大型动态群组的多播安全机制

Multicast Security Mechanism for Large Dynamic Multicast Groups

刘 璟 周明天

(电子科技大学计算机科学与工程学院 成都610054)

Abstract Many emerging applications (e g , teleconference, real-time information services, pay per view, distributed interactive simulation, and collaborative work) are based upon a group communications model As the process of proliferation of the Internet progresses, multicast applications are coming to be deployed for mainstream use, and the need to multicast technology will become urgent. As a result, securing group communication (i. e , providing confidentiality, integrity and authenticity of message delivered between group members) will become a critical networking issue. Now, the research of multicast technology has become a new thriving academic field. Many main results converge to such fields as the multicast routing, the flow control, the congestion control and reliable multicast. But the results referred to multicast security are very few, especially in domestic academia. In this paper, we present some main results in the field of multicast security. At the same time, we give a brief view of our solution scheme based on subgroup secure controllers which is superior to the Iolus System[25] and the solution of WGL[30] in scalability and performance. In a word, this paper reflects the new achievements in the field of multicast security.

Keywords Multicast security, Group communication, Access control, Key management, Key tree

1 引言

1.1 多播的应用领域和多播的安全问题

大多数的网络应用是基于客户机/服务器的计算模式并且利用单播(或点到点)分组投送。另一方面,现在很多的应用(如远程会议、多媒体远程教育、实时信息服务、视频点播、分布交互模拟、网络游戏、以及协同工作等)却是基于多播通信模式。即是说,分组从一个或多个授权发送者被传送给为数众多的授权接受者。这种多播模式(或组通信模式)的优点是:节约发送者的资源(通过一次发送实现为多个接受者服务);极大地节约网络带宽资源(更少的通信量)。可以将目前多播技术的应用领域大致分为三大类:

·一对多:音频或视频发布(最简单的模式是目前的电视广播和无线广播);PUSH 媒体(新闻、天气预报);文件分布和缓存(WEB 站点内容更新、镜像或缓存站点内容更新)、实时信息发布和监控(股票报价行情、传感器装置)等。

·多对多:多媒体远程会议、资源同步(目录服务和其它传统的信息系统数据库的同步)、并发过程、协同工作,远程教育、聊天组、分布交互模拟(DIS)、网络游戏等。

·多对一:资源发现、数据收集、网上拍卖、网上投票、网上记帐等。

虽然多播机制能给大型的群组(几万甚至上百万的成员)提供高效的组通信,但是相对于单播机制,多播机制下的路由、可靠性、流量控制、拥塞控制、安全性等问题由于可扩展性问题而变得十分复杂。目前,这些领域的学术研究相当活跃。

随着电子商务的日益全球化和因特网日益商业化,安全基础设施的建立已成为电子商务最迫切的要求。C/S 计算模式下的安全单播通信技术已经较为成熟。但是,安全组通信技术的许多领域还处于初期的学术研究阶段。组通信比单播通信存在更多的安全威胁,一个组通信分组的多个拷贝比一个单播通信的分组要通过更多的网络连接,这可能造成更多的安全漏洞。而且一旦攻击发生,多播机制将使得数量很大的成员受到影响。相信在不久的将来安全组通信(即为在组成员

刘 璟 博士生,研究方向:计算机网络安全、分布对象技术。周明天 教授,博导,研究方向:计算机网络、分布对象技术、并行分布处理和系统集成、虚拟现实。

间传送的信息提供加密、完整性和认证)将成为网络安全中最关键的问题之一。

1.2 多播安全机制不同于单播安全机制的复杂性

从概念上讲,由于每一个点对多点的通信可以分解为一组点到点的通信,于是目前基于安全单播通信的技术似乎可以很自然地扩展到安全组通信上。然而,这种扩展对一般的小型群组还行得通,却不能适用于大型动态群组(成员数目巨大且变动频繁的多播组)。

为了弄清楚这个问题,我们举一个较为具体的示例:先让我们对客户机和服务器间的安全单播通信作一个简要的描述。开始,客户机和服务器使用一种认证协议或服务进行相互认证;然后,产生一个共享的对称密钥(会话密钥)用于双向的加密通信。这一过程可以以如下方式扩展到一个组:存在一个共同信任的组服务器,用它来存储用于实施组访问控制的成员信息。当一个客户机想加入这个组时,客户机和组服务器使用一种认证协议相互认证。当每一个客户机通过认证并被接纳进入该组后,它们分别和组服务器共享一个密钥,这个密钥叫做成员的私有密钥。为了实现组通信,组服务器再给每一个成员安全地发送一个组通信密钥,该密钥为全体组成员所共享,所有的组通信都通过该组通信密钥加密。

对一个有n个成员的组,给所有的组成员安全地发送组通信密钥需要n条信息,这n条信息必须分别用每个成员的私有密钥加密(计算的开销与组的大小n成正比)。每一条信息被单独地用单播方式发送。另一种替代的办法是,这n条信息可以复合为一条信息用多播方式发送。无论哪一种方式通信的开销都与组大小n成正比(通过发送信息的数量或复合信息的大小来衡量)。

我们注意到,对于一次点到点的会话过程,仅在会话建立的开始需要付出会话建立和密钥发送的开销,并只有一次。但是,对组通信的会话过程,这种开销的付出可能持续很长一段时间,因为不断地有成员进入或离开会话。也因为如此,组通信密钥应该频繁地更新。为了达到较高的安全性,组通信密钥应该在每一个成员的加入和离开时更新,以使得以前的成员无法访问目前的通信(后向安全性),而一个新成员无法访问以前的通信(前向安全性)。

考虑一个组服务器,它在每一个成员的加入和离开时产生一个新的组通信密钥。考虑当一个成员离开的情况,以前的组通信密钥不能再使用(因为离开的成员知道),于是新的组通信密钥必须分别用每一成员的私有密钥加密并送给剩下的每一个成员,这样,我们看到当一个成员离开后组通信密钥的安全更新所引起的计算和通信的开销和组大小n成正比,和初始组通信密钥的发送一样。总之,一个成员加入和离开频繁的大型群组给我们提出了一个系统是否具备可扩展性的问题。这时单播的一些安全技术不再适宜。Iolus[10]方案中将上述可扩展问题总结为一个影响n个和一个不等于n个的问题。

上述示例仅向我们展示了多播和单播在密钥管理时的不同,多播通信引入的安全问题远比单播的安全问题复杂。

1.3 多播安全系统中亟待解决的问题

下面,我们列举了一些多播安全系统中亟待解决的问题。多数是所有多播应用都需要考虑的安全问题,在设计系统时必须解决的问题。

a)组成员资格控制和保密:这意味着,应该确保组通信仅能被合法的组成员访问。成员资格控制通常是通过让所有的组成员共享一个组通信密钥。所有的组通信数据都使用这个密钥利用对称加密机制进行加密。

b)分组数据源认证:这是指一个成员能够鉴别组通信的数据是发自组内的成员的过程。这里,组通信数据的接受者一般下能鉴别数据到底是发自组内的哪一个成员,但能鉴别出通信数据是来自组内的某一个成员。我们让所有的成员共享一个组通信密钥。利用这个密钥,再通过信息认证码(MAC)来对所有的通信数据进行认证。

c)个体分组数据源认证:这是指组成员能够鉴别组中发送数据的个体的身份的过程。在多播机制下,信息源认证的问题和在单播机制下有其固有的不同,基于单一MAC的解决方案(如IPSec中用到的)在这里不再适用。

d)安全系统的性能:因为多播群组通常有很大数目的成员,从几百,几十万到上百万。因此我们建立安全系统必须考虑系统的性能和可扩展性。我们列出可能影响系统性能的一些因素作为系统的性能参数:数据分组引起的延迟,带宽和管理开销;控制分组引起的延迟、带宽和管理开销;组初始化、成员的增加和删除操作付出的开销;发送初始化操作付出的开销;恢复操作引入的开销等。

其他安全问题,如匿名性、防抵赖、服务的可用性等问题我们就不在这里作详细阐述,由于这些问题跟具体的应用环境有关。

2 多播安全领域国际研究动态

多播安全的研究是目前计算机网络安全研究领域中一个较新的领域,有价值的研究成果还不多。国内的研究成果更是少见。国外的主要研究成果涉及三个重

要的方面：组秘钥管理，分组数据源认证、组成员资格的撤回。

2.1 组秘钥管理

该领域的工作集中在建立和管理一个为所有成员共享的通用组秘钥。该秘钥用于对数据的加密和组认证，但不能用于数据源认证、组管理和成员资格的撤回方法紧密相关，因为应该防止一个离开的成员能继续对组通信的数据解密。

GKMP 协议[7,8]为多播组的每一个成员产生和维护对称秘钥。在这个协议中，一个多播组有一个专有的组控制器(GC)，它负责管理组秘钥。GC 在与一个被选择的组成员的共同操作中产生组秘钥。然后，它和每一个成员联系并使允许成员进入组的许可有效，接着给成员发去组秘钥(用 GC 单独和每一个成员互相共享的秘钥加密)。这种办法可能存在可扩展性的问题，因为仅存在一个实体 GC，它负责向所有的组成员发送秘钥。

可扩展多播秘钥分配方案(SMKD)[3]是基于核心基本树路由算法(CBT)并使用一种可扩展的方法提供到一个 CBT 组树的安全连接。然而，这种方案缺点是与特定的路由协议相关，不提供路由和安全机制间的分离。(特别地，这种方案给予路由器很高的信任，由于在传送树中的每一个路由器作为组控制器都得到相同的秘钥)。

MKMP[6]秘钥管理协议使得初始的秘钥管理器以一种动态的方式把秘钥分配权力委派给被选定的其它组。它首先产生组秘钥。然后通过向申请这些成员组的多播组发送信息的方式把秘钥分配权力委派给选定的成员组。这个信息包含秘钥和访问控制列表，而且仅能为被申请的成员 组解密。当它们得到这个信息后，它们就可以作为组秘钥管理器开始运行。这种动态的方法有一个好处是：组的拓扑结构能够在线自适应。MKMP[6]为整个组使用一个唯一的秘钥并且不需要对有效载荷采用 hop-by-hop 方式的解密和重新加密。

Iolus 方案[10]通过引入所谓的"安全发送树"来处理可扩展性问题。多播组被划分为一些子组，它们通过分层的方式被安排起来。存在一个组安全控制器(GSC)来管理顶级组，而组安全中介(GSI)管理不同的子组。每一个子组都有它自己的子秘钥，该秘钥有它的管理器选定。一个 GSI 知道它管理的子组的秘钥和更高级的子组的秘钥，所以它能够"翻译"去到和来自高级组的信息。这种方案的一个缺点是由 GSIs 解密和重新加密每一个数据包所引入的延迟开销。另外，如何移除不可信任的 GSI 也是一个复杂的问题。

另外存在的分层解决方案如，PACB[1]，它改进了 GKMP[7,8]的一些不足。HCD[4]和 HCM[5]将网络分为许多的区域：多个"叶区域"和一个"主干区域"。不同的叶区域可以使用不同区域内组秘钥管理协议，而主干区域运行一个域间组秘钥管理协议。HCD[4]和 HCM[5]在抗高层接点故障方面比 Iolus 系统具有更强的健壮性，但它们也存在一些与 Iolus 系统相同的缺点。

2.2 分组数据源认证

分组数据源认证有三种级别，其中最基本的级别是一个注册的接收者能够判别接收到的分组是来自注册的组内成员(注册的分组发送者或其他的注册的分组接收者)，但不能知道发送者的具体身份。这种层次的认证仅能保证分组不是来自安全组以外的某个人。第二种级别的认证是注册的接收者能判别分组是来自注册的分组发送者。这种层次的认证能保证分组是来自某一个注册的分组发送者而不是来自其他的注册的分组接收者或组外的外来者。第三种级别，也是最吸引人的一种认证形式，它使得分组的接收者能够精确地鉴别出分组发送者的身份，目前的研究主要集中在第三种认证级别上。为了实现第一种级别的数据源认证，让所有组成员共享一个秘钥并使用信息认证码(MACs，如 HMAC[9])就足够了。然而，这种方法并不能满足第三种级别的数据源认证的要求，它不能用于认证一条信息是来自一个特定的成员。

如果信息的发送者使用数字签名方案对信息进行签名，第三种级别的数据源认证就可以办到。然而，计算和验证数字签名的计算复杂性以及签名的长度(认证信息必须包含在每一个分组中，使得签名的长度至关重要)将对系统性能造成影响。举例来说，目前的高端工作站每秒能够产生50个1024-bit 的 RSA 数字签名。而一些多播应用需求的分组吞吐率超过了每秒50个分组的速率，即使吞吐率要求较小的多播应用也不可能将宝贵的 CPU 周期中的一大部分用于分组签名。可以通过显著减少验证算法复杂性的方式来使 RSA 数字签名成为一种较为吸引人的分组签名方案。

我们也可以使用基于椭圆曲线的分组数字签名方案，这种方案相对其他签名方案在计算和通信量要求上较小。另一种较为有趣的方法是使用在线/离线数字签名方案 EGM[3]。

文[14]针对数据流的数字签名也作了讨论，他们的设计目标是提供高效的、延迟有界的数字签名，以及对个体分组的高效验证(这样就解决了不可靠通信的问题)。这种方案在 Client/Server 模式下具有很高的效率，因此它已经被提议为视频和音频的 RTP(Real-Time Transport Protocol)提供认证，然而在更多一般的场合(DIS，网络游戏等)这种方案就存在一些实际的缺点：延迟和将发送方的分组聚合成组不适合端到端的交互多播应用(DIS，网络游戏等)，因为附加于每

条信息的认证信息的大小不固定、没有提供用于平滑处理器峰值负载的机制。Cannetti 等[2]提出的一种数据源认证方案是基于高效的 MACs 而不是公钥数字签名。

2.3 组成员资格撤回

为了防止新加入的组成员访问他们加入前组内被发送的数据，同样为防止离开的组成员访问他们离开后组内被发送的数据，需要组控制器无论在任何时候，只要有组成员资格发生变动，都要更新组秘钥。

为了去除不可信成员，许多组秘钥管理协议 GKMP[7,8]、SMKD[3]、MKMP[6]中采用的方法是：产生一个新的组秘钥并把它发送给所有剩下的组成员（使用每一个组成员单独和组控制器共享的秘钥加密），这样就从本质上建立了一个没有不可信成员的新的多播组，然而这种方法不具有可扩展性。

如组秘钥管理一节中所述，另一种方法是将整个多播组分为具有独立子组秘钥的多播组。当一个成员被删除时，仅需要给被删除成员所在子组的成员发送单独加密的信息。这类方法如 Iolus[10]，PACB[11]，HCD[4]，HCM[5]更具有可扩展性。它需要每一个子组都包含一个可信的子组控制器（如 Iolus[10]系统中的组安全中介）。但是如果子组控制器变为不可信时，就应该运行一个更为复杂的资格撤回程序（这一点这些草案都没有描述）。

WGL 的方案[13]引入了密钥树概念，这是大型动态多播组密钥管理和组成员资格撤回问题方面的一个重要突破。密钥树在密钥管理方面的确具有相当的高效性和高度的安全性。WGL[13]方案的特例就是 WHA 方案[12]，WGL[13]方案中树的度数是任意的（虽然二叉树能达到最好的通信性能），该方案可以减少需要发送的组成员资格撤回信息和减小发送信息的大小。另外 CGIMNP 方案[2]在组成员增加时不会增加系统开销。基于被使用的加密函数的安全性（即是说伪随机性），CGIMNP 方案的安全性能够被严格地证明。基于密钥树的密钥管理方案存在的问题是：它需要一个可靠的多播基础设施；虽然这些方案能高效地处理大型的群组，但它们不适合处理大型的动态的群组（成员资格变动频繁的群组），因为不论如何高效地更新组密钥，仍然需要在每一个成员发生变动（离开或加入）的时候，向每一个组成员发送更新的组密钥。基于这一点，这一类的方案适合作为子组的密钥管理方案。

总之，这些成果本身都存在这样或那样的问题，并没有完善地解决相关领域的问题。多播安全领域还是一个比较年轻的学术领域，还有很多问题亟待解决，随着时间的推移相信会有更多的新技术取代或改进上述的种种方案。

3 我们目前的研究进展和成果

我们目前对多播系统安全的研究集中在组秘钥管理、组成员资格撤回和访问控制这几个方面。提出了一种基于子组安全控制器的组通信密钥管理和访问控制方案，该安全方案改进并解决了 Iolus[10]系统和 WGL 方案[13]中存在的一些问题[15]并简化了多播组安全访问控制，达到了预期的设计目标和要求。该方案引入了 WGL 方案中的密钥树概念，因为密钥树在密钥管理方面的确具有相当的高效性和高度的安全性。同时提出了子组安全控制器、子组安全密钥树、子组安全控制器密钥树（对密钥树概念的扩充，利用密钥树来管理子组安全控制器而非用户成员）等概念。这就使得我们的方案在运行机制上与 WGL 方案有很多不同之处。该方案的系统框架如图 1。其中 GSC（Group Security Controller）为组安全控制器，SGSC（Sub-Group Security Controller）为子组安全控制器。每一子组内部有一个子组密钥树由SGSC管理。整个系统框架的核

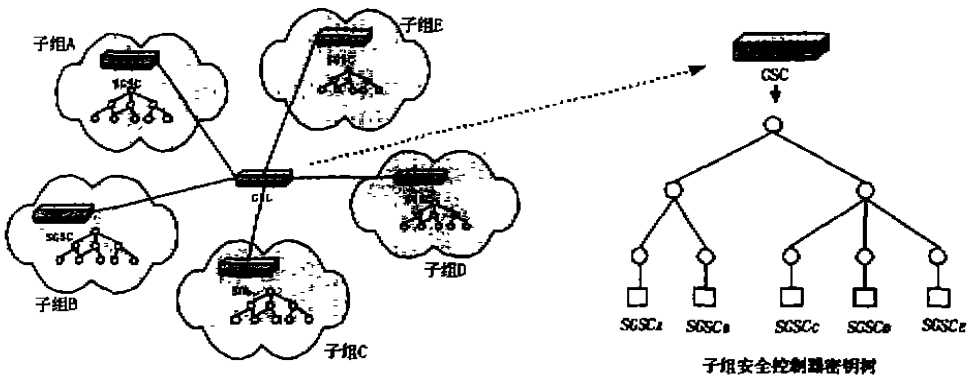

图1 系统核心框架示意图

心思想是：GSC 通过 SGSC 密钥树向各 SGSC 安全发送更新后的组通信密钥，而各 SGSC 一方面通过子组密钥树更新子组组密钥；另一方面向各子组用户成员安全发送更新后的组通信密钥（用子组组密钥对其进行加密），我们同时提出的系统核心算法和协议：组通信密钥更新算法和协议解决了组通信密钥的安全更新、访问控制和子组安全控制器的不可信等问题。详细算法和协议参见文[15]。

结论 这篇综述简要地介绍了目前多播安全的几个主要研究领域和国际上的主要研究成果，这些成果本身还不十分完善，并没有完全解决相关领域的问题。目前，一种较理想的解决方案是：针对具体的应用环境，集中上述多种方案的优点并有机地组合起来。当然，多播安全领域还是一个比较年轻的学术领域，还有很多问题亟待解决，随着时间的推移相信会有更多更好的技术取代或改进上述的种种方案。本文中我们提出的一个方案就很好地解决了文[13]的方案和 Iolus 系统存在的一些问题并简化了多播组安全访问控制，达到了预期的设计目标和要求，但我们的系统尚没有解决分组数据源认证问题，在解决该问题后，我们将基于上述思想开发出一个大型动态多播群组的密钥管理和认证系统的原型。

参 考 文 献

1 Ballardie A. Scalable Multicast Key Distribution. RFC 1949, May 1996

2 Canetti R, et al. Multicast Security: A Taxonomy and Efficient Authentication. to be presented at INFOCOM'99

3 Even S, Goldreich O, Micali S. On-line/off-line digital signatures. Advances in Cryptology-Crypto'89. Springer-Verlag LNCS 435, 1990. 263～277

4 Harditono T, Cain B, Doraswamy N. A Framework for Group Key Management for Multicast Security. internet draft draft-ietf-ipsec-gkmframework-00. txt, July 1998

5 Harditono T, Cain B, Monga I. Intra-Domain Group Key Management Protocol. internet draft, draft-ietf-ipsec-intragkm-00. txt, Nov 1998

6 Harkins D, Koraswamy N. A Secure, Scalable Multicast Key Management Protocol (MKMP)

7 Hareny H, Muckenhirn C. Group Key Management Protocol (GKMP) Architecture. RFC 2094, July 1997

8 Harney H, Muckenhirn C. Group Key Management Protocol (GKMP) Specification. RFC 2093, July 1997

9 Krawcayk H, Bellare M, Canetti R. HMAC, Keyed-Hashing for Message Authentication. RFC 2104, April 1997

10 Mittra S. Iolus: A Framework for Scalable Secure Multicast. In Proc of ACM SIGCOMM'97, Cannes, France, Sep. 1997

11 Poovendran R, Ahmed S, Corson S, Baras J. A Scalable Extension of Group Key Management Protocol. In: Proc. of the 2nd ATIRP Conf. University of Maryland, College Park, MD, 1998. 2～6

12 Wallner D M, Harder E G, Agee R C. Key Management for Multicast: Issues and Architecture. internet draft draft-wallner-key-arch-01. txt, Sep. 1998

13 Wong C K, Gouda M, Lam S S. Secure Group Communication Using Key Graphs: [Computer Science Technical Report R 97-23]. SIGCOMM'98. Also, University of Texas at Austin

14 Wong C K, Lam S S. Digital Signatures for Flows and Multicasts: [Computer Science Technical Report TR 98-15]. IEEE ICNP'98. Also, University of Texas at Austin

15 刘璟、周明天. 大型动态多播群组的密钥管理和访问控制方案. 软件学报审稿中

（上接第73页）

27 Poole D. Average-case analysis of a search alagorithm for estimating prior and posterior probabilities in Bayesian networks with extreme probabilities. In: Proc. 13th Intl. Joint Conf. On Artificial Intelligence. Chambery, France, August 1993

28 Poole D. The use of conflicts in searching Bayesian networks: [Technical Report 93]. Department of Computer Science, University of Britis Columgia, March 1993

29 Poole D. Probabilisftic partial evaluation: Exploiting rule structure in probabilistic inference. In: Proc. of the Fifteenth Intl. Joint Conf. on Artificial Intelligence. 1997

30 Shachter R, et al. Symbolic probabilistic inference in belief networks. In. Proc. Eighth National Conf. on AI, AAAI, August 1990. 126～131

31 Shachter R D, Peot M A. Simulating approaches to general probabuilistic inference on belief networks. In. Uncertainty in artificial Intelligence 5. Elsevier, Amsterdam, 1990. 221～231

32 Shimony S E, Charniak E. A new algorithm for finding MAP assignments to belief networks. In: Proc Sixth Conf. On Uncertainty in Artificial Intelligence. Cambridge, Mass., July 1990. 98～103

33 Shwe M, et al. Probabiklistic didagnosis using a reformulation of the INTERNIST-1/QMR knowledge base I. The probabilistic model and inference algorithms. Methods of Information in Medicine, 1991, 30: 241～255