[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/56 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810019663.2

[43] 公开日 2008 年 8 月 13 日

[11] 公开号 CN 101242365A

[22] 申请日 2008.3.11
[21] 申请号 200810019663.2
[71] 申请人 南京邮电大学
地址 210003 江苏省南京市新模范马路 66 号
[72] 发明人 孙知信 陈松乐

[74] 专利代理机构 南京经纬专利商标代理有限公司
代理人 叶连生

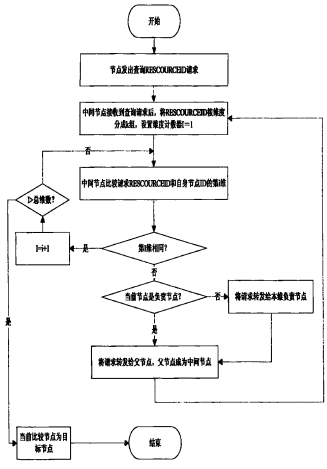
权利要求书 4 页 说明书 10 页 附图 2 页

[54] 发明名称

基于多维分布式哈希表的对等网络安全路由方法

[57] 摘要

基于多维分布式哈希表的对等网络安全路由方法分为多维分布式哈希表结构的设计、路由转发、恶意节点识别方法三部分；多维分布式哈希表它通过将节点的标识划分为不同的维以及每个维度上的负责节点，将整个 P2P 应用的节点组织成一个类似树形的结构，从而为安全的路由转发以及恶意节点的识别提供了基础；路由转发以多维 DHT 结构为基础，将路由转发过程转换为目标节点每个维度上逐步接近的过程，从而可以实现较高的路由效率；恶意节点的识别以分布式哈希表结构以及路由转发为基础，通过同一维度的节点保存的维度信息，识别出各种类型的恶意节点。 通过该结构，能够进行恶意节点有效识别问题，显著的提高了路由的效率。



1. 一种基于多维分布式哈希表的对等网络安全路由方法，其特征在于该方法分为多维分布式哈希表结构的设计、路由转发、恶意节点识别方法三部分；多维分布式哈希表它通过将节点的标识划分为不同的维以及每个维度上的负责节点，将整个P2P应用的节点组织成一个类似树形的结构，从而为安全的路由转发以及恶意节点的识别提供了基础；路由转发以多维DHT结构为基础，将路由转发过程转换为目标节点每个维度上逐步接近的过程，从而可以实现较高的路由效率；恶意节点的识别以分布式哈希表结构以及路由转发为基础，通过同一维度的节点保存的维度信息，识别出各种类型的恶意节点。

2. 根据权利要求1所述的基于多维分布式哈希表的对等网络安全路由方法，其特征在于所述的多维分布式哈希表结构的设计方法为：

假设节点标识、资源标识以n位二进制表示，则将n位标识值依次从最高位开始，取每k位二进制为一组，其中k经验值为16，共划分成m组，则m=n/k，每一组所对应的位数依次为g_1、g_2……g_m，且$\sum_{i=1}^{m} g_i = n$； g_1、g_2……g_m依次对应第1维、第2维……第m维；这些节点的标识通过这样的划分就组织成了一个类似森林的结构，该森林由2^k个子树组成，每个子树的高度是m，其中m是对n位标识值划分的组数，子树的每个节点实际上有2^k个孩子，但是每个节点只保存其中的一个孩子信息，这是因为每个节点的2^k个孩子都是具有相同的父节点，具有相同的维度标识，这2^k个孩子需要相互保存同维度上其他孩子的信息，森林上的节点分为普通节点和负责节点，负责节点就是其父节点保存的孩子节点，该森林上的叶子节点对应了实际P2P网络中的P2P节点，一个P2P节点可能是该森林中的一条搜索路径上的若干个节点。

3. 根据权利要求2所述的基于多维分布式哈希表的对等网络安全路由方法，其特征在于所述的每个普通节点，需要保存的信息如下：

3a. 维度标识：由于每个P2P节点对应了分布式哈希表结构上多个节点，所以通过维度标识来表示其在类森林结构上位置信息；

3b. 下一个维度的负责节点：类森林结构上的每个节点只保存其k个孩子的负责节点；

3c. 同层的所有节点；

3d. 同层的负责节点。

4. 根据权利要求2所述的基于多维分布式哈希表的对等网络安全路由方法，其特征在于所述的每个负责节点，保存的信息如下：

4a. 维度标识：由于每个P2P节点对应了分布式哈希表结构上多个节点，所以通过维度标识来表示其在类森林结构上位置信息；

4b. 下一个维度的负责节点：类森林结构上的每个节点只保存其2^k个孩子的负责节点；

4c. 同层的所有节点；

4d. 同层的负责节点；

4e. 上一个维度的父节点信息。

5. 根据权利要求1所述的基于多维分布式哈希表的对等网络安全路由方法，其特征在于所述的路由转发的方法为：

5a. 节点在进行路由转发的时候根据资源标识及本身所记录的其它节点标识的情况选择路由转发的目标节点；

5b. 当一个节点收到查询请求后，通过比较资源标识和自己的节点标识是否相同，如果相同，说明自己就是目标节点，路由结束，否则进行下一步；

5c. 普通节点收到查询请求后，比较资源标识和自己的维度标识开始前面的位，如果从节点标识的开始和自己维度标识开始之前的位相同，则将该报文转发给同维度的节点，如果从节点标识的开始和自己维度标识开始之前的位不相同，则直接向本维度的负责节点转发该请求；

5d. 负责节点接受到请求后，比较资源标识和自己的维度标识开始前面的位，如果从节点标识的开始和自己维度标识开始之前的位相同，则将该请求转发给同维度的节点，如果从节点标识的开始和自己维度标识开始之前的位不相同，则向上一个维度的父节点转发该请求；

5e. 收到资源请求报文的负责节点继续按上述过程执行路由转发功能，

5f. 最终目标节点：即资源请求报文路由过程中节点标识与查找资源的资源标识最后匹配的节点，也就是说，如果该节点上不存储该资源标识对应的资源信息，那么该资源便不存在。如果有恶意节点的不正确转发，则最终目标节点可能是错误的，该路由转发机制能够保证正确的查询目标节点与最终目标节点处于同

一维度空间。

6. 根据权利要求1所述的基于多维分布式哈希表的对等网络安全路由方法，其特征在于所述的恶意节点识别方法为：

6a. 为了对恶意节点进行有效的识别，系统设置一个全局检举中心，当查询失败的时候，发起查询的节点要把本次查询的历史信息保存到全局检举中心以作为节点在推选负责节点的参考，同时，在有节点进行举报时，检举中心接受检举请求并对提供的证据进行处理，

6b. 为了减少负责节点时恶意节点的概率，本系统对于负责节点采用推荐选举的方法，即每经过一段时间，同一维度的节点共同参予推选负责节点，推选的时候需要和全局检举中心进行交互，获取目标节点为本维节点但交易失败的历史信息、获取本维节点被举报的相关信息。

7. 根据权利要求1所述的基于多维分布式哈希表的对等网络安全路由方法，其特征在于所述的恶意节点的情况包括：

7a. 负责节点为恶意节点的情况：最终目标节点记录与同一维度的所有节点信息可以根据请求资源的资源标识与自己节点标识及其它同一维度空间节点的节点标识的比较判断自己是否为正确目标节点；如果不是正确目标节点，则将该资源请求报文继续转发给正确的目标节点，同时检举转发给自己该消息的负责节点为恶意节点；

7b. 最终目标节点为恶意节点的情况：最终目标节点已经为正确目标节点，但其仍将该资源请求报文转发给其它节点，则此时收到该报文的节点很容易根据自己记录的包括恶意最终目标节点在内的其它节点信息判断出最终目标节点的不正确路由行为；

7c. 最终目标节点与同一维空间其它节点联合进行恶意行为的情况：对于步骤7b）中的情况，联合节点对最终目标节点的恶意转发不检举，这里引进负责节点寻找到最终目标节点之后向资源请求节点报告最终目标节点信息的措施，这样如果资源请求节点最后接收到返回的资源查询结果与负责节点返回的不符，即可识别出恶意行为，并检索恶意节点；

7d. 进行的转发的负责节点与作为其转发目的节点的最终目标节点串通进行恶意行为的情况：即负责节点选择错误的最终目标节点，但该错误最终目标节点并不进行检举的情况，对于这种情况，由于负责节点采用每隔一段时间间隔就推

选的机制，在推选的时候需要到全局举报中心去获取本维节点交易失败信息，通过对交易失败信息的分析，能够有效的识别负责节点和同维中其它节点的串通。

基于多维分布式哈希表的对等网络安全路由方法

技术领域

本发明是一种用于提高 P2P（Peer-to-Peer：对等网络）应用安全性的方法，属于网络中安全技术领域。

背景技术

目前关于结构化P2P叠加网安全研究已经取得了一定的进展。Castro等人在文献[1]中提出，P2P叠加网的安全路由需要满足3个条件，即安全节点ID（标识）分配、路由表安全维护以及安全路由，针对Pastry算法，作者提出通过增加附加路由表来维护路由表安全，在查询到最终有节点声称对查询的key（散列值）负责时，发起节点让该节点返回它的路由表，根据返回的路由表信息判断是否路由正确，如果路由失败则使用冗余路由再次查询获得目标节点，通过这种方法来实现安全路由。尽管增加附加路由表能够限制恶意节点的破坏影响，但是同时降低了Pastry算法的路由效率，在实现安全路由时对于路由是否正确的判断算法在形式上无法证明，而且判断的结果趋向于路由是不正确的，此外，在冗余路由的时候会带来显著的网络流量负荷。Sit 和 Morris对DHT(Distributed Hash Table:分布式哈希表)和构建在DHT上应用受到的可能的攻击进行了分类，并且提出了一些最基本的设计原则来减少被攻击的可能性，但是没有对如何实现安全的路由和维护DHT的安全提出具体的解决方案。Mart等人在文献[2]中提出基于社会联系的DHT安全路由，即节点之间的信任关系是建立在社会联系上的，查询节点在路由的时候根据社会联系的信息来转发路由，而不是仅仅考虑路由的效率，然后，对于社会关系的建立的机制要依赖于其它已经获得广泛应用的网络服务，如Yahoo(雅虎)等，显然，这些网络服务在很多特定的应用场景下是没有提供的。在文献[3]中，作者提出了安全健壮的DHT路由算法:Myrmic，该算法在非在线CA(认证中心)的基础上，增加了在线的邻居认证中心NA(Neighborhood Certificate Authority)，在新的节点加入或者有节点离开的时候，NA通过给一些相关节点发布邻居证书的方式参与DHT的网络管理，查询节点通过收集邻居节点来验证声称对查询的key负责的节

点的正确性。然后NA的证书管理对于证书失效的管理，在快速加入、离开时证书的更新存在一些问题，而且增加的NA，本身就容易受到攻击，在NA失效的时候，新的节点无法加入，此外，这种结构也在一定程度上破坏了P2P的结构。

鉴于以上分析，针对结构化P2P的安全问题，目前解决方案及存在的问题总结如下：

1） 增加全局认证中心，通过认证中心来验证DHT区域邻居信息的正确性，但是认证中心容易遭到攻击，在一定程度上破坏了P2P结构；

2） 在路由选择时，不是基于最优的效率，而是基于一种信任关系，这种信任关系包括社会关系等，但是社会关系建立的机制一般要依赖于其它网络服务；

3） 路由选择时基于最优的路由效率，但是根据对路由的结果的正确性进行判断，判断的依据是根据P2P结构特征的近似判断，在判断结果是路由失败后通过冗余路由来查找正确的目标节点。由于是根据P2P结构特征来近似判断，判断的结果也是近似的，在冗余查询的时候容易导致显著的网络流量负载。

近年来，P2P 作为一种新型的网络技术获取了快速的发展，P2P 的应用范围也越来越广泛，然而，对于如何满足一些安全性要求较高的场景的要求，P2P 技术还面临着很多挑战，这一方面是由于 P2P 技术是一种新型的网络技术，还在不断的发展中，另一方面也是由于 P2P 技术本身的特点决定的。

参考文献

[1]M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. S. Wallach. Secure routing for structured peer-to-peer overlay tworks. In Proceedings of 5th Symposium on Operating Systems Design and Implementation (OSDI' 02), Boston, MA, Dec 2002.

[2] S. Marti, P. Ganesan, and H. Garcia-Molina, "DHT Routing Using Social Links," in First International Workshop on Peerto-Peer and Databases (P2PDB 2004), 2004.

[3] Peng Wang, Ivan Osipkov, Nicholas Hopper, and Yongdae Kim. "Myrmic: Provably secure and efficient DHT routing," 2006.

发明内容

技术问题：本发明的目的是提供一种基于多维 DHT(Distributed Hash Table：

分布式哈希表）的 P2P（对等网络）安全路由方法，通过建立多维 DHT 结构及其路由方法来解决 DHT 的安全维护问题。该方法通过对 NODEID（节点标识）和 RESOUCEID（资源标识）进行按位分解，同一维度的成员了解本维的所有成员信息。通过这样的一种新型 DHT 结构，一方面就能够克服传统 DHT 算法无法利用各个节点保存的部分邻近节点信息进行恶意节点有效识别问题，另一方面，由于实现了维和维的一步直接路由，显著的提高了路由的效率。

技术方案：当前结构化 P2P 网络广泛使用的 DHT，如 Chord、Pastry 都是通过某种散列得到节点的 ID（NODEID）和资源的 ID(RESOURCEID)，这些 NODEID 以及 RESOURCEID 在一维空间上构成了一个环。由于节点数量上的庞大导致每个节点只能维护整个系统中的一部分邻近节点信息，通过每个节点的邻近信息来完成路由，路由的正确性依赖于路由过程中每个路由中间节点的正确性，这就隐藏了很多安全隐患，特别是对如何判别恶意节点还没有简单、高效的方法。

本发明的基于多维分布式哈希表的对等网络安全路由方法分为多维分布式哈希表结构的设计、路由转发、恶意节点识别方法三部分；多维分布式哈希表它通过将节点的标识划分为不同的维以及每个维度上的负责节点，将整个P2P应用的节点组织成一个类似树形的结构，从而为安全的路由转发以及恶意节点的识别提供了基础；路由转发以多维DHT结构为基础，将路由转发过程转换为目标节点每个维度上逐步接近的过程，从而可以实现较高的路由效率；恶意节点的识别以分布式哈希表结构以及路由转发为基础，通过同一维度的节点保存的维度信息，识别出各种类型的恶意节点。

所述的多维分布式哈希表结构的设计方法为：

假设节点标识、资源标识以*n*位二进制表示，则将*n*位标识值依次从最高位开始，取每k位二进制为一组（k经验值为16），共划分成m组，则m=n/k，每一组所对应的位数依次为g_1、g_2……g_m，且$\sum_{i=1}^{m} g_i = n$； g_1、g_2……g_m依次对应第1维、第2维……第*m*维；这些节点的标识通过这样的划分就组织成了一个类似森林的结构，该森林由2^m个子树组成，每个子树的高度是m（m对n位标识值划分的组数），子树的每个节点实际上有k个孩子，但是每个节点只保存其中的一个孩子信息，这是因为每个节点的k个孩子都是具有相同的父节点，具有相同的维度标识，这k个孩子需要相互保存同维度上其他孩子的信息，森林上的节点分为普通节点和负责节

点，负责节点就是其父节点保存的孩子节点，该森林上的叶子节点对应了实际P2P网络中的P2P节点，一个P2P节点可能是该森林中的一条搜索路径上的若干个节点。

所述的每个普通节点，需要保存的信息如下：

3a. 维度标识：由于每个P2P节点对应了分布式哈希表结构上多个节点，所以通过维度标识来表示其在类森林结构上位置信息；

3b. 下一个维度的负责节点：类森林结构上的每个节点只保存其k个孩子的负责节点；

3c. 同层的所有节点；

3d. 同层的负责节点。

所述的每个负责节点，保存的信息如下：

4a. 维度标识：由于每个P2P节点对应了分布式哈希表结构上多个节点，所以通过维度标识来表示其在类森林结构上位置信息；

4b. 下一个维度的负责节点：类森林结构上的每个节点只保存其k个孩子的负责节点；

4c. 同层的所有节点；

4d. 同层的负责节点；

4e. 上一个维度的父节点信息。

所述的路由转发的方法为：

5a. 节点在进行路由转发的时候根据资源标识及本身所记录的其它节点标识的情况选择路由转发的目标节点；

5b. 当一个节点收到查询请求后，通过比较资源标识和自己的节点标识是否相同，如果相同，说明自己就是目标节点，路由结束，否则进行下一步；

5c. 普通节点收到查询请求后，比较资源标识和自己的维度标识开始前面的位，如果从节点标识的开始和自己维度标识开始之前的位相同，则将该报文转发给同维度的节点，如果从节点标识的开始和自己维度标识开始之前的位不相同，则直接向本维度的负责节点转发该请求；

5d. 负责节点接受到请求后，比较资源标识和自己的维度标识开始前面的位，如果从节点标识的开始和自己维度标识开始之前的位相同，则将该请求转发给同维度的节点，如果从节点标识的开始和自己维度标识开始之前的位不相同，则向

上一个维度的父节点转发该请求；

5e. 收到资源请求报文的负责节点继续按上述过程执行路由转发功能，

5f. 最终目标节点：即资源请求报文路由过程中节点标识与查找资源的资源标识最后匹配的节点，也就是说，如果该节点上不存储该资源标识对应的资源信息，那么该资源便不存在。如果有恶意节点的不正确转发，则最终目标节点可能是错误的，该路由转发机制能够保证正确的查询目标节点与最终目标节点处于同一维度空间。

所述的恶意节点识别方法为：

6a. 为了对恶意节点进行有效的识别，系统设置一个全局检举中心，当查询失败的时候，发起查询的节点要把本次查询的历史信息保存到全局检举中心以作为节点在推选负责节点的参考，同时，在有节点进行举报时，检举中心接受检举请求并对提供的证据进行处理，

6b. 为了减少负责节点时恶意节点的概率，本系统对于负责节点采用推荐选举的方法，即每经过一段时间，同一维度的节点共同参予推选负责节点，推选的时候需要和全局检举中心进行交互，获取目标节点为本维节点但交易失败的历史信息、获取本维节点被举报的相关信息。

所述的恶意节点的情况包括：

7a. 负责节点为恶意节点的情况：最终目标节点记录与同一维度的所有节点信息可以根据请求资源的资源标识与自己节点标识及其它同一维度空间节点的节点标识的比较判断自己是否为正确目标节点；如果不是正确目标节点，则将该资源请求报文继续转发给正确的目标节点，同时检举转发给自己该消息的负责节点为恶意节点；

7b. 最终目标节点为恶意节点的情况：最终目标节点已经为正确目标节点，但其仍将该资源请求报文转发给其它节点，则此时收到该报文的节点很容易根据自己记录的包括恶意最终目标节点在内的其它节点信息判断出最终目标节点的不正确路由行为；

7c. 最终目标节点与同一维空间其它节点联合进行恶意行为的情况：对于步骤7b）中的情况，联合节点对最终目标节点的恶意转发不检举，这里引进负责节点寻找到最终目标节点之后向资源请求节点报告最终目标节点信息的措施，这样如果资源请求节点最后接收到返回的资源查询结果与负责节点返回的不符，即可

识别出恶意行为，并检索恶意节点；

7d. 进行的转发的负责节点与作为其转发目的节点的最终目标节点串通进行恶意行为的情况：即负责节点选择错误的最终目标节点，但该错误最终目标节点并不进行检举的情况，对于这种情况，由于负责节点采用每隔一段时间间隔就推选的机制，在推选的时候需要到全局举报中心去获取本维节点交易失败信息，通过对交易失败信息的分析，能够有效的识别负责节点和同维中其它节点的串通。

现有DHT协议中，每个节点保存整个系统中一部分节点的信息，并利用这些所保存的其他节点信息完成路由转发功能。路由的正确性依赖于路由过程中每个路由中间节点的正确性，这就隐藏了很多安全隐患，其中一个比较严峻的问题是如何对恶意节点（进行不正确路由转发的节点）进行有效的识别。如以Chord为例，三个节点A、B、C，其存储的资源信息对应的RESOURCEID依次为5、7、9。A收到查询RESOURCEID=7的资源请求报文之后，故意进行不正确的路由转发，将该报文直接转发给C，如果C不知道其前面的节点B的相关信息的话，则便会导致该资源请求报文返回查找失败信息，而实际上该资源是存在的（参见附图1）。针对这一问题，本方案提出一种基于多维DHT的安全路由方法，并且提供了一种更为有效的进行不正确路由转发的恶意节点的判别方法。

本发明的安全路由方法基于多维的DHT结构，为了提高路由的安全性，本方案提出了一种新型的多维DHT结构，假设每个节点的NODEID、RESOURCEID以n位二进制表示，多维DHT将n位ID值依次（从最高位开始）划分成m组，每一组所对应的位数依次为g1、g2……gm，g1、g2……gm依次为第一维、第二维、…、第m维。每个节点需要保存的信息有维度标识、下一个维度的负责节点、同层的所有节点、同层的负责节点。对于每个维度的负责节点，还需要保存上一个维度的父节点信息。节点在进行路由转发的时候根据RESOURCEID及本身所记录的其它NODEID的情况选择路由转发的目标节点，正常情况下，只有每个维度上的负责节点参与路由，路由转发方法如下：

1）当一个节点收到查询请求后，首先比较RESOURCEID和时，首先在自己所存储的路由信息表中即在自己所处于的维度空间内查找，如果查找成功，则直接向查找结果节点发送资源请求报文；否则，至2）；

2）根据RESOURCEID及所记录的NODEID决定将该资源请求报文转发给哪一个负责节点（因为其所处于的维度空间内可能不止一个负责节点；

3）收到资源请求报文的负责节点继续按上述过程执行路由转发功能。

有益效果：

1） 路由信息表维护消耗小：现有技术如果系统中有一个节点变化，有可能涉及到整个系统中所有节点的路由表更新操作，而本方案中一个节点的变化最多涉及到两个维度空间内的节点；

2） 准确判断整个路由过程的正确性，并能简单有效的定位恶意节点；

3） 路由效率高：完成资源查找最多需要 2(m-1)+1跳（m为划分的维数），而现有技术最多则一般需要logN（N为整个系统中所有节点的数目）；

4） 适用于各种对于安全性较高的要求的P2P应用场景。

附图说明

图1是由于恶意节点的存在导致查找失败的示意图。

图2是多维DHT结构示意图。

图3是基于多维DHT的P2P安全路由方法的流程图。

具体实施方式

本发明的方法分为多维分布式哈希表结构的设计、路由转发、恶意节点识别方法三部分；多维分布式哈希表它通过将节点的标识划分为不同的维以及每个维度上的负责节点，将整个P2P应用的节点组织成一个类似树形的结构，从而为安全的路由转发以及恶意节点的识别提供了基础；路由转发以多维DHT结构为基础，将路由转发过程转换为目标节点每个维度上逐步接近的过程，从而可以实现较高的路由效率；恶意节点的识别以分布式哈希表结构以及路由转发为基础，通过同一维度的节点保存的维度信息，识别出各种类型的恶意节点。

多维DHT的设计

本发明的提出的P2P安全路由方法基于本方案提出的多维DHT结构，多维DHT的设计如附图2所示，假设NODEID、RESOURCEID以*n*位二进制表示，则将*n*位标识值依次从最高位开始，取每k位二进制为一组（k经验值为16），共划分成m组，则m=n/k，每一组所对应的位数依次为g_1、g_2……g_m，且$\sum_{i=1}^{m} g_i = n$。g_1、g_2……

g_m依次对应第1维、第2维……第m维。这些节点的标识通过这样的划分就组织成了一个类似森林的结构，该森林由2^k个子树组成，每个子树的高度是m，子树的每个节点实际上有2^k个孩子，但是每个节点只保存其中的一个孩子信息，这是因为每个节点的2^k个孩子都是具有相同的父节点，具有相同的维度标识，这2^k个孩子需要相互保存同维度上其他孩子的信息，森林上的节点分为普通节点和负责节点，负责节点就是其父节点保存的孩子节点，该森林上的叶子节点对应了实际P2P网络中的P2P节点，但是一个P2P节点可能是该森林中的一条搜索路径上的若干个节点，

每个普通节点需要保存的信息如下：

- 维度标识：由于每个P2P节点对应了DHT结构上多个节点，所以通过维度标识来表示其在类森林结构上位置信息；
- 下一个维度的负责节点：类森林结构上的每个节点只保存其2^k个孩子的负责节点；
- 同层的所有节点；
- 同层的负责节点；

每个负责节点，保存的信息如下：

- 维度标识：由于每个P2P节点对应了DHT结构上多个节点，所以通过维度标识来表示其在类森林结构上位置信息；
- 下一个维度的负责节点：类森林结构上的每个节点只保存其2^k个孩子的负责节点；
- 同层的所有节点；
- 同层的负责节点；
- 上一个维度的父节点信息。

例如，以MD5散列算法生产的节点标识为128位二进制值，则n=128，取k=16，则m=n/k=8，即将n=128位的节点标识划分为8维。这些节点标识组成的类似森林结构含有2^16个子树，每个子树的高度为8。每个父节点实际上拥有2^16节点，但是其只保存其中的一个子节点，属于同维的子节点拥有同维的2^16其它同维节点信息。负责节点还拥有父节点的信息。

路由转发

节点在进行路由转发的时候根据RESOURCEID及本身所记录的其它

NODEID的情况选择路由转发的目标节点。

- 当一个节点收到查询请求后，通过比较RESOURCEID和自己的ID是否相同，如果相同，说明自己就是目标节点，路由结束，否则进行下一步；

- 普通节点收到查询请求后，比较RESOURCEID和自己的维度标识开始前面的位，如果从ID的开始和自己维度标识开始之前的位相同，则将该报文转发给同维度的节点，如果从ID的开始和自己维度标识开始之前的位不相同，则直接向本维度的负责节点转发该请求；

- 负责节点接受到请求后，比较RESOURCEID和自己的维度标识开始前面的位，如果从ID的开始和自己维度标识开始之前的位相同，则将该请求转发给同维度的节点，如果从ID的开始和自己维度标识开始之前的位不相同，则向上一个维度的父节点转发该请求；

- 收到资源请求报文的负责节点继续按上述过程执行路由转发功能。

最终目标节点：即资源请求报文路由过程中NODEID与查找资源的RESOURCEID最后匹配的节点，也就是说，如果该节点上不存储该RESOURCEID对应的资源信息，那么该资源便不存在。如果有恶意节点的不正确转发，则最终目标节点可能是错误的。该路由转发机制能够保证正确的查询目标节点与最终目标节点处于同一维度空间

例如，取n=8，k=2，则m=8/2=4，设查找的资源的标识为11011000，设查询节点的标识为10000000，则查询节点比较自己的标识和查找资源的第一维不同，于是将查询请求转发给第一维的负责节点10******，（*标识该位为1或者0），由于该负责节点保存了第一维所有节点的信息，所以可以将查询直接发送给11******，该复制节点比较查询资源标识和自己负责的第一维相同，于是将查询发给下一维的负责节点1101****，……，重复该查询过程，直到查询到达目的节点11011100。

恶意节点识别方法

为了对恶意节点进行有效的识别，系统设置一个全局检举中心，当查询失败

的时候，发起查询的节点要把本次查询的历史信息保存到全局检举中心以作为节点在推选负责节点的参考，同时，在有节点进行举报时，检举中心接受检举请求并对提供的证据进行处理。

为了减少负责节点时恶意节点的概率，本系统对于负责节点采用推荐选举的方法，即每经过一段时间，同一维度的节点共同参予推选负责节点，推选的时候需要和全局检举中心进行交互，获取目标节点为本维节点但交易失败的历史信息、获取本维节点被举报的相关信息。

1） 负责节点为恶意节点的情况：因为最终目标节点记录与同一维度的所有节点信息，则可以根据请求资源的RESOURCEID与自己NODEID及其它同一维度空间节点的NODEID的比较判断自己是否为正确目标节点，如果不是，则将该资源请求报文继续转发给正确的目标节点，同时检举转发给自己该消息的负责节点为恶意节点；

2） 最终目标节点为恶意节点的情况：最终目标节点已经为正确目标节点，但其仍将该资源请求报文转发给其它节点，则此时收到该报文的节点很容易根据自己记录的包括恶意最终目标节点在内的其它节点信息判断出最终目标节点的不正确路由行为；

3） 最终目标节点与同一维空间其它节点联合进行恶意行为的情况：对于2）中的情况，联合节点对最终目标节点的恶意转发不检举。这里引进负责节点寻找到最终目标节点之后向资源请求节点报告最终目标节点信息的措施，这样如果资源请求节点最后接收到返回的资源查询结果与负责节点返回的不符，即可识别出恶意行为，并检索恶意节点；

4） 进行的转发的负责节点与作为其转发目的节点的最终目标节点串通进行恶意行为的情况：即负责节点选择错误的最终目标节点，但该错误最终目标节点并不进行检举的情况。对于这种情况，由于负责节点采用每隔一段时间间隔就推选的机制，在推选的时候需要到全局举报中心去获取本维节点交易失败信息，通过对交易失败信息的分析，能够有效的识别负责节点和同维中其它节点的串通。

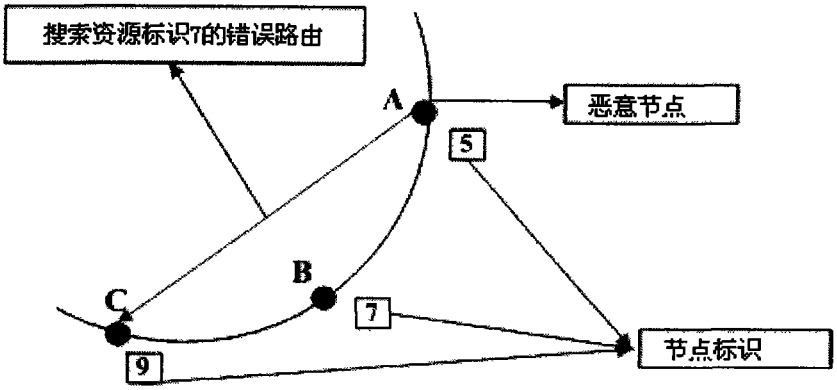


图 1

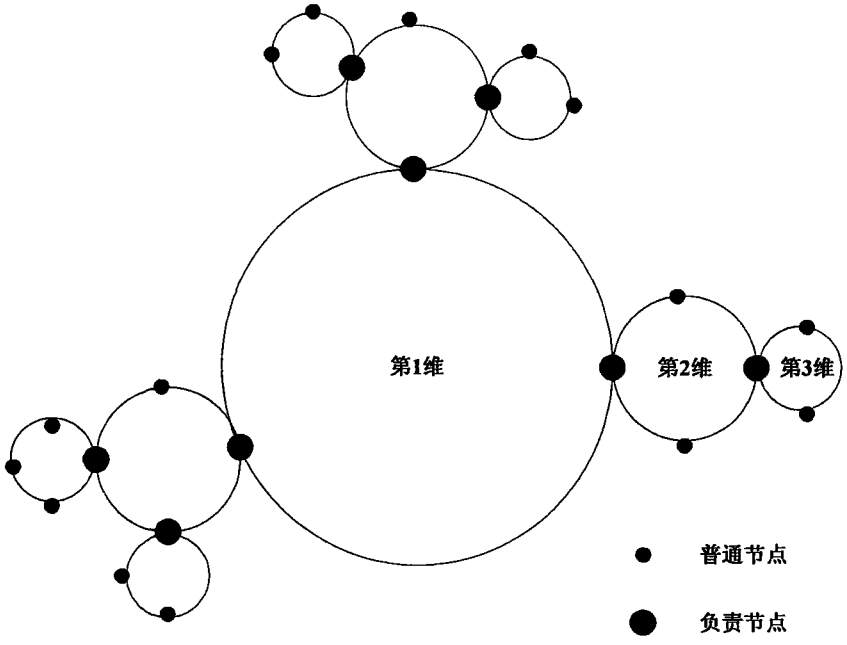


图 2

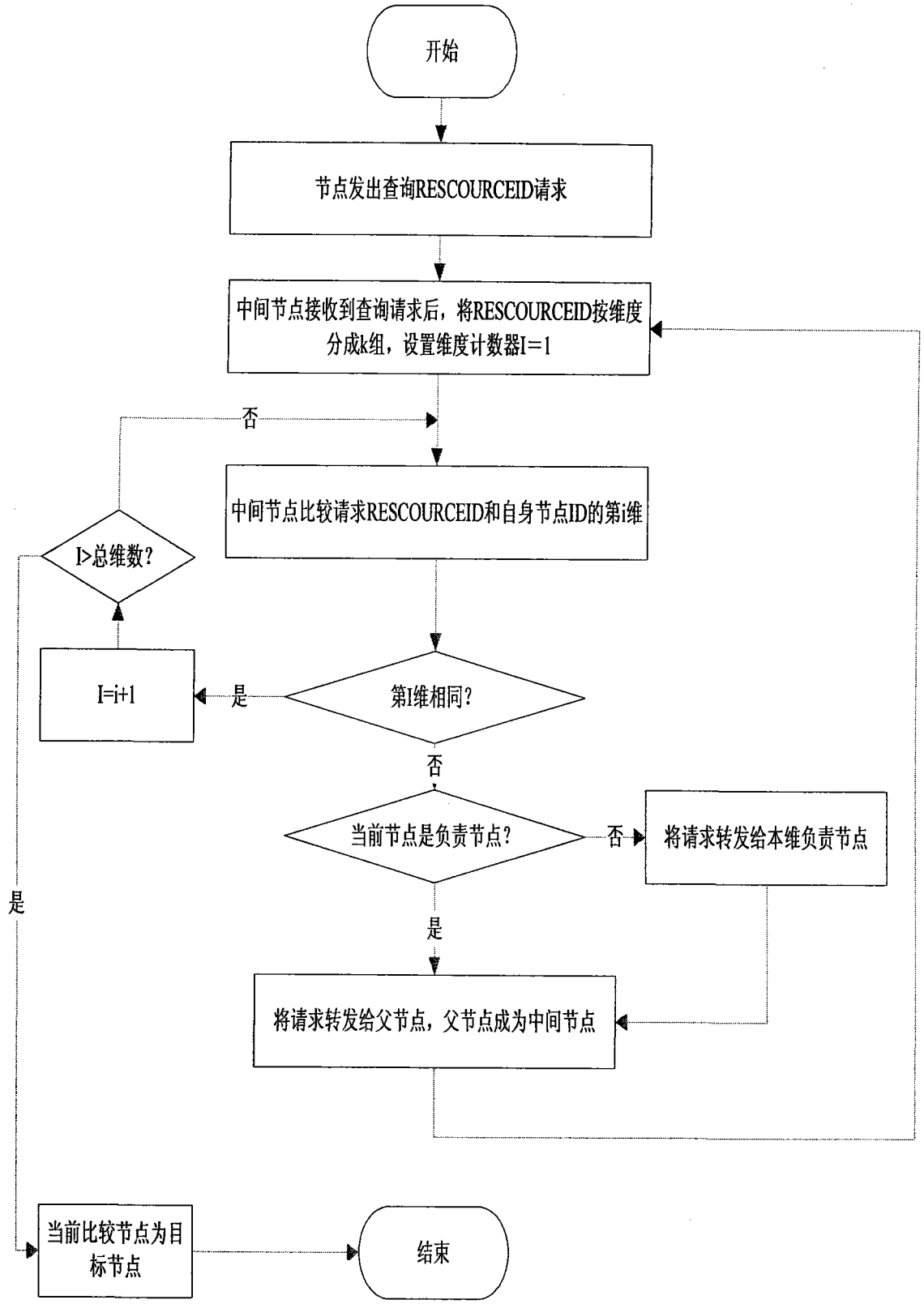

开始
节点发出查询RESCOURCEID请求
中间节点接收到查询请求后，将RESCOURCEID按维度分成k组，设置维度计数器I=1
否
中间节点比较请求RESCOURCEID和自身节点ID的第i维
I>总维数?
I=i+1
是
第I维相同?
否
当前节点是负责节点?
否
将请求转发给本维负责节点
是
是
将请求转发给父节点，父节点成为中间节点
当前比较节点为目标节点
结束

图 3