

发送和接收物理层协议数据单元的方法和通信装置

本申请要求于 2023 年 4 月 21 日提交中国国家知识产权局、申请号为 202310469546.0、申请名称为“发送和接收物理层协议数据单元的方法和通信装置”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

本申请涉及通信领域，并且更具体地，涉及一种发送和接收物理层协议数据单元的方法和通信装置。

背景技术

近几年来，控制帧在数据通信中变得越来越重要，例如控制帧可以被用来进行上行数据传输调度。因而针对控制帧的攻击类型也越来越多。例如，攻击者假装是接入点（access point, AP），发送基本触发（Basic Trigger）帧等，让站点（station, STA）长时间的发送数据和报告，占据空口，消耗电量。因此，可以在控制帧中携带用于保护控制帧的信息，以防止针对控制帧的攻击。但是如何携带相应的保护信息以保护控制帧目前还未明确。

发明内容

本申请实施例提供一种发送和接收物理层协议数据单元的方法和通信装置，明确了控制帧的保护机制，能够有效防止针对控制帧的攻击。

第一方面，提供了一种发送物理层协议数据单元的方法，该方法可以由第一设备执行，或者，也可以由配置于第一设备中的芯片或电路执行，本申请对此不作限定。

该方法可以包括：生成物理层协议数据单元 PPDU，PPDU 包括控制帧，控制帧包括 N 个第一用户信息字段，其中，第一用户信息字段中的关联标识指示第一用户信息字段中承载第一信息，第一信息包括用于保护控制帧的信息，N 为大于或等于 1 的整数；发送 PPDU。

上述技术方案中，通过在控制帧中的第一用户信息字段中携带控制帧的保护信息，以防止控制帧被攻击。利用该控制帧保护机制，对于支持控制帧保护的接收端设备来说，可以基于第一用户信息字段中的关联标识确定第一用户信息字段携带控制帧的保护信息，对于不支持控制帧保护的接收端设备来说，第一用户信息字段会被当作一个不是发给自己的其他设备的用户信息字段，因此不影响不支持控制帧保护的接收端设备接收控制帧。

第二方面，提供了一种接收物理层协议数据单元的方法。该方法可以由第二设备执行，或者，也可以由配置于第二设备中的芯片或电路执行，本申请对此不作限定。

该方法可以包括：接收物理层协议数据单元 PPDU，PPDU 包括控制帧，控制帧包括 N 个第一用户信息字段，其中，第一用户信息字段中的关联标识指示第一用户信息字段中承载第一信息，第一信息包括用于保护控制帧的信息，N 为大于或等于 1 的整数；解析 PPDU。

关于第二方面的有益效果参见第一方面中的描述，这里不再赘述。

在第一方面或第二方面的某些实现方式中，第一信息包括秘钥标识，报文数 PN，和消息完整性代码 MIC 中的至少一项。

在第二方面的某些实现方式中，控制帧中承载 MIC，该方法还包括：确定本地 MIC；确定本地 MIC 与控制帧中承载的 MIC 匹配，则认为控制帧没有被伪造。

在第二方面的某些实现方式中，控制帧中承载 PN，该方法还包括：确定控制帧中承载的 PN 大于上一次接收到的 PN，则认为控制帧没有发生重播攻击。

在第一方面或第二方面的某些实现方式中，N 个第一用户信息字段的 N 个关联标识中的任一关联标识为预定义的数值。

在第一方面或第二方面的某些实现方式中，控制帧的公共字段中承载第二信息，第二信息指示控制帧中承载了第一信息。

在第一方面或第二方面的某些实现方式中，控制帧的公共字段中承载第三信息，第三信息指示 N 个第一用户信息字段中的至少一个第一用户信息字段的位置。

在第一方面或第二方面的某些实现方式中，控制帧中的公共字段或帧校验序列 FCS 字段中的至少一个字段中承载第四信息，第四信息包括用于保护控制帧的信息。

上述技术方案中，通过在 FCS 字段中携带控制帧保护信息，可以减少控制帧携带保护信息的开销，此外，还考虑因为信道质量差造成的控制帧传输错误和因为伪造造成的 MIC 错误。

在第一方面或第二方面的某些实现方式中，控制帧的帧校验序列 FCS 字段的第一位置上承载第一异或结果，第一异或结果为 FCS 字段的第一位置上对应的循环冗余码 CRC 与第五信息的异或结果，第五信息包括用于保护控制帧的信息，FCS 字段的第一位置上的 CRC 对应的比特值与第五信息对应的比特值的比特个数相同。

上述技术方案中，通过在 FCS 字段中携带控制帧保护信息，可以减少控制帧携带保护信息的开销，此外，还考虑因为信道质量差造成的控制帧传输错误和因为伪造造成的 MIC 错误。

在第一方面或第二方面的某些实现方式中，N 个第一用户信息字段中最后一个第一用户信息字段结束到控制帧结束之间的时长大于或等于第一类型设备的最小触发帧处理时间，第一类型设备为能够解读第一用户信息字段的关联标识的设备。

第三方面，提供了一种发送物理层协议数据单元的方法，该方法可以由第一设备执行，或者，也可以由配置于第一设备中的芯片或电路执行，本申请对此不作限定。

该方法可以包括：生成物理层协议数据单元 PPDU，PPDU 包括控制包裹帧，控制包裹帧中包括第一信息和控制帧，第一信息包括用于保护控制帧的信息；发送 PPDU。

上述技术方案中，利用现有或新定义的控制包裹（Wrapper）帧去携带控制帧保护信息，以防止控制帧被攻击。该控制帧保护机制可以适用于任何控制帧，由于该保护机制不需要对控制帧本身进行修改或重新定义，尤其适用于帧结构固定的控制帧。

第四方面，提供了一种接收物理层协议数据单元的方法。该方法可以由第二设备执行，或者，也可以由配置于第二设备中的芯片或电路执行，本申请对此不作限定。

该方法可以包括：接收物理层协议数据单元 PPDU，PPDU 包括控制包裹帧，控制包裹帧中包括第一信息和控制帧，第一信息包括用于保护控制帧的信息；解析 PPDU。

关于第四方面的有益效果参见第三方面中的描述，这里不再赘述。

在第三方面或第四方面的实现方式中，第一信息包括密钥标识，报文数 PN，和消息完整性代码 MIC 中的至少一项。

在第三方面的某些实现方式中，控制包裹帧中承载 MIC，该方法还包括：确定本地 MIC；确定本地 MIC 与控制帧中承载的 MIC 匹配，则认为控制帧没有被伪造。

在第三方面的某些实现方式中，控制包裹帧中承载 PN，该方法还包括：确定控制帧中承载的 PN 大于上一次接收到的 PN，则认为控制帧没有发生重播攻击。

在第三方面或第四方面的实现方式中，第一信息承载在高吞吐率控制字段中。

在第三方面或第四方面的实现方式中，第一信息承载在控制帧保护信息字段中。

在第三方面或第四方面的实现方式中，控制包裹帧为触发帧，触发帧的公共信息字段中的触发类型字段携带第一数值，第一数值指示控制包裹帧中包括控制帧保护信息字段和所承载的帧字段，第一数值为 8 至 15 中的任一数值，控制帧承载在所承载的帧字段。

第五方面，提供了一种发送物理层协议数据单元的方法，该方法可以由第一设备执行，或者，也可以由配置于第一设备中的芯片或电路执行，本申请对此不作限定。

该方法可以包括：生成物理层协议数据单元 PPDU，PPDU 包括聚合媒介访问控制协议数据单元 A-MPDU，A-MPDU 中包含第一媒介访问控制协议数据单元 MPDU 和第二 MPDU，其中，第一 MPDU 中承载控制帧，第二 MPDU 中承载第一信息，第一信息包括用于保护控制帧的信息；发送 PPDU。

上述技术方案中，利用将多个 MPDU 聚合起来的 A-MPDU，在 A-MPDU 的一个 MPDU（帧）中承载控制帧，在另外一个 MPDU 承载第一信息，即通过 A-MPDU 跨帧对控制帧进行保护，该控制帧保护机制可以适用于任何控制帧，由于该保护机制不需要对控制帧本身进行修改或重新定义，尤其适用于无法更改帧格式的控制帧。

第六方面，提供了一种接收物理层协议数据单元的方法。该方法可以由第二设备执行，或者，也可

以由配置于第二设备中的芯片或电路执行，本申请对此不作限定。

该方法可以包括：接收物理层协议数据单元 PPDU，PPDU 包括聚合媒介访问控制协议数据单元 A-MPDU，A-MPDU 中包含第一媒介访问控制协议数据单元 MPDU 和第二 MPDU，其中，第一 MPDU 中承载控制帧，第二 MPDU 中承载第一信息，第一信息包括用于保护控制帧的信息；解析 PPDU。

关于第六方面的有益效果参见第五方面中的描述，这里不再赘述。

在第五方面或第六方面的实现方式中，第一信息包括秘钥标识，报文数 PN，和消息完整性代码 MIC 中的至少一项。

在第六方面的某些实现方式中，第二 MPDU 中承载 MIC，该方法还包括：确定本地 MIC；确定本地 MIC 与控制帧中承载的 MIC 匹配，则认为控制帧没有被伪造。

在第六方面的某些实现方式中，第二 MPDU 中承载 PN，该方法还包括：确定控制帧中承载的 PN 大于上一次接收到的 PN，则认为控制帧没有发生重播攻击。

第七方面，提供一种通信装置，该通信装置包括：处理单元，用于生成物理层协议数据单元 PPDU，PPDU 包括控制帧，控制帧包括 N 个第一用户信息字段，其中，第一用户信息字段中的关联标识指示第一用户信息字段中承载第一信息，第一信息包括用于保护控制帧的信息，N 为大于或等于 1 的整数；通信单元，用于发送 PPDU。

第八方面，提供一种通信装置，该通信装置包括：通信单元，用于接收物理层协议数据单元 PPDU，PPDU 包括控制帧，控制帧包括 N 个第一用户信息字段，其中，第一用户信息字段中的关联标识指示第一用户信息字段中承载第一信息，第一信息包括用于保护控制帧的信息，N 为大于或等于 1 的整数；处理单元，用于解析 PPDU。

在第七方面或第八方面的某些实现方式中，第一信息包括秘钥标识，报文数 PN，和消息完整性代码 MIC 中的至少一项。

在第八方面的某些实现方式中，控制帧中承载 MIC，所述处理单元还用于，确定本地 MIC；所述处理单元还用于，确认本地 MIC 与控制帧中承载的 MIC 匹配，所述处理单元还用于，确认控制帧没有被伪造。

在第八方面的某些实现方式中，控制帧中承载 PN，所述处理单元还用于，确认控制帧中承载的 PN 大于上一次接收到的 PN，所述处理单元还用于，确认控制帧没有发生重播攻击。

在第七方面或第八方面的某些实现方式中，N 个第一用户信息字段的 N 个关联标识中的任一关联标识为预定义的数值。

在第七方面或第八方面的某些实现方式中，控制帧的公共字段中承载第二信息，第二信息指示控制帧中承载了第一信息。

在第七方面或第八方面的某些实现方式中，控制帧的公共字段中承载第三信息，第三信息指示 N 个第一用户信息字段中的至少一个第一用户信息字段的位置。

在第七方面或第八方面的某些实现方式中，控制帧中的公共字段或帧校验序列 FCS 字段中的至少一个字段中承载第四信息，第四信息包括用于保护控制帧的信息。

在第七方面或第八方面的某些实现方式中，控制帧的帧校验序列 FCS 字段的第一位置上承载第一异或结果，第一异或结果为 FCS 字段的第一位置上对应的循环冗余码 CRC 与第五信息的异或结果，第五信息包括用于保护控制帧的信息，FCS 字段的第一位置上的 CRC 对应的比特值与第五信息对应的比特值的比特个数相同。

在第七方面或第八方面的某些实现方式中，N 个第一用户信息字段中最后一个第一用户信息字段结束到控制帧结束之间的时长大于或等于第一类型设备的最小触发帧处理时间，第一类型设备为能够解读第一用户信息字段的关联标识的设备。

第九方面，提供一种通信装置，该通信装置包括：处理单元，用于生成物理层协议数据单元 PPDU，PPDU 包括控制包裹帧，控制包裹帧中包括第一信息和控制帧，第一信息包括用于保护控制帧的信息；通信单元，用于发送 PPDU。

第十方面，提供一种通信装置，该通信装置包括：通信单元，用于接收物理层协议数据单元 PPDU，PPDU 包括控制包裹帧，控制包裹帧中包括第一信息和控制帧，第一信息包括用于保护控制帧的信息；处理单元，用于解析 PPDU。

在第九方面或第十方面的实现方式中，第一信息包括秘钥标识，报文数 PN，和消息完整性代码 MIC

中的至少一项。

在第九方面的某些实现方式中，控制包裹帧中承载 MIC，所述处理单元还用于，确定本地 MIC；所述处理单元还用于，确认本地 MIC 与控制帧中承载的 MIC 匹配，所述处理单元还用于，确认控制帧没有被伪造。

在第九方面的某些实现方式中，控制包裹帧中承载 PN，所述处理单元还用于，确认控制帧中承载的 PN 大于上一次接收到的 PN，所述处理单元还用于，确认控制帧没有发生重播攻击。

在第九方面或第十方面的实现方式中，第一信息承载在高吞吐率控制字段中。

在第九方面或第十方面的实现方式中，第一信息承载在控制帧保护信息字段中。

在第九方面或第十方面的实现方式中，控制包裹帧为触发帧，触发帧的公共信息字段中的触发类型字段携带第一数值，第一数值指示控制包裹帧中包括控制帧保护信息字段和所承载的帧字段，第一数值为 8 至 15 中的任一数值，控制帧承载在所承载的帧字段。

第十一方面，提供一种通信装置，该通信装置包括：处理单元，用于生成物理层协议数据单元 PPDU，PPDU 包括聚合媒介访问控制协议数据单元 A-MPDU，A-MPDU 中包含第一媒介访问控制协议数据单元 MPDU 和第二 MPDU，其中，第一 MPDU 中承载控制帧，第二 MPDU 中承载第一信息，第一信息包括用于保护控制帧的信息；通信单元，用于发送 PPDU。

第十二方面，提供一种通信装置，该通信装置包括：通信单元，用于接收物理层协议数据单元 PPDU，PPDU 包括聚合媒介访问控制协议数据单元 A-MPDU，A-MPDU 中包含第一媒介访问控制协议数据单元 MPDU 和第二 MPDU，其中，第一 MPDU 中承载控制帧，第二 MPDU 中承载第一信息，第一信息包括用于保护控制帧的信息；处理单元，用于解析 PPDU。

在第十一方面或第十二方面的实现方式中，第一信息包括秘钥标识，报文数 PN，和消息完整性代码 MIC 中的至少一项。

在第十二方面的某些实现方式中，第二 MPDU 中承载 MIC，所述处理单元还用于，确定本地 MIC；所述处理单元还用于，确认本地 MIC 与控制帧中承载的 MIC 匹配，所述处理单元还用于，确认控制帧没有被伪造。

在第十二方面的某些实现方式中，第二 MPDU 中承载 PN，所述处理单元还用于，确认控制帧中承载的 PN 大于上一次接收到的 PN，所述处理单元还用于，确认控制帧没有发生重播攻击。

第十三方面，提供一种通信装置，包括处理器。该处理器与存储器耦合，可用于执行存储器中的指令，以实现上述第一方面或第三方面或第五方面以及第一方面或第三方面或第五方面中任一种可能实现方式中的方法。可选地，该装置还包括存储器。可选地，该装置还包括通信接口，处理器与通信接口耦合。

在一种实现方式中，该装置为第一设备。当该装置为第一设备时，所述通信接口可以是收发器，或，输入/输出接口。

在另一种实现方式中，该装置为配置于第一设备中的芯片。当该装置为配置于第一设备中的芯片时，所述通信接口可以是输入/输出接口。

第十四方面，提供一种通信装置，包括处理器。该处理器与存储器耦合，可用于执行存储器中的指令，以实现上述第二方面或第四方面或第六方面以及第二方面或第四方面或第六方面中任一种可能实现方式中的方法。可选地，该装置还包括存储器。可选地，该装置还包括通信接口，处理器与通信接口耦合。

在一种实现方式中，该装置为第二设备。当该装置为第二设备时，所述通信接口可以是收发器，或，输入/输出接口。

在另一种实现方式中，该装置为配置于第二设备中的芯片。当该装置为配置于第二设备中的芯片时，所述通信接口可以是输入/输出接口。

第十五方面，提供一种计算机可读存储介质，其上存储有计算机指令，所述计算机指令被装置执行时，使得所述装置实现第一方面至第六方面以及第一方面至第六方面中任一种可能实现方式中的方法。

第十六方面，提供一种包含指令的计算机程序产品，其上包含计算机程序，所述计算机程序被装置执行时，使得装置实现第一方面至第六方面以及第一方面至第六方面中任一种可能实现方式中提供的方法。

第十七方面，提供了一种通信系统，该通信系统包括前述的第一设备和第二设备，其中，第一设备

用于执行上述第一方面或第三方面或第五方面或第一方面或第三方面或第五方面中任一种可能实现方式中的方法，所述第二设备用于执行上述第二方面或第四方面或第六方面或第二方面或第四方面或第六方面中任一种可能实现方式中的方法。

附图说明

- 图1是适用于本申请实施例的无线局域网的网络架构的示意图。
图2是本申请实施例提供的一种通信装置的示意图。
图3是本申请实施例提供的一种发送和接收物理层协议数据单元的方法的示意图。
图4是AP发送触发帧触发多用户上行传输的示意图。
图5是802.11be触发帧的帧结构的示意图。
图6是本申请提出一种触发帧保护机制的示意图。
图7是本申请提出的另一种触发帧保护机制的示意图。
图8是本申请提出一种NDPA帧保护机制的示意图。
图9是本申请实施例提供的另一种发送和接收物理层协议数据单元的方法的示意图。
图10是现有标准中的控制包裹帧的帧结构的示意图。
图11是本申请提出的一种新的控制包裹帧的帧结构示意图。
图12是本申请提出的一种基于触发帧的控制包裹帧的帧结构示意图。
图13是本申请实施例提供的又一种发送和接收物理层协议数据单元的方法的示意图。
图14为本申请提出的一种可能在A-MPDU携带第一信息的示意图。
图15是本申请实施例提供的通信装置200的示意性框图。
图16为本申请实施例提供的通信装置300的示意性框图。

具体实施方式

下面将结合附图，对本申请实施例中的技术方案进行描述。显然，所描述的实施例是本申请的一部分实施例，而不是全部实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都应属于本申请保护的范围。

在本申请实施例中，“示例的”、“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”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言，使用示例一词旨在以具体方式呈现概念。

本申请实施例描述的业务场景是为了更加清楚地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。

需要说明的是，本申请中所称“字段”可以泛指一部分信息，“字段”也可以称为“域”或“field”等。并且本申请中字段的名称只是一个示例，具体实现中也可以是其他的名称，本申请对此不作具体限定。

应理解，说明书通篇中提到的“实施例”意味着与实施例有关的特定特征、结构或特性包括在本申请的至少一个实施例中。因此，在整个说明书各个实施例未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。

还应理解，本申请实施例提及“第一”、“第二”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大小、内容、顺序、时序、优先级或者重要程度等。例如，第一信息和第二信息并不表示信息量大小、内容、优先级或者重要程度等的不同。

还应理解，在本申请中，“当...时”、“若”以及“如果”均指在某种客观情况下网元会做出相应的处理，并非限定时间，且也不要求网元实现时一定要有所判断的动作，也不意味着存在其它限定。

还应理解，在本申请各实施例中，“A对应的B”表示B与A相关联，根据A可以确定B。但还应理解，根据A确定B并不意味着仅仅根据A确定B，还可以根据A和/或其它信息确定B。

本申请中，“至少一个”是指一个或者多个，“多个”是指两个或两个以上。“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：包括单独存在A，同时存在A和B，以及单独存在B的情况，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-b,a-c,b-c,或a-b-c,其中a,b,c可以是单个,也可以是多个。

本申请实施例提供的技术方案可以适用于无线局域网(wireless local area network, WLAN)场景,例如,支持 IEEE 802.11 相关标准,例如 802.11a/b/g 标准、802.11n 标准、802.11ac 标准、802.11ax 标准、IEEE 802.11ax 下一代 Wi-Fi 协议,如 802.11be、Wi-Fi 7、802.11ad、802.11ay 或 802.11bf,再如 802.11be 下一代、Wi-Fi 8 等,还可以应用于基于超宽带(ultra wide band, UWB)的无线个人局域网系统,如 802.15 系列标准,还可以应用于感知(sensing)系统,如 802.11bf 系列标准。其中,802.11n 标准称为高吞吐率(high throughput, HT),802.11ac 标准称为非常高吞吐率(very high throughput, VHT),802.11ax 标准称为高效(high efficient, HE),802.11be 标准称为超高吞吐率(extremely high throughput, EHT),而对于 HT 之前的标准,如 802.11a/b/g 等统称叫做 Non-HT(非高吞吐率)。目前,IEEE 802.11be 之后的下一代标准也已经启动研究,其名称叫做极高可靠性(ultra-high reliability, UHR)。

虽然本申请实施例主要以部署 WLAN 网络,尤其是应用 IEEE 802.11 系统标准的网络为例进行说明,本领域技术人员容易理解,本申请实施例涉及的各个方面可以扩展到采用各种标准或协议的其它网络,例如,高性能无线局域网(high performance radio local area network, HIPERLAN)、无线广域网(wireless wide area network, WWAN)、无线个人区域网(wireless personal area network, WPAN)或其它现在已知或以后发展起来的网络。因此,无论使用的覆盖范围和无线接入协议如何,本申请实施例提供的各种方面可以适用于任何合适的无线网络。例如,本申请实施例还可以适用于物联网(internet of things, IoT)网络或车联网(vehicle to X, V2X)等无线局域网系统中。当然,本申请实施例还可以适用于其他可能的通信系统,例如,长期演进(long term evolution, LTE)系统、LTE 频分双工(frequency division duplex, FDD)系统、LTE 时分双工(time division duplex, TDD)、通用移动通信系统(universal mobile telecommunication system, UMTS)、全球互联微波接入(worldwide interoperability for microwave access, WiMAX)通信系统、第五代(5th generation, 5G)通信系统,以及未来的第六代(6th generation, 6G)通信系统等。

上述适用本申请的通信系统仅是举例说明,适用本申请的通信系统不限于此,在此统一说明,以下不再赘述。

WLAN 可以包括多个基本服务集(basic service set, BSS),BSS 中的网络节点为站点(station, STA)和接入点(access point, AP)。每个 BSS 可以包含一个 AP 和多个关联于该 AP 的 STA。

本申请实施例中的 AP 也可以称之为无线访问接入点或热点等。AP 是移动用户进入有线网络的接入点,主要部署于家庭、大楼内部以及园区内部,典型覆盖半径为几十米至上百米,当然,也可以部署于户外。AP 相当于一个连接有线网和无线网的桥梁,其主要作用是将各个无线网络客户端连接到一起,然后将无线网络接入以太网。示例的,AP 可以为支持 802.11ax 协议的设备以及支持 802.11ax 下一代 Wi-Fi 协议的设备,进一步的,AP 可以支持 802.11be 下一代,如 Wi-Fi 8, UHR 等 802.11 系列协议或后续版本等一种或多种 WLAN 制式的设备。

本申请实施例中的 STA 可以是无线通讯芯片、无线传感器或无线通信终端。例如:支持 Wi-Fi 通讯功能的移动电话、支持 Wi-Fi 通讯功能的平板电脑、支持 Wi-Fi 通讯功能的机顶盒、支持 Wi-Fi 通讯功能的智能电视、支持 Wi-Fi 通讯功能的智能可穿戴设备、支持 Wi-Fi 通讯功能的车载通信设备和支持 Wi-Fi 通讯功能的计算机。示例的,STA 可以为支持 802.11ax 制式的设备以及支持 802.11ax 下一代 Wi-Fi 协议的设备,进一步的,AP 可以支持 802.11be 下一代,如 Wi-Fi 8, UHR 等 802.11 系列协议或后续版本等一种或多种 WLAN 制式的设备。。

在本申请实施例中,作为一种示例结构,STA 或 AP 包括硬件层、运行在硬件层之上的操作系统层,以及运行在操作系统层上的应用层。该硬件层包括中央处理器(central processing unit, CPU)、内存管理单元(memory management unit, MMU)和内存(也称为主存)等硬件。该操作系统可以是任意一种或多种通过进程(process)实现业务处理的计算机操作系统,例如,Linux 操作系统、Unix 操作系统、Android 操作系统、iOS 操作系统或 Windows 操作系统等。该应用层包含浏览器、通讯录、文字处理软件、即时通信软件等应用。以上示例并未对本申请实施例提供的方法的执行主体的具体结构进行唯一实现形式的限定,只要能够通过运行记录有本申请实施例提供的方法的代码的程序,以根据本申请实施例提供的方法进行通信即可,例如,本申请实施例提供的方法的执行主体可以是 STA 或 AP,或者,是 STA 或

AP 中能够调用程序并执行程序的功能模块。

另外，本申请的各个方面或特征可以实现成方法、装置或使用标准编程和/或工程技术的制品。本申请中使用的术语“制品”涵盖可从任何计算机可读器件、载体或介质访问的计算机程序。例如，计算机可读介质可以包括，但不限于：磁存储器件（例如，硬盘、软盘或磁带等），光盘（例如，压缩盘（compact disc, CD）、数字通用盘（digital versatile disc, DVD）等），智能卡和闪存器件（例如，可擦写可编程只读存储器（erasable programmable read-only memory, EPROM）、卡、棒或钥匙驱动器等）。另外，本文描述的各种存储介质可代表用于存储信息的一个或多个设备和/或其他机器可读介质。术语“机器可读介质”可包括但不限于，无线信道和能够存储、包含和/或承载指令和/或数据的各种其它介质。

图 1 是适用于本申请实施例的无线局域网的网络架构的示意图。如图 1 所示，一个 AP 可以与一个或多个 STA 关联，即一个 AP 可以与一个或多个 STA 通信。如图 1 所示，无线局域网的网络架构中还可以包括多个 AP，不同 AP 之间也可以进行通信。例如图 1 中所示，图中示出了 AP#1 与 AP#2，以及与 AP#1 关联的 STA 11 和 STA 12。其中，AP#1 与 STA 11 或 STA 12 之间可以进行数据的传输，STA 11 与 STA 12 之间可以进行数据的传输，AP#1 和 AP#2 之间也可以进行通信。

应理解，图 1 只是示例性的，不应该对本申请适用的无线局域网的网络架构产生限制，例如，该网络架构还可以包括更多的 AP，每个 AP 还可以与更多的 STA 关联，本申请实施例在此不做限定。

图 2 是本申请实施例提供的一种通信装置的示意图。该通信装置可以包括如下部件中的一种或多种：处理器 210、发送器 220、存储器 230、接收器 240、信号检测器 250，数字信号处理器 260 和用户界面 270。应理解，该通信装置也可以仅包括图示中的部分模块，比如，该通信装置包括：处理器 210 和存储器 230。在一些可能的实现方式中，该通信装置可以是 AP 或者 STA。

当今社会信息安全至关重要。在无线局域网传输中，STA 和 AP 在进行数据传输之前，通常需要先进行关联，认证（Authentication），获取相关的密钥之后，才可以进行数据传输。

无线局域网传输中，用于通信的帧主要包括三种类型：数据帧、管理帧和控制帧。其中，数据帧用于承载上层的数据；管理帧，用于承载小区管理的一些信息，示例的，管理帧包括信标帧，关联请求帧等；控制帧，通常承载一些很短的控制指令，示例的，管理帧包括确认帧，触发帧等。目前，针对数据帧和管理帧的保护关注较多，因为控制帧通常携带一些简单的控制指令，而没有引起大家的足够重视。但近几年来，控制帧在数据通信中变得越来越重要，例如被用来进行上行数据传输调度。因而针对控制帧的攻击类型，也越来越多。例如，攻击者假装是 AP，发送基本触发（Basic Trigger）帧等，让 STA 长时间的发送数据和报告，占据空口，消耗电量。又例如，攻击者假装是 AP，发送多用户块确认请求（multiple user request to send, MU-RTS）触发帧，触发 STA 回复确认帧，并且清空本应保存的缓存。再例如，攻击者假装是 AP，发送多用户请求发送（multiple user block ack request, MU-BAR）触发帧，触发 STA 从低功耗模式唤醒为高功耗模式，并且响应发送允许发送帧。因此，可以在控制帧中携带用于保护控制帧的信息，以防止针对控制帧的攻击。但是如何携带相应的保护信息以保护控制帧目前还未明确。

有鉴于此，本申请提出一种发送和接收物理层协议数据单元的方法，明确了控制帧的保护机制，能够有效防止针对控制帧的攻击。

图 3 是本申请实施例提供的一种发送和接收物理层协议数据单元的方法的示意图。该方法包括以下步骤。示例的，该方法中第一设备为 AP，第二设备为 STA。

S310，第一设备生成物理层协议数据单元（physical layer protocol data unit, PPDU）。

其中，该 PPDU 包括控制帧，该控制帧包括 N 个第一用户信息字段，其中，第一用户信息字段中的关联标识指示第一用户信息字段中承载第一信息，第一信息包括用于保护控制帧的信息，N 为大于或等于 1 的整数。

需要说明的是，本申请实施例的控制帧中还可以包括除 N 个第一用户信息字段之外的一个或多个第一用户信息字段，本申请对此不做限制。

为便于描述，本申请实施例中将控制帧中携带的用于保护控制帧的所有信息称为保护信息#1。本申请实施例对保护信息#1 不做具体限制，凡能够用于保护控制帧的信息都在本申请实施例给出的保护信息#1 的保护范围内。其中，第一信息包括用于保护控制帧的信息，可以理解为第一信息包括保护信息#1 中的部分或全部信息。

示例的，为防止伪造（forgery）和重播（replay）攻击，保护信息#1 中可以包括密钥标识（Key ID），报文数（packet number, PN），和消息完整性代码（message integrity codes, MIC）中的至少一项。本申

请实施例中可以承载秘钥标识的字段称为秘钥标识字段，将承载 PN 的字段称为 PN 字段，将承载 MIC 的字段称为 MIC 字段。其中，PN 字段中的 PN 用于识别受到保护的帧，MIC 字段中携带基于受到保护的帧计算得到的 MIC，进行 MIC 计算，需要被加密的信息和秘钥，需要被加密的信息为受到保护的帧的部分帧体以及由帧控制、部分地址字段组成的其他身份验证数据（additional authentication data, AAD）。MIC 字段的长度取决于第一设备和第二设备在认证过程中获取的秘钥。例如，一种具体的算法中可以将 128 比特的秘钥和控制帧中需要被加密的 128 比特信息，通过加密算法，输出 128 比特的信息，最后取其中 8 字节（即 64 比特）作为 MIC。关于如何基于 PN 和 MIC 判断控制帧是否发生伪造和重播攻击，会在 S330 中进行具体描述，这里暂不展开叙述。

下面以控制帧为触发帧作为示例具体说明如何在触发帧的第一用户信息字段中承载第一信息。在介绍如何承载第一信息之前，先介绍一下触发帧的帧格式和基于触发帧的传输流程。通常 STA 通过信道竞争获得发送权之后再行进行上行数据传输，比如基于增强分布式信道接入（enhanced distributed channel access, EDCA）方式抢信道。802.11ax 标准引入了基于触发帧的调度式上行传输方法，802.11be 延续了基于触发帧的调度式上行传输方法。下面结合图 4 对 802.11be 标准中 AP 触发上行多用户传输的方案进行介绍。该方案包括以下步骤。

步骤 1：AP 发送触发帧。

图 5 是 802.11be 触发帧的帧结构的示意图。该触发帧包含公共信息字段（Common Info）和用户信息列表字段（User Info List），公共信息字段中包含的各字段的含义可以参考协议中的描述，这里不再一一赘述。用户信息列表字段包含多个用户信息字段（User Info），每个用户信息字段中包含一个关联标识 12（Association Identification 12, AID12）字段，其中，第一个用户信息字段的 AID12 字段的取值为 2007，该用户信息字段的 AID12 字段后边承载一些公共信息。第一个用户信息字段虽然是用户信息字段，但是承载着公共信息，因此第一个用户信息字段可以被叫做特殊用户信息字段。需要说明的是，在将 AID12 与 STA 关联时，AP 不会将任何一个 STA 的 AID12 分配为 2007，因此 STA 在接收到包含 AID12 取值为 2007 的触发帧时不会有歧义。从第二个用户信息字段开始，该用户信息字段的 AID12 字段具体指向一个 STA 用户，该用户信息字段包含指向的 STA 用户需要读取的信息，而该用户信息字段中的资源单元分配子字段（RU allocation）同主时隙 160 字段联合起来指示这个 STA 用户所分配到的具体的资源单元（resource unit, RU）或多资源单元（MRU）的位置。另外，图 5 对公共信息字段和用户信息列表字段中包含的字段所占的比特数分别进行了标注，这里仅举例说明，例如用户信息 1 中的 AID12 字段对应的 B0 至 B11，表示 AID12 字段为用户信息 1 字段中的前 12 个比特。

步骤 2：STA（例如 STA#1 和 STA#2）接收到触发帧，首先读取公共信息字段和特殊用户信息字段，之后，如果 STA 从触发帧中解析出需要自己读取的用户信息字段，则在该用户信息字段中的资源单元分配子字段所指示的 RU 或 MRU 上发送各自的极高吞吐量基于触发的数据分组（extremely high throughput trigger based PPDU, EHT TB PPDU）。

步骤 3：AP 接收到一个或多个站点发送的 EHT TB PPDU 后，回复多站点块确认（multi-STA block acknowledgement, M-BA）帧。

下面介绍如何在触发帧中承载第一信息，在触发帧的用户信息列表字段中，除了 AID12 字段的取值为 2007 的特殊用户信息字段，还可以增加另外一种类型的用户信息字段（即第一用户信息字段），该第一用户信息字段中的 AID12 字段的取值为一个预定义的数值，该预定义的数值可以指示第一用户信息字段中承载了第一信息。

示例的，该预定义的数值可以为 2008-2044 或 2047-4094 中的一个或多个取值。可以理解，第一用户信息字段的 AID12 字段的取值与现有的 STA 用户对应的 AID12 的取值不冲突，第一用户信息字段会被其他 STA 用户当作一个不是发给自己的其他 STA 的用户信息字段，因此不影响 STA 用户对触发帧的接收。

示例的，该预定义的数值也可以为 1-2006 中的一个或多个取值。可以理解，由于 802.11ax 标准考虑用户信息字段的顺序问题，标准建议分配给某个用户的用户信息字段（即用户信息字段的 AID12 字段的取值为 1~2007 的用户信息字段）需要放在用户信息列表字段的前边，因此，也可以将 1-2006 中的一个或多个取值作为第一用户信息字段中的 AID12 字段的取值，而不分配给某一个 STA，可以使得 STA 在用户信息列表的前部获取到控制帧保护信息，从而获取更多的触发帧处理时间。关于 STA 的触发帧处理时间参见图 7 中的描述，这里暂不展开叙述。

可选地，触发帧中包含一个第一用户信息字段，该第一用户信息字段中承载第一信息。如图 6 所示，

触发帧包括一个第一用户信息字段（即图中的用户信息字段 M），用户信息字段 M 中承载的第一信息包括秘钥标识、PN 和 MIC，具体的，用户信息字段 M 中的 B12（即秘钥标识字段）承载秘钥标识，B13 至 B23（即 PN 字段）承载 PN，B24 至 B39（即 MIC 字段）承载 MIC。应理解，图 6 仅是示意性给出携带的各信息的顺序，本申请对实际携带各信息的顺序不做限制。

可选地，触发帧中包括多个第一用户信息字段，该多个第一用户信息字段分别承载各自对对应的第一信息。如图 7 所示，触发帧包括两个第一用户信息字段（即图中的用户信息字段 M-1 和用户信息字段 #M），用户信息字段 M-1 承载的第一信息中包括秘钥标识和 PN，用户信息字段 M 承载的第一信息中包括 MIC，具体的，用户信息字段 M-1 中的 B12（即秘钥标识字段）承载秘钥标识，B13 至 B39（即 PN 字段）承载 PN，用户信息字段 M 中 B12 至 B39（即 MIC 字段）承载 MIC。触发帧可能还包括三个、四个或者更多的第一用户信息字段，这里不再一一举例说明。

可选地，多个第一用户信息字段的 AID12 字段的取值可以相同，也可以不同。

可选地，多个第一用户信息字段的位置可以是连续的，也可以是离散的，也可以部分连续，部分离散。

可选地，保护信息#1 中的信息除了可以承载在控制帧第一用户信息字段中，也可以承载在控制帧的公共字段中。本申请实施例中的公共信息字段可以包括公共信息字段和/或 AID12 字段取值为 2007 的用户信息字段（即特殊用户信息字段）。示例的，保护信息#1 中的部分信息可以承载在公共信息字段中的 B22、B53、B56 至 B63 中的一个或多个比特上。示例的，保护信息#1 中的部分信息也可以承载在 AID12 字段的取值为 2007 的用户信息字段中的 B25-B39 中的一个或多个比特上。

可选地，保护信息#1 中的信息也可以承载在控制帧的帧校验序列（frame check sequence, FCS）字段中。需要说明的是，如果 FCS 字段中不承载保护信息#1，则会携带循环冗余码（cyclic redundancy code, CRC）。下面给出两种具体实现方式。

在一种可能的实现方式中，控制帧的 FCS 字段的第一位置上承载第四信息，第四信息包括用于保护所述控制帧的信息（第四信息即保护信息#1 中包含的信息），可以理解，该实现方式是将 FCS 字段在第一位置上原先承载的 CRC 替换为第四信息。示例的，FCS 字段不携带保护信息#1 时，原本携带的 CRC 冗余码为 10110110010001001110001111100011，如果需要在 FCS 字段上携带的第四信息为 110，则可以将 FCS 字段中的任意 3 个比特替换为 110，这里以替换 FCS 字段中的前 3 个比特为例，替换后的 FCS 字段为 11010110010001001110001111100011。

在另一种可能的实现方式中，控制帧的 FCS 字段的第一位置上承载第一异或结果，第一异或结果为 FCS 字段不携带保护信息#1 时在第一位置上携带的 CRC 与第五信息的异或结果，第五信息包括用于保护控制帧的信息（第五信息即保护信息#1 中包含的信息），FCS 字段的第一位置上的 CRC 对应的比特值与第五信息对应的比特值的比特个数相同。示例的，同上，FCS 字段不携带保护信息#1 时，原本携带的 CRC 冗余码为 10110110010001001110001111100011，如果需要在 FCS 字段上携带的第五信息为 110，这里以第一位置为 FCS 字段中的前 3 个比特为例，则第一异或结果为 101 与 110 的异或结果 011，则 FCS 字段中承载的信息由 10110110010001001110001111100011 变为 01110110010001001110001111100011。

上述部分替换 FCS 字段中的 CRC 或异或 FCS 字段中的 CRC 的方案，可以减少控制帧携带保护信息的开销，此外，该方案还考虑了因为信道质量差造成的控制帧传输错误和因为伪造造成的 MIC 错误。原因如下，因为控制帧传输错误或者伪造 MIC，都会造成 FCS 字段发生错误，因此可以同时识别上述两种错误。

可选地，触发帧的公共字段中承载第二信息，第二信息指示该触发帧中承载了第一信息。示例的，第二信息可以通过公共信息字段中的 B22、B53、B56 至 B63 中的一个比特承载。示例的，保护信息#1 中的部分信息也可以通过 AID12 字段的取值为 2007 的用户信息字段中的 B25-B39 中的一个比特承载。如图 6 和图 7 所示，在一种可能的实现方式中，第二信息通过公共信息字段中的 B56 承载，示例的，B56 对应的字段可以称为受保护的字段。在触发帧公共字段中携带第二信息，可以帮助支持触发帧保护的 STA 在读取到第二信息后，提前做相应的准备以读取第一用户信息字段中承载的保护信息（即第一信息）。

此外，为了帮助 STA 快速定位第一用户信息字段的位置，还可以在公共字段中承载第三信息，第三信息指示触发帧中包含的至少一个第一用户信息字段的位置。示例的，第三信息可以通过公共信息字段中的 B22、B53、B56 至 B63 中的一个或多个比特承载。示例的，保护信息#1 中的部分信息也可以通过 AID12 字段的取值为 2007 的用户信息字段中的 B25-B39 中的一个或多个比特承载。例如，第三信息指示

触发帧中的第一个第一用户信息字段的位置，触发帧中的所有第一用户信息字段是连续的，示例的，第三信息承载在一个 5 比特字段中，取值为 00011，用于指示触发帧中的第一个第一用户信息字段为用户信息列表字段中的第 3 个用户信息字段。又例如，存在一个 5 比特的字段，例如 5 比特字段为 11111，用于指示用户信息列表字段中的第 1~32 个用户信息字段中承载着携带触发帧保护相关信息；进一步的，如果可能存在的第一用户信息字段比较多，可以增加指示颗粒度，比如同样存在一个 5 比特的字段，可以用于指示用户信息列表中的第 2, 4, 6, ..., 62, 64 个用户信息字段中承载着携带触发帧保护相关信息。如图 6 和图 7 所示，在一种可能的实现方式中，第三信息通过公共信息字段中的 B57 至 B62 承载，示例的，B57 至 B62 对应的字段可以称为保护信息位置指示字段。

另外，针对携带第一用户信息字段的触发帧，支持触发帧保护和不支持触发帧保护的 STA，其理解的触发帧处理时间不同。如图 7 所示，对于不支持触发帧保护的 STA#1，示例的，用户信息#2 为 STA#1 需要读取的用户信息字段，在解析触发帧的过程中，STA#1 在发现自己的用户信息字段后，即可以停止接收后边的用户信息列表字段，则 STA#1 理解的触发帧处理时间可以为从用户信息字段#2 结束到触发帧结束之间的时长；而对于支持触发帧保护的 STA#2，除了读取自己的用户信息字段，还可能需读取触发帧中的所有第一用户信息字段以获取第一信息，图 7 中触发帧包括的最后一个用户信息字段为用户信息字段#M，则 STA#2 理解的触发帧处理时间为用户信息字段#M 结束到触发帧结束之间的时长。因此，AP 在生成触发帧时，要合理设置支持触发帧保护和不支持触发帧保护的 STA 的触发帧处理时间，以保证支持和不支持触发帧保护的 STA 的触发帧处理时间大于或等于最小触发帧处理时间，获得足够的触发帧处理时间。

可选地，对于 PN，可以复用现有标准的 PN，也可以针对触发帧定义单独的 PN，比如触发帧 PN (trigger PN, TPN)，本申请对此不做限制。

对于触发帧，分为广播触发帧和单播触发帧。可选地，对于广播触发帧，其密钥可以复用现有的完整性组临时密钥 (integrity group temporal key, IGTK) 或信标完整性组临时密钥 (beacon IGTK, BIGTK)，IGTK 密钥标识可以为 4 或 5，BIGTK 密钥标识可以为 6 或 7。可选地，对于广播触发帧，其密钥也可以为单独定义的基于触发帧的完整性组临时密钥 (trigger IGTK, TIGTK)。可选地，对于单播触发帧，其密钥可以复用现有的成对瞬态密钥 (pairwise transient key, PTK)，也可以生成单独的触发帧临时密钥 (trigger temporal key, TTK)。另外，还可以针对上行和下行触发帧分别定义不同的密钥，本申请对此不做限制。

在一种可能的实施方式中，TTK 和 TIGTK 可以为控制帧临时密钥 (control frame temporal key, CTK) 和组播控制帧的完整性组播临时密钥 (control frame integrity group temporal key, CIGTK)。

其中，CTK 和 CIGTK 在多链路 (multi-link) 场景下，每条链路需要定义独立的 CTK 和 CIGTK。这里首先介绍多链路场景。多链路场景下包括 AP 多链路设备 (Multi-link device, MLD) 和 STA MLD，AP MLD 和 STA MLD 之间可以建立多个连接，示例的，AP MLD 中包括 3 个附属 AP，分别为 AP1、AP2 和 AP3。STA MLD 中包括 3 个附属 STA，分别为 STA1、STA2 和 STA3，多个连接分别为 AP1 和 STA1 之间的链路 1，AP2 和 STA2 之间的链路 2，以及，AP3 和 STA3 之间的链路 3，三条链路对应三个频段，分别为 2.4GHz、5GHz 和 6GHz 频段，这种多链路特性能够将频谱资源通过多条链路优化使用。其中，一个 CTK 与对应链路两端的媒体接入控制 (medium access control, MAC) 地址进行绑定，对应两端的 MAC 地址分别为一个 AP MLD 的附属 (affiliated) AP 的 MAC 地址和一个 STA MLD 的附属 STA 的 MAC 地址。一个 CIGTK 与对应的附属 AP 的 MAC 地址进行绑定。

为了进行 CIGTK 和 CTK 的密钥协商，需要定义相应的密钥数据封装 (key data encapsulation, KDE)。示例的，定义 CIGTK 的 KDE 格式如表 1 所示。

表 1

Key ID	Link ID	CIPN	CIGTK
--------	---------	------	-------

其中，Key ID 用于指示认证方选择的密钥标识，Link ID 是指示该 CIGTK 是针对哪条链路的 CIGTK，控制帧 IGTK 报文数 (control frame IGTK packet number, CIPN) 携带的是对应的 CIGTK 的包序列号，CIGTK 携带对应的 CIGTK。

示例的，定义 CTK 的 KDE 格式如表 2 所示。

表 2

Key ID	Link ID	ANonce	SNonce	Key Info
--------	---------	--------	--------	----------

其中，Key ID 用于指示认证方选择的密钥标识，Link ID 是指示该 CTK 是针对哪条链路的，Anonce 携带认证方的一个随机数，Snonce 携带一个申请方的一个随机数，Key Info 携带的是用于派生 CTK 的密钥相关信息。

同时，针对快速基本服务集合（basic service set，BSS）切换，需要在快速基本服务集合转移元素（fast BSS transition element，FTE）中定义 CIGTK 和 CTK 的相应子元素（subelement）。

示例的，定义 CIGTK 的 subelement 格式如表 3 所示。

表 3

Subelement ID	Length	Key ID	Link ID	CIPN	Key Length	CIGTK
---------------	--------	--------	---------	------	------------	-------

其中，Subelement ID 为子元素标识，Length 用于指示该 CIGTK 的 subelement 的长度，Key ID 用于指示认证方选择的密钥标识符，Link ID 是指示该 CIGTK 是针对哪条链路的，CIPN 携带的是对应的 CIGTK 的包序列号，Key Length 用于指示密钥长度，即 CIGTK 的长度，单位为字节，CIGTK 携带对应的 CIGTK。

示例的，定义 CTK 的 subelement 格式如表 4 所示。

表 4

Subelement ID	Length	Key ID	Link ID	ANonce	SNonce	Key Info
---------------	--------	--------	---------	--------	--------	----------

其中，Subelement ID 为子元素标识，Length 用于指示该 CTK 的 subelement 的长度，Key ID 用于指示认证方选择的密钥标识符，Link ID 是指示该 CTK 是针对哪条链路的，Anonce 携带认证方的一个随机数，Snonce 携带一个申请方的一个随机数，Key Info 携带的是用于派生 CTK 的密钥相关信息。

下面以控制帧为空数据分组声明（null data packet announcement，NDPA）帧作为示例具体说明如何在 NDPA 帧中承载保护信息#1。如图 8 所示，NDPA 帧采用了与触发帧类似的帧结构，该帧包括一个探测对话令牌字段（对应触发帧中的公共信息字段）和多个站点信息字段（对应触发帧中的用户信息字段），关于站点信息字段 1 中各字段的含义可以参考协议中的描述，这里不再赘述，可以看出，每个站点信息字段中也包括一个 AID12 字段，因此，也可以采用上述方法对 NDPA 帧进行保护。图 8 中示例性给出一种可能的 NDPA 帧中携带 NDPA 帧保护信息的方法，如图 8 所示，NDPA 帧中包括站点信息字段 N-1 和站点信息字段 N（对应触发帧中的第一用户信息字段），站点信息字段 N-1 中承载的第一信息包括密钥标识和 PN，站点信息字段 N 中承载的第一信息包括 MIC。

需要说明的是，NDPA 帧中的 AID 11 字段为 11 比特（B0 至 B10），因此用于承载 NDPA 帧保护信息的站点信息字段的 AID 11 字段的取值最大只能为 2047。

还需要说明的是，在承载保护信息#1 的站点信息字段中，B27 需要置 1，防止传统的 11ac STA 将一个 4 字节中包括两个 2 字节中的第二个 2 字节误认为是自己的站点信息字段。因此，如果图 8 中承载 MIC 大于 16 比特，例如 MIC 为 17 比特，则可以在站点信息字段#N 的 B11 至 B26 中携带 MIC 的任意 16 比特，额外在 B28-B31 中选 1 比特携带中剩余的 1 比特（比如最高比特），示例的，图 8 中在站点信息字段 M 的 B11 至 B26 中携带 MIC 的第 1 至 16 比特，在 B28 承载 MIC 的第 17 比特（即 MIC 的最高比特位）。

S320，第一设备向第二设备发送 PPDU。对应的，第二设备接收来自第一设备的 PPDU。

S330，第二设备解析 PPDU。

第二设备在接收到 PPDU 之后，基于 PPDU 中的用户信息字段的关联标识确定该用户信息字段承载了第一用户信息字段，之后，第二设备基于第一用户信息字段携带的第一信息确定保护信息#1，根据保护信息#1 确定控制帧是否受到攻击。如果受到攻击，则忽略该控制帧，否则，基于接收到的控制帧继续后续处理流程。

可选地，以图 6 为例，第二设备在 PPDU 的触发帧的公共信息字段中的 B56 中读取第二信息，第二信息指示该触发帧中承载了第一信息，第二设备在读取到第二信息后，可以提前做相应的准备以读取第一用户信息字段中承载的保护信息（即第一信息）。

可选地，以图 6 为例，第二设备在 PPDU 的触发帧的公共信息字段中的 B57 至 B62 中读取第三信息，第三信息指示触发帧中包含的至少一个第一用户信息字段的位置，第二设备在读取到第三信息后，可以快速定位第一用户信息字段的位置。

应理解,第一设备在控制帧中哪些位置哪些携带哪些类型的信息以及如何携带(例如 FCS 字段中的替换携带或异或携带),第二设备都是已知的,这样,第二设备才能在控制帧对应位置上读取相应的信息。

可选地,这里以保护信息#1 包括 PN 和 MIC 为例说明第二设备如何判断控制帧是否防止发生了伪造和重播攻击。由于密钥是在第一设备与第二设备的认证过程中获取的,攻击者无法获取密钥,因此无法伪造收发两端可以知道的 MIC。因此,第二设备可以在本地计算 MIC,应理解,第二设备确定本地 MIC 与第一设备确定控制帧中携带的 MIC 所使用的密钥和需要被加密的信息相同,也就是说,第二设备知道接收到的 PPDU 的控制帧中的哪些信息是用于确定本地 MIC 的信息。之后第二设备基于保护信息#1 中的 MIC,同自己本地计算的 MIC 作对比,如果匹配,则认为没有发生伪造攻击,如果不匹配,则认为发生了伪造攻击。另外,第二设备识别发送端发送的 PN,如果每次接收到的 PN,相比上一次,一直为单调上升,则认定正常,否则就认为发生了重播攻击。需要说明的是,攻击者无法伪造 PN,只能复制之前收到的 PN,进行重播攻击。因为伪造 PN,会导致 MIC 不匹配。

上述技术方案中,通过在控制帧中的第一用户信息字段中携带控制帧的保护信息,以防止控制帧被攻击。利用该控制帧保护机制,对于支持控制帧保护的接收端设备来说,可以基于第一用户信息字段中的关联标识确定第一用户信息字段携带控制帧的保护信息,对于不支持控制帧保护的接收端设备来说,第一用户信息字段会被当作一个不是发给自己的其他设备的用户信息字段,因此不影响不支持控制帧保护的接收端设备接收控制帧。

下面结合图 9 给出另一种控制帧的保护机制,该保护机制也能够能够有效防止针对控制帧的攻击。

图 9 是本申请实施例提供的另一种发送和接收物理层协议数据单元的方法的示意图。该方法包括以下步骤。示例的,该方法中第一设备为 AP,第二设备为 STA。

S910,第一设备生成 PPDU。其中,该 PPDU 包括控制包裹(wrapper)帧,控制包裹帧中包括第一信息和控制帧,第一信息包括用于保护控制帧的信息。

本申请实施例对第一信息不做具体限制,凡能够用于保护控制帧的信息都在本申请实施例给出的第一信息的保护范围内。

示例的,第一信息中可以包括密钥标识、PN 和 MIC 中的至少一项。本申请实施例中可以将承载密钥标识的字段称为密钥标识字段,将承载 PN 的字段称为 PN 字段,将承载 MIC 的字段称为 MIC 字段。

由于最初的控制帧不承载高吞吐率控制字段,为了帮助控制帧可以利用高吞吐率控制字段进行一些功能的实现,引入了控制包裹帧。图 10 为现有标准中的控制包裹帧的帧结构的示意图。该控制包裹帧中包括高吞吐率控制字段和所承载的帧字段。下面给出在控制包裹帧中承载第一信息和控制帧的具体实现方式。

在一种可能的实现方式中,可以利用控制包裹帧中的高吞吐率控制字段去帮助控制帧额外承载第一信息,即第一信息可以承载在高吞吐率控制字段中。示例的,可以在高吞吐率控制字段中的聚合(aggregated)控制信息(A-control)字段中的一个控制子字段中携带第一信息,如图 10 所示,聚合控制信息字段包含 N 个控制子字段,N 为正整数,可以在控制子字段#1 的控制信息字段中携带第一信息,控制子字段#1 包括控制标识符字段和控制信息字段,具体的,可以将控制标识符字段的取值设置为 10-14 中的一个取值,用于指示该控制子字段中的控制信息字段承载着第一信息,另外,在所承载的帧字段承载中控制帧。

在另一种可能的实现方式中,可以在现有控制包裹帧的基础上,额外引入新的字段,在新的字段中承载第一信息。示例的,如图 11,在现有控制包裹帧的基础上引入新字段,该新字段为图中新增控制帧保护信息字段,在该新字段中承载第一信息,另外,在所承载的帧字段承载中控制帧。

可以理解,图 11 中的控制包裹帧可以看做是一种新的控制包裹帧。新设计一种类型的控制包裹帧格式有很多种途径,一种途径是定义一种新的帧类型以及子类型,但是由于现有的帧类型以及子类型的种类不多了,特别是控制帧。因此,本申请提出一种利用现有触发帧去设计新的控制包裹帧的方法。如图 12 所示,该触发帧的公共信息字段中的触发类型字段携带第一数值,该第一数值指示控制包裹帧中包括控制帧保护信息字段和所承载的帧字段,第一数值为 8 至 15 中的任一数值,控制帧承载在所承载的帧字段。可以看出,可以通过将触发帧中的公共信息字段中的触发帧类型字段的取值规定为第一取值,从而可以重新定义触发帧中的帧格式,该方式的好处是节省尚未使用的帧类型和子类型种类。

S920,第一设备向第二设备发送 PPDU。对应的,第二设备接收来自第一设备的 PPDU。

S930, 第二设备解析 PPDU。

第二设备在接收到 PPDU 之后, 基于 PPDU 的控制包裹帧中携带的第一信息确定控制帧是否受到攻击。如果受到攻击, 则忽略该控制帧, 否则, 基于接收到的控制帧继续后续处理流程。具体判断过程参见 S330 中的描述, 这里不再赘述。

上述技术方案中, 利用现有或新定义的控制包裹 (Wrapper) 帧去携带控制帧保护信息, 以防止控制帧被攻击。该控制帧保护机制可以适用于任何控制帧, 由于该保护机制不需要对控制帧本身进行修改或重新定义, 尤其适用于帧结构固定的控制帧, 例如块确认请求 (block acknowledge request, BAR) 帧, 波束成形报告轮询 (beamforming report poll, BFRP) 帧等控制帧。

下面结合图 13 给出又一种控制帧的保护机制, 该保护机制也能够能够有效防止针对控制帧的攻击。

图 13 是本申请实施例提供的又一种发送和接收物理层协议数据单元的方法的示意图。该方法包括以下步骤。示例的, 该方法中第一设备为 AP, 第二设备为 STA。

S1310, 第一设备生成 PPDU。

其中, PPDU 包括聚合媒介访问控制协议数据单元 (aggregated medium access control protocol data unit, A-MPDU), 该 A-MPDU 中包含第一媒介访问控制协议数据单元 (medium access control protocol data unit, MPDU) 和第二 MPDU, 其中, 第一 MPDU 中承载控制帧, 第二 MPDU 中承载第一信息, 第一信息包括用于保护控制帧的信息。

本申请实施例对第一信息不做具体限制, 凡能够用于保护控制帧的信息都在本申请实施例给出的第一信息的保护范围内。

应理解, 该 A-MPDU 除了包括第一 MPDU 和第二 MPDU 之外, 还可以包括更多的 MPDU, 本申请对此不做限制。

示例的, 第一信息中可以包括密钥标识、PN 和 MIC 中的至少一项。本申请实施例中可以将承载密钥标识的字段称为密钥标识字段, 将承载 PN 的字段称为 PN 字段, 将承载 MIC 的字段称为 MIC 字段。

示例的, 该实施例中 PPDU 为 HT PPDU, VHT PPDU, HE PPDU, EHT PPDU, UHR PPDU 中的任一种。

示例的, 对于在第二 MPDU 中承载第一信息的方式, 可以利用一个管理帧, 比如行动帧或者无需确认的行动帧, 通过信息元素的方式去承载第一信息, 本申请对具体实现方式不作限定。

图 14 为本申请提出的一种可能在 A-MPDU 中携带第一信息的示意图。PPDU 的数据字段中包含 A-MPDU, A-MPDU 包含 n 个 A-MPDU 子帧字段, 每个 A-MPDU 子帧字段包括 MPDU 分隔符字段、MPDU 字段和填充字段, 其中, 在第一个 A-MPDU 子帧字段的 MPDU 字段中携带第一信息, 第一信息包括密钥标识、PN 和 MIC, 在第二个 A-MPDU 子帧字段的 MPDU 字段中携带确认 (acknowledgement, ACK) 帧 (即控制帧的一例)。

S1320, 第一设备向第二设备发送 PPDU。对应的, 第二设备接收来自第一设备的 PPDU。

S1330, 第二设备解析 PPDU。

第二设备在接收到 PPDU 之后, 基于 PPDU 的 A-MPDU 的第二 MPDU 中携带的第一信息确定第一 MPDU 中承载的控制帧是否受到攻击。如果受到攻击, 则忽略该控制帧, 否则, 基于接收到的控制帧继续后续处理流程。具体判断过程参见 S330 中的描述, 这里不再赘述。

上述技术方案中, 利用将多个 MPDU 聚合起来的 A-MPDU, 在 A-MPDU 的一个 MPDU (帧) 中承载控制帧, 在另外一个 MPDU 承载第一信息, 即通过 A-MPDU 跨帧对控制帧进行保护, 该控制帧保护机制可以适用于任何控制帧, 由于该保护机制不需要对控制帧本身进行修改或重新定义, 尤其适用于无法更改帧格式的控制帧。

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

还应理解, 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。

还应理解, 在上述一些实施例中, 主要以现有的网络架构中的设备为例进行了示例性说明, 应理解, 对于设备的具体形式本申请实施例不作限定。例如, 在未来可以实现同样功能的设备都适用于本申请实施例。

可以理解的是，上述各个方法实施例中，由设备（如上述如第一设备、第二设备等）实现的方法和操作，也可以由设备的部件（例如芯片或者电路）实现。

以上，结合图 1 至图 14 详细说明了本申请实施例提供的方法。上述方法主要从第一设备和第二设备之间交互的角度进行了介绍。可以理解的是，第一设备和第二设备，为了实现上述功能，其包含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，本申请能够以硬件或硬件和计算机软件的结合形式来实现。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。

以下，结合图 15 和图 16 详细说明本申请实施例提供的通信装置。应理解，装置实施例的描述与方法实施例的描述相互对应，因此，未详细描述的内容可以参见上文方法实施例，为了简洁，部分内容不再赘述。本申请实施例可以根据上述方法示例对第一设备或第二设备进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。需要说明的是，本申请实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。下面以采用对应各个功能划分各个功能模块为例进行说明。

以上对本申请提供的通信方法进行了详细说明，下面介绍本申请提供的通信装置。在一种可能的实现方式中，该装置用于实现上述方法实施例中的第一设备对应的步骤或流程。在另一种可能的实现方式中，该装置用于实现上述方法实施例中的第二设备对应的步骤或流程。

图 15 是本申请实施例提供的通信装置 200 的示意性框图。如图 15 所示，该装置 200 可以包括通信单元 210 和处理单元 220。通信单元 210 可以与外部进行通信，处理单元 220 用于进行数据处理。通信单元 210 还可以称为通信接口或收发单元。

在一种可能的设计中，该装置 200 可实现对应于上文方法实施例中的第一设备执行的步骤或者流程，其中，处理单元 220 用于执行上文方法实施例中第一设备的处理相关的操作，通信单元 210 用于执行上文方法实施例中第一设备的发送相关的操作。

在又一种可能的设计中，该装置 200 可实现对应于上文方法实施例中的第二设备执行的步骤或者流程，其中，通信单元 210 用于执行上文方法实施例中第二设备的接收相关的操作，处理单元 220 用于执行上文方法实施例中第二设备的处理相关的操作。

应理解，这里的装置 200 以功能单元的形式体现。这里的术语“单元”可以指应用特有集成电路（application specific integrated circuit, ASIC）、电子电路、用于执行一个或多个软件或固件程序的处理器（例如共享处理器、专有处理器或组处理器等）和存储器、合并逻辑电路和/或其它支持所描述的功能的合适组件。在一个可选例子中，本领域技术人员可以理解，装置 200 可以具体为上述实施例中的第一设备，可以用于执行上述方法实施例中与第一设备对应的各个流程和/或步骤，或者，装置 200 可以具体为上述实施例中的第二设备，可以用于执行上述方法实施例中与第二设备对应的各个流程和/或步骤，为避免重复，在此不再赘述。

上述各个方案的装置 200 具有实现上述方法中第一设备所执行的相应步骤的功能，或者，上述各个方案的装置 200 具有实现上述方法中第二设备所执行的相应步骤的功能。所述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。所述硬件或软件包括一个或多个与上述功能相对应的模块；例如通信单元可以由收发机替代（例如，通信单元中的发送单元可以由发送机替代，通信单元中的接收单元可以由接收机替代），其它单元，如处理单元等可以由处理器替代，分别执行各个方法实施例中的收发操作以及相关的处理操作。

此外，上述通信单元还可以是收发电路（例如可以包括接收电路和发送电路），处理单元可以是处理电路。在本申请的实施例，图 15 中的装置可以是前述实施例中的第一设备或第二设备，也可以是芯片或者芯片系统，例如：片上系统（system on chip, SoC）。其中，通信单元可以是输入输出电路、通信接口；处理单元为该芯片上集成的处理器或者微处理器或者集成电路。在此不做限定。

图 16 为本申请实施例提供的通信装置 300 的示意性框图。该装置 300 包括处理器 310 和收发器 320。其中，处理器 310 和收发器 320 通过内部连接通路互相通信，该处理器 310 用于执行指令，以控制该收发器 320 发送信号和/或接收信号。

可选地，该装置 300 还可以包括存储器 330，该存储器 330 与处理器 310、收发器 320 通过内部连接通路互相通信。该存储器 330 用于存储指令，该处理器 310 可以执行该存储器 330 中存储的指令。在一种可能的实现方式中，装置 300 用于实现上述方法实施例中的第一设备对应的各个流程和步骤。在另一种可能的实现方式中，装置 300 用于实现上述方法实施例中的第二设备对应的各个流程和步骤。

应理解，装置 300 可以具体为上述实施例中的第一设备或第二设备，也可以是芯片或者芯片系统。对应的，该收发器 320 可以是该芯片的收发电路，在此不做限定。具体地，该装置 300 可以用于执行上述方法实施例中与第一设备或第二设备对应的各个步骤和/或流程。可选地，该存储器 330 可以包括只读存储器和随机存取存储器，并向处理器提供指令和数据。存储器的一部分还可以包括非易失性随机存取存储器。例如，存储器还可以存储设备类型的信息。该处理器 310 可以用于执行存储器中存储的指令，并且当该处理器 310 执行存储器中存储的指令时，该处理器 310 用于执行上述与第一设备或第二设备对应的方法实施例的各个步骤和/或流程。

在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

应注意，本申请实施例中的处理器可以是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法实施例的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现场可编程门阵列（FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。本申请实施例中的处理器可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

可以理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（read-only memory，ROM）、可编程只读存储器（programmable ROM，PROM）、可擦除可编程只读存储器（erasable PROM，EPROM）、电可擦除可编程只读存储器（electrically EPROM，EEPROM）或闪存。易失性存储器可以是随机存取存储器（random access memory，RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（static RAM，SRAM）、动态随机存取存储器（dynamic RAM，DRAM）、同步动态随机存取存储器（synchronous DRAM，SDRAM）、双倍数据速率同步动态随机存取存储器（double data rate SDRAM，DDR SDRAM）、增强型同步动态随机存取存储器（enhanced SDRAM，ESDRAM）、同步连接动态随机存取存储器（synchlink DRAM，SLDRAM）和直接内存总线随机存取存储器（direct rambus RAM，DR RAM）。应注意，本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

需要说明的是，当处理器为通用处理器、DSP、ASIC、FPGA 或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件时，存储器（存储模块）可以集成在处理器中。还需要说明的是，本文描述的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

此外，本申请还提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机指令，当计算机指令在计算机上运行时，使得本申请各方法实施例中由第一设备或第二设备执行的操作和/或流程被执行。

本申请还提供一种计算机程序产品，计算机程序产品包括计算机程序代码或指令，当计算机程序代码或指令在计算机上运行时，使得本申请各方法实施例中由第一设备或第二设备执行的操作和/或流程被执行。

此外，本申请还提供一种通信系统，包括本申请实施例中的第一设备或第二设备。

还需要说明的是，本文描述的存储器旨在包括但不限于这些和任意其它适合类型存储器。

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。在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用，可以存储在一个计算机可读存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

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. 一种发送物理层协议数据单元的方法，其特征在于，包括：

生成物理层协议数据单元 PPDU，所述 PPDU 包括控制帧，所述控制帧包括 N 个第一用户信息字段，其中，所述第一用户信息字段中的关联标识指示所述第一用户信息字段中承载第一信息，所述第一信息包括用于保护所述控制帧的信息，所述 N 为大于或等于 1 的整数；

发送所述 PPDU。

2. 根据权利要求 1 所述的方法，其特征在于，所述第一信息包括秘钥标识，报文数 PN，和消息完整性代码 MIC 中的至少一项。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述 N 个第一用户信息字段的 N 个关联标识中的任一关联标识为预定义的数值。

4. 根据权利要求 1 至 3 中任一项所述的方法，其特征在于，所述控制帧的公共字段中承载第二信息，所述第二信息指示所述控制帧中承载了所述第一信息。

5. 根据权利要求 1 至 4 中任一项所述的方法，其特征在于，所述控制帧的公共字段中承载第三信息，所述第三信息指示所述 N 个第一用户信息字段中的至少一个第一用户信息字段的位置。

6. 根据权利要求 1 至 5 中任一项所述的方法，其特征在于，所述控制帧中的公共字段或帧校验序列 FCS 字段中的至少一个字段中承载第四信息，所述第四信息包括用于保护所述控制帧的信息。

7. 根据权利要求 1 至 6 中任一项所述的方法，其特征在于，

所述控制帧的帧校验序列 FCS 字段的第一位置上承载第一异或结果，所述第一异或结果为所述 FCS 字段的所述第一位置上对应的循环冗余码 CRC 与第五信息的异或结果，所述第五信息包括用于保护所述控制帧的信息，所述 FCS 字段的第一位置上的 CRC 对应的比特值与所述第五信息对应的比特值的比特个数相同。

8. 根据权利要求 1 至 7 中任一项所述的方法，其特征在于，所述 N 个第一用户信息字段中最后一个第一用户信息字段结束到所述控制帧结束之间的时长大于或等于第一类型设备的最小触发帧处理时间，所述第一类型设备为能够解读所述第一用户信息字段的关联标识的设备。

9. 一种接收物理层协议数据单元的方法，其特征在于，包括：

接收物理层协议数据单元 PPDU，所述 PPDU 包括控制帧，所述控制帧包括 N 个第一用户信息字段，其中，所述第一用户信息字段中的关联标识指示所述第一用户信息字段中承载第一信息，所述第一信息包括用于保护所述控制帧的信息，所述 N 为大于或等于 1 的整数；

解析所述 PPDU。

10. 根据权利要求 9 所述的方法，其特征在于，所述第一信息包括秘钥标识，报文数 PN，和消息完整性代码 MIC 中的至少一项。

11. 根据权利要求 10 所述的方法，其特征在于，所述控制帧中承载所述 MIC，所述方法还包括：

确定本地 MIC；

确定所述本地 MIC 与所述控制帧中承载的所述 MIC 匹配，则认为所述控制帧没有被伪造。

12. 根据权利要求 10 或 11 所述的方法，其特征在于，所述控制帧中承载所述 PN，所述方法还包括：

确定所述控制帧中承载的所述 PN 大于上一次接收到的 PN，则认为所述控制帧没有发生重播攻击。

13. 根据权利要求 9 至 12 中任一项所述的方法，其特征在于，所述 N 个第一用户信息字段的 N 个关联标识中的任一关联标识为预定义的数值。

14. 根据权利要求 9 至 13 中任一项所述的方法，其特征在于，所述控制帧的公共字段中承载第二信息，所述第二信息指示所述控制帧中承载了所述第一信息。

15. 根据权利要求 9 至 14 中任一项所述的方法，其特征在于，所述控制帧的公共字段中承载第三信息，所述第三信息指示所述 N 个第一用户信息字段中的至少一个第一用户信息字段的位置。

16. 根据权利要求 9 至 15 中任一项所述的方法，其特征在于，所述控制帧中的公共字段或帧校验序列 FCS 字段中的至少一个字段中承载第四信息，所述第四信息包括用于保护所述控制帧的信息。

17. 根据权利要求 9 至 16 中任一项所述的方法，其特征在于，

所述控制帧的帧校验序列 FCS 字段的第一位置上承载第一异或结果，所述第一异或结果为所述 FCS

字段的所述第一位置上对应的循环冗余码 CRC 与第五信息的异或结果, 所述第五信息包括用于保护所述控制帧的信息, 所述 FCS 字段的第一位置上的 CRC 对应的比特值与所述第五信息对应的比特值的比特个数相同。

18. 根据权利要求 9 至 17 中任一项所述的方法, 其特征在于, 所述 N 个第一用户信息字段中最后一个第一用户信息字段结束到所述控制帧结束之间的时长大于或等于第一类型设备的最小触发帧处理时间, 所述第一类型设备为能够解读所述第一用户信息的关联标识字段的设备。

19. 一种通信装置, 其特征在于, 所述通信装置包括用于执行所述权利要求 1 至 8 中任一方法的模块, 或, 所述通信装置包括用于执行权利要求 9 至 18 中任一方法的模块。

20. 一种通信装置, 其特征在于, 包括处理器, 所述处理器与存储器耦合, 可用于执行所述存储器中的指令, 以实现所述权利要求 1 至 8 中任一方法, 或者, 以实现所述权利要求 9 至 18 中任一方法。

21. 一种计算机可读存储介质, 其特征在于, 所述计算机可读存储介质上存储有计算机指令, 所述计算机指令被装置执行时, 使得所述装置实现所述权利要求 1 至 8 中任一方法, 或者, 使得所述装置实现所述权利要求 9 至 18 中任一方法。