

通信方法及装置

相关申请的交叉引用

本申请要求在2020年05月20日提交中国专利局、申请号为202010432218.X、申请名称为“通信方法及装置”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本申请实施例涉及通信技术领域，尤其涉及通信方法及装置。

背景技术

车联网（vehicle to everything, V2X）是智能交通运输系统的关键技术，被认为是物联网体系中最有产业潜力、市场需求最明确的领域之一。车联网一般是指通过装载在车上的传感器、车载终端等提供车辆信息，实现车辆到车辆（vehicle to vehicle, V2V），车辆到基础设施（vehicle to infrastructure, V2I），车辆到网络（vehicle to Network, V2N）以及车辆到行人（vehicle to pedestrian, V2P）之间的相互通信的通信网络。一般的，在 V2X 场景下，终端与其他终端之间进行直连通信的通信链路可以称之为边链或者侧链（sidelink, SL），SL 接口可以称之为 PC5 口。

15

在新空口（new radio, NR）V2X 中，终端之间的高可靠性业务对通信质量提出了更高的要求，如何保障终端之间的正确通信，是目前需要解决的问题。

发明内容

20

本申请实施例提供通信方法及装置，用以保障终端之间的正确通信。

25

第一方面，本申请实施例提供一种通信方法，包括：第一终端对接收到的 RRC 消息进行完整性保护校验；当完整性保护校验失败，第一终端的 RRC 层向第一终端的应用层发送第一指示和第二终端的标识，所述第一指示和第二终端的标识用于所述应用层断开第一终端与第二终端之间的单播连接。

30

基于上述方案，在第一终端对接收到的消息执行完整性保护校验失败的情况下，第一终端的 RRC 层可以向应用层上报第一指示和第二终端的标识，触发应用层断开第一终端与第二终端之间的单播连接。由于给定了对接收到的消息执行完整性保护校验失败情况下的处理机制，因而可以保障第二终端与第一终端之间的正确通信。并且，对接收到的消息执行完整性保护校验失败的原因一般是攻击者篡改了 RRC 消息中的某些信息，因此该方法通过断开两个终端之间的单播连接，可以保障通信安全。

35

在一种可能的实现方法中，第一终端的 RRC 层断开第一终端与所述第二终端之间的 RRC 连接；则所述第一指示为 RRC 连接断开指示，用于指示所述第一终端与所述第二终端之间的 RRC 连接已经断开。

基于上述方案，第一终端的 RRC 层先断开第一终端与第二终端之间的 RRC 连接，并将连接断开的结果上报给应用层，从而触发应用层断开第一终端与第二终端之间的单播连

接, 有助于实现第一终端与第二终端之间的正确通信。

在另一种可能的实现方法中, 第一指示为完整性保护校验失败指示, 用于指示所述第一终端对接收到的来自所述第二终端的 RRC 消息进行完整性保护校验失败。

5 基于上述方案, 第一终端将完整性保护校验失败的情况上报给应用层, 从而触发应用层断开第一终端与第二终端之间的单播连接, 有助于实现第一终端与第二终端之间的正确通信。

在一种可能的实现方法中, 第一终端的应用层更新第一终端的层 2 标识。

基于该方案, 由于更新了第一终端的层 2 标识, 可以防止攻击者重复攻击, 因而可以提升通信安全。

10 在一种可能的实现方法中, 第一终端使用新的密钥, 重新建立与第二终端之间的单播连接。

基于该方案, 由于使用新的密钥重建单播连接, 因而可以提升通信安全。

15 在一种可能的实现方法中, 所述第一终端向网络设备发送侧行链路信息, 所述侧行链路信息包括第二指示和第二终端的标识, 所述第二指示用于指示所述第一终端与所述第二终端之间的单播连接发生无线链路失败且失败原因是对接收到的来自所述第二终端的 RRC 消息进行完整性保护校验失败。

20 基于上述方案, 在第一终端对接收到的 RRC 消息执行完整性保护校验失败的情况下, 第一终端可以向网络设备上报第二指示和第二终端的标识。由于给定了对接收到的消息执行完整性保护校验失败的情况下的处理机制, 使得网络设备可以基于上报的信息去排查第一终端与第二终端之间的单播连接故障, 因而可以保障第二终端与第一终端之间的正确通信。

25 第二方面, 本申请实施例提供一种通信方法, 包括: 第一终端对接收到的 RRC 消息进行完整性保护校验; 当所述完整性保护校验失败, 第一终端向网络设备发送侧行链路信息, 所述侧行链路信息包括第二指示和第二终端的标识, 第二指示用于指示第一终端与第二终端之间的单播连接发生无线链路失败且失败原因是对接收到的来自第二终端的 RRC 消息进行完整性保护校验失败。

30 基于上述方案, 在第一终端对接收到的 RRC 消息执行完整性保护校验失败的情况下, 第一终端可以向网络设备上报第二指示和第二终端的标识。由于给定了对接收到的消息执行完整性保护校验失败的情况下的处理机制, 使得网络设备可以基于上报的信息去排查第一终端与第二终端之间的单播连接故障, 因而可以保障第二终端与第一终端之间的正确通信。

35 第三方面, 本申请实施例提供一种通信方法, 包括: 第一终端在确定新的密钥之后, 所述第一终端的应用层向所述第一终端的接入层发送第一指示, 用于指示重建用于接收数据的 PDCP 实体或用于指示 PDCP 层能够使用所述新的密钥处理单播连接上的接收数据, 所述新的密钥用于所述第一终端与第二终端之间的所述单播连接的通信, 所述用于接收数据的 PDCP 实体关联于所述单播连接; 所述第一终端在接收到使用所述新的密钥加密的信息之后, 所述第一终端的应用层向所述第一终端的接入层发送第二指示, 用于指示重建用于发送数据的 PDCP 实体或用于指示 PDCP 层能够使用所述新的密钥处理所述单播连接上的发送数据, 所述用于发送数据的 PDCP 实体关联于所述单播连接。

40 其中, “用于指示 PDCP 层能够使用所述新的密钥处理单播连接上的接收数据”, 也可

以理解为“用于指示 PDCP 层具有使用所述新的密钥处理单播连接上的接收数据的能力”。

其中，“用于指示 PDCP 层能够使用所述新的密钥处理单播连接上的发送数据”，也可以理解为“用于指示 PDCP 层具有使用所述新的密钥处理单播连接上的发送数据的能力”。

5 基于上述方案，终端的应用层可以在相应的时间点上通知接入层可以开始使用新的密钥对接收到数据进行解密，以及在相应的时间点上通知接入层可以开始使用新的密钥对需要发送的数据进行加密，从而可以保障第一终端与第二终端之间的正确通信。

10 在一种可能的实现方法中，所述第一终端在确定新的密钥之后，所述第一终端的应用层向所述第一终端的接入层发送第一指示，包括：所述第一终端在确定所述新的密钥，以及向所述第二终端发送了安全模式命令消息之后，所述第一终端的应用层向所述第一终端的接入层发送所述第一指示；或者，所述第一终端在确定所述新的密钥，以及确定能够使用所述新的密钥处理所述单播连接上的接收数据之后，所述第一终端的应用层向所述第一终端的接入层发送所述第一指示。

15 在一种可能的实现方法中，所述第一终端在接收到使用所述新的密钥加密的信息之后，所述第一终端的应用层向所述第一终端的接入层发送第二指示，包括：所述第一终端在接收到使用所述新的密钥加密的安全模式完成消息之后，所述第一终端的应用层向所述第一终端的接入层发送所述第二指示；或者，所述第一终端在接收到使用所述新的密钥加密的信息，以及确定能够使用所述新的密钥处理所述单播连接上的发送数据之后，所述第一终端的应用层向所述第一终端的接入层发送所述第二指示。

20 在一种可能的实现方法中，所述接入层为所述 PDCP 层；所述第一终端的应用层向所述第一终端的接入层发送第一指示，包括：所述第一终端的所述应用层向所述第一终端的所述 PDCP 层发送所述第一指示；所述第一终端的应用层向所述第一终端的接入层发送第二指示，包括：所述第一终端的所述应用层向所述第一终端的所述 PDCP 层发送所述第二指示。

25 在另一种可能的实现方法中，所述接入层为 RRC 层；所述第一终端的应用层向所述第一终端的接入层发送第一指示，包括：所述第一终端的所述应用层通过所述 RRC 层，向所述第一终端的所述 PDCP 层发送所述第一指示；所述第一终端的应用层向所述第一终端的接入层发送第二指示，包括：所述第一终端的所述应用层通过所述 RRC 层，向所述第一终端的所述 PDCP 层发送所述第二指示。

30 第四方面，本申请实施例提供一种通信方法，包括：第一终端接收来自第二终端的第一数据包，所述第一数据包携带密钥标识，所述密钥标识对应的密钥用于所述第一终端与所述第二终端之间的单播连接的通信；若所述第一终端内没有存储有所述密钥标识对应的密钥安全上下文，则所述第一终端丢弃所述第一数据包。

35 基于上述方案，第一终端接收到携带密钥标识的第一数据包之后，若第一终端没有存储该密钥标识对应的密钥安全上下文，则第一终端丢弃该第一数据包，而现有技术中是在解析该第一数据包并传输到 IP 层后才发现解析错误，进而丢弃该第一数据包。可以看出，本申请上述方案可以提前丢弃无法解析的数据包，因而可以保障该终端与其他终端之间的正确通信，同时还可以节约资源开销。

40 第五方面，本申请实施例提供一种通信装置，该装置可以是第一终端，还可以是用于第一终端的芯片。该装置具有实现上述第一方面至第四方面的方法，第一方面至第四方面的各可能的实现方法中的任意方法的功能。该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。该硬件或软件包括一个或多个与上述功能相对应的模块。

5 第六方面，本申请实施例提供一种通信装置，包括处理器和存储器；该存储器用于存储计算机执行指令，当该装置运行时，该处理器执行该存储器存储的该计算机执行指令，以使该装置执行如上述第一方面至第四方面的方法，第一方面至第四方面的各可能的实现方法中的任意方法。

第七方面，本申请实施例提供一种通信装置，包括用于执行上述第一方面至第四方面的方法，第一方面至第四方面的各可能的实现方法中的任意方法的各个步骤的单元或手段（means）。

10 第八方面，本申请实施例提供一种通信装置，包括处理器和接口电路，所述处理器用于通过接口电路与其它装置通信，并执行上述第一方面至第四方面的方法，第一方面至第四方面的各可能的实现方法中的任意方法。该处理器包括一个或多个。

第九方面，本申请实施例提供一种通信装置，包括处理器，用于与存储器相连，用于调用所述存储器中存储的程序，以执行上述第一方面至第四方面的方法，第一方面至第四方面的各可能的实现方法中的任意方法。该存储器可以位于该装置之内，也可以位于该装置之外。且该处理器包括一个或多个。

15 第十方面，本申请实施例还提供一种计算机可读存储介质，所述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，使得处理器执行上述第一方面至第四方面的方法，第一方面至第四方面的各可能的实现方法中的任意方法。

20 第十一方面，本申请实施例还提供一种计算机程序产品，该计算机产品包括计算机程序，当计算机程序运行时，使得上述第一方面至第四方面的方法，第一方面至第四方面的各可能的实现方法中的任意方法被执行。

第十二方面，本申请实施例还提供一种芯片系统，包括：处理器，用于执行上述第一方面至第四方面的方法，第一方面至第四方面的各可能的实现方法中的任意方法。

25 附图说明

- 图 1 为本申请实施例所适用的一种网络架构示意图；
- 图 2 为本申请实施例提供的一种协议栈的示意图；
- 图 3 为单播连接的两个终端之间的一种密钥更新流程示意图；
- 图 4 为本申请实施例提供一种通信方法示意图；
- 30 图 5 为本申请实施例提供又一种通信方法示意图；
- 图 6 为本申请实施例提供又一种通信方法示意图；
- 图 7 为本申请实施例提供又一种通信方法示意图；
- 图 8 为本申请实施例提供的一种终端示意图。

35 具体实施方式

如图 1 所示，为本申请实施例所适用的一种网络架构示意图，包括至少两个终端和至少一个网络设备。可选的，终端可以通过无线接口（如 Uu 口）与网络设备通信。终端之间可以通过网络设备进行通信，也可以进行直连通信，比如通过终端之间的 PC5 接口通信。终端之间的链路可以称为侧行链路，或者边链路，或者旁链路，或者 PC5 接口链路，或者

终端间链路。

终端(terminal),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、用户设备(user equipment, UE)等。本申请实施例中的终端与终端之间支持直连通信,终端与终端之间的直连通信也可以称为D2D通信。

网络设备,是一种为终端提供无线通信功能的设备,网络设备包括但不限于:第五代(5th generation, 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。

5G独立部署时,网络设备的逻辑体系可以采用集中单元(centralized unit, CU)和分布单元(distributed unit, DU)分离模式。基于协议栈功能的配置, CU-DU逻辑体系可以分为两种,即CU-DU分离架构和CU-DU融合架构。针对CU-DU分离架构,协议栈的功能可以动态配置和分割,其中一些功能在CU中实现,剩余功能在DU中实现。为满足不同分割选项的需求,需要支持理想传输网络和非理想传输网络。CU与DU之间的接口应当遵循第三代合作伙伴计划(3rd generation partnership project, 3GPP)规范要求。针对CU-DU融合架构, CU和DU的逻辑功能整合在同一个网络设备中,以实现协议栈的全部功能。

随着技术的发展,5G NR技术引入D2D通信和终端间的协作通信。NR V2X标准已经支持三种类型的侧行链路通信模式,包括广播、组播和单播。针对NR V2X单播连接,标准上已经允许两个单播连接的两个终端之间的通信进行加密和完整性保护,并且允许终端之间更新密钥。单播连接密钥更新是指侧行链路的两个终端更新数据传输的完整性保护算法和加密算法的过程,密钥更新在各自的PC5-S层完成,更新后的密钥需要被接入层(access stratum, AS)层的分组数据汇聚协议(Packet Data Convergence Protocol, PDCP)实体使用。

如图2所示,为本申请实施例提供的一种协议栈的示意图。终端的协议栈至少包括:应用层、无线资源控制(Radio Resource Control, RRC)层、PDCP层、无线链路控制(radio link control, RLC)层、媒体接入控制(media access control, MAC)层、物理层(PHY layer)。其中, RRC层、PDCP层、RLC层、MAC层、PHY层可以统称为属于接入层(AS)。

应用层,例如包括PC5-S层或V2X层,用于执行应用层面的控制。

RRC层用于支持无线资源的管理、RRC连接控制等功能。

对于其他的协议层,例如 PDCP 层、RLC 层等,其定义与功能可以参见现有技术的说明,在此不再赘述。

如图 3 所示,为单播连接的两个终端之间的一种密钥更新流程示意图。包括以下步骤:

5 步骤 301,第一终端向第二终端发送密钥更新请求消息。相应地,第二终端可以接收到该密钥更新请求消息。

该密钥更新请求消息用于请求更新该单播连接的密钥。该密钥更新请求消息比如可以是 DirectRekeyRequest 消息。

10 该密钥更新请求消息携带第一终端的安全能力信息、密钥更新请求指示和新的密钥标识的高 8 位。安全能力信息包括第一终端能够在该单播连接中支持的安全算法。这里的安全算法包括完整性保护算法和/或加密算法。

需要说明的是,第一终端与第二终端之间的密钥更新流程中,第一终端向第二终端发送密钥更新请求消息,是为了获取一个 256 位的新的密钥,可以通过新的密钥的标识(也称为新的密钥标识)进行标识。该新的密钥标识为 16 位,其中高 8 位是由第一终端提前
15 确认的,低 8 位是由第二终端确认的。由第一终端将新的密钥标识的高 8 位发送给第二终端,由第二终端将新的密钥标识的低 8 位发送给第一终端,从而第一终端和第二终端都可以获得新的密钥标识。

步骤 302,第二终端选择新的安全算法,并确定新的密钥。

20 第二终端根据第一终端的安全能力信息,从第一终端支持的完整性保护算法中选择一个完整性保护算法,和/或从第一终端支持的加密算法中选择一个加密算法。然后第二终端基于选择的完整性保护算法和/或选择的加密算法,确定一个新的密钥。

在第二终端确定新的密钥之后,则建立新密钥的安全上下文,后续第二终端可以开始在该单播连接上从第一终端接收使用新的密钥加密的数据。或者理解为,第二终端开启了在该单播连接上从第一终端接收使用新的密钥加密的数据的功能。

25 需要说明的是,第一终端与第二终端之间可以建立多条单播连接,每个单播连接使用一个密钥。第一终端与第二终端之间协商的新的密钥是针对其中某个单播连接的。

步骤 303,第二终端向第一终端发送安全模式命令消息。相应地,第二终端可以接收到该安全模式命令消息。

该安全模式命令消息比如可以是 DirectSecurityModeCommand 消息。

30 该安全模式命令消息中携带第二终端选择的新的完整性保护算法和/或新的加密算法的指示、第一终端的安全能力信息和新的密钥标识的低 8 位。

步骤 304,第一终端确定新的密钥。

35 第一终端先对接收到的安全模式命令消息进行完整性校验,并对携带的第一终端的安全能力信息进行验证,当验证结果都为正确,则第一终端根据安全模式命令消息中指示的新的完整性保护算法和/或新的加密算法,按照与第二终端相同的密钥推演方法,得到新的密钥,该新的密钥与第二终端推演得到的新的密钥相同。

40 第一终端确定新的密钥之后,则建立新密钥的安全上下文,确定后续可以开始在该单播连接上从第二终端接收使用新的密钥加密的数据,以及可以使用新的密钥对需要在该单播连接上发送至第二终端的数据进行加密。或者理解为,第二终端开启了在该单播连接上从第一终端接收使用新的密钥加密的数据的功能,以及开启了使用新的密钥对需要在该单

播连接上发送至第二终端的数据进行加密的功能。

步骤 305, 第一终端向第二终端发送安全模式完成消息。相应地, 第二终端可以接收到该安全模式完成消息。

5 该安全模式完成消息例如可以是 DirectSecurityModeComplete 消息, 用于指示第一终端已经完成密钥更新。

第二终端对接收到的安全模式完成消息进行完整性校验, 当校验结果为正确, 则第二终端确认第一终端的密钥更新正确。

10 第二终端确认第一终端的密钥更新正确之后, 则确定后续可以使用新的密钥对需要在该单播连接上发送至第一终端的数据进行加密。或者理解为, 第二终端开启了使用新的密钥对需要在该单播连接上发送至第一终端的数据进行加密的功能。

步骤 306, 第二终端删除旧的密钥对应的密钥安全上下文。

第二终端确认第一终端的密钥更新正确之后, 后续将使用新的密钥向第一终端发送数据, 因而删除旧的密钥对应的密钥安全上下文。

15 步骤 307, 第二终端向第一终端发送第一信令。相应地, 第一终端可以接收到该第一信令。

该第一信令是使用新的密钥进行加密的。

步骤 308, 第一终端删除旧的密钥对应的密钥安全上下文。

第一终端解析第一信令, 若能正确解析, 表明第一终端可以正确接收使用新的密钥加密的数据, 因而可以删除旧的密钥对应的密钥安全上下文。

20 需要说明的是, 上述步骤 306 也可以是在步骤 307 之后执行。

通过上述过程, 实现了第一终端与第二终端之间的密钥更新, 可以提升通信的安全性。

针对上述第一终端与第二终端之间的密钥更新流程, 至少存在以下两个问题:

25 问题 1)、第二终端接收数据与发送数据开始使用新的密钥的时机是不同的。具体的, 第二终端在确定新的密钥之后, 则可以开始从第一终端接收使用新的密钥加密的数据, 但是在确认第一终端的密钥更新正确之后才确定可以使用新的密钥对需要发送至第一终端的数据进行加密。由于第二终端接收数据与发送数据开始使用新的密钥的时机不同, 则第二终端的 AS 层如何获知在何时可以开始使用新的密钥对需要发送至第一终端的数据进行加密, 以及如何获知在何时可以从第一终端接收使用新的密钥加密的数据, 以保障第二终端与第一终端之间的正确通信, 是有待解决的问题。

30 问题 2)、第一终端与第二终端删除旧的密钥对应的密钥安全上下文的时机是不同的。参考图 3, 第一终端是在步骤 307 之后删除旧的密钥对应的密钥安全上下文, 而第二终端是在步骤 305 之后删除旧的密钥对应的密钥安全上下文。第二终端删除了旧的密钥对应的密钥安全上下文后, 可能继续收到第一终端发送的使用旧的密钥加密的数据。由于侧行链路密钥更新的流程中没有引入 RLC 实体重建及 MAC 实体重置等流程, 因此从第一终端接收到的使用旧的密钥加密的数据可能包括: RLC 缓存区未传完的数据、MAC 层缓存区未传完的数据、传输失败导致重传的数据中的一种或多种。此时, 第二终端如何识别并处理这些使用旧的密钥加密的数据, 以保障第二终端与第一终端之间的正确通信, 也是有待解决的问题。

40 此外, 在第一终端与第二终端完成密钥更新流程之后的正常通信过程中, 还可能出现

以下问题:

问题 3)、第一终端或第二终端对接收到的消息执行完整性保护校验失败的情况。该情况下,第一终端或第二终端该如何处理,以保障第二终端与第一终端之间的正确通信,也是有待解决的问题。

5

为解决上述问题 1) 至 3), 本申请实施例提供不同的通信方法。需要说明的是, 在这些通信方法中提到的密钥(如旧的密钥或新的密钥)均是针对第一终端与第二终端之间建立的某一条特定的单播连接。或者理解为, 第一终端与第二终端之间可以建立多条单播连接, 每个单播连接使用一个密钥。

10

为解决上述问题 1), 本申请实施例提供一种通信方法。该方法适用于第一终端与第二终端之间, 且第一终端与第二终端之间通过单播连接通信。

如图 4 所示, 该方法包括以下步骤:

步骤 401, 第一终端在确定新的密钥之后, 第一终端的应用层向第一终端的接入层发送第一指示, 该第一指示用于指示重建用于接收数据的 PDCP 实体或用于指示 PDCP 层能够使用新的密钥处理单播连接上的接收数据。该新的密钥用于第一终端与第二终端之间的单播连接的通信。

其中, 第一指示用于指示 PDCP 层能够使用新的密钥处理单播连接上的接收数据, 也可以理解为用于指示 PDCP 层能够接收使用该新的密钥进行加密的数据, 或者也可以理解为用于指示 PDCP 层具有使用所述新的密钥处理单播连接上的接收数据的能力。

所述第一指示可以是第一终端的应用层向第一终端的接入层发送的一个新的密钥处理接收数据的能力指示, 触发第一终端的应用层使用新的密钥及完整性保护和加密算法, 使得第一终端具备使用新的密钥处理所述单播连接上的接收数据的能力。第一指示也可以是第一终端的应用层向第一终端的接入层发送的一个该单播连接相关的接收数据的 PDCP 实体的重建指示, 所述接收数据的 PDCP 实体重建过程中应用了新的密钥及新的完整性保护和加密算法, 使得第一终端具备使用新的密钥处理所述单播连接上的接收数据的能力。

用于接收数据的 PDCP 实体关联于第一终端与第二终端之间的单播连接。或者理解为, 第一终端与第二终端之间可能会存在多个单播连接, 用于接收数据的 PDCP 实体关联于其中一个单播连接。当有多个单播连接时, 则需要不同的 PDCP 实体关联于不同的单播连接。

其中, 第一终端的应用层可以是 PC5-S 层或 V2X 层。

第一终端的应用层向接入层发送第一指示, 比如可以是应用层向 PDCP 层发送第一指示。再比如还可以是应用层向 RRC 层发送第一指示, RRC 层接收到第一指示后, 可以指示 PDCP 层重建用于接收单播连接的数据的 PDCP 实体。具体的, 重建用于使用新的密钥处理单播连接上的接收数据的 PDCP 实体, 也即新建立的 PDCP 实体使用新的密钥对接收到的单播连接的数据进行解密。

作为一种实现方法, 第一终端在确定新的密钥之后, 比如可以是在向第二终端发送了安全模式命令消息(如图 3 实施例中的步骤 303 的消息)之后。

作为另一种实现方法, 第一终端在确定新的密钥之后, 比如还可以是第一终端在接收密钥更新请求消息(如图 3 实施例中的步骤 301 的消息)并基于此确定能够使用新的密钥处

40

理单播连接上的接收数据之后。其中，第一终端在确定能够使用新的密钥处理单播连接上的接收数据，也可以理解为是第一终端能够使用旧的密钥处理单播连接上的发送数据以及能够使用新的密钥处理单播连接上的接收数据。

5 步骤 402，第一终端在接收到使用新的密钥加密的信息（如信令（signalling）、消息或数据）之后，第一终端的应用层向第一终端的接入层发送第二指示，该第二指示用于指示重建立用于发送数据的 PDCP 实体或用于指示 PDCP 层能够使用新的密钥处理单播连接上的发送数据。

10 其中，第二指示用于指示 PDCP 层能够使用新的密钥处理单播连接上的发送数据，也可以理解为用于指示 PDCP 层能够发送使用该新的密钥进行加密的单播连接的数据，或者也可以理解为用于指示 PDCP 层能够使用该新的密钥对需要发送的单播连接的数据进行加密并发送，或者也可以理解为用于指示 PDCP 层具有使用所述新的密钥处理单播连接上的发送数据的能力。

15 具体的，所述第二指示可以是第一终端的应用层向第一终端的接入层发送的一个新的密钥处理发送数据的能力指示，触发第一终端的应用层去应用新的密钥及完整性保护和加密算法，使得第一终端具备使用新的密钥处理所述单播连接上的发送数据的能力；也可以是第一终端的应用层向第一终端的接入层发送的一个该单播连接相关的发送数据的 PDCP 实体的重建立指示，所述接收数据的 PDCP 实体重建立过程中应用了新的密钥及新的完整性保护和加密算法，使得第一终端具备使用新的密钥处理所述单播连接上的发送数据的能力。

20 用于发送数据的 PDCP 实体关联于第一终端与第二终端之间的单播连接。或者理解为，第一终端与第二终端之间可能会存在多个单播连接，用于发送数据的 PDCP 实体关联于其中一个单播连接。当有多个单播连接时，则需要不同的 PDCP 实体关联于不同的单播连接。

需要说明的是，该实施例中的用于发送数据的 PDCP 实体与用于接收数据的 PDCP 实体是关联到同一个单播连接的。

25 第一终端的应用层向接入层发送第二指示，比如可以是应用层向 PDCP 层发送第一指示。或者还可以是应用层向 RRC 层发送第二指示，RRC 层接收到第二指示后，可以指示 PDCP 层重建立用于发送数据的 PDCP 实体。具体的，重建立用于使用新的密钥对需要发送的单播连接的数据进行加密和发送的 PDCP 实体。

30 作为一种实现方法，第一终端在接收到使用新的密钥加密的数据之后，比如可以是在从第二终端接收到安全模式完成消息（如图 3 实施例中的步骤 305 的消息）之后。

35 作为另一种实现方法，第一终端在确定新的密钥之后，也可以是第一终端在确定能够使用新的密钥处理单播连接上的发送数据之后，比如可以是验证从第一终端接收到的新的密钥加密的数据正确并基此认为第一终端已经确认新的密钥并建立了新的密钥相关的安全上下文之后。其中，第一终端在确定能够使用新的密钥处理单播连接上的发送数据，也可以理解为是第一终端能够使用新的密钥处理单播连接上的接收数据以及能够使用新的密钥处理单播连接上的发送数据。

需要说明的是，该图 4 实施例中的第一终端可以是图 3 实施例中的第二终端，该图 4 实施例中的第二终端可以是图 3 实施例中的第一终端。

40 作为一种实现方法，上述第一指示也可以称为 PDCP 实体重建立指示。当 PDCP 层接收到第一指示，则会重建立 PDCP 实体。上述第二指示也可以称为 PDCP 实体重建立指示。

当 PDCP 层接收到第二指示，则会重建 PDCP 实体。

基于上述方案，终端的应用层可以在相应的时间点上通知接入层可以开始使用新的密钥对接收到数据进行解密，以及在相应的时间点上通知接入层可以开始使用新的密钥对需要发送的数据进行加密，从而可以保障第一终端与第二终端之间的正确通信。

5

在一种实现方法中，针对上述图 3 实施例中的第一终端、或上述图 4 实施例中的第二终端，该终端在确定新的密钥之后，该终端的应用层向该终端的接入层发送第三指示，该第三指示用于指示重建用于发送数据的 PDCP 实体以及重建用于接收数据的 PDCP 实体，或者用于指示 PDCP 层能够使用新的密钥处理单播连接上的发送数据和接收数据。

10 需要说明的是，用于发送单播连接的数据的 PDCP 实体与用于接收单播连接的数据的 PDCP 实体是不同的 PDCP 实体。

其中，第三指示用于指示 PDCP 层能够使用新的密钥处理单播连接上的发送数据和接收数据，也可以理解为用于指示 PDCP 层能够使用该新的密钥对需要发送的单播连接的数据进行加密及发送，以及能够对接收到的单播连接的数据使用新的密钥进行解密。作为一种实现方法，上述第三指示也可以称为 PDCP 实体重建指示。当 PDCP 层接收到第三指示，则会重建 PDCP 实体。

15 其中，终端的应用层可以是 PC5-S 层或 V2X 层。

终端的应用层向接入层发送第三指示，比如可以是应用层向 PDCP 层发送第一指示。再比如还可以是应用层向 RRC 层发送第三指示，RRC 层接收到第三指示后，可以指示 PDCP 层重建用于发送单播连接的数据的 PDCP 实体以及重建用于接收单播连接的数据的 PDCP 实体。

作为一种实现方法，终端在确定新的密钥之后，例如可以是在确定新的密钥之后以及在发送安全模式完成消息（如图 3 实施例中的步骤 305 的消息）之前。

25 作为另一种实现方法，终端在确定新的密钥之后，还可以是终端在确定能够使用新的密钥处理单播连接上的发送数据和接收数据之后。例如可以是在接收并验证第二终端发送的安全模式命令消息（如图 3 实施例中的步骤 303 的消息）正确，并基此认为第二终端已经确认新的密钥并建立了新的密钥相关的安全上下文之后。

30 为解决上述问题 2)，本申请实施例提供一种通信方法，该方法适用于第一终端与第二终端之间，且第一终端与第二终端之间通过单播连接通信。

如图 5 所示，该方法包括以下步骤：

步骤 501，第一终端接收来自第二终端的第一数据包，该第一数据携带密钥标识，该密钥标识对应的密钥用于第一终端与第二终端之间的单播连接的通信。

35 该第一数据包是使用该密钥标识对应的密钥进行加密的。比如，第一数据包可以是接收数据的 PDCP 实体从下层接收的 PDCP Data 协议数据单元（protocol data unit, PDU），包括控制面的数据包和/或用户面的数据包。

在正常情况下，第一终端会存储该密钥标识对应的密钥安全上下文。在某些情况下，比如图 3 实施例中的密钥更新流程中，第一终端也会删除旧的密钥对应的密钥安全上下文，并建立新的密钥对应的密钥安全上下文。

40 在删除了旧的密钥对应的密钥安全上下文之后，第一终端也可能会继续收到使用旧的

密钥进行加密的数据。如上述图 3 实施例中的第二终端，在删除了旧的密钥对应的密钥安全上下文之后，可能会继续收到使用旧的密钥进行加密的数据。

步骤 502，若第一终端内没有存储有该密钥标识对应的密钥安全上下文，则第一终端丢弃该第一数据包。

5 若第一终端内存储有该密钥标识对应的密钥安全上下文，则第一终端接收并处理该第一数据包。比如第一终端使用该密钥标识对应的密钥对该第一数据包进行解密。

若第一终端内没有存储有该密钥标识对应的密钥安全上下文，表明第一终端与第二终端曾经使用该密钥标识对应的密钥，但由于某些原因，如密钥更新，导致第一终端删除了该密钥对应的密钥安全上下文。因此，第一终端若继续收到该密钥对应的密钥安全上下文，
10 则第一终端将无法解密该第一数据，因而第一终端可以丢弃该第一数据包。

作为一个示例，该实施例中的第一终端可以是图 3 对应实施例中的第二终端。

基于上述方案，第一终端接收到携带密钥标识的第一数据包之后，若第一终端没有存储该密钥标识对应的密钥安全上下文，则第一终端丢弃该第一数据包，而现有技术中是在解析该第一数据包并传输到互联网协议（internet protocol，IP）层后才发现解析错误，进
15 而丢弃该第一数据包。可以看出，本申请上述方案可以提前丢弃无法解析的数据包，因而可以保障该终端与其他终端之间的正确通信，同时还可以节约资源开销。

为解决上述问题 3)，本申请实施例提供一种通信方法，该方法适用于第一终端与第二终端之间，且第一终端与第二终端之间通过单播连接通信。

20 其中，第一终端与第二终端之间建立单播连接的过程为：第一终端与第二终端之间先建立单播连接，在单播连接建立成功后，则自动建立第一终端与第二终端之间的 RRC 连接。

第一终端与第二终端之间断开单播连接的过程为：第一终端与第二终端之间先断开单播连接，在单播连接断开成功后，则自动断开第一终端与第二终端之间的 RRC 连接。

25 如图 6 所示，该方法包括以下步骤：

步骤 601，第一终端对接收到的 RRC 消息进行完整性保护校验。

该步骤中的 RRC 消息也可以称为 PC5-RRC 消息。第一终端是从与第一终端建立了单播连接的第二终端接收到的 RRC 消息，并且对该 RRC 消息进行完整性保护校验。

步骤 602，当所述完整性保护校验失败，第一终端的 RRC 层向第一终端的应用层发送
30 第一指示和第二终端的标识，所述第一指示和所述第二终端的标识用于所述应用层断开所述第一终端与所述第二终端之间的单播连接。

这里的应用层可以是 PC5-S 层或 V2X 层。

第一终端的应用层从 RRC 层接收到第一指示和第二终端的标识之后，则根据第一指示和第二终端的标识，断开第一终端与第二终端之间的单播连接。对接收到的消息执行完整性保护校验失败的原因可能是攻击者篡改了接收到的 RRC 消息中的某些信息，因此该方法通过断开两个终端之间的单播连接，可以保障通信安全。

可选的，第一终端的应用层还可以更新层 2 标识（Layer2 ID），即第一终端的 MAC 层身份标识，从而提升通信安全。

40 可选的，第一终端还可以使用新的密钥，重新建立与第二终端之间的单播连接，从而提升通信安全。

基于上述方案，在第一终端对接收到的消息执行完整性保护校验失败的情况下，第一终端的 RRC 层可以向应用层上报第一指示和第二终端的标识，触发应用层断开第一终端与第二终端之间的单播连接。由于给定了对接收到的消息执行完整性保护校验失败的情况下的处理机制，因而可以保障第二终端与第一终端之间的正确通信。并且，对接收到的消息执行完整性保护校验失败的原因一般是攻击者篡改了 RRC 消息中的某些信息，因此该方法通过断开两个终端之间的单播连接，可以保障通信安全。

作为示例，下面给出上述步骤 602 中的第一指示的两种不同实现方法。

方法 1，第一指示为 RRC 连接断开指示。

该 RRC 连接断开指示用于指示第一终端与第二终端之间的 RRC 连接已经断开。

也即，基于该方法 1，则在步骤 601 之后，第一终端先断开第一终端与第二终端之间的 RRC 连接，然后在上述步骤 602 中第一终端的 RRC 层向应用层发送 RRC 连接断开指示和第二终端的标识。第一终端的应用层根据 RRC 连接断开指示，确定第一终端与第二终端之间的 RRC 连接已经断开，则触发第一终端的应用层断开第一终端与第二终端之间的单播连接。

方法 2，第一指示为完整性保护校验失败指示。

该完整性保护校验失败指示用于指示第一终端对接收到的 RRC 消息进行完整性保护校验失败。

也即，基于该方法 2，第一终端的 RRC 层在上述步骤 601 中对接收到的 RRC 消息进行完整性保护校验失败后，在上述步骤 602 中向第一终端的应用层发送完整性保护校验失败指示和第二终端的标识。第一终端的应用层根据完整性保护校验失败指示和第二终端的标识，断开第一终端与第二终端之间的单播连接。在第一终端与第二终端之间的单播连接断开之后，第一终端与第二终端之间的 RRC 连接也将自动断开。

为解决上述问题 3)，本申请实施例提供另一种通信方法，如图 7 所示，该方法包括以下步骤：

步骤 701，第一终端对接收到的 RRC 消息进行完整性保护校验。

该步骤中的 RRC 消息也可以是 PC5-RRC 消息。第一终端是从与第一终端建立了单播连接的第二终端接收到的 RRC 消息，并且对该 RRC 消息进行完整性保护校验。

步骤 702，当所述完整性保护校验失败，第一终端向网络设备发送侧行链路信息，该侧行链路信息包括第二指示和第二终端的标识。

作为一种实现方法，上述第二指示是一个完整性保护校验失败指示，用于指示第一终端对接收到的来自第二终端的 RRC 消息进行完整性保护校验失败。从而网络设备获知第一终端对接收到的来自第二终端的 RRC 消息完整性保护校验失败。

作为另一种实现方法，上述第二指示还可以用于指示第一终端与第二终端之间的单播连接发生无线链路失败 (Radio Link Failure, RLF) 且失败原因是对接收到的来自第二终端的 RRC 消息进行完整性保护校验失败。从而网络设备获知第一终端对接收到的来自第二终端的 RRC 消息完整性保护校验失败。

可选的，网络设备获知第一终端对接收到的来自第二终端的 RRC 消息完整性保护校验失败之后，可以尝试寻找攻击者或者是触发报警等。

基于上述方案，在第一终端对接收到的 RRC 消息执行完整性保护校验失败的情况下，

第一终端可以向网络设备上报第二指示和第二终端的标识。由于给定了对接收到的消息执行完整性保护校验失败的情况下的处理机制，使得网络设备可以基于上报的信息去排查第一终端与第二终端之间的单播连接故障，因而可以保障第二终端与第一终端之间的正确通信。

5 上述图 6 实施例或图 7 实施例中，当第一终端对接收到的控制面的 RRC 消息进行完整性保护校验失败时，给出了相应的处理方法。在另一种场景下，如果第一终端对接收到的用户面消息进行完整性保护校验失败，则第一终端可以向网络设备发送侧行链路信息，该侧行链路信息包括完整性保护校验失败指示和第二终端的标识。也即，当第一终端在对接收到的用户面消息进行完整性保护校验失败后，触发第一终端向网络设备上报携带完整性保护校验失败指示和第二终端的标识的侧行链路信息，从而网络设备获知第一终端对接收到的来自第二终端的 RRC 消息完整性保护校验失败。

10 可选的，网络设备获知第一终端对接收到的来自第二终端的用户面消息完整性保护校验失败之后，可以尝试寻找攻击者或者是触发报警等。

15 可选的，第一终端在确定由于用户面消息完整性保护校验失败而丢弃的数据包达到预设的一个阈值时，才触发第一终端向网络设备上报携带完整性保护校验失败指示和第二终端的标识的侧行链路信息。

20 基于上述方案，在第一终端对接收到的用户面消息执行完整性保护校验失败的情况下，第一终端可以向网络设备上报完整性保护校验失败指示和第二终端的标识。由于给定了对接收到的用户面消息执行完整性保护校验失败的情况下的处理机制，使得网络设备可以基于上报的信息去排查第一终端与第二终端之间的单播连接故障，因而可以保障第二终端与第一终端之间的正确通信。

25 需要说明的是，本申请中上述各个实施例可以单独实施例，也可以相互结合实施。具体的，图 4 至图 7 分别对应的实施例中的任意两个或两个以上的实施例都可以相互结合进行实施。

 需要说明的是，本申请上述任一实施例中的第二终端的标识，在具体实现中，比如可以是：第二终端的层 2 标识、或 IP 地址、或用户识别模块(Subscriber Identity Module, SIM)等。

30 参考图 8，为本申请实施例提供的一种终端的结构示意图。该终端用于实现以上实施例中终端（如第一终端或第二终端）的操作。如图 8 所示，该终端包括：天线 810、射频装置 820、信号处理部分 830。天线 810 与射频装置 820 连接。在下行方向上，射频装置 820 通过天线 810 接收网络设备或其他终端发送的信息，将网络设备或其他终端发送的信息发送给信号处理部分 830 进行处理。在上行方向上，信号处理部分 830 对终端的信息进行处理，并发送给射频装置 820，射频装置 820 对终端的信息进行处理后经过天线 810 发送给网络设备或其他终端。

35 信号处理部分 830 用于实现对数据各通信协议层的处理。信号处理部分 830 可以为该终端的一个子系统，则该终端还可以包括其它子系统，例如中央处理子系统，用于实现对终端操作系统以及应用层的处理；再如，周边子系统用于实现与其它设备的连接。信号处理部分 830 可以为单独设置的芯片。可选的，以上的装置可以位于信号处理部分 830。

信号处理部分 830 可以包括一个或多个处理元件 831, 例如, 包括一个主控 CPU 和其它集成电路, 以及包括接口电路 833。此外, 该信号处理部分 830 还可以包括存储元件 832。存储元件 832 用于存储数据和程序, 用于执行以上方法中终端所执行的方法的程序可能存储, 也可能不存储于该存储元件 832 中, 例如, 存储于信号处理部分 830 之外的存储器中, 使用时信号处理部分 830 加载该程序到缓存中进行使用。接口电路 833 用于与装置通信。以上装置可以位于信号处理部分 830, 该信号处理部分 830 可以通过芯片实现, 该芯片包括至少一个处理元件和接口电路, 其中处理元件用于执行以上终端执行的任一种方法的各个步骤, 接口电路用于与其它装置通信。在一种实现中, 实现以上方法中各个步骤的单元可以通过处理元件调度程序的形式实现, 例如该装置包括处理元件和存储元件, 处理元件调用存储元件存储的程序, 以执行以上方法实施例中终端执行的方法。存储元件可以为处理元件处于同一芯片上的存储元件, 即片内存储元件。

在另一种实现中, 用于执行以上方法中终端所执行的方法的程序可以在与处理元件处于不同芯片上的存储元件, 即片外存储元件。此时, 处理元件从片外存储元件调用或加载程序于片内存储元件上, 以调用并执行以上方法实施例中终端执行的方法。

在又一种实现中, 终端实现以上方法中各个步骤的单元可以是被配置成一个或多个处理元件, 这些处理元件设置于信号处理部分 830 上, 这里的处理元件可以为集成电路, 例如: 一个或多个 ASIC, 或, 一个或多个 DSP, 或, 一个或者多个 FPGA, 或者这些类集成电路的组合。这些集成电路可以集成在一起, 构成芯片。

实现以上方法中各个步骤的单元可以集成在一起, 以片上系统(system-on-a-chip, SOC)的形式实现, 该 SOC 芯片, 用于实现以上方法。该芯片内可以集成至少一个处理元件和存储元件, 由处理元件调用存储元件的存储的程序的形式实现以上终端执行的方法; 或者, 该芯片内可以集成至少一个集成电路, 用于实现以上终端执行的方法; 或者, 可以结合以上实现方式, 部分单元的功能通过处理元件调用程序的形式实现, 部分单元的功能通过集成电路的形式实现。

可见, 以上装置可以包括至少一个处理元件和接口电路, 其中至少一个处理元件用于执行以上方法实施例所提供的任一种终端执行的方法。处理元件可以以第一种方式: 即调用存储元件存储的程序的方式执行终端执行的部分或全部步骤; 也可以以第二种方式: 即通过处理器元件中的硬件的集成逻辑电路结合指令的方式执行终端执行的部分或全部步骤; 当然, 也可以结合第一种方式和第二种方式执行终端执行的部分或全部步骤。

这里的处理元件同以上描述, 可以是通用处理器, 例如 CPU, 还可以是被配置成实施以上方法的一个或多个集成电路, 例如: 一个或多个 ASIC, 或, 一个或多个微处理器 DSP, 或, 一个或者多个 FPGA 等, 或这些集成电路形式中至少两种的组合。存储元件可以是一个存储器, 也可以是多个存储元件的统称。

本领域普通技术人员可以理解: 本申请中涉及的第一、第二、第三等各种数字编号仅为描述方便进行的区分, 并不用来限制本申请实施例的范围, 也表示先后顺序。“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。“至少一个”是指一个或者多个。至少两个是指两个或者多个。“至少一个”、“任意一个”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、种), 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。“多个”是指两个或两个以上,其它量词与之类似。

应理解,在本申请的各种实施例中,上述各过程的序号的大小并不意味着执行顺序的先后,各过程的执行顺序应以其功能和内在逻辑确定,而不对本发明实施例的实施过程构成任何限定。

5 所属领域的技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的系统、装置和单元的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

在本申请所提供的几个实施例中,应该理解到,所揭露的系统、装置和方法,可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,所述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组
10 件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络
15 单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外,在本申请各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。

在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时,全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、
20 数字用户线(DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、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括一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质, (例如,软盘、硬盘、磁带)、光介质(例如, DVD)、或者半导体介质(例如固态硬盘(solid state disk, SSD))等。

30 本申请实施例中所描述的各种说明性的逻辑单元和电路可以通过通用处理器, 数字信号处理器, 专用集成电路(ASIC), 现场可编程门阵列(FPGA)或其它可编程逻辑装置, 离散门或晶体管逻辑, 离散硬件部件, 或上述任何组合的设计来实现或操作所描述的功能。通用处理器可以为微处理器, 可选地, 该通用处理器也可以为任何传统的处理器、控制器、微控制器或状态机。处理器也可以通过计算装置的组合来实现, 例如数字信号处理器和微
35 处理器, 多个微处理器, 一个或多个微处理器联合一个数字信号处理器核, 或任何其它类似的配置来实现。

本申请实施例中所描述的方法或算法的步骤可以直接嵌入硬件、处理器执行的软件单元、或者这两者的结合。软件单元可以存储于随机存取存储器(Random Access Memory, RAM)、闪存、只读存储器(Read-Only Memory, ROM)、EPROM 存储器、EEPROM 存
40 储器、寄存器、硬盘、可移动磁盘、CD-ROM 或本领域中其它任意形式的存储媒介中。示

例性地，存储媒介可以与处理器连接，以使得处理器可以从存储媒介中读取信息，并可以向存储媒介存写信息。可选地，存储媒介还可以集成到处理器中。处理器和存储媒介可以设置于 ASIC 中。

5 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。

10 本领域技术人员应该可以意识到，在上述一个或多个示例中，本申请所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是通用或专用计算机能够存取的任何可用介质。

15 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，则本申请也意图包括这些改动和变型在内。

20