(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118975172 A
(43)申请公布日 2024.11.15

(21)申请号 202380032000.7

(22)申请日 2023.03.23

(30)优先权数据
202241022313 2022.04.14 IN

(85)PCT国际申请进入国家阶段日
2024.09.29

(86)PCT国际申请的申请数据
PCT/US2023/016149 2023.03.23

(87)PCT国际申请的公布数据
WO2023/200572 EN 2023.10.19

(71)申请人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 A·P·帕蒂尔 G·切瑞安
A·阿斯特加迪 S·Y·D·何
G·奈克 A·K·阿贾米 孙延军
J·K·马利宁 S·库帕
P·V·卡尔蒂奇
G·R·弗雷德里克斯 J·S·赵

(74)专利代理机构 上海专利商标事务所有限公司 31100
专利代理师 周敏

(51)Int.Cl.
H04L 1/1607(2006.01)

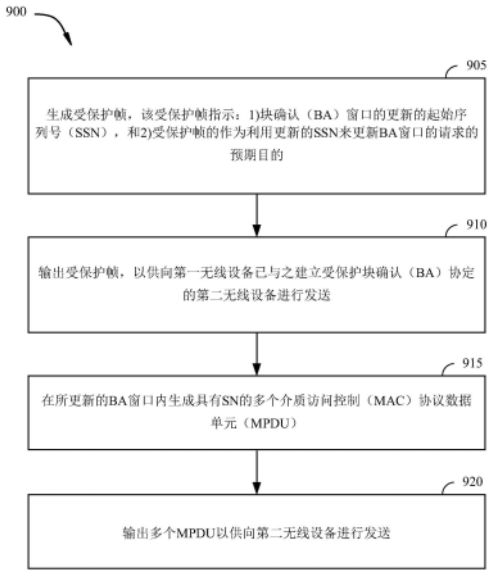
权利要求书2页 说明书17页 附图16页

(54)发明名称

受保护块确认机制

(57)摘要

本公开的某些方面提供了一种用于在第一无线设备处进行无线通信的方法。该方法一般包括:生成受保护帧,该受保护帧指示:1)块确认(BA)窗口的更新的起始序列号(SSN),和2)该受保护帧的作为利用该更新的SSN来更新BA窗口的请求的预期目的;输出该受保护帧,以供向该第一无线设备已与之建立受保护块确认(BA)协定的第二无线设备进行发送;在所更新的BA窗口内生成具有SN的多个介质访问控制(MAC)协议数据单元(MPDU);以及输出该多个MPDU以供向该第二无线设备进行发送。



CN 118975172 A

1.一种用于无线通信的装置,包括:

存储器,所述存储器包括指令;和

一个或多个处理器,所述一个或多个处理器被配置为执行所述指令并且使所述装置:

生成受保护帧,所述受保护帧指示:1)块确认(BA)窗口的更新的起始序列号(SSN),和2)所述受保护帧的作为利用所述更新的SSN来更新BA窗口的请求的预期目的;

输出所述受保护帧,以供向所述装置已与之建立受保护块确认(BA)协定的无线设备进行发送;

在所更新的BA窗口内生成具有SN的多个介质访问控制(MAC)协议数据单元(MPDU);以及

输出所述多个MPDU以供向所述无线设备进行发送。

2.根据权利要求1所述的装置,其中所述一个或多个处理器被进一步配置为执行所述指令并且使所述装置:

输出指示BA请求的MPDU以供向所述无线设备进行发送;以及

响应于所述请求而从所述无线设备获得BA,所述BA指示在所更新的BA窗口内的所述MPDU中的哪些MPDU是由所述无线设备成功接收的。

3.根据权利要求1所述的装置,其中所述受保护帧包括被设计用于更新所述BA窗口的BA动作帧。

4.根据权利要求3所述的装置,其中所述受保护帧经由所述受保护帧的类别字段或BA动作字段中的至少一者来指示所述预期目的。

5.根据权利要求1所述的装置,其中所述一个或多个处理器被进一步配置为执行所述指令并且使所述装置:从所述无线设备获得对所述受保护帧的确认。

6.根据权利要求1所述的装置,其中所述受保护帧包括添加BA(ADDBA)请求帧。

7.根据权利要求6所述的装置,其中所述受保护帧包括被设置为某个值以指示所述预期目的的字段。

8.根据权利要求7所述的装置,其中所述字段位于所述ADDBA请求帧的帧报头中。

9.根据权利要求1所述的装置,还包括:至少一个收发器,所述至少一个收发器被配置为发送所述受保护帧和所述多个MPDU,其中所述装置被配置为无线设备。

10.一种用于无线通信的装置,包括:

存储器,所述存储器包括指令;和

一个或多个处理器,所述一个或多个处理器被配置为执行所述指令并且使所述装置:

从所述装置已与之建立受保护块确认(BA)协定的无线设备获得受保护帧,所述受保护帧指示:1)块确认(BA)窗口的更新的起始序列号(SSN),和2)所述受保护帧的作为利用所述更新的SSN来更新BA窗口的请求的预期目的;以及

维持位图以跟踪所更新的BA窗口内的已由所述装置成功获得的具有SN的介质访问控制(MAC)协议数据单元(MPDU)。

11.根据权利要求10所述的装置,其中所述一个或多个处理器被进一步配置为执行所述指令并且使所述装置:

从所述无线设备获得BA请求;以及

输出指示BA的MPDU以供向所述无线设备进行发送,所述BA指示所更新的BA窗口内的所

述MPDU中的哪些MPDU是由所述装置根据所述位图成功获得的。

12.根据权利要求10所述的装置,其中所述受保护帧包括被设计用于更新所述BA窗口的BA动作帧。

13.根据权利要求12所述的装置,其中所述受保护帧经由所述受保护帧的类别字段或BA动作字段中的至少一者来指示所述预期目的。

14.根据权利要求10所述的装置,其中所述一个或多个处理器被进一步配置为执行所述指令并且使所述装置:输出对所述受保护帧的确认以供向所述装置进行发送。

15.根据权利要求10所述的装置,其中所述受保护帧包括添加BA(ADDBA)请求帧。

16.根据权利要求15所述的装置,其中所述ADDBA请求帧包括被设置为某个值以指示所述预期目的的字段。

17.根据权利要求16所述的装置,其中所述字段位于所述ADDBA请求帧的帧报头中。

18.根据权利要求10所述的装置,还包括:至少一个收发器,所述至少一个收发器被配置为接收所述受保护帧,其中所述装置被配置为无线设备。

受保护块确认机制

[0001] 相关申请的交叉引用

[0002] 本申请要求于2022年4月14日提交的印度专利申请202241022313号的优先权,该申请被转让给本申请的受让人并且据此全文以引用方式明确地并入,如同在下文完整地阐述一样并且用于所有适用目的。

技术领域

[0003] 本公开的某些方面整体涉及无线通信,并且更具体地涉及保护无线网络中的各种类型的消息。

背景技术

[0004] 无线通信网络被广泛部署以提供各种通信服务,诸如语音、视频、分组数据、消息接发、广播等。这些无线网络可以是能够通过共享可用的网络资源来支持多个用户的多址网络。这类多址网络的例子包括码分多址(CDMA)网络、时分多址(TDMA)网络、频分多址(FDMA)网络、正交FDMA(OFDMA)网络和单载波FDMA(SC-FDMA)网络。

[0005] 为了解决无线通信系统所需的增加的带宽需求的问题,正在开发不同的方案以允许多个用户终端在实现高数据吞吐量的同时通过共享信道资源与单个接入点通信。多输入多输出(MIMO)技术代表一种此类办法,该办法已涌现为一种用于通信系统的流行技术。MIMO技术已在若干无线通信标准(诸如电气与电子工程师协会(IEEE)802.11标准)中被采用。IEEE 802.11表示由IEEE 802.11委员会开发的用于短距离通信(诸如数十米到几百米)的无线局域网(WLAN)空中接口标准集合。

发明内容

[0006] 本公开的系统、方法和设备各自具有若干创新性方面,其中并不由任何单个方面全权负责本文所公开的期望属性。

[0007] 本公开的某些方面提供了一种用于在第一无线设备处进行的无线通信的方法。该方法一般包括:生成受保护帧,该受保护帧指示:1)块确认(BA)窗口的更新的起始序列号(SSN),和2)该受保护帧的作为利用该更新的SSN来更新BA窗口的请求的预期目的;输出该受保护帧,以供向该第一无线设备已与之建立受保护块确认(BA)协定的第二无线设备进行发送;在所更新的BA窗口内生成具有SN的多个介质访问控制(MAC)协议数据单元(MPDU);以及输出该多个MPDU以供向该第二无线设备进行发送。

[0008] 本公开的某些方面提供了一种用于在第二无线设备处进行的无线通信的方法。该方法一般包括:从该第二无线设备已与之建立受保护块确认(BA)协定的第一无线设备获得受保护帧,该受保护帧指示:1)块确认(BA)窗口的更新的起始序列号(SSN),和2)该受保护帧的作为利用该更新的SSN来更新BA窗口的请求的预期目的;以及维持位图以跟踪所更新的BA窗口内的已由该第二无线设备成功获得的具有SN的介质访问控制(MAC)协议数据单元(MPDU)。

[0009] 本公开的某些方面提供了一种用于在无线设备处进行的无线通信的方法。该方法一般包括:获得具有未能通过解密校验或完整性校验中的至少一者的介质访问控制(MAC)协议数据单元(MPDU)的数据帧;以及响应于该失败而清除:用于跟踪已由该无线设备成功获得的MPDU的位图中的条目;或用于跟踪已由该无线设备成功获得的MPDU的该位图中的与接收到的MPDU相对应的条目。

[0010] 本公开的某些方面提供了一种用于在第一无线设备处进行的无线通信的方法。该方法一般包括:生成具有使用应用于介质访问控制(MAC)协议数据单元(MPDU)的序列号(SN)的附加认证数据(AAD)来加密的MPDU的数据帧;以及输出该数据帧,以供向该第一无线设备已与之建立受保护块确认(BA)协定的第二无线设备进行发送。

[0011] 本公开的某些方面提供了一种用于在第二无线设备处进行的无线通信的方法。该方法一般包括:从第一无线设备获得该第一无线设备已利用其建立受保护块确认(BA)协定的数据帧;以及使用该介质访问控制(MAC)协议数据单元(MPDU)的序列号(SN)基于附加认证数据(AAD)解构来从该数据帧提取该MPDU。

[0012] 本公开的某些方面提供了一种用于在第一无线设备处进行的无线通信的方法。该方法一般包括:通过对原始介质访问控制(MAC)协议数据单元(MPDU)的序列号(SN)执行操作来修改该MPDU以获得修改的MPDU;生成具有所修改的MPDU的加密版本的数据帧;以及输出该数据帧,以供向该第一无线设备已与之建立受保护块确认(BA)协定的第二无线设备进行发送。

[0013] 本公开的某些方面提供了一种用于在第二无线设备处进行的无线通信的方法。该方法一般包括:从第二无线设备已与之建立受保护块确认(BA)协定的第一无线设备获得具有介质访问控制(MAC)协议数据单元(MPDU)的修改版本的序列号(SN)的数据帧;基于该MPDU的修改版本来执行循环冗余校验(CRC)测试;以及如果该CRC测试通过,则对该SN执行操作以在该CRC测试通过的情况下从该MPDU的该修改版本恢复原始MPDU;以及更新BA位图以指示对该原始MPDU的成功接收。

[0014] 为了实现前述和相关的目的,一个或多个方面包括以下全面描述的并在权利要求中特别指出的特征。以下描述和附图详细阐述了这一个或多个方面的某些例示性特征。然而,这些特征仅指示可采用各个方面的原理的各种方式中的仅一些方式。

附图说明

[0015] 为了能够详细理解本公开的上述特征的方式,以上简要概括的更具体的描述可通过参考各方面来获得,这些方面中的一些方面在附图中例示。然而,应注意,附图仅例示本公开的某些典型方面,并且描述可准许其他等同有效方面。

[0016] 图1是根据本公开的某些方面的示例无线通信网络的示图。

[0017] 图2是根据本公开的某些方面的示例接入点(AP)和示例无线站(STA)的框图。

[0018] 图3是根据本公开的各方面的例示示例块确认规程的调用流程图。

[0019] 图4是例示根据本公开的各方面的用于防范伪块确认请求(BAR)的示例机制的调用流图示。

[0020] 图5是例示根据本公开的各方面的用于防范伪数据帧的示例机制的调用流图示。

[0021] 图6A和图6B例示了根据本公开的各方面的用于防范伪数据帧的示例逻辑和示例

序列控制字段。

[0022] 图7是例示根据本公开的各方面的用于防范具有修改的序列号的数据帧的重放的示例机制的调用流图示。

[0023] 图8例示了根据本公开的各方面的用于防范具有修改的序列号的数据帧的重放的示例逻辑。

[0024] 图9例示了根据本公开的某些方面的用于在无线设备处进行的无线通信的示例操作。

[0025] 图10例示了根据本公开的某些方面的用于在无线设备处进行的无线通信的示例操作。

[0026] 图11例示了根据本公开的某些方面的用于在无线设备处进行的无线通信的示例操作。

[0027] 图12例示了根据本公开的某些方面的用于在无线设备处进行的无线通信的示例操作。

[0028] 图13例示了根据本公开的某些方面的用于在无线设备处进行的无线通信的示例操作。

[0029] 图14例示了根据本公开的某些方面的用于在无线设备处进行的无线通信的示例操作。

[0030] 图15例示了根据本公开的某些方面的用于在无线设备处进行的无线通信的示例操作。

[0031] 图16例示了能够执行本文所述的操作的示例组件。

[0032] 为了便于理解,已经在可能的情况下使用了相同的参考标号来表示附图共有的相同元素。可设想,在一个方面所公开的元素可有益地用于其他方面而无需具体叙述。

具体实施方式

[0033] 本公开的各方面整体涉及无线通信,并且更具体地涉及保护无线网络中的各种类型的消息。

[0034] 存在各种类型的攻击,敌对设备(攻击方)可执行这些攻击以在无线网络中造成损害。此类攻击的示例包括投入块确认请求(BAR)帧、投入伪数据帧以及重放真实数据帧,但是具有修改的序列号(SN)。

[0035] 这些类型的攻击中的每一者都可能影响系统性能,不仅由于带宽的消耗,而且还由于处理开销和有效帧递送中的潜在中断(拒绝服务)。在一些情况下,攻击可能无法被检测到,并且在此类情况下,中断在接收器处维持的记分板的上下文以由SN成功地接收分组。

[0036] 本公开的各方面提出了用于防范这些类型的攻击的各种机制。因此,这些机制可帮助防止有效帧递送中的潜在中断,并且因此可帮助改进总体系统性能。

[0037] 无线通信系统的概述

[0038] 下文参考附图更加充分地描述本公开的各个方面。然而,本公开可用许多不同形式来实施并且不应解释为被限于本公开通篇给出的任何具体结构或功能。而是,提供这些方面以使得本公开将是透彻的和完整的,以及将向本领域技术人员完整地传达本公开的保护范围。基于本文的教导内容,本领域的技术人员应当理解的是,本公开的范围旨在涵盖本

文所公开的公开的任何方面,无论其是独立实现的还是结合本公开的任何其他方面实现的。例如,可使用本文中阐述的任何数量的方面来实现装置或实践方法。此外,本公开的范围旨在涵盖使用除了本文中所阐述的公开的各个方面之外或不同于本文中所阐述的公开的各个方面的其他结构、功能或者结构和功能来实践的这样的装置或方法。应当理解,本文所公开的公开内容的任何方面可通过权利要求的一个或多个元素来实现。

[0039] 词语"示例性"在本文中用于意指"用作示例、实例或例示"。本文中被描述为"示例性"的任何方面不一定被解释为比其他方面优选或具有优势。

[0040] 尽管本文描述了特定方面,但这些方面的众多变型形式和排列落在本公开的范围之内。虽然提及了优选的方面的一些利益和优点,但是本公开内容的保护范围并不旨在受到特定的利益、用途或对象的限制。更确切地说,本公开内容的方面旨在广泛地适用于不同的无线技术、系统配置、网络和发送协议,其中的一些通过示例的方式在附图和优选方面的下文描述中进行了例示。具体实施方式和附图仅仅是对本公开的例示而不是限制,本公开的范围由所附权利要求书及其等效物来限定。

[0041] 本文所述的技术可用于各种宽带无线通信系统,包括基于正交复用方案的通信系统。此类通信系统的示例包括空分多址(SDMA)、时分多址(TDMA)、正交频分多址(OFDMA)系统、单载波频分多址(SC-FDMA)系统等等。SDMA系统可充分利用不同的方向来同时发送属于多个用户终端的数据。TDMA系统可通过将发送信号划分成不同的时隙,来允许多个用户终端共享相同的频率信道,每个时隙被指派给不同的用户终端。OFDMA系统利用正交频分复用(OFDM),该正交频分复用(OFDM)是将整个系统带宽分割成多个正交的子载波的调制技术。这些子载波也可被称为音调、频段(bin)等。通过OFDM,每个子载波可以是使用数据独立调制的。SC-FDMA系统可利用交织的FDMA(IFDMA)来在跨越系统带宽来分布的子载波上进行发送,利用集中式FDMA(localized FDMA,LFDMA)来在邻近子载波块上进行发送,或利用增强的FDMA(EFDMA)来在多个邻近子载波块上进行发送。一般来讲,调制符号在频域中使用OFDM传送,并且在时域中使用SC-FDMA传送。

[0042] 本文的教导内容可被纳入各种有线或无线装置(诸如,节点)中(诸如,在该装置内实现或由该装置执行)。在一些方面,根据本文的教导内容来实现的无线节点可包括接入点或接入终端。

[0043] 接入点("AP")可包括、实现为或者称为节点B、无线网络控制器("RNC")、演进型节点B(eNB)、基站控制器("BSC")、基站收发器("BTS")、基站("BS")、收发器功能单元("TF")、无线电路由器、无线电收发器、基本服务集("BSS")、扩展服务集("ESS")、无线电基站("RBS")或者某种其他术语。

[0044] 接入终端("AT")可包括、被实现为、或被称为订户站、订户单元、移动站(MS)、远程站、远程终端、用户终端(UT)、用户代理、用户设备、用户装备(UE)、用户站、或某个其他术语。在一些具体实施中,接入终端可包括蜂窝电话、无绳电话、会话发起协议("SIP")电话、无线本地环路("WLL")站、个人数字助理("PDA")、具有无线连接能力的手持式设备、站("STA")、或连接到无线调制解调器的某种其他合适的处理设备。因此,本文所教示的一个或多个方面可并入到电话(诸如蜂窝电话或智能电话)、计算机(诸如膝上型计算机)、平板设备、便携式通信设备、便携式计算设备(诸如个人数据助理)、娱乐设备(诸如音乐或视频设备、或卫星收音机)、全球定位系统(GPS)设备或者被配置为经由无线介质或有线介质进行

通信的任何其他合适的设备。在一些方面,该节点是无线节点。例如,这样的无线节点可经由有线或无线通信链路来提供针对网络(诸如,诸如互联网或蜂窝网络的广域网)的连接或到网络的连接。

[0045] 示例无线通信系统

[0046] 图1是例示根据本公开的某些方面的示例无线通信系统100的示图。系统100可以是多输入多输出(MIMO)/多链路操作(MLO)系统100。在各方面,AP 110和无线站120a可以是如本文关于图3进一步描述的MLD。

[0047] 为简单起见,图1中仅示出一个AP 110。AP通常是与无线STA进行通信的固定站,并且也可被称为基站(BS)或某个其他术语。无线STA可以是固定的或者移动的,并且也可被称作移动STA、无线设备、或某个其他术语。AP 110可在任何给定时刻在下行链路(DL)和/或上行链路(UL)上与一个或多个无线STA 120进行通信。DL(即,前向链路)是从AP 110到无线STA 120的通信链路,并且UL(即,反向链路)是从无线STA 120到AP 110的通信链路。无线STA 120也可,例如经由直接链路(诸如隧穿直接链路设立(TDLS)),与另一无线STA 120进行对等通信。系统控制器130可与该接入点通信并为该接入点提供协调和控制。

[0048] 虽然以下公开的各部分将描述能够经由空分多址(SDMA)来通信的无线STA 120,但对于某些方面,无线STA 120还可包括不支持SDMA的一些无线STA 120。因此,对于此类方面,AP 110可被配置为与SDMA和非SDMA无线STA 120两者进行通信。这一办法可便于允许较老版本的无线STA 120("旧式"站)仍被部署在企业中从而延长它们的有用寿命,同时允许在认为适当的场合引入较新的SDMA无线STA 120。

[0049] 系统100采用多个发送天线和多个接收天线来在DL和UL上进行数据发送。AP 110配备有N_{ap}个天线并且对于DL发送而言表示多输入(MI)而对于UL发送而言表示多输出(MO)。K个所选无线站120的集合共同地对于DL发送而言表示多输出并且对于UL发送而言表示多输入。对于纯SDMA,如果K个无线STA的数据符号流未通过某种手段在代码、频率或时间上复用,则期望$N_{ap} \geq K \geq 1$。如果数据符号流可使用TDMA技术、利用CDMA的不同代码信道、利用OFDM的不相交子带集等进行复用,则K可大于N_{ap}。每个所选无线STA向接入点发送用户特定的数据和/或从接入点接收用户特定的数据。通常,每个所选无线STA可配备有一个或多个天线(即,$N_{sta} \geq 1$)。K个所选无线STA可具有相同或不同数量的天线。

[0050] 系统100可以是时分双工(TDD)系统或者频分双工(FDD)系统。对于TDD系统,DL和UL共享相同的频带。对于FDD系统,DL和UL使用不同的频带。系统100还可以利用单个载波或者多个载波进行发送。每个无线STA可配备有单个天线或多个天线。如果无线STA 120通过将发送/接收划分到不同时隙中来共享相同频率信道,则系统100还可以是TDMA系统,每个时隙被指派给不同的无线STA 120。

[0051] 图2例示了根据本公开的某些方面的MIMO/MLO系统(诸如系统100)中的AP 110以及两个无线STA 120m和120x的框图。在某些方面,AP 110和/或无线STA 120m和120x可执行各种技术以确保非AP MLD能够接收组寻址帧。

[0052] AP 110配备有N_{ap}个天线224a至224t。无线STA 120m配备有$N_{sta,m}$个天线252ma至252mu,并且无线STA 120x配备有$N_{sta,x}$个天线252xa至252xu。AP 110是用于DL的发送实体和用于UL的接收实体。每个无线STA 120是用于UL的发送实体和用于DL的接收实体。如本文所使用的,"发送实体"是能够经由无线信道发送数据的独立操作的装置或设备,而"接收实

体"是能够经由无线信道接收数据的独立操作的装置或设备。术语通信一般指代发送、接收、或这两者。在下面的描述中,下标"DL"表示下行链路,下标"UL"表示上行链路,$_{N}U_{L}$个无线STA被选择用于在上行链路上进行同时发送,N_{DL}个无线STA被选择用于在下行链路上进行同时发送,N_{UL}可等于或者可不等于N_{DL},并且N_{UL}和N_{DL}可以是静态值,或者能够针对每个调度间隔而改变。可在接入点和无线站处使用波束转向或其他某种空间处理技术。

[0053] 在UL上,在被选择用于UL发送的每个无线STA 120处,发送(TX)数据处理器288接收来自数据源286的业务数据和来自控制器280的控制数据。TX数据处理器288基于与为该无线STA选择的速率相关联的译码和调制方案来处理(例如,编码、交织、以及调制)该无线站的业务数据并提供数据符号流。TX空间处理器290对数据符号流执行空间处理并向$N_{sta,m}$个天线提供$N_{sta,m}$个发送符号流。每个收发器(TMTR)254接收并处理(例如,转换至模拟、放大、滤波、及上变频)相应的发送符号流以生成上行链路信号。$N_{sta,m}$个收发器254提供$N_{sta,m}$个UL信号以供从$N_{sta,m}$个天线252向AP 110进行发送。

[0054] 可调度N_{UL}个无线STA以在上行链路上进行同时发送。这些无线STA中的每个无线STA对其数据符号流执行空间处理并在UL上向AP 110发送其发送符号流的集合。

[0055] 在AP 110处,N_{ap}个天线224a至224ap从全部N_{UL}个无线STA接收在UL上发送的UL信号。每个天线224向相应的收发器(RCVR)222提供接收信号。每个收发器222执行与由收发器254执行的处理互补的处理,并提供接收符号流。接收(RX)空间处理器240对来自N_{ap}个收发器222的N_{ap}个接收符号流执行接收器空间处理并提供N_{UL}个恢复的UL数据符号流。根据信道相关矩阵求逆(CCMI)、最小均方误差(MMSE)、软干扰消除(SIC)或者某种其他技术,来执行接收器空间处理。每个恢复的UL数据符号流是对由相应的无线站发送的数据符号流的估计。RX数据处理器242根据用于每个恢复的上行链路数据符号流的速率,对该流进行处理(例如,解调、解交织和解码),以获得解码的数据。关于每个无线STA的解码数据可被提供给数据宿244以供存储和/或提供给控制器230以供进一步处理。

[0056] 在DL上,在AP 110处,TX数据处理器210从数据源208接收用于被调度用于下行链路发送的N_{DL}个无线站的业务数据、来自控制器230的控制数据、以及可能来自调度器234的其他数据。各种类型的数据可以在不同的传输信道上进行传送。TX数据处理器210基于为每个无线站选择的速率来处理(例如,编码、交织、以及调制)该无线站的业务数据。TX数据处理器210为N_{DL}个无线站提供N_{DL}个DL数据符号流。TX空间处理器220对N_{DL}个DL数据符号流执行空间处理(诸如,进行如本公开中描述的预译码或波束成形),并且为N_{ap}个天线提供N_{ap}个发送符号流。每个收发器222接收并处理相应的发送符号流以生成DL信号。N_{ap}个收发器222提供N_{ap}个DL信号以供从N_{ap}个天线224向无线STA进行发送。

[0057] 在每个无线STA 120处,$N_{sta,m}$个天线252接收来自接入点110的N_{ap}个DL信号。每个收发器254处理来自相关联的天线252的接收信号并提供接收符号流。RX空间处理器260对来自$N_{sta,m}$个收发器254的$N_{sta,m}$个接收符号流执行接收器空间处理并为无线站提供恢复的DL数据符号流。根据CCMI、MMSE或某种其他技术来执行该接收器空间处理。RX数据处理器270处理(例如,解调、解交织以及解码)恢复的DL数据符号流以获得用于无线站的解码数据。

[0058] 在每个无线STA 120处,信道估计器278估计DL信道响应并提供DL信道估计,该DL信道估计可包括信道增益估计、SNR估计、噪声方差等。类似地,信道估计器228估计UL信道

响应并提供UL信道估计。每个无线STA的控制器280通常基于无线站的下行链路信道响应矩阵$H_{dn,m}$来导出用于该无线站的空间滤波器矩阵。控制器230基于有效UL信道响应矩阵$H_{up,eff}$来导出用于AP的空间滤波器矩阵。每个无线STA的控制器280可向AP传送反馈信息(例如,下行链路和/或上行链路本征向量、本征值、SNR估计等)。控制器230和280还分别控制AP 110和无线STA 120处的各个处理单元的操作。

[0059] 图3例示了根据本公开的某些方面的可在系统100内采用的无线设备302中利用的各种组件。无线设备302是可被配置为实现本文所述的各种方法的设备的示例。无线设备302可以是AP 110或用户终端。

[0060] 无线设备302可包括处理器304,该处理器控制无线设备302的操作。处理器304还可被称为中央处理单元(CPU)。可包括只读存储器(ROM)和随机存取存储器(RAM)两者的存储器306向处理器304提供指令和数据。存储器306的一部分还可包括非易失性随机存取存储器(NVRAM)。处理器304通常基于存储器306内存储的程序指令来进行逻辑和算术运算。存储器306中的指令可能够被执行以实现本文所述的方法。

[0061] 无线设备302还可包括外壳308,该外壳可包括发送器310和接收器312,以允许在无线设备302与远程位置之间发送和接收数据。发送器310和接收器312可被组合成收发器314。单个或多个发送天线316可被附连到外壳308并且电耦合到收发器314。无线设备302还可包括(未示出)多个发送器、多个接收器和多个收发器。

[0062] 无线设备302还可包括信号检测器318,该信号检测器可被用于检测和量化由收发器314接收的信号电平。信号检测器318可检测诸如总能量、每子载波每符号的能量、功率谱密度之类的信号和其他信号。无线设备302还可包括用于处理信号的数字信号处理器(DSP)320。

[0063] 可通过总线系统322将无线设备302的各个组件耦合在一起,该总线系统除了包括数据总线之外,还可包括电源总线、控制信号总线和状态信号总线。

[0064] 本公开的某些方面涉及用于实现多链路通信的装置和技术。例如,某些方面提供了用于通过MLD来管理跨多个链路的数据流的技术。可为无线设备实现多个频带。例如,无线设备可能能够支持2.4GHz频带、5GHz频带或6GHz频带中的至少一者并且在分布于这些频带上的多于一个的链路上操作。利用多链路通信,可跨可与不同频带相关联的多个无线链路发送数据流。

[0065] 示例块确认机制

[0066] 块确认(块Ack或BA)通常是指将多个MPDU的确认组合到单个帧中的机制。如图3所例示,BA会话可经由添加BA(ADDBA)请求和响应帧的交换在发送站(发起方STA)和接收站(接收方STA)之间建立(协商)。在一些情况下,发起方STA可首先基于BA能力比特来确认接收方STA能够参与安全BA会话。还应注意,发起方STA可以是AP或非AP设备。类似地,接收方STA可以是AP或非AP设备。换句话说,所协商的每个BA会话是针对特定方向(UL或DL)且针对每TID的。

[0067] 如果接收方STA能够参与安全BA会话,则发起方STA传送ADDBA请求帧,该ADDBA请求帧指示正在为其建立BA会话的业务ID(TID)。接收方STA将通过ADDBA响应帧来响应。接收方STA具有接受或拒绝该请求的选项。当接收方STA接受时,则受保护BA协定被称为存在于发起方STA和接收方STA之间。

[0068] 在受保护或不受保护的块ACK会话在AP和站之间协商之后,AP和WLAN站可参与无竞争突发,其中QoS数据帧(MPDU)的块可从发起方发送到接收方。接收方STA可维持用于在特定窗口内接收到的MPDU的记分卡,其中比特指示序列内的哪些MPDU被成功接收。

[0069] 发起方通过传送BA请求帧来请求对未完成的QoS数据帧的确认。该请求可被隐式地携带在数据帧本身内(在MAC报头中的字段中发信号通知),或者该请求可作为显式帧被传送。在不受保护的BA设置中,发起方可传送BlockAck请求(BAR)帧。作为响应,接收方STA可传送具有反映记分卡的位图的BA,该BA指示由AP成功接收的分组的数量。

[0070] 用于防范伪BAR帧的示例机制

[0071] BAR帧是控制帧,并且所有控制帧不受保护(或加密)。在一些情况下,敌对设备(攻击方)可通过发送(投入)伪BAR帧来执行攻击。这种类型的攻击是可能的,因为在常规无线系统中,BAR帧不受保护。

[0072] BAR帧通常用于两个一般目的。如上所述,第一个目的是获得在发送机会(TXOP)中传送的帧的先前突发的ACK信息。第二个目的是清除接收器处的接收重排序缓冲区。

[0073] 伪BAR帧的投入可能具有以下影响。攻击方可将BAR帧中的块确认起始序列控制子字段设置为任意值。如果这种类型的攻击未被注意到,则将中断接收方处的重排序缓冲区和记分板上下文。这种中断可导致起始序列号(SSN)的变化,并且导致关于接收方下一个预期序列号(WinStartB)的混淆。这可导致拒绝服务攻击,其中攻击方可阻止特定TID的真实数据帧的递送。

[0074] 根据常规规程,已经建立受保护的BA协定(会话)的STA不使用BAR帧中的SSN字段来更新WinStartB。相反,发起方STA发送受保护的管理帧(即,ADDBA请求帧)以更新WinStartB。接收方忽略ADDBA请求帧的除SSN之外的其他字段。

[0075] 然而,由于发起方被允许发送ADDBA请求帧以更新现有BA协定的参数(诸如超时),因此该现有规程产生潜在问题。然而,本公开的各方面可通过提供一种机制来解决这些潜在问题,该机制用于在被传送以使窗口(WinStartB)提前的ADDBA请求帧与被传送以更新参数的ADDBA请求帧之间进行区分。此外,本公开的各方面可帮助缓解关于当ADDBA请求被传送以提前窗口时是否需要ADDBA响应帧的模糊性。

[0076] 如图4所例示,本公开的某些方面可通过使用帧建立受保护BA协定来帮助防范伪BAR,该帧指示:1)块确认(BA)窗口的更新的起始序列号(SSN),和2)受保护帧的作为利用更新的SSN来更新BA窗口的请求的预期目的。存在可如何构造该帧的各种选项。

[0077] 例如,根据第一选项,可定义新的块确认动作帧。定义新的块Ack动作帧可提供传统的受保护BA规程和本文提出的更新的规程之间的清楚分离(区别)。假定典型常规系统不实现受保护BA帧,则这种变化(用于支持此新定义的BA动作帧)可对已部署的设备不具有影响。在支持BA动作帧的情况下,新帧可以提供与传统BA规程的清楚分离的方式来定义。这一办法还可帮助解决传统互用性的情况,其中已知一些设备不正确地通告对受保护BA规程的支持。

[0078] 这一办法的一个潜在益处在于,一些具体实施可使用单独的处理路径来快速地处理(新定义的)帧。通常,其他类型的管理帧(而不是动作帧)在更慢的路径上进行处理。使用ADDBA请求帧可迫使接收器使用此更快路径(例如,因为其可能无法区分被传送用于窗口推进或参数更新的ADDBA请求)。另一个潜在的好处在于,这一办法还可消除对显式(管理)响

应帧的需要,因为该新定义的帧能够被快速处理。这可帮助确保发起方和接收器关于WinStart0(其通常是指SN窗口中的最低序列号)处于相同状态(同步)并且WinStartB处于同步。

[0079] 在被传送以提前窗口(WinStartB)的ADDBA请求帧与被传送以更新参数的ADDBA请求之间进行区分的其他潜在选项包括使用ADDBA请求帧的动作字段中的现有字段(子字段)。例如,片段编号(FragNum)可被设置为某个值(例如,Frag Num=1)作为指示。另一选项是使用ADDBA请求帧的帧报头中的字段。由于帧报头被较早地处理,因此这一办法可帮助接收器快速地确定帧的意图,并且因此采取不同的(更快的)路径来处理帧。

[0080] 用于防范伪数据帧的示例机制

[0081] 在一些情况下,攻击方可发送(投入)伪数据帧,例如,具有任意序列号(SN)的数据帧。在常规系统中,这种类型的攻击可能直到执行解密/完整性校验才被检测到。遗憾的是,到那时,记分板上下文(以及可能地定义SN窗口开始的WinStartR)将得到更新。

[0082] 本公开的某些方面可通过使接收方STA响应于接收到具有未能通过解密校验或完整性校验中的至少一者的MPDU的数据帧而采取某些动作来帮助防范伪数据帧。作为示例,响应于该失败,接收方可清除用于跟踪已被无线设备成功接收的MPDU的位图中的条目,或者接收方可清除用于跟踪已由无线设备成功接收的MPDU的位图中的与所接收的MPDU相对应的条目。

[0083] 在接收方STA维持部分状态的情况下,接收方STA可清除BA记分板上下文(如果检测到伪数据帧)。如果接收方STA维持完全状态,如果检测到伪数据帧,则接收方STA可不更新WinStartR的值并且可清除该MPDU的BA记分板上下文。这一办法可能需要一些具体实施变化以便保持对MPDU的跟踪。作为另选方案,标准规范可强制或建议协商受保护BA的STA应当维持部分状态。

[0084] 用于防范真实数据帧的重放的示例机制

[0085] 在一些情况下,攻击方可通过重放(重新发送)真实的数据帧来执行攻击。例如,攻击方可记录真实MPDU(或AMPDU)并且用修改的序列号(或SN)重放该记录的(A)MPDU。攻击方可能知道实际的SN,因为携带SN的字段不受保护。由于该帧是重放帧,因此它应当会通过解密和完整性校验。结果,这种类型的攻击可能直到执行基于分组编号(PN)的重放校验才被注意到。遗憾的是,基于PN的重放校验通常在处理链中出现得晚得多。此时,记分板上下文(以及可能地WinStartR)将被更新。这也可能导致重排序缓冲区中的伪条目(并且可能地更新WinStartB)。

[0086] 如由图5的调用流图示500所例示,本公开的某些方面可通过使用应用于MPDU的序列号(SN)的附加认证数据(AAD)加密MPDU来帮助防范伪数据帧。接收方STA随后可使用MPDU SN基于AAD解构来提取MPDU。图6A的框图600例示了可如何使用将无掩蔽的SN比特作为输入的AAD构造逻辑来实现这种加密。如由图6B的示例字段650所例示,这可通过MPDU的序列控制(SC)字段的SN子字段中的无掩蔽比特来实现。

[0087] 防范具有修改的SN的真实数据帧的重放的这一办法可通过在受保护BA中强制SN保护来实现。在一些情况下,这可涉及对标准的更新以指定SN比特在AAD的计算期间不被掩蔽。如果使用部分状态,则刷新误差条件(SN校验未能通过)的记分板上下文。

[0088] 如由图7的调用流图示700所例示,在一些情况下,在发起方处,在加密MPDU之前,

MPDU的一部分可与SN进行逻辑异或(XOR)以生成修改的MPDU(示出为"MPDU")。所修改的MPDU(MPDU')然后被加密并且进一步向下传递。CRC基于所加密(修改)的MPDU和MAC报头(其包括序列控制字段中的SN)来生成。

[0089] 在接收方STA处,如果SN被修改(即,根据上述攻击场景),则针对所接收的MPDU的CRC验证将不能通过。MPDU被丢弃(不进一步沿链向上传递)。

[0090] 如由图8的处理流程图800所例示,如果SN未被修改(即,真实帧),则CRC校验将成功。因此,仅当CRC通过时,SN将被用于恢复原始MPDU并且被传递到记分板上下文,并且BA被传送。在MPDU解密之后,SN可与MPDU的该部分进行异或以恢复原始(未修改的MPDU)内容。然后,未修改的MPDU可被传递到重排序缓冲区并且稍后被处理以用于重放校验。在这种情况下,重放校验应当通过,因为具有修改的SN的重放的MPDU将不会在处理中到达该点(并且将在CRC校验未能通过之后被丢弃)。

[0091] 在一些情况下,如果被成功解密了并且通过了完整性校验的MPDU的重放校验未能通过,并且如果接收方STA维持部分状态,则接收方STA可不更新WinStartB值。在这种情况下,接收方STA可清除记分板上下文并且从重排序缓冲区清除用于该MPDU的条目。如果接收方STA维持完全状态,则接收方STA可不更新WinStartB和WinStartR的值。在这种情况下,接收方STA可清除该MPDU的记分板上下文,并且应当从重排序缓冲区清除该MPDU的条目。这一办法可涉及跟踪记分板上下文中的MPDU以及重排序缓冲区。

[0092] 本公开的各方面还可帮助解决发送器(发起方STA)接收未经索求的BA的场景。根据某些方面,发送器可被期望忽略意外到来的BA(例如,在接收到BA之前的SIFS没有从发送器索求MPDU)。以此方式忽略未经索求的BA可帮助避免发送器处的状态中断。

[0093] 示例操作

[0094] 图9是例示根据本公开的某些方面的用于无线通信的示例操作900的流程图。操作900可以是例如由第一无线设备(诸如无线站(STA))执行的。

[0095] 操作900在905处通过生成受保护帧而开始,该受保护帧指示:1)块确认(BA)窗口的更新的起始序列号(SSN),和2)该受保护帧的作为利用该更新的SSN来更新BA窗口的请求的预期目的。在910处,第一无线设备输出受保护帧,以供向该第一无线设备已与之建立受保护块确认(BA)协定的第二无线设备进行发送。在915处,第一无线站在所更新的BA窗口内生成具有SN的多个介质访问控制(MAC)协议数据单元(MPDU)。在920处,第一无线站输出多个MPDU以供向该第二无线设备进行发送。

[0096] 图10是例示根据本公开的某些方面的用于无线通信的示例操作1000的流程图。操作1000可例如由第二无线设备(例如,STA)来执行。

[0097] 操作1000在1005处通过从第二无线设备已与之建立受保护块确认(BA)协定的第一无线设备获得受保护帧而开始,该受保护帧指示:1)块确认(BA)窗口的更新的起始序列号(SSN),和2)该受保护帧的作为利用该更新的SSN来更新BA窗口的请求的预期目的。在1010处,第二无线设备维持位图以跟踪所更新的BA窗口内的已由第二无线设备成功获得的具有SN的介质访问控制(MAC)协议数据单元(MPDU)。

[0098] 图11是例示根据本公开的某些方面的用于无线通信的示例操作1100的流程图。操作1100可例如由无线设备(例如,STA)来执行。

[0099] 操作1100在1105处通过获得具有未能通过解密校验或完整性校验中的至少一者

的介质访问控制(MAC)协议数据单元(MPDU)的数据帧而开始。在1110处,响应于该失败,无线设备清除用于跟踪无线设备已经成功获得的MPDU的位图中的条目;或用于跟踪已由无线设备成功获得的MPDU的位图中的与接收到的MPDU相对应的条目。

[0100] 图12是例示根据本公开的某些方面的用于无线通信的示例操作1200的流程图。操作1200可例如由第一无线设备(例如,STA)来执行。

[0101] 操作1200在1205处通过生成具有使用应用于介质访问控制(MAC)协议数据单元(MPDU)的序列号(SN)的附加认证数据(AAD)来加密的MPDU的数据帧而开始。在1210处,第一无线设备输出数据帧,以供向该第一无线设备已与之建立受保护块确认(BA)协定的第二无线设备进行发送。

[0102] 图13是例示根据本公开的某些方面的用于无线通信的示例操作1300的流程图。操作1300可例如由第二无线设备(例如,STA)来执行。

[0103] 操作1300在1305处通过从第一无线设备获得第一无线设备已利用其建立受保护块确认(BA)协定的数据帧而开始。在1310处,第二无线设备使用介质访问控制(MAC)协议数据单元(MPDU)的序列号(SN)基于附加认证数据(AAD)解构来从该数据帧提取该MPDU。

[0104] 图14是例示根据本公开的某些方面的用于无线通信的示例操作1400的流程图。操作1400可例如由第一无线设备(例如,STA)来执行。

[0105] 操作1400在1405处通过对原始介质访问控制(MAC)协议数据单元(MPDU)的序列号(SN)执行操作来修改该MPDU以获得修改的MPDU而开始。在1410处,第一无线设备生成具有所修改的MPDU的加密版本的数据帧。在1415处,第一无线设备输出数据帧,以供向该第一无线设备已与之建立受保护块确认(BA)协定的第二无线设备进行发送。

[0106] 图15是例示根据本公开的某些方面的用于无线通信的示例操作1500的流程图。操作1500可例如由第二无线设备(例如,STA)来执行。

[0107] 操作1500在1505处通过从第二无线设备已与之建立受保护块确认(BA)协定的第一无线设备获得具有介质访问控制(MAC)协议数据单元(MPDU)的序列号(SN)修改版本的数据帧而开始。在1510处,第一无线设备基于该MPDU的修改版本来执行循环冗余校验(CRC)测试。在1515处,如果CRC测试通过,则第二无线设备对SN执行操作以在CRC测试通过的情况下从MPDU的修改版本恢复原始MPDU,并且更新BA位图以指示原始MPDU的成功接收。

[0108] 上述方法的各种操作可通过能够执行对应功能的任何合适的部件来执行。该部件可包括各种硬件或软件组件或模块,包括但不限于电路、专用集成电路(ASIC)或处理器。通常,在存在附图中例示的操作的情况下,那些操作可以具有相应的具有类似编号的对应部件加功能组件。

[0109] 示例设备

[0110] 图16例示了可包括能操作用于、被配置为或被适配成执行用于本文所公开的技术的操作(诸如图9至图15中例示的操作)的各种组件(诸如,对应于部件加功能组件)的通信设备1600。

[0111] 通信设备1600包括耦合到收发器1608(诸如发送器或接收器)的处理系统1602。收发器1608被配置为经由天线1610来发送和接收用于通信设备1600的信号,诸如本文中所述的各种信号。处理系统1602可被配置为执行用于通信设备1600的处理功能,包括处理由通信设备1600接收或将要发送的信号。

[0112] 处理系统1602包括经由总线1606耦合到计算机可读介质/存储器1612的处理器1604。在某些方面,计算机可读介质/存储器1612被配置为存储指令(诸如,计算机可执行代码),这些指令在由处理器1604执行时致使处理器1604执行图9至图15中例示的操作或者用于执行本文中所讨论的各种技术的其他操作。

[0113] 在某些方面,计算机可读介质/存储器1612存储用于输出的代码1614(诸如用于输出的部件的示例);用于获得的代码1615(诸如用于获得的部件的示例);用于维持的代码1616(诸如用于维持的部件的示例);用于生成的代码1617(诸如用于生成的部件的示例);用于提取的代码1618(诸如用于提取的部件的示例);和用于修改的代码1619(诸如用于修改的部件的示例)。

[0114] 在某些方面,处理器1604具有被配置为实现存储在计算机可读介质/存储器1612中的代码的电路。处理器1604包括用于输出的电路1624(诸如用于输出的部件的示例);用于获得的电路1625(诸如用于获得的部件的示例);用于生成的代码1626(诸如用于生成的部件的示例);用于提取的代码1627(诸如用于提取的部件的示例);和用于修改的电路1630(诸如用于修改的部件的示例)。

[0115] 收发器1608可提供用于接收信息(诸如分组、用户数据、或与各种信息信道(诸如控制信道、数据信道等)相关联的控制信息)的部件。信息可传递到设备1600的其他组件。收发器1608可以是参考图2描述的收发器254的各方面的示例。天线1610可对应于单个天线或一组天线。收发器1608可提供用于发送由设备1600的其他组件生成的信号的部件。

[0116] 在一些情况下,设备可具有用于输出帧以供发送的接口(用于输出的部件),而不是实际上发送帧。例如,处理器可经由总线接口将帧输出到射频(RF)前端以进行发送。类似地,设备可具有用于获得从另一设备接收的帧的接口(用于获得的部件),而不是实际上接收帧。例如,处理器可经由总线接口从用于接收的RF前端获得(或接收)帧。在一些情况下,用于输出帧以供发送的接口和用于获得帧的接口(在本文中可被称为第一接口和第二接口)可以是同一接口。

[0117] 用于建立的部件、用于维持的部件、用于生成的部件、用于提取的部件和/或用于修改的部件可包括图2或图16中示出的各种处理器和/或收发器中的任一者。

[0118] 示例方面

[0119] 在以下编号方面中描述了具体实施示例:

[0120] 方面1.一种用于在第一无线设备处进行的无线通信的方法,包括:生成受保护帧,所述受保护帧指示:1)块确认(BA)窗口的更新的起始序列号(SSN),和2)所述受保护帧的作为利用所述更新的SSN来更新BA窗口的请求的预期目的;输出所述受保护帧,以供向所述第一无线设备已与之建立受保护块确认(BA)协定的第二无线设备进行发送;在所更新的BA窗口内生成具有SN的多个介质访问控制(MAC)协议数据单元(MPDU);以及输出所述多个MPDU以供向所述第二无线设备进行发送。

[0121] 方面2.根据方面1所述的方法,还包括:输出指示BA请求的MPDU以供向所述第二无线设备进行发送;以及响应于所述请求而从所述第二无线设备获得BA,所述BA指示在所更新的BA窗口内的所述MPDU中的哪些MPDU是由所述第二无线设备成功接收的。

[0122] 方面3.根据方面1至2中任一项所述的方法,其中所述受保护帧包括被设计用于更新所述BA窗口的BA动作帧。

[0123] 方面4.根据方面3所述的方法,其中所述受保护帧经由所述受保护帧的类别字段或BA动作字段中的至少一者来指示所述预期目的。

[0124] 方面5.根据方面1至4中任一项所述的方法,还包括:从所述第二无线通信设备获得对所述受保护帧的确认。

[0125] 方面6.根据方面1至5中任一项所述的方法,其中所述受保护帧包括添加BA(ADDBA)请求帧。

[0126] 方面7.根据方面6所述的方法,其中所述受保护帧包括被设置为某个值以指示预期目的的字段。

[0127] 方面8.根据方面7所述的方法,其中所述字段位于所述ADDBA请求帧的帧报头中。

[0128] 方面9.一种用于在第二无线设备处进行的无线通信的方法,包括:从所述第二无线设备已与之建立受保护块确认(BA)协定的第一无线设备获得受保护帧,所述受保护帧指示:1)块确认(BA)窗口的更新的起始序列号(SSN),和2)所述受保护帧的作为利用所述更新的SSN来更新BA窗口的请求的预期目的;以及维持位图以跟踪所更新的BA窗口内的已由所述第二无线设备成功获得的具有SN的介质访问控制(MAC)协议数据单元(MPDU)。

[0129] 方面10.根据方面9所述的方法,还包括:从所述第一无线设备获得BA请求;以及输出指示BA的MPDU以供向所述第一无线设备进行发送,所述BA指示所更新的BA窗口内的所述MPDU中的哪些MPDU是由所述第二无线设备根据所述位图成功获得的。

[0130] 方面11.根据方面9至10中任一项所述的方法,其中所述受保护帧包括被设计用于更新所述BA窗口的BA动作帧。

[0131] 方面12.根据方面11所述的方法,其中所述受保护帧经由所述受保护帧的类别字段或BA动作字段中的至少一者来指示所述预期目的。

[0132] 方面13.根据方面9至12中任一项所述的方法,还包括:输出对所述受保护帧的确认,以供向所述第一无线设备进行发送。

[0133] 方面14.根据方面9至13中任一项所述的方法,其中所述受保护帧包括添加BA(ADDBA)请求帧。

[0134] 方面15.根据方面14所述的方法,其中所述受保护请求帧包括被设置为某个值以指示预期目的的字段。

[0135] 方面16.根据方面15所述的方法,其中所述字段位于所述ADDBA请求帧的帧报头中。

[0136] 方面17.一种用于无线设备处的无线通信的方法,包括:获得具有未能通过解密校验或完整性校验中的至少一者的介质访问控制(MAC)协议数据单元(MPDU)的数据帧;以及响应于所述失败而清除:用于跟踪已由所述无线设备成功获得的MPDU的位图中的条目;或用于跟踪已由所述无线设备成功获得的MPDU的所述位图中的与接收到的MPDU相对应的条目。

[0137] 方面18.根据方面17所述的方法,还包括:维持部分状态信息,其中针对特定业务ID(TID)的位图仅被维持达有限时间量。当前发送机会(TXOP)。

[0138] 方面19.根据方面17至18中任一项所述的方法,还包括:维持完全状态信息,其中用于针对不同业务类型的位图被维持直到相关联的块确认(BA)会话结束;所述位图用于与未能通过解密校验或完整性校验中的至少一者的MPDU相对应的会话;所述清除包括清除所

述位图。

[0139] 方面20.根据方面19所述的方法,其中在清除所述位图之后,所述无线设备维持表示所述位图中的最低序列号定位的参数的当前值。

[0140] 方面21.一种用于在第一无线设备处进行的无线通信的方法,包括:通过对原始介质访问控制(MAC)协议数据单元(MPDU)的序列号(SN)执行操作来修改所述MPDU以获得修改的MPDU;生成具有所修改的MPDU的加密版本的数据帧;以及输出所述数据帧,以供向所述第一无线设备已与之建立受保护块确认(BA)协定的第二无线设备进行发送。

[0141] 方面22.根据方面21所述的方法,其中通过对所述SN执行操作来修改所述原始MPDU包括:对所述原始MPDU的一部分和所述SN执行逻辑操作。

[0142] 方面23.根据方面21至22中任一项所述的方法,其中所述数据帧包括基于所修改的MPDU的所述加密版本和MAC报头生成的循环冗余校验(CRC)值。

[0143] 方面24.一种用于在第二无线设备处进行的无线通信的方法,包括:从第二无线设备已与之建立受保护块确认(BA)协定的第一无线设备获得具有介质访问控制(MAC)协议数据单元(MPDU)的修改版本的序列号(SN)的数据帧;基于所述MPDU的修改版本来执行循环冗余校验(CRC)测试;以及如果所述CRC测试通过,则对所述SN执行操作以在所述CRC测试通过的情况下从所述MPDU的所述修改版本恢复原始MPDU;以及更新BA位图以指示对所述原始MPDU的成功接收。

[0144] 方面25.根据方面24所述的方法,其中对所述SN执行操作以恢复所述原始MPDU包括:对所述MPDU的所述修改版本的一部分和所述SN执行逻辑操作。

[0145] 方面26.根据方面24至25中任一项所述的方法,还包括:如果CRC测试通过,则将所述MPDU的所述原始版本传递到重排序缓冲区。

[0146] 方面27.一种用于在第一无线设备处进行的无线通信的方法,包括:生成具有使用应用于介质访问控制(MAC)协议数据单元(MPDU)的序列号(SN)的附加认证数据(AAD)来加密的MPDU的数据帧;以及输出所述数据帧,以供向所述第一无线设备已与之建立受保护块确认(BA)协定的第二无线设备进行发送。

[0147] 方面28.一种用于在第二无线设备处进行的无线通信的方法,包括:从第一无线设备获得所述第一无线设备已利用其建立受保护块确认(BA)协定的数据帧;以及使用所述介质访问控制(MAC)协议数据单元(MPDU)的序列号(SN)基于附加认证数据(AAD)解构来从所述数据帧提取所述MPDU。

[0148] 方面29.一种用于在第一无线设备处进行的无线通信的方法,包括:从第二无线设备获得未经索求的块确认(BA)帧;以及忽略所述未经索求的BA帧。

[0149] 方面30.根据方面29所述的方法,其中所述未经索求的BA帧是独立于所述第一无线设备在获得所述未经索求的BA帧之前的短帧间空间(SIFS)输出索求帧以供发送而获得的。

[0150] 方面31.一种用于进行无线通信的装置,包括:存储器,所述存储器包括指令;和一个或多个处理器,所述一个或多个处理器被配置为执行所述指令并且使所述装置执行根据方面1至30中任一项所述的方法。

[0151] 方面32.一种用于无线通信的装置,包括:用于执行根据方面1至30中任一项所述的方法的部件。

[0152] 方面33.一种非暂态计算机可读介质,包括:指令,所述指令在由装置执行时使所述装置执行根据方面1至30中任一项所述的方法。

[0153] 方面34.一种无线设备,包括:至少一个收发器;存储器,所述存储器包括指令;和一个或多个处理器,所述一个或多个处理器被配置为执行所述指令并且使所述无线设备执行根据方面1至8中任一项所述的方法,其中所述至少一个收发器被配置为发送所述受保护帧和所述多个MPDU。

[0154] 方面35.一种无线设备,包括:至少一个收发器;存储器,所述存储器包括指令;和一个或多个处理器,所述一个或多个处理器被配置为执行所述指令并且使所述无线设备执行根据方面9至16中任一项所述的方法,其中所述至少一个收发器被配置为接收所述受保护帧。

[0155] 方面36.一种无线设备,包括:至少一个收发器;存储器,所述存储器包括指令;和一个或多个处理器,所述一个或多个处理器被配置为执行所述指令并且使所述无线设备执行根据方面17至20中任一项所述的方法,其中所述至少一个收发器被配置为接收所述数据帧。

[0156] 方面37.一种无线设备,包括:至少一个收发器;存储器,所述存储器包括指令;和一个或多个处理器,所述一个或多个处理器被配置为执行所述指令并且使所述无线设备执行根据方面21至23中任一项所述的方法,其中所述至少一个收发器被配置为发送所述数据帧。

[0157] 方面38:一种无线设备,包括:至少一个收发器;存储器,所述存储器包括指令;和一个或多个处理器,所述一个或多个处理器被配置为执行所述指令并且使所述无线设备执行根据方面24至26中任一项所述的方法,其中所述至少一个收发器被配置为接收所述数据帧。

[0158] 方面39.一种无线设备,包括:至少一个收发器;存储器,所述存储器包括指令;和一个或多个处理器,所述一个或多个处理器被配置为执行所述指令并且使所述无线设备执行根据方面27中任一项所述的方法,其中所述至少一个收发器被配置为发送所述数据帧。

[0159] 方面40.一种无线设备,包括:至少一个收发器;存储器,所述存储器包括指令;和一个或多个处理器,所述一个或多个处理器被配置为执行所述指令并且使所述无线设备执行根据方面28中任一项所述的方法,其中所述至少一个收发器被配置为接收所述数据帧。

[0160] 方面41.一种无线设备,包括:至少一个收发器;存储器,所述存储器包括指令;和一个或多个处理器,所述一个或多个处理器被配置为执行所述指令并且使所述无线设备执行根据方面29中任一项所述的方法,其中所述至少一个收发器被配置为接收所述未经索求的BA帧。

[0161] 附加注意事项

[0162] 如本文所用,术语"确定"涵盖各种各样的动作。例如,"确定"可包括计算、运算、处理、导出、调查、查找(诸如,在表、数据库或另一数据结构中查找)、断定等。另外,"确定"可包括接收(诸如接收信息)、访问(诸如访问存储器中的数据)和类似动作。另外,"确定"可包括解析、选择、挑选、建立等。

[0163] 如本文所用,提到项目列表"中的至少一者"的短语,指代这些项目的任何组合(其包括单一成员)。作为一个示例,"a、b或c中的至少一者"旨在涵盖:a、b、c、a′b、a-c、b—c和

a′b-c。

[0164] 结合本文所公开的具体实施描述的各种例示性逻辑部件、逻辑块、模块、电路和算法过程可以被实现为电子硬件、计算机软件或两者的组合。硬件和软件的可互换性已在功能性方面大致进行了描述,并且在上文所述的各种例示性组件、块、模块、电路和过程中例示。这种功能性是以硬件还是软件来实现取决于特定应用和加诸于整体系统的设计约束。

[0165] 可利用被设计为执行本文所描述的功能的通用单芯片或者多芯片处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其他可编程逻辑器件、分立门或者晶体管逻辑组件、分立硬件组件或者它们的任何组合来实现或执行用于实现结合本文所公开的各方面描述的各种例示性逻辑部件、逻辑块、模块和电路的硬件和数据处理装置。通用处理器可以是微处理器,或者,任何常规的处理器、控制器、微控制器或者状态机。处理器也可被实现为计算设备的组合,例如,DSP和微处理器的组合、多个微处理器、与DSP内核结合的一个或多个微处理器,或任何其他此类配置。在一些具体实施中,可以由特定于给定功能的电路来执行特定过程和方法。

[0166] 在一个或多个方面,所描述的功能可在硬件、数字电子电路、计算机软件、固件、包括本说明书中公开的结构和其结构等效物或在其任意组合中来实现。本说明书中描述的主题的具体实施还可实现为一个或多个计算机程序,即计算机程序指令的一个或多个模块,该一个或多个模块被编码在计算机存储介质上以用于由数据处理装置执行或控制数据处理装置的操作。

[0167] 如果以软件实现,则功能可以作为一个或多个指令或代码存储在计算机可读介质上或者通过计算机可读介质发送。本文所公开的方法或算法的过程可在可驻留在计算机可读介质上的处理器可执行软件模块中实现。计算机可读介质包括计算机存储介质和通信介质两者,通信介质包括能够实现将计算机程序从一个地方传递到另一个地方的任何介质。存储介质可以是计算机能够访问的任何可用介质。通过示例而非限制的方式,此类计算机可读介质可包括RAM、ROM、EEPROM、CD-ROM或其他光盘存储装置、磁盘存储装置或其他磁存储设备、或者可用于存储呈指令或数据结构形式的期望程序代码并且可由计算机存取的任何其他介质。此外,可将任何连接恰当地称作计算机可读介质。如本文中所使用的磁盘和光盘包括压缩光盘(CD)、激光盘、光盘、数字通用光盘(DVD)、软盘和蓝光盘,其中磁盘通常磁性复制数据,而光盘用激光光学复制数据。上述的组合应也被包括在计算机可读介质的范围内。附加地,方法或算法的操作可作为一个代码和指令集或者代码和指令集的任何组合,驻留在机器可读介质和计算机可读介质上,该机器可读介质和计算机可读介质可结合到计算机程序产品中。

[0168] 对本公开中描述的具体实施的各种修改对于本领域技术人员将是显而易见的,以及在不脱离本公开的精神或范围的情况下,本文所定义的通用原则可被应用到其他具体实施。因此,权利要求不旨在受限于本文示出的具体实施,而是要符合与本公开、本文所公开的原理和新颖性特征相一致的最广范围。

[0169] 在本说明书中描述的在单个具体实施的上下文中的某些特征还可在单个具体实施中组合地实现。相反地,在单个具体实施的上下文中描述的各个特征还可以在多个具体实施中单独地或者以任何适当的子组合来实现。此外,虽然上文将一些特征描述成以特定组合来工作并且甚至最初是如此要求保护的,但在一些情况下,可将来自所要求保护的组

合中的一个或多个特征从该组合中切割出来,并且所要求保护的组合可涉及子组合或者子组合的变型。

[0170] 类似地,虽然在图中以特定的次序描绘了操作,但是这并不应当被理解为要求此类操作以所示出的特定次序或者以顺序次序来执行,或者执行所有例示的操作来实现期望的结果。此外,附图可以流程图的形式示意性地描绘了一个或多个示例过程。然而,可在示意性地例示的示例过程中并入没有描绘的其他操作。例如,一个或多个附加操作可在所例示的操作中的任何操作之前、之后、同时或者在其之间执行。在某些环境下,多任务处理和并行处理可以是有利的。此外,在上文描述的具体实施中的各个系统组件的分离不应当被理解为在所有具体实施中都要求这样的分离,而是其应当被理解为所描述的程序组件和系统通常能够一起被整合在单个软件产品中,或者被封装到多个软件产品中。除此之外,其他具体实施在下面的权利要求的范围内。在一些情况下,权利要求中所记载的动作可按不同的顺序来执行并且仍然实现期望的结果。

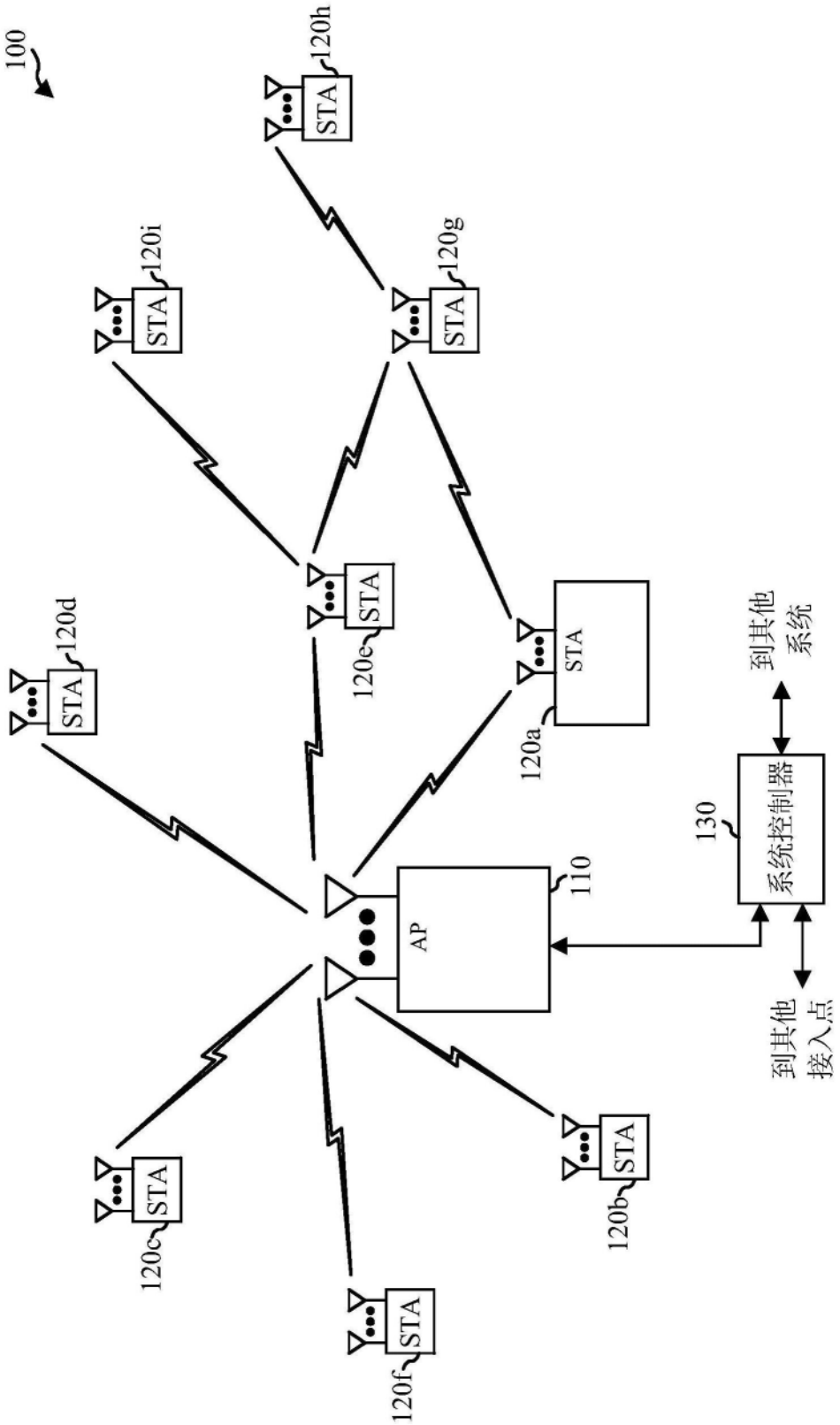

100
STA
120h
STA
120i
STA
120g
STA
120e
STA
120d
STA
120a
到其他
系统
130
系统控制器
AP
110
到其他
接入点
STA
120c
STA
120f
STA
120b

图1

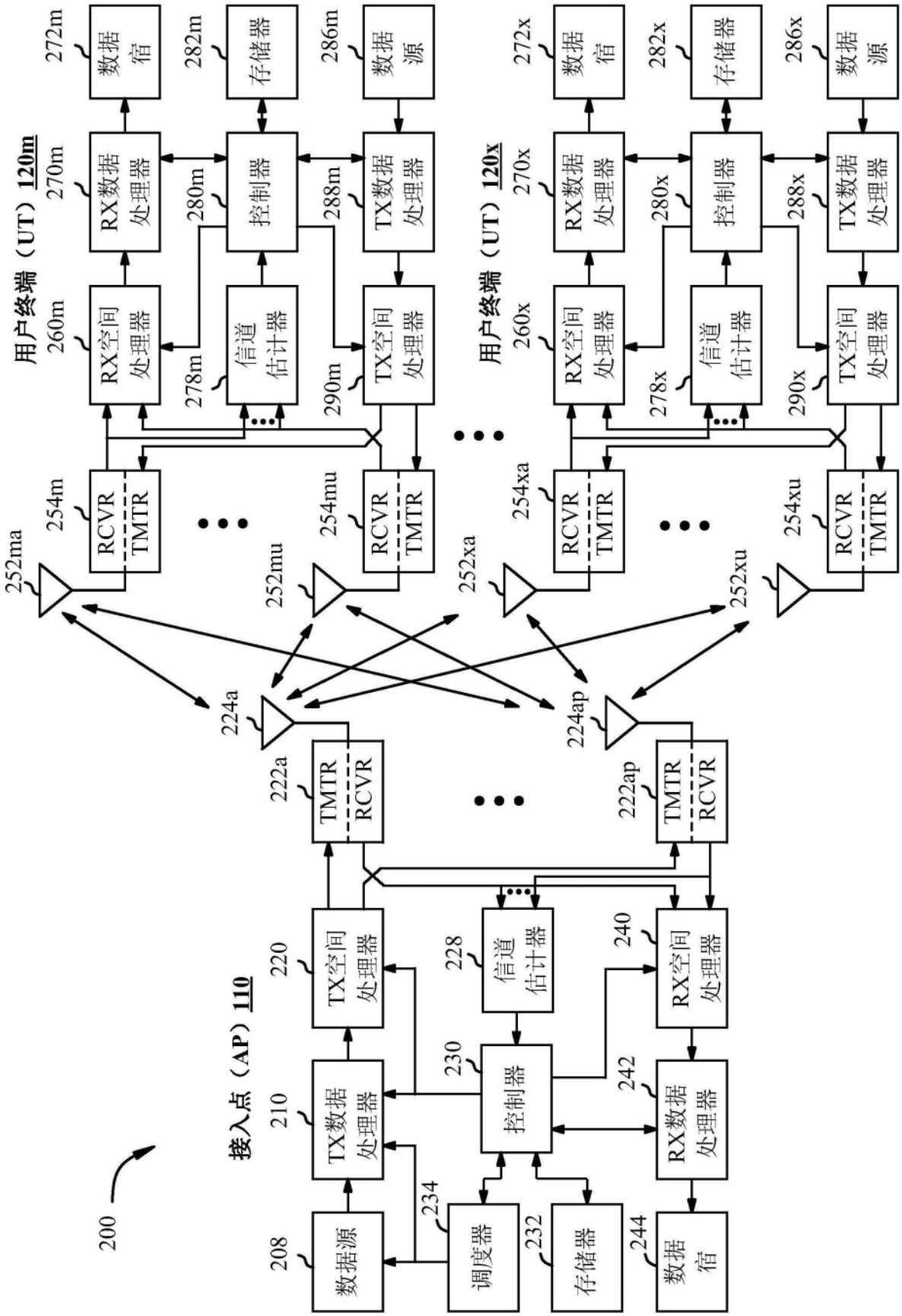

200
接入点（AP）110
208
数据源
210
TX数据处理器
220
TX空间处理器
222a
TMTR
RCVR
224a
252ma
254m
RCVR
TMTR
260m
RX空间处理器
270m
RX数据处理器
272m
数据宿
278m
信道估计器
280m
控制器
282m
存储器
288m
TX数据处理器
286m
数据源
290m
TX空间处理器
254mu
252mu
用户终端（UT）120m
222ap
224ap
252xa
254xa
260x
270x
272x
278x
280x
282x
288x
286x
290x
252xu
254xu
用户终端（UT）120x
228
信道估计器
230
控制器
232
存储器
234
调度器
240
RX空间处理器
242
RX数据处理器
244
数据宿

图2

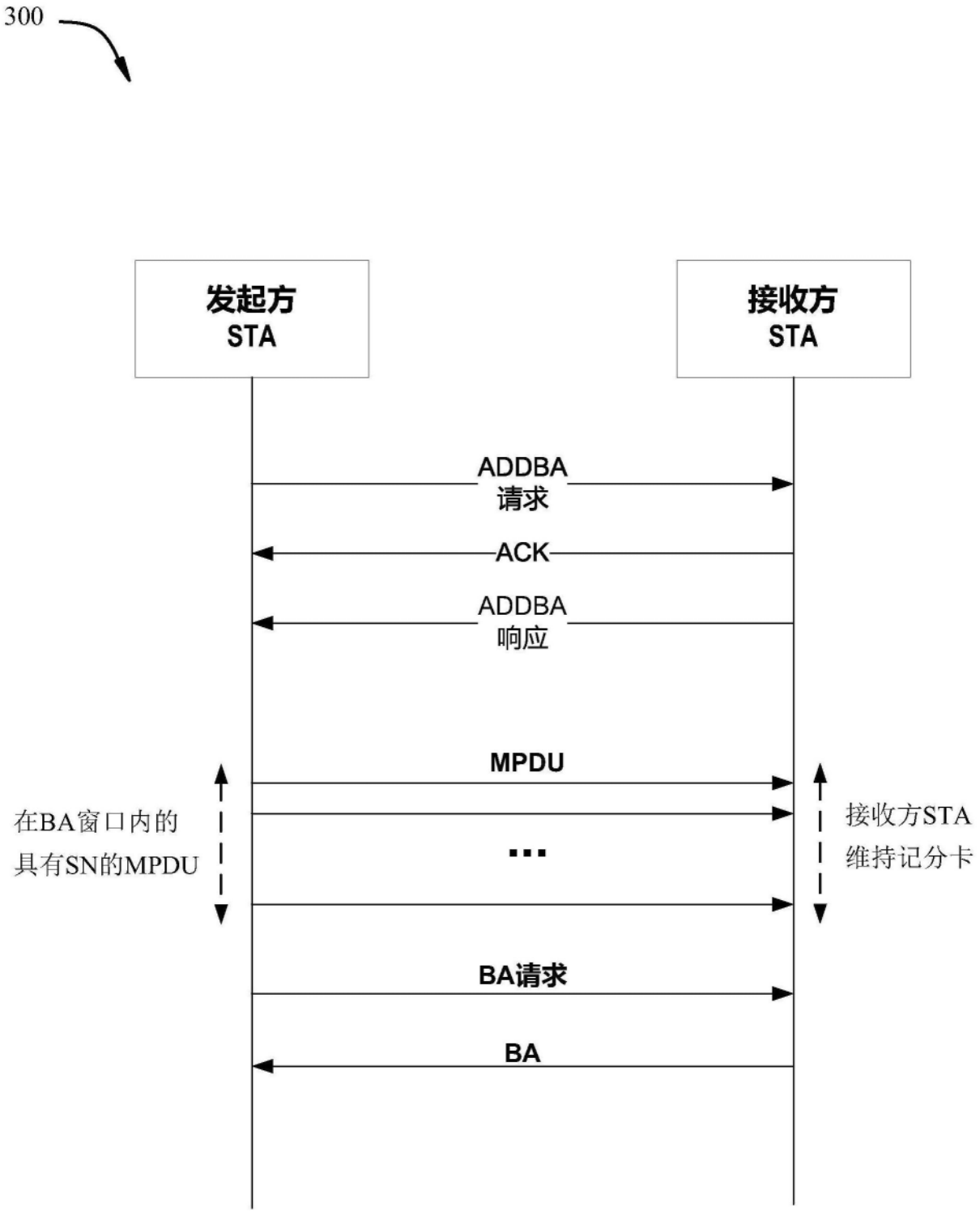

300
发起方
STA
接收方
STA
ADDBA
请求
ACK
ADDBA
响应
MPDU
在BA窗口内的
具有SN的MPDU
...
接收方STA
维持记分卡
BA请求
BA

图3

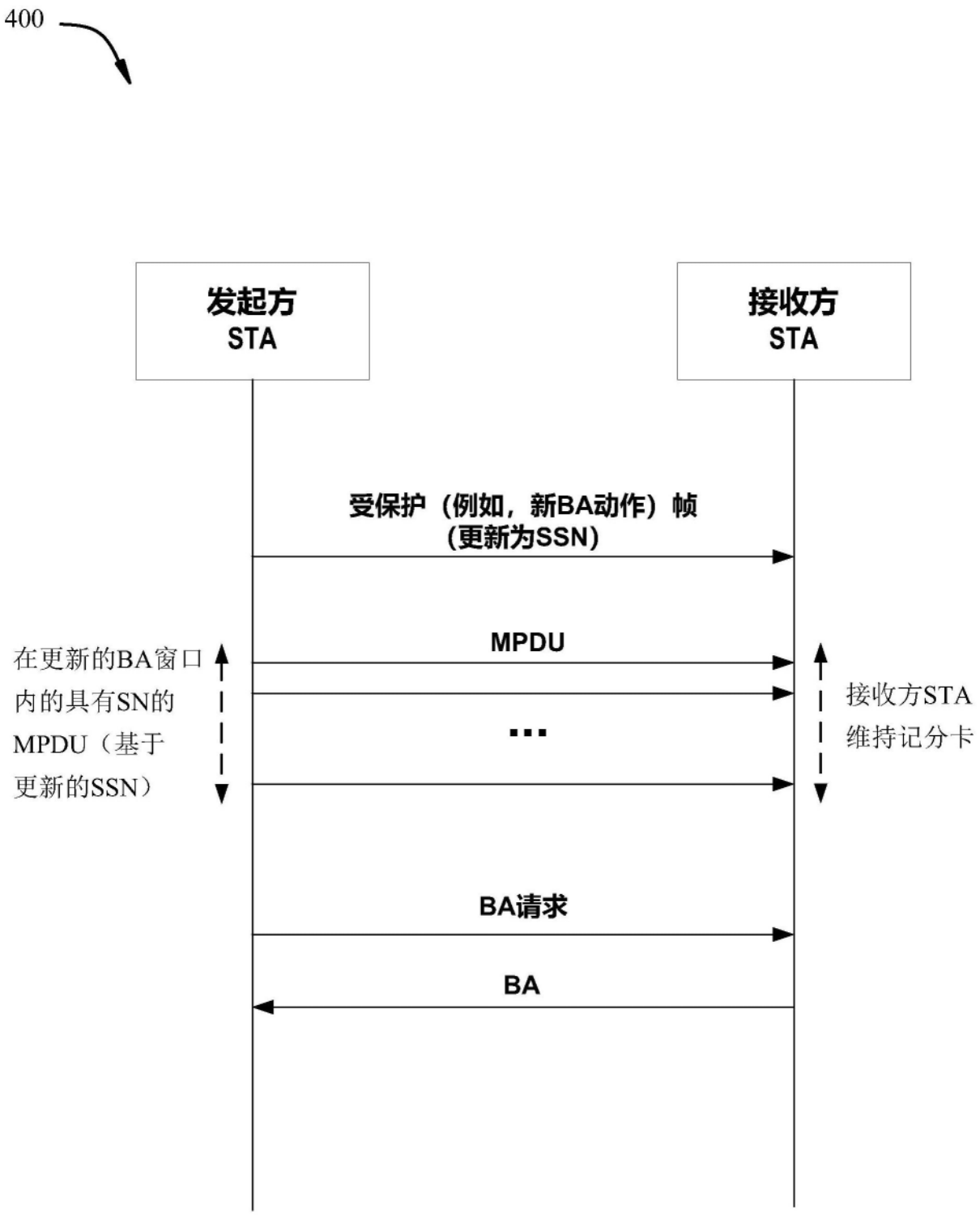

400
发起方
STA
接收方
STA
受保护（例如，新BA动作）帧
（更新为SSN）
MPDU
在更新的BA窗口
内的具有SN的
MPDU（基于
更新的SSN）
...
接收方STA
维持记分卡
BA请求
BA

图4

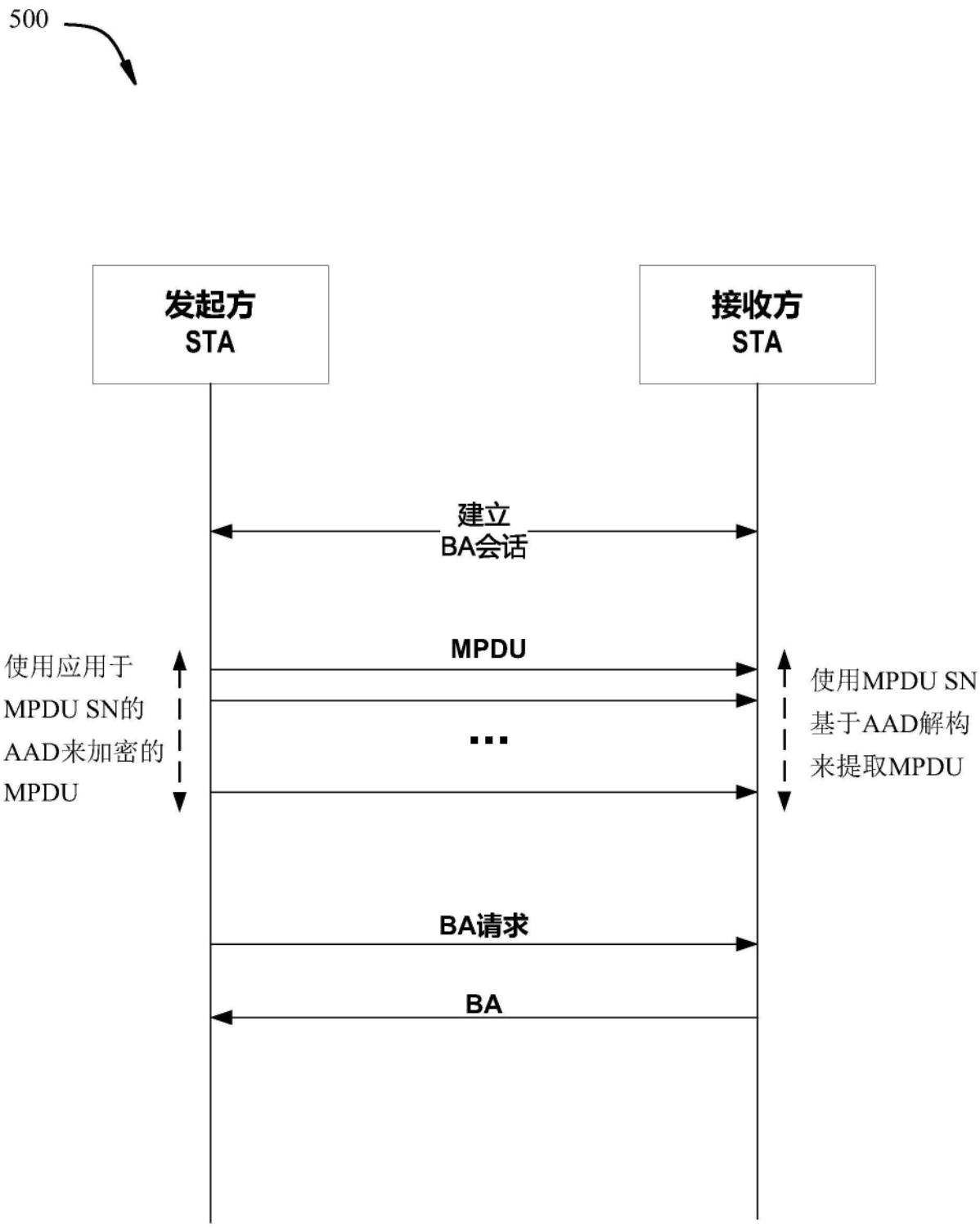

500
发起方
STA
接收方
STA
建立
BA会话
MPDU
使用应用于
MPDU SN的
AAD来加密的
MPDU
使用MPDU SN
基于AAD解构
来提取MPDU
BA请求
BA

图5

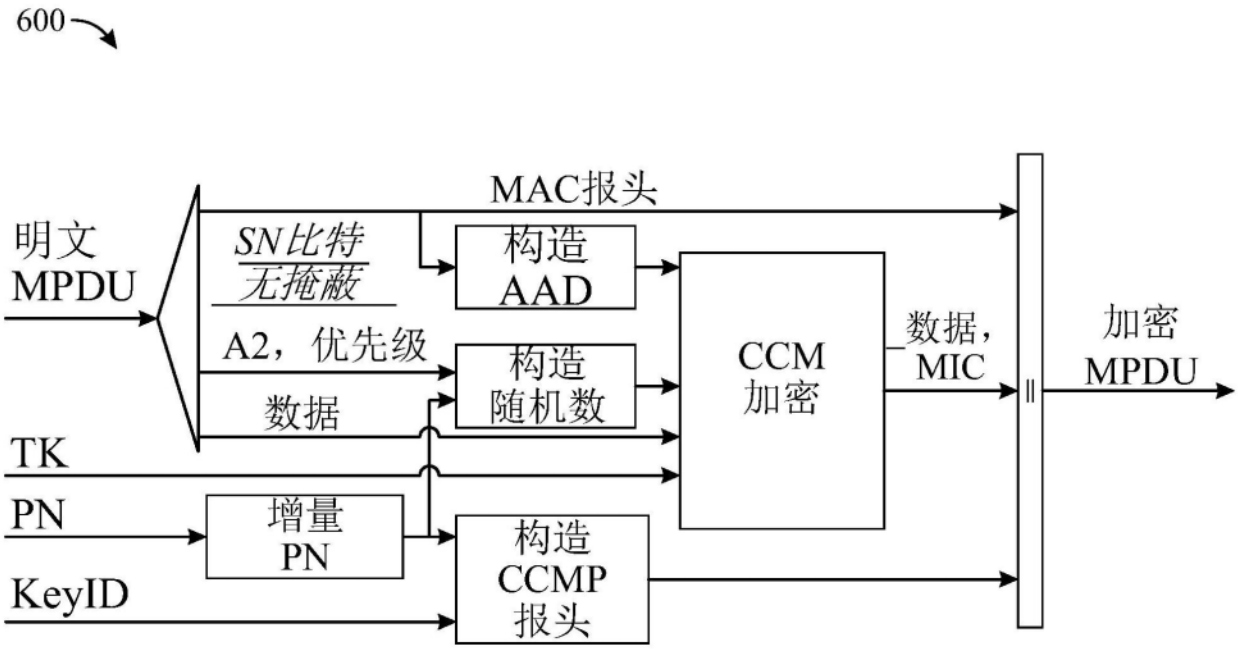

600
明文
MPDU
SN比特
无掩蔽
A2，优先级
数据
TK
PN
KeyID
增量
PN
MAC报头
构造
AAD
构造
随机数
构造
CCMP
报头
CCM
加密
数据，
MIC
加密
MPDU

图6A


650
FC
A1
A2
A3
SC
A4
QC
八位位组：
2
6
6
6
2
6
2
具有序列号子字段的SC-MPDU序列控制字段在
AAD构造时可不被掩蔽

图6B

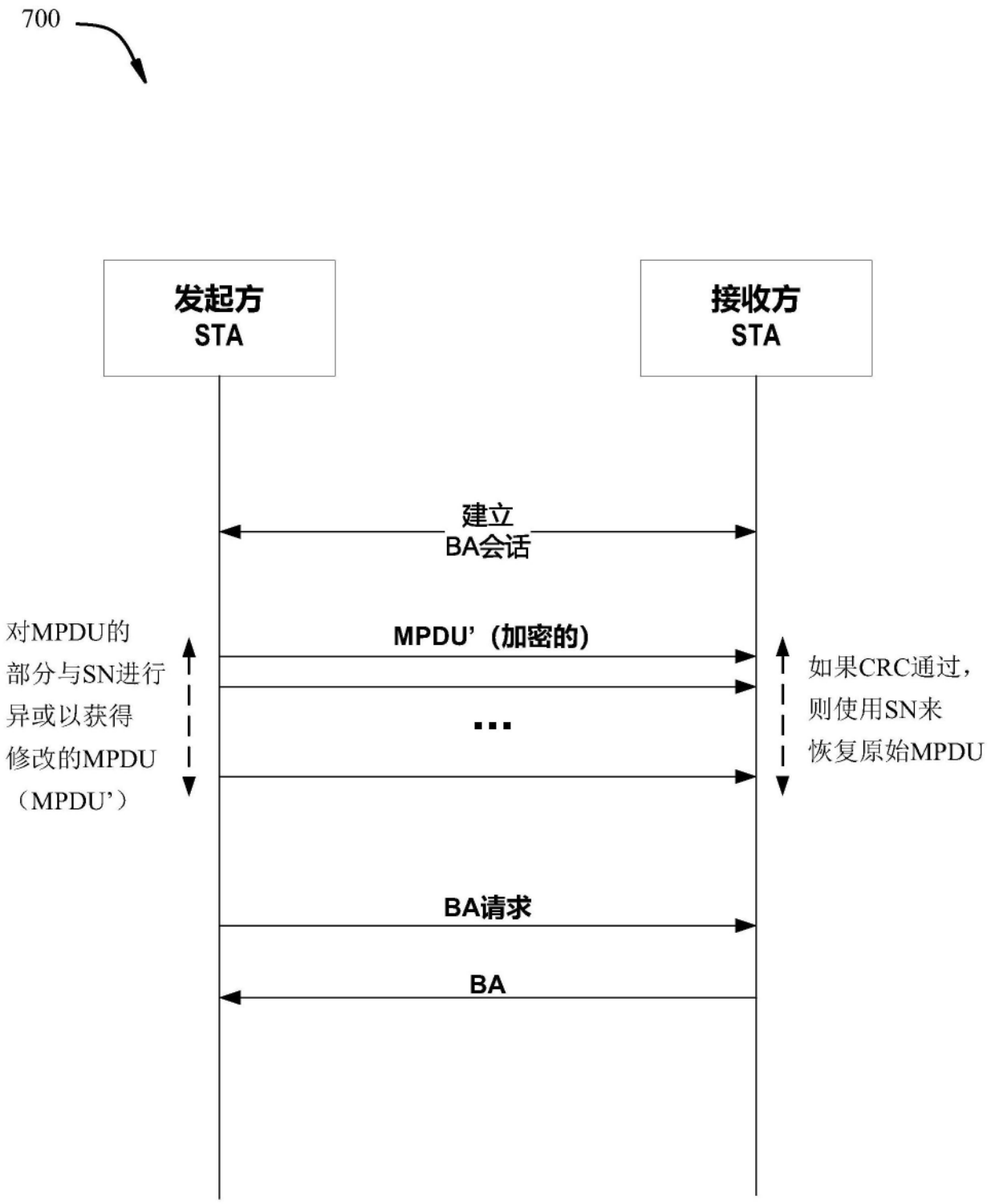

700
发起方
STA
接收方
STA
建立
BA会话
对MPDU的
部分与SN进行
异或以获得
修改的MPDU
（MPDU’）
MPDU’（加密的）
...
如果CRC通过，
则使用SN来
恢复原始MPDU
BA请求
BA

图7

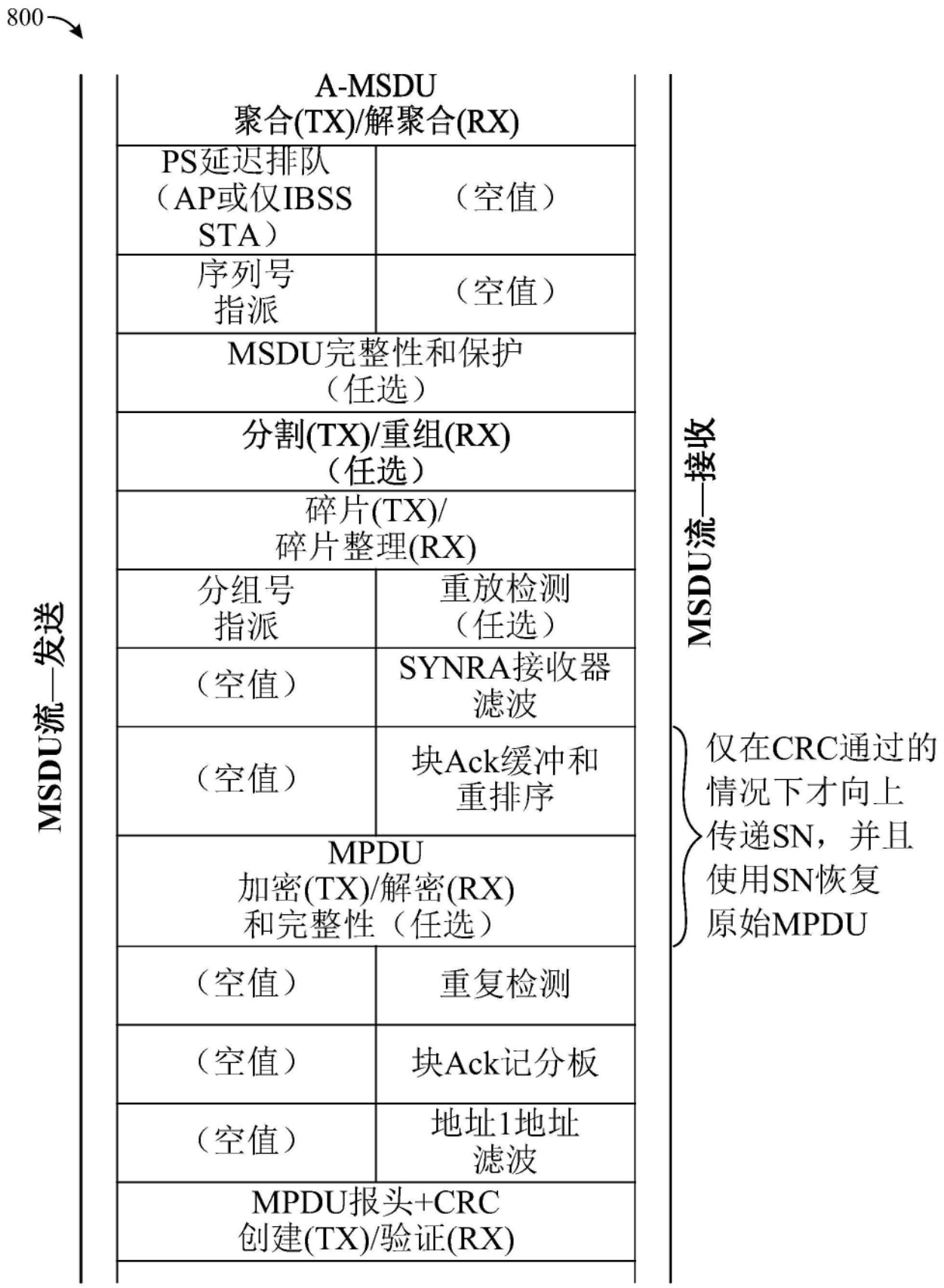

800
MSDU流—发送
MSDU流—接收
A-MSDU
聚合(TX)/解聚合(RX)
PS延迟排队（AP或仅IBSS STA）
（空值）
序列号指派
（空值）
MSDU完整性和保护（任选）
分割(TX)/重组(RX)（任选）
碎片(TX)/碎片整理(RX)
分组号指派
重放检测（任选）
（空值）
SYNRA接收器滤波
（空值）
块Ack缓冲和重排序
仅在CRC通过的情况下才向上传递SN，并且使用SN恢复原始MPDU
MPDU加密(TX)/解密(RX)和完整性（任选）
（空值）
重复检测
（空值）
块Ack记分板
（空值）
地址1地址滤波
MPDU报头+CRC创建(TX)/验证(RX)

图8

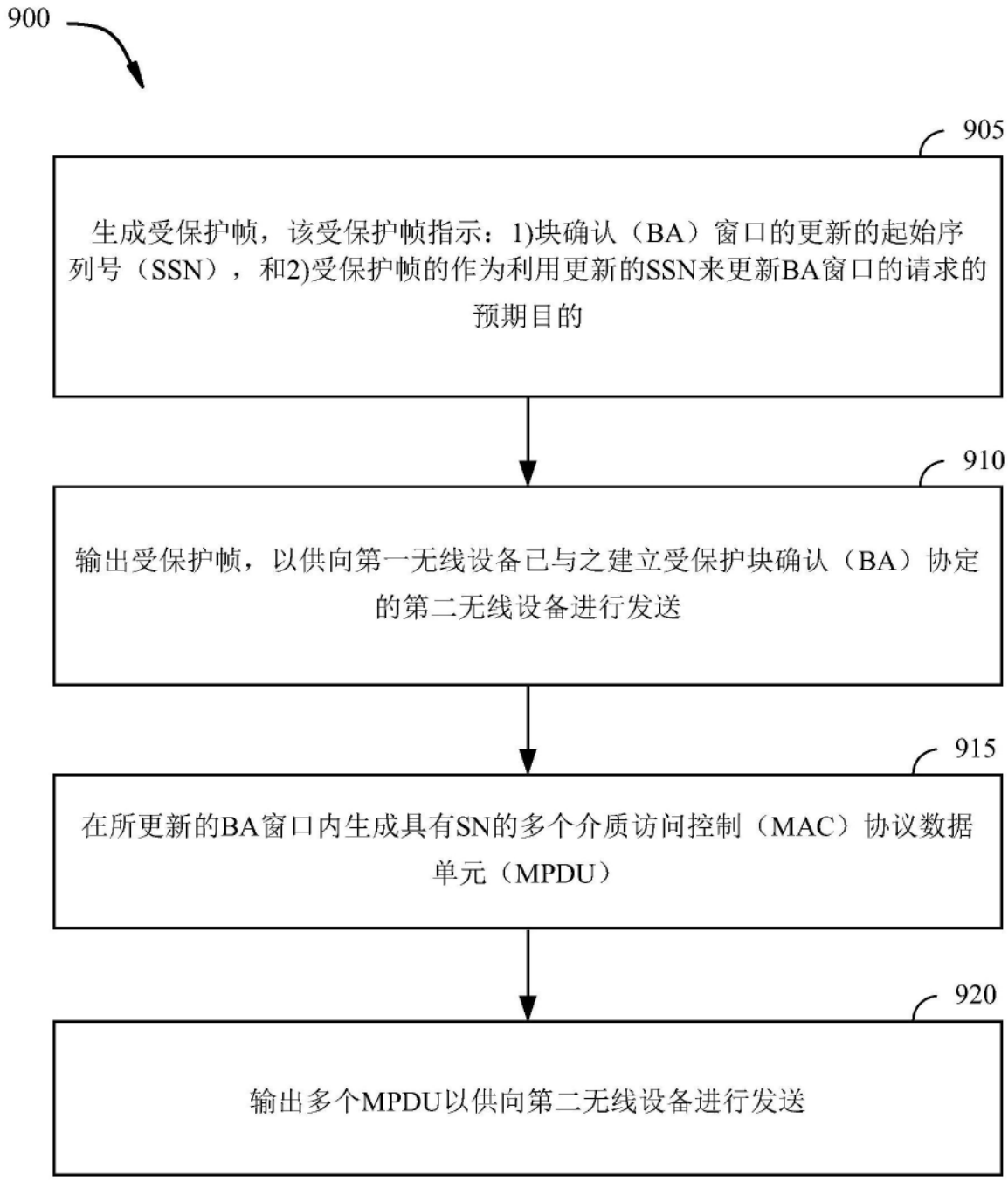

900
905
生成受保护帧，该受保护帧指示：1)块确认（BA）窗口的更新的起始序列号（SSN），和2)受保护帧的作为利用更新的SSN来更新BA窗口的请求的预期目的
910
输出受保护帧，以供向第一无线设备已与之建立受保护块确认（BA）协定的第二无线设备进行发送
915
在所更新的BA窗口内生成具有SN的多个介质访问控制（MAC）协议数据单元（MPDU）
920
输出多个MPDU以供向第二无线设备进行发送

图9

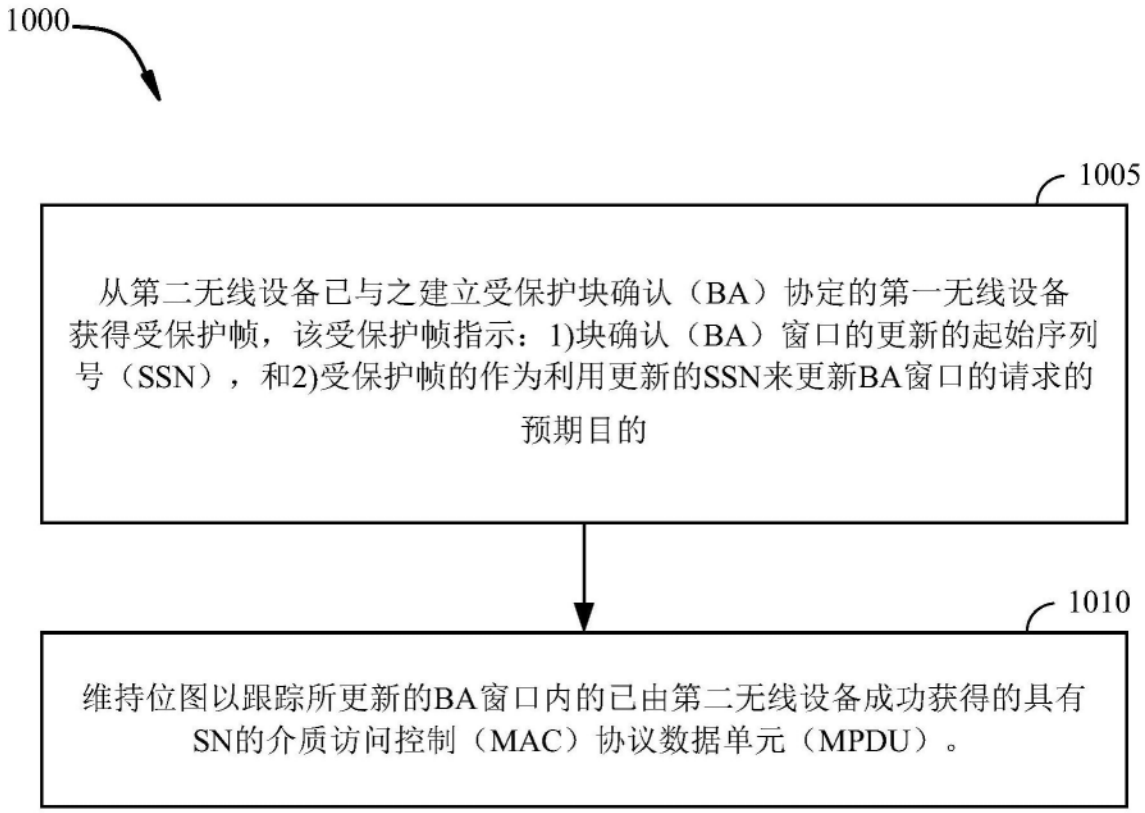

1000
1005
从第二无线设备已与之建立受保护块确认（BA）协定的第一无线设备获得受保护帧，该受保护帧指示：1)块确认（BA）窗口的更新的起始序列号（SSN），和2)受保护帧的作为利用更新的SSN来更新BA窗口的请求的预期目的
1010
维持位图以跟踪所更新的BA窗口内的已由第二无线设备成功获得的具有SN的介质访问控制（MAC）协议数据单元（MPDU）。

图10

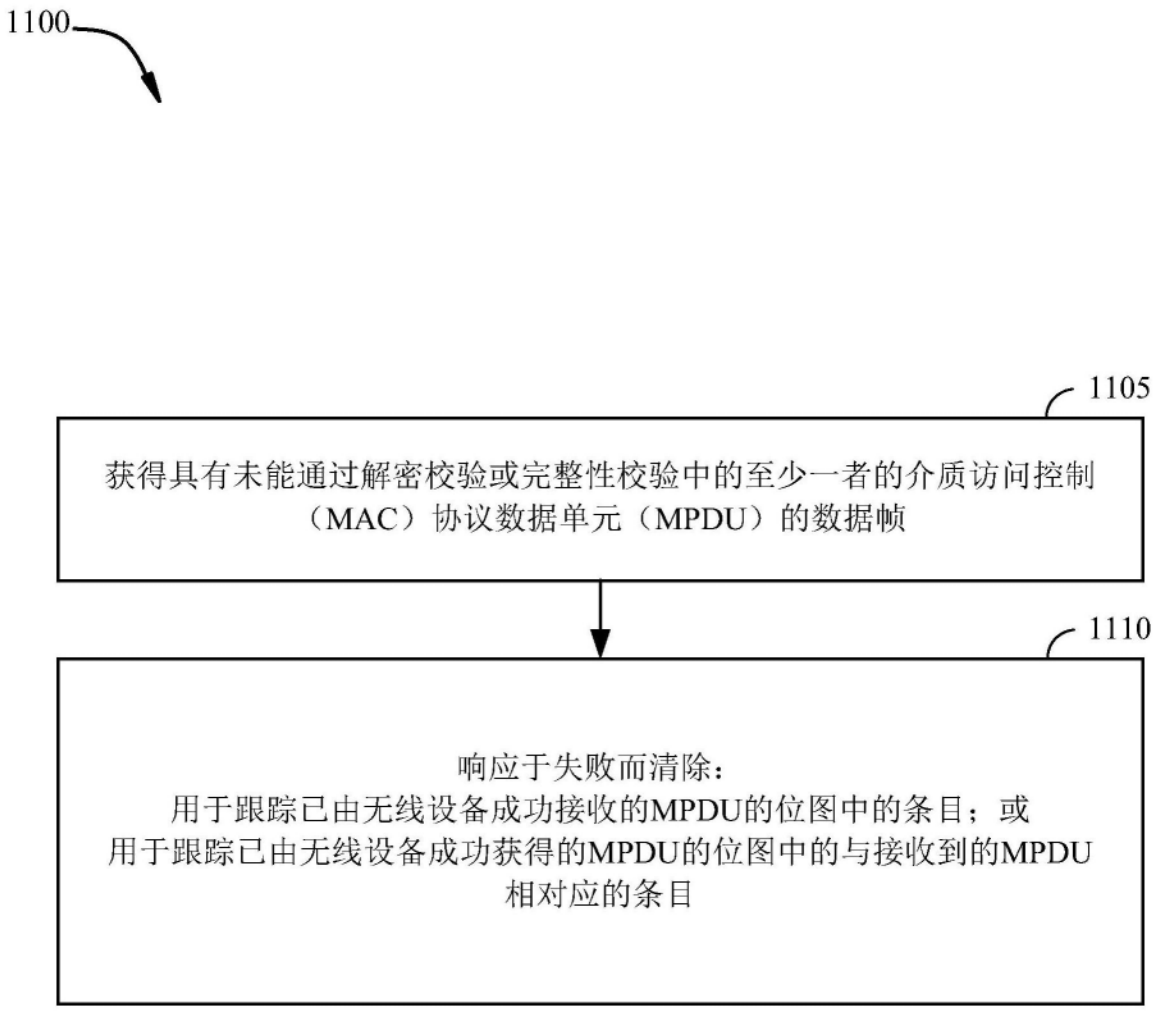

1100
1105
获得具有未能通过解密校验或完整性校验中的至少一者的介质访问控制（MAC）协议数据单元（MPDU）的数据帧
1110
响应于失败而清除：
用于跟踪已由无线设备成功接收的MPDU的位图中的条目；或
用于跟踪已由无线设备成功获得的MPDU的位图中的与接收到的MPDU相对应的条目

图11

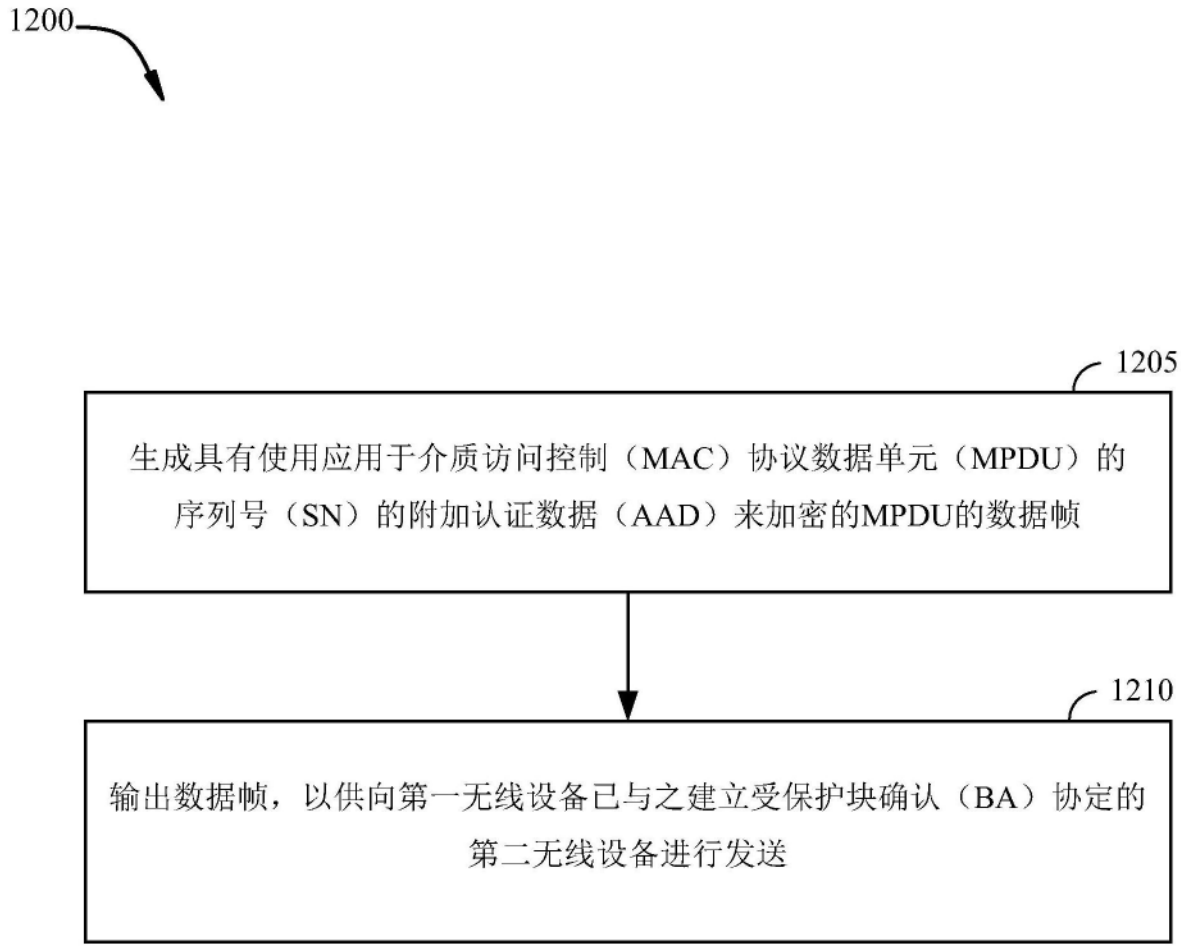

1200
1205
生成具有使用应用于介质访问控制（MAC）协议数据单元（MPDU）的序列号（SN）的附加认证数据（AAD）来加密的MPDU的数据帧
1210
输出数据帧，以供向第一无线设备已与之建立受保护块确认（BA）协定的第二无线设备进行发送

图12

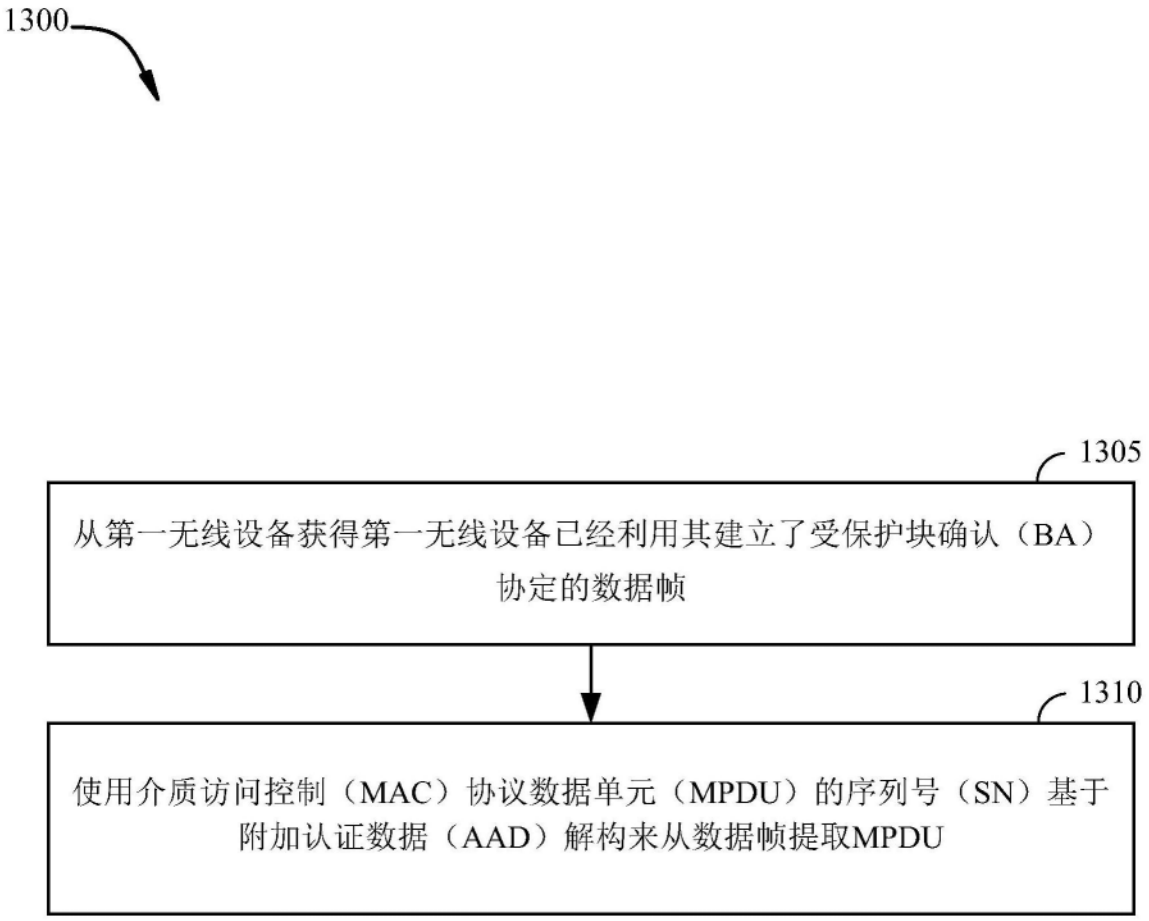

1300
1305
从第一无线设备获得第一无线设备已经利用其建立了受保护块确认（BA）协定的数据帧
1310
使用介质访问控制（MAC）协议数据单元（MPDU）的序列号（SN）基于附加认证数据（AAD）解构来从数据帧提取MPDU

图13

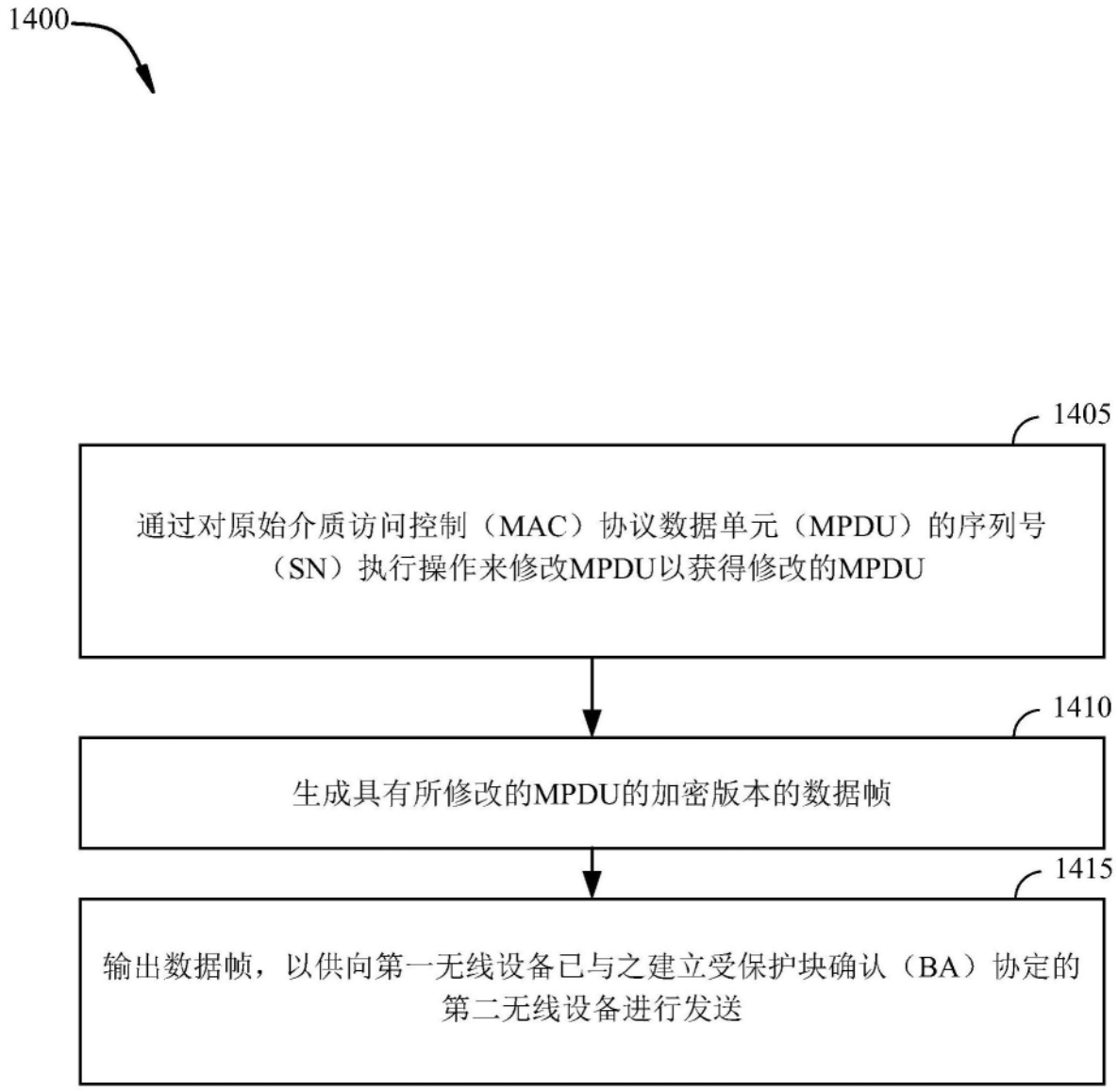

1400
1405
通过对原始介质访问控制（MAC）协议数据单元（MPDU）的序列号（SN）执行操作来修改MPDU以获得修改的MPDU
1410
生成具有所修改的MPDU的加密版本的数据帧
1415
输出数据帧，以供向第一无线设备已与之建立受保护块确认（BA）协定的第二无线设备进行发送

图14

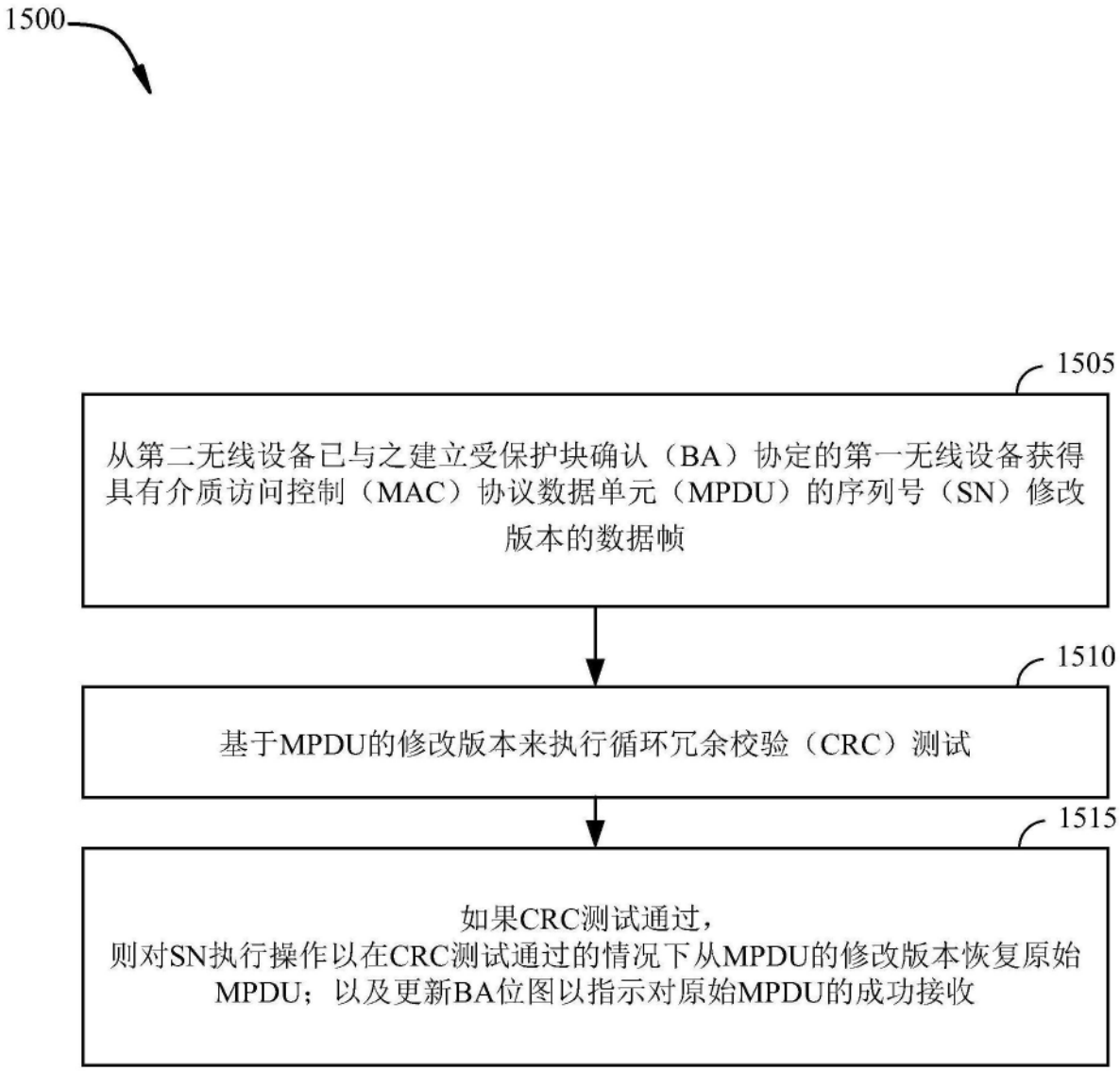

1500
1505
从第二无线设备已与之建立受保护块确认（BA）协定的第一无线设备获得具有介质访问控制（MAC）协议数据单元（MPDU）的序列号（SN）修改版本的数据帧
1510
基于MPDU的修改版本来执行循环冗余校验（CRC）测试
1515
如果CRC测试通过，
则对SN执行操作以在CRC测试通过的情况下从MPDU的修改版本恢复原始MPDU；以及更新BA位图以指示对原始MPDU的成功接收

图15

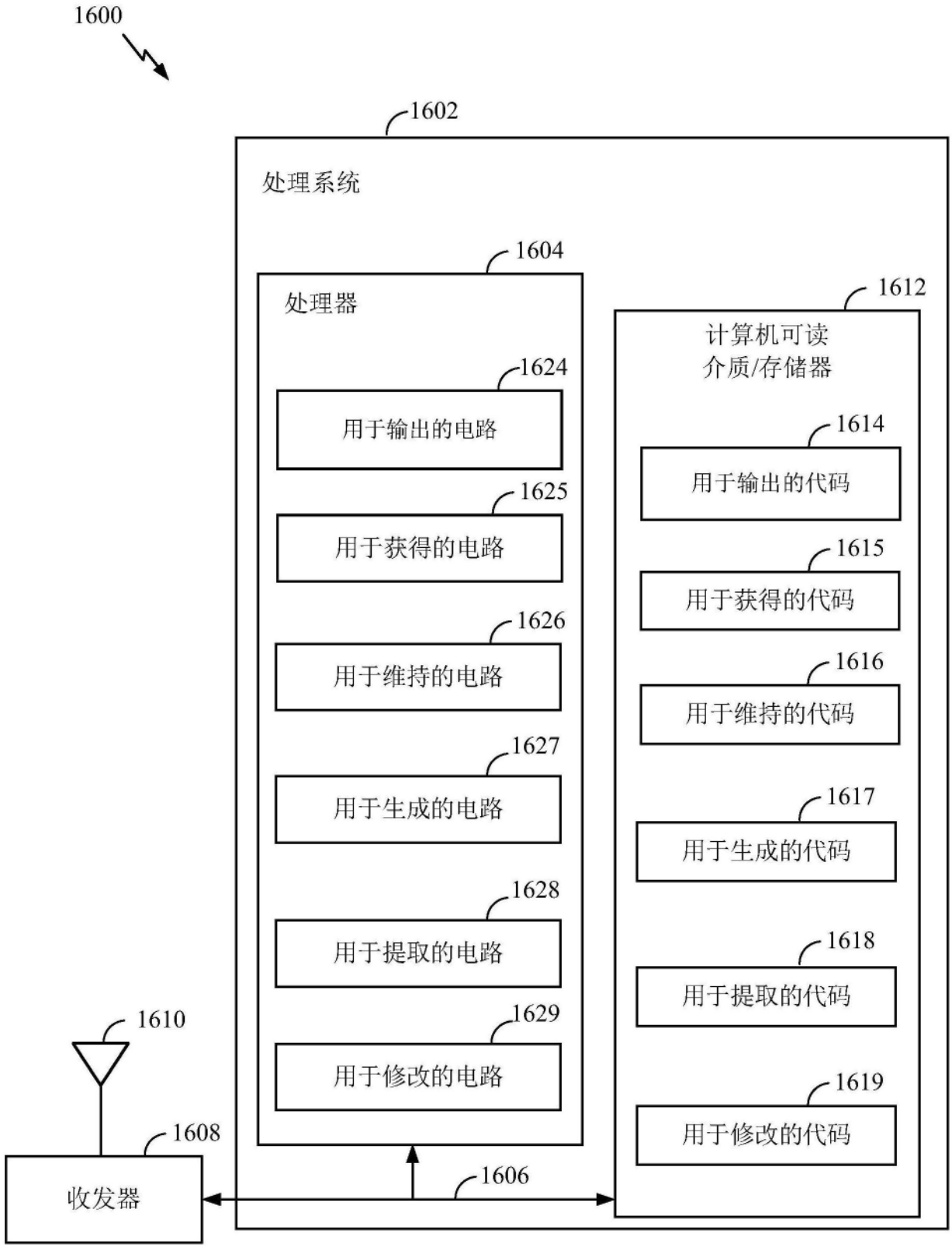

1600
1602
处理系统
1604
处理器
1624
用于输出的电路
1625
用于获得的电路
1626
用于维持的电路
1627
用于生成的电路
1628
用于提取的电路
1629
用于修改的电路
1610
1608
收发器
1606
1612
计算机可读
介质/存储器
1614
用于输出的代码
1615
用于获得的代码
1616
用于维持的代码
1617
用于生成的代码
1618
用于提取的代码
1619
用于修改的代码

图16