(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 101981864 B
(45)授权公告日 2015.07.22

(21)申请号 200980110985.0
(22)申请日 2009.04.03
(30)优先权数据
10-2008-0031885 2008.04.04 KR
(85)PCT国际申请进入国家阶段日
2010.09.27
(86)PCT国际申请的申请数据
PCT/KR2009/001737 2009.04.03
(87)PCT国际申请的公布数据
WO2009/145495 EN 2009.12.03
(73)专利权人 三星电子株式会社
地址 韩国京畿道
(72)发明人 瑟吉·N·塞莱兹内夫 李炳来
黄承吾 李国熙
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 钱大勇
(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
US 2006/0064584 A1,2006.03.23,1.
CN 101044754 A,2007.09.26, 全文.
US 2005/0157876 A1,2005.07.21, 全文.
CN 1408153 A,2003.04.02, 全文.
WO 02/082242 A1,2002.10.17, 全文.
EP 1223705 A2,2002.07.17, 全文.
CN 101150579 A,2008.03.26,1.
CN 1784899 A,2006.06.07, 全文.

审查员 张攀

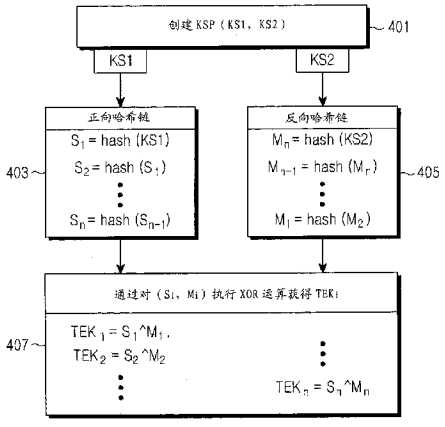
权利要求书3页 说明书10页 附图13页

(54)发明名称

通信系统中用于使用加密密钥提供广播服务的方法和装置

(57)摘要

提供了一种在通信系统中用于提供广播服务的方法和装置。该方法包括:创建包括第一密钥和第二密钥的种子密钥对;将种子密钥对发送到将为其提供广播服务的终端;使用该种子密钥对创建特定数目的加密密钥,该特定数目对应于种子密钥对的使用寿命;在该使用寿命内,使用该加密密钥来加密广播服务数据;以及广播所加密的广播服务数据。



CN 101981864 B

1. 一种在通信系统中用于提供广播服务的方法，该方法包括：

随机创建包括第一密钥和第二密钥的密钥种子对；

将该密钥种子对发送到广播服务将被提供到的终端；

使用该密钥种子对创建特定数目的加密密钥，该特定数目与该密钥种子对的使用寿命对应，其中使用该密钥种子对经过双向哈希操作和异或操作来创建该加密密钥；

在该使用寿命内，使用该加密密钥加密广播服务数据；以及

广播所加密的广播服务数据，

其中所述创建特定数目的加密密钥的步骤包括：

通过将正向哈希链应用于第一密钥来创建特定数目的正向加密密钥；

通过将反向哈希链应用于第二密钥来创建特定数目的反向加密密钥；以及

使用该正向加密密钥和反向加密密钥来创建特定数目的业务加密密钥，

其中所述创建特定数目的业务加密密钥的步骤包括：对正向加密密钥和反向加密密钥执行异或。

2. 如权利要求 1 所述的方法，还包括：当该终端是登记的终端并且使用寿命已经期满时，创建下一个密钥种子对并将其发送到终端。

3. 如权利要求 1 所述的方法，还包括：当该终端是按观看次数计费 (PPV) 终端并且使用寿命已经期满时，在从该终端接收到对于附加广播服务的请求后，创建下一个密钥种子对并将其发送到终端。

4. 一种在通信系统中由终端接收广播服务的方法，该方法包括：

接收在用于提供广播服务的装置中随机创建的包括第一密钥和第二密钥的密钥种子对；

使用接收的密钥种子对创建特定数目的加密密钥，该特定数目与该密钥种子对的使用寿命对应；以及

使用该加密密钥来解密在该使用寿命内广播的加密的广播服务数据，

其中使用该密钥种子对经过双向哈希操作和异或操作来创建该加密密钥，

其中所述创建特定数目的加密密钥的步骤包括：

通过将正向哈希链应用于第一密钥来创建特定数目的正向加密密钥；

通过将反向哈希链应用于第二密钥来创建特定数目的反向加密密钥；以及

使用该正向加密密钥和反向加密密钥来创建特定数目的业务加密密钥，

其中所述创建特定数目的业务加密密钥的步骤包括：对正向加密密钥和反向加密密钥执行异或运算。

5. 如权利要求 4 所述的方法，还包括：当该终端是登记的终端并且使用寿命已经期满时，接收下一个密钥种子对。

6. 如权利要求 4 所述的方法，还包括：当该终端是按观看次数计费 (PPV) 终端并且使用寿命已经期满时，如果该终端需要附加的广播服务，则发送对于附加广播服务的请求并接收响应于其的下一个密钥种子对。

7. 一种在通信系统中用于提供广播服务的装置，该装置包括：

种子密钥创建器，用于随机创建包括第一密钥和第二密钥的密钥种子对，以及用于通过收发器将该密钥种子对发送到该广播服务将被提供给的终端；

加密密钥创建器，用于使用该密钥种子对创建特定数目的加密密钥，该特定数目与该密钥种子对的使用寿命对应，其中使用该密钥种子对经过双向哈希操作和异或操作来创建该加密密钥；以及

数据加密器，用于在该使用寿命内使用该加密密钥加密广播服务数据，以及用于通过收发器广播所加密的广播服务数据，

其中该加密密钥创建器通过将正向哈希链应用于第一密钥来创建特定数目的正向加密密钥，通过将反向哈希链应用于第二密钥来创建特定数目的反向加密密钥，以及使用该正向加密密钥和反向加密密钥来创建特定数目的业务加密密钥，

其中所述加密密钥创建器通过对正向加密密钥和反向加密密钥执行异或来创建该业务加密密钥。

8. 如权利要求 7 所述的装置，还包括控制器，用于当该终端是登记的终端并且使用寿命已经期满时，控制该种子密钥创建器创建下一个密钥种子对并将其发送到终端。

9. 如权利要求 7 所述的装置，还包括控制器，用于当该终端是按观看次数计费 (PPV) 终端并且使用寿命已经期满时，在通过收发器从终端接收到对于附加广播服务的请求后，控制该种子密钥创建器创建下一个密钥种子对并将其发送到终端。

10. 一种在通信系统的终端中用于接收广播服务的装置，该装置包括：

收发器，用于接收在用于提供广播服务的装置中随机创建的包括第一密钥和第二密钥的密钥种子对；

加密密钥创建器，用于使用接收的密钥种子对创建特定数目的加密密钥，该特定数目与该密钥种子对的使用寿命对应，其中使用该密钥种子对经过双向哈希操作和异或操作来创建该加密密钥；以及

数据解密器，用于使用该加密密钥来解密在该使用寿命内广播的加密的广播服务数据，

其中该加密密钥创建器通过将正向哈希链应用于第一密钥来创建特定数目的正向加密密钥，通过将反向哈希链应用于第二密钥来创建特定数目的反向加密密钥，以及使用该正向加密密钥和反向加密密钥来创建特定数目的业务加密密钥，

其中所述加密密钥创建器通过对正向加密密钥和反向加密密钥执行异或来创建该业务加密密钥。

11. 如权利要求 10 所述的装置，还包括控制器，用于当该终端是登记的终端并且使用寿命已经期满时，通过该收发器接收下一个密钥种子对。

12. 如权利要求 10 所述的装置，还包括控制器，用于当该终端是按观看次数计费 (PPV) 终端并且使用寿命已经期满时，如果该终端需要附加的广播服务，则通过收发器发送对于附加广播服务的请求并通过收发器接收响应于该请求的下一个密钥种子对。

13. 一种在开放移动联盟广播 (OMA BCAST) 系统中用于提供广播服务的装置，该装置包括：

服务保护密钥分发单元 (SP-KD)，用于随机创建包括第一密钥和第二密钥的密钥种子对，以及用于将该密钥种子对发送到该广播服务将被提供给的终端；以及

服务提供商加密单元 (SP-E)，用于从 SP-KD 接收密钥种子对，用于创建特定数目的加密密钥，该数目与接收的密钥种子对的使用寿命对应，用于在该使用寿命内使用该加密密

钥来加密广播服务数据，以及用于将加密的广播服务数据发送到该终端，其中使用该密钥种子对经过双向哈希操作和异或操作来创建该加密密钥，

其中 SP-E 通过将正向哈希链应用于第一密钥来创建特定数目的正向加密密钥，通过将反向哈希链应用于第二密钥来创建特定数目的反向加密密钥，以及使用该正向加密密钥和反向加密密钥来创建特定数目的业务加密密钥，

其中所述 SP-E 通过对正向加密密钥和反向加密密钥执行异或来创建该业务加密密钥。

14. 如权利要求 13 所述的装置，其中当该终端是登记的终端并且使用寿命已经期满时，SP-KD 创建下一个密钥种子对并将其发送到终端。

15. 如权利要求 13 所述的装置，其中当该终端是按观看次数计费 (PPV) 终端并且使用寿命已经期满时，在从终端接收到对于附加广播服务的请求后，SP-KD 创建下一个密钥种子对并将其发送到终端。

通信系统中用于使用加密密钥提供广播服务的方法和装置

技术领域

[0001] 本发明涉及通信系统中的广播服务。更具体地，本发明涉及在通信系统中用于使用加密密钥提供广播服务的方法和装置。

背景技术

[0002] 近来，通信系统已被发展为向用户提供各种多媒体服务。因此，广播和多播服务可以用来向用户提供各种各样的内容。在这里，广播和多播服务将被称为“广播服务”。

[0003] 术语“广播服务”是指点到多点服务，其中一个源对象基于单向承载服务向它的服务范围内的多个接收者发送诸如音频数据、图像数据和 / 或视频数据之类的多媒体数据。广播服务支持广播模式和多播模式。在广播模式中，将数据广播给服务覆盖范围中的所有用户。另一方面，在多播模式中，用户必须订购由服务提供商 (SP) 提供的特定服务或服务群，以便享受多播服务。

[0004] 在多播模式中，广播服务数据在发送之前被加密，因此它可以仅被传送到已经订购了该广播服务的用户。发送的加密数据在使用之前必须由用户解密。因此，由服务供应商在加密广播数据时使用的加密密钥应当与用户共享。现在将描述在传统通信系统中服务提供商和用户之间的广播服务数据的加密密钥管理。

[0005] 图 1 示出了传统广播服务系统中的加密密钥管理。在基于微波接入全球互操作 (WiMax)(即，电气和电子工程师学会 (IEEE) 标准 802.16) 的广播服务系统中，加密密钥管理方法发生在网络和终端之间。为了参考，结合图 1 描述的加密密钥管理可以类似地应用于第三代伙伴项目 (3GPP) 广播系统。在给出加密密钥管理的详细描述之前，下面将描述用于加密密钥管理的因素。

[0006] 业务加密密钥 (TEK) 用于加密服务内容数据。TEK 被周期性地更新且发送到具有如下定义的群密钥 (GK) 的终端 (多个终端)。终端接收 TEK，并且可以使用接收的 TEK 来解密利用 TEK 加密的数据。

[0007] 群密钥 (GK) 是在已经订购广播服务的终端之间共享的密钥。通常在网络中创建的 GK 可以被周期性地更新且发送到已经订购特定服务组的终端。

[0008] 安全密钥 (SK) 由网络和已经订购了广播服务的终端通过特定的设置过程相互共享。SK 由网络使用来加密并发送 GK 等等。

[0009] 现在将基于用于加密密钥管理的因素来详细描述图 1。

[0010] 参考图 1，在步骤 101 中，网络 120 加密 GK 并将 GK 发送到终端 110。利用 SK 加密 GK，并且基于点对点将 GK 发送到每个终端 110。结果密钥由 $E_{SK}(GK_y)$ 指示，其中下标“y”指示当连接广播服务呼叫时 GK 被更新的次序。也就是说，结果密钥是在任意呼叫中更新的第 y 个。

[0011] 在步骤 103 中，网络 120 利用 GK_y 更新 TEK，并基于点对多点将结果密钥 TEK_{x+1} 发送到终端 110。网络 120 使用 TEK_{x+1} 加密实际的内容数据，而终端 110 使用 TEK_{x+1} 解密该加密的数据。由于 TEK 的使用寿命被设置为短于 GK 的使用寿命，因此与 GK 相比，TEK 被更频

繁地更新。在步骤 105 中，由 GK_y 加密并更新 TEK，并且结果密钥 TEK_{x+n} 被发送到终端 110。也就是说，从步骤 103 的 TEK_{x+1} 的过程至步骤 105 的 TEK_{x+n} 的过程，TEK 经历了 n 次更新过程。这里，相同的 GK_y 用于步骤 103 和 105 中。在步骤 107 中，因为 GK 109 的使用寿命期满，新的 GK 被更新，并且基于点对点被发送到终端 110。结果，利用新更新的 GK_{y+1} 加密并更新 TEK。

[0012] 参考图 2 和 3，现在将描述在开放移动联盟广播 (OMA BCAST) 系统中的传统加密密钥管理。图 2 示出了对于登记的终端的加密密钥管理，图 3 示出了对于按观看次数计费 (PPV) 的终端的加密密钥管理。“登记的终端”是指相对长期订购特定广播服务的终端，而“PPV 终端”是指以短时间为单位（例如，以特定节目为单位）订购服务的终端。例如，已经购买了一个月的任意广播服务的定购券 (coupon) 的终端可以对应于登记的终端。已经购买了在特定日期的单个剧目的定购券的终端对应于 PPV 终端。订购期限的长度是可变的。

[0013] 在 OMA BCAST 中，除了用于图 1 的 WiMax 的密钥以外，还使用服务加密密钥 (SEK) 和节目加密密钥 (PEK)。SEK 用于加密特定的广播服务，PEK 用于加密特定的节目。例如，广播服务可以由服务提供商提供，并且节目可以是服务供应商提供的特定的节目。

[0014] 首先来参考图 2 描述登记的终端中的加密密钥管理。

[0015] 图 2 示出了在传统的 OMABCAST 中登记的终端中的加密密钥管理。

[0016] 参考图 2，在步骤 201 中，网络 120 利用 SK 更新 SEK，并将结果密钥 SEK_y 发送到登记的终端 210。在步骤 203 中，网络 120 利用更新的 SEK_y 加密 PEK_z，利用加密的 PEK_z 更新 TEK，并将结果密钥 TEK_{x+1} 发送到登记的终端 210。网络 120 利用更新的 TEK_{x+1} 加密内容数据并发送加密的数据。登记的终端 210 使用发送的更新的 TEK_{x+1} 解密所发送的加密的数据。当 TEK_{x+1} 的使用寿命期满时，网络 120 在步骤 205 中再次更新 TEK。此外，当 SEK_y 209 的使用寿命期满时，在步骤 207 中，网络 120 利用 SK 更新 SEK 并将结果密钥 SEK_{y+1} 发送到登记的终端 210。SEK_{y+1} 然后用于 PEK 的加密。

[0017] 参考图 3，现在将描述 PPV 终端中的加密密钥管理。图 3 示出了在传统的 OMABCAST 中 PPV 终端中的加密密钥管理。

[0018] 参考图 3，在步骤 301 中，网络 120 在任意时间利用 SK 加密 PEK_z，并将加密的 PEK_z 发送到 PPV 终端 310，从而更新 PEK。在步骤 303 中，网络 120 更新 TEK。也就是说，网络 120 利用 SEK_y 加密 PEK_z，利用 PEK_z 加密 TEK_{x+1}，并将加密的密钥发送到 PPV 终端 310。其后，在 PEK_z 的使用寿命期间，网络 120 利用 PEK_z 加密 TEK，以依次更新 TEK。在 PEK_z 的使用寿命期满之后，在步骤 305 中，网络 120 更新下一个 PEK(PEK_{z+1})。也就是说，网络 120 利用 SK 加密 PEK_{z+1} 并将加密的 PEK_{z+1} 发送到 PPV 终端 310。因此，利用 PEK_{z+1} 加密 TEK 以更新 TEK，直到 PEK_{z+1} 309 的使用寿命期满。在步骤 307 中，利用 PEK_{z+m} 更新第 n 个 TEK(TEK_{x+n})。

发明内容

[0019] 技术问题

[0020] 如参考图 1 到 3 所述，由于网络利用 TEK 加密内容数据，并且终端利用该 TEK 解密所加密的数据，因此网络应当更新各种加密密钥若干次，并且将更新的 TEK 发送到终端。在这种情况下，为了更新加密密钥而在网络和终端之间消耗的资源可能会增加。

[0021] 因此，需要一种当更新加密密钥时降低网络中的资源的方法和装置。

[0022] 技术方案

[0023] 本发明的一方面解决至少以上问题和 / 或缺点并且提供至少下述优点。因此，本发明的一方面是提供一种在通信系统中降低用于创建广播服务数据的加密密钥和将加密密钥发送到终端的资源数量的方法和装置。

[0024] 本发明的另一方面是提供一种在通信系统中降低网络需要用来将广播服务数据的加密密钥发送到终端的资源的方法和装置。

[0025] 本发明的另一方面是提供一种在通信系统中终端从网络接收广播服务数据的加密密钥以创建业务加密密钥 (TEK) 并且利用 TEK 解密所接收的加密的数据的方法和装置。

[0026] 根据本发明的一方面，提供一种在通信系统中用于提供广播服务的方法。该方法包括 ：创建第一密钥和第二密钥的种子密钥对 ；将种子密钥对发送到将为其提供广播服务的终端 ；使用该种子密钥对创建特定数目的加密密钥，该特定数目对应于种子密钥对的使用寿命 ；在该使用寿命内，使用该加密密钥来加密广播服务数据 ；以及广播所加密的广播服务数据。

[0027] 根据本发明的另一方面，提供一种在通信系统中由终端接收广播服务的方法。该方法包括 ：接收第一密钥和第二密钥的种子密钥对 ；使用接收的种子密钥对创建特定数目的加密密钥，该特定数目对应于种子密钥对的使用寿命 ；在该使用寿命内，使用该加密密钥来解密所广播的加密的广播服务数据。

[0028] 根据本发明的又一方面，提供一种在通信系统中用于提供广播服务的装置。该装置包括 ：种子密钥创建器，用于创建包括第一密钥和第二密钥的种子密钥对，以及用于通过收发器将种子密钥对发送到为其提供广播服务的终端 ；加密密钥创建器，用于使用该种子密钥对创建特定数目的加密密钥，该特定数目对应于种子密钥对的使用寿命 ；和数据加密器，用于在该使用寿命内，使用该加密密钥来加密广播服务数据，以及用于通过该收发器广播所加密的广播服务数据。

[0029] 根据本发明的另一方面，提供一种在通信系统的终端中用于接收广播服务的装置。该装置包括 ：收发器，用于接收包括第一密钥和第二密钥的种子密钥对 ；加密密钥创建器，用于使用接收的种子密钥对创建特定数目的加密密钥，该特定数目对应于种子密钥对的使用寿命 ；和数据解密器，用于使用该加密密钥来解密在该使用寿命内广播的加密的广播服务数据。

[0030] 根据本发明的另一方面，提供一种在开放移动联盟广播 (OMA BCAST) 中用于提供广播服务的装置。该装置包括 ：服务保护密钥分发单元 (SP-KD)，用于创建包括第一密钥和第二密钥的种子密钥对，以及用于将该种子密钥对发送到为其提供广播服务的终端 ；和服务提供商加密单元 (SP-E)，用于从该 SP-KD 接收种子密钥对，用于创建特定数目的加密密钥，其数目对应于接收的种子密钥对的使用寿命，用于在该使用寿命内，使用加密密钥来加密广播服务数据，以及用于将加密的广播服务数据发送到终端。

[0031] 通过以下结合附图、公开了本发明的示范性实施例的详细描述，本发明的其它方面、优点和显著的特征对于本领域技术人员将变得明显。

附图说明

[0032] 通过下面结合附图的详细描述，本发明的某些示范性实施例的上述及其它方面、

特征和优点将更加明显，其中：

[0033] 图 1 示出了在传统广播服务系统中网络和终端之间的加密密钥管理；

[0034] 图 2 示出了在传统开放移动联盟广播 (OMA BCAST) 中登记的终端中的加密密钥管理；

[0035] 图 3 示出了在传统的 OMA BCAST 中按观看次数计费 (PPV) 终端中的加密密钥管理；

[0036] 图 4 示出了根据本发明的示范性实施例的广播服务系统中的加密密钥的创建；

[0037] 图 5 是示出了根据本发明的示范性实施例的广播服务系统中的网络的加密密钥管理方法；

[0038] 图 6 是示出了根据本发明的示范性实施例的广播服务系统中的终端的加密密钥管理方法；

[0039] 图 7 示出了根据本发明的示范性实施例的应用于 OMA BCAST 中的登记的终端的示范性加密密钥管理；

[0040] 图 8 示出了根据本发明的示范性实施例的应用于 OMA BCAST 中的 PPV 终端的示范性加密密钥管理；

[0041] 图 9 示出了根据本发明的示范性实施例的 OMA BCAST 中的在用于登记的终端的加密密钥管理中的每个实体的操作；

[0042] 图 10 示出了根据本发明的示范性实施例的在 OMA BCAST 中的按观看次数计费 (PPV) 终端的加密密钥管理中的每个实体的操作；

[0043] 图 11 示出了根据本发明的示范性实施例的在微波全球互联接入 (WiMax) 广播服务系统中的登记的终端的加密密钥管理；

[0044] 图 12 示出了根据本发明的示范性实施例的 WiMax 广播系统中的 PPV 终端的加密密钥管理；

[0045] 图 13 是示出了根据本发明的示范性实施例的广播服务系统中的用于管理加密密钥的网络装置；以及

[0046] 图 14 示出了根据本发明的示范性实施例的广播服务系统中的终端的加密密钥管理装置。

[0047] 贯穿全部附图，相同的附图参考数字将被理解为指代相同的元件、特征和结构。

具体实施方式

[0048] 提供参考附图的以下描述以帮助全面地理解由权利要求书和它们的等效物定义的本发明的示范性实施例。它包括各种细节来帮助理解，但是这些将被认为仅仅是示范性的。因此，本领域普通技术人员将认识到，可以在不脱离本发明的范围和精神的情况下，对这里描述的实施例做出各种变化和修改。此外，为了清楚和简明，省略了公知的功能和结构的描述。

[0049] 以下说明书和权利要求书中使用的术语和词语不局限于书面意义，而是仅仅被发明人使用来使得能够清楚且一致地理解本发明。因此，本领域技术人员显然可知，本发明的示范性实施例的以下说明仅仅是为了示例的目的提供，而不是为了限制由所附的权利要求书和它们的等效物定义的本发明。

[0050] 将理解，单数形式的“一”、“一个”和“该”包括多个涉及的对象，除非上下文明确指示。因而，例如，“一个组件表面”的指示包括一个或多个这样的表面的指示。

[0051] 以下，将简要地描述本发明的示范性实施例的基本构思。在本发明的示范性实施例中，提供广播服务的网络创建用于创建业务加密密钥 (TEK) 的种子密钥对并将该种子密钥对发送到终端。当使用种子密钥对时，网络和终端各自创建特定数目 n 的 TEK，其中 n 对应于种子密钥对的使用寿命。网络利用 n 个 TEK 加密数据，并且将数据发送到终端特定数目 n 次。终端还利用由终端本身创建的 n 个 TEK 来解密所发送的加密的数据。

[0052] 当随着所有的 n 个 TEK 都被使用而数据的发送 / 接收完成时，种子密钥对的使用寿命期满，并且网络创建下一个加密密钥对并将加密密钥对发送到终端。但是，如果终端是已经请求了特定的节目的按观看次数计费 (PPV) 终端，则该终端根据该特定的节目的广播时间来设置种子密钥对的使用寿命。因此，不需要再更新种子密钥对。网络可以是基站或控制基站的服务器，或者在提供广播服务的无线通信系统中提供广播服务的服务提供商的服务器。

[0053] 由本发明的示范性实施例提出的广播服务方法和装置可以应用于无线通信系统和有线通信系统中的广播服务。

[0054] 下面将基于上述基本构思来描述 TEK 的创建。

[0055] 图 4 示出了根据本发明的示范性实施例的广播服务系统中的加密密钥的创建。

[0056] 参考图 4，在步骤 401 中，创建加密密钥对，称为密钥种子对 (KSP)。KSP 包括两个密钥。也就是说，KSP 包括 KS_1 和 KS_2。KSP 在网络中可以被随机创建。

[0057] 其后，在步骤 403 和 405 中，哈希链分别应用于 KS_1 和 KS_2。也就是说，在步骤 403 中，正向哈希链应用于 KS_1，并且在步骤 405 中，反向哈希链应用于 KS_2。步骤 403 和 405 可以被同时执行或有时间差地执行。即使有时间差，步骤 403 和 405 的任何一个也都可以被首先执行。

[0058] 更具体地说，在步骤 403 中，通过将哈希函数应用于 KS_1 来确定 S_1，并且通过将哈希函数应用于 S_1 来获得 S_2。按类似方式执行直到 S_n 的确定。

[0059] 与正向哈希链相比，步骤 405 中的反向哈希链在相反方向上进行。也就是说，通过将哈希函数应用于 KS_2 首先获得 M_n，通过将哈希函数应用于 M_n 来确定 M_{n1}。以这样的方式，通过将哈希函数应用于 M_2 来确定直到 M_1。当完全执行步骤 403 和 405 时，可以创建 n(S_i，M_i) 对，其被定义为“双向哈希对 (BHP)”。

[0060] 在步骤 407 中，通过将特定操作应用于步骤 403 和 405 中确定的 n 个 BHP 来获得 n 个 TEK。使用的操作可以是异或 (XOR) 操作。也就是说，可以利用等式 $TEK_i = S_i \text{ XOR } M_i$ 获得 TEK。

[0061] 简言之，首先创建一个 $KSP(KS_1, KS_2)$，利用 KSP 产生 n 个 $BHP(S_i, M_i)$，并且利用 n 个 $BHP(S_i, M_i)$ 创建 n 个 TEK。创建 TEK 的过程可以在网络和 / 或终端中执行。

[0062] 如果终端是登记的终端，则网络发送 KSP，并且网络和终端使用上述方法确定 n 个 TEK。其后，网络可以加密数据，并且终端可以解密所加密的数据。

[0063] 但是，如果终端是 PPV 终端，则网络可以示出微小的差别，而不用 KSP。也就是说，网络未获得 KSP，但是获得接入有效对 (AVP)。其后，网络将 AVP 发送到 PPV 终端。“AVP”是指与向 PPV 终端提供广播服务的特定时间段对应的 (S_i, M_j) 信息对。PPV 终端通过将正向哈

希链应用于 S_i来获得直到 S_j的值，并通过将反向哈希链应用于 M_j来获得直到 M_i的值。也就是说，PPV 终端由 AVP 创建 m 个 BHP。如果在 PPV 终端中创建的 BHP 的数目是 m，则 m = ji+1。总之，PPV 终端使用 m 个 BHP 获得 m 个 TEK。

[0064] 简言之，从网络发送到登记的终端的加密密钥对是 KSP = (KS_1, KS_2)，并且发送到 PPV 终端的加密密钥对是 AVP = (S_i, M_j)。尽管 KSP 和 AVP 二者在名称方面不同，但是 KSP 和 AVP 实质上是相等的，因为它们是与向终端提供的广播服务的时间段期间的数据加密有关的信息。也就是说，如果与广播服务的参考时间段的开始时间时的数据加密有关的信息是 KS_1并且与结束时间时的数据加密有关的信息是 KS_2，则 S_i可以指示与属于该参考时间段的任意时间段中的开始时间时的数据加密有关的信息，和 M_j可以指示与任意时间段中的结束时间时的数据加密有关的信息。

[0065] 例如，如果用户可以逐月购买用于广播服务的定购券，则购买一个月的定购券的用户的终端可以被认为是登记的终端。当前被发送到登记的终端的 KSP，即 (KS_1,KS_2)，可以分别指示与一个月的开始时间和结束时间时的数据加密有关的信息。如果用户购买了用于单个剧目的定购券，则该用户的终端变为 PPV 终端，并且此时被发送到 PPV 终端的 AVP，即 (S_i, M_j)，可以分别指示与该剧目的开始时间和结束时间时的数据加密有关的信息。

[0066] 在上面的描述中，KSP 信息成对地用于登记的终端。但是，在一些情况下，对于登记的终端可以使用 KSP 信息中的一个，即 KS_1和 KS_2中的一个，而不是该信息对。由于信息条的数目不是二，因此不必用下标来标识信息。因此，信息可以简单地被命名为“KS”。KS 可以是与登记的终端的订购时段的开始时间或结束时间时的数据加密有关的信息。也就是说，当确定将反向哈希链应用于 KS 时，KS 可以指示与广播服务的结束时间时的数据加密有关的信息。如果确定将正向哈希链应用于 KS，则 KS 可以变为与广播服务的开始时间时的数据加密有关的信息。

[0067] 反向哈希链可以按照下面的方式应用于 KS。

[0068] 网络创建 KS 并将 KS 传送给登记的终端。在这种情况下，也可以一起发送与 KS 有关的其它参数（例如，TEK 的数目、TEK 的使用寿命等）。

[0069] 为了创建 n 个 TEK，在反方向上向 KS 应用哈希函数 n 次。也就是说，TEK 如下创建：

[0070] TEK_n= hash(KS)，TEK_{n1}= hash(TEK_n)，TEK_2= hash(TEK_3)...，TEK_1= hash(TEK_2)

[0071] 另外，KSP 或 AVP 可以与传统的 SEK 或 PEK 组合。例如，在 OMA BCAST 中，可以通过 SEK 和 PEK 加密 KSP 或 AVP，并传送到终端。TEK 可以在网络和终端中由 KSP 或 AVP 创建，如上所述。

[0072] 将分别参考图 5 和 6 描述网络和终端的本发明的示范性实施例的加密密钥管理方法。

[0073] 图 5 是示出了根据本发明的示范性实施例的广播服务系统中的网络的加密密钥管理方法。

[0074] 参考图 5，在步骤 501 中，网络从终端接收登记消息。“登记消息”是指包括终端为了从网络接收服务或节目而使用的终端登记信息的消息。在步骤 503 中，网络基于登记消息确定终端是登记的终端还是 PPV 终端。

[0075] 可以用各种方式来执行确定终端是登记的终端还是 PPV 终端。例如，从终端向网

络发送的登记消息可以包括指示终端是登记的终端还是 PPV 终端的单独的标识符，或者网络可以由连接到该网络的验证服务器（未示出）允许询问终端是登记的终端还是 PPV 终端。

[0076] 如果终端是登记的终端，则网络进行到步骤 505，并且如果终端是 PPV 终端，则进行到步骤 507。在步骤 505 中，网络向终端更新（即，创建和发送）KSP。

[0077] 在步骤 507 中，网络更新 AVP。也就是说，在步骤 507 中，网络创建 AVP 并将 AVP 发送到 PPV 终端。其后，在步骤 509 中，网络通过将正向和反向哈希链应用于 KSP 或 AVP 来创建 TEK。如果终端是登记的终端，则网络将使用 KSP 创建 n 个 TEK，并且如果终端是 PPV 终端，则使用 AVP 创建 m 个 TEK。在步骤 511 中，网络使用 TEK 加密数据并将加密的数据发送到终端。在步骤 513 中，网络确定 TEK 是使用 KSP 还是 AVP 创建的，并且根据结果经历不同的过程。也就是说，如果当前 TEK 是使用 KSP 创建的，则网络在步骤 515 中确定 KSP 的使用寿命是否已经期满。如果 KSP 的使用寿命已经期满，则网络返回到步骤 505 并且更新下一个 KSP。如果 KSP 的使用寿命没有期满，则网络返回到步骤 511，其中它使用下一个 TEK 加密数据并发送加密的数据。但是，如果当前 TEK 是使用 AVP 创建的，则网络在步骤 517 中确定 AVP 的使用寿命是否已经期满。如果 AVP 的使用寿命没有期满，则网络返回到步骤 511，其中它使用下一个 TEK 加密数据并发送加密的数据。但是，如果 AVP 的使用寿命已经期满，则由于不必再更新 AVP，因此网络结束所有过程。

[0078] 图 6 是示出了根据本发明的示范性实施例的广播服务系统中的终端的加密密钥管理方法。

[0079] 参考图 6，在步骤 601 中，终端向网络发送登记消息，并在步骤 603 中从网络接收更新的 KSP 或 AVP。也就是说，如果是登记的终端，则终端接收 KSP，并且如果是 PPV 终端，则接收 AVP。在步骤 605 中，终端使用 KSP 或 AVP 创建 TEK。在步骤 607 中，终端从网络接收加密的数据。在步骤 609 中，终端使用 TEK 解密所加密的数据。下面的操作根据 TEK 是使用 KSP 还是 AVP 创建的而有所不同。

[0080] 如果 TEK 是使用 KSP 创建的，换言之，如果终端是登记的终端，则终端进行到步骤 613。如果在步骤 613 中确定 KSP 的使用寿命已经期满，则终端返回到步骤 603 并且接收更新的 KSP。但是，如果 KSP 的使用寿命没有期满，则终端返回到步骤 609，并且利用使用当前 KSP 创建的下一个 TEK 来解密所加密的数据。

[0081] 但是，如果在步骤 611 中 TEK 是利用 AVP 创建的，换言之，如果终端是 PPV 终端，则终端进行到步骤 615。如果在步骤 615 中确定 AVP 的使用寿命没有期满，则终端返回到步骤 609 并且利用 TEK 连续地解密所加密的数据。但是，如果 AVP 的使用寿命已经期满，则由于终端已经解密了所有接收到的加密的数据，因此它终止而不执行任何操作。

[0082] 参考图 7 到 12，现在将描述参考图 4 到 6 描述的本发明的示范性实施例应用于不同的广播系统。图 7 到 10 示出了 OMA BCAST 中的登记的终端和 PPV 终端的可能的示例，图 11 和 12 示出了可应用于微波全球互联接入 (WiMax) 广播服务系统中的登记的终端和 PPV 终端的示例。

[0083] 图 7 示出了根据本发明的示范性实施例的应用于 OMA BCAST 中的登记的终端的示范性加密密钥管理。

[0084] 参考图 7，在步骤 701 中，网络 720 对于任意的呼叫更新 KSP(KSP_y)。也就是说，网

络 720 利用安全密钥 (SK) 加密 KS_1 和 KS_2，并将 KS_1 和 KS_2 发送到登记的终端 710。网络 720 利用 KSP 创建 n 个 BHP，由 BHP 创建 n 个 TEK，使用 n 个 TEK 加密数据，并将加密的数据发送到登记的终端 710。

[0085] 登记的终端 710 用和网络 720 一样的方法利用 KSP 创建 TEK，并解密从网络 720 接收到的加密的数据。如果因为使用了所有 n 个 TEK 而使得数据发送 / 接收完成，则 KSP_y 的使用寿命期满 705。因此，网络 720 在步骤 703 中更新下一个 KSP，KSP_{y+1}。

[0086] 图 8 示出了根据本发明的示范性实施例的应用于 OMA BCAST 中的 PPV 终端的示范性加密密钥管理。

[0087] 参考图 8，如果 PPV 终端 810 已经购买了可用于特定的接入时间段的广播服务，则在步骤 801 中，网络 820 更新 (即，创建并发送)AVP 到 PPV 终端 810。也就是说，网络 820 使用 SK 加密 (S_i, M_j) 对，并将结果发送到 PPV 终端 810。

[0088] PPV 终端 810 的以下操作与上面描述的 PPV 终端相似。也就是说，PPV 站 810 将正向和反向哈希链应用于接收的 (S_i, M_j) 对。然后，确定 $S = \{S_i, S_{i+1}, S_{i+2}, \ldots S_{j1}, S_j\}$ 和 $M = \{M_{j1}, M_{j2}, \ldots, M_{i+1}, M_i\}$ 的值。其后，PPV 终端 810 可以通过对确定的值执行 XOR 操作来获得 m 个 TEK，即 $TEK_i \sim TEK_j$。在这种情况下，$m = ji+1$。也就是说，m 的值可以由 (S_i, M_j) 确定。这里，(S_i, M_j) 的使用寿命 = m(TEK 的使用寿命)，并且 m 小于或等于 n(mn)，因为 n 指示 TEK 的数目，其对应于 KSP 的使用寿命，并且 m 指示 TEK 的数目，其对应于 AVP 805 的使用寿命。

[0089] 如果接入时间段 802 已经期满并且用户已经购买了可用于附加的接入时间段的广播服务，则在步骤 803 中，网络 820 更新新的 AVP 并将 AVP 发送到 PPV 终端 810。在步骤 804 中，PPV 终端 810 可接收对于新的接入时间段的广播服务。

[0090] 图 9 示出了根据本发明的示范性实施例的 OMA BCAST 中的在用于登记的终端的加密密钥管理中的每个实体的操作。

[0091] 图 7 的描述已被给定为具有两个实体，诸如登记的终端和网络。但是，网络可以由 OMA BCAST 中的多个实体组成。图 9 示出了构成网络的终端和实体之间的呼叫流。

[0092] 将首先描述 OMA BCAST 系统的实体，其可以共同应用于图 9 和 10。服务保护管理单元 (SP-M)930(或 1030) 具有登记和管理终端的功能。服务保护密钥分发单元 (SP-KD)940(或 1040) 创建 KSP 或 AVP，并将 KSP 或 AVP 传送到终端。此外，服务提供商加密单元 (SP-E)950(或 1050) 具有使用从 SP-KD 940(或 1040) 提供的 KSP 或 AVP 创建 TEK(多个 TEK)、利用 TEK 加密数据、以及将加密的数据直接发送到终端的功能。

[0093] 参考图 9，在步骤 901 中，登记的终端 960 向 SPM 930 发送登记消息。登记消息包括登记的终端 960 期望接收的广播服务的服务 ID(例如，001)。在步骤 903 中，SPM 930 与登记的终端 960 建立 SK。也就是说，SPM 930 通过交换必需的信息来建立与登记的终端 960 相同的 SK，以便与登记的终端 960 共享 SK。在步骤 905 中，SPM 930 向 SPKD 940 传送 SK。在步骤 907 中，SPKD 940 通过创建第一 KSP(KSP_1) 并将其传送到登记的终端 960，来更新用于登记的终端 960 的 KSP。在步骤 909 中，SPKD 940 向 SPE 950 传送 KSP_1。在步骤 911 中，SPE 950 使用 KSP_1 创建 n 个 TEK，利用创建的 n 个 TEK 中的一个 (由 TEK_x 指示) 来加密广播数据，并将加密的数据发送到登记的终端 960。在步骤 913 中，将利用创建的第 n 个 TEK 加密的数据发送到登记的终端 960。由于创建的 n 个 TEK 全部已被用于步骤 913 中，因此

KSP_1的使用寿命已经期满。因此，在步骤 915 中，SPKD 940 向登记的终端 960 更新（即，创建并发送）第二 KSP(KSP_2)。后续的过程与 KSP_1被更新之后的过程相同。

[0094] 图 10 示出了根据本发明的示范性实施例的在 OMA BCAST 中的 PPV 终端的加密密钥管理中的每个实体的操作。

[0095] 图 10 的描述将集中于与图 9 的差别。在图 10 的示例中，终端是 PPV 终端 1060。因此，在步骤 1001 中，PPV 终端 1060 发送的登记消息包括节目 ID（例如，002），其指示 PPV 终端 1060 需要特定的广播节目。在步骤 1007 中，SPKD 1040 更新 AVP_1并将 AVP_1发送到 PPV 终端 1060。在步骤 1013 中，SPE 1050 使用第 m 个 TEK(TEK_{x+m}) 加密数据，并将加密的数据发送到 PPV 终端 1060。在 AVP_1的使用寿命期满之后，不自动更新下一个 AVP_2。代替地，当用户另外请求特定的时间段的广播服务时，更新 AVP_2。图 10 的其它操作（即，SK 建立 1003、SK 传送 1005、AVP_1传送 1009 和发送加密的数据 1011）与图 9 的操作（即，SK 建立 903、SK 传送 905、KSP_1传送 909 和发送加密的数据 1011）相似。

[0096] 图 11 示出了根据本发明的示范性实施例的 WiMax 广播服务系统中的登记的终端的加密密钥管理。在 WiMax 广播服务系统中，加密密钥不是像在 OMA BCAST 中那样由多个实体管理，而是由一个多播和广播服务 (MCBCS) 服务器管理。

[0097] 参考图 11，当在步骤 1101 中登记的终端 1120 进行订购从 MCBCS 服务器 1130 提供的广播服务的过程时，在步骤 1103 中，MCBCS 服务器 1130 更新第一 KSP(KSP_1) 并将 KSP_1发送到登记的终端 1120。同时，MCBCS 服务器 1130 和登记的终端 1120 各自创建 n 个 TEK。在步骤 1105 中，MCBCS 服务器 1130 使用创建的 n 个 TEK 加密数据，并将加密的数据发送到登记的终端 1120。当因为 n 个 TEK 全部都被使用而使得 KSP_1的使用寿命期满时，在步骤 1107 中，MCBCS 服务器 1130 更新第二 KSP(KSP_2)，并将 KSP_2发送到登记的终端 1120。同时，MCBCS 服务器 1130 和登记的终端 1120 各自使用 KSP_2创建 n 个 TEK。在步骤 1109 中，将利用创建的 n 个 TEK 加密的数据发送到登记的终端 1120。

[0098] 图 12 示出了根据本发明的示范性实施例的 WiMax 广播系统中的 PPV 终端的加密密钥管理。

[0099] 图 12 的描述将集中在与图 11 的差别。在步骤 1201 中，PPV 终端 1220 购买它将接入 MCBCS 服务器 1230 以接收特定时间段的广播服务的接入时间。在步骤 1203 中，更新与特定时间段对应的 AVP_1。此外，MCBCS 服务器 1230 和 PPV 终端 1220 各自使用 AVP_1创建 TEK。在步骤 1205 中，将由利用 AVP_1创建的 TEK 加密的数据从 MCBCS 服务器 1230 发送到 PPV 终端 1220。这里，在 AVP_1的使用寿命期满后，不自动更新 AVP_2。也就是说，当在步骤 1207 中 PPV 终端 1220 购买更多的接入时间用于特定的广播服务时，在步骤 1209 中，MCBCS 服务器 1230 创建 AVP_2，并将 AVP_2发送到 PPV 终端 1220。图 12 的另一个操作（即，将利用创建的 n 个 TEK 加密的数据发送到登记的终端 1211）与图 11 的操作（即，将利用创建的 n 个 TEK 加密的数据发送到登记的终端 1120）相似。

[0100] 图 13 是示出了根据本发明的示范性实施例的广播服务系统中的用于管理加密密钥的网络装置。

[0101] 收发器 1301 从终端接收包括终端的登记信息的登记消息，并将登记消息提供给控制器 1303。控制器 1303 基于包括在接收的登记消息中的登记信息，确定终端是登记的终端还是 PPV 终端，并根据确定结果控制加密密钥管理器 1305 中的种子密钥创建器 1306。

[0102] 加密密钥管理器 1305 在控制器 1303 的控制下，创建适合于该类型终端的种子密钥，并使用创建的种子密钥来创建加密密钥，即 TEK。更具体地说，加密密钥管理器 1305 包括种子密钥创建器 1306 和加密密钥创建器 1307。种子密钥创建器 1306 创建适合于该类型终端的种子密钥。也就是说，如果终端是登记的终端，则种子密钥创建器 1306 创建 KSP，并且如果终端是 PPV 终端，则创建 AVP。将创建的 KSP 或 AVP 提供给收发器 1301 和加密密钥创建器 1307。将提供给收发器 1301 的 KSP 或 AVP 发送到终端，经历更新。终端使用更新的 KSP 或 AVP 创建 TEK。

[0103] 同时，已经接收了 KSP 或 AVP 的加密密钥创建器 1307 创建与对应于 KSP 或 AVP 的使用寿命的数目一样多的 TEK。也就是说，当终端是登记的终端时，加密密钥创建器 1307 将使用 KSP 创建 n 个 TEK，并且当终端是 PPV 终端时，使用 AVP 创建 m 个 TEK。在由 KSP 或 AVP 创建 TEK 时，可以如参考图 4 所述的那样来使用正向和反向哈希链。

[0104] 将 TEK 从加密密钥创建器 1307 提供给数据加密器 1309，并且数据加密器 1309 利用 TEK 加密数据，并通过收发器 1301 将加密的数据发送到终端。

[0105] 图 14 示出了根据本发明的示范性实施例的广播服务系统中的终端的加密密钥管理装置。

[0106] 控制器 1403 创建包括终端的登记信息的登记消息，并通过收发器 1401 将登记消息发送到网络。此外，控制器 1403 响应于登记消息通过收发器 1401 从网络接收种子密钥，即 KSP 或 AVP，并将 KSP 或 AVP 提供给加密密钥创建器 1405。加密密钥创建器 1405 更新提供的 KSP 或 AVP，创建与对应于更新的 KSP 或 AVP 的使用寿命的数目一样多的 TEK，并将 TEK 提供给数据解密器 1407。

[0107] 同时，在从网络接收到加密的数据后，收发器 1401 将接收的加密数据转发给数据解密器 1407。数据解密器 1407 使用从加密密钥创建器 1405 提供的 TEK 解密所加密的数据。数据解密之后的操作不应用于本发明的示范性实施例。

[0108] 从上面的描述显然可知，网络可以在特定时间创建特定的加密密钥并将其发送到终端，而不是每当网络将广播服务数据发送到终端时创建各种加密密钥并将其发送到终端。从而，降低了网络的复杂度。以这样的方式，降低了创建加密密钥并将其发送到终端的数目，从而使得可以有效利用通信资源。此外，终端可以通过在特定时间接收加密密钥而独自创建 TEK，并使用创建的 TEK 解密接收的加密数据，从而有助于增加终端的结构效率。

[0109] 本本发明的示范性实施例也可以被具体化为计算机可读记录介质上的计算机可读代码。计算机可读记录介质是可以储存其后可以被计算机系统读取的数据的任何数据存储设备。计算机可读记录介质的示例包括只读存储器 (ROM)、随机存取存储器 (RAM)、CD-ROM、磁带、软盘、光数据存储器件和载波（诸如经由有线或无线传输路径通过互联网的数据传输），而不限于此。计算机可读记录介质也可以被分布在网络耦合的计算机系统之上以使得计算机可读代码以分布式被存储和执行。此外，用于实现本发明的功能性程序、代码和代码段可被本发明所属领域的程序员容易地构造，而落入本发明的范围。

[0110] 尽管已经参考本发明的特定示范性的实施例和附图对本发明进行了示出和描述，但是本领域技术人员应当理解，在不脱离由所附权利要求书和它们的等效物所定义的本发明的精神和范围的情况下，可以对本发明做出形式和细节上的各种修改。

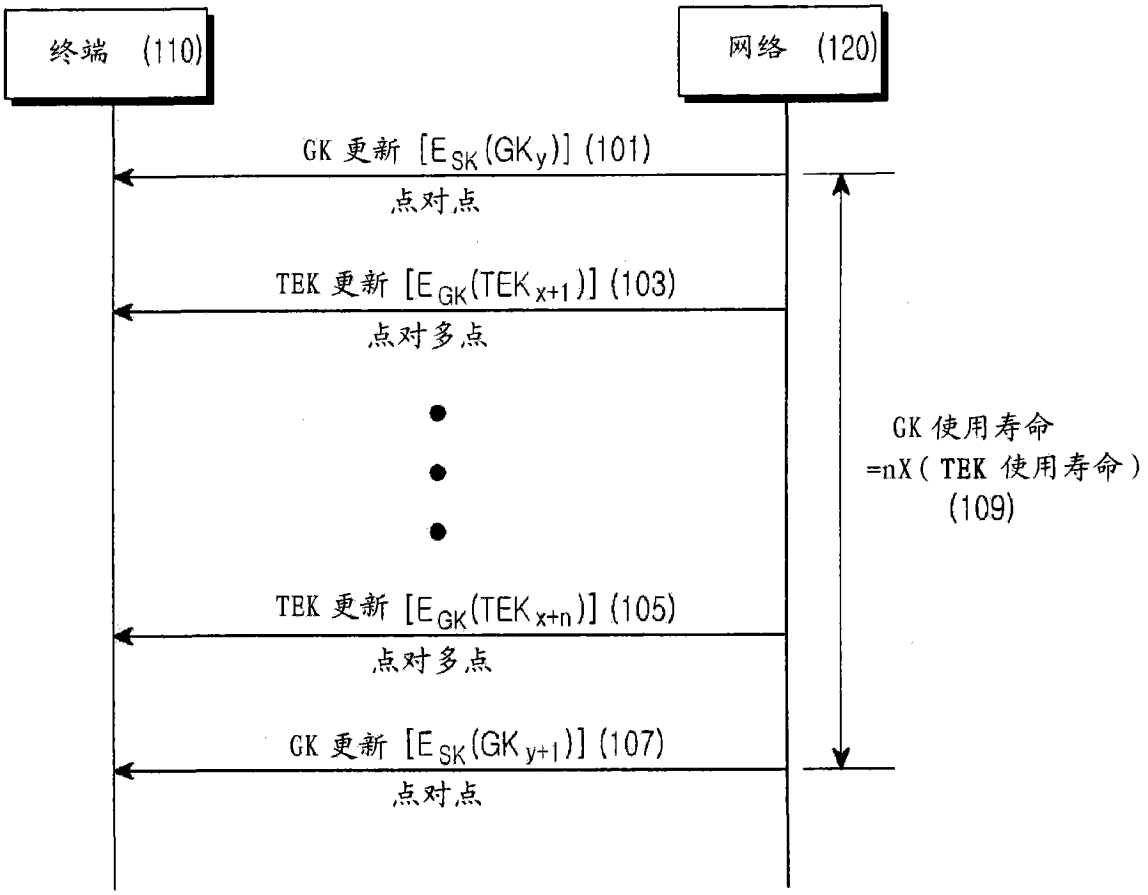

终端 (110)
网络 (120)
GK 更新 [$E_{SK}(GK_y)$] (101)
点对点
TEK 更新 [$E_{GK}(TEK_{x+1})$] (103)
点对多点
TEK 更新 [$E_{GK}(TEK_{x+n})$] (105)
点对多点
GK 更新 [$E_{SK}(GK_{y+1})$] (107)
点对点
GK 使用寿命
=nX(TEK 使用寿命)
(109)

图 1

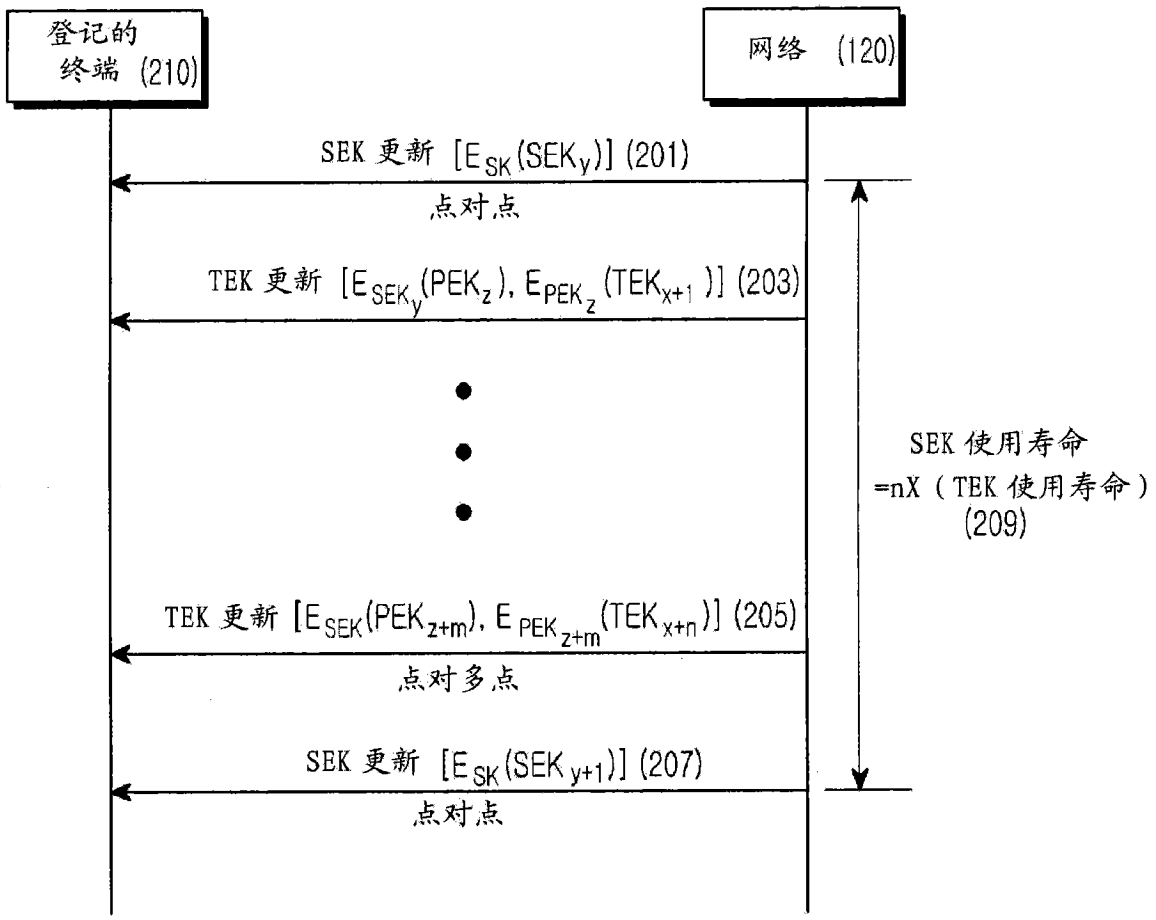

登记的
终端 (210)
网络 (120)
SEK 更新 [E SK(SEK y)] (201)
点对点
TEK 更新 [E SEK y(PEK z), E PEK z(TEK x+1)] (203)
SEK 使用寿命
=nX（TEK 使用寿命）
(209)
TEK 更新 [E SEK(PEK z+m), E PEK z+m(TEK x+n)] (205)
点对多点
SEK 更新 [E SK(SEK y+1)] (207)
点对点

图 2

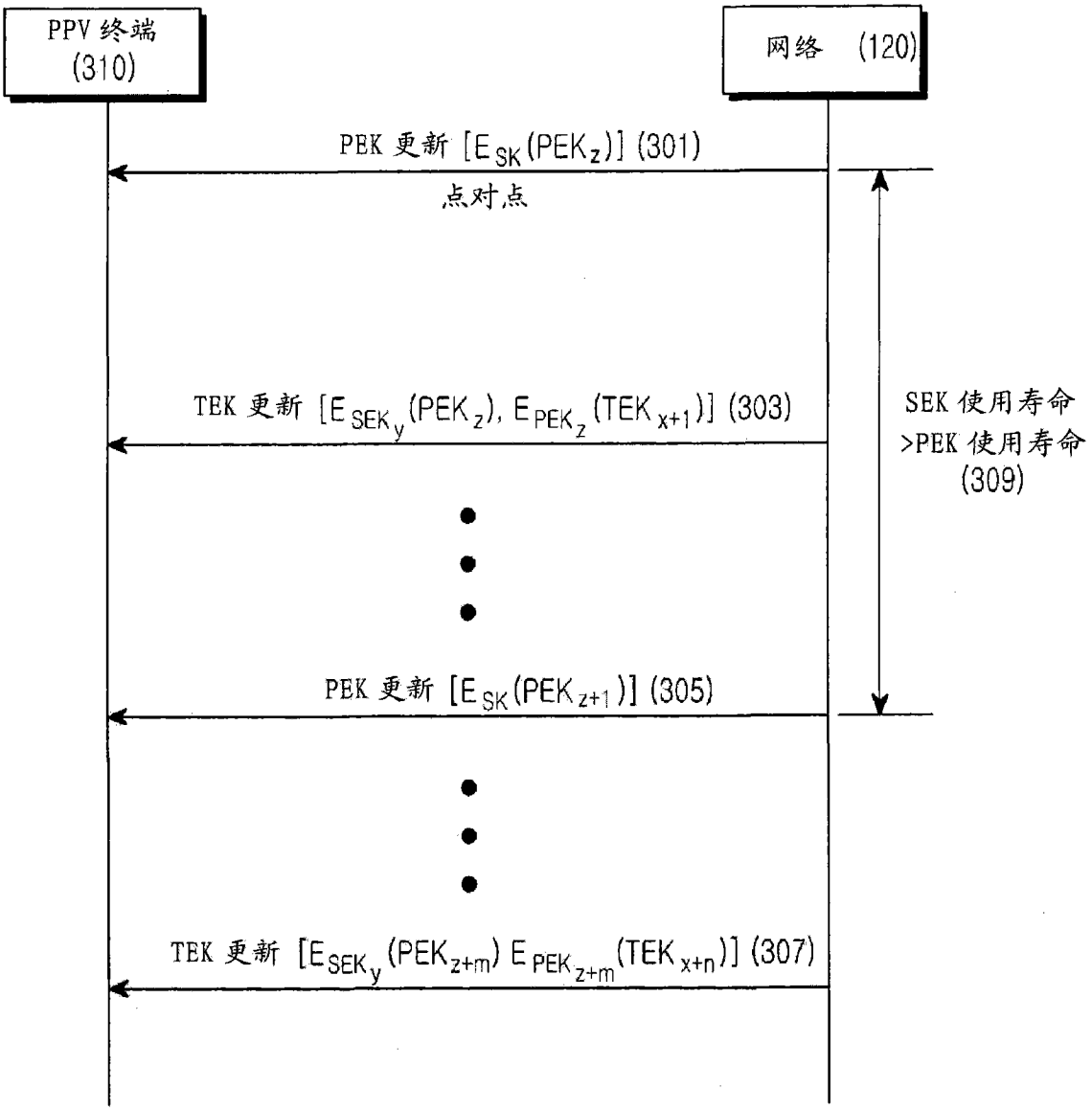

PPV 终端
(310)
网络 (120)
PEK 更新 [E SK(PEK z)] (301)
点对点
TEK 更新 [E SEK y(PEK z), E PEK z(TEK x+1)] (303)
SEK 使用寿命
>PEK 使用寿命
(309)
PEK 更新 [E SK(PEK z+1)] (305)
TEK 更新 [E SEK y(PEK z+m) E PEK z+m(TEK x+n)] (307)

图 3

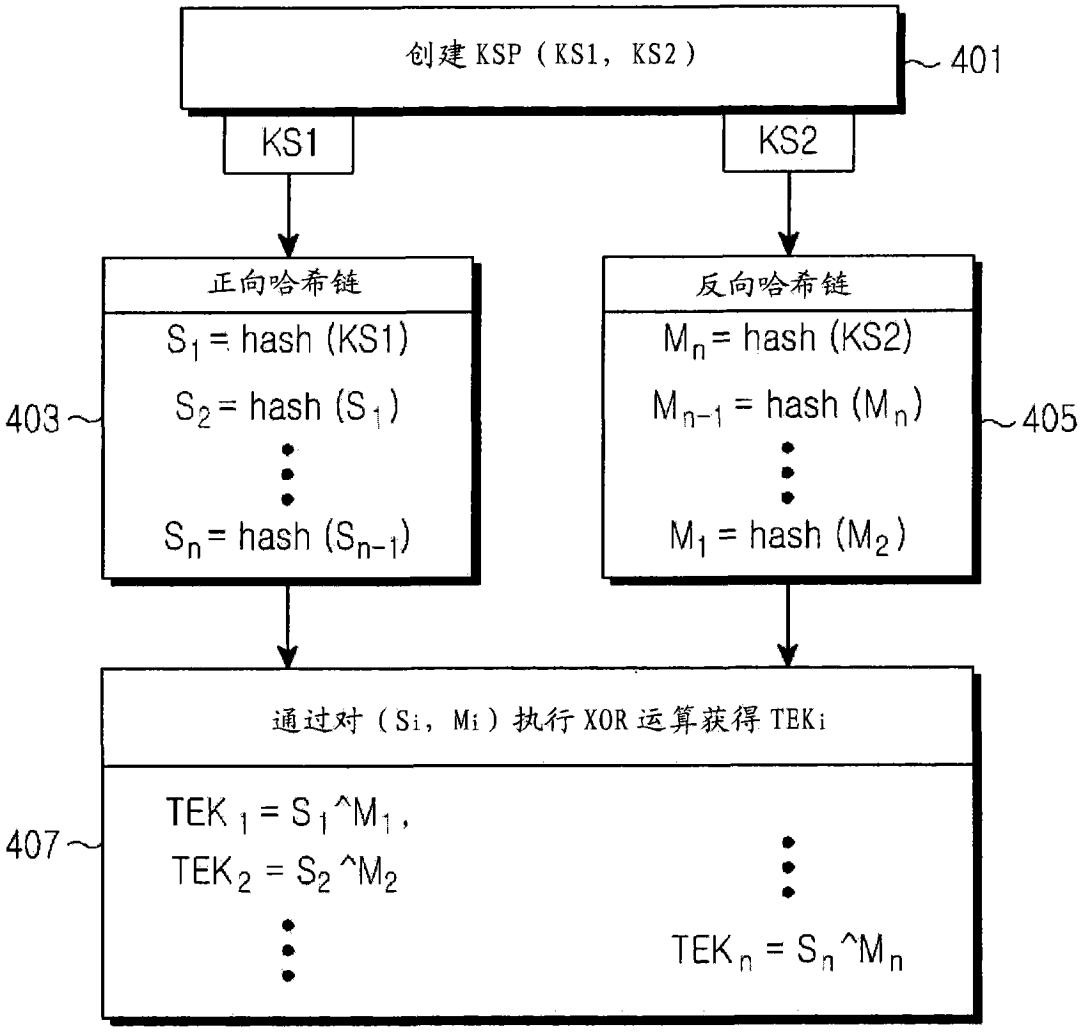

创建 KSP（KS1，KS2）
401
KS1
KS2
正向哈希链
S_1 = hash (KS1)
S_2 = hash (S_1)
S_n = hash (S_{n-1})
403
反向哈希链
M_n = hash (KS2)
M_{n-1} = hash (M_n)
M_1 = hash (M_2)
405
通过对（Si，Mi）执行 XOR 运算获得 TEKi
$TEK_1 = S_1 \hat{} M_1$，
$TEK_2 = S_2 \hat{} M_2$
$TEK_n = S_n \hat{} M_n$
407

图 4

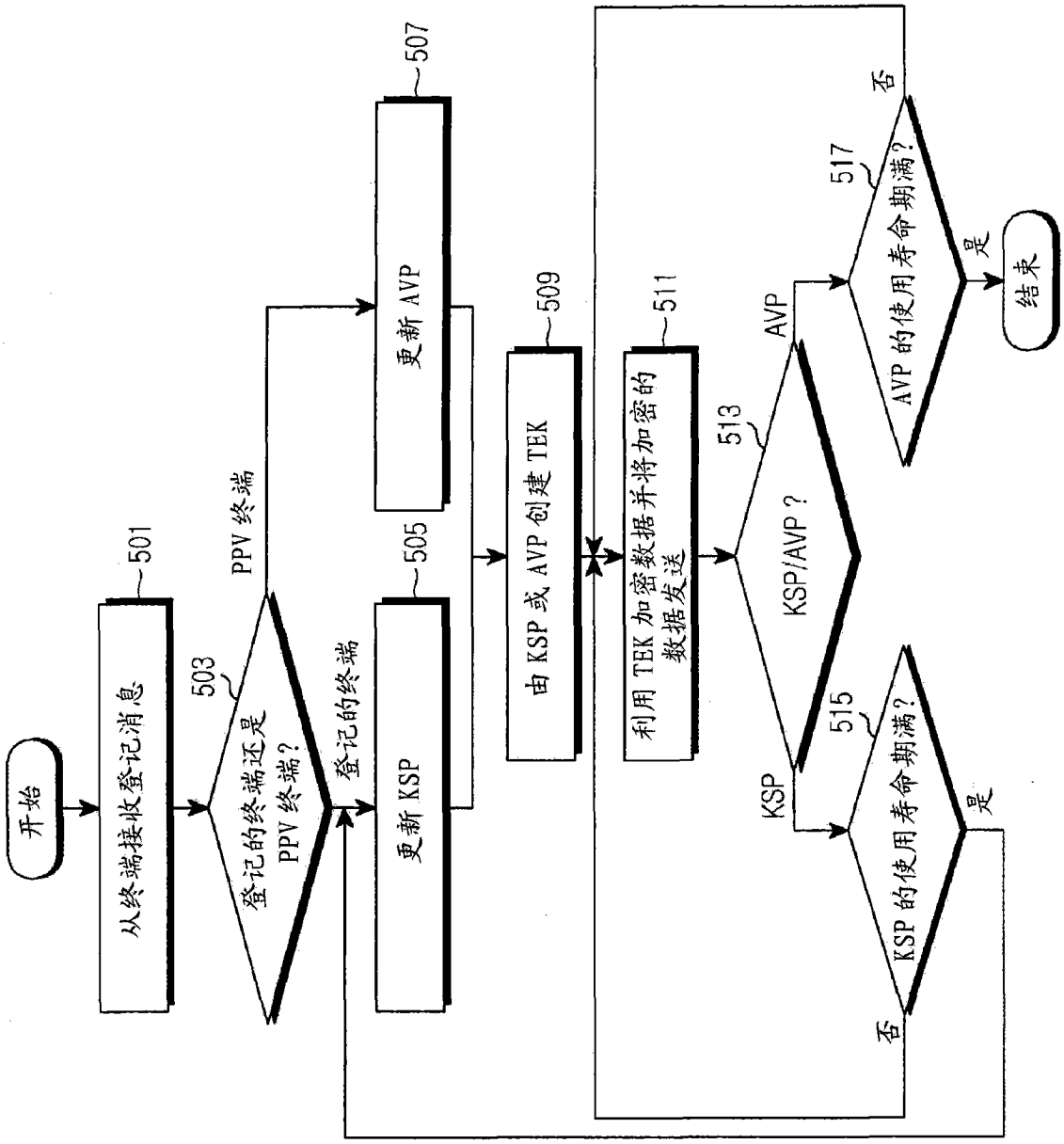

开始
从终端接收登记消息
501
登记的终端还是 PPV 终端？
503
PPV 终端
登记的终端
更新 KSP
505
更新 AVP
507
由 KSP 或 AVP 创建 TEK
509
利用 TEK 加密数据并将加密的数据发送
511
KSP/AVP ？
513
AVP
KSP
AVP 的使用寿命期满？
517
否
是
结束
KSP 的使用寿命期满？
515
否
是

图 5

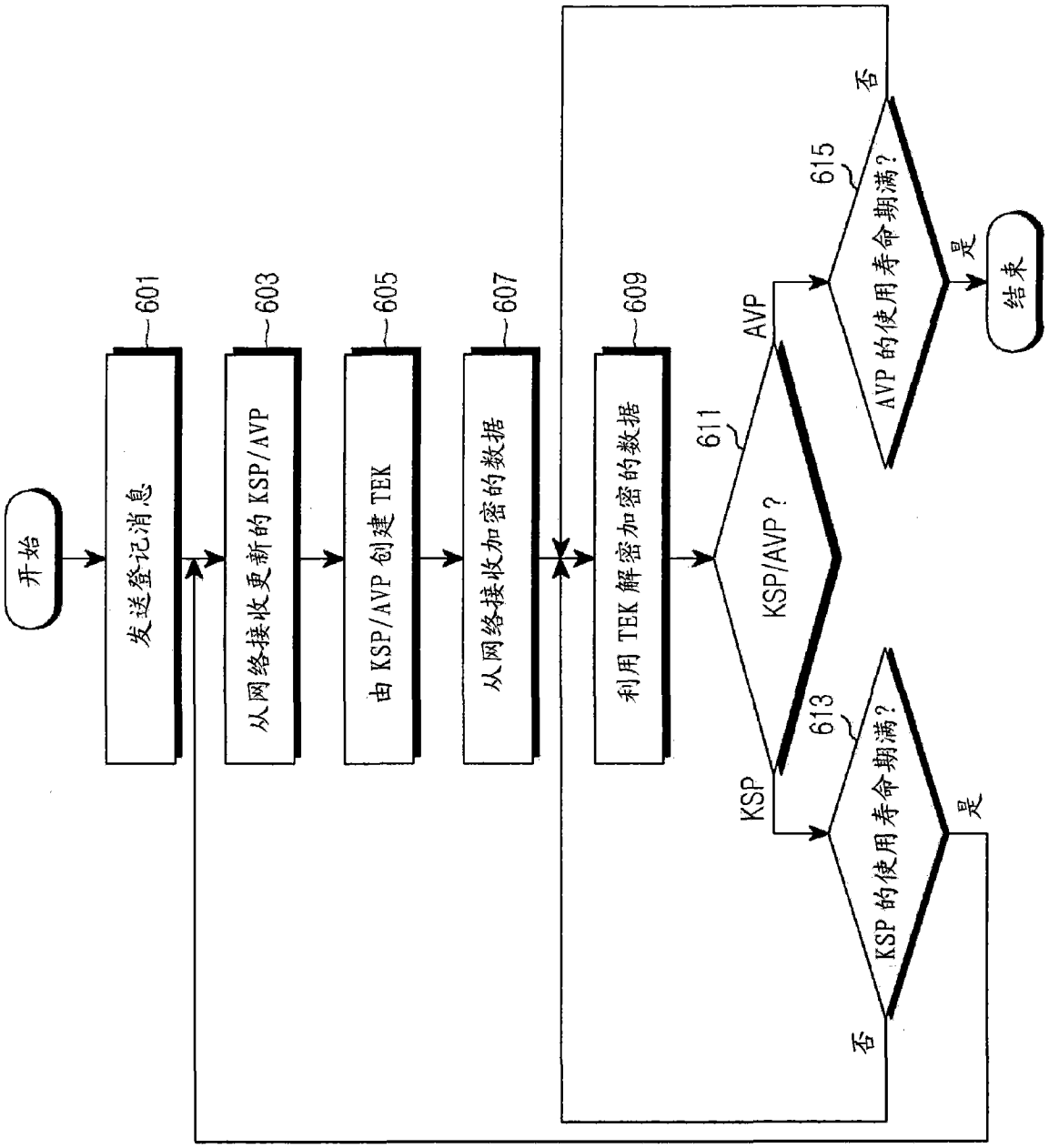

开始
601
发送登记消息
603
从网络接收更新的 KSP/AVP
605
由 KSP/AVP 创建 TEK
607
从网络接收加密的数据
609
利用 TEK 解密加密的数据
611
KSP/AVP ?
AVP
KSP
615
AVP 的使用寿命期满?
否
是
结束
613
KSP 的使用寿命期满?
否
是

图 6

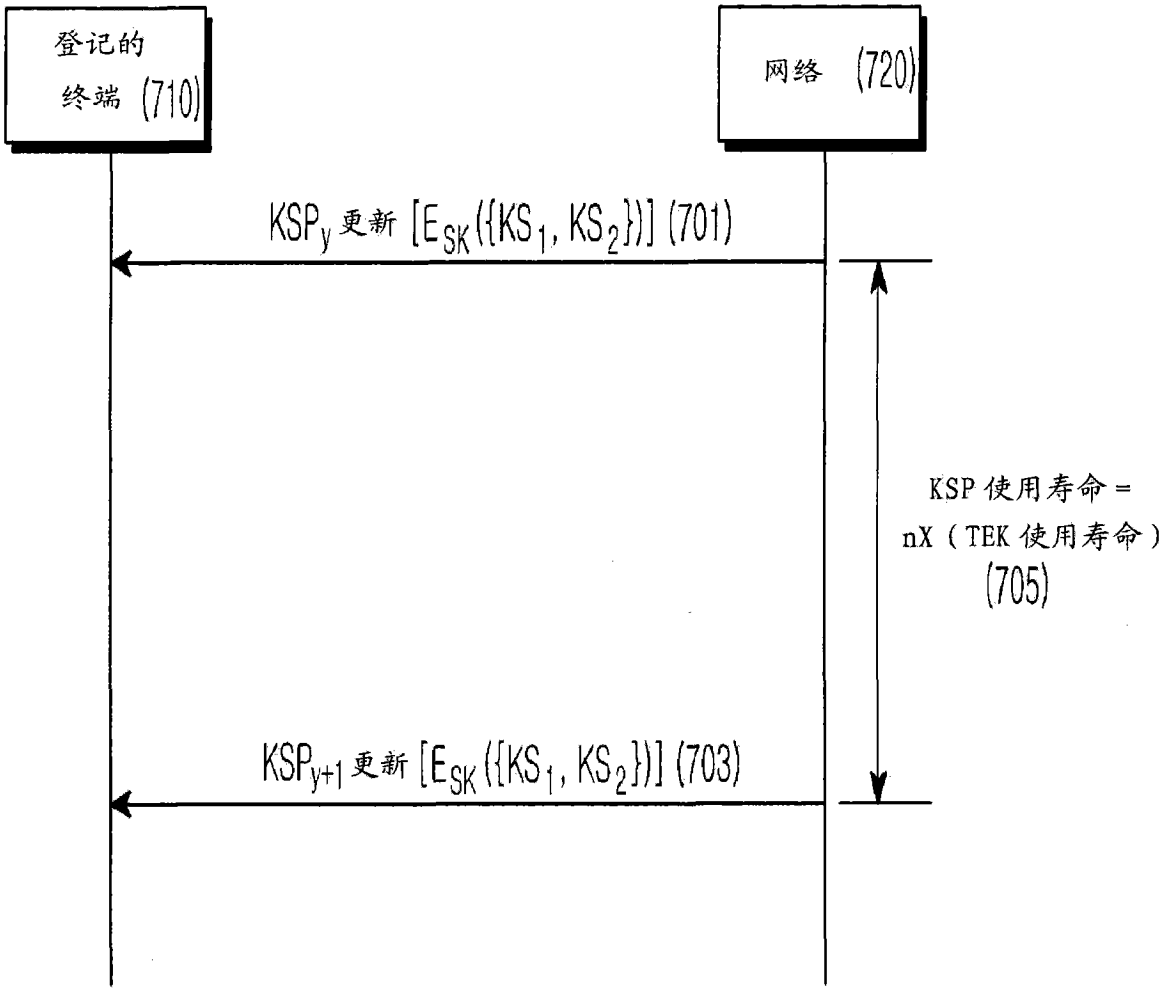

登记的
终端 (710)
网络 (720)
KSPy 更新 [ESK({KS1, KS2})] (701)
KSP 使用寿命 =
nX（TEK 使用寿命）
(705)
KSPy+1 更新 [ESK({KS1, KS2})] (703)

图 7

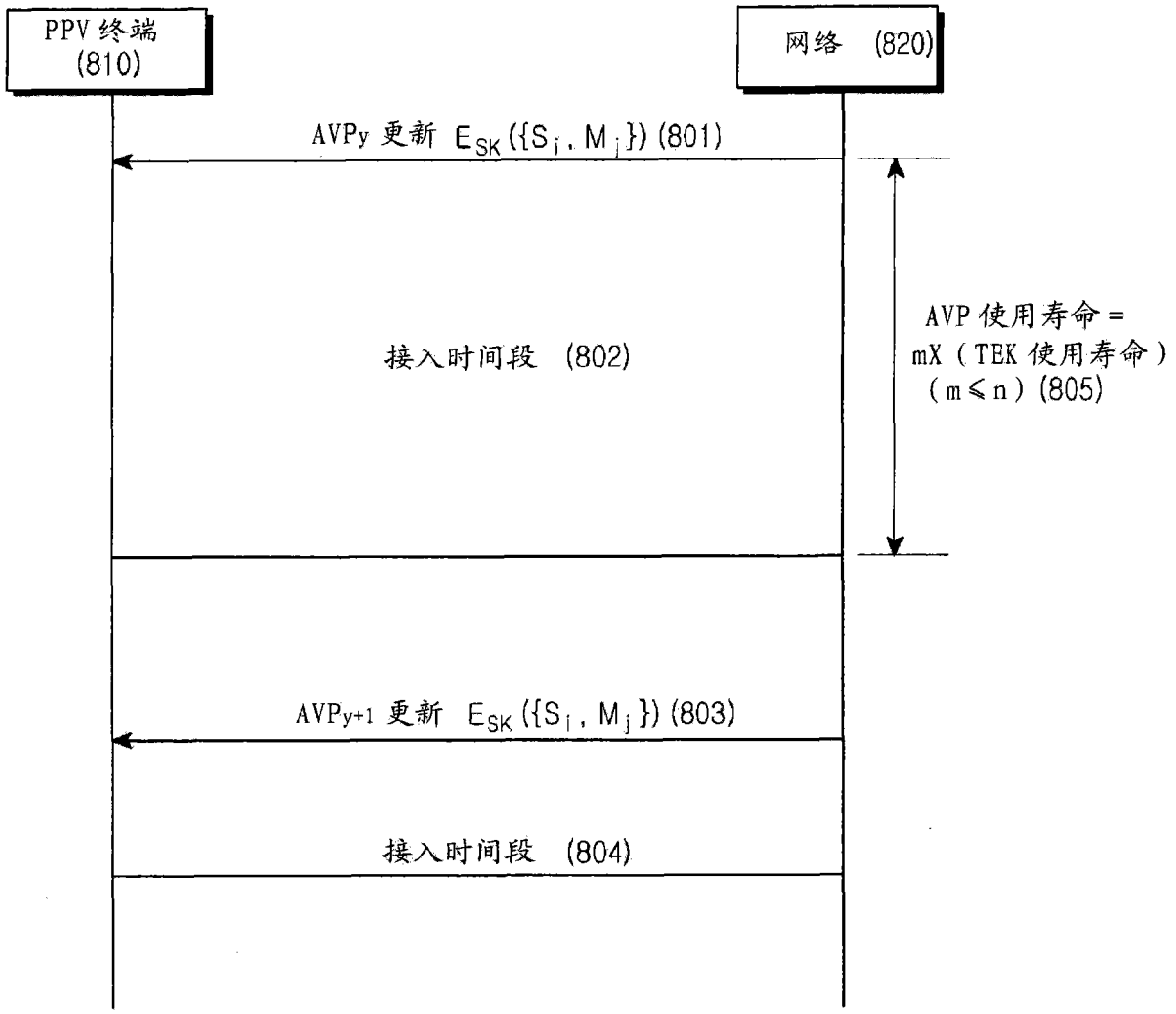

PPV 终端
(810)
网络 (820)
AVPy 更新 $E_{SK}(\{S_i, M_j\})$ (801)
接入时间段 (802)
AVP 使用寿命 =
mX（TEK 使用寿命）
（m≤n）(805)
AVPy+1 更新 $E_{SK}(\{S_i, M_j\})$ (803)
接入时间段 (804)

图 8

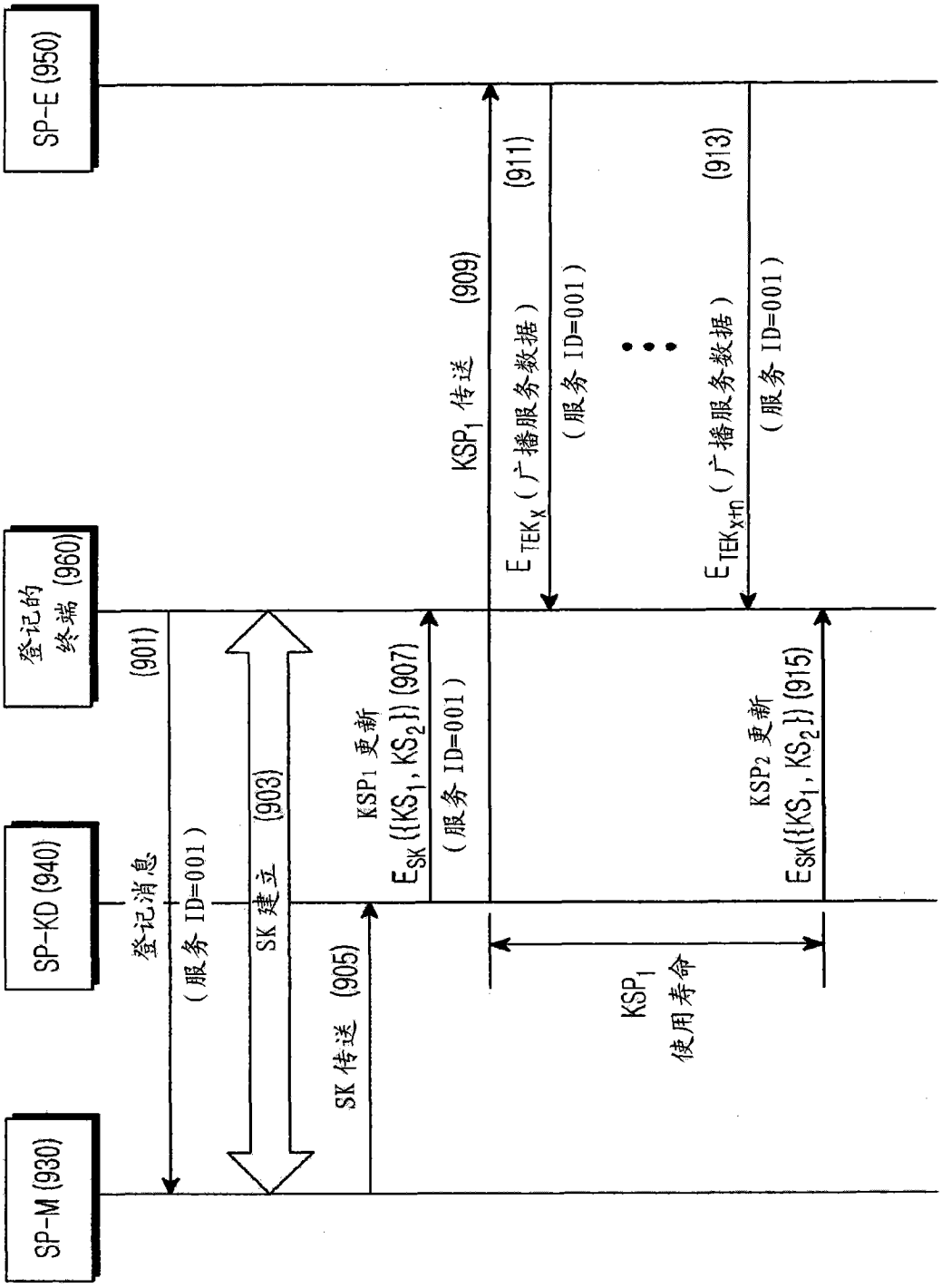

SP-E (950)
登记的终端 (960)
SP-KD (940)
SP-M (930)
登记消息 (901)
(服务 ID=001)
SK 建立 (903)
SK 传送 (905)
KSP1 更新 E_SK{{KS1, KS2}} (907)
(服务 ID=001)
KSP1 传送 (909)
E_TEKX (广播服务数据) (911)
(服务 ID=001)
E_TEKX+n (广播服务数据) (913)
(服务 ID=001)
KSP2 更新 E_SK{{KS1, KS2}} (915)
KSP1 使用寿命

图 9

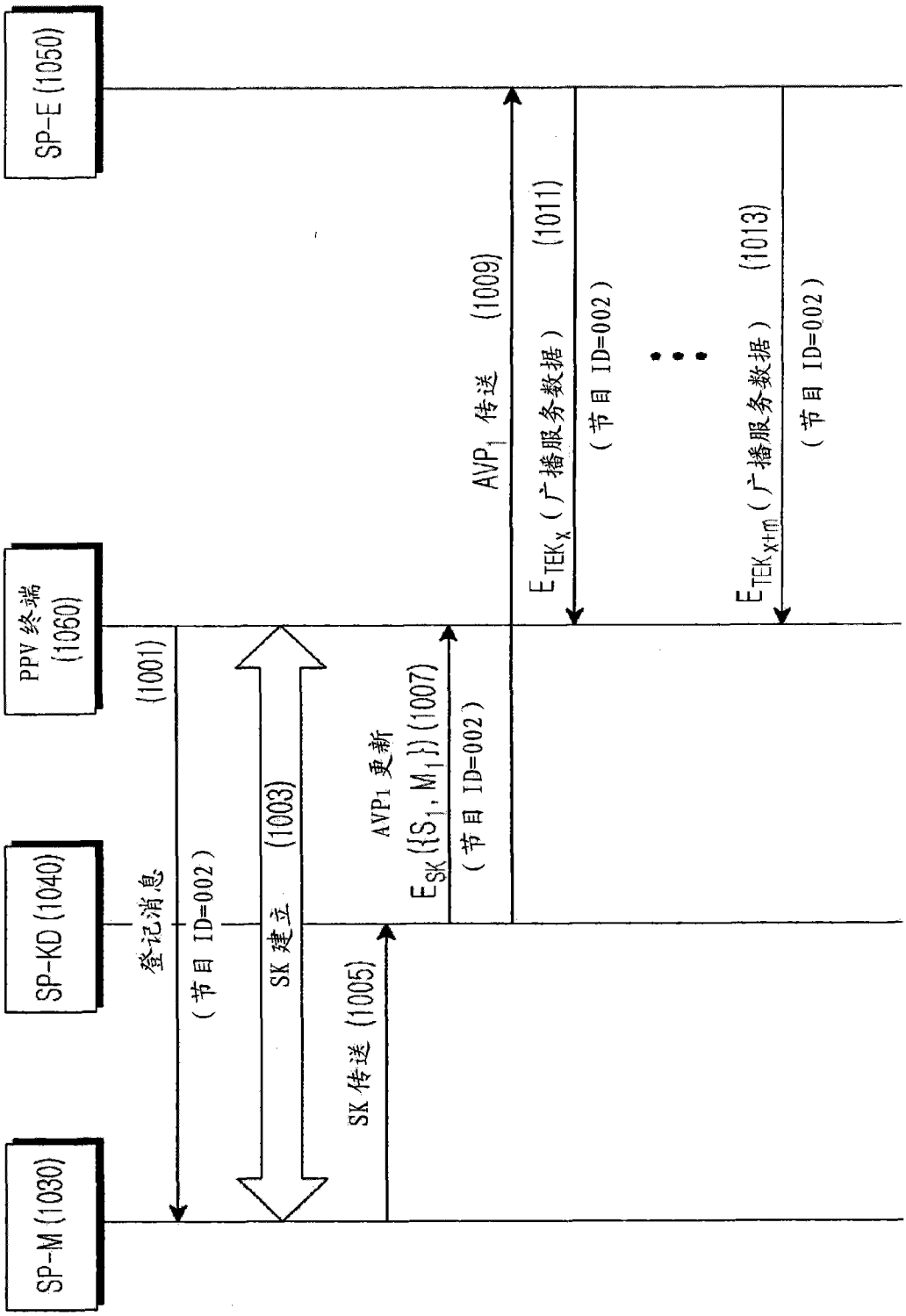

SP-E (1050)
PPV 终端 (1060)
SP-KD (1040)
SP-M (1030)
登记消息 (1001)
(节目 ID=002)
SK 建立 (1003)
SK 传送 (1005)
AVP1 更新
ESK({S1, M1}) (1007)
(节目 ID=002)
AVP1 传送 (1009)
ETEKX (广播服务数据) (1011)
(节目 ID=002)
ETEKX+m (广播服务数据) (1013)
(节目 ID=002)

图 10

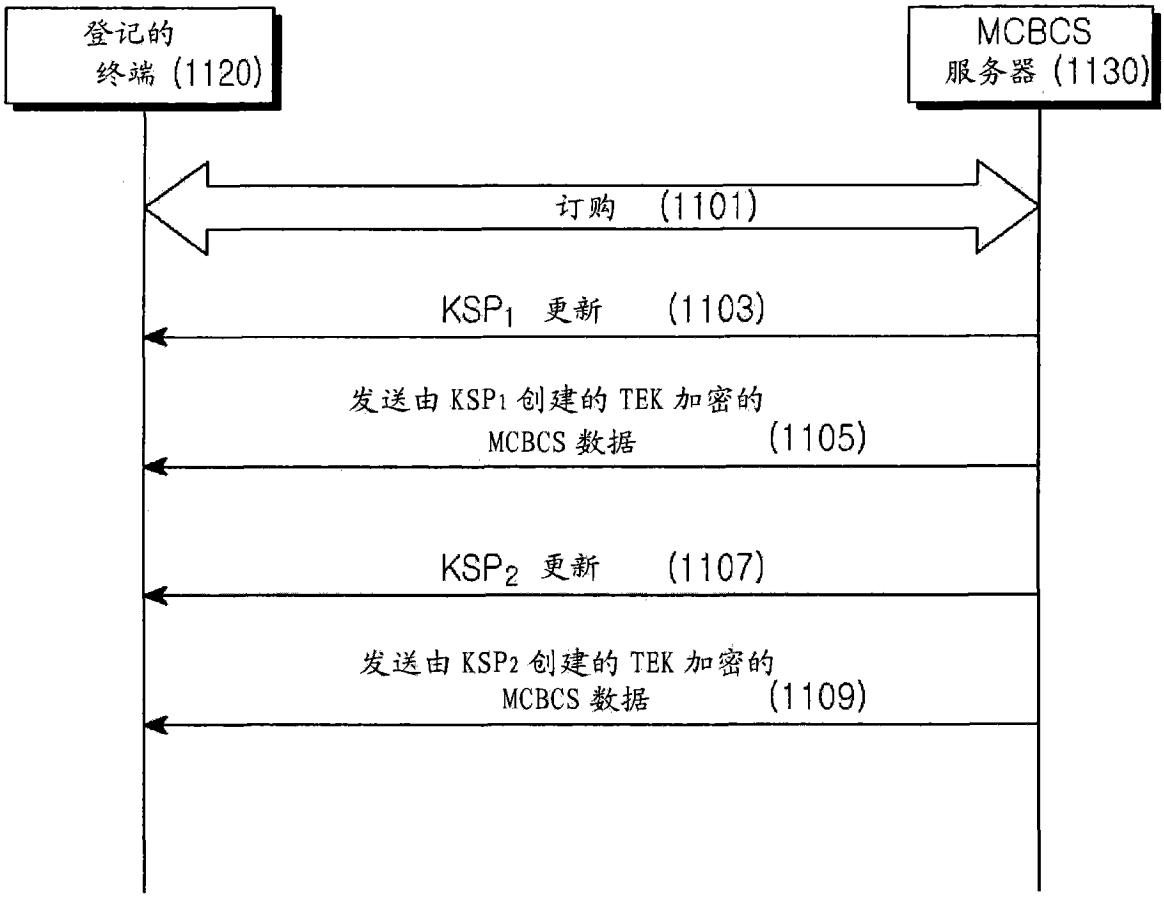

登记的
终端 (1120)
MCBCS
服务器 (1130)
订购 (1101)
KSP1 更新 (1103)
发送由 KSP1 创建的 TEK 加密的
MCBCS 数据 (1105)
KSP2 更新 (1107)
发送由 KSP2 创建的 TEK 加密的
MCBCS 数据 (1109)

图 11

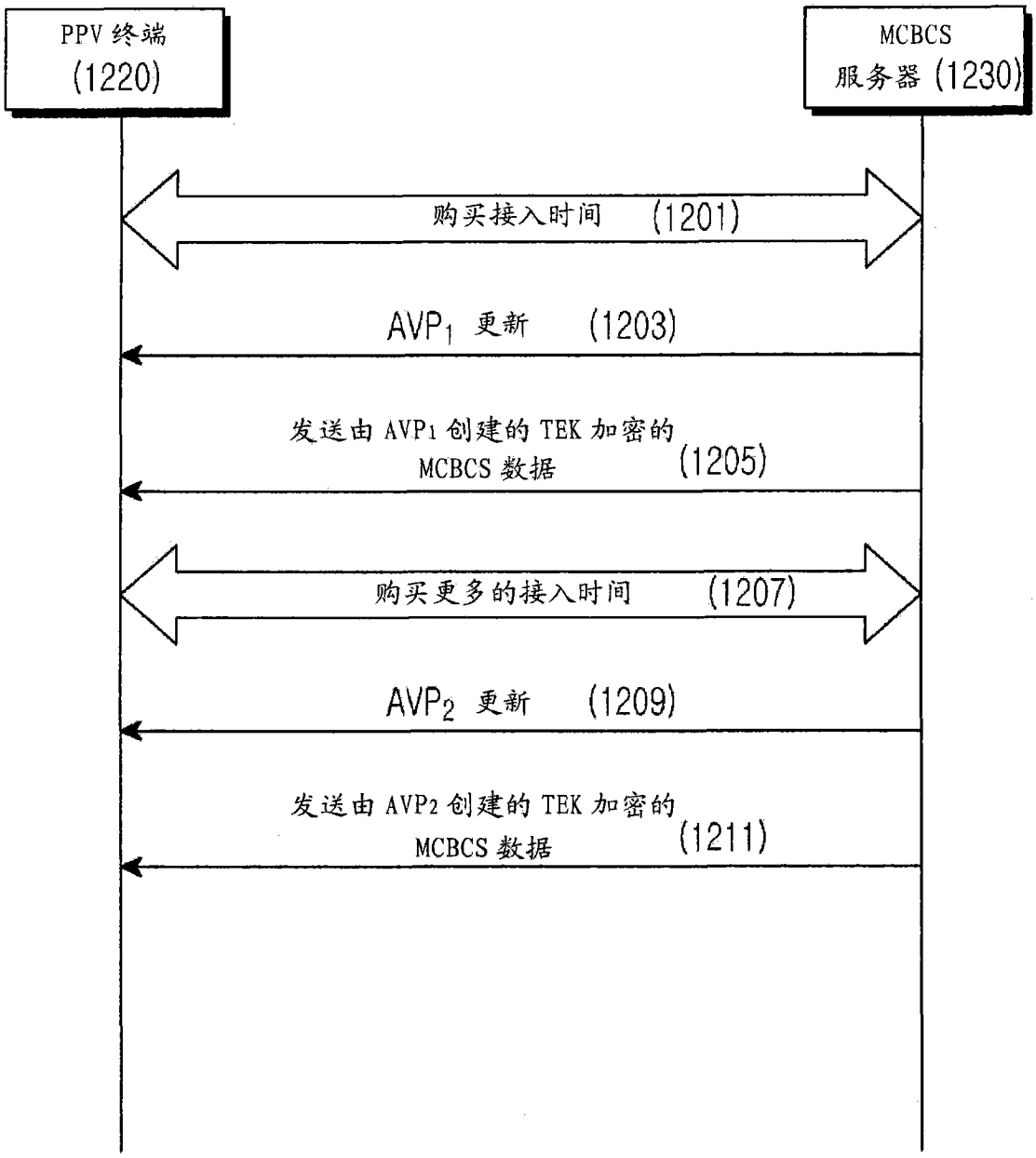

PPV 终端
(1220)
MCBCS
服务器 (1230)
购买接入时间 (1201)
AVP1 更新 (1203)
发送由 AVP1 创建的 TEK 加密的
MCBCS 数据 (1205)
购买更多的接入时间 (1207)
AVP2 更新 (1209)
发送由 AVP2 创建的 TEK 加密的
MCBCS 数据 (1211)

图 12

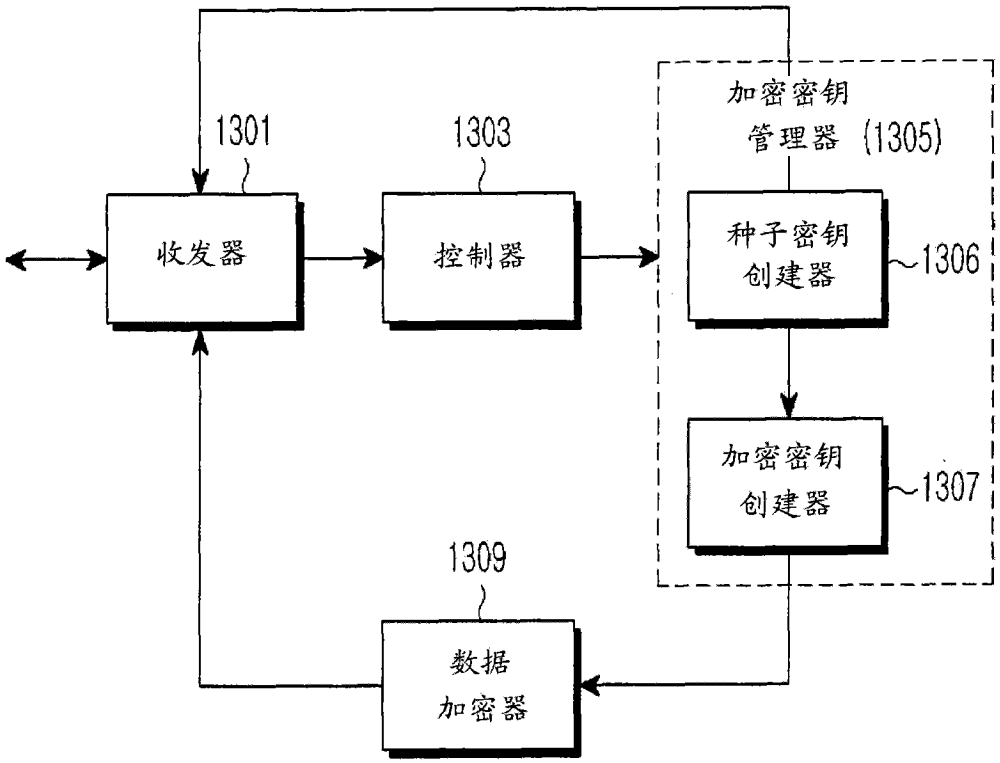

1301
1303
加密密钥
管理器 (1305)
收发器
控制器
种子密钥
创建器
1306
加密密钥
创建器
1307
1309
数据
加密器

图 13

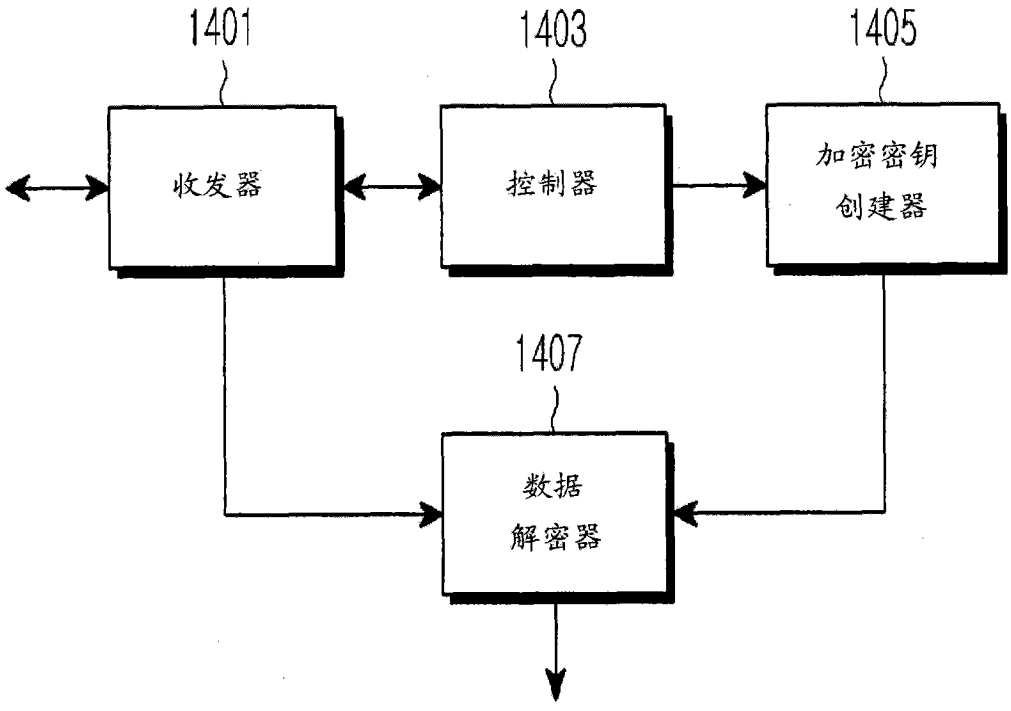

1401
1403
1405
收发器
控制器
加密密钥
创建器
1407
数据
解密器

图 14