一种通信方法及相关装置

本申请要求于2024年2月20日提交中国国家知识产权局、申请号为202410193052.9、申请名称为“一种通信方法及相关装置”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。

技术领域

本申请涉及通信技术领域，尤其涉及短距通信技术领域，例如智能汽车、智能家居、智能终端和智能制造等场景中的通信等，具体涉及一种通信方法及相关装置。

背景技术

随着通信技术的不断发展，智能家居、智能座舱、智能驾驶、智能制造、和智能运输等智能应用场景应运而生，实现多种多样的业务功能的通信系统，提高了生产力，也为人们的生活带来的便捷和趣味。人们对通信系统的功能要求也越要越高，这使得通信系统中的节点的数量和种类不断增加，在大多数包括多个节点的通信系统中，节点的身份和通信能力通常存在较大差异，一方面是为了便于管理多节点的系统，另一方面是为了兼容计算能力和通信能力不同的节点。但节点之间的差异，也间接导致节点之间的连接受到限制。

一些通信系统内包括主节点和从节点，主节点的通信能力较强且具有管理从节点的能力，可与多个从节点建立链路，使得主从节点之间可以进行通信，以实现各种功能。在这类通信系统中，从节点与从节点之间往往不具备建立链路的能力，使得从节点之间的通信需求难以实现。在两个从节点之间需要传输数据时，往往依赖于主节点进行转发，一方面，由主节点进行转发的通信方式，会使得主节点的通信压力增大。另一方面，从节点之间无法协商得到与安全通信相关的参数，使得二者之间的数据传输的安全性较低。

发明内容

本申请提供一种通信方法及相关装置，能够支持两个被其他节点所管理的节点之间直接地、安全地传输数据，提高数据传输的效率并提升通信安全性。

第一方面，本申请提供一种通信方法，包括：第一节点生成第一信息并向第二节点发送第一信息，以及向第三节点发送第一信息，该第一信息用于对第二节点和第三节点之间传输的数据进行安全保护。其中，第一节点分别与第二节点和第三节点连接，第二节点和第三节点被该第一节点管理。

安全保护包括完整性保护和/或机密性保护（即加密/解密）。管理是指能够定义、决策、或配置另一节点的通信过程（例如分配通信的资源、或设置通信过程中参数等）。一些实施方式中，第二节点和第三节点被第一节点管理，即：第一节点为发送资源管理信息的节点，第二节点和第二节点为接收资源管理信息并根据所述资源管理信息进行数据的发送和/或接收的节点。资源管理信息包括接入层资源管理信息。

在本申请中，第二节点和第三节点是被第一节点所管理的两个节点，而第一节点为二者生成第一信息，使得第二节点和第三节点均基于第一节点提供的第一信息，对第二节点和第三节点之间的数据传输过程进行安全保护。一方面，本申请实现了被其他节点所管理的两个节点之间的数据直接传输，提升了数据传输的效率。另一方面，二者之间通信的数据可基于第一节点生成并分发的第一信息来进行安全保护，提升了通信安全性。

可选地，第一信息可用于第二节点和第三节点之间的点对点链路的安全保护，也即，第二节点和第三节点之间传输的数据具体通过二者之间的通信链路传输。当然，本申请对于将第一信息用于对二者之间的基于无连接的通信进行安全保护的情况也同样适用，比如，一些方案中，该第一信息可用于对二者之间以广播形式传输的数据进行安全保护。

可选地，该方法可由第一节点中的模块执行，例如由芯片或软件模块执行。

在第一方面的一种可能的实施方式中，向第二节点发送第一信息包括：向第二节点发送第一消息，第一信息承载于第一消息。其中，第一消息用于指示第二节点与第三节点建立链路。比如，第一消息具有特定的格式或者携带了特殊的信息，以指示第二节点与第三节点建立链路。示例性地，第一消息中携带链路

的配置信息，第二节点可基于该链路的配置信息与第三节点建立链路。可选地，链路的配置信息包括于资源管理信息。

上述实施方式中，第二节点与第三节点可被第一节点指示建立二者之间的点对点的链路。而第一信息可在第一消息中携带，可减少建立链路过程中的信令数量，提升传输的效率。

本文中，链路是指两个节点之间点对点的、直接的链路，一些场景中也可称为承载（例如接入层承载）、连接、关联等。示例性地，第一节点可以为管理节点（或称 G 节点），第二节点和第三节点可以为终端节点（或称 T 节点）。第一消息例如为异步 TT 链路建链指示，以指示第二节点和第三节点之间建立 TT 链路（或称 T-T 链路），T-T 链路即 T 节点和 T 节点之间的链路。

在第一方面的又一种可能的实施方式中，向第三节点发送第一信息，包括：向第三节点发送第二消息，第一信息承载于第二消息。第二消息用于指示第三节点与第二节点建立通信链路，例如第二消息为异步 TT 链路建链指示。

可选地，第二消息中携带链路的配置信息，第三节点可基于链路的配置信息与第二节点建立链路。

在第一方面的又一种可能的实施方式中，发送给第二节点的第一信息承载于第三消息中，第三消息与第一消息不同，第三消息例如为安全参数指示信息。

在第一方面的又一种可能的实施方式中，方法还包括：向第二节点发送第一消息。其中，第一消息用于指示第二节点与第三节点建立通信链路。

进一步地，该第一信息不承载于第一消息。这种实施方式中，第一节点向第二节点发送第一消息以指示第二节点与第三节点建立通信链路，并通过额外的消息（如第三消息）将第一信息发送给第二节点，使得消息的功能更加细化、精细化，提升消息格式的可复用性和组合灵活性。

在第一方面的又一种可能的实施方式中，方法还包括：向第三节点发送第二消息，第二消息用于指示第三节点与第二节点建立通信链路。进一步地，第一信息不承载于第二消息。

在第一方面的又一种可能的实施方式中，发送给第三节点的第一信息承载于第四消息中，第四消息与第二消息不同，第四消息例如为安全参数指示信息。

在第一方面的又一种可能的实施方式中，第一信息包括第一指示。其中，第一指示承载于第一字段，第一字段的取值可指示第二节点和第三节点之间的链路的加密和完整性保护的启动状态。

示例性地，当第一字段为第一值时，指示第二节点和第三节点之间的链路加密和启动完整性保护同时启动。当第一字段为第二值时，指示第二节点和第三节点之间的链路不启动加密，启动完整性保护。当第一字段为第三值时，指示第二节点和第三节点之间的链路启动加密，不启动完整性保护。当第一字段为第四值时，指示第二节点和第三节点之间的链路启动加密，不启动完整性保护。

可选地，第一指示包括于第一消息，或第三消息中。类似地，第一指示包括于第二消息或第四消息中。第一指示的相关取值参见前述。

在第一方面的又一种可能的实施方式中，第一消息包括第二指示，第二指示用于指示第二节点先发送数据或后发送数据。其中，先发送数据的节点为先发节点，后发送数据的节点为后发节点。

比如，第二指示承载于第二字段，第二字段的取值可指示第二节点先发送数据或后发送数据。

在第一方面的又一种可能的实施方式中，第二消息包括第三指示，第三指示用于指示第三节点先发送数据或后发送数据。比如，第三指示承载于第三字段，第三字段的取值可指示第二节点先发送数据或后发送数据。

在第一方面的又一种可能的实施方式中，第一信息可包括安全算法指示、密钥指示、参与安全算法的参数的指示、或安全相关的状态指示等中的一项或者多项。其中，安全算法包括加密算法、完整性保护算法、密钥派生算法、或密钥协商算法等中的一项或者多项。密钥是执行安全算法的过程中输入的、具有机密性的参数。参与安全算法的参数是除了密钥之外，在执行安全算法中输入的参数，比如加密盐、或新鲜参数等，从而进一步提高安全性。安全相关的状态指示可用于配置状态参数，例如安全相关的状态指示可包括第一指示，该第一指示用于指示加密和/或完整性保护的开启状态。

可选地，第一信息可通过一条消息发送，也可通过多条消息发送。

在第一方面的又一种可能的实施方式中，第一信息包括以下信息中的一项或者多项：完整性保护算法指示、完整性保护密钥指示、加密算法指示、加密密钥指示、第一参数或第一指示等。

其中，完整性保护算法指示用于指示第二节点和第三节点之间的链路使用的第一完整性保护算法。可选地，第一完整性保护算法为第二节点和第三节点支持的完整性保护算法中优先级最高的算法，或者，第一完整性保护算法可为第一节点选择的算法。完整性保护密钥指示用于指示完整性保护算法（例如第一完

整性保护算法）使用的密钥。加密算法指示用于指示第二节点和第三节点之间的链路使用的第一加密算法。可选地，第一加密算法为第二节点和第三节点支持的加密算法中优先级最高的算法，或者，第一加密算法可为第一节点选择的算法。加密密钥指示用于指示加密算法（例如第一加密算法）使用的密钥。第一参数用于得到第二节点和第三节点之间的加密和/或完整性保护过程的输入参数，比如，第一参数为初始化基础值或初始化向量。

第二方面，本申请提供一种通信方法，包括：接收来自第一节点的第一信息，基于第一信息对第一数据进行安全保护，其中第一数据为在第二节点和第三节点之间传输的数据。

该方法应用于第二节点。可选地，该方法可由第二节点中的模块执行，例如由芯片或软件模块执行。

在第二方面的一种可能的实施方式中，接收来自第一节点的第一信息，包括：接收来自第一节点的第一消息，第一信息承载于第一消息。其中，第一消息用于指示第二节点与第三节点建立连接。

在第二方面的又一种可能的实施方式中，方法还包括：接收来自第一节点的第一消息。第一消息用于指示第二节点与第三节点建立连接。

在第二方面的又一种可能的实施方式中，方法还包括：与第三节点建立通信链路。

在第二方面的又一种可能的实施方式中，第一信息包括以下信息中的一项或者多项：完整性保护算法指示、完整性保护密钥指示、加密算法指示、加密密钥指示或第一参数。

其中，完整性保护算法指示用于指示第二节点和第三节点之间的链路使用的第一完整性保护算法。可选地，第一完整性保护算法为第二节点和第三节点支持的完整性保护算法中优先级最高的算法，或者，第一完整性保护算法可为第一节点选择的算法。完整性保护密钥指示用于指示完整性保护算法使用的密钥。加密算法指示用于指示第二节点和第三节点之间的链路使用的第一加密算法。可选地，第一加密算法为第二节点和第三节点支持的加密算法中优先级最高的算法，或者，第一加密算法可为第一节点选择的算法。

加密密钥指示用于指示加密算法使用的密钥。第一参数用于得到第二节点和第三节点之间的加密和/或完整性保护过程的输入参数。比如，第一参数为初始化基础值或初始化向量。

在第二方面的又一种可能的实施方式中，第一信息包括完整性保护算法指示和完整性保护密钥指示，完整性保护算法指示用于指示第一完整性保护算法，完整性保护密钥指示用于指示完整性保护密钥。基于第一信息对第一数据进行安全保护，包括：基于第一完整性保护算法和完整性保护密钥，对第一数据进行完整性保护。

在第二方面的又一种可能的实施方式中，第一信息包括完整性保护算法指示，完整性保护算法指示用于指示第一完整性保护算法。基于第一信息对第一数据进行安全保护，包括：基于第一完整性保护算法和完整性保护密钥，对第一数据进行完整性保护。其中，完整性保护密钥为第二节点和第三节点之间协商得到的。

在第二方面的又一种可能的实施方式中，第一信息包括完整性保护密钥指示，完整性保护密钥指示用于指示完整性保护密钥。基于第一信息对第一数据进行安全保护，包括：基于第一完整性保护算法和完整性保护密钥，对第一数据进行完整性保护。其中，第一完整性保护算法为第二节点和第三节点之间协商得到的。

在第二方面的又一种可能的实施方式中，基于第一完整性保护算法和完整性保护密钥，对第一数据进行完整性保护，包括：基于第一完整性保护算法、完整性保护密钥、第一完整性保护输入和第一数据，计算得到完整性检查码。

其中，完整性检查码用于检查第一数据的完整性。比如，该完整性校验码和第一数据可携带于同一个数据包。

在第二方面的又一种可能的实施方式中，第一完整性保护输入包括方向指示和/或第二参数。

其中，方向指示用于指示第一数据的发送方和接收方在事件中发送数据的先后顺序。示例性地，当方向指示为第五值时，指示先发节点发后发节点收，即第一数据为先发节点发送给后发节点的数据。当方向指示为第六值时，指示后发节点发先发节点收，即第一数据位后发节点发送给先发节点的数据。

其中，先发节点为在事件中先发送数据的节点，后发节点为在事件中后发送数据的节点。

一种实现中，第二参数与第一信息包括的第一参数相关。比如，第一参数为 A 个比特的初始化基础值，基于另一比特序列（例如为 B 个比特）对该初始化基础值进行处理（例如异或、同或处理），得到的最终值作为第二参数，其中 A、B 为大于等于 1 的整数。可选地，前述的 B 个比特的比特序列可与无线帧类型相关。示例性地，第二参数占用 64 比特，其中，初始化基础值为通过随机数生成器生成一个 64 比特的值，对于无线帧类型 1 和无线帧类型 2，将该初始化基础值的低 32 比特与同步序列的低 32 比特异或得到的最

终取值（64 比特）。对于无线帧类型 3 和无线帧类型 4，将该初始化基础值的低 24 比特与逻辑链路标识的 24 比特异或得到的最终取值。

又一种实现中，第二参数与来自第二节点的第三参数和/或来自第三节点的第四参数相关。比如，第二节点提供第三参数而第三节点提供第四参数，第二节点基于第三参数和第四参数得到第二参数。示例性地，第二节点向第三节点发送第三参数（如 32 比特），而第三节点向第二节点发送第四参数（32 比特），第二参数为拼接第三参数和第四参数得到的 64 比特的值。

在第二方面的又一种可能的实施方式中，第一数据携带于传输数据包的有效载荷。基于第一完整性保护算法、完整性保护密钥、第一完整性保护输入和第一数据，计算得到完整性检查码，包括：基于第一完整性保护算法、完整性保护密钥和第一完整性保护输入，得到第一输出，基于第一完整性保护算法、完整性保护密钥、第一输出和第二完整性保护输入，得到第二输出，基于第一完整性保护算法、完整性保护密钥、第二输出和传输数据包的有效载荷的第一个M字节得到对应有效载荷的第1个字节的完整性保护输出，M 为整数且 M≥1。

在传输数据包的有效载荷小于等于 M 个字节的情况下，对应有效载荷的第 1 个字节的完整性保护输出为最终输出。在传输数据包的有效载荷大于 M 个字节的情况下，基于第一完整性保护算法、完整性保护密钥和对应有效载荷的第 i-1 个 M 字节的完整性保护输出，得到对应有效载荷的第 i 个 M 字节的完整性保护输出，将对应有效载荷的最后部分字节的完整性保护输出作为最终输出，其中，i 为整数且 i 分别取 1 至 $\left\lceil \frac{\text{有效载荷字节数}}{M} \right\rceil$ 之间的整数，根据最终输出得到完整性检查码。其中，[x]表示对 x 进行向上取整得到的整数。

可选地，根据最终输出得到完整性检查码，包括：将最终输出的低 X 位作为完整性检查码。

在第二方面的又一种可能的实施方式中，第一信息包括加密算法指示和加密密钥指示，加密算法指示用于指示第一加密算法，加密密钥指示用于指示加密密钥。基于第一信息与第三节点进行安全通信，包括：基于第一加密算法和加密密钥对第一数据进行加密。

在第二方面的又一种可能的实施方式中，第一信息包括加密算法指示，加密算法指示用于指示第一加密算法。基于第一信息与第三节点进行安全通信，包括：基于第一加密算法和加密密钥对第一数据进行加密，其中，加密密钥为第二节点和第三节点之间协商得到的。

在第二方面的又一种可能的实施方式中，第一信息包括加密密钥指示，加密密钥指示用于指示加密密钥。基于第一信息与第三节点进行安全通信，包括：基于第一加密算法和加密密钥对第一数据进行加密，其中，第一加密算法为第二节点和第三节点之间协商得到的。

在第二方面的又一种可能的实施方式中，基于第一加密算法和加密密钥对第一数据进行加密，包括：基于第一加密算法、加密密钥和加密输入，对第一数据进行加密。

其中，加密输入包括方向指示和/或第二参数。

在第二方面的一种可能的实施方式中，第一数据携带于传输数据包的有效载荷，基于第一加密算法和加密密钥对第一数据进行加密，包括：对于有效载荷的所有字节，基于第一加密算法、加密密钥、有效载荷的第 j 个 K 字节和对应第 j 个 K 字节的加密输入，得到第 j 个加密输出，j 为整数且 j 分别取 1 至 $\left\lceil \frac{\text{有效载荷字节数}}{K} \right\rceil + 1$ 之间的整数。

在第二方面的一种可能的实施方式中，在第二节点和第三节点之间的完整性保护开启的情况下，基于第一加密算法、加密密钥、完整性检查码和对应完整性检查码的加密输入，得到加密的完整性检查码。

在第二方面的又一种可能的实施方式中，第一消息包括第一指示，第一指示承载于第一字段，第一字段的取值可指示第二节点和第三节点之间的链路的加密和完整性保护的启动状态。

在第二方面的又一种可能的实施方式中，第一消息包括第二指示，第二指示用于指示第二节点先发送数据或后发送数据。比如，第二指示承载于第二字段，第二字段的取值可指示第二节点先发送数据或后发送数据。

第三方面，本申请提供一种通信方法，包括：接收来自第一节点的第一消息，与第三节点建立链路，与第三节点协商确定第一信息，基于第一信息对第一数据进行安全保护。其中，第一消息用于指示第二节点与第三节点建立链路，第一数据为在第二节点和第三节点之间传输的数据。

该方法应用于第二节点。可选地，该方法可由第二节点中的模块执行，例如由芯片或软件模块执行。

在第三方面的又一种可能的实施方式中，第一信息包括以下信息中的一项或者多项：完整性保护算法指示、完整性保护密钥指示、加密算法指示、加密密钥指示或第一参数。

在第三方面的又一种可能的实施方式中，基于第一信息对第一数据进行安全保护，包括：基于第一完整性保护算法和完整性保护密钥，对第一数据进行完整性保护。

在第三方面的又一种可能的实施方式中，基于第一信息与第三节点进行安全通信，包括：基于第一加密算法和加密密钥对第一数据进行加密。

在第三方面的又一种可能的实施方式中，第一消息包括第一指示，第一指示承载于第一字段，第一字段的取值可指示第二节点和第三节点之间的链路的加密和完整性保护的启动状态。

在第三方面的又一种可能的实施方式中，第一消息包括第二指示，第二指示用于指示第二节点先发送数据或后发送数据。

第四方面，本申请提供一种通信装置，包括用于执行第一方面或第一方面任意一项可能的实施方式所描述方法的单元或模块，或者包括用于执行第二方面或第二方面任意一项可能的实施方式所描述方法的单元或模块，或者包括用于执行第三方面或第三方面任意一项可能的实施方式所描述方法的单元或模块。

示例性地，通信装置包括处理单元和通信单元。其中，处理单元用于实现处理、确定、生成、计算、加密、解密等一项或者多项操作，通信单元用于实现发送、接收等一项或者多项操作。

第五方面，本申请提供一种通信装置，该通信装置包括处理器和接口电路，所述接口电路用于接收来自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第一方面或第一方面任意一项可能的实施方式所描述的方法，或者用于实现第二方面或第二方面任意一项可能的实施方式所描述的方法，或者用于实现第三方面或第三方面任意一项可能的实施方式所描述的方法。

第六方面，本申请提供一种通信系统，通信系统包括第一节点、第二节点和第三节点，第一节点用于实现第一方面或第一方面任一项可能的实施方式所描述的方法，第二节点和第三节点用于实现第二方面或第二方面任一项可能的实施方式所描述的方法。

第七方面，本申请提供一种通信系统，所述通信系统包括第一节点、第二节点和第三节点，所述第二节点用于向所述第二节点发送第一消息以及向所述第三节点发送所述第二消息，所述第二节点和所述第三节点用于实现第三方面或第三方面任一项可能的实施方式所描述的方法。

第八方面，本申请提供一种终端，所述终端包括第四方面或第五方面所描述的通信装置，或者包括第六方面或第七方面所描述的通信系统。

第九方面，本申请提供一种可读存储介质，所述可读存储介质用于存储计算机程序，当所述计算机程序被处理器执行时，使得包括所述处理器的通信装置实现第一方面或第一方面任意一项可能的实施方式所描述的方法，或者实现第二方面或第二方面任意一项可能的实施方式所描述的方法，或者实现第三方面或第三方面任意一项可能的实施方式所描述的方法。

第十方面，本申请提供一种计算机程序，当所述计算机程序被处理器执行时，使得包括所述处理器的通信装置实现第一方面或第一方面任意一项可能的实施方式所描述的方法，或者实现第二方面或第二方面任意一项可能的实施方式所描述的方法，或者实现第三方面或第三方面任意一项可能的实施方式所描述的方法。

本申请第二方面至第十方面的有益效果可以参见第一方面的方案的有益效果。

附图说明

下面将对实施例描述中所需要使用的附图作简单地介绍。

图 1 是一种通信系统的架构图；

图 2 是一种通信系统的应用场景示意图；

图 3 是本申请实施例提供的一种通信系统的应用场景示意图；

图 4 是本申请实施例提供的又一种通信系统的应用场景示意图；

图 5 是本申请实施例提供的一种通信方法的流程示意图；

图 6 是本申请实施例提供的一种完整性保护过程的示意图；

图 7 是本申请实施例提供的一种完整性保护输入的数据内容示意图；

图 8 是本申请实施例提供的一种加密过程的示意图；

图 9 是本申请实施例提供的一种加密输入的数据内容示意图；

图 10 是本申请实施例提供的一种通信方法的流程示意图；

图 11 是本申请实施例提供的一种通信方法的流程示意图；

图 12 是本申请实施例提供的又一种通信方法的流程示意图；

图 13 是本申请实施例提供的又一种通信方法的流程示意图；

图 14 是本申请实施例提供的又一种通信方法的流程示意图；

图 15 是本申请实施例提供的一种通信装置的结构示意图；

图 16 是本申请实施例提供的又一种通信装置的结构示意图。

具体实施方式

下面先对部分技术术语进行介绍。

1.消息检查码

消息检查码，或称完整性检查、消息认证码（message authentication code，MAC）、消息鉴别码、文件消息认证码、或信息认证码等，是经过特定算法后产生的一小段信息，用于检查某段消息的完整性和/或作身份验证。

2.节点

节点是具有通信能力的设备，包括但不限于是用户设备、网络设备、工业设备等中的一项或者多项。其中，用户设备包括手持终端、可穿戴终端、交通工具、车载设备、感知设备、智能家居设备、或休闲娱乐设备等中的一项或者多项，手持终端包括但不限于是手机、平板、或笔记本电脑等，可穿戴设备包括但不限于是耳机、智能手环、智能手表、或智能眼镜等，交通工具包括但不限于是车辆、舰船、飞行器、轨道交通（如地铁、高铁等）、或物流机器人（如自动引导车（automated guided vehicle，AGV））等，车载设备包括但不限于是域控制器（domain controller，DC）、屏幕、麦克风、音响、电子钥匙、无钥匙进入、启动系统控制器、电池管理系统（battery management system，BMS）、电池包、或电芯等，感知设备包括但不限于是相机、雷达、激光雷达、光照传感器、温度传感器、或湿度传感器等，智能家居设备包括但不限于是投影仪、智能电视、智能冰箱、智能家庭网关、或安防设备等。休闲娱乐设备包括但不限于是虚拟现实（virtual reality，VR）设备、混合现实（mixed reality，MR）设备、按摩椅、家庭影院、游戏操控设备或4D影院座舱等。网络设备包括但不限于是路由器、交换机、或基站等。工业设备包括但不限于是工业机器人、或机械臂等。

应理解，本申请实施例的通信方法、通信装置、通信系统或节点等，适用于多种网络，例如适用于包括有线通信网络、无线通信网络、或者有线通信和无线通信组合形成的网络等。例如，无线通信网络包括通过如下通信技术连接的网络：星闪（SparkLink，或NearLink）、802.11b/g、蓝牙(blue tooth)、紫蜂(Zigbee)、无线射频识别技术(radio frequency identification，RFID)、超宽带(ultra-wideband，UWB)技术、或无线短距通信系统等。和/或，无线通信网络包括远距离连接技术包括基于长期演进（long term evolution，长期演进）的通信技术、第五代移动通信技术（5th generation mobile networks或5th generation wireless systems、5th-Generation，简称5G或5G技术）、全球移动通信系统(global system for mobile communications，GSM)、通用分组无线业务(general packet radio Service，GPRS)、通用移动通信系统(universal mobile telecommunications system，UMTS)等无线通信技术。再如，有线通信网络包括通过如下通信技术连接的网络：光纤连接技术、车载有线通信技术、控制器局域网（controller area network，CAN）、局域互联网络总线（local interconnect network，LIN）、CAN灵活数据速率（CAN flexible data-rate，CAN FD）、或车载以太网等中的一项或者多项。

本申请实施例中的节点可以应用于智能汽车、智能家居、智能终端、智能制造、智能展厅、移动互联网（mobile internet，MI）、工业控制（industrial control）、无人驾驶（self-driving）、运输安全（transportation safety）、或物联网（internet of things，IoT）等各个场景中。在某些应用场景、或某些网络类型中，类似具备通信能力的设备可能不称为节点，但是为了方便描述，本申请实施例中将具有通信能力的设备统称为节点。

3.通信系统

通信系统是用电信号（或光信号）传输信息的系统，其通常包括多个节点，节点之间进行通信以传输信息。通信系统中的节点可能具有不同的身份，和/或，具有不同的能力。在大部分通信系统中，节点具有主节点和从节点之分，主节点的通信能力较强且具有管理从节点的能力，可与多个从节点建立链路，使得主节点与主节点之间、主节点与从节点之间可进行通信，以实现各种功能。

如图1所示是一种通信系统的架构图，通信系统中包括管理节点（看作主节点）和终端节点（看作从节点）。终端节点均与管理节点连接，连接关系用虚线表示，管理节点与终端节点之间的通信包括是双向单播和/或广播通信。

其中，管理节点具有通信能力和管理能力，一些场景中也称为G节点、接入点(access point)、或授权节

点等。管理能力包括通信上的管理能力，例如能够进行连接管理、资源调度、或信息安全管理。示例性地，管理节点能够发送资源管理信息或数据调度信息，如接入层资源管理信息。终端节点，一些场景中也称为T节点，是具有通信能力的节点，可与管理节点之间进行业务传输。一些方案中，终端节点是接收资源管理信息（或数据调度信息）并根据资源管理信息（或数据调度信息）发送数据的节点。示例性地，终端设备可以包括用户设备(userequipment，UE)，例如包括条码、射频识别(radio frequency identification，RFID)、传感器、全球定位系统(globalpositioning system，GPS)、激光雷达、电芯等设备。

应理解，管理节点和终端节点的身份不是绝对的，只是便于在一种可能的连接情况下区分通信的节点所做的操作，所做出的示例性的命名。在一些场景中，一个节点同时归属于两个甚至更多个通信域，在部分通信域中作为终端节点，在另一部分通信域中可作为管理节点，为了便于理解部分实施例中将这种节点表示为G（T）节点。

前述对技术术语的解释可选用于下文的实施例中。

结合前述，在一些包括主节点和从节点的通信系统中，从节点之间往往不具备建立链路的能力，使得从节点之间的通信需求难以被实现。请参见图2，图2是一种通信系统的应用场景示意图，车辆包括4个位置锚点，即T1节点、T2节点、T3节点和T4节点。4个位置锚点接入到车辆的主节点（即G节点），T1节点、T2节点、T3节点和T4节点可分别与G节点建立GT链路。位置标签(如手机、车钥匙等)，即T5节点，也可接入G节点，与G节点建立GT链路。

在测量场景下，位置标签与位置锚点之间进行测量，位置标签的测量结果和位置锚点的测量结果通过GT链路发送给G节点，由G节点进行解算，如对位置标签进行定位。如图2，以T1节点和T5节点之间的测量过程为例，T1节点和T5节点交互测量帧并分别得到测量结果，T1节点和T5节点分别向G节点上报测量结果。具体实现中，交互测量的位置锚点的数量通常为多个，且测量的过程需要执行多次，使得主节点（G节点）的计算量较大，测量结果的解算速度较慢。若把解算功能分配到各位置锚点，可大大提高测量结果的解算速度。但是，把测量结果的解算分配到位置锚点的情况下，位置标签的测量结果需要提供给位置锚点，以图2为例，T5节点的测量结果需要提供给T1节点。由于T节点之间往往不具备建立链路的能力，使得T节点之间的通信需求难以被实现。若考虑通过G节点来进行转发，同样会增加G节点的通信压力，而且，T节点之间无法协商得到与安全通信相关的参数，使得T节点和T节点之间的数据传输的安全性较低，使得节点的通信安全受到威胁，进而影响整车安全。

有鉴于此，本申请提供一种通信方法及相关装置，能够支持两个被其他节点所管理的节点之间直接地、安全地传输数据，提高数据传输的效率并提升通信安全性。

请参见图3，在一种实施例中，G节点为T1节点和T5节点分别发送第一信息，该第一信息为与安全相关的参数。T1节点和T5节点之间基于第一信息，对二者之间传输的数据进行安全保护。进一步地，G节点还为T1节点和T5节点发送链路的配置信息，使得T1节点和T5节点基于链路的配置信息，建立TT链路。请参见图4，在又一种实施例中，G节点为T1节点和T5节点分别发送建链指示，T1节点和T5节点基于建链指示建立TT链路，该建链指示可包括链路的配置信息。T1节点和T5节点可协商得到第一信息，并基于第一信息对二者之间传输的数据进行安全保护。可选地，上述实施例还可以进行结合。即对数据进行安全保护所使用的信息中，部分信息为G节点提供的，部分信息为T1节点和T5节点之间协商得到的。

在上述实施例中，T1节点和T5节点之间直接地、安全地传输测量结果，无需经过G节点的转发，提高数据传输的效率还降低了主节点的通信压力和计算。由于T1和T5之间的传输的数据经过第一信息的保护，能够提升通信安全性。

当然，以上仅以测距过程为例，以T1、T5和G节点为例进行说明，具体实现过程中，对于类似的技术问题同样适用，对于存在类似问题的场景、包括更多或者更少数量的节点的通信系统同样适用。

下面介绍本申请提供的方法。

请参见图5，图5是本申请实施例提供的一种通信方法的流程示意图。可选地，该方法可以应用于通信系统，例如前述图1至图4中的一种或者多种通信系统。如图5所示的通信方法可以包括步骤S501至步骤S504中的一个或者多个步骤。应理解，此处为了方便描述，故通过步骤S501至步骤S504这一顺序进行描述，并不旨在限定一定通过上述顺序进行执行。本申请实施例对于上述一个或多个步骤的执行的先后顺序、执行的时间、执行的次数等不做限定。步骤S501至步骤S504具体如下：

步骤S501：第一节点生成第一信息。

其中，第一信息是与通信安全相关的参数。作为一种可能的实现，第一信息包括安全算法指示、密钥指示、参与安全算法的参数的指示、或安全相关的状态指示等中的一项或者多项。其中，安全算法包括加密算法、完整性保护算法、密钥派生算法、或密钥协商算法等中的一项或者多项。密钥是执行安全算法的过程中输入的、具有机密性的参数。参与安全算法的参数是除了密钥之外，在执行安全算法中输入的参数，比如加密盐、或新鲜参数等，从而进一步提高安全性。安全相关的状态指示可用于配置状态参数，例如安全相关的状态指示可包括第一指示(下文中介绍)，该第一指示用于指示加密和/或完整性保护的开启状态。

一些可能的实施方式中，第一信息包括以下信息中的一项或者多项：完整性保护算法指示、完整性保护密钥指示、加密算法指示、加密密钥指示、第一参数或第一指示等。示例性地，第一信息包括完整性保护算法指示、完整性保护密钥指示、加密算法指示、加密密钥指示、第一参数和第一指示。再示例性地，第一信息包括完整性保护算法指示。再示例性地，第一信息包括加密算法指示。再示例性地，第一信息包括完整性保护算法指示和加密算法指示。再示例性地，第一信息包括完整保护算法指示、完整性保护密钥指示、加密算法指示和加密密钥指示。

其中，完整性保护算法指示用于指示第二节点和第三节点之间的链路使用的完整性保护算法，便于描述称为第一完整性保护算法，例如可以为AES-128算法、SM4算法等。比如，结合表1，当完整性保护算法指示取0100时，指示第二节点和第三节点之间的链路使用“INT1”算法进行完整性保护。再比如，当完整性保护算法指示取1000时，指示第二节点和第三节点之间的链路使用“AUTH1”算法进行完整性保护。

表1安全算法信息表

算法类型	算法名称	算法对应的值
加密算法	ENC0	0000
	ENC1	0001
	ENC2	0010
	ENC3	0011
完整性保护算法	INT1	0100
	INT2	0101
	INT3	0110
	INT4	0111
认证加密算法	AUTH1	1000
	AUTH2	1001
	AUTH3	1010
	AUTH4	1011

一些实施方式中，第一完整性保护算法为第二节点和第三节点支持的完整性保护算法中优先级最高的算法。比如，第二节点支持的完整性保护算法为INT1、INT2、INT4，而第三节点支持的完整性保护算法为INT1、INT2、INT3、INT4，若则二者共同支持的完整性保护算法为INT1、INT2、INT4的优先级分别为1、2和4（以数字越小优先级越高为例），则第一完整性保护算法为INT1。也即，第一节点可以从第二节点和第三节点支持的完整性保护算法中选择优先级最高的算法作为第一完整性保护算法。当然，前述的实施方式仅为示例，一些方式中，第一节点可通过其他方式确定第一完整性保护算法，例如基于其他规则选择某一完整性保护算法作为第一完整性保护算法。

完整性保护密钥指示用于指示完整性保护算法使用的密钥。

加密算法指示用于指示第二节点和第三节点之间的链路使用的第一加密算法，例如可以为AES-128算法、SM4算法等。结合表1，当加密算法指示取0000时，指示第二节点和第三节点之间的链路使用“ENC0”算法进行加密。再比如，加密算法指示取1000时，指示第二节点和第三节点之间的链路使用“AUTH1”算法进行加密。不难看出，加密算法和完整性保护算法可能使用同一种算法。

可选地，第一加密算法为第二节点和第三节点支持的加密算法中优先级最高的算法，或者，第一加密算法可为第一节点选择的算法。

加密密钥指示用于指示加密算法使用的密钥。

第一参数用于得到第二节点和第三节点之间的加密和/或完整性保护过程的输入参数。比如，第一参数为初始化基础值，为第一节点随机生成的64比特的数据。再如，第一参数为64比特的随机数经过处理后的得到的参数，比如将64比特的随机数中的部分或者全部比特与一段比特序列进行异或处理后得到的64比特

的数据。当然，前述的比特数仅为示例，具体实现中可替换为其他比特数。

步骤S502：第一节点向第二节点发送第一信息。

相应地，第二节点接收来自第一节点的第一信息。该第一信息用于对第二节点和第三节点之间传输的数据进行安全保护。

其中，第一节点分别与第二节点和第三节点连接，结合图5，第一节点与第二节点之间建立了通信链路。比如，第一节点为G节点，第二节点为T节点，第三节点为T节点，第一节点和第二节点之间建立了连接，第一节点和第三节点之间也建立了连接。

进一步地，第二节点被该第一节点管理。管理是指能够定义、决策、或配置另一节点的通信过程（例如分配通信的资源、或设置通信过程中参数等）。一些实施方式中，第二节点和第三节点被第一节点管理，即：第一节点为发送资源管理信息的节点，第二节点和第二节点为接收资源管理信息并根据所述资源管理信息进行数据的发送或接收的节点。示例性地，资源管理信息包括接入层资源管理信息。

可选地，第一信息可通过一条消息发送，也可通过多条消息发送。

一种可能的实现中，第一信息承载于（即携带于）第一消息中向第二节点发送。其中，第一消息用于指示第二节点与第三节点建立链路。比如，第一消息具有特定的格式或者携带了特殊的信息，以指示第二节点与第三节点建立链路。示例性地，第一消息中携带链路的配置信息，第二节点可基于该链路的配置信息与第三节点建立链路。一些方案中，第一消息也被称为异步 TT 链路建链指示，以指示第二节点和第三节点之间建立 TT 链路（或称 T-T 链路），T-T 链路即 T 节点和 T 节点之间的链路。当然，本申请对消息的名称不进行严格限定，具体实现中，消息的名称、信息的名称、参数的名称可任意替换。一些实施方式中，链路的配置信息属于资源管理信息（或接入层资源管理信息）。

请参见表 2 和表 3，表 2 和表 3 是本申请实施例提供的一种异步 TT 链路建链指示的消息格式示意图。其中，异步 TT 链路建链指示包括链路的配置信息，例如先发后发指示、无线帧类型指示、逻辑链路标识、带宽指示、导频密度指示、协议数据单元最大值、或最大时间偏移量等，具体可参见表 2，此处不再一一说明。如此，第二节点可基于链路的配置信息配置与第三节点之间的链路。

表 2 异步 TT 链路建链指示的字段名称、信令位宽、信令取值范围和数量单位

字段名称	信令位宽	信令取值范围	数量单位
……	……	……	……
先发后发指示	1比特	0-1	逻辑值
……	……	……	……
先发链路无线帧类型指示	4比特	0-15	枚举值
后发链路无线帧类型指示	4比特	0-15	枚举值
……	……	……	……
先发链路逻辑链路标识	24比特	0-(2^24-1)	数值
后发链路逻辑链路标识	24比特	0-(2^24-1)	数值
先发链路带宽指示	2比特	0-3	枚举值
后发链路带宽指示	2比特	0-3	枚举值
先发链路导频密度指示	2比特	0-3	枚举值
后发链路导频密度指示	2比特	0-3	枚举值
先发链路协议数据单元最大值	11比特	0-2047	字节
后发链路协议数据单元最大值	11比特	0-2047	字节
先发链路最大时间偏移量	9比特	(0-511)+1	基础时隙
后发链路最大时间偏移量	9比特	(0-511)+1	基础时隙
……	……	……	……
加密算法指示（可选）	8比特	0-255	数值
完整性保护算法指示（可选）	8比特	0-255	数值
加密密钥指示（可选）	128比特	0-(2^128-1)	数值
完整性保护密钥指示（可选）	128比特	0-(2^128-1)	数值
第一指示（可选）	8比特	0-255	数值

初始化基础值（可选）	64比特	0-(2^64-1)	数值
……	……	……	……

表 3 异步 TT 链路建链指示的字段名称及信令描述

字段名称	信令描述
……	……
先发后发指示	指示信令接收方在事件中先发送数据还是后发送数据，0为先发，1为后发
先发链路无线帧类型指示	指示先发链路无线帧类型
后发链路无线帧类型指示	指示后发链路无线帧类型
……	……
先发链路逻辑链路标识	先发链路逻辑链路标识
后发链路逻辑链路标识	后发链路逻辑链路标识
先发链路带宽指示	0：1MHz 1：2MHz 2：4MHz 3：预留
后发链路带宽指示	0：1MHz 1：2MHz 2：4MHz 3：预留
先发链路导频密度指示	0：4:1 1：8:1 2：16:1 3：无导频
后发链路导频密度指示	0：4:1 1：8:1 2：16:1 3：无导频
先发链路协议数据单元最大值	指示先发链路协议数据单元最大值
后发链路协议数据单元最大值	指示后发链路协议数据单元最大值
先发链路最大时间偏移量	先发链路发送无线帧的最大时长(包含收发间隔时间)，以基础时隙为单位
后发链路最大时间偏移量	后发链路发送无线帧的最大时长(包含收发间隔时间)，以基础时隙为单位
……	……
加密算法指示（可选）	指示TT链路使用的加密算法
完整性保护算法指示（可选）	指示TT链路使用的完整性保护算法
加密密钥指示（可选）	指示加密算法使用的密钥
完整性保护密钥指示（可选）	指示完整性保护算法使用的密钥
第一指示（可选）	0：加密和完整性保护同时启动 1：不启动加密，启动完整性保护 2：启动加密，不启动完整性保护 3：不启动加密，不启动完整性保护 4-255：预留
初始化基础值（可选）	安全算法使用的初始化基础值

又一种可能的实现中，第一节点向第二节点发送第一消息，第一消息用于指示第二节点与第三节点建立链路。但第一信息并不承载于第一消息，而是通过额外的消息指示，例如，通过第三消息承载。一些方案中，第三消息被称为安全参数信息。

一些实施方式中，第一节点还向第二节点发送第一指示。第一指示承载于第一字段，第一字段的取值可指示第二节点和第三节点之间的链路的加密和完整性保护的启动状态。示例性地，结合表3，第一指示

通过8比特的字段指示，当第一字段为第一值（如0）时，指示第二节点和第三节点之间的链路加密和启动完整性保护同时启动。当第一字段为第二值（如1）时，指示第二节点和第三节点之间的链路不启动加密，启动完整性保护。当第一字段为第三值（如2）时，指示第二节点和第三节点之间的链路启动加密，不启动完整性保护。当第一字段为第四值（如3）时，指示第二节点和第三节点之间的链路启动加密，不启动完整性保护。一些场景中，第一指示可称为加密和完整性保护指示。进一步的，第一指示可包括两个指示，以分别指示加密的开启状态和完整性保护的开启状态。

一些实施方式中，第一指示包括于第一信息。又一些实施方式中，第一指示可承载于第一消息，第一字段为第一消息中的字段。或者可选地，第一指示可承载于第三消息，第一字段为第一消息中的字段。当然，第一指示可携带于其他消息中发送给第二节点，例如携带于第五消息中发送，第五消息与第一消息和第三消息不同。

一些实施方式中，第一节点还向第二节点发送第二指示，第二指示用于指示第二节点先发送数据或后发送数据。比如，第二指示承载于第二字段，第二字段的取值可指示第二节点先发送数据或后发送数据。其中，在事件中先发送数据的节点为先发节点，同理，在事件中后发送数据的节点为后发节点。

可选地，第二指示可承载于第一消息，第二字段为第一消息中的字段。或者可选地，第二指示可承载于第三消息，第二字段为第三消息中的字段。

步骤S503：第一节点向第三节点发送第一信息。

相应地，第三节点接收来自第一节点的第一信息。

第一信息用于对第二节点和第三节点之间传输的数据进行安全保护。而第一节点与第三节点连接，结合图5，第一节点与第三节点之间建立了通信链路。比如，第一节点为G节点，第三节点为T节点，第一节点和第三节点之间建立了G-T链路。进一步地，第三节点被该第一节点管理。

一种可能的实现中，第一信息承载于（即携带于）第二消息中向第三节点发送。其中，第二消息用于指示第三节点与第二节点建立链路。相关描述可参见前述对第二消息的介绍。一些方案中，第一消息也被称为异步 TT 链路建链指示。

又一种可能的实现中，第一节点向第三节点发送第二消息，第二消息用于指示第三节点与第二节点建立链路。但第一信息并不承载于第二消息，而是通过额外的消息指示，例如，通过第四消息承载。一些方案中，第四消息被称为安全参数信息。

一些实施方式中，第一节点还向第三节点发送第一指示，第一指示承载于第一字段，第一字段的取值可指示第二节点和第三节点之间的链路的加密和完整性保护的启动状态。可选地，第一指示包括于第一信息。可选地，第一指示可承载于第二消息，第一字段为第二消息中的字段。或者可选地，第一指示可承载于第四消息，第一字段为第四消息中的字段。

一些实施方式中，第一节点还向第三节点发送第三指示，第三指示用于指示第三节点先发送数据或后发送数据。比如，第三指示承载于第三字段，第三字段的取值可指示第三节点先发送数据或后发送数据。

可选地，第三指示可承载于第二消息，第三字段为第二消息中的字段。或者可选地，第三指示可承载于第四消息，第三字段为第四消息中的字段。

步骤S504：第二节点基于第一信息对第一数据进行安全保护。

第一数据为第二节点和第三节点之间传输的数据，安全保护包括加密和/或完整性保护等。下面列举几种可能的实现方式：

实现方式一，第二节点基于第一完整性保护算法和完整性保护密钥对第一数据进行完整性保护。可选地，第一完整性保护算法和完整性保护密钥可通过第一信息中的信息指示，例如，第一信息包括完整性保护算法指示和完整性保护密钥指示，完整性保护算法指示用于指示第一完整性保护算法，完整性保护密钥指示用于指示完整性保护密钥。或者可选地，第一完整保护算法或完整性保护密钥还可以是第二节点和第三节点协商得到的。

以第一数据为第二节点向第三节点发送的数据为例，第二节点基于第一完整性保护算法和完整性保护密钥计算得到完整性检查码，并向第三节点发送完整性检查码和第一数据，第三节点可根据完整性检查码，检查第一数据的完整性。

以第一数据为第三节点向第二节点发送的数据为例，第三节点基于第一完整性保护算法和完整性保护密钥计算得到完整性检查码，并向第二节点发送完整性检查码和第一数据。第二节点可第一完整性保护算法和完整性保护密钥计算校验码，并基于该校验码和完整性检查码检查第一数据的完整性。

下面以第二节点侧为例，示例性地介绍一种进行完整性保护的过程。第二节点基于第一完整性保护算

法、完整性保护密钥、第一完整性保护输入和第一数据，计算得到完整性检查码。作为一种完整性保护过程的示例，第一数据为传输数据包的有效载荷或第一数据携带与传输数据包的有效载荷，结合图6，第一个计算过程基于第一完整性保护算法、会话密钥和第一完整性保护输入（即图6所示的输入0），得到第一输出（即图6所示的输出0）。第二个计算过程基于第一完整性保护算法、会话密钥、第一输出和第二完整性保护输入（即图6所示的输入1），得到第二输出（即图6所示的输出1）。其中，“⊕”表示异或操作。第三个计算过程基于第一完整性保护算法、会话密钥、第二输出和传输数据包的有效载荷的第1个M字节得到对应有效载荷的第1个字节的完整性保护输出，M为整数且M≥1，例如，M为16、或32等。

在传输数据包的有效载荷小于等于M个字节的情况下，对应有效载荷的第1个字节的完整性保护输出为最终输出（即图6所示的输出2）。在传输数据包的有效载荷大于M个字节的情况下，第三个计算过程会执行多次，在第i次计算过程中，基于第一完整性保护算法、会话密钥和对应有效载荷的第i-1个M字节的完整性保护输出，得到对应有效载荷的第i个M字节的完整性保护输出，并将对应有效载荷的最后部分字节的完整性保护输出作为最终输出，其中，i为整数且i分别取1至$\left\lceil\frac{\text{有效载荷字节数}}{M}\right\rceil$之间的整数。基于最终输出可得到完整性检查码。应理解，当i取$\left\lceil\frac{\text{有效载荷字节数}}{M}\right\rceil$时，第i个M字节是指有效载荷的最后部分字节，该第i个M字节的实际字节数可能为M，也可能小于M。

可选地，基于最终输出得到完整性检查码，包括：将最终输出中的X位作为完整性检查码。如图6，虚线表示对剩余字节进行循环计算，直到将有效载荷的字节计算完成，而输出N即对应有效载荷的最后部分字节的完整性保护输出，将输出N中的X位作为完整性检查码。例如，将输出N的低位4个字节作为完整性检查码。

可选地，会话密钥包括完整性保护密钥、加密密钥、或认证加密密钥等。一些方案中，在得到完整性检查码的过程中，该会话密钥可替换为完整性保护密钥。

一些可能的实施方式中，第一完整性保护输入（即图6所示的输入0）包括方向指示、或第二参数等。其中，方向指示用于指示第一数据的发送方和接收方在事件中发送数据的先后顺序。示例性地，当方向指示为第五值时，指示先发节点发后发节点收。当方向指示为第六值时，指示后发节点发先发节点收。先发节点为在事件中先发送数据的节点，后发节点为在事件中后发送数据的节点。

第二参数属于参与安全算法的参数，可选为随机数，或者为基于随机数处理得到的参数。一些方案中，第二参数被称为初始化向量。

一种实现中，第二参数与前述第一参数相关，第一参数可选由第一节点提供给第二节点。比如，第一参数为A个比特的初始化基础值，基于另一比特序列（例如为B个比特）对该初始化基础值进行处理（例如异或、同或等处理），得到的最终值作为第二参数，其中A、B为大于等于1的整数。可选地，前述的B个比特的比特序列可与无线帧类型相关，可选地，无线帧类型为第二节点发送的无线帧的类型，或者第三节点发送的无线帧的类型。示例性地，第二参数占用64比特，其中，初始化基础值为通过随机数生成器生成一个64比特的值，对于无线帧类型1和无线帧类型2，第二参数为将该初始化基础值的低32比特与同步序列的低32比特异或得到的最终取值（64比特）。对于无线帧类型3和无线帧类型4，第二参数为将该初始化基础值的低24比特与逻辑链路标识的24比特异或得到的最终取值。

又一种实现中，第二参数与来自第二节点的第三参数和/或来自第三节点的第四参数相关。比如，第二节点提供第三参数而第三节点提供第四参数，第二节点基于第三参数和第四参数得到第二参数。示例性地，第二节点向第三节点发送第三参数（如32比特），而第三节点向第二节点发送第四参数（32比特），第二参数为拼接第三参数和第四参数得到的64比特的值。

第一完整性保护输入可选还包括其他信息，如标志位、有效载荷计数、或数据长度等中的一项或者多项。为了便于理解，下面结合图7介绍一种可能的第一完整性保护输入所包括的内容，第一完整性保护输入包括标志（1字节）、随机数（13字节）、数据长度高位（1字节）和数据长度低位（1字节）。示例性地，标志的取值可为第一标志值，该第一标志值可预先定义或者自定义，例如由第一节点、第二节点、或第三节点中的一个节点定义或者多个节点协商得到，比如第一标志值为0x49。随机数包括有效载荷计数、方向指示和初始化向量，其中，有效载荷计数占用39比特，指传输数据包有效载荷的累加编号。方向指示占用1比特，1表示先发节点发后发节点收，0表示先发节点收后发节点发。初始化向量（可看作第二参数）占用64比特。其确定方式为：先使用随机数生成器生成一个64比特的初始化基础值（该基础值可为第一参数，可选由第一节点或第二节点或第三节点生产），对于无线帧类型1和无线帧类型2，将该初始化基础值的低32比特与同步序列的低32比特异或得到的最终取值（64比特），对于无线帧类型3和无线帧类型4，将

该初始化基础值的低24比特与逻辑链路标识的24比特异或得到的最终取值。数据长度占用11比特，有效载荷占用的字节数。其中，数据长度高位字节占用3比特，为11比特数据长度的高3比特的取值。数据长度低位字节占用8比特，为11比特数据长度的低8比特的取值。数据长度高位其余5比特值为0。

实现方式二，第二节点基于第一加密算法和加密密钥对第一数据进行加密/或解密。例如，对于第二节点发送给第三节点的数据，第二节点基于第一加密算法和加密密钥对第一数据进行加密后发送。对于第三节点发送给第二节点的数据，第二节点基于第一加密算法和加密密钥，解密经过加密的第一数据，得到第一数据的明文。可选地，第一加密算法和加密密钥可通过第一信息中的信息指示，例如，第一信息包括加密算法指示和加密密钥指示，加密算法指示用于指示第一加密算法，加密密钥指示用于指示加密密钥。或者可选地，第一加密算法或加密密钥还可以是第二节点和第三节点协商得到的。

下面以第二节点进行加密为例，介绍一种加密过程。

一些实施方式中，第二节点可基于第一加密算法、加密密钥和加密输入，对第一数据进行加密。其中，加密输入包括方向指示和/或第二参数。作为一种加密过程的示例，第一数据为传输数据包的有效载荷或第一数据携带与传输数据包的有效载荷，结合图8，对于有效载荷的所有字节，基于第一加密算法、会话密钥、有效载荷的第j个K字节和对应第j个K字节的加密输入，得到第j个加密输出，j为整数且j分别取1至$\left\lceil\frac{\text{有效载荷字节数}}{k}\right\rceil$之间的整数，K为整数且K≥1，例如，K为16、或32等，可选K=M。比如，对于有效载荷的第1个K字节，基于输入1、会话密钥和第一加密算法得到输出，并将输出与有效载荷的第1个K字节进行异或（使用“⊕”表示），得到加密的有效载荷。同理，对于有效载荷的第2个K字节，基于输入2、会话密钥和第一加密算法得到输出，并将输出与有效载荷的第2个K字节进行异或（使用“⊕”表示），得到加密的有效载荷。以此类推，直到有效载荷的剩余字节加密完成。应理解，当j取$\left\lceil\frac{\text{有效载荷字节数}}{k}\right\rceil$时，第j个K字节是指有效载荷的最后部分字节，该第j个K字节的实际字节数可能为K，也可能小于K。

一些可能的实施方式中，在第二节点和第三节点之间的完整性保护开启的情况下，基于第一加密算法、会话密钥、完整性检查码和对应完整性检查码的加密输入（如图8所示的输入0），得到加密的完整性检查码。

可选地，会话密钥包括完整性保护密钥、加密密钥、或认证加密密钥等。一些方案中，在加密过程中，该会话密钥可替换为加密密钥。进一步地，加密密钥可与完整性保护密钥相同，即参与加密过程的会话密钥和参与完整性保护过程的会话密钥可相同，当然，二者也可不同。

一些可能的实施方式中，加密过程中的加密输入（如图8所示的输入0、输入1、或输入2等）可包括方向指示和/或第二参数，可选还包括其它信息，如标志位、有效载荷计数、或处理计数等中的一项或者多项。关于方向指示和第二参数的详细描述参见实现方式一。

为了便于理解，下面结合图9介绍一种可能的加密输入所包括的内容，加密输入包括标志（1字节）、随机数（13字节）、处理编号计数高位（1字节）和处理编号计数低位（1字节）。其中，标志的取值可以为第二标志值，该第二标志值可预先定义或者自定义，例如由第一节点、第二节点、或第三节点中的一个节点定义或者多个节点协商得到，比如第二标志值为0x01。随机数包括有效载荷计数、方向指示和初始化向量，其中，有效载荷计数占用39比特，指传输数据包有效载荷的累加编号。方向指示占用1比特，1表示先发节点发后发节点收，0表示先发节点收后发节点发，可选在单发或者单收场景下忽略。初始化向量占用64比特，其确定方式为：先使用随机数生成器生成一个64比特的初始化基础值（该基础值可为第一参数，可选由第一节点或第二节点或第三节点生产），对于无线帧类型1和无线帧类型2，将该初始化基础值的低32比特与同步序列的低32比特异或得到最终取值（64比特），对于无线帧类型3和无线帧类型4，将该初始化基础值的低24比特与逻辑链路标识的24比特异或得到最终取值。处理编号计数可用于指示进行加密处理的次数计数，以图8为例，输入0对应的处理编号计数为0，输入1对应的处理编号计数为1，以此类推，输入N对应的处理编号计数为N。其中，处理编号计数高位字节占用8比特，为16比特处理编号计数的高8比特的取值；处理编号计数低位字节占用8比特，指16比特处理编号计数的低8比特的取值。

应理解，以上加密和完整性保护的过程可以进行组合。一种示例性的实施方式中，在第二节点和第三节点之间的加密和完整性保护均开启的情况下，第二节点对第一数据进行完整性保护并对完整性检查码和第一数据进行加密。再一种示例性的实施方式中，在第二节点和第三节点之间的加密开启但完整性保护不开启的情况下，第二节点对第一数据进行加密。再一种示例性的实施方式中，在第二节点和第三节点之间的加密不开启但完整性保护开启的情况下，第二节点对第一数据进行完整性保护。

在一些可能的实施方式中，第二节点可与第三节点之间建立链路，该第一数据可以为通过第二节点和第三节点之间的链路传输的。比如，第二节点可接收第一消息，第一消息包括链路的配置信息，第二节点

基于链路的配置信息与第三节点建立通信链路。进一步地，第二节点和第三节点基于安全参数（即安全算法、安全密钥及参与安全算法的参数等）对第二节点和第三节点之间的链路进行加密和/或完整性保护，如此，通过该链路进行传输的数据可以基于安全参数进行加密和/或完整性保护。

在图 5 所示的实施例中，第二节点和第三节点是被第一节点所管理的两个节点，而第一节点可以为二者生成第一信息，使得第二节点和第三节点均可基于第一节点提供的第一信息，对二者之间的数据传输过程进行安全保护。一方面，本申请实现了被其他节点所管理的两个节点之间的数据传输，提升了数据传输的效率。另一方面，二者之间通信的数据可基于第一节点生成并分发的信息来进行安全保护，提升了通信安全性。

请参见图10，图10是本申请实施例提供的又一种通信方法的流程示意图。可选地，该方法可以应用于通信系统，例如前述图1至图4中的一种或者多种通信系统。如图10所示的通信方法可以包括步骤S1001和/或步骤S1005中的一个或者多个步骤。应理解，此处为了方便描述，故通过步骤S1001至步骤S1005这一顺序进行描述，并不旨在限定一定通过上述顺序进行执行。本申请实施例对于上述一个或多个步骤的执行的先后顺序、执行的时间、执行的次数等不做限定。步骤S1001至步骤S1005具体如下：

步骤S1001：第一节点向第二节点发送第一消息。

相应地，第二节点接收来自第一节点的第一消息。

其中，第一消息用于指示第二节点与第三节点建立链路。比如，第一消息具有特定的格式或者携带了特殊的信息，以指示第二节点与第三节点建立链路。示例性地，第一消息中携带链路的配置信息，第二节点可基于该链路的配置信息与第三节点建立链路。一些方案中，第一消息也被称为异步 TT 链路建链指示，以指示第二节点和第三节点之间建立 TT 链路（或称 T-T 链路），T-T 链路即 T 节点和 T 节点之间的链路。当然，本申请对消息的名称不进行严格限定，具体实现中，消息的名称、信息的名称、参数的名称可任意替换。

请参见表 2 和表 3，表 2 和表 3 是本申请实施例提供的一种异步 TT 链路建链指示的消息格式示意图。其中，异步 TT 链路建链指示包括链路的配置信息，例如先发后发指示、无线帧类型指示、逻辑链路标识、带宽指示、导频密度指示、协议数据单元最大值、或最大时间偏移量等，具体可参见表 2，此处不再一一说明。如此，第二节点可基于链路的配置信息配置与第三节点之间的链路。

步骤S1002：第一节点向第三节点发送第二消息。

相应地，第三节点接收来自第一节点的第二消息。

其中，第二消息用于指示第三节点与第二节点建立链路。

步骤 S1003：第二节点与第三节点建立通信连接。

步骤 S1004：第二节点与第三节点协商确定第一信息。

第一信息包括以下信息中的一项或者多项：完整性保护算法指示、完整性保护密钥指示、加密算法指示、加密密钥指示或第一参数。

步骤 S1005：第二节点基于第一信息对第一数据进行安全保护。

示例性地，第二节点和第三节点基于安全参数（即安全算法、安全密钥及参与安全算法的参数等）对第二节点和第三节点之间的链路进行加密和/或完整性保护，而通过该链路进行传输的数据可以基于安全参数进行加密和/或完整性保护。

安全保护的具体过程可参见步骤 S504 中的描述。

以上图 5、图 10 所示的实施例提供了多种可能的方案，下面继续结合图 11、图 12、图 13 或图 14 对其中的部分可能设计进行示例性的说明。应理解，图 11、图 12、图 13 或图 14 所示实施例中的逻辑、术语等可以参见前述。另外，本申请部分图示中，将消息指示的信息通过括号在附图中进行了示意性的描述，但这并不表示对消息内容的严格限定。

请参见图11，图11是本申请实施例提供的又一种通信方法的流程示意图。可选地，该方法应用于前述的通信系统。如图11所示的通信方法可以包括步骤S1101和/或步骤S1103中的一个或者多个步骤。步骤S1101至步骤S1103具体如下：

步骤 S1101：第一节点向第二节点发送第一消息。

其中，第一节点和第二节点之间建立了通信连接，例如建立了 G-T 链路。

第一消息用于指示第二节点与第三节点建立链路，比如，第一消息为 TT 链路建链指示，一些方案中，该第一消息还可以称为异步 TT 链路建链指示。

其中，第一消息包括第一信息。示例性地，第一信息包括以下信息中的一项或者多项：完整性保护算法指示、完整性保护密钥指示、加密算法指示、加密密钥指示或第一参数等。第一信息可由第一节点生成。

进一步地，第一消息还包括链路的配置信息，例如先发后发指示、无线帧类型指示、逻辑链路标识、带宽指示、导频密度指示、协议数据单元最大值、或最大时间偏移量等，具体可参见表 2。如此，第二节点可基于链路的配置信息建立、配置与第三节点之间的链路。

步骤 S1102：第一节点向第三节点发送第二消息。

其中，第一节点和第三节点之间建立了通信连接，例如建立了 G-T 链路。

第二消息用于指示第二节点与第三节点建立链路，比如，第二消息为 TT 链路建链指示，一些方案中，该第二消息还可以称为异步 TT 链路建链指示。第二消息包括第一信息，示例性地，第一信息包括以下信息中的一项或者多项：完整性保护算法指示、完整性保护密钥指示、加密算法指示、加密密钥指示或第一参数等。

进一步地，第二消息还包括链路的配置信息，第三节点可基于链路的配置信息建立、配置与第二节点之间的链路。

步骤 S1103：第二节点和第三节点基于配置的第一信息通信。

示例性地，第二节点和第三节点基于配置的第一信息，对第二节点和第三节点之间传输的数据进行安全保护，具体可参见步骤 S504。

在图 11 所示的实施例中，第二节点与第三节点可被第一节点指示建立二者之间的点对点的链路。而第一信息可在第一消息中携带，可减少建立链路过程中的信令数量，提升传输的效率。

请参见图12，图12是本申请实施例提供的又一种通信方法的流程示意图。可选地，该方法应用于前述的通信系统。如图12所示的通信方法可以包括步骤S1201和/或步骤S1205中的一个或者多个步骤。步骤S1201至步骤S1205具体如下：

步骤 S1201：第一节点向第二节点发送第一消息。

其中，第一节点和第二节点之间建立了通信连接，例如建立了 G-T 链路。

第一消息用于指示第二节点与第三节点建立链路。比如，第一消息为 TT 链路建链指示，一些方案中，该第一消息还可以称为异步 TT 链路建链指示。示例性地，第一消息还包括链路的配置信息，例如先发后发指示、无线帧类型指示、逻辑链路标识、带宽指示、导频密度指示、协议数据单元最大值、或最大时间偏移量等，具体可参见表 2。如此，第二节点可基于链路的配置信息建立、配置与第三节点之间的链路。

步骤 S1202：第一节点向第三节点发送第二消息。

其中，第一节点和第三节点之间建立了通信连接，例如建立了 G-T 链路。

第二消息用于指示第二节点与第三节点建立链路，比如，第二消息为 TT 链路建链指示，一些方案中，该第二消息还可以称为异步 TT 链路建链指示。进一步地，第二消息还包括链路的配置信息，第三节点可基于链路的配置信息建立、配置与第二节点之间的链路。

步骤 S1203：第一节点向第二节点发送第三消息。

第三消息包括第一信息。示例性地，第一信息包括加密算法指示、完整性保护算法指示、加密密钥指示、完整性保护密钥指示、第一指示和第一参数。第一信息可由第一节点生成。

详细说明可参见前述。示例性地，第三消息可称为安全参数指示信息。

步骤 S1204：第一节点向第三节点发送第四消息。

第四消息包括第一信息。示例性地，第一信息包括加密算法指示、完整性保护算法指示、加密密钥指示、完整性保护密钥指示、第一指示和第一参数。具体说明可参见前述。示例性地，第四消息可称为安全参数指示信息。

步骤 S1205：第二节点和第三节点基于配置的第一信息通信。

示例性地，第二节点和第三节点基于配置的安全参数（即安全算法、安全密钥及参与安全算法的参数等）对第二节点和第三节点之间的链路进行加密和/或完整性保护，而通过该链路进行传输的数据可以基于安全参数进行加密和/或完整性保护。具体过程可参见步骤 S504 中的描述。

在图12所示的实施例中，第一节点向第二节点发送第一消息以指示第二节点与第三节点建立通信链路，并通过额外的消息（如第三消息）将第一信息发送给第二节点，使得消息的功能更加细化、精细化，提升

消息格式的可复用性和组合灵活性。

比如，一些方案中，第一节点也可以指示另一个G节点与另一节点之间建立G-T链路（或G-G链路），此时，第一节点可向G节点发送G-T链路建链指示（或G-G链路建链指示）。由于G节点本身可配置安全相关的参数，第一节点无需向G节点发送安全相关的参数，因此G-T链路建链指示（或G-G链路建链指示）中无需设置与第一信息相关的字段。在上述实施例中，与安全相关的参数通过额外的第三消息、第四消息指示，细化了信令的功能，使得TT链路建链指示可G-T链路建链指示可使用同一消息格式，提升消息格式的可复用性和组合灵活性。

请参见图13，图13是本申请实施例提供的又一种通信方法的流程示意图。可选地，该方法应用于前述的通信系统。如图13所示的通信方法可以包括步骤S1301和/或步骤S1307中的一个或者多个步骤。步骤S1301至步骤S1307具体如下：

步骤 S1301：第一节点向第二节点发送第一消息。

其中，第一节点和第二节点之间建立了通信连接，例如建立了 G-T 链路。

第一消息用于指示第二节点与第三节点建立链路。比如，第一消息为 TT 链路建链指示，一些方案中，该第一消息还可以称为异步 TT 链路建链指示。示例性地，第一消息还包括链路的配置信息，例如先发后发指示、无线帧类型指示、逻辑链路标识、带宽指示、导频密度指示、协议数据单元最大值、或最大时间偏移量等，具体可参见表 2。如此，第二节点可基于链路的配置信息建立、配置与第三节点之间的链路。

可选地，第一消息可包括第一指示。

步骤 S1302：第一节点向第三节点发送第二消息。

其中，第一节点和第三节点之间建立了通信连接，例如建立了 G-T 链路。

第二消息用于指示第二节点与第三节点建立链路，比如，第二消息为 TT 链路建链指示，一些方案中，该第二消息还可以称为异步 TT 链路建链指示。进一步地，第二消息还包括链路的配置信息，第三节点可基于链路的配置信息建立、配置与第二节点之间的链路。

可选地，第二消息可包括第一指示。

步骤 S1303：第一节点向第二节点发送第三消息。

第三消息包括第一信息。示例性地，第一信息包括加密算法指示、完整性保护算法指示、加密密钥指示和完整性保护密钥指示。第一信息可由第一节点生成。示例性地，第三消息可称为安全参数指示信息。

步骤 S1304：第一节点向第三节点发送第四消息。

第四消息包括第一信息。示例性地，第一信息包括加密算法指示、完整性保护算法指示、加密密钥指示和完整性保护密钥指示。示例性地，第四消息可称为安全参数指示信息。

步骤 S1305：第二节点向第三节点发送第三参数。

示例性地，第三参数可称为第二节点初始化向量，例如为 32 比特。

步骤 S1306：第三节点向第二节点发送第四参数。

示例性地，第四参数可称为第三节点初始化向量，例如为 32 比特。

步骤 S1307：第二节点和第三节点进行安全通信。

其中，安全保护过程中所使用的第二参数通过第三参数和第四参数确定。例如，第二参数为 64 比特，且第二参数=第三参数+第四参数，其中+表示比特的联结。

可以看出，第二节点和第三节点可基于配置的第一信息和协商得到的第二参数，对第二节点和第三节点之间传输的数据进行安全保护。一些方案中，第二节点和第三节点基于安全参数（即安全算法、安全密钥及参与安全算法的参数等）对第二节点和第三节点之间的链路进行加密和/或完整性保护，而通过该链路进行传输的数据可以基于安全参数进行加密和/或完整性保护。

具体过程可参见步骤 S504 中的描述。

在图13所示的实施例中，第一节点向第二节点发送第一消息以指示第二节点与第三节点建立通信链路，并通过额外的消息（如第三消息）将第一信息发送给第二节点，使得消息的功能更加细化、精细化，提升消息格式的可复用性和组合灵活性。而且，第二节点和第三节点之间通过协商确定参与安全算法的参数（如第二参数），使得第二节点和第三节点之间的通信的安全性进一步提高。

请参见图14，图14是本申请实施例提供的又一种通信方法的流程示意图。可选地，该方法应用于前述的通信系统。如图14所示的通信方法可以包括步骤S1401和/或步骤S1405中的一个或者多个步骤。步骤

S1401至步骤S1405具体如下：

步骤 S1401：第一节点向第二节点发送第一消息。

其中，第一节点和第二节点之间建立了通信连接，例如建立了 G-T 链路。

第一消息用于指示第二节点与第三节点建立链路。比如，第一消息为 TT 链路建链指示，一些方案中，该第一消息还可以称为异步 TT 链路建链指示。示例性地，第一消息还包括链路的配置信息，例如先发后发指示、无线帧类型指示、逻辑链路标识、带宽指示、导频密度指示、协议数据单元最大值、或最大时间偏移量等，具体可参见表 2。如此，第二节点可基于链路的配置信息建立、配置与第三节点之间的链路。

步骤 S1402：第一节点向第三节点发送第二消息。

其中，第一节点和第三节点之间建立了通信连接，例如建立了 G-T 链路。

第二消息用于指示第二节点与第三节点建立链路，比如，第二消息为 TT 链路建链指示，一些方案中，该第二消息还可以称为异步 TT 链路建链指示。进一步地，第二消息还包括链路的配置信息，第三节点可基于链路的配置信息建立、配置与第二节点之间的链路。

步骤 S1403：第二节点和第三节点进行算法协商和密钥协商。

示例性地，第二节点可以向第三节点指示第二节点支持的安全算法，由第三节点从二者支持的安全算法中选择算法（例如选择优先级最高的算法）。或者，第三节点可以向第二节点指示第三节点支持的安全算法，由第二节点从二者支持的安全算法中选择算法（例如选择优先级最高的算法）。其中，安全算法包括加密算法、完整性保护算法和认证加密算法中的一项或者多项。

密钥协商可以通过 DH 算法确定，或者通过密钥信息确定。比如，第二节点和第三节点中设置了多个密钥，每个密钥对应了密钥信息。第二节点向第三节点发送密钥信息，第三节点基于密钥信息选择对应的密钥作为会话密钥。其中，会话密钥包括加密密钥、完整性保护密钥和认证加密密钥中的一项或者多项。

步骤 S1404：第二节点和第三节点协商确定第二参数。

比如，第二节点确定第二参数，并提供给第三节点。

或者，第三节点确定第二参数并提供给第二节点。

或者，第二节点确定第三参数并提供给第三节点，第三节点确定第四参数并提供给第二节点。第二参数基于第三参数和第四参数确定。

步骤 S1405：第二节点和第三节点进行安全通信。

示例性地，第二节点和第三节点基于协商得到的安全算法、会话密钥和参与安全算法的参数（如第二参数），对第二节点和第三节点之间传输的数据进行安全保护。安全保护的具体过程可参见步骤 S504。

在图14所示的实施例中，第一节点向第二节点发送第一消息以指示第二节点与第三节点建立通信链路，第二节点和第三节点之间通过协商确定安全算法、密钥和参与安全算法的参数（如第二参数），使得第二节点和第三节点之间的通信的安全性进一步提高。

上述详细阐述了本申请实施例的方法，下面提供本申请实施例的装置。

应理解,本申请实施例中所提供的装置，其中的单元的划分仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。此外，装置中的单元可以以处理器调用软件的形式实现。例如，装置中包括处理器，处理器与存储器连接，存储器中存储有指令，处理器调用存储器中存储的指令，以实现以上任一种方法或实现该装置各单元的功能，其中处理器例如为通用处理器，例如中央处理单元（central processing unit，CPU）或微处理器，存储器为装置内的存储器或装置外的存储器。

或者，装置中的单元可以以硬件电路的形式实现，可以通过对硬件电路的设计实现部分或全部单元的功能，该硬件电路可以理解为一个或多个处理器。例如，在一种实现中，该硬件电路为专用集成电路（application-specific integrated circuit，ASIC），通过对电路内元件逻辑关系的设计，实现以上部分或全部单元的功能。再如，在另一种实现中，该硬件电路为可以通过可编程逻辑器件（programmable logic device，PLD）实现，以现场可编程门阵列（Field Programmable Gate Array， FPGA）为例，其可以包括大量逻辑门电路，通过配置文件来配置逻辑门电路之间的连接关系，从而实现以上部分或全部单元的功能。

本申请实施例中，装置中的各单元可以是被配置成实施以上方法的一个或多个处理器（或处理电路），例如：CPU、（graphics processing unit，GPU）、神经网络处理单元（neural network processing Unit，NPU）、张量处理单元（tensor processing unit， TPU）、深度学习处理单元（deep learning processing unit, DPU）、微处理器（micro processor unit，MPU）、数字信号处理器（digital signal processor，DSP）、ASIC、FPGA，或这些处理器形式中至少两种的组合。

此外，以上装置中的各单元可以全部或部分可以集成在一起，或者可以独立实现。在一种实现中，这些单元集成在一起，以片上系统（system-on-a-chip，SOC，或称系统级芯片）的形式实现。该SOC中可以包括至少一个处理器，用于实现以上任一种方法或实现该装置各单元的功能，该至少一个处理器的种类可以不同，例如包括CPU和FPGA，或者包含CPU和人工智能处理器，或者包含CPU和GPU等。下面列举几种可能的装置。

请参见图15，图15是本申请实施例提供的一种通信装置的结构示意图。可选地，该通信装置150可以为独立设备，例如节点等。或者，该通信装置150也可以独立设备（如节点）中的一个器件，例如芯片或者集成电路等。该通信装置150用于实现前述的通信方法，例如图5，图10，图11，图12，图13，或图14所示的通信方法。

示例性地，通信装置 150 包含处理单元 1501 和通信单元 1502。其中，处理单元 1501 用于实现处理、确定、生成、计算、加密、解密等一项或者多项操作，通信单元 1502 用于实现发送、接收等一项或者多项操作。

一种可能的设计中，通信装置例如用于执行前述的通信方法中，由第一节点执行的方法。

在一种可能的实施方式中，处理单元 1501 用于生成第一信息。通信单元 1502 用于向第二节点发送第一信息，向第三节点发送第一信息。其中，该第一信息用于对第二节点和第三节点之间传输的数据进行安全保护。其中，第一节点分别与第二节点和第三节点连接，第二节点和第三节点被该第一节点管理。

在又一种可能的实施方式中，通信单元1502还用于向第二节点发送第一消息，第一信息承载于第一消息。可选地，第一消息中携带链路的配置信息，第二节点可基于链路的配置信息与第三节点建立链路。

在又一种可能的实施方式中，通信单元1502还用于向第三节点发送第二消息，第一信息承载于第二消息。可选地，第二消息中携带链路的配置信息，第三节点可基于链路的配置信息与第二节点建立链路。

在又一种可能的实施方式中，发送给第二节点的第一信息承载于第三消息中。也即，通信单元 1502 还用于向第二节点发送第三消息，第三消息包括第一信息。

在又一种可能的实施方式中，通信单元1502还用于向第二节点发送第一消息。其中，第一消息用于指示第二节点与第三节点建立通信链路。进一步地，该第一信息不承载于第一消息。

在又一种可能的实施方式中，通信单元 1502 还用于向第三节点发送第二消息，第二消息用于指示第三节点与第二节点建立通信链路。进一步地，第一信息不承载于第二消息。

在又一种可能的实施方式中，发送给第三节点的第一信息承载于第四消息中。也即，通信单元 1502 还用于向第三节点发送第四消息，第四消息包括第一信息。

相关描述参见前述实施例的描述，此处不再一一说明。

一种可能的设计中，通信装置例如用于执行前述的通信方法中，由第二节点执行的方法。

在一种可能的实施方式中，通信单元1502用于接收来自第一节点的第一信息。处理单元1501用于基于第一信息对第一数据进行安全保护，第一数据为在第二节点和第三节点之间传输的数据。

在一种可能的实施方式中，通信单元1502还用于接收来自第一节点的第一消息，第一信息承载于第一消息。其中，第一消息用于指示第二节点与第三节点建立连接。

在一种可能的实施方式中，通信单元1502还用于接收来自第一节点的第一消息。第一消息用于指示第二节点与第三节点建立连接。进一步地，第一信息不承载于第一消息。

在一种可能的实施方式中，通信单元1502还用于接收来自第一节点的第三消息，第一信息承载于第三消息。

在一种可能的实施方式中，处理单元1501和通信单元1502还用于与第三节点建立通信链路。

在一种可能的实施方式中，处理单元1501还用于基于第一完整性保护算法和完整性保护密钥，对第一数据进行完整性保护。

在一种可能的实施方式中，处理单元1501还用于基于第一完整性保护算法和完整性保护密钥，对第一数据进行完整性保护。其中，完整性保护密钥为第二节点和第三节点之间协商得到的。

在一种可能的实施方式中，处理单元1501还用于基于第一完整性保护算法和完整性保护密钥，对第一数据进行完整性保护。其中，第一完整性保护算法为第二节点和第三节点之间协商得到的。

在一种可能的实施方式中，处理单元1501还用于基于第一完整性保护算法、完整性保护密钥、第一完整性保护输入和第一数据，计算得到完整性检查码。

在一种可能的实施方式中，第一数据携带于传输数据包的有效载荷。处理单元1501还用于：基于第一完整性保护算法、完整性保护密钥和第一完整性保护输入，得到第一输出，基于第一完整性保护算法、完整性保护密钥、第一输出和第二完整性保护输入，得到第二输出，基于第一完整性保护算法、完整性保护密钥、第二输出和传输数据包的有效载荷的第一个M字节得到对应有效载荷的第1个字节的完整性保护输出，M为整数且M≥1。

在传输数据包的有效载荷小于等于M个字节的情况下，对应有效载荷的第1个字节的完整性保护输出为最终输出。在传输数据包的有效载荷大于M个字节的情况下，基于第一完整性保护算法、完整性保护密钥和对应有效载荷的第i-1个M字节的完整性保护输出，得到对应有效载荷的第i个M字节的完整性保护输出，将对应有效载荷的最后部分字节的完整性保护输出作为最终输出，其中，i为整数且i分别取1至$\left\lceil \frac{\text{有效载荷字节数}}{M} \right\rceil$之间的整数，根据最终输出得到完整性检查码。其中，[x]表示对x进行向上取整得到的整数。

可选地，根据最终输出得到完整性检查码，包括：将最终输出的低X位作为完整性检查码。

在一种可能的实施方式中，处理单元1501还用于基于第一加密算法和加密密钥对第一数据进行加密。

在一种可能的实施方式中，处理单元1501还用于基于第一加密算法和加密密钥对第一数据进行加密，其中，加密密钥为第二节点和第三节点之间协商得到的。

在一种可能的实施方式中，处理单元1501还用于基于第一加密算法和加密密钥对第一数据进行加密，其中，第一加密算法为第二节点和第三节点之间协商得到的。

在一种可能的实施方式中，处理单元1501还用于基于第一加密算法、加密密钥和加密输入，对第一数据进行加密。其中，加密输入包括方向指示和/或第二参数。

在一种可能的实施方式中，第一数据携带于传输数据包的有效载荷。处理单元1501还用于：对于有效载荷的所有字节，基于第一加密算法、加密密钥、有效载荷的第j个K字节和对应第j个K字节的加密输入，得到第j个加密输出，j为整数且j分别取1至$\left\lceil \frac{\text{有效载荷字节数}}{K} \right\rceil + 1$之间的整数。

在一种可能的实施方式中，在第二节点和第三节点之间的完整性保护开启的情况下，处理单元1501还用于基于第一加密算法、加密密钥、完整性检查码和对应完整性检查码的加密输入，得到加密的完整性检查码。

相关描述参见前述实施例的描述，此处不再一一说明。

一种可能的设计中，通信装置例如用于执行前述的通信方法中，由第二节点执行的方法。具体地，通信单元1502用于接收来自第一节点的第一消息，处理单元1501和通信单元1502用于与第三节点建立链路以及与第三节点协商确定第一信息，处理单元1501用于基于第一信息对第一数据进行安全保护。其中，第一消息用于指示第二节点与第三节点建立链路，第一数据为在第二节点和第三节点之间传输的数据。

在又一种可能的实施方式中，处理单元1501还用于基于第一完整性保护算法和完整性保护密钥，对第一数据进行完整性保护。

在又一种可能的实施方式中，处理单元1501还用于基于第一加密算法和加密密钥对第一数据进行加密。

相关描述参见前述实施例的描述，此处不再一一说明。

请参见图16，图16是本申请实施例提供的又一种通信装置的结构示意图。该通信装置160可以为独立设备，例如节点，也可以为包含于独立设备中的器件，例如芯片、软件模块、或集成电路等。该通信装置160可以包括至少一个处理器1601和通信接口1602。可选地，还可以包括至少一个存储器1603。进一步可选地，还可以包含连接线路1604，其中，处理器1601、通信接口1602和/或存储器1603通过连接线路1604相连，和/或，通过连接线路1604互相通信以传递控制信号和/或数据信号。

其中：

处理器1601是进行算术运算和/或逻辑运算的模块，具体可以包含以下模块中的一项或者多项：滤波器、调制解调器、功率放大器、低噪声放大器(low noise amplifier，LNA)、基带处理器、射频处理器、射频电路、中央处理器（central processing unit，CPU）、应用处理器(application processor，AP)、微电子控制单元(microcontroller unit, MCU)、电子控制单元(electronic control unit, ECU)、图形处理器(graphics processing unit，GPU)、微处理器（microprocessor unit，MPU）、专用集成电路（application specific integrated Circuit，ASIC）、图像信号处理器(image signal processor，ISP)、数字信号处理器(digital signal processor，DSP)、现场可编程逻辑门阵列（field programmable gate array，FPGA）、复杂可编程逻辑器件（complex programmable logic device，CPLD）、或协处理器等。

通信接口1602可以用于为至少一个处理器提供信息输入或者输出，或用于接收外部发送的信号和/或向外部发送信号。

例如，通信接口1602可以包含接口电路。

例如，通信接口1602可以包括诸如以太网电缆等的有线链路接口，也可以是无线链路（Wi-Fi、蓝牙、通用无线传输、车载短距通信技术以及其他短距无线通信技术等）接口。

可选地，通信接口1602还可以包括射频发射器、天线等。在通信接口1602包含天线的情况下，天线的数量可以是一个，也可以是多个。

作为一种可能的设计，若通信装置160为独立设备时，通信接口1602可以包括接收器和发送器。其中，接收器和发送器可以为相同的部件，或者为不同的部件。接收器和发送器为相同的部件时，可以将该部件称为收发器。

作为又一种可能的设计，若通信装置160为芯片或电路时，通信接口1602可以包括输入接口和输出接口，输入接口和输出接口可以是相同的接口，或者可以分别是不同的接口。

可选地，通信接口1602的功能可以通过收发电路或收发的专用芯片实现。

存储器1603用于提供存储空间，存储空间中可以存储操作系统和计算机程序等数据。存储器1603可以是随机存储记忆体（random access memory，RAM）、只读存储器（read-only memory， ROM）、可擦除可编程只读存储器（erasable programmable read only memory，EPROM）、或便携式只读存储器（compact disc read-only memory，CD-ROM）等等中的一种或者多种的组合。

其中，以上列举的通信装置160中各模块或单元的功能和动作仅为示例性说明。

通信装置160中各功能单元可用于实现前述的通信方法，例如图5，图10，图11，图12，图13，或图14所示的通信方法，例如用于执行第一节点或第二节点等执行的方法。

可选地，处理器1601，可以是专门用于执行前述方法的处理器（便于区别称为专用处理器），也可以是通过调用计算机程序来执行前述方法的处理器（便于区别称为专用处理器）。可选地，至少一个处理器还可以既包括专用处理器也包括通用处理器。

可选地，在通信装置160包括至少一个存储器1603的情况下，若处理器1601通过调用计算机程序来实现前述通信方法，该计算机程序可以存储在存储器1603中。

本申请实施例还提供了一种芯片，该芯片包括逻辑电路和通信接口。所述通信接口，用于接收信号或者发送信号；所述逻辑电路，用于通过所述通信接口接收信号或者发送信号。所述芯片用于实现前述的通信方法，例如图5，图10，图11，图12，图13，或图14所示的通信方法。

本申请实施例还提供了一种算机可读存储介质，所述计算机可读存储介质中存储有指令，当所述指令在至少一个处理器（或通信装置）上运行时，实现前述的通信方法，例如图5，图10，图11，图12，图13，或图14所示的通信方法。

本申请实施例还提供了一种计算机程序产品，该计算机程序产品包括计算机指令，所述计算指令用于实现前述的通信方法，例如图5，图10，图11，图12，图13，或图14所示的通信方法。

本申请实施例还提供了一种终端，该终端包含前述的通信装置150和/或通信装置160。

作为一种可能的实施方式，终端包含终端节点。进一步地，终端还包含第一管理节点和/或第二管理节点。进一步地，终端还包含控制节点。

示例性地，终端可以包含车辆、机器人、无人机、船舶、轮船等智能终端或交通工具。其中，车辆为广义概念上的车辆，可以是交通工具(如商用车、乘用车、摩托车、飞行车、火车等)，工业车辆(如：叉车、挂车、牵引车等)，工程车辆(如挖掘机、推土车、吊车等)，农用设备(如割草机、收割机等)等。再如，机器人可以为智能搬运机器人(automated guided vehicle，AGV)、可行走会话机器人、服务机器人等机器人。

需要说明的是，本申请实施例中，“示例性地”或者“例如”等词用于表示作例子、例证或说明。本申请中被描述为“示例性地”或者“例如”的任何实施例或设计方案不应被解释为比其他实施例或设计方案更优选或更具优势。确切而言，使用“示例性地”或者“例如”等词旨在以具体方式呈现相关概念。

本申请实施例中，信息和装置的名称等是为了方便理解本方案的内容进行地示例性地命名，在具体实现中，其名称可以有其他设计。此外，不同场景中（例如不同的通信层）对于同一个事物的名称也可以存在不同设计。例如，时间资源配置信息也可以称为参考信息等。再如，不同的通信层对于业务的数据的封装存在不同的命名，在应用层第一业务直接以数据的形式传输，但是在网络层该第一业务的数据被封装在第一业务的消息传输。

本申请中实施例提到的“至少一个”是指一个或者多个，“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和b）、（a和c）、（b和c）、或（a和b和c），其中a、b、c可以是单个，也可以是多个。“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，其中A、B可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。

以及，除非有相反的说明，本申请实施例使用“第一”、“第二”、“M1”、“M2”、“M3”、“M4”、“M5”、“S1”、“S2”、“S3”等序数词是用于对多个对象进行区分，不用于限定多个对象的顺序、时序、优先级或者重要程度。再如，第一节点、第二节点，只是为了方便在不同的实施方式中描述新鲜参数，并不表示其执行操作、重要程度、结构等的不同。

上述实施例中所用，根据上下文，术语“当……时”可以被解释为意思是“如果……”或“在……后”或“响应于确定……”或“响应于检测到……”。以上所述仅为本申请的可选实施例，并不用以限制本申请，凡在本申请的构思和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

权利要求书

1.一种通信方法，其特征在于，应用于第一节点，所述第一节点分别与第二节点和第三节点连接，所述第二节点和所述第三节点被所述第一节点管理，

所述方法包括：

生成第一信息，所述第一信息用于对所述第二节点和所述第三节点之间传输的数据进行安全保护；

向所述第二节点发送所述第一信息，以及向所述第三节点发送所述第一信息。

2.根据权利要求 1 所述的方法，其特征在于，所述向所述第二节点发送所述第一信息，包括：

向所述第二节点发送第一消息，所述第一信息承载于所述第一消息，所述第一消息用于指示所述第二节点与所述第三节点建立链路；

所述向所述第三节点发送所述第一信息，包括：

向所述第三节点发送第二消息，所述第一信息承载于所述第二消息，所述第二消息用于指示所述第三节点与所述第二节点建立链路。

3.根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

向所述第二节点发送第一消息，所述第一消息用于指示所述第二节点与所述第三节点建立链路；

向所述第三节点发送第二消息，所述第二消息用于指示所述第三节点与所述第二节点建立链路。

4.根据权利要求 1-3 任一项所述的方法，其特征在于，所述第一信息包括以下信息中的一项或者多项：

完整性保护算法指示、完整性保护密钥指示、加密算法指示、加密密钥指示或第一参数；

其中，所述完整性保护算法指示用于指示所述第二节点和所述第三节点之间的链路使用的第一完整性保护算法；

所述完整性保护密钥指示用于指示完整性保护算法使用的密钥；

所述的加密算法指示用于指示所述第二节点和所述第三节点之间的链路使用的第一加密算法；

所述加密密钥指示用于指示加密算法使用的密钥；

所述第一参数用于得到所述第二节点和所述第三节点之间的加密和/或完整性保护过程的输入参数。

5.根据权利要求 1-4 任一项所述的方法，其特征在于，所述第一信息还包括第一指示，所述第一指示承载于第一字段；

当所述第一字段为第一值时，指示所述第二节点和所述第三节点之间的链路加密和启动完整性保护同时启动；

或者，当所述第一字段为第二值时，指示所述第二节点和所述第三节点之间的链路不启动加密，启动完整性保护；

或者，当所述第一字段为第三值时，指示所述第二节点和所述第三节点之间的链路启动加密，不启动完整性保护；

或者，当所述第一字段为第四值时，指示所述第二节点和所述第三节点之间的链路不启动加密，不启动完整性保护。

6.一种通信方法，其特征在于，应用于第二节点，所述第二节点与第一节点连接，所述第一节点还与第三节点连接且所述第一节点管理所述第二节点和所述第三节点，

所述方法包括：

接收来自所述第一节点的第一信息；

基于所述第一信息对第一数据进行安全保护，所述第一数据为在所述第二节点和所述第三节点之间传输的数据。

7.根据权利要求 6 所述的方法，其特征在于，所述接收来自第一节点的第一信息，包括：

接收来自所述第一节点的第一消息，所述第一信息承载于所述第一消息，所述第一消息用于指示所述第二节点与所述第三节点建立链路。

8.根据权利要求 6 所述的方法，其特征在于，所述方法还包括：

接收来自所述第一节点的第一消息，所述第一消息用于指示所述第二节点与所述第三节点建立链路。

9.根据权利要求 6-8 任一项所述的方法，其特征在于，所述方法还包括：

与所述第三节点建立链路。

10.根据权利要求 6-9 任一项所述的方法，其特征在于，所述第一信息包括以下信息中的一项或者多项：

完整性保护算法指示、完整性保护密钥指示、加密算法指示、加密密钥指示或第一参数；

其中，所述完整性保护算法指示用于指示所述第二节点和所述第三节点之间的链路使用的第一完整性

保护算法，所述第一完整性保护算法为所述第二节点和第三节点支持的完整性保护算法中优先级最高的算法；

所述完整性保护密钥指示用于指示完整性保护算法使用的密钥；

所述的加密算法指示用于指示所述第二节点和所述第三节点之间的链路使用的第一加密算法，所述第一加密算法为所述第二节点和第三节点支持的加密算法中优先级最高的算法；

所述加密密钥指示用于指示加密算法使用的密钥；

所述第一参数用于得到所述第二节点和所述第三节点之间的加密和/或完整性保护过程的输入参数。

11.根据权利要求 6-10 任一项所述的方法，其特征在于，所述第一信息包括完整性保护算法指示和完整性保护密钥指示，所述完整性保护算法指示用于指示第一完整性保护算法，所述完整性保护密钥指示用于指示完整性保护密钥；

所述基于所述第一信息对第一数据进行安全保护，包括：

基于所述第一完整性保护算法和所述完整性保护密钥，对所述第一数据进行完整性保护。

12.根据权利要求 11 所述的方法，其特征在于，所述基于所述第一完整性保护算法和所述完整性保护密钥，对所述第一数据进行完整性保护，包括：

基于所述第一完整性保护算法、所述完整性保护密钥、第一完整性保护输入和所述第一数据，计算得到完整性检查码，所述完整性检查码用于检查所述第一数据的完整性；

其中，所述第一完整性保护输入包括方向指示和/或第二参数；

所述方向指示用于指示所述第一数据的发送方和接收方在事件中发送数据的先后顺序；

所述第二参数与所述第一信息包括的第一参数相关，或者，所述第二参数与来自第二节点的第三参数和/或来自所述第三节点的第四参数相关。

13.根据权利要求 6-12 任一项所述的方法，其特征在于，所述第一信息包括加密算法指示和加密密钥指示，所述加密算法指示用于指示第一加密算法，所述加密密钥指示用于指示加密密钥；

所述基于所述第一信息与所述第三节点进行安全通信，包括：

基于所述第一加密算法和所述加密密钥对所述第一数据进行加密。

14.根据权利要求 13 所述的方法，其特征在于，所述基于所述第一加密算法和所述加密密钥对所述第一数据进行加密，包括：

基于所述第一加密算法、所述加密密钥和加密输入，对所述第一数据进行加密；

所述加密输入包括方向指示和/或第二参数。

15.根据权利要求 12 或 14 所述的方法，其特征在于，

当所述方向指示为第五值时，指示先发节点发后发节点收；

当所述方向指示为第六值时，指示后发节点发先发节点收，所述先发节点为在事件中先发送数据的节点，所述后发节点为在事件中后发送数据的节点。

16.根据权利要求 6-15 任一项所述的方法，其特征在于，所述第一信息还包括第一指示，所述第一指示承载于第一字段；

当所述第一字段为第一值时，指示所述第二节点和所述第三节点之间的链路加密和启动完整性保护同时启动；

或者，当所述第一字段为第二值时，指示所述第二节点和所述第三节点之间的链路不启动加密，启动完整性保护；

或者，当所述第一字段为第三值时，指示所述第二节点和所述第三节点之间的链路启动加密，不启动完整性保护；

或者，当所述第一字段为第四值时，指示所述第二节点和所述第三节点之间的链路启动加密，不启动完整性保护。

17.一种通信方法，其特征在于，应用于第二节点，所述第二节点与第一节点连接，所述第一节点还与第三节点连接且所述第一节点管理所述第二节点和所述第三节点，

所述方法包括：

接收来自第一节点的第一消息，所述第一消息用于指示所述第二节点与所述第三节点建立链路；

与所述第三节点建立链路；

与所述第三节点协商确定第一信息；

基于所述第一信息对第一数据进行安全保护，所述第一数据为在所述第二节点和所述第三节点之间传

输的数据。

18.根据权利要求 17 所述的方法，其特征在于，所述第一信息包括以下信息中的一项或者多项：

完整性保护算法指示、完整性保护密钥指示、加密算法指示、加密密钥指示或第一参数；

其中，所述完整性保护算法指示用于指示所述第二节点和所述第三节点之间的链路使用的第一完整性保护算法；

所述完整性保护密钥指示用于指示完整性保护算法使用的密钥；

所述的加密算法指示用于指示所述第二节点和所述第三节点之间的链路使用的第一加密算法；

所述加密密钥指示用于指示加密算法使用的密钥；

所述第一参数用于得到所述第二节点和所述第三节点之间的加密和/或完整性保护过程的输入参数。

19.根据权利要求 17 或 18 所述的方法，其特征在于，第一消息包括第一指示，所述第一指示承载于第一字段；

当所述第一字段为第一值时，指示所述第二节点和所述第三节点之间的链路加密和启动完整性保护同时启动；

或者，当所述第一字段为第二值时，指示所述第二节点和所述第三节点之间的链路不启动加密，启动完整性保护；

或者，当所述第一字段为第三值时，指示所述第二节点和所述第三节点之间的链路启动加密，不启动完整性保护；

或者，当所述第一字段为第四值时，指示所述第二节点和所述第三节点之间的链路启动加密，不启动完整性保护。

20.一种通信装置，其特征在于，包括用于执行权利要求 1 至 5 任一项所述方法的单元或模块；

或者，包括用于执行权利要求 6 至 16 任一项所述方法的单元或模块；

或者，包括用于执行权利要求 17 至 19 任一项所述方法的单元或模块。

21.一种通信装置，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 19 任一项所述的方法。

22.一种通信系统，其特征在于，所述通信系统包括第一节点、第二节点和第三节点，所述第二节点用于执行权利要求 1-5 任一项所述的通信方法，所述第二节点和所述第三节点用于实现权利要求 6-16 任一项所述的通信方法。

23.一种通信系统，其特征在于，所述通信系统包括第一节点、第二节点和第三节点，所述第二节点用于向所述第二节点发送第一消息以及向所述第三节点发送所述第二消息，所述第二节点和所述第三节点用于实现权利要求 17-19 任一项所述的通信方法。

24.一种终端，其特征在于，所述终端包括权利要求 20 或 21 所述的通信装置，或者包括权利要求 22 或 23 所述的通信系统。

25.一种可读存储介质，其特征在于，所述可读存储介质用于存储计算机程序，当所述计算机程序被处理器执行时，使得包括所述处理器的通信装置执行如权利要求 1 至 19 中任一项所述的方法。

26.一种计算机程序，其特征在于，当所述计算机程序被处理器执行时，使得包括所述处理器的通信装置执行如权利要求 1 至 19 中任一项所述的方法。