(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 1836423 B
(45)授权公告日 2011.06.22

(21)申请号 200480023622.0

(22)申请日 2004.08.18

(30)优先权数据
60/496,153 2003.08.18 US
10/921,425 2004.08.17 US

(85)PCT申请进入国家阶段日
2006.02.17

(86)PCT申请的申请数据
PCT/US2004/027052 2004.08.18

(87)PCT申请的公布数据
WO2005/020544 EN 2005.03.03

(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 P·E·本德 R·F·小奎克
P·A·阿加西

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 丁艺

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
US 2002/0169724 A1,2002.11.14,说明书第0002-0008,0021-0024,0029-0030段.
WO 02/33993 A1,2002.04.25,全文.
CN 1163538 A,1997.10.29,全文.

审查员 汪德闯

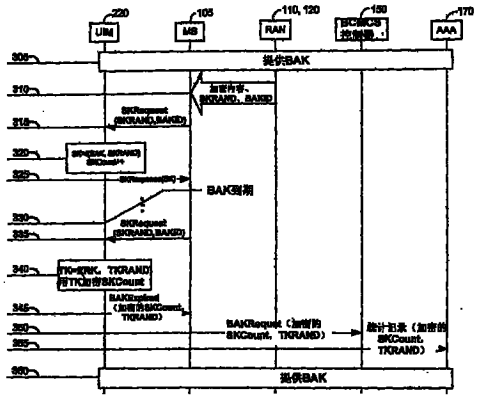
权利要求书 2 页 说明书 7 页 附图 3 页

(54)发明名称

用于无线通信系统中广播-多播业务(BCMCS)的基于时间计费的方法和设备

(57)摘要

本发明公开了一种基于时间对从无线通信系统的移动台上的广播-多播业务(BCMCS)浏览内容来计费的方法和设备。计数值(SKCount)是基于生成的用于解密来自BCMCS的特定内容的短期密钥(SK)的数量确定的。在移动台上浏览特定内容的时间量可以确定为计数值(SKCount)和生成短期密钥之间的周期(SKPeriod)的函数。由于浏览广播到移动台的特定内容需要短期密钥,所以这提供了关于用户的实际内容浏览时间的信息。



CN 1836423 B

1. 一种通信系统中的方法，包括：

接收周期性变化的数字；

接收带有表示业务信道具有相关内容的标识符的第一密钥；

在终端上生成作为至少所述周期性变化的数字和所述第一密钥的函数的至少一个第二密钥，所述至少一个第二密钥被配置成能访问所述内容；和

在终端上计算生成的第二密钥的数量以产生用于统计终端上所显示的所述内容的计数值。

2. 如权利要求 1 所述的方法，还包括：

确定所述生成所述一个第二密钥和随后生成第二密钥之间的周期。

3. 如权利要求 1 所述的方法，还包括：

加密所述计数值；和

向远程服务器发射加密的计数值。

4. 如权利要求 3 所述的方法，其中所述加密所述计数值还包括：

将所述计数值加密为登记密钥和随机数的函数。

5. 如权利要求 3 所述的方法，还包括：

在所述远程服务器上接收所述加密的计数值；和

解密所述加密的计数值。

6. 如权利要求 2 所述的方法，还包括：

将在所述终端上浏览所述内容的时间量确定为至少所述计数值和所述确定的周期的函数。

7. 一种通信系统中的设备，包括：

用于接收周期性变化的数字的装置；

用于接收带有表示业务信道具有相关内容的标识符的第一密钥的装置；

用于在终端上生成作为至少所述周期性变化的数字和所述第一密钥的函数的至少一个第二密钥的装置，所述至少一个第二密钥被配置成能访问所述内容；和

用于在终端上计算所述生成的第二密钥的数量以产生用于统计终端上显示的所述内容的计数值的装置。

8. 如权利要求 7 所述的设备，还包括：

用于确定生成所述一个第二密钥和随后生成第二密钥之间的周期的装置。

9. 如权利要求 7 所述的设备，还包括：

用于加密所述计数值的装置；和

用于向远程服务器发射加密的计数值的装置。

10. 如权利要求 9 所述的设备，其中用于加密所述计数值的所述装置还包括：

用于将所述计数值加密为登记密钥和随机数的函数的装置。

11. 如权利要求 9 所述的设备，还包括：

用于在所述远程服务器上接收所述加密的计数值的装置；和

用于解密所述加密的计数值的装置。

12. 如权利要求 8 所述的设备，还包括：

用于将所述终端上显示所述内容的时间量确定为至少所述计数值和所述确定的周期

的函数的装置。

13. 一种通信系统中的终端，包括：

接收器，用于接收周期性变化的数字和带有表示业务信道具有相关内容的标识符的第一密钥；

控制器，用于在终端上生成作为至少所述周期性变化的数字和所述第一密钥的函数的至少一个第二密钥，所述至少一个第二密钥被配置成能访问所述内容；和

其中所述控制器在终端上计算所述生成的第二密钥的数量以产生用于统计所述终端上显示的所述内容的计数值。

14. 如权利要求 13 所述的终端，其中所述控制器还确定生成所述一个第二密钥和随后生成第二密钥之间的周期。

15. 如权利要求 13 所述的终端，其中所述控制器加密所述计数值；并还包括：

用于向远程服务器发射所述加密的计数值的发射器。

16. 如权利要求 15 所述的终端，其中所述控制器将所述计数值加密为登记密钥和随机数的函数。

17. 如权利要求 15 所述的终端，其中所述远程服务器接收从所述终端发射的所述加密的计数值，并解密所述加密的计数值。

18. 如权利要求 15 所述的终端，其中所述远程服务器将所述终端上显示所述内容的时间量确定为至少所述计数值和所述确定的周期的函数。

19. 如权利要求 18 所述的终端，还包括

根据在所述终端上浏览所述内容的所述时间量对所述终端的用户计费。

用于无线通信系统中广播－多播业务（BCMCS）的基于时间计费的方法和设备

[0001] 要求美国35款119条下的优先权

[0002] 本申请要求2003年8月18日提交的第60/496,153号，标题为“用于广播－多播业务的基于时间计费（Time-Based Charging forBroadcast-Multicast Services）”的美国临时申请的优先权，并转让给其受让人，据此特别作为参考结合在本文中。

技术领域

[0003] 本发明通常涉及通信，更具体地涉及用于对利用广播－多播业务（BCMCS）的无线通信系统中的信息服务计费的方法和设备。

背景技术

[0004] 广播－多播业务（BCMCS）在无线通信系统中向通过无线通信媒体接收广播数据的多个移动台，提供点到多点通信业务。由无线通信系统发射到多个移动台的广播数据（即，内容）可以包括但不必局限于，新闻、电影、体育赛事等等。发射到移动台的内容的具体类型可以包括各种多媒体数据，如文本、音频、图片、流视频等等。内容典型地是由内容提供者生成的，并在无线通信系统的广播信道上被广播到预订该特定业务的移动台。

[0005] 广播内容典型地通过几级加密和解密被加密和解密，以提供至少某种水平的保证，使得未被授权的用户不能解密他们没有获得授权的内容（即，移动台的用户没有预订的内容）。为了能够对广播内容进行加密和解密，广播－多播业务利用了加密密钥的使用。

[0006] 长期加密密钥，通常称作广播接入密钥（BAK），其通过广播－多播业务被提供到移动台的存储器中。短期密钥（SK），来源于广播接入密钥BAK和随机数SKRAND。该内容被用短期密钥SK进行加密，并由无线通信系统通过空中将其与随机数SKRAND一起广播到移动台。移动台通过随机数SKRAND和广播接入密钥BAK，计算短期密钥SK，并使用短期密钥SK，来解密接收到的内容，以将内容显示给移动台的用户。

[0007] 典型地，接收到广播接入密钥BAK之后，对移动台的用户收取广播内容的费用。因此，不管用户实际上是否浏览了来自广播－多播业务的广播内容，用户由于接收到广播接入密钥（BAK）而被收费。当用户被收取他或她当前没有浏览的广播内容的费用时，用户负担了这些不必要引起的额外费用。

[0008] 本发明的目的是克服，或至少减小上述一个或多个问题的影响。

发明内容

[0009] 本发明的一个方面，提供了一种方法。该方法包括接收周期性变化的数字，和接收带有用于表示业务信道的标识符的第一密钥。生成作为至少周期性变化的数字和第一密钥的函数的至少一个第二密钥。计算所生成的第二密钥的数量，来产生用于统计终端上显示的内容的计数值。

[0010] 本发明的另一方面，提供了一种设备。该设备包括用于接收周期性变化的数字的

装置，和用于接收带有表示业务信道的标识符的第一密钥的装置。该设备还包括用于生成作为至少周期性变化的数字和第一密钥的函数的至少一个第二密钥的装置，和用于计算生成的第二密钥数量来产生用于统计终端上显示的内容的计数值的装置。

附图说明

[0011] 图 1 的示范性框图示出了根据本发明的一个实施例的利用广播 - 多播业务 (BCMCS) 的无线通信系统；

[0012] 图 2 的框图示出了图 1 中的无线通信系统的移动台的更详细表示；和

[0013] 图 3 的信令流程图示出了图 1 的无线通信系统各组件之间为实现基于时间收取浏览 BCMCS 内容的费用的信令。

具体实施方式

[0014] 现回到附图，并具体参考图 1，该图示出了根据本发明的一个实施例的无线通信系统 100 的示范性框图。无线通信系统 100 包括多个移动台 (MS)105，其与多个基收发信台 (BTS)110，其是地理上分散的，以在移动台 105 经过无线通信系统 100 时，提供对它们的连续的通信覆盖。移动台 105 可以采取能够从基收发信台 110 接收信息的任何装置形式，包括个人数字助理 (PDA)、无线电话、具有无线功能的便携式电脑、无线调制解调器、或任何其它可以无线通信的装置。

[0015] 根据一个实施例，无线通信系统 100 利用广播 - 多播业务 (BCMCS)，将数据分组点到多点地发射到在无线通信系统 100 内部通信的预定一组移动台 105。在一个实施例中，数据分组提供的内容诸如，例如在无线通信链路 115 上从基收发信台 110 发射到移动台 105 的新闻、电影、体育赛事等。要理解的是，发射到移动台 105 的内容的具体类型可以包括各种多媒体数据（例如，文本、音频、图片、流视频等等），并且因此不必需受到前述实例的限制。

[0016] 每个基收发信台 110 连接到基站控制器 (BSC)120，其控制基收发信台 110 和无线通信系统 100 的其它组件之间的连接。基收发信台 110 和基站控制器 120 共同形成无线接入网络 (RAN)，用于将内容传送到在无线通信系统 100 内部通信的多个移动台 105。在移动台 105 漫游时，无线接入网络既可以由向移动台 105 的用户提供预订业务的无线电信运营商所拥有，也可以是由向移动台 105 的用户提供业务的另一个电信运营商所拥有的被访问的网络。

[0017] 在一个实施例中，基站控制器 120 通过分组控制功能 (PCF) 连接到分组数据业务节点 (PDSN)140，其中分组控制功能 (PCF) 用于通过因特网协议 (IP) 媒体（未示出），将无线通信系统 100 连接到内容提供者 (CP)160。在 BCMCS 控制器 150 控制下，PDSN140 处理分配给移动台 105 的数据分组，其中 BCMCS 控制器 150 可以有也可以没有到 PDSN140 的直接连接。BCMCS 控制器 150 调度由内容提供者 160 所提供的内容的广播和多播，并执行广播 - 多播业务的安全功能。

[0018] 对于 BCMCS 业务，基收发信台 110 从 PDSN140 接收信息流，并将信息提供到指定的通往在无线通信系统 100 内部通信的一组预定的移动台 105 的无线通信链路 115 上。BCMCS 控制器 150 可以进一步连接到验证、授权，和统计 (AAA) 服务器 170，其提供对预订了

广播－多播业务的无线通信系统 100 的多个移动台 105 的验证、授权和统计。AAA 服务器 170 可以被实现为第三方服务器，其既不属于本地网络电信运营商，也不属于移动台 105 的服务网络电信运营商。

[0019] 内容提供者 160 生成要从基收发信台 110 广播到得到接收具体类型的内容授权的一组预定的移动台 105 的内容。内容提供者 160 可以被实现为第三方内容源，其既不属于本地网络电信运营商，也不属于移动台 105 的服务网络电信运营商。应该理解的是，基站控制器 120 也可以连接到各种其它类型的网络，如公共交换电话网 (PSTN)（未示出），例如以扩展无线通信系统 100 的通信能力。在示例性的实施例中，基收发信台 110 和移动台 105 根据码分多址 (CDMA) 方案运行。但是应该理解，无线通信系统 100 可以利用各种其它多址方案，如时分多址 (TDMA) 等等，而不脱离本发明的精神和范围。

[0020] 无线通信系统 100 能够通过包括有高数据速率能力的广播信道的无线通信链路 115，进行高速 BCMCS 业务，其将被大量移动台 105 接收。在本文中用术语广播信道来表示承载广播业务的单独的前向链路物理信道。也可以通过无线通信链路 115 的反向链路，将数据从移动台 105 发射到基收发信台 110。在一个实施例中，反向链路可以包括信令业务信道和数据速率控制 (DRC) 信道。可以通过向无线通信系统 100 指出可能用于在前向链路的广播信道上广播内容的可支持广播数据速率的数据速率请求，来使用反向链路的数据速率控制 (DRC) 信道。

[0021] 现参考图 2，该图示出了根据本发明的一个实施例的移动台 105 的框图。在其比较简单的一种形式中，移动台 105 包括用于调谐到广播信道以接收从基收发信台 110 发射的 BCMCS 内容的接收器 205。发射器 210 可以向正与移动台 105 进行通信的基收发信台 110 发射数据。移动台 105 还包括用于控制移动台 105 的各种操作功能的控制器 215。

[0022] 移动台 105 进一步配置有用户识别模块 (UIM)220。在一个实施例中，UIM220 可以是连接到移动台 105 的控制器 215 的可移动存储模块。但是要理解，UIM220 能可替代地被实现为移动台 105 的固定部分。UIM220 通常与移动台 105 的特定用户相关联，并被用于验证移动台 105 的特定用户被授予给予特定用户的特权，如接入无线通信系统 100、由系统 100 提供的特定业务 / 特征，和 / 或访问通过 BCMCS 业务预订的特定内容。

[0023] 移动台 105 还可以包括显示屏 230，以允许用户浏览内容提供者 160 所提供的内容。如上所述，图 2 中示出的移动台 105 是以它最简单的一种形式给出的。因此，移动台 105 可以包括用于提供各种其它功能的另外的组件，而不脱离本发明的精神和范围。另外，应该理解，移动台 105 的一些组件的功能可以集成到单独组件中，而不是以单独的实体组件来提供。

[0024] 经过几级加密和解密，对无线通信系统 100 内部的内容广播进行加密和解密，以提供至少几级保证，使得未被授权的用户不能解密他们没有被授权的内容（即，移动台 105 的用户没有预订的内容）。为了能够对内容进行加密和解密，BCMCS 业务利用了加密密钥的使用。密钥是与加密算法合作产生具体密文的值。在 2001 年 8 月 20 号提交的美国第 09/933,972 号，标题为“用于数据处理系统中的安全性的方法和设备 (Method and Apparatus for Security in a Data Processing System)”的专利中，描述了多播－广播－多媒体系统中的数据内容加密和解密方案的实例，其作为参考整体结合在本文中。

[0025] 为了在特定时间解密广播内容，移动台 105 需要知道当前解密密钥。为防止由

BCMCS提供的内容的业务盗窃，解密密钥通常是频繁更换的，例如，每分钟更换。这些解密密钥称作短期密钥(SK)，其用于在比较短的时期解密广播内容。

[0026] 为了获得对BCMCS控制器150的接入，移动台105的用户向BCMCS登记并接着进行预订。当预订得到授权时，与移动台105一起周期性更新各加密密钥。在登记过程中，BCMCS控制器150和移动台105的UIM220就充当用户和BCMCS之间的安全联系的登记密钥(PK)达成协议。接着，BCMCS控制器150可以向UIM220发送用登记密钥PK加密的进一步的保密信息。登记密钥PK在UIM220中保密，并且对于移动台105的给定UIM220是独一无二的(即，每个用户被分配不同的登记密钥PK)。

[0027] 在预订过程中，BCMCS控制器150向移动台105的UIM220发送公共广播接入密钥(BAK)的值，该密钥是中期的、共用密钥用于取得多个短期密钥SK，并以每个用户为基础被分发给预订用户的UIM220。BCMCS控制器150向UIM220发送使用只有该UIM220才有的登记密钥RK加密的广播接入密钥BAK的值。移动台105的UIM220能够使用其中存储的登记密钥RK，从加密文本恢复初始广播接入密钥BAK的值。广播接入密钥BAK充当BCMCS控制器150和该组预订了广播-多播业务的用户之间的安全联系。广播接入密钥标识符BAKID是用登记密钥RK与表示发射到移动台105的特定内容的标识符一起加密的广播接入密钥BAK。

[0028] 对于每个预订者，BCMCS控制器150使用临时密钥TK和随机数TKRAND来加密广播接入密钥BAK，以获得用户专用的加密广播接入密钥标识符BAKID，其中临时密钥TK是从存储在UIM220中的用户专用登记密钥RK中取得的。BCMCS控制器150向预订用户的移动台105发送相应的广播接入密钥标识符BAKID。例如，广播接入密钥BAK可以作为使用对应于每个UIM220的登记密钥RK加密的IP分组来发射。在示范性实施例中，广播接入密钥标识符BAKID是IPSec分组，并且广播接入密钥BAK是具有用登记密钥RK作为密钥加密的广播接入密钥BAK的IPSec分组。由于登记密钥RK是“每个用户”密钥，所以BCMCS控制器150向每个预订者分别发送广播接入密钥BAK。这样，广播接入密钥BAK不是在无线通信系统100的广播信道上发送的。移动台105将广播接入密钥标识符BAKID传递给UIM220。UIM220使用存储在UIM220中的登记密钥RK的值和广播接入密钥标识符BAKID的值来计算广播接入密钥BAK。接着将广播接入密钥BAK的值存储在UIM中。在一个实施例中，广播接入密钥标识符BAKID包括安全参数索引(SPI)值，其用于指示移动台105的控制器215将广播接入密钥标识符BAKID传递给UIM220，并指示UIM220使用登记密钥RK来解密广播接入密钥BAK。广播接入密钥BAK的更新周期被希望足以允许BCMCS控制器150将广播接入密钥BAK分别发送到每个预订者，而不导致重大开销。

[0029] 接着，BCMCS控制器150广播短期密钥SK，使得移动台105能够解密与该短期密钥相关联的特定内容。短期密钥SK是广播接入密钥BAK和周期性变化的数字SKRAND的函数。周期性变化的数字SKRAND可以是用类似于密码hash函数的散列(hashing)函数生成的随机数。周期性变化的数字SKRAND也可以是序列数、时间标记、或其它变化的值，只要其实施能使用户不能预先计算出短期密钥SK。UIM220通过使用广播接入密钥BAK和SKRAND的函数，从广播接入密钥BAK和SKRAN中提取出短期密钥SK，并将短期密钥SK传递给移动台105的控制器215。BCMCS控制器150使用当前短期密钥SK加密广播内容。在一个实施例中，采用了加密算法，例如高级加密标准(AES)密码算法。接着，IPsec分组根据封装安

全有效载荷 (ESP) 传递模式传递加密内容。IPsec 分组还包含 SPI 值，其指示移动台 105 使用当前短期密钥 SK 来解密接收到的广播内容。

[0030] 在本发明的领域内，也可以执行使用用于加密和解密的公共密钥或共用秘密 (sharcd-sccrct) 密钥的各其它实施例。例如，在可替代实施例中，可以通过使用本领域技术人员公知的公共密钥机制，例如 RSA 或 EIGamal，来提供安全交付或向 UIM220 提供广播接入密钥 BAK。

[0031] 图 3 是根据本发明的一个实施例的用于实现基于时间对广播 - 多播业务计费的信令流。感兴趣的特定信道的广播接入密钥 BAK 被提供到移动台 105 的用户识别模块 (UIM)220 的存储器中。如图 3 所示，在 305，广播接入密钥提供消息从 AAA 服务器 170 被提供给移动台 105 的 UIM220。BCMCS 控制器 150 用临时密钥 TK 加密广播接入密钥 BAK，其中临时密钥 TK 是基于登记密钥 RK 和随机数 TKRAND 得到的。在一个实施例中，在 305 的 BAK 提供开始之前，已经将登记密钥 RK 提供到移动台 105 的 UIM220 中了。

[0032] 在 310，由基站控制器 120 和基收发信台 110 一起组成的无线接入网络 (RAN)，通过广播信道向移动台 105 广播加密内容。与加密内容一起，无线接入网络还广播周期性变化的数字 SKRAND 和广播接入密钥标识符 BAKID，以识别广播接入密钥 BAK。移动台 105 使用周期性变化的数字 SKRAND 和广播接入密钥 BAK 来计算短期密钥 SK。

[0033] 移动台 105 从无线接入网络的基收发信台 110 接收加密内容、SKRAND 和 BAKID。在 315，移动台 105 的控制器 215，将接收到的 SKRAND 和 BAKID 与对短期密钥 SK 的请求 (SKRequest) 一起发送给 UIM220。发送到 UIM220 的请求 SKRequest 还包括广播信道的标识符。在 320，UIM220 从 SKRAND 和 BAK 标识符 BAKID 所标识的 BAK 计算短期密钥 SK。

[0034] UIM220 保留从每个广播信道得到的短期密钥 SK 的数量的短期密钥计数 (SKCount)。每当 UIM220 计算并取得新的短期密钥，它就将 SKCount 加一。可以通过用 SKcount 乘以短期密钥变化的周期 (即，SKPeriod)，得到用户浏览特定内容信道的时间量。在一个实施例中，系统操作者可以基于操作者的内容盗窃的潜在危险，来设置 SKPeriod。例如，SKPeriod 的变化范围可以从几秒到几分钟。

[0035] 在 325，UIM220 向移动台 105 的控制器 215 发送短期密钥 SK。从 UIM220 接收到短期密钥 SK 之后，移动台 105 的控制器 215 将能够使用短期密钥 SK 来解密内容，并将接收到的用于浏览的内容反映到移动台 105 的显示屏 230 上。

[0036] 每当移动台 105 从无线接入网络的基收发信台 110 接收到新的周期性变化的数字 SKRAND，就重复 310 到 325 的各过程。周期性变化的数字 SKRAND 可以频繁变化，以确保被授权用户浏览广播内容。

[0037] 在 330，存储在移动台 105 的 UIM220 中的广播接入密钥 BAK 可能到期或者接近到期。在 335，移动台 105 的控制器 215 将 SKRAND 和 BAKID 与对短期密钥 SK 的请求 SKRequest 一起发送到 UIM220。

[0038] 在 340，当 UIM220 确定广播接入密钥 BAK 已经到期时，UIM220 使用登记密钥 RK 和随机数 TKRAND 来计算临时密钥 TK。临时密钥 TK 是单独使用的用户专用密钥，其可用于加密和解密广播接入密钥 BAK 值。TKRAND 是随机数，其可以用类似于密码 hash 函数的散列函数来生成。因此，TK 是临时密钥，其使用登记密钥 RK 作为秘密密钥 (secret key)，并且 TK 是基于登记密钥 RK 和随机数 TKRAND 得到的。

[0039] 在345，UIM220使用临时密钥TK来加密短期密钥计数SKCount，并将加密的SKCount和TKRAND与需要新广播接入密钥BAK的指示一起发送到移动台105的控制器215。由于SKCount是用临时密钥TK加密的，移动台105的控制器215不知道临时密钥TK，所以控制器215不能智能地将加密的SKCount变成较低的值。这充分降低了内容盗窃的可能性，并保护用户避免未被授权的访问用户的内容浏览计数。

[0040] 在另一个实施例中，短期密钥SK可以不受阻碍地发射，并且UIM220可以用SKCount和临时密钥TK生成签名。在该实施例中，签名将被发射到AAA服务器170。

[0041] 在350，移动台105的控制器215向BCMCS控制器150发送对“新”(即，新建的)广播接入密钥BAK的请求。移动台105包括从UIM220接收到的加密的SKCount和TKRAND，还有广播接入密钥BAK请求。

[0042] 在355，BCMCS控制器150将加密的SKCount和TKRAND传递到AAA服务器170。AAA服务器170基于登记密钥RK和TKRAND计算临时密钥TK，并解密SKCount。AAA服务器170用SKCount更新用户的统计记录。在360，新的广播接入密钥BAK被提供到移动台105的UIM220中。如上所述，可以通过将SKCount乘以短期密钥变化周期(即，SKPeriod)，得到用户浏览特定内容的时间量。因此，可以根据用户实际浏览内容的时间量(由于浏览内容需要短期密钥SK)，对移动台105的用户计费，而不是从在移动台105上接收到BAK的时间开始计费。

[0043] 为了避免打断用户浏览的广播业务，移动台105可以在当前BAK到期之前从AAA服务器170取来新的广播接入密钥BAK。在这种情况下，移动台105在新的BAK被提供到UIM220中之后，将继续使用旧的BAK一段时间。

[0044] 确保正确地保留SKCount是很重要的。在一个实施例中，将SKCount发送到移动台105之后，UIM220为所考虑的广播信道废止旧的计数器并启用新的计数器。当新的BAK被提供到UIM220中时，可以删除旧的计数器。如果没有提供新的BAK，则下一次移动台110请求SKCount时，UIM220返回旧的和新的计数器总和作为SKCount。可以使用旧的和新的计数器的总和，执行验证、授权和统计(AAA)，以提供内容浏览时间。

[0045] 在另一个实施例中，将计数器的当前值发送到移动台105之后，UIM220继续将SKCount加一。当BCMCS控制器150发送新的BAK时，它还在BAK请求中以加密形式发回从UIM220接收到的计数。UIM220解密从BCMCS控制器150接收到的计数，并减去从SKCounter接收到的计数。该特定实施例允许将预付帐单应用到基于时间的计费。BCMCS控制器170保留付款的计数，并将它们发送到UIM220。接着，UIM220计算其差，并且如果需要的话，允许用户为更多计数付款。

[0046] 在另一个实施例中，当提供了新的BAK时，UIM220将SKCounter重新设置为零。在该特定实施例中，在发送SKCount和接收新的BAK期间，将不根据浏览广播内容对用户计费。

[0047] 本领域的技术人员将了解，可以使用各种不同工艺和技术中的任何一种来表示信息和信号。例如，上述描述通篇中可能提到的数据、指令、命令、信息、信号、比特、符号，和码片，可以用电压、电流、电磁波、磁场或粒子、光场或粒子、或它们的任意组合体来表示。

[0048] 本领域的技术人员将进一步理解，结合本文公开的实施例描述的不同示例性逻辑块、模块、电路，和算法步骤，可以实施为电子硬件、计算机软件、或二者的组合体。为了清楚

地说明硬件和软件的该可互换性，上面根据其功能性一般性地描述了不同的示例性组件、程序块、模块、电路，和步骤。这种功能性用硬件还是软件来实施取决于特定应用和整个系统上受到的设计约束条件。对于每个特定应用，熟练技术人员可以用不同的方法来实施所描述的功能，但是这种实施决策不应该被认为导致脱离本发明的范围。

[0049] 结合本文公开的实施例描述的不同的示例性逻辑块、模块，和电路，可以用通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或其它可编程逻辑器件、分立门或晶体管逻辑、分立的硬件组件、或设计成执行本文所描述的功能的它们的任何组合体来实施或执行。通用处理器可以是微处理器，但是可替代地，处理器可以是任何传统的处理器、控制器、微处理器、或状态机。处理器也可以实施为计算器件的组合体，例如，DSP 和微处理器、多个微处理器、一个或多个微处理器结合 DSP 芯、或者任何其它这种结构的组合体。

[0050] 结合本文公开的实施例描述的方法或算法的步骤可以直接在硬件、由处理器执行的软件模块、或者二者的组合体中实施。软件模块可以位于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动硬盘、CD-ROM、或本领域中公知的任何其它形式的存储介质中。示范性存储介质连接到处理器，使得处理器能够从存储介质读取信息和写入信息。可替代地，存储介质可以被集成到处理器。处理器和存储介质可以位于单独的 ASIC 中，或者例如作为移动站中的分离组件。

[0051] 先前提供的对公开的实施例的描述，是为了使本领域的任何专业熟练技术人员能够制造或使用本发明。对这些实施例的不同修改，对于本领域专业技术人员将是显而易见的，本文中定义的一般原理可以应用到其它实施例，而不脱离本发明的精神和范围。因此，本发明不受本文示出的实施例局限，而是与本文公开的原理和新颖性特征的最宽广的范围相一致。

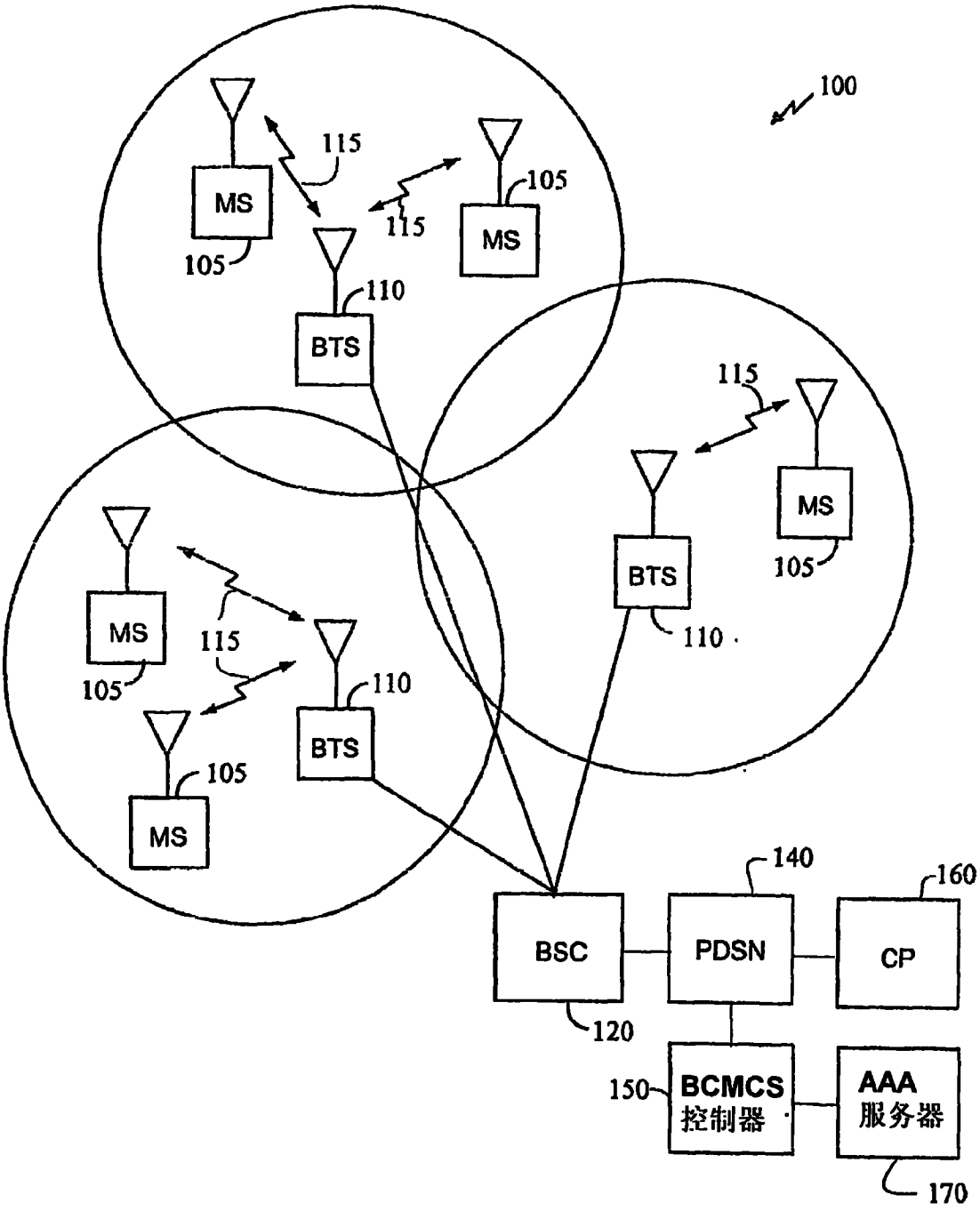

100
115
115
MS
105
105
MS
110
BTS
115
MS
105
BTS
110
MS
115
105
MS
110
BTS
105
MS
140
160
BSC
PDSN
CP
120
150
BCMCS
控制器
AAA
服务器
170

图 1

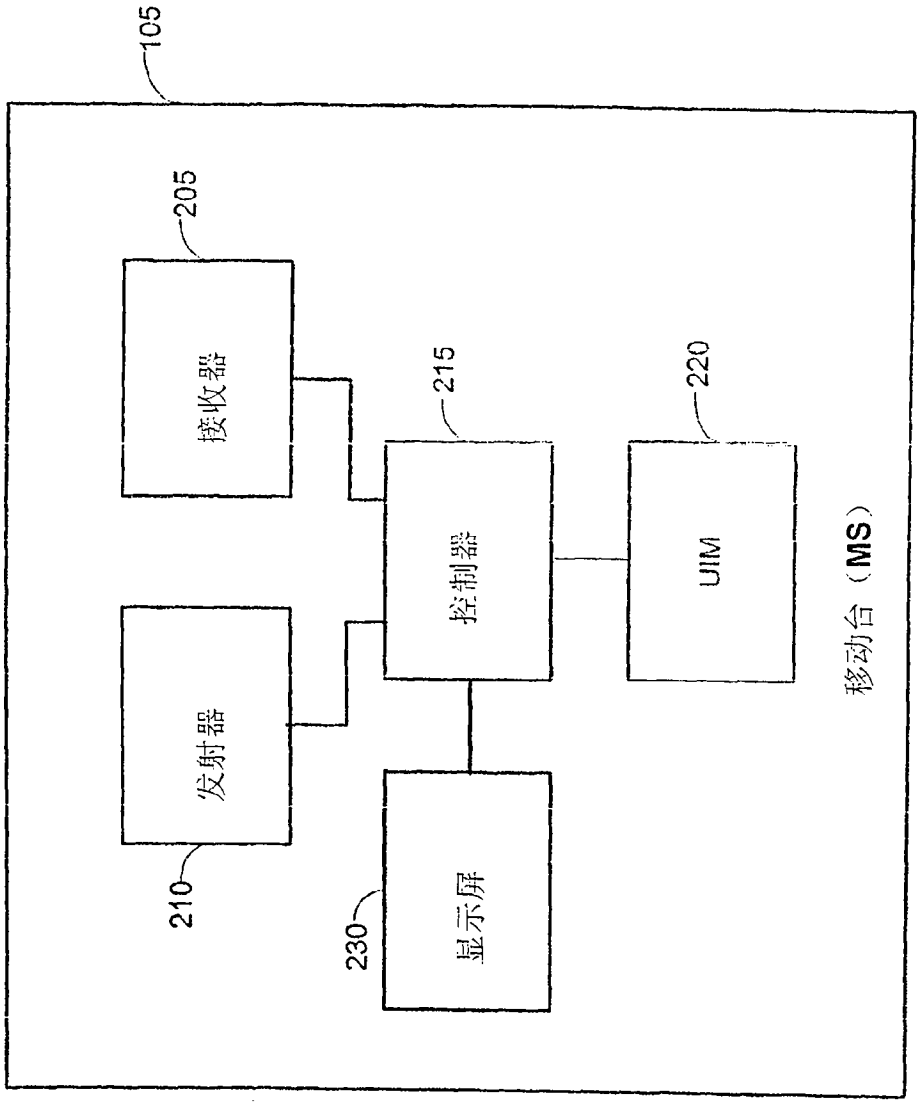


图2

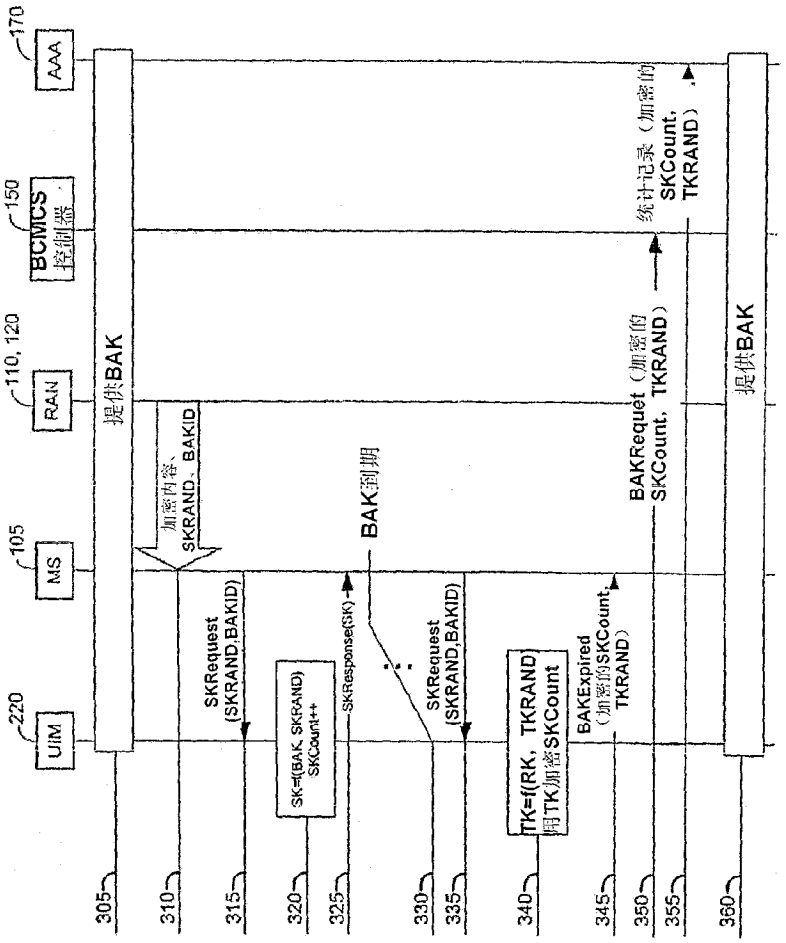

170
AAA
150
BCMCS
控制器
110, 120
RAN
105
MS
220
UIM
提供BAK
加密内容、
SKRAND、BAKID
SKRequest
(SKRAND,BAKID)
SK=f(BAK, SKRAND)
SKCount++
SKResponse(SK)
BAK到期
SKRequest
(SKRAND,BAKID)
TK=f(RK, TKRAND)
用TK加密SKCount
BAKExpired
(加密的SKCount,
TKRAND)
BAKRequet（加密的
SKCount, TKRAND）
统计记录（加密的
SKCount,
TKRAND）
提供BAK
305
310
315
320
325
330
335
340
345
350
355
360

图3