(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 110278271 A
(43)申请公布日 2019.09.24

(21)申请号 201910550107.6

(22)申请日 2019.06.24

(71)申请人 厦门美图之家科技有限公司
地址 361000 福建省厦门市火炬高新区软件园华讯楼C区B1F-089

(72)发明人 陈鸿图 阮永丽

(74)专利代理机构 北京超凡宏宇专利代理事务所(特殊普通合伙) 11463
代理人 刘亚飞

(51)Int.Cl.
H04L 29/08(2006.01)

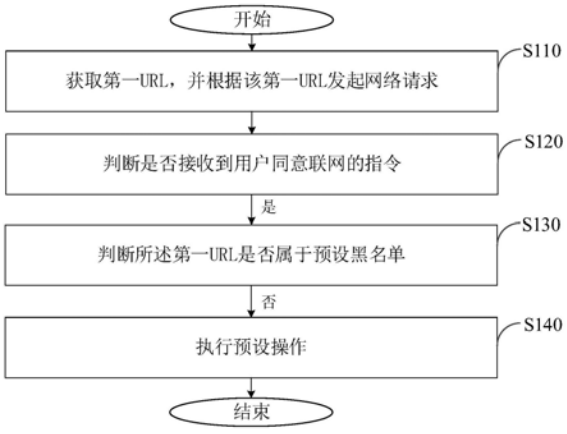
权利要求书2页 说明书7页 附图3页

(54)发明名称

网络请求控制方法、装置及终端设备

(57)摘要

本发明实施例提供的网络请求控制方法、装置及终端设备，涉及网络请求控制技术领域。所述网络请求控制方法包括：获取第一URL，并根据该第一URL发起网络请求；判断是否接收到用户同意联网的指令，其中，所述用户同意联网的指令基于所述终端设备响应用户的操作生成；若接收到用户同意联网的指令，则判断所述第一URL是否属于预设黑名单；若所述第一URL不属于预设黑名单，则执行预设操作，其中，该预设操作包括根据所述网络请求进行联网处理。通过上述方法，可以提高网络请求的控制效率。



CN 110278271 A

1.一种网络请求控制方法,其特征在于,应用于终端设备,该网络请求控制方法包括:

获取第一URL,并根据该第一URL发起网络请求;

判断是否接收到用户同意联网的指令,其中,所述用户同意联网的指令基于所述终端设备响应用户的操作生成;

若接收到用户同意联网的指令,则判断所述第一URL是否属于预设黑名单;

若所述第一URL不属于预设黑名单,则执行预设操作,其中,该预设操作包括根据所述网络请求进行联网处理。

2.如权利要求1所述的网络请求控制方法,其特征在于,所述终端设备与服务器通信连接,所述执行预设操作的步骤,包括:

根据所述网络请求建立网络连接;

判断所述第一URL是否被重定向到第二URL;

若所述第一URL未被重定向到第二URL,则根据所述网络连接向所述服务器发送数据请求,并接收所述服务器响应所述数据请求发送的响应数据。

3.如权利要求2所述的网络请求控制方法,其特征在于,所述执行预设操作的步骤,还包括:

若所述第一URL被重定向到第二URL,则判断所述第二URL是否属于所述预设黑名单;

若所述第二URL属于所述预设黑名单,则取消第二URL对应的网络请求,其中,在所述第一URL被重定向到第二URL时,根据该第二URL向所述服务器发起新的网络请求。

4.如权利要求3所述的网络请求控制方法,其特征在于,所述执行预设操作的步骤,还包括:

若所述第二URL不属于所述预设黑名单,则根据所述第二URL对应的网络请求进行联网处理。

5.如权利要求1-4任意一项所述的网络请求控制方法,其特征在于,所述获取第一URL的步骤,包括:

通过预设组件获取HttpUrlConnection组件对应的第一URL。

6.如权利要求1-4任意一项所述的网络请求控制方法,其特征在于,还包括预先建立所述预设黑名单的步骤,该步骤包括:

根据接收到的黑名单请求信息获取对应的URL;

根据获取的所述URL建立预设黑名单。

7.一种网络请求控制装置,其特征在于,应用于终端设备,该网络请求控制装置包括:

网络请求发起模块,用于获取第一URL,并根据该第一URL发起网络请求;

第一判断模块,用于判断是否接收到用户同意联网的指令,其中,所述用户同意联网的指令基于所述终端设备响应用户的操作生成;

第二判断模块,用于在接收到用户同意联网的指令时,判断所述第一URL是否属于预设黑名单;

执行模块,用于在所述第一URL不属于预设黑名单时,执行预设操作,其中,该预设操作包括根据所述网络请求进行联网处理。

8.如权利要求7所述的网络请求控制装置,其特征在于,所述终端设备与服务器通信连接,所述执行模块包括:

网络连接建立子模块，用于根据所述网络请求建立网络连接；

第一判断子模块，用于判断所述第一URL是否被重定向到第二URL；

数据请求子模块，用于在所述第一URL未被重定向到第二URL时，根据所述网络连接发送数据请求，并接收服务器响应所述数据请求发送的响应数据。

9.如权利要求8所述的网络请求控制装置，其特征在于，所述执行模块还包括：

第二判断子模块，用于在所述第一URL被重定向到第二URL时，判断所述第二URL是否属于所述预设黑名单；

网络请求取消子模块，用于在所述第二URL属于所述预设黑名单时，则取消第二URL对应的网络请求。

10.一种终端设备，其特征在于，包括存储器和处理器，所述处理器用于执行所述存储器中存储的可执行的计算机程序，以实现权利要求1-6任意一项所述的网络请求控制方法。

网络请求控制方法、装置及终端设备

技术领域

[0001] 本申请涉及网络请求控制技术领域，具体而言，涉及一种网络请求控制方法、装置及终端设备。

背景技术

[0002] 在实际应用中，需要控制App网络请求的开关或者定向停止掉某一个或某一类网络请求。在App开发中可以使用OkHttp网络组件在发起网络请求之前对每一个实例化的OkHttpClient中添加拦截器Interceptor，该拦截器中isNetworkTrafficAllowed变量为false时，则由该OkHttpClient发起的请求都会直接返回response code＝HTTP_BAD_REQUEST以中止进程。如果该isNetworkTrafficAllowed为true，则发起联网请求。

[0003] 但是，经发明人研究发现，在现有技术中，仍然要明文对每一个初始化的OkHttpClient设置相应的拦截器Interceptor，如果后续的业务开发新定义了一个OkHttpClient而没有添加拦截器，则仍然会访问网络，该请求不会被拦截下，并且有些第三方SDK是App进程创建后即自动运行的，不受App开发的逻辑控制，从而存在着控制效率低的问题。

发明内容

[0004] 有鉴于此，本发明的目的在于提供一种网络请求控制方法、装置及终端设备，以改善现有技术中存在的问题。

[0005] 为实现上述目的，本发明实施例采用如下技术方案：

[0006] 一种网络请求控制方法，应用于终端设备，该网络请求控制方法包括：

[0007] 获取第一URL，并根据该第一URL发起网络请求；

[0008] 判断是否接收到用户同意联网的指令，其中，所述用户同意联网的指令基于所述终端设备响应用户的操作生成；

[0009] 若接收到用户同意联网的指令，则判断所述第一URL是否属于预设黑名单；

[0010] 若所述第一URL不属于预设黑名单，则执行预设操作，其中，该预设操作包括根据所述网络请求进行联网处理。

[0011] 在本发明实施例较佳的选择中，所述执行预设操作的步骤，包括：

[0012] 根据所述网络请求建立网络连接；

[0013] 判断所述第一URL是否被重定向到第二URL；

[0014] 若所述第一URL未被重定向到第二URL，则根据所述网络连接向所述服务器发送数据请求，并接收所述服务器响应所述数据请求发送的响应数据。

[0015] 在本发明实施例较佳的选择中，所述执行预设操作的步骤，还包括：

[0016] 若所述第一URL被重定向到第二URL，则判断所述第二URL是否属于所述预设黑名单；

[0017] 若所述第二URL属于所述预设黑名单，则取消第二URL对应的网络请求，其中，在所

述第一URL被重定向到第二URL时，根据该第二URL向所述服务器发起新的网络请求。

[0018] 在本发明实施例较佳的选择中，所述执行预设操作的步骤，还包括：

[0019] 若所述第二URL不属于所述预设黑名单，则根据所述第二URL对应的网络请求进行联网处理。

[0020] 在本发明实施例较佳的选择中，所述获取第一URL的步骤，包括：

[0021] 通过预设组件获取HttpUrlConnection组件对应的第一URL。

[0022] 在本发明实施例较佳的选择中，所述网络请求控制方法还包括预先建立所述预设黑名单的步骤，该步骤包括：

[0023] 根据接收到的黑名单请求信息获取对应的URL；

[0024] 根据获取的所述URL建立预设黑名单。

[0025] 本发明实施例还提供了一种网络请求控制装置，应用于终端设备，该网络请求控制装置包括：

[0026] 网络请求发起模块，用于获取第一URL，并根据该第一URL发起网络请求；

[0027] 第一判断模块，用于判断是否接收到用户同意联网的指令，其中，所述用户同意联网的指令基于所述终端设备响应用户的操作生成；

[0028] 第二判断模块，用于在接收到用户同意联网的指令时，判断所述第一URL是否属于预设黑名单；

[0029] 执行模块，用于在所述第一URL不属于预设黑名单时，执行预设操作，其中，该预设操作包括根据所述网络请求进行联网处理。

[0030] 在本发明实施例较佳的选择中，所述终端设备与服务器通信连接，所述执行模块包括：

[0031] 网络连接建立子模块，用于根据所述网络请求建立网络连接；

[0032] 第一判断子模块，用于判断所述第一URL是否被重定向到第二URL；

[0033] 数据请求子模块，用于在所述第一URL未被重定向到第二URL时，根据所述网络连接发送数据请求，并接收服务器响应所述数据请求发送的响应数据。

[0034] 在本发明实施例较佳的选择中，所述执行模块还包括：

[0035] 第二判断子模块，用于在所述第一URL被重定向到第二URL时，判断所述第二URL是否属于所述预设黑名单；

[0036] 网络请求取消子模块，用于在所述第二URL属于所述预设黑名单时，则取消第二URL对应的网络请求。

[0037] 本发明实施例还提供了一种终端设备，包括存储器和处理器，所述处理器用于执行所述存储器中存储的可执行的计算机程序，以实现上述的网络请求控制方法。

[0038] 本发明实施例提供的网络请求控制方法、装置及终端设备，通过在发起网络请求后判断是否接收到用户同意联网的指令，并在接收到用户同意联网的指令后，判断第一URL是否属于预设黑名单，在所述第一URL不属于预设黑名单时，根据所述网络请求进行联网处理，以避免在发起网络请求之前针对每一个网络请求进行设置以判断是否属于预设的黑名单，以提高网络请求的控制效率。

附图说明

[0039] 为了更清楚地说明本申请实施例的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，应当理解，以下附图仅示出了本申请的某些实施例，因此不应被看作是对范围的限定，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相关的附图。

[0040] 图1为本发明实施例提供的网络请求控制系统的结构框图。

[0041] 图2为本发明实施例提供的终端设备的结构框图。

[0042] 图3为本发明实施例提供的网络请求控制方法的流程示意图。

[0043] 图4为本发明实施例提供的应用示意图。

[0044] 图5为本发明实施例提供的步骤S140的流程示意图。

[0045] 图6为本发明实施例提供的步骤S140的另一流程示意图。

[0046] 图7为本发明实施例提供的网络请求控制装置的结构框图。

[0047] 图标：10-网络请求控制系统；11-终端设备；12-存储器；14-处理器；20-服务器；100-网络请求控制装置；110-网络请求发起模块；120-第一判断模块；130-第二判断模块；140-执行模块。

具体实施方式

[0048] 为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。通常在此处附图中描述和示出的本申请实施例的组件可以以各种不同的配置来布置和设计。

[0049] 因此，以下对在附图中提供的本申请的实施例的详细描述并非旨在限制要求保护的本申请的范围，而是仅仅表示本申请的选定实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

[0050] 应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。

[0051] 如图1所示，本发明实施例提供了一种网络请求控制系统10。该网络请求控制系统10可以包括终端设备11和服务器20。

[0052] 其中，所述终端设备11的具体种类不受限制，可以根据实际应用需求进行设置。例如，可以包括，但不限于电脑、平板电脑、手机等电子设备。

[0053] 详细地，所述终端设备11和所述服务器20之间通信连接，以实现数据的传输或交互。

[0054] 结合图2，所述终端设备11可以包括存储器12、处理器14和网络请求控制装置100。所述存储器12和处理器14之间直接或间接地电性连接，以实现数据的传输或交互。例如，相互之间可通过一条或多条通讯总线或信号线实现电性连接。所述网络请求控制装置100包括至少一个可以软件或固件(firmware)的形式存储于所述存储器12中的软件功能模块。所述处理器14用于执行所述存储器12中存储的可执行的计算机程序，例如，所述网络请求控制装置100所包括的软件功能模块及计算机程序等，以实现网络请求控制方法。

[0055] 其中,所述存储器12可以是,但不限于,随机存取存储器(Random Access Memory,RAM),只读存储器(Read Only Memory,ROM),可编程只读存储器(Programmable Read-Only Memory,PROM),可擦除只读存储器(Erasable Programmable Read-Only Memory,EPROM),电可擦除只读存储器(Electric Erasable Programmable Read-Only Memory,EEPROM)等。

[0056] 所述处理器14可能是一种集成电路芯片,具有信号的处理能力。上述的处理器14可以是通用处理器,包括中央处理器(Central Processing Unit,CPU)、网络处理器(Network Processor,NP)、片上系统(System on Chip,SoC)等。

[0057] 可以理解,图2所示的结构仅为示意,所述终端设备11还可包括比图2中所示更多或者更少的组件,或者具有与图2所示不同的配置。

[0058] 结合图3,本发明实施例还提供了一种可应用于上述终端设备11的网络请求控制方法。其中,所述网络请求控制方法有关的流程所定义的方法步骤可以由所述终端设备11实现。其中,所述终端设备11的客户端包括OkHttp网络组件,以发起网络请求流程。下面将对图3所示的具体流程进行详细阐述。

[0059] 步骤S100,获取第一URL,并根据该第一URL发起网络请求。

[0060] 详细地,在本发明实施例中,发起网络请求的具体方式为OkHttp网络组件生成一个call对象,并执行callStart(),以开始网络请求。

[0061] 步骤S120,判断是否接收到用户同意联网的指令。

[0062] 其中,所述用户同意联网的指令基于所述终端设备11响应用户的操作生成。结合图4,在本发明实施例中,所述终端设备11响应用户的操作的具体方式可以是:在发起网络请求后,所述终端设备11弹出一包括是否同意联网选项的窗口以让用户进行选择。

[0063] 其中,在判断出接收到用户同意联网的指令时,可以执行步骤S130;在判断出未接收到用户同意联网的指令时,可以取消所述第一URL对应的网络请求。

[0064] 步骤S130,判断所述第一URL是否属于预设黑名单。

[0065] 详细地,在接收到用户同意联网的指令后,通过判断所述第一URL是否属于预设黑名单,以对所述第一URL对应的网络请求进行控制。例如,在判断出所述第一URL不属于预设黑名单时,可以执行步骤S140。

[0066] 步骤S140,执行预设操作。

[0067] 其中,该预设操作可以包括根据所述网络请求进行联网处理。

[0068] 通过以上设置,可以在发起网络请求之后统一设置以判断URL是否属于预设的黑名单,以避免在发起网络请求之前针对每一个网络请求进行设置以判断是否属于预设的黑名单,从而提高网络请求的控制效率。

[0069] 其中,在现有技术中,需要在网络请求之前对多处请求代码提前判断是否属于预设的黑名单,要逐一修改每一个请求的业务代码,工作量烦杂,还容易出错。通过以上设置可以在统一的请求流程中判断是否属于预设的黑名单,一处实现,全局生效,快捷方便高效。并且,在发起网络请求之后判断URL是否属于预设的黑名单,对第三方SDK发起的网络请求也可以进行控制。

[0070] 详细地,在本发明实施例中,在所述第一URL对应的协议为HTTPS协议时,所述建立网络连接的具体方式指:根据所述第一URL进行DNS解析得到服务器20的IP地址,通过TCP协议与服务器20建立网络连接,通过SSL协议对所述终端设备11和服务器20交互的数据进行

加密。

[0071] 在实际应用中,网络请求被运营商或恶意中间商代理通过302重定向到了一些恶意的网络或广告页面,由于重定向后的网络请求不会再次执行callStart(),以开始网络请求,在本发明实施例中通过在建立网络连接后进行判断,以对重定向后的网络请求进行控制。结合图5,所述步骤S140可以包括步骤S141、步骤S142和步骤S143。

[0072] 步骤S141,根据所述网络请求建立网络连接。

[0073] 详细地,所述建立网络连接是指所述终端设备11与服务器20建立网络连接以进行数据交互。

[0074] 步骤S142,判断所述第一URL是否被重定向到第二URL。

[0075] 详细地,在本实施例中,所述判断方式可以具体为:获取当前的URL并与第一URL进行比较。

[0076] 其中,在判断出所述第一URL未被重定向到第二URL时,可以执行步骤S143。

[0077] 步骤S143,根据所述网络连接发送数据请求,并接收服务器20响应所述数据请求发送的响应数据。

[0078] 进一步地,在判断出所述第一URL被重定向到第二URL时,结合图6,可以执行步骤S144和步骤S145。

[0079] 步骤S144,判断所述第二URL是否属于所述预设黑名单。

[0080] 其中,通过方法isBlackUrl(String url),以判断所述第二URL是不是属于预设的黑名单,若是则返回true,若不是则返回false。

[0081] 其中,在判断出所述第二URL属于所述预设黑名单时,可以执行步骤S145。

[0082] 步骤S145,若所述第二URL属于所述预设黑名单,则取消第二URL对应的网络请求。

[0083] 详细地,取消第二URL对应的网络请求的具体方式可以通过任务取消方法cancel()执行,以取消当前Call请求的网络行为。并且,在取消网络请求之后,当前的网络请求可以发送异常信息至对应的开发人员的显示设备。

[0084] 通过以上设置,可以保护用户的数据安全,避免被运营商或非法的网络节点劫持跳转到不安全的网络地址。

[0085] 其中,在重定向的网络地址并非恶意的网络或广告页面时,所述执行预设操作的步骤,还包括:根据第二URL对应的网络请求进行联网处理。

[0086] 其中,在另一实施例中,上述的方法步骤可以是直接判断当前的URL是否属于预设的黑名单,若属于预设的黑名单,则取消该URL对应的网络请求。也就是说,不判断所述第一URL是否被重定向到第二URL,直接判断当前的URL是否属于预设的黑名单,以提高网络请求的控制效率。

[0087] 进一步地,在实际应用中,Android/Java系统的支持的HttpUrlConnection组件并不通过本方法中的OkHttp组件来访问网络,并不能通过OkHttp组件控制HttpUrlConnection组件的网络请求,因此,所述获取第一URL的步骤,包括:通过预设组件获取HttpUrlConnection组件对应的第一URL。

[0088] 其中,在本发明实施例中,所述预设组件具体指“com.squareup.okhttp3:okhttp-urlconnection”组件,以使HttpUrlConnection组件通过OkHttp组件来访问网络。

[0089] 进一步地,在本发明实施例中,所述网络请求控制方法还包括预先建立所述预设

黑名单的步骤，该步骤可以包括：根据接收到的黑名单请求信息获取对应的URL；根据获取的所述URL建立预设黑名单。

[0090] 详细地，在本发明实施例中，通过建立一个集合listBlackUrls，以存放接收到的黑名单请求信息；通过方法addBlackUrl(String url)，以添加黑名单请求信息对应的URL，从而可以自定义网络请求的黑名单。

[0091] 结合图7，本发明实施例还提供了一种网络请求控制装置100，可以应用于所述终端设备11。其中，该网络请求控制装置100可以包括网络请求发起模块110、第一判断模块120、第二判断模块130和执行模块140。

[0092] 所述网络请求发起模块110，用于获取第一URL，并根据该第一URL发起网络请求。在本实施例中，所述网络请求发起模块110可以用于执行图3所示的步骤S110，关于所述网络请求发起模块110的相关内容可以参照前文对步骤S110的描述。

[0093] 所述第一判断模块120，用于判断是否接收到用户同意联网的指令，其中，所述用户同意联网的指令基于所述终端设备11响应用户的操作生成。在本实施例中，所述第一判断模块120可以用于执行图3所示的步骤S120，关于所述第一判断模块120的相关内容可以参照前文对步骤S120的描述。

[0094] 所述第二判断模块130，用于在接收到用户同意联网的指令时，判断所述第一URL是否属于预设黑名单。在本实施例中，所述第二判断模块130可以用于执行图3所示的步骤S130，关于所述第二判断模块130的相关内容可以参照前文对步骤S130的描述。

[0095] 所述执行模块140，用于在所述第一URL不属于预设黑名单时，执行预设操作，其中，该预设操作包括根据所述网络请求进行联网处理。在本实施例中，所述执行模块140可以用于执行图3所示的步骤S140，关于所述执行模块140的相关内容可以参照前文对步骤S140的描述。

[0096] 进一步地，所述终端设备11与服务器20通信连接，所述执行模块140可以包括网络连接建立子模块、第一判断子模块和数据请求子模块。

[0097] 所述网络连接建立子模块，用于根据所述网络请求建立网络连接。在本实施例中，所述网络连接建立子模块可以用于执行图5所示的步骤S141，关于所述网络连接建立子模块的相关内容可以参照前文对步骤S141的描述。

[0098] 所述第一判断子模块，用于判断所述第一URL是否被重定向到第二URL。在本实施例中，所述第一判断子模块可以用于执行图5所示的步骤S142，关于所述第一判断子模块的相关内容可以参照前文对步骤S142的描述。

[0099] 所述数据请求子模块，用于在所述第一URL未被重定向到第二URL时，根据所述网络连接发送数据请求，并接收服务器20响应所述数据请求发送的响应数据。在本实施例中，所述数据请求子模块可以用于执行图5所示的步骤S143，关于所述数据请求子模块的相关内容可以参照前文对步骤S143的描述。

[0100] 进一步地，所述执行模块140还可以包括第二判断子模块和网络请求取消子模块。

[0101] 所述第二判断子模块，用于在所述第一URL被重定向到第二URL时，判断所述第二URL是否属于所述预设黑名单。在本实施例中，所述第二判断子模块可以用于执行图6所示的步骤S144，关于所述第二判断子模块的相关内容可以参照前文对步骤S144的描述。

[0102] 所述网络请求取消子模块，用于在所述第二URL属于所述预设黑名单时，则取消第

二URL对应的网络请求。在本实施例中，所述网络请求取消子模块可以用于执行图6所示的步骤S145，关于所述网络请求取消子模块的相关内容可以参照前文对步骤S145的描述。

[0103] 综上所述，本发明实施例提供的网络请求控制方法、装置及终端设备11，通过在发起网络请求后判断是否接收到用户同意联网的指令，并在接收到用户同意联网的指令后，判断第一URL是否属于预设黑名单，在所述第一URL不属于预设黑名单时，根据所述网络请求进行联网处理，以避免在发起网络请求之前针对每一个网络请求进行设置以判断是否属于预设的黑名单，以提高网络请求的控制效率。

[0104] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

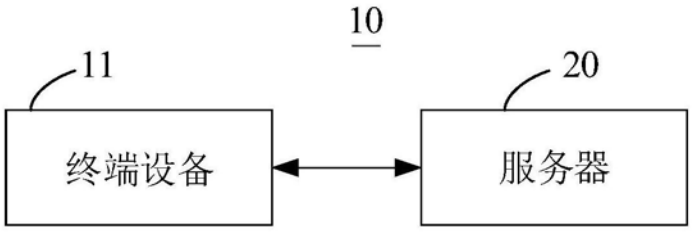

10
11
20
终端设备
服务器

图1

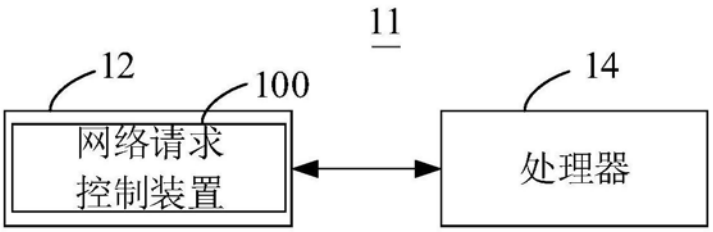

11
12
100
14
网络请求
控制装置
处理器

图2

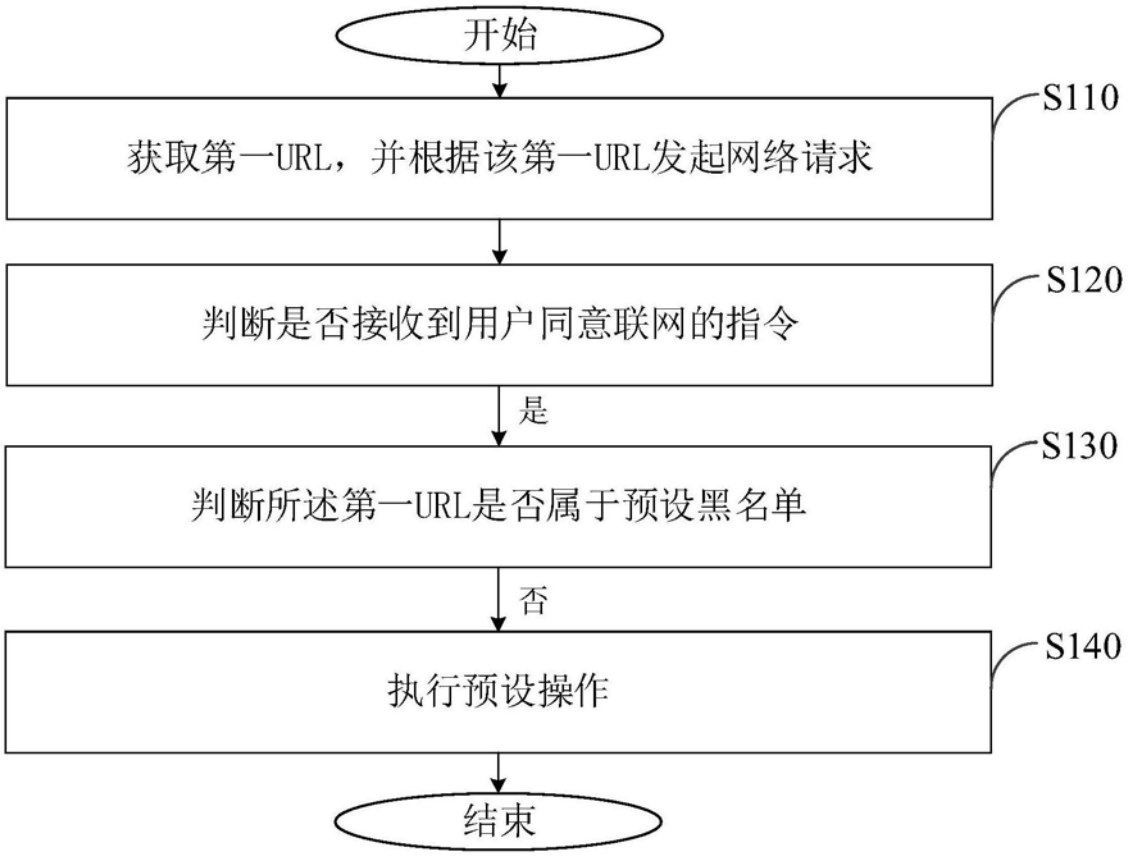

开始
获取第一URL，并根据该第一URL发起网络请求
S110
判断是否接收到用户同意联网的指令
S120
是
判断所述第一URL是否属于预设黑名单
S130
否
执行预设操作
S140
结束

图3

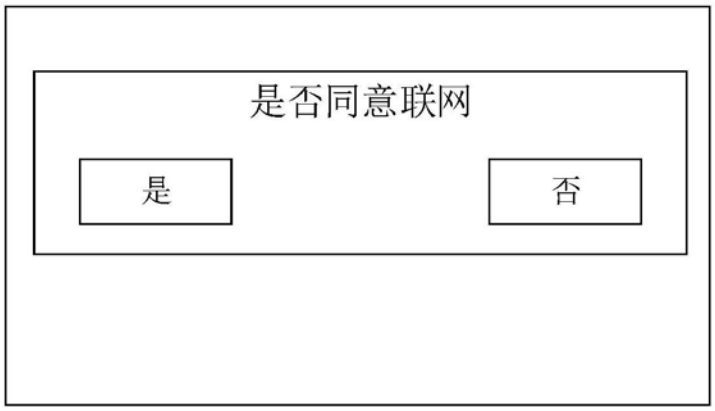

是否同意联网
是
否

图4

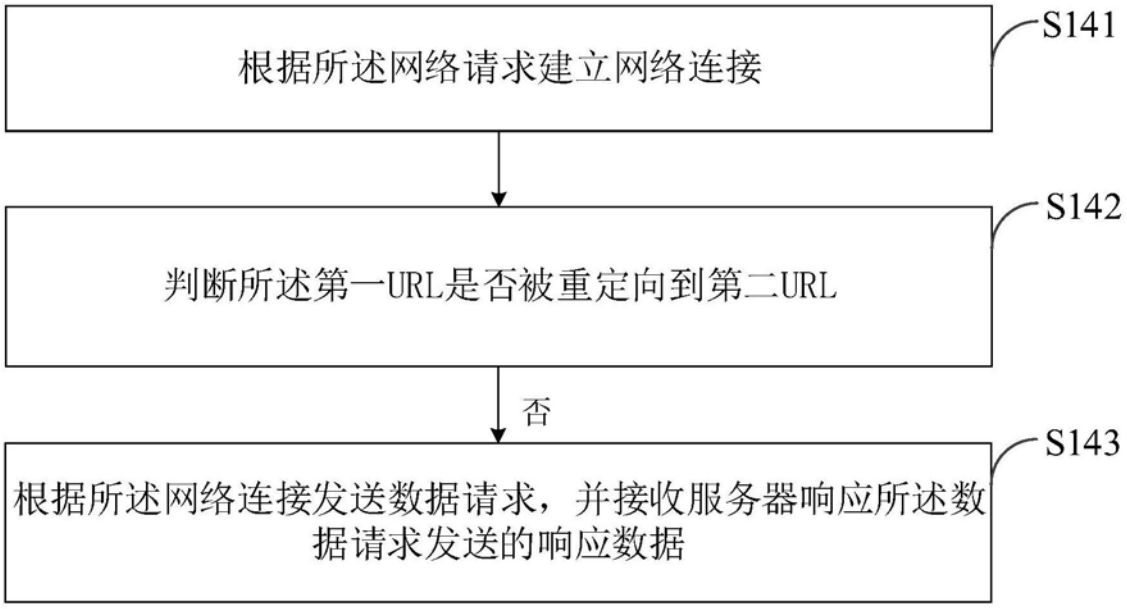

根据所述网络请求建立网络连接
S141
判断所述第一URL是否被重定向到第二URL
S142
否
根据所述网络连接发送数据请求，并接收服务器响应所述数据请求发送的响应数据
S143

图5


在所述第一URL被重定向到第二URL时，判断所述第二URL是否属于所述预设黑名单
S144
是
取消第二URL对应的网络请求
S145

图6

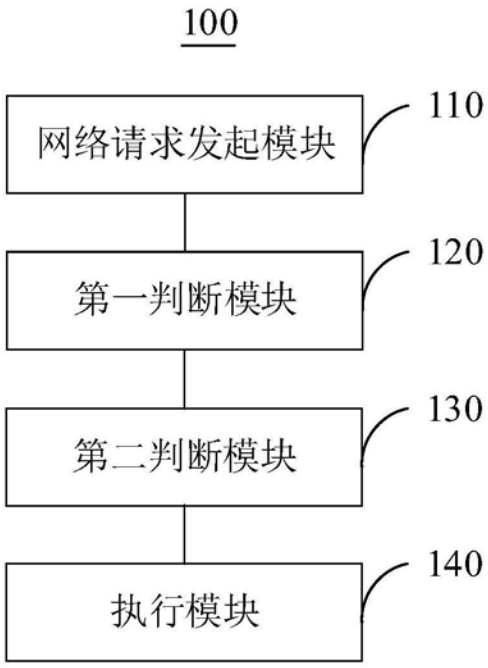


图7