

(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
2015 年 6 月 18 日 (18.06.2015)



(10) 国际公布号
WO 2015/085941 A1

- (51) 国际专利分类号:
H04W 8/22 (2009.01)
- (21) 国际申请号: PCT/CN2014/093637
- (22) 国际申请日: 2014 年 12 月 11 日 (11.12.2014)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201310685113.5 2013 年 12 月 13 日 (13.12.2013) CN
201310685287.1 2013 年 12 月 13 日 (13.12.2013) CN
201310687600.5 2013 年 12 月 13 日 (13.12.2013) CN
- (71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。奇智软件 (北京) 有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED) [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。
- (72) 发明人: 闫学松 (YAN, XueSong); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。谭云宇 (TAN, YunYu); 中国北京市朝阳区酒仙桥路 6

号院 2 号楼, Beijing 100015 (CN)。黄铮 (HUANG, Zheng); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。姜燕北 (JIANG, YanBei); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。范国峰 (FAN, GuoFeng); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。李彬 (LI, Bin); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: 北京智汇东方知识产权代理事务所 (普通合伙) (WISEAST INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区成府路 28 号优盛大厦 D 座-1111 室, Beijing 100083 (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。

[见续页]

(54) Title: METHOD AND DEVICE FOR PROCESSING STOLEN TERMINAL

(54) 发明名称: 被盗终端的处理方法及设备

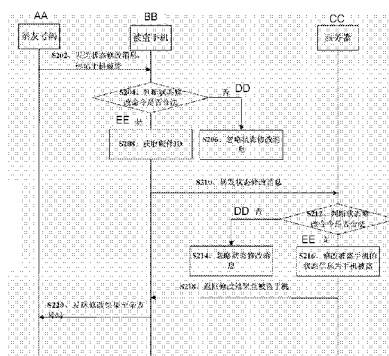


图 2 / FIG 2

S202 Send a status modification message for marking that the mobile phone is stolen
S204 Determine whether the status modification command is valid
S206 Acquire a hardware ID
S210 Forward the status modification message
S212 Determine whether the status modification command is valid
S214 Ignore the status modification message
S216 Modify the status information of the stolen mobile phone to be that the mobile phone is stolen
S216 Return a modification result to the stolen mobile phone
S220 Send the modification result to a phone number of a relative/friend
AA Phone number of relative/friend
BB Stolen mobile phone
CC Server
DD No
EE Yes

(57) Abstract: The present invention provides multiple methods and devices for processing a stolen terminal. A method for processing a stolen terminal comprises: receiving a status modification message from a sending party, the status modification message carrying the current status of the terminal; in a case where the status modification message is valid, forwarding the status modification message to a sever, so that the server modifies, according to the status modification message, status information of the terminal stored in the server to the current status. By means of the embodiments of the present invention, the status information of the terminal can be modified, solving the problem that the prior art cannot provide other identifications to indicate whether the terminal is stolen, increasing the probability of recovering the stolen terminal, and effectively reducing the theft.

(57) 摘要: 本发明提供了多种被盗终端的处理方法及设备。其中, 一种被盗终端的处理方法包括: 接收来自发送方的状态修改消息, 其中, 状态修改消息中携带有本终端的当前状态; 在状态修改消息合法的情况下, 将状态修改消息转发至服务器, 由服务器根据状态修改消息将服务器中存储的本终端的状态信息修改为当前状态。采用本发明实施例能够修改终端的状态信息, 解决了现有技术中无法提供其他标识说明终端是否被盗的问题, 能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

WO 2015/085941 A1



(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))。

被盗终端的处理方法及设备

技术领域

本发明涉及互联网应用领域，特别是涉及被盗终端的处理方法及设备。

5

背景技术

随着智能终端和网络的飞速发展，终端（包括电脑、手机、平板等多种设备）在人们生活中扮演的角色也越来越重要，越来越成为人们工作和生活中不可或缺的全方位“助手”。为方便使用，人们在使用终端的应用时通常会将各种账号信息、私人聊天记录以及图片照片等信息直接存储在终端。因此，若终端丢失，不仅会给用户带来财产损失，更为重要的是用户存储于终端内的私人信息，例如账号密码等财务信息。这些私人信息若被泄露，对用户造成的损失难以估计。因此，终端的防盗十分重要。

现有技术中，当终端丢失之后，失主仅能通过报警的手段说明终端被盗，无法提供其他标识说明终端被盗。但通过报警的手段说明终端被盗，仅仅失主以及警察等小范围人群能够知道终端被盗。大部分人，尤其是当偷盗者对被盗终端进行买卖交易时，购买被盗终端的人无法识别终端是否被盗。这种技术缺陷导致用户容易购买到被盗终端，进一步促进偷盗终端的不法行为的发生的恶劣后果。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的被盗终端的处理方法以及相应的设备。

依据本发明的一个方面，提供了一种被盗终端的处理方法，包括：接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有本终端的当前状态；在所述状态修改消息合法的情况下，将所述状态修改消息转发至服务器，由所述服务器根据所述状态修改消息将所述服务器中存储的本终端的状态信息修改为所述当前状态。

本发明还提供了一种被盗终端的处理客户端，包括：接收器，配置为接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有终端的当前状态；合法判断器，配置为判断所述状态修改消息是否合法；发送器，配置为在所述状态修改消息合法的情况下，将所述状态修改消息转发至服务器，由所述服务器根据所述状态修改消息将所述服务器中存储的所述终端的状态信息修改为所述当前状态。

本发明还提供了一种服务器，包括：命令接收器，配置为接收终端发送的状态修改消息，其中，所述状态修改消息中携带有所述终端的当前状态以及所述终端的身份标识信息；状态修改器，配置为根据所述状态修改消息将本服务器中存储的所述终端的状态信息修改为所述当前状态。

根据本发明实施例，接收来自发送方的状态修改消息之后，对状态修改消息进行合法性验证，保证收到的状态修改消息是真实有效可信的命令，避免接收来自不可信或恶意的发送方发送的状态修改指令，导致终端的状态信息被恶意修改。若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。在状态修改消息合法的情况下，本发明实施例提供的方法将状态修改消息转发至服务器，由服务器根据状态修改消息将服务器中存储的本终端的状态信息修改为当前状态，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如，当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

依据本发明的另一个方面，提供了另一种被盗终端的处理方法，包括：接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有状态发生改变的终端的身份标识信息；将所述状态修改消息转发至所述终端的身份标识信息对应的终端，由所述终端对其进行验证；根据所述终端验证所述状态修改消息通过时返回的状态修改请求，对所述终端的状态信息进行修改。

本发明还提供了一种服务器，包括：接收器，配置为接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有状态发生改变的终端的身份标识信息；发送器，配置为将所述状态修改消息转发至所述终端的身份标识信息对应的终端，由所述终端对其进行验证；状态修改器，配置为根据所述终端验证所述状态修改消息通过时返回的状态修改请求，对所述终端的状态信息进行修改。

本发明还提供了一种被盗终端的处理客户端，包括：消息接收器，配置为接收服务器转发的、来自发送方的状态修改消息；验证器，配置为对接收到的状态修改消息进行验证；请求发送器，配置为所述状态修改消息通过验证之后，返回状态修改请求至所述服务器，由所述服务器根据所述状态修改请求对终端的状态进行修改。

根据本发明实施例，接收来自发送方的状态修改消息，并将其转发至对应的终端，由终端对该状态修改消息进行验证，保证收到的状态修改消息是真实有效可信的消息，避免接收来自不可信或恶意的发送方发送的状态修改消息，导致终端的状态信息被恶意修改。若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。终端验证状态修改消息合法之后，本发明实施例接收终端返回的状态修改请求，并根据该状态修改请求对终端的状态信息进行修改，解决了现有技术中无法提供其他标识说明终端是

否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如，当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

依据本发明的又一个方面，提供了又一种被盗终端的处理方法，包括：接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有终端的身份标识信息以及所述终端的当前状态；利用服务器对所述状态修改消息进行合法性验证；根据通过合法性验证的所述状态修改消息修改所述身份标识信息对应的终端的状态信息至所述当前状态。

本发明还提供了一种服务器，包括：接收器，配置为接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有终端的身份标识信息以及所述终端的当前状态；判断器，配置为判断所述状态修改消息是否通过合法性验证；状态修改器，配置为根据通过合法性验证的所述状态修改消息修改所述身份标识信息对应的终端的状态信息至所述当前状态。

根据本发明实施例，接收来自发送方的状态修改消息，并利用服务器对该状态修改消息进行验证，保证收到的状态修改消息是真实有效可信的消息，避免接收来自不可信或恶意的发送方发送的状态修改消息，导致终端的状态信息被恶意修改。若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。状态修改消息通过合法性验证之后，本发明实施例根据该状态修改消息对终端的状态信息进行修改，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如，当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

根据本发明的再一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据本发明的被盗终端的处理方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了根据本发明的被盗终端的处理方法的计算机程序。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了根据本发明一个实施例的被盗终端的处理方法的处理流程图；

图 2 示出了根据本发明又一个实施例的被盗终端的处理方法的处理流程图；

图 3 示出了根据本发明一个实施例的被盗终端的处理客户端的结构示意图；

图 4 示出了根据本发明一个实施例的服务器的结构示意图；

图 5 示出了根据本发明又一个实施例的被盗终端的处理方法的处理流程图；

图 6 示出了根据本发明又一个实施例的被盗终端的处理方法的处理流程图；

图 7 示出了根据本发明又一个实施例的被盗终端的处理方法的处理流程图；

图 8 示出了根据本发明又一个实施例的服务器的结构示意图；

图 9 示出了根据本发明又一个实施例的被盗终端的处理客户端的结构示意图；

图 10 示出了根据本发明又一个实施例的被盗终端的处理方法的处理流程图；

图 11 示出了根据本发明又一个实施例的被盗终端的处理方法的处理流程图；

图 12 示出了根据本发明又一个优选实施例的被盗终端的处理方法的处理流程图；

图 13 示出了根据本发明又一个优选实施例的被盗终端的处理方法的处理流程图；

图 14 示出了根据本发明又一个实施例的服务器的结构示意图；

图 15 示意性地示出了用于执行根据本发明的被盗终端的处理方法的计算设备的框图；以及

图 16 示意性地示出了用于保持或者携带实现根据本发明的被盗终端的处理方法的程序代码的存储单元。

具体实施方式

下面结合附图和具体的实施方式对本发明作进一步的描述。

相关技术中提及，无法确定终端是否被盗，因此，当终端被盗之后，失主目前仅能通过报警的手段说明终端被盗，无法提供其他标识说明终端被盗。这种技术缺陷导致用户容易购买到被盗终端，使得偷盗终端的不法行为能够产生恶劣后果。

实施例一

为解决上述技术问题，本发明实施例提供了一种被盗终端的处理方法。图 1 示出了根据本发明一个实施例的被盗终端处理方法的处理流程图。如图 1 所示，该流程至少包括步骤 S102 至步骤 S104。

步骤 S102、接收来自发送方的状态修改消息，其中，状态修改消息中携带有本终端的当前状态。

步骤 S104、在状态修改消息合法的情况下，将状态修改消息转发至服务器，由服务器根据状态修改消息将服务器中存储的本终端的状态信息修改为当前状态。

5 本发明实施例接收来自发送方的状态修改消息之后，对状态修改消息进行合法性验证，保证收到的状态修改消息是真实有效可信的命令，避免接收来自不可信或恶意的发送方发送的状态修改指令，导致终端的状态信息被恶意修改。若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。在状态修改消息合法的情况下，本发明实施例提供的方法将状态修改消息转发至服务器，由服务器根据状态修改消息将服务器
10 中存储的本终端的状态信息修改为当前状态，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如，当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏
15 制偷盗行为的有益效果。

步骤 S102 在执行时，接收来自发送方的状态修改消息，其中，发送方的身份需要进行验证，若发送方身份验证通过，则证明来自发送方的状态修改消息是合法的，可以继续执行防盗操作；若发送方身份验证不通过，则证明来自发送方的状态修改消息是不合法的，不需要继续执行防盗操作。

20 本发明实施例中，发送方身份通常可以由一个号码指代，发送方与该号码一一对应。在被盗终端侧，为保证发送方身份验证的可靠性，通常提供一个可信任号码的列表，其中存储着该被盗终端的可信任号码，例如亲友号码、约定认证码等。因此，在对状态修改消息进行合法性验证时，可以将代表发送方的号码与被盗终端侧存储的可信任号码进行匹配。若两者匹配，则发送方身份验证通过，且由该发送方发出的状态修改消息合法。
25 若两者不匹配，则发送方身份验证不通过，相应的，由该发送方发出的状态修改消息也不合法。

考虑到发送方需要发送不同的命令，且需要进行身份合法验证，因此，在本例中，发送方可以为能够发出命令且具备独特标识的终端，例如手机之类的移动终端，每个移动终端具备独特的电话号码可供身份合法验证，且能够通过短信或网络等多种手段发出
30 消息或指令。

本发明实施例对状态修改消息进行合法性验证之后，根据验证结果执行不同操作。具体地，若状态修改消息未通过合法性验证，则本发明实施例忽略该状态修改消息，若状态修改消息通过合法性验证，则本发明实施例获取被盗移动终端的身份标识信息。本发明实施例中，获取到终端的身份标识信息之后，发送携带有身份标识信息的状态修改
35 消息至服务器。

服务器接收到携带有终端的身份标识信息的状态修改消息之后，本发明实施例利用

服务器验证该状态修改消息是否合法。具体地，本发明实施例通过判断状态修改消息中携带的身份标识信息与服务器中存储的身份标识信息是否匹配对状态修改消息的合法性进行验证。若状态修改消息中携带的身份标识信息与服务器中存储的身份标识信息匹配，则本发明实施例判断状态修改消息合法。若状态修改消息中携带的身份标识信息与服务器中存储的身份标识信息不匹配，则本发明实施例判断状态修改消息不合法。

上文提及，本发明实施例根据对状态修改消息合法性的判断结果执行下一步操作。当状态修改消息不合法时，本发明实施例忽略该状态修改消息。当状态修改消息合法时，本发明实施例触发服务器中的状态信息修改操作。服务器受到触发之后，根据状态修改消息将服务器中存储的终端的状态信息修改为当前状态。

优选地，本发明实施例中，当服务器将终端的状态信息修改为当前状态之后，服务器返回修改结果至终端，并通过终端发送该修改结果至上述发送方。本发明实施例中，对终端的当前状态修改之后，将修改结果发送至终端，再由终端转发至发送方，分别提醒终端和发送方两者该终端的当前状态已修改，进而使得终端以及发送方能够根据终端修改后的当前状态执行相应操作。例如，当终端为手机时，用户使用与被盗手机绑定的亲友号码发送状态修改消息至被盗手机，标记手机已被盗。当服务器根据状态修改消息修改手机当前状态为已被盗之后，若返回修改结果至被盗手机以及亲友号码，则被盗手机能够确定自身被盗，进而执行防盗操作，如对手机进行锁屏、获取偷盗者的指纹或者照片等防盗操作。另外，用户能够及时获知手机已标记被盗，进一步对被盗手机执行其他防盗操作。

本发明实施例中，终端的身份标识信息可以是终端的国际移动设备身份识别码（International Mobile Equipment Identity，以下简称 IMEI），可以是终端的用户身份标识码（Identity，以下简称 ID），还可以是任意能够唯一标识终端的身份标识信息，本发明实施例对此并不加以限定。为提高终端的安全性，确定服务器接收到的状态修改消息为经过终端验证的合法状态修改消息，优选地，本发明实施例提供一种终端身份标识。该终端身份标识为终端的硬件 ID。

现对该硬件 ID 的获取进行具体介绍。上文提及，本发明实施例确定发送方发送的状态修改消息合法之后，获取上述硬件 ID。为获取硬件 ID，本发明实施例首先获取终端的 IMEI，记为第一字符串。其次，本发明实施例获取被盗移动终端的网卡地址，并去除网卡地址中的非字母以及非数字字符，去除后的网卡地址记为第二字符串。获取到第一字符串以及第二字符串之后，本发明实施例获取终端的中央处理器（Central Processing Unit，以下简称 CPU）串号，记为第三字符串。获取到第一、第二以及第三字符串之后，本发明实施例按预定顺序合并上述三个字符串。其中，该预定顺序可以是按第一、第二、第三的顺序合并上述三个字符串，可以是按第三、第二、第一的倒序合并上述三个字符串，还可以是其他预定的顺序，本发明实施例对此并不加以限定。

合并上述字符串之后，本发明实施例将合并后得到的结果转换为大写格式，并记为第一结果。获取到第一结果之后，本发明实施例继续将该第一结果进行消息摘要算法第

五版（Message Digest Algorithm 5，以下简称 MD5）运算，得到第二结果。之后，本发明实施例将该第二结果转换为大写格式得到终端的硬件 ID。

本发明实施例中终端的硬件 ID 通过将终端的 IMEI、网卡地址以及 CPU 的串号进行合并运算能够保证服务器接收的状态修改消息是真实有效可信的，避免接收来自不可信或恶意发送端伪装成终端发送的状态修改消息导致服务器对终端的状态信息进行错误修改。例如，若不可信或恶意发送端伪装成终端发送状态修改消息指示服务器将终端的状态信息从被盗修改为解除被盗。当终端的状态信息修改为解除被盗之后，不法分子可以对终端进行刷机处理，导致失主无法找回终端的恶劣后果。本发明实施例将接收到的状态修改消息中携带的硬件 ID 与服务器本地存储的硬件 ID 进行匹配，若硬件 ID 匹配，则终端的 IMEI、网卡地址以及 CPU 串号均能够匹配，则能够确定本发明实施例接收到的状态修改消息的合法性。确定状态修改消息的合法性之后，对终端的状态信息进行修改保证服务器存储的终端的状态信息能够及时更新。

另外，本发明实施例中，终端的当前状态可以包括终端被盗以及终端未被盗、终端被盗后找回等等。当终端被盗之后，本发明实施例对终端的状态信息进行及时更新，以便服务器接收到终端的相关信息（如终端的实时位置、终端当前使用者的指纹等）之后，能够向失主提供被盗终端的相关线索，增加失主找回终端的可能性。当终端被盗后找回之后，本发明实施例及时更新终端的状态为被盗后找回，服务器也就无需浪费空间等资源查询以及存储终端的相关信息。进一步，本发明实施例的终端的当前状态还可以包括其他更为详细的说明，例如包括终端未出售、终端使用中以及终端被转卖等终端的出售购买状态信息，还可以是其他任意终端的当前状态信息，本发明实施例对此并不加以限定。

现以具体实施例对本发明的被盗终端的处理方法进行进一步说明。

图 2 示出了根据本发明一个优选实施例的被盗终端的处理方法的流程图，用于支持上述任意一个被盗终端的处理方法，将上述被盗终端的处理方法阐述得更加清晰易懂。参见图 2，该优选实施例至少包括步骤 S202 至步骤 S220。

需要说明的是，为将本优选实施例阐述得更加简单明白，本优选实施例中，将状态修改消息的发送方设置为亲友号码，将终端设置为被盗终端。其中，亲友号码为被盗手机被盗绑定的号码。

步骤 S202、亲友手机发送状态修改消息至被盗手机，标记手机被盗。

具体地，用户发现手机被盗之后，使用与被盗手机绑定的亲友号码发送携带有状态修改消息的短信至被盗手机，要求标记手机的当前状态为手机被盗。

步骤 S204、判断状态修改消息是否合法。

被盗手机接收到亲友号码发送的状态修改消息之后，判断状态修改消息的发送方与被盗手机存储的亲友号码是否匹配。若未能匹配，则执行步骤 S206。若能够匹配，则执行步骤 S208。

步骤 S206、当被盗手机判断状态修改消息不合法时，忽略状态修改消息。

步骤 S208、当被盗手机判断状态修改消息合法时，获取自身的硬件 ID。

步骤 S210、转发状态修改消息。

当被盗手机接收到状态修改消息并判断该命令合法之后，执行步骤 S210，转发携带有通过步骤 S208 获取的硬件 ID 的状态修改消息。

5 步骤 S212、判断状态修改消息是否合法。

服务器接收到被盗手机转发的状态修改消息之后，对状态修改消息中携带的被盗手机的硬件 ID 以及服务器本地存储的硬件 ID 进行匹配。若未能匹配，则服务器判断状态修改消息不合法，执行步骤 S214。若能够匹配，则服务器判断状态修改消息合法，执行步骤 S216。

10 步骤 S214、当服务器判断状态修改消息不合法时，忽略状态修改消息。

步骤 S216、当服务器判断状态修改消息合法时，修改被盗手机的状态信息为手机被盗。

当服务器判断接收到的状态修改消息合法之后，服务器根据状态修改消息将被盗手机的状态修改为手机被盗。

15 步骤 S218、返回修改结果至被盗手机。

服务器根据状态修改消息将手机的状态信息修改为手机被盗之后，返回该修改结果至被盗手机，保证被盗手机能够及时获知自身的当前状态。

步骤 S220、发送修改结果至亲友号码。

20 被盗手机接收到服务器返回的修改结果之后，将该修改结果发送至亲友号码。亲友号码接收到对被盗手机的状态信息的修改，则用户能够获知服务器已对被盗手机进行标识。

基于上文各优选实施例提供的被盗终端的处理方法，基于同一发明构思，本发明实施例提供一种被盗终端的处理客户端，用于实现上述被盗终端的处理方法。

25 图 3 示出了根据本发明一个实施例的被盗终端的处理客户端的结构示意图。参见图 3，本发明实施例的被盗终端的处理客户端至少包括：接收器 310、合法判断器 320 以及发送器 330。

现介绍本发明实施例的被盗终端的处理客户端的各器件或组成的功能以及各部分间的连接关系：

30 接收器 310，配置为接收来自发送方的状态修改消息，其中，状态修改消息中携带有终端的当前状态。

合法判断器 320，与接收器 310 相耦合，配置为判断状态修改消息是否合法。

发送器 330，与接收器 310 以及合法判断器 320 分别耦合，配置为在状态修改消息合法的情况下，将状态修改消息转发至服务器，由服务器根据状态修改消息将服务器中存储的终端的状态信息修改为当前状态。

35 本发明实施例接收来自发送方的状态修改消息之后，对状态修改消息进行合法性验证，保证收到的状态修改消息是真实有效可信的命令，避免接收来自不可信或恶意的发

送方发送的状态修改指令，导致终端的状态信息被恶意修改。若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。在状态修改消息合法的情况下，本发明

5 实施例将状态修改消息转发至服务器，由服务器根据状态修改消息将服务器中存储的本终端的状态信息修改为当前状态，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理客户端能够更改被盗终端的状态信息。例如当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的

10 线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

本发明实施例中，客户端中的接收器 310 接收来自发送方的状态修改消息，发送方的身份需要由合法判断器 320 进行验证，若经过合法判断器 320 验证，状态修改消息的发送方与终端中存储的可信任号码匹配，则状态修改消息通过合法性验证，可以继续执行

15 防盗操作；若经过合法判断器 320 验证，状态修改消息的发送方与终端中存储的可信任号码不匹配，不需要继续执行防盗操作。

本发明实施例中，发送方身份通常可以由一个号码指代，发送方与该号码一一对应。在终端侧，为保证发送方身份验证的可靠性，通常提供一个可信任号码的列表，其中存储着该终端的可信任号码，例如亲友号码、约定认证码等。因此，在对状态修

20 改消息进行合法性验证时，可以将代表发送方的号码与终端侧存储的可信任号码进行匹配。若两者匹配，则发送方身份验证通过，且由该发送方发出的状态修改消息合法。若两者不匹配，则发送方身份验证不通过，相应的，由该发送方发出的状态修改消息也不合法。

若经过合法判断器 320 的验证，状态修改消息不合法，则如图 3 所示的客户端忽略

25 该状态修改消息。若经过合法判断器 320 的验证，状态修改消息合法，则合法判断器 320 触发发送器 330，由发送器 330 获取终端的身份标识信息。发送器 330 获取到身份标识信息之后，发送携带有该身份标识信息的状态修改消息至服务器。

服务器接收到携带有终端的身份标识信息的状态修改消息之后，验证该状态修改消息是否合法。具体地，服务器通过判断状态修改消息中携带的身份标识信息与服务器本地存储的身份标识信息是否匹配对状态修改消息的合法性进行验证。若状态修改消息中

30 携带的身份标识信息与服务器中存储的身份标识信息匹配，则判断状态修改消息合法。若状态修改消息中携带的身份标识信息与服务器中存储的身份标识信息不匹配，则判断状态修改消息不合法。当服务器判断状态修改消息不合法时，服务器忽略该状态修改消息。当服务器判断该状态修改消息合法时，服务器根据该状态修改消息对本地存储的终

35 端的状态信息进行修改，并返回修改结果。

如图 3 所示的客户端中的接收器 310 接收到服务器返回的修改结果之后，触发发送

器 330, 由发送器 330 将该修改结果转发至上述状态修改消息的发送方。本发明实施例中, 对终端的当前状态修改之后, 将修改结果发送至如图 3 所示的客户端, 再由客户端转发至发送方, 分别提醒终端和发送方两者该终端的当前状态已修改, 进而使得发送方能够根据终端修改后的当前状态执行相应操作。例如, 当终端为手机时, 用户使用与被盗手机绑定的亲友号码发送状态修改消息至被盗手机, 标记手机已被盗。当服务器根据状态修改消息修改手机当前状态为已被盗之后, 若返回修改结果至亲友号码, 则用户能够及时获知手机已标记被盗, 进一步对被盗手机执行其他防盗操作。

本发明实施例中, 终端的身份标识信息可以是终端的 IMEI, 可以是终端的用户 ID, 还可以是任意能够唯一标识终端的身份标识信息, 本发明实施例对此并不加以限定。为提高终端的安全性, 确定服务器接收到的状态修改消息为经过终端验证的合法状态修改消息, 优选地, 本发明实施例提供一种终端身份标识。该终端身份标识为终端的硬件 ID。

现对该硬件 ID 的获取进行具体介绍。上文提及, 合法判断器 320 判断发送方发送的状态修改消息合法之后, 由发送器 330 获取作为终端的身份标识信息的硬件 ID。本发明实施中, 发送器 330 触发计算器 340, 由计算器 340 计算终端的硬件 ID。具体地, 计算器 340 首先获取终端的 IMEI, 记为第一字符串。其次, 计算器 340 获取被盗移动终端的网卡地址, 并去除网卡地址中的非字母以及非数字字符, 去除后的网卡地址记为第二字符串。计算器 340 获取到第一字符串以及第二字符串之后, 获取终端的 CPU 串号, 记为第三字符串。获取到第一、第二以及第三字符串之后, 计算器 340 按预定顺序合并上述三个字符串。其中, 该预定顺序可以是按第一、第二、第三的顺序合并上述三个字符串, 可以是按第三、第二、第一的倒序合并上述三个字符串, 还可以是其他预定的顺序, 本发明实施例对此并不加以限定。

合并上述字符串之后, 计算器 340 将合并后得到的结果转换为大写格式, 并记为第一结果。获取到第一结果之后, 计算器 340 将该第一结果进行 MD5 运算, 得到第二结果。之后, 计算器 340 将该第二结果转换为大写格式得到终端的硬件 ID。

本发明实施例中终端的硬件 ID 通过将终端的 IMEI、网卡地址以及 CPU 的串号进行合并运算能够保证服务器接收的状态修改消息是真实有效可信的, 避免接收来自不可信或恶意发送端伪装成终端发送的状态修改消息导致服务器对终端的状态信息进行错误修改。例如, 若不可信或恶意发送端伪装成终端发送状态修改消息指示服务器将终端的状态信息从被盗修改为解除被盗。当终端的状态信息修改为解除被盗之后, 不法分子可以对终端进行刷机 etc 处理, 导致失主无法找回终端的恶劣后果。本发明实施例将接收到的状态修改消息中携带的硬件 ID 与服务器本地存储的硬件 ID 进行匹配, 若硬件 ID 匹配, 则终端的 IMEI、网卡地址以及 CPU 串号均能够匹配, 则能够确定本发明实施例接收到的状态修改消息的合法性。确定状态修改消息的合法性之后, 对终端的状态信息进行修改保证服务器存储的终端的状态信息能够及时更新。

另外, 本发明实施例中, 终端的当前状态可以包括终端被盗以及终端未被盗、终端被盗后找回等等。当终端被盗之后, 本发明实施例对终端的状态信息进行及时更新, 以

便服务器接收到终端的相关信息（如终端的实时位置、终端当前使用者的指纹等）之后，能够向失主提供被盗终端的相关线索，增加失主找回终端的可能性。当终端被盗后找回之后，本发明实施例及时更新终端的状态为被盗后找回，服务器也就无需浪费空间等资源查询以及存储终端的相关信息。进一步，本发明实施例的终端的当前状态还可以包括其他更为详细的说明，例如包括终端未出售、终端使用中以及终端被转卖等终端的出售购买状态信息，还可以是其他任意终端的当前状态信息，本发明实施例对此并不加以限定。

在本实施例中，被盗终端的处理客户端（参见图 3）能够接收来自发送方的状态修改消息，并对其进行验证。当验证通过时，将该状态修改消息转发至服务器。即，本实施例中，被盗终端的处理客户端的功能为验证状态修改消息的合法性。

基于上文各优选实施例提供的被盗终端的处理方法及客户端，基于同一发明构思，本发明实施例提供了一种服务器，用于实现上述被盗终端的处理方法。

图 4 示出了根据本发明一个实施例的服务器的结构示意图。参见图 4，本发明实施例的服务器至少包括：命令接收器 410 以及状态修改器 430。

现介绍本发明实施例的服务器的各器件或组成的功能以及各部分间的连接关系：

命令接收器 410，配置为接收终端发送的状态修改消息，其中，状态修改消息中携带有终端的当前状态以及终端的身份标识信息；

状态修改器 430，与命令接收器 410 耦合，配置为根据状态修改消息将本服务器中存储的终端的状态信息修改为当前状态。

本发明实施例中，将状态修改消息转发至服务器，由服务器根据状态修改消息将服务器中存储的本终端的状态信息修改为当前状态，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

如图 4 所示的服务器中的命令接收器 410 接收到携带有终端的身份标识信息的状态修改消息之后，状态修改器 430 根据状态修改消息对本地存储的终端的状态信息进行修改。优选地，本发明实施例在服务器中添加如图 4 所示的判断器 420。当命令接收器 410 接收到状态修改消息之后，由判断器 420 判断该状态修改消息是否合法。具体地，判断器 420 通过判断状态修改消息中携带的身份标识信息与服务器中存储的身份标识信息是否匹配对状态修改消息的合法性进行验证。若状态修改消息中携带的身份标识信息与服务器中存储的身份标识信息匹配，则判断器 420 判断状态修改消息合法。若状态修改消息中携带的身份标识信息与服务器中存储的身份标识信息不匹配，则判断器 420 判断状态修改消息不合法。

本发明实施例中，终端的身份标识信息可以是终端的 IMEI，可以是终端的用户 ID，

还可以是任意能够唯一标识终端的身份信息，本发明实施例对此并不加以限定。为提高终端的安全性，确定服务器接收到的状态修改消息为经过终端验证的合法状态修改消息，优选地，本发明实施例提供一种终端身份标识。该终端身份标识为终端的硬件 ID。

判断器 420 对状态修改消息的合法性进行判断之后，触发状态修改器 430。状态修改器 430 根据判断器 420 的判断结果执行下一步操作。当状态修改消息不合法时，状态修改器 430 忽略该状态修改消息。当状态修改消息合法时，状态修改器 430 根据状态修改消息将服务器中存储的终端的状态信息修改为当前状态。

状态修改器 430 将本地存储的终端的状态信息修改为当前状态之后，由结果发送器 440 将修改结果发送至终端。本发明实施例中，状态修改器 430 对终端的当前状态修改之后，结果发送器 440 将修改结果发送至终端，并由终端发送该修改结果至发送方，提醒发送方终端的当前状态。发送方能够根据终端的当前状态执行相应操作。

另外，本发明实施例中，终端的当前状态可以包括终端被盗以及终端未被盗、终端被盗后找回等等。当终端被盗之后，客户端中的状态修改器 430 对终端的状态信息进行及时更新，以便服务器接收到终端的相关信息（如终端的实时位置、终端当前使用者的指纹等）之后，能够向失主提供被盗终端的相关线索，增加失主找回终端的可能性。当终端被盗后找回之后，状态修改器 430 及时更新终端的状态为被盗后找回，服务器也就无需浪费空间等资源查询以及存储终端的相关信息。进一步，本发明实施例的终端的当前状态还可以包括其他更为详细的说明，例如包括终端未出售、终端使用中以及终端被转卖等终端的出售购买状态信息，还可以是其他任意终端的当前状态信息，本发明实施例对此并不加以限定。

在本实施例中，服务器（参见图 4）接收经过终端验证的状态修改消息，对其进行修改。即，在本发明实施例中，服务器的功能是用于修改本地存储的终端的状态信息。当然，为增加安全性，可以对状态修改消息进行进一步验证。

根据上述任意一个优选实施例或多个优选实施例的组合，本发明实施例能够达到如下有益效果：

本发明实施例接收来自发送方的状态修改消息之后，对状态修改消息进行合法性验证，保证收到的状态修改消息是真实有效可信的命令，避免接收来自不可信或恶意的发送方发送的状态修改指令，导致终端的状态信息被恶意修改。若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。在状态修改消息合法的情况下，本发明实施例提供的方法将状态修改消息转发至服务器，由服务器根据状态修改消息将服务器中存储的本终端的状态信息修改为当前状态，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供

偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

实施例二

5 本实施例提供了一种被盗终端的处理方法。图 5 示出了根据本发明一个实施例的被盗终端的处理方法的处理流程图。如图 5 所示，该流程至少包括步骤 S502 至步骤 S506。

步骤 S502、接收来自发送方的状态修改消息，其中，状态修改消息中携带有状态发生改变终端的身份标识信息。

10 步骤 S504、将状态修改消息转发至终端的身份标识信息对应的终端，由终端对其进行验证。

步骤 S506、根据终端验证状态修改消息通过时返回的状态修改请求，对终端的状态信息进行修改。

本发明实施例接收来自发送方的状态修改消息，并将其转发至对应的终端，由终端对该状态修改消息进行验证，保证收到的状态修改消息是真实有效可信的消息，避免接收来自不可信或恶意的发送方发送的状态修改消息，导致终端的状态信息被恶意修改。15 若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。终端验证状态修改消息合法之后，本发明实施例接收终端返回的状态修改请求，并根据该状态修改请求对终端的状态信息进行修改，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如，当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。25

步骤 S502 在执行时，接收来自发送方的状态修改消息，其中，该状态修改消息中携带有状态发生改变的终端的身份标识信息。优选地，为保证接收到的状态修改消息真实有效可信，本发明实施例对接收到的状态修改消息进行验证。若状态修改消息通过验证，可以继续执行防盗操作；若状态修改消息未通过验证，不需要继续执行防盗操作。

30 本发明实施例中，状态修改消息中携带有终端的身份标识信息，而服务器中存储着的各个终端的身份标识信息。若状态修改消息中携带的终端的身份标识信息与服务器中存储的终端的身份标识信息能够匹配，则状态修改消息通过合法性验证，执行如图 5 所示的步骤 S504，本发明实施例将状态修改消息转发至上述身份标识信息对应的终端；若不匹配，则状态修改消息未通过合法性验证，相应的，本发明实施例忽略该状态修改消息，不执行任何操作。35

当本发明实施例将状态修改消息转发至对应的终端之后，终端无法保证转发该状态

修改消息的服务器为可靠服务器，进而，在服务器侧对状态修改消息进行的验证也就无法被信任。为保证终端接收到的状态修改消息不是恶意服务器发送至终端的状态修改消息，终端对接收到的状态修改消息再次进行合法性验证。当终端接收到状态修改消息之后，本发明实施例判断状态修改消息中携带的终端的标识信息与终端本地存储的身份标识信息是否匹配。若匹配，则该状态修改消息合法，若不匹配，则该状态修改消息不合法。

根据上述对状态修改消息合法性的验证结果，终端执行不同的操作。具体地，若状态修改消息不合法，则忽略该状态修改消息，若状态修改消息合法，则终端获取本身的ID，并返回携带有该硬件ID的状态修改请求。

本发明实施例接收到状态修改请求之后，根据状态修改请求中携带的硬件ID，对状态修改请求进行合法性验证。具体地，当状态修改请求中携带的硬件ID与服务器本地存储的硬件ID能够匹配，则状态修改请求通过合法性验证；若不能够匹配，则状态修改请求无法通过合法性验证。若状态修改请求无法通过合法性验证，本发明实施例忽略状态修改请求，不执行任何操作。若状态修改请求通过合法性验证，则本发明实施例利用服务器对终端的状态信息进行修改，保证服务器中存储的终端的状态信息能够及时更新至终端的当前状态。

本发明实施例中，对状态修改消息的两次合法性验证均通过终端的身份标识，而对状态修改请求的验证，为提高安全性，确定接收到的状态修改请求为合法状态修改请求，本发明实施例使用终端的硬件ID对状态修改请求进行合法性验证。

其中，终端的身份标识信息可以是终端的IMEI，可以是终端的用户ID，还可以是任意能够唯一标识终端的身份标识信息，本发明实施例对此并不加以限定。

终端的硬件ID为汇集多种终端身份标识信息的、综合的身份标识信息。现对该硬件ID的获取进行具体介绍。如上文所述，若状态修改消息合法，则本发明实施例获取上述终端的硬件ID。其中，硬件ID的获取方式与实施例一中的获取方式相同。

本发明实施例中终端的硬件ID通过将终端的IMEI、网卡地址以及CPU的串号进行合并运算能够保证服务器接收的状态修改消息是真实有效可信的，避免接收来自不可信或恶意发送端伪装成终端发送的状态修改消息导致服务器对终端的状态信息进行错误修改。例如，若不可信或恶意发送端伪装成终端发送状态修改消息指示服务器将终端的状态信息从被盗修改为解除被盗。当终端的状态信息修改为解除被盗之后，不法分子可以对终端进行刷机 etc 处理，导致失主无法找回终端的恶劣后果。本发明实施例将接收到的状态修改消息中携带的硬件ID与服务器本地存储的硬件ID进行匹配，若硬件ID匹配，则终端的IMEI、网卡地址以及CPU串号均能够匹配，则能够确定本发明实施例接收到的状态修改消息的合法性。确定状态修改消息的合法性之后，对终端的状态信息进行修改保证服务器存储的终端的状态信息能够及时更新。

本发明实施例中，对终端的状态信息进行修改可以包括修改终端的状态信息为被盗、未被盗或者终端被盗后找回等等。当终端被盗之后，本发明实施例对终端的状态信息进

行及时修改，以便服务器接收到终端的相关信息（如终端的实时位置、终端当前使用者的指纹等）之后，能够向失主提供被盗终端的相关线索，增加失主找回终端的可能性。当终端被盗后找回之后，本发明实施例及时修改终端的状态信息为被盗后找回，服务器也就无需浪费空间等资源查询以及存储终端的相关信息。进一步，本发明实施例的终端的状态信息还可以包括其他更为详细的说明，例如包括终端未出售、终端使用中以及终端被转卖等终端的出售购买状态信息，还可以是其他任意终端的当前状态信息，本发明实施例对此并不加以限定。

本发明实施例中，将终端的状态信息修改为当前状态之后，本发明实施例可以返回修改结果至状态修改消息的发送方。本发明实施例中，对终端的当前状态修改之后，将修改结果发送至发送方，提醒发送方终端的当前状态已修改，进而使得发送方能够根据终端修改后的当前状态执行相应操作。例如，当终端为手机时，用户使用与被盗手机绑定的亲友号码发送状态修改消息至被盗手机，标记手机已被盗。当服务器根据状态修改消息修改手机当前状态为已被盗之后，若返回修改结果至亲友号码，则用户能够及时获知手机已标记被盗，进一步对被盗手机执行其他防盗操作。

本发明实施例还可以在状态修改消息通过合法性验证之后，生成一个执行修改操作的任务 ID，并发送该任务 ID 至状态修改消息发送方。发送方接收到该任务 ID 之后，确定状态修改消息已经通过服务器的合法性验证。另外，发送方能够随时发送携带有该任务 ID 的查询请求至服务器，查询服务器的修改操作的执行情况。服务器接收到发送方的查询请求之后，根据查询请求中携带的任务 ID 确定当前修改操作的执行情况，并返回至发送方。例如，当终端为手机时，若手机丢失，用户能够发送状态修改消息至服务器，并接收到服务器返回的任务 ID。根据该任务 ID，用户能够随时查询服务器的状态修改操作的执行情况。若因为服务器故障等原因导致当前修改操作无法继续执行，用户能够及时获知操作无法执行的相关信息，并根据获知的相关信息采取相应措施，更加高效率地保护被盗手机的安全。

本发明实施例中，状态修改消息的发送方可以设置于移动终端，例如手机，笔记本电脑等等，并通过短信息或者网络的形式发送状态修改消息。本发明实施例中的发送方还可以设置于终端，例如电脑，并通过网络的形式发送上述状态修改消息。采用本发明实施例，能够及时修改终端的状态信息。例如，当终端被盗之后，用户能够通过各种消息发送平台发送状态修改消息，保证及时标记终端被盗。进一步能够及时获知被盗终端的相关信息，增大被盗终端找回的机率。

现以具体实施例对本发明的被盗终端的处理方法进行进一步说明。

图 6 示出了根据本发明一个优选实施例的被盗终端的处理方法的处理流程图，用于支持上述任意一个被盗终端的处理方法，将上述被盗终端的处理方法阐述得更加清晰易懂。参见图 6，该优选实施例至少包括步骤 S602 至步骤 S628。

需要说明的是，为将本优选实施例阐述得更加简单明白，本优选实施例中，将状态修改消息的发送方设置于亲友手机，将终端设置为被盗终端。其中，亲友手机为被盗手

机绑定的亲友号码所在的手机。

步骤 S602、发送状态修改消息，标记手机被盗。

当手机被盗之后，用户使用亲友手机通过网络发送状态修改消息至服务器，标记手机被盗。

5 步骤 S604、判断状态修改请求是否合法。

服务器接收到状态修改消息之后，判断该状态修改消息是否合法。若是，执行步骤 S608，若否，执行步骤 S606。

步骤 S606、状态修改消息不合法，忽略状态修改消息。

步骤 S608、发送任务 ID 至亲友手机。

10 具体地，当经过服务器判断，状态修改消息合法之后，服务器生成执行修改操作的任务 ID，并通过网络发送该任务 ID 至亲友手机。

步骤 S610、转发状态修改消息。

步骤 S612、判断状态修改消息是否合法。

15 服务器验证接收到的状态修改消息合法之后，转发该状态修改消息至被盗手机。被盗手机接收到该状态修改消息之后，再次对该状态修改消息进行合法性验证。若该状态修改消息未通过合法性验证，则执行步骤 S614，若通过验证，则执行步骤 S616。

步骤 S614、当状态修改消息未通过合法性验证，忽略状态修改消息。

步骤 S616、当状态修改消息通过合法性验证，被盗手机获取自身的硬件 ID。

步骤 S618、发送状态修改请求至服务器。

20 被盗手机获取到自身的硬件 ID 之后，发送携带有该硬件 ID 的状态修改请求至服务器。

步骤 S620、判断状态修改请求是否合法。

服务器接收到状态修改请求之后，根据状态修改请求中携带的硬件 ID 判断该状态修改请求是否合法。若不合法，执行步骤 S622，若合法，执行步骤 S624。

25 步骤 S622、当状态修改请求不合法，服务器忽略状态修改请求。

步骤 S624、当状态修改请求合法，执行修改状态信息操作。

步骤 S626、发送查询请求。

亲友手机接收到服务器发送的任务 ID 之后，能够通过网络发送携带有该任务 ID 的查询请求至服务器，查询服务器的修改操作的执行情况。

30 步骤 S628、发送修改执行情况至亲友手机。

服务器接收到亲友手机发送的查询请求之后，根据查询请求中携带的任务 ID 获取当前修改操作的执行情况，并将该执行情况通过网络返回至亲友手机。

35 图 7 示出了根据本发明另一个优选实施例的被盗终端的处理方法的处理流程图，用于支持上述任意一个被盗终端的处理方法，将上述被盗终端的处理方法阐述得更加清晰易懂。参见图 7，该优选实施例至少包括步骤 S702 至步骤 S724。

需要说明的是，为将本优选实施例阐述得更加简单明白，本优选实施例中，将状态

修改消息的发送方设置于亲友手机，将终端设置为被盗终端。其中，亲友手机为被盗手机绑定的亲友号码所在的手机。

步骤 S702、发送状态修改消息，标记手机被盗。

5 当手机被盗之后，用户使用亲友手机通过短信息发送状态修改消息至服务器，标记手机被盗。

步骤 S704、判断状态修改请求是否合法。

服务器接收到状态修改消息之后，判断该状态修改消息是否合法。若是，执行步骤 S708，若否，执行步骤 S706。

步骤 S706、状态修改消息不合法，忽略状态修改消息。

10 步骤 S708、转发状态修改消息。

步骤 S710、判断状态修改消息是否合法。

服务器验证接收到的状态修改消息合法之后，转发该状态修改消息至被盗手机。被盗手机接收到该状态修改消息之后，再次对该状态修改消息进行合法性验证。若该状态修改消息未通过合法性验证，则执行步骤 S712，若通过验证，则执行步骤 S714。

15 步骤 S712、当状态修改消息未通过合法性验证，忽略状态修改消息。

步骤 S714、当状态修改消息通过合法性验证，被盗手机获取自身的硬件 ID。

步骤 S716、发送状态修改请求至服务器。

被盗手机获取到自身的硬件 ID 之后，发送携带有该硬件 ID 的状态修改请求至服务器。

20 步骤 S718、判断状态修改请求是否合法。

服务器接收到状态修改请求之后，根据状态修改请求中携带的硬件 ID 判断该状态修改请求是否合法。若不合法，执行步骤 S720，若合法，执行步骤 S722。

步骤 S720、当状态修改请求不合法，服务器忽略状态修改请求。

步骤 S722、当状态修改请求合法，执行修改状态信息操作。

25 步骤 S724、通过短信息发送修改执行情况至亲友手机。

请注意，以上 S702 和 S724 中的发送步骤也可以通过网络来发送，本发明不限于此。

基于上文各优选实施例提供的被盗终端的处理方法，基于同一发明构思，本发明实施例提供一种服务器，用于实现上述被盗终端的处理方法。

图 8 示出了根据本发明一个实施例的服务器的结构示意图。参见图 8，本发明实施例
30 的服务器至少包括：接收器 810、发送器 830 以及状态修改器 840。

现介绍本发明实施例的服务器的各器件或组成的功能以及各部分间的连接关系：

接收器 810，配置为接收来自发送方的状态修改消息，其中，状态修改消息中携带有状态发生改变的终端的身份标识信息。

发送器 830，与接收器 810 相耦合，配置为将状态修改消息转发至终端的身份标识信息对应的终端，由终端对其进行验证。
35

状态修改器 840，与接收器 810 相耦合，配置为根据终端验证状态修改消息通过时返

回的状态修改请求，对终端的状态信息进行修改。

本发明实施例接收来自发送方的状态修改消息，并将其转发至对应的终端，由终端对该状态修改消息进行验证，保证收到的状态修改消息是真实有效可信的消息，避免接收来自不可信或恶意的发送方发送的状态修改消息，导致终端的状态信息被恶意修改。

5 若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。终端验证状态修改消息合法之后，本发明实施例接收终端返回的状态修改请求，并根据该状态修改请求对终端的状态信息进行修改，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如，当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

15 如图 8 所示的服务器中的接收器 810 接收来自发送方的状态修改消息，其中，该状态修改消息中携带有状态发生改变的终端的身份标识信息。优选地，为保证接收到的状态修改消息真实有效可信，服务器中判断器 820 对接收到的状态修改消息进行合法性判断。若经过判断器 820 的判断，状态修改消息合法，则继续执行防盗操作；若经过判断器 820 的判断，状态修改消息不合法，则不需要继续执行防盗操作。

20 本发明实施例中，状态修改消息中携带有终端的身份标识信息，而服务器中存储着的各个终端的身份标识信息。若状态修改消息中携带的终端的身份标识信息与服务器中存储的终端的身份标识信息能够匹配，则判断器 820 判断状态修改消息通过合法性验证，则由发送器 830 将状态修改消息转发至上述身份标识信息对应的终端；若不匹配，则判断器 820 判断状态修改消息未通过合法性验证，相应的，服务器忽略该状态修改消息，
25 不执行任何操作。

当状态修改消息发送至终端之后，终端对该状态修改消息进行合法性验证。若该状态修改消息通过未合法性验证，则终端忽略该状态修改消息。若该状态修改消息通过合法性验证，则终端获取自身的硬件 ID，并发送携带有该硬件 ID 的状态修改请求至如图 4 所示的服务器。

30 服务器中的接收器 810 接收到状态修改请求之后，触发判断器 820。判断器 820 判断该状态修改请求是否合法。本发明实施例中，判断器 820 通过判断状态修改请求中携带的硬件 ID 与服务器本地存储的硬件 ID 是否匹配判断状态修改请求是否合法。若状态修改请求中携带的硬件 ID 与服务器本地存储的硬件 ID 不匹配，则判断器 820 判断该状态修改请求不合法，则服务器忽略该状态修改请求。若状态修改请求中携带的硬件 ID 与服务器本地存储的硬件 ID 匹配，则判断器 820 判断该状态修改请求合法，并触发与其耦合的状态修改器 840。状态修改器 840 根据状态修改请求对终端的状态信息进行修改。

本发明实施例中，状态修改器 840 对终端的状态信息进行修改可以包括修改终端的状态信息为被盗、未被盗或者终端被盗后找回等等。当终端被盗之后，服务器中的状态修改器 840 对终端的状态信息进行及时修改，以便服务器接收到终端的相关信息（如终端的实时位置、终端当前使用者的指纹等）之后，能够向失主提供被盗终端的相关线索，增加失主找回终端的可能性。当终端被盗后找回之后，服务器中的状态修改器 840 及时修改终端的状态信息为被盗后找回，服务器也就无需浪费空间等资源查询以及存储终端的相关信息。进一步，本发明实施例的终端的状态信息还可以包括其他更为详细的说明，例如包括终端未出售、终端使用中以及终端被转卖等终端的出售购买状态信息，还可以是其他任意终端的当前状态信息，本发明实施例对此并不加以限定。

本发明实施例中，状态修改器 840 将终端的状态信息修改为当前状态之后，触发发送器 830。发送器 830 可以返回修改结果至状态修改消息的发送方。本发明实施例中，发送器 830 将修改结果发送至发送方，提醒发送方终端的当前状态已修改，进而使得发送方能够根据终端修改后的当前状态执行相应操作。例如，当终端为手机时，用户使用与被盗手机绑定的亲友号码发送状态修改消息至被盗手机，标记手机已被盗。当服务器根据状态修改消息修改手机当前状态为已被盗之后，若返回修改结果至亲友号码，则用户能够及时获知手机已标记被盗，进一步对被盗手机执行其他防盗操作。

本发明实施例还可以在判断器 820 判断状态修改消息通过合法性验证之后，生成一个执行修改操作的任务 ID，并由接收器 810 发送该任务 ID 至状态修改消息发送方。发送方接收到该任务 ID 之后，确定状态修改消息已经通过服务器的合法性验证。另外，发送方能够随时发送携带有该任务 ID 的查询请求至服务器，查询服务器的修改操作的执行情况。服务器中的接收器 810 接收到发送方的查询请求之后，根据查询请求中携带的任务 ID 确定当前修改操作的执行情况，并触发发送器 830 返回修改操作的执行情况至发送方。例如，当终端为手机时，若手机丢失，用户能够发送状态修改消息至服务器，并接收到服务器返回的任务 ID。根据该任务 ID，用户能够随时查询服务器的状态修改操作的执行情况。若因为服务器故障等原因导致当前修改操作无法继续执行，用户能够及时获知操作无法执行的相关信息，并根据获知的相关信息采取相应措施，更加高效率地保护被盗手机的安全。

在本实施例中，服务器（参见图 8）接收来自发送方的状态修改消息，将其转至对应终端进行身份验证。验证通过时终端向服务器发送状态修改请求，由服务器对其进行修改。即，在本发明实施例中，服务器的功能是用于转发状态修改消息，以及验证通过后根据相应请求修改本地存储的终端的状态信息。当然，为增加安全性，可以对状态修改消息进行进一步验证。

基于上文各优选实施例提供的被盗终端的处理方法及服务器，基于统一发明构思，本发明实施例提供一种被盗终端的处理客户端，用于实现上述被盗终端的处理方法。

图 9 示出了根据本发明一个实施例的被盗终端的处理客户端的结构示意图。参见图 9，本发明实施例的被盗终端的处理客户至少包括：消息接收器 910、验证器 920 以及请

求发送器 930。

现介绍本发明实施例的被盗终端的处理客户端的各器件或组成的功能以及各部分间的连接关系：

消息接收器 910，配置为接收服务器转发的、来自发送方的状态修改消息。

5 验证器 920，与消息接收器 910 相耦合，配置为对接收到的状态修改消息进行验证。

请求发送器 930，与验证器 920 相耦合，配置为状态修改消息通过验证之后，返回状态修改请求至服务器，由服务器根据状态修改请求对终端的状态进行修改。

本发明实施例接收来自发送方的状态修改消息，并将其转发至对应的终端，由终端对该状态修改消息进行验证，保证收到的状态修改消息是真实有效可信的消息，避免接收来自不可信或恶意的发送方发送的状态修改消息，导致终端的状态信息被恶意修改。若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。终端验证状态修改消息合法之后，本发明实施例接收终端返回的状态修改请求，并根据该状态修改请求对终端的状态信息进行修改，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如，当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

如图 9 所示的客户端中的消息接收器 910 接收到服务器转发的、来自发送方的状态修改消息之后，触发验证器 920。为保证接收到的状态修改消息不是非恶意服务器发送的状态修改消息，验证器 920 根据状态修改消息中携带的终端的身份标识信息对状态修改消息进行合法性验证。若经过验证器 920 的验证，状态修改消息中携带的终端的身份标识信息与终端本地存储的身份标识信息匹配，则状态修改消息合法。若经过验证器 920 的验证，状态修改消息中携带的终端的身份标识信息与终端本地存储的身份标识信息不匹配，则状态修改消息不合法。

如上文所述，验证器 920 验证消息接收器 910 接收到的状态修改消息是否合法，并根据验证结果执行下一步操作。具体地，若状态修改消息不合法，则如图 9 所示的客户端忽略该状态修改消息，不执行任何操作。若状态修改消息合法，则验证器 920 触发请求发送器 930。请求发送器 930 获取终端的硬件 ID，并发送携带有该硬件 ID 的状态修改请求至服务器。

请求发送器 930 发送状态修改请求至服务器之前，从与其耦合的计算器 940 处获取终端的硬件 ID。现对该硬件 ID 的获取进行具体介绍。如上文所述，验证器 920 验证状态修改消息合法之后，由请求发送器 930 获取作为终端的身份标识信息的硬件 ID。本发明实施中，请求发送器 930 触发计算器 940，由计算器 940 计算终端的硬件 ID。具体地，

计算器 940 首先获取终端的 IMEI，记为第一字符串。其次，计算器 940 获取被盗移动终端的网卡地址，并去除网卡地址中的非字母以及非数字字符，去除后的网卡地址记为第二字符串。计算器 940 获取到第一字符串以及第二字符串之后，获取终端的 CPU 串号，记为第三字符串。获取到第一、第二以及第三字符串之后，计算器 940 按预定顺序合并上述三个字符串。其中，该预定顺序可以是按第一、第二、第三的顺序合并上述三个字符串，可以是按第三、第二、第一的倒序合并上述三个字符串，还可以是其他预定的顺序，本发明实施例对此并不加以限定。

合并上述字符串之后，计算器 940 将合并后得到的结果转换为大写格式，并记为第一结果。获取到第一结果之后，计算器 940 将该第一结果进行 MD5 运算，得到第二结果。之后，计算器 940 将该第二结果转换为大写格式得到终端的硬件 ID。

本发明实施例中终端的硬件 ID 通过将终端的 IMEI、网卡地址以及 CPU 的串号进行合并运算能够保证服务器接收的状态修改消息是真实有效可信的，避免接收来自不可信或恶意发送端伪装成终端发送的状态修改消息导致服务器对终端的状态信息进行错误修改。例如，若不可信或恶意发送端伪装成终端发送状态修改消息指示服务器将终端的状态信息从被盗修改为解除被盗。当终端的状态信息修改为解除被盗之后，不法分子可以对终端进行刷机处理，导致失主无法找回终端的恶劣后果。本发明实施例将接收到的状态修改消息中携带的硬件 ID 与服务器本地存储的硬件 ID 进行匹配，若硬件 ID 匹配，则终端的 IMEI、网卡地址以及 CPU 串号均能够匹配，则能够确定本发明实施例接收到的状态修改消息的合法性。确定状态修改消息的合法性之后，对终端的状态信息进行修改保证服务器存储的终端的状态信息能够及时更新。

在本实施例中，被盗终端的处理客户端（参见图 9）能够接收来自服务器方的状态修改消息，并对其进行验证。当验证通过时，发送该状态修改请求转发至服务器。即，本实施例中，被盗终端的处理客户端的功能为验证状态修改消息的合法性。

根据上述任意一个优选实施例或多个优选实施例的组合，本发明实施例能够达到如下有益效果：

本发明实施例接收来自发送方的状态修改消息，并将其转发至对应的终端，由终端对该状态修改消息进行验证，保证收到的状态修改消息是真实有效可信的消息，避免接收来自不可信或恶意的发送方发送的状态修改消息，导致终端的状态信息被恶意修改。若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。终端验证状态修改消息合法之后，本发明实施例接收终端返回的状态修改请求，并根据该状态修改请求对终端的状态信息进行修改，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如，当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。

因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

实施例三

5 本实施例提供了一种被盗终端的处理方法。图 10 示出了根据本发明一个实施例的被盗终端的处理方法的处理流程图。如图 10 所示，该流程至少包括步骤 S1002 至步骤 S1006。

步骤 S1002、接收来自发送方的状态修改消息，其中，状态修改消息中携带有终端的身份标识信息以及终端的当前状态。

步骤 S1004、利用服务器对状态修改消息进行合法性验证。

10 步骤 S1006、根据通过合法性验证的状态修改消息修改身份标识信息对应的终端的状态信息至当前状态。

本发明实施例接收来自发送方的状态修改消息，并对该状态修改消息进行验证，保证收到的状态修改消息是真实有效可信的消息，避免接收来自不可信或恶意的发送方发送的状态修改消息，导致终端的状态信息被恶意修改。若终端的状态信息被恶意修改，
15 可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。状态修改消息通过合法性验证之后，本发明实施例根据该状态修改消息对终端的状态信息进行修改，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改
20 被盗终端的状态信息。例如，当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

如图 10 中的步骤 S1002 以及步骤 S1004 所示，接收到来自发送方的状态修改消息之
25 后，为保证接收的状态修改消息是真实有效可信的，避免接收来自不可信或恶意发送端发送的状态修改消息导致服务器对终端的状态信息进行错误修改，本发明实施例利用服务器对状态修改消息进行合法性验证。

上文提及，来自发送方的状态修改消息中携带有终端的身份标识信息，本发明实施例利用该终端的身份标识信息与服务器本地存储的身份标识信息是否匹配对状态修改消息的合法性进行验证。具体地，若状态修改消息中携带的终端的身份标识信息与服务器本地存储的身份标识信息能够匹配，则状态修改消息合法；若状态修改消息中携带的终端的身份标识信息与服务器本地存储的身份标识信息不能够匹配，则状态修改消息不合法。
30

根据对状态修改消息的验证结果，本发明实施例执行不同的操作。若状态修改消息
35 不合法，则本发明实施例无法保证服务器接收到的状态修改消息是真实有效可信的，并且无法保证状态修改消息的发送方不是不可信或恶意发送端。因此，当经本发明实施例

验证，状态修改消息不合法时，为保证服务器不会根据来自不可信方的状态修改消息对终端的状态信息进行错误修改，本发明实施例忽略接收到的状态修改信息，不执行任何操作。

若状态修改消息合法，则本发明实施例根据状态修改消息中携带的终端的标识信息确定该标识信息对应的终端。确定对应的终端之后，本发明实施例根据状态修改消息中该终端的当前状态对服务器本地存储的终端的状态信息进行对应修改，保证服务器存储的终端的状态信息能够得到及时更新。

本发明实施例中，终端的当前状态可以包括终端被盗以及终端未被盗、终端被盗后找回等等。当终端被盗之后，本发明实施例对终端的状态信息进行及时修改，以便服务器接收到终端的相关信息（如终端的实时位置、终端当前使用者的指纹等）之后，能够向失主提供被盗终端的相关线索，增加失主找回终端的可能性。当终端被盗后找回之后，本发明实施例及时修改终端的状态为被盗后找回，服务器也就无需浪费空间等资源查询以及存储终端的相关信息。进一步，本发明实施例的终端的当前状态还可以包括其他更为详细的说明，例如包括终端未出售、终端使用中以及终端被转卖等终端的出售购买状态信息，还可以是其他任意终端的当前状态信息，本发明实施例对此并不加以限定。

优选地，将终端的状态信息修改为当前状态之后，本发明实施例返回修改结果至状态修改信息的发送方。本发明实施例中，对终端的当前状态修改之后，将修改结果发送至发送方，提醒发送方该终端的当前状态已修改，进而使得发送方能够根据终端修改后的当前状态执行相应操作。例如，当终端为手机时，用户使用与被盗手机绑定的亲友号码发送状态修改消息至被盗手机，标记手机已被盗。当服务器根据状态修改消息修改手机当前状态为已被盗之后，若返回修改结果至亲友号码，则用户能够及时获知手机已标记被盗，进一步对被盗手机执行其他防盗操作。

本发明实施例中，终端的身份标识信息可以是终端的 IMEI，可以是终端的 ID，还可以是任意能够唯一标识终端的身份标识信息，本发明实施例对此并不加以限定。

为提高终端的安全性，确定接收到的状态修改消息为合法状态修改消息，优选地，本发明实施例提供一种终端身份标识。该终端身份标识为终端的硬件 ID。由于硬件 ID 的获取包括了对终端的 IMEI、终端的网卡地址以及终端的 CPU 串号进行的综合运算，因此，硬件 ID 是终端的一个综合的身份标识。将硬件 ID 作为终端的身份标识对状态修改消息进行合法性验证，若状态修改消息通过验证，则表明状态修改消息中携带的终端的 IMEI、终端的网卡地址以及终端的 CPU 串号均通过验证，对状态修改消息的合法性有了更高的保证。其中，硬件 ID 的计算方法请参见实施例一。

另外，本发明实施例中，状态修改消息的发送方可以设置于移动终端，例如手机，笔记本电脑等等，并通过短信息或者网络的形式发送状态修改消息。本发明实施例中的发送方还可以设置于终端，例如电脑，并通过网络的形式发送上述状态修改消息。采用本发明实施例，能够及时修改终端的状态信息。例如，当终端被盗之后，用户能够通过各种消息发送平台发送状态修改消息，保证及时标记终端被盗。进一步能够及时获知被

盗终端的相关信息，增大被盗终端找回的机率。

现以具体实施例对本发明的被盗终端的处理方法进行进一步说明。

图 11 示出了根据本发明一个优选实施例的被盗终端的处理方法的处理流程图，支持上述任意一个被盗终端的处理方法，将上述被盗终端的处理方法阐述得更加清晰易懂。

5 参见图 11，该流程至少包括步骤 S1102 至步骤 S1110。

需要说明的是，为将本优选实施例阐述得更加简单明白，本优选实施例中，将状态修改消息的发送方设置于亲友手机，将终端设置为被盗手机，其中，亲友手机为被盗手机绑定的亲友号码所在的手机。

步骤 S1102、发送状态修改消息，标记手机被盗。

10 具体地，用户发现手机被盗之后，能够通过预先与被盗手机绑定的亲友号码的手机发送状态修改消息至服务器。使用亲友手机时，本优选实施例能够通过短信息发送该状态修改信息至服务器。并且，发送至服务器的状态修改消息中携带有被盗手机的身份标识信息。

步骤 S1104、判断状态修改消息是否合法。

15 服务器接收到状态修改消息之后，对该状态修改消息进行合法性验证。若状态修改消息中携带的身份标识信息与服务器本地存储的身份标识信息不能够匹配，则服务器判断状态修改消息不能通过合法性验证，则执行步骤 S1106。若状态修改消息中携带的身份标识信息与服务器本地存储的身份标识信息能够匹配，则服务器判断状态修改消息通过合法性验证，则执行步骤 S1108。

20 步骤 S1106、状态修改消息未通过合法性验证，服务器忽略状态修改消息。

步骤 S1108、状态修改消息通过合法性验证，服务器根据状态修改消息修改被盗手机的状态信息。

当服务器判断状态修改消息通过验证之后，服务器根据该状态修改消息修改被盗手机的状态信息为手机已被盗。

25 步骤 S1110、返回修改结果。

服务器对被盗手机的状态信息修改完毕之后，通过短信息发送修改结果至状态修改消息的发送方，即本优选实施例中的亲友手机或个人电脑。状态修改消息的发送方接收到服务器返回的修改结果之后，确定已成功标记手机被盗。

30 图 12 示出了根据本发明另一个优选实施例的被盗终端的处理方法的处理流程图，永远支持上述任意一个被盗终端的处理方法，将上述被盗终端的处理方法阐述得更加清晰易懂。参见图 12，该流程至少包括步骤 S1202 至步骤 S1210。

需要说明的是，为将本优选实施例阐述得更加简单明白，本优选实施例中，将状态修改消息的发送方设置于个人电脑，将终端设置为被盗手机。

步骤 S1202、发送状态修改消息，标记手机被盗。

35 具体地，用户发现手机被盗之后，能够通过个人电脑发送状态修改消息至服务器。使用个人电脑时，本优选实施例能够通过网络发送状态修改消息至服务器。并且，发送

至服务器的状态修改消息中携带有被盗手机的身份标识信息。

步骤 S1204、判断状态修改消息是否合法。

服务器接收到状态修改消息之后，对该状态修改消息进行合法性验证。若状态修改消息中携带的身份标识信息与服务器本地存储的身份标识信息不能够匹配，则服务器判断状态修改消息不能通过合法性验证，则执行步骤 S1206。若状态修改消息中携带的身份标识信息与服务器本地存储的身份标识信息能够匹配，则服务器判断状态修改消息通过合法性验证，则执行步骤 S1208。

步骤 S1206、状态修改消息未通过合法性验证，服务器忽略状态修改消息。

步骤 S1208、状态修改消息通过合法性验证，服务器根据状态修改消息修改被盗手机的状态信息。

当服务器判断状态修改消息通过验证之后，服务器根据该状态修改消息修改被盗手机的状态信息为手机已被盗。

步骤 S1210、返回修改结果。

服务器对被盗手机的状态信息修改完毕之后，通过网络发送修改结果至状态修改消息的发送方，即本优选实施例中的亲友手机或个人电脑。状态修改消息的发送方接收到服务器返回的修改结果之后，确定已成功标记手机被盗。

图 13 示出了根据本发明又一个优选实施例的被盗终端的处理方法的处理流程图，支持上述任意一个被盗终端的处理方法，将上述被盗终端的处理方法阐述得更加清晰易懂。参见图 13，该流程至少包括步骤 S1302 至步骤 S1310。

需要说明的是，为将本优选实施例阐述得更加简单明白，本优选实施例中，将状态修改消息的发送方设置于亲友手机，将终端设置为被盗手机，其中，亲友手机为被盗手机绑定的亲友号码所在的手机。

步骤 S1302、发送状态修改消息，标记手机被盗。

具体地，用户发现手机被盗之后，能够通过预先与被盗手机绑定的亲友号码的手机发送状态修改消息至服务器。使用亲友手机时，本优选实施例能够通过网络发送该状态修改信息至服务器。并且，发送至服务器的状态修改消息中携带有被盗手机的身份标识信息。

步骤 S1304、判断状态修改消息是否合法。

服务器接收到状态修改消息之后，对该状态修改消息进行合法性验证。若状态修改消息中携带的身份标识信息与服务器本地存储的身份标识信息不能够匹配，则服务器判断状态修改消息不能通过合法性验证，则执行步骤 S1306。若状态修改消息中携带的身份标识信息与服务器本地存储的身份标识信息能够匹配，则服务器判断状态修改消息通过合法性验证，则执行步骤 S1308。

步骤 S1306、状态修改消息未通过合法性验证，服务器忽略状态修改消息。

步骤 S1308、状态修改消息通过合法性验证，服务器根据状态修改消息修改被盗手机的状态信息。

当服务器判断状态修改消息通过验证之后，服务器根据该状态修改消息修改被盗手机的状态信息为手机已被盗。

步骤 S1310、返回修改结果。

服务器对被盗手机的状态信息修改完毕之后，通过网络发送修改结果至状态修改消息的发送方，即本优选实施例中的亲友手机或个人电脑。状态修改消息的发送方接收到服务器返回的修改结果之后，确定已成功标记手机被盗。

基于上文各优选实施例提供的被盗终端的处理方法，基于同一发明构思，本发明实施例提供了一种服务器，用于实现上述被盗终端的处理方法。

图 14 示出了根据本发明一个实施例的服务器的结构示意图。参见图 14，本发明实施例的服务器至少包括：接收器 1410、判断器 1420 以及状态修改器 1430。

现介绍本发明实施例的服务器的各器件或组成的功能以及各部分间的连接关系：

接收器 1410，配置为接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有终端的身份标识信息以及终端的当前状态。

判断器 1420，与接收器 1410 相耦合，配置为判断状态修改消息是否通过合法性验证。

状态修改器 1430，与判断器 1420 相耦合，配置为根据通过合法性验证的状态修改消息修改身份标识信息对应的终端的状态信息至当前状态。

本发明实施例接收来自发送方的状态修改消息，并对该状态修改消息进行验证，保证收到的状态修改消息是真实有效可信的消息，避免接收来自不可信或恶意的发送方发送的状态修改消息，导致终端的状态信息被恶意修改。若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。状态修改消息通过合法性验证之后，本发明实施例根据该状态修改消息对终端的状态信息进行修改，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如，当终端被盗之后，采用本发明实施例能够更改终端的当前状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

如图 14 所示的服务器，接收器 1410 接收来自发送方的状态修改消息，其中，该状态修改消息中携带有状态信息发生改变的终端的身份标识。接收器 1410 接收到来自发送方的状态修改消息之后，为保证接受的状态修改消息是真实有效可信的，避免接收来自不可信或恶意发送端发送的状态修改消息导致服务器对终端的状态信息进行错误修改，接收器 1410 触发判断器 1420。判断器 1420 受到触发之后，对状态修改消息能够通过合法性进行判断。具体地，若状态修改消息中携带的终端的身份标识信息与服务器本地存储的终端的身份标识信息能够匹配，则判断器 1420 判断状态修改消息通过合法性验证。若状态修改消息中携带的终端的身份标识信息与服务器本地存储的终端的身份标识信息

不能够匹配, 则判断器 1420 判断状态修改消息未通过合法性验证。

判断器 1420 对接收器 1410 接收到的状态修改消息进行验证之后, 若状态修改消息未通过验证, 则服务器无法保证服务器接收到的状态修改消息是真实有效可信的, 并且无法保证状态修改消息的发送方不是不可信或恶意发送端。因此, 判断器 1420 判断状态
5 验证信息不合法时, 为保证服务器不会根据来自不可信方的状态修改消息对终端的状态信息进行错误修改, 服务器忽略该状态修改消息, 不执行任何操作。若判断器 1420 判断状态修改消息合法, 则触发与判断器 1420 耦合的状态修改器 1430。状态修改器收到触发之后, 根据状态修改消息中携带的终端的身份标识信息确定对应的终端。终端确定之后, 状态修改器 1420 根据状态修改消息对服务器本地存储的终端的状态信息进行修改, 保证
10 对终端的状态信息进行及时更新。

本发明实施例中, 终端的当前状态可以包括终端被盗以及终端未被盗、终端被盗后找回等等。当终端被盗之后, 状态修改器 1420 对终端的状态信息进行及时修改, 以便服务器接收到终端的相关信息 (如终端的实时位置、终端当前使用者的指纹等) 之后, 能够向失主提供被盗终端的相关线索, 增加失主找回终端的可能性。当终端被盗后找回之
15 后, 服务器中的状态修改器 1420 及时修改终端的状态为被盗后找回, 服务器也就无需浪费空间等资源查询以及存储终端的相关信息。进一步, 本发明实施例的终端的当前状态还可以包括其他更为详细的说明, 例如包括终端未出售、终端使用中以及终端被转卖等终端的出售购买状态信息, 还可以是其他任意终端的当前状态信息, 本发明实施例对此并不加以限定。

20 优选地, 状态修改器 1420 将终端的状态信息修改为当前状态之后, 触发发送器 1440。发送器 1440 返回修改结果状态修改信息的发送方。本发明实施例中, 对终端的当前状态修改之后, 由发送器 1440 将修改结果发送至发送方, 提醒发送方该终端的当前状态已修改, 进而使得发送方能够根据终端修改后的当前状态执行相应操作。例如, 当终端为手机时, 用户使用与被盗手机绑定的亲友号码发送状态修改消息至被盗手机, 标记手机已
25 被盗。当服务器根据状态修改消息修改手机当前状态为已被盗之后, 若返回修改结果至亲友号码, 则用户能够及时获知手机已标记被盗, 进一步对被盗手机执行其他防盗操作。

本发明实施例中, 终端的身份标识信息可以是终端的 IMEI, 可以是终端的用户 ID, 还可以是任意能够唯一标识终端的身份标识信息, 本发明实施例对此并不加以限定。

为提高终端的安全性, 确定接收到的状态修改消息为合法状态修改消息, 优选地,
30 本发明实施例提供一种终端身份标识。该终端身份标识为终端的硬件 ID。由于硬件 ID 的获取包括了对终端的 IMEI、终端的网卡地址以及终端的 CPU 串号进行的综合运算, 因此, 硬件 ID 是终端的一个综合的身份标识。将硬件 ID 作为终端的身份标识对状态修改消息进行合法性验证, 若状态修改消息通过验证, 则表明状态修改消息中携带的终端的 IMEI、终端的网卡地址以及终端的 CPU 串号均通过验证, 对状态修改消息的合法性
35 有了更高的保证。其中硬件 ID 的计算方式请参见实施例一。

另外, 本发明实施例中, 状态修改消息的发送方可以设置于移动终端, 例如手机,

笔记本电脑等等，并通过短信息或者网络的形式发送状态修改消息。本发明实施例中的发送方还可以设置于终端，例如电脑，并通过网络的形式发送上述状态修改消息。采用本发明实施例，能够及时修改终端的状态信息。例如，当终端被盗之后，用户能够通过各种消息发送平台发送状态修改消息，保证及时标记终端被盗。进一步能够及时获知被

5 盗终端的相关信息，增大被盗终端找回的机率。

在本实施例中，服务器（参见图 14）接收来自发送方的状态修改消息，对其进行身份验证，在验证通过时对其进行修改。即，在本发明实施例中，服务器的功能是用于验证状态修改消息，以及验证通过后根据相应请求修改本地存储的终端的状态信息。

根据上述任意一个优选实施例或多个优选实施例的组合，本发明实施例能够达到如下有益效果：

10 下有益效果：

本发明实施例接收来自发送方的状态修改消息，并对该状态修改消息进行验证，保证收到的状态修改消息是真实有效可信的消息，避免接收来自不可信或恶意的发送方发送的状态修改消息，导致终端的状态信息被恶意修改。若终端的状态信息被恶意修改，可能导致服务器反馈终端用户的实时位置至恶意发送方，泄露用户信息至恶意发送方，

15 或者可能导致被盗终端被解除被盗标识，进而无法得到被盗终端的相关信息，无法根据被盗终端的相关信息对偷盗者进行抓获。状态修改消息通过合法性验证之后，本发明实施例根据该状态修改消息对终端的状态信息进行修改，解决了现有技术中无法提供其他标识说明终端是否被盗的问题。采用本发明实施例提供的被盗终端的处理方法能够更改被盗终端的状态信息。例如，当终端被盗之后，采用本发明实施例能够更改终端的当前

20 状态为已被盗。若偷盗者对被盗终端进行交易，购买者能够查询到终端被盗，进而停止交易并提供偷盗者的线索。因此，采用本发明实施例能够达到增加被盗终端的找回机率并有效遏制偷盗行为的有益效果。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、

25 结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，

30 如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用

35 子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用

任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

5 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中
所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的
范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例
的任意之一都可以以任意的组合方式来使用。

10 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的
软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使
用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的多个设备中的一些
或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的
一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的
15 实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形
式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其
他形式提供。

例如，图 15 示出了可以实现根据本发明的被盗终端的处理方法的计算设备。该计算
设备传统上包括处理器 1510 和以存储器 1520 形式的计算机程序产品或者计算机可读介
质。存储器 1520 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、
20 硬盘或者 ROM 之类的电子存储器。存储器 1520 具有用于执行上述方法中的任何方法步
骤的程序代码 1531 的存储空间 1530。例如，用于程序代码的存储空间 1530 可以包括分
别用于实现上面的方法中的各种步骤的各个程序代码 1531。这些程序代码可以从一个或
者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计
算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样
25 的计算机程序产品通常为如参考图 16 所述的便携式或者固定存储单元。该存储单元可
以具有与图 15 的计算设备中的存储器 1520 类似布置的存储段、存储空间等。程序代码可
以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 1531’，即可以由例
如诸如 1510 之类的处理器读取的代码，这些代码当由计算设备运行时，导致该计算设备
执行上面所描述的方法中的各个步骤。

30 本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，
结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，
请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域
技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，
35 不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存
在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在

多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

- 5 此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

10

权 利 要 求

1. 一种被盗终端的处理方法，包括：

接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有本终端的当前
5 状态；

在所述状态修改消息合法的情况下，将所述状态修改消息转发至服务器，由所述服务器根据所述状态修改消息将所述服务器中存储的本终端的状态信息修改为所述当前状态。

2. 根据权利要求 1 所述的方法，其中，将所述状态修改消息转发至服务器之后，还
10 包括：

接收所述服务器返回的对本终端的状态信息的修改结果；
发送所述修改结果至所述发送方。

3. 根据权利要求 1 或 2 所述的方法，其中，按如下步骤判断所述状态修改消息是否
合法，包括：

15 判断所述发送方与本终端存储的可信任号码是否匹配；

若所述发送方与本终端存储的可信任号码不匹配，则所述状态修改消息不合法；

若所述发送方与本终端存储的可信任号码匹配，则所述状态修改消息合法。

4. 根据权利要求 3 所述的方法，其中，判断所述状态修改消息是否合法之后，还包
括：

20 若所述状态修改消息不合法，则忽略所述状态修改消息；

若所述状态修改消息合法，则获取本终端的身份标识信息；

将携带有所述身份标识信息的所述状态修改消息转发至所述服务器。

5. 根据权利要求 4 所述的方法，其中，将携带有所述身份标识信息的所述状态修改
消息转发至所述服务器之后，还包括：

25 利用所述服务器判断所述状态修改消息中携带的身份标识信息与所述服务器中存储
的身份标识信息是否匹配；

若所述状态修改消息中携带的身份标识信息与所述服务器中存储的身份标识信息均
不匹配，则忽略所述状态修改消息；

30 若所述状态修改消息中携带的身份标识信息与所述服务器中存储的身份标识信息匹
配，则触发所述服务器中的状态信息修改操作。

6. 根据权利要求 4 或 5 所述的方法，其中，所述身份标识信息至少包括下列任意之
一：

本终端的国际移动设备身份码 IMEI；

本终端的用户身份标识码 ID；

35 本终端的硬件身份标识码 ID。

7. 根据权利要求 6 所述的方法，其中，按如下步骤计算所述硬件 ID：

获取本终端的 IMEI，记为第一字符串；

获取本终端的网卡地址，将去除所述网卡地址中的非字母以及非数字字符的字符串记为第二字符串；

获取本终端的中央处理器 CPU 的串号，记为第三字符串；

- 5 按预定顺序合并所述第一字符串、所述第二字符串以及所述第三字符串，并转换合并后的字符串至大写格式，记为第一结果；

将所述第一结果进行消息摘要算法 MD5 运算得到第二结果；

转换所述第二结果至大写格式，得到所述硬件 ID。

8. 根据权利要求 1 至 7 任一项所述的方法，其中，所述发送方设置于移动终端。

- 10 9. 一种被盗终端的处理客户端，包括：

接收器，配置为接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有终端的当前状态；

合法判断器，配置为判断所述状态修改消息是否合法；

- 15 发送器，配置为在所述状态修改消息合法的情况下，将所述状态修改消息转发至服务器，由所述服务器根据所述状态修改消息将所述服务器中存储的所述终端的状态信息修改为所述当前状态。

10. 根据权利要求 9 所述的客户端，其中，还包括：

所述接收器还配置为，所述发送器将所述状态修改消息转发至服务器之后，接收所述服务器返回的对所述终端的状态信息的修改结果；以及

- 20 所述发送器还配置为，发送所述修改结果至所述发送方。

11. 根据权利要求 9 或 10 所述的客户端，其中，所述合法判断器还配置：

判断所述发送方与所述终端存储的可信任号码是否匹配；

若所述发送方与所述终端存储的可信任号码不匹配，则判断所述状态修改消息不合法；

- 25 若所述发送方与所述终端存储的可信任号码匹配，则判断所述状态修改消息合法。

12. 根据权利要求 11 所述的客户端，其中，所述发送器还配置为：

若所述状态修改消息不合法，则忽略所述状态修改消息；

若所述状态修改消息合法，则获取所述终端的身份标识信息，并将携带有所述身份标识信息的所述状态修改消息转发至所述服务器。

- 30 13. 根据权利要求 12 所述的客户端，其中，所述身份标识信息至少包括下列任意之一：

所述终端的国际移动设备身份码 IMEI；

所述终端的用户身份标识码 ID；

所述终端的硬件身份码 ID。

- 35 14. 根据权利要求 13 所述的客户端，其中，还包括：

计算器，配置为按如下步骤计算所述终端的硬件 ID：

获取所述终端的 IMEI，记为第一字符串；

获取所述终端的网卡地址，将去除所述网卡地址中的非字母以及非数字字符的字符串记为第二字符串；

获取所述终端的中央处理器 CPU 的串号，记为第三字符串；

- 5 按预定顺序合并所述第一字符串、所述第二字符串以及所述第三字符串，并转换合并后的字符串至大写格式，记为第一结果；

将所述第一结果进行消息摘要算法 MD5 运算得到第二结果；

转换所述第二结果至大写格式，得到所述终端的硬件 ID。

15. 一种服务器，包括：

- 10 命令接收器，配置为接收终端发送的状态修改消息，其中，所述状态修改消息中携带有所述终端的当前状态以及所述终端的身份标识信息；

状态修改器，配置为根据所述状态修改消息将本服务器中存储的所述终端的状态信息修改为所述当前状态。

16. 根据权利要求 15 所述的服务器，其中，还包括：

- 15 判断器，配置为所述命令接收器接收所述状态修改消息之后，判断所述终端的身份标识信息与本服务器中存储的身份标识信息是否匹配；

若不匹配，则判断所述状态修改消息不合法；

若匹配，则判断所述状态修改消息合法。

17. 根据权利要求 16 所述的服务器，其中，所述状态修改器还配置为：

- 20 若所述状态修改消息不合法，则忽略所述状态修改消息；

若所述状态修改消息合法，则将所述终端的状态信息修改为所述当前状态。

18. 根据权利要求 15 至 17 任一项所述的服务器，其中，还包括：

结果发送器，配置为所述状态修改器将所述终端的状态信息修改为所述当前状态之后，发送修改结果至所述终端。

- 25 19. 根据权利要求 15 至 18 任一项所述的服务器，其中，所述身份标识信息至少包括下列任意之一：

所述终端的国际移动设备身份码 IMEI；

所述终端的用户身份标识码 ID；

所述终端的硬件身份标识码 ID。

- 30 20. 一种被盗终端的处理方法，包括：

接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有状态发生改变的终端的身份标识信息；

将所述状态修改消息转发至所述终端的身份标识信息对应的终端，由所述终端对其进行验证；

- 35 根据所述终端验证所述状态修改消息通过时返回的状态修改请求，对所述终端的状态信息进行修改。

21. 根据权利要求 20 所述的方法, 其中, 所述接收来自发送方的状态修改消息之后, 还包括:

判断所述状态修改消息中携带的所述终端的身份标识信息与服务器本地存储的身份标识信息是否匹配;

5 根据匹配结果确定是否转发所述状态修改消息至终端。

22. 根据权利要求 21 所述的方法, 其中, 根据匹配结果确定是否转发状态修改消息至终端, 包括:

若所述状态修改消息中携带的所述终端的身份标识信息与所述服务器本地存储的身份标识信息均不匹配, 则忽略所述状态处理消息;

10 若所述状态修改消息中携带的所述终端的身份标识信息与所述服务器本地存储的身份标识信息匹配, 则转发所述状态修改消息至所述终端。

23. 根据权利要求 20 至 22 任一项所述的方法, 其中, 对所述终端的状态信息进行修改之后, 还包括:

返回对所述终端的状态信息的修改的执行情况至所述发送方。

15 24. 根据权利要求 23 所述的方法, 其中, 所述返回对所述终端的状态信息的修改的执行情况至所述发送方, 还包括:

发送执行修改所述终端的状态信息操作的任务身份标识码 ID 至所述发送方;

接收所述发送方发送的查询请求, 查询所述修改操作的执行情况, 其中, 所述查询请求中携带有所述任务 ID;

20 返回对所述终端的状态信息的修改的执行情况至所述发送方。

25. 根据权利要求 20 至 24 任一项所述的方法, 其中, 按如下步骤对所述状态修改消息进行验证, 包括:

利用所述终端判断所述状态修改消息中携带的所述终端的身份标识信息与所述终端中存储的身份标识信息是否匹配;

25 若匹配, 则所述状态修改消息合法;

若不匹配, 则所述状态修改消息不合法。

26. 根据权利要求 25 所述的方法, 其中, 对所述状态修改消息进行验证之后, 还包括:

若所述状态修改消息不合法, 则忽略所述状态修改消息;

30 若所述状态修改消息合法, 则获取所述终端的硬件身份标识码 ID, 并发送携带有所述硬件 ID 的所述状态修改请求至所述服务器。

27. 根据权利要求 26 所述的方法, 其中, 若所述状态修改消息合法, 按如下步骤计算所述硬件 ID:

获取所述终端的国际移动设备身份码 IMEI, 记为第一字符串;

35 获取所述终端的网卡地址, 将去除所述网卡地址中的非字母以及非数字字符的字符串记为第二字符串;

获取所述终端的中央处理器 CPU 的串号，记为第三字符串；

按预定顺序合并所述第一字符串、所述第二字符串以及所述第三字符串，并转换合并后的字符串至大写格式，记为第一结果；

将所述第一结果进行消息摘要算法 MD5 运算得到第二结果；

5 转换所述第二结果至大写格式，得到所述硬件 ID。

28 根据权利要求 20 至 27 任一项所述的方法，其中，所述终端验证所述状态修改消息通过时返回状态修改请求之后，还包括：

判断所述状态修改请求中携带的所述硬件 ID 与所述服务器中存储的硬件 ID 是否匹配；

10 若所述硬件 ID 与所述服务器中存储的硬件 ID 均不匹配，则忽略所述状态修改请求；
若所述硬件 ID 与所述服务器中存储的硬件 ID 匹配，则触发所述服务器对所述终端的状态信息进行修改的操作。

29. 根据权利要求 20 至 28 任一项所述的方法，其中，所述发送方设置于移动终端，并以短信息或者网络形式发送所述状态修改消息；或者

15 所述发送方设置于终端，并以网络形式发送所述状态修改消息。

30. 一种服务器，包括：

接收器，配置为接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有状态发生改变的终端的身份标识信息；

发送器，配置为将所述状态修改消息转发至所述终端的身份标识信息对应的终端，

20 由所述终端对其进行验证；

状态修改器，配置为根据所述终端验证所述状态修改消息通过时返回的状态修改请求，对所述终端的状态信息进行修改。

31. 根据权利要求 30 所述的服务器，其中，还包括：

判断器，配置为所述接收器接收来自发送方的状态修改消息之后，判断所述状态修改消息中携带的所述终端的身份标识信息与服务器本地存储的身份标识信息是否匹配。

25 32. 根据权利要求 31 所述的服务器，其中，所述发送器还配置为：

若根据所述判断器确定所述状态修改消息中携带的所述终端的身份标识信息与所述服务器本地存储的身份标识信息均未能匹配，忽略所述状态处理消息；

30 若根据所述判断器确定所述状态修改消息中携带的所述终端的身份标识信息与所述服务器本地存储的身份标识信息匹配，转发所述状态修改消息至所述终端。

33. 根据权利要求 30 至 32 任一项所述的服务器，其中，所述发送器还配置为：

对所述状态修改器对所述终端的状态信息进行修改之后，返回对所述终端的状态信息的修改的执行情况至所述发送方。

34. 根据权利要求 33 所述的服务器，其中，还包括：

35 所述发送器还配置为：发送执行修改所述终端的状态信息操作的任务身份标识码 ID 至所述发送方；

所述接收器还配置为，所述发送器发送所述任务 ID 至所述发送方之后，接收所述发送方发送的查询请求，查询所述修改操作的执行情况，其中，所述查询请求中携带有所述任务 ID；以及

所述发送器还配置为，返回对所述终端的状态信息的修改的执行情况至所述发送方。

5 35. 根据权利要求 30 至 34 任一项所述的服务器，其中，所述接收器还配置为：
接收所述终端发送的携带有所述终端的硬件身份标识码 ID 的状态修改请求。

36. 根据权利要求 35 所述的服务器，其中，所述判断器还配置为：

判断所述状态修改请求中携带的所述终端的硬件 ID 与所述服务器本地存储的硬件 ID 信息是否匹配。

10 37. 根据权利要求 36 所述的服务器，其中，所述状态修改器还配置为：

若根据所述判断器确定所述硬件 ID 与所述服务器本地存储的硬件 ID 信息均不匹配，则忽略所述状态修改请求；

若根据所述判断器确定所述硬件 ID 与所述服务器本地存储的硬件 ID 信息匹配，则对所述终端的状态进行修改。

15 38. 一种被盗终端的处理客户端，包括：

消息接收器，配置为接收服务器转发的、来自发送方的状态修改消息；

验证器，配置为对接收到的状态修改消息进行验证；

请求发送器，配置为所述状态修改消息通过验证之后，返回状态修改请求至所述服务器，由所述服务器根据所述状态修改请求对终端的状态进行修改。

20 39. 根据权利要求 38 所述的客户端，其中，所述验证器还配置为：

判断所述状态修改消息中携带的所述终端的身份标识信息与所述终端中存储的身份标识信息是否匹配，并得到匹配结果。

40. 根据权利要求 39 所述的客户端，其中，所述请求发送器还配置为：

若根据所述验证器确定所述匹配结果为不匹配，则忽略所述状态修改消息；

25 若根据所述验证器确定所述匹配结果为匹配，则获取所述终端的硬件身份标识码 ID，并发送携带有所述硬件 ID 的状态修改请求至所述服务器。

41. 根据权利要求 40 所述的客户端，其中，还包括：

计算器，配置为按如下步骤计算所述硬件 ID：

获取所述终端的国际移动设备身份码 IMEI，记为第一字符串；

30 获取所述终端的网卡地址，将去除所述网卡地址中的非字母以及非数字字符的字符串记为第二字符串；

获取所述终端的中央处理器 CPU 的串号，记为第三字符串；

按预定顺序合并所述第一字符串、所述第二字符串以及所述第三字符串，并转换合并后的字符串至大写格式，记为第一结果；

35 将所述第一结果进行消息摘要算法 MD5 运算得到第二结果；

转换所述第二结果至大写格式，得到所述终端的硬件 ID。

42. 一种被盗终端的处理方法，包括：

接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有终端的身份标识信息以及所述终端的当前状态；

利用服务器对所述状态修改消息进行合法性验证；

5 根据通过合法性验证的所述状态修改消息修改所述身份标识信息对应的终端的状态信息至所述当前状态。

43. 根据权利要求 42 所述的方法，其中，修改所述身份标识信息对应的终端的状态信息至所述当前状态之后，还包括：

返回对所述终端的状态信息进行修改的修改结果至所述发送方。

10 44. 根据权利要求 42 或 43 所述的方法，其中，利用服务器对所述状态修改消息进行合法性验证，包括：

利用所述服务器根据所述状态修改消息中携带的身份标识信息与所述服务器本地存储的身份标识信息是否匹配，验证所述状态修改消息是否合法；

15 若所述状态修改消息中携带的身份标识信息与所述服务器本地存储的身份标识信息均不匹配，则所述状态修改消息不合法；

若所述状态修改消息中携带的身份标识信息与所述服务器本地存储的身份标识信息匹配，则所述状态修改消息合法。

45. 根据权利要求 44 所述的方法，其中，对所述状态修改消息进行合法性验证之后，还包括：

20 若所述状态修改消息不合法，则忽略所述状态修改消息；

若所述状态修改消息合法，则触发所述状态信息修改操作。

46. 根据权利要求 42 至 45 任一项所述的方法，其中，所述终端的身份标识信息至少包括下列任意之一：

所述终端的国际移动设备身份码 IMEI；

25 所述终端的用户身份标识码 ID；

所述终端的硬件身份标识码 ID。

47. 根据权利要求 42 至 46 任一项所述的方法，其中，所述发送方设置于移动终端，并以短信息或网络形式发送所述状态修改消息；或者

所述发送方设置于终端，并以网络形式发送所述状态修改消息。

30 48. 一种服务器，包括：

接收器，配置为接收来自发送方的状态修改消息，其中，所述状态修改消息中携带有终端的身份标识信息以及所述终端的当前状态；

判断器，配置为判断所述状态修改消息是否通过合法性验证；

35 状态修改器，配置为根据通过合法性验证的所述状态修改消息修改所述身份标识信息对应的终端的状态信息至所述当前状态。

49. 根据权利要求 48 所述的服务器，其中，还包括：

发送器，配置为返回对所述终端的状态信息进行修改的修改结果至所述发送方。

50. 根据权利要求 48 或 49 所述的服务器，其中，所述判断器还配置为：

根据所述状态修改消息中携带的身份标识信息与所述服务器本地存储的身份标识信息是否匹配，判断所述状态修改消息是否通过合法性验证；

5 若所述状态修改消息中携带的身份标识信息与服务器本地存储的身份标识信息均不匹配，则所述判断器判断所述状态修改消息不合法；

若所述状态修改消息中携带的身份标识信息与所述服务器本地存储的身份标识信息匹配，则所述判断器判断所述状态修改消息合法。

51. 根据权利要求 50 所述的服务器，其中，所述状态修改器还配置为：

10 若所述判断器判断所述状态修改消息不合法，则忽略所述状态修改消息；

若所述判断器判断所述状态修改消息合法，则根据所述状态修改消息修改所述终端的状态信息。

52. 一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1-8 中的任一个所述的第一种被盗终端的处理方法，和/或，权利要求 20-29 中的任一个所述的第二种被盗终端的处理方法，和/或，
15 权利要求 42-47 中的任一个所述的第三种被盗终端的处理方法。

53. 一种计算机可读介质，其中存储了如权利要求 52 所述的计算机程序。

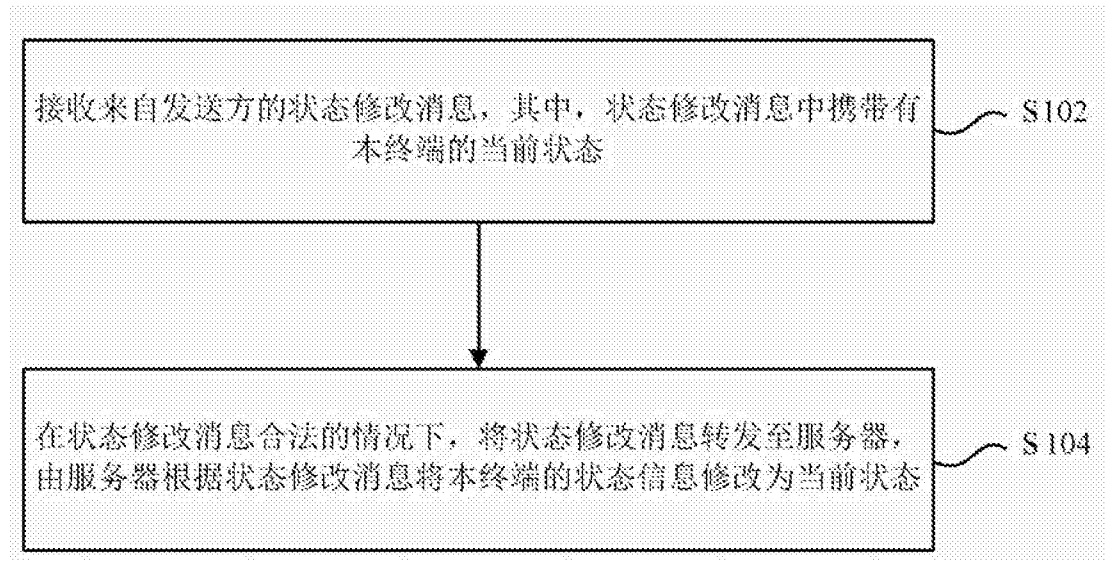


图 1

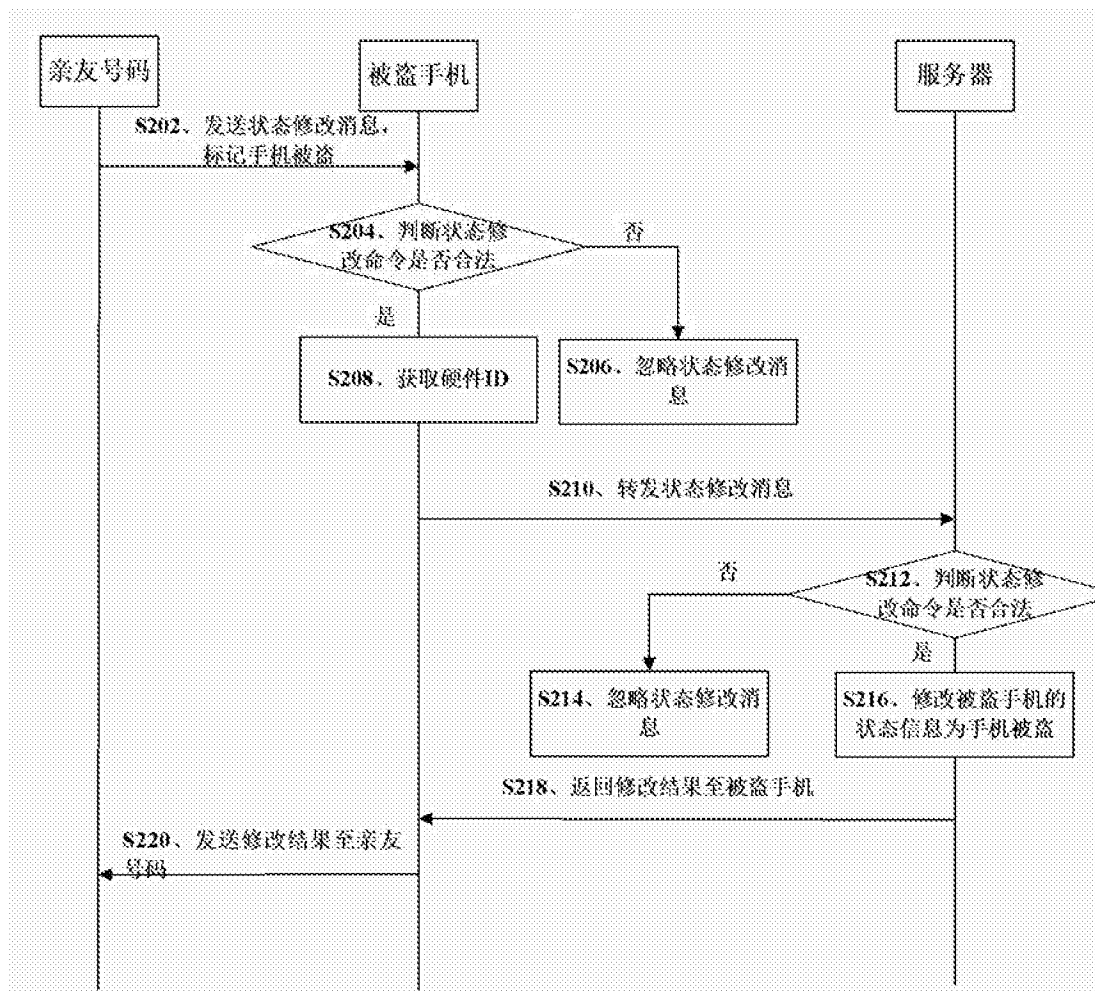


图 2

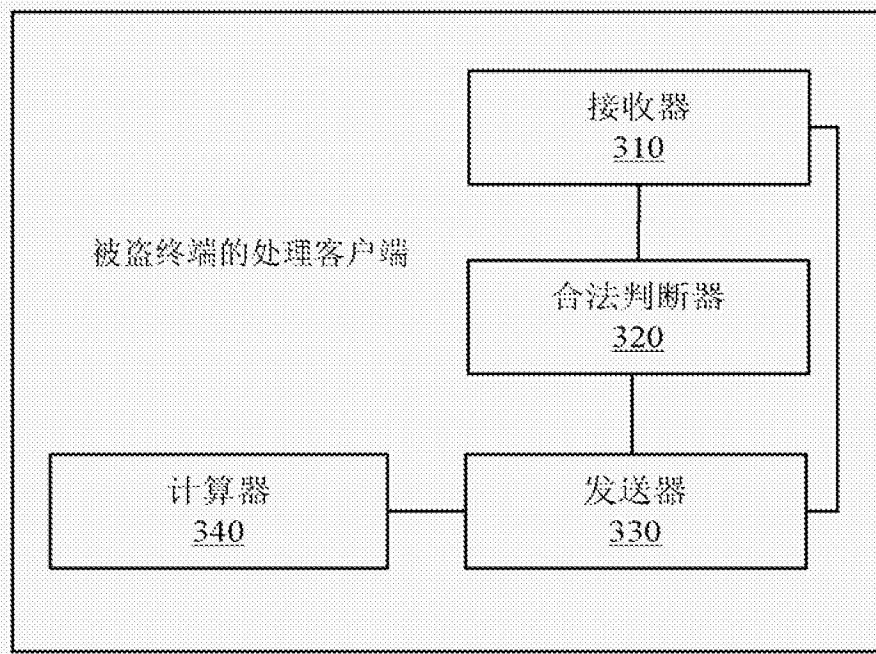


图 3

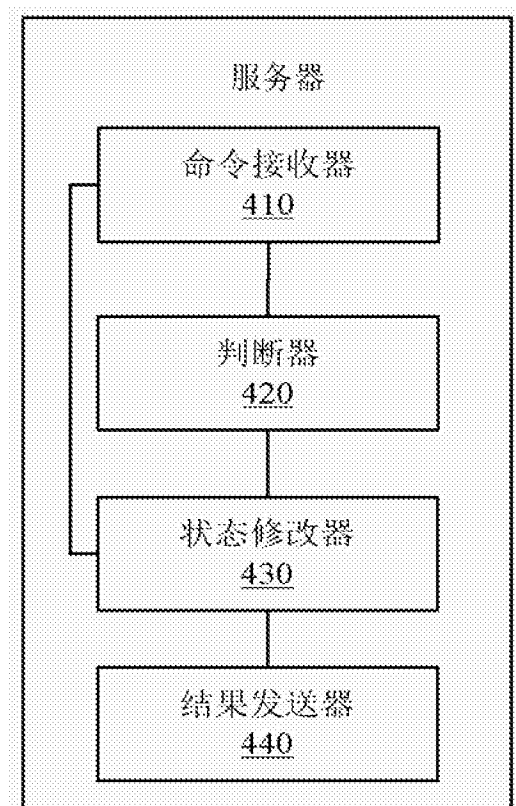


图 4

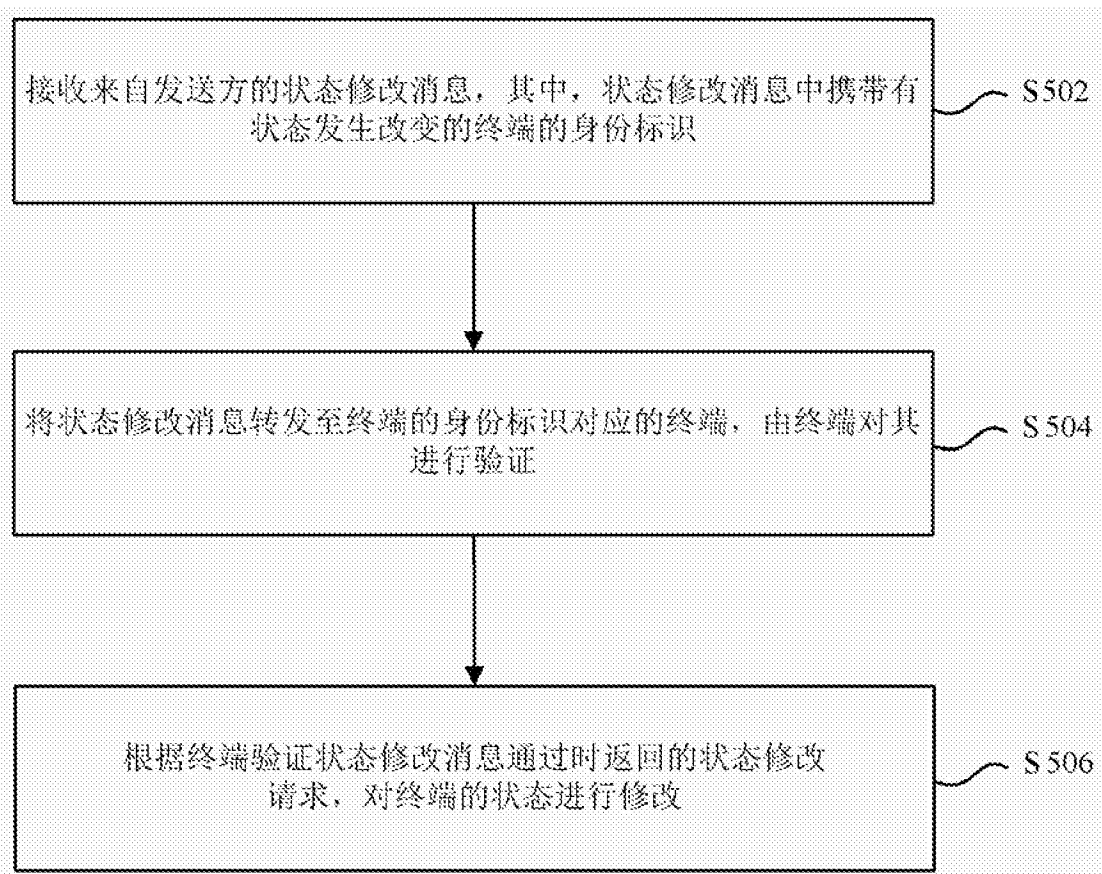


图 5

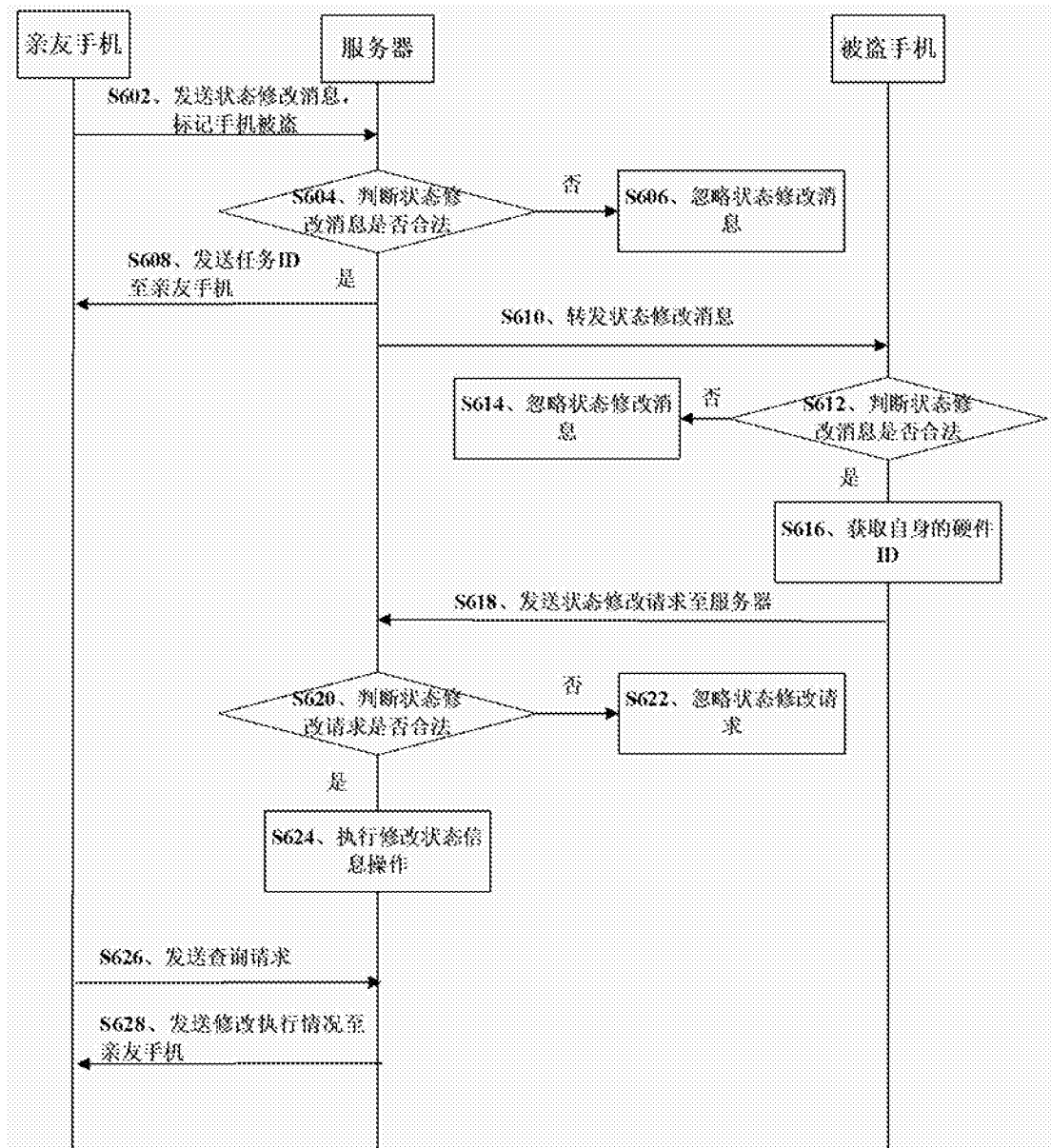


图 6

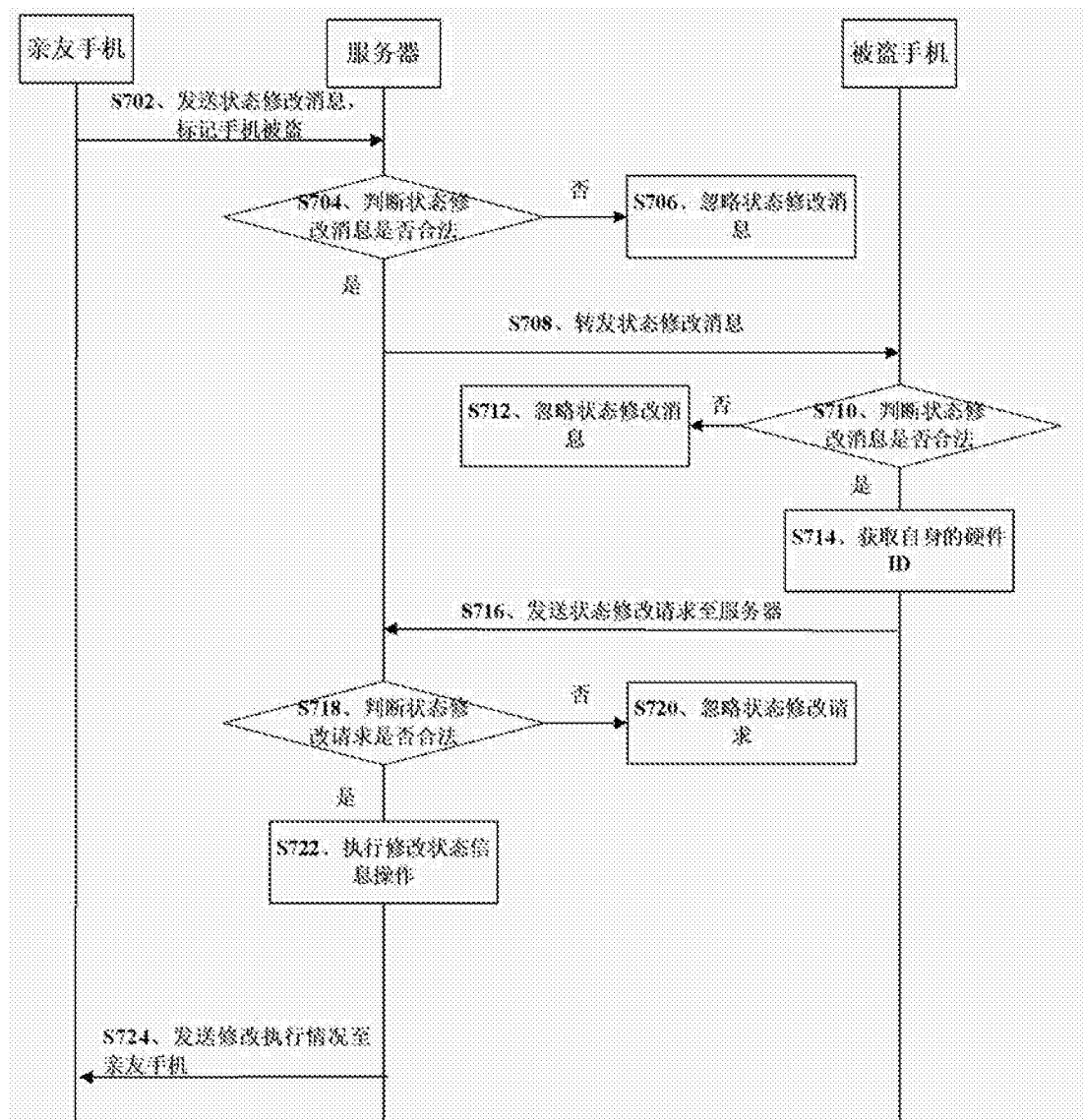


图 7

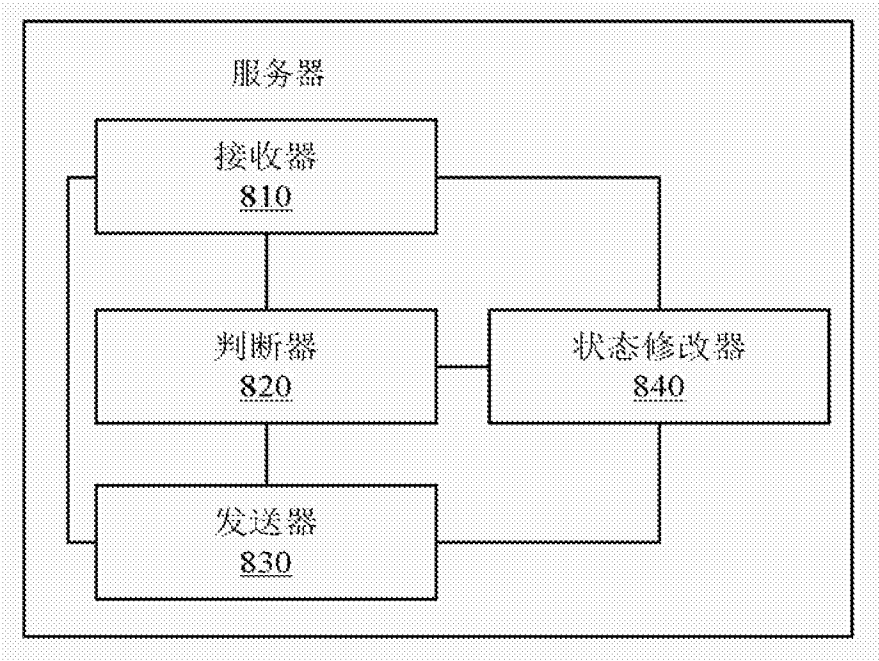


图 8

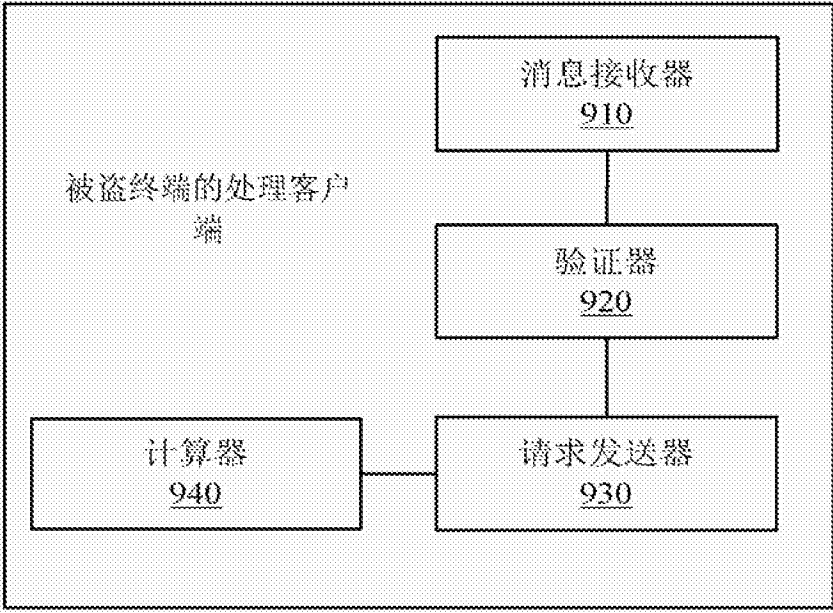


图 9

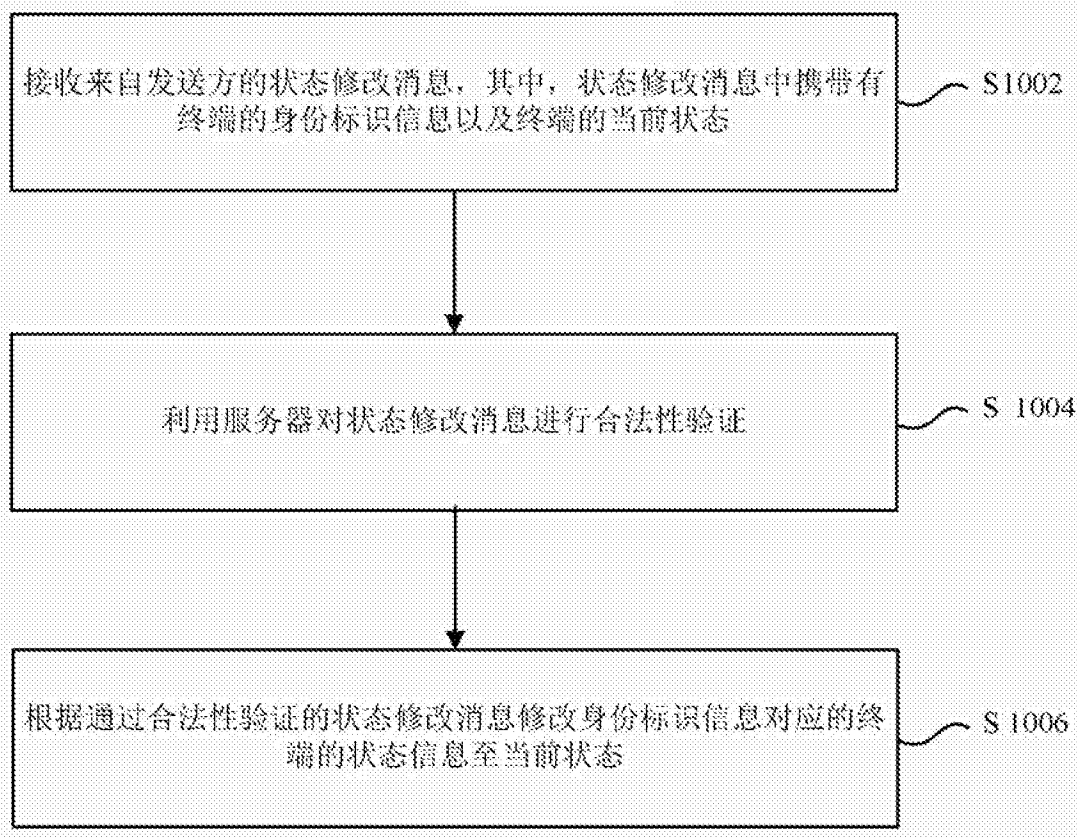


图 10

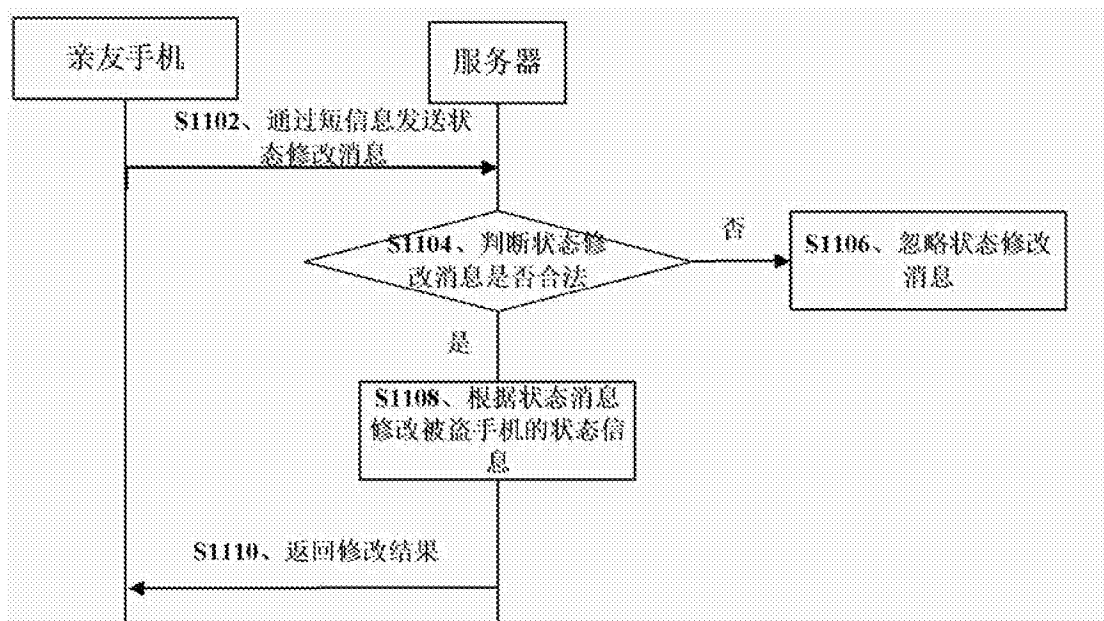


图 11

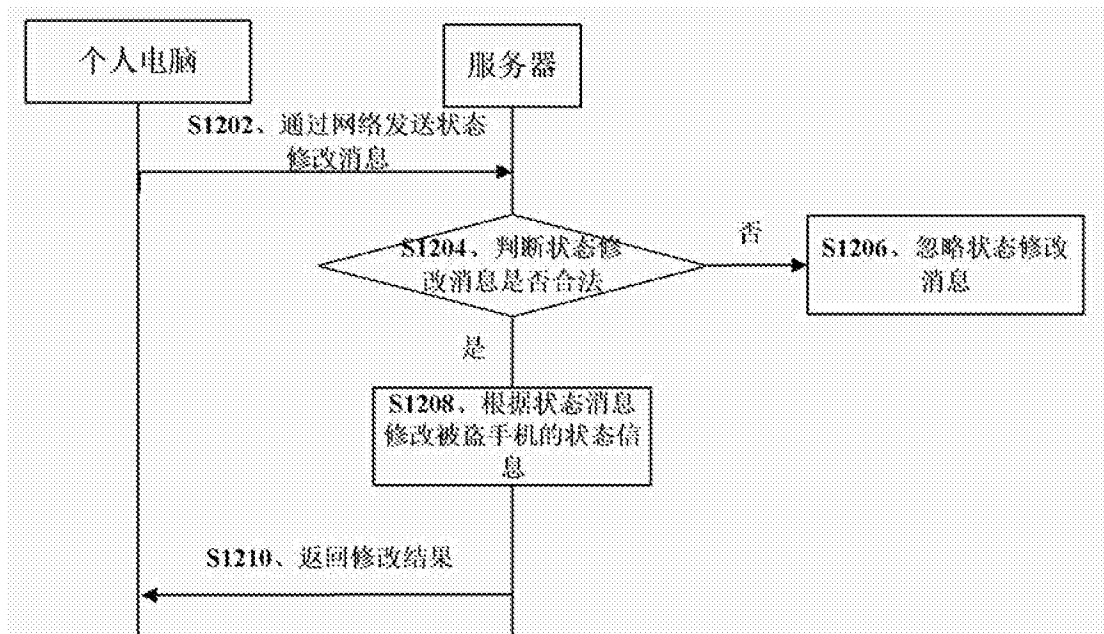


图 12

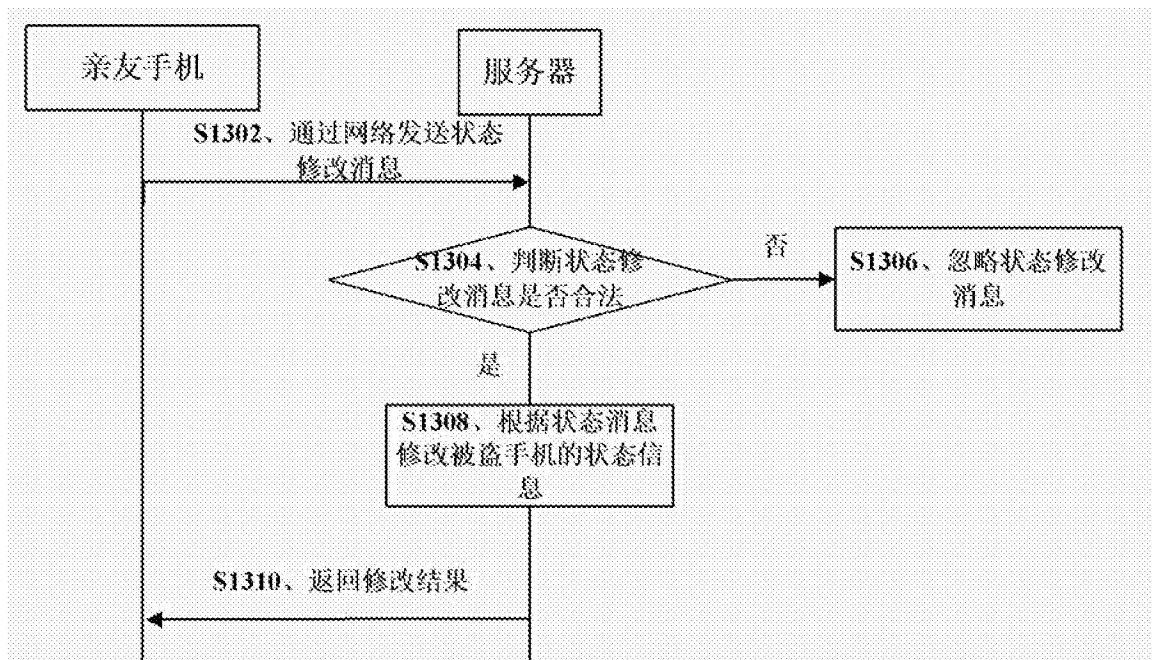


图 13

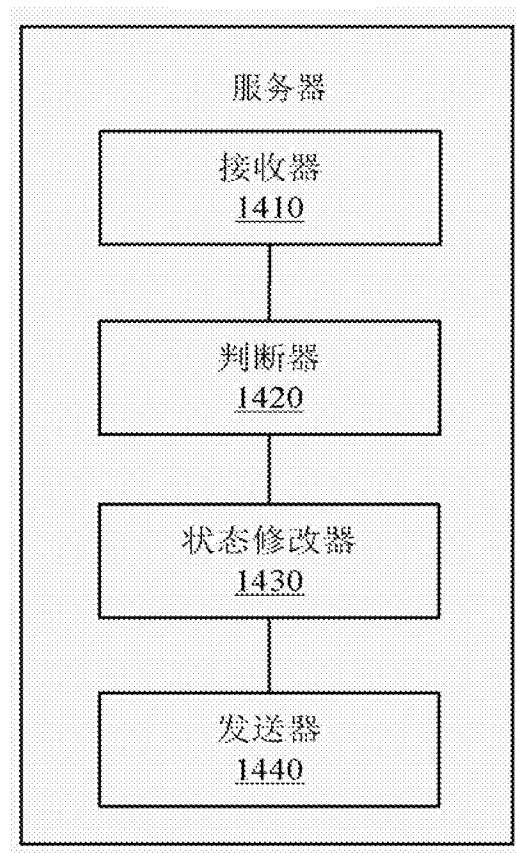


图 14

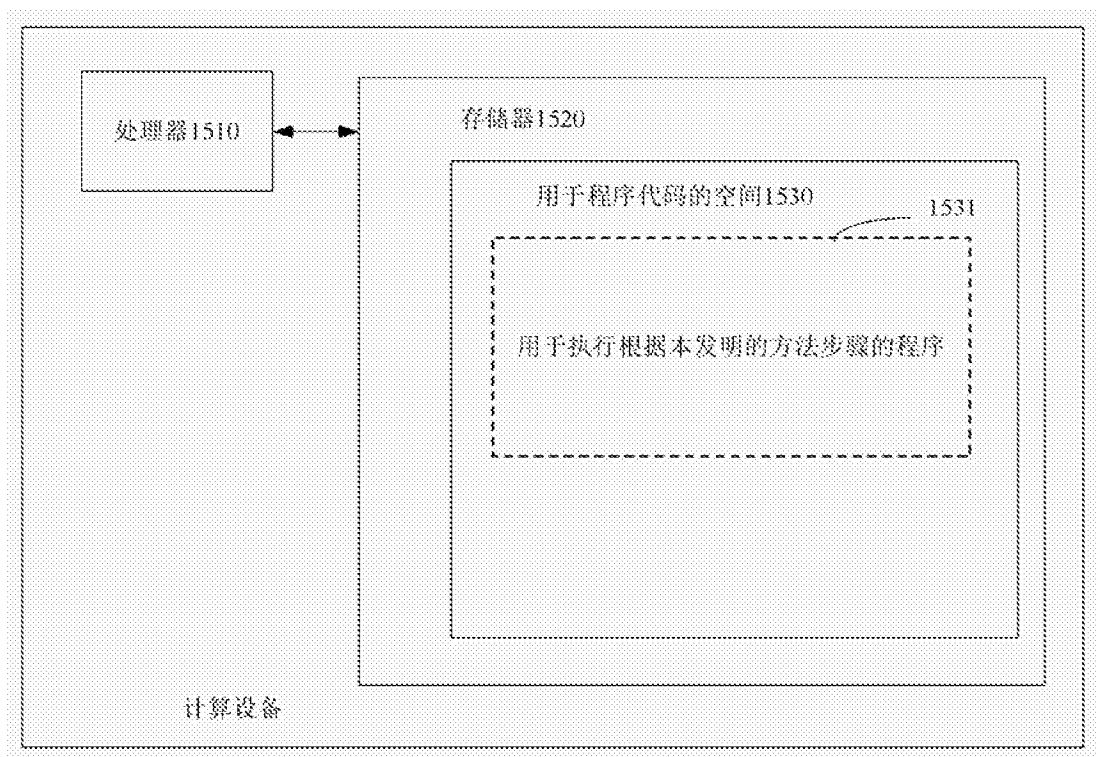


图 15

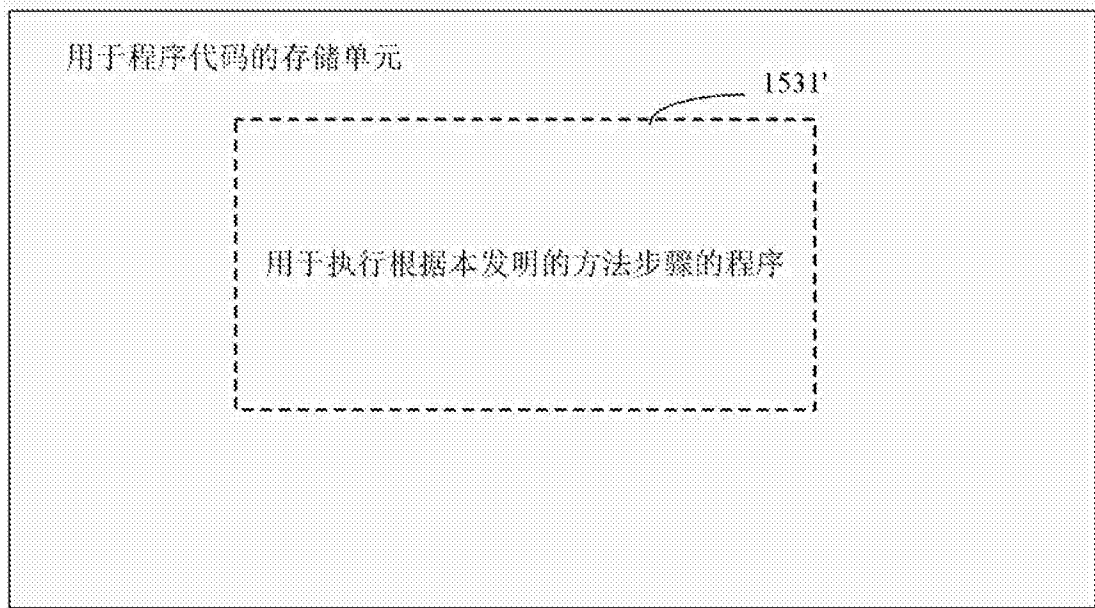


图 16

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/093637

A. CLASSIFICATION OF SUBJECT MATTER

H04W 8/22 (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

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)

CNXTX: mobile phone, modify, phone?, telephone, computer??. mobile, los+, state, send, transmit+, server, chang+, match+, legalit+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103702314 A (BEIJING QIHOO TECHNOLOGY CO., LTD.; QIZHI SOFTWARE (BEIJING) CO., LTD.), 02 April 2014 (02.04.2014), claims 1-10, and description, pages 2-3	1-19, 52-53
PX	CN 103702315 A (BEIJING QIHOO TECHNOLOGY CO., LTD.; QIZHI SOFTWARE (BEIJING) CO., LTD.), 02 April 2014 (02.04.2014), claims 1-10, and description, pages 2-3	20-41, 52-53
PX	CN 103699821 A (BEIJING QIHOO TECHNOLOGY CO., LTD.; QIZHI SOFTWARE (BEIJING) CO., LTD.), 02 April 2014 (02.04.2014), claims 1-10, and description, pages 2-3	42-53
X	CN 102843405 A (SHANGHAI BASECOM TECHNOLOGY CO., LTD.), 26 December 2012 (26.12.2012), abstract, and description, paragraphs [29] and [31]	1-2, 9-10, 15-26, 28, 30-40, 42-46, 48-53
Y	CN 102843405 A (SHANGHAI BASECOM TECHNOLOGY CO., LTD.), 26 December 2012 (26.12.2012), abstract, and description, paragraphs [29] and [31]	3-6, 8, 11-13, 29, 47

☒ 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 05 February 2015 (05.02.2015)	Date of mailing of the international search report 03 March 2015 (03.03.2015)
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 LIU, Huan Telephone No.: (86-10) 62411853

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2014/093637

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102833712 A (BEIJING XIAOMI TECHNOLOGY CO., LTD.), 19 December 2012 (19.12.2012), abstract, claim 1, and description, paragraphs [91]-[93] and [133]	3-6, 8, 11-13, 29, 47
A	CN 102780989 A (BEIJING XIAOMI TECHNOLOGY CO., LTD.), 14 November 2012 (14.11.2012), the whole document	1-53

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2014/093637

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103702314 A	02 April 2014	None	
CN 103702315 A	02 April 2014	None	
CN 103699821 A	02 April 2014	None	
CN 102843405 A	26 December 2012	None	
CN 102833712 A	19 December 2012	WO 2014032612 A1	06 March 2014
		US 2014094141 A1	03 April 2014
CN 102780989 A	14 November 2012	None	

国际检索报告

国际申请号

PCT/CN2014/093637

A. 主题的分类

H04W 8/22 (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

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))

CNTXT: 手机, 电脑, 移动, 丢失, 状态, 发送, 服务器, 修改, 改变, 匹配, 合法, phone?, telephone, computer?+, mobile, los+, state, send, transmit+, server, chang+, match+, legalit+

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
PX	CN 103702314 A (北京奇虎科技有限公司 奇智软件北京有限公司) 2014年 4月 2日 (2014 - 04 - 02) 权利要求1-10, 说明书第2-3页	1-19, 52-53
PX	CN 103702315 A (北京奇虎科技有限公司 奇智软件北京有限公司) 2014年 4月 2日 (2014 - 04 - 02) 权利要求1-10, 说明书第2-3页	20-41, 52-53
PX	CN 103699821 A (北京奇虎科技有限公司 奇智软件北京有限公司) 2014年 4月 2日 (2014 - 04 - 02) 权利要求1-10, 说明书第2-3页	42-53
X	CN 102843405 A (基信康信息技术上海有限公司) 2012年 12月 26日 (2012 - 12 - 26) 摘要、说明书第 [29], [31] 段	1-2, 9-10, 15-26, 28, 30-40, 42-46, 48-53
Y	CN 102843405 A (基信康信息技术上海有限公司) 2012年 12月 26日 (2012 - 12 - 26) 摘要、说明书第 [29], [31] 段	3-6, 8, 11-13, 29, 47

☒ 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

2015年 2月 5日

国际检索报告邮寄日期

2015年 3月 3日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
北京市海淀区蓟门桥西土城路6号
100088 中国

传真号 (86-10) 62019451

受权官员

刘欢

电话号码 (86-10) 62411853

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
Y	CN 102833712 A (北京小米科技有限责任公司) 2012年 12月 19日 (2012 - 12 - 19) 摘要、权利要求1、说明书第 [91] - [93] , [133] 段	3-6, 8, 11-13, 29, 47
A	CN 102780989 A (北京小米科技有限责任公司) 2012年 11月 14日 (2012 - 11 - 14) 全文	1-53

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2014/093637

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	103702314	A	2014年 4月 2日	无			
CN	103702315	A	2014年 4月 2日	无			
CN	103699821	A	2014年 4月 2日	无			
CN	102843405	A	2012年 12月 26日	无			
CN	102833712	A	2012年 12月 19日	WO	2014032612	A1	2014年 3月 6日
				US	2014094141	A1	2014年 4月 3日
CN	102780989	A	2012年 11月 14日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)