一种集中式可视会议的安全解决方案

A Security Scheme for the Centralized Video Conference

席国宝 陈惠芳 （杭州 浙江大学 信电系 310027）

摘要：简述了集中式可视会议系统和组播的安全要求，主要介绍了一种结合组播密钥管理和组播安全策略，应用于集中式可视会议的安全解决方案，从而提高可视会议的整体安全性能。

关键词：可视会议 组播安全 密钥管理 组安全策略

1 引言

可视会议(Video Conference)系统是通过网络通信技术实现的虚拟会议，是支持人们远距离进行实时信息交流与共享、开展协同工作的应用系统。可视会议系统通过网络传送成员的视频与音频信息，极大地方便了成员之间真实、直观的交流。目前可视会议在技术发展上已经大大的提升，在满足传统可视会议的同时，还能够提供更加丰富的数据会议功能，比如：会议过程中协同讨论、程序共享、投票、资料分发、视频广播、白板等功能。

从结构框架划分，可视会议系统可分为集中式和分布式两类。而集中式的可视会议系统的结构清晰、实现简单、管理方便，应用较为广泛。图 1 是集中式可视会议的典型网络结构。多点控制器(Multipoint Control Unit，简称 MCU)将所连接的可视会议终端的视、音频数据通过网络传送到视频服务器上进行保存，而视频服务器通过组播的方式向各个终端传送发言者的视、音频数据和其他一些数据。会议主席通过控制台实现会议的发起、成员的加入、发言权的授予、会议的结束等功能。

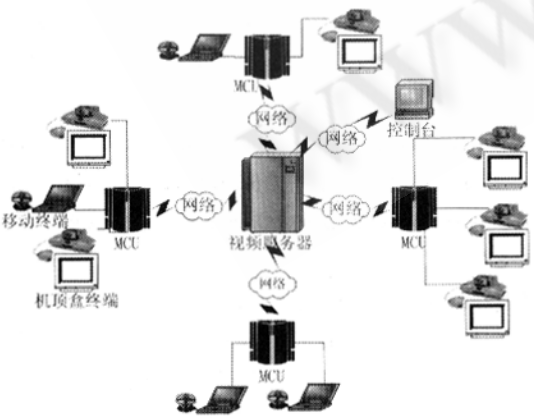

图 1　集中式可视会议的网络框架

可视会议一般是通过向加入特定 IP 组播组的会议成员组播发送数据来实现实时通信的。而基于 UDP 的组播传输方式没有实现任何的安全保证，所以只简单地使用组播实现传输的可视会议系统是相当不安全的。这样的可视会议系统容易造成会议内容的外露，重要数据的被截取等情况。基于此，我们有必要在可视会议系统中引入 IP 组播的一些安全解决方案，提高整个可视会议系统的安全性。

2 组播的安全要求

组播的安全要求主要有四个方面[4]：

组播数据机密性：当数据在公共的 Internet 上传输时，需要有一个机制来防止非认可的数据获取。

组播数据源认证：利用密码学方法保证数据源的辨别，这种认证还包括了数据一致性的证明。

组播安全策略：正确的定义、实现和管理组播安全的多种机制的策略是非常重要的一个环节。

组播组的密钥管理：利用属于同一个组播组成员共享的组密钥来实现数据包的安全。而这个组密钥需要在一个成员加入(或离开)组时更新，以达到后向访问控制(或前向访问控制)。发送者和接收者利用组播组密钥实现加密和解密。组播组密钥管理方式可以分为三个类型：集中控制式、分布式和分层分组式。

集中控制式组播密钥管理方案：存在一个结点，即根(Root)或组控制器(Group Controller，简称 GC)负责全组的密钥生成、分发和更新。这一方案有利于组播的管理，可以方便地实施身份认证等措施，很多组播应用在本质上存在着集中控制，适合采用集中控制式的组播密钥管理。但是这类方案对根的依赖性导致了单一失效点问题，同时 Root 结点可能会因为负载过大成为性能的瓶颈，影响系统的可扩展性。

分布式组播密钥管理方案：分布式的组播密钥管理中，参与通信的结点是对等的，通过某种密钥协商算法生成组密

钥。这类方案不存在集中控制中单一失效点的问题，并且很适合对等的应用模式。但是由于它缺少集中控制，给管理带来了困难。

分层分组式组播密钥管理方案：将参与组播的成员进行分组。每个小组(Subgroup)存在一个控制结点。这些控制结点组成了组播密钥管理的层次 I。小组内部的密钥管理属于层次 II。这两个层次可以独立的选择采用集中控制的管理方式或是分布式的管理方式。在每个层次上采用何种方式就会继承该方式的优缺点。

在组播的四个安全要求中，组播数据机密性是由发送端加密所传输的数据，接收端解密收到的数据来实现的，而数据加密和解密的密钥是由组播密钥管理来实现的。组播密钥管理实现组播中的密钥管理，组播安全策略的功能是管理组播组的成员加入、更新和离开和安全策略的选择等。这两者结合起来才能更好的实现组播应用的安全管理。接下来我们要介绍一种应用于集中式可视会议的安全解决方案。

3 集中式可视会议的安全解决方案

由于集中式可视会议系统本身的架构是采用集中式的 IP 组播的，因而在三种组播安全策略组播组密钥管理方式中，集中式的组播密钥管理方案是最合适的。

3.1 集中式基于树的密钥管理

可以利用逻辑密钥分布树来说明集中式基于树的密钥管理(Centralized Tree－Based Key Management，简称 CTKM)[3]的实现，组控制器和密钥服务器(Group Controller and Key Server，简称 GCKS)[1]将组密钥通过密钥加密密钥分发到分布树中的叶结点(成员)。

图 2 中的 CTKM 的分层树维数为 4，有 16 个成员(成员全部位于叶结点)。在逻辑密钥树中，根(Root)结点维护着一棵密钥树。树上的每个结点都对应一个密钥，树的叶子结点与组成员(不包括 Root 结点)一一对应。Root 结点知道所有的密钥，利用这些密钥来加密组密钥进行组密钥的分发和管理；其余每个组成员知道的密钥集合是位于该组成员对应的叶子结点到根结点的路径上的所有结点对应的密钥，并利用这些密钥来解密被加密的组密钥。所以，利用 CTKM 来实现组密钥的管理和分发。成员利用逻辑密钥分布树上的密钥加密密钥来获得组密钥。视频服务器利用组密钥来加密数据进行组播发送，各终端利用组密钥来解密接收到的数据。每一次加入/离开和每一次周期性的密钥变化时，组密钥和相应的节点密钥会发生变化。对于更新密钥方法，我们采用面向组的策略(Group－oriented strategy)[3]。

3.1.1 离开树

假设成员 m_{16} 离开树，GCKS 删除成员结点 m_{16} 和逻辑密钥分布树中对应的密钥结点 k_{16}，并在离开结点 k_{13-16} 处用 k_{13-15} 替换 k_{13-16}，用 k_{1-15} 替换 k_{1-16}。然后，它创建并向剩下的 15 个成员组播以下消息：

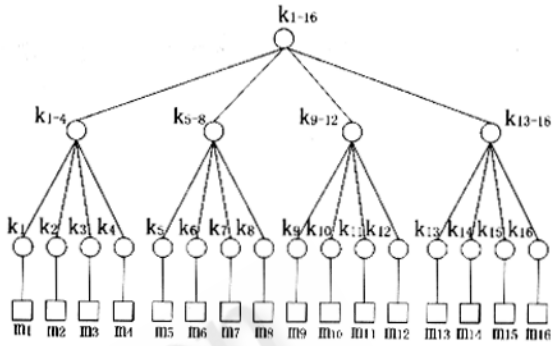

图 2　CTKM 的逻辑密钥分布树

L_0：$\{k_{1-15}\}k_{1-4}$，$\{k_{1-15}\}k_{5-8}$，$\{k_{1-15}\}k_{9-2}$，$\{k_{1-15}\}k_{13-15}$

L_1：$\{k_{13-15}\}k_13$，$\{k_{13-15}\}k_14$，$\{k_{13-15}\}k_15$

GCKS→$\{m_1, L, m_{15}\}$：L_0，L_1

其中，L_0 是利用逻辑密钥分布树的第一层密钥加密后的新组密钥；L_1 是利用用户密钥 k_{13}、k_{14}、k_{15} 加密的离开节点的新密钥。

3.1.2 加入树

新加入的成员被标注为 m_{16}。GCKS 为这个成员构建 k_{16}，创建一个新的成员结点和一个新的密钥结点，并将集合结点配属到接入结点 k_{13-15}。在用 k_{1-16} 替换 k_{1-15} 和用 k_{13-16} 替换 k_{13-15} 后，它创建并发送以下两个消息(第一个是组播到成员 1－15，第二个是单播到新加入的成员 16)：

GCKS→$\{m_1, L, m_{15}\}$：$\{k_{1-16}\}k_{1-15}$，$\{k_{13-16}\}k_{13-15}$

GCKS→m_{16}：$\{k_{1-16}, k_{13-16}\}k_{16}$

3.1.3 周期密钥更新

对于周期密钥更新，GCKS 创建并向整个组组播消息：

k'_{1-16}：新的组密钥 GCKS→$\{m_1, L, m_{16}\}$：$\{k'_{1-16}\}k_{1-4}$，$\{k'_{1-16}\}k_{5-8}$，$\{k'_{1-16}\}k_{9-12}$，$\{k'_{1-16}\}k_{13-16}$，

3.2 组安全联盟模型

一个组安全联盟(Group Security Association，简称 GSA)包括 3 种类别的安全联盟(Security Association，简称 SA)。这三个类别的 SA 对应于三种类型的通信。

3.2.1 SA1

需要在 GCKS 和一个组成员之间建立一个单播通信的 SA。这个 SA 只是建立在 GCKS 和一个成员之间。GCKS 负责组密钥的选择、获取控制和向成员发布组密钥。SA1 是组密钥管理的开始点。在组密钥管理中的成员加入要使用 SA1，控制更新组密钥和分发新的组密钥。

3.2.2 SA2

需要为从 GCKS 到所有的组成员密钥管理控制信息的组播传输建立一个 SA。SA2 不是商议产生的。GCKS 是可信的源，而且是为组成员获得 SA2 的唯一结点。这样，GCKS 还可以控制组播组成员以实现不同的安全策略。组密钥管理的周期更新组密钥时要使用 SA2，控制向整个组成员发布新的组密钥。

3.2.3 SA3

在发送者向接收者组播传输数据信息时需要一个 SA。SA3 也不是商议产生的，所有组成员从 GCKS 获得它。而 GCKS 本身并不使用 SA3，因为 GCKS 不发送实际数据。当视频服务器向接收终端组播传输数据信息时，把数据用组密钥加密发送，接收端用组密钥解密接收到的加密数据。这就是 SA3 的实现。

4 加入安全解决方案的集中式可视会议

采用我们所提出的安全解决方案的集中式可视会议结构如图 3 所示。假设所有的网络设备都支持安全解决方案，我们引入一个可视会议安全服务器作为安全解决方案中的 GCKS。

可视会议安全服务器(GCKS)：能够进行终端接入控制，进行身份认证，防止非授权用户加入；管理组密钥的保存、更新和分发；并能够控制组播组成员实现不同的安全策略。控制台可以控制 GCKS，实现成员管理和策略选择等功能。

GCKS 与每个成员之间有两个 SA：SA1(单播)和 SA2(组播)；中心视频服务器(发送者)和各个终端(接收者)之间有一个 SA：SA3(组播)。中心视频服务器利用组密钥加密数据进行发送。由于现在的可视会议中的视、音频数据通过 MPEG4、H.263、H.264 等格式压缩，这些压缩格式都是分层的，因此为了提高系统性能，可以只对基本层的数据进行加密，提高加密/解密速度[2]。每当有终端要求加入/离开时，整个可视会议的组密钥就会更新，能够实现后向/前向的访问控制。而且 GCKS 能够周期性地更新组密钥，在一定程度上能够防止非授权用户破解组密钥，进一步保证了整个系统的安全。

我们把中心视频服务器也看成一个组播组成员。这样不需要在 GCKS 和中心视频服务器之间建立新的 SA 和相应的组密钥管理机制，利用 CTKM 就可以实现对整个可视会议的组密钥管理。而且可视会议的中的组播组成员的个数不多，不会因为 GCKS 的性能造成瓶颈而影响整个可视会议系统的性能。

5 结束语

简单地使用组播实现传输的可视会议系统是不安全的，容易造成会议内容外露，重要数据被截取等情况。基于此，我们提出了一种应用于集中式可视会议的安全解决方案，以提高可视会议系统的安全性。本文提出的集中式可视会议系统的安全解决方案可以满足组播应用的保密、组成员认证等安全需求，而且该方案结构简单，便于实现，管理方便。在以后的研究中我们将进一步考虑数据的完整性和源认证等问题，更好地加强可视会议系统的安全性能。

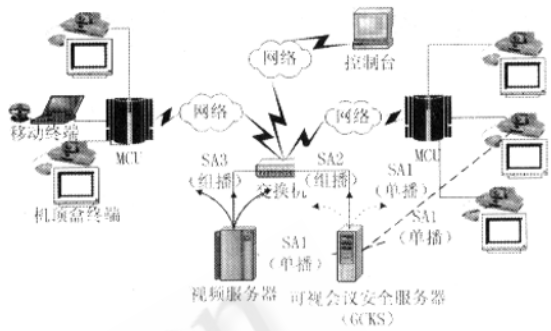

图 3　加入安全解决方案的集中式可视会议系统

参考文献

1 Thomas Hardjono, Mark Baugher, Hugh Harney. Group Key Management for IP Multicast: Model & Architecture[C], WETICE 2001: pp.223－228.

2 Ahmet M. Eskicioglu, Edward J. Delp. An Integrated Approach to Encrypting Scalable Video [C], Proceedings of the 2002 IEEE International Conference on Multimedia and Expo, pp. 573－576, Lausanne, Switzerland, August 26－29, 2002.

3 Ahmet M. Eskicioglu, Mehmet R. Eskicioglu. Multicast Security Using Key Graphs and Secret Sharing[C], Proceedings of the Joint International Conference on Wireless LANs and Home Networks (ICWLHN 2002) and Networking (ICN 2002), pp. 228－241, Atlanta, GA, August 26－29, 2002.

4 Ahmet M. Eskicioglu. Multimedia Security in Group Communicatins: Recent Progress in Key Management, Authentication, and Watermarking [J], ACM Multimedia Systems Journal, Special Issue on Multimedia Security, pp. 239－248, September 2003.

5 Naganand Doraswamy, Dan Harkins.《IPSec：新一代因特网安全标准》[M]，京京工作室 译，机械工业出版社，2000.1。