

侧链路通信方法及装置

技术领域

本公开涉及移动通信技术领域，特别涉及一种侧链路通信方法及装置。

背景技术

在侧链路（SL，sidelink）通信中，远程用户设备（UE，user equipment）利用用于发现过程中使用的的安全参数对直接通信请求（DCR，direct communication request）中用于进行侧链路通信的信息进行加密后，将该直接通信请求发送给 UE 到网络中继设备，而中继设备在接收到该直接通信请求后，需要利用对应的安全参数进行解密以获得用于侧链路通信的信息。然而，在现有技术规范中，并未规定中继设备如何获取对应的安全参数来进行解密。

发明内容

本公开提出了一种侧链路通信方法及装置，UE 在接收到直接通信请求后，能够根据直接通信请求中的目的地层 2 ID 来确定用于对直接通信请求中的加密信息进行解密的安全密钥，有助于实现安全的侧链路通信。

本公开的第一方面实施例提供了一种侧链路通信方法，由 UE 执行，所述方法包括：接收直接通信请求（DCR，direct communication request），其中所述 DCR 包括目的地层 2 标识（ID，identification）以及用于侧链路通信的加密信息；根据所述目的地层 2 ID，确定用于对所述加密信息进行解密的安全密钥；以及利用所述安全密钥对所述加密信息进行解密以便进行侧链路通信。

可选地，所述根据所述目的地层 2 ID，确定用于对所述加密信息进行解密的安全密钥包括：根据所述目的地层 2 ID，从预存储的一条或多条安全上下文中确定与所述目的地层 2 ID 匹配的安全上下文；根据所述匹配的安全上下文，确定所述安全密钥。

可选地，每条安全上下文包括用于标识侧链路通信的服务类型的服务代码、与所述服务代码对应的层 2 ID、以及与所述服务代码相关联的安全密钥。

可选地，所述服务代码包括以下中任一个：中继服务代码 RSC；邻近服务（ProSe，proximity based service）限制代码；ProSe 查询代码；ProSe 响应代码；测距（Ranging）服务代码。

可选地，每条安全上下文还包括以下中任一个或多个：UE 到网络中继层指示符；控制面安全指示符。

可选地，所述方法还包括：根据在发现过程中确定的层 2 ID、服务代码和安全密钥，创建并存储所述安全上下文。

可选地，所述创建并存储所述安全上下文包括以下中任一种：在确定用于所述发现过程的层 2 ID 时，创建并存储所述安全上下文；在发送用于所述发现过程的发现消息后，创建并存储所述安全上下文；在完成所述发现过程后，创建并存储所述安全上下文。

本公开的第二方面实施例提供了一种侧链路通信装置，用于 UE，所述装置包括：收发模块，用于接收直接通信请求 DCR，其中所述 DCR 包括目的地层 2 ID 以及用于侧链路通信的加密信息；处理模块，用于根据所述目的地层 2 ID，确定用于对所述加密信息进行解密的安全密钥；以及利用所述安全密钥对所述加密信息进行解密以便进行侧链路通信。

可选地，所述处理模块用于：根据所述目的地层 2 ID，从预存储的一条或多条安全上下文中确定与所述目的地层 2 ID 匹配的安全上下文；根据所述匹配的安全上下文，确定所述安全密钥。

可选地，每条安全上下文包括用于标识侧链路通信的服务类型的服务代码、与所述服务代码对应的层 2 ID、以及与所述服务代码相关联的安全密钥。

可选地，所述服务代码包括以下中任一个：中继服务代码 RSC；邻近服务（ProSe，proximity based service）限制代码；ProSe 查询代码；ProSe 响应代码；Ranging 服务代码。

可选地，每条安全上下文还包括以下中任一个或多个：UE 到网络中继层指示符；控制面安全指示符。

可选地，所述处理模块还用于：根据在发现过程中确定的层 2 ID、服务代码和安全密钥，创建并存储所述安全上下文。

可选地，所述处理模块用于执行以下任一步：在确定用于所述发现过程的层 2 ID 时，创建并存储所述安全上下文；在发送用于所述发现过程的发现消息后，创建并存储所述安全上下文；在完成所述发现过程后，创建并存储所述安全上下文。

本公开的第三方面实施例提供了一种通信设备，包括：收发器；存储器；处理器，分别与所述收发器及所述存储器连接，配置为通过执行所述存储器上的计算机可执行指令，控制所述收发器的无线信号收发，并能够实现本公开的第一方面所述的方法。

本公开的第四方面实施例提供了一种计算机存储介质，其中，所述计算机存储介质存储有计算机可执行指令；所述计算机可执行指令被处理器执行后，能够实现本公开的第一方面所述的方法。

本公开实施例提供了一种侧链路通信方法及装置，UE接收DCR，其中DCR包括目的地层2 ID和用于侧链路通信的加密信息，根据目的地层2 ID确定安全密钥，以及利用安全密钥对加密信息进行解密以便进行侧链路通信。由此，有助于实现安全的侧链路通信。

本公开附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本公开的实践了解到。

附图说明

本公开上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

- 图1为本公开实施例提供了一种通信系统的架构示意图；
- 图2为根据本公开实施例的一种侧链路通信方法的流程示意图；
- 图3为根据本公开实施例的一种侧链路通信方法的流程示意图；
- 图4为根据本公开实施例的一种侧链路通信方法的流程示意图；
- 图5为根据本公开实施例的模式A发现过程的流程示意图；
- 图6为根据本公开实施例的模式B发现过程的流程示意图；
- 图7为根据本公开实施例的一种侧链路通信装置的框图；
- 图8为本公开实施例提供了一种通信装置的结构示意图；
- 图9为本公开实施例提供了一种芯片的结构示意图。

具体实施方式

下面详细描述本公开的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，旨在用于解释本公开，而不能理解为对本公开的限制。

在本公开实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本公开实施例。在本公开实施例和所附权利要求书中所使用的单数形式的“一种”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

应当理解，尽管在本公开实施例可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本公开实施例范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”及“若”可以被解释成为“在……时”或“当……时”或“响应于确定”。

为了方便理解，以下对本申请实施例涉及的一些内容进行说明：

侧链路 (SL, sidelink)

长期演进 (LTE, Long Term Evolution) 系统从第12个发布版本开始支持侧链路，也可称为旁链路、边链路等，用于UE之间不通过网络设备进行直接数据传输。

LTE侧链路的设计可适用于特定的公共安全事务（例如，火灾场所或地震等灾难场所进行紧急通讯），或车联网 (V2X, Vehicle to Everything) 通信等。车联网通信可以包括各种业务，例如，基本安全类通信，自动驾驶，编队，传感器扩展等等。由于LTE侧链路只支持广播通信，因此主要用于基本安全类通信，其他在时延、可靠性等方面具有严格服务质量 (QoS, Quality of Service) 需求的高级V2X业务将通过新空口 (NR, New Radio) 侧链路支持。

5G 邻近服务 (ProSe, Proximity Service)

ProSe是指设备到设备之间或附近移动设备之间的侧链路通信。通过UE到UE中继，5G ProSe可以进一步扩大侧链路通信的范围。

用户设备到网络中继 (U2N Relay, UE to Network Relay)

U2N中继模式使得无论UE是否在覆盖范围内，UE都可以通过连接另一个中继UE来接入网络。

测距 (Ranging)

测距可用于确定两个或更多个UE之间的距离和/或方向和/或相对位置。

为了更好的理解本申请实施例公开的侧链路通信方法及装置，下面首先对本申请实施例适用的通信系统进行描述。

图1为本公开实施例可应用的一种无线通信系统的框图。无线通信系统包括第一用户设备(UE, user equipment)11、第二UE 12和网络设备13。网络设备与UE之间进行通信的链路为上下行链路，第一UE与第二UE之间的链路是侧链路。

可以理解的是，图1所示的无线通信系统仅是进行示意性说明，无线通信系统中还可包括其它网络设备，例如还可以包括核心网设备、无线中继设备和无线回传设备等，在图1中未示出。本公开实施例对该无线通信系统中包括的网络设备数目和终端数目不做限定。

进一步可以理解的是，本公开实施例的无线通信系统，是一种提供无线通信功能的网络。无线通信系统可以采用不同的通信技术，例如码分多址(code division multiple access, CDMA)、宽带码分多址(wideband code division multiple access, WCDMA)、时分多址(time division multiple access, TDMA)、频分多址(frequency division multiple access, FDMA)、正交频分多址(orthogonal frequency-division multiple access, OFDMA)、单载波频分多址(single carrier FDMA, SC-FDMA)、载波侦听多路访问/冲突避免(carrier sense multiple access with collision avoidance)。根据不同网络的容量、速率、时延等因素可以将网络分为2G(英文: generation)网络、3G网络、4G网络或者未来演进网络，如5G网络，5G网络也可称为是新无线网络(New Radio, NR)。为了方便描述，本公开有时会将无线通信网络简称为网络。

进一步的，本公开中涉及的网络设备也可以称为无线接入网设备。该无线接入网设备可以是:基站、演进型基站(evolved node B, eNB)、家庭基站、无线保真(wireless fidelity, WIFI)系统中的接入点(access point, AP)、无线中继节点、无线回传节点、传输点(transmission point, TP)或者发送接收点(transmission and reception point, TRP)等，还可以为NR系统中的gNB，或者，还可以是构成基站的组件或一部分设备等。当为车联网(V2X)通信系统时，网络设备还可以是车载设备。应理解，本公开的实施例中，对网络设备所采用的具体技术和具体设备形态不做限定。

进一步的，本公开中涉及的UE，也可以称为终端设备、终端、移动台(Mobile Station, MS)、移动终端(Mobile Terminal, MT)等，是一种向用户提供语音和/或数据连通性的设备，例如，终端可以是具有无线连接功能的手持式设备、车载设备等。目前，一些终端的举例为:智能手机(Mobile Phone)、口袋计算机(Pocket Personal Computer, PPC)、掌上电脑、个人数字助理(Personal Digital Assistant, PDA)、笔记本电脑、平板电脑、可穿戴设备、或者车载设备等。此外，当为车联网(V2X)通信系统时，终端设备还可以是车载设备。应理解，本公开实施例对终端所采用的具体技术和具体设备形态不做限定。

可以理解的是，本申请实施例描述的通信系统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，本领域普通技术人员可知，随着系统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。

目前，在侧链路通信中，5G ProSe 远程UE使用用于发现过程的代码接收安全参数对直接通信请求(DCR, direct communication request)中的诸如用户平面Prose远端UE密钥ID(User Plane Prose Remote User Key, UP-PRUK ID)/控制平面Prose远端UE密钥ID(Control Plane Prose Remote User Key, CP-PRUK ID)和服务代码(其标识侧链路通信的服务类型)的信息进行加密，5G ProSe UE到网络的中继设备在接收到DCR后，使用用于发现过程的代码发送安全参数对加密信息进行解密。

为了对DCR中的加密信息进行解密，需要使用与服务代码相关联的代码发送安全参数，然而由于服务代码是加密的，中继设备无法获得对应的代码发送安全参数。因此，如何对DCR中的加密信息进行解密成为亟需解决的问题。

为此，本申请提供了一种侧链路通信方法及装置，UE在接收到DCR后，能够根据直接通信请求中的层2ID来确定用于对DCR中的加密信息进行解密的安全密钥，有助于实现安全的侧链路通信。

请注意，在本公开中提及的代码发送安全参数、代码接收安全参数、代码安全参数包括用于加解密的安全密钥。

下面结合附图对本申请所提供的侧链路通信方法及装置进行详细地介绍。

图2示出了根据本公开实施例的一种侧链路通信方法的流程示意图。如图2所示，该方法可由UE执行，且可以包括以下步骤。

S201，接收直接通信请求(DCR, direct communication request)。

其中，DCR包括目的地层2标识(ID, identification)以及用于侧链路通信的加密信息。

在侧链路通信中，远程UE通过向中继UE发送DCR以请求在远程UE与中继UE之间创建用于进行侧链路通信的PC5链路。远程UE以其自身的层2ID作为源层2ID，以中继UE的层2ID作为目的

地层 2 ID, 向中继 UE 发送 DCR。除了层 2 ID 之外, DCR 还包括用于侧链路通信的加密信息, 以确保安全的侧链路通信。

S202, 根据目的地层 2 ID, 确定用于对加密信息进行解密的安全密钥。

UE 在接收到 DCR 后, 可以根据该 DCR 中包括的目的地层 2 ID 来确定用于对 DCR 中的加密信息进行解密的安全密钥。

S203, 利用安全密钥对加密信息进行解密以便进行侧链路通信。

在确定安全密钥后, UE 可以利用该安全密钥对 DCR 中的加密信息进行解密, 以获得用于侧链路通信的信息, 从而实现侧链路通信。

根据本公开实施例的侧链路通信方法, UE 接收 DCR, 其中 DCR 包括目的地层 2 ID 和用于侧链路通信的加密信息, UE 根据目的地层 2 ID 确定安全密钥并利用安全密钥对加密信息进行解密以便进行侧链路通信。由此, 有助于实现安全的侧链路通信。

图 3 示出了根据本公开实施例的一种侧链路通信方法的流程示意图。如图 3 所示, 该方法可由 UE 执行, 且包括以下步骤。

S301, 接收直接通信请求 DCR。

其中, DCR 包括目的地层 2 ID 以及用于侧链路通信的加密信息。

关于上述步骤 S301 及其相关细节的详细描述, 可以参考关于步骤 S201 及其相关细节的描述, 在此不再赘述。

S302, 根据目的地层 2 ID, 确定用于对加密信息进行解密的安全密钥。

在一些实施例中, 上述步骤 S302 可以包括以下步骤。

S3021, 根据目的地层 2 ID, 从预存储的一条或多条安全上下文中确定与目的地层 2 ID 匹配的安全上下文。

UE 中预存储有至少一条安全上下文。UE 在接收到 DCR 后, 可以根据 DCR 中的目的地层 2 ID, 从至少一条安全上下文中选择与目的地层 2 ID 匹配的安全上下文。应注意, 安全上下文也可被称为发现安全上下文或类似, 在本公开中对此不做限制。

在一些实施例中, 每条安全上下文包括用于标识侧链路通信的服务类型的服务代码、与该服务代码对应的层 2 ID、以及与该服务代码相关联的安全密钥。

作为示例, UE 可以存储有安全上下文的列表, 该列表包括三条安全上下文, 分别为 Context1、Context2 和 Context3。其中 Context1 包括服务代码 1、L2-ID1 (与服务代码 1 对应的层 2 ID) 以及 Key1 (与服务代码 1 相关联的安全密钥); Context2 包括服务代码 2、L2-ID2 (与服务代码 2 对应的层 2 ID) 以及 Key2 (与服务代码 2 相关联的安全密钥); Context3 包括服务代码 3、L2-ID3 (与服务代码 3 对应的层 2 ID) 以及 Key3 (与服务代码 3 相关联的安全密钥)。若 UE 接收到 DCR 中的目的地层 2 ID 为 L2-ID2, 则 UE 可以确定与该目的地层 2 ID 匹配的安全上下文为 Context2。

S3022, 根据匹配的安全上下文, 确定安全密钥。

在确定匹配的安全上下文后, 可以根据该匹配的安全上下文确定安全密钥。

如上述示例, 在确定 Context2 为匹配的安全上下文后, 可以将 Context2 包括的 Key2 作为安全密钥。

S303, 利用安全密钥对加密信息进行解密以便进行侧链路通信。

关于上述步骤 S303 及其相关细节的详细描述, 可以参考关于步骤 S203 及其相关细节的描述, 在此不再赘述。

例如, 在一实际应用中, 5G ProSe U2N 中继在接收到 DCR 后, 使用包括安全密钥的代码发送安全参数对其中的 UP-PRUK ID/CP-PRUK ID 和 RSC 进行解密。其中, 5G ProSe U2N 中继基于安全上下文来获取到代码发送安全参数的安全密钥, 例如, 通过查找包括与 DCR 中的目的地层 2 ID 匹配的层 2 ID 的安全上下文。

此外, 5G ProSe U2N 中继验证 RSC 是否与发现消息中发送的 RSC 匹配。如果不匹配, 则 5G ProSe U2N 中继放弃 PC5 直接链路通信过程。

根据本公开实施例的侧链路通信方法, UE 接收 DCR, 其中 DCR 包括目的地层 2 ID 和用于侧链路通信的加密信息, UE 根据目的地层 2 ID 确定安全密钥并利用安全密钥对加密信息进行解密以便进行侧链路通信。由此, 有助于实现安全的侧链路通信。

在一些实施例中, 服务代码可以包括以下中的任一个: 中继服务代码 (RSC, replay service code)、ProSe 限制代码、ProSe 查询代码、ProSe 响应代码、测距 (Ranging) 服务代码。

在一些实施例中, 每条安全上下文还可以包括以下中的一个或多个: UE 到网络中继层指示符、控制面安全指示符。

UE 到网络中继层指示符用于指示相关联的服务代码是提供 5G ProSe 层 2 中继服务还是 5G ProSe 层 3 中继服务。

如果针对服务代码提供控制面安全指示符, 则对于该服务代码的 UE 到网络中继通信执行基于控制面的安全过程, 否则执行基于用户面的安全过程。

图 4 示出了根据本公开实施例的一种侧链路通信方法的流程示意图。如图 4 所示, 该方法可由 UE 执行, 且包括以下步骤。

S401, 根据在发现过程中确定的层 2 ID、服务代码和安全密钥, 创建并存储安全上下文。

UE 可以根据在发现过程中确定的层 2 ID、服务代码和安全密钥, 创建包括该层 2 ID、服务代码和安全密钥的安全上下文, 并存储该安全上下文。应注意, 安全上下文也可被称为发现安全上下文或类似, 在本公开中对此不做限制。

在一些实施例中, UE 可以在确定用于发现过程中的层 2 ID 时, 创建并存储安全上下文。

在另一些实施例中, UE 可以在发送用于发现过程的发现消息后, 创建并存储安全上下文。

在另一些实施例中, UE 可以在完成发现过程后, 创建并存储安全上下文。

当前限定了两种用于发现过程的模式, 模式 A 和模式 B。

图 5 示出了模式 A 发现过程的流程示意图。在模式 A 中, 两种类型的 UE 参与了 ProSe 直接发现, 分别是:

- 宣告 UE: 宣告特定信息的 UE, 该特定信息可被附近拥有发现权限的 UE 使用。
- 监控 UE: 监听广播消息以发现附近的宣告 UE。

在此模型中, 宣告 UE 广播发现消息, 附近的监控 UE 读取并处理这些消息。

如图 5 所示, 宣告 UE 广播发现消息, 该发现消息可以包括发现消息的类型、标识侧链路通信的服务类型的服务代码 (诸如 ProSe 应用代码或 ProSe 限制代码或中继服务代码)、以及其他元数据等。其中应用层元数据可被作为发现消息中的元数据。发现消息中的内容是被代码发现安全参数或代码安全参数所保护的。

为了实现发现过程, 宣告 UE 自行选择用于发现过程 (诸如 5G ProSe 直接发现/5G ProSe U2N 发现/测距/SL 定位发现过程) 的源层 2 ID, 基于网络配置的信息确定用于发现过程的目的地层 2 ID。

作为一个示例, 宣告 UE 可以在广播发现消息之后, 创建包括自行选择的源层 2 ID、服务代码以及与该服务代码相关联的安全密钥的安全上下文, 并存储该安全上下文。

作为另一示例, 宣告 UE 可以在选择源层 2 ID 后, 创建包括自行选择的源层 2 ID、服务代码以及与该服务代码相关联的安全密钥的安全上下文, 并存储该安全上下文。

作为又一示例, 宣告 UE 可以在完成发现过程后, 创建包括自行选择的源层 2 ID、服务代码以及与该服务代码相关联的安全密钥的安全上下文, 并存储该安全上下文。

图 6 示出了模式 B 发现过程的流程示意图。在模式 B 中, 两种类型的 UE 参与 ProSe 直接发现, 分别是: 。

- 发现者 UE: 发送请求的 UE, 该请求包含关于它感兴趣发现的内容的特定信息。
- 被发现者 UE: 接收到请求消息的 UE 可以回复与发现者的请求相关的一些信息。

发现者 UE 发送关于希望接收到响应的其他 UE 的信息, 例如, 信息可以关于 UE 的标识信息, 信息可以关于 ProSe 查询代码, 信息还可以关于对应于组的 ProSe 应用身份, 并且该组的成员可以响应。

如图 6 所示, 发现者 UE 广播发现消息, 该发现消息可以包括发现消息的类型、标识侧链路通信的服务类型的服务代码 (诸如 ProSe 查询代码或中继服务代码) 等, 发现消息中的内容是被代码发现安全参数或代码安全参数所保护的。

为了实现发现过程, 发现者 UE 自行选择用于发现过程 (诸如 5G ProSe 直接发现/5G ProSe U2N 发现/测距/SL 定位发现) 的源层 2 ID, 基于网络配置确定用于发现过程的目的地层 2 ID。

作为一个示例, 发现者 UE 可以在广播发现消息之后, 创建包括自行选择的源层 2 ID、服务代码以及与该服务代码相关联的安全密钥的安全上下文, 并存储该安全上下文。

作为另一示例, 发现者 UE 可以在选择源层 2 ID 后, 创建包括自行选择的源层 2 ID、服务代码以及与该服务代码相关联的安全密钥的安全上下文, 并存储该安全上下文。

作为又一示例, 发现者 UE 可以在完成发现过程后, 创建包括自行选择的源层 2 ID、服务代码以及与该服务代码相关联的安全密钥的安全上下文, 并存储该安全上下文。

被发现者 UE 在接收到发现消息后, 匹配该发现消息的被发现者 UE 可以向发现者 UE 发送响应消息。响应消息可以包括发现消息的类型、标识侧链路通信的服务类型的服务代码 (诸如 ProSe 响应代码或中继服务代码)、元数据等。其中应用层元数据可被作为发现消息中的元数据。发现消息中的内容是被代码接收安全参数或代码安全参数所保护的。

被发现者 UE 自行选择用于发现过程 (诸如 5G ProSe 直接发现/5G ProSe U2N 发现/测距/SL 定位发现) 的源层 2 ID, 所接收的发现消息的源层 2 ID 被设置为目的地层 2 ID。

作为一个示例, 被发现者 UE 可以在发送响应消息之后, 创建包括自行选择的源层 2 ID、服务代码以及与该服务代码相关联的安全密钥的安全上下文, 并存储该安全上下文。

作为另一示例, 被发现者 UE 可以在选择源层 2 ID 后, 创建包括自行选择的源层 2 ID、服务代码以及与该服务代码相关联的安全密钥的安全上下文, 并存储该安全上下文。

作为又一示例, 被发现者 UE 可以在完成发现过程后, 创建包括自行选择的源层 2 ID、服务代码以及与该服务代码相关联的安全密钥的安全上下文, 并存储该安全上下文。

S402, 接收直接通信请求 DCR。

其中, DCR 包括目的地层 2 ID 以及用于侧链路通信的加密信息。

关于上述步骤 S301 及其相关细节的详细描述, 可以参考关于步骤 S201 及其相关细节的描述, 在此不再赘述。

S403, 根据目的地层 2 ID, 从预存储的一条或多条安全上下文中确定与目的地层 2 ID 匹配的安全上下文。

S404, 根据匹配的安全上下文, 确定安全密钥。

S405, 利用安全密钥对加密信息进行解密以便进行侧链路通信。

关于上述步骤 S402-D405 及其相关细节的详细描述, 可以参考关于步骤 S301-S303 及其相关细节的描述, 在此不再赘述。

根据本公开实施例的侧链路通信方法, UE 接收 DCR, 其中 DCR 包括目的地层 2 ID 和用于侧链路通信的加密信息, UE 根据目的地层 2 ID 确定安全密钥并利用安全密钥对加密信息进行解密以便进行侧链路通信。由此, 有助于实现安全的侧链路通信。

在一些实施例中, 服务代码可以包括以下中的任一个: 中继服务代码 (RSC, replay service code)、ProSe 限制代码、ProSe 查询代码、ProSe 响应代码、测距 (Ranging) 服务代码。

在一些实施例中, 每条安全上下文还可以包括以下中的一个或多个: UE 到网络中继层指示符、控制面安全指示符。

上述本申请提供的实施例中, 从用户设备的角度对本申请实施例提供的方法进行了介绍。为了实现上述本申请实施例提供的方法中的各功能, 用户设备可以包括硬件结构、软件模块, 以硬件结构、软件模块、或硬件结构加软件模块的形式来实现上述各功能。上述各功能中的某个功能可以以硬件结构、软件模块、或者硬件结构加软件模块的方式来执行。

与上述几种实施例提供的侧链路通信方法相对应, 本公开还提供一种侧链路通信装置, 由于本公开实施例提供的侧链路通信装置与上述几种实施例提供的侧链路通信方法相对应, 因此侧链路通信方法的实施方式也适用于本实施例提供的侧链路通信装置, 在本实施例中不再详细描述。

图 7 为本公开实施例提供的一种侧链路通信装置 700 的结构示意图, 该侧链路通信装置 700 可用于 UE。

如图 7 所示, 该装置 700 可以包括收发模块 701。

收发模块 701, 用于接收直接通信请求 DCR, 其中所述 DCR 包括目的地层 2 ID 以及用于侧链路通信的加密信息。

处理模块 702, 用于根据所述目的地层 2 ID, 确定用于对所述加密信息进行解密的安全密钥; 以及利用所述安全密钥对所述加密信息进行解密以便进行侧链路通信。

根据本公开实施例的侧链路通信装置, UE 接收 DCR, 其中 DCR 包括目的地层 2 ID 和用于侧链路通信的加密信息, UE 根据目的地层 2 ID 确定安全密钥并利用安全密钥对加密信息进行解密以便进行侧链路通信。由此, 有助于实现安全的侧链路通信。

在一些实施例, 所述处理模块 702 用于: 根据所述目的地层 2 ID, 从预存储的一条或多条安全上下文中确定与所述目的地层 2 ID 匹配的安全上下文; 根据所述匹配的安全上下文, 确定所述安全密钥。

在一些实施例, 每条安全上下文包括用于标识侧链路通信的服务类型的服务代码、与所述服务代码对应的层 2 ID、以及与所述服务代码相关联的安全密钥。

在一些实施例,所述服务代码包括以下中任一个:中继服务代码 RSC;邻近服务(ProSe, proximity based service)限制代码;ProSe 查询代码;ProSe 响应代码;Ranging 服务代码。

在一些实施例,每条安全上下文还包括以下中任一个或多个:UE 到网络中继层指示符;控制面安全指示符。

在一些实施例,所述处理模块 702 还用于:根据在发现过程中确定的层 2 ID、服务代码和安全密钥,创建并存储所述安全上下文。

在一些实施例,所述处理模块 702 用于执行以下任一步:在确定用于所述发现过程的层 2 ID 时,创建并存储所述安全上下文;在发送用于所述发现过程的发现消息后,创建并存储所述安全上下文;在完成所述发现过程后,创建并存储所述安全上下文。

请参见图 8,图 8 是本申请实施例提供的一种通信装置 800 的结构示意图。通信装置 800 可以是用户设备,也可以是支持网络设备实现上述方法的芯片、芯片系统、或处理器等,还可以是支持用户设备实现上述方法的芯片、芯片系统、或处理器等。该装置可用于实现上述方法实施例中描述的方法,具体可以参见上述方法实施例中的说明。

通信装置 800 可以包括一个或多个处理器 801。处理器 801 可以是通用处理器或者专用处理器等。例如可以是基带处理器或中央处理器。基带处理器可以用于对通信协议以及通信数据进行处理,中央处理器可以用于对通信装置(如,基站、基带芯片,终端设备、终端设备芯片,DU 或 CU 等)进行控制,执行计算机程序,处理计算机程序的数据。

可选的,通信装置 800 中还可以包括一个或多个存储器 802,其上可以存有计算机程序 804,处理器 801 执行所述计算机程序 804,以使得通信装置 800 执行上述方法实施例中描述的方法。可选的,所述存储器 802 中还可以存储有数据。通信装置 800 和存储器 802 可以单独设置,也可以集成在一起。

可选的,通信装置 800 还可以包括收发器 805、天线 806。收发器 805 可以称为收发单元、收发机、或收发电路等,用于实现收发功能。收发器 805 可以包括接收器和发送器,接收器可以称为接收机或接收电路等,用于实现接收功能;发送器可以称为发送机或发送电路等,用于实现发送功能。

可选的,通信装置 800 中还可以包括一个或多个接口电路 807。接口电路 807 用于接收代码指令并传输至处理器 801。处理器 801 运行所述代码指令以使通信装置 800 执行上述方法实施例中描述的方法。

在一种实现方式中,处理器 801 中可以包括用于实现接收和发送功能的收发器。例如该收发器可以是收发电路,或者是接口,或者是接口电路。用于实现接收和发送功能的收发电路、接口或接口电路可以是分开的,也可以集成在一起。上述收发电路、接口或接口电路可以用于代码/数据的读写,或者,上述收发电路、接口或接口电路可以用于信号的传输或传递。

在一种实现方式中,处理器 801 可以存有计算机程序 803,计算机程序 803 在处理器 801 上运行,可使得通信装置 800 执行上述方法实施例中描述的方法。计算机程序 803 可能固化在处理器 801 中,该种情况下,处理器 801 可能由硬件实现。

在一种实现方式中,通信装置 800 可以包括电路,所述电路可以实现前述方法实施例中发送或接收或者通信的功能。本申请中描述的处理器和收发器可实现在集成电路(integrated circuit, IC)、模拟 IC、射频集成电路 RFIC、混合信号 IC、专用集成电路(application specific integrated circuit, ASIC)、印刷电路板(printed circuit board, PCB)、电子设备等上。该处理器和收发器也可以用各种 IC 工艺技术来制造,例如互补金属氧化物半导体(complementary metal oxide semiconductor, CMOS)、N 型金属氧化物半导体(nMetal-oxide-semiconductor, NMOS)、P 型金属氧化物半导体(positive channel metal oxide semiconductor, PMOS)、双极结型晶体管(bipolar junction transistor, BJT)、双极 CMOS(BiCMOS)、硅锗(SiGe)、砷化镓(GaAs)等。

以上实施例描述中的通信装置可以是用户设备,但本申请中描述的通信装置的范围并不限于此,而且通信装置的结构可以不受图 8 的限制。通信装置可以是独立的设备或者可以是较大设备的一部分。例如所述通信装置可以是:

- (1) 独立的集成电路 IC,或芯片,或,芯片系统或子系统;
- (2) 具有一个或多个 IC 的集合,可选的,该 IC 集合也可以包括用于存储数据,计算机程序的存储部件;
- (3) ASIC,例如调制解调器(Modem);
- (4) 可嵌入在其他设备内的模块;

(5) 接收机、终端设备、智能终端设备、蜂窝电话、无线设备、手持机、移动单元、车载设备、网络设备、云设备、人工智能设备等等；

(6) 其他等等。

对于通信装置可以是芯片或芯片系统的情况，可参见图9所示的芯片的结构示意图。图9所示的芯片包括处理器901和接口902。其中，处理器901的数量可以是一个或多个，接口902的数量可以是多个。

可选的，芯片还包括存储器903，存储器903用于存储必要的计算机程序和数据。

本领域技术人员还可以了解到本申请实施例列出的各种说明性逻辑块（illustrative logical block）和步骤（step）可以通过电子硬件、电脑软件，或两者的结合进行实现。这样的功能是通过硬件还是软件来实现取决于特定的应用和整个系统的设计要求。本领域技术人员可以对于每种特定的应用，可以使用各种方法实现所述的功能，但这种实现不应被理解为超出本申请实施例保护的范围。

本申请还提供一种可读存储介质，其上存储有指令，该指令被计算机执行时实现上述任一方法实施例的功能。

本申请还提供一种计算机程序产品，该计算机程序产品被计算机执行时实现上述任一方法实施例的功能。

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程序。在计算机上加载和执行所述计算机程序时，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。所述计算机程序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，所述计算机程序可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber line, DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如，高密度数字视频光盘（digital video disc, DVD））、或者半导体介质（例如，固态硬盘（solid state disk, SSD））等。

本领域普通技术人员可以理解：本申请中涉及的第一、第二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。

本申请中的至少一个还可以描述为一个或多个，多个可以是两个、三个、四个或者更多个，本申请不做限制。在本申请实施例中，对于一种技术特征，通过“第一”、“第二”、“第三”、“A”、“B”、“C”和“D”等区分该种技术特征中的技术特征，该“第一”、“第二”、“第三”、“A”、“B”、“C”和“D”描述的技术特征间无先后顺序或者大小顺序。

如本文使用的，术语“机器可读介质”和“计算机可读介质”指的是用于将机器指令和/或数据提供给可编程处理器的任何计算机程序产品、设备、和/或装置（例如，磁盘、光盘、存储器、可编程逻辑装置（PLD）），包括，接收作为机器可读信号的机器指令的机器可读介质。术语“机器可读信号”指的是用于将机器指令和/或数据提供给可编程处理器的任何信号。

可以将此处描述的系统和技术实施在包括后台部件的计算系统（例如，作为数据服务器）、或者包括中间件部件的计算系统（例如，应用服务器）、或者包括前端部件的计算系统（例如，具有图形用户界面或者网络浏览器的用户计算机，用户可以通过该图形用户界面或者该网络浏览器来与此处描述的系统和技术的实施方式交互）、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信（例如，通信网络）来将系统的部件相互连接。通信网络的示例包括：局域网（LAN）、广域网（WAN）和互联网。

计算机系统可以包括客户端和服务端。客户端和服务端一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务器的关系。

应该理解，可以使用上面所示的各种形式的流程，重新排序、增加或删除步骤。例如，本公开中记载的各步骤可以并行地执行也可以顺序地执行也可以不同的次序执行，只要能够实现本公开公开的技术方案所期望的结果，本文在此不进行限制。

此外，应该理解，本申请所述的各种实施例可以单独实施，也可以在方案允许的情况下与其他实施例组合实施。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，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。

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。

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

权利要求书

- 1、一种侧链路通信方法，其特征在于，所述方法由用户设备 UE 执行，所述方法包括：
接收直接通信请求 DCR，其中所述 DCR 包括目的地层 2 标识 ID 以及用于侧链路通信的加密信息；
根据所述目的地层 2 ID，确定用于对所述加密信息进行解密的安全密钥；以及
利用所述安全密钥对所述加密信息进行解密以便进行侧链路通信。
- 2、如权利要求 1 所述的方法，其特征在于，所述根据所述目的地层 2 ID，确定用于对所述加密信息进行解密的安全密钥包括：
根据所述目的地层 2 ID，从预存储的一条或多条安全上下文中确定与所述目的地层 2 ID 匹配的安全上下文；
根据所述匹配的安全上下文，确定所述安全密钥。
- 3、如权利要求 2 所述的方法，其特征在于，每条安全上下文包括用于标识侧链路通信的服务类型的服务代码、与所述服务代码对应的层 2 ID、以及与所述服务代码相关联的安全密钥。
- 4、如权利要求 3 所述的方法，其特征在于，所述服务代码包括以下中任一个：
中继服务代码 RSC；
邻近服务 ProSe 限制代码；
ProSe 查询代码；
ProSe 响应代码；
测距 Ranging 服务代码。
- 5、如权利要求 3 或 4 所述的方法，其特征在于，每条安全上下文还包括以下中任一个或多个：
UE 到网络中继层指示符；
控制面安全指示符。
- 6、如权利要求 2-5 中任一项所述的方法，其特征在于，还包括：
根据在发现过程中确定的层 2 ID、服务代码和安全密钥，创建并存储所述安全上下文。
- 7、如权利要求 6 所述的方法，其特征在于，所述创建并存储所述安全上下文包括以下中任一种：
在确定用于所述发现过程的层 2 ID 时，创建并存储所述安全上下文；
在发送用于所述发现过程的发现消息后，创建并存储所述安全上下文；
在完成所述发现过程后，创建并存储所述安全上下文。
- 8、一种侧链路通信装置，其特征在于，用于用户设备 UE，所述装置包括：
收发模块，用于接收直接通信请求 DCR，其中所述 DCR 包括目的地层 2 标识 ID 以及用于侧链路通信的加密信息；
处理模块，用于根据所述目的地层 2 ID，确定用于对所述加密信息进行解密的安全密钥；以及利用所述安全密钥对所述加密信息进行解密以便进行侧链路通信。
- 9、如权利要求 8 所述的装置，其特征在于，所述处理模块用于：
根据所述目的地层 2 ID，从预存储的一条或多条安全上下文中确定与所述目的地层 2 ID 匹配的安全上下文；
根据所述匹配的安全上下文，确定所述安全密钥。
- 10、如权利要求 9 所述的装置，其特征在于，每条安全上下文包括用于标识侧链路通信的服务类型的服务代码、与所述服务代码对应的层 2 ID、以及与所述服务代码相关联的安全密钥。
- 11、如权利要求 10 所述的装置，其特征在于，所述服务代码包括以下中任一个：
中继服务代码 RSC；

邻近服务 ProSe 限制代码；
ProSe 查询代码；
ProSe 响应代码；
测距 Ranging 服务代码。

12、如权利要求 10 或 11 所述的装置，其特征在于，每条安全上下文还包括以下中任一个或多个：
UE 到网络中继层指示符；
控制面安全指示符。

13、如权利要求 8-12 中任一项所述的装置，其特征在于，所述处理模块还用于：
根据在发现过程中确定的层 2 ID、服务代码和安全密钥，创建并存储所述安全上下文。

14、如权利要求 13 所述的装置，其特征在于，所述处理模块用于执行以下任一步：
在确定用于所述发现过程的层 2 ID 时，创建并存储所述安全上下文；
在发送用于所述发现过程的发现消息后，创建并存储所述安全上下文；
在完成所述发现过程后，创建并存储所述安全上下文。

15、一种通信设备，其中，包括：收发器；存储器；处理器，分别与所述收发器及所述存储器连接，配置为通过执行所述存储器上的计算机可执行指令，控制所述收发器的无线信号收发，并能够实现权利要求 1-7 任一项所述的方法。

16、一种计算机存储介质，其中，所述计算机存储介质存储有计算机可执行指令；所述计算机可执行指令被处理器执行后，能够实现权利要求 1-7 任一项所述的方法。