

通信方法、装置及系统

5 技术领域

本申请涉及通信技术领域，尤其涉及通信方法、装置及系统。

背景技术

传统的移动网络中，用户设备（user equipment，UE）之间的信令通信和数据通信路径需要经过网络侧设备（如基站/服务网关（serving gateway，SGW）/分组数据网关（packet data network gateway，PGW））。不同的 UE 之间是不能直接进行通信的。即使两个距离很近的 UE 之间，以 UE1 和 UE2 为例，在进行数据传递时，也需要 UE1 先将数据发送给连接的基站 1，进而数据经过网络侧的传输到达 UE2 连接的基站 2（此时基站 1 和基站 2 可以为相同基站，也可为不同基站），最后由基站 2 将数据发送给 UE2，这样会对网络传输带宽有较大的需求量，并且传输效率较低。

在设备到设备通信（device-to-device，D2D）需要短距离直连通信的需求下，邻近业务（Proximity-based services，ProSe）课题被提出。ProSe 要求 UE 之间直接进行数据交换，或者仅通过基站而不经核心网设备（如 SGW/PGW）进行数据交换，因此可以提高距离较近的 UE 之间的通信效率。在第五代（5th generation，5G）通信技术中，短距离直连通信业务被用于车联网（vehicle-to-everything，V2X）中。

目前，ProSe 技术建立两个 UE 之间的数据交换前，需要按顺序执行 ProSe 发现流程和 PC5 建立流程。其中，ProSe 发现流程用于实现两个 UE 之间的彼此发现，PC5 建立流程用于建立两个 UE 之间通过 PC5 接口直连通信的信令连接与数据连接。然而，现有的 V2X PC5 建立流程（具体可参考第三代合作伙伴计划（3rd generation partnership project，3GPP）技术标准（technical standards，TS）23.303）中的安全保护机制并不完善，V2X PC5 建立流程中的控制面信令容易被中间攻击者攻击，从而可能造成安全等级降级。因此，如何提升 V2X PC5 建立流程的安全性，是目前亟待解决的问题。

发明内容

本申请实施例提供通信方法、装置及系统，用于提升 V2X PC5 建立流程的安全性。

为达到上述目的，本申请的实施例采用如下技术方案：

第一方面，提供了一种通信方法，该方法包括：第一终端设备获取第一安全保护方法，该第一安全保护方法为第一终端设备与第二终端设备之间的发现流程中确定的安全保护方法；第一终端设备根据第一安全保护方法确定第二安全保护方法，该第二安全保护方法为该第一终端设备与该第二终端设备之间的 PC5 连接的安全保护方法。由于本申请实施例在确定第二安全保护方法时，可以参考发现流程中确定的第一安全保护方法，因此可以使得确定的第二安全保护方法的安全等级不低于第一安全保护方法的安全等级。也就是说，第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级，这样可以达到安全不降级的目的。

在一种可能的实现方式中，该通信方法还包括：第一终端设备接收来自第二终端设备的第一消息，该第一消息为第一终端设备与第二终端设备之间的 PC5 建立流程中

的第一条消息；第一终端设备根据第一安全保护方法对第一消息进行解安全保护。也就是说，本申请实施例中，第一消息是采用第一安全保护方法进行安全保护的。这样，在第一安全保护方法包括完整性保护开启的情况下，由于第一终端设备可以使用第一安全保护方法对第一消息进行安全保护，因此可以避免 PC5 建立流程中的第一消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

第二方面，提供了一种通信方法，该方法包括：第一终端设备获取第一安全保护方法，该第一安全保护方法为第一终端设备与第二终端设备之间的发现流程中确定的安全保护方法；第一终端设备使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护后，向第二终端设备发送安全保护后的至少一条消息。基于本申请实施例提供的通信方法，一方面，在第一安全保护方法包括完整性保护开启的情况下，由于第一终端设备可以使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护，因此可以避免 PC5 建立流程中的消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。另一方面，在第一安全保护方法的安全等级高于或者等于第一终端设备与第二终端设备之间的 PC5 连接的控制面使用的安全保护方法的安全等级的情况下，由于第一终端设备可以使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护，因此可以避免 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的安全等级所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

在一种可能的实现方式中，至少一条消息包括第一消息，该第一消息为该 PC5 建立流程中的第一条消息。也就是说，本申请实施例中，第一消息是采用第一安全保护方法进行安全保护的。这样，在第一安全保护方法包括完整性保护开启的情况下，由于第一终端设备可以使用第一安全保护方法对第一消息进行安全保护，因此可以避免 PC5 建立流程中的第一消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

在一种可能的实现方式中，至少一条消息还包括第三消息，第三消息为该 PC5 建立流程中第一终端设备发送的用于协商第一终端设备和第二终端设备之间的 PC5 连接的用户面使用的安全保护方法的消息；第一终端设备使用第一安全保护方法对该 PC5 建立流程中的至少一条消息进行安全保护，包括：第一终端设备使用第一安全保护方法对该第一消息进行安全保护；在 PC5 连接的控制面使用的安全保护方法的安全等级低于该第一安全保护方法的安全等级的情况下，第一终端设备使用该第一安全保护方法对第三消息进行安全保护。一方面，在第一安全保护方法包括完整性保护开启的情况下，由于第一终端设备可以使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的第一消息进行安全保护，因此可以避免 PC5 建立流程中的第一消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。另一方面，在 PC5 连接的控制面使用的安全保护方法的安全等级低于该第一安全保护方法的安全等级的情况下，由于第一终端设备可以使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的第三消息进行安全保护，因此可以避免 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的

安全等级所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

在一种可能的实现方式中，该通信方法还可以包括：第一终端设备接收来自第二终端设备的第二消息，该第二消息包括该第二终端设备选择的该 PC5 连接的控制面的安全算法；第一终端设备根据该 PC5 连接的控制面的安全算法，确定该 PC5 连接的控制面使用的安全保护方法的安全等级低于该第一安全保护方法的安全等级。基于该方案，第一终端设备可以获知 PC5 连接的控制面使用的安全保护方法的安全等级低于该第一安全保护方法的安全等级。

在一种可能的实现方式中，至少一条消息包括第四消息，第四消息为该 PC5 建立流程中第一终端设备发送的用于协商第一终端设备和第二终端设备之间的 PC5 连接的用户面使用的安全保护方法的消息；第一终端设备使用第一安全保护方法对该 PC5 建立流程中的至少一条消息进行安全保护，包括：第一终端设备确定该 PC5 连接的控制面使用的安全保护方法的安全等级低于该第一安全保护方法的安全等级；第一终端设备使用该第一安全保护方法对该第四消息进行安全保护。该方案中，在 PC5 连接的控制面使用的安全保护方法的安全等级低于该第一安全保护方法的安全等级的情况下，由于第一终端设备可以使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的第四消息进行安全保护，因此可以避免 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的安全等级所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

在一种可能的实现方式中，本申请实施例提供的通信方法还包括：第一终端设备根据第一安全保护方法确定第二安全保护方法，该第二安全保护方法为该第一终端设备与该第二终端设备之间的 PC5 连接的安全保护方法。由于本申请实施例在确定第二安全保护方法时，可以参考发现流程中确定的第一安全保护方法，因此可以使得确定的第二安全保护方法的安全等级不低于第一安全保护方法的安全等级。也就是说，第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级，这样可以达到安全不降级的目的。

结合上述第一方面或第二方面，在一种可能的实现方式中，第一终端设备根据第一安全保护方法确定第二安全保护方法，包括：第一终端设备将第一安全保护方法确定为第二安全保护方法。也就是说，本申请实施例中，第一终端设备可以根据第一安全保护方法直接激活第一终端设备与第二终端设备之间的 PC5 连接的安全。该方案中，由于第一终端设备不需要与第二终端设备协商第二安全保护方法，而是直接将第一安全保护方法确定为第二安全保护方法，因此不仅简化了第一终端设备的处理逻辑，而且可以节省 PC5 建立流程的信令开销。

结合上述第一方面或第二方面，在一种可能的实现方式中，第一终端设备根据第一安全保护方法确定第二安全保护方法，包括：第一终端设备接收来自第二终端设备的第二安全策略，该第二安全策略为第二终端设备在该 PC5 连接中的安全策略；第一终端设备根据第二安全策略和第一安全保护方法，确定第二安全保护方法。该方案中，由于第一终端设备在确定第二安全保护方法时，还参考第二终端设备的第二安全策略，因此可以最大程度的使得第一终端设备确定出的第二安全保护方法也能被第二终端设备使用。

结合上述第一方面或第二方面，在一种可能的实现方式中，第一终端设备根据第二安全策略和第一安全保护方法，确定第二安全保护方法，包括：在第一安全保护方法满足第二安全策略的情况下，将第一安全保护方法确定为第二安全保护方法。由于该方案在第一安全保护方法满足第二安全策略时，将第一安全保护方法确定为第二安全保护方法，因此不仅可以使得第一终端设备确定出的第二安全保护方法也能被第二终端设备使用，而且保证了第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级，这样可以达到安全不降级的目的。

结合上述第一方面或第二方面，在一种可能的实现方式中，第一终端设备根据第二安全策略和第一安全保护方法，确定第二安全保护方法，包括：在第一安全保护方法满足第二安全策略的情况下，根据第二安全策略，选择安全等级不低于第一安全保护方法的安全保护方法作为该第一安全保护方法。由于该方案在第一安全保护方法满足第二安全策略时，根据第二安全策略，选择安全等级不低于第一安全保护方法的安全保护方法作为该第一安全保护方法，因此不仅可以使得第一终端设备确定出的第二安全保护方法也能被第二终端设备使用，而且保证了第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级，这样可以达到安全不降级的目的。

结合上述第一方面或第二方面，在一种可能的实现方式中，第一终端设备根据第二安全策略和第一安全保护方法，确定第二安全保护方法，包括：在第一安全保护方法不满足第二安全策略的情况下，根据第二安全策略，选择一个满足第二安全策略的安全保护方法作为第二安全保护方法。由于该方案在第一安全保护方法不满足第二安全策略时，根据第二安全策略，选择一个满足第二安全策略的安全保护方法作为第二安全保护方法，因此不仅可以使得第一终端设备确定出的第二安全保护方法也能被第二终端设备使用，而且保证了第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级，这样可以达到安全不降级的目的。

结合上述第一方面或第二方面，在一种可能的实现方式中，第二安全策略包括第二控制面安全策略和/或第二用户面安全策略；其中，第二控制面安全策略为第二终端设备在 PC5 连接中的控制面安全策略，第二用户面安全策略为第二终端设备在 PC5 连接中的用户面安全策略。本申请实施例中，第二控制面安全策略可以用于确定 PC5 连接的控制面使用的安全保护方法，第二用户面安全策略可以用于确定 PC5 连接的用户面使用的安全保护方法。

结合上述第一方面或第二方面，在一种可能的实现方式中，第二安全保护方法用于对该 PC5 连接的控制面信令中传递的部分或全部参数进行安全保护；和/或，第二安全保护方法用于对该 PC5 连接的部分或全部用户面数据进行安全保护。换言之，本申请实施例中的第二安全保护方法包括 PC5 连接的控制面使用的安全保护方法，和/或，PC5 连接的用户面使用的安全保护方法。其中，PC5 连接的控制面使用的安全保护方法用于对该 PC5 连接的控制面信令中传递的部分或全部参数进行安全保护，PC5 连接的用户面使用的安全保护方法用于对该 PC5 连接的部分或全部用户面数据进行安全保护。

结合上述第一方面或第二方面，在一种可能的实现方式中，第一终端设备获取第一安全保护方法，包括：第一终端设备向第一直连通信发现名称管理功能网元发送第

一信息和该第一终端设备的 3GPP 身份信息, 第一信息包括用于 ProSe 业务的身份信息或者用于确定用于 ProSe 业务的身份信息的信息; 第一终端设备接收来自第一直连通信发现名称管理功能网元的第一安全保护方法。基于该方案, 第一终端设备可以在第一终端设备与第二终端设备之间的发现流程中获取第一安全保护方法。

- 5 第三方面, 提供了一种通信方法, 该方法包括: 第一直连通信发现名称管理功能网元接收来自第一终端设备的第一信息和该第一终端设备的 3GPP 身份信息, 其中, 第一信息包括用于 ProSe 业务的身份信息或者用于确定用于 ProSe 业务的身份信息的信息; 第一直连通信发现名称管理功能网元根据第一信息和第一终端设备的 3GPP 身份信息, 确定第一终端设备使用该 ProSe 业务时所需的安全保护方法; 第一直连通信发现名称管理功能网元向第一终端设备发送第一终端设备使用该 ProSe 业务时所需的安全保护方法。基于本申请实施例提供的通信方法, 第一终端设备可以在第一终端设备与第二终端设备之间的发现流程中获取第一终端设备使用 ProSe 业务时所需的安全保护方法。

- 15 在一种可能的实现方式中, 第一直连通信发现名称管理功能网元根据第一信息和第一终端设备的 3GPP 身份信息, 确定第一终端设备使用该 ProSe 业务时所需的安全保护方法, 包括: 第一直连通信发现名称管理功能网元根据第一信息和第一终端设备的 3GPP 身份信息, 确定第一终端设备使用该 ProSe 业务时对应的多个可供选择的安全保护方法; 第一直连通信发现名称管理功能网元根据该多个可供选择的安全保护方法确定第一终端设备使用该 ProSe 业务时所需的安全保护方法。也就是说, 本申请实施例中, 第一终端设备使用该 ProSe 业务时所需的安全保护方法是从第一终端设备使用该 ProSe 业务时对应的多个可供选择的安全保护方法中确定的。

- 25 在一种可能的实现方式中, 本申请实施例提供的通信方法还包括: 第一直连通信发现名称管理功能网元从第二直连通信发现名称管理功能网元获取第二终端设备使用该 ProSe 业务时所需的安全保护方法; 第一直连通信发现名称管理功能网元根据该多个可供选择的安全保护方法确定第一终端设备使用该 ProSe 业务时所需的安全保护方法, 包括: 第一直连通信发现名称管理功能网元确定该多个可供选择的安全保护方法中是否包括第二终端设备使用该 ProSe 业务时所需安全保护方法; 当该多个可供选择的安全保护方法中包括第二终端设备使用该 ProSe 业务时所需的安全保护方法时, 第一直连通信发现名称管理功能网元将第二终端设备使用该 ProSe 业务时所需的安全保护方法确定为第一终端设备使用该 ProSe 业务时所需的安全保护方法。基于该方案, 可以使得第一终端设备和第二终端设备在第一终端设备与第二终端设备之间的发现流程获取相同的安全保护方法。

- 35 在一种可能的实现方式中, 本申请实施例提供的通信方法还包括: 第一直连通信发现名称管理功能网元从第二直连通信发现名称管理功能网元获取第二终端设备使用该 ProSe 业务时所需的安全保护方法; 第一直连通信发现名称管理功能网元根据该多个可供选择的安全保护方法确定第一终端设备使用该 ProSe 业务时所需的安全保护方法, 包括: 第一直连通信发现名称管理功能网元确定该多个可供选择的安全保护方法中是否包括第二终端设备使用该 ProSe 业务时所需安全保护方法; 当该多个可供选择的安全保护方法中不包括第二终端设备使用该 ProSe 业务时所需的安全保护方法时,

第一直连通信发现名称管理功能网元从该多个可供选择的安全保护方法中确定该第一终端设备使用该 ProSe 业务时所需的安全保护方法。基于该方案，第一终端设备可以在第一终端设备与第二终端设备之间的发现流程中获取第一终端设备使用 ProSe 业务时所需的安全保护方法。

5 在一种可能的实现方式中，该使用该 ProSe 业务时所需的安全保护方法用于对第五消息进行安全保护，该第五消息为该第一终端设备与第二终端设备之间的发现流程中的第一条 PC5 广播消息。基于该方案，可以实现第五消息的安全保护，从而可以避免第五消息被攻击者攻击或篡改。

10 在一种可能的实现方式中，该使用该 ProSe 业务时所需的安全保护方法用于确定第一终端设备与第二终端设备之间的 PC5 连接的安全保护方法。由于本申请实施例在确定第一终端设备与第二终端设备之间的 PC5 连接的安全保护方法时，可以参考发现流程中确定的安全保护方法，因此可以使得确定的第一终端设备与第二终端设备之间的 PC5 连接的安全保护方法的安全等级不低于发现流程中确定的安全保护方法的安全等级。也就是说，发现流程中确定的安全保护方法的安全等级是 PC5 建立流程中 PC5
15 连接的最低安全等级，这样可以达到安全不降级的目的。

 在一种可能的实现方式中，PC5 连接的安全保护方法用于对该 PC5 连接的控制面信令中传递的部分或全部参数进行安全保护；和/或，该 PC5 连接的安全保护方法用于对该 PC5 连接的部分或全部用户面数据进行安全保护。换言之，本申请实施例中，PC5
20 连接的安全保护方法包括 PC5 连接的控制面使用的安全保护方法，和/或，PC5 连接的用户面使用的安全保护方法。其中，PC5 连接的控制面使用的安全保护方法用于对该 PC5 连接的控制面信令中传递的部分或全部参数进行安全保护，PC5 连接的用户面使用的安全保护方法用于对该 PC5 连接的部分或全部用户面数据进行安全保护。

 在一种可能的实现方式中，该使用该 ProSe 业务时所需的安全保护方法用于对该第一终端设备与该第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护。
25 一方面，在使用该 ProSe 业务时所需的安全保护方法包括完整性保护开启的情况下，由于使用该 ProSe 业务时所需的安全保护方法用于对该第一终端设备与该第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护，因此可以避免 PC5 建立流程中的消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。另一方面，在使用该 ProSe 业务时所需的安全保护方法的安全等级高于或者等于第一终端设备与第二终端设备之间的 PC5 连接的控制面使用的安全保护方法的安全等级的情况下，由于使用该 ProSe 业务时所需的安全保护方法用于对该第一终端设备与该第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护，因此可以避免 PC5 连接的控制面使用的安全保护方法的安全等级低于发现流程中确定的使用该 ProSe 业务时所需的安全保护方法的安全等级所造成的安全等级降低的问题，提高
30 了 PC5 建立流程的安全等级。
35 在一种可能的实现方式中，该至少一条消息包括第一消息，第一消息为该 PC5 建立流程中的第一条消息。也就是说，本申请实施例中，第一消息是采用第一安全保护方法进行安全保护的。这样，在第一安全保护方法包括完整性保护开启的情况下，由于第一终端设备可以使用第一安全保护方法对第一消息进行安全保护，因此可以避免

PC5 建立流程中的第一消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

第四方面，提供了一种通信装置用于实现上述方法。该通信装置可以为上述第一方面或第二方面中的第一终端设备，或者包含上述第一终端设备的装置；或者，该通信装置可以为上述第三方面中的第一直连通信发现名称管理功能网元，或者包含上述第一直连通信发现名称管理功能网元的装置。该通信装置包括实现上述方法相应的模块、单元、或手段 (means)，该模块、单元、或 means 可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

第五方面，提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机指令，当该处理器执行该指令时，以使该通信装置执行上述任一方面所述的方法。该通信装置可以为上述第一方面或第二方面中的第一终端设备，或者包含上述第一终端设备的装置；或者，该通信装置可以为上述第三方面中的第一直连通信发现名称管理功能网元，或者包含上述第一直连通信发现名称管理功能网元的装置。

第六方面，提供了一种通信装置，包括：处理器；该处理器用于与存储器耦合，并读取存储器中的指令之后，根据该指令执行如上述任一方面所述的方法。该通信装置可以为上述第一方面或第二方面中的第一终端设备，或者包含上述第一终端设备的装置；或者，该通信装置可以为上述第三方面中的第一直连通信发现名称管理功能网元，或者包含上述第一直连通信发现名称管理功能网元的装置。

第七方面，提供了一种通信装置，包括：处理器和接口电路；接口电路，用于接收计算机程序或指令并传输至处理器；处理器用于执行所述计算机程序或指令，以使该通信装置执行如上述任一方面所述的方法。该通信装置可以为上述第一方面或第二方面中的第一终端设备，或者包含上述第一终端设备的装置；或者，该通信装置可以为上述第三方面中的第一直连通信发现名称管理功能网元，或者包含上述第一直连通信发现名称管理功能网元的装置。

第八方面，提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机可以执行上述任一方面所述的方法。

第九方面，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任一方面所述的方法。

第十方面，提供了一种通信装置（例如，该通信装置可以是芯片或芯片系统），该通信装置包括处理器，用于实现上述任一方面中所涉及的功能。在一种可能的实现方式中，该通信装置还包括存储器，该存储器，用于保存必要的程序指令和数据。该通信装置是芯片系统时，可以由芯片构成，也可以包含芯片和其他分立器件。

其中，第四方面至第十方面中任一种可能的实现方式所带来的技术效果可参见上述第一方面或第二方面或第三方面中不同设计方式所带来的技术效果，此处不再赘述。

第十一方面，提供了一种通信系统，该通信系统包括第一终端设备和第二终端设备。其中，第一终端设备，用于获取第一安全保护方法，该第一安全保护方法为第一终端设备与第二终端设备之间的发现流程中确定的安全保护方法；第一终端设备，还用于使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的

至少一条消息进行安全保护后，向第二终端设备发送安全保护后的至少一条消息；第二终端设备，用于接收安全保护后的至少一条消息，并使用第一安全保护方法对至少一条消息进行解安全保护。其中，第十一方面的技术效果可参考上述第二方面，在此不再赘述。

- 5 在一种可能的实现方式中，第一终端设备或第二终端设备，还用于根据第一安全保护方法确定第二安全保护方法，第二安全保护方法为第一终端设备与第二终端设备之间的 PC5 连接的安全保护方法。该方案的技术效果可参考上述第一方面，在此不再赘述。

- 10 在一种可能的实现方式中，该通信系统还包括第一直连通信发现名称管理功能网元和第二直连通信发现名称管理功能网元。其中，第一终端设备，用于获取第一安全保护方法，包括：第一终端设备，用于接收来自第一直连通信发现名称管理功能网元的第一终端设备使用 ProSe 业务时所需的安全保护方法。类似的，第二终端设备，还用于接收来自第二直连通信发现名称管理功能网元的第二终端设备使用 ProSe 业务时所需的安全保护方法。其中，第一终端设备使用 ProSe 业务时所需的安全保护方法与
15 第二终端设备使用 ProSe 业务时所需的安全保护方法均为上述第一安全保护方法。基于该方案，第一终端设备或第二终端设备可以在第一终端设备与第二终端设备之间的发现流程中获取使用 ProSe 业务时所需的安全保护方法。

- 第十二方面，提供了一种通信系统，该通信系统包括第一直连通信发现名称管理功能网元和第二直连通信发现名称管理功能网元；其中，第一直连通信发现名称管理功能网元，用于从第二直连通信发现名称管理功能网元获取第二终端设备使用 ProSe
20 业务时所需的安全保护方法；以及，第一直连通信发现名称管理功能网元，还用于确定第一终端设备使用该 ProSe 业务时对应的多个可供选择的安全保护方法，并根据多个可供选择的安全保护方法以及第二终端设备使用 ProSe 业务时所需的安全保护方法确定第一终端设备使用 ProSe 业务时所需的安全保护方法之后，向第一终端设备发送
25 第一终端设备使用 ProSe 业务时所需的安全保护方法。其中，第十二方面的技术效果可参考上述第三方面，在此不再赘述。

附图说明

- 图 1a 为本申请实施例提供的一种通信系统的结构示意图；
 图 1b 为本申请实施例提供的一种通信系统的结构示意图；
30 图 2 为本申请实施例提供的一种 5G 网络中 ProSe 控制面架构示意图；
 图 3 为本申请实施例提供的通信设备的结构示意图；
 图 4 为本申请实施例提供的一种通信方法的交互示意图；
 图 5 为本申请实施例提供的另一种通信方法的交互示意图；
 图 6 为本申请实施例提供的又一种通信方法的交互示意图；
35 图 7 为本申请实施例提供的又一种通信方法的交互示意图；
 图 8 为本申请实施例提供的一种通信方法的流程示意图；
 图 9 为本申请实施例提供的另一种通信方法的流程示意图；
 图 10 为本申请实施例提供的又一种通信方法的流程示意图；
 图 11 为本申请实施例提供的通信装置的结构示意图。

具体实施方式

为了方便理解本申请实施例的技术方案，首先给出本申请相关技术的简要介绍如下。

第一，发现类型（discovery type）：

- 5 本申请实施例中，发现类型包括开放发现（open discovery）或者限制发现（restricted discovery）。open discovery 与 restricted discovery 的相关描述可参考现有的第三代合作伙伴计划（3rd generation partnership project, 3GPP）技术标准（technical standards, TS）23.303, v15.1.0, 在此不予赘述。举个例子，比如一个终端设备自己打游戏，没有明确的游戏伙伴，则他可以发起一个开放发现，“随机”找到一个游戏伙伴就行。而
- 10 若终端设备打游戏有明确的伙伴，则他可以通过限制发现来“指定”一个伙伴，只有他指定的伙伴才能接入游戏，其他的则不行。因此，开放发现就如摇一摇应用，可以随意的摇到开起了摇一摇应用的另一个用户。限制发现则如面对面建群，只有知道群号的用户才可以接入。

第二，发现模式（discovery mode）：

- 15 在现有 4G ProSe 标准中（3GPP TS 23.303, v15.1.0），定义了模式 A（Model A）或模式 B（Model B）。Model A 和 Model B 的区别在于发起 discovery 的方式不同。Model A 的含义是“我在这”，Model A 发现流程中两端终端设备分为播报方用户设备（user equipment, UE）（announcing UE）和监听方 UE（monitoring UE），announcing UE 广播“我在这”，monitoring UE 接收到 announcing UE 广播的消息后根据是否符合自己业务需求确定是否与 announcing UE 建立邻近业务的连接。Model B 的含义是“谁在那？/你在哪？”，Model B 发现流程中两端终端设备分为被发现者 UE（discoveree UE）和发现者 UE（discoverer UE），discoverer UE 发起特定业务请求，请求中包括特定的信息，就是问“谁在那？/你在哪？”，discoveree UE 接收到 discoverer UE 发起的业务请求之后根据自己是否可以提供业务服务来确定是否回复该请求消息，若回复响应消息，
- 20 说明“我在这”。其中，本申请实施例以 open discovery 场景适用于 model A 发现模型，而 restricted discovery 场景适用于 model A 和 model B 两种发现模型为例进行说明，在此统一说明，以下不再赘述。

第三，发现命令（discovery command）：

- 本申请实施例中，发现命令用于告知网络侧互相通信的两个终端设备是
- 30 announcing UE 还是 monitoring UE；是响应终端设备（response UE）还是请求终端设备（query UE）。其中，announcing UE 与 monitoring UE 为上述 Model A 发现流程中的两端终端设备，response UE 与 query UE 分别对应上述 Model B 发现流程中的 discoveree UE 和 discoverer UE，在此统一说明，以下不再赘述。

第四，用于 ProSe 业务的身份信息（user identity）：

- 35 用于 ProSe 业务的身份信息例如可以是应用级别的用户标识（application level user identity）。例如，用于 ProSe 业务的身份信息可以是邻近业务应用标识（ProSe application ID），或者是限制邻近业务应用用户标识（restricted ProSe application user ID, RPAUID）或者是邻近发现 UE 标识（ProSe discovery UE ID, PDUID）等。其中，本申请实施例以 ProSe application ID 用于开放发现（open discovery）场景，PDUID 或

RPAUID 用于限制发现 (restricted discovery) 场景为例进行说明, 在此统一说明, 以下不再赘述。

第五, PC5 连接与 PC5 连接建立流程:

本申请实施例中的 PC5 连接是指基于 PC5 接口的终端设备之间的通信连接。

- 5 本申请实施例中的 PC5 连接建立流程用于在支持 PC5 接口的至少 2 个终端设备之间建立通信连接。其中, PC5 连接建立完成后, 至少 2 个终端设备可以利用 PC5 连接进行控制面信令协商和/或用户面数据传递。本申请实施例中的 PC5 连接建立流程可以包括 PC5 单播连接建立 (one-to-one communication) 流程和 PC5 多播连接建立 (one-to-many communication) 流程。PC5 单播连接建立流程用于在支持 PC5 接口的 2 个终端设备之间建立通信连接, PC5 多播连接建立流程用于在支持 PC5 接口的 2 个以上终端设备之间建立通信连接。本申请下述实施例均是示例性的以 2 个终端设备之间建立通信连接为例进行说明, 即本申请下述实施例均是示例性的以 PC5 单播连接建立流程为例进行说明。PC5 多播连接建立流程中任意 2 个终端设备之间建立通信连接的方式可参考 PC5 单播连接建立流程中 2 个终端设备之间建立通信连接的流程, 在此统一说明, 以下不再赘述。

第六, 安全策略:

安全策略是用于描述是否开启安全保护的策略, 可用于确定安全保护方法。本申请实施例中用于不同场景的安全策略包括以下至少一种:

PC5 连接中的控制面机密性保护策略;

- 20 PC5 连接中的控制面完整性保护策略;

PC5 连接中的用户面机密性保护策略;

或者, PC5 连接中的用户面完整性保护策略。

- 其中, 控制面机密性保护即保护信令在传输过程中的机密性; 控制面完整性保护即保护信令在传输过程中的完整性; 用户面机密性保护即保护用户面数据在传输过程中的机密性; 用户面完整性保护即保护用户面数据在传输过程中的完整性。本申请实施例中, 完整性是指获取到的信令或数据与原始的信令或数据一致, 没有被修改, 因此, 完整性保护是为了使得攻击者“攻击不成”。机密性是指无法被直接看出真实内容, 因此机密性保护是为了使得攻击者“读不懂”。此外, 本申请实施例中的机密性保护也可以称为加密保护, 在此统一说明, 以下不再赘述。

- 30 本申请实施例中, PC5 连接中的控制面机密性保护策略与 PC5 连接中的控制面完整性保护策略属于 PC5 连接中的控制面安全策略; PC5 连接中的用户面机密性保护策略与 PC5 连接中的用户面完整性保护策略属于 PC5 连接中的用户面安全策略, 在此统一说明, 以下不再赘述。

- 35 本申请实施例中, 保护策略共分有开启 (REQUIRED), 不开启 (NOT NEEDED) 和可选 (PREFERRED) 三种。REQUIRED 为需要开启安全, NOT NEEDED 为不需要开启安全, PREFERRED 偏好开启或者称为可选开启, 即可以开启安全但也可以不开启安全, 在此统一说明, 以下不再赘述。

示例性的, 以 PC5 连接中的控制面机密性保护策略为例, 则 PC5 连接中的控制面机密性保护策略包括: PC5 连接中的控制面机密性保护开启 (REQUIRED)、PC5 连

接中的控制面机密性保护不开启 (NOT NEEDED)、或者 PC5 连接中的控制面机密性保护可选 (PREFERRED)。PC5 连接中的控制面机密性保护策略、PC5 连接中的用户面机密性保护策略、或者 PC5 连接中的用户面完整性保护策略的示例可参考 PC5 连接中的控制面机密性保护策略的示例, 在此不再赘述。

5 需要说明的是, 本申请实施例中, 安全策略在被发送时, 一般情况下只会选择三种(REQUIRED、NOT NEEDED 和 PREFERRED)中的一种发送, 在某些特殊的场景下可能会选择至少 2 种发送, 并且其中一个是 PREFERRED。比如, 在发送 NOT NEEDED 和 PREFERRED 时, 代表倾向不开启安全保护; 在发送 REQUIRED 和 PREFERRED 时, 则代表倾向开启安全保护。

10 需要说明的是, 本申请实施例中, PC5 连接中的控制面机密性保护策略、PC5 连接中的控制面完整性保护策略、PC5 连接中的用户面机密性保护策略; 或者, PC5 连接中的用户面完整性保护策略中的多种保护策略可以相同, 本申请实施例对此不做具体限定。

第七, 安全能力:

15 本申请实施例中的安全能力包括以下至少一种:

PC5 连接中支持的一个或者多个控制面机密性保护算法;

PC5 连接中支持的一个或者多个控制面完整性保护算法;

PC5 连接中支持的一个或者多个用户面机密性保护算法;

或者, PC5 连接中支持的一个或者多个用户面完整性保护算法。

20 其中, 控制面机密性保护算法是指一种用于保护控制面的机密性保护算法。控制面完整性保护算法是指一种用于保护控制面的完整性保护算法。用户面机密性保护算法是指一种用于保护用户面的机密性保护算法。用户面完整性保护算法是指一种用于保护控制面的用户面保护算法。其中, PC5 连接中支持的一个或者多个控制面机密性保护算法与 PC5 连接中支持的一个或者多个控制面完整性保护算法属于 PC5 连接中的
25 控制面安全能力; PC5 连接中支持的一个或者多个用户面机密性保护算法与 PC5 连接中支持的一个或者多个用户面完整性保护算法属于 PC5 连接中的用户面安全能力, 在此统一说明, 以下不再赘述。

需要说明的是, 本申请实施例中, PC5 连接中支持的一个或者多个控制面机密性保护算法、PC5 连接中支持的一个或者多个控制面完整性保护算法、PC5 连接中支持
30 的一个或者多个用户面机密性保护算法、或者 PC5 连接中支持的一个或者多个用户面完整性保护算法中的多种保护算法可以相同或者存在共同项, 本申请实施例对此不做具体限定。

第八, 安全保护与解安全保护:

本申请实施例中的安全保护是指使用安全保护方法对用户面数据/控制面信令进
35 行保护; 本申请实施例中的解安全保护是指根据安全保护方法还原用户面数据/控制面信令。其中, 这里的安全保护方法包括机密性保护和/或完整性保护是否开启, 在此统一说明, 以下不再赘述。

具体的, 当机密性保护开启时, 可以使用加密密钥和加密算法对用户面数据/控制面信令进行加密保护; 当完整性保护开启时, 可以使用完整性保护密钥和完整性保护

算法对用户面数据/控制面信令进行完整性保护。此外，需要说明的是，当需要对用户面数据/控制面信令进行加密保护和完整性保护时，可以对用户面数据/控制面信令先进行加密保护，再进行完整性保护；也可以对用户面数据/控制面信令先进行完整性保护，再进行加密保护，本申请实施例不限定加密保护和完整性保护的执行顺序，在此统一说明，以下不再赘述。

具体的，当机密性保护开启时，可以使用加密密钥和加密算法对用户面数据/控制面信令进行解密；当完整性保护开启时，可以使用完整性保护密钥和完整性保护算法对用户面数据/控制面信令进行完整性保护验证。此外，可以理解的是，当同时对用户面数据/控制面信令进行加密保护和完整性保护时，如果用户面数据/控制面信令先被加密保护，再被完整性保护，则解安全保护的顺序是先进行完整性保护验证、再对加密后的用户面数据/控制面信令进行解密；如果用户面数据/控制面信令先被完整性保护，再被加密，则解安全保护的顺序是先对加密后的用户面数据/控制面信令进行解密，再进行完整性保护验证，在此统一说明，以下不再赘述。

示例性的，本申请实施例中的安全保护方法分为以下三类：

1、ProSe 发现流程中第一条 PC5 广播消息使用的安全保护方法，用于保护 ProSe 发现流程中第一条 PC5 广播消息中传递的全部参数或部分参数。其中，第一条 PC5 广播消息使用的安全保护方法例如可以包括第一条 PC5 广播消息的机密性保护和/或完整性保护是否开启。示例性的，“00”可以表示机密性保护不开启，且完整性保护不开启；“01”可以表示机密性保护不开启，完整性保护开启；“10”可以表示机密性保护开启，完整性保护不开启；“11”可以表示机密性保护开启，且完整性保护开启。需要说明的是，该示例以高比特表征机密性保护，低比特表征完整性保护为例进行说明，当然，也可以是低比特表征机密性保护，高比特表征完整性保护，本申请实施例对此不作具体限定。此外，该示例以“0”表示不开启，“1”表示开启为例进行说明，当然，也可以是“1”表示不开启，“0”表示开启，本申请实施例对此不作具体限定。

本申请实施例中，不同发现模式对应的第一条 PC5 广播消息是不同的。比如，model A 发现模式下，第一条 PC5 广播消息是由播报方 UE（announcing UE）发送的，第一条 PC5 广播消息可以为广播（announcing）消息；model B 发现模式下，第一条 PC5 广播消息是由发现者 UE（discoverer UE）发送的，第一条 PC5 广播消息可以为请求代码（Send Query Code）消息。在此统一说明，以下不再赘述。

2、PC5 连接的控制面使用的安全保护方法，用于保护 PC5 连接的控制面信令中传递的全部参数或部分参数。其中，PC5 连接的控制面使用的安全保护方法例如可以包括 PC5 连接的控制面的机密性保护和/或完整性保护是否开启。相关示例可参考第一条 PC5 广播消息使用的安全保护方法中的示例，在此不再赘述。

3、PC5 连接的用户面使用的安全保护方法，用于保护 PC5 连接的部分或全部用户面数据。其中，PC5 连接的用户面使用的安全保护方法例如可以包括 PC5 连接的用户面的机密性保护和/或完整性保护是否开启。相关示例可参考第一条 PC5 广播消息使用的安全保护方法中的示例，在此不再赘述。

需要说明的是，本申请实施例中，PC5 连接的控制面使用的安全保护方法也可以

称之为 PC5 连接的控制面信令使用的安全保护方法；PC5 连接的用户面使用的安全保护方法也可以称之为 PC5 连接的用户面数据使用的安全保护方法，在此统一说明，以下不再赘述。

第九、MIC 与期望 MIC:

5 以终端设备 1 向终端设备 2 发送消息 1 为例:

本申请实施例中的 MIC 是使用终端设备 1 的完整性保护密钥对终端设备 1 发送的消息 1 中传递的全部参数或部分参数做完整性保护后的生成参数，包含在消息 1 中。本申请实施例中的期望 MIC 是使用终端设备 2 的完整性保护密钥（与终端设备 1 的完整性保护密钥相同）对终端设备 2 接收到的消息 1 中传递的全部参数或部分参数进行完整性校验的生成参数，用于与终端设备 2 接收到的消息 1 中的 MIC 作对比，进而校验终端设备 2 接收到的消息 1 是否被篡改。其中，MIC 与期望 MIC 的相关示例将结合后续方法实施例详细阐述，在此不予赘述。

需要说明的是，本申请实施例中，终端设备 1 的完整性保护密钥可以理解为用于对终端设备 1 发送的消息 1 进行完整性保护的密钥，可以被生成 MIC 的设备使用。其中，生成 MIC 的设备例如可以包括终端设备 1 或者其他设备（如终端设备 1 对应的直连通信发现名称管理功能网元），本申请实施例对此不做具体限定。当然，在终端设备 1 作为接收消息的设备时，以终端设备 1 接收来自终端设备 2 的消息 2 为例，则终端设备 1 的完整性保护密钥可以理解为用于对终端设备 1 接收的消息 2 进行完整性校验的密钥，可以被生成期望 MIC 的设备使用。其中，生成期望 MIC 的设备例如可以包括终端设备 1 或者其他设备（如终端设备 1 对应的直连通信发现名称管理功能网元），本申请实施例对此不做具体限定。

需要说明的是，本申请实施例中，终端设备 2 的完整性保护密钥可以理解为用于对终端设备 2 接收的消息 1 进行完整性校验的密钥，可以被生成期望 MIC 的设备使用。其中，生成期望 MIC 的设备例如可以包括终端设备 2 或者其他设备（如终端设备 2 对应的直连通信发现名称管理功能网元），本申请实施例对此不做具体限定。当然，在终端设备 2 作为发送消息的设备时，以终端设备 2 向终端设备 1 发送消息 2 为例，则终端设备 2 的完整性保护密钥可以理解为用于对终端设备 2 发送的消息 2 进行完整性保护的密钥，可以被生成 MIC 的设备使用。其中，生成 MIC 的设备例如可以包括终端设备 2 或者其他设备（如终端设备 2 对应的直连通信发现名称管理功能网元），本申请实施例对此不做具体限定。

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述。其中，在本申请的描述中，除非另有说明，“/”表示前后关联的对象是一种“或”的关系，例如，A/B 可以表示 A 或 B；本申请中的“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况，其中 A、B 可以是单数或者复数。并且，在本申请的描述中，除非另有说明，“多个”是指两个或两个以上。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项(个)或复数项(个)的任意组合。例如，a，b，或 c 中的至少一项(个)，可以表示：a，b，c，a-b，a-c，b-c，或 a-b-c，其中 a，b，c 可以是单个，也可以是多个。另外，为了便于清楚描述本申请实施例的技术方案，

在本申请的实施例中，采用了“第一”、“第二”等字样对功能和作用基本相同的相同项或相似项进行区分。本领域技术人员可以理解“第一”、“第二”等字样并不对数量和执行次序进行限定，并且“第一”、“第二”等字样也并无限定一定不同。同时，在本申请实施例中，“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请实施例中，
5 中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用“示例性的”或者“例如”等词旨在以具体方式呈现相关概念，便于理解。

此外，本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限制，本领域普通
10 技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

以 UE1 与 UE2 之间的 V2X PC5 建立流程为例，现有的 V2X PC5 建立流程（具体可参考 3GPP TS 23.303）中，首条消息直连通信请求（direct communication request）中需要携带 UE1 在 PC5 连接中的控制面安全策略（signaling security policy）以辅助
15 UE2 进行 PC5 连接的控制面的安全策略协商，此条消息没有安全保护。这样，当 UE1 和 UE2 本身被配置的安全策略均为可选（PREFERRED）的情况下，中间攻击者在接收到 UE1 发送的直连通信请求后，可将直连通信请求中的 signaling security policy 篡改
20 为不开启（NOT NEEDED）。进而，UE2 发现 UE1 的需求为 PC5 连接的控制面不开启安全保护，于是确定 PC5 连接的控制面安全保护方法为控制面不开启安全保护，并向 UE1 发送直连安全模式命令（direct security mode command）。由于控制面不开
25 启安全保护，此时攻击者可以再将上述直连安全模式命令中的 signaling security policy 篡改回 UE1 在直连通信请求中发送的内容，后续 PC5 连接的控制面安全则在中间攻击者干扰下强行不开启控制面安全保护。而在 PC5 建立流程中，UE1 与 UE2 的控制面安全策略均为可选（PREFERRED）且没有中间攻击者篡改的情况下，本来是可以开启控制
30 面安全保护的。攻击者以上述方式强制关闭了 UE1 与 UE2 之间的控制面安全保护，将会造成安全等级降级，且在后续 PC5 连接的用户面安全策略协商时也会因为没有控制面的安全保护，被攻击者进一步攻击。

为解决该问题，本申请实施例提供一种通信系统 10。如图 1a 所示，该通信系统 10 包括具有 ProSe 应用功能的第一终端设备 101 和具有 ProSe 应用功能的第二终端
30 设备 102。其中，第一终端设备 101 获取第一安全保护方法，该第一安全保护方法为第一终端设备 101 与第二终端设备 102 之间的发现流程中确定的安全保护方法。进而，第一终端设备 101 使用第一安全保护方法对第一终端设备 101 与第二终端设备 102 之间的 PC5 建立流程中的至少一条消息进行安全保护后，向第二终端设备 102 发送安全
35 保护后的至少一条消息。该方案的具体实现将在后续方法实施例中详细描述，在此不予赘述。基于本申请实施例提供的通信系统，一方面，在第一安全保护方法包括完整性保护开启的情况下，由于第一终端设备可以使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护，因此可以避免 PC5 建立流程中的消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。另一方面，在第一安全保护方法的安全等级高于或者等于

第一终端设备与第二终端设备之间的 PC5 连接的控制面使用的安全保护方法的安全等级的情况下，由于第一终端设备可以使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护，因此可以避免 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的安全等级所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

可选的，本申请实施例中，第一终端设备 101 或者第二终端设备 102 还可以根据第一安全保护方法确定第二安全保护方法，第二安全保护方法为第一终端设备 101 与第二终端设备 102 之间的 PC5 连接的安全保护方法。由于本申请实施例在确定第二安全保护方法时，可以参考发现流程中确定的第一安全保护方法，因此可以使得确定的第二安全保护方法的安全等级不低于第一安全保护方法的安全等级。也就是说，第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级，这样可以达到安全不降级的目的。

可选的，如图 1a 所示，该通信系统 10 还可以包括第一直连通信发现名称管理功能网元 103 和第二直连通信发现名称管理功能网元 104。其中，第一终端设备 101 获取第一安全保护方法，包括：第一终端设备 101 接收来自第一直连通信发现名称管理功能网元 103 的第一终端设备 101 使用 ProSe 业务时所需的安全保护方法。类似的，第二终端设备 102 可以接收来自第二直连通信发现名称管理功能网元 104 的第二终端设备 102 使用 ProSe 业务时所需的安全保护方法。其中，第一终端设备 101 使用 ProSe 业务时所需的安全保护方法与第二终端设备 102 使用 ProSe 业务时所需的安全保护方法均为上述第一安全保护方法。基于该方案，第一终端设备或第二终端设备可以在第一终端设备与第二终端设备之间的发现流程中获取使用 ProSe 业务时所需的安全保护方法。

如图 1b 所示，为本申请实施例提供的另一种通信系统 20。该通信系统 20 包括第一直连通信发现名称管理功能网元 201 和第二直连通信发现名称管理功能网元 202。该第一直连通信发现名称管理功能网元 201 和第二直连通信发现名称管理功能网元 202 之间可以直接通信，也可以通过其他设备的转发进行通信，本申请实施例对此不做具体限定。

其中，第一直连通信发现名称管理功能网元 201 从第二直连通信发现名称管理功能网元 202 获取第二终端设备使用 ProSe 业务时所需的安全保护方法；以及，第一直连通信发现名称管理功能网元 201 确定第一终端设备使用该 ProSe 业务时对应的多个可供选择的安全保护方法。进而，第一直连通信发现名称管理功能网元 201 根据多个可供选择的安全保护方法以及第二终端设备使用 ProSe 业务时所需的安全保护方法确定第一终端设备使用 ProSe 业务时所需的安全保护方法之后，向第一终端设备发送第一终端设备使用 ProSe 业务时所需的安全保护方法。该方案的具体实现将在后续方法实施例中详细描述，在此不予赘述。基于本申请实施例提供的通信系统，第一终端设备可以在第一终端设备与第二终端设备之间的发现流程中获取第一终端设备使用 ProSe 业务时所需的安全保护方法。

可选的，图 1a 所示的通信系统 10 或图 1b 所示的通信系统 20 可以适用于目前正在讨论的 5G 网络，也可以适用于未来的其他网络等，本申请实施例对此不做具体限

定。

示例性的，以图 1a 所示的通信系统 10 或图 1b 所示的通信系统 20 适用于目前正在讨论的 5G 网络为例，则本申请实施例中的直连通信发现名称管理功能网元（包括图 1b 中的第一直连通信发现名称管理功能网元 201 和第二直连通信发现名称管理功能网元 202）所对应的网元或者实体可以为该 5G 网络中的直连通信发现名称管理功能（direct discovery name management function, DDNMF）网元。本申请实施例中的终端设备（包括图 1a 中的第一终端设备 101 和第二终端设备 102）所对应的网元或者实体可以为该 5G 网络中的具有 ProSe 应用功能的终端设备。

如图 2 所示，为本申请实施例提供的一种 5G 网络中 ProSe 控制面架构示意图，包括一个或多个终端设备（图 2 以包括终端设备 1、终端设备 2、终端设备 3 与终端设备 4 为例进行示意）、下一代无线接入网络（next generation-radio access network, NG-RAN）设备、统一数据存储（unified data repository, UDR）网元、统一数据管理（unified data management, UDM）网元、会话管理功能（session management function, SMF）网元、接入和移动性管理功能（access and mobility management function, AMF）网元、网络开放功能（network exposure function, NEF）网元、策略控制功能（policy control function, PCF）网元、用户面功能（user plane function, UPF）网元、5G DDNMF 网元以及数据网络（data network, DN）。

其中，与传统蜂窝网络通信相比，可以用于 ProSe 通信的终端设备需要有临近业务应用（ProSe application）功能，具有 ProSe 应用功能的终端设备之间通过 PC5 口通信。与 ProSe 应用相对应的是 ProSe 应用服务器。ProSe 应用服务器可以是 DN 中的应用功能（application function, AF）网元。具有 ProSe 应用服务器功能的 AF 具有 23.501 R-15 版本中定义的 AF 的所有功能，以及用于 ProSe 业务的相关功能。也就是说，在 5G 网络中 ProSe 控制面架构中，ProSe 应用服务器与终端设备是通过终端设备-NG-RAN 设备-UPF 网元-AF 网元的路径进行用户面通信。此外，ProSe 应用服务器还可以通过 NEF 与 5G 核心网（5G core network, 5GC）中的其他网络功能（network function, NF）进行通信，比如通过 NEF 网元与 PCF 网元通信。

本申请实施例中，DDNMF 网元具有为开放临近业务直连发现（open ProSe direct discovery）分配和处理临近业务应用标识（ProSe application ID）与 ProSe 发现使用的 code 之间映射关系的作用。在限制性临近业务直连发现（restricted ProSe direct discovery）中，DDNMF 网元与 ProSe 应用服务器通过 PC2 接口通信，用于处理发现请求的授权。

此外，AMF 网元、UDR 网元、SMF 网元、UPF 网元、UDM 网元、NEF 网元或者 PCF 网元的相关描述可参考现有的 3GPP 5G 标准，在此不予赘述。

可选的，本申请实施例中的终端设备，可以是用于实现无线通信功能的设备，例如终端或者可用于终端中的芯片等，其可以部署在陆地上，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）。其中，终端可以是 5G 网络或者未来演进的公共陆地移动网（public land mobile network, PLMN）中的 UE、接入终端、终端单元、终端站、移动站、移动台、远方站、远程终端、移动设备、无线通信设备、终端代理或终端装置等。接入终端可以是蜂窝

电话、无绳电话、会话启动协议 (session initiation protocol, SIP) 电话、无线本地环路 (wireless local loop, WLL) 站、个人数字助理 (personal digital assistant, PDA)、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备或可穿戴设备, 无人机 (unmanned aerial vehicle, UAV) 和无人机控制器 (UAV controller, UAVC), 虚拟现实 (virtual reality, VR) 终端设备、增强现实 (augmented reality, AR) 终端设备、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。终端可以是移动的, 也可以是固定的。

可选的, 本申请实施例中的 RAN 设备, 是一种为终端设备提供无线通信功能的设备。接入网设备例如包括但不限于: 5G 中的下一代基站 (gnodeB, 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。

可选的, 本申请实施例中的第一终端设备、第二终端设备、第一直连通信发现名称管理功能网元与第二直连通信发现名称管理功能网元也可以称之为通信装置, 其可以是一个通用设备或者是一个专用设备, 本申请实施例对此不作具体限定。

可选的, 本申请实施例中的第一终端设备、第二终端设备、第一直连通信发现名称管理功能网元与第二直连通信发现名称管理功能网元的相关功能可以由一个设备实现, 也可以由多个设备共同实现, 还可以是由一个设备内的一个或多个功能模块实现, 本申请实施例对此不作具体限定。可以理解的是, 上述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的软件功能, 或者是硬件与软件的结合, 或者是平台 (例如, 云平台) 上实例化的虚拟化功能。

例如, 本申请实施例中的第一终端设备、第二终端设备、第一直连通信发现名称管理功能网元与第二直连通信发现名称管理功能网元的相关功能可以通过图 3 中的通信设备 300 来实现。图 3 所示为本申请实施例提供的通信设备 300 的结构示意图。该通信设备 300 包括一个或多个处理器 301, 通信线路 302, 以及至少一个通信接口 (图 3 中仅是示例性的以包括通信接口 304, 以及一个处理器 301 为例进行说明), 可选的还可以包括存储器 303。

处理器 301 可以是一个通用中央处理器 (central processing unit, CPU), 微处理器, 特定应用集成电路 (application-specific integrated circuit, ASIC), 或一个或多个用于控制本申请方案程序执行的集成电路。

通信线路 302 可包括一通路, 用于连接不同组件之间。

通信接口 304, 可以是收发模块用于与其他设备或通信网络通信, 如以太网, RAN, 无线局域网 (wireless local area networks, WLAN) 等。例如, 所述收发模块可以是收发器、收发机一类的装置。可选的, 所述通信接口 304 也可以是位于处理器 301 内的收

发电路，用以实现处理器的信号输入和信号输出。

存储器 303 可以是具有存储功能的装置。例如可以是只读存储器 (read-only memory, ROM) 或可存储静态信息和指令的其他类型的静态存储设备, 随机存取存储器 (random access memory, RAM) 或者可存储信息和指令的其他类型的动态存储设备, 也可以是电可擦可编程只读存储器 (electrically erasable programmable read-only memory, EEPROM)、只读光盘 (compact disc read-only memory, CD-ROM) 或其他光盘存储、光碟存储 (包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质, 但不限于此。存储器可以是独立存在, 通过通信线路 302 与处理器相连接。存储器也可以和处理器集成在一起。

其中, 存储器 303 用于存储执行本申请方案的计算机执行指令, 并由处理器 301 来控制执行。处理器 301 用于执行存储器 303 中存储的计算机执行指令, 从而实现本申请实施例中提供的通信方法。

或者, 可选的, 本申请实施例中, 也可以是处理器 301 执行本申请下述实施例提供的通信方法中的处理相关的功能, 通信接口 304 负责与其他设备或通信网络通信, 本申请实施例对此不作具体限定。

可选的, 本申请实施例中的计算机执行指令也可以称之为应用程序代码, 本申请实施例对此不作具体限定。

在具体实现中, 作为一种实施例, 处理器 301 可以包括一个或多个 CPU, 例如图 3 中的 CPU0 和 CPU1。

在具体实现中, 作为一种实施例, 通信设备 300 可以包括多个处理器, 例如图 3 中的处理器 301 和处理器 308。这些处理器中的每一个可以是一个单核 (single-core) 处理器, 也可以是一个多核 (multi-core) 处理器。这里的处理器可以包括但不限于以下至少一种: 中央处理单元 (central processing unit, CPU)、微处理器、数字信号处理器 (DSP)、微控制器 (microcontroller unit, MCU)、或人工智能处理器等各类运行软件的计算设备, 每种计算设备可包括一个或多个用于执行软件指令以进行运算或处理的核。

在具体实现中, 作为一种实施例, 通信设备 300 还可以包括输出设备 305 和输入设备 306。输出设备 305 和处理器 301 通信, 可以以多种方式来显示信息。例如, 输出设备 305 可以是液晶显示器 (liquid crystal display, LCD), 发光二极管 (light emitting diode, LED) 显示设备, 阴极射线管 (cathode ray tube, CRT) 显示设备, 或投影仪 (projector) 等。输入设备 306 和处理器 301 通信, 可以以多种方式接收用户的输入。例如, 输入设备 306 可以是鼠标、键盘、触摸屏设备或传感设备等。

上述的通信设备 300 有时也可以称为通信装置, 其可以是一个通用设备或者是一个专用设备。例如通信设备 300 可以是台式机、便携式电脑、网络服务器、掌上电脑 (personal digital assistant, PDA)、移动手机、平板电脑、无线终端设备、嵌入式设备、上述终端设备, 上述网络设备、或具有图 3 中类似结构的设备。本申请实施例不限定通信设备 300 的类型。

下面将结合附图, 对本申请实施例提供的通信方法进行示例性说明。

需要说明的是，本申请下述实施例中各个网元之间的消息名字或消息中各参数的名字等只是一个示例，具体实现中也可以是其他的名字，本申请实施例对此不作具体限定。

需要说明的是，本申请实施例中，“对消息进行安全保护”可以理解为对消息中
5 传递的全部参数或部分参数进行安全保护，在此统一说明，以下不再赘述。

本申请实施例提供一种通信方法，该通信方法使用 ProSe 发现流程中确定的安全保护方法对 PC5 建立流程中的一条或多条消息进行保护，从而可以提升 PC5 建立流程的安全等级。可选的，本申请实施例可以根据 ProSe 发现流程中确定的安全保护方法确定 PC5 连接的控制面使用的安全保护方法和/或 PC5 连接的用户面使用的安全保护
10 方法，其中，PC5 连接的控制面使用的安全保护方法和/或 PC5 连接的用户面使用的安全保护方法的安全等级不低于 ProSe 发现流程中确定的安全保护方法。也就是说，ProSe 发现流程中确定的安全保护方法是 PC5 建立流程中 PC5 连接的最低安全要求。这样可以达到安全不降级的目的。

下面将结合几个示例对该通信方法进行详细阐述。

一种可能的实现方式中，以 UE1 与 UE2 的交互为例，本申请实施例提供一种通信方法，该通信方法使用 ProSe 发现流程中确定的安全保护方法对 UE1 与 UE2 之间的 PC5 建立流程中的一条或多条消息进行完整性保护。同时在 PC5 建立流程中协商 UE1 与 UE2 之间的 PC5 连接（方便起见，后续将 UE1 与 UE2 之间的 PC5 连接简称为 PC5 连接）的控制面使用的安全保护方法和第一 PC5 连接的用户面使用的安全保护方法。
20 示例性的，如图 4 所示，本申请实施例提供的通信方法包括如下步骤：

S401、UE1 确定第一安全保护方法包括完整性保护开启。其中，该第一安全保护方法为 UE1 与 UE2 之间的 ProSe 发现流程中获取的安全保护方法。本申请实施例中不限定 ProSe 发现流程中确定安全保护方法的方式。一种可能的实现方式中，ProSe 发现流程中确定安全保护方法的方式可参考后续图 7 所示的实施例。

示例性的，本申请实施例中的 UE1 可以为 model A 发现模式下的播报方 UE（announcing UE），或者 UE1 可以为 model B 发现模式下的发现者 UE（discoverer UE）。

可选的，本申请实施例中的第一安全保护方法可以用于对 UE1 与 UE2 之间的 ProSe 发现流程中的第一条 PC5 广播消息进行安全保护。第一条 PC5 广播消息与安全保护方法的相关描述可参考具体实施方式前序部分，在此不再赘述。

30 可选的，本申请实施例中的第一安全保护方法还可以包括机密性保护开启，本申请实施例对此不做具体限定。

S402、UE1 向 UE2 发送直连通信请求（direct communication request）。相应的，UE2 接收来自 UE1 的直连通信请求。该直连通信请求包括 UE1 在 PC5 连接中的控制面安全策略、UE1 在 PC5 连接中的控制面安全能力以及 MIC1。其中，PC5 连接中的
35 控制面安全策略与控制面安全能力的相关描述可参考具体实施方式前序部分，在此不再赘述。

当然，本申请实施例中，该直连通信请求还可以包括 UE1 的部分或全部发现参数，发现参数的相关描述可参考图 7 所示的实施例中的表一、表二、表三或表四，在此不再赘述。

本申请实施例中，直连通信请求中传递的全部参数或部分参数是采用第一安全保护方法进行安全保护的。比如，可以采用第一安全保护方法对 UE1 在 PC5 连接中的控制面安全策略或者 UE1 在 PC5 连接中的控制面安全能力的至少一种进行安全保护。

5 本申请实施例中，MIC1 是使用 UE1 的完整性保护密钥对直连通信请求中传递的全部参数或部分参数做完整性保护后的生成参数。其中，UE1 的完整性保护密钥可以是 UE1 生成的，也可以是网络侧下发的，本申请实施例对此不做具体限定。

可选的，本申请实施例中，UE1 在 PC5 连接中的控制面安全策略和/或 UE1 在 PC5 连接中的控制面安全能力可以作为生成 MIC1 的输入参数。一种可能的实现方式中， $MIC1 = KDF(\text{参数一}, \text{参数二}, \text{其他参数})$ 。其中，参数一可以为 PC5 连接中的控制面安全策略，参数二可以为 PC5 连接中的控制面安全能力，密钥衍生功能 (key derivation function, KDF) 为计算 MIC1 的函数。示例性的，KDF 可以是一个哈希函数。示例性的，其他参数可以包括 UE1 的完整性保护密钥。

可选的，本申请实施例中，MIC1 可能是 UE1 自己生成的，也可能是 UE1 对应的 DDNMF 网元(可以称之为 DDNMF1 网元)生成的，本申请实施例对此不做具体限定。
15 其中，若 MIC1 是由 DDNMF1 网元生成，则在 UE1 向 UE2 发送直连通信请求之前，UE1 接收来自 DDNMF1 网元的 MIC1。可选的，若生成 MIC1 的输入参数中包括 UE1 在 PC5 连接中的控制面安全策略和/或 UE1 在 PC5 连接中的控制面安全能力，则一种可能的实现方式中，DDNMF1 网元生成 MIC1 所需的 UE1 在 PC5 连接中的控制面安全策略和/或 UE1 在 PC5 连接中的控制面安全能力是由 UE1 发送给 DDNMF1 网元的。
20 S403、UE2 验证 MIC1。

本申请实施例中，验证 MIC1 的过程也就是将接收到的直连通信请求中的 MIC1 与 MIC1 的期望 MIC 作对比的过程。其中，MIC1 的期望 MIC 是使用 UE2 的完整性保护密钥(与 UE1 的完整性保护密钥相同)对 UE2 接收到的直连通信请求中传递的全部参数或部分参数进行完整性校验的生成参数，用于与 UE2 接收到的直连通信请求中的 MIC1 作对比，进而校验 UE2 接收到的直连通信请求是否被篡改。具体的，当 MIC1 的期望 MIC 与 UE2 接收到的直连通信请求中的 MIC1 相同时，可以确定 MIC1 验证通过，即 UE2 可以确定接收到的直连通信请求未被篡改；或者，当 MIC1 的期望 MIC 与 UE2 接收到的直连通信请求中的 MIC1 不相同时，可以确定 MIC1 验证未通过，即 UE2 可以确定接收到的直连通信请求被篡改。其中，生成 MIC1 的期望 MIC 的公式与生成 MIC1 的公式相同，具体可参考生成 MIC1 的公式，在此不再赘述。
25 30

可选的，本申请实施例中，UE2 可以自己验证 MIC1，或者要通过匹配上报 (match report) 流程验证 MIC1，本申请实施例对此不做具体限定。其中，match report 可参考现有的 3GPP TS 33.303 标准，本申请实施例对此不予赘述。

一种可能的实现方式中，若 UE2 可以自己验证 MIC1，则此时由 UE2 根据 UE2 的完整性保护密钥(与 UE1 的完整性保护密钥相同)生成 MIC1 的期望 MIC。可选的，UE2 的完整性保护密钥可以是 UE2 从网络侧获得的，比如，UE2 在发现参数获取流程中从 UE1 对应的 DDNMF 网元(可以称之为 DDNMF1 网元)获得的。或者，可选的，UE2 的完整性保护密钥可以是 UE2 根据网络侧下发的完整性保护密钥的生成材料生成的。本申请实施例对完整性保护密钥的生成材料不做具体限定。示例性的，完整性保
35

护密钥的生成材料可以包括一个根密钥，还可以包括其他密钥生成参数等，在此统一说明，以下不再赘述。

另一种可能的实现方式中，若 UE2 要通过 match report 流程验证 MIC1，则可以由 UE2 对应的 DDNMF 网元（可以称之为 DDNMF2 网元）根据 UE2 的完整性保护密钥（与 UE1 的完整性保护密钥相同）生成 MIC1 的期望 MIC。可选的，UE2 的完整性保护密钥可以是 DDNMF2 网元从网络侧获取的，也可以是 DDNMF2 网元根据网络侧下发的完整性保护密钥的生成材料生成的，本申请实施例对此不做具体限定。可选的，若生成 MIC1 的期望 MIC 的输入参数中包括 UE1 在 PC5 连接中的控制面安全策略和/或 UE1 在 PC5 连接中的控制面安全能力，则一种可能的实现方式中，DDNMF2 网元生成 MIC1 的期望 MIC 所需的 UE1 在 PC5 连接中的控制面安全策略和/或 UE1 在 PC5 连接中的控制面安全能力是由 UE2 发送给 DDNMF2 网元的。进一步地，该方案中，DDNMF2 网元可以在 match report 流程中将 UE2 的完整性保护密钥发送给 UE2；或者 DDNMF2 网元可以在 match report 流程中将完整性保护密钥的生成材料发送给 UE2，由 UE2 根据完整性保护密钥的生成材料生成 UE2 的完整性保护密钥。UE2 获取 UE2 的完整性保护密钥后，保存 UE2 的完整性保护密钥，以便后续使用。

又一种可能的实现方式中，若 UE2 要通过 match report 流程验证 MIC1，则可以由 UE1 对应的 DDNMF 网元（可以称之为 DDNMF1 网元）根据 UE2 的完整性保护密钥（与 UE1 的完整性保护密钥相同）生成 MIC1 的期望 MIC。可选的，UE2 的完整性保护密钥可以是 DDNMF1 网元从网络侧获取的，也可以是 DDNMF1 网元根据网络侧下发的完整性保护密钥的生成材料生成的，本申请实施例对此不做具体限定。可选的，若生成 MIC1 的期望 MIC 的输入参数中包括 UE1 在 PC5 连接中的控制面安全策略和/或 UE1 在 PC5 连接中的控制面安全能力，则一种可能的实现方式中，DDNMF1 网元生成 MIC1 的期望 MIC 所需的 UE1 在 PC5 连接中的控制面安全策略和/或 UE1 在 PC5 连接中的控制面安全能力是由 UE2 通过 DDNMF2 网元发送给 DDNMF1 网元的。进一步的，该方案中，DDNMF1 网元可以在 match report 流程中通过 DDNMF2 网元将 UE2 的完整性保护密钥发送给 UE2，或者 DDNMF1 网元可以在 match report 流程通过 DDNMF2 网元中将完整性保护密钥的生成材料发送给 UE2，由 UE2 根据完整性保护密钥的生成材料生成 UE2 的完整性保护密钥。UE2 获取 UE2 的完整性保护密钥后，保存 UE1 的完整性保护密钥，以便后续使用。

本申请实施例中，若 MIC1 验证成功，可以说明步骤 S402 中的直连通信请求中传递的全部参数或部分参数保护完整，未受到外界攻击者攻击，进而可以继续执行下述步骤 S404。

S404、UE2 根据 UE1 在 PC5 连接中的控制面安全策略与 UE2 在 PC5 连接中的控制面安全策略，确定 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全保护方法；以及，UE2 根据 UE1 在 PC5 连接中的控制面安全能力与 UE2 在 PC5 连接中的控制面安全能力，确定 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全算法。其中，步骤 S404 的实现可参考现有技术，在此不予赘述。PC5 连接的控制面使用的安全保护方法的相关描述可参考具体实施方式前序部分，在此不予赘述。

本申请实施例中，PC5 连接的控制面使用的安全算法包括一个或者多个机密性保

护算法、以及一个或者多个完整性保护算法。

本申请实施例中，安全算法的选择遵循以下原则：

第一，控制面完整性保护不开启的情况下，对应选择的完整性和机密性保护算法均为空算法（null）。

5 第二，控制面完整性保护开启的情况下，对应选择的控制面完整性保护算法需要为非空算法（non-null）以表示控制面完整性保护开启；如果此时控制面机密性保护开启则对应选择的控制面机密性保护算法需要为非空算法（non-null）以表示控制面机密性保护开启；如果此时控制面机密性保护不开启则对应选择的控制面机密性保护算法需要为空算法（null）以表示控制面机密性保护不开启。

10 S405、UE2 向 UE1 发送直连安全模式命令（direct security mode command）。相应的，UE1 接收来自 UE2 的直连安全模式命令。其中，该直连安全模式命令中包括 UE2 选择的 PC5 连接的控制面使用的安全算法。

 可选的，本申请实施例中，该直连安全模式命令中还可以包括 UE1 在 PC5 连接中的控制面安全策略和/或 UE1 在 PC5 连接中的控制面安全能力。进而，UE1 接收来自
15 UE2 的直连安全模式命令之后，在 UE1 确定最终的 PC5 连接的控制面使用的安全保护方法包括控制面完整性保护不开启的情况下，UE1 需要确定直连安全模式命令中包括的 PC5 连接中的控制面安全策略是否是自己发送的 PC5 连接中的控制面安全策略，PC5 连接中的安全能力是否是自己发送的 PC5 连接中的安全能力，如果验证通过，可以继续执行后续流程，否则终止当前流程。这样可以防止降质攻击（bidding down
20 attack）。

 一种可能的实现方式中，本申请实施例中，若 UE2 确定 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全保护方法包括完整性保护开启，则本申请实施例可以采用 UE2 选择的 PC5 连接的控制面使用的安全算法对直连安全模式命令中传递的全部参数或部分参数进行完整性保护，具体的完整性保护方法可参考现有技术，在此不予赘述。

25 另一种可能的实现方式中，本申请实施例中，若 UE2 确定 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的安全等级（比如 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全保护方法包括完整性保护不开启，第一安全保护方法包括完整性保护开启），则本申请实施例中的直连安全模式命令中还包括 MIC2。MIC2 是使用 UE2 的完整性保护密钥对直连安全模式命令中传递的全部
30 参数或部分参数做完整性保护后的生成参数。示例性的，使用 UE2 的完整性保护密钥进行完整性保护的部分参数例如可以包括 UE2 选择的 PC5 连接的控制面使用的安全算法（选择的空算法）、UE1 在 PC5 连接中的控制面安全策略、UE1 在 PC5 连接中的控制面安全能力中的至少一种。在 UE2 确定 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的安全等级的情况下，由于该方案
35 可以使用 UE2 的完整性保护密钥对直连安全模式命令中传递的全部参数或部分参数做完整性保护，因此可以确保直连安全模式命令中的信息是可以被 UE1 信任的。进一步的，UE1 接收来自 UE2 的直连安全模式命令之后，还需要验证 MIC2。其中，UE1 验证 MIC2 的方式与上述 UE2 验证 MIC1 的方式类似，在此不再赘述。若 MIC2 验证成功，可以说明该直连安全模式命令中传递的全部参数或部分参数保护完整，未受到外

界攻击者攻击，进而可以继续执行下述步骤 S406。

可选的，本申请实施例中，UE2 的完整性保护密钥可以是 UE2 生成的，也可以是网络侧下发的，本申请实施例对此不做具体限定。

需要说明的是，本申请实施例中，生成的各个 MIC 或期望 MIC 所使用的完整性保护密钥是相同的，比如生成 MIC2 所使用的完整性保护密钥与上述生成 MIC1 或 MIC1 的期望 MIC 所使用的完整性保护密钥是相同的，下述生成 MIC3、MIC3 的期望 MIC、MIC4 或 MIC4 的期望 MIC 所使用的完整性保护密钥与上述生成 MIC1 或 MIC1 的期望 MIC 所使用的完整性保护密钥也是相同的，在此统一说明，以下不再赘述。

S406、UE1 根据 UE2 选择的 PC5 连接的控制面使用的安全算法确定最终的 PC5 连接的控制面使用的安全保护方法。

可选的，本申请实施例中，UE1 根据 UE2 选择的 PC5 连接的控制面使用的安全算法确定最终的 PC5 连接的控制面使用的安全保护方法，包括：

若 PC5 连接的控制面使用的安全算法中完整性保护算法为空算法（null），则最终的 PC5 连接的控制面使用的安全保护方法为：该 PC5 连接的控制面完整性保护和机密性保护均不开启。也就是说，PC5 连接中后续的控制面信令均不需要进行完整性保护与机密性保护。

若 PC5 连接的控制面使用的安全算法中完整性保护算法为 non-null，PC5 连接的控制面使用的安全算法中机密性保护算法为 non-null，则最终的 PC5 连接的控制面使用的安全保护方法为：该 PC5 连接的控制面完整性保护开启，且控制面机密性开启。也就是说，PC5 连接中后续的控制面信令均需要进行完整性保护与机密性保护。

若 PC5 连接的控制面使用的安全算法中完整性保护算法为 non-null，PC5 连接的控制面使用的安全算法中机密性保护算法为 null，则最终的 PC5 连接的控制面使用的安全保护方法为：该 PC5 连接的控制面完整性保护开启，且控制面机密性不开启。也就是说，PC5 连接中后续的控制面信令需要进行完整性保护，不需要进行机密性保护。

需要说明的是，本申请实施例中，UE1 确定的 PC5 连接的控制面使用的安全保护方法可用于后续协商 UE1 和 UE2 之间的 PC5 连接的用户面使用的安全保护方法的消息的保护，如步骤 S407 中的直连安全模式完成消息的安全保护以及步骤 S409 中直连通信接受消息的安全保护。此外，UE1 确定的 PC5 连接的控制面使用的安全保护方法还可以用于图 4 所示的 PC5 建立流程之后的控制面信令的安全保护，在此统一说明，以下不再赘述。

S407、UE1 向 UE2 发送直连安全模式完成（direct security mode complete）消息。相应的，UE2 接收来自 UE1 的直连安全模式完成消息。其中，该直连安全模式完成消息包括 UE1 在 PC5 连接中的用户面安全策略。

可选的，本申请实施例中，当 PC5 连接中的用户面安全能力与 PC5 连接中的控制面安全能力不相同，该直连安全模式完成消息还可以包括 UE1 在 PC5 连接中的用户面安全能力。

需要说明的是，本申请实施例中，假设标准规定 UE1 在 PC5 连接中的用户面安全能力与 UE1 在 PC5 连接中的控制面安全能力相同，或者安全能力不区分用户面与控制

面,则该直连安全模式完成消息不需要携带 UE1 在 PC5 连接中的用户面安全能力。该场景下,下述 UE1 在 PC5 连接中的用户面安全能力即为 UE1 在 PC5 连接中的控制面安全能力(也可以称之为 UE1 在 PC5 连接中的安全能力),在此统一说明,以下不再赘述。

5 其中,PC5 连接中的用户面安全策略与 PC5 连接中的用户面安全能力的相关描述可参考具体实施方式前序部分,在此不再赘述。

一种可能的实现方式中,本申请实施例中,若 UE1 确定最终的 PC5 连接的控制面使用的安全保护方法包括完整性保护开启,则本申请实施例可以采用 UE2 选择的 PC5 连接的控制面使用的安全算法对直连安全模式完成消息中传递的全部参数或部分参数
10 进行完整性保护,具体的完整性保护方法可参考现有技术,在此不予赘述。

另一种可能的实现方式中,本申请实施例中,若 UE1 确定最终的 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的安全等级(比如最终的 PC5 连接的控制面使用的安全保护方法的安全保护方法包括完整性保护不开启,第一安全保护方法包括完整性保护开启),则本申请实施例中的直连安全模式完成消息还包括 MIC3。MIC3 是使用 UE1 的完整性保护密钥对直连安全模式完成消息中传递的全部参数或部分参数做完整性保护后的生成参数。示例性的,使用 UE1 的完整性保护密
15 钥进行完整性保护的部分参数例如可以包括 UE1 在 PC5 连接中的用户面安全策略、UE1 在 PC5 连接中的用户面安全能力(可选)。在 UE1 确定最终的 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的安全等级的情况下,由于
20 该方案可以使用 UE1 的完整性保护密钥对直连安全模式完成消息中传递的全部参数或部分参数做完整性保护,因此可以确保直连安全模式完成消息中的信息是可以被 UE2 信任的。进一步的,UE2 接收来自 UE1 的直连安全模式完成消息之后,需要验证 MIC3。其中,UE2 验证 MIC3 的方式与上述 UE2 验证 MIC1 的方式类似,在此不再赘述。若 MIC3 验证成功,可以说明该直连安全模式完成消息中传递的全部参数或部分参数保护
25 完整,未受到外界攻击者攻击,进而可以继续执行下述步骤 S408。

可选的,本申请实施例中,UE1 在 PC5 连接中的用户面安全策略与 UE1 在 PC5 连接中的用户面安全能力(可选)可以作为生成 MIC3 的输入参数。具体的,MIC3 的计算方式可参考上述 MIC1 的计算方式,在此不予赘述。

可选的,本申请实施例中,MIC3 可能是 UE1 自己生成的,也可能是 UE1 对应的
30 DDNMF 网元(可以称之为 DDNMF1 网元)生成的,本申请实施例对此不做具体限定。其中,若 MIC3 是由 DDNMF1 网元生成,则在 UE1 向 UE2 发送直连安全模式完成消息之前,UE1 接收来自 DDNMF1 网元的 MIC3。可选的,若生成 MIC1 的输入参数中包括 UE1 在 PC5 连接中的用户面安全策略与 UE1 在 PC5 连接中的用户面安全能力(可选),则一种可能的实现方式中,DDNMF1 网元生成 MIC3 所需的 UE1 在 PC5 连接
35 中的用户面安全策略与 UE1 在 PC5 连接中的用户面安全能力(可选)是由 UE1 发送给 DDNMF1 网元的。

可选的,本申请实施例中,若 UE1 确定最终的 PC5 连接的控制面使用的安全保护方法包括机密性保护开启,则该直连安全模式完成消息中传递的全部参数或部分参数还需要进行机密性保护,具体的保护方式可参考现有技术,在此不予赘述。

S408、UE2 根据 UE1 在 PC5 连接中的用户面安全策略与 UE2 在 PC5 连接中的用户面安全策略，确定 UE1 与 UE2 之间的 PC5 连接的用户面使用的安全保护方法。其中，步骤 S408 的具体实现可参考现有技术，在此不予赘述。PC5 连接的用户面使用的安全保护方法的相关描述可参考具体实施方式前序部分，在此不予赘述。

- 5 可选的，本申请实施例中，若 PC5 连接的控制面使用的安全算法与 PC5 连接的用户面使用的安全算法不同，UE2 还需要根据 UE1 在 PC5 连接中的用户面安全能力与 UE2 在 PC5 连接中的用户面安全能力，确定 UE1 与 UE2 之间的 PC5 连接的用户面使用的安全算法，本申请实施例对此不做具体限定。其中，PC5 连接的用户面使用的安全算法包括一个或者多个机密性保护算法、以及一个或者多个完整性保护算法。安全
- 10 算法的选择遵循的原则可参考步骤 S404，在此不再赘述。

S409、UE2 向 UE1 发送直连通信接受（direct communication accept）消息。相应的，UE1 接收来自 UE2 的直连通信接受消息。其中，该直连通信接受消息包括 PC5 连接的用户面使用的安全保护方法。

- 可选的，本申请实施例中，该直连通信接受消息中还可以包括 UE1 在 PC5 连接中的用户面安全策略和 UE1 在 PC5 连接中的用户面安全能力（可选）。进而，UE1 接收来自 UE2 的直连通信接受消息之后，在 UE1 确定最终的 PC5 连接的控制面使用的安全保护方法包括控制面完整性保护不开启的情况下，UE1 需要确定直连通信接受消息中包括的 PC5 连接中的用户面安全策略是否是自己发送的 PC5 连接中的用户面安全策略，PC5 连接中的安全能力是否是自己发送的 PC5 连接中的安全能力，如果验证通过，
- 15 可以继续执行后续流程，否则终止当前流程。这样可以防止降质攻击。

可选的，本申请实施例中，若 UE2 确定 PC5 连接的用户面使用的安全算法，则该直连通信接受消息还包括 PC5 连接的用户面使用的安全算法。

- 一种可能的实现方式中，本申请实施例中，若步骤 S404 中 UE2 确定该 PC5 连接的控制面使用的安全保护方法包括控制面完整性保护，则本申请实施例可以采用 UE2
- 25 选择的 PC5 连接的控制面使用的安全算法对该直连通信接受消息中传递的全部参数或部分参数进行完整性保护，具体的完整性保护方法可参考现有技术，在此不予赘述。

- 另一种可能的实现方式中，本申请实施例中，若步骤 S407 中的直连安全模式完成消息中包括 MIC3，则步骤 S409 中的直连通信接受消息中还包括 MIC4。MIC4 是使用 UE2 的完整性保护密钥对直连通信接受消息中传递的全部参数或部分参数做完整性保护后的生成参数。示例性的，使用 UE2 的完整性保护密钥进行完整性保护的部分参数例如可以包括 PC5 连接的用户面使用的安全保护方法、PC5 连接的用户面使用的安全算法（可选）。在 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的安全等级（比如 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全保护方法包括完整性保护不开启，第一安全保护方法包括完整性保护开启）
- 30 的情况下，由于该方案可以使用 UE2 的完整性保护密钥对直连通信接受消息中传递的全部参数或部分参数做完整性保护，因此可以确保直连通信接受消息中的信息是可以被 UE1 信任的。进一步的，UE1 接收来自 UE2 的直连通信接受消息之后，还需要验证 MIC4。其中，UE1 验证 MIC4 的方式与上述 UE2 验证 MIC1 的方式类似，在此不再赘述。若 MIC4 验证成功，可以说明该直连通信接受消息中传递的全部参数或部分
- 35

参数保护完整，未受到外界攻击者攻击，进而可以继续执行后续流程。

基于本申请实施例提供的通信方法，由于 UE1 确定第一安全保护方法包括完整性保护开启之后，在 UE1 与 UE2 之间的 PC5 建立流程中，UE1 和 UE2 可以使用第一安全保护方法对 PC5 建立流程中的消息进行完整性保护，因此可以避免 PC5 建立流程中的消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

其中，上述步骤 S401 至 S409 中 UE1 或者 UE2 的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码以指令该 UE1 或者 UE2 执行，本实施例对此不作任何限制。

另一种可能的实现方式中，以 UE1 与 UE2 的交互为例，本申请实施例提供一种通信方法，该通信方法使用 ProSe 发现流程中确定的安全保护方法对 UE1 与 UE2 之间的 PC5 建立流程中的一条或多条消息进行安全保护。同时在 PC5 建立流程中根据 ProSe 发现流程中确定的安全保护方法确定 UE1 与 UE2 之间的 PC5 连接（方便起见，后续将 UE1 与 UE2 之间的 PC5 连接简称为 PC5 连接）的控制面使用的安全保护方法与 PC5 连接的用户面使用的安全保护方法。示例性的，如图 5 所示，本申请实施例提供的通信方法包括如下步骤：

S501、UE1 向 UE2 发送直连通信请求（direct communication request）。相应的，UE2 接收来自 UE1 的直连通信请求。其中，该直连通信请求包括 UE1 在 PC5 连接中的控制面安全能力。其中，PC5 连接中的控制面安全能力的相关描述可参考具体实施方式前序部分，在此不再赘述。

当然，本申请实施例中，该直连通信请求还可以包括 UE1 的部分或全部发现参数，具体可参考现有的 3GPP TS23.303，v15.1.0 标准，在此不再赘述。

可选的，本申请实施例中，直连通信请求中传递的全部参数或部分参数是采用第一安全保护方法进行安全保护的。比如，可以采用第一安全保护方法对 UE1 在 PC5 连接中的控制面安全能力进行安全保护。其中，第一安全保护方法为 UE1 与 UE2 之间的 ProSe 发现流程中获取的安全保护方法。本申请实施例中不限定 ProSe 发现流程中确定安全保护方法的方式。一种可能的实现方式中，ProSe 发现流程中确定安全保护方法的方式可参考后续图 7 所示的实施例。

可选的，本申请实施例中，该直连通信请求还可以包括 UE1 在 PC5 连接中的控制面安全策略，UE1 在 PC5 连接中的控制面安全策略可用于后续确定 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全保护方法。其中，UE1 在 PC5 连接中的控制面安全策略可以采用第一安全保护方法进行安全保护。PC5 连接中的控制面安全策略的相关描述可参考具体实施方式前序部分，在此不再赘述。

可选的，本申请实施例中，在 UE1 确定第一安全保护方法包括完整性保护开启的情况下，该直连通信请求还可以包括 MIC1。其中，MIC1 的相关描述可参考图 4 所示的实施例，在此不再赘述。进一步的，UE2 接收来自 UE1 的直连通信请求之后，可以验证 MIC1，MIC1 的验证方式可参考图 4 所示的实施例，在此不再赘述。若 MIC1 验证成功，可以说明步骤 S501 中的直连通信请求中传递的全部参数或部分参数保护完整，未受到外界攻击者攻击，进而可以继续执行下述步骤 S502。

S502、UE2 根据第一安全保护方法确定 PC5 连接的控制面使用的安全保护方法；以及，UE2 根据 UE1 在 PC5 连接中的控制面安全能力与 UE2 在 PC5 连接中的控制面安全能力，确定 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全算法。

下面给出 UE2 确定 PC5 连接的控制面使用的安全保护方法的两种具体实现。

- 5 一种可能的实现方式中，UE2 可以直接将第一安全保护方法确定为 PC5 连接的控制面使用的安全保护方法，即 UE2 直接按照第一安全保护方法激活 PC5 连接的控制面安全。示例性的，若第一安全保护方法为机密性保护开启，则 UE2 确定激活控制面机密性保护；若第一安全保护方法为机密性保护不开启，则 UE2 确定不激活控制面机密性保护；若第一安全保护方法为完整性保护开启，则 UE2 确定激活控制面控制完整性保护；若第一安全保护方法为完整性保护不开启，则 UE2 确定不激活控制面完整性保护。该方案中，由于 UE2 不需要与 UE1 协商 PC5 连接的控制面使用的安全保护方法，而是直接将第一安全保护方法确定为 PC5 连接的控制面使用的安全保护方法，因此不仅简化了 UE2 的处理逻辑，而且可以节省 PC5 建立流程的信令开销。

- 15 另一种可能的实现方式中，UE2 在确定 PC5 连接的控制面使用的安全保护方法时，还参考 UE1 在 PC5 连接中的控制面安全策略。

- 其中，在第一安全保护方法满足 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略（也可以理解为第一安全保护方法可以被 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略支持）的情况下，UE2 可以将第一安全保护方法确定为 PC5 连接的控制面使用的安全保护方法，即 UE2 按照第一安全保护方法激活 PC5 连接的控制面安全。比如，若第一安全保护方法为机密性保护不开启，完整性保护开启，并且 UE1 在 PC5 连接中的控制面安全策略为机密性保护可选，完整性保护可选，则 UE2 可以确定 PC5 连接的控制面使用的安全保护方法为机密性保护不开启，完整性保护开启。由于该方案在第一安全保护方法满足 UE1 在 PC5 连接中的控制面安全策略时，将第一安全保护方法确定为 PC5 连接的控制面使用的安全保护方法，因此不仅可以使得 UE2 确定出的 PC5 连接的控制面使用的安全保护方法能被 UE1 支持，而且保证了第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级，这样可以达到安全不降级的目的。

- 在第一安全保护方法不满足 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略（也可以理解为第一安全保护方法不可以被 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略支持）的情况下，UE2 可以选择一个满足 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略的安全保护方法作为 PC5 连接的控制面使用的安全保护方法，从而 UE2 按照选择的安全保护方法激活 PC5 连接的控制面安全。比如，若第一安全保护方法为机密性保护不开启，完整性保护开启，并且 UE1 在 PC5 连接中的控制面安全策略为机密性保护开启，完整性保护可选，则 UE2 可以确定 PC5 连接的控制面使用的安全保护方法为机密性保护开启，完整性保护开启。当然，本申请实施例中，在第一安全保护方法不满足 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略的情况下，UE2 也可以拒绝 UE1 的加入，本申请实施例对此不做具体限定。由于该方案在第一安全保护方法不满足 UE1 在 PC5 连接中的控制面安全策略时，UE2 根据 UE1 在 PC5 连接中的控制面安全策略，选择一

个满足 UE1 在 PC5 连接中的控制面安全策略的安全保护方法作为 PC5 连接的控制面使用的安全保护方法,因此不仅可以使得 UE2 确定出的 PC5 连接的控制面使用的安全保护方法能被 UE1 支持,而且保证了第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级,这样可以达到安全不降级的目的。

- 5 在第一安全保护方法满足 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略(也可以理解为第一安全保护方法可以被 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略支持)的情况下,UE2 还可以根据 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略,选择安全等级不低于第一安全保护方法的安全保护方法作为 PC5 连接的控制面使用的安全保护方法,从而 UE2 按照选择的
- 10 安全保护方法激活 PC5 连接的控制面安全。比如,若第一安全保护方法为机密性保护不开启,完整性保护不开启,并且 UE1 在 PC5 连接中的控制面安全策略为机密性保护可选,完整性保护可选,则 UE2 可以确定 PC5 连接的控制面使用的安全保护方法为机密性保护开启,完整性保护开启。由于该方案在第一安全保护方法满足 UE1 在 PC5 连接中的控制面安全策略时,UE2 根据 UE1 在 PC5 连接中的控制面安全策略,选择安全等级不低于第一安全保护方法的安全保护方法作为 PC5 连接的控制面使用的安全保护方法,因此不仅可以使得 UE2 确定出的 PC5 连接的控制面使用的安全保护方法也能被 UE1 使用,而且保证了第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级,这样可以达到安全不降级的目的。
- 15

- 又一种可能的实现方式中,UE2 在确定 PC5 连接的控制面使用的安全保护方法时,
- 20 还参考 UE1 在 PC5 连接中的控制面安全策略和 UE2 在 PC5 连接中的控制面安全策略。

- 其中,在第一安全保护方法可以同时满足 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略和 UE2 在本地保存或者从跟其他网元获取的 UE2 在 PC5 连接中的控制面安全策略(也可以理解为第一安全保护方法可以同时被 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略和 UE2 在本地保存或者从跟其他网元获取的 UE2 在 PC5 连接中的控制面安全策略支持)的情况下,UE2 可以将第一安全保护方法确定为 PC5 连接的控制面使用的安全保护方法,即 UE2 按照第一安全保护方法激活 PC5 连接的控制面安全。比如,若第一安全保护方法为机密性保护不开启,完整性保护开启,并且 UE1 在 PC5 连接中的控制面安全策略为机密性保护可选且完整性保护可选,UE2 在 PC5 连接中的控制面安全策略为机密性不开启,完整性保护可选,
- 25 则 UE2 可以确定 PC5 连接的控制面使用的安全保护方法为机密性保护不开启,完整性保护开启。由于该方案在第一安全保护方法可以同时满足 UE1 在 PC5 连接中的控制面安全策略和 UE2 在 PC5 连接中的控制面安全策略时,将第一安全保护方法确定为 PC5 连接的控制面使用的安全保护方法,因此不仅可以使得 UE2 确定出的 PC5 连接的控制面使用的安全保护方法能被 UE1 和 UE2 同时支持,而且保证了第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级,这样可以达到安全不降级的目的。
- 30
- 35

在第一安全保护方法不满足 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略或者 UE2 在本地保存或者从跟其他网元获取的 UE2 在 PC5 连接中的控制面安全策略(也可以理解为第一安全保护方法不可以同时被 UE1 在直连通信请求发

送的 UE1 在 PC5 连接中的控制面安全策略和 UE2 在本地保存或者从跟其他网元获取的 UE2 在 PC5 连接中的控制面安全策略支持)的情况下, UE2 可以选择一个满足 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略, 且满足 UE2 在本地保存或者从跟其他网元获取的 UE2 在 PC5 连接中的控制面安全策略的安全保护方法作为 PC5 连接的控制面使用的安全保护方法, 从而 UE2 按照选择的安全保护方法激活 PC5 连接的控制面安全。比如, 若第一安全保护方法为机密性保护不开启, 完整性保护开启, 并且 UE1 在 PC5 连接中的控制面安全策略为机密性保护开启且完整性保护可选, UE2 在 PC5 连接中的控制面安全策略为机密性保护开启且完整性保护可选, 则 UE2 可以确定 PC5 连接的控制面使用的安全保护方法为机密性保护开启, 完整性保护开启。

当然, 本申请实施例中, 在第一安全保护方法不满足 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略或者 UE2 在本地保存或者从跟其他网元获取的 UE2 在 PC5 连接中的控制面安全策略的情况下, UE2 也可以拒绝 UE1 的加入, 本申请实施例对此不做具体限定。由于该方案在第一安全保护方法不满足 UE1 在 PC5 连接中的控制面安全策略或者 UE2 在 PC5 连接中的控制面安全策略时, UE2 根据 UE1 在 PC5 连接中的控制面安全策略以及 UE2 在 PC5 连接中的控制面安全策略, 选择一个满足 UE1 在 PC5 连接中的控制面安全策略且满足 UE2 在 PC5 连接中的控制面安全策略的安全保护方法作为 PC5 连接的控制面使用的安全保护方法, 因此不仅可以使得 UE2 确定出的 PC5 连接的控制面使用的安全保护方法能被 UE1 和 UE2 同时支持, 而且保证了第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级, 这样可以达到安全不降级的目的。

在第一安全保护方法可以同时满足 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略和 UE2 在本地保存或者从跟其他网元获取的 UE2 在 PC5 连接中的控制面安全策略(也可以理解为第一安全保护方法可以同时被 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略和 UE2 在本地保存或者从跟其他网元获取的 UE2 在 PC5 连接中的控制面安全策略支持)的情况下, UE2 还可以根据 UE1 在直连通信请求发送的 UE1 在 PC5 连接中的控制面安全策略以及 UE2 在本地保存或者从跟其他网元获取的 UE2 在 PC5 连接中的控制面安全策略, 选择安全等级不低于第一安全保护方法的安全保护方法作为 PC5 连接的控制面使用的安全保护方法, 从而 UE2 按照选择的安全保护方法激活 PC5 连接的控制面安全。比如, 若第一安全保护方法为机密性保护开启, 完整性保护不开启, 并且 UE1 在 PC5 连接中的控制面安全策略为机密性保护可选且完整性保护可选, UE2 在 PC5 连接中的控制面安全策略的机密性保护不开启, 则 UE2 可以确定 PC5 连接的控制面使用的安全保护方法为机密性保护开启, 完整性保护开启。由于该方案在第一安全保护方法同时满足 UE1 在 PC5 连接中的控制面安全策略和 UE2 在 PC5 连接中的控制面安全策略时, UE2 根据 UE1 在 PC5 连接中的控制面安全策略以及 UE2 在 PC5 连接中的控制面安全策略, 选择安全等级不低于第一安全保护方法的安全保护方法作为 PC5 连接的控制面使用的安全保护方法, 因此不仅可以使得 UE2 确定出的 PC5 连接的控制面使用的安全保护方法能被 UE1 和 UE2 同时支持, 而且保证了第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级, 这样可以达到安全不降级的目的。

综上，也就是说，本申请实施例中，UE2 确定的 PC5 连接的控制面使用的安全保护方法的安全等级不低于第一安全保护方法的安全等级。也就是说，第一安全保护方法的安全等级是控制面信令交互的最低安全等级要求，这样可以达到安全不降级的目的。

- 5 进一步地，本申请实施例中，在 UE2 确定 PC5 连接的控制面使用的安全保护方法之后，UE2 可以根据 UE1 在 PC5 连接中的控制面安全能力与 UE2 在 PC5 连接中的控制面安全能力，结合 UE2 确定的 PC5 连接的控制面使用的安全保护方法确定 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全算法。其中，PC5 连接的控制面使用的安全算法包括一个或者多个机密性保护算法、以及一个或者多个完整性保护算法。安全算
10 法的选择遵循的原则可参考步骤 S404，在此不再赘述。

S503、UE2 向 UE1 发送直连安全模式命令（direct security mode command）。相应的，UE1 接收来自 UE2 的直连安全模式命令。其中，该直连安全模式命令中包括 UE2 选择的 PC5 连接的控制面使用的安全算法。

- 可选的，本申请实施例中，该直连安全模式命令中还可以包括 UE1 在 PC5 连接中的控制面安全策略和/或 UE1 在 PC5 连接中的控制面安全能力。进而，UE1 接收来自
15 UE2 的直连安全模式命令之后，在 UE1 确定最终的 PC5 连接的控制面使用的安全保护方法包括控制面完整性保护不开启的情况下，UE1 需要确定直连安全模式命令中包括的 PC5 连接中的控制面安全策略是否是自己发送的 PC5 连接中的控制面安全策略，PC5 连接中的安全能力是否是自己发送的 PC5 连接中的安全能力，如果验证通过，可
20 以继续执行后续流程，否则终止当前流程。这样可以防止降质攻击（bidding down attack）。

- 本申请实施例中，直连安全模式命令中传递的全部参数或部分参数是采用 UE2 确定的 PC5 连接的控制面使用的安全保护方法进行安全保护的。比如，若 UE2 将第一安全保护方法确定为 PC5 连接的控制面使用的安全保护方法，则直连安全模式命令中传递的全部参数或部分参数是采用第一安全保护方法进行安全保护的。其中，对直连安全模式命令中传递的全部参数或部分参数进行安全保护的方式可参考现有技术，在此不予赘述。示例性的，直连安全模式命令中进行安全保护的部分参数例如可以包括 UE2 选择的 PC5 连接的控制面使用的安全算法、UE1 在 PC5 连接中的控制面安全策略、UE1 在 PC5 连接中的控制面安全能力中的至少一种。

- 30 S504、UE1 根据 UE2 选择的 PC5 连接的控制面使用的安全算法确定最终的 PC5 连接的控制面使用的安全保护方法。

 其中，步骤 S504 的相关描述可参考图 4 所示的实施例步骤 S406，在此不再赘述。

- 需要说明的是，本申请实施例中，UE1 确定的 PC5 连接的控制面使用的安全保护方法可用于后续协商 UE1 和 UE2 之间的 PC5 连接的用户面使用的安全保护方法的消息的保护，如步骤 S505 中的直连安全模式完成消息的安全保护以及步骤 S507 中直连通信接受消息的安全保护。此外，UE1 确定的 PC5 连接的控制面使用的安全保护方法还可以用于图 5 所示的 PC5 建立流程之后的控制面信令的安全保护，在此统一说明，
35 以下不再赘述。

S505、UE1 向 UE2 发送直连安全模式完成（direct security mode complete）消息。

相应的，UE2 接收来自 UE1 的直连安全模式完成消息。

可选的，本申请实施例中，该直连安全模式完成消息可以包括 UE1 在 PC5 连接中的用户面安全策略，UE1 在 PC5 连接中的用户面安全策略可用于后续确定 UE1 与 UE2 之间的 PC5 连接的用户面使用的安全保护方法。其中，PC5 连接中的用户面安全策略的相关描述可参考具体实施方式前序部分，在此不再赘述。

可选的，本申请实施例中，当 PC5 连接中的用户面安全能力与 PC5 连接中的控制面安全能力不相同，该直连安全模式完成消息还可以包括 UE1 在 PC5 连接中的用户面安全能力。

需要说明的是，本申请实施例中，假设标准规定 UE1 在 PC5 连接中的用户面安全能力与 UE1 在 PC5 连接中的控制面安全能力相同，或者安全能力不区分用户面与控制面，则该直连安全模式完成消息不需要携带 UE1 在 PC5 连接中的用户面安全能力。该场景下，下述 UE1 在 PC5 连接中的用户面安全能力即为 UE1 在 PC5 连接中的控制面安全能力，在此统一说明，以下不再赘述。

本申请实施例中，直连安全模式完成消息中传递的全部参数或部分参数是采用 UE1 确定的 PC5 连接的控制面使用的安全保护方法进行安全保护的。比如，若 UE2 将第一安全保护方法确定为 PC5 连接的控制面使用的安全保护方法，则直连安全模式完成消息中传递的全部参数或部分参数是采用第一安全保护方法进行安全保护的。其中，对直连安全模式完成消息中传递的全部参数或部分参数进行安全保护的方式可参考现有技术，在此不予赘述。示例性的，直连安全模式完成消息中进行安全保护的部分参数例如可以 UE1 在 PC5 连接中的用户面安全策略或 UE1 在 PC5 连接中的用户面安全能力中的至少一种。

S506、UE2 根据第一安全保护方法确定 PC5 连接的用户面使用的安全保护方法。

本申请实施例中，UE2 根据第一安全保护方法确定 PC5 连接的用户面使用的安全保护方法的实现方式与上述步骤 S502 中 UE2 根据第一安全保护方法确定 PC5 连接的控制面使用的安全保护方法的实现方式类似，区别比如在于：1、将步骤 S502 中的控制面替换为步骤 S506 中的用户面；2、步骤 S506 中 UE1 在 PC5 连接中的用户面安全策略来自 UE1 向 UE2 发送的直连安全模式完成消息，其余相关描述可参考上述步骤 S502，在此不再赘述。

也就是说，本申请实施例中，UE2 确定的 PC5 连接的用户面使用的安全保护方法的安全等级不低于第一安全保护方法的安全等级。也就是说第一安全保护方法的安全等级是用户面数据交互的最低安全要求，这样可以达到安全不降级的目的。

可选的，本申请实施例中，若 PC5 连接的控制面使用的安全算法与 PC5 连接的用户面使用的安全算法不同，则在 UE2 确定 PC5 连接的用户面使用的安全保护方法之后，UE2 还需要根据 UE1 在 PC5 连接中的用户面安全能力与 UE2 在 PC5 连接中的用户面安全能力，结合 UE2 的确定 PC5 连接的用户面使用的安全保护方法，确定 UE1 与 UE2 之间的 PC5 连接的用户面使用的安全算法，本申请实施例对此不做具体限定。其中，PC5 连接的用户面使用的安全算法包括一个或者多个机密性保护算法、以及一个或者多个完整性保护算法。安全算法的选择遵循的原则可参考步骤 S404，在此不再赘述。

S507、UE2 向 UE1 发送直连通信接受（direct communication accept）消息。相应

的，UE1 接收来自 UE2 的直连通信接受消息。其中，该直连通信接受消息包括 PC5 连接的用户面使用的安全保护方法。

可选的，本申请实施例中，该直连通信接受消息中还可以包括 UE1 在 PC5 连接中的用户面安全策略和 UE1 在 PC5 连接中的用户面安全能力（可选）。进而，UE1 接收来自 UE2 的直连通信接受消息之后，在 UE1 确定最终的 PC5 连接的控制面使用的安全保护方法包括控制面完整性保护不开启的情况下，UE1 需要确定直连通信接受消息中包括的 PC5 连接中的用户面安全策略是否是自己发送的 PC5 连接中的用户面安全策略，PC5 连接中的安全能力是否是自己发送的 PC5 连接中的安全能力，如果验证通过，可以继续执行后续流程，否则终止当前流程。这样可以防止降质攻击。

可选的，本申请实施例中，若 UE2 确定 PC5 连接的用户面使用的安全算法，则该直连通信接受消息还包括 PC5 连接的用户面使用的安全算法。

本申请实施例中，直连通信接受消息中传递的全部参数或部分参数是采用 UE2 确定的 PC5 连接的控制面使用的安全保护方法进行安全保护的。比如，若 UE2 将第一安全保护方法确定为 PC5 连接的控制面使用的安全保护方法，则直连通信接受消息中传递的全部参数或部分参数是采用第一安全保护方法进行安全保护的。其中，对直连通信接受消息中传递的全部参数或部分参数进行安全保护的方式可参考现有技术，在此不予赘述。示例性的，直连通信接受消息中进行安全保护的部分参数例如可以包括 PC5 连接的用户面使用的安全保护方法、UE1 在 PC5 连接中的用户面安全策略和 UE1 在 PC5 连接中的用户面安全能力、或者 PC5 连接的用户面使用的安全算法中的至少一种。

基于本申请实施例提供的通信方法，一方面，由于本申请实施例在 PC5 建立流程中可以根据第一安全保护方法确定 PC5 连接的控制面使用的安全保护方法和 PC5 连接的用户面使用的安全保护方法，其中，PC5 连接的控制面使用的安全保护方法和 PC5 连接的用户面使用的安全保护方法的安全等级均不低于第一安全保护方法的安全等级。也就是说，第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级要求，这样可以达到安全不降级的目的。另一方面，本申请实施例可以使用第一安全保护方法对 PC5 建立流程中的第一条消息进行保护，则在第一安全保护方法包括完整性保护开启时，UE1 和 UE2 可以使用 ProSe 发现流程中确定的第一安全保护方法对 PC5 建立流程中的第一条消息进行完整性保护，因此可以避免 PC5 建立流程中的消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

其中，上述步骤 S501 至 S507 中 UE1 或者 UE2 的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码以指令该 UE1 或者 UE2 执行，本实施例对此不作任何限制。

需要说明的是，图 5 所示的实施例以根据第一安全保护方法确定 PC5 连接的控制面使用的安全保护方法与 PC5 连接的用户面使用的安全保护方法为例进行说明。可选的，本申请实施例中，也可以根据第一安全保护方法确定 PC5 连接的控制面使用的安全保护方法，通过图 4 所示的实施例中步骤 S407-S409 的方式协商 PC5 连接的用户面使用的安全保护方法；或者，本申请实施例中，也可以根据第一安全保护方法确定 PC5 连接的用户面使用的安全保护方法，通过类似图 4 所示的实施例中步骤 S402-S406 的方式协商 PC5 连接的控制面使用的安全保护方法，本申请实施例对此不做具体限定。

另一种可能的实现方式中，以 UE1 与 UE2 的交互为例，本申请实施例提供一种通信方法，该通信方法使用 ProSe 发现流程中确定的安全保护方法对 UE1 与 UE2 之间的 PC5 建立流程中的一条或多条消息进行安全保护。同时在 PC5 建立流程中根据 ProSe 发现流程中确定的安全保护方法确定 UE1 与 UE2 之间的 PC5 连接（方便起见，后续将 UE1 与 UE2 之间的 PC5 连接简称为 PC5 连接）的控制面使用的安全保护方法，协商 PC5 连接的用户面使用的安全保护方法。示例性的，如图 6 所示，本申请实施例提供的通信方法包括如下步骤：

S601、UE1 向 UE2 发送直连通信请求（direct communication request）。相应的，UE2 接收来自 UE1 的直连通信请求。其中，该直连通信请求包括 UE1 在 PC5 连接中的用户面安全策略以及 UE1 在 PC5 连接中的控制面安全能力。其中，PC5 连接中的用户面安全策略与 PC5 连接中的控制面安全能力的相关描述可参考具体实施方式前序部分，在此不再赘述。

当然，本申请实施例中，该直连通信请求还可以包括 UE1 的部分或全部发现参数，具体可参考现有的 3GPP TS23.303，v15.1.0 标准，在此不再赘述。

需要说明的是，假设标准规定 UE1 在 PC5 连接中的控制面安全能力与 UE1 在 PC5 连接中的用户面安全能力相同，或者安全能力不区分用户面与控制面，则本申请实施例中，PC5 连接中的控制面安全能力也可以称之为 PC5 连接中的安全能力，在此统一说明，以下不再赘述。

可选的，本申请实施例中，直连通信请求中传递的全部参数或部分参数是采用第一安全保护方法进行安全保护的。比如，可以第一安全保护方法对 UE1 在 PC5 连接中的用户面安全策略和/或 UE1 在 PC5 连接中的控制面安全能力进行安全保护。其中，第一安全保护方法为 UE1 与 UE2 之间的 ProSe 发现流程中获取的安全保护方法。本申请实施例中不限定 ProSe 发现流程中确定安全保护方法的方式。一种可能的实现方式中，ProSe 发现流程中确定安全保护方法的方式可参考后续图 7 所示的实施例。

可选的，本申请实施例中，该直连通信请求还可以包括 UE1 在 PC5 连接中的控制面安全策略，UE1 在 PC5 连接中的控制面安全策略可用于后续确定 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全保护方法。其中，UE1 在 PC5 连接中的控制面安全策略可以采用第一安全保护方法进行安全保护。PC5 连接中的控制面安全策略的相关描述可参考具体实施方式前序部分，在此不再赘述。

可选的，本申请实施例中，当 PC5 连接中的用户面安全能力与 PC5 连接中的控制面安全能力不相同，该直连通信请求还可以包括 UE1 在 PC5 连接中的用户面安全能力。

可选的，本申请实施例中，在 UE1 确定第一安全保护方法包括完整性保护开启的情况下，该直连通信请求还可以包括 MIC3。其中，MIC3 的相关描述可参考图 4 所示的实施例，在此不再赘述。进一步的，UE2 接收来自 UE1 的直连通信请求之后，可以验证 MIC3，MIC3 的验证方式可参考图 4 所示的实施例，在此不再赘述。若 MIC3 验证成功，可以说明步骤 S601 中的直连通信请求中传递的全部参数或部分参数保护完整，未受到外界攻击者攻击，进而可以继续执行下述步骤 S602。

S602、UE2 根据第一安全保护方法确定 PC5 连接的控制面使用的安全保护方法；

以及, UE2 根据 UE1 在 PC5 连接中的控制面安全能力与 UE2 在 PC5 连接中的控制面安全能力, 确定 UE1 与 UE2 之间的 PC5 连接的控制面使用的安全算法。

其中, 步骤 S602 的相关描述可参考图 5 所示的实施例中的步骤 S502, 在此不再赘述。

- 5 S603、UE2 根据 UE1 在 PC5 连接中的用户面安全策略与 UE2 在 PC5 连接中的用户面安全策略, 确定 UE1 与 UE2 之间的 PC5 连接的用户面使用的安全保护方法。

其中, 步骤 S603 的相关描述可参考图 4 所示的实施例中的步骤 S408, 在此不再赘述。

- 10 S604、UE2 向 UE1 发送直连安全模式命令 (direct security mode command)。相应的, UE1 接收来自 UE2 的直连安全模式命令。其中, 该直连安全模式命令中包括 PC5 连接的用户面使用的安全保护方法以及 UE2 选择的 PC5 连接的控制面使用的安全算法。

- 可选的, 本申请实施例中, 该直连安全模式命令中还可以包括 UE1 在 PC5 连接中的用户面安全策略、UE1 在 PC5 连接中的控制面安全能力 (可选)、UE1 在 PC5 连接中的用户面安全能力 (可选) 以及 UE1 在 PC5 连接中的控制面安全策略 (可选)。进而, UE1 接收来自 UE2 的直连安全模式命令之后, 在 UE1 确定最终的 PC5 连接的控制面使用的安全保护方法包括控制面完整性保护不开启的情况下, UE1 需要确定直连安全模式命令中包括的 PC5 连接中的用户面安全策略是否是自己发送的 PC5 连接中的用户面安全策略, PC5 连接中的控制面安全能力是否是自己发送的 PC5 连接中的控制面安全能力, PC5 连接中的用户面安全能力是否是自己发送的 PC5 连接中的用户面安全能力, PC5 连接中的控制面安全策略是否是自己发送的 PC5 连接中的控制面安全策略。如果验证通过, 可以继续执行后续流程, 否则终止当前流程。这样可以防止降质攻击。

- 25 可选的, 本申请实施例中, 若 UE2 确定 PC5 连接的用户面使用的安全算法, 则该直连安全模式命令还包括 PC5 连接的用户面使用的安全算法。

- 本申请实施例中, 直连安全模式命令中传递的全部参数或部分参数是采用 UE2 确定的 PC5 连接的控制面使用的安全保护方法进行安全保护的。比如, 若 UE2 将第一安全保护方法确定为 PC5 连接的控制面使用的安全保护方法, 则直连安全模式命令中传递的全部参数或部分参数是采用 ProSe 发现流程中确定的第一安全保护方法进行安全保护的。其中, 对直连安全模式命令中传递的全部参数或部分参数进行安全保护的方式可参考现有技术, 在此不予赘述。示例性的, 直连安全模式命令中进行安全保护的部分参数例如可以包括 UE2 选择的 PC5 连接的控制面使用的安全算法、PC5 连接的用户面使用的安全保护方法、UE1 在 PC5 连接中的用户面安全策略、UE1 在 PC5 连接中的用户面安全能力、UE1 在 PC5 连接中的控制面安全能力、UE1 在 PC5 连接中的控制面安全策略、PC5 连接的用户面使用的安全算法中的至少一种。

S605、UE1 根据 UE2 选择的 PC5 连接的控制面使用的安全算法确定最终的 PC5 连接的控制面使用的安全保护方法。

其中, 步骤 S605 的相关描述可参考图 4 所示的实施例步骤 S406, 在此不再赘述。

至此, UE1 和 UE2 均可以获知 PC5 连接的控制面使用的安全保护方法以及 PC5

连接的用户面使用的安全保护方法。

需要说明的是，本申请实施例中，UE1 确定的 PC5 连接的控制面使用的安全保护方法可用于图 6 所示的 PC5 建立流程之后的控制面信令的安全保护，在此统一说明，以下不再赘述。

- 5 可选的，本申请实施例中步骤 S601 中的直连通信请求也可以替换为直连安全模式完成消息，步骤 S604 中的直连安全模式命令也可以替换为直连通信接受消息。即通过现有的 PC5 连接的用户面使用的安全保护方法的协商流程的消息进行上述 PC5 连接的用户面使用的安全保护方法的协商，本申请实施例对此不做具体限定。

- 10 基于本申请实施例提供的通信方法，一方面，由于本申请实施例在 PC5 建立流程中可以根据第一安全保护方法确定 PC5 连接的控制面使用的安全保护方法，其中，PC5 连接的控制面使用的安全保护方法的安全等级均不低于第一安全保护方法的安全等级。也就是说，第一安全保护方法的安全等级是控制面信令交互的最低安全等级要求，这样可以达到安全不降级的目的。另一方面，本申请实施例可以使用第一安全保护方法对 PC5 建立流程中的第一条消息进行保护，则在第一安全保护方法包括完整性保护开启时，UE1 和 UE2 可以使用第一安全保护方法对 PC5 建立流程中的第一条消息进行完整性保护，因此可以避免 PC5 建立流程中的消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

- 15 需要说明的是，图 6 所示的实施例以在 PC5 建立流程中根据第一安全保护方法确定 PC5 连接的控制面使用的安全保护方法，协商 PC5 连接的用户面使用的安全保护方法为例进行说明。可选的，本申请实施例还可以提供一种通信方法，该通信方法使用第一安全保护方法对 PC5 建立流程中的一条或多条消息进行安全保护。同时在 PC5 建立流程中根据第一安全保护方法确定 PC5 连接的用户面使用的安全保护方法，协商 PC5 连接的控制面使用的安全保护方法。其中，该方法的具体实现可参考图 6 所示的实施例，在此不再赘述。

- 25 其中，上述步骤 S601 至 S605 中 UE1 或者 UE2 的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码以指令该 UE1 或者 UE2 执行，本实施例对此不作任何限制。

- 30 需要说明的是，图 5 或图 6 所示的实施例以根据第一安全保护方法确定 PC5 连接的控制面使用的安全保护方法和/或 PC5 连接的用户面使用的安全保护方法为例进行说明。当然，本申请实施例也可以在 ProSe 发现流程中获取 PC5 连接的控制面使用的安全保护方法和/或 PC5 连接的用户面使用的安全保护方法，从而 PC5 建立流程不需要协商 PC5 连接的控制面使用的安全保护方法，也不需要协商 PC5 连接的用户面使用的安全保护方法，从而可以节省 PC5 建立流程的信令开销。进一步的，当 ProSe 发现流程中获取的 PC5 连接的控制面使用的安全保护方法包括控制面完整性保护开启时，由于可以对 PC5 建立流程中的所有消息进行完整性保护，因此可以避免 PC5 建立流程中的消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

35 本申请实施例还提供一种通信方法，该通信方法用于获取图 4 至图 6 任一实施例中的第一安全保护方法。可选的，通过该通信方法还可以获取 PC5 连接的控制面使用

的安全保护方法和/或 PC5 连接的用户面使用的安全保护方法。示例性的,如图 7 所示,该通信方法包括如下步骤:

S701、终端设备 1 向 DDNMF1 网元发送发现请求 (discovery request)。相应的, DDNMF1 网元接收来自终端设备 1 的发现请求。

5 其中,该发现请求包括终端设备 1 的 3GPP 身份信息、用于 ProSe 业务的身份信息、发现模式 (discovery mode)、发现命令 (discovery command)、发现类型 (discovery type) 和应用标识 (application ID) 中的一个或多个。发现类型、发现模式、发现命令或者用于 ProSe 业务的身份信息的相关描述可参考具体实施方式前序介绍部分,在此不再赘述。

10 示例性的,本申请实施例中的终端设备 1 可以为 model A 发现模式下的播报方 UE (announcing UE),下述的终端设备 2 可以为 model A 发现模式下的监听方 UE (monitoring UE);或者,本申请实施例中的终端设备 1 可以为 model B 发现模式下的被发现者 UE (discoveree UE),下述的终端设备 2 可以为 model B 发现模式下的发现者 UE (discoverer UE),在此统一说明,以下不再赘述。

15 一种可能的实现方式中,本申请实施例中,终端设备 1 可以通过控制面的非接入层 (non access stratum, NAS) 消息向 DDNMF1 网元发送发现请求,即此时发现请求本身就是一条 NAS 消息,或者是被 NAS 消息承载的一种实现发现请求的功能的参数;另一种可能的实现方式中,终端设备 1 可以通过用户面向 DDNMF1 网元发送,即此时发现请求是被互联网协议 (internet protocol, IP) 或者非 IP 承载的,本申请实施例对发现请求的发送方式不做具体限定。

20 可选的,本申请实施例中,终端设备 1 的 3GPP 身份信息例如可以为签约隐藏标识 (subscription concealed identifier, SUCI)、5G-全球唯一临时标识 (global unique temporary identifier, GUTI)、通用公共用户标识符 (generic public subscription identifier, GPSI)、永久设备标识符 (permanent equipment identifier, PEI) 中的一个。若终端设备 1 通过控制面流程接入 DDNMF1 网元,则可以使用 SUCI 或者 5G-GUTI 等身份信息作为终端设备 1 的 3GPP 身份信息;若终端设备 1 通过用户面流程接入 DDNMF1 网元,则可以使用 GPSI 或 PEI 等身份信息作为终端设备 1 的 3GPP 身份信息。在此统一说明,以下不再赘述。

30 可选的,本申请实施例中的应用标识用于表示某个特定的应用。其中,应用标识可以是预配置在终端设备 1 上的。一种可能的实现方式中,本申请实施例中,DDNMF1 网元根据应用标识可以确定对应的用于 ProSe 业务的身份信息。示例性的,假设一个应用标识对应的发现类型是固定的,即一个应用标识对应一种发现类型 (比如是 open discovery 还是 restricted discovery),则由于发现类型可以对应用于 ProSe 业务的 user identity (比如 ProSe application ID 用于开放发现场景;PDUID 或 RPAUID 用于限制发现场景),因此根据应用标识可以间接确定出对应的用于 ProSe 业务的身份信息。

35 可选的,本申请实施例中的发现请求还可以包括服务类型 (service type)。该服务类型是应用标识下一个更细的粒度,即一个应用标识可以对应不同的服务类型。其中,该服务类型用于辅助应用标识确定对应的用于 ProSe 业务的身份信息。也就是说,本申请实施例中,DDNMF1 网元根据应用标识和服务类型可以确定对应的用于 ProSe

业务的身份信息。

可选的，本申请实施例中的服务类型可以用于表征应用标识所标识的应用下的具体业务需求。比如服务类型用来表示一个应用下的收费业务或者免费业务。其中，本申请实施例通过引入服务类型可以提升应用使用的灵活性。

- 5 可选的，本申请实施例中的服务类型的内容可以根据表示的不同信息有不同的存储或者传递方法。比如，用 0 或者 1 代表是收费的还是免费的业务，本申请实施例对此不做具体限定。

- 10 可选的，本申请实施例中的服务类型可以是在安装应用标识所标识的应用时配置在终端设备 1 上的，也可以是网络侧发送给终端设备 1 的，本申请实施例对此不做具体限定。

- 需要说明的是，本申请实施例中，发现请求在终端设备 1 与 DDNMF1 网元之间传递时，可能经过其他网元的转发与处理。也就是说，发现请求在终端设备 1 与 DDNMF1 网元之间传递时，消息的内容可以做适当的变形，本申请实施例仅是从功能方面对消息进行描述，在此统一说明，以下不再赘述。比如，终端设备 1 在通过控制面向 DDNMF1 网元发送发现请求的过程中，终端设备 1 的 3GPP 身份信息需要经过 AMF 网元或者其他网元的“翻译”转化为终端设备 1 的签约永久标识(subscription permanent identifier, SUPI)。或者，终端设备 1 在通过用户面向 DDNMF1 网元发送发现请求的过程中，终端设备 1 的 3GPP 身份信息可能经过 NEF 网元或者其他网元的“翻译”转化为终端设备 1 的 SUPI。当然，若 DDNMF1 网元获取到的终端设备 1 的 3GPP 身份信息中不包括 SUPI，DDNMF1 网元还可以通过与 UDM 网元(或者其他网元)的交互获取终端设备 1 的 SUPI。示例性的，DDNMF1 网元向 UDM 网元发送 UE ID 请求(UE ID request)消息，该 UE ID 请求消息包括终端设备 1 的 3GPP 身份信息(比如 GPSI 或 PEI)。UDM 网元接收来自 DDNMF1 网元的 UE ID 请求消息，并根据终端设备 1 的 3GPP 身份信息确定终端设备 1 的 SUPI 之后，向 DDNMF1 网元发送终端设备 1 的 SUPI。

- 25 S702、DDNMF1 网元根据用于 ProSe 业务的身份信息和应用标识对终端设备 1 进行 ProSe 业务发现授权检查。

- 可选的，本申请实施例中，DDNMF1 网元可以根据应用标识确定对应的邻近业务应用服务器(ProSe app server)并由 ProSe app server 完成授权检查后通知给 DDNMF1 网元。本申请实施例中，ProSe app server 授权检查用于验证终端设备 1 是否可以合法使用该 ProSe 业务，在此统一说明，以下不再赘述。

- 30 可选的，本申请实施例中，若终端设备 1 携带了多个用于 ProSe 业务的身份信息，则根据上面的描述，DDNMF1 网元要根据各个用于 ProSe 业务的身份信息，分别对终端设备 1 进行 ProSe 业务发现授权检查，上述多个授权可分别在独立流程中进行，也可在统一的流程中进行，在此统一说明，以下不再赘述。

- 35 S703、DDNMF1 网元获取终端设备 1 使用 ProSe 业务时对应的发现参数以及安全信息。

本申请实施例中，DDNMF1 网元可以根据终端设备 1 的 3GPP 身份信息和用于 ProSe 业务的身份信息，获取终端设备 1 使用 ProSe 业务时对应的发现参数以及安全信息。其中，DDNMF 网元获取终端设备 1 使用 ProSe 业务时对应的发现参数与安全信

息的方式包括：发现参数与安全信息均从 DDNMF1 网元本地获取；或者，发现参数与安全信息中的部分内容从 DDNMF1 网元本地获取，部分内容从 ProSe 业务发现授权检查流程中 ProSe app server 回复的认证响应（authentication request）中获取；或者，发现参数与安全信息均从 ProSe 业务发现授权检查流程中 ProSe app server 回复的认证响应中获取，本申请实施例对此不做具体限定。

5 本申请实施例中，在 restricted discovery 的发现场景下，终端设备 1 的发现参数例如可以如表一所示：

表一

	Model A	Model B
ProSe 发现使用的 code	ProSe Code	ProSe Response Code
发现参数 container	Code-Send-SecParams	Code-Send-SecParams Code-Rcv-SecParams
发现时间限制参数	CURRENT_TIME, MAX_OFFSET	

其中，在 Model A 模式下，Code-Send-SecParams 包含用来在 PC5 接口上的发现流程中保护 Prose Restricted Code 所用的发现参数；在 Model B 模式下，Code-Send-SecParams 用来在 PC5 接口上的发现流程中保护 ProSe Response Code 所用的发现参数，Code-Rcv-SecParams 包含用来在 PC5 接口上的发现流程中获取对端发来的 ProSe 发现使用的 code 所用的发现参数。表一中发现参数的相关描述可参考现有的 3GPP TS 23.303, v15.1.0 和 3GPP TS 33.303, v15.0.0 标准，在此不予赘述。

15 本申请实施例中，在 open discovery 的发现场景下，终端设备 1 的发现参数例如可以如表二所示：

表二

	Model A
ProSe 发现使用的 code	ProSe Application Code
发现参数	Discovery Key
发现时间限制参数	CURRENT_TIME, MAX_OFFSET

其中，Discovery Key 包含用来在发现流程中保护 ProSe Application Code 所用的发现参数，即上述发现参数用于在 PC5 接口上保护 ProSe 发现使用的 Code。表二中发现参数的相关描述可参考现有的 3GPP TS 23.303, v15.1.0 和 3GPP TS 33.303, v15.0.0 标准，在此不予赘述。

可选的，本申请实施例中，终端设备 1 使用 ProSe 业务时对应的安全信息包括终端设备 1 使用 ProSe 业务时所需的安全保护方法，或者终端设备 1 使用 ProSe 业务时对应的多个可供选择的安全保护方法。

25 其中，本申请实施例中，终端设备 1 使用 ProSe 业务时所需的安全保护方法为固定的安全保护方法。可选的，该安全保护方法可以用于对后续第一条 PC5 广播消息进行安全保护；和/或，该安全保护方法可以用于对 PC5 建立流程中的一条或多条消息进行安全保护；和/或，该安全保护方法可以用于确定终端设备 1 与终端设备 2 之间的 PC5 连接的安全保护方法。其中，PC5 连接的安全保护方法用于对 PC5 连接的控制面信令中传递的部分或全部参数进行安全保护；和/或，PC5 连接的安全保护方法用于对 PC5

连接的部分或全部用户面数据进行安全保护。示例性的，该安全保护方法用于对 PC5 建立流程中的一条或多条消息进行安全保护；和/或，该安全保护方法用于确定终端设备 1 与终端设备 2 之间的 PC5 连接的安全保护方法的示例可参考图 4 至图 6 所示的任一实施例，在此不再赘述。其中，第一条 PC5 广播消息的相关描述可参考具体实施方式前序部分，在此不再赘述。

可选的，本申请实施例中，终端设备 1 使用 ProSe 业务时所需的安全保护方法可以为多个安全保护方法。比如，一个安全保护方法为第一条 PC5 广播消息使用的安全保护方法；一个安全保护方法为 PC5 连接的控制面使用的安全保护方法；一个安全保护方法为 PC5 连接的用户面使用的安全保护方法。其中，第一条 PC5 广播消息使用的安全保护方法、PC5 连接的控制面使用的安全保护方法以及 PC5 连接的用户面使用的安全保护方法可以相同，也可以不相同，本申请实施例对此不作具体限定。

示例性的，本申请实施例中，终端设备 1 使用 ProSe 业务时所需的安全保护方法例如可以包括以下任意一个：机密性保护开启+完整性保护开启，机密性保护开启+完整性保护不开启，机密性保护不开启+完整性保护开启，或者，机密性保护不开启+完整性保护不开启。其中，默认该待使用的安全保护方法至少可用于对后续第一条 PC5 广播消息进行安全保护。

或者，示例性的，本申请实施例中，终端设备 1 使用 ProSe 业务时所需的安全保护方法例如可以包括：

第一条 PC5 广播消息所使用的安全保护方法为：机密性保护不开启+完整性保护开启；PC5 连接的控制面使用的安全保护方法为：机密性保护开启+完整性保护开启；以及，PC5 连接的用户面使用的安全保护方法为：机密性保护开启+完整性保护开启。其中，第一条 PC5 广播消息所使用的安全保护方法、PC5 连接的控制面使用的安全保护方法与 PC5 连接的用户面使用的安全保护方法均不相同。

或者，示例性的，本申请实施例中，终端设备 1 使用 ProSe 业务时所需的安全保护方法例如可以包括：

第一条 PC5 广播消息所使用的安全保护方法以及 PC5 连接的控制面使用的安全保护方法为：机密性保护不开启+完整性保护开启；PC5 连接的用户面使用的安全保护方法为：机密性保护开启+完整性保护开启。

或者，示例性的，本申请实施例中，终端设备 1 使用 ProSe 业务时所需的安全保护方法例如可以包括：

第一条 PC5 广播消息所使用的安全保护方法为：机密性保护不开启+完整性保护开启；以及，PC5 连接的控制面使用的安全保护方法为：机密性保护开启+完整性保护开启。

或者，示例性的，本申请实施例中，终端设备 1 使用 ProSe 业务时所需的安全保护方法例如可以包括：

第一条 PC5 广播消息所使用的安全保护方法为：机密性保护不开启+完整性保护开启；以及，PC5 连接的用户面使用的安全保护方法为：机密性保护开启+完整性保护开启。

其中，本申请实施例中，多个可供选择的安全保护方法例如可以是 ProSe app server

推荐的安全策略对应的安全保护方法。进一步的，多个可供选择的安全保护方法可以有优先级排序。

- 5 示例性的，有优先级排序的多个可供选择的安全保护方法例如可以包括：机密性保护不开启+完整性保护开启>机密性保护开启+完整性保护开启>机密性保护不开启+完整性保护不开启。其中，这里的“>”可以理解为“安全等级高于”，在此统一说明，以下不再赘述。

可选的，本申请实施例中，对于不同的发现模式，比如上述 Model A 或 Model B，可以分别采用不同的安全信息，也可以采用相同的安全信息，本申请实施例对此不做具体限定。

- 10 可选的，本申请实施例中的安全信息也可以与表一或表二中的 ProSe 发现使用的 code 相关联，即不同的 ProSe 发现使用的 code，可以对应不同的安全信息，也可以采用相同的安全信息，本申请实施例对此不做具体限定。

需要说明的是，本申请实施例中的安全信息可能包含在发现参数中，本申请实施例对此不做具体限定。

- 15 进一步的，当本申请实施例中的终端设备 1 使用 ProSe 业务时对应的安全信息包括终端设备 1 使用 ProSe 业务时对应的多个可供选择的安全保护方法时，则需要继续执行下述步骤 S704 之后再执行步骤 S705；当本申请实施例中的终端设备 1 使用 ProSe 业务时对应的安全信息包括终端设备 1 使用 ProSe 业务时所需的安全保护方法时，则直接执行步骤 S705，不需要执行步骤 S704。

- 20 S704、DDNMF1 网元根据多个可供选择的安全保护方法，确定终端设备 1 使用 ProSe 业务时所需的安全保护方法。

可选的，本申请实施例中，DDNMF1 网元可以根据终端的设备 1 的状态、终端设备 1 的类型以及当前业务的服务质量（quality of service, QoS）要求等参数，从多个可供选择的安全保护方法中选择终端设备 1 使用 ProSe 业务时所需的安全保护方法。

- 25 示例性的，若是一个低时延的业务，则 DDNMF1 网元可以将安全等级最低的安全保护方法确定为终端设备 1 使用 ProSe 业务时所需的安全保护方法。或者，比如，若是一个高可靠的业务，则 DDNMF1 网元可以将安全等级最高的安全保护方法确定为终端设备 1 使用 ProSe 业务时所需的安全保护方法。

- 30 当然，本申请实施例中，DDNMF1 网元也可以将多个可供选择的安全保护方法中安全等级最高的安全保护方法直接确定为终端设备 1 使用 ProSe 业务时所需的安全保护方法，本申请实施例对此不作具体限定。

S705、DDNMF1 网元向终端设备 1 发送发现响应（discovery response）。相应的，终端设备 1 接收来自 DDNMF1 网元的发现响应。其中，该发现响应包括终端设备 1 使用 ProSe 业务时对应的发现参数和所需的安全保护方法。

- 35 需要说明的是，本申请实施例中，终端设备 1 使用 ProSe 业务时所需的安全保护方法可能包含在发现参数中，本申请实施例对此不做具体限定。

综上，通过步骤 S701-S705，终端设备 1 可以获取终端设备 1 使用 ProSe 业务时对应的发现参数和所需的安全保护方法。

S706、终端设备 2 向 DDNMF2 网元发送发现请求。相应的，DDNMF2 网元接收

来自终端设备 2 的发现请求。

S707、DDNMF2 网元根据用于 ProSe 业务的身份信息和应用标识对终端设备 2 进行 ProSe 业务发现授权检查。

S708、DDNMF2 网元获取终端设备 2 使用 ProSe 业务时对应的发现参数以及安全信息。

进一步的，当本申请实施例中的终端设备 2 使用 ProSe 业务时对应的安全信息包括终端设备 2 使用 ProSe 业务时对应的多个可供选择的安全保护方法时，则需要继续执行下述步骤 S709 之后再执行步骤 S710；当本申请实施例中的终端设备 2 使用 ProSe 业务时对应的安全信息包括终端设备 2 使用 ProSe 业务时所需的安全保护方法时，则直接执行步骤 S710，不需要执行步骤 S709。

S709、DDNMF2 网元根据多个可供选择的安全保护方法，确定终端设备 2 使用 ProSe 业务时所需的安全保护方法。

S710、DDNMF2 网元向终端设备 2 发送发现响应。相应的，终端设备 2 接收来自 DDNMF2 网元的发现响应。其中，该发现响应包括终端设备 2 使用 ProSe 业务时对应的发现参数和所需的安全保护方法。

本申请实施例中，在 restricted discovery 的发现场景下，终端设备 2 的发现参数例如可以如表三所示：

表三

	Model A	Model B
ProSe 发现使用的 code	Prose Restricted Code	ProSe Query Code
发现参数 container	Code-Rcv-SecParams	Code-Send-SecParams Code-Rcv-SecParams
发现时间限制参数	CURRENT_TIME, MAX_OFFSET	

其中，在 Model A 模式下，Code-Rcv-SecParams 包含用来在 PC5 接口上的发现流程中保护 Prose Restricted Code 所用的发现参数；在 Model B 模式下，Code-Send-SecParams 包含用来在 PC5 接口上的发现流程中保护 ProSe Query Code 所用的发现参数，Code-Rcv-SecParams 包含用来在 PC5 接口上的发现流程中获取对端发来的 ProSe 发现使用的 code 所用的发现参数。即上述发现参数用于在 PC5 接口上保护 ProSe 发现使用的 Code。表三中发现参数的相关描述可参考现有的 3GPP TS 23.303，v15.1.0 和 3GPP TS 33.303，v15.0.0 标准，在此不予赘述。

本申请实施例中，在 open discovery 的发现场景下，终端设备 2 的发现参数例如可以如表四所示：

表四

	Model A
ProSe 发现使用的 code	ProSe Application Code
发现时间限制参数	CURRENT_TIME, MAX_OFFSET

需要说明的是，open discovery 的发现场景下，终端设备 2 不需要对应的 discovery key，解密依靠匹配上报（match report）流程。也就是说，此时终端设备 2 不存在对应的发现参数。相关描述可参考现有的 3GPP TS 23.303，v15.1.0 和 3GPP TS 33.303，

v15.0.0 标准，在此不予赘述。

其中，上述步骤 S706-S710 的具体实现可参考上述步骤 S701-S705，区别比如在于：将步骤 S701-S705 中的终端设备 1 替换为步骤 S706-S710 中的终端设备 2；将步骤 S701-S705 中的 DDNMF1 网元替换为步骤 S706-S710 中的 DDNMF2 网元等，其余相关描述可参考上述步骤 S701-S705，在此不再赘述。

综上，通过步骤 S706-S710，终端设备 2 可以获取终端设备 2 使用 ProSe 业务时对应的发现参数和所需的安全保护方法。

需要说明的是，步骤 S706-S710 以 DDNMF2 网元自己确定使用 ProSe 业务时所需的安全保护方法为例进行说明。可选的，本申请实施例中，DDNMF2 网元还可以通过与 DDNMF1 网元的协商确定使用 ProSe 业务时所需的安全保护方法。

一种可能的实现方式中，DDNMF2 网元从 DDNMF1 网元获取终端设备 1 使用该 ProSe 业务时所需的安全保护方法；进一步的，DDNMF2 网元根据终端设备 2 使用 ProSe 业务时对应的多个可供选择的安全保护方法和终端设备 1 使用所述 ProSe 业务时所需的安全保护方法确定终端设备 2 使用所述 ProSe 业务时所需的安全保护方法。例如，DDNMF2 网元确定终端设备 2 使用 ProSe 业务时对应的多个可供选择的安全保护方法中是否包括终端设备 1 使用该 ProSe 业务时所需的安全保护方法；当终端设备 2 使用 ProSe 业务时对应的多个可供选择的安全保护方法中包括终端设备 1 使用该 ProSe 业务时所需的安全保护方法时，DDNMF2 网元将终端设备 1 使用该 ProSe 业务时所需的安全保护方法确定为终端设备 2 使用该 ProSe 业务时所需的安全保护方法。再例如，当终端设备 2 使用 ProSe 业务时对应的多个可供选择的安全保护方法中不包括终端设备 1 使用该 ProSe 业务时所需的安全保护方法时，DDNMF2 网元从终端设备 2 使用 ProSe 业务时对应的多个可供选择的安全保护方法中确定终端设备 2 使用该 ProSe 业务时所需的安全保护方法。比如，DDNMF2 网元获取的终端设备 2 使用 ProSe 业务时对应的多个可供选择的安全保护方法中包括完整性保护开启+机密性保护不开启、完整性保护开启+机密性保护开启，即只要完整性保护开启，机密性保护可以开启也可以不开启。假设终端设备 1 使用该 ProSe 业务时所需的安全保护方法包括完整性保护开启+机密性保护不开启，或者终端设备 1 使用该 ProSe 业务时所需的安全保护方法包括完整性保护开启+机密性保护开启，则 DDNMF2 网元可以确定终端设备 1 使用该 ProSe 业务时所需的安全保护方法即为终端设备 2 使用该 ProSe 业务时所需的安全保护方法。

另一种可能的实现方式中，DDNMF2 网元从 DDNMF1 网元获取终端设备 1 使用该 ProSe 业务时所需的安全保护方法；进一步的，在 DDNMF2 网元确定终端设备 2 使用该 ProSe 业务时所需的安全保护方法之后，可以进一步确定终端设备 1 使用该 ProSe 业务时所需的安全保护方法与终端设备 2 使用该 ProSe 业务时所需的安全保护方法是否相同，若相同，DDNMF 网元可以继续执行步骤 S710；若不相同，则 DDNMF2 网元可以将终端设备 1 使用该 ProSe 业务时所需的安全保护方法确定为最终终端设备 2 使用该 ProSe 业务时所需的安全保护方法，并在步骤 S710 中携带该终端设备 2 使用该 ProSe 业务时所需的安全保护方法，本申请实施例对此不作具体限定。

需要说明的是，当终端设备 1 或终端设备 2 需要获取多个 ProSe 发现使用的 code 对应的安全保护方法时，DDNMF2 网元从 DDNMF1 网元获取终端设备 1 使用该 ProSe

业务时所需的安全保护方法之后，若终端设备 1 使用该 ProSe 业务时所需的安全保护方法中包括多个 ProSe 发现使用的 code 对应的安全保护方法，则 DDNMF2 网元确定终端设备 2 使用 ProSe 业务时对应的多个可供选择的安全保护方法中是否存在某个 ProSe 发现使用的 code 对应的安全保护方法与终端设备 1 使用该 ProSe 业务时所需的安全保护方法中相同 ProSe 发现使用的 code 对应的安全保护方法相同，若存在，则 DDNMF2 网元可以进一步执行步骤 S710，并在步骤 S710 中携带该 ProSe 发现使用的 code 对应的安全保护方法，在此统一说明，以下不再赘述。

可选的，本申请实施例中，DDNMF2 网元从 DDNMF1 网元获取终端设备 1 使用 ProSe 业务时所需的安全保护方法，可以包括：DDNMF2 网元向 DDNMF1 网元发送请求消息，该请求消息用于请求终端设备 1 使用 ProSe 业务时所需的安全保护方法。其中，该请求消息包括终端设备 2 发送的用于 ProSe 业务的身份信息，或者可以关联到终端设备 1 发送的用于 ProSe 业务的身份信息的信息，或者可以关联到目标应用的信息。进而，DDNMF2 网元接收来自 DDNMF1 网元的终端设备 1 使用 ProSe 业务时所需的安全保护方法。

可选的，本申请实施例中，DDNMF2 网元可以使用现有技术确定是否从 DDNMF1 网元获取终端设备 1 使用 ProSe 业务时所需的安全保护方法，本申请实施例对此不做具体限定。

需要说明的是，本申请实施例以终端设备 1 发送的用于 ProSe 业务的身份信息与终端设备 2 发送的用于 ProSe 业务的身份信息相同为例进行说明，在此统一说明，以下不再赘述。当然，本申请实施例中，终端设备 1 发送的用于 ProSe 业务的身份信息与终端设备 2 发送的用于 ProSe 业务的身份信息也可以不相同。此时，DDNMF1 网元/DDNMF2 网元可以根据终端设备 2 发送的用于 ProSe 业务的身份信息、以及终端设备 1 发送的用于 ProSe 业务的身份信息确定待使用的安全保护方法。比如，DDNMF1 网元/DDNMF2 网元可以关联终端设备 2 发送的用于 ProSe 业务的身份信息、以及终端设备 1 发送的用于 ProSe 业务的身份信息。比如可以通过应用 ID 关联，本申请实施例对此不做具体限定。

可选的，本申请实施例提供的通信方法还包括如下发现广播流程。

以 Model A 发现场景为例，则本申请实施例提供的通信方法还可以包括如下步骤 S711-S712：

S711、终端设备 1 向终端设备 2 发送广播（announcing）消息。相应的，终端设备 2 接收来自终端设备 1 的广播消息。其中，该广播消息使用步骤 S705 中获取的终端设备 1 使用 ProSe 业务时所需的安全保护方法进行安全保护。

可选的，本申请实施例中，该广播消息中可以包括对该广播消息进行安全保护的安全保护方法，从而使得使用这种安全保护方法的终端设备 2 可以接收该广播消息。

其中，对该广播消息进行安全保护的安全保护方法可以隐式携带在该广播消息中，也可以显示携带在该广播消息中，本申请实施例对此不做具体限定。

示例性的，隐士的方式比如不同的 ProSe 发现使用的 code 代表不同的安全保护方法。即 DDNMF1 网元可以发送多个 ProSe 发现使用的 code 给 announcing UE，不同的 ProSe 发现使用的 code 对应不同的安全保护方法。进一步的，终端设备 2 接收广播消

息之后，可以根据 ProSe 发现使用的 code 确定对应的安全保护方法。

或者，示例性的，显示的方式比如在广播消息中携带安全指示信息，该安全指示信息用于指示该广播消息使用的安全保护方法。比如，安全指示信息是 2 个 bit，0 代表安全没有开启，1 代表安全开启。比如，00 代表机密性保护未开启且完整性保护未开启，10 代表机密性保护开启，但是完整性保护未开启，01 代表机密性保护未开启，但是完整性保护没有开启，11 代表机密性保护未开启且完整性保护未开启。进一步的，终端设备 2 接收广播消息之后，可以根据安全指示信息确定对应的安全保护方法。

S712、终端设备 2 验证广播消息。

步骤 S712 可参考现有的实现方式，在此不再赘述。

10 示例性的，假设终端设备 2 接收到的 DDNMF2 网元发送的终端设备 2 使用 ProSe 业务时所需的安全保护方法为：机密性保护开启+完整性保护不开启，但是终端设备 2 接收到的广播消息指示的该广播消息使用的安全保护方法为：机密性保护开启+完整性保护开启，则即使终端设备 2 与终端设备 1 对相同的应用感兴趣，也不能建立后续的 PC5 连接。换言之，终端设备 1 与终端设备 2 之间仅是因为安全要求不匹配而不能建立 PC5 连接。

或者，示例性的，假设终端设备 2 接收到的广播消息指示的该广播消息使用的安全保护方法为：机密性保护开启+完整性保护开启，终端设备 2 接收到的 DDNMF2 网元发送的终端设备 2 使用 ProSe 业务时所需的安全保护方法中包括：机密性保护开启+完整性保护开启，则终端设备 2 可以确定对终端设备 1 的应用建立 PC5 连接。

20 可选的，以 Model B 发现场景为例，则本申请实施例提供的通信方法还可以包括如下步骤 S713-S716：

S713、终端设备 2 向终端设备 1 发送请求代码 (Send Query Code) 消息。相应的，终端设备 1 接收来自终端设备 2 的发送请求代码消息。

25 其中，该请求代码消息使用步骤 S710 中获取的终端设备 2 使用 ProSe 业务时所需的安全保护方法进行安全保护。

30 可选的，本申请实施例中，该请求代码消息中可以包括对该请求代码消息进行安全保护的安全保护方法，从而使得使用这种安全保护方法的终端设备 1 可以接收该请求代码消息。其中，对该请求代码消息进行安全保护的安全保护方法可以隐式携带在该请求代码消息中，也可以显示携带在该请求代码消息中，本申请实施例对此不做具体限定。

示例性的，隐士的方式比如不同的 ProSe 发现使用的 code 代表不同的安全保护方法。即 DDNMF2 网元可以发送多个 ProSe 发现使用的 code 给 discoverer UE，不同的 ProSe 发现使用的 code 对应不同的安全保护方法。进一步的，终端设备 1 接收请求代码消息之后，可以根据 ProSe 发现使用的 code 确定对应的安全保护方法。

35 或者，示例性的，显示的方式比如在请求代码消息中携带安全指示信息，该安全指示信息用于指示该请求代码消息使用的安全保护方法。比如，安全指示信息是 2 个 bit，0 代表安全没有开启，1 代表安全开启。比如，00 代表机密性保护未开启且完整性保护未开启，10 代表机密性保护开启，但是完整性保护未开启，01 代表机密性保护未开启，但是完整性保护没有开启，11 代表机密性保护未开启且完整性保护未开启。

进一步的，终端设备 1 接收请求代码消息之后，可以根据安全指示信息确定对应的安全保护方法。

S714、终端设备 1 验证发送请求代码消息。

步骤 S417 可参考现有的实现方式，在此不再赘述。

- 5 示例性的，假设终端设备 1 接收到的 DDNMF1 网元发送的终端设备 1 使用 ProSe 业务时所需的安全保护方法为：机密性保护开启+完整性保护不开启，但是终端设备 1 接收到的请求代码消息指示的该请求代码消息使用的安全保护方法为：机密性保护开启+完整性保护开启，则即使终端设备 2 与终端设备 1 对相同的应用感兴趣，也不能建立后续的 PC5 连接。换言之，终端设备 1 与终端设备 2 之间仅是因为安全要求不匹配
10 而不能建立 PC5 连接。

可选的，本申请实施例中，终端设备 1 验证发送请求代码消息准确后，还可以继续执行下述步骤 S715。

S715、终端设备 1 向终端设备 2 发送响应代码（Send response Code）消息。相应的，终端设备 2 接收来自终端设备 1 的发送响应代码消息。

- 15 S716、终端设备 2 验证发送响应代码消息。

可选的，本申请实施例中，在 Model A 或者 Model B 上述流程结束之后，还可能包括发现匹配上报（match report）流程，具体可参考现有的 3GPP TS 23.303，v15.1.0 和 3GPP TS 33.303，v15.0.0 标准，在此不予赘述。

- 20 基于本申请实施例提供的通信方法，可以在 ProSe 发现流程中获取终端设备使用 ProSe 业务时所需的安全保护方法。可选的，通过该通信方法还可以获取 PC5 连接的控制面使用的安全保护方法和/或 PC5 连接的用户面使用的安全保护方法。

- 其中，上述步骤 S701 至 S716 中 DDNMF1 网元、DDNMF2 网元、终端设备 1 或者终端设备 2 的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码以指令该 DDNMF1 网元、DDNMF2 网元、终端设备 1 或者终端设备 2 执行，本实施例对此不作任何限制。
25

- 需要说明的是，本申请实施例图 4 至图 6 所示的 PC5 建立流程可以使用通过上述图 7 所示的实施例获取的终端设备使用 ProSe 业务时所需的安全保护方法，即图 4 至图 6 所示的 PC5 建立流程中的第一安全保护方法可以为图 7 所示的实施例中终端设备 1 或者终端设备 2 获取的使用 ProSe 业务时所需的安全保护方法。当然，本申请实施例图 4 至图 6 所示的 PC5 建立流程可以使用通过其他方式在 ProSe 发现流程中获取的安全保护方法，本申请实施例对此不做具体限定。
30

- 可选的，本申请实施例中，若图 7 所示的终端设备 1 与终端设备 2 获取到的使用 ProSe 业务时所需的安全保护方法包括完整性保护开启，则可以通过图 7 所示的实施例中的第一条 PC5 广播消息携带图 4 或图 5 或图 6 所示的实施例中直连通信请求传输的参数，此时可以不用执行 UE1 向 UE2 发送直连通信请求的步骤（如图 4 中的步骤 S402、图 5 中的步骤 S501 或者图 6 中的步骤 S601），从而可以进一步节省信令开销，在此统一说明，以下不再赘述。
35

如图 8 所示，为本申请实施例提供的一种通信方法，包括如下步骤：

S801、第一终端设备获取第一安全保护方法，该第一安全保护方法为第一终端设

备与第二终端设备之间的发现流程中确定的安全保护方法。

其中，步骤 S801 的具体实现可参考图 7 所示的实施例，在此不再赘述。

需要说明的是，本申请实施例中的第一终端设备可以为图 7 所示的实施例中的终端设备 1，第二终端设备可以为图 7 所示的实施例中的终端设备 2；或者，本申请实施例中的第一终端设备可以为图 7 所示的实施例中的终端设备 2，第二终端设备可以为图 7 所示的实施例中的终端设备 1，在此统一说明，以下不再赘述。

S802、第一终端设备根据第一安全保护方法确定第二安全保护方法，第二安全保护方法为第一终端设备与第二终端设备之间的 PC5 连接的安全保护方法。

其中，步骤 S802 的具体实现可参考图 5 所示的实施例中的步骤 S502 与步骤 S506；或者，步骤 S802 的具体实现可参考图 6 所示的实施例中的步骤 S602，在此不再赘述。

需要说明的是，本申请实施例中，第一终端设备可以为图 5 或图 6 所示的实施例中的 UE2，第二终端设备可以为图 5 或图 6 所示的实施例中的 UE1，在此统一说明，以下不再赘述。

由于本申请实施例在确定第二安全保护方法时，可以参考发现流程中确定的第一安全保护方法，因此可以使得确定的第二安全保护方法的安全等级不低于第一安全保护方法的安全等级。也就是说，第一安全保护方法的安全等级是 PC5 建立流程中 PC5 连接的最低安全等级，这样可以达到安全不降级的目的。

其中，上述步骤 S801 至 S802 中第一终端设备的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码以指令该第一终端设备执行，本实施例对此不作任何限制。

如图 9 所示，为本申请实施例提供一种通信方法，包括如下步骤：

S901、第一终端设备获取第一安全保护方法，第一安全保护方法为第一终端设备与第二终端设备之间的发现流程中确定的安全保护方法。

其中，步骤 S801 的具体实现可参考图 7 所示的实施例，在此不再赘述。

需要说明的是，本申请实施例中的第一终端设备可以为图 7 所示的实施例中的终端设备 1，第二终端设备可以为图 7 所示的实施例中的终端设备 2；或者，本申请实施例中的第一终端设备可以为图 7 所示的实施例中的终端设备 2，第二终端设备可以为图 7 所示的实施例中的终端设备 1，在此统一说明，以下不再赘述。

S902、第一终端设备使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护，并向第二终端设备发送安全保护后的至少一条消息。

其中，步骤 S902 的具体实现可参考图 4 所示的实施例中的步骤 S402、步骤 S405、步骤 S407 与步骤 S409；或者，步骤 S902 的具体实现可参考图 5 所示的实施例中的步骤 S501、步骤 S503、步骤 S505 与步骤 S507；或者，步骤 S902 的具体实现可参考图 6 所示的实施例中的步骤 S601 与步骤 S604，在此不再赘述。

需要说明的是，本申请实施例中，第一终端设备可以为图 4 或图 5 或图 6 所示的实施例中的 UE2，第二终端设备可以为图 4 或图 5 或图 6 所示的实施例中的 UE1；或者，本申请实施例中，第一终端设备可以为图 4 或图 5 或图 6 所示的实施例中的 UE1，第二终端设备可以为图 4 或图 5 或图 6 所示的实施例中的 UE2，在此统一说明，以下

不再赘述。

基于本申请实施例提供的通信系统，一方面，在第一安全保护方法包括完整性保护开启的情况下，由于第一终端设备可以使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护，因此可以避免 PC5 建立流程中的消息被攻击者攻击或篡改所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。另一方面，在第一安全保护方法的安全等级高于或者等于第一终端设备与第二终端设备之间的 PC5 连接的控制面使用的安全保护方法的安全等级的情况下，由于第一终端设备可以使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护，因此可以避免 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的安全等级所造成的安全等级降低的问题，提高了 PC5 建立流程的安全等级。

其中，上述步骤 S901 至 S902 中第一终端设备的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码以指令该第一终端设备执行，本实施例对此不作任何限制。

如图 10 所示，为本申请实施例提供的一种通信方法，包括如下步骤：

S1001、第一直连通信发现名称管理功能网元接收来自第一终端设备的第一信息和第一终端设备的 3GPP 身份信息，其中，第一信息包括用于 ProSe 业务的身份信息或者用于确定用于 ProSe 业务的身份信息的信息。

S1002、第一直连通信发现名称管理功能网元根据第一信息和第一终端设备的 3GPP 身份信息，确定第一终端设备使用所述 ProSe 业务时所需的安全保护方法。

S1003、第一直连通信发现名称管理功能网元向第一终端设备发送第一终端设备使用 ProSe 业务时所需的安全保护方法。

其中，图 10 所示的实施例的具体实现可参考图 7 所示的实施例，在此不再赘述。

需要说明的是，本申请实施例中，第一直连通信发现名称管理功能网元例如可以为图 7 中的 DDNMF1 网元，第一终端设备例如可以为图 7 中的终端设备 1，第二直连通信发现名称管理功能网元例如可以为图 7 中的 DDNMF2 网元，第二终端设备例如可以为图 4 中的终端设备 2；或者，本申请实施例中，第一直连通信发现名称管理功能网元例如可以为图 7 中的 DDNMF2 网元，第一终端设备例如可以为图 7 中的终端设备 2，第二直连通信发现名称管理功能网元例如可以为图 7 中的 DDNMF1 网元，第二终端设备例如可以为图 7 中的终端设备 1，在此统一说明，以下不再赘述。

基于本申请实施例提供的通信方法，第一终端设备可以在第一终端设备与第二终端设备之间的发现流程中获取第一终端设备使用 ProSe 业务时所需的安全保护方法。

其中，上述步骤 S1001 至 S1003 中第一直连通信发现名称管理功能网元的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码以指令该第一终端设备第一直连通信发现名称管理功能网元执行，本实施例对此不作任何限制。

可以理解的是，图 4 至图 10 所示的实施例中，由第一终端设备（如图 4 至图 6 所示的实施例中的 UE1 或 UE2、或者如图 7 所示的实施例中的终端设备 1 或终端设备 2、或者如图 8 或图 9 所示的实施例中的第一终端设备）实现的方法和/或步骤，也可

可以由可用于第一终端设备的部件（例如芯片或者电路）实现；由第一直连通信发现名称管理功能网元（如图 7 所示的实施例中的 DDNMF1 网元或者 DDNMF 网元、或者如图 10 所示的实施例中的第一直连通信发现名称管理功能网元）实现的方法和/或步骤，也可以由可用于第一直连通信发现名称管理功能网元的部件（例如芯片或者电路）实现。

上述主要从各个网元之间交互的角度对本申请实施例提供的方案进行了介绍。相应的，本申请实施例还提供了通信装置，该通信装置可以为上述方法实施例中的第一终端设备，或者包含上述第一终端设备的装置，或者为可用于第一终端设备的部件；或者，该通信装置可以为上述方法实施例中的第一直连通信发现名称管理功能网元，或者包含上述第一直连通信发现名称管理功能网元的装置，或者为可用于第一直连通信发现名称管理功能网元的部件。可以理解的是，该通信装置为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，结合本文中公开的实施例描述的各示例的单元及算法步骤，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

图 11 示出了一种通信装置 110 的结构示意图。该通信装置 110 包括收发模块 1101 和处理模块 1102。所述收发模块 1101，也可以称为收发单元用以实现收发功能，例如可以是收发电路，收发机，收发器或者通信接口。

以通信装置 110 为上述方法实施例中的第一终端设备或者设置在该第一终端设备中的芯片或其他部件为例，一种可能的实现方式中：

处理模块 1102，用于获取第一安全保护方法，第一安全保护方法为第一终端设备与第二终端设备之间的发现流程中确定的安全保护方法。处理模块 1102，还用于根据第一安全保护方法确定第二安全保护方法，第二安全保护方法为第一终端设备与第二终端设备之间的 PC5 连接的安全保护方法。

可选的，第二安全保护方法的安全等级不低于第一安全保护方法的安全等级。

可选的，处理模块 1102，用于根据第一安全保护方法确定第二安全保护方法，包括：将第一安全保护方法确定为第二安全保护方法。

可选的，处理模块 1102，用于根据第一安全保护方法确定第二安全保护方法，包括：通过收发模块 1101 接收来自第二终端设备的第二安全策略，第二安全策略为第二终端设备在 PC5 连接中的安全策略；根据第二安全策略和第一安全保护方法，确定第二安全保护方法。

可选的，处理模块 1102，用于根据第二安全策略和第一安全保护方法，确定第二安全保护方法，包括：在第一安全保护方法满足第二安全策略的情况下，将第一安全保护方法确定为第二安全保护方法；或者，在第一安全保护方法满足第二安全策略的情况下，根据第二安全策略，选择安全等级不低于第一安全保护方法的安全保护方法作为第一安全保护方法；或者，在第一安全保护方法不满足第二安全策略的情况下，根据第二安全策略，选择一个满足第二安全策略的安全保护方法作为第二安全保护方

法。

可选的，第二安全策略包括第二控制面安全策略和/或第二用户面安全策略；其中，第二控制面安全策略为第二终端设备在 PC5 连接中的控制面安全策略，第二用户面安全策略为第二终端设备在 PC5 连接中的用户面安全策略。

- 5 可选的，第二安全保护方法用于对 PC5 连接的控制面信令中传递的部分或全部参数进行安全保护；和/或，第二安全保护方法用于对 PC5 连接的部分或全部用户面数据进行安全保护。

- 10 可选的，收发模块 1101，还用于接收来自第二终端设备的第一消息，第一消息为第一终端设备与第二终端设备之间的 PC5 建立流程中的第一条消息；处理模块 1102，还用于使用第一安全保护方法对第一消息进行安全保护。

可选的，处理模块 1102，用于获取第一安全保护方法，包括：通过收发模块 1101 向第一直连通信发现名称管理功能网元发送第一信息和第一终端设备的 3GPP 身份信息，第一信息包括用于 ProSe 业务的身份信息或者用于确定用于 ProSe 业务的身份信息的信息；

- 15 通过收发模块 1101 接收来自第一直连通信发现名称管理功能网元的第一安全保护方法。

或者，以通信装置 110 为上述方法实施例中的第一终端设备或者设置在该第一终端设备中的芯片或其他部件为例，另一种可能的实现方式中：

- 20 处理模块 1102，用于获取第一安全保护方法，第一安全保护方法为第一终端设备与第二终端设备之间的发现流程中确定的安全保护方法。处理模块 1102，还用于使用第一安全保护方法对第一终端设备与第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护。收发模块 1101，用于向第二终端设备发送安全保护后的至少一条消息。

可选的，至少一条消息包括第一消息，第一消息为 PC5 建立流程中的第一条消息。

- 25 可选的，至少一条消息还包括第三消息，第三消息为 PC5 建立流程中第一终端设备发送的用于协商第一终端设备和第二终端设备之间的 PC5 连接的用户面使用的安全保护方法的消息；处理模块 1102，用于使用第一安全保护方法对 PC5 建立流程中的至少一条消息进行安全保护，包括：用于使用第一安全保护方法对第一消息进行安全保护；以及，在 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的安全等级的情况下，使用第一安全保护方法对第三消息进行安全保护。

- 30 可选的，在处理模块 1102 使用第一安全保护方法对第三消息进行安全保护之前，收发模块 1101，还用于接收来自第二终端设备的第二消息，第二消息包括第二终端设备选择的 PC5 连接的控制面的安全算法；处理模块 1102，还用于根据 PC5 连接的控制面的安全算法，确定 PC5 连接的控制面使用的安全保护方法的安全等级低于第一安全保护方法的安全等级。

可选的，至少一条消息包括第四消息，第四消息为 PC5 建立流程中第一终端设备发送的用于协商第一终端设备和第二终端设备之间的 PC5 连接的用户面使用的安全保护方法的消息；处理模块 1102，用于使用第一安全保护方法对 PC5 建立流程中的至少一条消息进行安全保护，包括：用于在确定 PC5 连接的控制面使用的安全保护方法的

安全等级低于第一安全保护方法的安全等级后，使用第一安全保护方法对第四消息进行安全保护。

可选的，处理模块 1102，还用于根据第一安全保护方法确定第二安全保护方法，第二安全保护方法为第一终端设备与第二终端设备之间的 PC5 连接的安全保护方法。

5 可选的，第二安全保护方法的安全等级不低于第一安全保护方法的安全等级。

可选的，处理模块 1102，用于根据第一安全保护方法确定第二安全保护方法，包括：用于通过收发模块 1101 接收来自第二终端设备的第二安全策略，第二安全策略为第二终端设备在 PC5 连接中的安全策略；根据第二安全策略和第一安全保护方法，确定第二安全保护方法。

10 可选的，处理模块 1102，用于根据第二安全策略和第一安全保护方法，确定第二安全保护方法，包括：在第一安全保护方法满足第二安全策略的情况下，将第一安全保护方法确定为第二安全保护方法；或者，在第一安全保护方法满足第二安全策略的情况下，根据第二安全策略，选择安全等级不低于第一安全保护方法的安全保护方法作为第一安全保护方法；或者，在第一安全保护方法不满足第二安全策略的情况下，
15 根据第二安全策略，选择一个满足第二安全策略的安全保护方法作为第二安全保护方法。

可选的，处理模块 1102，用于获取第一安全保护方法，包括：用于通过收发模块 1101 向第一直连通信发现名称管理功能网元发送第一信息和第一终端设备的 3GPP 身份信息，第一信息包括用于 ProSe 业务的身份信息或者用于确定用于 ProSe 业务的身份信息的信息；通过收发模块 1101 接收来自第一直连通信发现名称管理功能网元的第一安全保护方法。
20

或者，以通信装置 110 为上述方法实施例中的第一直连通信发现名称管理功能网元或者设置在该第一直连通信发现名称管理功能网元中的芯片或其他部件为例，一种可能的实现方式中：

25 收发模块 1101，用于接收来自第一终端设备的第一信息和第一终端设备的 3GPP 身份信息，其中，第一信息包括用于 ProSe 业务的身份信息或者用于确定用于 ProSe 业务的身份信息的信息。处理模块 1102，用于根据第一信息和第一终端设备的 3GPP 身份信息，确定第一终端设备使用 ProSe 业务时所需的安全保护方法。收发模块 1101，还用于向第一终端设备发送第一终端设备使用 ProSe 业务时所需的安全保护方法。

30 可选的，处理模块 1102，用于根据第一信息和第一终端设备的 3GPP 身份信息，确定第一终端设备使用 ProSe 业务时所需的安全保护方法，包括：用于根据第一信息和第一终端设备的 3GPP 身份信息，确定第一终端设备使用 ProSe 业务时对应的多个可供选择的安全保护方法；根据多个可供选择的安全保护方法确定第一终端设备使用 ProSe 业务时所需的安全保护方法。

35 可选的，处理模块 1102，还用于从第二直连通信发现名称管理功能网元获取第二终端设备使用 ProSe 业务时所需的安全保护方法；处理模块 1102，用于根据多个可供选择的安全保护方法确定第一终端设备使用 ProSe 业务时所需的安全保护方法，包括：用于确定多个可供选择的安全保护方法中是否包括第二终端设备使用 ProSe 业务时所需的安全保护方法；当多个可供选择的安全保护方法中包括第二终端设备使用 ProSe

业务时所需的安全保护方法时，将第二终端设备使用 ProSe 业务时所需的安全保护方法确定为第一终端设备使用 ProSe 业务时所需的安全保护方法；或者，当多个可供选择的安全保护方法中不包括第二终端设备使用 ProSe 业务时所需的安全保护方法时，从多个可供选择的安全保护方法中确定第一终端设备使用 ProSe 业务时所需的安全保护方法。

可选的，使用 ProSe 业务时所需的安全保护方法用于对第五消息进行安全保护，第五消息为第一终端设备与第二终端设备之间的发现流程中的第一条 PC5 广播消息。

可选的，使用 ProSe 业务时所需的安全保护方法用于确定第一终端设备与第二终端设备之间的 PC5 连接的安全保护方法。

10 可选的，PC5 连接的安全保护方法用于对 PC5 连接的控制面信令中传递的部分或全部参数进行安全保护；和/或，PC5 连接的安全保护方法用于对 PC5 连接的部分或全部用户面数据进行安全保护。

可选的，使用 ProSe 业务时所需的安全保护方法用于对第一终端设备与第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护。

15 可选的，至少一条消息包括第一消息，第一消息为 PC5 建立流程中的第一条消息。

其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再赘述。

在本实施例中，该通信装置 110 以采用集成的方式划分各个功能模块的形式来呈现。这里的“模块”可以指特定 ASIC，电路，执行一个或多个软件或固件程序的处理器和存储器，集成逻辑电路，和/或其他可以提供上述功能的器件。在一个简单的实施例中，本领域的技术人员可以想到该通信装置 110 可以采用图 3 所示的通信设备 300 的形式。

比如，图 3 所示的通信设备 300 中的处理器 301 可以通过调用存储器 303 中存储的计算机执行指令，使得通信设备 300 执行上述方法实施例中的通信方法。

25 具体的，图 11 中的收发模块 1101 和处理模块 1102 的功能/实现过程可以通过图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的计算机执行指令来实现。或者，图 11 中的处理模块 1102 的功能/实现过程可以通过图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的计算机执行指令来实现，图 11 中的收发模块 1101 的功能/实现过程可以通过图 3 中所示的通信设备 300 中的通信接口 304 来实现。

30 由于本实施例提供的通信装置 110 可执行上述通信方法，因此其所能获得的技术效果可参考上述方法实施例，在此不再赘述。

需要说明的是，以上模块或单元的一个或多个可以软件、硬件或二者结合来实现。当以上任一模块或单元以软件实现的时候，所述软件以计算机程序指令的方式存在，并被存储在存储器中，处理器可以用于执行所述程序指令并实现以上方法流程。该处理器可以内置于 SoC（片上系统）或 ASIC，也可是一个独立的半导体芯片。该处理器内处理用于执行软件指令以进行运算或处理的核外，还可进一步包括必要的硬件加速器，如现场可编程门阵列（field programmable gate array, FPGA）、PLD（可编程逻辑器件）、或者实现专用逻辑运算的逻辑电路。

当以上模块或单元以硬件实现的时候，该硬件可以是 CPU、微处理器、数字信号

处理 (digital signal processing, DSP) 芯片、微控制单元 (microcontroller unit, MCU)、人工智能处理器、ASIC、SoC、FPGA、PLD、专用数字电路、硬件加速器或非集成的分立器件中的任一个或任一组合, 其可以运行必要的软件或不依赖于软件以执行以上方法流程。

5 可选的, 本申请实施例还提供了一种通信装置 (例如, 该通信装置可以是芯片或芯片系统), 该通信装置包括处理器, 用于实现上述任一方法实施例中的方法。在一种可能的实现方式中, 该通信装置还包括存储器。该存储器, 用于保存必要的程序指令和数据, 处理器可以调用存储器中存储的程序代码以指令该通信装置执行上述任一方法实施例中的方法。当然, 存储器也可以不在该通信装置中。该通信装置是芯片系统时, 可以由芯片构成, 也可以包含芯片和其他分立器件, 本申请实施例对此不作具体限定。

10 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。当使用软件程序实现时, 可以全部或部分地以计算机程序产品的形式来实现。该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、服务器或者数据中心通过有线 (例如同轴电缆、光纤、数字用户线 (digital subscriber line, DSL)) 或

15 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存取的任何可用介质或者是包含一个或多个可以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, DVD)、或者半导体介质 (例如固态硬盘 (solid state disk, SSD)) 等。

20 尽管在此结合各实施例对本申请进行了描述, 然而, 在实施所要求保护的本申请过程中, 本领域技术人员通过查看所述附图、公开内容、以及所附权利要求书, 可理解并实现所述公开实施例的其他变化。在权利要求中, “包括” (comprising) 一词不排除其他组成部分或步骤, “一”或“一个”不排除多个的情况。单个处理器或其他单元可以实现权利要求中列举的若干项功能。相互不同的从属权利要求中记载了某些措施, 但这并不表示这些措施不能组合起来产生良好的效果。

25 尽管结合具体特征及其实施例对本申请进行了描述, 显而易见的, 在不脱离本申请的精神和范围的情况下, 可对其进行各种修改和组合。相应地, 本说明书和附图仅仅是所附权利要求所界定的本申请的示例性说明, 且视为已覆盖本申请范围内的任意和所有修改、变化、组合或等同物。显然, 本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样, 倘若本申请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, 则本申请也意图包含这些改动和变型在内。

30

35

权 利 要 求 书

1、一种通信方法，其特征在于，所述方法包括：

第一终端设备获取第一安全保护方法，所述第一安全保护方法为所述第一终端设备与第二终端设备之间的发现流程中确定的安全保护方法；

5 所述第一终端设备根据所述第一安全保护方法确定第二安全保护方法，所述第二安全保护方法为所述第一终端设备与所述第二终端设备之间的 PC5 连接的安全保护方法。

2、根据权利要求 1 所述的方法，其特征在于，所述第二安全保护方法的安全等级不低于所述第一安全保护方法的安全等级。

10 3、根据权利要求 1 或 2 所述的方法，其特征在于，所述第一终端设备根据所述第一安全保护方法确定第二安全保护方法，包括：

所述第一终端设备将所述第一安全保护方法确定为所述第二安全保护方法。

4、根据权利要求 1 或 2 所述的方法，其特征在于，所述第一终端设备根据所述第一安全保护方法确定第二安全保护方法，包括：

15 所述第一终端设备接收来自所述第二终端设备的第二安全策略，所述第二安全策略为所述第二终端设备在所述 PC5 连接中的安全策略；

所述第一终端设备根据所述第二安全策略和所述第一安全保护方法，确定所述第二安全保护方法。

20 5、根据权利要求 4 所述的方法，其特征在于，所述第一终端设备根据所述第二安全策略和所述第一安全保护方法，确定所述第二安全保护方法，包括：

在所述第一安全保护方法满足所述第二安全策略的情况下，将所述第一安全保护方法确定为所述第二安全保护方法；或者，

25 在所述第一安全保护方法满足所述第二安全策略的情况下，根据所述第二安全策略，选择安全等级不低于所述第一安全保护方法的安全保护方法作为所述第一安全保护方法；或者，

在所述第一安全保护方法不满足所述第二安全策略的情况下，根据所述第二安全策略，选择一个满足所述第二安全策略的安全保护方法作为所述第二安全保护方法。

30 6、根据权利要求 4 或 5 所述的方法，其特征在于，所述第二安全策略包括第二控制面安全策略和/或第二用户面安全策略；其中，所述第二控制面安全策略为所述第二终端设备在所述 PC5 连接中的控制面安全策略，所述第二用户面安全策略为所述第二终端设备在所述 PC5 连接中的用户面安全策略。

7、根据权利要求 1-6 任一项所述的方法，其特征在于，所述第二安全保护方法用于对所述 PC5 连接的控制面信令中传递的部分或全部参数进行安全保护；和/或，所述第二安全保护方法用于对所述 PC5 连接的部分或全部用户面数据进行安全保护。

35 8、根据权利要求 1-7 任一项所述的方法，其特征在于，所述方法还包括：

所述第一终端设备接收来自所述第二终端设备的第一消息，所述第一消息为所述第一终端设备与所述第二终端设备之间的 PC5 建立流程中的第一条消息；

所述第一终端设备使用所述第一安全保护方法对所述第一消息进行解安全保护。

9、根据权利要求 1-8 任一项所述的方法，其特征在于，所述第一终端设备获取第

一安全保护方法，包括：

所述第一终端设备向第一直连通信发现名称管理功能网元发送第一信息和所述第一终端设备的第三代合作伙伴计划 3GPP 身份信息，所述第一信息包括用于 ProSe 业务的身份信息或者用于确定所述用于 ProSe 业务的身份信息的信息；

- 5 所述第一终端设备接收来自第一直连通信发现名称管理功能网元的所述第一安全保护方法。

10、一种通信方法，其特征在于，所述方法包括：

第一终端设备获取第一安全保护方法，所述第一安全保护方法为所述第一终端设备与第二终端设备之间的发现流程中确定的安全保护方法；

- 10 所述第一终端设备使用所述第一安全保护方法对所述第一终端设备与所述第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护；

所述第一终端设备向所述第二终端设备发送安全保护后的至少一条消息。

11、根据权利要求 10 所述的方法，其特征在于，所述至少一条消息包括第一消息，所述第一消息为所述 PC5 建立流程中的第一条消息。

- 15 12、根据权利要求 11 所述的方法，其特征在于，所述至少一条消息还包括第三消息，所述第三消息为所述 PC5 建立流程中所述第一终端设备发送的用于协商所述第一终端设备和所述第二终端设备之间的 PC5 连接的用户面使用的安全保护方法的消息；所述第一终端设备使用所述第一安全保护方法对所述 PC5 建立流程中的至少一条消息进行安全保护，包括：

- 20 所述第一终端设备使用所述第一安全保护方法对所述第一消息进行安全保护；以及，

在所述 PC5 连接的控制面使用的安全保护方法的安全等级低于所述第一安全保护方法的安全等级的情况下，所述第一终端设备使用所述第一安全保护方法对所述第三消息进行安全保护。

- 25 13、根据权利要求 12 所述的方法，其特征在于，所述方法还包括：

所述第一终端设备接收来自所述第二终端设备的第二消息，所述第二消息包括所述第二终端设备选择的所述 PC5 连接的控制面的安全算法；

所述第一终端设备根据所述 PC5 连接的控制面的安全算法，确定所述 PC5 连接的控制面使用的安全保护方法的安全等级低于所述第一安全保护方法的安全等级。

- 30 14、根据权利要求 10 所述的方法，其特征在于，所述至少一条消息包括第四消息，所述第四消息为所述 PC5 建立流程中所述第一终端设备发送的用于协商所述第一终端设备和所述第二终端设备之间的 PC5 连接的用户面使用的安全保护方法的消息；所述第一终端设备使用所述第一安全保护方法对所述 PC5 建立流程中的至少一条消息进行安全保护，包括：

- 35 所述第一终端设备确定所述 PC5 连接的控制面使用的安全保护方法的安全等级低于所述第一安全保护方法的安全等级；

所述第一终端设备使用所述第一安全保护方法对所述第四消息进行安全保护。

15、根据权利要求 10 或 11 所述的方法，其特征在于，所述方法还包括：

所述第一终端设备根据所述第一安全保护方法确定第二安全保护方法，所述第二

安全保护方法为所述第一终端设备与所述第二终端设备之间的 PC5 连接的安全保护方法。

16、根据权利要求 15 所述的方法，其特征在于，所述第二安全保护方法的安全等级不低于所述第一安全保护方法的安全等级。

5 17、根据权利要求 15 或 16 所述的方法，其特征在于，所述第一终端设备根据所述第一安全保护方法确定第二安全保护方法，包括：

所述第一终端设备接收来自所述第二终端设备的第二安全策略，所述第二安全策略为所述第二终端设备在所述 PC5 连接中的安全策略；

10 所述第一终端设备根据所述第二安全策略和所述第一安全保护方法，确定所述第二安全保护方法。

18、根据权利要求 17 所述的方法，其特征在于，所述第一终端设备根据所述第二安全策略和所述第一安全保护方法，确定所述第二安全保护方法，包括：

在所述第一安全保护方法满足所述第二安全策略的情况下，将所述第一安全保护方法确定为所述第二安全保护方法；或者，

15 在所述第一安全保护方法满足所述第二安全策略的情况下，根据所述第二安全策略，选择安全等级不低于所述第一安全保护方法的安全保护方法作为所述第一安全保护方法；或者，

在所述第一安全保护方法不满足所述第二安全策略的情况下，根据所述第二安全策略，选择一个满足所述第二安全策略的安全保护方法作为所述第二安全保护方法。

20 19、根据权利要求 10-18 任一项所述的方法，其特征在于，所述第一终端设备获取第一安全保护方法，包括：

所述第一终端设备向第一直连通信发现名称管理功能网元发送第一信息和所述第一终端设备的第三代合作伙伴计划 3GPP 身份信息，所述第一信息包括用于 ProSe 业务的身份信息或者用于确定所述用于 ProSe 业务的身份信息的信息；

25 所述第一终端设备接收来自第一直连通信发现名称管理功能网元的所述第一安全保护方法。

20、一种通信方法，其特征在于，所述方法包括：

30 第一直连通信发现名称管理功能网元接收来自第一终端设备的第一信息和所述第一终端设备的第三代合作伙伴计划 3GPP 身份信息，其中，所述第一信息包括用于 ProSe 业务的身份信息或者用于确定所述用于 ProSe 业务的身份信息的信息；

所述第一直连通信发现名称管理功能网元根据所述第一信息和所述第一终端设备的 3GPP 身份信息，确定所述第一终端设备使用所述 ProSe 业务时所需的安全保护方法；

35 所述第一直连通信发现名称管理功能网元向所述第一终端设备发送所述第一终端设备使用所述 ProSe 业务时所需的安全保护方法。

21、根据权利要求 20 所述的方法，其特征在于，所述第一直连通信发现名称管理功能网元根据所述第一信息和所述第一终端设备的 3GPP 身份信息，确定所述第一终端设备使用所述 ProSe 业务时所需的安全保护方法，包括：

所述第一直连通信发现名称管理功能网元根据所述第一信息和所述第一终端设备

的 3GPP 身份信息，确定所述第一终端设备使用所述 ProSe 业务时对应的多个可供选择的安全保护方法；

所述第一直连通信发现名称管理功能网元根据所述多个可供选择的安全保护方法确定所述第一终端设备使用所述 ProSe 业务时所需的安全保护方法。

- 5 22、根据权利要求 21 所述的方法，其特征在于，所述方法还包括：

所述第一直连通信发现名称管理功能网元从第二直连通信发现名称管理功能网元获取第二终端设备使用所述 ProSe 业务时所需的安全保护方法；

所述第一直连通信发现名称管理功能网元根据所述多个可供选择的安全保护方法确定所述第一终端设备使用所述 ProSe 业务时所需的安全保护方法，包括：

- 10 所述所述第一直连通信发现名称管理功能网元确定所述多个可供选择的安全保护方法中是否包括所述第二终端设备使用所述 ProSe 业务时所需的安全保护方法；

当所述多个可供选择的安全保护方法中包括所述第二终端设备使用所述 ProSe 业务时所需的安全保护方法时，所述第一直连通信发现名称管理功能网元将所述第二终端设备使用所述 ProSe 业务时所需的安全保护方法确定为所述第一终端设备使用所述 ProSe 业务时所需的安全保护方法；或者，

- 15 当所述多个可供选择的安全保护方法中不包括所述第二终端设备使用所述 ProSe 业务时所需的安全保护方法时，所述第一直连通信发现名称管理功能网元从所述多个可供选择的安全保护方法中确定所述第一终端设备使用所述 ProSe 业务时所需的安全保护方法。

- 20 23、根据权利要求 20-22 任一项所述的方法，其特征在于，所述使用所述 ProSe 业务时所需的安全保护方法用于对第五消息进行安全保护，所述第五消息为所述第一终端设备与第二终端设备之间的发现流程中的第一条 PC5 广播消息。

- 24、根据权利要求 20-23 任一项所述的方法，其特征在于，所述使用所述 ProSe 业务时所需的安全保护方法用于确定所述第一终端设备与第二终端设备之间的 PC5 连接的安全保护方法。

25、根据权利要求 24 所述的方法，其特征在于，所述 PC5 连接的安全保护方法用于对所述 PC5 连接的控制面信令中传递的部分或全部参数进行安全保护；和/或，所述 PC5 连接的安全保护方法用于对所述 PC5 连接的部分或全部用户面数据进行安全保护。

- 30 26、根据权利要求 20-25 任一项所述的方法，其特征在于，所述使用所述 ProSe 业务时所需的安全保护方法用于对所述第一终端设备与第二终端设备之间的 PC5 建立流程中的至少一条消息进行安全保护。

27、根据权利要求 26 所述的方法，其特征在于，所述至少一条消息包括第一消息，所述第一消息为所述 PC5 建立流程中的第一条消息。

- 35 28、一种通信装置，其特征在于，包括用于执行如权利要求 1-9 中任一项所述方法的模块，或者，包括用于执行如权利要求 10-19 中任一项所述方法的模块，或者，包括用于执行如权利要求 20-27 中任一项所述方法的模块。

29、一种通信装置，其特征在于，所述通信装置包括：处理器和接口电路；
所述接口电路，用于接收计算机程序或指令并传输至所述处理器；

所述处理器用于执行所述计算机程序或指令，以使所述通信装置执行如权利要求 1-9 中任一项所述的方法，或者，以使所述通信装置执行如权利要求 10-18 中任一项所述的方法，或者，以使所述通信装置执行如权利要求 20-27 中任一项所述的方法。

- 5 30、一种计算机可读存储介质，其特征在于，包括指令，当所述指令在通信装置上运行时，以使所述通信装置执行如权利要求 1-9 中任一项所述的方法，或者，以使所述通信装置执行如权利要求 10-19 中任一项所述的方法，或者，以使所述通信装置执行如权利要求 20-27 中任一项所述的方法。