(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 105917625 B
(45)授权公告日 2020.03.27

(21)申请号 201380080326.3
(22)申请日 2013.10.18
(65)同一申请的已公布的文献号
申请公布号 CN 105917625 A
(43)申请公布日 2016.08.31
(85)PCT国际申请进入国家阶段日
2016.04.18
(86)PCT国际申请的申请数据
PCT/EP2013/071902 2013.10.18
(87)PCT国际申请的公布数据
WO2015/055259 EN 2015.04.23
(73)专利权人 瑞典爱立信有限公司
地址 瑞典斯德哥尔摩
(72)发明人 T•拉森 T•克弗恩维克
S•莫里茨 N•赛韦特
(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 梁洪源 康泉
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)
(56)对比文件
WO 2010114363 A1,2010.10.07,
WO 2008121945 A2,2008.10.09,
US 2012233311 A1,2012.09.13,
CN 1767452 A,2006.05.03,
审查员 尤一名

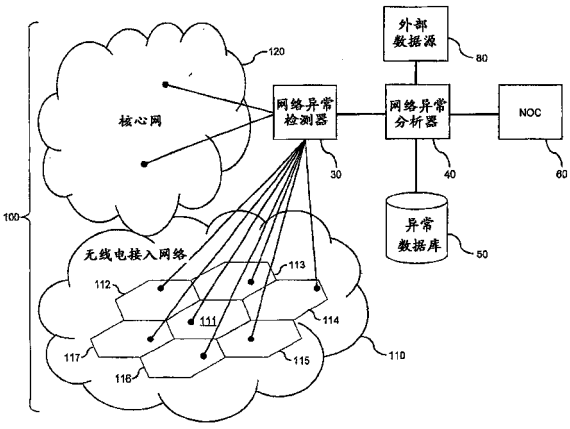
权利要求书4页 说明书11页 附图9页

(54)发明名称

使用附加数据的检测到的网络异常的分类

(57)摘要

网络异常检测器(30)通过监视通信网络(100)来检测网络异常，并向网络异常分析器(40)提供检测到的网络异常的指示。网络异常分析器(40)接收检测到的网络异常的指示，并且基于表示检测到的网络异常的数据以及例如来自通信网络(100)外部的附加数据来执行检测到的网络异常的分类。取决于检测到的网络异常的分类，网络异常分析器(40)向另一节点(60)提供关于检测到的网络异常的报告。例如，如果检测到的网络异常被分类为预期行为，则可以制止检测到的网络异常的报告。



CN 105917625 B

1.一种用于分析通信网络中的网络异常的方法,所述方法包括:

接收通过监视所述通信网络而检测到的网络异常的指示,其中所述指示包括数据,所述数据依照其时间和/或位置以及依照具有属性时间序列的异常模式来表示所述检测到的网络异常;

基于表示检测到的网络异常的数据且基于附加数据,通过表示所述检测到的网络异常的所述异常模式与异常数据库中存储的并与一个或多个先前检测到的网络异常有关的异常模式之间的模式匹配,执行所述检测到的网络异常的分类;

响应于确定所述检测到的网络异常被分类为预期行为,制止所述检测到的网络异常的报告;以及

响应于确定所述检测到的网络异常被分类为非预期行为,提供所述检测到的网络异常的报告,

其中所述附加数据包括来自所述通信网络外部的信息。

2.根据权利要求1所述的方法,

其中来自所述通信网络外部的信息包括与所述通信网络的服务区中的事件有关的信息。

3.根据权利要求1或2所述的方法,

其中来自所述通信网络外部的信息包括与所述通信网络的服务区中的天气有关的信息。

4.根据权利要求1-2中的任一项所述的方法,

其中所述附加数据包括与一个或多个先前检测到的网络异常有关的信息。

5.根据权利要求4所述的方法,

其中所述检测到的网络异常的所述分类基于相对于异常信息的模式匹配,所述异常信息从与一个或多个先前检测到的网络异常有关的信息中获得。

6.根据权利要求1-2中的任一项所述的方法,

其中所述检测到的网络异常的所述分类基于表示所述检测到的网络异常的数据与所述附加数据的时域相关。

7.根据权利要求1-2中的任一项所述的方法,

其中所述检测到的网络异常的所述分类基于表示所述检测到的网络异常的数据与所述附加数据的位置域相关。

8.根据权利要求1-2中的任一项所述的方法,

其中所述报告指示所述分类的结果。

9.根据权利要求1-2中的任一项所述的方法,包括:

取决于所述分类,向用于检测所述网络异常的网络异常检测器提供反馈。

10.一种用于分析通信网络中的网络异常的设备,所述设备包括至少一个处理器,

其中所述至少一个处理器配置成:

- 接收通过监视所述通信网络而检测到的网络异常的指示,其中所述指示包括数据,所述数据依照其时间和/或位置以及依照具有属性时间序列的异常模式来表示所述检测到的网络异常;

- 基于表示检测到的网络异常的数据且基于附加数据,通过表示所述检测到的网络异

常的所述异常模式与异常数据库中存储的并与一个或多个先前检测到的网络异常有关的异常模式之间的模式匹配，执行所述检测到的网络异常的分类；

- 响应于确定所述检测到的网络异常被分类为预期行为，制止所述检测到的网络异常的报告；以及

- 响应于确定所述检测到的网络异常被分类为非预期行为，提供所述检测到的网络异常的报告，

其中所述附加数据包括来自所述通信网络外部的信息。

11.根据权利要求10所述的设备，包括：

用于从网络异常检测器接收所述检测到的网络异常的所述指示的接口。

12.根据权利要求10或11所述的设备，包括：

用于发送关于所述检测到的网络异常的报告的接口。

13.根据权利要求10所述的设备，

其中来自所述通信网络外部的信息包括与所述通信网络的服务区中的事件有关的信息。

14.根据权利要求13所述的设备，

其中来自所述通信网络外部的信息包括与所述通信网络的服务区中的天气有关的信息。

15.根据权利要求10或11所述的设备，

其中所述附加数据包括与一个或多个先前检测到的网络异常有关的信息。

16.根据权利要求15所述的设备，

其中所述检测到的网络异常的所述分类基于相对于异常信息的模式匹配，所述异常信息从与一个或多个先前检测到的网络异常有关的信息中获得。

17.根据权利要求10或11所述的设备，

其中所述检测到的网络异常的所述分类基于表示所述检测到的网络异常的数据与所述附加数据的时域相关。

18.根据权利要求10或11所述的设备，

其中所述检测到的网络异常的所述分类基于表示所述检测到的网络异常的数据与所述附加数据的位置域相关。

19.根据权利要求10或11所述的设备，

其中所述报告指示所述分类的结果。

20.根据权利要求10或11所述的设备，

其中所述至少一个处理器配置成取决于所述分类，向用于检测网络异常的网络异常检测器提供反馈。

21.根据权利要求10或11所述的设备，

其中所述至少一个处理器配置成执行根据权利要求1-9中的任一项所述的方法的步骤。

22.一种用于分析通信网络中的网络异常的系统，所述系统包括：

网络异常检测器；以及

网络异常分析器，

其中所述网络异常检测器配置成通过监视所述通信网络来检测网络异常，以及向所述网络异常分析器提供检测到的网络异常的指示，其中所述指示包括数据，所述数据依照其时间和/或位置以及依照具有属性时间序列的异常模式来表示所述检测到的网络异常，以及

其中所述网络异常分析器配置成：

- 接收所述检测到的网络异常的指示；

- 基于表示所述检测到的网络异常的数据以及附加数据，通过表示所述检测到的网络异常的所述异常模式与异常数据库中存储的并与一个或多个先前检测到的网络异常有关的异常模式之间的模式匹配，执行所述检测到的网络异常的分类；

- 响应于确定所述检测到的网络异常被分类为预期行为，制止所述检测到的网络异常的报告以及

- 响应于确定所述检测到的网络异常被分类为非预期行为，提供所述检测到的网络异常的报告，

其中所述附加数据包括来自所述通信网络外部的信息。

23.根据权利要求22所述的系统，

其中所述网络异常分析器配置成执行根据权利要求1-9中的任一项所述的方法的步骤。

24.一种用于分析通信网络中的网络异常的设备，所述设备包括：

接收模块，用于接收通过监视所述通信网络而检测到的网络异常的指示，其中所述指示包括数据，所述数据依照其时间和/或位置以及依照具有属性时间序列的异常模式来表示所述检测到的网络异常；

分析模块，用于基于表示检测到的网络异常的数据且基于附加数据，通过表示所述检测到的网络异常的所述异常模式与异常数据库中存储的并与一个或多个先前检测到的网络异常有关的异常模式之间的模式匹配，执行所述检测到的网络异常的分类；以及

报告模块，用于响应于确定所述检测到的网络异常被分类为预期行为，制止所述检测到的网络异常的报告，并且响应于确定所述检测到的网络异常被分类为非预期行为，提供所述检测到的网络异常的报告，

其中所述附加数据包括来自所述通信网络外部的信息。

25.根据权利要求24所述的设备，包括：

用于从网络异常检测器接收所述检测到的网络异常的所述指示的接口。

26.根据权利要求24或25所述的设备，包括：

用于发送关于所述检测到的网络异常的报告的接口。

27.根据权利要求24所述的设备，

其中来自所述通信网络外部的信息包括与所述通信网络的服务区中的事件有关的信息。

28.根据权利要求27所述的设备，

其中来自所述通信网络外部的信息包括与所述通信网络的服务区中的天气有关的信息。

29.根据权利要求24或25所述的设备，

其中所述附加数据包括与一个或多个先前检测到的网络异常有关的信息。

30.根据权利要求29所述的设备，

其中所述检测到的网络异常的所述分类基于相对于异常信息的模式匹配，所述异常信息从与一个或多个先前检测到的网络异常有关的信息中获得。

31.根据权利要求24或25所述的设备，

其中所述检测到的网络异常的所述分类基于表示所述检测到的网络异常的数据与所述附加数据的时域相关。

32.根据权利要求24或25所述的设备，

其中所述检测到的网络异常的所述分类基于表示所述检测到的网络异常的数据与所述附加数据的位置域相关。

33.根据权利要求24或25所述的设备，

其中所述报告指示所述分类的结果。

34.根据权利要求24或25所述的设备，

其中所述设备配置成取决于所述分类，向用于检测网络异常的网络异常检测器提供反馈。

35.根据权利要求24或25所述的设备，

其中所述设备配置成执行根据权利要求1-9中的任一项所述的方法的步骤。

使用附加数据的检测到的网络异常的分类

技术领域

[0001] 本发明涉及用于分析网络异常的方法以及相应的设备。

背景技术

[0002] 在通信网络、例如3GPP(第三代合作伙伴计划)规定的蜂窝网络中,网络异常检测可以用于更好地支持通信网络的管理和维护。例如,检测到的网络异常可以指示出现故障的网络组件或是无法胜任的网络基础架构。

[0003] 用于此类目的的网络异常检测器可以监视通信网络以检测网络数据的不正常模式。例如,此类模式可以依照高出平常的数据业务量、高出平常的失败语音呼叫数量等等来限定。也就是说,网络异常可作为从正常(例如平均)网络行为的偏差来检测。由于检测到的网络异常可以指示通信网络、例如发生故障的网络组件的关键状态,因此可以将其用于触发警报。在US2008/0208526A1中描述了将来自网络的时间序列数据用作输入的相应异常检测系统的示例。

[0004] 然而,由于通信网络的操作条件在现实场景中会有相当大的变化,因此,对正常行为和偏离正常行为的偏差进行区分有可能是复杂的任务。而这有可能会出现检测到的网络异常实际对应的是指定状况下的预期行为的效果。例如,对于因为高出平常的数据业务量而被检测到的网络异常来说,其有可能归因于通信网络覆盖区域中的某个地点发生了重大事件,例如吸引大批受众的体育赛事或文化活动。在这种情况下,检测到的网络异常可被认为是非关键的,并且不必产生警报。

[0005] 相应地,有必要具有允许有效处理网络异常的技术。

发明内容

[0006] 根据本发明的实施例,所提供的是一种用于分析通信网络中的网络异常的方法。依照该方法,接收关于通过监视通信网络而检测到的网络异常的指示。基于表示检测到的网络异常的数据并基于附加数据,对检测到的网络异常进行分类。依照检测到的网络异常的分类,提供关于检测到的网络异常的报告。

[0007] 根据本发明的另一实施例,所提供的是一种用于分析通信网络中的网络异常的设备。该设备包括至少一个处理器。该至少一个处理器配置成接收关于通过监视通信网络而检测到的网络异常的指示。更进一步,该至少一个处理器配置成基于表示检测到的网络异常的指示并基于附加数据来对检测到的网络异常进行分类。更进一步,该至少一个处理器配置成依照检测到的网络异常的分类来提供关于检测到的网络异常的报告。该设备可以包括用于从网络异常检测器接收关于检测到的网络异常的指示的接口。该设备还可以包括用于发送关于检测到的网络异常的报告的接口。

[0008] 根据本发明的另一实施例,所提供的是一种用于分析通信网络中的网络异常的系统。该系统包括网络异常检测器和网络异常分析器。网络异常检测器配置成通过监视通信网络来检测网络异常,以及向网络异常分析器提供关于检测到的网络异常的指示。网络异

常分析器配置成接收关于检测到的网络异常的指示，以及基于表示检测到的网络异常的数据和附加数据，对检测到的网络异常进行分类。更进一步，网络异常分析器配置成依照检测到的网络异常的分类来提供关于检测到的网络异常的报告。

[0009] 根据本发明的另一实施例，所提供的是一种计算机程序。该计算机程序包括由设备的至少一个处理器运行以分析通信网络中的网络异常的程序代码。运行该程序代码使该至少一个处理器接收关于通过监视通信网络而检测到的网络异常的指示。更进一步，运行该程序代码使该至少一个处理器基于表示检测到的网络异常的数据且基于附加数据来对检测到的网络异常进行分类。更进一步，运行该程序代码使该至少一个处理器依照检测到的网络异常的分类来提供关于检测到的网络异常的报告。

附图说明

[0010] 图1示意性地示出可以应用根据本发明的实施例实施的网络异常分析的示例性通信网络环境。

[0011] 图2示出根据本发明的实施例来分析网络异常的示例性处理。

[0012] 图3示出可以在本发明的实施例中使用的示例性异常模式。

[0013] 图4示出可以在本发明的实施例中使用的示例性异常模型。

[0014] 图5显示用于示出根据本发明的实施例的方法的流程图。

[0015] 图6显示用于示出根据本发明的实施例的另一方法的流程图。

[0016] 图7显示用于示出根据本发明的实施例的另一方法的流程图。

[0017] 图8显示用于示出根据本发明的实施例的另一方法的流程图。

[0018] 图9示意性地示出根据本发明的实施例的网络异常分析器的结构。

具体实施方式

[0019] 以下将参考附图来对根据本发明的实施例的概念进行更详细说明。所示出的概念涉及通信网络、尤其是例如3GPP规定的蜂窝通信网络中的网络异常分析。通信网络可以支持各种无线电接入技术，例如GSM(全球移动通信系统)、UMTS(通用陆地移动电信系统)或宽带CDMA(码分多址)、CDMA2000、WiMaX或LTE(长期演进)。然而，应该理解，所示出的概念也可应用于其他类型的通信网络，例如使用诸如数字订户线(DSL)、同轴电缆或光纤之类的有线接入技术的网络或是基于网际协议(IP)的局域网(LAN)或广域网(WAN)。

[0020] 在所示出的概念中，所采用的是两阶段网络异常分析处理。在第一个阶段，通过监视通信网络来检测网络异常。为此目的，可以应用各种用于分析网络数据的已知机制，例如M.Thottan等人发表于Algorithms for Next Generation Networks，Computer Communications and Networks，Springer London(2010)第239-261页的“Anomaly Detection Approaches for Communication Networks”。通常，此类机制可以基于检测网络数据的一个或多个属性与这些属性的正常出现的偏差。这可以通过使用基于模型的算法和/或通过统计算法来完成。在第二个阶段，对在第一个阶段中检测到的网络异常进行更进一步的分析。该分析基于例如依照时间和/或位置来表示检测到的网络异常的数据以及基于附加数据。举例来说，此类附加数据可以包括来自通信网络外部的信息，其在下文中也被称为外部数据。关于此类外部数据的示例是提供与通信网络服务区中的天气有关的信息的

天气数据、提供与通信网络服务区中的事件有关的信息的事件进度表、与诸如灾害之类的其他事件有关的信息、来自社交媒体或社交网络平台的信息、或是来自在通信网络服务区中运营的公共事业供应商的信息。作为补充或替换，该附加数据可以包括与先前检测到的网络异常有关的历史信息。执行第二阶段的分析以获取检测到的网络异常的分类。例如，检测到的网络异常可以分类成预期行为或非预期行为。更进一步，该分类可用于在不同类型的网络异常、例如与组件故障相关的异常，与过载相关的异常等等之间进行区分。

[0021] 图1示意性地示出了通信系统100以及用于实施两阶段网络异常分析处理的系统的组件。如所示，通信系统100可以包括无线电接入网络110，其中该网络具有多个小区111、112、113、114、115、116，以允许用户设备(UE)接入通信网络100。更进一步，通信网络100可以包括核心网120。核心网120可以采用已知的方式来提供用于控制无线电接入网络110的功能性，例如关于移动性、计费或服务质量。更进一步，核心网120还可以提供与因特网之类的其他网络的连接。更进一步，核心网可以向用户提供某些服务，例如多媒体服务。

[0022] 提供网络异常检测器30以实施第一阶段的分析处理。如所示，网络异常分析器30可以耦合到通信网络100中的不同节点，以允许监视通信网络100。如所示，这些节点可以位于无线电接入网络110和/或核心网120。所述监视可以基于不同类型的网络数据来执行。例如，在监视业务负载时，此类网络数据可以包括数据平面业务量。更进一步，作为示例，在监视成功或未成功的连接建立过程、在小区111、112、113、114、115、116之间的成功或未成功的切换、UE的成功或未成功的消息发送尝试、拥塞指示、警报消息、故障单等等的时候，此类网络数据可以包括控制平面业务。网络数据可以对照一个或多个属性随时间和/或在指定位置的发生而被分析。如上所述，网络异常检测器30可以通过监视网络数据来应用各种用于检测网络异常的算法。

[0023] 提供网络异常分析器40以实施第二阶段的分析处理。网络异常分析器40与网络异常检测器30耦合，以接收关于网络异常检测器30检测到的网络异常的指示。作为示例，此类指示可以包括依照检测到的网络异常的时间和/或位置而表示检测到的网络异常的数据。表示检测到的网络异常的数据还可以包括用于表征检测到的网络异常的一个或多个属性的模式。

[0024] 如进一步图示的那样，网络异常分析器40可以耦合到异常数据库50。作为示例，异常数据库50可以存储先前检测到的网络异常的异常模式。更进一步，异常数据库50还可以存储描述已知类型的网络异常的异常模型。

[0025] 如进一步图示的那样，网络异常分析器40耦合到一个或多个外部数据源80。这样的外部数据源80可用于提供来自通信网络100外部的潜在地与检测到的网络异常相关的信息。例如，来自外部数据源80的外部数据可以包括天气信息或来自事件进度表的信息。作为示例，来自事件进度表的示例性信息可以包括事件名称、事件开始日期和/或时间、事件结束日期和/或时间、事件持续时间、事件位置、事件重复模式等等。

[0026] 由此，网络异常分析器40可以使用来自外部数据源的外部数据和/或来自异常数据库50的数据来进一步分析检测到的网络异常。如上所述，这种更进一步的分析的目的是对检测到的网络异常进行分类。然后，依照该分类，网络异常分析器40可以提供关于检测到的网络异常的报告。作为示例，报告可以包含警报。举例来说，如果检测到的网络异常被分类到非预期行为，那么网络异常分析器40可以向另一个节点发送关于检测到的网络异常的

报告，其中在图示示例中，所述另一个节点与网络操作中心(NOC)60相对应。在这里，应该指出的是，网络异常分析器可以向需要与检测到的网络异常有关的报告的不同类型的节点乃至多个节点发送报告，作为示例，此类节点可以是用于聚合商业管理信息的节点、用于聚合基础设施规划信息的节点、或是用于聚合针对其他目的的信息的节点，例如用于调度工作人员的信息、用于向处于通信网络服务区的人员提供商业产品的信息。另一方面，如果检测到的网络异常被分类到预期行为，那么可以制止该检测到的网络异常的报告，例如通过不发送报告或者在报告中不考虑检测到的网络异常来制止。这样做可以避免不需要的报告或者避免产生虚假警报。此外，通过对相关信息划分优先级，可有助于对此类报告的自动或手动分析。

[0027] 在示例性场景中，检测到的网络异常可以对应于在诸如足球比赛之类的吸引大批受众的大型公共事件期间不断增长的SMS(短消息服务)业务，并且这是预期行为。外部数据又可以包括来自指定了事件时间的事件进度表的信息。通过将检测到的网络异常和所调度的事件的时间相关联，网络异常分析器可以将检测到的网络异常归类为预期行为，并且可以制止向NOC 60发送关于检测到的异常的报告。此外，在一些实施方式中还可以定义更复杂的过滤判据，以便依照分类来控制选择性的报告。例如，此类过滤判据可以定义只发送针对某些分类的报告，同时制止报告检测到的关于其他分类的网络异常。此外，此类过滤判据可以规定：关于某种分类的报告应该与关于该分类的指示一起发送。更进一步，此类过滤判据可用于定义报告的接收方，也就是依照分类来选择报告的接收方。

[0028] 网络异常分析器40可以使用各种机制来对检测到的网络异常进行分类。

[0029] 在一些实施方式中，网络异常分析器40可以使用模式匹配。为此目的，在异常数据库50中可以存储关于检测到的网络异常的异常模式，并且网络异常分析器40可以将新检测到的网络异常的异常模式与已存储的一个或多个异常模式相比较。所存储的异常模式可以反映网络异常或是其某些属性出现的时间、检测到的网络异常的持续时间、其发生的频率等等。更进一步，所存储的异常模式还可以反映网络异常的幅度，作为示例，该幅度可以依据针对某个属性测得的值，例如消息或其他数据的丢失率。如果发现新检测到的模式与一个或多个已存储的异常模式相似，那么网络异常分析器40可以将新检测到的网络异常分类成预期行为。同时，已存储的相似的异常模式可被标记成与预期行为相关联。由此，网络异常分析器可以自动学习应该产生作为预期行为的分类的异常模式。并且网络异常分析器40还可以通过分析过去检测到的多个已存储的异常模式来寻找规律，以及指定定期出现的网络异常，例如在新年前夜出现的一年一次的网络异常，在一周中的某一天出现的网络异常，或是以别的定期重复时间间隔出现的网络异常，抑或是在其他方面类似于同一分类的网络异常。另外，异常模式也可以是基于较短的时间量程而被分析。例如，所分析的可以是网络数据的一个或多个属性在诸如足球比赛之类的具有特定持续时间的某个事件中出现的顺序。作为示例，此类模式的属性可以由该事件期间的不同时间间隔中的SMS消息和/或语音呼叫的数量来定义。

[0030] 如上所述，作为替换或补充，与来自通信网络100外部的外部数据的相关性可被用于执行分类。例如，此类外部数据可以包括来自事件日历的信息，并且可以指定通信网络100中的服务区中的某个事件的时间，此外通常还可以指定该事件的位置，举例来说，此类事件可以是足球比赛、音乐会、假日。另一个示例是天气数据，其中作为示例，该数据反映的

是通信网络100的服务区中的强降雨、强降雪、雷暴和/或其他极端天气状况的时间和/或位置。网络分析器40可以对外部数据以及表示新检测到的网络异常的数据执行时域相关和/或位置域相关，以便对新检测到的网络异常进行分类。举例来说，如果检测到的网络异常的时间和位置匹配于某个事件的时间和位置，那么可以因为该事件而将该网络异常分类为预期。同样，如果检测到的网络异常的时间和位置匹配于特定天气状况的时间和位置，那么可以因为所述特定的天气状况而对该网络异常进行分类。在另一个示例中，检测到的网络异常可能归因于服务区中某个部分的停电事故，而这可能会导致通信网络中的节点切换到电池备份电源以及发送相应的通知。相应地，通过使用来自供应方的相应信息，网络异常检测器40会因为停电事故而将检测到的网络异常归类为预期。同样，检测到的网络异常还有可能是由某些节点在从电池备份电源切回至正常电源时的不规则的行为引起的，而这则是一种通常需要进行报告的紧急情况。

[0031] 类似的分类还可以针对已存储的网络异常来执行，并且可以使用基于外部数据的分类来将已存储的异常模式指定至某个类，例如通过依照与外部数据相关的结果来对其进行标记。通过组合使用模式匹配以及与外部数据的相关，网络异常分析器40由此可以获取指配至一个或多个类的已存储的异常模式。此类分类可以使用与异常模式一起存储的标签来指示。例如，此类标签可以简单地指示异常模式与预期行为相关，例如用标签“EXPECTED(预期的)”来指示。更进一步，也可以使用更复杂的标签，其中该标签还指示了附加信息，例如关于预期行为的原因。作为示例，此类复杂标签可以指示“EXPECTED DUE TO WEATHER(由于天气而是预期的)”。更进一步，也可以使用不同标签的组合，例如“EXPECTED(预期的)”与“FOOTBALL(足球)”的组合或“EXPECTED(预期的)”与“RAINFALL(降雨)”的组合。

[0032] 作为补充或替换，已存储的异常模式还可以由操作人员手动分类和标记，或者操作人员也可以对自动生成的已存储的异常模式的分类进行核实。

[0033] 在一些实施方式中，网络异常分析器还可以使用网络异常模型来对检测到的网络异常进行分类。例如，此类模型可以通过分析一个或多个已存储的异常模式并且确定再现了所分析的异常模式的一个或多个特性的模型而被创建。与将新检测到的网络异常与先前检测到的网络异常的已存储异常模式相比较不同，新检测到的异常模式的异常模式可以与异常模型相比较。这可以促进该比较过程，并且可以提供更精确的结果，其原因在于与单独存储的异常模式相比，异常模型不易受到随机变化的影响。与已存储的异常模式相似，异常模型可被指定至一个或多个分类，如上所述，这一点可以通过将异常模型与一个或多个标签一起存储来指示。

[0034] 图2示出了以上述概念为基础的用于分析网络异常的示例性过程。图2的过程涉及位于诸如无线电接入网络110和/或核心网120的一个或多个网络数据源10，用于提供诸如事件进度表信息或天气数据之类的来自通信网络100外部的外部数据的一个或多个外部数据源，网络异常检测器30、网络异常分析器40以及作为用于接收检测到的网络异常的报告的示例性节点的NOC 60。

[0035] 在图示过程中，网络数据源10首先可以向网络异常检测器30提供网络数据201。例如，网络数据201可以包括属性的时间序列，例如一系列的时间间隔中的业务量速率、消息发送或丢失率、切换、或是成功或未成功的连接建立尝试。网络数据还可以用位置参考，也就是包含关于网络数据201所属的通信网络100的服务区内的位置的指示。例如，此类位置

可以依照地理位置和/或通过指定通信网络100的一个或多个小区111、112、113、114、115、116来指示。

[0036] 网络异常检测器30接收网络数据201，然后，如步骤202所示，其可以基于网络异常检测算法并使用该网络数据来执行模型或模式训练。更进一步，网络异常检测器30分析网络数据201来检测网络异常。在图2的示例中，假设网络异常检测器30检测到网络异常，并且向网络异常分析器40提供检测到的网络异常的指示203。指示203包含依照时间(例如时间戳)和/或位置(例如地理位置或小区或小区群组)、以及依照具有属性时间序列的异常模式来表示检测到的网络异常的数据。此外，同样可以包含这些信息，例如依照幅度和/或持续时间或用于指定检测到的网络异常的属性的信息来量化网络异常的一个或多个值。

[0037] 然后，如消息204、205所示，网络异常分析器40可以从外部数据源80获取外部数据205。例如，此类外部数据205可以是天气数据、来自事件进度表的信息，或与检测到的网络异常所在位置的灾害有关的信息。

[0038] 然后，如步骤206所示，通过使用从网络异常检测器30接收的指示203中的表示检测到的网络异常的数据以及外部数据205，网络异常分析器40对检测到的网络异常进行分析。在图示的示例中，假设作为步骤206的分析的结果而将检测到的网络异常分类为预期行为。作为示例，该分析可以揭示检测到的网络异常的时间和位置与强降雨相关，检测到的网络异常源自强降雨造成的恶劣无线电状况，以及该异常是预期行为。由此，网络异常分析器40可以将检测到的网络异常的异常模式存入异常数据库50(在图2中并未显示)，并且提供具有标签“EXPECTED”和“RAINFALL”的已存储异常模式。

[0039] 更进一步，如步骤207所示，网络异常分析器40还可以执行针对异常模型的训练，其中该训练将会再现该异常模型的特性。例如，在这里可以使用针对异常模式的取平均值、小波表示或分析函数拟合处理。更进一步，对于模式匹配来说，作为示例，为其许可的偏差范围可以通过对近似过程进行统计评估来调节。由此还可以获取异常模型，该模型被保存在异常数据库50中(在图2中并未显示)，并且提供带有恰当标签的存储的异常模式，例如，在采用以上的强降雨所导致的恶劣无线电状况的示例时，该标签可以是“EXPECTED”和“RAINFALL”。

[0040] 由于将检测到的网络异常分类到预期，因此，网络异常分析器40会制止进一步报告所检测到的网络异常。

[0041] 如进一步图示的那样，网络异常分析器40可以向网络异常检测器30提供反馈208。如步骤209所示，网络异常检测器30可以使用反馈208来进一步执行对所使用的网络异常检测算法的训练。特别地，网络异常检测算法可以使用反馈208来改进关于正常网络行为的表示。

[0042] 然后，如步骤211所示，网络异常检测器30可以接收其他网络数据210，其中网络异常检测器30可以通过分析这些网络数据来检测其他网络异常。网络异常检测器30向网络异常分析器40提供关于检测到的网络异常的指示212。该指示212包含依照检测到的网络异常的时间和/或位置以及依照带有关于属性的时间序列的异常模式来表示所述检测到的网络异常的数据。

[0043] 然后，如步骤213所示，通过分别使用从网络异常检测器30接收的指示212中的表示检测到的网络异常的数据以及从步骤206和207获得的已存储的异常模式和/或异常模

型，网络异常分析器40对检测到的网络异常进行分析。在图示的示例中，假设作为步骤213的分析结果，由于检测到的网络异常不与任何已存储的异常模式或异常模型相匹配，因此将其归类为非预期行为。由此，网络异常分析器40向NOC 60发送关于检测到的网络异常的报告。更进一步，网络异常分析器40可以将检测到的网络异常的异常模式存入异常数据库50，以便将其用于以后的分析。

[0044] 图3显示了可以在上述过程中使用的示例性的异常模式。如所示，该异常模式是在网络数据属性的时间序列中出现的。对于用例如时间戳标识的时间间隔序列t1、t2、...、tn来说，从被监视的网络业务中可以确定一个或多个属性。在图示的示例中，示例性属性被称为“X”，并且是用范围在0到1的值量度。例如，该属性“X”的值可以是关于以下各项的量度：连接至UE的成功或未成功尝试比率、诸如SMS消息之类的某种已发送消息的比率、丢失数据的比率、通常会在服务区的指定区域或某个部分监视的某种警报的比率，作为示例，所述区域或部分是依照地理位置或是一个或多个小区限定的。图3所示的介于垂直虚线之间的异常模式构成了从该属性的正常行为的偏差。在所示的概念中，此类异常模式可被转发至网络异常分析器，以便用于对检测到的网络异常进行分类。

[0045] 在图4中示意性地示出可被产生以再现图3中的异常模式的异常模型的示例。例如，该异常模型可以基于检测到的多个相似模式的分组以及确定近似于被分组的异常模式的模型函数，作为示例，所述近似可以通过取平均值、小波表示或是分析函数拟合来实施。在图4中，虚线示出来自此类近似的统计值的25％和75％的四分位数。

[0046] 作为示例，模式匹配可以基于欧几里德距离。也就是说，如果两个模式之间的欧几里德距离很短，例如低于某个阈值，那么可以认为这两个模式匹配。该模式匹配还可以基于动态事件规整(DTW)或小波。举例来说，如果所使用的是图4所示的异常模式，那么，如果某一个模式模型处于25％或75％的四分位数范围以内或或者处于可以从异常模型的近似统计中得出的其他某个范围以内，例如处于使用其他四分位数值定义的范围以内，那么可以认为该异常模式与异常模型匹配。两种模式间的匹配还可以包括将这些模式归一化到同一个范围，例如0与1之间，和/或对这些属性值执行平滑化处理，例如使用移动平均函数来平滑。

[0047] 如上所述，网络异常分析器40还可以对模式进行分析来确定是否在相同位置重复出现相同的异常模式。如果检测到周期性或其他类型的规律性，那么网络异常分析器40可以将相似的异常模式分类为预期，并且还可以由所确定的规律性推断以后，然后可以将其用于对新检测到的网络异常进行分类。关于此类规律性的示例包括在每天的同一时间、每周的同一天、每月的同一天、每季度的同一天、每年的同一天发生的网络异常，作为示例，所述网络异常可以归因于假日，例如圣诞节、感恩节等等。

[0048] 外部数据可用于标记异常模式或异常模型，并且由此可以细化分类。举例来说，如果检测到的网络异常的时间和/或位置与某个外部数据、例如足球比赛之类的事件相关联，那么可以将其异常模式与诸如“FOOTBALL”之类的相应标签保存在一起。

[0049] 图5显示可用于实施网络异常分析器40的训练的方法。

[0050] 在步骤510，网络异常分析器40获取异常模式。该异常模式可以与关于检测到的网络异常的指示一起从网络异常检测器30接收。该异常模式可以采用结合图3示例所说明的方式来定义。

[0051] 在步骤520，网络异常分析器40将该异常模式与外部数据相关联。如上所述，作为示例，这可以包括与外部数据的时域相关和/或位置域相关。例如，该外部数据可以包括来自事件进度表或天气数据的信息。

[0052] 在步骤530，依照步骤520的相关结果来标记异常模式。举例来说，如果网络异常的时间并且通常还有位置与外部数据指示的某个事件、例如足球比赛或音乐会的时间和/或位置相关，那么可以相应地标记该异常模式，例如用标签“FOOTBALL”来标记。更进一步，如果网络异常的时间并且通常还有位置与外部数据所指示的特定天气状况相关，那么可以相应地标记该异常模式，例如用标签“SUNNY”或“RAINFALL”来标记。

[0053] 在步骤540，使用被标记的异常模式来执行训练。这可以包括存储被标记的异常模式。作为补充或替换，这可以包括使用该异常模式作为用于确定异常模型的近似过程的输入数据，以便确定诸如结合图4说明的异常模型或者适配此类异常模型。特别地，被标记的异常模式可以与带有相同标签的其他异常模式一起使用，以便确定或适配异常模型。

[0054] 图6显示可供包含网络异常检测器30和网络异常分析器40的系统用来实施对网络异常进行分析的整个过程的方法。

[0055] 在步骤610，网络异常检测器30获取网络数据。如上所述，这些网络数据可以通过监视通信网络100来获取，并且位于通信网络100、例如位于无线电接入网络110和/或核心网120的不同节点可以充当网络数据的来源。网络数据可以作为一个或多个属性的时间序列来提供，例如业务负载、某种消息的发送率或丢失率、警报比率、连接UE的成功或未成功尝试、切换比率等等。

[0056] 在步骤620，网络异常检测器30检测网络数据中的网络异常。如上所述，这通常是通过识别偏离正常行为的一个或多个属性来完成的。各种网络异常检测算法均可用于该目的，例如基于模型的算法或统计算法。

[0057] 在步骤630，网络异常检测器30向网络异常分析器40指示检测到的网络异常。这是连同表示检测到的网络异常、例如指示其时间和/或位置的数据一起完成的。表示检测到的网络异常的数据还可以包括从网络数据中提取的异常模式，例如包含了在步骤620识别的一个或多个偏差属性的网络数据的子集。

[0058] 在步骤640，网络异常分析器40对检测到的网络异常进行分类。这可以基于使用外部数据的先前训练来完成，作为示例，该训练与图5的方法中的训练相同。举例来说，与已存储的异常模式或异常模型所进行的模式匹配处理可以用于该分类。该分类可以区分预期和非预期行为。举例来说，如果异常模式与已存储的异常模式或是某个异常模型匹配，那么可以将检测到的网络异常分类为预期行为。此外，更精细的分类也是可行的。

[0059] 在步骤650，网络分析器40可以报告检测到的网络异常，例如向NOC或其他某个节点发送报告。该报告依照步骤640的分类来执行。举例来说，如果将检测到的网络异常分类为预期行为，那么可以制止报告检测到的网络异常，例如通过不发送报告或者在报告中不考虑该检测到的网络异常来制止。此外，在一些实施方式中还可以定义更复杂的过滤判据，以便控制依照分类的选择性报告。例如，此类过滤判据可以限定只发送针对某些分类的报告，同时制止报告检测到的关于其他分类的网络异常，即使所述其他分类对应于预期行为。并且，此类过滤判据可以规定，对于某个分类来说，该报告应该与关于该分类的指示一起发送。更进一步，该分类过滤判据可用于限定哪个节点应该接收该报告，也就是依照分类来选

择报告的接收方。此外，该过滤判据还可以是可配置的，例如可以由一个或多个可能接收该报告的节点来配置，由此可以灵活控制哪个分类应该触发报告以及哪个分类不应该触发报告。

[0060] 作为示例，这种由网络异常分析器40选择性报告检测到的网络异常的处理可以通过图7的方法来实施。

[0061] 在步骤710，网络异常分析器40开始分类处理，例如通过执行与采用如上所述的方式标记的一个或多个已存储异常模式和/或一个或多个异常模型的模式匹配而开始执行分类处理。

[0062] 在步骤720，网络异常分析器40检查检测到的网络异常的分类是否成功。如果是的话，那么如分支“是(Y)”所示，网络异常分析器40前进到步骤730。

[0063] 在步骤730，网络异常分析器40获取发现匹配的已存储异常模式或异常模型的标签。

[0064] 在步骤740，网络异常分析器40基于标签来检查是否需要发送关于检测到的网络异常的报告。举例来说，如果这些标签指示因为足球比赛或特定天气状况所导致的某种类型的预期行为，那么如分支“否(N)”所示，网络异常分析器40可以确定不需要发送报告，并且前进到步骤750。

[0065] 在步骤750，网络异常分析器40可以将与检测到网络异常分类成功相对应的事件记入日志。此外，作为示例，网络异常分析器40还可以存储检测到的网络异常的异常模式，例如将其用于训练异常模型。

[0066] 如果步骤720的检查揭示该分类不成功，也即是没有发现匹配的已存储异常模式或异常模型，那么如分支“N”所示，网络异常分析器40将该网络异常分类为非预期，并且前进到步骤760。

[0067] 在步骤760，网络异常分析器40将异常模式馈送至训练处理，作为示例，该馈送是通过存储该异常模式以进行未来的模式匹配尝试或是通过使用该异常模式创建新的异常模型实施的。

[0068] 在步骤770，网络异常分析器40发送检测到的网络异常的报告。

[0069] 如果步骤740的检查揭示的是需要发送报告，那么网络异常分析器40也前进到步骤760以发送报告。作为示例，这可以是当标签指示预期行为非常关键的情况。

[0070] 在步骤760发送的报告还可以包括分类结果，例如指示检测到的网络异常的标签或分类。此类信息对于报告的接收方来说是有价值的，因为其有助于对网络异常做出反应。如果将检测到的网络异常分类为非预期行为，那么也可以对此进行指示。对于非预期行为来说，诸如NOC 60之类的报告接收方可以返回与检测到的网络异常有关的信息，例如返回采用了标签的形式的信息。然后，网络异常分析器40可以在未来的分类过程中使用该信息。

[0071] 从图7的方法中可以看出，网络异常分析器40可以持续聚合用于训练的新的信息，由此可以允许网络异常分析器40动态适配新的网络异常类和/或提升分类精度。

[0072] 图8示出另一用于分析通信网络中的网络异常的方法。图8的方法可用于在分析检测到的网络异常的设备中实施上述概念，例如网络异常分析器40。也就是说，图8的方法的步骤可以由此类用于分析检测到的网络异常的设备来执行。

[0073] 在步骤810，接收关于网络异常的指示，其中该异常是先前通过监视通信网络检测

到的。

[0074] 在步骤820，可获取附加数据。该附加数据可以包括来自通信网络外部的信息，也就是外部数据。例如，来自通信网络外部的这类数据可以包括关于通信网络服务区中的事件的信息，作为示例，该事件可以来自事件进度表。关于此类事件的示例是足球比赛或音乐会之类的吸引大批受众的事件、假日、灾害等等。作为示例，该信息可以指定事件的定时、例如时间和/或持续时间、或位置。来自通信网络外部的此类信息还可以包括关于通信网络的服务区中的天气的信息，作为示例，该信息尤其与服务区内部的某个位置或是服务区的某个部分相关。该附加数据可以包括关于先前检测到的一个或多个网络异常的信息，例如如上所述的已存储的异常模式或异常模型。

[0075] 在步骤830，对检测到的网络异常进行分类。该分类是以表示检测到的网络异常的数据以及来自步骤820的附加数据为基础完成的。对检测到的网络异常的分类可以以对照从一个或多个先前检测到的网络异常中获取的异常信息的模式匹配为基础，例如如上所述的已存储的异常模式或异常模型。

[0076] 检测到的网络异常的分类可以区分预期行为和非预期行为。此外，更精细的或是其他的分类也是可行的。

[0077] 与步骤810的指示一起接收的表示检测到的网络异常的数据可以包括检测到的网络异常的定时，例如，检测到的网络异常的开始时间、结束时间和/或持续时间。更进一步，表示检测到的网络异常的数据包括检测到的网络异常的位置，例如，依照地理位置或通信网络服务区的某个部分，例如小区或小区群组。

[0078] 对检测到的网络异常所做的分类可以基于表示检测到的网络异常的数据与附加数据的时域相关，和/或基于表示检测到的网络异常的数据与附加数据的位置域相关。

[0079] 在步骤840，提供检测到的网络异常的报告。这是依照步骤830的分类完成的。举例来说，如果将检测到的网络异常分类为预期行为，那么可以制止报告检测到的网络异常，例如通过不发送报告或者在报告中不考虑所述检测到的网络异常来制止。此外，在一些实施方式中还可以定义更复杂的过滤判据，以便控制依照分类的选择性报告。例如，此类过滤判据可以限定只发送针对某些分类的报告，同时制止报告检测到的关于其他分类的网络异常，即使这些其他分类对应于预期行为。并且，此类过滤判据可以规定，对于某个分类来说，该报告应该与关于该分类的指示一起发送。更进一步，这种分类过滤判据可以用来定义哪个节点应该接收该报告，也就是依照分类来选择报告接收方。此外，该过滤判据还可以是可配置的，例如可以由一个或多个可能接收该报告的节点来配置，由此可以灵活控制哪个分类应该触发报告以及哪个分类不应该触发报告。

[0080] 在一些实施方式中，可以例如用消息208向用于检测网络异常的网络异常检测器提供反馈。该反馈也可以取决于分类的结果。在一些实施方式中，附加数据可以包括响应于先前检测和报告的网络异常而被接收的反馈。

[0081] 图9示出可用于实施上述概念的网络异常分析设备的示例性实施方式。作为示例，所示结构可用于实施网络异常分析器40的上述功能。

[0082] 在图示的示例中，该设备包括可用于与至少一个网络异常检测器、例如网络异常检测器30进行通信的检测器接口920。例如，检测器接口920可用于接收检测到的网络异常的指示。更进一步，检测器接口920可用于向网络异常检测器例如在消息208中提供反馈。此

外，该设备可以包括报告接口930。报告接口930可用于向诸如NOC之类的至少一个其他节点发送关于检测到的网络异常的报告。更进一步，报告接口930可用于接收来自此类其他节点的反馈信息，例如用于以后的相似网络异常分类的标签。

[0083] 更进一步，该设备包括与接口920、930耦合的一个或多个处理器950以及与一个或多个处理器950耦合的存储器960。存储器960可以包括诸如闪速ROM之类的只读存储器(ROM)，诸如动态RAM(DRAM)或静态RAM(SRAM)之类的随机存取存储器(RAM)，诸如硬盘或固态盘之类的大容量存储等等。存储器960包括适当配置的程序代码模块，其中该模块由一个或多个处理器950运行，以便实施如上所述的网络异常分析器40的功能。更具体地说，存储器960中的程序代码模块可以包括分析模块970，以便实施如上所述的用于分析异常模式的功能来对检测到的网络异常进行分类，例如通过模式匹配和/或与外部数据相关来分类。更进一步，存储器960中的程序代码模块可以包括报告模块980，以便实施如上所述的有选择地发送关于检测到的网络异常的报告的功能。更进一步，该存储器960可以包括用于存储异常模式或异常模型的异常数据库990。相应地，该设备还可以集成异常数据库50的功能性。

[0084] 应该理解的是，图9所示的结构仅仅是示意性的，并且该设备实际还可以包含为了清楚起见而未被图示的其他组件，例如其他接口或其他处理器。此外还应该理解，存储器960可以包括未图示的其他类型的程序代码模块，例如用于实施已知的模式分析功能、训练算法、近似算法和/或比较算法的程序代码模块。此外，在一些实施方式中还可以提供用于实施网络异常分析器40的功能的计算机程序，例如以存储了将要存入存储器960的程序代码模块的物理介质的形式来提供，或者通过致使所述程序代码可被下载来提供。

[0085] 可以看出的是，上述概念可用于有效地分析和报告网络异常。通过执行分类，可以排除非必要的报告以及虚假警报。网络异常分析器可以充当用于滤除检测到的可被视为非重要或不相关的网络异常的过滤器。更进一步，该分类处理可以提供能被包含在报告中的有价值的附加信息。此外，所示概念的这种分两个阶段的处理考虑了具有不同类型的网络异常检测器乃至多个网络异常检测器的模块化设计。

[0086] 应该理解的是，上述示例和实施例仅仅是说明性的，并且很容易对其进行各种修改。例如，这些概念可以与不同类型的通信网络一起使用，而不局限于这里述及的通信网络的示例。此外还应该理解，上述概念既可以使用由现有设备的一个或多个处理器运行并以相应的方式设计的软件来实施，也可以使用专用设备硬件来实施。并且，这里描述的网络异常分析器可以由单个设备或多个设备实施，例如设备云或协作设备系统。

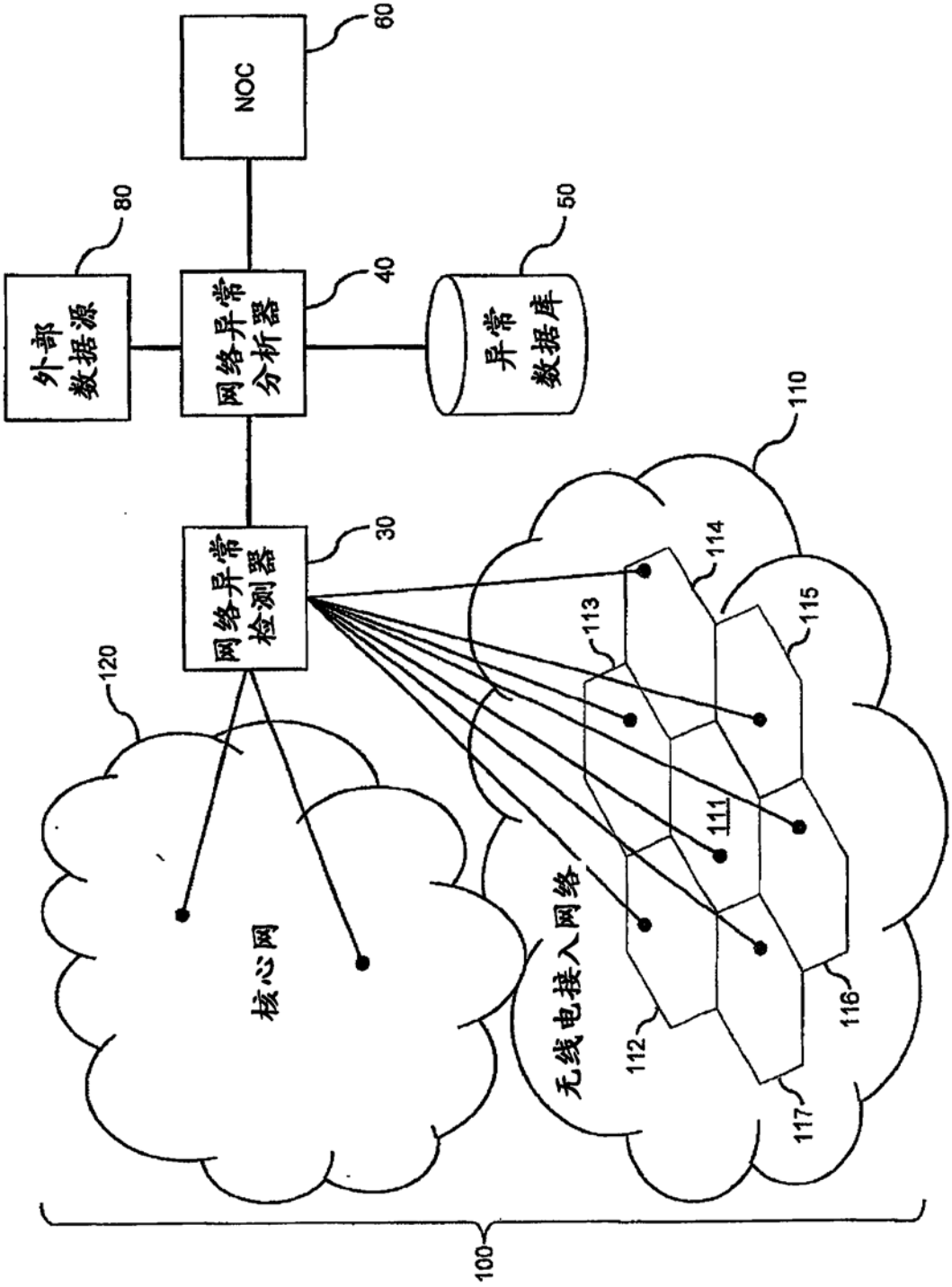

NOC
60
外部数据源
80
网络异常分析器
40
异常数据库
50
网络异常检测器
30
110
114
113
115
120
111
核心网
无线电接入网络
112
116
117
100

图1

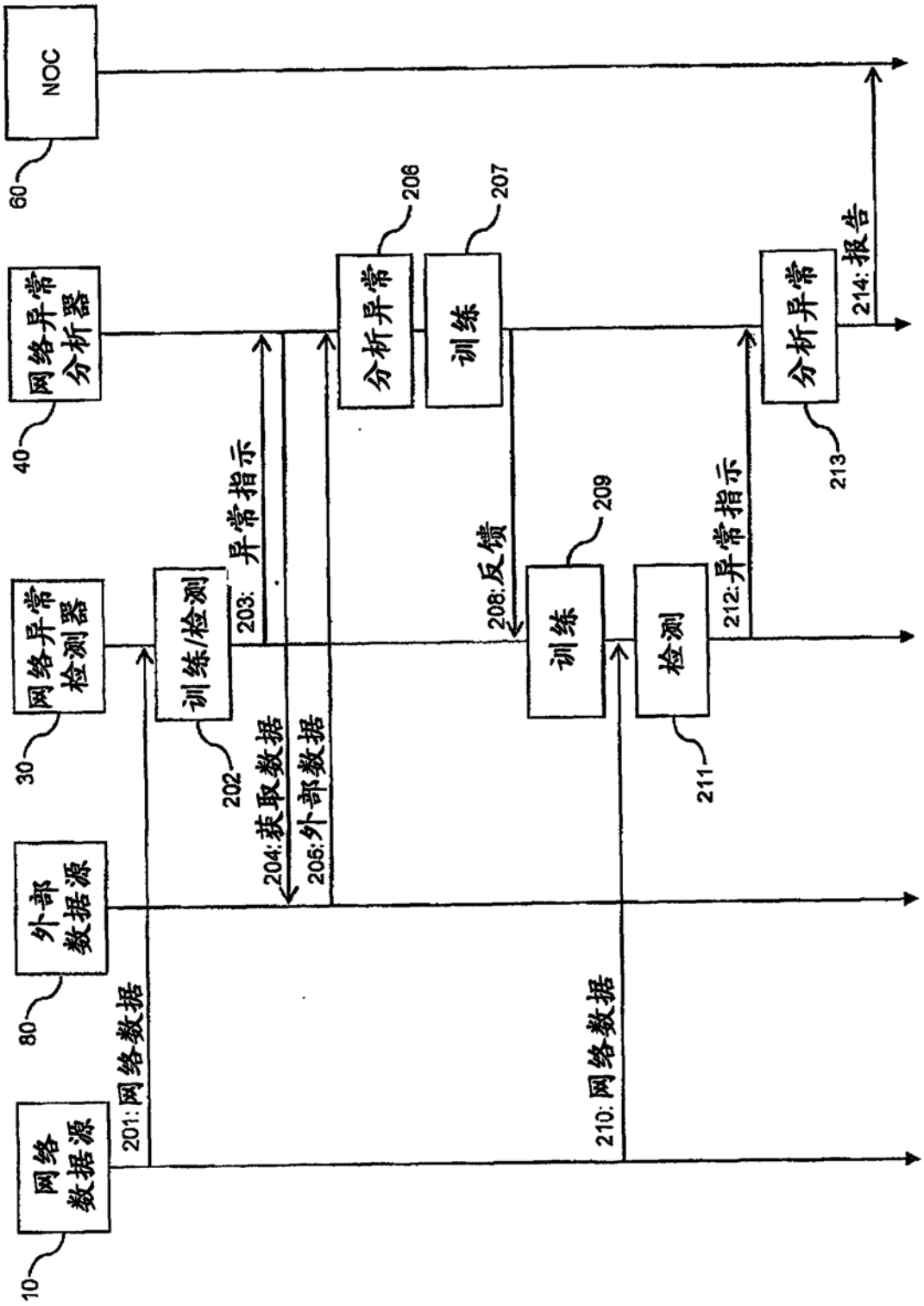

NOC
60
网络异常分析器
40
网络异常检测器
30
外部数据源
80
网络数据源
10
训练/检测
202
分析异常
206
训练
207
训练
209
检测
211
分析异常
213
201:网络数据
203:异常指示
204:获取数据
205:外部数据
208:反馈
210:网络数据
212:异常指示
214:报告

图2

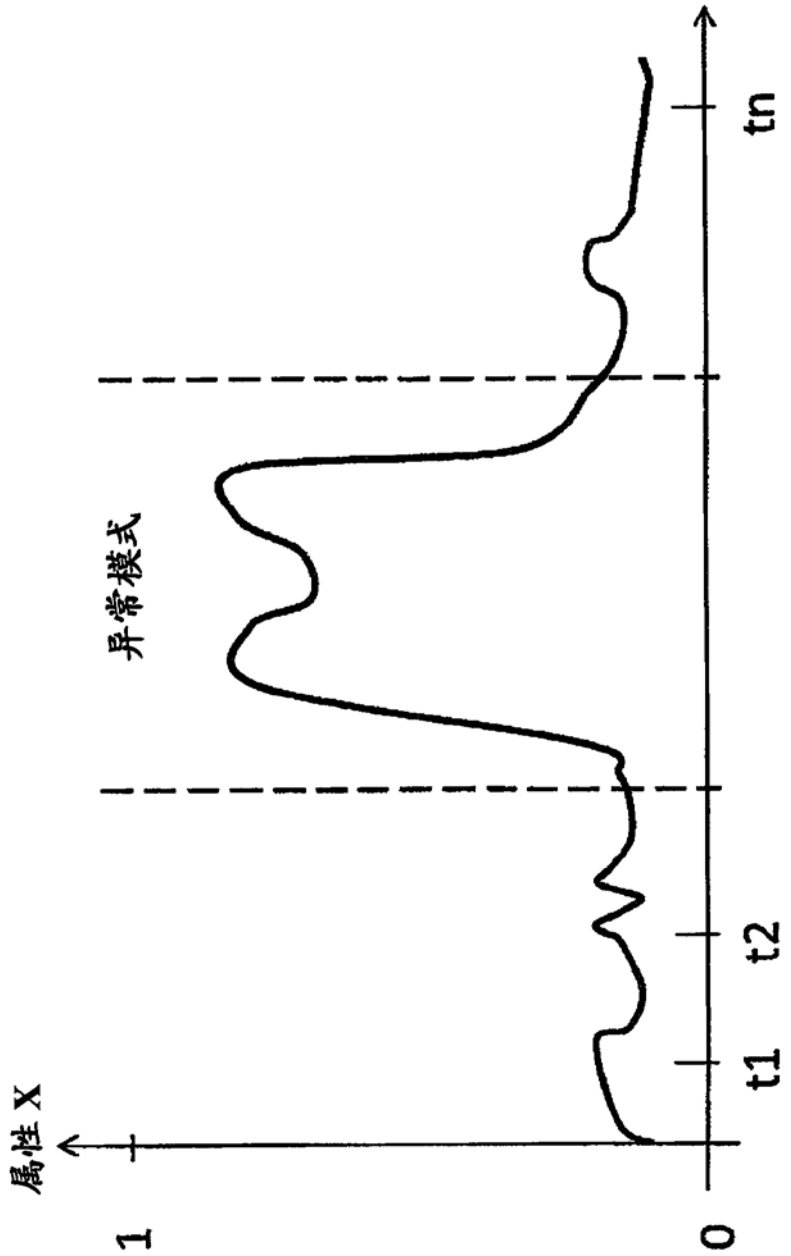


图3

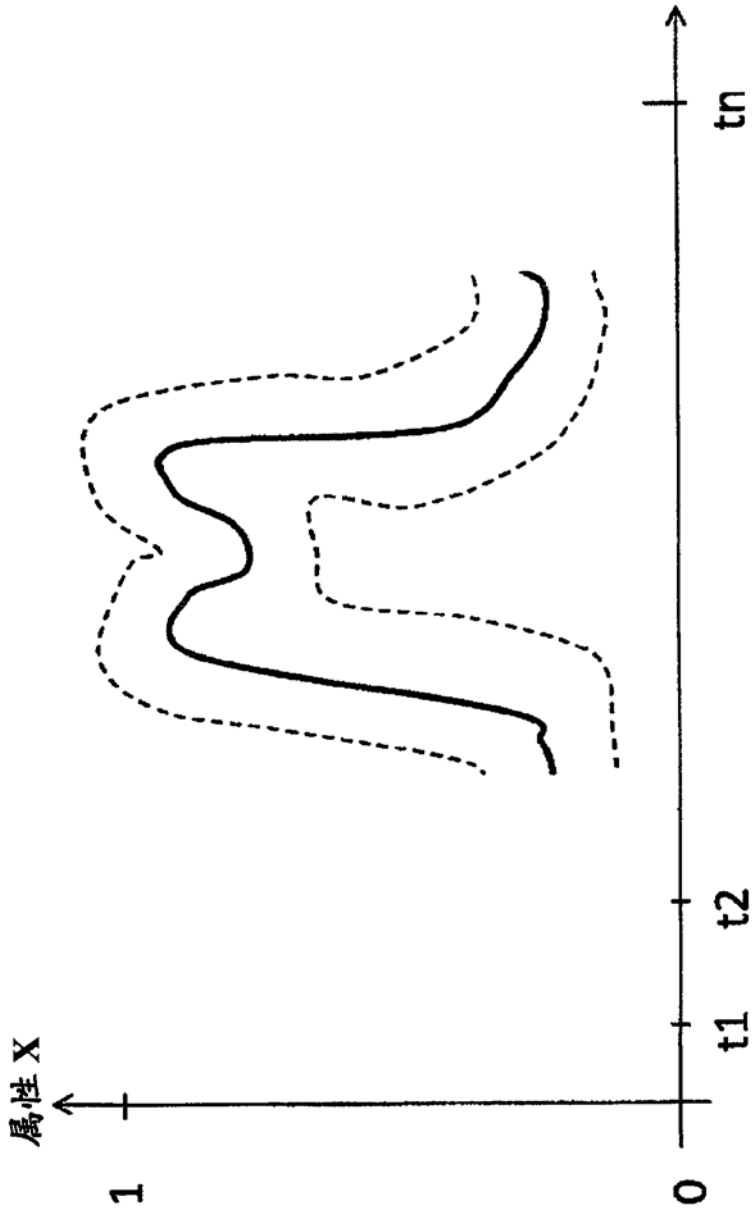


图4

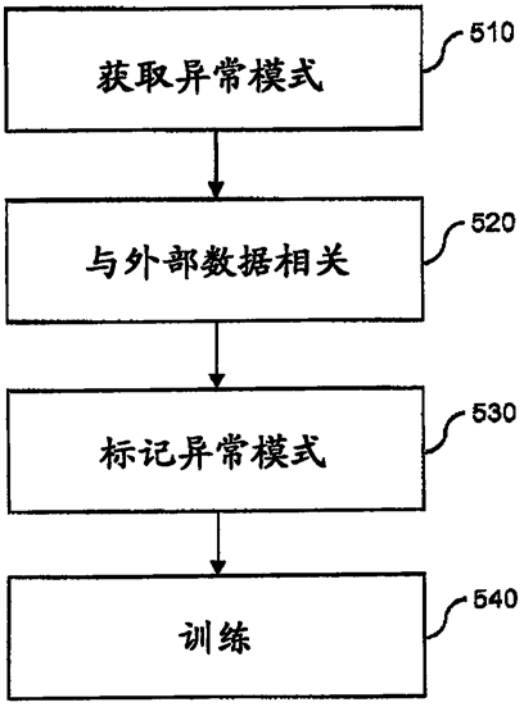


图5

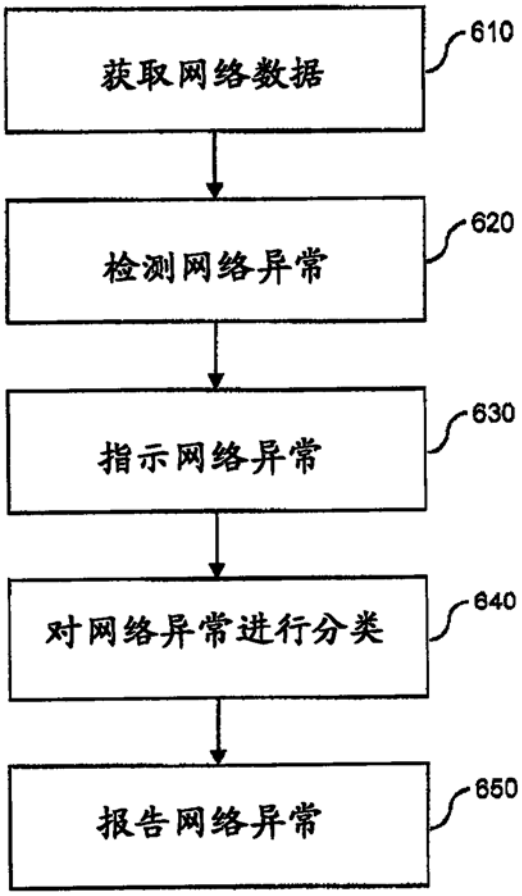


图6

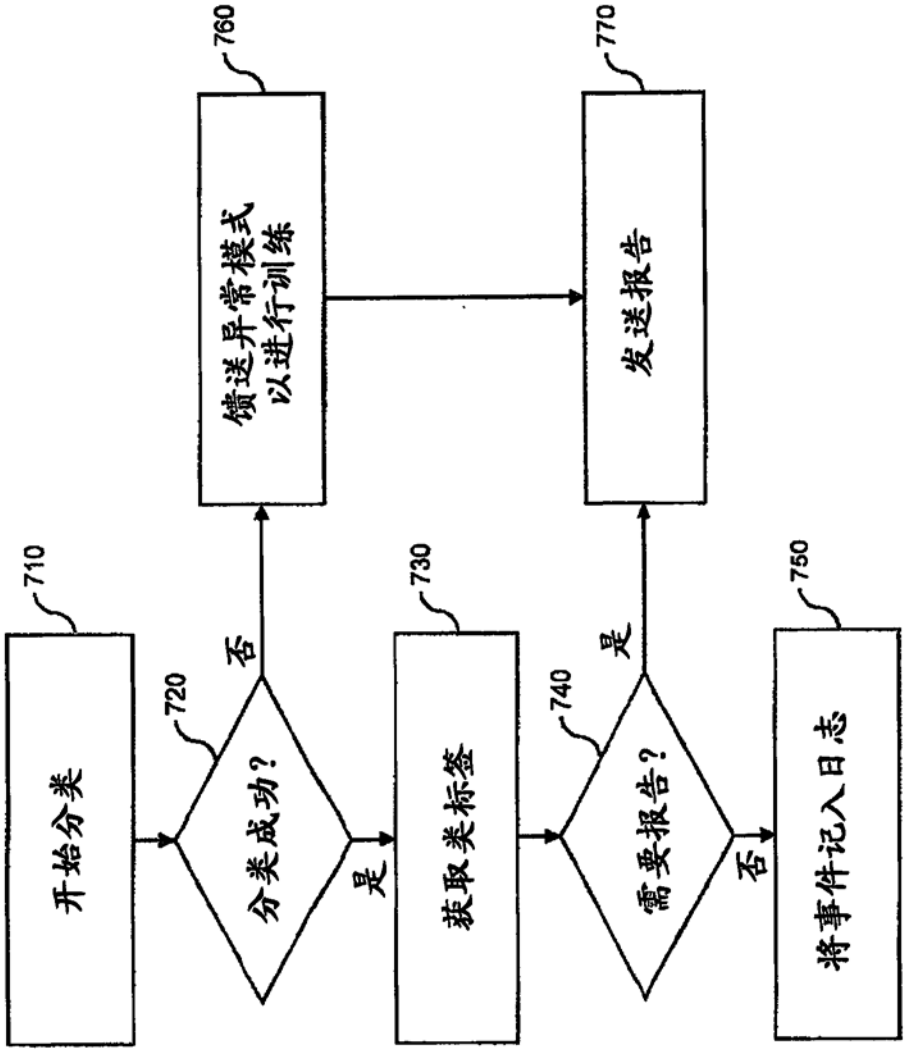

760
770
馈送异常模式以进行训练
发送报告
710
730
750
开始分类
720
否
分类成功?
是
获取类标签
740
是
需要报告?
否
将事件记入日志

图7

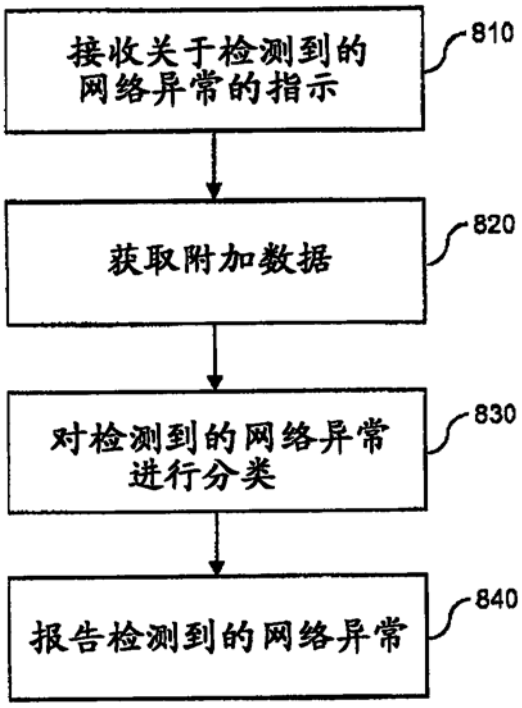

接收关于检测到的网络异常的指示
810
获取附加数据
820
对检测到的网络异常进行分类
830
报告检测到的网络异常
840

图8

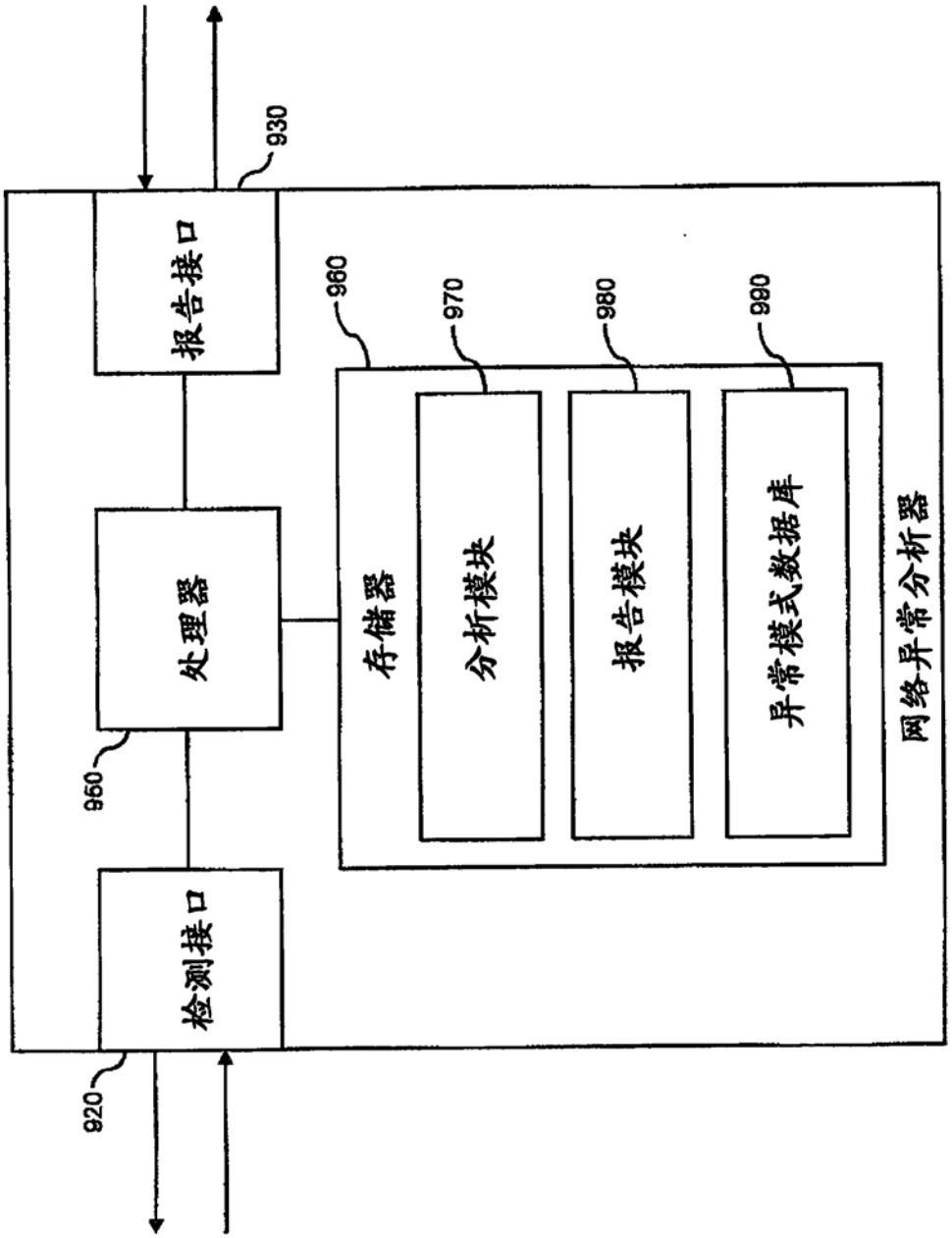

930
报告接口
960
970
980
990
处理器
存储器
分析模块
报告模块
异常模式数据库
网络异常分析器
960
检测接口
920

图9