(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109618349 A
(43)申请公布日 2019.04.12

(21)申请号 201910017126.2

(22)申请日 2019.01.08

(71)申请人 中国联合网络通信集团有限公司
地址 100033 北京市西城区金融大街21号
申请人 联通支付有限公司

(72)发明人 徐华美 胡红星

(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健

(51)Int.Cl.
H04W 12/12(2009.01)
H04L 29/06(2006.01)

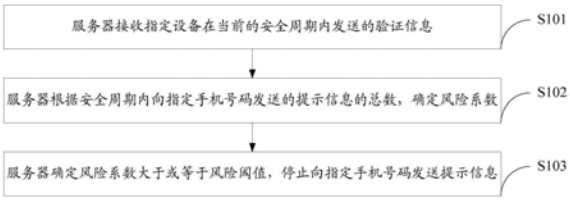
权利要求书3页 说明书9页 附图6页

(54)发明名称

一种数据传输方法和服务器

(57)摘要

本发明的实施例提供了一种数据传输方法和服务器，涉及通信技术领域，解决了如何识别出用户的手机号码是否被“短信轰炸”的问题。该方法包括，服务器接收指定设备在当前的安全周期内发送的验证信息；其中，验证信息用于指示服务器向指定手机号码发送提示信息；服务器根据安全周期内向指定手机号码发送的提示信息的总数，确定风险系数；其中，风险系数用于指示向指定手机号码发送提示信息的频率；服务器确定风险系数大于或等于风险阈值时，停止向指定手机号码发送提示信息。



CN 109618349 A

1.一种数据传输方法,其特征在于,包括:

服务器接收指定设备在当前的安全周期内发送的验证信息;其中,所述验证信息用于指示所述服务器向指定手机号码发送提示信息;

所述服务器根据所述安全周期内向所述指定手机号码发送的提示信息的总数,确定风险系数;其中,所述风险系数用于指示所述安全周期内向所述指定手机号码发送提示信息的频率;

所述服务器确定所述风险系数大于或等于风险阈值时,停止向所述指定手机号码发送提示信息。

2.根据权利要求1所述的数据传输方法,其特征在于,所述服务器根据所述安全周期内向所述指定手机号码发送的提示信息的总数,确定风险系数,包括:

所述服务器根据第一预设公式和所述安全周期内向所述指定手机号码发送的提示信息的总数,确定风险系数;其中,所述第一预设公式包括:

$N=m+n\times y$;

其中,N表示所述安全周期的风险系数,m表示初始风险系数,n为常数,y表示所述安全周期内向所述指定手机号码发送的提示信息的总数。

3.根据权利要求1所述的数据传输方法,其特征在于,所述服务器确定所述风险系数大于或等于风险阈值时,停止向所述指定手机号码发送提示信息,包括:

所述服务器根据第二预设公式和累计周期内向所述指定手机号码发送的提示信息的总数,确定累计安全系数;其中,所述累计周期包括至少两个安全周期,所述累计安全系数用于指示所述至少两个安全周期内向所述指定手机号码发送提示信息的频率,所述第二预设公式包括:

$$\alpha_{(i,j)}=\sum_{j=1}^{j=j-1}N_{(i,j-1)};$$

其中,$\alpha_{(i,j)}$表示第i个累计周期内第j个安全周期的累计安全系数,$N_{(i,j-1)}$表示第i个累计周期内第j-1个安全周期的风险系数,j为大于或等于2的整数;

所述服务器确定所述风险系数小于风险阈值,并且所述累计安全系数大于或等于安全阈值时,停止向所述指定手机号码发送提示信息。

4.根据权利要求3所述的数据传输方法,其特征在于,所述提示信息包括验证码;

所述方法还包括:

所述服务器确定所述风险系数小于所述风险阈值时,向所述指定手机号码发送提示信息;

或者,

所述服务器确定所述风险系数小于所述风险阈值,并且所述累计安全系数小于所述安全阈值时,向所述指定手机号码发送提示信息;

所述服务器确定从所述指定设备接收到所述提示信息时,将所述风险系数重置为初始风险系数,并将所述安全周期内向所述指定手机号码发送的提示信息的总数置零。

5.根据权利要求1所述的数据传输方法,其特征在于,所述服务器确定所述风险系数大于或等于风险阈值时,停止向所述指定手机号码发送提示信息,包括:

所述服务器确定所述风险系数大于或等于风险阈值时,向所述指定设备发送携带所述

第一校验识别信息的控制信息;其中,所述控制信息指示所述指定设备显示所述第一校验识别信息,所述第一校验识别信息包括图形验证码;

所述服务器确定从所述指定设备接收的第二校验识别信息与所述第一校验识别信息相同时,根据第三预设公式确定更新后的风险系数;其中,所述第三预设公式包括:

$$M=N\times\left(1-\frac{1}{i}\right);$$

其中,M_j表示所述安全周期更新后的风险系数,i表示所述安全周期内第二校验识别信息与所述第一校验识别信息相同的累计次数;

所述服务器确定所述更新后的风险系数大于或等于所述风险阈值时,停止向所述指定手机号码发送提示信息。

6.一种服务器,其特征在于,包括:

收发单元,用于接收指定设备在当前的安全周期内发送的验证信息;其中,所述验证信息用于指示所述服务器向指定手机号码发送提示信息;

处理单元,用于根据所述安全周期内所述收发单元向所述指定手机号码发送的提示信息的总数,确定风险系数;其中,所述风险系数用于指示向所述指定手机号码发送提示信息的频率;

所述处理单元,还用于确定所述风险系数大于或等于风险阈值时,控制所述收发单元停止向所述指定手机号码发送提示信息。

7.根据权利要求6所述的服务器,其特征在于,所述处理单元,具体用于根据第一预设公式和所述安全周期内所述收发单元向所述指定手机号码发送的提示信息的总数,确定风险系数;其中,所述第一预设公式包括:

$N=m+n\times y$;

其中,N表示所述安全周期的风险系数,m表示初始风险系数,n为常数,y表示所述安全周期内向所述指定手机号码发送的提示信息的总数。

8.根据权利要求6所述的服务器,其特征在于,所述处理单元,还用于根据第二预设公式和累计周期内所述收发单元向所述指定手机号码发送的提示信息的总数,确定累计安全系数;其中,所述累计周期包括至少两个安全周期,所述累计安全系数用于指示所述至少两个安全周期内向所述指定手机号码发送提示信息的频率,所述第二预设公式包括:

$$\alpha_{(i,j)}=\sum_{j=1}^{j=j-1}N_{(i,j-1)};$$

其中,$\alpha_{(i,j)}$表示第i个累计周期内第j个安全周期的累计安全系数,$N_{(i,j-1)}$表示第i个累计周期内第j-1个安全周期的风险系数,j为大于或等于2的整数;

所述处理单元,具体用于确定所述风险系数小于所述风险阈值,并且所述累计安全系数大于或等于所述安全阈值时,控制所述收发单元停止向所述指定手机号码发送提示信息。

9.根据权利要求8所述的服务器,其特征在于,所述提示信息包括验证码;

所述处理单元,还用于确定所述风险系数小于所述风险阈值时,控制所述收发单元向所述指定手机号码发送提示信息;

或者,

所述处理单元，还用于确定所述风险系数小于所述风险阈值，并且所述累计安全系数小于所述安全阈值时，控制所述收发单元向所述指定手机号码发送提示信息；

所述处理单元，还用于确定从所述指定设备接收到所述提示信息时，将所述当前的安全周期的风险系数重置为初始风险系数，并将所述安全周期内向所述指定手机号码发送的提示信息的总数置零。

10.根据权利要求6所述的服务器，其特征在于，所述处理单元，还用于确定所述风险系数大于或等于所述风险阈值或者所述风险系数小于风险阈值时，控制所述收发单元向所述指定设备发送携带所述第一校验识别信息的控制信息；其中，所述控制信息指示所述指定设备显示所述第一校验识别信息，所述第一校验识别信息包括图形验证码；

所述处理单元，还用于确定所述收发单元从所述指定设备接收的第二校验识别信息与所述第一校验识别信息相同时，根据第三预设公式确定更新后的风险系数；其中，所述第三预设公式包括：

$$M=N\times\left(1-\frac{1}{i}\right);$$

其中，M表示所述安全周期更新后的风险系数，i表示所述安全周期内第二校验识别信息与所述第一校验识别信息相同的累计次数；

所述处理单元，还用于确定所述更新后的风险系数大于或等于所述风险阈值时，控制所述收发单元停止向所述指定手机号码发送提示信息。

11.一种计算机存储介质，其特征在于，包括指令，当其在计算机上运行时，使得计算机执行如上述权利要求1-5任一项所述的数据传输方法。

12.一种服务器，其特征在于，包括：通信接口、处理器、存储器、总线；存储器用于存储计算机执行指令，处理器与存储器通过总线连接，当服务器运行时，处理器执行存储器存储的计算机执行指令，以使服务器执行如上述权利要求1-5任一项所述的数据传输方法。

一种数据传输方法和服务器

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种数据传输方法和服务器。

背景技术

[0002] 随着科技进步、互联网技术不断发展，互联网应用越来越多，很多互联网应用也被人们熟知并广泛使用。同时，手机号作为每个人的一个标识，大部分互联网应用系统会绑定用户手机号并把手机号作为用户名。如此，验证手机号的真实性就成为了不可或缺的一个步骤，而且通过发送短信验证码验证手机号真实性已成为当今主流趋势。

[0003] 而发送短信验证码验证手机号随着被广泛熟知，一些问题也随之而来，比如：“短信轰炸”；其中，短信轰炸的实现过程如下：

[0004] 恶意轰炸方利用这个手机验证码的机制，用非常非常多的网站做成列表，从而通过列表中的每个网站的注册接口向指定手机号发送手机验证码，使得该指定手机号一直处于接收手机验证码的状态中，造成用户无法正常使用该指定手机号。

[0005] 由上述可知，现有技术中，如何识别出用户的手机号码是否被“短信轰炸”成为了一个亟待解决的问题。

发明内容

[0006] 本发明的实施例提供一种数据传输方法和服务器，解决了如何识别出用户的手机号码是否被“短信轰炸”的问题。

[0007] 为达到上述目的，本发明的实施例采用如下技术方案：

[0008] 第一方面、本发明的实施例提供一种数据传输方法，包括：服务器接收指定设备在当前的安全周期内发送的验证信息；其中，验证信息用于指示服务器向指定手机号码发送提示信息；服务器根据安全周期内向指定手机号码发送的提示信息的总数，确定风险系数；其中，风险系数用于指示向指定手机号码发送提示信息的频率；服务器确定风险系数大于或等于风险阈值时，停止向指定手机号码发送提示信息。

[0009] 由上述方案可知，本发明的实施例提供的数据传输方法，当服务器接收到指定设备在当前的安全周期内发送的验证信息时，根据该安全周期内向指定手机号码发送的提示信息的总数，从而可以判别出在该安全周期内向该指定手机号码发送提示信息的频率，当确定风险系数大于或等于风险阈值时，说明在当前的安全周期向该指定手机号码发送提示信息的频率过高，存在“短信轰炸”可能，因此停止向该指定手机号码发送提示信息，使得用户可以正常使用该指定手机号码的体验，保证了用户体验，解决了如何识别出用户的手机号码是否被“短信轰炸”的问题。

[0010] 第二方面、本发明的实施例提供一种服务器，包括：收发单元，用于接收指定设备在当前的安全周期内发送的验证信息；其中，验证信息用于指示服务器向指定手机号码发送提示信息；处理单元，用于根据安全周期内收发单元向指定手机号码发送的提示信息的总数，确定风险系数；其中，风险系数用于指示向指定手机号码发送提示信息的频率；处理

单元，还用于确定风险系数大于或等于风险阈值时，控制收发单元停止向指定手机号码发送提示信息。

[0011] 第三方面，本发明的实施例提供一种服务器，包括：通信接口、处理器、存储器、总线；存储器用于存储计算机执行指令，处理器与存储器通过总线连接，当服务器运行时，处理器执行存储器存储的计算机执行指令，以使服务器执行如上述第一方面提供的方法。

[0012] 第四方面，本发明的实施例提供一种计算机存储介质，包括指令，当其在计算机上运行时，使得计算机执行如上述第一方面提供的方法。

[0013] 可以理解地，上述提供的任一种服务器用于执行上文所提供的第一方面对应的方法，因此，其所能达到的有益效果可参考上文第一方面的方法以及下文具体实施方式中对应的方案的有益效果，此处不再赘述。

附图说明

[0014] 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，下面描述中的附图仅仅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。

[0015] 图1为本发明的实施例提供的一种数据传输方法的网络架构图；

[0016] 图2为本发明的实施例提供的一种数据传输方法的流程示意图之一；

[0017] 图3为本发明的实施例提供的一种数据传输方法的流程示意图之二；

[0018] 图4为本发明的实施例提供的一种数据传输方法的流程示意图之三；

[0019] 图5为本发明的实施例提供的一种数据传输方法的流程示意图之四；

[0020] 图6为本发明的实施例提供的一种数据传输方法的流程示意图之五；

[0021] 图7为本发明的实施例提供的一种服务器的结构示意图之一；

[0022] 图8为本发明的实施例提供的一种服务器的结构示意图之二。

[0023] 附图标记：

[0024] 服务器-10；

[0025] 收发单元-101；处理单元-102。

具体实施方式

[0026] 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，所描述的实施例仅仅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。

[0027] 为了便于清楚描述本发明实施例的技术方案，在本发明的实施例中，采用了“第一”、“第二”等字样对功能和作用基本相同的相同项或相似项进行区分，本领域技术人员可以理解“第一”、“第二”等字样并不是在对数量和执行次序进行限定。

[0028] 在本发明实施例中，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本发明实施例中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”等词旨

在以具体方式呈现相关概念。

[0029] 在本发明实施例的描述中，除非另有说明，“多个”的含义是指两个或两个以上。例如，多个网络是指两个或两个以上的网络。

[0030] 本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。本文中符号“/”表示关联对象是或者的关系，例如A/B表示A或者B。

[0031] 图1为本发明提供的数据传输方法的网络架构图，包括：指定设备1、服务器2、基站3和用户设备(英文全称：User Equipment，简称：UE)4；其中，指定通信设备1通过通信链路与服务器2相连接，服务器2通过通信链路与基站3相连接，UE 4位于该基站3的覆盖范围内，每个UE 4对应一个指定手机号码。通常情况下，如果用户本身通过通信设备1向服务器2发送验证信息(即通信设备1和UE 4均被该用户使用)，此时服务器会发送提示信息至UE 4，用户可以根据该提示信息，将对应的提示信息输入该通信设备1，并通过通信设备1将该提示信息发送至服务器2，从而服务器2对提示信息的真伪进行判别，完成相应的认证；而如果用户恶意利用上述过程(即使用通信设备1的用户和使用UE 4的用户不是同一个用户)，通过该服务器2提供的网站的注册接口向指定手机号发送手机验证码，使得该指定手机号一直处于接收手机验证码的状态中，造成用户无法正常使用该指定手机号；为了解决上述问题，本发明实施例提供的数据传输方法，服务器通过判别每个安全周期内向指定手机号码发送的提示信息的总数，从而判别用户的手机号码是否被“短信轰炸”的问题，具体的实现过程如下：

[0032] 其中，本发明实施例中的通信设备1和UE 4可以为智能移动终端。该智能移动终端为具有操作系统的移动终端。该智能移动终端可以为：智能手机、平板电脑、笔记本电脑、超级移动个人计算机(ultra-mobile personal computer，UMPC)、上网本、个人数字助理(personal digital assistant，PDA)、智能手表、智能手环等终端设备，或者该智能移动终端还可以为其他类型的智能移动终端，本发明实施例不作具体限制。

[0033] 实施例一

[0034] 本发明的实施例提供一种数据传输方法，如图2所示包括：

[0035] S101、服务器接收指定设备在当前的安全周期内发送的验证信息；其中，验证信息用于指示服务器向指定手机号码发送提示信息。

[0036] 具体的，当安全周期的统计时长越长，期间向该指定手机号码发送的提示信息的总数越大，得到的风险系数的准确度越高，从而可以更加精确的判别用户的手机号码是否被“短信轰炸”；示例性的，可以将安全周期设置为1天(即24小时)。

[0037] 具体的，用户可以根据实际的情况自行设定安全周期的时长。

[0038] S102、服务器根据安全周期内向指定手机号码发送的提示信息的总数，确定风险系数；其中，风险系数用于指示安全周期内向指定手机号码发送提示信息的频率。

[0039] 可选的，服务器根据安全周期内向指定手机号码发送的提示信息的总数，确定风险系数，如图3所示包括：

[0040] S1020、服务器根据第一预设公式和安全周期内向指定手机号码发送的提示信息的总数，确定风险系数；其中，第一预设公式包括：

[0041] $N=m+n\times y$；

[0042] 其中，N表示安全周期的风险系数，m表示初始风险系数，n为常数，y表示安全周期内向指定手机号码发送的提示信息的总数。

[0043] S103、服务器确定风险系数大于或等于风险阈值，停止向指定手机号码发送提示信息。

[0044] 需要说明的是，在实际的应用中，服务器通过判别每个指定手机号码在安全周期内的风险系数，可以防止短时连续“短信轰炸”的问题，从而保证用户的体验；具体的，风险系数在每个安全周期结束后，需要进行重置，即每个安全周期开始时，该风险系数均为初始设定值；示例性的，该初始设定值可以为0。

[0045] 具体的，提示信息包括验证码，如图3所示该方法还包括：

[0046] S104、服务器确定风险系数小于风险阈值时，向指定手机号码发送提示信息。

[0047] S105、服务器确定从指定设备接收到提示信息时，将当前的安全周期的风险系数重置为初始风险系数，并将安全周期内向指定手机号码发送的提示信息的总数置零。

[0048] 需要说明的是，指定手机号码对应的UE、基站、服务器和指定设备的交互图如图4所示；进行正常验证时，指定设备通过服务器提供的指定验证页面进行验证，服务器首先需要确定指定设备输入的指定账号，以及该指定账号提供的指定手机号码；当用户通过指定设备操作指定手机号码对该指定账号进行验证时，当服务器在有效期内接收到的验证码与该指定设备输入的验证码相同时，则验证成功(这里的验证包括注册验证(用于使用指定手机号码新建账号)、登录验证(通过指定手机号码登记与该指定手机号码绑定的账号)、绑定验证(用于将已有账号和指定手机号码进行绑定)、支付验证(用户通过与该指定手机号码绑定的支付账号进行支付)和安全验证(用于通过指定手机号码对与该指定手机号码绑定的账号进行密码、安全问题的修改)中的任一项)；其中，该验证码可以是字符组合验证码或者数字验证码，每个验证码均具有有效期；示例性的，如该验证码为数字验证码时，验证过程如下：

[0049] 服务器确定风险系数小于风险阈值时，服务器为该指定手机号码生成验证码234567，并通过基站将该验证码234567发送至该指定手机号码对应的UE(服务器将该验证码234567封装在信令消息中，通过通信链路将该信令消息发送给基站，由基站寻呼该指定手机号码当前所处的通信小区，并与该指定手机号码对应的UE建立连接，从而将该验证码234567发送至该UE)。

[0050] 此时，如果从指定设备接收到验证码234567时，由于指定设备输入的验证码与服务器为该指定手机号码生成的验证码234567一致，则验证成功。

[0051] 具体的，当服务器判别每个指定手机号码在安全周期内的风险系数低于风险阈值时，此时说明向该指定手机号码发送提示信息并不存在“短信轰炸”的风险，因此可以正常向该指定手机号码发送提示信息，保证用户的体验。

[0052] 可选的，如图5所示服务器确定风险系数大于或等于风险阈值，停止向指定手机号码发送提示信息，包括：

[0053] S1030、服务器确定风险系数大于或等于风险阈值或者风险系数小于风险阈值时，向指定设备发送携带第一校验识别信息的控制信息；其中，控制信息指示指定设备显示第一校验识别信息，第一校验识别信息包括图形验证码。

[0054] S1031、服务器确定从指定设备接收的第二校验识别信息与第一校验识别信息相

同时，根据第三预设公式确定更新后的风险系数；其中，第三预设公式包括：

[0055] $$M=N\times\left(1-\frac{1}{i}\right);$$

[0056] 其中，M_j表示安全周期更新后的风险系数，i表示安全周期内第二校验识别信息与第一校验识别信息相同的累计次数。

[0057] 具体的，服务器未从指定设备接收到第二校验识别信息或者服务器从指定设备接收到第二校验识别信息与第一校验识别信息不同时，此时存在“短信轰炸”的风险，从而服务器停止向指定手机号码发送提示信息。

[0058] S1032、服务器确定更新后的风险系数大于或等于风险阈值时，停止向指定手机号码发送提示信息。

[0059] 具体的，为了防止用户由于操作失误，导致该指定手机号码在安全周期内的风险系数大于或等于风险阈值，此时用户仍有继续想服务器验证的诉求；因此，当服务器确定风险系数大于或等于风险阈值或者风险系数小于风险阈值时，触发人机校验识别；其中，人机校验识别包括：

[0060] 服务器生成第一校验识别信息，并发生携带该第一校验识别信息的可知信息至指定设备；其中，该第一校验识别信息还包括：字符验证码。

[0061] 当服务器确定从指定设备接收的第二校验识别信息与第一校验识别信息相同时，根据第三预设公式确定更新后的风险系数M：

[0062] $$M=\left(m+n\times y\right)\times\left(1-\frac{1}{i}\right);$$

[0063] 由上述可知，这里引入人机校验识别并不影响风险系数M的增长趋势，即如果用户通过指定设备进行人机校验识别的验证成功次数(即安全周期内第二校验识别信息与第一校验识别信息相同的累计次数)后，如果更新后的风险系数仍大于或等于风险阈值时，此时该指定手机号码存在“短信轰炸”的风险；因此服务器不再向该指定手机号码发送提示信息，也不会再次触发人机校验识别。此处，引入人机校验识别仅为了防止用户由于操作失误，导致该指定手机号码在安全周期内的风险系数大于或等于风险阈值，从而使得用户可以正常的向服务器进行验证。

[0064] 具体的，字符验证码的验证过程与图形验证码的验证类似，此时不再赘述。

[0065] 可选的，如图6所示服务器根据第一预设公式和安全周期内向指定手机号码发送的提示信息的总数，确定风险系数，包括：

[0066] S106、服务器根据第二预设公式和累计周期内向指定手机号码发送的提示信息的总数，确定累计安全系数；其中，累计周期包括至少两个安全周期，累计安全系数用于指示至少两个安全周期内向指定手机号码发送提示信息的频率，第二预设公式包括：

[0067] $$\alpha_{(i,j)}=\sum_{j=1}^{j=j-1}N_{(i,j-1)};$$

[0068] 其中，$\alpha_{(i,j)}$表示第i个累计周期内第j个安全周期的累计安全系数，$N_{(i,j-1)}$表示第i个累计周期内第j-1个安全周期的风险系数，j为大于或等于2的整数。

[0069] S107、服务器确定风险系数小于风险阈值，并且累计安全系数大于或等于安全阈值时，停止向指定手机号码发送提示信息。

[0070] 需要说明的是，为了防止在多个安全周期内并且在每个安全周期内该指定手机号码的风险系数均小于风险阈值的情况，这里引入累计安全系数，用于连续多安全周期内较少次数的向该指定手机号码发送提示信息的情况；因此，当累计周期内该指定手机号码的累计安全系数大于或等于安全系数时，此时存在“短信轰炸”的风险，从而服务器停止向指定手机号码发送提示信息。

[0071] 具体的，当服务器停止向指定手机号码发送提示信息时，此时可以认为服务器将该指定手机号码锁定，即该手机号码在该服务器处于一个锁定的状态；用户在进行解除锁定状态时，可以在下一个安全周期，进行相应的验证操作(如用户通过指定设备向服务器发起解除指定手机号码的锁定状态的请求时，服务器在接收到该解除指定手机号码的锁定状态的请求后，生成对应的第一解除验证码，并通过基站将该第一解除验证码发送至该指定手机号码对应的UE，如果用户通过该指定设备将第二解除验证码发生至服务器，并且服务器判定从该指定设备接收的第二解除验证码与第一解除验证码相同时，则解除该指定手机号码的锁定状态)，从而保证用户的正常使用。

[0072] 具体的，由于累计安全系数是基于该累计周期内每个安全周期的风险系数确定的；因此，随着时间的推移，该累计安全系数也会随着风险系数的更新而进行更新。

[0073] 可选的，提示信息包括验证码；如图6所示该方法还包括：

[0074] S108、服务器确定风险系数小于风险阈值，并且累计安全系数小于安全阈值时，向指定手机号码发送提示信息。

[0075] S105、服务器确定从指定设备接收到提示信息时，将当前的安全周期的风险系数重置为初始风险系数，并将安全周期内向指定手机号码发送的提示信息的总数置零。

[0076] 需要说明的是，在实际的应用中，将当前的安全周期的风险系数重置为初始风险系数，并将安全周期内向指定手机号码发送的提示信息的总数置零后，如果服务器在该安全周期内还是接收到了指定设备发送的验证信息，此时重新执行S101、S102和S103即可。

[0077] 由上述方案可知，本发明的实施例提供的数据传输方法，当服务器接收到指定设备在当前的安全周期内发送的验证信息时，根据该安全周期内向指定手机号码发送的提示信息的总数，从而可以判别出在该安全周期内向该指定手机号码发送提示信息的频率，当确定风险系数大于或等于风险阈值时，说明在当前的安全周期向该指定手机号码发送提示信息的频率过高，存在“短信轰炸”可能，因此停止向该指定手机号码发送提示信息，使得用户可以正常使用该指定手机号码的体验，保证了用户体验，解决了如何识别出用户的手机号码是否被“短信轰炸”的问题。

[0078] 实施例二

[0079] 本发明的实施例提供一种服务器，如图7所示包括：

[0080] 收发单元101，用于接收指定设备在当前的安全周期内发送的验证信息；其中，验证信息用于指示服务器向指定手机号码发送提示信息。

[0081] 处理单元102，用于根据安全周期内收发单元101向指定手机号码发送的提示信息的总数，确定风险系数；其中，风险系数用于指示向指定手机号码发送提示信息的频率。

[0082] 处理单元102，还用于确定风险系数大于或等于风险阈值时，控制收发单元停止向指定手机号码发送提示信息。

[0083] 可选的，处理单元102，具体用于根据第一预设公式和安全周期内收发单元101向

指定手机号码发送的提示信息的总数，确定风险系数；其中，第一预设公式包括：

[0084] N＝m+n×y；

[0085] 其中，N表示安全周期的风险系数，m表示初始风险系数，n为常数，y表示安全周期内向指定手机号码发送的提示信息的总数。

[0086] 可选的，处理单元102，还用于根据第二预设公式和累计周期内收发单元101向指定手机号码发送的提示信息的总数，确定累计安全系数；其中，累计周期包括至少两个安全周期，累计安全系数用于指示至少两个安全周期内向指定手机号码发送提示信息的频率，第二预设公式包括：

[0087] $\alpha_{(i,j)}=\sum_{j=1}^{j=j-1}N_{(i,j-1)}$；

[0088] 其中，$\alpha_{(i,j)}$表示第i个累计周期内第j个安全周期的累计安全系数，$N_{(i,j-1)}$表示第i个累计周期内第j-1个安全周期的风险系数，j为大于或等于2的整数。

[0089] 处理单元102，具体用于确定风险系数小于风险阈值，并且累计安全系数大于或等于安全阈值时，控制收发单元101停止向指定手机号码发送提示信息。

[0090] 可选的，提示信息包括验证码；处理单元102，还用于确定风险系数小于风险阈值时，控制收发单元101向指定手机号码发送提示信息。

[0091] 或者，

[0092] 处理单元102，还用于确定风险系数小于风险阈值，并且累计安全系数小于安全阈值时，控制收发单元101向指定手机号码发送提示信息。

[0093] 处理单元102，还用于确定从指定设备接收到提示信息时，将当前的安全周期的风险系数重置为初始风险系数，并将安全周期内向指定手机号码发送的提示信息的总数置零。

[0094] 可选的，处理单元102，还用于确定风险系数大于或等于风险阈值或者风险系数小于风险阈值时，控制收发单元101向指定设备发送携带第一校验识别信息的控制信息；其中，控制信息指示指定设备显示第一校验识别信息，第一校验识别信息包括图形验证码。

[0095] 处理单元102，还用于确定收发单元101从指定设备接收的第二校验识别信息与第一校验识别信息相同时，根据第三预设公式确定更新后的风险系数；其中，第三预设公式包括：

[0096] $M=N\times\left(1-\frac{1}{i}\right)$；

[0097] 其中，M表示安全周期更新后的风险系数，i表示安全周期内第二校验识别信息与第一校验识别信息相同的累计次数。

[0098] 处理单元102，还用于确定更新后的风险系数大于或等于风险阈值时，控制收发单元101停止向指定手机号码发送提示信息。

[0099] 其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，其作用在此不再赘述。

[0100] 在采用集成的模块的情况下，服务器包括：存储单元、处理单元以及收发单元。处理单元用于对服务器的动作进行控制管理，例如，处理单元用于支持服务器执行图2中的过程S101、S102和S103；收发单元用于支持服务器与其他设备的信息交互。存储单元，用于存

储服务器的程序代码和数据。

[0101] 其中，以处理单元为处理器，存储单元为存储器，收发单元为通信接口为例。其中，服务器参照图8中所示，包括通信接口501、处理器502、存储器503和总线504，通信接口501、处理器502通过总线504与存储器503相连。

[0102] 处理器502可以是一个通用中央处理器(Central Processing Unit，CPU)，微处理器，特定应用集成电路(Application-Specific Integrated Circuit，ASIC)，或一个或多个用于控制本申请方案程序执行的集成电路。

[0103] 存储器503可以是只读存储器(Read-Only Memory，ROM)或可存储静态信息和指令的其他类型的静态存储设备，随机存取存储器(Random Access Memory，RAM)或者可存储信息和指令的其他类型的动态存储设备，也可以是电可擦可编程只读存储器(Electrically Erasable Programmable Read-only Memory，EEPROM)、只读光盘(Compact Disc Read-Only Memory，CD-ROM)或其他光盘存储、光碟存储(包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器可以是独立存在，通过总线与处理器相连接。存储器也可以和处理器集成在一起。

[0104] 其中，存储器503用于存储执行本申请方案的应用程序代码，并由处理器502来控制执行。通讯接口501用于与其他设备进行信息交互，例如与遥控器的信息交互。处理器502用于执行存储器503中存储的应用程序代码，从而实现本申请实施例中所述的方法。

[0105] 此外，还提供一种计算存储媒体(或介质)，包括在被执行时进行上述实施例中的服务器执行的方法操作的指令。另外，还提供一种计算机程序产品，包括上述计算存储媒体(或介质)。

[0106] 应理解，在本发明的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。

[0107] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0108] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0109] 在本申请所提供的几个实施例中，应该理解到，所揭露的系统、设备和方法，可以通过其它的方式实现。例如，以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，仅仅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，设备或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0110] 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。

[0111] 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。

[0112] 所述功能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(可以是个人计算机，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、移动硬盘、只读存储器(英文全称：read-only memory，英文简称：ROM)、随机存取存储器(英文全称：random access memory，英文简称：RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0113] 可以理解地，上述提供的任一种服务器用于执行上文所提供的实施例一对应的方法，因此，其所能达到的有益效果可参考上文实施例一的方法以及下文具体实施方式中对应的方案的有益效果，此处不再赘述。

[0114] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

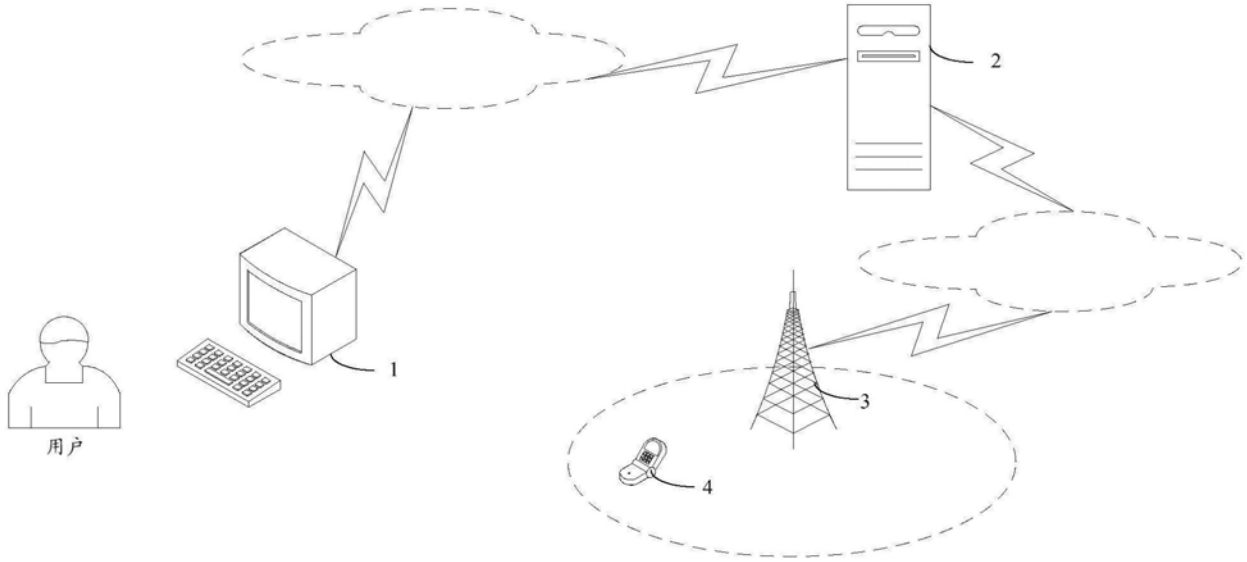

2
1
用户
3
4

图1

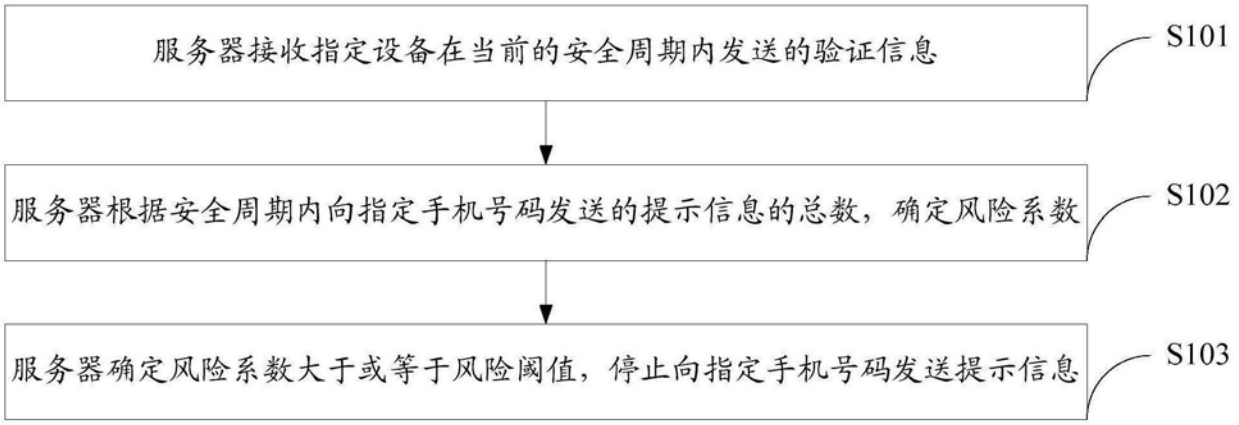

服务器接收指定设备在当前的安全周期内发送的验证信息
S101
服务器根据安全周期内向指定手机号码发送的提示信息的总数，确定风险系数
S102
服务器确定风险系数大于或等于风险阈值，停止向指定手机号码发送提示信息
S103

图2

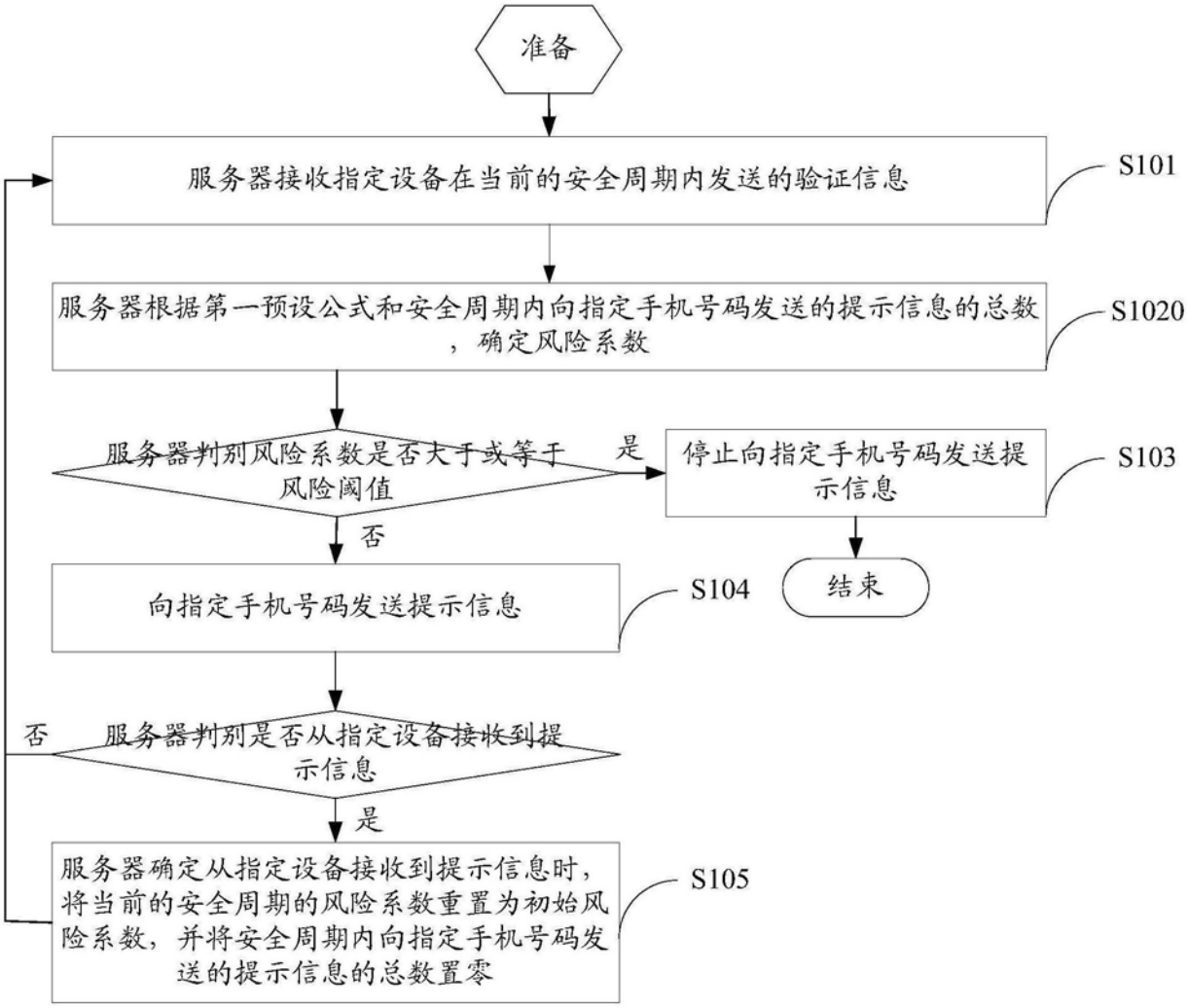

准备
服务器接收指定设备在当前的安全周期内发送的验证信息
S101
服务器根据第一预设公式和安全周期内向指定手机号码发送的提示信息的总数，确定风险系数
S1020
服务器判别风险系数是否大于或等于风险阈值
是
停止向指定手机号码发送提示信息
S103
结束
否
向指定手机号码发送提示信息
S104
否
服务器判别是否从指定设备接收到提示信息
是
服务器确定从指定设备接收到提示信息时，将当前的安全周期的风险系数重置为初始风险系数，并将安全周期内向指定手机号码发送的提示信息的总数置零
S105

图3

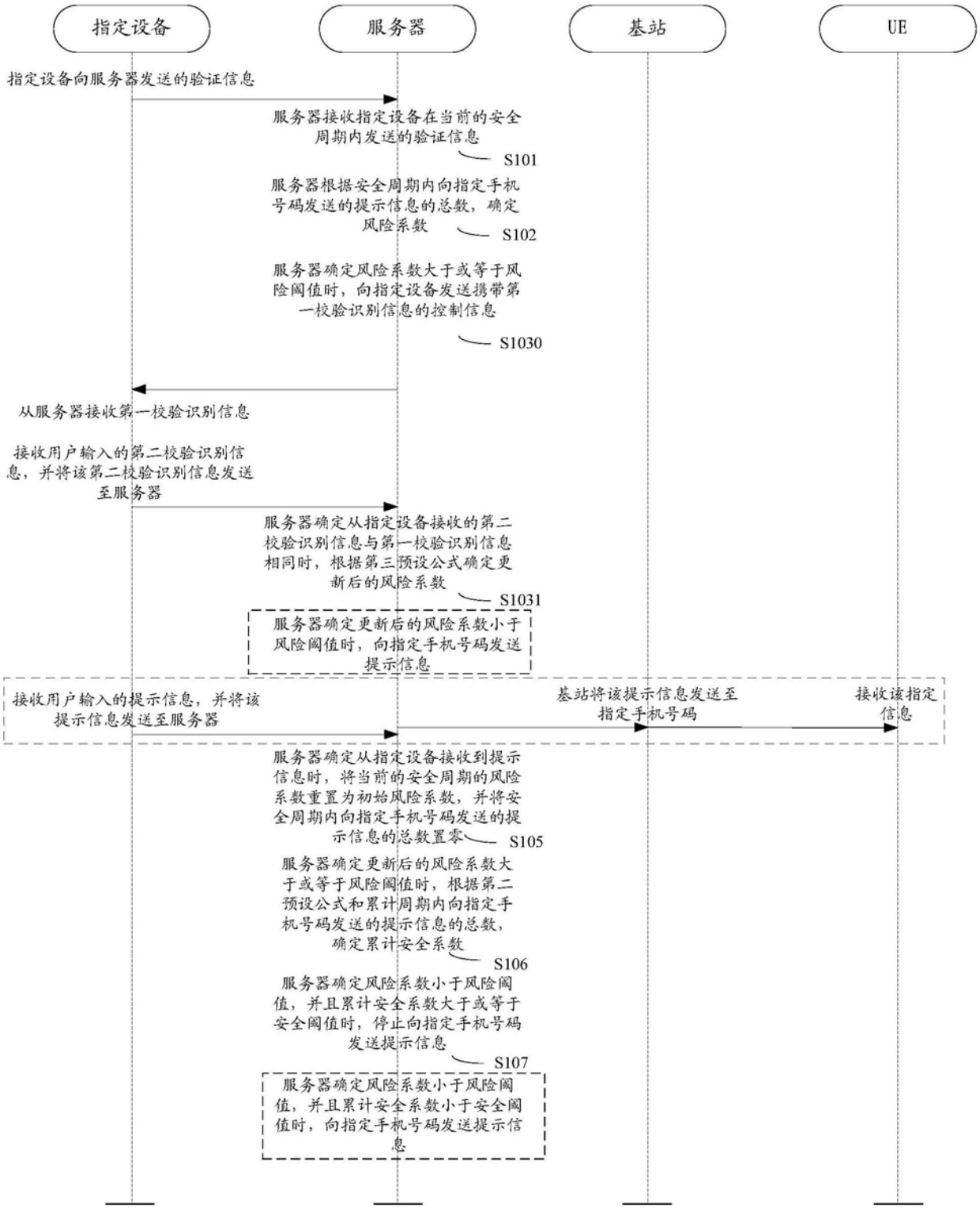

指定设备
服务器
基站
UE
指定设备向服务器发送的验证信息
服务器接收指定设备在当前的安全周期内发送的验证信息
S101
服务器根据安全周期内向指定手机号码发送的提示信息的总数，确定风险系数
S102
服务器确定风险系数大于或等于风险阈值时，向指定设备发送携带第一校验识别信息的控制信息
S1030
从服务器接收第一校验识别信息
接收用户输入的第二校验识别信息，并将该第二校验识别信息发送至服务器
服务器确定从指定设备接收的第二校验识别信息与第一校验识别信息相同时，根据第三预设公式确定更新后的风险系数
S1031
服务器确定更新后的风险系数小于风险阈值时，向指定手机号码发送提示信息
接收用户输入的提示信息，并将该提示信息发送至服务器
基站将该提示信息发送至指定手机号码
接收该指定信息
服务器确定从指定设备接收到提示信息时，将当前的安全周期的风险系数重置为初始风险系数，并将安全周期内向指定手机号码发送的提示信息的总数置零
S105
服务器确定更新后的风险系数大于或等于风险阈值时，根据第二预设公式和累计周期内向指定手机号码发送的提示信息的总数，确定累计安全系数
S106
服务器确定风险系数小于风险阈值，并且累计安全系数大于或等于安全阈值时，停止向指定手机号码发送提示信息
S107
服务器确定风险系数小于风险阈值，并且累计安全系数小于安全阈值时，向指定手机号码发送提示信息

图4

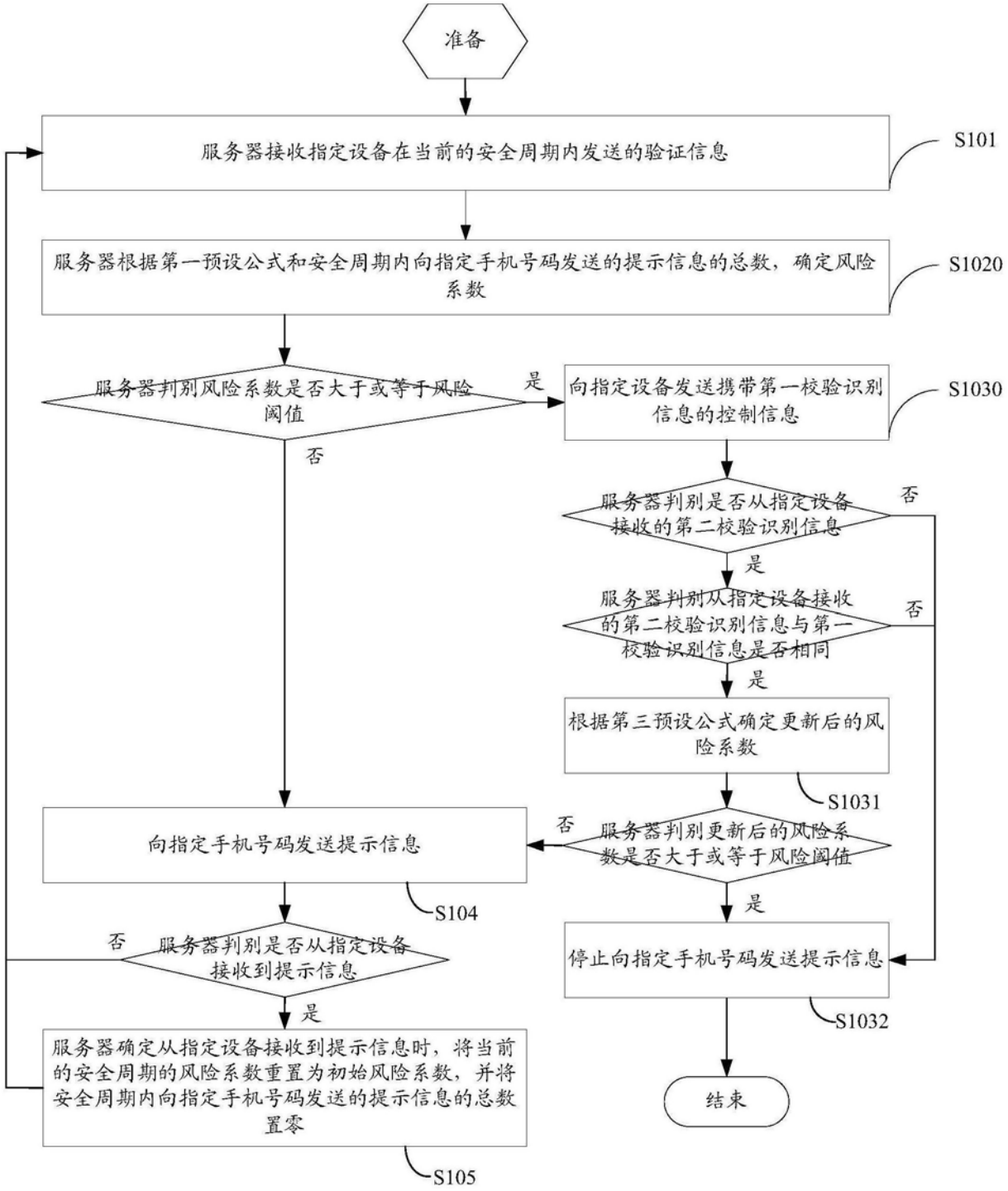

准备
服务器接收指定设备在当前的安全周期内发送的验证信息
S101
服务器根据第一预设公式和安全周期内向指定手机号码发送的提示信息的总数，确定风险系数
S1020
服务器判别风险系数是否大于或等于风险阈值
是
否
向指定设备发送携带第一校验识别信息的控制信息
S1030
服务器判别是否从指定设备接收的第二校验识别信息
否
是
服务器判别从指定设备接收的第二校验识别信息与第一校验识别信息是否相同
否
是
根据第三预设公式确定更新后的风险系数
S1031
服务器判别更新后的风险系数是否大于或等于风险阈值
否
是
向指定手机号码发送提示信息
S104
停止向指定手机号码发送提示信息
S1032
服务器判别是否从指定设备接收到提示信息
否
是
服务器确定从指定设备接收到提示信息时，将当前的安全周期的风险系数重置为初始风险系数，并将安全周期内向指定手机号码发送的提示信息的总数置零
S105
结束

图5

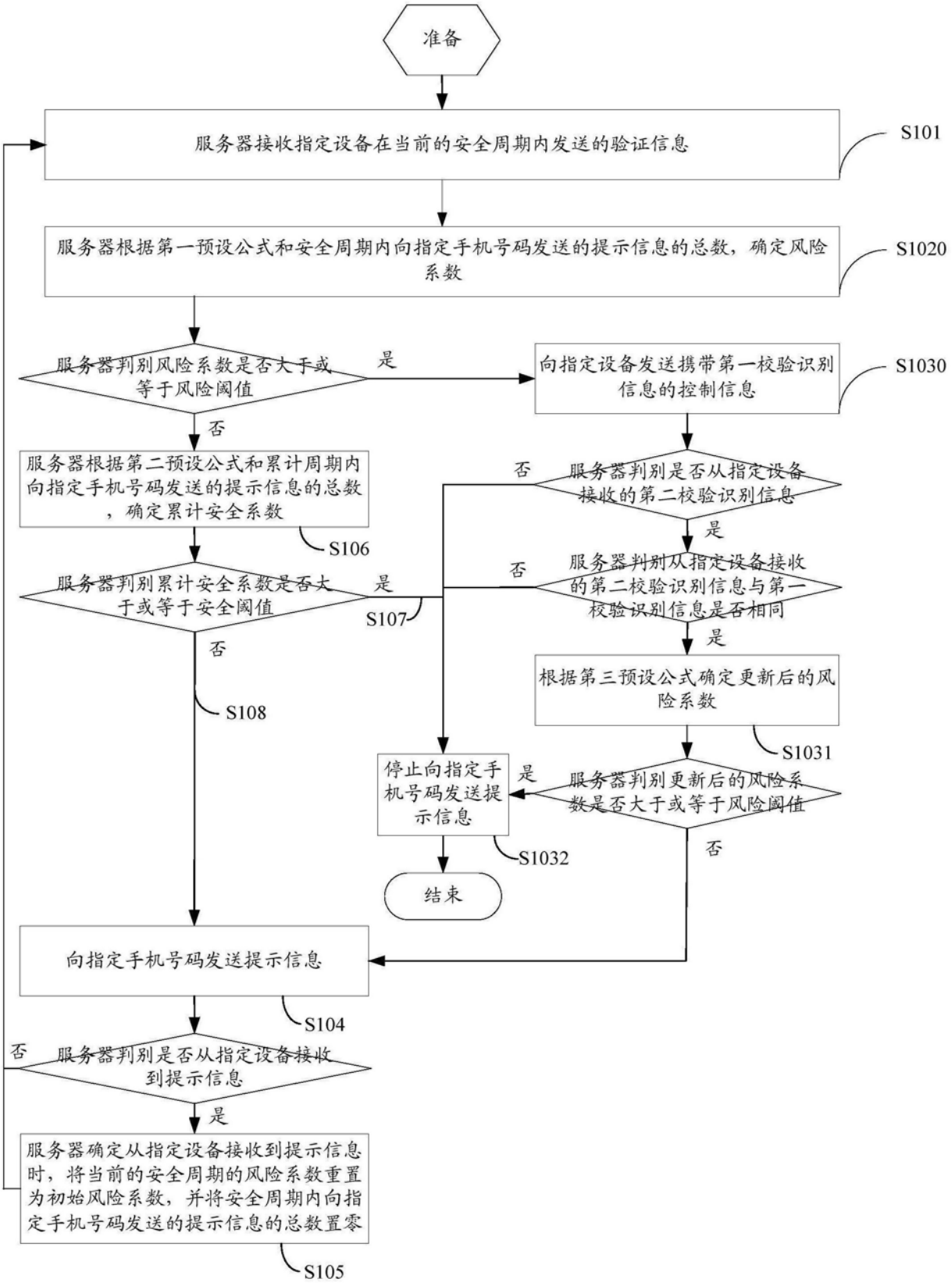

准备
服务器接收指定设备在当前的安全周期内发送的验证信息
S101
服务器根据第一预设公式和安全周期内向指定手机号码发送的提示信息的总数，确定风险系数
S1020
服务器判别风险系数是否大于或等于风险阈值
是
向指定设备发送携带第一校验识别信息的控制信息
S1030
否
服务器根据第二预设公式和累计周期内向指定手机号码发送的提示信息的总数，确定累计安全系数
S106
否
服务器判别是否从指定设备接收的第二校验识别信息
是
服务器判别累计安全系数是否大于或等于安全阈值
是
S107
否
服务器判别从指定设备接收的第二校验识别信息与第一校验识别信息是否相同
是
否
S108
根据第三预设公式确定更新后的风险系数
S1031
停止向指定手机号码发送提示信息
是
服务器判别更新后的风险系数是否大于或等于风险阈值
S1032
否
结束
向指定手机号码发送提示信息
S104
否
服务器判别是否从指定设备接收到提示信息
是
服务器确定从指定设备接收到提示信息时，将当前的安全周期的风险系数重置为初始风险系数，并将安全周期内向指定手机号码发送的提示信息的总数置零
S105

图6

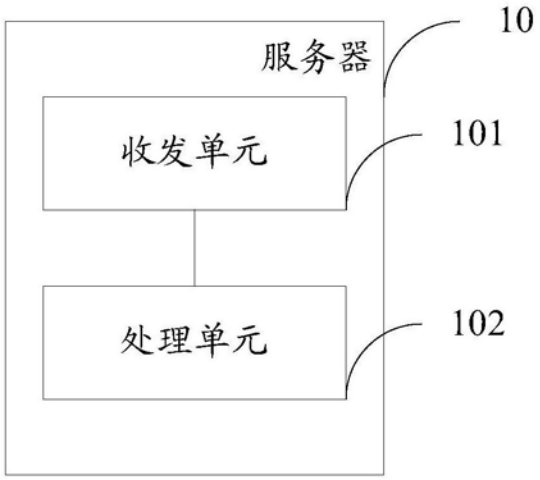


图7

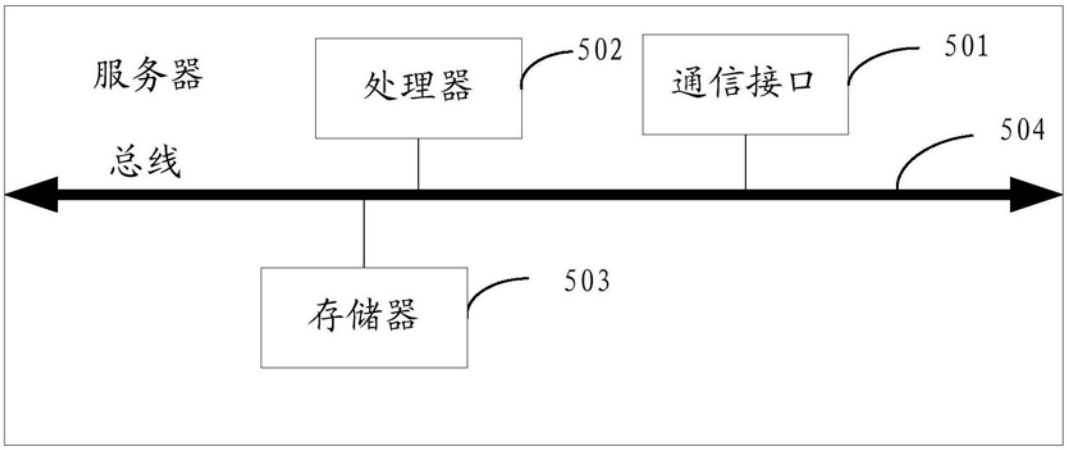


图8