(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
2025 年 7 月 3 日 (03.07.2025)

WIPO | PCT

(10) 国际公布号
WO 2025/138024 A1

(51) 国际专利分类号:
H04W 12/37 (2021.01)

(21) 国际申请号: PCT/CN2023/142889

(22) 国际申请日: 2023 年 12 月 28 日 (28.12.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: **OPPO** 广 东 移 动 通 信 有 限 公 司 **(GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.)** [CN/CN]; 中国广东省东莞市长安镇乌沙海滨路18号 523860 (CN)。

(72) 发明人: 甘露 **(GAN, Lu)**; 中国广东省东莞市长安镇乌沙海滨路18号 523860 (CN)。 付玉龙 **(FU, Yulong)**; 中国广东省东莞市长安镇乌沙海滨路18号 523860 (CN)。 曹进 **(CAO, Jin)**; 中国广东省东莞市长安镇乌沙海滨路18号 523860 (CN)。 易威 **(YI, Wei)**; 中国广东省东莞市长安镇乌沙海滨路18号 523860 (CN)。 魏腾龙 **(WEI, Tenglong)**; 中国广东省东莞市长安镇乌沙海滨路18号 523860 (CN)。 蔺如嫣 **(LIN, Ruyan)**; 中国广东省东莞市长安镇乌沙海滨路18号 523860 (CN)。 李晖 **(LI, Hui)**; 中国广东省东莞市长安镇乌沙海滨路18号 523860 (CN)。

(74) 代理人: 北京布瑞知识产权代理有限公司 **(BEIJING BRIGHT IP AGENCY CO., LTD.)**; 中国北京市昌平区七北路42号院3号楼12层3单元1202 102200 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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)。

(54) **Title:** METHOD FOR GENERATING SECURITY POLICY, AND COMMUNICATION DEVICE

(54) 发明名称: 用于生成安全策略的方法及通信设备

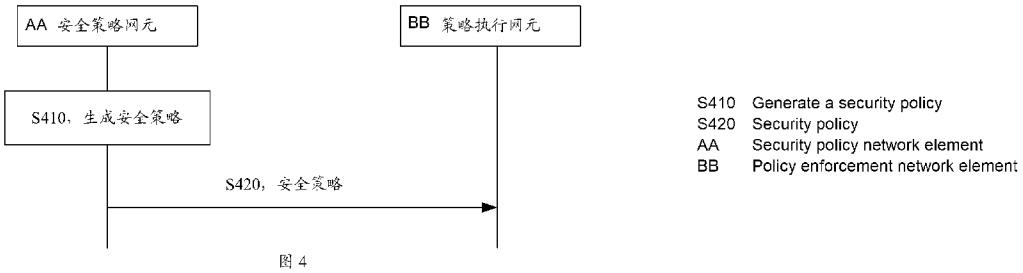

图 4

(57) **Abstract:** The present application provides a method for generating a security policy, and a communication device. The method comprises: a security policy network element generates a security policy, the security policy being associated with a service of a terminal device; and the security policy network element sends the security policy to a policy enforcement network element.

(57) 摘要: 本申请提供了一种用于生成安全策略的方法及通信设备。该方法包括：安全策略网元生成安全策略，所述安全策略与终端设备的业务相关联；所述安全策略网元向策略执行网元发送所述安全策略。

WO 2025/138024 A1

[见续页]

本国际公布:
— 包括国际检索报告(条约第21条(3))。

用于生成安全策略的方法及通信设备

技术领域

本申请涉及通信技术领域，并且更为具体地，涉及一种用于生成安全策略的方法及通信设备。

背景技术

为了保证通信系统的安全性，通信系统中的设备可以使用安全策略进行通信。安全策略可以由零信任架构中的网元（如安全策略网元）生成。

目前，安全策略网元是基于网络状态生成安全策略的。但是，随着通信系统的不断演进，这种生成方式已经不能满足通信系统的安全要求。

发明内容

本申请提供一种用于生成安全策略的方法及通信设备。下面对本申请涉及的几个方面进行详细介绍。

第一方面，提供了一种用于生成安全策略的方法，包括：安全策略网元生成安全策略，所述安全策略与终端设备的业务相关联；所述安全策略网元向策略执行网元发送所述安全策略。

第二方面，提供了一种用于生成安全策略的方法，包括：策略执行网元向第一网元发送第一请求消息，所述第一请求消息用于请求安全策略，所述安全策略与所述终端设备的业务相关联，所述第一网元包括安全策略网元和/或策略检测网元；所述策略执行网元接收来自所述安全策略网元的所述安全策略。

第三方面，提供了一种用于生成安全策略的方法，包括：策略检测网元接收来自策略执行网元的第一请求消息，所述第一请求消息用于请求安全策略；响应于所述第一请求消息，所述策略检测网元生成与所述终端设备的业务对应的安全需求；所述策略检测网元向安全策略网元发送所述安全需求，所述安全需求用于所述安全策略网元生成所述安全策略。

第四方面，提供了一种用于生成安全策略的方法，包括：终端设备向策略执行网元发送第一指示信息，所述第一指示信息用于指示所述终端设备的业务发生变化；所述终端设备接收来自所述策略执行网元的安全策略，所述安全策略与所述终端设备的业务相关联。

第五方面，提供了一种通信设备，所述通信设备为安全策略网元，所述通信设备包括：生成单元，用于生成安全策略，所述安全策略与终端设备的业务相关联；发送单元，用于向策略执行网元发送所述安全策略。

第六方面，提供了一种通信设备，所述通信设备为策略执行网元，所述通信设备包括：发送单元，用于向第一网元发送第一请求消息，所述第一请求消息用于请求安全策略，所述安全策略与所述终端设备的业务相关联，所述第一网元包括安全策略网元和/或策略检测网元；接收单元，用于接收来自所述安全策略网元的所述安全策略。

第七方面，提供了一种通信设备，所述通信设备为策略检测网元，所述通信设备包括：接收单元，用于接收来自策略执行网元的第一请求消息，所述第一请求消息用于请求安全策略；生成单元，用于响应于所述第一请求消息，生成与所述终端设备的业务对应的安全需求；发送单元，用于向安全策略网元发送所述安全需求，所述安全需求用于所述安全策略网元生成所述安全策略。

第八方面，提供了一种通信设备，所述通信设备为终端设备，所述通信设备包括：发送单元，用于向策略执行网元发送第一指示信息，所述第一指示信息用于指示所述终端设备的业务发生变化；接收单元，用于接收来自所述策略执行网元的安全策略，所述安全策略与所述终端设备的业务相关联。

随着通信系统的不断演进，通信系统中的业务场景也越来越丰富，本申请可以生成与终端设备的业务相关联的安全策略，使得生成的安全策略能够与终端设备的业务相匹配，以满足通信系统的安全要求。

附图说明

图 1 是本申请实施例应用的无线通信系统 100。

图 2 是一种传统的零信任架构的结构示意图。

图 3 是一种智能零信任架构的结构示意图。

图 4 是本申请实施例提供的一种用于生成安全策略的示意性流程图。

图 5 是本申请实施例提供的另一种用于生成安全策略的示意性流程图。

图 6 是本申请实施例提供的另一种用于生成安全策略的示意性流程图。

图 7 是本申请实施例提供的另一种用于生成安全策略的示意性流程图。

图 8 是本申请实施例提供的一种零信任架构的结构示意图。

图 9 是本申请实施例提供的另一种零信任架构的结构示意图。
图 10 是本申请实施例提供的一种生成安全策略的示意性流程图。
图 11 是本申请实施例提供的另一种生成安全策略的示意性流程图。
图 12 是本申请实施例提供的一种通信设备的示意性框图。
图 13 是本申请实施例提供的另一种通信设备的示意性框图。
图 14 是本申请实施例提供的另一种通信设备的示意性框图。
图 15 是本申请实施例提供的另一种通信设备的示意性框图。

具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

图 1 是本申请实施例应用的无线通信系统 100。该无线通信系统 100 可以包括网络设备 110 和终端设备 120。网络设备 110 可以是与终端设备 120 通信的设备。网络设备 110 可以为特定的地理区域提供通信覆盖，并且可以与位于该覆盖区域内的终端设备 120 进行通信。

图 1 示例性地示出了一个网络设备和两个终端设备，可选地，该无线通信系统 100 可以包括多个网络设备并且每个网络设备的覆盖范围内可以包括其它数量的终端设备，本申请实施例对此不做限定。

可选地，该无线通信系统 100 还可以包括网络控制器、移动管理实体等其他网络实体，本申请实施例对此不作限定。

应理解，本申请实施例的技术方案可以应用于各种通信系统，例如：第五代（5th generation，5G）系统或新无线（new radio，NR）、长期演进（long term evolution，LTE）系统、LTE 频分双工（frequency division duplex，FDD）系统、LTE 时分双工（time division duplex，TDD）等。本申请提供的技术方案还可以应用于未来的通信系统，如第六代移动通信系统，又如卫星通信系统，等等。

本申请实施例中的终端设备也可以称为用户设备（user equipment，UE）、接入终端、用户单元、用户站、移动站、移动台（mobile station，MS）、移动终端（mobile terminal，MT）、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置。本申请实施例中的终端设备可以是指向用户提供语音和/或数据连通性的设备，可以用于连接人、物和机，例如具有无线连接功能的手持式设备、车载设备等。本申请的实施例中的终端设备可以是手机（mobile phone）、平板电脑（Pad）、笔记本电脑、掌上电脑、移动互联网设备（mobile internet device，MID）、可穿戴设备，虚拟现实（virtual reality，VR）设备、增强现实（augmented reality，AR）设备、工业控制（industrial control）中的无线终端、无人驾驶（self driving）中的无线终端、远程手术（remote medical surgery）中的无线终端、智能电网（smart grid）中的无线终端、运输安全（transportation safety）中的无线终端、智慧城市（smart city）中的无线终端、智慧家庭（smart home）中的无线终端等。可选地，UE 可以用于充当基站。例如，UE 可以充当调度实体，其在车辆外联（vehicle-to-everything，V2X）或设备到设备（device to device，D2D）等中的 UE 之间提供侧行链路信号。比如，蜂窝电话和汽车利用侧行链路信号彼此通信。蜂窝电话和智能家居设备之间通信，而无需通过基站中继通信信号。

本申请实施例中的网络设备可以是用于与终端设备通信的设备，该网络设备也可以称为接入网设备或无线接入网设备，如网络设备可以是基站。本申请实施例中的网络设备可以是指将终端设备接入到无线网络的无线接入网（radio access network，RAN）节点（或设备）。基站可以广义的覆盖如下中的各种名称，或与如下名称进行替换，比如：节点 B （NodeB）、演进型基站（evolved NodeB，eNB）、下一代基站（next generation NodeB，gNB）、中继站、传输点（transmitting and receiving point，TRP）、发射点(transmitting point，TP)、主站 MeNB、辅站 SeNB、多制式无线（MSR）节点、家庭基站、网络控制器、接入节点、无线节点、接入点（access point，AP）、传输节点、收发节点等。基站可以是宏基站、微基站、中继节点、施主节点或类似物，或其组合。基站还可以指用于设置于前述设备或装置内的通信模块、调制解调器或芯片。基站还可以是移动交换中心以及设备到设备 D2D、V2X、机器到机器（machine-to-machine，M2M）通信中承担基站功能的设备、6G 网络中的网络侧设备、未来的通信系统中承担基站功能的设备等。基站可以支持相同或不同接入技术的网络。本申请的实施例对网络设备所采用的具体技术和具体设备形态不做限定。

基站可以是固定的，也可以是移动的。例如，直升机或无人机可以被配置成充当移动基站，一个或多个小区可以根据该移动基站的位置移动。在其他示例中，直升机或无人机可以被配置成用作与另一基站通信的设备。

在一些部署中，本申请实施例中的网络设备可以是指 CU 或者 DU，或者，网络设备包括 CU 和 DU。gNB 还可以包括 AAU。

网络设备和终端设备可以部署在陆地上，包括室内或室外、手持或车载；也可以部署在水面上；还

可以部署在空中的飞机、气球或卫星上。本申请实施例中对网络设备和终端设备所处的场景不做限定。

应理解，本申请中的通信设备的全部或部分功能也可以通过在硬件上运行的软件功能来实现，或者通过平台（例如云平台）上实例化的虚拟化功能来实现。

零信任架构

零信任架构（zero trust architecture，ZTA）可以为美国国家标准与技术研究院（national institute of standards and technology，NIST）零信任架构。零信任架构的目的是确保网络资源的安全访问，通过实施严格的访问控制和监控，以响应不断变化的威胁环境。这种架构的设计旨在提高安全性，减少对传统网络边界的依赖，并确保即使在高度动态和分散的网络环境中也能保持数据和资源的安全。零信任架构的理念是：网络中的每个请求都不被默认信任、每次访问都需要经过严格的授权和监控。

参见图 2，NIST 零信任架构中的网元或组件可以包括策略引擎（policy engine，PE）、策略管理员（policy administrator，PA）以及策略执行点（policy enforcement point，PEP）。

策略引擎负责对给定主体的资源访问进行最终决策。策略引擎可以根据企业策略以及来自外部来源（如连续诊断和缓解（continuous diagnostics and mitigation，CDM）系统、威胁情报服务）的输入作为信任算法的输入，以授予、拒绝或撤销对资源的访问。策略引擎和策略管理员可以相互配合使用。策略引擎可以进行决策并记录决策结果（批准或拒绝），策略管理员可以执行决策。

策略管理员可以负责在主体和资源之间建立和/或关闭通信路径。例如，策略管理员可以向策略执行点发送命令，以建立或关闭主体与资源之间的通信路径。在一些实现方式中，策略管理员可以通过与策略执行点通信，以创建通信路径。策略管理员与策略执行点之间的通信可以通过控制平面进行。

策略管理员可以生成每个会话特定的身份验证令牌或凭证，客户端可以使用该令牌或凭证来访问企业资源。策略管理员与策略引擎密切相关，策略管理员可以基于策略引擎的决策来允许或拒绝会话。如果会话经过授权并且请求经过身份验证，则策略管理员可以向策略执行点发送命令，以允许会话开始。如果会话被拒绝或之前的批准被撤销，则策略管理员可以向策略执行点发送命令以关闭连接。

在一些实现方式中，策略管理员和策略引擎为两个独立的组件，或者，策略管理员和策略引擎集成在一个组件上。

策略执行点可以负责启用、监控以及中止主体与资源之间的连接。策略执行点可以与策略管理员进行通信。策略执行点可以转发请求和/或从策略管理员接收策略更新。

在零信任架构中，策略执行点为一个单一的逻辑组件，但是策略执行点也可以划分为两个组件。例如，策略执行点可以包括客户端和资源端。客户端例如可以为终端设备上的代理，资源端例如可以为控制访问的资源前端网关组件。

上述组件可以通过一个分离的控制平面进行通信，而应用数据可以在数据平面进行传输。

继续参见图 2，零信任架构还可以包括其他的组件。例如，零信任架构还可以包括以下组件中的一种或多种：CDM 系统、行业合规系统、威胁情报源、网络和系统活动日志、数据访问策略、身份管理系统、安全信息和事件管理（security information and event management，SIEM）系统、企业公钥基础设施（public key infrastructure，PKI）。

智能零信任架构

参见图 3，智能零信任架构（intelligent zero trust architecture，i-ZTA）中的组件可以包括智能策略引擎（intelligent policy engine, IPE）和智能代理门户（intelligent agent portal, IAP）。

IPE 可以负责动态授权访问请求。IPE 可以使用强化学习算法来最大化保证分数，即评估和调整信任策略，以响应实时观察到的用户或设备的行为、网络资源访问事件以及新检测到的异常行为。IAP 可以支持联合学习（federated learning，FL），联合学习方法为一种分布式的学习方法，可以在多个代理之间共享和更新模型，以此来提供一个全面的网络环境模型。

继续参见图 3，智能零信任架构还可以包括智能网络安全状态分析（Intelligent Network Security State Analysis，INSSA）。INSSA 使用图神经网络（graph neural network，GNN）对网络进行建模，并采用对抗学习进行风险评估。这种方法能够动态监测网络资产的安全状态，并实时评估它们是否符合安全政策规则。

智能零信任架构的运作流程涉及多个交互层面。当一个设备或用户尝试访问网络资源时，IPE 会评估该请求，并根据当前的网络环境和历史行为数据决定是否授权。如果设备缺乏计算能力，IAP 会介入，通过联合学习机制来评估和处理请求。同时，INSSA 持续监控网络状态，确保所有通信行为都符合安全策略。这些组件的相互作用确保了即使在网络环境发生变化时，安全策略也能实时更新和执行。

通信系统架构

随着技术的发展，人们对通信系统的要求越来越高，一方面希望通信系统能够实现更高的系统性能，另一方面还希望通信系统为一个极简的系统，以降低部署和运营成本。一种可行的解决方案是：在一个

极简的共性技术核心上，设计多个子系统，多个子系统之间可以解绑，且多个子系统可以各自优化，从而实现一个“能力按需分配、功能灵活组合”的“极简多能”的通信系统。

上述通信系统可以由一个最小化的极简核心提供共性能力，如提供内生智能策略、安全、灵活频谱管理等能力。

上述通信系统可以针对四个能力方向做专门优化，这四个能力方向包括：云连接（clouding）、关键物联（critical IoT）、泛在物联（ubiquitous IoT）和感知（sensing）。

在每个能力方向上可以设计一个或多个子系统。在一些实现方式中，可以根据应用场景、频谱、接口类型等，选择对应的关键技术，并分别进行硬件系统设计。例如，子系统可以包括以下中的一种或多种子系统：宽带蜂窝、D2D、高可靠低时延通信（ultra reliable low latency communication，URLLC）、定位与感知、大规模物联网和空天通信等。

子系统之间可以按需选择是否保持空口兼容性，按需确定与宽带蜂窝子系统共用空口技术与硬件设计的程度。

上述通信系统可以黑箱化、专业化的人工智能（artificial intelligence，AI）算法库替代通用而复杂的传统软件算法，实现各个子系统的“相对独立、各自优化”和通信协议的大幅简化。通过多种 AI 算法的切换和组合，实现多个子系统的切换和组合。

上述通信系统可以适用于任意一种通信系统，如 6G 系统或未来的通信系统等。

为了保证通信系统的安全性，通信系统中的设备可以使用安全策略进行通信。安全策略可以由零信任架构中的网元生成。例如，安全策略可以由 PE 生成。另外，在需要更新安全策略的情况下，PE 可以对安全策略进行更新。

一些通信系统（如 6G 系统）引入了各种各样的业务。例如，通信系统中的业务场景可以包括智慧家庭、智能穿戴设备、零功耗设备、通感互联网、孪生体域网、智能交互、智赋农业、智赋工业、超能交通、精准医疗、普智教育、虚拟畅游、即时抢险、“无人区”探测等。丰富的业务场景也对通信系统的安全性提出了新的挑战。目前，零信任架构中的安全策略与业务数据融合度不足，已经不能满足通信系统中不同业务的安全需求。

以 6G 系统为例，6G 网络环境预期将实现对业务数据与网络状态的深度感知，而这需要安全策略能够与实时业务数据和网络状态信息无缝融合，以实现精准的风险评估与策略部署。ZTA 和 i-ZTA 虽然考虑到数据驱动的安全策略实施，但尚未完全实现与 6G 网络环境中丰富的业务数据和网络状态信息的深入整合。因此，在快速变化的网络环境中，目前的安全策略可能无法充分利用实时数据进行有效的风险预测和应对，导致安全响应不够精确或者安全响应的时效性不足，未能充分发挥数据驱动安全策略的潜力。

针对 NIST 零信任架构，安全策略的生成或更新依赖于预设条件和人工干预，在安全策略的部署和调整上显示出被动和滞后的特点，无法满足动态变化的业务需求。例如，只有在满足预设条件的情况下，才会更新安全策略或生成新的安全策略。又例如，在需要更新安全策略的情况下，都是采用人工手动进行更新。虽然 i-ZTA 引入了智能化组件，但是 i-ZTA 并没有与业务数据相融合，而仅是基于网络环境的变化来更新安全策略。

为了解决上述问题中的一个或多个，本申请实施例提供一种用于生成安全策略的方法，通过将安全策略与终端设备的业务相关联，在生成安全策略时，可以生成与终端设备的业务相关联的安全策略，从而可以满足通信系统中不同业务的安全需求。

下面结合图 4，对本申请实施例的方案进行详细介绍。

参见图 4，在步骤 S410，安全策略网元生成安全策略。安全策略网元例如可以为 PE。在一些实施例中，安全策略网元可以为 AI Sec PE。

需要说明的是，在一些实现方式中，安全策略网元也可以替换为其他的术语，如安全策略网元可以替换为策略引擎或策略引擎网元等。

在一些实施例中，安全策略可以与终端设备的业务相关联。例如，安全策略网元可以基于终端设备的业务，生成与该业务对应的安全策略。在一些实现方式中，不同的业务可以对应不同的安全策略。当然，不同的业务也可以对应相同的安全策略，本申请实施例对此不做具体限定。本申请实施例通过将业务数据与安全策略进行融合，可以实现精准的风险评估与策略部署。

在一些实现方式中，安全策略可以基于终端设备的业务变化进行更新，以提高安全策略的实时性。例如，安全策略网元可以在终端设备的业务发生变化的情况下，更新安全策略。通过由终端设备的业务变化来触发安全策略的更新，使得安全策略可以实时响应业务的变化，满足通信系统对时延的要求。以 6G 系统为例，6G 网络预期将支持更高的数据速率和更低的延迟，这意味着网络环境和业务需求将更加动态和多变。本申请实施例通过基于终端设备业务的变化对安全策略进行更新，能够实时响应业务的动

态变化，生成与终端设备的业务对应的安全策略。

终端设备的业务是否发生变化可以由策略执行网元进行检测。在一些实施例中，策略执行网元可以检测终端设备的业务是否发生变化，在终端设备的业务发生变化的情况下，策略执行网元可以向安全策略网元发送指示信息，以指示终端设备的业务发生变化。在一些实现方式中，在终端设备的业务发生变化的情况下，策略执行网元可以向安全策略网元发送第一请求消息（如图 5 中的步骤 S510），该第一请求消息用于请求安全策略。安全策略网元接收到第一请求消息后，可以生成安全策略。

本申请实施例对策略执行网元不做具体限定，策略执行网元也可以称为业务功能网元。策略执行网元可以为 PEP。在一些实现方式中，策略执行网元可以包括以下中的一种或多种：应用功能（application function，AF），网络开放功能（network exposure function，NEF），网络存储功能（network repository function，NRF），策略控制功能（policy control function，PCF），接入与移动管理功能（access and mobility management function，AMF），认证服务功能（authentication server function，AUSF），基站，用户平面功能（user plane function，UPF），边缘节点等。

在一些实施例中，安全策略可以基于网络状态的变化进行更新。例如，安全策略网元可以在网络状态发生变化的情况下，更新安全策略或生成新的安全策略。通过将安全策略与网络状态信息相融合，可以实现精准的风险评估和策略部署。

在一些实现方式中，策略执行网元可以通过策略管理网元向安全策略网元发送第一请求消息。例如，策略执行网元可以向策略管理网元发送第一请求消息，策略管理网元接收到第一请求消息后，可以将第一请求消息转发至安全策略网元。

本申请实施例中的策略管理网元可以为 PA。

本申请实施例对策略执行网元确定终端设备的业务是否发生变化的方式不做具体限定。作为一个示例，策略执行网元可以对终端设备的业务进行监测，以确定终端设备的业务是否发生变化。作为另一个示例，终端设备可以在业务发生变化的情况下，向策略执行网元发送第一指示信息，第一指示信息用于指示终端设备的业务发生变化。也就是说，策略执行网元可以基于终端设备的指示，确定终端设备的业务是否发生变化。

在一些实施例中，虽然终端设备的业务发生变化，但是变化之前的业务和变化之后的业务所需要的安全策略有可能相同，在该情况下，安全策略网元可以不生成或更新安全策略，以降低开销。也就是说，安全策略网元可以在生成安全策略之前，判断是否需要生成安全策略，例如，判断是否需要新的安全策略或判断是否需要更新安全策略。如果需要生成安全策略，则安全策略网元生成安全策略；如果不需要生成安全策略，则安全策略网元可以不生成安全策略。举例说明，如果安全策略网元判断需要新的安全策略，则安全策略网元生成新的安全策略；如果安全策略网元判断不需要新的安全策略，则安全策略网元可以不生成新的安全策略。或者，如果安全策略网元判断需要更新安全策略，则安全策略网元更新安全策略；如果安全策略网元判断不需要更新安全策略，则安全策略网元可以不更新安全策略。

在一些实施例中，业务发生变化可以包括以下情况中的一种或多种：新增了业务、当前的业务条件发生了变化。

在一些实施例中，安全策略网元可以基于第一模型生成安全策略。第一模型可以为任意一种神经网络模型。例如，第一模型可以为 AI 模型或机器学习（machine learning，ML）模型。在一些实现方式中，第一模型可以为深度森林模型。

深度森林（deep forest，DF）是一种具有级联结构的决策树集成方法，包括多粒度扫描和级联森林两个部分。其中，多粒度扫描通过设置不同粒度的滑动窗口，对原始输入特征进行扫描以生成新的特征向量；级联森林通过对上一级联的输出与原始输入特征进行处理，以生成下一级联的输入数据。本申请可以采用度量感知特征重用（measure-aware feature reuse，MAFR）和度量感知层增长（measure-aware layer growth，MALG）以实现深度森林多标签输出任务目标。其中，MAFR 基于上一级联输出的置信度来选择下一级联的输入，MALG 则根据最优评估指标确定级联层训练是否结束。由于深度森林模型的训练速度快、并且可很容易地进行并行化处理，能够处理大规模的数据集，因此，通过使用深度森林模型生成安全策略，可以提高生成安全策略的速度以及保证安全策略的准确性。

在一些实施例中，第一模型的输入参数可以包括系统类型。该系统类型可以为与终端设备的业务对应的系统类型，或者说，该系统类型可以是基于终端设备的业务确定的。通过将系统类型作为第一模型的输入参数，可以使得生成的安全策略与系统类型对应，从而能够满足不同系统的安全需求。例如，在系统类型发生变化的情况下，安全策略网元可以生成新的安全策略或更新安全策略。

在一些实现方式中，系统类型也可以称为系统能力。该系统类型例如可以为 6G 系统中的系统能力或子系统能力。

在一些实现方式中，通信系统可以包括以下一种或多种系统类型：宽带蜂窝、D2D、URLLC、定位

与感知、大规模物联网和空天通信等。在另一些实现方式中，通信系统可以包括以下一种或多种系统类型：通信感知一体化（integrated sensing and communication，ISAC）、零功耗通信、太赫兹、AI/ML、可重构智能表面（reconfigurable intelligent surface，RIS）、多输入多输出（multiple-input multiple-output，MIMO）等。

以通信系统的类型包括零功耗通信系统为例，由于零功耗通信系统的计算能力受限，因此，零功耗通信系统需要在资源受限的情况下完成安全功能，例如，安全策略需要终端设备在花费较少的资源的情况下即可完成执行。基于此，零功耗通信系统的安全策略可以包括以下子策略中的一种或多种：轻量级安全凭证管理、轻量级认证和物理层密钥保护等。

在一些实施例中，第一模型的输入参数可以包括安全需求。该安全需求可以为与终端设备的业务对应的安全需求，或者说，该安全需求可以是基于终端设备的业务确定的。通过将安全需求作为第一模型的输入参数，可以使得生成的安全策略与安全需求对应，从而可以生成不同安全需求下的安全策略。例如，在安全需求发生变化的情况下，安全策略网元可以生成新的安全策略或更新安全策略。

在一些实施例中，安全需求可以包括多个子需求。多个子需求之间可以相互组合，形成最终的安全需求。通过将安全需求划分为多个子需求，使得子需求可以根据终端设备的业务需求灵活组合，以满足终端设备的业务需求，从而使得安全策略的生成更加灵活化。

在一些实施例中，安全需求可以包括不同协议层的安全需求。例如，安全需求可以包括以下中的一种或多种：非接入层的安全需求、无线资源控制（radio resource control，RRC）层的安全需求、物理层的安全需求和应用层的安全需求。非接入层的安全需求可以包括以下中的一种或多种：认证和密钥协商、数据保密性、数据完整性和异常处理机制。RRC 层的安全需求可以包括以下中的一种或多种：数据保密性、数据完整性、安全模式命令设置、序列号同步机制和异常处理机制。物理层的安全需求可以包括以下中的一种或多种：加密、信道编码与调制、物理层身份验证和指纹识别。应用层的安全需求可以包括以下中的一种或多种：网络切片安全、用户隐私保护和开放接口的安全。

在一些实施例中，安全需求可以包括以下中的一个或多个子需求：业务领域、数据类型、数据流向、安全等级、网络环境、交互模式、业务优先级、延迟要求、隐私级别、身份与授权机制、网络隔离程度、加密密钥强度等。

在一些实施例中，不同的安全需求可以对应不同的安全策略。以安全等级为例，不同的安全等级可以对应不同的加密强度和访问控制的严格程度。以数据类型为例，不同的数据类型（如用户数据、机器数据和模型数据等）可能需要不同的保护级别和处理方式。

在一些实施例中，安全需求中的子需求可以为安全需求列表中的子需求，换句话说，安全需求可以包括安全需求列表中的多个子需求。安全需求列表可以为预设的安全需求列表。通过从安全需求列表中选择安全需求，可以简化安全需求的确定过程，使得生成的安全需求更加规范化，从而可以降低生成安全策略的难度。

在一些实现方式中，可以将安全需求列表作为第一模型的输入。第一模型可以建立终端设备的业务与子需求之间的对应关系，可以基于终端设备的业务选择对应的子需求。

在一些实施例中，安全策略可以包括多个子策略，或者说，安全策略可以通过多个子策略组合而成，通过子策略的设计，使得在生成安全策略时，可以根据终端设备的业务需要，灵活组合不同的子策略，增加生成安全策略的灵活性。

在一些实施例中，安全策略可以包括多个子策略，多个子策略可以分别与多个子需求对应。换句话说，多个子策略可以与多个子需求一一对应。一个子策略对应一个子需求。在生成安全策略时，可以针对多个子需求，生成分别与多个子需求对应的多个子策略，将多个子策略进行组合形成最终的安全策略。

举例说明，假设安全需求包括轻量级认证、分布式安全、数据授权和低层安全保护，则生成的安全策略可以包括以下子策略：与轻量级认证对应的子策略、与分布式安全对应的子策略、与数据授权对应的子策略以及与低层安全保护对应的子策略。

在一些实施例中，第一模型的输入参数可以包括安全能力。该安全能力可以为与终端设备的业务对应的安全能力，或者说，该安全能力可以是基于终端设备的业务确定的。在一些实施例中，安全能力也可以称为安全功能。通过将安全能力作为第一模型的输入参数，可以使得生成的安全策略与安全能力对应，能够满足不同安全能力的安全需求。例如，在安全能力发生变化的情况下，安全策略网元可以生成新的安全策略或更新安全策略。

在一些实现方式中，安全能力也可以称为安全机制或第三代合作伙伴计划（3rd generation partnership project，3GPP）安全机制。

在一些实现方式中，安全能力可以包括多个子能力，或者说，安全能力可以为模块化的安全能力。通过将安全能力模块化，在生成安全策略时，可以根据具体的安全需求快速地选择和组合不同的安全模

块，以有效实现预定的安全策略。

在一些实现方式中，上述子能力可以为安全能力库中的子能力。该安全能力库例如可以为 3GPP 安全能力库。安全能力库中包括多个子能力。在生成安全策略时，可以根据实际的业务需要，选择对应的子能力。

在一些实现方式中，安全能力库也可以称为模块化安全能力库。

在一些实现方式中，可以将安全能力库作为第一模型的输入。第一模型可以建立终端设备的业务与子能力之间的对应关系，可以基于终端设备的业务选择对应的子能力。

例如，安全能力（或安全能力库）可以包括以下中的一个或多个子能力：128 位密钥、认证与密钥协商（authentication and key agreement，AKA）、基于身份的授权、PKI、抗量子密钥、分布式认证、基于属性的授权、授权（Oauth）、物理层密钥、轻量级认证、基于数据的授权、区块链等。

在一些实施例中，AKA 可以包括以下中的一种或多种：5G-AKA、AES-AKA、EAP-AKA、BEST-AKA、EPS-AKA、EAP-TLS、EAP-AKA'等。

可以理解的是，子能力划分的颗粒度越细，子能力之间的组合会越灵活，生成的安全策略将会更符合终端设备的业务需求。

在一些实施例中，安全能力可以跨越从物理层到应用层的多个安全领域。安全能力可以包括身份验证、授权、数据加密、完整性验证和重放攻击防护等多种机制。

在一些实现方式中，安全能力可以包括与安全需求对应的安全能力。例如，安全能力可以包括不同协议层的安全能力。例如，安全能力可以包括以下中的一种或多种：非接入层的安全能力、RRC 层的安全能力、物理层的安全能力和应用层的安全能力。非接入层的安全能力可以包括针对以下中一种或多种安全需求对应的安全能力：认证和密钥协商、数据保密性、数据完整性和异常处理机制。RRC 层的安全能力可以包括针对以下中一种或多种安全需求对应的安全能力：数据保密性、数据完整性、安全模式命令设置、序列号同步机制和异常处理机制。物理层的安全能力可以包括针对以下中一种或多种安全需求对应的安全能力：加密、信道编码与调制和物理层身份验证和指纹识别。应用层的安全能力可以包括针对以下中一种或多种安全需求对应的安全能力：网络切片安全、用户隐私保护和开放接口的安全。

在一些实现方式中，以非接入层为例，与认证与密钥协商对应的安全能力可以包括以下中的一种或多种：EPS-AKA、5G-AKA、EAP-AKA、EAP-AKA'、EAP-TLS、轻量级认证协议（如 BEST-AKA）、超轻量级认证协议。与数据保密性对应的安全能力可以包括以下中的一种或多种：EEA0、EEA1、EEA2、EEA3、NEA0、NEA1、NEA2。与数据完整性对应的安全能力可以包括以下中的一种或多种：EIA0、EIA1、EIA2、EIA3、NEA0、NEA1、NEA2。与异常处理机制对应的安全能力可以包括以下中的一种或多种：认证异常处理、网络失败和恢复、安全模式命令错误处理、分布式拒绝服务（distributed denial of service，DDOS）处理。

在一些实现方式中，以 RRC 层为例，与数据保密性对应的安全能力可以包括以下中的一种或多种：EEA0、EEA1、EEA2、EEA3、NEA0、NEA1、NEA2。与数据完整性对应的安全能力可以包括以下中的一种或多种：EIA0、EIA1、EIA2、EIA3、NEA0、NEA1、NEA2。与安全模式命令设置对应的安全能力可以包括指定使用的加密算法和/或完整性算法。与异常处理机制对应的安全能力可以包括以下中的一种或多种：安全模式失败、连接丢失和重建丢失。

在一些实现方式中，以物理层为例，与加密对应的安全能力可以包括数据加扰。与信道编码与调制对应的安全能力可以包括以下中的一种或多种：低密度奇偶校验（low-density parity-check，LDPC）、Turbo 码和 polar 码。与物理层身份验证和指纹识别对应的安全能力可以包括以下中的一种或多种：设备特定的射频特征识别、时间和频率分析、信号波形分析、环境和信道特性。

在一些实现方式中，以应用层为例，与网络切片安全对应的安全能力可以包括以下中的一种或多种：切片隔离、切片二次认证。与用户隐私保护对应的安全能力可以包括以下中的一种或多种：用户隐藏标识符（subscription concealed identifier，SUCI）、临时移动用户识别码（temporary mobile subscriber identity，TMSI）、全球唯一临时 UE 标识（globally unique temporary UE identity，GUTI）（如 5G-GUTI）、用户同意（user consent）、订阅者数据管理与暴露。与开放接口的安全对应的安全能力可以包括以下中的一种或多种：OAuth 2.0、OpenID Connect 和应用的认证与密钥管理（authentication and key management for application，AKMA）。

通过模块化的安全能力设计，使得安全能力可以兼容不同通信网络（如 4G 网络、5G 网络等）的安全机制，并针对未来的网络环境提供必要的扩展性，能够确保随着网络技术的发展，本申请实施例提供的安全措施仍然能够保持前瞻性和灵活性。

在一些实施例中，安全能力可以包括多个子能力，安全策略可以包括多个子策略，多个子策略可以分别与多个子能力对应。换句话说，多个子策略可以与多个子能力一一对应。一个子策略对应一个子能

力。在生成安全策略时，可以针对多个子能力，生成分别与多个子能力对应的多个子策略，将多个子策略进行组合形成最终的安全策略。

以终端设备的业务为工业互联网业务为例，工业互联网需要考虑全产业链环节不同地点的数据搜集与处理，因此，需要的安全能力可以包括分布式认证以及基于业务数据的授权。在生成安全策略时，可以生成与分布式认证对应的子策略以及与基于业务数据的授权对应的子策略。

在一些实施例中，为了使安全策略能够适应网络的动态变化，第一模型的输入参数中可以包括安全规则和/或安全态势。安全态势可以包括系统安全态势和/或网络安全态势。安全态势例如可以包括以下中的一种或多种：网络行为监测、安全运维管理和系统事件日志。

安全规则可以包括合规要求和/或威胁分析。在一些实现方式中，安全规则可以包括静态规则和/或动态规则。静态规则可以包括不经常变化的规则集。静态规则可以包括以下中的一种或多种：数据访问策略、公钥基础设施、身份管理规则以及安全信息和事件管理的配置等。动态规则可以包括以下中的一种或多种：数据监控的实时反馈、合规性检测、威胁情报更新和活动日志等。这些信息有助于核心网理解当前的安全环境和正在发生的事件。

在安全规则和/或安全态势发生变化的情况下，安全策略网元可以更新安全策略或生成新的安全策略，使得生成的安全策略可以适应快速变化的网络环境以及适应新出现的威胁。

第一模型的输入参数可以包括上述参数中的任意一种，或者，第一模型的输入参数可以包括上述参数中的多种。例如，第一模型的输入参数可以包括系统类型、安全需求、安全能力、安全规则和安全态势，如图 8 所示。又例如，第一模型的输入参数可以包括系统类型、安全需求和安全能力，如图 9 所示。

本申请实施例对安全需求的确定方式不做具体限定。作为一个示例，安全需求可以是预设的安全需求。安全需求可以是工作人员人工确定的。工作人员确定好安全需求后，可以将安全需求输入到第一模型中。在一些实现方式中，工作人员可以基于安全需求列表确定安全需求。例如，工作人员可以根据终端设备的业务，从安全需求列表中选择一个或多个子需求，形成最终的安全需求。

作为另一个示例，安全需求可以是基于第二模型生成的。通过第二模型生成安全需求可以使得安全需求的生成更加智能化。

第二模型可以为任意一种神经网络模型。例如，第二模型可以为 AI 模型或 ML 模型。在一些实现方式中，第二模型可以为深度森林模型。

在一些实现方式中，安全需求可以由安全策略网元之外的其他网元生成。例如，安全需求可以由策略检测网元生成。策略检测网元例如可以为 PD。通过由其他网元生成安全策略，可以增加安全策略生成过程的灵活性和动态适应能力。

在一些实现方式中，策略检测网元可以基于第二模型生成安全需求。策略检测网元在生成安全需求后，可以向安全策略网元发送安全需求，如图 9 所示。在一些实现方式中，策略检测网元可以通过策略管理网元向安全策略网元发送安全需求。

安全策略网元接收到来自策略检测网元的安全需求后，可以认为终端设备的业务发生了变化，在该情况下，安全策略网元可以生成安全策略。

在一些实施例中，第二模型的输入参数可以包括以下中的一种或多种：安全规则和业务数据。业务数据可以包括以下中的一种或多种：网络流量、设备状态和服务质量参数等。业务数据的变化可以反映业务需求的变化。例如，如果终端设备从一个低安全需求的业务过渡到一个高安全需求的业务，则对应的业务数据也会发生变化。

安全规则可以包括静态规则和/或动态规则。静态规则可以包括不经常变化的规则集。静态规则可以包括以下中的一种或多种：数据访问策略、公钥基础设施、身份管理规则以及安全信息和事件管理的配置等。动态规则可以包括以下中的一种或多种：数据监控的实时反馈、合规性检测、威胁情报更新和活动日志等。这些信息有助于核心网理解当前的安全环境和正在发生的事件。

策略检测网元（或第二模型）的输出包括安全需求。安全需求可以基于业务数据和/或安全规则来生成。安全需求可以为安全需求列表中的安全需求。策略检测网元可以具有智能分析和预测功能，可以利用第二模型和数据分析技术来处理和解释输入数据，从而生成准确的安全需求。

在一些实施例中，策略检测网元可以在终端设备的业务发生变化的情况下，生成安全需求。在一些实现方式中，策略执行网元可以检测终端设备的业务是否发生变化，在终端设备的业务发生变化的情况下，策略执行网元可以向策略检测网元发送第一请求消息（如图 5 中的步骤 S510 或图 6 中的步骤 S610），第一请求消息用于请求安全策略。响应于第一请求消息，策略检测网元生成安全需求（如图 6 中的步骤 S620）。例如，策略检测网元可以基于第二模型生成安全需求。在生成安全需求后，策略检测网元可以向安全策略网元发送安全需求（如图 6 中的步骤 S630）。

在一些实现方式中，策略执行网元可以通过策略管理网元向策略检测网元发送第一请求消息。例如，策略执行网元可以向策略管理网元发送第一请求消息，策略管理网元接收到第一请求消息后，可以将第一请求消息转发至策略检测网元。

本申请实施例对策略执行网元确定终端设备的业务是否发生变化的方式不做具体限定。作为一个示例，策略执行网元可以对终端设备的业务进行监测，以确定终端设备的业务是否发生变化。作为另一个示例，终端设备可以在业务发生变化的情况下，向策略执行网元发送第一指示信息（如图 7 中的步骤 S710），第一指示信息用于指示终端设备的业务发生变化。也就是说，策略执行网元可以基于终端设备的指示，确定终端设备的业务是否发生变化。

在一些实施例中，策略检测网元也可以根据安全策略网元的指示生成安全需求。例如，安全策略网元可以基于一定的规则（如计算出的信任值）确定是否需要生成或更新安全策略。在确定需要生成或更新安全策略的情况下，安全策略网元可以向策略检测网元发送指示信息，以指示策略检测网元生成新的安全需求。

下面结合图 8 和图 9，对本申请实施例涉及的安全架构进行介绍。

本申请实施例的方案可以包括两种安全架构。一种安全架构包括安全策略网元。安全策略网元可以为一种引擎组件，因此，该架构也可以称为单引擎架构，如图 8 所示。另一种安全架构包括安全策略网元和策略检测网元。安全策略网元和策略检测网元可以均为引擎组件，因此，该架构也可以称为双引擎架构，如图 9 所示。下面对图 8 和图 9 所示的方案分别进行介绍。

参见图 8，安全策略网元可以基于第一模型生成安全策略。第一模型的输入参数可以包括以下中的一种或多种：安全需求、安全能力、系统类型、安全规则和安全态势。

参见图 9，策略检测网元可以基于第二模型生成安全需求。策略检测网元可以将生成的安全需求发送至安全策略网元。第二模型的输入参数可以包括以下中的一种或多种：业务数据和安全规则。

安全策略网元可以基于第一模型生成安全策略。第一模型的输入参数可以包括以下中的一种或多种：安全需求、安全能力和系统类型。

需要说明的是，图 8 和图 9 中将安全策略网元和策略管理网元分为两个网元进行介绍，但是，在一些实施例中，安全策略网元和策略管理网元也可以集成在一个网元中。

在一些实现方式中，安全策略网元向策略执行网元发送安全策略（参见图 4 中的步骤 S420 和图 5 中的步骤 S520）。安全策略网元在生成安全策略后，可以向策略执行网元发送安全策略，以使策略执行网元可以执行该安全策略。

在一些实施例中，安全策略网元可以通过策略管理网元向策略执行网元发送安全策略。例如，安全策略网元向策略管理网元发送安全策略，策略管理网元可以将安全策略转发至策略执行网元。

在一些实施例中，策略执行网元可以向终端设备发送安全策略（如图 7 中的步骤 S720），以使终端设备和策略执行网元中的安全策略相同，终端设备和策略执行网元可以基于相同的安全策略进行安全通信。例如，终端设备和策略执行网元可以采用相同的物理层密钥进行安全传输保护。

下面结合两个具体的示例，对本申请实施例的方案进行详细阐述。需要说明的是，下文中的示例仅是为了便于理解，对本申请实施例的方案进行的解释说明，本申请实施例不应局限于以下实施例。

示例一

示例一的方案适用于图 8 所示的架构。

参见图 10，在步骤 S1010，PEP 向 PE 发送请求消息。PEP 在发送请求消息之前，可以先确定终端设备的业务是否发生变化。在终端设备的业务发生变化的情况下，PEP 向 PE 发送请求消息，该请求消息用于请求安全策略。

在一些实现方式中，步骤 S1010 可以包括步骤 S1010a 和步骤 S1010b。在步骤 S1010a，PEP 向 PA 发送请求消息。在步骤 S1010b，PA 向 PE 转发该请求消息。

在一些实现方式中，在步骤 S1010 之前，图 10 所示的方法还可以包括步骤 S1005。在步骤 S1005，PEP 可以接收 UE 发送的指示信息，该指示信息用于指示 UE 的业务发生变化。

在步骤 S1020，PE 判断是否需要新的安全策略。如果需要新的安全策略，则执行步骤 S1030；如果不需要新的安全策略，则结束流程。

在步骤 S1030，PE 使用第一模型生成安全策略。第一模型为深度森林模型。

在步骤 S1040，PE 向 PA 发送安全策略。

在步骤 S1050，PA 向 PEP 转发安全策略。

在步骤 S1060，PEP 向 UE 发送安全策略。

通过上述流程，PE 可以在 UE 的业务发生变化的情况下，触发 PE 发起安全策略的更新。另外，PEP 和 UE 可以获得相同的安全策略，后续 PEP 和 UE 可以基于相同的安全策略和安全功能进行安全保

护。例如，PEP 和 UE 可以采用相同的物理层密钥机制进行安全传输保护。

示例二

示例二的方案适用于图 9 所示的架构。

参见图 11，在步骤 S1110，PEP 向 PD 发送请求消息。PEP 在发送请求消息之前，可以先确定终端设备的业务是否发生变化。在终端设备的业务发生变化的情况下，PEP 向 PD 发送请求消息，该请求消息用于请求安全策略。

在一些实现方式中，步骤 S1110 可以包括步骤 S1110a 和步骤 S1110b。在步骤 S1110a，PEP 向 PA 发送请求消息。在步骤 S1110b，PA 向 PD 转发该请求消息。

在一些实现方式中，在步骤 S1110 之前，图 11 所示的方法还包括步骤 S1105。在步骤 S1105，PEP 可以接收 UE 发送的指示信息，该指示信息用于指示 UE 的业务发生变化。

在步骤 S1120，PD 利用第二模型生成安全需求。第二模型可以为深度森林模型。

在步骤 S1130，PD 向 PE 发送第一消息，第一消息中包括安全需求。

在一些实现方式中，步骤 S1130 可以包括步骤 S1130a 和步骤 S1130b。在步骤 S1130a，PD 向 PA 发送第一消息。在步骤 S1130b，PA 向 PE 转发第一消息。

在步骤 S1140，PE 判断是否需要新的安全策略。如果需要新的安全策略，则执行步骤 S1150；如果不需要新的安全策略，则结束流程。

在步骤 S1150，PE 使用第一模型生成安全策略。第一模型为深度森林模型。第一模型的输入参数可以包括 PD 生成的安全需求。

在步骤 S1160，PE 向 PA 发送安全策略。

在步骤 S1170，PA 向 PEP 转发安全策略。

在步骤 S1180，PEP 向 UE 发送安全策略。

示例二与示例一的区别在于，示例二中的安全需求是 PD 生成的，通过由 PD 生成安全需求，可以提高安全策略生成的灵活性。

通过上述流程，PE 可以在 UE 的业务发生变化的情况下，触发 PE 发起安全策略的更新。另外，PEP 和 UE 可以获得相同的安全策略，后续 PEP 和 UE 可以基于相同的安全策略和安全功能进行安全保护。例如，PEP 和 UE 可以采用相同的物理层密钥机制进行安全传输保护。

本申请对第一模型和第二模型的训练过程不做具体限定。在一些实施例中，PE 可以对第一模型进行训练。以图 8 所示的架构为例，PE 可以向核心网网元（如网络数据分析功能（network data analytics function，NWDAF）网元）请求相关数据，PE 可以利用相关数据对第一模型进行训练。相关数据可以包括安全需求、安全规则、安全态势、系统类型、安全能力等。以图 9 所示的架构为例，PE 可以向核心网网元（如 NWDAF 网元）请求相关数据，PE 可以利用相关数据对第一模型进行训练。相关数据可以包括安全需求、安全规则、安全态势、系统类型、安全能力等。

在一些实施例中，PD 可以对第二模型进行训练。以图 9 所示的架构为例，PD 可以向核心网网元（如 NWDAF 网元）请求相关数据，PD 可以利用相关数据对第二模型进行训练。相关数据可以包括业务数据、动态安全规则和静态安全规则。业务数据例如可以包括：网络活动数据、设备行为数据、用户交互数据和安全事件数据等。

下面结合三个应用示例，来体现本申请中安全策略的高效编排和实施。

场景一、智慧家庭场景

以现代化的住宅为例，其中布局了众多智慧家居和感知传感器，构建了一套完善的智能家庭系统。在日常生活中，该系统能够实时响应居住者的需求。例如，当居住者于清晨醒来，系统通过感知技术自动识别其位置和行为，进而自动调节窗帘、电灯，为其营造最佳的室内环境。又例如，感知技术还能识别居住者的日常活动，如健身运动状态。系统能够通过无线信号实时感知和分析居住者的身体动作，如仰卧起坐或跑步，从而为其提供合适的运动反馈。又例如，考虑到居住者可能长时间不在家的情况，系统设有入侵检测功能。当有外部人员试图非法进入，系统会通过 6G 网络的精准感知，分析收集到的信号变化，进而判定入侵者的存在。一旦确认有异常情况发生，系统将立即向居住者的移动设备发送警报，确保家庭财产的安全。

在对不同的场景深入分析后，每个业务场景因其独特的特性都伴随着独特的安全需求。无论是常规家居操作、用户行为状态的实时监测，还是非法入侵的即时报警，背后的安全挑战与需求都有其特有的层次和差异。具体的安全需求可以如表 1 所示。

表 1

安全维度	正常使用场景	行为状态监测场景	入侵检测场景
用户隐私保护	传输和存储时防止用户数据非法访问或泄露	提供加强的加密和匿名化手段以保护更深入的用户数据	传输和存储时防止用户数据非法访问或泄露
数据完整性和真实性	确保传输数据不被篡改或损坏	确保数据在传输和处理中不被篡改	确保数据在传输和处理中不被篡改
设备身份验证	只允许已认证的设备和应用与核心网交互	只允许已认证的设备和应用与核心网交互，确保多个传感器和设备之间的协同安全工作	只允许已认证的设备和应用与核心网交互，确保多个传感器和设备之间的协同安全工作
密钥等级	中	高	高
授权访问	只有授权的用户或服务能访问数据和控制	根据用户行为和场景调整安全策略	确保只有授权人员可访问
威胁监测和响应	持续监测可能的网络攻击或异常流量行为	定义和防护特定行为的策略，如老人摔倒时的隐私保护	定义和防护特定行为的策略，实时报警，确保高优先级、实时传输和通信链路的可靠性
远程控制与访问	-	当用户收到紧急情况时，可远程访问设备	当用户收到紧急情况时，可远程访问设备
网络的隔离与保护	-	-	对入侵检测网络和其他家用网络进行隔离
数据的精确性与可靠性	-	数据准确性影响用户健康和安全，加强感知频率	确保高度准确性，避免频繁误报

场景二、智慧穿戴场景

以某用户的生活为例，其智慧手环、智慧鞋、智慧眼镜和智慧腕带，都可以与网络（如 6G 网络）通信，共同构建了一个完整的智慧健康和运动管理系统。当用户开始新的一天，智慧手环自动启动，凭借先进的感知技术，实时监测他的心率、血压、呼吸频率等关键健康指标。随着用户开始他的日常锻炼，例如羽毛球训练，智慧鞋可以准确捕捉他的运动数据，如步伐、速度和跳跃，同时智慧眼镜通过高速的网络实时分析运动场上的数据，为他提供即时反馈和指导。当用户在锻炼中遭遇不测，如扭伤脚踝，他的穿戴设备立即感知到这一异常，启动紧急模式。智慧手环借助 AR 技术为他展示伤势处理的步骤，智慧腕带内置的低频电疼痛治疗仪则迅速减轻他的疼痛。在此期间，所有数据均通过网络实时传输，确保用户在第一时间得到最佳的医疗建议和救援。

随着智慧穿戴设备在各个方面的广泛应用，其背后所涉及的业务也变得越来越复杂。这些业务不仅关乎到用户的日常健康与运动，更涉及到紧急医疗救援、运动反馈指导、甚至伤势的实时处理。每一种业务都有其独特的数据和操作流程，因此它们的安全需求也各不相同。日常健康监测可能更加注重数据的完整性和隐私保护；而运动性能检测更侧重于数据的实时性和精确性；基于 AR 的伤势处理则需确保数据的可用性和应急响应能力。表 2 示出了三种智慧穿戴设备使用场景下的安全需求。

表 2

安全维度	日常监测场景	运动性能检测场景	基于 AR 的运动伤病康复辅助场景
数据收集策略	最小数据收集原则	根据运动类型收集相关数据	收集所有与伤病治疗相关的必要数据
用户隐私保护	中，不收集非必要的个人标识信息	低，不收集个人标识信息	高，不收集非必要的个人标识信息
数据保密性	数据加密存储与传输	数据加密存储与传输	数据加密存储与传输
密钥等级	中	中	低

数据完整性	确保心率、血压等数据不被篡改	防止运动数据如步伐、速度等被篡改	AR 内容和治疗建议不被篡改
数据授权	征得用户同意，仅授权第三方使用	征得用户同意，仅授权第三方使用	征得用户同意，仅授权第三方使用
设备身份认证	手环、智慧眼镜等设备的身份验证	智慧鞋、运动分析设备的身份验证	AR 设备和其他相关设备的身份验证
用户身份认证	确保只有用户本人可以访问其运动数据	确保只有用户本人可以访问其运动数据	-
防篡改机制	-	-	AR 应用和治疗数据的可追溯与防篡改机制
业务优先级	低	低	高
应急响应机制	对异常健康数据快速响应	实时 URLLC 切片，对运动伤害或其他突发情况进行快速响应	大带宽 eMBB 切片，对用户伤病的快速 AR 指导响应

场景三、智慧物联网设备场景

智慧物联网设备在多个场景中都有所体现，而购物中心是一个比较好的例子。例如，针对商品供销管理，可以通过部署 3GPP IoT 设备于店铺货架与存储区，以实时地感知商品存货状态并据此调整供销策略，保障供需平衡且避免库存积压。又例如，IoT 设备可以实时地感知并适应购物中心中的人流变化和温度变化，如照明与空调系统可以自动调节，以为公众创造出一个比较适宜的购物环境，另外，还可以降低能源消耗，从而实现了运营成本的有效优化。又例如，购物中心引入了基于环境 IoT 驱动的室内导航系统，以为顾客提供精确的室内导航服务，轻松地引导他们找到停车位与目的店铺。

上述不同场景可以对应不同的安全需求，如表 3 所示。

表 3

安全维度	3GPP IoT 设备的供销管理	Ambient IoT 的能源管理	Ambient IoT 的室内导航
实体认证	轻量级设备认证协议	超轻量级设备认证协议	超轻量级设备身份认证协议+用户身份认证
隐私保护	-	-	防止位置跟踪、加密位置数据、位置匿名化
数据保密性	加密传输库存数据	中庭环境数据的加密	用户位置信息加密
数据完整性	确保数据完整性	确保数据完整性	确保数据完整性
数据源认证	数据来源验证	数据来源验证	-
通信保密性	加密设备间通信	加密设备间通信	加密设备与用户间通信

上文结合图 1 至图 11，详细描述了本申请的方法实施例，下面结合图 12 至图 15，详细描述本申请的装置实施例。应理解，方法实施例的描述与装置实施例的描述相互对应，因此，未详细描述的部分可以参见前面方法实施例。

图 12 是本申请实施例提供的一种通信设备的示意性框图。图 12 所示的通信装置 1200 可以为上文描述的任意一种安全策略网元。图 12 所示的通信装置包括生成单元 1210 和发送单元 1220。

在一些实施例中，生成单元 1210 和判断单元可以为处理器，发送单元 1220 和接收单元可以为收发器。在一些实现方式中，通信装置 1200 还可以包括存储器。

生成单元 1210，用于生成安全策略，所述安全策略与终端设备的业务相关联。

发送单元 1220，用于向策略执行网元发送所述安全策略。

在一些可能的实现方式中，所述生成单元用于：基于第一模型生成所述安全策略。

在一些可能的实现方式中，所述第一模型的输入参数包括以下至少之一：与所述终端设备的业务对

应的系统类型、与所述终端设备的业务对应的安全需求、与所述终端设备的业务对应的安全能力。

在一些可能的实现方式中，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

在一些可能的实现方式中，所述安全需求包括安全需求列表中的多个子需求。

在一些可能的实现方式中，所述第一模型的输入参数还包括以下至少之一：安全规则、网络安全态势、系统安全态势。

在一些可能的实现方式中，所述通信设备还包括：接收单元，用于接收来自策略检测网元的所述安全需求。

在一些可能的实现方式中，所安全需求是在所述终端设备的业务发生变化的情况下生成。

在一些可能的实现方式中，所述安全需求基于第二模型生成。

在一些可能的实现方式中，在生成安全策略之前，所述通信设备还包括：接收单元，用于接收所述策略执行网元发送的第一请求消息，所述第一请求消息用于请求所述安全策略，所述第一请求消息是在所述终端设备的业务发生变化的情况下发送。

在一些可能的实现方式中，所述通信设备还包括判断单元，所述判断单元，用于判断是否需要生成所述安全策略；所述生成单元，用于在需要生成所述安全策略的情况下，生成所述安全策略。

图 13 是本申请实施例提供的一种通信设备的示意性框图。图 13 所示的通信装置 1300 可以为上文描述的任意一种策略执行网元。图 13 所示的通信装置包括发送单元 1310 和接收单元 1320。

在一些实施例中，发送单元 1310 和接收单元 1320 可以为收发器。在一些实现方式中，通信装置 1300 还可以包括存储器和处理器。

发送单元 1310，用于向第一网元发送第一请求消息，所述第一请求消息用于请求安全策略，所述安全策略与所述终端设备的业务相关联，所述第一网元包括安全策略网元和/或策略检测网元。

接收单元 1320，用于接收来自所述安全策略网元的所述安全策略。

在一些可能的实现方式中，所述安全策略基于第一模型生成。

在一些可能的实现方式中，所述第一模型的输入参数包括以下至少之一：与所述终端设备的业务对应的系统类型、与所述终端设备的业务对应的安全需求、与所述终端设备的业务对应的安全能力。

在一些可能的实现方式中，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

在一些可能的实现方式中，所述安全需求包括安全需求列表中的多个子需求。

在一些可能的实现方式中，所述第一模型的输入参数还包括以下至少之一：安全规则、网络安全态势、系统安全态势。

在一些可能的实现方式中，所述安全需求由所述策略检测网元发送至所述安全策略网元。

在一些可能的实现方式中，所述安全需求是在所述终端设备的业务发生变化的情况下生成。

在一些可能的实现方式中，所述安全需求基于第二模型生成。

在一些可能的实现方式中，在向第一网元发送第一请求消息之前，所述接收单元还用于：接收来自终端设备的第一指示信息，所述第一指示信息用于指示所述终端设备的业务发生变化。

图 14 是本申请实施例提供的一种通信设备的示意性框图。图 14 所示的通信装置 1400 可以为上文描述的任意一种策略检测网元。图 14 所示的通信装置包括接收单元 1410、生成单元 1420 和发送单元 1430。

在一些实施例中，接收单元 1410 和发送单元 1430 可以为收发器，生成单元 1420 可以为处理器。在一些实现方式中，通信装置 1400 还可以包括存储器。

接收单元 1410，用于接收来自策略执行网元的第一请求消息，所述第一请求消息用于请求安全策略。

生成单元 1420，用于响应于所述第一请求消息，生成与所述终端设备的业务对应的安全需求。

发送单元 1430，用于向安全策略网元发送所述安全需求，所述安全需求用于所述安全策略网元生成所述安全策略。

在一些可能的实现方式中，所述安全策略基于第一模型生成。

在一些可能的实现方式中，所述第一模型的输入参数包括以下至少之一：与所述终端设备的业务对应的系统类型、所述安全需求、与所述终端设备的业务对应的安全能力。

在一些可能的实现方式中，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

在一些可能的实现方式中，所述安全需求包括安全需求列表中的多个子需求。

在一些可能的实现方式中，所述安全需求基于第二模型生成。

图 15 是本申请实施例提供的一种通信设备的示意性框图。图 15 所示的通信装置 1500 可以为上文描述的任意一种终端设备。图 15 所示的通信装置包括发送单元 1510 和接收单元 1520。

在一些实施例中，发送单元 1510 和接收单元 1520 可以为收发器。在一些实现方式中，通信装置 1500 还可以包括存储器和处理器。

发送单元 1510，用于向策略执行网元发送第一指示信息，所述第一指示信息用于指示所述终端设备的业务发生变化；

接收单元 1520，用于接收来自所述策略执行网元的安全策略，所述安全策略与所述终端设备的业务相关联。

在一些可能的实现方式中，所述安全策略基于第一模型生成。

在一些可能的实现方式中，所述第一模型的输入参数包括以下至少之一：与所述终端设备的业务对应的系统类型、与所述终端设备的业务对应的安全需求、与所述终端设备的业务对应的安全能力。

在一些可能的实现方式中，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

在一些可能的实现方式中，所述安全需求属于安全需求列表中的多个子需求。

在一些可能的实现方式中，所述第一模型的输入参数还包括以下至少之一：安全规则、网络安全态势、系统安全态势。

在一些可能的实现方式中，所述安全需求由策略检测网元发送至所述安全策略网元。

在一些可能的实现方式中，所述安全需求是在所述终端设备的业务发生变化的情况下生成。

在一些可能的实现方式中，所述安全需求基于第二模型生成。

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。

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，所述单元的划分，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。

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。

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个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、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber line，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、服务器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读取的任何可用介质或者是包含一个或多个可用介质集成的服务器、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，数字通用光盘（digital video disc，DVD））或者半导体介质（例如，固态硬盘（solid state disk，SSD））等。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1、一种用于生成安全策略的方法，其特征在于，所述方法包括:

安全策略网元生成安全策略，所述安全策略与终端设备的业务相关联;

所述安全策略网元向策略执行网元发送所述安全策略。

2、根据权利要求 1 所述的方法，其特征在于，所述安全策略网元生成安全策略，包括:

所述安全策略网元基于第一模型生成所述安全策略。

3、根据权利要求 2 所述的方法，其特征在于，所述第一模型的输入参数包括以下至少之一：与所述终端设备的业务对应的系统类型、与所述终端设备的业务对应的安全需求、与所述终端设备的业务对应的安全能力。

4、根据权利要求 3 所述的方法，其特征在于，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

5、根据权利要求 3 或 4 所述的方法，其特征在于，所述安全需求包括安全需求列表中的多个子需求。

6、根据权利要求 3-5 中任一项所述的方法，其特征在于，所述第一模型的输入参数还包括以下至少之一：安全规则、网络安全态势、系统安全态势。

7、根据权利要求 3 或 4 所述的方法，其特征在于，所述方法还包括:

所述安全策略网元接收来自策略检测网元的所述安全需求。

8、根据权利要求 7 所述的方法，其特征在于，所安全需求是在所述终端设备的业务发生变化的情况下生成。

9、根据权利要求 8 所述的方法，其特征在于，所述安全需求基于第二模型生成。

10、根据权利要求 1-9 中任一项所述的方法，其特征在于，在所述安全策略网元生成安全策略之前，所述方法还包括:

所述安全策略网元接收所述策略执行网元发送的第一请求消息，所述第一请求消息用于请求所述安全策略，所述第一请求消息是在所述终端设备的业务发生变化的情况下发送。

11、根据权利要求 1-10 中任一项所述的方法，其特征在于，在所述安全策略网元生成安全策略之前，所述方法还包括:

所述安全策略网元判断是否需要生成所述安全策略;

所述安全策略网元生成安全策略，包括:

在需要生成所述安全策略的情况下，所述安全策略网元生成所述安全策略。

12、一种用于生成安全策略的方法，其特征在于，包括:

策略执行网元向第一网元发送第一请求消息，所述第一请求消息用于请求安全策略，所述安全策略与所述终端设备的业务相关联，所述第一网元包括安全策略网元和/或策略检测网元;

所述策略执行网元接收来自所述安全策略网元的所述安全策略。

13、根据权利要求 12 所述的方法，其特征在于，所述安全策略基于第一模型生成。

14、根据权利要求 13 所述的方法，其特征在于，所述第一模型的输入参数包括以下至少之一：与所述终端设备的业务对应的系统类型、与所述终端设备的业务对应的安全需求、与所述终端设备的业务对应的安全能力。

15、根据权利要求 14 所述的方法，其特征在于，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

16、根据权利要求 14 或 15 所述的方法，其特征在于，所述安全需求包括安全需求列表中的多个子需求。

17、根据权利要求 14-16 中任一项所述的方法，其特征在于，所述第一模型的输入参数还包括以下至少之一：安全规则、网络安全态势、系统安全态势。

18、根据权利要求 14 或 15 所述的方法，其特征在于，所述安全需求由所述策略检测网元发送至所述安全策略网元。

19、根据权利要求 18 所述的方法，其特征在于，所述安全需求是在所述终端设备的业务发生变化的情况下生成。

20、根据权利要求 18 或 19 所述的方法，其特征在于，所述安全需求基于第二模型生成。

21、根据权利要求 12-20 中任一项所述的方法，其特征在于，在所述策略执行网元向第一网元发送第一请求消息之前，所述方法还包括:

所述策略执行网元接收来自终端设备的第一指示信息，所述第一指示信息用于指示所述终端设备的业务发生变化。

22、一种用于生成安全策略的方法，其特征在于，包括:

策略检测网元接收来自策略执行网元的第一请求消息，所述第一请求消息用于请求安全策略;

响应于所述第一请求消息，所述策略检测网元生成与所述终端设备的业务对应的安全需求;

所述策略检测网元向安全策略网元发送所述安全需求，所述安全需求用于所述安全策略网元生成所述安全策略。

23、根据权利要求 22 所述的方法，其特征在于，所述安全策略基于第一模型生成。

24、根据权利要求 23 所述的方法，其特征在于，所述第一模型的输入参数包括以下至少之一：与所述终端设备的业务对应的系统类型、所述安全需求、与所述终端设备的业务对应的安全能力。

25、根据权利要求 24 所述的方法，其特征在于，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

26、根据权利要求 24 或 25 所述的方法，其特征在于，所述安全需求包括安全需求列表中的多个子需求。

27、根据权利要求 22-26 中任一项所述的方法，其特征在于，所述安全需求基于第二模型生成。

28、一种用于生成安全策略的方法，其特征在于，包括:

终端设备向策略执行网元发送第一指示信息，所述第一指示信息用于指示所述终端设备的业务发生变化;

所述终端设备接收来自所述策略执行网元的安全策略，所述安全策略与所述终端设备的业务相关联。

29、根据权利要求 28 所述的方法，其特征在于，所述安全策略基于第一模型生成。

30、根据权利要求 29 所述的方法，其特征在于，所述第一模型的输入参数包括以下至少之一：与所述终端设备的业务对应的系统类型、与所述终端设备的业务对应的安全需求、与所述终端设备的业务对应的安全能力。

31、根据权利要求 30 所述的方法，其特征在于，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

32、根据权利要求 30 所述的方法，其特征在于，所述安全需求属于安全需求列表中的多个子需求。

33、根据权利要求 30-32 中任一项所述的方法，其特征在于，所述第一模型的输入参数还包括以下至少之一：安全规则、网络安全态势、系统安全态势。

34、根据权利要求 30 或 31 所述的方法，其特征在于，所述安全需求由策略检测网元发送至所述安全策略网元。

35、根据权利要求 34 所述的方法，其特征在于，所述安全需求是在所述终端设备的业务发生变化的情况下生成。

36、根据权利要求 35 所述的方法，其特征在于，所述安全需求基于第二模型生成。

37、一种通信设备，其特征在于，所述通信设备为安全策略网元，所述通信设备包括:

生成单元，用于生成安全策略，所述安全策略与终端设备的业务相关联;

发送单元，用于向策略执行网元发送所述安全策略。

38、根据权利要求 37 所述的通信设备，其特征在于，所述生成单元用于:

基于第一模型生成所述安全策略。

39、根据权利要求 38 所述的通信设备，其特征在于，所述第一模型的输入参数包括以下至少之一：与所述终端设备的业务对应的系统类型、与所述终端设备的业务对应的安全需求、与所述终端设备的业务对应的安全能力。

40、根据权利要求 39 所述的通信设备，其特征在于，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

41、根据权利要求 39 或 40 所述的通信设备，其特征在于，所述安全需求包括安全需求列表中的多个子需求。

42、根据权利要求 39-41 中任一项所述的通信设备，其特征在于，所述第一模型的输入参数还包括以下至少之一：安全规则、网络安全态势、系统安全态势。

43、根据权利要求 39 或 40 所述的通信设备，其特征在于，所述通信设备还包括:

接收单元，用于接收来自策略检测网元的所述安全需求。

44、根据权利要求 43 所述的通信设备，其特征在于，所安全需求是在所述终端设备的业务发生变化的情况下生成。

45、根据权利要求 44 所述的通信设备，其特征在于，所述安全需求基于第二模型生成。

46、根据权利要求 37-45 中任一项所述的通信设备，其特征在于，在生成安全策略之前，所述通信

设备还包括:

接收单元，用于接收所述策略执行网元发送的第一请求消息，所述第一请求消息用于请求所述安全策略，所述第一请求消息是在所述终端设备的业务发生变化的情况下发送。

47、根据权利要求 37-46 中任一项所述的通信设备，其特征在于，所述通信设备还包括判断单元，所述判断单元，用于判断是否需要生成所述安全策略;

所述生成单元，用于在需要生成所述安全策略的情况下，生成所述安全策略。

48、一种通信设备，其特征在于，所述通信设备为策略执行网元，所述通信设备包括:

发送单元，用于向第一网元发送第一请求消息，所述第一请求消息用于请求安全策略，所述安全策略与所述终端设备的业务相关联，所述第一网元包括安全策略网元和/或策略检测网元;

接收单元，用于接收来自所述安全策略网元的所述安全策略。

49、根据权利要求 48 所述的通信设备，其特征在于，所述安全策略基于第一模型生成。

50、根据权利要求 49 所述的通信设备，其特征在于，所述第一模型的输入参数包括以下至少之一:与所述终端设备的业务对应的系统类型、与所述终端设备的业务对应的安全需求、与所述终端设备的业务对应的安全能力。

51、根据权利要求 50 所述的通信设备，其特征在于，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

52、根据权利要求 50 或 51 所述的通信设备，其特征在于，所述安全需求包括安全需求列表中的多个子需求。

53、根据权利要求 50-52 中任一项所述的通信设备，其特征在于，所述第一模型的输入参数还包括以下至少之一:安全规则、网络安全态势、系统安全态势。

54、根据权利要求 50 或 51 所述的通信设备，其特征在于，所述安全需求由所述策略检测网元发送至所述安全策略网元。

55、根据权利要求 54 所述的通信设备，其特征在于，所述安全需求是在所述终端设备的业务发生变化的情况下生成。

56、根据权利要求 54 或 55 所述的通信设备，其特征在于，所述安全需求基于第二模型生成。

57、根据权利要求 48-56 中任一项所述的通信设备，其特征在于，在向第一网元发送第一请求消息之前，所述接收单元还用于:

接收来自终端设备的第一指示信息，所述第一指示信息用于指示所述终端设备的业务发生变化。

58、一种通信设备，其特征在于，所述通信设备为策略检测网元，所述通信设备包括:

接收单元，用于接收来自策略执行网元的第一请求消息，所述第一请求消息用于请求安全策略;

生成单元，用于响应于所述第一请求消息，生成与所述终端设备的业务对应的安全需求;

发送单元，用于向安全策略网元发送所述安全需求，所述安全需求用于所述安全策略网元生成所述安全策略。

59、根据权利要求 58 所述的通信设备，其特征在于，所述安全策略基于第一模型生成。

60、根据权利要求 59 所述的通信设备，其特征在于，所述第一模型的输入参数包括以下至少之一:与所述终端设备的业务对应的系统类型、所述安全需求、与所述终端设备的业务对应的安全能力。

61、根据权利要求 60 所述的通信设备，其特征在于，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

62、根据权利要求 60 或 61 所述的通信设备，其特征在于，所述安全需求包括安全需求列表中的多个子需求。

63、根据权利要求 58-62 中任一项所述的通信设备，其特征在于，所述安全需求基于第二模型生成。

64、一种通信设备，其特征在于，所述通信设备为终端设备，所述通信设备包括:

发送单元，用于向策略执行网元发送第一指示信息，所述第一指示信息用于指示所述终端设备的业务发生变化;

接收单元，用于接收来自所述策略执行网元的安全策略，所述安全策略与所述终端设备的业务相关联。

65、根据权利要求 64 所述的通信设备，其特征在于，所述安全策略基于第一模型生成。

66、根据权利要求 65 所述的通信设备，其特征在于，所述第一模型的输入参数包括以下至少之一:与所述终端设备的业务对应的系统类型、与所述终端设备的业务对应的安全需求、与所述终端设备的业务对应的安全能力。

67、根据权利要求 66 所述的通信设备，其特征在于，所述安全能力包括多个子能力，所述安全策略包括多个子策略，所述多个子策略分别与所述多个子能力对应。

68、根据权利要求 66 所述的通信设备，其特征在于，所述安全需求属于安全需求列表中的多个子需求。

69、根据权利要求 66-68 中任一项所述的通信设备，其特征在于，所述第一模型的输入参数还包括以下至少之一：安全规则、网络安全态势、系统安全态势。

70、根据权利要求 66 或 67 所述的通信设备，其特征在于，所述安全需求由策略检测网元发送至所述安全策略网元。

71、根据权利要求 70 所述的通信设备，其特征在于，所述安全需求是在所述终端设备的业务发生变化的情况下生成。

72、根据权利要求 71 所述的通信设备，其特征在于，所述安全需求基于第二模型生成。

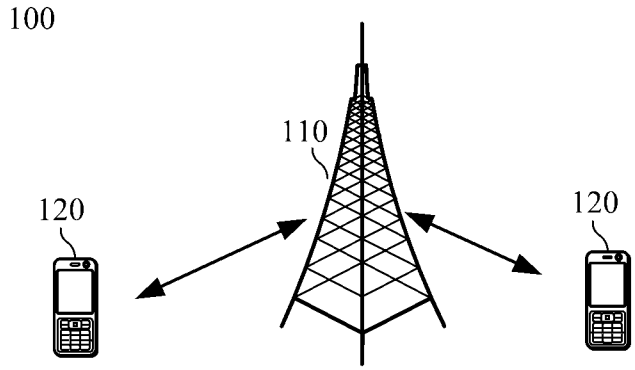
100
110
120
120

图 1

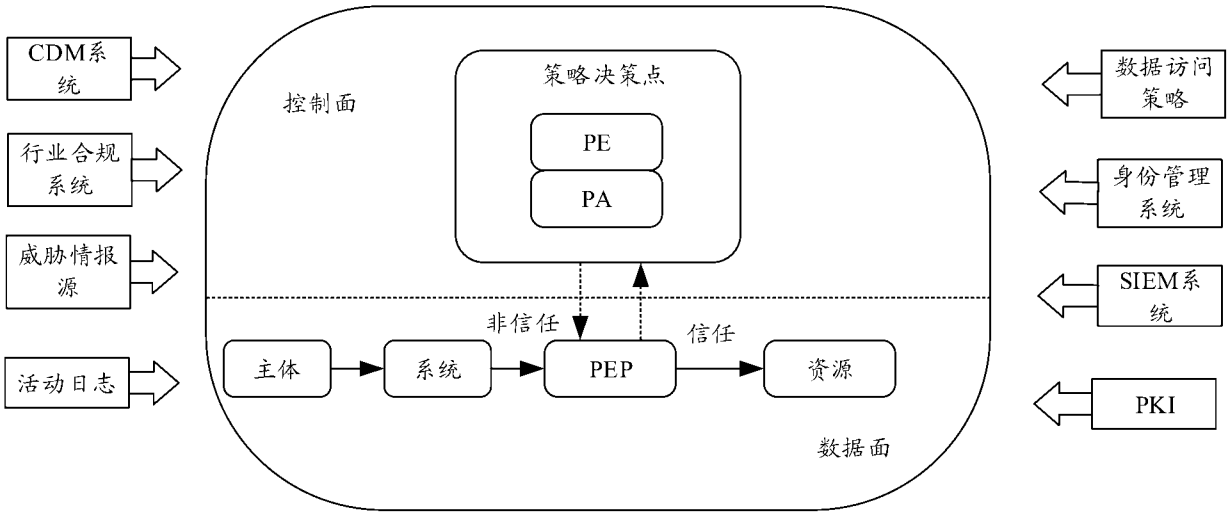
CDM系统
行业合规系统
威胁情报源
活动日志
控制面
策略决策点
PE
PA
非信任
信任
主体
系统
PEP
资源
数据面
数据访问策略
身份管理系统
SIEM系统
PKI

图 2

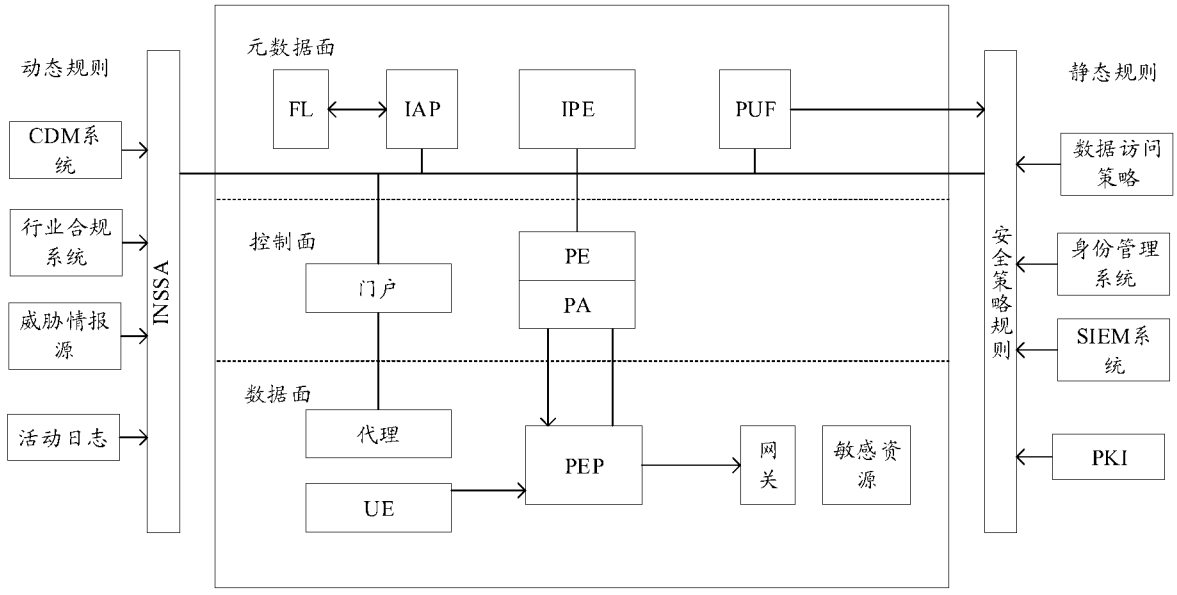
动态规则
CDM系统
行业合规系统
威胁情报源
活动日志
INSSA
元数据面
FL
IAP
IPE
PUF
控制面
门户
PE
PA
数据面
代理
UE
PEP
网关
敏感资源
安全策略规则
静态规则
数据访问策略
身份管理系统
SIEM系统
PKI

图 3

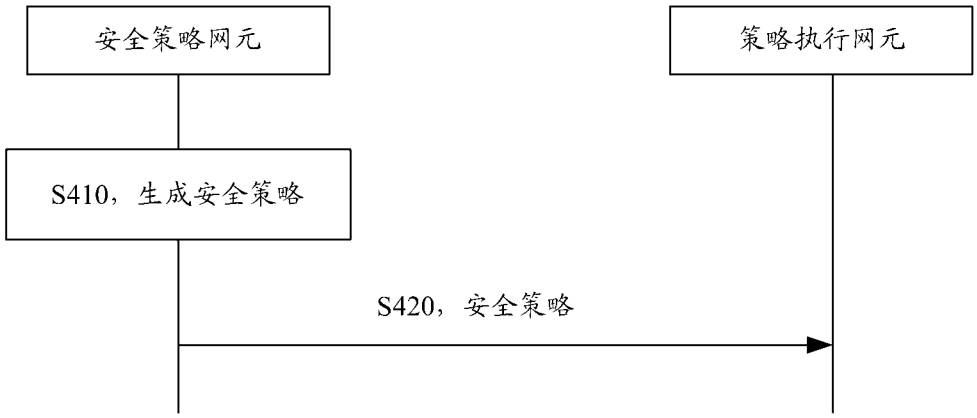
安全策略网元
策略执行网元
S410，生成安全策略
S420，安全策略

图 4

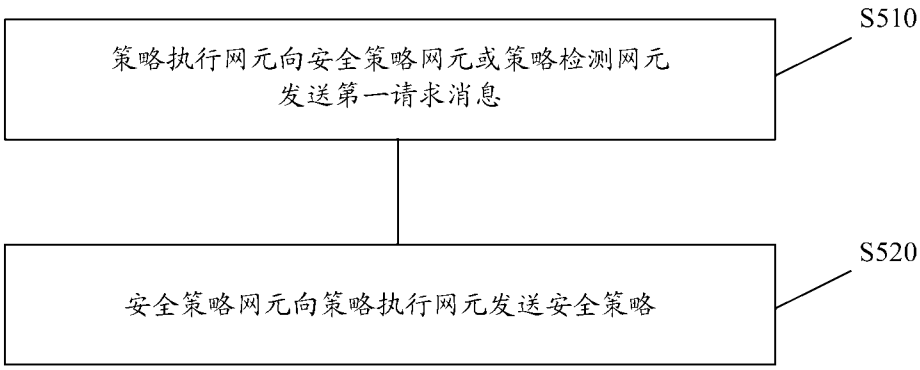
策略执行网元向安全策略网元或策略检测网元
发送第一请求消息
S510
安全策略网元向策略执行网元发送安全策略
S520

图 5

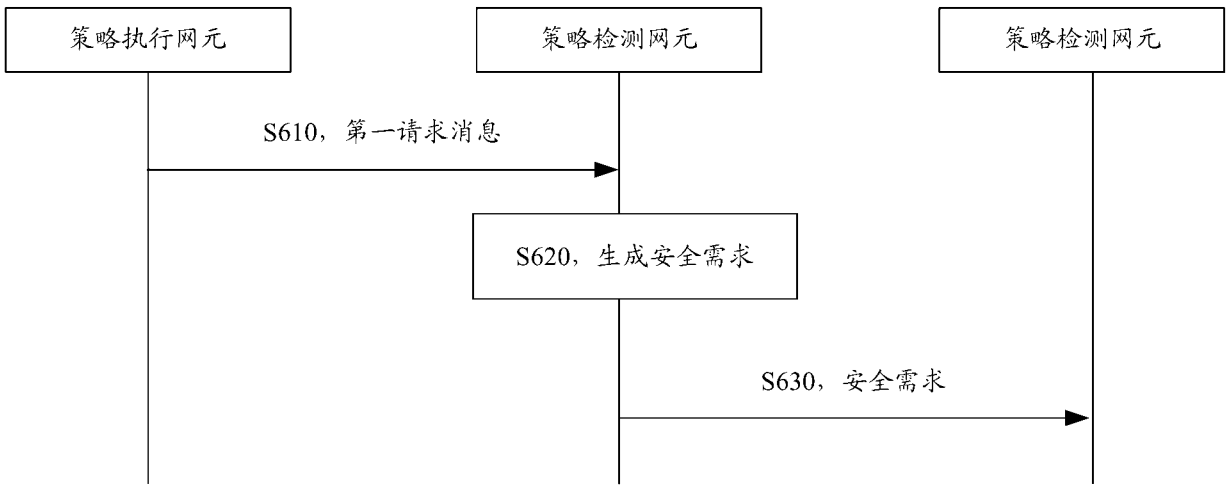
策略执行网元
策略检测网元
策略检测网元
S610，第一请求消息
S620，生成安全需求
S630，安全需求

图 6

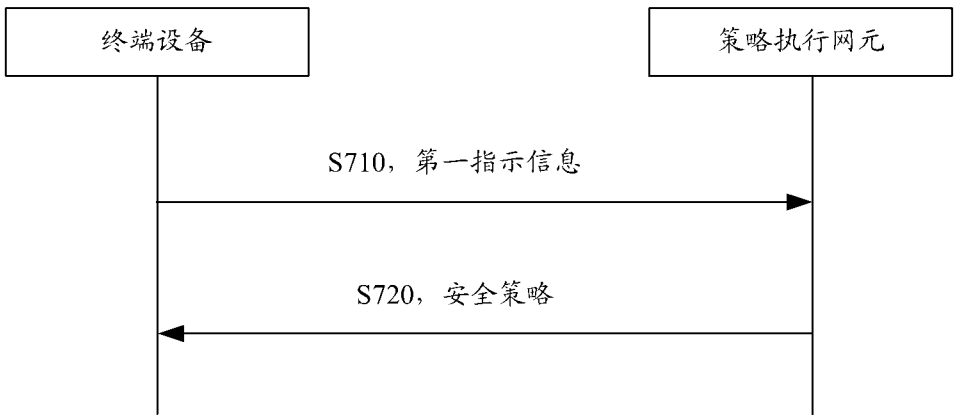
终端设备
策略执行网元
S710，第一指示信息
S720，安全策略

图 7

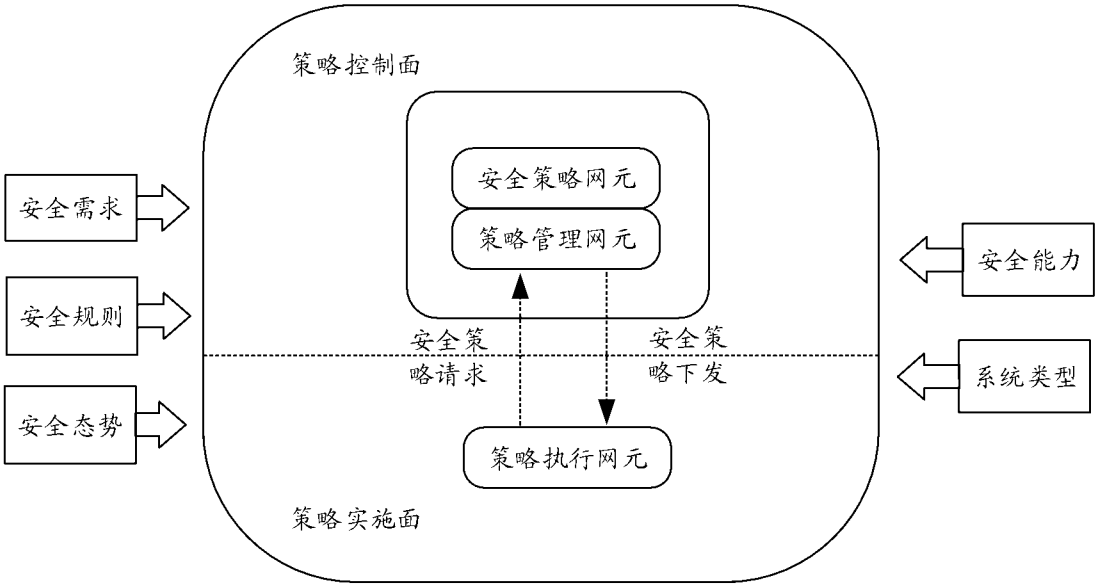
策略控制面
安全策略网元
策略管理网元
安全需求
安全规则
安全态势
安全能力
系统类型
安全策略请求
安全策略下发
策略执行网元
策略实施面

图 8

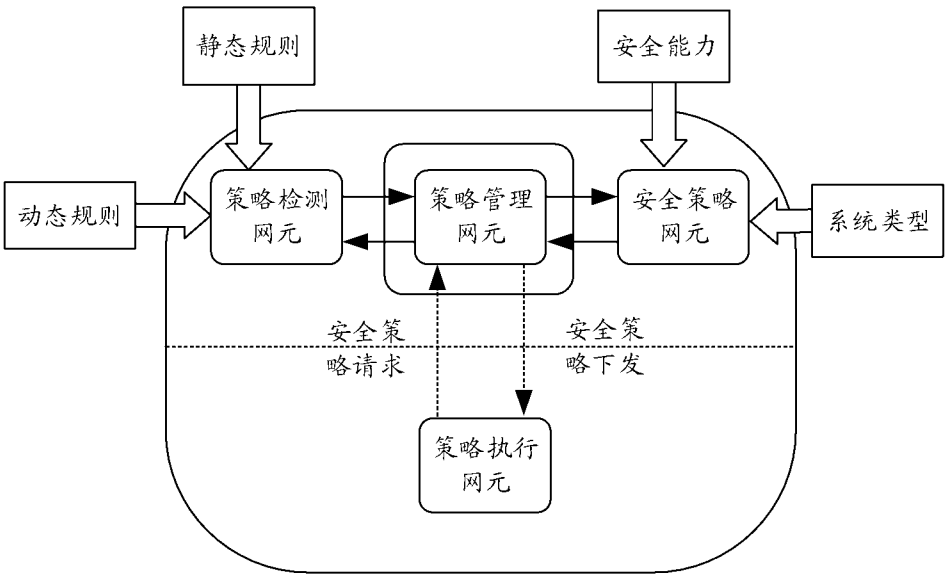
静态规则
安全能力
动态规则
策略检测网元
策略管理网元
安全策略网元
系统类型
安全策略请求
安全策略下发
策略执行网元

图 9

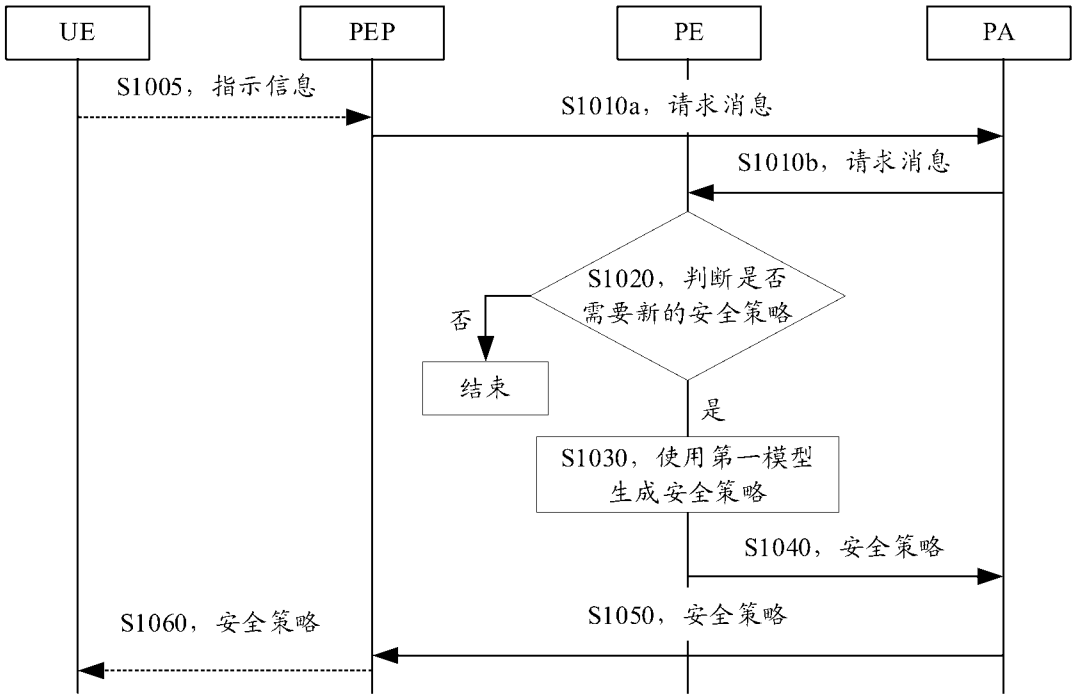
UE
PEP
PE
PA
S1005，指示信息
S1010a，请求消息
S1010b，请求消息
S1020，判断是否需要新的安全策略
否
结束
是
S1030，使用第一模型生成安全策略
S1040，安全策略
S1050，安全策略
S1060，安全策略

图 10

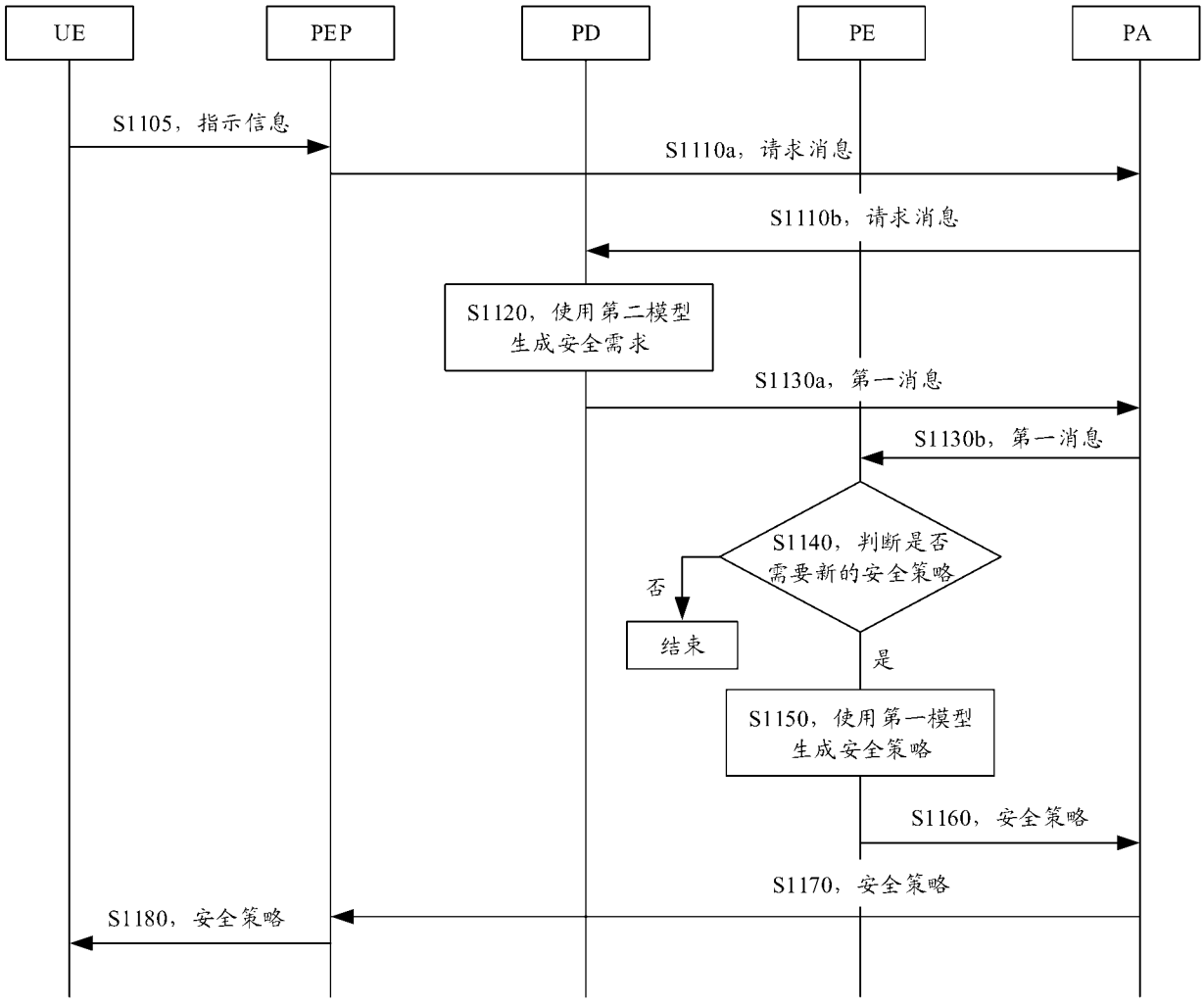
UE
PEP
PD
PE
PA
S1105，指示信息
S1110a，请求消息
S1110b，请求消息
S1120，使用第二模型生成安全需求
S1130a，第一消息
S1130b，第一消息
S1140，判断是否需要新的安全策略
否
结束
是
S1150，使用第一模型生成安全策略
S1160，安全策略
S1170，安全策略
S1180，安全策略

图 11

图 12

图 13

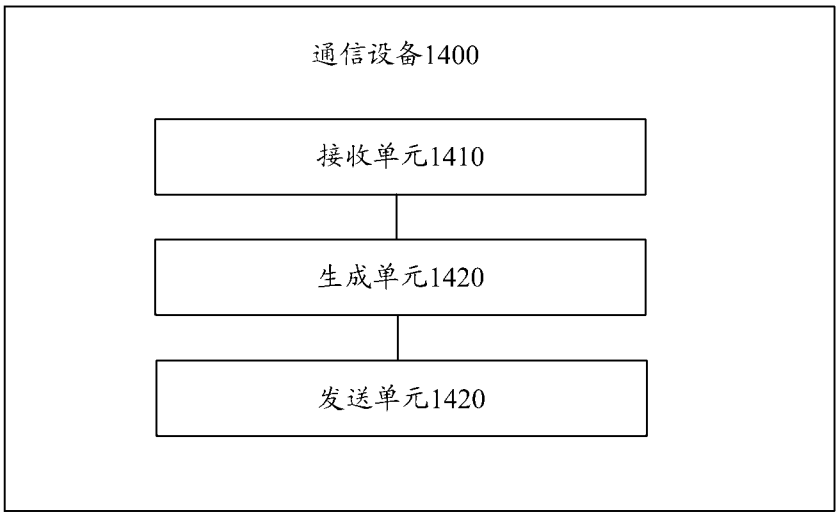

图 14

图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/142889

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/37(2021.01)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)

IPC:H04W,H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNTXT, ENTXT, ENTXTC, VEN, 3GPP, arXiv: 零信任, 架构, 组网, 安全策略, 生成, 制定, 业务, 相关, 关联, 需求, Zero Trust Architecture, security policy, safety, strategy, decision, association, related, request, demand, session, 5G, 6G

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2018187961 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 18 October 2018 (2018-10-18) claims 1-98, description, page 18, line 9 to page 31, line 6	1-72
X	CN 109600339 A (HUAWEI TECHNOLOGIES CO., LTD.) 09 April 2019 (2019-04-09) description, paragraphs 226-316	1-72
A	CN 115696332 A (CHINA ACADEMY OF INFORMATION AND COMMUNICATIONS TECHNOLOGY et al.) 03 February 2023 (2023-02-03) entire document	1-72
A	CN 113949573 A (TIANYI DIGITAL LIFE TECHNOLOGY CO., LTD.) 18 January 2022 (2022-01-18) entire document	1-72
A	RAMEZANPOUR, K. et al. "Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the context of O-RAN" *arXiv*, 27 July 2022 (2022-07-27), entire document	1-72

☑ 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
"D" document cited by the applicant in the international application
"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
09 August 2024	**21 August 2024**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/142889

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MITRE. "New KI: Support for Policy Decision Points and Policy Enforcement Points within 5GC SBA" *3GPP TSG-SA3 Meeting #110, S3-230720,* 24 February 2023 (2023-02-24), entire document	1-72

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2023/142889

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2018187961 A1	18 October 2018	CN 109863772 A	07 June 2019
CN 109600339 A	09 April 2019	US 2020228975 A1	16 July 2020
		WO 2019062672 A1	04 April 2019
		EP 3678412 A1	08 July 2020
		IN 202017014112 A	14 August 2020
		CN 114500008 A	13 May 2022
CN 115696332 A	03 February 2023	None	
CN 113949573 A	18 January 2022	None	

国际检索报告

国际申请号
PCT/CN2023/142889

A. 主题的分类

H04W 12/37(2021.01)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)

IPC:H04W,H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNTXT,ENTXT,ENTXTC,VEN,3GPP,arXiv:零信任,架构,组网,安全策略,生成,制定,业务,相关,关联,需求,Zero Trust Architecture,security policy,safety,strategy,decision,association,related,request,demand,session,5G,6G

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	WO 2018187961 A1 (华为技术有限公司) 2018年10月18日 (2018 - 10 - 18) 权利要求1-98，说明书第18页第9行-第31页第6行	1-72
X	CN 109600339 A (华为技术有限公司) 2019年4月9日 (2019 - 04 - 09) 说明书第226-316段	1-72
A	CN 115696332 A (中国信息通信研究院等) 2023年2月3日 (2023 - 02 - 03) 全文	1-72
A	CN 113949573 A (天翼数字生活科技有限公司) 2022年1月18日 (2022 - 01 - 18) 全文	1-72
A	RAMEZANPOUR, Keyvan et al. "Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the context of O-RAN" arXiv, 2022年7月27日 (2022 - 07 - 27), 全文	1-72

☑ 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

“D” 申请人在国际申请中引证的文件

“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
2024年8月9日	2024年8月21日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 贡伟洋 电话号码 (+86) 010-53961678

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
A	MITRE. "New KI: Support for Policy Decision Points and Policy Enforcement Points within 5GC SBA" 3GPP TSG-SA3 Meeting #110 S3-230720, 2023年2月24日 (2023 - 02 - 24), 全文	1-72

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/142889

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)
WO	2018187961	A1	2018年10月18日	CN	109863772	A	2019年6月7日
CN	109600339	A	2019年4月9日	US	2020228975	A1	2020年7月16日
				WO	2019062672	A1	2019年4月4日
				EP	3678412	A1	2020年7月8日
				IN	202017014112	A	2020年8月14日
				CN	114500008	A	2022年5月13日
CN	115696332	A	2023年2月3日	无			
CN	113949573	A	2022年1月18日	无			