系列的互不相交的子集 $S_1,S_2,\cdots,S_w,S_i\subseteq N$，满足 $N\backslash R=\bigcup_{i=1}^{t}S_i$，每个子集 S_i 都被赋予一个组密钥 GK_i；属于 S_i 的每个用户 U_w 都可以从他存储的秘密信息推导出其子密钥 K_w。对于任一子集 S_i 而言，不妨假定 $|S_i|=m$，中心选择一个适当大小的 a 并构建一个 a 叉树 T_a，树根为 V_0，d为层数，其中，$a^d=m$；a 是大于或等于 2 的正整数。每一个用户对应一个叶子节点，从左至右标为 U_1，U_2，…，U_m。中心选取一个伪随机函数 PRF：$f_s(x)=f(x,s)$，其中，x 是变量；s 是只能由中心控制的安全随机数；$x,s\in\{0,1\}^*$，$f:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*$。对于第 i 层第 j 个节点，中心用 PRF 为其生成相应的节点密钥：$L_{i,j}=f_s(x)=$

基金项目：国家自然科学基金资助项目(60473030)；教育部科学技术资助重点项目(205136)；四川省科技厅资助重点项目(05JY029-131)
作者简介：赖 霞(1972－)，男，硕士研究生，主研方向：密码学与信息安全；何明星，教授、博士
收稿日期：2007-03-10 **E-mail：**laixia811@yahoo.com.cn

$f_s(g(i,j))$，其中，在多项式时间里，$g(i,j)$ 可以转化为 x。

在 T_a 中，规定从根节点 V_0 到每一个用户所对应的叶子节点的路径中各节点的节点密钥构成组密钥 GK，规定从根节点 V_0 到与所有退出用户对应的叶子节点形成的子树为最小子树，记为 Min$T(R)$，规定所有与 Min$T(R)$ 中节点相连且输出度为 1 的节点(不包括代表退出用户的叶子节点)密钥为加密密钥 $JK=\{L_{i_1,j_1},L_{i_2,j_2},\cdots,L_{i_{m'},j_{m'}}\}$，其中 m' 与退出用户数 r' 有关 $(1\le m'\le m)$。例如：设 $m=4^3,a=4,d=3$，如图 1，U_{33} 的节点密钥为 $K_{33}=\{L_{0,0},\ L_{1,3},\ L_{2,9},\ L_{3,33}\}$，故 $GK=\{K_1,K_2,\cdots;K_{64}\}$，其中 $|K_i|=d\ (1\le i\le 64)$。设退出子集 $R_1=\{U_8,U_{33}\}$，中心构建 $MinT(R_1)$ 如图 2，粗线条所示，加密密钥 $JK_1=\{L_{1,2},L_{1,4},L_{2,1},L_{2,3},L_{2,4},L_{2,10},L_{2,11},L_{2,12},L_{3,5},L_{3,6},L_{3,7},L_{3,34},L_{3,35},L_{3.36}\}$，由图中虚线所连接的节点密钥构成。

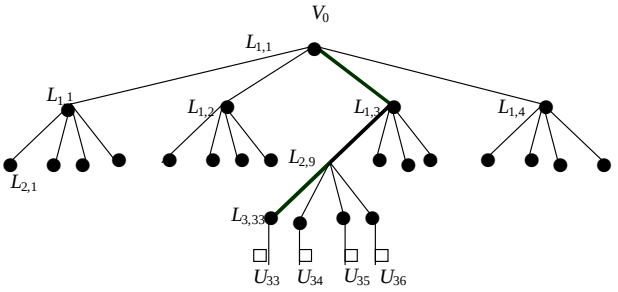

图 1　密钥树

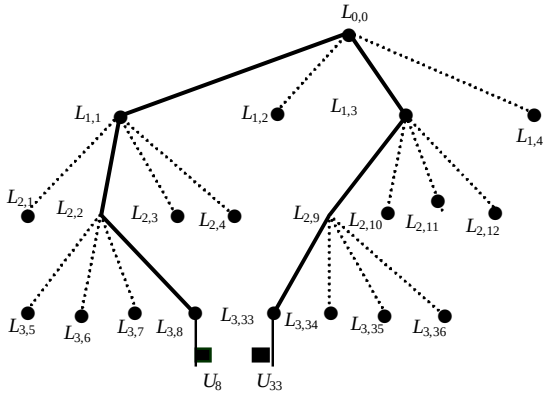

图 2　Min$T$ (R_1)和 JK_1

2.2　广播加密阶段中心广播消息

$<[(i_1,j_1),(i_2,j_2),\cdots,(i_{m'},j_{m'}),E_{L_{3,3}}(k),E_{L_{2,12}}(k),\cdots,E_{L_{i_{m'},j_{m'}}}(k)],E'_K(M)>$。

消息中方括号部分为头部，$E'_K(M)$ 是主体，M 是当前的消息，K 是随机选择的当前会话密钥，E和E'是 2 个对称加密算法，如 *AES* 或 *DES* 等。就上述例子，中心广播消息：$<(1,2),(1,4),(2,1),(2,3),(2,4),(2,10),(2,11),(2,12),(3,5),(3,6),(3,7),(3,34),(3,35),(3,36),[E_{L_{1,2}}(k),E_{L_{1,4}}(K),E_{L_{2,1}}(K),E_{L_{2,3}}(K),E_{L_{2,4}},E_{L_{2,10}}(K),E_{L_{2,11}}E_{L_{2,12}}(K),E_{L_{3,5}}(K),E_{L_{3,6}}(K),E_{L_{3,7}}(K),E_{L_{3,34}}(K),E_{L_{3,35}}(K),E_{L_{3,36}}(K)],E'_K(M)>$。

2.3　解密阶段

当合法用户(如 $U_w(1\le w\le m)$)收到广播消息后，首先根据自身节点标记 (d,w) 搜寻自己所在子集 S_i，然后根据中心发给他的秘密信息，在广播消息中搜索并验证是否存在密钥子集标记 $(i_w,j_w)\in\{(i_1,j_1),(i_2,j_2),\cdots,(i_{m'},j_{m'})\}$ (若$U_w\in R$，不存在这样的 (i_w,j_w))，然后导出 L_{i_w,j_w}，并计算出 $D_{L_{iw,jw}}((E_{L_{iw,jw}}(K))$ 获得当前会话密钥 K，再通过计算 $D'_K(E'_K(M)$，从而得到当前消息 M，其中 D和D'是对应 E和E'的解密算法。

在上述例子中，非退出用户 U_9 根据他的 GK 子集消息 $K_9=\{L_{0,0},\ L_{1,1},\ L_{2,3},\ L_{3,9}\}$，得到 $(2,3)\in\{(1,2),(1,4),(2,1),(2,3),(2,4),(2,10),(2,11),(2,12),(3,5),(3,6),(3,7),(3,34),(3,35),(3,36)\}$，然后导出 $L_{2,3}$，通过计算 $D_{L_{2,3}}((E_{L_{2,3}}(K))$ 得到当前会话密钥 K，再计算 $D'_K(E'_K(M)$ 得到当前消息 M。再如 U_{34}，在导出相应的节点密钥 $L_{3,34}$ 后，可以计算出当前会话密钥 K，得到消息 M。

3　新方案扩展为多对多群通信方案

笔者提出的新方案很容易扩展到多对多的群通信中，对任一合法用户 U_m 想要给其余用户广播消息，都可以通过下面 3 个阶段来实现。

3.1　初始化阶段

假定 $|N|=n$，$|R|=r$。(1)中心为每一位用户构建完全逻辑a叉密钥树 T_a，假定用户 $U_1,U_2,\cdots,U_n$ 分别对应密钥树为 $T_1,T_2,\cdots,T_n$。在 $T_m(1\le m\le n)$ 中，叶子节点从左至右与其余 $n-1$ 个用户相连，对于第 i 层第 j 列节点，中心用PRF[4]为其生成节点密钥：$L_{i,j}^{(m)}=f_{s_m}(x)=f_{s_m}(g(i,j))$，$s_m$ 是中心分发给 T_m 的随机安全参数。(2)中心通过安全渠道为每一位用户分发秘密信息。例如，中心为 $U_m(1\le m\le n)$ 发送 $<T_m,\ K_m^1,\ K_m^2,\cdots,K_m^{m-1},K_m^{m+1},\cdots,K_m^n>$，其中 K_m^n 表示从 T_n 中分发给 U_m 的 GK 子集。值得注意的是，a叉密钥树 T_a 的构建，节点密钥生成，以及给其余 $n-1$ 个用户分发秘密信息，都是中心事先做的，用户 U_m 仅仅是消息的发布者，见表 1。

表 1　各用户 *GK* 和对应密钥树

用户	密钥树 $T_i(1\le i\le n)$	T_j发给U_i的$GK(1\le i\ne j\le n)$
U_1	T_1	$\{K_1^2,K_1^3,\cdots,K_1^n\}$
U_2	T_2	$\{K_2^1,K_2^3,\cdots,K_2^n\}$
⋮	⋮	⋮
U_m	T_m	$\{K_m^1,K_m^2,\cdots,K_m^{m-1},K_m^{m+1},\cdots,K_m^n\}$
⋮	⋮	⋮
U_n	T_n	$\{K_n^1,K_n^2,\cdots,K_n^{n-1}\}$

3.2　广播加密阶段

假定用户 $U_m(1\le m\le n)$ 想要给其余用户广播消息，他只需从中心为其构建的 $MinT(R)$ 中找到加密密钥 JK，假定 $JK=\{L_{i1,j1}^{(m)},L_{i2,j2}^{(m)},\cdots,L_{im',jm'}^{(m)}\}$，其中 m' 与 r'有关$(1\le m'\le n)$，用 JK 加密会话密钥 K 并广播消息：$<[U_m,(i_1,j_1),\ (i_2,j_2),\cdots,(i_{m'},j_{m'}),E_{L_{i1,j1}^{(m)}}(k),E_{L_{i2,j2}^{(m)}}(k),\cdots;E_{L_{im',jmf}^{(m)}}(k)],E'_K(M)>$。消息中 U_m 表示消息发布源。

3.3　解密阶段

接收用户(如 U_w)收到来自 U_m 的广播消息后，他可以从他的 GK 中找到 K_w^m，并搜索其标记是否 $(i_w,j_w)\in\{(i_1,j_1),(i_2,j_2),\cdots,(i_{m'},j_{m'})\}$，然后可导出节点密钥 $L_{iw,jw}^{(m)}$，并计算 $D_{L_{iw,jw}^{(m)}}((E_{L_{iw,jw}^{(m)}}(K))$ 获得 K 后，再计算 $D'_K(E'_K(M)$ 从而获得当前消息 M。

4　新方案性能及效率

4.1　添加用户及更新密钥

(1)当 R 中的退出用户想重新回到 $N\backslash R$ 中时，中心无需重新划分，按照退出协议在保号期(承诺退出后保留其叶子节点标记期限)内可直接回到原叶子节点。中心在每一次广播消息

时，接收者(如U_w)的节点密钥K_w不会改变，但随着R中成员的改变，GK会相应更新，从而用来加密当前会话密钥K的加密密钥JK也就随之更新。

(2)当新用户加入时，中心也无需重新进行$N \setminus R$的划分，可填充超出保号期的退出用户对应叶子节点，也可向中心申请T_a中的预留叶子节点[5]。超出保号期用户视为新用户。

4.2 新方案密钥存储

在进行广播之前，预留节点将被视为退出节点，所以，在新方案中，中心分发给各用户(如U_w)的GK子集K_w不会改变，故每一位用户应存储的密钥数为$1+\log_a n$，其复杂度为$O(\log_a n)$。

下面讨论本文提出的扩展方案的密钥存储情况：每一位合法用户从其余$n-1$位用户中任一位的密钥树获得的GK子集的节点密钥数为$1+\log_a(n-1)$，所以每一位接收者共获得的密钥数为

$$1+(n-1)(1+\log_a(n-1)) = n+n\log_a(n-1)-\log_a(n-1) = O(n\log_a(n-1))$$

例如，$n=2^{10}+1$时，当$a=2$时，每一位用户应储藏11 265个密钥；当$a=4$时应储藏6 145个密钥。从上述结果可以知道，中心选取适当较大的a值可以减少用户的密钥存储量，但这并不意味着选取的a越大越好。还应注意到结合用户数和有利于区组的划分，以及用户密钥安全存储等因素。

下面就本方案及扩展方案在$a=2$时，与文献[3]的基于逻辑树方案和文献[4]方案等在中心控制密钥量、用户密钥存储量以及用户无状态接收特性等方面进行了比较，见表2。

表2 a=2时新方案及扩展方案与其他方案比较

	Wong et al 方案	Mihaljevic 方案	本文 基本方案	本文 扩展方案
中心控制密钥量复杂度	$O(n)$	$O(n)$	$O(1)$	$O(n)$
用户密钥存储量复杂度	$O(1bn)$	$O(H_0 1.5-H_0-1bn)$ 其中$H_0<1bn$	$O(1bn)$	$O(n1bn)$
无状态	不	是	是	是

从表2可以看出，本文提出的新方案与其余两个方案在中心密钥存储上有明显的优势，能保持到一个常数，而用户密钥存储量不高于其他方案的存储量，适合无状态接收者场合[2]，即解密操作仅依赖于当前接受的广播加密信息和接收设备(程序)存储的秘密信息的条件下，方案是安全的。

5 安全性分析

在本文的方案中，中心使用了PRF[3]来生成群密钥，并通过秘密渠道给每一位用户分发子密钥。PRF中的秘密随机参数s由中心唯一控制，由PRF生成的数，攻击者不可能预测到前一个数和后一个数，即或是退出用户全部合谋勾结起来，也不可能计算出群密钥或导出s来，因而也就无从知道当前会话密钥K和原始消息M。

在扩展方案中，每一个要广播消息的广播者(如U_m)都唯一掌控着相应的随机安全参数s_m，其安全性也如新方案一样。另外，在节点预留的处理上采用了预留节点分组[5]，并且在广播时将分组后的预留节点视为退出节点，这样就保障了后向安全性，从而保障了在安全性上与新方案是一致的。

6 结束语

广播加密方案实现了在不安全的广播信道上进行消息的安全发送，已有的基于二叉树广播加密方案拥有简洁的密钥分配算法和子集覆盖算法，但是这些方案中中心存储开销较大，缺乏用户扩展能力，使得这些方案只能用在注册用户固定的场合。本文提出的方案在中心的密钥存储量上有明显的优势，能保持到一个常数$O(1)$，而用户密钥存储量不高于其他方案的存储量，并且很容易扩展为多对多群组通信方案。在引入节点预留方法后，笔者对预留节点进行了分组，能有效地完成密钥的分发、用户添加以及加密密钥更新等功能。

参考文献

[1] Fiat A, Naor M. Broadcast Encryption[C]//Proc. of Conf. on Advances in Cryptology-CRYPTO'93. Berlin: Springer-Verlag, 1994: 480-491.

[2] Naor M. Revocation and Tracing Schemes for Stateless Receivers[C]//Proc. of Conf. on Advances in Cryptology-CRYPTO'01. Santa Barbara, California: [s. n.], 2001: 41-62.

[3] Wong C K, Gouda M, Lam S. Secure Phs[J]. IEEE/ACM Transactions on Networking, 2000, 8(1): 16-30.

[4] Mihaljevic M. Key Management Schemes for Stateless Receivers Based on Time Varying of Heterogeneous Logical Key Hierarchy[C]//Proc. of Conf. on Advances in Cryptology-Asiacrypt'03. Heidelberg: Springer-Verlag, 2003: 137-154.

[5] 匡建民, 谷大武. 广播加密方案的一个注记[J]. 计算机工程, 2006, 32(2): 147-259.

（上接第154页）

参考文献

[1] Akyildiz I F, Su Weilian, Yogesh S, et al. Wireless Sensor Networks: A Survey[J]. Computer Networks, 2002, 38(4): 393-422.

[2] Perrig A, Stankovic J, Wagner D. Security in Wireless Sensor Networks[J]. Communications of the ACM, 2004, 47(6): 53-57.

[3] Harney H, Muckenhirn C, Rivers T. Group Key Management Protocol Architecture[S]. RFC 2094, 1997.

[4] Balenson D, McGrew D, Sherman A. Key Management for Large Dynamic Groups: One-way Function Trees and Amortized Initialization[Z]. IETF Internet draft, 2000.

[5] Blundo C, Santis A De, Herzberg A, et al. Perfectly-secure Key Distribution for Dynamic Conferences[C]//Proc. of the 12th Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer-Verlag, 1993.

[6] Zhang Wensheng, Cao Guohong. Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach[C]//Proc. of IEEE INFOCOM'05. Mliami, FL: IEEE Press, 2005.

[7] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy Efficient Communication Protocol for Wireless Microsensor Networks[C]// Proceedings of the 33rd Hawaii International Conference on System Sciences. Maui: IEEE Press, 2000.

[8] Shehab M, Bertino E, Ghafoor A. Efficient Hierarchical Key Generation and Key Diffusion for Sensor Networks[C]//Proc. of IEEE SECON'05. [S. l.]: IEEE Press, 2005.

[9] Chang Chih-Yung, Shih K P, Lee S C. ZBP: A Zone-based Broadcasting Protocol for Wireless Sensor Networks[J]. Wireless Personal Communications, 2005, 33(1): 53-68.