广西科学院学报
Journal of Guangxi Academy of Sciences
2006,22(4):263～265
Vol. 22,No. 4 November 2006

一种新的组播安全通信密钥管理协议*

A New Key Management Protocol of Multicast Secure Communication

魏楚元[1],李陶深[2],吕 橙[1]
WEI Chu-yuan[1],LI Tao-shen[2],Lü Cheng[1]

(1. 北京建筑工程学院计算机科学与技术系,北京 100044;2. 广西大学计算机与电子信息学院,广西南宁 530004)
(1. Department of Computer Science and Technology, Beijing Institute of Architecture and Engineering, Beijing, 100044, China; 2. School of Computer, Electronics and Information, Guangxi University, Nanning, Guangxi, 530004, China)

摘要:在分析群组通信安全问题的基础上,采用一种折中的方法,提出一种混合的分组分层的组播群组密钥管理协议,以解决组规模较大的安全组播应用中存在的问题。新的组播安全通信协议有效地降低了协议通信带宽、解密和加密计算等负载,具有较好的可扩展性,适合大型动态组播。

关键词:组播 群组通信 密钥管理
中图法分类号:TP393 **文献标识码**:A **文章编号**:1002-7378(2006)04-0263-03

Abstract: The group key management scheme is a basic technique in the security of group communication. A hybrid protocol of grouped and layered key management is presented in order to solve the problems existed in application of secure group communication in lager scale.

Key words: multicast, group communication, key management

安全群组通信[1](SGC)是当前国际上分布式计算领域和信息安全领域研究的一个热点问题。群组通信的应用可以通过 IP 组播方式传输数据给群组内的所有成员,能够有效的节省带宽。但是,IP 组播没有提供有效的机制确保只有得到授权的群组用户才能访问被传输的数据,任何一个支持组播的主机都能够发送一个 Internet 组管理协议(IGMP)报文给它最近的路由器,请求加入一个组播群组,而已有的组播协议都没有提供相应的安全机制进行组成员身份认证和存取控制[2]。一个安全群组通信系统提供的基本安全服务应包括数据保密性、完整性、成员认证和存取控制等。实现对信息的限制访问通常采用的办法是对群组的消息进行加密。如果所有的群组成员都共享一个共同的密钥,就可以很方便地实现这些安全服务,这个共享的密钥被称为群组密钥。如果规定只有群组的成员才能获知组密钥,这样可以控制只有持有组密钥的群组成员才能解密群组的消息。因此,研究群组密钥的生成、分发和更新维护的机制成为了群组密钥管理机制需要解决的主要问题。

近年来国内外很多研究机构和学者都对此进行了研究,提出了很多面向群组的密钥管理协议,以解决安全群组通信系统中安全问题[3,4]。本文在分析群组通信安全问题的基础上,采用一种折中的方法,提出一种混合的分组分层的组播群组密钥管理协议,以解决组规模较大的安全组播应用中存在的问题。

1 群组通信的安全问题

群组通信系统的开放环境存在着潜在的安全问题,而组播作为一种新的数据传送机制,在安全性方面也存在不足。由于组播开放性的特点,组播通信比单播通信更容易受到攻击,具有更大的安全风险,而且容易受到拒绝服务攻击(DOS)。组播协议在安全性方面主要存在以下不足[3]:

(1)现有组播协议没有提供对组播群组中成员

收稿日期:2006-07-21
作者简介:魏楚元(1977-),男,湖北武汉人,硕士,讲师,主要从事计算机网络安全、安全多方计算研究。
* 本文得到广西自然科学基金项目(桂科自 06400026)和广西留学回国人员科学基金项目(桂科回 0342001)联合资助。

资格进行认证和访问控制相应的机制，这使得攻击者容易模仿或欺骗组内某个合法成员。

(2)IP 组播的组地址是公开的，这使得攻击者很容易找到一个组播组的 IP 地址，并成为其合法的组成员之一。

(3)组播中没有提供任何能阻止组成员或者非组内成员向这个组发送数据的机制。如果组的规模比较大，一旦攻击者恶意地向这个组发送大量数据包，就很容易造成网络拥塞从而导致拒绝服务。

(4)相对于单播通信，组播报文将在更广泛的网络上传输，这无疑给攻击者更多机会拦截和窃听数据报文。

鉴于组播协议存在的不足，必须研究一种有效的组管理和访问控制机制，确保只有合法的参与方能获得发给这个组的数据。

2 一种新的组播密钥管理协议

针对群组通信的安全问题，需要采用组播密钥管理协议保证网络的安全性，如保密性，完整性和身份认证、抗共谋勾结等，甚至尽可能地有一定的容忍入侵和容错机制，确保密钥分发与更新在不可靠的网络环境下正确执行。

2.1 组播密钥管理的性能考虑

组播密钥管理协议的性能主要考虑两个方面的因素：(1)“1 影响 N” 问题。为了保证前向和后向保密性，对于组播组中每一个成员的加入或退出，都需要更新组密钥。当组成员规模 N 较大时，一个成员的加入或退出带来的是全局组密钥的更新，即“1 影响 N” 问题，特别当组成员变化频率(组的动态性)较高时，组密钥管理中心负载大幅增加；(2)为了提高组播密钥管理协议的可扩展性，鉴于 Iolus[5]提出的划分子组的思想，将整个组播组划分为若干子组，在组播网络的局部子网中设置子组安全控制器 SGSC，每个 SGSC 拥有局部独立的数据加密密钥，可以有效地分担组密钥管理中心密钥更新的负载，降低了“1 影响 N” 问题，但是局部 SGSC 存在解密/重新加密的负载，对组播的通信带宽和延时有一定的影响。

2.2 新组播密钥管理协议的思路

我们认为可以采用一种折中的方法，解决组规模较大的安全组播应用中存在的问题。我们的思路是：将适用于较小规模组播的集中式方法和大规模组播的分布式子组方法结合起来，在组播密钥管理安全框架基础上，采用一种分组分层式的密钥管理体系结构，组播组由一些分布的组播子组构成，因为组播子组内组成员数目相对较小，采用集中式方法的代表性协议 LKH[3]实现子组内密钥管理，设计了一种混合的分组分层的密钥管理协议，并通过增加签名标记来解决现有密钥管理协议对成员身份认证的不足；同时对以上协议的安全认证做了进一步的改进，使得协议较好地减少了“1 影响 N” 问题，具有较好的可扩展性，尽量降低了组安全代理解密和重新加密的计算负载，取得一种折中的性能。

2.3 基于组安全控制代理的组播拓扑结构

新组播密钥管理协议的拓扑结构如图 1 所示。图 1 描述一种基于代理的动态组播密钥管理协议的拓扑结构，其本质是一种层组式的密钥管理体系结构。

图 1 基于组安全控制代理(GSCA)的组播拓扑结构

基于组安全控制代理(GSCA)的组播拓扑结构将整个组播组组织成一个由多个子组生成的树，每一个子组采用一个密钥管理的 Agent 充当子组安全控制器，负责局部子组内的密钥管理。本文所提出的组播密钥管理协议的框架是一个由组播子组形成的层次结构，整个层次结构形成了一个组播组。拓扑结构中主要的实体有：一个组播源 S 所在的组安全控制器(GSC)、一些分布在局部子网的组安全控制代理(GSCA)和一些用户节点，GSC 和 GSCA 在网络上是分布存在的，它们只是在逻辑上存在一种层次关系，但在分布上并没有任何体现。GSC 设为组播组的管理控制中心，它是初始群组发起者和全局密钥管理中心，它的基本功能是通过向全组成员发送 GROUP _ CONSTRUCT 消息宣布组播开始，在组播过程中管理全局成员控制和通信安全，进行全局密钥控制和组播参数调节。协议拓扑结构图对应的逻辑结构如图 2 所示，GSC 负责管理各个 GSCA，形成了一个逻辑树结构。GSC 管理组播组的数据加密密钥 TEK 和密钥加密密钥 KEK，通过组播网络向用户发送报文，用组密钥 TEK 和 KEK 共同来实现通信安全。GSC 通过 KEK 将 TEK 安全分发到各 GSCA，GSC 开始组播后，它用 TEK 加密组播数据，

不断地通过组播网络发送给各 GSCA,各 GSCA 在接收到组播数据后,进行解密,然后用局部子组的 TEK(由 GSCA 产生,并安全分发到子组内成员)重新加密后发送到子组内的成员用户节点,终端用户节点在接收到组播数据后,用局部子组的 TEK 解密后得到组播数据。

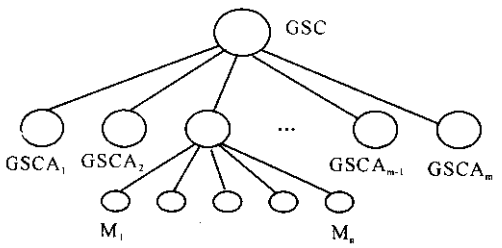

图 2 GSC 与 GSCA 层次结构

2.4 协议性能分析与比较

群组密钥管理协议一般从通信负载、存储负载、计算负载等方面来评价其性能的。从现有的文献来看,在进行理论分析时,很难提供一个精确的数学模型计算出所有密码计算的总数和通信开销等,而且对不同的密码运算所耗费的时间也不相同。现有的研究更多是从通信模式上分析密钥更新协议在通信带宽方面的开销。近期也有研究人员采用实验仿真方法来测试协议的性能,但实验仿真的方法也很难测量协议在密码学运算方面的计算开销,对组密钥管理协议进行实验仿真也是一个值得深入研究的问题。

考虑上述因素,我们采用的方法是,协议尽量采用在计算性能上更好的签名认证方法和密钥生成的方法,如 RSA 签名、基于椭圆曲线密码体制的签名方法,它们具有一些公认的优点。在衡量协议的通信开销时,我们通过网络仿真器 NS2 作为仿真工具,构造群组通信模型,测量协议运行的通信开销。

从密钥管理协议密钥更新时的计算开销、存储需求、通信带宽、延迟等因素,将新组播密钥管理协议与集中式方法的代表性协议 LKH 和分布式子组方案的代表性协议 Iolus 进行比较。为了方便讨论,以一次成员关系变化为例,假设整个组播组的成员数目(组规模)为 $N(N=1024)$,组安全控制代理 GSCA 的数目为 $m(m=8)$,每一个子组的规模为 $n(n=N/m)$。我们在一台 P4 2.6G 的微机上用 DES 算法加密 1MB(2^{20}字节)数据测试出其花费的时间为 41ms,以速率 r 为 100MB/s,组安全控制代理的负载值为 8.2。从表 1 中的结果可以看出,在密钥存储量上,新组播密钥管理协议的性能与 Iolus 协议相当,但好于 LKH 协议;在通信带宽开销上,新组播密钥管理协议的性能好于 LKH 和 Iolus 协议。这说明了新组播密钥管理协议有效地降低了协议通信带宽、解密和加密计算等负载,较好地降低了"1 影响 N"问题,具有较好的可扩展性,适合于大型动态组播。

表 1 组播密钥管理方案的比较

协议	计算开销及延迟	密钥存储量			通信带宽开销
		组安全控制器	组安全代理(中介)	用户节点	
LKH 协议	—	$O(N)$	—	$O(\log N)$	$O(\log N)$
Iolus 协议	$2rDES_t \log m = 24.6$	$O(m)$	$O(N/m)$	$O(1)$	$O(N/m)$
本文协议	$2rDES_t = 8.2$	$O(m)$	$O(N/m)$	$O(\log(N/m))$	$O(\log(N/m))$

3 结束语

本文采用一种折中的方法,提出一种混合的分组分层的组播群组密钥管理协议。通过性能分析对比表明,本文提出的协议性能适中,可以较好地解决规模较大的安全组播应用中存在的问题。

参考文献:

[1] GREGORY V. CHOCKLER, IDIT KEIDAR, ROMAN VITENBERG. Group communication specifications: A comprehensive study[J]. ACM Computing Surveys, 2001, 33(4): 1-4.

[2] HARDJONO T, TSUDIK G. IP multicast security: issues and directions[J]. ACM, 2000, 33(4): 792-807.

[3] WALLNER D, HARDER E, AGEE R. Key management for multicast: issues and architectures IETF RFC 2627[EB/OL]. (1999-06-10). http://www.ietf.irg.

[4] SANDRO, RAFAELI, D HUTCHISON. A survey of key management for secure group communication[J]. ACM Computing Surveys, 2003, 35(3): 309-329.

[5] MITTRA S. Iolus: a framework for scalable secure multicasting: in proceedings of ACM SIGCOMM'97 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, cannes, France, 1997[C]. [S. L]: [s. n], 1997: 277-288.

(责任编辑:韦廷宗)