



(12)发明专利

(10)授权公告号 CN 104838689 B

(45)授权公告日 2018.10.02

(21)申请号 201380064585.7

(22)申请日 2013.12.12

(65)同一申请的已公布的文献号
申请公布号 CN 104838689 A

(43)申请公布日 2015.08.12

(30)优先权数据
61/736,513 2012.12.12 US
13/840,166 2013.03.15 US

(85)PCT国际申请进入国家阶段日
2015.06.10

(86)PCT国际申请的申请数据
PCT/US2013/074614 2013.12.12

(87)PCT国际申请的公布数据
W02014/093597 EN 2014.06.19

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州

(72)发明人 A·阿斯特加迪 M·M·温廷克
S·莫林

(74)专利代理机构 上海专利商标事务所有限公
司 31100

代理人 亓云

(51)Int.Cl.
H04W 28/06(2006.01)

(56)对比文件
US 2003/0191955 A1,2003.10.09,
US 2008/0247413 A1,2008.10.09,
WO 2012/159082 A2,2012.11.22,
WO 2009/098572 A1,2009.08.13,
US 2005/0169480 A1,2005.08.04,
US 6032197 A,2000.02.29,
US 2011/0055558 A1,2011.03.03,
US 2009/0052388 A1,2009.02.26,

审查员 刘英杰

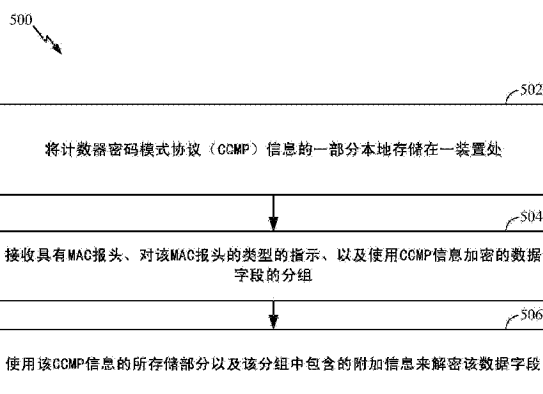
权利要求书6页 说明书10页 附图9页

(54)发明名称

使用短MAC报头的分组的安全性

(57)摘要

本公开的某些方面提供了用于向分组(例如,利用短MAC报头的分组)应用安全性的方法和装置。



1. 一种用于无线通信的装置,包括:

处理系统,其被配置成将计数器密码模式协议CCMP信息的第一部分本地存储在所述装置处,所述CCMP信息的第一部分是经由具有完整CCMP报头的先前接收到的分组所获得的;

接收机,其被配置成接收分组,所述分组包括基于所述CCMP信息来编码的数据字段;以及

解码器,其被配置成使用所述CCMP信息的所存储的第一部分以及所述分组中包含的附加信息来解码所述数据字段,其中:

所述处理系统被配置成:

从所述分组中包含的经压缩CCMP报头获得所述CCMP信息的第二部分;

获得所述CCMP信息的所存储的第一部分;以及

使用所述CCMP信息的所获得的第一部分和第二部分来解码所述数据字段。

2. 如权利要求1所述的装置,其特征在于,所述分组包括MAC报头和所述MAC报头包括具有相对于正常MAC报头而言经缩减数量的字节的短MAC报头的指示。

3. 如权利要求1所述的装置,其特征在于:

所述CCMP信息的所存储的第一部分包括用于加密所述数据字段的分组号的第一部分,其中所述分组号随每一传输而递增。

4. 如权利要求3所述的装置,其特征在于:

所述分组包括具有所述分组号的第二部分的CCMP报头。

5. 如权利要求3所述的装置,其特征在于,所述处理系统被配置成基于所述分组号中存储在所述装置处的第一部分和MAC报头中包含的序列号来生成所述分组号。

6. 如权利要求3所述的装置,其特征在于:

所述分组号中存储在所述装置处的所述第一部分包括所述分组号的最高有效位;以及

所述处理系统被配置成检测所述分组号的翻转,并且响应于所述检测来更新所述分组号中存储在所述装置处的所述最高有效位。

7. 如权利要求1所述的装置,其特征在于,所述处理系统被进一步配置成:

接收具有CCMP信息的经更新版本的后续分组;以及

更新所述CCMP信息的所存储部分。

8. 如权利要求1所述的装置,其特征在于:

所述分组包括缺少保留字节的CCMP报头;以及

所述处理系统使用所述CCMP报头中包含的信息和所存储信息来解码所述数据字段。

9. 一种用于无线通信的装置,包括:

处理系统,其被配置成使用计数器密码模式协议CCMP信息来编码数据字段;以及

发射机,其被配置成:

向另一装置发信号通知所述CCMP信息的第一部分;

向所述另一装置传送具有经编码数据字段的分组,其中所述分组缺少用于编码所述数据字段的所述CCMP信息中的一些;

在所述分组中包含的经压缩CCMP报头中向所述另一装置提供用于编码所述数据字段的所述CCMP信息的第二部分;以及

在先前接收到的分组中包含的完整CCMP报头中向所述另一装置提供用于编码所述数

据字段的所述CCMP信息的所述第一部分,所述完整CCMP报头具有所述经压缩CCMP报头中未包含的至少一些CCMP信息。

10. 如权利要求9所述的装置,其特征在于,所述分组包括MAC报头和所述MAC报头包括具有相对于正常MAC报头而言经缩减数量的字节的短MAC报头的指示。

11. 如权利要求9所述的装置,其特征在于:

所述CCMP信息中发信号通知的第一部分包括用于编码所述数据字段的分组号的第一部分,其中所述分组号随每一传输而递增。

12. 如权利要求11所述的装置,其特征在于:

所述分组包括具有所述分组号的第二部分的CCMP报头。

13. 如权利要求9所述的装置,其特征在于,所述处理系统被进一步配置成:

传送具有CCMP信息的经更新版本的后续分组。

14. 如权利要求9所述的装置,其特征在于:

所述分组包括缺少保留字节的CCMP报头。

15. 一种用于无线通信的设备,包括:

用于将计数器密码模式协议CCMP信息的第一部分本地存储在所述设备处的装置,所述CCMP信息的第一部分是经由具有完整CCMP报头的先前接收到的分组所获得的;

用于接收分组的装置,所述分组包括基于所述CCMP信息来编码的数据字段;

用于使用所述CCMP信息的所存储的第一部分以及所述分组中包含的附加信息来解码所述数据字段的装置;

用于从所述分组中包含的经压缩CCMP报头获得所述CCMP信息的第二部分的装置;以及

用于获得所述CCMP信息的所存储的第一部分的装置;

其中所述用于解码的装置被适配成使用所述CCMP信息的所获得的第一部分和第二部分来解码所述数据字段。

16. 如权利要求15所述的设备,其特征在于,所述分组包括MAC报头和所述MAC报头包括具有相对于正常MAC报头而言经缩减数量的字节的短MAC报头的指示。

17. 如权利要求15所述的设备,其特征在于:

所述CCMP信息的所存储的第一部分包括用于加密所述数据字段的分组号的第一部分,其中所述分组号随每一传输而递增。

18. 如权利要求17所述的设备,其特征在于:

所述分组包括具有所述分组号的第二部分的CCMP报头。

19. 如权利要求17所述的设备,其特征在于,所述用于解码的装置被配置成基于所述分组号中存储在所述设备处的第一部分和MAC报头中包含的序列号来生成所述分组号。

20. 如权利要求17所述的设备,其特征在于:

所述分组号中存储在所述设备处的所述第一部分包括所述分组号的最高有效位;以及
所述设备进一步包括用于检测所述分组号的翻转的装置以及用于响应于所述检测而更新所述分组号中存储在所述设备处的所述最高有效位的装置。

21. 如权利要求15所述的设备,其特征在于,所述设备进一步包括:

用于接收具有CCMP信息的经更新版本的后续分组的装置;以及

用于更新所述CCMP信息的所存储部分的装置。

22. 如权利要求15所述的设备,其特征在于:

所述分组包括缺少保留字节的CCMP报头;以及

所述用于解码的装置被配置成使用所述CCMP报头中包含的信息和所存储信息来解码所述数据字段。

23. 一种用于无线通信的设备,包括:

用于使用计数器密码模式协议CCMP信息来编码数据字段的装置;

用于向另一设备发信号通知所述CCMP信息的第一部分的装置;以及

用于向所述另一设备传送具有经编码数据字段的分组的装置,其中所述分组缺少用于编码所述数据字段的所述CCMP信息中的一些,其中:

所述用于发信号通知的装置被配置成:

在所述分组中包含的经压缩CCMP报头中向所述另一装置提供用于编码所述数据字段的所述CCMP信息的第二部分;以及

在先前接收到的分组中包含的完整CCMP报头中向所述另一装置提供用于编码所述数据字段的所述CCMP信息的所述第一部分,所述完整CCMP报头具有所述经压缩CCMP报头中未包含的至少一些CCMP信息。

24. 如权利要求23所述的设备,其特征在于,所述分组包括MAC报头和所述MAC报头包括具有相对于正常MAC报头而言经缩减数量的字节的短MAC报头的指示。

25. 如权利要求23所述的设备,其特征在于:

所述CCMP信息中发信号通知的第一部分包括用于编码所述数据字段的分组号的第一部分,其中所述分组号随每一传输而递增。

26. 如权利要求25所述的设备,其特征在于:

所述分组包括具有所述分组号的第二部分的CCMP报头。

27. 如权利要求23所述的设备,其特征在于,进一步包括:

用于传送具有CCMP信息的经更新版本的后续分组的装置。

28. 如权利要求23所述的设备,其特征在于:

所述分组包括缺少保留字节的CCMP报头。

29. 一种用于由一装置进行无线通信的方法,包括:

将计数器密码模式协议CCMP信息的第一部分本地存储在所述装置处,所述CCMP信息的第一部分是经由具有完整CCMP报头的先前接收到的分组所获得的;

接收分组,所述分组包括基于所述CCMP信息来编码的数据字段;以及

使用所述CCMP信息的所存储的第一部分以及所述分组中包含的附加信息来解码所述数据字段,其中:

所述方法进一步包括:

从所述分组中包含的经压缩CCMP报头获得所述CCMP信息的第二部分;

获得所述CCMP信息的所存储的第一部分;以及

使用所述CCMP信息的所获得的第一部分和第二部分来解码所述数据字段。

30. 如权利要求29所述的方法,其特征在于,所述分组包括MAC报头和所述MAC报头包括具有相对于正常MAC报头而言经缩减数量的字节的短MAC报头的指示。

31. 如权利要求29所述的方法,其特征在于:

所述CCMP信息的所存储的第一部分包括用于加密所述数据字段的分组号的第一部分，其中所述分组号随每一传输而递增。

32. 如权利要求31所述的方法，其特征在于：

所述分组包括具有所述分组号的第二部分的CCMP报头。

33. 如权利要求31所述的方法，其特征在于，进一步包括基于所述分组号中存储在所述装置处的第一部分和MAC报头中包含的序列号来生成所述分组号。

34. 如权利要求31所述的方法，其特征在于：

所述分组号中存储在所述装置处的所述第一部分包括所述分组号的最高有效位；以及所述方法进一步包括检测所述分组号的翻转，并且响应于所述检测的而更新所述分组号中存储在所述装置处的所述最高有效位。

35. 如权利要求29所述的方法，其特征在于，所述方法进一步包括：

接收具有CCMP信息的经更新版本的后续分组；以及更新所述CCMP信息的所存储部分。

36. 如权利要求29所述的方法，其特征在于：

所述分组包括缺少保留字节的CCMP报头；以及

所述解码包括使用所述CCMP报头中包含的信息和所存储信息来解码所述数据字段。

37. 一种用于由一装置进行无线通信的方法，包括：

使用计数器密码模式协议CCMP信息来编码数据字段；

向另一装置发信号通知所述CCMP信息的第一部分；以及

向所述另一装置传送具有经编码数据字段的分组，其中所述分组缺少用于编码所述数据字段的所述CCMP信息中的一些，其中：

所述发信号通知包括：

在所述分组中包含的经压缩CCMP报头中向所述另一装置提供用于编码所述数据字段的所述CCMP信息的第二部分；以及

在先前接收到的分组中包含的完整CCMP报头中向所述另一装置提供用于编码所述数据字段的所述CCMP信息的所述第一部分，所述完整CCMP报头具有所述经压缩CCMP报头中未包含的至少一些CCMP信息。

38. 如权利要求37所述的方法，其特征在于，所述分组包括MAC报头和所述MAC报头包括具有相对于正常MAC报头而言经缩减数量的字节的短MAC报头的指示。

39. 如权利要求37所述的方法，其特征在于：

所述CCMP信息中发信号通知的第一部分包括用于编码所述数据字段的分组号的第一部分，其中所述分组号随每一传输而递增。

40. 如权利要求39所述的方法，其特征在于：

所述分组包括具有所述分组号的第二部分的CCMP报头。

41. 如权利要求37所述的方法，其特征在于，进一步包括：

传送具有CCMP信息的经更新版本的后续分组。

42. 如权利要求37所述的方法，其特征在于：

所述分组包括缺少保留字节的CCMP报头。

43. 如权利要求37所述的方法，其特征在于：

所述编码包括使用密钥ID来编码所述数据字段。

44. 如权利要求43所述的方法,其特征在于,所述发信号通知包括经由管理帧交换或完整CCMP报头来向所述另一装置传送所述密钥ID。

45. 一种其上存储有计算机可执行指令的计算机可读介质,所述指令可执行以用于:

将计数器密码模式协议CCMP信息的第一部分本地存储在一装置处,所述CCMP信息的第一部分是经由具有完整CCMP报头的先前接收到的分组所获得的;

接收分组,所述分组包括基于所述CCMP信息来编码的数据字段;

使用所述CCMP信息的所存储的第一部分以及所述分组中包含的附加信息来解码所述数据字段,其中:

所述指令进一步可执行以用于:

从所述分组中包含的经压缩CCMP报头获得所述CCMP信息的第二部分;

获得所述CCMP信息的所存储的第一部分;以及

使用所述CCMP信息的所获得的第一部分和第二部分来解码所述数据字段。

46. 一种其上存储有计算机可执行指令的计算机可读介质,所述指令可执行以用于:

使用计数器密码模式协议CCMP信息来编码数据字段;

向另一装置发信号通知所述CCMP信息的第一部分;

向所述另一装置传送具有经编码数据字段的分组,其中所述分组缺少用于编码所述数据字段的所述CCMP信息中的一些,其中:

所述发信号通知包括:

在所述分组中包含的经压缩CCMP报头中向所述另一装置提供用于编码所述数据字段的所述CCMP信息的第二部分;以及

在先前接收到的分组中包含的完整CCMP报头中向所述另一装置提供用于编码所述数据字段的所述CCMP信息的所述第一部分,所述完整CCMP报头具有所述经压缩CCMP报头中未包含的至少一些CCMP信息。

47. 一种站,包括:

至少一个天线;

处理系统,其被配置成将计数器密码模式协议CCMP信息的第一部分本地存储在所述站处,所述CCMP信息的第一部分是经由具有完整CCMP报头的先前接收到的分组所获得的;

接收机,其被配置成经由所述至少一个天线接收分组,所述分组包括使用所述CCMP信息来编码的数据字段;以及

解码器,其被配置成使用所述CCMP信息的所存储的第一部分以及所述分组中包含的附加信息来解码所述数据字段,其中

所述处理系统被进一步配置成:

从所述分组中包含的经压缩CCMP报头获得所述CCMP信息的第二部分;

获得所述CCMP信息的所存储的第一部分;以及

使用所述CCMP信息的所获得的第一部分和第二部分来解码所述数据字段。

48. 一种接入点,包括:

至少一个天线;

处理系统,其被配置成使用计数器密码模式协议CCMP信息来编码数据字段;以及

发射机,其被配置成:

经由所述至少一个天线向站发信号通知所述CCMP信息的第一部分;

向所述站传送具有经编码数据字段的分组,其中所述分组缺少用于编码所述数据字段的所述CCMP信息中的一些;

在所述分组中包含的经压缩CCMP报头中向所述站提供用于编码所述数据字段的所述CCMP信息的第二部分;以及

在先前接收到的分组中包含的完整CCMP报头中向所述站提供用于编码所述数据字段的所述CCMP信息的所述第一部分,所述完整CCMP报头具有所述经压缩CCMP报头中未包含的至少一些CCMP信息。

使用短MAC报头的分组的安全性

[0001] 根据35U.S.C.§119的优先权要求

[0002] 本申请要求于2012年12月12日提交的美国临时专利申请S/N.61/736,513的权益，其通过引用被纳入于此。

发明领域

[0003] 本公开的某些方面一般涉及无线通信，更具体地涉及用于使用短MAC报头来启用分组开销的技术。

[0004] 相关背景

[0005] 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。这类多址网络的示例包括码分多址 (CDMA) 网络、时分多址 (TDMA) 网络、频分多址 (FDMA) 网络、正交FDMA (OFDMA) 网络、以及单载波FDMA (SC-FDMA) 网络。

[0006] 为了解决对更大的覆盖和增加的通信射程的期望，正开发各种方案。一种此类方案是正由电气电子工程师协会 (IEEE) 802.11ah任务组开发的亚1GHz频率范围 (例如，在美国工作在902-928MHz范围中)。此种开发由要利用具有比其它IEEE 802.11群更大的无线范围并具有更低的阻挡损耗的频率范围的愿望来驱动。

[0007] 概述

[0008] 本公开的某些方面提供了一种用于无线通信的装置。该装置通常包括：处理系统，其一般被配置成：将信息集的一部分本地存储在该装置处；接收分组，所述分组包括使用该信息集编码的数据字段；以及使用该信息集的所存储部分以及该分组中包含的附加信息来解码该数据字段。

[0009] 本公开的某些方面提供了一种用于无线通信的装置。该装置通常包括：处理系统，其被配置成：向接收实体发信号通知用于编码分组的数据部分的信息集的一部分；以及向该接收实体传送具有使用该信息集来编码的数据字段的分组，其中该分组缺少用于编码该数据字段的信息集中的一些。

[0010] 本公开的某些方面提供了一种用于无线通信的设备。该设备通常包括：用于将信息集的一部分本地存储在该设备处的装置；用于接收分组的装置，该分组包括使用该信息集编码的数据字段；以及用于使用该信息集的所存储部分以及该分组中包含的附加信息来解码该数据字段的装置。

[0011] 本公开的某些方面提供了一种用于无线通信的设备。该设备通常包括：用于向接收实体发信号通知用于编码分组的数据部分的信息集的一部分的装置；以及用于向该接收实体传送具有使用该信息集来编码的数据字段的分组的装置，其中该分组缺少用于编码数据字段的信息集中的一些。

[0012] 本公开的某些方面提供了一种用于由装置进行无线通信的方法。该方法通常包括：将信息集的一部分本地存储在该装置处；接收分组，该分组包括使用该信息集编码的数据字段；以及使用该信息集的所存储部分以及该分组中包含的附加信息来解码该数据字

段。

[0013] 本公开的某些方面提供了一种用于由装置进行无线通信的方法。该方法通常包括：向接收实体发信号通知用于编码分组的数据部分的信息集的一部分；以及向该接收实体传送具有使用该信息集来编码的数据字段的分组，其中该分组缺少用于编码数据字段的该信息集中的一些。

[0014] 本公开的某些方面提供了一种用于由装置进行无线通信的计算机程序产品，该计算机程序产品包括其上存储有指令的计算机可读介质。这些指令一般可执行用于：将信息集的一部分本地存储在该装置处；接收分组，该分组包括使用该信息集编码的数据字段；以及使用该信息集的所存储部分以及该分组中包含的附加信息来解码数据字段。

[0015] 本公开的某些方面提供了一种用于由装置进行无线通信的计算机程序产品，该计算机程序产品包括其上存储有指令的计算机可读介质。这些指令一般可执行用于：向接收实体发信号通知用于编码分组的数据部分的信息集的一部分；以及向该接收实体传送具有使用该信息集来编码的数据字段的分组，其中该分组缺少用于编码数据字段的该信息集中的一些。

[0016] 本公开的某些方面提供了一种用于无线通信的站。该站通常包括：处理系统，其一般被配置成：将信息集的一部分本地存储在该站处；接收分组，该分组包括使用该信息集编码的数据字段；以及使用该信息集的所存储部分以及该分组中包含的附加信息来解码数据字段。

[0017] 本公开的某些方面提供了一种用于无线通信的接入点。该接入点一般包括：处理系统，其被配置成：向站发信号通知用于编码分组的数据部分的信息集的一部分；以及向该站传送具有使用该信息集来编码的数据字段的分组，其中该分组缺少用于编码数据字段的该信息集中的一些。

[0018] 附图简述

[0019] 为了能详细理解本公开的以上陈述的特征所用的方式，可参照各方面来对以上简要概述的内容进行更具体的描述，其中一些方面在附图中解说。然而应该注意，附图仅解说了本公开的某些典型方面，故不应被认为限定其范围，因为本描述可允许有其他等同有效的方面。

[0020] 图1解说了根据本公开的某些方面的示例无线通信网络的示意图。

[0021] 图2解说了根据本公开的某些方面的示例接入点和用户终端的框图。

[0022] 图3解说了根据本公开的某些方面的示例无线设备的框图。

[0023] 图4解说了利用短MAC报头的示例分组结构。

[0024] 图5解说了根据本公开的某些方面的用于由接收机进行无线通信的示例操作的框图。

[0025] 图5A解说了能够执行图5中示出的操作的示例装置。

[0026] 图6解说了根据本公开的某些方面的用于由发射机进行无线通信的示例操作的框图。

[0027] 图6A解说了能够执行图6中示出的操作的示例装置。

[0028] 图7解说了根据本公开的各方面的具有经压缩CCMP报头的示例分组结构。

[0029] 图7A解说了根据本公开的各方面的示例经压缩CCMP报头。

[0030] 图8解说了根据本公开的各方面的具有经压缩CCMP报头的另一示例分组结构。

[0031] 图8A解说了根据本公开的各方面的示例经压缩CCMP报头。

[0032] 图9解说了根据本公开的各方面的不带有CCMP报头的示例分组结构。

[0033] 详细描述

[0034] 以下参照附图更全面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定于本公开通篇给出的任何具体结构或功能。相反，提供这些方面是为了使得本公开将是透彻和完整的，并且其将向本领域技术人员完全传达本公开的范围。基于本文中的教导，本领域技术人员应领会，本公开的范围旨在覆盖本文中所披露的本公开的任何方面，不论其是与本公开的任何其他方面相独立地还是组合地实现的。例如，可以使用本文所阐述的任何数目的方面来实现装置或实践方法。另外，本公开的范围旨在覆盖使用作为本文中所阐述的本公开的各种方面的补充或者另外的其他结构、功能性、或者结构及功能性来实践的此类装置或方法。应当理解，本文中所披露的本公开的任何方面可由权利要求的一个或多个元素来实施。

[0035] 尽管本文描述了特定方面，但这些方面的众多变体和置换落在本公开的范围之内。尽管提到了优选方面的一些益处和优点，但本公开的范围并非旨在被限定于特定益处、用途或目标。确切而言，本公开的各方面旨在宽泛地适用于不同的无线技术、系统配置、网络、和传输协议，其中一些藉由示例在附图和以下对优选方面的描述中解说。详细描述和附图仅仅解说本公开而非限定本公开，本公开的范围由所附权利要求及其等效技术方案来定义。

[0036] 示例无线通信系统

[0037] 本文所描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。SDMA系统可利用充分不同的方向来同时传送属于多个用户终端的数据。TDMA系统可通过将传输信号划分成不同时隙、每个时隙被指派给不同的用户终端来允许多个用户终端共享相同的频率信道。OFDMA系统利用正交频分复用 (OFDM)，这是一种将整个系统带宽分成多个正交副载波的调制技术。这些副载波也可以被称为频调、频槽等。在OFDM中，每个副载波可以用数据独立调制。SC-FDMA系统可以利用交织式FDMA (IFDMA) 在跨系统带宽分布的副载波上传送，利用局部化FDMA (LFDMA) 在毗邻副载波的块上传送，或者利用增强型FDMA (EFDMA) 在毗邻副载波的多个块上传送。一般而言，调制码元在OFDM中是在频域中被发送的，而在SC-FDMA中是在时域中被发送的。

[0038] 本文中的教导可被纳入各种有线或无线装置 (例如节点) 中 (例如实现在其内或由其执行)。在一些方面，根据本文中的教导实现的无线节点可包括接入点或接入终端。

[0039] 接入点 (“AP”) 可包括、被实现为、或被称为B节点、无线网络控制器 (“RNC”)、演进型B节点 (eNB)、基站控制器 (“BSC”)、基收发机站 (“BTS”)、基站 (“BS”)、收发机功能 (“TF”)、无线电路由器、无线电收发机、基本服务集 (“BSS”)、扩展服务集 (“ESS”)、无线电基站 (“RBS”)、或其它某个术语。

[0040] 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、或其他某个术语。在一些实现中，接入终端可包括蜂窝电话、无绳电话、会话发起协议 (“SIP”) 话机、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其他某种合适的处理设备。相应地，本文中所教导的一个或多

个方面可被纳入到电话(例如,蜂窝电话或智能电话)、计算机(例如,膝上型计算机)、平板、便携式通信设备、便携式计算设备(例如,个人数据助理)、娱乐设备(例如,音乐或视频设备、或卫星无线电)、全球定位系统(GPS)设备、或配置成经由无线或有线介质通信的任何其它合适的设备中。在一些方面,节点是无线节点。此类无线节点可例如经由有线或无线通信链路来为网络(例如,广域网(诸如因特网)或蜂窝网络)提供连通性或提供至该网络的连通性。

[0041] 图1解说了具有接入点和用户终端的多址多输入多输出(MIMO)系统100。为简单起见,图1中仅示出一个接入点110。接入点一般是与各用户终端通信的固定站,并且也可被称为基站或其他某个术语。用户终端可以是固定的或者移动的,并且也可称作移动站、无线设备、或其他某个术语。接入点110可在任何给定时刻在下行链路和上行链路上与一个或多个用户终端120通信。下行链路(即,前向链路)是从接入点至用户终端的通信链路,而上行链路(即,反向链路)是从用户终端至接入点的通信链路。用户终端还可与另一用户终端进行对等通信。系统控制器130耦合至各接入点并提供对这些接入点的协调和控制。

[0042] 尽管以下公开的各部分将描述能够经由空分多址(SDMA)来通信的用户终端120,但对于某些方面,用户终端120还可包括不支持SDMA的一些用户终端。因此,对于这些方面,AP 110可被配置成与SDMA用户终端通信和非SDMA用户终端两者通信。这一办法可便于允许较老版本的用户终端(“传统”站)仍就部署在企业中以延长其有用寿命,同时允许在认为恰当的场所引入较新的SDMA用户终端。

[0043] 系统100采用多个发射天线和多个接收天线来进行下行链路和上行链路上的数据传输。接入点110装备有 N_{ap} 个天线并且对于下行链路传输而言表示多输入(MI)而对于上行链路传输而言表示多输出(MO)。具有 K 个选定用户终端120的集合共同地对于下行链路传输表示多输出而对于上行链路传输表示多输入。对于纯SDMA而言,如果用于 K 个用户终端的数据码元流没有通过某种手段在码、频率或时间上复用,则期望具有 $N_{ap} \geq K \geq 1$ 。如果数据码元流能够使用TDMA技术、在CDMA下使用不同的码信道、在OFDM下使用不相交的子频带集合等进行复用,则 K 可以大于 N_{ap} 。每个选定用户终端向接入点传送因用户而异的数据和/或从接入点接收因用户而异的数据。一般而言,每个选定用户终端可装备有一个或多个天线(即, $N_{ut} \geq 1$)。这 K 个选定用户终端可具有相同或不同数目的天线。

[0044] SDMA系统可以是时分双工(TDD)系统或频分双工(FDD)系统。对于TDD系统,下行链路和上行链路共享相同频带。对于FDD系统,下行链路和上行链路使用不同频带。MIMO系统100还可利用单载波或多载波进行传输。每个用户终端可装备有单个天线(例如为了抑制成本)或多个天线(例如在能够支持附加成本的场合)。如果诸用户终端120通过将传输/接收划分到不同时隙中、每个时隙被指派给不同的用户终端120的方式来共享相同的频率信道,则系统100还可以是TDMA系统。

[0045] 图2解说了MIMO系统100中的接入点110以及两个用户终端120m和120x的框图。接入点110装备有 N_t 个天线224a到224t。用户终端120m装备有 $N_{ut,m}$ 个天线252ma到252mu,而用户终端120x装备有 $N_{ut,x}$ 个天线252xa到252xu。接入点110对于下行链路而言是传送方实体,而对于上行链路而言是接收方实体。每个用户终端120对于上行链路而言是传送方实体,而对于下行链路而言是接收方实体。如本文中所使用的,“传送方实体”是能够经由无线信道传送数据的独立操作的装置或设备,而“接收方实体”是能够经由无线信道接收数据的独立

操作的装置或设备。在以下描述中,下标“dn”标示下行链路,下标“up”标示上行链路, N_{up} 个用户终端被选定进行上行链路上的同时传输, N_{dn} 个用户终端被选定进行下行链路上的同时传输, N_{up} 可以等于或不等于 N_{dn} ,且 N_{up} 和 N_{dn} 可以是静态值或者可随每个调度区间而改变。可在接入点和用户终端处使用波束转向或其他某种空间处理技术。

[0046] 在上行链路上,在被选择用于上行链路传输的每个用户终端120处,发射(TX)数据处理单元288接收来自数据源286的话务数据和来自控制器280的控制数据。TX数据处理单元288基于与为该用户终端选择的速率相关联的编码及调制方案来处理(例如,编码、交织、和调制)该用户终端的话务数据并提供数据码元流。TX空间处理器290对该数据码元流执行空间处理并向 $N_{ut,m}$ 个天线提供 $N_{ut,m}$ 个发射码元流。每个发射单元(TMTR)254接收和处理(例如,转换至模拟、放大、滤波、及上变频)相应的发射码元流以生成上行链路信号。 $N_{ut,m}$ 个发射机单元254提供 $N_{ut,m}$ 个上行链路信号以进行从 $N_{ut,m}$ 个天线252到接入点的传输。

[0047] N_{up} 个用户终端可被调度用于在上行链路上进行同时传输。这些用户终端中的每一个对其自己的数据码元流执行空间处理并在上行链路上向接入点传送自己的发射码元流集。

[0048] 在接入点110处, N_{ap} 个天线224a到224ap从在上行链路上进行传送的所有 N_{up} 个用户终端接收上行链路信号。每个天线224向各自相应的接收机单元(RCVR)222提供收到信号。每个接收机单元222执行与由发射机单元254执行的处理互补的处理,并提供收到码元流。RX空间处理器240对来自 N_{ap} 个接收机单元222的 N_{ap} 个收到码元流执行接收机空间处理并提供 N_{up} 个恢复出的上行链路数据码元流。接收机空间处理是根据信道相关矩阵求逆(CCMI)、最小均方误差(MMSE)、软干扰消去(SIC)、或其他某种技术来执行的。每个恢复出的上行链路数据码元流是对由各自相应用户终端传送的数据码元流的估计。RX数据处理单元242根据用于每个恢复出的上行链路数据码元流的速率来处理(例如,解调、解交织、和解码)此恢复出的上行链路数据码元流以获得经解码数据。每个用户终端的经解码数据可被提供给数据阱244以供存储和/或提供给控制器230以供进一步处理。

[0049] 在下行链路上,在接入点110处,TX数据处理单元210接收来自数据源208的给用于下行链路传输所调度的 N_{dn} 个用户终端的话务数据、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。可在不同的传输信道上发送各种类型的数据。TX数据处理单元210基于为每个用户终端选定的速率来处理(例如,编码、交织、和调制)该用户终端的话务数据。TX数据处理单元210为 N_{dn} 个用户终端提供 N_{dn} 个下行链路数据码元流。TX空间处理器220对 N_{dn} 个下行链路数据码元流执行空间处理(诸如预编码或波束成形,如本公开中所描述的那样)并为 N_{ap} 个天线提供 N_{ap} 个发射码元流。每个发射机单元222接收和处理各自相应的发射码元流以生成下行链路信号。 N_{ap} 个发射机单元222提供 N_{ap} 个下行链路信号以进行从 N_{ap} 个天线224到用户终端的传输。

[0050] 在每个用户终端120处, $N_{ut,m}$ 个天线252接收 N_{ap} 个来自接入点110的下行链路信号。每个接收机单元254处理来自相关联的天线252的收到信号并提供收到码元流。RX空间处理器260对来自 $N_{ut,m}$ 个接收机单元254的 $N_{ut,m}$ 个收到码元流执行接收机空间处理并提供恢复出的给该用户终端的下行链路数据码元流。接收机空间处理是根据CCMI、MMSE、或其他某种技术来执行的。RX数据处理单元270处理(例如,解调、解交织和解码)恢复出的下行链路数据码元流以获得给该用户终端的经解码数据。

[0051] 在每个用户终端120处,信道估计器278估计下行链路信道响应并提供下行链路信道估计,下行链路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估计上行链路信道响应并提供上行链路信道估计。每个用户终端的控制器280通常基于该用户终端的下行链路信道响应矩阵 $H_{dn,m}$ 来推导该用户终端的空间滤波矩阵。控制器230基于有效上行链路信道响应矩阵 $H_{up,eff}$ 来推导接入点的空间滤波矩阵。每个用户终端的控制器280可向接入点发送反馈信息(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还分别控制接入点110和用户终端120处的各种处理单元的操作。

[0052] 图3解说了可在MIMO系统100内可采用的无线设备302中利用的各种组件。无线设备302是可被配置成实现本文描述的各种方法的设备的示例。无线设备302可以是接入点110或用户终端120。

[0053] 无线设备302可包括控制无线设备302的操作的处理器304。处理器304也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执行逻辑和算术运算。存储器306中的指令可以是可执行的以实现本文描述的方法。

[0054] 无线设备302还可包括外壳308,该外壳308可包括发射机310和接收机312以允许在无线设备302和远程位置之间进行数据的传送和接收。发射机310和接收机312可被组合成收发机314。单个或多个发射天线316可被附连至外壳308且电耦合至收发机314。无线设备302还可包括(未示出)多个发射机、多个接收机和多个收发机。

[0055] 无线设备302还可包括可用于力图检测和量化由收发机314收到的信号电平的信号检测器318。信号检测器318可检测诸如总能量、每副载波每码元能量、功率谱密度之类的信号以及其它信号。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。

[0056] 无线设备302的各个组件可由总线系统322耦合在一起,该总线系统322除数据总线外还可包括电源总线、控制信号总线以及状态信号总线。

[0057] 具有短MAC报头的分组的示例安全性

[0058] 具有短MAC报头(相对于完整MAC报头而言经压缩)的分组结构的使用已在一些标准中被接受,诸如IEEE 802.11ah。802.11ah中定义的短MAC报头被从正常MAC报头的34字节缩减至12字节。短MAC报头中经缩减数量的位允许减少开销并且尤其有益于其中开销占总体分组大小的较大百分比的短数据分组。

[0059] 本文呈现的技术提供了用于减少经加密分组(例如使用短MAC报头的那些分组)的开销的技术。本文呈现的技术提供了用于减少与每分组加密相关联的开销的各种选项。这些技术可被分开使用或者在一些情况下组合使用以达成更大的开销减少。

[0060] 图4解说了具有短MAC报头410而非完整CCMP报头420的分组400(在所解说的示例中是MPDU)的示例。如所解说的,MAC报头420包含数据分组的目的地和源地址,而CCMP报头具有分组号(PN)、Ext IV、以及密钥ID。如所解说的,分组号是跨6个八位位组来存储的48位数(如所解说的,PN码是CCMP报头的前两个和最后四个八位位组)且随每一后续分组递增。密钥ID八位位组包含Ext IV(位5)、密钥ID(位6-7)以及保留子字段(位0-4)。

[0061] CCMP报头中的这一信息被用于加密数据单元和保护分组的完整性和真实性的消息完整性码(MIC)。用于检错和纠错的帧校验序列(FCS)未被加密。

[0062] 本文呈现的技术可以帮助减少与传送CCMP报头相关联的开销。根据一些方面, CCMP信息的一部分(常规上被携带在完整CCMP报头中)可被存储在接收机处。例如, 如果PN的前4个字节被存储, 则CCMP报头可减少4字节。作为补充或者作为替换, 不必要的(保留)字段可被移除(1字节)。下文讨论的其他技术可造成进一步减少。

[0063] 图5是根据本公开的各方面的用于由接收实体进行无线通信的示例操作500的框图。操作500可由诸如站或接入点之类的装置来执行。

[0064] 在502, 该装置将计数器密码模式协议(CCMP)信息的一部分本地存储在该装置处。在504, 该装置接收具有MAC报头、对MAC报头的类型的指示、以及使用CCMP信息加密的数据字段的分组。在506, 该装置使用该CCMP信息的所存储部分以及分组中包含的附加信息来解密数据字段。

[0065] 图6是根据本公开的各方面的用于由传送方实体进行无线通信的示例操作600的框图。操作600可由诸如站或接入点之类的装置来执行。

[0066] 在602, 该装置向接收方实体发信号通知计数器密码模式协议(CCMP)信息中要被存储在接收方实体处的一部分。在604, 该装置传送具有MAC报头、对MAC报头的类型的指示、以及使用CCMP信息加密的数据字段的分组, 其中该分组缺少用于加密数据字段的CCMP信息中的一些。

[0067] 图7解说了根据本公开的各方面的具有短(经压缩)CCMP报头720的示例分组700。

[0068] 如所解说的, 通过定义基PN(在所解说的示例中, $BPN = PN2 | PN3 | PN4 | PN5$)来执行CCMP报头压缩是可能的。BPN可被存储在接收方实体处且可通过管理帧交换来获得。根据某些方面, CCMP报头的其余部分可与分组一起发送(例如, 与所发送的PN的最低有效位和密钥ID一起, $PN0 | PN1 | \text{密钥ID}$)。这可被称为分组PN(PPN)。

[0069] 根据这一信息, 连同所存储的信息, 可以在接收机处重构完整CCMP报头信息。例如, 完整PN可以根据(所传送的)PPN和(所存储的)BPN来重构如下: $PN = \text{串接PPN} | BPN$ 。BPN可能需要在 $PN0 | PN1$ 翻转之际更新。对于802.11ah应用而言, 基于16位的翻转预期非常低且可以在接收机处检测(并且BPN相应地更新)。

[0070] 如图7A所示, 使用这一办法, CCMP报头从8个八位位组缩减为3个八位位组, 因为只有 $PN0 | PN1 | \text{密钥ID}$ 八位位组需要连同分组一起传送。

[0071] 图8解说了根据本公开的各方面的具有短CCMP报头820的另一示例的示例分组800。

[0072] 如所解说的, 执行更高效的CCMP报头压缩是可能的。此进一步压缩可例如通过允许所传送的序列控制(SC)号(在MAC报头中)担当 $PN0 | PN1$ 而是可能的。换言之, $PN0 | PN1 = SC (= \text{序列号(SN)} | \text{分段号(FN)})$ 。在一些情形中, 在MSDU未被分段时, 分组号以16为步长增加。结果, PN可有效地缩减4位。

[0073] 如图8A所解说的, 这一办法可导致被缩减为仅1个八位位组的CCMP报头, 因为仅密钥ID八位位组需要与该分组一起传送。

[0074] 如图9所解说的, 发送根本不具有CCMP报头的分组甚至是可能的(如空CCMP报头920所指示的)。此进一步压缩可通过移除密钥ID八位位组而是可能的。这可以是可能的, 因为(密钥ID八位位组中包括的)Ext IV的值对于CCMP而言总是1。此外, 因为密钥更新(re-keying)对于单播话务而言可能从不发生, 并且群话务不使用短MAC报头, 因此密钥ID也可

被省略。结果,CCMP报头基本上从短MAC报头中消除。在这一情形中,分组号(的LSB)可以根据序列控制号SC来确定,例如 $PN0 \mid PN1 = SC$ 。

[0075] 如本文描述的,通过将CCMP报头的CCMP信息的一部分(例如, $PN2 \mid PN3 \mid PN4 \mid PN5$)作为基PN存储在接收机处(例如,通过管理帧交换获得的基PN),CCMP报头开销可被显著减少。根据某些方面,CCMP报头的保留字段的八位位组可以在与短MAC报头联用时被移除。此外,CCMP报头的密钥ID字段在与短MAC报头联用时也可被存储在接收机处(并通过管理帧交换来获得)。在协商新密钥时,密钥更新可以通过临时地使用具有正常MAC报头和当前密钥的正常帧来实现。在新密钥(以及密钥ID)已经被协商时,它可变成用于短MAC报头的密钥(以及密钥ID),且可以恢复使用短MAC报头。

[0076] 根据某些方面,在CCMP报头与短MAC报头联用时,短MAC报头的序列控制字段可被用作CCMP报头的 $PN0 \mid PN1$ 。

[0077] 以上所描述的方法的各种操作可由能够执行相应功能的任何合适的装置来执行。这些装置可包括各种硬件和/或软件组件和/或模块,包括但不限于电路、专用集成电路(ASIC)、或处理器。一般而言,在存在附图中解说的操作的场合,那些操作可具有带相似编号的相应配对装置加功能组件。例如,在图5和图6中解说的操作500和600分别对应于在图5A和图6A中解说的装置500A和600A。

[0078] 例如,用于传送的装置可包括图2中解说的接入点110的发射机(例如,发射机单元222)和/或(诸)天线224,或者图3中描绘的发射机310和/或(诸)天线316。用于接收的装置可包括图2中解说的接入点110的接收机(例如,接收机单元222)和/或(诸)天线224,或者图3中描绘的接收机312和/或(诸)天线316。用于处理的装置、用于确定的装置、用于检测的装置、用于扫描的装置、用于选择的装置、或用于终止操作的装置可包括处理系统,该处理系统可包括一个或多个处理器,诸如图2中所解说的接入点110的RX数据处理器242、TX数据处理器210和/或控制器230或者图3所描述的处理器304和/或DSP 320。

[0079] 如本文所使用的,术语“确定”涵盖各种各样的动作。例如,“确定”可包括演算、计算、处理、推导、研究、查找(例如,在表、数据库或其他数据结构中查找)、探知及诸如此类。而且,“确定”可包括接收(例如,接收信息)、访问(例如,访问存储器中的数据)及诸如此类。而且,“确定”还可包括解析、选择、选取、确立及类似动作。

[0080] 如本文中所使用的,引述一系列项目中的“至少一个”的短语是指这些项目的任何组合,包括单个成员。作为示例,“a、b或c中的至少一个”旨在涵盖:a、b、c、a-b、a-c、b-c、以及a-b-c。

[0081] 结合本公开描述的各种解说性逻辑块、模块、以及电路可用通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)或其他可编程逻辑器件(PLD)、分立的门或晶体管逻辑、分立的硬件组件、或其设计成执行本文中描述的功能的任何组合来实现或执行。通用处理器可以是微处理器,但在替换方案中,处理器可以是任何可商业购得的处理器、控制器、微控制器、或状态机。处理器还可以被实现为计算设备的组合,例如DSP与微处理器的组合、多个微处理器、与DSP核心协同的一个或多个微处理器、或任何其它此类配置。

[0082] 结合本公开所描述的方法或算法的步骤可直接在硬件中、在由处理器执行的软件模块中、或在这两者的组合中体现。软件模块可驻留在本领域所知的任何形式的存储介质

中。可使用的存储介质的一些示例包括随机存取存储器 (RAM)、只读存储器 (ROM)、闪存、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动盘、CD-ROM, 等等。软件模块可包括单条指令、或许多条指令, 且可分布在若干不同的代码段上, 分布在不同的程序间以及跨多个存储介质分布。存储介质可被耦合到处理器以使得该处理器能从/向该存储介质读写信息。替换地, 存储介质可以被整合到处理器。

[0083] 本文所公开的方法包括用于实现所描述的方法的一个或多个步骤或动作。这些方法步骤和/或动作可以彼此互换而不会脱离权利要求的范围。换言之, 除非指定了步骤或动作的特定次序, 否则具体步骤和/或动作的次序和/或使用可以改动而不会脱离权利要求的范围。

[0084] 所描述的功能可在硬件、软件、固件或其任何组合中实现。如果以硬件实现, 则示例硬件配置可包括无线节点中的处理系统。处理系统可以用总线架构来实现。取决于处理系统的具体应用和整体设计约束, 总线可包括任何数目的互连总线和桥接器。总线可将包括处理器、机器可读介质、以及总线接口的各种电路链接在一起。总线接口可用于尤其将网络适配器等经由总线连接至处理系统。该网络适配器可用于实现PHY层的信号处理功能。在接入终端120 (见图1) 的情形中, 用户接口 (例如, 按键板、显示器、鼠标、操纵杆, 等等) 也可以被连接到总线。总线还可以链接各种其他电路, 诸如定时源、外围设备、稳压器、功率管理电路以及类似电路, 它们在本领域中是众所周知的, 因此将不再进一步描述。

[0085] 处理器可负责管理总线和一般处理, 包括执行存储在机器可读介质上的软件。处理器可用一个或多个通用和/或专用处理器来实现。示例包括微处理器、微控制器、DSP 处理器、以及其他能执行软件的电路系统。软件应当被宽泛地解释成意指指令、数据、或其任何组合, 无论是被称作软件、固件、中间件、微代码、硬件描述语言、或其他。作为示例, 机器可读介质可以包括RAM (随机存取存储器)、闪存、ROM (只读存储器)、PROM (可编程只读存储器)、EPROM (可擦式可编程只读存储器)、EEPROM (电可擦式可编程只读存储器)、寄存器、磁盘、光盘、硬驱动器、或者任何其他合适的存储介质、或其任何组合。机器可读介质可被实施在计算机程序产品中。该计算机程序产品可以包括包装材料。

[0086] 在硬件实现中, 机器可读介质可以是处理系统中与处理器分开的一部分。然而, 如本领域技术人员将容易领会的, 机器可读介质、或其任何部分可在处理系统外部。作为示例, 机器可读介质可包括传输线、由数据调制的载波、和/或与无线节点分开的计算机产品, 所有这些都可由处理器通过总线接口来访问。替换地或补充地, 机器可读介质、或其任何部分可被集成到处理器中, 诸如高速缓存和/或通用寄存器文件可能就是这种情形。

[0087] 处理系统可以被配置为通用处理系统, 该通用处理系统具有一个或多个提供处理器功能性的微处理器、和提供机器可读介质中的至少一部分的外部存储器, 它们都通过外部总线架构与其他支持电路系统链接在一起。替换地, 处理系统可以用带有集成在单块芯片中的处理器、总线接口、用户接口 (在接入终端情形中)、支持电路系统、和至少一部分机器可读介质的ASIC (专用集成电路) 来实现, 或者用一个或多个FPGA (现场可编程门阵列)、PLD (可编程逻辑器件)、控制器、状态机、门控逻辑、分立硬件组件、或者任何其他合适的电路系统、或者能执行本公开通篇所描述的各种功能性的电路的任何组合来实现。取决于具体应用和加诸于整体系统上的总设计约束, 本领域技术人员将认识到如何最佳地实现关于处理系统所描述的功能性。

[0088] 机器可读介质可包括数个软件模块。这些软件模块包括当由处理器执行时使处理系统执行各种功能的指令。这些软件模块可包括传输模块和接收模块。每个软件模块可以驻留在单个存储设备中或者跨多个存储设备分布。作为示例,当触发事件发生时,可以从硬驱动器中将软件模块加载到RAM中。在软件模块执行期间,处理器可以将一些指令加载到高速缓存中以提高访问速度。随后可将一个或多个高速缓存行加载到通用寄存器文件中以供由处理器执行。在以下谈及软件模块的功能性时,将理解此类功能性是在处理器执行来自该软件模块的指令时由该处理器来实现的。

[0089] 如果以软件实现,则各功能可作为一条或多条指令或代码存储在计算机可读介质上或藉其进行传送。计算机可读介质包括计算机存储介质和通信介质两者,这些介质包括促成计算机程序从一地向另一地转移的任何介质。存储介质可以是能被计算机访问的任何可用介质。作为示例而非限定,这样的计算机可读介质可包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储、磁盘存储或其它磁存储设备、或能用于携带或存储指令或数据结构形式的期望程序代码且能被计算机访问的任何其它介质。任何连接也被正当地称为计算机可读介质。例如,如果软件是使用同轴电缆、光纤电缆、双绞线、数字订户线(DSL)、或无线技术(诸如红外(IR)、无线电、以及微波)从web网站、服务器、或其他远程源传送而来,则该同轴电缆、光纤电缆、双绞线、DSL或无线技术(诸如红外、无线电、以及微波)就被包括在介质的定义之中。如本文中所使用的盘(disk)和碟(disc)包括压缩碟(CD)、激光碟、光碟、数字多用碟(DVD)、软盘、和蓝光[®]碟,其中盘(disk)常常磁性地再现数据,而碟(disc)用激光来光学地再现数据。因此,在一些方面,计算机可读介质可包括非瞬态计算机可读介质(例如,有形介质)。另外,对于其他方面,计算机可读介质可包括瞬态计算机可读介质(例如,信号)。上述的组合应当也被包括在计算机可读介质的范围内。

[0090] 因此,一些方面可包括用于执行本文中给出的操作的计算机程序产品。例如,此类计算机程序产品可包括其上存储(和/或编码)有指令的计算机可读介质,这些指令能由一个或多个处理器执行以执行本文中所描述的操作。对于一些方面,计算机程序产品可包括包装材料。

[0091] 此外,应当领会,用于执行本文中所描述的方法和技术的模块和/或其它恰适装置能由用户终端和/或基站在适用的场合下载和/或以其他方式获得。例如,此类设备能被耦合至服务器以促成用于执行本文中所描述的方法的装置的转移。替换地,本文所述的各种方法能经由存储装置(例如,RAM、ROM、诸如压缩碟(CD)或软盘等物理存储介质等)来提供,以使得一旦将该存储装置耦合至或提供给用户终端和/或基站,该设备就能获得各种方法。此外,可利用适于向设备提供本文中所描述的方法和技术的任何其他合适的技术。

[0092] 将理解,权利要求并不被限定于以上所解说的精确配置和组件。可在以上所描述的方法和设备的布局、操作和细节上作出各种改动、更换和变形而不会脱离权利要求的范围。

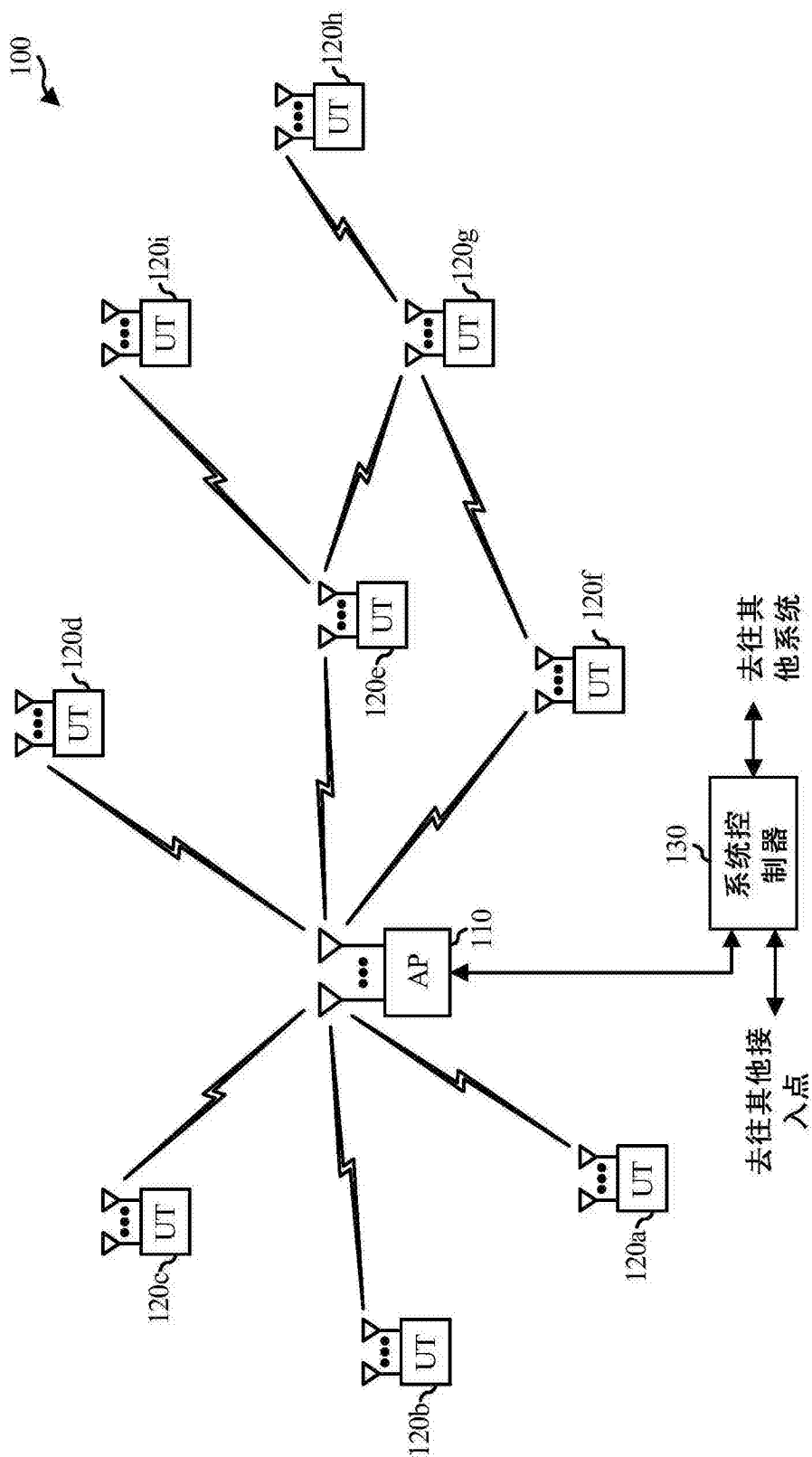


图1

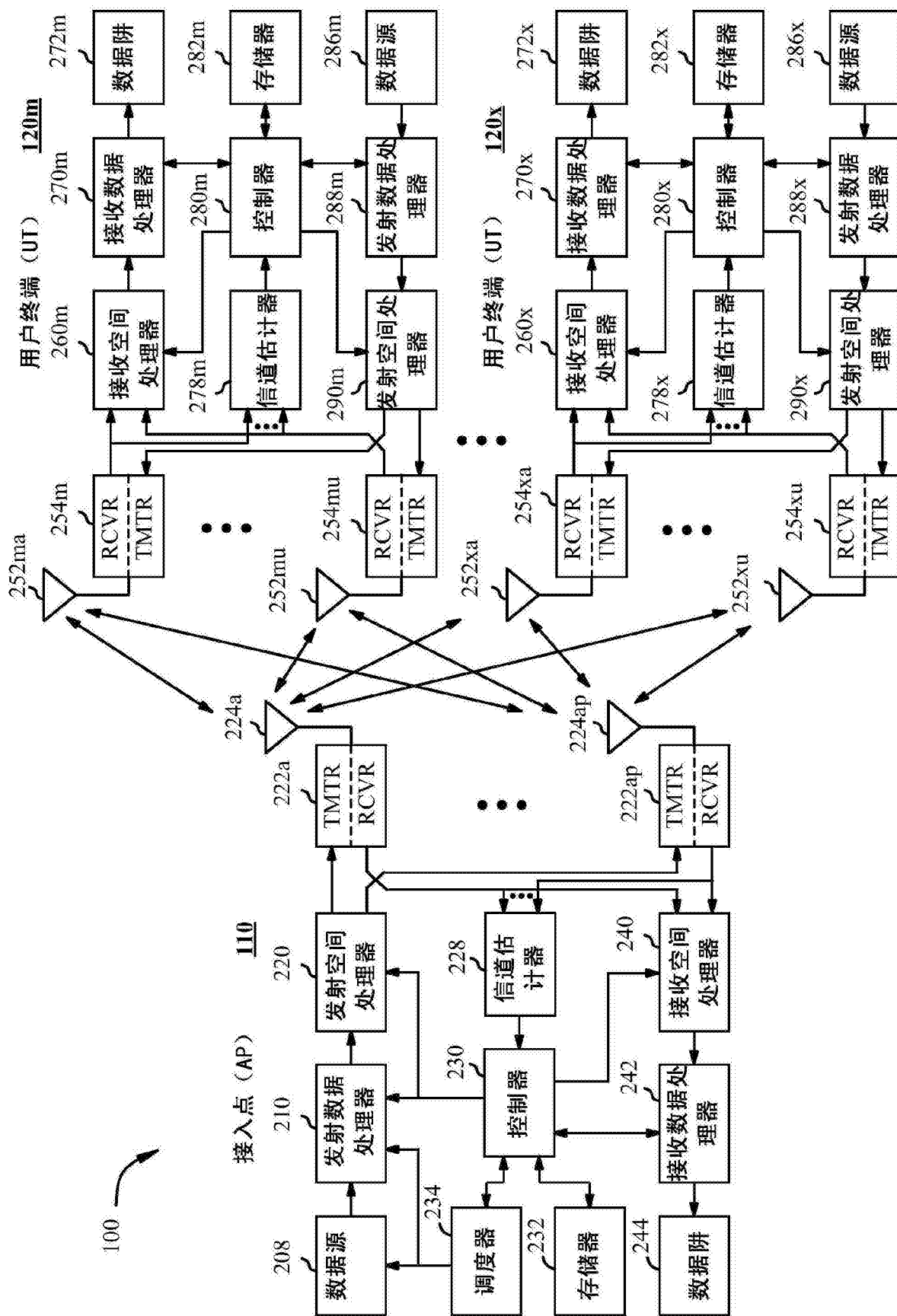


图2

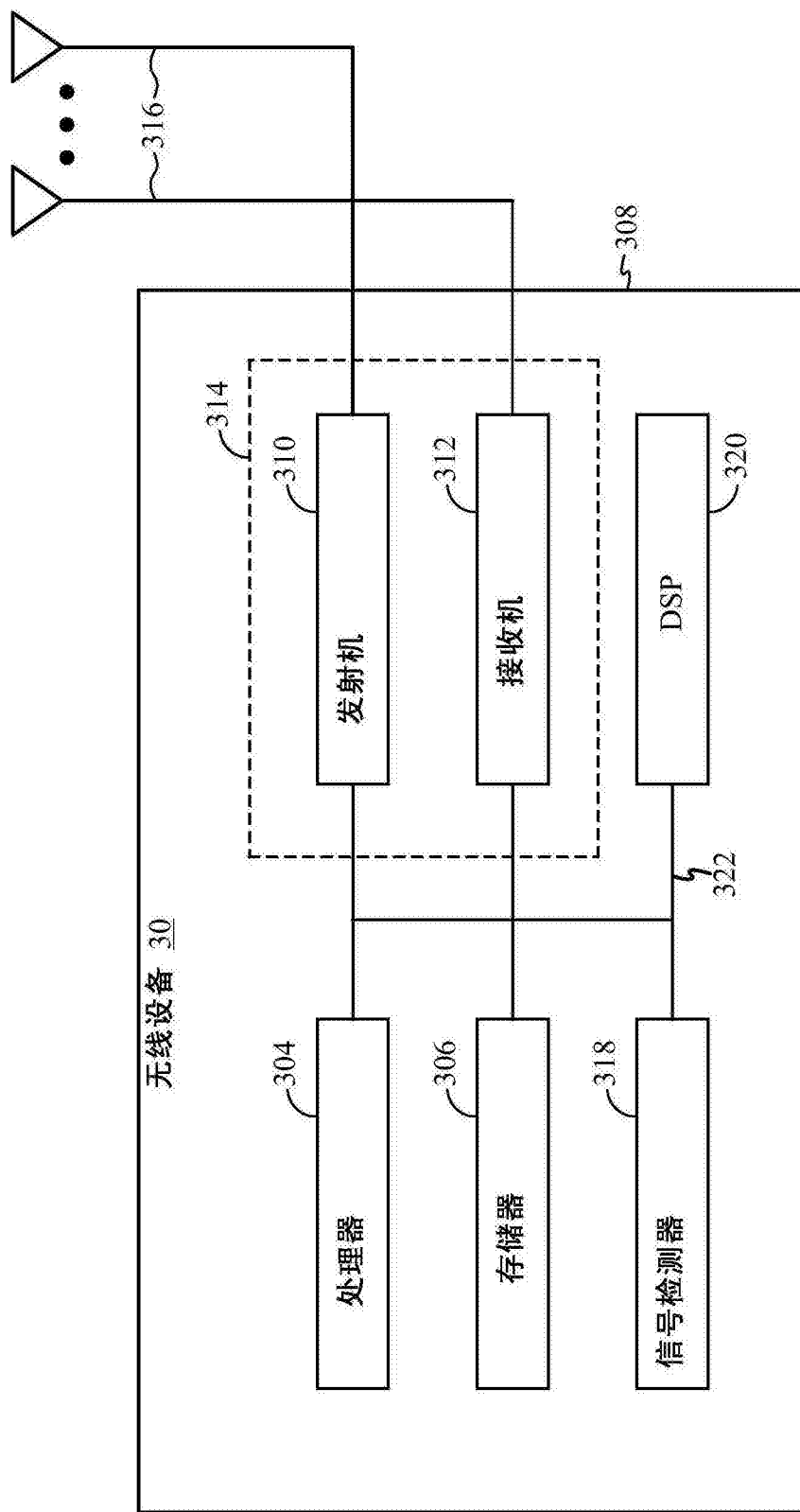


图3

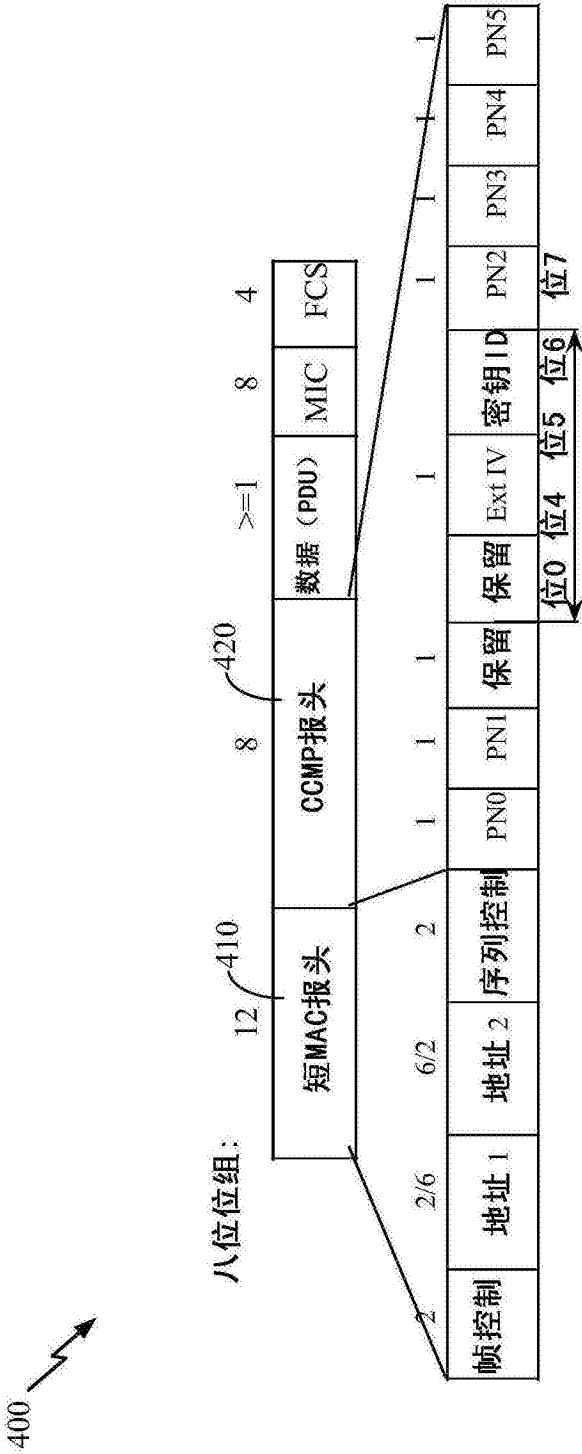


图4

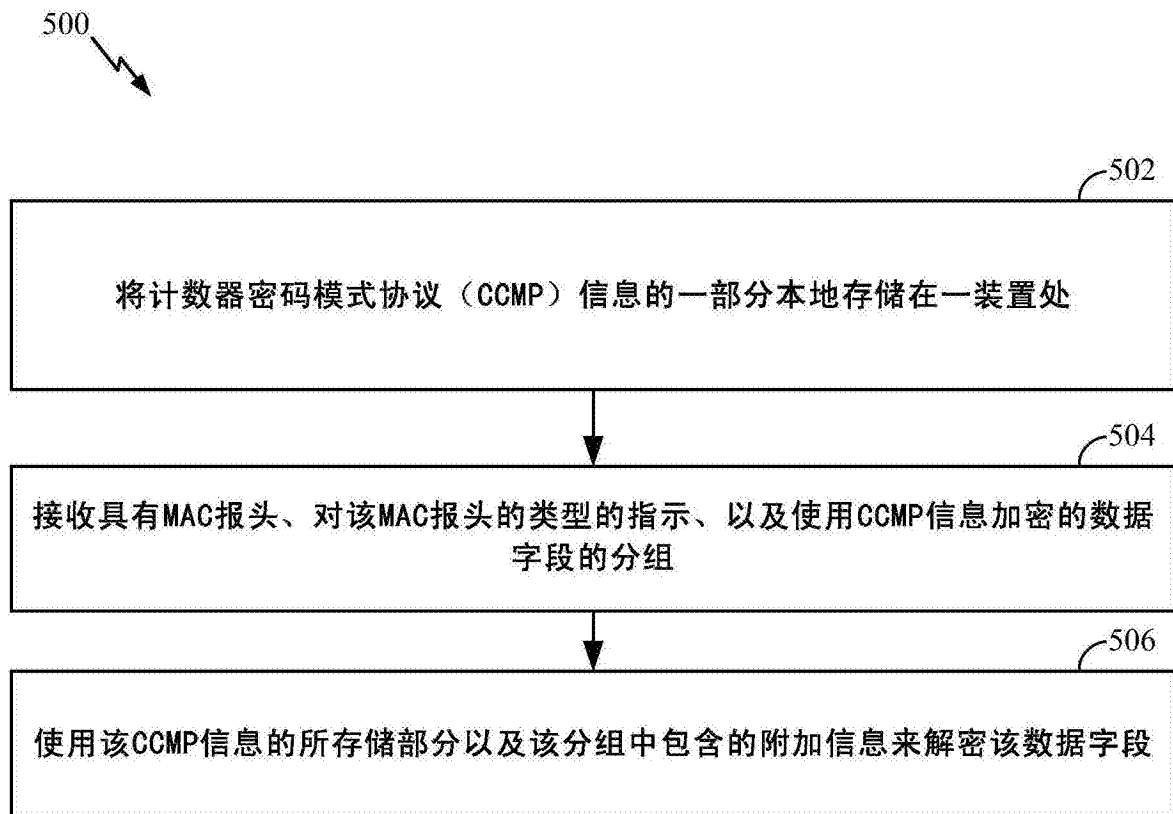


图5

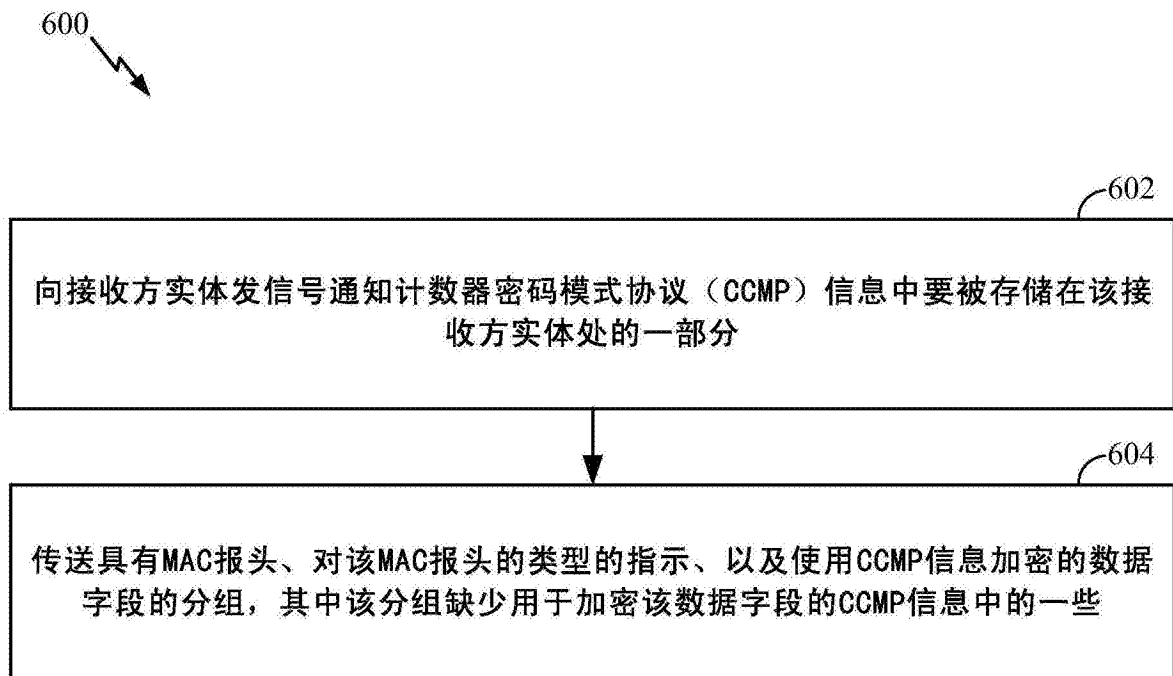


图6

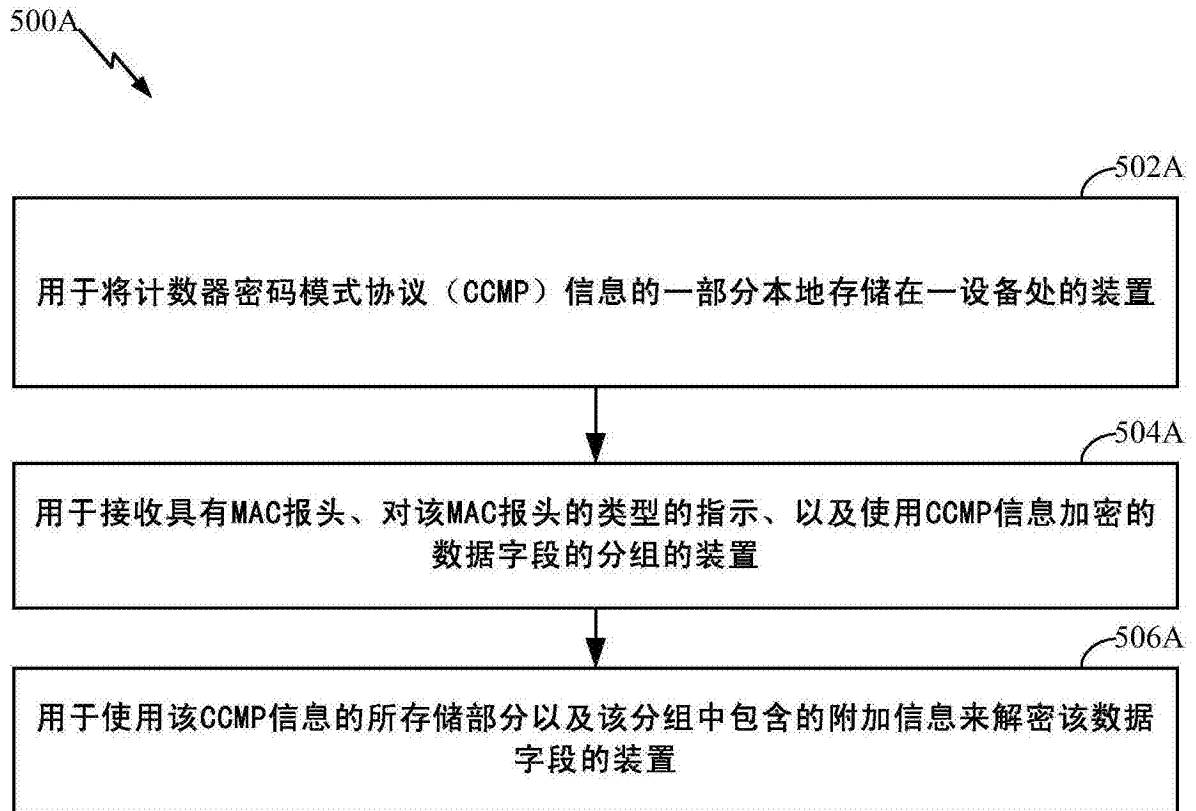


图5A

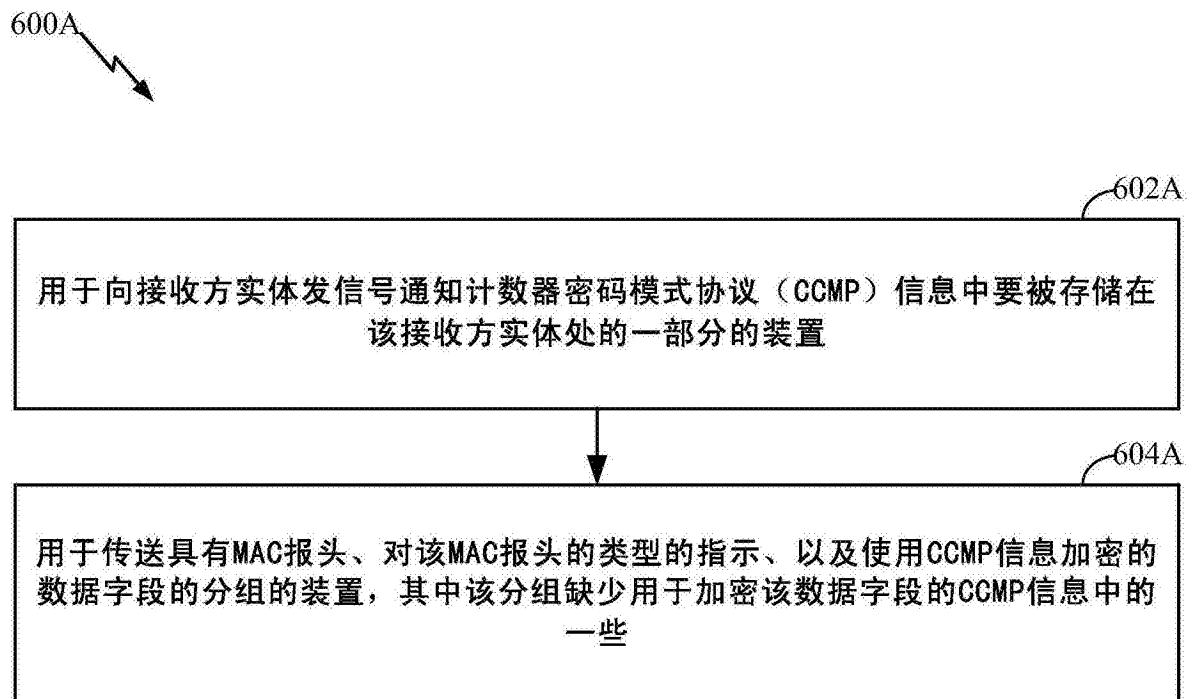
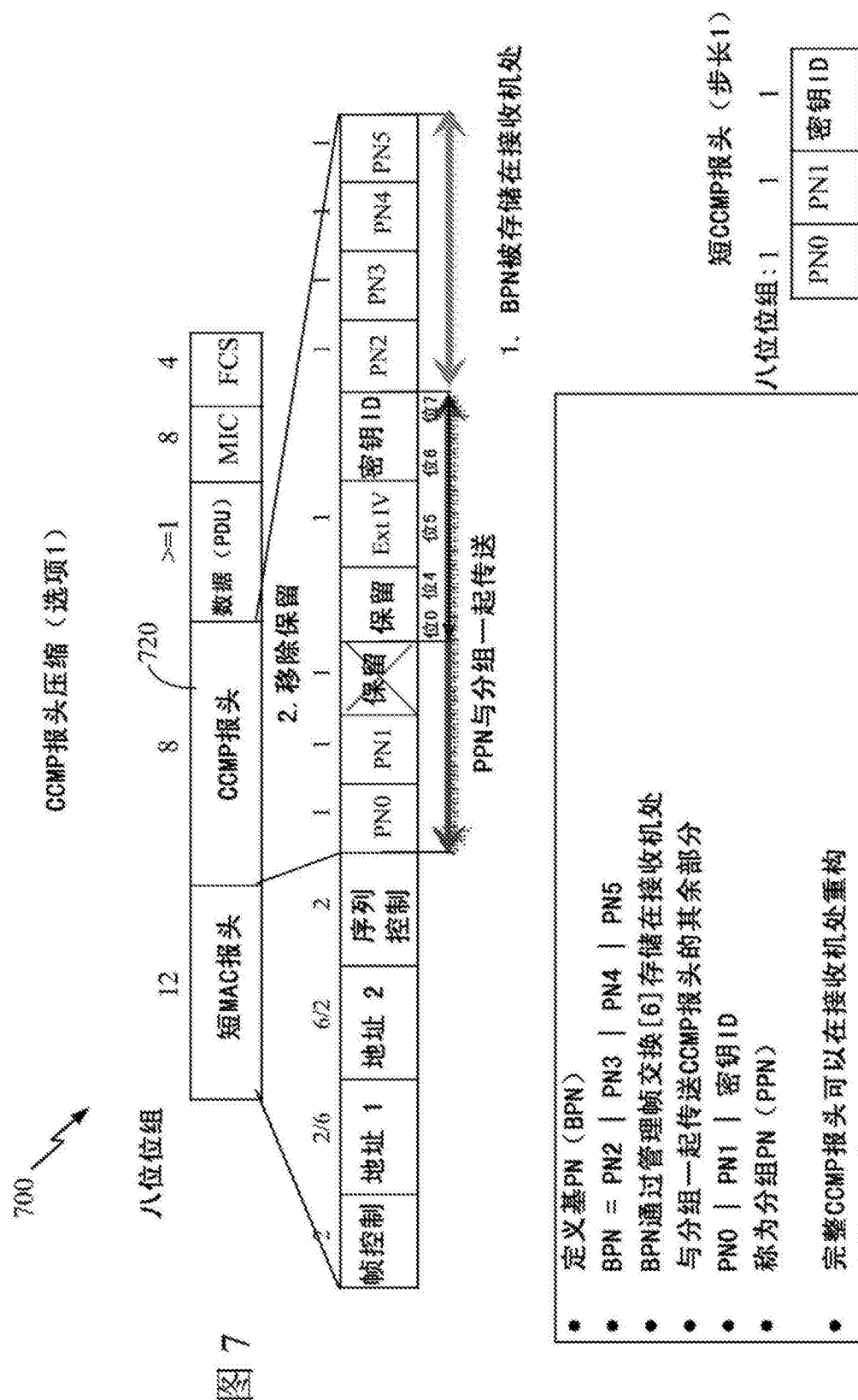
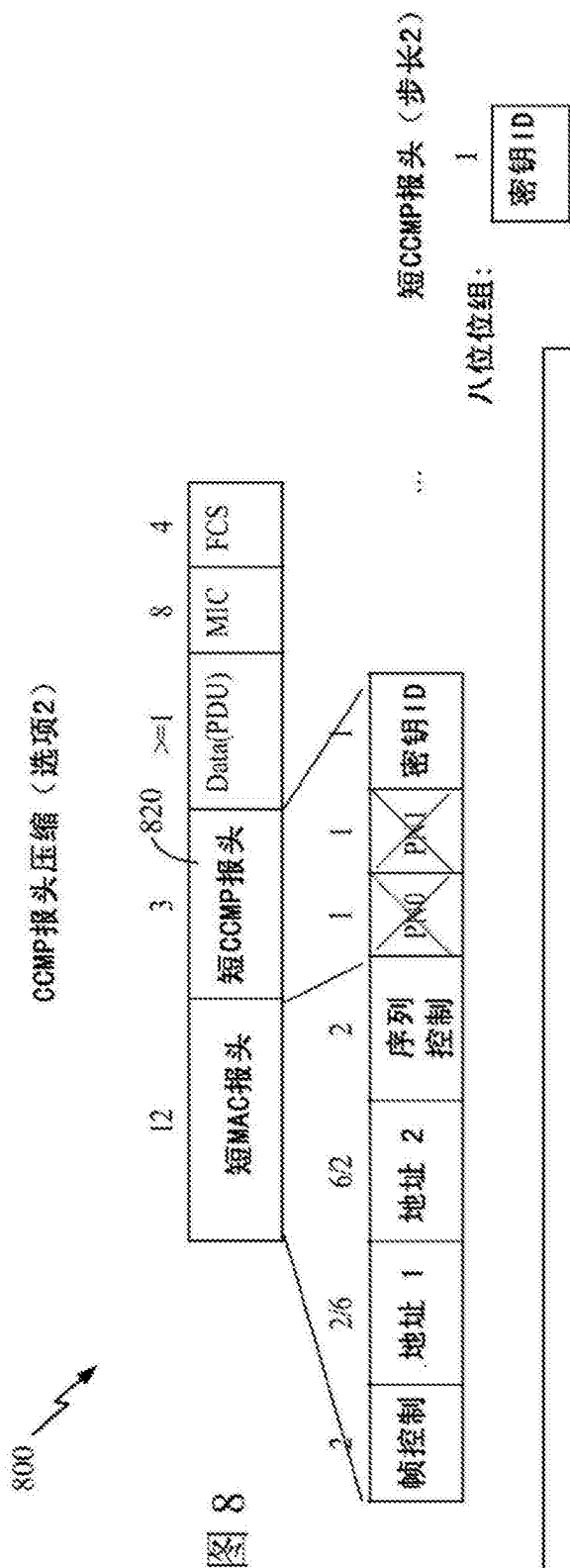


图6A

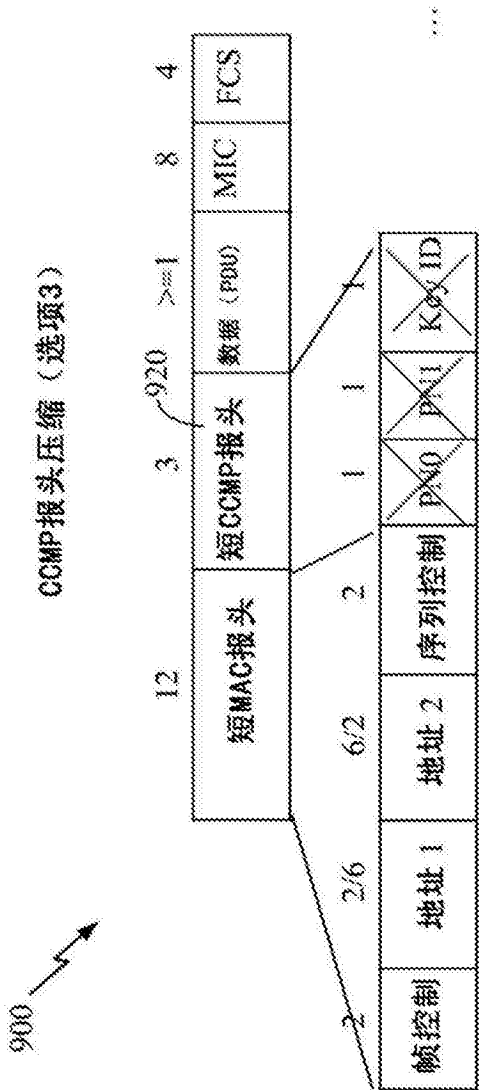


- 定义基PN (BPN)
- $BPN = PN2 \mid PN3 \mid PN4 \mid PN5$
- BPN通过管理帧交换[6]存储在接收机处
- 与分组一起传送CCMP报头的其余部分
- $PN0 \mid PN1 \mid$ 密钥ID
- 称为分组PN (PPN)
- 完整CCMP报头可以在接收机处重构
- 串接PPN $\mid$ BPN
- BPN需要在PN0 $\mid$ PN1翻转之际更新
- 对于11ah应用而言, 基于16位的翻转预期非常低
- CCMP报头从8个八位位组缩减为3个八位位组
- 只有PN0 $\mid$ PN1 $\mid$ 密钥ID八位位组需要连同分组一起传送



- 如果允许序列控制担当PNO | PN1, 则进一步压缩是可能的
 - PNO | PN1 = SC (= SN | FN)
 - 在MSDU未分段时分组号按16的步长增加
 - 这意味着PN有效地缩减4位
- CCMP报头缩减为仅1个八位组
 - 密钥ID八位组需要连同分组一起传送

图 8A



- 通过移除密钥ID八位位组，进一步压缩是可能的
 - 对于CCMP, Ext IV总是1
 - 密钥更新对于单播话务而言从不发生，并且群话务不使用短MAC报头，所以密钥ID也可被省略
- CCMP报头基本上从短MAC报头中消除
 - PNO | PN1 | = SC

图9