(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106332000 B
(45)授权公告日 2020.01.10

(21)申请号 201610672019.X

(22)申请日 2016.08.15

(65)同一申请的已公布的文献号
申请公布号 CN 106332000 A

(43)申请公布日 2017.01.11

(73)专利权人 宇龙计算机通信科技(深圳)有限公司
地址 518057 广东省深圳市南山区高新技术产业园(北区)梦溪道2号

(72)发明人 汤镇辉 牛溢华

(74)专利代理机构 广州三环专利商标代理有限公司 44202
代理人 郝传鑫 熊永强

(51)Int.Cl.
H04W 4/02(2018.01)
H04W 8/24(2009.01)
H04W 12/02(2009.01)
H04W 12/04(2009.01)
H04W 12/06(2009.01)

(56)对比文件
CN 105050046 A,2015.11.11,
CN 102413132 A,2012.04.11,
CN 103873260 A,2014.06.18,

审查员 赵小植

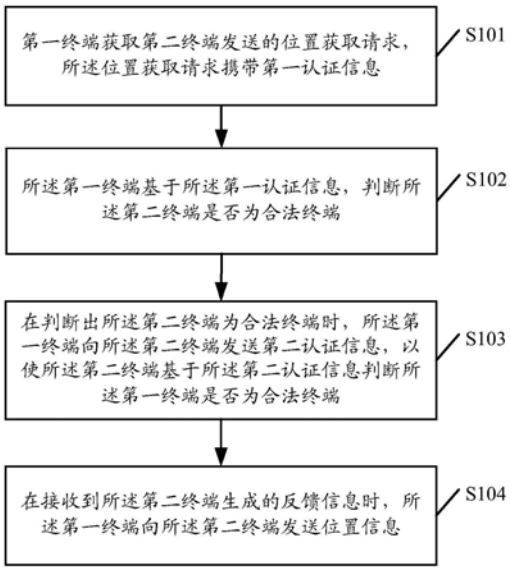
权利要求书2页 说明书10页 附图3页

(54)发明名称

一种终端位置信息获取方法及装置

(57)摘要

本发明实施例公开了一种终端位置信息获取方法及装置,其中的方法包括:第一终端获取第二终端发送的位置获取请求,位置获取请求携带第一认证信息;第一终端基于第一认证信息,判断第二终端是否为合法终端;在判断出第二终端为合法终端时,第一终端向第二终端发送第二认证信息,以使第二终端基于第二认证信息判断第一终端是否为合法终端;在接收到第二终端生成的反馈信息时,第一终端向第二终端发送位置信息,其中,反馈信息是第二终端判断出第一终端为合法终端时发送的。本发明实施例还公开了相应的终端位置信息获取装置。本发明实施例提供的技术方案能够在终端丢失时,获取终端的位置信息,进而找回终端,减小经济损失。



CN 106332000 B

1.一种终端位置信息获取方法,其特征在于,包括:

第一终端获取第二终端发送的位置获取请求,所述位置获取请求携带第一认证信息,所述第一认证信息是所述第二终端基于所述第一终端的账户标识、鉴权信息、所述第二终端的时间戳以及所述第二终端预存的加密函数以及所述第二终端预存的加密服务器秘钥生成的,所述第一认证信息包括加密账户标识、加密鉴权信息、所述第二终端的时间戳以及第一加密认证信息;

所述第一终端基于所述第一认证信息,判断所述第二终端是否为合法终端,所述所述第一终端基于所述第一认证信息,判断所述第二终端是否为合法终端包括:所述第一终端获取所述第一终端的时间戳,并判断所述第一终端的时间戳与所述第二终端的时间戳之间的差值是否小于预设时间段阈值;所述第一终端在判断出所述差值小于预设时间段阈值时,生成第二加密认证信息;所述第一终端判断所述第一加密认证信息与所述第二加密认证信息是否匹配;若所述第一加密认证信息与所述第二加密认证信息匹配,则所述第一终端判断所述第二终端为合法终端;

在判断出所述第二终端为合法终端时,所述第一终端向所述第二终端发送第二认证信息,以使所述第二终端基于所述第二认证信息判断所述第一终端是否为合法终端;

在接收到所述第二终端生成的反馈信息时,所述第一终端向所述第二终端发送位置信息,其中,所述反馈信息是所述第二终端基于所述第二认证信息判断出所述第一终端为合法终端时发送的。

2.如权利要求1所述的方法,其特征在于,所述第一终端获取第二终端发送的位置获取请求之前,所述方法还包括:

所述第一终端获取用户输入的账户标识以及与所述账户标识对应的鉴权信息;

所述第一终端向服务器发送注册请求;

所述第一终端接收所述服务器响应所述注册请求生成的加密函数以及加密服务器秘钥;

所述第一终端基于所述加密函数、加密服务器秘钥、账户标识以及鉴权信息,生成加密账户标识、加密鉴权信息以及第一加密注册信息,并将所述加密账户标识、加密鉴权信息以及第一加密注册信息发送至所述服务器,以使所述服务器基于加密账户标识、加密鉴权信息以及第一加密注册信息,生成第二加密注册信息,并判断所述第二加密注册信息与第一加密注册信息是否匹配;

所述第一终端接收所述服务器生成的用于表示所述第一终端注册成功的反馈消息,其中,所述反馈消息是所述服务器在判断出所述第二加密注册信息与第一加密注册信息匹配时发送的。

3.如权利要求1至2任一项所述的方法,其特征在于,所述在接收到所述第二终端生成的反馈信息时,所述第一终端向所述第二终端发送位置信息,包括:

所述第一终端响应所述第二终端生成的反馈信息,获取所述第一终端的位置信息;

所述第一终端将所述位置信息发送至所述第二终端。

4.一种终端位置信息获取装置,其特征在于,包括:

获取单元,用于获取第二终端发送的位置获取请求,所述位置获取请求携带第一认证信息,所述第一认证信息是所述第二终端基于第一终端的账户标识、鉴权信息、所述第二终

端的时间戳以及所述第二终端预存的加密函数以及所述第二终端预存的加密服务器秘钥生成的，所述第一认证信息包括加密账户标识、加密鉴权信息、所述第二终端的时间戳以及第一加密认证信息；

判断单元，用于基于所述第一认证信息，判断所述第二终端是否为合法终端，所述判断单元还用于获取所述第一终端的时间戳，并判断所述第一终端的时间戳与所述第二终端的时间戳之间的差值是否小于预设时间段阈值；在判断出所述差值小于预设时间段阈值时，生成第二加密认证信息；判断所述第一加密认证信息与所述第二加密认证信息是否匹配；若所述第一加密认证信息与所述第二加密认证信息匹配，则判断所述第二终端为合法终端；

发送单元，用于在判断出所述第二终端为合法终端时，向所述第二终端发送第二认证信息，以使所述第二终端基于所述第二认证信息判断所述第一终端是否为合法终端；

所述发送单元，还用于在接收到所述第二终端生成的反馈信息时，所述第一终端向所述第二终端发送位置信息，其中，所述反馈信息是所述第二终端基于所述第二认证信息判断出所述第一终端为合法终端时发送的。

5.如权利要求4所述的装置，其特征在于，所述装置还包括：

注册单元，在所述获取单元获取第二终端发送的位置获取请求之前，用于获取用户输入的账户标识以及与所述账户标识对应的鉴权信息；向服务器发送注册请求；接收所述服务器响应所述注册请求生成的加密函数以及加密服务器秘钥；基于所述加密函数、加密服务器秘钥、账户标识以及鉴权信息，生成加密账户标识、加密鉴权信息以及第一加密注册信息，并将所述加密账户标识、加密鉴权信息以及第一加密注册信息发送至所述服务器，以使所述服务器基于加密账户标识、加密鉴权信息以及第一加密注册信息，生成第二加密注册信息，并判断所述第二加密注册信息与第一加密注册信息是否匹配；接收所述服务器生成的用于表示所述第一终端注册成功的反馈消息，其中，所述反馈消息是所述服务器在判断出所述第二加密注册信息与第一加密注册信息匹配时发送的。

6.如权利要求4至5任一项所述的装置，其特征在于，

所述发送单元在用于在接收到所述第二终端生成的反馈信息时，所述第一终端向所述第二终端发送位置信息时，具体用于响应所述第二终端生成的反馈信息，获取所述第一终端的位置信息；将所述位置信息发送至所述第二终端。

一种终端位置信息获取方法及装置

技术领域

[0001] 本发明涉及通信领域，具体涉及一种终端位置信息获取方法及装置。

背景技术

[0002] 随着社会的发展、通讯技术的进步，移动电话等通讯产品已成为人们重要的通讯工具。同时伴随着移动电话的使用日益频繁，人们对移动电话的要求也越来越高。

[0003] 然而由于手机轻便、随身携带、价格较高的特点，使得其很容易丢失，造成较大的经济损失。更重要的是，手机中通常存储有很多联系人，丢失手机有时意味着失去了一些朋友或客户的联系方式。同时，随着互联网的发展，手机逐步成为支付宝、网上银行的重要取款凭证；如果手机落入不法分子手中，可能会造成较大财产损失。因此如何获取丢失终端的位置信息成为一项重要技术。

发明内容

[0004] 本发明实施例提供了一种终端位置信息获取方法及装置，以期在终端丢失时，获取终端的位置信息，进而找回终端，减小经济损失。

[0005] 本发明实施例第一方面提供一种终端位置信息获取方法，包括：

[0006] 第一终端获取第二终端发送的位置获取请求，所述位置获取请求携带第一认证信息；

[0007] 所述第一终端基于所述第一认证信息，判断所述第二终端是否为合法终端；

[0008] 在判断出所述第二终端为合法终端时，所述第一终端向所述第二终端发送第二认证信息，以使所述第二终端基于所述第二认证信息判断所述第一终端是否为合法终端；

[0009] 在接收到所述第二终端生成的反馈信息时，所述第一终端向所述第二终端发送位置信息，其中，所述反馈信息是所述第二终端基于所述第二认证信息判断出所述第一终端为合法终端时发送的。

[0010] 结合第一方面，在一些可能的实现的方式中，所述第一终端获取第二终端发送的位置获取请求之前，所述方法还包括：

[0011] 所述第一终端获取用户输入的账户标识以及与所述账户标识对应的鉴权信息；

[0012] 所述第一终端向服务器发送注册请求；

[0013] 所述第一终端接收所述服务器响应所述注册请求生成的加密函数以及加密服务器秘钥；

[0014] 所述第一终端基于所述加密函数、加密服务器秘钥、账户标识以及鉴权信息，生成加密账户标识、加密鉴权信息以及第一加密注册信息，并将所述加密账户标识、加密鉴权信息以及第一加密注册信息发送至所述服务器，以使所述服务器基于加密账户标识、加密鉴权信息以及第一加密注册信息，生成第二加密注册信息，并判断所述第二加密注册信息与第一加密注册信息是否匹配；

[0015] 所述第一终端接收所述服务器生成的用于表示所述第一终端注册成功的反馈消

息，其中，所述反馈消息是所述服务器在判断出所述第二加密注册信息与第一加密注册信息匹配时发送的。

[0016] 结合第一方面，在一些可能的实现的方式中，所述第一认证信息是所述第二终端基于所述第一终端的账户标识、鉴权信息、所述第二终端的时间戳以及所述第二终端预存的加密函数以及所述第二终端预存的加密服务器秘钥生成的，所述第一认证信息包括加密账户标识、加密鉴权信息、所述第二终端的时间戳以及第一加密认证信息。

[0017] 结合第一方面，在一些可能的实现的方式中，所述第一终端基于所述第一认证信息，判断所述第二终端是否为合法终端，包括：

[0018] 所述第一终端获取所述第一终端的时间戳，并判断所述第一终端的时间戳与所述第二终端的时间戳之间的差值是否小于预设时间段阈值；

[0019] 所述第一终端在判断出所述差值小于预设时间段阈值时，生成第二加密认证信息；

[0020] 所述第一终端判断所述第一加密认证信息与所述第二加密认证信息是否匹配；

[0021] 若所述第一加密认证信息与所述第二加密认证信息匹配，则所述第一终端判断所述第二终端为合法终端。

[0022] 结合第一方面，在一些可能的实现的方式中，所述在接收到所述第二终端生成的反馈信息时，所述第一终端向所述第二终端发送位置信息，包括：

[0023] 所述第一终端响应所述第二终端生成的反馈信息，获取所述第一终端的位置信息；

[0024] 所述第一终端将所述位置信息发送至所述第二终端。

[0025] 本发明实施例第二方面提供一种终端位置信息获取装置，包括：

[0026] 获取单元，用于获取第二终端发送的位置获取请求，所述位置获取请求携带第一认证信息；

[0027] 判断单元，用于基于所述第一认证信息，判断所述第二终端是否为合法终端；

[0028] 发送单元，用于在判断出所述第二终端为合法终端时，向所述第二终端发送第二认证信息，以使所述第二终端基于所述第二认证信息判断所述第一终端是否为合法终端；

[0029] 所述发送单元，还用于在接收到所述第二终端生成的反馈信息时，所述第一终端向所述第二终端发送位置信息，其中，所述反馈信息是所述第二终端基于所述第二认证信息判断出所述第一终端为合法终端时发送的。

[0030] 结合第二方面，在一些可能的实现的方式中，所述第一终端获取第二终端发送的位置获取请求之前，所述装置还包括：

[0031] 注册单元，在所述获取单元获取第二终端发送的位置获取请求之前，用于获取用户输入的账户标识以及与所述账户标识对应的鉴权信息；向服务器发送注册请求；接收所述服务器响应所述注册请求生成的加密函数以及加密服务器秘钥；基于所述加密函数、加密服务器秘钥、账户标识以及鉴权信息，生成加密账户标识、加密鉴权信息以及第一加密注册信息，并将所述加密账户标识、加密鉴权信息以及第一加密注册信息发送至所述服务器，以使所述服务器基于加密账户标识、加密鉴权信息以及第一加密注册信息，生成第二加密注册信息，并判断所述第二加密注册信息与第一加密注册信息是否匹配；接收所述服务器生成的用于表示所述第一终端注册成功的反馈消息，其中，所述反馈消息是所述服务器在

判断出所述第二加密注册信息与第一加密注册信息匹配时发送的。

[0032] 结合第二方面，在一些可能的实现的方式中，所述第一认证信息是所述第二终端基于所述第一终端的账户标识、鉴权信息、所述第二终端的时间戳以及所述第二终端预存的加密函数以及所述第二终端预存的加密服务器秘钥生成的，所述第一认证信息包括加密账户标识、加密鉴权信息、所述第二终端的时间戳以及第一加密认证信息。

[0033] 结合第二方面，在一些可能的实现的方式中，所述判断单元，具体用于获取所述第一终端的时间戳，并判断所述第一终端的时间戳与所述第二终端的时间戳之间的差值是否小于预设时间段阈值；在判断出所述差值小于预设时间段阈值时，生成第二加密认证信息；判断所述第一加密认证信息与所述第二加密认证信息是否匹配；若所述第一加密认证信息与所述第二加密认证信息匹配，则判断所述第二终端为合法终端。

[0034] 结合第二方面，在一些可能的实现的方式中，所述发送单元在用于在接收到所述第二终端生成的反馈信息时，所述第一终端向所述第二终端发送位置信息时，具体用于响应所述第二终端生成的反馈信息，获取所述第一终端的位置信息；将所述位置信息发送至所述第二终端。

[0035] 可以看出，本发明实施例技术方案中，第一终端获取第二终端发送的携带第一认证信息的位置获取请求，基于该第一认证信息，判断第二终端是否为合法终端，第一终端在判断出第二终端为合法终端时，向第二终端发送第二认证信息，以使第二终端基于该第二认证信息判断第一终端是否为合法终端，第二终端基于第二认证信息判断出第一终端为合法终端时向第一终端发送反馈信息，在接收到第二终端生成的反馈信息时，第一终端向第二终端发送位置信息，通过实施本发明实施例能够在第一终端丢失时，通过第二终端获取第一终端的位置信息，进而找回第一终端，减小经济损失。

附图说明

[0036] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述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。

[0037] 图1是本发明第一实施例提供的一种终端位置信息获取方法的流程示意图；

[0038] 图2是本发明第二实施例提供的一种终端位置信息获取方法的流程示意图；

[0039] 图3是本发明第三实施例提供的一种终端位置信息获取装置的结构示意图；

[0040] 图4是本发明第四实施例提供的一种获取装置的结构示意图。

具体实施方式

[0041] 为了使本技术领域的人员更好地理解本发明方案，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作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。

[0042] 本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”等是用于区别不同对象，而不是用于描述特定顺序。此外，“包括”和“具有”以及它们任

何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其他步骤或单元。

[0043] 在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本发明的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

[0044] 本发明实施例中的第一终端与第二终端均为e-SIM(embedded-Subscriber Identification Module，客户识别模块)卡终端。

[0045] 请参阅图1，图1是本发明第一实施例提供的一种终端位置信息获取的流程示意图，如图1所示，本发明实施例中的终端位置信息获取包括以下步骤：

[0046] S101、第一终端获取第二终端发送的位置获取请求，所述位置获取请求携带第一认证信息。

[0047] 其中，所述第一认证信息是所述第二终端基于所述第一终端的账户标识、鉴权信息、所述第二终端的时间戳以及所述第二终端预存的加密函数以及所述第二终端预存的加密服务器秘钥生成的，所述第一认证信息包括加密账户标识、加密鉴权信息、所述第二终端的时间戳以及第一加密认证信息。

[0048] S102、所述第一终端基于所述第一认证信息，判断所述第二终端是否为合法终端。

[0049] S103、在判断出所述第二终端为合法终端时，所述第一终端向所述第二终端发送第二认证信息，以使所述第二终端基于所述第二认证信息判断所述第一终端是否为合法终端。

[0050] S104、在接收到所述第二终端生成的反馈信息时，所述第一终端向所述第二终端发送位置信息，其中，所述反馈信息是所述第二终端基于所述第二认证信息判断出所述第一终端为合法终端时发送的。

[0051] 其中，所述第一终端获取第二终端发送的位置获取请求之前，所述第一终端还可以执行以下操作：

[0052] 所述第一终端获取用户输入的账户标识以及与所述账户标识对应的鉴权信息；

[0053] 所述第一终端向服务器发送注册请求；

[0054] 所述第一终端接收所述服务器响应所述注册请求生成的加密函数以及加密服务器秘钥；

[0055] 所述第一终端基于所述加密函数、加密服务器秘钥、账户标识以及鉴权信息，生成加密账户标识、加密鉴权信息以及第一加密注册信息，并将所述加密账户标识、加密鉴权信息以及第一加密注册信息发送至所述服务器，以使所述服务器基于加密账户标识、加密鉴权信息以及第一加密注册信息，生成第二加密注册信息，并判断所述第二加密注册信息与第一加密注册信息是否匹配；

[0056] 所述第一终端接收所述服务器生成的用于表示所述第一终端注册成功的反馈消息，其中，所述反馈消息是所述服务器在判断出所述第二加密注册信息与第一加密注册信息匹配时发送的。

[0057] 其中，所述第一认证信息是所述第二终端基于所述第一终端的账户标识、鉴权信

息、所述第二终端的时间戳以及所述第二终端预存的加密函数以及所述第二终端预存的加密服务器秘钥生成的，所述第一认证信息包括加密账户标识、加密鉴权信息、所述第二终端的时间戳以及第一加密认证信息。

[0058] 作为一种可选的实施方式，所述第一终端基于所述第一认证信息，判断所述第二终端是否为合法终端的具体实现方式可以是：

[0059] 所述第一终端获取所述第一终端的时间戳，并判断所述第一终端的时间戳与所述第二终端的时间戳之间的差值是否小于预设时间段阈值；

[0060] 所述第一终端在判断出所述差值小于预设时间段阈值时，生成第二加密认证信息；

[0061] 所述第一终端判断所述第一加密认证信息与所述第二加密认证信息是否匹配；

[0062] 若所述第一加密认证信息与所述第二加密认证信息匹配，则所述第一终端判断所述第二终端为合法终端。

[0063] 作为一种可选的实施方式，所述在接收到所述第二终端生成的反馈信息时，所述第一终端向所述第二终端发送位置信息的具体实现方式可以是：

[0064] 所述第一终端响应所述第二终端生成的反馈信息，获取所述第一终端的位置信息；

[0065] 所述第一终端将所述位置信息发送至所述第二终端。

[0066] 可以看出，本发明实施例技术方案中，第一终端获取第二终端发送的携带第一认证信息的位置获取请求，基于该第一认证信息，判断第二终端是否为合法终端，第一终端在判断出第二终端为合法终端时，向第二终端发送第二认证信息，以使第二终端基于该第二认证信息判断第一终端是否为合法终端，第二终端基于第二认证信息判断出第一终端为合法终端时向第一终端发送反馈信息，在接收到第二终端生成的反馈信息时，第一终端向第二终端发送位置信息，通过实施本发明实施例能够在第一终端丢失时，通过第二终端获取第一终端的位置信息，进而找回第一终端，减小经济损失。

[0067] 请参阅图2，图2是本发明第二实施例提供的一种终端位置信息获取方法的流程示意图，如图2所示，本发明实施例中的终端位置信息获取方法包括以下步骤：

[0068] S201、所述第一终端获取用户输入的账户标识以及与所述账户标识对应的鉴权信息。

[0069] 具体地，用户输入一个账户标识UID和对应的鉴权信息UK。

[0070] S202、所述第一终端向服务器发送注册请求。

[0071] S203、所述第一终端接收所述服务器响应所述注册请求生成的加密函数以及加密服务器秘钥。

[0072] 具体地，服务器会会响应所述注册请求，向第一终端发送加密函数，所述加密函数可以是哈希函数Hash(*)和加密服务器秘钥Hash(RSK)，其中RSK表示服务器秘钥。

[0073] S204、所述第一终端基于所述加密函数、加密服务器秘钥、账户标识以及鉴权信息，生成加密账户标识、加密鉴权信息以及第一加密注册信息，并将所述加密账户标识、加密鉴权信息以及第一加密注册信息发送至所述服务器，以使所述服务器基于加密账户标识、加密鉴权信息以及第一加密注册信息，生成第二加密注册信息，并判断所述第二加密注册信息与第一加密注册信息是否匹配。

[0074] 具体地，所述第一终端基于所述加密函数Hash(*)、加密服务器秘钥Hash(RSK)、账户标识UID以及鉴权信息UK，生成加密账户标识HID、加密鉴权信息HUK以及第一加密注册信息$HRSK_U$，其中，HID＝Hash(UID)，HUK＝Hash(UK)，HRSKu＝Hash(HID⊕Hash(RSK))⊕HUK，其中⊕为异或运算。所述第一终端将生成的加密账户标识HID、加密鉴权信息HUK以及第一加密注册信息HRSKu发送至服务器，服务器根据加密账户标识HID、加密鉴权信息HUK以及第一加密注册信息HRSKu，生成第二加密注册信息HRSKr，其中，HRSKr＝Hash(HID⊕Hash(RSK))⊕HUK。

[0075] S205、所述第一终端接收所述服务器生成的用于表示所述第一终端注册成功的反馈消息，其中，所述反馈消息是所述服务器在判断出所述第二加密注册信息与第一加密注册信息匹配时发送的。

[0076] 服务器判断第二加密注册信息HRSKr与所述第二加密注册信息HRSKu是否相等，若相等，则表示所述第一终端注册成功，若不相等，则表示所述第一终端失败，在所述第一终端注册成功时，所述服务器生成用于表示所述第一终端注册成功的反馈消息，并将所述反馈消息发送至第一种终端。

[0077] S206、第一终端获取第二终端发送的位置获取请求，所述位置获取请求携带第一认证信息。

[0078] 其中，所述第一认证信息是所述第二终端基于所述第一终端的账户标识、鉴权信息、所述第二终端的时间戳以及所述第二终端预存的加密函数以及所述第二终端预存的加密服务器秘钥生成的，所述第一认证信息包括加密账户标识、加密鉴权信息、所述第二终端的时间戳以及第一加密认证信息。

[0079] 具体地，第二终端获取第一终端的账户标识UID鉴权信息UK以及所述第二终端的时间戳T2，并使用第二终端中的哈希函数Hash(*)生成加密账户标识HID、加密鉴权信息HUK、第一加密认证信息SK1，其中，HID＝Hash(ID)，HUK＝Hash(UK)，SK1＝Hash(Hash(HID⊕Hash(RSK))⊕T2)。

[0080] S207、所述第一终端获取所述第一终端的时间戳，并判断所述第一终端的时间戳与所述第二终端的时间戳之间的差值是否小于预设时间段阈值。

[0081] 所述第一终端获取所述第二终端发送的加密账户标识HID、加密鉴权信息HUK、第一加密认证信息SK1以及所述第二终端的时间戳T2，并获取所述第一终端当前的时间戳T1与的第二终端的时间戳T2的差值，T1-T2是否小于或等于预设时间段阈值△t。

[0082] S208、所述第一终端在判断出所述差值小于预设时间段阈值时，生成第二加密认证信息。

[0083] 具体地，若T1-T2≤△t，则第一终端生成第二加密认证信息SK2，其中，SK2＝Hash(Hash(RSK)⊕HUK⊕T2)。

[0084] S209、所述第一终端判断所述第一加密认证信息与所述第二加密认证信息是否匹配。

[0085] 所述第一终端判断所述第一加密认证信息SK1与所述第二加密认证信息SK2是否相等，若相等，则所述第一终端判断所述第二终端为合法终端。

[0086] S210、若所述第一加密认证信息与所述第二加密认证信息匹配，则所述第一终端判断所述第二终端为合法终端。

[0087] S211、在判断出所述第二终端为合法终端时，所述第一终端向所述第二终端发送第二认证信息，以使所述第二终端基于所述第二认证信息判断所述第一终端是否为合法终端。

[0088] 具体地，基于与所述第一终端判断所述第二终端为合法终端的相同的验证过程，第一终端生成第三加密认证信息SK3＝Hash(Hash(HID⊕Hash(RSK))⊕T1)，并向所述第二终端发送当前的时间戳T1，第二终端获取接收到第二认证信息时刻的时间戳T2'，并检测T2'－T1是否小于或等于预设时间段阈值，在检测到T2'－T1小于或等于预设时间段阈值时，生成第四加密认证信息，SK4＝Hash(Hash(RSK)⊕HUK⊕T1)。所述第二终端判断所述第三加密认证信息SK3与所述第四加密认证信息SK4是否相等，若相等，则所述第二终端判断所述第一终端为合法终端。

[0089] S212、在接收到所述第二终端生成的反馈信息时，所述第一终端响应所述第二终端生成的反馈信息，获取所述第一终端的位置信息。

[0090] S213、所述第一终端将所述位置信息发送至所述第二终端。

[0091] 其中，所述反馈信息是所述第二终端基于所述第二认证信息判断出所述第一终端为合法终端时发送的。

[0092] 可以看出，本发明实施例技术方案中，第一终端获取第二终端发送的携带第一认证信息的位置获取请求，基于该第一认证信息，判断第二终端是否为合法终端，第一终端在判断出第二终端为合法终端时，向第二终端发送第二认证信息，以使第二终端基于该第二认证信息判断第一终端是否为合法终端，第二终端基于第二认证信息判断出第一终端为合法终端时向第一终端发送反馈信息，在接收到第二终端生成的反馈信息时，第一终端向第二终端发送位置信息，通过实施本发明实施例能够在第一终端丢失时，通过第二终端获取第一终端的位置信息，进而找回第一终端，减小经济损失。

[0093] 下面为本发明装置实施例，本发明装置实施例用于执行本发明方法实施例一至二实现的方法，为了便于说明，仅示出了与本发明实施例相关的部分，具体技术细节未揭示的，请参照本发明实施例一和实施例二。

[0094] 请参阅图3，图3是本发明第三实施例提供的一种终端位置信息获取装置的结构示意图，如图3所示，本发明实施例中的终端位置信息获取装置包括以下单元：

[0095] 获取单元301，用于获取第二终端发送的位置获取请求，所述位置获取请求携带第一认证信息；

[0096] 判断单元302，用于基于所述第一认证信息，判断所述第二终端是否为合法终端；

[0097] 发送单元303，用于在判断出所述第二终端为合法终端时，向所述第二终端发送第二认证信息，以使所述第二终端基于所述第二认证信息判断所述第一终端是否为合法终端；

[0098] 所述发送单元303，还用于在接收到所述第二终端生成的反馈信息时，所述第一终端向所述第二终端发送位置信息，其中，所述反馈信息是所述第二终端基于所述第二认证信息判断出所述第一终端为合法终端时发送的。

[0099] 作为一种可选的实施方式，所述装置还包括：

[0100] 注册单元304，在所述获取单元301获取第二终端发送的位置获取请求之前，用于获取用户输入的账户标识以及与所述账户标识对应的鉴权信息；向服务器发送注册请求；

接收所述服务器响应所述注册请求生成的加密函数以及加密服务器秘钥;基于所述加密函数、加密服务器秘钥、账户标识以及鉴权信息,生成加密账户标识、加密鉴权信息以及第一加密注册信息,并将所述加密账户标识、加密鉴权信息以及第一加密注册信息发送至所述服务器,以使所述服务器基于加密账户标识、加密鉴权信息以及第一加密注册信息,生成第二加密注册信息,并判断所述第二加密注册信息与第一加密注册信息是否匹配;接收所述服务器生成的用于表示所述第一终端注册成功的反馈消息,其中,所述反馈消息是所述服务器在判断出所述第二加密注册信息与第一加密注册信息匹配时发送的。

[0101] 作为一种可选的实施方式,所述第一认证信息是所述第二终端基于所述第一终端的账户标识、鉴权信息、所述第二终端的时间戳以及所述第二终端预存的加密函数以及所述第二终端预存的加密服务器秘钥生成的,所述第一认证信息包括加密账户标识、加密鉴权信息、所述第二终端的时间戳以及第一加密认证信息。

[0102] 作为一种可选的实施方式,所述判断单元302,具体用于获取所述第一终端的时间戳,并判断所述第一终端的时间戳与所述第二终端的时间戳之间的差值是否小于预设时间段阈值;在判断出所述差值小于预设时间段阈值时,生成第二加密认证信息;判断所述第一加密认证信息与所述第二加密认证信息是否匹配;若所述第一加密认证信息与所述第二加密认证信息匹配,则判断所述第二终端为合法终端。

[0103] 作为一种可选的实施方式,所述发送单元303在用于在接收到所述第二终端生成的反馈信息时,所述第一终端向所述第二终端发送位置信息时,具体用于响应所述第二终端生成的反馈信息,获取所述第一终端的位置信息;将所述位置信息发送至所述第二终端。

[0104] 具体的,上述各个单元的具体实现可参考图1至图2对应实施例中相关步骤的描述,在此不赘述。

[0105] 可以看出,本发明实施例技术方案中,第一终端获取第二终端发送的携带第一认证信息的位置获取请求,基于该第一认证信息,判断第二终端是否为合法终端,第一终端在判断出第二终端为合法终端时,向第二终端发送第二认证信息,以使第二终端基于该第二认证信息判断第一终端是否为合法终端,第二终端基于第二认证信息判断出第一终端为合法终端时向第一终端发送反馈信息,在接收到第二终端生成的反馈信息时,第一终端向第二终端发送位置信息,通过实施本发明实施例能够在第一终端丢失时,通过第二终端获取第一终端的位置信息,进而找回第一终端,减小经济损失。

[0106] 请参考图4,图4是本发明第四实施例提供的一种终端位置信息获取装置的结构示意图。如图4所示,本发明实施例中的终端位置信息获取装置包括:至少一个处理器401,例如CPU,至少一个接收器403,至少一个存储器404,至少一个发送器405,至少一个通信总线402。其中,通信总线402用于实现这些组件之间的连接通信。其中,本发明实施例中装置的接收器403和发送器405可以是有线发送端口,也可以为无线设备,例如包括天线装置,用于与其他节点设备进行信令或数据的通信。存储器404可以是高速RAM存储器,也可以是非不稳定的存储器(non-volatile memory),例如至少一个磁盘存储器。存储器404可选的还可以是至少一个与前述处理器401相连接的存储装置。存储器404中存储一组程序代码,且所述处理器401可通过通信总线402,调用存储器404中存储的代码以执行相关的功能。

[0107] 所述处理器401,用于获取第二终端发送的位置获取请求,所述位置获取请求携带第一认证信息;基于所述第一认证信息,判断所述第二终端是否为合法终端;在判断出所述

第二终端为合法终端时，向所述第二终端发送第二认证信息，以使所述第二终端基于所述第二认证信息判断所述第一终端是否为合法终端；在接收到所述第二终端生成的反馈信息时，向所述第二终端发送位置信息，其中，所述反馈信息是所述第二终端基于所述第二认证信息判断出所述第一终端为合法终端时发送的。

[0108] 作为一种可选的实施方式，所述处理器401，在用于获取第二终端发送的位置获取请求之前，还可以用于获取用户输入的账户标识以及与所述账户标识对应的鉴权信息；向服务器发送注册请求；接收所述服务器响应所述注册请求生成的加密函数以及加密服务器秘钥；基于所述加密函数、加密服务器秘钥、账户标识以及鉴权信息，生成加密账户标识、加密鉴权信息以及第一加密注册信息，并将所述加密账户标识、加密鉴权信息以及第一加密注册信息发送至所述服务器，以使所述服务器基于加密账户标识、加密鉴权信息以及第一加密注册信息，生成第二加密注册信息，并判断所述第二加密注册信息与第一加密注册信息是否匹配；接收所述服务器生成的用于表示所述第一终端注册成功的反馈消息，其中，所述反馈消息是所述服务器在判断出所述第二加密注册信息与第一加密注册信息匹配时发送的。

[0109] 作为一种可选的实施方式，所述第一认证信息是所述第二终端基于所述第一终端的账户标识、鉴权信息、所述第二终端的时间戳以及所述第二终端预存的加密函数以及所述第二终端预存的加密服务器秘钥生成的，所述第一认证信息包括加密账户标识、加密鉴权信息、所述第二终端的时间戳以及第一加密认证信息。

[0110] 作为一种可选的实施方式，所述处理器401，在用于基于所述第一认证信息，判断所述第二终端是否为合法终端时，具体用于获取所述第一终端的时间戳，并判断所述第一终端的时间戳与所述第二终端的时间戳之间的差值是否小于预设时间段阈值；在判断出所述差值小于预设时间段阈值时，生成第二加密认证信息；判断所述第一加密认证信息与所述第二加密认证信息是否匹配；若所述第一加密认证信息与所述第二加密认证信息匹配，则端判断所述第二终端为合法终端。

[0111] 作为一种可选的实施方式，所述处理器401，在用于在接收到所述第二终端生成的反馈信息时，所述第一终端向所述第二终端发送位置信息时，具体用于响应所述第二终端生成的反馈信息，获取所述第一终端的位置信息；将所述位置信息发送至所述第二终端。

[0112] 具体的，上述各个单元的具体实现可参考图1至图2对应实施例中相关步骤的描述，在此不赘述。

[0113] 可以看出，本发明实施例技术方案中，第一终端获取第二终端发送的携带第一认证信息的位置获取请求，基于该第一认证信息，判断第二终端是否为合法终端，第一终端在判断出第二终端为合法终端时，向第二终端发送第二认证信息，以使第二终端基于该第二认证信息判断第一终端是否为合法终端，第二终端基于第二认证信息判断出第一终端为合法终端时向第一终端发送反馈信息，在接收到第二终端生成的反馈信息时，第一终端向第二终端发送位置信息，通过实施本发明实施例能够在第一终端丢失时，通过第二终端获取第一终端的位置信息，进而找回第一终端，减小经济损失。

[0114] 本发明实施例还提供一种计算机存储介质，其中，该计算机存储介质可存储有程序，该程序执行时包括上述方法实施例中记载的任何一种服务进程的监控方法的部分或全部步骤。

[0115] 需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和单元并不一定是本发明所必须的。

[0116] 本发明实施例的方法的步骤顺序可以根据实际需要进行调整、合并或删减。本发明实施例的终端的单元可以根据实际需要进行整合、进一步划分或删减。

[0117] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0118] 在本申请所提供的几个实施例中，应该理解到，所揭露的装置，可通过其它的方式实现。例如，以上所描述的装置实施例是示意性的，例如所述单元的划分，为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性或其它的形式。

[0119] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0120] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0121] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0122] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括:闪存盘、只读存储器(英文:Read-Only Memory，简称:ROM)、随机存取器(英文:Random Access Memory，简称:RAM)、磁盘或光盘等。

[0123] 以上对本发明实施例所提供的一种终端位置信息获取方法及装置进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想;同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

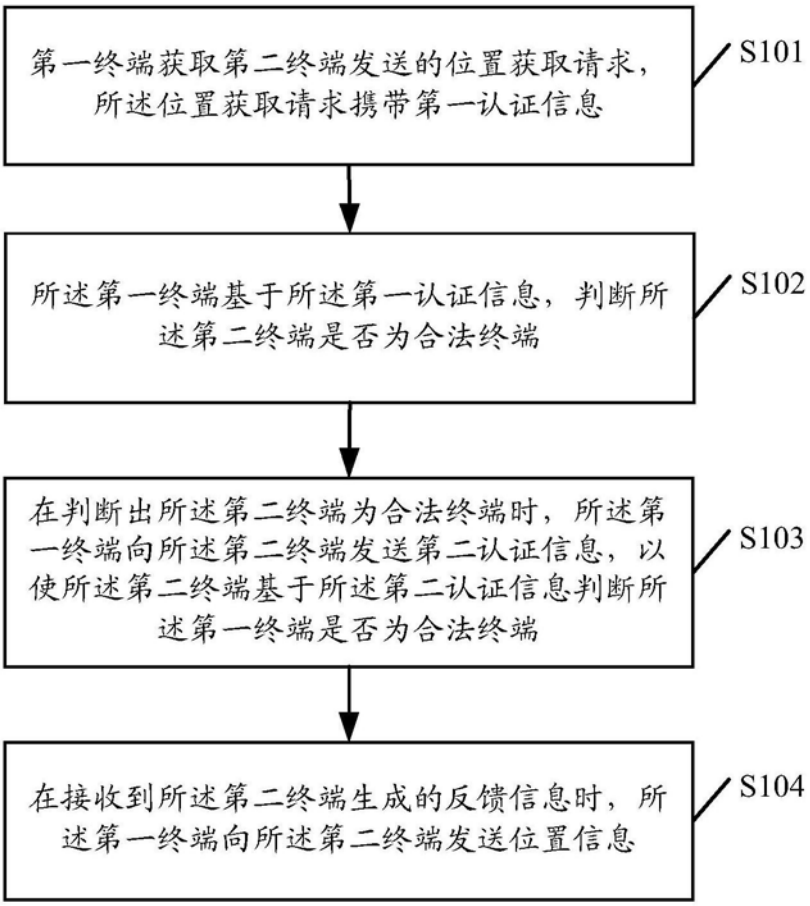

第一终端获取第二终端发送的位置获取请求，所述位置获取请求携带第一认证信息
S101
所述第一终端基于所述第一认证信息，判断所述第二终端是否为合法终端
S102
在判断出所述第二终端为合法终端时，所述第一终端向所述第二终端发送第二认证信息，以使所述第二终端基于所述第二认证信息判断所述第一终端是否为合法终端
S103
在接收到所述第二终端生成的反馈信息时，所述第一终端向所述第二终端发送位置信息
S104

图1

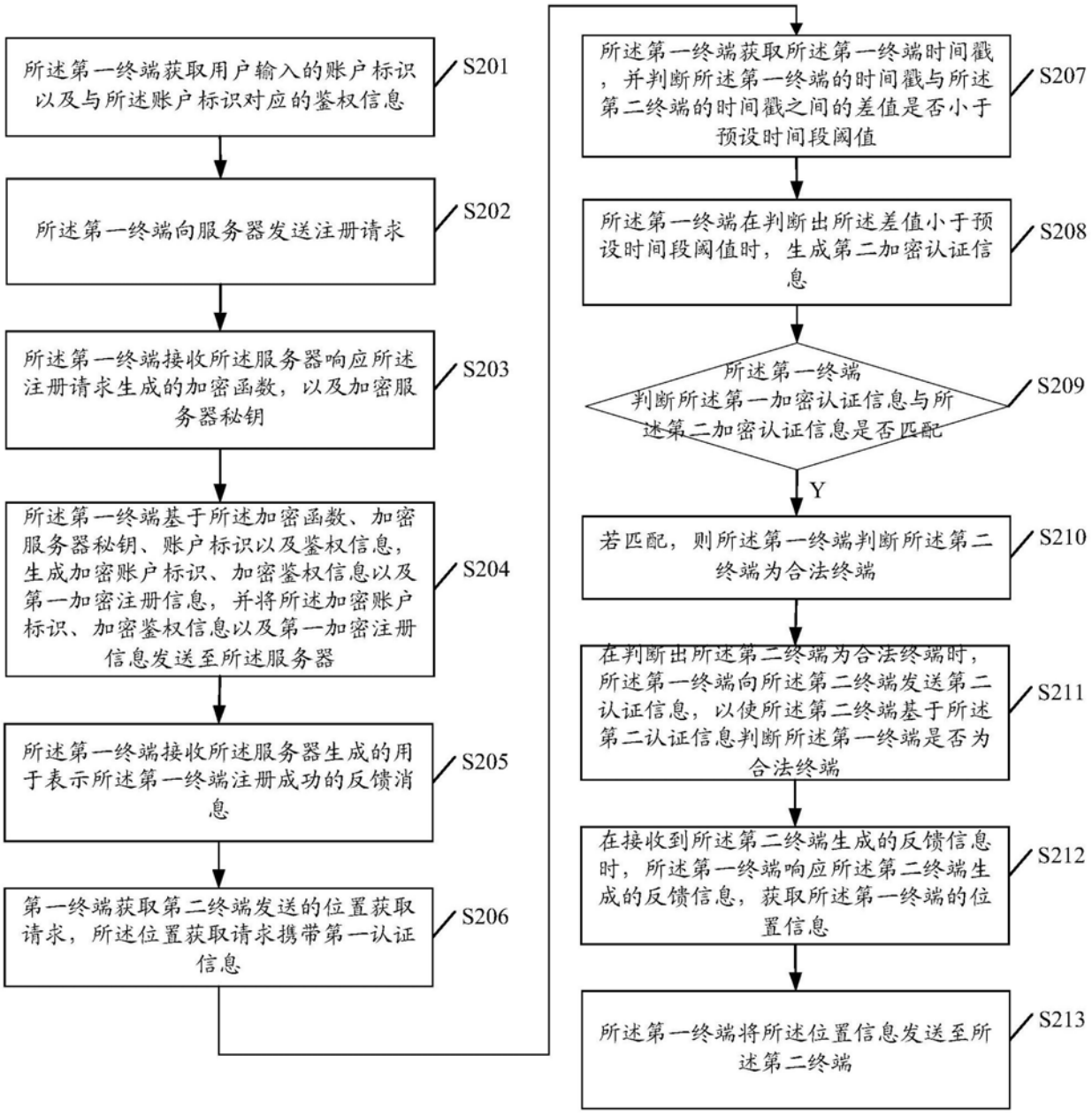

所述第一终端获取用户输入的账户标识以及与所述账户标识对应的鉴权信息
S201
所述第一终端向服务器发送注册请求
S202
所述第一终端接收所述服务器响应所述注册请求生成的加密函数，以及加密服务器秘钥
S203
所述第一终端基于所述加密函数、加密服务器秘钥、账户标识以及鉴权信息，生成加密账户标识、加密鉴权信息以及第一加密注册信息，并将所述加密账户标识、加密鉴权信息以及第一加密注册信息发送至所述服务器
S204
所述第一终端接收所述服务器生成的用于表示所述第一终端注册成功的反馈消息
S205
第一终端获取第二终端发送的位置获取请求，所述位置获取请求携带第一认证信息
S206
所述第一终端获取所述第一终端时间戳，并判断所述第一终端的时间戳与所述第二终端的时间戳之间的差值是否小于预设时间段阈值
S207
所述第一终端在判断出所述差值小于预设时间段阈值时，生成第二加密认证信息
S208
所述第一终端判断所述第一加密认证信息与所述第二加密认证信息是否匹配
S209
Y
若匹配，则所述第一终端判断所述第二终端为合法终端
S210
在判断出所述第二终端为合法终端时，所述第一终端向所述第二终端发送第二认证信息，以使所述第二终端基于所述第二认证信息判断所述第一终端是否为合法终端
S211
在接收到所述第二终端生成的反馈信息时，所述第一终端响应所述第二终端生成的反馈信息，获取所述第一终端的位置信息
S212
所述第一终端将所述位置信息发送至所述第二终端
S213

图2

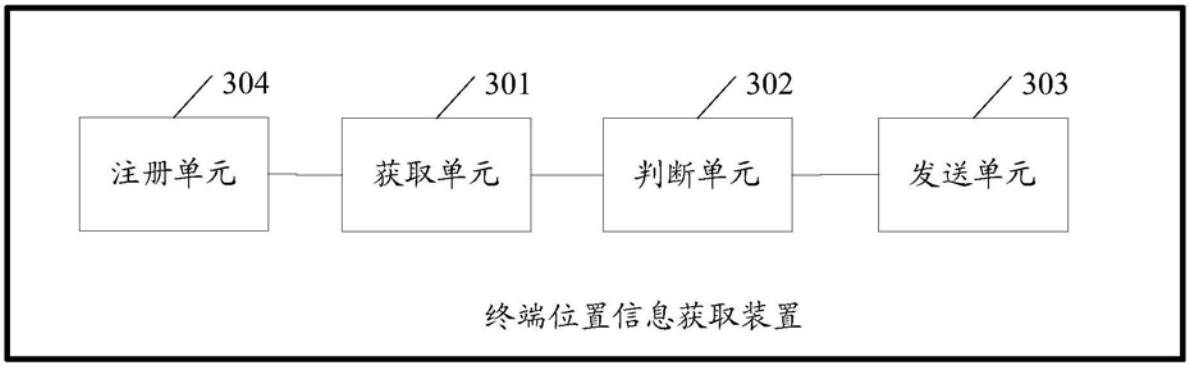

304
301
302
303
注册单元
获取单元
判断单元
发送单元
终端位置信息获取装置

图3

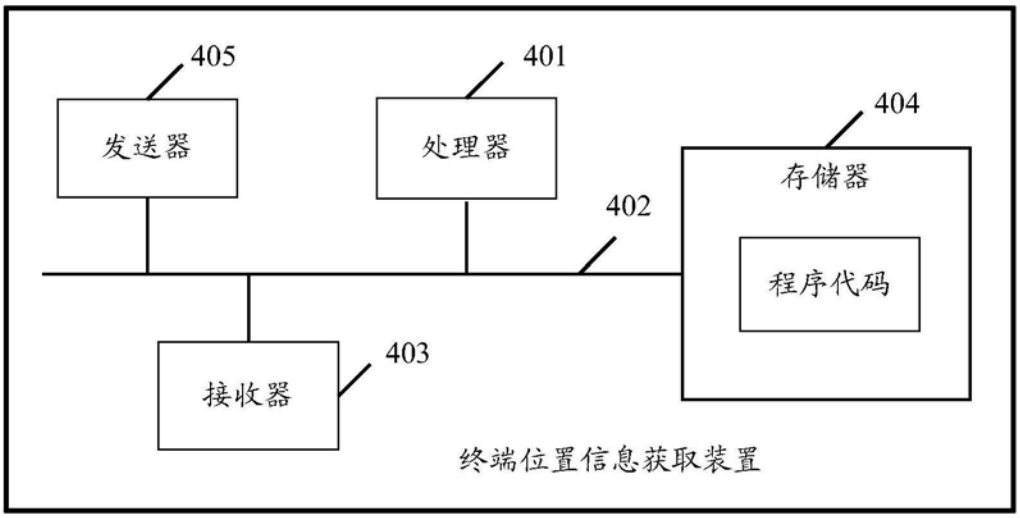

405
401
404
发送器
处理器
存储器
402
程序代码
403
接收器
终端位置信息获取装置

图4