(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 101453732 B
(45)授权公告日 2012.10.10

(21)申请号 200810179849.4

(22)申请日 2008.12.05

(30)优先权数据
60/992,675 2007.12.05 US

(73)专利权人 创新音速有限公司
地址 毛里求斯路易士港

(72)发明人 郭丰旗

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 蒲迈文

(51)Int.Cl.
*H04W 12/04*(2006.01)
*H04W 12/08*(2006.01)

(56)对比文件
3GPP,MOBILE COMPETENCE CENTRE.3rd Generation Partnership Project
Technical Specification Group Radio Access Network
Radio Resource Control(RRC).Protocol Specification TS 25.331 V8.0.0(Release 8).2007,112-125,270-275,309-318.

Huawei.Key Update in LTE-ACTIVE state.3GPP TSG RAN WG3 Meeting #57bis,Sophia Antipolis,FRANCE.2007, 全文.

Huawei.Key Update in LTE-ACTIVE state.3GPP TSG RAN WG3 Meeting #57bis,Sophia Antipolis,FRANCE.2007, 全文.

审查员 张琦

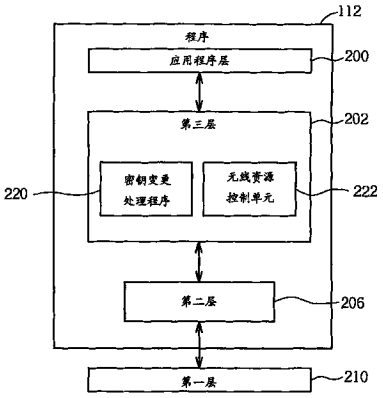
权利要求书 1 页 说明书 5 页 附图 4 页

(54)发明名称

处理密钥变更的方法及其相关通信装置

(57)摘要

一种处理密钥变更的方法及通信装置,用于一无线通信系统的一客户端中,其包括利用一无线资源控制程序启动密钥变更,该程序同时涵盖伴随一授权与密钥认证程序与不伴随一授权与密钥认证程序两种情形。




CN 101453732 B

1. 一种用于无线通信系统的网络端中启动密钥变更的方法，其特征在于，所述方法包括：

利用切换程序 HANDOVER 启动密钥变更，所述切换程序包含第一种情形及第二种情形，所述第一种情形是所述密钥变更伴随授权与密钥认证程序，所述第二种情形是所述密钥变更不伴随所述授权与密钥认证程序；以及

通过所述切换程序，传送用来启动所述密钥变更的无线资源控制信息，所述无线资源控制信息包含一指示器，所述指示器用来指示所述密钥变更是否伴随所述授权与密钥认证程序。

2. 一种用于无线通信系统的客户端中的处理密钥变更的方法，其特征在于，所述方法包括：通过一切换程序 HANDOVER，接收用来启动密钥变更的无线资源控制信息，所述无线资源控制信息包含一指示器，所述指示器用来指示所述密钥变更是否伴随授权与密钥认证程序；以及

根据所述指示器，判断所述密钥变更是否伴随所述授权与密钥认证程序；

当所述密钥变更伴随所对应的所述授权与密钥认证程序时，根据所述授权与密钥认证程序所对应的母密钥，产生安全密钥集；以及

当所述密钥变更不伴随所对应的所述授权与密钥认证程序时，根据先前的基站密钥或先前的母密钥，产生所述安全密钥集；

其中，所述安全密钥集包含使用者平台密钥及无线资源控制密钥。

3. 根据权利要求 2 所述的方法，其特征在于，其中所述客户端操作于无线资源控制连线状态或长期演进主动状态。

# 处理密钥变更的方法及其相关通信装置

## 技术领域

[0001] 本发明涉及一种用于无线通信系统的方法及其相关装置，尤其涉及一种用于无线通信系统中处理密钥变更的方法及其相关装置。

## 背景技术

[0002] 第三代移动通信技术可提供高度频谱利用效率、无边界的覆盖率及高品质、高速率的多媒体数据传输，同时更能同时满足各种不同的 QoS（服务质量）服务要求，提供具弹性的多样化双向传输服务，并提供较佳的通信品质，有效降低通信中断率。

[0003] 为了避免用户数据与某些信息被截收而遭到冒用的损害，已知第三代移动通信系统可通过一安全模式控制程序，以进行完整性保护 (IntegrityProtection) 或加密保护，使信息传递更为安全。加密保护的运作方式通过一加密演算法 (Ciphering Algorithm)，计算出用以提供加密保护机制所需的密钥串 (Keystream) 区块。接着，传输端将密钥串区块与明文 (Plain Text) 区块加密得到密文 (Cipher Text) 区块，而接收端则可藉与传输端相同的密钥串区块对所接收的密文 (Cipher Text) 区块进行解密，从而得到明文区块。

[0004] 第三代移动通信系统中信息交换的安全性考量是依据第三代合作伙伴计划 (the 3rd Generation Partnership Project，3GPP) 所制定的一安全架构协议规范，其提供一授权与密钥认证 (Authentication and Key Agreement，AKA) 程序，在客户端与网络端间提供认证及产生密钥的机制，以确保数据的保密性与安全性。也就是说，当移动管理 (Mobile Management) 层级执行完授权与密钥认证后会分配一组新的密钥给客户端使用。

[0005] 请参考图 1，图 1 为已知用于一长期演进 (Long Term Evolution，LTE) 无线通信系统的密钥层级的示意图。针对不同层级的安全机制，客户端包含一永久密钥 K、一加密密钥 (Ciphering Key，CK)、一完整性密钥 (IntegrityKey，IK)、一母密钥 $K_{ASME}$、一非存取层级加密密钥 $K_{(NAS,enc)}$、一非存取层级完整性密钥 $K_{(NAS,int)}$ 及一基站层级密钥 $K_{eNB}$。永久密钥 K 储存于客户端 的用户通用识别模块 (Universal Subscriber Identity Module，USIM)。加密密钥及完整性密钥用于通用移动电信系统 (Universal Mobile TelecommunicationSystem，UMTS) 的加密与完整性机制。母密钥 $K_{ASME}$ 用于客户端与一存取安全管理单元 (Access Stratum Management Entity，ASME) 之间。对于非存取层级部分，非存取层级加密密钥 $K_{(NAS,enc)}$ 及非存取层级完整性密钥 $K_{(NAS,int)}$ 分别用于非存取信息的加密与完整性机制。基站层级密钥 $K_{eNB}$ 可再衍生出一使用者平台密钥 $K_{eNB-UP-enc}$ 及无线资源控制密钥 $K_{eNB-RRC-int}$ 与 $K_{eNB-RRC-enc}$，其分别用于使用者平面数据的加密、无线资源控制完整性及无线资源控制加密机制。图 1 显示为各密钥的衍生关系，例如，基站层级密钥 $K_{eNB}$ 可由母密钥 $K_{ASME}$ 经过特殊演算法而得出，其余类推。当客户端操作于无线资源控制连线状态 (RRC_CONNECTED) 或长期演进主动状态 (LTE_ACTIVE) 时，基站密钥 $K_{eNB}$ 衍生出使用者平台密钥 $K_{eNB-UP-enc}$ 以及无线资源控制密钥 $K_{eNB-RRC-int}$、$K_{eNB-RRC-enc}$，一旦客户端转换至无线资源控制闲置状态或长期演进闲置状态时，基站密钥 $K_{eNB}$、使用者平台密钥 $K_{eNB-UP-enc}$ 以及无线资源控制密钥 $K_{eNB-RRC-int}$、$K_{eNB-RRC-enc}$ 则会从加强式基站中删除。除此之外，当客户端完成授权与密钥认证程序时，图 1 的所有密钥必须

于后续密钥变更启动时更新。

[0006] 当客户端操作于无线资源控制连线状态或长期演进主动状态时，在以下四种特定情形时，加强式基站需执行密钥变更，以确保数据的保密与安全性：

[0007] 1、用于使用者平台或无线资源控制加密/完整性保护的序号(SequenceNumber)具一有限位长度。当超过序号的表示位数所能表示的数值时，序号会回归起始值(即零)重新开始累加，所以当序号即将绕回(Wrap Around)时，密钥必须更新以确保数据的保密性与安全性。

[0008] 2、当客户端操作于长期演进主动状态一段长时间后，即使用于客户端或无线资源控制加密/完整性保护的序列数目尚未绕回，密钥必须更新以避免密钥被破解。

[0009] 3、母密钥 $K_{ASME}$ 的生命周期达到限定周期时，也须更新以避免同一母密钥使用时间过久。

[0010] 4、当客户端从第二代/第三代无线接入网络系统(GERAN/UTRAN)进入长期演进系统时，即系统间切换(Inter-RAT handover)完成后几秒钟内，也必须完成密钥更新。

[0011] 然而，分析上述四种情形我们可以发现，情形1和2不一定需要执行授权与密钥认证程序，情形3和4则必须执行授权与密钥认证程序，以产生全新的安全密钥集。例如上述情形1和2，新的使用者平台密钥以及无线资源控制密钥可通过原本的基站密钥或是原本的母密钥来产生一新基站密钥，因此密钥变更不须伴随授权与密钥认证程序。

[0012] 就目前来说，启动密钥变更的方式尚未定案，其中一种可能的方式是通过一小区内切换(Intra-Cell Handover)程序用来启动密钥变更。换句话说，于客户端所在的小区内，网络端执行相同于转换小区间(Inter-Cell)的切换程序(Handover procedure)时，密钥变更随即启动。也就是说，切换前使用原本的安全密钥，切换后使用新的安全密钥。

[0013] 根据已知技术，当无线资源控制连线状态或长期演进主动状态时，密钥变更的需求包含两种情况，密钥变更伴随授权与密钥认证以及密钥变更不伴随授权与密钥认证。然而，目前尚没有明确的密钥变更机制同时涵盖这两种情况。

[0014] 发明内容

[0015] 因此，本发明的主要目的即在于提供一种处理密钥变更的方法及通信装置，以改善现有技术的缺失。

[0016] 本发明揭露一种用于无线通信系统的网络端中启动密钥变更的方法，其特征在于，所述方法包括：利用切换程序HANDOVER启动密钥变更，所述切换程序包含第一种情形及第二种情形，所述第一种情形是所述密钥变更伴随授权与密钥认证程序，所述第二种情形是所述密钥变更不伴随所述授权与密钥认证程序；以及通过所述切换程序，传送用来启动所述密钥变更的无线资源控制信息，所述无线资源控制信息包含一指示器，所述指示器用来指示所述密钥变更是否伴随所述授权与密钥认证程序。

[0017] 本发明揭露一种用于无线通信系统的客户端中的处理密钥变更的方法，其特征在于，所述方法包括：通过一切换程序HANDOVER，接收用来启动密钥变更的无线资源控制信息，所述无线资源控制信息包含一指示器，所述指示器用来指示所述密钥变更是否伴随所述授权与密钥认证程序；以及根据所述指示器，判断所述密钥变更是否伴随所述授权与密钥认证程序；当所述密钥变更伴随所对应的所述授权与密钥认证程序时，根据所述授权与密钥认 证程序所对应的母密钥，产生安全密钥集；以及当所述密钥变更不伴随所对应的所

述授权与密钥认证程序时，根据先前的基站密钥或先前的母密钥，产生所述安全密钥集；其中，所述安全密钥集包含使用者平台密钥及无线资源控制密钥。

[0018] 本发明另揭露一种用于无线通信系统中的网络端用来启动密钥变更的通信装置，其特征在于，所述通信装置包括：中央处理器，用来执行处理方法；以及储存装置，耦接于所述中央处理器，用来储存用以执行所述处理方法的程序，其中所述处理方法包括：利用切换程序 HANDOVER 启动密钥变更，所述切换程序包含第一情形及第二情形，所述第一情形是所述密钥变更伴随授权与密钥认证程序，所述第二情形是所述密钥变更不伴随所述授权与密钥认证程序；以及通过所述切换程序，传送用来启动所述密钥变更的无线资源控制信息，所述无线资源控制信息包含一指示器，所述指示器用来指示所述密钥变更是否伴随所述授权与密钥认证程序。

[0019] 本发明另揭露一种用于无线通信系统的客户端中用来执行密钥变更的通信装置，其特征在于，所述通信装置包括：中央处理器，用于执行处理方法；以及储存装置，耦接于所述中央处理器，用来储存用以执行所述处理方法的程序，其中所述处理方法包括：通过一切换程序 HANDOVER，接收用来启动密钥变更的无线资源控制信息，所述无线资源控制信息包含一指示器，所述指示器用来指示所述密钥变更是否伴随所述授权与密钥认证程序；以及根据所述指示器，判断所述密钥变更是否伴随所对应的所述授权与密钥认证程序；当所述密钥变更伴随授权与密钥认证程序时，根据所述授权与密钥认证程序所对应的母密钥，产生安全密钥集；以及当所述密钥变更不伴随所述授权与密钥认证程序时，根据先前的基站密钥或先前的母密钥，产生所述安全密钥集，其中，所述安全密钥集包含使用者平台密钥及无线资源控制密钥。

[0020] 本发明处理密钥变更的方法及通信装置利用一无线资源控制程序来启动密钥变更，同时客户端经由判断密钥变更是否伴随授权与密钥认证程序得知如何更新安全密钥集。

[0021] 附图说明

[0022] 图 1 为一已知用于一长期演进无线通信系统的密钥层级的示意图。

[0023] 图 2 为一无线通信系统的示意图。

[0024] 图 3 为一无线通信装置的功能方块图。

[0025] 图 4 为图 3 中一程序的示意图。

[0026] 图 5 为本发明实施例的流程图。

[0027] 具体实施方式

[0028] 请参考图 2，图 2 为一无线通信系统 10 的示意图。无线通信系统 10 较佳地为一长期演进无线通信系统，其简略地由一网络端及多个客户端组成。在图 2 中，网络端及客户端用来说明无线通信系统 10 的架构；实际上，网络端可视不同需求而包括多个基站、无线网络控制器等；而客户端则可以是移动电话、计算机系统等设备。

[0029] 请参考图 3，图 3 为一无线通信系统的无线通信装置 100 的功能方块图。无线通信装置 100 可以用来实现图 1 中的客户端。为求简洁，图 2 仅绘出无线通信装置 100 的一输入装置 102、一输出装置 104、一控制电路 106、一中央处理器 108、一储存装置 110、一程序 112 及一收发器 114。在无线通信装置 100 中，控制电路 106 通过中央处理器 108 执行储存于储存装置 110 中的程序 112，从而控制无线通信装置 100 的运作，其可通过输入装置

102(如键盘)接收使用者输入的信号,或通过输出装置104(如屏幕、喇叭等)输出图像、声音等信号。收发器114用以接收或发送无线信号,并将所接收的信号传送至控制电路106,或将控制电路106所产生的信号以无线电方式输出。换言之,以通信协议的架构而言,收发器114可视为第一层的一部分,而控制电路106则用来实现第二层及第三层的功能。

[0030] 请继续参考图4,图4为图3中程序112的示意图。程序112包括一应用程序层200、一第三层202及一第二层206,并与一第一层210连接。一无线资源控制(Radio Resource Control,RRC)单元222位于第三层202,用来利用无线资源控制程序与一基站或一无线接入网络交换无线资源控制信息,并根据信息中的子件,设定第一层210及第二层206的操作。此外,无线资源控制单元222可转换无线通信装置100在一无线资源控制闲置(RRC_IDLE)状态或一无线资源控制连线(RRC_CONNECTED)状态之间。

[0031] 当无线通信装置100处于无线资源控制连线状态时,本发明实施例在程序112中提供一密钥变更处理程序220,用来判断密钥变更是否伴随授权与密钥认证程序。请参考图5,图5为本发明实施例一流程40的示意图。流程40用于一无线通信系统的一客户端中处理密钥变更,其可被编译为密钥变更处理程序220。流程40包括以下步骤:

[0032] 步骤400:开始。

[0033] 步骤402:利用加强式基站起始的一无线资源控制程序,以启动一密钥变更。

[0034] 步骤404:利用该无线资源控制程序,得知该密钥变更与对应于该密钥变更的一授权与密钥认证程序的伴随关系。

[0035] 步骤406:根据步骤404中,密钥变更与对应于该密钥变更的一授权与密钥认证程序的伴随关系,产生新的安全密钥集。

[0036] 步骤408:结束。

[0037] 根据流程40,本发明实施例利用一无线资源控制程序启动密钥变更,无线资源控制程序同时涵盖密钥变更伴随所对应的授权与密钥认证程序以及密钥变更不伴随所对应的授权与密钥认证程序两种情形。较佳地,当客户端操作于一无线资源控制连线状态或一长期演进主动状态时,通过该无线资源控制程序,客户端接收来自加强式基站的无线资源控制信息,其包含一指示器,用来指示密钥变更是否伴随该授权与密钥认证程序。

[0038] 较佳地,关于密钥变更的安全密钥(Access Stratum Key,AS Key)集包含一使用者平台密钥 $K_{eNB-UP-enc}$ 及无线资源控制密钥 $K_{eNB-RRC-int}$ 与 $K_{eNB-RRC-enc}$。所述密钥集的衍生关系可参考前述说明,于此不再赘述。如果指示器指示密钥变更伴随该授权与密钥认证程序,则表示先前已完成授权与密钥认证程序,因此客户端须重新产生新的安全密钥集。因此新的安全密钥集须通过新的母密钥而产生。相反地,如果指示器指示密钥变更不伴随该授权与密钥认证程序,则新的安全密钥集是通过先前(旧有)的母密钥 $K_{ASME}$ 或基站密钥 $K_{eNB}$ 而产生。因此,客户端可藉由无线资源控制信息中的指示器,判断密钥变更是否伴随该授权与密钥认证程序,而产生相应的新安全密钥集。

[0039] 另一方面,客户端可以自行使用一状态指标,其用来指示伴随该授权与密钥认证程序时所对应的新安全密钥集的启用状态。当执行该授权与密钥认证程序时,状态指针设定为一第一数值,其指示安全密钥集尚未被启用。在密钥变更启动后,将状态指标设定为一第二数值,其指示安全密钥集已被启用。举例来说,状态指针可用一位表示,当位值为“0”时,表示存在一已启用安全密钥集,当位值为“1”时,表示新安全密钥集已通过授权与密钥

认证程序重新产生但是尚未启用。当新安全密钥集被启用后，该位值重设为“0”。

[0040] 除此之外，在一无线资源控制连线状态或一长期演进主动状态中，当客户端接收到来自加强式基站用来启动密钥变更的无线资源控制信息时，客户端根据状态指标，判断该密钥变更与该授权与密钥认证程序的伴随关系。当状态指标为第一数值时，判断密钥变更伴随该授权与密钥认证程序；以及于状态指标为第二数值时，判断密钥变更不伴随该授权与密钥认证程序。举例来说，当状态指标为“0”时，其表示新的安全密钥集通过故有的母密钥或基站密钥（$K_{eNB}$）而产生，因此客户端判断密钥变更不伴随该授权与密钥认证程序。当状态指标为“1”时，其表示新的安全密钥集已重新分配，因此客户端判断密钥变更伴随该授权与密钥认证程序。同时于该密钥变更启动程序结束后，将状态指标重设为“0”，用来指示伴随该授权与密钥认证程序所对应的新安全密钥集已启用。

[0041] 由上可知，通过判断密钥变更是否伴随授权与密钥认证程序，客户端可得知如何更新安全密钥集。

[0042] 综上所述，本发明实施利利用一无线资源控制程序来启动密钥变更，同时客户端经由判断密钥变更是否伴随授权与密钥认证程序得知如何更新安全密钥集。

[0043] 以上所述仅为本发明的较佳实施例，凡依本发明权利要求书所做的均等变化与修饰，皆应属本发明的涵盖范围。

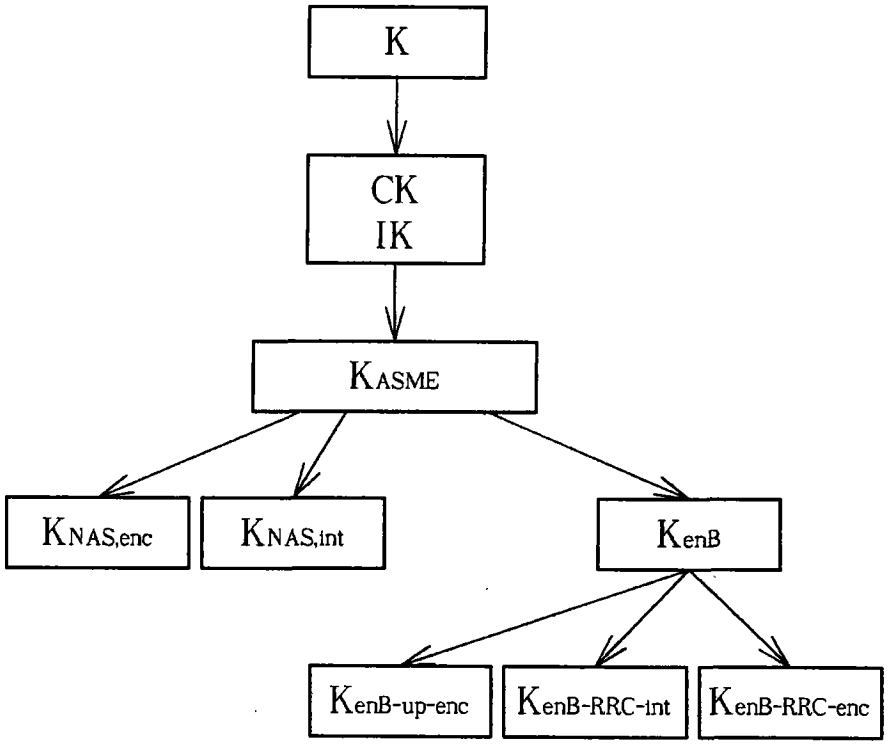

K
CK
IK
KASME
KNAS,enc
KNAS,int
KenB
KenB-up-enc
KenB-RRC-int
KenB-RRC-enc

图 1

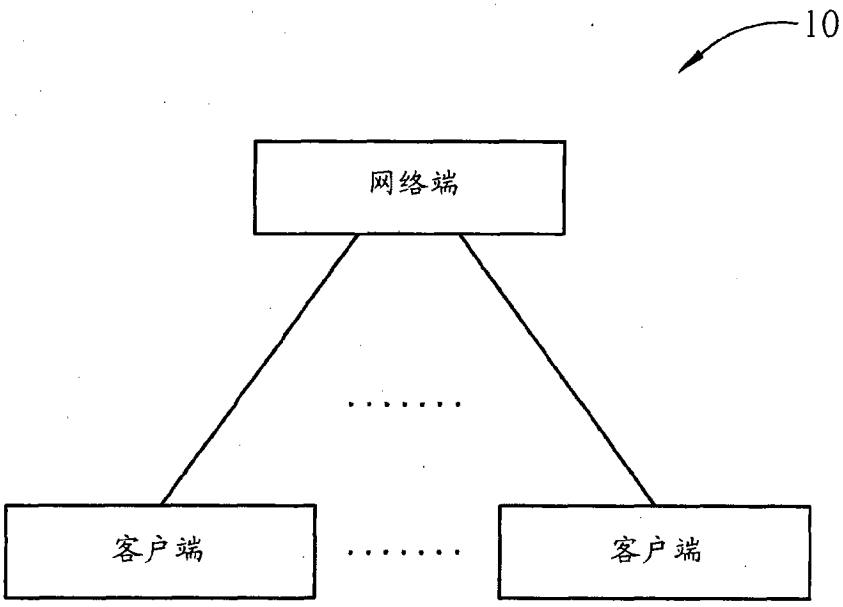

10
网络端
客户端
客户端

图 2

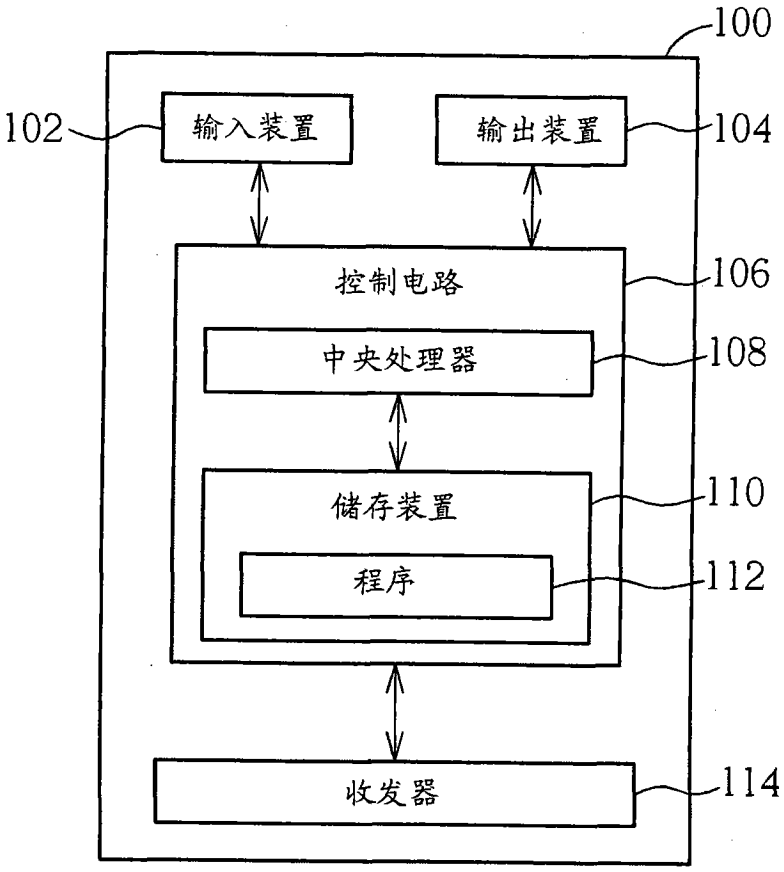

100
102
输入装置
输出装置
104
控制电路
106
中央处理器
108
储存装置
110
程序
112
收发器
114

图 3

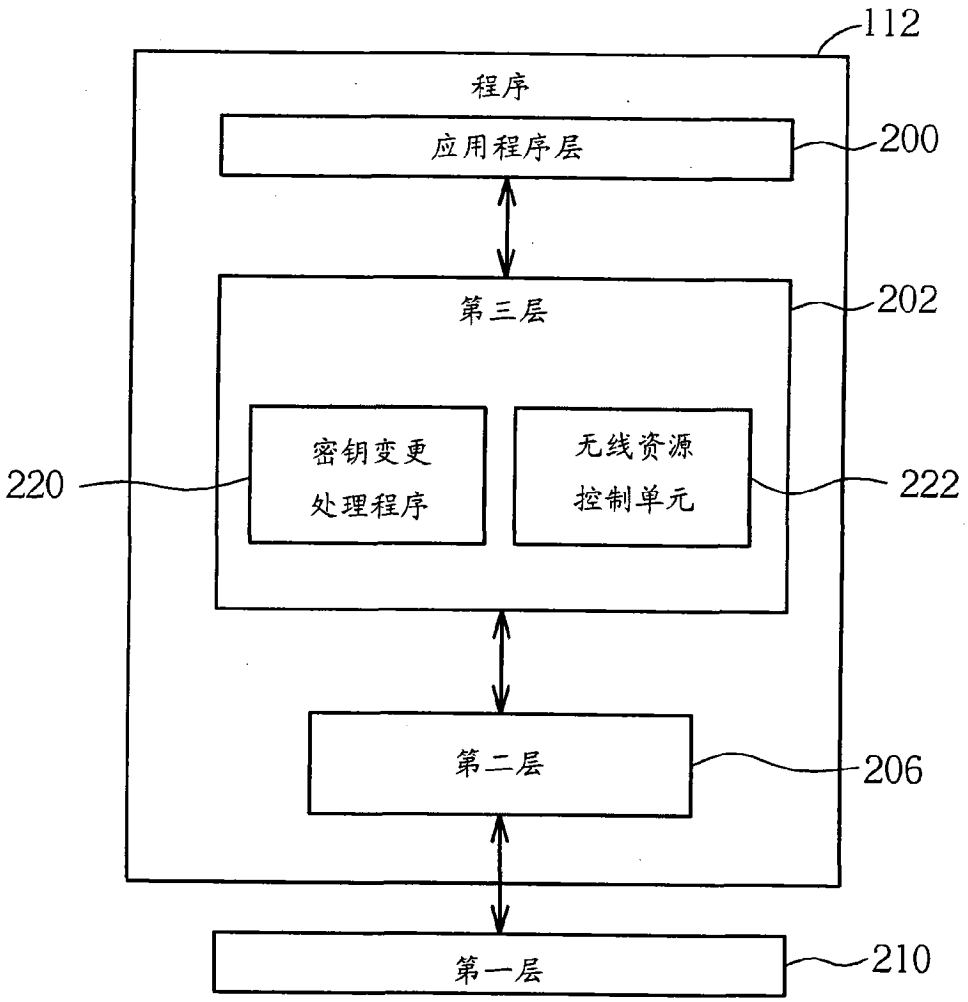

112
程序
应用程序层
200
第三层
202
密钥变更
处理程序
220
无线资源
控制单元
222
第二层
206
第一层
210

图 4

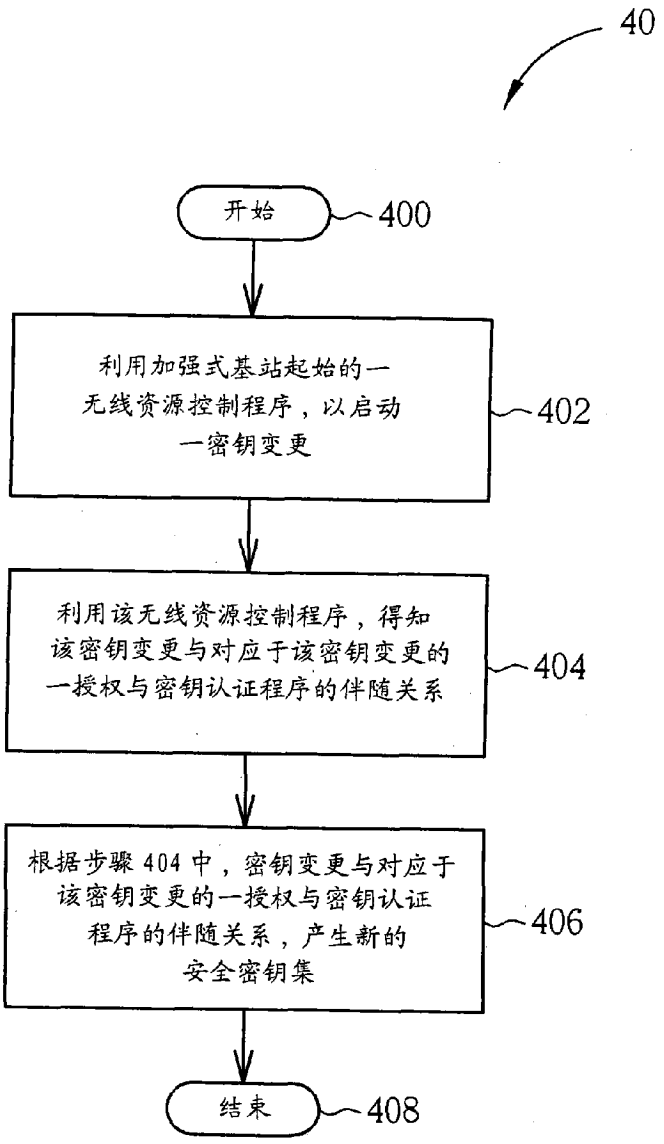

40
开始
400
利用加强式基站起始的一无线资源控制程序，以启动一密钥变更
402
利用该无线资源控制程序，得知该密钥变更与对应于该密钥变更的一授权与密钥认证程序的伴随关系
404
根据步骤 404 中，密钥变更与对应于该密钥变更的一授权与密钥认证程序的伴随关系，产生新的安全密钥集
406
结束
408

图 5