

(12) 发明专利

(10) 授权公告号 CN 101505462 B

(45) 授权公告日 2011.08.24

(21) 申请号 200910105782.4

CN 101262335 A, 2008.09.10,

(22) 申请日 2009.03.17

EP 1104496 B1, 2003.10.29,

(73) 专利权人 中兴通讯股份有限公司

审查员 张迎新

地址 518057 广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦A座6层

(72) 发明人 宋玉林

(74) 专利代理机构 深圳市世纪恒程知识产权代理事务所 44287

代理人 胡海国

(51) Int. Cl.

H04W 4/12 (2008.01)

H04W 12/04 (2009.01)

H04W 12/06 (2009.01)

H04H 60/23 (2008.01)

H04H 60/91 (2008.01)

(56) 对比文件

CN 1631038 A, 2005.06.22,

KR 20080000950 A, 2008.01.03,

CN 1980121 A, 2007.06.13,

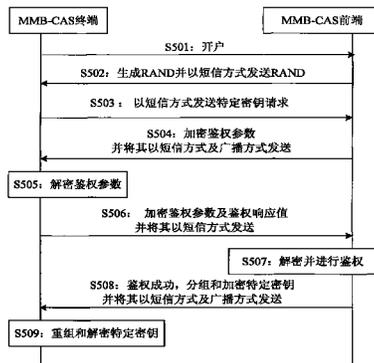
权利要求书 2 页 说明书 6 页 附图 5 页

(54) 发明名称

一种移动多媒体广播条件接收的鉴权方法及系统

(57) 摘要

本发明公开一种移动多媒体广播条件接收的鉴权方法及系统,所述鉴权方法包括如下步骤:前端对请求特定密钥的终端进行鉴权,当鉴权成功时,所述前端分组特定密钥并通过双向信道及单向信道发送所述特定密钥给所述终端。本发明通过单向信道和双向信道结合的方法实现在鉴权过程中的数据传输,提高了信息传输的安全性。



1. 一种移动多媒体广播条件接收的鉴权方法,包括:

前端对请求特定密钥的终端进行鉴权,当鉴权成功时,所述前端分组特定密钥并通过双向信道及单向信道发送所述特定密钥给所述终端,所述前端对所述终端进行鉴权的过程如下:所述前端通过双向信道及单向信道下发鉴权参数给所述终端,所述终端获取到鉴权参数后将鉴权响应结果发送给所述前端,所述前端根据所述鉴权响应结果判断鉴权是否成功,所述前端下发鉴权参数给所述终端时,所述前端在所述终端开户时生成一对应所述终端的随机值并发送所述随机值给所述终端,其中所述终端或前端分析所述随机值能得出鉴权参数的个数及各信道传送鉴权参数的个数,所述前端下发鉴权参数前根据分析所述随机值得到的鉴权参数的个数及各信道传送鉴权参数的个数,随机性地确定通过所述双向信道下发和通过所述单向信道下发的具体鉴权参数。

2. 如权利要求1所述的移动多媒体广播条件接收的鉴权方法,其特征在于:所述鉴权响应结果包括鉴权参数和鉴权响应值,判断鉴权是否成功按如下过程进行:所述前端先判断收到的鉴权参数与所述前端储存的鉴权参数是否一致,若不一致,认为所述终端是非合法的,鉴权失败,若一致,所述前端再根据鉴权参数算出一鉴权响应值,所述前端判断算出的鉴权响应值与所述终端发送的鉴权响应值是否一致,若一致,鉴权成功,若不一致,鉴权失败。

3. 如权利要求1所述的移动多媒体广播条件接收的鉴权方法,其特征在于:所述前端在发送所述鉴权参数、所述特定密钥给所述终端及所述终端发送鉴权响应结果给所述前端的过程中,发送信息的一端通过所述随机值对发送的信息进行加密处理后再发送,接收信息的一端通过所述随机值对接收到的信息进行解密处理。

4. 如权利要求1所述的移动多媒体广播条件接收的鉴权方法,其特征在于:所述特定密钥为用户密钥或承载业务密钥。

5. 如权利要求1所述的移动多媒体广播条件接收的鉴权方法,其特征在于:所述双向信道为短信信道,所述单向信道为广播信道。

6. 一种移动多媒体广播条件接收的系统,包括一前端及一终端,所述前端包括一前端业务控制模块、一第一双向信道发送接收模块及一单向信道发送模块,所述终端包括一终端业务控制模块、一第二双向信道发送接收模块及一单向信道接收模块,其中:

所述终端业务控制模块,用于在所述终端开户后将请求特定密钥下发的信息发送给所述前端及在所述终端获取到来自所述前端的鉴权参数后将鉴权响应结果通过所述第二双向信道发送接收模块发送给所述前端的第一双向信道发送接收模块;

所述前端业务控制模块,用于在所述前端收到所述来自终端的请求特定密钥下发的信息后下发鉴权参数给所述终端及在所述前端收到所述鉴权响应结果后根据所述鉴权响应结果判断鉴权是否成功,若鉴权成功,通过所述第一双向信道发送接收模块及所述单向信道发送模块发送所述特定密钥给所述终端的对应的第二双向信道发送接收模块及所述单向信道接收模块;

所述前端还包括一前端随机值生成维护模块,所述前端随机值生成维护模块用于在所述终端开户时对应所述终端生成一随机值并通过所述第一双向信道发送接收模块发送所述随机值给所述终端的第二双向信道发送接收模块,其中,所述终端或前端分析所述随机值能得出鉴权参数的个数及各信道传送鉴权参数的个数;

所述前端业务控制模块,还用于根据分析所述随机值得到的鉴权参数的个数及各信道传送鉴权参数的个数,随机性地确定通过第一双向信道发送接收模块及所述单向信道发送模块下发的具体鉴权参数。

一种移动多媒体广播条件接收的鉴权方法及系统

技术领域

[0001] 本发明涉及中国移动多媒体广播领域,尤其涉及一种移动多媒体广播条件接收的鉴权方法及系统。

背景技术

[0002] 中国移动多媒体广播(CMMB,China Mobile multimedia broadcasting)是广电总局主导并推荐的行业标准。CMMB是一个广播式的单向数据传输通道,因此除了可以传输电视节目、广播节目的音视频信号之外,各种电子数据都可以通过它来发送。CMMB主要面向手机、PDA等小屏幕便携手持终端以及车载电视等终端提供广播电视服务。

[0003] 目前CMMB终端播放清流实现比较简单的;对于播放加密流,CMMB提出了“移动多媒体广播条件接收(Mobile multimedia broadcasting-Conditional Access System,简称为MMB-CAS)”。MMB-CAS可为移动多媒体广播业务提供传输过程中的保护,即针对业务的单向信道以及双向信道提供保护。移动多媒体广播运营商通常在播出时针对移动多媒体业务加入MMB-CAS条件接收控制机制。采用MMB-CAS,移动多媒体广播运营商可针对业务或业务包向指定用户或用户组授权,使得只有授权用户或用户组才能接收相关业务。

[0004] MMB-CAS分为前端子系统和终端子系统两部分,在移动多媒体广播系统中的位置如图1所示。其中,双向信道(如短信信道)是可选的,可以为前端与移动多媒体接收终端之间提供点对点的数据交互通道。本部分所定义和规定的条件接收系统既可适用于单向信道(如广播信道),也可适用于单向信道和双向信道相结合的场景。

[0005] 在仅有单向信道或单向终端的情况下,MMB-CAS可通过前端向终端单向授权信息方式向用户授权,或结合使用加密授权与电子钱包功能,通过终端本地交互方式实现用户自授权。在单向信道与双向信道和双向终端均可用的情况下,MMB-CAS还可通过双向信道以前端与终端点对点交互方式向用户授权。

[0006] MMB-CAS以四层密钥模型为基础,如图2所示,建立密钥安全管理与授权控制管理及分发机制,利用加扰技术,实现对业务的条件接收。整个密钥模型包含用户注册层、授权/安全管理层、授权控制层和业务加扰层。该模型的特点是密钥分层保护;每个密钥都有各自的生命周期;下层密钥由上层密钥加密后传输。

[0007] 用户注册层实现用户密钥(UK)在终端安全模块中的预置,或实现按双向注册方式的用户密钥分发。UK用来对业务密钥(SEK,Service Encryption Key)进行加密/解密。

[0008] 授权管理层实现授权管理信息(EMM,Entitlement Management Message,授权管理信息)数据从前端到终端的安全传递。前端利用UK对SEK信息加密,生成EMM,通过广播或双向信道传输给终端,终端进行解密获得SEK。SEK用来对控制字(CW,Control Word)进行加密/解密。

[0009] 安全管理层实现系统信令数据从前端到终端的安全传递。通常将系统信令利用UK加密后封装EMM中,通过广播或双向信道传输给终端,终端进行解密获得系统信令。利用系统信令进行系统的安全控制、密钥管理、功能管理等。

[0010] 授权控制层实现授权控制信息 (ECM) 数据从前端到终端的安全传递。前端利用 SEK 对 CW 进行加密,生成 ECM,通过广播信道传输给终端,终端进行解密获得 CW。CW 用来对传输的业务进行加扰 / 解扰。

[0011] 业务加扰层实现业务数据从前端到终端的安全传递。前端利用 CW 对业务进行加扰,通过广播信道传送给终端,终端利用 CW 对加扰业务进行解扰。

[0012] 承载业务密钥的授权管理信息 (Entitlement Manager Message, 简称 EMM) 通过广播信道分发,在有可选双向信道的条件下,也可通过双向信道分发。

[0013] 用户密钥可预置在图 1 中的 MMB-CAS 终端的安全模块中,在有可选双向信道的条件下,也可以双向认证的方式通过双向信道分发。

[0014] 从图 2 中可以看出, UK 以及 SEK 是可以单向或双向发下去的,而单一信道传送在传送过程中容易被窃听,从而影响信息传送的安全性。

发明内容

[0015] 本发明要解决的技术问题是,在移动多媒体广播条件接收系统中,利用单一信道传输数据安全性不高的问题。

[0016] 为解决上述技术问题,本发明提供一种移动多媒体广播条件接收的鉴权方法,所述方法包括:

[0017] 前端对请求特定密钥的终端进行鉴权,当鉴权成功时,所述前端分组特定密钥并通过双向信道及单向信道发送所述特定密钥给所述终端。

[0018] 进一步地,在上述方法中,所述前端对所述终端进行鉴权的过程如下:所述前端下发鉴权参数给所述终端,所述终端获取到鉴权参数后将鉴权响应结果发送给所述前端,所述前端根据所述鉴权响应结果判断鉴权是否成功。

[0019] 进一步地,在上述方法中,所述前端下发鉴权参数给所述终端时,所述前端通过双向信道及单向信道下发鉴权参数给所述终端。

[0020] 进一步地,在上述方法中,所述前端在所述终端开户时生成一对应所述终端的随机值并发送所述随机值给所述终端,其中所述终端或前端分析所述随机值能得出鉴权参数的个数及各信道传送鉴权参数的个数,所述前端下发鉴权参数给所述终端时,所述前端通过双向信道及单向信道下发鉴权参数给所述终端,所述前端下发鉴权参数前根据分析所述随机值得到的鉴权参数的个数及各信道传送鉴权参数的个数,随机性地确定通过所述双向信道下发和通过所述单向信道下发的具体鉴权参数。

[0021] 进一步地,在上述方法中,所述鉴权响应结果包括鉴权参数和鉴权响应值,判断鉴权是否成功按如下过程进行:所述前端先判断收到的鉴权参数与所述前端储存的鉴权参数是否一致,若不一致,认为所述终端是非法的,鉴权失败,若一致,所述前端再根据鉴权参数算出一鉴权响应值,所述前端判断算出的鉴权响应值与所述终端发送的鉴权响应值是否一致,若一致,鉴权成功,若不一致,鉴权失败。

[0022] 进一步地,在上述方法中,所述前端在发送所述鉴权参数、所述特定密钥给所述终端及所述终端发送鉴权响应结果给所述前端的过程中,发送信息的一端通过所述随机值对发送的信息进行加密处理后再发送,接收信息的一端通过所述随机值对接收到的信息进行解密处理。

[0023] 进一步地,在上述方法中,所述特定密钥为用户密钥或承载业务密钥。

[0024] 进一步地,在上述方法中,所述双向信道为短信信道,所述单向信道为广播信道。

[0025] 本发明也提供一种移动多媒体广播条件接收的系统,所述系统包括:一前端及一终端,所述前端包括一前端业务控制模块、一第一双向信道发送接收模块及一单向信道发送模块,所述终端包括一终端业务控制模块、一第二双向信道发送接收模块及一单向信道接收模块,其中:

[0026] 所述终端业务控制模块,用于在所述终端开户后将请求特定密钥下发的信息发送给所述前端及在所述终端获取到来自所述前端的鉴权参数后将鉴权响应结果通过所述第二双向信道发送接收模块发送给所述前端的第一双向信道发送接收模块;

[0027] 所述前端业务控制模块,用于在所述前端收到所述来自终端的请求特定密钥下发的信息后下发鉴权参数给所述终端及在所述前端收到所述鉴权响应结果后根据所述鉴权响应结果判断鉴权是否成功,若鉴权成功,通过所述第一双向信道发送接收模块及所述单向信道发送模块发送所述特定密钥给所述终端的对应的第二双向信道发送接收模块及所述单向信道接收模块。

[0028] 进一步地,在上述系统中,所述前端包括一前端随机值生成维护模块,所述前端随机值生成维护模块用于在所述终端开户时对应所述终端生成一随机值并通过所述第一双向信道发送接收模块发送所述随机值给所述终端的第二双向信道发送接收模块,其中,所述终端或前端分析所述随机值能得出鉴权参数的个数及各信道传送鉴权参数的个数;

[0029] 所述前端业务控制模块,还用于根据分析所述随机值得到的鉴权参数的个数及各信道传送鉴权参数的个数,随机性地确定通过所述第一双向信道发送接收模块及所述单向信道发送模块下发的具体鉴权参数。

[0030] 相较于现有技术,本发明通过单向信道和双向信道结合的方法实现在鉴权过程中的数据传输,从而提高了信息传输的安全性。

附图说明

[0031] 图 1 为传统的移动多媒体广播条件接收系统框图;

[0032] 图 2 为传统的移动多媒体广播条件接收系统四层密钥示意图;

[0033] 图 3 为本发明较佳实施例移动多媒体广播条件接收的系统框图;

[0034] 图 4 为图 3 中的系统的工作原理流程图;

[0035] 图 5 为本发明较佳实施例移动多媒体广播条件接收的鉴权方法的流程图。

具体实施方式

[0036] 本发明提供了一种移动多媒体广播条件接收的鉴权方法及系统实现在鉴权过程中的数据传输,比单一的广播信道或者简单的双向信道进行数据传输,认证安全性更高。下面结合附图和实施例对本发明进行详细的说明。

[0037] 请参阅图 3,本发明较佳实施例移动多媒体广播条件接收的系统包括一 MMB-CAS 前端 32 及一 MMB-CAS 终端 31,所述 MMB-CAS 前端 32 包括一前端 RAND 生成维护模块 321、一前端业务控制模块 322、一第一短信发送接收模块 323 及一广播发送模块 324。所述 MMB-CAS 终端 31 包括一终端 RAND 维护模块 311、一终端业务控制模块 312、一第二短信发送接收模

块 313 及一广播接收模块 314。所述前端 RAND 生成维护模块 321 用于生成并储存 RAND (随机值), 所述前端业务控制模块 322 用于控制前端的业务操作。MMB-CAS 终端 31 开户时, MMB-CAS 前端 32 的 RAND 生成模块 321 对应该 MMB-CAS 终端 31 生成一 RAND。

[0038] RAND 有一定的有效期, 如果 RAND 过期后, MMB-CAS 前端 32 的前端 RAND 生成维护模块 321 会发短信给 MMB-CAS 终端 31, RAND 经过被分析就知道的鉴权参数的个数以及每个信道传输鉴权参数的个数的信息, RAND 用于加密或解密传输的信息。

[0039] 本发明主要是针对用户注册层以及授权、安全管理层的特定密钥请求进行鉴权时做的安全保护。两层所采用的保护原理是一样的, 下面对鉴权过程进行详细说明。

[0040] 图 4 是本发明较佳实施例移动多媒体广播条件接收的系统的工作原理流程图, 该流程包括步骤:

[0041] S401: MMB-CAS 终端 31 开户时, MMB-CAS 前端 32 的前端 RAND 生成维护模块 321 生成 RAND 并通过第一短信发送接收模块 323 以短信方式发送 RAND 给 MMB-CAS 终端 31 的第二短信发送接收模块 313;

[0042] S402: MMB-CAS 终端 31 如果要请求特定密钥 (用户密钥或业务密钥), 终端业务控制模块 312 通过第二短信发送接收模块 313 以短信方式发送请求给 MMB-CAS 前端 32 的第一短信发送接收模块 323;

[0043] S403: MMB-CAS 前端 32 收到短信后, 前端业务控制模块 322 根据 RAND 分析有几个鉴权参数及每个信道传输鉴权参数的个数确定通过广播发送模块 324 下发和通过第一短信发送接收模块 323 下发鉴权参数的个数, 下发前通过前端 RAND 生成维护模块 321 的 RAND 对鉴权参数进行加密, 这样就可以保证两个信道下发信息的保密, 不容易被对方捕获;

[0044] S404: MMB-CAS 终端 31 的广播接收模块 314 及第二短信发送接收模块 313 收到广播、短信信道信息后, 终端业务控制模块 312 根据终端 RAND 维护模块 311 储存的 RAND 分析鉴权参数个数以及各信道传输的鉴定参数的个数, 这样可以有效的得到消息完整内容, 等完全接收鉴权参数后, 通过 RAND 解密得到所需要的原文。得到原文后, 通过和 MMB-CAS 前端 32 协商的算法, 算出一个鉴权响应值, 然后把鉴权响应结果 (所有的鉴权参数以及鉴权响应值) 通过 RAND 进行加密并通过第二短信发送接收模块 313 以短信方式发送给 MMB-CAS 前端 32 的第一短信发送接收模块 323;

[0045] 通过分析 RAND 可以知道消息的完整内容, 例如: MMB-CAS 前端生成特定的 5 个参数, 这个 5 个参数是不一样的; 分析 RAND 可以知道 2 个信道发送的个数, 具体分配是随机的, MMB-CAS 终端 31 只要根据鉴权参数总数以及 2 个信道各传输的个数就能得到所有参数;

[0046] 具体的运算就是通过一些算法得到鉴权参数对应的鉴权响应值, 例如: MMB-CAS 前端 32 生成 5 个鉴权参数: a_1, a_2, a_3, a_4, a_5 , 算法就是把这些参数作为入参进行一些运算, 例如函数 $F()$;

[0047] $a_1, a_2, a_3, a_4, a_5 \rightarrow F(a_1, a_2, a_3, a_4, a_5) \rightarrow \text{response 值}$;

[0048] S405: MMB-CAS 前端 32 收到来自 MMB-CAS 终端 31 的鉴权参数以及鉴权响应值后, 前端业务控制模块 322 根据 RAND 解密所有的鉴权参数以及鉴权响应值, 然后将收到的鉴权参数与前端业务控制模块 322 储存的鉴权参数对比, 如果参数不一致, 就认为 MMB-CAS 终端 31 是非法的, 直接拒绝 MMB-CAS 终端 31 的请求; 如果一致, 前端业务控制模块 322 根据鉴

权参数以 MMB-CAS 终端 31 同样的算法算出一鉴权响应值,如果 MMB-CAS 前端 32 算出的鉴权响应值与 MMB-CAS 终端 31 算出的鉴权响应值相等,表明鉴权成功,利用一算法来分组特定密钥,采用 RAND 加密然后通过广播发送模块 324 下发和通过第一短信发送接收模块 323 下发已分组的特定密钥。MMB-CAS 终端收到特定密钥后,终端业务控制模块 312 通过同样的算法重组加密的特定密钥,并通过 RAND 解密得到原始的特定密钥。如果鉴权参数合法,鉴权响应值不等,也拒绝 MMB-CAS 终端 31 的请求。

[0049] 图 5 是本发明较佳实施例移动多媒体广播条件接收的鉴权方法的流程图,该方法包括步骤:

[0050] S501:MMB-CAS 终端开户;

[0051] S502:MMB-CAS 前端生成 RAND 并通过短信信道发送 RAND 给 MMB-CAS 终端;

[0052] S503:MMB-CAS 终端请求特定密钥(用户密钥或业务密钥),通过短信信道发送请求给 MMB-CAS 前端;

[0053] S504:MMB-CAS 前端收到请求短信后,根据 RAND 分析有几个鉴权参数及每个信道传输鉴权参数的个数确定通过广播信道下发和通过短信信道下发鉴权参数的个数,下发前通过 RAND 对鉴权参数进行加密,这样就可以保证两个信道下发信息的保密,不容易被对方捕获;

[0054] S505:MMB-CAS 终端接收到鉴权参数时,根据 RAND 分析鉴权参数个数以及各信道传输的鉴定参数的个数,这样可以有效的得到消息完整内容,等完全接收鉴权参数后,通过 RAND 解密得到所需要的原文。

[0055] S506:得到原文后,通过和 MMB-CAS 前端协商的算法,算出一个鉴权响应值,然后把鉴权响应结果(所有的鉴权参数以及鉴权响应值)通过 RAND 进行加密并通过短信信道发送给 MMB-CAS 前端;

[0056] 具体的运算就是通过一些算法得到鉴权参数对应的鉴权响应值,例如:MMB-CAS 前端 32 生成 5 个鉴权参数:a1,a2,23,a4,a5,算法就是把这些参数作为入参进行一些运算,例如函数 F():

[0057] a1,a2,23,a4,a5---->F(a1,a2,23,a4,a5)----->responce 值;

[0058] S507:MMB-CAS 前端收到来自 MMB-CAS 终端的鉴权参数以及鉴权响应值后,根据 RAND 解密所有的鉴权参数以及鉴权响应值,然后将收到的鉴权参数与 MMB-CAS 前端储存的鉴权参数对比,如果参数不一致,就认为 MMB-CAS 终端是非法的,直接拒绝 MMB-CAS 终端的请求;如果一致,前端 MMB-CAS 根据鉴权参数以 MMB-CAS 终端同样的算法算出一鉴权响应值,如果 MMB-CAS 前端算出的鉴权响应值与 MMB-CAS 终端算出的鉴权响应值相等,表明鉴权成功,如果鉴权参数合法,鉴权响应值不等,也拒绝 MMB-CAS 终端的请求。

[0059] S508:鉴权成功后,MMB-CAS 前端利用一算法来分组特定密钥,采用 RAND 加密然后通过广播信道和短信信道下发已分组的特定密钥,例如:一个 200 字节的特定密钥分割为几个包,每个包都会有关联上下 2 个包的信息,然后随机把这些包通过 2 个信道传输,这样终端接收到后,可以一次组包。

[0060] S509:MMB-CAS 终端收到特定密钥后,通过重组加密的特定密钥,并通过 RAND 解密得到原始的特定密钥。

[0061] 通过本发明的技术方案,运用广播信道以及短信信道鉴权使得 UK、SEK 下发很安

全,有效的提高了信息传输的安全性。

[0062] 以上所述仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等,均应包含在本发明的保护范围之内。

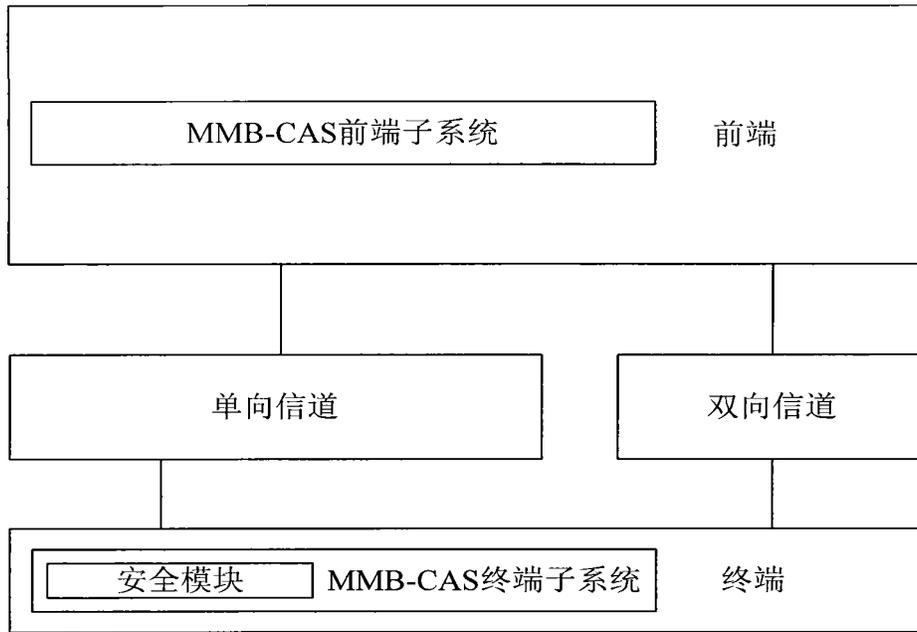


图 1

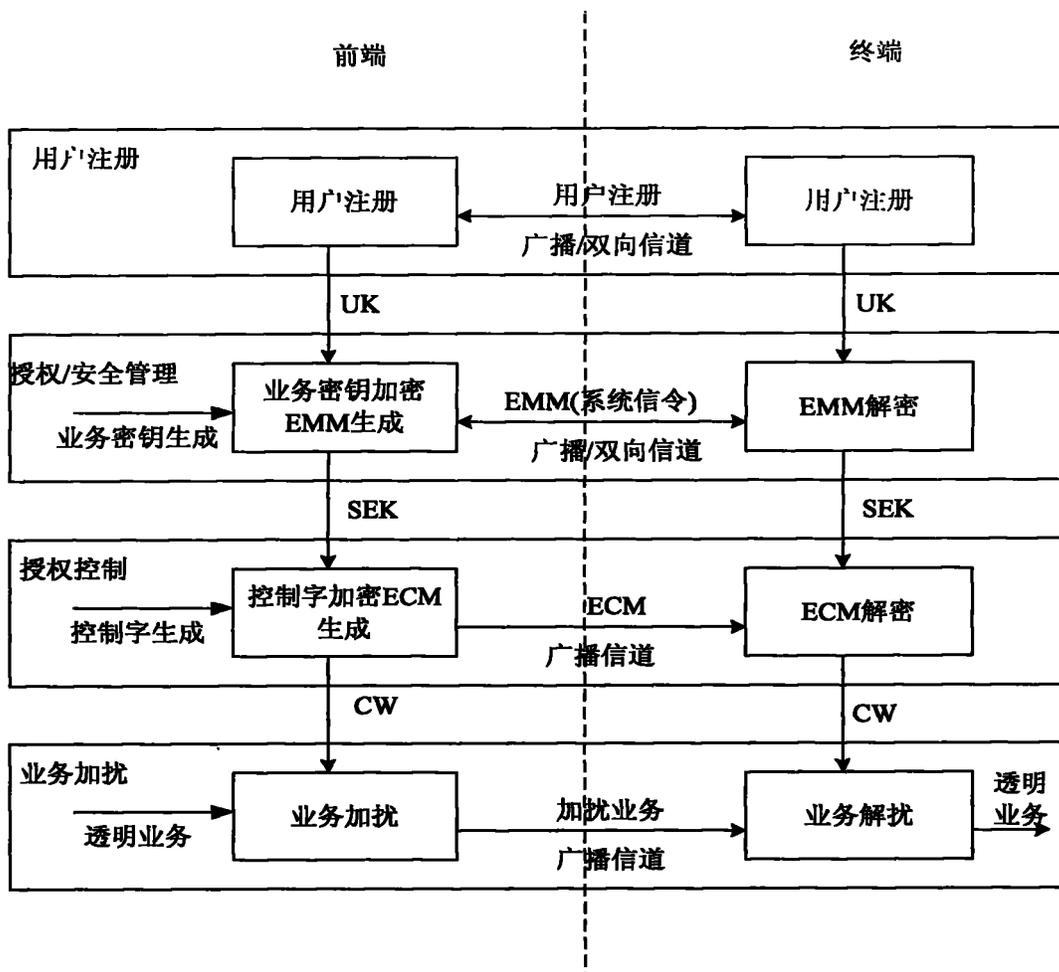


图 2

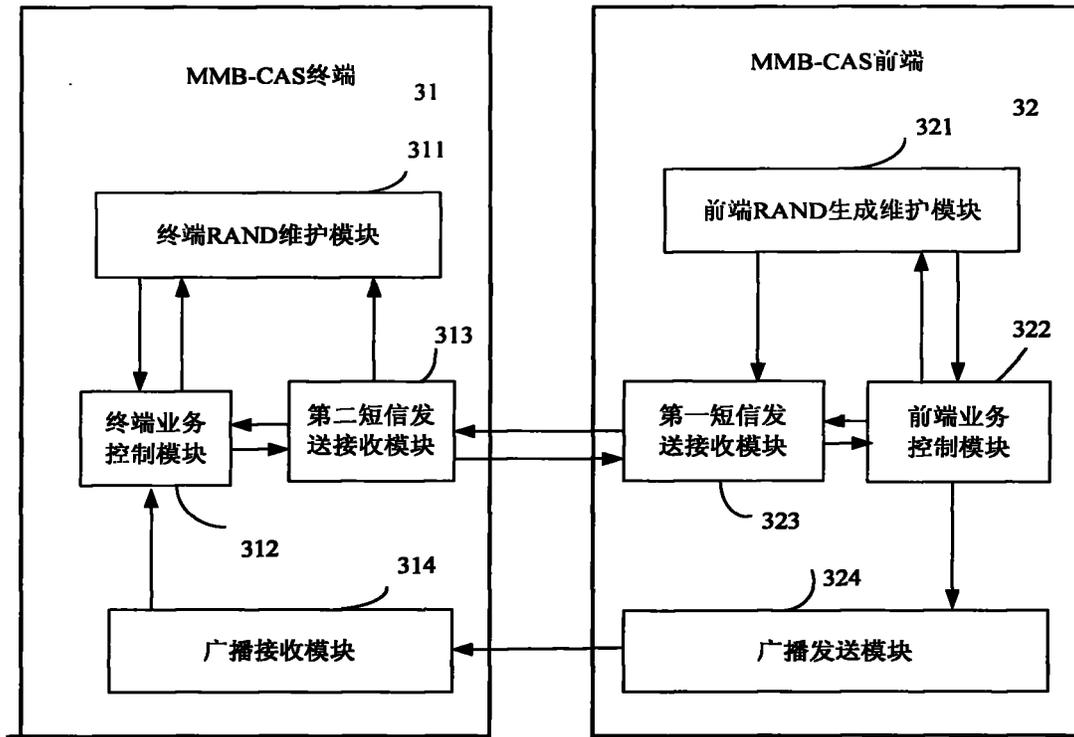


图 3

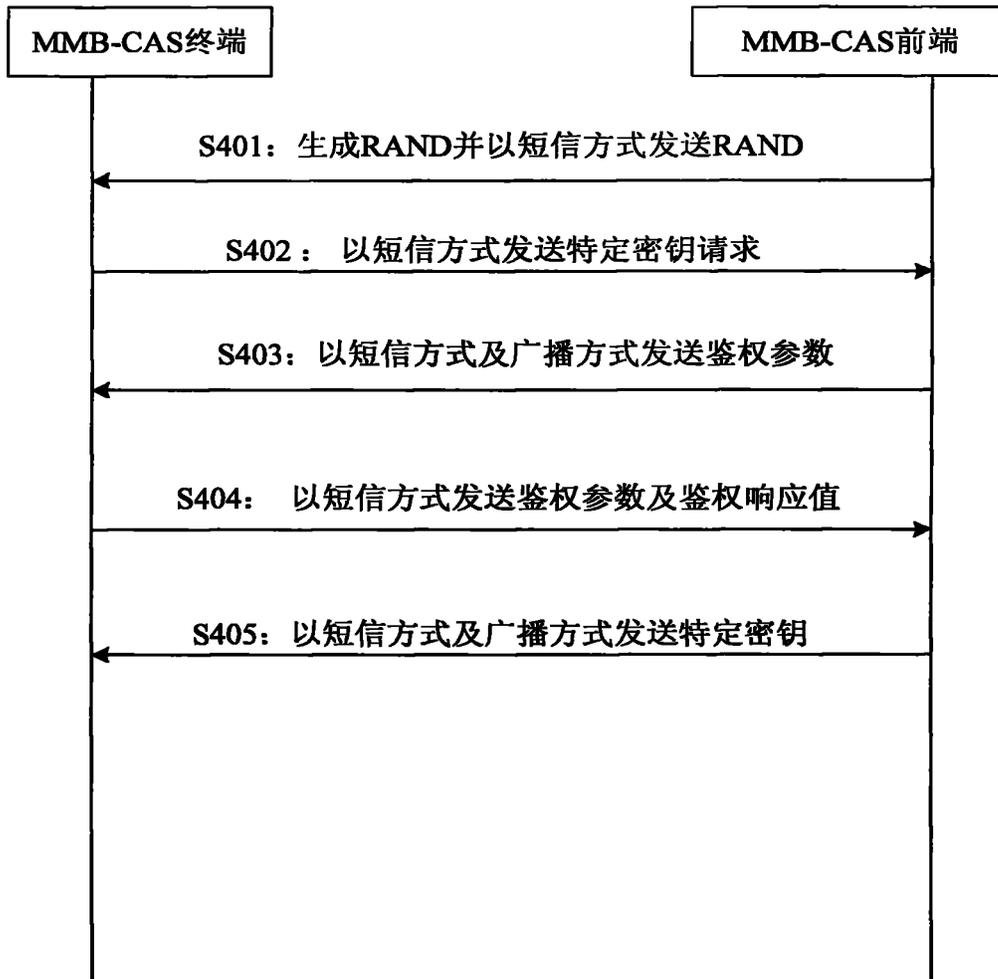


图 4

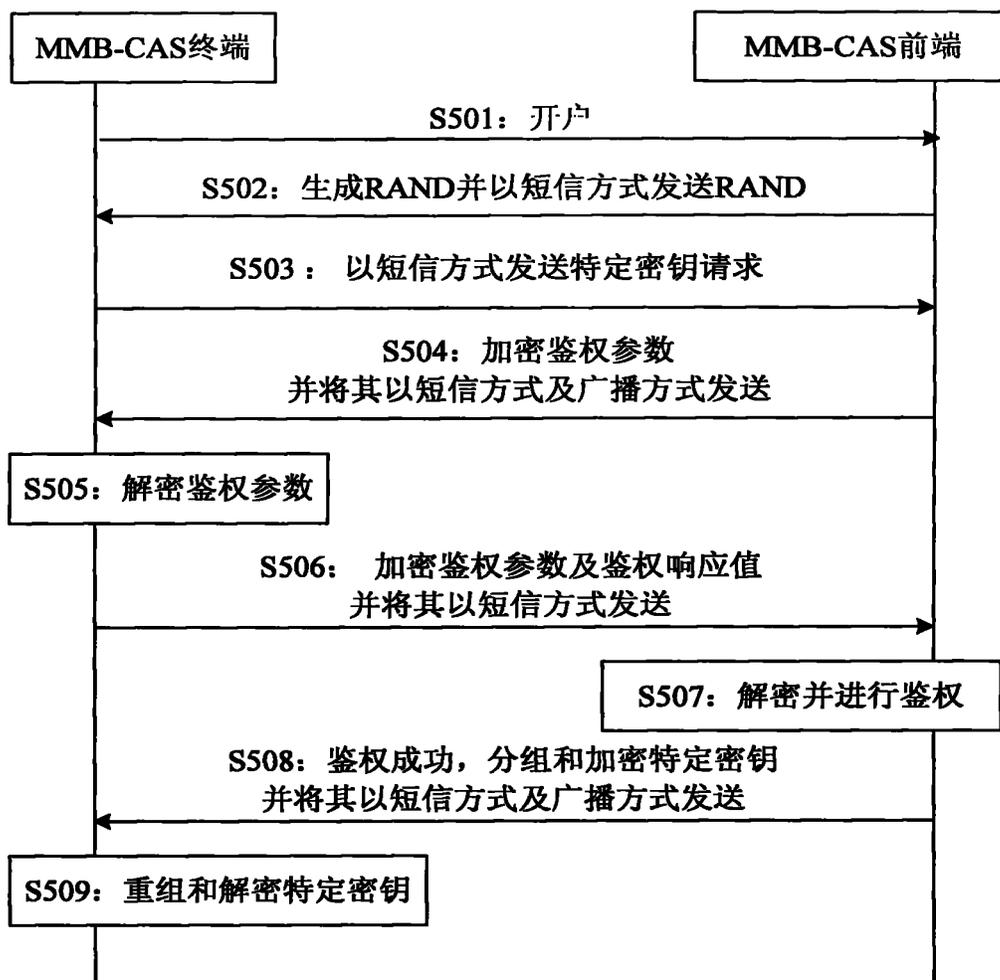


图 5