(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 102624677 A
(43)申请公布日 2012.08.01

(21)申请号 201110030037.5

(22)申请日 2011.01.27

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼岛资本大厦一座四层 847 号邮箱

(72)发明人 侯雷明

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 郭润湘

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)

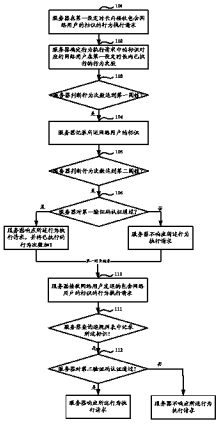
权利要求书 2 页 说明书 9 页 附图 4 页

(54)发明名称

一种网络用户行为监控方法及服务器

(57)摘要

本申请公开了一种网络用户行为监控方法及服务器，主要内容包括：将在设定时长内已执行的行为次数作为是否需要输入验证码的判断依据，在已执行的行为次数达到第一阈值时，将该用户的标识记录至违规列表中，进而在已执行的行为次数达到更高的第二阈值时，要求用户正确输入验证码来表明用户的合法性，并确定是否响应用户的行为执行请求，既可以屏蔽用户通过机器人方式执行的行为，又可以避免高活跃用户被误操作。并且，在当前设定时长结束后，当记录在违规列表中的标识对应的网络用户再次发起行为执行请求时，该网络用户需要通过再次输入验证码来表明其合法性，可以在确保用户行为安全性的同时，降低对用户业务体验的影响。



CN 102624677 A

1. 一种网络用户行为监控的方法，其特征在于，包括：

服务器在第一设定时长内接收包含网络用户的标识的行为执行请求时，确定该标识对应的网络用户在第一设定时长内已执行行为的行为次数；

服务器判断所述行为次数是否达到第一阈值，在达到所述第一阈值时，记录所述网络用户的标识，以及

判断所述执行次数是否达到第二阈值，在达到所述第二阈值时，指示网络用户输入第一验证码，并在输入的第一验证码认证通过时，响应所述执行请求，在第一验证码认证未通过时，不响应所述执行请求，所述第一阈值小于第二阈值；

服务器在第一设定时长结束后，当接收到包含记录的所述网络用户的标识的行为执行请求时，指示记录的所述网络用户的标识对应的网络用户输入第二验证码，并在输入的第二验证码认证通过时，响应记录的所述网络用户的标识对应的网络用户的行为执行请求，否则，不响应该执行请求。

2. 如权利要求 1 所述的方法，其特征在于，所述第一阈值中包含多个数值，其中每个数值表示一个预设周期内允许执行的最大行为次数，不同数值表示的预设周期的时长不同；

服务器判断所述行为次数是否达到第一阈值，具体包括：

服务器确定从第一设定时长开始时至在第一时长内接收所述执行请求的经过时长；

服务器判断所述经过时长内的任一预设周期中已执行的行为次数是否达到该预设周期内允许执行的最大行为次数，若达到，则确定所述行为次数达到第一阈值。

3. 如权利要求 1 所述的方法，其特征在于，在输入的第二验证码认证通过时，所述方法还包括：

服务器在第二验证码认证通过之后的第二设定时长内，始终响应该标识对应的网络用户的行为执行请求。

4. 如权利要求 1 所述的方法，其特征在于，在输入的第一验证码认证通过之后，且响应在第一时长内接收到的所述执行请求之前，所述方法还包括：

服务器判断所述执行次数是否达到第三阈值，在没有达到所述第三阈值时，响应所述执行请求；

所述第二阈值小于第三阈值。

5. 如权利要求 1 ～ 4 任一所述的方法，其特征在于，所述方法还包括：

服务器根据网络用户的优先级确定所述第一阈值和第二阈值，其中，网络用户的优先级越高，确定的第一阈值和第二阈值越大。

6. 一种网络用户行为监控的服务器，其特征在于，包括：

次数确定模块，用于在第一设定时长内接收包含网络用户的标识的行为执行请求时，确定该标识对应的网络用户在第一设定时长内已执行行为的行为次数；

第一判断模块，用于判断所述行为次数是否达到第一阈值，在达到所述第一阈值时，记录所述网络用户的标识，并触发第二判断模块；

第二判断模块，用于判断所述执行次数是否达到第二阈值，并触发验证模块，所述第一阈值小于第二阈值；

验证模块，用于在达到所述第二阈值时，指示网络用户输入预设的第一验证码，在输入的第一验证码认证通过时，响应所述执行请求，否则，不响应所述执行请求，以及，在第一

设定时长结束后，当接收到包含记录的所述网络用户的标识的行为执行请求时，指示记录的所述网络用户的标识对应的网络用户输入第二验证码，并在输入的第二验证码认证通过时，响应记录的所述网络用户的标识对应的网络用户的行为执行请求，否则，不响应该执行请求。

7. 如权利要求 6 所述的服务器，其特征在于，所述第一判断模块，包括 ：

经过时长确定子模块，用于确定从第一设定时长开始时至在第一时长内接收所述执行请求的经过时长 ；

比较子模块，用于在第一阈值中包含多个数值，且其中每个数值表示一个预设周期内允许执行的最大行为次数，不同数值表示的预设周期的时长不同时，判断所述经过时长内的任一预设周期中已执行的行为次数是否达到该预设周期内允许执行的最大行为次数，若达到，则确定所述行为次数达到第一阈值 ；

记录子模块，用于在比较子模块确定所述行为次数达到第一阈值时，记录所述网络用户的标识，并触发第二判断模块。

8. 如权利要求 6 所述的服务器，其特征在于，

所述验证模块，还用于在输入的第二验证码认证通过之后的第二设定时长内始终响应该标识对应的网络用户的行为执行请求。

9. 如权利要求 6 所述的服务器，其特征在于，还包括 ：

第三判断模块，用于在验证模块对输入的第一验证码认证通过之后，判断所述执行次数是否达到第三阈值，在没有达到所述第三阈值时，触发验证模块响应在第一时长内接收到的所述执行请求，所述第二阈值小于第三阈值。

10. 如权利要求 6 ～ 9 任一所述的服务器，其特征在于，还包括 ：

阈值确定模块，用于根据网络用户的优先级确定所述第一阈值和第二阈值，其中，网络用户的优先级越高，确定的第一阈值和第二阈值越大。

一种网络用户行为监控方法及服务器

技术领域

[0001] 本申请涉及计算机技术领域，尤其涉及一种网络用户行为监控方法及服务器。

背景技术

[0002] 随着网络技术的不断发展，越来越多的用户通过网络进行信息交流、购物等。网络的无限潜力也让不法分子乘机潜入，他们通过高频度访问来攻击网络服务器，或者通过网络散布广告，这些行为威胁到网络的安全。

[0003] 为了提高网络安全，防止高频度攻击以及恶意散布广告等行为，提出了如下两种对网络用户的行为进行监控的方案：

[0004] 第一种网络用户行为监控方案是，对用户行为的频度进行监控，其具体内容为：

[0005] 首先，对网络用户的行为实时进行统计，确定一段时间内网络用户行为的发生次数。然后，将已响应的网络用户行为的发生次数与预先设定的次数上限值进行比较，若行为的发生次数已达到次数上限值，则认为该网络用户的行为是通过机器人方式（如通过恶意软件自动触发行为运行的方式）执行的，可认为是非法行为，在确定网络用户行为的发生次数达到次数上限值后，网络用户在该时间段内再次请求的用户行为将不被响应。

[0006] 第二种网络用户行为监控方案是，利用验证码进行监控的方案，其具体内容为：

[0007] 首先，在响应用户请求的行为之前，向用户提供输入界面，要求用户输入系统给出的验证码。然后，将用户输入的验证码与系统给出的验证码进行匹配，若匹配成功，表示该用户行为不是通过机器人方式执行用户行为，因此该用户请求的用户行为将被响应；若匹配不成功，表示该用户行为可能是通过机器人方式执行用户行为，需要重新给出验证码，要求用户输入重新给出的验证码，直至验证码匹配成功才响应用户请求的行为，否则，不响应用户请求的行为。

[0008] 上述两种监控方案虽然能够过滤网络用户通过机器人方式来高频度攻击网络服务器以及恶意散布广告的行为，但仍存在如下缺点：

[0009] 针对第一种频度监控方案，次数上限值很难优选，若次数上限值取值过大，则会使大量的恶意行为被响应，影响网络的安全性，若次数上限值取值过小，又会使某些高活跃用户的合法行为不被响应，影响网络用户的业务体验。即使在次数上限制取值合理的情况下，也有可能使某些特殊的高活跃用户的合法行为不被响应。

[0010] 针对第二种验证码监控方案，由于网络用户的每次用户行为都需要输入验证码，对于大多数合法用户而言，会影响用户行为的流畅体验，增大用户行为执行的复杂度。

发明内容

[0011] 本申请目的在于，提供一种网络用户行为监控方法及服务器，用以解决现有技术中存在的网络用户行为监控不准确以及监控导致用户行为执行复杂的问题。

[0012] 一种网络用户行为监控的方法，包括：

[0013] 服务器在第一设定时长内接收包含网络用户的标识的行为执行请求时，确定该标

识对应的网络用户在第一设定时长内已执行行为的行为次数；

[0014] 服务器判断所述行为次数是否达到第一阈值，在达到所述第一阈值时，记录所述网络用户的标识，以及

[0015] 判断所述执行次数是否达到第二阈值，在达到所述第二阈值时，指示网络用户输入第一验证码，并在输入的第一验证码认证通过时，响应所述执行请求，在第一验证码认证未通过时，不响应所述执行请求，所述第一阈值小于第二阈值；

[0016] 服务器在第一设定时长结束后，当接收到包含记录的所述网络用户的标识的行为执行请求时，指示记录的所述网络用户的标识对应的网络用户输入第二验证码，并在输入的第二验证码认证通过时，响应记录的所述网络用户的标识对应的网络用户的行为执行请求，否则，不响应该执行请求。

[0017] 一种网络用户行为监控的服务器，包括：

[0018] 次数确定模块，用于在第一设定时长内接收包含网络用户的标识的行为执行请求时，确定该标识对应的网络用户在第一设定时长内已执行行为的行为次数；

[0019] 第一判断模块，用于判断所述行为次数是否达到第一阈值，在达到所述第一阈值时，记录所述网络用户的标识，并触发第二判断模块；

[0020] 第二判断模块，用于判断所述执行次数是否达到第二阈值，并触发验证模块，所述第一阈值小于第二阈值；

[0021] 验证模块，用于在达到所述第二阈值时，指示网络用户输入预设的第一验证码，在输入的第一验证码认证通过时，响应所述执行请求，否则，不响应所述执行请求，以及，在第一设定时长结束后，当接收到包含记录的所述网络用户的标识的行为执行请求时，指示记录的所述网络用户的标识对应的网络用户输入第二验证码，并在输入的第二验证码认证通过时，响应记录的所述网络用户的标识对应的网络用户的行为执行请求，否则，不响应该执行请求。

[0022] 本申请有益效果如下：

[0023] 本申请实施例将在设定时长内已执行的行为次数作为是否需要输入验证码的判断依据，在已执行的行为次数达到第一阈值时，将该用户的标识记录至违规列表中，但暂时不作处理，进而在已执行的行为次数达到更高的第二阈值时，要求用户正确输入验证码来表明用户不是通过机器人方式执行行为，根据用户是否能够正确输入验证码来确定是否响应用户的行为执行请求，可以通过次数的阈值来屏蔽用户通过机器人方式执行的行为，又可以通过输入正确的验证码来避免高活跃用户被误操作。并且，在当前设定时长结束后，当记录在违规列表中的标识对应的网络用户再次发起行为执行请求时，该网络用户需要通过再次输入验证码来表明其合法性，可以在确保用户行为安全性的同时，降低对用户业务体验的影响。

附图说明

[0024] 图 1(a) 和图 1(b) 为实施例一的网络用户行为监控方法示意图；

[0025] 图 2 为实施例二的客户端查看好友列表的行为次数分布示意图；

[0026] 图 3(a) 和图 3(b) 为实施例三的网络用户行为监控服务器结构示意图。

具体实施方式

[0027] 为了实现本申请目的，本申请实施例方案提出将在设定时长内已执行的行为次数作为是否需要输入验证码的判断依据，在已执行的行为次数达到第一阈值时，将该用户的标识记录至违规列表中，但暂时不作处理，进而在已执行的行为次数达到更高的第二阈值时，要求用户正确输入验证码来表明用户不是通过机器人方式执行行为，根据用户是否能够正确输入验证码来确定是否响应用户的行为执行请求；并在当前设定时长结束后，由于该用户的标识被记录至违规列表中，因此，该用户再次发起行为执行请求时，该用户需要通过再次输入验证码来表明合法性。通过本申请方案，可以通过次数的阈值来屏蔽用户通过机器人方式执行的行为，又可以通过输入正确的验证码来避免高活跃用户被误操作，同时，当已执行的行为次数达到第一阈值时将用户的标识记录至归为列表中，但在当前设定时长内不对该用户进行处理，而是延迟一段时间后再处理，可以在最大程度上降低对用户业务体验的影响。

[0028] 本申请各实施例中涉及的网络用户可以是通过登录的客户端或启动的浏览器访问网络服务器的用户，也可以是通过登录的客户端或启动的浏览器向网络中的其他客户端或浏览器发送广告等信息的用户。

[0029] 下面结合说明书附图对本申请实施例进行详细说明。

[0030] 实施例一

[0031] 本申请实施例一提供一种网络用户行为监控的方法，如图 1(a) 和图 (b) 所示，该方法包括行为统计期和行为处理期。行为统计期是在设定时长内对网络用户行为进行统计的过程，行为处理期是在设定时长结束后，根据设定时长内确定的违规信息，对网络用户进行处理的过程。

[0032] 行为统计期的具体说明如下：

[0033] 步骤 101：服务器在第一设定时长内接收包含网络用户的标识的行为执行请求。

[0034] 在本步骤中，当某一网络用户在访问网络服务器或是向其他网络用户发送信息之前，需要首先向服务器发送包含自身标识的行为执行请求，在服务器同意响应该行为执行请求时，网络用户请求的行为才得以执行；否则，网络用户请求的行为无法执行。

[0035] 步骤 102：服务器确定行为执行请求中的标识对应的网络用户在第一设定时长内已执行的行为次数。

[0036] 本步骤中确定的行为次数可以是从设定时长开始至当前接收到行为执行请求时，服务器已为所述网络用户响应的行为次数。

[0037] 步骤 103：服务器判断所述行为次数是否达到第一阈值，若到达，则执行步骤 104；否则，执行步骤 108。

[0038] 本步骤是本实施例一方案中的第一次判断步骤，用于根据网络用户在第一设定时长内已执行的行为次数，来判断所述网络用户是否有非法用户的嫌疑。若已执行的行为次数没有达到第一阈值，表示目前网络用户行为没有异常，可以响应该网络用户发起的行为执行请求；若已执行的行为次数达到第一阈值，表示目前网络用户行为存在异常，但服务器是否响应该网络用户发起的行为执行请求需要做进一步判断。

[0039] 步骤 104：服务器记录所述网络用户的标识。

[0040] 在本步骤中，服务器维护一张违规列表，当步骤 103 中的判断结果是行为次数达

到第一阈值时，由于目前网络用户存在异常，因此将所述网络用户的标识记录在违规列表中，同时还可以在违规列表中记录第一设定时长的结束时间，但在第一设定时长内（也就是行为统计期内）不处理该网络用户。

[0041] 步骤 105：服务器判断所述执行次数是否达到第二阈值，若达到，则执行步骤 106；否则，执行步骤 108。

[0042] 所述第一阈值小于第二阈值。

[0043] 本实施例中的网络用户可以设定有不同的优先级（该优先级可以根据网络用户的角色或设定的用户分档方式确定），所述第一阈值和第二阈值的大小可以根据网络用户的优先级的不同而不同。优先级高的网络用户在本实施例中使用的第一阈值和第二阈值大于优先级低的网络用户，也就是说，网络用户的优先级越高，所使用的第一阈值和第二阈值越大。

[0044] 第二阈值是根据经验值或统计值确定的一个临界值，当执行次数达到第二阈值时，表示所述网络用户行为的执行次数过多，该网络用户可能是高活跃用户，但也很可能是通过机器人方式执行行为的用户，因此，可对这一类网络用户采用验证码的监控方案来判断该网络用户是高活跃用户还是通过机器人方式执行行为的用户。

[0045] 需要说明的是，步骤 104 和步骤 105 的执行顺序不固定，可以是先执行步骤 105，再执行步骤 104，或是步骤 104 和步骤 105 同时执行，本实施例不作限定。

[0046] 步骤 106：服务器要求网络用户输入预设的第一验证码，并对输入的第一验证码进行认证；若认证通过，则执行步骤 107；否则，执行步骤 109。

[0047] 在本步骤中，服务器向网络用户提供输入窗口，并向网络用户显示预设的第一验证码，要求网络用户通过输入窗口正确输入显示的所述第一验证码。若网络用户输入的第一验证码与预设的第一验证码匹配，表示网络用户不是通过机器人方式执行行为的用户，而是高活跃用户，该网络用户发送的行为执行请求可以被服务器响应；若网络用户输入的第一验证码与预设的第一验证码不匹配（包括在要求的时间内没有输入或是输入有误），表示网络用户可能是通过机器人方式执行行为的用户，该网络用户发送的行为执行请求还不可以被服务器响应。此时，服务器可更新预设的第一验证码，并要求网络用户重新输入更新后的第一验证码，直至网络用户输入的第一验证码认证通过后服务器才响应该网络用户发送的行为执行请求；若在第一设定时长结束时，网络用户仍没有正确输入第一验证码，则网络用户发送的行为执行请求将被丢弃，行为统计期也将结束。

[0048] 步骤 107：服务器判断所述执行次数是否达到第三阈值，若达到，则在第一设定时长内不再响应该网络用户的所有行为执行请求，结束行为统计期；否则，执行步骤 108。

[0049] 本步骤是本实施一的优选步骤，所述第三阈值是根据服务器的处理能力确定的能够响应的行为执行请求的上限值，表示该服务器在设定时长内能够响应的行为执行请求的最大数量，该第三阈值的取值大小与服务器的硬件能力相关。

[0050] 第三阈值的取值大小除了能够控制服务器的硬件压力外，还能够控制业务上需要承接的服务量上限。

[0051] 步骤 108：服务器响应所述行为执行请求，并将已执行的行为次数加 1，并跳转至步骤 101。

[0052] 步骤 109：服务器不响应所述行为执行请求，并更新预设的第一验证码后跳转至

步骤 106。

[0053] 上述步骤 101 ～步骤 109 是行为统计期的内容，在第一设定时长结束后，进入行为处理期，行为处理期的具体说明如下：

[0054] 步骤 110：服务器接收网络用户发送的包含网络用户的标识的行为执行请求。

[0055] 步骤 111：服务器从违规列表中查询是否记录了所述标识，若是，则执行步骤 112；否则，跳转执行步骤 101。

[0056] 服务器可以在第一设定时长结束后接收到的任意一条行为执行请求时执行行为处理期。优选地，在第一设定时长结束后接收到同一网络用户发送的第一条行为执行请求时执行行为处理期。这样做的好处是：若该网络用户是通过机器人方式执行行为的非法用户，虽然在第一设定时长内执行行为的次数最多等于第二阈值，但在第一设定时长结束后，当重新执行步骤 101 ～步骤 109 的方案时，该非法网络用户还是能够执行第二阈值次非法行为，导致一定的不安全因素。而在第一设定时长结束后立即进入行为处理期，则该非法用户的行为执行请求将不能被响应，最大程度地减少通过机器人方式执行的行为数量。

[0057] 步骤 112：服务器要求网络用户输入预设的第二验证码，并对输入的第二验证码进行认证；若认证通过，则执行步骤 113；否则，执行步骤 114。

[0058] 本步骤的目的是：由于网络用户在行为统计期内已执行的行为次数达到第一阈值，被认为有非法的嫌疑，因此，在本步骤中以验证码的方式来判断该网络用户是否是通过机器人方式执行行为的用户。

[0059] 步骤 113：服务器响应行为执行请求，并在之后的第二设定时长内始终响应该标识对应的网络用户的行为执行请求。

[0060] 在本步骤中，若网络用户能够正确输入第二验证码，则认为该网络用户是高活跃用户而不是通过机器人方式执行行为的用户，因此，可以在连续的第二时长内认为该网络用户一直合法，不必重新进入行为统计期，在第二时长结束后，再重新进入行为统计期，并在违规列表中删除该网络用户的标识。

[0061] 步骤 114：服务器不响应行为执行请求，并更新预设的第二验证码后跳转至步骤 112。

[0062] 若网络用户一直无法正确输入第二验证码，则该网络用户的行为执行请求将不会被响应，也不会重新进入行为统计期，直至网络用户正确输入第二验证码后，才能够执行步骤 113。由于通过机器人方式执行行为的非法用户是不能正确输入第二验证码的，因此此类非法用户的行为执行请求将不会被服务器响应，这减少了非法用户对服务器的高频度攻击以及恶意散布广告的行为发生。

[0063] 实施例二

[0064] 本申请实施例二通过一个具体的实例对实施例一的方案进行详细描述。

[0065] 假设本实施例二中网络用户行为是即时通信客户端查看好友列表的行为，如图 2 所示，为三天内针对不同查看次数对应的人数，以查看次数 1 次为例，在第 1 天有 26458 人查看 1 次，第 2 天有 29567 人查看 1 次，第 3 天有 25962 人查看 1 次。

[0066] 从图 2 中可以看出，绝大部分网络用户每天查看好友列表的次数在 14 次以内，少部分网络用户每天查看好友列别的次数在 15 ～ 19 次，但在每天查看好友列表的次数为 20 次时，人数突然增加，可以认为每天查看好友列别的次数为 20 次是出现异常的临界点。

[0067] 因此，本实施例二对网络用户行为进行抽样检测，将第二阈值设置为 20 次，表示超过 20 次的网络用户需要通过输入验证码来表明自身的合法性。

[0068] 第一阈值设置为 18 次，表示当行为次数达到 18 次时该网络用户将会被认为有非法嫌疑，录入违规列表。

[0069] 第三阈值为 100 次，表示服务器在第一设定时长内最多能够响应 100 次行为执行请求。

[0070] 第一设定时长为 1 天，从 00:00 起连续 24 小时，第二设定时长为 2 天，即连续的 48 小时。

[0071] 本实施例二的方案如下：

[0072] 第一步：服务器在 12:00 时接收到网络用户发起的查看请求，从第一设定时长开始时间 00:00 已经经过 12 小时，设定此时经过时长为 12 小时。

[0073] 第二步：服务器根据计数器确定网络用户在这 12 小时内已查看好友列表 12 次。

[0074] 第三步：服务器判断已查看好友列表的次数是否达到第一阈值。

[0075] 在本实施例中，可以只以一个数值作为第一阈值，但可能出现网络黑客破解设定的第一阈值的问题，这是因为：网络黑客可以通过不断地改变在第一设定时长内执行的查看操作次数来破解所述第一阈值，非法用户只要在设定时长内执行不超过第一阈值次数的查看操作，就可以规避进入行为处理期，使得非法用户的查看请求能够一直被服务器响应却无需通过输入验证码来证明合法性。为此，本实施例二中的第一阈值可以是一组数值，第一阈值中的每个数值分别表示一个预设周期内允许执行的最大行为次数，不同数值表示的预设周期的时长可以不同。在经过的时长内，只要存在某一预设周期内已执行的查看操作次数达到该预设周期内允许执行的最大行为次数时，就认为在第一设定时长内已执行的行为次数达到第一阈值，该网络用户有非法的嫌疑。由上述内容可知，所述第一阈值中包含的数值越多，被破解的难度就越大。

[0076] 具体的做法为：

[0077] 首先，服务器确定从第一设定时长开始时至在第一时长内接收所述执行请求的经过时长。

[0078] 在本实施例中，当前的经过时长为 12 小时。

[0079] 然后，服务器确定第一阈值中包含的每个数值，以及每个数值对应的预设周期。

[0080] 假设预设有 2 个周期，第一个周期的时长是 1 分钟，第 1 个周期内允许执行的最大行为次数为 5 次；第二个周期的时长是 6 小时，第 2 周期内内允许执行的最大行为次数为 15 次。

[0081] 最后，服务器判断在经过时长的 12 小时内，是否满足以下条件：

[0082] 有 1 分钟内执行的行为次数达到 5 次，或有 6 小时内执行的行为次数达到 15 次的情况。

[0083] 只要上述任一条件满足，服务器就判定已查看好友列表的次数达到第一阈值。假设本实施例中，在第一设定时长开始后在 00:05 ～ 00:06 这 1 分钟内执行的行为次数达到了 5 次，即使其他 1 分钟周期内执行的行为次数都没达到 5 次，且每 6 小时周期内执行的行为也没有达到 15 次，也认为已查看好友列表的次数达到第一阈值。

[0084] 上述判断已查看好友列表的次数是否达到第一阈值的方案可以在每次收到网络

用户发起的查看请求时执行。较优地，考虑到服务器要为大量的网络用户提供服务，若在每一次接收到查看请求时都重复统计每个预设周期内的行为次数，可能会导致服务器的运算量较大，因此，本实施例提出以下这种较优的方案：

[0085] 以预设的周期为单位，实时计算在该预设的周期内执行的行为次数，当某一预设的周期内的行为次数达到最大行为次数时，就认为该网络用户查看好友列表的次数达到第一阈值，在第一设定时长结束之前，不必再对该网络用户查看好友列表的次数是否达到第一阈值进行判断。例如：若预设的周期是 1 分钟，允许执行的最大行为次数为 5 次时，可以以 1 分钟为周期，记录 1 分钟内执行的行为次数。例如：记录 00:00 ～ 00:01 的行为次数为 1 次，00:01 ～ 00:02 的行为次数为 2 次，以此类推。若在 00:10 ～ 00:15 的行为次数达到最大行为次数 5 次时，确定该网络用户查看好友列表的次数达到第一阈值，在 02:00 接收到该网络用户发起的查看请求时，可以不再重复判断，直接认定网络用户查看好友列表的次数达到第一阈值。若在 00:05 ～ 00:06 这 1 分钟的周期内行为次数达到最大行为次数 5 次，则在 00:06 之后的第一设定时长内接收到该网络用户发起的查看请求时，只需要根据在 00:05 ～ 00:06 这 1 分钟的周期内执行的行为次数达到 5 次的信息，确定网络用户查看好友列表的次数已达到第一阈值。

[0086] 第四步：服务器在违规列表中记录网络用户的标识，但在第一设定时长内不对该网络用户作任何处理。

[0087] 第五步：服务器判断已查看好友列表的次数是否达到第二阈值，若达到，则执行第六步；否则，执行第七步。

[0088] 第六步：服务器响应网络用户的查看请求，并将已查看好友列表的次数加 1 次后跳转至第一步。

[0089] 循环执行上述步骤，在已查看好友列表的次数达到 20 次时，执行第七步：向网络用户显示第一验证码。

[0090] 第八步：对网络用户输入的验证码（包括网络用户没有输入即内容为空的验证码）与第一验证码进行匹配，在匹配成功时跳转至第九步；否则跳转至第十步。

[0091] 第九步：服务器判断已查看好友列表的次数是否达到第三阈值，若是，不响应该查看请求；否则，跳转至第六步。

[0092] 第十步：服务器更新第一验证码后跳转至第八步。

[0093] 直至第一设定时长结束，进入行为处理期。

[0094] 第十一步：服务器接收网络用户发送的查询请求，该网络用户的标识记录在违规列表中。

[0095] 第十二步：服务器要求网络用户输入预设的第二验证码，若输入的第二验证码认证通过，则执行第十三步；否则，执行第十四步。

[0096] 第十三步：服务器响应查看请求，并在之后的 48 小时内始终响应该标识对应的网络用户的查看请求。

[0097] 第十四步：服务器不响应行为执行请求，并更新第二验证码后跳转至第十二步。

[0098] 实施例三

[0099] 如图 3(a) 所示，为本申请实施例三中提供的一种网络用户行为监控的服务器结构示意图，包括次数确定模块 11、第一判断模块 12、第二判断模块 13 和验证模块 14，其中：

次数确定模块 11 用于在第一设定时长内接收包含网络用户标识的行为执行请求时，确定该标识对应的网络用户在第一设定时长内已执行行为的行为次数；第一判断模块 12 用于判断所述行为次数是否达到第一阈值，在达到所述第一阈值时，记录所述网络用户的标识，并触发第二判断模块 13；第二判断模块 13 用于判断所述执行次数是否达到第二阈值，并触发验证模块 14；验证模块 14 用于在达到所述第二阈值时，指示网络用户输入预设的第一验证码，在输入的第一验证码认证通过时，响应所述执行请求，否则，不响应所述执行请求，以及，在第一设定时长结束后，当接收包含记录的所述网络用户的标识的行为执行请求时，指示网络用户输入第二验证码，并在输入的第二验证码认证通过时，响应记录的所述网络用户的标识对应的网络用户的行为执行请求，否则，不响应该执行请求。

[0100] 所述验证模块 14 还用于在输入的第二验证码认证通过之后的第二设定时长内始终响应该标识对应的网络用户的行为执行请求。

[0101] 进一步地，如图 3(b) 所示，所述服务器还包括第三判断模块 15，用于在验证模块 14 对输入的第一验证码认证通过之后，判断所述执行次数是否达到第三阈值，在没有达到所述第三阈值时，触发验证模块 14 响应在第一时长内接收到的所述执行请求。

[0102] 所述服务器还包括阈值确定模块 16，用于根据网络用户的优先级确定所述第一阈值和第二阈值，其中，网络用户的优先级越高，确定的第一阈值和第二阈值越大。

[0103] 所述第一判断模块 12 进一步包括经过时长确定子模块 21、比较子模块 22 和记录子模块 23，其中：经过时长确定子模块 21 用于确定从第一设定时长开始时至在第一时长内接收所述执行请求的经过时长；比较子模块 22 用于在第一阈值中包含多个数值，且其中每个数值表示一个预设周期内允许执行的最大行为次数，不同数值表示的预设周期的时长不同时，判断所述经过时长内的任一预设周期中已执行的行为次数是否达到该预设周期内允许执行的最大行为次数，若达到，则确定所述行为次数达到第一阈值；记录子模块 23 用于在比较子模块 22 确定所述行为次数达到第一阈值时，记录所述网络用户的标识，并触发第二判断模块 13。

[0104] 本实施例三中的服务器还包括能够实现实施例一和实施例二各步骤的功能实体。

[0105] 通过本申请实施例提供的方案，可以相对宽松地设定第二阈值，对于高活跃用户而言，在第一设定时长内执行次数达到第二阈值时可以通过输入的验证码表明自身的合法性，既避免了由于第二阈值的限制将高活跃用户的行为被限制的问题，又克服了每次都要输入验证码导致业务平滑性受到影响的问题；同时，根据设定的第一阈值将有非法嫌疑的网络用户的标识记录在违规列表中，但在第一设定时长内不对网络用户进行处理，而是延后至第一设定时长结束后再进行处理，一方面使服务器对网络用户的监控不易被用户察觉，另一方面由于处理的延后也使网络黑客不易测试出第一阈值的数值；另外，第一阈值可以设置为多个值，可以进一步防止黑客破解第一阈值的数值。除了上述有益效果外，本申请实施例方案中还根据服务器的硬件能力设置第三阈值，使服务器的业务压力不至于过大，还能够控制业务上需要承接的服务量上限；另外，在行为处理期对网络用户输入的第二验证码认证通过时可以确定该网络用户是高活跃用户，所以在第二设定时长内始终信任该网络用户，可以在保证网络安全的情况下减少服务器的处理数据量，还可以保证用户体验的顺畅，让正常用户的业务流程不会被验证码输入操作打断。

[0106] 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序

产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[0107] 本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0108] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0109] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0110] 尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

[0111] 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

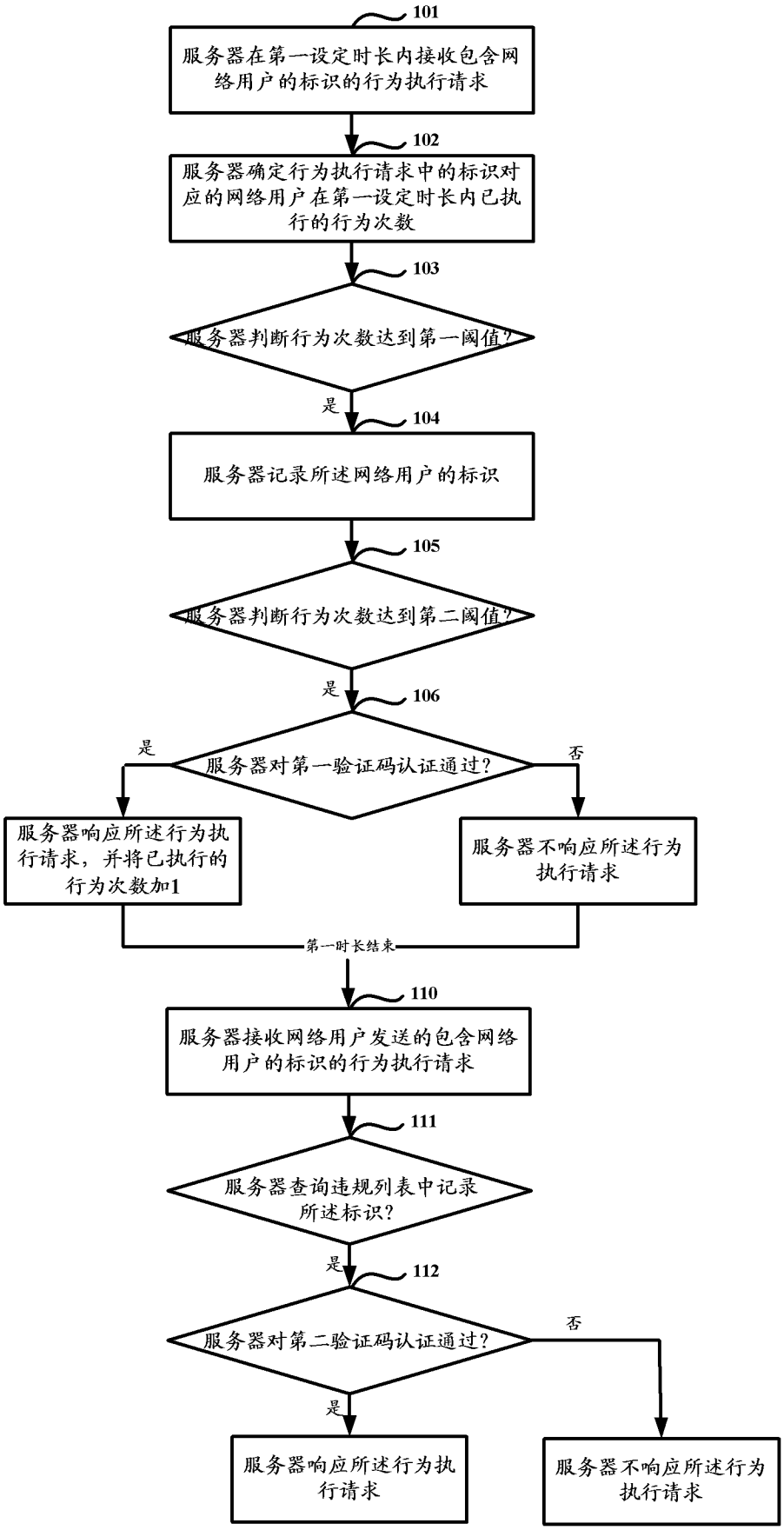

101
服务器在第一设定时长内接收包含网络用户的标识的行为执行请求
102
服务器确定行为执行请求中的标识对应的网络用户在第一设定时长内已执行的行为次数
103
服务器判断行为次数达到第一阈值?
是
104
服务器记录所述网络用户的标识
105
服务器判断行为次数达到第二阈值?
是
106
服务器对第一验证码认证通过?
是
否
服务器响应所述行为执行请求，并将已执行的行为次数加1
服务器不响应所述行为执行请求
第一时长结束
110
服务器接收网络用户发送的包含网络用户的标识的行为执行请求
111
服务器查询违规列表中记录所述标识?
是
112
服务器对第二验证码认证通过?
否
是
服务器响应所述行为执行请求
服务器不响应所述行为执行请求

图 1(a)

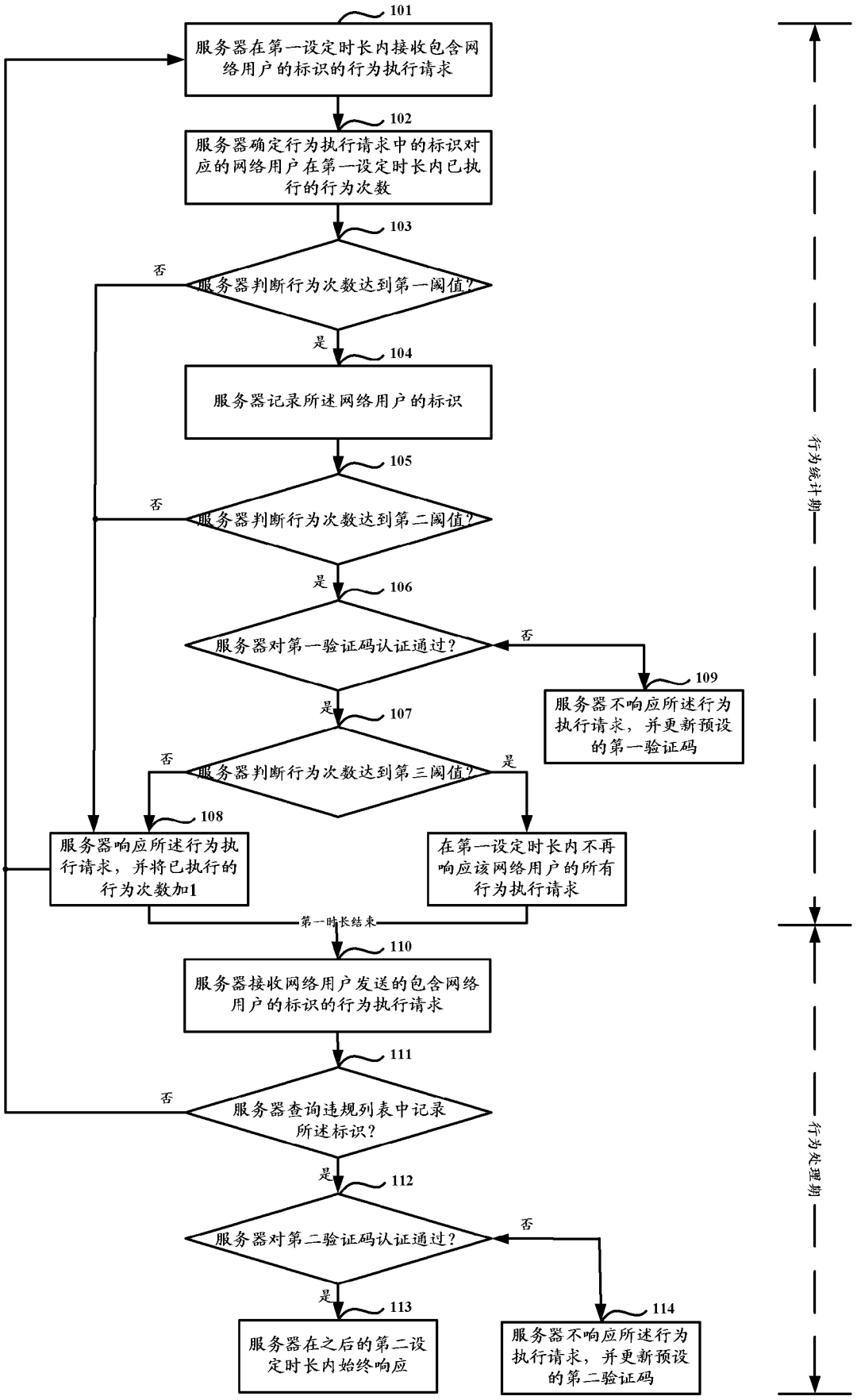

101
服务器在第一设定时长内接收包含网络用户的标识的行为执行请求
102
服务器确定行为执行请求中的标识对应的网络用户在第一设定时长内已执行的行为次数
103
服务器判断行为次数达到第一阈值?
否
是
104
服务器记录所述网络用户的标识
105
服务器判断行为次数达到第二阈值?
否
是
106
服务器对第一验证码认证通过?
否
109
服务器不响应所述行为执行请求，并更新预设的第一验证码
是
107
服务器判断行为次数达到第三阈值?
否
是
108
服务器响应所述行为执行请求，并将已执行的行为次数加1
在第一设定时长内不再响应该网络用户的所有行为执行请求
第一时长结束
110
服务器接收网络用户发送的包含网络用户的标识的行为执行请求
111
服务器查询违规列表中记录所述标识?
否
是
112
服务器对第二验证码认证通过?
否
是
113
服务器在之后的第二设定时长内始终响应
114
服务器不响应所述行为执行请求，并更新预设的第二验证码
行为统计期
行为处理期

图 1(b)

查看次数	第1天	第2天	第3天
1	26458	29567	25962
2	4469	4188	4146
3	2571	4870	7106
4	1519	1544	1467
5	1429	1366	1467
6	828	847	1028
7	559	612	640
8	369	394	422
9	273	273	326
10	211	238	248
11	168	182	188
12	134	126	165
13	103	130	134
14	100	85	121
15	88	95	102
16	47	62	78
17	37	51	80
18	34	44	51
19	44	35	52
20	507	495	515
21	0	1	1
23	1	0	0
42	0	0	0
100	0	1	0

图 2

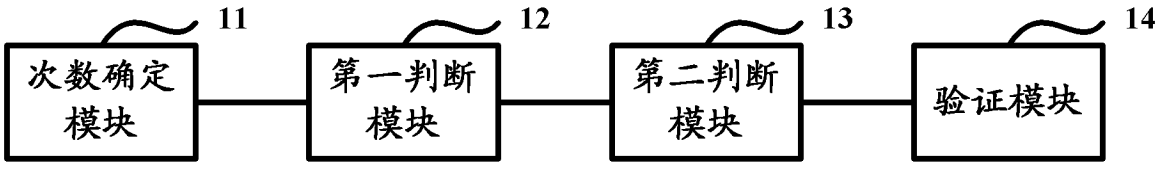


图 3(a)

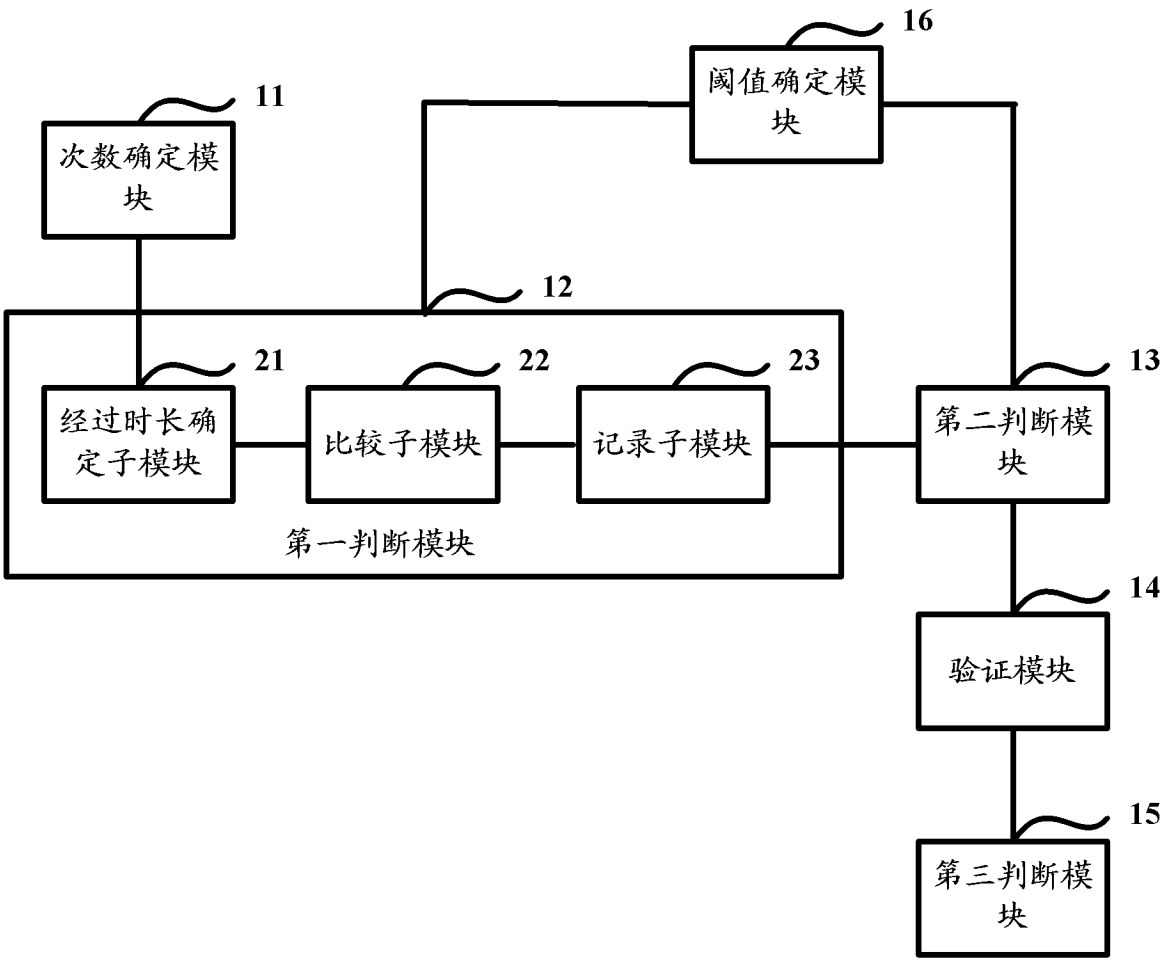

16
阈值确定模块
11
次数确定模块
12
21
22
23
13
经过时长确定子模块
比较子模块
记录子模块
第二判断模块
第一判断模块
14
验证模块
15
第三判断模块

图 3(b)