

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 2 月 2 日 (02.02.2017)



(10) 国际公布号
WO 2017/016067 A1

- (51) 国际专利分类号:
H04W 12/06 (2009.01)
- (21) 国际申请号: PCT/CN2015/091338
- (22) 国际申请日: 2015 年 9 月 30 日 (30.09.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510454359.0 2015 年 7 月 29 日 (29.07.2015) CN
- (71) 申请人: 宇龙计算机通信科技(深圳)有限公司
(YULONG COMPUTER TELECOMMUNICATION
SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中
国广东省深圳市南山区科技园北区梦溪道 2 号,
Guangdong 518057 (CN)。
- (72) 发明人: 王健 (WANG, Jian); 中国广东省深圳市南
山区科技园北区梦溪道 2 号, Guangdong 518057
(CN)。 叶志远 (YE, Zhiyuan); 中国广东省深圳市
南山区科技园北区梦溪道 2 号, Guangdong 518057
(CN)。
- (74) 代理人: 北京友联知识产权代理事务所(普通合
伙) (YOULINK INTELLECTUAL PROPERTY

LAW FIRM); 中国北京市海淀区学清路 8 号科技财
富中心 A 座 506 室尚志峰, Beijing 100192 (CN)。

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

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

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(54) Title: METHOD OF RESPONDING TO COMMUNICATION CONNECTION REQUEST AND USER TERMINAL

(54) 发明名称: 一种通信连接请求的响应方法及用户终端

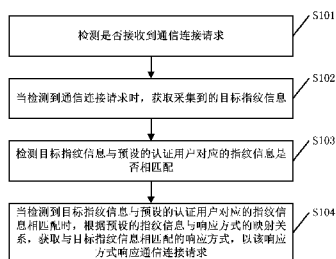


图 1

S101 Detect whether a communication connection request is received

S102 If the communication connection request is detected, acquire collected target fingerprint information

S103 Detect whether the target fingerprint information matches preset fingerprint information corresponding to an authenticated user

S104 If it is detected that the target fingerprint information matches the preset fingerprint information corresponding to the authenticated user, acquire a responding mode matching the target fingerprint information according to a mapping relationship between the preset fingerprint information and the responding mode, and respond to the communication connection request in the responding mode

(57) Abstract: Provided in the present invention are a method of responding to a communication connection request and a user terminal. The method comprises: when a communication connection request is detected and received, acquiring, by a terminal, collected target fingerprint information (S102); detecting whether the target fingerprint information matches preset fingerprint information corresponding to an authenticated user (S103); and if it is detected that the target fingerprint information matches the preset fingerprint information corresponding to the authenticated user, acquiring a responding mode matching the target fingerprint information according to a mapping relationship between the preset fingerprint information and the responding mode, and responding to the communication connection request in the responding mode (S104). The present invention can improve the security of communication between terminals.

(57) 摘要: 本发明提供了一种通信连接请求的响应方法及用户终端, 包括: 当检测接收到通信连接请求时, 终端获取采集到的目标指纹信息 (S102); 检测目标指纹信息与预设的认证用户对应的指纹信息是否相匹配 (S103); 当检测到目标指纹信息与预设的认证用户对应的指纹信息相匹配时, 根据预设的指纹信息与响应方式的映射关系, 获取与目标指纹信息相匹配的响应方式, 以该响应方式响应通信连接请求 (S104)。本发明能够提高利用终端通信联系的安全性。



WO 2017/016067 A1

说明书

一种通信连接请求的响应方法及用户终端

技术领域

本发明涉及通信技术领域，尤其涉及一种通信连接请求的响应方法及用户终端。

背景技术

随着电子技术的快速发展以及终端的迅速普及，终端的功能日益完善。例如，用户可以利用终端访问外部网络数据资源、拍照以及与其他通信用户进行通信联系等等。具体地，当某一通信终端接收到其他通信终端发送的通信连接请求时，任意用户都可以通过输入确认指令，以响应该通信连接请求，建立通信连接。然而，当该通信终端被不法分子所获取时，则不法分子可以通过模仿该通信终端的机主的声音，以欺骗其他通信用户。由此可见，目前利用终端进行通信联系时，安全性不高。

发明内容

本发明实施例提供了一种通信连接请求的响应方法及用户终端，能够提高利用终端通信联系的安全性。

第一方面，本发明实施例公开了一种通信连接请求的响应方法，包括：

检测是否接收到通信连接请求；

当检测接收到所述通信连接请求时，获取采集到的目标指纹信息；

检测所述目标指纹信息与预设的认证用户对应的指纹信息是否相匹配；

当检测到所述目标指纹信息与所述预设的认证用户对应的指纹信息相匹配时，根据预设的指纹信息与响应方式的映射关系，获取与所述目标指纹信息相匹配的响应方式，以所述响应方式响应所述通信连接请求。

结合第一方面的实现方式，在第一方面的第一种可能的实现方式中，在执行步骤检测接收到所述通信连接请求之后，所述获取采集到的目标指纹信息之前，还可以包括以下步骤：

获取所述通信连接请求的发送方的通信信息；

根据所述通信信息判断所述发送方是否为预设的需要开启安全通信模式的通信用户；

当根据所述通信信息判断所述发送方为所述预设的需要开启安全通信模式的通信用户时，开启所述安全通信模式，并在所述安全通信模式下执行所述获取采集到的目标指纹信息。

结合第一方面的实现方式，在第一方面的第二种可能的实现方式中，步骤获取采集到的目标指纹信息，包括：

当检测到在指纹采集区域输入的触控指令时，获取所述触控指令对应的指纹信息，并将所述指纹信息作为所述目标指纹信息，其中，所述指纹采集区域与当检测接收到所述通信连接请求时，终端显示的用于输入指纹信息输入区域不同。

结合第一方面的实现方式，在第一方面的第三种可能的实现方式中，在步骤检测接收到所述通信连接请求之后，所述获取采集到的目标指纹信息之前，还可以包括以下步骤：

获取所述通信连接请求的发送方的目标通信信息；

根据预先存储的通信信息与认证用户的映射关系，确定与所述目标通信信息相匹配的目标认证用户；

其中，所述检测所述目标指纹信息与预设的认证用户对应的指纹信息是否相匹配，包括：

检测所述目标指纹信息与预设的所述目标认证用户对应的指纹信息是否相匹配。

结合第一方面的实现方式、第一方面的第一种可能的实现方式、第一方面的第二种可能的实现方式中以及第一方面的第三种可能的实现方式中的任意一种实现方式，在第一方面的第四种可能的实现方式中，还可以包括以下步骤：

当检测到采集到的 N 个目标指纹信息都匹配失败时，输出报警提示，所述 N 为正整数。

第二方面，本发明实施例还公开了一种用户终端，包括：

第一检测单元，用于检测是否接收到通信连接请求；

第一获取单元，用于当检测接收到所述通信连接请求时，获取采集到的目

标指纹信息;

第二检测单元,用于检测所述目标指纹信息与预设的认证用户对应的指纹信息是否相匹配;

第二获取单元,用于当所述第二检测单元检测到所述目标指纹信息与所述预设的认证用户对应的指纹信息相匹配时,根据预设的指纹信息与响应方式的映射关系,获取与所述目标指纹信息相匹配的响应方式,以所述响应方式响应所述通信连接请求。

结合第二方面的用户终端,在第二方面的第一种可能的用户终端中,所述用户终端还包括:

第三获取单元,用于在所述第一检测单元检测接收到所述通信连接请求时,获取所述通信连接请求的发送方的通信信息;

判断单元,用于根据所述第三获取单元获取的通信信息判断所述发送方是否为预设的需要开启安全通信模式的通信用户;

开启单元,用于当所述判断单元根据所述通信信息判断所述发送方为所述预设的需要开启安全通信模式的通信用户时,开启所述安全通信模式,并触发所述第一获取单元在所述安全通信模式下获取采集到的目标指纹信息。

结合第二方面的用户终端,在第二方面的第二种可能的用户终端中,所述第一获取单元具体用于当检测到在指纹采集区域输入的触控指令时,获取所述触控指令对应的指纹信息,并将所述指纹信息作为所述目标指纹信息,其中,所述指纹采集区域与当检测接收到所述通信连接请求时,终端显示的用于输入指纹信息输入区域不同。

结合第二方面的用户终端,在第二方面的第三种可能的用户终端中,所述用户终端还包括:

第四获取单元,用于在所述第一检测单元检测接收到所述通信连接请求时,获取所述通信连接请求的发送方的目标通信信息;

确定单元,用于根据预先存储的通信信息与认证用户的映射关系,确定与所述目标通信信息相匹配的目标认证用户;

其中,所述第二检测单元具体用于检测所述目标指纹信息与预设的所述目标认证用户对应的指纹信息是否相匹配。

结合第二方面的用户终端、第二方面的第一种可能的用户终端、第二方面

的第二种可能的用户终端以及第二方面的第三种可能的用户终端中的任意一种用户终端，在第二方面的第四种可能的用户终端中，所述用户终端还包括：

输出单元，用于当检测到采集到的 N 个目标指纹信息都匹配失败时，输出报警提示，所述 N 为正整数。

本发明实施例中，当检测接收到通信连接请求时，终端可以获取采集到的目标指纹信息；并检测目标指纹信息与预设的认证用户对应的指纹信息是否相匹配；若检测到目标指纹信息与预设的认证用户对应的指纹信息相匹配时，根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，以该响应方式响应通信连接请求。在本发明实施例中，在检测接收到通信连接请求时，终端会先检测获取到的目标指纹信息与预设的认证用户对应的指纹信息是否相匹配，只有当检测到获取到的目标指纹信息与预设的认证用户对应的指纹信息相匹配时，终端才会根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，并以响应方式响应通信连接请求。由此可见，实施本发明实施例能够提高利用终端通信联系的安全性。

附图说明

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

图 1 是本发明实施例公开的一种通信连接请求的响应方法的流程示意图；

图 2 是本发明实施例公开的另一种通信连接请求的响应方法的流程示意图；

图 3 是本发明实施例公开的一种用户终端的结构示意图；

图 4 是本发明实施例公开的另一种用户终端的结构示意图；

图 5 是本发明实施例公开的又一种用户终端的结构示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳

动前提下所获得的所有其他实施例，都属于本发明保护的范围。

本发明实施例公开了一种通信连接请求的响应方法及用户终端。在本发明实施例中，在检测接收到所述通信连接请求时，终端会先检测获取到的目标指纹信息与预设的认证用户对应的指纹信息是否相匹配，只有当检测到获取到的目标指纹信息与预设的认证用户对应的指纹信息相匹配时，终端才会根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，并以响应方式响应通信连接请求。由此可见，实施本发明实施例能够提高利用终端通信联系的安全性。

请参阅图 1，图 1 是本发明实施例公开的一种通信连接请求的响应方法的流程示意图。其中，图 1 所示的方法可以应用于智能手机（如Android 手机、iOS 手机等）、平板电脑、掌上电脑以及移动互联网设备（Mobile Internet Devices, MID）、PAD 等具有接收通信连接请求功能的用户终端中。如图 1 所示，该通信连接请求的响应方法可以包括以下步骤：

S101、检测是否接收到通信连接请求。

本发明实施例中，该通信连接请求可以包括语音通信连接请求，也可以是视频通信连接请求。

S102、当检测接收到通信连接请求时，获取采集到的目标指纹信息。

本发明实施例中，当检测接收到其他通信用户发送的通信连接请求时，可以在终端显示区域输出用于输入指纹信息的输入区域，当检测到用户在此输入区域输入触控指令时，终端可以获取与该触控指令相对应的指纹信息。

S103、检测目标指纹信息与预设的认证用户对应的指纹信息是否相匹配。

本发明实施例中，可以在终端中预设至少一个认证用户的指纹信息。其中，预设的至少一个认证用户的指纹信息也可以根据需要进行修改。举例来说，当认证用户 A 的指纹信息存储在终端 A 中，但后续该终端 A 转让给其他用户时，则可以在终端 A 中删除与认证用户 A 相对应的指纹信息。又如，当认证用户 A 预设的指纹信息只包括拇指对应的指纹信息，若后续需要，则认证用户 A 也可以将食指对应的指纹信息或者其他手指对应的指纹信息存储在该终端中。本发明不限定。

具体地，当终端获取到指纹信息后，则可以将获取到的指纹信息与预设的认证用户对应的指纹信息进行匹配。

S104、当检测到目标指纹信息与预设的认证用户对应的指纹信息相匹配时，根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，以该响应方式响应通信连接请求。

本发明实施例中，可以在终端中预先设定指纹信息与响应方式的映射关系，该映射关系可以是用户根据需要进行设定，也可以是终端根据用户的历史设定记录进行设定。

本发明实施例中，预设的指纹信息与响应方式的映射关系对于不同的认证用户可以相同，也可以不同。举例来说，认证用户 A 对应的指纹信息与响应方式的映射关系可以包括：拇指指纹信息对应的响应方式为拒绝通信连接请求（则拒绝与该通信连接请求发送方建立通信连接）；食指指纹信息对应的响应方式为同意与该通信连接请求发送方建立通信连接；中指指纹信息对应的响应方式为先拒绝与该通信连接请求发送方建立通信连接，十分钟后再向该发送方发送通信连接请求。而认证用户 B 对应的指纹信息与响应方式的映射关系可以包括：拇指指纹信息对应的响应方式为同意与该通信连接请求发送方建立通信连接；食指指纹信息对应的响应方式为拒绝与该通信连接请求发送方建立通信连接；中指指纹信息对应的响应方式为先拒绝与该通信连接请求发送方建立通信连接，十分钟后再向该发送方发送通信连接请求。

本发明实施例中，当终端根据用户的历史设定记录进行设定指纹信息与响应方式的映射关系时，可以包括以下步骤：

- 11) 获取终端中针对指纹信息与响应方式的映射关系的历史设定记录；
- 12) 根据上述历史设定记录确定用户的设定偏好；
- 13) 根据上述设定偏好设定指纹信息与响应方式的映射关系。

本发明实施例中，针对指纹信息与响应方式的映射关系也可以在设定后进行修改。

本发明实施例中，当终端检测到目标指纹信息与预设的认证用户对应的指纹信息相匹配时，根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，以该响应方式响应通信连接请求。举例来说，当预设的指纹信息与响应方式的映射关系包括：拇指指纹信息对应的响应方式为同意与该通信连接请求发送方建立通信连接；食指指纹信息对应的响应方式为拒绝与该通信连接请求发送方建立通信连接；中指指纹信息对应的响应方式为先

拒绝与该通信连接请求发送方建立通信连接，十分钟后再向该发送方发送通信连接请求。当获取到的目标指纹信息为食指指纹信息时，则拒绝与该通信连接请求发送方建立通信连接。

在图 1 中，当检测接收到通信连接请求时，终端可以获取采集到的目标指纹信息；并检测目标指纹信息与预设的认证用户对应的指纹信息是否相匹配；若检测到目标指纹信息与预设的认证用户对应的指纹信息相匹配时，根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，以该响应方式响应通信连接请求。在本发明实施例中，在检测接收到通信连接请求时，终端会先检测获取到的目标指纹信息与预设的认证用户对应的指纹信息是否相匹配，只有当检测到获取到的目标指纹信息与预设的认证用户对应的指纹信息相匹配时，终端才会根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，并以响应方式响应通信连接请求。由此可见，实施本发明实施例能够提高利用终端通信联系的安全性。

请参阅图 2，图 2 是本发明实施例公开的另一种通信连接请求的响应方法的流程示意图。如图 2 所示，该通信连接请求的响应方法可以包括以下步骤：

S201、检测是否接收到通信连接请求。

S202、当检测接收到通信连接请求时，获取通信连接请求的发送方的目标通信信息。

本发明实施例中，当检测接收到其他通信用户发送的通信连接请求时，可以获取通信连接请求的发送方的目标通信信息。其中，通信连接请求的发送方的目标通信信息可以包括但不限于发送方的账号信息、发送方的昵称信息、发送方的归属地信息以及发送方的当前发送地信息等等。

S203、根据预先存储的通信信息与认证用户的映射关系，确定与目标通信信息相匹配的目标认证用户。

本发明实施例中，可以在终端中预设通信信息与认证用户的映射关系。也即，对于不同的发送方可以设置不同的认证用户，也即，对于同一个发送方，其终端中预设的认证用户的优先级不一样。举例来说，当发送通信连接的发送方 A 与认证用户 A 的关系紧密一点，则可以将认证用户 A 的优先级设置为最高。也即，当通信连接请求是发送方 A 发送的，则终端中默认认证用户 A 为目标认

证用户。

本发明实施例中，对于同一个通信连接请求发送方，与其对应的目标认证用户的数量可以包括至少一个，且针对于至少一个目标认证用户中，每一个目标认证用户的优先级可以相同，也可以不同，本发明不作限定。

具体地，在获取到通信连接请求发送方的通信信息之后，根据预设的通信信息与认证用户的映射关系，确定与目标通信信息相匹配的目标认证用户。

S204、获取采集到的目标指纹信息。

本发明实施例中，采集到的指纹信息主要用于与预设的认证用户对应的指纹信息进行匹配。

作为一种可选的实施方式，在检测接收到通信连接请求之后，获取采集到的目标指纹信息之前，还可以包括以下步骤：

21) 获取通信连接请求的发送方的通信信息；

22) 根据通信信息判断发送方是否为预设的需要开启安全通信模式的通信用户；

23) 当根据通信信息判断发送方为预设的需要开启安全通信模式的通信用户时，开启安全通信模式，并在安全通信模式下执行获取采集到的目标指纹信息。

本发明实施例中，通信信息可以包括但不限于发送方的账号信息、发送方的昵称信息、发送方的归属地信息以及发送方的当前发送地信息等等。

本发明实施例中，安全通信模式包括在接收到通信连接请求时，会通过采集目标指纹信息，并将目标指纹信息与预先存储的认证用户对应的指纹信息进行匹配，只有匹配成功，方可对该通信连接请求进行响应的模式。

本发明实施例中，可以在终端中预先设置需要开启安全通信模式的通信用户，也即，对于部分通信用户只有某一个认证用户的指纹信息可以匹配成功，而对于部分通信用户有至少一个通信用户可以匹配成功。

本发明实施例中，预先设置需要开启安全通信模式的通信用户可以是用户根据需要进行设定，也可以是终端根据用户的历史设定记录进行设定，还可以是终端中默认某些通信用户群组为需要开启安全通信模式的通信用户，也即，对于该群组中的每一个通信用户均为需要开启安全通信模式的通信用户。

本发明实施例中，当终端根据用户的历史设定记录进行设定需要开启安全

通信模式的通信用户时，可以包括以下步骤：

- 31) 获取终端中针对，需要开启安全通信模式的通信用户的历史设定记录；
- 32) 根据上述历史设定记录确定通信用户的类型；
- 33) 根据上述类型设定需要开启安全通信模式的通信用户。

本发明实施例中，通信用户的类型可以包括好友类型、亲人类型、同事类型以及同学类型等等。

本发明实施例中，在确定是否将某一通信用户设置成需要开启安全通信模式的通信用户时，可以先确定该通信用户的类型，在检测该类型中的通信用户是否均需要设置成需要开启安全通信模式的通信用户，若是，则将该通信用户设置成需要开启安全通信模式的通信用户；若否，则无需将该用户设置成需要开启安全通信模式的通信用户。举例来说，当接收到通信连接请求的发送方为通信用户 A，其中，终端检测到通信用户 A 的类型为同事类型。当预设的同事类型的通信用户均设置为需要开启安全通信模式的通信用户，则终端可以将通信用户 A 设置为需要开启安全通信模式的通信用户。

作为一种可选的实施方式，步骤获取采集到的目标指纹信息可以具体包括：当检测到在指纹采集区域输入的触控指令时，获取触控指令对应的指纹信息，并将指纹信息作为目标指纹信息。

本发明实施例中，指纹采集区域与当检测接收到通信连接请求时，终端显示的用于输入指纹信息输入区域不同。也即，在终端显示区域的任意一个地方均可作为指纹信息采集区域。具体地，当检测到用户输入触控指令时，确定该触控指令对应的位置信息，根据该位置信息确定指纹信息采集区域。

S205、检测目标指纹信息与预设的目标认证用户对应的指纹信息是否相匹配。

S206、当检测到目标指纹信息与预设的目标认证用户对应的指纹信息匹配时，根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，以该响应方式响应通信连接请求。

本发明实施例中，预设的指纹信息与响应方式的映射关系对于不同的认证用户可以相同，也可以不同。举例来说，认证用户 A 对应的指纹信息与响应方式的映射关系可以包括：拇指指纹信息对应的响应方式为拒绝通信连接请求（则拒绝与该通信连接请求发送方建立通信连接）；食指指纹信息对应的响应方

式为同意与该通信连接请求发送方建立通信连接；中指指纹信息对应的响应方式为先拒绝与该通信连接请求发送方建立通信连接，十分钟后再向该发送方发送通信连接请求。而认证用户 B 对应的指纹信息与响应方式的映射关系可以包括：拇指指纹信息对应的响应方式为同意与该通信连接请求发送方建立通信连接；食指指纹信息对应的响应方式为拒绝与该通信连接请求发送方建立通信连接；中指指纹信息对应的响应方式为先拒绝与该通信连接请求发送方建立通信连接，十分钟后再向该发送方发送通信连接请求。

本发明实施例中，当终端检测到目标指纹信息与预设的认证用户对应的指纹信息相匹配时，根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，以该响应方式响应通信连接请求。举例来说，当预设的指纹信息与响应方式的映射关系包括：拇指指纹信息对应的响应方式为同意与该通信连接请求发送方建立通信连接；食指指纹信息对应的响应方式为拒绝与该通信连接请求发送方建立通信连接；中指指纹信息对应的响应方式为先拒绝与该通信连接请求发送方建立通信连接，十分钟后再向该发送方发送通信连接请求。当获取到的目标指纹信息为食指指纹信息时，则拒绝与该通信连接请求发送方建立通信连接。

在图 2 中，详细描述了终端根据通信连接请求的发送方的信息确定目标认证用户，且对于不同一个发送方，对应的认证用户的优先级不相同，由此可见，实施本发明实施例，可以进一步提高利用终端通信联系的安全性。

请参阅图 3，图 3 是本发明实施例公开的一种用户终端的结构示意图，用于执行上述通信连接请求的响应方法。其中，图 3 所示的用户终端可以包括但不限于智能手机（如 Android 手机、iOS 手机等）、平板电脑、掌上电脑以及移动互联网设备（Mobile Internet Devices, MID）、PAD 等具有接收通信连接请求功能的用户终端。如图 3 所示，该用户终端可以包括：第一检测单元 301、第一获取单元 302、第二检测单元 303 以及第二获取单元 304，其中，

第一检测单元 301，用于检测是否接收到通信连接请求。

本发明实施例中，该通信连接请求可以包括语音通信连接请求，也可以是视频通信连接请求。

第一获取单元 302，用于当第一检测单元 301 检测接收到通信连接请求时，

获取采集到的目标指纹信息。

本发明实施例中，当检测接收到其他通信用户发送的通信连接请求时，可以在终端显示区域输出用于输入指纹信息的输入区域，当检测到用户在此输入区域输入触控指令时，终端可以获取与该触控指令相对应的指纹信息。

第二检测单元 303，用于检测目标指纹信息与预设的认证用户对应的指纹信息是否相匹配。

本发明实施例中，可以在终端中预设至少一个认证用户的指纹信息。其中，预设的至少一个认证用户的指纹信息也可以根据需要进行修改。举例来说，当认证用户 A 的指纹信息存储在终端 A 中，但后续该终端 A 转让给其他用户时，则可以在终端 A 中删除与认证用户 A 相对应的指纹信息。又如，当认证用户 A 预设的指纹信息只包括拇指对应的指纹信息，若后续需要，则认证用户 A 也可以将食指对应的指纹信息或者其他手指对应的指纹信息存储在该终端中。本发明不作限定。

具体地，当第一获取单元 302 获取到指纹信息后，则第二检测单元 303 可以将获取到的指纹信息与预设的认证用户对应的指纹信息进行匹配。

第二获取单元 304，用于当第二检测单元 303 检测到目标指纹信息与预设的认证用户对应的指纹信息相匹配时，根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，以该响应方式响应通信连接请求。

本发明实施例中，可以在终端中预先设定指纹信息与响应方式的映射关系，该映射关系可以是用户根据需要进行设定，也可以是终端根据用户的历史设定记录进行设定。

本发明实施例中，预设的指纹信息与响应方式的映射关系对于不同的认证用户可以相同，也可以不同。举例来说，认证用户 A 对应的指纹信息与响应方式的映射关系可以包括：拇指指纹信息对应的响应方式为拒绝通信连接请求（则拒绝与该通信连接请求发送方建立通信连接）；食指指纹信息对应的响应方式为同意与该通信连接请求发送方建立通信连接；中指指纹信息对应的响应方式为先拒绝与该通信连接请求发送方建立通信连接，十分钟后向该发送方发送通信连接请求。而认证用户 B 对应的指纹信息与响应方式的映射关系可以包括：拇指指纹信息对应的响应方式为同意与该通信连接请求发送方建立通信连接；食指指纹信息对应的响应方式为拒绝与该通信连接请求发送方建立通信连

接；中指指纹信息对应的响应方式为先拒绝与该通信连接请求发送方建立通信连接，十分钟后再向该发送方发送通信连接请求。

本发明实施例中，当根据用户的历史设定记录进行设定指纹信息与响应方式的映射关系时，可以包括以下步骤：

- 11) 获取终端中针对指纹信息与响应方式的映射关系的历史设定记录；
- 12) 根据上述历史设定记录确定用户的设定偏好；
- 13) 根据上述设定偏好设定指纹信息与响应方式的映射关系。

本发明实施例中，针对指纹信息与响应方式的映射关系也可以在设定后进行修改。

本发明实施例中，当第二检测单元 303 检测到目标指纹信息与预设的认证用户对应的指纹信息相匹配时，第二获取单元 304 根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，以该响应方式响应通信连接请求。举例来说，当预设的指纹信息与响应方式的映射关系包括：拇指指纹信息对应的响应方式为同意与该通信连接请求发送方建立通信连接；食指指纹信息对应的响应方式为拒绝与该通信连接请求发送方建立通信连接；中指指纹信息对应的响应方式为先拒绝与该通信连接请求发送方建立通信连接，十分钟后再向该发送方发送通信连接请求。当第一获取单元 302 获取到的目标指纹信息为食指指纹信息时，则拒绝与该通信连接请求发送方建立通信连接。

在图 3 中，当第一检测单元 301 检测接收到通信连接请求时，第一获取单元 302 可以获取采集到的目标指纹信息；第二检测单元 303 并检测目标指纹信息与预设的认证用户对应的指纹信息是否相匹配；若第二检测单元 303 检测到目标指纹信息与预设的认证用户对应的指纹信息相匹配时，第二获取单元 304 根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，以该响应方式响应通信连接请求。在本发明实施例中，在第一检测单元 301 检测接收到通信连接请求时，第二检测单元 303 会先检测获取到的目标指纹信息与预设的认证用户对应的指纹信息是否相匹配，只有当第二检测单元 303 检测到获取到的目标指纹信息与预设的认证用户对应的指纹信息相匹配时，第二获取单元 304 才会根据预设的指纹信息与响应方式的映射关系，获取与目标指纹信息相匹配的响应方式，并以响应方式响应通信连接请求。由此可见，实施本发明实施例能够提高利用终端通信联系的安全性。

请参阅图 4，图 4 是本发明实施例公开的另一种用户终端的结构示意图，用于执行上述通信连接请求的响应方法。其中，图 4 是在图 3 的基础上进一步细化得到，除包括图 3 所示的所有单元外，还可以包括：第三获取单元 305、判断单元 306、开启单元 307、第四获取单元 308、确定单元 309 以及输出单元 310，其中，

第三获取单元 305，用于在 301 第一检测单元检测接收到通信连接请求时，获取通信连接请求的发送方的通信信息。

判断单元 306，用于根据第三获取单元 305 获取的通信信息判断发送方是否为预设的需要开启安全通信模式的通信用户。

开启单元 307，用于当判断单元 306 根据通信信息判断发送方为预设的需要开启安全通信模式的通信用户时，开启安全通信模式，并触发第一获取单元 302 在安全通信模式下获取采集到的目标指纹信息。

本发明实施例中，通信信息可以包括但不限于发送方的账号信息、发送方的昵称信息、发送方的归属地信息以及发送方的当前发送地信息等等。

本发明实施例中，安全通信模式包括在接收到通信连接请求时，会通过采集目标指纹信息，并将目标指纹信息与预先存储的认证用户对应的指纹信息进行匹配，只有匹配成功，方可对该通信连接请求进行响应的模式。

本发明实施例中，可以在终端中预先设置需要开启安全通信模式的通信用户，也即，对于部分通信用户只有某一个认证用户的指纹信息可以匹配成功，而对于部分通信用户有至少一个通信用户可以匹配成功。

本发明实施例中，预先设置需要开启安全通信模式的通信用户可以是用户根据需要进行设定，也可以是终端根据用户的历史设定记录进行设定，还可以是终端中默认某些通信用户群组为需要开启安全通信模式的通信用户，也即，对于该群组中的每一个通信用户均为需要开启安全通信模式的通信用户。

本发明实施例中，当根据用户的历史设定记录进行设定需要开启安全通信模式的通信用户时，可以包括以下步骤：

- 31) 获取终端中针对，需要开启安全通信模式的通信用户的历史设定记录；
- 32) 根据上述历史设定记录确定通信用户的类型；
- 33) 根据上述类型设定需要开启安全通信模式的通信用户。

本发明实施例中，通信用户的类型可以包括好友类型、亲人类型、同事类型以及同学类型等等。

本发明实施例中，在确定是否将某一通信用户设置成需要开启安全通信模式的通信用户时，可以先确定该通信用户的类型，在检测该类型中的通信用户是否均需要设置成需要开启安全通信模式的通信用户，若是，则将该通信用户设置成需要开启安全通信模式的通信用户；若否，则无需将该用户设置成需要开启安全通信模式的通信用户。举例来说，当接收到通信连接请求的发送方为通信用户 A，其中，终端检测到通信用户 A 的类型为同事类型。当预设的同事类型的通信用户均设置为需要开启安全通信模式的通信用户，则终端可以将通信用户 A 设置为需要开启安全通信模式的通信用户。

作为一种可选的实施方式，步骤获取采集到的目标指纹信息可以具体包括：当检测到在指纹采集区域输入的触控指令时，获取触控指令对应的指纹信息，并将指纹信息作为目标指纹信息。

本发明实施例中，指纹采集区域与当检测接收到通信连接请求时，终端显示的用于输入指纹信息输入区域不同。也即，在终端显示区域的任意一个地方均可作为指纹信息采集区域。具体地，当检测到用户输入触控指令时，确定该触控指令对应的位置信息，根据该位置信息确定指纹信息采集区域。

第四获取单元 308，用于在第一检测单元 301 检测接收到通信连接请求时，获取通信连接请求的发送方的目标通信信息。

确定单元 309，用于根据预先存储的通信信息与认证用户的映射关系，确定与目标通信信息相匹配的目标认证用户。

本发明实施例中，当第一检测单元 301 检测接收到其他通信用户发送的通信连接请求时，第四获取单元 308 可以获取通信连接请求的发送方的目标通信信息。其中，通信连接请求的发送方的目标通信信息可以包括但不限于发送方的账号信息、发送方的昵称信息、发送方的归属地信息以及发送方的当前发送地信息等等。

本发明实施例中，可以在终端中预设通信信息与认证用户的映射关系。也即，对于不同的发送方可以设置不同的认证用户，也即，对于同一个发送方，其终端中预设的认证用户的优先级不一样。举例来说，当发送通信连接的发送方 A 与认证用户 A 的关系紧密一点，则可以将认证用户 A 的优先级设置为最高。

也即，当通信连接请求是发送方 A 发送的，则终端中默认认证用户 A 为目标认证用户。

本发明实施例中，对于同一个通信连接请求发送方，与其对应的目标认证用户的数量可以包括至少一个，且针对于至少一个目标认证用户中，每一个目标认证用户的优先级可以相同，也可以不同，本发明不作限定。

具体地，在获取到通信连接请求发送方的通信信息之后，根据预设的通信信息与认证用户的映射关系，确定与目标通信信息相匹配的目标认证用户。

其中，第二检测单元 303 具体用于检测目标指纹信息与预设的目标认证用户对应的指纹信息是否相匹配。

输出单元 310，用于当检测到采集到的 N 个目标指纹信息都匹配失败时，输出报警提示，N 为正整数，例如，N 为 1、7、23 等。

本发明实施例中，当第三检测单元检测到采集到的 N 个目标指纹信息都匹配失败时，输出单元 310 可以输出报警提示。

在图 4 中，详细描述了根据通信连接请求的发送方的信息确定目标认证用户，且对于不同一个发送方，对应的认证用户的优先级不相同，由此可见，实施本发明实施例，可以进一步提高利用终端通信联系的安全性。

请参阅图 5，图 5 是本发明实施例公开的又一种用户终端的结构示意图，用于执行上述通信连接请求的响应方法。如图 5 所示，该终端 500 可以包括：至少一个处理器 501，至少一个输入装置 502，至少一个输出装置 503，存储器 505 等组件。其中，这些组件通过一条或多条总线 504 进行通信连接。本领域技术人员可以理解，图 5 中示出的终端的结构并不构成对本发明实施例的限定，它既可以是总线形结构，也可以是星型结构，还可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。其中：

处理器 501 为终端的控制中心，利用各种接口和线路连接整个终端的各个部分，通过运行或执行存储在存储器 505 内的程序和/或模块，以及调用存储在存储器 505 内的数据，以执行终端的各种功能和处理数据。处理器 501 可以由集成电路(Integrated Circuit, 简称 IC) 组成，例如可以由单颗封装的 IC 所组成，也可以由连接多颗相同功能或不同功能的封装 IC 而组成。举例来说，处理器 501 可以仅包括中央处理器(Central Processing Unit, 简称 CPU)，也可以是 CPU、数

字信号处理器(digital signal processor, 简称 DSP)、图形处理器(Graphic Processing Unit, 简称 GPU)及各种控制芯片的组合。在本发明实施方式中, CPU 可以是单运算核心, 也可以包括多运算核心。

输入装置 502 可以包括标准的触摸屏、键盘等, 也可以包括有线接口、无线接口等。

输出装置 503 可以包括显示屏、扬声器等, 也可以包括有线接口、无线接口等。

存储器 505 可用于存储软件程序以及模块, 处理器 501、输入装置 502 以及输出装置 503 通过调用存储在存储器 505 中的软件程序以及模块, 从而执行终端的各项功能应用以及实现数据处理。存储器 505 主要包括程序存储区和数据存储区, 其中, 程序存储区可存储操作系统、至少一个功能所需的应用程序等; 数据存储区可存储根据终端的使用所创建的数据等。在本发明实施例中, 操作系统可以是 Android 系统、iOS 系统或 Windows 操作系统等等。

具体的, 处理器 501 调用存储在存储器 505 中的应用程序, 用于执行以下操作:

处理器 501 检测是否接收到通信连接请求;

当处理器 501 检测接收到通信连接请求时, 处理器 501 获取采集到的目标指纹信息;

处理器 501 检测目标指纹信息与预设的认证用户对应的指纹信息是否相匹配;

当处理器 501 检测到目标指纹信息与预设的认证用户对应的指纹信息相匹配时, 处理器 501 根据预设的指纹信息与响应方式的映射关系, 获取与目标指纹信息相匹配的响应方式, 以该响应方式响应通信连接请求。

本发明实施例中, 处理器 501 调用存储在存储器 505 中的应用程序, 在执行步骤检测接收到通信连接请求之后, 步骤获取采集到的目标指纹信息之前, 还可以执行以下步骤:

处理器 501 获取通信连接请求的发送方的通信信息;

处理器 501 根据通信信息判断发送方是否为预设的需要开启安全通信模式的通信用户;

当处理器 501 根据通信信息判断发送方为预设的需要开启安全通信模式的

通信用户时，开启安全通信模式，并在安全通信模式下执行获取采集到的目标指纹信息。

本发明实施例中，处理器 501 调用存储在存储器 505 中的应用程序，执行步骤获取采集到的目标指纹信息，主要包括：

当处理器 501 检测到在指纹采集区域输入的触控指令时，获取触控指令对应的指纹信息，并将指纹信息作为目标指纹信息，其中，指纹采集区域与当检测接收到通信连接请求时，终端显示的用于输入指纹信息输入区域不同。

本发明实施例中，处理器 501 调用存储在存储器 505 中的应用程序，在执行步骤检测接收到通信连接请求之后，步骤获取采集到的目标指纹信息之前，还可以执行以下步骤：

处理器 501 获取通信连接请求的发送方的目标通信信息；

处理器 501 根据预先存储的通信信息与认证用户的映射关系，确定与目标通信信息相匹配的目标认证用户；

其中，处理器 501 检测目标指纹信息与预设的认证用户对应的指纹信息是否相匹配，包括：

处理器 501 检测目标指纹信息与预设的目标认证用户对应的指纹信息是否相匹配。

本发明实施例中，处理器 501 调用存储在存储器 505 中的应用程序，还用于执行以下步骤：

当处理器 501 检测到采集到的 N 个目标指纹信息都匹配失败时，处理器 501 控制输出装置 503 输出报警提示。

具体的，本发明实施例中介绍的终端可以实施本发明结合图1、图2介绍的通信连接请求的响应方法实施例中的部分或全部流程。

本发明所有实施例中的模块或子模块，可以通过通用集成电路，例如CPU（Central Processing Unit，中央处理器），或通过ASIC（Application Specific Integrated Circuit，专用集成电路）来实现。

本发明实施例方法中的步骤可以根据实际需要进行顺序调整、合并和删减。

本发明实施例终端中的单元可以根据实际需要进行合并、划分和删减。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算

机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory, ROM）或随机存取存储器（Random Access Memory, 简称 RAM）等。

以上所揭露的仅为本发明较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

权 利 要 求 书

1、一种通信连接请求的响应方法，其特征在于，包括：

检测是否接收到通信连接请求；

当检测接收到所述通信连接请求时，获取采集到的目标指纹信息；

检测所述目标指纹信息与预设的认证用户对应的指纹信息是否相匹配；

当检测到所述目标指纹信息与所述预设的认证用户对应的指纹信息相匹配时，根据预设的指纹信息与响应方式的映射关系，获取与所述目标指纹信息相匹配的响应方式，以所述响应方式响应所述通信连接请求。

2、根据权利要求 1 所述的方法，其特征在于，在检测接收到所述通信连接请求之后，所述获取采集到的目标指纹信息之前，所述方法还包括：

获取所述通信连接请求的发送方的通信信息；

根据所述通信信息判断所述发送方是否为预设的需要开启安全通信模式的通信用户；

当根据所述通信信息判断所述发送方为所述预设的需要开启安全通信模式的通信用户时，开启所述安全通信模式，并在所述安全通信模式下执行所述获取采集到的目标指纹信息。

3、根据权利要求 1 所述的方法，其特征在于，所述获取采集到的目标指纹信息，包括：

当检测到在指纹采集区域输入的触控指令时，获取所述触控指令对应的指纹信息，并将所述指纹信息作为所述目标指纹信息，其中，所述指纹采集区域与当检测接收到所述通信连接请求时，终端显示的用于输入指纹信息输入区域不同。

4、根据权利要求 1 所述的方法，其特征在于，在检测接收到所述通信连接请求之后，所述获取采集到的目标指纹信息之前，所述方法还包括：

获取所述通信连接请求的发送方的目标通信信息；

根据预先存储的通信信息与认证用户的映射关系，确定与所述目标通信信

息相匹配的目标认证用户；

其中，所述检测所述目标指纹信息与预设的认证用户对应的指纹信息是否相匹配，包括：

检测所述目标指纹信息与预设的所述目标认证用户对应的指纹信息是否相匹配。

5、根据权利要求 1~4 中任意一项所述的方法，其特征在于，所述方法还包括：

当检测到采集到的 N 个目标指纹信息都匹配失败时，输出报警提示，所述 N 为正整数。

6、一种用户终端，其特征在于，包括：

第一检测单元，用于检测是否接收到通信连接请求；

第一获取单元，用于当所述第一检测单元检测接收到所述通信连接请求时，获取采集到的目标指纹信息；

第二检测单元，用于检测所述目标指纹信息与预设的认证用户对应的指纹信息是否相匹配；

第二获取单元，用于当所述第二检测单元检测到所述目标指纹信息与所述预设的认证用户对应的指纹信息相匹配时，根据预设的指纹信息与响应方式的映射关系，获取与所述目标指纹信息相匹配的响应方式，以所述响应方式响应所述通信连接请求。

7、根据权利要求 6 所述的用户终端，其特征在于，所述用户终端还包括：

第三获取单元，用于在所述第一检测单元检测接收到所述通信连接请求时，获取所述通信连接请求的发送方的通信信息；

判断单元，用于根据所述第三获取单元获取的通信信息判断所述发送方是否为预设的需要开启安全通信模式的通信用户；

开启单元，用于当所述判断单元根据所述通信信息判断所述发送方为所述预设的需要开启安全通信模式的通信用户时，开启所述安全通信模式，并触发所述第一获取单元在所述安全通信模式下获取采集到的目标指纹信息。

8、根据权利要求 6 所述的用户终端，其特征在于，所述第一获取单元具体用于当检测到在指纹采集区域输入的触控指令时，获取所述触控指令对应的指纹信息，并将所述指纹信息作为所述目标指纹信息，其中，所述指纹采集区域与当检测接收到所述通信连接请求时，终端显示的用于输入指纹信息输入区域不同。

9、根据权利要求 6 所述的用户终端，其特征在于，所述用户终端还包括：

第四获取单元，用于在所述第一检测单元检测接收到所述通信连接请求时，获取所述通信连接请求的发送方的目标通信信息；

确定单元，用于根据预先存储的通信信息与认证用户的映射关系，确定与所述目标通信信息相匹配的目标认证用户；

其中，所述第二检测单元具体用于检测所述目标指纹信息与预设的所述目标认证用户对应的指纹信息是否相匹配。

10、根据权利要求 6~9 中任意一项所述的用户终端，其特征在于，所述用户终端还包括：

输出单元，用于当检测到采集到的 N 个目标指纹信息都匹配失败时，输出报警提示，所述 N 为正整数。

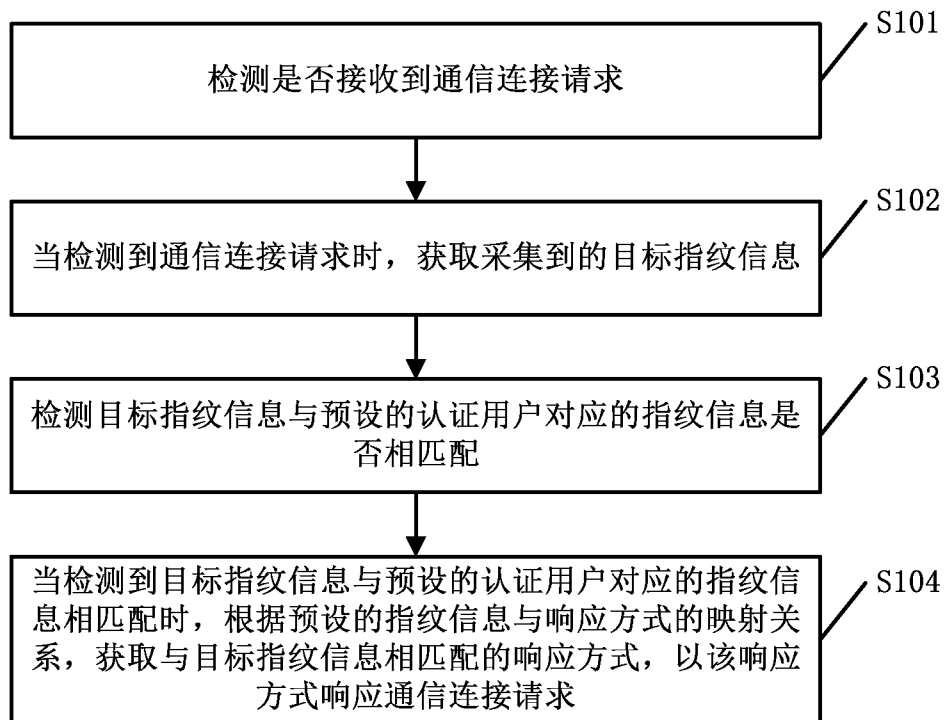


图 1

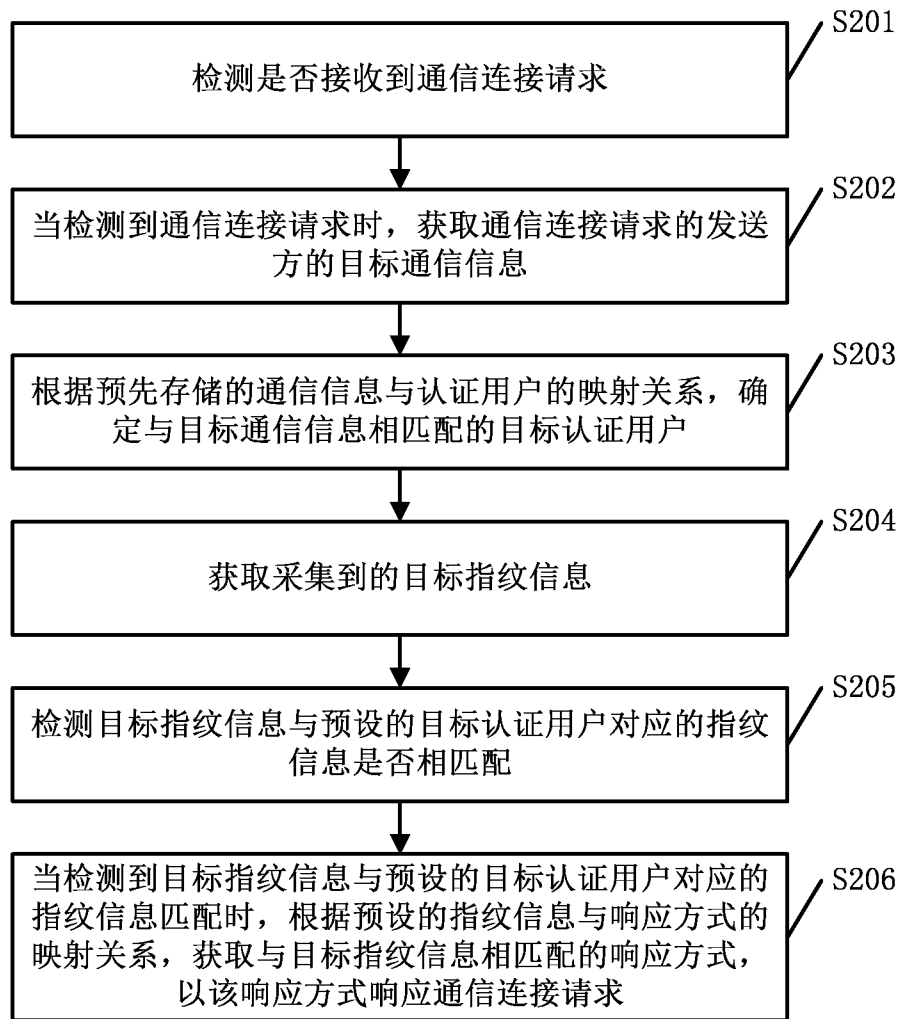


图 2

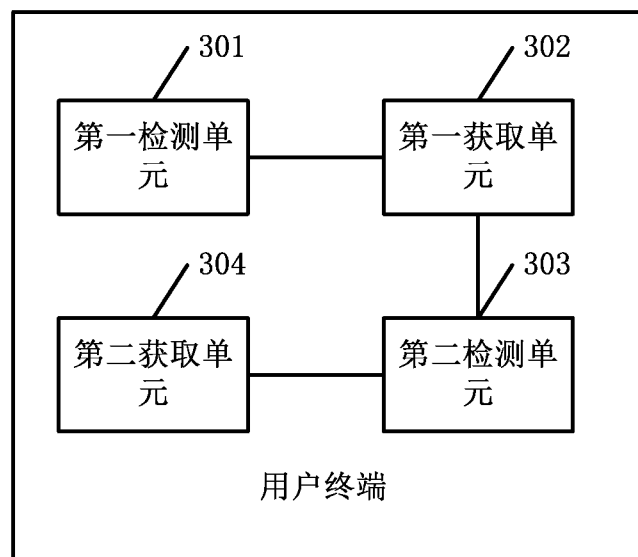


图 3

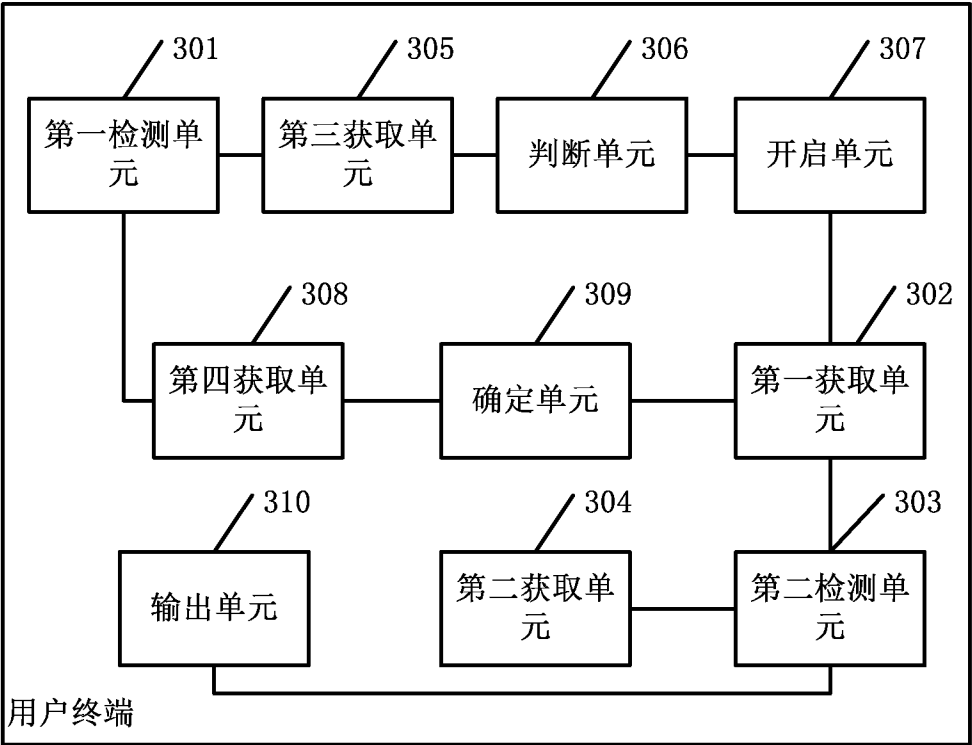


图 4

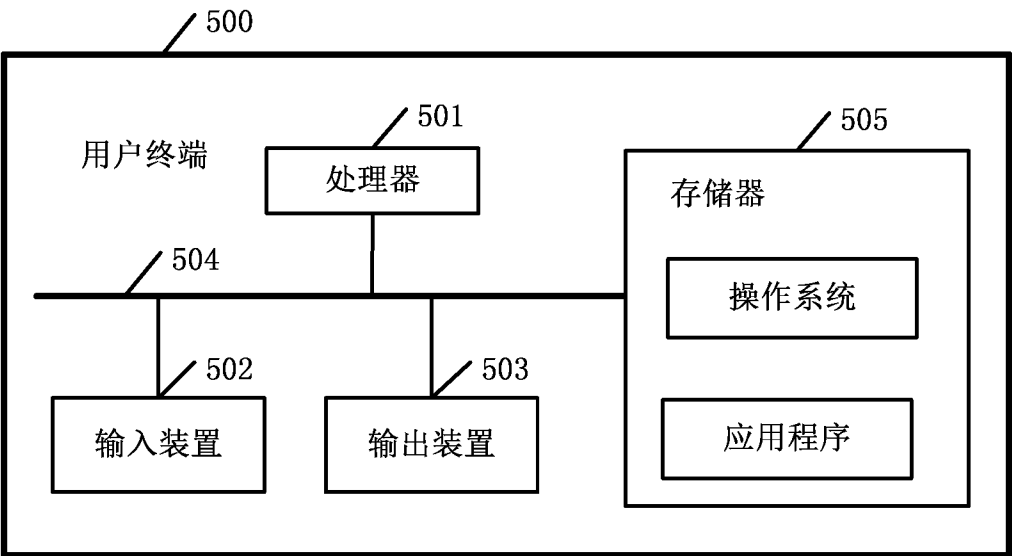


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/091338

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W H04L

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

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

USTXT; CNTXT; CNABS; DWPI; CNKI, SIPOABS: fingerprint, communicat+, link, response, match+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104618905 A (GUANG DONG OPPO MOBILE TELECOMMUNICATIONS CO., LTD.), 13 May 2015 (13.05.2015), claims 1-9, description, paragraphs [0019]-[0065], and figures 1-5	1, 5, 6, 10
A	US 2015205367 A1 (BANDT, H.B.D.), 23 July 2015 (23.07.2015), the whole document	1-10
A	US 2012116918 A1 (ANDERSSON, J. et al.), 10 May 2012 (10.05.2012), the whole document	1-10
A	CN 204392264 U (SHANGHAI PEOPLE NETNETWORK SECURITY TECHNOLOGY CO., LTD.), 10 June 2015 (10.06.2015), the whole document	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

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

Date of the actual completion of the international search 13 April 2016 (13.04.2016)	Date of mailing of the international search report 27 April 2016 (27.04.2016)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer ZHANG, Xiaohui Telephone No.: (86-10) 62411321

International application No.
PCT/CN2015/091338

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类		
H04W 12/06 (2009.01) i		
按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域		
检索的最低限度文献 (标明分类系统和分类号)		
H04W H04L		
包含在检索领域中的除最低限度文献以外的检索文献		
在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用))		
USTXT; CNTXT; CNABS; DWPI; CNKI, SIPOABS: 指纹, 通讯, 连接, 响应, 匹配; fingerprint, communicat+, link, response, match+		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 104618905 A (广东欧铂移动通信有限公司) 2015年 5月 13日 (2015 - 05 - 13) 权利要求1-9, 说明书第[0019]-[0065]段, 图1-5	1, 5, 6, 10
A	US 2015205367 A1 (BANDT-HORN BENJAMIN D) 2015年 7月 23日 (2015 - 07 - 23) 全文	1-10
A	US 2012116918 A1 (ANDERSSON JONAS等) 2012年 5月 10日 (2012 - 05 - 10) 全文	1-10
A	CN 204392264 U (上海众人网络安全技术有限公司) 2015年 6月 10日 (2015 - 06 - 10) 全文	1-10
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期		国际检索报告邮寄日期
2016年 4月 13日		2016年 4月 27日
ISA/CN的名称和邮寄地址		授权官员
中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		张晓辉 电话号码 (86-10) 62411321

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/091338

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104618905	A	2015年 5月 13日	无			
US	2015205367	A1	2015年 7月 23日	US	9007302	B1	2015年 4月 14日
US	2012116918	A1	2012年 5月 10日	EP	2453400	A1	2012年 5月 16日
CN	204392264	U	2015年 6月 10日	无			