

广播消息保护方法及相关装置

技术领域

本申请涉及无线通信技术领域，尤其涉及一种广播消息保护方法及相关装置。

背景技术

无线通信技术中，网络设备空口发送的广播消息是面向小区覆盖范围内的所有终端的，所以，网络设备广播的消息无法使用用户级对称密钥进行加密保护。在初始入网阶段，终端需先接收来自网络设备空口广播的系统消息，才能与网络设备建立通信连接；在小区搜索和同步过程中，终端也需接收来自网络设备空口广播的系统消息后，才能发起随机接入过程，以便接入小区并在该小区正常的工作。

因此，如果网络设备空口发送的广播消息没有任何安全保护，将会对用户带来巨大的损失。例如，若系统消息没有任何安全保护，那么，合法基站发送的系统消息很容易被伪基站窃取与仿冒，比如，伪基站可以先与合法基站完成频率和时间同步，然后，仿冒合法基站特定的系统消息，以更大功率发送仿冒的系统消息，导致终端被伪基站吸附和欺骗。这样，伪基站即可窃取终端中的用户隐私信息，或使得终端无法正常工作，或由于伪基站篡改仿冒系统消息中的重要字段，导致终端主叫能力被禁、无法接收到网络被叫服务、很长时间内无法上网、发短信、拨打电话等等情况。因此，如何对网络设备空口发送的广播消息进行安全保护是一个亟待解决的问题。

发明内容

本申请提供一种广播消息保护方法及相关装置，可对网络设备空口发送的广播消息进行安全保护。

第一方面，本申请提供了一种广播消息保护方法，该方法可由通信装置执行，通信装置可以是通信设备或能够支持通信设备实现该方法所需的功能的通信装置，例如芯片。示例性地，该通信装置为网络设备，或者为设置在网络设备中的用于实现网络设备的功能的芯片，或者为用于实现网络设备的功能的其他部件。以网络设备作为执行主体为例进行阐述。

该方法包括：网络设备生成第一广播消息的完整性保护信息，该完整性保护信息是基于发送第一广播消息的波束的波束索引生成的；发送该第一广播消息的完整性保护信息。

可见，该广播消息保护方法中引入发送广播消息的波束的波束索引生成完整性保护信息，一方面可以波束方向为粒度，对不同波束方向上的广播消息进行保护，另一方面，可防止不同波束方向上的广播消息被重放，从而实现对空口发送的广播消息进行安全保护。

一种可选的实施方式中，该方法还可包括：网络设备发送该第一广播消息在该波束下对应的签名周期，该第一广播消息在该波束下对应的签名周期是该波束下该第一广播消息的完整性保护信息的发送周期。可选的，对于该第一广播消息以波束扫描的方式在 M 个波束上分别发送的情况（ M 为大于 1 的整数），第一广播消息在该 M 个波束中各波束下对应的签名周期可相同或不同，是独立配置的。可选的，不同的广播消息在同一波束下对应的签名周期也可相同或不同。可见，该实施方式中，第一广播消息的完整性保护信息是周期性发送的，从

而可降低发送完整性保护信息所带来的额外空口时频资源开销。

一种可选的实施方式中，该方法还可包括：网络设备接收该第一广播消息的响应信息，该响应信息包括该波束索引和该第一广播消息的完整性保护信息的校验结果；网络设备根据第一广播消息的完整性保护信息的校验结果，调整该第一广播消息在该波束下对应的签名周期。可见，该实施方式中，网络设备可根据广播消息的完整性保护信息的校验结果，对该波束下对应的签名周期进行调整，例如，基于校验结果确定该波束方向可能存在伪基站等攻击者，可缩短签名周期，防范空口攻击；基于校验结果确定该波束方向不存在攻击，可增大签名周期，从而，有利于降低完整性保护信息所带来的额外空口时频资源开销。

可选的，同一波束下，不同广播消息的完整性保护信息可以独立生成，也可联合生成。可选的，同一波束下，该第一广播消息可包括具有相同或不同传输周期的不同广播消息，或者，该第一广播消息可包括具有相同或不同传输周期，以及相同广播发送策略的不同广播消息，或者，该第一广播消息可包括具有相同或不同传输周期、相同广播发送策略以及相同签名周期的不同广播消息。可选的，广播消息中可新增信元表示广播消息的签名周期，或者，在已有信元中添加广播消息的签名周期。可选的，同一波束下，针对完整性保护信息可以联合生成的多条广播消息，该多条广播消息对应的签名周期大于或等于该多条广播消息的传输周期中的最大传输周期。

一种可选的实施方式中，网络设备发送的完整性保护信息，不仅基于该波束的波束索引，还基于发送该第一广播消息的时间戳、下行链路频率和小区标识生成。

一种可选的实施方式中，该第一广播消息的响应信息还包括防重放参数，相应的，该方法还包括：网络设备利用该防重放参数，验证该第一广播消息的响应信息是否为重放消息；若不为重放消息，执行所述的根据该第一广播消息的完整性保护信息的校验结果，调整该第一广播消息在该波束下对应的签名周期的步骤。可见，该实施方式可防止该第一广播消息的响应信息是重放消息。

一种可选的实施方式中，该第一广播消息的响应信息是加密的，该方法还包括：网络设备对该第一广播消息的响应信息进行解密，获得波束索引和该第一广播消息的完整性保护信息的校验结果。从而，提升接收到的校验结果的安全性。

第二方面，本申请还提供一种广播消息保护方法，与第一方面所述的广播消息保护方法相对应，该方法可由通信装置执行，通信装置可以是通信设备或能够支持通信设备实现该方法所需的功能的通信装置，例如芯片。示例性地，该通信装置为终端设备，或者为设置在终端设备中的用于实现终端设备的功能的芯片，或者为用于实现终端设备的功能的其他部件。以终端设备作为执行主体为例进行阐述。该方法包括：终端设备接收第一广播消息的完整性保护信息；终端设备根据接收该第一广播消息的波束的波束索引，对完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

可见，该广播消息保护方法中，终端设备以接收广播消息的波束的波束索引对完整性保护信息进行校验，一方面能够以波束方向为粒度，确认不同波束方向上的广播消息的安全性，另一方面，可防止不同波束方向上的广播消息是被重放的，从而提升空口接收的广播消息的安全性。

一种可选的实施方式中，该方法还可包括：终端设备接收该第一广播消息在该波束下对应的签名周期，该第一广播消息在该波束下对应的签名周期是该波束下该第一广播消息的完整性保护信息的发送周期。可选的，该波束是终端设备接收到该第一广播消息的波束中信号强度最大的波束。可见，该实施方式中，该波束下，第一广播消息的完整性保护信息是周期

性发送的，从而可降低接收完整性保护信息所带来的额外空口时频资源开销。

一种可选的实施方式中，该方法还可包括：终端设备发送该第一广播消息的响应信息，该响应信息包括该波束索引和该第一广播消息的完整性保护信息的校验结果；其中，该第一广播消息的完整性保护信息的校验结果，用于网络设备调整该第一广播消息在该波束下对应的签名周期。可见，该实施方式中，终端设备上报广播消息的完整性保护信息的校验结果，有利于网络设备对该波束下对应的签名周期进行调整。

可选的，同一波束下，不同广播消息的完整性保护信息可以是终端设备分别独立接收的，也可联合接收的。可选的，同一波束下，该第一广播消息可包括具有相同或不同传输周期的不同广播消息，或者，该第一广播消息可包括具有相同或不同传输周期，以及相同广播发送策略的不同广播消息，或者，该第一广播消息可包括具有相同或不同传输周期、相同广播发送策略以及相同签名周期的不同广播消息。可选的，广播消息中可新增信元表示广播消息的签名周期，或者，在已有信元中添加广播消息的签名周期。可选的，同一波束下，针对完整性保护信息可以联合接收的多条广播消息，该多条广播消息对应的签名周期大于或等于该多条广播消息的传输周期中的最大传输周期。

一种可选的实施方式中，终端设备根据接收该第一广播消息的波束的波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果，可具体为：根据接收该第一广播消息的时间戳、下行链路频率、小区标识以及该波束的波束索引，对完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

一种可选的实施方式中，该第一广播消息的响应信息还包括防重放参数，用于网络设备验证该第一广播消息的响应信息是否为重放消息。

一种可选的实施方式中，终端设备发送该第一广播消息的响应信息，包括：对该第一广播消息的响应信息进行加密，获得加密后的第一广播消息的响应信息；发送加密后的该第一广播消息的响应信息。从而，提升校验结果的安全性。

第三方面，本申请提供一种广播消息保护方法，该方法与上述第一方面和第二方面所述的广播消息保护方法相对应，是从网络设备与终端设备交互的角度进行阐述，该部分的有益效果可参见上述第一方面和第二方面中的相关阐述，此处不再详述。另外，该方法以网络设备发送的多个波束中的一个波束，以及该波束的覆盖范围内其中一个终端设备为例进行阐述的。

该方法包括：网络设备生成并发送第一广播消息的完整性保护信息，该完整性保护信息是基于发送第一广播消息的波束的波束索引生成的；终端设备接收该第一广播消息的完整性保护信息；根据接收该第一广播消息的波束的波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

一种可选的实施方式中，该方法还可包括：网络设备发送该第一广播消息在该波束下对应的签名周期，终端设备接收该第一广播消息在该波束下对应的签名周期，该第一广播消息在该波束下对应的签名周期是该波束下该第一广播消息的完整性保护信息的发送周期。

一种可选的实施方式中，该方法还可包括：终端设备发送该第一广播消息的响应信息，网络设备接收该第一广播消息的响应信息，该响应信息包括该波束索引和该第一广播消息的完整性保护信息的校验结果；网络设备根据第一广播消息的完整性保护信息的校验结果，调整该第一广播消息在该波束下对应的签名周期。

一种可选的实施方式中，该第一广播消息包括具有相同或不同传输周期的不同广播消息。

一种可选的实施方式中，网络设备发送的完整性保护信息，不仅基于该波束的波束索引，

还基于发送该第一广播消息的时间戳、下行链路频率和小区标识生成的。相应的，终端设备根据接收该第一广播消息的时间戳、下行链路频率、小区标识以及波束的波束索引，对完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

一种可选的实施方式中，该第一广播消息的响应信息还包括防重放参数，相应的，该方法还包括：网络设备利用该防重放参数，验证该第一广播消息的响应信息是否为重放消息；若不为重放消息，执行所述的根据该第一广播消息的完整性保护信息的校验结果，调整该第一广播消息在该波束下对应的签名周期的步骤。

一种可选的实施方式中，终端设备对该第一广播消息的响应信息进行加密，获得加密后的该第一广播消息的响应信息；终端设备发送加密后的该第一广播消息的响应信息；相应的，网络设备对接收的第一广播消息的响应信息进行解密，获得该第一广播消息的响应信息。

该部分的相关阐述还可参见上述第一方面和第二方面中的阐述，此处不再详述。

第四方面，本申请还提供一种广播消息保护方法，该方法可由通信装置执行，通信装置可以是通信设备或能够支持通信设备实现该方法所需的功能的通信装置，例如芯片。示例性地，该通信装置为网络设备，或者为设置在网络设备中的用于实现网络设备的功能的芯片，或者为用于实现网络设备的功能的其他部件。以网络设备作为执行主体为例进行阐述。该方法包括：发送第一广播消息；接收该第一广播消息的响应信息，该响应信息中包括终端设备接收该第一广播消息的波束的波束索引，以及，终端设备基于该波束索引生成的第一广播消息的完整性保护信息；根据该第一广播消息和该波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整信息保护信息的校验结果。

可见，该广播消息保护方法有利于网络设备基于第一广播消息的完整信息保护信息的校验结果，识别出该波束上的终端设备是否有被伪基站攻击，如被伪基站篡改第一广播消息的内容。

一种可选的实施方式中，该方法还包括：网络设备根据该第一广播消息的完整性保护信息的校验结果，调整第一广播消息在所述波束下对应的签名周期；其中，第一广播消息在该波束下对应的签名周期是该波束下网络设备发送该第一广播消息的完整性保护信息的发送周期。也就是说，该签名周期与终端设备发送的该第一广播消息的完整性保护信息的周期无关。

可见，该实施方式中，网络设备可根据广播消息的完整性保护信息的校验结果，对该波束下对应的签名周期进行调整，例如，基于校验结果确定该波束方向可能存在伪基站等攻击者，可缩短签名周期，防范空口攻击；基于校验结果确定该波束方向不存在攻击，可增大签名周期，从而，有利于降低完整性保护信息所带来的额外空口时频资源开销。

一种可选的实施方式中，该方法还包括：网络设备可发送该第一广播消息在该波束下对应的签名周期。

一种可选的实施方式中，同一波束下，网络设备针对不同广播消息的完整性保护信息可以是独立生成，也可以是联合生成。可选的，同一波束下，网络设备可生成的第一广播消息的完整性保护信息中，该第一广播消息可包括具有相同或不同传输周期的不同广播消息，或者，该第一广播消息可包括具有相同或不同传输周期，以及相同广播发送策略的不同广播消息，或者，该第一广播消息可包括具有相同或不同传输周期、相同广播发送策略以及相同签名周期的不同广播消息。可选的，广播消息中可新增信元表示广播消息的签名周期，或者，在已有信元中添加广播消息的签名周期。可选的，同一波束下，针对完整性保护信息可以联合生成的多条广播消息，该多条广播消息对应的签名周期大于或等于该多条广播消息的传输周期中的最大传输周期。

一种可选的实施方式中，网络设备根据第一广播消息和所述波束索引，对完整性保护信息进行校验，获得第一广播消息的完整信息保护信息的校验结果，具体为：根据该第一广播消息以及发送该第一广播消息的时间戳、下行链路频率、小区标识和波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

一种可选的实施方式中，该响应信息还包括防重放参数，相应的，该方法还包括：网络设备利用防重放参数，验证该第一广播消息的响应信息是否为重放消息；若不为重放消息，执行所述的根据该第一广播消息和该波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整信息保护信息的校验结果的步骤。可见，该实施方式可防止该第一广播消息的响应信息是重放消息。

一种可选的实施方式中，响应信息是加密的，网络设备需对该第一广播消息的响应信息进行解密，获得该波束索引，以及该第一广播消息的完整性保护信息。从而，提升接收到的信息的安全性。

第五方面，本申请还提供一种广播消息保护方法，与第四方面所述的广播消息保护方法相对应，该方法可由通信装置执行，通信装置可以是通信设备或能够支持通信设备实现该方法所需的功能的通信装置，例如芯片。示例性地，该通信装置为终端设备，或者为设置在终端设备中的用于实现终端设备的功能的芯片，或者为用于实现终端设备的功能的其他部件。以终端设备作为执行主体为例进行阐述。

该方法包括：终端设备接收第一广播消息；终端设备生成该第一广播消息的完整性保护信息，该完整性保护信息是基于接收该第一广播消息的波束的波束索引生成的；发送该第一广播消息的响应信息，该响应信息中包括该波束索引，以及，该第一广播消息的完整性保护信息。

可见，该广播消息保护方法中，终端设备可上报第一广播消息的完整性保护信息，有利于网络设备识别出该波束方向上的终端设备是否有被伪基站攻击，如被伪基站篡改第一广播消息的内容。

一种可选的实施方式中，终端设备根据接收该第一广播消息的波束的波束索引，生成该第一广播消息在该波束下的完整性保护信息之前，所述方法还包括：终端设备接收该第一广播消息在所述波束下对应的签名周期。其中，该第一广播消息在该波束下对应的签名周期是该波束下网络设备发送该第一广播消息的完整性保护信息的发送周期。也就是说，该签名周期与终端设备发送的该第一广播消息的完整性保护信息的周期无关。可见，该实施方式中，该波束下，网络设备是周期性发送第一广播消息的完整性保护信息的，从而可降低发送完整性保护信息所带来的额外空口时频资源开销。

一种可选的实施方式中，该第一广播消息包括具有相同或不同传输周期的不同广播消息。一种可选的实施方式中，终端设备发送的完整性保护信息还基于接收该第一广播消息的时间戳、下行链路频率和小区标识生成。

一种可选的实施方式中，响应信息还包括防重放参数，用于网络设备验证该第一广播消息的响应信息是否为重放消息。可见，该实施方式可避免第一广播消息的响应信息是重放消息。

一种可选的实施方式中，终端设备可对该第一广播消息的响应信息进行加密，获得加密后的第一广播消息的响应信息；发送加密后的该第一广播消息的响应信息。可见，该实施方式可提升第一广播消息的响应信息的安全性。

第六方面，本申请提供一种广播消息保护方法，该方法与上述第四方面和第五方面所述

的广播消息保护方法相对应，是从网络设备与终端设备交互的角度进行阐述，该部分的有益效果可参见上述第四方面和第五方面中的相关阐述，此处不再详述。另外，该方法以网络设备发送的多个波束中的一个波束，以及该波束的覆盖范围内其中一个终端设备为例进行阐述的。

该方法包括：网络设备发送第一广播消息；终端设备接收第一广播消息；终端设备生成该第一广播消息的完整性保护信息，该完整性保护信息是基于接收该第一广播消息的波束的波束索引生成的；终端设备发送该第一广播消息的响应信息，相应的，网络设备接收该第一广播消息的响应信息，该响应信息中包括终端设备接收该第一广播消息的波束的波束索引，以及，终端设备基于该波束索引生成的第一广播消息的完整性保护信息；网络设备根据该第一广播消息和该波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整信息保护信息的校验结果。

可见，该广播消息保护方法中，终端设备可上报第一广播消息的完整性保护信息，有利于网络设备识别出该波束方向上的终端设备是否有被伪基站攻击，如被伪基站篡改第一广播消息的内容。例如，对于网络设备在该波束下没有发送第一广播消息的完整性保护信息的情况，终端设备也可主动上报该第一广播消息的完整性保护信息，从而，便于网络设备及时识别出该波束方向上是否有攻击存在，进而提升广播消息的安全性。

一种可选的实施方式中，该方法还包括：网络设备根据该第一广播消息的完整性保护信息的校验结果，调整第一广播消息在所述波束下对应的签名周期；相应的，网络设备可发送该第一广播消息在该波束下对应的签名周期；终端设备接收该第一广播消息在所述波束下对应的签名周期。其中，第一广播消息在该波束下对应的签名周期是该波束下网络设备发送该第一广播消息的完整性保护信息的发送周期。也就是说，该签名周期与终端设备发送的该第一广播消息的完整性保护信息的周期无关。

可见，该实施方式中，网络设备可根据广播消息的完整性保护信息的校验结果，及时对该波束下对应的签名周期进行调整，例如，基于统计周期内校验结果确定该波束方向可能存在伪基站等攻击者，可缩短签名周期，防范空口攻击；基于统计周期内校验结果确定该波束方向不存在攻击，可增大签名周期，从而，有利于降低完整性保护信息所带来的额外空口时频资源开销。

一种可选的实施方式中，同一波束下，网络设备针对不同广播消息发送的完整性保护信息可以是独立生成，也可以是联合生成。

一种可选的实施方式中，终端设备发送的完整性保护信息还基于接收该第一广播消息的时间戳、下行链路频率和小区标识生成。相应的，网络设备根据第一广播消息和所述波束索引，对完整性保护信息进行校验，获得第一广播消息的完整信息保护信息的校验结果，具体为：根据该第一广播消息以及发送该第一广播消息的时间戳、下行链路频率、小区标识和波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

一种可选的实施方式中，响应信息还包括防重放参数，相应的，该方法还包括：网络设备利用防重放参数，验证该第一广播消息的响应信息是否为重放消息；若不为重放消息，执行所述的根据该第一广播消息和该波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整信息保护信息的校验结果的步骤。可见，该实施方式可防止该第一广播消息的响应信息是重放消息。

一种可选的实施方式中，终端设备可对该第一广播消息的响应信息进行加密，获得加密后的第一广播消息的响应信息；终端设备发送加密后的该第一广播消息的响应信息；相应的，

网络设备接收该第一广播消息的响应信息，并对其进行解密，获得该第一广播消息的响应信息。可见，该实施方式可提升第一广播消息的响应信息的安全性。

该部分的相关阐述还可参见上述第四方面和第五方面中的阐述，此处不再详述。

第七方面，本申请提供了一种通信装置，该通信装置可以是网络设备，也可以是网络设备中的装置，或者是能够和网络设备匹配使用的装置。该通信装置的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单元或模块。该单元或模块可以是软件和/或硬件。

可选的，该通信装置包括处理单元和通信单元，执行第一方面所述的方法，其中：

处理单元，用于生成第一广播消息的完整性保护信息，该完整性保护信息是基于发送第一广播消息的波束的波束索引生成的；

通信单元，用于发送该第一广播消息的完整性保护信息。

一种可选的实施方式中，通信单元还用于发送该第一广播消息在该波束下对应的签名周期，该第一广播消息在该波束下对应的签名周期是该波束下该第一广播消息的完整性保护信息的发送周期。

一种可选的实施方式中，通信单元还用于接收该第一广播消息的响应信息，该响应信息包括该波束索引和该第一广播消息的完整性保护信息的校验结果；处理单元还用于根据第一广播消息的完整性保护信息的校验结果，调整该第一广播消息在该波束下对应的签名周期。

一种可选的实施方式中，该第一广播消息的响应信息还包括防重放参数，相应的，处理单元利用该防重放参数，验证该第一广播消息的响应信息是否为重放消息；若不为重放消息，执行根据该第一广播消息的完整性保护信息的校验结果，调整该第一广播消息在该波束下对应的签名周期的操作。

一种可选的实施方式中，该第一广播消息的响应信息是加密的，处理单元还用于对该第一广播消息的响应信息进行解密，获得波束索引和该第一广播消息的完整性保护信息的校验结果。

该通信装置执行的相关操作及有益效果可以参见上述第一方面所述的方法以及有益效果。

可选的，该通信装置包括通信单元和处理单元，执行第四方面所述的方法，其中：

通信单元，用于发送第一广播消息；

通信单元，还用于接收该第一广播消息的响应信息，该响应信息中包括终端设备接收该第一广播消息的波束的波束索引，以及，终端设备基于该波束索引生成的第一广播消息的完整性保护信息；

处理单元，用于根据该第一广播消息和该波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整信息保护信息的校验结果。

一种可选的实施方式中，处理单元还用于根据该第一广播消息的完整性保护信息的校验结果，调整第一广播消息在所述波束下对应的签名周期；其中，第一广播消息在该波束下对应的签名周期是该波束下网络设备发送该第一广播消息的完整性保护信息的发送周期。

一种可选的实施方式中，通信单元还用于发送该第一广播消息在该波束下对应的签名周期。

一种可选的实施方式中，处理单元根据第一广播消息和所述波束索引，对完整性保护信息进行校验，获得第一广播消息的完整信息保护信息的校验结果，具体为：根据该第一广播消息以及发送该第一广播消息的时间戳、下行链路频率、小区标识和波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

一种可选的实施方式中，该响应信息还包括防重放参数，相应的，处理单元利用防重放参数，验证该第一广播消息的响应信息是否为重放消息；若不为重放消息，执行所述的根据该第一广播消息和该波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果的操作。

一种可选的实施方式中，响应信息是加密的，处理单元还需对该第一广播消息的响应信息进行解密，获得该波束索引，以及该第一广播消息的完整性保护信息。

该通信装置执行的相关操作及有益效果可以参见上述第四方面所述的方法以及有益效果。

第八方面，本申请提供了一种通信装置，该通信装置可以是终端设备，也可以是终端设备中的装置，或者是能够与终端设备匹配使用的装置。其中，该通信装置还可以为芯片系统。该通信装置的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单元或模块。该单元或模块可以是软件和/或硬件。

可选的，该通信装置可执行第二方面所述的通信方法，其可包括处理单元和通信单元，其中：

通信单元，用于接收第一广播消息的完整性保护信息；

处理单元，用于根据接收该第一广播消息的波束的波束索引，对完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

一种可选的实施方式中，通信单元还用于接收该第一广播消息在该波束下对应的签名周期，该第一广播消息在该波束下对应的签名周期是该波束下网络设备发送该第一广播消息的完整性保护信息的发送周期。

一种可选的实施方式中，通信单元还用于发送该第一广播消息的响应信息，该响应信息包括该波束索引和该第一广播消息的完整性保护信息的校验结果；其中，该第一广播消息的完整性保护信息的校验结果，用于网络设备调整该第一广播消息在该波束下对应的签名周期。

一种可选的实施方式中，处理单元根据接收该第一广播消息的波束的波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果，可具体为：根据接收该第一广播消息的时间戳、下行链路频率、小区标识以及该波束的波束索引，对完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

一种可选的实施方式中，处理单元还对该第一广播消息的响应信息进行加密，获得加密后的第一广播消息的响应信息；相应的，通信单元具体发送加密后的该第一广播消息的响应信息。

该通信装置执行的操作及有益效果可以参见上述第二方面所述的方法以及有益效果。

可选的，该通信装置可执行第五方面所述的通信方法，其可包括处理单元和通信单元，其中：

通信单元，用于接收第一广播消息；

处理单元，用于生成该第一广播消息的完整性保护信息，该完整性保护信息是基于接收该第一广播消息的波束的波束索引生成的；

通信单元，还用于发送该第一广播消息的响应信息，该响应信息中包括该波束索引，以及，该第一广播消息的完整性保护信息。

一种可选的实施方式中，通信单元，还用于接收该第一广播消息在该波束下对应的签名周期。

一种可选的实施方式中，处理单元还用于对该第一广播消息的响应信息进行加密，获得加密后的第一广播消息的响应信息；具体的，通信单元发送加密后的该第一广播消息的响应

信息。可见，该实施方式可提升第一广播消息的响应信息的安全性。

该通信装置执行的操作及有益效果可以参见上述第五方面所述的方法以及有益效果。

第九方面，本申请提供了一种计算机可读存储介质，所述存储介质中存储有指令，当所述计算机程序或指令被通信装置执行时，实现如第一方面、第二方面、第四方面以及第五方面中任一方面或其任意一种可能的实施方式中所示的方法。

第十方面，本申请提供一种包括指令的计算机程序产品，当通信装置读取并执行该指令时，使得通信装置执行如第一方面、第二方面、第四方面以及第五方面中任一方面或其任意一种可能的实施方式中所示的方法。

第十一方面，本申请提供了一种通信系统，包括至少一个用于执行上述第七方面所述的方法的通信装置，至少一个用于执行上述第八方面所述方法的通信装置。

第十二方面，本申请提供一种电路，该电路与存储器耦合，该电路被用于执行如第一方面、第二方面、第四方面以及第五方面中任一方面或其任意一种可能的实施方式中所示的方法。该电路可包括芯片电路。

附图说明

图 1 是伪基站仿冒广播消息的通信场景示意图；

图 2 是广播消息进行波束扫描场景的示意图；

图 3 是本申请实施例提供的一种生成广播消息的完整性保护信息的示意图；

图 4 是本申请实施例提供的一种生成多条广播消息的完整性保护信息的示意图；

图 5 是本申请实施例提供的一种不同波束下广播消息独立配置签名周期以及同一波束下不同广播消息可联合签名的示意图；

图 6 是本申请实施例提供的一种广播消息保护方法 100 的流程示意图；

图 7 是本申请实施例提供的一种广播消息保护方法 101 的流程示意图；

图 8 是本申请实施例提供的一种广播消息保护方法 200 的流程示意图；

图 9 是本申请实施例提供的一种广播消息保护方法 201 的流程示意图；

图 10 是本申请实施例提供的一种广播消息保护方法 300 的流程示意图；

图 11 是本申请实施例提供的一种通信装置的结构示意图；

图 12 是本申请实施例提供的另一种通信装置的结构示意图。

具体实施方式

本申请实施例中，网络设备也可称为接入网络设备，接入网络设备可以是为终端设备提供无线接入的设备，可以包括无线接入网(radio access network, RAN)设备和接入节点(Access Node, AN)设备。RAN 设备主要是 3GPP 网络中的无线网络设备，AN 设备可以是非 3GPP 定义的接入网络设备。RAN 设备，主要负责空口侧的无线资源管理、服务质量(quality of service, QoS)管理、数据压缩和加密等功能。RAN 设备可以包括各种形式的基站，例如宏基站，微基站(也可称为小站)，中继站，接入点，气球站等。在采用不同的无线接入技术的系统中，具备基站功能的设备的名称可能会有所不同，例如，在长期演进(long term evolution, LTE)系统、第五代(5th generation, 5G)、第六代(6th generation, 6G)甚至第七代(7th generation, 7G)系统中，网络设备可称为：RAN 或者下一代基站(next-generation Node base station, gNB)、演进的节点 B(evolved NodeB, eNB 或 eNodeB)、网络设备控制器(base station controller,

BSC)、网络设备收发台(base transceiver station, BTS)、家庭网络设备(例如, home evolved Node B, 或 home Node B, HNB)、基带单元(baseband unit, BBU)、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、收发节点(transmission and reception point, TRP)、传输点(transmission point, TP)等;或者5G系统中的网络设备的一个或一组(包括多个天线面板)天线面板,或者,还可以为构成gNB或传输点的网络节点,如基带单元(BBU),或,分布式单元(distributed unit, DU),或,车联网(vehicle to everything, V2X)或者智能驾驶场景中的路侧单元(road side unit, RSU)。

在一些部署中,gNB或传输点可以包括集中式单元(centralized unit, CU)和DU等。gNB或传输点还可以包括射频单元(radio unit, RU)。CU实现gNB或传输点的部分功能,DU实现gNB或传输点的部分功能,比如,CU实现无线资源控制(radio resource control, RRC),分组数据汇聚层协议(packet data convergence protocol, PDCP)层的功能,DU实现无线链路控制(radio link control, RLC)、媒体接入控制(media access control, MAC)和物理(physical, PHY)层的功能。由于RRC层的信息最终会变成物理层的信息,或者,由物理层的信息转变而来,因而,在这种架构下,高层信令,如RRC层信令或PDCP层信令,也可以认为是由DU发送的,或者,由DU+RU发送的。可以理解的是,网络设备可以为CU节点、或DU节点、或包括CU节点和DU节点的设备。可选的,网络设备也可以为辅助通信设备,如卫星。

本申请实施例中,终端设备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、穿戴或车载;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)。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、车载终端设备、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、可穿戴终端设备等等。终端有时也可以称为终端设备、用户设备(user equipment, UE)、接入终端设备、车载终端、工业控制终端、UE单元、UE站、移动站、移动台、远方站、远程终端设备、移动设备、UE代理或UE装置等。终端也可以是固定的或者移动的。

本申请可以适用于各种无线接入技术(radio access technology, RAT)的通信系统中,例如可以是LTE通信系统,也可以是5G(或者称为新无线(new radio, NR))通信系统,也可以是LTE通信系统与5G通信系统之间的过渡系统,该过渡系统也可以称为4.5G通信系统,当然也可以是未来的通信系统,如第六代(6th generation, 6G)甚至第七代(7th generation, 7G)系统等。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定,本领域普通技术人员可知,随着通信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。

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”等字样也并不限定一定不同。“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。

无线通信技术中，网络设备空口发送的广播消息是面向小区覆盖范围内的所有终端的，所以，网络设备广播的消息无法使用用户级对称密钥进行加密保护。在初始入网阶段，终端需先接收来自网络设备空口广播的系统消息，才能与网络设备建立通信连接；在小区搜索和同步过程中，终端也需接收来自网络设备空口广播的系统消息后，才能发起随机接入过程，以便接入小区并在该小区正常的工作。

因此，如果网络设备空口发送的广播消息没有任何安全保护，将会对用户带来巨大的损失。例如，若系统消息没有任何安全保护，那么，合法基站发送的系统消息很容易被伪基站窃取与仿冒，如图 1 所示的伪基站仿冒广播消息的通信场景，伪基站 101 可以先与合法基站 102 完成频率和时间同步，然后，仿冒合法基站 102 特定的系统消息，以更大功率发送仿冒的系统消息，导致终端设备 103 被伪基站 101 吸附和欺骗。这样，伪基站 101 即可窃取终端设备 103 中的用户隐私信息，或使得终端设备 103 无法正常工作，或由于伪基站 101 篡改仿冒系统消息中的重要字段，导致终端设备 103 主叫能力被禁、无法接收到网络被叫服务、很长时间内无法上网、发短信、拨打电话等等情况。因此，如何对网络设备空口发送的广播消息进行安全保护是一个亟待解决的问题。

本申请基于波束扫描的场景，提供的广播消息保护方法，可基于波束索引生成对应波束方向上广播消息的完整性保护信息，以提升需要安全保护的广播消息的安全性。

为便于理解本申请，以下对本申请实施例涉及的一些概念进行阐述。

1. 广播消息

本申请中，网络设备与终端设备之间在空口以广播方式发送的消息，统称为广播消息。例如，网络设备与终端设备之间传输的系统消息以及寻呼消息等是以广播方式发送的，即广播消息可以是系统消息或寻呼消息。其中，系统消息可以是主信息块(Master Information Block, MIB)或系统信息块(System Information Block, SIB)。其中，MIB+SIB1 被称为最小系统信息(Minimum System Information, MSI)，MIB 和 SIB1 之外的其他系统信息，如 SIB2 至 SIB12，被称为其他系统信息块(Other System Information, OSI)。SIB1 也被称为剩余最小系统消息(Remaining Minimum System Information, RMSI)。

其中，MIB 携带终端设备接入网络的必要信息，如用于终端设备与网络侧之间进行时间同步的系统帧号(System Frame Number, SFN)、子载波间隔以及指示承载调度 SIB1 的 DCI 的参数配置等。MIB 消息承载在物理广播信道(Physical Broadcast Channel, PBCH)上发送，主同步信号 PSS、辅同步信号 SSS 和广播信道 PBCH 组成一个同步信号块(Synchronization Signal Block, SSB)一起发送，1 个 SSB 在频域上占用 20 个资源块(resource block, RB)，在时域上占用 4 个符号。其中，该符号可以是正交频分复用(Orthogonal Frequency Division Multiplexing, OFDM)符号，1 个 RB 包含 12 个子载波。

其中，SIB1 携带小区接入信息、OSI 的调度信息以及接入限制参数等，OSI 一般包含当前小区的驻留参数，以及重选参数，同频、异频、异系统邻区等参数，此处不再详述。SIB1 和 OSI 在物理下行共享信道(Physical Downlink Shared CHannel, PDSCH)上传输，且传输 SIB1 和 OSI 的 PDSCH 所占的 RB(或频域位置)是动态调度的。

2. 传输周期

本申请中，广播消息是以传输周期进行周期性传输的。本申请中，广播消息的传输周期是指广播消息在层 1 的发送周期。本申请中，MIB 或 SIB1 的传输周期是指 MIB 或 SIB1 在层

1 的重复发送周期；MIB 或 SIB1 的调度传输周期是指该系统信息在层 3 的发送周期，如在各自的调度传输周期内，MIB 或 SIB1 的 RRC 层消息内容不变。例如，MIB 的调度传输周期是 80ms，且该 MIB 可在 80ms 内以 20ms 为周期重复发送，即在 80ms 内重复发送四次，即重复发送周期是 20ms。再例如，SIB1 的调度传输周期是 160ms，重复发送周期是 20ms，即该 SIB1 可在 160ms 内以 20ms 为周期重复发送。可选的，对于其他 SIB 来说，若在层 1 无需重复发送，那么，其他 SIB 的传输周期等于层 3 的调度传输周期。

可选的，网络设备通过系统信息中信元“ssb-periodicityServingCell”，可配置 SSB 周期为 5ms、10ms、20ms、40ms、80ms、160ms。其中，SSB 周期是 SSB 波束扫描周期，在该 SSB 周期内发送多个 SSB，每个 SSB 可对应不同的波束方向，以完成波束扫描。

3. 波束扫描

本申请中，广播消息是以波束扫描的方式发送的。波束扫描是指在特定周期或者时间段内，波束采用预先设定的方向上进行发送和/或接收，以覆盖特定空间区域。例如，图 2 所示的波束扫描场景的示意图，以广播消息是 SSB 为例，假设该 SSB 的波束扫描集合配置 8 个 SSB，每个 SSB 对应一个 SSB 波束或一个 SSB 资源块，从时域上看，在每个 SSB 传输周期的半帧 5ms 内，网络设备会在每个 SSB 波束下发送一个 SSB，发送 8 次 SSB，如 SSB0 至 SSB7，即网络设备采用波束扫描的方式发送 8 个不同波束方向的 SSB，以完成整个小区覆盖的波束扫描。终端设备在系统中移动时会持续的基于 SSB 进行小区搜索和测量，选择合适的 SSB 波束，解析出来一个 SSB 后，可以获取小区标识、系统帧号（System Frame Number，SFN）以及所解析的该 SSB 的 SSB 索引等信息，实现终端设备初始接入和移动性管理。其中，SSB 索引可作为波束索引。1 个 SSB 是指 1 个 SSB 索引对应的 1 个 SSB 资源块或 1 个 SSB 波束。

本申请基于波束扫描的场景，提供一种广播消息保护方法 100，网络设备可基于发送广播消息的波束的波束索引，生成并发送该广播消息的完整性保护信息，相应的，终端设备可接收广播消息的完整性保护信息；并且，终端设备根据接收该广播消息的波束的波束索引，对完整性保护信息进行校验，获得该广播消息的完整性保护信息的校验结果，如识别该广播消息是否安全，或是否来自合法基站。可见，该广播消息保护方法 100 将波束索引作为生成完整性保护信息算法的输入参数，一方面，可对波束粒度上的广播消息进行保护，另一方面，可防止不同波束的广播消息被重放，从而提升广播消息的安全性。

本申请基于波束扫描的场景，还提供一种广播消息保护方法 200，网络设备发送广播消息，终端设备接收该广播消息，并基于接收该广播消息的波束的波束索引生成该广播消息的完整性保护信息；终端设备发送该广播消息的响应信息，该响应信息包括该波束索引和该完整性保护信息；网络设备接收该广播消息的响应信息，并根据该广播消息和该波束索引，对该完整性保护信息进行校验，获得该广播消息的完整信息保护信息的校验结果。可见，该广播消息保护方法 200 能够使得网络设备识别出该波束方向上是否有伪基站攻击，如被伪基站篡改广播消息的内容，从而提升广播消息的安全性。

本申请基于波束扫描的场景，还提供一种广播消息保护方法 300，该广播消息保护方法 300 可包括广播消息保护方法 100 和广播消息保护方法 200。对于网络设备未发送完整性保护信息的广播消息，终端设备接收该广播消息后，可选择生成该广播消息的完整性保护信息，以使得网络设备对该完整性保护信息进行校验，获得该广播消息的完整信息保护信息的校验结果，及时识别出该波束方向上是否有伪基站攻击，如被伪基站篡改广播消息的内容；对于

网络设备发送完整性保护信息的广播消息，终端设备可及时上报校验结果，使得网络设备及时获知终端设备接收的广播消息是否安全，从而提升广播消息的安全性。

可选的，本申请中，网络设备还可发送广播消息在波束下对应的签名周期，广播消息在波束下对应的签名周期是该波束下广播消息的完整性保护信息的发送周期。这样，本申请以签名周期发送广播消息的完整性保护信息，可降低完整性保护信息带来的空口时频资源开销。

可选的，本申请中，网络设备可基于波束下广播消息的完整性保护信息的校验结果，调整广播消息在该波束下对应的签名周期。这样，网络设备可在存在伪基站的波束上缩短签名周期以提升广播消息的安全性，可在不存在伪基站的波束上增大签名周期以降空口时频资源开销。

可选的，本申请针对一个波束下的广播消息所阐述的广播消息保护方法，可适用于广播消息配置的多个扫描波束中部分或全部波束，本申请不做限定。

可选的，用于获得完整性保护信息的安全算法可分为对称方案和非对称方案两类。其中，对称方案是采用对称密钥用于完整性保护，即生成完整性保护信息所使用的密钥，与对完整性保护信息进行校验所使用的密钥相同。该完整性保护信息可以是哈希（HASH）值，或用于完整性的消息认证码（Message Authentication Code for Integrity，MAC-I）；对称方案的安全算法可包括但不限于基于哈希运算的消息认证码-安全散列算法（Hash-based Message Authentication Code-Security Hash Algorithm，HMAC-SHA）2、HMAC-SHA3 等消息认证算法，或者是后量子算法。

非对称方案是采用非对称密钥用于完整性保护，即生成完整性保护信息的密钥与校验完整性保护信息的密钥不同。例如，网络设备利用基站私钥生成完整性保护信息，终端设备利用主公钥以及来自网络设备的基站公钥对完整性保护信息进行校验。其中，核心网设备会生成一对主公钥（Master Public Key，MPK）和主私钥（Master Private Key，MSK），主私钥安全地存储在核心网设备中，主公钥安全地发放给终端设备，可以在终端设备出厂时预置在终端设备中。网络设备与核心网设备基于互联网安全协议（Internet Protocol Security，IPsec）进行双向身份认证后，网络设备向核心网设备发送请求消息，请求消息中包括基站公钥，该请求消息用于请求基站公钥对应的基站私钥，该基站公钥由基站身份标识和有效期组成；核心网设备接收到该请求消息后，根据基站公钥和本地存储的主私钥为基站生成基站私钥，并将该基站私钥发送给网络设备。其中，非对称方案中，完整性保护信息可以是数字签名（digital signature，DS）。非对称方案主要分为两类，一类是基于数字证书或公钥基础设施（Public Key Infrastructure，PKI）的签名保护方案，完整性保护信息需要携带数字签名和数字证书，另一类是基于身份标识的签名保护方案，完整性保护信息需要携带数字签名和身份标识。非对称方案的安全签名算法可包括但不限于椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm，ECDSA）、或者罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）一起提出的 RSA 等经典密码算法，或者基于格（Lattice-based）算法等后量子密码算法。

可选的，广播消息的完整性保护信息，不仅基于发送或接收该广播消息的波束的波束索引，还可基于发送或接收该广播消息的以下一项或多项信息生成：时间戳、下行链路频率和小区标识。可选的，网络设备发送的广播消息与该广播消息的完整性保护信息可以一并发送，也可以相对独立的发送，如另外定义一个消息传输该广播消息的完整性保护信息。可选的，网络设备发送的广播消息不仅可携带完整性保护信息，还可携带该波束索引以及上述一项或多项信息，这些信息可称为防重放参数，用于由终端设备确定该广播消息是否是重放消息。

例如，请参阅图 3，图 3 是本申请实施例提供的一种待发送的广播消息的结构示意图。图 3 以携带完整性保护信息的广播消息为例，如图 3 所示，发送该广播消息时不仅携带该广播消息本身和其完整性保护信息，而且还会携带发送或接收该广播消息的波束的波束索引、下行链路频率和小区标识（如物理小区标识）、时间戳。其中，基于安全算法生成完整性保护信息可以是：将广播消息、时间戳、下行链路频率和小区标识、发送或接收该广播消息的波束的波束索引以及密钥作为安全算法的输入，获得完整性保护信息。其中，待发送的广播消息携带的广播消息本身，或安全算法输入的广播消息本身，可以是该广播消息来自高层的信元，如该广播消息是系统消息的情况，那么，广播消息本身是该系统消息在层 3 的消息内容，该广播消息携带的其他参数可以是物理层增加的参数信息。

可选的，本申请中，完整性保护信息的生成除了基于波束索引外，还可基于其他波束索引信息来代替该波束索引，如与波束索引有映射对应关系的其他参数，如 SSB 索引、该波束下发送广播消息对应的 SFN 或时隙、子帧号等。可选的，该小区标识可以是物理小区标识符（physical cell identifier, PCI）；下行链路频率可以是下行绝对射频信道号（Absolute Radio Frequency Channel Number, DL ARFCN）；时间戳可包括与传输时间（传输时间间隔（transmission time interval, TTI）、子帧、时隙（slot）、微时隙（minislot）等）相对应的年、月、日期、小时、分钟、秒（毫秒或微秒）等信息。可选的，若终端与网络设备的时间同步精确到分钟级，可以选择不传输年/月/日/时，仅传输“分钟 mod 3”的数值和秒的数值，以减少空口传输开销。这样，终端设备侧可以结合截断后的时间戳和广播消息承载发送的系统帧号获得与接入网同步的完整时间。可选的，该时间戳也可以采用时间计数器，时间计数器是协调世界时（Universal Time Coordinated, UTC），如以秒或分钟或其他。时间戳或时间计数器可采用最低有效位（least significant bit, lsb）代替全值。可选的，该时间戳也可采用序列号。

可选的，在小区覆盖范围内，广播消息配置的不同扫描波束下对应的签名周期是独立配置的，并且，网络设备根据终端设备上报的校验结果或完整性保护信息，对相应波束下广播消息的签名周期进行自适应调整。

可选的，同一波束下，具有相同或不同的传输周期的不同广播消息，或者，具有相同或不同传输周期，以及相同广播发送策略的不同广播消息，或者，具有相同或不同传输周期、相同广播发送策略以及相同签名周期的不同广播消息，可联合生成对应的完整性保护信息（也可称为可联合签名）。可选的，广播消息中可新增信元表示广播消息的签名周期，或者，在已有信元中添加广播消息的签名周期。

可选的，同一波束下，针对完整性保护信息可以联合生成多条广播消息，该多条广播消息对应的签名周期大于或等于该多条广播消息的传输周期中的最大传输周期。例如，SIB1 的调度传输周期为 160ms（该调度传输周期内 SIB1 的 RRC 层消息内容不改变），160ms 内网络设备重复发送 8 次（为了不同终端设备能够尽快接入基站，缩小终端设备入网时延的关键指标），即物理层 SIB1 的重复发送周期为 20ms。假设 SIB2 和 SIB4 的传输周期为 320ms；假设 SIB5 的传输周期为 640ms，那么，假设网络设备选择 SIB1、SIB2 以及 SIB4 联合签名，则签名周期需大于或等于 SIB1、SIB2 和 SIB4 的传输周期 20ms、320ms 中的最大值，如签名周期最小可以设置为 320ms。假设网络设备选择 SIB1、SIB2、SIB4 以及 SIB5 联合签名，则签名周期需大于或等于 SIB1、SIB2、SIB4 以及 SIB5 的传输周期 20ms、320ms、640ms 中的最大值，如该签名周期最小可以设置为 640ms。

可选的，多条广播消息联合生成的完整性保护信息可以在每条广播消息中携带传输，或

在其中一条广播消息中携带传输，或可以在最后一条广播消息（即多条广播消息中同一传输周期内时域资源位置最靠后的广播消息）中携带传输，或可以另外定义一个消息携带传输。其中，该多条广播消息也可称为联合签名的广播消息。

请参阅图 4，图 4 是本申请实施例提供的另一种待发送的广播消息的结构示意图。图 4 以完整性保护信息在其中一条广播消息中携带传输为例。如图 4 所示，对于具有相同波束索引、下行链路频率和小区标识的多条广播消息，可联合生成完整性保护信息。与图 3 所示的生成完整性保护信息的方式相比不同之处在于，图 4 所示的安全算法的输入是联合签名的广播消息，即该多条广播消息。如图 4 所示，采用安全算法生成完整性保护信息可以是：将联合签名的广播消息、时间戳、下行链路频率和小区标识、波束索引以及密钥作为安全算法的输入，获得的。

再例如，图 5 是本申请实施例提供的一种独立配置广播消息在不同波束下对应的签名周期以及同一波束下不同广播消息可联合签名的示意图。如图 5 所示，假设 MIB 和 SIB1 具有相同的广播发送策略（如均以广播方式发送）、相同传输周期以及相同的签名周期，可联合签名。如图 5 所示，同一波束 0 下，MIB 和 SIB1 的联合签名（即联合生成的完整性保护信息）可在 SIB1 中以非关键字段中携带，或在新信元中携带，或在该 SIB1 的层 1 或层 2 的载荷（payload）中携带，另外，该波束 0 下，MIB 和 SIB1 对应的签名周期为 N_{00} ；同一波束 0 下，SIB3 和 SIB5 的联合签名（即联合生成的完整性保护信息）可在 SIB5 中以非关键字段中携带，或在新信元中携带，或在该 SIB5 的层 1 或层 2 的载荷（payload）中携带，另外，该波束 0 下，SIB3 和 SIB5 对应的签名周期为 N_{01} 。同一波束 1 下，MIB 和 SIB1 的联合签名（即联合生成的完整性保护信息）可在 SIB1 中以非关键字段中携带，或在新信元中携带，或在该 SIB1 的层 1 或层 2 的载荷（payload）中携带，另外，该波束 1 下，MIB 和 SIB1 对应的签名周期为 N_{10} ；同一波束 1 下，SIB3 和 SIB5 的联合签名（即联合生成的完整性保护信息）可在 SIB5 中以非关键字段中携带，或在新信元中携带，或在该 SIB5 的层 1 或层 2 的载荷（payload）中携带，另外，该波束 1 下，SIB3 和 SIB5 对应的签名周期为 N_{11} 。可见，网络设备可独立配置 MIB 和 SIB1 在不同波束，如波束 0 和波束 1 下，对应的签名周期为 N_{00} 、 N_{10} 。

以下结合附图对本申请实施例提供的广播消息保护方法进行进一步的阐述。

请参阅图 6，图 6 是本申请实施例提供的一种广播消息保护方法 100 的流程示意图。如图 6 所示，该广播消息保护方法 100 可由网络设备生成并发送广播消息的完整性保护信息，该广播消息保护方法 100 可包括但不限于以下步骤：

S101、网络设备生成第一广播消息的完整性保护信息，该完整性保护信息是基于发送该第一广播消息的波束的波束索引生成的；

可选的，网络设备生成第一广播消息的完整性保护信息的方法可参见图 3 至图 5 任一项所述的相关内容，此处不再详述。例如，网络设备采用对称方案生成的完整性保护信息可以是 HASH 值或 MAC-I；网络设备采用非对称方案生成的完整性保护信息可以是数字签名。相应的，第一广播消息可以是一条广播消息如 MIB，也可以是多条广播消息，如 MIB 和 SIB1。

S102、网络设备发送第一广播消息的完整性保护信息，相应的，终端设备接收该第一广播消息的完整性保护信息；

如前文所述，网络设备可将该完整性保护信息携带在第一广播消息中一并发送，或者，与第一广播消息相对独立的发送，此处不再详述。对于网络设备将该波束下的第一广播消息与该波束下第一广播消息的完整性保护信息相对独立的发送的情况，网络设备需也在该波束上发送该第一广播消息的完整性保护信息。

S103、终端设备根据接收该第一广播消息的波束的波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果；

可选的，对于终端设备来说，终端设备可能能够接收到多个波束下的第一广播消息，但该终端设备进行校验的完整性保护信息是该终端设备接收的第一广播消息的信号接收强度最大的波束下第一广播消息的完整性保护信息。

可选的，图3至图4所述的安全算法的输入参数中，时间戳、下行链路频率和小区标识、以及波束索引也可称为防重放参数，以避免终端设备接收的广播消息是重放消息。相应的，网络设备可将该防重放参数与完整性保护信息一并发送给终端设备，终端设备可基于防重放参数以及完整性保护信息验证广播消息是否来自合法基站。

一种可选的实施方式中，若网络设备采用对称方案生成完整性保护信息，则终端设备可基于防重放参数以及完整性保护信息，以及与网络设备侧相同的密钥和相同的安全算法验证第一广播消息是否来自合法基站。具体的，步骤S103可包括：终端设备基于接收的防重放参数（其中包括波束索引）、接收的第一广播消息以及相同的密钥和相同的安全算法，生成完整性保护信息；终端设备校验该生成的完整性保护信息与网络设备发送的完整性保护信息是否一致（即是否完全相同），若一致，则该第一广播消息的完整性保护信息的校验结果是该第一广播消息来自合法基站；若不一致，则该第一广播消息的完整性保护信息的校验结果是该第一广播消息来自非法基站。

另一种可选的实施方式中，若网络设备采用非对称方案生成完整性保护信息，则终端设备可基于防重放参数、完整性保护信息、已有的公钥，验证第一广播消息是否来自合法基站。具体的，步骤S103可包括：终端设备基于接收的防重放参数（其中包括波束索引）、接收的第一广播消息、已有的公钥和已知相同的安全算法对网络设备发送的完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果，如该第一广播消息来自合法基站，或该第一广播消息来自非法基站。

可见，该广播消息保护方法100将波束索引作为生成完整性保护信息算法的输入参数，一方面，可对波束粒度上的广播消息进行保护，另一方面，可防止不同波束的广播消息被重放，从而提升广播消息的安全性。

请参阅图7，图7是本申请实施例提供的一种广播消息保护方法101的流程示意图。图7所示的广播消息保护方法101与图6所示的广播消息保护方法100的不同之处在于，该广播消息保护方法101中，网络设备可发送广播消息在波束下对应的签名周期，以及基于该波束下广播消息的完整性保护信息的校验结果，调整广播消息在该波束下对应的签名周期。如图7所示，该广播消息保护方法101可包括但不限于以下步骤：

S101、网络设备生成第一广播消息的完整性保护信息，该完整性保护信息是基于发送该第一广播消息的波束的波束索引生成的；

S102、网络设备发送第一广播消息的完整性保护信息以及该第一广播消息对应的签名周期，相应的，终端设备接收该第一广播消息的完整性保护信息以及该波束下该第一广播消息对应的签名周期；

如前文所述，该签名周期可携带于第一广播消息中发送，如新增信元或已有信元等，此处不再详述，该波束下第一广播消息的完整性保护信息可与第一广播消息一并携带发送，也可分开发送。对于终端设备来说，终端设备可基于该签名周期，周期性接收对应波束下第一广播消息的完整性保护信息。

S103、终端设备根据接收该第一广播消息的波束的波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果；

可选的，步骤 S101 至 S103 的相关内容还可参见图 6 所述的广播消息保护方法 100，此处不再详述。

S104、终端设备发送该第一广播消息的响应信息，相应的，网络设备接收该第一广播消息的响应信息，该响应信息包括该波束索引和该第一广播消息的完整性保护信息的校验结果；

可选的，终端设备可选择对响应信息进行加密后反馈给网络设备。例如，终端设备在无线资源控制（radio resource control, RRC）连接态下，可以选择用对称密钥加密响应信息，或者在 RRC 非连接态下选择使用基站公钥加密响应信息。相应的，网络设备需采用对应的密钥解密接收的响应信息，获得第一广播消息的完整性保护信息的校验结果。

可选的，响应信息包括的校验结果可以是用于指示该校验结果的指示信息。可选的，若校验结果是校验失败，则该响应信息中还可包括签名获取指示，用于请求网络设备在该波束上再次发送该广播消息时需生成并发送完整性保护信息。

可选的，终端设备可采用如下信令发送响应信息，比如随机接入过程中的消息，消息（Message, MSG）3（RRC 建立请求（RRCSetupRequest）消息），MSG5（RRC 建立完成（RRCSetupComplete）消息），注册请求（RegistrationRequest）消息，非接入层身份响应（NAS Identity Response）消息，认证响应（AuthenticationResponse）消息，非接入层安全模式完成（NAS SecurityModeComplete）消息，接入层安全模式完成（AS SecurityModeComplete）消息、测量上报（MeasurementReport）消息等；终端设备也可以采用重新定义的新消息类型，发送响应信息。

S105、网络设备根据第一广播消息的完整性保护信息的校验结果，调整该第一广播消息在该波束下对应的签名周期。

可选的，若第一广播消息的完整性保护信息的校验结果是终端设备识别第一广播消息来自合法基站或是安全的，则可增大该第一广播消息在该波束下对应的签名周期；若第一广播消息的完整性保护信息的校验结果是终端设备识别第一广播消息来自非法基站或是被篡改的，则可减小该第一广播消息在该波束下对应的签名周期。

可选的，网络设备也可对统计周期内该波束下第一广播消息的完整性保护信息的校验结果进行统计分析，以适应性调整该波束下该第一广播消息对应的签名周期。例如，统计周期内，该波束下第一广播消息的完整性保护信息的校验结果中成功率高，则增大该波束下第一广播消息对应的签名周期，成功率低，则减小该波束下第一广播消息对应的签名周期。可选的，该波束下第一广播消息的完整性保护信息的校验结果中成功率高可以是：校验成功的校验结果在该统计周期内所有校验结果中所占比例大于或等于一阈值；该波束下第一广播消息的完整性保护信息的校验结果中成功率低可以是：校验成功的校验结果在该统计周期内所有校验结果中所占比例小于该阈值。可选的，该阈值可以是系统预设的或信令指示的，本申请不做限定。

可见，该广播消息保护方法 101 不仅可引入波束索引，提升波束方向上的广播消息的安全性，还可适应性调整该波束下广播消息对应的签名周期，从而获得广播消息的安全性和所需的空口时频资源开销之间的平衡。

请参阅图 8，图 8 是本申请实施例提供的一种广播消息保护方法 200 的流程示意图。如图 8 所示，该广播消息保护方法 200 可由终端设备生成并发送广播消息的完整性保护信息，

该广播消息保护方法 200 可包括但不限于以下步骤：

S201、网络设备发送第一广播消息；相应的，终端设备接收第一广播消息；

S202、终端设备生成该第一广播消息的完整性保护信息，该完整性保护信息是基于接收该第一广播消息的波束的波束索引生成的；

可选的，对于终端设备来说，终端设备可能能够接收到多个波束下的该第一广播消息，但该终端设备生成的完整性保护信息是该终端设备接收的第一广播消息的信号接收强度最大的波束下第一广播消息的完整性保护信息。

可选的，终端设备生成第一广播消息的完整性保护信息的方法可参见图 3 至图 5 任一项所述的相关内容，此处不再详述。另外，该方法中，终端设备采用前文所述的对称方案生成第一广播消息的完整性保护信息，该完整性保护信息可以是 HASH 值或 MAC-I。

S203、终端设备发送该第一广播消息的响应信息，相应的，网络设备接收该第一广播消息的响应信息，该响应信息中包括该波束的波束索引，以及，终端设备生成的第一广播消息的完整性保护信息；

可选的，终端设备可选择对响应信息进行加密后反馈给网络设备。例如，终端设备在无线资源控制（radio resource control, RRC）连接态下，可以选择用对称密钥加密响应信息，或者在 RRC 非连接态下选择使用基站公钥加密响应信息。相应的，网络设备可对该响应信息进行解密，获得响应信息携带的波束索引，以及，该波束下第一广播消息的完整性保护信息。

可选的，获得完整性保护信息所采用的安全算法的输入参数中，时间戳、下行链路频率和小区标识、以及波束索引也可称为防重放参数，相应的，终端设备可将该防重放参数与完整性保护信息一并发送给网络设备，网络设备可基于防重放参数判断该第一广播消息的响应信息是否为重放消息，如果不是，则解密响应信息。

其中，第一广播消息在该波束下对应的签名周期是该波束下网络设备发送该第一广播消息的完整性保护信息的发送周期。也就是说，该签名周期与终端设备发送的第一广播消息的完整性保护信息的周期无关，例如，终端设备可自己确定是否上报第一广播消息的完整性保护信息。

可选的，终端设备接收到该广播消息未携带完整性保护信息，可在响应信息中携带签名获取指示，用于请求网络设备在该波束上再次发送该广播消息时需生成并发送完整性保护信息。

可选的，终端设备可采用上述所述的各种消息或信令发送响应信息，此处不再详述。

S204、网络设备根据该第一广播消息和该波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整信息保护信息的校验结果。

该方法中，网络设备基于防重放参数以及完整性保护信息，以及与终端设备侧相同的密钥和相同的安全算法验证第一广播消息是否来自合法基站。具体的，步骤 S204 可包括：网络设备基于接收的防重放参数（其中包括波束索引）、发送的第一广播消息以及相同的密钥和相同的安全算法，生成完整性保护信息；网络设备校验该生成的完整性保护信息与终端设备发送的完整性保护信息是否一致，若一致，则该第一广播消息的完整性保护信息的校验结果是校验成功或终端设备接收的第一广播消息未被篡改；若不一致，则该第一广播消息的完整性保护信息的校验结果是校验失败或终端设备接收的第一广播消息已被篡改。

可见，该广播消息保护方法 200 将波束索引作为生成完整性保护信息算法的输入参数，能够使得网络设备识别出该波束方向上是否有伪基站攻击，如被伪基站篡改广播消息的内容，从而提升广播消息的安全性。

请参阅图 9，图 9 是本申请实施例提供的一种广播消息保护方法 201 的流程示意图。图 9 所示的广播消息保护方法 201 与图 8 所示的广播消息保护方法 200 的不同之处在于，该广播消息保护方法 201 中，网络设备可发送广播消息在波束下对应的签名周期，以及基于该波束下广播消息的完整性保护信息的校验结果，调整广播消息在该波束下对应的签名周期。如图 9 所示，该广播消息保护方法 201 可包括但不限于以下步骤：

S201、网络设备发送第一广播消息以及该第一广播消息对应的签名周期；相应的，终端设备接收第一广播消息以及该第一广播消息对应的签名周期；

如前文所述，该波束下该第一广播消息对应的签名周期可携带在第一广播消息中，此处不再详述。

S202、终端设备生成该第一广播消息的完整性保护信息，该完整性保护信息是基于接收该第一广播消息的波束的波束索引生成的；

S203、终端设备发送该第一广播消息的响应信息，相应的，网络设备接收该第一广播消息的响应信息，该响应信息中包括终端设备接收该第一广播消息的波束的波束索引，以及，终端设备基于该波束索引生成的第一广播消息的完整性保护信息；

S204、网络设备根据该第一广播消息和该波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整信息保护信息的校验结果。

可选的，步骤 S201 至 S204 的相关阐述可参见图 8 所述的广播消息保护方法 200，此处不再详述。

S205、网络设备根据该第一广播消息的完整性保护信息的校验结果，调整第一广播消息在所述波束下对应的签名周期。

相应的，网络设备可发送调整后的，该第一广播消息在该波束下对应的签名周期；相应的，终端设备接收调整后的，该第一广播消息在所述波束下对应的签名周期。

可选的，网络设备也可对统计周期内该波束下第一广播消息的完整性保护信息的校验结果进行统计分析，以适应性调整该波束下该第一广播消息对应的签名周期。例如，统计周期内，该波束下第一广播消息的完整性保护信息的校验结果中校验成功率高，则增大该波束下第一广播消息对应的签名周期，校验成功率低，则减小该波束下第一广播消息对应的签名周期。

可见，该广播消息保护方法 201 不仅可引入波束索引由终端设备生成完整性保护信息，使得网络设备识别出该波束方向上是否有伪基站攻击，如被伪基站篡改广播消息的内容，而且，网络设备还可调整自身在该波束下发送第一广播消息的完整性保护信息的签名周期，从而获得广播消息的安全性和所需的空口时频资源开销之间的平衡。

请参阅图 10，图 10 是本申请实施例提供的一种广播消息保护方法 300 的流程示意图。如图 10 所示，该广播消息保护方法 300 可不仅可由网络设备生成并发送广播消息的完整性保护信息，而且还可由终端设备生成并发送广播消息的完整性保护信息，以同一波束 i 下的同一条广播消息，网络设备在不同时刻发送为例，假设该广播消息 P （比如系统消息 SIB1）在不同发送时刻 j 、时刻 k 、时刻 m 可以分别表示为广播消息 $P(j)$ 、 $P(k)$ 、 $P(m)$ 。广播消息 $P(j)$ 、 $P(k)$ 、 $P(m)$ 携带的签名周期可能不同，分别表示为 $\text{Period}(j)$ 、 $\text{Period}(k)$ 、 $\text{Period}(m)$ 。其中，在该广播消息保护方法 300 可包括但不限于以下步骤：

S301、网络设备在时刻 j ，在波束 i 下发送广播消息 $P(j)$ ，相应的，终端设备接收该广播

消息 $P(j)$;

其中,假设终端设备接收的各波束方向上的该条广播消息,该波束 i 上的信号强度最大。另外,该广播消息 $P(j)$ 携带签名周期 $Period(j)$ 。

S302、终端设备生成该广播消息 $P(j)$ 的完整性保护信息 $Int(j)$,该完整性保护信息 $Int(j)$ 是基于接收该广播消息 $P(j)$ 的波束 i 的波束索引生成的;

其中,终端设备生成该广播消息 $P(j)$ 的完整性保护信息 $Int(j)$ 的方法可参见前文所述的对称方案,此处不再详述。

S303、终端设备发送该广播消息 $P(j)$ 的响应信息 $Resp(j)$,相应的,网络设备接收该广播消息 $P(j)$ 的响应信息 $Resp(j)$,该响应信息 $Resp(j)$ 中包括该波束 i 的波束索引,以及,该广播消息 $P(j)$ 的完整性保护信息 $Int(j)$;

S304、网络设备根据发送的该广播消息 $P(j)$ 和该波束 i 的波束索引,对该完整性保护信息 $Int(j)$ 进行校验,获得该广播消息 $P(j)$ 的完整信息保护信息 $Int(j)$ 的校验结果 $check(j)$;

S305、网络设备根据该广播消息 $P(j)$ 的完整性保护信息 $Int(j)$ 的校验结果 $check(j)$,调整该条广播消息在该波束 i 下对应的签名周期 $Period(j)$ 到签名周期 $Period(k)$ 。

可选的,步骤 S305 中,网络设备可根据时刻 j 至时刻 k 之间,这一统计周期内,该广播消息 P 的完整性保护信息的校验结果,调整签名周期,以获得时刻 k ,在波束 i 下发送广播消息 $P(k)$ 所需携带的签名周期 $Period(k)$ 。

S306、网络设备在时刻 k ,在波束 i 下发送广播消息 $P(k)$,相应的,终端设备接收该广播消息 $P(k)$;

其中,该广播消息 $P(k)$ 携带签名周期 $Period(k)$ 以及网络设备生成的该广播消息 $P(k)$ 的完整信息保护信息 $Int(k)$ 。假设终端设备接收的各波束方向上的该条广播消息,该波束 i 上的信号强度最大。

S307、终端设备根据接收该广播消息 $P(k)$ 的波束 i 的波束索引,对该完整性保护信息 $Int(k)$ 进行校验,获得该广播消息 $P(k)$ 的完整性保护信息 $Int(k)$ 的校验结果 $check(k)$;

S308、终端设备发送该广播消息 $P(k)$ 的响应信息 $Resp(k)$,网络设备接收该广播消息 $P(k)$ 的响应信息 $Resp(k)$,该响应信息 $Resp(k)$ 包括该波束 i 的波束索引和该广播消息 $P(k)$ 的完整性保护信息 $Int(k)$ 的校验结果 $check(k)$;

S309、网络设备在时刻 m ,在波束 i 下发送广播消息 $P(m)$,相应的,终端设备接收该广播消息 $P(m)$ 。

其中,该广播消息 P 可基于自身配置的传输周期发送,不限于图 10 举例的三个广播消息 $P(i)$ 至 $P(m)$ 。

其中,该广播消息 $P(m)$ 携带签名周期 $Period(m)$,还携带网络设备生成的该广播消息 $P(m)$ 的完整信息保护信息 $Int(m)$;或者,该广播消息 $P(m)$ 携带签名周期 $Period(m)$,但不携带该广播消息 $P(m)$ 的完整信息保护信息 $Int(m)$ 。假设终端设备接收的各波束方向上的该条广播消息,该波束 i 上的信号强度最大。

可见,该广播消息保护方法 300 中,对于网络设备未发送完整性保护信息的广播消息 $P(j)$,终端设备接收该广播消息 $P(j)$ 后,可选择生成该广播消息 $P(j)$ 的完整性保护信息 $Int(j)$,以使得网络设备对该完整性保护信息 $Int(j)$ 进行校验,获得该广播消息 $P(j)$ 的完整信息保护信息 $Int(j)$ 的校验结果 $check(j)$,及时识别出该波束方向上是否有伪基站攻击,如被伪基站篡改广播消息的内容;对于网络设备发送了完整性保护信息 $Int(k)$ 的广播消息 $P(k)$,终端设备可及时上报校验结果 $check(k)$,使得网络设备及时获知该波束下广播消息 P 是否安全,从而提升广播消息

的安全性。

可以理解的是，为了实现上述实施例中功能，网络设备和终端设备包括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，结合本申请中所公开的实施例描述的各示例的单元及方法步骤，本申请能够以硬件或硬件和计算机软件相结合的形式来实现。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场景和设计约束条件。

图 11 和图 12 为本申请的实施例提供的可能的通信装置的结构示意图。这些通信装置可以用于实现上述方法实施例中网络设备或终端设备的功能，因此也能实现上述方法实施例所具备的有益效果。在本申请的实施例中，该通信装置可以是前文所述的具有无线收发功能的任一可能的终端设备，也可以是前文所述的能够为终端设备提供无线接入的任一可能的网络设备，还可以是应用于网络设备或终端设备的模块（如芯片）。

如图 11 所示，该通信装置包括处理单元 410 和通信单元 420。该通信装置用于实现上述图 3 至图 10 中任一所示的实施例及其实施方式中网络设备或终端设备的功能。例如：

当该通信装置用于实现图 6 或图 7 所示的方法实施例中网络设备的功能时：

处理单元 410 用于生成第一广播消息的完整性保护信息，该完整性保护信息是基于发送第一广播消息的波束的波束索引生成的；通信单元 420 用于发送该第一广播消息的完整性保护信息。

一种可选的实施方式中，通信单元 420 还用于发送该第一广播消息在该波束下对应的签名周期，该第一广播消息在该波束下对应的签名周期是该波束下该第一广播消息的完整性保护信息的发送周期。

一种可选的实施方式中，通信单元 420 还用于接收该第一广播消息的响应信息，该响应信息包括该波束索引和该第一广播消息的完整性保护信息的校验结果；处理单元 410 还用于根据第一广播消息的完整性保护信息的校验结果，调整该第一广播消息在该波束下对应的签名周期。

一种可选的实施方式中，该第一广播消息的响应信息还包括防重放参数，相应的，处理单元 410 利用该防重放参数，验证该第一广播消息的响应信息是否为重放消息；若不为重放消息，执行根据该第一广播消息的完整性保护信息的校验结果，调整该第一广播消息在该波束下对应的签名周期的操作。

一种可选的实施方式中，该第一广播消息的响应信息是加密的，处理单元 410 还用于对该第一广播消息的响应信息进行解密，获得该第一广播消息的完整性保护信息的校验结果。

当该通信装置用于实现图 6 或图 7 所示的方法实施例中终端设备的功能时：

通信单元 420，用于接收第一广播消息的完整性保护信息；处理单元 410，用于根据接收该第一广播消息的波束的波束索引，对完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

一种可选的实施方式中，通信单元 420 还用于接收该第一广播消息在该波束下对应的签名周期，该第一广播消息在该波束下对应的签名周期是该波束下网络设备发送该第一广播消息的完整性保护信息的发送周期。

一种可选的实施方式中，通信单元 420 还用于发送该第一广播消息的响应信息，该响应信息包括该波束索引和该第一广播消息的完整性保护信息的校验结果；其中，该第一广播消息的完整性保护信息的校验结果，用于网络设备调整该第一广播消息在该波束下对应的签名

周期。

一种可选的实施方式中，处理单元 410 根据接收该第一广播消息的波束的波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果，可具体为：根据接收该第一广播消息的时间戳、下行链路频率、小区标识以及该波束的波束索引，对完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

一种可选的实施方式中，处理单元 410 还对该第一广播消息的响应信息进行加密，获得加密后的第一广播消息的响应信息；相应的，通信单元 420 具体发送加密后的该第一广播消息的响应信息。

有关上述处理单元 410 和通信单元 420 更详细的描述可以直接参考图 6 或图 7 所示的方法实施例中相关描述直接得到，这里不加赘述。

当该通信装置用于实现图 8 或图 9 所示的方法实施例中网络设备的功能时：

通信单元 420，用于发送第一广播消息；通信单元 420，还用于接收该第一广播消息的响应信息，该响应信息中包括终端设备接收该第一广播消息的波束的波束索引，以及，终端设备基于该波束索引生成的第一广播消息的完整性保护信息；处理单元 410，用于根据该第一广播消息和该波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整信息保护信息的校验结果。

一种可选的实施方式中，处理单元 410 还用于根据该第一广播消息的完整性保护信息的校验结果，调整第一广播消息在所述波束下对应的签名周期；其中，第一广播消息在该波束下对应的签名周期是该波束下网络设备发送该第一广播消息的完整性保护信息的发送周期。

一种可选的实施方式中，通信单元 420 还用于发送该第一广播消息在该波束下对应的签名周期。

一种可选的实施方式中，处理单元 410 根据第一广播消息和所述波束索引，对完整性保护信息进行校验，获得第一广播消息的完整信息保护信息的校验结果，具体为：根据该第一广播消息以及发送该第一广播消息的时间戳、下行链路频率、小区标识和波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整性保护信息的校验结果。

一种可选的实施方式中，该响应信息还包括防重放参数，相应的，处理单元 410 利用防重放参数，验证该第一广播消息的响应信息是否为重放消息；若不为重放消息，执行所述的根据该第一广播消息和该波束索引，对该完整性保护信息进行校验，获得该第一广播消息的完整信息保护信息的校验结果的操作。

一种可选的实施方式中，响应信息是加密的，处理单元 410 还需对该第一广播消息的响应信息进行解密，获得波束索引和该第一广播消息的完整性保护信息。

当该通信装置用于实现图 8 或图 9 所示的方法实施例中终端设备的功能时：

通信单元 420，用于接收第一广播消息；处理单元 410，用于生成该第一广播消息的完整性保护信息，该完整性保护信息是基于接收该第一广播消息的波束的波束索引生成的；通信单元 420，还用于发送该第一广播消息的响应信息，该响应信息中包括该波束索引，以及，该第一广播消息的完整性保护信息。

一种可选的实施方式中，通信单元 420，还用于接收该第一广播消息在该波束下对应的签名周期。

一种可选的实施方式中，处理单元 410 还用于对该第一广播消息的响应信息进行加密，获得加密后的第一广播消息的响应信息；具体的，通信单元 420 发送加密后的该第一广播消

息的响应信息。

有关上述处理单元 410 和通信单元 420 更详细的描述可以直接参考图 8 或图 9 所示的方法实施例中相关描述直接得到，这里不加赘述。

当通信装置用于实现图 10 所示的方法实施例中网络设备的功能时：

通信单元 420，用于在时刻 j ，在波束 i 下发送广播消息 $P(j)$ ；通信单元 420，还用于接收该广播消息 $P(j)$ 的响应信息 $Resp(j)$ ，该响应信息 j 中包括该波束 i 的波束索引，以及，该广播消息 $P(j)$ 的完整性保护信息 $Int(j)$ ；处理单元 410，用于根据发送的该广播消息 $P(j)$ 和该波束 i 的波束索引，对该完整性保护信息 $Int(j)$ 进行校验，获得该广播消息 $P(j)$ 的完整信息保护信息 $Int(j)$ 的校验结果 j ；处理单元 410，还用于根据该广播消息 $P(j)$ 的完整性保护信息 $Int(j)$ 的校验结果，调整该条广播消息在该波束 i 下对应的签名周期 $Period(j)$ 到签名周期 $Period(k)$ ；通信单元 420，还用于在时刻 k ，在波束 i 下发送广播消息 $P(k)$ ，该广播消息 $P(k)$ 携带签名周期 $Period(k)$ 以及网络设备生成的该广播消息 $P(k)$ 的完整信息保护信息 $Int(k)$ ；通信单元 420，还用于接收该广播消息 $P(k)$ 的响应信息 $Resp(k)$ ，该响应信息 $Resp(k)$ 包括该波束 i 的波束索引和该广播消息 $P(k)$ 的完整性保护信息 $Int(k)$ 的校验结果 $check(k)$ 。

当通信装置用于实现图 10 所示的方法实施例中终端设备的功能时：

通信单元 420，用于在时刻 j ，在波束 i 下接收广播消息 $P(j)$ ；处理单元 410，用于生成该广播消息 $P(j)$ 的完整性保护信息，该完整性保护信息是基于接收该广播消息 $P(j)$ 的波束 i 的波束索引生成的；通信单元 420，还用于发送该广播消息 $P(j)$ 的响应信息 $Resp(j)$ ，该响应信息 $Resp(j)$ 中包括该波束 i 的波束索引，以及，该广播消息 $P(j)$ 的完整性保护信息 $Int(j)$ ；通信单元 420，还用于接收该广播消息 $P(k)$ ，该广播消息 $P(k)$ 携带签名周期 $Period(k)$ 以及网络设备生成的该广播消息 $P(k)$ 的完整信息保护信息 $Int(k)$ ；处理单元 410，还用于根据接收该广播消息 $P(k)$ 的波束 i 的波束索引，对该完整性保护信息 $Int(k)$ 进行校验，获得该广播消息 $P(k)$ 的完整性保护信息 $Int(k)$ 的校验结果 $check(k)$ ；通信单元 420，还用于发送该广播消息 $P(k)$ 的响应信息 $Resp(k)$ ，该响应信息 $Resp(k)$ 包括该波束 i 的波束索引和该广播消息 $P(k)$ 的完整性保护信息 $Int(k)$ 的校验结果 $check(k)$ 。

有关上述处理单元 410 和通信单元 420 更详细的描述可以直接参考图 10 所示的方法实施例中相关描述直接得到，这里不加赘述。

如图 12 所示，该通信装置包括处理器 510 和接口电路 520。处理器 510 和接口电路 520 之间相互耦合。可以理解的是，接口电路 520 可以为收发器或输入输出接口。可选的，通信装置还可以包括存储器 530，用于存储处理器 510 执行的指令或存储处理器 510 运行指令所需要的输入数据或存储处理器 510 运行指令后产生的数据。

当通信装置用于实现图 6 至图 10 任一所示的方法时，处理器 510 用于实现上述处理单元 410 的功能，接口电路 520 用于实现上述通信单元 420 的功能。

当上述通信装置为应用于终端设备的芯片时，该芯片实现上述方法实施例中终端设备的功能。该芯片从终端设备中的其它模块（如射频模块或天线）接收信息，该信息是网络设备发送给终端设备的；或者，该芯片向终端设备中的其它模块（如射频模块或天线）发送信息，该信息是终端设备发送给网络设备的。

当上述通信装置为应用于网络设备的模块时，该模块实现上述方法实施例中网络设备的功能。该模块从网络设备中的其它模块（如射频模块或天线）接收信息，该信息是终端设备

发送给网络设备的；或者，该模块向网络设备中的其它模块（如射频模块或天线）发送信息，该信息是网络设备发送给终端设备的。这里的模块可以是网络设备的基带芯片，也可以是分布式单元（distributed unit, DU）或其他模块，这里的 DU 可以是开放式无线接入网（open radio access network, O-RAN）架构下的 DU。

可以理解的是，本申请的实施例中的处理器可以是中央处理单元（Central Processing Unit, CPU），还可以是其它通用处理器、数字信号处理器（Digital Signal Processor, DSP）、专用集成电路（Application Specific Integrated Circuit, ASIC）、现场可编程门阵列（Field Programmable Gate Array, FPGA）或者其它可编程逻辑器件、晶体管逻辑器件，硬件部件或者其任意组合。通用处理器可以是微处理器，也可以是任何常规的处理器。

本申请的实施例中的方法步骤可以通过硬件的方式来实现，也可以由处理器执行软件指令的方式来实现。软件指令可以由相应的软件模块组成，软件模块可以被存放于随机存取存储器、闪存、只读存储器、可编程只读存储器、可擦除可编程只读存储器、电可擦除可编程只读存储器、寄存器、硬盘、移动硬盘、CD-ROM 或者本领域熟知的任何其它形式的存储介质中。一种示例性的存储介质耦合至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息。当然，存储介质也可以是处理器的组成部分。处理器和存储介质可以位于 ASIC 中。另外，该 ASIC 可以位于基站或终端中。当然，处理器和存储介质也可以作为分立组件存在于基站或终端中。

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程序或指令。在计算机上加载和执行所述计算机程序或指令时，全部或部分地执行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、网络设备、用户设备或者其它可编程装置。所述计算机程序或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，所述计算机程序或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或无线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集成一个或多个可用介质的服务器、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；也可以是光介质，例如，数字视频光盘；还可以是半导体介质，例如，固态硬盘。该计算机可读存储介质可以是易失性或非易失性存储介质，或可包括易失性和非易失性两种类型的存储介质。

在本申请的各个实施例中，如果没有特殊说明以及逻辑冲突，不同的实施例之间的术语和/或描述具有一致性、且可以相互引用，不同的实施例中的技术特征根据其内在的逻辑关系可以组合形成新的实施例。

可以理解的是，在本申请的实施例中涉及的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的实施例的范围。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。

权 利 要 求 书

- 1.一种广播消息保护方法，其特征在于，所述方法包括：
生成第一广播消息的完整性保护信息，所述完整性保护信息是基于发送所述第一广播消息的波束的波束索引生成的；
发送所述第一广播消息的完整性保护信息。
- 2.根据权利要求1所述的方法，其特征在于，所述方法还包括：
发送所述第一广播消息在所述波束下对应的签名周期，所述第一广播消息在所述波束下对应的签名周期是所述波束下所述第一广播消息的完整性保护信息的发送周期。
- 3.根据权利要求2所述的方法，其特征在于，所述方法还包括：
接收所述第一广播消息的响应信息，所述响应信息包括所述波束索引和所述第一广播消息的完整性保护信息的校验结果；
根据所述第一广播消息的完整性保护信息的校验结果，调整所述第一广播消息在所述波束下对应的签名周期。
- 4.根据权利要求1至3任一项所述的方法，其特征在于，所述第一广播消息包括具有相同传输周期的不同广播消息。
- 5.根据权利要求1至4任一项所述的方法，其特征在于，所述完整性保护信息还基于发送所述第一广播消息的时间戳、下行链路频率和小区标识生成。
- 6.根据权利要求3所述的方法，其特征在于，所述响应信息还包括防重放参数，所述方法还包括：
利用所述防重放参数，验证所述第一广播消息的响应信息是否为重放消息；
若不为重放消息，执行所述的根据所述第一广播消息的完整性保护信息的校验结果，调整所述第一广播消息在所述波束下对应的签名周期的步骤。
- 7.根据权利要求3所述的方法，其特征在于，所述响应信息是加密的，所述方法还包括：
对所述第一广播消息的响应信息进行解密，获得所述波束索引和所述第一广播消息的完整性保护信息的校验结果。
- 8.一种广播消息保护方法，其特征在于，所述方法包括：
接收第一广播消息的完整性保护信息；
根据接收所述第一广播消息的波束的波束索引，对所述完整性保护信息进行校验，获得所述第一广播消息的完整性保护信息的校验结果。
- 9.根据权利要求8所述的方法，其特征在于，所述方法还包括：
接收所述第一广播消息在所述波束下对应的签名周期，所述第一广播消息在所述波束下对应的签名周期是所述波束下所述第一广播消息的完整性保护信息的发送周期。

10.根据权利要求 9 所述的方法,其特征在于,所述方法还包括:

发送所述第一广播消息的响应信息,所述响应信息包括所述波束索引和所述第一广播消息的完整性保护信息的校验结果;

所述第一广播消息的完整性保护信息的校验结果,用于网络设备调整所述第一广播消息在所述波束下对应的签名周期。

11.根据权利要求 8 至 10 任一项所述的方法,其特征在于,所述第一广播消息包括具有相同传输周期的不同广播消息。

12.根据权利要求 8 至 11 任一项所述的方法,其特征在于,根据接收所述第一广播消息的波束的波束索引,对所述完整性保护信息进行校验,获得所述第一广播消息的完整性保护信息的校验结果,包括:

根据接收所述第一广播消息的时间戳、下行链路频率、小区标识以及波束的波束索引,对所述完整性保护信息进行校验,获得所述第一广播消息的完整性保护信息的校验结果。

13.根据权利要求 10 所述的方法,其特征在于,所述响应信息还包括防重放参数,用于网络设备验证所述第一广播消息的响应信息是否为重放消息。

14.根据权利要求 10 所述的方法,其特征在于,所述发送所述第一广播消息的响应信息,包括:

对所述第一广播消息的响应信息进行加密,获得加密后的所述第一广播消息的响应信息;发送加密后的所述第一广播消息的响应信息。

15.一种广播消息保护方法,其特征在于,所述方法还包括:

发送第一广播消息;

接收所述第一广播消息的响应信息,所述响应信息中包括终端设备接收所述第一广播消息的波束的波束索引,以及,所述终端设备基于所述波束索引生成的所述第一广播消息的完整性保护信息;

根据所述第一广播消息和所述波束索引,对所述完整性保护信息进行校验,获得所述第一广播消息的完整性保护信息的校验结果。

16.根据权利要求 15 所述的方法,其特征在于,所述方法还包括:

根据所述第一广播消息的完整性保护信息的校验结果,调整所述第一广播消息在所述波束下对应的签名周期;

所述第一广播消息在所述波束下对应的签名周期是所述波束下发送所述第一广播消息的完整性保护信息的发送周期。

17.根据权利要求 16 所述的方法,其特征在于,所述根据所述第一广播消息的完整性保护信息的校验结果,调整所述第一广播消息在所述波束下对应的签名周期之前,所述方法还包括:

发送所述第一广播消息在所述波束下对应的签名周期。

18.根据权利要求 15 至 17 任一项所述的方法，其特征在于，所述第一广播消息包括具有相同传输周期的不同广播消息。

19.根据权利要求 15 至 18 任一项所述的方法，其特征在于，根据所述第一广播消息和所述波束索引，对所述完整性保护信息进行校验，获得所述第一广播消息的完整信息保护信息的校验结果，包括：

根据所述第一广播消息以及发送所述第一广播消息的时间戳、下行链路频率、小区标识和所述波束索引，对所述完整性保护信息进行校验，获得所述第一广播消息的完整性保护信息的校验结果。

20.根据权利要求 15 至 19 任一项所述的方法，其特征在于，所述响应信息还包括防重放参数，所述方法还包括：

利用所述防重放参数，验证所述第一广播消息的响应信息是否为重放消息；

若不为重放消息，执行所述的根据所述第一广播消息和所述波束索引，对所述完整性保护信息进行校验，获得所述第一广播消息的完整信息保护信息的校验结果的步骤。

21.根据权利要求 15 至 20 任一项所述的方法，其特征在于，所述响应信息是加密的，所述方法还包括：

对所述第一广播消息的响应信息进行解密，获得所述波束索引和所述完整性保护信息。

22.一种广播消息保护方法，其特征在于，所述方法还包括：

接收第一广播消息；

生成所述第一广播消息的完整性保护信息，所述完整性保护信息是基于接收所述第一广播消息的波束的波束索引生成的；

发送所述第一广播消息的响应信息，所述响应信息中包括所述波束索引，以及，所述第一广播消息的完整性保护信息。

23.根据权利要求 22 所述的方法，其特征在于，所述根据接收所述第一广播消息的波束的波束索引，生成所述第一广播消息在所述波束下的完整性保护信息之前，所述方法还包括：

接收所述第一广播消息在所述波束下对应的签名周期，

所述第一广播消息在所述波束下对应的签名周期是所述波束下网络设备发送所述第一广播消息的完整性保护信息的发送周期。

24.根据权利要求 22 或 23 所述的方法，其特征在于，所述第一广播消息包括具有相同传输周期的不同广播消息。

25.根据权利要求 22 至 24 任一项所述的方法，其特征在于，所述完整性保护信息还基于接收所述第一广播消息的时间戳、下行链路频率和小区标识生成。

26.根据权利要求 22 至 25 任一项所述的方法，其特征在于，所述响应信息还包括防重放参数，用于网络设备验证所述第一广播消息的响应信息是否为重放消息。

27.根据权利要求 22 至 26 任一项所述的方法，其特征在于，所述发送所述第一广播消息的响应信息，包括：

对所述第一广播消息的响应信息进行加密，获得加密后的所述第一广播消息的响应信息；
发送加密后的所述第一广播消息的响应信息。

28.一种通信系统，其特征在于，所述通信系统包括网络设备和终端设备，所述网络设备用于执行根据权利要求 1 至 7 任一项所述的方法，所述终端设备用于执行根据权利要求 8 至 14 任一项所述的方法；或者，

所述网络设备用于执行根据权利要求 15 至 21 任一项所述的方法，所述终端设备用于执行根据权利要求 22 至 27 任一项所述的方法。

29.一种通信装置，包括用于执行如权利要求 1 至 7 中的任一项所述方法的模块，或者，包括用于执行如权利要求 8 至 14 中的任一项所述方法的模块，或者，包括用于执行如权利要求 15 至 21 中的任一项所述方法的模块，或者，包括用于执行如权利要求 22 至 27 中的任一项所述方法的模块。

30.一种通信装置，其特征在于，包括处理器和接口电路，所述接口电路用于接收来自所述通信装置之外的其它通信装置的信号并传输至所述处理器或将来自所述处理器的信号发送给所述通信装置之外的其它通信装置，所述处理器通过逻辑电路或执行代码指令用于实现如权利要求 1 至 7 中任一项所述的方法，或者，用于实现如权利要求 8 至 14 中的任一项所述的方法，或者，用于实现如权利要求 15 至 21 中的任一项所述的方法，或者，用于实现如权利要求 22 至 27 中的任一项所述的方法。

31.一种计算机可读存储介质，其特征在于，所述存储介质中存储有计算机程序或指令，当所述计算机程序或指令被通信装置执行时，实现如权利要求 1 至 7 中任一项所述的方法，或者，实现如权利要求 8 至 14 中的任一项所述的方法，或者，实现如权利要求 15 至 21 中的任一项所述的方法，或者，实现如权利要求 22 至 27 中的任一项所述的方法。

32.一种通信装置，其特征在于，所述通信装置包括处理器和收发器；

其中，所述收发器用于与其他通信装置进行通信，所述处理器用于运行计算机程序，以使得所述通信装置实现如权利要求 1 至 7 中任一项所述的方法，或者，实现如权利要求 8 至 14 中的任一项所述的方法，或者，实现如权利要求 15 至 21 中的任一项所述的方法，或者，实现如权利要求 22 至 27 中的任一项所述的方法。

33.一种通信装置，其特征在于，所述通信装置包括存储器、处理器和收发器；

其中，所述收发器，用于接收信号或者发送信号，所述存储器用于存储指令或计算机程序，所述处理器用于执行所述存储器所存储的计算机程序或指令，以使所述通信装置执行如权利要求 1 至 7 中任一项所述的方法，或者，实现如权利要求 8 至 14 中的任一项所述的方法，

或者，实现如权利要求 15 至 21 中的任一项所述的方法，或者，实现如权利要求 22 至 27 中的任一项所述的方法。

34.一种计算机程序产品，其特征在于，包括计算机指令，当所述计算机指令在计算机上运行时，使得所述计算机执行如权利要求 1 至 7 中任一项所述的方法，或者，实现如权利要求 8 至 14 中的任一项所述的方法，或者，实现如权利要求 15 至 21 中的任一项所述的方法，或者，实现如权利要求 22 至 27 中的任一项所述的方法。