组播安全中的组密钥更新问题

Rekeying Group Key for Multicast Security

张 斌 邬江兴

(国家数字交换系统工程技术研究中心 郑州 450002)

Abstract Security management of group key is becoming a key problem of multicast security. This paper summarizes five kinds of policy of rekeying group key and some of evaluating criteria of rekeying method, then discusses rekeying group key problem based on some current group key management method. Finally, a method to resist preventing rekeying message from transmitting is proposed.

Keywords Group key, Rekeying group key, Multicast security

1. 引言

随着 Internet 网的广泛应用,组播也得到了迅速的发展,诸如 Internet 视频传输、消息发布、股票报价、软件更新、在线视频游戏等应用。使用组播可以节省发送者资源、减少网络流量。组播相对于单播的主要优点是它允许发送者对每个报文只发送一次,由路由器自动地转发报文到每个目的接收者,可以最小化网络中传输的报文的拷贝数。然而由于其路由报文到很大的接收组的内在复杂性,使得其可靠性和安全性问题变得比单播更为复杂。在组播安全问题中组密钥的安全管理是一个重要的研究课题,已成为目前研究的焦点,而组密钥更新问题是组密钥安全管理的核心问题[1]。组密钥更新指的是为了适应组成员关系的高度变化,同时保证组成员加入或离开组的秘密性(加入秘密性指的是新加入的成员不能得到过去被加密的消息,离开秘密性指的是已离开成员不能得到当前或未来消息)对组通信所使用的组密钥以及用于方便组密钥管理而引入的有关辅助密钥的改变、更新。根据不同的组通信应用安全需要,可以采用下列一些不同的组密钥更新策略。

2. 组密钥更新策略

组密钥更新和组成员关系的变化有着密切的关系,组成员事件(成员加入事件、成员离开事件、成员失效事件和成员被排除事件)的发生对于安全性要求较高的系统往往要触发密钥更新事件的发生,要求组管理者分配一个新的会话组密钥,用以确保加入秘密性和离开秘密性。根据对不同事件的安全敏感性,一般可分为以下策略:

1)时间敏感性组密钥更新策略 这种策略要求周期性地更新组密钥,与组成员事件无关,试图通过只在有限的时间内使用组密钥来抵抗密码分析攻击。攻击者也可能通过阻塞新的组密钥的传递来促使组成员继续使用当前的组密钥加密通信,因此使用这种策略,在当前组密钥超期而新的组密钥又没有被建立的情况下,组成员将不再使用当前过期的组密钥进行通信。

2)成员离开敏感性组密钥更新策略 在发生成员离开、成员失效和成员被排除事件时,进行组密钥更新,这种策略要求已经离开组的组成员不能访问当前或未来的组通信内容。

3)成员加入敏感性组密钥更新策略 只在发生成员加入事件时进行组密钥更新。刚加入组的任何成员不能访问在其未加入此组前这个组的任何通信内容,这种策略不保证已离开这个组或被从此组中排除的前组成员不能访问当前的组通信内容。

4)成员关系敏感性组密钥更新策略 任何组成员事件都可触发密钥更新,这种策略保证了加入秘密性和离开秘密性,可以说是成员离开敏感性策略和成员加入敏感性策略的结合。很明显,这种策略提供的安全性最高。

5)其它组密钥更新策略 由于具体应用的安全需要不同,可能需要以上策略的组合或使用不同的策略,例如在某些商业应用中,只有当某些重要的组成员离开时才进行组密钥更新。时间敏感性策略可以和任何其它策略相结合,用以阻止攻击者长时间阻塞密钥更

张 斌 博士生,主要研究方向为计算机网络安全。邬江兴 教授,博导,主要研究方向为交换理论、通信网、计算机网络安全和高速路由器等。

新消息和抵抗密码分析攻击。

3. 评价组密钥更新方案的标准

1)可放缩性　组密钥更新方案是否能处理很大的、在网络上广泛分布的组，是否能以小的代价处理频繁的组密钥更新，即适应高度动态的组成员关系。

2)组控制器和组成员拥有密钥数　简单密钥分配中心 SKDC(Simple Key Distribution Center)方法的组控制器需要存储 n+1 个(n 为组成员个数)密钥，其它方案可能存储更多的密钥以进行有效的密钥更新。SKDC 方法的每个组成员只需要存储 2 个密钥，但这种方法为了进行组密钥更新所消耗的网络带宽无法接受，其它方案可能要求每个组成员存储更多的密钥以减少对网络带宽的需要。

3)加入和离开秘密性　根据不同的组密钥更新策略，保证加入秘密性或离开秘密性，或者两种都保证。一般地，加入秘密性可通过用老的组密钥加密新的组密钥组播传输至整个组而有效地达到，而对于离开秘密性则需要新的方法。

4)组成员加入或离开时更新密钥所需消息数目　为了有效地在组成员加入或离开时进行组密钥更新，需要尽可能地减少用于此目的更新消息的数目，尽量减少占用网络带宽。

5)组管理者计算量　在组成员加入或离开时，为了保证加入秘密性和离开秘密性，组管理者必须产生新的组密钥，加密、签名后向组成员进行传递，组管理者计算量的大小直接影响到组密钥更新的效率。

6)组密钥管理的安全性　组的安全将不依赖于安全性最差的成员的安全能力，如果一个组成员的密钥被有意或无意地泄露，组的安全将不会被完全地泄露，并能迅速地排除已泄露密钥的组成员，被泄露所影响的将是接收组的一小部分。

4. 两种重要的组密钥更新方案

目前，已有多种组密钥管理方案用以保证组播安全，它们采用了不同的组密钥更新方法处理组成员的组密钥更新问题。

SKDC 方法是最简单的密钥分配方法，组管理者和每一个组成员共享一个密钥，它所采用的组密钥更新方法是：组管理者顺序地使用与每个成员共享的密钥传递组密钥组给这个成员，在一个具有 n 个成员的组中，添加或排除一个成员组管理者必须执行 n+1 或 n-1 次加密并传递 n+1 或 n-1 次新生成的组密钥，这种方法不具有可放缩性，组管理者计算量大且拥有的密钥数为 n+1，只适用于相对小的组。

组密钥管理协议 GKMP(Group Key Management Protocol)靠的是每个组成员都拥有的组密钥加密密钥 GKEK 来进行组密钥更新[2]，且只适用于时间敏感性组密钥更新策略，单个组成员的 GKEK 泄露将使整个组失去安全，不支持成员的离开敏感性密钥更新策略，由于每个组只有一个组控制器，因此还存在单点失效和可放缩性问题。

可放缩组播密钥分配协议 SMKD(Scalable Multicast Key Distribution)基于 CBT 组播路由协议提供可放缩的组密钥分配方案。在 CBT 树中，由树的核心负责产生组密钥和组密钥加密密钥，加入树中的路由器也被授予认证和密钥分配的能力，具有高度的可放缩性[3]，然而这种安全机制依赖于特定的路由协议，也不支持成员离开敏感性密钥更新策略，树中任何一个路由器或成员的泄露都将影响到整个 CBT 树的安全。

Iolus 系统为了进行有效的密钥更新，把一个组播组划分成多个层次化的子组，同时引入了安全分配树的概念，这个树由组安全代理 GSA 组成，根节点的 GSA 称为组安全控制器 GSC，其它 GSA 称为组安全中间人 GSI。GSI 负责管理子组密钥以及本子组和其它子组的安全通信[4]。每个 GSI 在子组内部都实现了加入和离开敏感性组密钥更新策略。这种方案的优点在于把组成员事件变化的影响定位在子组内部，由 GSI 处理，减轻了组控制器的负担和对网络带宽的消耗，同时把安全管理的任务分布在多个 GSI 和一个 GSC 完成。提高了系统抵抗单个控制节点失效的能力，从而改进了整个系统的可靠性。然而，Iolus 系统为了管理组播组需要大量的资源开销，子组间的信息传输多了一次加密和解密操作，最高级节点 GSC 成为系统可靠性和安全性的瓶颈。以上方案要么不适合动态组的密钥更新要求，要么代价太高、安全性较差，为此引入以下两种组密钥更新方案。

4.1　逻辑密钥层次树 LKHT(Logical Key Hierarchy Tree)组密钥更新方案

这种基于树的组密钥更新体制由 Waller 等人[1]和 Wong 等人[5]分别提出，Waller 方案较之 Wong 方案对于组密钥更新需要更少的通信开销，因此以下重点讨论 Waller 方案。

此体制使用 n(n≥2)叉树来存储密钥，在 LKHT 建立阶段通过许可控制之后，每个成员建立一个和组管理者共享的密钥，称为最低级的密钥加密密钥 KEK，这些密钥存储在树中的叶子节点，之后组管理者为每个树中的剩余节点产生密钥，这些节点并不代表实际的组成员，只表示虚拟的层次，属于逻辑节点，主要是用于在组成员发生变化时有效地传递新的密钥，每个成员拥有从代表其叶子节点到根节点这条路径上的所有密钥，根节点的密钥被称为流量加密密钥

TEK 或组密钥，中间节点的 KEK 用于只传播新密钥到特定的有限接收者集合，禁止其它成员解密特定的消息。

假定组播组由 $u_0, u_1, \cdots, u_{n-1}$ 共 n 个组成员组成，若使用二叉密钥分配树，则每个成员需要存储 $\log_2^n+1$ 个密钥。

考虑深度为 3 的二叉树，如图 1 所示，此树可支持 8 个组成员的组播组。

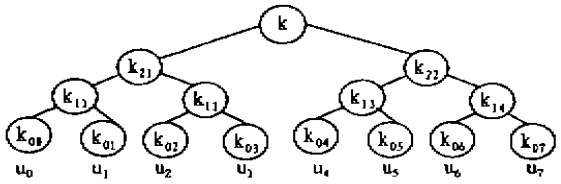

图 1　二叉密钥分配树

假定成员 u_0 离开，采用离开敏感性组密钥更新策略，则成员 u_0 拥有的密钥 $\{k, k_{21}, k_{11}, k_{00}\}$ 将无效，密钥 $\{k, k_{21}, k_{11}\}$ 需要被更新为 $\{k', k'_{21}, k'_{11}\}$，和成员 u_0 拥有部分相同密钥的组成员 u_i ($1 \leqslant i \leqslant 7$) 需要接收这些被更新的密钥。

假定符号 $\{m\}_E$ 表示使用密钥 E 加密消息 m，则组管理者加密和传输如下消息：

1)向 u_1 单播传输 $\{k'_{11}\}_{k_{01}}$，$\{k'_{21}\}_{k_{11}}$；

2)向 $\{u_2, u_3\}$ 组播传输 $\{k'_{21}\}_{k_{12}}$，向 $\{u_1, u_2, u_3\}$ 组播传输 $\{k'\}_{k_{21}}$；

3)向 $\{u_4, u_5, u_6, u_7\}$ 组播传输 $\{k'\}_{k_{22}}$。

此方案的通信开销大约为 $2\log_2 n$，也就是说为了进行密钥更新需要执行 $2\log_2 n$ 次加密操作。

4.2　改进的逻辑密钥层次树组密钥更新方案

为了减少密钥更新过程的通信开销，基于伪随机函数引进了一种新的组密钥更新方法。假定 G(x) 是一个伪随机函数，它能加倍输入变量的长度，若用 x 表示输入变量，则 $G(x)=L(x)R(x)$，L(x) 和 R(x) 分别表示输出串的左半部分和右半部分，且 L(x)、R(x) 和 x 的长度相等。采用这种方法，当一个组成员离开或被强制排除时，这个成员拥有的密钥和 LKHT 方案一样也要被更新，只不过更新的方法不同。以图 1 为例，树中代表密钥的节点编号规则如图 1，则成员 u_0 离开的一般更新过程算法如下：

```
1)选择一个新的随机数 r，用和离开成员在树中互为兄弟节点
  的组成员 s 的与组管理者共享的密钥 E 加密后传送至 s；
2)j := 0;
  for i := 0 to h-1 do{h 为树的深度，h=log2n;
  begin
        G(R^i(r))=L(R^i(r))R(R^i(r)); {R^0(r)=r}
        {以下计算树中辅助节点密钥和组密钥}
        j := j+1;
    k'_j1 = L(R^i(r)); {k'_j1为更新的辅助密钥，k'_h1表示新的
                        组密钥}
        向适当的子组成员传送{R^i(r)}_k_i2;
end;
```

其密钥更新过程如图2，其中 $G_1=\{u_1\}$，$G_2=\{u_2, u_3\}$，$G_3=\{u_4, u_5, u_6, u_7\}$。

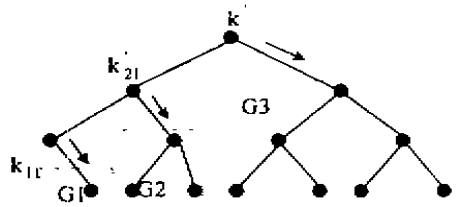

图2　密钥更新过程图

具体过程解释如下：

1)组管理者向 G_1 传递 $\{r\}_{k_{02}}$，向 G_2 传递 $\{R(r)\}_{k_{12}}$，向 G_3 传递 $\{R(R(r))\}_{k_{22}}$；

2)　组管理者和组成员根据需要分别计算新的辅助密钥和组密钥，其中：

$k'_{11}=L(r)$，$k'_{21}=L(R(r))$，$k'=L(R(R(r)))$

这种方案的安全性依赖于伪随机函数 G(x) 的安全性，可以证明，如果 $G(x)=L(x)R(x)$ 是一个具有密码强度的伪随机函数发生器，选择 $k=L(R\cdots(r)\cdots)$ 将是非常困难的[5]。比较这两种方案可知，改进的 LKHT 将使通信开销从 $2\log_2 n$ 降低为 $\log_2 n$（对于二叉密钥分配树），有效地减轻了网络负载，同时增加了每个组成员的计算量。

5. 抵抗攻击者阻止组密钥更新消息传递的方法

以上这些密钥更新方案无疑要求密钥更新消息的可靠、安全传输，然而一旦这些消息无法按要求及时、准确地到达目的组成员，这可能是由于网络流量超载或攻击者拦截从而丢失密钥更新消息或者一些组成员接收更新消息比其它组成员快，这将不仅阻止合法组成员间的安全通信，而且若被攻击者利用当前组成员拥有不一致的密钥这一事实，恶意的攻击者可能使用过时的密钥向当前组发送非法的信息，或欺骗一些当前的组成员使用过时密钥加密发送合法信息。为了阻止这种攻击，拟采用如下方法：

1)组管理者周期性地向组成员发送最新组状态；

Group Manager→Group Member：gi，sn，$\{H(gi, sn)\}_{k_{private}}$

其中 gi 为组标识符，sn 为组管理者产生的顺序号，H 为强单向 Hash 函数，$k_{private}$ 为组管理者的私钥。组成员接收到组播消息后，经解密和完整性验证后，和自身拥

（下转第23页）

含数据本身也包含一小段程序代码。当封装后的主动数据包到达某个节点后，主动数据包所携带的程序代码被执行，以处理数据包所携带的数据。若该封装体中的程序需要调用的处理方法不在该主动节点上，则可通过点播(on demand)在别的主动节点上下载该方法。这种方法具有更大的灵活性和可编程性，但实现起来也更复杂。

4.3 离散法和集成法结合使用

交换机小程序是离散法和集成法结合使用的一个例子，它由两部分组成，一部分是可编程的密封舱，另一部分是充当主动节点的交换机。使用这种方法的意义是：一方面在某些情况下，密封舱需要某些资源(如路由表等)，而它自己又不可能提供，必须由主动节点(如路由器、交换机)来提供。另一面，在密封舱和主动节点之间划分指令可避免密封舱变得过于庞大而降低网络性能。

总结 Opensig 和主动网从不同角度代表了可编程网络发展的两个基本思想，前者着眼于开放网络体系编程接口(如网络 APIs)以实现网络的可编程性，这是一种相对静态的网络可编程思想；而后者则强调能在网络体系中动态地加载客户化程序(无论是采用离散法、集成法或混合法)，通过网络节点上加载的不同程序来提供定制业务，这是一种更为灵活的方法。可编程网络的出现加速了网络发展的步伐，在可编程网上新的技术标准或协议从提出到应用不再需要漫长的标准化过程。用户可以根据自身需要迅速开发新业务。已有的研究成果表明可编程网的诸多技术能有效地改善网络性能，对 Internet 遗留的问题能提供有效的解决方法，被称为下一阶段网络发展的方向。因此，开展对可编程网的研究对我国的网络技术的发展具有重要意义。

参 考 文 献

1 Tennenhouse D, et al. A survey of active network research. IEEE Commum. Mag, 1997, 35(1): 80~86

2 Adam C M, Lazar A A, Lim K -S, Macroncini F The Binding Interface Base Specification Revision 2 0. OPENSIG Workshop on Open Signalling for ATM, Internet and Mobile Networks. Cambridge, UK, April 1997

3 Biswas J, et al. The IEEE P1520 Stabdards Initiative for Programmable Network Interfaces, IEEE Communications Magazine, Special Issue on Programmable Networks. Oct. 1998

4 Alexander D S, et al. The SwitchWare Active Network Architecture IEEE Network, May/June 1998

5 Wetherall D, et al. Introducing New Internet Services Why and How. IEEE Network, May/June 1998

6 Commentaries on Active Networking and End-To-End Arguments. IEEE Network, May/June 1998

7 Available at: http: // www. darpa. mil/ito/research/anets/

8 Available at: http: // www. cc. gatech. edu/projects/canes/

(上接第 47 页)

有的组状态信息相比较，用以确定组成员是否处在当前最新状态。

2)与时间敏感性组密钥更新策略相结合。当然可以使用时间敏感性组密钥更新策略周期性地强制要求组成员更新密钥，杜绝以上问题的发生，但对于较大型的组，进行一次全面的密钥更新要消耗较多的网络带宽，因此可以合理设置第一种方法的时间间隔 t，使其低于时间敏感性策略的定时器值，这样可以设置较大的定时器值，在每一个 t 间隔内，靠第一种方法来检测密钥更新消息是否及时正确地传递。

3)组成员向组管理者发送组密钥更新消息重传请求

Group Member → Group Manager: gi, mi, r, |H(gi, mi, r)|$_{k_{ai}}$

其中 mi 为组成员标识符，r 为组成员每次发请求时产生的不同随机数且对给定的组成员只准使用一次，k_{ai} 为组成员和组管理者共享的密钥。组管理者证实重传请求后，向指定组成员重新发送组密钥更新消息。

结论 本文给出的两种组密钥更新方案具有可放缩性好、消耗网络资源少、便于高效管理和能适应组成员动态变化等特性，是解决组播密钥更新问题的首选方案，同时针对在组密钥更新过程中易被忽略的组密钥更新消息的正确传输问题提出了有效的解决方法，需要进一步研究的问题是两种方案都靠组管理者集中控制，存在组管理者单点失效和瓶颈问题，如何在 Internet 网上提供一个分布式组播安全的组密钥更新方案是一个非常值得研究的问题。

参 考 文 献

1 Wallner D, Harder E, Agee R. Key Management for Multicast: Issues and Architectures. RFC2617, 1999

2 Harney H, Muckenhirn C. Group Key Management Protocol(GKMP) Specification. RFC2093, 1997

3 Ballardie A. Scalable Multicast Key Distribution. RFC1949, 1996

4 Mittra S. Iolus: A Framework for Scalable Secure Multicasting. Proc. ACM SIGCOMM, 1997

5 Wong C K, Gouda M, Lam S S. Secure Group Communications Using Key Graphs. Proc. ACM SIGCOMM, 1998

6 Blum M, Micali S. How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits. SIAM J. on Comp., 1984