Ad Hoc 网络中一种基于环状分层结构的组密钥协商协议*)

章丽平[1,2] 崔国华[1] 喻志刚[3] 雷建云[1] 许静芳[1]

(华中科技大学计算机学院 武汉 430074)[1] (中国地质大学计算机学院 武汉 430074)[2]

(武汉邮电科学研究院虹信技术有限责任公司 新一代光纤通信技术和网络国家重点实验室 武汉 430074)[3]

摘 要 移动 ad hoc 网络是一种新型的移动多跳无线网络。其自身的特征,如网络规模庞大、动态的拓扑结构、有限的计算、通信和存储能力等,使得传统的密钥分配和管理机制无法直接应用于该网络。提出了一种新的适用于移动 ad hoc 网络的组密钥协商协议。该协议在环状分层结构上基于多线性映射进行组密钥的协商和分配,使得节点在密钥协商过程中具有低计算开销与低通信开销的优势,较好地解决了在移动 ad hoc 网络中进行组密钥协商时所遇到的节点能量受限问题,适用于移动 ad hoc 网络。

关键词 Ad hoc 网络,组密钥协商,环状分层,多线性映射

Group Key Agreement Protocol Based on Circular Hierarchical for Ad Hoc Networks

ZHANG Li-ping[1,2] CUI Guo-hua[1] YU Zhi-gang[3] LEI Jian-yun[1] XU Jing-fang[1]

(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)[1]

(College of Computer Science and Technology, China University of Geosciences, Wuhan 430074, China)[2]

(Wuhan Research Institute of Posts&Telecommunication State Key Laboratory for New Optical Communication Technologies and Networks, Wuhan 430074, China)[3]

Abstract A mobile ad hoc network is a new-style mobile multihop wireless network. Providing a suitable key establishment scheme in mobile ad hoc networks is challenging due to all the characteristics of these networks, such as dynamically changing topology and limitations of power, computation capability and storage resources. A new group key agreement protocol based on circular hierarchical for mobile ad hoc networks was proposed. In this protocol multi-linear map is employed on circular hierarchical structure to establish and allocate group key. So our protocol can not only meet security demands of mobile ad hoc networks but also improve executing performance.

Keywords Ad hoc networks, Group key agreement, Circular hierarchical, Multi-linear map

1 引言

移动 ad hoc 网络是一种新型的移动多跳无线网络,与传统的无线网络不同,它不依赖于任何固定的基础设施和管理中心,而是通过传输范围内有限的移动节点间相互协作和自我组织来保持网络连接和实现数据传递。其自身的特征,如节点的有限物理保护、动态的拓扑结构等,使得在移动 ad hoc 网络中提供安全的保护措施成为一种挑战[1]。密钥管理机制则是构建安全的移动 ad hoc 网络的核心技术。

Ingemarsson 等人提出了第一个组密钥管理协议 ING 协议[2]。在此基础上,Steiner 等人提出了一组 GDH 组密钥协商协议[3-5]。该协议中,最后一个组成员相当于整个组的控制者,承担了大量的计算和通信工作,需要具有较高的能量。而移动 ad hoc 网络中所有节点的资源都是有限的,并且能量较低。因此,GDH 协议在移动 ad hoc 网络中应用时会受到节点自身资源的限制。Kim 等人在 Perrig 提出的基于树的密钥管理模式[6]上进行了扩展,提出了基于树的组密钥管理协议 TGDH 协议[7]。与 GDH 协议相比,该协议避免了单个节点承担过多计算和通信开销的问题,但该协议中每个节点却需要承担大量的计算和大量的通信工作。因而,该协议也很难适用于移动 ad hoc 网络。为了降低节点的计算和通信开销,Jason 等人提出了一种层簇式密钥协商协议[8]。该协议将移动 ad hoc 网络划分成若干个簇,每个簇由一个簇头进行管理。每个簇的簇头作为成员加入上一层,依此类推,构建层簇结构。然后,在此结构上应用 D-H 密钥协商协议进行组密钥的协商。该协议有效地减少了组密钥协商过程中节点的资源消耗,但该协议需要在线服务器的协作来完成层密钥和簇密钥的更新操作。Lee 等人提出了一种基于 Hamming 距离的混合密钥管理协议[9],该协议将 Hamming 距离的概念引入到密钥预分配中,并结合对称密钥和非对称密钥各自的优势在移动 ad hoc 网络中实现了密钥的预分配和管理。该方案的优点在于有效地降低了移动 ad hoc 网络中每个节点所需存储的密钥数,并保证了网络中任意两个节点间拥有共享密钥的惟一性,从而保证了网络的强健壮性。但是,当网络中有节点大量频繁退出时,该方案不能保证需要进行通信的双方节点间存在安全的通信路径,这就会造成无法通信的严重后果。因此,该方案并不适用于移动 ad hoc 网络。

本文提出了一种基于环状分层结构的组密钥协商协议(CH-DMDH)。该协议在环状分层结构[10]上,基于多线性映射进行组密钥的协商和分配,使得节点在密钥协商过程中具

*)国家自然科学基金资助项目(60403027)资助,中国地质大学(武汉)优秀青年教师资助计划资助项目(CUGQNL0836)。**章丽平** 博士研究生,讲师,研究方向为密码学和网络安全;**崔国华** 教授,博士生导师,主要研究方向为密码学和信息安全。

有低计算开销与低通信开销的优势，适用于移动 ad hoc 网络。

2 预备知识

设 G_1 和 G_2 分别是同为 p 阶的加群和乘群，并假设 P 为 G_1 的生成元。假设在群 G_1 和 G_2 中，离散对数问题是难解的。定义多线性映射为 $e:G_1^d \rightarrow G_2$，并满足以下特性[11]：

(1)多线性。对 $\forall a_1,\cdots,a_d \in Z_p^*$ 和 $\forall P_1,\cdots,P_d \in G_1^*$，有 $e(a_1P_1,\cdots,a_dP_d)=e(P_1,\cdots,P_d)^{a_1\cdots a_d}$。

(2)非退化性。若 P 是 G_1 的生成元，则 $e(P,\cdots,P)$ 是 G_2 的生成元。

(3)可计算性。存在有效的算法，对于 $P_1,\cdots,P_d \in G_1^*$，可计算 $e(P_1,\cdots,P_d)$。

定义 1(可判断 multi-linear Diffie-Hellman(DMDH)问题) 给定 $(P,a_1P,a_2P,\cdots,a_{d+1}P)$ 和 $z\in G_2$，判断是否有 $z=e(P,P,\cdots,P)^{a_1a_2\cdots a_{d+1}}$ 成立。

定义 2(DMDH 假设) 假设 DMDH 问题是困难的，即不存在一个概率多项式算法解 DMDH 问题。

3 基于环状分层结构的组密钥协商协议

基于环状分层结构的组密钥协商协议(CH-DMDH)中使用到的符号的说明如表 1 所示。

表 1 符号说明表

符号	符号说明
p	大素数
G_1,G_2	分别是同为 p 阶的加群和乘群
$e:G_1^d \rightarrow G_2$	G_1 和 G_2 上的多线性映射
P	G_1 的生成元
$H:G_2 \rightarrow Z_p^*$	哈希函数
n	组大小，即移动 ad hoc 网络中节点总数
c	每个子组的组成员总数
h	环状分层结构中的总层数
L_i	环状分层结构中的第 i 层，其中 $i\in[0,\cdots,h-1]$
$SG_j^{(L_i)}$	L_i 层中第 j 个子组，其中 $j\in[0,\cdots,c^i-1]$
$U_{SG_j^i}^{(L_i)}$	L_i 层中第 j 个子组的子组控制者
$U_{(j,k)}^{(L_i)}$	$SG_j^{(L_i)}$ 子组中第 k 个组成员，其中 $k=jc+l,l\in[0,\cdots,c-1]$
$\{m\}_e$	采用安全的对称密钥加密模式用密钥 e 加密明文信息 m
$r_{(j,k)}$	$U_{(j,k)}^{(L_{h-1})}$ 选择的秘密随机整数，$r_{(j,k)}\in Z_p^*$
$K,K_{SG_j^{(L_i)}}$	分别为组密钥和子组 $SG_j^{(L_i)}$ 的子组密钥

移动 ad hoc 网络中节点的规模可以从几个节点到上万个节点甚至更多，为了在含有 n 个节点的移动 ad hoc 网络中实现安全的组通信，CH-DMDH 协议采用了环状分层结构，其结构如图 1 所示。

设定 L_0 为环状分层结构中的最高层，L_{h-1} 为该结构中的最底层。最底层的每个子组的组成员对应于移动 ad hoc 网络中的一个节点，其它层的组成员则为逻辑节点。环状分层结构中，若组成员总数为 $n=c^h$，则每一层 L_i($i\in[0,\cdots,h-1]$)中含有 c^i 个子组，且每个子组含有 c 个组成员。子组中所有组成员依次排列，第一个组成员与最后一个组成员首尾相连，形成一个封闭的环。当 $n<c^h$ 时，最底层的 L_{h-1} 层所拥有的子组数或者小于 c^{h-1} 个，或者 L_{h-1} 层中含有 c^{h-1} 个子组，但有一个子组的组成员数小于 c 个。设每个子组 $SG_j^{(L_i)}$ 中的第一个组成员充当该子组的子组控制者 $U_{(j,jc)}^{(L_i)}=U_{SG_j^i}^{(L_i)}$，管理 $SG_j^{(L_i)}$ 子组。除了最底层，每层中的子组成员 $U_{(j,k)}^{(L_i)}$($L_i\neq L_{h-1}$)同时也是下一层 L_{i+1} 层中子组 $SG_k^{(L_{i+1})}$ 的子组控制者 $U_{(j,k)}^{(L_i)}=U_{SG_k^i}^{(L_{i+1})}$。

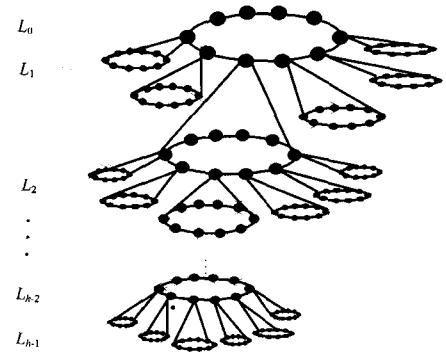

图 1 $c=10$ 的环状分层结构图

3.1 组密钥协商协议

基于环状分层结构的组密钥协商协议的基本思想是：首先，L_{h-1} 层中的每个子组基于多线性映射进行子组密钥的协商，分别获取它们的子组密钥 $K_{SG_j^{(L_{h-1})}}$。然后，L_m 层($m\in[h-2,\cdots,0]$)中的每个子组再按照类似的方法获取相应的子组密钥，直至得到最终的组密钥 $K=K_{SG_0^{(L_0)}}$。最后，采用对称密钥算法实现组密钥以及子组密钥的安全分发。方案的具体步骤如下：

步骤 1 该协议从环状分层结构的最底层开始执行。L_{h-1} 层中的每个子组采用如下方法进行子组密钥的协商：首先，子组 $SG_j^{(L_{h-1})}$ 中的每个组成员 $U_{(j,k)}^{(L_{h-1})}$ 随机选取一个整数 $r_{(j,k)}\in Z_p^*$ 作为其自身的私钥。然后，计算其公钥 $r_{(j,k)}P$，并将该公钥信息广播给全组。组成员 $U_{(j,k)}^{(L_{h-1})}$ 在获取了组内其它组成员的公钥信息后，计算密钥 $K_{U_{(j,k)}^{(L_{h-1})}}=e(r_{(j,jc)}P,\cdots,r_{(j,k-1)}P,r_{(j,k+1)}P,\cdots,r_{(j,jc+c-1)}P)^{r_{(j,k)}}$。由于

$$\begin{aligned}K_{U_{(j,k)}^{(L_{h-1})}}&=e(r_{(j,jc+1)}P,r_{(j,jc+2)}P,\cdots,r_{(j,jc+c-1)}P)^{r_{(j,jc)}}\\&=e(r_{(j,jc)}P,r_{(j,jc+2)}P\cdots,r_{(j,jc+c-1)}P)^{r_{(j,jc+1)}}\\&=e(r_{(j,jc)}P,\cdots,r_{(j,k-1)}P,r_{(j,k+1)}P,\cdots,r_{(j,jc+c-1)}P)^{r_{(j,k)}}\\&=\cdots=e(P,P,\cdots,P)^{r_{(j,jc)}r_{(j,jc+1)}\cdots r_{(j,jc+c-1)}}\end{aligned}$$

因此，子组 $SG_j^{(L_{h-1})}$ 中的每个组成员 $U_{(j,k)}^{(L_{h-1})}$ 在获取了组内其它组成员的公钥信息后，都可以计算出该子组的子组密钥 $K_{SG_j^{(L_{h-1})}}=K_{U_{(j,k)}^{(L_{h-1})}}$。当 L_{h-1} 层中的每个子组都通过上述方法计算得到其自身的子组密钥后，该过程结束。

步骤 2 由于 L_m($m\in[h-2,\cdots,0]$)层中的每个子组 $SG_j^{(L_m)}$($j\in[0,\cdots,c^m-1]$)中的每个组成员 $U_{(j,k)}^{(L_m)}$($k=jc+l$，$l\in[0,\cdots,c-1]$)同时又是第 L_{m+1} 层 $SG_k^{(L_{m+1})}$ 子组的子组控制者 $U_{SG_k^i}^{(L_{m+1})}$。所以组成员 $U_{(j,k)}^{(L_m)}$ 拥有 L_{m+1} 层 $SG_k^{(L_{m+1})}$ 子组的子组密钥 $K_{SG_k^{(L_{m+1})}}$。因此，L_m 层中的每个子组 $SG_j^{(L_m)}$ 在采用类似步骤 1 所描述的方法进行子组密钥协商时，该子组的组成员 $U_{(j,k)}^{(L_m)}$ 将采用 $SG_k^{(L_{m+1})}$ 子组的子组密钥哈希值 $H(K_{SG_k^{(L_{m+1})}})$ 作为其私钥进行子组密钥的协商，获取该子组的子组密钥 $K_{SG_j^{(L_m)}}$。当 L_0 层中的 $SG_0^{(L_0)}$ 子组获取了组密钥 $K=K_{SG_0^{(L_0)}}$ 后，该过程结束。

步骤 3 最高层 L_0 层中的每个组成员 $U_{(0,k)}^{(L_0)}$ 采用对称密钥算法，用子组 $SG_k^{(L_1)}$ 的子组密钥 $K_{SG_k^{(L_1)}}$ 对组密钥 $K=K_{SG_0^{(L_0)}}$ 进行加密，并将加密后的信息多播给 L_1 层中的子组 $SG_k^{(L_1)}$。

第 $L_m(m\in[1,\cdots,h-2])$ 层中的每个组成员 $U_{(j,k)}^{(L_m)}$ 在接收到来自于 L_{m-1} 层的相对应的子组控制者 $U_{SG_j}^{(L_m)}$ 发送的信息 $\{K\|\cdots\cdots\|K_{SG_{\lceil j/c\rceil-1}^{(L_{m-1})}}\}_{K_{SG_j^{(L_m)}}}$ 后，用子组密钥 $K_{SG_j^{(L_m)}}$ 对该信息进行解密，并将其自身的子组密钥值 $K_{SG_j^{(L_m)}}$ 串接在解密所得到的信息之后。由于 $U_{(j,k)}^{(L_m)}$ 同时也是 L_{m+1} 层中子组 $SG_k^{(L_{m+1})}$ 的子组控制者 $U_{SG_k}^{(L_{m+1})}$，因此每个组成员 $U_{(j,k)}^{(L_m)}$ 可以采用对称密钥算法，用子组 $SG_k^{(L_{m+1})}$ 的子组密钥 $K_{SG_k^{(L_{m+1})}}$ 对串接值 $\{K\|\cdots\cdots\|K_{SG_{\lceil j/c\rceil-1}^{(L_{m-1})}}\|K_{SG_j^{(L_m)}}\}$ 进行加密，并将加密信息 $\{K\|\cdots\cdots\|K_{SG_{\lceil j/c\rceil-1}^{(L_{m-1})}}\|K_{SG_j^{(L_m)}}\}_{K_{SG_j^{(L_{m+1})}}}$ 多播给 L_{m+1} 层的子组 $SG_k^{(L_{m+1})}$。L_{h-1} 层中的每个子组 $SG_j^{(L_{h-1})}$ 的所有组成员 $U_{(j,k)}^{(L_{h-1})}$ 接收到来自 L_{h-2} 层的相对应的子组控制者 $U_{SG_j}^{(L_{h-1})}$ 发送的信息 $\{K\|\cdots\cdots\|K_{SG_{\lceil j/c\rceil-1}^{(L_{h-2})}}\}_{K_{SG_j^{(L_{h-1})}}}$ 后对其进行解密，获取最终组密钥 K 以及该子组上层所有相对应的子组密钥，该过程结束。这样，所有的组成员都将安全的获取组密钥 K 以及相应的子组密钥。

3.2 密钥更新

当有新合法组成员 U_{n+1} 请求加入网络时，若网络中组成员总数 $n=c^h$，则重新构建环状分层结构，运行 CH-DMDH 协议实施新的密钥协商和分配。若网络中组成员总数 $n<c^h$，则分两种情况讨论：

1)若 L_{h-1} 层所拥有的子组数小于 c^{h-1} 个，且每个子组均含有 c 个组成员，此时新合法组成员 U_{n+1} 自己构成一个子组。该子组在 L_m 层($m\in[h-2,\cdots,0]$)上的所有相对应的子组都重新运行子组密钥协商协议，更新相对应的子组密钥，并将更新后的组密钥和子组密钥安全地分发给相应的组成员。

2)若 L_{h-1} 层所拥有的子组数小于等于 c^{h-1} 个，且有一个子组 $SG_j^{(L_{h-1})}(j\in[0,\cdots,c^{h-1}-1])$ 的组成员数小于 c 个，此时新合法组成员 U_{n+1} 加入子组 $SG_j^{(L_{h-1})}$，该子组重新计算子组密钥，并对其所有上层相对应的子组密钥进行更新。同样将更新后的组密钥和子组密钥安全地分发给相应的组成员。

当子组 $SG_j^{(L_{h-1})}$ 中的组成员 $U_{(j,k)}^{(L_{h-1})}$ 请求退出时，该子组内其它组成员 $U_{(j,t)}^{(L_{h-1})}(t=jc+l,l\in[0,\cdots,c-1]$ 且 $t\neq k)$ 在接收到其退出请求后，删除该组成员的信息，并通过重新运行子组密钥协商算法，更新该子组的子组密钥。该子组所有上层相对应的子组也重新运行子组密钥协商协议，进行密钥更新。组密钥 K 的更新完成后，将更新后的组密钥和子组密钥安全地分发给相应的组成员。

4 安全性分析

CH-DMDH 协议的安全性基于 DMDH 假设和对称密钥系统的安全性。

子组密钥协商过程中，每一个组成员都将自己的公钥广播给全组。这样，子组内任何一个组成员都可以获取该子组内所有其它组成员的公钥，并可以利用这些公钥和自己的私钥基于多线性映射，计算出该子组的子组密钥。显然，子组密钥协商过程的安全性是基于 DMDH 假设的。假设敌手 A 要获取子组密钥，他就必须获取该子组中某个组成员的私钥。要想获取组成员的私钥，敌手 A 就只能从组成员广播的公钥信息中提取其私钥。而从公钥中进行私钥的提取，该过程等价于解决一个离散对数问题。因此，敌手 A 无法获取任何组成员的私钥，也就无法获取子组密钥。

组密钥协商过程中，L_{m+1} 层中每个子组 $SG_k^{(L_{m+1})}$ 进行子组密钥协商获取该子组的子组密钥 $K_{SG_k^{(L_{m+1})}}$。$L_m(m\in[h-2,\cdots,0])$ 层的子组 $SG_j^{(L_m)}$ 中的每个组成员 $U_{(j,k)}^{(L_m)}$ 再采用 $SG_k^{(L_{m+1})}$ 子组的子组密钥哈希值 $H(K_{SG_k^{(L_{m+1})}})$ 作为其私钥进行子组密钥协商。直到最高层的子组获取组密钥 K，该过程结束。显然，组密钥协商协议的安全性是基于子组密钥协商过程安全性的。由前面的分析知，子组密钥协商过程是安全的，那么敌手 A 即使能够窃听到组内所有组成员之间发送的消息，在其不知道任何一个组成员私钥的情况下，敌手 A 不能够通过监听到的信息获取任何组成员的私钥，也就无法计算出子组密钥和组密钥。

密钥分发过程中，采用对称密钥算法对组密钥以及子组密钥进行加密，再将加密信息从最高层分发给相应的子组成员。密钥分发过程的安全性是基于对称密钥系统安全性的。若采用的对称密钥算法能够抵抗密文攻击，则攻击者无法获取组密钥和子组密钥，除非攻击者能破解该对称密钥算法。

CH-DMDH 协议具有前向安全性和后向安全性。当节点 B 加入某个子组时，由密钥更新过程，该子组以及该子组所对应的所有上层子组都将更新自己的子组密钥，并将更新后的组密钥和子组密钥安全发送给相应的组成员。因此，节点 B 无法获取其加入前的组密钥和任何子组密钥。由前面的安全性分析知，节点 B 在不知道任何子组密钥和组密钥的情况下，将无法破解组内成员在其加入前的通信内容，保证了后向安全性。同样，当节点 B 退出后，B 原先所在的子组将对其子组密钥进行更新，该子组所对应的所有上层子组也相应地更新原有的子组密钥，并将更新后的组密钥和子组密钥安全地进行分发。所以，节点 B 除非重新加入该组，否则它将无法破解它离开后组内成员所发送信息的内容，保证了前向安全性。

5 性能分析

CH-DMDH 协议在计算复杂度和通信复杂度方面与 TGDH 协议和 GDH 协议的比较如表 1 所示。计算代价为指数运算次数或多线性映射运算次数。其中，CH-DMDH 协议中运算次数指多线性映射运算次数，其它协议中运算次数指有限域离散指数模运算次数。由文献[12,13]知，指数计算量和多线性映射计算量要远远高于对称密钥的加密/解密计算量。因此，忽略对称密钥加密/解密的计算开销。通信代价为组成员发送和接收消息数。表 1 中的 h 表示环状分层结构中的总层数或 TGDH 协议中树的高度。Users 表示 CH-DMDH 协议中 L_{h-1} 层的每个子组的组成员。

表 1 计算代价和通信代价表

		运算次数	发送消息数	接收消息数
TGDH		$2h$	h	h
GDH	U_1-U_{n-2}	3	2	3
	U_{n-1}	2	1	2
	U_n	n	1	$n-1$
GH-DMDH	$SG_0^{(L_0)}$	h	$2h-1$	hc
	$SG_j^{(L_m)}$ $m\in[1,\cdots,h-2]$	$h-m$	$2h-2m-1$	$(h-m)c+1$
	Users	1	1	c

由于 TGDH 协议中 $h=\log_2 n$，而环状分层结构中 $h=\log_c n$，因此，CH-DMDH 协议与 TGDH 协议相比显著降低了

计算和通信开销，n 越大，优势越明显。由表 1，CH-DMDH 协议与 GDH 协议相比，则显著降低了最后一个组成员 U_n 的计算开销以及接收数据的通信开销。此外，GDH 协议中，尽管组成员 U_n 只发送了一条消息，但该消息中包含 $n-1$ 个 1024 位的密钥信息。

由以上分析，CH-DMDH 协议能有效地降低移动 ad hoc 网络中节点在进行安全的组密钥协商时所需要的资源开销。

结束语 随着移动 Ad Hoc 网络的应用与发展，其密钥管理问题日益成为研究热点。本文提出的基于环状分层结构的组密钥协商协议，在环状分层结构上基于多线性映射在移动 ad hoc 网络中实现了组密钥的协商和分配。与 GDH 和 TGDH 组密钥协商协议相比，有效地减少了密钥协商过程中节点的资源消耗，适用于移动 ad hoc 网络。但是 CH-DMDH 协议在节点频繁加入的情况下，可能会需要重新运行协议来完成组密钥的协商和分配。因此，如何采用批量更新的方法来减少协议重新运行的次数将是下一步研究的重点。

参 考 文 献

[1] Ateniese G, Steiner M, Tsudik G. New multi-party authentication services and key agreement protocols. IEEE Journal on Selected Areas in Communications[J], 2000, 18(4): 628-640

[2] Ingemarsson I, Tang D T, Wong C K. A conference key distribution system. IEEE Transactions on Information Theory[J], 1982, 28(5): 714-720

[3] Steiner M, Tsudik G, Waidner M. Differ-Hellman key distribution extended to group communication[C] // Conference on Computer and Communications Security. Usenix: ACM Press, 1996: 31-37

[4] Steiner M, Tsudik G, Waidner M. DLIQUES: A New Approach to Group Key Agreement[C]// Proceeding of the 18th International Conference on Distributed Computing Systems. 1998: 380-387

[5] Steiner M, Tsudik G, Waidner M. Key Agreement in Dynamic Peer Groups[J]. IEEE Transactions on Parallel and Distributed Systems, 2000, 11(8): 769-780

[6] Perrig A. Efficient collaborative key management protocols for secure autonomous group communication[C] // International Workshop on Cryptographic Techniques and Electronic Commerce. 1999: 192-202

[7] Kim Y, Perring A, Tsudik G. Tree-based Group Key Agreement [J]. ACM Transaction on Information and System Security, 2004, 7(1): 60-96

[8] Li J H, Renato Levy, Miao Yu. A Scalable Key Management and Clustering Scheme for Ad Hoc Networks // INFOSCALE'06. 2006: 1-10

[9] Lee Seok-Lae, Jeun In-Kyung, Song Joo-Seok. Mixed Key Management Using Hamming Distance for Mobile Ad-Hoc Networks[C]// ICCS 2007, LNCS4488. 2007: 665-672

[10] Ming T J C, How T C. Energy-Efficient and Scalable Group Key Agreement for Large Ad Hoc Networks[C]//PE-WASUN'05. 2005: 114-121

[11] Wang Wei, Ma Jianfeng, SangJae M. Efficient Group Key Management for Dynamic Peer Networks [C] // MSN 2005, LNCS3794. 2005: 753-762

[12] Carman D W, Kruss P S, Matt B J. Constraints nd approaches for distributed sensor network security[R]. NAI Labs Technical Report. 2000

[13] Trappe W, Wang Y, Liu K J. Resource-aware conference key establishment for heterogeneous networks [J]. IEEE/ACM Transactions on Networking, 2005, 13(1): 134-146

(上接第 60 页)

我们观察到，初始随机生成的网络中，由于文件的无序组织，SAS 的搜索成功率仅为 79.3%，平均搜索路径长度为4.8。而 SAS 通过网络自组织调整基本达到收敛状态以后(第 6 个周期)，系统搜索成功率提高到 98.4%，平均搜索路径长度降低到 1.34(表明大部分查询在 1 个跳数内完成)。这是因为 SAS 在资源搜索时，消息在社区间扩散而不是盲目地针对随机分布在整个网络上的资源进行泛洪，增强了资源发现的针对性，因此能够在保证高搜索成功率的同时提高系统的搜索效率。

从第 30 个周期开始，我们每隔 3 万次查询随机选取 40%的节点，对它们的兴趣，即共享文件和搜索请求进行随机互换。可以看出，SAS 在兴趣发生变化的瞬间搜索性能恶化，搜索成功率下降，平均搜索路径长度增长，但随着搜索的进行，SAS 的查询效果越来越好，并且能够很快恢复到收敛状态，(基本上在 5 个周期内完成)。由于 SAS 可以通过选择路由方向决定搜索的路径，基于资源连接和需求连接的路由机制随着资源分布以及搜索内容的变化做动态自适应的调整，因此能快速地自动优化搜索性能，相对减轻了兴趣转移带来的搜索性能恶化的程度。

结束语 针对节点的兴趣变化对搜索性能造成的影响，提出了一种动态自适应的搜索机制 SAS，通过消息转发的智能性(进行节点路由方向决策)，及时反映资源分布以及搜索内容的动态变化，从而能够在节点兴趣发生转移的情况下迅速定位资源提供节点。实验分析表明 SAS 能自动优化搜索性能，搜索性能好，在动态环境下具有很好的自适应性。

参 考 文 献

[1] Stephanos A T, Diomidis S. A survey of Peer-to-Peer content distribution technologies. ACM Computing Surveys, 2004, 36(4): 335-371

[2] Lua E K, Crowcroft J, Pias M, et al. A survey and comparison of Peer-to-Peer overlay network schemes. Journal of IEEE Communications Survey and Tutorial, 2005, 7(2)

[3] 何盈捷，冯月利，王珊. Peer-to-Peer 环境下基于内容的智能搜索. 计算机研究与发展，2004，41(增刊)：112-118

[4] 杨舰，吕智慧，钟亦平，等. 一种基于兴趣域的高效对等网络搜索方案. 计算机研究与发展，2005，42(5)：804-809

[5] Upadrashta Y, Vassileva J, Grassmann W. Social networks in Peer-to-Peer systems// Proceedings of the 38th Annual Hawaii International Conference (HICSS'05). Kona, Hawaii, 2005

[6] Tsoumakos D, Roussopoulos N. Adaptive probabilistic search for Peer-to-Peer networks// Proceedings of 3rd Int'l Conf. Peer-to-Peer Computing (P2P 2003). Linkoping, Sweden: IEEE Computer Society, 2003: 102-110

[7] Zeinalipour-Yazti D, Kalogeraki V, Gunopulos D. Exploiting locality for scalable information retrieval in Peer-to-Peer networks. Journal of Information Systems, 2005, 30(4): 277-298

[8] Menasce D, Kanchanapalli L. Probabilistic scalable P2P resource location services. ACM SIGMETRICS Performance Evaluation Review, 2002, 30(2): 48-58

[9] Sripanidkulchai K, Maggs B, Zhang H. Efficient content location using interest-based locality in Peer-to-Peer systems. IEEE Infocom 2003. San Francisco, USA, 2003

[10] Ramanathan M K, Kalogeraki V, Pruyne J. Finding good peers in Peer-to-Peer networks// Proceedings of International Parallel and Distributed and Computing Symposium (IPDPS' 02). Fort Lauderdale, FL, 2002

[11] 陈海涛，龚正虎，黄遵国. 一种基于学习的 P2P 搜索算法. 计算机研究与发展，2005，42(9)：1600-1604

[12] 肖卫东，唐九阳，汤大权，等. 基于社会学原理的 P2P 网络模型 REC. 计算机科学，2007，34(6)：38-40

[13] 唐九阳，张维明，肖卫东，等. 类人类社会基于社区的对等网自组织构造. 计算机研究与发展，2006，43(8)：1383-1390