



(12) 发明专利

(10) 授权公告号 CN 1820264 B

(45) 授权公告日 2011.06.29

(21) 申请号 200480001309.7

(56) 对比文件

(22) 申请日 2004.07.29

US 6463464 B1, 2002.10.08, 权利要求

(30) 优先权数据

1-75、说明书第2栏第50行到第9栏第59行。

10/693,516 2003.10.23 US

WO 2002063474, 2002.02.01, 全文。

(85) PCT申请进入国家阶段日

US 5812776 A, 1998.09.22, 说明书第3栏第

2005.05.20

10行到第30行。

(86) PCT申请的申请数据

US 20030177178 A1, 2003.09.18, 说明书第

PCT/US2004/024341 2004.07.29

1页第4段到第3页第32段、权利要求1-12、附图

1-3.

(87) PCT申请的公布数据

审查员 俞晨

W02005/045741 EN 2005.05.19

(73) 专利权人 微软公司

地址 美国华盛顿州

(72) 发明人 M·萨塔吉潘 K·卡梅伦

(74) 专利代理机构 上海专利商标事务所有限公司 31100

代理人 陈斌

(51) Int. Cl.

G06F 15/16 (2006.01)

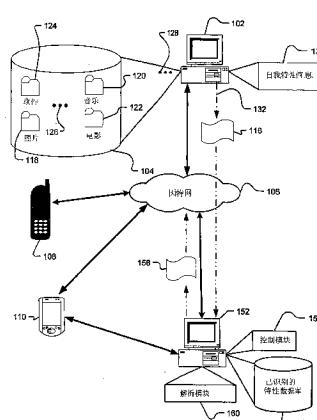
权利要求书 3 页 说明书 13 页 附图 7 页

(54) 发明名称

名称解析的系统和方法

(57) 摘要

依照不同的方面，本发明涉及在网络环境中彼此连接的两个计算机系统或节点之间访问和发布文档。这种用于名称解析的系统和方法为存储这些文档的发布节点存储包含表示比如 email 地址的身份和比如 IP 地址的机器位置的用户友好的句柄的身份信息文档。接着，当起初的请求包括用户友好的句柄并用机器位置替代用户友好的句柄时，这种系统和方法截取起初的用于访问文档的请求，这样，网络用户可以轻松地通过仅具有用户友好的句柄的知识来访问这些文档。



1. 一种通过第二计算机系统访问存储在第一计算机系统上的文档的方法,所述第一和第二计算机系统在网络环境中相连接,所述方法包括:

在所述第二计算机系统上存储来自第一计算机系统的身份信息文档,该身份信息文档包括标识第一计算机系统的当事人和机器位置的用户友好的句柄;

在第二计算机系统上实现的用户界面上接收对访问存储在所述第一计算机系统上的文档的请求,所述请求包括所述用户友好的句柄并指向所述第一计算机系统;

当来自所述第二计算机系统的用户的访问文档的请求包括所述用户友好的句柄时,在所述第二计算机系统上截取所述请求;

在所述第二计算机系统上用所述机器位置替代所述请求的所述用户友好的句柄;以及向第一计算机系统的所述机器位置发送所述访问文档的请求。

2. 如权利要求1所述的方法,其特征在于,所述用户友好的句柄包括一email地址。

3. 如权利要求1所述的方法,其特征在于,所述机器位置包括一IP地址。

4. 如权利要求1所述的方法,其特征在于,所述机器位置包括一公共密匙。

5. 如权利要求1所述的方法,其特征在于,所述访问文档的请求包括一当事人启动的请求。

6. 如权利要求1所述的方法,其特征在于,进一步包括在所述第二计算机系统接收来自第一计算机系统的身份信息文档的起始步骤。

7. 一种在多个节点之间发布文档的方法,所述节点在网络环境中相连接,所述方法包括:

从发布节点向访问节点发送身份信息文档,该身份信息文档包括标识发布节点的当事人和机器位置的用户友好的句柄;

在所述访问节点上存储所述身份信息文档;

在所述访问节点上用访问文档的请求中的机器位置解析所述用户友好的句柄,其中该请求是从访问节点的用户通过访问节点上实现的用户界面向发布节点做出的;以及

从访问节点向发布节点发送所述访问文档的请求。

8. 如权利要求7所述的方法,其特征在于,所述用户友好的句柄包括一email地址。

9. 如权利要求7所述的方法,其特征在于,所述用户友好的句柄包括一电话号码。

10. 如权利要求7所述的方法,其特征在于,所述机器位置包括一IP地址。

11. 如权利要求7所述的方法,其特征在于,所述机器位置包括一公共密匙。

12. 如权利要求11所述的方法,其特征在于,进一步包括:

使用所述公共密匙为发布节点确定当前的机器位置。

13. 如权利要求11所述的方法,其特征在于,进一步包括:

向DNS服务器注册用于发布节点的加密机器名称和注册机器位置;

用所述公共密匙解析所述用户友好的句柄;

将所述公共密匙转换为所述加密机器名称;

使用所述加密机器名称在DNS服务器上查找发布节点的注册机器位置;以及向所述注册机器位置发送访问文档的请求。

14. 如权利要求7所述的方法,其特征在于,进一步包括:

验证访问节点具有来自发布节点的授权以在发布所请求的文档之前审查所请求的文

档。

15. 如权利要求 7 所述的方法,其特征在于,进一步包括:

将存储在发布节点上的文档的路径名称传递到访问节点。

16. 如权利要求 15 所述的方法,其特征在于,通过 email 向访问节点传递该路径名称。

17. 如权利要求 7 所述的方法,其特征在于,进一步包括:

将存储在发布节点上的文档的路径名称传递到访问节点的当事人。

18. 如权利要求 17 所述的方法,其特征在于,通过电话呼叫向访问节点的当事人传递该路径名称。

19. 如权利要求 7 所述的方法,其特征在于,所述解析步骤进一步包括:

当所述访问文档的请求被指向用户友好的句柄时,截取所述请求;

找到具有与所述请求中的用户友好的句柄相匹配的用户友好的句柄的匹配身份信息文档;

从所述匹配身份信息文档中确定所述机器位置;以及

修正所述请求以用所述机器位置取代所述用户友好的句柄。

20. 如权利要求 7 所述的方法,进一步包括:

向访问节点传递与所述用户友好的句柄组合的路径名称;以及

在用所述机器位置解析所述用户友好的句柄之前,从所述用户友好的句柄中分析所述路径名称。

21. 如权利要求 20 所述的方法,其特征在于,进一步包括:

在向发布节点发送所述访问文档的请求之前,将所述路径名称添加至所述访问文档的请求。

22. 如权利要求 7 所述的方法,其特征在于,所述身份信息文档进一步包括一个以上的用于由所述用户友好的句柄标识的当事人的机器位置。

23. 一种使用用户友好的句柄来访问存储在网络环境中的第一计算机系统上的文档的方法,该方法包括:

在第二计算机系统上存储来自第一计算机系统的身份信息文档,该身份信息文档包括标识所述第一计算机系统的第一用户和所述第一计算机系统的机器位置的用户友好的句柄;

在所述第二计算机系统上实现一用户界面,使得第二计算机系统的第二用户能够请求对存储在所述第一计算机系统上的文档的访问;

在所述第二计算机系统上实现的所述用户界面上接收来自所述第二计算机系统的所述第二用户访问存储在所述第一计算机系统上的文档中的第一文档的请求,所述请求包括所述用户友好的句柄并指向所述第一计算机系统;

在所述第二计算机系统上截取来自所述用户界面访问所述第一文档的所述请求;

在所述第二计算机系统修正所述请求以用所述第一计算机系统的机器位置替代所述用户友好的句柄;

从所述第二计算机系统向第一计算机系统的机器位置发送经修正的请求;以及

在所述第二计算机系统上访问所述第一文档。

24. 如权利要求 23 所述的方法,其特征在于,所述用户友好的句柄是一 email 地址。

25. 如权利要求 23 所述的方法,其特征在于,所述机器位置包括一 IP 地址。

26. 如权利要求 23 所述的方法,其特征在于,所述机器位置包括一公共密匙。

27. 如权利要求 26 所述的方法,其特征在于,进一步包括:

使用所述公共密匙确定发布节点的当前机器位置。

28. 如权利要求 23 所述的方法,其特征在于,进一步包括:

接收来自第一计算机系统的所述身份信息文档。

29. 如权利要求 23 所述的方法,进一步包括:接收来自第一计算机系统的发布的文档。

30. 一种计算机系统,包括:

存储模块,用于存储接收到的来自另一计算机系统的身份信息文档,该身份信息文档包括标识所述另一计算机系统的当事人和机器位置的用户友好的句柄;

通信上与所述存储模块连接的通信模块,用于从所述计算机系统的用户发送对访问所述另一计算机系统上存储的文档的请求;

通信上连接到所述存储模块和所述通信模块的名称解析模块,用于截取对访问所述另一计算机系统上存储的文档的请求,并修正每个请求以用机器位置替代用户友好的句柄;以及

用户界面模块,配置成使得所述计算机系统的所述用户能够访问并控制所述存储模块、所述通信模块和所述名称解析模块中的任一个。

31. 如权利要求 30 所述的计算机系统,其特征在于,用户友好的句柄是一 email 地址。

32. 如权利要求 30 所述的计算机系统,其特征在于,所述机器位置包括一 IP 地址。

33. 如权利要求 30 所述的计算机系统,其特征在于,所述机器位置包括一公共密匙。

34. 如权利要求 30 所述的计算机系统,其特征在于,进一步包含:

连接到所述名称解析模块的通信模块,用于向所述另一计算机系统发送通信并接收来自所述另一计算机系统的通信。

名称解析的系统和方法

[0001] 本发明的技术领域

[0002] 本发明涉及发布存储在分布式网络中的单独的机器,或节点上的文档和信息并与网络中的其他节点共享这些文档。更为具体地,本发明涉及用于提供给另一个用户访问这些已发布的文档的系统和方法。

[0003] 本发明的背景

[0004] 在具有许多相连的节点或进程的分布式网络或系统中,在网络的节点之间共享文件、文档和信息的能力是很重要的。

[0005] 用户有几种常规的方法可以共享文件和文档,包括在 web 服务器上传递文档,其中访问对任何人公开或由口令保护系统限定在预先批准的用户。伴随这种系统的问题是双重性的。首先,它一般要求第三方,比如 web 主宿服务来维持在服务器计算机上的文档,这通常要求初始的安装费和连续的维护费。第二个,第三方的参与自然减少了用户对存储在 web 服务器上的文件或文档的控制。

[0006] 另一种在分布式网络的用户间共享文件的方法是对希望与另一个用户(“访问者”)共享文件的用户(“发布者”)来说,提供给访问者他的或她的机器位置和文档存储的机器上的路径名称。访问者通过在 web 浏览器或其他访问程序内输入机器名称和路径名称访问发布者的文档来到达发布者的机器。这种情况下,发布者的机器一般提供只允许批准访问的用户访问的安全系统。

[0007] 为了输入机器的位置,用户必须知道机器的位置。输入机器位置的一种方法包括输入互联网协议(“IP”)地址。“IP 地址”是标识因特网上的计算机的唯一的数字串。IP 地址包含 32 位,组织成四组三个阿拉伯数字 0 到 255 之间的数字,它们由句点分开,类似:123.123.023.002。所有因特网上的机器必须具有 IP 地址而且没有两个计算机系统同时具有相同的 IP 地址。IP 地址可以是动态的或是静态的。静态的 IP 地址是永久指派给计算机系统的地址——它是唯一由该系统使用的 IP 地址。动态的 IP 地址是例如,从指派给组织的一组 IP 地址中在运行中指派的地址。尽管两个计算机系统不能同时使用一个 IP 地址,但每个计算机系统可以使用多个不同的 IP 地址。IP 地址并不是用户友好的的因为他们只包含具有不易懂的意思的数字。为此,对人们来说,记住他们自己的 IP 地址几乎是不可能的,更不用说属于其他人的机器的 IP 地址了。

[0008] 域名系统(DNS)通过允许使用类似的字母串(“域名”)而非晦涩难解的 IP 地址来使得找到机器的位置更加容易。因此并非记住并打入 66.201.69.207,用户能够打入 www.microsoft.com。域名也被用于获得 e-mail 地址和其他因特网应用。域名被解析,即通过主存在位于整个因特网的许多服务器上的服务将域名转换为 IP 地址。然而,DNS 至少有两个限制。第一个,它要求使用第三方设备,即 DNS 服务器来处理名称解析。第二个,它不是非常安全的,因为几乎所有人能为任何计算机系统确定特定的机器名称和位置。因此,常规的 DNS 并不是用于在计算机系统上发布资源的非常有效的方法。

[0009] 另一种获得机器位置的方法是使用公共密匙。公共密匙与特定的人有关并包括一长串字节,例如,32 个数字和字母,比如 KP12JSP2345L1298FE23KLKSERQ0C38S。公共密匙一

般被用于使用户能够使不安全的公共网络,比如因特网变得安全并通过使用通过可信赖的权威机构获得的共享的公共和个人的密码密匙对来秘密地交换数据。公共密匙密码是因特网上用于认证消息发送者或加密消息的最普通的方法。公共密匙可用许多种方法获得。例如,公共密匙可通过当一个人在计算机系统上创建帐户时,由操作系统创建并指派。或者,在公共密匙密码中,由鉴定权威机构使用相同的算法同时创建公共密匙和个人密匙。

[0010] 公共密匙通过使用对等名解析协议(“PNRP”)被连接到机器的位置,该协议在公共可用列表中存储每个人的带有它们的当前位置的公共密匙或者一些其他可搜索的数据结构。因此,如果你知道一个人的公共密匙,你可以使用 PNRP 来确定它相关联的当前机器位置,它通常是以 IP 地址的形式。然而,像 IP 地址一样,公共密匙是许多没有意义的一串比特并且甚至比 IP 地址本身更难记住。

[0011] 然而另一种确定机器位置的方法包括接收(比如通过 email)加入或包含机器位置的链路。当选择了该链路时,浏览器自动在浏览器内输入与链路有关的 IP 地址或公共密匙。然而不幸地是,访问当事人(principal)需要在每次访问节点希望访问发布节点的资源时都要储存 email 并找到和打开它。这是耗时的、麻烦的并浪费访问机器上的存储容量。

[0012] 本发明可以作为计算机进程、计算系统或作为比如计算机程序产品或计算机可读介质的一件物品来实现。计算机程序产品可以是可由计算机系统读取并编码用于执行计算机进程的计算机程序指令的计算机存储介质。计算机程序产品也可以是在可由计算系统读取并且编码用于执行计算机进程的计算机程序指令的载波上的传播信号。

[0013] 表现本发明特点的这些以及不同的其他特征和优势从阅读了以下的详细描述并回顾了相关联的附图中,可以变得更加明显。

发明内容

[0014] 本发明涉及在网络环境中彼此连接的两个计算机或节点之间访问和发布文档,更具体地,涉及用于通过以存储着文档的机器位置来表示身份的用户友好的句柄进行名称解析的系统和方法,从而使网络用户可以通过用户友好的句柄的知识轻松地访问这些文档。换言之,可通过使用标识用户的用户友好的句柄和描述感兴趣的文档的路径名称来访问用户文档,该句柄和路径名称被解析为文档被存储的机器的位置。Email 地址是用户友好的句柄的示例性的例子而 IP 地址或公共密匙是机器位置的示例性的例子。存储着文档的计算机系统或节点称为发布计算机系统或节点而寻求访问存储在发布节点上的文档的计算机系统是被称为访问计算机系统或节点。

[0015] 依照特定的方面,当来自第一计算机系统的身份信息文档被存储在第二计算机系统上时,一种通过第二访问计算机系统来访问存储在第一发布计算机系统上的文档的方法就开始了。这种身份信息文档至少具有为第一计算机系统标识了当事人和机器位置的用户友好的句柄。当做出包含该用户友好的句柄的访问文档的最初请求时,第二计算机系统截取它。第二计算机系统用机器位置替代用户友好的句柄并向第一计算机系统的机器位置发送已修正的请求。这种方法允许第二计算机系统仅用关于为用户友好的句柄的知识即可访问在第一计算机系统上的文档。第一计算机系统的机器位置、IP 地址或公共密匙的知识不是必需的。

[0016] 依照其他方面,本发明涉及在网络环境中连接的多个节点之间发布文档的方法。

该方法由从发布节点向访问节点发送身份信息文档开始。身份信息文档至少包括为发布节点标识当事人和机器位置的用户友好的句柄。此后，身份信息文档被存储在访问节点上。当从访问节点向发布节点做出最初的访问文档的请求时，用机器位置解析用户友好的句柄。接着，从访问节点向发布节点的机器位置发送已修正的访问文档的请求。

[0017] 依照再其他的方面，本发明涉及包括用于存储从第二计算机系统接收的身份信息文档的存储模块和连接到该存储模块的名称解析模块的计算机系统。名称解析模块截取访问存储在身份信息文档的用户友好的句柄处的文档的请求并修正该请求以用来自身份信息文档的机器位置替代用户友好的句柄。

[0018] 依照再其他的方面，本发明涉及编码用于执行名称解析的计算机进程的指令的计算机程序的计算机可读介质。该进程从存储来自发布计算机系统的身份信息文档的存储操作开始。接下来，当最初请求包含用户友好的句柄时，截取操作截取用于访问存储在发布计算机系统上的文档的最初请求。最后，修正操作修正请求以用机器位置替代用户友好的句柄。

[0019] 附图简述

[0020] 图 1 说明结合了本发明的各方面的节点的通信或分布式网络。

[0021] 图 2 说明依照本发明的特殊方面可以使用的计算机系统。

[0022] 图 3 说明依照本发明的特殊方面的身份信息文档的结构。

[0023] 图 4 说明依照本发明的各方面的软件环境的表示。

[0024] 图 5 说明关于访问节点的本发明的操作特性的流程图。

[0025] 图 6 说明关于访问节点和发布节点的本发明的替代性的实施例的操作特性的流程图。

[0026] 图 7 说明关于访问节点和发布节点的仍是本发明的替代性的实施例操作特性的流程图。

[0027] 优先的实施例的详细描述

[0028] 图 1 显示了结合本发明的各方面的分布式环境 100。环境 100 至少具有一个计算机系统 102 和潜在的其他计算机系统比如 108、110 和 152，其中不同的计算机系统被称之为“节点”或“机器”。作为这里所使用的，“计算机系统”应被广义理解并被定义为“一个或多个执行用于显示并处理文本、图形、码元、声频、视频和 / 或数字的程序的设备或机器”。网络中的节点可为任何类型的计算机系统，包括但不限于，比如节点 108 的电话、比如节点 110 的 PDA、比如节点 102 和 152 的桌上型电脑、膝上电脑（未显示）以及许多其他系统。而且，尽管作为计算机系统显示，节点 102、108、110 和 152 或者可以是计算机系统内的计算机进程。或者，节点 102、108、110 和 152 可组合跨局域网、广域网分布的单独的计算机系统的组合或单独的网络通信的组合。

[0029] 正如所阐述的，计算机系统 102、108、110 和 152 的每一个是环境 100 内能够与环境 100 内的其他节点进行通信并与其他网络节点共享文档、信息和资源的所考虑的节点。而且，这些节点可通过在比如因特网 106 的网络实现的单独的协议，比如 TCP/IP 或其他网络和 / 或通信协议来通信。即，尽管显示为表面上的直接箭头连接，但实际上单独节点 102、108、110 和 152 可通过其他间接方式而与其他节点通信。实际上，100 中显示的连接仅仅指示节点可与另一个节点通信。

[0030] 正如所阐述的,通过许多通信协议,可以得到机器 102、108、110 和 152 之间的通信。这里使用的通信的定义涉及消息、事件或任何其他从一个节点到另一个节点的信息的传递。一个实施例中,环境 100 的节点可与网络 100 中的所有其他节点通信,但这样一种要求并不是必需的。为了从第一节点到第二节点进行通信信息,第一个节点需要机器位置或用于访问节点的一些其他的标识信息。使用机器位置,发送节点可以使用任何传输协议发送信息。

[0031] 尽管图 1 只显示了四个节点 102、108、110 和 152,但网络环境可包括其他节点。实际上,环境 100 的节点数量可为从数千到好几个节点或者更多的非常多的数量。因此,本发明在确定所需要的环境 100 规模方面是有益的,所以实际上依照本发明,任何数量的节点都可以通信信息。

[0032] 本发明涉及用于与另一个网络节点——“访问节点”发布或共享存储在一个网络节点——“发布节点”上的资源的用户友好的的系统和方法。计算机系统 102 是发布节点的一个例子并包括数据库 104,该数据库拥有组织成一个或多个目录、或文件夹,比如文件夹 118、120、122 和 124 的数据。数据库 104 涉及通用文件系统和其他有组织的数据系统用于存储并检索电子文档。这样,数据库 104 可包括任何类型的数据或文件,这里可指作为“文档”。术语“文档”应被广泛理解并可包括但不限于,照片、视频片段、音频片段、文本文件、演示、软件代码和任何其他存储在计算机系统上的个人资源。文档可以任何方式被组织在数据库内,包括但不限于,以带有描述符的文件夹和子文件夹。例如,文件夹 118 可包含“jpeg”文件并被命名为“照片”,文件夹 120 可包含音频片段并被标记为音乐,文件夹 122 可包含“mpeg”文件并被标记为视频,而文件夹 124 可包含可执行的代码并被标记为“软件”。省略号 126 指示数据库 104 中一般可以存在任何数量的文件夹,包含了任何类型的文档。

[0033] 尽管只显示了数据库 104,省略号 128 指示机器 102 可拥有多于一个的数据库,该数据库可用与数据库 104 相同或不同的方式被组织。例如,数据库 104 可特定于机器的主要用户并被存储在位于机器 102 内的那个当事人的简介中。作为这里使用,“当事人”应被广泛理解并被定义为任何能够数字式行动的实体。当事人包括但不限于,个人、团体或几组意指个人、家庭、组织、明显表达的团体和扮演公共角色的人或者共享某些属性和各种电子设备的人,这些个人通过这些电子设备而采取行动。另一个当事人拥有存储在机器 102 内仅由那个当事人访问的不同的数据库。

[0034] 计算机系统 102 又维护一组自身身份信息 130,该身份信息包含各种由计算机系统 102 表示或使用计算机系统 102 的有关当事人的信息。例如,这种信息可包括名称、email 地址、web 站点 URL、实际邮寄地址、用于当事人的计算机系统的机器位置、以及其他个人信息和描述怎样使用这种信息的使用策略。这些不同的标识要素的每一种此后将被指作为身份权利要求。重要地,该组身份权利要求至少包括标识计算机系统 102 和机器位置的用户友好的句柄。

[0035] 计算机系统 102 能够创建包含一些或所有自身身份信息 130 的身份信息文档 116 并向环境 100 内的任何其他节点发送身份信息文档 116,如图 1 中的虚线箭头所示。如这里所使用的,“身份信息文档”意思是为从一个机器发送到另一个机器以便允许接收身份信息文档的设备识别当事人和当事人相关联的数字事件的当事人的身份信息的子集。一个用于身份信息文档 116 的可能格式的细节下面将关于图 3 进行讨论。然而,一般来说,身份信

息文档 116 可以是以适合穿越各种类型的信道在完全不同的系统间传递信息的格式。用于从计算机系统 102 到接收系统,比如计算机系统 152 传递身份信息文档 116 的信道可是各种可能的媒体的任何一种。例如,emai1、即时消息、广播、和一些其他可用作为信道的机制。而且,信道可能是安全的或可能不是安全的。

[0036] 计算机系统 152 是访问节点的一个例子并且包含读取进入的身份信息文档 116 并根据不同变量接受或拒绝它的控制模块。例如,如果身份信息文档 116 来源于已知的当事人,计算机系统 152 将接受并存储身份信息文档 116。然而,如果身份信息文档 116 来源于一个未知的当事人,或者如果害怕冒充者有足够的动机来打开并修改或仿造身份信息文档 152,则计算机系统 152 可拒绝身份信息文档 116 或寻求其权威机构的进一步验证。

[0037] 一个实施例中,一旦接受了身份信息文档 116,它包含的特性权利要求被附加到已识别的计算机系统 152 的身份信息数据库 156 上,数据库可在未来使用这种信息来校验并验证计算机系统 102 并使用与不可能另外信任的那个当事人交互的信道。那么,由身份信息文档 116 表示的当事人可以,例如,被验证并可以访问计算机系统 152 上的资源,比如存储在类似计算机系统 102 的数据库 104 的数据库中的 文档。

[0038] 此外,计算机系统 152 接受并在其数据库 156 中存储身份信息文档 116 之后,它会为计算机系统 102 的当事人使用身份权利要求以便容易和快速地访问包含在计算机系统 102 的数据库 104 内的文档,下面将关于图 4-6 做详细解释。

[0039] 然而,一般来说,计算机系统 152 具有截取请求以访问计算机系统 102 上的文档的解析模块 160,这种请求可能来自于使用计算机系统 152 的当事人或可能是自动产生的。来自当事人的最初请求包括用户友好的句柄,例如来自计算机系统 102 的用户友好的句柄身份权利要求。解析模块 160 将用户友好的句柄转换为机器位置,也从计算机系统 102 中接收并在计算机系统 152 的 web 浏览器内输入适当的信息,反之,在计算机系统 102 上访问请求的数据。因为解析模块 160 的解析操作,计算机系统 152 的当事人不需要为计算机系统 102 记住机器位置、IP 地址或公共密匙,但相反地,只需要记住用户友好的句柄(以及相关联的路径)。

[0040] 本发明的一个实施例中,计算机系统 152 也包含自身身份信息(未显示)并且计算机系统 102 也包含控制模块(未显示)和已识别的身份数据库(未显示)。为了使计算机系统 152 的当事人可以访问计算机系统 102 的数据库 104 内的文档,计算机系统 152 的当事人必须在他或她被准许访问数据库 104 中的文档之前向计算机系统 102 发送自己的身份信息文档 158。换而言之,必须存在为计算机系统 152 的当事人的身份信息文档 116 和 158 的互换以容易地请求并获得对数据库 104 中的文档的访问。或者,计算机系统 102 不可能要求验证或认证进程而允许任何访问当事人访问包含在数据库 104 中的文档。这种情况下,只有计算机系统 102 需要向计算机系统 152 发送身份信息文档 116 以便使系统 152 访问数据库 104。即,只需要一种从发布节点到访问节点的身份信息文档的单向交换。

[0041] 图 2 显示了可表示比如图 1 显示的 102 或 152 的其中一个节点的计算机系统 200,该系统依照本发明接收并传播信息和发布及共享文档。系统 200 至少具有一个处理器 202 和存储器 204。处理器 202 使用存储器 204 在数据库,比如数据库 104、自身身份信息 130 和已识别的特性数据库 156 内存储文档。

[0042] 在最基本的配置中,图 2 中用虚线 206 说明计算系统 200。此外,系统 200 也包括

附加的存储器（可移动的和 / 或不可移动的），包括但不限于，磁盘或光盘或磁带或光带。在图 2 中用可移动的存储器 208 和不可移动的存储器 210 说明这种附加的存储器。计算机存储介质包括易失性的和非易失性的介质、可移动的和 不可移动的介质，这些介质以用于信息存储的任何方法或技术，比如计算机可读指令、数据结构、程序模块或其它数据来实现。存储器 204、可移动的存储器 208 和不可移动的存储器 210 是计算机存储介质的所有例子。计算机存储介质包括但不限于，RAM、ROM、EEPROM、闪存或其它存储技术、CDROM、数字化视频光盘 (DVD) 或其它光盘存储器、磁性磁带、磁性录音带、磁性磁盘存储器或其它磁性存储器设备，或可被用于存储需要的信息并可由系统 200 访问的任何其它介质。任何这样的计算机存储介质是系统 200 的一部分。根据计算设备的配置和类型，存储器 204 可以是易失性的、非易失性的或两者的结合。

[0043] 系统 200 也可以包含允许设备与其他设备通信的设备，比如图 1 显示的其他节点 108、110 或者 152 的通信连接 212。此外，系统 200 可具有比如键盘、鼠标、笔 (pen)、声音输入设备、触摸输入设备等的输入设备 214。也可以包括比如显示器、扬声器、打印机等的输出设备 216。所有这些设备在本领域是已知的，并不需要在这里详细描述。

[0044] 计算机系统 200 一般包括至少一些形式的计算机可读介质。计算机可读介质可以是可由系统 200 访问的任何可用介质。作为例子，而非限制，计算机可读介质可包括计算机存储介质和通信介质。计算机存储介质以上已经作出了描述。通信介质一般包括计算机可读的指令、数据结构、程序模块或在调制数据信号比如载波波形或其它传输装置中的其它数据并且包括任何信息传递介质。术语“调制数据信号”意思是信号中具有一个或多个它的特征被设置或以编码信息的方式变换的信号。作为例子，而非限制，通信介质包括比如有线网络或直接有线连接的有线介质，和比如声频、RF、红外线和其它无线介质的无线介质。任何以上的组合也应该包括在计算机可读介质的范围内。

[0045] 图 3 说明为可代表为图 1 显示的一个或两个身份信息文档 116 和 158 的身份信息文档 300 的示例性的格式。作为数据结构，身份信息文档 300 是身份权利要求和被公共密匙约束并由嵌入的使用策略所控制的其他属性 / 性质规定的集合。XML 可被用于作为身份信息文档的编码语言。然而，其他格式被认为是同样适合的。如果身份信息文档 300 的要素包含必须维持的机密性，它们也可以任选地被加密。

[0046] 身份信息文档 300 内的数据可被分为两个种类，包括一组逻辑组件 302 和一组属性标记 316。身份信息文档 300 有六个主要的逻辑分量：1) 当事人标识符 304；2) 一个或多个当事人的身份权利要求 306；3) 一个显示名称和 0 个或多个当事人的有选择性的揭示的属性 308；4) 一个或多个用于当事人的以任何可接受的格式（例如，X509v3 证书内的公共密匙 310）封装的密匙 310；5) 表达了当事人的个人要求的使用策略 312；和 6) 全部身份信息内容之上的数字签名 314，该签名保护数据的完整性并在身份信息升级的情况下认证发送者。下面将依次讨论这六个逻辑分量 302 的每一个。

[0047] 当事人标识符 304 是标识当事人的用户友好的句柄，该当事人是包含在身份信息文档 300 内的身份权利要求的当事人。如果当事人是人的话，优先的当事人标识符 304 是当事人的 email 地址。然而，当事人标识符应被广泛理解为独特地标识了当事人的任何类型的用户友好的句柄，并可包括但不限于，email 地址、电话号码、移动电话号码等等。

[0048] 身份权利要求 306 包括附加的关于为身份信息文档主题的当事人的构造信息。身

份权利要求应被广泛理解为有关当事人的描述信息,它可包括但不限于,实际的邮寄地址、电话号码和传真号码、雇主信息、出生日期等。即使更为具体地,“身份权利要求”是有关一个实体(人、团体等)独一无二地真实的。因此,一些情况下,电话号码是为一个人合法的身份权利要求。例如,移动电话号码,直拨工作号码或家庭号码可以是对于某个不共享移动电话号码、直拨工作号码或是独自生活的人的合法的身份权利要求。其他的情况下,电话号码可能不是单个人的合法的身份权利要求,比如由一家人共享的家庭电话号码。这种情况下,家庭电话号码可能是身份权利要求以表示一家人而非一个个体。

[0049] 机器位置 308 为当事人的计算机系统提供了独特的地址,并可包括但不限于,IP 地址或公共密匙。类似实际的街道地址,机器位置对分布式网络中的计算机系统定位、与之连接和 / 或与之通信是必需的。如果当事人具有多于一个的计算机系统或如果计算机系统是移动的,比如膝上计算机系统或 PDA,机器位置 308 实际上可包括一机器位置列表。一个实施例中,每个机器位置可包含一存储在那个机器位置上的文档列表。例如,如果当事人有在“照片”路径名称处存储 jpeg 文档的第一个计算机系统和在“音乐”路径名称处存储声音记录的 第二个计算机系统,则机器位置 308 可包括用于第一个和第二个计算机系统的每一个的 IP 地址并且具有一指示,指明“照片”被存储在用于第一计算机系统的机器位置上以及指明“音乐”被存储在为第二个计算机系统的机器位置上。

[0050] 密匙部分 310 包含一个或多个密匙,比如封装在证书格式(例如 X509v3 证书)内的公共密匙。密匙 310 可为公共密匙并且包括在身份信息内作为识别信息或身份信息的主题。如果使用证书,它可能是自我签名或由证书权威机构发布的。

[0051] 使用策略 312 为身份信息文档 300 的内容传递有关许可的使用的当事人的指令。例如,使用策略 312 可指示身份信息的内容不应被泄露给其他人。接受者的已识别的身份信息数据库,比如图 1 中的数据库 156 将使用策略与定义当事人的信息的剩余部分一起存储。

[0052] 数字签名 314 提供给当事人在身份信息文档内签名数据的能力。XML 签名具有三种有关签名文档的方式:封装、被封装和被分离。依照本发明的一个实施例,当签名身份信息内容时,身份信息文档使用 XML 已封装的签名。

[0053] 身份信息文档 300 能传递关于身份信息文档 316 本身的六个或更多的属性标记 316。尽管没有显示,属性标记可包括为身份信息文档 300 的 ID 值、文档 300 的版本信息和 / 或文档 300 代表的当事人类型,例如,人、计算机或组织。也可以使用其他的属性标记。

[0054] 一个实施例中,将身份信息文档以一般化的方式存储在主要的计算机系统内,比如以上分别结合图 1 和图 4 描述的系统 102 和 402。

[0055] 图 4 说明关于在两个或多个计算机系统 402 和 450 之间访问和共享或发布文档的功能性的部件。即,图 4 表示依照本发明的各方面的软件组件或模块。特别是,图 4 说明了依照本发明用于发布和访问文档的发布节点或计算机系统 402 以及访问节点和计算机系统 452 和它们相关联的模块。计算机系统 402 除了未显示的其他模块外还具有下列部件:1) 数据库 404;2) 身份信息文档模块 414;3) 用户界面模块 416;4) 验证和发布模块 418;5) 存储器访问模块 420;6) 通信模块 422;和 7) 自身身份信息数据库 424。

[0056] 类似图 1 显示的数据库 104,数据库 404 包含可被组织成文件夹 406、408、410 和 412 的文档。此例中,这些文档表示向系统 452 发布并因此由系统 452 访问的文档。

[0057] 用户界面模块 416 允许计算机系统 402 的当事人访问并控制任何其他的模块,包括但不限于,存储器访问模块 420、身份信息模块 414 和通信模块 422。尽管本发明以及特别地,图 4 显示的例子期望在系统 402 上的用户交互,但这不是完成本发明的各方面所必需的。

[0058] 存储器访问模块 420 允许计算机系统 402 和 / 和当事人访问存储在系统上的数据,比如包含在数据库 402 内的数据和 / 和包含在自身身份信息数据库 424 内的数据。或者,计算机系统 402 可通过其他模块,比如身份信息文档模块 414 或验证和发布模块 418 来访问存储器访问模块 420。当事人使用用户界面模块 416 来控制存储器访问模块 414。

[0059] 身份信息文档模块 414 通过使用存储器访问模块 414 检索以从信息数据库 424 中拉出数据来创建身份信息文档,比如图 3 显示的身份信息文档 300。身份信息文档模块 414 通过用户界面模块 416 针对来自当事人的命令创建身份信息文档或者在没有直接来自当事人命令的情况下,通过标准化的过程来创建身份信息文档。身份信息文档模块 414 向通信模块 422 传递身份信息用于与网络中的其他节点进行通信。在其他的实施例中,身份信息文档被简单地存储在存储器中,并且在请求时,通过通信模块 422 向另一个系统传递文档。

[0060] 通信模块 422 控制计算机系统 402 和网络中的其他节点之间的通信,包括向其他网络节点,比如计算机系统 452 发送并从其中接收信息。一般来说,当事人通过用户界面模块 416 来控制通信模块 422 并可通过这一进程来命令将身份信息文档发送给其他计算机系统,比如计算机系统 452。通信模块 422 也允许当事人向网络的其他节点发送其他类型的信息,比如 email。

[0061] 验证和发布模块 420 接收请求以通过通信模块 422 从其他网络节点访问并发布文档,比如在数据库 404 内的那些。一个实施例中,验证和发布模块 422 执行门控(gate-keeping)功能并尝试验证访问计算机系统具有来自当事人的许可以接收发布的文档。如果存在许可,验证和发布模块 420 使用存储器访问模块 420 以检索要求的文档并通过向通信模块 422 发送来发布这些文档用于与访问计算机系统通信。如果不存在许可,验证和发布模块 420 拒绝发布的请求,它通过通信模块 422 连接到访问者。在替代性的实施例中,验证和发布模块 420 不扮演守门的角色,而是接收并发布所有请求的文档。

[0062] 计算机系统 452 是访问节点的例子,与图 1 的节点 152 类似,并包含下列部件:1)通信模块 454;2)验证模块 460;3)存储模块 458;4)名称解析模块 456;和 5)用户界面模块 462。

[0063] 与用户界面模块 416 类似,用户界面模块 462 允许计算机系统 452 的当事人访问并控制任何其他的模块,包括但不限于,通信模块 422。因此,例如,系统 452 的当事人可能使用用户界面模块 416 来指示通信模块 422 向发布节点 402 发送发布文档的请求。

[0064] 类似通信模块 422,通信模块 454 控制计算机系统 452 和网络的其他节点,间的通信,包括从其他网络节点,比如计算机系统 402 发送并从其中接收信息。通信模块 454 负责向验证模块 460 转发从其他网络节点接收的身份信息文档。

[0065] 验证模块 460 负责翻译身份信息文档并确定它们是否来自可信任的来源、可信任的信道或者可以被认证。如果身份信息文档被接受,验证模块向存储模块 458 传递身份信息文档。实质上,验证模块 460 涉及图 1 内的控制模块 154 的一些功能,因为它读取进入的

身份信息文档 116 并依据不同的变量接受它或拒绝它。

[0066] 存储模块 458 存储身份信息文档用于以后由计算机系统 452 使用。由于有了验证模块 460，存储模块 458 也执行结合图 1 显示并描述的控制模块 154 的一些功能，因为它存储接受的身份信息文档。

[0067] 最后，名称解析模块 456 负责截取请求以访问已发布来自另一个网络节点、以来自通信模块 454 的用户友好的句柄的形式的文档。如以上讨论，该请求最可能是通过用户界面模块 462 来自当事人的。名称解析模块 456 进一步负责搜索存储模块 458 以找到带有匹配截取的用户友好的句柄的当事人标识符（比如图 3 中的当事人标识符 304）的身份信息文档、修正该请求以用在身份信息文档中提出的机器位置取代或替代用户友好的句柄、并向通信模块 454 发送返回请求以机器位置的形式发布文档。名称解析模块 456 与来自图 1 的解析模块 160 类似，因为它截取来自访问节点的请求以访问文档、为发布节点将用户友好的句柄转换为机器位置、并在计算机系统 152 的 web 浏览器内输入适当的信息，反之，在发布节点上访问请求的数据。

[0068] 图 5 显示了用于向访问计算机系统，比如图 1 的计算机系统 152 或图 4 的计算机系统 452 发布位于发布计算机系统，比如图 1 的计算机系统 102 或图 4 的计算机系统 402 上的文档的方法。流程 500 一般涉及由访问节点执行的进程。

[0069] 流程 500 始于存储操作 502，其中身份信息文档，比如一个来自发布节点的文档被存储在访问计算机系统，比如在图 1 的已识别的数据库 156 上的一个位置内。类似图 3 中显示的身份信息文档 300，接收的身份信息文档将至少包含标识发布系统的当事人，比如 email 地址的用户友好的句柄和用于当事人的计算机系统的机器位置，比如 IP 地址。其后某个时刻，截取操作 504 截取最初请求以访问存储在发布节点上的已发布的文档。该请求可能是一个由访问节点的当事人启动的请求、一个由访问计算机系统内的另一个模块启动的请求、或是一个自动的请求。该请求将以标识发布节点的当事人或发布节点本身的用户友好的句柄的形式或者包含发布节点的当事人或发布节点本身。例如，这种请求可访问定位于 e-mail 地址的文档。

[0070] 接着，搜索操作 506 搜索先前接收的并存储的身份信息文档以确定当事人标识符是否匹配在请求操作 504 内接收的用户友好的句柄。如果系统不能在步骤 506 定位匹配的身份信息文档，则流程 500 分出分支 N0507 通知当事人或其他模块该请求已经失败。一旦通知当事人请求已经失败，进程 500 终止。此时，当事人可重新输入这个或另一个类似的请求以启动进程。

[0071] 如果相反搜索操作 506 定位匹配的身份信息文档，即具有匹配在步骤 504 接收的 e-mail 地址的当事人标识符的一个文档，流程 500 分出分支 YES 给确定操作 508。确定操作 508 确定机器位置，这包括于在步骤 506 定位的身份信息文档中。

[0072] 接着确定操作 508，解析操作 510，用机器位置例如，IP 地址 123.123.023.002 替代用户友好的句柄，例如 email 地址。接着，发送操作 512 以机器位置的形式，而不是以用户友好的句柄的形式向发布节点发送请求以发布文档。

[0073] 步骤 506 和 508-512 发生在情景背后并不向当事人显示。相反地，它显示给当事人他的或她的用于访问已发布文档的请求是以用户友好的句柄、email 地址而不是以无意义的机器位置的形式被传递。这种方式下，当事人可以通过仅关于标识发布计算机系统的

当事人的用户友好的句柄的知识来访问位于不需要知道或记住麻烦的数字,比如 IP 地址以访问这些文档。

[0074] 图 6 同样显示了用于发布位于发布计算机系统上的文档的方法,但显示了由发布节点,比如计算机系统 102 或 402 和访问节点,比如计算机系统 152 或 452 执行的进程。

[0075] 流程 600 始于传递操作 602,它向另一个节点,比如访问节点传递用于一个或多个文档的位置的路径名称和标识发布节点的当事人的用户友好的句柄。例如,发送操作可能包含来自发布节点的当事人的 email 消息,其名字是 Bob,这样说 :在 bsb@xyz. com/photos 取出我的照片。或者,当事人可以通过电话呼叫、传真文件或一些其他的方式向访问节点或当事人发送路径名称和用户友好的句柄。流程 600 移动至接收操作 604,其中访问机器接收文档的路径名称和标识发布机器的当事人的用户友好的句柄。接着,发送操作 606 发送给访问节点用于发布机器的当事人的身份信息文档,此例中,是 Bob 的身份信息文档。接收操作 608 接收 Bob 的身份信息文档,随后的是存储操作 609,它将身份信息文档存储在已识别的特性数据库内,与结合图 1 描述并显示的数据库 156 类似。

[0076] 在替代性的实施例中,验证操作(未显示)在接收操作 608 之后存储操作 609 之前发生。验证操作试图验证由身份信息文档所表示的当事人并就是否接受并存储身份信息文档做出决定。

[0077] 其后某时,截取操作 610 截取最初的请求用于访问文档。这种最初的请求可来源于当事人或一些其他的来源并寻求在用户友好的句柄 / 路径位置,比如 bob@xyz. com/photos 处获得对文档的访问。接着,解析操作 612 解析最初的请求以通过用图 5 中详细描述的进程用机器位置取代用户友好的句柄,即找到匹配的身份信息文档、确定机器位置并用取代机器位置来替代用户友好的句柄以创建修正的请求。

[0078] 在替代性的实施例中,解析操作(未显示)分开用户友好的句柄和路径名称并搜索仅与最初请求的用户友好的句柄部分的匹配。例如,解析操作卸下“/ 照片”并在 bob@xyz. com 处搜寻带有 Bob 的 email 的当事人标识符。

[0079] 仍是在另一个替代性的实施例中,当事人的身份信息文档包括多于一个机器位置和附加的搜索操作(未显示),搜索操作在身份信息文档内搜索每个机器位置以确定哪个位置包含包括截取请求内的路径名称。然后,解析操作 612 取代与最初的请求内提出的路径名称相一致的机器位置。

[0080] 解析操作 612 完成之后,发送操作 614 使用机器位置而非用户友好的句柄为已发布的文档发送修正的请求。如果包括了路径名称,发送操作 614 进一步包括请求以访问位于那个路径上的文档。

[0081] 在这个点,流程 600 在接收操作 616 处返回到发布机器,接收修正的请求以在指定的路径上,这种情况下,是在照片文件夹、比如图 1 中的文件夹 118 上访问文档。接着,验证操作 618 确定访问节点的当事人是否被授权查看请求的文档。如果访问当事人未被授权,流程 600 分出分支 NO 给否定操作 620,它拒绝了用于访问文档的请求,并且进程终止。

[0082] 如果访问当事人被授权,流程 600 分出分支 YES 到定位操作 622,它使用包括在发送操作 614 内的路径名称来定位请求的文档。最后,发布操作 624 发布请求的文档并且流程 600 终止。

[0083] 在本发明的一个实施例中,验证操作 618 核查以确定访问当事人是否被列出在已

识别的特性数据库内,即,访问当事人是否先前已经发送给发布节点他的或她的身份信息文档。如果答案为是,验证操作 618 分出分支 YES 到定位操作 622。因此,在这个实施例中,对将要由一个机器向另一个机器发布的文档来说,要求身份信息文档的互换。这是发布文档最安全的方式。

[0084] 在本发明的替代性的实施例中,验证操作 618 不要求访问当事人发送它的身份信息文档。相反地,验证操作 618 在确定是否允许访问请求的文档时要考虑其他的变量或者验证操作 618 和否定操作 620 可从流程 600 中一起忽略。相反地,流程 600 将从接收操作 616 直接前进到定位操作 622。换句话说,发布机器可决定它允许任何人用其身份信息文档在它的系统上访问文档。尽管这种方法比上一种简单,但它不如要求身份信息文档的互换那样安全。

[0085] 仍是在另一个替代性的实施例中,通知操作(未显示)通知访问节点,用于访问文档的请求已经被否定。一旦通知,另一个发送操作(未显示)可发送给发布节点一代表访问节点或其当事人的身份信息文档并通过截取操作 610 启动该进程。如果发布节点已经接收了访问节点的身份信息文档,流程 600 更可能分出分支 YES 到定位操作 622 而非分出分支 NO 到否定操作 620。

[0086] 而且,在本发明的替代性的实施例中,身份信息文档的机器位置部分可包含公共密匙而非 IP 地址。正如这里所使用的,“公共密匙”应被广义地理解并被定义为包含有未识别意义的数字和 / 或字母的独特的当事人的编码。前述的系统和方法将如上所述地工作,但有一个例外,将在下面描述。

[0087] 当在身份信息文档内使用公共密匙作为机器位置时,公共密匙被用于使用对等名解析协议(“PNRP”)查找当事人的当前机器位置,它可能是 IP 地址。PNRP 一般包含包括公共密匙和当前机器位置的散列的分布式系统的知识。因此,公共密匙被用于发现当事人的“当前的”机器位置。作为这里使用,“当前的机器位置”应被广义地理解为意指在给定点的当时的机器位置。例如,如果计算机系统使用动态的 IP 地址,它的当前机器位置可从当时的第一个点改变到第二个、当时的后来的点。公共密匙和 PNRP 的使用将允许访问节点访问来自发布节点的文档,即使发布节点使用动态的 IP 地址。

[0088] 或者,如果机器是移动的,比如膝上电脑系统或 PDA,当前的机器位置可以改变。PNRP 也能够跟踪移动机器的当前的机器位置。而且,公共密匙和 PNRP 的使用会允许访问节点访问来自发布节点的文档,即使发布节点是移动的。

[0089] 如果公共密匙被用于作为机器位置,访问节点必须指定发布节点的公共密匙,以便为了获得对发布节点的文档的访问。访问节点获得发布节点的公共密匙的唯一方法是为发布节点发送访问节点自己的密匙。这种方式中,发布节点能够有效地通过控制向谁发送它自己的公共密匙来控制谁能够访问其资源。

[0090] 图 7 仍显示了本发明的另一个实施例,该实施例包括一种用于向访问计算机系统比如计算机系统 152 或 452,发布位于发布计算机系统,比如计算机系统 102 或 402 上的文档的方法。

[0091] 流程 700 始于向常规的 DNS 服务器注册加密的机器名称、主机域名和相关联的已注册的机器位置的注册操作。DNS 服务器一般存储有相应的已注册的机器位置、附加在主机域名上的机器名称,比如 IP 地址的列表。网络用户使用 DNS 服务器来为指定的机器查询已

注册的 IP 地址。作为这里使用，“加密的机器名称”意思是已经被改变为人们不能明白或在普通设备上使用的秘密代码的公共密匙。一种创建加密的机器位置的方法是对公共密匙应用算法。

[0092] 接着，传递操作 706 为一个或多个文档的位置传递路径名称和标识发布节点的当事人的用户友好的句柄。流程 700 移动至接收操作 706，其中访问机器接收为文档的路径名称和标识发布机器的当事人的用户友好的句柄。其后某时，发送操作 708 发送给访问节点用于发布机器的当事人的身份信息文档。这种身份信息文档至少包括为发布节点的当事人的当事人标识符、公共密匙和域名主机。接收操作 610 接收身份信息文档，跟随其后的是存储操作 712，它在已识别的特性数据库内存储身份信息文档，与结合图 1 描述并显示的数据 156 类似。

[0093] 其后某时，截取操作 712 截取最初的请求用于访问文档。最初的请求可来源于当事人或其他一些来源并寻求获得在用户友好的句柄 / 路径位置上对文档的访问。接着，使用图 5 中详细描述的进程，解析操作 714 解析在带有在与用户友好的句柄匹配的当事人标识符的身份信息文档内提出的公共密匙和域名主机的最初请求内的用户友好的句柄。

[0094] 接着，转换操作 718 在公共密匙上执行计算以将其转换为已加密的机器名称并且操作 720 将已加密的机器名称附加到域名主机。一个实施例中，转换操作包含对公共密匙执行算法，其中该算法与由发布节点在注册操作 702 中使用的算法相同。这种算法可以是一般由许多网络节点使用的标准算法，或者是以一些其他的方式由访问节点接收的指定的算法。

[0095] 然后，流程 700 移动至查找操作 722，它使用已加密的机器名称 / 域名主机的结合来在 DNS 服务器上查找已注册的机器位置。查找操作 722 完成之后，修正操作 724 修正最初的请求以用已注册的机器位置取代用户友好的句柄并使用已注册的机器位置而非用户友好的句柄为发布的文档发送修正的请求。如果涉及路径名称，发送操作 614 进一步包括请求以访问位于那个路径上的文档。

[0096] 使用由流程 700 说明的方法的益处是当使用常规的 DNS 服务器时，它允许发布机器应用附加的安全措施。一般地，DNS 地址是公开可用的并且潜在的黑客能够使用 DNS 服务器来得知发布节点的机器名称和机器位置。然后，黑客可以使用这种信息来获得经授权的访问发布节点的资源。向 DNS 服务器注册已加密的机器名称阻止了黑客得知公共节点的机器名称，但却使得经授权的用户获得对发布节点资源的访问更加困难。进程 700 允许经授权的访问节点用 仅为用户友好的句柄的知识来访问发布节点的资源。发布节点为了访问发布节点的资源，不需要知道不友好的已加密机器名称或域名主机。安全得到增强，因为访问节点为了使用名称解析方法必须接收发布节点的身份信息文档。

[0097] 尽管本发明已经以特定于计算机结构特征、方法行为和由计算机可读介质的语言做出了描述，但应该理解，附加的权利要求中定义的本发明并不必然限定于已描述的特定特征、行为或媒体。作为例子，可以使用除 XML 之外的不同的格式来编码标识信息。因此，揭示的特定的结构特征、行为和媒体是作为实现主张的本发明的示例性的实施例。

[0098] 使用以上描述的名称解析的方法，本发明建立了标识发布机器的当事人的用户友好的句柄可与机器位置相关联或解决机器位置以便访问机器的当事人为了在发布机器上访问请求的文档，只需要知道用户友好的句柄。而且关联进程是透明的，并在不用当事人的

知识或当事人的卷入就可以发生。

[0099] 以上的说明、例子和数据提供了本发明组成的制作和使用的完整描述。由于可以做出本发明的许多实施例，而不脱离本发明的精神和范围，那么本发明驻存于其后附加的权利要求中。

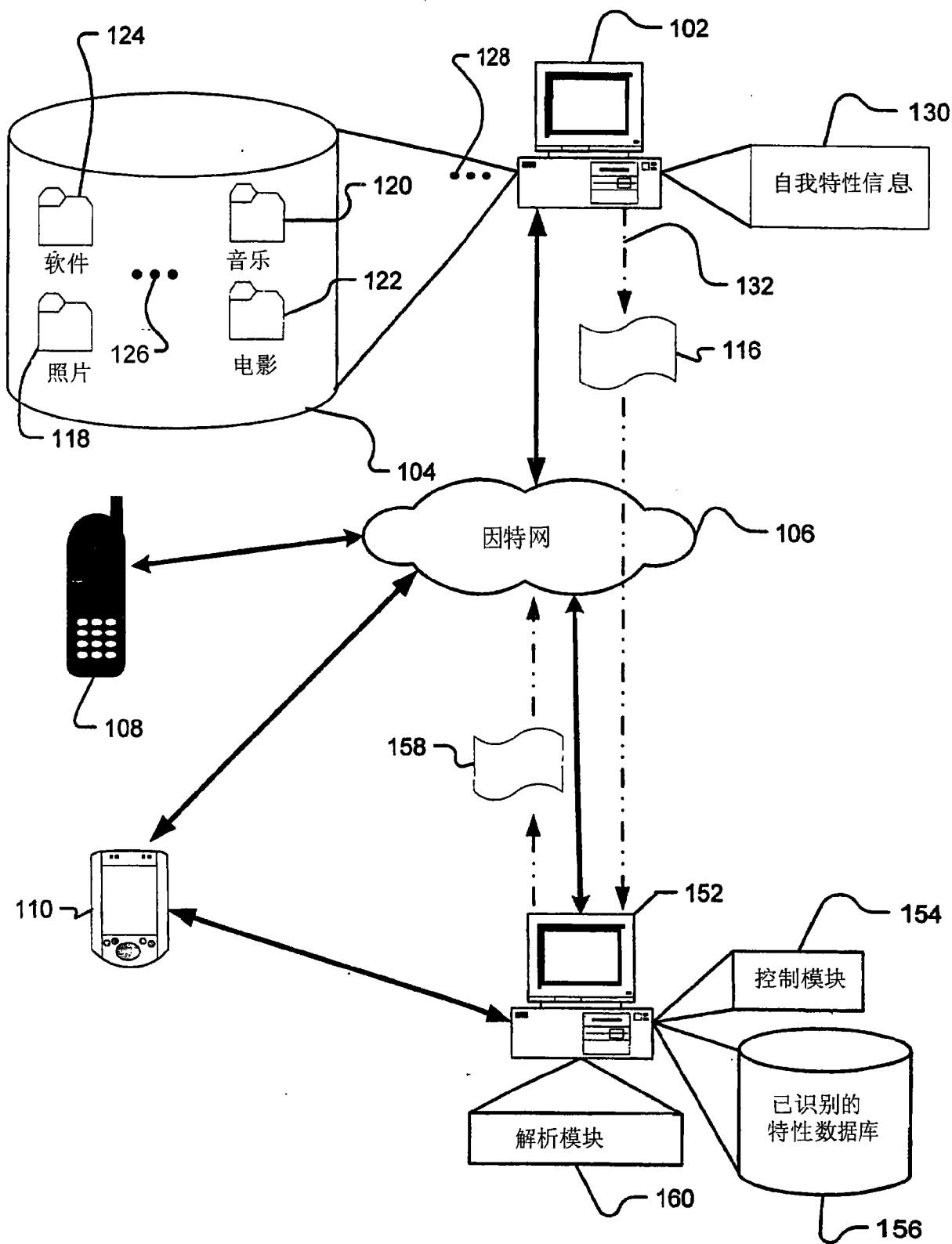


图 1

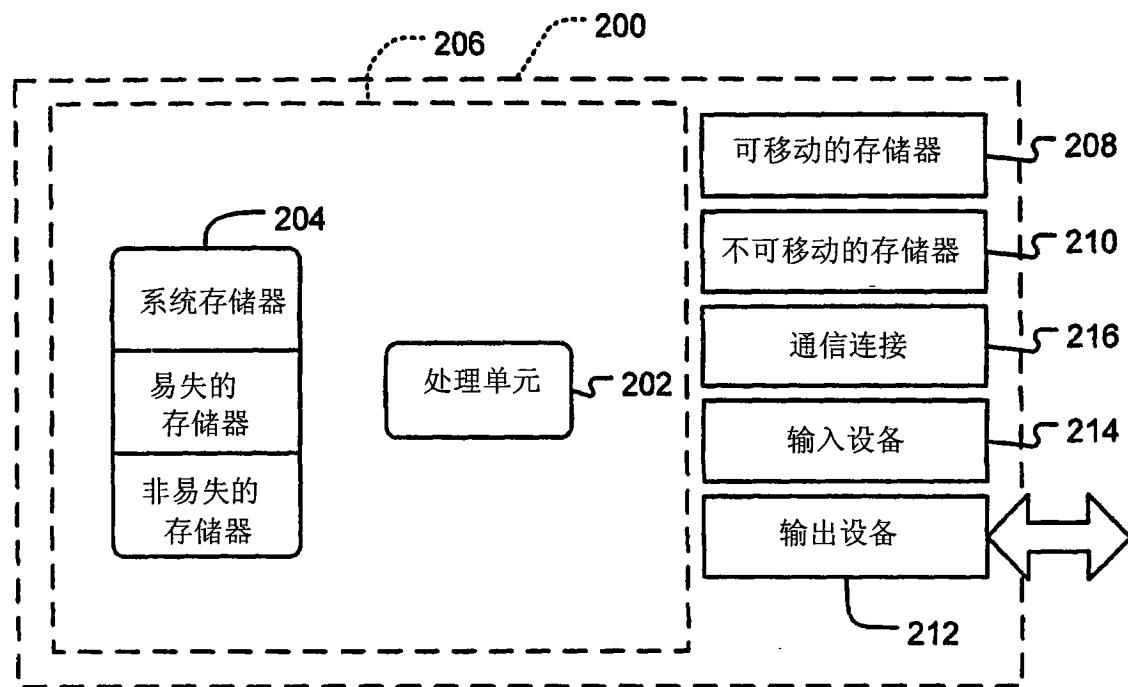


图 2

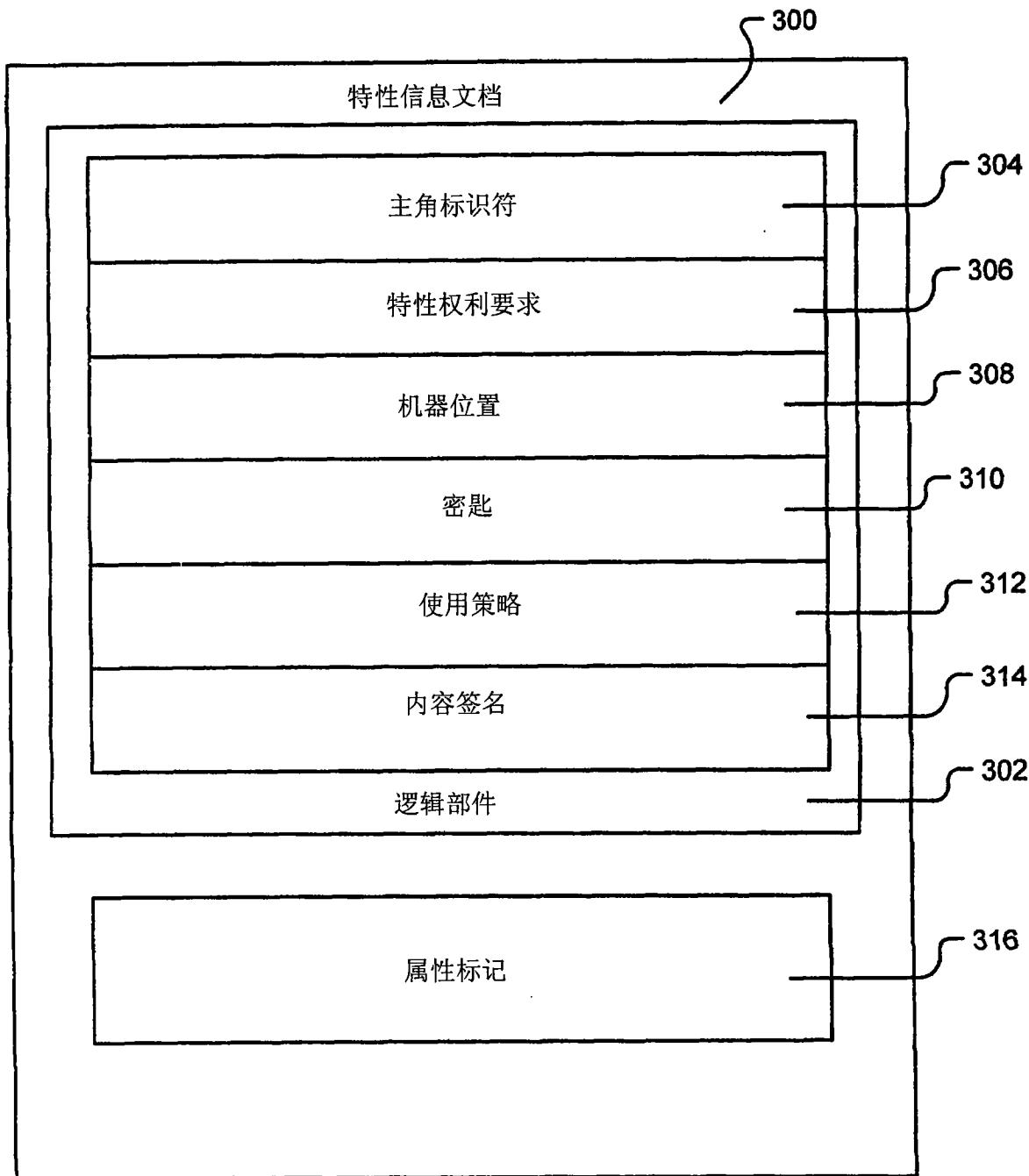


图 3

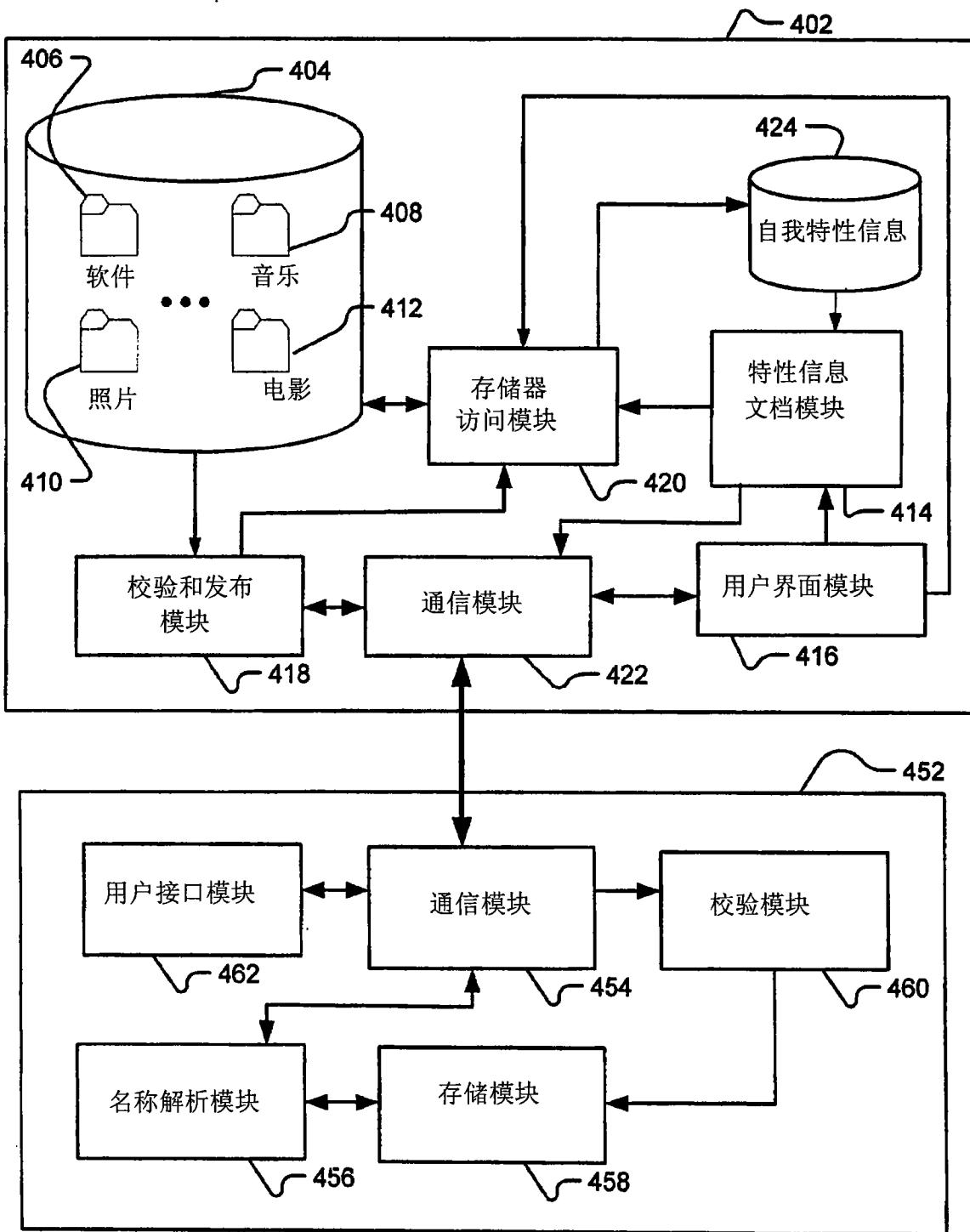


图 4

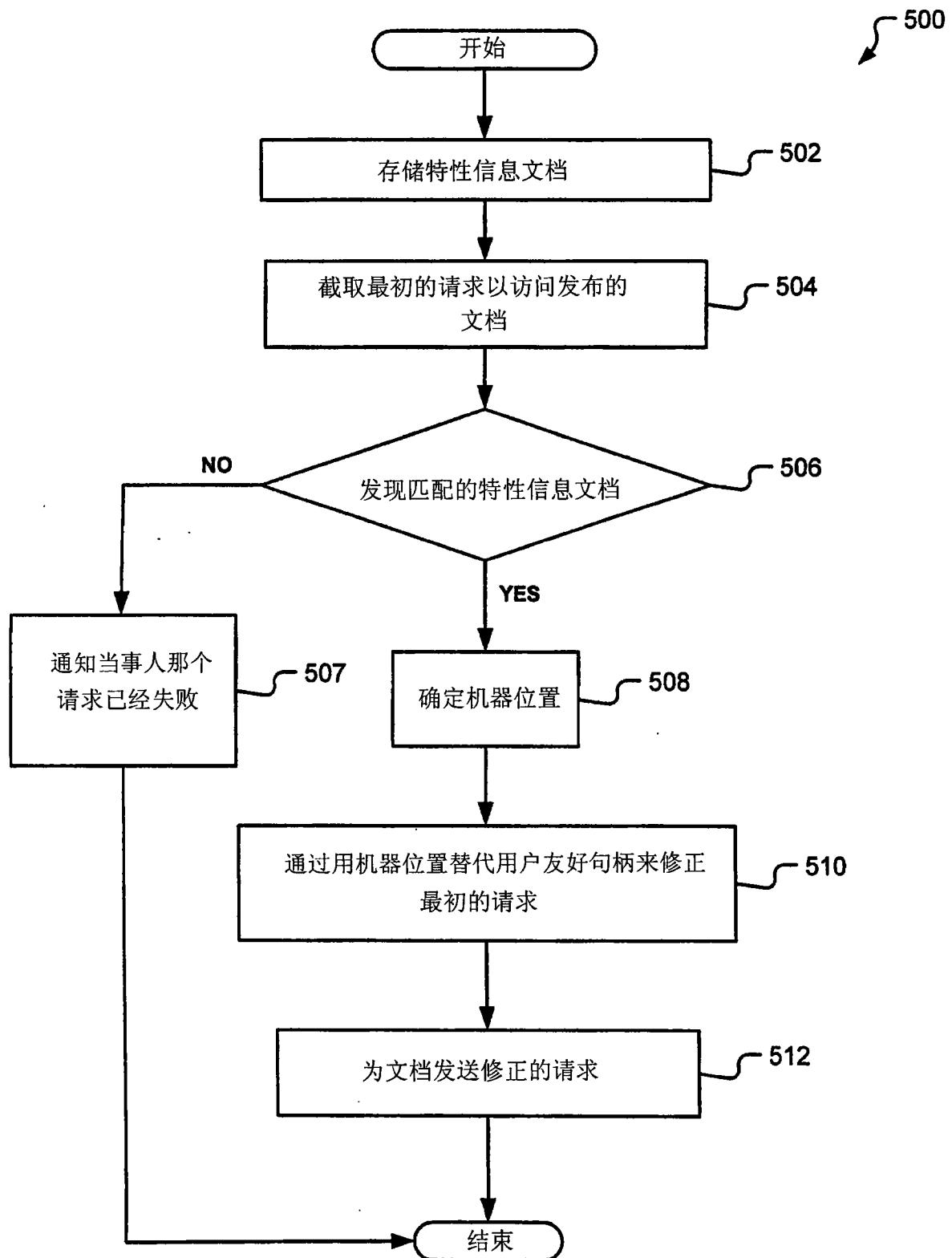


图 5

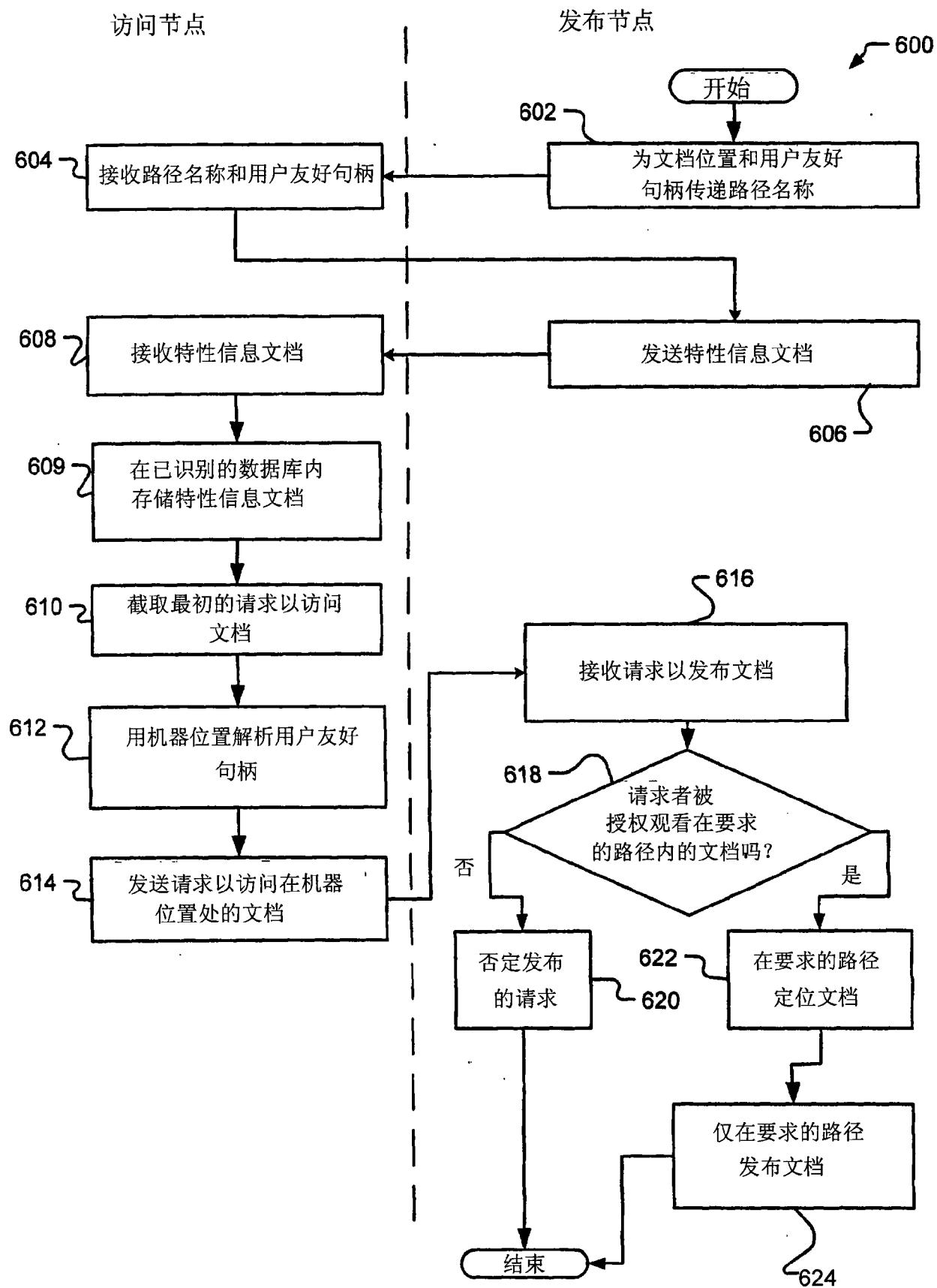


图 6

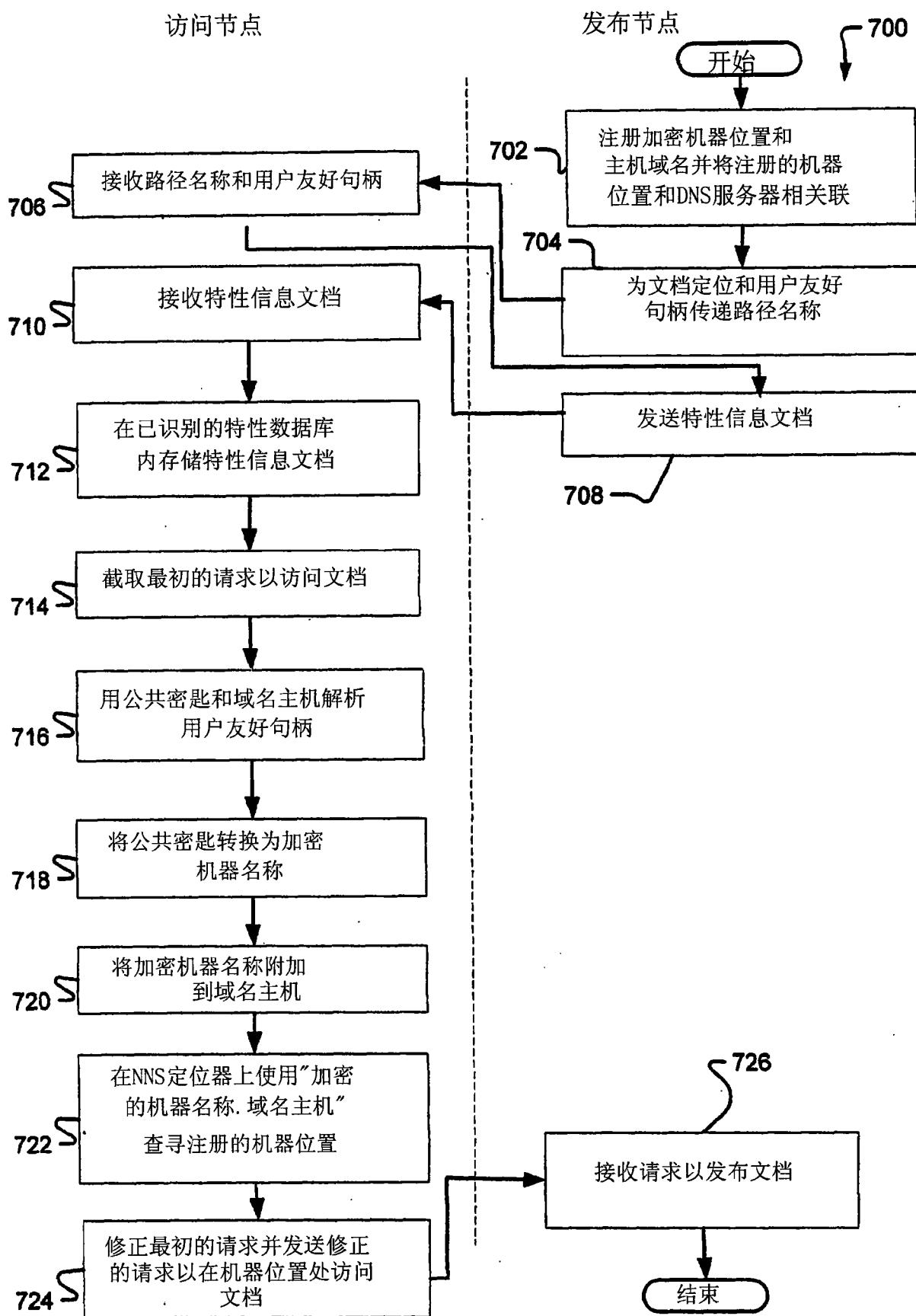


图 7