企业级安全组播体系研究

Secure Multicast Architecture Study of Enterprise

常志勇 （合肥中国科学技术大学 230026）
范植华 （中科院软件所GSL实验室 100080）

摘 要：论文在建立组播隧道转发器的基础上，对组播数据包进行重新封装，通过Internet传输，从而实现在企业内异地网段上进行组播通信。并针对此网络结构，运用了组播密钥分配策略，实现了网络数据传输的安全性。

关键词：安全组播 隧道转发器 密钥分配

随着计算机技术、多媒体技术的发展，以及计算机网络的广泛普及，企业的信息化管理及资源共享得以实现和发展。组播技术作为多媒体会议、邮件群发，网上教学应用系统的传输载体，必将以其巨大的优势在企业中得到广泛应用。

“组播”也称“多点传送”（Multicasting），是一种让数据从一个成员送出，然后复制给其他多个成员的技术。采用这种技术，可有效减轻网络通信的负担，避免资源的无谓浪费。最开始的时候，设计这一技术的目的是弥补“广播”（Broadcasting）通信的不足。假如过度使用广播技术，极易造成网络带宽的大幅占用，影响整个网络的通信效率。多播通信则不同。对一个网络内的工作站来说，只有在其上面运行的进程表示自己"有兴趣”，多播数据才会复制给相应的进程。

1 企业组播系统的建立

由于国内缺乏像Mbone那样直接支持多播的网络，大部分路由器出于防止IP分组泛滥的考虑都关闭了组播路由功能。因此，必须通过相应技术跨越这些障碍来实现组播。在Mbone中，组播是通过隧道技术来实现的：Mbone由Internet上多个组播岛（multicastisland）及连接这些孤岛的隧道组成。在组播岛内，数据以组播方式传输，组播岛之间数据的传输依赖于Internet单播隧道。

为了实现企业各个异地网段的组播通信，在企业的各局域网中，用一台主机做为组播隧道转发器，这些转发器是具有自主能力的实体抽象，具有自治性、协作性等特点。他们通过Internet网，协同工作，将不同组播网段内数据以单播的形式进行传递。也就是说，转发器将本组网段内部的组播Packet，封装为一个个单播的Packet分别发送给其他各个网段的隧道转发器。对于收到的第一个单播Packet则进行解包处理后，将组播Packet在其组播网段内发送。

隧道转发器收到本网段内主机发送的加入组播的注册信息后，将此信息以单播形式向其他转发器发送。每个转发器都维护一个组播映射表，记录着其他转发器传递注册的各个组播地址。当转发器收到本网段内的组播信息后，根据映射表内的信息向相应的转发器进行单播发送。

局域网内的其他主机都嵌入一个Agent客户端程序，全权负责本机的组播事宜。而在主机上运行的应用程序只需处理好与Agent的接口问题，而组播的传输、管理都交由Agent处理，从而简化了各种应用组播的应用程序的设计。当主机的某一应用程序申请加入组播组时，向Agent发送注册消息。Agent将此信息以单播发送给隧道转向器。转发器对此信息进行记录后，加入到组播组内，并向应用

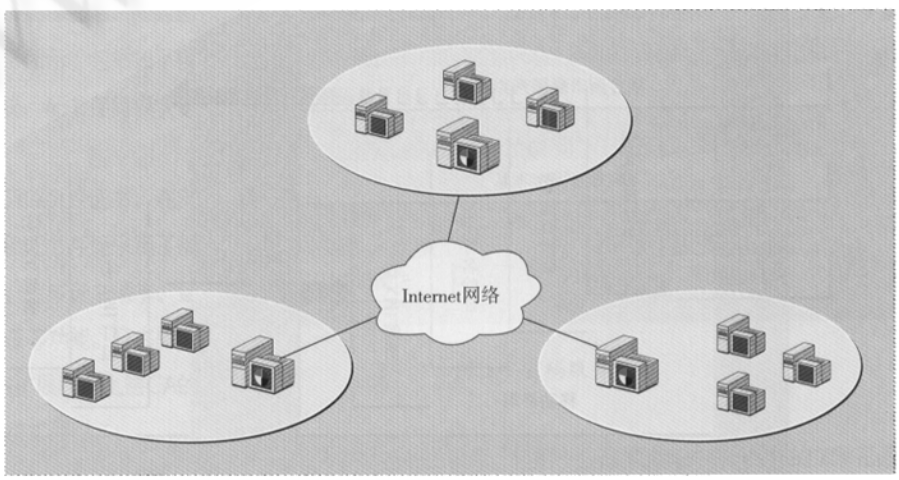

图1 隧道转发器工作示意图

程序反馈加入组播组成功信息。应用程序的数据发送与接收也是通过消息通知Agent，由Agent负责封装或解包组播Packet，并进行发送与接收。通过以上策略解决了组播在Internet网上的传输问题。

2 安全组播的建立

随着组播技术的普及，越来越多的应用提出了安全性要求。因此，针对组播技术自身的特点，构造高效的、可扩展的安全协议和技术已成为当前许多组播应用的迫切需求。

2.1 组播通信的安全需求

一般来说，数据安全性这一概念包括4个基本方面：机密性、真实性、完整性和认可性。要在不安全的网络上（例如Internet）进行安全的数据传输，也要从这4个方面入手。对于网络传输来说，机密性指的是只有真正的接收者才能够接收数据；真实性指的是身份正确的接收者可以检验数据是否一致；完整性指的是正确的接收者可以检验数据是否被改动过；认可性指的是正确的接收者可以向第三方保证数据的来源是一致的。

实际的组播通信中可能出现的攻击类型与单播通信中类型相似，包括：示经授权的创建、更改、删除数据，拒绝服务，非法使用数据等。由于组播通信涉及的范围更广，因此受到的威胁比单播通信更大。

2.2 安全组播组的评价准则

对于安全组播组可以按以下准则进行评判：

（1）系统的鲁棒性。理想的系统在遇到网络或主机故障时其性能会逐步降低，但不会立即完全失效。

（2）可扩展性。理想的设计方案可以处理分布广泛的组，组中的密钥可以频繁更新，组的成员关系可以经常变化。

（3）加入和离开的安全性。在组通信中，加入时的安全性是指任何新的组成员都不能阅读该组中过去的信息，离开时的安全性是指任何离开的组成员都不能阅读该组中当前和未来的信息。

（4）系统需要维护和管理的密钥总数。让应用完全满足以上这些准则是不现实的。根据实际的运行环境，不同的应用可以侧重于某几个方面。

2.3 组密钥管理

由于组播充分利用了网络链接的特点，以一点同时向多点发送，所以以一个组播密钥加密组播信息是非常自然的。组播密钥作为一个安全密钥分配给组内的所有成员。组播密钥加密组播信息后分发给所有组播成员，组成员能够用组播密钥解密这些信息。应用组密钥非常简单，但进行组密钥的分配是复杂的。

当一些组成员离开本组时，所有的组密钥应进行更新，以便离开的组成员无法接收到以后发送的信息。由于我们没有其他的安全组播密钥用以加密更新后的新组播密钥，以安全地发送给组成员，所以我们必须用组成员单独拥有的单播密钥加密新的组密钥或应用其他方法产生新的组密钥。从性能方面的考虑，如果组成员非常多，且只有一个成员负责组密钥的更新工作，密钥的更新操作是相当繁重的。另外以单播的形式向组成员逐一发送组密钥也是很不经济的。

在进行密钥管理策略的选择及确定前，应先了解密钥分配系统的特性，以便有针对性地设计密钥分配系统。

（1）组管理者掌握的密钥数量。在一般的（非扩展性）密钥分配系统中，一个有n个成员的组播组中，组管理者应存储n+1个密钥：组密钥及各个成员的私有密钥或加密会话密钥的密钥（KEK）。在设计的更加完善的系统中，存储密钥的数量可能更多。

（2）组成员掌握的密钥数量。在最一般的分配系统中，每个成员需存储两个密钥，但这种方案需要极高的带宽。因此，在多数高效的分配策略中，都是以增加组成员存储密钥的数量来减少对带宽的需求。

（3）新成员加入及组成员离开的安全问题。新成员加入后应不能接收到以前的消息，这一点可以通过更新组密钥加以保证。新成员加入的安全性是很容易得到保证的，只要用旧的密钥传送新的密钥给所有的组成员就可以了。但组成员离开的安全性就不是很容易保证了。因为离去的组成员掌握着本组密钥，但又没有其他的组密钥可以用来加密新的组密钥，也就不能保证离去的组成员不能读取组播信息。所有的组播密钥分配系统都是针对这样的问题进行设计的。

（4）当成员加入时更新密钥所需传递信息的数量。成员离开时更新密钥所需传递信息的数量：成员离开时最一般的密钥更新策略是组管理员需发送n个消息（以单播向组成员一一发送）。我们可以通过增加密钥存储数量为代价，并且把所有组成员分成多个组（subgroup）的方式，以减少信息传递的数量达到优化的效果。

2.4 组播密钥管理的设计思路

在组播应用不断普及的同时，组播安全性问题也得到了广泛的关注，许多组播加密方法应运而生。但此项工作还仅处在研究阶段，还未最终产生出一套达到共识的解决方案。只有针对不同的系统应用不同的方案。

在进行组播密钥策略的设计时，可以对整个的组播实施组播加密策略，从而在转发器间以单播进行转发时就不再需要另外进行加密了。但这种方案设计起来十分复杂。从现在组播密钥管理的研究成果看，将整个组播按一定策略分成若干子组来进行密钥分配的结构是比较优化的方案。在本系统中，每一个网段都是一个自治结构，它可以看成是整个组播组中的一个子组，而隧道转发器就是这个子组的密钥分配控制器。在子组中应用组播密钥分配策略，而在转发器之间，应用单播的密钥分配策略，从而减少了组播密钥管理的复杂度。当然，由于应用了两种加密方案，在每个转发器上都要增加一次重新

的加解密过程，增加了一定的开销。但总体上还是优化了密钥管理。

2.5 组播密钥管理的体系

一般组播密钥体系由一个组密钥及一组组私钥组成。组密钥用于加密传输的数据，而组私钥用于建立安全通道，安全地传送组密钥。隧道转发器作为本网段子组组播密钥管理的控制中心（GC），它负责本组播组密钥及组私钥的维护。由于GC又是隧道转发器，它的工作负载比较繁重，所以在设计组播密钥管理体系时，应尽量减少GC的工作负担。运用互补的特性，由GC将为加入的子组成员（各主机的Agent）分别编号，并对应每个编号产生一个私钥。则每个子组成员加入组播组后，将分配到除本身编号，并对应每个编号产生一个私钥。则每个子组成员加入组播后，将分配到除本身编号外的所有私钥及对应的编号。当有成员离开时，子组管理员向本组发送更新子组密钥的消息，及离开成员的编号。子组成员接收到消息后，利用此编号对应的私钥及子组密钥，通过使用单向散列函数h产生出新的子组密钥，New SubGrpKey=h(kx,old SubGrpKey)(kx表示离开成员的编号对应的私钥)。由于离开的子组成员并不知道本机编号所对应的密钥，它们可以同时产生一个相同的新的子组密钥。其他组成员及GC都存储着这个密钥，它们可以同时产生一个相同的新的子组密钥。

为更好地说明本设计方案，现举一个例子加以说明。假设一个子组有四个成员，故管理员须产生四个编号及对应的四把私钥K1、K2、K3及K4。用户U1注册后，GC为其传送了编号2-4及对应的私钥K2-K4；用户U2则分配到了编号1、3、4及私钥K1、K3和K4；U3及U4也如此分配。在系统工作过程中，若用户U1离开了，GC则向子组成员发送组播并携带着编号1。由于U2、U3及U4都存储着K1，所以它们可以据此私钥通过单向散列函数同时计算出新的子组密钥。而U1没有K1，所以它不可能计算出新的子组密钥。

此方法使得每个子组成员都将存储N-1把私钥（N表示子组中组成员的个数），增加了密钥存储量，但进行密钥更新时只进行了两次组播，大大减少了网络通信量。

2.6 新成员的加入

当某台主机的Agent向隧道转发器申请加入组播时，GC将为准备加入本子组的新成员分配子组私钥并将子组密钥及组密钥传送给新结点；同时还要更新其他结点的子组私钥。

（1）GC在本机的子组私钥列表中为新的组成员增加一个编号，并相应地产生一个私钥。

（2）GC用子组密钥加密这个编号及私钥后以组播方式传送出去。组成员收到信息后，更新本结点的子组私钥列表。由于此时新加入的结点还未得到管理员要求加入本组的信息，它尚未加入本子组。而且，GC也未为其传送子组密钥，所以新成员不可能得到本结点的编号及相应的私钥信息。

（3）管理员以安全单播将除本成员编号及私钥的子组私钥列表及子组密钥传送给新加入的成员，并要求其加入本组。

（4）新成员收到信息后，将其保存，并调用Jointgroup函数加入到本组。

这样就完成了新成员的加入过程。整个系统又恢复到了一个安全通信的网络结构。

2.7 组成员的离开

当GC得知某一本组成员离开后，立即以组播的形式向本子组其他成员传递更新子组密钥信息，信息中携带了离去成员的编号。子组成员得到信息后，立刻与GC同步进行子组密钥的更新，即利用单向散列函数及离开成员编号对应的私钥进行计算，求出新的子组密钥。同时，子组中的各结点从本结点的子组私钥列表中删除已离开结点的编号及对应的私钥。

2.8 子组密钥的主动更新（Rekeying）

为了组播密钥的安全，在子组密钥长期未得到更新时，GC应进行主动的子组密钥更新。GC应用伪随机数生成器随机产生一个新的密钥来完成密钥的更新。新的子组密钥经过旧的子组密钥加密后，由GC用组播发送给每个子组成员；子组成员收到信息后更新子组密钥，从而达到更新及交换组密钥的目的。

3 结束语

通过以上方案，使组播在企业及Internet网上得到实现。同时通过组播密钥的管理策略，提高了系统的安全性。当然，随着网络技术的发展，象Mbone这样的技术将在网络上得到发展与完善，但这毕竟还需要一段时间。通过隧道技术来实现组播应用，还会有一定的发展空间，也必将为企业带来便捷。

参考文献

1 胡欣、许林英，多播通信中的安全性问题，计算机工程，第29卷，第3期，2003年。

2 屈劲、葛建华、蒋铭，安全组播的Huffman层次密钥管理。软件学报，2003，Vol.14,No.1。

3 杨武勇、史美林、张少华，SmartBoard：全复制结构下电子白板工具的研究与实现。http://cscw.cs.tsinghua.edu.cn/PaperList.htm

4（美）Anthony Jones/Jim Ohlund.Windwos网络编程技术。机械工业出版社，2000年3月。