文章编号:1001 - 9081(2005)10 - 2291 - 03

一种基于成员发现协议的可扩展组播密钥管理方案

魏楚元[1],李陶深[1,2],王高才[1]
(1. 广西大学 计算机与电子信息学院,广西 南宁 530004;
2. 中南大学 信息科学与工程学院,湖南 长沙 410083)
(tshli@gxu.edu.cn)

摘 要:在分析现有组播密钥管理协议的基础上,提出了一种基于成员发现协议的组播密钥管理方案。针对实际的 Internet 拓扑结构,引入成员发现协议生成包含组成员的覆盖树,再通过组生成算法将整个参与组播的各终端用户形成的组播组划分成若干个虚拟的组播子组,组安全控制器将组密钥安全分发给各个子组安全控制器,子组内采用 LKH 方法实现密钥管理。该协议本质为一种二级层次结构的密钥管理协议,具有较好的可扩展性,在密钥更新代价方面取得了较好的性能,适合于大型组播群组。

关键词:组播密钥管理;组密钥;成员发现协议;密钥更新;可扩展性
中图分类号: TP393.08 **文献标识码**:A

Scalable Key management scheme based on member discovery protocol for IP multicast

WEI Chu-yuan[1], LI Tao-shen[1,2], WANG Gao-cai[1]
(1. *College of Computer and Electronics Information, Guangxi University, Nanning Guangxi* 53004, *China*;
2. *College of Information Science and Engineering, Central South University, Changsha Hunan* 410083, *China*)

Abstract: On the basis of analyzing existed schemes, a key management scheme based on member discovery protocol for IP multicast was proposed. Aiming at realistic Internet-like topologies, the member discovery protocol was embeded in our protocol to output a member overlay tree. The multicast group which consisted of all end-users was divided into some virtual subgroups by group-constructing algorithm. Logical Key Hierarchy(LKH) protocol was adopted to implement key management in every subgroup. The group key was distributed to all subgroup security controllers by the group security controller. The protocol was a two-level key management protocol. The improved protocol possesses better scalablity than other schemes, better performance about group rekeying and can be applied to large multicast group.

Key words: multicast key management; group key; member discovery protocol; rekeying; scalability

0 引言

组播通信安全是当前研究的一个热点问题,主要集中在组播群组数据保密性、完整性、组成员的认证等三个方面[1]。数据保密性由发送方使用加密算法对组播的通信数据进行加密,在接收方用一个对应的解密密钥进行解密,这个密钥被称为组密钥,由群组中的每一个成员掌握;完整性和成员认证主要通过数字签名技术实现。其中,数据保密性是组播安全中最具有挑战性的问题,首要解决的是组播密钥管理问题,它包括群组密钥的生成、分发和密钥的更新。从密钥管理机制的评价来看,需要充分考虑密钥管理协议的一些计算开销、存储需求、网络带宽、延迟等因素,例如密钥生成需要的计算量,当节点的计算资源不足或密钥更新频繁时,需要考虑密钥生成给节点带来的负载等问题。因此,设计一个组播密钥管理方案,需要将组播的安全需求及组播密钥管理的安全性、可扩展性、可靠性、鲁棒性等结合起来考虑,进一步降低密钥管理的代价。本文以讨论组播密钥管理为重点,提出一种基于成员发现机制的组播密钥管理方案。

1 几种组播密钥管理方法分析

当前的组播密钥管理方法主要有基于逻辑密钥树的方法与安全组播框架方法。逻辑密钥树方法通过建立密钥管理中心(即密钥服务器 KS 或组控制器 GC),组播成员持有一个秘密份额,通过一棵逻辑密钥层次树来生成组密钥。安全组播框架方法是为了解决大型组播提出的一种框架协议,通过设计组安全代理来分担密钥管理服务器的负载,将组播组划分为不同的子组,以降低组播组密钥更新负载。从层次结构上看,可以进一步分为基于组的层次结构机制与基于密钥的层次结构机制。基于密钥的层次结构机制是一种集中式的密钥管理方法,存在一个单一的实体成员控制这个组播组,负责密钥的生成、分发和更新,这个节点充当领导成员的角色,被成为组控制器,典型的代表协议有逻辑密钥层次树 LKH[3],这种协议的缺陷是组控制器负载过重,容易导致单点失效的问题;基于组的层次结构机制通过把一个组播组组织成若干个具有层次结构的子组,把密钥管理服务的功能分布在子组中,最大的特点是密钥管理的非集中化和具备较好的可扩展性,

收稿日期:2005 - 04 - 20 **基金项目**:广西自然科学基金资助项目(0342001);广西科技攻关项目(033008 - 9).
作者简介:魏楚元(1977 -),男,湖北人,硕士研究生,主要研究方向:网络安全; 李陶深(1958 -),男,广西人,教授,主要研究方向:计算机网络、信息安全; 王高才(1976 -),男,广西人,副教授,博士,主要研究方向:计算机网络.

典型的代表协议有 Iolus[4]，因为采取不同的控制器管理子组，组控制器单点失效的问题得到了解决，但也缺少集中控制给管理带来的优点。

通过对 LKH、Iolus 等协议的分析，可以发现大部分协议都支持网络层多播，网络层多播侧重将数据复制等任务放在路由器上完成，应用层多播则把数据复制等任务放到终端主机而不是路由器上进行，这些终端系统形成了被用来传输数据到终端用户的一种覆盖网。利用这一特性，组播密钥安全管理协议的设计可以针对更具体的实际的 Internet 拓扑结构来考虑。Iolus 方案通过将整个组播组分成多个子组，很好的解决了密钥更新的可扩展性问题，但它对子组的规模大小没有定义，组规模大小不均衡，提供 Iolus 性能分析比较困难。本文提出的密钥管理方案，结合实际的 Internet 网络拓扑结构，引用一种组生成算法将整个参与组播的各终端用户形成的组播组划分成若干个组播子组，对子组的大小可以控制在一定的范围内，每个子组由一个充当组控制器管理角色的成员负责维护和管理子组，更符合实际组播应用的特征。图 1 描述了组播协议的拓扑结构。

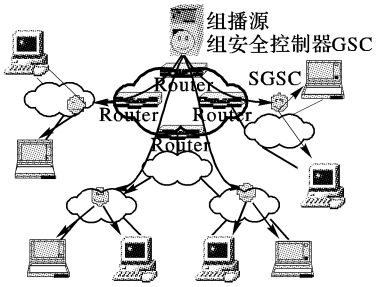


图 1 组播拓扑结构

2 组播子组的生成

文献[5]中 Suman Banerjee 提出的一种簇生成算法，本文引入这一方法并加以改进，该协议将一个较大规模的组播组的成员分成规模相对固定的、成员非重叠的一些簇，簇所拥有的成员数目在 k 到 $2k$ 之间，k 是一个整数变量。这里簇的概念相当于一个子组，每一个簇都有一个簇密钥，选举一个成员作为领导负责对该簇的密钥管理，对于各个簇的领导成员，由组播控制中心管理，形成了二级层次结构。密钥服务器负责上层密钥的生成。我们对该协议进行了改进，目标是将整个组播组划分为若干子组，先建立一个成员覆盖树，负责处理成员的加入，然后把成员覆盖树作为一种基本的组播数据结构，输出该覆盖树的非重叠的相互连接的子集，每一个子集对应一个子组，子组的成员规模控制在 k 到 $2k$ 之间。

2.1 成员发现协议

一个成员覆盖树描述了组播组成员之间的关系，它仅仅包含组播组的成员作为节点。当成员申请加入组播组后，使用一个组成员发现协议在覆盖树中建立每一个新加入成员的父节点。成员发现协议定义了组播树中不同的成员之间的父子关系，它将组播拓扑结构作为输入，输出一个成员覆盖树。

定义 1 设 $d(u,v)$ 表示与组播发送源 S 连接的两个成员 x 和 y 的距离，可用路由器的跳数计算。当且仅当以下两个条件成立时，成员 y 是成员 x 的父节点，S 是组播源节点。

$$d(S,y) \leqslant d(S,x) \tag{1}$$

$$\forall z \text{ 满足条件(1)，且 } d(y,x) \leqslant d(z,x) \tag{2}$$

条件(1)保证父节点比子节点离组播源 S 更近，条件(2)选择一个满足条件(1)的最靠近的成员。成员发现协议使用两个周期性的消息，一个是组播源 S 为根节点，周期性的组播一个心跳包给组内所有的成员，每一个成员由此推断出它到 S 的距离；另一个消息是每一个成员周期性的组播一个 TTL_Scoped 消息给覆盖树中它的父节点与所有的孩子节点，例如 x，这个消息包含一个元组 $< d(S,x), P(x) >$，$P(x)$ 表示覆盖树中 x 的父节点。该协议求解出一个描述组播成员节点关系覆盖树，作为下一步组播子组生成的输入。

2.2 组播子组生成协议

将组播组划分为若干个子组，能够较好地解决较大规模组播组密钥管理的可展性问题。对于子组的规模，大小在 k 到 $2k$ 之间，子组采用逻辑密钥树 LKH 密钥管理方案。组播子组生成协议将成员发现协议生成的成员覆盖树作为一个基本的数据结构，k 是一个待定的整数变量。规定规模在 k 到 $2k$ 之间的子组为稳定的子组，规模小于 k 或大于 $2k$ 的子组为不稳定的子组(短暂存在)。算法的基本思想是：通过一个合并子集的算法对不稳定子组的合并，生成一个成员数目在 k 到 $2k$ 之间的稳定子组。记 T_v 为一棵以某个节点 v 为根的子树，并且不能被加入到任何一个以 v 为根的子组，对于这样不稳定的子树，必须被加入到一个以 v 节点的上游节点为根的子组中。子组生成协议的过程如下：

1) 起始时，当一个成员 u 加入组播组，建立一个只包含自己唯一成员的不稳定的子组，记 $T_u = \{u\}$；

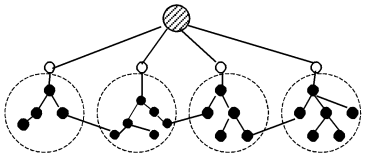
2) 每个成员 u 周期性的发送一个包含值 $|T_u|$ 的消息给它的父节点，$|T_u|$ 表示以 u 节点为根的子树的成员数目；

3) 从子节点 v 到父节点 u 的周期性消息要么是一个新的以节点 v 为根的不稳定的子树的通知消息，要么是一个现存的以节点 v 为根的不稳定的子树的通知消息。分为两种情况考虑，(a) 如果 T_v 是一个以前已知的子树，它可能是某个现存的以节点 u 为根的子组或者以节点 u 为根的不稳定的子树的一部分，u 检查 T_v 的规模是否已经改变了，如果大小足够充分地改变了，u 必须分裂或合并包含 T_v 部分的子组。如果 T_v 是一个不稳定子树的一部分，u 立刻可以创建一个新的稳定的子组；(b) 如果 T_v 是一个以前未知的子树，这棵新的子树被添加到以节点 u 为根的不稳定的子树，节点 u 设法将它的新的上游子组与它现存的子组合并，这个过程会产生一个新的以节点 u 为根的稳定的子组。对于所有不能被并入任何子组的子树，又形成了新的以节点 u 为根的不稳定的子树。

通过成员发现协议与组播子组生成协议，将整个参与组播的各终端用户形成的组播组划分成若干组播子组，对子组的规模可以控制在一定的范围，可以根据相应的组播业务的需求，合理选取子组规模大小参数 k，确定合理的分组方案，较好的解决密钥管理的可扩展性问题。

3 协议的设计与分析

3.1 子组安全控制器的设计



◎组安全控制器 ○子组安全控制器 ●组成员

图 2 组播组的密钥管理层次结构

对每个组播子组，设计一个子组安全控制器(SGSC)负责管理，它具有以下的能力：1)广播和单播数据的能力；2)提供对新申请加入成员的认证与授权，准许成员的加入离开，甚至驱逐某些成员；3)维护子组的辅助密钥管理树，实现成员加入或离开的密钥更新，保证多播组的动态安全性。我们设计

了一个全局组安全控制器(GSC)充当密钥管理服务器,负责对各组播子组安全控制器的管理,它一般驻留在密钥管理服务器上,维护对各子组安全控制器的层次密钥管理,通过成员发现子组生成协议,充分利用组播控制信息,主动或被动获取系统状态,并能根据系统状态变化实时作出正确的反应,使得分层分组的密钥管理机制更为健壮。

3.2　密钥更新策略

组播组是动态的,在任何一个时刻,可能有潜在的用户需要加入组播组或者用户退出组播组,为了保证前向和后向安全性,必须对组密钥进行更新。密钥更新是一种更新组密钥并把它们分发给组成员的过程。在安全组播会话中,密钥更新能确保仅仅当前组内成员能够发送加密的组播数据,并能对组播数据解密。对于每一个申请加入的成员,它选择一个合适的子组安全控制器 SGSC,通过一个安全的信道单播一个包含有必要的认证信息的单播请求给该 SGSC,接收到新加入成员的请求加入的消息后,SGSC 检查该认证消息的合法性,SGSC 由此决定是否同意它加入组播组。我们在子组内采用逻辑密钥树方法实现密钥管理。如图 3 是一个逻辑密钥树的示意图,假定现有一个有 8 个成员的组播子组,对应为逻辑密钥树的叶子节点。组成员 $m3$ 所知道的密钥是从它所对应的叶子节点到根节点(对应子组的组密钥)路径上所有的密钥,即$\{K_3, K_{14}, K_{18}\}$,K_{18} 对应根节点,为该子组的组密钥。

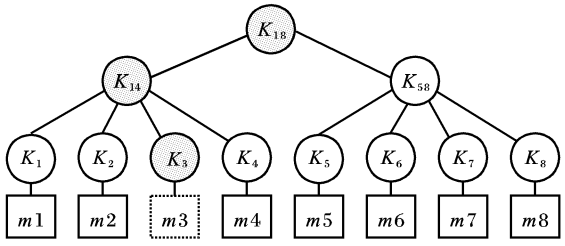


图 3　子组成员逻辑密钥树

对于每一个新申请加入的成员(如 $m3$)加入组播组,SGSC 建立一个新的仅仅同 $m3$ 共享的子组密钥 K',使用以前的子组密钥 K 加密新的子组密钥 K',并将它广播给当前子组所有的成员,SGSC 维护子组内辅助的逻辑密钥树,对于新加入的成员在逻辑密钥树上创建一个叶子节点,作为新加入成员在逻辑密钥树中对应的密钥份额的体现。

对于子组成员的离开,为了确保前向加密安全性,SGSC 需要更新所有被删除成员所知道的并被其他成员使用的密钥,以确保离开的组成员无法解密密钥更新消息和组播的内容,从叶子节点到根节点路径上所有的节点都必须进行密钥更新,用子节点的密钥对父节点的密钥消息进行加密。例如图 3 中,$m3$ 离开组播组,需要更新 K_{14},K_{18},SGSC 使用组播来分发密钥,首先发送$(K'_{14})_{K1}$,$(K'_{14})_{K2}$,$(K'_{14})_{K4}$ 给 $m1$,$m2$,$m4$ 以更新 K_{14},然后发送$(K'_{18})_{K'14}$ 给 $m1$,$m2$,$m4$,$(K'_{18})_{K58}$ 给 $m5$,$m6$,$m7$,$m8$ 以更新子组密钥 K_{18}。

3.3　组密钥的更新与分发

组播子组划分算法可以将整个组播组划分为一些局部区域的子组,它能够根据成员加入或离开的变化实现子组的生成、撤销,确定子组数目的变化。每一个子组由一个成员充当子组安全控制器的角色,子组内已经通过逻辑密钥树协商生成子组内的子组密钥。组播组的控制器或密钥服务器需要将组密钥安全分发给各个子组的安全控制器,因为子组安全控制器的数目远小于组播组成员数目,组控制器密钥更新负载得到有效的降低。组控制器将组密钥分别用各个 SGSC 的公钥加密后,发送给各个 SGSC,SGSC 在接收到组控制器发送的组密钥后,将该密钥用子组内生成的子组密钥加密,然后组播发送给子组内所有的成员,至此完成组密钥的安全分发。当各个子组内成员关系发生变化时,由 SGSC 负责逻辑密钥树的更新,生成新的子组密钥后,同时向组控制器中心发送组密钥更新请求消息,组控制中心接受到密钥更新请求的消息后,立即启动组密钥更新,并将更新的组密钥重新加密发送到各个 SGSC,SGSC 负责将新的组密钥安全分发给子组内成员。

3.4　协议性能分析

协议通过一个成员发现协议和组播组的划分算法,将整个组播组划分为若干个子组,算法的执行需要一定的时间,在协议的初始化阶段完成;对于划分子组的密钥管理,密钥更新的完成需要占用带宽和进行密钥更新的计算,这里的计算与其他密钥管理方法类似,因此主要从协议通信带宽负载方面来分析协议的性能。

采用组播子组生成算法来划分组播组,对于组播源,周期性的多播一个心跳包消息给组内所有的成员,另一个是每一个成员周期性的多播一个 TTL_Scoped 消息给覆盖树中它的父节点与所有的孩子节点。在组播初始化阶段,通信开销所占用的带宽为组内成员总数 N 的常量阶,即 $O(N)$,忽略其他的计算开销。采用子组安全控制器 SGSC 实现二级方式的密钥管理,对于子组内成员的密钥管理,采用逻辑密钥树协议 LKH 方法,在组规模较小时能取得较好的性能。

在全局密钥更新方面,这里由 GSC 负责对各 SGSC 管理,有效地降低 GSC 作为密钥分发中心服务器的负载,对于各个子组内的密钥更新,成员叶子节点数目在 $k \sim 2k$ 之间,采用 LKH 方法,协议的通信带宽负载为 $O(\log k)$。

4　结语

目前组播密钥管理的框架性协议并没有最后定型,可选择的方案有成熟的集中控制式、分层式、分布式等多种密钥管理方案,这些方案有结合网络层组播的,也有结合 IP 组播的。我们倾向于结合实际网络的结构,在应用层实现组播密钥管理协议,更具有一般的普遍性与实用性。本文采用成员发现协议,通过对组播树结构的处理,避免了集中式方法的缺陷,有效地降低了组的规模,采用现有策略构造一个二级层次结构的密钥管理方案,该协议取得了较好的可扩展性,有效地降低了“1 影响 N”的问题。如何取得较好的可扩展性,有效的降低密钥更新的代价,在计算负载和通信负载、密钥存储量等方面的性能取得一种折衷的效果,是值得进一步研究的问题。

参考文献:

[1] WALLER DM, HARDER EJ, AGEE RC. Key management for multicast: Issues and Architectures[S]. RFC 2627, June 1999.

[2] CHANG K-C, CHAN S-HG. Key management approaches to offer data confidentiality for secure muliticast[J]. IEEE Network, Sep/Oct 2003:30 - 39.

[3] WONG C, GOUDA M, LAM S. Secure group communication using key graphs[A]. In Proceedings of the ACM SIGCOMM'98[C], Oct 1998.

[4] IOLUS SM. a framework for scalable secure multicasting[J]. Proc ACM SIGCOMM'97, 1997:277 - 288.

[5] BANERJEE S, BHATTACHARJEE B. Scalable secure communication over IP Multicast[A]. JSAC Special Issue on Network Support for Group Communication[C], 2002, 20(8):156 - 163.

[6] HUANG J-H, MISHRA S. Mykil: A highly scalable key distribution protocol for large group multicast[C]. ICDCS 2003.

[7] 徐明伟,董晓虎,徐恪. 组播密钥管理的研究进展[J]. 软件学报, 2004, 15(1):141 - 150.