(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
2022 年 1 月 20 日 (20.01.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/012490 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2021/105890

(22) 国际申请日: 2021 年 7 月 13 日 (13.07.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010688400.1 2020年7月16日 (16.07.2020) CN

(71) 申请人: 华为技术有限公司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 周艳 (**ZHOU, Yan**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 何承东 (**HE, Chengdong**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 林青春 (**LIN, Qingchun**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 深圳市深佳知识产权代理事务所 (普通合伙) (**SHENPAT INTELLECTUAL PROPERTY AGENCY**); 中国广东省深圳市罗湖区南湖街道春风路庐山大厦B座18C2、18D、18E、18E2, Guangdong 518001 (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,

(54) **Title:** TRUSTED COMMUNICATION METHOD AND RELATED APPARATUS

(54) 发明名称: 一种可信通信方法以及相关装置

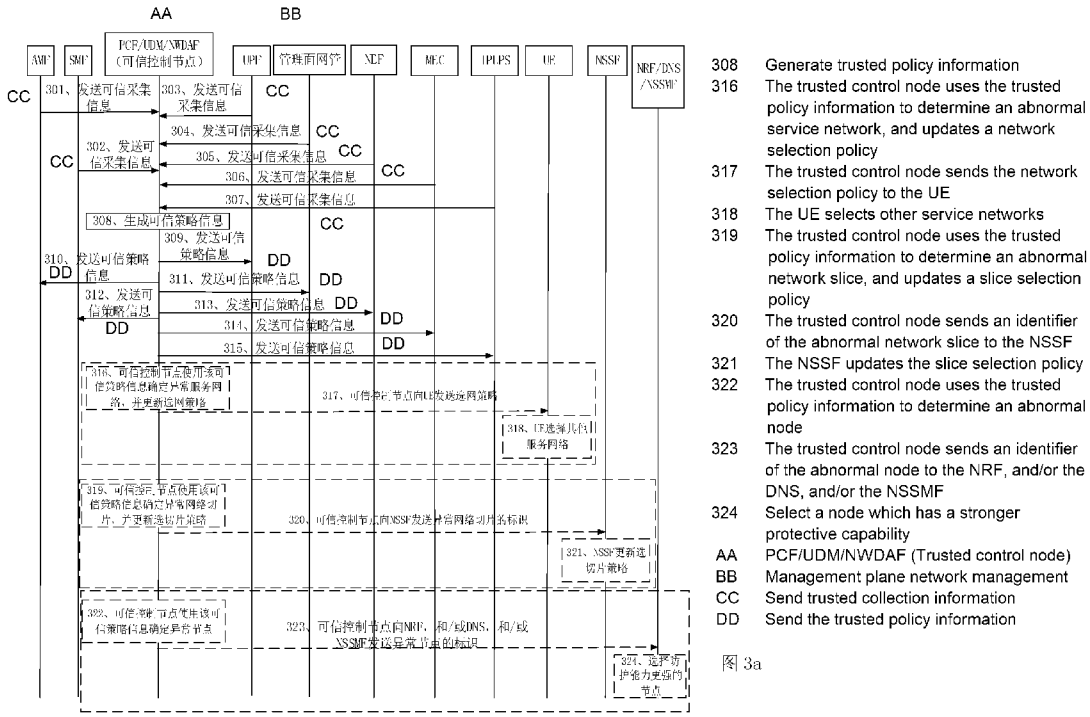


图 3a

(57) **Abstract:** Disclosed in embodiments of the present application is a trusted communication method. A core network device (e.g. a session management function (SMF), an access and mobility management function (AMF) and/or a user plane function (UPF)) can detect, by using trusted policy information, a non-access stratum (NAS) message which flows through the core network device, and/or, whether user data is abnormal; and when the NAS message is detected, and/or, it is detected that the user data is abnormal, the NAS message and/or a service corresponding to the user data can be reported and/or stopped, and abnormal information reporting signaling

[见续页]

WO 2022/012490 A1

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, 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)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

can be reported to a trusted control node (an independent network function entity, an existing control network element, or an existing management network element), such that the trusted control node updates the trusted policy information in a timely manner, and/or notifies each network element to use a trusted protective behavior. The security of a communication system is thus effectively improved.

(57) 摘要：本申请实施例公开了一种可信通信方法，核心网设备(例如会话管理功能SMF、接入和移动管理功能AMF和/或用户面功能UPF)使用可信策略信息，可以检测流经核心网设备的非接入层NAS消息，和/或，用户数据是否异常。当检测该NAS消息，和/或，用户数据为异常时，可以通报和/或阻止该NAS消息，和/或，用户数据对应的业务，并向可信控制节点(独立网络功能实体、或现有控制网元、或现有管理网元)上报异常信息通报信令。以便可信控制节点及时更新可信策略信息，和/或通知各网元采取可信防护行为。有效提升了通信系统的安全性。

一种可信通信方法以及相关装置

本申请要求于 2020 年 07 月 16 日提交中国专利局、申请号为 202010688400.1、发明名称为“一种可信通信方法以及相关装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及通信技术领域，尤其涉及一种可信通信方法以及相关装置。

背景技术

随着无线通信技术的快速发展，第五代(Fifth Generation，5G)移动通信网络(简称 5G 网络)应运而生。传统的通信网络中，按照安全域进行隔离，使用防火墙来防护不同安全域的边界。

以网络切片(Network Slice，NS)为例。在 5G 网络中，为了满足不同客户(如业务提供商或者租户)的业务需求，提出了 NS 的概念。其中，NS 是一个用于支持特定网络能力与网络特性的逻辑隔离的网络，可以提供端到端(end to end，E2E)的网络服务。例如，终端(user equipment，UE）可以向网络切片发送携带有终端的身份信息(如：用户永久标识(Subscription Permanent Identifier，SUPI))的请求消息，请求网络切片中的网络功能(Network Function，NF)为终端建立承载在网络切片上的协议数据单元(protocol data unit，PDU)会话(Session)，使终端通过 PDU session 接入数据网络(data network，DN)。

不同的网络切片属于不同的安全域，当风险来自同一安全域内（防火墙内），则防火墙无法起到防护作用。当防火墙被穿透，则防火墙同样无法起到防护作用。因此，需要一种新的可信通信方法保护通信网络。

发明内容

本申请实施例提供了一种可信通信方法，以期提升网络设备的通信安全性能。

第一方面，本申请实施例提出一种可信通信方法，包括：

会话管理功能 SMF 接收非接入层 NAS 消息；

该 SMF 获取可信策略信息；

根据该可信策略信息，该 SMF 检测该 NAS 消息是否异常；

若异常，则该 SMF 通报和/或阻止该 NAS 消息，和/或，向可信控制节点上报异常信令，和/或，向接入和移动管理功能 AMF 上报该异常信令，该异常信令包括该 NAS 消息中的全部或部分、或异常规则判断信息；

若正常，则 SMF 正常执行该 NAS 消息。

本申请实施例中，将可信控制节点从各个网络功能（还包括无线接入网设备 RAN、终端设备 UE、公共陆地移动通信网络间用户面安全功能 IPUPS 和/或移动边缘计算设备 MEC）采集的信息称为可信采集信息。

下面，对可信采集信息和可信策略信息分别进行描述：

1、可信采集信息：

可信采集信息包括：异常信令，和/或异常数据，和/或异常规则判断信息。异常信令包括异常的NAS消息的部分或全部，和/或异常的基于服务的架构（Service Based Architecture，SBA）接口消息的部分或全部，和/或异常的N2接口消息的部分或全部，和/或异常的N4接口消息的部分或全部；异常数据包括异常的用户数据的部分或全部；异常规则判断信息为：网络功能根据异常信令和/或异常数据生成的判断规则，该异常规则判断信息可以作为可信策略信息的一部分。

本申请实施例中，将可信控制节点从各个网络功能（还包括RAN、UE、IPUPS和/或MEC）采集的信息称为可信采集信息。可信采集信息包括但不限于：

全球唯一临时UE标识（Globally Unique Temporary UE Identity，GUTI），用户密封标识（Subscription Concealed Identifier，SUCI），用户永久标识（Subscription Permanent Identifier，SUPI），服务质量（Quality of Service，QoS）参数，终端设备互联网协议地址（UE Internet Protocol Address），协议数据单元会话标识（PDU Session ID），核心网隧道信息（CN tunnel info），和/或，接入网隧道信息（AN tunnel info）等，还可以是终端设备的数据吞吐量，和/或终端设备的定位信息等、注册类型（registration type），最近访问的跟踪区域标识（last visited TAI），请求的网络切片选择辅助信息（Requested NSSAI），请求的网络切片选择辅助信息（Mapping Of Requested NSSAI），协议数据单元会话状态（PDU Session status），选择的数据网络名称（selected DNN），用户设备请求的数据网络名称（UE requested DNN），AMF标识（AMF ID），PCF标识（PCF ID），用户位置信息（User location information），无线接入类型（RAT Type），通用公共签约标识（GPSI），本地区域数据网络服务区域中的用户位置（UE presence in LADN service area），单一的网络切片选择辅助信息（S-NSSAI(s)），请求的协议数据单元会话状态会话类型（Request PDU Session type），小数据速率控制状态（Small Data Rate Control Status），服务质量规则（QoS Rule(s)）和服务质量流级别（QoS Flow level）。源IP（ source IP）、目标IP（destination IP）、 源端口（source port）、目标端口（destination port）、传输控制协议（TCP）、用户数据协议（UDP）和/或流控制传输协议（SCTP）。

可信采集信息根据来源网络功能的不同，存在一定差异，此处不做限定。

2、可信策略信息：

本申请实施例中，可信控制节点采集可信采集信息后，根据这些可信采集信息，生成可信策略信息。该可信策略信息用于检测通信系统中交互的信令和/或用户数据，是否安全可信。示例性的：当终端设备在一定时间内数据吞吐量较大时，确定该终端设备处于异常。例如：终端设备为物联网设备（例如是水表），可信控制节点根据采集到的可信策略信息，确定该水表在每个月1号上传数据。当该水表在其他时间段上传大量数据，则可信控制节点确定该水表处于异常；

当终端设备在一定时间内向未被授权的切片发送大量访问请求，则确定该终端设备处于异常。

可信控制节点采集可信采集信息后，根据这些可信采集信息，生成可信策略信息。该可信策略信息用于检测通信系统中交互的信令和/或用户数据，是否安全可信。

SMF 使用可信策略信息，可以检测流经 SMF 的 NAS 消息是否异常。当检测该 NAS 消息为异常时，可以通报和/或阻止该 NAS 消息，并向可信控制节点（和/或 AMF）上报异常信令。以便可信控制节点及时更新可信策略信息。有效提升了通信系统的安全性。

结合第一方面，在第一方面的一种可选的实现方式中，该 SMF 从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

本申请实施例中，可信控制节点可以是独立的网络功能节点，也可以与 PCF、UDM 或 NWDAF 中至少一个网络功能节点合设。SMF 可以通过多种不同的网络功能节点（与可信控制节点合设的 PCF、UDM 或 NWDAF）获取可信策略信息。提升了方案的实现灵活性。

结合第一方面，在第一方面的一种可选的实现方式中，该 SMF 获取该可信策略信息，包括：

该 SMF 接收用户面功能 UPF 发送的用户面异常信息；

该 SMF 根据该用户面异常信息，生成该可信策略信息。

本申请实施例中，SMF 还可以接受用户面功能 UPF 发送的用户面异常信息，该用户面异常信息可以是 UPF 使用可信策略信息对接收到的用户数据进行检测，当用户数据为异常时，UPF 根据该异常数据，生成用户面异常信息；

该用户面异常信息也可以是，由管理面网管根据 UPF 上报的异常数据生成的相关信息。具体的，一种可选的实现方式中，该 UPF 统计一段时间内检测的异常数据后，将这些异常数据上报至管理面网管。在另一种可选的实现方式中，该 UPF 实时向管理面网管上报检测到的异常数据。或 UPF 根据 AI 的在线识别模式，根据用户面实时信息来判断是否存在异常，该用户面实时信息包括但不限于流行为模式、或包长、或包头信息、或海量连接指向同一地址等。管理面网管接收到这些异常数据后，对异常数据进行统计分析，生成用户面异常信息。管理面网管可以向 SMF 或可信控制节点发送该用户面异常信息。该用户面异常信息用于更新可信策略信息。

SMF 根据该用户面异常信息，可以生成可信策略信息；也可以使用该用户面异常信息，更新存储于本地的可信策略信息。SMF 可以根据来自 UPF 的用户面异常信息，生成可信策略信息。提升了方案的实现灵活性。

第二方面，本申请实施例提出一种可信通信方法，包括：

接入和移动管理功能 AMF 接收非接入层 NAS 消息；

该 AMF 获取可信策略信息；

根据该可信策略信息，该 AMF 检测该 NAS 消息是否异常；

若异常，则该 AMF 通报和/或阻止该 NAS 消息，和/或，向该可信控制节点上报异常信令，该异常信令包括该 NAS 消息中的全部或部分。

本申请实施例中，与第一方面类似的，AMF 使用可信策略信息，可以检测流经 AMF 的 NAS 消息是否异常。当检测该 NAS 消息为异常时，可以通报和/或阻止该 NAS 消息，并向可信控制节点上报异常信令。以便可信控制节点及时更新可信策略信息。有效提升了通信系统的安全性。

结合第二方面，在第二方面的一种可选的实现方式中，该 AMF 获取该可信策略信息，包括：

该 AMF 从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

本申请实施例中，可信控制节点可以是独立的网络功能节点，也可以与 PCF、UDM 或 NWDAF 中至少一个网络功能节点合设。AMF 可以通过多种不同的网络功能节点（与可信控制节点合设的 PCF、UDM 或 NWDAF）获取可信策略信息。提升了方案的实现灵活性。

结合第二方面，在第二方面的一种可选的实现方式中，该 AMF 获取该可信策略信息，包括：

该 AMF 接收会话管理功能 SMF 发送的该异常信令；

该 AMF 根据该异常信令，生成该可信策略信息。

本申请实施例中，AMF 根据来自 SMF 的异常信令，可以生成可信策略信息；也可以使用该异常信令，更新存储于本地的可信策略信息。AMF 可以根据来自 SMF 的异常信令，生成可信策略信息。提升了方案的实现灵活性。

结合第二方面，在第二方面的一种可选的实现方式中，该 AMF 向该可信控制节点上报该异常信令，包括：

该 AMF 向该 NWDAF 发送该异常信令；

该 NWDAF 向该可信控制节点上报该异常信令。

本申请实施例中，当可信控制节点与 NWDAF 相互独立时，AMF 可以通过 NWDAF 向可信控制节点上报异常信令。以便可信控制节点及时更新可信策略信息。有效提升了通信系统的安全性。

第三方面，本申请实施例提出一种可信通信方法，包括：

用户面功能 UPF 接收用户数据；

该 UPF 获取可信策略信息；

根据该可信策略信息，该 UPF 检测该用户数据是否异常；

若异常，则该 UPF 通报和/或阻止该用户数据对应的业务，和/或，向该可信控制节点上报异常数据，和/或，向管理面网管上报该异常数据，该异常数据包括该用户数据，和/或，向会话管理功能 SMF 上报该异常数据，该异常数据包括该用户数据。

本申请实施例中，与前述第一方面或第二方面类似的，UPF 使用可信策略信息，可以检测流经 UPF 的用户数据是否异常。当检测该用户数据为异常时，可以通报和/或阻止该用户数据对应的业务，并向可信控制节点上报异常数据。以便可信控制节点及时更新可信策略信息。有效提升了通信系统的安全性。

结合第三方面，在第三方面的一种可选的实现方式中，该 UPF 获取可信策略信息，包括：

该 UPF 从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

本申请实施例中，可信控制节点可以是独立的网络功能节点，也可以与 PCF、UDM 或

NWDAF 中至少一个网络功能节点合设。UPF 可以通过多种不同的网络功能节点（与可信控制节点合设的 PCF、UDM 或 NWDAF）获取可信策略信息。提升了方案的实现灵活性。

结合第三方面，在第三方面的一种可选的实现方式中，还包括：

该 UPF 接收该管理面网管和/或该 SMF 发送的用户面异常信息，该用户面异常信息由该管理面网管和/或该 SMF 根据该异常数据生成；

该 UPF 根据该用户面异常信息，生成该可信策略信息。

本申请实施例中，UPF 接收管理面网管发送的用户面异常信息，和/或，UPF 接收 SMF 发送的用户面异常信息。

该用户面异常信息可以是 UPF 使用可信策略信息对接收到的用户数据进行检测，当用户数据为异常时，UPF 根据该异常数据，生成用户面异常信息；该用户面异常信息还可以是 SMF 根据异常信令生成的相关信息；该用户面异常信息也可以是，由管理面网管根据 UPF 上报的异常数据生成的相关信息。具体的，一种可选的实现方式中，该 UPF 统计一段时间内检测的异常数据后，将这些异常数据上报至管理面网管。在另一种可选的实现方式中，该 UPF 实时向管理面网管上报检测到的异常数据。检测方法中可以包含 AI 技术。管理面网管接收到这些异常数据后，对异常数据进行统计分析，生成用户面异常信息。管理面网管可以向 SMF 或可信控制节点发送该用户面异常信息。该用户面异常信息用于更新可信策略信息。

UPF 根据该用户面异常信息，可以生成可信策略信息；也可以使用该用户面异常信息，更新存储于本地的可信策略信息。UPF 可以根据用户面异常信息，生成可信策略信息。提升了方案的实现灵活性。

结合第三方面，在第三方面的一种可选的实现方式中，该 UPF 向该可信控制节点上报该异常信令，包括：

该 UPF 向该 NWDAF 发送该异常数据；

该 NWDAF 向该可信控制节点上报该异常数据。

本申请实施例中，当可信控制节点与 NWDAF 相互独立时，UPF 可以通过 NWDAF 向可信控制节点上报异常信令。以便可信控制节点及时更新可信策略信息。有效提升了通信系统的安全性。

第四方面，本申请实施例提出一种可信通信方法，包括：

会话管理功能 SMF 接收异常基站信息；

该 SMF 获取可信策略信息；

该 SMF 根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力高于第二 UPF，该第二 UPF 用于当前处理该异常基站的数据。

具体的，首先，第二 UPF 使用可信策略信息，检测该基站是否异常。示例性的，检测一段统计时间内该基站中异常信令的数量，和/或，异常数据的数量大于某一阈值时，确定该基站为异常基站。示例性的，在 24 小时内，当某一基站中累计异常信令数量大于 30 时，确定该基站为异常基站。

其次，第二 UPF 向可信控制节点发送异常基站信息。示例性的，异常基站信息例如：

该异常基站的互联网协议 IP 地址等。

再次，SMF 接收该异常基站信息。SMF 获取该可信策略信息。当 SMF 确定存在异常基站时，SMF 确定第一 UPF，该第一 UPF 的防护能力（或称为安全性能）高于第二 UPF。并使用该第一 UPF 处理该异常基站的相关数据。其次，SMF 删除第二 UPF 的数据，包括但不限于：SMF 释放第二 UPF 上的资源。

具体的，SMF 可以通过网络仓库功能 NRF 或者网络切片选择功能 NSSF，选择防护能力较高的 UPF，作为第一 UPF。NRF 或 NSSF 中存储各个 UPF 的可信等级（或防护能力）。

本申请实施例中，核心网设备（SMF）可以确定基站是否异常。当基站为异常基站时，SMF 确定防护能力更高的第一 UPF。进而使用防护能力更高的 UPF 处理该基站的相关数据。提升了通信的安全性。

结合第四方面，在第四方面的一种可选的实现方式中，该 SMF 根据该可信策略信息确定该第一 UPF 后，还包括：

该 SMF 指示该第一 UPF 处理该异常基站的数据；

该 SMF 指示该第二 UPF 删除该异常基站的数据。

本申请实施例中，SMF 具体指示可信等级更高的第一 UPF 处理该异常基站的数据，SMF 还可以指示第二 UPF(原 UPF)删除该异常基站的数据，以便该第二 UPF 继续处理其他数据。

结合第四方面，在第四方面的一种可选的实现方式中，该 SMF 接收该第一异常基站信息，包括：

该 SMF 从接入和移动管理功能 AMF、UPF 或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个，接收该异常基站信息。

本申请实施例中，SMF 可以通过多种途径，接收该异常基站信息。

结合第四方面，在第四方面的一种可选的实现方式中，该 SMF 获取该可信策略信息，包括：

该 SMF 从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

本申请实施例中，可信控制节点可以是独立的网络功能节点，也可以与 PCF、UDM 或 NWDAF 中至少一个网络功能节点合设。SMF 可以通过多种不同的网络功能节点（与可信控制节点合设的 PCF、UDM 或 NWDAF）获取可信策略信息。提升了方案的实现灵活性。

第五方面，本申请实施例提出一种可信通信方法，包括：

会话管理功能 SMF 获取可信策略信息；

该 SMF 接收异常用户设备信息或异常归属网络信息，其中，该异常用户设备归属于该异常归属网络；

如果该异常归属网络中该异常用户设备的数量超过第一阈值，

该 SMF 根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力高于第二 UPF，该第二 UPF 用于当前处理该异常归属网络的数据。

本申请实施例中，首先，第二 UPF 使用可信策略信息检测归属网络中各个用户设备是

否异常。检测方式包括但不限于：检测用户设备的数据，和/或，检测用户设备在一段时间内的访问目的地与访问次数，和/或，检测用户设备在一段时间内的数据流量，和/或，检测用户设备在一定时间内的移动距离。示例性的，当一段时间内，用户设备访问未经允许的网络切片的访问次数，达到某一阈值。则第二 UPF 确定该用户设备为异常用户设备。

可信控制节点（或第二 UPF）统计该异常用户设备信息对应的归属网络中异常用户设备的总数。当一段统计时间内该异常用户设备的数量超过第一阈值，则可信控制节点确定该归属网络为异常归属网络。

当 SMF 确定存在异常归属网络时，SMF 确定第一 UPF，该第一 UPF 的防护能力（或称为安全性能）高于第二 UPF，并使用该第一 UPF 处理该异常归属网络的相关数据。其次， SMF 删除第二 UPF 的数据，包括但不限于：SMF 释放第二 UPF 上的资源。

结合第五方面，在第五方面的一种可选的实现方式中，该 SMF 根据该可信策略信息确定该第一 UPF 后，还包括：

该 SMF 指示该第一 UPF 处理该异常归属网络的数据；

该 SMF 指示该第二 UPF 删除该异常归属网络的数据。

本申请实施例中，核心网设备（SMF）可以根据异常用户设备信息或异常归属网络信息，确定是否存在异常归属网络。当异常归属网络时，SMF 确定防护能力更高的第一 UPF。进而使用防护能力更高的 UPF 处理该异常归属网络的相关数据。提升了通信的安全性。

结合第五方面，在第五方面的一种可选的实现方式中，该 SMF 接收该异常用户设备信息或该异常归属网络信息，包括：

该 SMF 从接入和移动管理功能 AMF、该第二 UPF，或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个，接收该异常用户设备信息或该异常归属网络信息。

本申请实施例中，SMF 具体指示防护能力更高的第一 UPF 处理该异常归属网络的数据，SMF 还可以指示第二 UPF（原 UPF）删除该异常归属网络的数据，以便该第二 UPF 继续处理其他数据。

结合第五方面，在第五方面的一种可选的实现方式中，该 SMF 获取该可信策略信息，包括：

该 SMF 从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

本申请实施例中，可信控制节点可以是独立的网络功能节点，也可以与 PCF、UDM 或 NWDAF 中至少一个网络功能节点合设。SMF 可以通过多种不同的网络功能节点（与可信控制节点合设的 PCF、UDM 或 NWDAF）获取可信策略信息。提升了方案的实现灵活性。

第六方面，本申请实施例提出一种可信通信方法，包括：

可信控制节点从接入和移动管理功能 AMF、会话管理功能 SMF、用户面功能 UPF、管理面网管、网络能力开放功能实体 NEF、多接入边缘计算设备 MEC 或，公共陆地移动通信网络间用户面安全功能 IPUPS 中的至少一个，获取可信采集信息；

该可信控制节点根据该可信采集信息，确定可信策略信息；

该可信控制节点该 AMF、该 SMF、该 UPF、该管理面网管、该 NEF、该 MEC 或，该 IPUPS 中的至少一个，发送该可信策略信息。

本申请实施例中，可信控制节点可以获取通信系统中多个网络功能的可信采集信息，并根据该可信采集信息生成可信策略信息。然后，可信控制节点向多个网络功能下发该可信策略信息，以便这些网络功能使用该可信策略信息检测交互的数据和/或信令等。可以有效提升通信系统的安全性。

具体的，该可信控制节点通过该 NEF 接收该 MEC 发送的该可信采集信息；

该可信控制节点通过该 NEF 向该 MEC 发送该可信策略信息；

和/或，该可信控制节点通过该 UPF 接收该 MEC 发送的该可信采集信息；

该可信控制节点通过该 UPF 向该 MEC 发送该可信策略信息。

该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个。

结合第六方面，在第六方面的一种可选的实现方式中，还包括：

该可信控制节点根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常服务网络；

该可信控制节点向 PCF 或 UDM 发送该异常服务网络的标识，以使该 PCF 或 UDM 更新选网策略中该异常服务网络的标识的优先级，并向终端设备发送该选网策略。

和/或，

该可信控制节点根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常网络切片；

该可信控制节点向切片选择功能 NSSF 发送该异常网络切片的标识，以使该 NSSF 更新选切片策略中该异常网络切片的标识的优先级。和/或，该可信控制节点通知接入和移动管理功能 AMF 和/或会话管理功能 SMF 选择防护能力更强的其他网络切片；

和/或，

该可信控制节点根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常节点；

该可信控制节点向网络仓库功能 NRF、网域名称服务器（Domain Name Server，DNS）、SMF、网络切片管理功能（Network Slice Subnet Management Function，NSSMF）、其它网络功能中的至少一个发送该异常节点的标识，以使该 NRF、DNS、SMF、NSSMF、其它网络功能中的至少一个选择防护能力更强的节点（该节点例如 AMF 或 UPF 等）。和/或，该可信控制节点通知其他网络功能选择防护能力更强的节点（例如通知 SMF 选择防护能力更强的 UPF）。例如：可信控制节点向 NRF 发送 UPF1 为异常节点，NRF 更新配置后（比如降低 UPF1 的优先级），NRF 通知 SMF 选择防护能力更强的 UPF2。

如下以可信控制节点更新选网策略为例进行说明。

具体的，可信控制节点根据可信策略信息，或，根据可信策略信息和可信采集信息，确定异常服务网络。该异常服务网络为，存在异常用户数量大于某一阈值的服务网络。示例性的，当某一服务网络中服务的异常用户一段统计时间内数量大于 M(M 为正整数)时，可

信控制节点确定该服务网络为异常服务网络。或者，可信控制节点检测某一服务网络的一段统计时间内流量水平显著超过历史水平 100 倍时，可信控制节点确定该服务网络为异常服务网络、或网络切片异常。

当可信控制节点确定异常服务网络后，记录该异常网络切片、或该异常服务网络的标识，在漫游接入场景下，该异常服务网络的标识可以是服务-公共陆地移动网标识（serving plmn ID）。然后根据该异常服务网络的标识，更新选网策略。

可选的，该选网策略由一个或多个异常服务网络的标识组成，选网策略中记录的异常服务网络的标识为黑名单。

可选的，该选网策略由一个或多个异常服务网络的标识组成，选网策略中记录的异常服务网络的标识为低优先级。

终端设备接收该选网策略后，更新本地存储的选网策略。根据该选网策略选择其他服务网络，避免终端设备选择异常服务网络，以提升终端设备的通信安全性。

当判断切片异常时，则通知运营方生成新的正常切片、或者启用另外的正常服务切片。

第七方面，本申请实施例提出一种可信通信方法，包括：

核心网设备接收非接入层 NAS 消息、和/或用户数据，核心网设备可以包括 NEF、DNS、NWDAF、UDM、PCF、AMF、或 SMF 等，还可以包括网络切片选择功能(network slice selection function，NSSF)等网络功能节点；

该核心网设备获取可信策略信息；

根据该可信策略信息，该核心网设备检测该 NAS 消息和/或该用户数据是否异常；

若异常，则该核心网设备通报和/或阻止该 NAS 消息、和/或该用户数据对应的业务。

本申请实施例中，将可信控制节点从各个网络功能（还包括无线接入网设备 RAN、终端设备 UE、公共陆地移动通信网络间用户面安全功能 IPUPS 和/或移动边缘计算设备 MEC）采集的信息称为可信采集信息。可信采集信息包括但不限于：全球唯一临时 UE 标识（Globally Unique Temporary UE Identity，GUTI），用户密封标识（Subscription Concealed Identifier，SUCI），用户永久标识（Subscription Permanent Identifier，SUPI），服务质量（Quality of Service，QoS）参数，终端设备互联网协议地址（UE Internet Protocol Address），AMF 标识（AMF ID），PCF 标识（PCF ID），协议数据单元会话标识（PDU Session ID），核心网隧道信息（CN tunnel info），和/或，接入网隧道信息（AN tunnel info）等，还可以是终端设备的数据吞吐量，和/或终端设备的定位信息，或异常判断所需要的信息等。

可信控制节点采集可信采集信息后，根据这些可信采集信息，生成可信策略信息。该可信策略信息用于检测通信系统中交互的信令和/或用户数据，是否安全可信。示例性的：当终端设备的位置在短时间内移动距离较大时，确定该终端设备处于异常。例如，当终端设备在一定时间内数据吞吐量较大时，确定该终端设备处于异常。例如：终端设备为物联网设备（例如是水表），可信控制节点根据采集到的可信策略信息，确定该水表在每个月 1 号上传数据。当该水表在其他时间段上传大量数据，则可信控制节点确定该水表处于异常；当终端设备在一定时间内向未被授权的切片发送大量访问请求，则确定该终端设备处于异

常。

本申请实施例中，当核心网设备为 SMF 时，SMF 使用可信策略信息，可以检测流经 SMF 的 NAS 消息是否异常。当检测该 NAS 消息为异常时，可以通报和/或阻止该 NAS 消息，并向可信控制节点（和/或 AMF）上报异常信令。以便可信控制节点及时更新可信策略信息。有效提升了通信系统的安全性。当核心网设备为 AMF 时，AMF 使用可信策略信息，可以检测流经 AMF 的 NAS 消息是否异常。当检测该 NAS 消息为异常时，可以通报和/或阻止该 NAS 消息，并向可信控制节点上报异常信令。以便可信控制节点及时更新可信策略信息。有效提升了通信系统的安全性。当核心网设备为 UPF 时，UPF 使用可信策略信息，可以检测流经 UPF 的用户数据是否异常。当检测该用户数据为异常时，可以通报和/或阻止该用户数据对应的业务，并向可信控制节点上报异常数据。以便可信控制节点及时更新可信策略信息。有效提升了通信系统的安全性。

结合第七方面，在第七方面的一种可选的实现方式中，还包括：

该核心网设备记录异常信令，和/或，异常数据，该异常信令包括全部或部分的该 NAS 消息。

结合第七方面，在第七方面的一种可选的实现方式中，该核心网设备接收该非接入层 NAS 消息、和/或该用户数据，包括：

会话管理功能 SMF 接收该非接入层 NAS 消息，和/或，

接入和移动管理功能 AMF 接收该 NAS 消息，和/或，

用户面功能 UPF 接收该用户数据。

结合第七方面，在第七方面的一种可选的实现方式中，该核心网设备获取该可信策略信息，包括：

该核心网设备从可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

结合第七方面，在第七方面的一种可选的实现方式中，该核心网设备获取该可信策略信息，包括：

会话管理功能 SMF 接收用户面功能 UPF 发送的用户面异常信息，该用户面异常信息由该 UPF 根据该异常数据生成；

该 SMF 根据该用户面异常信息，生成该可信策略信息；

和/或，

接入和移动管理功能 AMF 接收该 SMF 发送的该异常信令；

该 AMF 根据该异常信令，生成该可信策略信息；

和/或，

该 UPF 接收管理面网管发送的该用户面异常信息；

该 UPF 根据该用户面异常信息，生成该可信策略信息。

第八方面，本申请实施例提出一种通信装置，包括：

收发器，用于接收非接入层 NAS 消息；

该收发器，还用于获取可信策略信息；

处理器，用于根据该可信策略信息，检测该 NAS 消息是否异常；

若异常，

该处理器，还用于通报和/或阻止该 NAS 消息，和/或，

该收发器，还用于向可信控制节点上报异常信令，和/或，

该收发器，还用于向接入和移动管理功能 AMF 上报该异常信令，该异常信令包括该 NAS 消息中的全部或部分。

结合第八方面，在第八方面的一种可能的实现方式中，

该收发器，具体用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

结合第八方面，在第八方面的一种可能的实现方式中，

该收发器，具体用于接收用户面功能 UPF 发送的用户面异常信息；

该处理器，具体用于根据该用户面异常信息，生成该可信策略信息。

第九方面，本申请实施例提出一种通信装置，包括：

收发器，用于接收非接入层 NAS 消息；

该收发器，还用于获取可信策略信息；

处理器，用于根据该可信策略信息，检测该 NAS 消息是否异常；

若异常，

该处理器，还用于通报和/或阻止该 NAS 消息，和/或，

该收发器，还用于向该可信控制节点上报异常信令，该异常信令包括该 NAS 消息中的全部或部分。

结合第九方面，在第九方面的一种可能的实现方式中，

该收发器，具体用于从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

结合第九方面，在第九方面的一种可能的实现方式中，

该收发器，具体用于接收会话管理功能 SMF 发送的该异常信令；

该收发器，具体用于根据该异常信令，生成该可信策略信息。

结合第九方面，在第九方面的一种可能的实现方式中，

该收发器，具体用于向该 NWDAF 发送该异常信令；

该收发器，具体用于向该可信控制节点上报该异常信令。

第十方面，本申请实施例提出一种通信装置，包括：

收发器，用于接收用户数据；

该收发器，还用于获取可信策略信息；

处理器，用于根据该可信策略信息，检测该用户数据是否异常；

若异常，

该处理器，还用于通报和/或阻止该用户数据对应的业务，和/或，

该收发器，还用于向该可信控制节点上报异常数据，和/或，

该收发器，还用于向管理面网管上报该异常数据，该异常数据包括该用户数据，和/或，

该收发器，还用于向会话管理功能 SMF 上报该异常数据，该异常数据包括该用户数据。

结合第十方面，在第十方面的一种可能的实现方式中，

该收发器，具体用于从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

结合第十方面，在第十方面的一种可能的实现方式中，

该收发器，还用于接收该管理面网管和/或该 SMF 发送的用户面异常信息，该用户面异常信息由该管理面网管和/或该 SMF 根据该异常数据生成；

该处理器，还用于根据该用户面异常信息，生成该可信策略信息。

结合第十方面，在第十方面的一种可能的实现方式中，

该收发器，还用于向该 NWDAF 发送该异常数据；

该收发器，还用于向该可信控制节点上报该异常数据。

第十一方面，本申请实施例提出一种通信装置，包括：

收发器，用于接收异常基站信息；

该收发器，还用于获取可信策略信息；

处理器，用于根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力高于第二 UPF，该第二 UPF 用于当前处理该异常基站的数据。

结合第十一方面，在第十一方面的一种可能的实现方式中，

该收发器，还用于指示该第一 UPF 处理该异常基站的数据；

该收发器，还用于指示该第二 UPF 删除该异常基站的数据。

结合第十一方面，在第十一方面的一种可能的实现方式中，

该收发器，具体用于从接入和移动管理功能 AMF、UPF 或网络数据分析功能 NWDAF 中的至少一个，接收该异常基站信息。

结合第十一方面，在第十一方面的一种可能的实现方式中，

该收发器，还用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

第十二方面，本申请实施例提出一种通信装置，包括：

收发器，用于获取可信策略信息；

该收发器，还用于接收异常用户设备信息或异常归属网络信息，其中，该异常用户设备归属于该异常归属网络；

如果该异常归属网络中该异常用户设备的数量超过第一阈值，

处理器，用于根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力

高于第二 UPF，该第二 UPF 用于当前处理该异常归属网络的数据。

结合第十二方面，在第十二方面的一种可能的实现方式中，

该收发器，还用于指示该第一 UPF 处理该异常归属网络的数据；

该收发器，还用于指示该第二 UPF 删除该异常归属网络的数据。

结合第十二方面，在第十二方面的一种可能的实现方式中，

该收发器，还用于从接入和移动管理功能 AMF、该第二 UPF，或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个，接收该异常用户设备信息或该异常归属网络信息。

结合第十二方面，在第十二方面的一种可能的实现方式中，

该收发器，还用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

第十三方面，本申请实施例提供了一种通信装置，包括：

收发器，还用于从策略控制功能 PCF、接入和移动管理功能 AMF、会话管理功能 SMF、用户面功能 UPF、管理面网管、网络能力开放功能实体 NEF、多接入边缘计算设备 MEC 或，公共陆地移动通信网络间用户面安全功能 IPUPS 中的至少一个，获取可信采集信息；

处理器，用于根据该可信采集信息，确定可信策略信息；

该收发器，还用于向该 AMF、该 SMF、该 UPF、该管理面网管、该 NEF、该 MEC 或，该 IPUPS 中的至少一个，发送该可信策略信息。

结合第十三方面，在第十三方面的一种可能的实现方式中，

该收发器，还用于通过该 NEF 接收该 MEC 发送的该可信采集信息；

该收发器，还用于通过该 NEF 向该 MEC 发送该可信策略信息；

和/或，

该收发器，还用于通过该 UPF 接收该 MEC 发送的该可信采集信息；

该收发器，还用于通过该 UPF 向该 MEC 发送该可信策略信息。

结合第十三方面，在第十三方面的一种可能的实现方式中，

该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个。

结合第十三方面，在第十三方面的一种可能的实现方式中，

该处理器，还用于根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常服务网络；

该收发器，还用于向策略控制功能 PCF 或统一数据管理 UDM 发送该异常服务网络的标识、或异常网络切片标识，以使该 PCF 或 UDM 更新选网策略中该异常服务网络或网络切片标识优先级，并向终端设备发送该选网策略。

和/或，

该处理器，还用于根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常网络切片；

该收发器，还用于向切片选择功能 NSSF 发送该异常网络切片的标识，以使该 NSSF 更

新选切片策略中该异常网络切片的标识的优先级。和/或，该收发器，还用于通知接入和移动管理功能 AMF 和/或会话管理功能 SMF 选择防护能力更强的其他网络切片；

和/或，

该处理器，还用于根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常节点；

该收发器，还用于向网络仓库功能 NRF、网域名称服务器（Domain Name Server，DNS）、SMF、网络切片管理功能（Network Slice Subnet Management Function，NSSMF）、其它网络功能中的至少一个发送该异常节点的标识，以使该 NRF、DNS、SMF、NSSMF、其它网络功能中的至少一个选择防护能力更强的节点，和/或，该收发器，还用于通知其他网络功能选择防护能力更强的节点（例如通知 SMF 选择防护能力更强的 UPF）。

第十四方面，本申请实施例提供了一种通信装置，包括：

收发模块，用于接收非接入层 NAS 消息；

该收发模块，还用于获取可信策略信息；

处理模块，用于根据该可信策略信息，检测该 NAS 消息是否异常；

若异常，

该处理模块，还用于通报和/或阻止该 NAS 消息，和/或，

该收发模块，还用于向可信控制节点上报异常信令，和/或，

该收发模块，还用于向接入和移动管理功能 AMF 上报该异常信令，该异常信令包括该 NAS 消息中的全部或部分。

结合第十四方面，在第十四方面的一种可能的实现方式中，

该收发模块，具体用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个。

结合第十四方面，在第十四方面的一种可能的实现方式中，

该收发模块，具体用于接收用户面功能 UPF 发送的用户面异常信息；

该处理模块，具体用于根据该用户面异常信息，生成该可信策略信息。

第十五方面，本申请实施例提供了一种通信装置，包括：

收发模块，用于接收非接入层 NAS 消息；

该收发模块，还用于获取可信策略信息；

处理模块，用于根据该可信策略信息，检测该 NAS 消息是否异常；

若异常，

该处理模块，还用于通报和/或阻止该 NAS 消息，和/或，

该收发模块，还用于向该可信控制节点上报异常信令，该异常信令包括该 NAS 消息中的全部或部分。

结合第十五方面，在第十五方面的一种可能的实现方式中，

该收发模块，具体用于从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个。

结合第十五方面，在第十五方面的一种可能的实现方式中，

该收发模块，具体用于接收会话管理功能 SMF 发送的该异常信令；

该收发模块，具体用于根据该异常信令，生成该可信策略信息。

结合第十五方面，在第十五方面的一种可能的实现方式中，

该收发模块，具体用于向该 NWDAF 发送该异常信令；

该收发模块，具体用于向该可信控制节点上报该异常信令。

第十六方面，本申请实施例提供了一种通信装置，包括：

收发模块，用于接收用户数据；

该收发模块，还用于获取可信策略信息；

处理模块，用于根据该可信策略信息，检测该用户数据是否异常；

若异常，

该处理模块，还用于通报和/或阻止该用户数据对应的业务，和/或，

该收发模块，还用于向该可信控制节点上报异常数据，和/或，

该收发模块，还用于向管理面网管上报该异常数据，该异常数据包括该用户数据，和/或，

该收发模块，还用于向会话管理功能 SMF 上报该异常数据，该异常数据包括该用户数据。

结合第十六方面，在第十六方面的一种可能的实现方式中，

该收发模块，具体用于从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

结合第十六方面，在第十六方面的一种可能的实现方式中，

该收发模块，还用于接收该管理面网管和/或该 SMF 发送的用户面异常信息，该用户面异常信息由该管理面网管和/或该 SMF 根据该异常数据生成；

该处理模块，还用于根据该用户面异常信息，生成该可信策略信息。

结合第十六方面，在第十六方面的一种可能的实现方式中，

该收发模块，还用于向该 NWDAF 发送该异常数据；

该收发模块，还用于向该可信控制节点上报该异常数据。

第十七方面，本申请实施例提供了一种通信装置，包括：

收发模块，用于接收异常基站信息；

该收发模块，还用于获取可信策略信息；

处理模块，用于根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力高于第二 UPF，该第一 UPF 用于当前处理该异常基站的数据。

结合第十七方面，在第十七方面的一种可能的实现方式中，

该收发模块，还用于指示该第一 UPF 处理该异常基站的数据；

该收发模块，还用于指示该第二 UPF 删除该异常基站的数据。

结合第十七方面，在第十七方面的一种可能的实现方式中，

该收发模块，具体用于从接入和移动管理功能 AMF、UPF 或网络数据分析功能 NWDAF 中

的至少一个，接收该异常基站信息。

结合第十七方面，在第十七方面的一种可能的实现方式中，

该收发模块，还用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

第十八方面，本申请实施例提供了一种通信装置，包括：

收发模块，用于获取可信策略信息；

该收发模块，还用于接收异常用户设备信息或异常归属网络信息，其中，该异常用户设备归属于该异常归属网络；

如果该异常归属网络中该异常用户设备的数量超过第一阈值，

处理模块，用于根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力高于第二 UPF，该第一 UPF 用于当前处理该异常归属网络的数据。

结合第十八方面，在第十八方面的一种可能的实现方式中，

该收发模块，还用于指示该第一 UPF 处理该异常归属网络的数据；

该收发模块，还用于指示该第二 UPF 删除该异常归属网络的数据。

结合第十八方面，在第十八方面的一种可能的实现方式中，

该收发模块，还用于从接入和移动管理功能 AMF、该第二 UPF，或网络数据分析功能 NWDAF 中的至少一个，接收该异常用户设备信息或该异常归属网络信息。

结合第十八方面，在第十八方面的一种可能的实现方式中，该收发模块，还用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

第十九方面，本申请实施例提供了一种通信装置，包括：

收发模块，还用于从策略控制功能 PCF、接入和移动管理功能 AMF、会话管理功能 SMF、用户面功能 UPF、管理面网管、网络能力开放功能实体 NEF、多接入边缘计算设备 MEC 或，公共陆地移动通信网络间用户面安全功能 IPUPS 中的至少一个，获取可信采集信息；

处理模块，用于根据该可信采集信息，确定可信策略信息；

该收发模块，还用于向该 AMF、该 SMF、该 UPF、该管理面网管、该 NEF、该 MEC 或，该 IPUPS 中的至少一个，发送该可信策略信息。

结合第十九方面，在第十九方面的一种可能的实现方式中，

该收发模块，还用于通过该 NEF 接收该 MEC 发送的该可信采集信息；

该收发模块，还用于通过该 NEF 向该 MEC 发送该可信策略信息；

和/或，

该收发模块，还用于通过该 UPF 接收该 MEC 发送的该可信采集信息；

该收发模块，还用于通过该 UPF 向该 MEC 发送该可信策略信息。

结合第十九方面，在第十九方面的一种可能的实现方式中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个。

结合第十九方面，在第十九方面的一种可能的实现方式中，

该处理模块，还用于根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常服务网络；

该收发模块，还用于向策略控制功能 PCF 或统一数据管理 UDM 发送该异常服务网络的标识、或异常网络切片的标识，以使该 PCF 或 UDM 更新选网策略中该异常服务网络标识/或异常网络切片标识的优先级，并向终端设备发送该选网策略。

和/或，

该处理模块，还用于根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常网络切片；

该收发模块，还用于向切片选择功能 NSSF 发送该异常网络切片的标识，以使该 NSSF 更新选切片策略中该异常网络切片的标识的优先级。和/或，该收发模块，还用于通知接入和移动管理功能 AMF 和/或会话管理功能 SMF 选择防护能力更强的其他网络切片；

和/或，

该处理模块，还用于根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常节点；

该收发模块，还用于向网络仓库功能 NRF、网域名称服务器（Domain Name Server，DNS）、SMF、网络切片管理功能（Network Slice Subnet Management Function，NSSMF）、其它网络功能中的至少一个发送该异常节点的标识，以使该 NRF、DNS、SMF、NSSMF、其它网络功能中的至少一个选择防护能力更强的节点，和/或，该收发模块，还用于通知其他网络功能选择防护能力更强的节点（例如通知 SMF 选择防护能力更强的 UPF）。

第二十方面，本申请实施例提出一种通信装置，包括：

收发模块，用于接收非接入层 NAS 消息、和/或用户数据，核心网设备可以包括 NEF、DNS、NWDAF、UDM、PCF、AMF、或 SMF 等，还可以包括网络切片选择功能(network slice selection function，NSSF)等网络功能节点；

收发模块，还用于获取可信策略信息；

处理模块，用于根据该可信策略信息，检测该 NAS 消息和/或该用户数据是否异常；

若异常，

处理模块，还用于通报和/或阻止该 NAS 消息、和/或该用户数据对应的业务。

结合第二十方面，在第二十方面的一种可选的实现方式中，还包括：

处理模块，还用于记录异常信令，和/或，异常数据，该异常信令包括全部或部分的该 NAS 消息。

结合第二十方面，在第二十方面的一种可选的实现方式中，该核心网设备接收该非接入层 NAS 消息、和/或该用户数据，包括：

收发模块，还用于接收该非接入层 NAS 消息，和/或，

收发模块，还用于接收该 NAS 消息，和/或，

收发模块，还用于接收该用户数据。

结合第二十方面，在第二十方面的一种可选的实现方式中，该核心网设备获取该可信策略信息，包括：

收发模块，还用于可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

结合第二十方面，在第二十方面的一种可选的实现方式中，该核心网设备获取该可信策略信息，包括：

收发模块，还用于接收用户面功能 UPF 发送的用户面异常信息，该用户面异常信息由该 UPF 根据该异常数据生成；

处理模块，还用于根据该用户面异常信息，生成该可信策略信息；

和/或，

收发模块，还用于接收该 SMF 发送的该异常信令；

处理模块，还用于根据该异常信令，生成该可信策略信息；

和/或，

收发模块，还用于接收管理面网管发送的该用户面异常信息；

处理模块，还用于根据该用户面异常信息，生成该可信策略信息。

第二十一方面，本申请实施例提出一种通信装置，包括：

收发器，用于接收非接入层 NAS 消息、和/或用户数据，核心网设备可以包括 NEF、DNS、NWDAF、UDM、PCF、AMF、或 SMF 等，还可以包括网络切片选择功能(network slice selection function，NSSF)等网络功能节点；

收发器，还用于获取可信策略信息；

处理器，用于根据该可信策略信息，检测该 NAS 消息和/或该用户数据是否异常；

若异常，

处理器，还用于通报和/或阻止该 NAS 消息、和/或该用户数据对应的业务。

结合第二十一方面，在第二十一方面的一种可选的实现方式中，还包括：

处理器，还用于记录异常信令，和/或，异常数据，该异常信令包括全部或部分的该 NAS 消息。

结合第二十一方面，在第二十一方面的一种可选的实现方式中，该核心网设备接收该非接入层 NAS 消息、和/或该用户数据，包括：

收发器，还用于接收该非接入层 NAS 消息，和/或，

收发器，还用于接收该 NAS 消息，和/或，

收发器，还用于接收该用户数据。

结合第二十一方面，在第二十一方面的一种可选的实现方式中，该核心网设备获取该可信策略信息，包括：

收发器，还用于可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

结合第二十一方面，在第二十一方面的一种可选的实现方式中，该核心网设备获取该可信策略信息，包括：

收发器，还用于接收用户面功能 UPF 发送的用户面异常信息，该用户面异常信息由该 UPF 根据该异常数据生成；

处理器，还用于根据该用户面异常信息，生成该可信策略信息；

和/或，

收发器，还用于接收该 SMF 发送的该异常信令；

处理器，还用于根据该异常信令，生成该可信策略信息；

和/或，

收发器，还用于接收管理面网管发送的该用户面异常信息；

处理器，还用于根据该用户面异常信息，生成该可信策略信息。

第二十二方面，本申请实施例提供了一种通信装置，该通信装置可以实现上述第一、二、三、四、五、六或七方面所涉及方法中 NWDAF、UDM、PCF、AMF、SMF、UPF、管理面网管、IPUPS、UE 或 NEF 所执行的功能。该通信装置包括处理器、存储器以及与该处理器连接的接收器和与该处理器连接的发射器；该存储器用于存储程序代码，并将该程序代码传输给该处理器；该处理器用于根据该程序代码中的指令驱动该接收器和该发射器执行如上述第一、二、三、四、五、六或七方面该的方法；接收器和发射器分别与该处理器连接，以执行上述各个方面的该的方法中 NWDAF、UDM、PCF、AMF、SMF、UPF、管理面网管、IPUPS、UE 或 NEF 的操作。具体地，发射器可以进行发送的操作，接收器可以进行接收的操作。

第二十三方面，本申请实施例提供一种通信装置，该通信装置可以包括网络设备或者芯片等实体，该通信装置包括：处理器，存储器；该存储器用于存储指令；该处理器用于执行该存储器中的该指令，使得该通信装置执行如前述第一、二、三、四、五、六或七方面中任一项该的方法。

第二十四方面，本申请实施例提供了一种存储一个或多个计算机执行指令的计算机可读存储介质，当该计算机执行指令被处理器执行时，该处理器执行如前述第一、二、三、四、五、六或七方面中任意一种可能的实现方式。

第二十五方面，本申请实施例提供一种存储一个或多个计算机执行指令的计算机程序产品(或称计算机程序)，当该计算机执行指令被该处理器执行时，该处理器执行前述第一、二、三、四、五、六或七方面中任意一种可能的实现方式。

第二十六方面，本申请提供了一种芯片系统，该芯片系统包括处理器，用于支持计算机设备实现上述方面中所涉及的功能。在一种可能的设计中，该芯片系统还包括存储器，该存储器，用于保存计算机设备必要的程序指令和数据。该芯片系统，可以由芯片构成，也可以包括芯片和其他分立器件。

第二十七方面，本申请提供了一种通信系统，该通信系统包括如上述第八方面至第十三方面，或第二十一方面中的通信装置。

附图说明

图 1 为本申请实施例提供的 5G 通信系统示意图；

图 2 为本申请实施例中通信装置的硬件结构示意图；

图 3a 为本申请实施例提出的一种可信通信方法的实施例示意图；

图 3b 为本申请实施例提出的又一种通信系统的拓扑示意图；

图 3c 为本申请实施例提出的又一种通信系统的拓扑示意图；

图 4 为本申请实施例提出的又一种可信通信方法的实施例示意图；

图 5 为本申请实施例提出的又一种可信通信方法的实施例示意图；

图 6 为本申请实施例提出的又一种可信通信方法的实施例示意图；

图 7a 为本申请实施例提出的又一种可信通信方法的实施例示意图；

图 7b 为本申请实施例提出的又一种可信通信方法的实施例示意图；

图 8a 为本申请实施例提出的又一种可信通信方法的实施例示意图；

图 8b 为本申请实施例提出的又一种可信通信方法的实施例示意图；

图 9a 为现有技术下网络功能的系统架构示意图；

图 9b 为本申请实施例提出的网络功能的一种架构示意图；

图 10 为本申请实施例中通信装置的一种实施例示意图；

图 11 为本申请实施例中通信装置的一种实施例示意图；

图 12 为本申请实施例中通信装置的一种实施例示意图；

图 13 为本申请实施例中通信装置的一种实施例示意图；

图 14 为本申请实施例中通信装置的一种实施例示意图；

图 15 为本申请实施例中通信装置的一种实施例示意图；

图 16 为本申请实施例中通信装置的一种实施例示意图；

图 17 为本申请实施例提出的一种处理装置示意图。

具体实施方式

本申请实施例提供了一种可信通信方法以及相关装置。首先，核心网设备接收非接入层 NAS 消息，和/或用户数据，该核心网设备获取可信策略信息。其次，根据该可信策略信息，核心网设备检测该 NAS 消息和/或该用户数据是否异常。如果异常，则 SMF 通报和/或阻止该该 NAS 消息和/或该用户数据对应的业务。核心网设备根据可信策略信息，检测 NAS 消息，和/或用户数据。无论数据与信令的来源是否位于同一安全域内，通过对数据与信令的实时监控，提升了网络设备的通信安全性能。

本申请的说明书和权利要求书及上述附图中的术语“第一”、第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的术语在适当情况下可以互换，这仅仅是描述本申请的实施例中对相同属性的对象在描述时所采用的区分方式。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，以便包含一系列单元的过程、方法、系统、产品或设备不必限于那些单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它单元。

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地描述。在本申请的描述中，除非另有说明，“/”表示或的意思，例如，A/B 可以表示 A 或 B；本申请中的“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。另外，在本申请的描述中，“至少一项”是指一项或者多项，“多项”是指两项或两项以上。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项(个)或复数项(个)的任意组合。例如，a，b，或 c 中的至少一项(个)，可以表示：a，b，c，a-b，a-c，b-c，或 a-b-c，其中 a，b，c 可以是单个，也可以是多个。

图 1 示出了本申请实施例提供的 5G 通信系统示意图。在 5G 移动网络架构中，移动网管的控制面功能和转发面功能解耦，其分离出来的控制面功能与第三代合作伙伴计划(third generation partnership project，3GPP)传统的控制移动性管理实体(mobility management entity，MME)等合并成统一的控制面(control plane)。用户面功能(User plane function，UPF)能实现服务网管(serving gateway，SGW)和分组数据网络网管(packet data network gateway，PGW)的用户面功能(SGW-U 和 PGW-U)。进一步的，统一的控制面可以分解成接入和移动管理功能(access and mobility management function，AMF)和会话管理功能(session management function，SMF)。网络开放功能(Network Exposure Function，NEF)、网络功能仓储功能 (Network Function Repository Function，NRF)、策略控制功能(Policy Control Function，PCF)、统一数据管理(Unified Data Management，UDM)、网络数据分析功能(Network Data Analysis Function，NWDAF)等，用户面的网络功能设备有：用户面功能(User Plane Function，UPF)等。与 UPF 连接的移动边缘计算设备（mobile edge computing，MEC），公共陆地移动通信网络间用户面安全功能（inter public land mobile network user plane security function，IPUPS），无线接入网（radio access network，RAN）设备，与 RAN 连接的终端设备或称为用户设备（user equipment，UE）。需要说明的是，IPUPS 也可以集成于 UPF 中。

该通信系统还包括：网域名称服务器（Domain Name Server，DNS），网络切片选择功能(Network Slice Selection Function，NSSF) ，网络功能虚拟化配器（Network Function Virtualization Orchestrator，NFVO），虚拟化网络功能管理（virtualized network function Manager，VNFM）或管理面网管。

该通信系统中，新设立一个网络功能称为：可信控制节点。可信控制节点用于从各个网络功能中采集可信采集信息，根据可信采集信息生成可信策略信息，并将可信策略信息分发至各个网络功能。各个网络功能根据该可信策略信息对信令和/或数据进行检测，以保证通信系统中通信的安全性。可信控制节点可以是新设的独立网络功能，也可以与 NWDAF、UDM，和/或 PCF 合设，该可信控制节点还可以与该通信系统中其它网络功能合设，此处不做限定。本申请实施例中，为了便于描述，以可信控制节点与 NWDAF、UDM，和/或 PCF 合设为例进行说明。

本系统中所涉及到的终端设备不受限于 5G 网络，包括：手机、物联网设备、智能家居设备、工业控制设备、车辆设备、无人机设备等等。本申请实施例中，终端设备为各种具有线通信功能的终端设备或装置，例如：移动电话（或称为“蜂窝”电话）和具有移动终端的计算机，还可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置，它们与无线接入网交换语言和/或数据。例如，个人通信业务（personal communication

service，PCS）电话、无绳电话、会话发起协议（SIP）话机、无线本地环路（wireless local loop，WLL）站、个人数字助理（personal digital assistant，PDA）等设备。终端设备也可以称为系统、订户单元（subscriber unit）、订户站（subscriber station），移动站（mobile station）、移动台（mobile）、远程站（remote station）、接入点（access point）、远程终端（remote terminal）、接入终端（access terminal）、用户终端（user terminal）、用户代理（user agent）、用户设备（user device）、或用户装备。例如车辆、车载设备、车载模块或单元、飞行器（包括但不限于无人机）、机载设备、机载模块或单元、路测基础设备、手持设备、可穿戴设备、计算设备或连接到无线调制解调器的其它处理设备，例如车辆用户设备（vehicle user equipment，VUE）或空调用户设备等等。

无线接入网设备（RAN）的主要功能是控制用户通过无线接入到移动通信网络。RAN是移动通信系统的一部分。它实现了一种无线接入技术。从概念上讲，它驻留某个设备之间(如移动电话、一台计算机，或任何远程控制机)，并提供与其核心网的连接。RAN设备包括但不限于：5G中的(g node B，gNB)、演进型节点B(evolved node B，eNB)、无线网络控制器(radio network controller，RNC)、节点B(node B，NB)、基站控制器(base station controller，BSC)、基站收发台(base transceiver station，BTS)、家庭基站(例如，home evolved nodeB，或 home node B，HNB)、基带单元(Base Band Unit，BBU)、传输点(transmitting and receiving point，TRP)、发射点(transmitting point，TP)、移动交换中心等，此外，还可以包括无线保真(wireless fidelity，wifi)接入点(access point，AP)等。本申请实施例中，为了便于描述，将无线接入网设备称为基站。

上述各网络功能既可以是在专用硬件上实现的网络元件，也可以是在专用硬件上运行的软件实例，或者是在适当平台上虚拟化功能的实例，例如，上述虚拟化平台可以为云平台。

此外，本申请实施例还可以适用于面向未来的其他通信技术，例如6G等。本申请描述的网络架构以及业务场景是为了更加清楚的说明本申请的技术方案，并不构成对本申请提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请提供的技术方案对于类似的技术问题，同样适用。

需要说明的是，在图1中，还可包括其它的（功能实体），在这里仅重点描述本申请涉及的几个（功能实体）。各之间通过Nx接口连接。

需要说明的是，图1所示的通信系统中，核心网设备可以包括NEF、DNS、NWDAF、UDM、PCF、AMF、或SMF等，还可以包括网络切片选择功能(network slice selection function，NSSF)等图中未示出的网络功能。

需要说明的是，本申请实施例中的网络功能，可以有多种表述方式，包括：网络功能节点，网络功能，节点，网络功能实体，或网元等。

图2为本申请实施例中通信装置的硬件结构示意图。该通信装置可以是本申请实施例中网络设备（包括核心网设备与无线接入网设备）或终端设备的一种可能的实现方式。如图2所示，通信装置至少包括处理器202，存储器203，和收发器202，存储器203进一步用于存储指令2032和数据2032。可选的，该通信装置还可以包括天线206，I/O(输入/输

出，Input/Output)接口210和总线212。收发器202进一步包括发射器2022和接收器2022。此外，处理器202，收发器202，存储器203和I/O接口210通过总线212彼此通信连接，天线206与收发器202相连。

处理器202可以是通用处理器，例如但不限于，中央处理器(Central Processing Unit，CPU)，也可以是专用处理器，例如但不限于，数字信号处理器(Digital Signal Processor，DSP)，应用专用集成电路(Application Specific Integrated Circuit，ASIC)和现场可编程门阵列(Field Programmable Gate Array，FPGA)等。此外，处理器202还可以是多个处理器的组合。特别的，在本申请实施例提供的技术方案中，处理器202可以用于执行，后续方法实施例中通信方法的相关步骤。处理器202可以是专门设计用于执行上述步骤和/或操作的处理器，也可以是通过读取并执行存储器203中存储的指令2032来执行上述步骤和/或操作的处理器，处理器202在执行上述步骤和/或操作的过程中可能需要用到数据2032。

收发器202包括发射器2022和接收器2022，在一种可选的实现方式中，发射器2022用于通过天线206发送信号。接收器2022用于通过天线206之中的至少一根天线接收信号。特别的，在本申请实施例提供的技术方案中，发射器2022具体可以用于通过天线206之中的至少一根天线执行，例如，后续方法实施例中通信方法应用于网络设备或终端设备时，网络设备或终端设备中接收模块或发送模块所执行的操作。

在本申请实施例中，收发器202用于支持通信装置执行前述的接收功能和发送功能。将具有处理功能的处理器视为处理器202。接收器2022也可以称为接收机、输入口、接收电路等，发射器2022可以称为发射机、发射器或者发射电路等。

处理器202可用于执行该存储器203存储的指令，以控制收发器202接收消息和/或发送消息，完成本申请方法实施例中通信装置的功能。作为一种实现方式，收发器202的功能可以考虑通过收发电路或者收发的专用芯片实现。本申请实施例中，收发器202接收消息可以理解为收发器202输入消息，收发器202发送消息可以理解为收发器202输出消息。

存储器203可以是各种类型的存储介质，例如随机存取存储器(Random Access Memory，RAM)，只读存储器(Read Only Memory，ROM)，非易失性RAM(Non-Volatile RAM，NVRAM)，可编程ROM(Programmable ROM，PROM)，可擦除PROM(Erasable PROM，EPROM)，电可擦除PROM(Electrically Erasable PROM，EEPROM)，闪存，光存储器和寄存器等。存储器203具体用于存储指令2032和数据2032，处理器202可以通过读取并执行存储器203中存储的指令2032，来执行本申请方法实施例中所述的步骤和/或操作，在执行本申请方法实施例中操作和/或步骤的过程中可能需要用到数据2032。

可选的，该通信装置还可以包括I/O接口210，该I/O接口210用于接收来自外围设备的指令和/或数据，以及向外围设备输出指令和/或数据。

下面介绍本申请实施例的方法部分，本申请实施例提出的可信通信方法，按照流程可以划分为：1、可信控制节点采集可信采集信息并生成可信策略信息；2、核心网设备根据可信策略信息检测信令和/或用户数据。下面分别进行描述。

为了生成可信策略信息，可信控制节点需要采集可信采集信息。具体的，请参阅图3a，

图 3a 为本申请实施例提出的一种可信通信方法的实施例示意图，本申请实施例提出的一种可信通信方法，包括：

301、AMF 向可信控制节点发送可信采集信息。

本实施例中，AMF 向可信控制节点发送可信采集信息，该可信采集信息包括但不限于：5G 临时用户标识/永久用户标识（5G-GUTI/SUPI），注册类型（registration type），最近访问的跟踪区域标识（last visited TAI），请求的网络切片选择辅助信息（Requested NSSAI），请求的网络切片选择辅助信息（Mapping Of Requested NSSAI），协议数据单元会话状态（PDU Session status），选择的数据网络名称（selected DNN），用户设备请求的数据网络名称（UE requested DNN），AMF 标识（AMF ID），PCF 标识（PCF ID），用户位置信息(User location information)，无线接入类型(RAT Type)，通用公共签约标识(GPSI)，本地区域数据网络服务区域中的用户位置（UE presence in LADN service area），单一的网络切片选择辅助信息（S-NSSAI(s)），请求的协议数据单元会话状态会话类型（Request PDU Session type），小数据速率控制状态（Small Data Rate Control Status），用户设备 IP 地址（UE ip address），服务质量规则（QoS Rule(s)）和服务质量流级别（QoS Flow level）或服务质量参数（ QoS parameters）。

在一种可选的实现方式中，AMF 可以周期性向可信控制节点发送该可信采集信息。

在另一种可选的实现方式中，AMF 可以接收可信控制节点发送的指示，并根据该指示向可信控制节点发送可信采集信息。

在另一种可选的实现方式中，该可信采集信息，还可以包括异常类型，例如：用户设备信令的异常。

302、SMF 向可信控制节点发送可信采集信息。

本实施例中，SMF 向可信控制节点发送可信采集信息，该可信采集信息包括但不限于：SUPI，selected DNN，UE requested DNN，AMF ID，PCF ID，User location information，RAT Type，GPSI，UE presence in LADN service area，S-NSSAI(s)，UE Requested DNN，PDU Session ID，Request PDU Session type，Small Data Rate Control Status，UE ip address，核心网隧道信息（CN tunnel info），QoS Rule(s) and QoS Flow level 和/或 QoS parameters。

在一种可选的实现方式中，SMF 可以周期性向可信控制节点发送该可信采集信息。

在另一种可选的实现方式中，SMF 可以接收可信控制节点发送的指示，并根据该指示向可信控制节点发送可信采集信息。

在另一种可选的实现方式中，该可信采集信息，还可以包括异常类型，例如：用户设备信令的异常。

303、UPF 向可信控制节点发送可信采集信息。

本实施例中，UPF 向可信控制节点发送可信采集信息，该可信采集信息包括但不限于：源 IP（ source IP） 、目标 IP （destination IP）、 源端口（source port）、目标端口（destination port）、传输控制协议(TCP)、用户数据协议(UDP)、流控制传输协议(SCTP)、核心网隧道信息（CN tunnel info）和/或接入网隧道信息（AN tunnel info）。

示例性的，UPF、基站与可信控制节点之间的连接关系，如图 3b 所示。图 3b 为本申请实施例提出的又一种通信系统的拓扑示意图。图 3b 中，UPF-A、gNB-A 和 UE-A；UPF-B、gNB-B 和 UE-B；MEC。上述网络功能节点可以属于相同或不同网络。IPUPS、UPF-C、gNB-C 和 UE-C 属于不同网络。当 UPF（包括 UPF-A、UPF-B 和 UPF-C）向可信控制节点发送可信采集信息时，该可信采集信息分别携带各侧网络的相关标识。例如：UPF-A 向可信控制节点发送关于 UE-A 的可信采集信息，该可信采集信息包括 UE-A 的信息（例如是 IP 地址）；UPF-A 向可信控制节点发送关于 UE-A 至 UE-B 的会话的可信采集信息，则该可信采集信息包括 UE-A 的标识和 UE-B 的信息（例如是 IP 地址）。

需要说明的是，UPF 向可信控制节点发送的可信采集信息，还可以记录于区块链中。可信控制节点通过调用该区块链即可获取 UPF 发送的可信采集信息。具体的，该区块链中存放可信采集信息的相关凭据，包括但不限于各侧网络的相关标识。以确保可信采集信息的可追溯性。

在一种可选的实现方式中，UPF 可以周期性向可信控制节点发送该可信采集信息。

在另一种可选的实现方式中，UPF 可以接收可信控制节点发送的指示，并根据该指示向可信控制节点发送可信采集信息。

在另一种可选的实现方式中，该可信采集信息，还可以包括异常类型，例如：用户设备数据的异常。

304、管理面网管向可信控制节点发送可信采集信息。

本实施例中，管理面网管可以是 NFVO，和/或 VNFM 等，用于管理网络设备中各个网络功能节点。

具体的，管理面网管向可信控制节点发送的可信采集信息包括异常数据。该异常数据为管理面网管接收 UPF 上报的异常数据，该异常数据由 UPF 使用可信策略信息检测用户数据得到，具体检测流程请参见后续实施例。

需要说明的是，该管理面网管向可信控制节点发送的可信采集信息还可以包括其它信息，例如前述步骤 301-303 中的可信采集信息，此处不做限定。

在一种可选的实现方式中，管理面网管可以周期性向可信控制节点发送该可信采集信息。

在另一种可选的实现方式中，管理面网管可以接收可信控制节点发送的指示，并根据该指示向可信控制节点发送可信采集信息。

在另一种可选的实现方式中，该可信采集信息，还可以包括异常类型，例如：用户设备日志的异常。

305、NEF 向可信控制节点发送可信采集信息。

本实施例中，核心网设备通过 NEF 获取外部网络下发的可信采集信息，该可信采集信息与前述步骤 301-303 中的可信采集信息类似，它还可以包括应用功能 AF 的标识信息等，此处不再赘述。该外部网络可以是互联网。然后，NEF 向可信控制节点发送该可信采集信息。

在另一种可选的实现方式中，可信控制节点通过 NEF 直接获取可信策略信息，并更新

本地的可信策略信息。该可信策略信息，可以是以软件包的形式从外部网络发送至该 NEF。

在一种可选的实现方式中，NEF 网管可以周期性向可信控制节点发送该可信采集信息。具体的，NEF 周期性的从外部网络获取可信采集信息，该可信采集信息可以是外部网络在一定时间内统计得到的可信采集信息。

在另一种可选的实现方式中，NEF 可以接收可信控制节点发送的指示，并根据该指示从外部网络获取该可信采集信息。然后 NEF 向可信控制节点发送该可信采集信息。

在另一种可选的实现方式中，该可信采集信息，还可以包括异常类型，例如：用户设备数据的异常。

306、MEC 向可信控制节点发送可信采集信息。

本实施例中，MEC 可以通过多种方式，向位于核心网设备中的可信控制节点发送可信采集信息。示例性的，MEC、基站与核心网设备之间的连接关系，如图 3c 所示。图 3c 为本申请实施例提出的又一种通信系统的拓扑示意图。图 3c 中，核心网设备中部署有可信控制节点，该核心网设备通过基站 1 与 UE1 建立连接。该核心网设备通过基站 2 与 UE2 建立连接。MEC1 与核心网设备建立连接。UE1 可以通过基站 1 向可信控制节点发送可信采集信息，UE2 可以通过基站 2 向可信控制节点发送可信采集信息。MEC1/MEC2 可以(通过 UPF1 或 UPF2 或 NEF)向可信控制节点发送可信采集信息。示例性的，MEC1 和 MEC2 作为网络切片租用方。租用运营商（核心网设备）的部分业务。需要说明的是。MEC1 与核心网设备之间的通信交互，既可以直接通过部署于核心网设备的 UPF 完成，也可以通过基站 3（图中未示出）完成，此处不做限定。

在一种可选的实现方式中，可信控制节点还可以分别部署于核心网设备，和，MEC。此时，MEC1 和 MEC2 作为网络切片租用方，基于实际业务需求，MEC1 和 MEC2 向可信控制节点（核心网设备）发送的可信采集信息，以 MEC1 为例：该发送的可信采集信息，可以是 MEC1 中的可信控制节点对 MEC1 的可信采集信息进行分析后，得到的分析结果。具体的分析方法包括但不限于：行为规律分析、规则判断，和，人工智能（Artificial Intelligence，AI）检测。由于行业用户的 MEC 有数据不回传的安全要求，因此运营商可以通过核心网设备下发可信策略信息。MEC 不回传本地的原始数据给运营商（核心网设备），仅在 MEC 本地使用可信策略信息检测数据或信令，并通报该检测结果、或留存该检测结果、或将该检测结果同步至区块链等。当该检测结果为异常时，MEC 向管理面网管通报该异常、或 MEC 向可信控制节点通报该异常。这将使运营商在涉及重大网络安全时可以采取一定实时防护行动或者进行审计/核查。原始数据票据（包括但不限于 MEC 本地的原始数据、或检测结果）可以用哈希值（Hash）、标签、或校验码等数学方式防止篡改。

该可信采集信息，还可以包括异常类型，例如：用户设备数据的异常。

在另一种可选的实现方式中，MEC 还可以直接向核心网设备（可信控制节点）发送原始的可信采集信息。该可信采集信息与前述步骤 301-303 中描述的可信采集信息类似，此处不做限定。

在一种可选的实现方式中，MEC 通过 N6 接口向可信控制节点发送可信采集信息。

在另一种可选的实现方式中，MEC 通过 NEF 接口向可信控制节点发送可信采集信息。

在另一种可选的实现方式中，MEC 通过内部网元接口向可信控制节点发送可信采集信息。

需要说明的是，MEC 向可信控制节点发送的可信采集信息，还可以记录于区块链中。可信控制节点通过调用该区块链即可获取 MEC 发送的可信采集信息。具体的，该区块链中存放可信采集信息的相关凭据，包括但不限于 MEC 的标识。以确保可信采集信息的可追溯性。

307、IPUPS 向可信控制节点发送可信采集信息。

本实施例中，IPUPS 向可信控制节点发送可信采集信息。具体的，步骤 307 与前述步骤 303 或 306 类似，此处不再赘述。

在另一种可选的实现方式中，该可信采集信息，还可以包括异常类型，例如：用户设备数据的异常。

308、可信控制节点生成可信策略信息。

本实施例中，可信控制节点根据步骤 301-307 中任一项可信采集信息，生成可信策略信息。该可信策略信息包括但不限于：终端设备（也称为用户）的可信策略检测标准，基站的可信策略检测标准，归属网络的可信策略检测标准，或服务网络的可信策略检测标准等。

示例性的：终端设备的可信策略检测标准包括：终端设备在一段时间内移动距离；终端设备在一段时间内的访问目的地地址，和访问次数；终端设备发起访问的时间点；终端设备在一段时间内数据流量等等。

基站的可信策略检测标准包括但不限于：当前基站服务的异常终端设备的数量，等等；

归属网络的可信策略检测标准包括但不限于：当前归属网络服务的异常终端设备的数量，等等；

服务网络的可信策略检测标准包括但不限于：当前服务网络服务的异常终端设备的数量。

可信策略检测标准，可以包括：正常规则，或，异常规则。

当可信控制节点生成可信策略信息后（可选的，包括通过 NEF 获取的外部网络生成的可信策略信息），可信控制节点向其他各个网络功能分发该可信策略信息。如步骤 309-315。

可选的，可信控制节点根据不同的网络功能，适应性调整各个下发的可信策略信息。

在一种可选的实现方式中，可信控制节点周期性下发可信策略信息。

在另一种可选的实现方式中，可信控制节点根据各个网络功能上报的请求信息，下发可信策略信息。

需要说明的是，该可信策略信息，可以是动态生成的可信策略信息，例如可信控制节点独立部署时，可以是动态生成的可信策略信息或者静态配置的可信策略信息；可信控制节点与 NWDAF 合设时，由 NWDAF 根据可信采集信息动态的生成可信策略信息；也可以是静态配置的可信策略信息，例如可信控制节点与 PCF 或 UDM 合设时，该可信策略信息为 PCF 或 UDM 预先配置的。该可信策略信息同样适用于本申请实施例中所有的实施例，后文不再赘述。

可选的，可信控制节点可以使用该可信策略信息，检测来自各个网络功能的可信采集信息，以此确定这些可信采集信息是否出现异常。

309、可信控制节点向 UPF 发送可信策略信息。

310、可信控制节点向 AMF 发送可信策略信息。

311、可信控制节点向管理面网管发送可信策略信息。

312、可信控制节点向 SMF 发送可信策略信息。

313、可信控制节点向 NEF 发送可信策略信息。

314、可信控制节点向 MEC 发送可信策略信息。

315、可信控制节点向 IPUPS 发送可信策略信息。

需要说明的是，在步骤 309~315 中，当可信控制节点独立部署时，可信策略信息可以由可信控制节点直接发给 UPF、AMF、管理面网管、SMF、NEF、MEC 和/或 IPUPS；也可以通过 NWDAF 或 PCF 或 UDM，发送给 UPF、AMF、管理面网管、SMF、NEF、MEC 和/或 IPUPS；当可信控制节点与 NWDAF 合设时，可信策略信息可以由可信控制节点直接发给 UPF、AMF、管理面网管、SMF、NEF、MEC 和/或 IPUPS；当可信控制节点与 PCF 或 UDM 合设时，可信策略信息可以由可信控制节点直接发给 UPF、AMF、管理面网管、SMF、NEF、MEC 和/或 IPUPS。上述说明同样适用于本申请实施例中所有的实施例，后文不再赘述。

316、可信控制节点使用该可信策略信息确定异常服务网络，并更新选网策略。

本实施例中，可信控制节点根据可信策略信息，或，根据可信策略信息和可信采集信息，确定异常服务网络。该异常服务网络为，存在异常用户数量大于某一阈值的服务网络。示例性的，当某一服务网络中服务的异常用户一段统计时间内数量大于 M(M 为正整数)时，可信控制节点确定该服务网络为异常服务网络。或者，示例性的，可信控制节点检测某一服务网络的一段统计时间内流量水平显著超过正常 100 倍时，可信控制节点确定该服务网络为异常服务网络。

当可信控制节点确定异常服务网络后，记录该异常服务网络的标识，该异常服务网络的标识可以是服务-公共陆地移动网标识（serving plmn ID)。然后根据该异常服务网络的标识，更新选网策略。

可选的，该选网策略由一个或多个异常服务网络的标识组成，选网策略中记录的异常服务网络的标识为黑名单。示例性的，该选网策略如表 1-1 所示。

选网策略-黑名单
serving plmn ID-1
serving plmn ID-5
serving plmn ID-7
serving plmn ID-10

表 1-1

表 1-1 中表示服务网络 1、5、7 和 10 为异常服务网络。

可选的，该选网策略由一个或多个异常服务网络的标识组成，选网策略中记录的异常服务网络的标识为低优先级。示例性的，该选网策略如表 1-2 所示。

服务网络名称	服务网络优先级
serving plmn ID-1	-1
serving plmn ID-6	1
serving plmn ID-8	2
serving plmn ID-2	1

表 1-2

表 1-2 中表示服务网络 1 为异常服务网络（对应 serving plmn ID-1 ），其服务优先级最低，为-1。服务网络优先级为：1、2 和 1 指示对应的服务网络为正常服务网络，即服务网络 2、6 和 8 为正常服务网络。

317、可信控制节点向 UE 发送选网策略。

本实施例中，可信控制节点向统一数据管理 UDM 或策略控制功能 PCF 发送该异常服务网络的标识，以使该 PCF 或 UDM 更新选网策略中该异常服务网络的标识的优先级，并向终端设备发送该选网策略。

在另一种可选的实现方式中，可信控制节点根据可信策略信息，或，根据可信策略信息和可信采集信息，确定异常网络切片后，可信控制节点既可以向 UE 发送更新的选切片策略（比如可信级别更高的新切片标识）；也可以通知核心网设备，请求核心网设备生成新的网络切片，或者该可信控制节点向切片选择功能 NSSF 发送该异常网络切片的标识，以使该 NSSF 更新选切片策略中该异常网络切片的标识的优先级（比如降低该异常网络切片的优先级），以选择其它防护能力更强的网络切片替代该异常网络切片。和/或，该可信控制节点通知接入和移动管理功能 AMF 和/或会话管理功能 SMF 选择防护能力更强的其他网络切片。此处不做限制。

318、UE 选择其他服务网络。

本实施例中，终端设备接收该选网策略后，更新本地存储的选网策略。根据该选网策略选择其他服务网络，例如选择服务网络 2。

需要说明的是，步骤 316-318 为可选步骤。

319、可信控制节点使用该可信策略信息确定异常网络切片，并更新选切片策略。

本实施例中，可信控制节点根据可信策略信息，或，根据可信策略信息和可信采集信息，确定异常网络切片。该可信控制节点向切片选择功能 NSSF 发送该异常网络切片的标识，以使该 NSSF 更新选切片策略中该异常网络切片的标识的优先级（比如降低该异常网络切片的优先级）。和/或，该可信控制节点通知接入和移动管理功能 AMF 和/或会话管理功能 SMF 选择防护能力更强的其他网络切片（简称为切片）。此处不再赘述。

320、可信控制节点向 NSSF 发送异常网络切片的标识。

本实施例中，在一种可选的实现方式中，可信控制节点根据可信策略信息，或，根据可信策略信息和可信采集信息，确定异常网络切片后，向切片选择功能 NSSF 发送该异常网络切片的标识，以使该 NSSF 更新选切片策略中该异常网络切片的标识的优先级（比如降低该异常网络切片的优先级），以选择其它防护能力更强的网络切片替代该异常网络切片。和/或，该可信控制节点通知接入和移动管理功能 AMF 和/或会话管理功能 SMF 选择防护能力

更强的其他网络切片。此处不做限制。

在另一种可选的实现方式中，可信控制节点确定异常网络切片后，更新选切片策略，并通过 PCF 或 UDM 将该选切片策略发送至 UE。使得 UE 更新选切片策略。该选切片策略可以是可信级别更高的新网络切片标识。UE 根据选切片策略，选择可信级别更高的新网络切片，例如选择网络切片 2。

在另一种可选的实现方式中，可信控制节点确定异常网络切片后，也可以通知核心网设备，请求核心网设备生成新的网络切片。

321、NSSF 更新选切片策略。

本实施例中，NSSF 根据接收到的异常网络切片的标识，或，选切片策略，更新本地的选切片策略。

需要说明的是，步骤 319-321 为可选步骤。

322、可信控制节点使用该可信策略信息确定异常节点。

本实施例中，在另一种可选的实现方式中，可信控制节点根据可信策略信息，或，根据可信策略信息和可信采集信息,确定异常节点(例如异常基站、异常的 AMF 或异常的 UPF)，该可信控制节点向网络仓库功能 NRF、网域名称服务器（Domain Name Server，DNS)、SMF、网络切片管理功能（Network Slice Subnet Management Function，NSSMF)、其它网络功能中的至少一个发送该异常节点的标识，以使该 NRF、DNS、SMF、NSSMF、其它网络功能中的至少一个选择防护能力更强的节点（例如：防护能力更强的 AMF 或防护能力更强的 UPF 等)，和/或，该可信控制节点通知其他网络功能选择防护能力更强的节点（例如通知 SMF 选择防护能力更强的 UPF)，此处不再赘述。

323、可信控制节点向 NRF，和/或 DNS，和/或 NSSMF 发送异常节点的标识。

本实施例中，可信控制节点可以通知 NRF、网域名称服务器（Domain Name Server，DNS)、网络切片管理功能（Network Slice Subnet Management Function，NSSMF)、其它网络功能中的至少一个，选择防护能力更强的节点。例如：可信控制节点向 SMF 发送异常节点的标识，使得 SMF 选择防护能力更强的节点。

具体的，可信控制节点向 NRF、DNS、SMF、NSSMF 和/或其它网络功能中的至少一个，发送异常节点的标识，例如发送异常 UPF 的标识。

324、NRF 和/或 DNS 和/或 NSSMF 选择防护能力更强的节点。

本实施例中，NRF、DNS、SMF、NSSMF 和/或其它网络功能中的至少一个接收到来自可信控制节点发送的异常节点的标识后，NRF、DNS、SMF、NSSMF 和/或其它网络功能中的至少一个选择防护能力更强的节点。以 NRF 为例：可信控制节点向 NRF 发送 UPF1 为异常节点，NRF 更新配置后（比如降低 UPF1 的优先级)，NRF 通知 SMF 选择防护能力更强的 UPF2 需要说明的是，步骤 322-324 为可选步骤。

本申请实施例中，可信控制节点可以获取通信系统中多个网络功能的可信采集信息，并根据该可信采集信息生成可信策略信息。然后，可信控制节点向多个网络功能下发该可信策略信息，以便这些网络功能使用该可信策略信息检测交互的数据和/或信令等。可以有效提升通信系统的安全性。

在图 3a-3c 所示实施例的基础上，核心网设备使用可信策略信息检测信令和/或用户数据。下面，以 AMF、SMF 与 UPF 为例，介绍网络功能是如何检测信令和/或用户数据。需要说明的是，网络设备中其它网络功能（例如 IPUPS 等）使用可信策略信息检测信令和/或用户数据的方法，与下列方法类似，此处不再赘述。可信控制节点还可以将可信策略信息传输给 UE，或 MEC 等其它设备，UE 或 MEC 使用该可信策略信息检测信令和/或用户数据的方法，与下列方法类似，此处不再赘述。

SMF 可以接收多种信令，例如：NAS 消息，SBA 消息，N4 接口消息等。具体的，以 SMF 检测 NAS 消息为例，请参阅图 4，图 4 为本申请实施例提出的又一种可信通信方法的实施例示意图，本申请实施例提出的一种可信通信方法，包括：

401、SMF 接收 NAS 消息。

本实施例中，SMF 接收 NAS 消息，该 NAS 消息包括但不限于：PDU 会话建立请求消息、PDU 会话修改请求消息、或 PDU 会话时候删除请求消息等。

402、SMF 接收可信控制节点发送的可信策略信息。

403、SMF 接收 UPF 发送的用户面异常信息。

本实施例中，UPF 使用可信策略信息对接收到的用户数据进行检测，当用户数据为异常时，UPF 根据该异常数据，生成用户面异常信息。SMF 接收该用户面异常信息，并使用该用户面异常信息更新本地的可信策略信息。

可选的，该用户面异常信息还可以由管理面网管根据 UPF 上传的异常数据生成。

具体的，UPF 生成用户面异常信息的方法，请参阅图 6 所示实施例。

需要说明的是，本实施例中不对步骤 401、步骤 402、步骤 403 的执行顺序进行限定。比如，可以先执行步骤 401，再执行步骤 402，再执行步骤 403；也可以先执行步骤 403，再执行步骤 401，再执行步骤 402；还可以先执行步骤 402，再执行步骤 401，再执行步骤 403；还可以先执行步骤 402，再执行步骤 403，再执行步骤 401 等，此处不再赘述。

404、SMF 检测 NAS 消息是否异常。

本实施例中，SMF 使用可信策略信息，检测接收到的 NAS 消息是否异常。

若异常，则进入步骤 406；若正常，则进入步骤 405。

405、SMF 执行 NAS 消息。

本实施例中，当该 NAS 消息为正常，则 SMF 执行该 NAS 消息。

406、SMF 通报和/或阻止 NAS 消息。

本实施例中，当该 NAS 消息为异常消息，SMF 通报和/或阻止该 NAS 消息。示例性的，SMF 阻止该 NAS 消息发送至其他网络功能。

在另一种可选的实现方式中，该 SMF 还可以该异常的 NAS 消息传输至安全防护增强的网络功能中执行业务。

407、SMF 向 AMF 上报异常信令。

本实施例中，SMF 可以向 AMF 上报异常信令，该异常信令包括该异常的 NAS 消息的部分内容或全部内容。例如：包括该 NAS 消息中携带的 IP 地址或端口号等。

408、SMF 向可信控制节点上报异常信令。

本实施例中，SMF 可以向可信控制节点上报异常信令。该异常信令作为可信采集信息的一部分，以便可信控制节点更新可信策略信息。

本申请实施例中，SMF 使用可信策略信息，可以检测流经 SMF 的 NAS 消息是否异常。当检测该 NAS 消息为异常时，可以通报和/或阻止该 NAS 消息，并向可信控制节点（和/或 AMF）上报异常信令。以便可信控制节点及时更新可信策略信息。有效提升了通信系统的安全性。需要说明的是，SMF 还可以使用可信策略信息检测其它的信令，包括但不限于：SBA 消息等，具体检测方法与图 4 所示实施例类似，此处不再赘述。

AMF 可以接收多种信令，例如：NAS 消息，SBA 消息，N2 接口消息等。具体的，以 AMF 检测 NAS 消息为例，具体的，请参阅图 5，图 5 为本申请实施例提出的又一种可信通信方法的实施例示意图，本申请实施例提出的一种可信通信方法，包括：

501、AMF 接收 NAS 消息。

本实施例中，与前述步骤 401 类似，此处不再赘述。

502、AMF 接收 SMF 发送的异常信令。

本实施例中，AMF 可以接收前述步骤 407 中 SMF 向 AMF 上报的异常信令。具体的，请参阅前述步骤 407，此处不再赘述。

503、AMF 接收可信控制节点发送的可信策略信息。

需要说明的是，本实施例中不对步骤 501、步骤 502、步骤 503 的执行顺序进行限定。比如，可以先执行步骤 501，再执行步骤 502，再执行步骤 503；也可以先执行步骤 503，再执行步骤 501，再执行步骤 502；还可以先执行步骤 502，再执行步骤 501，再执行步骤 503；还可以先执行步骤 502，再执行步骤 503，再执行步骤 501 等，此处不再赘述。

504、AMF 检测 NAS 消息是否异常。

本实施例中，与前述步骤 404 类似，此处不再赘述。

若异常，则进入步骤 506；若正常，则进入步骤 505。

505、AMF 执行 NAS 消息。

本实施例中，与前述步骤 505 类似，此处不再赘述。

506、AMF 通报和/或阻止 NAS 消息。

本实施例中，与前述步骤 406 类似，此处不再赘述。

507、AMF 向可信控制节点上报异常信令。

本实施例中，与前述步骤 408 类似，此处不再赘述。

本申请实施例中，与 SMF 类似的，AMF 使用可信策略信息，可以检测流经 AMF 的 NAS 消息是否异常。当检测该 NAS 消息为异常时，可以通报和/或阻止该 NAS 消息，并向可信控制节点上报异常信令。以便可信控制节点及时更新可信策略信息。有效提升了通信系统的安全性。需要说明的是，AMF 还可以使用可信策略信息检测其它的信令，包括但不限于：SBA 消息等，具体检测方法与图 5 所示实施例类似，此处不再赘述。

具体的，请参阅图 6，图 6 为本申请实施例提出的又一种可信通信方法的实施例示意图，本申请实施例提出的一种可信通信方法，包括：

601、UPF 接收用户数据。

本实施例中，UPF 接收用户数据，该用户数据包括但不限于该 UPF 管理的基站的数据、该基站管理的终端设备的数据、或该 UPF 管理的 MEC 的数据，或者 UPF 接收的外部数据网络的数据。

602、UPF 接收可信控制节点发送的可信策略信息。

603、UPF 接收管理面网管发送的用户面异常信息。

本实施例中，UPF 接收来自管理面网管发送的用户面异常信息。UPF 使用该用户面异常信息更新本地的可信策略信息。

具体的，与前述步骤 403 类似，此处不再赘述。

需要说明的是，本实施例中不对步骤 601、步骤 602、步骤 603 的执行顺序进行限定。比如，可以先执行步骤 601，再执行步骤 602，再执行步骤 603；也可以先执行步骤 603，再执行步骤 601，再执行步骤 602；还可以先执行步骤 602，再执行步骤 601，再执行步骤 603；还可以先执行步骤 602，再执行步骤 603，再执行步骤 601 等，此处不再赘述。

604、UPF 检测数据是否异常。

本实施例中，UPF 使用可信策略信息，检测接收到的用户数据是否异常。

若异常，则进入步骤 606；若正常，则进入步骤 605。

605、UPF 执行数据对应的业务。

本实施例中，若该用户数据为正常，则 UPF 只需该数据对应的业务。

606、UPF 通报和/或阻止数据对应的业务。

本实施例中，若该用户数据为异常，则 UPF 通报和/或阻止该数据对应的业务。包括但不限于：通报和/或阻止该用户数据对应的数据流，或，通报和/或阻止该用户数据对应的终端设备（或 MEC）访问。

在另一种可选的实现方式中，该 UPF 还可以该异常的用户数据传输至安全防护增强的网络功能中执行业务。

607、UPF 向管理面网管上报异常数据。

本实施例中，UPF 向管理面网管上报该异常数据。

一种可选的实现方式中，该 UPF 统计一段时间内检测的异常数据后，将这些异常数据上报至管理面网管。

在另一种可选的实现方式中，该 UPF 实时向管理面网管上报检测到的异常数据。

管理面网管接收到这些异常数据后，对异常数据进行统计分析，生成用户面异常信息。管理面网管可以向 SMF 或可信控制节点发送该用户面异常信息。该用户面异常信息用于更新可信策略信息。

608、UPF 向可信控制节点上报异常数据。

本实施例中，UPF 可以直接向可信控制节点上报该异常数据。

一种可选的实现方式中，该 UPF 统计一段时间内检测的异常数据后，将这些异常数据上报至可信控制节点。

在另一种可选的实现方式中，该 UPF 实时向可信控制节点上报检测到的异常数据。

609、UPF 向 SMF 上报异常数据。

本实施例中，UPF 还可以向 SMF 上报异常数据，SMF 使用该异常数据更新本地的可信策略信息。

本申请实施例中，与前述 SMF 和 AMF 类似的，UPF 使用可信策略信息，可以检测流经 UPF 的用户数据是否异常。当检测该用户数据为异常时，可以通报和/或阻止该用户数据对应的业务，并向可信控制节点上报异常数据。以便可信控制节点及时更新可信策略信息。有效提升了通信系统的安全性。

在图 3a-图 6 所示实施例的基础上，UPF 还可以使用可信策略信息，检测归属网络中用户设备（也称为终端设备、终端或用户）是否异常。当确定该归属网络为异常归属网络时，SMF 还可以确定防护等级更高的 UPF，本申请实施例中，将防护等级更高的 UPF 称为第一 UPF，将原 UPF 称为第二 UPF。该第一 UPF 用于处理异常归属网络的数据。具体的，请参阅图 7a，图 7a 为本申请实施例提出的又一种可信通信方法的实施例示意图，本申请实施例提出的一种可信通信方法，包括：

本实施例中，SMF 获知异常归属网络的相关信息。存在多种可选的实现方案，分别对应于步骤 701a-步骤 704a；步骤 701b-步骤 702b；步骤 701c-步骤 702c；步骤 701d-步骤 703d；步骤 701e-步骤 703e。下面分别进行说明。

步骤 701a-步骤 704a：

701a、第二 UPF 检测归属网络中用户设备是否异常。

本实施例中，第二 UPF 使用可信策略信息检测归属网络中各个用户设备是否异常。检测方式包括但不限于：检测用户设备的数据，和/或，检测用户设备在一段时间内的访问目的地与访问次数，和/或，检测用户设备在一段时间内的数据流量，和/或，检测用户设备在一定时间内的移动距离。

示例性的，当一段时间内，用户设备访问未经允许的网络切片的访问次数，达到某一阈值。则第二 UPF 确定该用户设备为异常用户设备。

可选的，可信控制节点根据行为模式分析，或，AI 处理方法，检测用户设备是否异常。

702a、第二 UPF 向可信控制节点发送异常用户设备信息。

本实施例中，第二 UPF 向可信控制节点发送异常用户设备信息，例如：该异常用户设备的媒体接入控制（media access control，MAC）地址等。该异常用户设备信息中还包括该归属网络的标识，例如 PLMN ID 等，此处不做限定。

703a、可信控制节点检测归属网络是否异常。

本实施例中，可信控制节点接收异常用户设备信息后，统计该异常用户设备信息对应的归属网络中异常用户设备的总数。当一段统计时间内该异常用户设备的数量超过第一阈值，则可信控制节点确定该归属网络为异常归属网络。

在一种可选的实现方式中，该第一阈值为预配置的固定值，此处不做限定。

在另一种可选的实现方式中，可信控制节点生成的可信策略信息中可以包括该第一阈值。即，可信控制节点根据可信采集信息，确定该第一阈值。

在另一种可选的实现方式中，可信控制节点可以根据其它算法，确定该归属网络对应的第一阈值，此处不做限定。

可选的，可信控制节点根据行为模式分析，或，AI 处理方法，检测归属网络是否异常。

704a、可信控制节点向 SMF 发送异常归属网络信息。

本实施例中，可信控制节点向 SMF 发送异常归属网络信息，该异常归属网络信息包括异常归属网络的标识，例如该异常归属网络的 PLMN ID。

步骤 704a 后，执行步骤 705。

步骤 701b-步骤 702b：

701b、第二 UPF 检测归属网络中用户设备是否异常。

本实施例中，步骤 701b 与前述步骤 701a 类似，此处不再赘述。

702b、第二 UPF 向 SMF 发送异常用户设备信息。

本实施例中，第二 UPF 向 SMF 发送异常用户设备信息，例如：该异常用户设备的媒体接入控制（media access control，MAC）地址等。该异常用户设备信息中还包括该归属网络的标识，例如 PLMN ID 等，此处不做限定。

SMF 接收异常用户设备信息后，统计该异常用户设备信息对应的归属网络中异常用户设备的总数。当一段统计时间内该异常用户设备的总数达到某一阈值，则 SMF 确定该归属网络为异常归属网络。

可选的，SMF 根据行为模式分析，或，AI 处理方法，检测基站是否异常。

步骤 701b 后，执行步骤 705。

步骤 701c-步骤 702c：

701c、可信控制节点检测归属网络中用户设备是否异常。

本实施例中，首先，可信控制节点采集第二 UPF 中的可信采集信息，该可信采集信息包括该归属网络中用户设备的相关数据。其次，可信控制节点使用可信策略信息检测该可信采集信息，并确定该归属网络中用户设备是否异常。具体检测的方法与前述步骤 701b 类似，此处不再赘述。

702c、可信控制节点向 SMF 发送异常归属网络信息。

本实施例中，与前述步骤 704a 类似，此处不再赘述。

步骤 702c 后，执行步骤 705。

步骤 701d-步骤 703d：

701d、可信控制节点检测归属网络中用户设备是否异常。

本实施例中，与前述步骤 701c 类似，此处不再赘述。

702d、可信控制节点向 AMF 发送异常归属网络信息。

703d、AMF 向 SMF 发送异常归属网络信息。

本实施例中，AMF 向 SMF 转发来自可信控制节点的该异常归属网络信息。

步骤 703d 后，执行步骤 705。

步骤 701e-步骤 703e：

701e、第二 UPF 检测归属网络中用户设备是否异常。

本实施例中，与前述步骤 701a 类似，此处不再赘述。

702e、第二 UPF 向 AMF 发送异常归属网络信息。

本实施例中，与前述步骤 702d 类似，此处不再赘述。

703e、AMF 向 SMF 发送异常归属网络信息。

本实施例中，与前述步骤 703d 类似，此处不再赘述。

步骤 703e 后，执行步骤 705。

705、SMF 确定第一 UPF。

本实施例中，当 SMF 确定存在异常归属网络时，SMF 确定第一 UPF，该第一 UPF 的防护能力（或称为安全性能）高于第二 UPF，并使用该第一 UPF 处理该异常归属网络的相关数据。其次，SMF 删除第二 UPF 的数据，包括但不限于：SMF 释放第二 UPF 上的资源。

具体的，SMF 可以通过网络仓库功能 NRF 或者网络切片选择功能 NSSF，选择防护能力较高的 UPF，作为第一 UPF。NRF 或 NSSF 中存储各个 UPF 的可信等级（含防护能力）。

本申请实施例中，核心网设备可以确定归属网络是否异常。进而使用防护能力更高的 UPF 处理该归属网络的相关数据。提升了通信的安全性。

当 SMF 确定第一 UPF 后，SMF 使用第一 UPF 处理该异常归属网络的数据。具体流程，请参阅图 7b，请参阅图 7b，图 7b 为本申请实施例提出的又一种可信通信方法的实施例示意图，本申请实施例提出的一种可信通信方法，包括：

S1、SMF 向第一 UPF 发送会话建立请求消息。

本实施例中，SMF 指示该归属网络中的各个用户（终端设备）通过该 SMF 向第一 UPF 发送会话建立请求消息。该会话建立请求消息中还携带各个终端设备的标识。

S2、第一 UPF 向 SMF 发送会话建立响应消息（携带核心网隧道信息）。

本实施例中，根据该会话建立请求消息，第一 UPF 向 SMF 发送会话建立响应消息。该会话建立响应消息中携带第一核心网隧道信息（CN tunnel info），该核心网隧道信息包括该第一 UPF 所在核心网的 IP 地址、隧道号和/或端口号等。

S3、SMF 向 AMF 发送第一核心网隧道信息。

本实施例中，SMF 向 AMF 发送第一核心网隧道信息。示例性的，通过 Namf_communication_N1N2MessageTransfer 服务消息发送该第一核心网隧道信息。

S4、AMF 向 RAN 发送 N2 PDU 会话修改请求消息（携带第一核心网隧道信息）。

本实施例中，示例性的 AMF 向 RAN 发送该 N2 PDU 会话修改请求（N2 PDU session modify request）消息，该 N2 PDU 会话修改请求消息中携带第一核心网隧道信息。

S5、RAN 向 AMF 发送 N2 PDU 会话修改响应消息（携带接入网隧道信息）。

本实施例中，RAN 向 AMF 发送 N2 PDU 会话修改响应消息，该 N2 PDU 会话修改响应消息中携带接入网隧道信息。该接入网隧道信息包括 RAN 的 IP 地址、隧道号和/或端口号等。

S6、AMF 向 SMF 发送 PDU 会话更新上下文响应消息（携带接入网隧道信息）。

本实施例中，示例性的，该 PDU 会话更新上下文响应消息为 Nsmf_PDUSession_UpdateSMContextRequest。该 PDU 会话更新上下文响应消息中携带该接入网隧道信息。

S7、SMF 向第一 UPF 发送 N4 会话修改请求消息（携带接入网隧道信息）。

本实施例中，示例性的，该 N4 会话修改请求消息为 N4 Session modify request。该

N4 会话修改请求消息中携带该接入网隧道信息。

S8、第一 UPF 向 SMF 发送 N4 会话修改响应消息。

本实施例中，当第一 UPF 向 SMF 发送 N4 会话修改响应（N4 Session modify response）消息后，示意该归属网络（异常）的终端设备的相关数据，以转移至第一 UPF 处理。核心网设备可以删除第二 UPF。

在图 3a-图 6 所示实施例的基础上，UPF 还可以使用可信策略信息，检测基站是否异常。当确定该基站为异常基站时，SMF 还可以确定可信等级更高的 UPF，本申请实施例中，将可信等级更高的 UPF 称为第一 UPF，将原 UPF 称为第二 UPF。该第一 UPF 用于处理异常基站的数据。具体的，请参阅图 8a，图 8a 为本申请实施例提出的又一种可信通信方法的实施例示意图，本申请实施例提出的一种可信通信方法，包括：

本实施例中，UPF 获知异常基站的相关信息。存在多种可选的实现方案，分别对应于步骤 801a-步骤 803a；步骤 801b-步骤 802b；步骤 801c-步骤 802c；步骤 801d-步骤 803d；步骤 801e-步骤 803e。下面分别进行说明。

步骤 801a-步骤 803a：

801a、第二 UPF 检测基站是否异常。

本实施例中，第二 UPF 使用可信策略信息，检测该基站是否异常。具体的，检测一段统计时间内该基站中异常信令的数量，和/或，异常数据的数量大于某一阈值时，确定该基站为异常基站。示例性的，在 M 小时内，当某一基站中累计异常信令数量大于 N 时，确定该基站为异常基站，其中，M 为正整数，N 为正整数。

可选的，第二 UPF 根据行为模式分析，或，AI 处理方法，检测基站是否异常。

802a、第二 UPF 向可信控制节点发送异常基站信息。

本实施例中，第二 UPF 向可信控制节点发送异常基站信息。示例性的，异常基站信息例如：该异常基站的 IP 地址等。

803a、可信控制节点向 SMF 发送异常基站信息。

步骤 803a 后，执行步骤 805。

步骤 801b-步骤 802b：

801b、第二 UPF 检测基站是否异常。

本实施例中，步骤 801b 与前述步骤 801a 类似，此处不再赘述。

802b、第二 UPF 向 SMF 发送异常基站信息。

本实施例中，第二 UPF 直接向 SMF 发送异常基站信息。

步骤 802b 后，执行步骤 805。

步骤 801c-步骤 802c：

801c、可信控制节点检测基站是否异常。

本实施例中，首先，可信控制节点采集第二 UPF 中的可信采集信息，该可信采集信息包括该基站的相关数据。其次，可信控制节点使用可信策略信息检测该可信采集信息，并确定该基站是否异常。具体检测的方法与前述步骤 801a 类似，此处不再赘述。

802c、可信控制节点向 SMF 发送异常基站信息。

步骤 802c 后，执行步骤 805。

步骤 801d-步骤 803d：

801d、可信控制节点检测基站是否异常。

本实施例中，与前述步骤 801c 类似，此处不再赘述。

802d、可信控制节点向 AMF 发送异常基站信息。

803d、AMF 向 SMF 发送异常基站信息。

本实施例中，AMF 向 SMF 转发来自可信控制节点的该异常基站信息。

步骤 803d 后，执行步骤 805。

步骤 801e-步骤 803e：

801e、第二 UPF 检测基站是否异常。

本实施例中，前述步骤 801a 类似，此处不再赘述。

802e、第二 UPF 向 AMF 发送异常基站信息。

803e、AMF 向 SMF 发送异常基站信息。

步骤 803e 后，执行步骤 805。

805、SMF 确定第一 UPF

本实施例中，当 SMF 确定存在异常基站时，SMF 确定第一 UPF，该第一 UPF 的防护能力（或称为安全性能）高于第二 UPF。并使用该第一 UPF 处理该异常基站的相关数据。其次，SMF 删除第二 UPF 的数据，包括但不限于：SMF 释放第二 UPF 上的资源。

具体的，SMF 可以通过网络仓库功能 NRF 或者网络切片选择功能 NSSF，选择防护能力较高的 UPF，作为第一 UPF。NRF 或 NSSF 中存储各个 UPF 的可信等级（含防护能力）。

本申请实施例中，核心网设备可以确定基站是否异常。进而使用防护能力更高的 UPF 处理该基站的相关数据。提升了通信的安全性。

当 SMF 确定第一 UPF 后，SMF 使用第一 UPF 处理该异常基站的数据。具体流程，请参阅图 8b，请参阅图 8b，图 8b 为本申请实施例提出的又一种可信通信方法的实施例示意图，本申请实施例提出的一种可信通信方法，包括：

D1、SMF 向第一 UPF 发送会话建立请求消息。

本实施例中，SMF 指示该基站中的各个用户（终端设备）通过该 SMF 向第一 UPF 发送会话建立请求消息。该会话建立请求消息中还携带各个终端设备的标识。

D2、第一 UPF 向 SMF 发送会话建立响应消息（携带第一核心网隧道信息）。

本实施例中，根据该会话建立请求消息，第一 UPF 向 SMF 发送会话建立响应消息。该会话建立响应消息中携带第一核心网隧道信息（CN tunnel info），该核心网隧道信息包括该第一 UPF 所在核心网的 IP 地址、隧道号和/或端口号等。

D3、SMF 向 AMF 发送第一核心网隧道信息和异常接入网隧道信息。

本实施例中，SMF 向 AMF 发送第一核心网隧道信息和异常接入网隧道信息。例如，通过 Namf_communication_N1N2MessageTransfer 服务消息发送该第一核心网隧道信息和该异常接入网隧道信息。该异常接入网隧道信息为异常基站的接入网隧道信息，包括：该异常基站的 IP 地址、隧道号和/或端口号等。

D4、AMF 向 RAN 发送 N2 PDU 会话请求消息（携带第一核心网隧道信息）。

本实施例中，AMF 根据异常接入网隧道信息来确定 RAN。然后，AMF 向该 RAN 发送该 N2 PDU 会话请求（N2 PDU session Request）消息，该 N2 PDU 会话请求消息中携带第一核心网隧道信息。

D5、RAN 向 AMF 发送 N2 PDU 会话响应消息（携带第一接入网隧道信息）。

本实施例中，RAN 向 AMF 发送 N2 PDU 会话修改响应消息，该 N2 PDU 会话修改响应消息中携带第一接入网隧道信息。该第一接入网隧道信息与异常接入网隧道信息可能不一样。

D6、AMF 向 SMF 发送 PDU 会话更新上下文响应消息（携带第一接入网隧道信息）。

本实施例中，示例性的，该 PDU 会话更新上下文响应消息为 Nsmf_PDUSession_UpdateSMContextRequest。

D7、SMF 向第一 UPF 发送 N4 会话修改请求消息（携带第一接入网隧道信息）。

本实施例中，示例性的，该 N4 会话修改请求消息为 N4 Session modify request。

D8、第一 UPF 向 SMF 发送 N4 会话修改响应消息。

本实施例中，当第一 UPF 向 SMF 发送 N4 会话修改响应（N4 Session modify response）消息后，示意该异常基站的相关数据，以转移至第一 UPF 处理。核心网设备可以删除第二 UPF。

在前述图 1-图 8b 所示实施例的基础上，本申请实施例中，还可以对网络设备中各个网络功能按照可信等级划分。具体的，请参阅图 9a，图 9a 为现有技术下网络功能的系统架构示意图。按照网络权限划分，各项网络功能可以分为：网络运营方、签约数据方、网络切片租用方和漫游方。

网络运营方包括实体运营商和虚拟运营商。实体运营商按网号(PLMN 当中包含国家码、网号）生成数字主权边界，对应到实体的网络设备。网络可信管理由运营商承担国家法律责任和基础设施运营责任、对个人用户的隐私保护责任；实体运营商对自己用户的可信签约管理负责。虚拟运营商从实体运营商租用网络使用权，在每个运营商拥有自己的号段（在统一数据管理（UDM）、归属用户服务器（HSS）、归属位置寄存器（HLR）或 PCF/策略和计费规则功能（PCRF）等分配），不对应实体的网络设备，通过签约数据约定网络区域、功能、服务保障和计费等。独立的签约数据设备可信管理由虚拟运营商自行负责。网络可信管理由运营商承担国家法律责任和基础设施运营责任、对个人用户的隐私保护责任。

网络切片租用方：互联网公司越过运营商（OTT）业务、第三方运营商或个人从实体运营商租用切片，拥有部分网络资源切片租用期内的使用权。如果切片租用方独立放号，那么切片租用方需要承担签约数据的可信管理责任。其余网络责任，按照可信要求和运营商共同行使双方管理，例如行业要求数据不上传，那么运营商的监管则只能通过探测手段、遇到可疑情况留存双方共同和监管部门检测。

漫游方：拜访网络作为实体运营商承担拜访地国家法律责任和基础设施运营责任、对个人用户在拜访地的隐私保护责任。归属地运营商对个人用户在归属地的通信服务和隐私负责，同时承担签约数据的可信管理责任。

具体的，网络运营方包括以下网络功能节点的至少一项：NFVO、DNS、NRF、NSSF、NWDAF、

NEF、AMF、SMF、UP、RAN、IPUPS 和/或 MEC 等以及签约数据方所包括的网络功能节点。签约数据方包括以下网络功能节点的至少一项：UDM、PCF、鉴权服务器功能（AUSF）、归属签约用户服务器(HSS)/归属位置寄存器(HLR)和/或，验证、授权和记账服务器(AAA server)。网络切片租用方包括：MEC。漫游方包括：通过 IPUPS 通讯的另一个网络运营方。

网络运营方的数字主权的管理的最小集是 DNS/NRF/网管/NSSF，决定了网络拓扑，以及 Default AMF，和最小集 SMF/UPF 提供基础服务；在此基础上可以分信任等级建设 AMF/SMF/UPF/NWDAF/NEF/gNB，各网络功能节点是可选组合。

本申请实施例中，对网络运营方提供的上述这些网络功能节点，按照可信等级划分。不同业务可以通过不同可信等级的网络功能处理。以可信等级包括：高可信度、中可信度和低可信度三个等级为例进行说明。请参阅图 9b，图 9b 为本申请实施例提出的网络功能的一种架构示意图。

图 9b 中，网络运营方（和数据签约方）的网络功能节点这些不同可信等级的网络功能节点，可以根据实际可信等级需求的不同，为不同的 UE、MEC 或 IPUPS 提供服务。

在一种可选的实现方式中，按照使用者的预先配置，为不同的网络功能预先配置不同的可信等级。

上述主要以方法的角度对本申请实施例提供的方案进行了介绍。可以理解的是，通信装置为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的模块及算法步骤，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，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申请的范围。

本申请实施例可以根据上述方法示例对网络设备（包括核心网设备与无线接入网设备）或终端设备进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。需要说明的是，本申请实施例中对模块的划分是示意性的，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。

下面对本申请中的通信装置进行详细描述，请参阅图 10，图 10 为本申请实施例中通信装置的一种实施例示意图。通信装置可以部署于网络设备中，通信装置包括：

收发模块 1001，用于接收非接入层 NAS 消息；

该收发模块 1001，还用于获取可信策略信息；

处理模块 1002，用于根据该可信策略信息，检测该 NAS 消息是否异常；

若异常，

该处理模块 1002，还用于通报和/或阻止该 NAS 消息，和/或，

该收发模块 1001，还用于向可信控制节点上报异常信令，和/或，

该收发模块 1001，还用于向接入和移动管理功能 AMF 上报该异常信令，该异常信令包括该 NAS 消息中的全部或部分。

在本申请的一些可选实施例中，

该收发模块 1001，具体用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

在本申请的一些可选实施例中，

该收发模块 1001，具体用于接收用户面功能 UPF 发送的用户面异常信息；

该处理模块 1002，具体用于根据该用户面异常信息，生成该可信策略信息。

请参阅图 11，图 11 为本申请实施例中通信装置的一种实施例示意图。通信装置，包括：

收发模块 1101，用于接收非接入层 NAS 消息；

该收发模块 1101，还用于获取可信策略信息；

处理模块 1102，用于根据该可信策略信息，检测该 NAS 消息是否异常；

若异常，

该处理模块 1102，还用于通报和/或阻止该 NAS 消息，和/或，

该收发模块 1101，还用于向该可信控制节点上报异常信令，该异常信令包括该 NAS 消息中的全部或部分。

在本申请的一些可选实施例中，

该收发模块 1101，具体用于从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

在本申请的一些可选实施例中，

该收发模块 1101，具体用于接收会话管理功能 SMF 发送的该异常信令；

该收发模块 1101，具体用于根据该异常信令，生成该可信策略信息。

在本申请的一些可选实施例中，

该收发模块 1101，具体用于向该 NWDAF 发送该异常信令；

该收发模块 1101，具体用于向该可信控制节点上报该异常信令。

请参阅图 12，图 12 为本申请实施例中通信装置的一种实施例示意图。通信装置，包括：

收发模块 1201，用于接收用户数据；

该收发模块 1201，还用于获取可信策略信息；

处理模块 1202，用于根据该可信策略信息，检测该用户数据是否异常；

若异常，

该处理模块 1202，还用于通报和/或阻止该用户数据对应的业务，和/或，

该收发模块 1201，还用于向该可信控制节点上报异常数据，和/或，

该收发模块 1201，还用于向管理面网管上报该异常数据，该异常数据包括该用户数据，和/或，

该收发模块 1201，还用于向会话管理功能 SMF 上报该异常数据，该异常数据包括该用

户数据。

在本申请的一些可选实施例中，

该收发模块 1201，具体用于从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

在本申请的一些可选实施例中，

该收发模块 1201，还用于接收该管理面网管和/或该 SMF 发送的用户面异常信息，该用户面异常信息由该管理面网管和/或该 SMF 根据该异常数据生成；

该处理模块 1202，还用于根据该用户面异常信息，生成该可信策略信息。

在本申请的一些可选实施例中，

该收发模块 1201，还用于向该 NWDAF 发送该异常数据；

该收发模块 1201，还用于向该可信控制节点上报该异常数据。

请参阅图 13，图 13 为本申请实施例中通信装置的一种实施例示意图。通信装置，包括：

收发模块 1301，用于接收异常基站信息；

该收发模块 1301，还用于获取可信策略信息；

处理模块 1302，用于根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力高于第二 UPF，该第一 UPF 用于当前处理该异常基站的数据。

在本申请的一些可选实施例中，

该收发模块 1301，还用于指示该第一 UPF 处理该异常基站的数据；

该收发模块 1301，还用于指示该第二 UPF 删除该异常基站的数据。

在本申请的一些可选实施例中，

该收发模块 1301，具体用于从接入和移动管理功能 AMF、UPF 或网络数据分析功能 NWDAF 中的至少一个，接收该异常基站信息。

在本申请的一些可选实施例中，

该收发模块 1301，还用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

请参阅图 14，图 14 为本申请实施例中通信装置的一种实施例示意图。通信装置，包括：

收发模块 1401，用于获取可信策略信息；

该收发模块 1401，还用于接收异常用户设备信息或异常归属网络信息，其中，该异常用户设备归属于该异常归属网络；

如果该异常归属网络中该异常用户设备的数量超过第一阈值，

处理模块 1402，用于根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力高于第二 UPF，该第一 UPF 用于当前处理该异常归属网络的数据。

在本申请的一些可选实施例中，

该收发模块 1401，还用于指示该第一 UPF 处理该异常归属网络的数据；

该收发模块 1401，还用于指示该第二 UPF 删除该异常归属网络的数据。

在本申请的一些可选实施例中，

该收发模块 1401，还用于从接入和移动管理功能 AMF、该第二 UPF，或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个，接收该异常用户设备信息或该异常归属网络信息。

在本申请的一些可选实施例中，该收发模块 1401，还用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个。

请参阅图 15，图 15 为本申请实施例中通信装置的一种实施例示意图。通信装置，包括：

收发模块 1501，还用于从策略控制功能 PCF、接入和移动管理功能 AMF、会话管理功能 SMF、用户面功能 UPF、管理面网管、网络能力开放功能实体 NEF、多接入边缘计算设备 MEC 或，公共陆地移动通信网络间用户面安全功能 IPUPS 中的至少一个，获取可信采集信息；

处理模块 1502，用于根据该可信采集信息，确定可信策略信息；

该收发模块 1501，还用于向该 AMF、该 SMF、该 UPF、该管理面网管、该 NEF、该 MEC 或，该 IPUPS 中的至少一个，发送该可信策略信息。

在本申请的一些可选实施例中，

该收发模块 1501，还用于通过该 NEF 接收该 MEC 发送的该可信采集信息；

该收发模块 1501，还用于通过该 NEF 向该 MEC 发送该可信策略信息；

和/或，

该收发模块 1501，还用于通过该 UPF 接收该 MEC 发送的该可信采集信息；

该收发模块 1501，还用于通过该 UPF 向该 MEC 发送该可信策略信息。

在本申请的一些可选实施例中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个。

在本申请的一些可选实施例中，

该处理模块 1502，还用于根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常服务网络；

该收发模块 1501，还用于向 PCF 或统一数据管理 UDM 发送该异常服务网络的标识，以使该 PCF 或 UDM 更新选网策略中该异常服务网络的标识的优先级，并向终端设备发送该选网策略。

和/或，

该处理模块 1502，还用于根据所述可信策略信息或根据所述可信策略信息和所述可信采集信息，确定异常网络切片；

该收发模块 1501，还用于向切片选择功能 NSSF 发送所述异常网络切片的标识，以使所述 NSSF 更新选切片策略中所述异常网络切片的标识的优先级。和/或，该收发模块 1501，

还用于通知接入和移动管理功能AMF和/或会话管理功能SMF选择防护能力更强的其他网络切片。

和/或，

该处理模块1502，还用于根据所述可信策略信息或根据所述可信策略信息和所述可信采集信息，确定异常节点；

该收发模块1501，还用于向网络仓库功能NRF、网域名称服务器(Domain Name Server，DNS)、SMF、网络切片管理功能（Network Slice Subnet Management Function， NSSMF)、其它网络功能中的至少一个发送该异常节点的标识，以使该NRF、该DNS、该SMF、该NSSMF、该其它网络功能中的至少一个选择防护能力更强的节点，和/或，该收发模块 1501，还用于通知其他网络功能选择防护能力更强的节点（例如通知SMF选择防护能力更强的UPF)。

请参阅图 16，图 16 为本申请实施例中通信装置的一种实施例示意图。通信装置，包括：

收发模块 1601，用于接收非接入层 NAS 消息、和/或用户数据，核心网设备可以包括NEF、DNS、NWDAF、UDM、PCF、AMF、或 SMF 等，还可以包括网络切片选择功能(network slice selection function，NSSF)等网络功能节点；

收发模块1601，还用于获取可信策略信息；

处理模块 1602，用于根据该可信策略信息，检测该 NAS 消息和/或该用户数据是否异常；

若异常，

处理模块1602，还用于通报和/或阻止该NAS消息、和/或该用户数据对应的业务。

在本申请的一些可选实施例中，还包括：

处理模块 1602，还用于记录异常信令，和/或，异常数据，该异常信令包括全部或部分的该NAS消息。

在本申请的一些可选实施例中，该核心网设备接收该非接入层NAS消息、和/或该用户数据，包括：

收发模块1601，还用于接收该非接入层NAS消息，和/或，

收发模块1601，还用于接收该NAS消息，和/或，

收发模块1601，还用于接收该用户数据。

在本申请的一些可选实施例中，该核心网设备获取该可信策略信息，包括：

收发模块1601，还用于可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能PCF、统一数据管理UDM、或网络数据分析功能NWDAF、或独立网络功能实体中的至少一个。

在本申请的一些可选实施例中，该核心网设备获取该可信策略信息，包括：

收发模块1601，还用于接收用户面功能UPF发送的用户面异常信息，该用户面异常信息由该UPF根据该异常数据生成；

处理模块1602，还用于根据该用户面异常信息，生成该可信策略信息；

和/或，

收发模块 1601，还用于接收该 SMF 发送的该异常信令；

处理模块 1602，还用于根据该异常信令，生成该可信策略信息；

和/或，

收发模块 1601，还用于接收管理面网管发送的该用户面异常信息；

处理模块 1602，还用于根据该用户面异常信息，生成该可信策略信息。

上述实施例中的通信装置，可以是网络设备，也可以是应用于网络设备中的芯片或者其他可实现上述网络设备功能的组合器件、部件等。当通信装置是网络设备时，接收模块与发送模块可以是收发器，该收发器可以包括天线和射频电路等，处理模块可以是处理器，例如基带芯片等。当通信装置是具有上述网络设备功能的部件时，接收模块与发送模块可以是射频单元，处理模块可以是处理器。当通信装置是芯片系统时，接收模块可以是芯片系统的输入端口，发送模块可以是芯片系统的输出接口、处理模块可以是芯片系统的处理器，例如：中央处理器（central processing unit，CPU）。

在本申请实施例中，该通信装置所包括的存储器主要用于存储软件程序和数据，例如存储上述实施例中所描述的第一消息和第二消息等。该通信装置还具有以下功能：

一种通信装置，包括：

收发器，用于接收非接入层 NAS 消息；

该收发器，还用于获取可信策略信息；

处理器，用于根据该可信策略信息，检测该 NAS 消息是否异常；

若异常，

该处理器，还用于通报和/或阻止该 NAS 消息，和/或，

该收发器，还用于向可信控制节点上报异常信令，和/或，

该收发器，还用于向接入和移动管理功能 AMF 上报该异常信令，该异常信令包括该 NAS 消息中的全部或部分。

在本申请的一些可选实施例中，

该收发器，具体用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

在本申请的一些可选实施例中，

该收发器，具体用于接收用户面功能 UPF 发送的用户面异常信息；

该处理器，具体用于根据该用户面异常信息，生成该可信策略信息。

该通信装置，包括：

收发器，用于接收非接入层 NAS 消息；

该收发器，还用于获取可信策略信息；

处理器，用于根据该可信策略信息，检测该 NAS 消息是否异常；

若异常，

该处理器，还用于通报和/或阻止该 NAS 消息，和/或，

该收发器，还用于向该可信控制节点上报异常信令，该异常信令包括该 NAS 消息中的

全部或部分。

在本申请的一些可选实施例中，

该收发器，具体用于从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

在本申请的一些可选实施例中，

该收发器，具体用于接收会话管理功能 SMF 发送的该异常信令；

该收发器，具体用于根据该异常信令，生成该可信策略信息。

在本申请的一些可选实施例中，

该收发器，具体用于向该 NWDAF 发送该异常信令；

该收发器，具体用于向该可信控制节点上报该异常信令。

该通信装置，包括：

收发器，用于接收用户数据；

该收发器，还用于获取可信策略信息；

处理器，用于根据该可信策略信息，检测该用户数据是否异常；

若异常，

该处理器，还用于通报和/或阻止该用户数据对应的业务，和/或，

该收发器，还用于向该可信控制节点上报异常数据，和/或，

该收发器，还用于向管理面网管上报该异常数据，该异常数据包括该用户数据，和/或，

该收发器，还用于向会话管理功能 SMF 上报该异常数据，该异常数据包括该用户数据。

在本申请的一些可选实施例中，

该收发器，具体用于从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

在本申请的一些可选实施例中，

该收发器，还用于接收该管理面网管和/或该 SMF 发送的用户面异常信息，该用户面异常信息由该管理面网管和/或该 SMF 根据该异常数据生成；

该处理器，还用于根据该用户面异常信息，生成该可信策略信息。

在本申请的一些可选实施例中，

该收发器，还用于向该 NWDAF 发送该异常数据；

该收发器，还用于向该可信控制节点上报该异常数据。

该通信装置，包括：

收发器，用于接收异常基站信息；

该收发器，还用于获取可信策略信息；

处理器，用于根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力高于第二 UPF，该第一 UPF 用于当前处理该异常基站的数据。

在本申请的一些可选实施例中，

该收发器，还用于指示该第一 UPF 处理该异常基站的数据；

该收发器，还用于指示该第二 UPF 删除该异常基站的数据。

在本申请的一些可选实施例中，

该收发器，具体用于从接入和移动管理功能 AMF、UPF 或网络数据分析功能 NWDAF 中的至少一个，接收该异常基站信息。

在本申请的一些可选实施例中，

该收发器，还用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

该通信装置，包括：

收发器，用于获取可信策略信息；

该收发器，还用于接收异常用户设备信息或异常归属网络信息，其中，该异常用户设备归属于该异常归属网络；

如果该异常归属网络中该异常用户设备的数量超过第一阈值，

处理器，用于根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力高于第二 UPF，该第一 UPF 用于当前处理该异常归属网络的数据。

在本申请的一些可选实施例中，

该收发器，还用于指示该第一 UPF 处理该异常归属网络的数据；

该收发器，还用于指示该第二 UPF 删除该异常归属网络的数据。

在本申请的一些可选实施例中，

该收发器，还用于从接入和移动管理功能 AMF、该第二 UPF，或网络数据分析功能 NWDAF 中的至少一个，接收该异常用户设备信息或该异常归属网络信息。

在本申请的一些可选实施例中，

该收发器，还用于从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

该通信装置，包括：

收发器，还用于从策略控制功能 PCF、接入和移动管理功能 AMF、会话管理功能 SMF、用户面功能 UPF、管理面网管、网络能力开放功能实体 NEF、多接入边缘计算设备 MEC 或，公共陆地移动通信网络间用户面安全功能 IPUPS 中的至少一个，获取可信采集信息；

处理器，用于根据该可信采集信息，确定可信策略信息；

该收发器，还用于向该 AMF、该 SMF、该 UPF、该管理面网管、该 NEF、该 MEC 或，该 IPUPS 中的至少一个，发送该可信策略信息。

在本申请的一些可选实施例中，

该收发器，还用于通过该 NEF 接收该 MEC 发送的该可信采集信息；

该收发器，还用于通过该 NEF 向该 MEC 发送该可信策略信息；

和/或，

该收发器，还用于通过该 UPF 接收该 MEC 发送的该可信采集信息；

该收发器，还用于通过该 UPF 向该 MEC 发送该可信策略信息。

在本申请的一些可选实施例中，

该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个。

在本申请的一些可选实施例中，

该处理器，还用于根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常服务网络；

该收发器，还用于向策略控制功能 PCF 或统一数据管理 UDM 发送该异常服务网络、或异常服务切片的标识，以使该 PCF 或 UDM 更新选网策略中该异常服务网络、或异常服务切片标识的优先级，并向终端设备发送该选网策略。

和/或，

该处理器，还用于根据所述可信策略信息或根据所述可信策略信息和所述可信采集信息，确定异常网络切片；

该收发器，还用于向切片选择功能 NSSF 发送所述异常网络切片的标识，以使所述 NSSF 更新选切片策略中所述异常网络切片的标识的优先级。和/或，该收发器，还用于通知接入和移动管理功能 AMF 和/或会话管理功能 SMF 选择防护能力更强的其他网络切片。

和/或，

该处理器，还用于根据所述可信策略信息或根据所述可信策略信息和所述可信采集信息，确定异常节点；

该收发器，还用于向网络仓库功能 NRF、网域名称服务器（Domain Name Server，DNS）、SMF、网络切片管理功能（Network Slice Subnet Management Function， NSSMF）、其它网络功能中的至少一个发送该异常节点的标识，以使该 NRF、该 DNS、该 SMF、该 NSSMF、该其它网络功能中的至少一个选择防护能力更强的节点，和/或，该收发器，还用于通知其他网络功能选择防护能力更强的节点（例如通知 SMF 选择防护能力更强的 UPF）。

该通信装置，包括：

收发器，用于接收非接入层 NAS 消息、和/或用户数据，核心网设备可以包括 NEF、DNS、NWDAF、UDM、PCF、AMF、或 SMF 等，还可以包括网络切片选择功能(network slice selection function，NSSF)等网络功能节点；

收发器，还用于获取可信策略信息；

处理器，用于根据该可信策略信息，检测该 NAS 消息和/或该用户数据是否异常；

若异常，

处理器，还用于通报和/或阻止该 NAS 消息、和/或该用户数据对应的业务。

在本申请的一些可选实施例中，还包括：

处理器，还用于记录异常信令，和/或，异常数据，该异常信令包括全部或部分的该 NAS 消息。

在本申请的一些可选实施例中，该核心网设备接收该非接入层 NAS 消息、和/或该用户数据，包括：

收发器，还用于接收该非接入层 NAS 消息，和/或，

收发器，还用于接收该 NAS 消息，和/或，

收发器，还用于接收该用户数据。

在本申请的一些可选实施例中，该核心网设备获取该可信策略信息，包括：

收发器，还用于可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

在本申请的一些可选实施例中，该核心网设备获取该可信策略信息，包括：

收发器，还用于接收用户面功能 UPF 发送的用户面异常信息，该用户面异常信息由该 UPF 根据该异常数据生成；

处理器，还用于根据该用户面异常信息，生成该可信策略信息；

和/或，

收发器，还用于接收该 SMF 发送的该异常信令；

处理器，还用于根据该异常信令，生成该可信策略信息；

和/或，

收发器，还用于接收管理面网管发送的该用户面异常信息；

处理器，还用于根据该用户面异常信息，生成该可信策略信息。

本申请实施例还提供了一种处理装置，请参阅图 17，图 17 为本申请实施例提出的一种处理装置示意图。处理装置包括处理器和接口；该处理器，用于执行上述任一方法实施例该的可信通信方法。

应理解，上述处理装置可以是一个芯片，该处理器可以通过硬件实现也可以通过软件来实现，当通过硬件实现时，该处理器可以是逻辑电路、集成电路等；当通过软件来实现时，该处理器可以是一个通用处理器，通过读取存储器中存储的软件代码来实现，该存储器可以集成在处理器中，可以位于该处理器之外，独立存在。

其中，“通过硬件实现”是指通过不具有程序指令处理功能的硬件处理电路来实现上述模块或者单元的功能，该硬件处理电路可以通过分立的硬件元器件组成，也可以是集成电路。为了减少功耗、降低尺寸，通常会采用集成电路的形式来实现。硬件处理电路可以包括 ASIC（application-specific integrated circuit，专用集成电路），或者 PLD（programmable logic device，可编程逻辑器件）；其中，PLD 又可包括 FPGA（field programmable gate array，现场可编程门阵列）、CPLD（complex programmable logic device，复杂可编程逻辑器件）等等。这些硬件处理电路可以是单独封装的一块半导体芯片（如封装成一个 ASIC）；也可以跟其他电路（如 CPU、DSP）集成在一起后封装成一个半导体芯片，例如，可以在一个硅基上形成多种硬件电路以及 CPU，并单独封装成一个芯片，这种芯片也称为 SoC，或者也可以在硅基上形成用于实现 FPGA 功能的电路以及 CPU，并单独封闭成一个芯片，这种芯片也称为 SoPC（system on a programmable chip，可编程片上系统）。

本申请还提供一种通信系统，其包括通信装置（核心网设备，无线接入网设备和/或终

端设备）。

本申请实施例还提供的一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机执行：

步骤 A：会话管理功能 SMF 接收非接入层 NAS 消息；

步骤 B：该 SMF 获取可信策略信息；

步骤 C：根据该可信策略信息，该 SMF 检测该 NAS 消息是否异常；

步骤 D：若异常，则该 SMF 通报和/或阻止该 NAS 消息，和/或，向可信控制节点上报异常信令，和/或，向接入和移动管理功能 AMF 上报该异常信令，该异常信令包括该 NAS 消息中的全部或部分。

步骤 E：该 SMF 从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

步骤 F：该 SMF 接收用户面功能 UPF 发送的用户面异常信息；

步骤 G：该 SMF 根据该用户面异常信息，生成该可信策略信息。

和/或，

步骤 H：接入和移动管理功能 AMF 接收非接入层 NAS 消息；

步骤 I：该 AMF 获取可信策略信息；

步骤 J：根据该可信策略信息，该 AMF 检测该 NAS 消息是否异常；

步骤 K：若异常，则该 AMF 通报和/或阻止该 NAS 消息，和/或，向该可信控制节点上报异常信令，该异常信令包括该 NAS 消息中的全部或部分。

步骤 L：该 AMF 从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

步骤 M：该 AMF 接收会话管理功能 SMF 发送的该异常信令；

步骤 N：该 AMF 根据该异常信令，生成该可信策略信息。

步骤 O：该 AMF 向该 NWDAF 发送该异常信令；

步骤 P：该 NWDAF 向该可信控制节点上报该异常信令。

和/或，

步骤 Q：用户面功能 UPF 接收用户数据；

步骤 R：该 UPF 获取可信策略信息；

步骤 S：根据该可信策略信息，该 UPF 检测该用户数据是否异常；

步骤 T：若异常，则该 UPF 通报和/或阻止该用户数据对应的业务，和/或，向该可信控制节点上报异常数据，和/或，向管理面网管上报该异常数据，该异常数据包括该用户数据，和/或，向会话管理功能 SMF 上报该异常数据，该异常数据包括该用户数据。

步骤 U：该 UPF 从可信控制节点获取该可信策略信息，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

步骤 V：该 UPF 接收该管理面网管和/或该 SMF 发送的用户面异常信息，该用户面异常信息由该管理面网管和/或该 SMF 根据该异常数据生成；

步骤 W：该 UPF 根据该用户面异常信息，生成该可信策略信息。

步骤 X：该 UPF 向该 NWDAF 发送该异常数据；

步骤 Y：该 NWDAF 向该可信控制节点上报该异常数据。

步骤 Z：会话管理功能 SMF 接收异常基站信息；

步骤 AA：该 SMF 获取可信策略信息；

步骤 AB：该 SMF 根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力高于第二 UPF，该第一 UPF 用于当前处理该异常基站的数据。

步骤 AC：该 SMF 指示该第一 UPF 处理该异常基站的数据；

步骤 AD：该 SMF 指示该第二 UPF 删除该异常基站的数据。

步骤 AE：该 SMF 从接入和移动管理功能 AMF、UPF 或网络数据分析功能 NWDAF 中的至少一个，接收该异常基站信息。

步骤 AF：该 SMF 从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

和/或，

步骤 AG：会话管理功能 SMF 获取可信策略信息；

步骤 AH：该 SMF 接收异常用户设备信息或异常归属网络信息，其中，该异常用户设备归属于该异常归属网络；

步骤 AI：如果该异常归属网络中该异常用户设备的数量超过第一阈值，

步骤 AJ：该 SMF 根据该可信策略信息确定第一用户面功能 UPF，该第一 UPF 的防护能力高于第二 UPF，该第一 UPF 用于当前处理该异常归属网络的数据。

步骤 AK：该 SMF 指示该第一 UPF 处理该异常归属网络的数据；

步骤 AL：该 SMF 指示该第二 UPF 删除该异常归属网络的数据。

步骤 AM：该 SMF 从接入和移动管理功能 AMF、该第二 UPF，或网络数据分析功能 NWDAF 中的至少一个，接收该异常用户设备信息或该异常归属网络信息。

步骤 AN：该 SMF 从该可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

步骤 AO：可信控制节点从接入和移动管理功能 AMF、会话管理功能 SMF、用户面功能 UPF、管理面网管、网络能力开放功能实体 NEF、多接入边缘计算设备 MEC 或，公共陆地移动通信网络间用户面安全功能 IPUPS 中的至少一个，获取可信采集信息；

步骤 AP：该可信控制节点根据该可信采集信息，确定可信策略信息；

步骤 AQ：该可信控制节点该 AMF、该 SMF、该 UPF、该管理面网管、该 NEF、该 MEC 或，该 IPUPS 中的至少一个，发送该可信策略信息。

步骤 AR：该可信控制节点通过该 NEF 接收该 MEC 发送的该可信采集信息；

步骤 AS：该可信控制节点通过该 NEF 向该 MEC 发送该可信策略信息；

和/或，

步骤 AT：该可信控制节点通过该 UPF 接收该 MEC 发送的该可信采集信息；

步骤 AU：该可信控制节点通过该 UPF 向该 MEC 发送该可信策略信息。

步骤 AV：该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个。

步骤 AW：该可信控制节点根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常服务网络；

步骤 AX：该可信控制节点向策略控制功能 PCF 或 UDM 发送该异常服务网络的标识，以使该 PCF 或 UDM 更新选网策略中该异常服务网络的标识的优先级，并向终端设备发送该选网策略。

和/或，

步骤 AW：该可信控制节点根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常网络切片；

步骤 AX：该可信控制节点向切片选择功能 NSSF 发送该异常网络切片的标识，以使该 NSSF 更新选切片策略中该异常网络切片的标识的优先级（比如降低该异常网络切片的优先级）。和/或，该可信控制节点通知接入和移动管理功能 AMF 和/或会话管理功能 SMF 选择防护能力更强的其他网络切片。

和/或，

步骤 AW：该可信控制节点根据该可信策略信息或根据该可信策略信息和该可信采集信息，确定异常节点；

步骤 AX：该可信控制节点向网络仓库功能 NRF、网域名称服务器(Domain Name Server，DNS)、SMF、网络切片管理功能（Network Slice Subnet Management Function，NSSMF）、其它网络功能中的至少一个发送该异常节点的标识，以使该 NRF、DNS、SMF、NSSMF、其它网络功能中的至少一个选择防护能力更强的节点，和/或，该可信控制节点通知其他网络功能选择防护能力更强的节点（例如通知 SMF 选择防护能力更强的 UPF）。

和/或，

步骤 AY：核心网设备接收非接入层 NAS 消息、和/或用户数据，核心网设备可以包括 NEF、DNS、NWDAF、UDM、PCF、AMF、或 SMF 等，还可以包括网络切片选择功能(network slice selection function，NSSF)等网络功能节点；

步骤 AZ：该核心网设备获取可信策略信息；

步骤 BA：根据该可信策略信息，该核心网设备检测该 NAS 消息和/或该用户数据是否异常；

步骤 BB：若异常，则该核心网设备通报和/或阻止该 NAS 消息、和/或该用户数据对应的业务。

步骤 BC：该核心网设备记录异常信令，和/或，异常数据，该异常信令包括全部或部分的该 NAS 消息。

步骤 BD：会话管理功能 SMF 接收该非接入层 NAS 消息，和/或，

步骤 BE：接入和移动管理功能 AMF 接收该 NAS 消息，和/或，

步骤 BF：用户面功能 UPF 接收该用户数据。

步骤 BG：该核心网设备从可信控制节点获取该可信策略信息，其中，该可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个。

步骤 BH：会话管理功能 SMF 接收用户面功能 UPF 发送的用户面异常信息，该用户面异常信息由该 UPF 根据该异常数据生成；

步骤 BI：该 SMF 根据该用户面异常信息，生成该可信策略信息；

和/或，

步骤 BJ：接入和移动管理功能 AMF 接收该 SMF 发送的该异常信令；

步骤 BK：该 AMF 根据该异常信令，生成该可信策略信息；

和/或，

步骤 BL：该 UPF 接收管理面网管发送的该用户面异常信息；

步骤 BM：该 UPF 根据该用户面异常信息，生成该可信策略信息。

本申请实施例还提供的一种计算机程序产品，该计算机程序产品包括计算机程序代码，当该计算机程序代码在计算机上运行时，使得计算机执行上述步骤 A-步骤 G，和/或，步骤 H-步骤 P，和/或，步骤 Q-步骤 Y，和/或，步骤 Z-步骤 AF，和/或，步骤 AG-步骤 AN，和/或，步骤 AO-步骤 AX，和/或，步骤 AY-步骤 BM。

本申请实施例还提供一种芯片，包括存储器和处理器，该存储器用于存储计算机程序，该处理器用于从该存储器中调用并运行该计算机程序，使得芯片执行上述步骤步骤 A-步骤 G，和/或，步骤 H-步骤 P，和/或，步骤 Q-步骤 Y，和/或，步骤 Z-步骤 AF，和/或，步骤 AG-步骤 AN，和/或，步骤 AO-步骤 AX，和/或，步骤 AY-步骤 BM。

本申请实施例还提供一种芯片，包括处理器，该处理器用于调用并运行计算机程序，使得芯片执行上述步骤 A-步骤 G，和/或，步骤 H-步骤 P，和/或，步骤 Q-步骤 Y，和/或，步骤 Z-步骤 AF，和/或，步骤 AG-步骤 AN，和/或，步骤 AO-步骤 AX，和/或，步骤 AY-步骤 BM。

另外需说明的是，以上所描述的装置实施例仅仅是示意性的，其中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模块来实现本实施例方案的目的。另外，本申请提供的装置实施例附图中，模块之间的连接关系表示它们之间具有通信连接，具体可以实现为一条或多条通信总线或信号线。

通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件的方式来实现，当然也可以通过专用硬件包括专用集成电路、专用 CPU、专用存储器、专用元器件等来实现。一般情况下，凡由计算机程序完成的功能都可以很容易地用相应的硬件来实现，而且，用来实现同一功能的具体硬件结构也可以是多种多样的，例如模拟电路、数字电路或专用电路等。但是，对本申请而言更多情况下软件程序实现是

更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献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可读取的存储介质中，如计算机的软盘、U 盘、移动硬盘、ROM、RAM、磁碟或者光盘等，包括若干指令用以使得一台计算机设备执行本申请各个实施例所述的方法。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。

所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、通信装置、计算设备或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、通信装置、计算设备或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存储的任何可用介质或者是包含一个或多个可用介质集成的通信装置、数据中心等数据存储设备。所述可用介质可以是磁性介质，(例如，软盘、硬盘、磁带)、光介质（例如，DVD)、或者半导体介质（例如固态硬盘（Solid State Disk，SSD)）等。

应理解，说明书通篇中提到的“一个实施例”或“一实施例”意味着与实施例有关的特定特征、结构或特性包括在本申请的至少一个实施例中。因此，在整个说明书各处出现的“在一个实施例中”或“在一实施例中”未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。应理解，在本申请的各种实施例中，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，而不应对本申请实施例的实施过程构成任何限定。

另外，本文中术语“系统”和“网络”在本文中常被可互换使用。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。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

应理解，在本申请实施例中，“与 A 相应的 B”表示 B 与 A 相关联，根据 A 可以确定 B。但还应理解，根据 A 确定 B 并不意味着仅仅根据 A 确定 B，还可以根据 A 和/或其它信息确定 B。

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、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。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申请的范围。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，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。

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，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，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，装置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。

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。

另外，在本申请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。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

集成的单元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，本申请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全部或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）执行本申请各个实施例方法的全部或部分步骤。

总之，以上所述仅为本申请技术方案的较佳实施例而已，并非用于限定本申请的保护范围。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

权 利 要 求

1、一种可信通信方法，其特征在于，包括：

会话管理功能 SMF 接收非接入层 NAS 消息；

所述 SMF 获取可信策略信息；

根据所述可信策略信息，所述 SMF 检测所述 NAS 消息是否异常；

若异常，则所述 SMF 通报和/或阻止所述 NAS 消息，和/或，向可信控制节点上报可信采集信息，和/或，向接入和移动管理功能 AMF 上报所述可信采集信息。

2、根据权利要求 1 所述的方法，其特征在于，所述 SMF 获取所述可信策略信息，包括：

所述 SMF 从所述可信控制节点获取所述可信策略信息，其中，所述可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个、或独立网络功能实体；

或者，

所述 SMF 接收用户面功能 UPF 发送的用户面异常信息；

所述 SMF 根据所述用户面异常信息，生成所述可信策略信息。

3、一种可信通信方法，其特征在于，包括：

接入和移动管理功能 AMF 接收非接入层 NAS 消息；

所述 AMF 获取可信策略信息；

根据所述可信策略信息，所述 AMF 检测所述 NAS 消息是否异常；

若异常，则所述 AMF 通报和/或阻止所述 NAS 消息，和/或，向所述可信控制节点上报可信采集信息。

4、根据权利要求 3 所述的方法，其特征在于，所述 AMF 获取所述可信策略信息，包括：

所述 AMF 从可信控制节点获取所述可信策略信息，所述可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个、或独立网络功能实体；

或者，

所述 AMF 接收会话管理功能 SMF 发送的所述可信采集信息；

所述 AMF 根据所述可信采集信息，生成所述可信策略信息。

5、根据权利要求 3-4 中任一项所述的方法，其特征在于，所述 AMF 向所述可信控制节点上报所述可信采集信息，包括：

所述 AMF 向所述 NWDAF 发送所述可信采集信息；

所述 NWDAF 向所述可信控制节点上报所述可信采集信息。

6、一种可信通信方法，其特征在于，包括：

用户面功能 UPF 接收用户数据；

所述 UPF 获取可信策略信息；

根据所述可信策略信息，所述 UPF 检测所述用户数据是否异常；

若异常，则所述 UPF 通报和/或阻止所述用户数据对应的业务，和/或，向所述可信控制节点上报可信采集信息，和/或，向管理面网管上报所述可信采集信息，和/或，向会话

管理功能 SMF 上报所述可信采集信息。

7、根据权利要求 6 所述的方法，其特征在于，所述 UPF 获取可信策略信息，包括：

所述 UPF 从可信控制节点获取所述可信策略信息，所述可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF 中的至少一个；

或者，

所述 UPF 接收所述管理面网管和/或所述 SMF 发送的用户面异常信息，所述用户面异常信息由所述管理面网管和/或所述 SMF 根据所述可信采集信息生成；

所述 UPF 根据所述用户面异常信息，生成所述可信策略信息。

8、根据权利要求 6-7 中任一项所述的方法，其特征在于，所述 UPF 向所述可信控制节点上报所述可信采集信息，包括：

所述 UPF 向所述 NWDAF 发送所述可信采集信息；

所述 NWDAF 向所述可信控制节点上报所述可信采集信息。

9、一种可信通信方法，其特征在于，包括：

会话管理功能 SMF 从接入和移动管理功能 AMF、用户面功能 UPF 或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个，接收异常基站信息；

所述 SMF 从可信控制节点获取可信策略信息，其中，所述可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个；

所述 SMF 根据所述可信策略信息确定第一用户面功能 UPF，所述第一 UPF 的防护能力高于第二 UPF，所述第二 UPF 用于当前处理所述异常基站的数据；

所述 SMF 指示所述第一 UPF 处理所述异常基站的数据；

所述 SMF 指示所述第二 UPF 删除所述异常基站的数据。

10、一种可信通信方法，其特征在于，包括：

会话管理功能 SMF 从可信控制节点获取可信策略信息，其中，所述可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个；

所述 SMF 从接入和移动管理功能 AMF、第二 UPF，或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个，接收所述异常用户设备信息或所述异常归属网络信息，其中，所述异常用户设备归属于所述异常归属网络；

如果所述异常归属网络中所述异常用户设备的数量超过第一阈值，

所述 SMF 根据所述可信策略信息确定第一用户面功能 UPF，所述第一 UPF 的防护能力高于第二 UPF，所述第二 UPF 用于当前处理所述异常归属网络的数据；

所述 SMF 指示所述第一 UPF 处理所述异常归属网络的数据；

所述 SMF 指示所述第二 UPF 删除所述异常归属网络的数据。

11、一种可信通信方法，其特征在于，包括：

可信控制节点从接入和移动管理功能 AMF、会话管理功能 SMF、用户面功能 UPF、管理面网管、网络能力开放功能实体 NEF、多接入边缘计算设备 MEC 或，公共陆地移动通信网

络间用户面安全功能 IPUPS 中的至少一个，获取可信采集信息，

所述可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个；

所述可信控制节点根据所述可信采集信息，确定可信策略信息；

所述可信控制节点所述 AMF、所述 SMF、所述 UPF、所述管理面网管、所述 NEF、所述 MEC 或，所述 IPUPS 中的至少一个，发送所述可信策略信息。

12、根据权利要求 11 所述的方法，其特征在于，所述方法具体包括：

所述可信控制节点通过所述 NEF 接收所述 MEC 发送的所述可信采集信息；

所述可信控制节点通过所述 NEF 向所述 MEC 发送所述可信策略信息；

和/或，

所述可信控制节点通过所述 UPF 接收所述 MEC 发送的所述可信采集信息；

所述可信控制节点通过所述 UPF 向所述 MEC 发送所述可信策略信息。

13、根据权利要求 11-12 中任一项所述的方法，其特征在于，所述方法还包括：

所述可信控制节点根据所述可信策略信息或根据所述可信策略信息和所述可信采集信息，确定异常服务网络；

所述可信控制节点向策略控制功能 PCF 或统一数据管理 UDM 发送所述异常服务网络的标识，以使所述 PCF 或所述 UDM 更新选网策略中所述异常服务网络的标识的优先级，并向终端设备发送所述选网策略；

和/或，

所述可信控制节点根据所述可信策略信息，或根据所述可信策略信息和所述可信采集信息，确定异常网络切片；

所述可信控制节点向切片选择功能 NSSF 发送所述异常网络切片的标识，以使所述 NSSF 更新选切片策略中所述异常网络切片的标识的优先级，和/或，所述可信控制节点通知所述 AMF 和/或所述 SMF 选择防护能力更强的其他网络切片；

和/或，

所述可信控制节点根据所述可信策略信息，或根据所述可信策略信息和所述可信采集信息，确定异常节点；

所述可信控制节点向网络仓库功能 NRF 发送所述异常节点的标识，以使所述 NRF 选择防护能力更强的节点，和/或，所述可信控制节点通知其他网络功能选择防护能力更强的节点。

14、一种通信装置，其特征在于，包括：

收发器，用于接收非接入层 NAS 消息；

所述收发器，还用于获取可信策略信息；

处理器，用于根据所述可信策略信息，检测所述 NAS 消息是否异常；

若异常，

所述处理器，还用于通报和/或阻止所述 NAS 消息，和/或，

所述收发器，还用于向可信控制节点上报可信采集信息，和/或，

所述收发器，还用于向接入和移动管理功能 AMF 上报所述可信采集信息。

15、根据权利要求 14 所述的通信装置，其特征在于，

所述收发器，具体用于从所述可信控制节点获取所述可信策略信息，其中，所述可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个；

或者，

所述收发器，具体用于接收用户面功能 UPF 发送的用户面异常信息；

所述处理器，具体用于根据所述用户面异常信息，生成所述可信策略信息。

16、一种通信装置，其特征在于，包括：

收发器，用于接收非接入层 NAS 消息；

所述收发器，还用于获取可信策略信息；

处理器，用于根据所述可信策略信息，检测所述 NAS 消息是否异常；

若异常，

所述处理器，还用于通报和/或阻止所述 NAS 消息，和/或，

所述收发器，还用于向所述可信控制节点上报可信采集信息。

17、根据权利要求 16 所述的通信装置，其特征在于，

所述收发器，具体用于从可信控制节点获取所述可信策略信息，所述可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个；

或者，

所述收发器，具体用于接收会话管理功能 SMF 发送的所述可信采集信息；

所述收发器，具体用于根据所述可信采集信息，生成所述可信策略信息。

18、根据权利要求 16-17 中任一项所述的通信装置，其特征在于，

所述收发器，具体用于向所述 NWDAF 发送所述可信采集信息；

所述收发器，具体用于向所述可信控制节点上报所述可信采集信息。

19、一种通信装置，其特征在于，包括：

收发器，用于接收用户数据；

所述收发器，还用于获取可信策略信息；

处理器，用于根据所述可信策略信息，检测所述用户数据是否异常；

若异常，

所述处理器，还用于通报和/或阻止所述用户数据对应的业务，和/或，

所述收发器，还用于向所述可信控制节点上报可信采集信息，和/或，

所述收发器，还用于向管理面网管上报所述可信采集信息，和/或，

所述收发器，还用于向会话管理功能 SMF 上报所述可信采集信息。

20、根据权利要求 19 所述的通信装置，其特征在于，

所述收发器，具体用于从可信控制节点获取所述可信策略信息，所述可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能

实体中的至少一个；

或者，

所述收发器，还用于接收所述管理面网管和/或所述 SMF 发送的用户面异常信息，所述用户面异常信息由所述管理面网管和/或所述 SMF 根据所述可信采集信息生成；

所述处理器，还用于根据所述用户面异常信息，生成所述可信策略信息。

21、根据权利要求 19-20 中任一项所述的通信装置，其特征在于，

所述收发器，还用于向所述 NWDAF 发送所述可信采集信息；

所述收发器，还用于向所述可信控制节点上报所述可信采集信息。

22、一种通信装置，其特征在于，包括：

收发器，用于从接入和移动管理功能 AMF、UPF 或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个，接收异常基站信息；

所述收发器，还用于从可信控制节点获取可信策略信息，其中，所述可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个；

处理器，用于根据所述可信策略信息确定第一用户面功能 UPF，所述第一 UPF 的防护能力高于第二 UPF，所述第二 UPF 用于当前处理所述异常基站的数据；

所述处理器，还用于指示所述第一 UPF 处理所述异常基站的数据；

所述处理器，还用于指示所述第二 UPF 删除所述异常基站的数据。

23、一种通信装置，其特征在于，包括：

收发器，用于从可信控制节点获取可信策略信息，其中，所述可信控制节点包括：策略控制功能 PCF、统一数据管理 UDM、或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个；

所述收发器，还用于从接入和移动管理功能 AMF、第二用户面功能 UPF，或网络数据分析功能 NWDAF、或独立网络功能实体中的至少一个，接收异常用户设备信息或异常归属网络信息，其中，所述异常用户设备归属于所述异常归属网络；

处理器，用于如果所述异常归属网络中所述异常用户设备的数量超过第一阈值，根据所述可信策略信息确定第一用户面功能 UPF，所述第一 UPF 的防护能力高于第二 UPF，所述第二 UPF 用于当前处理所述异常归属网络的数据；

所述处理器，还用于指示所述第一 UPF 处理所述异常归属网络的数据；

所述处理器，还用于指示所述第二 UPF 删除所述异常归属网络的数据。

24、一种通信装置，其特征在于，包括：

收发器，还用于从策略控制功能 PCF、接入和移动管理功能 AMF、会话管理功能 SMF、用户面功能 UPF、管理面网管、网络能力开放功能实体 NEF、多接入边缘计算设备 MEC 或，公共陆地移动通信网络间用户面安全功能 IPUPS 中的至少一个，获取可信采集信息；

处理器，用于根据所述可信采集信息，确定可信策略信息；

所述收发器，还用于向所述 AMF、所述 SMF、所述 UPF、所述管理面网管、所述 NEF、所述 MEC 或，所述 IPUPS 中的至少一个，发送所述可信策略信息。

25、根据权利要求 24 所述的通信装置，其特征在于，

所述收发器，还用于通过所述 NEF 接收所述 MEC 发送的所述可信采集信息；

所述收发器，还用于通过所述 NEF 向所述 MEC 发送所述可信策略信息；

和/或，

所述收发器，还用于通过所述 UPF 接收所述 MEC 发送的所述可信采集信息；

所述收发器，还用于通过所述 UPF 向所述 MEC 发送所述可信策略信息。

26、根据权利要求 24-25 中任一项所述的通信装置，其特征在于，

所述处理器，还用于根据所述可信策略信息或根据所述可信策略信息和所述可信采集信息，确定异常服务网络；

所述收发器，还用于向策略控制功能 PCF 或 UDM 发送所述异常服务网络的标识，以使所述 PCF 所述 UDM 更新选网策略中所述异常服务网络的标识的优先级，并向终端设备发送所述选网策略；

和/或，

所述处理器，还用于根据所述可信策略信息或根据所述可信策略信息和所述可信采集信息，确定异常网络切片；

所述收发器，还用于向切片选择功能 NSSF 发送所述异常网络切片的标识，以使所述 NSSF 更新选切片策略中所述异常网络切片的标识的优先级。和/或，所述收发器，还用于通知接入和移动管理功能 AMF 和/或会话管理功能 SMF 选择防护能力更强的其他网络切片；

和/或，

所述处理器，还用于根据所述可信策略信息或根据所述可信策略信息和所述可信采集信息，确定异常节点；

所述收发器，还用于向网络仓库功能 NRF 发送所述异常节点的标识，以使所述 NRF 选择防护能力更强的节点，和/或，所述收发器，还用于通知其他网络功能选择防护能力更强的节点。

27、一种计算机程序存储介质，其特征在于，所述计算机程序存储介质具有程序指令，当所述程序指令被直接或者间接执行时，使得如权利要求 1-2，或，3-5，或，6-8，或，9，或，10，或，11-13 中任一所述的方法被执行。

28、一种芯片系统，其特征在于，所述芯片系统包括至少一个处理器，当程序指令在所述至少一个处理器中执行时，使得如权利要求 1-2，或，3-5，或，6-8，或，9，或，10，或，11-13 中任一所述的方法被执行。

29、一种通信系统，其特征在于，所述通信系统包括：如权利要求 14-15，或，16-18，或，19-21，或，22，或，23，或，24-26 中任一所述的通信装置。

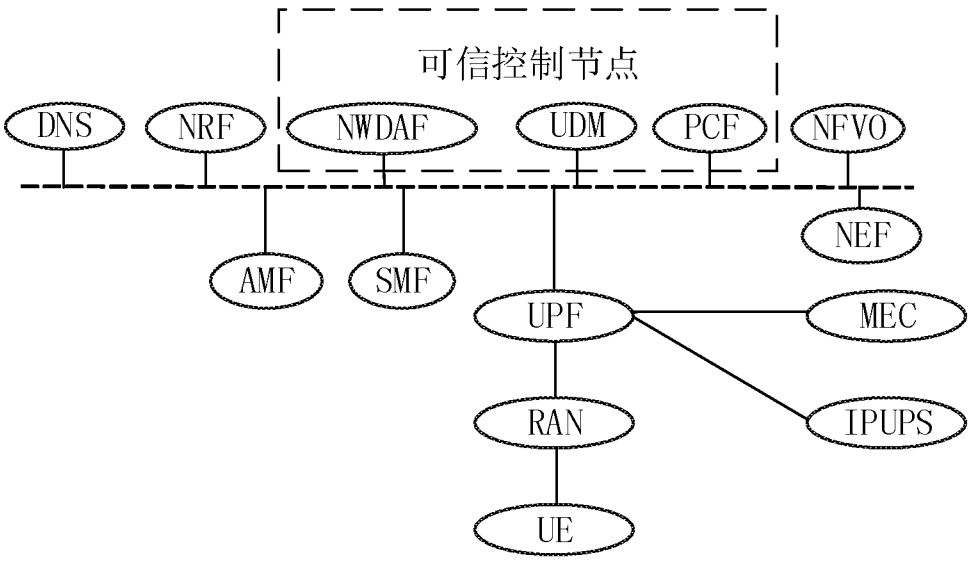

可信控制节点
DNS
NRF
NWDAF
UDM
PCF
NFVO
NEF
AMF
SMF
UPF
MEC
RAN
IPUPS
UE

图 1

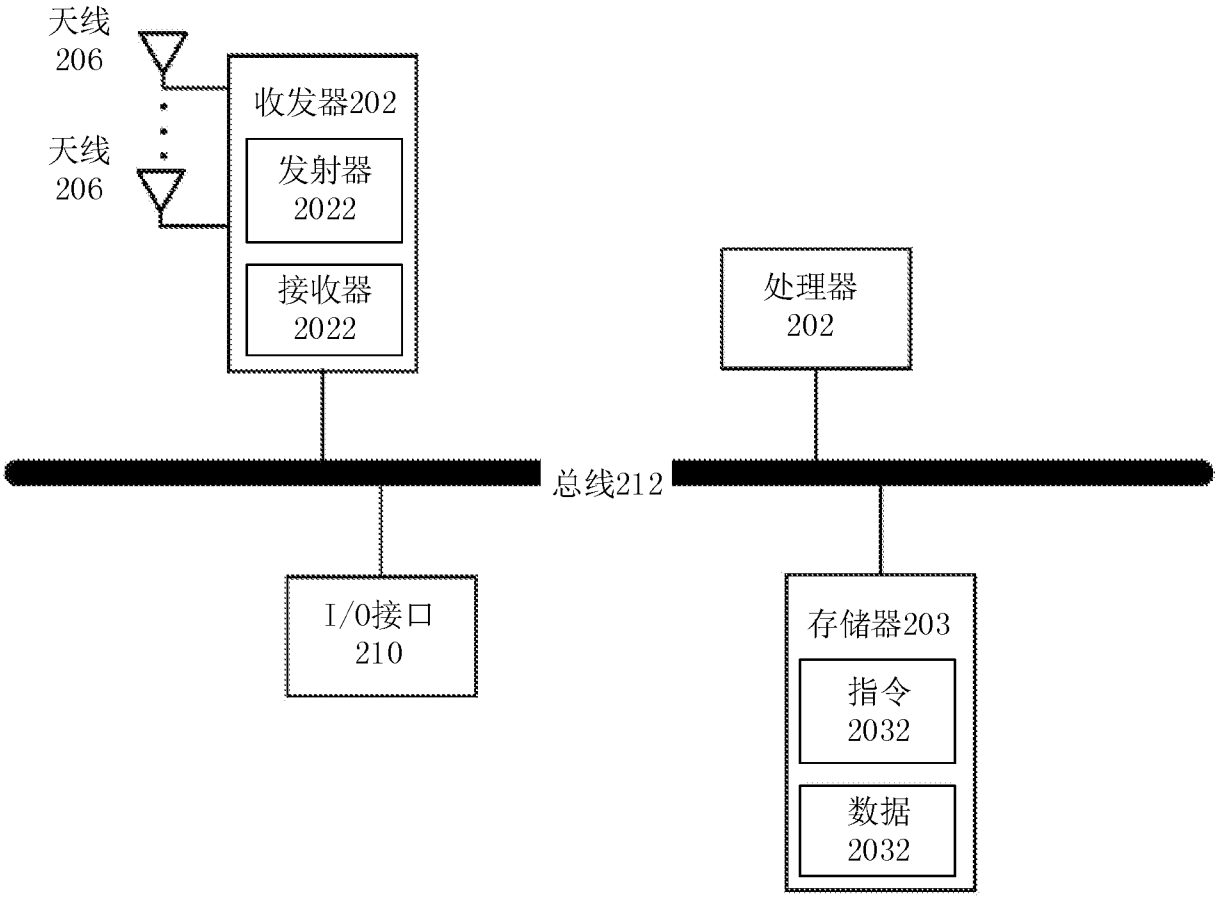

天线
206
天线
206
收发器202
发射器
2022
接收器
2022
处理器
202
总线212
I/O接口
210
存储器203
指令
2032
数据
2032

图 2

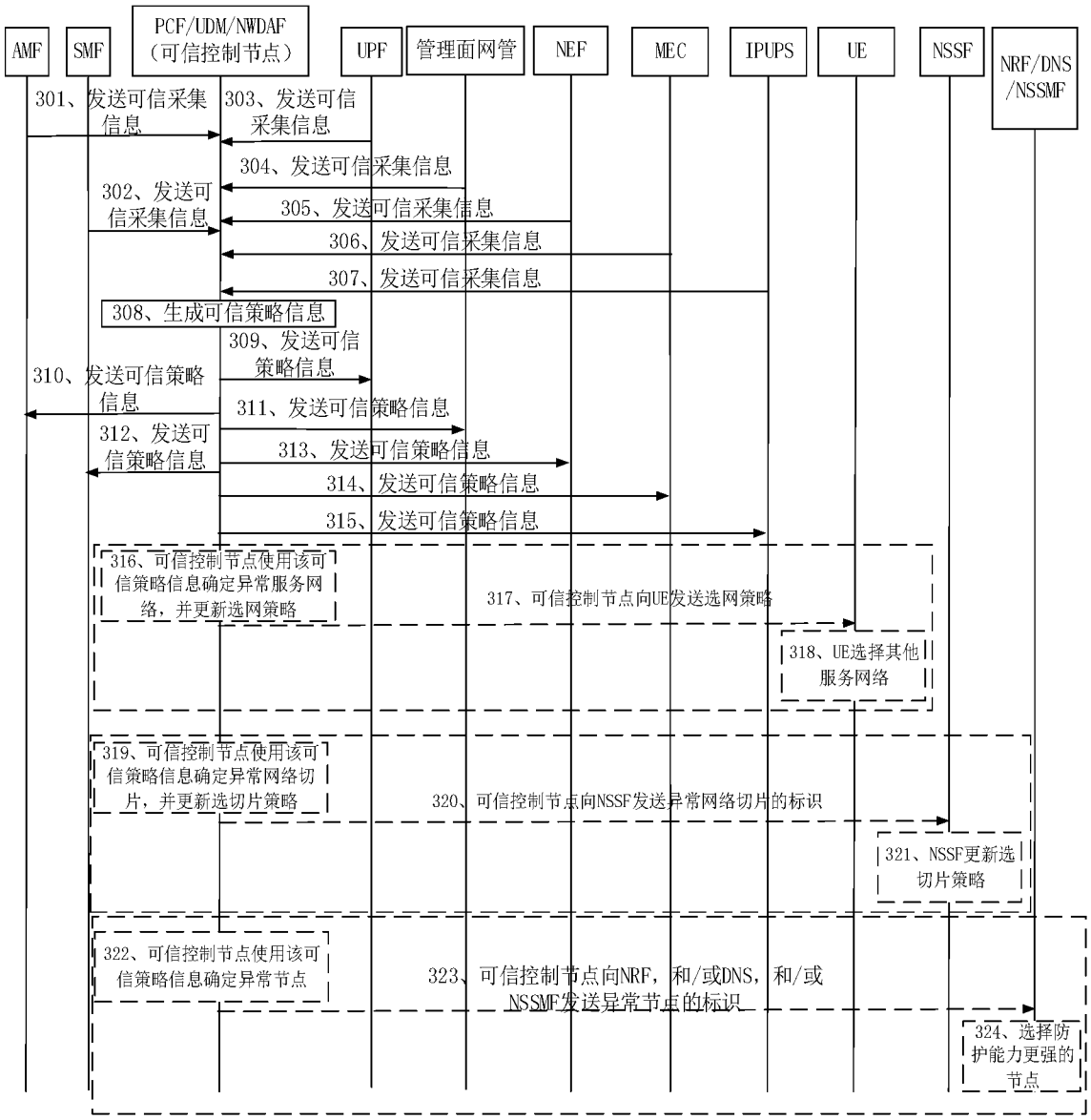

AMF
SMF
PCF/UDM/NWDAF
（可信控制节点）
UPF
管理面网管
NEF
MEC
IPUPS
UE
NSSF
NRF/DNS
/NSSMF
301、发送可信采集信息
303、发送可信采集信息
304、发送可信采集信息
302、发送可信采集信息
305、发送可信采集信息
306、发送可信采集信息
307、发送可信采集信息
308、生成可信策略信息
309、发送可信策略信息
310、发送可信策略信息
311、发送可信策略信息
312、发送可信策略信息
313、发送可信策略信息
314、发送可信策略信息
315、发送可信策略信息
316、可信控制节点使用该可信策略信息确定异常服务网络，并更新选网策略
317、可信控制节点向UE发送选网策略
318、UE选择其他服务网络
319、可信控制节点使用该可信策略信息确定异常网络切片，并更新选切片策略
320、可信控制节点向NSSF发送异常网络切片的标识
321、NSSF更新选切片策略
322、可信控制节点使用该可信策略信息确定异常节点
323、可信控制节点向NRF，和/或DNS，和/或NSSMF发送异常节点的标识
324、选择防护能力更强的节点

图 3a

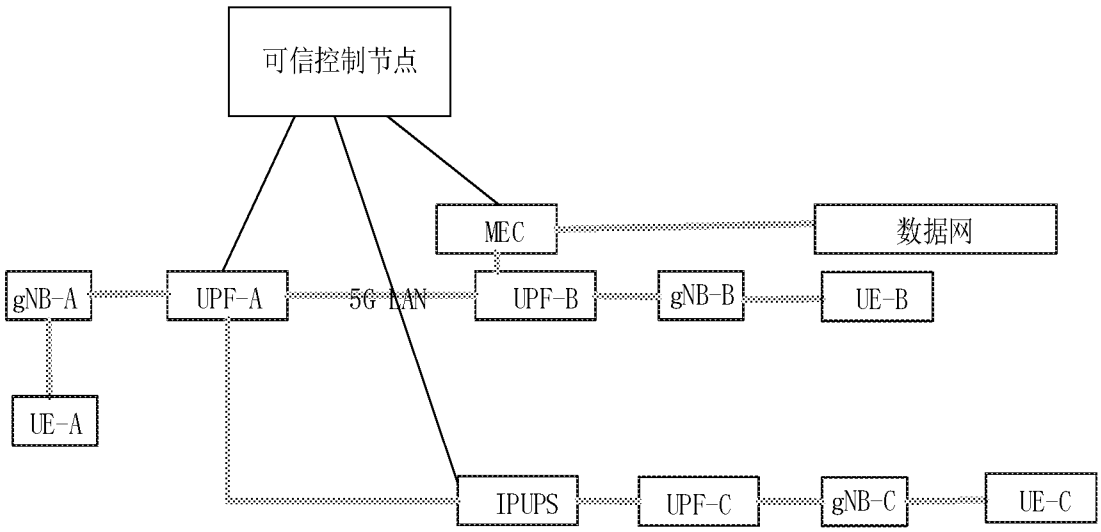

可信控制节点
MEC
数据网
gNB-A
UPF-A
5G LAN
UPF-B
gNB-B
UE-B
UE-A
IPUPS
UPF-C
gNB-C
UE-C

图 3b

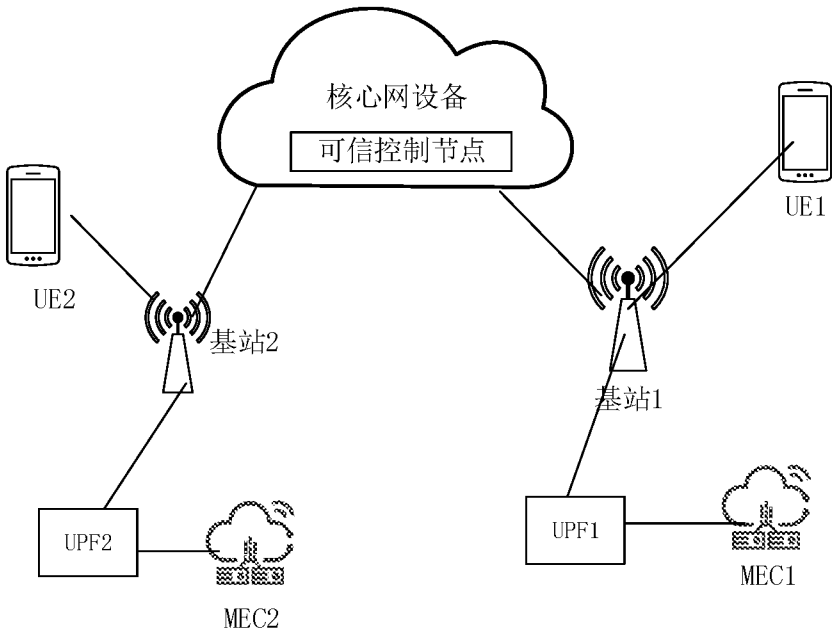

核心网设备
可信控制节点
UE1
UE2
基站2
基站1
UPF2
MEC2
UPF1
MEC1

图 3c

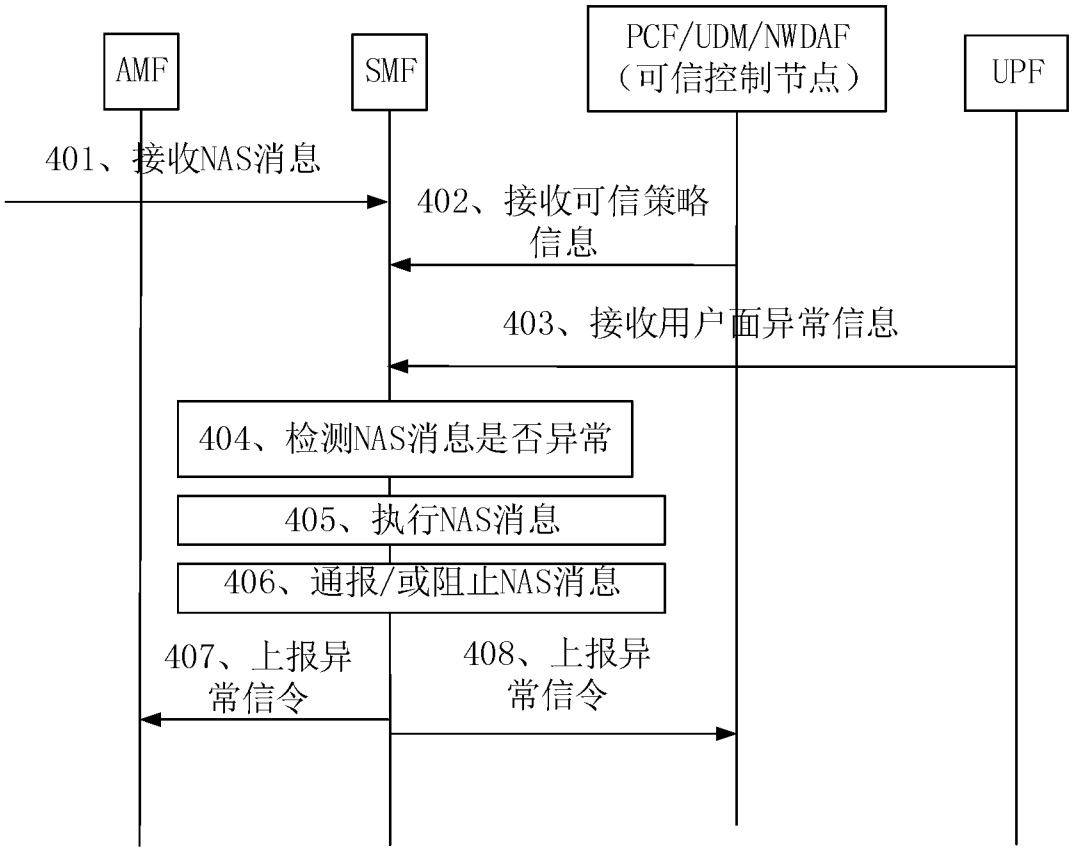

AMF
SMF
PCF/UDM/NWDAF
（可信控制节点）
UPF
401、接收NAS消息
402、接收可信策略信息
403、接收用户面异常信息
404、检测NAS消息是否异常
405、执行NAS消息
406、通报/或阻止NAS消息
407、上报异常信令
408、上报异常信令

图 4

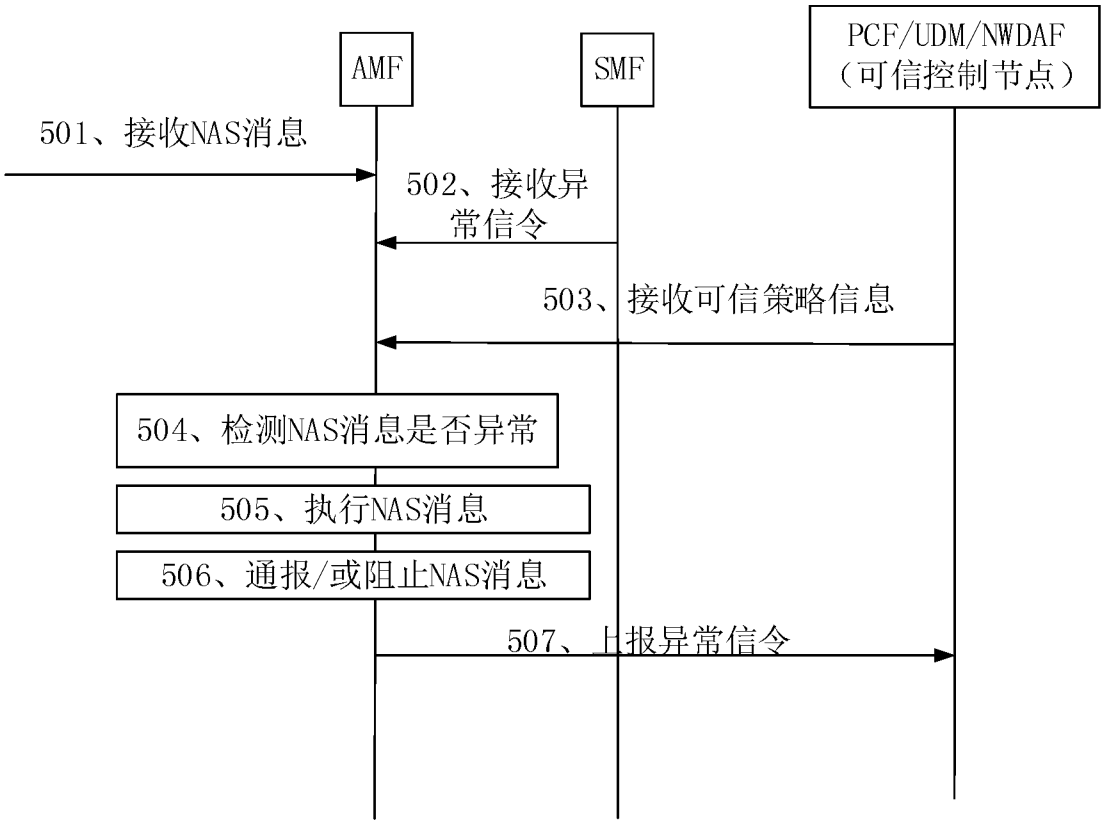

AMF
SMF
PCF/UDM/NWDAF
（可信控制节点）
501、接收NAS消息
502、接收异常信令
503、接收可信策略信息
504、检测NAS消息是否异常
505、执行NAS消息
506、通报/或阻止NAS消息
507、上报异常信令

图 5

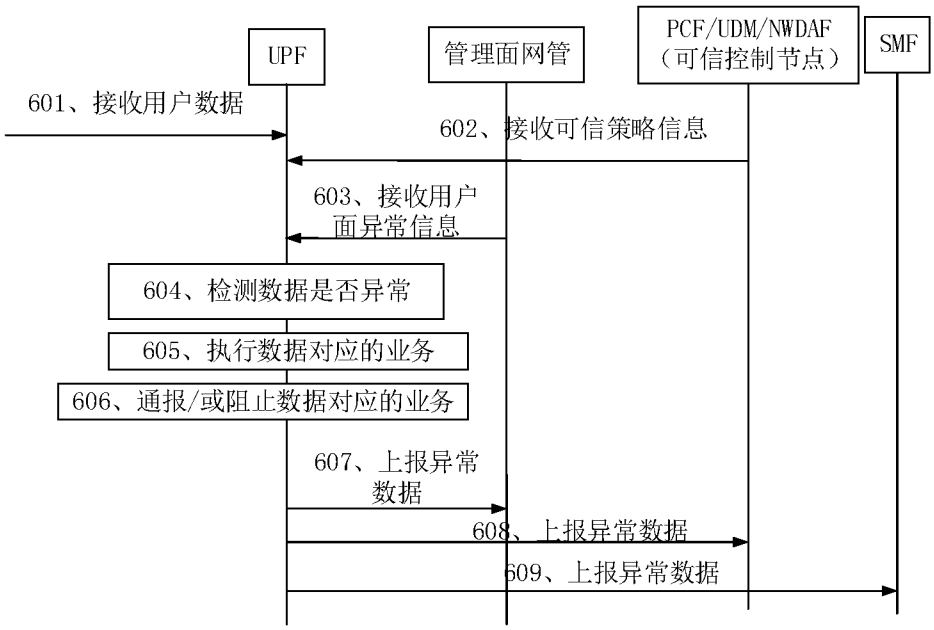

UPF
管理面网管
PCF/UDM/NWDAF
（可信控制节点）
SMF
601、接收用户数据
602、接收可信策略信息
603、接收用户面异常信息
604、检测数据是否异常
605、执行数据对应的业务
606、通报/或阻止数据对应的业务
607、上报异常数据
608、上报异常数据
609、上报异常数据

图 6

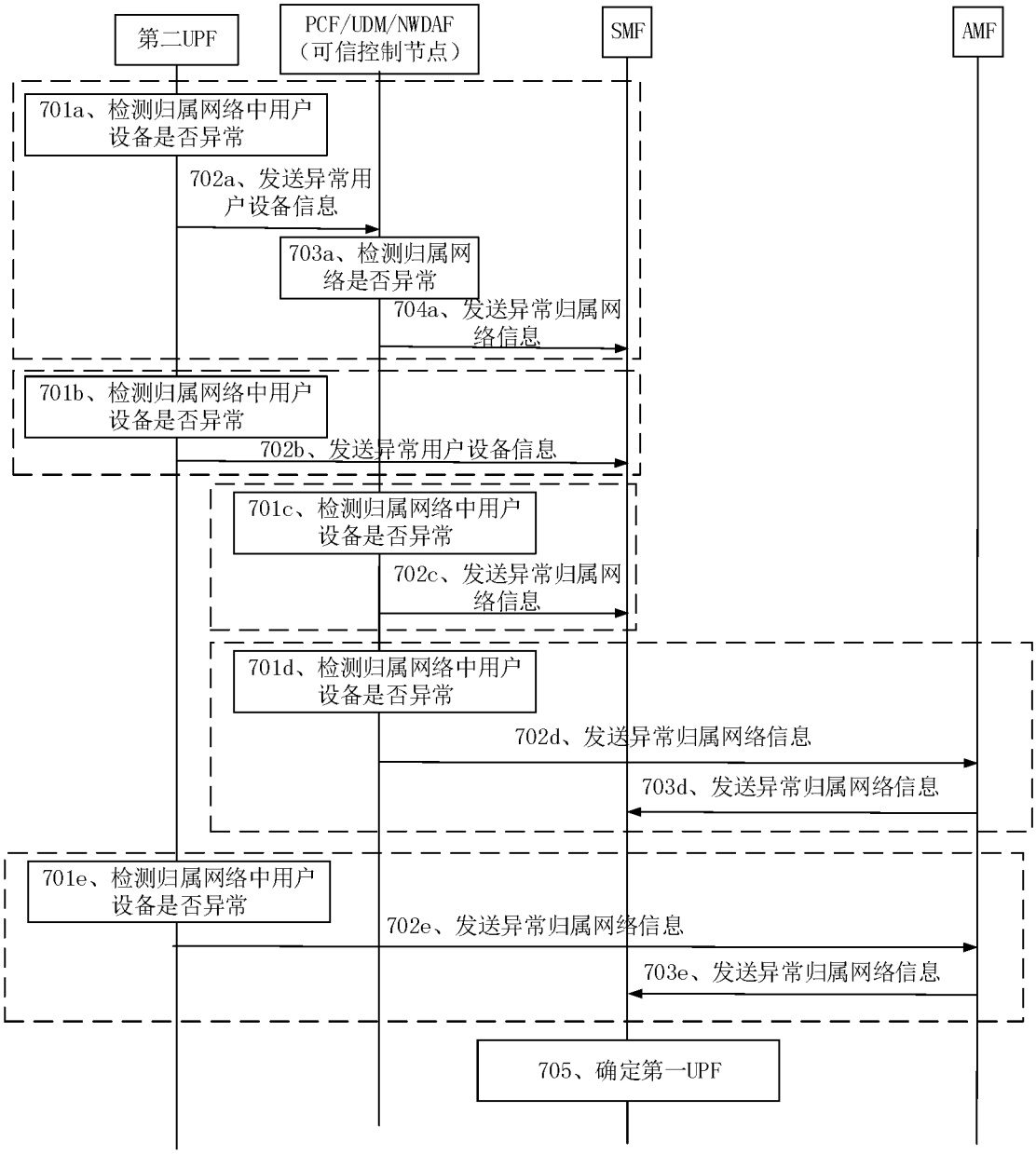

第二UPF
PCF/UDM/NWDAF
（可信控制节点）
SMF
AMF
701a、检测归属网络中用户设备是否异常
702a、发送异常用户设备信息
703a、检测归属网络是否异常
704a、发送异常归属网络信息
701b、检测归属网络中用户设备是否异常
702b、发送异常用户设备信息
701c、检测归属网络中用户设备是否异常
702c、发送异常归属网络信息
701d、检测归属网络中用户设备是否异常
702d、发送异常归属网络信息
703d、发送异常归属网络信息
701e、检测归属网络中用户设备是否异常
702e、发送异常归属网络信息
703e、发送异常归属网络信息
705、确定第一UPF

图 7a

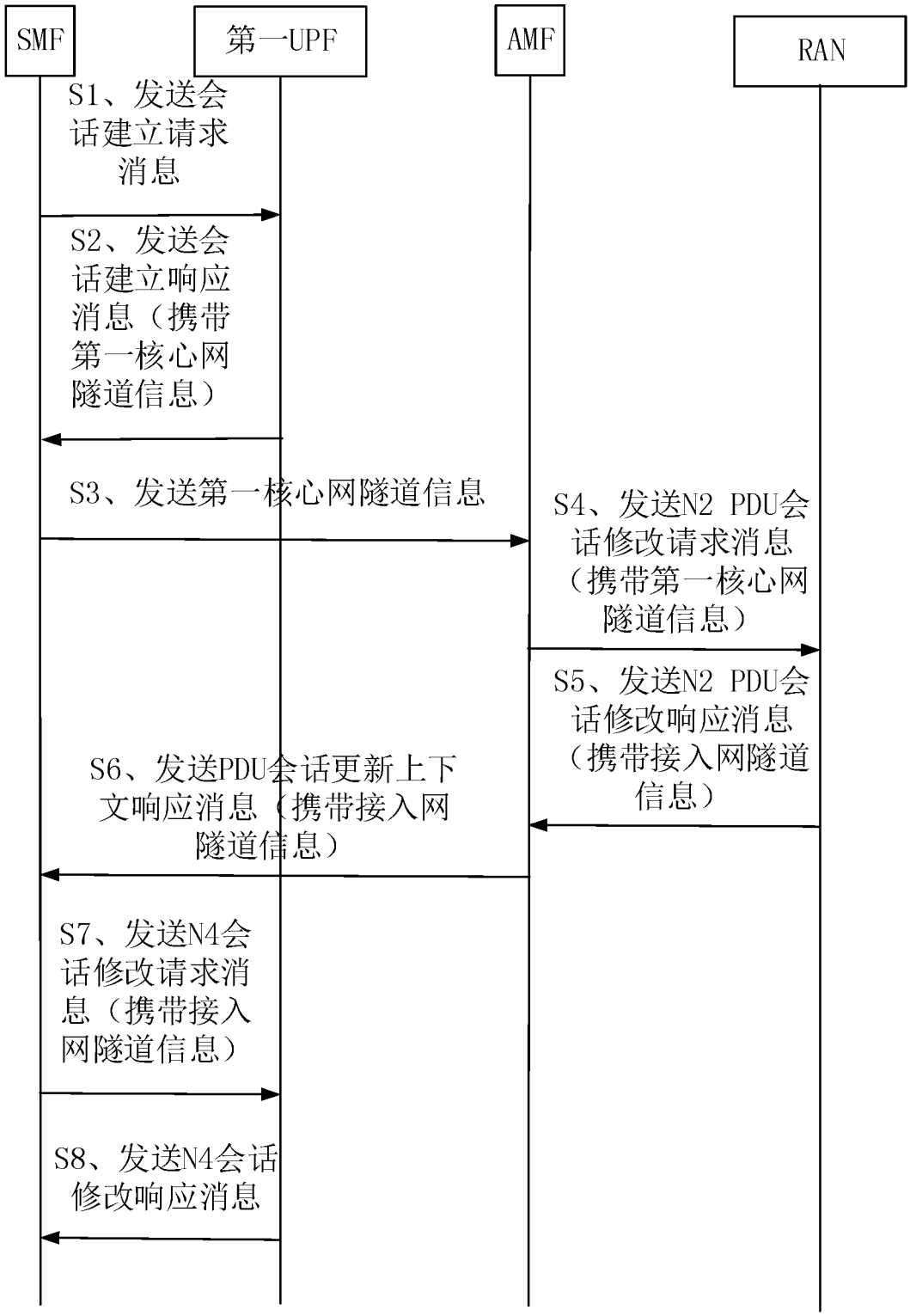

SMF
第一UPF
AMF
RAN
S1、发送会话建立请求消息
S2、发送会话建立响应消息（携带第一核心网隧道信息）
S3、发送第一核心网隧道信息
S4、发送N2 PDU会话修改请求消息（携带第一核心网隧道信息）
S5、发送N2 PDU会话修改响应消息（携带接入网隧道信息）
S6、发送PDU会话更新上下文响应消息（携带接入网隧道信息）
S7、发送N4会话修改请求消息（携带接入网隧道信息）
S8、发送N4会话修改响应消息

图 7b

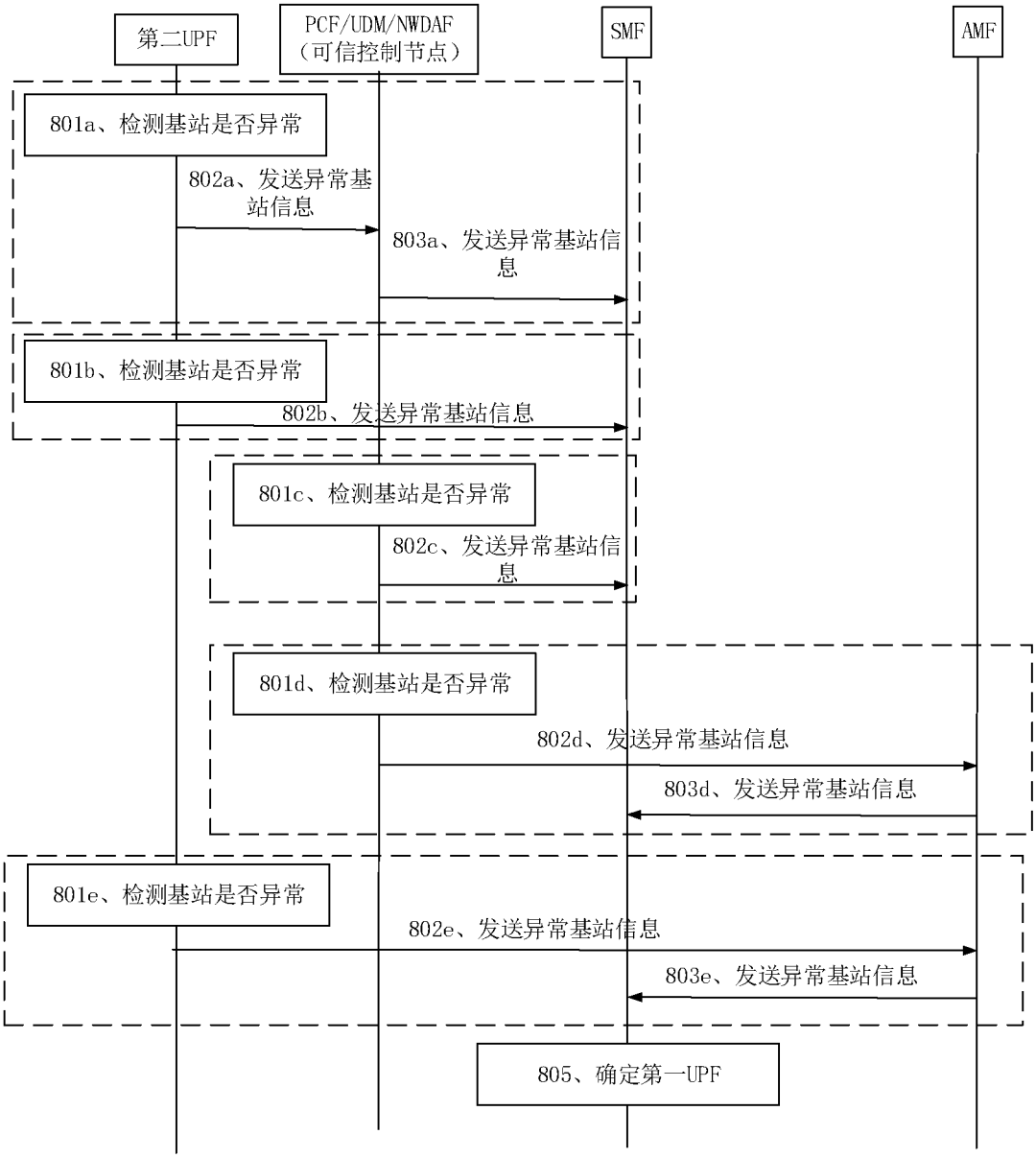

第二UPF
PCF/UDM/NWDAF
（可信控制节点）
SMF
AMF
801a、检测基站是否异常
802a、发送异常基站信息
803a、发送异常基站信息
801b、检测基站是否异常
802b、发送异常基站信息
801c、检测基站是否异常
802c、发送异常基站信息
801d、检测基站是否异常
802d、发送异常基站信息
803d、发送异常基站信息
801e、检测基站是否异常
802e、发送异常基站信息
803e、发送异常基站信息
805、确定第一UPF

图 8a

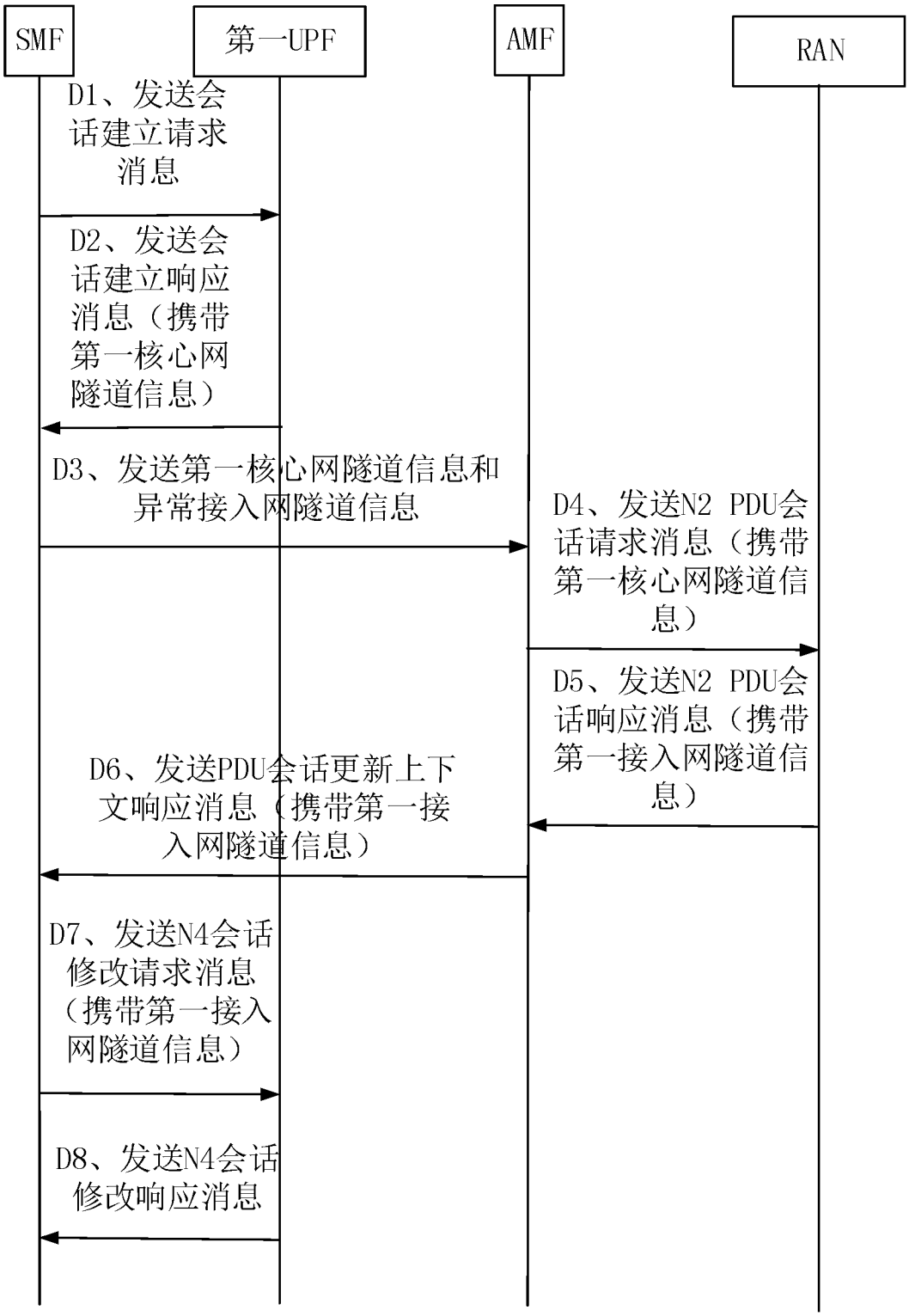

SMF
第一UPF
AMF
RAN
D1、发送会话建立请求消息
D2、发送会话建立响应消息（携带第一核心网隧道信息）
D3、发送第一核心网隧道信息和异常接入网隧道信息
D4、发送N2 PDU会话请求消息（携带第一核心网隧道信息）
D5、发送N2 PDU会话响应消息（携带第一接入网隧道信息）
D6、发送PDU会话更新上下文响应消息（携带第一接入网隧道信息）
D7、发送N4会话修改请求消息（携带第一接入网隧道信息）
D8、发送N4会话修改响应消息

图 8b

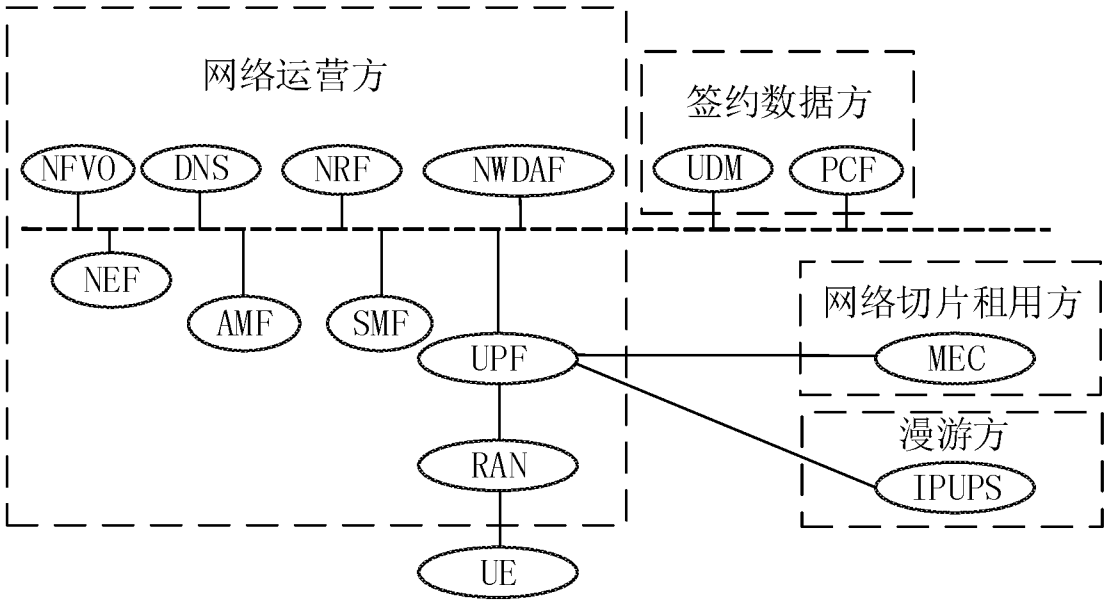

网络运营方
签约数据方
NFVO
DNS
NRF
NWDAF
UDM
PCF
NEF
AMF
SMF
UPF
网络切片租用方
MEC
漫游方
RAN
IPUPS
UE

图 9a

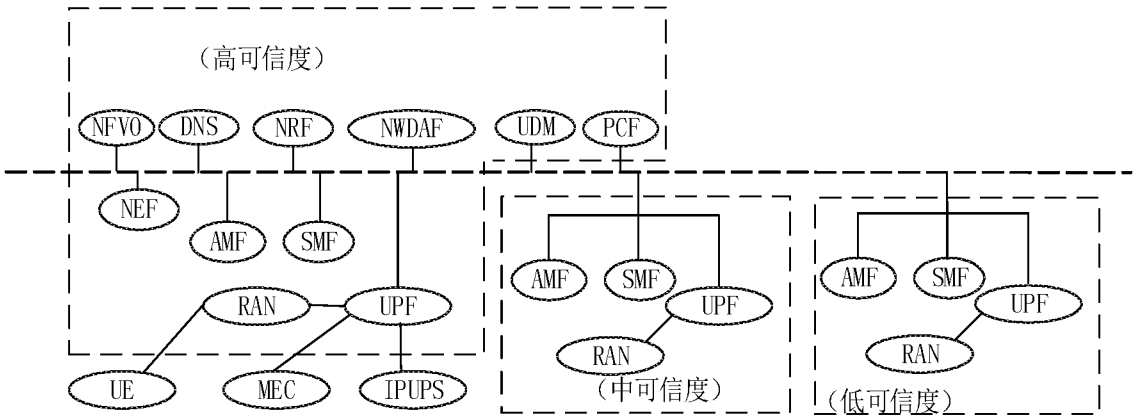

（高可信度）
NFVO
DNS
NRF
NWDAF
UDM
PCF
NEF
AMF
SMF
RAN
UPF
UE
MEC
IPUPS
AMF
SMF
UPF
RAN
（中可信度）
AMF
SMF
UPF
RAN
（低可信度）

图 9b

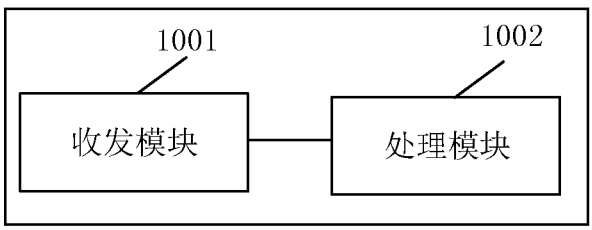

1001
1002
收发模块
处理模块

图 10

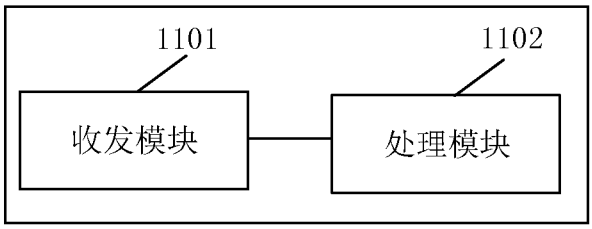


图 11

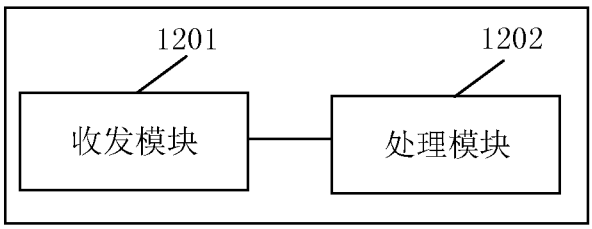


图 12

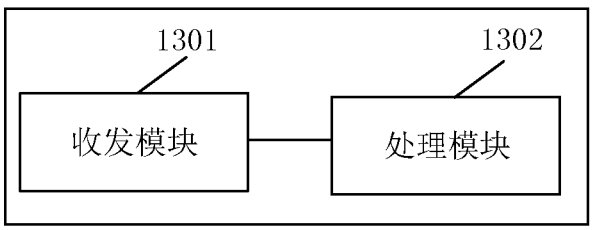


图 13

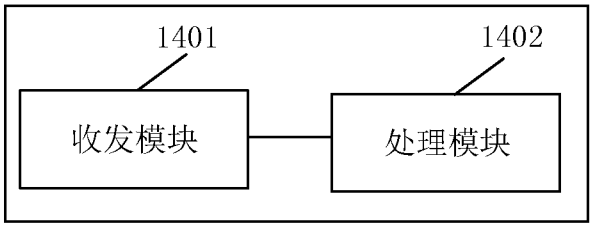


图 14

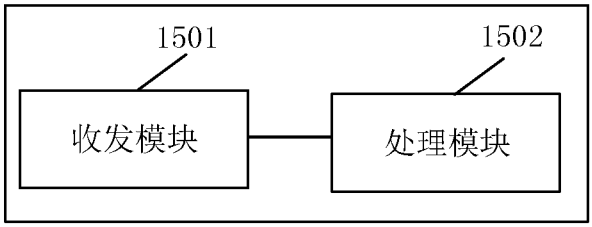


图 15

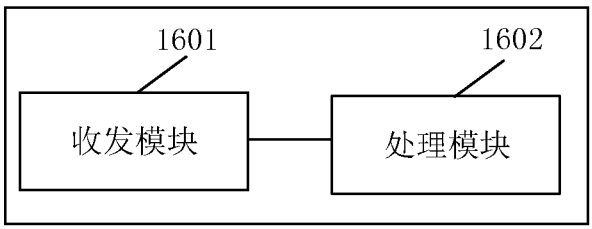


图 16

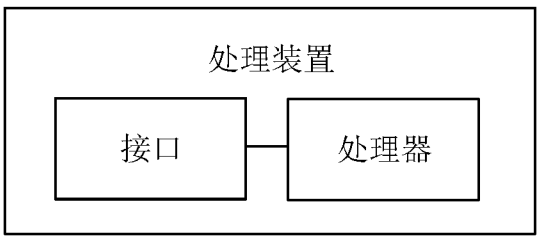


图 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/105890

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)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)

H04L; H04W

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)

WPI; EPODOC; CNPAT; CNKI; 3GPP: AMF, SMF, PCF, UDM, AF, NEF, NWDAF, Analytics, risk, polici+, Abnormal, behaviour, 可信, 策略, 异常, 分析, 报告, 上报, 采集, 阻止, 攻击

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	3GPP. "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for 5G System (5GS) to supportnetwork data analytics services(Release 16)" *3GPP TS 23.288 V16.4.0,* 09 July 2020 (2020-07-09), sections 6.5 and 6.7	1-8, 11-21, 24-29
A	3GPP. "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for 5G System (5GS) to supportnetwork data analytics services(Release 16)" *3GPP TS 23.288 V16.4.0,* 09 July 2020 (2020-07-09), sections 6.5 and 6.7	9, 10, 22, 23
A	CN 110830542 A (HUAWEI TECHNOLOGIES CO., LTD.) 21 February 2020 (2020-02-21) entire document	1-29
A	CN 110912854 A (HUAWEI TECHNOLOGIES CO., LTD.) 24 March 2020 (2020-03-24) entire document	1-29

☐ 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	Date of mailing of the international search report
08 October 2021	**14 October 2021**
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** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/105890

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110830542 A	21 February 2020	WO 2020035000 A1	20 February 2020
CN 110912854 A	24 March 2020	WO 2020052416 A1	19 March 2020
		EP 3820198 A1	12 May 2021

国际检索报告

国际申请号
PCT/CN2021/105890

A. 主题的分类

H04L 29/06(2006.01)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)

H04L; H04W

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））

WPI;EPODOC;CNPAT;CNKI;3GPP: AMF, SMF, PCF, UDM, AF, NEF, NWDAF, Analytics, risk, polici+, Abnormal, behaviour, 可信, 策略, 异常, 分析, 报告, 上报, 采集, 阻止, 攻击

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
X	3GPP. "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for 5G System (5GS) to supportnetwork data analytics services(Release 16)" 3GPP TS 23.288 V16.4.0, 2020年 7月 9日 (2020-07-09), 6.5、6.7节	1-8, 11-21, 24-29
A	3GPP. "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for 5G System (5GS) to supportnetwork data analytics services(Release 16)" 3GPP TS 23.288 V16.4.0, 2020年 7月 9日 (2020-07-09), 6.5、6.7节	9, 10, 22, 23
A	CN 110830542 A (华为技术有限公司) 2020年 2月 21日 (2020-02-21) 全文	1-29
A	CN 110912854 A (华为技术有限公司) 2020年 3月 24日 (2020-03-24) 全文	1-29

☐ 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	国际检索报告邮寄日期
2021年 10月 8日	2021年 10月 14日

ISA/CN的名称和邮寄地址	受权官员
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	张华晶
传真号 (86-10)62019451	电话号码 86-010-53961629

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/105890

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	110830542	A	2020年 2月 21日	WO	2020035000	A1	2020年 2月 20日
CN	110912854	A	2020年 3月 24日	WO	2020052416	A1	2020年 3月 19日
				EP	3820198	A1	2021年 5月 12日