

(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
2021 年 2 月 25 日 (25.02.2021)



(10) 国际公布号
WO 2021/031761 A1

(51) 国际专利分类号:
H04W 24/02 (2009.01)

(21) 国际申请号: PCT/CN2020/102816

(22) 国际申请日: 2020 年 7 月 17 日 (17.07.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910776929.6 2019年8月22日 (22.08.2019) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 田文凯 (TIAN, Wenkai); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 广州嘉权专利商标事务所有限公司 (JIAQUAN IP LAW); 中国广东省广州市天河区黄埔大道西 100 号富力盈泰广场 A 栋 910, Guangdong 510627 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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,

(54) Title: METHOD FOR PROCESSING ABNORMAL TERMINAL, NETWORK MANAGEMENT DEVICE AND COMPUTER-READABLE MEDIUM

(54) 发明名称: 异常终端的处理方法、网管设备及计算机可读介质

根据各个基站上传的在执行MDT任务时, 所获取的异常终端类型标识和异常行为的类型的对应关系, 生成第一防护表 S1

将接收的各个基站上传的第一防护表上传至云服务器, 以使云服务器对各个网管设备上传的第一防护表进行汇总, 生成第二防护表 S2

接收云服务器下发的第二防护表, 并将第二防护表中的至少部分异常终端类型标识和异常行为类型的对应关系下发至基站, 以使基站控制具有异常终端类型标识的终端终止执行MDT任务 S3

S1 Generate a first protection table according to the correspondence between abnormal terminal type identifiers and abnormal behavior types which are acquired when executing an MDT task and which are uploaded by various base stations
S2 Upload to a cloud server received first protection tables uploaded by various base stations so that the cloud server collects first protection tables uploaded by various network management devices so as to generate a second protection table
S3 Receive the second protection table issued by the cloud server, and issue to the base station the correspondence between at least part of the abnormal terminal type identifiers and the abnormal behavior types in the second protection table so that the base station controls a terminal having an abnormal terminal type identifier to terminate the execution of the MDT task

图 1

(57) Abstract: A method for processing an abnormal terminal, a network management device, an electronic device and a computer-readable medium, which relate to the technical field of communications. The method for processing an abnormal terminal in an embodiment of the present disclosure comprises: generating a first protection table according to the correspondence between abnormal terminal type identifiers and abnormal behavior types which are acquired when executing a minimization drive test task and which are uploaded by various base stations (S1); uploading the first protection table to a cloud server so that the cloud server collects first protection tables uploaded by various network management devices so as to generate a second protection table (S2); and receiving the second protection table issued by the cloud server, and issuing to a base station the correspondence between at least part of the abnormal terminal type identifiers and abnormal behavior types in the second protection table so that the base station controls a terminal having

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US,
UZ, VC, VN, WS, ZA, ZM, ZW。

- (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)。

根据细则4.17的声明:

- 发明人资格(细则4.17(iv))

本国际公布:

- 包括国际检索报告(条约第21条(3))。

an abnormal terminal type identifier to terminate the execution of the minimization drive test task (S3).

(57) 摘要: 一种异常终端的处理方法、网管设备、电子设备及计算机可读介质, 属于通信技术领域。本公开实施例的异常终端的处理的方法, 包括: 根据各个基站上传的在执行最小化路测任务时, 所获取到的异常终端类型标识和异常行为的类型的对应关系, 生成第一防护表(S1); 将所述第一防护表上传至云服务器, 以使所述云服务器对各个网管设备上传的第一防护表进行汇总, 生成第二防护表(S2); 接收云服务器下发的所述第二防护表, 并将所述第二防护表中的至少部分异常终端类型标识和异常行为类型的对应关系, 下发至所述基站, 以使所述基站控制具有异常终端类型标识的终端终止执行最小化路测任务(S3)。

异常终端的处理方法、网管设备及计算机可读介质

相关申请的交叉引用

本申请基于申请号为 201910776929.6、申请日为 2019 年 8 月 22 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本公开属于通信技术领域，具体涉及一种异常终端的处理方法、网管设备、电子设备及计算机可读介质。

背景技术

在无线通讯领域，随着移动通信的普及和移动终端的广泛应用，移动市场下充斥着各种各样类型的终端；在众多终端类型中，存在部分异常终端，由于硬件缺陷或者没严格按照协议实现业务行为，导致在做特定业务时，出现掉线、接入失败、切换失败或测量数据频繁上报基站等异常现象，严重影响网络的掉线率、重建率、接入成功率、切换成功率等关键指标，给整个网络的维测造成了极大困难。

最小化路测 (Minimization Drive Test; MDT) 就是让现网的商用终端代替人工做路测，进行相关量的测量并上报。网络根据终端上报的测量对现网覆盖、切换、接入、干扰等情况进行分析，发现问题并解决网络中存在覆盖问题、切换问题、接入问题以及干扰等问题。

发明内容

本公开旨在至少解决一些情形中存在的技术问题之一，提供一种异常终端的处理的方法。

第一方面，本公开实施例提供一种异常终端的处理的方法，包括：根据各个基站上传的在执行最小化路测任务时，所获取的异常终端类型标识和异常行为的类型的对应关系，生成第一防护表；将所述第一防护表上传至云服务器，以使所述云服务器对各个网管设备上传的第一防护表进行汇总，生成第二防护表；接收云服务器下发的所述第二防护表，并将所述第二防护表中的至少部分异常终端类型标识和异常行为类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行最小化路测任务。

第二方面，本公开实施例提供一种网管设备，包括：生成模块，用于根据各个基站上传的在执行最小化路测任务时，所获取的异常终端类型标识和异常行为的类型的对应关系，生成第一防护表；上传模块，用于将所述第一防护表上传至云服务器，以使所述云服务器对各个网管设备上传的第一防护表进行汇总，生成第二防护表；控制模块，用于接收云服务器下发的所述第二防护表，并将所述第二防护表中的至少部分异常终端类型标识和异常行为类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端

终止执行最小化路测任务。

第三方面，本公开实施例提供一种电子设备，其包括：一个或多个处理器；存储装置，其上存储有一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现上述所谓任意一项所述的方法。

第四方面，本公开实施例提供一种计算机可读介质，其上存储有计算机程序，所述程序被处理器执行时实现上述的任意一项所述的方法。

附图说明

图 1 为本公开实施例的异常终端的处理方法的流程图；

图 2 为本公开实施例的步骤 S0 的流程图；

图 3 为本公开实施例中的步骤 S3 中的步骤 S31-S35 流程图；

图 4 为本公开实施例中的步骤 S3 中的步骤 S36-S37 流程图；

图 5 为本公开实施例的网管设备的一种结构框图；

图 6 为本公开实施例的网管设备的另一种结构框图；

图 7 为本公开实施例的网管设备的控制模块的一种结构框图；

图 8 为本公开实施例的网管设备的控制模块的另一种结构框图；

图 9 为本公开实施例的电子设备的结构图。

具体实施方式

为使本领域的技术人员更好地理解本公开的技术方案，下面结合附图对本公开提供的异常终端的处理方法、网管设备、电子设备及计算机可读介质进行详细描述。

在下文中将参考附图更充分地描述示例实施例，但是所述示例实施例可以以不同形式来体现且不应当被解释为限于本文阐述的实施例。反之，提供这些实施例的目的在于使本公开透彻和完整，并将使本领域技术人员充分理解本公开的范围。

如本文所使用的，术语“和/或”包括一个或多个相关列举条目的任何和所有组合。

本文所使用的术语仅用于描述特定实施例，且不意欲限制本公开。如本文所使用的，单数形式“一个”和“该”也意欲包括复数形式，除非上下文另外清楚指出。还将理解的是，当本说明书中使用术语“包括”和/或“由……制成”时，指定存在所述特征、整体、步骤、操作、元件和/或组件，但不排除存在或添加一个或多个其它特征、整体、步骤、操作、元件、组件和/或其群组。

本文所述实施例可借助本公开的理想示意图而参考平面图和/或截面图进行描述。因此，可根据制造技术和/或容限来修改示例图示。因此，实施例不限于附图中所示的实施例，而是包括基于制造工艺而形成的配置的修改。因此，附图中例示的区具有示意性属性，并且图中所示区的形状例示了元件的区的具体形状，但并不旨在是限制性的。

除非另外限定，否则本文所用的所有术语(包括技术和科学术语)的含义与本领域普通技术人员通常理解的含义相同。还将理解，诸如那些在常用字典中限定的那些术语应当被

解释为具有与其在相关技术以及本公开的背景下的含义一致的含义，且将不解释为具有理想化或过度形式上的含义，除非本文明确如此限定。

在一些情形中，基站给终端下发时延信息测量，全球卫星定位系统（Global Navigation Satellite System；GNSS）信息测量，无线局域网（Wireless Local Area Network；WLAN）信息测量，蓝牙信息测量，空闲态 MDT（Logged MDT）测量等，由于问题终端的测量能力缺陷，出现掉线，重建，切换失败现象；基站给终端下发空闲态 MDT（Logged MDT），无线链路失败 MDT（Radio Link Failure；RLF MDT），无线资源控制连接建立失败 MDT（Radio Resource Control Connection Establishment Failure；RCEF MDT）任务时，终端没有按照协议规定，在上报测量数据后清除数据缓存，导致无限制上报测量数据现象，对后端数据解析形成巨大压力。

本公开实施例所提供的异常终端的处理方法是以网管设备作为执行主体。通过网管设备、基站、云服务器之间进行信息的交互，以实现树状的共享机制。其中，云服务器与多个网管设备能够进行信息的交互，每个网管设备与其所管辖范围内的多个基站之间信息的交互。

在此需要说明的是，在下述实施例中所谓的学习策略是指：获取异常终端类型标识和异常行为的类型的对应关系的具体方法。

图 1 为本公开实施例的异常终端的处理方法的流程图。

第一方面，参照图 1，本公开实施例提供一种异常终端的处理方法，包括如下步骤：

S1、根据各个基站上传的执行 MDT 任务时，所获取的异常终端类型标识和异常行为的类型的对应关系，生成第一防护表。

在此需要说明的是，在本公开实施例中第一防护表只是用于存储异常终端类型标识和异常行为的类型的对应关系的一种形式，并非严格意义上的表格。

其中，终端类型标识可以为特性群指示 FGI、国际移动设备识别码 IMEI、国际移动设备识别码-型号认证码 IMEI-TAC、国际移动设备识别码-软件版本 IMEI-SV 中的任意一种；在本实施例中以特性群指示 FGI 为例进行说明。

具体的，当网管设备检测到用以对网络维护的性能指标发生异常时，例如基站的掉话率、数据解析服务器的使用率等参数大于预设的参考值。网管设备将根据异常行为的类型，控制基站对终端采取相应的学习策略和防护策略。以下举例进行说明：

第一种：异常行为的类型为掉话率增加；具体的，当网络维护人员发现部分终端在接收到 Logged MD 后，会进入空闲态进行数据测量，下次接入后如果携带 Logged MDT 数据，会出现重配超时现象；网管设备下发给基站对终端所采取的学习策略和防护策略，具体如下：

S011、控制基站给接入的终端下发 Logged MDT 测量任务。

S012、基站对携带 Logged MDT 数据，并出现重配超时的终端按照终端类型标识 FGI

进行记录，形成记录表。

S013、统计记录表中各个终端按照终端类型标识 FGI 出现的次数，获取出现次数大于预设值的终端类型标识 FGI，并将这些 FGI 记作异常终端类型标识 FGI，并将异常终端类型标识 FGI 与异常行为的类型的对应关系进行存储，生成第一防护表。其中，异常终端类型标识 FGI 与异常行为的类型的对应关系可以用{FGI，异常行为的类型}表示。S014、基站根据第一防护表对具有异常终端类型标识 FGI 的终端采取防护策略。具体防护策略为，在后期出现掉话率增加的异常行为时，基站出不再向具有异常终端类型标识 FGI 的终端下发 Logged MDT 测量任务。

第二种：数据解析服务器的使用率大于预设值；具体的当网络维护人员发现部分终端无限制上报 Logged MDT 数据，且上报频繁，给数据解析服务器造成巨大压力时，网管设备下发给基站对终端所采取的学习策略和防护策略，具体如下：

S021、控制基站给接入的终端下发 Logged MDT 测量任务。

S022、根据 Logged MDT 任务的测量时长和测量间隔，算出最大测量次数。

S023、判断终端每次上报 Logged MDT 数据的次数，是否大于步骤 S022 中计算得到的最大测量次数。由于终端每次上报 Logged MDT 数据中至少包含一次测量；理论上终端的最大上报次数不超过最大测量次数；若终端每次上报 Logged MDT 数据的次数大最大测量次数，则将这些 FGI 记作异常终端类型标识 FGI，并将异常终端类型标识 FGI 与异常行为的类型的对应关系进行存储，生成第一防护表。其中，异常终端类型标识 FGI 与异常行为的类型的对应关系可以用{FGI，异常行为的类型}表示。S024、基站根据第一防护表对具有异常终端类型标识 FGI 的终端采取防护策略。具体防护策略为，在后期出现掉话率增加的异常行为时，基站出不再向具有异常终端类型标识 FGI 的终端下发 Logged MDT 测量任务；同时基站也不再请求具有异常终端类型标识 FGI 的终端上报 Logged MDT 数据。在步骤 S1 中，网管设备可以接收各个基站按照上述步骤所获取的第一防护表。

在需要说明的是，无论是上述的基站根据第一种还是第二种异常行为所采用的学习策略均为周期性的，上述描述只是描述了第一个学习周期的具体方法。而对于之后的学习，基站则对已经识别出的异常终端类型的标识不再进行学习，只学习未识别的异常终端类型的标识，实现增量学习；因为异常终端类型的标识是有限的，随着不断地对未识别异常终端类型的标识学习，学习结果也趋于收敛，增量的学习方式保证了学习过程的收敛性；其中基站识别异常终端类型的标识的方式可以依靠自身基站学习识别，也可以依靠获取其他基站分享的学习信息识别。

S2、将接收的各个基站上传的第一防护表上传至云服务器，以使云服务器对各个网管设备上传的第一防护表进行汇总，生成第二防护表。

在此需要说明的是，在本公开实施例中第二防护表只是用于存储异常终端类型标识和异常行为的类型的对应关系的一种形式，并非严格意义上的表格。

在步骤 S2 中，网管设备将其所接收到的各个基站上传的第一防护表进行汇总，将各个第一防护表中不同的异常终端类型标识与异常行为的类型的对应关系汇总成第二防护表；云服务器将第二防护表再下发至各个网管设备，这样一来，实现连接不同网管设备的各个基站的学习结果共享，以使总体的学习更加有效。

S3、接收云服务器下发的第二防护表，并将第二防护表中的至少部分异常终端类型标识和异常行为类型的对应关系下发至基站，以使基站控制具有异常终端类型标识的终端终止执行 MDT 任务。

在步骤 S3 中，网管设备接收来自云服务器下发的第二防护表；之后，再根据基站所能够接收的异常终端类型标识和异常行为类型的对应关系的数量，将所接收到的第二防护表中相应数量的异常终端类型标识和异常行为类型的对应关系下发至相应的基站，以使所述基站控制具有异常终端类型标识的终端终止执行 MDT 任务。

同时，由于第二防护表是由各个网管设备将其所接收到的各个基站上传的第一防护表中进行汇总，再将各个第一防护表中不同的异常终端类型标识与异常行为的类型的对应关系汇总成第二防护表，这样一来，实现连接不同网管设备的各个基站的学习结果共享，以使总体的学习更加有效，从而使得每个基站的防护范围更加广泛，同时使得基站性能的消耗更低。

图 2 为本公开实施例的步骤 S0 的流程图。

在一些实施例中，参照图 2，在本公开上述实施例的步骤 S1 之前还包括步骤 S0；步骤 S0 具体可以包括如下步骤：

S01、根据异常行为类型，判断基站是否开启了引起异常行为所对应的相关功能。

在步骤 S01 中，网管设备需要根据其所接收到网络维护人员所检测的性能指标所对应的异常行为类型，判断基站是否开启了引起异常行为所对应的相关功能。因为只有基站开启了相应功能，才允许网络设备控制该基站进行异常行为的学习策略，从而可以保证学习策略开启范围的准确性。其中，学习策略也即例如上述实施例中第一种和第二种异常行为类型所对应的学习策略。若在步骤 S01 中判断出基站开启了引起异常行为对应的相关功能，则执行步骤 S02；若判断出基站没有开启引起异常行为对应的相关功能，则终止该方法。

S02、检测基站对应异常行为的性能指标。

在步骤 S02 中，网管设备根据基站根据异常行为的类型，获取相应的性能指标。具体的，网管设备所检测的性能指标可以是基站的掉话率、数据解析服务器的使用率等参数。

S03、判断所检测的性能指标是否大于第一阈值。

在步骤 S3 中，网管设备判断在步骤 S02 中所检测到的、用以对网络维护的性能指标是否大于第一阈值，例如基站的掉话率、数据解析服务器的使用率等参数大于预设的参考值。若判断出该性能指标大于第一阈值。则执行步骤 S04；若判断出该性能指标小于等于第一阈值，则返回步骤 S02。

S04、控制基站根据所引起的异常行为的类型，获取异常终端类型标识和异常行为的类型的对应关系。

在步骤 S04 中，当网管设备检测到用以对网络维护的性能指标发生异常时，例如基站的掉话率、数据解析服务器的使用率等参数大于预设的参考值。网管设备将根据异常行为的类型，控制基站对终端采取相应的学习策略和防护策略。具体的学习策略和防护策略可以与上述实施例中步骤 S011~S014，以及步骤 S021~S024 相同，因此不再详细描述。

在此需要说明的是，网管设备控制基站的学习（也就是获取异常终端类型标识和异常行为的类型的对应关系的过程）是周期性的，因此，基站对已识别的异常终端类型标识不再进行学习，只学习未识别的异常终端类型标识，实现增量学习；因为异常终端类型标识是有限的，随着不断地对未识别异常终端类型标识学习，学习结果也趋于收敛，增量的学习方式保证了学习过程的收敛性；其中，基站识别异常终端类型标识的方式可以依靠自身学习识别，也可以依靠获取其他基站分享的学习信息识别。

图 3 为本公开实施例中的步骤 S3 中的步骤 S31-S35 流程图。

在一些实施例，参照图 3，上述实施例中的步骤 S3，具体可以包括如下步骤：

S31、接收云服务器下发的第二防护表。

在步骤 S31 中，网管设备接收云服务器下发的第二防护表。其中，第二防护表包括多个异常终端类型标识和异常行为类型的对应关系。

S32、获取第二防护表中不同的异常终端类型标识的个数，记作 M ；以及获取基站能够接收的不同的异常终端类型标识的个数，记作 N 。

在步骤 S32 中，网管设备获取第二防护表中不同的异常终端类型标识的个数，记作 M ；以及获取基站能够接收的不同的异常终端类型标识的个数，记作 N 。在此需要说明的是，第二防护表中不同的异常终端类型标识的个数并不等于，第二防护表中异常终端类型标识和异常行为的类型的对应关系的数量；因为在第二防护表中，有可能存在两个异常终端类型标识和异常行为的类型的对应关系中，异常终端类型标识是相同的情况，也即存在{FGI-1, 异常行为的类型 1}和{FGI-1, 异常行为的类型 2}。

S33，判断 M 是否大于 N 。

在步骤 S33 中，网管设备若判断出 $M > N$ ，则执行步骤 S34；网管设备若判断出 $M \leq N$ ，则执行步骤 S35。

S34、将第二防护表中 N 个不同的异常终端类型标识和异常行为的类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行 MDT 任务。

在步骤 S34 中，网管设备可以将第二防护表的 M 个不同的异常终端类型标识和异常行为的类型的对应关系进行排序，将其中的前 N 个下发至所述基站，也可以在 M 个不同的异常终端类型标识和异常行为的类型的对应关系中随机抽取 N 个下发至所述基站。

S35、将第二防护表下发至所述基站，以使所述基站控制具有异常终端类型标识的终

端终止执行 MDT 任务。

在步骤 S34 中，网管设备可以将第二防护表中所有的异常终端类型标识和异常行为的类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行 MDT 任务。

图 4 为本公开实施例中的步骤 S3 中的步骤 S36-S37 流程图。

在一些实施例中，参照图 4，在上述实施例中的步骤 S34 之后还可以包括以下步骤：

S36、接收基站发送的替换请求；所述替换请求包括：基站在周期性的检测对异常终端类型标识所对应的终端的防护次数，且在出现防护次数为 0 的终端时发送的请求。

具体的，当基站周期性的检测对异常终端类型标识所对应的终端的防护次数，若发现某一异常终端类型标识所对应的终端的防护次数为 0，此时则向网管设备发送替换请求。

S37、根据所述替换请求，通过所述第二防护表中未被下发至基站的异常终端类型标识和异常行为的类型的对应关系，将防护次数为 0 的终端所对应的异常终端类型标识和异常行为的类型的对应关系进行替换。

具体的，网管设备在接收到基站所下发的替换请求后，则通过第二防护表中未被下发至基站的异常终端类型标识和异常行为的类型的对应关系，将防护次数为 0 的终端所对应的异常终端类型标识和异常行为的类型的对应关系进行替换。

本公开实施例所提供的异常终端的处理方法，通过网管设备将与之连接的基站所上传的异常终端类型标识和异常行为的类型的对应关系进行汇总，得到第一防护表，并上传至云服务器，之后云服务器再对与之连接各个网管设备所上传的第一防护表进行汇总生成第二防护表，此时，第二防护表中的异常终端类型标识和异常行为的类型的对应关系，为多个网管设备所连接的基站上传的异常终端类型标识和异常行为的类型的对应关系汇总，最后，网管设备接收云服务器下发的所述第二防护表，并将第二防护表中的至少部分异常终端类型标识和异常行为类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行 MDT 任务。这样一来，实现连接不同网管设备的各个基站的学习结果共享，以使总体的学习更加有效，从而使得每个基站的防护范围更加广泛，同时使得基站性能消耗更低。

图 5 为本公开实施例的网管设备的一种结构框图。

第二方面，参照图 5，本公开实施例提供一种网管设备，其可用于执行上述任一实施例中的异常终端的处理方法。该网管设备具体包括：生成模块 1、上传模块 2 和控制模块 3。

具体的，生成模块 1 用于根据各个基站上传的在执行 MDT 任务时，所获取的异常终端类型标识和异常行为的类型的对应关系，生成第一防护表。

上传模块 3 用于将第一防护表上传至云服务器，以使云服务器对各个网管设备上传的第一防护表进行汇总，生成第二防护表。

控制模块 3 用于接收云服务器下发的第二防护表，并将第二防护表中的至少部分异常终端类型标识和异常行为类型的对应关系，下发至基站，以使基站控制具有异常终端类型标识的终端终止执行 MDT 任务。

在需要说明的是，本公开实施例中的生成模块 1 可用于执行上述实施例中的步骤 S1；上传模块 2 可用于执行上述实施例中的步骤 S2；控制模块 3 可用于执行上述实施例中的步骤 S3。

图 6 为本公开实施例的网管设备的另一种结构框图。

在一些实施例中，参照图 6，该网管设备不仅包括上述结构，还可以包括：第一判断模块 4、检测模块 5、第二判断模块 6、第一获取模块 7。

具体的，第一判断模块 4 用于根据异常行为类型，判断基站是否开启引起异常行为所对应的相关功能。

检测模块 5 用于当所述第一判断模块 4 判断出基站开启了引起异常行为对应的相关功能时，检测所述基站对应该异常行为的性能指标。

第二判断模块 6 用于判断所检测的性能指标是否大于第一阈值。

获取模块 7 用于当第二判断模块 6 判断出所检测的性能指标大于第一阈值时，控制基站根据所引起的异常行为的类型，获取异常终端类型标识和异常行为的类型的对应关系。

在此需要说明的，本公开实施例中的第一判断模块 4 可用于执行上述实施例中的步骤 S01；检测模块 5 可用于执行上述实施例中的步骤 S02；第二判断模块 6 可用于执行上述实施例中的步骤 S03；获取模块 7 可用于执行上述实施例中的步骤 S04。

图 7 为本公开实施例的网管设备的控制模块的一种结构框图。

在一些实施例中，参照图 7，上述的控制模块可以包括：第一接收单元 31、获取单元 32、判断单元 33、控制单元 34。

具体的，第一接收单元 31 用于接收云服务器下发的第二防护表。

获取单元 32 用于获取所述第二防护表中不同的异常终端类型标识的个数，记作 M ；以及获取基站能够接收的不同的异常终端类型标识的个数，记作 N 。

判断单元 33 用于判断 M 是否大于 N 。

控制单元 34 用于在判断单元 33 判断出 $M > N$ 时，将所述第二防护表中 N 个不同的异常终端类型标识和异常行为的类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行 MDT 任务；以及，在判断单元 33 判断出若判断出 $M \leq N$ 时，将第二防护表下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行 MDT 任务。

在此需要说明的，本公开实施例中的第一接收单元 31 可用于执行上述实施例中的步骤 S31；获取单元 32 可用于执行上述实施例中的步骤 S32；判断单元 33 可用于执行上述实施例中的步骤 S33；控制单元 34 可用于执行上述实施例中的步骤 S34 和 S35。

图 8 为本公开实施例的网管设备的控制模块的另一种结构框图。

在一些实施例中，参照图 8，上述的控制模块不仅包括上述结构，还可以包括：第二接收单元 35 和替换单元 36。

具体的，第二接收单元 35 用于接收基站发送的替换请求；该替换请求包括：基站在周期性的检测对异常终端类型标识所对应的终端的防护次数，且在出现防护次数为 0 的终端时发送的请求。

替换单元 36 用于根据替换请求，通过第二防护表中未被下发至基站的异常终端类型标识和异常行为的类型的对应关系，将防护次数为 0 的终端所对应的异常终端类型标识和异常行为的类型的对应关系进行替换。

在此需要说明的，本公开实施例中的第二接收单元 35 可用于执行上述实施例中的步骤 S36；替换单元 36 可用于执行上述实施例中的步骤 S37。

本公开实施例所提供的网管设备可以采用上述的实施例中异常终端的处理方法，即通过网管设备将与之连接的基站所上传的异常终端类型标识和异常行为的类型的对应关系进行汇总，得到第一防护表，并上传至云服务器，之后云服务器再对与之连接各个网管设备所上传的第一防护表进行汇总生成第二防护表，此时，第二防护表中的异常终端类型标识和异常行为的类型的对应关系，为多个网管设备所连接的基站上传的异常终端类型标识和异常行为的类型的对应关系汇总，最后，网管设备接收云服务器下发的所述第二防护表，并将第二防护表中的至少部分异常终端类型标识和异常行为类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行 MDT 任务。这样一来，实现连接不同网管设备的各个基站的学习结果共享，以使总体的学习更加有效，从而使得每个基站的防护范围更加广泛，同时使得基站性能消耗更低。

第三方面，参考图 9，本公开实施例提供一种电子设备，其包括：

一个或多个处理器 91；

存储装置 92，其上存储有一个或多个程序，当一个或多个程序被一个或多个处理器 91 执行，使得一个或多个处理器 91 实现上述任意一种异常终端的处理方法。

第四方面，本公开实施例提供一种计算机可读介质，其上存储有计算机程序，程序被处理器执行时实现上述任意一种异常终端的处理方法。

本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统、装置中的功能模块/单元可以被实施为软件、固件、硬件及其适当的组合。在硬件实施方式中，在以上描述中提及的功能模块/单元之间的划分不一定对应于物理组件的划分；例如，一个物理组件可以具有多个功能，或者一个功能或步骤可以由若干物理组件合作执行。某些物理组件或所有物理组件可以被实施为由处理器，如中央处理器、数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质（或非暂时性

介质)和通信介质(或暂时性介质)。如本领域普通技术人员公知的,术语计算机存储介质包括在用于存储信息(诸如计算机可读指令、数据结构、程序模块或其它数据)的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其它存储器技术、CD-ROM、数字多功能盘(DVD)或其它光盘存储、磁盒、磁带、磁盘存储或其它磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其它的介质。此外,本领域普通技术人员公知的是,通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其它传输机制之类的调制数据信号中的其它数据,并且可包括任何信息递送介质。

本文已经公开了示例实施例,并且虽然采用了具体术语,但它们仅用于并仅应当被解释为一般说明性含义,并且不用于限制的目的。在一些实例中,对本领域技术人员显而易见的是,除非另外明确指出,否则可单独使用与特定实施例相结合描述的特征、特性和/或元素,或可与其它实施例相结合描述的特征、特性和/或元件组合使用。因此,本领域技术人员将理解,在不脱离由所附的权利要求阐明的本公开的范围的情况下,可进行各种形式和细节上的改变。

可以理解的是,以上实施方式仅仅是为了说明本公开的原理而采用的示例性实施方式,然而本公开并不局限于此。对于本领域内的普通技术人员而言,在不脱离本公开的精神和实质的情况下,可以做出各种变型和改进,这些变型和改进也视为本公开的保护范围。

权利要求书

1. 一种异常终端的处理的方法，包括：

根据各个基站上传的在执行最小化路测任务时，所获取的异常终端类型标识和异常行为的类型的对应关系，生成第一防护表；

将所述第一防护表上传至云服务器，以使所述云服务器对各个网管设备上传的第一防护表进行汇总，生成第二防护表；

接收云服务器下发的所述第二防护表，并将所述第二防护表中的至少部分异常终端类型标识和异常行为类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行最小化路测任务。

2. 根据权利要求1所述的异常终端的处理方法，其中，在所述根据各个基站上传的在执行最小化路测任务时，所获取的异常终端类型标识和异常行为类型的对应关系，生成第一防护表之前，还包括：

根据异常行为类型，判断基站是否开启引起异常行为所对应的相关功能；

若判断出基站开启了引起异常行为对应的相关功能，检测所述基站对应该异常行为的性能指标；

判断所检测的性能指标是否大于第一阈值；

若判断出大于第一阈值，则控制基站根据所引起的异常行为的类型，获取异常终端类型标识和异常行为的类型的对应关系。

3. 根据权利要求1所述的异常终端的处理方法，其中，所述接收云服务器下发的所述第二防护表，并将所述第二防护表中的至少部分异常终端类型标识和异常行为类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行最小化路测任务，包括：

接收云服务器下发的第二防护表；

获取所述第二防护表中不同的异常终端类型标识的个数，记作 M ；以及获取基站能够接收的不同的异常终端类型标识的个数，记作 N ；

判断 M 是否大于 N ；

若判断出 $M > N$ ，则将所述第二防护表中 N 个不同的异常终端类型标识和异常行为的类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行最小化路测任务；

若判断出若判断出 $M \leq N$ ，则将第二防护表下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行最小化路测任务。

4. 根据权利要求3所述的异常终端的处理方法，其中，所述若判断出 $M > N$ ，则将所述第二防护表中 N 个不同的异常终端类型标识和异常行为的类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行最小化路测任务之后，还

包括：

接收基站发送的替换请求；所述替换请求包括：基站在周期性的检测对异常终端类型标识所对应的终端的防护次数，且在出现防护次数为 0 的终端时发送的请求；

根据所述替换请求，通过所述第二防护表中未被下发至基站的异常终端类型标识和异常行为的类型的对应关系，将防护次数为 0 的终端所对应的异常终端类型标识和异常行为的类型的对应关系进行替换。

5. 根据权利要求 1 所述的异常终端的处理方法，其中，所述异常终端类型标识包括：特性群指示、国际移动设备识别码、国际移动设备识别码-型号认证码、国际移动设备识别码-软件版本中的任意一种。

6. 一种网管设备，包括：

生成模块，用于根据各个基站上传的在执行最小化路测任务时，所获取的异常终端类型标识和异常行为的类型的对应关系，生成第一防护表；

上传模块，用于将所述第一防护表上传至云服务器，以使所述云服务器对各个网管设备上传的第一防护表进行汇总，生成第二防护表；

控制模块，用于接收云服务器下发的所述第二防护表，并将所述第二防护表中的至少部分异常终端类型标识和异常行为类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行最小化路测任务。

7. 根据权利要求 6 所述的网管设备，其中，还包括：

第一判断模块，用于根据异常行为类型，判断基站是否开启引起异常行为所对应的相关功能；

检测模块，用于当所述第一判断模块判断出基站开启了引起异常行为对应的相关功能时，检测所述基站对应该异常行为的性能指标；

第二判断模块，用于判断所检测的性能指标是否大于第一阈值；

获取模块，用于当第二判断模块判断出所检测的性能指标大于第一阈值时，控制基站根据所引起的异常行为的类型，获取异常终端类型标识和异常行为的类型的对应关系。

8. 根据权利要求 6 所述的网管设备，其中，所述控制模块包括：

第一接收单元，用于接收云服务器下发的第二防护表；

获取单元，用于获取所述第二防护表中不同的异常终端类型标识的个数，记作 M ；以及获取基站能够接收的不同的异常终端类型标识的个数，记作 N ；

判断单元，用于判断 M 是否大于 N ；

控制单元，用于在判断单元判断出 $M > N$ 时，将所述第二防护表中 N 个不同的异常终端类型标识和异常行为的类型的对应关系，下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止执行最小化路测任务；以及，在判断单元判断出若判断出 $M \leq N$ 时，将第二防护表下发至所述基站，以使所述基站控制具有异常终端类型标识的终端终止

执行最小化路测任务。

9. 根据权利要求 8 所述的网管设备，其中，所述控制模块还包括：

第二接收单元，用于接收基站发送的替换请求；所述替换请求包括：基站在周期性的检测对异常终端类型标识所对应的终端的防护次数，且在出现防护次数为 0 的终端时发送的请求；

替换单元，用于根据所述替换请求，通过所述第二防护表中未被下发至基站的异常终端类型标识和异常行为的类型的对应关系，将防护次数为 0 的终端所对应的异常终端类型标识和异常行为的类型的对应关系进行替换。

10. 一种电子设备，其包括：

一个或多个处理器；

存储装置，其上存储有一个或多个程序，其中，当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现权利要求 1-5 中任意一项所述的方法。

11. 一种计算机可读介质，其上存储有计算机程序，其中，所述程序被处理器执行时实现权利要求 1-5 中任意一项所述的方法。

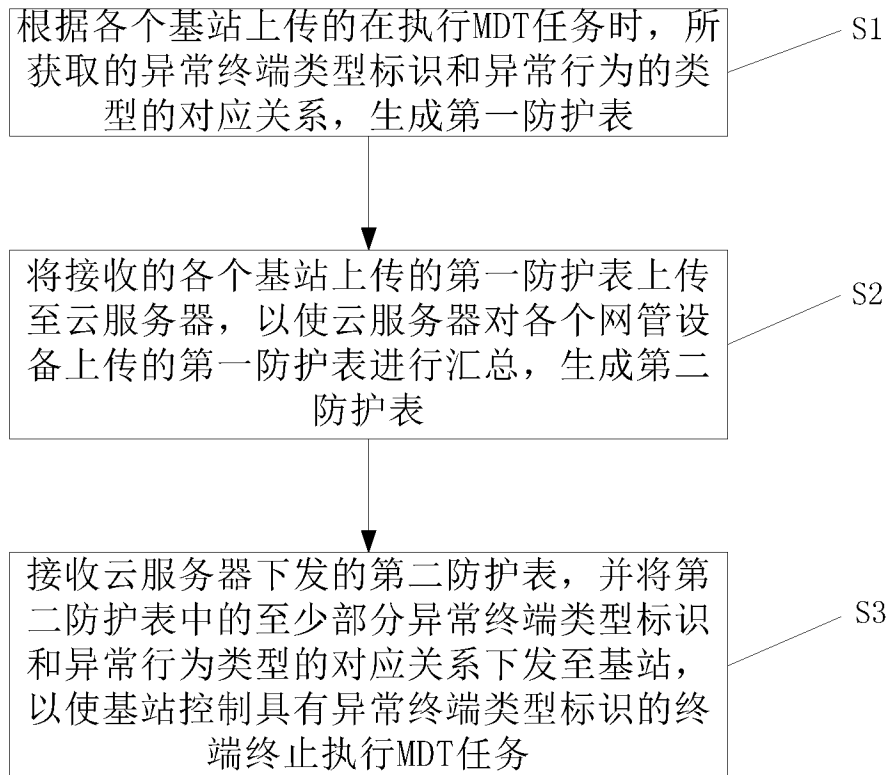


图 1

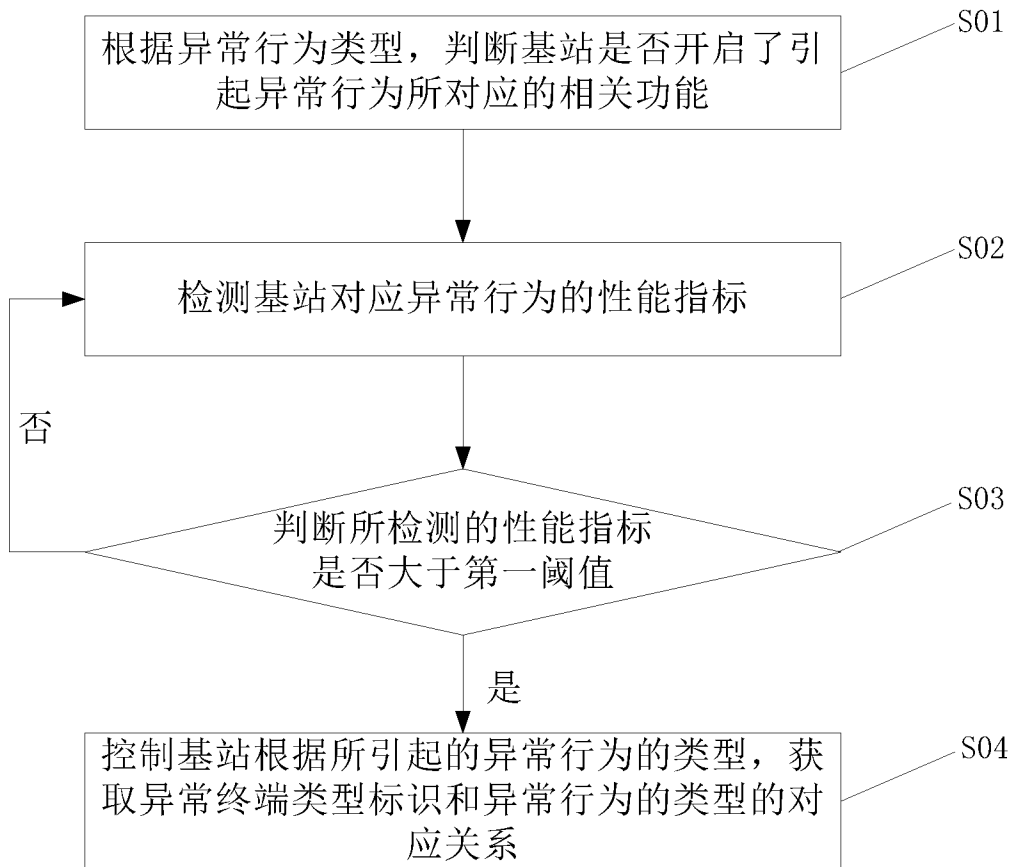


图 2

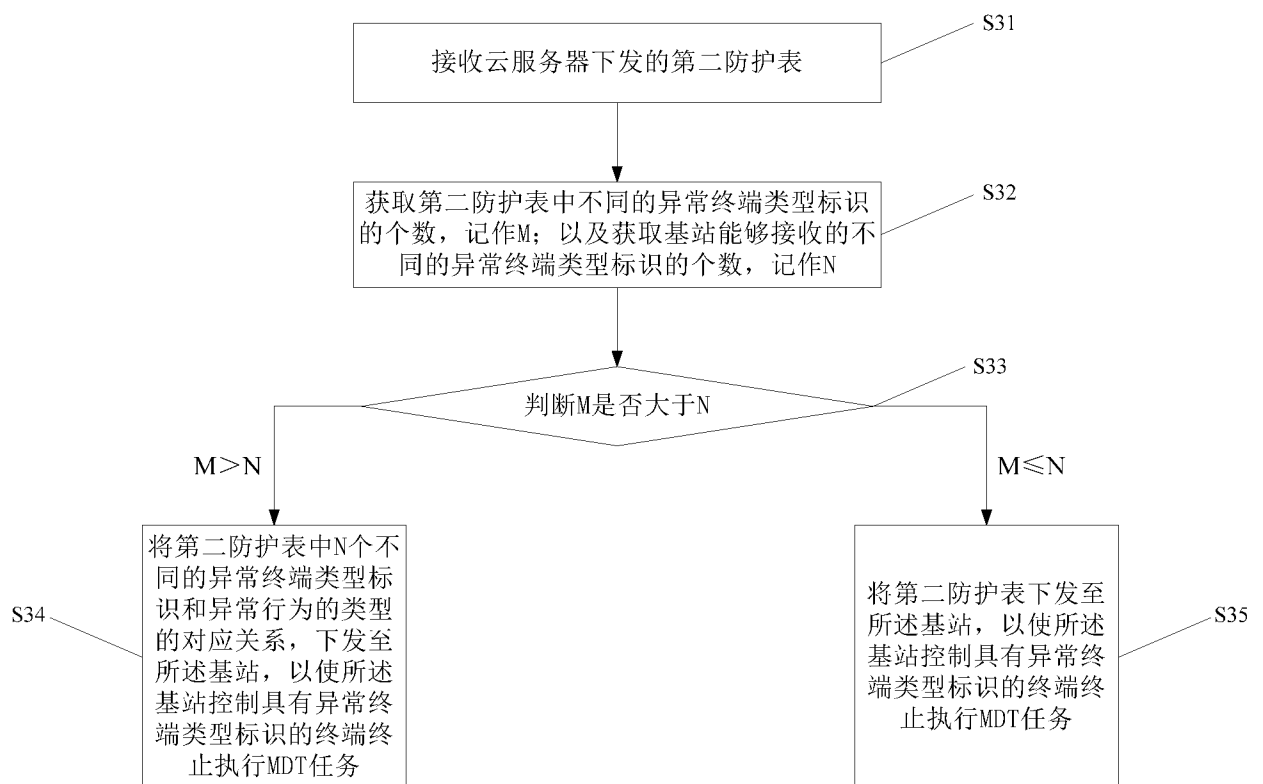


图 3

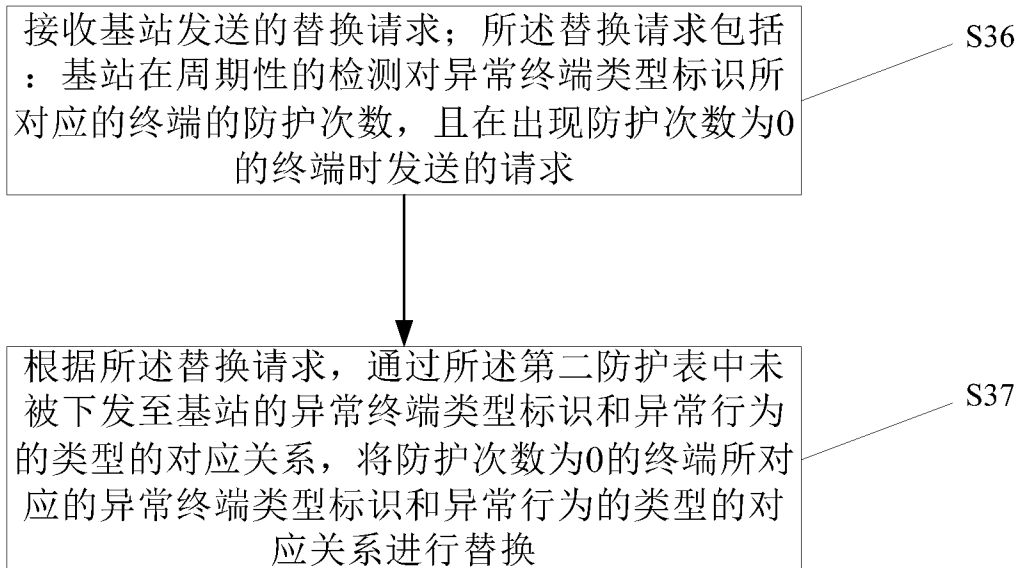


图 4

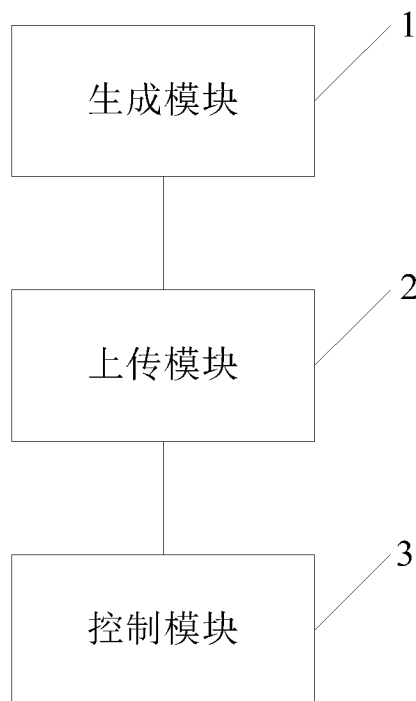


图 5

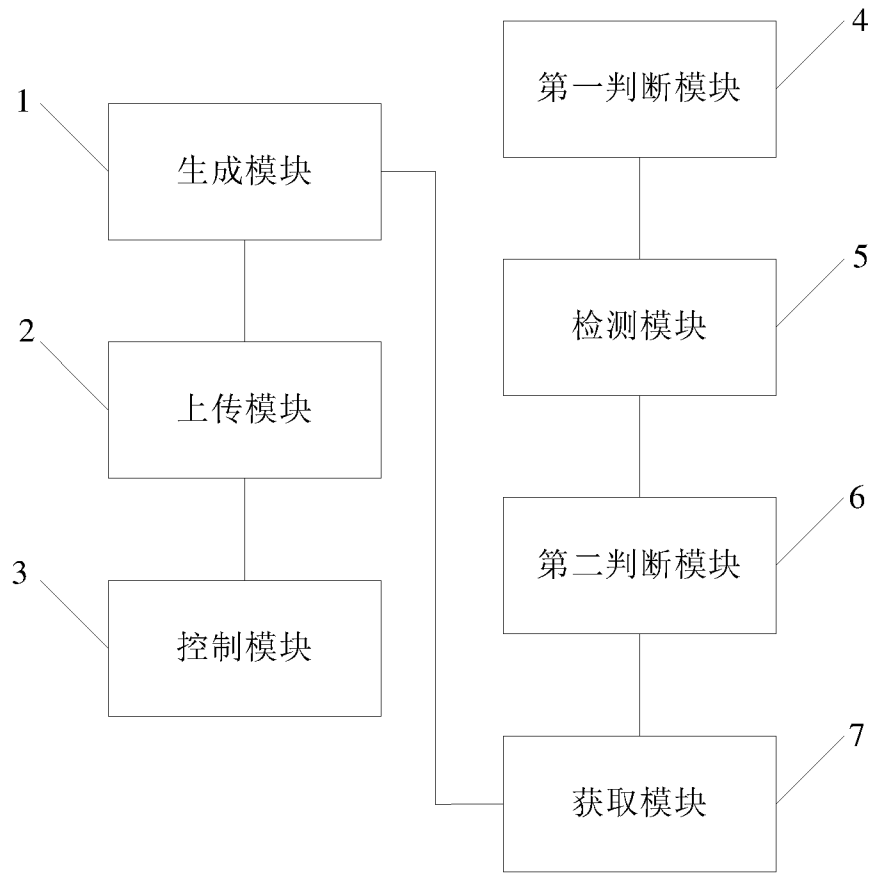


图 6

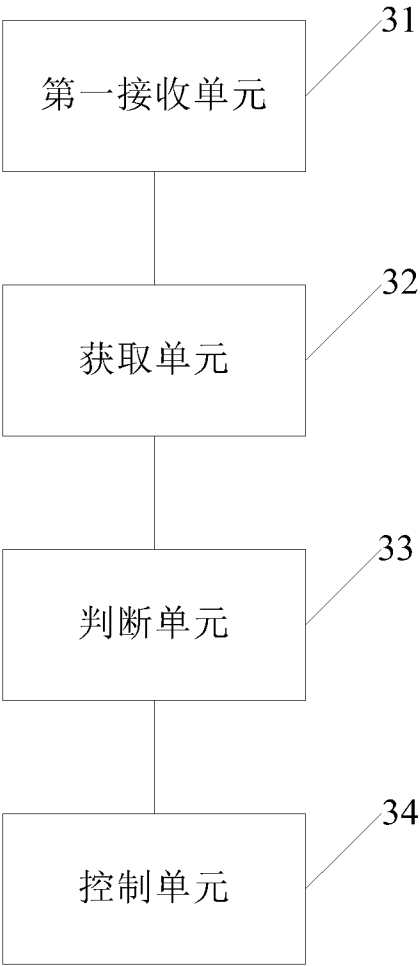


图 7

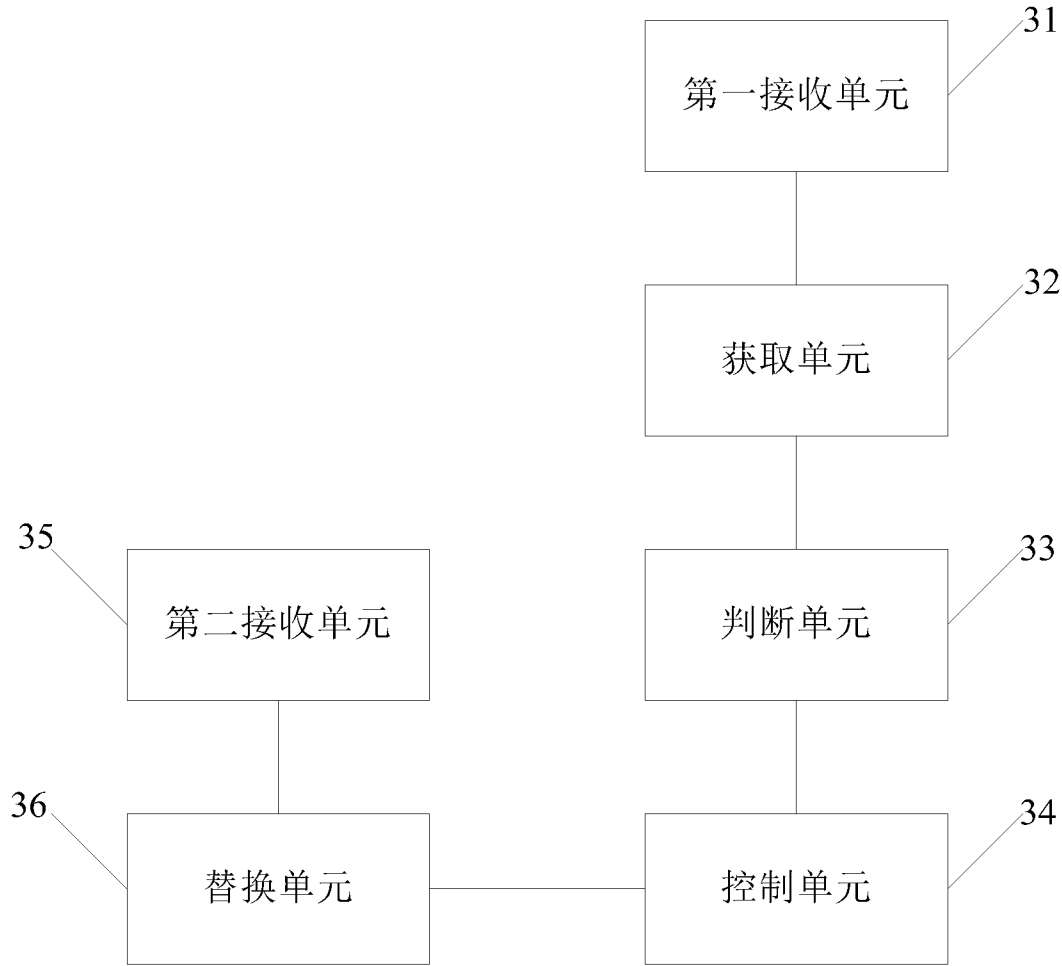


图 8

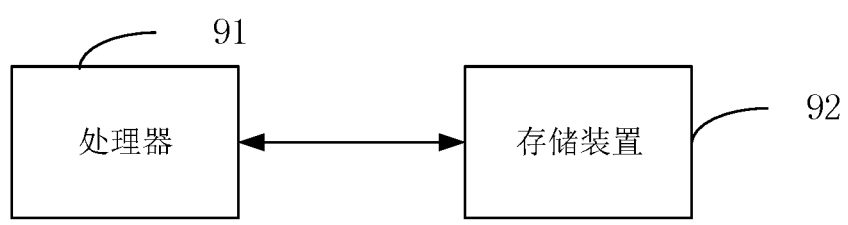


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/102816

A. CLASSIFICATION OF SUBJECT MATTER

H04W 24/02(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; H04L

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)

CNABS, CNTXT, CNKI: 云, 服务器, 标识, MDT, 设备, 异常, 终端, UE, 最小化路测, MDT, 表, 检测, 性能, 行为 VEN, EPTXT, USTXT, WOTXT, 3GPP: cloud, server, identity, ID, MDT, minimization drive test, abnormal, failure, UE, terminal, behavior

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 109391933 A (ZTE CORPORATION) 26 February 2019 (2019-02-26) description, paragraphs [0047]-[0070]	1-11
Y	CN 108668318 A (QIKU INTERNET NETWORK SCIENTIFIC (SHENZHEN) CO., LTD.) 16 October 2018 (2018-10-16) description, paragraph [0075]	1-11
A	KR 20180086593 A (LG UPLUS CORP.) 01 August 2018 (2018-08-01) abstract	1-11
A	CN 109818770 A (VIVO COMMUNICATION TECHNOLOGY CO., LTD.) 28 May 2019 (2019-05-28) entire document	1-11

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“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)

“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

“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

“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

“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

“&” document member of the same patent family

Date of the actual completion of the international search

15 September 2020

Date of mailing of the international search report

29 September 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Authorized officer

Facsimile No. (86-10)62019451

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/102816

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109391933	A	26 February 2019	WO	2019024939	A1	07 February 2019
CN	108668318	A	16 October 2018	WO	2019233218	A1	12 December 2019
KR	20180086593	A	01 August 2018	None			
CN	109818770	A	28 May 2019	WO	2019101124	A1	31 May 2019

国际检索报告

国际申请号

PCT/CN2020/102816

A. 主题的分类

H04W 24/02 (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; H04L

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))

CNABS, CNTXT, CNKI: 云, 服务器, 标识, MDT, 设备, 异常, 终端, UE, 最小化路测, MDT, 表, 检测, 性能, 行为, VEN, EPTXT, USTXT, WOTXT, 3GPP: cloud, server, identity, ID, MDT, minimization drive test, abnormal, failure, UE, terminal, behavior

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 109391933 A (中兴通讯股份有限公司) 2019年 2月 26日 (2019 - 02 - 26) 说明书第[0047]-[0070]段	1-11
Y	CN 108668318 A (奇酷互联网科技深圳有限公司) 2018年 10月 16日 (2018 - 10 - 16) 说明书第[0075]段	1-11
A	KR 20180086593 A (LG电信株式会社) 2018年 8月 1日 (2018 - 08 - 01) 摘要	1-11
A	CN 109818770 A (维沃移动通信有限公司) 2019年 5月 28日 (2019 - 05 - 28) 全文	1-11

☐ 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

2020年 9月 15日

国际检索报告邮寄日期

2020年 9月 29日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (ISA/CN)

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

授权官员

刘若琦

电话号码 010-62411401

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/102816

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	109391933	A	2019年 2月 26日	W0	2019024939	A1	2019年 2月 7日
CN	108668318	A	2018年 10月 16日	W0	2019233218	A1	2019年 12月 12日
KR	20180086593	A	2018年 8月 1日	无			
CN	109818770	A	2019年 5月 28日	W0	2019101124	A1	2019年 5月 31日