[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/12 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410088014.X

[45] 授权公告日 2009 年 5 月 20 日

[11] 授权公告号 CN 100490373C

[22] 申请日 2004.10.28
[21] 申请号 200410088014.X
[30] 优先权
[32] 2003.10.29 [33] US [31] 10/694,881
[73] 专利权人 诺基亚公司
地址 芬兰埃斯波
[72] 发明人 阿托·帕林 马库·A.·奥克萨宁
哈莱尔德·卡吉 朱哈·萨洛坎尼尔
[56] 参考文献
CN1290438A 2001.4.4
EP1274194A1 2003.1.8
WO99/38302A1 1999.7.29
审查员 庄 湧

[74] 专利代理机构 北京市中咨律师事务所
代理人 杨晓光 李 峥

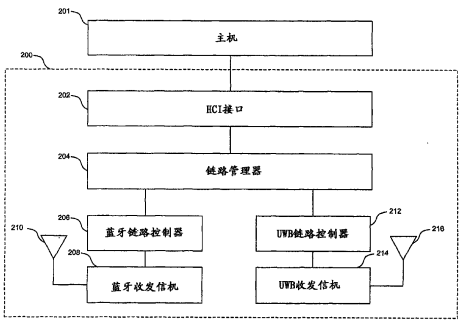
权利要求书 3 页 说明书 16 页 附图 12 页

[54] 发明名称

用于提供通信安全的方法和系统

[57] 摘要

从数据流生成被保护的内容流在短程无线通信网络内提供了增强的安全性。 通过第一短程通信链路传送所述被保护的内容流。 此外，通过第二链路传送用于将所述被保护的内容流转换成数据流的信息。 所述第一链路可能是超宽带(UWB)链路，而所述第二链路是蓝牙链路。



1、一种提供通信安全的方法，所述方法包括:

（a）从数据流中生成被保护的内容流;

（b）通过第一短程无线电通信链路传送所述被保护的内容流；以及

（c）通过第二短程无线电通信链路传送用于将所述被保护的内容流转换成所述数据流的信息;

其中所述被保护的内容流包括一个或多个数据分组，并且步骤（a）包括将一个或多个差错插入包含一个或多个分组的内容流中。

2、根据权利要求1的方法，其中步骤（a）还包括将所述一个或多个差错插入分组的一部分中，所述部分位于所述分组内的预定位置上。

3、根据权利要求2的方法，其中步骤（a）还包括选择所述预定位置。

4、根据权利要求2的方法，其中步骤（a）还包括利用代码生成所述一个或多个差错。

5、根据权利要求4的方法，其中步骤（c）包括通过所述第二短程无线电通信链路传送所述预定位置和所述代码。

6、根据权利要求1的方法，其中步骤（a）包括:

将所述数据流格式化为多个数据分组，每个所述数据分组都包含具有差错检测码和/或差错校正码的字段;

生成至少一个附加分组，所述附加分组包含具有差错检测码和/或差错校正码的字段；以及

将所述至少一个附加分组和所述多个数据分组设置成所述被保护的内容流。

7、根据权利要求6的方法，其中步骤（a）还包括随机选择所述至少一个附加分组在所述被保护的内容流中的位置。

8、根据权利要求6的方法，其中步骤（c）包括通过所述第二短程无线电通信链路传送所述至少一个附加分组在所述被保护的内容流中的位置。

9、根据权利要求1的方法：

其中步骤（a）包括利用加密密钥加密所述数据流；以及

其中步骤（c）包括通过所述第二短程无线电通信链路传送所述加密密钥。

10、根据权利要求1的方法：

其中步骤（a）包括利用加密密钥加密所述数据流；以及

其中步骤（c）包括通过所述第二短程无线电通信链路传送解密密钥，所述解密密钥对应于所述加密密钥。

11、根据权利要求1的方法，其中所述第一短程无线电通信链路是超宽带（UWB）链路。

12、根据权利要求1的方法，其中所述第二短程无线电通信链路是蓝牙链路。

13、一种无线通信设备，包括：

用于通过第一短程无线电通信链路接收被保护的内容流的装置，其中所述被保护的内容流包含具有一个或多个插入差错的分组；

用于通过第二短程无线电通信链路接收用于将所述被保护的内容流转换成数据流的信息的装置；

用于根据所述被保护的内容流生成数据流的装置。

14、一种无线通信设备，包括：

控制器，用于通过将一个或多个差错插入分组中，从数据流中生成包含所述分组的被保护内容流；

第一收发信机，用于通过第一短程无线电通信链路传送所述被保护的内容流；以及

第二收发信机，用于通过第二短程无线电通信链路传送用于将所述被保护的内容流转换成数据流的信息。

15、根据权利要求14的无线通信设备，其中所述第一短程无线电通信链路是超宽带（UWB）链路，所述第二短程无线电通信链路是蓝牙链路。

16、一种无线通信设备，包括：

超宽带收发信机，用于从超宽带通信链路接收被保护的内容流，其中所述被保护的内容流包含具有一个或多个插入差错的分组；

蓝牙收发信机，用于从蓝牙通信链路接收用于将所述被保护的内容流转换成数据流的信息；以及

控制器，用于根据所述被保护的内容流生成所述数据流。

17、一种处理器，包括：

用于使所述处理器从数据流中生成被保护的内容流的装置；

用于使所述处理器通过第一短程无线电通信链路传送所述被保护的内容流的装置；以及

用于使所述处理器通过第二短程无线电通信链路传送用以将所述被保护的内容流转换成数据流的信息的装置；

其中所述被保护的内容流包含一个或多个数据分组，并且所述用于使处理器生成被保护的内容流的装置包括使所述处理器将一个或多个差错插入包含一个或多个分组的数据流中的装置。

18、一种提供通信安全的方法，包括：

从第一短程无线电通信链路接收被保护的内容流，其中所述被保护的内容流包含具有一个或多个插入差错的分组；

从第二短程无线电通信链路接收用以将所述被保护的内容流转换成数据流的信息；以及

根据所述被保护的内容流生成所述数据流。

用于提供通信安全的方法和系统

技术领域

本发明涉及无线通信。本发明尤其涉及用于提供通信安全的技术。

背景技术

通过短程无线通信网传送的信息通常易受窃听设备的窃听。当传输被窃听时，关于个人的隐私可能被公开。此外，传输的窃听可能会降低各种形式内容的价值，例如多媒体娱乐、音乐和软件。因此，需要阻止非计划接收人窃听无线通信。

当前存在着各种用于保护内容的技术。这些技术包括借助诸如加密密钥的机制来加密内容。一旦被接收，预定的接收人（其还处理所述加密密钥或对应解密密钥）会解密所传送的内容。但是，根据所述技术，所使用的加密密钥在性质上是固定的。因此，如果窃听者得到所使用的密钥，则可以使用所述密钥来解密所传送的数据。

存在着各种形式的短程网络。由于在 2002 年得到联邦通信委员会（FCC）的批准，超宽带（UWB）技术已变成用于短程无线通信的有利解决方案，因为它们允许设备以相对较高的数据速率交换信息。

尽管用于短程网络的 UWB 系统相对较新，它们的传输技术几十年前就众所周知了。实际上，当海因里希.赫兹在 1887 发现无线电波时，第一次无线电传输是借助 UWB 技术实现的。该发明是借助火花隙发射机完成的，其可被视为早期的 UWB 无线电。后来，这种发射机被禁用了，因为其发射宽谱传输。

最近，FCC 法令允许在 3.1 和 10.6 GHz 之间的频带内用于通信目的的 UWB 传输。但是，对于这种传输而言，谱线密度必须在-41.3 dBm/MHz 之下，且所使用带宽必须高于 500 MHz。

许多UWB传输技术可以满足这些要求。一种常见且实用的UWB技术被称为脉冲无线电（IR）。在IR中，使用在时间上以间隙分离的短基带脉冲来传送数据。因此，IR并不使用载波信号。这些间隙使得IR与常规连续波无线电相比免受多径传播问题。RF门控是IR的特殊类型，其中所述脉冲是门控RF脉冲。所述的门控脉冲是在具有某种脉冲波形的时域内被屏蔽的正弦波。

IR传输设备便利了相对简单的发射机设计，其通常需要脉冲生成器和天线。这种设计无需功率放大器，因为传输功率要求较低。此外，这种设计通常不需要诸如压控振荡器（VCO）和混频器的调制部件，因为所述脉冲是基带信号。

一般而言，IR接收机设计比其对应发射机设计更为复杂。但这些设计通常要比常规接收机设计简单许多，因为它们通常不使用中频（IF）信号或滤波器。但为了满足光谱要求，IR脉冲必须持续时间非常短（例如两毫微秒）。这种要求对接收机定时精确性提出了严格的定时要求。满足这些要求也可以向IR接收机提供精确的时间解决方案和定位性能。

其它短程网络同样存在，但无法提供UWB所提供的高数据速率。一种所述网络是蓝牙。蓝牙定义了一种短程无线电网络，其最初旨在代替电缆。其可被用于生成最多八个设备的自组织网络，其中一个设备被称为主设备。其它设备被称为从设备。所述从设备可与所述主设备通信，并经由所述主设备相互通信。2001年2月22日蓝牙特别利益组的“蓝牙系统技术规范”卷1和2，核心与简介：版本1.1描述了蓝牙设备操作的原理和通信协议。该文献整体并入本文作为参考。所述设备在为工科医（ISM）应用一般使用保留的2.4 GHz无线电频带内操作。蓝牙设备被设计为在其通信范围内找到其它蓝牙设备，以及所述蓝牙设备所提供的业务。

其它短程网络标准包括IEEE 802.11x、IEEE802.15、IrDa以及HIPERLAN。

发明内容

本发明在短程无线通信网络内提供了增强的安全性。因此，本发明指向根据从数据流生成被保护的内容流，并通过第一短程通信链路传送所述被保护的内容流的方法和设备。此外，所述方法和设备通过第二短程通信链路传送用于将所述被保护的内容流转换成数据流的信息。所述第一链路是 UWB 链路，而所述第二链路是蓝牙链路。

所述被保护的内容流可能包括一个或多个分组，每个所述分组都包括插入预定位置的差错。因此，所述用于将所述被保护的内容流转换成数据流的信息包括差错位置和用于生成所述差错的代码。这些差错的位置可随机选择。诸如基于多项式代码的代码可被用于生成所述差错。此外，所述分组可能包括差错检测码和/或差错校正码。

在本发明的一些方面中，可通过将所述数据流格式化为多个数据分组、生成至少一个附加分组并将所述附加分组和所述数据分组设置为被保护的内容流来生成所述的被保护的内容流。因此，所述用于转换的信息包括所述附加分组的位置。所述附加分组的位置可随机选择。在这些方面中，每个所述数据分组和附加分组都包括具有差错检测码和/或差错校正码的字段。

在本发明的另一些方面中，通过将所述数据流置于多个分组内来生成所述的被保护的内容流，每个所述分组都具有所设置的差错校正码。在这一点处，差错被注入所述分组，从而使得对应差错校正码无法校正所述差错。这些差错的值和位置被包括在所述用于转换的信息内，且可随机选择。

同样，可通过加密密钥来加密所述数据流来生成所述的被保护的内容流。在某些方面，所述用于转换的信息包括用于解密所述的受保护数据流的密钥。所述密钥可能是所述加密密钥或对应的解密密钥。

本发明还指向从所述第一短程通信链路接收所述被保护的内容流，并从所述第二短程通信链路接收用于将所述的被保护的内容流转换成数据流的信息的方法和设备。一旦所述信息被接收，可根据所述的被保护的内容流生成所述数据流。

以下描述和附图将使得本发明的其它特征和优点变得清晰。

附图说明

在所述附图中，相同附图标记一般指示相同的、功能类似的和/或结构类似的单元。单元最先出现的附图由附图标记的最左边数字指示。以下将参考所述附图来描述本发明，在所述附图中：

图 1 示出了示例性操作环境；

图 2 是根据本发明实施例的示例性通信设备体系结构的方框图；

图 3 是示例性通信设备实施方式的方框图；

图 4 示出了示例性传输分组；

图 5 是安全通信技术的流程图；

图 6 是根据第一技术的被保护的内容流生成的流程图；

图 7 示出了根据第一技术的用于执行内容流生成的实施方式；

图 8 是根据第二技术的被保护的内容流生成的流程图；

图 9 示出了根据第二技术的用于执行内容流生成的实施方式；

图 10 是根据第三技术的被保护的内容流生成的流程图；

图 11 示出了根据第三技术的用于执行内容流生成的实施方式；以及

图 12 是由接收设备执行的操作顺序的流程图。

具体实施方式

I. 操作环境

在详细描述本发明之前，描述使用本发明的环境是有帮助的。因此，图 1 示出了一种包括无线通信设备 102 和 104 的操作环境。

设备 102 和 104 能够参与通过至少两种不同类型短程无线链路的无线通信。例如，设备 102 和 104 可支持蓝牙和 UWB 链路两者。

设备 102 和 104 都具有以覆盖区定义的通信范围。如图 1 所示，覆盖区 103 定义了设备 102 的通信范围，而覆盖区 105 定义了设备 104 的通信范围。这些覆盖区示出了一个其中对应设备可通过两种不同类

型链路（例如蓝牙和 UWB）通信的范围。

在图 1 的环境中，设备 102 和 104 在相互的通信范围内。因此，第一无线通信链路 110 和第二无线通信链路 112 在设备 102 和 104 之间得以建立。这些链路可能是不同类型的。例如，第一链路 110 可能是 UWB 链路，而第二链路 112 可能是蓝牙链路。

在建立这些链路中可使用各种技术。例如，设备 102 可通过第一链路 110 通信，以建立第二链路 112，并启动通过链路 112 的通信。这种技术的实例在 2003 年 9 月 12 日公开的未决美国专利申请“用于建立无线通信链路的方法和系统”，代理摘要 No.4208-4144（应用序列号当前未指定），作者 Arto Palin、Juha Solokannel 以及 Jukka Reunamaki 内描述。将此申请全部在此引入作为参考。

在图 1 的环境中，借助设备 102 通过第一链路 110 以受保护（例如扰频）格式发射内容，本发明提供了安全通信。此外，设备 102 通过第二链路 112 以安全消息的形式传送扰频所述被保护的内容所需的信息。以这种方式使用两条链路提供了增强的安全性，因为窃听设备必须从两条链路接收传输，以去扰频所述的被保护的内容。此外，在本发明的一些方面中，可动态改变适合于扰频所述内容的属性，以使窃听所述内容变得更困难。当动态改变发生时，可能会经由链路 112 发射新的安全消息，以将所述新的属性通知预定接收者。

II.无线通信设备

图 2 是示出了根据本发明的可能用于设备 102 和 104 的无线通信设备体系结构的方框图。所述体系结构可能会与本文所述用于通过两个通信链路安全传送内容的各种系统与方法一起使用。尽管以上在蓝牙和 UWB 通信的语境内描述了所述体系结构，但其可与其它无线通信技术一起使用。

图 2 的设备体系结构包括主机 201，所述主机 201 耦合到段 200。主机 201 负责包括用户应用和更高协议层的功能，而段 200 负责低层协议，例如蓝牙（例如基本速率、中间速率或高速率）、UWB 和/或其它特定通信。

如图 2 所示，段 200 包括主机控制器接口（HCI）202、链路管理器 204、蓝牙（BT）链路控制器 206、蓝牙（BT）收发信机 208、天线 210、UWB 链路控制器 212、UWB 高速率（UWB/HR）收发信机 214 和天线 216。

链路管理器 204 执行与蓝牙链路和 UWB 链路建立、安全和控制相关的功能。所述功能涉及在远程设备处发现对应的链路管理器，并根据所述链路管理协议（LMP）与其通信。具体而言，链路管理器 204 与远程设备处的链路管理器交换 LMP PDU。

链路管理器 204 通过 HCI 202 与主机 201 交换信息。所述信息可能包括从主机 201 接收的指令，以及传送到主机 201 的信息。HCI 202 定义一组为所述信息交换提供的消息。

BT 链路控制器 206 作为链路管理器 204 与 BT 收发信机 208 之间的中介物操作。链路控制器 206 还执行蓝牙传输的基带处理，例如差错校正编码和译码。此外，链路控制器 206 根据物理层协议，在远程设备的对应链路控制器之间交换数据。物理层协议的实例包括诸如自动重复请求（ARQ）协议的重新传输协议。

BT 收发信机 208 耦合到天线 210。收发信机 208 包括（结合天线 210）与诸如远程设备 104 的设备交换无线蓝牙信号的电子仪器。所述电子仪器包括调制器、解调器、放大器和滤波器。

UWB 链路控制器 212 作为链路管理器 204 与 UWB/HR 收发信机 214 之间的中介物操作。链路控制器 212 还执行 UWB 传输的基带处理，例如差错校正编码和译码。此外，链路控制器 212 根据物理层协议，在远程设备的对应链路控制器之间交换数据。所述物理层协议的实例包括诸如自动重复请求（ARQ）协议的重新传输协议。

UWB/HR 收发信机 214 耦合到天线 216。收发信机 214 包括（结合天线 216）与诸如远程设备 104 的设备交换无线 UWB 或 HR 信号的电子仪器。对于传输 UWB 信号而言，所述电子仪器可能包括脉冲生成器。对于接收 UWB 而言，所述电子仪器可能包括定时电路和滤波器。

图 2 的体系结构可被实施在硬件、软件、固件或其任何组合内。图 3 示出了一种实施方式。所述实施方式包括处理器 310、存储器 312 和用户接口 314。此外，图 3 的实施方式还包括蓝牙收发信机 214、天线 216、UWB 收发信机 220 和天线 222。如参照图 2 所述，实施收发信机 214 和 220。

如图 3 所示，处理器 310 耦合到收发信机 214 和 220。处理器 310 控制设备操作。处理器 310 可能会与一个或多个微处理器一起实施，每个所述微处理器能够执行存储在存储器 312 内的软件指令。

存储器 312 包括随机存取存储器（RAM）、只读存储器（ROM）和/或闪存，并以数据形式存储信息以及软件成分（本文也被称为模块）。所述软件成分包括可由处理器 310 执行的指令。各种类型的软件成分都可被存储在存储器 312 内。例如，存储器 312 可能会存储控制收发信机 214 和 220 的操作的软件成分。此外，存储器 312 可能还会存储提供主机 202、HCI 接口 208、链路管理器 210、链路控制器 212 和 UWB 模块 218 的功能的软件成分。

此外，存储器 312 可能会存储控制通过用户接口 314 交换信息的软件成分。如图 3 所示，用户接口 314 还耦合到处理器 310。用户接口 314 便利了与用户的信息交换。图 3 示出了所述用户接口 314 包括用户输入部分 316 和用户输出部分 318。用户输入部分 316 可能包括允许用户输入信息的一个或多个设备。所述设备的实例包括键盘、触屏和话筒。用户输出部分 318 允许用户从 WCD 102 接收信息。因此，用户输出部分 318 可能包括各种设备，例如显示器、一个或多个音频扬声器。示范性显示器包括液晶显示器（LCD）和视频显示器。

图 3 所示的单元可能被根据各种技术耦合。一个所述技术包括通过一个或多个总线接口耦合收发信机 214 和 220、处理器 310、存储器 312 和用户接口 314。此外，每个所述部件都耦合到功率源，例如可移动和可充电的电池组（未显示）。

III.分组通信

根据本发明，通过经由第一通信链路传送被保护的内容，并经由

第二通信链路传送安全消息来提供安全通信。所述的被保护的内容可能采取分组形式。图 4 示出了经由所述第一通信链路传输的示范性分组格式。

图 4 示出了分组（也被称为帧）400。分组 400 包括有效负荷部分 402，所述有效负荷部分 402 包括数据（即内容）和开销部分 404。开销部分 404 可能包括与传送所述数据相关的信息，例如信源和/或目的地地址。

此外，开销部分可能还包括差错检测和/或差错校正码 406，分组 400 的接收机可使用所述差错检测和/或差错校正码 406 来检测和/或校正差错有效负荷部分 402。在传输期间内，所述差错可能是由诸如电磁噪声和干扰传输的信源引起的。

此外，根据本发明，差错可能是由传送所述被保护的内容流的设备故意引入的。所述差错引入生成扰频传输。然后可在一个或多个安全消息内，经由所述第二链路传送关于故意引入的差错的细节。在接收所述扰频传输和所述（多个）安全消息时，所述接收设备可能会使用所述（多个）安全消息内的信息来扰频所述传输。根据所述技术，窃听所述的被保护的内容流同样需要接收所述（多个）安全消息。

代码 406 包括差错校正码。所述误码可能是诸如汉明码的组码。然而，也可使用其它差错校正码，例如李特-所罗门编码和维特比编码。在实施例中，代码 406 可能包括链接码，例如内码（李特-所罗门编码）和外码（例如维特比）。作为选择或附加地，代码 406 可能包括差错检测码，例如循环冗余校验（CRC）。

Ⅳ.安全通信

图 5 是由诸如设备 102 的通信设备执行的操作顺序的流程图。所述顺序包括可以各种顺序执行的多个步骤。此外，可同时执行任何数量的所述步骤。此外，可能会对所述顺序做出修改，例如执行附加步骤。

所述过程开始于步骤 502，其中所述通信设备和远程设备（例如设备 104）进入短程通信邻近。然后，在步骤 504 中，所述通信设备

与所述远程设备建立第一和第二通信链路。所述链路可能被连续建立。例如，可能会建立第二链路（例如蓝牙链路），然后所述第二链路用于建立所述第一链路（例如 UWB 链路）。所述技术的实例在 2003 年 9 月 12 日公开的未决美国专利申请领域，“用于建立无线通信链路的方法和系统”代理摘要 No.4208-4144（当前未指配的专利连续号）内描述。

如以上参照图 1 所述，所述第一和第二链路可能是不同类型的短程链路。例如，所述第一链路可能是超宽带（UWB）链路，而第二链路可能是蓝牙链路。然而，可使用其它的链路类型。其它的链路类型的实例包括那些与诸如 IEEE 802.11x、IEEE 802.15、IrDA 和/或 HIPERLAN 的标准兼容的链路。

在步骤 506 中，所述通信设备选择一个或多个安全属性。如以下所述，所述属性的实例包括安全技术、误码、差错位置和/或加密密钥。

在步骤 508 中，从应用接收数据流。所述应用可能在所述设备上运行，例如在主机 201 内。然而，就其它方面而言，所述应用可能在耦合到所述通信设备的独立设备上运行。应用实例包括服务器应用、视频应用、电话应用以及其它应用。

在步骤 510 中，所述设备从所述数据流生成被保护的内容流。所述生成基于在步骤 506 内选择的（多个）安全属性。步骤 510 可能包括将所述数据流格式化为一个或多个数据分组。如以上参照图 4 所述，每个所述数据分组都可能包括具有差错检测码和/或差错校正码的字段。所述代码的实例包括 CRC 和汉明码。

在步骤 512 中，所述设备生成安全消息。所述消息包括用于将所述的被保护的内容流转换为所述数据流的信息。所述信息的实例包括误码、差错位置和/或加密密钥。

在步骤 514 中，所述设备将所述的被保护的内容流通过所述第一通信链路传送到远程设备（例如设备 104）。

在步骤 516 中，所述设备将所述安全消息通过所述第二通信链路传送到所述远程设备。可能会同时执行步骤 514 和 516。

对于本领域技术人员而言，显然可重复图 5 的步骤。此外，本发明提供了可动态改变的安全属性。例如，步骤 518 示出了所述通信设备可能会在传输所述的被保护的内容期间的任何时点，改变安全属性（例如误码、差错位置和/或加密密钥）。如果改变任何安全属性，则图 5 示出了操作继续到步骤 512，其中生成新的安全消息。所述新消息传递用于根据当前安全属性将所述的被保护的内容流转换为所述数据流的信息。

如上所述，在步骤 510 内生成受保护的内容流。各种技术可能用于生成此内容流。以下将参照图 6-11 描述所述技术的示例。

Ⅴ.差错插入

第一种技术涉及将差错插入分组的位置。所述技术的实例在图 6 的流程图内说明。如图 6 所示，所述技术包括步骤 602，其中所述通信设备在步骤 510 内选择所述数据分组内的一个或多个位置。所述选择可能是随机的。

在步骤 604 内，所述通信设备以代码生成一个或多个差错。所述代码可能基于多项式。

在步骤 606 中，所述通信设备将在步骤 604 内生成的差错插入所述分组的部分。所述分组的所述部分位于在步骤 602 内选择的位置。

步骤 606 之后是步骤 608。在此步骤中，所述通信设备为每个所述分组设置所述差错校正码。

如以上参照图 5 所述，所述通信设备在步骤 516 内传送一个或多个安全消息。当执行图 6 的步骤时，所述一个或多个安全消息传递在步骤 602 内选择的预定位置，以及用于在步骤 606 内生成一个或多个差错的代码。

图 7 是可能用于使用参照图 6 所述技术的实施方式的方框图。所述实施方式包括位置选择模块 702、误码生成器 704、安全消息模块 706、分组生成器 708、差错插入模块 710 和编码器 711。图 7 的单元可能会在硬件、软件、固件或其任何组合内实施。所述实施方式被作为实例提供。其它用于执行所述差错插入技术的实施方式同样在本发

明范围内。

位置选择模块 702 选择数据分组内的一个或多个位置来插入差错。所述位置可能是随机选择的。所选择的位置可规定跨越一个或多个邻接符号（例如比特）的分组部分。图 7 示出了所述位置选择模块 702 生成指示被选择为插入差错的（多个）位置的信号 720。例如，图 7 示出了选择三个有效负荷位置（符号 N、3 和 2）。所述三个位置规定插入每个分组的差错的重复模式。

误码生成器 704 生成代码 722，所述代码 722 用于将差错插入数据分组内的位置选择模块 702 所选择的位置处。所述代码可能是定义移位寄存器操作的多项式。

分组生成器 708 接收数据流 724，并将其格式化为数据分组流 726，所述数据分组流 726 包括多个分组 730。所述分组可能会采取参照图 4 描述的格式。如图 7 所示，差错插入模块 710 接收数据分组流 726、位置信号 720 和代码 722。差错插入模块 710 从所述输入生成扰频内容流 727。扰频内容流 727 包括多个分组 732。图 7 示出了每个所述分组包括差错插入模块 710 所插入的差错 734。

差错插入模块 710 包括存储器 712、插入控制器 714、路由模块 716 和移位寄存器 718。存储器 712 存储由位置信号 720 指示的（多个）位置。插入控制器 714 基于存储在存储器 712 内的（多个）位置生成插入信号 731。当数据分组流 726 位于所选择（多个）位置中的一个时，所述信号被发送到路由模块 716。

在接收插入信号 730 时，路由模块 716 将数据分组流 726 内的符号发送到移位寄存器 718。移位寄存器 718 根据代码 722 所定义的多项式操作。因此，移位寄存器 718“扰频”其从路由模块 716 接收的数据分组流 726 的部分。所述扰频导致扰频后的内容流 727。

如上所述，被保护的内容流 727 包括多个分组 732，每个所述分组都具有所插入的差错，在图 7 内以阴影指示。例如，分组 732c 包括移位寄存器 718 所插入的差错 734a-c。所述差错位于位置信号 720 所规定的位置处。

编码器 711 接收扰频后内容流 727。在接收每个分组 732 时，编码器 711 计算对应的差错检测和/或校正码。编码器 711 然后将所述代码插入所述分组 732 的差错检测/校正字段。因此，编码器 711 生成被保护的内容流 728。

安全消息模块 706 接收位置信号 720 和代码 722。模块 706 从所述输入生成将通过所述第二短程通信链路发送到远程设备的安全消息 723。如上所述，所述消息允许所述远程设备将被保护的内容流 728 转换为分组数据流 726。

图 7 的单元可能被分配给图 2 体系结构内的各个部分。在示范性分配中，位置选择模块 702 和误码生成器 704 可能包括在链路管理器 204 内，而安全消息模块 706 可能包括在蓝牙链路控制器 206 内。此外，在所述示范性分配中，分组生成器 708、差错插入模块 710 和编码器 711 可能包括在 UWB 链路控制器 212 内。

VI.附加分组生成

生成所述的被保护的内容流的第二种技术包括生成附加分组。图 8 的流程图示出了所述技术的实例。

所述技术包括步骤 802。在此步骤中，除了在步骤 510 内生成的数据分组之外，所述通信设备还生成一个或多个分组。如同在步骤 510 内生成的数据分组一样，所述（多个）附加分组还包括具有差错检测码和/或差错校正码的字段。

在步骤 804 中，所述通信设备选择所述至少一个附加分组的位置。所述位置可能是随机选择的。

步骤 804 之后是步骤 806。在此步骤中，所述通信设备将一个或多个附加分组和所述数据分组设置到所述受保护的内容流内。

当执行图 8 的步骤时，在步骤 516 内传送的（多个）安全消息包括所述（多个）附加分组在所述的被保护的内容流内的位置。

图 9 是可能用于使用参照图 8 所述技术的实施方式的方框图。所述实施方式包括位置选择模块 902、附加分组生成器 904、安全消息模块 906、分组生成器 908、分组插入模块 910 和编码器 911。图 9 的单

元可能会在硬件、软件、固件或其任何组合内实施。所述实施方式被作为实例提供。其它用于执行所述差错插入技术的实施方式同样在本发明范围内。

分组生成器 908 接收数据流 924，并将其格式化为数据分组流 926，所述数据分组流 926 包括多个分组 930。

位置选择模块 902 选择（多个）附加分组被插入数据分组流 926 内的一个或多个位置。所述位置可能是随机选择的。所选择的位置可规定跨越多个符号（例如比特）的分组的邻接部分。图 9 示出了位置选择模块 902 生成位置信号 920，所述位置信号指示被选择为插入任何附加分组的位置。

附加分组生成器 904 生成一个或多个分组 922，所述分组 922 被插入数据分组流 926 内的位置选择模块 902 所选择的（多个）位置处。所述附加分组可能包括随机生成的符号。

如图 9 所示，分组插入模块 910 接收数据分组流 926 和位置信号 920。分组插入模块 910 从所述输入生成扰频后内容流 927。扰频后内容流 927 包括数据分组流 926 的分组 930。此外，扰频后内容流 928 包括附加分组生成器 904 所生成的（多个）附加分组 922。所述附加分组位于位置信号 920 所指示的（多个）位置处。

编码器 911 接收扰频后内容流 927。在接收每个分组 932 时，编码器 911 计算并插入对应的差错检测和/或校正码。编码器然后将所述代码插入所述分组 930 和 922 的差错检测/校正字段。因此，编码器 911 生成被保护的内容流 928。

安全消息模块 906 接收位置信号 920。模块 906 从所述输入生成将通过所述第二短程通信链路发送到远程设备（例如设备 104）的安全消息 923。如上所述，所述消息允许所述远程设备将被保护的内容流 928 转换为分组数据流 926。

图 9 的单元可能被分配给图 2 体系结构内的各个部分。在示范性分配中，位置选择模块 902 和附加分组生成器 904 可能包括在链路管理器 204 内。此外，根据所述分配，安全消息模块 906 可能包括在蓝

牙链路控制器 206 内，而分组生成器 708、分组插入模块 910 和编码器 911 可能包括在 UWB 链路控制器 212 内。

Ⅶ.扩展差错注入

第三种生成所述的被保护的内容流的技术包括将差错注入在步骤 510 内生成的数据分组。图 10 示出了此技术的实例。根据此技术，所述通信设备在步骤 1002 内为每个所述数据分组设置差错检测码和/或差错校正码。

在步骤 1004 中，所述通信设备选择一个或多个差错值和位置。所述选择可能是随机的。

步骤 1004 之后是步骤 1006。在步骤 1006 中，所述通信设备将所述差错值注入到所述数据分组内的所选择位置处。所注入的差错被以使得对应差错校正码无法校正所述差错的程度注入所述数据分组。

当执行图 10 的步骤时，在步骤 516 内传送的一个或多个安全消息传递每个所注入差错的（多个）值和（多个）位置。

图 11 是可能用于使用参照图 10 所述技术的实施方式的方框图。所述实施方式包括位置选择模块 1102、误码生成器 1104、安全消息模块 1106、分组生成器 1108、差错插入模块 1110 和编码器 1111。图 11 的单元可能会在硬件、软件、固件或其任何组合内实施。所述实施方式被作为实例提供。其它用于执行所述差错插入技术的实施方式同样在本发明范围内。

位置选择模块 1102 选择差错被插入数据分组内的一个或多个位置。所述位置可能是随机选择的。所选择的位置可规定跨越一个或多个邻接符号（例如比特）的分组部分。在这种情况下，位置选择模块 1102 生成位置信号 1120，所述位置信号 1120 指示被选择为注入差错以使差错无法得到校正的相对大量位置。例如，图 11 示出了三个位置的选择。所述三个位置规定差错插入的重复模式。

误码生成器 1104 生成代码 1122，所述代码 1122 被插入所述数据分组内的位置选择模块 1102 所选择的位置处。所述代码可能是定义移位寄存器操作的多项式。

分组生成器 1108 接收数据流 1124，并将其格式化为数据分组流 1126，所述数据分组流 1126 包括多个分组 1130。如图 11 所示，数据分组流被发送到编码器 1111，所述编码器 1111 接收数据分组流 1126。对于每个分组 1130 而言，编码器 1111 计算对应的差错检测和/或校正码。编码器 1111 然后将所述代码插入所述分组 1130 的差错检测/校正字段。因此，编码器 1111 生成内容流 1127。

如图 11 所示，差错插入模块 1110 接收内容流 1127、位置信号 1120 和代码 1122。差错插入模块 1110 从所述输入生成受保护的内容流 1128。被保护的内容流 1128 包括多个分组 1132。图 11 示出了每个所述分组都包括以阴影指示的差错。如图 7 所示，分组 1132 被阴影完全覆盖，指示大量差错注入全部分组。差错注入模块 1110 可以参照图 7 所述方式实施。

如上所述，被保护的内容流 1128 包括多个分组 1132。图 11 示出了每个所述分组都包括一个或多个由模块 1110 注入的差错 1134。所述差错位于位置信号 1120 所规定的位置处。

安全消息模块 1106 接收位置信号 1120 和代码 1122。模块 1106 从所述输入生成将通过所述第二短程通信链路发送到远程设备（例如设备 104）的安全消息 1123。如上所述，所述消息允许所述远程设备将被保护的内容流 1128 转换为分组数据流 1126。

图 11 的单元可能被分配给图 2 体系结构内的各个部分。例如，位置选择模块 1102 和误码生成器 1104 可能包括在链路管理器 204 内，而安全消息模块 1106 可能包括在蓝牙链路控制器 206 内，而分组生成器 1108、差错插入模块 1110 和编码器 1111 可能包括在 UWB 链路控制器 212 内。

Ⅷ.其它技术

还可能使用其它生成被保护的内容流的技术。例如，在步骤 510 内，通过以加密密钥加密所述数据流生成所述被保护的内容流。在这种技术中，所述加密密钥和/或对应的解密密钥包括在所述安全消息内。

IX.接收机

图 12 是接收根据本发明内容的无线通信设备所执行的操作流程图。如图 12 所示，所述顺序包括步骤 1202，其中所述设备从诸如 UWB 链路的第一短程通信链路接收被保护的内容流。

在步骤 1204 中，所述设备从诸如蓝牙链路的第二通信链路接收安全消息。所述消息包括用于将所述的被保护的内容流转换为数据流的信息。因此，所述消息可能包括安全属性，例如安全技术、误码、差错位置和/或加密密钥。

在步骤 1206 中，所述设备从所述的被保护的内容流生成所述数据流。这可能基于以上参照图 6-11 描述的安全技术及其相关属性（例如，误码、位置和/或加密密钥）。可能会同时执行图 12 的步骤，例如步骤 1202 和 1204。

可以参照图 2 和 3 所述的方式实施所述接收设备。例如，步骤 1202 可能由收发信机 214 执行，步骤 1204 可能由收发信机 208 执行，而步骤 1206 可能由控制器 212 执行。所述实施方式可能在硬件、软件、固件或其任何组合内实施。

X.结论

尽管以上描述了本发明的各个实施例，但应当理解的是，所述实施例仅是借助实例示出的，并不具有限制意义。例如，尽管已描述了涉及蓝牙和 UWB 技术的实例，其它短程和远程通信技术同样在本发明范围内。

因此，对于本领域技术人员而言，在并不背离本发明精神和范围的情况下，可对形式和细节做出改变。因此，本发明的广度和范围不应当受任何上述示范性实施例限制，而是应当根据以下权利要求书及其等价物定义。

图 1

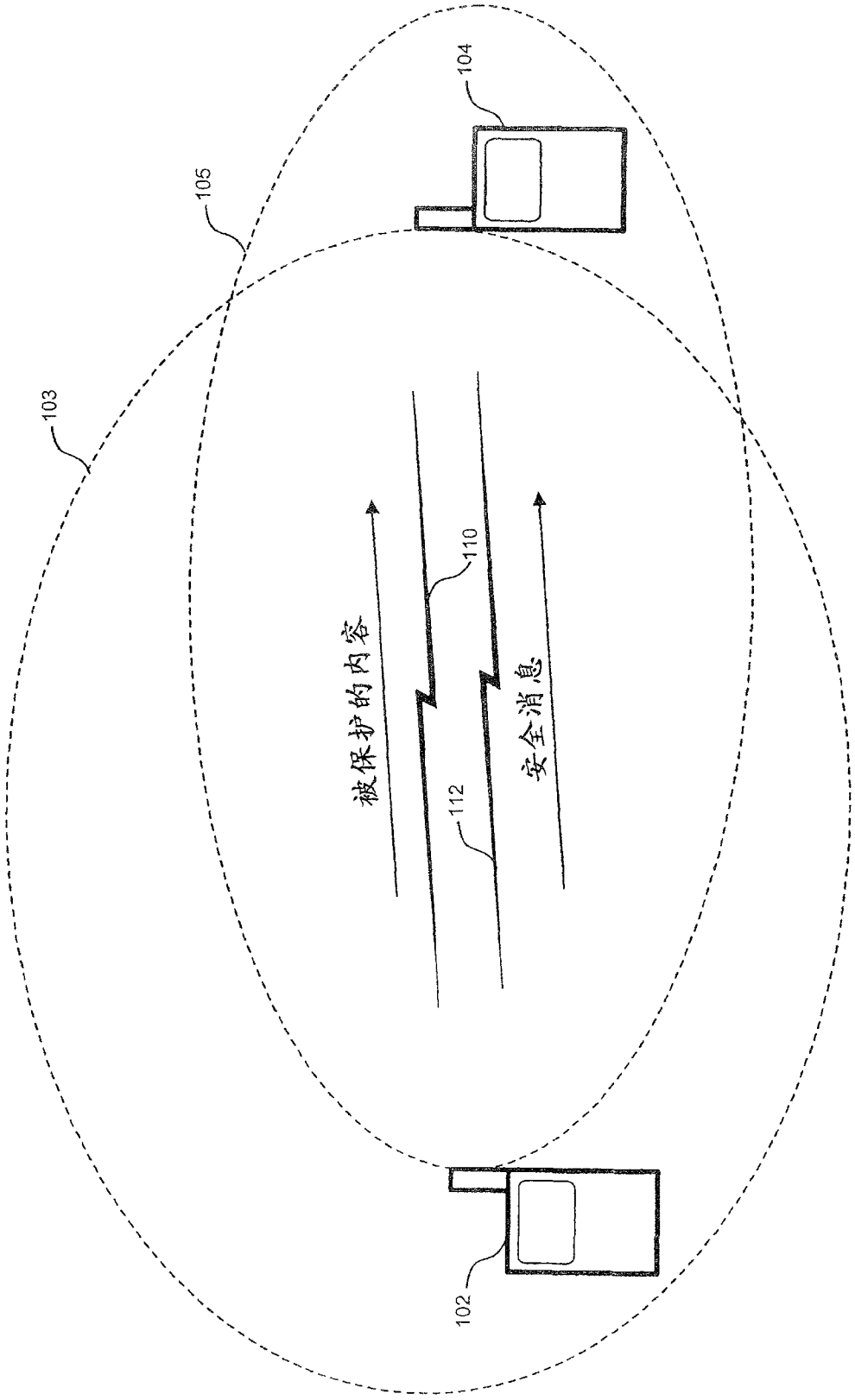


图 2

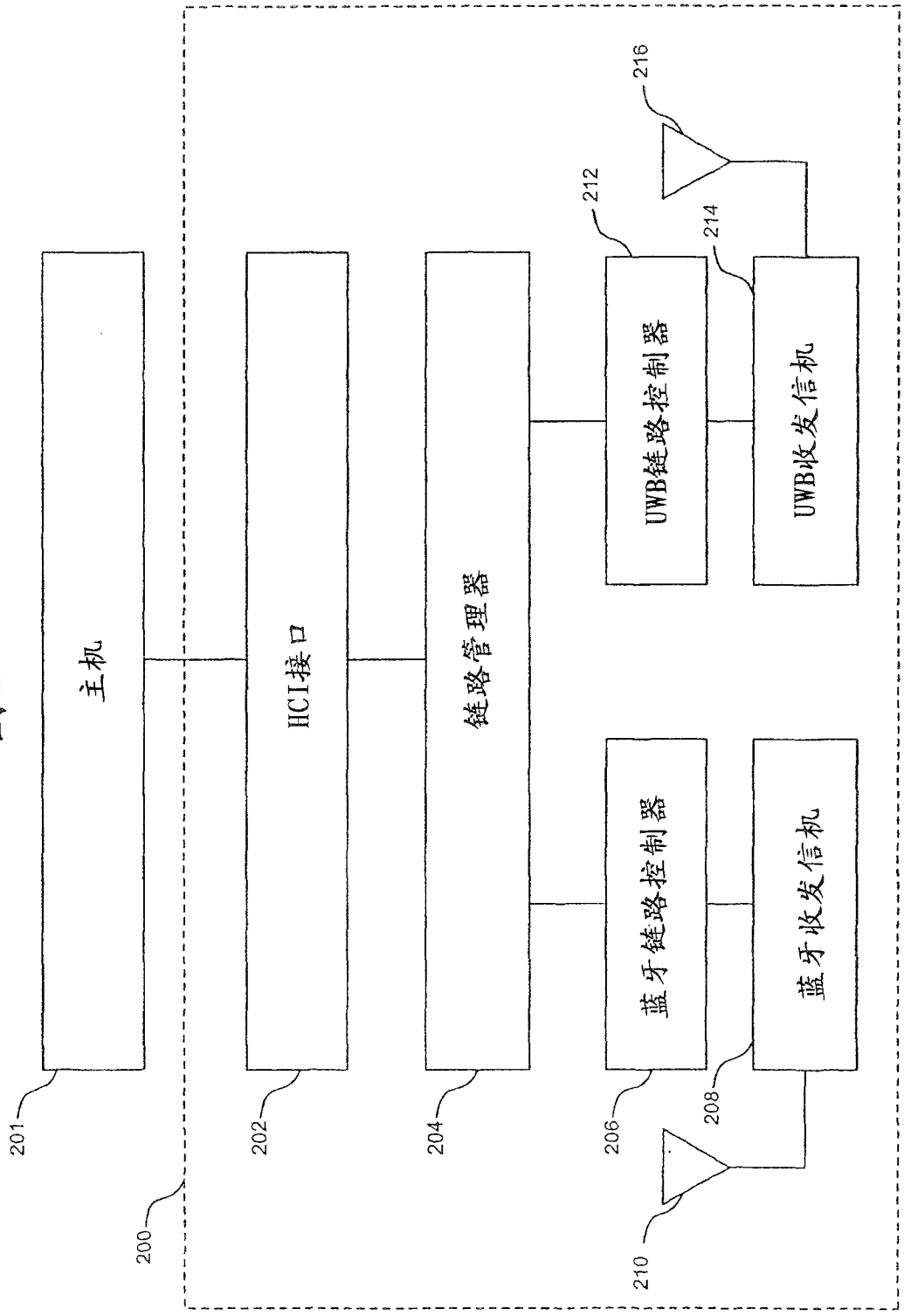
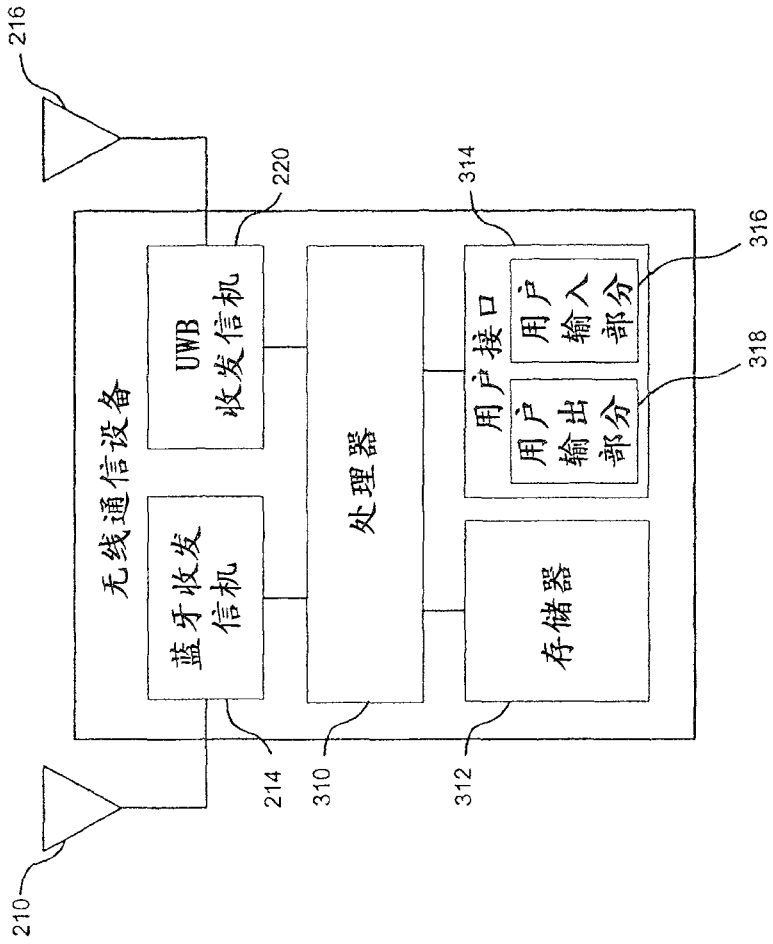

主机
HCI接口
链路管理器
UWB链路控制器
UWB收发信机
蓝牙链路控制器
蓝牙收发信机
200
201
202
204
206
208
210
212
214
216

图 3


216
220
314
316
318
无线通信设备
UWB
收发信机
蓝牙收发
信机
处理器
用户接口
用户
输入
部分
用户
输出
部分
存储器
214
310
312
210

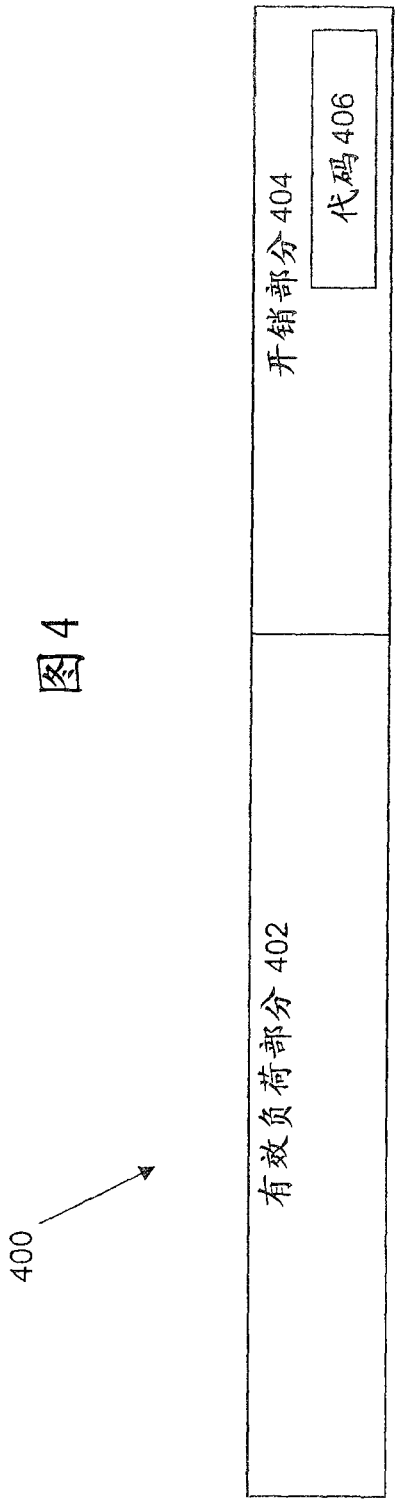


图 4

图 5

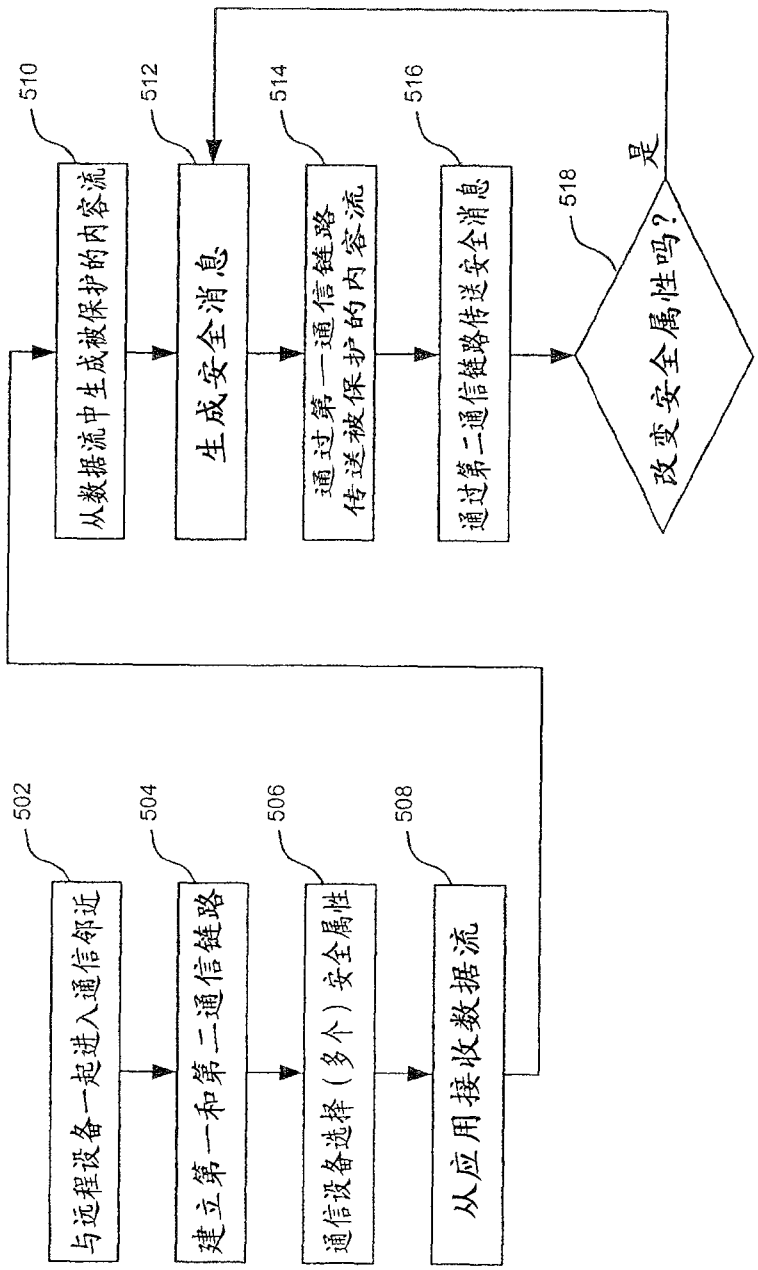

502
与远程设备一起进入通信邻近
504
建立第一和第二通信链路
506
通信设备选择（多个）安全属性
508
从应用接收数据流
510
从数据流中生成被保护的内容流
512
生成安全消息
514
通过第一通信链路传送被保护的内容流
516
通过第二通信链路传送安全消息
518
改变安全属性吗?
是

图6

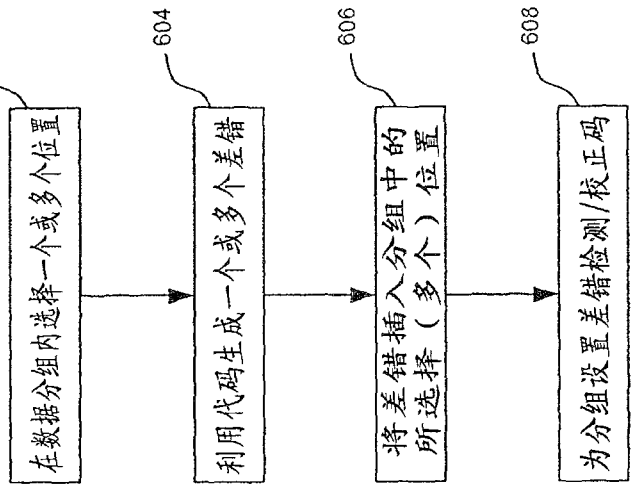

602
在数据分组内选择一个或多个位置
604
利用代码生成一个或多个差错
606
将差错插入分组中的所选择（多个）位置
608
为分组设置差错检测/校正码

图 7

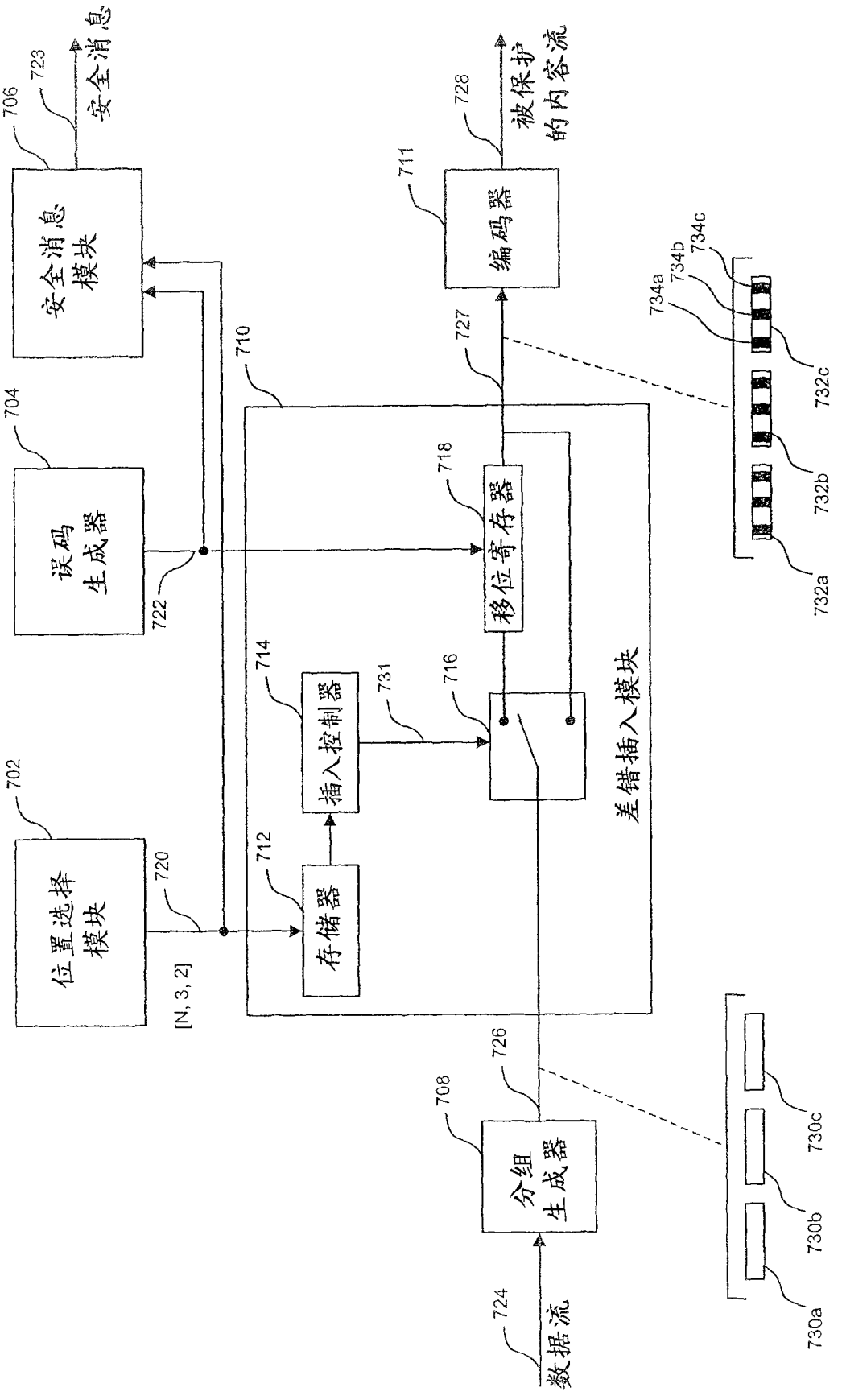

安全消息
723
706
安全消息模块
704
误码生成器
722
710
711
编码器
728
被保护的内容流
727
718
移位寄存器
734a
734b
734c
732c
732b
732a
714
插入控制器
731
716
712
存储器
差错插入模块
702
位置选择模块
720
[N, 3, 2]
708
分组生成器
726
724
数据流
730a
730b
730c

图8

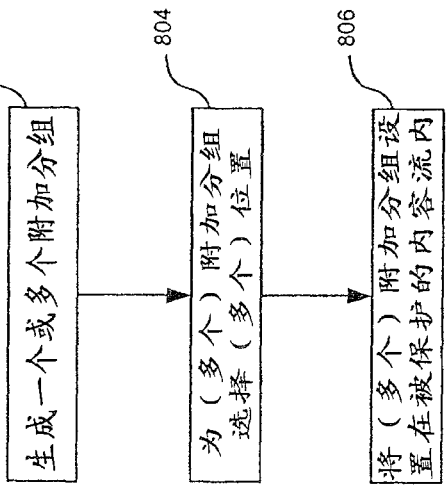

802
生成一个或多个附加分组
804
为（多个）附加分组选择（多个）位置
806
将（多个）附加分组设置在被保护的内容流内

图9

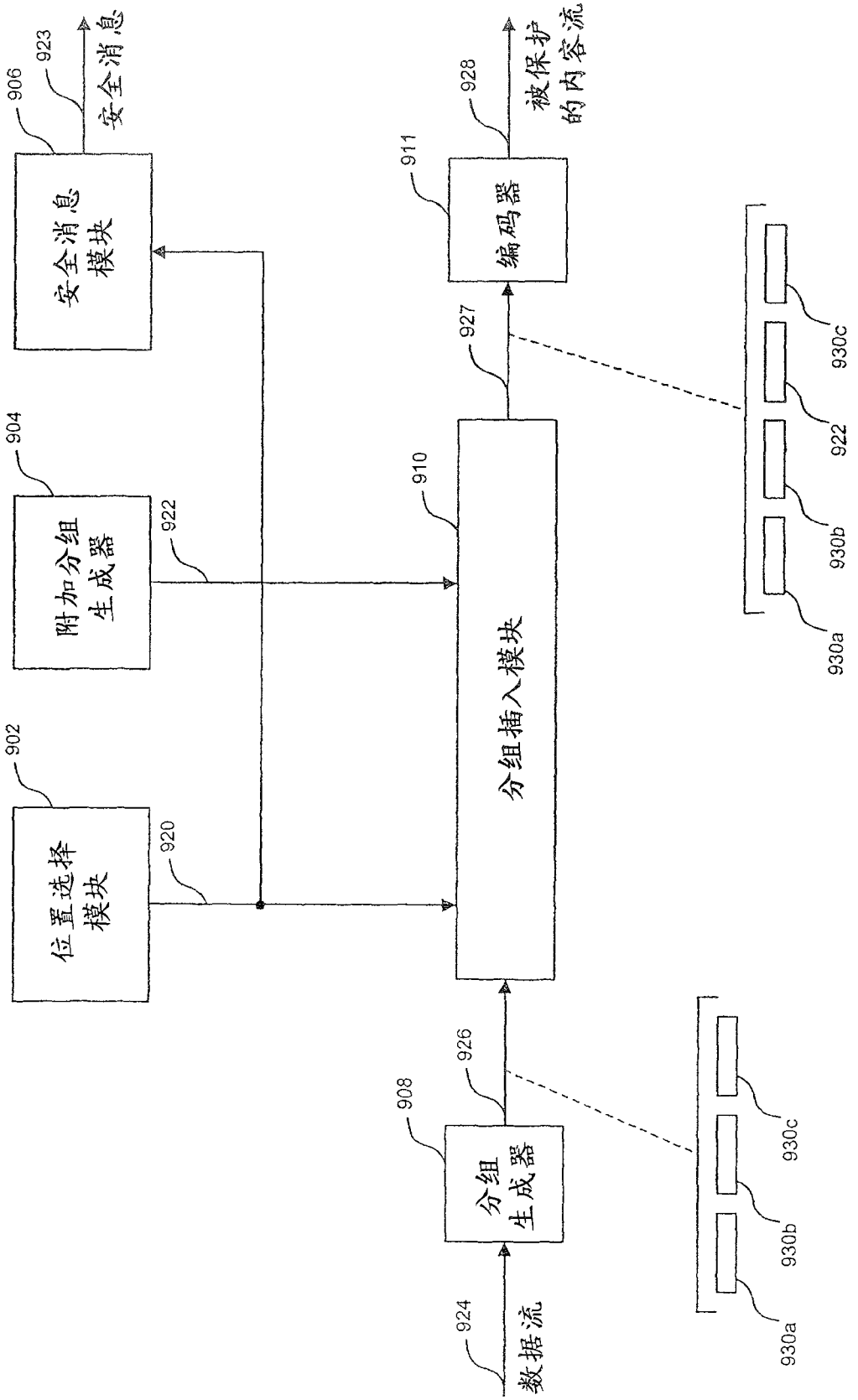

902
位置选择模块
920
904
附加分组生成器
922
906
923
安全消息模块
安全消息
910
分组插入模块
911
编码器
928
被保护的内容流
927
908
分组生成器
926
924
数据流
930a
930b
930c
922

图10

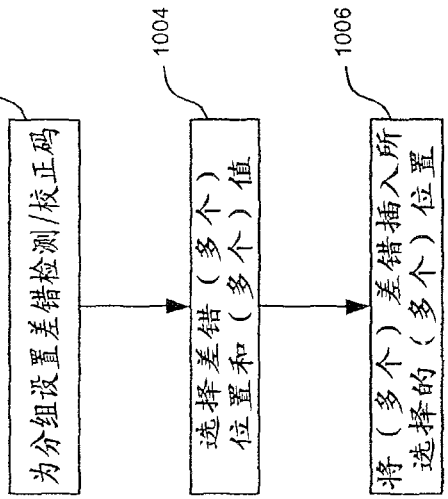

1002
为分组设置差错检测/校正码
1004
选择差错（多个）位置和（多个）值
1006
将（多个）差错插入所选择的（多个）位置

图11

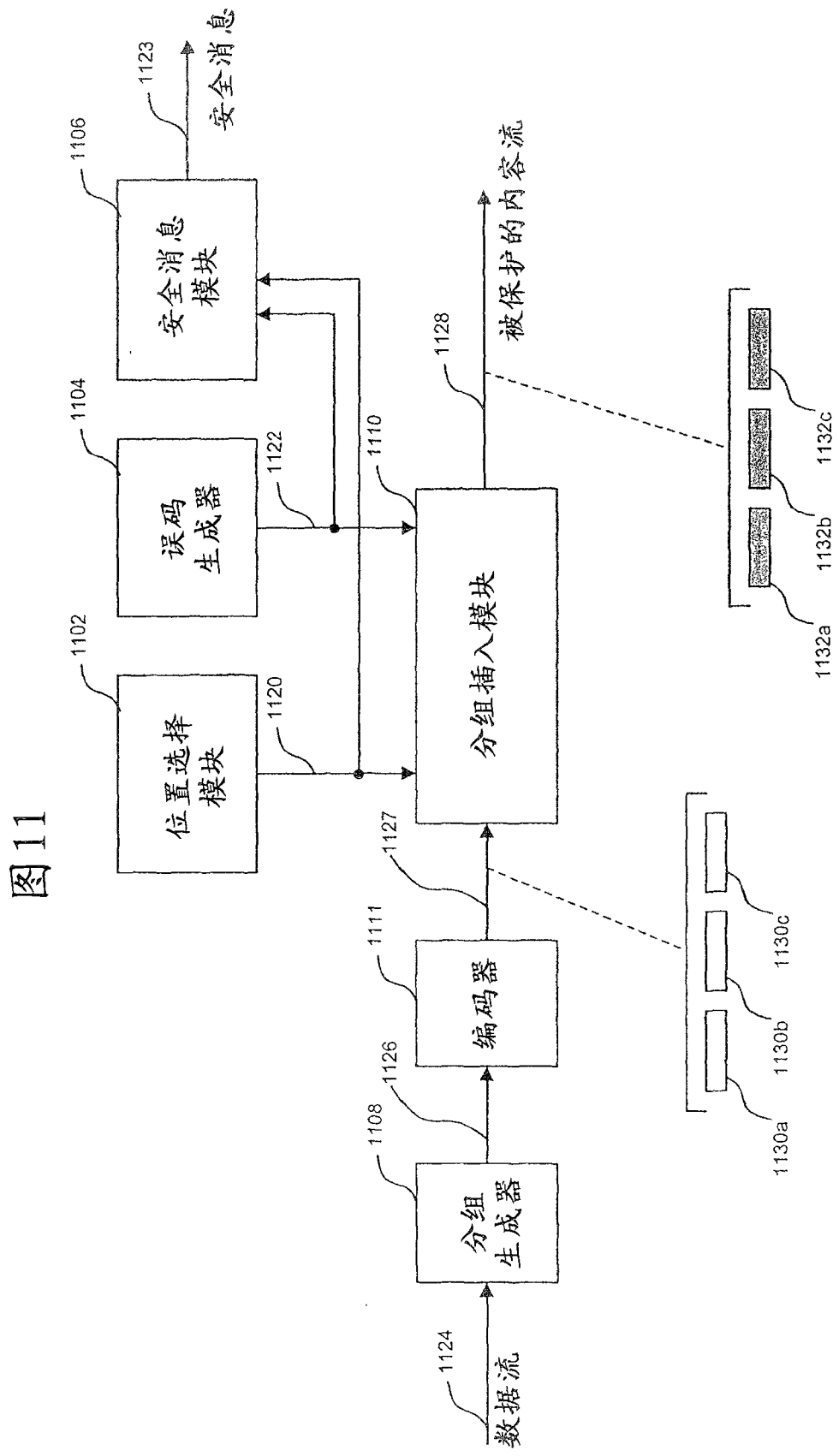
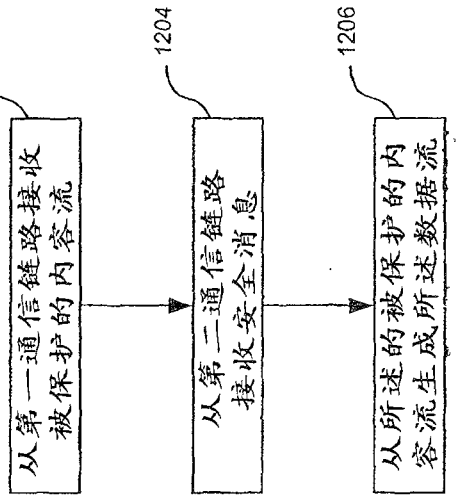

1102
位置选择模块
1104
误码生成器
1106
安全消息模块
1108
分组生成器
1110
分组插入模块
1111
编码器
1120
1122
1123
安全消息
1124
数据流
1126
1127
1128
被保护的内容流
1130a
1130b
1130c
1132a
1132b
1132c

图12


1202
从第一通信链路接收被保护的内容流
1204
从第二通信链路接收安全消息
1206
从所述的被保护的内容流生成所述数据流