(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101557335 B
(45)授权公告日 2012.11.21

(21)申请号 200810103905.6

(22)申请日 2008.04.11

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 郑合文

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 何文彬

(51)Int.Cl.
H04L 12/46(2006.01)
H04L 12/28(2006.01)

(56)对比文件
CN 101035270 A,2007.09.12,
CN 101060455 A,2007.10.24,
US 2007/0233832 A1,2007.10.04,
Wen Ji etc..GARM:A Group-Anonymity Reputation Model in Peer-to-Peer System.《IEEE COMPUTER SOCIETY》.2007,
Danyu Zhu etc..Promoting Cooperation Among Strangers to Access Internet Services from an Ad Hoc Network.《IEEE COMPUTER SOCIETY》.2004,

审查员 白雪慧

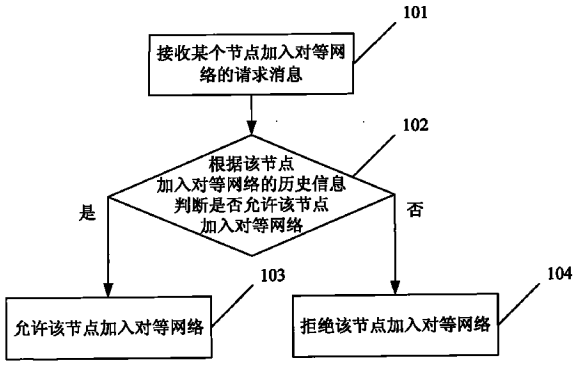
权利要求书 1 页 说明书 7 页 附图 3 页

(54)发明名称

控制节点加入对等网络的方法和装置

(57)摘要

本发明公开了一种控制节点加入对等网络的方法和装置，属于对等网络技术领域。所述方法包括：接收节点加入对等网络的请求消息；根据所述节点加入对等网络的历史信息和已接收的加入对等网络的请求消息的历史信息中的至少一种，确定出不允许所述节点加入所述对等网络时，拒绝所述节点加入所述对等网络。所述装置包括：接收模块和处理模块。本发明实现了对节点加入对等网络进行控制，限制了节点频繁地加入对等网络，从而在一定程度上解决了由于恶意节点频繁加入而导致的对等网络路由抖动、资源不可用甚至失去以及节点拒绝服务等等。与现有的Puzzle机制相比，不需要存储大量的难题，极大地节省了开销，且具有更好的控制效果。



CN 101557335 B

1. 一种控制节点加入对等网络的方法，其特征在于，所述方法包括：

接收节点加入对等网络的请求消息；

判断是否在规定时间内接收到所述节点加入对等网络的请求消息的数目高于预设的第一阈值，并且所述节点在对等网络上多次停留的平均时间低于预设的第二阈值，并且在规定时间内接收到的所有加入对等网络的请求消息的数目高于预设的第三阈值；

如果是，则拒绝所述节点加入所述对等网络。

2. 根据权利要求 1 所述的控制节点加入对等网络的方法，其特征在于，所述拒绝所述节点加入所述对等网络之后，还包括：

记录所述节点本次申请加入所述对等网络的相关信息。

3. 根据权利要求 1 或 2 所述的控制节点加入对等网络的方法，其特征在于，所述拒绝所述节点加入所述对等网络之后，还包括：

通知所述节点在规定时间后重新申请加入所述对等网络。

4. 一种控制节点加入对等网络的装置，其特征在于，所述装置包括：

接收模块，用于接收节点加入对等网络的请求消息；

处理模块，用于在所述接收模块接收到所述请求消息后，判断是否在规定时间内接收到所述节点加入对等网络的请求消息的数目高于预设的第一阈值，并且所述节点在对等网络上多次停留的平均时间低于预设的第二阈值，并且在规定时间内接收到的所有加入对等网络的请求消息的数目高于预设的第三阈值，如果是，则拒绝所述节点加入所述对等网络。

5. 根据权利要求 4 所述的控制节点加入对等网络的装置，其特征于，所述装置还包括：

记录模块，用于记录所述节点本次申请加入所述对等网络的相关信息。

6. 根据权利要求 4 或 5 所述的控制节点加入对等网络的装置，其特征在于，所述装置还包括：

通知模块，用于通知所述节点在规定时间后重新申请加入所述对等网络。

控制节点加入对等网络的方法和装置

技术领域

[0001] 本发明涉及对等网络技术领域，特别涉及一种控制节点加入对等网络的方法和装置。

背景技术

[0002] P2P(Peer to Peer，对等网络）由多个独立的节点相互连接形成，这些节点被称为对等节点。每个对等节点贡献自己的能力并相互协作来提供对等网络服务，当前对等网络服务主要包括分布式存储服务和分布式传送服务。对等网络不是一个实际的物理网络而是一个逻辑网络，它承载于其它网络比如 Internet 之上，通常对等网络由对等节点之间通过传送层连接比如 TCP 连接形成拓扑，这些传送层连接充当对等网络的逻辑链路。对等网络本质上是一个叠加 (Overlay) 网络，可以为不同的应用提供服务，而且由多个对等节点协作提供服务，避免了传统的客户端 / 服务器架构下网络的单点失效风险。目前广泛应用的是结构化对等网络，其特征是对等节点按照选定的规则如 DHT(Distributed Hash Table，分布式哈希表）算法互联并形成邻居关系，通过该算法组织路由表明显降低了节点开销，并确保了分布式查询的成功率与效率。

[0003] 对等节点在对等网络中有着自己独立并且唯一的标识，这个标识被称为对等节点标识即 Peer-D，对等节点标识与该节点在底层承载网络中的 IP 地址无关，与接入网络的位置也无关。使用分布式存储服务保存在对等网络中的资源，在对等网络中也有自己独立的标识，这个标识被称为资源标识即 Resource-ID。在对等网络中，资源标识与节点标识位于同一个数值空间，它们之间可以直接比较，资源通常使用分布式数据库算法保存在固定的对等节点上，该对等节点具有与该资源标识最接近的节点标识。对等网络使用标识（包括节点标识和资源标识）进行路由。

[0004] DHT 算法按照一定的规则，如 Pastry 算法、Tapestry 算法以及 Chord 算法等，将完整的 ID 空间分割为多个独立的 ID 子空间，每个对等节点负责存储一个对应一段资源标识范围的 ID 子空间。对等节点根据获知的邻居节点负责的 ID 空间信息以及学习到的其它节点负责的 ID 空间信息，形成自己的对等网络路由表，并在此基础上完成对等网络路由决策 :在对等网络路由表中选择比自己的节点标识更接近目的节点标识的节点作为对等网络路由转发的下一跳，如果没有找到这样的节点，则自己就是目的节点。

[0005] 对等网络具有良好的自组织与自管理特性，对等节点可以自由的加入和退出对等网络，这使得对等网络具有良好的可扩展性。通常对等网络中会引入集中式的注册服务器 (Enrollment Server)，用来控制节点（包括对等节点与客户节点）的加入，并负责为申请加入的节点分配 ID 以及指定安全的引导节点 (Bootstrap Peer) 等。对等节点加入对等网络时，会按照选定的 DHT 算法找到自己在 ID 空间的位置，然后负责存储资源标识落在自己责任空间的资源，加入的节点还需要学习其它节点负责的 ID 空间信息。相应地，其它节点也需要学习加入的节点的信息，并将由加入的节点负责存储的资源转移给加入的节点存储。

[0006] 对等节点加入对等网络的过程与客户节点加入对等网络的过程是有区别的。当对等节点申请加入对等网络时，请求节点 (Joining Peer) 首先与注册服务器通讯，被许可加入后，获得分配的节点标识Peer-D以及指定的安全的引导节点列表，然后发送Join请求消息给选定的引导节点；该引导节点使用P2P路由模式在对等网络上转发该请求消息，直到负责该节点标识的许可节点(Admitting Peer)收到该请求消息后返回应答消息，从而建立了请求节点与许可节点的连接，该许可节点是在对等网络的ID空间中ID最靠近请求节点的节点。当客户节点申请加入对等网络时，客户节点首先与注册服务器通讯，完成认证和授权处理，获得候选的联系节点 (Associated Peers) 的联系地址以及可能的客户节点标识Client-ID；然后向候选的每个联系节点发送Inquire查询请求消息；客户节点根据候选的联系节点返回的查询应答消息中的联系节点能提供的对等网络服务的信息，如DHT算法以及节点状态信息等，向选定的联系节点发送对等网络服务连接请求消息；该联系节点返回应答消息许可客户节点加入对等网络，从而完成建立连接。

[0007] 当节点离开对等网络时，其它的节点需要了解离开的节点的信息，然后更新路由表以防止路由黑洞（即不可到达或访问的ID空间）持续存在，但是在对等网络节点的路由收敛之前不可避免存在路由黑洞，这个过程即为路由抖动。当有恶意节点频繁地加入和退出对等网络时，甚至是在退出对等网络时不将自己负责存储的资源转移到其它节点上，这样的攻击将导致对等网络的路由空间出现不可到达的黑洞，同时还会导致大量存储在对等网络上的资源不可用甚至丢失；另外，恶意节点频繁的加入和退出也会增加对等节点的处理负担，从而导致因为节点太忙而DoS(Denial of Service，拒绝服务)。由此可见，对等网络中节点的自由加入和退出将直接影响对等网络的路由以及资源的可用性。

[0008] 现有技术中对于恶意节点频繁加入对等网络的行为，通常有两种处理方法，一种是在收到节点加入对等网络的请求时，抛出一个难题 (Puzzle) 给该节点解答，只有当该节点给出正确的答案时才允许该节点加入对等网络，从而限制节点加入对等网络的频率。另一种是在资源发布到对等网络上进行分布式存储时，通过复制和重发布的机制备份这些资源，这样即使恶意节点频繁加入和退出对等网络，也不会影响这些资源的可用性。

[0009] 在对现有技术进行分析后，发明人发现：

[0010] 第一种方法的效果严重依赖于具体采用的Puzzle机制，需要存储大量的难题，实现开销比较大，且当恶意节点能给出答案时，仍不能防止恶意节点频繁加入和退出对等网络。比如难题是要求提供图片表示的数字，则由于恶意节点采用对应的图片识别技术而导致该方法失效。第二种方法不能解决由于恶意节点频繁加入对等网络带来的路由抖动、信令开销以及可能的拒绝服务，而且如果恶意节点多次加入对等网络时，带走的是已发布的资源及其备份，则这些资源仍然不可用甚至丢失。

发明内容

[0011] 为了限制节点频繁地加入对等网络，本发明实施例提供了一种控制节点加入对等网络的方法和装置。所述技术方案如下：

[0012] 一种控制节点加入对等网络的方法，所述方法包括：

[0013] 接收节点加入对等网络的请求消息；

[0014] 判断是否在规定时间内接收到所述节点加入对等网络的请求消息的数目高于预

设的第一阈值，并且所述节点在对等网络上多次停留的平均时间低于预设的第二阈值，并且在规定时间内接收到的所有加入对等网络的请求消息的数目高于预设的第三阈值；

[0015] 如果是，则拒绝所述节点加入所述对等网络。

[0016] 一种控制节点加入对等网络的装置，所述装置包括：

[0017] 接收模块，用于接收节点加入对等网络的请求消息；

[0018] 处理模块，用于在所述接收模块接收到所述请求消息后，判断是否在规定时间内接收到所述节点加入对等网络的请求消息的数目高于预设的第一阈值，并且所述节点在对等网络上多次停留的平均时间低于预设的第二阈值，并且在规定时间内接收到的所有加入对等网络的请求消息的数目高于预设的第三阈值，如果是，则拒绝所述节点加入所述对等网络。

[0019] 本发明实施例通过根据节点加入对等网络的历史信息和已接收的请求消息的历史信息中的至少一种对该节点的合法性进行判断，并在确定出不允许该节点加入对等网络时，拒绝该节点加入对等网络，实现了对节点加入对等网络进行控制，限制了节点频繁地加入对等网络，从而在一定程度上解决了由于恶意节点频繁加入而导致的对等网络路由抖动、资源不可用甚至失去以及节点拒绝服务等等。与现有的 Puzzle 机制相比，不需要存储大量的难题，极大地节省了开销，且具有更好的控制效果。

附图说明

[0020] 图 1 是本发明实施例提供的一种控制节点加入对等网络的方法流程图；

[0021] 图 2 是本发明实施例提供的另一种控制节点加入对等网络的方法流程图；

[0022] 图 3 是本发明实施例提供的对等网络结构示意图；

[0023] 图 4 是本发明实施例提供的对等节点加入对等网络流程示意图；

[0024] 图 5 是本发明实施例提供的客户节点加入对等网络流程示意图；

[0025] 图 6 是本发明实施例提供的控制节点加入对等网络的装置结构示意图。

具体实施方式

[0026] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0027] 本发明实施例提供的控制节点加入对等网络的方法，通过在接收到节点加入对等网络的请求消息后，根据该节点加入对等网络的历史信息和已接收的加入对等网络的请求消息的历史信息中的至少一种，确定出不允许该节点加入对等网络时，拒绝该节点加入该对等网络。

[0028] 参见图 1，为本发明实施例提供的一种控制节点加入对等网络的方法流程图，该方法具体包括：

[0029] 101 ：接收某个节点加入对等网络的请求消息。

[0030] 102 ：根据该节点加入对等网络的历史信息，判断是否允许该节点加入对等网络，如果是，则执行 103 ；否则，执行 104。

[0031] 根据该节点加入对等网络的历史信息判断是否允许该节点加入对等网络，可以采用多种方式，包括但不限于以下两种中的至少一种：

[0032] 1) 判断在规定时间内接收到该节点加入对等网络的请求消息的数目是否高于预设的第一阈值，如果是，则拒绝该节点加入对等网络；否则，允许该节点加入对等网络。

[0033] 2) 判断该节点在对等网络上多次停留的平均时间是否低于预设的第二阈值，如果是，则拒绝该节点加入对等网络；否则，允许该节点加入对等网络。

[0034] 其中，规定时间、第一阈值和第二阈值可以根据需要进行设置，如规定时间为 1 个小时，设置第一阈值为 10，第二阈值为 5 分钟等等。当同时采用上述两种方式进行判断时，二者不分先后顺序。

[0035] 另外，上述节点加入对等网络的历史信息中提及的对等网络可以是指定的对等网络，如上述节点请求加入的对等网络，也可以是所有的对等网络。

[0036] 103：允许该节点加入对等网络，相应地，回复应答消息给该节点，并将给该节点分配的节点标识以及引导节点 (Bootstrap Peer) 列表等信息发送给该节点，然后结束。

[0037] 104：拒绝该节点加入对等网络，进一步地，还可以丢弃该请求消息，并记入日志或产生告警信息，然后结束。

[0038] 进一步地，拒绝该节点加入对等网络之后，还可以通知该节点在规定时间后重新申请加入对等网络。例如，在本地设备比较繁忙的情况下，拒绝该节点本次的申请，并设置延迟时间 30 分钟，通知该节点可以在 30 分钟后重新进行下一次申请。

[0039] 另外，还可以将该节点本次申请加入对等网络的相关信息如控制的结果（拒绝或允许加入）记录到已保存该节点加入对等网络的历史信息中，以方便后续收到加入对等网络的请求消息时，结合本次控制的结果进行判断。

[0040] 图 1 所示的方法，通过根据节点加入对等网络的历史信息对该节点的合法性进行判断，并在判断出不允许该节点加入对等网络时，拒绝该节点加入对等网络，实现了对节点加入对等网络进行控制，限制了节点频繁地加入对等网络，从而在一定程度上解决了由于恶意节点频繁加入而导致的对等网络路由抖动、资源不可用甚至失去以及节点拒绝服务等问题。与现有的 Puzzle 机制相比，不需要存储大量的难题，极大地节省了开销，且具有更好的控制效果。在判断是否允许节点加入对等网络时，既可以根据接收请求消息的频率进行判断，也可以根据节点停留的时间进行判断，或者结合起来进行判断，简单方便，容易实现，应用更灵活。

[0041] 参见图 2，为本发明实施例提供的另一种控制节点加入对等网络的方法流程图，该方法具体包括：

[0042] 201：接收某个节点加入对等网络的请求消息。

[0043] 202：根据已接收的加入对等网络的请求消息的历史信息，判断是否允许该节点加入对等网络，如果是，则执行 203；否则，执行 204。

[0044] 根据已接收的加入对等网络的请求消息的历史信息判断是否允许节点加入对等网络，可以采用多种方式，包括但不限于以下方式：

[0045] 判断在规定时间内接收到的所有加入对等网络的请求消息的数目（即所有节点加入对等网络的平均频率）是否高于预设的第三阈值，如果是，则拒绝该节点加入对等网络；否则，允许该节点加入对等网络。

[0046] 其中，规定时间和第三阈值可以根据需要进行设置，如规定时间为 1 个小时，设置第三阈值为 50 等等。

[0047] 另外，上述节点加入对等网络的历史信息中提及的对等网络可以是指定的对等网络，如上述节点请求加入的对等网络，也可以是所有的对等网络。

[0048] 203：允许该节点加入对等网络，然后结束。

[0049] 204：拒绝该节点加入对等网络，进一步地，还可以丢弃该请求消息，并记入日志或产生告警信息，然后结束。

[0050] 进一步地，拒绝该节点加入对等网络之后，还可以通知该节点在规定时间后重新申请加入对等网络。

[0051] 另外，还可以将该节点本次申请加入对等网络的相关信息如控制的结果（拒绝或允许加入）记录到已保存的加入对等网络的请求消息的历史信息中，以方便后续收到加入对等网络的请求消息时，结合本次控制的结果进行判断。

[0052] 图 2 所示的方法，通过根据本地已接收的加入对等网络的请求消息的历史信息对该节点的合法性进行判断，并在判断出不允许该节点加入对等网络时，拒绝该节点加入对等网络，实现了对节点加入对等网络进行控制，限制了节点频繁地加入对等网络，从而在一定程度上解决了由于恶意节点频繁加入而导致的对等网络路由抖动、资源不可用甚至失去以及节点拒绝服务等等。与现有的 Puzzle 机制相比，不需要存储大量的难题，极大地节省了开销，且具有更好的控制效果。判断是否允许节点加入对等网络的过程，简单方便，容易实现，应用更灵活。

[0053] 为了达到更好的控制效果，进一步地，本发明实施例中还可以将图 1 所示的技术方案与图 2 所示的技术方案结合起来应用，即根据请求节点加入对等网络的历史信息和本地已接收的加入对等网络的请求消息的历史信息，判断是否允许该请求节点加入对等网络，此时，两种判断不分先后，可以先根据该请求节点加入对等网络的历史信息进行判断，也可以先根据本地已接收的加入对等网络的请求消息的历史信息进行判断，具体的判断过程以及后续的处理均与上述实施例中的相关描述相同，此处不再赘述。通过以上两种判断，可以达到更好的控制效果，避免节点过于频繁地加入对等网络，并能较好地缓解由于恶意节点频繁加入而导致的对等网络路由抖动、资源不可用甚至失去以及节点拒绝服务等问题。

[0054] 上述所有实施例提供的技术方案中对请求加入对等网络的节点进行判断以及相应处理的功能可以集成在对等网络中的注册服务器上，也可以集成在对等网络中的对等节点上，如引导节点、为客户节点提供对等网络服务的对等节点等等。当集成在对等节点上时，该对等节点可以从注册服务器获取申请加入的节点的历史信息，如果在网络部署中该对等节点相对于申请加入的节点是固定的（如网关），则该对等节点可以自己收集申请加入的节点的历史信息；甚至所有的对等节点可以将申请加入的节点的历史信息作为一种资源记录，并使用对等网络的分布式存储服务存储到对等网络上，以方便需要时从对等网络上获取。

[0055] 例如，参见图 3，对等网络中有 7 个对等节点，节点 1 至节点 7，注册服务器分别与节点 1 和节点 2 相连。当节点 1 请求加入对等网络时，可以由集成了上述功能的注册服务器进行判断和处理，也可以由集成了上述功能的其它节点如节点 2 进行判断和处理。

[0056] 在P2PSIP(Peer-to-Peer Session Initiation Protocol，对等会话初始化协议)网络参考模型中，对等节点可以耦合 SIP 功能，如 SIP Proxy Server（代理服务器）功能、

SIP Redirect Server(重定向服务器)功能、SIP UA(UserAgent,用户代理)功能和信令网关功能等等,客户节点通常耦合SIP UA功能。对等节点之间通过P2PSIP PeerProtocol(对等会话初始化对等协议)通讯,客户节点与没有耦合SIP功能的对等节点与之间使用P2PSIP ClientProtocol(对等会话初始化客户协议)通讯,SIP UA实体与耦合了SIP Proxy Server功能或者SIP Redirect Server功能的对等节点之间采用SIP通讯。

[0057] 下面以P2PSIP网络参考模型为例,分别说明对等节点与客户节点加入对等网络的过程。参见图4,为对等节点加入对等网络的流程示意图,以图3中的节点1请求加入对等网络为例进行说明,该过程具体如下:

[0058] 1. 节点1向注册服务器发送请求加入对等网络的Join请求消息;

[0059] 2. 注册服务器按照上述方法判断是否允许节点1加入对等网络,如果否,则拒绝节点1加入对等网络,丢弃该请求消息;

[0060] 3. 如果允许节点1加入对等网络,则注册服务器返回给该节点分配的Peer-D、引导节点列表等信息;

[0061] 4. 节点1向引导节点2(Bootstrap Peer)发送Join请求消息;

[0062] 5. 节点2将该请求消息转发给允许节点3(Admittion Peer);

[0063] 6. 节点3回复Response应答消息给节点2;

[0064] 7. 节点2将该应答消息转发给节点1,从而完成节点1与节点3建立连接,结束节点1加入对等网络的过程。

[0065] 参见图5,为客户节点加入对等网络的流程示意图,以图3中的客户节点1请求加入对等网络为例进行说明,该过程具体如下:

[0066] 1. 客户节点1向注册服务器发送请求加入对等网络的Join请求消息;

[0067] 2. 注册服务器按照上述方法判断是否允许客户节点1加入对等网络,如果否,则拒绝客户节点1加入对等网络,丢弃该请求消息;

[0068] 3. 如果允许客户节点1加入对等网络,则注册服务器返回给该节点分配的Client-ID、候选的联系节点(Associated Peers)列表等信息,其中包括节点1和节点2;

[0069] 4. 客户节点1向节点1发送Inquire查询请求消息;

[0070] 5. 客户节点1向节点2发送Inquire查询请求消息;

[0071] 6. 节点1回复Response应答消息给客户节点1,其中携带节点1能提供的对等网络服务的信息(如DHT算法)以及节点1的状态信息等等;

[0072] 7. 节点2回复Response应答消息给客户节点1,其中携带节点2能提供的对等网络服务的信息(如DHT算法)以及节点2的状态信息等等;

[0073] 8. 客户节点1根据收到的信息选择节点1为联系节点,并向其发送Join请求消息;

[0074] 9. 节点1回复Response应答消息,如果客户节点1发来的Join请求消息中未携带认证需要的身份信息,则在应答消息中设置标识404,要求客户节点1提供身份信息;

[0075] 10. 客户节点1发送携带身份信息的Join请求消息给节点1;

[0076] 11. 节点1回复Response应答消息,从而完成客户节点1与节点1建立连接,结束客户节点1加入对等网络的过程。

[0077] 如果步骤8中客户节点1提供了身份信息,则步骤9即完成建立连接,不需要执行

步骤 10 和 11。

[0078] 利用上述方法控制客户节点加入对等网络，可以限制恶意客户节点频繁的加入对等网络，从而缓解了由于恶意客户节点频繁加入对等网络而导致直接相连的对等节点性能降低甚至拒绝服务。

[0079] 参见图 6，本发明实施例还提供了一种控制节点加入对等网络的装置，具体包括：

[0080] 接收模块，用于接收节点加入对等网络的请求消息；

[0081] 处理模块，用于在接收模块接收到上述请求消息后，根据该节点加入对等网络的历史信息和已接收的加入对等网络的请求消息的历史信息中的至少一种，确定出不允许该节点加入对等网络时，拒绝该节点加入对等网络。

[0082] 其中，处理模块具体包括：

[0083] 第一处理单元，用于在接收模块接收到上述请求消息后，判断在规定时间内接收到该节点加入对等网络的请求消息的数目是否高于预设的第一阈值，如果是，则拒绝该节点加入对等网络。

[0084] 或者，处理模块具体包括：

[0085] 第二处理单元，用于在接收模块接收到上述请求消息后，判断该节点在对等网络上多次停留的平均时间是否低于预设的第二阈值，如果是，则拒绝该节点加入对等网络。

[0086] 或者，处理模块具体包括：

[0087] 第三处理单元，用于在接收模块接收到上述请求消息后，判断在规定时间内接收到的所有加入对等网络的请求消息的数目是否高于预设的第三阈值，如果是，则拒绝该节点加入对等网络。

[0088] 进一步地，上述装置还包括：

[0089] 记录模块，用于记录该节点本次申请加入对等网络的相关信息。

[0090] 进一步地，上述装置还可以包括：

[0091] 通知模块，用于通知该节点在规定时间后重新申请加入对等网络。

[0092] 图 6 所示的装置通过对申请加入的节点的合法性进行判断，并在判断出不允许该节点加入对等网络时，拒绝该节点加入对等网络，实现了对节点加入对等网络进行控制，限制了节点频繁地加入对等网络，从而在一定程度上解决了由于恶意节点频繁加入而导致的对等网络路由抖动、资源不可用甚至失去以及节点拒绝服务等等。与现有的 Puzzle 机制相比，不需要存储大量的难题，极大地节省了开销，且具有更好的控制效果。在判断是否允许节点加入对等网络时，可以根据接收请求消息的频率进行判断，或根据该节点停留的时间进行判断，或根据收到的所有请求消息的数目进行判断，或者结合起来进行判断，简单方便，容易实现，应用更灵活。

[0093] 本发明实施例可以利用软件实现，相应的软件程序可以存储在可读取的存储介质中，例如，计算机的硬盘、缓存或光盘中。

[0094] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

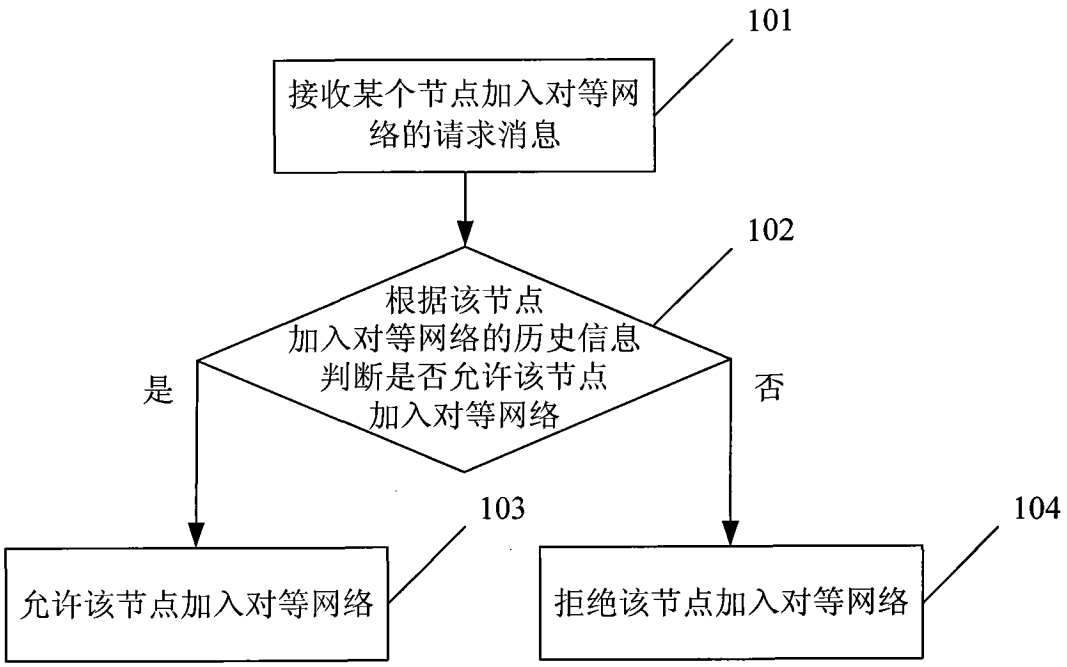

101
接收某个节点加入对等网络的请求消息
102
根据该节点加入对等网络的历史信息判断是否允许该节点加入对等网络
是
否
103
允许该节点加入对等网络
104
拒绝该节点加入对等网络

图 1

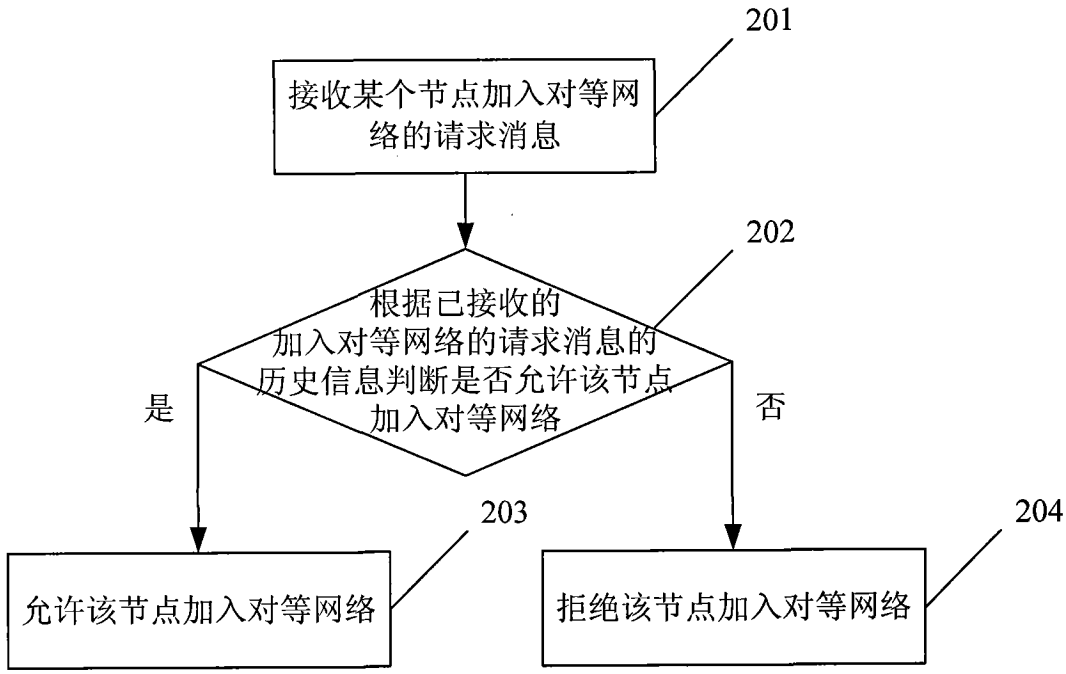

201
接收某个节点加入对等网络的请求消息
202
根据已接收的加入对等网络的请求消息的历史信息判断是否允许该节点加入对等网络
是
否
203
允许该节点加入对等网络
204
拒绝该节点加入对等网络

图 2

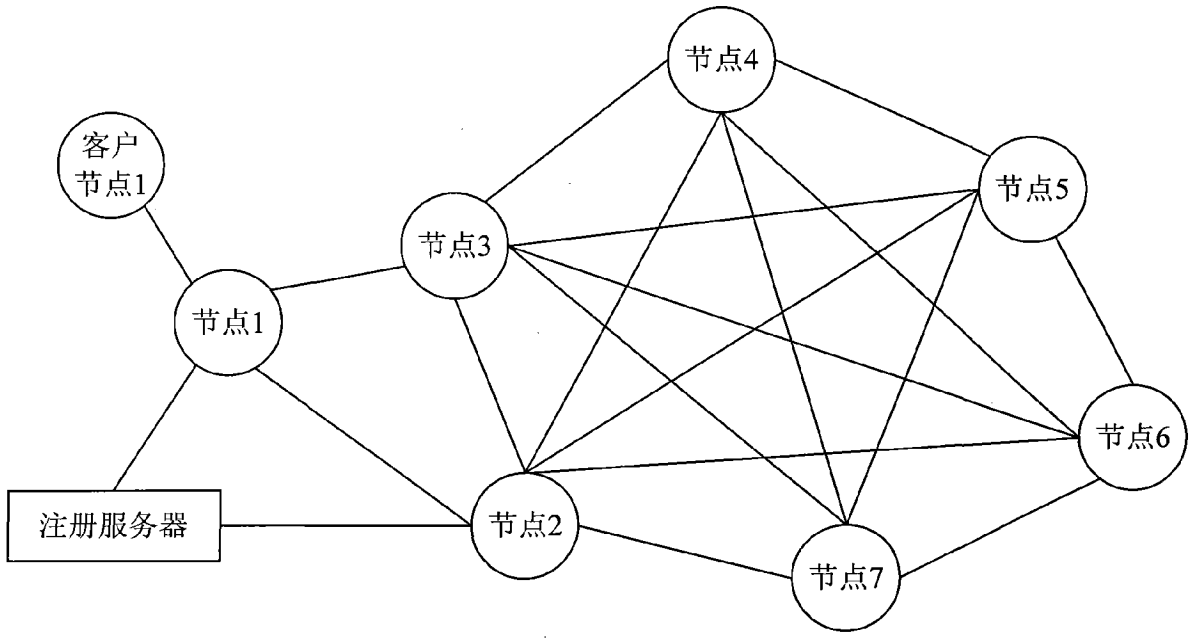

节点4
客户
节点1
节点5
节点3
节点1
节点6
注册服务器
节点2
节点7

图 3

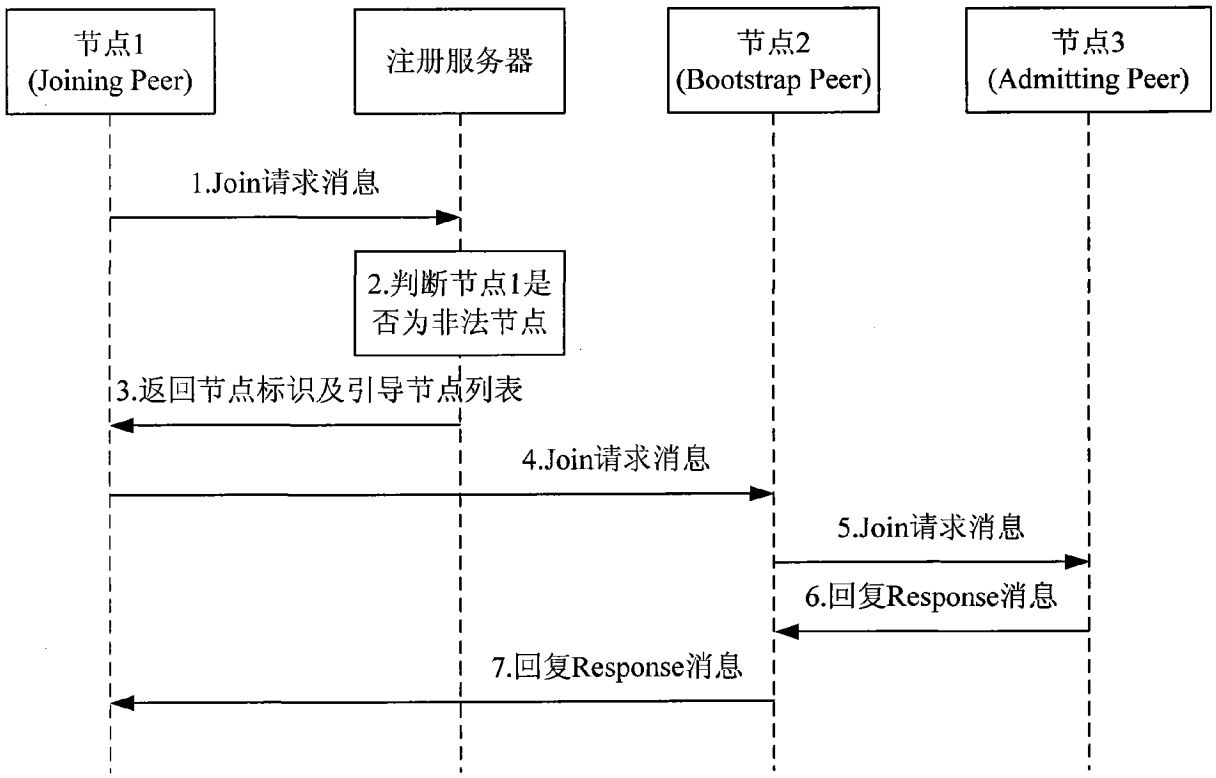

节点1
(Joining Peer)
注册服务器
节点2
(Bootstrap Peer)
节点3
(Admitting Peer)
1.Join请求消息
2.判断节点1是
否为非法节点
3.返回节点标识及引导节点列表
4.Join请求消息
5.Join请求消息
6.回复Response消息
7.回复Response消息

图 4

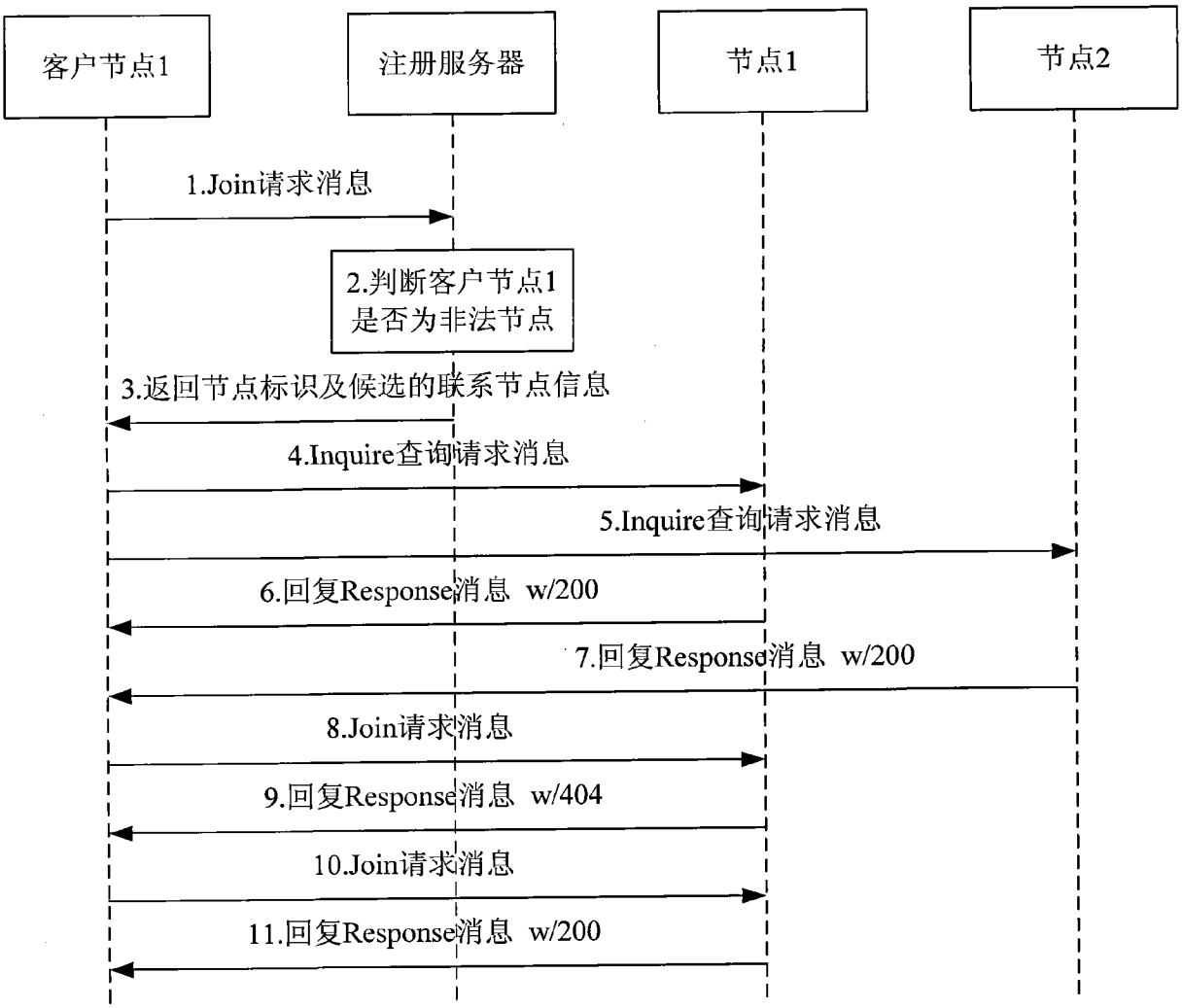

客户节点1
注册服务器
节点1
节点2
1.Join请求消息
2.判断客户节点1是否为非法节点
3.返回节点标识及候选的联系节点信息
4.Inquire查询请求消息
5.Inquire查询请求消息
6.回复Response消息 w/200
7.回复Response消息 w/200
8.Join请求消息
9.回复Response消息 w/404
10.Join请求消息
11.回复Response消息 w/200

图 5

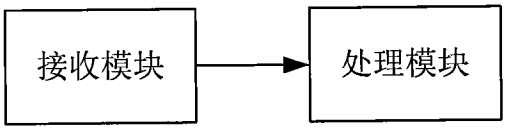

接收模块
处理模块

图 6