(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103947173 A
(43)申请公布日 2014.07.23

(21)申请号 201280046888.1
(22)申请日 2012.09.24
(30)优先权数据
TO2011A000858 2011.09.26 IT
(85)PCT国际申请进入国家阶段日
2014.03.26
(86)PCT国际申请的申请数据
PCT/IB2012/055063 2012.09.24
(87)PCT国际申请的公布数据
WO2013/046109 EN 2013.04.04
(71)申请人 讯息网络有限公司
地址 意大利米兰
(72)发明人 M.A. 菲奥伦蒂诺 A.M. 加尔里
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 张涛 刘春元
(51)Int.Cl.
H04L 29/06(2006.01)
H04M 3/436(2006.01)

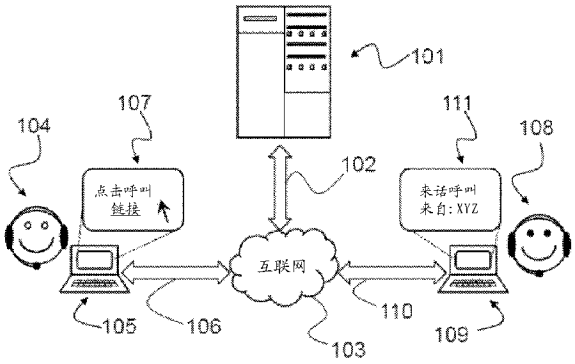
权利要求书2页 说明书9页 附图6页

(54)发明名称

用于管理两个用户之间的通信的方法和系统

(57)摘要

本发明涉及一种用于管理主叫用户(104)与被叫用户(108)之间的通信的方法,其中,所述通信通过互联网网络而实时发生,所述方法包括以下步骤:接收(201、301、401、501、601)来自主叫用户(104)的用以发起与被叫用户(108)的通信的请求;请求(202、302、402、502、603)所述主叫用户(104)提供身份元素;验证(203)所述主叫用户(104)的身份元素;将已验证的身份元素发送(204、305、406、504、606)到所述被叫用户(108)。本方法寻求在“点击呼叫”技术领域中的应用;在优选实施例中,所述身份元素包括验证元素传送到的所述主叫用户(104)的电子邮件地址。本方法进一步涉及一种用于管理主叫用户(104)与被叫用户(108)之间的通信的有关系统。



CN 103947173 A

1. 一种用于管理主叫用户(104)与被叫用户(108)之间的通信的方法,其中,所述通信通过互联网网络而实时发生,所述方法包括以下步骤:

- 接收(201、301、401、501、601)来自主叫用户(104)的用以发起与被叫用户(108)的通信的请求;

- 请求(202、302、402、502、603)所述主叫用户(104)提供身份元素;

- 验证(203、503)所述主叫用户(104)的所述身份元素;

- 将验证的所述身份元素发送(204、305、406、504、606)到所述被叫用户(108)。

2. 如权利要求 1 所述的方法,其中,所述身份元素导入到适用于接收信息元素的接收方,所述验证(203)所述身份元素的步骤包括:

- 传送(303、403)定址到所述身份元素的验证元素;

- 从所述主叫用户(104)接收(304、404)基于所述验证元素的回复,以确认(304、405)所述身份元素的可用性。

3. 如权利要求 2 所述的方法,其中,所述身份元素包括电子邮件地址,并且所述验证元素包括能够由所述主叫用户(104)激活的 web 链接,其中,所述方法包括以下步骤:接收(304)所述 web 链接的激活的确认。

4. 如权利要求 3 所述的方法,进一步包括以下步骤:与所述 web 链接的所述激活同时地向所述被叫用户(108)转发用以发起所述通信的请求。

5. 如权利要求 2 所述的方法,其中,所述验证元素(403)包括字母数字代码,并且其中,所述方法包括:对于所述主叫用户(104)请求(404)用于所述字母数字代码,以确证(405)所述主叫用户(104)匹配于所述验证元素。

6. 如权利要求 5 所述的方法,其中,所述身份元素包括蜂窝网络号码。

7. 如权利要求 1 所述的方法,其中,所述身份元素包括从电子身份装置获取(502)的至少一条信息。

8. 如权利要求 1 至 7 之一所述的方法,进一步包括以下步骤:存储(605)与验证的所述身份元素关联的信息。

9. 如权利要求 8 所述的方法,其中,在针对与验证的所述身份元素关联的已存储的信息而搜索(602)存储器之后,请求(202、302、402、502、603)所述身份元素。

10. 如权利要求 9 所述的方法,其中,所述已存储的信息包含在所述主叫用户(104)的终端(105)的存储器中,并且在该存储器中被搜索,并且所述方法进一步包括以下步骤:优选地自动对所述已存储的信息与跟 web 服务器(101)关联的存储器中所存储的附加引用信息进行比较。

11. 如权利要求 1 至 10 之一所述的方法,进一步包括以下步骤:向所述被叫用户(108)转发用以发起所述通信的请求;从所述被叫用户(108)接收接受信号;响应于所述接受信号而发起(701)所述通信。

12. 如权利要求 1 至 11 之一所述的方法,其中,所述通信包括语音、视频或文本通信。

13. 如权利要求 1 至 12 之一所述的方法,其中,在执行所述请求(202、302、402、502、603)、验证(203、503)和发送(204、305、406、504、606)步骤之前,必须逝去预定的时间,或必须接收到预定数量的通信发起请求。

14. 如权利要求 1 至 13 之一所述的方法,其中,在所述请求(202、302、402、502、603)、

验证(203、503)和发送(204、305、406、504、606)步骤之前,要求所述被叫用户(108)表达他/她的有关于所述通信的管理的偏好。

15. 一种用于管理至少一个主叫用户与至少一个被叫用户之间的通信的系统,所述系统包括至少一个处理器、至少一个操作存储器以及至少一个到互联网网络的连接,其特征在于,所述系统具体地适用于实现根据权利要求 1 至 14 之一所述的方法。

用于管理两个用户之间的通信的方法和系统

技术领域

[0001] 本发明涉及一种用于通过互联网来管理两个用户之间的通信的方法和系统。

[0002] 一般地，本发明寻求在互联网通信(特别是，“点击呼叫(Click-to-call)”类型的语音或电话互联网通信)领域中的应用。

背景技术

[0003] 互联网通信现已经变得广泛，并且使用许多不同的技术。可用的互联网通信技术包括所谓的“点击呼叫”技术，其中，用户可以点击 Web 页面上所示的元素以便实时请求对另一用户的即刻连接。典型地，这种通信通过语音(例如通过基于 IP 的语音(VoIP)协议)而发生，因此与传统电话或视频电话呼叫相似。

[0004] 在这种“点击呼叫”技术的变形当中，最有趣的一种变形允许主叫用户点击 web 链接以建立对由所点击的元素(例如链接)所标识的被叫用户的语音连接。以此方式，倘若互联网连接在两个用户之间是可用的，那么主叫用户可以“通过电话”联络到被叫用户，而不造成任何直接成本。在一些情况下，在 web 浏览器自身中实现用于语音和 / 或视频电话通信的软件，从而客户无需在他 / 她自己的操作系统中安装及配置任何附加的软件。这种特征在被叫用户被分配永久 web 链接时尤其有用，不会有任何时间限制，即使主叫方不知道用户的电话号码，他 / 她(被叫用户)也可以然后使该特征可用而作为联络到他 / 她的替换和免费手段。

[0005] 该技术在被叫用户是公司并且主叫用户是可能成为主顾的人时变得尤其有趣。在此局面下，“点击呼叫”技术对有效后继者呈现熟知的“免付费”号码。

[0006] 就这一方面而言很明显的技术的一个示例是 Skype© 服务。该服务允许用户通过相应的 Skype© 账户仅以一次点击来呼叫其它用户。然而，Skype© 服务要求两个用户都已经注册到服务，因此使得未注册的各用户之间的交互困难。

[0007] 由于想要改进“点击呼叫”通信的便捷度，因此允许任何主叫用户(甚至未注册的主叫用户)能够作出对被叫用户的呼叫变得必要。

[0008] 然而，还允许任何主叫用户发起通信可能引起问题。

[0009] 实际上，利用“点击呼叫”元素，想被可联络到的用户赚取了可见性，并且可能更容易地与第三方通信，但是同时，他 / 她将把他 / 她自己暴露于接收不想要的呼叫的风险。

[0010] 另外，由于“点击呼叫”服务的理想形式对于主叫用户是无偿的，并且与普遍的公共服务(诸如互联网)关联，因此存在这样的明确风险：被叫用户将被淹没于甚至来自恶意主叫用户的不想要的呼叫(这是一种“垃圾信息”)。

[0011] 致力于控制通过互联网的语音通信，Ryan 的专利申请 US2003/0152207 提出了一种控制系统，根据该控制系统，互联网电话通信服务的用户可以单独控制分配给各种被叫用户的通信选项，包括建立电话连接的可能性。

[0012] 在第一实施例中，Ryan 的专利 US2003/0152207 使用待由被叫用户填写的主叫用户标识符的列表，并且仅该列表中所包括的那些用户将被允许建立电话连接。如果一方面

该第一实施例有效地避免了不想要的呼叫的问题，则另一方面其明显地局限了用户交互的可能性，因为用户必须被包括于事先已知的“受欢迎”标识符的列表中。

[0013] 在第二实施例中，Ryan 的专利 US2003/0152207 采用了“紧急呼叫”模式，其中，即使主叫用户并未被包括在事先已知的“受欢迎”标识符的列表中，他 / 她也可以联系到被叫用户。在该第二实施例中，要求主叫用户提供电子邮件地址，然后验证代码将发送至该电子邮件地址，所述代码必须由主叫用户在 Web 页面上输入。如果主叫用户所输入的代码正确，则他 / 她将能够发起对被叫用户的呼叫。虽然该第二实施例确实限制了不想要的呼叫的问题，但是其仍然有过度限制用户通信的灵活性的缺点；因此，仅针对管理能够通过任意手段联系到被叫用户是极其重要的紧急情况推荐该方法。例如，甚至该第二实施例未对被叫用户给出用于依靠主叫用户的身份来决定是否应该应答呼叫的有用信息。

发明内容

[0014] 本发明的目的在于提供一种允许克服现有技术的上述缺点以及其它问题的方法和系统。特别是，本发明的一个目的是提供一种方法和系统，其通过改进“点击呼叫”服务的使用便捷度和安全性来使得对于用户而言更想要使用“点击呼叫”服务。

[0015] 本发明的另一目的是提供一种方法和系统，其中，主叫用户可以通过“点击呼叫”服务来容易地并且立即地发起与被叫用户的通信。

[0016] 最后，本发明的进一步的目的是提供一种方法和系统，其中，借助“点击呼叫”服务所呼叫的用户可以有效地过滤来话呼叫，并且可以避免任何不想要的呼叫。

[0017] 通过用于管理两个用户之间的互联网通信的方法和系统来达成本发明的这些和其它目的，其包括在作为本说明的一体部分的所附权利要求中所阐述的特征。

[0018] 基于本发明的一般性想法在于提供一种用于管理主叫用户与被叫用户之间的通信的方法，其中，所述通信通过互联网网络而实时发生，所述方法包括以下步骤：从主叫用户接收请求以发起与被叫用户的通信；请求所述主叫用户提供身份元素；验证所述主叫用户的身份元素；将所述已验证的身份元素发送到所述被叫用户。

[0019] 以此方式，所述被叫用户可以更好地估计是否应该应答“点击呼叫”呼叫。

[0020] 此外，“点击呼叫”通信服务的提供商可以能够将永久“点击呼叫”web 地址分配给其客户，并且能够管理被导入至想被呼叫的客户并且由可能想与所选择的被叫用户通信的多个主叫用户作出的通信请求。

[0021] 有利地，被叫用户被给予主叫用户的已验证的身份元素(即关于被叫用户的身份的偏于可靠的信息)；以此方式，主叫用户被通知主叫用户的某些个人数据。有利地，验证过程允许主叫用户获得对实际和有用的服务的访问，其中，他 / 她可以选择并且建立与被叫用户的通信，并且简单地通过提供待由服务提供商验证的身份元素来完成验证过程。

[0022] 优选地，身份元素导入到适用于接收数字信息的接收方，并且验证处理包括以下步骤：传送被定址到身份元素的验证元素；从主叫用户接收基于所述验证元素的回复以确认身份元素的实际可用性。有利地，这凭借通过简短但有效的过程来确证主叫用户所提供的身份元素与来自同一主叫用户的身份元素的实际可用性之间的对应性而改进了所述方法的安全性。以此方式，可以向被叫用户发送更可靠地表示主叫用户的身份的身份元素，从而被叫用户可以决定是否接听呼叫。

[0023] 在优选实施例中，主叫用户所提供的身份元素包括电子邮件地址，所述方法提供将验证链接传送到所述电子邮件地址；通过所述验证链接，所述主叫用户可以然后确认身份元素的实际可用性。

[0024] 在一个可能的优选实施例中，被叫用户所接收到的通信请求包括关于所述主叫用户的电子邮件地址的一条信息，并且通信请求是与所述主叫用户验证所述电子邮件地址同时作出的。

[0025] 在另一优选实施例中，主叫用户所提供的身份元素包括电话号码（优选地，蜂窝电话号码），所述方法提供将验证信息（诸如例如字母数字代码）传送到所述电话号码，然后对于主叫用户请求验证信息，以便确认所述身份元素的实际可用性，从而所述呼叫请求可以包括主叫方的电话号码。

[0026] 有利地，这两个实施例都依赖于已经普遍并且可用的工具，这允许改进主叫用户与被叫用户之间的实时通信。此外，这些标识符允许以合理程度的可靠性并且以对于用户而言快速且廉价的方式来提供身份元素。在再一优选实施例中，主叫用户直接提供由第三方所证实的数字标识符（例如包括“智能卡”的身份文档），从而所述标识符可以连同通信请求一起发送到被叫用户。要是智能卡标识技术变得普遍，那么该实施例可能显得尤其有利。

[0027] 优选地，在所有上面描述情况下，所述方法提供例如通过将“甜饼（Cookies）”存储到互联网浏览器而将验证确认存储到计算机终端中，主叫用户通过所述计算机终端来访问“点击呼叫”服务。对于单个被叫用户或对于可能在未来被呼叫的任何其它用户而言，这在仍然确保必要的安全性的同时，有利地避免了不得不针对来自同一用户的后续“点击呼叫”呼叫而重复验证过程。在已验证的身份元素已经被发送到被叫用户之后，所述方法进一步包括步骤：如果被叫用户接受所述呼叫，则开始通信。因此，虽然被叫用户的“点击呼叫”服务提供商提供关于主叫方的身份元素的信息，但允许被叫用户自由地决定是否建立通信；有利地，这改进了针对被叫用户（即服务的主要客户）的服务质量，被叫用户被置于能够根据他／她的偏好来处理呼叫流程的状况。

[0028] 特别是，根据本发明的用于管理主叫用户与被叫用户之间的通信的方法可应用于通过依赖于通信网络（诸如互联网）而建立的实时语音或视频电话通信。

[0029] 优选地，通过数字计算机系统来实现所述方法，所述数字计算机系统包括或关联于合适的软件，适用于管理主叫用户和被叫用户之间的通信。所述计算机系统可以包括Web服务器，例如受控于服务提供商的、被连接到互联网并且适用于通过该Web服务器接口至主叫用户和被叫用户所使用的计算机终端的Web服务器。

[0030] 根据下面的详细说明以及以非限制性示例的方式供给的附带的附图，本发明的进一步的目的和优点将变得更清楚。

附图说明

[0031] 在说明中所参照的附图中，相同参考符号指明相同或等同元素或动作。

[0032] - 图1示意性示出两个用户之间通过互联网的“点击呼叫”通信；

- 图2是图解根据本发明的方法的实施例的流程图；
- 图3是图解根据本发明的方法的实施例的进一步的流程图；
- 图4是图解根据本发明的方法的实施例的进一步的流程图；

- 图 5 是图解根据本发明的方法的实施例的进一步的流程图；
- 图 6 是图解根据本发明的方法的实施例的进一步的流程图；
- 图 7 是图解根据本发明的方法的实施例的进一步的流程图。

具体实施方式

[0033] 图 1 图解服务提供商的服务器 101 进行的“点击呼叫”通信的管理。服务器 101 通过连接 102 连接到允许装置交换数据的数字网络。在该示例中，连接 102 允许服务器 101 连接到互联网 103。

[0034] 服务器 101 向多个用户给出对“点击呼叫”系统的访问。

[0035] 用户 104 具有通过连接 106 而连接到互联网 103 的计算机终端 105。例如，用户 104 可以具有通过 WiFi 系统连接到互联网的膝上型装置。替换地，用户 104 可以具有借助 WWAN 技术连接到互联网的智能电话。

[0036] 服务器 101 适用于向终端 105 给出对可以根据用户 104 而进行动作的至少一个“点击呼叫”链接的访问。

[0037] 在该示例中，用户 104 在屏幕 107 上显示包含与用户 104 希望呼叫的用户 108 关联的“点击呼叫”链接的 Web 页面。

[0038] 在替代的示例中，在仍然允许通过互联网网络 103 的通信的同时，用户 104 具有正运行专用“点击呼叫”应用(或程序)的终端 105 (即包括除了 Web 页面之外的用户接口)。

[0039] 在本说明中，将在无论如何也不将用户 104 限制为“主叫用户”并且将用户 108 限制为“被叫用户”的情况下作出引用，应理解，通信可以在互换的角色的情况下发生，或可以包括彼此相互通信的在主叫侧和被叫侧这两侧上的大量用户。若是并未依照以下将提供的教导在两个用户之间建立通信，则术语“被叫用户”和“主叫用户”将必须理解为潜在的资质(例如“要被呼叫的他 / 她”和“想进行呼叫的他 / 她”)。

[0040] 主叫用户 104 可以因此作用于屏幕 107 上所显示的 Web 链接，以向服务器 101 转发请求以发起与被叫用户 107 的“点击呼叫”通信。

[0041] 该“点击呼叫”通信优选地是实时语音或视频电话通信，并且因此主叫用户 104 将使用耳机和麦克风或免提系统。在本说明中，将简单地通过将实时通信指明为“呼叫”来对其作出引用，应理解，通信也可以以其它已知的形式发生，诸如：视频电话呼叫、即时传信、文件共享、数据共享等。

[0042] 一旦服务器 101 接收到来自用户 104 的“点击呼叫”请求，根据本发明的通信管理方法就开始，如以下将详细描述的那样。

[0043] 一般地，服务器 101 包括处理器和操作存储器，并且适用于提示主叫用户 104 提供他 / 她的“身份元素”。通过以下将详细描述的方式，服务器 101 适用于验证用户 104 的身份元素。

[0044] 然后，服务器 101 将关于身份元素的信息转发到被叫用户 108。被叫用户 108 还配备有扬声器和麦克风，并且进而使用通过连接 110 (例如 ADSL 连接)而连接到互联网 103 的计算机终端 109。

[0045] 服务器 101 还适用于与终端 109 交换数据。为此，在实施例的一个示例中，被叫用户 108 的终端 109 优选地包括 un web 浏览器中的 Java® applet 的形式的软件，其执行 web

电话的功能。

[0046] 所述软件接口至音量可由用户调整的音频装置(例如麦克风和扬声器),对 IP 分组中的语音进行编码和解码,处理信令,并且将身份元素示出给被叫用户。作为替换,可以借助针对由主叫用户使用以打开 web 链接的浏览器点对点地创建的“插件”或者借助也可以实现 VoIP 功能的普通“插件”(诸如例如 Adobe Flash),来在浏览器内直接实现 VoIP 部件。

[0047] 相似地,在实施例的一个示例中,主叫用户 104 的终端 105 优选地包括如上面描述的 web 浏览器的软件,其执行 web 电话的功能。所述软件接口至音量可由用户调整的音频装置(例如麦克风和扬声器),对 IP 分组中的语音进行编码和解码,并且处理信令。

[0048] 服务器 101 然后将信号(优选地,视觉和 / 或听觉信号,其表示这样的事实 :用户 104 希望建立经由“点击呼叫”的通信)传送到用户 108。屏幕 111 然后显示包括关于主叫用户 104 的身份元素的、由服务器 101 验证的信息的消息。这样的信息也可以由在被叫用户的装置上运行的软件应用来处理,从而例如通过使用“黑名单”(即包含不受欢迎的用户的标识符的列表)来便利将导致应答或不应答呼叫的决定处理。

[0049] 在接收到该信号时,被叫用户 108 可以决定接受该呼叫 ;在这样的情况下,服务器 101 将在终端 105 与终端 109 之间发起通信,因此允许被叫用户 108 和主叫用户 104 如后者所请求的那样而彼此通信。

[0050] 替换地,在接收到该信号时,被叫用户 108 可以决定拒绝该呼叫。在这种情况下,服务器 101 将向主叫用户 104 通知不可能建立通信,或其将简单地中断与主叫用户 104 的连接。

[0051] 应注意,用户 108 是客户而用户 104 是外部用户的“点击呼叫”服务提供商所处理的服务器 101 的角色仅给出在各用户之间建立通信的可能性以及向被叫用户通知存在未决呼叫请求的可能性。

[0052] 因此而构建的服务器 101(即服务提供商)的角色允许创建“越顶(over-the-top)”服务,即其中在物理通信手段(互联网)与用户的身份之间存在分离的服务。服务提供商因此确保在所提供的合理可能性内与主叫用户的身份元素有关的一条信息被传递到被叫用户。以此方式,是否接受呼叫仍然取决于被叫用户,从而以极度的灵活性来表征服务。

[0053] 当没有用户之间事先已知的关系(无论是契约关系、个人关系还是利益关系)时,本发明的方法尤其有效。

[0054] 图 2 示出由服务器 101 和可选地连接至服务器 101 的设备(例如终端 105 和 109)所实现的用于管理用户 104 与 108 之间的通信的方法的实施例。

[0055] 在步骤 201,例如,如参照图 1 所描述的那样,接收来自主叫用户 104 的用以发起与被叫用户 108 的通信的请求。

[0056] 回复在步骤 201 接收到的“点击呼叫”请求,在步骤 202,要求主叫用户 104 提供他 / 她自己的身份元素。在主叫用户 104 已经提供了他 / 她自己的身份元素之后,在步骤 203,验证由主叫用户 104 提供的身份元素。根据参照图 3、图 4 和图 5 的其它实施例的更详细的描述,步骤 202 和 203 的实现细节将变得更清楚。

[0057] 最后,例如,如参照图 1 所描述的那样,在步骤 204,已验证的身份元素被发送到被叫用户 108,从而被叫用户 108 接收关于主叫方 104 的身份的精确信息,并且可以决定是否接受呼叫并且建立通信。

[0058] 图 3 图解通信管理方法的更详细的实施例。

[0059] 在步骤 301，例如，如参照图 1 所描述的那样，接收来自主叫用户 104 的用以发起与被叫用户 108 的“点击呼叫”通信的请求。在步骤 302，例如通过将主叫用户 104 的电子邮件地址输入到屏幕 107 上所显示的 Web 页面上所示的表单中来要求主叫用户 104 提供他 / 她自己的电子邮件地址。用户 104 的电子邮件地址将被用作与该用户关联的“身份元素”。在步骤 303，例如由服务器 101 将电子邮件消息传送到主叫用户 104 所指定的电子邮件地址，该消息包含验证元素（诸如例如用户 104 可以点击的非公开验证链接）。

[0060] 在步骤 304，接收指示已经正确地点击验证链接的确认。在此情况下，可以确实假设用户 104 实际上在他 / 她的部署（disposal）处具有在步骤 302 所指定的电子邮件地址。

[0061] 在步骤 305，关于用户 104 的已验证的电子邮件地址的信息被发送到被叫用户 108。

[0062] 优选地，该发送是与用以发起与其已验证的身份元素被示出的用户 104 的呼叫的请求同时发生的。例如，如参照图 1 所描述的那样，因此可以建立各用户之间的通信。在优选实施例中，连同将已验证的身份元素发送到被叫用户 108 一起，用户 104 一点击验证链接，就传送用以发起“点击呼叫”通信的请求。

[0063] 图 4 图解通信管理方法的另一更详细的实施例。

[0064] 在步骤 401，例如，如参照图 1 所描述的那样，接收来自主叫用户 104 的用以发起与被叫用户 108 的“点击呼叫”通信的请求。在步骤 402，例如通过将主叫用户 104 的蜂窝电话号码输入到屏幕 107 上所显示的 Web 页面上所示的表单中来要求主叫用户 104 提供他 / 她自己的蜂窝电话号码。用户 104 的蜂窝电话号码将被用作与该用户关联的“身份元素”。

[0065] 在步骤 403，消息（例如由服务器 101 经由合适的蜂窝连接传送的 SMS 消息）被传送到主叫用户 104 所指定的蜂窝电话号码，该消息包含用户 104 可访问的验证元素（诸如例如非公开字母数字代码）。

[0066] 在步骤 404，例如通过将验证代码输入到屏幕 107 上所显示的 Web 页面上所示出的合适表单中来要求主叫用户 103 提供验证元素。

[0067] 在步骤 405，确证主叫用户 104 是否已经正确地提供所请求的验证元素。如果例如主叫用户 104 已经输入正确代码，则可以确实假设用户 104 实际上在他 / 她的部署处具有在步骤 402 所指定的蜂窝电话号码。

[0068] 然后，在步骤 406，关于用户 104 的已验证蜂窝电话号码的信息被发送到被叫用户 108。优选地，该发送是与用以发起与其已验证的身份元素被示出的用户 104 的呼叫的请求同时发生的。例如，如参照图 1 所描述的那样，因此可以建立各用户之间的通信。

[0069] 替换地，可以预想这样的实施例 :其中，主叫用户 104 提供不能接收所写入的消息的固定网络号码。在这样的情况下，可以通过电话联系到主叫用户 104，并且例如可以借助语音合成系统向他 / 她给出密码以被用作如先前描述的验证元素。

[0070] 在此无论如何没有任何限制地参照图 3 和图 4 描述的实施例可以与允许将验证元素传送到主叫用户的任何技术（例如，电话、视频电话、传真、电子邮件、社交网络等）组合，并且可能地还接收验证确认。

[0071] 图 5 图解通信管理方法的另一更详细的实施例。

[0072] 在步骤 501，例如，如参照图 1 所描述的那样，接收来自主叫用户 104 的用以发起与

被叫用户 108 的“点击呼叫”通信的请求。在步骤 502，例如通过将智能卡插入连接到终端 105 的合适的智能卡读卡器来请求主叫用户 104 提供所证实的电子标识符。由于其本身性质的原因，遵从生效的隐私法规，由所证实的电子标识符提供的一条信息将被用作与主叫用户 102 关联的“身份元素”。

[0073] 在很多国家，官方身份文档的使用正快速增长，这与允许对很多种类的服务进行访问的智能卡型的电子标识符关联。因此，能够使用同一标识符以便获得对“点击呼叫”服务的访问看起来是有利的。

[0074] 在步骤 504，根据依靠电子标识符中所包含的信息的拓扑和编码的准则来接收并且验证主叫用户 104 的电子标识符。在此情况下，可以甚至更加确实地假设用户 104 实际上在他 / 她的部署处具有在步骤 502 所提供的身份元素。

[0075] 然后，在步骤 504，关于用户 104 的已验证的身份元素的信息被发送到被叫用户 108。优选地，该发送是与用以发起与其已验证的身份元素被示出的用户 104 的呼叫的请求同时发生的。例如，如参照图 1 所描述的那样，因此可以建立各用户之间的通信。

[0076] 图 6 图解当主叫用户 104 作出多次连续“点击呼叫”请求时尤其有利的通信管理方法的实施例。例如，当各用户之间存在个人认识关系(例如朋友)或常规客户关系(例如提供帮助服务)时，该情况尤为相关。

[0077] 在步骤 601，例如，如参照图 1 所描述的那样，接收来自主叫用户 104 的用以发起与被叫用户 108 的“点击呼叫”通信的请求。在步骤 602，搜索关于已经针对同一主叫用户 104 验证的身份元素的信息。例如，服务器 101 可以向终端 105 传送请求以确证将证明身份元素已被验证的互联网浏览器的“甜饼(cookies)”的存在。

[0078] 优选地，属于已经验证的身份元素的信息被存储在服务器 101 和主叫用户 104 的终端 105 这两者中。

[0079] 优选地，表示所述信息的 cookie 是特有的，并且不能由要欺骗验证系统的恶意用户预测或合成。优选地，cookies 中所包含的信息并非与主叫用户的身份在算法上相关。

[0080] 在优选实施例中，甚至必须自动对主叫用户 104 的终端 105 中所存储的信息与服务器 101 中所存储的相对应的信息进行比较。为此目的，服务器 101 包括对主叫方的身份与分配至主叫方的身份的 cookies 进行匹配的表。同样，服务器 101 包括用于生成 cookies 并且将它们与主叫方的身份关联的单元。

[0081] 如果关于已验证的身份元素所存储的信息并不可用，则将执行步骤 603，其中，要求主叫用户 104 提供身份元素。

[0082] 在步骤 604，例如，如先前描述的那样，验证由主叫用户 104 提供的身份元素。

[0083] 在步骤 605，与当前已验证的身份元素有关的一条信息被存储（例如通过将其保存到终端 105 上）。这可以通过在主叫用户 104 所使用的 Web 浏览器上设定“cookie”(即通过在专用“点击呼叫”应用中存储私有信息)来容易地达到。

[0084] 然后，在步骤 606，关于用户 104 的已验证的身份元素的信息被发送到被叫用户 108。优选地，该发送是与用以发起与其已验证的身份元素被示出的用户 104 的呼叫的请求同时发生的。例如，如参照图 1 所描述的那样，因此可以建立各用户之间的通信。

[0085] 反之，如果已经在步骤 602 取得关于针对主叫用户 104 的先前验证的身份元素的所存储的信息，则处理将直接进入上面描述的步骤 606，而无需重复验证过程，因为后者已

经被执行。

[0086] 例如，通过提供为关于先前已验证的身份元素的所存储的信息具有有效性期限(例如一个月)，在此参照图 6 所描述的实施例可以使用用于存储与用户关联的访问凭证的已知技术。“公共终端”访问模式也是可预期的，其中，不存储关于已验证的身份元素的信息，因此有条件地返回到参照图 2 的说明。此外，存储与先前已验证的身份元素有关的信息的动作可以赋予对身份元素的验证而不将这限制于被叫用户 108，因此还在主叫用户 104 可能想呼叫的所有其它用户前面标识主叫用户 104。

[0087] 图 7 图解包括例如在已经参照图 2 描述的步骤 201、202、203 和 204 之后的最终步骤 701 的通信管理方法的实施例。

[0088] 在步骤 701，用户 108 被传送表示用户 104 希望建立“点击呼叫”通信的事实的信号。该信令例如通过听觉告警(例如传统的“振铃”)或另外通过听觉 / 视觉信号而发生。

[0089] 优选地，该信令是与已经描述的步骤 204 同时的，或可以甚至超前于步骤 204。

[0090] 在接收到该信号时，被叫用户 108 可以决定接受呼叫，在此情况下，被叫用户 108 与主叫用户 104 之间的通信将如后者所请求的那样并且如已经例如参照图 1 所描述的那样被建立。

[0091] 作为替换，例如，如已经参照图 1 所描述的那样，在接收到该信号时，被叫用户可以拒绝呼叫。

[0092] 通过当然包括借助计算机网络相互连接的一台或更多台计算机的管理系统来实现根据本发明的用于管理各用户之间的通信的方法。在图 1 的示例中，管理系统包括服务器 101，其可选地连接到多个终端(例如终端 105 和 109)。

[0093] 服务器 101 以及终端 105 和 109 在与其关联的操作存储器中包括适用于实现本发明的方法的程序或代码部分。

[0094] 只要终端 105 和 109 中的至少一个(优选地，被叫终端)在与其关联的操作存储器中包括适用于实现本发明的方法的程序或代码部分，就也可以仅通过它们之间的交互来实现本发明的方法。

[0095] 可以在驻留在计算机中的存储器(即“自固定”存储器，诸如可拆卸硬盘、闪速存储器或光盘)中或甚至驻留在用户可以从其下载程序的互联网服务器中的存储器中，包含可在一台或更多台计算机上执行并且适用于通过到计算机网络的连接来实现本发明的通信管理方法的程序或代码部分。

[0096] 一般地，在不管怎样都不脱离如在所附权利要求中阐述的那样的本发明的保护范围的情况下，可预期结合本发明的教导来使用其它用户验证技术。

[0097] 例如，可以仅在“点击呼叫”服务的“免费”使用的预定时间之后请求主叫用户的身份元素的验证；如果主叫用户是例如谨慎地保持链接以便被呼叫而不使其公开的私人用户，则这可能是有利的。

[0098] 在另一实施例中，被叫用户可以通过事先表达偏好来决定是否使用用于验证主叫用户的身份元素的方法，该偏好将保持有效，直到被叫用户决定改变它。例如，某些用户可能要被任何人呼叫而没有任何过滤器；因此还将该选项提供给被叫用户是有利的。

[0099] 此外，可能仅在预定数量的“点击呼叫”请求之后要求主叫用户的身份元素的验证；若主叫用户是对各种呼叫接收方作出许多不想要的呼叫的诈骗用户，则这可能是有利

的。

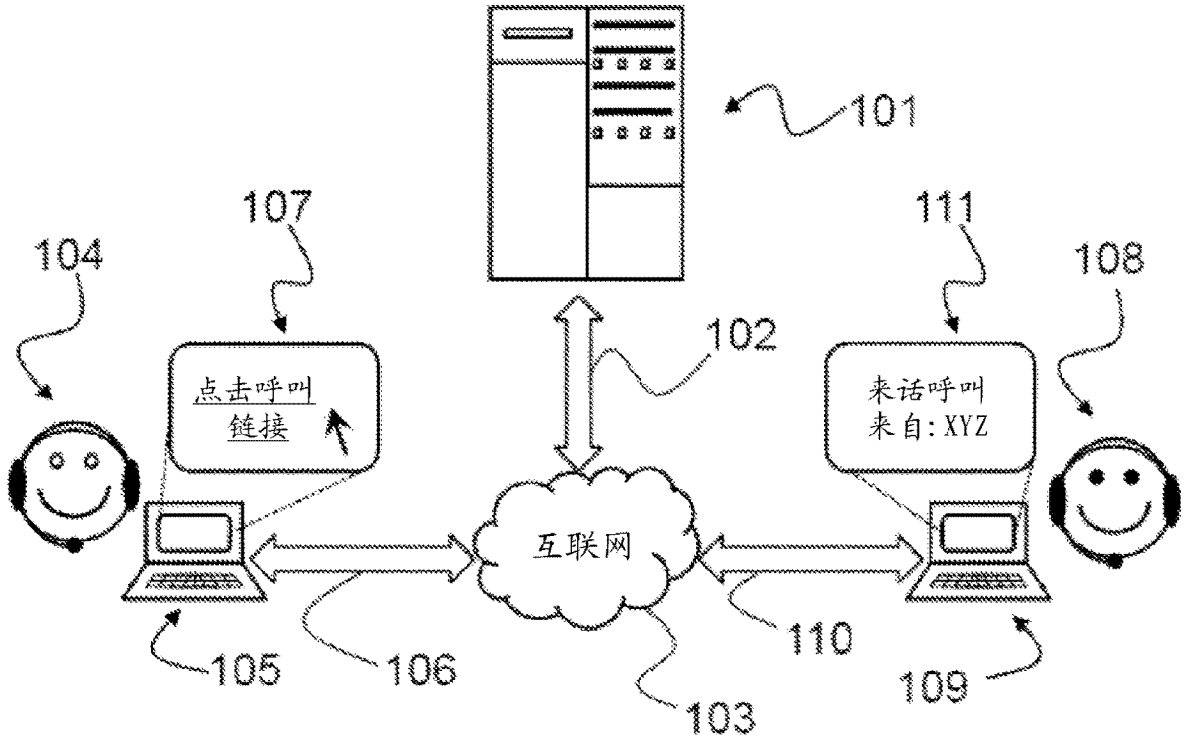

101
107
111
104
108
102
点击呼叫
链接
来话呼叫
来自:XYZ
互联网
105
106
110
109
103

图 1

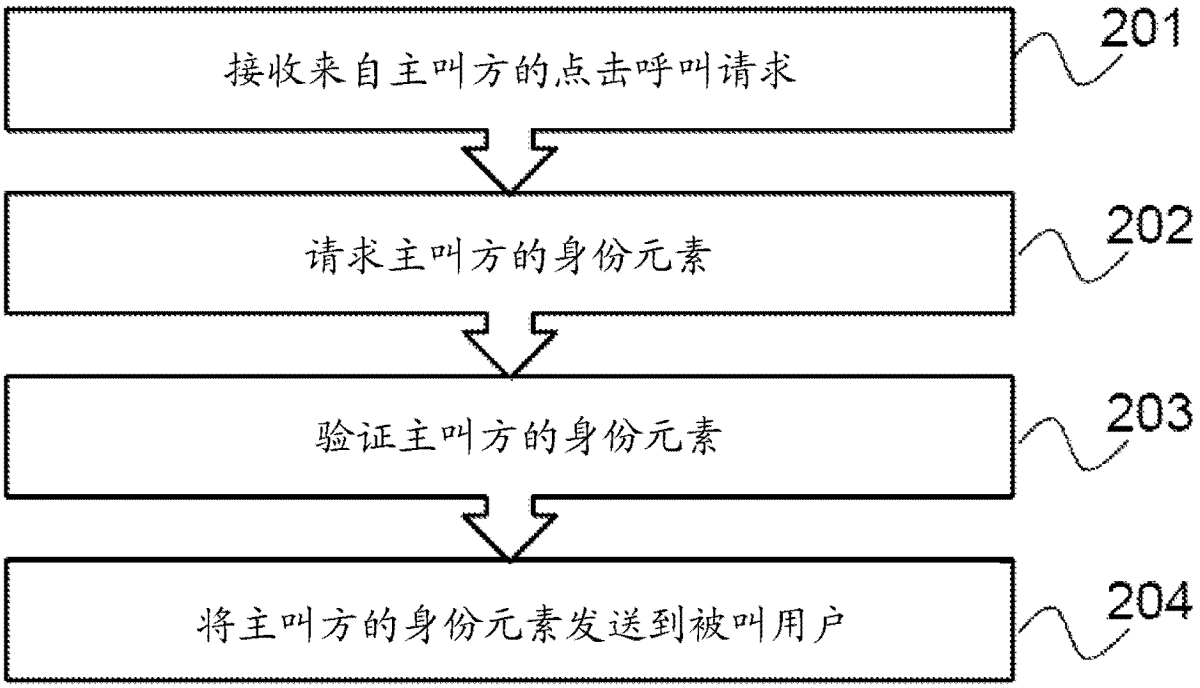

接收来自主叫方的点击呼叫请求
201
请求主叫方的身份元素
202
验证主叫方的身份元素
203
将主叫方的身份元素发送到被叫用户
204

图 2

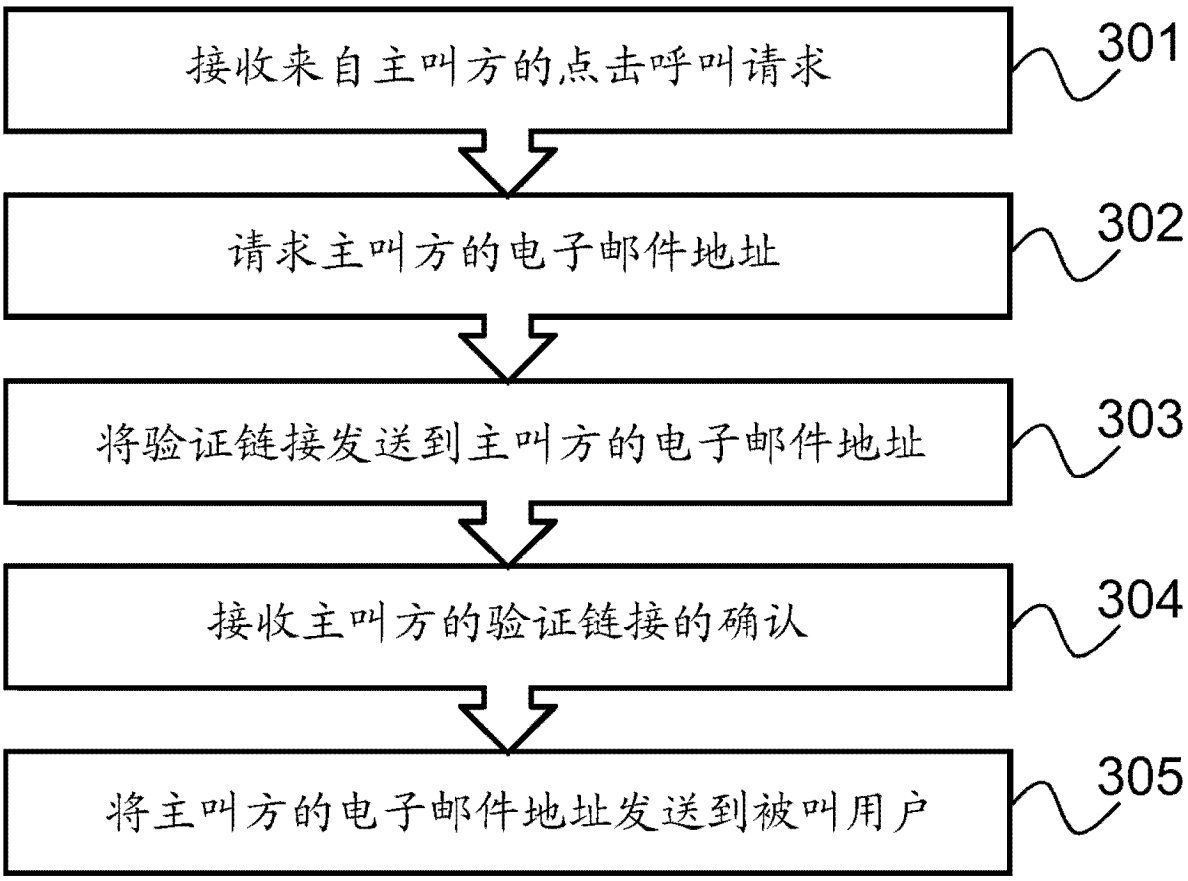

接收来自主叫方的点击呼叫请求
301
请求主叫方的电子邮件地址
302
将验证链接发送到主叫方的电子邮件地址
303
接收主叫方的验证链接的确认
304
将主叫方的电子邮件地址发送到被叫用户
305

图 3

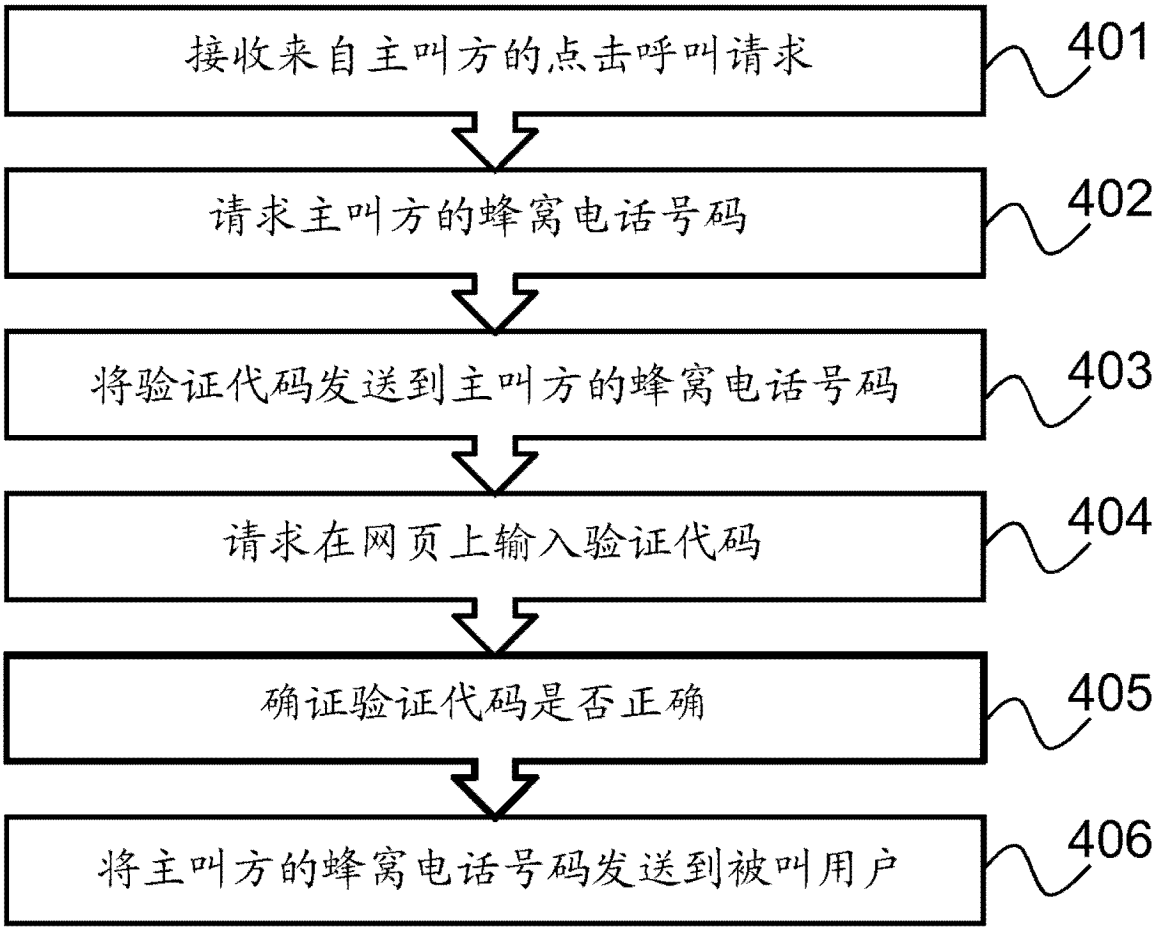

接收来自主叫方的点击呼叫请求
401
请求主叫方的蜂窝电话号码
402
将验证代码发送到主叫方的蜂窝电话号码
403
请求在网页上输入验证代码
404
确证验证代码是否正确
405
将主叫方的蜂窝电话号码发送到被叫用户
406

图 4

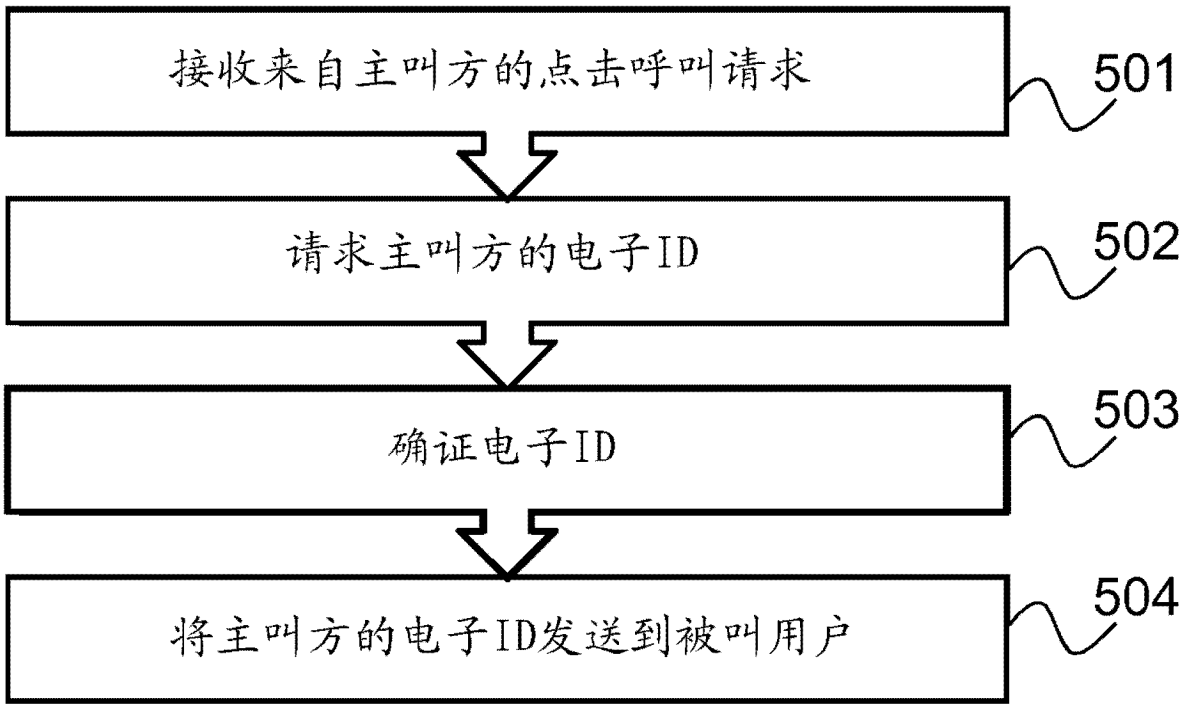

接收来自主叫方的点击呼叫请求
501
请求主叫方的电子ID
502
确证电子ID
503
将主叫方的电子ID发送到被叫用户
504

图 5

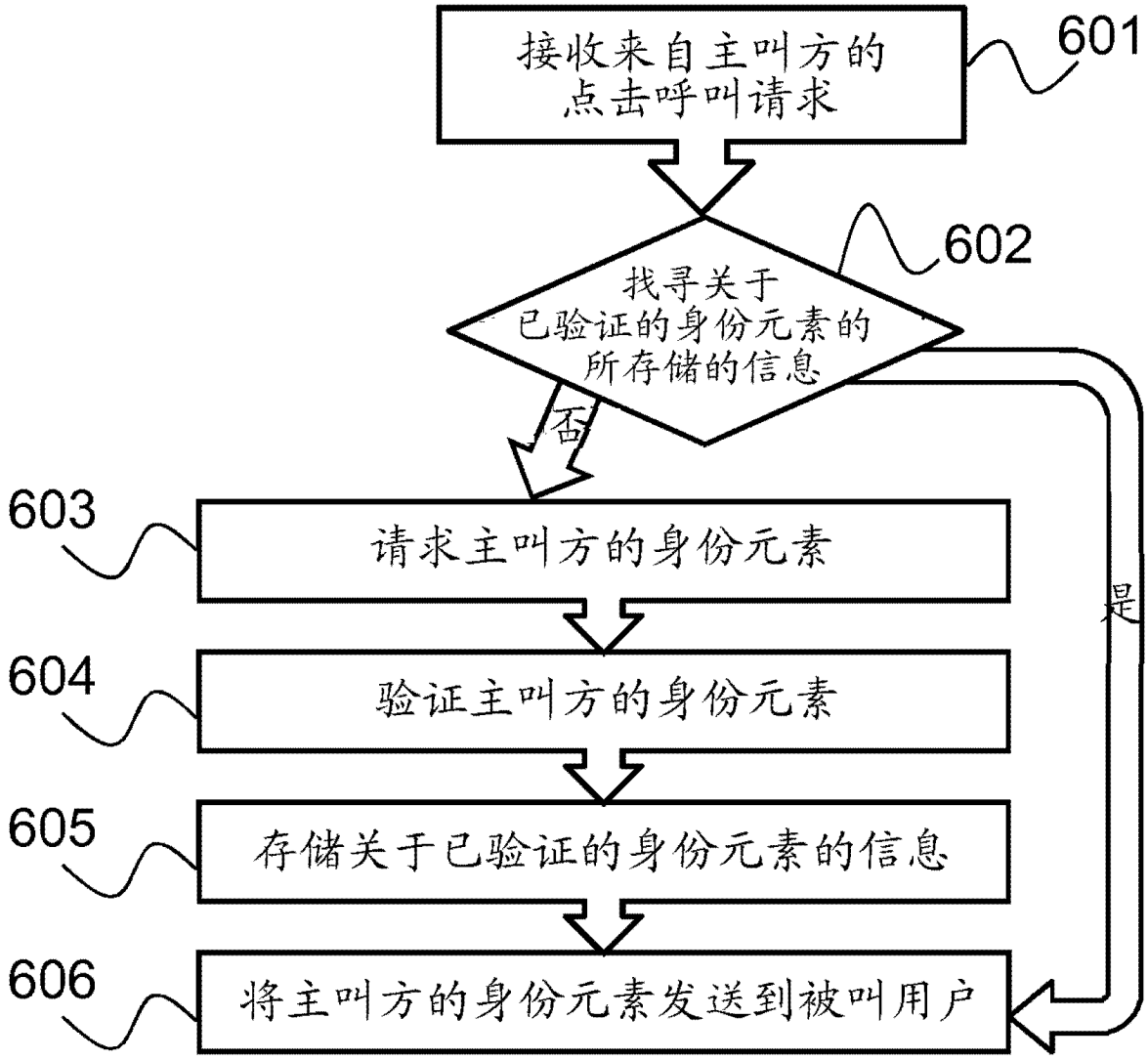

接收来自主叫方的
点击呼叫请求
601
找寻关于
已验证的身份元素的
所存储的信息
602
否
是
603
请求主叫方的身份元素
604
验证主叫方的身份元素
605
存储关于已验证的身份元素的信息
606
将主叫方的身份元素发送到被叫用户

图 6

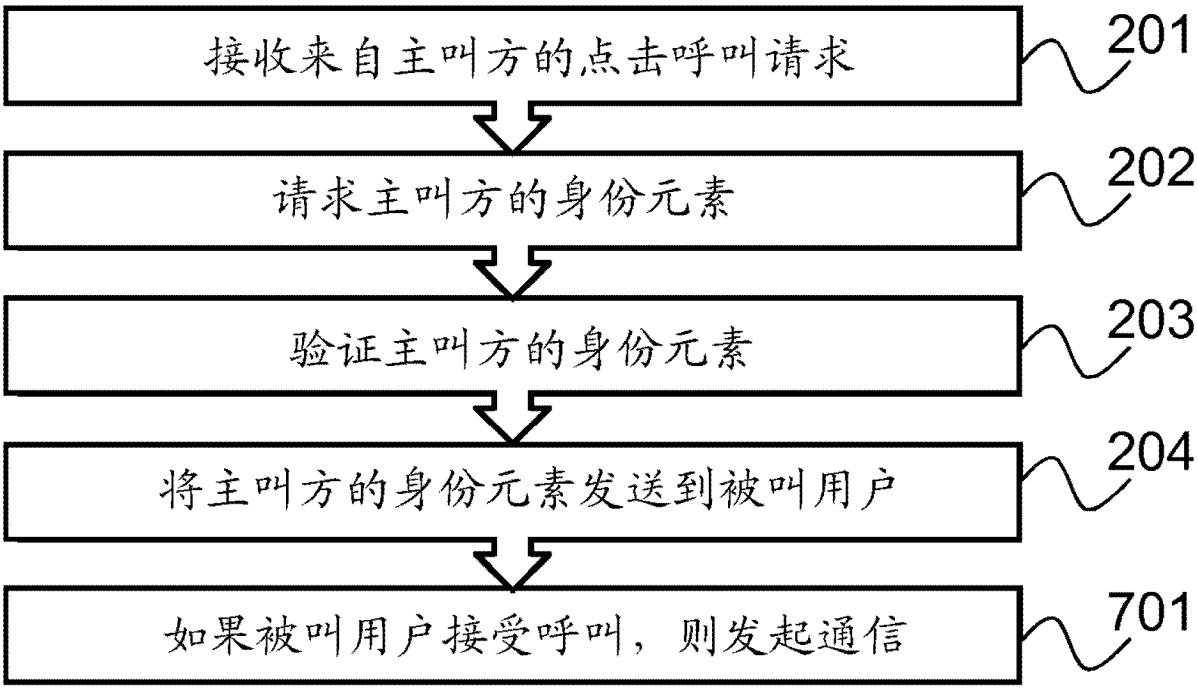

接收来自主叫方的点击呼叫请求
201
请求主叫方的身份元素
202
验证主叫方的身份元素
203
将主叫方的身份元素发送到被叫用户
204
如果被叫用户接受呼叫，则发起通信
701

图 7