

一种通信的方法及装置

技术领域

本申请实施例涉及无线通信技术领域，尤其涉及一种通信的方法及装置。

5 背景技术

在目前的无线网络中，存在多种类型的业务，比如，单播业务和多播业务等。单播业务和多播业务这两种不同类型的数据的安全需求可能不同。比如，多播业务可以是在线直播的带版权的体育赛事，多播业务数据包有加密的安全需求；多播业务也可以是在线直播的公开新闻资讯，多播业务数据包没有加密的安全需求。再比如，单播业务可以是终端回看的带版权的体育赛事，单播业务数据包有加密的安全需求；单播业务也可以是终端点播的公开新闻资讯，单播业务数据包没有加密的安全需求。

在现有机制中，终端完成注册后，通过协议数据单元（protocol data unit，PDU）会话建立流程建立终端和网络之间的单播传输链路，用来传输终端和网络之间的单播业务数据包。当终端和网络之间需要传输多播业务数据包时，终端发起多播业务加入过程。由于目前接入设备或者终端不具有使用多播传输方式的能力，多播业务数据包也需要通过单播传输链路方式发送给终端。此时，同一个 PDU 会话中需要传输两种业务的数据，即单播业务数据和多播业务数据。在这种场景下，如何保证多播业务数据包的传输安全是需要解决的问题。

20 发明内容

本申请提供一种通信的方法及装置，用以保证多播业务数据包的传输安全需求。

第一方面，提供一种通信的方法，该方法包括：接入设备向终端发送第一消息，所述第一消息包括第一指示，所述第一指示用于指示 PDU 会话的传输多播业务数据的数据无线承载（data radio bearer，DRB）的用户面安全激活状态，所述用户面安全激活状态包括完整性保护是否激活和/或机密性保护是否激活；并且，所述接入设备根据所述传输多播业务数据的 DRB 的用户面安全激活状态，配置多播的分组数据汇聚协议（packet data convergence protocol，PDCP）层实体。

所述第一指示所指示的传输多播业务数据包的 DRB 的用户面安全激活状态与所述 PDU 会话的传输单播业务数据包的 DRB 的用户面安全激活状态可能相同，也可能不同。接入设备向终端发送第一消息与接入设备配置多播 PDCP 层实体的先后循序不进行限制。

现有技术中，在一个 PDU 会话中，用户面安全激活状态为 PDU 会话粒度的，例如多播 DRB 的用户面安全激活状态可以默认以单播 DRB 的用户面安全激活状态为准。而在该实施例中，接入设备可以向终端指示多播 DRB 的用户面安全激活状态，终端就可以根据接入设备的第一指示，来确定多播 DRB 的用户面安全激活状态。这种指示的方式，相对于默认以单播 DRB 的用户面安全激活状态为准的方式，可以更加灵活地确定多播 DRB 的用户面安全激活状态，更加适用多播业务数据的传输安全需求。

在一种可能的实现中，所述接入设备向终端发送第一消息之前，所述接入设备可以先根据第一参数集合确定所述传输多播业务数据包的 DRB 的用户面安全激活状态，其中，

所述第一参数集合包括但不限于以下一种或多种参数：所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态、多播安全策略。此处的多播安全策略，可以是接入设备从 SMF 处获取的，该多播安全策略可以是根据签约信息生成的。

5 接入设备根据多个参数，来确定多播 DRB 的用户面安全激活状态，可以更加灵活地确定多播 DRB 的用户面安全激活状态，更加适用多播业务数据的传输安全需求。

在一种可能的实现中，所述接入设备在确定所述传输多播业务数据包的 DRB 的用户面安全激活状态时，具体可以是所述接入设备将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定为所述传输多播业务数据的 DRB 的用户面安全激活状态。也就是可以不考虑多播安全策略，以单播 DRB 的用户面安全激活状态为准，来确定多播
10 DRB 的用户面安全激活状态，单播 DRB 和多播 DRB 的用户面安全激活状态相同。

在一种可能的实现中，当所述传输单播业务数据的 DRB 的用户面安全激活状态为开启（开启可以等同于用户面安全激活状态为激活）时，所述接入设备将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定为所述传输多播业务数据的 DRB 的用户面安全激活状态。单播 DRB 的用户面安全激活状态为开启时，完整性保护激活和/
15 或机密性保护激活，此时以单播 DRB 的用户面激活状态为准，可以使确定的多播 DRB 的用户面安全激活状态也处于激活状态，保证多播的传输安全需求。

在一种可能的实现中，当所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭（关闭可以等同于用户面安全激活状态为去激活），且所述多播安全策略为偏好策略或不需要策略时，所述接入设备将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全
20 激活状态，确定为所述传输多播业务数据的 DRB 的用户面安全激活状态；其中，所述偏好策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启或关闭；所述不需要策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

当多播安全策略指示用户面安全激活状态为可关闭或可开启时，也就多播业务未强制开启安全传输，此时以单播 DRB 的用户面安全激活状态为准。当单播 DRB 的用户面安全
25 激活状态为关闭时，使确定的多播 DRB 的用户面安全激活状态也处于关闭（去激活）状态，避免多播业务进行安全保护而带来的传输复杂性。

在一种可能的实现中，所述接入设备确定所述传输多播业务数据包的 DRB 的用户面安全激活状态时，具体可以是接入设备根据多播安全策略，确定所述传输多播业务数据的 DRB 的用户面安全激活状态；所述多播安全策略为必须策略或者偏好策略或者不需要策略；
30 所述必须策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启；所述偏好策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启或关闭；所述不需要策略指示所述传输多播业务数据的 DRB 的用户面安全激活状态为关闭。也就是可以不考虑单播 DRB 的用户面安全激活状态，以多播安全策略为准，来确定多播 DRB 的用户面安全激活状态，这样可以更符合多播业务传输安全需求。

35 在一种可能的实现中，当所述传输单播业务数据的 DRB 的用户面安全激活状态为开启或关闭（开启可以等同于用户面安全激活状态为激活，关闭可以等同于用户面安全激活状态为去激活），且所述多播安全策略为必须策略（所述必须策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启）或不需要策略（所述不需要策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为关闭）时，所述接入设备根据
40 所述多播安全策略，确定所述 PDU 会话的传输多播业务数据的 DRB 的用户面安全激活状

态。

在该实施例中，在多播安全策略为必须策略时，指示多播 DRB 的用户面安全状态为开启（激活），此时不管单播 DRB 的用户面安全激活状态是否开启，都可以根据多播安全策略确定多播 DRB 的用户面安全激活状态，以保障多播业务的传输安全需求。在多播安全策略为不需要策略时，指示多播 DRB 的用户面安全激活状态为关闭（去激活），此时不管单播 DRB 的用户面安全激活状态是否开启，都可以根据多播安全策略确定多播 DRB 的用户面安全激活状态，以适应多播业务的传输安全需求，避免多播业务进行安全保护而带来的传输复杂性。

在一种可能的实现中，接入设备发送给终端的第一消息还包括但不限于以下指示中的一种或多种；第二指示、第三指示和第四指示。所述第二指示用于指示所述终端将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态修改为所述传输多播业务数据的 DRB 的用户面安全激活状态，或者，所述第二指示用于指示修改后的所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态；第二指示所指示的传输单播业务数据的 DRB 的用户面安全激活状态通常与传输多播业务数据的 DRB 的用户面安全激活状态相同。所述第三指示为需要修改用户面安全激活状态的 DRB 的标识；此处的 DRB 的标识为传输单播业务数据的 DRB 的标识。所述第四指示用于指示所述终端对所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态进行修改，通过第四指示可以显示指示终端对传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

通过接入设备向终端下发第二指示、第三指示和第四指示中的一种或多种指示，以便于终端根据多播 DRB 的用户面安全激活状态对单播 DRB 的用户面安全激活状态进行修改，以适用单播业务的传输安全需求。当然，在本申请中，协议可以预先规定，单播 DRB 的用户面安全激活状态以多播 DRB 的用户面安全激活状态为准，也就是接入设备即是不向终端下发第二指示、第三指示和第四指示中的一种或多种指示，终端也可以根据第一指示所指示的多播 DRB 的用户面安全激活状态，对单播 DRB 的用户面安全激活状态进行修改。

在一种可能的实现中，所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭或开启，且所述多播安全策略为必须时，接入设备向终端发送第一消息，可选的，该第一消息包括第二指示、第三指示和第四指示中的一种或多种指示。当多播安全策略为必须时，指示多播 DRB 的用户面安全激活状态为开启，此时以多播 DRB 的用户面安全激活状态为准，确定的单播 DRB 的用户面安全激活状态也为开启，可以保证单播业务的传输安全需求，保证业务传输安全不降级。

第二方面，提供了一种通信的方法，终端接收来自接入设备的第一消息，所述第一消息用于指示 PDU 会话的传输多播业务数据的 DRB 的用户面安全激活状态，所述用户面安全激活状态包括完整性保护是否激活和/或机密性保护是否激活。所述终端根据所述传输多播业务数据的 DRB 的用户面安全激活状态，配置多播的 PDCP 层实体。

现有技术中，在一个 PDU 会话中，多播 DRB 的用户面安全激活状态可以默认以单播 DRB 的用户面安全激活状态为准。而在该实施例中，接入设备可以向终端指示多播 DRB 的用户面安全激活状态，终端就可以根据接入设备的第一指示，来确定多播 DRB 的用户面安全激活状态。这种指示的方式，相对于默认以单播 DRB 的用户面安全激活状态为准的方式，可以更加灵活地确定多播 DRB 的用户面安全激活状态，更加适用多播业务数据

的传输安全需求。

在一种可能的实现中，所述第一消息还包括但不限于以下指示中的一种或多种；第二指示、第三指示和第四指示。所述第二指示用于指示所述终端将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态修改为所述传输多播业务数据的 DRB 的用户面安全激活状态，或者，所述第二指示用于指示修改后的所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态；第二指示所指示的传输单播业务数据的 DRB 的用户面安全激活状态通常与传输多播业务数据的 DRB 的用户面安全激活状态相同。所述第三指示为需要修改用户面安全激活状态的 DRB 的标识；此处的 DRB 的标识为单播 DRB 的标识。所述第四指示用于指示所述终端对所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态进行修改，通过第四指示可以显示指示终端对传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

在一种可能的实现中，当所述第一消息中包括第二指示时，所述终端根据所述传输多播业务数据的 DRB 的用户面安全激活状态，或者所述修改后的传输单播业务数据的 DRB 的用户面安全激活状态，对所述传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

在一种可能的实现中，当所述第一消息中包括第三指示时，所述终端修改所述标识的 DRB 的用户面安全激活状态。

在一种可能的实现中，当所述第一消息中包括第四指示时，所述终端对所述传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

通过接入设备向终端下发第二指示、第三指示和第四指示中的一种或多种指示，以便于终端根据多播 DRB 的用户面安全激活状态对单播 DRB 的用户面安全激活状态进行修改，以适用单播业务的传输安全需求。当然，在本申请中，协议可以预先规定，单播 DRB 的用户面激活状态以多播 DRB 的用户面安全激活状态为准，也就是接入设备即是不向终端下发第二指示、第三指示和第四指示中的一种或多种指示，终端也可以根据第一指示所指示的多播 DRB 的用户面安全激活状态，对单播 DRB 的用户面安全激活状态进行修改。

第三方面，提供了一种通信的方法，在拒绝多播业务数据传输的情况下，接入设备向 SMF 设备发送第一消息，所述第一消息包括第一指示，所述第一指示用于指示所述接入设备拒绝多播业务数据传输。SMF 设备在接收到来自接入设备的第一消息后，可以向 AMF 设备或者 UPF 设备发送接入设备拒绝多播业务数据传输的第一指示，以告知 AMF 设备或者 UPF 设备，该接入设备拒绝多播业务数据传输，以便 AMF 设备或者 UPF 设备进行相应的处理。

在一种可能的实现中，所述第一消息还可以包括第二指示，所述第二指示用于指示所述接入设备拒绝多播业务数据传输的原因。接入设备不但告知 SMF 设备接入设备拒绝多播传输，还告知拒绝的原因，以便 SMF 设备可以进行相应的处理。在某些情况下，第二指示和第一指示也可以是同一条指示。

在一种可能的实现中，所述拒绝多播业务数据传输的原因包括：所述 PDU 会话的多播业务数据传输安全需求与单播业务数据传输安全需求不一致或者无法满足多播业务传输安全要求。

在一种可能的实现中，接入设备还可以根据多播安全策略和 PDU 会话的传输单播业

务数据的 DRB 的用户面安全激活状态, 确定拒绝多播业务数据传输。

在一种可能的实现中, 所述传输单播业务数据的 DRB 的用户面安全激活状态为开启, 且所述多播安全策略为不需要策略时, 所述接入设备确定拒绝多播业务数据传输; 其中, 所述不需要策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

- 5 在一种可能的实现中, 所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭, 且所述多播安全策略为必须策略时, 所述接入设备确定拒绝多播业务数据传输; 其中, 所述必须策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为开启。

在这两种可能的实现中, 单播 DRB 的用户面安全激活状态, 与多播安全策略指示的多播 DRB 的用户面安全激活状态不一致, 则可以拒绝多播业务传输。

10

另外, 需要注意的是, 上述的第一方面至第三方面以及任一可能的实现中的多播安全策略, 可以是具体实施例方式中的第二多播安全策略, 该第二多播安全策略可以是多播上下文中的多播安全策略。

- 15 第四方面, 提供了一种通信的方法, SMF 设备通过 AMF 设备向接入设备发送第一消息, 所述第一消息包括 PDU 会话的第一多播安全策略, 所述第一多播安全策略为必须策略或不需要策略; 所述必须策略指示传输多播业务数据的 DRB 的用户面安全激活状态为开启; 所述不需要策略指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

- 20 所述第一多播安全策略所指示的传输多播业务数据包的 DRB 的用户面安全激活状态与所述 PDU 会话的传输单播业务数据包的 DRB 的用户面安全激活状态可能相同, 也可能不同。现有技术中, 在一个 PDU 会话中, 用户面安全激活状态为 PDU 会话粒度的, 例如, 多播 DRB 的用户面安全激活状态可以默认以单播 DRB 的用户面安全激活状态为准。而在该实施例中, SMF 设备向接入设备指示第一多播安全策略, 接入设备就可以根据第一多播安全策略, 来确定多播 DRB 的用户面安全激活状态。这种方式, 相对于默认以单播 DRB 的用户面安全激活状态为准的方式, 可以更加灵活地确定多播 DRB 的用户面安全激活状态, 更加适用多播业务数据的传输安全需求。

- 25 在一种可能的实现中, 所述 SMF 设备通过 AMF 设备向接入设备发送第一消息之前, 所述 SMF 设备根据第二参数集合确定所述第一多播安全策略; 其中, 所述第二参数集合包括以下一种或多种参数: 第二多播安全策略、所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态。SMF 设备根据多个参数, 来确定多播 DRB 的用户面安全激活状态, 可以更加灵活地确定多播 DRB 的用户面安全激活状态, 更加适用多播业务数据的传输安全需求。此处的第二多播安全策略, 可以是多播上下文中的多播安全策略。

- 30 在一种可能的实现中, 所述 SMF 设备根据所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态, 确定所述第一多播安全策略。具体的, 将传输单播业务数据的 DRB 的用户面安全激活状态确定为传输多播业务数据的 DRB 的用户面安全激活状态, 然后再根据确定的传输多播业务数据的 DRB 的用户面安全激活状态, 确定所述第一多播安全策略。示例的, 传输多播 (或单播) 业务数据的 DRB 的用户面安全激活状态为开启时, 所述第一多播安全策略为必须, 传输多播 (或单播) 业务数据的 DRB 的用户面安全激活状态为关闭时, 所述第一多播安全策略为不需要。也就是可以不考虑多播安全策略, 以单播 DRB 的用户面安全激活状态为准, 来确定多播 DRB 的用户面安全激活状态, 单播 DRB 和

40

多播 DRB 的用户面安全激活状态相同。

在一种可能的实现中，所述传输单播业务数据的 DRB 的用户面安全激活状态为开启时，所述 SMF 设备根据所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定所述第一多播安全策略；或者，所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭，且多播上下文中的第二多播安全策略为偏好策略或不需要策略时，SMF 设备根据所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定所述第一多播安全策略；其中，所述偏好策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启或关闭；所述不需要策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

当第二多播安全策略指示用户面安全激活状态为可关闭或可开启时，也就多播业务未强制开启安全传输，此时可以以单播 DRB 的用户面安全激活状态为准。当单播 DRB 的用户面安全激活状态为关闭时，使确定的多播 DRB 的用户面安全激活状态也处于关闭（去激活）状态，避免多播业务进行安全保护而带来的传输复杂性。

在一种可能的实现中，所述 SMF 设备根据所述第二多播安全策略，确定所述第一多播安全策略。示例的，第二多播安全策略为开启，则所述第一多播安全策略为开启，第二多播安全策略为关闭，则所述第一多播安全策略为关闭。也就是可以不考虑单播 DRB 的用户面安全激活状态，以第二多播安全策略为准，来确定多播 DRB 的用户面安全激活状态，这样可以更符合多播业务传输安全需求。

在一种可能的实现中，所述传输单播业务数据的 DRB 的用户面安全激活状态为开启或关闭，且所述第二多播安全策略为必须策略或不需要策略时，所述 SMF 设备根据所述第二多播安全策略，确定所述第一多播安全策略。

在该实施例中，在第二多播安全策略为必须策略时，指示多播 DRB 的用户面安全状态为开启（激活），此时不管单播 DRB 的用户面安全激活状态是否开启，都可以根据第二多播安全策略确定多播 DRB 的用户面安全激活状态，以保障多播业务的传输安全需求。在第二多播安全策略为不需要策略时，指示多播 DRB 的用户面安全激活状态为关闭（去激活），此时不管单播 DRB 的用户面安全激活状态是否开启，都可以根据第二多播安全策略确定多播 DRB 的用户面安全激活状态，以适应多播业务的传输安全需求，避免多播业务进行安全保护而带来的传输复杂性。

在一种可能的实现中，所述第一消息还包括：PDU 会话的标识和/或单播安全策略；其中，所述单播安全策略为必须策略或者不需要策略；所述必须策略用于指示所述传输单播业务数据的 DRB 的用户面安全激活状态为开启；所述不需要策略指示所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭。

通过 SMF 向接入设备下发 PDU 会话的标识和/或单播安全策略，以便于接入设备根据多播 DRB 的用户面安全激活状态对单播 DRB 的用户面安全激活状态进行修改，以适用单播业务的传输安全需求。当然，在本申请中，协议可以预先规定，单播 DRB 的用户面激活状态以多播 DRB 的用户面安全激活状态为准，也就是 SMF 设备即是不向接入设备下发 PDU 会话的标识和/或单播安全策略，接入设备也可以根据第一多播安全策略所指示的多播 DRB 的用户面安全激活状态，对单播 DRB 的用户面安全激活状态进行修改。

在一种可能的实现中，所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭或开启，且所述第二多播安全策略为必须策略时，所述 SMF 设备通过 AMF 设备向接入设

备发送第一消息。可选的，该第一消息包括 PDU 会话的标识和/或单播安全策略。当第二多播安全策略为必须时，指示多播 DRB 的用户面安全激活状态为开启，此时以多播 DRB 的用户面安全激活状态为准，确定的单播 DRB 的用户面安全激活状态也为开启，可以保证单播业务的传输安全需求，保证业务传输安全不降级。

5 在一种可能的实现中，所述第二多播安全策略可以根据以下参数中的一种或多种信息确定，例如传输模式、或业务信息、或签约信息、或者多播业务安全模式等参数。

当所述多播业务安全模式为：终端和核心网之间、或、终端与应用服务器之间进行安全保护的的模式时，所述 SMF 设备确定所述第二多播安全策略为不需要。也就是确定接入设备和终端之间的安全保护为不需要，可以避免重复进行安全保护而带来的冗余。

10

第五方面，提供了一种通信的方法，接入设备通过 AMF 设备接收来自 SMF 设备发送的第一消息，所述第一消息包括 PDU 会话的第一多播安全策略，所述第一多播安全策略为必须策略或不需要策略；所述必须策略指示传输多播业务数据的 DRB 的用户面安全激活状态为开启；所述不需要策略指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭。所述接入设备根据所述第一多播安全策略，确定传输多播业务数据的 DRB 的用户面安全激活状态，并配置多播的分组数据汇聚协议 PDCP 层实体。

15

所述第一多播安全策略所指示的传输多播业务数据包的 DRB 的用户面安全激活状态与所述 PDU 会话的传输单播业务数据包的 DRB 的用户面安全激活状态可能相同，也可能不同。现有技术中，在一个 PDU 会话中，多播 DRB 的用户面安全激活状态可以默认以单播 DRB 的用户面安全激活状态为准。而在该实施例，SMF 设备向接入设备指示第一多播安全策略，接入设备就可以根据第一多播安全策略，来确定多播 DRB 的用户面安全激活状态。这种方式，相对于默认以单播 DRB 的用户面安全激活状态为准的方式，可以更加灵活地确定多播 DRB 的用户面安全激活状态，更加适用多播业务数据的传输安全需求。

20

在一种可能的实现中，所述第一消息还包括：PDU 会话的标识和/或单播安全策略；其中，所述单播安全策略为必须策略或者不需要策略；所述必须策略用于指示所述传输单播业务数据的 DRB 的用户面安全激活状态为开启；所述不需要策略指示所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭。

25

在一种可能的实现中，所述接入设备根据所述单播安全策略和 PDU 会话的标识，修改所述标识的 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态。

30

通过 SMF 向接入设备下发 PDU 会话的标识和/或单播安全策略，以便于接入设备根据多播 DRB 的用户面安全激活状态对单播 DRB 的用户面安全激活状态进行修改，以适用单播业务的传输安全需求。当然，在本申请中，协议可以预先规定，单播 DRB 的用户面激活状态以多播 DRB 的用户面安全激活状态为准，也就是 SMF 设备即是不向接入设备下发 PDU 会话的标识和/或单播安全策略，接入设备也可以根据第一多播安全策略所指示的多播 DRB 的用户面安全激活状态，对单播 DRB 的用户面安全激活状态进行修改。

35

在一种可能的实现中，接入设备向终端发送第一指示，所述第一指示用于指示 PDU 会话的传输多播业务数据的 DRB 的用户面安全激活状态，所述用户面安全激活状态包括完整性保护是否激活和/或机密性保护是否激活；并且，所述接入设备根据所述传输多播业务数据的 DRB 的用户面安全激活状态，配置多播的分组数据汇聚协议 PDCP 层实体。

40

在一种可能的实现中，接入设备向终端发送以下指示中的一种或多种：第二指示、第

三指示和第四指示。所述第二指示用于指示所述终端将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态修改为所述传输多播业务数据的 DRB 的用户面安全激活状态，或者，所述第二指示用于指示修改后的所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态；第二指示所指示的传输单播业务数据的 DRB 的用户面安全激活状态通常与传输多播业务数据的 DRB 的用户面安全激活状态相同。所述第三指示为需要修改用户面安全激活状态的 DRB 的标识；此处的 DRB 的标识为单播 DRB 的标识。所述第四指示用于指示所述终端对所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态进行修改，通过第四指示可以显示指示终端对传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

通过接入设备向终端下发第二指示、第三指示和第四指示中的一种或多种指示，以便于终端根据多播 DRB 的用户面安全激活状态对单播 DRB 的用户面安全激活状态进行修改，以适用单播业务的传输安全需求。当然，在本申请中，协议可以预先规定，单播 DRB 的用户面安全激活状态以多播 DRB 的用户面安全激活状态为准，也就是接入设备即是不向终端下发第二指示、第三指示和第四指示中的一种或多种指示，终端也可以根据第一指示所指示的多播 DRB 的用户面安全激活状态，对单播 DRB 的用户面安全激活状态进行修改。

第六方面，提供了一种通信的方法，在拒绝多播业务数据传输的情况下，所述 SMF 设备通过 AMF 设备或 UPF 设备向接入设备发送第一消息，所述第一消息包括第一指示，所述第一指示用于指示所述 SMF 设备拒绝多播业务数据传输。SMF 设备向 AMF 设备或者 UPF 设备发送 SMF 设备拒绝多播业务数据传输的第一指示，以告知 AMF 设备或者 UPF 设备，该 SMF 设备拒绝多播业务数据传输，以便 AMF 设备或者 UPF 设备进行相应的处理。

在一种可能的实现中，所述第一消息还包括：第二指示，所述第二指示用于指示所述 SMF 设备拒绝多播业务数据传输的原因。SMF 设备不但告知 SMF 设备拒绝多播传输，还告知拒绝的原因，以便对应设备可以进行相应的处理。在某些情况下，第二指示和第一指示也可以是同一条指示。

在一种可能的实现中，所述拒绝多播业务数据传输的原因包括：所述 PDU 会话的多播业务数据传输安全需求与单播业务数据传输安全需求不一致或者无法满足多播业务传输安全要求。

在一种可能的实现中，SMF 设备根据 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态和第二多播安全策略，确定拒绝多播业务数据传输。此处的第二多播安全策略例如可以是多播上下文的多播安全策略。

在一种可能的实现中，所述传输单播业务数据的 DRB 的用户面安全激活状态为开启，且所述第二多播安全策略为不需要策略时，所述 SMF 设备确定拒绝多播业务数据传输，所述不需要策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

在一种可能的实现中，所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭，且所述第二多播安全策略为必须策略时，所述 SMF 设备确定拒绝多播业务数据传输，所述必须策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为开启。

在这两种可能的实现中，单播 DRB 的用户面安全激活状态，与第二多播安全策略指示的多播 DRB 的用户面安全激活状态不一致，则可以拒绝多播业务传输。

第七方面，提供了一种通信的装置，所述装置具有实现上述第一方面及第一方面任一可能的实现中的功能，或实现上述第二方面及第二方面任一可能的实现中的功能，或实现上述第三方面及第三方面任一可能的实现中的功能，或实现上述第四方面及第四方面任一可能的实现中的功能，或实现上述第五方面及第五方面任一可能的实现中的功能，或实现上述第六方面及第六方面任一可能的实现中的功能。这些功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的功能模块。

第八方面，提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行上述第一方面及第一方面任一可能的实现中由接入设备执行的方法，或执行上述第二方面及第二方面任一可能的实现中由终端执行的方法，或执行上述第三方面及第三方面任一可能的实现中由接入设备执行的方法，或执行上述第四方面及第四方面任一可能的实现中由 SMF 设备执行的方法，或执行上述第五方面及第五方面任一可能的实现中由接入设备执行的方法，或执行上述第六方面及第六方面任一可能的实现中由 SMF 设备执行的方法。

第九方面，本申请提供了一种芯片（可以称为芯片系统），该芯片系统包括处理器和存储器，所述处理器、所述存储器之间电耦合；所述存储器，用于存储计算机程序指令；所述处理器，用于执行所述存储器中的部分或者全部计算机程序指令，当所述部分或者全部计算机程序指令被执行时，用于实现上述第一方面及第一方面任一可能的实现的方法中接入设备的功能，或实现上述第二方面及第二方面任一可能的实现中终端的功能，或实现上述第三方面及第三方面任一可能的实现中接入设备的功能，或实现上述第四方面及第四方面任一可能的实现中 SMF 设备的功能，或实现上述第五方面及第五方面任一可能的实现中接入设备的功能，或实现上述第六方面及第六方面任一可能的实现中 SMF 设备的功能。

在一种可能的设计中，所述芯片系统还可以包括收发器，所述收发器，用于发送所述处理器处理后的信号，或者接收输入给所述处理器的信号。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。

第十方面，提供了一种计算机存储介质，用于存储计算机程序，所述计算机程序包括用于实现第一方面及第一方面任一可能的实现中的功能的指令，或用于实现第二方面及第二方面任一可能的实现中的功能的指令，或用于实现第三方面及第三方面任一可能的实现中的功能的指令，或用于实现第四方面及第四方面任一可能的实现中的功能的指令，或用于实现第五方面及第五方面任一可能的实现中的功能的指令，或用于实现第六方面及第六方面任一可能的实现中的功能的指令。

上述第七方面至第十方面的技术效果可以参照第一方面至第六方面中的描述，重复之处不再赘述。

附图说明

图1a为本申请实施例中的一种可能的通信系统示意图；

图1b为本申请实施例中的一种可能的通信系统示意图；

图2为本申请实施例中的一种可能的通信过程示意图；

- 图3为本申请实施例中的一种可能的通信过程示意图；
图4为本申请实施例中的一种可能的通信过程示意图；
图5为本申请实施例中的一种可能的通信过程示意图；
图6为本申请实施例中的一种可能的通信过程示意图；
5 图7为本申请实施例中的一种可能的通信过程示意图；
图8为本申请实施例中的一种可能的通信过程示意图；
图9为本申请实施例中的一种可能的通信装置结构图；
图10为本申请实施例中的一种可能的通信装置结构图；
图11为本申请实施例中的一种可能的通信装置结构图；
10 图12为本申请实施例中的一种可能的通信装置结构图。

具体实施方式

下面将结合附图，对本申请实施例进行详细描述。

在目前的无线网络中，存在多种类型的业务，比如，单播业务和多播业务等。针对单播业务，接入网设备在与终端设备建立的 PDU 会话中，分配/建立用于传输单播业务对应数据包的无线承载（data radio bearer, DRB）。一个 PDU 会话可以包括一个或者多个传输单播业务数据的 DRB，且所有的传输单播业务数据的 DRB 的用户面安全策略都与该 PDU 会话的用户面安全策略相同。接入网设备与不同的终端设备之间会建立不同的 PDU 会话，不同的 PDU 会话包括用于传输不同业务数据包的多播业务数据的 DRB。为了保护终端设备和接入网设备之间的用户面数据传输安全，接入网设备与不同终端设备之间生成不同的用户面安全密钥（包含加密密钥、完整性保护密钥），所述用户面安全密钥用于保护接入网设备与终端设备之间的用户面数据传输。比如，接入网设备需要给终端设备 1 发送单播业务的数据包 1，则接入网设备首先确定用于传输该数据包 1 的 PDU 会话 1 中的传输单播业务数据的 DRB1。之后，接入网设备根据 PDU 会话 1 对应的用户面安全策略（例如开启加密保护，不开启完整性保护），确定传输单播业务数据的 DRB1 的用户面安全激活状态。在从核心网接收到发送给终端设备 1 的数据包 1 时，接入网设备根据传输单播业务数据的 DRB1 的用户面安全激活状态对数据包 1 执行加密保护，并将加密保护后的数据包 1 发送给终端设备 1。终端设备 1 接收到加密保护的数据包 1 后，根据传输单播业务数据的 DRB1 的用户面安全激活状态对数据包 1 进行解密，得到明文的数据包 1。

当前，多播业务可以通过单播传输方式或者多播传输方式进行传输。针对单播传输方式，接入网设备可根据接收多播业务的终端设备数量，将从核心网节点接收到的数据包，复制多份。比如，接入网设备确定 3 个终端设备需接收该多播业务，则接入网设备可将核心网节点接收的数据包，复制 3 份，分别为数据包 1、数据包 2 和数据包 3。接入网设备向不同的 3 个终端设备分别发送上述数据包 1、数据包 2 和数据包 3。针对多播传输方式，接入网设备仅发送一份数据包，需要多个终端设备均支持该数据包的接收与处理。

单播业务数据包对应的一种类型的数据，即特定 UE 数据。多播业务数据包对应一种类型的数据，即多播业务数据。不同类型的数据的安全需求可能不同。比如，多播业务可以是在线直播的带版权的体育赛事，多播业务数据包有加密的安全需求；多播业务也可以是在线直播的公开新闻资讯，多播业务数据包没有加密的安全需求。再比如，单播业务可以是 UE 回看的带版权的体育赛事，单播业务数据包有加密的安全需求；单播业务也可以

是 UE 点播的公开新闻资讯, 单播业务数据包没有加密的安全需求。

在现有机制中, UE 完成注册后, 通过 PDU 会话建立流程建立 UE 和 AF 之间的单播传输链路, 用来传输 UE 和 AF 之间的单播业务数据包。当 UE 和 AF 之间需要传输多播业务数据包时, UE 发起多播业务加入过程, 由于目前接入设备或者 UE 不具有使用多播传输方式的能力, 多播业务数据包也需要通过单播传输承载方式发送给 UE。此时, 同一个 PDU 会话中需要传输两种业务的数据, 即单播业务数据和多播业务数据。在这种场景下, 如何同时保证单播业务数据包和多播业务数据包的安全需求是需要解决的问题。

在一种实施方式中, 在 PDU 会话建立过程中, 所建立的传输单播业务数据包的 DRB 使用的用户面安全激活状态满足 UE 特定数据的安全要求, 该 DRB 称为第一 DRB, 传输多播业务数据包的 DRB 也采用第一 DRB 的用户面安全激活状态, 该传输多播业务数据包的 DRB 称为第二 DRB。也就是, 对于一个 PDU 会话中, 所有 DRB 的安全激活状态完全相同, 也就是 PDU 会话粒度的安全需求。但在该实施方式中, 由于不同类型的数据安全需求不同, 存在数据泄露的风险。例如, 单播业务数据包要求不加密, 故第一 DRB 的用户面安全激活状态为机密性关闭, 但多播业务数据包要求加密时, 则第二 DRB 的用户面安全激活状态为机密性打开。如果按照单播业务数据包要求不加密的安全需求, 显然, 第一 DRB 的用户面安全激活状态无法满足多播业务数据包的安全要求。

基于此, 本申请提供了一种确定传输多播业务数据包的 DRB 的用户面安全激活状态的方式, 以适应多播业务数据包的安全性要求。能够保证无线接入网在单播承载传输多播业务数据包和单播业务数据包时, 满足多播业务和单播业务对于用户面的安全要求, 使得用户能够正确解析数据包。可选的, 还可以修改传输单播业务数据包的 DRB 的用户面安全激活状态, 以进一步适应单播业务数据包的安全性要求。

为便于理解本申请实施例的技术方案, 下面将对本申请实施例提供的通信的方法的系统架构进行简要说明。可理解的, 本申请实施例描述的系统架构是为了更加清楚的说明本申请实施例的技术方案, 并不构成对于本申请实施例提供的技术方案的限定。

本申请实施例的技术方案可以应用于各种通信系统, 例如: 无线局域网 (wireless local area network, WLAN) 通信系统, 全球移动通讯 (global system of mobile communication, GSM) 系统、码分多址 (code division multiple access, CDMA) 系统、宽带码分多址 (wideband code division multiple access WCDMA) 系统、通用分组无线业务 (general packet radio service, GPRS) 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)、通用移动通信系统 (universal mobile telecommunication system, UMTS)、全球互联微波接入 (worldwide interoperability for microwave access, WiMAX) 通信系统、第五代 (5th generation, 5G) 系统或新无线 (new radio, NR) 等。

以下作为示例性说明, 仅以第五代通信系统为例, 描述本申请实施例的应用场景以及本申请实施例的方法。

本申请以 5G 通信系统进行举例说明。

例如, 图 1a 为本申请可以适用的一种 5G 的通信系统架构示意图。具体的, 图 1a 为基于服务化架构的 5G 网络架构示意图。

例如, 图 1b 为本申请可以适用的另一种 5G 的通信系统架构示意图。具体的, 图 1b 为基于点对点的 5G 架构示意图。图 1a 与图 1b 的主要区别在于, 图 1a 中的各个网元之间

的接口是服务化的接口，图 1b 的各个网元之间的接口是点对点的接口。

图 1a 和图 1b 所示的 5G 网络架构中可包括终端设备部分、接入网部分、核心网部分。可选的，还包括数据网络（data network，DN）和应用功能（application function，AF）网元部分。终端通过接入网接入核心网，核心网与 DN 或 AF 进行通信。下面对其中的部分网元的功能进行简单介绍说明。

终端设备（terminal device），也可以称为用户设备（user equipment，UE），是一种具有无线收发功能的设备，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（如轮船等）；还可以部署在空中（例如飞机、气球和卫星上等）。所述终端设备可以是手机（mobile phone）、平板电脑（pad）、带无线收发功能的电脑、虚拟现实（virtual reality，VR）终端、增强现实（augmented reality，AR）终端、工业控制（industrial control）中的无线终端、无人驾驶（self driving）中的无线终端、远程医疗（remote medical）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。

本申请中的（R）AN 设备，是一种为终端设备提供无线通信功能的设备，（R）AN 设备也称为接入网设备。本申请中的 RAN 设备包括但不限于：5G 中的下一代基站（g nodeB，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（baseBand unit，BBU）、传输点（transmitting and receiving point，TRP）、发射点（transmitting point，TP）、移动交换中心等。在采用不同的无线接入技术的系统中，具备基站功能的设备的名称可能会有所不同，例如，在第五代（5th generation，5G）系统中，称为 RAN 或者 gNB（5G NodeB）；在 LTE 系统中，称为演进的节点 B（evolved NodeB，eNB 或者 eNodeB）；在第三代（3rd generation，3G）系统中，称为节点 B（Node B）等。

数据网络 DN，可部署多种业务，可为终端设备提供数据和/或语音等服务。例如，DN 是某智能工厂的私有网络，智能工厂安装在车间的传感器可为终端设备，DN 中部署了传感器和控制服务器，控制服务器可为传感器提供服务。传感器可与控制服务器通信，获取控制服务器的指令，根据指令将采集的传感器数据传送给控制服务器等。又例如，DN 是某公司的内部办公网络，该公司员工的手机或者电脑可为终端设备，员工的手机或者电脑可以访问公司内部办公网络上的信息、数据资源等。

应用网元，主要支持与第三代合作伙伴计划（3rd generation partnership project，3GPP）核心网交互来提供服务，例如影响数据路由决策，策略控制功能或者向网络侧提供第三方的一些服务。在 5G 通信系统中，该应用网元可以是应用功能（application function，AF）网元。在未来通信系统中，应用网元仍可以是 AF 网元，或者，还可以有其它的名称，本申请不做限定。

核心网部分可包括以下网元中的一个或多个：

接入管理网元，是由运营商网络提供的控制面网元，负责终端设备接入运营商网络的接入控制和移动性管理，例如包括移动状态管理，分配用户临时身份标识，认证和用户等功能。在 5G 通信系统中，该接入管理网元可以是接入与移动性管理功能（access and mobility

management function, AMF) 网元。在未来通信系统中, 接入管理网元仍可以是 AMF 网元, 或者, 还可以有其它的名称, 本申请不做限定。

会话管理网元, 主要负责移动网络中的会话管理, 如会话建立、修改、释放。具体功能如为用户分配 IP 地址、选择提供报文转发功能的用户面网元等。在 5G 通信系统中, 该
5 会话管理网元可以是会话管理功能 (session management function, SMF) 网元。在未来通信系统中, 会话管理网元仍可以是 SMF 网元, 或者, 还可以有其它的名称, 本申请不做限定。

用户面网元 负责终端设备中用户数据的转发和接收 可以从数据网络接收用户数据, 通过接入网设备传输给终端设备; 用户面网元还可以通过接入网设备从终端设备接收用户
10 数据, 转发到数据网络。用户面网元中为终端设备提供服务的传输资源和调度功能由 SMF 网元管理控制的。在 5G 通信系统中, 该用户面网元可以是用户面功能 (user plane function, UPF) 网元。在未来通信系统中, 用户面网元仍可以是 UPF 网元, 或者, 还可以有其它的名称, 本申请不做限定。

数据管理网元 用于生成认证信任状, 用户标识处理(如存储和管理用户永久身份等),
15 接入控制和签约数据管理等。在 5G 通信系统中, 该数据管理网元可以是统一数据管理 (unified data management, UDM) 网元。在未来通信系统中, 统一数据管理仍可以是 UDM 网元, 或者, 还可以有其它的名称, 本申请不做限定。

策略控制网元, 主要支持提供统一的策略框架来控制网络行为, 提供策略规则给控制层网络功能, 同时负责获取与策略决策相关的用户签约信息。在 4G 通信系统中, 该策略
20 控制网元可以是策略和计费规则功能 (policy and charging rules function, PCRF) 网元。在 5G 通信系统中, 该策略控制网元可以是策略控制功能 (policy control function, PCF) 网元。在未来通信系统中, 策略控制网元仍可以是 PCF 网元, 或者, 还可以有其它的名称, 本申请不做限定。

网络存储网元, 可用于提供网元发现功能, 基于其他网元的请求, 提供网元类型对应的网元信息。NRF 还提供网元管理服务, 如网元注册、更新、去注册以及网元状态订阅和
25 推送等。在 5G 通信系统中, 该网络存储网元可以是网络注册功能 (network repository function, NRF) 网元。在未来通信系统中, 网络存储网元仍可以是 NRF 网元, 或者, 还可以有其它的名称, 本申请不做限定。

网络开放功能网元, 可用于提供用于安全地向外部开放由 3GPP 网络功能设备提供的业务和能力等。在 5G 通信系统中, 网络开放功能网元可以是网络开放功能 (network
30 exposure function, NEF) 网元。在未来通信系统中, 网络开放功能网元仍可以是 NEF 网元, 或者, 还可以有其它的名称, 本申请不做限定。

网络切片选择网元, 可用于为终端的业务选择合适的网络切片。在 5G 通信系统中, 网络切片选择网元可以是网络切片选择功能 (network slice selection function, NSSF) 网元。
35 在未来通信系统中, 网络开放功能网元仍可以是 NSSF 网元, 或者, 还可以有其它的名称, 本申请不做限定。

网络数据分析网元, 可以从各个网络功能 (network function, NF), 例如策略控制网元、会话管理网元、用户面网元、接入管理网元、应用功能网元 (通过网络能力开放功能网元) 收集数据, 并进行分析和预测。在 5G 通信系统中, 网络数据分析网元可以是网络
40 数据分析功能 (network data analytics function, NWDAF)。在未来通信系统中, 网络开放

功能网元仍可以是 NWDAF 网元, 或者, 还可以有其它的名称, 本申请不做限定。

统一数据存储网元, 负责存储结构化的数据信息, 其中包括签约信息, 策略信息, 以及有标准格式定义的网络数据或业务数据。在 5G 通信系统中, 统一数据存储网元可以是统一数据存储 (unified data repository, UDR)。在未来通信系统中, 网络开放功能网元仍可以是 UDR 网元, 或者, 还可以有其它的名称, 本申请不做限定。

可以理解的是, 上述网元或者功能既可以是硬件设备中的网络元件, 也可以是在专用硬件上运行软件功能, 或者是平台 (例如, 云平台) 上实例化的虚拟化功能。一种可能的实现方式, 上述网元或者功能可以由一个设备实现, 也可以由多个设备共同实现, 还可以是一个设备内的一个功能模块, 本申请实施例对此不作具体限定。

为便于理解本申请实施例, 以下对本申请实施例的部分用语进行解释说明, 以便于本领域技术人员理解。

1)、PDU 会话: UE 和数据网络之间的关联, 用于提供 PDU 一个连接服务。

2)、DRB: 定义数据包在空口的处理。不同的 DRB 对应不同的数据包处理, 一个 PDU 会话中可以建立一个或者多个 DRB, 用于传输不同的 QoS 需求的业务。

3)、PDCP: 主要用于处理空中接口上承载网络层的分组数据, 比如安全功能 (加密和完整性保护) 的实现。一个 DRB 对应一个 PDCP 实体。

4) 完整性保护, 指在传输、存储信息或数据的过程中, 确保信息或数据不被未授权的设备更改或在更改后能够被迅速发现。另外, 需要说明的是本申请中的具有完整性保护的消息, 还可以具有机密性保护, 其中机密性保护指信息无法被未经授权的个人、实体、流程访问或披露。

接下来将结合附图对方案进行详细介绍。附图中以虚线标识的特征或内容可理解为本申请实施例的可选操作或者可选结构。需要注意的是, 本申请中“传输多播业务数据包的 DRB 的用户面安全激活状态”和“传输多播业务数据的 DRB 的用户面安全激活状态”为同一含义。另外, 下文中的“多播 DRB”为“传输多播业务数据包的 DRB”, 下文仅是为了简化描述进而方便理解, “多播 DRB”不对“传输多播业务数据包的 DRB”造成限定。同理, 下文中的“单播 DRB”为“传输单播业务数据包的 DRB”, “单播 DRB”不对“传输单播业务数据包的 PDU 会话的 DRB”造成限定。

图 2 为本申请实施例中的一种可能的通信过程示意图, 包括以下步骤:

步骤 201: 接入设备确定传输多播业务数据的 DRB 的用户面安全激活状态。

在一种示例 1 中, 接入设备根据第一参数集合确定所述传输多播业务数据包的 DRB 的用户面安全激活状态, 其中, 所述第一参数集合包括但不限于以下一种或多种参数: 所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态、多播安全策略。此处的多播安全策略可以是多播上下文的多播安全策略, 即下文描述的第二多播安全策略, 通常是由 SMF 设备生成的。该示例的具体过程在图 3 中进行介绍。此处的传输单播业务数据的 DRB 的用户面安全激活状态可以根据单播安全策略确定, 所述单播安全策略可以是 SMF 设备发送给接入设备的, 传输单播业务数据的 DRB 的用户面安全激活状态通常是在建立单播业务传输过程中确定的, 此处的传输单播业务数据的 DRB 的用户面安全激活状态可以是存储在签约信息中, 也有可能存储在 SMF 设备中的, 也有可能从 PCF 等网元获取。详细内容在后续图 3 的步骤 31 中介绍。

在一种示例 2 中, 所述接入设备根据第一多播安全策略确定所述传输多播业务数据包的 DRB 的用户面安全激活状态。此处的第一多播安全策略可以是 SMF 设备决定了传输多播业务数据的 DRB 的用户面安全激活状态后, 将该多播的 DRB 的状态转换为第一多播安全策略后发送给接入设备的, 与上一示例 1 的第二多播安全策略有所不同。该示例 2 的具体过程在图 5 中介绍。

在另一种示例 3 中, 接入设备可以从其它设备处获取传输多播业务数据的 DRB 的用户面安全激活状态, 例如接入设备接收 AMF 设备或 SMF 设备发送的传输多播业务数据的 DRB 的用户面安全激活状态。在示例的具体过程在图 7 中介绍。

在该示例 2 和示例 3 中, SMF 设备可以根据第二参数集合确定所述传输多播业务数据包的 DRB 的用户面安全激活状态, 其中, 所述第二参数集合包括但不限于以下一种或多种参数: 所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态、第二多播安全策略。

在另一种示例 4 中, 接入设备可以根据多播业务安全模式, 确定所述传输多播业务数据包的 DRB 的用户面安全激活状态。例如, 当所述多播业务安全模式为终端与核心网之间的安全保护模式时, 接入设备可以确定传输多播业务数据的 DRB 的用户面安全激活状态为关闭, 也就是确定接入设备和终端之间的安全保护为不需要, 可以避免重复进行安全保护而带来的冗余。该示例的具体过程在图 8 中介绍。

单播安全策略包括必须策略, 偏好策略, 不需要策略。必须策略用于指示传输单播业务数据的 DRB 的用户面安全激活状态为开启, 偏好策略用于指示传输单播业务数据的 DRB 的用户面安全激活状态可以为开启, 也可以为关闭。不需要策略用于指示传输单播业务数据的 DRB 的用户面安全激活状态为关闭。

多播安全策略包括必须策略, 偏好策略, 不需要策略。必须策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为开启, 偏好策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态可以为开启, 也可以为关闭。不需要策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

开启可以等同于用户面安全激活状态为激活, 关闭也就是不开启, 关闭可以等同于用户面安全激活状态为去激活。

步骤 202: 所述接入设备根据所述传输多播业务数据包的 DRB 的用户面安全激活状态, 配置多播的 PDCP 层实体。

步骤 203: 接入设备向终端发送第一消息, 相应的, 终端接收接入设备发送的第一消息, 所述第一消息包括第一指示, 所述第一指示用于指示 PDU 会话的传输多播业务数据的 DRB 的用户面安全激活状态, 所述用户面安全激活状态包括完整性保护是否激活和/或机密性保护是否激活。

上述步骤 202 和步骤 203 的先后顺序不进行限制。可以是接入设备先向终端发送第一消息, 再根据传输多播业务数据包的 DRB 的用户面安全激活状态, 配置多播的 PDCP 层实体。也可以是接入设备先根据传输多播业务数据包的 DRB 的用户面安全激活状态, 配置多播的 PDCP 层实体, 再向终端发送所述第一消息。也可以是两者同时执行。

步骤 204: 所述终端根据所述传输多播业务数据的 DRB 的用户面安全激活状态, 配置多播的 PDCP 层实体。

现有技术中, 在一个 PDU 会话中, 用户面安全激活状态为 PDU 会话粒度的, 通常多

播 DRB 的用户面安全激活状态可以默认以单播 DRB 的用户面安全激活状态为准。而在该实施例中,接入设备可以向终端指示多播 DRB 的用户面安全激活状态,终端就可以根据接入设备的第一指示,来确定多播 DRB 的用户面安全激活状态。这种指示的方式,相对于默认以单播 DRB 的用户面安全激活状态为准的方式,可以更加灵活地确定多播 DRB 的用户面安全激活状态,更加适用多播业务数据的传输安全需求。

可选的,接入设备还可以再重新确定单播 DRB 的用户面安全激活状态。

一种示例 1 中,接入设备根据第一参数集合确定所述传输单播业务数据包的 DRB 的用户面安全激活状态,其中,所述第一参数集合包括但不限于以下一种或多种参数:所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态、多播安全策略。该示例的具体过程在图 3 中介绍。

在一种示例 2 中,接入设备根据单播安全策略确定所述传输单播业务数据包的 DRB 的用户面安全激活状态。此处的单播安全策略可以是 SMF 设备决定了传输单播业务数据的 DRB 的用户面安全激活状态后,将该单播的 DRB 的状态转换为单播安全策略后发送给接入设备的。该示例的具体过程在图 5 中介绍。

在另一种示例 3 中,接入设备可以从其它设备处获取传输单播业务数据的 DRB 的用户面安全激活状态,例如接入设备接收 AMF 设备或 SMF 设备发送的传输单播业务数据的 DRB 的用户面安全激活状态。在示例的具体过程在图 7 中介绍。

在上述示例 2 和示例 3 中,SMF 设备可以根据第二参数集合确定所述传输单播业务数据包的 DRB 的用户面安全激活状态,其中,所述第二参数集合包括但不限于以下一种或多种参数:所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态、第二多播安全策略。

本申请中,接入设备或者 SMF 设备或者其它设备,在根据传输单播业务数据的 DRB 的用户面安全激活状态、第二多播安全策略(第一参数集合或第二参数集合),确定传输多播业务数据包的 DRB 的用户面安全激活状态和传输单播业务数据包的 DRB 的用户面安全激活状态时,可以分为以下 3 种方式,另外,在某些情况下,接入设备或者 SMF 设备或者其它设备也可以拒绝多播业务数据传输。

方式 1(单播为准):以传输单播业务数据包的 DRB 的用户面安全激活状态为准。

在执行方式 1 时,可以将传输单播业务数据的 DRB 的用户面安全激活状态,确定为传输多播业务数据的 DRB 的用户面安全激活状态。也就是单播 DRB 的用户面安全激活状态为开启时,多播 DRB 的用户面安全激活状态也为开启;单播 DRB 的用户面安全激活状态为关闭时,多播 DRB 的用户面安全激活状态也为关闭。

方式 2(多播为准):以传输多播业务数据包的 DRB 的用户面安全激活状态为准。传输多播业务数据包的 DRB 的用户面安全激活状态和传输单播业务数据包的 DRB 的用户面安全激活状态相同。该过程不仅涉及传输多播业务数据包的 DRB 的用户面安全激活状态的配置,也涉及已建立的传输单播业务数据包的 DRB 的用户面安全激活状态的改动。

在执行方式 2 时:可以根据第二多播安全策略,确定传输多播业务数据的 DRB 的用户面安全激活状态。例如,第二多播安全策略为必须策略,则确定传输多播业务数据的 DRB 的用户面安全激活状态为开启,第二多播安全策略为不需要策略,则确定传输多播业务数据的 DRB 的用户面安全激活状态为关闭。并将传输多播业务数据的 DRB 的用户面安全激活状态,作为传输单播业务数据的 DRB 的用户面安全激活状态,来对单播 DRB 进行修改。

- 方式3（各自为站）：传输多播业务数据包的DRB的用户面安全激活状态和传输多播业务数据包的DRB的用户面安全激活状态各不相关。该过程不涉及已建立的传输单播业务数据包的DRB的用户面安全激活状态的改动。可以理解的是，一个PDU会话中，多播DRB和单播DRB的用户面安全激活状态可能存在差别，即实现DRB粒度的用户面安全保护。
- 5 在执行方式3时：可以根据第二多播安全策略，确定传输多播业务数据的DRB的用户面安全激活状态。
- 方式4：拒绝多播业务数据传输。

- 10 参见以下表1所示，介绍了在哪种场景下，采用上述方式1至方式4中的哪种方式。
- 表1

场景	单播安全策略	传输单播业务数据包的DRB的用户面安全激活状态	多播安全策略	推荐方式
1	必须	on（开启）	必须/preferred（偏好）	方式1
2	必须	on	不需要	方式1（安全不降级）/ 方式3/ 方式4
3	不需要	off（关闭）	不需要/preferred	方式1
4	不需要	off	必须	方式2（安全不降级）/ 方式3/ 方式4
5	preferred	on	必须/preferred	方式1
6	preferred	on	不需要	方式1（安全不降级）/ 方式3/ 方式4
7	preferred	off	不需要/preferred	方式1
8	preferred	off	必须	方式2（安全不降级）/ 方式3/ 方式4

- 示例的，结合场景1、2、5、6，所述传输单播业务数据的DRB的用户面安全激活状态为开启时，多播安全策略可以是必须策略，或偏好策略，或不需要策略，采用方式1：以单播为准。
- 15 单播DRB的用户面安全激活状态为开启时，完整性保护激活和/或机密性保护激活，此时以单播DRB的用户面激活状态为准，可以使确定的多播DRB的用户面安全激活状态也处于激活状态，保证多播的传输安全需求。
- 示例的，结合场景3和7，所述传输单播业务数据的DRB的用户面安全激活状态为关

闭,且所述多播安全策略为偏好策略或不需要策略时,采用方式1:以单播为准。

当多播安全策略指示用户面安全激活状态为可关闭或可开启时,也就多播业务未强制安全传输,此时以单播 DRB 的用户面安全激活状态为准。当单播 DRB 的用户面安全激活状态为关闭时,使确定的多播 DRB 的用户面安全激活状态也处于关闭(去激活)状态,避免多播业务进行安全保护而带来的传输复杂性。

示例的,结合场景4和8,当所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭或开启,且所述多播安全策略为必须策略时,采用方式2:以多播为准。

当多播安全策略为必须时,指示多播 DRB 的用户面安全激活状态为开启,此时以多播 DRB 的用户面安全激活状态为准,确定的单播 DRB 的用户面安全激活状态也为开启,可以保证单播业务的传输安全需求,保证业务传输安全不降级。

示例的,结合场景2、4、6和8,当所述传输单播业务数据的 DRB 的用户面安全激活状态为开启,且所述多播安全策略为不需要策略时,采用方式3。当所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭,且所述多播安全策略为必须策略时,采用方式3。

也就是单播 DRB 的用户面安全激活状态,与多播安全策略指示的多播 DRB 的用户面安全激活状态不一致,则可以单播 DRB 和多播 DRB 可以相互独立、互相解耦。

示例的,当所述传输单播业务数据的 DRB 的用户面安全激活状态为开启,且所述多播安全按策略为需要策略时,采用方式3。当所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭,且所述多播安全按策略为不需要策略时,采用方式3。也就是单播 DRB 与多播 DRB 的传输安全需求一致时,也可以相互独立,互相解耦,以适应各自的业务传输安全需求。

示例的,结合场景2、4、6和8,当所述传输单播业务数据的 DRB 的用户面安全激活状态为开启,且所述多播安全策略为不需要策略时,采用方式4。当所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭,且所述多播安全策略为必须策略时,采用方式4。

也就是单播 DRB 的用户面安全激活状态,与多播安全策略指示的多播 DRB 的用户面安全激活状态不一致,则可以拒绝多播业务传输。

针对方式2,以传输多播业务数据包的 DRB 的用户面安全激活状态为准。

在一可选的示例中,上述步骤203中的第一消息还包括以下指示中的一种或多种;第二指示、第三指示和第四指示;

所述第二指示用于指示所述终端将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态修改为所述传输多播业务数据的 DRB 的用户面安全激活状态。或者,所述第二指示用于指示修改后的所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态;第二指示所指示的修改后的传输单播业务数据的 DRB 的用户面安全激活状态,通常与传输多播业务数据的 DRB 的用户面安全激活状态相同,此时第二指示可以为单独的 IE,与多播 DRB 的用户面安全激活状态的第一指示相同,当然该第二指示也可以不携带。

所述第三指示为需要修改用户面安全激活状态的 DRB 的标识;此处的 DRB 的标识为单播的 DRB 的标识。可以是一个,也可以是多个。如果不携带第三指示,可以是对当前 PDU session 下的所有单播 DRB 的用户面安全激活状态进行修改。

所述第四指示用于指示所述终端对所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态进行修改, 通过第四指示可以显示指示终端对传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

5 接入设备通过向终端下发第二指示、第三指示和第四指示中的一种或多种指示, 以便于终端对单播的用户面安全激活状态进行修改, 以适用单播的传输安全需求。

另外, 接入设备还可以执行步骤 202a:

步骤 202a: 接入设备将所述传输多播业务数据包的 DRB 的用户面安全激活状态确定为传输单播业务数据包的 DRB 的用户面安全激活状态, 并修改已配置的单播的 PDCP 层实体。

10 相应的, 终端在接收到第一消息后, 还可以执行步骤 204a:

步骤 204a: 终端将所述传输多播业务数据包的 DRB 的用户面安全激活状态确定为传输单播业务数据包的 DRB 的用户面安全激活状态, 并修改已配置的单播的 PDCP 层实体。

具体的, 终端在接收到第二指示时, 所述终端可以根据所述传输多播业务数据的 DRB 的用户面安全激活状态, 或者所述修改后的传输单播业务数据的 DRB 的用户面安全激活状态, 对所述传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

15 终端在接收到第三指示时, 所述终端可以修改所述标识的 DRB 的用户面安全激活状态。

终端在接收到第四指示时, 所述终端可以对所述传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

20 当然, 在本申请中协议可以预先规定, 单播 DRB 的用户面激活状态以多播 DRB 的用户面安全激活状态为准, 也就是接入设备不向终端下发第二指示、第三指示和第四指示中的一种或多种指示, 接入设备也执行步骤 202a, 终端也执行步骤 204a。

接下来结合图 3, 对接入设备来决定采用方式 1 至方式 3 这三种方式中的任一方式的通信过程进行详细说明。在该示例中, SMF 设备将多播上下文中的第二多播安全策略不进行改动, 直接发送给接入设备, 则接入设备参考第二多播安全策略和单播 DRB 的用户面安全激活状态, 决定采用方式 1 至方式 3 这三种方式中的任一方式。

在图 3 中, 当前为 UE 服务的 SMF 是 SMF1。SMF1 可以是锚点 SMF。如果 SMF1 不是锚点 SMF, 则 SMF2 为锚点 SMF。同理, 当前处理 UE 的 PDU 会话的 UPF 是 UPF1。UPF1 可以是锚点 UPF。如果 UPF1 不是锚点 UPF, 则 UPF2 为锚点 UPF。

30 图 2 中的 SMF 设备为图 3 中的 SMF1 设备。

步骤 31: 终端注册, 并建立 PDU 会话。

UE 注册到网络中, 并与 AF 建立 PDU 会话。PDU 会话建立完成后, UE 和接入设备之间建立了单播 DRB。在 PDU 会话建立过程中, SMF1 向接入设备发送单播用户面安全策略 (在本申请中, 将用户面安全策略简称为安全策略), 相应的, 接入设备接收 SMF1 发送的单播安全策略。

接入设备根据单播安全策略, 确定单播 DRB 的用户面安全激活状态, 并根据确定的单播 DRB 的用户面安全激活状态, 配置单播 DRB 的安全保护方法, 例如配置单播的 PDCP 层实体。

40 所述单播安全策略可以为完整性保护: 必须策略/偏好 preferred 策略/不需要策略; 机

密性保护：必须策略/ preferred 策略 /不需要策略。所述单播 DRB 的用户面安全激活状态可以为完整性保护开启/关闭；机密性保护开启/关闭。接入设备在确定单播 DRB 的用户面安全激活状态时不会违背单播安全策略。

5 当所述单播安全策略为必须策略时，接入设备可以确定单播 DRB 的用户面安全激活状态为开启。示例的，完整性保护必须，则单播 DRB 的用户面安全激活状态为完整性保护开启。机密性保护必须，则单播 DRB 的用户面安全激活状态为机密性开启。当安全策略为必须时，对应的单播 DRB 的用户面安全激活状态为开启，这种对应关系可以是接入设备与 SMF1 预先约定的，则接入设备无需向 SMF1 通知单播 DRB 的用户面安全状态。

10 当所述安全策略为不需要策略时，接入设备可以确定单播 DRB 的用户面安全激活状态为关闭。示例的。完整性保护不需要，则单播 DRB 的用户面安全激活状态为完整性保护关闭。机密性保护不需要，则单播 DRB 的用户面安全激活状态为机密性关闭。当安全策略为不需要时，对应的单播 DRB 的用户面安全激活状态为关闭，这种对应关系可以是接入设备与 SMF1 预先约定的，则接入设备无需向 SMF1 通知用户面安全状态。

15 当所述安全策略为 preferred 时（表示可激活，也可去激活），可选的，接入设备来决定单播 DRB 的用户面安全激活状态。例如，接入设备决定用户面安全激活状态为完整性保护开启，机密性保护关闭。或者接入设备决定用户面安全保护为完整性保护关闭，机密性保护关闭。或者接入设备决定用户面安全激活状态为完整性保护开启，机密性保护开启。或者接入设备决定用户面安全保护为完整性保护关闭，机密性保护开启。进一步可选的，接入设备还可以将决定的单播 DRB 的用户面安全激活状态发送给 SMF1。

20 经过上述过程，SMF1 可以获知接入设备使用的单播 DRB 的用户面安全激活状态。

另外，单播安全策略为 PDU 会话粒度的，即一个 PDU 会话中多个不同的单播 DRB 的用户面安全激活状态相同。

25 步骤 32：服务提供商（例如 AF）可以通过上层（比如应用层等）消息（例如 multicast announcement 多播服务告知消息），告知 UE 开始提供多播服务，上层消息中至少包括多播标识，例如多播标识为提供多播服务的多播 IP 地址。

步骤 33：UE 在接收到该上层消息后，可以加入多播服务。

30 在一种示例中，UE 可以通过用户面方式加入多播服务。具体的，UE 可以向 UPF1 发送多播加入消息，该多播加入消息为用户面消息，多播加入消息中包括多播标识。UPF1 可以充当多播路由器的作用，UPF1 在接收来自 UE 的多播加入消息后，可以向 SMF1 发送用户面事件通知消息，该用户面事件通知消息为信令面消息，用户面事件通知消息中携带多播标识，例如多播标识为多播 IP 地址。

35 在另一种示例中，UE 可以通过信令面方式加入多播服务。具体的，UE 可以向 AMF 发送 PDU 会话修改请求消息，该 PDU 会话修改请求消息中包括多播标识。AMF 在接收到来自 UE 的 PDU 会话修改请求消息后，可以向 SMF1 发送消息，所述消息中包括多播标识，例如多播标识为多播 IP 地址。

UE 可以选择上述两种方式中的任一种方式加入多播服务，也可以通过其它方式加入多播服务。

40 步骤 34：SMF1 在接收到多播标识后，SMF1 可以向 UDM 进行多播传输会话检查，即检查 UDM 中是否存在多播标识对应的多播上下文（比如 QoS 信息）。具体的，SMF1 向 UDM 发送多播标识，例如多播标识为多播 IP 地址。UDM 在接收到来自 SMF1 的多播

标识后,可以检查 UDM 中是否存在该多播标识对应的多播上下文。

如果存在,UDM 可以向 SMF1 发送该多播标识对应的多播上下文,多播上下文包括第二多播安全策略。可选的,多播上下文中还包括锚点 SMF 的信息,即锚点 SMF 为 SMF2,以及锚点 SMF 对应的路由信息,即如何找到锚点 SMF。UDM 中保存的第二多播安全策略为 SMF2 确定后,保存到 UDM 中的。

如果不存在,则 SMF1 为锚点 SMF,UDM 可以指示 SMF1 创建多播上下文,多播上下文中包括第二多播安全策略。则 SMF1 可以确定多播上下文,并将该多播上下文保存到 UDM 中,也就是将该第二多播安全策略保存到 UDM 中,以便其它设备调用。

示例的,SMF1 或 SMF2 可以根据传输模式、或业务信息、或签约信息、或者多播业务安全模式等参数,确定第二多播安全策略。第二多播安全策略可以为完整性保护必须/preferred/不需要,机密性保护必须/preferred/不需要。

传输模式指多播传输或广播传输。多播业务安全模式可以为模式 1: UE 和接入设备之间进行安全保护的(也就是终端和接入设备之间进行安全保护),也可以是模式 2: UE 和核心网之间或终端与应用服务器之间进行安全保护的(也就是终端和核心网/应用服务器之间进行安全保护),此处核心网网元可以是多播广播业务用户面网元(multicast/broadcast service user plane, MBSU)或用户面网关(user plane gateway, UPF/UPGW)等。模式 3: UE 和接入设备之间、接入网设备和核心网/应用服务器分别进行安全保护的

模式。示例的,当传输模式为广播传输时,可以确定第二多播安全策略为不需要策略。当传输模式为多播传输时,SMF1 可以根据业务信息或签约信息或者多播业务安全模式确定第二多播安全策略。当多播业务安全模式为模式 2 时,可以确定第二多播安全策略为不需要策略。这样可以避免在终端与核心网之间已经进行安全保护的基础上,再对终端与基站进行安全保护而带来的安全保护冗余。当多播业务安全模式为模式 1 或模式 3 时,SMF1 可以根据业务信息或签约信息确定第二多播安全策略。例如签约信息中包括指示信息,来指示第二多播安全策略。

如果 SMF1 非锚点 SMF,SMF2 为锚点 SMF,SMF2 上维护有多播上下文,多播上下文包括第二多播安全策略等。SMF1 可以执行步骤 35-步骤 37,以向 SMF2 请求第二多播安全策略。

如果 SMF1 为锚点 SMF,SMF1 创建多播上下文,该多播上下文中包括第二多播安全策略。则可以跳过步骤 35-步骤 37,直接执行步骤 38。也就是说步骤 35-步骤 37 为可选项。

步骤 35: SMF1 配置 SMF2 通过单播传输承载传输多播业务数据。示例的,SMF1 向 SMF2 (锚点 SMF) 发送多播会话传输请求消息,请求建立多播业务数据用户面,该多播会话传输请求消息中携带多播标识,例如多播标识为多播 IP 地址。

步骤 36: SMF2 在接收到来自 SMF1 发送的多播会话传输请求消息后,SMF2 可以向 UPF2 进行 N4 会话修改,即配置 UPF2 向 UPF1 发送多播业务数据。示例的,SMF2 向 UPF2 发送 N4 会话修改请求消息,其中包括 UPF1 的路由信息。

步骤 37: SMF2 向 SMF1 发送多播会话传输响应消息,该多播会话传输响应消息中包括第二多播安全策略。相应的,SMF1 接收来自 SMF2 的第二多播安全策略。

步骤 38: SMF1 判断当前的单播 DRB 的用户面安全激活状态是否符合第二多播安全策略要求。如果符合,SMF1 则可以配置 UPF1 通过单播传输承载发送多播业务数据。示

例的, SMF1 向 UPF1 发送 N4 会话修改请求消息。

如果不符合, 可以拒绝多播业务数据传输。SMF1 拒绝多播业务数据传输后的具体过程, 与图 6 中的 SMF1 设备确定采用方式 4: 拒绝多播业务数据传输后的具体过程相同。并且不再执行步骤 39 及后续步骤。

- 5 具体的, SMF1 在拒绝多播业务数据传输时, 可以将拒绝多播业务数据传输的指示信息告知接入设备和 UE。

 示例的, 在步骤 33 中, 如果 UE 通过用户面方式加入多播服务, 则 SMF1 可以通过 UPF1 告知接入设备和 UE 拒绝多播业务数据传输, 例如 SMF1 向 UPF1 发送用户面事件通知响应消息, 该消息为信令面消息, 消息中携带拒绝多播业务数据传输的指示和/拒绝原因值。然后, UPF1 向接入设备发送多播业务数据传输的指示和/拒绝原因值。

10 示例的, 在步骤 33 中, 如果 UE 通过信令面方式加入多播服务, 则 SMF1 可以通过 AMF 告知接入设备和 UE 拒绝多播业务数据传输, 例如 SMF1 向 AMF 发送消息, 消息中包括拒绝多播业务数据传输的指示和/拒绝原因值。AMF 再将拒绝多播业务数据传输的指示和/拒绝原因值发送给接入设备。

- 15 单播 DRB 的用户面安全激活状态不符合第二多播安全策略要求的判断条件可以包括但不限于下述条件中的一种:

 单播 DRB 的用户面安全激活状态为开启, 第二多播用户面安全策略为不需要; 或者单播 DRB 的用户面安全激活状态为关闭, 第二多播用户面安全策略为必须。

20 上述的步骤 38 中: SMF1 判断当前单播 DRB 的用户面安全激活状态是否符合第二多播安全策略要求的过程, 是可选的, SMF1 也可以跳过该判断过程, 继续执行: SMF1 配置 UPF1 通过单播传输承载发送多播业务数据。

 步骤 39: SMF1 向 AMF 发送配置消息, 该配置信息包括业务配置信息和第二多播安全策略。在上述步骤 34-步骤 37 中已经介绍过, 如果 SMF1 是锚点 SMF, 该第二多播安全策略是 SMF1 创建的多播安全上下中包含的。如果 SMF1 不是锚点 SMF, SMF2 是锚点 SMF, 该第二多播安全策略是 SMF1 从 SMF2 处获取的。

 步骤 310: AMF 在接收到来自 SMF1 的业务配置信息和第二多播安全策略后, 可以向接入设备发送 N2 会话修改请求消息, 该会话修改请求消息中携带上述步骤 39 中的业务配置信息和第二多播安全策略。相应的, 接入设备接收来自 AMF 的业务配置信息和第二多播安全策略。

30 步骤 311: 接入设备根据业务配置信息中的公共信息, 确定该业务用来传输多播业务数据。此处判断的是接入设备与 UPF 之间是否满足条件。具体的, 所述公共信息可以包括但不限于以下的一种或多种:

- 1) 业务标识, 如 TMGI、多播组标识 group Id、业务的 IP 多播地址。
35 2) 传输多播组地址信息, 用于接入设备加入该组播接收该业务。
 3) 公共通道的隧道信息 (针对已建立公共通道的场景)。

 例如, 业务配置信息对应的业务属于可用于多个 UE 共同接收的业务, 则该业务可以用来传输多播业务数据。

 如果该业务可以用来传输多播业务数据, 接入设备根据公共信息将该业务关联到一个公共数据通道上, 该公共数据通道是 UPF1 到接入设备之间的一个公共数据通道上。该公

40

共数据通道向接收该业务的 UE 提供服务。

该公共数据通道可以为之前已经建立好的，也可以是此时触发建立的，公共数据通道的建立方式可以采用现有的建立方式，此处不再详细赘述。

本申请不关注，该业务不用来传输多播业务数据的情况。则步骤 311 是一个可选项，也可以不执行，直接执行步骤 312。相应的，步骤 39 和步骤 310 中的业务配置信息也是可选的。

步骤 312：接入设备选择执行上述方式 1 单播为准、方式 2 多播为准和方式 3 相互独立中的任一种方式。

具体的，接入设备创建多播 DRB，确定多播 DRB 的用户面安全激活状态，配置多播的 PDCP 层实体安全，用于传输多播业务数据。在确定多播 DRB 的用户面安全激活状态时，接入设备可以根据单播 DRB 的用户面安全激活状态、第二多播安全策略等参数（步骤 201 处描述的第一参数集合中的参数）确定多播 DRB 的用户面安全激活状态。

可选的，接入设备如果选择方式 2，还可以根据多播 DRB 的用户面安全激活状态，修改单播 DRB 的用户面安全激活状态，以及修改已配置的单播 DRB 的 PDCP 层实体。

在配置多播 PDCP 层实体安全的过程中，可包含将密钥和算法与多播 PDCP 实体关联的过程，具体的过程可参见现有的方式，不再详细介绍。多播 PDCP 层实体所关联的密钥和算法可以与单播 PDCP 层实体所关联的密钥和算法相同，也可以不同。后续，接入网设备可根据上述多播的 PDCP 实体安全的配置，对多播业务的数据包进行用户面安全保护；而终端设备根据多播 PDCP 实体安全的配置，对多播业务的数据包进行解用户面安全保护，实现了对多播业务的用户面安全保护。

步骤 312 与步骤 313 的先后顺序可以不进行限制。

步骤 313：当执行方式 1 至方式 3 的任一方式时，接入设备还可以向终端发送第一指示，该第一指示可以用于指示 PDU 会话的多播 DRB 的用户面安全激活状态。相应的，UE 接收来自接入设备的第一指示。示例的，接入设备通过 RRC 重配置信息，发送该第一指示。此处的 RRC 重配置消息可以对应图 2 的步骤 203 中的第一消息，第一指示可以对应图 2 的步骤 203 中的第一指示。

接入设备选择执行方式 2 以多播为准时，可以是协议规定，传输单播业务数据包的 DRB 的用户面安全激活状态以传输多播业务数据包的 DRB 的用户面安全激活状态为准，也可以是接入设备向终端发送指示信息，来指示所述终端根据多播 DRB 的用户面安全激活状态修改单播 DRB 的用户面安全激活状态，具体可以参见上面描述的图 2 的步骤 203 中的第一消息中第二指示、第三指示和第四指示，此处不再重复赘述。

步骤 314：UE 在接收到来自接入设备的第一指示所指示的用于指示多播 DRB 的用户面安全激活状态时，终端配合接入设备创建多播 DRB，并且 UE 可以根据该第一指示配置多播的 PDCP 层实体安全，用于传输所述多播业务数据。

可选的，如果 UE 还可能接收到第二指示、第三指示和第四指示中的一个或多个。UE 在接收到这些指示信息后执行的操作在上述过程中已经介绍，此处不再重复。或者协议规定多播为准，即使接入设备不向终端发送第二指示、第三指示和第四指示中的一个或多个指示信息，来指示所述终端根据多播 DRB 的用户面安全激活状态修改单播 DRB 的用户面安全激活状态，终端也会对单播 DRB 的用户面安全激活状态进行修改，以及对已配置的单播 PDCP 层实体进行修改。

无论是接入设备还是 UE，配置多播 PDCP 实体安全的过程，可包含将密钥和算法与多播 PDCP 实体关联的过程。

步骤 315: 接入设备向 AMF 发送 N2 会话修改回复消息。示例的，针对步骤 310 中的 N2 会话修改请求消息的回复消息。

5 步骤 316: AMF 向 SMF1 发送回复消息。示例的，针对步骤 39 中的配置消息的回复消息。

步骤 317: 多播业务数据从 AF 发送到 UPF2。

步骤 318: 多播业务数据从 UPF2 发送到 UPF1。

步骤 319: 多播业务数据从 UPF1 发送到接入设备。

10 步骤 320: 接入设备选择单播承载，可根据上述多播 PDCP 实体安全的配置，对多播业务数据进行用户面安全保护。

步骤 321: 多播业务数据从接入设备发送给 UE。

综上，图 3 介绍了接入设备参考第二多播安全策略和单播 DRB 的用户面安全激活状态，来决定采用方式 1 至方式 3 中的任一方式的通信过程。

15

接下来参见如图 4 所示，提供了一种接入设备参考第二多播安全策略和单播 DRB 的用户面安全激活状态，来决定采用方式 4: 拒绝多播业务传输的通信过程示意图。该示例中的第一消息、第一指示和第二指示，与上面图 2 和图 3 的示例中的第一消息、第一指示和第二指示无关。

20 步骤 41-步骤 411 与图 3 中的步骤 31-步骤 311 相同，重复之处不再赘述。

步骤 412: 接入设备选择执行方式 4: 拒绝多播业务数据传输。

接入设备可以根据第二多播安全策略和 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定拒绝多播业务数据传输。通常单播的 DRB 的用户面安全激活状态，与第二多播安全策略指示的多播的 DRB 的用户面安全激活状态不一致，则可以拒绝多播业务传输。

25

在一种示例中，所述传输单播业务数据的 DRB 的用户面安全激活状态为开启，且所述第二多播安全策略为不需要策略时，所述接入设备确定拒绝多播业务数据传输；其中，所述不需要策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

30 在另一种示例中，所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭，且所述第二多播安全策略为必须策略时，所述接入设备确定拒绝多播业务数据传输；其中，所述必须策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为开启。

步骤 413: 接入设备向 SMF 设备发送第一消息，所述第一消息包括第一指示，所述第一指示用于指示所述接入设备拒绝多播业务数据传输。

35 可选的，所述第一消息还包括：第二指示，所述第二指示用于指示所述接入设备拒绝多播业务数据传输的原因。接入设备不但告知 SMF 设备接入设备拒绝多播传输，还告知拒绝的原因，以便 SMF 设备可以进行相应的处理。在某些情况下，第二指示和第一指示也可以是同一条指示。

示例的，所述拒绝多播业务数据传输的原因包括：所述 PDU 会话的多播业务数据传输安全需求与单播业务数据传输安全需求不一致或者无法满足多播业务传输安全要求。

40 在步骤 43 中，如果终端通过信令面加入多播服务，则执行步骤 414a: SMF 设备在接

收到来自接入设备的第一消息后，可以向 AMF 设备发送接入设备拒绝多播业务数据传输的第一指示，以告知 AMF 设备接入设备拒绝多播业务数据传输，以便进行相应的处理。

步骤 415a: AMF 设备在接收到接入设备拒绝多播业务数据传输的第一指示时，还可以将该第一指示告知接入设备。

- 5 在步骤 43 中，如果终端通过信令面加入多播服务，则执行步骤 414b: SMF 设备在接收到来自接入设备的第一消息后，可以向 UPF1 设备发送接入设备拒绝多播业务数据传输的第一指示，以告知 UPF 设备接入设备拒绝多播业务数据传输，以便进行相应的处理。

步骤 415b: UPF1 设备在接收到接入设备拒绝多播业务数据传输的第一指示时，还可以将该第一指示告知接入设备。

- 10 步骤 416: 接入设备在接收到来自 AMF 或 UPF1 的第一指示后，可以将拒绝多播业务数据传输的第一指示告知终端。

可选的，在上述的步骤 413、步骤 414a、步骤 414b、步骤 415a、步骤 415b、以及步骤 416 中，均可以携带第二指示：第二指示用于指示所述接入设备拒绝多播业务数据传输的原因。

- 15 综上，介绍了接入设备参考第二多播安全策略和单播 DRB 的用户面安全激活状态，来决定采用方式 4 的通信过程。

接下来参见如图 5 所示，提供了一种 SMF 设备参考第二多播安全策略和单播 DRB 的用户面安全激活状态，来决定采用方式 1 至方式 3 中的任一方式的通信过程。

- 20 步骤 51-步骤 58 与图 3 中的步骤 31-步骤 38 相同，重复之处不再赘述。经过步骤 58 后，SMF1 获取到了第二多播安全策略。

- 步骤 59a: SMF1 根据单播 DRB 的用户面安全激活状态、第二多播安全策略（步骤 201 处描述的第而参数集合中的参数）决定使用方式 1、方式 2、还是方式 3。也就是确定多播 DRB 的用户面安全激活状态，可选的，还可以确定单播 DRB 的用户面安全激活状态。该
25 过程可以参见上面的表 1，及对应的描述，此处不再重复赘述。此处的传输单播业务数据的 DRB 的用户面安全激活状态可以是存储在签约信息中，也有可能存储在 SMF1 设备本地的，也有可能从 PCF 等网元获取。

步骤 59: SMF1 向 AMF 发送第一多播安全策略。可选的，还发送业务配置信息。

- 值得注意的是，此处第一多播安全策略与步骤 57 之前获取到的第二多播安全策略不同，步骤 57 之前获取到的第二多播安全策略包括必须策略、偏好 preferred 策略和不需要策略。上述图 3 中的步骤 31 中已经介绍过 SMF1 下发给接入设备偏好 preferred 策略时，是由接入设备来决定单播 DRB 的用户面安全激活状态，同理，如果 SMF1 下发给接入设备的第一多播安全策略为偏好 preferred 策略时，由接入设备来决定多播 DRB 的用户面安全激活状态。在该示例中，主要关注由 SMF1 设备决定多播 DRB 的用户面安全激活状态，
30 所以步骤 59 中的第一多播安全策略可以不包括 preferred 状态。当步骤 59a 中确定的多播 DRB 用户面安全激活状态为开启时，步骤 59 中的第一多播安全策略为必须策略。当步骤 59a 中确定的多播 DRB 的用户面安全激活状态为关闭时，步骤 59 中的第一多播安全策略为不需要策略。

- 可选的，如果 SMF1 选择执行方式 2 以多播为准，需要对单播 DRB 的用户面安全激活状态进行修改时，步骤 59 中还可以发送单播安全策略和/或 PDU session ID。以便于接入
40

设备根据单播安全策略对单播 DRB 的用户面安全激活状态进行修改。PDU session ID 对应一个或多个 DRB ID。接入设备感知 DRB，SMF 不感知 DRB，所以 SMF1 下发的是 PDU session ID。如果 SMF1 选择执行方式 1 以单播为准，或者选择执行方式 3 各自为准，则可以不对单播 DRB 的用户面安全激活状态进行修改，则可以携带单播安全策略和 PDU session ID。

当然也可以是协议规定，以多播为准，这样无需发送单播安全策略和/或 PDU session ID，接入设备也会根据多播 DRB 的用户面安全激活状态，对单播 DRB 的用户面安全激活状态进行修改。

步骤 59 中的单播安全策略可以不包括 preferred 状态。当步骤 59a 中确定的单播 DRB 用户面安全激活状态为开启时，步骤 59 中的单播安全策略为必须策略。当步骤 59a 中确定的单播 DRB 的用户面安全激活状态为关闭时，步骤 59 中的单播安全策略为不需要策略。步骤 59 中的第一多播安全策略与单播安全策略通常是相同的，即第一多播安全策略为必须策略时，单播安全策略也为必须策略，第一多播安全策略为不需要时，单播安全策略也为不需要策略。这样才能保证以多播为准。

步骤 510: AMF 在接收到来自 SMF1 的第一多播安全策略后，可以向接入设备发送消息，消息中携带上述步骤 59 中的第一多播安全策略。可选的，还携带单播安全策略和/或 PDU session ID。该消息例如可以是 N2 会话修改请求消息。

相应的，接入设备接收来自 AMF 的业务配置信息和第一多播安全策略。可选的，还可以接收到单播安全策略和/或 PDU session ID。

可选的，消息中携带上述步骤 59 中的业务配置信息。

可选的，步骤 511: 接入设备根据业务配置信息中的公共信息，确定该业务用来传输多播业务数据。该过程与图 3 中的步骤 311 相同，重复之处不再赘述。步骤 512: 接入设备创建多播 DRB，并根据步骤 510 中的第一多播安全策略确定多播 DRB 的用户面安全激活状态，还可以配置多播的 PDCP 层实体安全，用于传输多播业务数据。可选的，还可以修改单播 DRB 的用户面安全激活状态，以及修改已配置的单播 DRB 的 PDCP 层实体。例如，根据步骤 510 中的单播安全策略和/或 PDU 会话的标识，修改对应的单播 DRB 的用户面安全激活状态，或者即使步骤 510 中不包括单播安全策略和/或 PDU 会话的标识，终端也可以根据多播 DRB 的用户面安全激活状态，修改单播 DRB 的用户面安全激活状态。

步骤 513: 接入设备还可以向终端发送第一指示，该第一指示可以用于指示 PDU 会话的多播 DRB 的用户面安全激活状态，相应的，UE 接收来自接入设备的第一指示。示例的，接入设备通过 RRC 重配置信息，发送该第一指示。此处的 RRC 重配置消息可以对应图 2 的步骤 203 中的第一消息，第一指示可以对应图 2 的步骤 203 中的第一指示。

如果接入设备接收到单播安全策略和/或 PDU session ID，则接入设备还可以向终端发送指示信息，来指示所述终端根据多播 DRB 的用户面安全激活状态修改单播 DRB 的用户面安全激活状态，具体可以参见上面描述的图 2 的步骤 203 中的第一消息中第二指示、第三指示和第四指示，此处不再重复赘述。

或者，协议规定以多播为准，即使接入设备未接收到单播安全策略和/或 PDU session ID，则接入设备也可以向终端发送第二指示、第三指示和第四指示，来指示所述终端根据多播 DRB 的用户面安全激活状态修改单播 DRB 的用户面安全激活状态。

再或者，协议规定多播为准，即使接入设备不向终端发送第二指示、第三指示和第四

指示中的至少一个指示信息,来指示所述终端根据多播 DRB 的用户面安全激活状态修改单播 DRB 的用户面安全激活状态,终端也会对单播 DRB 的用户面安全激活状态进行修改。

步骤 512 与步骤 513 的先后顺序可以不进行限制。

步骤 514 至步骤 521 与图 3 中的步骤 314 至步骤 321 相同,重复之处不再赘述。

5 综上,图 5 介绍了 SMF 设备参考第二多播安全策略和单播 DRB 的用户面安全激活状态,来决定采用方式 1 至方式 3 中的任一方式的通信过程。

接下来参见如图 6 所示,提供了一种 SMF 设备参考第二多播安全策略和单播 DRB 的用户面安全激活状态,来决定采用方式 4: 拒绝多播业务传输的通信过程示意图。该示例
10 中的第一消息、第一指示和第二指示,与上面图 2、图 3 和图 5 的示例中的第一消息、第一指示和第二指示无关。

步骤 61-步骤 68 与图 3 中的步骤 31-步骤 38 相同,重复之处不再赘述。

步骤 69: SMF 设备选择执行方式 4: 拒绝多播业务数据传输。

SMF 设备可以根据第二多播安全策略和 PDU 会话的传输单播业务数据的 DRB 的用户
15 面安全激活状态,确定拒绝多播业务数据传输。通常单播的 DRB 的用户面安全激活状态,与第二多播安全策略指示的多播的 DRB 的用户面安全激活状态不一致,则可以拒绝多播业务传输。具体示例可参见上述描述,不再重复介绍。

在步骤 63 中,如果终端通过信令面加入多播服务,则执行步骤 610a: SMF 设备向 AMF
20 设备发送接入设备拒绝多播业务数据传输的第一指示,以告知 AMF 设备接入设备拒绝多播业务数据传输,以便进行相应的处理。步骤 611a: AMF 设备在接收到接入设备拒绝多播业务数据传输的第一指示时,还可以将该第一指示告知接入设备。

在步骤 63 中,如果终端通过信令面加入多播服务,则执行步骤 610b: SMF 设备向 UPF1
25 设备发送接入设备拒绝多播业务数据传输的第一指示,以告知 UPF 设备接入设备拒绝多播业务数据传输,以便进行相应的处理。步骤 611b: UPF1 设备在接收到接入设备拒绝多播业务数据传输的第一指示时,还可以将该第一指示告知接入设备。

步骤 612: 接入设备在接收到来自 AMF 或 UPF1 的第一指示后,可以将接入设备拒绝多播业务数据传输的第一指示告知终端。

可选的,在上述的步骤 610a、步骤 610b、步骤 611a、步骤 611b、以及步骤 612 中,
均可以携带第二指示: 第二指示用于指示所述接入设备拒绝多播业务数据传输的原因。
30 SMF 设备不但告知 AMF 设备或 UPF 设备 SMF 设备拒绝多播传输,还告知拒绝的原因,以便对应设备可以进行相应的处理。在某些情况下,第二指示和第一指示也可以是同一条指示。示例的,所述拒绝多播业务数据传输的原因包括: 所述 PDU 会话的多播业务数据传输安全需求与单播业务数据传输安全需求不一致或者无法满足多播业务传输安全要求。

综上,介绍了 SMF 设备参考第二多播安全策略和单播 DRB 的用户面安全激活状态,
35 来决定采用方式 4 的通信过程。

接下来结合图 7 所示,提供了另一种 SMF 设备参考第二多播安全策略和单播 DRB 的用户面安全激活状态,来决定采用方式 1 至方式 3 中的任一方式的通信过程。与图 5 的示例的不同之处在于: 图 5 的示例中, SMF 设备通过第一多播安全策略告知接入设备,多播
40 DRB 的用户面安全激活状态,在图 7 的示例中, SMF 设备直接将多播 DRB 的用户面安全

激活状态告知接入设备。

步骤 71-步骤 79a, 与图 5 中的步骤 51-步骤 59a 相同, 重复之处不再赘述。经过步骤 79a, SMF1 确定出了多播 DRB 的用户面安全激活状态, 可选的, 还可能确定出了单播 DRB 的用户面安全激活状态。

- 5 步骤 79: SMF1 向 AMF 发送多播 DRB 的用户安全激活状态。可选的, 还发送业务配置信息。

可选的, 步骤 79 中还可以发送单播 DRB 的用户面安全激活状态和/或 PDU session ID。

- 10 步骤 710: AMF 在接收到来自 SMF1 的多播 DRB 的用户面安全激活状态后, 可以向接入设备发送消息, 消息中携带上述步骤 59 中的多播 DRB 的用户面安全激活状态。可选的, 还携带单播 DRB 的用户面安全激活状态和/或 PDU session ID。该消息例如可以是 N2 会话修改请求消息。

相应的, 接入设备接收来自 AMF 的业务配置信息和多播 DRB 的用户面安全激活状态。可选的, 还可以接收到单播 DRB 的用户面安全激活状态和/或 PDU session ID。

可选的, 还可以向接入设备发送业务配置信息。

- 15 步骤 79 和步骤 710 中的单播 DRB 的用户面安全激活状态, 也可以替换为单播安全策略, 与图 5 的示例类似。

可选的, 步骤 711: 接入设备根据业务配置信息中的公共信息, 确定该业务用来传输多播业务数据。该过程与图 3 中的步骤 311 相同, 与图 5 中的步骤 511 相同重复之处不再赘述。

- 20 步骤 712: 接入设备创建多播 DRB, 并根据步骤 710 中的多播 DRB 的用户面安全激活状态配置多播的 PDCP 层实体安全, 用于传输多播业务数据。可选的, 还可以修改单播 DRB 的用户面安全激活状态, 以及修改已配置的单播 DRB 的 PDCP 层实体。例如, 根据步骤 710 中的单播 DRB 的用户面安全激活状态和/或 PDU 会话的标识, 修改对应的单播 DRB 的用户面安全激活状态, 或者即使步骤 710 中不包括单播 DRB 的用户面安全激活状态和/或 PDU 会话的标识, 终端也可以根据多播 DRB 的用户面安全激活状态, 修改单播 DRB 的用户面安全激活状态。

步骤 713: 接入设备还可以向终端发送第一指示, 该第一指示可以用于指示 PDU 会话的多播 DRB 的用户面安全激活状态。

- 30 可选的, 接入设备也可以向终端发送第二指示、第三指示和第四指示, 来指示所述终端根据多播 DRB 的用户面安全激活状态修改单播 DRB 的用户面安全激活状态。

步骤 712 与步骤 713 的先后顺序可以不进行限制。

步骤 714 至步骤 721 与图 5 中的步骤 514 至步骤 521 相同, 重复之处不再赘述。

综上, 图 7 介绍了 SMF 设备参考第二多播安全策略和单播 DRB 的用户面安全激活状态, 来决定采用方式 1 至方式 3 中的任一方式的通信过程。

- 35 接下来参见图 8 所示, 介绍了一种接入设备根据多播业务安全模式, 确定所述传输多播业务数据包的 DRB 的用户面安全激活状态。

步骤 81: SMF 设备向 AMF 设备发送多播业务安全模式。

- 40 多播业务安全模式可以为模式 1: UE 和接入设备之间进行安全保护的模式 (也就是终端和接入设备之间进行安全保护), 也可以是模式 2: UE 和核心网或者终端和应用服务器

之间进行安全保护的模式（也就是终端和核心网/应用服务器之间进行安全保护）。也可以是模式 3：UE 和接入设备之间、接入网设备和核心网/应用服务器分别进行安全保护的模
式。

5 步骤 82：AMF 在接收到来自 SMF1 的多播业务安全模式后，向接入设备发送所述多播业务安全模式。相应的，接入设备接收所述多播业务安全模式。

步骤 83：接入设备创建多播 DRB，根据多播业务安全模式确定多播 DRB 的用户面安全激活状态，配置多播的 PDCP 层实体安全，用于传输多播业务数据。

10 当多播业务安全模式为终端和接入设备之间进行安全保护的模式时，或者为 UE 和接入设备之间、接入网设备和核心网/应用服务器分别进行安全保护的模
式时，可以确定多播 DRB 的用户面安全激活状态为开启。

当多播业务安全模式为终端和核心网之间或这终端和应用服务器之间进行安全保护的模
式时，可以确定多播 DRB 的用户面安全激活状态为关闭。这样可以避免在终端与核
心网之间已经进行安全保护的基础上，再对终端与基站进行安全保护而带来的安全保护冗
余。

15 在图 8 的该示例中，可选的，SMF 设备还可以决定单播 DRB 的用户面安全激活状态，
并下发给接入设备。例如，与图 5 的示例类似，向接入设备下发单播安全策略。再例如，
与图 7 的示例类似，向接入设备下发单播 DRB 的用户面安全激活状态。

在图 8 的该示例中，可选的，接入设备还可以决定单播 DRB 的用户面安全激活状态。
例如，与图 3 的示例类似。

20 可选的，接入设备还可以根据多播 DRB 的用户面安全激活状态，修改单播 DRB 的用
户面安全激活状态，以及修改已配置的单播 DRB 的 PDCP 层实体。

步骤 84：接入设备向终端发送第一指示来指示多播 DRB 的用户面安全激活状态，可
选的，还可以发送第二指示，第三指示、第四指示中的一个或多个，来指示修改单播 DRB
的用户面安全激活状态。与上述图 3、图 5 和图 7 的示例相同，重复之处不再赘述。

25 步骤 85：终端创建多播 DRB，确定多播 DRB 的用户面安全激活状态，配置多播的 PDCP
层实体安全，用于传输多播业务数据。可选的，终端还可以修改单播 DRB 的用户面安全
激活状态，以及修改已配置的单播 DRB 的 PDCP 层实体。

图 3 的示例、图 5 的示例和图 7 的示例均可以与图 8 的示例结合，形成的技术方案，
均在本申请的保护范围内。

30 示例的，图 8 的示例可以与图 5 的示例结合，SMF1 通过 AMF 设备向接入设备发送单
播安全策略和/或 PDU 会话的标识。

示例的，图 8 的示例可以与图 7 的示例结合，SMF1 通过 AMF 设备向接入设备发送单
播 DRB 的用户面安全激活状态和/或 PDU 会话的标识。

35 另外，接入设备中也可以预先配置有多播业务保护方式，例如模式 1，或模式 2，或
模式 3。接入设备无需从 SMF 设备处获取，就可以根据预先配置的多播业务安全模式，确
定多播 DRB 的用户面安全激活状态，配置多播的 PDCP 层实体安全，用于传输多播业务
数据。

40 前文介绍了本申请实施例的通信的方法，下文中将介绍本申请实施例中的通信装置。
方法、装置是基于同一技术构思的，由于方法、装置解决问题的原理相似，因此装置与方

法的实施可以相互参见。

基于与上述通信方法的同一技术构思，如图 9 所示，提供了一种通信装置 900，装置 900 可以包括：收发模块 920，处理模块 910，可选的，还包括存储模块 930；处理模块 910 可以分别与存储模块 930 和收发模块 920 相连，所述存储模块 930 也可以与收发模块 920 相连。

在一种示例中，装置 900 能够执行上述图 2-图 8 的方法中由接入设备执行的各个步骤。装置 900 可以为接入设备，也可以为应用于接入设备中的芯片。

在一种示例中，所述收发模块 920，用于向终端发送第一消息，所述第一消息包括第一指示，所述第一指示用于指示 PDU 会话的传输多播业务数据的数据无线承载 DRB 的用户面安全激活状态，所述用户面安全激活状态包括完整性保护是否激活和/或机密性保护是否激活；所述处理模块 910，用于根据所述传输多播业务数据的 DRB 的用户面安全激活状态，配置多播的分组数据汇聚协议 PDCP 层实体。

在一种示例中，所述处理模块 910，用于根据第一参数集合确定所述传输多播业务数据的 DRB 的用户面安全激活状态，其中，所述第一参数集合包括以下一种或多种参数：所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态、第二多播安全策略。

在一种示例中，所述处理模块 910，具体用于将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定为所述传输多播业务数据的 DRB 的用户面安全激活状态。

在一种示例中，所述处理模块 910，具体用于当所述传输单播业务数据的 DRB 的用户面安全激活状态为开启时，将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定为所述传输多播业务数据的 DRB 的用户面安全激活状态。或者，当所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭，且所述第二多播安全策略为偏好策略或不需要策略时，将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定为所述传输多播业务数据的 DRB 的用户面安全激活状态；其中，所述偏好策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启或关闭；所述不需要策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

在一种示例中，所述处理模块 910，具体用于根据所述第二多播安全策略，确定所述传输多播业务数据的 DRB 的用户面安全激活状态；所述第二多播安全策略为必须策略或者偏好策略或者不需要策略；所述必须策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启；所述偏好策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启或关闭；所述不需要策略指示所述传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

在一种示例中，所述处理模块 910，具体用于当所述传输单播业务数据的 DRB 的用户面安全激活状态为开启或关闭，且所述第二多播安全策略为必须策略或不需要策略时，根据所述第二多播安全策略，确定所述 PDU 会话的传输多播业务数据的 DRB 的用户面安全激活状态。

在一种示例中，所述第一消息还包括以下指示中的一种或多种：第二指示、第三指示和第四指示；所述第二指示用于指示所述终端将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态修改为所述传输多播业务数据的 DRB 的用户面安全激活状态，或者，所述第二指示用于指示修改后的所述 PDU 会话的传输单播业务数据的 DRB 的用户面

安全激活状态；所述第三指示为需要修改用户面安全激活状态的 DRB 的标识；所述第四指示用于指示所述终端对所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

5 在一种示例中，所述处理模块 910，具体用于当所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭或开启，且所述第二多播安全策略为必须策略时，通过所述收发模块 920 向终端发送第一消息。可选的，所述第一消息包括第二指示，第三指示、第四指示中的一种或多种。

10 在一种示例中，在拒绝多播业务数据传输的情况下，所述收发模块 920，用于向 SMF 设备发送第一消息，所述第一消息包括第一指示，所述第一指示用于指示所述装置拒绝多播业务数据传输。

在一种示例中，所述处理模块 910，用于根据第二多播安全策略和 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定拒绝多播业务数据传输。

15 在一种示例中，所述处理模块 910，具体用于当所述传输单播业务数据的 DRB 的用户面安全激活状态为开启，且所述第二多播安全策略为不需要策略时，确定拒绝多播业务数据传输，所述不需要策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭；或者，所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭，且所述第二多播安全策略为必须策略时，确定拒绝多播业务数据传输，所述必须策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为开启。

20 在一种示例中，所述收发模块 920，用于通过 AMF 设备接收来自 SMF 设备发送的第一消息，所述第一消息包括 PDU 会话的第一多播安全策略，所述第一多播安全策略为必须策略或不需要策略；所述必须策略指示传输多播业务数据的 DRB 的用户面安全激活状态为开启；所述不需要策略指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭；所述处理模块 910，用于根据所述第一多播安全策略，确定传输多播业务数据的 DRB 的用户面安全激活状态，并配置多播的分组数据汇聚协议 PDCP 层实体。

25 在一种示例中，所述第一消息还包括：PDU 会话的标识和/或单播安全策略；其中，所述单播安全策略为必须策略或者不需要策略；所述必须策略用于指示所述传输单播业务数据的 DRB 的用户面安全激活状态为开启；所述不需要策略指示所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭。

30 在一种示例中，所述处理模块 910，用于根据所述单播安全策略和 PDU 会话的标识，修改所述标识的 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态。

在一种示例中，存储模块 930 可以存储接入设备侧的方法的计算机执行指令，以使处理模块 910 执行上述示例中的方法。

35 基于与上述通信方法的同一技术构思，如图 10 所示，提供了一种通信装置 1000，装置 1000 可以包括：收发模块 1020，处理模块 1010，可选的，还包括存储模块 1030；处理模块 1010 可以分别与存储模块 1030 和收发模块 1020 相连，所述存储模块 1030 也可以与收发模块 1020 相连。

40 在一种示例中，装置 1000 能够执行上述图 2-图 8 的方法中由终端设备执行的各个步骤。装置 1000 可以为终端设备，也可以为应用于终端设备中的芯片。

在一种示例中，所述收发模块 1020，用于接收来自接入设备的第一消息，所述第一消息包括第一指示，所述第一指示用于指示 PDU 会话的传输多播业务数据的数据无线承载 DRB 的用户面安全激活状态，所述用户面安全激活状态包括完整性保护是否激活和/或机密性保护是否激活；所述处理模块 1010，用于根据所述传输多播业务数据的 DRB 的用户面安全激活状态，配置多播的分组数据汇聚协议 PDCP 层实体。

在一种示例中，所述第一消息还包括以下指示中的一种或多种：第二指示、第三指示和第四指示；所述第二指示用于指示所述装置将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态修改为所述传输多播业务数据的 DRB 的用户面安全激活状态，或者，所述第二指示用于指示修改后的所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态；所述第三指示为需要修改用户面安全激活状态的 DRB 的标识；所述第四指示用于指示所述装置对所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

在一种示例中，当所述第一消息中包括第二指示时，所述处理模块 1010，还用于根据所述传输多播业务数据的 DRB 的用户面安全激活状态，或者所述修改后的传输单播业务数据的 DRB 的用户面安全激活状态，对所述传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

在一种示例中，当所述第一消息中包括第三指示时，所述处理模块 1010，还用于修改所述标识的 DRB 的用户面安全激活状态。

在一种示例中，当所述第一消息中包括第四指示时，所述处理模块 1010，还用于对所述传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

在一种示例中，存储模块 1030 可以存储终端设备侧的方法的计算机执行指令，以使处理模块 1010 执行上述示例中的方法。

基于与上述通信方法的同一技术构思，如图 11 所示，提供了一种通信装置 1100，装置 1100 可以包括：收发模块 1120，处理模块 1110，可选的，还包括存储模块 1130；处理模块 1110 可以分别与存储模块 1130 和收发模块 1120 相连，所述存储模块 1130 也可以与收发模块 1120 相连。

在一种示例中，装置 1100 能够执行上述图 2-图 8 的方法中由 SMF 设备执行的各个步骤。装置 1000 可以为 SMF 设备，也可以为应用于 SMF 设备中的芯片。

在一种示例中，所述收发模块 1120，用于通过 AMF 设备向接入设备发送第一消息，所述第一消息包括 PDU 会话的第一多播安全策略，所述第一多播安全策略为必须策略或不需要策略；所述必须策略指示传输多播业务数据的 DRB 的用户面安全激活状态为开启；所述不需要策略指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

在一种示例中，所述处理模块 1110，用于根据第二参数集合确定所述第一多播安全策略；其中，所述第二参数集合包括以下一种或多种参数：第二多播安全策略、所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态。

在一种示例中，所述处理模块 1110，具体用于根据所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定所述第一多播安全策略。

在一种示例中，所述处理模块 1110，具体用于所述传输单播业务数据的 DRB 的用户面安全激活状态为开启时，根据所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全

激活状态，确定所述第一多播安全策略；或者，所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭，且所述第二多播安全策略为偏好策略或不需要策略时，根据所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定所述第一多播安全策略；其中，所述偏好策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启或关闭；所述不需要策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

在一种示例中，所述处理模块 1110，具体用于根据所述第二多播安全策略，确定所述第一多播安全策略。

在一种示例中，所述处理模块 1110，具体用于所述传输单播业务数据的 DRB 的用户面安全激活状态为开启或关闭，且所述第二多播安全策略为必须策略或不需要策略时，根据所述第二多播安全策略，确定所述第一多播安全策略。

在一种示例中，所述第一消息还包括：PDU 会话的标识和/或单播安全策略；

其中，所述单播安全策略为必须策略或者不需要策略；所述必须策略用于指示所述传输单播业务数据的 DRB 的用户面安全激活状态为开启；所述不需要策略指示所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭。

在一种示例中，所述处理模块 1110，具体用于所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭或开启，且所述第二多播安全策略为必须策略时，通过所述收发模块 1120 向接入设备发送第一消息。

在一种示例中，所述处理模块 1110，具体用于当所述多播业务安全模式为在终端和核心网之间进行安全保护的模式时，确定所述第二多播安全策略为不需要。

在一种示例中，所述收发模块 1120，具体用于在拒绝多播业务数据传输的情况下，通过 AMF 设备或 UPF 设备向接入设备发送第一消息，所述第一消息包括第一指示，所述第一指示用于指示所述装置设备拒绝多播业务数据传输。

在一种示例中，所述第一消息还包括：第二指示，所述第二指示用于指示所述装置设备拒绝多播业务数据传输的原因。

在一种示例中，所述处理模块 1110，用于根据 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态和第二多播安全策略，确定拒绝多播业务数据传输。

在一种示例中，所述处理模块 1110，用于所述传输单播业务数据的 DRB 的用户面安全激活状态为开启，且所述第二多播安全策略为不需要策略时，确定拒绝多播业务数据传输，所述不需要策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭；或者，

所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭，且所述第二多播安全策略为必须策略时，确定拒绝多播业务数据传输，所述必须策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为开启。

在一种示例中，存储模块 1130 可以存储 SMF 设备侧的方法的计算机执行指令，以使处理模块 1110 执行上述示例中的方法。

存储模块可以包括一个或者多个存储器，存储器可以是一个或者多个设备、电路中用于存储程序或者数据的器件。存储模块可以是寄存器、缓存或者 RAM 等，存储模块可以

和处理模块集成在一起。存储模块可以是 ROM 或者可存储静态信息和指令的其他类型的静态存储设备, 存储模块可以与处理模块相独立。

所述收发模块可以是输入或者输出接口、管脚或者电路等。

5 另外, 如图 12 所示的本申请提供了另一种通信的装置。应理解, 所述装置能够执行上述图 2-图 8 的方法中由接入设备、SMF 设备, 终端执行的各个步骤。装置 1200 包括: 处理器 1210 和收发器 1220, 可选的, 还包括存储器 1230。该收发器, 可以用于接收程序指令并传输至所述处理器, 或者, 该收发器可以用于该装置与其他通信设备进行通信交互, 比如交互控制信令和/或业务数据等。该收发器可以为代码和/或数据读写收发器, 或者, 10 该收发器可以为通信处理器与收发机之间的信号传输收发器。所述处理器 1210 和所述存储器 1230 之间电耦合。

 示例的, 存储器 1230, 用于存储计算机程序; 所述处理器 1210, 可以用于调用所述存储器中存储的计算机程序或指令, 执行上述的通信的方法, 或者通过所述收发器 1220 执行上述的通信的方法。

15 图 9 中的处理模块 910、图 10 中的处理模块 1010、图 11 中的处理模块 1110 可以通过处理器 1210 来实现。

 图 9 中的收发模块 920、图 10 中的收发模块 1020、图 11 中的收发模块 1120 可以通过收发器 1220 来实现。

20 图 9 中的存储模块 930、图 10 中的存储模块 1030、图 11 中的存储模块 1130 可以通过存储器 1230 来实现。

 上述的处理器可以是中央处理器 (central processing unit, CPU), 网络处理器 (network processor, NP) 或者 CPU 和 NP 的组合。处理器还可以进一步包括硬件芯片或其他通用处理器。上述硬件芯片可以是专用集成电路 (application-specific integrated circuit, ASIC), 可编程逻辑器件 (programmable logic device, PLD) 或其组合。上述 PLD 可以是复杂可编程逻辑器件 (complex programmable logic device, CPLD), 现场可编程逻辑门阵列 (field-programmable gate array, FPGA), 通用阵列逻辑 (generic array logic, GAL) 及其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等或其任意组合。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

 还应理解, 本申请实施例中提及的存储器可以是易失性存储器或非易失性存储器, 或 30 可包括易失性和非易失性存储器两者。其中, 非易失性存储器可以是只读存储器 (Read-Only Memory, ROM)、可编程只读存储器 (Programmable ROM, PROM)、可擦除可编程只读存储器 (Erasable PROM, EPROM)、电可擦除可编程只读存储器 (Electrically EPROM, EEPROM) 或闪存。易失性存储器可以是随机存取存储器 (Random Access Memory, RAM), 其用作外部高速缓存。通过示例性但不是限制性说明, 许多形式的 RAM 可用, 例如静态随机存取存储器 (Static RAM, SRAM)、动态随机存取存储器 (Dynamic RAM, DRAM)、同步动态随机存取存储器 (Synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器 (Double Data Rate SDRAM, DDR SDRAM)、增强型同步动态随机存取存储器 (Enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器 (Synchlink DRAM, SLD RAM) 和直接内存总线随机存取存储器 (Direct Rambus RAM, DR RAM)。应注意, 35 本申请描述的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

40

本申请实施例所述的收发器，可以是接口电路、或者收发器中可以包括单独的发送器，和/或，单独的接收器，也可以是发送器和接收器集成一体。接口电路、或者收发器可以在相应的处理器的指示下工作。可选的，发送器可以对应物理设备中发射机，接收器可以对应物理设备中的接收机。

5 本申请实施例还提供了一种计算机存储介质，存储有计算机程序，该计算机程序被计算机执行时，可以使得所述计算机用于执行上述图 2-图 8 的通信的方法。

本申请实施例还提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述图 2-图 8 的通信的方法。

10 本申请中的“和/或”，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。字符“/”一般表示前后关联对象是一种“或”的关系。本申请中所涉及的多个，是指两个或两个以上。另外，需要理解的是，在本申请的描述中，“第一”、“第二”等词汇，仅用于区分描述的目的，而不能理解为指示或暗示相对重要性，也不能理解为指示或暗示顺序。

15 本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包括有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

20 本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

25 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

30 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

35 尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

40 显然，本领域的技术人员可以对本申请实施例进行各种改动和变型而不脱离本申请实施例的精神和范围。这样，倘若本申请实施例的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包括这些改动和变型在内。

权 利 要 求

1、一种通信的方法，其特征在于，所述方法包括：

5 接入设备向终端发送第一消息，所述第一消息包括第一指示，所述第一指示用于指示 PDU 会话的传输多播业务数据的数据无线承载 DRB 的用户面安全激活状态，所述用户面安全激活状态包括完整性保护是否激活和/或机密性保护是否激活；并且，

所述接入设备根据所述传输多播业务数据的 DRB 的用户面安全激活状态，配置多播的分组数据汇聚协议 PDCP 层实体。

2、如权利要求 1 所述的方法，其特征在于，所述接入设备向终端发送第一消息之前，所述方法还包括：

10 所述接入设备根据第一参数集合确定所述传输多播业务数据的 DRB 的用户面安全激活状态，其中，所述第一参数集合包括以下一种或多种参数：

所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态、多播安全策略。

3、如权利要求 2 所述的方法，其特征在于，所述接入设备根据第一参数集合确定所述传输多播业务数据的 DRB 的用户面安全激活状态，包括：

15 所述接入设备将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定为所述传输多播业务数据的 DRB 的用户面安全激活状态。

4、如权利要求 3 所述的方法，其特征在于，所述接入设备将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定为所述传输多播业务数据的 DRB 的用户面安全激活状态，包括：

20 所述传输单播业务数据的 DRB 的用户面安全激活状态为开启时，所述接入设备将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定为所述传输多播业务数据的 DRB 的用户面安全激活状态；或者，

25 所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭，且所述多播安全策略为偏好策略或不需要策略时，所述接入设备将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定为所述传输多播业务数据的 DRB 的用户面安全激活状态；其中，所述偏好策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启或关闭；所述不需要策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

30 5、如权利要求 2 所述的方法，其特征在于，所述接入设备根据第一参数集合确定所述传输多播业务数据的 DRB 的用户面安全激活状态，包括：

35 接入设备根据所述多播安全策略，确定所述传输多播业务数据的 DRB 的用户面安全激活状态；所述多播安全策略为必须策略或者偏好策略或者不需要策略；所述必须策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启；所述偏好策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启或关闭；所述不需要策略指示所述传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

6、如权利要求 5 所述的方法，其特征在于，所述接入设备根据所述多播安全策略，确定所述 PDU 会话的传输多播业务数据的 DRB 的用户面安全激活状态，包括：

所述传输单播业务数据的 DRB 的用户面安全激活状态为开启或关闭，且所述多播安全策略为必须策略或不需要策略时，所述接入设备根据所述多播安全策略，确定所述 PDU

会话的传输多播业务数据的 DRB 的用户面安全激活状态。

7、如权利要求 5 所述的方法，其特征在于，所述第一消息还包括以下指示中的一种或多种：第二指示、第三指示和第四指示；

5 所述第二指示用于指示所述终端将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态修改为所述传输多播业务数据的 DRB 的用户面安全激活状态，或者，所述第二指示用于指示修改后的所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态；

所述第三指示为需要修改用户面安全激活状态的 DRB 的标识；

10 所述第四指示用于指示所述终端对所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

8、如权利要求 7 所述的方法，其特征在于，所述接入设备向终端发送第一消息，包括：

所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭或开启，且所述多播安全策略为必须策略时，所述接入设备向终端发送第一消息。

15 9、一种通信的方法，其特征在于，所述方法包括：

终端接收来自接入设备的第一消息，所述第一消息包括第一指示，所述第一指示用于指示 PDU 会话的传输多播业务数据的数据无线承载 DRB 的用户面安全激活状态，所述用户面安全激活状态包括完整性保护是否激活和/或机密性保护是否激活；

20 所述终端根据所述传输多播业务数据的 DRB 的用户面安全激活状态，配置多播的分组数据汇聚协议 PDCP 层实体。

10、如权利要求 9 所述的方法，其特征在于，所述第一消息还包括以下指示中的一种或多种：第二指示、第三指示和第四指示；

25 所述第二指示用于指示所述终端将所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态修改为所述传输多播业务数据的 DRB 的用户面安全激活状态，或者，所述第二指示用于指示修改后的所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态；

所述第三指示为需要修改用户面安全激活状态的 DRB 的标识；

所述第四指示用于指示所述终端对所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

30 11、如权利要求 10 所述的方法，其特征在于，还包括：

当所述第一消息中包括第二指示时，所述终端根据所述传输多播业务数据的 DRB 的用户面安全激活状态，或者所述修改后的传输单播业务数据的 DRB 的用户面安全激活状态，对所述传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

12、如权利要求 10 所述的方法，其特征在于，还包括：

35 当所述第一消息中包括第三指示时，所述终端修改所述标识的 DRB 的用户面安全激活状态。

13、如权利要求 10 所述的方法，其特征在于，还包括：

当所述第一消息中包括第四指示时，所述终端对所述传输单播业务数据的 DRB 的用户面安全激活状态进行修改。

40 14、一种通信的方法，其特征在于，所述方法包括：

在拒绝多播业务数据传输的情况下，接入设备向 SMF 设备发送第一消息，所述第一消息包括第一指示，所述第一指示用于指示所述接入设备拒绝多播业务数据传输。

15、如权利要求 14 所述的方法，其特征在于，所述第一消息还包括：第二指示，所述第二指示用于指示所述接入设备拒绝多播业务数据传输的原因。

5 16、如权利要求 15 所述的方法，其特征在于，所述拒绝多播业务数据传输的原因包括：所述 PDU 会话的多播业务数据传输安全需求与单播业务数据传输安全需求不一致，或者，无法满足多播业务传输安全要求。

17、如权利要求 14-16 任一项所述的方法，其特征在于，还包括：

10 所述接入设备根据多播安全策略和 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定拒绝多播业务数据传输。

18、如权利要求 17 所述的方法，其特征在于，所述接入设备根据多播安全策略和 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定拒绝多播业务数据传输，包括：

15 所述传输单播业务数据的 DRB 的用户面安全激活状态为开启，且所述多播安全策略为不需要策略时，所述接入设备确定拒绝多播业务数据传输，所述不需要策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭；或者，

所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭，且所述多播安全策略为必须策略时，所述接入设备确定拒绝多播业务数据传输，所述必须策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为开启。

20 19、一种通信的方法，其特征在于，所述方法包括：

SMF 设备通过 AMF 设备向接入设备发送第一消息，所述第一消息包括 PDU 会话的第一多播安全策略，所述第一多播安全策略为必须策略或不需要策略；所述必须策略指示传输多播业务数据的 DRB 的用户面安全激活状态为开启；所述不需要策略指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

25 20、如权利要求 19 所述的方法，其特征在于，所述 SMF 设备通过 AMF 设备向接入设备发送第一消息之前，还包括：

所述 SMF 设备根据第二参数集合确定所述第一多播安全策略；其中，所述第二参数集合包括以下一种或多种参数：

30 第二多播安全策略、所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态。

21、如权利要求 20 所述的方法，其特征在于，所述 SMF 设备根据第二参数集合确定所述第一多播安全策略，包括：

所述 SMF 设备根据所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定所述第一多播安全策略。

35 22、如权利要求 21 所述的方法，其特征在于，所述 SMF 设备根据所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定所述第一多播安全策略，包括：

所述传输单播业务数据的 DRB 的用户面安全激活状态为开启时，所述 SMF 设备根据所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态，确定所述第一多播安全策略；或者，

40 所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭，且所述第二多播安全

策略为偏好策略或不需要策略时, SMF 设备根据所述 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态, 确定所述第一多播安全策略; 其中, 所述偏好策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为开启或关闭; 所述不需要策略用于指示所述传输多播业务数据的 DRB 的用户面安全激活状态为关闭。

- 5 23、如权利要求 21 所述的方法, 其特征在于, 所述 SMF 设备根据第二参数集合确定所述第一多播安全策略, 包括:

所述 SMF 设备根据所述第二多播安全策略, 确定所述第一多播安全策略。

24、如权利要求 23 所述的方法, 其特征在于, 所述 SMF 设备根据所述第二多播安全策略, 确定所述第一多播安全策略, 包括:

- 10 所述传输单播业务数据的 DRB 的用户面安全激活状态为开启或关闭, 且所述第二多播安全策略为必须策略或不需要策略时, 所述 SMF 设备根据所述第二多播安全策略, 确定所述第一多播安全策略。

25、如权利要求 19 所述的方法, 其特征在于, 所述第一消息还包括: PDU 会话的标识和/或单播安全策略;

- 15 其中, 所述单播安全策略为必须策略或者不需要策略; 所述必须策略用于指示所述传输单播业务数据的 DRB 的用户面安全激活状态为开启; 所述不需要策略指示所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭。

26、如权利要求 25 所述的方法, 其特征在于, 所述 SMF 设备通过 AMF 设备向接入设备发送第一消息, 包括:

- 20 所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭或开启, 且所述第二多播安全策略为必须策略时, 所述 SMF 设备通过 AMF 设备向接入设备发送第一消息。

27、如权利要求 20 所述的方法, 其特征在于, 还包括:

当所述多播业务安全模式为在终端和核心网或者终端和应用服务器之间进行安全保护的的模式时, 所述 SMF 设备确定所述第二多播安全策略为不需要。

- 25 28、一种通信的方法, 其特征在于, 所述方法包括:

接入设备通过 AMF 设备接收来自 SMF 设备发送的第一消息, 所述第一消息包括 PDU 会话的第一多播安全策略, 所述第一多播安全策略为必须策略或不需要策略; 所述必须策略指示传输多播业务数据的 DRB 的用户面安全激活状态为开启; 所述不需要策略指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭;

- 30 所述接入设备根据所述第一多播安全策略, 确定传输多播业务数据的 DRB 的用户面安全激活状态, 并配置多播的分组数据汇聚协议 PDCP 层实体。

29、如权利要求 28 所述的方法, 其特征在于, 所述第一消息还包括: PDU 会话的标识和/或单播安全策略;

- 35 其中, 所述单播安全策略为必须策略或者不需要策略; 所述必须策略用于指示所述传输单播业务数据的 DRB 的用户面安全激活状态为开启; 所述不需要策略指示所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭。

30、如权利要求 29 所述的方法, 其特征在于, 还包括:

所述接入设备根据所述单播安全策略和 PDU 会话的标识, 修改所述标识的 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态。

- 40 31、一种通信的方法, 其特征在于, 所述方法包括:

在拒绝多播业务数据传输的情况下，所述 SMF 设备通过 AMF 设备或 UPF 设备向接入设备发送第一消息，所述第一消息包括第一指示，所述第一指示用于指示所述 SMF 设备拒绝多播业务数据传输。

5 32、如权利要求 31 所述的方法，其特征在于，所述第一消息还包括：第二指示，所述第二指示用于指示所述 SMF 设备拒绝多播业务数据传输的原因。

33、如权利要求 32 所述的方法，其特征在于，所述拒绝多播业务数据传输的原因包括：所述 PDU 会话的多播业务数据传输安全需求与单播业务数据传输安全需求不一致或者无法满足多播业务传输安全要求。

10 34、如权利要求 31-33 任一项所述的方法，其特征在于，还包括：
SMF 设备根据 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态和第二多播安全策略，确定拒绝多播业务数据传输。

35、如权利要求 34 所述的方法，其特征在于，SMF 设备根据 PDU 会话的传输单播业务数据的 DRB 的用户面安全激活状态和所述第二多播安全策略，确定拒绝多播业务数据传输，包括：

15 所述传输单播业务数据的 DRB 的用户面安全激活状态为开启，且所述第二多播安全策略为不需要策略时，所述 SMF 设备确定拒绝多播业务数据传输，所述不需要策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为关闭；或者，

20 所述传输单播业务数据的 DRB 的用户面安全激活状态为关闭，且所述第二多播安全策略为必须策略时，所述 SMF 设备确定拒绝多播业务数据传输，所述必须策略用于指示传输多播业务数据的 DRB 的用户面安全激活状态为开启。

36、一种通信的装置，其特征在于，包括用于执行权利要求 1-8 任一项方法的模块，或者执行权利要求 9-13 任一项方法的模块，或者执行权利要求 14-18 任一项方法的模块，或者执行权利要求 19-27 任一项方法的模块，执行权利要求 28-30 任一项方法的模块，或者执行权利要求 31-35 任一项方法的模块。

25 37、一种通信的装置，其特征在于，包括处理器和存储器；

所述存储器，用于存储计算机程序指令；

30 所述处理器，用于执行所述存储器中的部分或者全部计算机程序指令，当所述部分或者全部计算机程序指令被执行时，用于实现如权利要求 1-8 任一项所述的方法的步骤，或实现如权利要求 9-13 任一项所述的方法的步骤，或者如权利要求 14-18 任一项所述的方法的步骤，或者如权利要求 19-27 任一项所述的方法的步骤，或者如权利要求 28-30 任一项所述的方法的步骤，或者如权利要求 31-35 任一项所述的方法的步骤。

35 38、一种计算机程序，其特征在于，所述计算机程序包括用于执行权利要求 1-8 任一项方法的指令，或者包括用于执行权利要求 9-13 任一项方法的指令，或者包括用于执行权利要求 14-18 任一项方法的指令，或者包括用于执行权利要求 19-27 任一项方法的指令，或者包括用于执行权利要求 28-30 任一项方法的指令，或者包括用于执行权利要求 31-35 任一项方法的指令。

40 39、一种计算机可读存储介质，其特征在于，用于存储计算机程序，所述计算机程序包括用于实现权利要求 1-8 任一项所述的方法的指令，或者实现权利要求 9-13 中任一项所述的方法的指令，或者实现权利要求 14-18 中任一项所述的方法的指令，或者实现权利要求 19-27 中任一项所述的方法的指令，或者实现权利要求 28-30 中任一项所述的方法的指

令，或者实现权利要求 31-35 中任一项所述的方法的指令。