(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 104509030 B
(45)授权公告日 2017.12.05

(21)申请号 201380018997.7

(22)申请日 2013.03.11

(65)同一申请的已公布的文献号
申请公布号 CN 104509030 A

(43)申请公布日 2015.04.08

(30)优先权数据
61/622,434 2012.04.10 US
13/791,879 2013.03.08 US

(85)PCT国际申请进入国家阶段日
2014.10.08

(86)PCT国际申请的申请数据
PCT/US2013/030277 2013.03.11

(87)PCT国际申请的公布数据
WO2013/154714 EN 2013.10.17

(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·帕拉尼格朗德 J·王 X·张 G·K·沃克

(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.
H04L 12/18(2006.01)
H04L 29/06(2006.01)
H04W 12/06(2006.01)
H04W 4/06(2006.01)
H04L 9/32(2006.01)

(56)对比文件
US 2004203615 A1,2004.10.14,
CN 102047636 A,2011.05.04,
Technical Specification Group Services and System Aspects.Security of Multimedia Broadcast/Multicast Service (MBMS).《3rd Generation Partnership Project》.2010, (续)

审查员 汪三骏

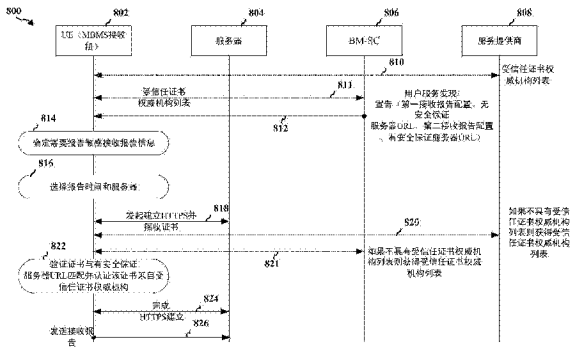
权利要求书7页 说明书14页 附图15页

(54)发明名称

用于安全MBMS接收报告的方法和设备

(57)摘要

在第一配置中,UE(802)从服务提供商(808)接收证书权威机构列表(811)。该证书权威机构列表是基于由UE和服务提供商知晓并存储在UE中的智能卡上的凭证来进行完好性保护或加密中的一者的。UE使用收到的证书权威机构列表来认证服务器。在第二配置中,UE接收包括接收报告配置和服务器地址的用户服务发现/宣告(812)。UE基于接收报告配置将受保护的接收报告发送给服务器(826)。在第三配置中,UE接收受保护的广播宣告(812)并基于该广播宣告来通信(826)。该广播宣告是基于由UE知晓并存储在UE中的智能卡上的凭证来进行完好性保护或加密中的至少一者的。



CN 104509030 B

[转续页]

[接上页]

(56)对比文件

Technical Specification Group Services and System Aspects.Security of Multimedia Broadcast/Multicast Service (MBMS).《3rd Generation Partnership Project》.2010,

Technical Specification Group Services and System Aspects.Multimedia Broadcast/Multicast Service (MBMS).《3rd Generation Partnership Project》.2012,

1.一种用户装备UE无线通信的方法,包括:

从服务提供商接收证书权威机构列表,所述证书权威机构列表是基于由所述UE和所述服务提供商知晓并存储在所述UE中的智能卡上的凭证来进行完好性保护或加密中的至少一者的;

接收包括接收报告配置和服务器的地址的用户服务发现/宣告;

建立与所述服务器的安全连接;

使用收到的证书权威机构列表来认证所述服务器;以及

基于所述地址和所述接收报告配置通过所述安全连接将接收报告发送给所述服务器。

2.如权利要求1所述的方法,其特征在于,所述证书权威机构列表包括受信任证书权威机构的证书。

3.如权利要求1所述的方法,其特征在于,进一步包括:

接收所述服务器的证书;以及

在认证所述服务器之际确定要建立与所述服务器的所述安全连接,

其中所述认证包括基于收到的证书与所述证书权威机构列表的比较来确定所述收到的证书是来自受信任证书权威机构。

4.如权利要求1所述的方法,其特征在于,所述凭证是由所述UE和所述服务提供商知晓的共享密钥。

5.如权利要求4所述的方法,其特征在于,所述共享密钥基于多媒体广播多播服务器MBMS请求密钥MRK、MBMS用户密钥MUK、或从所述MRK或所述MUK之一导出的密钥。

6.如权利要求1所述的方法,其特征在于,所述安全连接是通过安全超文本传输协议HTTPS。

7.如权利要求1所述的方法,其特征在于,所述用户服务发现/宣告是基于由所述UE和广播多播服务中心BM-SC知晓的凭证来进行完好性保护或加密中的至少一者的。

8.如权利要求7所述的方法,其特征在于,所述凭证是基于多媒体广播多播服务器MBMS服务密钥MSK的。

9.一种无线通信的方法,包括:

接收包括接收报告配置和服务器的地址的用户服务发现/宣告;

响应于接收到报告配置和服务器的地址的用户服务发现/宣告,确定是否发送受保护的接收报告;

基于确定发送所述受保护的接收报告设置与所述服务器的安全连接;以及

基于所述接收报告配置或所述服务器的地址之一或两者通过所述安全连接将受保护的接收报告发送给所述服务器。

10.如权利要求9所述的方法,其特征在于,进一步包括建立与所述服务器的安全连接,其中所述受保护的接收报告是通过所述安全连接来发送的。

11.如权利要求10所述的方法,其特征在于,所述安全连接是通过安全超文本传输协议HTTPS。

12.如权利要求9所述的方法,其特征在于,进一步包括:

从服务提供商接收证书权威机构列表;

接收所述服务器的证书;以及

使用收到的证书权威机构列表和所述证书来认证所述服务器。

13.如权利要求12所述的方法，其特征在于，所述证书权威机构列表是基于由用户装备和所述服务提供商知晓的凭证来进行完好性保护或加密中的至少一者的。

14.如权利要求12所述的方法，其特征在于，所述证书权威机构列表包括受信任证书权威机构的证书。

15.如权利要求9所述的方法，其特征在于，进一步包括对所述接收报告进行完好性保护和/或加密。

16.如权利要求15所述的方法，其特征在于，所述进行完好性保护和/或加密是基于多媒体广播多播服务器MBMS注册密钥MRK的。

17.如权利要求9所述的方法，其特征在于，所述用户服务发现/宣告是基于由用户装备和广播多播服务中心BM-SC知晓的凭证来进行完好性保护或加密中的至少一者的。

18.如权利要求17所述的方法，其特征在于，所述凭证是基于多媒体广播多播服务器MBMS服务密钥MSK的。

19.一种用户装备UE无线通信的方法，包括：

接收受保护的广播宣告，所述广播宣告是基于由所述UE知晓并存储在所述UE中的智能卡上的凭证来进行完好性保护或加密中的至少一者的；

在所述广播宣告是经加密的时基于所述凭证解密所述广播宣告和/或在所述广播宣告是受完好性保护的时基于所述凭证验证所述广播宣告的完好性；

确定所述广播宣告是否成功解密和/或完好性检查是否通过；以及

如果所述广播宣告成功解密和/或所述完好性检查通过，基于所述广播宣告来通信。

20.如权利要求19所述的方法，其特征在于，进一步包括在所述广播宣告是经加密的时基于多媒体广播多播服务器MBMS服务密钥MSK来解密所述广播宣告。

21.如权利要求19所述的方法，其特征在于，进一步包括在所述广播宣告是受完好性保护的时基于多媒体广播多播服务器MBMS服务密钥MSK来验证所述广播宣告的完好性，其中所述通信在所述广播宣告的完好性得到验证时基于所述广播宣告而发生。

22.如权利要求19所述的方法，其特征在于，所述广播宣告是包括接收报告配置和服务器的地址的用户服务发现/宣告，并且基于所述广播宣告来通信包括基于所述地址和所述接收报告配置将接收报告发送给所述服务器。

23.如权利要求22所述的方法，其特征在于，所述接收报告是通过安全连接来发送的。

24.如权利要求22所述的方法，其特征在于，所述接收报告是基于多媒体广播多播服务器MBMS注册密钥MRK来进行完好性保护或加密中的至少一者的。

25.一种用于无线通信的设备，包括：

用于从服务提供商接收证书权威机构列表的装置，所述证书权威机构列表是基于由所述设备和所述服务提供商知晓并存储在所述设备中的智能卡上的凭证来进行完好性保护或加密中的至少一者的；

用于接收包括接收报告配置和服务器的地址的用户服务发现/宣告的装置；

用于建立与所述服务器的安全连接的装置；

用于使用收到的证书权威机构列表来认证所述服务器的装置；以及

用于基于所述地址和所述接收报告配置通过所述安全连接将接收报告发送给所述服

务器的装置。

26.如权利要求25所述的设备，其特征在于，所述证书权威机构列表包括受信任证书权威机构的证书。

27.如权利要求25所述的设备，其特征在于，进一步包括：

用于接收所述服务器的证书的装置；以及

用于在认证所述服务器之际确定要建立与所述服务器的所述安全连接的装置，

其中所述用于认证的装置通过基于收到的证书与所述证书权威机构列表的比较从而确定所述收到的证书来自受信任证书权威机构来认证所述服务器。

28.如权利要求25所述的设备，其特征在于，所述凭证是由所述设备和所述服务提供商知晓的共享密钥。

29.如权利要求28所述的设备，其特征在于，所述共享密钥是基于多媒体广播多播服务器MBMS请求密钥MRK、MBMS用户密钥MUK、或从所述MRK或所述MUK之一导出的密钥。

30.如权利要求25所述的设备，其特征在于，所述安全连接是通过安全超文本传输协议HTTPS。

31.如权利要求25所述的设备，其特征在于，所述用户服务发现/宣告是基于由所述设备和广播多播服务中心BM-SC知晓的凭证来进行完好性保护或加密中的至少一者的。

32.如权利要求31所述的设备，其特征在于，所述凭证是基于多媒体广播多播服务器MBMS服务密钥MSK的。

33.一种用于无线通信的设备，包括：

用于接收包括接收报告配置和服务器的地址的用户服务发现/宣告的装置；

用于响应于接收到报告配置和服务器的地址的用户服务发现/宣告，确定是否发送受保护的接收报告的装置；

用于基于确定发送所述受保护的接收报告设置与所述服务器的安全连接的装置；以及

用于基于所述接收报告配置或所述服务器的地址之一或两者通过所述安全连接将受保护的接收报告发送给所述服务器的装置。

34.如权利要求33所述的设备，其特征在于，进一步包括用于建立与所述服务器的安全连接的装置，其中所述受保护的接收报告是通过所述安全连接来发送的。

35.如权利要求34所述的设备，其特征在于，所述安全连接是通过安全超文本传输协议HTTPS。

36.如权利要求33所述的设备，其特征在于，进一步包括：

用于从服务提供商接收证书权威机构列表的装置；

用于接收所述服务器的证书的装置；以及

用于使用收到的证书权威机构列表和所述证书来认证所述服务器的装置。

37.如权利要求36所述的设备，其特征在于，所述证书权威机构列表是基于由所述设备和所述服务提供商知晓的凭证来进行完好性保护或加密中的至少一者的。

38.如权利要求36所述的设备，其特征在于，所述证书权威机构列表包括受信任证书权威机构的证书。

39.如权利要求33所述的设备，其特征在于，进一步包括用于对所述接收报告进行完好性保护和/或加密的装置。

40.如权利要求39所述的设备，其特征在于，所述用于进行完好性保护和/或加密的装置基于多媒体广播多播服务器MBMS请求密钥MRK或MBMS用户密钥MUK来进行完好性保护和/或加密。

41.如权利要求33所述的设备，其特征在于，所述用户服务发现/宣告是基于由所述设备和广播多播服务中心BM-SC知晓的凭证来进行完好性保护或加密中的至少一者的。

42.如权利要求41所述的设备，其特征在于，所述凭证是基于多媒体广播多播服务器MBMS服务密钥MSK的。

43.一种用于用户装备UE的无线通信的设备，包括：

用于接收受保护的广播宣告的装置，所述广播宣告是基于由所述UE知晓并存储在所述UE中的智能卡上的凭证来进行完好性保护或加密中的至少一者的；

用于在所述广播宣告是经加密的时基于所述凭证解密所述广播宣告和/或在所述广播宣告是受完好性保护的时基于所述凭证验证所述广播宣告的完好性的装置；

用于确定所述广播宣告是否成功解密和/或完好性检查是否通过的装置；以及

用于如果所述广播宣告成功解密和/或所述完好性检查通过，基于所述广播宣告来通信的装置。

44.如权利要求43所述的设备，其特征在于，进一步包括用于在所述广播宣告是经加密的时基于多媒体广播多播服务器MBMS服务密钥MSK来解密所述广播宣告的装置。

45.如权利要求43所述的设备，其特征在于，进一步包括用于在所述广播宣告是受完好性保护的时基于多媒体广播多播服务器MBMS服务密钥MSK来验证所述广播宣告的完好性的装置，其中所述用于通信的装置在所述广播宣告的完好性得到验证时基于所述广播宣告进行通信。

46.如权利要求43所述的设备，其特征在于，所述广播宣告是包括接收报告配置和服务器的地址的用户服务发现/宣告，并且所述用于通信的装置通过基于所述地址和所述接收报告配置将接收报告发送给所述服务器来基于所述广播宣告进行通信。

47.如权利要求46所述的设备，其特征在于，所述接收报告是通过安全连接来发送的。

48.如权利要求46所述的设备，其特征在于，所述接收报告是基于多媒体广播多播服务器MBMS请求密钥MRK或MBMS用户密钥MUK来进行完好性保护或加密中的至少一者的。

49.一种用于无线通信的装置，包括：

存储器；以及

耦合至所述存储器的至少一个处理器，其被配置成：

从服务提供商接收证书权威机构列表，所述证书权威机构列表是基于由所述装置和所述服务提供商知晓并存储在所述装置中的智能卡上的凭证来进行完好性保护或加密中的至少一者的；

接收包括接收报告配置和服务器的地址的用户服务发现/宣告；

建立与所述服务器的安全连接；

使用收到的证书权威机构列表来认证所述服务器；以及

基于所述地址和所述接收报告配置通过所述安全连接将接收报告发送给所述服务器。

50.如权利要求49所述的装置，其特征在于，所述证书权威机构列表包括受信任证书权威机构的证书。

51.如权利要求49所述的装置，其特征在于，所述至少一个处理器被进一步配置成：

接收所述服务器的证书；以及

在认证所述服务器之际确定要建立与所述服务器的所述安全连接，

其中所述至少一个处理器通过基于收到的证书与所述证书权威机构列表的比较从而确定所述收到的证书来自受信任证书权威机构来进行认证。

52.如权利要求49所述的装置，其特征在于，所述凭证是由所述装置和所述服务提供商知晓的共享密钥。

53.如权利要求52所述的装置，其特征在于，所述共享密钥是基于多媒体广播多播服务器MBMS请求密钥MRK、MBMS用户密钥MUK、或从所述MRK或所述MUK之一导出的密钥。

54.如权利要求49所述的装置，其特征在于，所述安全连接是通过安全超文本传输协议HTTPS。

55.如权利要求49所述的装置，其特征在于，所述用户服务发现/宣告是基于由所述装置和广播多播服务中心BM-SC知晓的凭证来进行完好性保护或加密中的至少一者的。

56.如权利要求55所述的装置，其特征在于，所述凭证是基于多媒体广播多播服务器MBMS服务密钥MSK的。

57.一种用于无线通信的装置，包括：

存储器；以及

耦合至所述存储器的至少一个处理器，其被配置成：

接收包括接收报告配置和服务器的地址的用户服务发现/宣告；

响应于接收到报告配置和服务器的地址的用户服务发现/宣告，确定是否发送受保护的接收报告；

基于确定发送所述受保护的接收报告设置与所述服务器的安全连接；以及

基于所述接收报告配置或所述服务器的地址之一或两者通过所述安全连接将受保护的接收报告发送给所述服务器。

58.如权利要求57所述的装置，其特征在于，所述至少一个处理器被进一步配置成建立与所述服务器的安全连接，其中所述受保护的接收报告是通过所述安全连接来发送的。

59.如权利要求58所述的装置，其特征在于，所述安全连接是通过安全超文本传输协议HTTPS。

60.如权利要求57所述的装置，其特征在于，所述至少一个处理器被进一步配置成：

从服务提供商接收证书权威机构列表；

接收所述服务器的证书；以及

使用收到的证书权威机构列表和所述证书来认证所述服务器。

61.如权利要求60所述的装置，其特征在于，所述证书权威机构列表是基于由所述装置和所述服务提供商知晓的凭证来进行完好性保护或加密中的至少一者的。

62.如权利要求60所述的装置，其特征在于，所述证书权威机构列表包括受信任证书权威机构的证书。

63.如权利要求57所述的装置，其特征在于，所述至少一个处理器被进一步配置成对所述接收报告进行完好性保护和/或加密。

64.如权利要求63所述的装置，其特征在于，所述至少一个处理器基于多媒体广播多播

服务器MBMS请求密钥MRK或MBMS用户密钥MUK来进行完好性保护和/或加密。

65.如权利要求57所述的装置，其特征在于，所述用户服务发现/宣告是基于由所述装置和广播多播服务中心BM-SC知晓的凭证来进行完好性保护或加密中的至少一者的。

66.如权利要求65所述的装置，其特征在于，所述凭证是基于多媒体广播多播服务器MBMS服务密钥MSK的。

67.一种用于用户装备UE的无线通信的装置，包括：

存储器；以及

耦合至所述存储器的至少一个处理器，其被配置成：

接收受保护的广播宣告，所述广播宣告是基于由所述UE知晓并存储在所述UE中的智能卡上的凭证来进行完好性保护或加密中的至少一者的；

在所述广播宣告是经加密的时基于所述凭证解密所述广播宣告和/或在所述广播宣告是受完好性保护的时基于所述凭证验证所述广播宣告的完好性；

确定所述广播宣告是否成功解密和/或完好性检查是否通过；以及

如果所述广播宣告成功解密和/或所述完好性检查通过，基于所述广播宣告来通信。

68.如权利要求67所述的装置，其特征在于，所述至少一个处理器被进一步配置成在所述广播宣告是经加密的时基于多媒体广播多播服务器MBMS服务密钥MSK来解密所述广播宣告。

69.如权利要求67所述的装置，其特征在于，所述至少一个处理器被进一步配置成在所述广播宣告是受完好性保护的时基于多媒体广播多播服务器MBMS服务密钥MSK来验证所述广播宣告的完好性，其中所述至少一个处理器在所述广播宣告的完好性得到验证时基于所述广播宣告进行通信。

70.如权利要求67所述的装置，其特征在于，所述广播宣告是包括接收报告配置和服务器的地址的用户服务发现/宣告，并且所述至少一个处理器通过基于所述地址和所述接收报告配置将接收报告发送给所述服务器来基于所述广播宣告进行通信。

71.如权利要求70所述的装置，其特征在于，所述接收报告是通过安全连接来发送的。

72.如权利要求70所述的装置，其特征在于，所述接收报告是基于多媒体广播多播服务器MBMS注册密钥MRK来进行完好性保护或加密中的至少一者的。

73.一种与用户装备UE相关联的计算机可读介质，其包括用于以下操作的代码：

从服务提供商接收证书权威机构列表，所述证书权威机构列表是基于由所述UE和所述服务提供商知晓并存储在所述UE中的智能卡上的凭证来进行完好性保护或加密中的至少一者的；

接收包括接收报告配置和服务器的地址的用户服务发现/宣告；

建立与所述服务器的安全连接；

使用收到的证书权威机构列表来认证所述服务器；以及

基于所述地址和所述接收报告配置通过所述安全连接将接收报告发送给所述服务器。

74.一种计算机可读介质，其包括用于以下操作的代码：

接收包括接收报告配置和服务器的地址的用户服务发现/宣告；

响应于接收到报告配置和服务器的地址的用户服务发现/宣告，确定是否发送受保护的接收报告；

基于确定发送所述受保护的接收报告设置与所述服务器的安全连接;以及

基于所述接收报告配置或所述服务器的地址之一或两者通过所述安全连接将受保护的接收报告发送给所述服务器。

75.一种与用户装备UE相关联的计算机可读介质,其包括用于以下操作的代码:

接收受保护的广播宣告,所述广播宣告是基于由所述UE知晓并存储在所述UE中的智能卡上的凭证来进行完好性保护或加密中的至少一者的;

在所述广播宣告是经加密的时基于所述凭证解密所述广播宣告和/或在所述广播宣告是受完好性保护的时基于所述凭证验证所述广播宣告的完好性;

确定所述广播宣告是否成功解密和/或完好性检查是否通过;以及

如果所述广播宣告成功解密和/或所述完好性检查通过,基于所述广播宣告来通信。

用于安全MBMS接收报告的方法和设备

[0001] 相关申请的交叉引用

[0002] 本申请要求于2012年4月10日提交的题为“Secure Reception Reporting(安全接收报告)”的美国临时申请S/N.61/622,434以及于2013年3月8日提交的题为“Secure Resource Reporting(安全资源报告)”的美国专利申请No.13/791,879的权益,这两件申请通过援引被整体明确纳入于此。

技术领域

[0003] 本公开一般涉及通信系统,更具体地涉及安全接收报告。

背景技术

[0004] 无线通信系统被广泛部署以提供诸如电话、视频、数据、消息收发、和广播等各种电信服务。典型的无线通信系统可采用能够通过共享可用的系统资源(例如,带宽、发射功率)来支持与多用户通信的多址技术。这类多址技术的示例包括码分多址(CDMA)系统、时分多址(TDMA)系统、频分多址(FDMA)系统、正交频分多址(OFDMA)系统、单载波频分多址(SC-FDMA)系统、和时分同步码分多址(TD-SCDMA)系统。

[0005] 这些多址技术已在各种电信标准中被采纳以提供使不同的无线设备能够在城市、国家、地区、以及甚至全球级别上进行通信的共同协议。新兴电信标准的一示例是长期演进(LTE)。LTE是对由第三代伙伴项目(3GPP)颁布的通用移动电信系统(UMTS)移动标准的增强集。它被设计成通过提高频谱效率、降低成本、改善服务、利用新频谱、以及更好地与在下行链路(DL)上使用OFDMA、在上行链路(UL)上使用SC-FDMA以及使用多输入多输出(MIMO)天线技术的其他开放标准整合来更好地支持移动宽带因特网接入。然而,随着对移动宽带接入的需求持续增长,存在要在LTE技术中作出进一步改进的需要。较佳地,这些改进应当适用于其他多址技术以及采用这些技术的电信标准。

发明内容

[0006] 在本公开的一方面,提供了方法、计算机程序产品、和装置UE。该UE从服务提供商接收证书权威机构列表。该证书权威机构列表是基于由UE和服务提供商知晓并存储在UE中的智能卡上的凭证来进行完好性保护或加密中的至少一者的。另外,UE使用收到的证书权威机构列表来认证服务器。

[0007] 在本公开的一方面,提供了方法、计算机程序产品、和装置。该装置接收包括接收报告配置和服务器地址的用户服务发现/宣告。另外,该装置基于接收报告配置将受保护的接收报告发送给服务器。

[0008] 在本公开的一方面,提供了方法、计算机程序产品、和装置。该装置可以是UE。UE接收受保护的广播宣告。该广播宣告是基于由UE知晓并存储在UE中的智能卡上的凭证来进行完好性保护或加密中的至少一者的。另外,UE基于广播宣告来通信。

附图说明

[0009] 图1是解说网络架构的示例的示图。

[0010] 图2是解说接入网的示例的示图。

[0011] 图3是解说LTE中的DL帧结构的示例的示图。

[0012] 图4是解说LTE中的UL帧结构的示例的示图。

[0013] 图5是解说用于用户面和控制面的无线电协议架构的示例的示图。

[0014] 图6是解说接入网中的演进型B节点和用户装备的示例的示图。

[0015] 图7A是解说多播广播单频网中演进型多媒体广播多播服务信道配置的示例的示图。

[0016] 图7B是解说多播信道调度信息媒体接入控制的控制元素的格式的示图。

[0017] 图8是解说用于发送安全接收报告的第一示例性方法的示图。

[0018] 图9是解说用于发送安全接收报告的第二示例性方法的示图。

[0019] 图10是解说用于接收和处理安全用户服务发现/宣告的示例性方法的示图。

[0020] 图11是第一无线通信方法的流程图。

[0021] 图12是第二无线通信方法的流程图。

[0022] 图13是第三无线通信方法的流程图。

[0023] 图14是解说示例性设备中的不同模块/装置/组件之间的数据流的概念性数据流图。

[0024] 图15是解说采用处理系统的装置的硬件实现的示例的示图。

具体实施方式

[0025] 以下结合附图阐述的详细描述旨在作为各种配置的描述，而无意表示可实践本文所描述的概念的仅有配置。本详细描述包括具体细节来提供对各种概念的透彻理解。然而，对于本领域技术人员将显而易见的是，没有这些具体细节也可实践这些概念。在一些实例中，以框图形式示出众所周知的结构和组件以便避免淡化此类概念。

[0026] 现在将参照各种装置和方法给出电信系统的若干方面。这些装置和方法将在以下详细描述中进行描述并在附图中由各种框、模块、组件、电路、步骤、过程、算法等(统称为“元素”)来解说。这些元素可使用电子硬件、计算机软件或其任何组合来实现。此类元素是实现成硬件还是软件取决于具体应用和加诸于整体系统上的设计约束。

[0027] 作为示例，元素、或元素的任何部分、或者元素的任何组合可用包括一个或多个处理器的“处理系统”来实现。处理器的示例包括：微处理器、微控制器、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、可编程逻辑器件(PLD)、状态机、门控逻辑、分立的硬件电路以及其他配置成执行本公开中通篇描述的各种功能性的合适硬件。处理系统中的一个或多个处理器可以执行软件。软件应当被宽泛地解释成意为指令、指令集、代码、代码段、程序代码、程序、子程序、软件模块、应用、软件应用、软件包、例程、子例程、对象、可执行件、执行的线程、规程、函数等，无论其是用软件、固件、中间件、微代码、硬件描述语言、还是其他术语来述及皆是如此。

[0028] 相应地，在一个或多个示例性实施例中，所描述的功能可被实现在硬件、软件、固

件，或其任何组合中。如果被实现在软件中，那么这些功能可作为一条或多条指令或代码被存储或编码在计算机可读介质上。计算机可读介质包括计算机存储介质。存储介质可以是能被计算机访问的任何可用介质。作为示例而非限制，此类计算机可读介质可包括RAM、ROM、EEPROM、CD-ROM或其他光盘存储、磁盘存储或其他磁存储设备、或能被用来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他介质。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)、和软盘，其中盘常常磁性地再现数据，而碟用激光来光学地再现数据。上述的组合也应被包括在计算机可读介质的范围内。

[0029] 图1是解说LTE网络架构100的示图。LTE网络架构100可称为演进型分组系统(EPS)100。EPS 100可包括一个或多个用户装备(UE)102、演进型UMTS地面无线电接入网(E-UTRAN)104、演进型分组核心(EPC)110、归属订户服务器(HSS)120以及运营商的网际协议(IP)服务122。EPS可与其他接入网互连，但出于简单化起见，那些实体/接口并未示出。如图所示，EPS提供分组交换服务，然而，如本领域技术人员将容易领会的，本公开中通篇给出的各种概念可被扩展到提供电路交换服务的网络。

[0030] E-UTRAN包括演进型B节点(eNB)106和其他eNB 108。eNB 106提供朝向UE 102的用户面和控制面的协议终接。eNB 106可经由回程(例如，X2接口)连接到其他eNB 108。eNB 106也可称为基站、B节点、接入点、基收发机站、无线电基站、无线电收发机、收发机功能、基本服务集(BSS)、扩展服务集(ESS)、或其他某个合适的术语。eNB 106为UE 102提供去往EPC 110的接入点。UE 102的示例包括蜂窝电话、智能电话、会话发起协议(SIP)电话、膝上型设备、个人数字助理(PDA)、卫星无线电、全球定位系统、多媒体设备、视频设备、数字音频播放器(例如，MP3播放器)、相机、游戏控制台、平板设备、或任何其他类似的功能设备。UE 102也可被本领域技术人员称为移动站、订户站、移动单元、订户单元、无线单元、远程单元、移动设备、无线设备、无线通信设备、远程设备、移动订户站、接入终端、移动终端、无线终端、远程终端、手持机、用户代理、移动客户端、客户端、或其他某个合适的术语。

[0031] eNB 106连接到EPC 110。EPC 110包括移动性管理实体(MME)112、其他MME 114、服务网关116、多媒体广播多播服务(MBMS)网关124、广播多播服务中心(BM-SC)126、以及分组数据网络(PDN)网关118。MME 112是处理UE 102与EPC 110之间的信令的控制节点。一般而言，MME 112提供承载和连接管理。所有用户IP分组通过服务网关116来传递，服务网关116自身连接到PDN网关118。PDN网关118提供UE IP地址分配以及其他功能。PDN网关118连接到运营商的IP服务122。运营商的IP服务122可包括因特网、内联网、IP多媒体子系统(IMS)、以及PS流送服务(PSS)。BM-SC 126可提供用于MBMS用户服务置备和递送的功能。BM-SC 126可用作内容提供商MBMS传输的进入点、可用来授权和发起PLMN内的MBMS承载服务、并且可用来调度和递送MBMS传输。MBMS网关124可用来向属于广播特定服务的多播广播单频网(MBSFN)区域的eNB(例如，106、108)分发MBMS话务，并且可负责会话管理(开始/停止)并负责收集eMBMS相关的收费信息。

[0032] 图2是解说LTE网络架构中的接入网200的示例的示图。在这一示例中，接入网200被划分成数个蜂窝区划(蜂窝小区)202。一个或多个较低功率类eNB 208可具有与这些蜂窝小区202中的一个或多个蜂窝小区交叠的蜂窝区划210。较低功率类eNB 208可以是毫微微蜂窝小区(例如，家用eNB(HeNB))、微微蜂窝小区、微蜂窝小区或远程无线电头端(RRH)。宏

eNB 204各自被指派给相应的蜂窝小区202并且配置成为蜂窝小区202中的所有UE 206提供去往EPC 110的接入点。在接入网200的这一示例中，没有集中式控制器，但是在替换性配置中可以使用集中式控制器。eNB 204负责所有与无线电有关的功能，包括无线电承载控制、准入控制、移动性控制、调度、安全性、以及与服务网关116的连通性。eNB可支持一个或多个(例如，三个)蜂窝小区(也称为扇区)。术语“蜂窝小区”可指eNB的最小覆盖区域和/或服务特定覆盖区域的eNB子系统。此外，术语“eNB”、“基站”和“蜂窝小区”可在本文中可互换地使用。

[0033] 接入网200所采用的调制和多址方案可以取决于正部署的特定电信标准而变动。在LTE应用中，在DL上使用OFDM并且在UL上使用SC-FDMA以支持频分双工(FDD)和时分双工(TDD)两者。如本领域技术人员将容易地从以下详细描述中领会的，本文给出的各种概念良好地适用于LTE应用。然而，这些概念可以容易地扩展到采用其他调制和多址技术的其他电信标准。作为示例，这些概念可扩展到演进数据最优化(EV-DO)或超移动宽带(UMB)。EV-DO和UMB是由第三代伙伴项目2(3GPP2)颁布的作为CDMA2000标准族的一部分的空中接口标准，并且采用CDMA向移动站提供宽带因特网接入。这些概念还可扩展到采用宽带CDMA(W-CDMA)和其他CDMA变体(诸如TD-SCDMA)的通用地面无线电接入(UTRA)；采用TDMA的全球移动通信系统(GSM)；以及采用OFDMA的演进型UTRA(E-UTRA)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20和Flash-OFDM。UTRA、E-UTRA、UMTS、LTE和GSM在来自3GPP组织的文献中描述。CDMA2000和UMB在来自3GPP2组织的文献中描述。所采用的实际无线通信标准和多址技术将取决于具体应用以及加诸于系统的整体设计约束。

[0034] eNB 204可具有支持MIMO技术的多个天线。MIMO技术的使用使得eNB 204能够利用空域来支持空间复用、波束成形和发射分集。空间复用可被用于在相同频率上同时传送不同的数据流。这些数据流可被传送给单个UE 206以增大数据率或传送给多个UE 206以增加系统总容量。这是藉由对每一数据流进行空间预编码(即，应用振幅和相位的比例缩放)并且随后通过多个发射天线在DL上传送每一经空间预编码的流来达成的。经空间预编码的数据流带有不同空间签名地抵达(诸)UE 206处，这使得(诸)UE 206中的每个UE 206能够恢复以该UE 206为目的地的一个或多个数据流。在UL上，每个UE 206传送经空间预编码的数据流，这使得eNB 204能够标识每个经空间预编码的数据流的源。

[0035] 空间复用一般在信道状况良好时使用。在信道状况不那么有利时，可使用波束成形来将发射能量集中在一个或多个方向上。这可以藉由对数据进行用于通过多个天线发射的空间预编码来达成。为了在蜂窝小区边缘处达成良好覆盖，单流波束成形传输可结合发射分集来使用。

[0036] 在以下详细描述中，将参照在DL上支持OFDM的MIMO系统来描述接入网的各种方面。OFDM是将数据调制到OFDM码元内的数个副载波上的扩频技术。这些副载波以精确频率分隔开。该分隔提供使得接收机能够从这些副载波恢复数据的“正交性”。在时域中，可向每个OFDM码元添加保护区间(例如，循环前缀)以对抗OFDM码元间干扰。UL可使用经DFT扩展的OFDM信号形式的SC-FDMA来补偿高峰均功率比(PAPR)。

[0037] 图3是解说LTE中的DL帧结构的示例的示图300。帧(10ms)可被划分成10个相等大小的子帧。每个子帧可包括两个连贯的时隙。可使用资源网格来表示2个时隙，每个时隙包括资源块(RB)。该资源网格被划分成多个资源元素。在LTE中，资源块包含频域中的12个连

贯副载波，并且对于每个OFDM码元中的正常循环前缀而言，包含时域中的7个连贯OFDM码元，或即包含84个资源元素。对于扩展循环前缀而言，资源块包含时域中的6个连贯OFDM码元，并具有72个资源元素。指示为R 302、304的一些资源元素包括DL参考信号(DL-RS)。DL-RS包括因蜂窝小区而异的RS(CRS)(有时也称为共用RS)302以及因UE而异的RS(UE-RS)304。UE-RS 304仅在对应的物理DL共享信道(PDSCH)所映射到的资源块上传送。由每个资源元素携带的比特数目取决于调制方案。因此，UE接收的资源块越多且调制方案越高，该UE的数据率就越高。

[0038] 图4是解说LTE中的UL帧结构的示例的示图400。用于UL的可用资源块可分割成数据区段和控制区段。该控制区段可形成在系统带宽的2个边缘处并且可具有可配置大小。该控制区段中的这些资源块可被指派给UE用于控制信息的传输。该数据区段可包括所有不被包括在控制区段中的资源块。该UL帧结构导致该数据区段包括毗连的副载波，这可允许单个UE被指派该数据区段中的所有毗连副载波。

[0039] UE可被指派控制区段中的资源块410a、410b以向eNB传送控制信息。该UE还可被指派数据区段中的资源块420a、420b以向eNB传送数据。该UE可在该控制区段中获指派的资源块上在物理UL控制信道(PUCCH)中传送控制信息。该UE可在该数据区段中获指派的资源块上在物理UL共享信道(PUSCH)中仅传送数据或传送数据和控制信息两者。UL传输可横跨子帧的这两个时隙并且可跨频率跳跃。

[0040] 资源块集合可被用于在物理随机接入信道(PRACH)430中执行初始系统接入并达成UL同步。PRACH 430携带随机序列并且不能携带任何UL数据/信令。每个随机接入前置码占用与6个连贯资源块相对应的带宽。起始频率由网络来指定。即，随机接入前置码的传输被限制于特定的时频资源。对于PRACH不存在跳频。PRACH尝试被携带在单个子帧(1ms)中或在包含数个毗连子帧的序列中，并且UE每帧(10ms)可仅作出单次PRACH尝试。

[0041] 图5是解说LTE中用于用户面和控制面的无线电协议架构的示例的示图500。用于UE和eNB的无线电协议架构被示为具有三层：层1、层2和层3。层1(L1层)是最低层并实现各种物理层信号处理功能。L1层将在本文中被称为物理层506。层2(L2层)508在物理层506之上并且负责UE与eNB之间在物理层506之上的链路。

[0042] 在用户面中，L2层508包括媒体接入控制(MAC)子层510、无线电链路控制(RLC)子层512、以及分组数据汇聚协议(PDCP)514子层，它们在网络侧上终接于eNB。尽管未示出，但是UE在L2层508之上可具有若干个上层，包括在网络侧终接于PDN网关118的网络层(例如，IP层)、以及终接于连接的另一端(例如，远端UE、服务器等)的应用层。

[0043] PDCP子层514提供不同无线电承载与逻辑信道之间的复用。PDCP子层514还提供对上层数据分组的头部压缩以减少无线电传输开销，通过将数据分组暗码化来提供安全性，以及提供对UE在各eNB之间的切换支持。RLC子层512提供对上层数据分组的分段和重装、对丢失数据分组的重传、以及对数据分组的重排序以补偿由于混合自动重复请求(HARQ)造成的脱序接收。MAC子层510提供逻辑信道与传输信道之间的复用。MAC子层510还负责在各UE间分配一个蜂窝小区中的各种无线电资源(例如，资源块)。MAC子层510还负责HARQ操作。

[0044] 在控制面中，用于UE和eNB的无线电协议架构对于物理层506和L2 层508而言基本相同，区别仅在于对控制面而言没有头部压缩功能。控制面还包括层3(L3层)中的无线电资源控制(RRC)子层516。RRC子层516负责获得无线电资源(例如，无线电承载)以及使用eNB与

UE之间的RRC信令来配置各下层。

[0045] 图6是接入网中eNB 610与UE 650处于通信的框图。在DL中，来自核心网的上层分组被提供给控制器/处理器675。控制器/处理器675实现L2层的功能性。在DL中，控制器/处理器675提供头部压缩、暗码化、分组分段和重排序、逻辑信道与传输信道之间的复用、以及基于各种优先级度量对UE 650的无线电资源分配。控制器/处理器675还负责HARQ操作、丢失分组的重传、以及对UE 650的信令。

[0046] 发射(TX)处理器616实现用于L1层(即，物理层)的各种信号处理功能。这些信号处理功能包括编码和交织以促成UE 650处的前向纠错(FEC)以及基于各种调制方案(例如，二进制相移键控(BPSK)、正交相移键控(QPSK)、M相移键控(M-PSK)、M正交振幅调制(M-QAM))向信号星座进行的映射。随后，经编码和调制的码元被拆分成并行流。每个流随后被映射到OFDM副载波、在时域和/或频域中与参考信号(例如，导频)复用、并且随后使用快速傅里叶逆变换(IFFT)组合到一起以产生携带时域OFDM码元流的物理信道。该OFDM流被空间预编码以产生多个空间流。来自信道估计器674的信道估计可被用来确定编码和调制方案以及用于空间处理。该信道估计可以从由UE 650传送的参考信号和/或信道状况反馈推导出来。每个空间流随后可经由分开的发射机618TX被提供给一不同的天线620。每个发射机618TX可用各自的空间流来调制RF载波以供传输。

[0047] 在UE 650处，每个接收机654RX通过其各自的天线652来接收信号。每个接收机654RX恢复出调制到RF载波上的信息并将该信息提供给接收(RX)处理器656。RX处理器656实现L1层的各种信号处理功能。RX处理器656可对该信息执行空间处理以恢复出以UE 650为目的地的任何空间流。如果有多个空间流以该UE 650为目的地，那么它们可由RX处理器656组合成单个OFDM码元流。RX处理器656随后使用快速傅里叶变换(FFT)将该OFDM码元流从时域变换到频域。该频域信号对该OFDM信号的每个副载波包括单独的OFDM码元流。通过确定最有可能由eNB 610传送了的信号星座点来恢复和解调每个副载波上的码元、以及参考信号。这些软判决可以基于由信道估计器658计算出的信道估计。这些软判决随后被解码和解交织以恢复出原始由eNB 610在物理信道上传送的数据和控制信号。这些数据和控制信号随后被提供给控制器/处理器659。

[0048] 控制器/处理器659实现L2层。控制器/处理器可以与存储程序代码和数据的存储器660相关联。存储器660可称为计算机可读介质。在UL中，控制器/处理器659提供传输信道与逻辑信道之间的分用、分组重装、暗码译解、头部解压缩、控制信号处理以恢复出来自核心网的上层分组。这些上层分组随后被提供给数据阱662，后者代表L2层之上的所有协议层。各种控制信号也可被提供给数据阱662以进行L3处理。控制器/处理器659还负责使用确收(ACK)和/或否定确收(NACK)协议进行检错以支持HARQ操作。

[0049] 在UL中，数据源667被用来将上层分组提供给控制器/处理器659。数据源667代表L2层之上的所有协议层。类似于结合由eNB 610进行的DL传输所描述的功能性，控制器/处理器659通过提供头部压缩、暗码化、分组分段和重排序、以及基于由eNB 610进行的无线电资源分配在逻辑信道与传输信道之间进行复用，来实现用户面和控制面的L2层。控制器/处理器659还负责HARQ操作、丢失分组的重传、以及对eNB 610的信令。

[0050] 由信道估计器658从由eNB 610所传送的参考信号或者反馈推导出的信道估计可由TX处理器668用来选择恰适的编码和调制方案以及促成空间处理。由TX处理器668生成的

诸空间流经由分开的发射机654TX提供给不同的天线652。每个发射机654TX可用各自的空间流来调制RF载波以供传输。

[0051] 在eNB 610处以与结合UE 650处的接收机功能所描述的方式相类似的方式来处理UL传输。每个接收机618RX通过其各自的天线620来接收信号。每个接收机618RX恢复出调制到RF载波上的信息并将该信息提供给RX处理器670。RX处理器670可实现L1层。

[0052] 控制器/处理器675实现L2层。控制器/处理器675可以与存储程序代码和数据的存储器676相关联。存储器676可称为计算机可读介质。在UL中，控制/处理器675提供传输信道与逻辑信道之间的分用、分组重组、暗码译解、头部解压缩、控制信号处理以恢复出来自UE 650的上层分组。来自控制器/处理器675的上层分组可被提供给核心网。控制器/处理器675还负责使用ACK和/或NACK协议进行检错以支持HARQ操作。

[0053] 图7A是解说MBSFN中的演进型MBMS(eMBMS)信道配置的示例的示图750。蜂窝小区752'中的eNB 752可以形成第一MBSFN区域并且蜂窝小区754'中的eNB 754可以形成第二MBSFN区域。eNB 752、754可以各自与其他MBSFN区域(例如最多达总共8个MBSFN区域)相关联。MBSFN区域内的蜂窝小区可被指定为保留蜂窝小区。保留蜂窝小区不提供多播/广播内容，但与蜂窝小区752'、754'在时间上同步并且在MBSFN资源上具有受限功率以限制对MBSFN区域的干扰。MBSFN区域中的每一eNB同步地传送相同的eMBMS控制信息和数据。每一区域可以支持广播、多播、以及单播服务。单播服务是旨在给特定用户的服务，例如，语音呼叫。多播服务是可被一群用户接收的服务，例如，订阅视频服务。广播服务是可被所有用户接收的服务，例如，新闻广播。参考图7A，第一MBSFN区域可支持第一eMBMS广播服务，诸如通过向UE 770提供特定新闻广播。第二MBSFN区域可以支持第二eMBMS广播服务，诸如通过向UE 760提供不同的新闻广播。每一MBSFN区域支持多个物理多播信道(PMCH)(例如，15个PMCH)。每一PMCH对应于一多播信道(MCH)。每一MCH可以复用多个(例如，29个)多播逻辑信道。每一MBSFN区域可具有一个多播控制信道(MCCH)。由此，一个MCH可以复用一个MCCH和多个多播话务信道(MTCH)，并且其余MCH可以复用多个MTCH。

[0054] UE可占驻在LTE蜂窝小区上以发现eMBMS服务接入的可用性以及对应接入阶层配置。在第一步骤中，UE可获取系统信息块(SIB)13(SIB13)。在第二步骤中，基于SIB13，UE可获取MCCH上的MBSFN区域配置消息。在第三步骤中，基于该MBSFN区域配置消息，UE可获取MCH调度信息(MSI)MAC控制元素。SIB13指示(1)蜂窝小区所支持的每个MBSFN区域的MBSFN区域标识符；(2)用于获取MCCH的信息，诸如MCCH重复周期(例如，32、64、……、256个帧)、MCCH偏移(例如，0、1、……、10个帧)、MCCH修改周期(例如，512、1024个帧)、信令调制和编码方案(MCS)、指示如由重复周期和偏移所指示的无线电帧的哪些子帧可传送MCCH的子帧分配信息；以及(3)MCCH改变通知配置。对于每个MBSFN区域存在一个MBSFN区域配置消息。MBSFN区域配置消息指示(1)由PMCH内的逻辑信道标识符所标识的每一MTCH的临时移动群身份(TMGI)和可任选的会话标识符，(2)所分配的用于传送MBSFN区域的每一PMCH的资源(即无线电帧和子帧)以及对该区域中的所有PMCH所分配的资源的分配周期(例如，4、8、……、256个帧)，以及(3)在其上传送MSI MAC控制元素的MCH调度周期(MSP)(例如，8、16、32、……、或者1024个无线电帧)。

[0055] 图7B是解说MSI MAC控制元素的格式的示图790。MSI MAC控制元素可每MSP被发送一次。MSI MAC控制元素可在PMCH的每个调度周期的第一子帧中发送。MSI MAC控制元素可

指示PMCH内每个MTCH的停止帧和子帧。每MBSFN区域每PMCH可存在一个MSI。

[0056] UE(即,MBMS接收机)可接收MBMS用户服务发现/宣告。该用户服务发现/宣告包括服务描述信息和接收报告配置。接收报告配置可包括UE可向其发送MBMS接收报告的一个或多个服务器统一资源定位符(URL)。对于MBMS下载递送,接收报告被用于报告对一个或多个文件的完整接收和/或报告关于该下载递送的统计。对于MBMS流送式递送,接收报告被用于报告关于该流送式递送的统计。UE基于报告类型在接收报告中包括信息。报告类型包括接收确收(RAck)、对于成功接收的统计报告(StaR)、对于所有内容接收的统计报告(StaR-all)、以及不带接收确收的统计报告(StaR-only)。当UE标识对内容项的完整接收或会话完成时,该UE确定是否接收报告是否被要求。UE可基于接收报告配置中的收到样本百分比属性来确定是否要发送接收报告。UE选择要用于发送包括接收报告的接收报告请求的时间并且从列表中选择要向哪个服务器发送接收报告请求。UE随机且均匀分布地选择时间和服务器。UE随后通过超文本传输协议(HTTP) 投递操作将接收报告请求发送给服务器。UE随后通过HTTP响应操作从服务器接收一接收报告响应。

[0057] 目前,接收报告和用户服务发现/宣告不受保护。接收报告可能包含与用户或网络有关的敏感信息。例如,接收报告可包括标识UE正接收的内容以及UE正在什么位置接收该内容的信息。又如,接收报告可包括网络拓扑信息(例如,蜂窝小区ID等)以及无线电链路信息(例如,MBSFN参考信号收到功率(RSRP)、参考信号收到质量(RSRQ)、和/或信号对干扰加噪声比(SINR)信息)。此外,用户服务发现/宣告可包括敏感数据字段,和/或可能通过使UE接收致使该UE将接收报告发送给流氓服务器(例如,不与服务提供商相关联的服务器)的欺诈用户服务发现/宣告而经受篡改。以下提供了用于提供安全接收报告和对用户服务发现/宣告的安全接收的方法、计算机程序产品、和装置。

[0058] 图8是解说用于发送安全接收报告的第一示例性方法的示图800。如图8中所示,在步骤810,UE 802可从服务提供商808接收受信任证书权威机构列表。在另一配置中,不执行步骤810,并且在步骤811,UE 802可从广播多播服务中心(BM-SC)806接收受信任证书权威机构列表。受信任证书权威机构列表包括受信任证书权威机构的证书。受信任证书权威机构是UE 802可信任其证书以用于与提供了该证书的服务器建立安全连接的权威机构。受信任证书权威机构列表可基于由UE 802和服务提供商808/BM-SC 806知晓的凭证来加密和/或进行完好性保护。该凭证可存储在UE 802中的智能卡上。该凭证可以是仅为UE 802和服务提供商808/BM-SC 806知晓的共享密钥。此种共享密钥的示例包括基于UE向服务提供商的订阅(例如,在通用集成电路卡(UICC)智能卡上的通用订户身份模块(USIM)应用上)从为服务提供商808/BM-SC 806和UE 802知晓的根密钥(例如Ki,其是用于无线接入认证的根密钥)导出的任何密钥。此种导出密钥的示例包括但不限于,MBMS用户密钥(MUK)、MBMS请求密钥(MRK)、从MUK或MRK导出的密钥、或从共享密钥导出的任何其它密钥。为了对受信任证书权威机构列表进行完好性保护,可使用凭证通过带密钥的散列函数(诸如基于散列的消息认证码(HMAC)(其可以是诸如MUK或MRK 之类的共享密钥的函数))来散列受信任证书权威机构列表以获得散列值(也称为散列码、散列和、校验码、或散列),并且该散列值可与受信任证书权威机构列表一起被包括,从而UE 802可检查受信任证书权威机构列表内的字段自完好性保护以来是否已被修改。

[0059] 在步骤812,UE 802可从BM-SC 806接收用户服务发现/宣告。用户服务发现/宣告

可包括一个或多个接收报告配置以及UE可向其发送接收报告的一个或多个服务器地址。在一个示例中，用户服务发现/宣告包括用于发送不安全接收报告的第一接收报告配置和无安全保证服务器URL、以及用于发送安全接收报告的第二接收报告配置和有安全保证服务器URL。无安全保证服务器URL可以是用于通过HTTP发送接收报告的URL。有安全保证服务器URL可以是用于通过安全HTTP(HTTPS)(例如，带有传输层安全性(TLS)协议的HTTP)发送接收报告的URL。用户服务发现/宣告可自身是基于由UE 802和BM-SC 806知晓的凭证来进行完好性保护和/或加密的。该凭证可存储在UE 802中的智能卡上。凭证可以是被获得授权来接收用户服务发现/宣告的UE集知晓的群共享密钥(诸如MBMS服务密钥(MSK))，或是从MSK导出的密钥。替换地，群共享密钥可被预先配置在UE上(例如，使用任何配置机制，诸如越空(OTA)配置或开放移动联盟设备管理(OMA-DM)配置协议)。

[0060] 在步骤814，UE 802确定是否要发送接收报告以及敏感接收报告信息是否可被包括在该接收报告中。步骤814可发生在UE 802标识出对MBMS内容项的完整接收或MBMS会话的完成之后。在步骤816，UE 802选择报告时间和服务器。如果UE 802确定敏感接收报告信息将不被包括在接收报告中，则UE 802可选择通过无安全保证连接将接收报告发送至无安全保证服务器URL。如果UE 802确定敏感接收报告信息将被包括在接收报告中，则UE 802可选择通过有安全保证连接将接收报告发送至有安全保证服务器URL。

[0061] 假定UE 802选择通过有安全保证连接将接收报告发送至服务器804，则在步骤818，UE 802发起HTTPS的建立。在步骤818，UE 802接收服务器804的证书。该证书可以是X.509服务器证书。如果UE 802尚未接收到受信任证书权威机构列表(步骤810或步骤811尚未发生)，则在步骤820，UE 802从服务提供商808获得受信任证书权威机构列表，或者在步骤821，UE 802从BM-SC 806获得受信任证书权威机构列表。在步骤822，UE 802验证该证书属于由有安全保证服务器URL标识的服务器(例如，通过验证X.509服务器证书中的subjectAltName(主体别名)与用户服务发现/宣告中的服务器地址相同)并且通过检查收到的证书是否是基于包括在受信任证书权威机构列表中的根证书所发出的来认证使用该证书的服务器。服务器认证向UE 802提供了安全服务器地址未曾被篡改并且UE正与之连接的服务器真实可信的保证。在步骤824，如果UE 802能够认证服务器804，则UE 802确定要完成与服务器804的安全连接的建立。UE 802随后通过HTTPS完成与服务器804的安全连接的建立。在步骤826，UE 802基于相应的接收报告配置通过HTTPS连接发送接收报告。

[0062] 步骤818被示为发生在步骤816之后。然而，步骤818可发生在步骤814之前。在步骤810、820，UE从服务提供商808接收受信任证书权威机构列表。然而，在步骤811、821，可作为UE eMBMS服务注册规程的一部分或者通过UE与服务提供商之间的另一单播机制来从BM-SC接收受信任证书权威机构列表。为了作为UE eMBMS服务注册规程的一部分获得受信任证书权威机构列表，UE可将HTTP投递消息发送给BM-SC 806。该消息可包括注册指示、MBMS用户服务ID、以及对证书权威机构列表的请求。BM-SC 806可作出响应并发送证书权威机构列表。BM-SC 806可基于MRK、MUK、或从MRK或MUK之一导出的密钥来对证书权威机构列表进行完好性保护和/或加密。在另一配置中，受信任证书权威机构列表可以预先配置在UE 802上。例如，该预先配置可以是eMBMS OTA配置或设备管理的一部分或者可由原始设备制造商(OEM)代表服务提供商808来完成。

[0063] 图9是解说用于发送安全接收报告的第二示例性方法的示图900。在步骤908，服务

器904从BM-SC 906接收MUK或MRK或从MUK或MRK导出的密钥。在步骤910，UE 902接收用户服务发现/宣告。用户服务发现/宣告可基于MSK或类似群密钥来进行完好性保护和/或加密。在步骤912，UE 902确定是否要发送接收报告以及接收报告是否将包括敏感信息。在步骤914，UE 902选择用于发送接收报告的报告时间。在步骤916，UE基于MUK或MRK或其导出密钥来对接收报告进行完好性保护和/或加密。在步骤918，UE将受保护的接收报告发送给服务器904。应注意，要保护用户服务发现/宣告的决定是独立于要保护接收报告的决定的。

[0064] UE 902可通过以散列函数散列接收报告或接收报告中的一个或多个字段以获得散列值来对接收报告进行完好性保护。散列函数可自身是MUK或MRK或其导出密钥的函数。UE 902可将散列值连同接收报告发送给服务器904。替换地或附加地，UE 902可通过基于MUK或MRK(例如，使用MUK或MRK或从MUK或MRK导出的密钥)加密整个接收报告或接收报告中的一个或多个字段来加密接收报告。

[0065] 图10是解说用于接收和处理安全用户服务发现/宣告的示例性方法的示图1000。在步骤1008，BM-SC 1006对用户服务发现/宣告进行完好性保护和/或加密。BM-SC 1006可对完整的用户服务发现/宣告或者用户服务发现/宣告的一个或多个字段进行完好性保护和/或加密。例如，BM-SC 1006可仅对用户服务发现/宣告内的接收报告配置或仅对服务器URL字段进行完好性保护和/或加密。BM-SC 1006可通过以散列函数散列用户服务发现/宣告或用户服务发现/宣告中的一个或多个字段以获得散列值来对用户服务发现/宣告进行完好性保护。散列函数可自身是为UE群和服务提供商知晓的MSK或类似群密钥的函数。BM-SC 1006可将该散列值连同用户服务发现/宣告发送给UE 1002。替换地或附加地，BM-SC 1006可通过基于MSK(例如，使用MSK或从MSK导出的密钥)加密整个用户服务发现/宣告或该用户服务发现/宣告中的一个或多个字段来加密用户服务发现/宣告。如果BM-SC 1006决定仅保护用户服务发现/宣告中的一个或多个字段，则BM-SC 1006可通过在用户服务发现/宣告中发送的字段类型来向UE 1002指示该决定。字段类型也可以是受完好性保护的。UE可通过OTA配置或设备管理规程被预先配置有将受保护的字段，或者UE可事先被编程以知晓哪些字段将受保护。

[0066] 在步骤1010，BM-SC 1006可将用户服务发现/宣告发送给UE 1002。在步骤1012，如果用户服务发现/宣告是受完好性保护的，则UE 1002基于MSK来验证用户服务发现/宣告的完好性。另外，如果用户服务发现/宣告是经加密的，则UE 1002基于MSK来解密用户服务发现/宣告。在步骤1014，UE 1002确定是否要发送接收报告以及接收报告是否可包含敏感信息。在步骤1016，UE 1002选择用于发送接收报告的时间。在步骤1018，UE 1002将接收报告发送给服务器1004。在一种配置中，UE 1002通过安全连接(例如，HTTPS)将接收报告发送给服务器1004。在另一配置中，UE 1002在将接收报告发送给服务器1004之前对接收报告进行完好性保护和/或加密。

[0067] 图11是第一无线通信方法的流程图1100。该方法可由UE来执行。在步骤1102，UE从服务提供商接收证书权威机构列表。该证书权威机构列表包括受信任证书权威机构的证书。证书权威机构列表是基于由UE和服务提供商知晓的凭证来进行完好性保护和/或加密的。该凭证可存储在UE中的智能卡上。该凭证可基于为UE和服务提供商知晓的任何共享密钥，诸如MUK或MRK或从MUK或MRK导出的密钥。在步骤1104，UE接收包括接收报告配置和服务器地址的用户服务发现/宣告。整个用户服务发现/宣告或该用户服务发现/宣告内的一个

或多个字段可以是基于由UE和BM-SC知晓的凭证来进行完好性保护和/或加密的。该凭证可存储在UE中的智能卡上。该凭证可以是共享密钥，诸如MSK或从MSK导出的密钥。在步骤1104之后，如果UE标识出对内容项的完整接收或会话的完成并确定接收报告是被要求的，则在步骤1106，UE确定该接收报告是否包括敏感接收报告信息。步骤1106中的确定可基于接收报告的报告类型RAck、StaR、StaR-all、或StaR-only或者基于其它信息。

[0068] 如果接收报告不包括敏感信息，则在步骤1108，UE基于收到的服务器地址和接收报告配置通过无安全保证连接将接收报告发送给服务器。

[0069] 如果接收报告包括敏感信息，则在步骤1110，UE发起安全连接建立(例如，HTTPS)并接收服务器的证书。在步骤1112，UE使用收到的证书权威机构列表以及该证书来认证服务器。UE可通过验证该证书属于与收到的服务器URL相同的服务器地址并通过将该证书与证书权威机构列表作比较以验证收到的证书是基于收到的证书权威机构列表中的根证书所发出的来认证服务器。在步骤1114，UE在认证了服务器之际确定要建立与服务器的安全连接，并建立与服务器的安全连接。在步骤1116中，UE基于收到的服务器地址和接收报告配置通过安全连接将接收报告发送给服务器。

[0070] 图12是第二无线通信方法的流程图1200。该方法可由UE来执行。在步骤1202，UE接收包括接收报告配置和服务器地址的用户服务发现/宣告。整个用户服务发现/宣告或用户服务发现/宣告的一部分可以是受完好性保护和/或加密的。在步骤1202之后，如果UE标识出对内容项的完整接收或会话的完成并确定接收报告是被要求的，则在步骤1204，UE确定该接收报告是否包括敏感接收报告信息。步骤1204中的确定可基于接收报告的报告类型RAck、StaR、StaR-all、或StaR-only或者基于其它信息。如果接收报告不包括敏感信息，则在步骤1208，UE基于收到的服务器地址和接收报告配置将不受保护的接收报告发送给服务器。如果接收报告包括敏感信息，则在步骤1206，UE通过对接收报告进行完好性保护和/或加密、和/或建立用于发送接收报告的安全连接来保护接收报告。在步骤1210，UE基于接收报告配置将受保护的接收报告发送给服务器。

[0071] 图13是第三无线通信方法的流程图1300。该方法可由UE来执行。在步骤1302，UE接收受保护的广播宣告。该广播宣告是受完好性保护和/或加密的。广播宣告可以是基于UE和BM-SC知晓的凭证而进行完好性保护和/或加密的。该凭证可存储在UE中的智能卡上。当广播宣告受完好性保护时，该凭证可包括校验和或散列和。该凭证可存储在UE中的智能卡上。该凭证可以是共享密钥，诸如MSK或从MSK导出的密钥。在步骤1304，当广播宣告是经加密的时，UE基于凭证/共享密钥/MSK来解密广播宣告，和/或当广播宣告是受完好性保护的时，UE基于凭证/共享密钥/MSK来验证广播宣告的完好性。UE通过重新计算校验和/散列和并将重新计算出的校验和/散列和与凭证中提供的校验和/散列和作比较来验证广播宣告的完好性。当重新计算出的校验和/散列和与凭证中的校验和/散列和匹配时，完好性检查通过。否则，完好性检查失败。在步骤1306，UE确定广播宣告是否被成功解密和/或完好性检查是否通过。如果UE能够解密广播宣告和/ 或验证广播宣告的完好性，则在步骤1308，UE可基于该广播宣告来通信(例如，发送接收报告)。

[0072] 图14是解说示例性设备1402中的不同模块/装置/组件之间的数据流的概念性数据流图1400。该设备可以是UE。该设备包括通信模块1404，其可被配置成经由eNB 1450从服务提供商接收证书权威机构列表。该证书权威机构列表可包括受信任证书权威机构的证

书。证书权威机构列表可以是基于由UE和服务提供商知晓的凭证来进行完好性保护和/或加密的。该凭证可存储在UE中的智能卡上。该凭证可以是共享密钥。该共享密钥可以是为UE和服务提供商知晓的任何共享密钥，诸如MUK或MRK或从MUK或MRK导出的密钥。通信模块1404可被配置成向服务器认证模块1410提供证书权威机构列表。服务器认证模块1410可被配置成通过加密/解密模块1408来解密证书权威机构列表并且可被配置成通过完好性保护模块1412来验证该证书权威机构列表的完好性。加密/解密模块1408可被配置成基于为UE和服务器知晓的凭证(诸如共享密钥(例如，MUK/MRK或从MUK/MRK导出的密钥))来解密证书权威机构列表。该凭证可存储在UE中的智能卡上。完好性保护模块1412可被配置成基于为UE和服务器知晓的凭证(诸如共享密钥(例如，MUK/MRK或从MUK/MRK导出的密钥))来验证该证书权威机构列表的完好性。该凭证可存储在UE中的智能卡上。

[0073] 通信模块1404可被配置成接收包括接收报告配置和服务器地址的用户服务发现/宣告。用户服务发现/宣告可以是基于由UE和BM-SC知晓的凭证来进行完好性保护和/或加密的。该凭证可存储在UE中的智能卡上。该凭证可以是共享密钥。该共享密钥可以是MSK或从MSK导出的密钥。通信模块1404可被配置成将收到的用户服务发现/宣告提供给接收报告处理模块1406。接收报告处理模块1406可被配置成通过加密/解密模块1408来解密用户服务发现/宣告，并且可被配置成通过完好性保护模块1412来验证用户服务发现/宣告的完好性。加密/解密模块1408可被配置成基于为UE和BM-SC知晓的凭证(诸如共享密钥(例如，MSK或从MSK导出的密钥))来解密用户服务发现/宣告。该凭证可存储在UE中的智能卡上。完好性保护模块1412可被配置成基于为UE和BM-SC知晓的凭证(诸如共享密钥(例如，MSK或从MSK导出的密钥))来验证用户服务发现/宣告的完好性。该凭证可存储在UE中的智能卡上。

[0074] 通信模块1404可被配置成在发起与服务器的安全连接之际接收该服务器的证书。通信模块1404可被配置成向服务器认证模块1410提供该证书。服务器认证模块1410可被配置成使用收到的证书权威机构列表和收到的证书来认证服务器。服务器认证模块1410可被配置成在认证服务器之际确定要建立与服务器的安全连接(例如，HTTPS)。服务器认证模块1410可被配置成与通信模块1404通信，从而通信模块1404建立与服务器的安全连接。当存在对内容项的完整接收或会话的完成时，通信模块1404可与接收报告处理模块1406通信。接收报告处理模块1406可确定接收报告是否被要求，并且如果接收报告是被要求的，则生成接收报告。接收报告处理模块1406可被配置成通过加密/解密模块1408来加密接收报告。加密/解密模块1408可被配置成基于为UE和服务器知晓的凭证(诸如共享密钥(例如，MUK/MRK或从MUK/MRK导出的密钥))来加密接收报告。该凭证可存储在UE中的智能卡上。接收报告处理模块1406可被配置成通过完好性保护模块1412来对接收报告进行完好性保护。完好性保护模块1412可被配置成基于为UE和服务器知晓的凭证(诸如共享密钥(例如，MUK/MRK或从MUK/MRK导出的密钥))来对接收报告进行完好性保护。该凭证可存储在UE中的智能卡上。接收报告处理模块1406可以将所生成的接收报告提供给通信模块1404，通信模块1404可被配置成将接收报告发送给服务器。如果通信模块1404已经与服务器建立了安全连接，则通信模块1404可被配置成通过该安全连接将接收报告发送给服务器。

[0075] 该设备可包括执行前述图8-图 10的示图和图11-图 13的流程图中的算法的每个步骤的附加模块。如此，前述图8-图 10的示图和图11-图 13流程图中的每个步骤可由一模块来执行且该设备可包括这些模块中的一个或多个模块。各模块可以是专门配置成实施所

述过程/算法的一个或多个硬件组件、由配置成执行所述过程/算法的处理器实现的、存储在计算机可读介质中以供由处理器实现的、或其某个组合。

[0076] 图15是解说采用处理系统1514的设备1402'的硬件实现的示例的示图。处理系统1514可实现成具有由总线1524一般化地表示的总线架构。取决于处理系统1514的具体应用和整体设计约束，总线1524可包括任何数目的互连总线和桥接器。总线1524将包括一个或多个处理器和/或硬件模块(由处理器1504、模块1404、1406、1408、1410、1412和计算机可读介质1506表示)的各种电路链接在一起。总线1524还可链接各种其它电路，诸如定时源、外围设备、稳压器和功率管理电路，这些电路在本领域中是众所周知的，且因此将不再进一步描述。

[0077] 处理系统1514可耦合至收发机1510。收发机1510被耦合至一个或多个天线1520。收发机1510提供用于通过传输介质与各种其它装置通信的手段。处理系统1514包括耦合至计算机可读介质1506的处理器1504。处理器1504负责一般性处理，包括执行存储在计算机可读介质1506上的软件。该软件在由处理器1504执行时使处理系统1514执行上文针对任何特定装置描述的各种功能。计算机可读介质1506还可被用于存储由处理器1504在执行软件时操纵的数据。处理系统进一步包括模块1404、1406、1408、1410和1412中的至少一个模块。各模块可以是在处理器1504中运行的软件模块、驻留/存储在计算机可读介质1506中的软件模块、耦合至处理器1504的一个或多个硬件模块、或其某种组合。处理系统1514可以是UE 650的组件且可包括存储器660和/或TX处理器668、RX处理器656、和控制器/处理器659中的至少一者。

[0078] 在一种配置中，用于无线通信的设备1402/1402'包括用于从服务提供商接收证书权威机构列表的装置。证书权威机构列表是基于由该设备和服务提供商知晓的凭证来进行完好性保护或加密中的至少一者的。该凭证可存储在该设备中的智能卡上。该设备进一步包括用于使用收到的证书权威机构列表来认证服务器的装置。该设备可进一步包括用于接收服务器的证书的装置、以及用于在认证服务器之际确定要建立与服务器的安全连接的装置。该设备可进一步包括用于接收包括接收报告配置和服务器地址的用户服务发现/宣告的装置、用于建立与服务器的安全连接的装置、以及用于基于该地址和接收报告配置通过安全连接将接收报告发送给服务器的装置。

[0079] 前述装置可以是设备1402的前述模块和/或设备1402'中配置成执行由前述装置叙述的功能的处理系统1514中的一者或多者。如上所述，处理系统1514可包括TX处理器668、RX处理器656、以及控制器/处理器659。如此，在一种配置中，前述装置可以是配置成执行由前述装置所述的功能的TX处理器668、RX处理器656、以及控制器/处理器659。

[0080] 在一种配置中，用于无线通信的设备1402/1402'包括用于接收包括接收报告配置和服务器地址的用户服务发现/宣告的装置、以及用于基于接收报告配置将受保护的接收报告发送给服务器的装置。该设备可进一步包括用于建立与服务器的安全连接的装置。该设备可进一步包括用于从服务提供商接收证书权威机构列表的装置、用于接收服务器的证书的装置、以及用于使用收到的证书权威机构列表和证书来认证服务器的装置。该设备可进一步包括用于对接收报告进行完好性保护和/或加密的装置。

[0081] 前述装置可以是设备1402的前述模块和/或设备1402'中配置成执行由前述装置叙述的功能的处理系统1514中的一者或多者。如上所述，处理系统1514可包括TX处理器

668、RX处理器656、以及控制器/处理器659。如此，在一种配置中，前述装置可以是配置成执行由前述装置所述的功能的TX处理器668、RX处理器656、以及控制器/处理器659。

[0082] 在一种配置中，用于无线通信的设备1402/1402'包括用于接收受保护的广播宣告的装置。该广播宣告是基于由该设备知晓并存储在该设备中的智能卡上的凭证来进行完好性保护或加密中的至少一者的。该设备进一步包括用于基于广播宣告来通信的装置。该设备可进一步包括用于在广播宣告是经加密的时基于MSK来解密广播宣告的装置。该设备可进一步包括用于在广播宣告是受完好性保护的时基于MSK来验证广播宣告的完好性的装置。

[0083] 前述装置可以是设备1402的前述模块和/或设备1402'中配置成执行由前述装置叙述的功能的处理系统1514中的一者或多者。如上所述，处理系统1514可包括TX处理器668、RX处理器656、以及控制器/处理器659。如此，在一种配置中，前述装置可以是配置成执行由前述装置所述的功能的TX处理器668、RX处理器656、以及控制器/处理器659。

[0084] 应理解，所公开的过程中各步骤的具体次序或层次是示例性办法的解说。应理解，基于设计偏好，可以重新编排这些过程中各步骤的具体次序或层次。此外，一些步骤可被组合或被略去。所附方法权利要求以样本次序呈现各种步骤的要素，且并不意味着被限定于所呈现的具体次序或层次。

[0085] 提供之前的描述是为了使本领域任何技术人员均能够实践本文中所描述的各种方面。对这些方面的各种改动将容易为本领域技术人员所明白，并且在本文中所定义的普适原理可被应用于其他方面。因此，权利要求并非旨在被限定于本文中所示出的方面，而是应被授予与语言上的权利要求相一致的全部范围，其中对要素的单数形式的引述除非特别声明，否则并非旨在表示“有且仅有一个”，而是“一个或多个”。除非特别另外声明，否则术语“一些/某个”指的是一个或多个。诸如“A、B或C中的至少一者”、“A、B和C中的至少一者”以及“A、B、C或其任何组合”之类的组合包括A、B和/或C的任何组合，并且可包括多个A、多个B或者多个C。具体地，诸如“A、B或C中的至少一者”、“A、B和C中的至少一者”以及“A、B、C或其任何组合”之类的组合可以是仅A、仅B、仅C、A和B、A和C、B和C、或者A和B和C，其中任何此类组合可包含A、B或C中的一个或多个成员。本公开通篇描述的各种方面的要素为本领域普通技术人员当前或今后所知的所有结构上和功能上的等效方案通过引用被明确纳入于此，且旨在被权利要求所涵盖。此外，本文中所公开的任何内容都并非旨在贡献给公众，无论这样的公开是否在权利要求书中被显式地叙述。没有任何权利要求元素应被解释为装置加功能，除非该元素使用短语“用于……的装置”来明确叙述的。

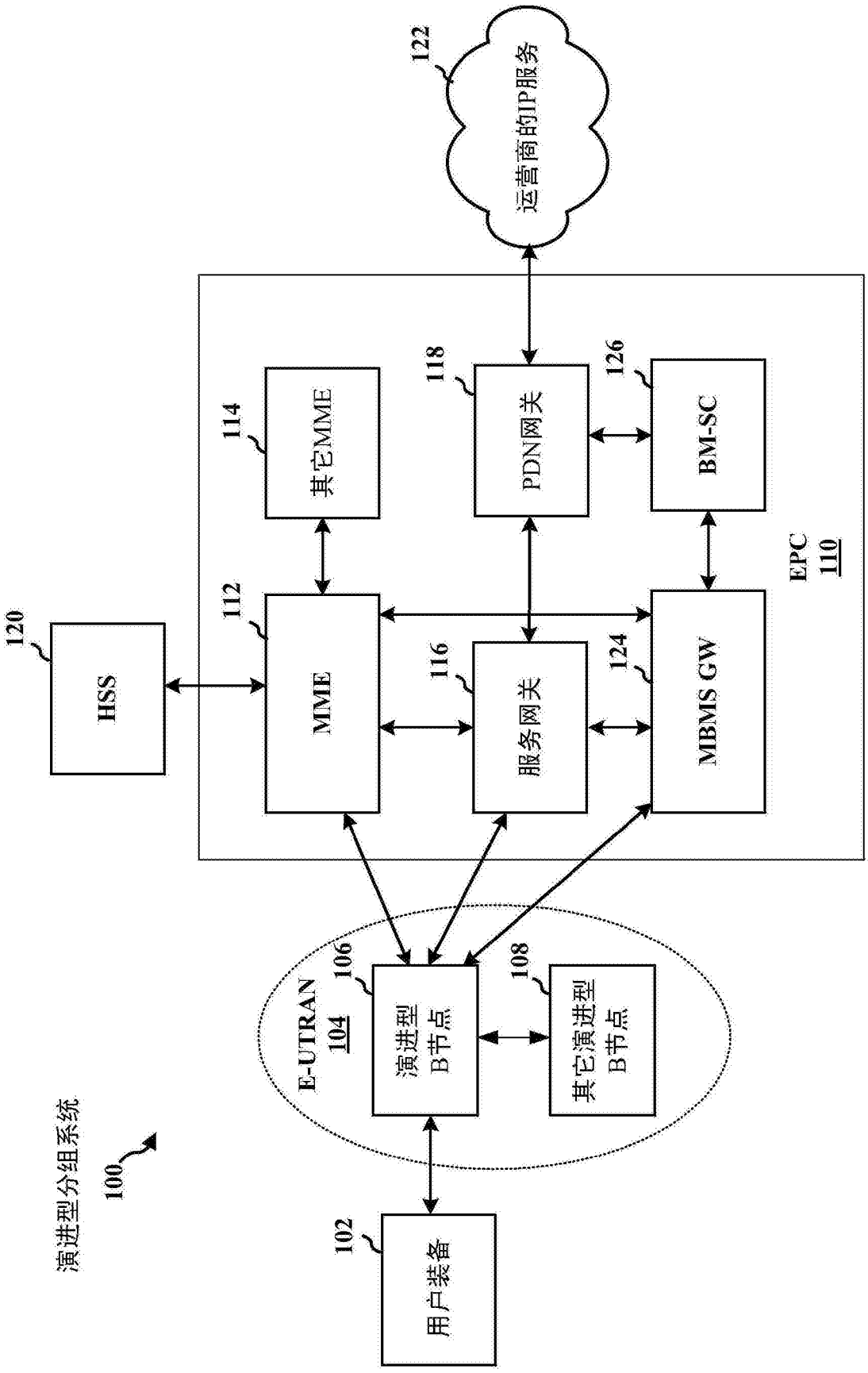

演进型分组系统
100
用户装备
102
E-UTRAN
104
演进型
B节点
106
其它演进型
B节点
108
HSS
120
MME
112
服务网关
116
MBMS GW
124
EPC
110
其它MME
114
PDN网关
118
BM-SC
126
运营商的IP服务
122

图1

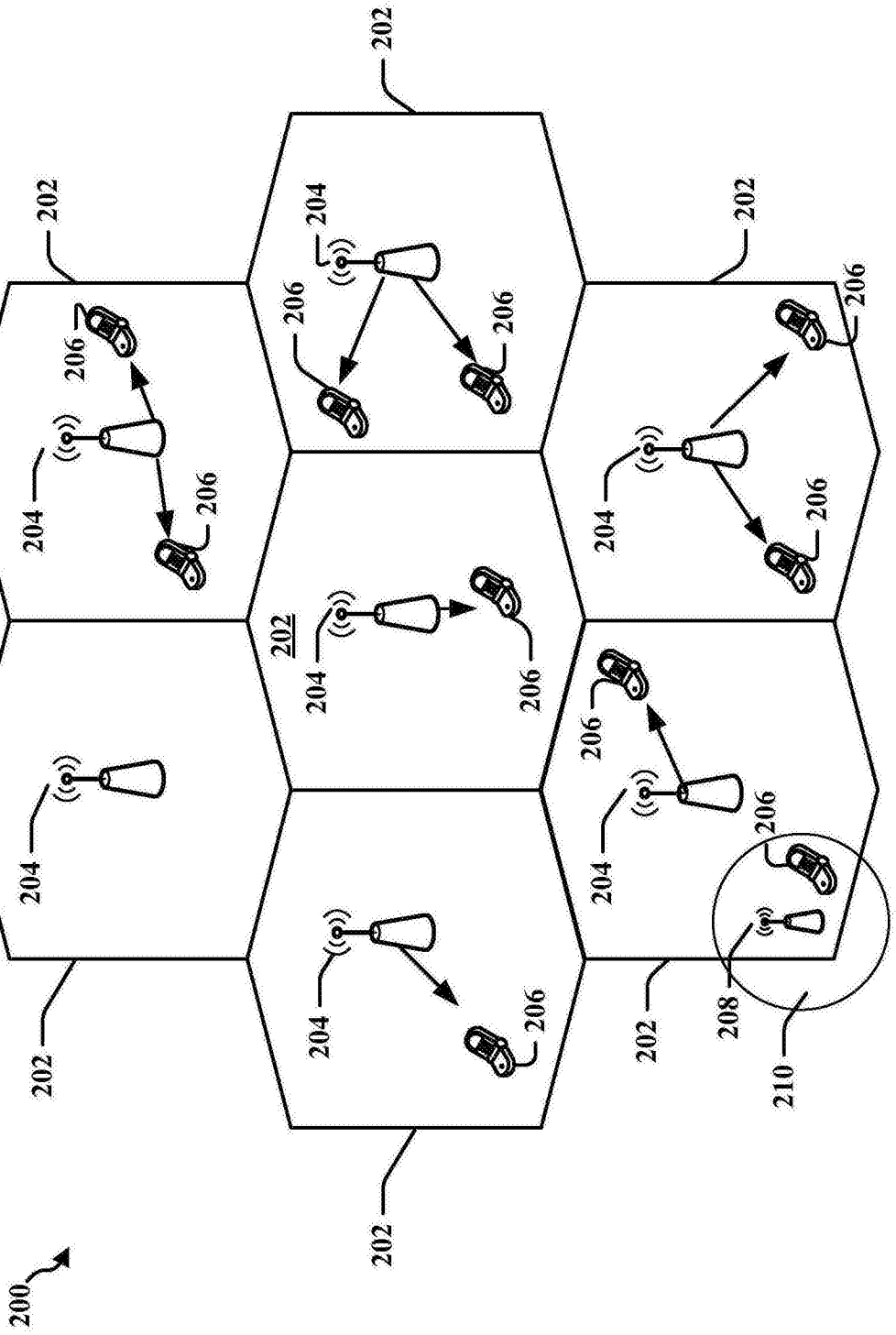


图2

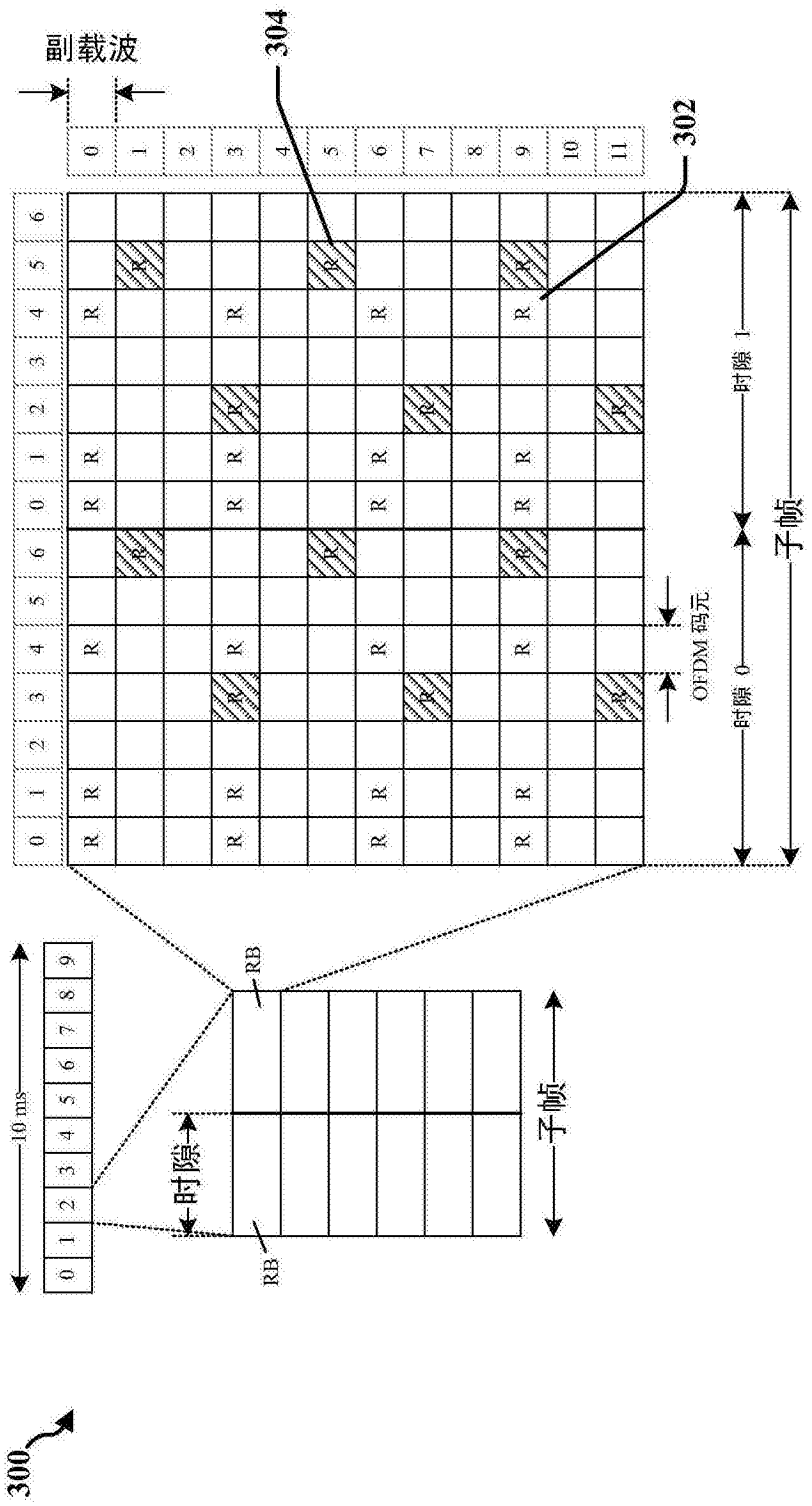

副载波
304
302
0 1 2 3 4 5 6 7 8 9 10 11
R
时隙 1
时隙 0
子帧
OFDM 码元
RB
10 ms
时隙
子帧
300

图3

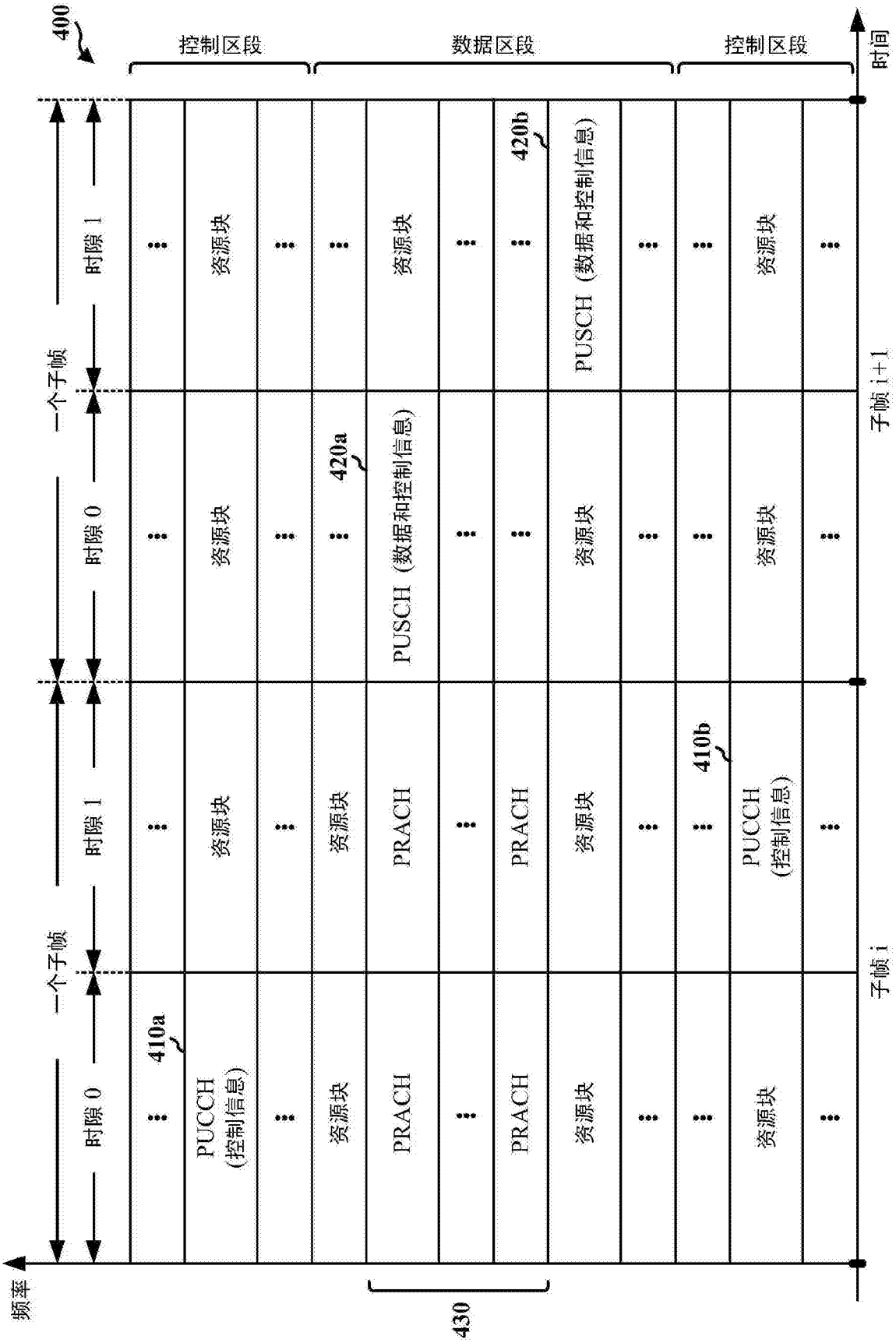

400
控制区段
数据区段
控制区段
时间
一个子帧
时隙 0
时隙 1
一个子帧
时隙 0
时隙 1
频率
410a
PUCCH
(控制信息)
资源块
PRACH
420a
PUSCH (数据和控制信息)
420b
410b
PUCCH
(控制信息)
430
子帧 i
子帧 i+1

图4

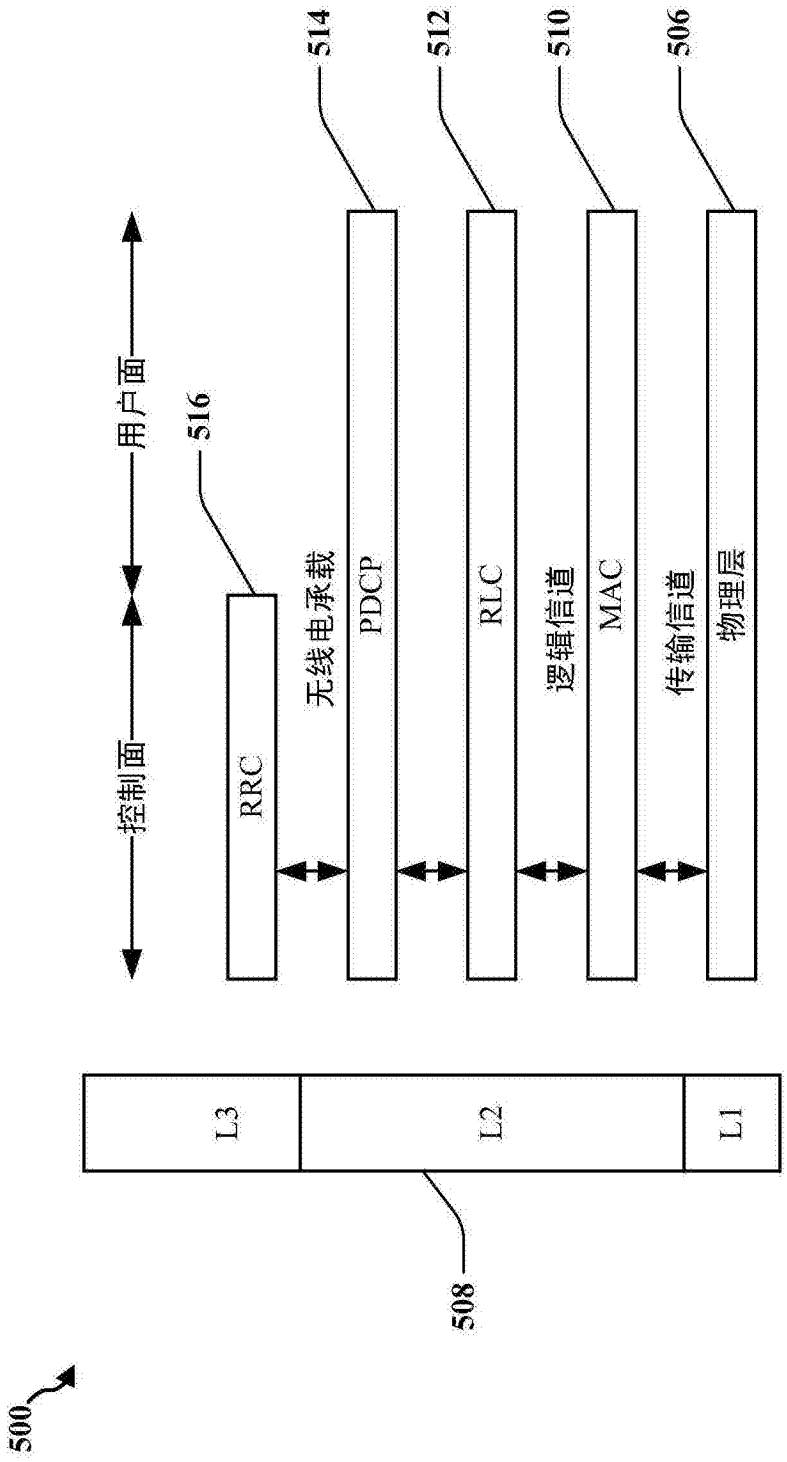

514
512
510
506
用户面
控制面
516
RRC
无线电承载
PDCP
RLC
逻辑信道
MAC
传输信道
物理层
L3
L2
L1
508
500

图5

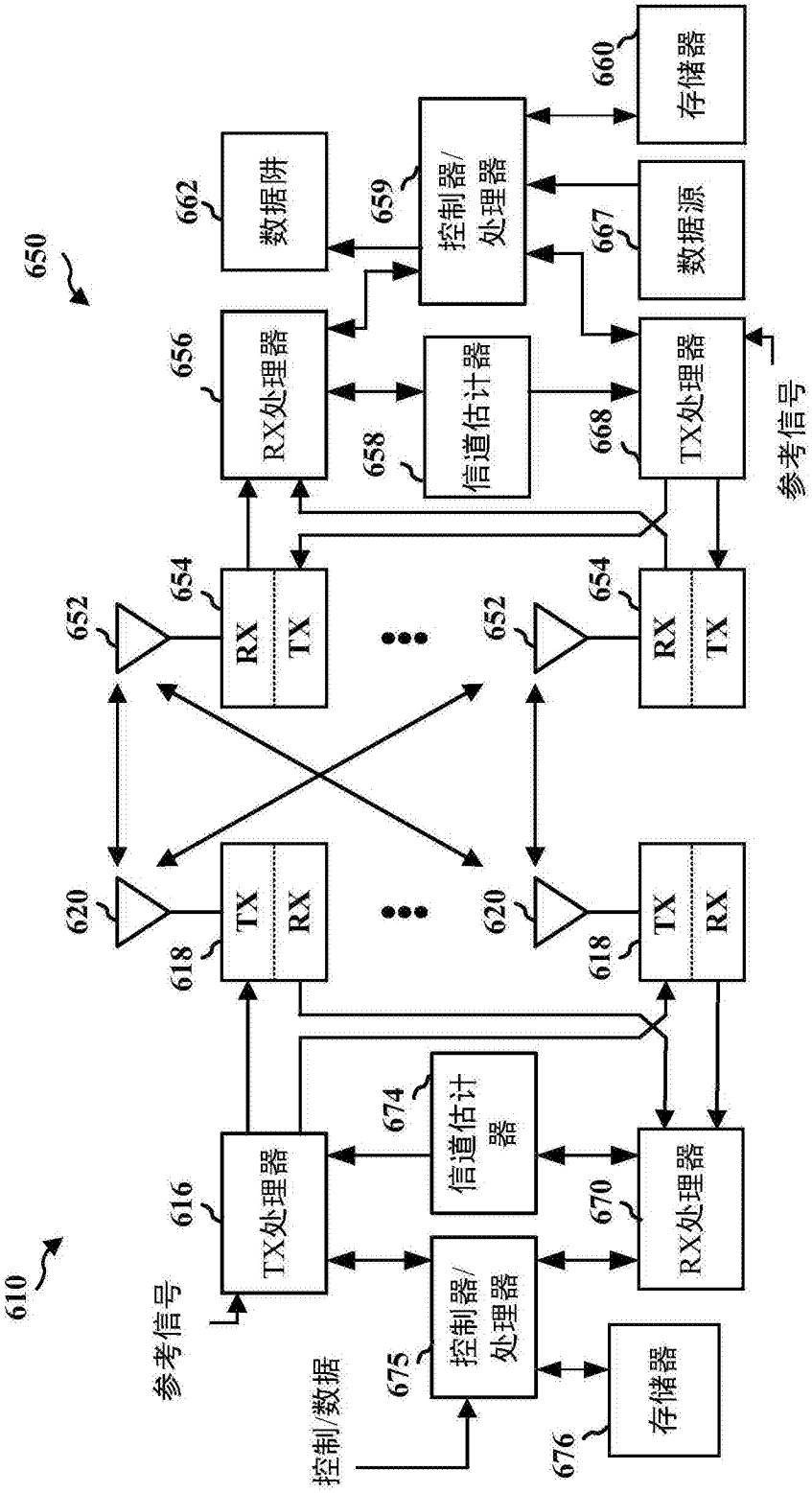

650
662
数据阱
659
控制器/处理器
660
存储器
667
数据源
656
RX处理器
658
信道估计器
668
TX处理器
参考信号
654
652
RX
TX
620
618
610
616
TX处理器
674
信道估计器
670
RX处理器
参考信号
控制/数据
675
控制器/处理器
676
存储器

图6

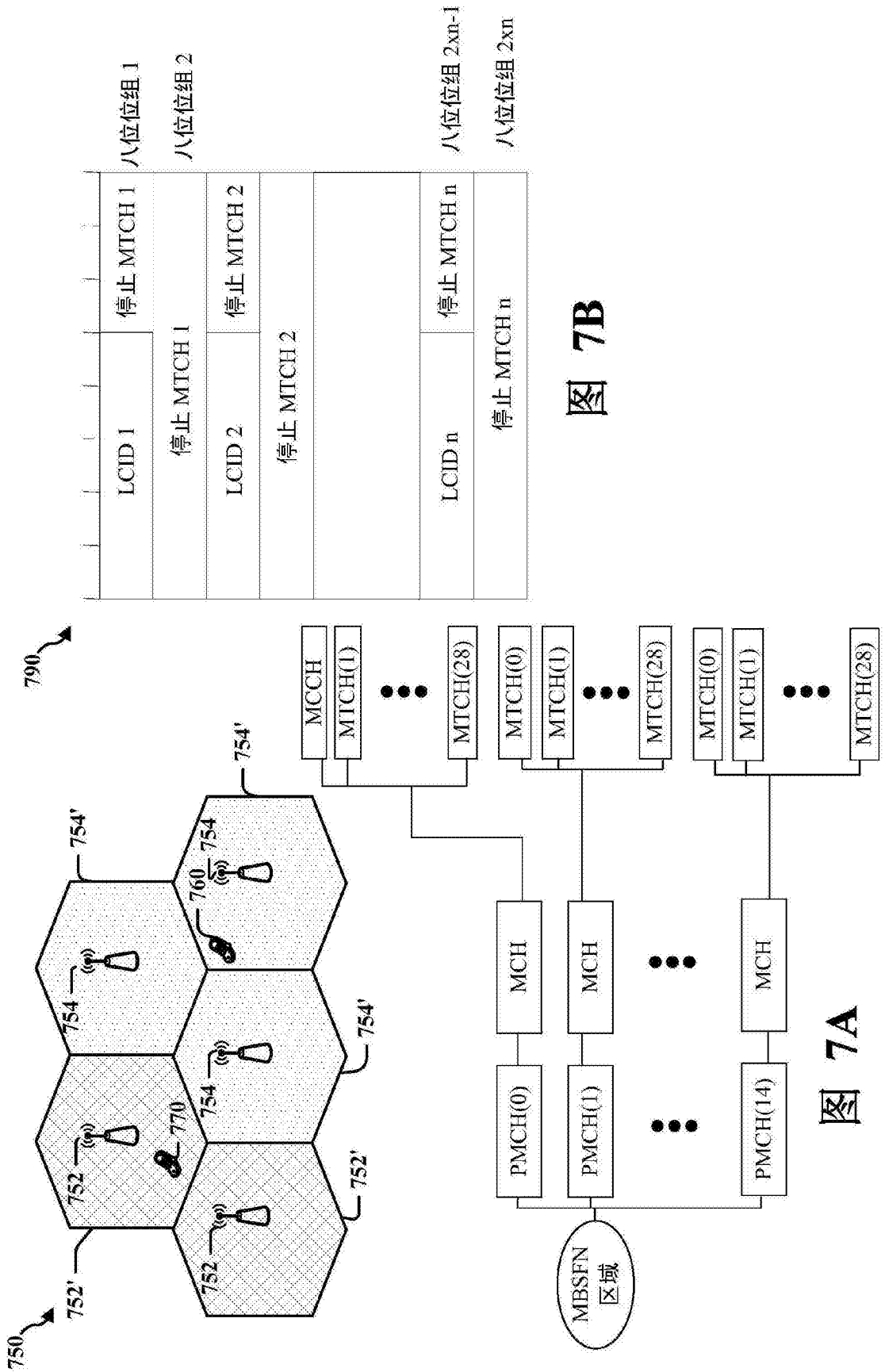


图 7A

LCID 1	停止 MTCH 1	八位位组 1
停止 MTCH 1		八位位组 2
LCID 2	停止 MTCH 2	
停止 MTCH 2		
LCID n	停止 MTCH n	八位位组 2xn-1
停止 MTCH n		八位位组 2xn

图 7B

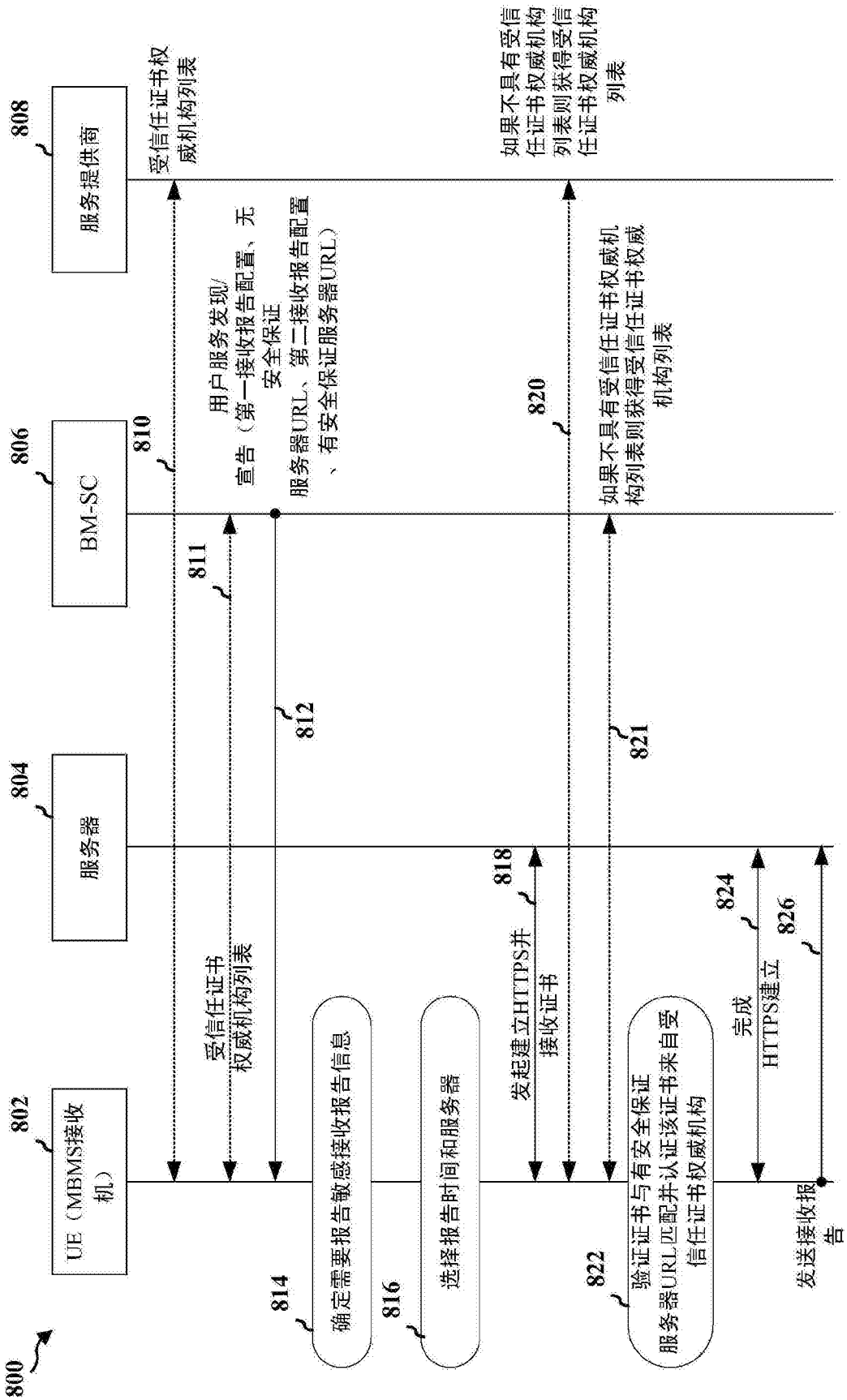

800
802
UE（MBMS接收机）
804
服务器
806
BM-SC
808
服务提供商
810
811
812
814
816
818
820
821
822
824
826
受信任证书权威机构列表
用户服务发现/宣告（第一接收报告配置、无安全保证
服务器URL、第二接收报告配置、有安全保证服务器URL）
如果不具有受信任证书权威机构列表则获得受信任证书权威机构列表
受信任证书权威机构列表
如果不具有受信任证书权威机构列表则获得受信任证书权威机构列表
确定需要报告敏感接收报告信息
选择报告时间和服务器
发起建立HTTPS并接收证书
验证证书与有安全保证服务器URL匹配并认证该证书来自受信任证书权威机构
完成HTTPS建立
发送接收报告

图8

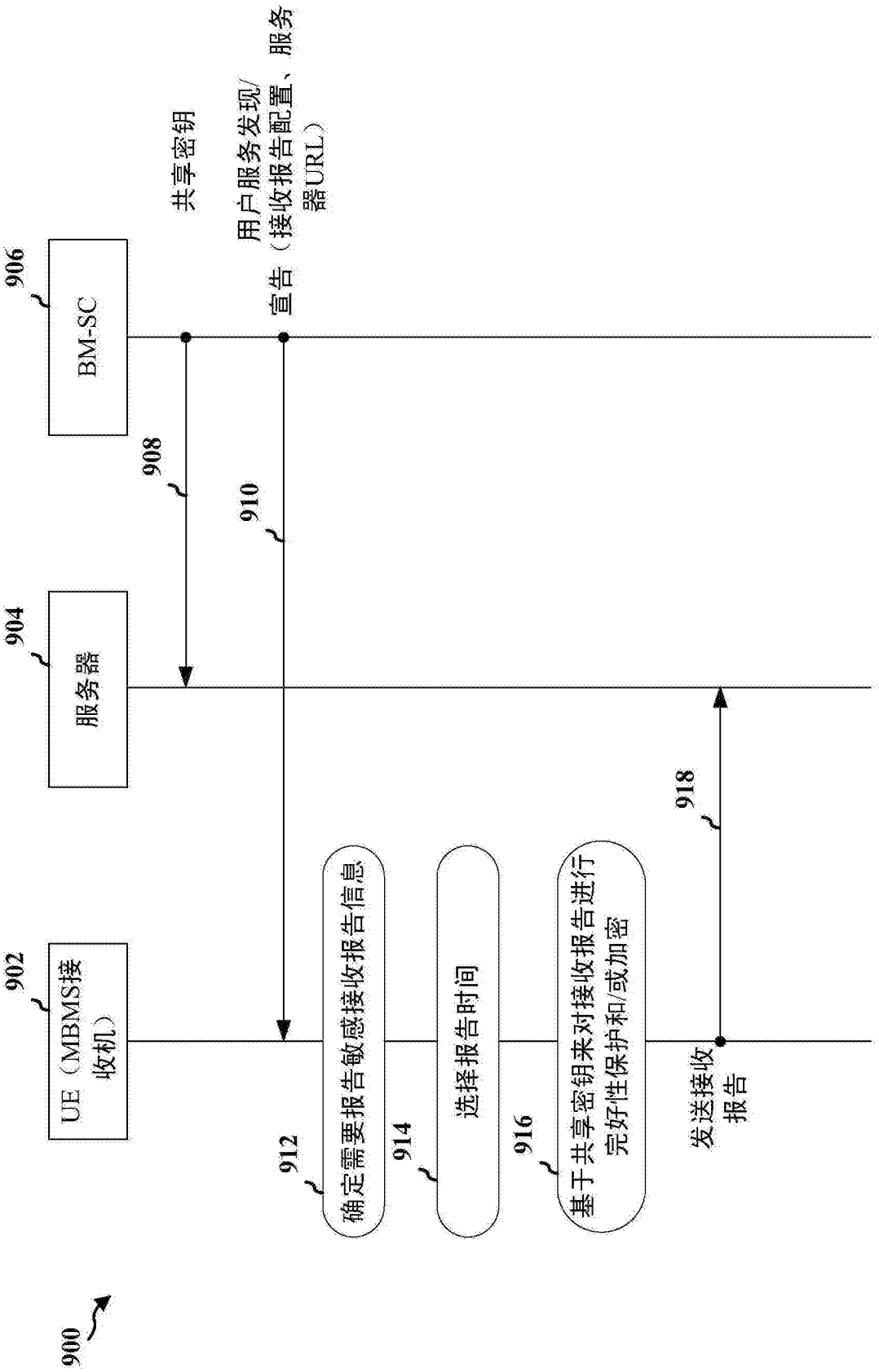

900
UE（MBMS接收机）
902
服务器
904
BM-SC
906
共享密钥
用户服务发现/宣告（接收报告配置、服务器URL）
908
910
确定需要报告敏感接收报告信息
912
选择报告时间
914
基于共享密钥来对接收报告进行完好性保护和/或加密
916
发送接收报告
918

图9

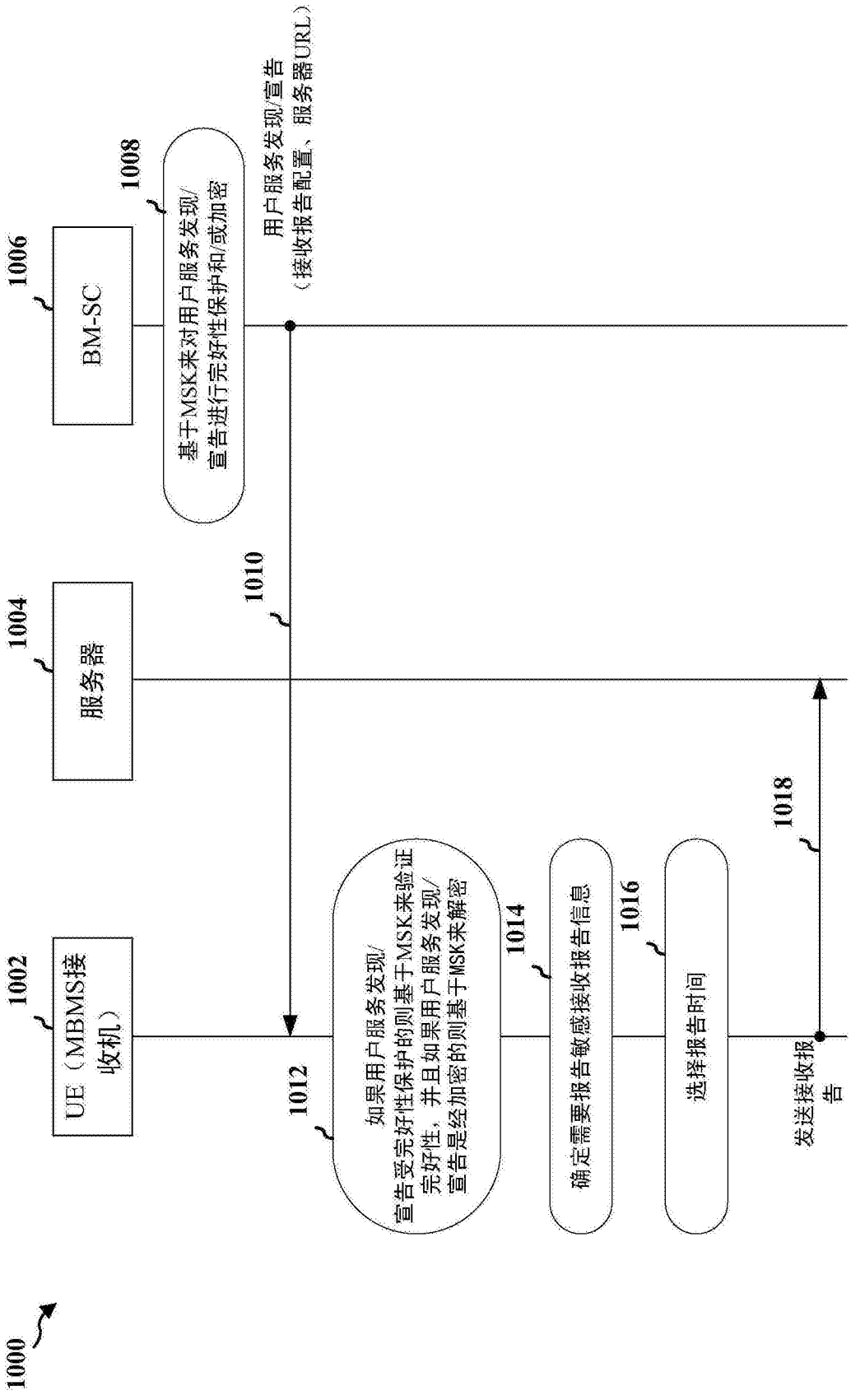

1000
UE（MBMS接收机）
1002
服务器
1004
BM-SC
1006
1008
基于MSK来对用户服务发现/宣告进行完好性保护和/或加密
用户服务发现/宣告（接收报告配置、服务器URL）
1010
1012
如果用户服务发现/宣告受完好性保护的则基于MSK来验证完好性，并且如果用户服务发现/宣告是经加密的则基于MSK来解密
1014
确定需要报告敏感接收报告信息
1016
选择报告时间
1018
发送接收报告

图10

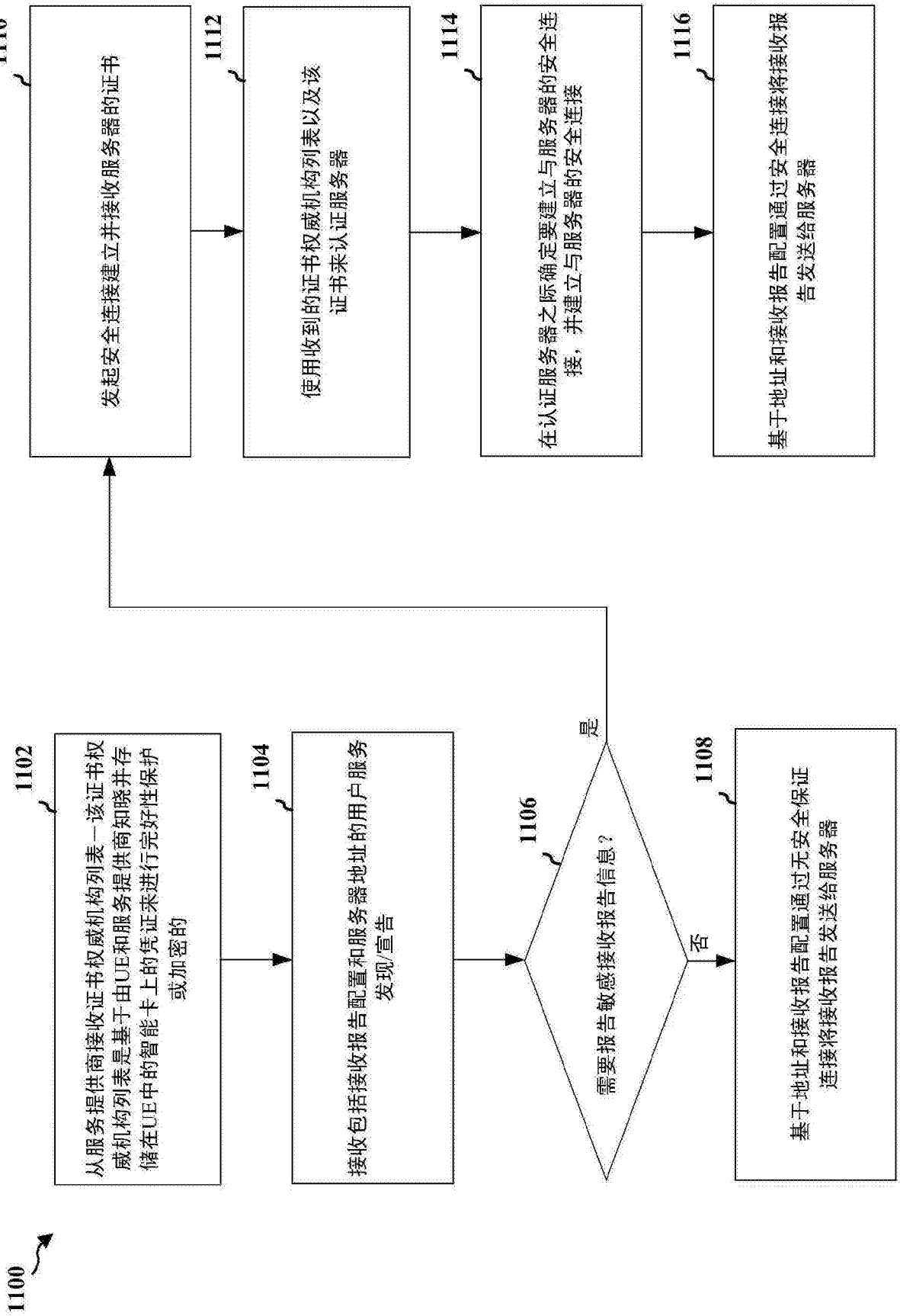

1100
1102
从服务提供商接收证书权威机构列表—该证书权威机构列表是基于由UE和服务提供商知晓并存储在UE中的智能卡上的凭证来进行完好性保护或加密的
1104
接收包括接收报告配置和服务器地址的用户服务发现/宣告
1106
需要报告敏感接收报告信息？
是
否
1108
基于地址和接收报告配置通过无安全保证连接将接收报告发送给服务器
1110
发起安全连接建立并接收服务器的证书
1112
使用收到的证书权威机构列表以及该证书来认证服务器
1114
在认证服务器之际确定要建立与服务器的安全连接，并建立与服务器的安全连接
1116
基于地址和接收报告配置通过安全连接将接收报告发送给服务器

图11

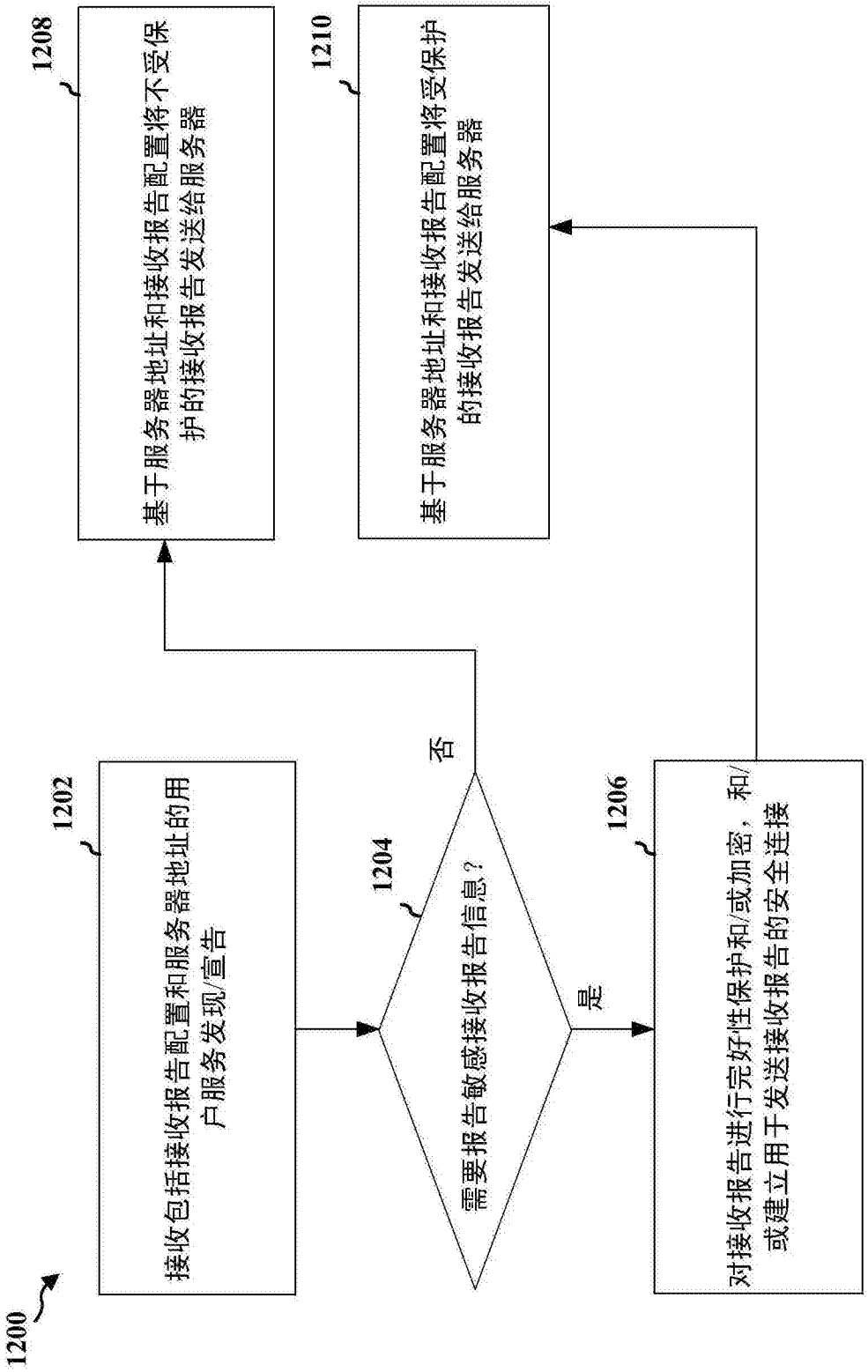

1200
1202
接收包括接收报告配置和服务器地址的用户服务发现/宣告
1204
需要报告敏感接收报告信息？
否
是
1206
对接收报告进行完好性保护和/或加密，和/或建立用于发送接收报告的安全连接
1208
基于服务器地址和接收报告配置将不受保护的接收报告发送给服务器
1210
基于服务器地址和接收报告配置将受保护的接收报告发送给服务器

图12

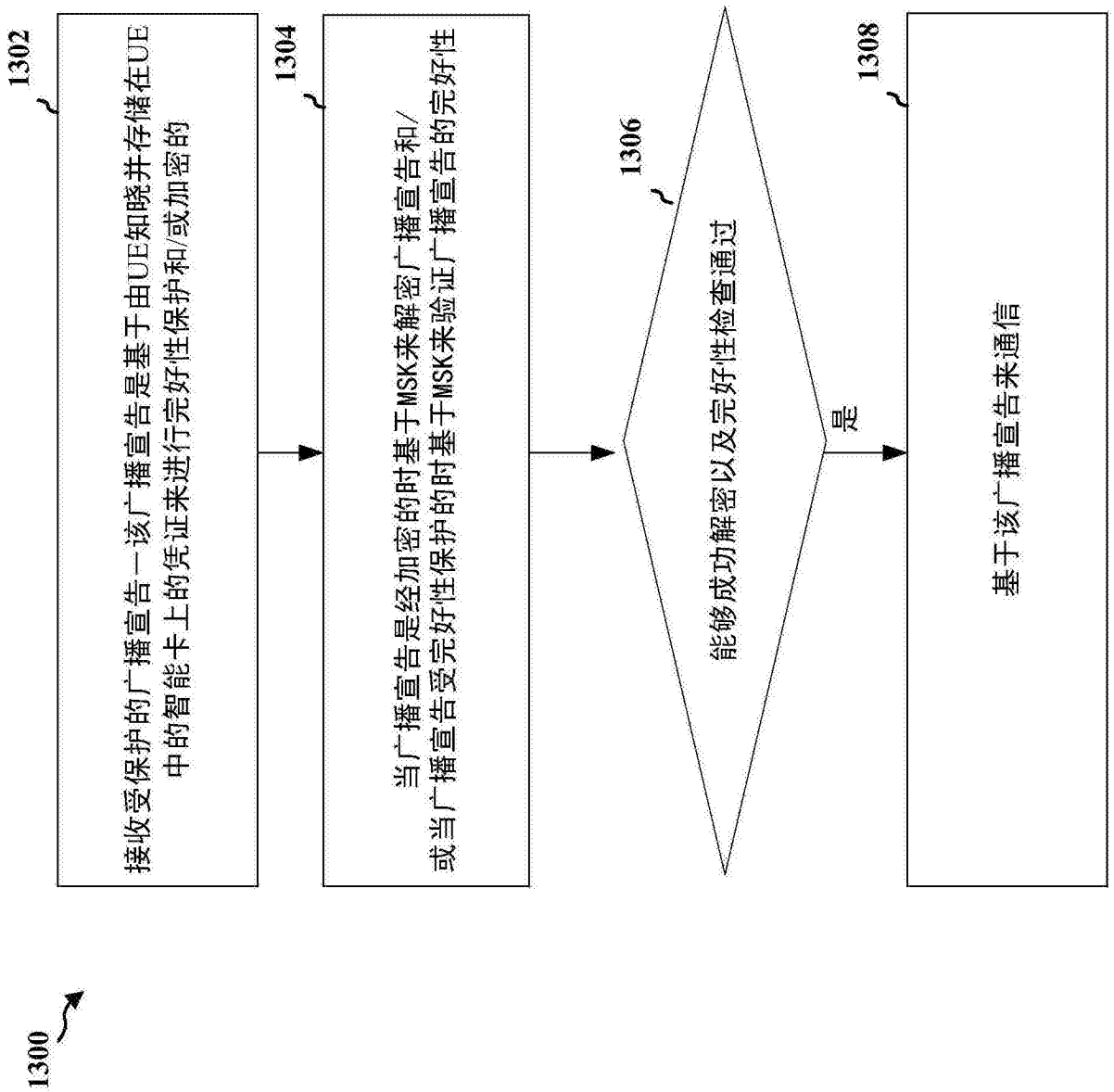

1300
1302
接收受保护的广播宣告—该广播宣告是基于由UE知晓并存储在UE中的智能卡上的凭证来进行完好性保护和/或加密的
1304
当广播宣告是经加密的时基于MSK来解密广播宣告和/或当广播宣告受完好性保护的时基于MSK来验证广播宣告的完好性
1306
能够成功解密以及完好性检查通过
是
1308
基于该广播宣告来通信

图13

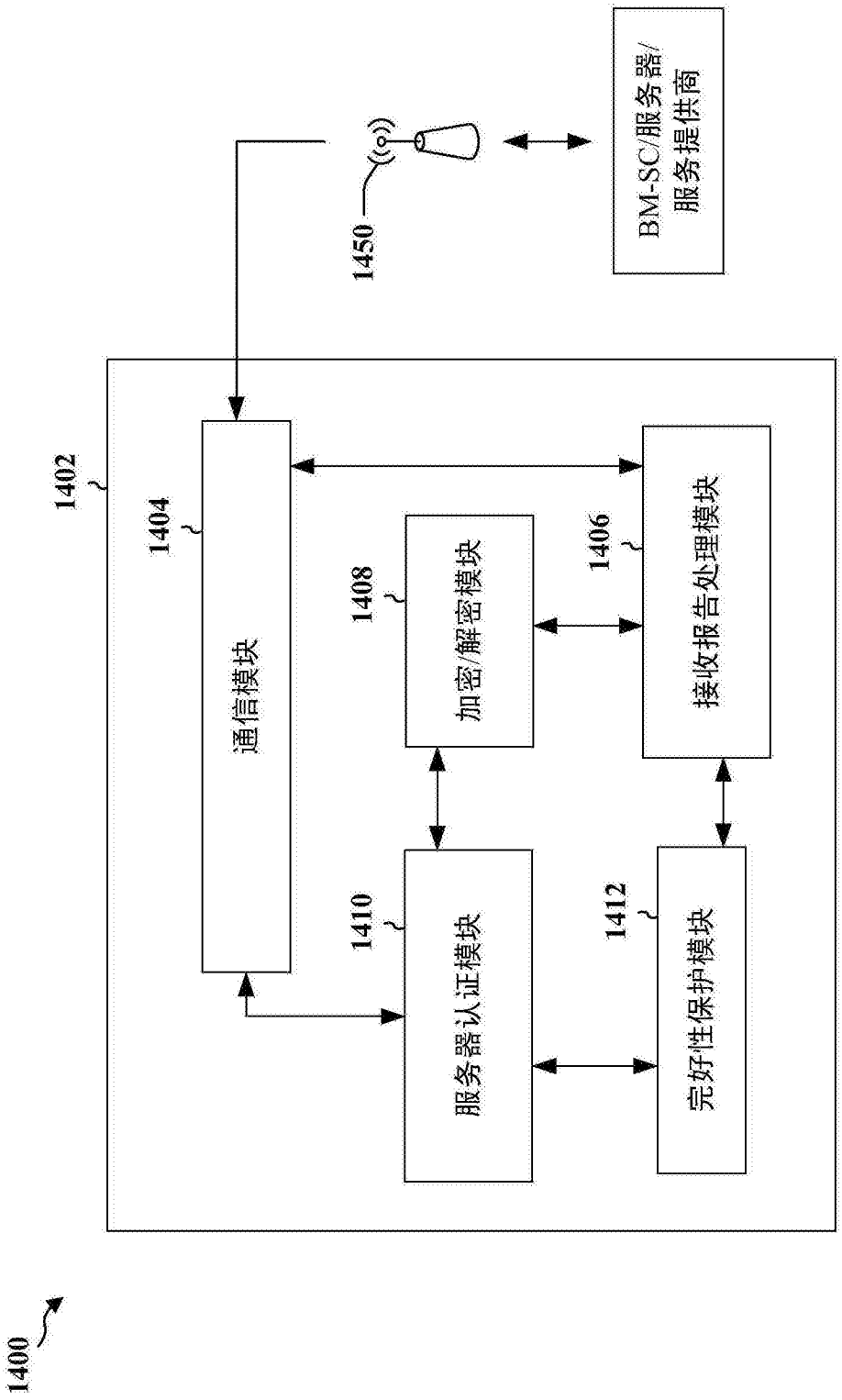

BM-SC/服务器/
服务提供商
1450
1402
1404
通信模块
1408
加密/解密模块
1406
接收报告处理模块
1410
服务器认证模块
1412
完好性保护模块
1400

图14

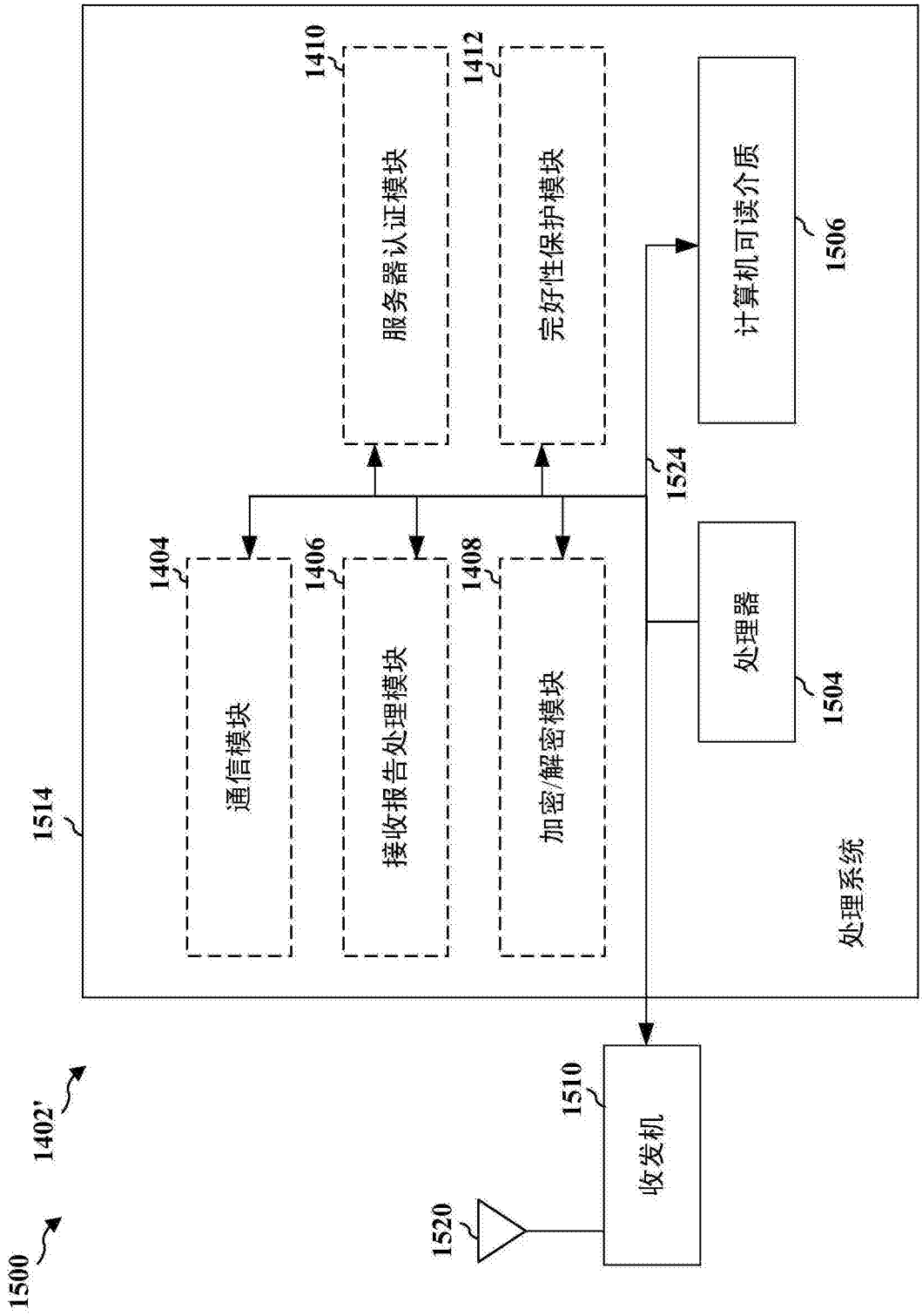

1500
1402'
1514
1404
通信模块
1406
接收报告处理模块
1408
加密/解密模块
1410
服务器认证模块
1412
完好性保护模块
1524
处理器
1504
计算机可读介质
1506
处理系统
1510
收发机
1520

图15