(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104012134 B
(45)授权公告日 2018.09.11

(21)申请号 201280064027.6
(22)申请日 2012.12.24
(65)同一申请的已公布的文献号
申请公布号 CN 104012134 A
(43)申请公布日 2014.08.27
(30)优先权数据
4551/CHE/2011 2011.12.23 IN
(85)PCT国际申请进入国家阶段日
2014.06.23
(86)PCT国际申请的申请数据
PCT/KR2012/011349 2012.12.24
(87)PCT国际申请的公布数据
WO2013/095074 EN 2013.06.27

(73)专利权人 三星电子株式会社
地址 韩国京畿道
(72)发明人 A.阿基瓦尔 姜贤贞
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 张泓

(51)Int.Cl.
H04W 12/08(2006.01)
H04W 28/06(2006.01)
(56)对比文件
US 2009164788 A1,2009.06.25,
审查员 陈静

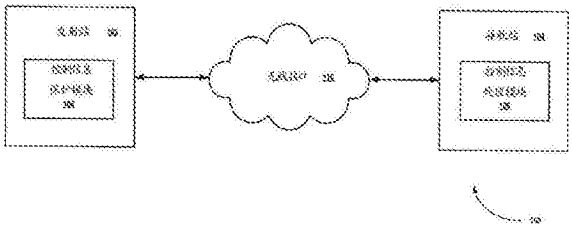
权利要求书3页 说明书14页 附图19页

(54)发明名称

用于无线网络环境中的控制信息的安全通信的方法和系统

(57)摘要

本发明提供用于在无线网络环境中安全地传递控制信息的方法和系统。当发射站必须向接收站传送控制信息时，发射站确定控制信息属于第一类型还是第二类型。如果控制信息是第二类型的控制信息，则发射站使用为了保护第二类型的控制信息而计算的计数器值、CMAC值和安全密钥来对第二类型的控制信息进行保密。一旦对控制信息进行了保密，发射站就向接收站传送经保密的控制信息。



CN 104012134 B

1.一种用于在无线通信系统中传送控制信息的方法,该方法包括:

在机器对机器M2M处生成用于根据基于密文的消息认证码CMAC来认证控制信息的认证密钥;以及

在M2M设备处传送基于该认证密钥而保护的控制信息,控制信息包括指示该控制信息是否使用CMAC来保护的指示符,

其中基于CMAC业务加密密钥TEK预密钥和作为用于认证密钥的预定义的常数的CMACSIG来生成所述认证密钥。

2.根据权利要求1所述的方法,其中,所述控制信息是异常掉电信令报头。

3.根据权利要求2所述的方法,其中,所述生成认证密钥的步骤包括:使用用于帧编号的8位翻转计数器ROC当中的3个最低有效位LSB。

4.根据权利要求2所述的方法,还包括:

使用基于CMAC生成的相同的密钥每帧传送一个异常掉电信令报头。

5.根据权利要求2所述的方法,其中,所述异常掉电信令报头包括:指示异常掉电信令报头是否受到保护的1位;指示接收异常掉电信令报头的帧编号的计数器的3位;以及指示CMAC的第三字段。

6.根据权利要求2所述的方法,其中,使用基于TEK预密钥、CMACSIG和认证密钥长度的Dot16KDF函数来生成所述认证密钥,

其中,从认证密钥AK中导出TEK预密钥,CMACSIG是M2M设备的签名,长度是128位。

7.根据权利要求2所述的方法,其中,通过使用以下等式来生成CMAC:

CMAC值=Truncate(CMAC(CMAC_SIG_KEY_U,AKID|22bit super frame number|2bit frame index|STID|FID|counter value|16bit zero padding|signalling header content),16),

其中,CMAC_SIG_KEY_U是认证密钥AK,AKID是AK标识符,流标识符FID,STID是M2M设备的站ID,接收异常掉电信令报头的帧编号的计数器值,16位补零,signalling header content是异常掉电信令报头的内容,并且16是CMAC值的尺寸。

8.根据权利要求2所述的方法,其中,异常掉电信令报头还包括:指示被设置为0b0010的流标识符FID的4位;M2M设备的站ID,STID;指示异常掉电信令报头的长度的4位;如果STID仅被指配给M2M设备则指示被设置为0的STID有效偏移的3位;如果紧急状况类型是停电则指示被设置为“0b0”的紧急状况类型的1位。

9.一种用于在无线通信系统中接收控制信息的方法,该方法包括:

从机器对机器M2M接收根据基于密文的消息认证码CMAC而保护的控制信息,控制信息包括指示该控制信息是否使用CMAC来保护的指示符;以及

使用基于从控制信息中得到的值而生成的认证密钥来认证控制信息,

其中基于CMAC业务加密密钥TEK预密钥和作为用于认证密钥的预定义的常数的CMACSIG来生成所述认证密钥。

10.根据权利要求9所述的方法,其中,所述控制信息是异常掉电信令报头。

11.根据权利要求10所述的方法,其中,所述生成认证密钥的步骤包括:使用用于帧编号的8位翻转计数器ROC当中的3个最低有效位LSB。

12.根据权利要求10所述的方法,还包括:

认证使用基于CMAC生成的相同的密钥每帧传送的一个异常掉电信令报头。

13.根据权利要求10所述的方法，其中，该值包括：指示异常掉电信令报头是否受到保护的1位；指示接收异常掉电信令报头的帧编号的计数器的3位；以及指示CMAC的第三字段。

14.根据权利要求10所述的方法，其中，使用基于TEK预密钥、CMACSIG和认证密钥长度的Dot16KDF函数来生成所述认证密钥，

其中，从认证密钥AK中导出TEK预密钥，CMACSIG是M2M设备的签名，长度是128位。

15.根据权利要求10所述的方法，其中，通过使用以下等式来生成CMAC：

CMAC值＝Truncate(CMAC(CMAC_SIG_KEY_U,AKID|22bit super frame number|2bit frame index|STID|FID|counter value|16bit zero padding|signalling header content),16)，

其中，CMAC_SIG_KEY_U是认证密钥AK，AKID是AK标识符，流标识符FID，STID是M2M设备的站ID，接收异常掉电信令报头的帧编号的计数器值，16位补零，signalling header content是异常掉电信令报头的内容，并且16是CMAC值的尺寸。

16.根据权利要求10所述的方法，其中，该值还包括：指示被设置为0b0010的流标识符FID的4位；M2M设备的站ID，STID；指示异常掉电信令报头的长度的4位；如果STID仅被指配给M2M设备则指示被设置为0的STID有效偏移的3位；如果紧急状况类型是停电则指示被设置为“0b0”的紧急状况类型的1位。

17.一种用于在无线通信系统中传送控制信息的机器对机器M2M设备，该设备包括：

控制器，用于生成用于根据基于密文的消息认证码CMAC来认证控制信息的认证密钥；以及

传送器，用于传送基于该认证密钥而保护的控制信息，控制信息包括指示该控制信息是否使用CMAC来保护的指示符，

其中基于CMAC业务加密密钥TEK预密钥和作为用于认证密钥的预定义的常数的CMACSIG来生成所述认证密钥。

18.根据权利要求17所述的M2M设备，其中，所述控制信息是异常掉电信令报头。

19.根据权利要求18所述的M2M设备，其中，所述控制器生成认证密钥包括：使用用于帧编号的8位翻转计数器ROC当中的3个最低有效位LSB。

20.根据权利要求18所述的M2M设备，还包括：

控制器控制传送器来使用基于CMAC生成的相同的密钥每帧传送一个异常掉电信令报头。

21.根据权利要求18所述的M2M设备，其中，所述异常掉电信令报头包括：指示异常掉电信令报头是否受到保护的1位；指示接收异常掉电信令报头的帧编号的计数器的3位；以及指示CMAC的第三字段。

22.根据权利要求18所述的M2M设备，其中，使用基于TEK预密钥、CMACSIG和认证密钥长度的Dot16KDF函数来生成所述认证密钥，

其中，从认证密钥AK中导出TEK预密钥，CMACSIG是M2M设备的签名，长度是128位。

23.根据权利要求18所述的M2M设备，其中，通过使用以下等式来生成CMAC：

CMAC值＝Truncate(CMAC(CMAC_SIG_KEY_U,AKID|22bit super frame number|2bit frame index|STID|FID|counter value|16bit zero padding|signalling header

content),16),

其中,CMAC_SIG_KEY_U是认证密钥AK,AKID是AK标识符,流标识符FID,STID是M2M设备的站ID,接收异常掉电信令报头的帧编号的计数器值,16位补零,signalling header content是异常掉电信令报头的内容,并且16是CMAC值的尺寸。

24.根据权利要求18所述M2M设备,其中,异常掉电信令报头还包括:指示被设置为0b0010的流标识符FID的4位;M2M设备的站ID,STID;指示异常掉电信令报头的长度的4位;如果STID仅被指配给M2M设备则指示被设置为0的STID有效偏移的3位;如果紧急状况类型是停电则指示被设置为"0b0"的紧急状况类型的1位。

25.一种用于在无线通信系统中接收控制信息的基站,该基站包括:

接收器,用于从机器对机器M2M接收根据基于密文的消息认证码CMAC而保护的控制信息,控制信息包括指示该控制信息是否使用CMAC来保护的指示符;以及

控制器,用于使用基于从控制信息中得到的值而生成的认证密钥来认证控制信息,

其中基于CMAC业务加密密钥TEK预密钥和作为用于认证密钥的预定义的常数的CMACSIG来生成所述认证密钥。

26.根据权利要求25所述的基站,其中,所述控制信息是异常掉电信令报头。

27.根据权利要求25所述的基站,其中,所述控制器生成认证密钥包括:使用用于帧编号的8位翻转计数器ROC当中的3个最低有效位LSB。

28.根据权利要求25所述的基站,还包括:

控制器认证使用基于CMAC生成的相同的密钥每帧传送的一个异常掉电信令报头。

29.根据权利要求25所述的基站,其中,该值包括:指示异常掉电信令报头是否受到保护的1位;指示接收异常掉电信令报头的帧编号的计数器的3位;以及指示CMAC的第三字段。

30.根据权利要求25所述的基站,其中,使用基于TEK预密钥、CMACSIG和认证密钥长度的Dot16KDF函数来生成所述认证密钥,

其中,从认证密钥AK中导出TEK预密钥,CMACSIG是M2M设备的签名,长度是128位。

31.根据权利要求25所述的基站,其中,通过使用以下等式来生成CMAC:

CMAC值=Truncate(CMAC(CMAC_SIG_KEY_U,AKID|22bit super frame number|2bit frame index|STID|FID|counter value|16bit zero padding|signalling header content),16),

其中,CMAC_SIG_KEY_U是认证密钥AK,AKID是AK标识符,流标识符FID,STID是M2M设备的站ID,接收异常掉电信令报头的帧编号的计数器值,16位补零,signalling header content是异常掉电信令报头的内容,并且16是CMAC值的尺寸。

32.根据权利要求25所述的基站,其中,该值还包括:指示被设置为0b0010的流标识符FID的4位;M2M设备的站ID,STID;指示异常掉电信令报头的长度的4位;如果STID仅被指配给M2M设备则指示被设置为0的STID有效偏移的3位;如果紧急状况类型是停电则指示被设置为"0b0"的紧急状况类型的1位。

用于无线网络环境中的控制信息的安全通信的方法和系统

技术领域

[0001] 本发明总体上涉及无线通信领域，并且更具体地涉及在无线网络环境中安全地传递控制信息。

背景技术

[0002] 基于各种标准(例如，基于电气与电子工程师协会(IEEE)802.16e的全球微波接入互操作性(WiMAX)标准和其对IEEE802.16m的演进)的宽带无线网络提供诸如语音、分组数据等等的各种类型的服务。最近，正在考虑基于IEEE 802.16m和IEEE 802.16e的标准来使得能够进行用于诸如智能电网、车辆跟踪、保健等等的应用的机器对机器(M2M)通信。由于其将被用于诸如保健和智能电网之类的许多关键应用，所以安全性是标准的重要需求之一。

[0003] 在移动站或M2M设备与基站之间交换若干类型的控制信息以彼此通信。典型地，以在M2M设备与基站之间建立的信令连接或流上传送的控制消息的形式来交换控制信息。当前，使用基于密文的消息认证码(CMAC)算法来保护控制消息，其中使用在国家标准与技术协会(NIST)特种出版物 800-38B中描述的CMAC构造来生成8字节的CMAC，并且在于信令连接或流上传输之前将8字节的CMAC附加到控制消息。可选地，也可以对控制消息的内容进行加密。3字节计数器或分组编号(PN)也用于提供针对重放攻击的保护。在传输每个控制消息之后递增计数器。从不重复元组<control security key(控制安全密钥)，PN>。也将用于生成CMAC的安全密钥的序列号与控制消息一起传送。保护控制消息的方法向每个控制消息添加12字节的开销。典型地，在媒体访问控制(MAC)协议数据单元(PDU)中携带使用 CMAC值保护的控制消息。携带受到保护的控制消息的MAC PDU包含MAC 报头和有效载荷。有效载荷包含控制消息，其后是由安全密钥序列号组成的安全信息、保留位、分组编号和CMAC值。

[0004] 也以作为特殊类型的MAC报头的MAC信令报头的形式来交换控制信息。在MAC PDU中向接收站传送MAC信令报头。能够注意到，携带MAC 信令报头的MAC PDU除MAC信令报头之外不包含任何有效载荷。MAC信令报头在尺寸上非常短(几个字节)，但是携带至关重要的信息。通常，MAC 信令报头的尺寸是6至7字节。MAC信令报头可以包括流标识符字段、类型字段、长度字段和内容字段。流标识符字段指示与MAC信令报头相关联的流标识符。类型字段指示MAC信令报头的类型。长度字段指示MAC信令报头的长度。内容字段携带MAC信令报头的实际内容。当前，以不安全的方式在移动站或M2M设备与基站之间交换MAC信令报头。

发明内容

[0005] 技术问题

[0006] 保护控制消息的当前技术不能被应用于MAC信令报头，这是因为与控制信息本身相比，大的开销可能被添加到MAC信令报头的尺寸。

[0007] 技术方案

[0008] 根据本公开的一个方面，提供一种在无线通信环境中对控制信息进行保密的方

法，该方法包括：在发射站生成用于对第一类型的控制信息进行保密的一个或多个安全密钥和用于对第二类型的控制信息进行保密的一个或多个安全密钥；计算用于第一类型的控制信息的第一类型的计数器和用于第二类型的控制信息的第二类型的计数器；计算用于第一类型的控制信息的、第一类型的基于密文的消息认证码(CMAC)和用于第二类型的控制信息的、第二类型的CMAC；使用为第一类型的控制信息导出的第一类型的CMAC、第一类型的计数器和一个或多个安全密钥来对第一类型的控制信息进行保密；以及使用为第二类型的控制信息导出的第二类型的CMAC、第二类型的计数器和一个或多个安全密钥来对第二类型的控制信息进行保密。

[0009] 根据本公开的另一个方面，提供了一种发射站，包括：处理器；和存储器，通信地耦合到处理器，其中，存储器包括被配置用于如下操作的控制信息保护模块：生成用于对第一类型的控制信息进行保密的一个或多个安全密钥和用于对第二类型的控制信息进行保密的一个或多个安全密钥；计算用于第一类型的控制信息的第一类型的计数器和用于第二类型的控制信息的第二类型的计数器；计算用于第一类型的控制信息的第一类型的基于密文的消息认证码(CMAC)和用于第二类型的控制信息的第二类型的CMAC；使用为第一类型的控制信息导出的第一类型的CMAC、第一类型的计数器和一个或多个安全密钥来对第一类型的控制信息进行保密；以及使用为第二类型的控制信息导出的第二类型的CMAC、第二类型的计数器和一个或多个安全密钥来对第二类型的控制信息进行保密。

[0010] 根据本公开的另一个方面，提供一种在无线通信环境中安全地传递信令报头的方法，该方法包括：由发射站计算用于将被安全地传送到接收站的信令报头的计数器值；计算用于信令报头的基于密文的消息认证码(CMAC) 值；使用为信令报头导出的CMAC值、计数器值和一个或多个安全密钥来对信令报头进行保密；以及向接收站传送经保密的信令报头。

[0011] 根据本公开的另一个方面，提供了一种发射站，包括：处理器；和存储器，通信地耦合到处理器，其中，存储器包括被配置用于如下操作的控制信息保护模块：计算用于将被安全地传送到接收站的信令报头的计数器值；计算用于信令报头的基于密文的消息认证码(CMAC)值；使用为信令报头导出的CMAC值、计数器值和一个或多个安全密钥来对信令报头进行保密；以及向接收站传送经保密的信令报头。

[0012] 根据本公开的另一个方面，提供一种对从发射站接收的信令报头进行处理的方法，该方法包括：确定从发射站接收的信令报头是否受到保护；验证信令报头中的计数器值；如果计数器值是有效的，则确定在其中从发射站接收信令报头的帧的帧编号；基于计数器值、帧编号、认证密钥标识符、移动站逻辑地址、流标识符和信令报头的内容来计算基于密文的消息认证码 (CMAC)值；确定计算的CMAC值是否与信令报头中的CMAC值匹配；以及如果计算的CMAC值与信令报头中的CMAC值匹配，则处理信令报头的内容。

[0013] 根据本公开的另一个方面，提供了一种接收站，包括：处理器；和存储器，通信地耦合到处理器，其中，存储器包括被配置用于如下操作的控制信息处理模块：确定从发射站接收的信令报头是否受到保护；验证信令报头中的计数器值；如果计数器值是有效的，则确定在其中从发射站接收信令报头的帧的帧编号；基于计数器值、帧编号、认证密钥标识符、移动站逻辑地址、流标识符和信令报头的内容来计算基于密文的消息认证码(CMAC)值；确定计算的CMAC值是否与信令报头中的CMAC值匹配；以及如果计算的 CMAC值与信令报头中的CMAC值匹配，则处理信令报头的内容。

[0014] 根据本公开的另一个方面，提供一种在无线网络环境中安全地传送信令报头的方法，该方法包括：生成用于对将被传送到接收站的信令报头进行保密的安全密钥信息；将安全密钥信息附加于信令报头的内容；为附加于信令报头的内容的安全密钥信息生成循环冗余校验(CRC)值；将CRC值附加于信令报头的内容；以及，向接收站传送具有附加到信令报头的内容的CRC值的信令报头。

[0015] 根据本公开的另一个方面，提供了一种发射站，包括：处理器；和存储器，通信地耦合到处理器，其中，存储器包括被配置用于如下操作的控制信息保护模块：生成用于对将被传送到接收站的信令报头进行保密的安全密钥信息；将安全密钥信息附加于信令报头的内容；为附加于信令报头的内容的安全密钥信息生成循环冗余校验(CRC)值；将CRC值附加于信令报头的内容；以及向接收站传送具有附加到信令报头的内容的CRC值的信令报头。

[0016] 根据本公开的另一个方面，提供一种在无线网络环境中处理受到保护的信令报头的方法，该方法包括：当从发射站接收到具有循环冗余校验(CRC) 值的受到保护的信令报头时，生成安全密钥信息；将安全密钥信息附加于信令报头的内容；基于附加于信令报头的内容的安全密钥信息来生成CRC值；确定所生成的CRC值是否与信令报头中的CRC值匹配；以及如果所生成的 CRC值与信令报头中的CRC值匹配，则处理信令报头的内容。

[0017] 根据本公开的另一个方面，提供一种在无线网络环境中处理受到保护的信令报头的方法，该方法包括：当从发射站接收到具有循环冗余校验(CRC) 值的受到保护的信令报头时，生成安全密钥信息；将安全密钥信息附加于信令报头的内容；基于附加于信令报头的内容的安全密钥信息来生成CRC值；确定所生成的CRC值是否与信令报头中的CRC值匹配；以及如果所生成的 CRC值与信令报头中的CRC值匹配，则处理信令报头的内容。

附图说明

[0018] 图1图示出根据一个实施例的、用于在发射站与接收站之间安全地传递控制信息的无线网络系统的框图。

[0019] 图2是图示出根据一个实施例的、对将被传送到接收站的控制信息进行保密的方法的处理流程图。

[0020] 图3a和图3b是根据一个实施例的、对信令报头进行保密的详细方法的处理流程图。

[0021] 图4a图示出根据一个实施例的受到保护的介质访问控制(MAC)信令报头的示例性格式。

[0022] 图4b图示出根据另一个实施例的受到保护的MAC信令报头的示例性格式。

[0023] 图5a图示出根据另一个实施例的受到保护的异常掉电信令报头 (abnormal power down signaling header)的示例性格式。

[0024] 图5b图示出根据另一个实施例的受到保护的异常掉电信令报头的另一个示例性格式。

[0025] 图5c图示出根据另一个实施例的受到保护的异常掉电信令报头的又一个示例性格式。

[0026] 图5d图示出根据另一个实施例的受到保护的异常掉电信令报头的又一个示例性格式。

[0027] 图5e图示出根据另一个实施例的受到保护的异常掉电信令报头的又一个示例性格式。

[0028] 图6是图示出根据一个实施例的、对从发射站接收的信令报头进行处理的示例性方法的处理流程图。

[0029] 图7a是图示出根据一个实施例的、对与第一类型的控制信息和第二类型的控制信息相关联的安全密钥进行刷新的示例性方法的处理流程图。

[0030] 图7b是图示出根据另一个实施例的、对与第一类型的控制信息和第二类型的控制信息相关联的安全密钥进行刷新的示例性方法的处理流程图。

[0031] 图7c是图示出根据又一个实施例的、对与第一类型的控制信息和第二类型的控制信息相关联的安全密钥进行刷新的示例性方法的处理流程图。

[0032] 图8是图示出根据替选实施例的、对信令报头进行保密的详细方法的处理流程图。

[0033] 图9是根据替选实施例的、对从发射站接收的受到保护的信令报头进行处理的详细方法的处理流程图。

[0034] 图10是示出用于实施本主题的实施例的各个组件的发射站的框图。

[0035] 图11是示出用于实施本主题的实施例的各个组件的接收站的框图。

[0036] 在本文描述的附图仅仅用于说明目的，并且无论如何不意图限制本公开的范围。

具体实施方式

[0037] 本发明提供用于在无线网络环境中安全地传递控制信息的方法和系统。在本发明的实施例的下面的详细描述中，对形成本文的一部分并且在其中作为说明可以实践本发明的特定实施例而被示出的附图进行参考。足够详细地描述这些实施例以使得那些本领域技术人员能够实践本发明，并且应当理解，可以利用其他实施例，并且可以在不背离本发明的范围的情况下作出改变。因此，不以限制意义进行以下详细描述，并且仅仅由所附权利要求来限定本发明的范围。

[0038] 贯穿文档，术语“经保密的”和“受到保护的”意思相同并且可互换地使用。

[0039] 图1图示出根据一个实施例的、用于在发射站与接收站之间安全地传递控制信息的无线网络系统100的框图。在图1中，系统100包括发射站102、接收站104和无线接口110。发射站102包括控制信息保护模块106，并且接收站104包括控制信息处理模块108。发射站102可以是移动站或基站。接收站104可以是移动站或基站。

[0040] 当发射站102必须向接收站104传送控制信息时，控制信息保护模块106 确定控制信息是否将被保护。如果控制信息将被保护，则控制信息保护模块 106确定控制信息属于第一类型还是第二类型。例如，第一类型的控制信息可以包括将通过建立的信号连接/流被传送的控制消息(例如，电气与电子工程师协会(IEEE)802.16.1系统中的管理消息、长期演进(LTE)系统中的无线电资源连接控制消息，等等)。第二类型的控制信息可以包括信令报头(例如，IEEE802.16.1系统中的独立(standalone)信令报头、LTE系统中的介质访问控制(MAC)信令报头)。第二类型的控制信息的尺寸多达7字节。如果控制信息是第一类型的控制信息，则控制信息保护模块106使用为了保护第一类型的控制信息而计算的第一类型的计数器、第一类型的基于密文的消息认证码(CMAC)值和安全密钥来对第一类型的控制信息进行保密。如果控制信息是第二类型的控制信息，则控制信息保护模块106使用为了保护第二

类型的控制信息而计算的第二类型的计数器值、第二类型的CMAC值和安全密钥来对第二类型的控制信息进行保密。一旦对控制信息进行了保密，则发射站102通过无线接口110向接收站104传送经保密的控制信息。

[0041] 当接收到经保密的控制信息时，控制信息处理模块108确定从发射站102 接收的控制信息的类型。相应地，控制信息处理模块108基于控制信息的类型对所接收的控制信息进行解码。在以下描述中更详细地描述对控制信息进行保密并且对经保密的控制信息进行处理的处理。

[0042] 图2是图示出根据一个实施例的、对将被传送到接收站的控制信息进行保密的方法的处理流程图式200。通常，发射站102向接收站104传送两种类型的控制信息。两种类型的控制信息都携带重要的信息，因此两种类型的控制信息都需要被安全地传送到接收站104。处理流程图式200提供用于在向接收站104传送之前对第一和第二类型的控制信息进行保密的方法步骤。

[0043] 在步骤202，根据认证密钥(AK)生成预密钥。典型地，在授权过程期间在发射站102(例如，基站)和接收站104(例如，移动站)共同地导出认证密钥。认证密钥的长度是160位。预密钥可以用于生成分别用于对第一类型的控制信息和第二类型的控制信息进行保密的不同的上行链路和下行链路安全密钥。在步骤204，根据预密钥导出用于第一类型的控制信息的上行链路和下行链路安全密钥以及用于第二类型的控制信息的上行链路和/或下行链路安全密钥。例如，上行链路安全密钥可以用于认证在上行链路中传送的控制信息，而下行链路安全密钥可以用于认证在下行链路中传送的控制信息。在一个示例性实施方式中，用于第一和第二类型的控制信息的上行链路和下行链路安全密钥的长度是128位。在替选的示例性实施方式中，用于第一和第二类型的控制信息的上行链路和下行链路安全密钥的长度能够是不同尺寸。能够注意到，根据预密钥导出安全密钥的过程为本领域技术人员所公知，并且省略其解释。根据在图7a至7c中图示的方法周期性生成新的安全密钥。

[0044] 在步骤206，计算用于第一类型的控制信息的第一类型的计数器。例如，第一类型的计数器可以是在其中将传送第一类型的控制信息的MAC PDU的分组编号(PN)。在一些实施例中，确定用于第一类型的控制信息的分组编号。在这些实施例中，基于第一类型的控制信息来计算第一类型的计数器。在步骤208，计算用于第一类型的控制信息的第一类型的CMAC。基于如在国家标准与技术协会(NIST)特种出版物800-38B中规定的CMAC结构来计算第一类型的CMAC。例如，第一类型的CMAC等于truncate(Security key for first type of control information,authentication key identifier|PN|Mobile station logical address|Flow Identifier|Zero Padding|first type of control information, 64)(截断(用于第一类型的控制信息的安全密钥、认证密钥标识符|PN|移动站逻辑地址|流标识符|补零|第一类型的控制信息,64))。在步骤210，使用为第一类型的控制信息导出的第一类型的CMAC、第一类型的计数器和安全密钥来对第一类型的控制信息进行保密。计算用于对第一类型的控制信息进行保密的第一类型的计数器和第一类型的CMAC的方法也为本领域技术人员所公知，并且因此省略其解释。

[0045] 步骤212至216图示出根据本发明的用于对诸如信令报头的第二类型的控制信息进行保密的过程。在步骤212，计算用于第二类型的控制信息的第二类型的计数器。在步骤214，计算用于第二类型的控制信息的第二类型的 CMAC。基于如在国家标准与技术协会

(NIST)特种出版物800-38B中规定的CMAC结构来计算第二类型的CMAC。例如，第二类型的CMAC等于 truncate(Security key for second type of control information, authentication key identifier|Frame number|Mobile station logical address|Flow Identifier|Second Type of Counter Value|Zero Padding|second type of control information,16)(截断(用于第二类型的控制信息的安全密钥、认证密钥标识符|帧编号|移动站逻辑地址|流标识符|第二类型的计数器值|补零|第二类型的控制信息，16))。在步骤216，使用为第二类型的控制信息导出的第二类型的CMAC、第二类型的计数器和安全密钥来对第二类型的控制信息进行保密。在步骤 212，向接收站104传送利用第二类型的CMAC和第二类型的计数器附加的第二类型的信息。能够注意到，第二类型的计数器和第二类型的CMAC不同于第一类型的计数器和第一类型的CMAC，并且适合于对第二类型的控制信息进行保密。例如，第二类型的CMAC与第一类型的CMAC相比可以具有更小的长度，并且使用与用于计算第一类型的CMAC的方法不同的方法来计算第二类型的CMAC。在一些实施例中，计算第二类型的计数器和第二类型的CMAC，使得包括经保密的第二类型的控制信息、第二类型的CMAC和第二类型的计数器的分组的总尺寸不超过经保密的第二类型的控制信息的阈值可容许尺寸。在图3b和图3a中更详细地解释用于对诸如信令报头的第二类型的控制信息进行保密的详细处理。

[0046] 图3a是根据一个实施例的、对信令报头进行保密的详细方法的处理流程图式300，以及图3b是根据一个实施例的、对信令报头进行保密的详细方法的处理流程图式300。考虑发射站102具有将被传送到接收站104的信令报头。在步骤302，确定是否将向接收站104安全地传送信令报头。如果将以未保护的方式传送信令报头，则在步骤304，向接收站104传送不保密的信令报头。如果将安全地传送信令报头，则在步骤306，确定安全密钥是否可用于对信令报头进行保密。如果安全密钥是不可用的，则执行步骤304。

[0047] 如果安全密钥是可用的，则在步骤310，确定与可用资源相关联的帧的帧编号。替换地，如果安全密钥是可用的，则可以在步骤308中确定是否有足够的资源可用于安全地传送信令报头。例如，基站传递分配给移动站的由移动站进行每个传输的资源。基于所分配的资源，移动站可以确定是否有足够的资源可用于信令报头的安全传输。如果不存在可用的资源，则执行步骤 309，其中等待资源的分配。如果足够的资源是可用的，则执行步骤310。

[0048] 在步骤312，确定与帧相关联的翻转计数器。例如，在每个帧翻转之后递增翻转计数器。在步骤314，确定与信令报头相关联的信令报头索引(也被称为控制信息索引)。对于每个帧，为将在每个帧中传送的每个信令报头指配唯一的信令报头索引。也就是说，在将在帧中被传送的信令报头中信令报头索引是唯一的。在步骤316，基于帧的翻转计数器和信令报头索引来计算用于信令报头的计数器值(先前称作“第二类型的计数器”)。计数器值用于提供针对重放攻击的保护。重放攻击是恶意地或欺骗性地重复或延迟有效数据传输的网络攻击的形式。

[0049] 在一个实施例中，计数器值构成对应于翻转计数器的“n1”个最高有效位和对应于信令报头索引的“n-n1”个最低有效位。当帧翻转发生时，对应于翻转计数器的“n1”个最高有效位递增等于1模$2^{(n1)}$的值。例如，如果帧编号由24位组成并且“n1”是5个位，则当帧编号从0xFFFFFF到达0x000000 时，计数器值的“n1”个最高有效位递增1模32。以下述的方式来向信令报头分配对应于信令报头索引的“n-n1”个最低有效位：即，没有使用相同安全密钥

的同一帧中的两个信令报头具有相同的计数器值。这将允许发射站102 使用相同的安全密钥来每帧对$2^{(n-n1)}$个信令报头进行保密。因此，发射站102 将每$2^{(n1+n2)}$个帧生成新的安全密钥，其中“n2”是表示帧编号的位的数量。

[0050] 在另一个实施例中，计数器值构成对应于翻转计数器的“n1”个最低有效位和对应于信令报头索引的“n-n1”个最高有效位。当帧翻转发生时，对应于翻转计数器的“n1”个最低有效位递增等于1模$2^{(n1)}$的值。例如，如果帧编号由24位组成并且“n1”是5位，则当帧编号从0xFFFFFF到达0x000000 时，计数器值的“n1”个最低有效位递增1模32。以下述的方式来向信令报头分配对应于信令报头索引的“n-n1”个最高有效位：即，没有使用相同安全密钥的同一帧中的两个信令报头具有相同的计数器值。因此，发射站102 将每$2^{(n1+n2)}$个帧生成新的安全密钥，其中“n2”是表示帧编号的位的数量。

[0051] 在又一个实施例中，计数器值构成帧的翻转计数器。当帧翻转发生时，翻转计数器递增等于1模$2^{(n)}$的值。例如，如果帧编号由24位组成并且“n1”是5位，则当帧编号从0xFFFFFF到达0x000000时，计数器值递增1模32。这将允许发射站102使用相同的安全密钥每帧仅仅对一个信令报头进行保密。因此，发射站102将每$2^{(n+n2)}$个帧生成新的安全密钥，其中“n2”是表示帧编号的位的数量。

[0052] 在又一个实施例中，计数器值构成与信令报头相关联的信令报头索引。基于将被使用相同的安全密钥每帧安全地传送的信令报头的数量来计算信令报头的尺寸。例如，如果信令报头索引的尺寸是“n”位，则发射站102能够使用相同的安全密钥来每帧对2^n个信令报头进行保密。因此，发射站102将每2^{n2}个帧生成新的安全密钥，其中“n2”是表示帧编号的位的数量。

[0053] 在步骤318，在信令报头中设置指示以指示信令报头受到保护。在一个实施例中，在信令报头的流标识符字段中设置流标识符来指示信令报头是否受到保护。例如，当信令报头受到保护时，流标识符在流标识符字段中被设置为值“0b0100”。在另一个实施例中，在信令报头的EC字段中设置EC值来指示信令报头是否受到保护。例如，如果信令报头受到保护，则EC字段被设置为值“1”。可选地，在步骤318，在信令报头的长度字段中设置信令报头的长度。在步骤320，计算用于信令报头的CMAC值(也被称为“第二类型的CMAC”)。使用CMAC生成函数来生成CMAC值。提供以下参数作为用于生成CMAC值的CMAC生成函数的输入：用于第二类型的控制信息的安全密钥、认证密钥标识符、后面是帧编号、后面是信令报头索引、后面是流标识符、后面是计数器值、后面是信令报头的内容。例如，CMAC值等于truncate(security key for second type of control information|authentication key identifier|Frame Number|Mobile station logical address|Flow Identifier|Counter Value|content of signalling header,16)(截断(用于第二类型的控制信息的安全密钥|认证密钥标识符|帧编号|移动站逻辑地址|流标识符|信令报头的内容,16))。在一个示例性实施方式中，上述计算的值的16个最低有效位被用作CMAC值。在另一个示例性实施方式中，上述计算的值的其他 16个位被用作CMAC值。

[0054] 在步骤322，通过向信令报头的内容附加计数器值和CMAC值来生成经保密的信令报头。在一个实施例中，当计数器值构成翻转计数器的“n1”个最高有效位和信令报头索引的“n-n1”个最低有效位时，通过向信令报头的内容附加CMAC值和计数器值的至少“n-n1”个最低有效位来生成经保密的信令报头。在另一个实施例中，当计数器值构成翻转计数器的

“n1”个最低有效位和信令报头索引的“n-n1”个最高有效位时，通过附加CMAC值和计数器值的至少“n-n1”个最高有效位来生成经保密的信令报头。在又一个实施例中，当计数器值等于翻转计数器时，通过附加CMAC值和翻转计数器来生成经保密的信令报头。在又一个实施例中，当计数器值等于帧的翻转计数器时，通过附加CMAC值和帧的翻转计数器的“n1”个最低有效位来生成经保密的信令报头。在又一个实施例中，当计数器值等于信令报头索引时，通过附加CMAC值和/或信令报头索引来生成经保密的信令报头。例如，如果每帧允许被传送的信令报头的数量等于一，则通过附加CMAC值来生成经保密的信令报头。能够注意到，向信令报头的内容附加CMAC值和计数器值，使得信令报头的总尺寸不超过总的可容许尺寸(例如，7字节)。在步骤324，向接收站104传送经保密的信令报头。

[0055] 以下描述解释在(IEEE)802.16.1b系统中保护信令报头的示例性过程。考虑到，IEEE 802.16.1b中的移动站必须向基站安全地传送信令报头。也考虑，如下导出分别用于对上行链路和下行链路中的信令报头进行认证的安全密钥 CMAC_SIG_KEY_U和CMAC_SIG_KEY_D：

[0056] CMAC_SIG_KEY_U|CMAC_SIG_KEY_D＝Dot16KDF(CMAC-TEKpreke y,″CMACSIG″,256)。

[0057] 一旦获取安全密钥，则移动站将计数器值重置为零。计数器值的尺寸为 8位。计数器值的前5个位表示用于将在其中传送信令报头的帧的翻转计数器。计数器值的接下来的3个最低有效位表示分配给信令报头的信令报头索引。能够注意到，以下述的方式来向信令报头分配信令报头索引：即，没有使用相同安全密钥的同一帧中的两个信令报头具有相同的计数器值。这允许移动站使用相同的安全密钥在每5毫秒持续时间的帧保护8个信令报头。因为帧编号的尺寸是24位并且翻转计数器的尺寸是5位，因此当帧编号从 0xFFFFFF到达0x000000时，移动站将计数器值递增1模32的值。进一步，需要在每$2^{24}*2^{5}=2^{29}$个帧之后导出新的安全密钥。

[0058] 然后，移动站通过由以下组成的字段计算CMAC值：认证密钥标识符 (AKID)、后面是24位的帧编号、后面是12位的站标识符(STID)和信令报头的4位流标识符(FID)、后面是8位计数器值、后面是16位补零、后面是信令报头的内容。基于22位超帧编号和2位帧索引来计算帧编号。例如，如下计算用于信令报头的CMAC值：

[0059] CMAC值＝Truncate(CMAC(CMAC_SIG_KEY,AKID|22bit super frame number|2bit frame index|STID|FID|counter value|16bit zero padding| signalling header content),16)(截断(CMAC(CMAC_SIG_KEY、AKID|22 位超帧编号|2位帧索引|STID|FID|计数器值|16位补零|信令报头内容),16))。应当理解，如在NIST特种出版物800-38B中规定的来构造CMAC 值。移动站使用结果得到DEAES-CMAC计算中的LSB 16位作为CMAC值和计数器值的3个LSB来生成经保密的信令报头。

[0060] 在以下描述中解释在IEEE802.16.1b系统中保护异常掉电信令报头的示例性过程。考虑到IEEE802.16.1b中的机器对机器(M2M)设备必须在上行链路方向上安全地传送异常掉电信令报头。也考虑，如下导出用于对在上行链路方向上由M2M设备传送的异常掉电信令报头进行认证的安全密钥 CMAC_SIG_KEY_U：

[0061] CMAC_SIG_KEY_U＝Dot16KDF(CMAC-TEK prekey,″CMACSIG″, 128)。

[0062] 一旦获取安全密钥，移动站将计数器值重置为零。计数器值等于用于帧的翻转计

数器并且尺寸是8位。当帧编号从0xFFFFFF到达0x000000时，M2M设备将计数器值递增“1模8”的值。因此，M2M设备能够使用相同的上行链路安全密钥每帧安全地传送一个异常掉电信令报头。进一步，需要在每$2^{24}*2^{8}=2^{32}$个帧之后导出新的安全密钥。

[0063] 然后，移动站通过由以下组成的字段计算CMAC值：认证密钥标识符 (AKID)、后面是24位的帧编号、后面是12位的站标识符(STID)和信令报头的4位流标识符(FID)、后面是8位计数器值、后面是16位补零、后面是异常掉电信令报头的内容。基于22位超帧编号和2位帧索引来计算帧编号。例如，如下计算用于异常掉电信令报头的CMAC值：

[0064] CMAC值＝Truncate(CMAC(CMAC_SIG_KEY,AKID|22bit super frame number|2bit frame index|STID|FID|counter value|16 bit zero padding| signalling header content),16)(截断(CMAC(CMAC_SIG_KEY、AKID|22 位超帧编号|2位帧索引|STID|FID|计数器值|16位补零|信令报头内容),16))。应当理解，如在NIST特种出版物800-38B中规定的来构造CMAC 值。移动站使用结果得到AES-CMAC计算中的LSB 16位作为CMAC值和计数器值的3个LSB来生成经保密的异常掉电信令报头。

[0065] 图4a图示出根据一个实施例的受到保护的MAC信令报头400的示例性格式。MAC信令报头400包括FID字段402、类型字段404、长度字段406、内容字段408、计数器字段410和CMAC值字段412。

[0066] FID字段402包括指示MAC信令报头是否受到保护的、与MAC信令报头400相关联的流标识符。例如，如果MAC信令报头400受到保护，FID字段402包括值“0b100”。如果MAC信令报头400没有受到保护，则FID字段402包括值“0b0010”。因此，基于在FID字段402中设置的值，接收站 104确定MAC信令报头400是受到保护还是未受到保护。FID字段402的尺寸是4位。类型字段404指示MAC信令报头400的类型并且尺寸是5位。长度字段406指示FID字段402、类型字段404和内容字段406的长度。长度字段406的尺寸是4位。例如，如果MAC信令报头的尺寸是2字节，则长度字段406被设置为值“0b010”。

[0067] 内容字段408包含MAC信令报头400的内容并且多达36位的尺寸。计数器字段410包括为MAC信令报头400计算的计数器值并且尺寸是8位。 CMAC字段412包括为MAC信令报头400计算的CMAC值并且尺寸是16 位。应当理解，如果FID字段402被设置为值“0b0010”(即，当MAC信令报头未受到保护时)，MAC信令报头400可以不包括计数器字段410和CMAC 字段412。

[0068] 图4b图示出根据另一个实施例的受到保护的MAC信令报头450的示例性格式。能够看出，除了在长度字段406中携带的信息之外，图4b的MAC 信令报头450与图4a 的MAC信令报头400类似。在MAC信令报头450中，长度字段406指示FID字段402、类型字段404、内容字段408、计数器字段 410和CMAC字段412的长度的总和。

[0069] 图5a图示出根据另一个实施例的受到保护的异常掉电信令报头500的示例性格式。异常掉电信令报头500包括FID字段502、类型字段504、长度字段506、STD字段508、STID有效偏移510、紧急状况类型字段512、EC字段514、计数器字段516和CMAC字段518。

[0070] FID字段502包括将MAC信令报头与其他MAC PDU区分的流标识符。FID字段402的尺寸是4位。类型字段504指示异常掉电信令报头500的类型并且尺寸是5位。长度字段506指示异常掉电信令报头500的总长度。长度字段506的尺寸是4位。STID字段508包括与传送异常掉电信令报头500 的移动站相关联的STID。当相同的STID被指配给多于一个移动站时，

STID 字段510指示指配给该移动站的STID有效偏移。如果STID被唯一地指配给单个移动站，则移动站将STID有效偏移字段510设置为值“0”。STID有效偏移字段510的尺寸是3位。

[0071] 紧急状况类型字段512指示为了其传送异常掉电信令报头的紧急状况的类型。紧急状况字段512的尺寸是1位。例如，如果紧急状况类型是停电，则紧急状况类型字段512被设置为值“0b0”。EC字段514指示异常掉电信令报头500是否受到保护并且具有1位的尺寸。例如，如果异常掉电信令报头 500受到保护，则EC字段514包括值“1”。如果异常掉电信令报头500没有受到保护，则EC字段514包括值“0”。因此，基于在EC字段514中设置的值，接收站104确定异常掉电信令报头500是受到保护还是未受到保护。

[0072] 计数器字段516包括为异常掉电信令报头500计算的计数器值。计数器字段516的尺寸是3位。CMAC字段518包括为异常掉电信令报头500计算的CMAC值并且尺寸是16位。应当理解，当异常掉电信令报头未受到保护时，异常掉电信令报头500可以不包括计数器字段516和CMAC字段518并且包括尺寸19位或3位的保留字段。

[0073] 图5b图示出根据另一个实施例的受到保护的异常掉电信令报头550的另一个示例性格式。能够看出，除了异常掉电信令报头550不包括EC字段514 之外，图5b的异常掉电信令报头550与图5a的异常掉电信令报头500相同。在异常掉电信令报头550中，FID字段502被设置为指示异常掉电信令报头 550是否受到保护。例如，如果异常掉电信令报头550受到保护，则FID字段被设置为值“0b0100”。

[0074] 图5c图示出根据又一个实施例的受到保护的异常掉电信令报头560的又一个示例性格式。具体地，图5c图示出根据IEEE 802.16p系统的异常掉电信令报头560。异常掉电信令报头560包括HT字段561、EC字段562、类型字段563、扩展类型字段564、CID字段565、紧急状况类型字段566、CMAC 指示符字段567、CMAC值字段568、计数器字段569、保留字段570和报头检查序列字段571。

[0075] CMAC指示符字段567指示异常掉电信令报头560是否受到保护。例如，如果异常掉电信令报头受到保护，则CMAC指示符字段567被设置为值“1”。替换地，当异常掉电信令报头568没有受到保护时，CMAC指示符被设置为值“0”。CMAC字段568包括为异常掉电信令报头560计算的CMAC值并且尺寸是16位。计数器字段569包括为异常掉电信令报头560计算的计数器值。计数器字段569的尺寸是2位。应当理解，当CMAC指示符字段567被设置为值“0”时，异常掉电信令报头560不包括CMAC字段568和计数器字段 569。而且，当CMAC指示符字段567被设置为值“0”时，尺寸18位的保留字段571被包括在异常掉电信令报头560中。因为其他字段561至566和 571为本领域技术人员所公知，所以省略其解释。

[0076] 图5d图示出根据又一个实施例的受到保护的异常掉电信令报头575的又一个示例性格式。能够看出，除了异常掉电信令报头575不包括扩展类型字段564之外，图5d的异常掉电信令报头575与图5c的异常掉电信令报头560 相同。在异常掉电信令报头575中，类型字段563用于指示类型为M2M异常掉电信令报头575。能够注意到，去除扩展类型字段564使得与异常掉电信令报头560中的2个LSB相比发射站102能够在异常掉电信令报头575中包括计数器值的3个LSB。

[0077] 图5e图示出根据另一个实施例的受到保护的异常掉电信令报头585的又一个示例性格式。能够看出，除了异常掉电信令报头585不包括计数器字段 569之外，图5e的异常掉电信令报头585与图5c的异常掉电信令报头560 相同。

[0078] 从图5a至5e能够看出，以下面的方式来将字段添加到异常掉电信令报头：即，异常掉电信令报头的总尺寸不超过六个字节。这便于发射站102(例如，M2M设备)基于带宽请求过程在(6字节的)所分配的资源中安全地传送异常信令报头而非带宽请求信令报头。

[0079] 图6是图示出根据一个实施例的、对从发射站102接收的信令报头进行处理的示例性方法的处理流程图式600。在步骤602，从发射站102接收信令报头。在步骤604，基于在信令报头中设置的指示符来确定信令报头是否受到保护。例如，如果信令报头的流标识符字段用于指示信令报头受到保护，则基于在流标识符字段中设置的值来确定信令报头是否受到保护。替换地，如果信令报头的EC字段用于指示信令报头受到保护，则基于在EC字段中设置的值来确定信令报头是否受到保护。如果指示符指示信令报头没有受到保护，则在步骤606，直接处理信令报头。

[0080] 如果指示符指示信令报头受到保护，则在步骤608，读取信令报头的长度字段中的信息。能够注意到，如果信令报头是可变长度信令报头，则接收站104读取长度字段。在步骤610，读取信令报头的计数器字段中的计数器值。在步骤612，基于计数器值确定信令报头是否是有效的。换句话说，在步骤612中，确定先前是否接收到具有相同的计数器值的任何信令报头。如果信令报头不是有效的，则在步骤614丢弃信令报头。

[0081] 在步骤616，确定在其中接收信令报头的帧的帧编号。每个帧被指配帧编号。当从发射站102接收包含信令报头的MAC PDU时，接收站104确定在其中传送信令报头的帧并且然后确定与该帧相关联的帧编号。在步骤618，基于帧编号和计数器值生成用于信令报头的CMAC值。在步骤620，确定生成的CMAC值是否与所接收的信令报头的CMAC字段中的CMAC值匹配。如果确定是真，则在步骤622，对信令报头进行处理。否则，在步骤624，丢弃信令报头。

[0082] 图7a是图示出根据一个实施例的、对与第一类型的控制信息和第二类型的控制信息相关联的安全密钥进行刷新的示例性方法的处理流程图式700。在步骤702，确定是否满足用于对为第一类型的信息和第二类型的信息导出的安全密钥进行刷新的预定条件。在一个实施例中，当与帧编号级联的帧的翻转计数器相对应的计数器值的“n1”个位达到阈值时，就说满足了预定条件。在该实施例中，阈值可以等于$2^{(n1+n2)}$个帧，其中“n2”是表示帧编号的位的数量。在另一个实施例中，当与帧编号级联的帧的翻转计数器达到阈值时，就说满足了预定条件。在该实施例中，阈值可以等于$2^{(n+n2)}$个帧，其中“n”表示帧的翻转计数器并且“n2”是表示帧编号的位的数量。在又一个实施例中，当帧编号达到阈值时，就说满足了预定条件。在该实施例中，阈值可以等于2^{n2}个帧，其中“n2”是表示帧编号的位的数量。

[0083] 如果确定满足预定条件，则在步骤704，在发射站102与接收站104之间建立新的授权密钥上下文。在步骤706，基于新的授权密钥上下文来生成新的预密钥。在步骤708，使用预密钥来导出用于对第一类型的控制信息和第二类型的控制信息进行保密的一个或多个新的安全密钥。在步骤710，一旦导出新的安全密钥就将计数器值设置为“0”，并且在每个帧翻转之后将计数器值递增值“1”。

[0084] 图7b是图示出根据另一个实施例的、对与第一类型的控制信息和第二类型的控制信息相关联的安全密钥进行刷新的示例性方法的处理流程图式750。在步骤752，确定是否满足用于对为第一类型的信息和第二类型的信息导出的安全密钥进行刷新的预定条件。如果确定满足预定条件，则在步骤754，将与认证密钥上下文相关联的认证密钥计数器值递增值“1”。发射站维持认证密钥计数器以跟踪是否满足预定条件。这将消除执行图7a的步骤

702的需要。在步骤756，当与认证密钥相关联的认证密钥计数器值被递增时，根据新的授权密钥上下文生成新的预密钥。在步骤758，使用新的预密钥来导出用于对第一类型的控制信息和第二类型的控制信息进行保密的一个或多个新的安全密钥。在步骤760，一旦导出新的安全密钥就将计数器值设置为“0”，并且在每个帧翻转之后将计数器值递增值“1”。

[0085] 图7c是图示出根据又一个实施例的、对与第一类型的控制信息和第二类型的控制信息相关联的安全密钥进行刷新的示例性方法的处理流程图式770。在步骤772，确定是否满足用于对为第二类型的信息(例如，信令报头)导出的安全密钥进行刷新的预定条件。如果确定满足预定条件，则在步骤774，将与为第二类型的控制信息导出的安全密钥相关联的安全密钥计数器递增值“1”。发射站102维持安全密钥计数器以跟踪是否满足预定条件。这将消除执行图7a的步骤702和704的需要。在步骤776，当将与一个或多个安全密钥相关联的安全密钥计数器值递增值“1”时，使用现有预密钥导出用于对第二类型的控制信息进行保密的一个或多个新的安全密钥。因此，当用于第二类型的控制信息的安全密钥计数器被递增“1”时，发射站102不必导出用于两种类型的控制信息的新的安全密钥。本领域技术人员能够预见，发射站102 能够维持用于第一类型的控制信息的分离的安全密钥计数器，并且在安全密钥计数器被递增时根据预密钥来导出用于对第一类型的控制信息进行保密的新的安全密钥。在步骤778，一旦导出新的安全密钥就将计数器值设置为“0”，并且在每个帧翻转之后将计数器值递增值“1”。

[0086] 图8是图示出根据替选实施例的、对信令报头进行保密的详细方法的处理流程图式800。在步骤802，生成用于对将被传送到接收站102的信令报头进行保密的安全信息。如下生成安全信息：

[0087] 安全信息＝安全密钥ID＝Dot16KDF(安全密钥、安全密钥计数|移动站标识符|基站标识符|帧编号|补零(可选)|安全密钥ID,n)。在一个实施例中，“n”的值是64位。在每次帧翻转时更新安全密钥计数，并且在安全密钥计数达到其最大值之前刷新安全密钥。

[0088] 在步骤804，将安全信息附加到信令报头的内容。在步骤806，基于安全信息和信令报头的内容来生成循环冗余校验(CRC)值。生成CRC值的过程在现有技术中是公知的，并且省略其解释。在步骤808，将CRC信息附加到信令报头的原始内容。信令报头的FID字段或EC字段可以用于指示信令报头是否受到保护。在步骤810，向接收站104传送具有CRC信息的信令报头。

[0089] 图9是根据替选实施例的、对从发射站接收的受到保护的信令报头进行处理的详细方法的处理流程图式900。在步骤902，从发射站102接收信令报头。在步骤904，基于在信令报头中的流标识符/EC字段来确定信令报头是否受到保护。如果流标识符/EC字段指示信令报头没有受到保护，则在步骤 906，直接处理信令报头。

[0090] 如果流标识符指示安全信息受到保护，则在步骤908，生成安全信息。在步骤910，将安全信息附加到信令报头的内容。在步骤912，使用附加于信令报头的内容的安全信息来生成CRC值。在步骤914，确定所生成的CRC 是否与受到保护的信令报头中的CRC值匹配。如果发现匹配，则在步骤916，对受到保护的信令报头的内容进行处理。然而，如果发现不匹配，则在步骤 918丢弃信令报头。

[0091] 图10是示出用于实施本主题的实施例的各个组件的发射站102的框图。在图10中，发射站102包括处理器1002、存储器1004、只读存储器(ROM) 1006、发射机1008、总线1010、

显示器1012、输入设备1014和光标控制1016。

[0092] 如在本文所使用的，处理器1002意指任何类型的计算电路，诸如但不限于微处理器、微控制器、复杂指令集计算微处理器、精简指令集计算微处理器、超长指令字微处理器、显式并行指令计算微处理器、图形处理器、数字信号处理器或任何其他类型的处理电路。处理器1002也可以包括嵌入式控制器，诸如通用或可编程逻辑设备或阵列、专用集成电路、单片计算机、智能卡，等等。

[0093] 存储器1004和ROM1006可以是易失性存储器和非易失性存储器。存储器1004包括根据一个或多个上面描述的实施例的用于对第一类型的控制信息和第二类型的控制信息进行保密的控制信息保护模块106。可以在存储元件中存储各种计算机可读存储媒介，并且从存储元件访问各种计算机可读存储媒介。存储元件可以包括用于存储数据和机器可读指令的任何适当的存储器设备(或多个)，诸如只读存储器、随机存取存储器、可擦可编程序只读存储器、电可擦可编程只读存储器、硬盘驱动器、用于处理光盘的可移除的媒体驱动器、数字视频磁盘、软磁盘、盒式磁带、存储卡、Memory Sticks™，等等。

[0094] 可以结合包括用于执行任务或定义抽象数据类型或低级别硬件上下文的功能、规程、数据结构和应用程序的模块来实施本主题的实施例。可以以上面提及的存储媒介中的任何一项上的机器可读指令的形式来存储控制信息保护模块106，并且可以由处理器1002执行控制信息保护模块106。例如，计算机程序可以包括根据本主题的教导和在本文描述的实施例的、能够对第一类型的控制信息和第二类型的控制信息进行保密的机器可读指令。在一个实施例中，程序可以被包括在光盘只读存储器(CD-ROM)上，并且从CD-ROM 被加载到非易失性存储器中的硬盘驱动器。

[0095] 收发信机1008可以能够安全地向接收站104传送第一类型的控制信息和第二类型的控制信息。总线1010充当发射站102的各个组件之间的互连。诸如显示器1012、输入设备1014和光标控制1016之类的组件为本领域技术人员所公知，并且因此省略其解释。

[0096] 图11是示出用于实施本主题的实施例的各个组件的接收站104的框图。在图11中，接收站104包括处理器1102、存储器1104、只读存储器(ROM) 1106、接收机1108、总线1110、显示器1112、输入设备1114和光标控制1116。

[0097] 如在本文所使用的，处理器1102意指任何类型的计算电路，诸如但不限于微处理器、微控制器、复杂指令集计算微处理器、精简指令集计算微处理器、超长指令字微处理器、显式并行指令计算微处理器、图形处理器、数字信号处理器，或任何其他类型的处理电路。处理器1102也可以包括嵌入式控制器，诸如通用或可编程逻辑设备或阵列、专用集成电路、单片计算机、智能卡，等等。

[0098] 存储器1104和ROM 1106可以是易失性存储器和非易失性存储器。存储器1104包括根据一个或多个上面描述的实施例的、用于对第一类型的控制信息和第二类型的控制信息进行处理的控制信息处理模块108。可以在存储元件中存储各种计算机可读存储媒介，并且从存储元件访问各种计算机可读存储媒介。存储元件可以包括用于存储数据和机器可读指令的任何适当的存储器设备，诸如只读存储器、随机存取存储器、可擦可编程序只读存储器、电可擦可编程只读存储器、硬盘驱动器，用于处理光盘的可移除的媒体驱动器、数字视频磁盘、软磁盘、盒式磁带、存储卡、Memory Sticks™，等等。

[0099] 可以结合包括用于执行任务或定义抽象数据类型或低级别硬件上下文的功能、规

程、数据结构和应用程序的模块来实施本主题的实施例。可以以上面提及的存储媒介中的任何一项上的机器可读指令的形式来存储控制信息处理模块108，并且可以由处理器1102执行控制信息处理模块108。例如，计算机程序可以包括根据本主题的教导和在本文描述的实施例的、能够对经保密的第一类型的控制信息和经保密的第二类型的控制信息进行处理的机器可读指令。在一个实施例中，计算机程序可以被包括在光盘只读存储器 (CD-ROM)上，并且从CD-ROM被加载到非易失性存储器中的硬盘驱动器。

[0100] 接收机1108可以能够安全地接收来自发射站102的第一类型的控制信息和第二类型的控制信息。总线1110充当接收站104的各个组件之间的互连。诸如显示器1112、输入设备1114和光标控制1116之类的组件为本领域技术人员所公知，并且因此省略其解释。

[0101] 尽管参考IEEE802.16系统并且具体地参考IEEE802.16.1系统描述以上描述的实施例，但本领域技术人员能够理解，对IEEE802.16.1的参考纯粹是示例性的，并且在不丧失普遍性的情况下本公开的实施例也适用于其他蜂窝式通信。

[0102] 已经参考特定示例实施例描述了目前的实施例；显然的是，可以在不背离各个实施例的更宽的精神和范围的情况下对这些实施例进行各种修改和改变。此外，可以使用体现在机器可读媒介中的例如基于互补金属氧化物半导体的逻辑电路、固件、软件和/或硬件、固件，和/或软件的任何组合来实现和操作在本文描述的各种设备、模块等等。例如，可以使用晶体管、逻辑门和诸如专用集成电路的电气电路来体现各种电气结构和方法。

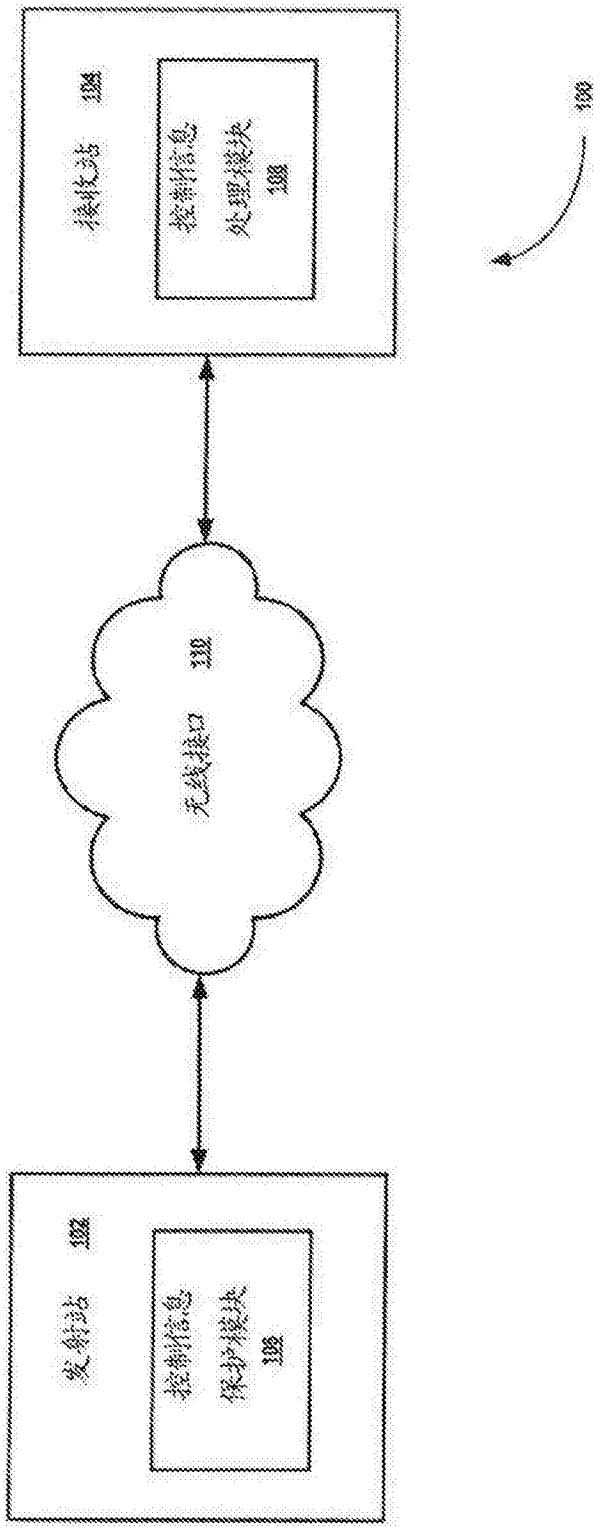


图1

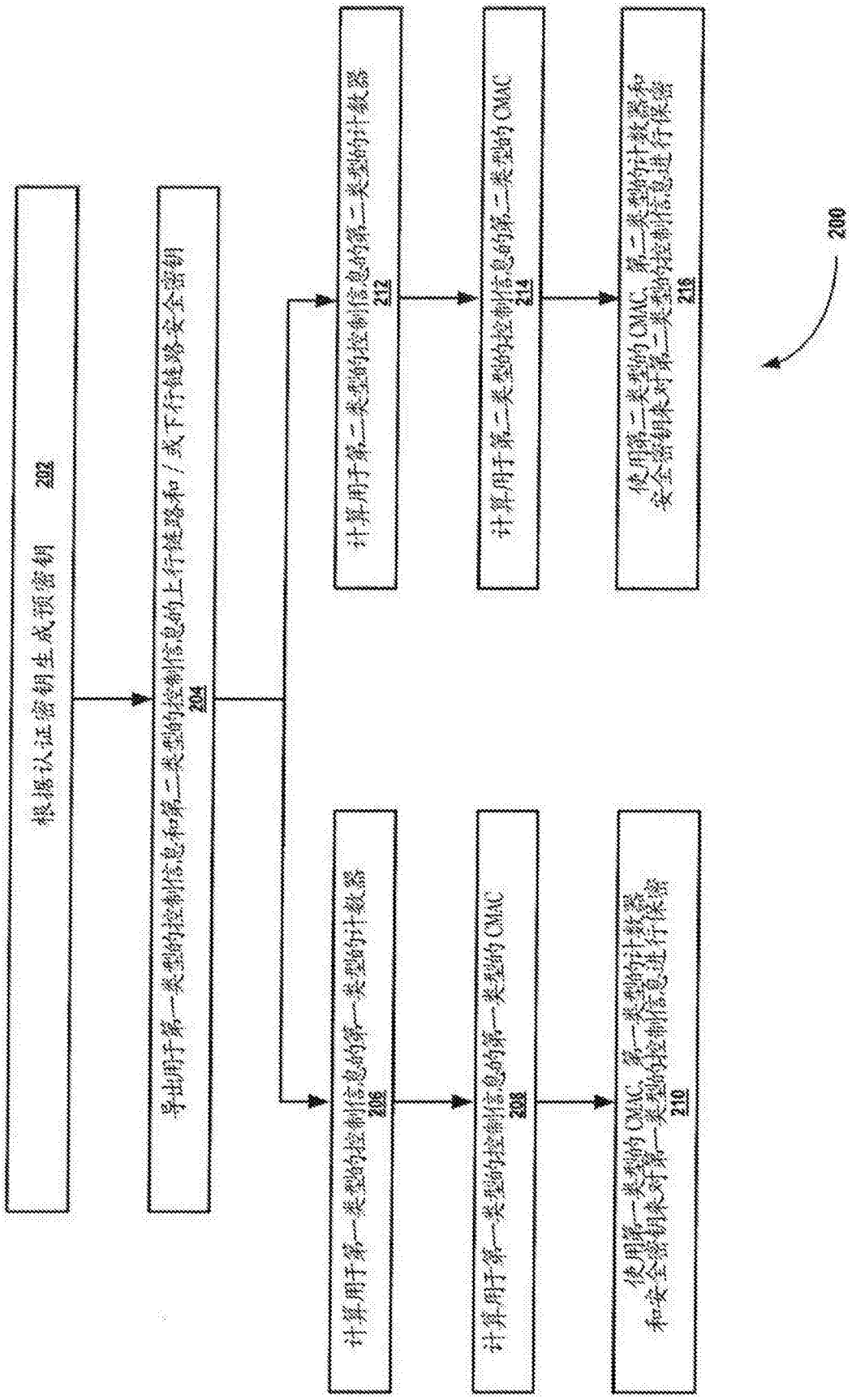

根据认证密钥生成预密钥
202
导出用于第一类型的控制信息和第二类型的上行链路和/或下行链路安全密钥
204
计算用于第二类型的控制信息的第二类型的计数器
212
计算用于第二类型的控制信息的第二类型的 CMAC
214
使用第二类型的 CMAC、第二类型的计数器和安全密钥来对第二类型的控制信息进行保密
216
200
计算用于第一类型的控制信息的第一类型的计数器
206
计算用于第一类型的控制信息的第一类型的 CMAC
208
使用第一类型的 CMAC、第一类型的计数器和安全密钥来对第一类型的控制信息进行保密
210

图2

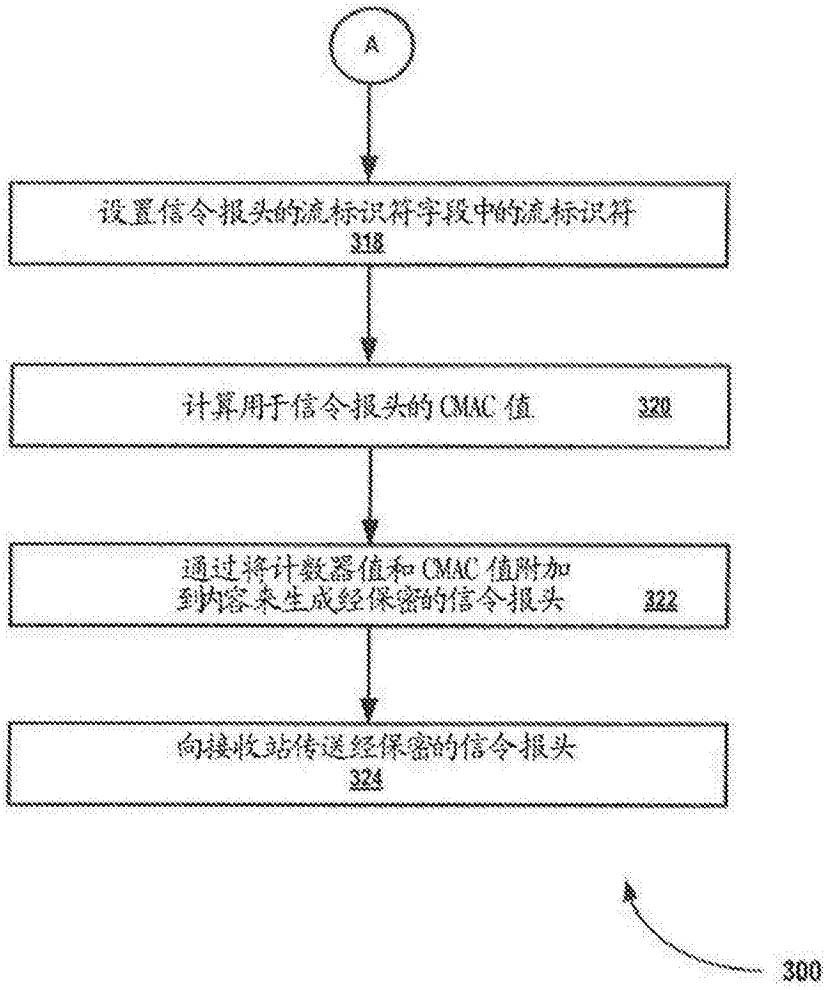

A
设置信令报头的流标识符字段中的流标识符
318
计算用于信令报头的 CMAC 值
320
通过将计数器值和 CMAC 值附加
到内容来生成经保密的信令报头
322
向接收站传送经保密的信令报头
324
300

图3a

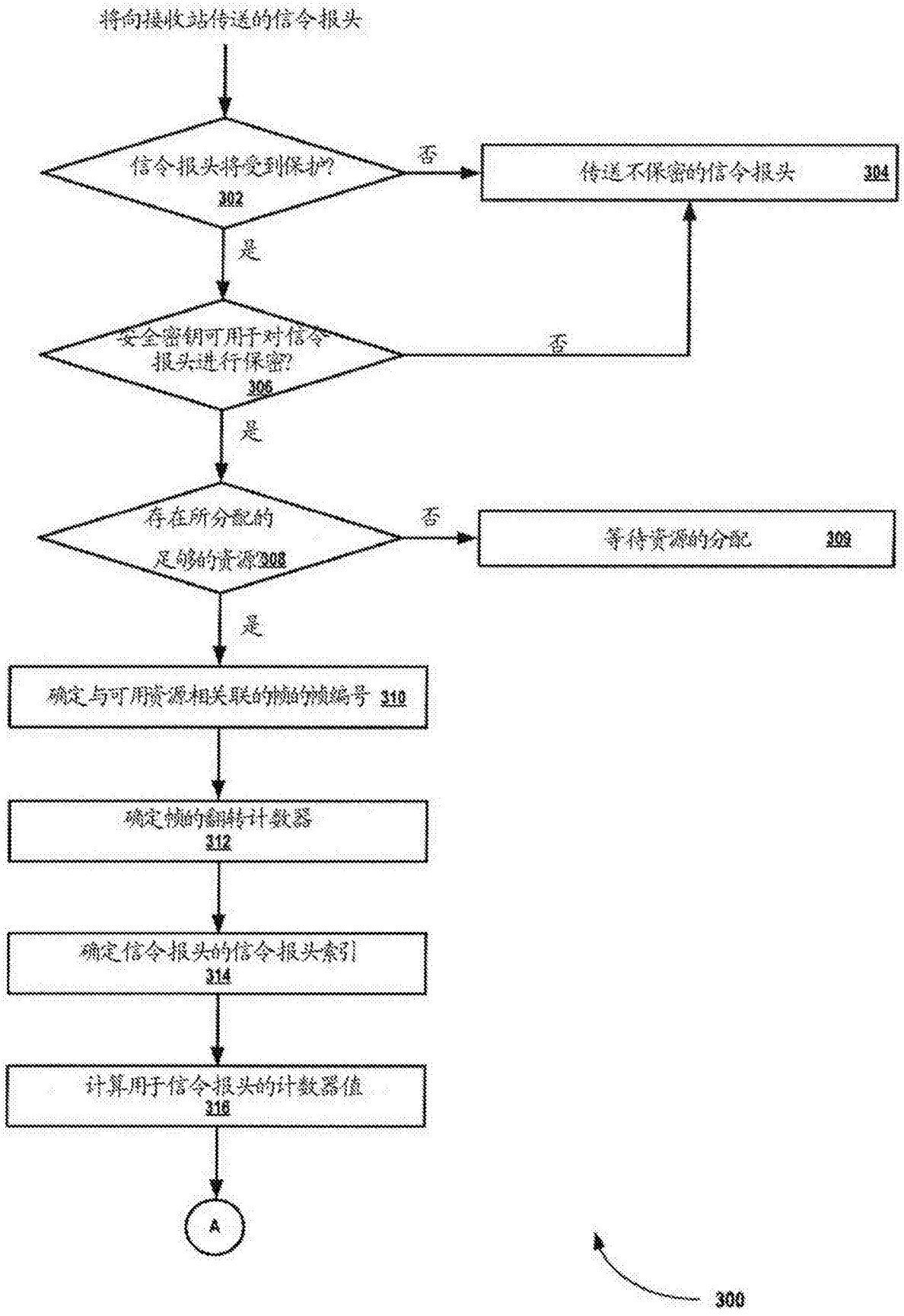

将向接收站传送的信令报头
信令报头将受到保护?
302
否
传送不保密的信令报头
304
是
安全密钥可用于对信令报头进行保密?
306
否
是
存在所分配的足够的资源?
308
否
等待资源的分配
309
是
确定与可用资源相关联的帧的帧编号
310
确定帧的翻转计数器
312
确定信令报头的信令报头索引
314
计算用于信令报头的计数器值
316
A
300

图3b

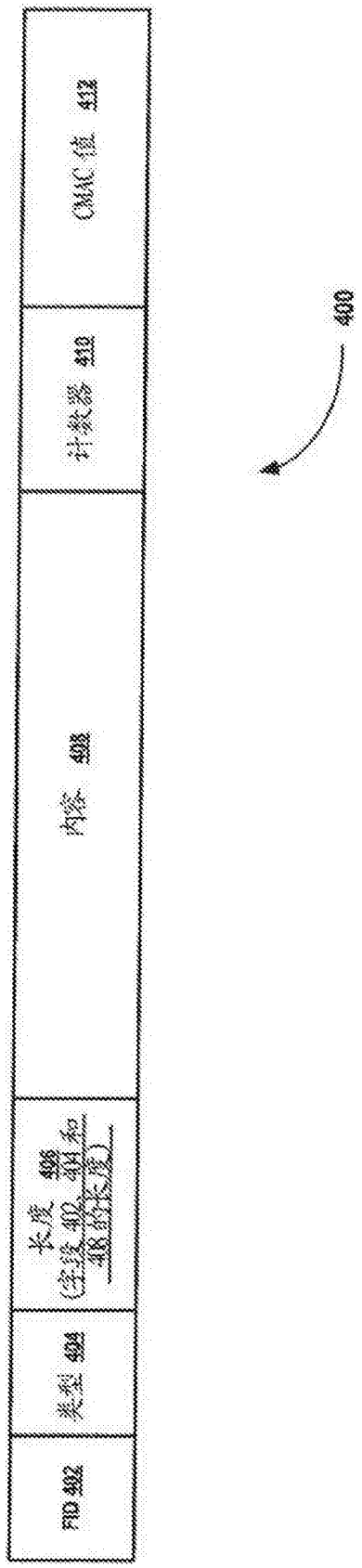

CMAC 值 412
计数器 410
400
内容 408
长度 406
(字段 402、404 和 406 的长度)
类型 404
ID 402

图4a

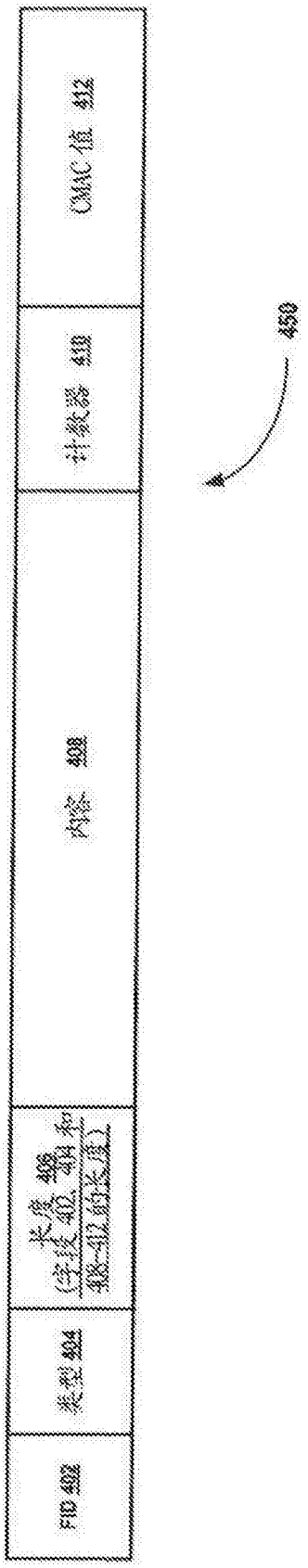

CMAC 值 412
计数器 410
450
内容 408
长度 406
(字段 404 和
406-412 的长度)
类型 404
FID 402

图4b

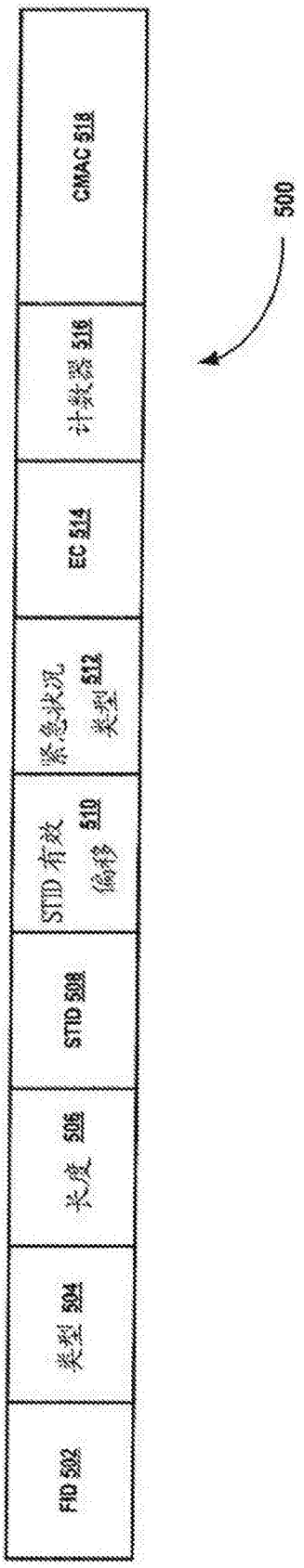

500
CMAC 518
计数器 516
EC 514
紧急状况类型 512
STID 有效偏移 510
STID 508
长度 506
类型 504
FID 502

图5a

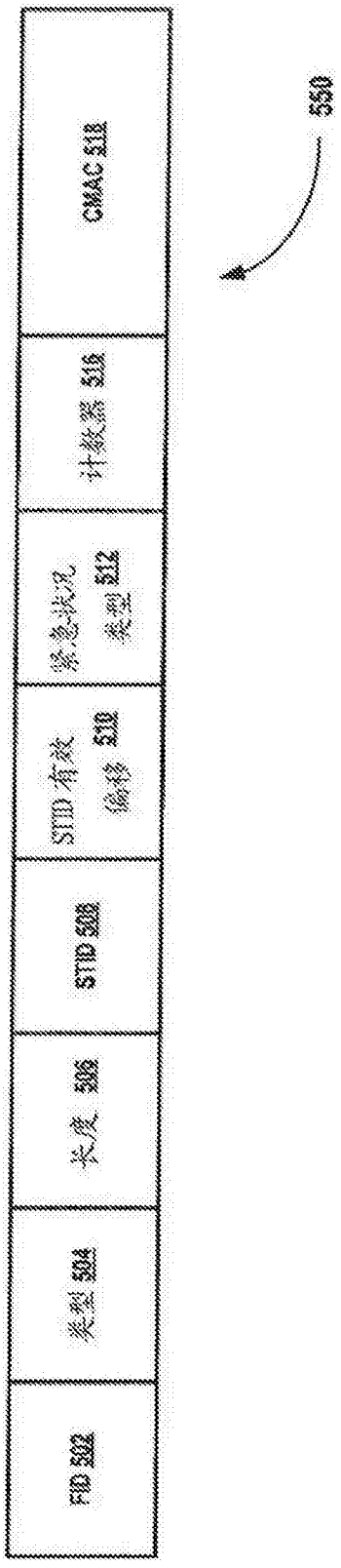

550
CMAC 518
计数器 516
紧急状况类型 512
STID 有效偏移 510
STID 508
长度 506
类型 504
FID 502

图5b

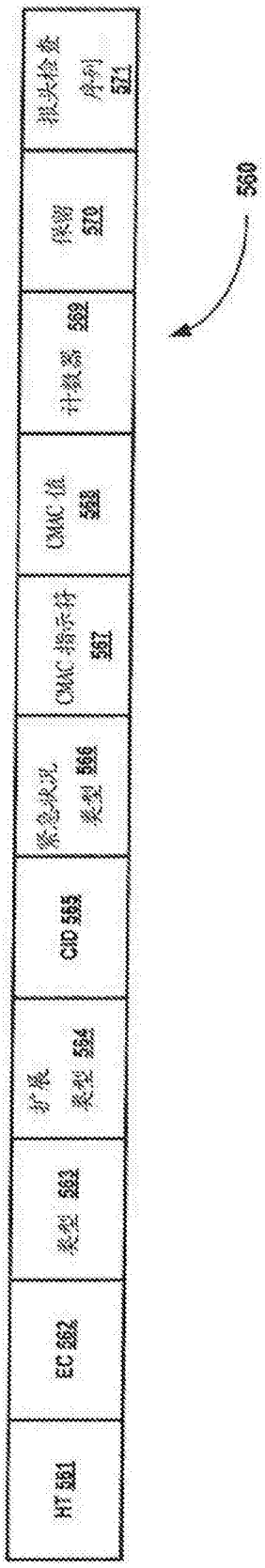

550
HT 581
EC 582
类型 583
扩展 类型 584
CID 585
紧急状况 类型 586
CMAC 指示符 587
CMAC 值 588
计数器 589
保留 570
视决检查 单元 571

图5c


HT 681
EC 682
类型 683
CID 685
紧急状况 类型 688
CMAC 指示符 687
CMAC 值 689
计数器 686
保留 670
报头检查 序列 671
675

图5d

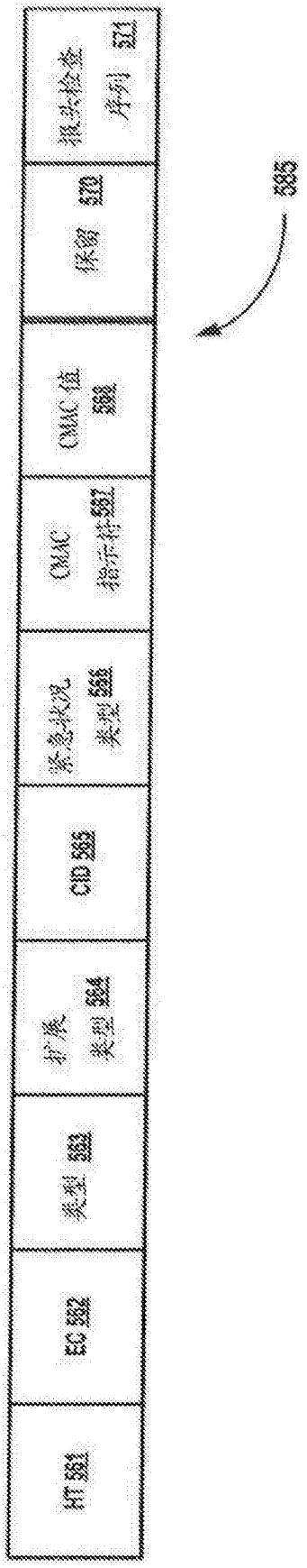

HT 881
EC 882
类型 883
扩展 类型 884
CID 885
紧急状况 类型 886
CMAC 指示符 887
CMAC 值 888
保留 870
报头检查 序列 871
885

图5e

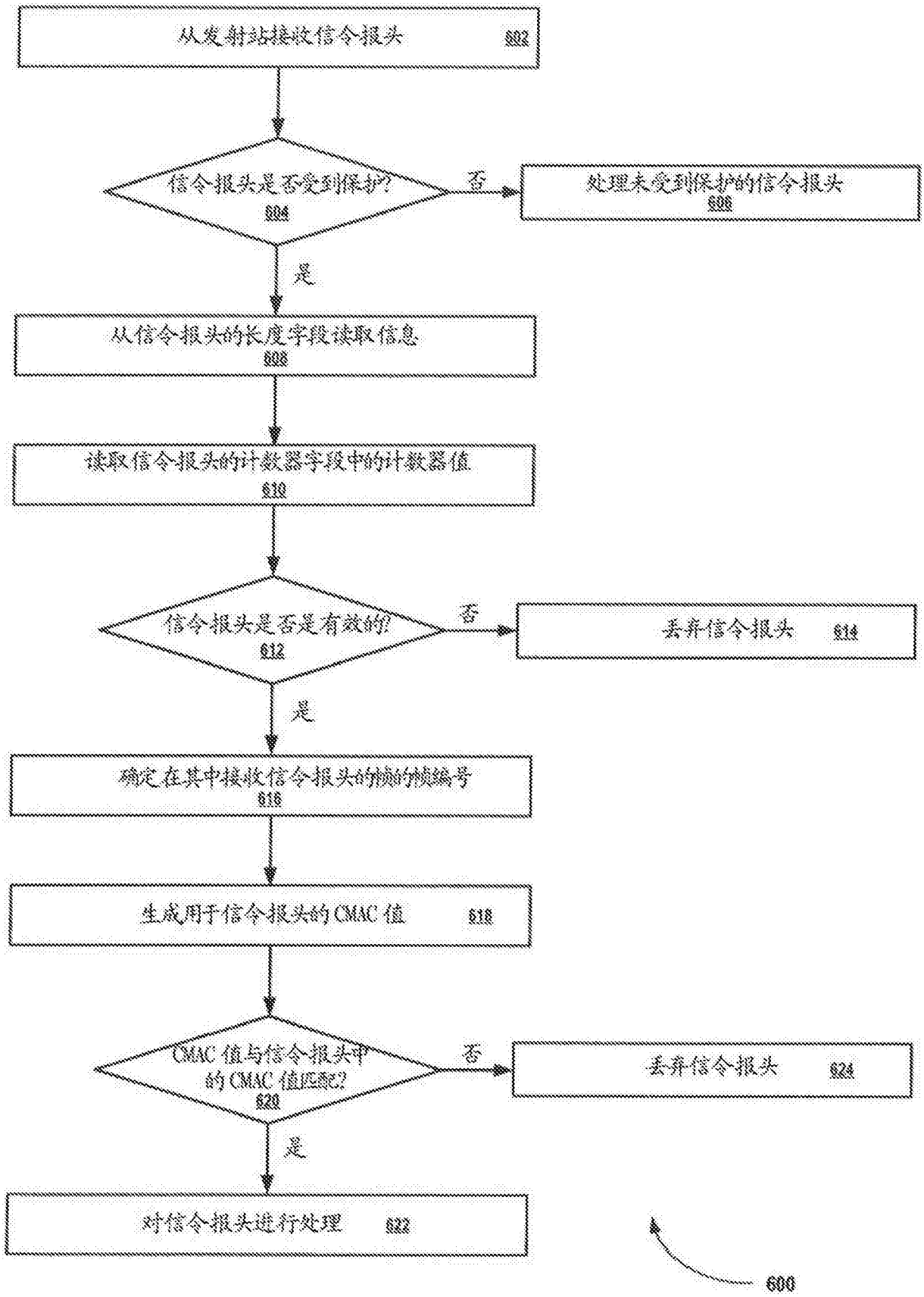

从发射站接收信令报头
802
信令报头是否受到保护?
804
否
处理未受到保护的信令报头
806
是
从信令报头的长度字段读取信息
808
读取信令报头的计数器字段中的计数器值
810
信令报头是否是有效的?
812
否
丢弃信令报头
814
是
确定在其中接收信令报头的帧的帧编号
816
生成用于信令报头的CMAC值
818
CMAC值与信令报头中的CMAC值匹配?
820
否
丢弃信令报头
824
是
对信令报头进行处理
822
600

图6

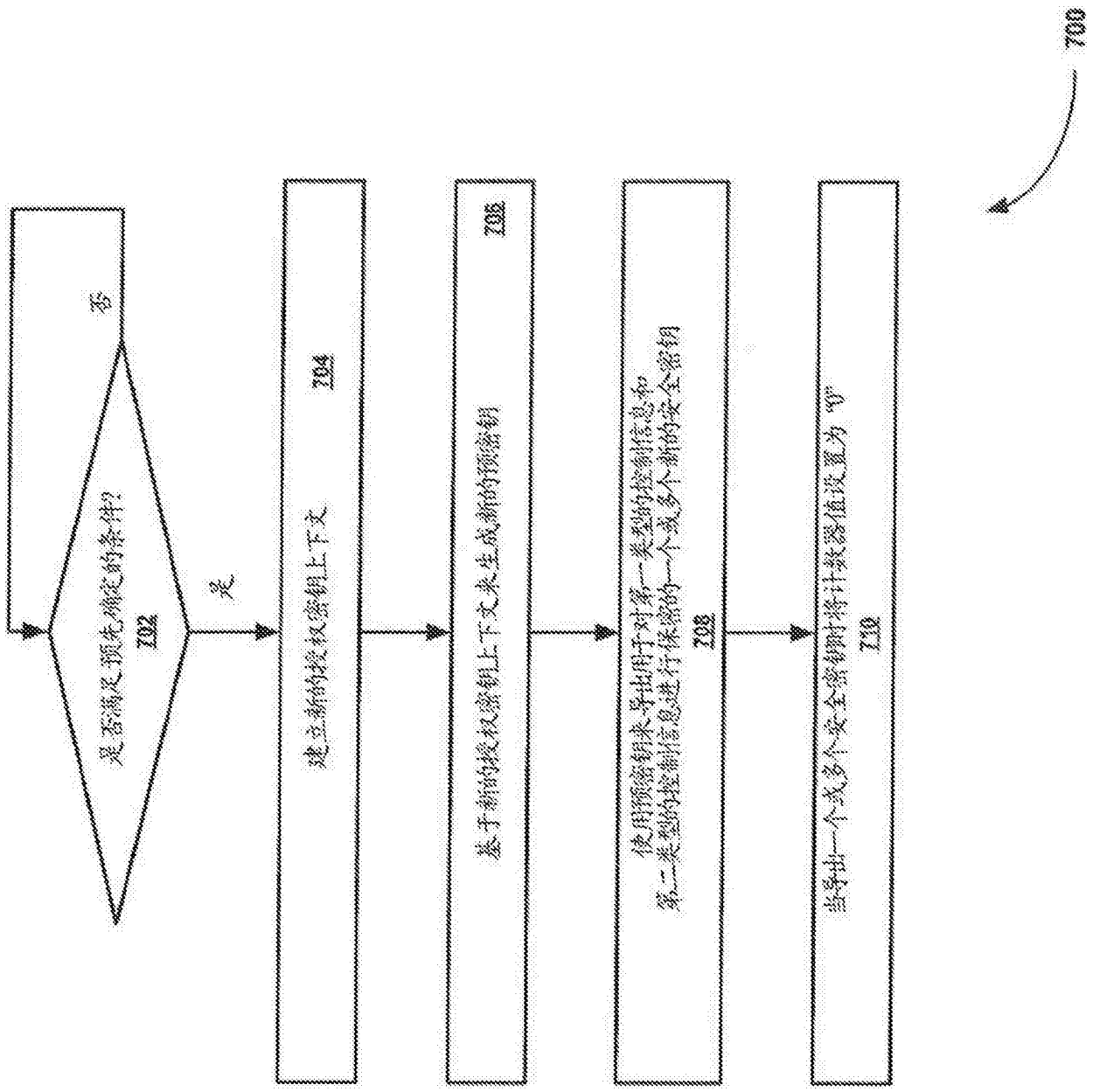

700
否
是否满足预先确定的条件?
702
是
建立新的授权密钥上下文
704
基于新的授权密钥上下文来生成新的预密钥
706
使用预密钥来导出用于对第一类型的控制信息和
第二类型的控制信息进行保密的一个或多个新的安全密钥
708
当导出一个或多个安全密钥时将计数器值设置为"0"
710

图7a

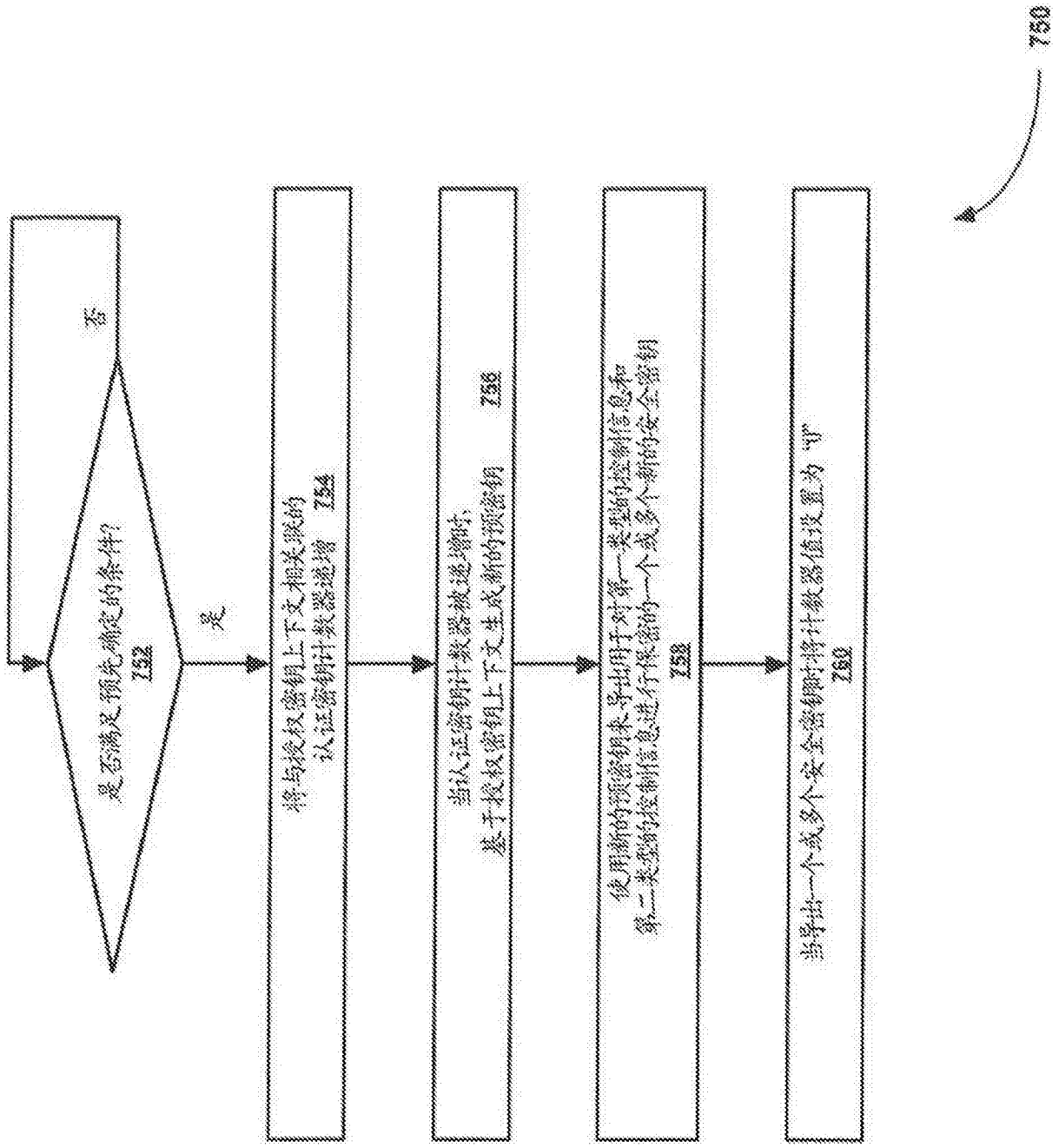

750
否
是否满足预先确定的条件?
732
是
将与授权密钥上下文相关联的
认证密钥计数器递增 734
当认证密钥计数器被递增时,
基于授权密钥上下文生成新的预密钥 736
使用新的预密钥来导出用于对第一类型的控制信息和
第二类型的控制信息进行保密的一个或多个新的安全密钥
738
当导出一个或多个安全密钥时将计数器值设置为"0"
740

图7b

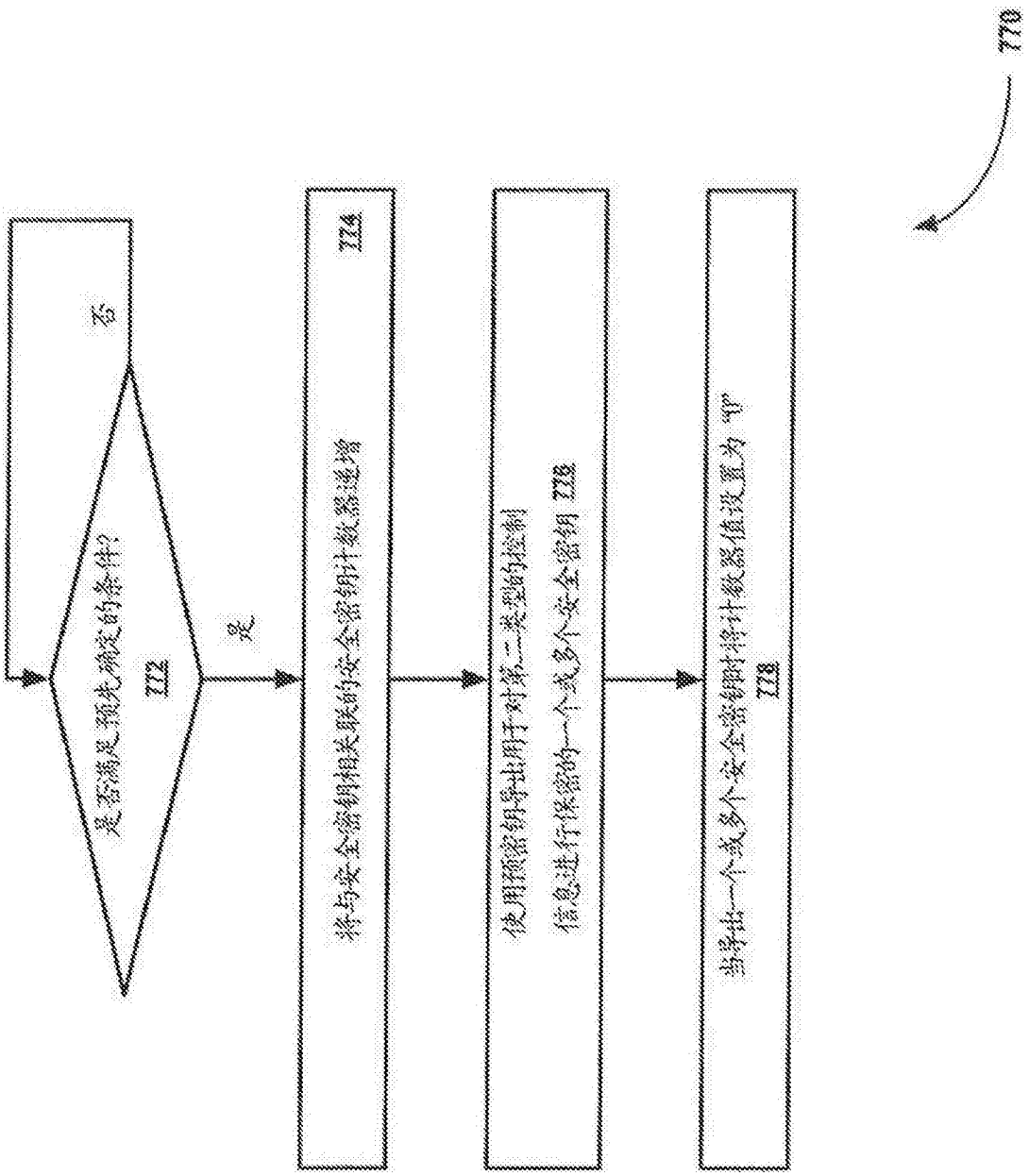

770
否
是否满足预先确定的条件?
772
是
将与安全密钥相关联的安全密钥计数器递增
774
使用预密钥导出用于对第二类型的控制
信息进行保密的一个或多个安全密钥 776
当导出一个或多个安全密钥时将计数器值设置为"0"
778

图7c

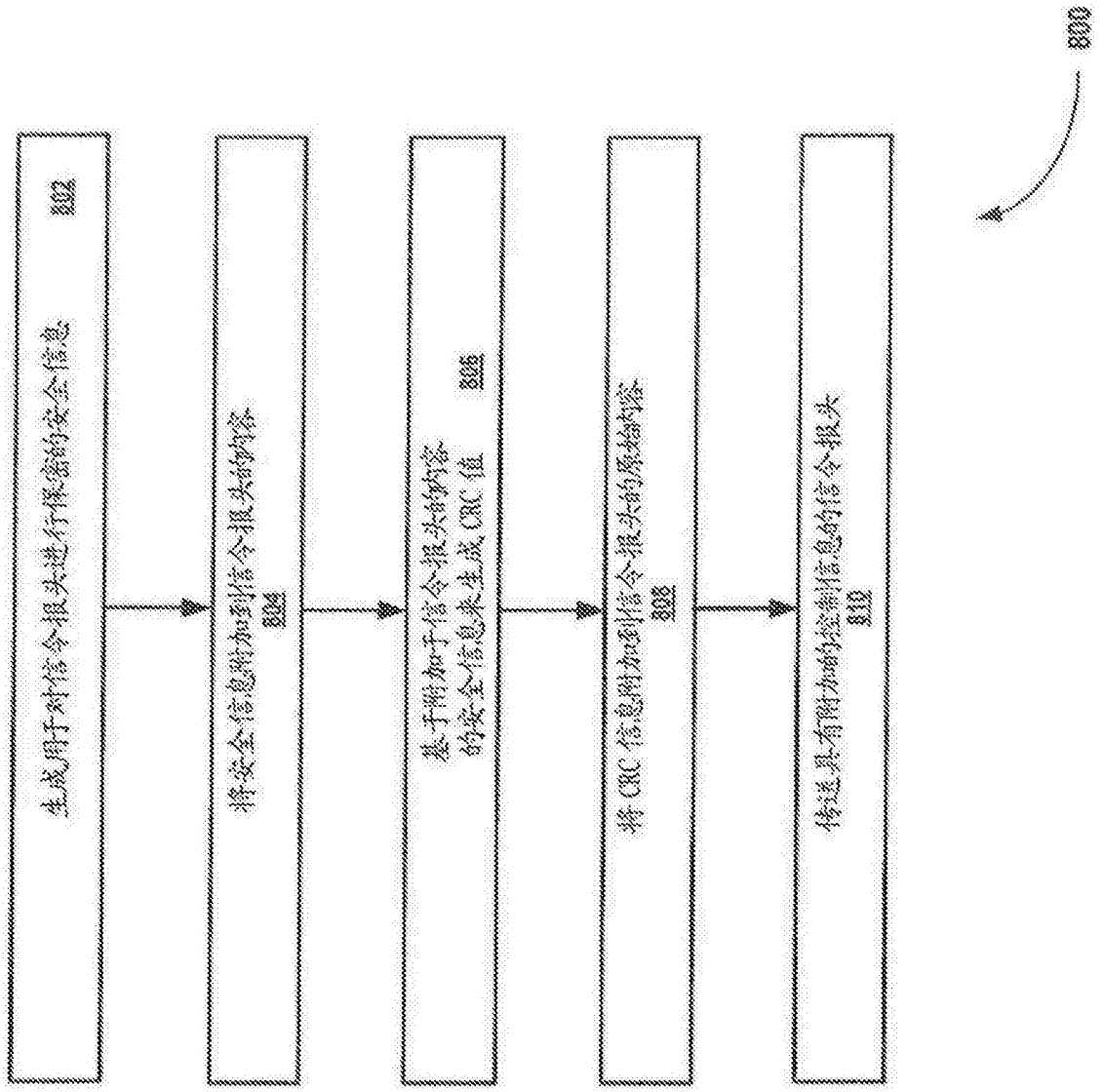

800
生成用于对信令报头进行保密的安全信息
802
将安全信息附加到信令报头的内容
804
基于附加于信令报头的内容的安全信息来生成 CRC 值
806
将 CRC 信息附加到信令报头的原始内容
808
传送具有附加的控制信息的信令报头
810

图8

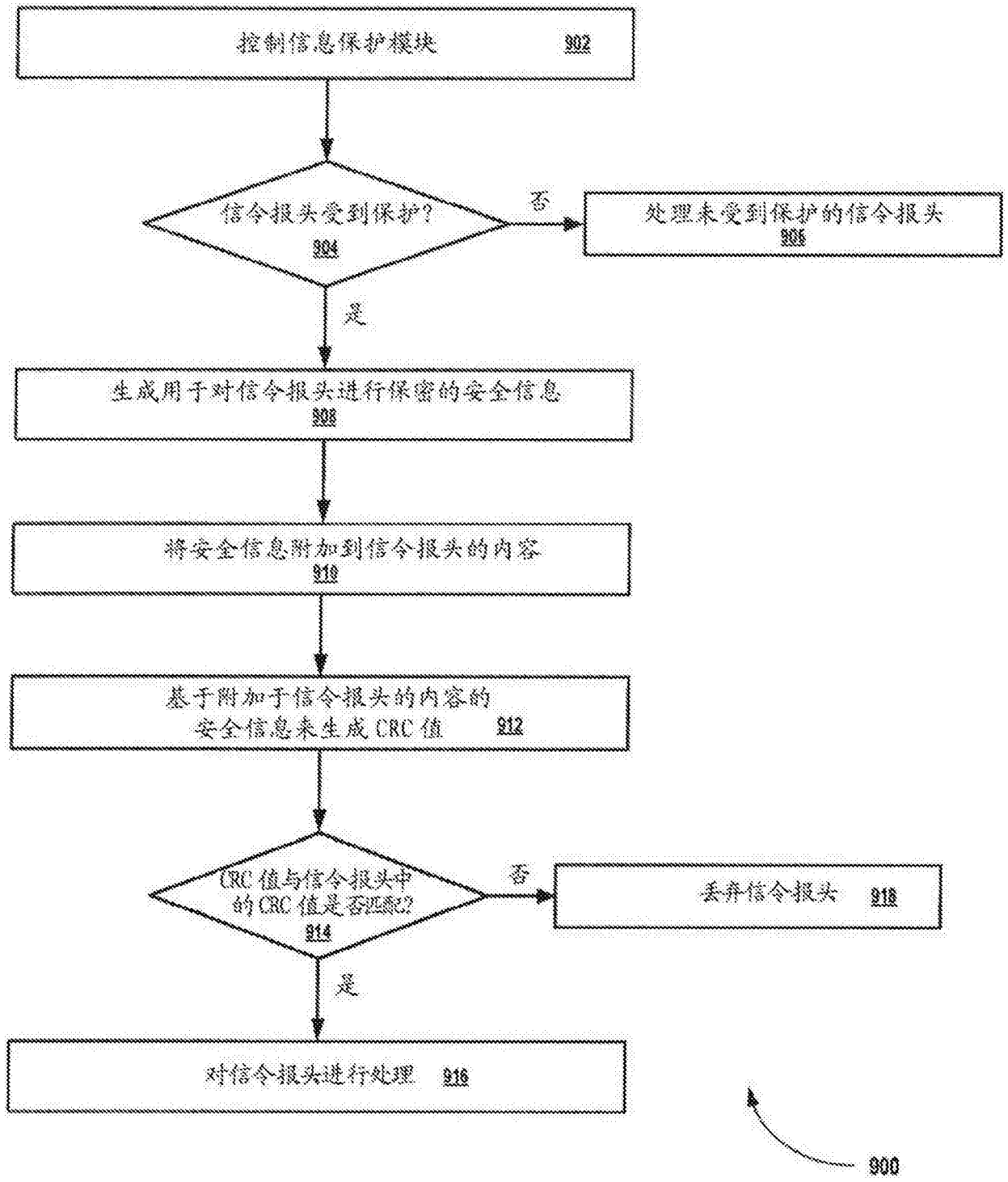

控制信息保护模块 902
信令报头受到保护? 904
否
处理未受到保护的信令报头 906
是
生成用于对信令报头进行保密的安全信息 908
将安全信息附加到信令报头的内容 910
基于附加于信令报头的内容的安全信息来生成 CRC 值 912
CRC 值与信令报头中的 CRC 值是否匹配? 914
否
丢弃信令报头 918
是
对信令报头进行处理 916
900

图9

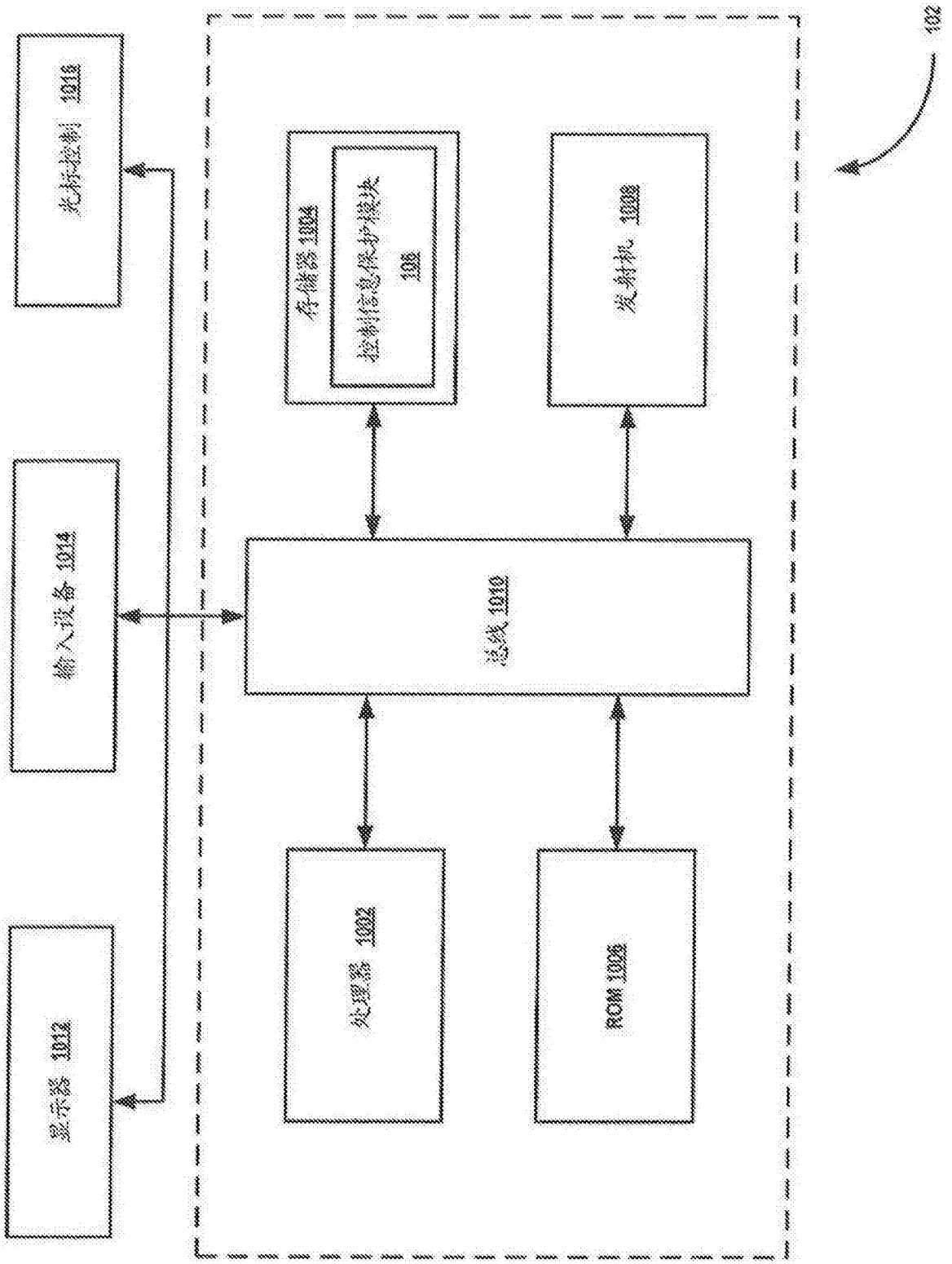

102
光标控制 1016
存储器 1004
控制信息保护模块 108
发射机 1008
输入设备 1014
总线 1010
处理器 1002
ROM 1006
显示器 1012

图10

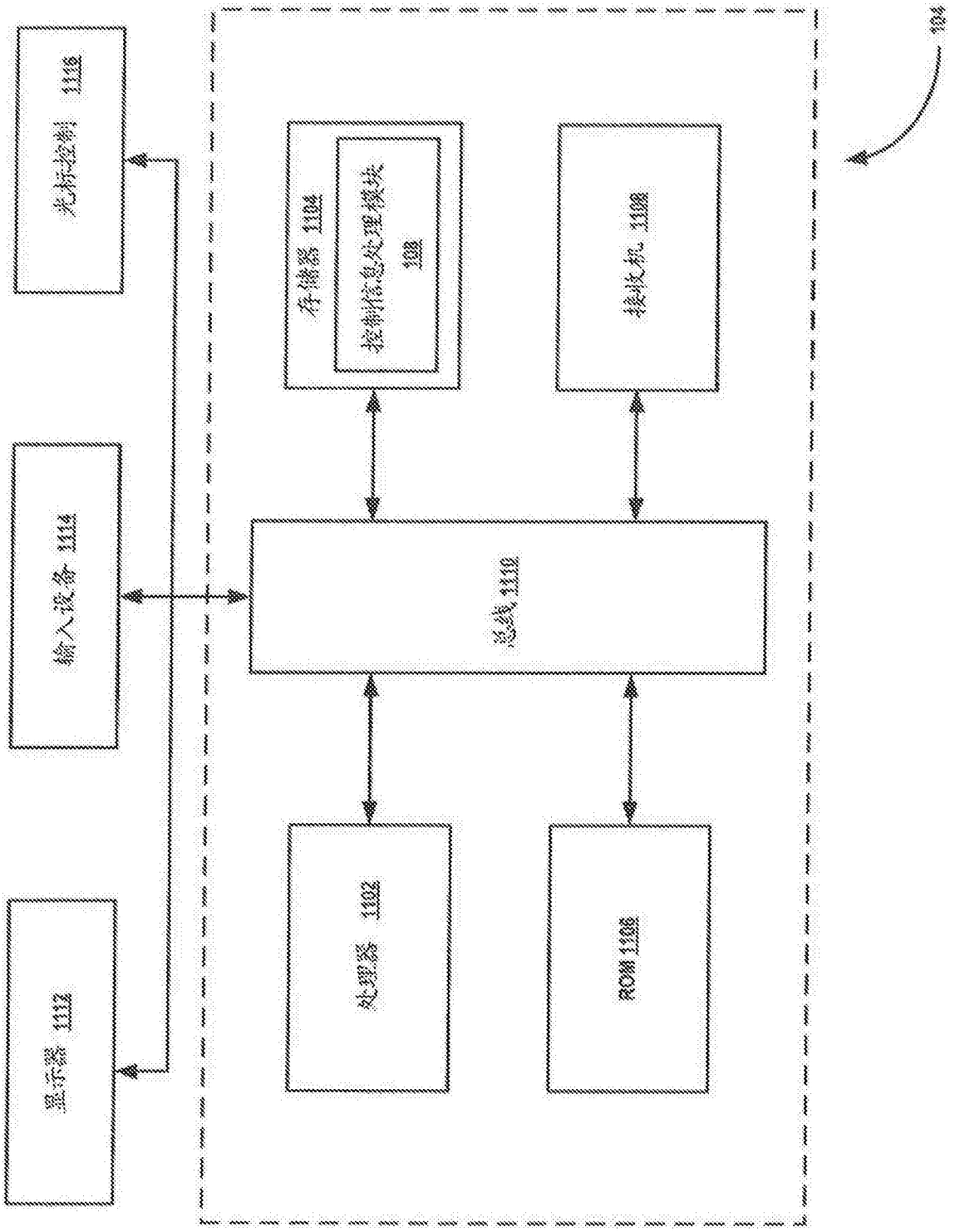

光标控制 1116
存储器 1104
控制信息处理模块 102
接收机 1108
输入设备 1114
总线 1110
处理器 1102
ROM 1106
显示器 1112
104

图11