

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 6 月 29 日 (29.06.2017)



(10) 国际公布号
WO 2017/107462 A1

- (51) 国际专利分类号:
H04L 29/08 (2006.01)
- (21) 国际申请号: PCT/CN2016/089464
- (22) 国际申请日: 2016 年 7 月 8 日 (08.07.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510969745.3 2015 年 12 月 21 日 (21.12.2015) CN
- (71) 申请人: 乐视控股(北京)有限公司 (LE HOLDINGS (BEIJING) CO., LTD.) [CN/CN]; 中国北京市朝阳区姚家园路 105 号 3 号楼 10 层 1102, Beijing 100025 (CN)。乐视云计算有限公司 (LECLOUD COMPUTING CO., LTD.) [CN/CN]; 中国北京市朝阳区姚家园路 105 号观湖国际大厦 1 号楼 15 层, Beijing 100025 (CN)。
- (72) 发明人: 李卓 (LI, Zhuo); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 1 号楼 15 层, Beijing 100025 (CN)。
- (74) 代理人: 北京鼎佳达知识产权代理事务所(普通合伙) (BEIJING DINGJIADA IP FIRM); 中国北京

市朝阳区北苑路 172 号欧陆大厦 A2002 刘铁生, Beijing 100101 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:

— 关于申请人有权要求在先申请的优先权(细则 4.17(iii))

[见续页]

(54) Title: P2P NETWORK-BASED DATA PROCESSING METHOD, APPARATUS AND SYSTEM

(54) 发明名称: 基于 P2P 网络的数据处理方法、装置及系统

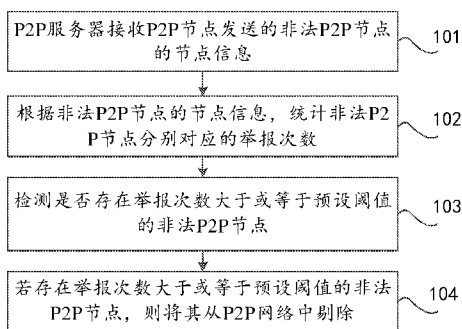


图 1

- 101 A P2P server receives node information of illegal P2P nodes sent by a P2P node
- 102 Count the numbers of reporting times respectively corresponding to the illegal P2P nodes according to the node information of the illegal P2P nodes
- 103 Detect whether there is an illegal P2P node having the number of reporting times greater than or equal to a present threshold
- 104 If there is an illegal P2P node having the number of reporting times greater than or equal to the present threshold, remove the illegal P2P node from the P2P network

(57) Abstract: Provided are a P2P network-based data processing method, apparatus and system. The present invention relates to the technical field of information, and can achieve the purpose of purifying P2P network environments and improve the sharing efficiency of a P2P network. The method comprises: first, a P2P server receives node information of an illegal P2P node sent by a P2P node, wherein the node information of an illegal P2P node is sent by the P2P node when the P2P node detects that there is an illegal P2P node, and the illegal P2P node is a P2P node of which the number of pieces of false data sent thereby is greater than or equal to a preset amount threshold; and then, counting the numbers of reporting times respectively corresponding to the illegal P2P nodes according to the node information of the illegal P2P nodes; finally, detecting whether there is an illegal P2P node having the number of reporting times greater than or equal to a present threshold; and if yes, removing the illegal P2P node having the number of reporting times greater than or equal to the present threshold from the P2P network.

(57) 摘要: 本发明提供了一种基于 P2P 网络的数据处理方法、装置及系统, 涉及信息技术领域, 可以实现净化 P2P 网络环境的目的, 可以提高 P2P 网络的分享效率。所述方法包括: 首先 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息, 所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的, 所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点; 然后根据所述非法 P2P 节点的节点信息, 统计非法 P2P 节点分别对应的举报次数; 最后检测是否存在举报次数大于或等于预设阈值的非法 P2P 节点; 若

存在, 则将所述举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除。



WO 2017/107462 A1



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

基于 P2P 网络的数据处理方法、装置及系统

本申请基于申请号为 2015109697453、申请日为 2015 年 12 月 21 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本发明实施例涉及信息技术领域，尤其涉及一种基于 P2P 网络的数据处理方法、装置及系统。

背景技术

近些年来，随着信息技术的不断发展，P2P 技术得到了广泛的应用，P2P 是英文 Peer-to-Peer（对等）的简称，又被称为“点对点”。“对等”技术是一种新兴的网络技术，主要依赖于网络中参与者的计算能力和带宽，而并非把所有依赖都聚集在成本较为昂贵的服务器上去。P2P 亦是 point-to-point（点对点）的简称。也就是说它自己的下载的同时，也要上载给网络上的其他节点。参与 P2P 网路的用户越多，相应的上载者就越多，上载者数量越多，P2P 终端到服务器上取数据的机会也就越小，所以 P2P 的存在不但使服务器压力大大减少，更达到了人数越多速度就越快的效果。

目前，在 P2P 网络中节点与节点之间进行数据交互时，有时其中的一个 P2P 节点在获取得到另外一个 P2P 节点的节点信息之后，会与其进行恶意链接，并向其发送虚假数据；或者由于网络延迟等原因，会导致数据交互的不完整，进而会造成一方节点误认为另一方节点发送的是虚假数据。无论以上哪种方式都会占用 P2P 节点连接资源，进而会影响 P2P 网络的分享效率。

发明内容

本发明实施例提供了一种基于 P2P 网络的数据处理方法、装置及系统，用以解决目前由于存在恶意发送虚假数据的 P2P 节点、网络延迟等原因会导致影响 P2P 网络的分享效率的问题。

针对现有技术存在的问题，本发明实施例提供了一种基于 P2P 网络的数据处理方法，包括：

P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法

P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点；

根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数；

5 检测是否存在举报次数大于或等于预设阈值的非法 P2P 节点；

若存在，则将所述举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除。

进一步地，所述若存在，则将所述举报次数大于或等于预设阈值的非法节点从 P2P 网络中剔除之后，所述方法还包括：

10 输出提示信息，所述提示信息用于提示所述举报次数大于或等于预设阈值的非法节点已从 P2P 网络中剔除。

本发明实施例提供了另一种基于 P2P 网络的数据处理方法，包括：

当确定接收到 P2P 节点发送的数据为虚假数据时，检测接收到所述 P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈值；

15 若所述虚假数据的个数大于或等于所述预置个数阈值，则确定所述 P2P 节点为非法 P2P 节点；

与所述非法 P2P 节点断开连接并记录所述非法 P2P 节点的节点信息，以便当再次接收到所述非法 P2P 节点发送的连接请求时，不与所述非法 P2P 节点进行连接；

20 向 P2P 服务器发送所述非法 P2P 节点的节点信息，所述 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，以使得所述 P2P 服务器根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数并进行检测，当检测出存在举报次数大于或等于预设阈值的非法 P2P 节点时将其从 P2P 网络中剔除。

25 进一步地，所述当检测出接收到 P2P 节点发送的数据为虚假数据时，检测接收到所述 P2P 节点发送的虚假数据的个数是否大于或等于预置个数阈值之前，所述方法还包括：

通过预置 CRC32 校验算法，将所述 P2P 节点发送的数据进行验证，得到对应的 CRC32 值；

30 检测所述 CRC32 值是否与预置 M3U8 文件中的预置 CRC32 值匹配；若不匹配，则将所述 P2P 节点发送的数据确定为虚假数据。

进一步地，所述若所述虚假数据的个数大于或等于所述预置个数阈值，则确定所述 P2P 节点为非法 P2P 节点之后，所述方法还包括：

输出提示信息，所述提示信息用于提示所述 P2P 节点为非法 P2P 节点。

35 本发明实施例提供了一种 P2P 服务器，包括：

接收单元，用于接收 P2P 节点发送的非法 P2P 节点的节点信息，所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点；

5 统计单元，用于根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数；

检测单元，用于检测是否存在举报次数大于或等于预设阈值的非法 P2P 节点；

10 剔除单元，用于若所述检测单元检测出存在举报次数大于或等于预设阈值的非法 P2P 节点，则将所述举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除。

优选地，所述 P2P 服务器还包括：

输出单元，用于输出提示信息，所述提示信息用于提示所述举报次数大于或等于预设阈值的非法节点已从 P2P 网络中剔除。

15 本发明实施例提供了一种 P2P 节点，其特征在于，包括：

检测单元，用于当确定接收到 P2P 节点发送的数据为虚假数据时，检测接收到所述 P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈值；

20 确定单元，用于若所述检测单元检测出虚假数据的个数大于或等于所述预置个数阈值，则确定所述 P2P 节点为非法 P2P 节点；

断开单元，用于与所述非法 P2P 节点断开连接；

记录单元，用于记录所述非法 P2P 节点的节点信息，以便当再次接收到所述非法 P2P 节点发送的连接请求时，不与所述非法 P2P 节点进行连接；

25 发送单元，用于向 P2P 服务器发送所述非法 P2P 节点的节点信息，所述 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，以使得所述 P2P 服务器根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数并进行检测，当检测出存在举报次数大于或等于预设阈值的非法 P2P 节点时将其从 P2P 网络中剔除。

优选地，所述 P2P 节点还包括：验证单元；

30 所述验证单元，用于通过预置 CRC32 校验算法，将所述 P2P 节点发送的数据进行验证，得到对应的 CRC32 值；

所述检测单元，还用于检测所述 CRC32 值是否与预置 M3U8 文件中的预置 CRC32 值匹配；

35 所述确定单元，还用于若所述检测单元检测出所述 CRC32 值与所述预置 M3U8 文件中的预置 CRC32 值不匹配，则将所述 P2P 节点发送的数据确

定为虚假数据。

优选地，所述 P2P 节点还包括：

输出单元，用于输出提示信息，所述提示信息用于提示所述 P2P 节点为非法 P2P 节点。

5 本发明实施例提供了一种基于 P2P 网络的数据处理系统，包括：P2P 服务器和 P2P 节点；

所述 P2P 节点，用于当确定接收到 P2P 节点发送的数据为虚假数据时，检测接收到所述 P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈值；若所述虚假数据的个数大于或等于所述预置个数阈值，则确定所述
10 P2P 节点为非法 P2P 节点；与所述非法 P2P 节点断开连接并记录所述非法 P2P 节点的节点信息，以便当再次接收到所述非法 P2P 节点发送的连接请求时，不与所述非法 P2P 节点进行连接；向所述 P2P 服务器发送所述非法 P2P 节点的节点信息；

所述 P2P 服务器，用于接收不同 P2P 节点发送的不同非法 P2P 节点的节点信息；根据所述不同非法 P2P 节点的节点信息，统计不同非法 P2P 节点分别对应的举报次数；检测是否存在举报次数大于或等于预设阈值的非法 P2P
15 节点；若存在，则将所述举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除。

本发明实施例提供了一种基于 P2P 网络的数据处理装置，所述装置包
20 括：

处理器，和

存储器，被配置为存储所述处理器的可执行指令；

所述的处理器被配置为：

P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，所述非法
25 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点；

根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数；

30 检测是否存在举报次数大于或等于预设阈值的非法 P2P 节点；

若存在，则将所述举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除。

本发明实施例提供了一种基于 P2P 网络的数据处理装置，所述装置包
括：

35 处理器，和

存储器，被配置为存储所述处理器的可执行指令；
所述的处理器被配置为：

当确定接收到 P2P 节点发送的数据为虚假数据时，检测接收到所述 P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈值；

5 若所述虚假数据的个数大于或等于所述预置个数阈值，则确定所述 P2P 节点为非法 P2P 节点；

与所述非法 P2P 节点断开连接并记录所述非法 P2P 节点的节点信息，以便当再次接收到所述非法 P2P 节点发送的连接请求时，不与所述非法 P2P 节点进行连接；

10 向 P2P 服务器发送所述非法 P2P 节点的节点信息，其中，所述 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，以使得所述 P2P 服务器根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数并进行检测，当检测出存在举报次数大于或等于预设阈值的非法 P2P 节点时将其从 P2P 网络中剔除。

15 本发明实施例提供一种基于 P2P 网络的数据处理方法、装置及系统，首先 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，其中所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点，然后通过 P2P 服务器统计非法 P2P 节点分
20 别对应的举报次数，将举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除，可以实现将一些恶意发送虚假数据的 P2P 节点以及一些上传速度不好的 P2P 节点从 P2P 网络中剔除，进而可以实现净化 P2P 网络环境的目的，从而可以提高 P2P 网络的分享效率。

25 附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附
30 图。

图 1 为本发明实施例提供的一种基于 P2P 网络的数据处理方法流程示意图；

图 2 为本发明实施例提供的另一种基于 P2P 网络的数据处理方法流程示意图；

35 图 3 为本发明实施例提供的又一种基于 P2P 网络的数据处理方法流程

示意图；

图 4 为本发明实施例提供的一种 P2P 服务器结构示意图；

图 5 为本发明实施例提供的另一种 P2P 服务器结构示意图；

图 6 为本发明实施例提供的一种 P2P 节点结构示意图；

5 图 7 为本发明实施例提供的另一种 P2P 节点结构示意图；

图 8 为本发明实施例提供的一种基于 P2P 网络的数据处理系统结构示意图；

图 9 为本发明实施例提供的一种 P2P 服务器的实体结构示意图。

10 具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

本发明实施例提供了一种基于 P2P 网络的数据处理方法，可以应用于 P2P 服务器，如图 1 所示，所述方法包括：

101、P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息。

其中，所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述节点信息中可以包含节点名称、ID（Identity，身份标识号码）号等。所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点。所述预置个数阈值可以根据实际需求进行配置。

102、根据非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数。

例如，当 P2P 服务器接收到一个 P2P 节点发送的一个非法 P2P 节点的节点信息时，根据该非法 P2P 节点的节点信息，可以确定该非法 P2P 节点为当前 P2P 网络中的 4 号 P2P 节点，将 4 号 P2P 节点对应的举报次数累计加 1，利用相同的方式最终可以统计得到当前 P2P 网络中不同非法 P2P 节点分别对应的举报次数。

103、检测是否存在举报次数大于或等于预设阈值的非法 P2P 节点。

其中，所述预设阈值可以根据实际需求进行配置，也可以由系统默认进行配置，本发明实施例不做限定。

104、若存在举报次数大于或等于预设阈值的非法 P2P 节点，则将其从 P2P 网络中剔除。

对于本发明实施例，通过将举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除，可以实现将一些恶意发送虚假数据的 P2P 节点以及一些上传速度不好的 P2P 节点从 P2P 网络中剔除，进而可以实现净化 P2P 网络环境的目的。

5 进一步地，在执行步骤 104 之后，所述方法还可以包括：输出提示信息，所述提示信息用于提示所述举报次数大于或等于预设阈值的非法节点已从 P2P 网络中剔除。所述提示信息可以为文本提示信息、图片提示信息、音频提示信息、视频提示信息等。需要说明的是，在执行步骤 104 之后，通过
10 输出提示信息，可以使 P2P 网络维护人员明确一些举报次数大于或等于预设阈值的非法节点已从 P2P 网络中剔除，可以增强用户的体验。

本发明实施例提供的一种基于 P2P 网络的数据处理方法，首先 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，其中所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P
15 节点，然后通过 P2P 服务器统计非法 P2P 节点分别对应的举报次数，将举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除，可以实现将一些恶意发送虚假数据的 P2P 节点以及一些上传速度不好的 P2P 节点从 P2P 网络中剔除，进而可以实现净化 P2P 网络环境的目的，从而可以提高 P2P 网络的分享效率。

20 本发明实施例提供了另一种基于 P2P 网络的数据处理方法，可以应用于 P2P 节点，如图 2 所示，所述方法包括：

201、当确定接收到 P2P 节点发送的数据为虚假数据时，检测接收到该 P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈值。

其中，所述虚假数据可以为与需要获取的数据不匹配的数据，也可以为
25 数据不完整、存在数据丢失的数据。所述预置个数阈值可以根据实际需求进行配置，用于校验 P2P 节点是否为非法 P2P 节点。

202、若虚假数据的个数大于或等于预置个数阈值，则确定 P2P 节点为非法 P2P 节点。

203、与非法 P2P 节点断开连接并记录非法 P2P 节点的节点信息。

30 进一步地，以便于当再次接收到所述非法 P2P 节点发送的连接请求时，不与所述非法 P2P 节点进行连接，进而可以避免出现占用其他节点连接资源的情况。其中，所述节点信息可以为节点名称、ID 号等。

204、向 P2P 服务器发送非法 P2P 节点的节点信息。

35 其中，所述 P2P 服务器接收不同 P2P 节点发送的不同非法 P2P 节点的节点信息，进一步地，以使得所述 P2P 服务器根据所述不同非法 P2P 节点的节

点信息，统计不同非法 P2P 节点分别对应的举报次数并进行检测，当检测出存在举报次数大于或等于预设阈值的非法 P2P 节点时将其从 P2P 网络中剔除。以便达到净化 P2P 网络环境的目的，可以提高 P2P 网络的分享效率。

5 本发明实施例提供的另一种基于 P2P 网络的数据处理方法，首先 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，其中所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点，然后通过 P2P 服务器统计非法 P2P 节点分别对应的举报次数，将举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除，可以实现
10 将一些恶意发送虚假数据的 P2P 节点以及一些上传速度不好的 P2P 节点从 P2P 网络中剔除，进而可以实现净化 P2P 网络环境的目的，从而可以提高 P2P 网络的分享效率。

本发明实施例提供了又一种基于 P2P 网络的数据处理方法，可以应用于 P2P 节点，如图 3 所示，所述方法包括：

15 301、通过预置 CRC32 校验算法，将 P2P 节点发送的数据进行验证，得到对应的 CRC32 值。

302、检测 CRC32 值是否与预置 M3U8 文件中的预置 CRC32 值匹配。

其中，所述预置 M3U8 文件可以为 UTF-8 编码格式的 M3U 文件。所述预置 CRC32 值可以为本地需要获取的数据对应的 CRC32 值。具体地，可以
20 预先将所述预置 CRC32 值保存在预置 M3U8 文件中，以便当需要对数据进行虚假数据校验时进行调用。

303、若 CRC32 值与预置 M3U8 文件中的预置 CRC32 值不匹配，则将 P2P 节点发送的数据确定为虚假数据。

25 304、检测接收到 P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈值。

其中，所述虚假数据可以为数据不完整、存在数据丢失的数据，也可以为与需要获取的数据不匹配的数据。所述预置个数阈值可以根据实际需求进行配置。

30 305、若虚假数据的个数大于或等于预置个数阈值，则确定 P2P 节点为非法 P2P 节点。

进一步地，在执行所述步骤 305 之后，还可以包括：输出提示信息，所述提示信息用于提示所述 P2P 节点为非法 P2P 节点。其中，所述提示信息可以为文本提示信息、图片提示信息、音频提示信息、视频提示信息等。需要说明的是，在执行步骤 305 之后，通过输出提示信息，可以使用户了解存在
35 非法 P2P 节点，方便用户进行后期处理，可以增强用户的体验。

306、与非法 P2P 节点断开连接并记录非法 P2P 节点的节点信息。

进一步地，以便于当再次接收到所述非法 P2P 节点发送的连接请求时，不与所述非法 P2P 节点进行连接，进而可以避免出现占用其他节点连接资源的情况。

5 307、向 P2P 服务器发送非法 P2P 节点的节点信息。

其中，所述 P2P 服务器接收不同 P2P 节点发送的不同非法 P2P 节点的节点信息。进一步地，以使得所述 P2P 服务器根据所述不同非法 P2P 节点的节点信息，统计不同非法 P2P 节点分别对应的举报次数并进行检测，当检测出存在举报次数大于或等于预设阈值的非法 P2P 节点时将其从 P2P 网络中剔除。
10 以便达到净化 P2P 网络环境的目的，可以提高 P2P 网络的分享效率。

本发明实施例提供的又一种基于 P2P 网络的数据处理方法，首先 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，其中所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的
15 P2P 节点，然后通过 P2P 服务器统计非法 P2P 节点分别对应的举报次数，将举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除，可以实现将一些恶意发送虚假数据的 P2P 节点以及一些上传速度不好的 P2P 节点从 P2P 网络中剔除，进而可以实现净化 P2P 网络环境的目的，从而可以提高 P2P 网络的分享效率。

20 进一步地，作为图 1 所述方法的具体实现，本发明实施例提供了一种 P2P 服务器，如图 4 所示，所述 P2P 服务器包括：接收单元 41、统计单元 42、检测单元 43、剔除单元 44。

所述接收单元 41，可以用于接收 P2P 节点发送的非法 P2P 节点的节点信息，所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或
25 等于预置个数阈值的 P2P 节点。所述接收单元 41 面向各个 P2P 节点。

所述统计单元 42，可以用于根据所述接收单元 41 接收的非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数。所述统计单元 32 为本 P2P 服务器中统计非法 P2P 节点对应举报次数的主要功能模块。

30 所述检测单元 43，可以用于检测是否存在举报次数大于或等于预设阈值的非法 P2P 节点。所述检测单元 43 为本 P2P 服务器中检测是否存在举报次数大于或等于预设阈值的非法 P2P 节点的主要功能模块。

所述剔除单元 44，可以用于若所述检测单元 43 检测出存在举报次数大于或等于预设阈值的非法 P2P 节点，则将所述举报次数大于或等于预设阈值的
35 非法 P2P 节点从 P2P 网络中剔除。所述剔除单元 44 为本 P2P 服务器中将

举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除的主要功能，以便实现净化 P2P 网络环境的目的。

需要说明的是，本发明实施例提供的一种 P2P 服务器所涉及各功能单元的其他相应描述，可以参考图 1 中的对应描述，在此不再赘述。本发明实施例中可以通过硬件处理器 (hardware processor) 来实现相关功能模块。

本发明实施例提供的一种 P2P 服务器，首先 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，其中所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点，然后通过 P2P 服务器统计非法 P2P 节点分别对应的举报次数，将举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除，可以实现将一些恶意发送虚假数据的 P2P 节点以及一些上传速度不好的 P2P 节点从 P2P 网络中剔除，进而可以实现净化 P2P 网络环境的目的，从而可以提高 P2P 网络的分享效率。

具体地，本发明实施例提供的另一种 P2P 服务器，如图 5 所示，所述 P2P 服务器还包括：输出单元 45。

所述输出单元 45，可以用于输出提示信息，所述提示信息用于提示所述举报次数大于或等于预设阈值的非法节点已从 P2P 网络中剔除。

进一步地，作为图 2 所述方法的具体实现，本发明实施例提供了一种 P2P 节点，如图 6 所示，所述 P2P 节点包括：检测单元 61、确定单元 62、断开单元 63、记录单元 64、发送单元 65。

所述检测单元 61，可以用于当确定接收到 P2P 节点发送的数据为虚假数据时，检测接收到所述 P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈值。所述检测单元 61 为本 P2P 节点中检测是否存在非法 P2P 节点的主要功能模块。

所述确定单元 62，可以用于若所述检测单元 61 检测出虚假数据的个数大于或等于所述预置个数阈值，则确定所述 P2P 节点为非法 P2P 节点。

所述断开单元 63，可以用于与所述非法 P2P 节点断开连接。所述断开单元 63 为本 P2P 节点中控制与非法 P2P 节点之间连接的主要功能模块。

所述记录单元 64，可以用于记录所述非法 P2P 节点的节点信息。所述记录单元 64 为本 P2P 节点中记录非法 P2P 节点的节点信息的主要功能模块。

进一步地，以便于当再次接收到所述非法 P2P 节点发送的连接请求时，不与所述非法 P2P 节点进行连接。

所述发送单元 65，可以用于向 P2P 服务器发送所述非法 P2P 节点的节点信息，所述 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息。所述发送单元 65 面向 P2P 服务器。

进一步地，以使得所述 P2P 服务器根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数并进行检测，当检测出存在举报次数大于或等于预设阈值的非法 P2P 节点时将其从 P2P 网络中剔除。

需要说明的是，本发明实施例提供的一种 P2P 节点所涉及各功能单元的其他相应描述，可以参考图 2 中的对应描述，在此不再赘述。本发明实施例中可以通过硬件处理器来实现相关功能模块。

本发明实施例提供的一种 P2P 节点，首先 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，其中所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点，然后通过 P2P 服务器统计非法 P2P 节点分别对应的举报次数，将举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除，可以实现将一些恶意发送虚假数据的 P2P 节点以及一些上传速度不好的 P2P 节点从 P2P 网络中剔除，进而可以实现净化 P2P 网络环境的目的，从而可以提高 P2P 网络的分享效率。

进一步地，作为图 3 所述方法的具体实现，本发明实施例提供了另一种 P2P 节点，如图 7 所示，所述 P2P 节点包括：检测单元 71、确定单元 72、断开单元 73、记录单元 74、发送单元 75。

所述检测单元 71，可以用于当确定接收到 P2P 节点发送的数据为虚假数据时，检测接收到所述 P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈值。所述检测单元 71 为本 P2P 节点中检测是否存在非法 P2P 节点的主要功能模块。

所述确定单元 72，可以用于若所述检测单元 71 检测出虚假数据的个数大于或等于所述预置个数阈值，则确定所述 P2P 节点为非法 P2P 节点。

所述断开单元 73，可以用于与所述非法 P2P 节点断开连接。所述断开单元 73 为本 P2P 节点中控制与非法 P2P 节点之间连接的主要功能模块。

所述记录单元 74，可以用于记录所述非法 P2P 节点的节点信息。所述记录单元 74 为本 P2P 节点中记录非法 P2P 节点的节点信息的主要功能模块。

进一步地，以便于当再次接收到所述非法 P2P 节点发送的连接请求时，不与所述非法 P2P 节点进行连接。

所述发送单元 75，可以用于向 P2P 服务器发送所述非法 P2P 节点的节点信息，所述 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息。所述发送单元 75 面向 P2P 服务器。

进一步地，以使得所述 P2P 服务器根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数并进行检测，当检测出存在举报次数大于或等于预设阈值的非法 P2P 节点时将其从 P2P 网络中剔除。

进一步地，所述 P2P 节点还包括：验证单元 76。

所述验证单元 76，可以用于通过预置 CRC32 校验算法，将所述 P2P 节点发送的数据进行验证，得到对应的 CRC32 值。

5 所述检测单元 71，还可以用于检测所述 CRC32 值是否与预置 M3U8 文件中的预置 CRC32 值匹配。

所述确定单元 72，还可以用于若所述检测单元 71 检测出所述 CRC32 值与所述预置 M3U8 文件中的预置 CRC32 值不匹配，则将所述 P2P 节点发送的数据确定为虚假数据。

进一步地，所述 P2P 节点还包括：输出单元 77。

10 所述输出单元 77，可以用于输出提示信息，所述提示信息用于提示所述 P2P 节点为非法 P2P 节点。

需要说明的是，本发明实施例提供的另一种 P2P 节点所涉及各功能单元的其他相应描述，可以参考图 3 中的对应描述，在此不再赘述。本发明实施例中可以通过硬件处理器来实现相关功能模块。

15 本发明实施例提供的另一种 P2P 节点，首先 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，其中所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点，然后通过 P2P 服务器统计非法 P2P 节点分别对应的举报次数，将举报次数大于或等于
20 预设阈值的非法 P2P 节点从 P2P 网络中剔除，可以实现将一些恶意发送虚假数据的 P2P 节点以及一些上传速度不好的 P2P 节点从 P2P 网络中剔除，进而可以实现净化 P2P 网络环境的目的，从而可以提高 P2P 网络的分享效率。

进一步地，本发明实施例提供了一种基于 P2P 网络的数据处理系统，包括：P2P 服务器 81 和 P2P 节点 82。

25 所述 P2P 节点 82，可以用于当确定接收到 P2P 节点发送的数据为虚假数据时，检测接收到所述 P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈值；若所述虚假数据的个数大于或等于所述预置个数阈值，则确定所述 P2P 节点为非法 P2P 节点；与所述非法 P2P 节点断开连接并记录所述非法 P2P 节点的节点信息，以便当再次接收到所述非法 P2P 节点发送的连接
30 请求时，不与所述非法 P2P 节点进行连接；向所述 P2P 服务器 81 发送所述非法 P2P 节点的节点信息。

所述 P2P 服务器 81，用于接收不同的所述 P2P 节点 81 发送的不同非法 P2P 节点的节点信息；根据所述不同非法 P2P 节点的节点信息，统计不同非法 P2P 节点分别对应的举报次数；检测是否存在举报次数大于或等于预设阈值的非法 P2P 节点；若存在，则将所述举报次数大于或等于预设阈值的非法
35

P2P 节点从 P2P 网络中剔除。

示例性的，如图 9 所示，图 9 示出了本发明实施例提供的一种 P2P 服务器的实体结构示意图，该 P2P 服务器可以包括：处理器(processor)91、通信接口(Communications Interface)92、存储器(memory)93 和总线 94，其中，处
5 理器 91、通信接口 92、存储器 93 通过总线 94 完成相互间的通信。通信接口 92 可以用于服务器与客户端之间的信息传输。处理器 91 可以调用存储器 93 中的逻辑指令，以执行如下方法：P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的
10 个数大于或等于预置个数阈值的 P2P 节点；根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数；检测是否存在举报次数大于或等于预设阈值的非法 P2P 节点；若存在，则将所述举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除。此外，上述的存储器 93 中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用
15 时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备
20 等）执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

本发明实施例提供的一种基于 P2P 网络的数据处理系统，首先 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，其中所述非法 P2P 节点的
25 节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点，然后通过 P2P 服务器统计非法 P2P 节点分别对应的举报次数，将举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除，可以实现将一些
30 恶意发送虚假数据的 P2P 节点以及一些上传速度不好的 P2P 节点从 P2P 网络中剔除，进而可以实现净化 P2P 网络环境的目的，从而可以提高 P2P 网络的分享效率。

以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络
35 单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例

方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等等）执行各个实施例或者实施例的某些部分所述的方法。

最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

权利要求

1、一种基于 P2P 网络的数据处理方法，其特征在于，包括：

P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点；

根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数；

检测是否存在举报次数大于或等于预设阈值的非法 P2P 节点；

若存在，则将所述举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除。

2、根据权利要求 1 所述的基于 P2P 网络的数据处理方法，其特征在于，所述若存在，则将所述举报次数大于或等于预设阈值的非法节点从 P2P 网络中剔除之后，所述方法还包括：

输出提示信息，所述提示信息用于提示所述举报次数大于或等于预设阈值的非法节点已从 P2P 网络中剔除。

3、一种基于 P2P 网络的数据处理方法，其特征在于，包括：

当确定接收到 P2P 节点发送的数据为虚假数据时，检测接收到所述 P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈值；

若所述虚假数据的个数大于或等于所述预置个数阈值，则确定所述 P2P 节点为非法 P2P 节点；

与所述非法 P2P 节点断开连接并记录所述非法 P2P 节点的节点信息，以便当再次接收到所述非法 P2P 节点发送的连接请求时，不与所述非法 P2P 节点进行连接；

向 P2P 服务器发送所述非法 P2P 节点的节点信息，其中，所述 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，以使得所述 P2P 服务器根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数并进行检测，当检测出存在举报次数大于或等于预设阈值的非法 P2P 节点时将其从 P2P 网络中剔除。

4、根据权利要求 3 所述的基于 P2P 网络的数据处理方法，其特征在于，所述当检测出接收到 P2P 节点发送的数据为虚假数据时，检测接收到所述 P2P 节点发送的虚假数据的个数是否大于或等于预置个数阈值之前，所述方法还包括：

通过预置 CRC32 校验算法，将所述 P2P 节点发送的数据进行验证，得到

对应的 CRC32 值;

检测所述 CRC32 值是否与预置 M3U8 文件中的预置 CRC32 值匹配;
若不匹配,则将所述 P2P 节点发送的数据确定为虚假数据。

5 5、根据权利要求 3 所述的基于 P2P 网络的数据处理方法,其特征在于,
所述若所述虚假数据的个数大于或等于所述预置个数阈值,则确定所述 P2P
节点为非法 P2P 节点之后,所述方法还包括:

输出提示信息,所述提示信息用于提示所述 P2P 节点为非法 P2P 节点。

6、一种 P2P 服务器,其特征在于,包括:

10 接收单元,用于接收 P2P 节点发送的非法 P2P 节点的节点信息,所述非
法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的,所述
非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个
数阈值的 P2P 节点;

统计单元,用于根据所述接收单元接收的非法 P2P 节点的节点信息,统
计非法 P2P 节点分别对应的举报次数;

15 检测单元,用于检测是否存在举报次数大于或等于预设阈值的非法 P2P
节点;

剔除单元,用于若所述检测单元检测出存在举报次数大于或等于预设阈
值的非法 P2P 节点,则将所述举报次数大于或等于预设阈值的非法 P2P 节点
从 P2P 网络中剔除。

20 7、根据权利要求 6 所述的 P2P 服务器,其特征在于,所述 P2P 服务器
还包括:

输出单元,用于输出提示信息,所述提示信息用于提示所述举报次数大
于或等于预设阈值的非法节点已从 P2P 网络中剔除。

8、一种 P2P 节点,其特征在于,包括:

25 检测单元,用于当确定接收到 P2P 节点发送的数据为虚假数据时,检测
接收到所述 P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈
值;

确定单元,用于若所述检测单元检测出虚假数据的个数大于或等于所述
预置个数阈值,则确定所述 P2P 节点为非法 P2P 节点;

30 断开单元,用于与所述非法 P2P 节点断开连接;

记录单元,用于记录所述非法 P2P 节点的节点信息,以便当再次接收到
所述非法 P2P 节点发送的连接请求时,不与所述非法 P2P 节点进行连接;

35 发送单元,用于向 P2P 服务器发送所述非法 P2P 节点的节点信息,所述
P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息,以使得所述 P2P
服务器根据所述非法 P2P 节点的节点信息,统计非法 P2P 节点分别对应的举

报次数并进行检测，当检测出存在举报次数大于或等于预设阈值的非法 P2P 节点时将其从 P2P 网络中剔除。

9、根据权利要求 8 所述的 P2P 节点，其特征在于，所述 P2P 节点还包括：验证单元；

5 所述验证单元，用于通过预置 CRC32 校验算法，将所述 P2P 节点发送的数据进行验证，得到对应的 CRC32 值；

所述检测单元，还用于检测所述 CRC32 值是否与预置 M3U8 文件中的预置 CRC32 值匹配；

10 所述确定单元，还用于若所述检测单元检测出所述 CRC32 值与所述预置 M3U8 文件中的预置 CRC32 值不匹配，则将所述 P2P 节点发送的数据确定为虚假数据。

10、根据权利要求 9 所述的 P2P 节点，其特征在于，所述 P2P 节点还包括：

15 输出单元，用于输出提示信息，所述提示信息用于提示所述 P2P 节点为非法 P2P 节点。

11、一种基于 P2P 网络的数据处理系统，其特征在于，包括：权利要求 6-7 任一项所述的 P2P 服务器和权利要求 8-10 任一项所述的 P2P 节点。

12、一种基于 P2P 网络的数据处理装置，其特征在于，所述装置包括：处理器，和

20 存储器，被配置为存储所述处理器的可执行指令；
所述的处理器被配置为：

25 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，所述非法 P2P 节点的节点信息为 P2P 节点检测出存在非法 P2P 节点时发送的，所述非法 P2P 节点为向所述 P2P 节点累计发送虚假数据的个数大于或等于预置个数阈值的 P2P 节点；

根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数；

检测是否存在举报次数大于或等于预设阈值的非法 P2P 节点；

30 若存在，则将所述举报次数大于或等于预设阈值的非法 P2P 节点从 P2P 网络中剔除。

13、一种基于 P2P 网络的数据处理装置，其特征在于，所述装置包括：处理器，和

存储器，被配置为存储所述处理器的可执行指令；

所述的处理器被配置为：

35 当确定接收到 P2P 节点发送的数据为虚假数据时，检测接收到所述

P2P 节点累计发送的虚假数据的个数是否大于或等于预置个数阈值；

若所述虚假数据的个数大于或等于所述预置个数阈值，则确定所述 P2P 节点为非法 P2P 节点；

5 与所述非法 P2P 节点断开连接并记录所述非法 P2P 节点的节点信息，以便当再次接收到所述非法 P2P 节点发送的连接请求时，不与所述非法 P2P 节点进行连接；

10 向 P2P 服务器发送所述非法 P2P 节点的节点信息，其中，所述 P2P 服务器接收 P2P 节点发送的非法 P2P 节点的节点信息，以使得所述 P2P 服务器根据所述非法 P2P 节点的节点信息，统计非法 P2P 节点分别对应的举报次数并进行检测，当检测出存在举报次数大于或等于预设阈值的非法 P2P 节点时将其从 P2P 网络中剔除。

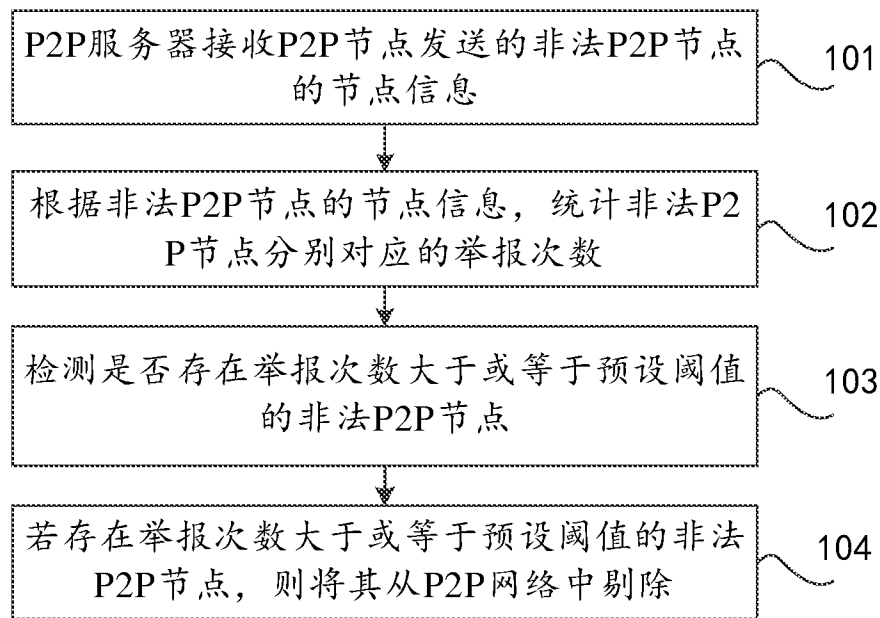


图 1

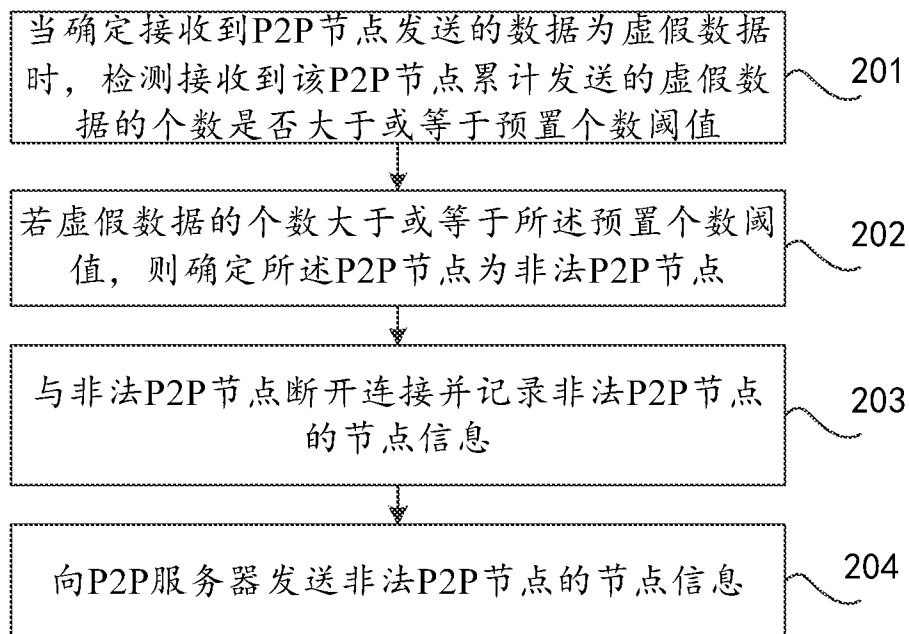


图 2

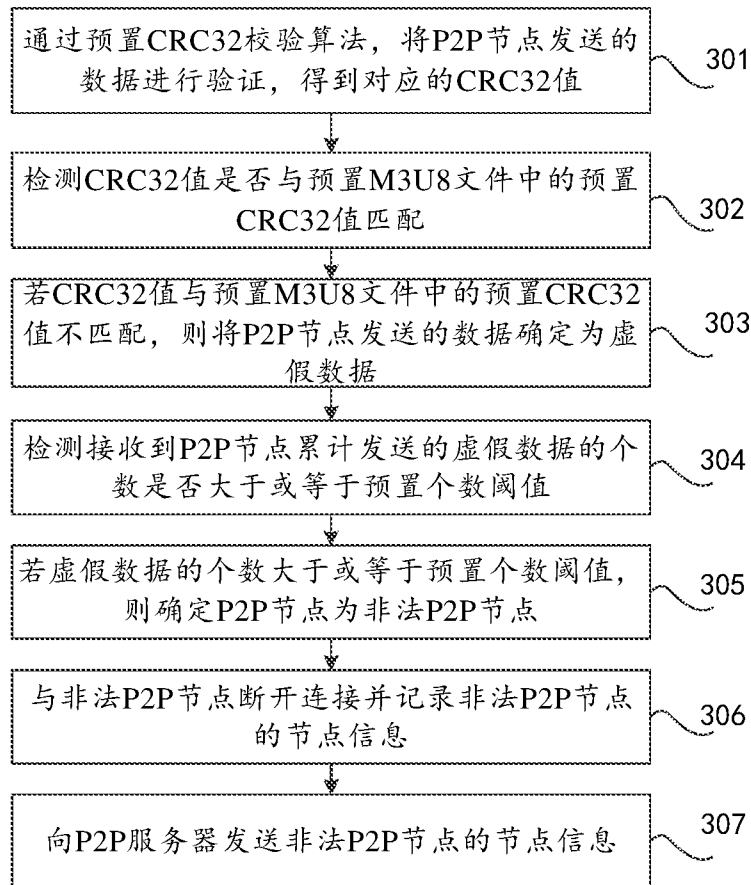


图 3

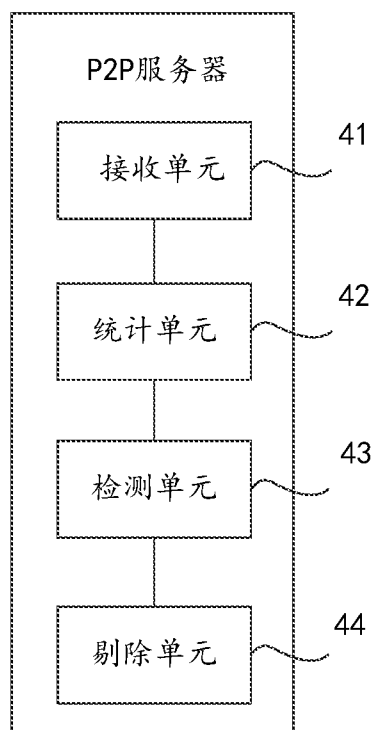


图 4

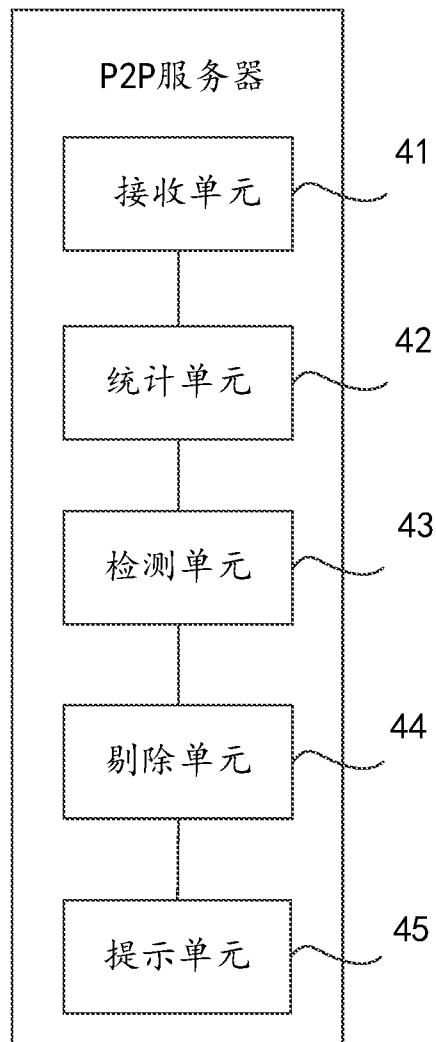


图 5

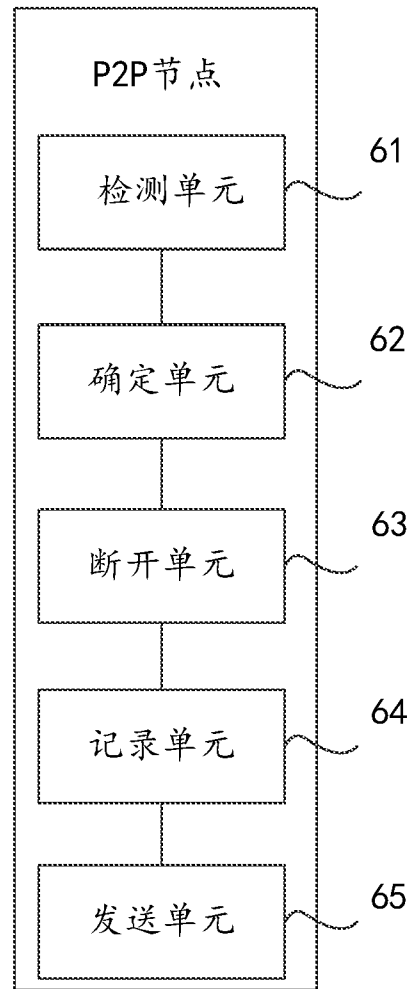


图 6

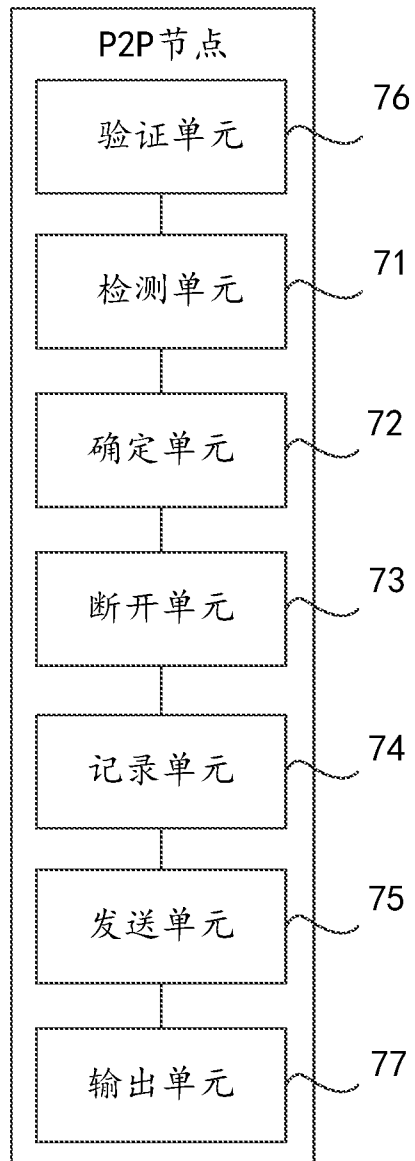


图 7

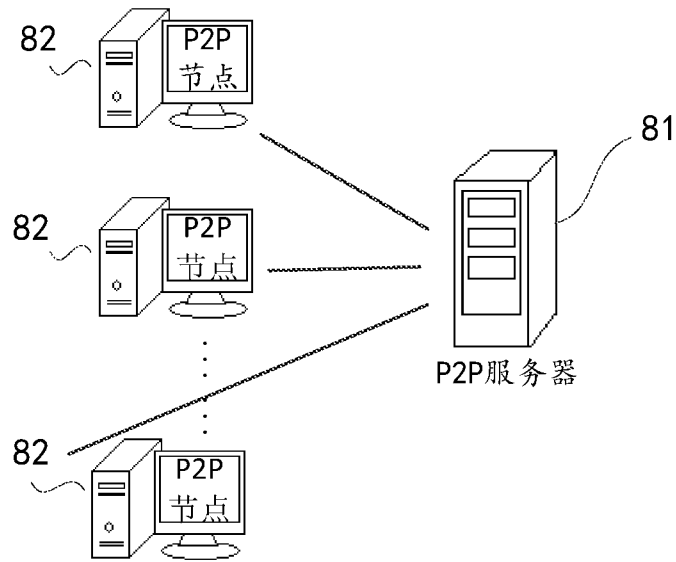


图 8

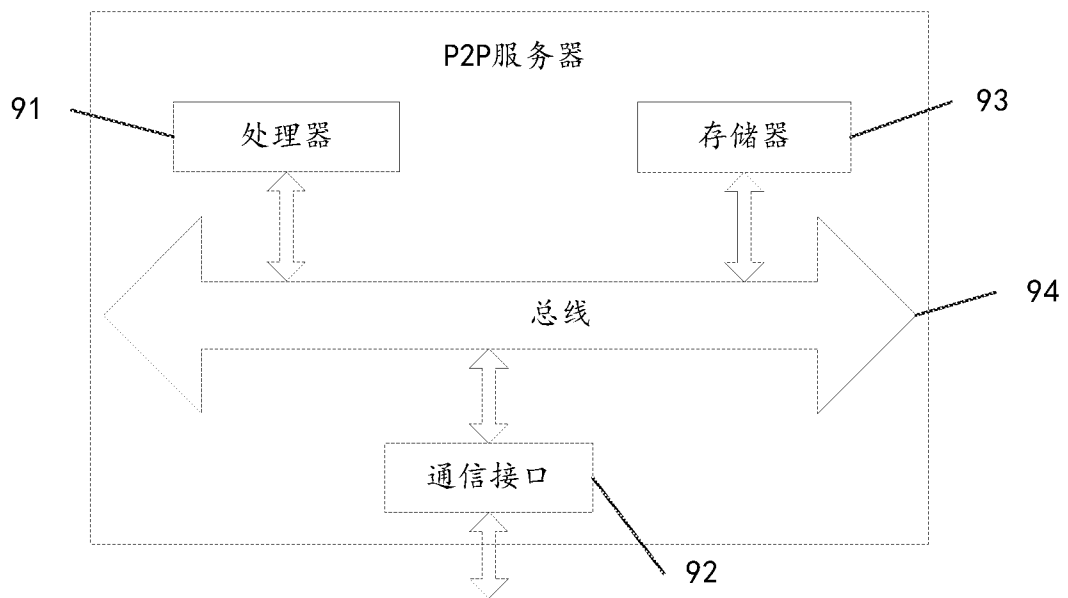


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/089464**A. CLASSIFICATION OF SUBJECT MATTER**

H04L 29/08 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: P2P, peer to peer, node, connect+, reliability, threshold, illegal, credit, report, alarm, abnormal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101282366 A (BEIJING CE OPEN SOURCE SOFTWARE CO., LTD.), 08 October 2008 (08.10.2008), description, pages 4-5 and 11	1-13
A	CN 101599996 A (CHENGDU HUAWEI SYMANTEC TECHNOLOGIES CO., LTD.), 09 December 2009 (09.12.2009), the whole document	1-13
A	CN 102231761 A (LESHI INTERNET INFORMATION AND TECHNOLOGY CORP., BEIJING), 02 November 2011 (02.11.2011), the whole document	1-13
A	CN 105049463 A (CASIO COMPUTER CO., LTD.), 11 November 2015 (11.11.2015), the whole document	1-13

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 30 August 2016 (30.08.2016)	Date of mailing of the international search report 27 September 2016 (27.09.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer LI, Lin Telephone No.: (86-10) 62413203

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/089464

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101282366 A	08 October 2008	None	
CN 101599996 A	09 December 2009	None	
CN 102231761 A	02 November 2011	None	
CN 105049463 A	11 November 2015	JP 2015210550 A	24 November 2015
		US 2015312334 A1	29 October 2015

国际检索报告

国际申请号

PCT/CN2016/089464

A. 主题的分类

H04L 29/08(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT, CNKI, WPI, EPODOC; P2P, peer to peer, node, connect+, reliability, threshold, 点对点, 节点, 连接, 非法, 信誉, 举报, 告警, 异常, 阈值

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 101282366 A (北京中企开源信息技术有限公司) 2008年 10月 8日 (2008 - 10 - 08) 说明书第4-5、11页	1-13
A	CN 101599996 A (成都市华为赛门铁克科技有限公司) 2009年 12月 9日 (2009 - 12 - 09) 全文	1-13
A	CN 102231761 A (乐视网信息技术北京股份有限公司) 2011年 11月 2日 (2011 - 11 - 02) 全文	1-13
A	CN 105049463 A (卡西欧计算机株式会社) 2015年 11月 11日 (2015 - 11 - 11) 全文	1-13

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2016年 8月 30日

国际检索报告邮寄日期

2016年 9月 27日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

李琳

电话号码 (86-10)62413203

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/089464

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	101282366	A	2008年 10月 8日	无			
CN	101599996	A	2009年 12月 9日	无			
CN	102231761	A	2011年 11月 2日	无			
CN	105049463	A	2015年 11月 11日	JP	2015210550	A	2015年 11月 24日
				US	2015312334	A1	2015年 10月 29日

表 PCT/ISA/210 (同族专利附件) (2009年7月)