



(12) 发明专利申请

(10) 申请公布号 CN 103597783 A

(43) 申请公布日 2014. 02. 19

(21) 申请号 201280027289. 5

(74) 专利代理机构 中国国际贸易促进委员会专
利商标事务所 11038

(22) 申请日 2012. 05. 31

代理人 罗亚男

(30) 优先权数据

61/492, 903 2011. 06. 03 US

(51) Int. Cl.

13/224, 599 2011. 09. 02 US

H04L 12/58 (2006. 01)

(85) PCT国际申请进入国家阶段日

2013. 12. 03

(86) PCT国际申请的申请数据

PCT/US2012/040314 2012. 05. 31

(87) PCT国际申请的公布数据

W02012/166990 EN 2012. 12. 06

(71) 申请人 苹果公司

地址 美国加利福尼亚

(72) 发明人 A · A · 梅迪纳 A · H · 威若斯

D · N · 布洛 J · T · 戴维

J · E · 桑塔玛利亚 J · N · 伍德

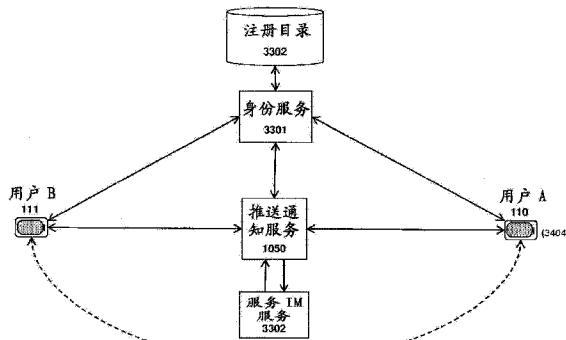
权利要求书3页 说明书46页 附图36页

(54) 发明名称

用于安全即时消息传输的系统与方法

(57) 摘要

描述了用于安全即时消息传输的系统与方法。例如，在一种实施例中，第一用户利用第二用户的ID码为即时消息传输会话识别第二用户。作为响应，为第一用户提供第二用户的网络信息和与第二用户关联的公钥。然后，第一用户利用第二用户的公钥和一个私钥加密即时消息。在一种实施例中，第一用户利用第二用户的公钥加密即时消息的内容(例如，任何文字和 / 或附件)并且利用第一用户的私钥签署内容。加密的消息从第一用户发送到第二用户。然后，第二用户利用第二用户的私钥解密该即时消息并且利用第一用户的公钥验证签名。



1. 一种用于实现安全即时消息传输的方法，包括：

从第一用户接收与第二用户建立即时消息传输会话的请求，该请求包括识别第二用户的识别码；

确定第二用户是否具有在网络服务上注册的一个或多个移动设备；

如果第二用户具有注册的一个或多个移动设备，则为第一用户提供识别所述一个或多个移动设备的寻址信息和与第二用户关联的公钥；

利用第二用户的公钥和第一用户的私钥加密即时消息来生成加密的即时消息；

把加密的即时消息从第一用户的移动设备发送到第二用户的所述一个或多个移动设备；及

在第二用户的移动设备处利用一私钥解密该即时消息。

2. 如权利要求 1 所述的方法，其中识别码包括第二用户的电子邮件地址。

3. 如权利要求 1 所述的方法，其中地址信息包括在网络服务上唯一识别第二用户的所述一个或多个移动设备的令牌。

4. 如权利要求 1 所述的方法，其中发送进一步包括：

把加密的即时消息提供给第二移动设备向其注册的推送通知服务，作为响应，该推送通知服务把加密的消息推送到第二移动设备。

5. 如权利要求 1 所述的方法，其中确定进一步包括：

查询注册数据库以确定第二用户是否在网络服务上注册，该注册数据库把第二用户与一个或多个识别码关联。

6. 如权利要求 1 所述的方法，其中加密即时消息进一步包括利用第二用户的公钥加密包括任何文字和 / 或附件的即时消息的内容，并且利用第一用户的私钥签署该内容。

7. 如权利要求 6 所述的方法，其中第二用户利用第二用户的私钥解密内容并且利用第一用户的公钥验证签名。

8. 如权利要求 7 所述的方法，其中第二用户从网络服务检索第一用户的公钥。

9. 如权利要求 1 所述的方法，进一步包括：

为第一用户提供会话密钥，该会话密钥包括利用第一和第二用户的识别码及第一和第二用户的网络信息生成的签名。

10. 如权利要求 9 所述的方法，进一步包括：

把会话密钥和即时消息发送到安全即时消息服务；及

利用会话密钥验证第一和第二用户的识别码及第一和第二用户的网络信息。

11. 如权利要求 10 所述的方法，其中验证包括在安全即时消息传输服务处重新生成签名。

12. 一种实现安全即时消息传输的系统，包括用于存储程序代码的存储器和用于处理该程序代码以便执行以下操作的至少一个处理器：

从第一用户接收与第二用户建立即时消息传输会话的请求，该请求包括识别第二用户的识别码；

确定第二用户是否具有在网络服务上注册的一个或多个移动设备；

如果第二用户具有注册的一个或多个移动设备，则为第一用户提供识别所述一个或多个移动设备的寻址信息和与第二用户关联的公钥；

利用第二用户的公钥和第一用户的私钥加密即时消息来生成加密的即时消息；

把加密的即时消息从第一用户的移动设备发送到第二用户的所述一个或多个移动设备；及

在第二用户的移动设备处利用一私钥解密该即时消息。

13. 如权利要求 12 所述的系统，其中识别码包括第二用户的电子邮件地址。

14. 如权利要求 12 所述的系统，其中地址信息包括在网络服务上唯一识别第二用户的所述一个或多个移动设备的令牌。

15. 如权利要求 12 所述的系统，其中发送进一步包括：

把加密的即时消息提供给第二移动设备向其注册的推送通知服务，作为响应，该推送通知服务把加密的消息推送到第二移动设备。

16. 如权利要求 12 所述的系统，其中确定进一步包括：

查询注册数据库，确定第二用户是否在网络服务上注册，该注册数据库把第二用户与一个或多个识别码关联。

17. 如权利要求 12 所述的系统，其中加密即时消息进一步包括利用第二用户的公钥加密包括任何文字和 / 或附件的即时消息的内容，并且利用第一用户的私钥签署该内容。

18. 如权利要求 17 所述的系统，其中第二用户利用第二用户的私钥解密内容并且利用第一用户的公钥验证签名。

19. 如权利要求 18 所述的系统，其中第二用户从网络服务检索第一用户的公钥。

20. 如权利要求 12 所述的系统，包括附加的程序代码，使处理器执行以下附加操作：

为第一用户提供会话密钥，该会话密钥包括利用第一和第二用户的识别码及第一和第二用户的网络信息生成的签名。

21. 如权利要求 20 所述的系统，包括附加的程序代码，使处理器执行以下附加操作：

把会话密钥和即时消息发送到安全即时消息服务；及

利用会话密钥验证第一和第二用户的识别码及第一和第二用户的网络信息。

22. 如权利要求 21 所述的系统，其中验证包括在安全即时消息传输服务处重新生成签名。

23. 一种具有存储在其上的程序代码的机器可读介质，当程序代码被机器执行时，使机器执行以下操作：

从第一用户接收与第二用户建立即时消息传输会话的请求，该请求包括识别第二用户的识别码；

确定第二用户是否具有在网络服务上注册的一个或多个移动设备；

如果第二用户具有注册的一个或多个移动设备，则为第一用户提供识别所述一个或多个移动设备的寻址信息和与第二用户关联的公钥；

利用第二用户的公钥和第一用户的私钥加密即时消息来生成加密的即时消息；

把加密的即时消息从第一用户的移动设备发送到第二用户的所述一个或多个移动设备；及

在第二用户的移动设备处利用一私钥解密该即时消息。

24. 如权利要求 23 所述的机器可读介质，其中识别码包括第二用户的电子邮件地址。

25. 如权利要求 23 所述的机器可读介质，其中地址信息包括在网络服务上唯一识别第

二用户的所述一个或多个移动设备的令牌。

26. 如权利要求 23 所述的机器可读介质, 其中发送进一步包括 :

把加密的即时消息提供给第二移动设备向其注册的推送通知服务, 作为响应, 该推送通知服务把加密的消息推送到第二移动设备。

27. 如权利要求 23 所述的机器可读介质, 其中确定进一步包括 :

查询注册数据库以确定第二用户是否在网络服务上注册, 该注册数据库把第二用户与一个或多个识别码关联。

28. 如权利要求 23 所述的机器可读介质, 其中加密即时消息进一步包括利用第二用户的公钥加密包括任何文字和 / 或附件的即时消息的内容, 并且利用第一用户的私钥签署该内容。

29. 如权利要求 17 所述的机器可读介质, 其中第二用户利用第二用户的私钥解密内容并且利用第一用户的公钥验证签名。

30. 如权利要求 29 所述的机器可读介质, 其中第二用户从网络服务检索第一用户的公钥。

31. 如权利要求 23 所述的机器可读介质, 包括附加的程序代码, 使机器执行以下附加操作 :

为第一用户提供会话密钥, 该会话密钥包括利用第一和第二用户的识别码及第一和第二用户的网络信息生成的签名。

32. 如权利要求 31 所述的机器可读介质, 包括附加的程序代码, 使机器执行以下附加操作 :

把会话密钥和即时消息发送到安全即时消息服务 ; 及

利用会话密钥验证第一和第二用户的识别码及第一和第二用户的网络信息。

33. 如权利要求 32 所述的机器可读介质, 其中验证包括在安全即时消息传输服务处重新生成签名。

用于安全即时消息传输的系统与方法

[0001] 对优先权的保护

[0002] 本申请根据美国法典第 35 章 119 (e)条要求于 2011 年 6 月 3 日提交的美国临时申请号 61/492,903 的申请日的利益。

技术领域

[0003] 本发明总体上涉及计算机联网领域。更具体地说，本发明涉及用于安全即时消息传输的改进装置与方法。

背景技术

[0004] 对等 (“P2P”) 计算指由计算节点组成的分布式网络体系结构，这些计算节点使其资源的一部分可以让其它的网络参与者直接获得。与其中服务器提供资源而客户端消费资源的传统客户端 - 服务器模型形成对比，P2P 网络中的对等体彼此建立直接通信信道并且既充当客户端又充当服务器。

[0005] 许多目前的 P2P 应用，诸如即时消息传输和视频聊天，都没有提供保护在对等体之间所发送的底层内容的适当安全措施。因此，需要改进的技术来经网络识别对等体并且提供安全的 P2P 事务。

附图说明

[0006] 对本发明的更好理解可以结合以下附图从以下具体描述获得，其中：

[0007] 图 1 说明了一种网络体系结构，其中一组移动设备与服务经网络通信。

[0008] 图 2a-2c 说明了连接数据交换 (CDX) 服务、匹配器服务和 / 或邀请服务的一种实施例之间的事务。

[0009] 图 3 说明了票据数据结构的一种实施例。

[0010] 图 4 说明了由 CDX 服务实现的方法的一种实施例。

[0011] 图 5 说明了由移动设备实现的方法的一种实施例。

[0012] 图 6 说明了通过主要和次要通信信道连接的一组移动设备。

[0013] 图 7 说明了用于在主要和次要通信信道之间进行选择的移动设备的一种实施例。

[0014] 图 8a-8b 说明了通过主要和次要通信信道连接的一组移动设备及结果产生的网络拓扑。

[0015] 图 9 说明了用于在主要和次要通信信道之间进行选择的计算机实现方法的一种实施例。

[0016] 图 10 说明了一种网络体系结构，其中一组移动设备和服务经网络通信，其中服务包括目录服务和推送通知服务。

[0017] 图 11 说明了邀请服务、推送通知服务和连接数据交换 (CDX) 服务的一种实施例之间的事务。

[0018] 图 12 说明了邀请服务、推送通知服务和中继服务的一种实施例之间的事务。

- [0019] 图 13 说明了用于在两个或更多个移动设备之间建立中继连接的中继服务的一种实施例。
- [0020] 图 14 说明了用于确定 NAT 兼容性的 NAT 兼容性图表的一种实施例。
- [0021] 图 15 说明了用于为在线应用匹配移动设备的匹配器服务的一种实施例。
- [0022] 图 16 说明了用于匹配用户 / 设备的方法的一种实施例。
- [0023] 图 17a-17d 说明了为匹配用户 / 设备而执行的示例性表更新序列。
- [0024] 图 18 说明了利用不同的匹配适合变量来匹配用户 / 设备的方法。
- [0025] 图 19 说明了揭示用于应用的应用编程接口 (API) 和用于与一组服务通信的服务 API 的框架。
- [0026] 图 20 说明了具有用于应用的 API、游戏守护进程和用于与服务通信的游戏服务模块的游戏框架的一种实施例。
- [0027] 图 21 说明了 API 实现软件组件和 API 调用软件组件的一种实施例。
- [0028] 图 22 说明了其中在操作系统、服务与应用之间进行 API 调用的一种实施例。
- [0029] 图 23 说明了示例性计算机系统体系结构的一种实施例。
- [0030] 图 24 说明了示例性计算机系统体系结构的另一种实施例。
- [0031] 图 25 说明了通过多个不同的服务提供商连接的多个用户。
- [0032] 图 26 说明了采用布隆过滤器 (bloom filter) 来识别用户位置的本发明的实施例。
- [0033] 图 27 说明了使用布隆过滤器的方法的一种实施例。
- [0034] 图 28 说明了使用布隆过滤器的方法的另一种实施例。
- [0035] 图 29 说明了根据本发明一种实施例、建立点到点 (P2P) 连接的两个用户。
- [0036] 图 30 说明了通过由特定服务提供商使用的中继服务建立 P2P 连接的两个用户。
- [0037] 图 31 说明了用于通过中继服务建立 P2P 连接的本发明的另一种实施例。
- [0038] 图 32 说明了在本发明一种实施例中采用的、具有 RFC3984 首部的 RTP 分组。
- [0039] 图 33 说明了推送通知服务与安全即时消息传输服务。
- [0040] 图 34 说明了用于建立安全即时消息传输会话的方法的一种实施例。
- [0041] 图 35 说明了用于建立安全即时消息传输会话的方法的另一种实施例。
- [0042] 图 36 说明了包括身份服务与应用认证服务的系统体系结构。
- [0043] 图 37 说明了用于安全地认证用户的方法的一种实施例。
- [0044] 图 38 说明了利用高速缓存与指纹有效地改善认证的本发明的一种实施例。

发明内容

- [0045] 描述了用于安全即时消息传输的系统与方法。例如，在一种实施例中，第一用户利用第二用户的 ID 码为即时消息传输会话识别第二用户。作为响应，为第一用户提供第二用户的网络信息和与第二用户关联的公钥。然后，第一用户利用第二用户的公钥和一个私钥加密即时消息。在一种实施例中，第一用户利用第二用户的公钥加密即时消息的内容(例如，任何文字和 / 或附件)并且利用第一用户的私钥签署内容。加密的消息从第一用户发送到第二用户。然后，第二用户利用第二用户的私钥解密该即时消息并且利用第一用户的公钥验证签名。

具体实施例

[0046] 以下描述的是用于在网络上建立、维护和利用主要和 / 或备份对等 (“P2P”) 通信信道的装置、方法与机器可读介质的实施例。还描述了分别用于邀请用户和匹配用户以进行 P2P 会话的邀请服务和匹配器服务。此外，还描述了允许用户在某些具体条件下建立中继连接的中继服务。最后，描述了允许应用开发者设计利用本文所述各种协作在线特征的应用的应用框架和关联的应用编程接口 (API)。

[0047] 贯穿本描述，为了解释，阐述了各种具体细节，以便提供对本发明的透彻理解。但是，对本领域技术人员来说将很显然，本发明没有这些具体细节中的一些也可以实践。在其它情况下，众所周知的结构与设备没有示出或者以框图形式示出，以避免模糊本发明的基本原理。

[0048] 用于有效且安全地交换连接数据的装置与方法

[0049] 如图 1 中所说明的，在本发明一种实施例中实现的通用网络拓扑可以包括一组“客户端”或“对等体”移动计算设备 A-D，分别为 120-123，这些移动设备经网络 120 彼此并且与一个或多个服务 110-112 通信。虽然在图 1 中说明为单个网络云，但是“网络”120 可以包括多种不同组件，包括诸如互联网的公共网络和诸如本地 Wi-Fi 网络（例如，802.11n 家用无线网络或者无线热点）、局域以太网、蜂窝数据网络（例如，3G、Edge 等）和 WiMAX 网络的专用网络，这仅仅是一些例子。例如，移动设备 A120 可以连接到由网络链路 125 表示的家用 Wi-Fi 网络，移动设备 B121 可以连接到由网络链路 126 表示的 3G 网络（例如，通用移动电信系统（“UMTS”）、高速上行链路分组接入（“HSUPA”）等），移动设备 C122 可以连接到由网络链路 127 表示的 WiMAX 网络，而移动设备 123 可以连接到由网络链路 128 表示的公共 Wi-Fi 网络。移动设备 120-123 在其上连接的每个本地网络链路 125-128 都可以通过网关和 / 或 NAT 设备（图 1 中未示出）耦合到诸如互联网的公共网络，由此启用各个移动设备 120-123 之间经公共网络的通信。但是，如果两个移动设备在相同的本地或专用网络（例如，相同的 Wi-Fi 网络）上，则这两个设备可以经那个本地 / 专用网络直接通信，从而绕过公共网络。当然，应当指出，本发明的基本原理不限于任何特定集合的网络类型或网络拓扑。

[0050] 图 1 中所说明的每个移动设备 120-123 都可以与连接数据交换 (CDX) 服务 110、匹配器服务 111 和邀请服务 112 通信。在一种实施例中，服务 110-112 可以实现为跨诸如服务器的一个或多个物理计算设备执行的软件。如图 1 中所示，在一种实施例中，服务 110-112 可以在由相同实体（例如，相同的数据服务提供商）管理并且可以由每个移动设备 120-123 经网络 120 访问的更大数据服务 100 的背景下实现。数据服务 100 可以包括连接各种类型服务器与数据库的局域网（例如，基于以太网的 LAN）。数据服务 100 也可以包括用于存储数据的一个或多个存储区域网络（“SAN”）。在一种实施例中，数据库存储并管理与每个移动设备 120-123 及那些设备的用户相关的数据（例如，用户帐号数据、设备帐号数据、用户应用数据、... 等等）。

[0051] 在一种实施例中，匹配器服务 111 可以基于规定的条件集合匹配两个或更多个移动设备以进行协作性 P2P 会话。例如，两个或更多个移动设备的用户可能对玩一个特定的多玩家游戏感兴趣。在这种情况下，匹配器服务 111 可以基于多个变量来识别要参与该游戏的一组移动设备，所述变量诸如是每个用户的经验级别、每个用户的年龄、匹配请求的定

时、为其请求匹配的特定游戏及各种特定于游戏的变量。作为例子但不是限制，匹配器服务 111 可以尝试在玩一个特定的游戏时匹配具有相似经验级别的用户。此外，成人可以与其他成人匹配，儿童可以与其他儿童匹配。而且，匹配器服务 111 可以基于接收那些请求的次序给用户请求排定优先次序。本发明的基本原理不限于任何特定的匹配标准设置或者任何特定类型的 P2P 应用。

[0052] 如以下具体描述的，响应于匹配请求，匹配器服务 111 可以与 CDX 服务 111 配合，以确保所有匹配的参与者都接收到必要的连接数据，用于以有效且安全的方式建立 P2P 会话。

[0053] 在一种实施例中，邀请服务 112 也识别要参与协作性 P2P 会话的移动设备。但是，在邀请服务 112 的情况下，至少一个参与者被另一个参与者具体地识别。例如，移动设备 A120 的用户可以具体地请求与移动设备 B121 的用户的协作会话(例如，利用用户 ID 或电话号码识别移动设备 B)。与匹配器服务 111 一样，响应于邀请请求，邀请服务 112 可以识别参与者集合并且与 CDX 服务 110 配合，以确保所有参与者都接收到必要的连接数据，以用于以有效且安全的方式建立 P2P 会话。

[0054] 如以上所提到的，在一种实施例中，CDX 服务 110 作为用于在两个或更多个移动设备之间建立 P2P 会话所需的连接数据的中心交换点操作。具体而言，响应于使外部服务和客户端通过每个移动设备的 NAT 通信(即，“打孔”通过 NAT，以到达设备)的移动设备请求，CDX 服务的一种实施例生成 NAT 遍历数据(有时候称为“打孔”数据)。例如，在一种实施例中，CDX 服务检测与移动设备通信所需的外部 IP 地址与端口并且把这个信息提供给移动设备。在一种实施例中，CDX 服务还接收并处理由匹配器服务 111 和邀请服务 112 生成的移动设备的列表，并且有效且安全地把连接数据分发到这个列表上包括的每个移动设备(如以下具体描述的)。

[0055] 在一种实施例中，移动设备与 CDX 服务 110 之间的通信是利用相对轻量级的网络协议，诸如用户数据报协议(“UDP”)套接字，建立的。如本领域技术人员已知的，UDP 套接字连接不需要握手对话来保证分组的可靠性、排序或者数据完整性，而且，因此，不消耗像 TCP 套接字连接那么多的分组处理开销。因此，UDP 的轻量级、无状态本质对于应答来自大量客户端的小查询的服务器来说是有用的。而且，不像 TCP，UDP 与分组广播(其中，分组发送到本地网络上的所有设备)和多播(其中，分组发送到本地网络上所有设备的一个子集)兼容。如以下所描述的，即使 UDP 可以使用，也可以通过利用会话密钥加密 NAT 遍历数据来维护关于 CDX 服务 110 的安全性。

[0056] 与 CDX 服务 110 所使用的低开销、轻量级网络协议形成对比，在一种实施例中，移动设备 120-123 与匹配器服务 111 和 / 或邀请服务 112 之间的通信是利用固有的安全网络协议，诸如超文本传输协议安全(“HTTPS”)，建立的，其中 HTTPS 依赖于安全套接字层(“SSL”)或传输层安全(“TLS”)连接。与这些协议关联的细节是本领域技术人员众所周知的。

[0057] 图 2a 说明了可以由 CDX 服务器实现的示例性事务序列。当描述 CDX 服务的一种实施例的操作时，以下术语将具有以下意义：

[0058] 连接数据 - 这是潜在对等体为了建立对等会话而需要彼此交换的信息。以下描述的是这种信息可以如何交换的机制的实施例。

[0059] CDX 服务器 - 在一种实施例中,CDX 服务器是经过认证的多播反射器,它允许被授权的实体交换任意数据。这个数据被称为有效载荷。

[0060] CDX 会话 - CDX 会话指可以经 CDX 服务器彼此通信的一组客户端设备。为作为会话一部分的每个客户端设备指定一张 CDX 票据。每个会话都具有唯一的 CDX 会话 ID,这个 ID 是一个大整数,其可以用于识别或指代个别的会话。

[0061] CDX 请求 - 从客户端设备发送到 CDX 服务器的请求。一个请求通常包括两部分 : CDX 票据与有效载荷。在这种实施例中,有效载荷是利用会话密钥加密的连接数据。

[0062] CDX 响应 - CDX 响应是在一个 CDX 会话中当 CDX 服务器从该 CDX 会话的一个成员接收到 CDX 请求时“反射”回到另一个设备的内容。它是通过把有效载荷附加到给定 CDX 请求中使用的 CDX 票据的 CDX 票据根而构成的。

[0063] CDX 票据 - CDX 票据告诉 CDX 服务器如何向 CDX 会话的成员发送有效载荷。在一种实施例中,它是利用 CDX 票据密钥“签署的”,以防伪造或篡改。如图 3 中所说明的,在一种实施例中,CDX 票据包含以下信息 :

[0064] 会话 ID301,在一种实施例中,其没有被加密或混淆(obfuscate)。

[0065] 会话中参与者的数目 302,在一种实施例中,这没有被加密或混淆。

[0066] 会话中这个票据所指的参与者的索引 303(在一种实施例中,没有被加密或混淆)。

[0067] 到期时间 / 日期 304,在这个时间 / 日期之后,票据被认为是无效的(在一种实施例中,没有被加密或混淆)。

[0068] 用于会话中每个参与者的 CDX 打孔数据 305-306,在一种实施例中,其被利用 CDX 票据密钥加密。

[0069] 利用 CDX 票据密钥的消息认证码 307,这充当“数字签名”来确保票据是可信的。

[0070] CDX 票据根 - CDX 票据的第一部分,除去 CDX 打孔数据与消息认证码。

[0071] 有效载荷 - 这是 CDX 请求和 CDX 响应的第二部分。有效载荷是客户端设备希望在 CDX 会话中传送到其它设备的数据。在这种实施例中,有效载荷是利用会话密钥加密的连接数据。在一种实施例中,CDX 服务器不解密有效载荷,只是保持不变地传递它。

[0072] 会话密钥 - 这是由客户端用于加密连接数据的密钥。在一种实施例中,这个密钥是 CDX 服务器不知道的。在这种实施例中,会话密钥是通过匹配器服务生成的并且连同它们个别的 CDX 票据发送到客户端。

[0073] CDX 票据密钥 - 这是用于创建并“签署”CDX 票据的密钥。CDX 票据密钥只有 CDX 服务器和生成 CDX 票据的服务(如下所述,这可以是匹配器服务和 / 或邀请服务)知道。

[0074] CDX 打孔请求 - 一种具体的 CDX 请求类型,用于从 CDX 服务器获得 CDX 打孔数据。

[0075] CDX 打孔数据 - 这是描述 CDX 服务器如何可以把信息发送到最初请求它的客户端的不透明数据块。它是通过向 CDX 服务器发送 CDX 打孔请求获得的。CDX 打孔数据必须在可以生成 CDX 票据之前在 CDX 会话中从每个客户端设备收集。CDX 打孔数据(有时候称为“NAT 遍历数据”)可以包括发出请求的设备的公共 IP 地址与端口。

[0076] 现在转向图 2a,在一种实施例中,移动设备 A120 和移动设备 B121 可以执行协作应用,诸如需要与一个或多个其它计算设备进行 P2P 连接的多玩家游戏或者协作聊天会话。在 201a,移动设备 A120 向 CDX 服务器 110 发送 CDX 打孔请求。然后,在 202a,CDX 服务器 110 利用 CDX 打孔数据作出响应。在一种实施例中,打孔数据括移动设备 A 的公共 IP 地址

与端口和 / 或打孔通过移动设备 A 的 NAT 所需的任何其它数据(例如,定义移动设备 A 的 NAT 类型的 NAT 类型数据)。类似的事务分别在 201b 和 202b 对移动设备 B 执行。

[0077] 然后,在 203a 和 203b,移动设备 A 和 B 向匹配器服务发送包括 CDX 打孔数据的匹配请求,连同任何的附加的匹配标准(以下描述)。在这个阶段,移动设备 A 和 B 可以开始构造建立 P2P 连接所需的连接数据。例如,这可以(例如,由 NAT 遍历服务)利用诸如标准互联网连接建立(“ICE”)事务的事务来实现。但是,本发明的基本原理不限于用于确定连接数据的任何特定机制。

[0078] 在一种实施例中,一旦匹配器服务 111 已经发现了带匹配标准的一组客户端设备,它就可以生成唯一 CDX 会话 ID、针对 CDX 会话的每个成员的唯一 CDX 票据,及唯一会话密钥。在一种实施例中,匹配器服务 111 可以利用唯一 CDX 票据密钥加密用于 CDX 票据的 CDX 打孔数据。然后,在 204a 和 204b,匹配器服务可以向移动设备 A 和 B 中的每一个发送它们的 CDX 票据和所述会话密钥。

[0079] 移动设备 A 接收 CDX 票据和会话密钥并且利用该会话密钥加密其先前确定的连接数据,产生有效载荷。在一种实施例中,移动设备 A 通过把构造好的有效载荷附加到 CDX 票据来构造 CDX 请求。在 205a,移动设备 A 把 CDX 请求发送到 CDX 服务器 110。移动设备 B 也可以执行相同的操作并且在 205b 把请求发送到 CDX 服务器。

[0080] 在 206a,CDX 服务器 110 接收 CDX 请求,检查票据以便确保它是有效而且可信的(例如,基于消息认证码 307)。如果 CDX 票据是无效的,则请求被丢弃。在一种实施例中,随后 CDX 服务器利用 CDX 票据密钥解密包含在 CDX 票据中的 CDX 打孔数据集。在一种实施例中,CDX 票据密钥可以包括也可以利用票据发送的到期时间 / 日期。CDX 服务 110 与匹配器服务 111 可以存储用于加密 / 解密的两个(或更多个)不同的 CDX 票据密钥 - 第一个是目前有效的而第二个将在到达第一个的到期时间 / 日期的时候变得有效。一接收到票据,CDX 服务 110 就可以读取到期时间 / 日期,以确定使用哪个票据密钥。当一个 CDX 票据密钥已经到期时,CDX 服务 110 和匹配器服务 111 每个都可以生成新的票据密钥(这将是当前票据密钥到期后要使用的下一个密钥)。在一种实施例中,CDX 服务 110 和匹配器服务 111 执行相同的密钥生成算法,以确保与两个票据密钥的一致性。例如,可以使用诸如用于众所周知的 RSA SecurID 认证机制的那些技术之类的技术,其中以固定的间隔生成新的认证代码。在一种实施例中,新的 CDX 票据密钥按天生成。但是,本发明的基本原理不限于用于生成 CDX 票据密钥的任何特定机制。

[0081] 相同的操作可以像所示出的那样在 206b 对移动设备 B 执行。CDX 服务器从 CDX 请求构造 CDX 响应,然后使用 CDX 打孔数据把 CDX 响应发送到 CDX 会话中的参与者(在 207a 发送到移动设备 B 并且在 207b 发送到移动设备 A)。

[0082] 移动设备 B 从 CDX 服务器接收 CDX 响应 207a。客户端设备 B 检查 CDX 票据根,以确保会话 ID 匹配它自己 CDX 票据的会话 ID。然后,移动设备 B 可以利用该会话密钥解密有效载荷,产生来自移动设备 A 的连接数据。然后,移动设备 B 使用来自移动设备 A 的连接数据来开始建立 P2P 会话的过程。在一种实施例中,这些涉及标准的 ICE 事务。但是,本发明的基本原理不限于用于建立 P2P 通信的任何特定机制。

[0083] 如以上所提到的,在一种实施例中,移动设备 A 和 B 建立与匹配器服务 111 通信的超本文传输协议安全(“HTTPS”)会话(例如,利用 HTTPS 请求 / 响应事务)并且建立与 CDX

服务通信的 UDP 套接字。匹配请求 204a、204b 可以包括先前为每个对应移动设备确定的 NAT 类型和打孔数据(例如,公共 IP 地址与端口)。在涉及多玩家游戏的一种实施例中,每个匹配请求可以识别每个移动设备上的玩家(例如,利用唯一玩家 ID 码)、每个玩家想玩的游戏、参与游戏的玩家数目和 / 或与期望的游戏关联的其它游戏配置变量。作为例子但不是限制,与游戏关联的游戏配置变量可以包括难度级别(例如,容易、普通、困难)、用户的年龄(例如,“低于 13 岁”)、游戏的子区(例如,“第二关”)和 / 或玩家的经验级别(例如,专家、初级玩家、中级玩家)。如以下具体描述的,这些变量有时候称为游戏“桶”(bucket)而且利用唯一的“桶 ID”来识别。每个游戏可以包括不同的桶 ID 设置,以便识别不同的游戏配置变量。

[0084] 在一种实施例中,移动设备 B 在 208a 和 209a 发送确认。类似地,移动设备 A 的确认是在 208b 和 209b 发送的。如果移动设备 A 或 B 的确认在规定的时段之后没有收到,则连接数据 207a 可以重新发送到移动设备 B212。或者 CDX 服务 110 可以启动重试和 / 或移动设备 A120 可以启动重试。

[0085] 图 2b 说明了一个更具体的例子,其中三个不同的移动设备 120-122 利用 CDX 服务和匹配器服务 111 协商 P2P 连接。图 2b 还说明了由移动设备 120-122 用于建立连接的两个附加服务:用于确定 NAT 类型的 NAT 遍历服务 291 和用于为每个移动设备确定完全连接数据的 NAT 遍历服务 290 (例如,利用 ICE 连接数据事务)。但是,应当指出,单独的服务不是为了遵循本发明的基本原理所必需的。例如,在一种备用实施例中,由这些服务 290-291 中每个执行的 NAT 遍历功能可以直接集成在 CDX 服务 110 和 / 或匹配器服务 111 中。类似地,NAT 遍历服务 290-291 都执行的功能可以集成在单个 NAT 遍历服务中。概括地说,图 2b 中所示的具体功能分离不是为了遵循本发明的基本原理所必需的。

[0086] 现在转向图 2b 的具体细节,在 220,移动设备 A 向 NAT 遍历服务 291 发送 NAT 类型请求。作为响应,NAT 遍历服务 291 可以使用各种已知的技术,包括实现一系列事务,来确定移动设备 A 所使用的 NAT 类型。例如,NAT 遍历服务 291 可以尝试打开移动设备 A 的 NAT 上的不同 IP 地址与端口,并且利用不同的 IP/ 端口组合通过那些端口与移动设备 A 通信。以这种方式,移动设备 A 所采用的 NAT 可以归类为上述 NAT 类型中的一种(例如,完全圆锥形、受限锥形、端口受限锥形、对称)或者备用的 NAT 类型。然后,这种信息可以提供给移动设备 A120,如所说明的。

[0087] 在 221,移动设备 A120 利用 CDX 服务 110 启动 NAT 遍历请求。作为响应,CDX 服务 110 可以读取用于该请求的公共 IP 地址与公共端口号并且把这种信息发送回移动设备 A120。如上所述,如果设备在 NAT 的后面,则其公共端口和 IP 地址将分别与其私有端口和 IP 地址不同。因而,依赖于所使用的 NAT 的类型,公共 IP 地址与端口可以用于“打孔”通过 NAT 设备,到达移动设备。

[0088] 在 222,移动设备 A120 向匹配器服务 111 发送匹配请求 222。如上所述,在一种实施例中,移动设备 A 利用超文本传输协议安全(“HTTPS”)会话向匹配器服务 111 传送(例如,利用 HTTPS 请求 / 响应事务)。匹配请求可以包括先前为移动设备 A120 确定的 NAT 类型与打孔数据(例如,公共 IP 地址与端口)。在涉及多玩家游戏的一种实施例中,匹配请求可以识别移动设备 A 上的玩家(例如,利用唯一玩家 ID 码)、用户想玩的游戏、参与游戏的玩家的数目和 / 或与期望的游戏关联的其它游戏配置变量(如前面关于图 2a 描述过的)。

[0089] 在 223-225, 为移动设备 B121 执行对应于事务 220-222 的一组事务, 并且在 226-228, 为移动设备 C122 执行对应于事务 220-222 的一组事务。因而, 在事务 228 之后, 匹配器服务 111 已经接收到用于全部三个移动设备 120-122 的匹配请求。在这个具体的例子中, 匹配请求导致移动设备 120-122 对于特定的协作会话而匹配, 特定的协作会话诸如是多玩家游戏(例如, 这些移动设备的用户可能已经选择了具有相同或相似变量设置的相同游戏, 由此导致匹配器服务 111 的匹配)。

[0090] 匹配器服务 111 使用包含在每个匹配请求中的数据来生成票据 A, 在 229 它把票据 A 发送到移动设备 A; 生成票据 B, 在 230 它把票据 B 发送到移动设备 B; 并且生成票据 C, 在 231 它把票据 C 发送到移动设备 C。虽然没有在图 2b 中示出, 但是匹配器服务 111 可以利用推送通知服务分别把票据 A、B 和 C 推送到移动设备 A、B 和 C (例如, 像图 11-12 中所说明的推送通知服务 1050)。用于票据 A、B 和 C 的票据数据结构的一种实施例在以上关于图 3 进行了描述。

[0091] 在 232, 移动设备 A120 与 NAT 遍历服务 290 通信, 以确定其自己的连接数据。在一种实施例中, 这可以包括标准的 ICE 连接数据事务。如前面所提到的, 连接数据可以包括用于移动设备 A120 的公共 / 私有 IP 地址、端口和 NAT 类型。

[0092] 移动设备 A120 把它的连接数据附加到票据 A 并且在 233 把带连接数据的票据 A 发送到 CDX 服务 110。在一种实施例中, CDX 服务 110 如上所述地处理票据 A 并且在 234 把(可能加密的)连接数据发送到移动设备 B121 和移动设备 C122。对于这些事务, CDX 服务 110 可以利用与票据 A 一起包括的用于移动设备 B 和 C 的 NAT 遍历数据。

[0093] 在 236-238, 利用票据 B 执行对应于事务 232-234 的一组事务并且在 238-240 为票据 C 执行对应于事务 232-234 的一组事务。因而, 在事务 240 之后, 连接数据已经在移动设备 120-122 中每个之间共享。利用连接数据, P2P 会话在移动设备 A 和 B、移动设备 A 和 C 及移动设备 B 和 C 之间建立。

[0094] 如图 2c 中所说明的, 邀请服务 112 也可以与 CDX 服务 110 一起使用(代替匹配器服务 111 或者作为其补充)。在一种实施例中, 邀请服务 112 处理用于与具体移动设备和 / 或用户的 P2P 连接的邀请请求。邀请服务 112 可以实现为无状态服务(即, 不附带(tack)每个无线设备之间事务的当前状态的服务)。

[0095] 转向这个特定的例子, 在 250, 移动设备 A120 向 NAT 遍历服务 291 发送 NAT 类型请求。作为响应, NAT 遍历服务 291 可以使用各种已知的技术来确定移动设备 A 所使用的 NAT 类型(其中有些在上面描述过了)。在 251, 移动设备 A120 对 CDX 服务 110 启动 NAT 遍历请求。作为响应, CDX 服务 110 可以读取用于该请求的公共 IP 地址与公共端口号并且把这个信息发送回移动设备 A120。如上所述, 如果一个设备在 NAT 后面, 则其公共端口与 IP 地址将分别与其私有端口和 IP 地址不同。因而, 依赖于所使用的 NAT 类型, 公共 IP 地址与端口可以用于“打孔”通过 NAT 设备, 以到达移动设备。

[0096] 就像对于匹配器服务, 在一种实施例中, 每个移动设备都利用超文本传输协议安全(“HTTPS”)会话与邀请服务 112 通信(例如, 利用 HTTPS 请求 / 响应事务)。

[0097] 在 252, 移动设备 A120 把邀请请求发送到邀请服务 112, 这个请求包括移动设备 A 的 NAT 遍历数据(例如, NAT 类型、公共 IP 地址 / 端口)。在使用推送通知服务(以下更具体地描述)的实施例中, 邀请请求还可以包括移动设备 A 的推送令牌。邀请请求 252 还可以包

括识别一个或多个其它用户 / 设备 - 在这个例子中,是移动设备 B121 和 C122 的用户 - 的识别码。可以使用各种不同的识别码类型。例如,在多玩家游戏的情况下,识别码可以包括特定于游戏的玩家 ID 码。在音频 / 视频聊天会话的情况下,识别码可以包括从移动设备 A 用户的“伙伴”列表的用户中识别一个或多个用户的电话号码或者唯一 ID 码。

[0098] 在一种实施例中,邀请服务 112 从邀请请求读取识别码并且在注册数据库(未示出)中执行查找,以便定位移动设备 B 和 C 中的每一个。在一种特定的实施例中,移动设备 B 和 C 中的每一个先前都注册了从邀请服务 112 接收推送通知的推送服务。因而,在这种实施例中,邀请服务 112 分别在 253 和 254 使用推送通知服务把邀请请求推送到移动设备 B121 和移动设备 C122。关于推送通知服务的附加细节在下面(见例如图 11-12 和关联的文字)和以上引用的推送通知应用中描述。

[0099] 在一种实施例中,邀请请求 253 和 254 包括图 3 中说明并且在以上参考图 2a-2b 描述过的票据数据结构。具体而言,发送到移动设备 B 的票据包括识别移动设备 A 和 B 的加密列表而且发送到移动设备 C 的票据包括识别移动设备 A 和 C 的加密列表。在一种实施例中,因为邀请服务 112 可能还没有移动设备 B 的 NAT 遍历数据,所以在 253 “票据”可以包括识别移动设备 B 的其它信息。例如,如以下关于使用中继服务和推送通知服务(见例如图 11-12)的实施例所阐述的,在 253 “票据”可以包括用于移动设备 A 的 NAT 遍历数据、设备 A 的 ID 码、设备 A 的推送令牌、设备 B 的 ID 码及用于移动设备 B 的推送令牌。在 254 可以为移动设备 A 和 C 提供相同类型的信息。

[0100] 在 255,移动设备 B 可以与 NAT 遍历服务 291 通信,以便确定其 NAT 类型并且,在 256,移动设备 B 可以与 CNX 服务 110 通信,以确定其 NAT 遍历数据(例如,公共 IP 地址 / 端口)。在 257,移动设备 B 向邀请服务 112 发送邀请响应,该邀请响应包含移动设备 A 的和移动设备 B 的识别码、NAT 遍历数据及,如果使用推送通知服务的话,用于移动设备 A 和 B 的推送令牌。在 258,移动设备 B 可以通过与 NAT 遍历服务 290 通信检索其当前的连接数据。在 259,移动设备 B 把带其当前连接数据的票据(票据 B)发送到 CDX 服务 110。作为响应,CDX 服务 110 如上所述地处理票据并且把连接数据转发到移动设备 A120。

[0101] 接收到移动设备 B 的邀请响应,邀请服务 112 可以为移动设备 A 生成加密的票据并且在 260 把票据发送到移动设备 A。在一种实施例中,票据包括用于移动设备 A 和 B 的 NAT 遍历数据、NAT 类型和推送令牌(如果使用推送通知服务的话)。关于图 2c 描述的“票据”可以与关于匹配器服务 111 描述的“票据”的数据结构相同或不同。例如,不是如上所述地生成加密的“票据”,邀请服务 112 可以简单地生成唯一会话 ID,以便识别与每个移动设备的邀请会话。

[0102] 在 261,移动设备 A 通过与 NAT 遍历服务 290 通信来检索其当前的连接数据。然后,移动设备 A 可以把其连接数据附加到票据并且在 262 把带有其连接数据的票据发送到 CDX 服务 110。CDX 服务 110 如上所述地处理票据并且把移动设备 A 的连接数据转发到移动设备 B。最后,在 263,移动设备 A 和 B 使用交换后的连接数据打开直接 P2P 连接。如下所述,在移动设备 A 和 B 的 NAT 类型不兼容的情况下,中继服务可以用于启用移动设备 A 与 B 之间的通信。

[0103] 在 264-272,移动设备 C122 与移动设备 A 可以执行一系列事务,以便为移动设备 B 和 A 建立如在 255-263 所描述的 P2P 连接。具体而言,在 264,移动设备 C122 与 NAT 遍历服

务 291 通信,以确定其 NAT 类型,并且在 265 与 CDX 服务 110 通信,以确定其 NAT 遍历数据(例如,公共 IP 地址 / 端口)。在 266,移动设备 C 发送包含移动设备 C 和移动设备 A 的 NAT 类型、NAT 遍历数据和推送令牌(如果使用推送通知服务的话)的邀请响应。在 267,移动设备 C 通过 NAT 遍历 P2P 服务 290 检索其当前的连接数据并且在 268 移动设备 C 把其连接数据附加到票据 C 并且把票据 C 发送到 CDX 服务 110。CDX 服务 110 如上所述地处理票据并且把移动设备 C 的连接数据转发到移动设备 A120。

[0104] 在 269,移动设备 A120 从邀请服务 112 接收移动设备 C 的邀请响应,该响应包括移动设备 A 和 C 的 NAT 类型、NAT 遍历数据和推送令牌(如果使用推送服务的话)。在 270,移动设备 A 从 NAT 遍历服务 290 检索其当前的连接数据、把其当前的连接数据附加到票据 A 并且在 271 把票据 A 发送到 CDX 服务 110。作为替代,事务 270 可能是不需要的,因为移动设备在事务 261 确定其连接数据。CDX 服务器 110 如上所述地处理票据 A 并且把移动设备 A 的连接数据转发到移动设备 C。最后,在 272,移动设备 A 和 C 使用交换后的连接数据建立直接的 P2P 连接 272。

[0105] 在一种实施例中,邀请服务 112 和匹配器服务 111 可以依赖推送通知服务(未示出)把数据推送到移动设备。例如,在图 2c 中,邀请请求 253 和 254 可以经推送通知服务被推送到移动设备 B121 和 C122。类似地,在图 2a 中,票据 A 和 B 可以被推送到移动设备 A120 和 B121。在一种实施例中,当移动设备在网络上被激活时,它可以在由推送通知服务访问的中心注册目录中注册其推送令牌。在一种实施例中,注册目录把受密码保护的用户 ID 或电话号码与推送令牌关联。如果推送令牌可以在目录中识别,则推送通知服务可以使用该推送令牌把推送通知发送到移动设备。在一种实施例中,推送通知服务是由本申请受让人设计并且在例如以上引用的推送通知应用中描述的 Apple 推送通知服务(“APNS”)。但是,应当指出,推送通知服务器不是图 2a-c 中所示本发明的实施例所要求的。例如,推送通知不是 CDX 服务 110 执行本文所述操作所要求的。

[0106] 图 4 说明了可以由 CDX 服务 110 实现以便交换连接数据的方法,而图 5 说明了可以由移动设备实现以便交换连接数据并且建立 P2P 连接的方法。这些方法的某些方面已经在上面关于图 1-2c 描述过了。特别地,这些方法可以在图 1-2c 所示网络体系结构的背景下实现,但是它们不限于这种体系结构。在一种实施例中,这些方法在程序代码中体现,程序代码当被处理器执行时,使得该方法的操作得以执行。在被处理器执行的同时,程序代码可以存储在机器可读介质中,诸如随机存取存储器(“RAM”)。处理器可以是通用处理器(例如, **Intel® Core™** 处理器)或者专用处理器。但是,这些方法可以利用硬件、软件和固件的任意组合实现。此外,程序代码可以存储在诸如硬盘驱动器、光盘(例如,数字视频盘或致密盘)之类的非易失性存储设备或者诸如闪存存储器设备的非易失性存储器上。

[0107] 现在转向图 4 中所示的方法,在 401,为特定的移动设备 - 在这个例子中是“移动设备 A” - 接收 NAT 遍历请求(有时候也称为“打孔”请求)。在 402,生成 NAT 遍历响应并且发送到移动设备 A。在一种实施例中,生成 NAT 遍历响应可以包括确定移动设备 A 的当前公共 IP 地址 / 端口和 / 或 NAT 类型。

[0108] 用于移动设备 A 的票据可以随后生成并且由诸如如上所述的匹配器服务 111 或邀请服务 112 之类的票据生成实体加密。在 403,接收为移动设备 A 生成的票据(“票据 A”),该票据包括(用于设备 A 和一个或多个其它设备的)NAT 遍历数据及用于设备 A 的连接数据。

在 404, 利用消息认证码认证票据并且利用与票据生成实体加密票据所使用的密钥相同的 CDX 票据密钥来解密打孔数据。如以上所提到的, 在一种实施例中, 正确的 CDX 票据密钥是利用与该 CDX 票据密钥关联的到期时间 / 日期识别的。

[0109] 在 405, 提取用于移动设备的 NAT 遍历数据。在 406, 用于移动设备 A 的连接数据利用 NAT 遍历数据发送到每个对等体。在 407, 从每个对等体接收确认。如果在 408 确定还没有从所有对等体接收到确认, 则在 409 移动设备 A 的连接数据重新发送到那些还没有响应的对等体。当在 408 确定所有连接数据都确认之后, 该方法终止。

[0110] 在一种实施例中, 图 4 中所示的方法可以对 P2P 事务中所涉及的每个对等体执行, 以确保每个对等体都接收到建立 P2P 连接所需的连接数据。

[0111] 图 5 说明了根据本文所述本发明的实施例的可以由移动设备执行的方法。在 501, 发送 NAT 遍历请求并且, 在 502, 接收 NAT 遍历响应。如前面所描述的, 响应中所包含的 NAT 遍历数据可以包括发出请求的设备的公共端口 / IP 地址。在 503, 发送包含 NAT 遍历数据的匹配请求。用于移动设备的票据可以随后生成并且由诸如上述匹配器服务 111 或邀请服务 112 之类的票据生成实体生成。作为上述票据数据结构的一种备选, 匹配器服务 111 和 / 或邀请服务 112 可以简单地利用唯一会话 ID 识别每个参与者。

[0112] 在 504, 可以接收票据; 在 505, 用于移动设备的连接数据附加到票据; 而且, 在 506, 发送带连接数据的票据。在 507, 接收建立与一个或多个其它对等体的 P2P 连接所需的连接数据。在 508, 接收指示一个或多个其它无线设备已经接收到在 506 发送的连接数据的确认。如果那时候还没有接收到所有的确认, 则在 510, 连接数据重新发送到那些还没有从其接收到确认的移动设备。如果在 509 确定接收到了所有确认, 则在 507 接收到的连接数据用于建立与其它移动设备的 P2P 会话。

[0113] 建立并利用备用通信信道的装置与方法

[0114] 目前的移动设备能够经多种不同的通信信道通信。例如, Apple iPhoneTM 能够经 Wi-Fi 网络(例如, 802.11b、802.11g、802.11n 网络); 3G 网络(例如, 通用移动电信系统 (“UMTS”) 网络、高速上行链路分组接入 (“HSUPA”) 网络等); 及蓝牙网络(称为个人区域网络 (“PAN”)) 通信。未来的移动设备将能够经另外的通信信道通信, 诸如 WiMAX、高级国际移动电信 (“IMT”) 和高级长期演进 (“LTE”), 这仅仅是一些例子。

[0115] 在操作中, 目前的移动设备从一组可用信道中选择一个主要的通信信道。例如, 如果 Wi-Fi 可用的话, 移动设备常常配置成选择 Wi-Fi 连接, 而且如果 Wi-Fi 不可用的话就选择蜂窝数据连接(例如, UMTS 连接)。

[0116] 在本发明的一种实施例中, 一组移动设备最初利用标准的 ICE 连接数据交换和 / 或利用上述连接数据交换技术来建立主要的对等 (“P2P”) 通信信道。然后, 移动设备可以经主要信道交换连接数据, 以便建立一个或多个次要通信信道, 这些次要通信信道用作当任意主要信道发生故障时的备用信道。在一种实施例中, 通过经这些信道周期性地发送“心跳”分组, 次要通信信道通过 NAT 防火墙维持打开。

[0117] 如本文所使用的, 通信 “信道” 指两个移动设备之间的全网络路径, 而通信 “链路” 指通信路径中所使用的一个特定连接。例如, 如果设备 A 利用 Wi-Fi 连接连接到互联网而设备 B 利用 3G 连接连接到互联网, 则设备 A 与设备 B 之间的“信道” 由 Wi-Fi 链路与 3G 链路二者共同来定义; 设备 A 具有 Wi-Fi 通信 “链路”, 而设备 B 具有 3G 通信 “链路”。因此,

如果设备 A 从 Wi-Fi 链路切换到 3G 链路，则设备 A 与设备 B 之间的“信道”改变，虽然设备 B 的 3G 链路的事实保持相同。

[0118] 现在将关于图 6 描述其中移动设备建立主要和次要通信信道的具体例子。但是，应当指出，本发明的基本原理不限于图 6 中所示的通信链路与通信信道的特定设置。

[0119] 在图 6 中，移动设备 A601 能够利用 NAT 设备 611 经通信链路 605 并且利用 NAT 设备 612 经通信链路 606 连接到网络 610（例如，互联网）。类似地，设备 C603 能够利用 NAT 设备 613 经通信链路 609 并且利用 NAT 设备 614 经通信链路 610 连接到网络 610（例如，互联网）。作为例子但不是限制，通信链路 605 与 609 可以是 3G 通信链路，而通信链路 606 与 610 可以是 Wi-Fi 通信链路。

[0120] 因此，在这个例子中，在移动设备 A 与移动设备 B 之间可以建立四种不同的通信信道：使用链路 605 和 609 的第一信道；使用链路 605 和 610 的第二信道；使用链路 606 和 609 的第三信道；及使用链路 606 和 610 的第四信道。在一种实施例中，移动设备 A 和 B 将基于优先化方案选择这些信道中的一个作为主要通信信道，并且将选择剩余的三个信道作为备用通信信道。例如，一个优先化方案可以是选择具有最高带宽的信道作为主要信道并且使用剩余的信道作为次要信道。如果两个或多个信道具有可比的带宽，则优先化方案可以包括选择最不贵的信道（假设用户要为使用一个或多个信道付费）。作为替代，优先化方案可以是选择最不贵的信道作为主要信道而且，如果每个信道的成本相同的话，就选择最高带宽的信道。在仍然遵循本发明基本原理的同时，可以实现各种不同的优先化方案。

[0121] 移动设备 A601 和 C603 可以利用上述技术来建立主要通信信道（例如，通过经 CDX 服务 110 交换连接数据）。作为替代，移动设备 601、603 可以实现标准互联网连接建立（“ICE”）事务，以交换连接数据。不管主要信道是怎么建立的，一旦它成了主要信道，移动设备 A601 和 C603 就可以经该主要通信信道交换用于次要通信信道的连接数据。例如，如果图 6 中的主要通信信道包括通信链路 606 和通信链路 609，则这个连接一旦建立之后就可以用于交换用于次要通信信道的连接数据，其中次要通信信道包括通信链路 605 和 609。在这个例子中，经主要通信信道交换的连接数据可以包括用于 NAT611 和 NAT613 的 NAT 遍历数据与 NAT 类型数据，包括用于每个移动设备的公共和私有 IP 地址 / 端口。

[0122] 一旦次要通信信道已经建立，它们就利用心跳分组保持打开。例如，设备 A 可以周期性地向设备 C 发送小的“心跳”分组和 / 或设备 C 可以周期性地向设备 A 发送小的“心跳”分组，以确保用于次要信道的 NAT 端口保持打开（NAT 将常常由于不活动性而关闭端口）。心跳分组可以是无有效载荷的 UDP 分组，虽然本发明的基本原理不限于任何特定的分组格式。心跳分组可以是在其有效载荷首部中具有自识别类型字段的 UDP 分组，而且可以包含可选的附加格式化信息，包括但不限于信道生存时间值。

[0123] 如图 7 中所说明的，每个移动设备 601 都存储并维护一个包含主要和次要通信信道的列表的数据结构 710（例如，表、文本文件、数据库等）。为每个通信信道提供单独的条目并且条目包括利用那个信道所需的连接数据（例如，私有 / 公共 IP 地址、NAT 类型，等等）和那个信道的当前状态（例如，主要、次要 1、次要 2，等等）。

[0124] 在一种实施例中，通信接口 701 和 702 分别用于经通信链路 605 和通信链路 606 通信。故障检测模块 705 可以在移动设备 601 上执行，以便检测何时特定的通信接口 / 链路故障或者降级到低于规定的阈值。作为响应，链路管理模块 706 可以读取主要 / 次要连

接数据 710,以便把具有次最高优先级的次要信道提升成主要信道。次要信道的优先化可以利用与以上对主要信道讨论过的相同原理来实现(例如,基于带宽、成本、可靠性等)。一旦已经选择了次要信道,链路管理模块 706 就可以向其它移动设备上的链路管理模块发送链路故障指示,通知那些设备把次要通信信道提升成主要通信信道。然后,那些设备将利用与选定的主要信道关联的连接数据。

[0125] 在一种实施例中,主要通信信道的完全“故障”不是强迫切换到一个次要通信信道所必需的。例如,在一种实施例中,如果主要通信信道劣化足够多(例如,低于特定的带宽、比特速率或者可靠性阈值),则改变到次要信道可以如本文所述的那样实现。在一种实施例中,只有当次要信道能够支持比当前主要信道更好的性能(例如,带宽、比特速率或可靠性)时,才执行到次要信道的切换。

[0126] 图 8a 说明了与图 6 中所示相同的网络配置,添加了直接连接到网络 610 并且通过专用网络连接 620 连接到设备 C603 的移动设备 B602。专用网络 620 可以是设备 B602 与设备 C603 之间的蓝牙 PAN 连接。从这个例子可以看到,从主要信道切换到次要信道可能显著改变网络拓扑。例如,如图 8b 中所示,如果用于移动设备的主要信道 801 包括通信链路 609 (导致设备 A、B 与 C 之间的直接连接)而且次要信道包括专用网络 620,则网络拓扑可以如图 8c 中所说明的那样改变,因为设备 A 和设备 C 利用该专用网络通信的唯一途径是通过设备 B。虽然这是只具有三个设备的简化例子,但是可以使用显著更大量的设备,从而当在主要与次要通信信道之间切换时导致非常不同的网络拓扑配置。

[0127] 用于建立和维护次要信道的方法的一种实施例在图 9 中说明。在一种实施例中,该方法可以由每个移动设备上的链路管理模块 706 执行。但是,该方法不限于任何特定的设备配置。

[0128] 在 901,选择主要 P2P 通信信道。如以上所提到的,主要信道可以基于预定义的优先化方案来选择。例如,某些通信信道类型可以比其它通信信道类型优先。信道还可以基于诸如带宽、使用成本和 / 或可靠性的变量来优先化。

[0129] 在 902,建立备用 P2P 通信信道。在一种实施例中,这是通过经主要通信信道在所有移动设备之间共享连接数据来实现的。在 903,维护备用信道。在一种实施例中,这涉及经次要通信信道周期性地发送数据(例如,以周期性心跳分组的形式)。

[0130] 在 904,如果主要 P2P 信道发生故障(例如,因为特定移动设备的通信链路失败或者移动设备移出通信链路的范围),则在 905,移动设备把最高优先级的备用信道提升成主要信道。在一种实施例中,这涉及具有故障链路的移动设备经次要信道向其它设备发送其链路故障的通知。最后,在 906,使备用信道成为主要信道,而且过程返回到 902 (其中,任何附加的备用信道都被发现并添加到优先化方案)。

[0131] 为邀请服务建立对等(P2P)通信信道的装置与方法

[0132] 如图 10 中所说明的,除了 CDX 服务 110,匹配器服务 111 和邀请服务 112 (其有些实施例在上面描述了),本发明的一种实施例还可以包括注册 / 目录服务 1052、推送通知服务 1050 和中继服务 1051。如以上所提到的,在一种实施例中,邀请服务 112 和 / 或匹配器服务 111 可以使用注册 / 目录服务 1052 识别所注册的移动设备并使用推送通知服务 1050 把数据推送到移动设备。在一种实施例中,当移动设备在网络上被激活时,通过关联推送令牌与受密码保护的用户 ID 或电话号码,它向由注册 / 目录服务 1052 维护的数据库注册“推

送令牌”(在推送通知应用中有时候称为“通知服务帐号标识符”)。如果推送令牌在注册目录中被识别出来(例如,通过利用用户 ID 执行查询),则推送通知服务 1050 可以使用该推送令牌把推送通知发送到移动设备。在一种实施例中,推送通知服务是由本申请受让人设计并且在例如以上引用的推送通知应用中描述的 Apple 推送通知服务(“APNS”)。

[0133] 图 11 说明了本发明的一种实施例,其中推送通知服务 1051 用于在两个移动设备之间建立直接 P2P 连接,而图 12 说明了用于通过中继服务 1051 建立 P2P 连接的实施例。如以下所描述的,关于是否使用中继服务 1051 建立 P2P 连接的决定可以基于在移动设备之间建立直接 P2P 连接的可行性(例如,基于 NAT 兼容性问题)。

[0134] 现在转向图 11,在 1101,移动设备 A120 发送邀请移动设备 B121 进入 P2P 通信会话(例如,协作视频游戏、P2P 视频聊天等)的邀请。在一种实施例中,邀请包括在特定在线应用的背景下识别移动设备 B121(和 / 或移动设备 B 的用户)的用户 ID。例如,用户 ID 码可以是用于特定多玩家 P2P 游戏的玩家 ID,而且可以采用例如通用唯一标识符(UUID)的形式。作为替代,在有些实施例中,ID 码可以是移动设备 B121 的电话号码。游戏 ID 码可以用于识别移动设备 A 邀请移动设备 B 加入的多玩家游戏。桶 ID 可以用于识别用于那个游戏的配置(如本文关于匹配器服务所描述过的)。

[0135] 邀请 1101 还可以包括识别移动设备 A120 的 ID 码和与移动设备 A 关联的 NAT 遍历 / 连接数据(例如,用于移动设备 A 的公共 / 私有 IP 地址与端口和用于设备 A 的 NAT 设备的 NAT 类型)。NAT 遍历 / 连接数据或 NAT 类型数据可以先前已经在邀请请求 1101 之前由移动设备 A 确定了(例如,经 NAT 遍历、NAT 类型与连接数据事务,诸如在以上关于图 2a-2c 所讨论过的那些)。如前面所提到的,邀请请求 1101 可以采用 HTTPS 请求的形式。此外,为了附加的安全性,邀请请求 1101 可以包括由预先规定的证书机构签署的客户端证书。

[0136] 不管用于识别移动设备 B 的 ID 码的特定类型,该 ID 码是由邀请服务 112 接收的并且,在 1102,邀请服务 112 可以在目录服务 1052(在图 11 中未示出)中执行查找,以便识别通知服务帐号标识符,诸如用于把通知推送到移动设备 B 的推送令牌(“推送令牌 B”)。在一种实施例中,查找操作可以执行几种检查,以确定邀请是否应当被允许。首先,它可以确认用于移动设备 A 的标识码(“ID-A”)和设备 A 的推送令牌(“推送令牌 -A”)是目录服务数据库中注册的关联。查找操作 1102 还可以确认移动设备 A 的用户被允许邀请移动设备 B 的用户(例如,移动设备 B 的用户可以规定只有注册为 B 的朋友的那些其他用户才能邀请用户 B;或者可以规定不允许邀请)。在一种实施例中,如果任何这些检查都失败,则取消邀请,而且邀请服务 112 向移动设备 B 返回错误。

[0137] 虽然在这种实施例中描述了“推送令牌”,但是应当指出,本发明的基本原理不限于将“推送令牌”或者任何其它特定数据结构用于认证和把通知推送到移动设备。

[0138] 在一种实施例中,在识别出推送令牌之后,邀请服务 112 可以生成指定给邀请会话并且在所有进一步事务中用于识别会话的安全的、一次性“会话令牌”。然后,该会话令牌的拷贝发送回移动设备 A120 并且和邀请请求一起发送到移动设备 B。在一种实施例中,会话令牌与上述票据数据结构一起使用,而在另一种实施例中,只使用会话令牌。

[0139] 在 1103,邀请服务 112 向推送通知服务 1050 发送推送请求。在一种实施例中,推送请求可以包括用于移动设备 A 的 NAT 遍历数据、设备 A 的 ID 码、推送令牌 A、设备 B 的 ID 码和推送令牌 B。在一种实施例中,这种信息可以在“票据”数据结构中打包并且加密,如上

所述。在另一种实施例中，数据简单地和邀请会话 ID 一起发送。

[0140] 因为在这个例子中移动设备 B121 注册了推送通知服务 1050，所以在 1104 推送通知服务 1050 能够定位邀请请求并把它推送到移动设备 B121。被推送的邀请 1104 可以包括会话令牌、移动设备 A 的 NAT 遍历数据 / 连接数据和移动设备 B 的 ID 码。响应于该邀请请求，移动设备 B 可以通过如上所述调用 NAT 遍历服务或 CDX 服务 110 来确定其联网信息(例如，NAT 遍历 / 连接数据、NAT 类型等)。

[0141] 在 1105，移动设备 B 接受邀请。接受 1105 可以采用对邀请服务 112 的 HTTPS 调用的形式而且可以包括由预先规定的证书机构签署的客户端证书(以上关于邀请请求所提到的)。在一种实施例中，接受 1105 可以包括用于移动设备 A 和 B 的 ID 码和用于移动设备 A 和 B 的 NAT 遍历 / 连接数据和 / 或 NAT 类型。接受 1105 还可以包括用于移动设备 A 和 B 的推送令牌和 / 或会话令牌。在一种实施例中，接受 1105 还可以包含关于它是否是来自前面失败的直接连接尝试的重试的指示。但是，在另一种实施例中，接受 1105 不包含重试指示。相反，一检测到失败的 P2P 连接尝试，两个移动设备中的一个就可以向邀请服务 112 发送特定的“中继邀请”。作为响应，服务可以直接启动以下关于图 12 所述的中继事务序列(在 1201 开始)。

[0142] 在 1106，邀请服务 112 可以执行兼容性检查，以确定移动设备 A 与 B 之间的直接 P2P 连接是否可行。例如，在一种实施例中，如果从移动设备 B 接收到的接受 1105 指示它是来自一次前面失败的直接连接尝试的重试(或者规定次数的前面失败的直接连接尝试的重试)，则邀请服务可以得出直接 P2P 连接不可行的结论。邀请服务 112 可以比较用于移动设备 A 与 B 的 NAT 类型数据，以确定移动设备 A 与 B 的 NAT 设备是否将支持直接 P2P 连接。已知 NAT 类型的某些组合是与建立 P2P 连接不兼容的。例如，除闭合 / 防火墙 NAT 外，完全圆锥形 NAT 可以与任何其它 NAT 类型一起用于建立直接 P2P 连接。作为对比，对称 NAT 只能与完全圆锥形 NAT 一起用于建立直接 P2P 连接。在本发明一种实施例中组合各种 NAT 类型的可行性在图 14 中所示的 NAT 兼容性表 1400 中阐述，其中列代表一个移动设备(例如，移动设备 A)的 NAT 类型，而行代表另一个移动设备(例如，移动设备 B)的 NAT 类型。单元格中的“1.0”指示所关联的行与列中的 NAT 类型是兼容的，而“0.0”指示 NAT 类型是不兼容的。

[0143] 在一种实施例中，如果兼容性检查 1106 确定直接 P2P 是不可行的，则邀请服务 112 可以如以下关于图 12 所描述的那样发送中继查找请求 1201。但是，如果兼容性检查 1106 确定直接 P2P 连是可行的，则邀请服务 112 可以把推送请求 1107 发送到推送通知服务 1050，该请求包含移动设备 B 对移动设备 A 的邀请的接受。推送请求 1107 和从推送通知服务 1050 到移动设备 A 的后续推送通信 1108 可以包括会话令牌及移动设备 A 和 B 二者的推送令牌、ID 码和 / 或 NAT 遍历 / 连接数据。在一种实施例中，这种信息可以在上述“票据”数据结构中打包(见例如图 2a-2c 和关联的文字)而且可以利用唯一的密钥加密。作为替代，这种信息可以简单地与唯一邀请会话 ID 一起发送。邀请服务 1050 还可以通知移动设备 B 将尝试直接连接。

[0144] 在这个阶段，移动设备 A 和 B 具有足够的信息来建立直接 P2P 连接。在一种实施例中，这是利用上述 CDX 服务 110 实现的。例如，移动设备 B 把其连接数据附加到票据 B 而且，在 1109，把(带连接数据的)票据 B 发送到 CDX 服务。就在这个事务之前，移动设备 B 可

以实现例如图 2b 中所示事务 235 的事务,以确保其连接数据是当前的。然后,CDX 服务 110 认证票据(例如,利用如上所述的唯一会话密钥)、提取移动设备 B 的连接数据并且在 1110 把该连接数据转发到移动设备 A。类似地,移动设备 A 把其连接数据附加到票据 A 并且,在 1111,把(带连接数据的)票据 A 发送到 CDX 服务 110。就在这个事务之前,移动设备 A 可以实现例如图 2b 中所示事务 232 的事务,以确保其连接数据是当前的。然后,CDX 服务 110 认证票据(例如,利用如上所述的唯一会话密钥)、提取移动设备 A 的连接数据并且在 1111 把该连接数据转发到移动设备 B。最后,在 1113,移动设备 A 和 B 利用交换后的连接数据进入直接 P2P 连接。

[0145] 现在转向图 12,如果兼容性检查 1106 确定直接 P2P 连接不可行,则邀请服务 112 可以向中继服务 1051 发送中继查找请求 1201,以确定由每个移动设备所使用的中继主机。请求 1201 可以包含用于移动设备 A 和 B 的联网信息(例如,NAT 遍历 / 连接数据和 / 或 NAT 类型数据),这些信息由中继服务 1051 用于为两个移动设备选择适当的中继主机。如图 13 中所说明的,中继服务 1051 的一种实施例包括多个中继主机 1302-1303 以及包含与每个中继主机关联的网络信息的中继主机数据库 1301。邀请服务 112 向中继查找服务 1300 发送中继查找请求 1201,其中中继查找服务 1300 利用用于移动设备 A 和 B 的网络信息查询中继主机数据库 1301。一接收到数据库结果,中继查找服务 1300 就提供识别选定的中继主机 1302-1303 的响应 1202。

[0146] 在一种实施例中,中继查找响应 1202 包含由中继服务生成的中继令牌和由移动设备 A 和 B 用于中继连接的中继主机 1302-1303 的网络地址(IP 地址 / 端口)。在一种实施例中,中继令牌与中继会话关联并且由中继主机 1302-1303 用于一连接到中继服务 1051 就认证移动设备 A 和 B。令牌可以采用各种形式,包括例如唯一 ID 中继会话 ID 码、数字证书和 / 或与中继会话关联的唯一加密密钥。

[0147] 在 1203,邀请服务向移动设备 B121 发送包含将进行中继连接的指示的中继响应 1203。在一种实施例中,中继响应 1203 可以包括中继令牌和用于中继主机 B1303 的网络信息。在一种实施例中,响应 1203 可以直接发送到移动设备 B(绕过推送通知服务 1050),因为它是响应于移动设备 B 的接受 1105 而发送的。

[0148] 邀请服务 112 向移动设备 A 发送可以包括用于中继主机 B1303 的网络信息和中继令牌的中继响应 1204。在这种情况下,响应 1204 在事务 1205 经推送通知服务 1050 推送到移动设备 A。

[0149] 在 1206,移动设备 A120 使用用于中继主机 A1302 的网络信息与中继服务 1051 建立连接。类似地,在 1207,移动设备 B121 使用用于中继主机 B1303 的网络信息来建立与中继服务 1051 的连接。在这些事务的每一个当中,在移动设备 A 和 B 的任何 NAT 防火墙中打开新的洞而且用于移动设备 A 和 B 的 NAT 遍历 / 连接数据可以由中继服务 1051 确定并分别返回到移动设备 A 和 B(例如,通过确定用于设备的公共 IP/ 端口)。在一种实施例中,中继服务 1051 及移动设备 A 和 B 实现利用中继 NAT 的遍历(“TURN”)协议,如本领域技术人员所理解的,该协议允许 NAT 或防火墙后面的元素经 TCP 或 UDP 连接接收进入的数据。

[0150] 在 1208,移动设备 A 向邀请服务 112 发送中继更新,该中继更新在 1209 转发到推送通知服务并且在 1210 推送到移动设备 B。类似地,在 1211,移动设备 B 向邀请服务 112 发送中继更新,该中继更新在 1212 转发到推送通知服务并且在 1213 推送到移动设备 A。由移

动设备 A 发送的中继更新可以包括会话令牌、每个设备的 ID 码及由中继器在 1206 和 1207 确定的 NAT 遍历 / 连接数据(即,移动设备 A 把其 NAT 遍历 / 连接数据发送到移动设备 B,并且反之亦然)。在一种实施例中,因为每个移动设备的 NAT 信息都可能改变,所以执行中继更新操作。

[0151] 最后,在 1214 和 1215,移动设备 A 和 B 分别通过中继服务 1051 建立 P2P 连接。在一种实施例中,中继连接可以在移动设备 A 向中继服务 1051 发送移动设备 B 的 NAT 遍历 / 连接数据的时候建立,而且反之亦然,由此允许中继服务确定到每个对等体的中继主机 1302-1303 的正确路径。

[0152] 利用上述技术,邀请服务 112 可以实现为无状态服务,这种服务本质上是可缩放和有弹性的,即使在具有非常大量移动设备的大规模系统中也是这样。例如,因为推送通知服务 1050 本质上能够定位并把内容推送到注册了的移动设备,所以不需要邀请服务跟踪每个设备的当前位置。此外,因为设备可以对每个请求与响应发送整个会话状态数据,所以从不需要邀请服务维护任何每连接状态信息,由此减少邀请服务的存储与处理需求。这种实现在大规模系统中特别有用。

[0153] 用于为在线会话匹配用户的系统与方法

[0154] 如图 15 中所说明的,匹配器服务 111 的一种实施例可以包括用于接收匹配请求并且把匹配响应推送到移动设备 120-122 的匹配器调度器 1501;用于在请求表 1502 中存储匹配请求并且用于在匹配表集合标识符(“MSI”)表 1503 中存储可匹配集合数据的数据 1512;及用于从数据库 1512 提取匹配请求、执行匹配操作并且把匹配结果存储回数据库 1512 中的一个或多个匹配器 1510。但是,应当指出,本发明的基本原理不限于图 15 中所示的具体体系结构。

[0155] 在一种实施例中,匹配器调度器 1501 充当到匹配器服务 111 的接口,从移动设备 120-122 接收请求、把那些请求翻译成命令以在数据库 1512 中存储请求、从数据库 1512 读取匹配结果并且翻译那些结果并传送到移动设备 120-122。

[0156] 在操作中,当新的匹配请求到达时,匹配器调度器 1501 可以在一排请求表 1502 中存储请求。在一种实施例中,调度器 1501 为每个匹配请求指定请求 ID(“RID”)码,在图 15 中简单地说明为“A”、“B”和“C”(分别对应于移动设备 A、B 和 C)。虽然在图 15 中为了简单而使用字母命名,但是 RID 码可以是串、整数或者任何其它适于跟踪数据库中的匹配请求的任何其它变量类型。

[0157] 可以为每个匹配请求指定存储在请求表 1502 中的可匹配集合标识符(“MSI”)值。在一种实施例中,MSI 可以识别为其请求匹配的具体应用和 / 或要为那个应用使用的配置参数。例如,12:4 的 MSI 值可以识别具有标识符“12”的特定多玩家游戏而且可以识别具有标识符“4”的用于该游戏的特定配置。更具体地说,12 的 ID 码可以识别特定的多玩家赛车游戏而且 4 的 ID 码可以规定特定的赛车道、速度或赛车游戏的玩家经验级别。在一种实施例中,为应用开发者提供了以这种方式利用 MSI 值规定应用配置参数的选项。在一种实施例中,不是直接规定 MSI,而是应用开发者规定游戏 ID(以便识别特定的游戏)和桶 ID(以便识别特定的游戏配置)而且这些值由匹配器调度器 1501 映射到 MSI 值。

[0158] 此外,几个不同的 MSI 值可以在单个 MSI 中使用,以便规定多个不同的配置参数(例如,12:4:1 可能代表 :12= 赛车游戏 ;4= 赛车道 ;及 1= 经验级别)。如以下更具体描述

的,在一种实施例中,每个 MSI 由匹配器 1510 用于识别其中可以执行匹配器操作的一组匹配请求(例如,请求是基于 MSI 分组的而且匹配在每个 MSI 组中执行)。在一种实施例中,每个 MSI 可以由调度器动态修改 / 选择,以便包括识别不同机器分区的分区 ID。例如,如果一个特定的 MSI 变得超载,则调度器可以在两个或多个不同的服务器和 / 或存储分区之间分割该 MSI (例如,利用像 4:3:1 和 4:3:2 的指定,其中最后的数字分别识别分区 1 和 2)。然后,不同的匹配器可以独立地从来自每个不同服务器的每个不同 MSI 检索并处理请求。

[0159] 如图 15 中所说明的,匹配请求数据还可以存储在用于每个请求的请求表 1502 中。请求数据可以包括可用于给出匹配决策的任何数据和 / 或访问经网络启动请求的移动设备所需的任何数据。例如,在一种实施例中,用于每个请求的匹配请求数据包括用于启动请求的移动设备的 NAT 类型数据和 / 或 NAT 遍历 / 连接数据。其它类型的请求数据也可以存储在请求表 1502 中,诸如设备连接速度(100kbps、1Mbps 等)、连接类型(例如,3G、EDGE、WiFi 等)、设备位置(例如,由地理定位技术确定的)、语言(英语、西班牙语等)和 / 或用户偏好。请求数据可以由每个移动设备 120-122 确定并且与每个匹配请求一起发送到匹配器调度器 1501。例如,每个移动设备可以利用各种技术确定其连接数据、连接类型、设备位置等,其中有些技术在本文描述(例如,与 NAT 遍历服务器通信以便确定 NAT 遍历 / 连接数据、利用 GPS 确定设备位置、读取 HTTP 信息以便确定语言,等等)。

[0160] 如图 15 中所说明的,在一种实施例中,每个有效的 MSI 都可以在 MSI 表 1503 中指定一行。在一种实施例中,当新的请求到达时,除了把该请求添加到请求表 1502,调度器 1501 还检查 MSI 表 1503,以确定 MSI 是否已经对那个请求存在(即,具有相同 MSI 的其它请求是否已经接收到)。如果没有找到匹配的 MSI,则调度器 1501 可以在 MSI 表 1503 中为该新请求创建新的条目。如果找到匹配的 MSI,则调度器可以简单地把该新请求添加到请求表 1502,如上所述。

[0161] 一旦请求表 1502 和 MSI 表 1503 被匹配器调度器 1501 更新,匹配器模块 1510 的实例(下文中简单地称为“匹配器 1510”)就提取数据,以便执行牵线操作。多个匹配器实例可以同时执行,以便执行牵线请求,而且单个匹配器 1510 可以同时在多个不同的 MSI 组上处理多个匹配操作。

[0162] 在一种实施例中,当匹配器 1510 变得可用时(例如,在为一个 MSI 组完成匹配操作之后或者在初始化之后),它查询 MSI 表 1503,以便识别要处理的新 MSI。在图 15 中,匹配器 ID 字段中用于 MSI3:1 的“N/A”值指示用于处理这个 MSI 的责任还没有指定给匹配器。在一种实施例中,每个 MSI 条目是加了时间戳的而且匹配器 1510 选择具有最老时间戳的 MSI。

[0163] 在一种实施例中,当匹配器 1510 假设对一个特定 MSI 有责任时,它更新 MSI 表 1503 中其匹配器 ID 码并且规定用于那个 MSI 的租赁持续时间(例如,5 秒)。在一种实施例中,匹配器 1510 在其为那个 MSI 处理匹配的时候持续地更新租赁值。该租赁值可以用于识别指定给发生故障的匹配器 1510 的 MSI。例如,如果租赁值到期,则那个 MSI 可以被新的匹配器认领,而不管 MSI 表 1503 指示该 MSI 已经指定给一个匹配器的事实。

[0164] 一旦匹配器 1510 已经假设对一个 MSI 有责任,它就可以查询请求表 1502,以便把与那个 MSI 关联的请求读到存储器中。然后,匹配器 1510 可以执行匹配操作,以根据一组匹配标准匹配用户与移动设备(例如,如下所述)。匹配器 1510 可以更新请求表 1512,以便指示何时进行移动设备的匹配。例如,匹配器可以从请求表 1512 中的 MSI 列除去 MSI 值并

且输入预先定义的值,以便指示匹配已经完成。此外,匹配器 1510 可以更新用于每个参与者的“请求数据”字段,以便识别与那个参与者匹配的其它参与者(例如,通过写与其它参与者通信所需的 NAT 遍历 / 连接数据)。

[0165] 调度器 1501 可以周期性地查询请求表 1502,以便识别完成的匹配。响应于检测到完成的匹配,调度器 1501 可以向匹配中所涉及的移动设备发送推送通知(例如,利用本文及共同未决的申请中所述的推送通知技术)。在一种实施例中,推送通知包括上述“票据”数据结构。然后,移动设备可以使用它们的每张票据来经 CDX 服务 110 交换连接数据,如上所述。

[0166] 除了使用推送通知,在一种实施例中,移动设备 120-122 还可以周期性地查询调度器 1501,以便确定是否已经进行了匹配。在推送通知还没有对移动设备进行时,周期性的查询是有用的。但是,因为使用了推送体系结构,所以周期性查询可以设置到相对低的速率,由此减小匹配器服务 111 上的负荷。

[0167] 图 16 说明了其中两个移动设备,A 和 B,由匹配器服务 111 匹配的方法的示例性实施例。图 17a-17d 说明了在所述方法前进时可能发生的对请求表 1502 和 MSI 表 1503 的示例性更新。

[0168] 在 1601,从移动设备 A 接收匹配请求。在 1602,移动设备 A 的请求输入到请求表中而且新的 MSI 条目(MSI1:1)输入到 MSI 表中(如果还不存在的话),如图 17a 中所说明的。在 1603,从设备 B 接收匹配请求并且,在 1604,移动设备 B 的匹配请求也输入到请求表中,如图 17b 中所说明的。

[0169] 在 1605,特定的匹配器实例(匹配器 #N)检查 MSI 表并且检测到 MSI1:1 还没有被另一个匹配器实例认领。作为替代,匹配器可以检测具有到期租赁的 MSI 表条目,指示先前对该 MSI 工作的匹配器已经发生故障。在一种实施例中,具有到期租赁的 MSI 条目比(还没有指定匹配器的)新 MSI 条目被赋予更高的优先级。此外,在一种实施例中,相对来说更旧的 MSI 条目可以比相对来说更新的 MSI 条目赋予更高的优先级。不管匹配器如何选择 MSI,当它在这么做的时候,它添加其标识符并且为该 MSI 条目设定新的租赁值,如图 17c 中所说明的(例如,在所说明的实施例中,利用 5 秒的租赁值)。然后,匹配器可以查询请求表并把具有那个 MSI 的请求表条目读到存储器中,使得它们可以被处理。

[0170] 在 1606,匹配器执行一系列匹配操作,以便为每个请求选择适当的匹配。匹配操作的某些实施例在下面关于图 18 进行描述。简而言之,在一种实施例中,为了确定“适当”匹配而被评估的变量包括NAT 类型(例如,完全圆锥形、端口受限、对称等)、连接类型(例如, WiFi、3G、Edge 等)、与用户关联的语言(从 HTTP 请求接受语言首部得到的)及每个匹配请求的年龄。总的来说,匹配器 1510 可以尝试匹配具有兼容 NAT 类型(虽然有时候可以使用中继服务,如下所述)、相同连接类型和相同语言的移动设备。在一种实施例中,基于匹配请求的年龄,匹配器 1510 可以对匹配需求更自由(即,请求越老,将更自由地应用匹配约束)。

[0171] 返回图 16,在 1607,在匹配决策之后,匹配器 1510 可以更新请求表,以便指示匹配完成,如图 17d 中所指示的。作为更新的一部分,匹配器还可以更新用于移动设备 A 和 B 的请求数据。例如,在一种实施例中,匹配器 1510 在用于移动设备 A 的请求数据列中写移动设备 B 的 NAT 遍历 / 连接数据,并且在用于移动设备 B 的请求列中写移动设备 A 的 NAT 遍历 / 连接数据。

[0172] 在 1608, 调度器 1501 可以从头到尾读一遍请求表, 以便识别已经匹配的请求条目。在一种实施例中, 当检测到移动设备 A 和 B 已经匹配时, 它读取(如上所述由匹配器更新的)请求数据, 并且为移动设备 A 和 B 生成通知。在一种实施例中, 通知是上述加密的“票据”数据结构而且包括用于每个移动设备的 NAT 遍历 / 连接数据。如前面所描述的, 在一种实施例中, 推送通知服务 1050 用于把通知推送到移动设备 A 和 B。此外, 移动设备 A 和 B 可以周期性地轮询调度器 1501, 以确定是否已进行匹配。在这种实施例中, 轮询技术可以相对慢的速率进行, 以便识别出于某个原因而没有成功推送到移动设备之一的匹配。利用推送通知管理轮询请求负荷显著减小了匹配器服务 111 上的负荷, 否则, 这些负荷将由来自移动设备的轮询请求加载。

[0173] 如果在 1608 确定附加的匹配请求对相同的 MSI 是未决的, 则匹配器可以继续匹配 MSI 中的移动设备 / 用户。在 1610, 匹配器可以重置 MSI 表 1503 中的租赁值。在 1611, 执行附加的匹配并且请求表被更新(如上所述)。在 1612, 附加的匹配从请求表读出而且附加的移动设备被更新(如上所述)。如果没有附加的匹配请求对该 MSI 是未决的, 则在 1609 该 MSI 条目从 MSI 表除去(例如, 经来自调度器和 / 或匹配器的删除命令)。

[0174] 图 18 说明了用于在移动设备 / 用户之间执行匹配的方法的一种实施例(图 16 中的操作 1606)。在 1801, 所有当前的 MSI 请求(例如, 对于特定的应用 / 桶组合)按对布置。在 1802, 评估每一对之间的匹配“适合”(Fit)并且, 在 1803, 按适合的降序排列给这些对排序。“适合”是基于多个不同变量来评估的, 包括但不限于 NAT 类型(例如, 完全圆锥形、端口受限、对称等)、连接类型(例如, WiFi、3G、Edge 等)、与用户关联的语言(从 HTTP 请求接受语言首部得到的)及每个匹配请求的年龄。可以在匹配决策中作为因素考虑的其它变量包括每个移动设备的位置(例如, 对于尝试匹配特定位置的用户);最小化和 / 或最大化玩家需求(例如, 由用户和 / 或应用规定的);MSI 中所包括的一个或多个用户是否是“朋友”或者先前曾进入到 P2P 连接中过(例如, 优选匹配“朋友”或之前的熟人);及用户对应用的经验(例如, 对于多玩家游戏, 每个用户的排行榜排名可以作为因素考虑, 优选匹配具有相似经验的用户)。

[0175] 如下表 A 中所指示的, 在一种实施例中, “适合性”的评估是 0.0 到 1.0 之间的一个数字值。利用浮点值允许对每个标准的适合性的规格化。为了避免浮点运算, 非规格化的整数值可以对合适的评估使用, 使得适合性值可以比较。

[0176] 在一种实施例中, 所有标准都具有二进制适合, 其中它们是兼容的(具有规格化值 1.0)或者不兼容的(具有小于 1.0 的规格化值)。根据需要, 这些可以被看作标准, 其中适合随年龄而变(如下所述)。如果位置作为变量添加, 则最佳适合可能是与匹配所需标准的最近玩家的适合。

[0177] 匹配适合性 - 表 A

[0178]

因素	权重	规格化
NAT 兼容性	2.0	0.4
连接类型	2.0	0.4

语言	1.0	0.2
总计	5.0	1.0

[0179] 在一种实施例中,适合等于用于上述每个标准的(规格化权重 * 老化的因素值)之和。老化的因素值可以从值 1 开始并且在经过预定时间段后增加。然后,它可以随着更多时间经过而继续增加(例如,周期性地增加规定的量)。在一种实施例中,代替利用上述老化因素值,年龄阈值可以如下所述地建立。诸如连接类型与语言的某些变量的规格化 / 加权值可以高于某些年龄阈值而应用(即使它们不匹配)。

[0180] 在一种实施例中,一对请求, A 和 B, 之间的“适合”是 A 与 B 和 B 与 A 的适合的平均值。而且,对于每个因素 A 与 B 的适合都可以基于 A 的年龄来调节(而且反之亦然)。在一种实施例中,1.0 的适合对于兼容性匹配可能是需要的。这意味着 A 和 B 将只在 NAT 兼容性、连接类型和语言匹配的时候(导致 1.0 的规格化值)或者 A 和 / 或 B 已经老化使得有些上述变量(例如,连接类型和语言)被有效忽略的时候(例如,利用阈值以上的或者以下的老化因素)匹配。

[0181] 年龄 - 表 B

[0182]

年龄	阈值 1	阈值 2	阈值 3	阈值 4	阈值 5
比…老	0 秒	1 秒	5 秒	10 秒	30 秒

[0183] 年龄阈值可以如上表 B 中阐述的那样建立。当通过每个年龄阈值时(即,当请求变得比规定阈值老时),老化的因素值可以增加到后续更大的值(例如,1.5、2.0 等)。作为替代,或者附加地,当通过不同的年龄阈值时,用于某些变量的加权值可以添加到匹配决策(例如,像以下所述的连接类型和语言)。

[0184] 在一种实施例中,对于给定的 MSI, 表 B 中规定的请求年龄限制是根据匹配流速率调节的。在一种实施例中,流速率规定为每个规定的单位时间(例如,每 10 秒、每分钟等)执行的匹配的次数。因而,流速率提供了关于一个特定 MSI 集合有多忙的指示。在一种实施例中,该集合越忙,以上每个阈值可以在上表 B 中设置得越低,以便增加早期成功匹配的可能性并减小匹配器上的负荷。而且,给定 MSI 集合的负荷可以提供给终端用户(例如,以估计的到匹配值的时间的形式),因此终端用户可以选择是否尝试进入特别忙的多玩家游戏。负荷值可以推送通知的形式提供给用户。

[0185] 现在转向来自表 A 的每个变量,在一种实施例中, NAT 兼容性是从图 14 中所示的 NAT 兼容性图表 1400 确定的。如果基于这个图表确定两个 NAT 兼容,则可以应用 NAT 兼容性权重。

[0186] 连接类型 - 表 C

[0187]

	A/B	WiFi	Edge	3G
WiFi	1.0	0.0	0.0	

Edge	0. 0	1. 0	0. 0
3G	0. 0	0. 0	1. 0

[0188] 连接类型可以利用如上表 C 中所示的图表来评估。在这个例子中,如果设备 A 与 B 的连接类型相同(如由单元格中的 1. 0 所指示的,其中相同的连接类型相遇),则来自表 A 的加权连接类型值可以包括在适合性确定中。如以上所提到的,每个请求的年龄可以用于影响连接类型确定。例如,在一种实施例中,用于连接类型的适合值是利用表 C 中的矩阵为处于阈值 1、2 和 3 的年龄选择的。对于处于阈值 4 或者更高的年龄,连接类型可以设置成 1. 0 (即使对于不匹配的连接类型)而且可以应用对应的加权连接类型值。虽然在有些实施例中使用连接“类型”,但是连接速度也可以确定并且与连接类型一起或者代替其使用。例如,某些规定范围内的连接速度可以被认为是“兼容的”(例如,0–100 kbps ;100–500 kbps ;500–1000 kbps ;1000–1500 kbps 等)。本文所讨论的任何匹配变量也都可以作为权重应用到匹配适合计算并且如上所述那样老化。

[0189] 在一种实施例中,玩家语言可以从 HTTP 请求接受语言首部导出,该首部可以包含具有偏好 q 因子的一种或多种语言。调度器可以提取最优先的语言并且把这个信息传递到匹配器。在一种实施例中,如果语言相同,则来自表 A 的加权语言值设置成 1. 0 ;或者如果不相同就设置成 0. 0。但是,在一种实施例中,即使语言不同,但是如果年龄高于规定阈值的话(例如,如果年龄在表 B 中的阈值 2 或者更高),则加权语言值也可以应用。

[0190] 在一种实施例中,可以在具有不兼容 NAT 类型的两个用户之间进行匹配。例如,如果匹配器难以以为一个特定的 MSI 匹配用户,则在规定的时间段之后,它可以利用上述技术通过中继服务 1051 路由连接。以这种方式,中继服务 1051 充当压力阀门,允许老化匹配不管不兼容的 NAT 类型而发生。中继服务 1051 还可以响应检测到一次或多次失败的匹配尝试而使用。在这种实施例中,由移动设备提交的每个匹配请求可以包括关于先前是否尝试了一次或多次不成功匹配的指示。

[0191] 各种附加的匹配标准都可以被评估并且作为匹配适合确定的一部分被提供加权值,作为例子但不是限制,包括关于请求匹配的任何用户是否是朋友的指示。例如,匹配器 1510 可以尝试通过对匹配适合计算应用“朋友”权重来为是“朋友”的用户匹配任何请求。类似地,朋友的朋友也可以被加权(例如,具有 2 或更多分离度)。此外,玩家可以对特定的游戏给其他玩家分级并且匹配器可以在执行匹配的时候评估那些等级(具有匹配用户与具有相对更高等级的那些玩家和不匹配用户与具有低等级的那些玩家的趋势)。而且,用户连接的等待时间可以(例如,利用简单的查验(ping)操作)被评估并且用作匹配决策的一部分。

[0192] 用于匹配玩家的还有另一个变量可以是设备类型。例如,匹配器 1510 可以尝试匹配具有相似设备类型(例如, iPad、iPod、iTouch、iPhone、RIM Blackberry 等)的玩家。附加的变量可以包括用户的排行榜排名、当前位置、当前住处、年龄、性别,而且可以针对匹配确定类似地评估类似的游戏集合(即,在许多情况下,趋于促成具有相似标准的那些用户之间的匹配)。最后,家长控制可以由匹配器 1510 评估,以确保用户只与适当的 MSI 并且与相同年龄的其他用户匹配。

[0193] 匹配器服务 111 可以从数据服务 100 中管理的一个或多个数据库(例如,见以下关于图 19 所述的数据库 1920)检索任何以上变量。例如,用户的朋友数据可以从朋友服务数

据库访问,而诸如每个用户的年龄、性别、游戏集合等其它信息可以从一个或多个其它数据库(例如,用户简档、游戏数据库、排行榜数据库等)访问。在一种实施例中,为本文所述的所有服务都提供了对相同中央数据库(或数据库组)的访问,该中央数据库用于存储用于作出匹配决策的全部各种不同类型的用户 / 设备数据。

[0194] 虽然以上提供了几个具体的例子,但是应当认识到,本发明的基本原理不限于用于为匹配确定适合性级别的任何特定变量集合。在一种实施例中,设计要在本文所述的系统与方法上运行的应用的应用程序员可以规定他们自己利用不同 MSI 标准进行匹配和 / 或用于分组请求的标准集合。

[0195] 回过头来看图 18 的方法,一旦在 1803 确定了每对之间的匹配“适合”,这些对就按适合的降序来排序(例如,具有最高适合的对在列表的顶部)。在 1804,利用具有高于规定阈值的最高适合值的那些对对“匹配集合”播种。如上所述,“阈值”值可以设置成上表 A 中所示的规格化值 1.0。在 1805,向匹配集合添加与匹配集合中一个或全部当前成员具有高于规定阈值的适合值的新的潜在合作伙伴。例如,如果一个匹配集合最初利用 A 和 B 播种,则如果 A-C 和 / 或 B-C 的适合值高于规定阈值的话,则 C 就可以添加到该匹配集合。在一种实施例中,如果只有单个匹配适合高于用于潜在一方的阈值,则那一方可以添加到匹配集合(即,因为,如果必要的话,那一方将能够通过它与其具有合适匹配适合的一方向所有各方通信)。一旦新的一方或多方已经添加到匹配集合,如果在 1806 确定已经满足匹配的尺寸需求,则匹配结果就在 1807 被存储并报告(例如,通过更新请求表 1502 并且发送通知,如上所述)。在一种实施例中,单个匹配请求可以代表多个用户(例如,当一个匹配请求跟在如下所述的邀请序列之后时)。在这种情况下,基于每个匹配请求代表的用户数目评估尺寸需求。如果尺寸需求还没有满足,则过程返回 1805 而且新的一方添加到匹配集合(即,与集合中的一个或多个当前成员具有高于规定阈值的匹配适合的一方)。

[0196] 在 1808,匹配的请求从匹配器 1510 处理的当前请求集合中除去。在 1809,选择下一个播种的匹配集合并且过程返回 1804,进行附加的匹配。虽然在图 18 中说明为顺序过程,但是应当指出,在仍然遵循本发明的基本原理的情况下,多个播种的匹配集合可以同时处理。

[0197] 虽然在上面描述为单独的服务,但是匹配器服务 111 和邀请服务 112 可以一起操作来连接 P2P 用户。例如,在一种实施例中,第一用户可以邀请一个或多个朋友到在线会话并且请求与一个或多个附加用户的匹配(例如,邀请朋友“Bob”并且为多玩家视频游戏匹配 3 个附加的玩家)。在这种情况下,邀请服务 112 可以最初处理第一用户的邀请请求,以便连接第一用户和第一用户的朋友。然后,该邀请请求的结果(例如,成功的 P2P 连接)可以被报告回用户的移动设备。然后,匹配器服务 111 可以从第一用户的移动设备(或者,在一种实施例中,直接从邀请服务或者从第一用户的朋友)接收请求附加玩家的匹配请求。作为响应,匹配器服务 111 可以把第一用户与一个或多个与第一用户的请求具有相同 MSI 的其它匹配请求匹配(如上所述)。匹配请求可以只包括第一用户的匹配标准或者可以包括第一用户和第一用户朋友的匹配标准(例如,NAT 类型、连接类型、语言、位置等)。在一种实施例中,如果第一用户的一个或多个朋友不能与另一个匹配的用户建立直接 P2P 连接,则该匹配用户与第一用户朋友的连接可以通过第一用户的 data 处理设备建立(例如,利用第一用户的移动设备作为连接的代理)和 / 或中继服务可以用于连接用户(如上所述)。

[0198] 在一种实施例中,第一用户可以最初与一个或多个用户通过匹配服务匹配(如上所述)而且然后第一用户可以邀请一个或多个朋友加入与第一用户和匹配用户的在线会话。在这种实施例中,用户的信息和匹配用户的信息(例如,NAT/连接数据、用户 ID、推送令牌等)都可以通过邀请服务与被邀请的用户交换(如上所述)。不管是匹配首先发生然后再邀请还是邀请首先发生然后再匹配,本发明的基本原理都保持相同。

[0199] 具有用于协作在线应用的应用编程接口的应用框架

[0200] 如图 19 中所说明的,本发明的一种实施例是在移动设备 120 的背景下实现的,移动设备 120 具有预定义的软件框架 1912,其具有用于与一个或多个应用 1911 接口的应用编程接口(“API”) 1910 和用于与多个网络服务 1901-1903 通信的服务侧 API1910 通信的。如图 19 中所示,网络服务 1901-1903 可以由相同的在线数据服务 100 设计和 / 或管理(虽然这种配置不是必需的)。例如 P2P 游戏应用和其它类型协作在线应用的应用 1911 可以设计成通过对 API1910 进行调用而通过 API1910 来访问网络服务 1901-1903。应用 1911 的设计可以利用由框架 1912 和网络服务 1901-1903 的开发者提供的软件开发包(“SDK”)来方便其进行。框架 1912 和 API1910、1913 的更具体实现在下面参考图 20 描述。

[0201] 如所说明的,可以为每种服务提供对用于存储服务所使用数据的数据库 1920 的访问。一个特定的例子是由匹配器服务 111 使用的数据库 1512 (以上所述)。其它例子可以包括用于存储排行榜数据的排行榜数据库、存储朋友状态记录的朋友服务数据库、存储用户简档数据的简档数据库和存储关于在线游戏的数据的游戏数据库。任何类型的数据库都可以使用(例如,MySQL、Microsoft SQL 等),但是在一种特定的实施例中,可以使用例如 Berkley DB 和 / 或 MZBasic DB 的键 / 值(key/value)数据库。数据库可以跨存储区域网络(SAN)或其它存储配置中的大量大容量存储设备(例如,硬驱)散布。

[0202] 因此,当特定的服务如上所述处理和 / 或存储数据时,数据可以存储在数据库 1920 中。但是,有些服务可以不利用数据库。例如,如上所述,邀请服务 112 可以实现为无状态服务而且,因此,可能不需要在数据库 1920 中存储数据(虽然,根据本发明的基本原理,这种实现仍然是可能的)。

[0203] API1913 可以设计成利用任何合适的网络协议堆栈,包括例如位于网络层的 TCP/IP 或 UDP/IP 和位于应用层的 HTTPS,来与网络服务 1901-1903 通信并交换信息。可以使用 HTTP 或 HTTPS 上基于远程过程调用(RPC)的协议,例如 SOAP,或者可以使用表征状态转移(REST)协议。而且,服务可以在任何计算平台上实现,作为例子,包括 Xserver 或者运行 Unix、Linux 或 Apache 软件平台的类似计算平台。在一种特定的实施例中,所述平台包括在 Linux 上实现的 Web 对象。以上例子仅仅是为了说明而提供的。本发明的基本原理不限于把应用链接到服务或者任何特定的网络协议集合的任何特定机制。

[0204] 图 20 说明了本发明一种实施例中更具体的软件体系结构,包括可以在无线设备 120 上实现的应用编程接口(API)2001a-2001b。虽然这种实施例是在多玩家游戏框架 2000 的背景下描述的,但是本发明的基本原理不限于游戏实现。例如,图 20 中所示的软件体系结构可以用于支持各种非游戏的协作应用(例如,协作聊天、多玩家协作音频 / 视频等)。

[0205] 在图 20 所示的体系结构中,提供了支持本文所述各种多玩家特征和 P2P 特征的游戏框架 2000。在一种实施例中,游戏框架 2000 设计成运行在移动设备的操作系统 2005 上。例如,如果移动设备 120 是 iPhone、iPad 或 iPod Touch,则操作系统 2005 可以是 iPhone

OS,这是由本申请受让人设计的一种移动操作系统。

[0206] 游戏框架 2000 可以包括公共应用编程接口(API) 2001b 和私有的或“安全”API2001a。在一种实施例中,设计成提供本文所述各种与游戏相关的特征的游戏中心应用 2031 可以对公共 API2001b 和私有 API2001a 都提供调用,而为其它应用 2030 (例如,由第三方设计的应用) 提供对仅公共 API2001b 的访问。例如,移动设备 120 的设计者可能希望保持涉及可能敏感信息的某些 API 功能在公共 API2001b 之外,以避免由第三方开发者滥用(例如,朋友请求,朋友列表等)。但是,安全 API2001a 和公共 API2001b 可以融合到可以由移动设备上的所有应用访问的单个 API 中(即,把 API 分成单独的公共和私有组成部分不是为了遵循本发明的基本原理所必需的)。指定“API2001”有时候在下面指可以在公共 API2001b 和 / 或私有 API2001a 中找到的操作。

[0207] 在于 2010 年 4 月 7 日提交、标题为“Systems and Methods for Providing a Game Center”、代理人案号为 4860.P9127USP1、序列号为 ____、发明人是 Marcel Van Os 和 Mike Lampell 的共同未决申请(下文中称为“游戏中心专利申请”)中记载了游戏中心应用 2031 的一种实施例,该申请被转让给本申请的受让人并且通过引用而被结合于此。简而言之,游戏中心应用 2031 包括游戏中心图形用户界面(GUI),用于导览多玩家游戏;购买新游戏;检索与游戏相关的信息(例如,排行榜信息、成绩、朋友信息等);联系朋友来玩游戏;请求与其他用户的游戏匹配;及邀请具体的用户。由游戏中心应用 2031 执行的各种其它功能在以上引用的游戏中心专利申请中描述。有些游戏中心功能可以由游戏框架 2000 提供并且可以让其它应用 2030 通过公共 API2001b 访问。

[0208] 在一种实施例中,由游戏框架 2000 揭示的 API2001 简化了为移动设备 120 设计多玩家、协作游戏的过程。特别地,在一种实施例中,API2001 允许开发者进行简单的 API 调用,以便为多玩家的 P2P 游戏会话启用相对复杂的连接用户的过程。例如,像 INVITE(玩家 B ID,桶 ID) 的简单 API 调用可以从 API2001 启用,以便启动上述具体邀请序列。类似地,像 MATCH(玩家 A ID,桶 ID) 的 API 调用可以从 API2001 启用,以便启动上述具体匹配序列。INVITE 和 MATCH 功能有时候在本文中统称为“P2P 连接功能”。在一种实施例中,游戏框架 2000 包括管理邀请所需的程序代码和响应这些 API 调用的匹配操作(如以下更具体地描述的)。应当指出,实际的 API 功能可以具有与以上述那些稍不同的数据格式(虽然它们可以导致由游戏框架 2000 执行的相似操作)。本发明的基本原理不限于规定 API 功能的任何特定格式。

[0209] 各种其它类型的游戏相关事务与信息也可以由游戏框架 2000 代表游戏中心 2031 与其它应用 2030 管理。有些这种信息在游戏中心专利申请中进行了描述。作为例子但不是限制,这种信息可以包括关于已经对每个游戏实现了最高得分的那些用户的“排行榜”信息和识别已经完成了某些特定于游戏的成绩的用户的“成绩”信息。每个应用开发者可以为每个游戏应用 2030 规定他们自己的“成绩”集合(例如,完成了关 1-3;在 5 分钟内完成第一关;每一关超过 50 次击杀;撞倒 20 个标志;等等)。

[0210] 游戏框架 2000 还可以包括用于管理用户的朋友数据和用于在游戏中心 2031 和其它游戏应用 2030 的背景下集成朋友数据的程序代码。例如,当用户选择了指向游戏中心 2031 中特定游戏的链接时,可以为那个游戏显示与该用户的每个朋友关联的信息(例如,该朋友在排行榜上的排名、该朋友的成绩、当用户与他 / 她的每个朋友玩该游戏时的结果,

等等)。在一种实施例中,游戏框架 2000 的 API2001 包括用于访问由朋友服务管理的朋友数据,例如在于 2010 年 4 月 7 日提交、标题为“Apparatus and Method for Efficiently Managing Data in a Social Networking Service”、代理人案号为 4860.P9240、序列号为 ____、发明人是 Amol Pattekar、Jeremy Werner、Patrick Gates 与 Andrew H. Vyrros 的共同未决申请(下文中称为“朋友服务申请”)中所描述的朋友服务,该申请被转让给本申请的受让人并且通过引用被结合于此。

[0211] 如图 20 中所说明的,在一种实施例中,游戏守护进程 2020 可以把游戏框架 2000 接口到第一组服务 2050 而且游戏服务组件 2010 可以把游戏框架 2000 接口到第二组服务 2051。作为例子,第一组服务 2050 可以包括上述邀请服务 112、匹配器服务 111 和中继服务 1051 及以上引用的朋友服务申请中所描述的朋友服务。可以经游戏守护进程 2020 访问的其它服务包括排行榜服务(提供排行榜数据);游戏服务(提供关于每个游戏的统计数据与其它数据及购买游戏的能力);用户认证服务(用于认证移动设备的用户);和 / 或用户简档服务(用于存储诸如用户偏好的用户简档数据)。经游戏服务组件 2010 访问的第二组服务 2051 可以包括上述连接数据交换(CDX)服务 110 和 NAT 遍历服务 290-291。虽然在图 20 中为了说明的目的而说明为独立的组件,但是游戏守护进程 2020 和游戏服务模块 2010 实际上可以是游戏框架 2000 的组成部分。在一种实施例中,游戏守护进程 2020 和 2010 通过预先定义的 API 与每个网络服务 2050-2051 通信,在一种实施例中,预先定义的 API 是私有 API (即,没有公布给第三方开发者)。

[0212] 在一种实施例中,游戏守护进程 2020 可以利用 HTTPS 协议与匹配器服务 111、邀请服务 112 和其它服务 2050 通信,而游戏服务模块 2010 可以利用相对轻量级的协议,例如 UDP 套接字,与 CDX 服务 110 和 NAT 遍历服务 290-291 通信。但是,如前面所提到的,在仍然遵循本发明基本原理的情况下,可以采用各种其它网络协议。

[0213] 此外,如图 20 中所说明的,游戏守护进程 2020 可以接收由某些服务 2052 (例如,邀请服务和匹配器服务)生成的推送通知 2052,而其它类型的推送通知 2053 可以直接由游戏中心接收(例如,像新朋友请求的朋友服务通知)。在一种实施例中,这些推送通知 2053 直接提供给游戏中心 2031,以确保用户的敏感数据是第三方应用开发者设计的应用 2030 访问不到的。

[0214] 返回以上在图 11 中阐述的游戏邀请例子,当移动设备 A 上的应用 2030 对游戏框架 2000 的 API2001b 进行邀请调用以便邀请移动设备 B 的用户时(例如,INVITE(玩家 B ID, 游戏 / 桶 ID)),游戏框架 2000 可以把该邀请请求传递到移动设备 A 的游戏守护进程 2020。然后,游戏守护进程 2020 可以与邀请服务 112 通信,以便提交邀请请求。然后,邀请服务 112 可以使用推送通知服务 1050 (如上所述) 把邀请推送到移动设备 B 的游戏守护进程 2020。然后,移动设备 B 的游戏守护进程 2020 可以与移动设备 B 的游戏框架 2000 通信,以便确定为其发送邀请的游戏是否安装在移动设备 B 上。如果是,则游戏框架 2000 可以触发应用 2030 和 / 或生成邀请的可见通知。如果应用没有安装,则游戏框架 2000 可以向移动设备 B 的用户触发邀请的可见通知,该通知带有购买游戏的提供(例如,经游戏中心 2031GUI)。作为替代,该可见通知可以通过运行在移动设备 120 上的推送通知守护进程(未示出)生成。如果移动设备 B 的用户购买了该游戏,则邀请序列可以在购买之后继续。如果移动设备 B 的用户接受邀请请求,则移动设备 B 的游戏框架 2000 可以把邀请请求传递到其游戏守护进

程 2020,然后该守护进程 2020 可以对邀请服务 112 作出响应。

[0215] 还记得在图 11 中兼容性检查 1106 确定移动设备 A 和 B 的 NAT 类型是兼容的。因而,在 1108,移动设备 A 的游戏守护进程 2020 可以接收移动设备 B 的接受(例如,在这个例子中是经推送通知)而且,在一种实施例中,把接受传递到游戏框架 2000。在这个阶段,移动设备 A 的游戏框架 2000 可以通知发出请求的应用 2030 移动设备 B 已经接受(经 API2001)或者可以等待,直到设备已经成功连接才通知发出请求的应用。在任何一种情况下,游戏框架 2000 都可以把连接请求传递到游戏服务模块 2010,在一种实施例中,游戏服务模块 2010 可以启动与移动设备 B 的连接数据交换。特别地,游戏服务模块可以利用 CDX 服务 110 把移动设备 A 的连接数据发送到移动设备 B (见例如图 11 中的事务 1111 和 1112)。如上所述,这种通信可以利用安全的“票据”数据结构实现为 UDP 连接。

[0216] 还记得在图 12 中如果兼容性检查 1106 确定移动设备 A 和 B 的 NAT 类型不兼容,则中继服务 1051 可以用于在设备之间提供连接。因此,移动设备 B 的游戏守护进程 2020 可以从邀请服务接收中继响应 1203 (图 12 中所示)而且移动设备 A 的游戏守护进程 2020 可以从邀请服务接收中继响应(经推送通知服务 1050)。移动设备 A 与 B 的游戏守护进程 2020 可以在 1206 与 1207 与中继服务通信,以便检索配置数据。在 1210,移动设备 B 的游戏守护进程 2020 接收来自移动设备 A 的中继更新数据并且,在 1213,移动设备 A 的游戏守护进程 2020 接收来自移动设备 B 的中继更新数据。

[0217] 图 11 和 12 中所示过程的最终结果是移动设备 A 与 B 彼此建立了连接(或者是直接的 P2P 连接或者是中继连接)。在一种实施例中,一检测到成功的连接,游戏框架 2000 就可以通知利用 API 调用(例如,CONNECTED(玩家 A ID,玩家 B ID))请求该连接的应用 2030。然后,移动设备 A 与 B 可以利用所建立的连接玩规定的游戏或者其它协作应用 2030。

[0218] 因而,响应来自 API2001 的相对简单的调用(例如,INVITE(玩家 B ID,游戏 / 桶 ID)),可以由游戏框架 2000 管理一系列复杂的事务,以便在移动设备 A 与 B 之间建立 P2P 或中继连接。在一种实施例中,游戏框架 2000 执行连接移动设备 A 与 B 的操作序列,然后把结果提供给发出请求的应用 2030,由此留下对应用设计者透明的 API 的细节。因此,应用设计者不需要理解如何在网络上连接移动设备 A 和 B,或者如何执行用于在设备之间建立通信所需的各种其它功能,由此简化应用设计过程。

[0219] 以相似的方式,游戏框架 2000 可以利用以上关于图 2a-2b 所述的匹配器服务 111 在移动设备 A 与其它参与者之间建立匹配。在这个例子中,应用 2030 可以对 API2001 进行简单的调用,诸如 MATCH(玩家 A ID,游戏 / 桶 ID)。作为响应,游戏框架 2000 可以管理匹配和连接数据交换操作。当匹配操作和 / 或 P2P 连接完成时,游戏框架 2000 把结果提供回应用 2030。

[0220] 例如,在图 2b 中,游戏框架 2000 可以使用游戏服务模块 2010 与连接数据交换(CDX)服务 111 和 NAT 遍历服务 290-291 通信而且可以使用游戏守护进程来与匹配器服务 111 通信。一旦匹配已经建立,移动设备 A 的游戏守护进程 2020 就在 229 接收票据 A 并且游戏框架 2000 使用这个信息通过游戏服务模块 2010 实现连接数据交换。例如,在 232,它可以通过 NAT 遍历服务 290 请求它自己的连接数据并且然后可以通过 CDX 服务 110 在 233-234 交换其连接数据。在 237 与 240,移动设备 A 的游戏服务模块 2010 分别接收用于移动设备 B 和 C 的连接数据。在这些交换之后,游戏服务模块 2010 在 241 建立 P2P 连接并且游戏框

架 2000 利用 API 通知(例如, MATCH COMPLETE(玩家 B ID, 玩家 C ID))通知应用 2030 连接过程已经完成。然后, 应用可以利用所建立的 P2P 连接执行。

[0221] 在有些实施例中, 可以给予用户与当前注册为“在线”的其他朋友玩游戏的选项。在这种情况下, 某些朋友在线的通知可以经推送通知 2052 或推送通知 2053 (其由游戏中心 2031 直接接收) 提供。然后, 游戏中心 2031 和 / 或应用 2030 可以向用户提供通知并且为用户提供与一个或多个选定的在线朋友玩的选项。但是, 应当指出, 不管是否提供在线通知, 本发明所述的邀请序列都将工作。在一种实施例中, 用户的在线状态可以由游戏守护进程 2020 可访问的服务(例如, 由以上提到的朋友服务或者由单独的“存在”服务) 来监视。

[0222] 游戏框架 2000 的一种实施例提供了组合邀请 / 匹配操作, 其中用户可以邀请一个或多个朋友与一组未知的匹配参与者玩游戏。例如, 如果一个游戏需要 4 个玩家而且第一个用户邀请第二个用户玩游戏, 然后邀请服务 112 可以首先连接第一用户与第二用户, 然后匹配器服务 111 可以将第一用户和第二用户与两个(或更多个)其他玩家匹配。在这种实施例中, 游戏框架 2000 可以首先执行上述邀请序列来连接第一用户和第二用户。在一种实施例中, 一旦第一用户和第二用户已经成功连接, 游戏框架 2000 就可以实现匹配序列来识别其他用户并与其它用户连接。如以上所提到的, 在一种实施例中, 由匹配服务应用的匹配标准可以既包括第一用户又包括第二用户(例如, 第一和第二用户二者的 NAT 类型、连接类型、语言等)。作为替代, 这两个用户中一个的标准可以被评估, 以便作出匹配决策。

[0223] 一旦所有用户都连接了, 游戏框架 2000 就可以经 API 2001 向请求该连接的应用 2030 提供连接结果。同样, 响应由应用 2030 进行的相对简单的 API 调用, 游戏框架 2000 进入连接每个设备的一组复杂事务。一旦设备已经成功连接, 游戏框架 2000 就把结果提供回发出请求的应用 2030。

[0224] 如图 20 中所说明的, 游戏框架 2000 可以包括通信缓冲区 2003, 以便临时存储用户和其他游戏参与者之间的通信。通信可以包括例如文字、音频和 / 或视频通信。游戏框架 2000 可以基于每个应用 2030 的需求建立缓冲区 2003。例如, 对于利用慢网络连接的音频 / 视频通信, 可能需要相对大的缓冲区 2003。在一种实施例中, 每个应用 2030 可以经 API 2001 (例如, 利用 BUFFER(size) 命令) 进行建立某个尺寸的通信缓冲区的明确请求。作为替代, 游戏框架 2000 可以自动地基于每个应用的通信需求创建缓冲区。例如, 游戏框架 2000 可以基于是否需要支持文字、音频和 / 或视频来选择特定的缓冲区尺寸。

[0225] 在一种实施例中, 通信缓冲区 2003 可以在已在用户之间建立所有 P2P 连接之前临时存储通信流。例如, 在邀请服务 112 或匹配器服务 111 已经识别出每个用户之后但是在 CDX 服务 110 完成连接数据交换操作之前, 每个用户可以得到其他游戏参与者处于连接过程中的通知。在这个阶段, 移动设备 120 的用户可以向其他参与者发送文字、音频和 / 或视频通信流。游戏框架 2000 将在通信缓冲区 2003 中存储用于还没有连接的那些参与者的通信流。然后, 当用于每个设备的连接完成时, 游戏框架 2000 可以从缓冲区 2003 发送文字、音频和 / 或视频。

[0226] 在一种实施例中, 游戏守护进程 2020 包括用于高速缓存每个服务 2050 上持久化的数据以便减小网络流量的高速缓存 2021。例如, 如由高速缓存管理策略所规定的, 用户的朋友列表、排行榜数据、成绩数据、存在数据和简档数据可以存储在高速缓存 2021 中。在一种实施例中, 高速缓存管理策略由数据在其上存储的每个个别服务驱动。因此, 对于 n 个

不同的服务, n 个不同的高速缓存管理策略可以应用到高速缓存 2021。此外, 因为高速缓存管理策略被服务驱动, 所以它可以基于当前的网络和 / 或服务器负载条件被动态修改。例如, 在服务负荷很重的时段内(例如, 圣诞节、新产品发布日等), 服务可以动态规定具有相对不频繁的高速缓存更新的高速缓存管理策略(例如, 每 12 小时更新)。作为对比, 在服务负荷不重的时段内, 服务可以规定具有更频繁高速缓存更新的高速缓存策略(例如, 每 1/2 小时、每小时、每 2 小时等更新)。

[0227] 在一种实施例中, 高速缓存管理策略是利用用于存储在高速缓存 2021 中的某些数据记录的生存时间(TTL)值规定的。当数据记录已经存储在高速缓存中超过其 TTL 值时, 那个数据被认为是“陈旧的”而且对那个数据的本地请求可以直接转发到与那个数据关联的服务。在一种实施例中, 请求包括识别该数据的当前版本的 ID 码。如果该 ID 码与服务上的 ID 码匹配, 则数据仍然有效而且不需要更新。然后, 响应可以从服务发送回去, 指示高速缓存中的数据是当前的而且用于该数据记录的 TTL 值可以重置。

[0228] 除了使用如上所述的高速缓存管理策略, 在一种实施例中, 用于某些类型数据的高速缓存更新可以利用推送通知服务 1050 推送到移动设备。例如, 对用户朋友列表或者对用户朋友当前在线状态的改变可以动态地推送到用户的移动设备 120。推送通知可以由游戏守护进程 2020 接收, 然后, 游戏守护进程 2020 可以更新高速缓存 2021, 以便包括由服务推送的数据的相关部分(即, 可能不需要更新高速缓存中与那种服务关联的所有数据)。作为对比, 有些推送通知可以指示游戏守护进程 2020 重写高速缓存的全部内容(或者高速缓存中至少与执行推送的服务关联的部分)。

[0229] 利用推送来更新高速缓存 2021 的那些服务可以选择相对高的 TTL 值(和 / 或可以不设置 TTL 值), 因为他们具有推送通知来更新高速缓存 2021 中所储存数据的能力。在一种实施例中, 每个服务都规定一组可以触发推送通知高速缓存更新的事件。例如, 高速缓存更新事件可以包括对朋友在线状态的改变、新朋友请求、朋友请求的接受、去掉朋友操作、一个朋友在玩一个特定游戏的指示、朋友达到的游戏成绩、对特定排行榜中前 10 名的更新或者被认为对担保高速缓存更新足够重要的任何其它事件。以这种方式利用推送通知来更新高速缓存 2021 可以减小网络与服务负荷, 因为, 利用推送更新, 移动设备与服务之间周期性的轮询不需要了。

[0230] 游戏框架 2000 的一种实施例基于用户的国家和 / 或地理位置唯一地格式化呈现给终端用户的数据。例如, 像当前日期、时间和币值的值可以为处于不同国家与位置的用户不同地呈现。作为例子, 在美国, 日期格式可以是 [月日, 年] (例如, 4 月 25 日, 2010 年), 而在其它国家, 日期格式可以是 [日月, 年] (例如, 25 日 4 月, 2010 年)。类似地, 当在美国和某些其它国家表示时间时, AM/PM 指定可以使用而且在小时和分钟之间可以使用冒号(例如, 3:00PM)。作为对比, 许多其它国家不使用 AM/PM 命令和 / 或在小时和分钟之间使用逗号(例如, 15, 00)。作为另一个例子, 世界上许多地方使用米制系统, 而世界上有些地方不使用(例如, 美国)。应当指出, 这些是可以由本发明某些实施例使用的简单说明性例子。本发明的基本原理不限于任何特定的数据格式设置。

[0231] 在一种实施例中, 这些不同的数据格式可以在显示排行榜数据、成绩数据、朋友数据和 / 或游戏框架 2000 处理的任何其它数据的时候被选择。游戏框架 2000 可以用各种方式确定用户的国家和 / 或地理位置。例如, 在一种实施例中, 这种信息是在用户的简档数据

中简单提供的和 / 或可以基于用户的蜂窝服务提供商确定。用户的位置也可以利用例如全球定位系统(GPS)跟踪来确定。

[0232] 与地理位置和 / 或国家无关的其它类型数据格式化也可以由游戏框架 2000 管理。例如,当显示排行榜数据时,知道最低得分应当把用户放在排行榜顶部还是底部是很重要的。对于有些游戏(例如,高尔夫、田径、赛车、滑雪等),越低的数字指示越好的表现,而在其它游戏(例如,足球、棒球等)中,越高的数字指示越好的表现。因而,在一种实施例中,应用 2030 规定将经 API2001 使用的得分类型(例如,“升序”或“降序”)。然后,游戏框架 2000 可以使用适当的标签设置和格式化来显示得分。

[0233] 游戏框架 2000 的一种实施例还基于用户与用户朋友之间的关系过滤用户数据。例如,本发明的一种实施例允许“详细”视图、“朋友”视图和“公共”视图。在一种实施例中,详细视图可以由拥有该数据(即,用户的个人信息)的用户使用;朋友视图可以由用户的朋友使用;而公共视图可以由所有其他用户使用。

[0234] 作为例子,公共视图可以简单地包括与每个用户关联的“别名”名字、该别名玩的游戏和关联的得分及玩游戏的日期 / 时间。这种信息可以由游戏框架 2000 用于填充公共排行榜,然后排行榜可以经游戏中心 2031 显示。

[0235] 朋友视图可以包括来自通用视图的所有信息及要在用户的朋友中间共享的任何附加信息,包括例如用户所拥有的游戏;用户玩的游戏;用户的战绩与得分;用户有多少朋友;那些朋友的身份;识别用户头像的 URL 和 / 或用户的在线状态,这仅仅是几个例子。在一种实施例中,“朋友”视图提供了要与朋友共享的缺省信息集合,但是终端用户可以调整这个缺省配置并且特别地规定要由每个个别朋友或朋友组(例如,同事、家庭成员、大学 / 高中时代的朋友等)共享的信息类型。

[0236] “详细”视图可以包括来自“公共”和“朋友”视图的所有信息及由各种服务 2050 代表终端用户管理的任何其它信息。作为例子,这可以包括用户的所有简档数据;用户的通用唯一标识符(“UUID”)(本文中有时候称为“玩家 ID”);玩家名字;别名名字;游戏的个数和游戏的身份;用户的朋友;用户的所有成绩等。

[0237] 在有些情况下,应用 2030 可能只需要关于每个用户的少量信息,例如每个用户的玩家 ID。例如,在一种实施例中,当匹配被请求时,游戏框架 2000 可能最初只需要每个玩家的 ID。当匹配器服务进行匹配时(见上面),游戏框架 2000 可以确定任何匹配的用户是否是朋友(例如,经与朋友服务的通信和 / 或通过询问用户的本地朋友数据)。如果是,则游戏框架 2000 可以检索附加的用户数据并且把那种数据提供给任何匹配的朋友。以这种方式,游戏框架 2000 基于用户的身份和每个用户之间的关系过滤信息。

[0238] 在一种实施例中,如果两个用户不具有朋友关系的话,则游戏框架 2000 首先在一用户和第二用户之间提供公共视图。但是,在一种实施例中,游戏框架 2000 允许第一用户向第二用户发送朋友请求(例如,利用第二用户的别名)。如果接受了朋友请求,则游戏框架 2000 将向每个用户提供附加的信息(例如,缺省的“朋友”视图)。

[0239] 不同 API 实施例

[0240] 在一种实施例中实现的 API 是由软件组件(下文中称为“API 实现软件组件”)实现的、允许不同的软件组件(下文中称为“API 调用软件组件”)访问并使用由 API 实现软件组件提供的一个或多个函数、方法、过程、数据结构和 / 或其它服务的接口。例如,API 允许

API 调用软件组件的开发者(这可以是第三方开发者)充分利用由 API 实现软件组件提供的规定特征。可以有一个 API 调用软件组件或可以有多于一个这种软件组件。API 可以是计算机系统或程序库为了支持对来自软件应用的服务的请求而提供的源代码接口。API 可以关于编程语言来规定, 编程语言可以在建立应用的时候被解释或编译, 而不是对数据如何在存储器中布置的明确低级描述。

[0241] API 定义了当访问和使用 API 实现软件组件的规定特征时 API 调用软件组件所使用的语言和参数。例如, API 调用软件组件通过 API 暴露的一个或多个 API 调用(有时候称为函数或方法调用)访问 API 实现软件组件的规定特征。响应来自 API 调用软件组件的 API 调用, API 实现软件组件可以通过 API 返回值。虽然 API 定义了 API 调用的语法与结果(例如, 如何启用 API 调用及 API 调用做什么), 但 API 一般不揭示 API 调用如何实现由 API 调用规定的功能。各种函数调用或消息经调用软件(API 调用组件组件)和 API 实现软件组件之间的一个或多个应用编程接口传送。传送函数调用或消息可以包括发布、启动、启用、调用、接收、返回或者响应函数调用或消息。由此, API 调用软件组件可以传送调用而且 API 实现软件组件可以传送调用。

[0242] 作为例子, API 实现软件组件 2010 和 API 调用软件组件可以是操作系统、库、设备驱动器、API、应用程序或者其它软件模块(应当理解, API 实现软件组件和 API 调用软件组件可以是彼此相同或不同类型的软件模块)。API 调用软件组件可以是本地软件组件(即, 与 API 实现软件组件在相同的数据处理系统上)或者是经网络通过 API 与 API 实现软件组件通信的远端软件组件(即, 与 API 实现软件组件在不同的数据处理系统上)。应当理解, API 实现软件组件也可以充当 API 调用软件组件(即, 它可以对不同的 API 实现软件组件暴露的 API 进行 API 调用), 而 API 调用软件组件也可以通过实现暴露给不同 API 调用软件组件的 API 来充当 API 实现软件组件。

[0243] API 可以允许用不同编程语言编写的多个 API 调用软件组件与 API 实现软件组件通信(因而, API 可以包括用于在 API 实现软件组件与 API 调用软件组件之间翻译调用与返回的特征);但是, API 可以关于具体的编程语言来实现。

[0244] 图 21 说明了包括实现 API2120 的 API 实现软件组件 2110(例如, 操作系统、库、设备驱动器、API、应用程序或者其它软件模块)的 API 体系结构的一种实施例。API2120 规定可以由 API 调用软件组件 2130 使用的 API 实现软件组件的一个或多个函数、方法、类、对象、协议、数据结构、格式和 / 或其它特征。API2120 可以规定至少一个调用惯例, 该调用惯例规定 API 实现软件组件中的函数如何从 API 调用软件组件接收参数并且该函数如何把结果返回到 API 调用软件组件。API 调用软件组件 2130(例如, 操作系统、库、设备驱动器、API、应用程序或者其它软件模块)通过 API2120 进行 API 调用, 以便访问并使用 API 实现软件组件 2110 中由 API2120 规定的特征。响应 API 调用, API 实现软件组件 2110 可以通过 API2120 把值返回到 API 调用软件组件 2130。

[0245] 将认识到, API 实现软件组件 2110 可以包括没有通过 API2120 规定而且 API 调用软件组件 2130 不可用的附加函数、方法、类、数据结构和 / 或其它特征。应当理解, API 调用软件组件 2130 可以在与 API 实现软件组件 2110 相同的系统上或者可以远离 API 实现软件组件 2110 并且经网络利用 API2120 访问它。虽然图 21 说明了与 API2120 交互的单个 API 调用软件组件 2130, 但是应当理解, 用与 API 调用软件组件 2130 不同语言(或者相同语言)

编写的其它 API 调用软件组件也可以使用 API2120。

[0246] API 实现软件组件 2110、API2120 和 API 调用软件组件 2130 可以存储在机器可读介质中,该机器可读介质包括用于以机器(例如,计算机或者其它数据处理系统)可读的形式存储信息的任何机制。例如,机器可读介质包括磁盘、光盘、随机存取存储器、只读存储器、闪存存储器设备等。

[0247] 在图 22 中(“软件堆栈”),一种示例性实施例,应用可以利用几个服务 API 对服务 1 或 2 进行调用并且利用几个 OS API 对操作系统(OS)进行调用。服务 1 和 2 可以利用几个 OS API 对 OS 进行调用。

[0248] 应当指出,服务 2 有两个 API,其中一个(服务 2API1)从应用 1 接收调用并向其返回值,而另一个(服务 2API2)从应用 2 接收调用并向其返回值。(可以是例如软件库的)服务 1 对 OS API1 进行调用并从其接收返回的值,而(可以是例如软件库的)服务 2 对 OS API1 和 OS API2 都进行调用并从其接收返回值。应用 2 可以对 OS API2 进行调用并从其接收返回值。

[0249] 示例性数据处理设备

[0250] 图 23 是说明在本发明一些实施例中可以使用的示例性计算机系统的框图。应当理解,虽然图 23 说明了计算机系统的各种组件,但它不是要代表互连组件的任何特定体系结构或方式,因为这种细节对于本发明没有密切关系。将认识到,具有更少组件或更多组件的其它计算机系统也可以与本发明一起使用。

[0251] 如图 23 中所说明的,数据处理系统形式的计算机系统 2300 包括与处理系统 2320、电源 2325、存储器 2330 和非易失性存储 2340 (例如,硬驱、闪存存储器、相变存储器 (PCM) 等)耦合的总线 2350。总线 2350 可以通过本领域中众所周知的各种桥接器、控制器和 / 或适配器彼此连接。处理系统 2320 可以从存储器 2330 和 / 或非易失性存储器 2340 检索指令,并且执行指令,以便如上所述地执行操作。总线 2350 把以上组件互连到一起并且把那些组件互连到可选的扩展坞 2360、显示器控制器 & 显示器设备 2370、输入 / 输出设备 2380 (例如,NIC (网络接口卡)、光标控制(例如,鼠标、触摸屏、触摸板等)、键盘等)和可选的无线收发器 2390 (例如,蓝牙、WiFi、红外线等)。

[0252] 图 24 是说明可以在本发明有些实施例中使用的示例性数据处理系统的框图。例如,数据处理系统 2400 可以是手持式计算机、个人数字助理(PDA)、移动电话、便携式游戏系统、便携式媒体播放器、可以包括移动电话、媒体播放器和 / 或游戏系统的平板或手持式计算设备。作为另一个例子,数据处理系统 2400 可以是网络计算机或者另一个设备中的嵌入式处理设备。

[0253] 根据本发明的一种实施例,数据处理系统 2400 的示例性体系结构可以用于上述移动设备。数据处理系统 2400 包括处理系统 2420,这可以包括集成电路上的一个或多个微处理器和 / 或系统。处理系统 2420 与存储器 2410、电源 2425 (包括一个或多个电池)、音频输入 / 输出 2440、显示器控制器和显示器设备 2460、可选的输入 / 输出 2450、输入设备 2470 和无线收发器 2430 耦合。将认识到,在本发明的某些实施例中,未在图 24 中示出的附加组件也可以是数据处理系统 2400 的一部分,而在本发明的某些实施例中,可以使用比图 24 中所示更少的组件。此外,将认识到,如在本领域中众所周知的,未在图 24 中示出的一种或多种总线可以用于互连各种组件。

[0254] 存储器 2410 可以存储数据和 / 或程序, 供数据处理系统 2400 执行。音频输入 / 输出 2440 可以包括麦克风和 / 或扬声器, 以便例如通过扬声器和麦克风播放音乐和 / 或提供电话功能。显示器控制器和显示器设备 2460 可以包括图形用户界面(GUI)。无线(例如, RF)收发器 2430 (例如, WiFi 收发器、红外线收发器、蓝牙收发器、无线蜂窝电话收发器等)可以用于与其它数据处理系统通信。一个或多个输入设备 2470 允许用户向系统提供输入。这些输入设备可以是键区、键盘、触摸面板、多点触摸面板等。可选的其它输入 / 输出 2450 可以是用于扩展坞的连接器。

[0255] 用于管理跨不同服务提供商的 P2P 连接的实施例

[0256] 在本发明的一种实施例中, 上述体系结构扩展成允许位于不同服务提供商的对等体建立对等(P2P)连接, 诸如实时的音频、视频和 / 或聊天连接。因为不同的服务提供商可以使用他们自己的协议和他们自己的客户端 ID 命名空间, 所以本发明的这些实施例提供了允许设备互操作的技术, 而不管所使用的协议, 并且把命名空间集成到单个全局的命名空间中。

[0257] 可以维护一个全局数据库, 以便对所有系统上的所有用户跟踪全局命名空间。但是, 给定跨服务提供商散布的大量用户, 全局数据库方法可能是难以管理的。作为替代, 用于识别用户和 / 或数据处理设备的名字(例如, 用户 ID、电话号码)可以广播到所有其它服务提供商, 以便识别谁会对所请求的连接作出响应。但是, 同样, 这种系统不能很好地扩展(即, 用于每个尝试的连接的广播消息将消耗显著的带宽量)。

[0258] 为了解决以上问题, 本发明的一种实施例使用布隆过滤器在连接尝试过程中定位相关的服务提供商。这种实施例将关于图 25-26 中所示的体系结构来描述。在图 25 中说明了四个服务提供商 - 服务提供商 A2510、服务提供商 B2511、服务提供商 C2512 和服务提供商 D2513。就像在前面的实施例中, 每个服务提供商管理一个注册数据库 2520-2523, 这些数据库包含一组用户的用户 ID 和 / 或电话号码, 其中为这些用户提供来自服务提供商的数据通信服务。作为例子, 在图 25 中, 为用户 A-C2501-2503 提供来自服务提供商 A2510 的服务, 并且为用户 D-F 提供来自服务提供商 D2513 的服务。如前面所描述的, 在一种实施例中, 注册数据库 2520-2523 把电话号码或用户 ID 映射到每个用户的数据处理设备的推送令牌。因而, 由服务提供商维护的服务器使特定服务提供商的用户能够利用上述技术定位并建立彼此的对等(P2P)连接(见例如图 10-14 和关联的文字)。作为一个例子, 由服务提供商维护的服务器允许用户彼此建立音频 / 视频聊天会话, 诸如 FaceTime™ 聊天会话(由本专利申请受让人设计的一种技术)。

[0259] 除了在服务提供商自己的用户之间启用 P2P 连接, 图 25 和 26 中所说明的实施例还使得不同服务提供商的用户能够彼此建立 P2P 连接。特别地, 如图 26 中所示, 每个服务提供商都包括用户位置服务 2600、2610, 以用于首先查询服务提供商的注册数据库 2520、2523, 以便确定一个特定的用户是否由该服务提供商管理。(为了简化, 在图 26 中只说明了两个服务提供商(提供商 A 和 D))。如果用户 A2501 请求与同一服务提供商管理的另一用户 - 例如, 用户 B2502 - 的 P2P 连接, 则服务提供商 A 的用户位置服务 2600 将从注册数据库识别用户 B 并且向用户 B 发送连接请求(例如, 与从注册数据库 2520 检索出的用户 B 的推送令牌一起)。

[0260] 但是, 如果用户 A 请求与不同服务提供商管理的用户 - 例如, 用户 F2506 - 的 P2P

连接，则服务提供商 A2510 的位置服务 2600 将尝试利用从每个其它服务提供商接收到的布隆过滤器 2601-2603 在不同的服务提供商定位用户 F。特别地，如图 26 中所说明的，每个服务提供商都包括布隆过滤器发生器 2650、2651，用于基于其注册数据库 2520、2523 的当前内容生成布隆过滤器。如本领域技术人员已知的，布隆过滤器是空间有效的概率数据结构，用于测试一个元素是否是一个集合的成员。假阳性是有可能的，但假阴性是不可能的。在本文所述的实施例中，用于生成每个布隆过滤器的“元素”是每个用户的用户 ID 和 / 或电话号码。在图 26 中，例如，服务提供商 A2510 的布隆过滤器发生器 2650 使用其所有用户 ID (Andy123、Tom456 等) 生成其布隆过滤器 2604。类似地，服务提供商 D2513 的布隆过滤器发生器 2651 使用其注册数据库中的所有用户 ID (Woody123、Rick456 等) 生成其布隆过滤器 2603。在一种实施例中，每个服务提供商都以这种方式生成其自己的布隆过滤器并且周期性地把布隆过滤器发送到所有其它服务提供商。然后，每个服务提供商可以使用从其它服务提供商接收到的布隆过滤器来测试并确定特定用户是否是由其它服务提供商管理的。

[0261] 作为例子，在图 26 中，如果具有用户 ID Andy123 的用户 A2501 尝试与具有用户 ID Woody123 的用户 F2506 建立 P2P 会话(例如，个人音频 / 视频聊天)，则服务提供商 A2510 的用户位置服务 2600 可以首先尝试在其自己的注册数据库 2520 中定位用户 F 的用户名，Woody123。如果不成功，则在一种实施例中，它将查询其它服务提供商的布隆过滤器 2601-2603，尝试定位管理用户 ID “Woody123”的服务提供商。如所提到的，布隆过滤器可能提供假阳性但不会提供假阴性。因而，如果布隆过滤器指示服务提供商 B 和 C 不管理 Woody123，则服务提供商 A 将明确地知道 Woody123 不受这些服务提供商管理。在所说明的例子中，布隆过滤器查询指示 Woody123 可能由服务提供商 D 管理，而且还可能指示 Woody123 由一个或多个其它服务提供商管理。因而，在一种实施例中，服务提供商 A 将向有可能管理这个用户 ID 的每个服务提供商发送启动消息(例如，邀请用户 F 到 P2P 会话的 INVITE 命令)。事实上管理这个用户 ID 的服务提供商将肯定地对服务提供商 A 作出响应。一旦正确的服务提供商已经识别出它自己 - 在这个例子中是服务提供商 D - 这两个服务提供商就可以充当它们各自用户(在这个例子中是用户 A 与 F)的代理并且在用户之间打开通信信道。一旦用户 A 与 F 已经交换了连接数据，他们就可以打开彼此直接的 P2P 通信信道(例如，通过利用以上关于图 11 所述的技术交换和 / 或实现标准的互联网连接建立(“ICE”)事务)。作为替代，如果直接的 P2P 连接不可行(例如，因为不兼容的 NAT 类型)，则用户 A 和 F 可以利用图 13 中所说明的中继服务 1051 打开中继连接(也见图 12 和关联的文字)。

[0262] 在一种实施例中，预期每个服务提供商都持续地更新其自己的布隆过滤器并且把该布隆过滤器发送到参与的每个其它服务提供商，以便支持 P2P 音频 / 视频连接。更新可以按规律的间隔(例如，每小时、每天等一次)发生和 / 或在一定数量的新用户 ID 添加到注册数据库之后发生。本发明的基本原理不限于在服务提供商之间交换布隆过滤器的任何特定机制。

[0263] 用于生成并更新布隆过滤器的方法的一种实施例在图 27 中示出。该方法可以在图 25-26 所示的体系结构上执行，但是不限于任何特定的系统体系结构。在 2701，更新位于特定服务提供商的用户注册数据库。例如，新用户 ID/ 电话号码可以添加而且旧用户 ID/ 电话号码可以删除。在 2702，新布隆过滤器利用用户 ID/ 电话号码的完整集合生成。在 2703，新布隆过滤器发送到参与的服务提供商。

[0264] 使用布隆过滤器为一个客户端定位服务提供商的方法的一种实施例在图 28 中示出。该方法可以在图 25-26 所示的体系结构上执行,但是不限于任何特定的系统体系结构。在 2801,接收一组参与的服务提供商的布隆过滤器。布隆过滤器可以存储在易失性存储器中,供有效访问,和 / 或持久化到非易失性存储位置。在 2802,从用户(在这个例子中是用户 A)接收与另一个用户(用户 F)建立 P2P 连接的连接请求。在 2803,对用户 F 的用户 ID(例如,以上例子中的 Woody123)执行布隆过滤器功能,以便排除某些服务提供商。如果布隆过滤器功能对特定的布隆过滤器返回阴性结果,则用户 F 不被那个特定的布隆过滤器管理。但是,如果对一个布隆过滤器返回阳性结果,则存在与该布隆过滤器关联的服务提供商管理用户 F 的合理机会。如果只返回了一个阳性结果,则在 2804,连接邀请发送到那个服务提供商。如果返回了多个阳性结果,则在 2804 单独的连接邀请可以发送到每个相关的服务提供商。

[0265] 然后,用户 F 在其具有注册的服务提供商肯定地响应,而且这两个服务提供商可以在 2806 充当代理,以便允许用户交换连接数据,如上所述(例如,推送令牌、公共 / 私有网络地址 / 端口、NAT 类型等)。如果多于一个服务提供商肯定地响应(意味着两个服务提供商支持具有相同用户 ID 的用户),则可以采取附加的步骤来识别正确的用户(例如,比较电话号码、真实名字、网络地址或关于期望与其建立连接的用户的其它已知信息)。

[0266] 一旦识别出用户 F 的正确服务提供商,并且交换了必要的连接数据,就在 2807,直接 P2P 连接或中继连接(如果必要的话)在用户 A 与用户 F 之间建立,如上所述。

[0267] 如以上关于图 11-12 所提到的,在本发明的有些实施例中,用于在两个(或更多个)用户之间建立 P2P 连接的各个服务器不需要在连接过程中维护任何连接状态信息。这包括,例如,邀请服务 112 和连接数据交换服务 110。相反,在这些实施例中,包括但不限于公共 / 私有 IP 与端口(有时候通称为网络信息)、NAT 类型、用户 ID、推送令牌等的完整连接状态被累积并与每个后续的用户事务一起发送。如图 29 中所说明的,多提供商背景下与每个事务一起发送的一个附加状态信息块是提供商 ID 码。

[0268] 转向图 29 的具体细节,用户 A 发送启动请求 2901(有时候在本文中称为“邀请”请求),这包括利用上述技术确定的其自己的网络 ID(ID-A)、其自己的网络信息(例如,公共 / 私有 IP / 端口数据、NAT 类型等)、其自己的推送令牌(令牌 -A),及用于用户 F 的 ID 码、电话号码和 / 或其它类型的标识符。启动请求最初是由用户 A 的服务提供商接收的,该服务提供商可以实现以上关于图 25-28 所述的任何技术,以便定位用户 F 的服务提供商(例如,利用布隆过滤器排除某些服务提供商)。(为了简化,用户 A 和用户 F 的服务提供商在图 29 中未说明。)

[0269] 在一种实施例中,一旦识别出用户 F 的服务提供商,启动推送操作 2902 就从用户 F 的服务提供商发送到用户 F,这个操作包括用户 A 的服务提供商 - 在这个例子中是“提供商 A” - 的标识符。提供商 A 的标识符可以像 N 位识别码一样简单(例如,16 位、32 位、64 位等)。作为替代,提供商 A 的标识符可以包括识别提供商 A 的网络网关的公共 IP 地址或者连接到提供商 D 所需的其它联网数据。不管用于利用 P2P 连接事务序列识别提供商 A 的格式,本发明的基本原理保持相同。

[0270] 在一种实施例中,推送事务 2902 由推送通知服务,诸如以上讨论的推送通知服务 1050(见例如图 11 和关联的文字),生成。如所提到的,用户 A 提供的所有原始状态信息和

服务提供商 A 的服务器收集的任何附加状态信息都包括在启动推送事务 2902 中。

[0271] 在图 29 所示的例子中, 用户 F 用包含所有先前状态信息 (ID-A、NetInfo-A、提供商 A) 连同建立 P2P 连接所需的用户 F 的信息的接受事务 2903 作出响应, 其中, 作为例子但不是限制, 用户 F 的信息包括用户 F 的 ID (ID-F)、用户 F 的网络信息 (NetInfo-F; 这可以包括公共 / 私有 IP 地址 / 端口、NAT 类型等) 和用户 F 的令牌 (令牌 -F)。用于用户 A 和用户 F 的所有连接状态信息是由用户 F 的服务提供商 (在这个例子中是“提供商 D”) 接收的, 该提供商把其自己的提供商 ID 码附连到事务 (提供商 -ID) 并且把它转发到用户 A 的服务提供商。如以上对提供商 A 所描述的, 用于提供商 D 的标识符可以像 N 位的标识码一样简单。作为替代, 提供商 D 的标识符可以包括识别提供商 D 的网络网关的公共 IP 地址或者连接到提供商 D 所需的其它联网数据。不管用于利用 P2P 连接事务序列识别提供商 D 的格式, 本发明的基本原理保持相同。

[0272] 一旦所有连接状态数据都被用户 A 接收到 (包括提供商 -D 数据), 用户 A 和用户 F 就可以利用上述技术建立 P2P 连接, 如由事务 2905 所指示的。

[0273] 如以上所讨论的, 在某些条件下, 用户 A 和用户 F 可能需要通过中继服务 1051 建立连接 (见例如图 10), 而不是直接 P2P 连接。如图 30 中所说明的, 在一种实施例中, 服务提供商 A 和 F 都可以使用它们自己的中继服务 3001-3002 (和 / 或与第三方中继服务有关系)。在一种实施例中, 如果用户 A 与用户 F 之间所尝试的 P2P 连接失败, 则服务提供商 A 的中继服务 3001 (即, 启动该 P2P 连接的用户的提供商) 用于支持该连接。在一种备用实施例中, 用户 F 的中继服务 3002 (即, 请求与其连接的用户的提供商) 用于支持该连接 (如由图 31 中用户 A2501、中继服务 3002 和用户 F2506 之间的点线所指示的)。在还有另一种实施例中, 所有提供商都对单一中继服务意见一致并且使用那个中继服务在用户之间建立 P2P 连接。

[0274] 本发明的一种实施例组合多种不同的通信协议来支持用户设备之间的安全音频 / 视频 P2P 通信。这些协议包括 (但不限于) 数据报传输层安全 (DTLS) 协议, 以便经 P2P 连接提供安全通信; 安全实时传输协议 (或 SRTP), 该协议定义 RTP (实时传输协议) 的简档, 要对单播 (设备到设备) 和多播 (设备到多个设备) 应用的 RTP 数据都提供加密、消息认证和完整性及重放保护; 及会话启动协议 (SIP), 以便在用户设备之间建立语音 / 视频连接。这些协议可以在本文所述本发明的任何实施例背景下采用。

[0275] 在一种实施例中, 在图 25 中所说明的开放、提供商之间的网络上的每个设备将可以让其它设备安全地识别, 用于利用 STRP 的身份验证和流的端到端加密。需要由每个服务提供商发布以便启用安全通信的证书格式在下面描述。

[0276] 在一种实施例中, 每个提供商将需要知道如何发现其他的对等体提供商。在一种实施例中, 存在查询调用路由和对等体信息的提供商的全局和安全列表。这是可信任服务器及其寻址信息的列表。其中一个提供商可以托管这种服务。

[0277] 以下描述的是提供商之间验证并信任它们之间的连接所需的安全性与认证级别。这可以是与在提供商与全局查找数据库之间所使用的及认证 P2P 连接所使用的那些不同的凭证集合。

[0278] 在一种实施例中, 在呼叫路由时, 接收方的提供商 (即, 被呼叫的用户) 提供对等体证书, 以便返回到呼叫者, 用来验证端点之间的 P2P 连接。这种证书可以能够由外部实体签署而且证书要求可以允许任何类型的身份, 而不仅仅是电子邮件。

[0279] 此外,在一种实施例中,音频、视频和信令数据经单个数据端口在每个数据处理设备上多路复用到一起。然后,音频、视频和信令数据在目的地设备多路分解并解码。

[0280] 图 25 中所说明的提供商之间的网络包括多个互操作层。这些层的交互可以由各种协议规定。这种交互的目的是处理建立连接的用户请求,在用户端点(在图 25 中识别为用户 A-F2501-2506)之间执行必要的信息交换,使得他们可以建立音频 / 视频呼叫会话。

[0281] 在操作中,图 25 中所示的提供商之间的网络实现为彼此通信的一组服务器,发起请求和对请求作出响应。这些请求是转发请求所必需的协议动作,使得用户端点可以交换媒体信道连接数据并构成音频 / 视频呼叫会话。在一种实施例中,每个服务提供商管理与其用户端点的所有直接通信。

[0282] 在一种实施例中,用户端点是经识别控制端点的一方的统一资源标识符(URI)表示的。最初被支持的 URI 方案是 tel :(对于电话号码)和 mailto :(对于电子邮件地址)。其它的 URI 方案在未来可能会被支持。

[0283] 在一种实施例中,URI 到每个用户端点的映射不是身份映射;它是多对多的关系。单个 URI 可以映射到多个端点,而且单个端点可以被多个 URI 映射到。此外,URI 到端点的映射可以跨多个提供商。例如,在提供商 A 上可以有一个端点,并且在提供商 B 上有一个不同的端点,而且这两个端点都可以被相同的 URI 映射。(但是,在一种实施例中,端点可以一次只能由单个提供商托管。)在一种实施例中,端点 URI 是一般性的用户级标识符,像电话号码与电子邮件地址。这些到提供商与端点的映射是由系统执行的,并且是对终端用户透明的。

[0284] 在一种实施例中,用于图 25 中所说明的提供商之间的通信的元协议是 HTTP 上的词典。在这种实施例中,所有动作都是作为 HTTP GET 或 POST 执行的。如果动作被规定为 HTTP GET,则主体将是空的。如果动作被规定为 HTTP POST,则主体将包含编码为词典的请求参数。响应将具有包含编码为词典的响应参数的主体。在一种实施例中,词典的初始编码是 Apple XML 属性列表。诸如 JSON 或协议缓冲区的其它编码也可以使用。在一种实施例中,不同的服务提供商可以使用任何协议或通信机制集合与个别的用户设备通信。

[0285] 在一种实施例中,采用提供商发现协议,以便允许图 25 中所示的服务提供商彼此发现。在一种实施例中,自展引导(bootstrap)URI 由网络的管理实体(例如,主要或管理服务提供商)发布。这种自展引导 URI 指向包含作为这个网络的被接受成员的提供商的集合的发现目录。对于每个服务提供商,这个词典都包含识别信息,及规定如何与这个提供商通信的进一步的 URI。在一种实施例中,当服务提供商启动后,并且在之后周期性地,它们检索发现词典。然后,它们把它们自己配置成基于词典中的信息与其它提供商通信。

[0286] 现在将描述用于在用户之间建立 P2P 通信会话的特定协议集合的细节。但是,应当指出,这些具体细节只是代表特定的实施例而不是为了遵循本发明的基本原理所必需的。

[0287] 1. 邀请协议

[0288] 一种实施例的邀请协议用于初始呼叫设置。这是由用户端点(例如,图 25 中的用户端点 2501-2506)使用的带外信令,以便交换媒体信道连接数据,这种数据将用于为视频呼叫会话建立媒体信道。

[0289] 1.1 动作

- [0290] 在邀请协议中有四个主要动作。
- [0291] 1. 1. 1 邀请
- [0292] 由启动端点发送,以便开始呼叫。
- [0293] 字段 :session-id, self-uri, self-token, self-blob, peer-uri。
- [0294] 1. 1. 2 接受
- [0295] 由接收端点发送,以便指示它愿意参与该呼叫。
- [0296] 字段 :session-id, self-uri, self-token, self-blob, peer-uri, peer-token, peer-blob。
- [0297] 1. 1. 3 拒绝
- [0298] 由接收端点发送,以便指示它不愿意参与该呼叫。
- [0299] 字段 :session-id, self-uri, self-token, self-blob, peer-uri, peer-token, peer-blob。
- [0300] 1. 1. 4 取消
- [0301] 由任何一个端点发送,以便指示呼叫应当终止。
- [0302] 字段 :session-id, self-uri, self-token, self-blob, peer-uri, peer-token, peer-blob。
- [0303] 1. 2 动作变量
- [0304] 依赖于为动作提供服务的一方,这些可以采取三种形式 :
- [0305] * 请求(从端点到提供商)
- [0306] * 转发(从提供商到提供商)
- [0307] * 推送(从提供商到端点)
- [0308] 1. 3 呼叫流
- [0309] 1. 3. 1 用户条目
- [0310] 当一个端点希望建立连接时,它需要 URI 识别接收端点。这个 URI 最有可能从用户提供的某种信息导出,例如拨过的电话号码或者存储在地址本中的电子邮件地址。然后,端点在其托管提供商上调用启动请求。
- [0311] 1. 3. 2 启动请求
- [0312] 启动提供商看 URI,并且确定寄存被这个 URI 映射到的端点的接收提供商集合。(这个提供商集合可以包括启动提供商自己。)然后,它在所有可应用的接收提供商上调用启动转发。
- [0313] 1. 3. 3 启动转发
- [0314] 每个接收提供商确定接收端点,并且向其发送启动推送。
- [0315] 1. 3. 4 启动推送
- [0316] 接收端点得到启动推送,并且把该信息呈现给用户。(这将一般是沿着“XXX 在呼叫”的线的 UI。)如果用户决定接听该呼叫,端点就将调用接受请求。(否则,它将调用拒绝请求。)
- [0317] 1. 3. 5 接受请求
- [0318] 接收端点在其托管提供商上调用接受请求。
- [0319] 1. 3. 6 接受转发

[0320] 接收提供商向启动端点发送接受推送。

[0321] 1. 3. 7 接受推送

[0322] 启动端点得到接受推送，并且向用户指示它可以继续形成连接。在这个时候，两个端点都具有交换的媒体信道连接数据，因此它们准备好建立用于音频 / 视频呼叫会话的媒体信道。从这里开始，流利用媒体信道建立继续，如在(以下)媒体会话管理中所证明的。

[0323] 2. 调度优化协议

[0324] 如以上具体讨论的，在一种实施例中，布隆过滤器用于选择能够对启动呼叫请求作出响应的候选服务提供商。在一种实施例中，需要提供商维护代表它们当前所托管端点的所有 URI 的最近布隆过滤器。用于所有提供商的布隆过滤器可以按递增的方式分发到所有其它提供商。

[0325] 调度优化协议。当调度源发的呼叫时，提供商首先咨询所有其它提供商的布隆过滤器。根据这个，他们将获得可以实际为该呼叫提供服务的提供商的候选集合。然后，启动动作只发送到这个候选列表。

[0326] 3. 媒体会话管理

[0327] 媒体会话管理指媒体信道及在该媒体信道上运行的媒体流的设置、控制和拆卸。媒体会话管理在以下部分中具体描述。

[0328] 4. 媒体信道建立

[0329] 用于媒体信令、媒体流和会话拆卸的网络分组经媒体信道发送。媒体信道是通过 NAT 遍历或中继配置(在上面具体描述)建立。NAT 遍历与中继配置需要每个端点都拥有用于两个端点的媒体信道连接数据。

[0330] 4. 1 NAT 遍历协议

[0331] 在一种实施例中，NAT 遍历协议用于经直接的对等连接建立媒体信道。它包括交互式连接建立(ICE) 中所覆盖的技术的使用 [RFC5245]。

[0332] 4. 2 中继配置协议

[0333] 在一种实施例中，中继协议用于经中继网络建立媒体信道。在一种实施例中，它包括 TURN 的使用 [RFC5761]。

[0334] 5. 媒体信道信令

[0335] 媒体信令覆盖用于媒体协商与媒体加密的安全性设置，及用于音频和视频参数的媒体协商。

[0336] 5. 1 安全性设置

[0337] 如所提到的，在一种实施例中，数据报传输层安全性(DTLS) [RFC4347] 用于保护媒体信道上网络流量的安全通信。DTLS 协议可以实现为提供端到端的加密，使得服务提供商将不能够访问在用户之间发送的语音 / 视频分组中的加密内容。

[0338] 5. 2 媒体协商

[0339] 在一种实施例中，SIP[RFC3261] 用于协商视频呼叫会话的音频与视频参数。

[0340] 5. 3 音频与视频加密

[0341] 在一种实施例中，SRTP[RFC3711] 用于加密音频与视频有效载荷。

[0342] 6. 媒体流控制

[0343] 媒体流控制覆盖活动媒体流的管理及媒体状态变化经媒体信道的通知。

[0344] 6.1 网络适配

[0345] 在一种实施例中,实现了考虑通信信道波动的网络适配技术。特别地,用户端点可以调整流参数,诸如音频和 / 或视频位速率,以便适应变化的网络条件,诸如吞吐量的变化、分组丢失和等待时间。

[0346] 6.2 视频静音

[0347] 发送视频的端点可以静音 / 取消静音视频。通知利用 SIPMESSAGE 发送到远端端点。

[0348] 6.3 视频朝向

[0349] 发送视频的端点可以更改视频的朝向。通知利用 RFC 首部扩展信息发送到远端端点。

[0350] 6.4 视频切换

[0351] 发送视频的端点可以切换视频的来源。例如,在既包括朝前又包括朝后照相机的用户设备上,视频可以从朝前切换到朝后。通知可以利用 RTP 首部扩展信息发送到远端端点。

[0352] 6.5 挂断

[0353] 在一种实施例中,端点可以通过发送 SIP BYE 消息明确地终止活动的会话。

[0354] 7. 媒体信道拆卸

[0355] 媒体会话可以明确地或者隐含地拆卸。媒体信道的明确拆卸是经发送或接收 SIP BYE 消息进行的。隐含的拆卸可以由于网络连接丢失或差的网络性能而发生。

[0356] 8. 安全性

[0357] 8.1 证书

[0358] 在一种实施例中,图 25 中所示的提供商之间的系统中的端点之间的通信是利用公钥密码体制来保护的。每个实体(提供商和端点)具有由可信任的 CA 发布的证书,该 CA 签署其身份。这种证书包含属于该实体的 URI 及其它识别信息。证书可以在通信的时候由对方用于验证该实体的身份。

[0359] 8.2 媒体信道信令

[0360] SIP 消息可以利用 DTLS[RFC4347] 来保护。

[0361] 8.3 音频与视频

[0362] 音频与视频流可以利用 SRTP[RFC3711] 来保护。

[0363] 9. 编码

[0364] 9.1 音频

[0365] 9.1.1 音频编解码器

[0366] 音频编解码器可以与 MPEG-4 增强低延迟 AAC (AAC-ELD、ISO/IEC14496-3) 兼容。

[0367] 9.1.2 音频质量

[0368] 在一种实施例中,音频信号的声学特征是由用于宽带(WideBand)电话终端的 3GPP 规范、TS26.131 和 TS26.132 规定的。

[0369] 9.1.2 音频 RTP 有效载荷格式

[0370] 9.2 视频

[0371] 在一种实施例中,序列参数集(SPS)和图片参数集(PPS) NALU 用于在位流中携带

视频流描述。

[0372] 9.2.1 视频编解码器

[0373] 在一种实施例中,用于在图 25 中的用户之间通信的视频编解码器是 H.264 高剖面,没有 b- 框架,级别 1.2 (有效地是 QVGA15fps, 最大 300kbps)。但是,应当指出,本发明的基本原理不限于任何特定的音频 / 视频格式。

[0374] 9.2.2 视频 RTP 有效载荷格式

[0375] 如所提到的,实时传输协议(RTP)可以用于支持用户端点之间的音频 / 视频通信。如图 32 中所说明的,在一种实施例中,RFC3984 首部 3202(即,如由 RFC3984, 用于 H.264 视频的 RTP 有效载荷格式,定义的)附加到每个 12 字节的 RTP 有效载荷 3201 (包含 RTP 数据分组)。该首部规定 RTP 数据如何利用 H.264 图像描述扩展被打包。

[0376] 用于安全即时消息传输的系统与方法

[0377] 本发明的一种实施例提供了在移动设备之间为诸如即时消息传输和视频聊天的应用启用安全的对等会话的体系结构。如图 33 中所说明的,本发明的这种实施例包括用于认证用户的身份服务 3301、用于把通知推送到移动设备的推送通知服务 1050 (如前所述) 及用于在两个或更多个移动用户(在图 33 中说明了用户 A110 和 B111) 之间建立安全即时消息传输会话的安全即时消息传输服务 3302。在一种实施例中,身份服务 3301 管理活动用户 ID、认证密钥和推送令牌的用户注册目录 3302, 如上所述, 这些信息可以由通知服务 1050 用于把推送通知发送到移动设备。虽然本发明的基本原理不限于用户 ID 的任何特定类型,但是,在一种实施例中,用户 ID 是电子邮件地址。而且,单个用户可以具有用于不同应用(例如,即时消息传输、视频聊天、文件共享等)的多个用户 ID 而且可以具有不同的移动设备(例如, iPhoneTM 与独立的 iPadTM - 由本专利申请的受让人设计的设备)。

[0378] 用于建立安全的对等通信信道的计算机实现的方法的一种实施例在图 34 中说明。虽然这种方法最初将在图 33 中所示体系结构的背景下描述,但是应当指出,本发明的基本原理不限于这种特定的体系结构。

[0379] 在 3401, 用户 A 向身份服务 3301 发送包括用户 B 的标识符(例如, 用户 B 的电子邮件地址和 / 或电话号码)的查询,以便启动与用户 B 的安全通信信道。作为响应,在 3402, 身份服务 3301 确定是否有任何用户 ID 匹配该查询(例如, 用户 B 的电子邮件地址或电话号码是否在身份服务中注册)。如果没有,则在 3403, 身份服务向用户 A 发送失败通知。

[0380] 如果找到匹配,则在 3404, 用户 A 从身份服务 3301 检索用户 B 的网络地址信息与公钥。在一种实施例中,地址信息包括用于用户 B 的计算设备的令牌,由此授权用户 A 与具有这个具体地址的用户 B 讲话(设备 A 的令牌可以向 B 的令牌讲话)。如果用户 B 有多个设备,则多个令牌可以从身份服务 3301 提供(每个设备一个令牌)并且单独地路由到用户 A。

[0381] 在一种实施例中,还生成会话密钥(在本文中有时候称为“查询签名”),这是对由身份服务 3301 提供的当前时间的时间戳、用户 A 的 ID、用户 B 的 ID、用户 A 的令牌和用户 B 的令牌的一个签名。这个会话密钥随后由安全 IM 服务 3302 用于认证这两个用户,而不涉及身份服务(如下所述)。

[0382] 用户 A 现在具有寻址信息和用于这些地址单元中每一个的公钥(目标 ID/ 令牌)。在 3404, 设备 A 利用用户 A 的私钥和设备 B 的公钥加密要发送到用户 B 的消息和附件。在一种实施例中,这包括利用用户 B 的密钥加密文字 / 附件的内容并且利用用户 A 的密钥签署

内容。一旦加密了,消息就不能在位于用户 A 和用户 B 之间的任何服务器解密,虽然这些服务器能够看到所发送的消息的类型(例如,它是文字消息还是已读回执(read receipt))。作为利用用户 B 的公钥进行加密的结果,只有用户 B 可以读取消息的内容。用户 B 还可以利用用户 A 的签名验证发送方(用户 A)。

[0383] 在 3406,用户利用数据报传输层安全性(DTLS)打开与推送通知服务 1050 的安全通信信道并且把加密消息与用户 B 的令牌、用户 ID 和用户 A 的用户 ID 一起发送到推送通知服务 1050。如本领域技术人员已知的,DTLS 协议提供了通信隐私性,从而允许基于数据报的应用以设计成防止窃听、篡改或消息伪造的方式通信。与 DTLS 协议关联的具体细节是众所周知的,因此在这里不具体描述。

[0384] 在一种实施例中,用户 A 的令牌在这一步中不发送到推送通知服务 1050,而是基于用户 A 与推送通知服务 1050 的通信来推断的。在 3407,推送通知服务 1050 打开与安全即时消息传输服务 3302 的安全通信信道而且一请求就利用用户 A 的推送令牌提供安全即时消息传输服务。因而,在这个阶段,安全即时消息传输服务 3302 具有用户 B 的令牌和 ID,及用户 A 的令牌与 ID。在一种实施例中,它利用以上提到的会话密钥验证这个信息,例如,通过利用用户 B 的令牌与 ID、用户 A 的令牌与 ID 和时间戳重新生成会话密钥并且比较所生成的会话密钥与从推送通知服务 1050 接收的会话密钥。在一种实施例中,如果当前时间戳在原始时间戳之前很远,则签名将不匹配而且验证失败将发生。如果签名匹配(即,如果消息得到很好的签署),则在 3409,安全即时消息传输服务 3302 打开与推送通知服务 1050 的第二个、向外的安全通信信道,把用户 A 的推送令牌添加到消息(连同用户 B 的推送令牌与 ID 一起)并且把该消息发送到推送通知服务 1050,以交给用户 B。很显著地,在这个阶段,安全 IM 服务 3302 不需要查询身份服务 3301 进行验证,由此节省了网络带宽。

[0385] 在 3401,推送通知服务利用传输层安全性(TLS)打开与用户 B 的安全通信信道并且把消息推送到用户 B。在 3411,用户 B 执行如上对用户 A 描述的相同验证操作,以便验证并解密消息。特别地,用户 B 可以查询身份服务 3301 来检索用户 A 的公钥并且然后使用该公钥验证(先前已经利用用户 A 的私钥签署并且利用用户 B 的公钥加密的)消息。在这个阶段,用户 A 和 B 具有在 3410 建立安全 IM 会话所需的全部信息(例如,公钥和令牌)。

[0386] 在图 35 中说明的一种实施例中,关闭记录发消息(OTR)协商可以代替上述技术或者附加地使用。如本领域技术人员已知的,OTR 是为即时消息传输惯例提供强加密的一种加密协议,它使用 AES 对称密钥算法、Diffie-Hellman 密钥交换和 SHA-1 哈希函数的组合。在一种实施例中,尝试上述安全发消息技术而且,如果不成功的话,则采用图 35 中所说明的 OTR 技术。

[0387] 在 3501,用户 A 利用用户 B 的 ID(例如,电子邮件地址、电话号码等)查询身份服务并且从身份服务检索用户 B 的公钥。在 3502,用户 A 通过利用用户 B 的公钥加密生成安全 OTR 会话请求并且把该请求发送到用户 B。在 3503,用户 B 利用用户 B 的私钥解密并且,响应于该会话请求,用户 B 检索用户 A 的公钥。

[0388] 在 3504,用户 B 生成 OTR 响应,利用用户 A 的公钥加密响应。在 3505,用户 A 和 B 交换附加的 OTR 连接消息。在这个阶段交换的具体消息可以由当前的 OTR 规范定义并且因此在这里不具体描述。在 3506,一旦所有必需的连接数据都已经交换,用户 A 和 B 就可以打开彼此的安全即时消息传输通信信道。

[0389] 虽然上述实施例集中在即时消息传输实现,但是本发明的基本原理可以利用其它类型的对等通信服务,诸如对等音频和 / 或视频服务,实现。

[0390] 用于连接移动用户的身份服务的实施例

[0391] 如以上所提到的,在一种实施例中,身份服务 3301 管理活动用户 ID、认证密钥和推送令牌的用户注册目录 3302。身份服务 3301 由其它服务,诸如推送通知服务 1050 和安全即时消息传输服务 3302,用于基于人可用的输入为移动设备和用户提供有效的识别信息。特别地,在一种实施例中,身份服务包括共享的用户注册数据库 3302,该数据库具有把方便的用户可读用户 ID 码(例如,电话号码、电子邮件地址、游戏中心昵称等)映射到详细的用户 / 设备信息的表。

[0392] 在一种实施例中,单个用户 ID 可以映射到用户注册目录 3302 中的多个物理设备。例如,具有 ID tom@bstz.com 的用户可以具有多个移动设备,诸如 iPhone™ 和独立的 iPad™(由本专利申请的受让人设计的设备)和独立的笔记本 / 台式个人计算机。具有必要认证凭证的任何用户或服务可以查询身份服务来检索关于其它用户的信息。虽然为了说明的目的使用以上具体设备,但是本发明的基本原理不限于任何特定的设备类型。

[0393] 在一种实施例中,为每个设备维护的设备信息包括(1)用于设备的推送令牌(包括用于设备的网络寻址信息,如上所述)和(2)设备的能力集合。能力可以包括用于该设备的服务提供商的身份(例如,AT&T 对 Verizon)、设备版本信息(例如,软件 OS 版本和 / 或应用版本)及设备支持的一种或多种协议(例如,基于安装在该设备上的应用程序代码)。例如,如果设备安装了 Facetime™ 应用,则这种信息将由身份服务连同设备信息一起存储。此外,设备信息可以规定每个用户能够与之通信的服务类型(例如,像上述安全即时消息传输服务)。

[0394] 因而,响应于检索用户 B 的设备信息的查询,用户 A 可以从身份服务 3301 接收包含用户 B 的每个设备的上述设备信息的响应。这将有效地通知用户 A 的设备用户 A 的设备可以与用户 B 通信的不同方式。例如,如果用户 A 具有安装了正确版本的一些与用户 B 相同的通信应用(例如,相同的即时消息传输客户端、Facetime 应用、文件共享应用等),则用户 A 的设备可以使用这种信息尝试打开与用户 B 的通信信道。

[0395] 在一种实施例中,设备信息还包括识别用于每个应用的具体应用能力的一组标志。回到以上的 Facetime 例子,设备信息可以规定用户 B 的设备经 3G 网络支持 Facetime 信道。在这种情况下,用户 A 的设备可以随后尝试利用用户 B 的设备所支持的具体协议打开经 3G 网络与用户 B 的设备的通信信道。当然,以上仅仅是说明性例子,本发明的基本原理不限于应用能力或协议的任何特定集合。

[0396] 在图 36 中所说明的本发明一种实施例中,为了与身份服务交互,存在设备可以执行的四种操作:(1) 认证 ;(2) 注册 ;(3) 规范化(canonicalize);及(4) 查询。

[0397] (1) 认证

[0398] 如本文所使用的,“认证”指证明特定用户标识符(ID)的身份。在一种实施例中,所执行的认证对不同类型的 ID 码(例如,电子邮件地址、服务昵称、用户 ID 码、电话号码等)可以不同。例如,电子邮件地址的认证可以与电话号码或服务 ID 码的认证不同。

[0399] 这些操作将关于图 36 中所示的系统体系结构和图 37 中所述的方法来描述。但是,应当指出,图 37 中所说明的方法可以在不同的系统体系结构上实现,同时仍然遵循本发明

的基本原理。

[0400] 在 3701, 用户 A 把一组特定于应用的凭证发送到应用认证服务 3601。在电子邮件应用的情况下, 例如, 凭证可以包括用户 A 的电子邮件地址与密码; 在游戏应用的情况下, 这可以包括用于游戏服务的用户 ID 与密码; 而且在电话号码的情况下, 这可以包括短消息服务(SMS)签名。而且, 虽然在图 36 中说明为单独的服务, 但是应用认证服务 3601 和身份服务 3301 可以构成单个集成的服务。

[0401] 作为响应, 在 3702, 应用认证服务 3601 取得所提供的认证凭证, 给它们签名, 把它们放到认证证书中, 在本文称为“提供证书”, 并且把该提供证书发送到用户 A。在一种实施例中, 提供证书包括密码随机数(例如, 时间戳)和签名。

[0402] 除了提供证书, 在一种实施例中, 用户 A 还具有在 3703 从推送通知服务接收到的“推送证书”, 该证书包括对用户 A 的推送令牌的签名、随机数(例如, 时间戳)和用户 A 的能力列表(例如, 安装在用户 A 的设备上的具体应用)的签名。在一种实施例中, 当用户 A 的设备最初在网络上提供时, 推送证书提供给用户 A 的设备。

[0403] (2) 注册

[0404] 在 3704, 用户 A 向身份服务注册其推送证书及其提供证书并且, 在 3705, 身份服务从推送证书和提供证书提取某些预定信息, 并且为这些实体生成其自己的签名, 在本文称为用户 A 的“身份证书”, 随后这可以用于对网络上的任何服务验证用户 A 的身份(即, 不需要服务为了验证而独立地连接身份服务)。

[0405] (3) 规范化

[0406] 某些类型的用户 ID 是“嘈杂的”, 这意味着它们常常利用多种不同的格式表示。例如, 相同的电话号码可以表示为 408-555-1212、1-408-555-212 或者 4085551212。还有多种采取不同格式的国际接入码和运营商接入码。因此, 第一用户可能知道第二用户的电话号码, 但是, 给定在注册数据库 3302 中定位第二用户电话号码的当前背景(例如, 用户当前在哪里漫游, 电话号码如何格式化), 可能不知道到达该用户所需的具体格式。

[0407] 在注册数据库中存储一个特定用户 ID 的每种不同变体是低效的(即, 这将消耗显著数量的空间而且可能不能成功地捕捉到所有不同的可能格式)。因此, 为了解决这个问题, 本发明的一种实施例在把用户 ID 存储到注册数据库 3302 之前规范化用户 ID(例如, 利用一致同意的规范化格式)。

[0408] 在一种实施例中, 身份服务 3301 包括基于用户的当前背景和发出请求的设备的设置执行规范化的逻辑。例如, 在图 37 中, 用户 B 可以为身份服务 3301 提供其家庭运营商(例如, AT&T)的身份、其当前漫游运营商(例如, TMobile)、用户设置(例如, 关于是否使用国际协助的指示)和原始的目标 ID 码(例如, 非规范化形式的用户 A 的电话号码, 像 4085551212)。作为响应, 身份服务 3301 将在对注册数据库 3302 执行查询之前基于上述所有变量规范化原始目标 ID。因而, 响应于用户 B 查询身份服务, 用户 A 的规范化 ID(不是原始 ID)提供给用户 B(以下更具体地描述)。

[0409] (4) 查询

[0410] 如前面所描述的, 为了与目标用户建立安全通信信道, 用户首先查询身份服务, 以便检索用于目标用户的身份。如图 36 中所说明的, 用户 B 发送对用户 A 的身份的查询, 作为该查询的一部分发送其自己的身份证书。作为响应, 身份服务发送回 0 个或更多个身份

证书,每个证书都包括用户 A 的 ID 码(如以上提到的,以规范化的格式)、用于那个身份的推送令牌和对用户 A 的 ID 与推送令牌及用户 B 的 ID 与推送令牌生成的查询签名。

[0411] 在每次需要认证时强迫每个服务查询 IDS 将是低效的。例如,当用户 A 想向用户 B 发送消息时,上述即时消息传输服务将需要利用用户 A 的令牌与签名和用户 B 的令牌与签名来查询身份服务,这将消耗网络资源。

[0412] 为了解决这个问题,在本文所述本发明的实施例中,由身份服务为用户之间的每个事务生成一组 0 个或更多个签名而且这组签名与每个请求一起发送到每个服务。签名是关于如下元组的:源 ID、源令牌、目标 ID、目标令牌与时间戳,如上所述。因而,任何服务都可以通过对这些实体动态生成密码签名以便进行验证来自己执行验证,而不需要联系身份服务。

[0413] 此外,每个个别服务都可以关于为了让验证成功发生,时间戳需要多新来作出决定。只要验证是在从身份服务生成的原始时间戳开始的预先规定的时间窗口内发生的,事务就将被成功验证。因而,身份服务提供了允许应用服务认证用户的工具,但是不对认证应当如何发生作出决策决定(例如,时间戳需要多新)。因而,不同的应用可以具有不同的认证策略。

[0414] 身份服务的一种实施方式为查询实现了高速缓存体系结构,以便进一步减小网络流量。如图 38a-38b 中所说明的,在这种实施例中,用户 ID 的设备高速缓存 3801 在每个用户设备 111 上维护而且中间系统高速缓存 3802 在身份服务 3301 和设备 3801 之间的网络上实现,以便为身份请求提供服务并且由此减小关于身份服务的负荷。在一种实施例中,系统高速缓存 3802 是由诸如目前可以从 Akamai 和其它内容分发服务获得的内容分发网络提供的。

[0415] 如图 38a 中所说明的,如果系统高速缓存目前对用户 A 不具有有效条目,则它将把请求转发到身份服务,身份服务将用用户 A 的 0 个或更多个身份作出响应,如上所述。此外,在图 38a 所示的实施例中,身份服务生成用于用户 A 身份的指纹并且把该指纹发送回到系统高速缓存。在一种实施例中,指纹是对包括用户 A 的身份(即,A 的规范化 ID、推送令牌和时间戳)在内的实体的哈希。虽然本发明的基本原理不受任何特定类型的哈希算法限制,但是,在一种实施例中,哈希是 SHA-1 哈希。

[0416] 然后,指纹利用用户 A 的身份高速缓存在系统高速缓存上,如图 38b 中所指示的(例如,利用用户 A 的规范别名加索引)。此外,指纹与关联的 ID 可以高速缓存在用户 B 的设备上的设备高速缓存 3801 中。

[0417] 当用户 B 随后需要查询用户 A 的身份时,用户 B 将首先在设备高速缓存 3801 中查看,以确定是否存在用户 A 的身份的有效高速缓存条目。在一种实施例中,每个高速缓存条目都具有与其关联的生存时间(TTL)值(如由图 38 中所示的时间戳列所确定的)。只要对身份的请求在从该时间戳开始的规定时间窗口内发生,则设备高速缓存 3801 中的条目就是有效的而且不需要经网络的查询(即,用户 B 从设备高速缓存 3801 读取用户 A 的身份)。

[0418] 但是,如果设备高速缓存 3801 中的高速缓存条目已经到期(即,过了 TTL 值),则用户 B 向系统高速缓存 3802 发送对用户 A 的身份的查询,系统高速缓存 3802 查找用户 A 的指纹(利用用户 A 的规范化 ID 码)并且把该指纹连同对用户 A 的查询一起发送到身份服务 3301。如果指纹仍然有效,如由身份服务 3301 所确定的(例如,如果时间戳仍然在有效时间

窗口内),则身份服务 3301 唯一所需的响应是指纹有效性的指示。然后,系统高速缓存 3802 把其高速缓存的用户 A 身份的拷贝返回到用户 B,如图 38b 中所指示的。以上高速缓存技术节省了在别的情况下对用户 B 和用户 A 的身份生成一组新签名将需要的显著数量的处理资源。

[0419] 在一种实施例中,以上提到的高速缓存 TTL 值可以按每个应用为基础来配置(即,基于应用设计者的安全性偏好)。因而,例如,可以为像 FacetimeTM 的应用提供与 iChatTM 不同的 TTL 值。此外,TTL 值可以基于当前的网络条件动态设置。例如,如果网络当前流量超负荷,则 TTL 值可以动态设置成较高的值(使得高速缓存的身份更长时间有效)。此外,在一种实施例中,以上所述的所有高速缓存技术都在暴露给应用开发者的 API 中实现。因此,身份的高速缓存对使用它们的应用透明地发生。

[0420] 本发明的实施例可以包括如上所述的各种步骤。步骤可以体现在机器可执行的指令中,这些指令使通用或专用处理器执行某些步骤。作为替代,这些步骤可以由包含用于执行这些步骤的硬连线逻辑的专用硬件组件或者由编程计算机组件和定制硬件组件的任意组合执行。

[0421] 本发明的元素还可以作为用于存储机器可执行程序代码的机器可读介质提供。机器可读介质可以包括,但不限于,软盘、光盘、CD-ROM 和磁光盘、ROM、RAM、EPROM、EEPROM、磁卡或光卡或者适合存储电子程序代码的其它类型的介质 / 机器可读介质。

[0422] 贯穿以上描述,为了解释,阐述了众多具体细节,以便提供对本发明的透彻理解。但是,对本领域技术人员来说将很显然,本发明没有这些具体细节中的一些也可以实践。例如,对本领域技术人员来说将很显然,本文所述的功能性模块与方法可以实现为软件、硬件或者其任何组合。而且,虽然本发明的实施例在本文中是在移动计算环境的背景下描述的(即,利用移动设备 120-123 ;601-603),但是本发明的基本原理不限于移动计算实现。基本上任何类型的客户端或对等体数据处理设备都可以在一些实施例中使用,包括例如台式或工作站计算机。相应地,本发明的范围与主旨应当关于以下权利要求来判断。

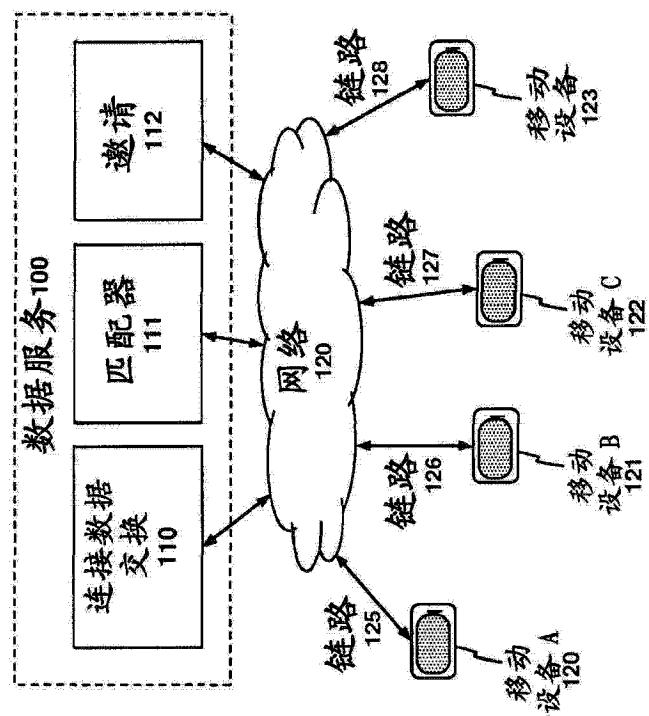


图 1

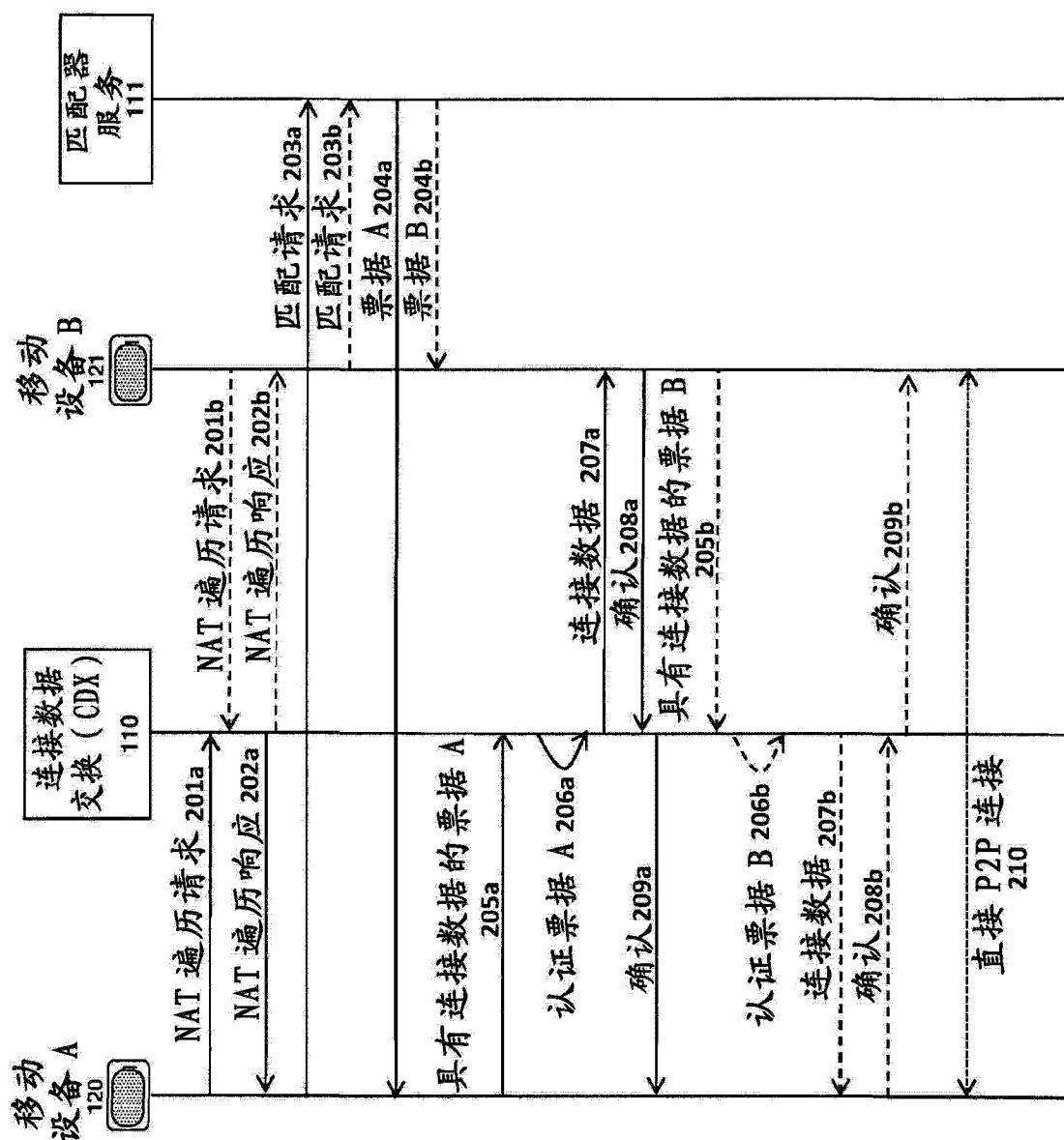


图 2a

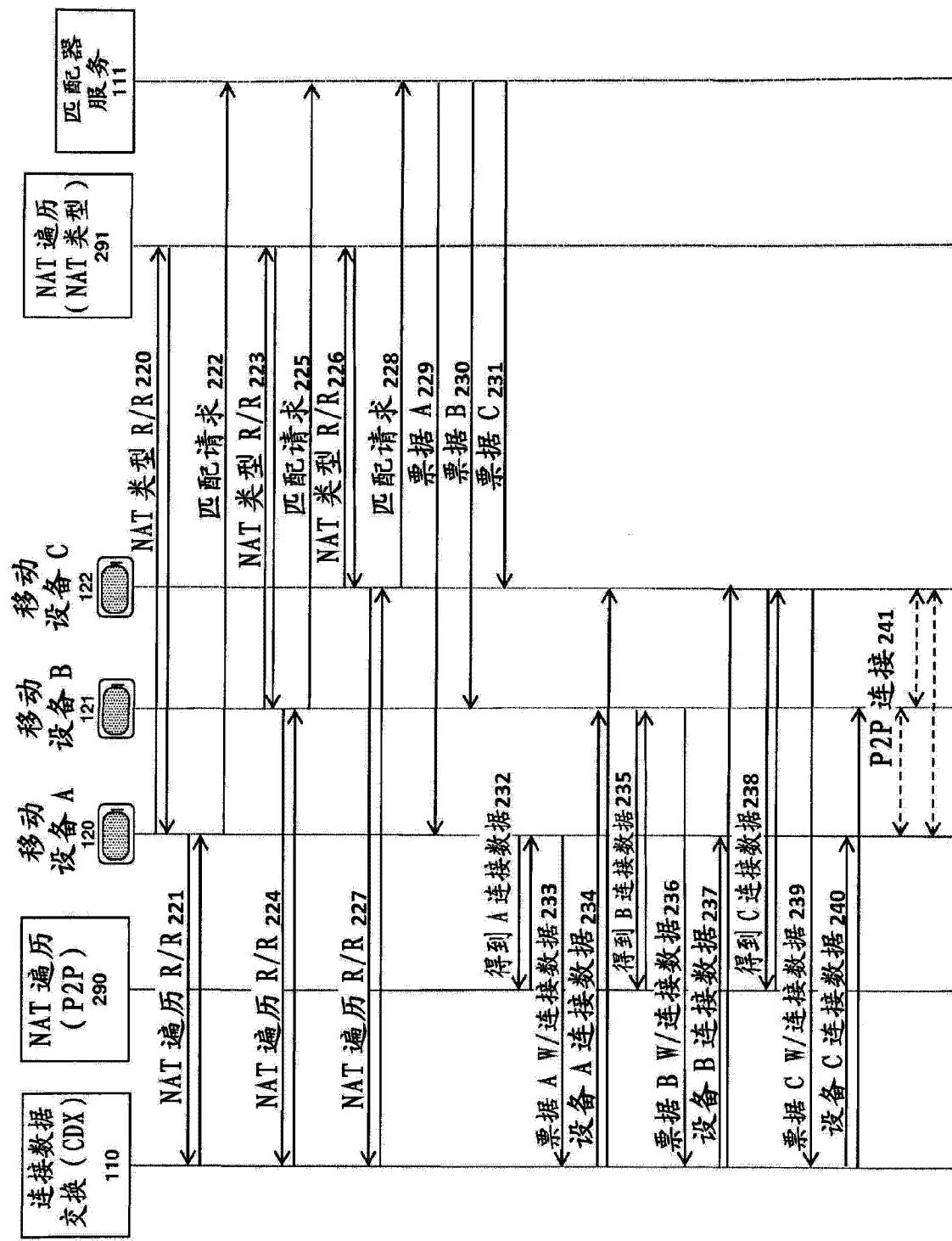


图 2b

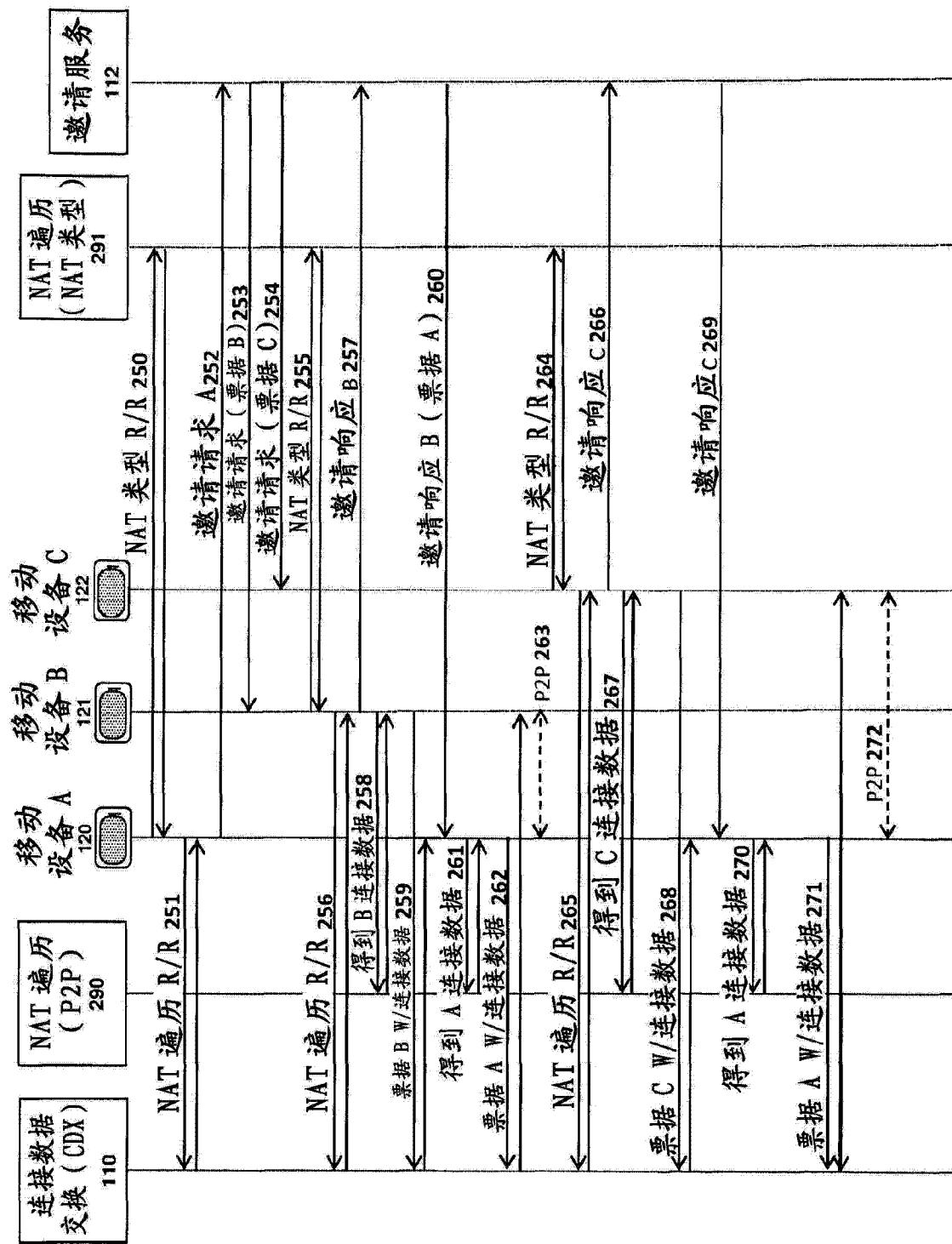


图 2c

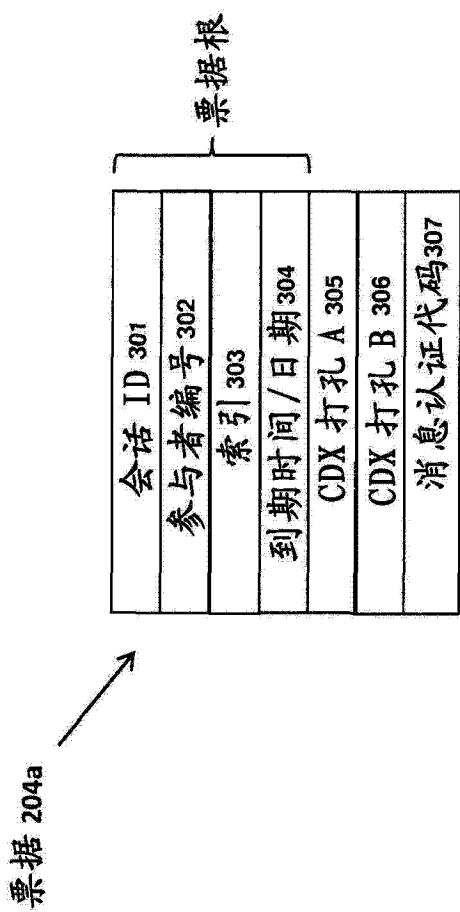


图 3

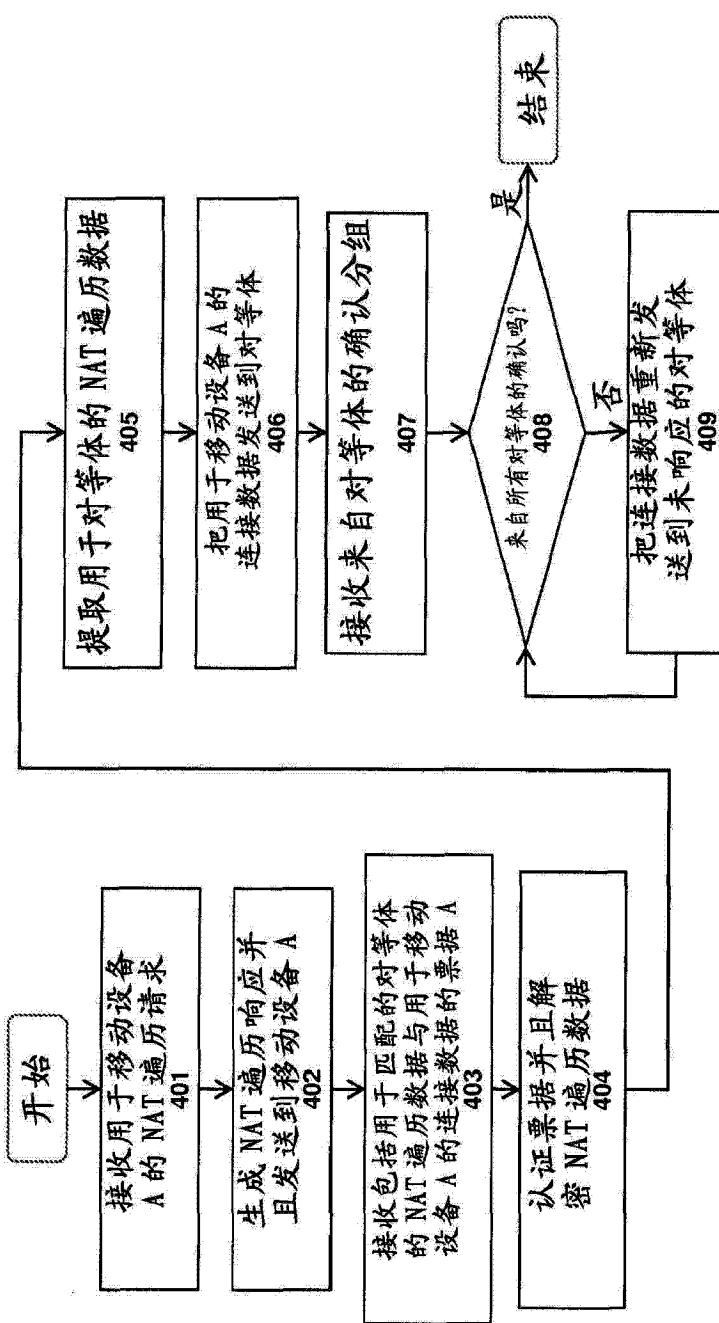
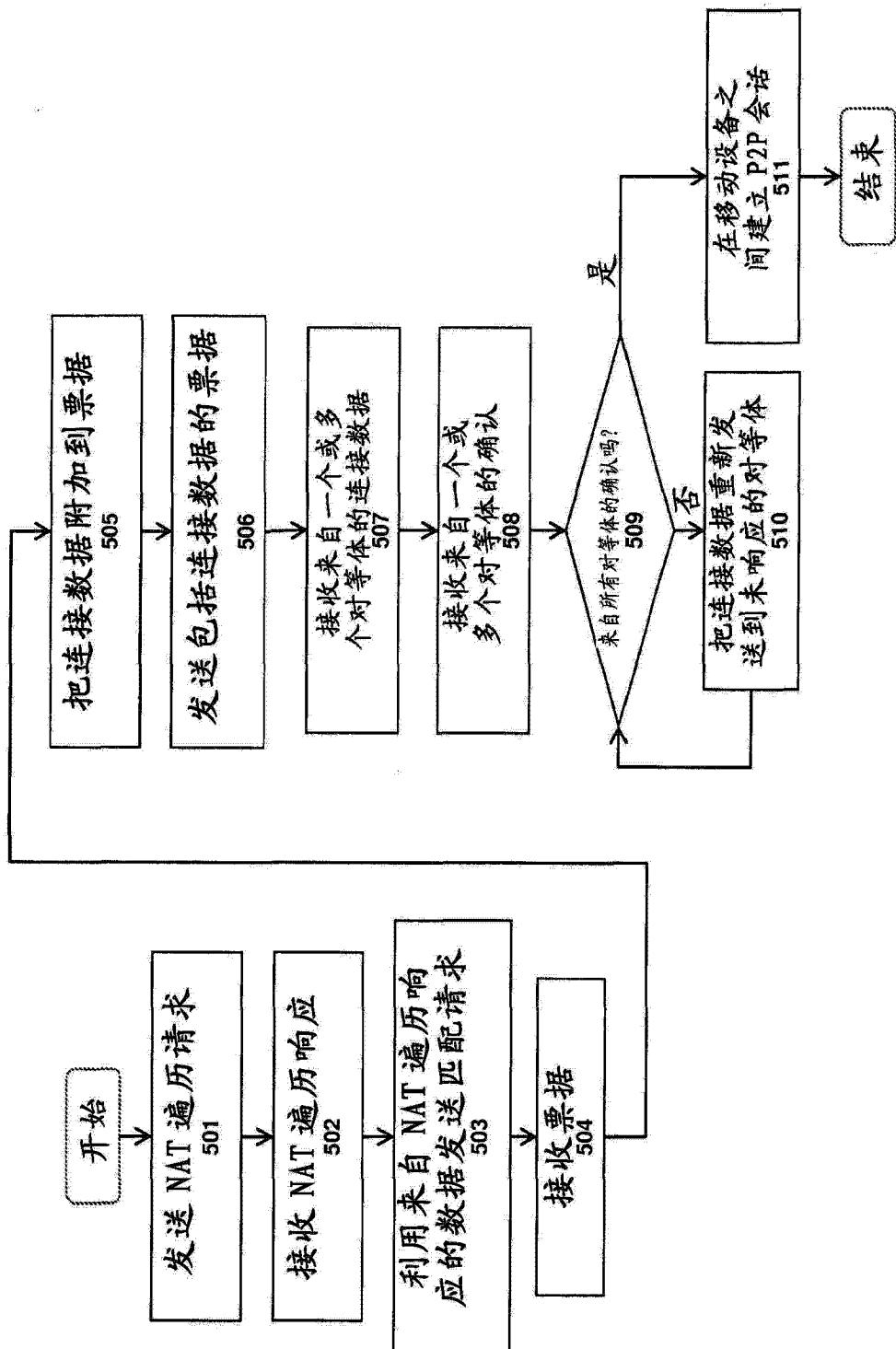


图 4



四 5

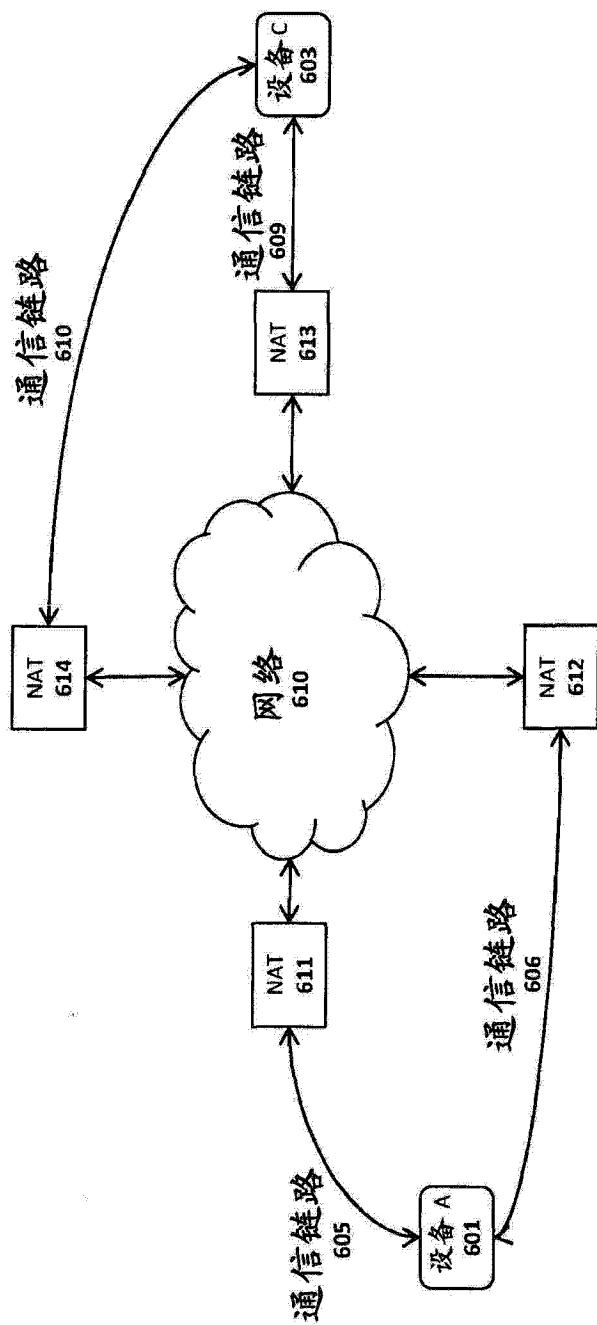


图 6

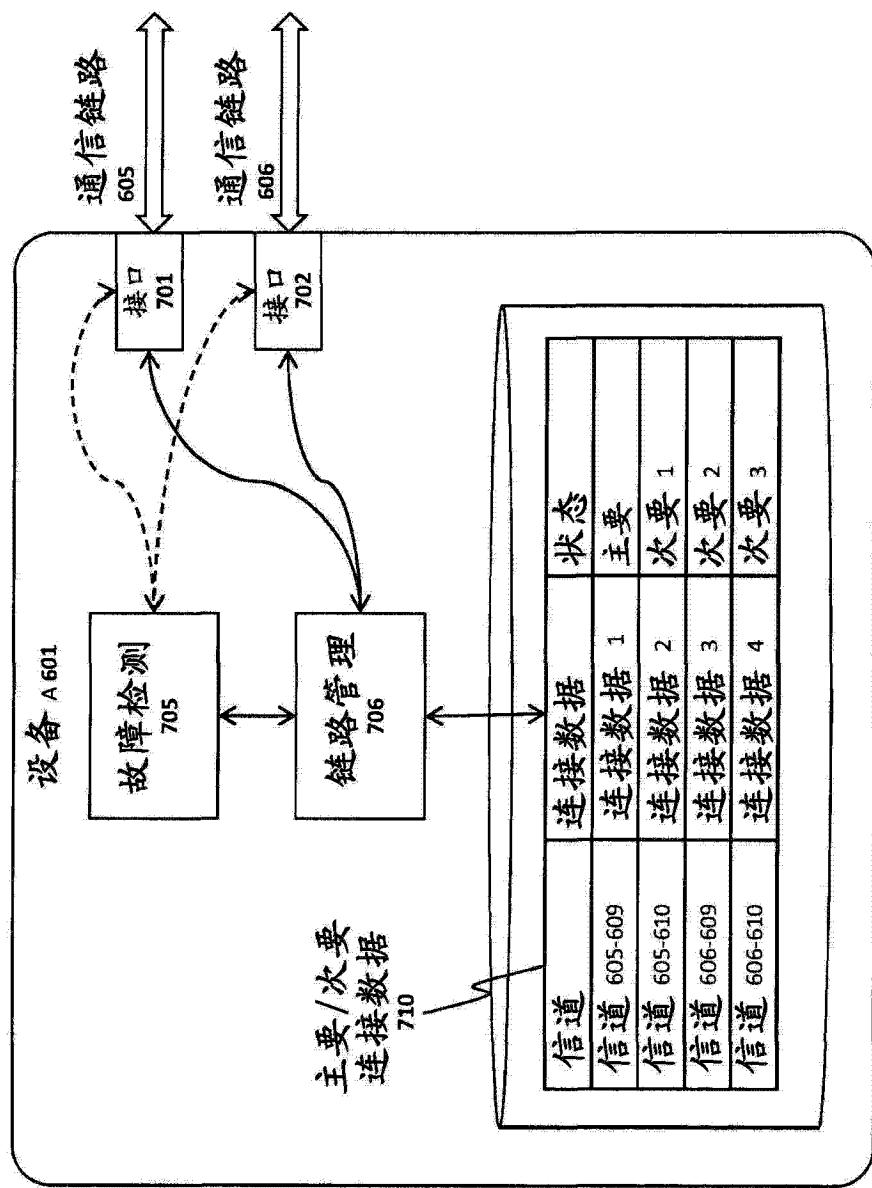


图 7

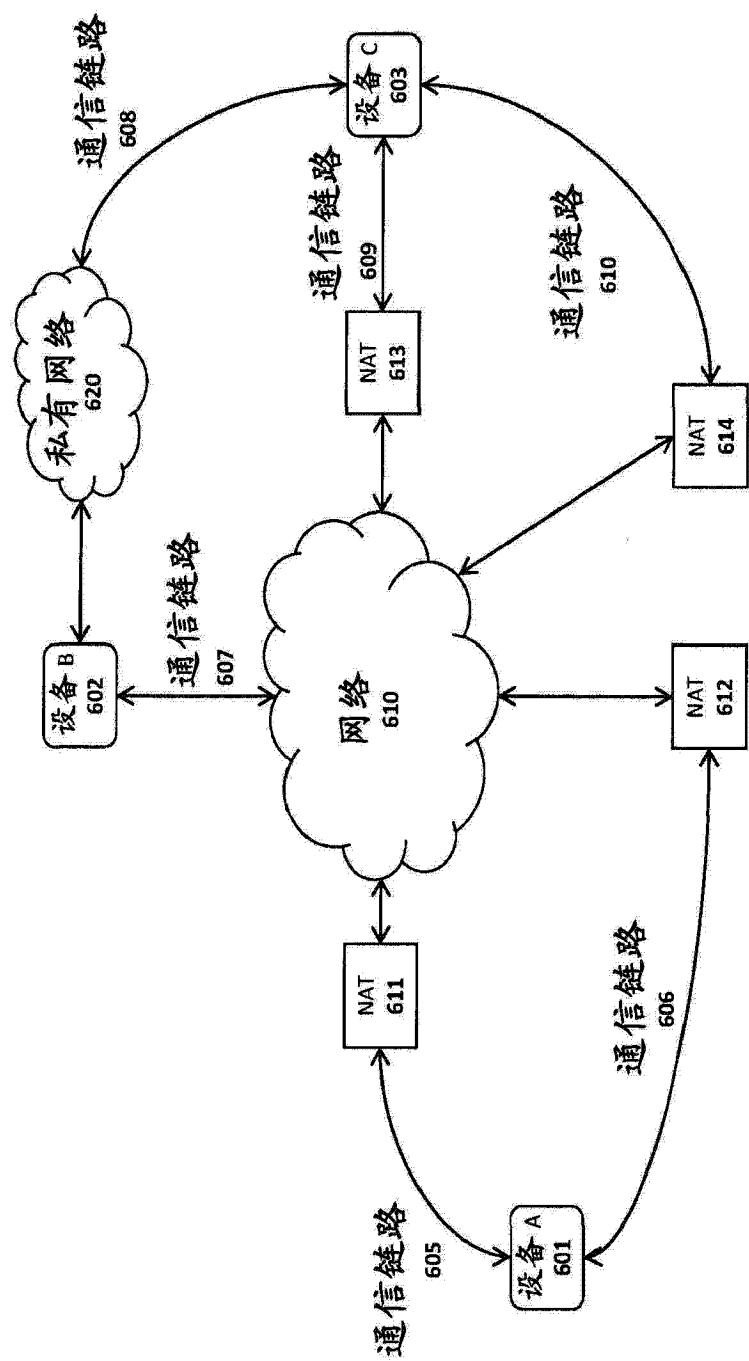


图 8a

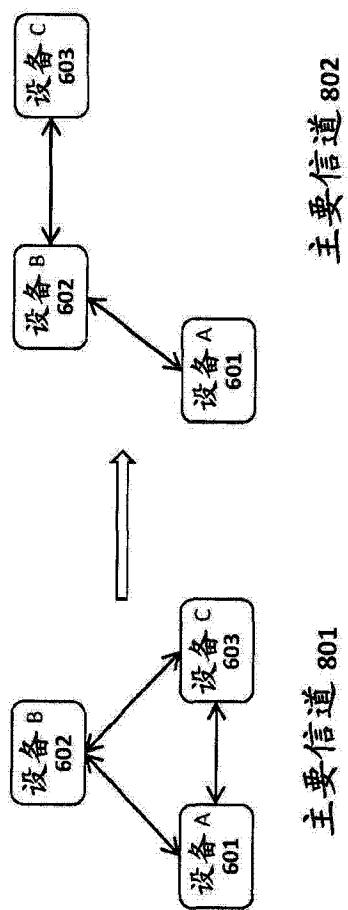


图 8b

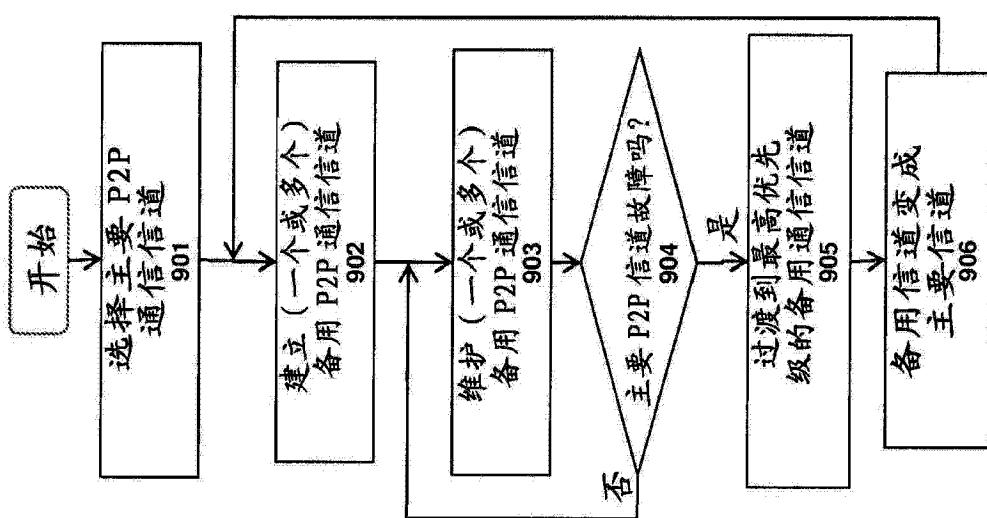


图 9

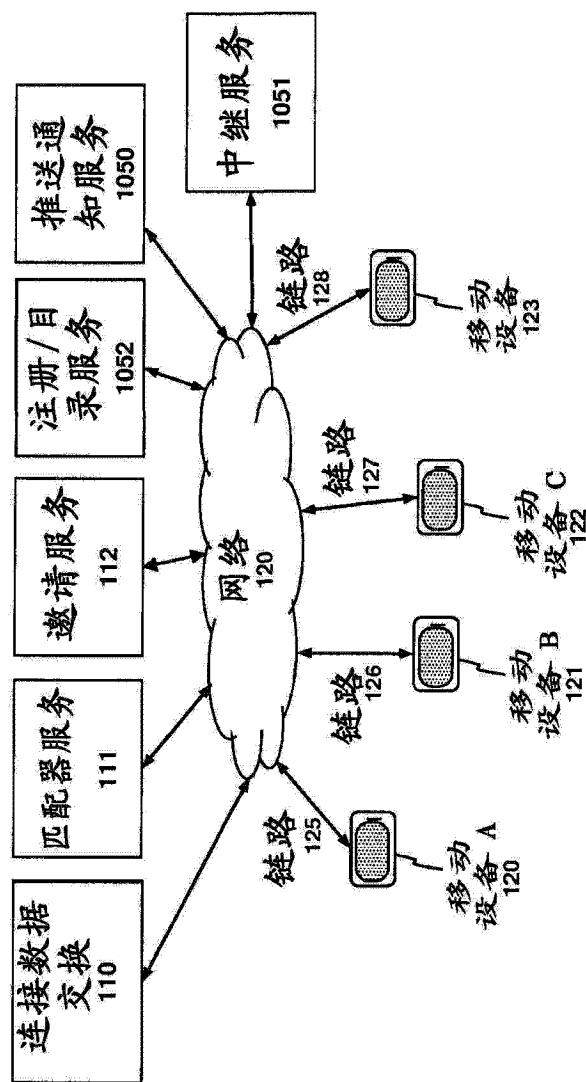


图 10

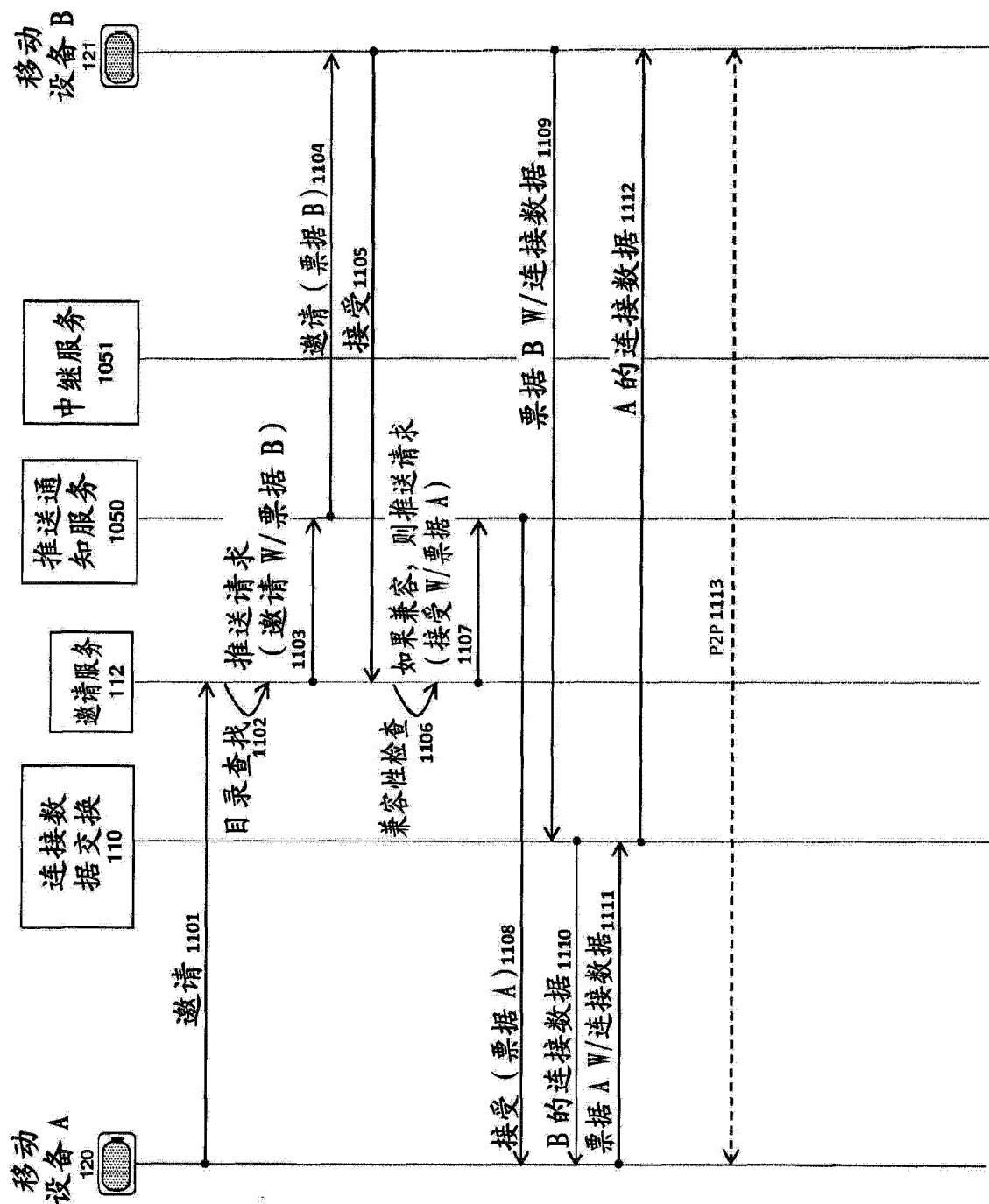


图 11

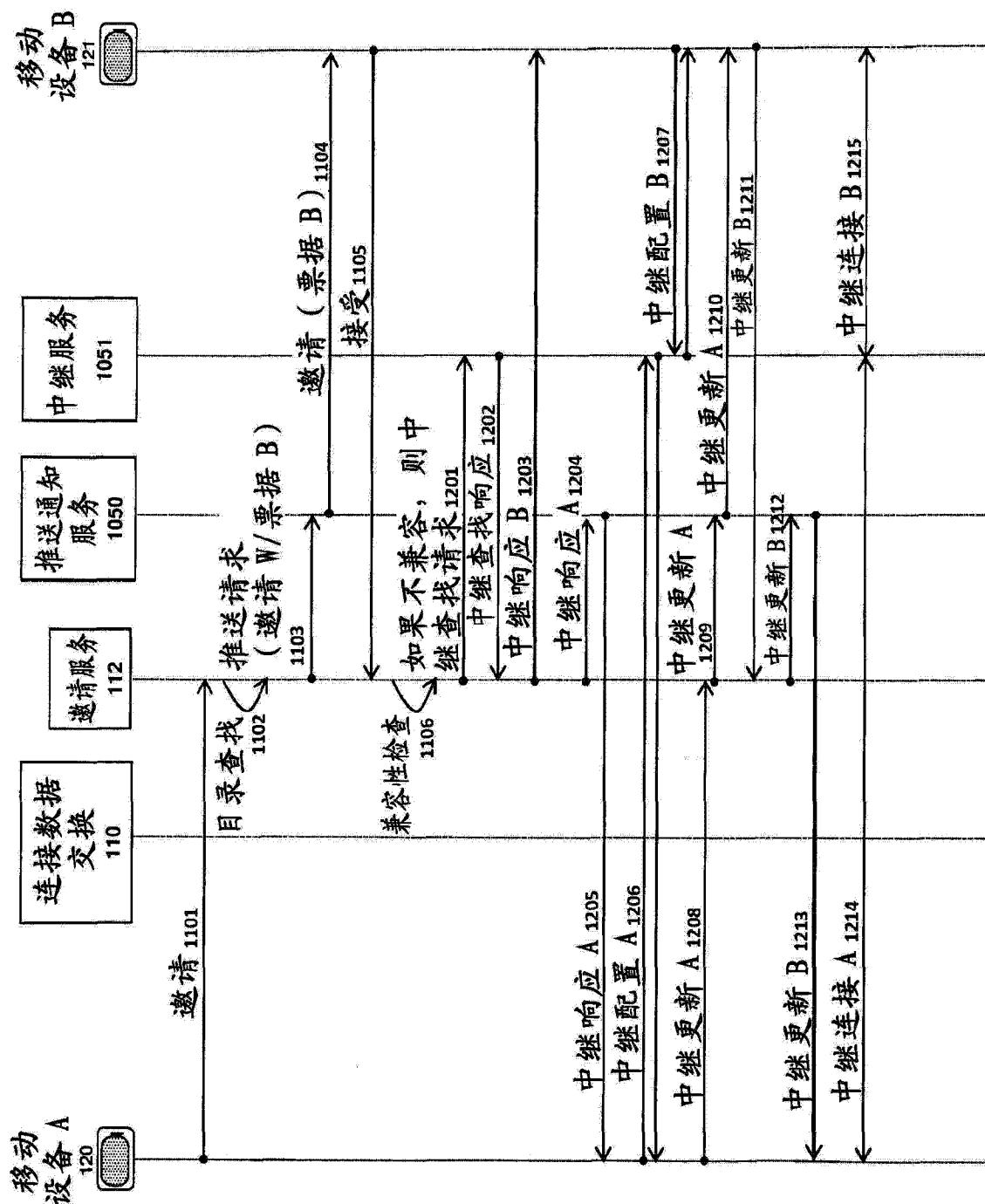


图 12

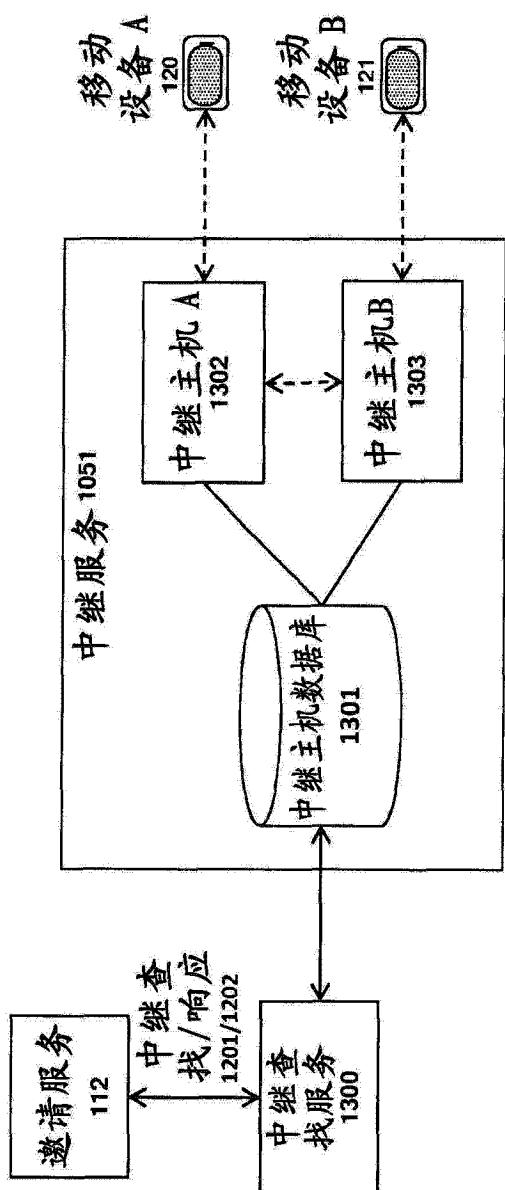


图 13

NAT 兼容性表 1400

A/B	未知	完全圆锥形	端口受限	对称	闭合
未知	0.0	1.0	0.0	0.0	0.0
完全圆锥形	1.0	1.0	1.0	1.0	0.0
端口受限	0.0	1.0	1.0	0.0	0.0
对称	0.0	1.0	0.0	0.0	0.0
闭合	0.0	0.0	0.0	0.0	0.0

图 14

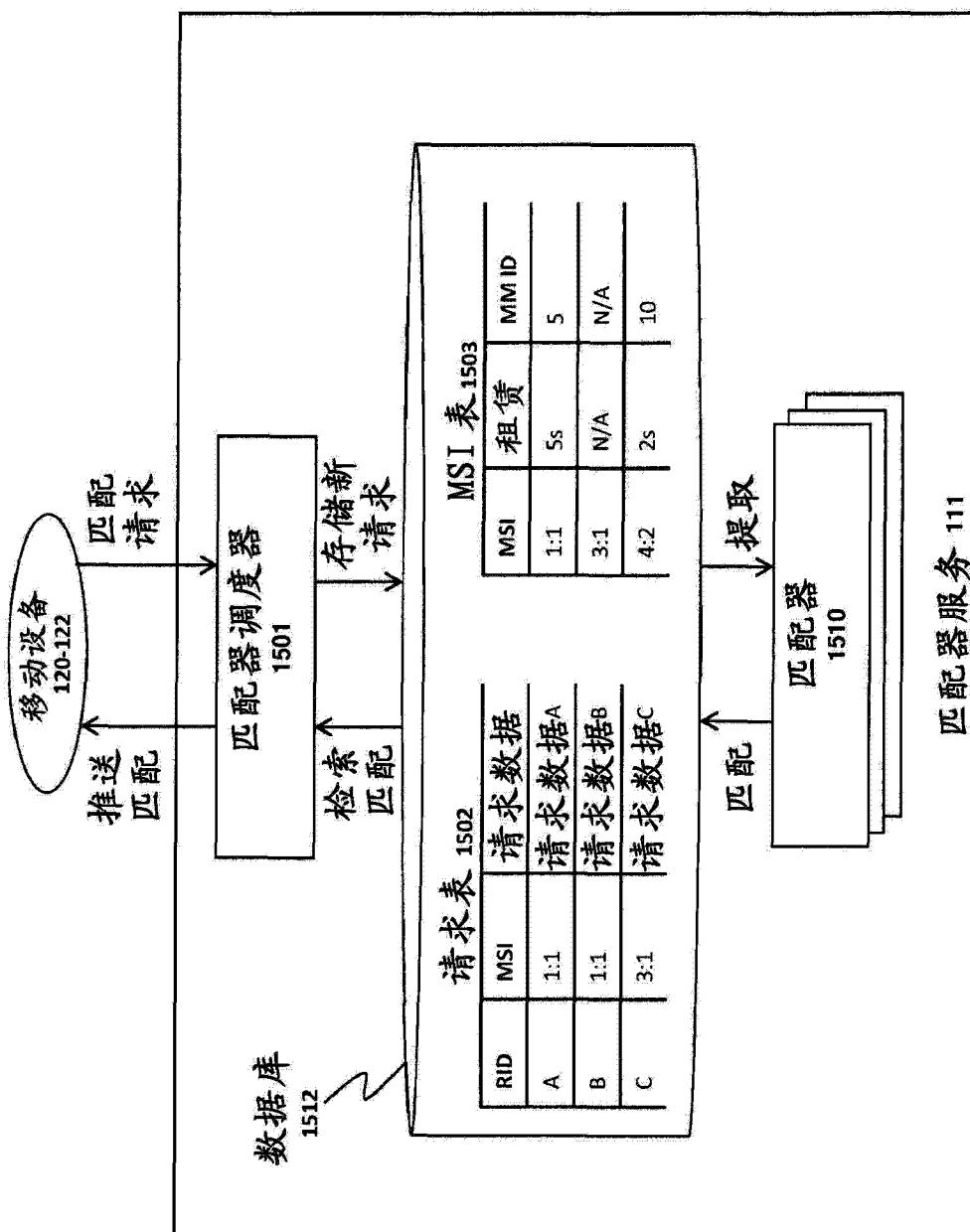


图 15

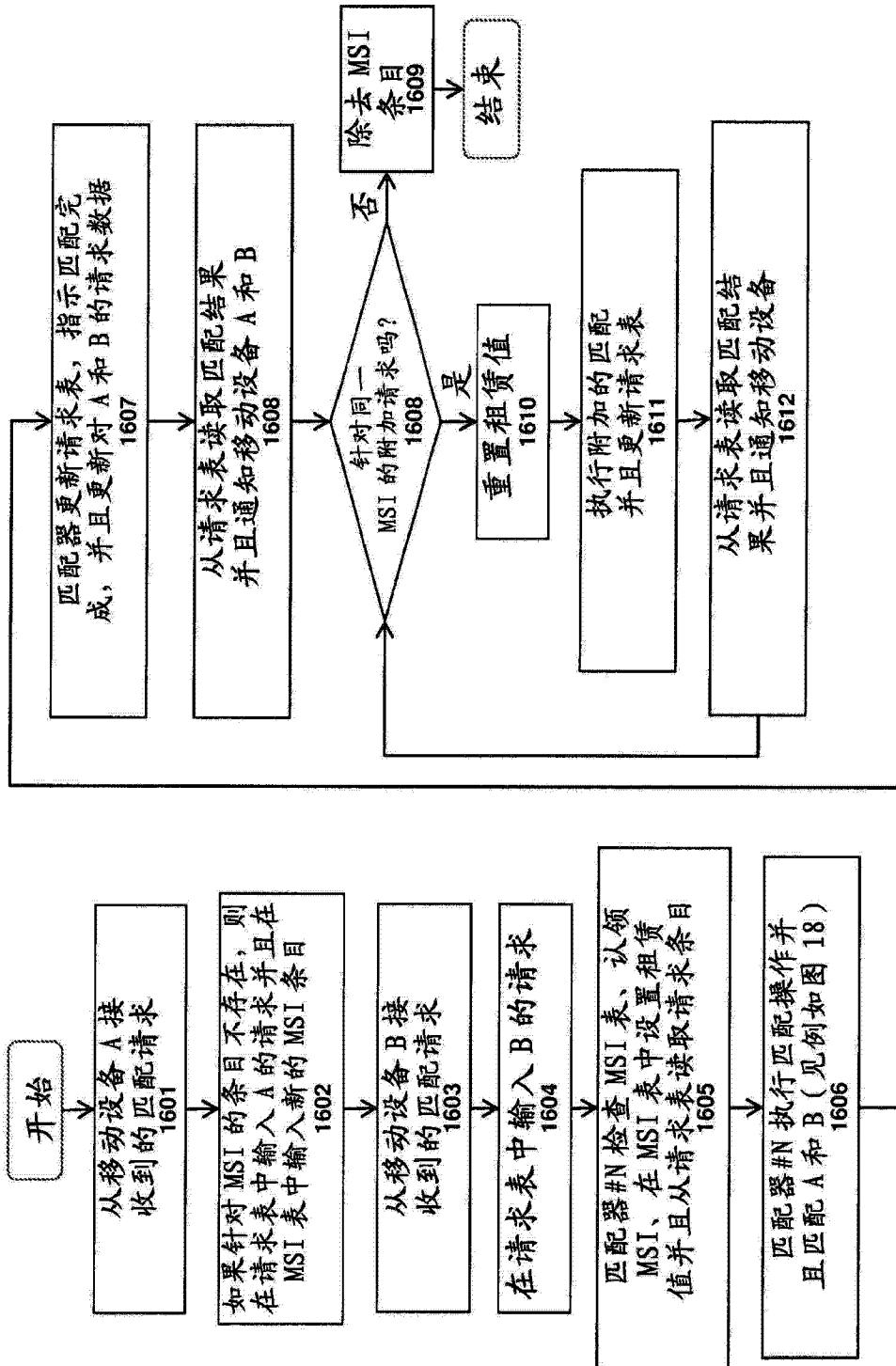


图 16

请求表 1502		
RID	MSI	请求数据
A	1:1	请求数据 A

图 17a

请求表 1502		
RID	MSI	请求数据
A	1:1	请求数据 A
B	1:1	请求数据 B

图 17b

MSI 表 1503		
	MSI	租赁
1:1	N/A	N/A

MSI 表 1503		
	MSI	租赁
1:1	N/A	N/A

MSI 表 1503		
	MSI	租赁
1:1	N/A	N/A

MSI 表 1503		
	MSI	租赁
1:1	N/A	N/A

请求表 1502		
RID	MSI	请求数据
A	完成	请求数据 B
B	完成	请求数据 A

请求表 1502		
RID	MSI	请求数据
A	完成	请求数据 B
B	完成	请求数据 A

请求表 1502		
RID	MSI	请求数据
A	完成	请求数据 B
B	完成	请求数据 A

MSI 表 1503		
	MSI	租赁
1:1	5 sec	MM#N

MSI 表 1503		
	MSI	租赁
1:1	5 sec	MM#N

MSI 表 1503		
	MSI	租赁
1:1	5 sec	MM#N

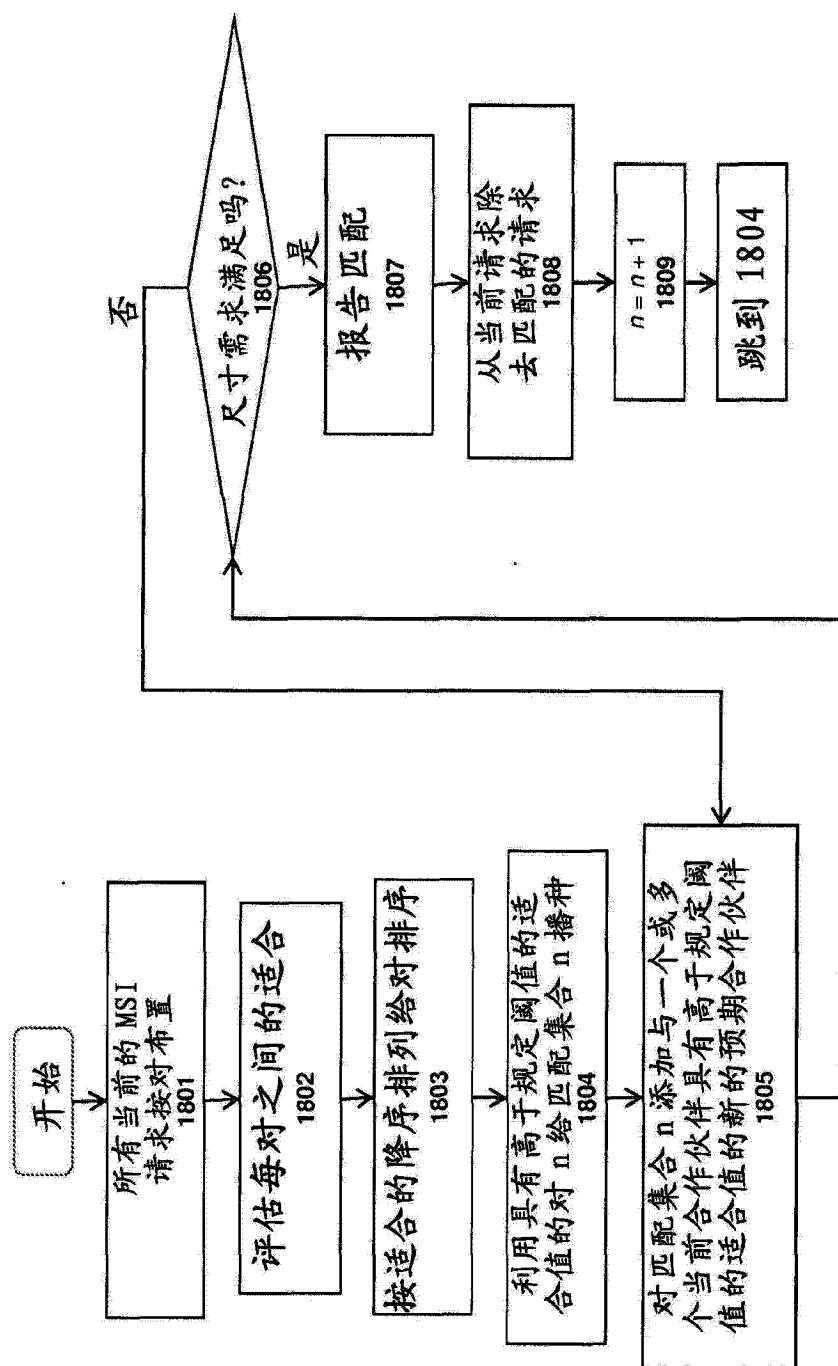


图 18

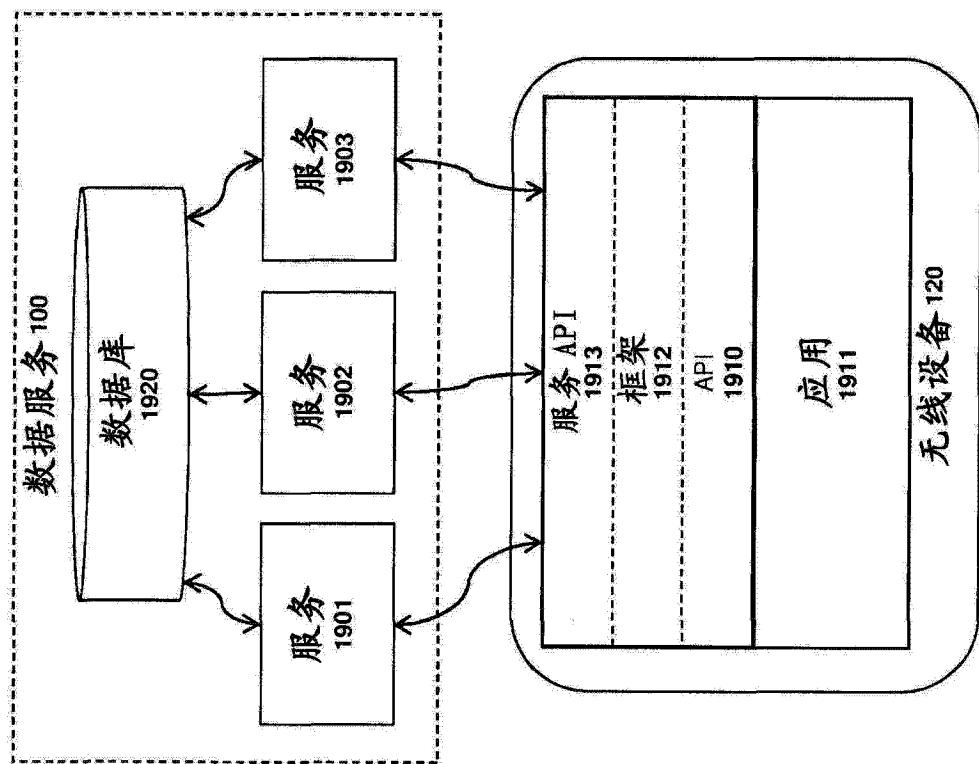


图 19

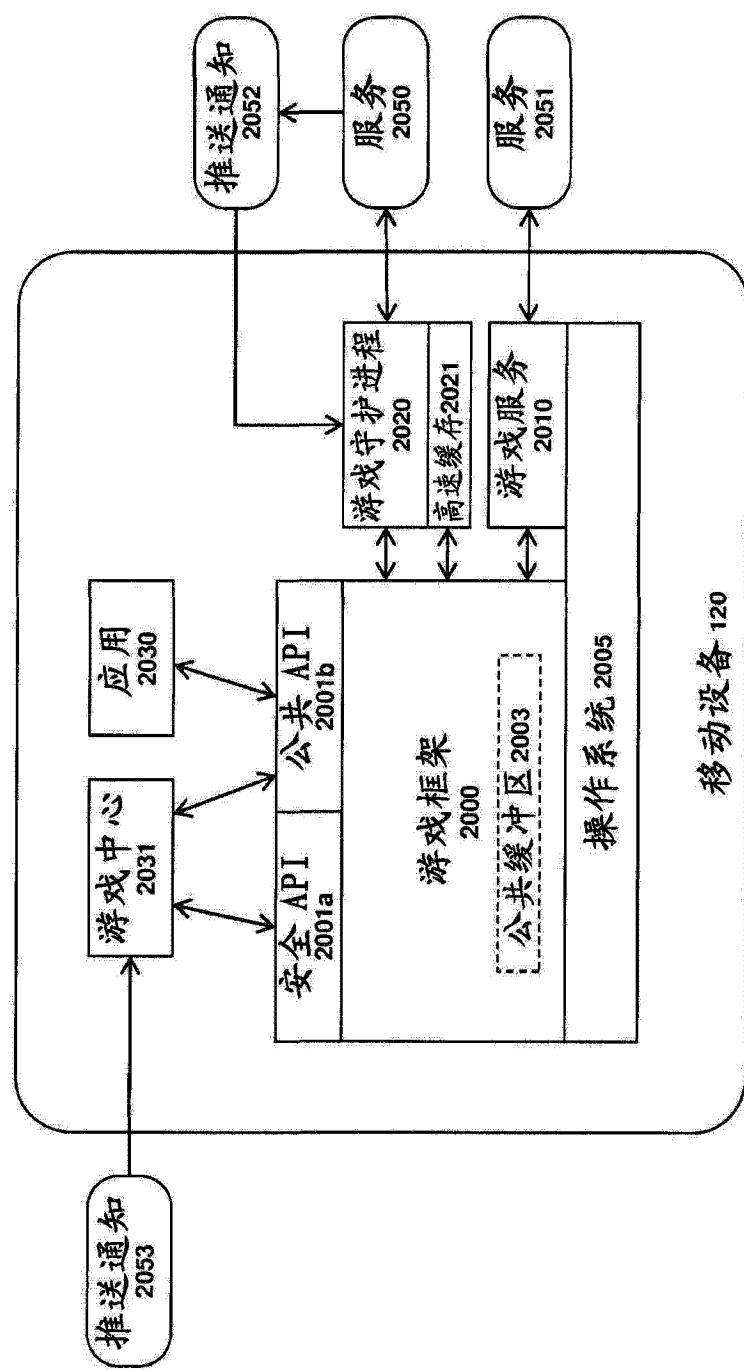


图 20

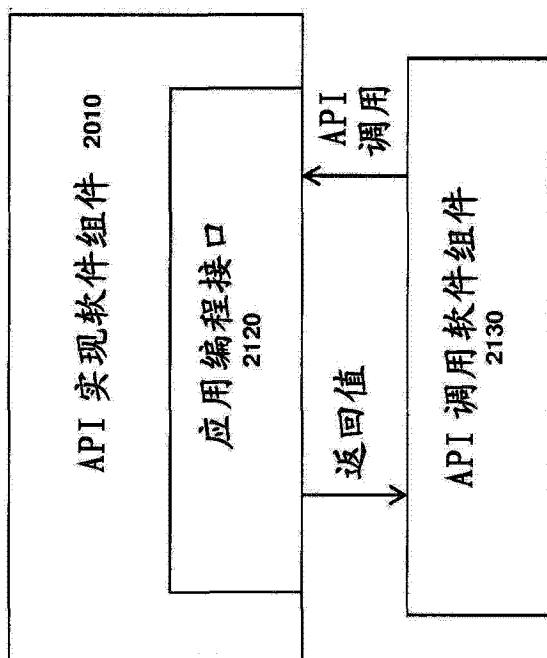


图 21

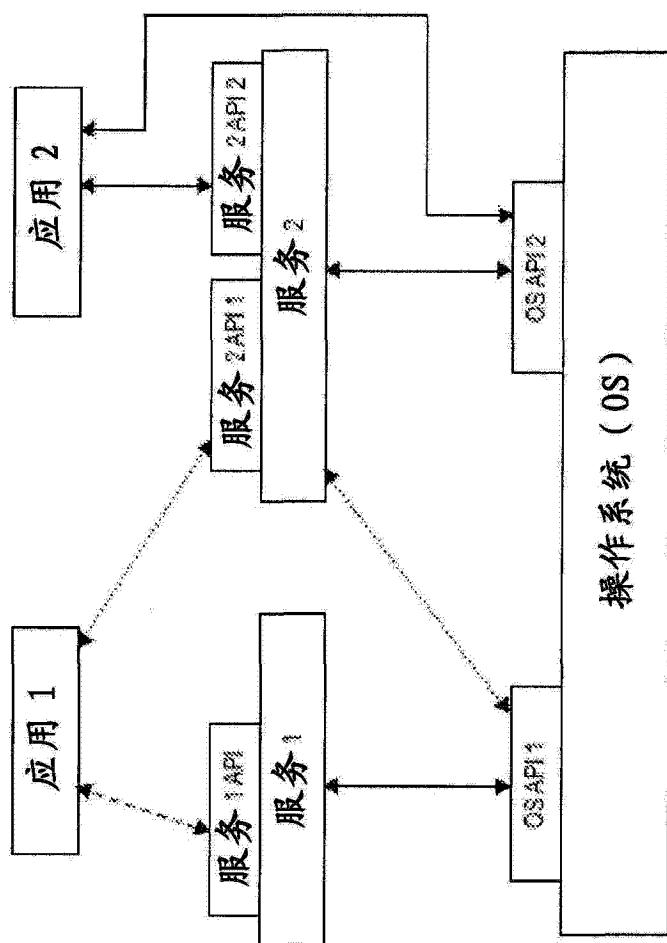


图 22

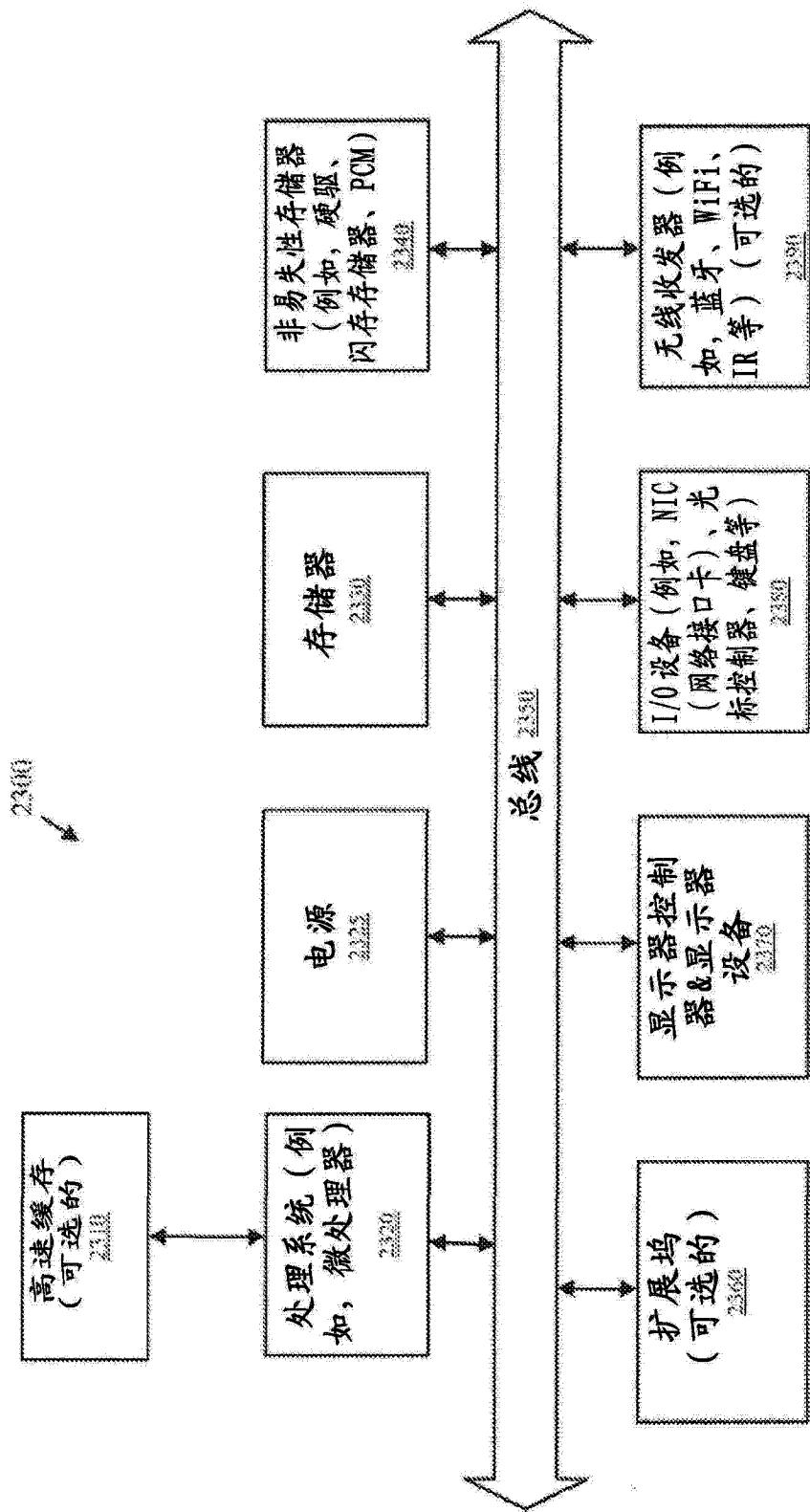


图 23

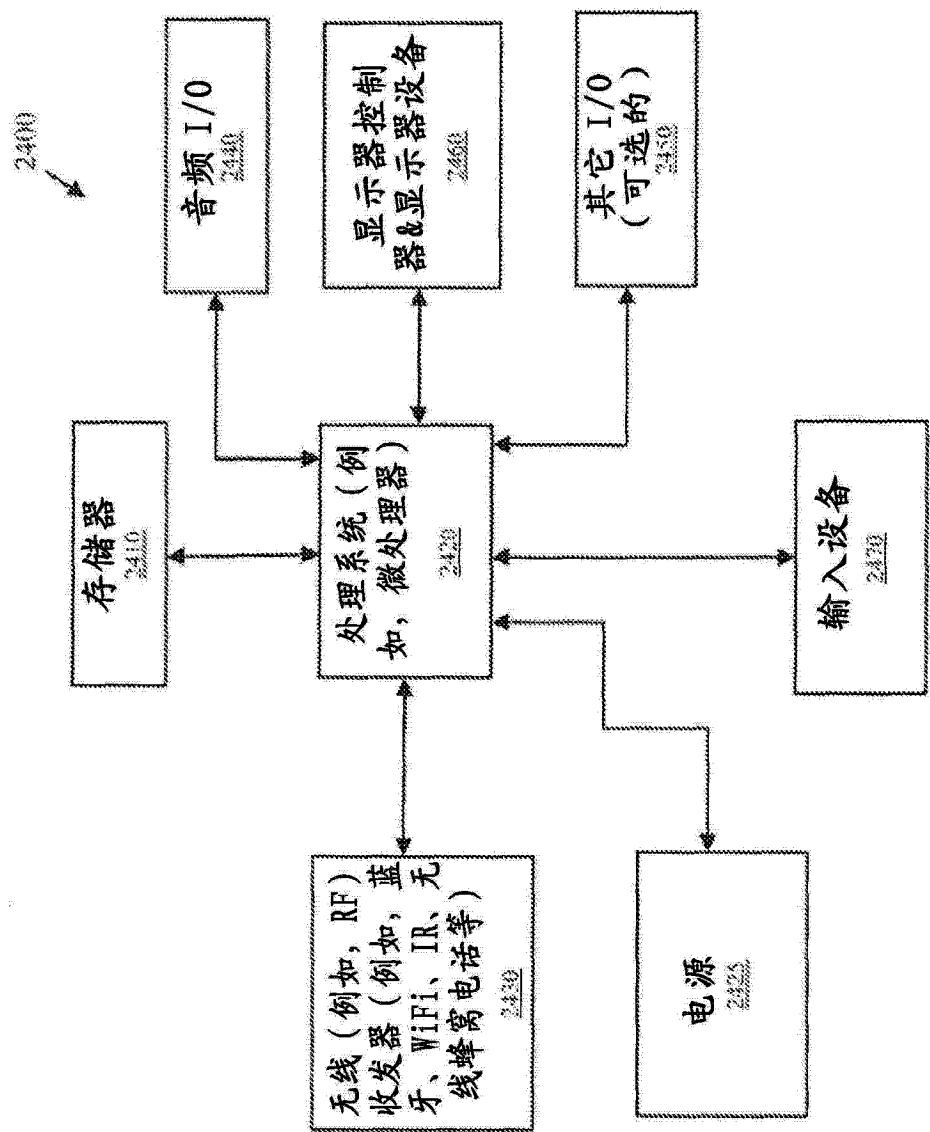


图 24

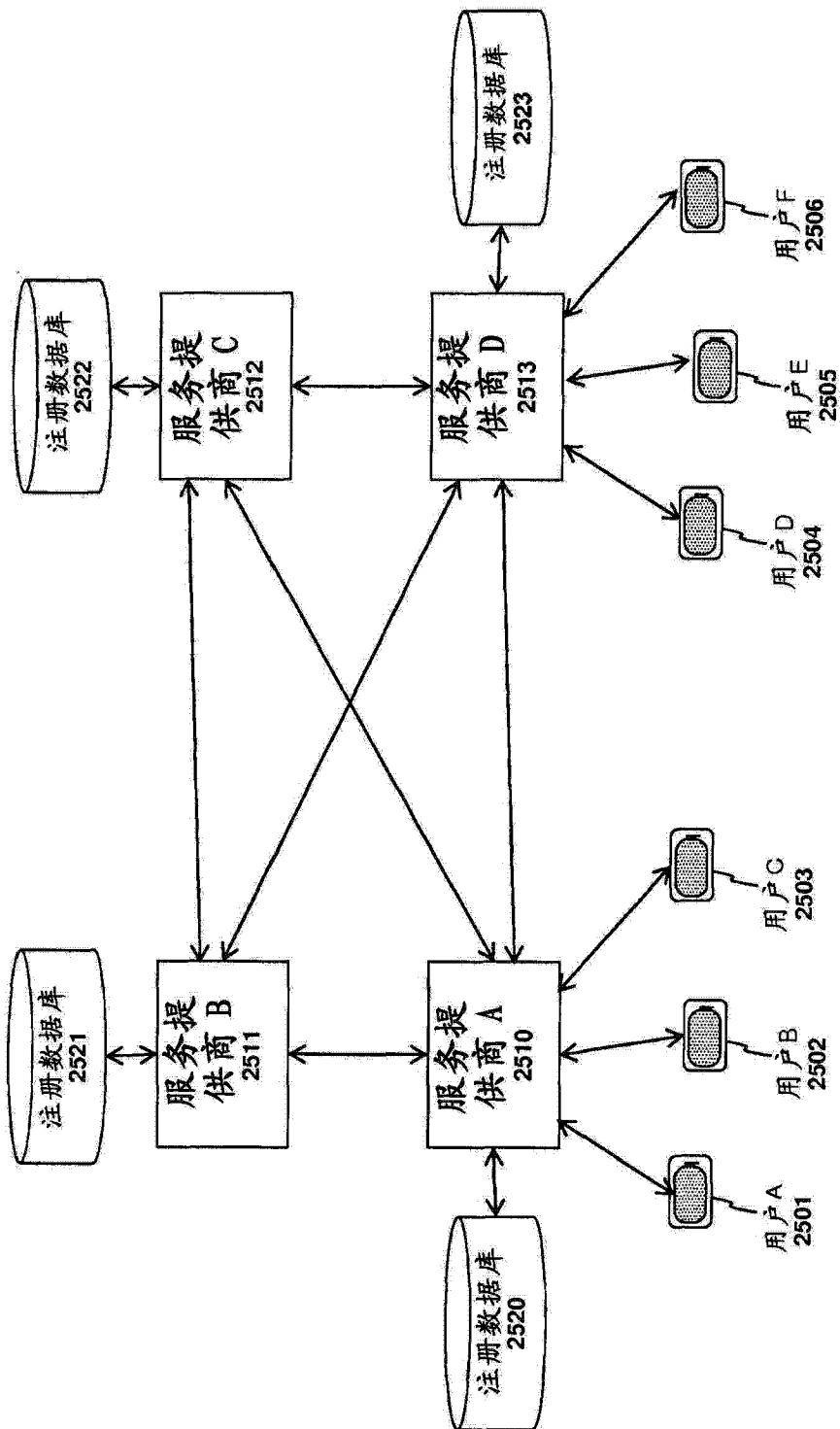


图 25

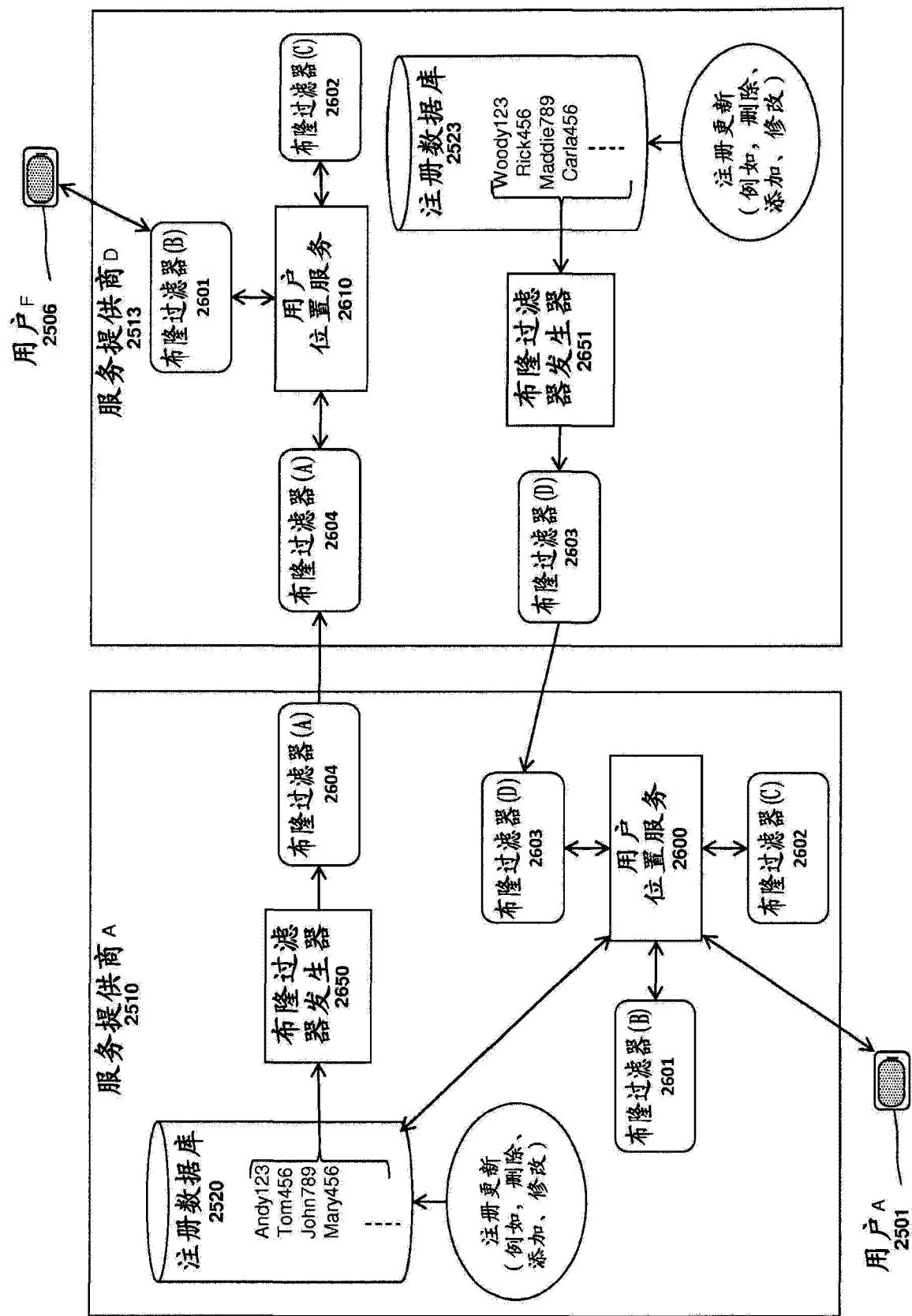


图 26

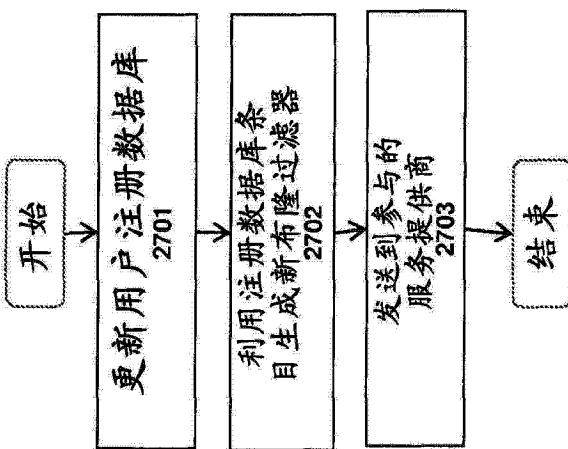


图 27

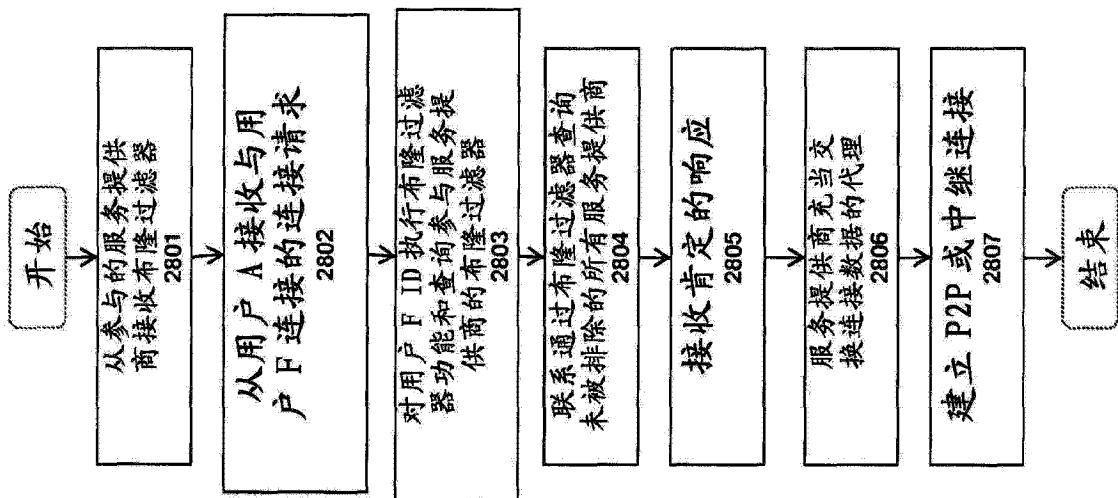


图 28

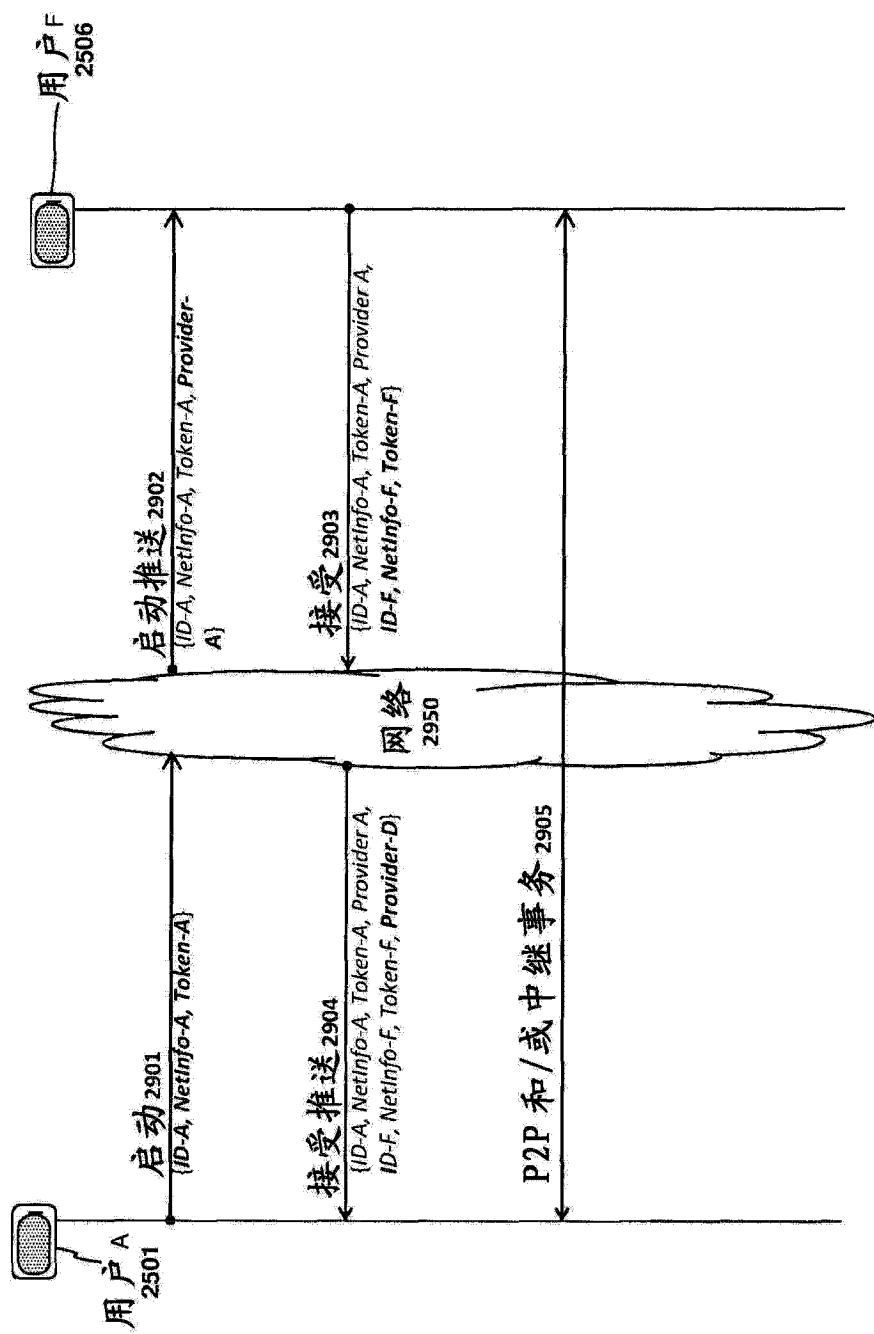


图 29

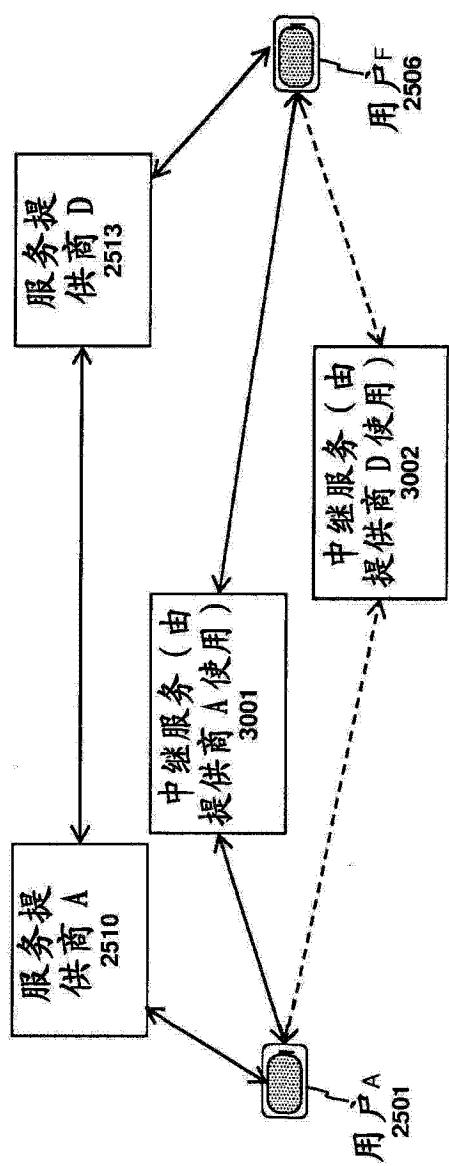


图 30

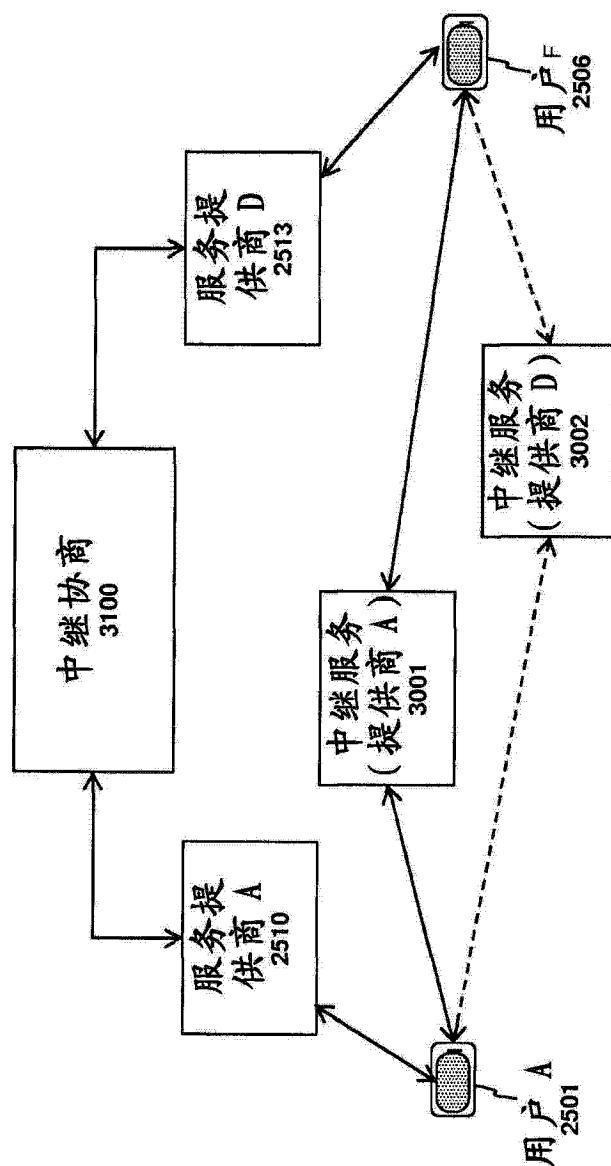


图 31

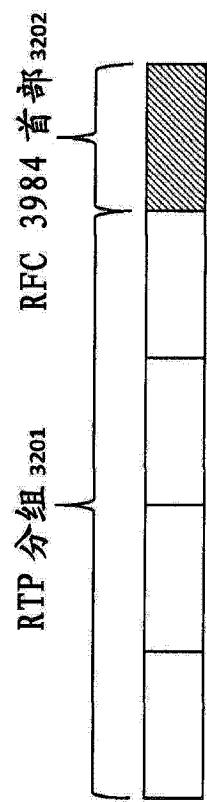


图 32

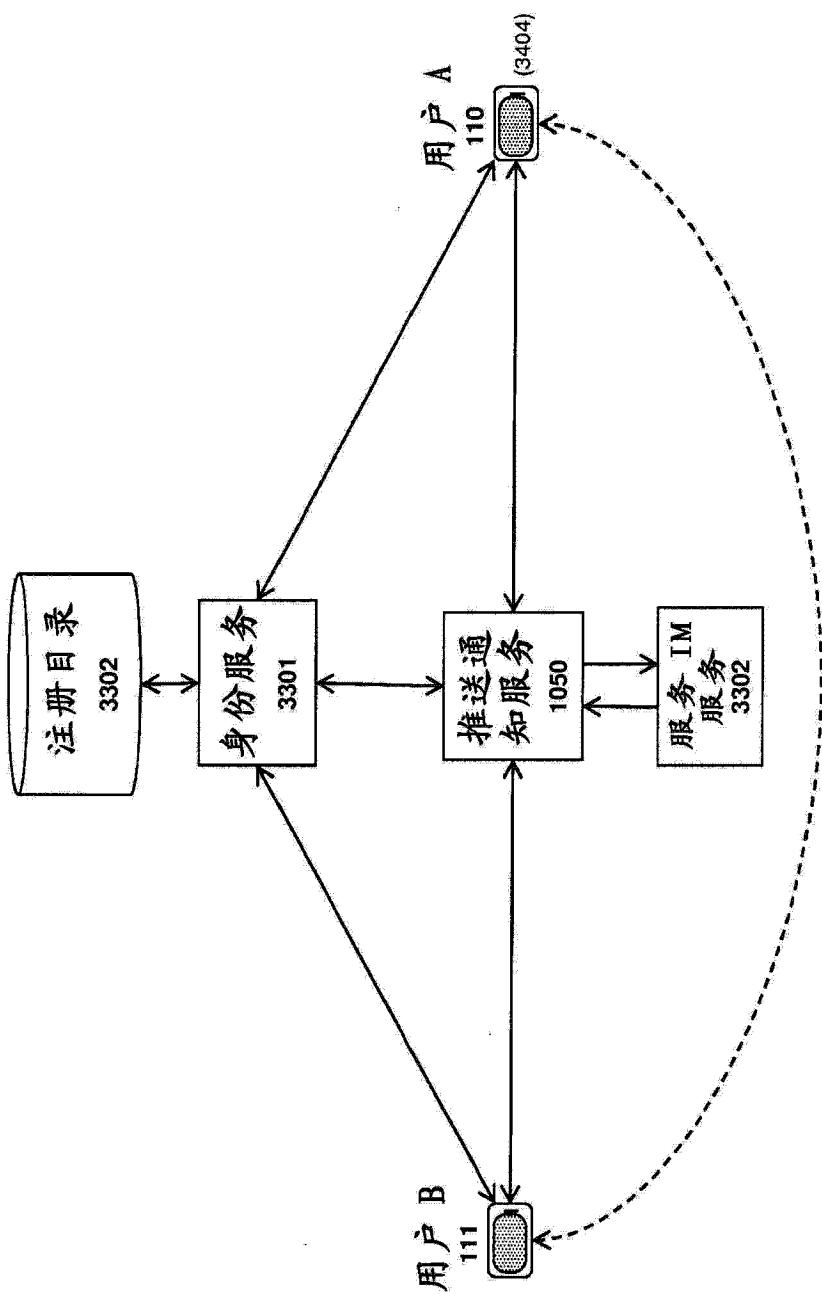


图 33

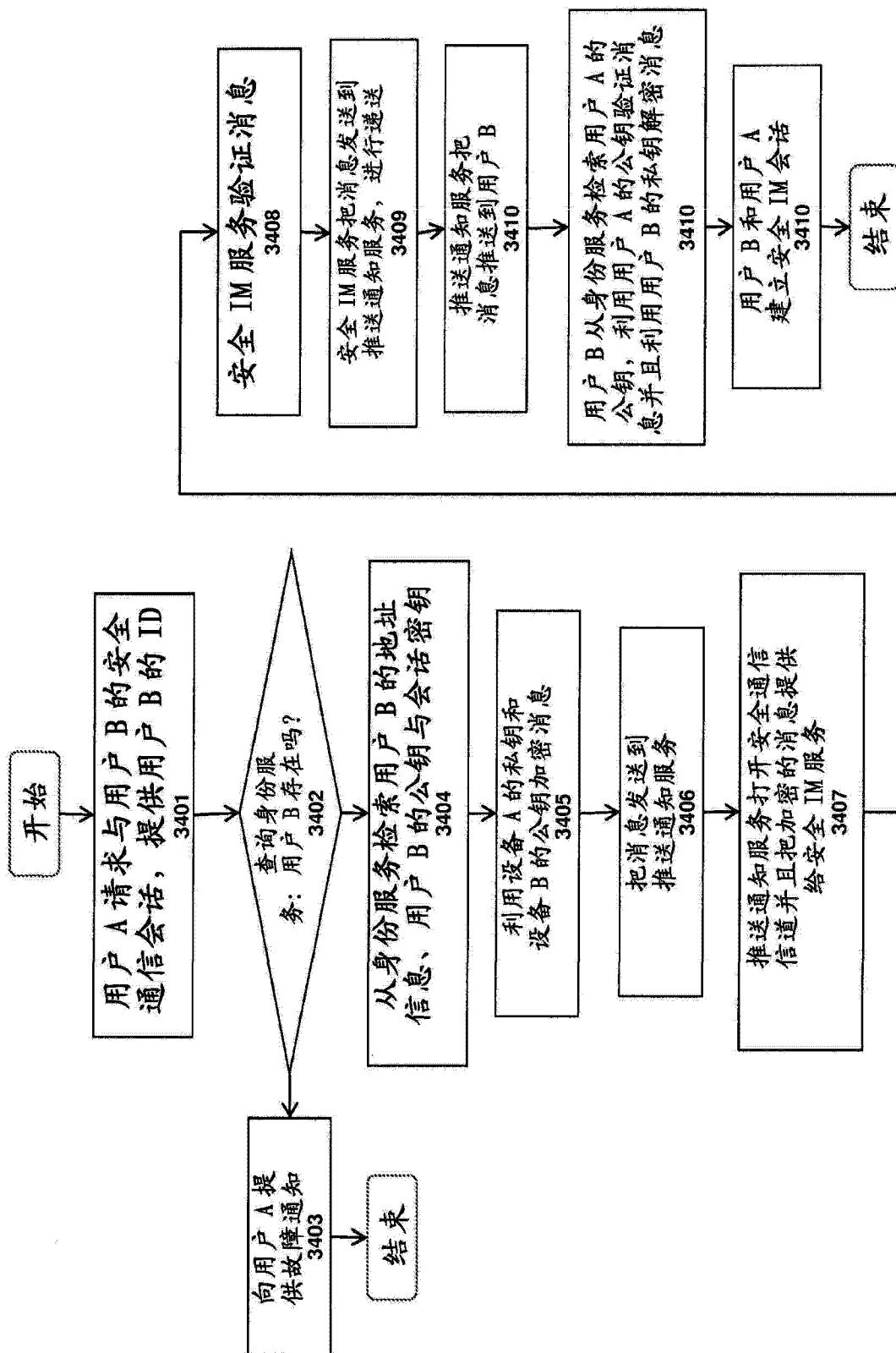


图 34

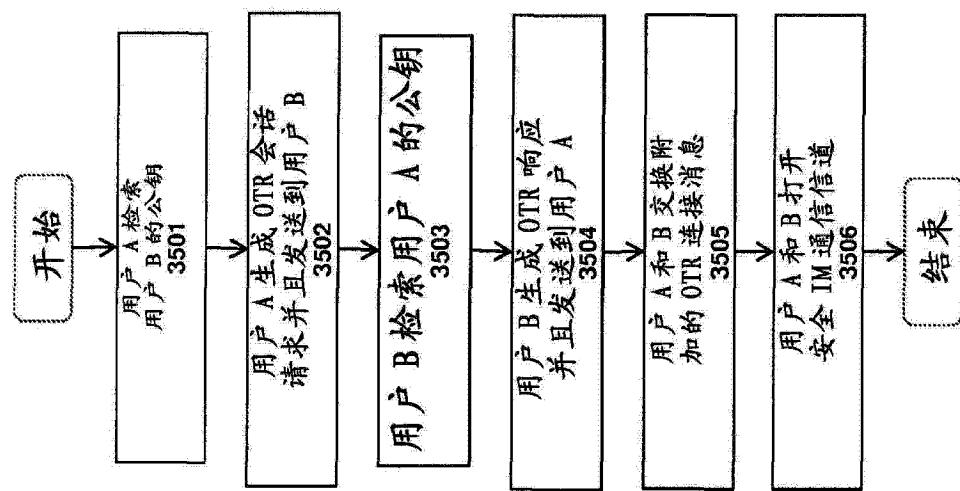


图 35

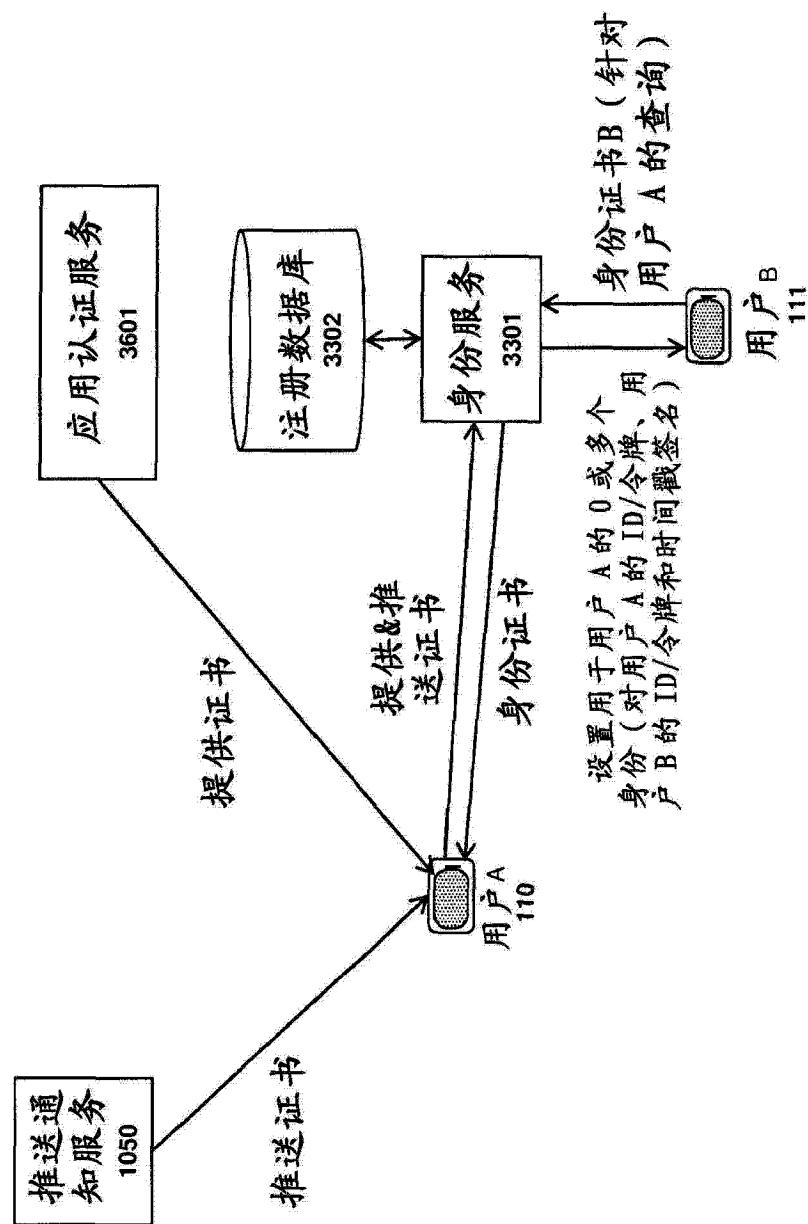


图 36

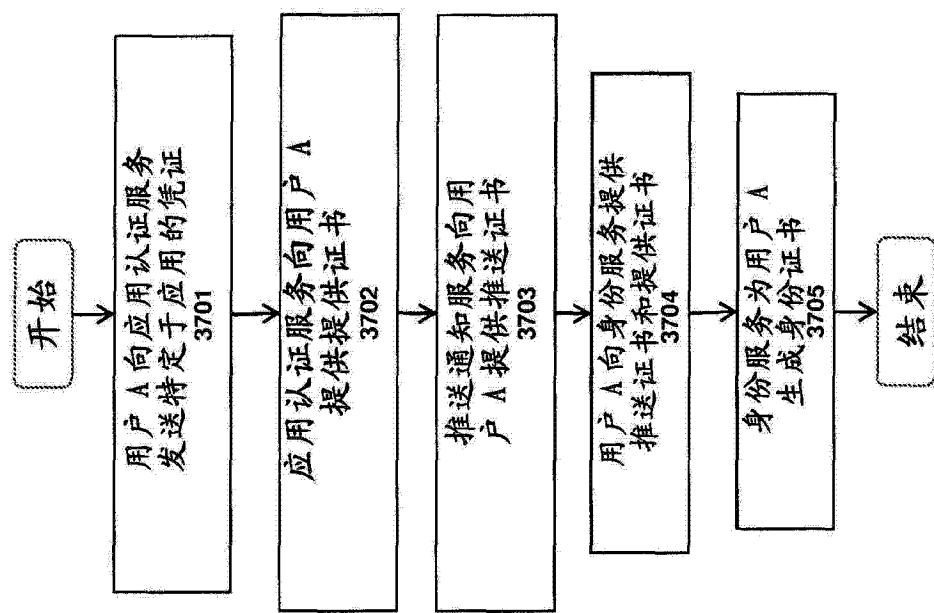


图 37

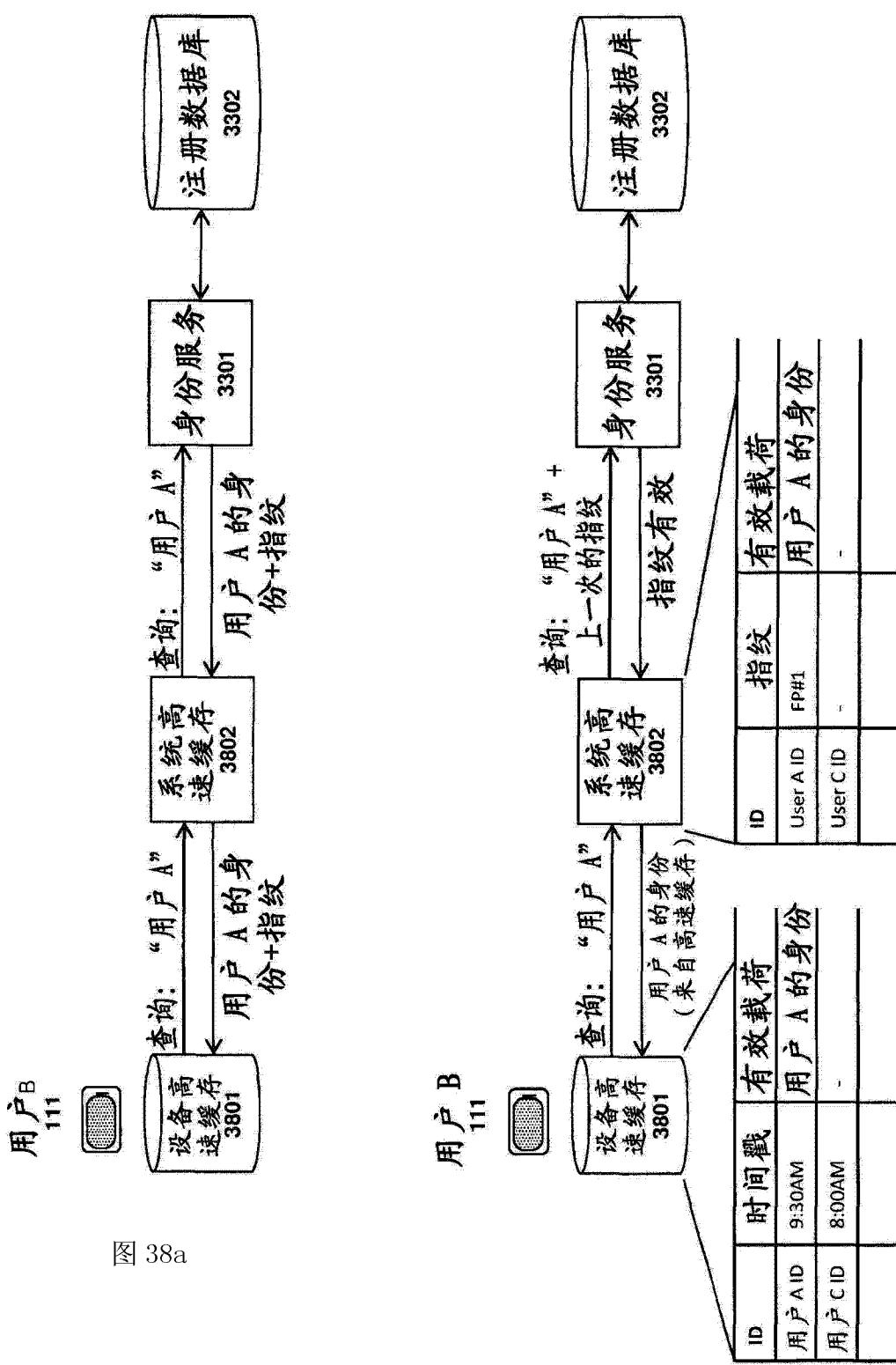


图 38a

图 38b