基于信息空间划分的高效发布订阅路由技术*)

逯 鹏[1,2] 刘旭东[2] 林学练[2] 王 斌[2]

(郑州大学电气工程学院 郑州 450001)[1] (北京航空航天大学计算机学院 北京 100083)[2]

摘 要 在大规模的基于内容发布订阅系统中,路由效率是影响系统性能的关键因素。本文在基于K-D树划分信息空间方法实现内容发布订阅系统的基础上,利用K-D树的索引机制,实现了面向扁平网络的应用层分级路由算法Spanhop。该算法机制减少了应用层路由跳,将路由效率提高到O(lnN)。进一步,针对路由算法中应用层和网络层相邻关系不一致的问题,采用GNP(Global Network Position)空间与ESPN(Event Space Partition Network)空间建立映射关系并在代理网络中维护GNP坐标索引的方法,支持应用层代理基于网络层的相邻关系搜索并选择下一跳路由。该方法减少了Spanhop路由过程中消息在网络层的实际转发路径和响应时间,在低维护代价条件下,提高了路由的效率。算法性能分析表明,上述方法解决了基于信息空间划分的内容发布/订阅系统的路由效率问题。

关键词 信息空间,路由,网络,拓扑感知

Efficient Routing Technique for Publish/Subscribe System Based on Information Partitioning

LU Peng[1,2] LIU Xu-Dong[2] LIN Xue-Lian[2] WANG Bin[2]

(School of Computer Science and Technology, Beihang University, Beijing 100083)[1]

(School of Electrical Engineering , Zhengzhou University, Zhengzhou 450001)[2]

Abstract Routing efficiency is key to design a large scale content-based publish/subscribe system. The K-D tree partition method is used to realize content-based publish/subscribe system which is based on partitioning information space. On this basis, a hierarchical application-level routing algorithm which oriented flat network with the K-D trees index mechanism was implemented. This algorithm reduced the application-level routing hops and got routing efficiency to O(lnN). Furthermore, in view of the inconsistencies of neighboring relations between application-level and the network-level in the routing algorithm, the method of constructing mapping relation between two Cartesian spaces which was GNP(Global Network Position) and ESPN(Event Space Partition Network) and maintaining coordinates of GNP in broker network was used to support brokers in application-level search and select next hop based on the neighboring relation of network-level nodes. This method reduced the real message forwarding path length and routing latency and got high routing efficiency with low maintaining cost. Performance analysis shows that these algorithms addressed efficient routing problems in content-based publish/subscribe system based on information space partitioning.

Keywords Publish/subscribe, Routing, Load balancing, Network

基于内容发布订阅系统是分布式通信领域研究的热点[1~3]。与基于主题的系统相比较,它通过一组事件内容的属性表达事件,更具有通用性。但高语义表达能力也增加了系统内容匹配和路由算法的复杂度,降低了系统的效率[2]。因此,近年来大量工作关注高效率的内容匹配和路由算法问题。文[3、4]均采用了事件空间划分的方法实现基于内容的发布订阅系统,并基于贪婪路由机制取消了路由过程中的内容匹配操作,提高了路由的效率。但与传统因特网的路由效率相比较,仍不能满足面向广域网络的发布订阅系统的性能要求。

我们在文[4]提出的K-D树划分信息空间方法的基础上,提出了面向扁平网络的分级路由算法Spanhop,目的是减少消息路由路径长度。采用网络拓扑感知的方法支持应用层代理,选择网络层相邻的下一跳代理,目的是在低维护代价下减少消息在网络层的实际转发跳数。主要的贡献在于:①基于K-D树的划分提出了一种面向扁平网络的分级路由算法Spanhop及其相关的路由更新和维护策略,将事件路由效率提高到O(lnN);②基于GNP(Globla Network Position)提出了基于网络层拓扑感知的路由优化方法,优化了网络层路由效率。

1 信息空间的K-D树划分

信息空间划分的基本思想是首先假定发布订阅系统中事件内容的d个属性分别表示信息空间Ω的d维;然后将空间划分为多个逻辑订阅区域,区域连接了具有共同兴趣的发布和订阅者;最后,发布者和订阅者向区域发布和订阅相关事件,以及区域代理的匹配和路由操作完成通知订阅者的过程。

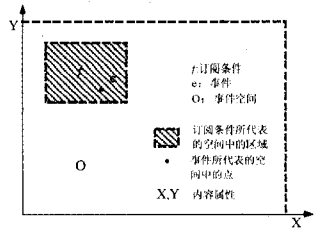

图1 事件空间

*)国家自然科学基金(No. 90412011);国家"863"计划(No. 2003AA119030)。逯 鹏 讲师,博士。

文[4]提出了采用 K-D 树划分的方法，优化信息空间的划分。划分过程首先假定空间 Ω 代表二叉树的根，然后沿 Ω 的第 t 维划分为两个负载相同的区域 z_1，z_2，即 $M(z_1)=M(z_2)$，负载函数 M 与数据分布相关；二叉树的叶子节点分别为 z_1，z_2；此后分别以左子树和右子树为根，层次遍历叶子节点。在每个叶子节点依次并循环沿 Ω 的不同维划分当前区域，直至形成 N 个区域。代理的加入和退出可以理解为叶子节点的合并和分裂过程。二维信息空间划分如图 1 所示，K-D 划分树如图 2 所示。基本 K-D 树划分中，区域代理只需要维护四元组（ID，IP，Zone-corrdinate，Last-Dimension）和相邻代理的信息，就能够基于贪婪路由算法完成发布订阅通信，路由效率是 $O(\frac{d}{4}N^{1/d})$，如图 3 所示。其中，ID、IP 标识了代理的命名和网络层地址，Zone-corrdinate、Last-Dimension 标识了区域[1]的信息空间坐标和最后一次划分维。更详细描述参见文[4]。

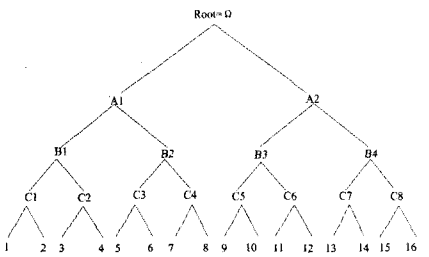

图 2　事件空间的划分树

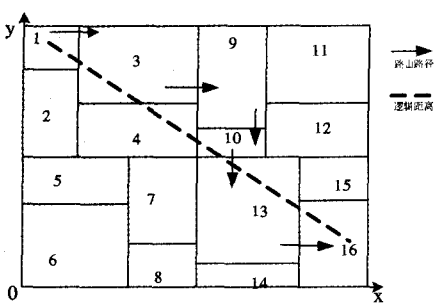

图 3　信息空间划分及贪婪路由示意图

2　路由优化

在信息空间维数（d）一定的情况下，当系统规模（N）增加，贪婪路由 $O(\frac{d}{4}N^{1/d})$ 的效率只能通过增加事件属性（d）提高。但事件匹配的复杂性 $O(d!)$ 增加，降低了内容匹配的效率，增加了路由维护代价（$O(2d)$），因此造成了路由效率、匹配效率、系统可伸缩性之间的矛盾。利用 K-D 树索引能够实现优于贪婪路由的分层路由且路由效率与 d 无关，称为 Spanhop 路由算法。

2.1　算法思想

将 K-D 树不同层次的中间区域划分状态理解为相应的代理网络，则整个划分完成便形成了层叠网络。如图 4 所示，空间 Ω 形成了 5 个划分：

$P_0=\{root\}$，

$P_1=\{AL1,AL2\}$，

$P_2=\{BL1,BL2,BL3,BL4\}$，

$P_3=\{CL1,CL2,\cdots,CL8\}$，

$P_4=\{B1,B2,\cdots,B16\}$。

P_4 映射为代理网络，如图 3 所示。$P_0\sim P_3$ 是 P_4 的中间状态。如果将 P_j 中有共同祖先的代理理解为一个路由域，那么上层划分 $P_k(k<j)$ 中祖先的相邻关系就确定了路由域之间的相邻关系。例如：将 P_4 分为四个路由域{B1，B2，…，B4}，{B5，B6，…，B8}，{B9，B10…，B12} {B13，B14，…，B16}，那么上层 P_2 中{BL1，BL2，BL3，BL4}的相邻关系则决定了 P_4 中四个路由域间的相邻关系。因此，除区域相邻关系外，代理间还具有共同祖先关系。基于上述分析，Spanhop 分层路由的基本过程是：首先确定事件的目的代理所在的路由域，然后将事件基于分层路由机制通过相邻路由域转发到该路由域，最后在域内使用贪婪路由转发目的代理，如图 3 所示。

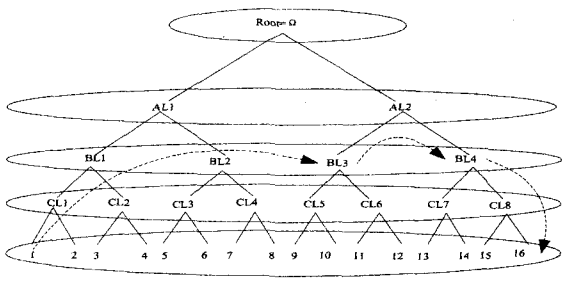

图 4　Spanhop 路由示意图

2.2　Spanhop 路由算法

在基本 K-D 树划分中代理只维护了相邻代理的信息，如何建立并维护层叠网络的索引信息，是实现分级路由的关键问题。

设路由表 RT 记录了相邻代理信息。其中，RT. cz 标识了区域坐标，RT. nb 记录了相邻代理列表，RT. L 标识了当前区域已经进行的分裂次数，即当前虚拟层叠网络的层次。设置路由数据结构祖先队列 AQ(Ancestor Queue)，维护祖先代理的相邻关系。其建立策略是：Bx 所在区域每经过 *lbm* 次划分，则将当前 Bx. RT 复制到队列 Bx. AQ。新加入代理则继承父代理的 AQ. AQ 解决了 K-D 树划分过程中保存树索引信息的问题，主要用于域间分层路由。m 限定了路由域内代理的数量，即分层路由的跨度。如图 3 所示，$m=4$，$lbm=2$，即每经过 2 次划分，代理当前的路由表则加入队列。B1. AQ 维护了与 BL3 的相邻关系。Spanhop 路由如算法 1 所示。

算法 1　Spanhop 路由算法

```
输入：事件 e
输出：无
步骤：
1. for(j=0;j<d;j++){
2.   if((e. Cor_j. Low>RT. cz. Cor_j. Low)
3.     and(e. Cor_j. Up<RT. cz. Cor_j. Up)){
4.     receivee);
5.     break;
6.   }//if e⊆RT. cz
7. }//for
8. for (i=0;i<AQ. length;i++){
9.   qRT=AQ. item [i];
10.    for(j=0;j<d;j++){
11.      if((e. Cor_j. Low<qRT. Cor_j. Low)
12.        or(e. Cor_j. Up>qRT. Cor_j. Up)){
13.      AQroute(e ,qRT. nb);
14.      break;
15.    }//if (e. zoneq⊄RT. cz)
```

[1] 以下根据上下文混合使用区域和代理名词，表达同一含义。

```
16.    }//for
17. }//for
18. Route(e,RT. nb);
```

算法 1 中(Cor_i. Low, Cor_i. Up]是第 i 维坐标区间. *e. zone* 表示了事件 e 的目的区域。算法首先基于 e 与当前区域的坐标关系判断是否接收 e(第 1～7 行);是,则接收完成路由(第 4～5 行);否则,顺序查找 AQ 中其路由表所属区域不包含 e 的 RT_i(第 8～17 行),这是当前跨度最大的路由跳;未找到,则使用当前 RT 基于相邻关系路由。

如图 5 所示:设 *e. zone*=$B16$。$RT.cz.B1$ 接收到 e 后,判断 *e. zone*⊄$B1.RT.cz$;顺序查找 $B1.AQ$,判断 *e. zone*⊂$B1.RT_0.cz=\Omega$ 不符合条件,而 *e. zone*⊄$B1.RT_1.cz$;符合判断条件。因此使用 $B1.RT_1$ 转发 e 到 $B9$。类似地,$B9$ 转发 e 到 $B13$;$B13$ 则通过 $B13.RT.nb$ 路由 e 到目标代理 $B16$;$B16$ 判断 e⊂$B16.cz$,接受 e,路由完成。图 4 是该过程在 K-D 树上的过程显示。

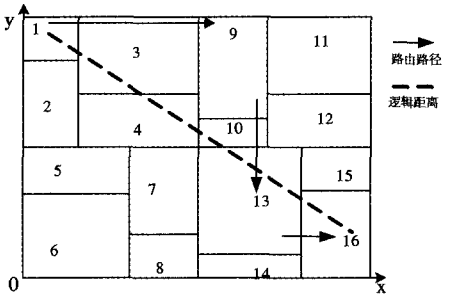

图 5　Spanhop 路由示意图

算法 1 中顺序查找 AQ 保证了 Spanhop 路由的每跳是当前跨度最大的一跳。订阅条件路由算法与算法 1 相同,但由于订阅条件与区域并不是完全重合,所以需要由接入代理将其转换为多个目标区域。目标区域代理基于到达的订阅条件进行事件匹配,并完成通知分发的过程。通知路由可以采用单播的 Spanhop 路由,但更有效的方式是采用多播实现,作为后续工作讨论。

2.3　路由维护和失效处理

通过心跳算法进行周期性的探测,能够实现 RT 的维护和更新[4]。AQ 队列的维护则是在区域的分裂和合并过程中通过 RT 的入/出队操作实现。主要的问题在于,当 AQ 中路由表所记录的代理失效,如何处理。处理策略包括三种情况:

(1)由于路由域内代理具有共同祖先且继承了其路由表,从而具有相同的域间路由能力。因此,当其中一个代理失效,可以选择域内其它代理,实现路由。例如当 $B9$ 失效,Spanhop 可以通过选择路径 $B1$,$B5$,$B13$,$B16$ 的方式实现路由。

(2)如果域内 m 个代理全部失效,则可以通过减小跨度,即选择 AQ 的下一个路由表($AQ.RT_{[i+1]}$)寻找其它路由转发代理,实现路由。

(3)当 AQ 中记录的所有代理失效,则使用 RT 完成路由。

上述失效处理表明,Spanhop 是一种辅助的高效路由方法,系统仍可以基于邻接代理的协议实现路由。

2.4　算法分析

Spanhop 将路由空间分为 $O(\log_m N)$层,每个路由域有 m 个代理,由于贪婪路由平均路径长度是 $O(\frac{d}{4}N^{1/d})$[4],因此 Spanhop 路由效率是 $O(\frac{d}{4}m^{1/d}*(\log_m N)$。设 $g(m)=\frac{d}{4}m^{1/d}*(\log_m N)$,并且令 $g'(m)=0$,求得 $m\approx e^d$ 时 Spanhop 的平均路径长度取得最小值,近似为 $O(\ln N)$。由于使用了 K-D 树划分,因此 Spanhop 的平均路径与信息空间的维数 d 无关。设每个地址的存储量为常数 c,增长率是 $O(\log_m N)$。当 $m=8$,$N=2^{20}$,*AQ. length*≈6,则每个代理增加的存储代价是 $6dc$。

当 $d=2$ 的时候,随着代理数量的增加,量中路由的平均路由跳数的比较如图 6 所示。

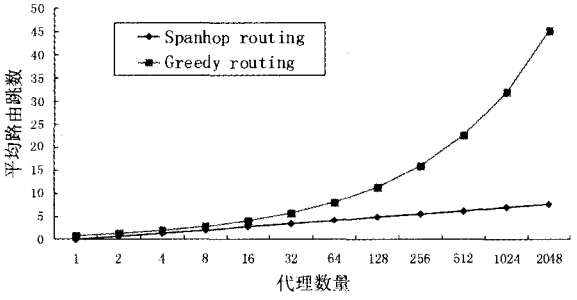

图 6　路由效率比较

图 6 表明,在 d 较小的情况下,随着系统规模的增加,Spanhop 路由效果更为明显。虽然,在 d 较大的情况下,例如 $d>7$ 的情况下,贪婪路由能够达到同样的路由效果,但其事件匹配的复杂度 $O(d!)>5040$。由于 Spanhop 路由与 d 无关,所以其优势在于不增加匹配复杂性的情况下提高了路由的效率。

传统的基于内容发布订阅系统通常基于路由树实现消息转发[5,14]。其中,代理既是路由器也是匹配器,并基于每跳路由过程中的匹配结果确定下一跳。这种方法的路由效率是 $O(N)$。虽然结合多播机制能够提高路由的效率[10],但是系统的可伸缩性和可维护性仍较弱。Hermes[11],Scribe[12]等基于 P2P 实现的内容发布/订阅系统虽然取消了拓扑结构的限制,但也使用了基于广播机制的逆向路径转发算法,并且内容属性转换为关键字或者数字标识,不支持基于属性区间的订阅机制。路由效率介于 $O(N)$～$O(\mathrm{lb}N)$。

3　网络拓扑感知的路由

在一些发布订阅系统中[6～9],采用基于网络层相邻关系部署代理的方法保持层叠网络之间相邻关系的一致性,要求代理必须部署在与其网络层相邻的代理附近。这种部署方法造成了代理的部署位置与其实际网络层位置的紧耦合并产生依赖性。此外,应用层节点的非均匀部署易造成节点负载的失衡,增加系统维护代价,进一步限制发布订阅系统的可伸缩性和应用场景。基于信息空间划分的发布订阅系统,其中的特点是代理所驻留的逻辑区域网络(称之为 ESPN: Event Space Partition Network)是动态变化的,并基于区域网络的动态变化而不是物理代理部署位置的变化,提高系统路由效率。但产生的问题是:应用层相邻的代理在网络层并不一定是相邻的,并且可能距离很大,从而造成应用层的下一跳在网络层需要多跳,增加了路由的实际响应时间。因此,本节主要解决如何在基于信息空间划分的路由中选择网络层距离最近的相邻代理作为下一跳。

3.1　算法思想

文[5]描述了一种基于界标服务器的因特网节点间距离度量方法。该方法通过测量节点到一组界标服务器的距离,

赋予每个节点一个笛卡尔空间坐标，并使用坐标之间的距离表示节点之间的实际距离，称为全局网络定位 GNP(Global Network Position)方法。由于 GNP 具有与信息空间相类似的笛卡儿空间，因此网络拓扑感知算法的基本思想是建立代理的网络层 GNP 坐标和应用层 ESPN 坐标之间的关联关系，从而使代理能够基于相邻区域中驻留代理的 GNP 坐标索引选择网络层相邻的下一跳。

算法思想的基本原理是 GNP 空间中相邻的代理在 ESPN 网络区域中的映像仍然相邻。如图 7 所示。由于 GNP 方法支持向 $n(n<m)$ 维笛卡尔空间的转换[5]，因此不妨设 GNP 空间与事件空间同维。映射函数 Scale()[2] 将 GNP 坐标映射为一个 ESPN 坐标，且保留了 GNP 坐标之间的距离和相邻关系。由于两个空间是同维笛卡尔空间，因此 Scale()可以采用两个空间之间的投影实现，即将整个 GNP 坐标伸缩到信息空间中的一个区域。

称这种基于笛卡尔空间映射关系感知网络层拓扑的方法为 MGNP(Mixture Global Network Position)。

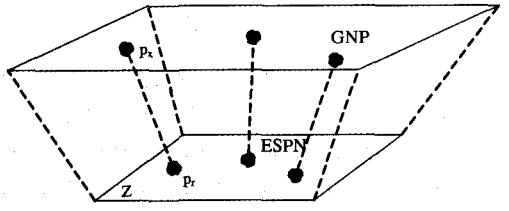

图 7　GNP 空间和 ESPN 空间中区域的映射关系

3.2　算法描述

实现上述算法思想主要基于两个步骤：首先是将 GNP 坐标在 ESPN 网络的区域中进行发布，如算法 2 所示；其次，是代理基于其 GNP 坐标获得索引并选择近程代理，如算法 3 所示。

GNP 坐标的发布过程需要注意的是，位于 Spanhop 路由路径上的代理 Bx 在逻辑网络的所有层次区域都有驻留，因此需要将 GNP 坐标映射到其驻留的各个层次的 ESPN 网络区域(最多 $\log_m N$ 个区域)中分别发布，并且在区域的驻留代理维护该坐标。

算法 2　代理 Bx 的 GNP 坐标发布过程

```
输入:代理 Bx
输出:无
步骤:
1. Bx. GNP=getGNP();
2. if(Bx is new broker)then{
3.    for(i=1;i<=logmN;i++){//logmN 是当前层数
4.       P'=Scale(Bx. GNP,RTi. Zone);
5.       B=getbyindex(P');
6.       B. index={RTi. cz,Bx. ip,Bx. GNP}
7.    }//for
8. }//if
9. if(Bx. L mod log2m=0){
10.    Bx. AQ. Enqueue(Bx. RT);
11.    P'=Scale(Bx. GNP,Bx. cz);//将 GNP 坐标映射到区域 Z
12.    B=getbyindex(P');//获得 P'所在区域的代理;
13.    B. index={RT. cz,Bx. ip,Bx. GNP};//将 GNP 坐标存储在 P'
       所在的区域的代理
14. }//if
15. end.
```

算法中，代理仅当区域逻辑分层时发布 GNP 信息，而新加入代理必须在所有层次的驻留区域中发布，保证 GNP 坐标信息得到完整的发布。算法首先获得代理的 GNP 坐标(算法第 1 行)。如果是新加入代理，则代理需要在其所处的各个层次网络中的区域发布其 GNP 坐标(算法第 2～8 行)。如果代理是系统中已有的代理，则每当其分裂 lbm 次，在其所处的新的区域中发布 GNP 坐标(算法第 9～14 行)。

算法 3 在 ESPN 网络中建立 GNP 坐标的索引系统，算法 3 支持任意代理获得该索引，并进一步在本地判断网络层相邻的节点。

算法 3　近程代理选择

```
步骤:
1. Z=Bx. neighbor. cz;//获得当前代理下一跳目标区域的坐标 Z;
2. P=Scale(By. GNP,Z);//将 By 的 GNP 坐标映射到区域 Z 中的坐
   标;
3. B=getbrokerbyGNP(P);//获得 P 所在区域的代理 B;
4. if B. index()null then
5.    return B. index;
6. else
7. do {
8. modify(P);// 修正 P
9. By=getbrokerbyGNP(P);
10. }while (By. index = null)
11. nexthop= Shortest_distance(B. index,Bx);
12. return nexthop;
13. end.
```

算法 3 首先获得当前代理下一跳目标区域的坐标 Z(算法第 1 行)；然后将代理的 GNP 坐标映射到区域 Z，从而索引到相应位置的代理 Bx(算法第 2～3 行)；如果 Bx 中已经存在发布的 GNP 信息，则获取并返回(算法 4～5 行)，否则修正 P_x，寻找当前最接近的区域驻留代理(算法第 6～10 行)，基于返回的 GNP 信息和当前代理的 GNP 坐标，选择其中网络层距离最近的作为下一跳(算法第 11 行)。

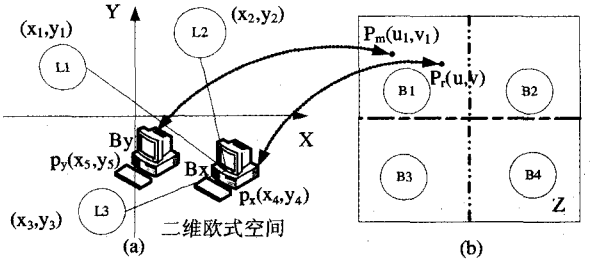

图 8　坐标映射

算法 3 的举例如图 8 所示。By 首先将其坐标映射到区域 Z 中的 P_m，然后获得该位置的驻留代理 $B1$ 的信息并由 $B1$ 获得在该代理发布的 GNP 坐标信息 Bx，因此，By 查找到 Bx 为近程代理。如果没有查找到 Bx，则 By 在 P_m 附近的区域中查找近程代理信息，例如 $B2$，$B3$ 所在的区域。需要指出的是，近程代理只需要定位一次。当接受订阅的代理发生区域和位置的变化，则基于订阅信息通知所有的订阅代理改变其存储的索引信息或者重新进行定位。

上述步骤详细描述为：设代理 Bx 的 GNP 坐标是 p_x，映射函数 $Scale()$ 将 $p_x=(x_4,y_4)$ 映射为信息空间 Spanhop 区域中的坐标 $p_r=(u,v)$。然后，Bx 将 p_x 发布到 p_r 的驻留代理 $B1$。发布完成，区域 Z 中形成了 p_x 的映射 p_r，任意代理可以订阅 Bx 的 GNP 信息，从而判断是否选择 Bx 作为近程路由的下一跳代理，其订阅条件是 p_x。例如，代理 Bx 的 GNP 坐标 $p_x(x_4,y_4)$，经过 $Scale()$ 映射到区域 Z 中的坐标 $p_r(u,v)$，p_r 点所在区域的驻留代理是 $B1$，因此 Bx 的 GNP 坐标信息发布到 $B1$，并由 $B1$ 维护其相关信息。

3.3　算法分析

通过 ESPN 网络与 GNP 方法的结合，算法搜索范围的直径由 n-hops 缩小到 1-hop，其代价是在层叠网络中每个代理

[2] 由于是同维空间，$Scale()$可以是形如 $P_1=\alpha P_2$，$0<\alpha<1$ 的两个坐标空间的转换，α 是伸缩系数。

最多维护 $\log_m N$ 个 GNP 坐标的信息。假定 $N=2^{20}$，$m=4$，$\log_m N=10$。在每个代理增加了 10 个辅助的 GNP 坐标索引的存储开销。这种搜索效率优于分布式系统中通常采用的网络层拓扑感知方法，例如扩展环搜索、启发式搜索，$O(n)$的搜索效率。

在文[13]以及其它发布订阅系统中，通常采用度量所有相邻代理的 RTT(Round-Trip-Time)的方法来解决应用层路由中存在的问题。但在大规模系统中，这种方法需要在每跳路由进行 $O(m)$次度量，m 是相邻代理的数量，效率比较低。本文的方法通过获取 GNP 坐标，取消了每跳度量 RTT 产生的开销。

结束语 在基于 K-D 树划分信息空间实现发布订阅系统的基础上，Spanhop 路由算法和相关拓扑感知策略不仅减少了消息在系统中的转发次数，同时通过网络层的拓扑感知减少了网络层的实际转发距离。同时，算法对于解决扁平层叠网络中的消息路由问题具有一定的参考作用。存在的主要问题是，对信息空间划分方法的依赖性比较强，目前适用的范围有限。后续的工作是进一步研究在信息空间划分基础上的多播通知路由策略以及基于发布订阅中间件系统的实现相关问题。

参 考 文 献

1 Eugster Patrick T H, Felber P, Guerraoui R, et al. The Many Faces of Publish/Subscribe [J]. ACM Computing Surveys, 2003, 35(2): 114～131

2 Carzaniga A, Rosenblum D S, Wolf A L. Archieving scalability and expressiveness in an Internet-Scale event notification service [A]. In: Proceedings of 19th ACM Symposium on Principles of Distributed Computing(PODC2000)[C], 2000. 219～227

3 Wang Y M, Qiu L, Achlioptas D, et al. Subscription partitioning and routing in content-based publish/subscribe networks [A]. In: Dahlia Malkhi, ed. 16th International Symposium on Distributed Computing [C]. Berlin: Springer- Verlag, 2002. 28～30

4 逯鹏，刘旭东，林学练，等. 基于兴趣划分的内容发布订阅系统关键算法[J]. 北京航空航天大学学报，2006，32(8)：992～997

5 Eugene Ng T S, Zhang Hui. Towards Global Network Positioning [A]. In: Proceedings of the ACM SIGCOMM Internet Measurement Workshop [C]. New York: ACM Press, 2001. 25～29

6 Cao F, Singh J P. MEDYM: An architecture for content-based publish-subscribe networks. In: Proceedings of ACM SIGCOMM, Portland, OG, Aug. 2004

7 Cugola G, Nitto E D, Fuggetta A. The JEDI event-based infrastructure and its application to the development of the OPSS WFMS. IEEE Trans. on Software Engineering, 2001, 27(9): 827～850

8 Carzaniga A, Rutherford M J, Wolf A L. A routing scheme for content-based networking. In: Proceedings of IEEE INFOCOM, Hongkong, China, Mar. 2004

9 Mühl G. Large-Scale content-based publish/subscribe systems: [Ph. D Thesis]. Darmstadt University of Technology, 2002

10 薛涛，冯博琴. 内容发布订阅系统路由算法和自配置策略研究[J]. 软件学报，2005, 16(2): 251～259

11 Pietzuch P R. Hermes: A scalable event-based middleware: [Ph D Thesis]. University of Cambridge, 2004

12 Castro M, Druschel P, et al. SCRIBE: A large-scale and decentralized application-level multicast infrastructure [J]. IEEE Journal on Selected Areas in communications (JSAC), 2002, 20(8): 1489～1499

13 Baldoni R, Marchetti C, Virgillito A. Content-based Publish-Subscribe over Structured Overlay Networks [A]. In: Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICSCS'05)[C], 2005. 437～446

14 Banavar G, Chandra T, Mukherjee B, et al. An efficient multicast protocol for content-based publish-subscribe systems [A]. In: Dahlin M, ed. International Conference on Distributed Computing Systems [C], Washington, DC USA: IEEE Computer Society, 1999. 262～272

(上接第 82 页)

$$\log_2 n'_i \geqslant n(w-1) \geqslant (n-1)w \geqslant 0$$

于是，作为密钥更新开销的一部分，密钥更新消息(n'_1, n'_2)的比特长度为 $\log_2 n'_1 + \log_2 n'_2 = \Omega(w)$。这使得 C 方案仍未摆脱传统两两密钥类方案的一个共同局限性——承受不可扩展的通信开销。

结束语 本文研究了 C 密码和 C 方案的安全性及其在安全组播通信中的应用可行性问题。计算出的密钥量表明 C 密码能较好地抵抗穷举密钥攻击；尽管 C 方案不具备严格意义上的前向/后向保密性，但对密钥组合攻击和同余碰撞攻击是计算上安全的。然而，C 密码对已知明文攻击的脆弱性使得它不适于对组播通信提供保密性安全服务；尽管 C 方案是与传统两两密钥管理不同的新方案，但仍未摆脱通信开销不可扩展的传统局限性。

鉴于 C 密码是图像加密系统中广义猫映射的运用和 Hill 密码的变种、对称密码学中的置换密码又可视为 Hill 密码的特款[9]、影子密钥概念包含公钥密码学中起着基础作用的大素数模运算，本文的方法与结果将对 GKM 的研究产生一定积极作用。

参 考 文 献

1 Hardjono T, Dondeti L R. Multicast and Group Security. Norwood [M]. MA: Artech House, INC, 2003

2 Challal Y, Bouabdallah A, Seba H. A Taxonomy of Group Key Management Protocols: Issues and Solutions [J]. Transactions on Engineering, Computing and Technology, 2005, 6 (2): 5～17

3 Chiu Y P, Lei C L, Huang C Y. Secure Multicast Using Proxy Encryption [C]. In: Proceedings of the 7th International Conference on Information and Communications Security (ICICS '05, Beijing), Springer LNCS 3783, 2005. 280～290

4 Wong C K, Gouda M, Lam S S. Secure Group Communications Using Key Graphs [J]. IEEE/ ACM Trans on Networking, 2000, 8(1): 16～31

5 Canetti R, Malkin T, Nissim K. Efficient communication storage tradeoffs for multicast encryption [C]. In: Advances in Cryptology-EUROCRYPT'99, LNCS 1592. Berlin: Springer- Verlag, 1999. 459～474

6 Snoeink J, Suri S, Varghese G. A lower bound for multicast key distribution [J]. Computer Networks, 2005, 47(3): 429～441

7 马在光，丘水生. 基于广义猫映射的一种图像加密系统[J]. 通信学报，2003, 24(2): 51～57

8 曹国梁，周杰. 一种适用于安全多播的加密算法及密钥管理方案[J]. 通信学报，2005, 26(1A): 100～105

9 Stinson D R 著. 密码学原理与实践(第二版)[M]. 冯登国译. 北京：电子工业出版社，2003

10 Jacbson N. Basic Algebra I. 2nd edition [M]. New York: W H Freeman and Company, 1989

11 Menezes A J, van Oorschot P, Vanstone S 著. 应用密码学手册[M]. 胡磊，等译. 北京：电子工业出版社，2005

12 潘承洞，潘承彪. 初等数论. 第二版[M]. 北京：北京大学出版社，2003