

完整性保护失败的处理方法、装置和用户设备

相关申请的交叉引用

本申请主张在 2020 年 5 月 15 日在中国提交的中国专利申请号 No. 202010415321.3 的优先权，其全部内容通过引用包含于此。

技术领域

本申请属于通信技术领域，尤其涉及一种完整性保护失败的处理方法、装置和用户设备。

背景技术

新空口（New Radio, NR）副链路（Sidelink, SL，也可称为侧链路，边链路等）传输主要分广播，组播，单播几种传输形式。目前 NR Sidelink 单播通信已经引入了副链路无线资源控制 Sidelink RRC 信令，用于传输 Sidelink RRC 信令的无线承载称之为副链路信令承载 SL-SRB。为了信令传输的安全性，需要进行副链路信令承载传输的完整性验证。现有技术中，并未有关于副链路信令承载在完整性验证失败情况下的处理方法，使得副链路通信安全性较低。

发明内容

本申请提供一种完整性保护失败的处理方法、装置和用户设备，以解决的相关技术缺少副链路信令承载在完整性验证失败情况下的后续处理方法，以进一步提高副链路通信的安全性。

第一方面，本申请实施例提供一种完整性保护失败的处理方法，用于第一用户设备，所述第一用户设备基于目的地址进行副链路通信，所述完整性保护失败的处理方法包括：

至少在接收到关于副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作。

第二方面，本申请实施例提供一种完整性保护失败的处理装置，用于第

一用户设备，所述第一用户设备基于目的地址进行副链路通信，所述装置包括：

第一执行模块，用于至少在接收到关于副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作。

第三方面，本申请实施例提供一种用户设备，包括：存储器、处理器及存储在该存储器上并可在所述处理器上运行的程序或者指令，所述程序或者指令被所述处理器执行时实现如第一方面所述的完整性保护失败的处理方法中的步骤。

第四方面，本申请实施例提供一种可读存储介质，所述可读存储介质上存储有程序或指令，所述程序或指令被处理器执行时实现如第一方面所述的完整性保护失败的处理方法中的步骤。

本申请实施例中，第一用户设备至少在接收到关于副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作。即第一用户设备在接收到关于副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作，可提高副链路通信的安全性。

附图说明

图 1 是本申请实施例提供的一种完整性保护失败的处理方法的一流程图；

图 2 为用户设备侧的控制平面协议栈结构示意图；

图 3 是本申请实施例提供的一种完整性保护失败的处理方法的另一流程图；

图 4 是本申请实施例提供的一种完整性保护失败的处理装置的结构图；

图 5 是本申请实施例提供的一种用户设备的结构图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

本申请的说明书和权利要求书中的术语“包括”以及它的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。此外，说明书以及权利要求中使用“和/或”表示所连接对象的至少其中之一，例如 A 和/或 B，表示包含单独 A，单独 B，以及 A 和 B 都存在三种情况。

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。

本申请的说明书和权利要求书中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本申请的实施例例如能够以除了在这里图示或描述的那些以外的顺序实施。

首先，应该申明的是，现有技术的 NR Uu 接口上的完整性检测失败的处理流程并不适用于副链路信令承载的完整性验证失败。因为 Uu 接口上的完整性检测失败可以通过重新选择合适的小区的重建安全。然而副链路是建立在一对特定的用户设备(或一对特定的目的地址)上，无法通过其他的 UE(或目的地址)来重建安全。

现有技术的机制无法应用于副链路信令承载的完整性验证失败的处理，也给本发明实施例的实现带来了一定的困难。

图 1 是本申请实施例提供的一种完整性保护失败的处理方法的流程图，如图 1 所示，本申请实施例提供一种完整性保护失败的处理方法，用于第一用户设备，所述第一用户设备基于目的地址进行副链路通信，所述完整性保护失败的处理方法包括：

步骤 101、至少在接收到关于副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作。

如图 2 所示，为用户设备侧的控制平面协议栈结构示意图，其包括物理层(Physical Layer, PHY)、媒体接入控制(Medium Access Control, MAC)层、

无线链路控制（Radio Link Control, RLC）层、分组数据汇聚协议（Packet Data Convergence Protocol, PDCP）层、无线资源控制（Radio Resource Control, RRC）层和非接入层（Non-Access Stratum, NAS）；其中，PDCP 协议层的主要目的是发送或接收对等 PDCP 实体的分组数据，其主要完成以下几方面的功能：IP 包头压缩与解压缩、数据与信令的加密，以及信令的完整性保护。

而完整性保护功能包括完整性保护和完整性验证两个过程。用于 PDCP 实体的完整性保护功能的算法和 KEY 由上层配置。一旦激活安全功能,完整性保护功能即被激活，该功能应用于高层指示的所有 PDCP 协议数据单元（Protocol Data Unit, PDU）。

通过以上描述可以发现，本发明具体实施例中，所述完整性验证失败指示（Integrity Check Failure Indication）可由 PDCP 实体发送，而完整性保护失败的处理方法由无线资源控制（Radio Resource Control, RRC）实体执行。

当应当理解的是，在本申请实施例中，完整性验证失败指示不限于通过 PDCP 实体发送的方式来获取，还可以通过其他途径获取，在此不做限定。只要第一用户设备能够确定发生了副链路信令承载的完整性验证失败，则可以执行安全控制操作，可提高副链路通信的安全性。

换句话说，本发明具体实施例的完整性保护失败的处理方法，用于第一用户设备，所述第一用户设备基于目的地址进行副链路通信，所述完整性保护失败的处理方法包括：

在检测到发生副链路信令承载的完整性验证失败事件的情况下，执行安全控制操作。

而从 PDCP 实体接收到关于副链路信令承载的完整性验证失败指示的情况下，则可以认为检测到发生副链路信令承载的完整性验证失败事件。

本发明具体实施例中，第一用户设备可为手机、电脑、车载用户设备等。目的地址是指与第一用户设备进行单播通信的地址，目标地址可对应第二用户设备，但应当理解的是，第一用户设备可以建立多个副链路通信，也就是说，第一用户设备可以具有多个目的地址。多个目的地址可以对应一个目的用户设备，也可以对应多个目的用户设备。即多个目的地址都对应第二用户设备，也可能分别对应第二用户设备，第三用户设备，...，等等。

本实施例中，第一用户设备至少在接收到关于副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作。即第一用户设备在接收到关于副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作，提高副链路通信的安全性。

本发明具体实施例中，可以通过高层配置或者协议预定义不同的完整性验证失败的判断标准，例如如下列举的不同的完整性验证失败的判断标准：

所述副链路信令承载的任意一个 PDCP PDU 发生完整性验证失败；

累计预定数量的 PDCP PDU 发生完整性验证失败；

连续预定数量的 PDCP PDU 发生完整性验证失败。

如图 3 所示，在本申请一个实施例中，所述完整性保护失败的处理方法还包括：

步骤 102、在检测到副链路无线链路失败的情况下，执行安全控制操作。

步骤 101 与步骤 102 之间不限定先后顺序。第一用户设备可在接收到关于副链路信令承载的完整性验证失败指示的情况下，同时执行安全控制操作，也可在检测到副链路无线链路失败的情况下，执行安全控制操作。

本发明具体实施例的方法可以应用于各种通信制式的副链路通信，当应用于 5G NR 的副链路通信时，在本申请一个实施例中，所述副链路信令承载为副链路信令承载 1（即 SL-SRB1）、副链路信令承载 2（即 SL-SRB2）和副链路信令承载 3（即 SL-SRB3）中的至少一个。即在 SL-SRB1，SL-SRB2，SL-SRB3 中至少一个副链路信令承载上接收到完整性验证失败的情况下，执行安全控制操作。其中，SL-SRB1 用于传输激活安全的 PC5 Signaling (PC5-S) 信令，SL-SRB2 用于传输需要安全保护的 PC5-S 信令，SL-SRB3 用于传输需要安全保护的 PC5 RRC 信令。这里的安全保护指的是加密和完整性保护需求。

也就是说，本发明具体实施例可以应用于部分副链路信令承载，也可以应用于所有副链路信令承载。

完整性保护功能的设置是为了提高通信的安全性，例如防止数据被篡改。当发生完整性验证失败时，此时表明副链路通信不再满足安全性要求，此时可以进行安全控制操作。

本发明具体实施例中，安全控制操作可采用如下三类操作中的一种：

第一类是释放副链路通信的相关承载或连接，其使得副链路通信的传输通道不再存在，从而阻止副链路通信的继续进行。

例如，释放副链路通信的相关承载或连接可以是如下操作中的至少一个：释放所述第一用户设备基于所述目的地址进行副链路通信对应的数据承载；

释放所述第一用户设备基于所述目的地址进行副链路通信对应的信令承载；

释放所述第一用户设备基于所述目的地址进行副链路通信对应的 PC5 接口的 RRC 连接，副链路接口又可以称作 PC5 接口。

第二类是删除副链路信令承载的相关配置信息，使得副链路通信无法发起。

例如，删除副链路信令承载的相关配置信息可以是如下操作中的至少一个：

删除所述第一用户设备基于所述目的地址进行副链路通信对应的配置信息。其中，配置信息可为来自 RRC 信令、PC5 RRC 信令或者预配置（pre-configuration）信令的配置信息。

删除所述第一用户设备基于所述目的地址进行副链路通信对应的安全密钥。

上述的安全密钥包括 K_{NRP} 、 $K_{NRP-scsc}$ 、NRPEK 以及 NRPIK 等。其中， K_{NRP} 是一个在进行 Sidelink 通信的两个用户设备之间共享的根密钥，需要通过 PC5 接口进行交互。通过 K_{NRP} 可以推导出实际安全上下文使用的根密钥 $K_{NRP-scsc}$ 。再进一步通过 $K_{NRP-scsc}$ 推导出加密算法使用的加密密钥 NRPEK 和完整性算法使用的完整性密钥 NRPIK。而第三类是通过停止定时器来阻止副链路通信的进行，例如：

停止所述第一用户设备基于所述目的地址进行副链路通信对应的定时器，或，停止所述第一用户设备进行副链路通信的所有定时器。

上述定时器可包含在配置信息里。

即，所述安全控制操作具体可包括如下操作中的至少一项：

释放所述第一用户设备基于所述目的地址进行副链路通信对应的数据承

载；

释放所述第一用户设备基于所述目的地址进行副链路通信对应的信令承载；

释放所述第一用户设备基于所述目的地址进行副链路通信对应的副链路接口无线资源控制 PC5 RRC 连接；

删除所述第一用户设备基于所述目的地址进行副链路通信对应的配置信息；

删除所述第一用户设备基于所述目的地址进行副链路通信对应的安全密钥；

停止所述第一用户设备基于所述目的地址进行副链路通信对应的定时器，或，停止所述第一用户设备进行副链路通信的所有定时器。

例如，停止 sidelink 通信相关的所有定时器，或者，停止与目的地址进行 sidelink 通信相关的定时器。进一步的，所述定时器至少包括 T400，T400 用于副链路 RRC 重配置流程，在 sidelink UE 发送副链路 RRC 重配置消息的时刻启动。

在本申请一个实施例中，在步骤 101、接收到关于所述副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作之后，还包括：

发送 RRC 消息到网络侧设备，所述 RRC 消息用于上报所述第一用户设备与所述目的地址进行副链路通信失败。

发送到网络侧设备的 RRC 消息可以使用已有的副链路用户设备信息 SidelinkUEInformation 消息。第一用户设备将 RRC 消息发送给网络侧设备，以上报所述第一用户设备与所述目的地址进行副链路通信失败。

当网络侧设备收到该消息后，即可释放分配给第一用户设备基于所述目的地址进行副链路通信的相关资源，减少资源浪费。

进一步的，所述 RRC 消息还用于指示所述副链路通信失败的原因为完整性验证失败，以告知网络侧设备副链路通信失败的原因，可使得网络侧设备能够基于副链路通信失败的原因做更加有针对性的处理，提高处置的准确度。

在本申请一个实施例中，在接收到关于所述副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作之后，还包括：

发送指示信息到所述第一用户设备的上层实体，所述指示信息用于通知所述 PC5 RRC 连接被释放。

本发明具体实施例中，上层实体可以是接入层 Access Stratum (AS) 以上，例如 V2X layer、应用层等实体。

第一用户设备在执行安全控制操作之后，发送指示信息到第一用户设备的上层实体，使得上层实体停止基于目的地址进行的副链路通信，避免了上层实体继续处理和/或发送需通过副链路传输的数据。

进一步的，所述指示信息还用于通知所述 PC5 RRC 连接被释放的原因因为完整性验证失败或 PC5 RRC 连接失败。

在本申请一个实施例中，所述完整性保护失败的处理方法还包括：

发送 PC5 RRC 消息到所述目的地址对应的第二用户设备，所述 PC5 RRC 消息用于指示所述第二用户设备停止基于目的地址进行的副链路通信。

本实施例中的步骤可在第一用户设备执行安全控制操作之前，也可在第一用户设备执行安全控制操作之后，其执行顺序取决于安全控制操作的具体内容。当该发送 PC5 RRC 消息的动作在安全操作之前执行时，则其不受到安全控制操作的具体内容的影响。而当该发送 PC5 RRC 消息的动作在第一用户设备执行安全控制操作之后执行，则第一用户设备执行的安全控制操作不包括释放信令承载的情况，即第一用户设备在执行上文中的至少一项安全控制操作时，不包括释放所述第一用户设备基于所述目的地址进行副链路通信对应的信令承载，由于该信令承载未被释放，此时可利用保留的信令承载来传输 PC5 RRC 消息。

第二用户设备停止基于目的地址进行的副链路通信的操作可包括：释放对应的数据承载（即上文中的释放副链路通信的相关承载或连接），释放对应的配置信息（即上文中的删除副链路信令承载的相关配置信息）等。

第一用户设备将 PC5 RRC 消息发送给第二用户设备，这样，第二用户设备可不用再基于目的地址做数据监听和接收。

进一步的，所述 PC5 RRC 消息携带副链路配置重置指示。该 PC5 RRC 消息可以是 PC5 RRC 专用消息，例如可为 sl-ResetConfig-r16 消息（R16 副链路配置重置消息），通过重用 sl-ResetConfig-r16 消息来通知第二用户设备与所

述目的地址进行副链路通信对应的数据承载和配置都被释放，第二用户设备可不用再基于目的地址做数据监听和接收，因此能够降低用户设备的功耗和处理器资源。

请参见图 4，图 4 是本申请实施例提供的一种完整性保护失败的处理装置的结构图，该装置应用于第一用户设备，所述第一用户设备基于目的地址进行副链路通信，如图 4 所示，完整性保护失败的处理装置 300 包括：

第一执行模块 301，用于至少在接收到关于副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作。

在本申请一个实施例中，所述完整性验证失败指示由分组数据汇聚协议 PDCP 实体发送。

在本申请一个实施例中，完整性保护失败的处理装置 300 还包括：

第二执行模块，用于在检测到副链路无线链路失败的情况下，执行安全控制操作。

在本申请一个实施例中，所述副链路信令承载为副链路信令承载 1、副链路信令承载 2 和副链路信令承载 3 中的至少一个。

在本申请一个实施例中，所述安全控制操作具体包括如下操作中的至少一项：

释放所述第一用户设备基于所述目的地址进行副链路通信对应的数据承载；

释放所述第一用户设备基于所述目的地址进行副链路通信对应的信令承载；

释放所述第一用户设备基于所述目的地址进行副链路通信对应的副链路接口无线资源控制 PC5 RRC 连接；

删除所述第一用户设备基于所述目的地址进行副链路通信对应的配置信息；

删除所述第一用户设备基于所述目的地址进行副链路通信对应的安全密钥；

停止所述第一用户设备基于所述目的地址进行副链路通信对应的定时器，或，停止所述第一用户设备进行副链路通信的所有定时器。

在本申请一个实施例中，完整性保护失败的处理装置 300 还包括：

第一发送模块，用于发送 RRC 消息到网络侧设备，所述 RRC 消息用于上报所述第一用户设备与所述目的地址进行副链路通信失败。

在本申请一个实施例中，所述 RRC 消息还用于指示所述副链路通信失败的原因完整性验证失败。

在本申请一个实施例中，所述装置还包括：

第二发送模块，用于发送指示信息到所述第一用户设备的上层实体，所述指示信息用于通知所述 PC5 RRC 连接被释放。

在本申请一个实施例中，所述指示信息还用于通知所述 PC5 RRC 连接被释放的原因完整性验证失败或 PC5 RRC 连接失败。

在本申请一个实施例中，完整性保护失败的处理装置 300 还包括：

第三发送模块，用于发送 PC5 RRC 消息到所述目的地址对应的第二用户设备，所述 PC5 RRC 消息用于指示所述第二用户设备停止基于目的地址进行的副链路通信。

在本申请一个实施例中，所述 PC5 RRC 消息携带副链路配置重置指示。

本申请实施例提供的完整性保护失败的处理装置 300 能够实现图 1、图 3 的方法实施例中的各个过程，为避免重复，此处不再赘述。本实施例中，第一用户设备至少在接收到关于副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作。即第一用户设备在接收到关于副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作，以提高副链路通信的安全性。

需要说明的是，本申请实施例中的完整性保护失败的处理装置可以是装置，也可以是用户设备中的部件、集成电路、或芯片。

图 5 为实现本申请实施例的一种用户设备的硬件结构示意图。

该用户设备 400 包括但不限于：射频单元 401、网络模块 402、音频输出单元 403、输入单元 404、传感器 405、显示单元 406、用户输入单元 407、接口单元 408、存储器 409、以及处理器 410 等部件。

本领域技术人员可以理解，用户设备 400 还可以包括给各个部件供电的电源（比如电池），电源可以通过电源管理系统与处理器 410 逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。图 5 中示出

的电子设备结构并不构成对电子设备的限定，电子设备可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置，在此不再赘述。

其中，处理器 410，用于至少在接收到关于副链路信令承载的完整性验证失败指示的情况下，执行安全控制操作。

进一步的，所述完整性验证失败指示由分组数据汇聚协议 PDCP 实体发送。

进一步的，处理器 410，还用于在检测到副链路无线链路失败的情况下，执行安全控制操作。

进一步的，所述副链路信令承载为副链路信令承载 1、副链路信令承载 2 和副链路信令承载 3 中的至少一个。

进一步的，所述安全控制操作具体包括如下操作中的至少一项：

释放所述第一用户设备基于所述目的地址进行副链路通信对应的数据承载；

释放所述第一用户设备基于所述目的地址进行副链路通信对应的信令承载；

释放所述第一用户设备基于所述目的地址进行副链路通信对应的副链路接口无线资源控制 PC5 RRC 连接；

删除所述第一用户设备基于所述目的地址进行副链路通信对应的配置信息；

删除所述第一用户设备基于所述目的地址进行副链路通信对应的安全密钥；

停止所述第一用户设备基于所述目的地址进行副链路通信对应的定时器，或，停止所述第一用户设备进行副链路通信的所有定时器。

进一步的，射频单元 401，用于发送 RRC 消息到网络侧设备，所述 RRC 消息用于上报所述第一用户设备与所述目的地址进行副链路通信失败。

进一步的，所述 RRC 消息还用于指示所述副链路通信失败的原因为完整性验证失败。

进一步的，射频单元 401，用于发送指示信息到所述第一用户设备的上层实体，所述指示信息用于通知所述 PC5 RRC 连接被释放。

进一步的，所述指示信息还用于通知所述 PC5 RRC 连接被释放的原因因为完整性验证失败或 PC5 RRC 连接失败。

进一步的，射频单元 401，用于发送 PC5 RRC 消息到所述目的地址对应的第二用户设备，所述 PC5 RRC 消息用于指示所述第二用户设备停止基于目的地址进行的副链路通信。

进一步的，所述 PC5 RRC 消息携带副链路配置重置指示。

可选的，本申请实施例还提供一种用户设备，包括处理器 410，存储器 409，存储在存储器 409 上并可在所述处理器 410 上运行的程序或指令，该程序或指令被处理器 410 执行时实现上述完整性保护失败的处理方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。

本申请实施例另提供了一种芯片，所述芯片包括处理器和通信接口，所述通信接口和所述处理器耦合，所述处理器用于运行程序或指令，实现上述用户设备的完整性保护失败的处理方法实施例的各个过程，且能达到相同的技术效果，为避免重复，此处不再赘述。

应理解，本申请实施例提到的芯片还可以称为系统级芯片、系统芯片、芯片系统或片上系统芯片等。

需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。此外，需要指出的是，本申请实施方式中的方法和装置的范围不限按示出或讨论的顺序来执行功能，还可包括根据所涉及的功能按基本同时的方式或按相反的顺序来执行功能，例如，可以按不同于所描述的次序来执行所描述的方法，并且还可以添加、省去、或组合各种步骤。另外，参照某些示例所描述的特征可在其他示例中被组合。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的

技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台用户设备（可以是手机，计算机，服务器，空调器，或者网络设备等等）执行本申请各个实施例所述的方法。

上面结合附图对本申请的实施例进行了描述，但是本申请并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本申请的启示下，在不脱离本申请宗旨和权利要求所保护的范围情况下，还可做出很多形式，均属于本申请的保护之内。