维普资讯 http://www.cqvip.com

基于秘密共享的 P2P 组成员管理模型*)

布 和 吴邦欲
(清华大学软件学院 北京 100084)

摘 要 随着 P2P 网络越来越多地应用于企业环境,安全问题变得越来越重要。成员管理是其中一个主要方面。本文提出了一种基于秘密共享的成员管理模型,并通过模拟实验分析了效率与安全性之间的关系。在此模型中,P2P 组内节点间的信息是加密传输的,只有组内成员才拥有用于加密解密的成员密钥。只有得到一定数量的现有成员许可并赞助的外部节点才能加入 P2P 组,并且退出的节点无法得到后续的成员密钥。

关键词 P2P 网络,成员管理,秘密共享,安全

A P2P Membership Management Model Based on Secret Sharing

BU He WU Bang-Yu
(School of Software, Tsinghua University, Beijing 100084)

Abstract With the popularization and application of P2P network in enterprise environment, security becomes more and more important. Membership management is a main concern. This paper proposes a membership management model based on secret sharing. In this model, information transmitted on network is encrypted and only the members of the P2P group have the encryption/decryption key. A node can join the group after has got the permission and sponsorship of certain amounts of existing members and one which has quitted or been revoked from the group cannot get the keys of the latter sessions.

Keywords P2P network, Membership management, Secret sharing, Security

1 引言

P2P 网络由一组地位相等的节点组成,具有完全分布式的体系结构。与集中式结构相比,P2P 结构在可扩展性、实时性、可靠性和负载平衡方面具有天生优势[11]。所以 P2P 网络得到了越来越广泛的应用。典型应用包括文件共享、即时通信等。目前流行的 P2P 网络有:Napster, Gnutella, JXTA, Freenet, Chord, CAN, Pastry, Tapestry 等[1]。

随着 P2P 网络越来越多地应用于企业环境,安全问题变得越来越重要。以往的研究主要集中在访问控制和安全通信等领域(文[2,12]等),而很少有人研究 P2P 网络中的安全的成员管理问题。在文[3,4]中介绍了 P2P 网络中的成员管理问题并提出了基于门限密码学的解决方案,但是都只考虑了成员的加入,没有考虑成员退出。由于 P2P 网络所具有的动态性,成员退出也时常发生,所以不仅需要考虑节点动态加入问题,而且还需解决成员节点的安全退出问题。本文提出了一种基于秘密共享的成员管理模型。在此模型中,组内成员地位平等且成员节点间的信息是加密传输的,只有组内成员才拥有用于加密解密的成员密钥。只有得到一定数量的现有成员许可并赞助的外部节点才能加入,并且退出(自愿退出或被强行从组内删除,以下简称退出)的节点无法得到后续的成员密钥。

2 P2P 组成员管理模型定义

我们的模型考虑这样的应用背景:有许多用户需要在 P2P 网络上动态地建立一个或多个组,组内成员可以相互共享资源并可以相互通信。例如,具有一定安全性的即时通信中,一组用户相互通信但要求其它用户无法看到通信内容,这时他们就可以组成一个组。如图 1 所示。

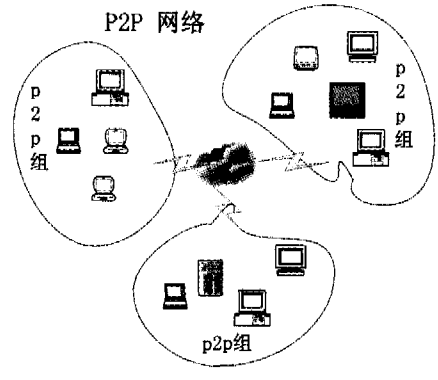

图 1 P2P 组

模型定义如下:P2P 网络上的一个动态组由一组节点 $u=\{U_1,U_2,\cdots,U_n\}$ 组成,组内没有固定的管理员节点,各成员间相互平等。成员节点间能够共享资源并且可以相互通信。只有合法成员才能得到有效数据,而外部节点却无法得到。组内成员动态变化,满足一定条件的外部节点可以加入组中,现有成员也可以自愿退出,并且也可以强行删除违反规则的成员节点。

此模型中,网络上传送的内容都要经过加密(可以使用传

*)基金项目:国家 863 计划课题(2003AA413031)。**布 和** 硕士研究生,研究方向为 Linux 操作系统、信息安全。**吴邦欲** 博士研究生,研究方向为操作系统、信息安全、分布式系统和并行计算。

维普资讯 http://www.cqvip.com

统的 DES,AES 等加密算法)后传输。只有合法成员才拥有用于加密解密的成员密钥。由于没有固定的管理员节点,所以需要时由任意一个节点充当临时管理员的角色。在组建立阶段,每个成员得到一个私有密钥并把它安全地保存起来。然后临时管理员广播一条消息,成员节点根据这条广播消息和先前得到的私有密钥计算成员密钥。这样 P2P 组就建立起来了。如果有一个节点想加入已经存在的 P2P 组,那么它必须得到 $t+1$(t 为门限值)个现有成员的许可并赞助,即赞助节点给新节点传给一些信息,新节点根据得到的 $t+1$ 个赞助信息计算出自己的私有密钥。新节点得到私有密钥后就可以与后续收到的广播消息结合计算出成员密钥了。这样新节点就成为这个 P2P 组的成员了。由于 P2P 网络的动态性,经常会有节点自愿退出,并且有必要强行从组内删除一些违反规则的节点,比如泄露秘密或传播非法信息的节点。这就需要更新现有成员密钥并且保证退出节点计算不出后续会话中的成员密钥。我们假定退出节点能够收到后续的广播消息。所以必须保证退出节点即使结合广播消息和自己的私有密钥也无法正确地计算出后续的成员密钥。

3 基于秘密共享的 P2P 组成员管理

在我们的模型中使用了文[5]中介绍的算法并对其不适合 P2P 网络的部分进行了改进。此算法基于秘密共享(Secret Sharing)[6]的思想,即将秘密 S 分割并分发给一组用户,一定数量的用户一起合作可以恢复此秘密 S。文[6]中给出了一种基于拉格朗日插值的参考方案。文[5]是它的一种扩展。分割秘密的任务由管理员节点完成,但是由于不能破坏 P2P 网络的分布式体系结构,所以不能由固定的节点充当管理员的角色,因此在每次会话中都需要由一个任意节点充当临时管理员的角色,完成秘密 S 的分割等任务。文[5]中应用二元多项式巧妙地解决了这个问题。这里每次会话中的成员密钥就是一个秘密 S,它被分成了 $t+1$ 份,每个成员必须得到 t 份信息才能与自己的私有密钥结合起来计算出秘密 S,即成员密钥。

此模型包含 P2P 组建立、新节点加入、成员节点退出、成员密钥的建立或更新等事件。

3.1 建立 P2P 组

由一个节点充当临时管理员的角色,完成建立 P2P 组的任务。等 P2P 组建立起来以后就不需要这个临时管理员了,在后续会话中任何一个节点都可以充当临时管理员的角色。由于时间短暂,这个没有破坏 P2P 网络的分布式特点。具体步骤如下:

步骤 1:临时管理员选择系统参数 t,生成两个大素数 p,q(满足条件 $q|p-1$)和 g(乘法群 $GF(p)$的一个生成器)并公布 p,q 和 g 。

步骤 2:构建多项式:

$F(x,y)=\sum_{j=0}^{t}\sum_{k=0}^{t}a_{j,k}x^jy^k \bmod q$,其中 $a_{j,k}\in GF(q)(0\leqslant j\leqslant t,0\leqslant k\leqslant t)$是随机选择的,且 $a_{j,k}=a_{k,j}$。临时管理员秘密保存 $F(x,y)$。

步骤 3:为每个现有用户 $U_i\in U$,管理员计算多项式 $F_{U_i}(x)=F(x,i) \bmod q(i\in GF(q)$是用户标识),并通过安全通道把 $F_{U_i}(x)$传给用户 U_i。其中 $F_{U_i}(x)=\sum_{j=0}^{t}A_jU_iX^j \bmod q$,$A_jU_i=\sum_{k=0}^{t}a_{j,k} \bmod q$。用户 U_i 把 $F_{ui}(x)$当作私有密钥 K_{ui} 保存起来,用于后续会话中的秘密 S 的生成和分割。

步骤 4:临时管理员通过成员密钥建立或更新流程为 P2P 组建立新的成员密钥。这样 P2P 组就建立起来了。

3.2 新成员加入

如果有一个新节点要加入现有 P2P 组,则它首先发出 JOIN_REQUEST 请求。收到请求后由 $t+1$ 个现有成员合作完成新成员加入工作。具体步骤如下:

步骤 1:临时管理员 $U_z\in g$ 通过成员密钥建立或更新流程建立新的成员密钥 K_u。

步骤 2:全部现有用户 $U_i\in U$ 更新它们的私有多项式(即私有密钥)$F_{ui}^*(x)=K_u+F_{ui}(x) \bmod q$。

步骤 3:临时管理员为每个新用户 $U_l\in J$ 分配一个唯一标识 l,$J_{id}\cap u_{id}=\varnothing$且 $0\notin J_{id}$。

步骤 4:选择至少 $t+1$ 个赞助者。每个赞助者 $U_z\in g$ 计算 $f_{z,l}^*=F_{U_z}^*(l) \bmod q$,并各自通过安全通道独立地传送给每个新用户 $U_l\in J$。

步骤 5:由于得到 $t+1$ 份信息,所以每个新用户 $U_l\in J$ 就可以使用拉格朗日插值函数计算出各自的秘密,即私有密钥(私有多项式)$F_{Ul}^*(x)$:

$$F_{Ul}^*(x)=\sum_{z\in R_{id}}f_{z,l}^*\prod_{k\in R_{id},k\neq z}\frac{x-k}{z-k} \bmod q。$$

步骤 6:临时管理员通过成员密钥建立或更新流程建立新的成员密钥。

3.3 成员退出

我们假定退出的节点仍能够获得后续会话中的广播消息,所以为了保证退出节点无法计算出后续会话中的成员密钥,在后续的广播消息中包含退出节点的信息,这样由于得不到足够的($t+1$ 份)信息,退出节点就无法计算出成员密钥(秘密 S)了。具体步骤如下:

步骤 1:设 U_z 为临时管理员。U_z 广播一条消息 M,以便各成员建立或更新密钥 $K_{u\backslash R}$。设当前成员 $u_{id}=\{i|U_i\in u\}$,退出用户集合 R。广播消息 M 由以下步骤构建:

1. 随机生成整数 $r\in GF(q)$并计算 $G=g^r \bmod p$。

2. 从 $GF(q)$中随机选择一组整数 J,满足$|J|=t-|R|$,$a\neq b$,$\forall a,b\in J$,且 $J\cap u_{id}=\varnothing$。U_z 为全部 $j\in R_{id}\cup J$ 计算 $G_j=G^{F_{Uz}(j)} \bmod p$。

步骤 2:广播消息 M,其中 $M=\{G,z,G_j \| j|j\in R_{id}\cup J\}$。

步骤 3:计算成员密钥。每个成员 $U_i\in u\backslash R$(包括 U_z)使用各自的私有密钥 $F_{Ui}(x)$ 和 M 计算成员密钥:$K_{u\backslash R}=(G)^{F_{Ui}(z)\times L(R_{id}\cup J\cup\{i\},i)}\times\prod_{j\in R_{id}\cup J}(Gj)^{L(R_{id}\cup J\cup\{i\},j)} \bmod p$。其中 $L(\Psi,W)=\prod t/(t-w) \bmod q$($\forall\Psi$:集合,$\forall W$:整数,$t\in\Psi\backslash\{w\}$)为拉格朗日差值函数。由于退出节点无法得到 $t+1$ 个插值点,所以无法计算出新的成员密钥。

3.4 成员密钥建立或更新

成员密钥建立或更新流程与上面的成员退出流程基本一致,只是退出用户集合 $R=\varnothing$。

4 安全性分析及改进

此模型涉及两种安全问题。前向安全(Forward Security)和后向安全(Backward Security)。所谓前向安全就是新加入的节点无法计算出加入之前各会话中的成员密钥。定义如下:一组新加入的节点 $U_l\in J$,广播消息 M_j(加入前某次会话中的广播消息),全部 $U_l\in J$ 无法计算 K_j($H(K_j|M_j,\{S'_i\}_{Ui\in J})=H(K_j)$)。其中 H 为熵函数(请参见文[8])。后

维普资讯 http://www.cqvip.com

向安全是指已经退出的节点即使得到后续会话中的广播消息也无法计算出成员密钥。定义如下[7]：一组退出用户 $R\subseteq\{U_1,\cdots,U_n\}(|R|\leqslant t)$，广播消息 M_j，全部 $U_i\notin R$ 都能计算 $K_j(H(K_j|M_j,S_i)=0)$，而退出节点却无法计算 $K_j(H(K_j|M_j,\{S_j'\}_{U_i\in R})=H(K_j))$。这是通过在广播消息中包含退出节点的信息来保证的。从成员退出流程可以看到每次最多只能包含 t 个信息(因为 $|J|=t-|R|$)，所以一次只能退出 t 个节点。如果要永久性地删除一个节点，那么可以把其信息包含在每次广播的消息中。但是总的退出用户数也不能超过 t。这不符合 P2P 网络的动态性特点。解决的办法是定期更新私有密钥。在文[9,10]中提出了叫主动秘密共享(Provocative Secret Sharing)的方法。这里我们简单地用上一次会话中的成员密钥更新私有密钥，即在成员退出阶段中的第三步之后用新的成员密钥更新私有密钥：$F_{U_i}^{*}(x)=K_{U\setminus R}+F_{U_i}(x)\bmod q$。这样在此之前退出的节点信息就不用包含在后续的广播中了。

5 实验结果

此模型中 t 值的选择至关重要。它直接影响系统的安全性和效率，t 值越高安全性也越高，而广播消息就越大，而且需要更多的节点一起合作处理新成员加入，所以相应的系统效率就越低。还有 t 值可以是动态的，即可以根据成员数目变化，也可以是固定的，即不随成员数变化。但是当成员数目小于 $t+1$ 时就必须调整 t 值了，因为必须有 $t+1$ 个成员才能处理新成员加入请求。我们实现了一个实验平台，模拟了固定 t 值下的系统运行。我们做了 40 个节点的实验比较了各种 t 值下用户退出和加入时的时间开销。实验硬件环境：两台 Intel Celeron(R)1.7G CPU，256M 内存，60G 硬盘。软件环境：Linux2.6.8，jdk1.5。两台机器由 100M 高速以太网相互连接。每台机器模拟 20 个节点。实验中大素数 p 选择为 512 位。实验结果如下：

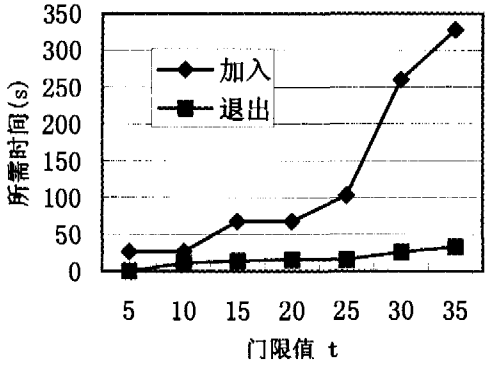

图 2 节点加入和退出所需时间

由实验结果可以看出 t 值对成员退出的效率影响不是很大(广播大小线性增长)，而对成员加入影响比较大。这可能是由于新节点必须等待收到全部的 $t+1$ 个赞助者的赞助信息所花的等待时间造成的。

结论与展望 本文提出了一种基于秘密共享的 P2P 组成员管理模型。此模型允许成员的动态加入和退出，并且能够保证没有成员资格的节点无法解密成员间传送的信息(加密传输)。本文还讨论了系统安全性和效率之间的关系，并给出了模拟环境下的实验结果。如何在不稳定的网络环境下，某个节点即使没有收到某次会话中的广播消息也能够自己恢复相应的成员密钥而不需依赖其它节点是作者下一步的主要研究目标和兴趣所在。

参 考 文 献

1 Zhou Shijie, Qin Zhiguang, Liu Jinde. Distributing the Keys into P2P Network. GCC 2003, LNCS 3032, 2004. 460～463

2 Tran Huu, Hitchens M, Varadharajan V, Watters P. A Trust based Access Control Framework for P2P File-Sharing Systems. System Sciences, 2005. HICSS '05. In: Proc. of the 38th Annual Hawaii Int. Conf. on, 2005

3 Narasimha M, Tsudik G, Yi J H. On the utility of distributed cryptography in P2P and MANETs-the case of membership control. Network Protocols, 2003, In: Proc. 11th IEEE Int. Conf. on 2003. 336～345

4 Kim Y, Mazzocchi D, Tsudik G. Admission control in peer groups. In IEEE NCA, 2003

5 Kurnio H, Safavi-Naini R, Wang Huaxiong. A Group Key Distribution Scheme with Decentralized User Join. SCN 2002, LNCS 2576, 2003. 146～163

6 Shamir A. How to share a secret. Comm. Assoc. Comput. Mach., 1979, 22(11): 612～613

7 Staddon J, Miner S, Franklin M, Balfanz D, Malkin M, Dean D. Self-Healing Key Distribution with Revocation. IEEE Symposium on Security and Privacy, Berkeley, California, 2002

8 Cover T, Thomas J. Elements of Information Theory. John Wiley and Sons, Inc., 1991

9 Frankel Y, Gemmell P, MacKenzie P D, Yung M. Optimal resilience proactive public-key cryptosystems. In FOCS, 1997

10 Herzberg A, Jarecki S, Krawczyk H, Yung M. Proactive secret sharing, or: How to cope with perpetual leakage. In CRYPTO, 1995

11 周晋，路海明，李衍达. 用 Small-World 设计无组织 P2P 系统的路由算法. Journal of Software, 2004, 15(6): 915～923

12 叶润国，宋成，吴迪，李文印，陈震. P2P 网络中对等节点间安全通信研究. 微电子学与计算机, 2004, 21(6): 95～99