第 26 卷第 7 期 电 子 与 信 息 学 报 Vol.26No.7
2004 年 7 月 Journal of Electronics & Information Technology July 2004

# 基于分级密钥管理的安全组播方案 [1]

李远征

(北京邮电大学信息安全中心 北京 100876)

**摘 要**: 该文提出了一个新的适用于大型动态组播群组的密钥管理方案，在分级结构中采用 Hash 链作为数据传递密钥来实现层与层之间的数据传递，在子组内利用数字信封来实现密钥管理. 此方案具有良好的计算、存储性能及动态安全性，为进一步研究提供了一个有价值的参考.

**关键词**: 组密钥管理，单向 Hash 函数，数字信封

**中图分类号**: TN918 **文献标识码**: A **文章编号**: 1009-5896(2004)07-1053-04

# A Security Multicast Scheme with the Hierarchical Group Key Management

Li Yuan-zheng

(*Info. Security Center, Beijing University of Posts and Telecom., Beijing* 100876, *China*)

**Abstract** A new key management scheme applied for large dynamic multicast group is proposed in this paper. In the hierarchical structure one-way hash chain is used as transmission key to transmit the data between the levels. Digital envelope is used to realize key management in subgroups. This scheme is of good attributes in computation, storage and dynamic security. It provides a valuable reference to further study.

**Key words** Group key management, One-way hash function, Digital envelope

## 1 引言

随着因特网的广泛应用，组播也得到了迅速的发展，如 Internet 视频传输、消息发布等应用，使用组播可以节省发送者资源、减少网络流量，但是可靠性和安全性问题变得比单播更为复杂. 在组播安全问题中组密钥的安全管理是一个重要的研究课题，已成为目前研究的焦点.

组播的密钥分配不同于传统的单播密钥分配，尤其在大型、动态、变化的组中有效地管理密钥更是一个困难的问题. 每次当一个成员从一个组中退出时，组密钥必须改变，当有新的成员加入时同样是这样. 组成员必须能够有效地计算新的密钥，而退出成员的任意联合不能够得到它. 在满足这些安全要求的同时，存储代价及通信代价必须考虑在内，因此这一问题的解决变得很复杂.

本文提出了可扩展的安全组密钥管理方案的数学模型，采用分级管理结构，可高效地处理组成员的动态加入和退出，由于运用了基于单向 Hash 函数及数字信封 [1] 的方法，其安全性也是可证明的，这一方案可灵活应用于集中式和分布式环境.

## 2 系统结构及算法描述

### 2.1 分级结构

近年来对组播组密钥管理的研究已不是局限于静态的或小的组，而是主要着眼于频繁变化的大型动态组播系统. 根据组密钥的产生方式，组密钥管理方法大致可分为三类，即集中式管理、分散式子组管理和分散式管理. 集中式管理方法是只有一个组控制器来管理所有的成员；

[1] 2003-03-12 收到，2003-11-06 改回

国家“863”项目 (2002AA143041)、国家“973”项目 (G1999035804)、国家自然科学基金项目 (60073049, 90204017) 资助课题

分散式子组管理方法将整个组分成若干个子组，每个子组有自已的子组控制器来管理子组内成员；分散式组密钥管理没有固定的组控制器，由所有组共同建立组密钥.

本文提出的方案基于分散式子组管理. 组播系统的结构是建立在原有发送接收关系树基础上的分级树结构，即原有的上下级层次关系不变，对每一层的成员分组，每个成员加入一个子组. 发送者即为根结点，根结点有子组，这些子组是由接收者组成的，每个子组从成员中选出一个作为组安全控制器 (Group Security Controller, GSC) 管理本子组的密钥安全并实现上下级的数据传递，也可以另外加入一个 GSC 到子组中来完成管理功能. 分级结构如图 1 所示.

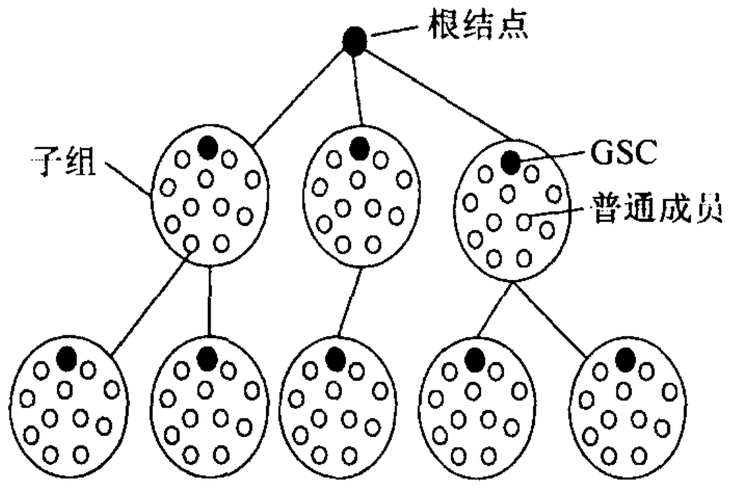


图 1 分级组密钥管理示意图

### 2.2 GSC 与密钥管理

在整个组播系统中，GSC 是密钥管理的中心，密钥的初始化或更新是在组播组产生时，接收者加入、离开子组及子组合并、拆分时进行. GSC 可以由组内的某一成员担任，也可以设置专门的成员完成其功能. 设组播组共分为 $m$ 层，$r$ 个子组，第 $i$ 个组中有 $n$ 个成员，$i_1,\cdots,i_n$，密钥的管理描述如下：

首先将有关符号作一说明 (文中提到的公钥算法可采用 RSA，对称算法可采用 3DES)：$E_K(M)$ 为使用密钥为 $K$ 的 RSA 算法对明文 $M$ 加密. $E(M,k)$ 为用密钥为 $k$ 的对称密码算法对明文 $M$ 加密. $H(m)$ 为用 Hash 算法计算 $m$ 的 Hash 值. $\|$ 为连接操作.

系统初始化：由根结点产生种子 $K_0$，并通过安全通道 (利用公钥密码或通过安全载体由人分发) 将各个 Hash 值送给子组的 GSC 作为层间传递密钥；GSC 负责生成对应于组内各成员的公私钥对，公钥由 GSC 保存在它的成员信息表内，私钥通过安全通道 (通过安全载体由人分发) 传递给各成员. 每个子组的 GSC(以第 $j$ 层第 $i$ 个子组为例) 需保存的参数：$K_j,e_{i_1},\cdots,e_{i_n}$，具体描述如下：

$K_j$ ——层间传递密钥，保密，$j=0,\cdots,m$，$j$ 为从根结点算起的分层数. 每一层的 GSC 保存一个相同的传递密钥，对应于 Hash 链的一个结点，最高层即根结点产生并保存此 Hash 链的种子密钥记为 $K_0$，以下各层依次为 $K_1,\cdots,K_m$. 定义 $H$ 为单向 Hash 函数，各层传递密钥之间的关系为：$K_{j+1}=H(K_j)$，由于此函数的单向性，由第 $j+1$ 层的 $K_{j+1}$ 是不可能推出第 $j$ 层的 $K_j$ 值的. 传递密钥需定期更换.

$e_{i_1},\cdots,e_{i_n}$ ——第 $i$ 个子组内各成员的公钥，公开，与对应的私钥结合对每次生成的用于加密数据的对称密钥 $k_i$ 进行保护.

组内各成员需保存自己的私钥：

$d_{i_l}$ ——第 $i$ 个子组内的第 $l$ 个成员的私钥，保密，用于解密出对称密钥 $k_i$，之后用 $k_i$ 解密出数据.

GSC 作为子组中的安全控制器，主要有以下几个功能：

(1) 数据传递：GSC 接收上一层的数据，用本层的传递密钥 $K_j$ 将数据解密后，将数据重新封装传给下一层，同时传给本组内的成员.

(2) 密钥管理： GSC 管理子组内的密钥，当一个新的成员加入子组时， GSC 创建一对新的公私钥对，将公钥加入到成员表中，将私钥通过安全通道传给这个新成员。当由于子组合并或拆分而有新的子组生成时，由它来重新进行密钥初始化，即产生并分发公私钥对。

由上面的描述可知， GSC 作为组安全控制器，会成为被攻击的重点，在实际应用中，如果需要分散它的功能，可将其产生并分发公私钥对的功能转移出去，由专门的机构实现。

### 2.3 组间数据传递算法

文献 [2] 中提到的数据传递方式是，每个子组的控制中心保存本组及其父结点的密钥，当该子组接收到父结点传来的数据包后，用其父结点的密钥解密该数据包，然后用本组的密钥将该数据重新加密发送给本组内的成员．本文的方案中采用了一条 Hash 链来对应各层的用于数据传递的密钥， Hash 链的单向传递关系简化了密钥的管理，使得上下层传递数据时，下层不必保存上一层的密钥，由上层可推出下一层的密钥，而下一层不可能推出上一层的密钥，从而数据传递的安全性得以保障，尤其对于存在上下级关系的组播，这种结构更实用．当然，如果有组退出或根结点定期更换密钥时，要通知所有的 GSC 同时更换传递密钥．

数据传递是这样实现的：第 $j$ 层向第 $j+1$ 层传递时的数据包为： $E(R,K_{j+1})\|E(M,R)$ ，即由发送者生成一个随机数 $R$ ，用该随机数作为密钥加密数据 $M$ ，然后用第 $j+1$ 层的传递密钥 $K_{j+1}$ 来加密这个随机数，使用随机数的目的是在逐级传递时，不必反复解密并加密数据，而只需解密并加密这个随机数即可，这样可以提高传输效率，当数据传到第 $j+1$ 层后，第 $j+1$ 层各子组的 GSC 用 $K_{j+1}$ 解密数据 $M$ 并用本子组内的对称密钥 $k_i$ 及各成员的公钥加密 $M$ 传给组内的其余各成员，如需向下一层传送，则由第 $j+1$ 层的 GSC 将 $E(R,K_{j+2})\|E(M,R)$ 传给第 $j+2$ 层．

### 2.4 子组内密钥管理算法

当子组内的 GSC 得到数据后，需要将数据传送给组内的各成员．在组播安全解决方案中多采用对称密码来加密数据，密钥的管理相对困难，再加上成员的加入和退出，需频繁地更换密钥，更增加了难度，若采用公钥算法会大大简化密钥的管理，但是会使计算开销过大．本文提出了一种新的建立在数字信封技术上的组内密钥管理算法，它结合了对称密码加密技术和公开密钥加密技术的优点，用公钥技术来保护对称密钥，每次组内发送数据时产生新的对称密钥，既保持了数据传送的高效性，又保障了安全性．

该算法可具体描述如下：

GSC ：如前所述，第 $i$ 个组内各成员 $i_1,\cdots,i_n$ 具有公钥 $e_{i_1},\cdots,e_{i_n}$ ，当 GSC 从上一层收到数据 $M$ 后，需向组内各成员传送，它首先产生一个对称密钥 $k_i$ ，用该对称密钥加密要发送的数据，再用各成员的公钥加密上述对称密钥，然后将这两步的结果群发给各成员，如在第 $i$ 个组内的第 $l$ 个成员收到的信息是： $E_{e_{il}}(k_i)\|E(M,k_i)$ ．

成员：以第 $i$ 个组内的第 $l$ 个成员为例，它收到上述信息后，首先用自己的私钥 $d_{i_l}$ 通过 $E_{e_{il}}(k_i)$ 解密出 $k_i$ ，然后用 $k_i$ 通过 $E(M,k_i)$ 解密出数据 $M$ ．

密钥的更新：由于采用了公钥和私钥，并且每次组内发送数据采用不同的对称密钥，因此公私钥相对稳定，只需定期更换．

## 3 动态安全性

### 3.1 子组的加入和退出

当子组合并、拆分或有新的子组加入时，子组中的密钥需重新初始化，由 GSC 生成新的公私钥对，并由安全通道将私钥分发给相应的成员，由根结点将传递密钥由安全信道传递给新的 GSC ，若 GSC 由组内成员担任，当子组合并时需由根结点重新分配所有的传递密钥．

当有子组退出时，需重新分配传递密钥，由根结点生成新的 $K_0$ ，并通过安全通道将各个 Hash 值送给子组的 GSC ．

### 3.2 成员的加入和退出

当有成员 $P_{n+1}$ 加入时，由 GSC 产生新的公私钥对，公钥由 GSC 加入到成员表中，私钥通过安全通道发放给 $P_{n+1}$ ．多个成员的加入与此类似．

当有成员 $P_i$ 退出时，将其对应的公钥从 GSC 的成员表中删除即可．多个成员的退出与此类似．

### 3.3 GSC 的退出

当某个 GSC 退出时，首先从组成员中选取一个作为新的 GSC 或重新设置一专用的 GSC，同时需重新进行组内密钥的初始化，由新的 GSC 生成并分发新的公私钥对，系统更新传递密钥．

### 3.4 安全性分析

**子组的独立性** 本文所提出的方案保持了子组的独立性，不同层的组之间由传递密钥来实现数据的传递，不同的子组使用不同的组内密钥，组内的密钥由 GSC 来产生及更新，某一个子组内的密钥泄漏不会影响到其它子组的安全，从而简化了密钥的分配并提高了整个系统的安全性．

**组间传递的安全性** 在文献 [3] 中，层与层之间是靠每个子组中的密钥控制中心存储本组及父结点的密钥来实现上下层之间数据的传递，这样安全性差，同时不便于密钥更新，本方案用 Hash 链实现了层与层之间的密钥传递，每个 GSC 不必存储下一级的密钥，而是用 Hash 函数的单向性解决了这一问题，既简化又保证了安全性．

**组内传递的安全性** 组内由于采用了数字信封技术，每次传送数据使用不同的对称密钥，系统有了额外的安全保证，有效地防止了成员泄漏对称密钥可能造成的安全威胁，而且成员加入和退出时也因不涉及对称密钥不会影响到安全性．

## 4 性能分析

(1) 密钥管理简便 每个 GSC 只需保存一个传递密钥及各成员的公钥，组内的密钥生成及更换由 GSC 完成即可，每个成员只需存储自己的私钥．与文献 [3] 相比，每个 GSC 不必存储本级及上一级的两个密钥，在 Wallner, *et al*[4] 提出的 HBT 方案中，每个成员要存储从根结点到父结点的路线上的所有密钥，相比之下本方案存储量小．成员的加入、退出不需要更换密钥，省去了大多数方案中每次成员加入和退出都要更换密钥或更换保护密钥的代价．

(2) 传输效率高 由于上下层传递数据时，由 GSC 产生随机数密钥来加密数据，而传递密钥只用来加密随机数密钥，层间传递时不必频繁地加密解密数据，只需加密解密随机数密钥，因此提高了层与层之间的传输效率．在组内传送数据时使用了数字信封技术，既保证了安全性又保障了效率．

## 5 结论

对于大型动态组的密钥安全管理，为了支持大型动态组的安全组播，密钥管理方案应该具有可放缩性，即它能处理大型分布式组的频繁的密钥更新，能够适应组成员关系的调试变化，能保证成员加入或退出组的秘密性，本文给出的组密钥管理总体方案及数学模型很好地满足了这些要求，并具有很好的灵活性和可扩展性．

**致谢** 本文是在导师杨义先教授的指导下完成的，特此致谢．

## 参 考 文 献

[1] Schneier B. 吴世忠，祝世雄，张文政等译. 应用密码学：协议、算法与 C 源程序. 北京：机械工业出版社，2000: 33–52.

[2] Mittra S. Iolus: A framework for scalable secure multicasting. Proceedings of ACM SIGCOMM'97, September 14–18, Cannes, France, 1997: 277–288.

[3] Cho S, Kim C. A secure multicast architecture with the decentralized key management. ICEC 2000, Seoul, Korea, August 21–24, 2000: 1.

[4] Wallner D, Harder E, Agee R. Key management for multicast: Issues and architectures. RFC 2627, June 1999.

李远征： 女，1972 年生，博士生，主要研究方向为密码学、信息安全等．