



(12) 发明专利

(10) 授权公告号 CN 102428475 B

(45) 授权公告日 2015. 06. 24

(21) 申请号 201080021197. 7

(51) Int. Cl.

(22) 申请日 2010. 04. 29

G06F 21/60(2013. 01)

(30) 优先权数据

12/468, 738 2009. 05. 19 US

(56) 对比文件

US 2007/0073728 A1, 2007. 03. 29, 说明书第 0003-0275 段.

(85) PCT国际申请进入国家阶段日

2011. 11. 15

CN 101063968 A, 2007. 10. 31, 全文.

(86) PCT国际申请的申请数据

PCT/EP2010/055854 2010. 04. 29

审查员 苗伟

(87) PCT国际申请的公布数据

W02010/133440 EN 2010. 11. 25

(73) 专利权人 国际商业机器公司

地址 美国纽约阿芒克

(72) 发明人 T. W. 格兰迪森 刘鹏

E. M. 麦克西米利恩 E. 特齐

(74) 专利代理机构 北京市柳沈律师事务所

11105

代理人 黄小临

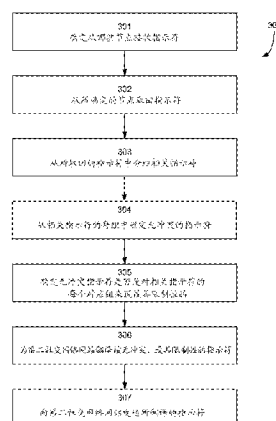
权利要求书2页 说明书16页 附图4页

(54) 发明名称

管理安全性和 / 或隐私设置的系统和方法

(57) 摘要

描述了用于管理安全性和 / 或隐私设置的系统和方法。在一个实施例中, 该方法可以包括将第一客户端可通信地耦接到第二客户端。该方法还可以包括将第一客户端的多个安全性和 / 或隐私设置的一部分从第一客户端传播到第二客户端。该方法还可以包括在第二客户端处接收第一客户端的多个安全性和 / 或隐私设置的该部分后, 将所接收的第一客户端的多个安全性和 / 或隐私设置的部分并入到第二客户端的多个安全性和 / 或隐私设置中。



1. 一种管理安全性和 / 或隐私设置的方法, 该方法包括:

将第一社交网络上的简档可通信地耦接到第二社交网络上的简档;

将所述第一社交网络上的简档的多个安全性和 / 或隐私设置的一部分从所述第一社交网络上的简档传播到所述第二社交网络上的简档; 以及

在所述第二社交网络上的简档处接收所述第一社交网络上的简档的多个安全性和 / 或隐私设置的该部分后, 将所接收的所述第一社交网络上的简档的多个安全性和 / 或隐私设置的部分并入到所述第二社交网络上的简档的多个安全性和 / 或隐私设置中。

2. 根据权利要求 1 的方法, 其中, 所述第一社交网络和所述第二社交网络在相同的社交网络网站上。

3. 根据权利要求 1 的方法, 其中: 所述第一社交网络和所述第二社交网络在不同的社交网络网站上。

4. 根据权利要求 1 的方法, 还包括:

将所述第一社交网络上的简档的多个安全性和 / 或隐私设置与所述第二社交网络上的简档的多个安全性和 / 或隐私设置相比较; 以及

从所述比较中确定要传播到所述第二社交网络上的简档的多个安全性和 / 或隐私设置的部分。

5. 根据权利要求 1 的方法, 还包括:

将第二社交网络的多个用户简档可通信地耦接到所述第二社交网络上的简档;

将所述第二社交网络上的简档的多个安全性和 / 或隐私设置与该多个用户简档的每个的多个安全性和 / 或隐私设置相比较;

从所述比较中确定要将该多个用户简档的哪些安全性和 / 或隐私设置并入到所述第二社交网络上的简档的多个安全性和 / 或隐私设置中;

将要并入的安全性和 / 或隐私设置传播到所述第二社交网络上的简档; 以及

在所述第二社交网络上的简档处接收到要并入的安全性和 / 或隐私设置后, 将所接收的安全性和 / 或隐私设置并入到所述第二社交网络上的简档的多个安全性和 / 或隐私设置中。

6. 根据权利要求 5 的方法, 其中, 该多个用户简档和所述第二社交网络上的简档是形成所述第二社交网络上的简档的社交图的在社交网络上的多个简档。

7. 根据权利要求 6 的方法, 其中比较多个安全性和 / 或隐私设置包括计算所述第一社交网络上的简档的隐私风险分数。

8. 一种管理安全性和 / 或隐私设置的系统, 包括:

耦接模块, 被配置为将第一社交网络上的简档可通信地耦接到第二社交网络上的简档;

传播模块, 被配置为将所述第一社交网络上的简档的多个安全性和 / 或隐私设置的一部分从所述第一社交网络上的简档传播到所述第二社交网络上的简档; 以及

集成模块, 被配置为在所述第二社交网络上的简档处接收到来自所述第一社交网络上的简档的安全性和 / 或隐私设置的该部分时, 将所接收的所述第一社交网络上的简档的多个安全性和 / 或隐私设置的部分并入到所述第二社交网络上的简档的多个安全性和 / 或隐私设置中。

9. 根据权利要求 8 的系统, 其中, 所述第一社交网络和所述第二社交网络在相同的社交网络网站上。

10. 根据权利要求 8 的系统, 其中: 所述第一社交网络和所述第二社交网络在不同的社交网络网站上。

11. 根据权利要求 8 的系统, 还包括比较模块, 其被配置为:

将所述第一社交网络上的简档的多个安全性和 / 或隐私设置与所述第二社交网络上的简档的多个安全性和 / 或隐私设置相比较; 以及

从所述比较中确定所述第一社交网络上的简档的、要传播到所述第二社交网络上的简档的多个安全性和 / 或隐私设置的部分。

12. 根据权利要求 8 的系统, 其中:

该耦接模块进一步被配置为将第二社交网络的多个用户简档可通信地耦接到所述第二社交网络上的简档;

该系统进一步包括: 比较模块, 被配置为:

将所述第二社交网络上的简档的多个安全性和 / 或隐私设置与该多个用户简档的每个的多个安全性和 / 或隐私设置相比较; 以及

从所述比较中确定要将该多个用户简档的哪些安全性和 / 或隐私设置并入到所述第二社交网络上的简档的多个安全性和 / 或隐私设置中;

该传播模块进一步被配置为将要并入到所述第二社交网络上的简档的多个安全性和 / 或隐私设置中的安全性和 / 或隐私设置传播到所述第二社交网络上的简档; 以及

该集成模块进一步被配置为在所述第二社交网络上的简档处接收到要并入的安全性和 / 或隐私设置后, 将所接收的安全性和 / 或隐私设置并入到所述第二社交网络上的简档的多个安全性和 / 或隐私设置中。

13. 根据权利要求 12 的系统, 其中, 该多个用户简档和所述第二社交网络上的简档是形成所述第二社交网络上的简档的社交图的在社交网络上的多个简档。

14. 根据权利要求 13 的系统, 其中, 在比较多个安全性和 / 或隐私设置期间为所述第一社交网络上的简档计算隐私风险分数。

管理安全性和 / 或隐私设置的系统和方法

技术领域

[0001] 本公开的实施例通常涉及数据处理系统的领域。例如,本公开的实施例涉及用于管理安全性和 / 或隐私设置的系统和方法。

背景技术

[0002] 在一些计算应用中,比如网页应用和服务,大量的个人数据暴露给其他人。例如,关于社交网络网站,该网站从用户请求个人信息,包括姓名、职业、电话号码、地址、生日、好友、同事、雇主、就读高中等。因此,用户在配置他 / 她的隐私和安全性设置时被给予了一些决定权以便确定个人信息可以与其他人共享多少和何种程度。

[0003] 在确定适当的隐私和安全性设置时,可以给予用户各种选择。例如,一些网站在试图确定适当设置时向用户询问多页问题。回答这些问题可能对用户变成乏味且费时的任务。因此,用户可能放弃 (forego) 配置他 / 她的优选安全性和隐私设置。

发明内容

[0004] 描述了用于管理安全性和 / 或隐私设置的系统和方法。在一个实施例中,该方法包括将第一客户端可通信地耦接到第二客户端。该方法还包括将第一客户端的多个安全性和 / 或隐私设置的一部分从第一客户端传播到第二客户端。该方法还包括在第二客户端处接收第一客户端的多个安全性和 / 或隐私设置的该部分后,将所接收的第一客户端的多个安全性和 / 或隐私设置的部分并入到第二客户端的多个安全性和 / 或隐私设置中。

[0005] 提及这些例示实施例不限制或限定本发明,而是提供例子帮助其理解。在具体实施例中讨论了例示的实施例,且在那里提供本公开的进一步描述。通过查阅本说明书可以进一步理解由本公开的各种实施例提供的优点。

附图说明

[0006] 当参考附图来阅读以下具体实施方式时,更好地理解本发明的这些和其他特征、方面和优点,附图中:

[0007] 图 1 图示用户的社交网络的示例社交图。

[0008] 图 2 是在第一社交网络网站上具有用户简档和在第二社交网络网站上具有用户简档的人的社交网络图。

[0009] 图 3 是用于通过控制台在社交网络之间传播隐私设置的示例方法的流程图。

[0010] 图 4 图示用于实现隐私设置和 / 或隐私环境的计算的示例计算机架构。

具体实施方式

[0011] 本公开的实施例通常涉及数据处理系统的领域。例如,本公开的实施例涉及用于管理安全性和 / 或隐私设置的系统和方法。在本说明书通篇,为了说明的目的,阐述多个具体细节以便提供本发明的彻底理解。但是,对本领域技术人员将显而易见的是,可以没有这

些具体细节中的一些而实践本发明。在其他例子中，以方框图形式示出公知的结构和设备，以避免混淆本公开的基本原理。

[0012] 在管理隐私和 / 或安全性设置时，系统使用其他的隐私和 / 或安全性以便配置用户的隐私和 / 或安全性设置。因此，传播并比较来自其他用户的设置以便自动创建用户的设置的优选配置。可以在客户端之间的各种氛围下发生隐私和 / 或安全性设置的自动创建。例如，可以在使用安全性软件的计算机系统、各种计算机的因特网浏览器、一个计算机上的多个因特网浏览器、社交网络网站中的用户简档、多个社交网络网站之间的用户简档、和一个或多个因特网购物网站之间的购物者简档之间发生创建。

[0013] 为了说明的目的，参考在一个或多个社交网络网站之间的用户简档来描述实施例。以下描述不应为限制性的，因为对于本领域技术人员而言在不同氛围下的实施方式、包括以上列出的是显而易见的。

[0014] 社交网络

[0015] 社交应用 / 网络允许人们创建与其他人的连接。用户创建简档，然后经由他 / 她的简档连接到其他用户。例如，第一用户可以向他 / 她认识的第二用户发送好友请求。如果该请求被接受，则第二用户成为第一用户的标识的好友。一个用户的简档的连接的全体创建该用户的人际关系图。

[0016] 社交网络平台可以被用户用作平台操作环境，允许在好友之间的几乎即时的通信。例如，该平台可以允许好友共享程序、传递即时消息、或查看其他好友的简档的具体部分，同时允许用户进行诸如玩游戏（离线或在线）、编辑文档或发送电子邮件的标准任务。该平台还可以允许来自其他源、包括例如新闻馈送（news feeds）、便捷购物（easy access shopping）、银行业务等的信息。由于多个源提供信息，因此为用户创建 mashup（糅合）。

[0017] mashup 被定义为将来自多于一个源的数据组合到整合工具中的网页应用。许多 mashup 可以被整合到社交网络平台上。mashup 还需要一些量的用户信息。因此，通过用户的隐私和 / 或安全性设置来确定 mashup 是否可访问用户简档中存储的用户信息。

[0018] 隐私和 / 或安全性设置

[0019] 在一个实施例中，可以在如下六个宽泛类别中定义要通过隐私和 / 或安全性设置保护的社交网络的部分：用户简档、用户搜索、馈送（feed）（例如新闻）、消息和好友请求、应用和外部网站。对用户简档的隐私设置控制可由谁访问简档信息的哪个子集。例如，好友具有对用户简档的完全访问，但陌生人则具有对用户简档的受限访问。对搜索的隐私设置控制谁可以找到用户的简档以及简档的多少在搜索期间可用。

[0020] 对馈送的隐私设置控制哪些信息可以在馈送中发送给用户。例如，该设置可以控制什么类型的新闻故事可以经由新闻馈送发送给用户。对消息和好友请求的隐私设置控制当正向用户发送消息或好友请求时可见用户简档的哪部分。对应用类别的隐私设置控制对连接到用户简档的应用的设置。例如，该设置可以确定是否允许应用通过社交网络网站接收用户的活动信息。对外部网站类别的隐私设置控制可以由外部网站发送给用户的信息。例如，该设置可以控制航空公司的网站是否可以转发关于最后一刻航班协议（last minute flight deal）的信息。

[0021] 因此，可以使用隐私和 / 或安全性设置来控制用户材料或访问的部分。例如，对于六个宽泛类别的隐私设置可以用于限制外部网站对用户的访问，并限制用户对程序或应用

的访问。

[0022] 用于传播隐私和 / 或安全性设置的实施例

[0023] 替代手动地设置隐私设置的所有分量以使用户完全控制且知道用户的隐私设置, 在当前隐私模型中存在两种类型的隐私保护: (1) 可以通过将个人隐藏在大量其他个人中来保护该个人的隐私, 以及 (2) 可以通过使得该个人隐藏在受信代理之后来保护该个人的隐私。对于第二概念, 受信代理以该个人的名义执行任务, 而不泄露关于该个人的信息。

[0024] 为了创建集体 (collective), 可能需要添加虚构的个体或删除真实的个人, 包括添加或删除关系。因此, 个人将隐藏在社交图的严格编辑后的版本中。这种方法的一个问题是阻碍或可能不保留网络的效用。例如, 将需要中央应用来记住对社交图进行的所有编辑, 以便在集体中隐藏个人。在使用受信代理时, 难以且可能成本高地找到可以信任或将仅进行已被请求的任务的代理。因此, 本发明的一个实施例通过使得设置用户隐私设置的任务自动化来消除对集体或受信代理的需求。

[0025] 图 1 图示了用户 101 的社交网络的示例社交图 100。社交图 100 图示了用户 101 的社交网络包括直接连接到用户 101 的人 1 102、人 2 103、人 3 104、人 4 105 和人 5 106 (分别是连接 107-111)。例如, 人们可能是已接受用户 101 作为联系人且用户 101 已接受其为联系人的同事、好友或商务联系人或其他。关系 112 和 113 示出了人 4 105 和人 5 106 是彼此的联系人, 且人 4 105 和人 3 104 是彼此的联系人。人 6 114 是人 3 104 的联系人 (关系 115), 但人 6 114 不是用户 101 的联系人。通过将每个用户的社交图绘出并将他们链接到一起, 可以创建完整的社交网络的图。

[0026] 在社交图 100 中的每个人 / 用户被看作节点。在一个实施例中, 每个节点具有其自己的隐私设置。各个节点的隐私设置创建该节点的隐私环境。参考一个例子中的用户 101, 用户 101 隐私环境被定义为 $E_{user} = \{e_1, e_2, \dots, e_m\}$, 其中, e_i 是定义隐私环境 E 的指示符, 且 m 是定义隐私环境 E_{user} 的用户 101 的社交网络中的指示符的数量。在一个实施例中, 指示符 e 是 { 实体, 算符, 动作, 产物 } (entity, operator, action, artifact) 形式的元组 (tuple)。实体指社交网络中的对象。示例的对象包括但不限于人、网络、组、动作、应用和外部网站。算符指实体的能力或形态。示例的算符包括但不限于 can (可以)、cannot (不可以)、和 can in limited form (以有限形式可以)。算符的解释依赖于使用的背景和 / 或社交应用或网络。动作指在社交网络中的基本的 (atomic) 可执行任务。产物 (Artifact) 指基本可执行任务的目标对象或数据。指示符的部分的句法和语义可以依赖于正被建模的社交网络。例如, 指示符 $er = \{X, "can", Y, Z\}$, 这是 " 实体 X 可以对产物 Z 进行动作 Y "。指示符可以彼此依赖。但是为了例示目的, 将提供基本指示符作为例子。

[0027] 在一个实施例中, 隐私设置配置与实体、动作和产物相关的算符。因此, 可以使用隐私设置来确定对于指示符 $\{X, " ", Y, Z\}$, 不允许实体 X 在任何时间进行动作 Y 。因此, 隐私设置将设置指示符作为 $\{X, "cannot", Y, Z\}$ 。

[0028] 在一个实施例中, 当用户参与在他 / 她的当前经历以外的新活动时, 则用户可以有效利用 (leverage) 在他的网络中的与这种活动有关的人的隐私设置。例如, 如果用户 101 想要安装新应用, 则人 1-5 (107-111) ——如果他们已经安装了该新应用——的隐私设置可以用于设置用户 101 的关于该新应用的隐私设置。然后, 用户 101 将具有该应用是否可被信任的参考。

[0029] 在一个实施例中,如果用户想要安装应用且用户连接到在他的社交网络中的先前已经安装了该应用的仅另外一人,则来自该人的关于该应用的隐私设置将被复制到该用户。例如,在实体为人、“安装”为动作和产物为应用时,对该人的指示符可以是{人,“can”,安装,应用}。因此,用户将接收作为{用户,“can”,安装,应用}的该指示符作为他/她的隐私环境的部分。

[0030] 如果连接到该用户的两个或多个人包括相关指示符(例如,所有指示符包括在先前例子中的产物“应用”),则相关指示符全体可以用于确定该用户的指示符。在一个实施例中,为该用户创建的指示符包括两个属性。第一属性是,用户指示符不与相关指示符冲突。第二属性是,用户指示符与所有相关指示符相比是最有限制性的。

[0031] 参考在指示符之间的冲突,指示符共享相同的实体、动作和产物,但是指示符之间的算符彼此冲突(例如,“can”相对于“cannot”)。无冲突指的是当确定用户指示符时已经解决了所有冲突。在一个实施例中,解决冲突包括找到冲突中的最相关的、限制性的算符,丢弃所有其他算符。例如,如果三个相关指示符是{A,“can”,B,C},{A,“can in limited form”,B,C},以及{A,“can not”,B,C},则最具限制性的算符为“cannot”。因此,无冲突指示符将是{A,“cannot”,B,C}。如所示,无冲突指示符也是最具限制性的,因此满足这两个属性。

[0032] 在一个实施例中,用户的隐私环境关于用户的社交网络中的任何改变而改变。例如,如果一个人被添加到用户的社交网络,则该人的指示符可以用于更新用户的指示符。在另一实施例中,连接到用户的某些人可以比其他用户更受信任。例如,与其他人相比,已经连接到用户达更长时间段的、其简档较旧的和/或已经被标记为被其他用户信任的人的指示符可以被给予更大的权重。例如,用户101可以设置人1102作为在网络100中的最受信任的人。因此,可以依赖人1的指示符超过其他较不被信任的指示符,即使这些较不被信任的指示符的算符更有限制性。

[0033] 在一个实施例中,在两个单独的社交网络网站上具有用户简档的人可以使用来自一个网站的隐私设置来在另一网站上设置隐私设置。因此,指示符将从一个网站翻译到另一个。图2图示具有在第一社交网络网站202上的用户简档101和在第二社交网络网站204上的用户简档203的人201。大多数社交网络网站彼此并不交流。因此,在一个实施例中,用户控制台205将被用于隐私环境的社交网络间创建。

[0034] 图3是用于通过控制台205在社交网络之间传播隐私设置的示例方法300的流程图。在301开始,控制台205确定从哪个节点接收指示符。例如,如果图2中的用户203需要对于存在于社交网络202和204两者上的应用的隐私设置,则确定连接到用户节点101的哪些人具有用于该应用的指示符。在一个实施例中,从用户节点101指示符取出(pull)该指示符,其中,可能已使用其他人的指示符确定了该隐私设置。因此,为了创建隐私环境,控制台205可以确定从哪些节点接收所有指示符或那些节点,以便计算隐私环境。如果指示符不涉及社交网络网站204(例如,在网络网站202上访问的网站不能在网络网站204上访问),则控制台205可以在这些指示符被接收时忽略这些指示符。

[0035] 继续到302,控制台205从所确定的节点取回指示符。如先前所述的,可以从每个节点取回所有指示符。在另一实施例中,可以仅取回感兴趣的指示符。在另一实施例中,系统可以继续更新隐私设置,因此周期地取回更新的或新的指示符以便更新用户203的隐私

环境。

[0036] 继续到 303,控制台 205 将来自取回的指示符的相关指示符分组。例如,如果对每个所确定的节点取出所有指示符,则控制台 205 可以确定哪些指示符与相同或类似的实体、动作和产物相关。继续到 304,控制台 205 从每组相关指示符中确定无冲突的指示符。无冲突的指示符的集合将被用于用户节点 203 的隐私环境。

[0037] 继续到 305,控制台 205 对每个无冲突指示符确定该指示符是否是对其组的相关指示符来说最具限制性的。如果无冲突指示符不是最具限制性的,则控制台 205 可以改变该指示符来重新确定该指示符。或者,控制台 205 可以忽略该指示符,且不将其包括在确定用户节点 203 的隐私环境中。继续到 306,控制台 205 翻译用于第二社交网络网站的该无冲突、最具限制性的指示符。例如," can in limited form" 可以是不由两个不同社交网络网站不同地解释的算符。在另一例子中,在第一社交网络网站中的一个实体在第二社交网络网站上可以具有不同的名称。因此,控制台 205 试图将该指示符映射到与第二社交网络网站 204 相关的格式。在翻译指示符后,在 307 中,控制台 205 将这些指示符发送到第二社交网络网站 204 中的用户节点 203。然后为用户 203 设置指示符以创建用户 203 的社交网络的其隐私环境。

[0038] 对于一些社交网络网站,数页指向用户的问题设置隐私环境。一些社交网络网站具有过滤器组 and 用户控制来设置隐私环境。因此,在一个实施例中,可以取出对问题的答案、过滤器或用户设置。如此,从取出的信息创建指示符。另外,翻译指示符可以包括确定对用户问题的答案或设置过滤器和对第二社交网络网站的用户设置。因此,控制台 205 (或在社交网络网站上的客户端) 可以设置问题或用户控制以便创建用户节点的隐私设置。

[0039] 虽然在两个社交网络网站之间图示了上述方法,但是可以存在多个社交网络或者用户可以在相同的社交网络网站上。因此,用户节点可以具有依赖于社交网络的不同隐私设置。因此,该方法还可以用于在相同社交网络网站上的各社交网络之间传播隐私设置。

[0040] 在一个实施例中,隐私设置可以取决于事件而改变。例如,如果事件 A 发生,则指示符可能变得更少限制(算符从" cannot" 改变到" can in limited form")。因此,指示符可以包括用于考虑依赖性的信息的子集。例如,实体可以或可以不具有被社交网络网站信任的状态。因此,如果实体不被信任,则关于该实体的算符可以是限制性的(例如,{ 实体 A[不受信任], " cannot" ,B,C})。在变得被信任后,指示符可以被更新以考虑到这些(例如,{ 实体 A[受信任], " can" ,B,C})。例如,受信任的人可能能够搜索用户的全部简档,而不受信任的人不可以。

[0041] 用户的隐私环境还可以依赖于社交网络中的用户的活动。例如,与不是社交网络中的活跃用户的一些人相比,泄漏了更多信息的用户参与更有风险的活动。因此,用户可以是信息的子集,以便确定用户的隐私环境应该为何。在一个实施例中,隐私风险分数用于使用户的隐私设置更具限制性或更少限制性。以下描述了用于计算用户的隐私风险分数的实施例。

[0042] 计算用户隐私风险分数的示例实施例

[0043] 对于社交网络用户 j,可以将隐私风险分数计算为由其简档项目(item)的每一个对 j 引起的隐私风险的总和。总共隐私风险中的每个简档项目的贡献依赖于该项目的敏感性及其由于 j 的隐私设定及 j 在网络中的位置而获得的可见度。在一个实施例中,所有 N

个用户对相同的 n 个简档项目指定他们的隐私设置。这些设置被存储在 $n \times N$ 响应矩阵 R 中。对于项目 i 的用户 j 的简档设置 $R(i, j)$ 是确定 j 愿意公开关于 i 的信息的程度的整数值；该值越高， j 越愿意公开关于项目 i 的信息。

[0044] 通常， R 的大值暗示较高的可见度。另一方面，项目的隐私设置的小值是高敏感度的指示，其是大多数人试图保护的高度敏感的项目。因此，存储在响应矩阵 R 中的用户对他们的简档项目的隐私设置具有关于用户的隐私行为的有价值的信息。因此，第一实施例使用该信息通过使用以下概念来计算用户的隐私风险：在社交网络中的每个用户的位置也影响他的隐私风险，且简档项目的可见度设置取决于用户在网络中的角色而增强（或压制）。在隐私风险计算中，考虑社交网络结构和来自信息传播和病毒营销研究的使用模型及算法。

[0045] 在一个实施例中，社交网络 G 由 N 个节点组成，在 $\{1, \dots, N\}$ 中的每个节点 j 与网络的用户相关联。用户通过对应于 G 的边的链接而连接。原则上，这些链接是无权重且无定向的。但是，通常， G 是定向的，且无定向的网络通过为每个输入的无定向边 (j, j') 添加两个定向的边 $(j \rightarrow j')$ 和 $(j' \rightarrow j)$ 而转换为定向网络。每个用户具有由 n 个简档项目组成的简档。对于每个简档项目，用户设置确定使用者公开与该项目相关联的信息的意愿性的隐私级别。由所有 N 个用户为 n 个简档项目挑选的隐私级别被存储在 $n \times N$ 响应矩阵 R 中。 R 的行对应于简档项目，且列对应于用户。

[0046] $R(i, j)$ 指在 R 的第 i 行且第 j 列中的项 (entry)； $R(i, j)$ 指用户 j 对项目 i 的隐私设置。如果响应矩阵 R 的项被限制为在 $\{0, 1\}$ 中取值，则 R 是二分的 (dichotomous) 响应矩阵。另外，如果 R 中的项在 $\{0, 1, \dots, 1\}$ 中取任意非负的整数值，则矩阵 R 是多分的 (polytomous) 响应矩阵。在二分响应矩阵 R 中， $R(i, j) = 1$ 意味着用户 j 已使得与简档项目 i 相关联的信息公共可用。如果用户 j 已经保持与项目 i 相关联的信息为隐私的，则 $R(i, j) = 0$ 。在多分响应矩阵中出现的值的解释是类似的： $R(i, j) = 0$ 意味着用户 j 保持简档项目 i 为隐私； $R(i, j) = 1$ 意味着 j 仅向他的直接 (immediate) 好友公开关于项目 i 的信息。通常， $R(i, j) = k$ (k 在 $\{0, 1, \dots, 1\}$ 内) 意味着 j 向 G 中的至多距离 k 个链接的用户公开与项目 i 相关的信息。通常， $R(i, j) \leq R(i', j)$ 意味着 j 对项目 i' 比项目 i 具有更保守的隐私设置。由 R_i 表示的 R 的第 i 行代表所有用户对于简档项目 i 的设置。类似地，由 R_j 表示的 R 的第 j 列代表用户 j 的简档设置。

[0047] 用户对不同简档项目的设置可以常被认为是由概率分布描述的随机变量。在这种情况下，观察到的响应矩阵 R 是遵循该概率分布的响应的样本。对于二分响应矩阵， $P(i, j)$ 表示用户 j 选择 $R(i, j) = 1$ 的概率。也就是说， $P(i, j) = \text{Prob}_R(i, j) = 1$ 。在多分情况下， $P(i, j, k)$ 表示用户 j 设置 $R(i, j) = k$ 的概率。也就是说， $P(i, j, k) = \text{Prob}_R(i, j) = k$ 。

[0048] 二分设置中的隐私风险

[0049] 用户的隐私风险是测量他的隐私保护的分数。用户的隐私风险越高，对他的隐私威胁越高。用户的隐私风险取决于其为他的简档项目挑选的隐私级别。隐私风险的定义的基本前提如下：

[0050] • 用户揭露的敏感信息越多，他的隐私风险越高。

[0051] • 知道关于用户的某些信息片段的人越多，他的隐私风险越高。

[0052] 以下两个例子例示了这两个前提。

[0053] 例子 1。假设用户 j 和两个简档项目, $i = \{\text{移动电话号码}\}$ 且 $i' = \{\text{爱好}\}$ 。 $R(i, j) = 1$ 是比 $R(i', j) = 1$ 对 j 有更多风险的设置;即使一大群人知道 j 的爱好,但这不可能是与相同组的人知道 j 的移动电话号码的情形相同的打扰情形。

[0054] 例子 2。再次假设用户 j , 且使 $i = \{\text{移动电话号码}\}$ 是单个简档项目。自然, 设置 $R(i, j) = 1$ 是比设置 $R(i, j) = 0$ 更有风险的行为;使得 j 的移动电话公开可得到增加了 j 的隐私风险。

[0055] 在一个实施例中, 用户 j 的隐私风险被定义为两个参数的单调增加的函数: 简档项目的敏感度和这些项目接收的可见度。简档项目的敏感度: 例子 1 和 2 例示了项目的敏感度取决于项目本身。因此, 项目的敏感度被定义如下。

[0056] 定义 1。在 $\{1, \dots, n\}$ 中的项目 i 的敏感度由 β_i 表示, 且取决于项目 i 的本性。

[0057] 一些简档项目本性上比其他的更敏感。在例子 1 中, $\{\text{移动电话号码}\}$ 被认为是对相同隐私级别比 $\{\text{爱好}\}$ 更敏感。简档项目的可见度: 由于 j 导致的简档项目 i 的可见度获得 (capture) 对于 i 的 j 值在网络中变得已知的程度; 其扩展得越多, 项目的可见度越高。由 $V(i, j)$ 表示的可见度取决于值 $R(i, j)$ 、以及具体用户 j 及其在社交网络 G 中的位置。可见度的最简单的可能的定义是 $V(i, j) = I(R(i, j) = 1)$, 其中, $I(\text{条件})$ 是当“条件”为真时变为 1 的指示符变量。这是项目 i 和用户 j 的观察到的可见度。通常, 可以假设 R 是来自所有可能的响应矩阵上的概率分布的样本。然后, 基于该假设来计算可见度。

[0058] 定义 2。如果 $P(i, j) = \text{Prob}_R(i, j) = 1$, 则可见度是 $V(i, j) = P(i, j) \times 1 + (1 - P(i, j)) \times 0 = P(i, j)$ 。

[0059] 概率 $P(i, j)$ 取决于项目 i 和用户 j 两者。所观察的可见度是其中 $P(i, j) = I(R(i, j) = 1)$ 的可见度的实例。用户的隐私风险: 由 $\text{Pr}(i, j)$ 表示的由于项目 i 引起的个人 j 的隐私风险可以是敏感度和可见度的任意组合。也就是说, $\text{Pr}(i, j) = \beta_i V(i, j)$ 。算符 N 用于表示任意的组合函数, 其遵守 $\text{Pr}(i, j)$ 随敏感度和可见度两者单调增加。

[0060] 为了估算由 $\text{Pr}(j)$ 表示的用户 j 的整体隐私风险, j 的隐私风险可以由于不同的项目而被组合。再次, 可以使用任意组合函数来组合每个项目的隐私风险。在一个实施例中, 个人 j 的隐私风险被如下计算: $\text{Pr}(j) = \text{Pr}(i, j)$ 的从 $i = 1$ 到 n 的总和 $= \beta_i \times V(i, j)$ 的从 $i = 1$ 到 n 的总和 $= \beta_i \times P(i, j)$ 的从 $i = 1$ 到 n 的总和。再次, 观察到的隐私风险是其中由观察到的可见度代替 $V(i, j)$ 的隐私风险。

[0061] 二分设置中的隐私风险的朴素 (native) 计算

[0062] 计算隐私风险分数的一个实施例是隐私风险的朴素计算。敏感度的朴素计算: 项目 i 的敏感度 β_i 直观地获得用户使得与第 i 个简档项目相关的信息公开可得的困难程度。如果 $|R_i|$ 表示设置 $R(i, j) = 1$ 的用户的数量, 则对于敏感度的朴素计算, 计算不情愿公开项目 i 的用户的比例。也就是说, $\beta_i = (N - |R_i|) / N$ 。如在公式中计算的, 敏感度取 $[0, 1]$ 中的值; β_i 的值越高, 项目 i 越敏感。可见度的朴素计算: 可见度的计算 (见定义 2) 需要对概率 $P(i, j) = \text{Prob}_R(i, j) = 1$ 的估算。假设项目和个人之间的独立性, 计算 $P(i, j)$ 为在行 R_i 中的 1 的概率乘以列 R_j 中的 1 的概率的乘积。也就是说, 如果 $|R^j|$ 是 j 对其设置 $R(i, j) = 1$ 的项目的数量, 则 $P(i, j) = |R_i| / N \times |R_j| / n = (1 - \beta_i) \times |R_j| / n$ 。概

率 $P(i, j)$ 对于更不敏感的项目以及对于倾向于公开其许多简档项目的用户而言更高。以此方式计算的隐私风险分数是 Pr 朴素分数。

[0063] 在二分设置中的隐私风险的基于 IRT 的计算

[0064] 计算隐私风险分数的另一个实施例是使用来自项目 - 响应理论 (Item-Response Theory, IRT) 的概念的用户隐私风险。在一个实施例中, 可以使用两参数 IRT 模型。在该模型中, 每个受审查人 (examinee) j 的特征由其能力级别 θ_j 表示, θ_j 在 $(-1, 1)$ 内。每个问题 q_i 的特征由一对参数 $\xi_i = (\alpha_i, \beta_i)$ 来表示。 β_i 在 $(-1, 1)$ 内, 参数 β_i 表示 q_i 的难度。 α_i 在 $(-1, 1)$ 内, 参数 α_i 量化 q_i 的辨别能力。该模型的基本随机变量是受审查人 j 对具体问题 q_i 的响应。如果该响应被标记为“对”或“错”(二分响应), 则在两参数模型中, j 正确回答的概率由 $P(i, j) = 1/(1 + e^{-(\alpha_i(\theta_j - \beta_i))})$ 给出。因此, $P(i, j)$ 是参数 θ_j 和 $\xi_i = (\alpha_i, \beta_i)$ 的函数。对于给定的问题 q_i 与参数 $\xi_i = (\alpha_i, \beta_i)$, 作为 θ_j 的函数的上述等式的绘图被称为项目特征曲线 (Item Characteristic Curve, ICC)。

[0065] 参数 β_i 、即项目难度指示在 $P(i, j) = 0.5$ 处的点, 这意味着项目的难度是项目本身的特性, 不是响应了该项目的人的特性。另外, IRT 将 β_i 和 θ_j 放置在相同尺度上, 以便它们可以被比较。如果受审查人的能力高于问题的难度, 则他具有更高的概率来得到正确的答案, 且反之亦然。参数 α_i 、即项目辨别与 $P(i, j) = P_i(\theta_j)$ 在 $P(i, j) = 0.5$ 的点处的斜率成比例; 该斜率越陡, 问题的辨别能力越高, 意味着该问题可以在能力低于和高于该问题的难度的受审查人之间很好地区分。

[0066] 在我们的基于 IRT 的隐私风险计算中, 使用上述等式, 使用用户和简档项目, 来估算概率 $Prob R(i, j) = 1$ 。该映射是将每个受审查人映射到用户, 且将每个问题映射到简档项目。受审查人的能力可以用于量化用户的态度: 对于用户 j , 他的态度 θ_j 量化了 j 对他的隐私的关注程度; θ_j 的低值指示保守的用户, 而 θ_j 的高值指示粗心的用户。困难参数 β_i 用于量化简档项目 i 的敏感度。具有高敏感度值 β_i 的项目更难公开。通常, 参数 β_i 可以取 $(-1, 1)$ 内的任意值。为了维持隐私风险针对项目的敏感度的单调性, 保证对于 $\{1, \dots, n\}$ 内的所有 i , β_i 大于或等于 0。这可以通过将所有项目的敏感度值偏移 $\beta_{\min} = \arg\min_i \in \{1, \dots, n\} \beta_i$ 来处理。在上述映射中, 忽略参数 α_i 。

[0067] 为了计算隐私风险, 计算对于在 $1, \dots, n$ 内的所有项目 i 的敏感度 β_i 和概率 $P(i, j) = Prob R(i, j) = 1$ 。对于后一计算, 确定对于 1 小于或等于 i 、 i 小于或等于 n 的所有参数 $\xi_i = (\alpha_i, \beta_i)$ 以及对于 1 小于或等于 j 、 j 小于或等于 N 的 θ_j 。

[0068] 三个独立性假设是 IRT 模型中固有的: (a) 项目之间的独立性, (b) 用户之间的独立性, 以及 (c) 用户和项目之间的独立性。使用这些方法计算的隐私风险分数是 Pr IRT 分数。

[0069] 敏感性的基于 IRT 的计算

[0070] 在计算具体项目 i 的敏感度 β_i 时, 对于相同项目的 α_i 的值作为副产物而获得。由于项目是独立的, 因此对每个项目单独计算参数 $\xi_i = (\alpha_i, \beta_i)$ 。以下示出如何计算 ξ_i , 假设给出了 N 个个人的态度 $\sim \theta = (\theta_1, \dots, \theta_N)$ 作为输入的部分。进一步示出了当不知道态度时项目的参数的计算。

[0071] 项目参数估算

[0072] 似然函数被定义为:

$$[0073] \quad \prod_{j=1}^N P_{ij}^{R(i,j)} (1 - P_{ij})^{1-R(i,j)}$$

[0074] 因此,估算 $\xi_i = (\alpha_i, \beta_i)$ 以便最大化似然函数。上述似然函数假设每个用户的不同态度。在一个实施例中,在线社交网络用户形成将用户集 $\{1, \dots, N\}$ 划分为 K 个非重叠组 $\{F_1, \dots, F_K\}$ 的分组,以便 F_g 的 $g = 1$ 到 K 的并集 $= \{1, \dots, N\}$ 。使得 θ_g 为组 F_g 的态度 (F_g 的所有成员共享相同态度 θ_g) 且 $f_g = |F_g|$ 。而且,对于每个项目 i ,使得 r_{ig} 为 F_g 中的设置了 $R(i, j) = 1$ 的人数,即 $r_{ig} = |\{j | j \text{ 在 } F_g \text{ 内且 } R(i, j) = 1\}|$ 。给定该分组,可以将似然函数写为:

$$[0075] \quad \prod_{g=1}^K \binom{f_g}{r_{ig}} [P_i(\theta_g)]^{r_{ig}} [1 - P_i(\theta_g)]^{f_g - r_{ig}}.$$

[0076] 在忽略常数之后,对应的 $\log$ -似然函数是:

$$[0077] \quad L =$$

$$[0078] \quad \sum_{g=1}^K [r_g \log P_i(\theta_g) + (f_g - r_{ig}) \log (1 - P_i(\theta_g))]$$

[0079] 估算项目参数 $\xi_i = (\alpha_i, \beta_i)$ 以便最大化 $\log$ -似然函数。在一个实施例中,使用 Newton-Raphson 方法。Newton-Raphson 方法是在给出偏导数:

$$[0080] \quad L_1 = \frac{\partial L}{\partial \alpha_i} \text{ 和 } L_2 = \frac{\partial L}{\partial \beta_i},$$

[0081] 以及

$$[0082] \quad L_{11} = \frac{\partial^2 L}{\partial \alpha_i^2}, \quad L_{22} = \frac{\partial^2 L}{\partial \beta_i^2}, \quad L_{12} = L_{21} = \frac{\partial^2 L}{\partial \alpha_i \partial \beta_i},$$

[0083] 的情况下迭代地评估参数 $\xi_i = (\alpha_i, \beta_i)$ 的方法。在迭代 $(t+1)$ 处,从迭代 t

处的对应估算来计算由 $\begin{bmatrix} \hat{\alpha}_i \\ \hat{\beta}_i \end{bmatrix}_{t+1}$ 表示的参数的估算,如下:

$$[0084] \quad \begin{bmatrix} \hat{\alpha}_i \\ \hat{\beta}_i \end{bmatrix}_{t+1} = \begin{bmatrix} \hat{\alpha}_i \\ \hat{\beta}_i \end{bmatrix}_t - \begin{bmatrix} L_{11} & L_{12} \\ L_{21} & L_{22} \end{bmatrix}_t^{-1} \times \begin{bmatrix} L_{11} \\ L_{21} \end{bmatrix}_t$$

[0085] 在迭代 $(t+1)$ 处,使用在迭代 t 处计算的 α_i 和 β_i 的估算来计算导数 $L_1, L_2, L_{11}, L_{22}, L_{12}$ 和 L_{21} 的值。

[0086] 在对于 $\{1, \dots, n\}$ 中的所有项目 i 计算 $\xi_i = (\alpha_i, \beta_i)$ 的一个实施例中,具有态度 $\sim \theta$ 的 N 个用户的集合被划分为 K 个组。该划分实现了基于用户的态度将用户 1- 维聚类为 K 个群集,这可以可选地使用动态编程来进行。

[0087] 该过程的结果是将用户分组为 K 个组 $\{F_1, \dots, F_K\}$ 的分组,组态度 $\theta_{g,1}$ 小于或等于 g, g 小于或等于 K 。给出该分组,计算对于 1 小于或等于 i, i 小于或等于 n 和 1 小于或等于 g, g 小于或等于 K 的 f_g 和 r_{ig} 的值。给出这些值,项目 NR 估算对 n 个项目的每个实施上述等式。

[0088]

算法1 用于所有项目 $i \in (1, \dots, n)$ 的 $\xi_i = (\alpha_i, \beta_i)$ 的项目参数估计。

输入： 响应矩阵 R 、用户态度 $\vec{\theta} = (\theta_1, \dots, \theta_N)$ 及用户的态度组的数量 K 。

输出： 项目参数 $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$ 及 $\vec{\beta} = (\beta_1, \dots, \beta_n)$ 。

1: $\{F_g, \theta_g\}_{g=1}^K \leftarrow \text{PartitionUsers}(\vec{\theta}, K)$

2: 对于 $g=1$ 到 K 进行

[0089]

3: $f_g \leftarrow |F_g|$

4: 对于 $i=1$ 到 n 进行

5: $r_{ig} \leftarrow \left| \left\{ j \in F_g \text{ 以及 } R(i, j) = 1 \right\} \right|$

6: 对于 $i=1$ 到 n 进行

7: $(\alpha_i, \beta_i) \leftarrow \text{NR_Item_Estimation}(R_i, \{f_g, r_{ig}, \theta_g\}_{g=1}^K)$

[0090] 项目参数估算的 EM 算法

[0091] 在一个实施例中,可以计算项目参数而不用知道用户态度,因此仅具有响应矩阵 R 作为输入。令 $\sim \xi = (\xi_1, \dots, \xi_n)$ 为所有项目的参数的向量。因此, ξ 是在给出响应矩阵 R 时估算的 (即,最大化 $P(R | \sim \xi)$ 的 $\sim \xi$)。令 $\sim \theta$ 为隐藏且观察不到的变量。因此, $P(R | \sim \xi) = P(R, \sim \theta | \sim \xi)$ 对于 $\sim \theta$ 的总和。使用期望值最大化 (EM), 计算如下 $\sim \xi$: 对于该 $\sim \xi$, 通过最大化以下期望函数, 以上边限 (marginal) 实现本地最大值:

[0092]
$$\mathbf{E}_{\vec{\theta} \sim P(\vec{\theta} | R, \vec{\xi})} [\log P(R, \vec{\theta} | \vec{\xi})]$$

[0093] 对于将用户分为 K 组的分组:

[0094]
$$\log P(R, \vec{\theta} | \vec{\xi}) =$$

[0095]
$$\sum_{i=1}^n \sum_{g=1}^K [r_{ig} \log P_i(\theta_g) + (f_g - r_{ig}) \log (1 - P_i(\theta_g))]$$

[0096] 取其的期望 E 产生:

[0097]
$$\mathbf{E} [\log P(R, \vec{\theta} | \vec{\xi})] = \sum_{i=1}^n \sum_{g=1}^K [\mathbf{E}[r_{ig}] \log P_i(\theta_g) + \mathbf{E}[f_{ig} - r_{ig}] \log (1 - P_i(\theta_g))]$$

[0098] 使用 EM 算法来最大化该等式, 使用以下递归, 从迭代 t 处估算的参数来计算在迭代 $(t+1)$ 处的参数的估算:

[0099]
$$\vec{\xi}^{(t+1)} = \operatorname{argmax}_{\vec{\xi}} \mathbf{E}_{\vec{\theta} \sim P(\vec{\theta} | R, \vec{\xi}^{(t)})} [\log P(R, \vec{\theta} | \vec{\xi})]$$

[0100] 在以下算法 2 中给出了 EM 算法的伪码 (pseudocode)。该算法的每个迭代由期望和最大化步骤组成。

[0101]

算法2 用于估计对于所有项目 $i \in \{1, \dots, n\}$ 的项目参数 $\xi_i = (\alpha_i, \beta_i)$ 的EM算法。

输入： 响应矩阵 R 及具有相同态度的用户组的数量 K 。

输出： 项目参数 $\vec{\alpha} = (\alpha_1, \dots, \alpha_n)$, $\vec{\beta} = (\beta_1, \dots, \beta_n)$ 。

1: 对于 $i=1$ 到 n 进行

2: $\alpha_i \leftarrow$ 随机数

3: $\beta_i \leftarrow$ 随机数

4: $\xi_i \leftarrow (\alpha_i, \beta_i)$

5: $\vec{\xi} \leftarrow (\xi_1, \dots, \xi_n)$

6: **重复**

 // 期望步骤

7: 对于 $i=1$ 到 n 进行

8: 对于 $g=1$ 到 K 进行

9: 从 $P(\theta_g | R, \vec{\xi})$ 采样 θ_g

10: 使用等式 (9) 计算 $\bar{f}_{ig}$

11: 使用等式 (10) 计算 $\bar{r}_{ig}$ 。

 // 最大化步骤

12: 对于 $i=1$ 到 n 进行

13: $(\alpha_i, \beta_i) \leftarrow \text{NR_Item_Estimation}(R_i, \{\bar{f}_{ig}, \bar{r}_{ig}, \theta_g\}_{g=1}^K)$

14: $\xi_i \leftarrow (\alpha_i, \beta_i)$

15: **直到收敛**

[0102] 对于固定的估算 $\sim \xi$, 在期望步骤中, 从后验概率分布 $P(\theta | R, \xi)$ 中采样 $\sim \theta$, 且计算该期望。首先, 在假设 K 组的情况下采样 $\sim \theta$ 意味着对于每组 $g \in \{1, \dots, K\}$, 我们可以从分布 $P(\theta_g | R, \sim \xi)$ 中采样态度 θ_g 。假设已知要计算概率, 可以使用期望的定义来计算对于每个项目 i 和组 $g \in \{1, \dots, K\}$ 的式子 $E[f_{ig}]$ 和 $E[r_{ig}]$ 。也就是说,

$$[0103] \quad E[f_{ig}] = \bar{f}_{ig} = \sum_{j=1}^N P(\theta_g | R^j, \vec{\xi}) \text{ 以及}$$

$$[0104] \quad E[r_{ig}] = \bar{r}_{ig} = \sum_{j=1}^N P(\theta_g | R^j, \vec{\xi}) \times R(i, j)$$

[0105] 一组中的用户的成员关系是有概率性的。也就是说, 每个人以某概率属于每一

组；这些成员关系概率的总和等于知道所有组的 fig 和 rig 的值，且所有项目允许期望等式的估算。在最大化步骤中，计算最大化期望的新的 $\sim \xi$ 。通过对每个项目 i 独立地计算参数 ξ_i 来形成向量 $\sim \xi$ 。

[0106] 态度 $\sim \theta$ 的后验概率：为了应用 EM 框架，从后验概率分布 $P(\sim \theta | R, \sim \xi)$ 中采样向量 $\sim \theta$ 。虽然实际上该概率分布可能未知，但是仍然可以进行该采样。向量 $\sim \theta$ 由每个个体 $j \in \{1, \dots, N\}$ 的态度级别组成。另外，存在具有态度 $\{\theta_g\}$ 、 $g = 1$ 到 K 的 K 个组的存在假设。采样如下进行：对于每个组 g ，对能力级别 θ_g 采用，且计算该任何用户 $j \in \{1, \dots, N\}$ 具有能力级别 $\theta_j = \theta_g$ 的后验概率。通过定义概率，该后验概率为：

$$[0107] \quad P(\theta_j | R^j, \vec{\xi}) = \frac{P(R^j | \theta_j, \vec{\xi}) g(\theta_j)}{\int P(R^j | \theta_j, \vec{\xi}) g(\theta_j) d\theta_j}$$

[0108] 函数 $g(\theta_j)$ 是在全体用户中的态度的概率密度函数。其用于对关于用户态度的先前知识进行建模（称为用户态度的先前分布）。遵循标准惯例，假设先前分布对于所有用户都相同。另外，假设函数 g 是正态分布 (normal distribution) 的密度函数。

[0109] 每个态度 θ_j 的先验概率的估算需要对积分的估算。如下克服该问题：由于假设存在 K 个组，因此在能力程度上采样仅 K 个点 $X_1, \dots, X_K$ 。对于每个 $t \in \{1, \dots, N\}$ ，对于在态度值 X_t 处的态度函数的密度计算 $g(X_t)$ 。然后，设置 $A(X_t)$ 作为由点 $(X_t - 0.5, 0)$ ， $(X_t + 0.5, 0)$ ， $(X_t - 0.5, g(X_t))$ 和 $(X_t + 0.5, g(X_t))$ 定义的矩形的面积。标准化 $A(X_t)$ 值，以便 (X_t) 的从 $t = 1$ 到 K 的总和 = 1。以此方式，通过以下等式来获得 X_t 的后验概率：

$$[0110] \quad P(X_t | R^j, \vec{\xi}) = \frac{P(R^j | X_t, \vec{\xi}) A(X_t)}{\sum_{t=1}^K P(R^j | X_t, \vec{\xi}) A(X_t)}$$

[0111] 可见度的基于 IRT 的计算

[0112] 可见度的计算需要对 $P(i, j) = \text{Prob}(R(i, j) = 1)$ 的估算。

[0113] 描述 NR 态度估算算法，其是在给出项目参数 $\sim \alpha = (\alpha_1, \dots, \alpha_n)$ 以及 $\sim \beta = (\beta_1, \dots, \beta_n)$ 的情况下计算个人的态度的 Newton-Raphson 过程。这些项目参数可以作为输入给出，或者可以使用 EM 算法（见算法 2）来计算它们。对于每个个人 j ，该 NR 态度估算计算 θ_j ，该 θ_j 使被定义为 $P(i, j) \wedge (R(i, j)) (1 - P(i, j)) \wedge (1 - R(i, j))$ 的从 $i = 1$ 到 n 的乘法序列的似然或对应的 $\log$ -似然最大化，如下：

$$[0114] \quad L = \sum_{i=1}^n [R(i, j) \log P_{ij} + (1 - R(i, j)) \log (1 - P_{ij})]$$

[0115] 由于 $\sim \alpha$ 和 $\sim \beta$ 是输入的部分，因此用于最大化的变量是 θ_j 。再次使用 Newton-Raphson 方法来迭代地获得由 $\hat{\theta}_j$ 表示的 θ_j 的估算。使用在迭代 t 处的估算 $[\hat{\theta}_j]_t$ 来计算在迭代 $(t+1)$ 处的估算 $\hat{\theta}_j$ ， $[\hat{\theta}_j]_{t+1}$ ，如下：

$$[0116] \quad [\hat{\theta}_j]_{t+1} = [\hat{\theta}_j]_t - \left[\frac{\partial^2 L}{\partial \theta_j^2} \right]_t^{-1} \left[\frac{\partial L}{\partial \theta_j} \right]_t$$

[0117] 多分设置的隐私风险

[0118] 已经描述了当该输入是二分响应矩阵 R 时用户的隐私风险的计算。以下，在先前部分中描述的定义和方法被扩展以处理多分响应矩阵。在多分矩阵中，每个项 $R(i, j) = k$ ，

其中 $k \in \{0, 1, \dots, l\}$ 。 $R(i, j)$ 的值越小 ; 用户 j 相对于简档项目 i 的隐私设置越保守。将先前给出的隐私风险的定义扩展到多分情况。以下也示出可以如何使用朴素和基于 IRT 的方法来计算隐私风险。

[0119] 如在二分情况下, 用户 j 相对于简档项目 i 的隐私风险是项目 i 的敏感度和由于 j 导致的项目 i 在社交网络中得到的可见度的函数。在多分情况下, 敏感度和可见度两者取决于该项目本身和分配给它的隐私级别 k 。因此, 项目关于隐私级别 k 的敏感度被定义如下。

[0120] 定义 3 : 项目 $i \in \{1, \dots, n\}$ 关于隐私级别 $k \in \{0, \dots, l\}$ 的敏感度由 β_{ik} 表示。函数 β_{ik} 关于 k 单调增加 ; 为项目 i 挑选的隐私级别 k 越大, 其敏感度越高。

[0121] 在以下例子中看出定义 3 的相关性。

[0122] 例子 5。假设用户 j 和项目 $i = \{\text{移动电话号码}\}$ 。设置 $R(i, j) = 3$ 比设置 $R(i, j) = 1$ 使得项目 i 更敏感。在前一情况下, 向更多用户公开 i , 且因此存在其可能被误用的更多方式。

[0123] 类似地, 项目的可见度变为其隐私级别的函数。因此, 定义 2 可以被扩展如下。

[0124] 定义 4 : 如果 $P_{i,j,k} = \text{Prob}\{R(i, j) = k\}$, 则在级别 k 处的可见度是 $V(i, j, k) = P_{i,j,k} \times k$ 。

[0125] 给出了定义 3 和 4, 如下计算用户 j 的隐私风险 :

$$[0126] \quad \text{PR}(j) = \sum_{i=1}^n \sum_{k=1}^l \beta_{ik} \times P_{ijk} \times k$$

[0127] 计算多分设置的隐私风险的朴素方法

[0128] 在多分情况下, 对于每个级别 k 单独计算项目的敏感度。因此, 敏感度的朴素计算如下 :

$$[0129] \quad \beta_{ik} = \frac{N - \sum_{j=1}^N I_{(R(i,j)=k)}}{N}$$

[0130] 在多分情况下的可见度需要计算概率 $P_{i,j,k} = \text{Prob}\{R(i, j) = k\}$ 。通过假设项目和用户之间的独立性, 该概率可以被计算如下 :

$$[0131] \quad P_{ijk} = \frac{\sum_{j=1}^N I_{(R(i,j)=k)}}{N} \times \frac{\sum_{i=1}^n I_{(R(i,j)=k)}}{n}$$

$$[0132] \quad = (1 - \beta_{ik}) \times \frac{\sum_{i=1}^n I_{(R(i,j)=k)}}{n}$$

[0133] 概率 P_{ijk} 是要在行 i 中观察到值 k 的概率乘以要在列 j 中观察到值 k 的概率的积。如在二分情况下那样, 使用上述等式计算的分数是 Pr 朴素分数。

[0134] 确定多分设置的隐私风险分数的基于 IRT 的方法

[0135] 处理多分响应矩阵对于基于 IRT 的隐私风险稍微更复杂。计算隐私风险是将多分响应矩阵 R 变换为 $(l+1)$ 个二分响应矩阵 $R^*0, R^*1, \dots, R^*l$ 。每个矩阵 R^*k (对于 $k \in \{0, 1, \dots, l\}$) 被构造以便如果 $R(i, j) \geq k$ 则 $R^*k(i, j) = 1$, 否则 $R^*k(i, j) = 0$ 。令 $P^*_{ijk} = \text{Prob}\{R(i, j) \geq k\}$ 。由于矩阵 R^*i0 使所有项等于一, 因此对于所有用户, $P^*_{ij0} = 1$ 。对于其他二分响应矩阵 R^*k , 其中 $k \in \{1, \dots, l\}$, 设置 $R^*k(i, j) = 1$ 的概率被给出为 :

$$[0136] \quad P_{ijk}^* = \frac{1}{1 + e^{-\alpha_{ik}^* (\theta_j - \beta_{ik}^*)}}$$

[0137] 通过构造,对于每个 $k', k \in \{1, \dots, l\}$ 且 $k' < k$, 矩阵 R^{*k} 仅包含在矩阵 $R^{*k'}$ 中出现的项 1 的子集。因此, $P_{ijk'}^* \geq P_{ijk}$ 。因此,对于 $k \in \{1, \dots, l\}$, P_{ijk} 的 ICC 曲线不交叉。该观察得到以下推论:

[0138] 推论 1:对于项目 i 和隐私级别 $k \in \{1, \dots, l\}$, $\beta_{i*1} < \dots < \beta_{ik} < \dots < \beta_{il}$ 。此外,由于曲线 P_{ijk} 不交叉,因此 $\alpha_{i*1} = \dots = \alpha_{ik} = \dots = \alpha_{il} = \alpha_{i*}$ 。

[0139] 由于 $P_{ij0} = 1$, 因此未定义 α_{i*0} 及 β_{i*0} 。

[0140] 隐私风险的计算可能需要计算 $P_{ijk} = \text{Prob}\{R(i, j) = k\}$ 。该概率不同于 P_{ijk}^* , 因为前者指的是项 $R(i, j) = k$ 的概率,而后者是累积概率 $P_{ijk}^* = P_{ijk}$ 的从 $k' = k$ 到 1 的总和。或者:

$$[0141] \quad \text{Prob}\{R(i, j) = k\} = \text{Prob}\{[R_k^*(i, j) - R_{k+1}^*(i, j)]\}$$

[0142] 上述等式可以概括为 P_{ik}^* 和 P_{ik} 之间的以下关系:对于每个项目 i , 态度 θ_j 和隐私级别 $k \in \{0, \dots, l-1\}$,

$$[0143] \quad P_{ik}(\theta_j) = P_{ik}^*(\theta_j) - P_{i(k+1)}^*(\theta_j)$$

[0144] 对于 $k = l$, $P_{il}(\theta_j) = P_{il}^*(\theta_j)$ 。

[0145] 命题 1:对于 $k \in \{1, \dots, l-1\}$, $\beta_{ik} = (\beta_{ik}^* + \beta_{i(k+1)}^*)/2$ 。而且 $\beta_{i0} = \beta_{i*1}$ 且 $\beta_{il} = \beta_{*il}$ 。

[0146] 从命题 1 和推论 1, 提供了推论 2:

[0147] 推论 2. 对于 $k \in \{0, \dots, l\}$, $\beta_{i0} < \beta_{i1} < \dots < \beta_{il}$ 。

[0148] 多分设置的基于 IRT 的敏感度:项目 i 相对于隐私级别 k 的敏感度 β_{ik} 是 P_{ijk} 曲线的敏感度参数。其通过首先计算敏感度参数 β_{ik}^* 和 $\beta_{i(k+1)}^*$ 来计算。然后,使用命题 1 来计算 β_{ik} 。

[0149] 目标是对每个项目 i 计算敏感度参数 $\beta_{i*1}, \dots, \beta_{*il}$ 。考虑两种情况:用户的态度 $\sim \theta$ 作为输入的一部分与响应矩阵 R 一起给出的情况,以及输入仅由 R 组成的情况。在参考第二情况时,同时计算对 $1 \leq k \leq l$ 的所有 $(l+1)$ 个未知参数 α_{i*} 和 β_{ik}^* 。假设 N 个个人的集合可以被划分为 K 个组,以便在第 g 组中的所有个人具有相同态度 θ_g 。而且,令 $P_{ik}(\theta_g)$ 为组 g 中的个人 j 设置 $R(i, j) = k$ 的概率。最后,由 f_g 表示在第 g 组中的用户的总数,且由 r_{gk} 表示在第 g 组中的设置 $R(i, j) = k$ 的人数。给出该分组,在多种情况下的数据的似然可以写为:

$$[0150] \quad \prod_{g=1}^K \frac{f_g!}{r_{g1}! r_{g2}! \dots r_{ge}!} \prod_{k=1}^l [P_{ik}(\theta_g)]^{r_{gk}}$$

[0151] 在忽略常数之后,对应的 log- 似然函数是:

$$[0152] \quad L = \sum_{g=1}^K \sum_{k=1}^l r_{gk} \log P_{ik}(\theta_g)$$

[0153] 使用对后三个等式的减法,可以将 L 变换为其中仅未知 $(l+1)$ 个参数 (α_{i*} , $\beta_{i*1}, \dots, \beta_{*il}$) 的函数。使用迭代 Newton-Raphson 过程来进行这些参数的计算,除了差别以外,类似于先前所述,在此该差别是存在对于其要计算 log- 似然 L 的偏导数的更多未

知参数。

[0154] 多分设置的基于 IRT 的可见度:在多分情况下计算可见度值需要对所有个人计算态度 $\sim \theta$ 。给出项目参数 $\alpha * i$ 、 $\beta * i_1$ 、 $\cdots$ 、 $\beta * i_l$,可以使用类似于 NR 态度估算的过程对每个用户独立地进行计算。差别在于用于该计算的似然函数是在先前等式中给出的似然函数。

[0155] 用于多分响应矩阵的敏感度和可见度的基于 IRT 的计算为每个用户给出隐私风险分数。如在二分 IRT 计算中那样,如此获得的分数被称为 Pr IRT 分数。

[0156] 实施系统和方法的示例计算机架构

[0157] 图 4 图示用于实现隐私设置和 / 或隐私环境的计算的示例计算机架构。在一个实施例中,计算机架构是图 2 中的控制台 205 的例子。图 4 的示例计算系统包括:1) 一个或多个处理器 401;2) 存储器控制集线器 (MCH) 402;3) 系统存储器 403 (存在不同类型,比如 DDR RAM, EDO RAM 等);4) 缓存 404;5) I/O 控制集线器 (ICH) 405;6) 图形处理器 406;7) 显示器 / 屏幕 407 (存在不同类型,比如阴极射线管 (CRT)、薄膜晶体管 (TFT)、液晶显示器 (LCD), DPL, 等);和 / 或 8) 一个或多个 I/O 设备 408。

[0158] 一个或多个处理器 401 执行指令以便进行计算系统实现的任何软件例程。例如,处理器 401 可以进行确定和翻译指示符或确定隐私风险分数的操作。这些指令经常涉及在数据上进行的某种操作。数据和指令两者被存储在系统存储器 403 和缓存 404 中。数据可以包括指示符。缓存 404 通常被涉及为具有比系统存储器 403 更短的等待时间。例如,缓存 404 可以被集成到与处理器相同的硅芯片上和 / 或用较快的 SRAM 单元来构造,而系统存储器 403 可以用较慢的 DRAM 单元构造。通过相比于系统存储器 403 而试图在缓存 404 中存储更频繁使用的指令和数据,计算系统的整体性能效率改善。

[0159] 慎重地使得系统存储器 403 对计算系统内的其他组件可用。例如,从计算系统的各种接口 (例如,键盘和鼠标、打印机端口、LAN 端口、调制解调器端口等) 接收的或从计算系统的内部存储元件 (例如,硬盘) 取回的数据,在由一个或多个处理器 401 在软件程序的实现中对它们进行操作之前,通常临时被排队到系统存储器 403 中。类似地,软件程序确定应该通过计算系统接口之一从计算系统发送到外部实体的或被存储到外部存储元件中的数据在其被传输或存储之前通常临时被排队在系统存储器 403 中。

[0160] ICH 405 负责保证在系统存储器 403 及其适当的对应计算系统接口 (和内部存储器件,如果如此设计计算系统的话) 之间恰当地传递这种数据。MCH 402 负责管理处理器 401、接口和内部存储元件之间对系统存储器 403 访问的各种竞争请求,这些各种竞争请求可能彼此在时间上接近地出现。

[0161] 一个或多个 I/O 设备 408 也在典型的计算系统中实现。I/O 设备通常负责向和 / 或从计算系统 (例如,网络适配器) 传送数据;或负责计算系统内的大规模非易失性存储 (例如,硬盘)。ICH 405 具有在其本身和所观察的 I/O 设备 408 之间的双向点对点链接。在一个实施例中, I/O 设备从社交网络网站发送和接收信息,以便确定用户的隐私设置。

[0162] 所要求保护的系统的不同实施例的模块可以包括软件、硬件、固件或其任意组合。模块可以是运行专有或公共软件的公共或专用或通用处理器可用的软件程序。该软件还可以是为签名创建和组织并重编译管理专门写出的专用程序。例如,系统的存储器可以包括,但不限于硬件 (比如软盘、光盘、CD-ROM 和磁光盘、ROM、RAM、EPROM、EEPROM、快闪卡、磁卡

或光卡、传播介质或其他类型的介质 / 机器可读介质)、软件(比如需要在硬件存储单元上存储信息的指令)或其任意组合。

[0163] 另外,本发明的元件还可以提供为用于存储机器可执行指令的机器可读介质。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、快闪卡、磁卡或光卡、传播介质或适用于存储电子指令的其他类型的介质 / 机器可读介质。

[0164] 对于图中所示的示例方法,本发明的实施例可以包括上述的各种处理。这些处理可以体现在机器可执行指令中,该机器可执行指令使得通用或专用处理器进行特定步骤。或者,这些处理可以由包含用于进行处理的硬连接的逻辑的专用硬件组件或由编程的计算机组件和定制的硬件组件的任意组合来执行。

[0165] 本发明的实施例不需要所有的给出的各种处理,且本领域技术人员可以想到在没有给出的具体处理或具有未给出的额外处理的情况下如何实践本发明的实施例。

[0166] 概括

[0167] 本发明的实施例的前述描述仅为了图示和描述的目的而给出,且不意图穷举或限制本发明到所公开的精确的形式。在不脱离本发明的精神和范围的情况下,各种修改和适应对本领域技术人员是显而易见的。例如,虽然已经描述了社交网络内或其之间传播隐私设置,但是可以在诸如共享隐私设置的两个计算机的设备之间发生设置的传播。

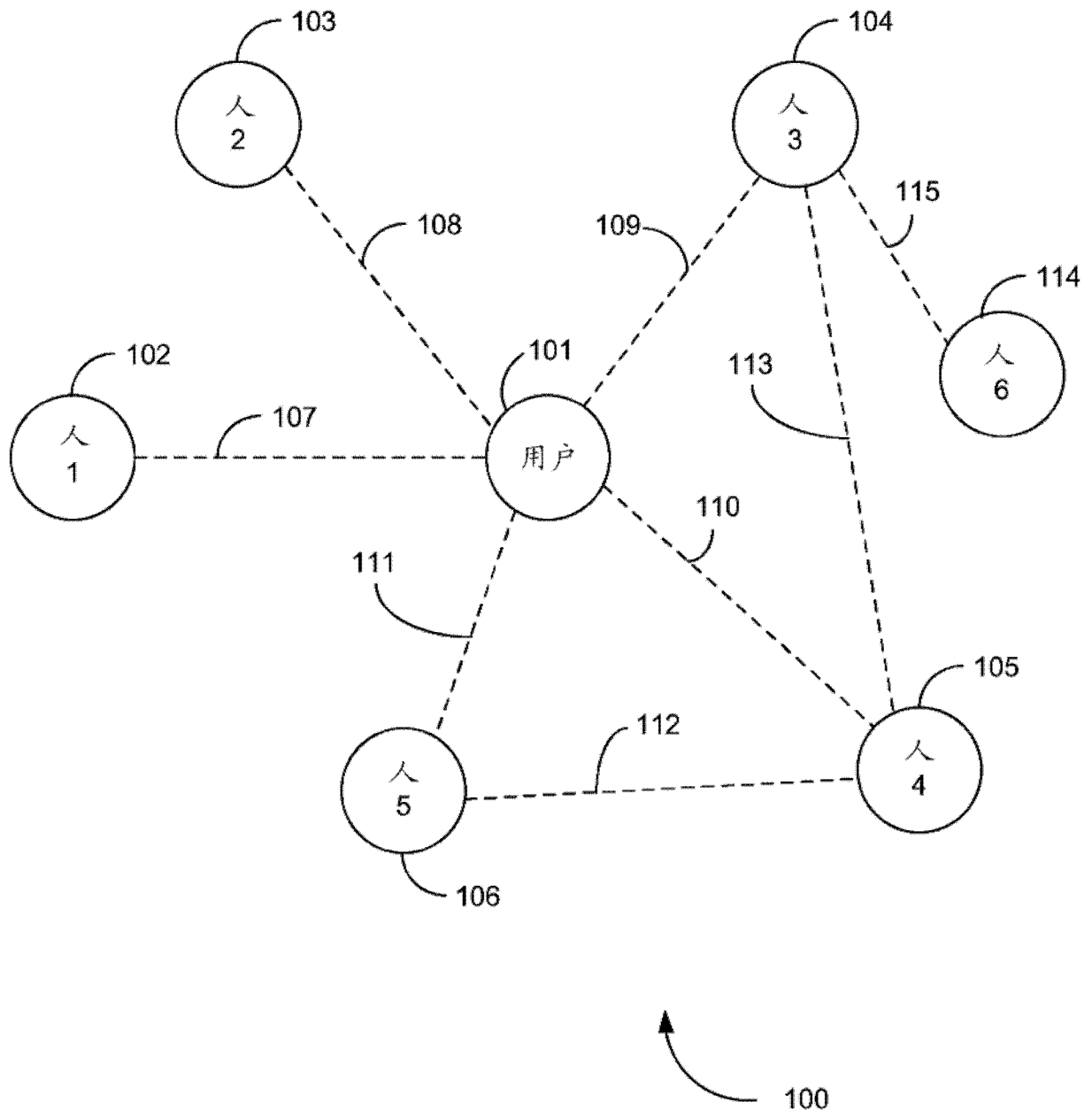


图 1

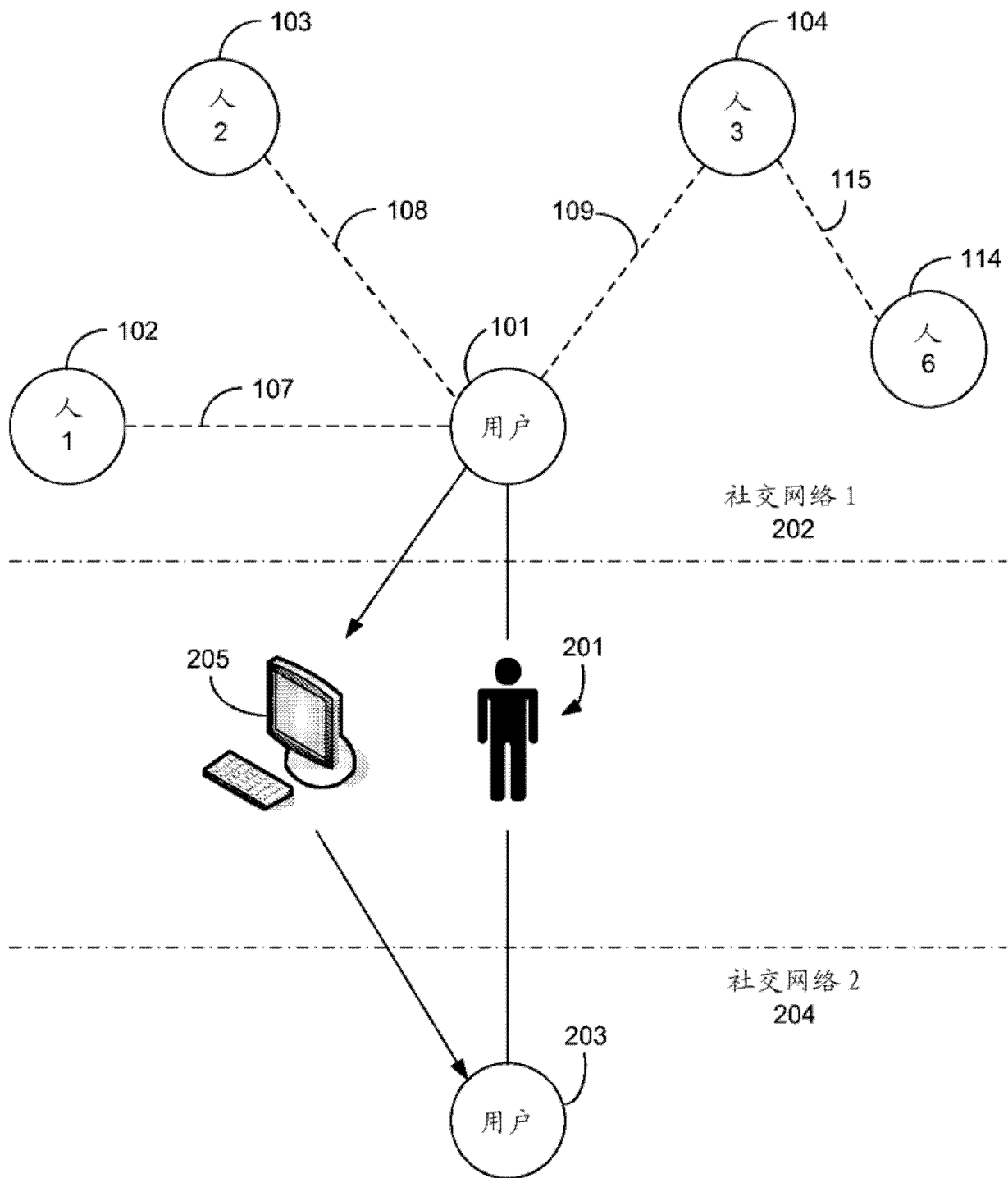


图 2

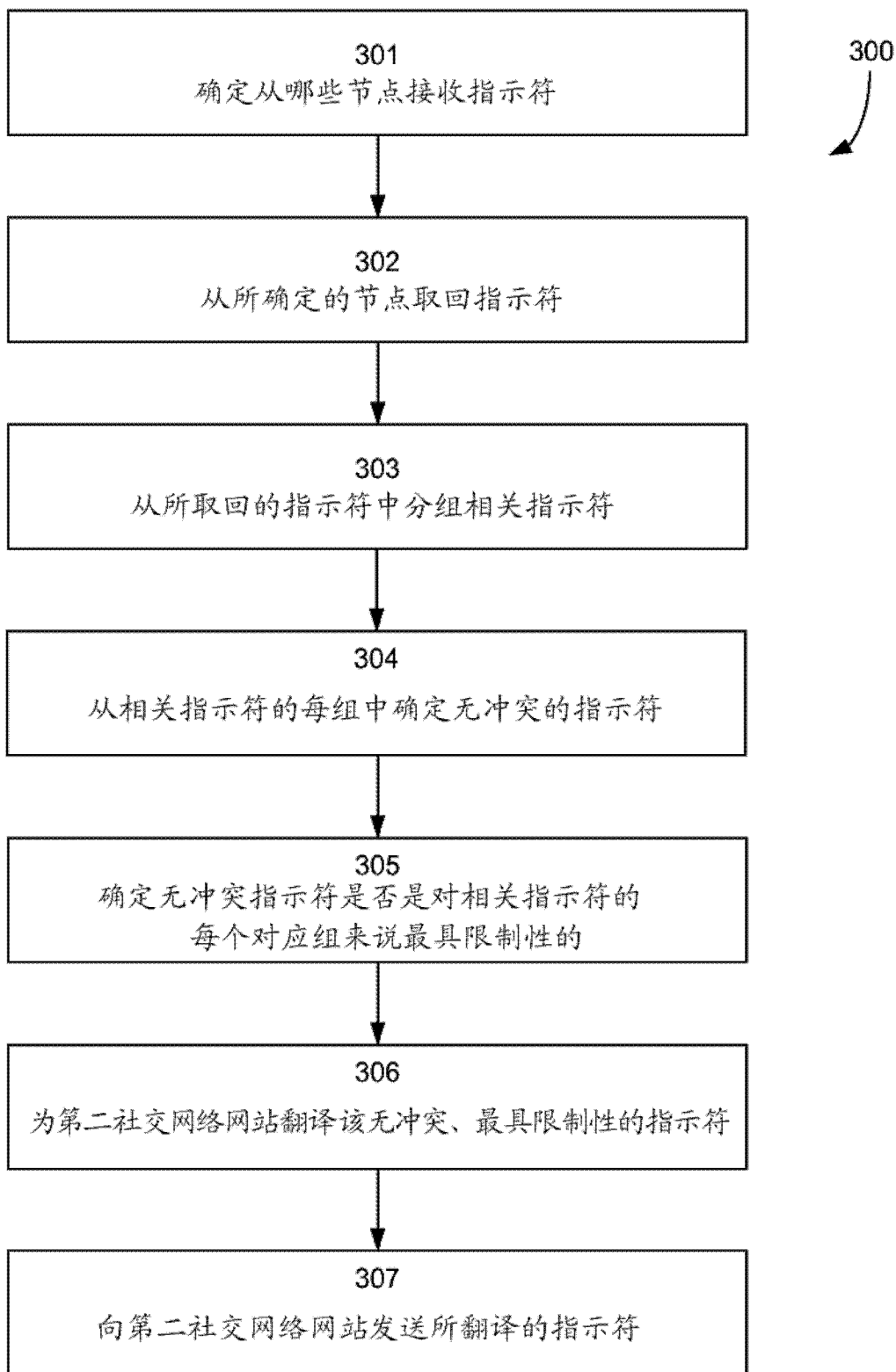


图 3

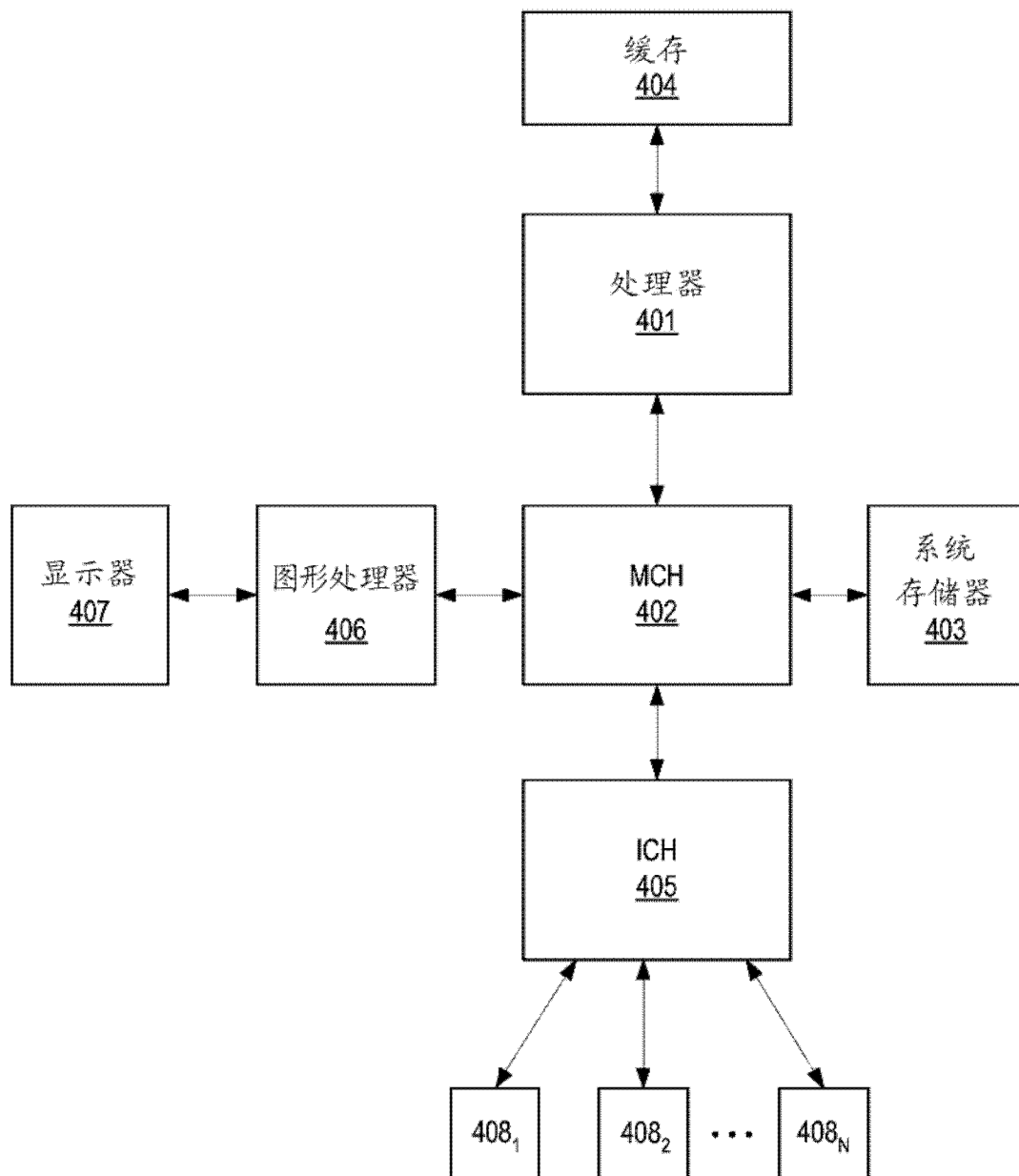


图 4