



(12) 发明专利

(10) 授权公告号 CN 101568070 B

(45) 授权公告日 2012. 11. 28

(21) 申请号 200810093229. 9

(22) 申请日 2008. 04. 23

(73) 专利权人 中兴通讯股份有限公司

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法律部

(72) 发明人 王晔 姚清华 文海龙

(74) 专利代理机构 北京安信方达知识产权代理有限公司 11262

代理人 龙洪 霍育栋

(56) 对比文件

CN 1735192 A, 2006. 02. 15, 全文.

CN 1248837 A, 2000. 03. 29, 权利要求 1-11.

CN 1549595 A, 2004. 11. 24, 权利要求 1-24, 说明书第 10 页 4 行一第 11 页 23 行, 图 1-5.

CN 101145932 A, 2008. 03. 19, 全文.

审查员 王玉婧

(51) Int. Cl.

H04L 9/28 (2006. 01)

H04W 4/06 (2009. 01)

H04W 12/04 (2009. 01)

H04W 88/18 (2009. 01)

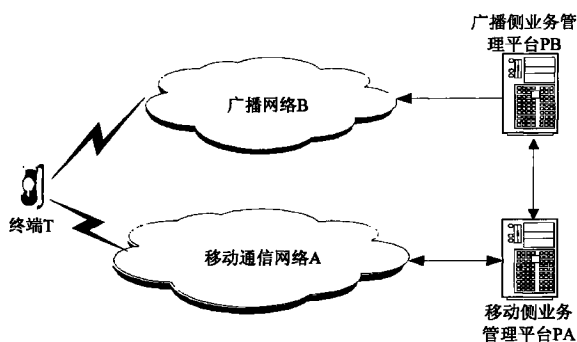
权利要求书 2 页 说明书 5 页 附图 2 页

(54) 发明名称

一种移动终端管理系统和方法

(57) 摘要

一种移动终端管理系统,包括广播侧业务管理平台和移动侧业务管理平台,其中:移动侧业务管理平台,用于保存终端的移动侧身份信息;在终端请求业务密钥时,向广播侧业务管理平台请求所述业务密钥并且在收到后,使用保存的终端的移动侧身份信息加密业务密钥后,发送给终端;广播侧业务管理平台,用于保存终端的广播侧身份信息;在终端通过移动侧业务管理平台请求业务密钥时,用于根据保存的终端的广播侧身份信息加密业务密钥后,发送给移动侧业务管理平台。本发明还公开了一种移动终端管理方法。本发明使得广播侧和移动侧双方既可以同时获取用户数据,又能避免一方绕过另一方的管理平台,从而导致某一方的用户数据不真实而产生的利益损失。



1. 一种移动终端管理系统,其特征在于,所述系统包括广播侧业务管理平台和移动侧业务管理平台,其中:

所述移动侧业务管理平台,用于保存终端的移动侧身份信息;在终端请求业务密钥时,向所述广播侧业务管理平台请求所述业务密钥并且在收到后,使用所述保存的终端的移动侧身份信息加密所述收到的使用广播侧身份信息加密后的业务密钥后,发送给终端;

所述广播侧业务管理平台,用于保存终端的广播侧身份信息;在所述终端通过所述移动侧业务管理平台请求业务密钥时,用于根据所述保存的终端的广播侧身份信息加密所述业务密钥后,发送给所述移动侧业务管理平台,

所述终端的移动侧身份信息包括该终端的移动侧身份编号和其对应的密钥信息;所述终端的广播侧身份信息包括该终端的广播侧身份编号和其对应的密钥信息。

2. 如权利要求 1 所述系统,其特征在于,所述系统还包括被所述移动侧业务管理平台和广播侧业务管理平台管理的终端,所述终端包括存储模块、业务密钥解密模块、播放模块,其中:

所述存储模块,用于保存该终端的移动侧身份信息和该终端的广播侧身份信息,还用于保存该终端解密后的业务密钥;

所述业务密钥解密模块,在所述终端收到所述移动侧业务管理平台发送的加密的业务密钥后,先用保存的该终端的移动侧身份信息解密一次,再用保存的该终端的广播侧身份信息继续解密,得到业务密钥;

所述播放模块,在收到广播网络发送的业务数据后,用所述保存的该终端解密后的业务密钥最终解密所述业务数据,播放收到的业务节目。

3. 如权利要求 1 所述系统,其特征在于,在所述终端的状态发生改变时,所述移动侧业务管理平台还用于发送所述终端的状态改变信息给所述广播侧业务管理平台;所述广播侧业务管理平台收到后,还用于对所述终端的状态改变信息进行确认。

4. 如权利要求 3 所述系统,其特征在于,在所述终端的状态发生改变时,所述移动侧业务管理平台、广播侧业务管理平台用于与所述终端先使用保存的该终端的身份信息互相验证可信任性后,所述移动侧业务管理平台才发送所述终端的状态改变信息给所述广播侧业务管理平台;所述广播侧业务管理平台收到后,对所述终端的状态改变信息进行确认。

5. 一种移动终端管理方法,其特征在于,包括如下步骤:

(1) 在广播侧业务管理平台中设置保存终端的广播侧身份信息;在移动侧业务管理平台中也设置保存所述终端的移动侧身份信息;

(2) 在所述终端通过所述移动侧业务管理平台向所述广播侧业务管理平台请求业务密钥时,所述广播侧业务管理平台根据所述保存的终端的广播侧身份信息加密所述业务密钥后,发送给所述移动侧业务管理平台;

(3) 所述移动侧业务管理平台收到后,使用所述保存的终端的移动侧身份信息加密所述收到的使用广播侧身份信息加密后的业务密钥后,发送给所述终端,

所述终端的移动侧身份信息包括该终端的移动侧身份编号和其对应的密钥信息;所述终端的广播侧身份信息包括该终端的广播侧身份编号和其对应的密钥信息。

6. 如权利要求 5 所述方法,其特征在于,步骤 (1) 中,在所述终端中也设置保存该终端的广播侧身份信息和该终端的移动侧身份信息。

7. 如权利要求 6 所述方法,其特征在于,所述方法还包括如下步骤:

(4) 所述终端收到所述移动侧业务管理平台发送的加密的业务密钥后,先用保存的该终端的移动侧身份信息解密一次,再用保存的该终端的广播侧身份信息继续解密,得到业务密钥后进行保存;

(5) 所述终端在收到广播网络发送的业务数据后,用所述保存的该终端解密后的业务密钥最终解密所述业务数据,播放收到的业务节目。

8. 如权利要求 5 所述方法,其特征在于,步骤 (1) 之后,所述终端的状态发生改变时,所述移动侧业务管理平台发送所述终端的状态改变信息给所述广播侧业务管理平台;所述广播侧业务管理平台收到后,对所述终端的状态改变信息进行确认。

9. 如权利要求 8 所述方法,其特征在于,在所述终端的状态发生改变时,所述移动侧业务管理平台、广播侧业务管理平台与所述终端先使用保存的该终端的身份信息互相验证可信任性后,所述移动侧业务管理平台才发送所述终端的状态改变信息给所述广播侧业务管理平台;所述广播侧业务管理平台收到后,对所述终端的状态改变信息进行确认。

一种移动终端管理系统和方法

技术领域

[0001] 本发明涉及移动多媒体广播技术,尤其涉及一种移动终端管理系统和方法。

背景技术

[0002] 随着网络技术的发展,移动通信网络的功能日益增强,与之相应的手机业务也日益丰富。在此基础上,多媒体音视频业务作为新的业务增长点备受运营商的重视。

[0003] 广播网络可以通过广播方式下发数据,它的特点是带宽资源丰富,缺点是单向通信。移动通信网络是用于给用户丰富服务的网络,它的特点是双向通信,缺点是带宽资源紧张。

[0004] 移动网络和广播网络结合的运营方式,是网络时代的应用热点。这种结合既解决了移动网络无线信道带宽受限的问题,又解决了地面广播信道单向发送不便于信息交互的问题,是手机电视一种比较好的解决方案。

[0005] 但是目前这样的结合方式存在以下的问题:在广播网络运营商和移动网络运营商分离的情况下,只建立一套业务管理平台不利于双方的合作运营。因为不管该业务管理平台放在哪一方维护,对另一方来说,都存在用户数据不透明的情况,会对运营商之间的合作产生影响。

发明内容

[0006] 本发明提供一种移动终端管理系统和方法,使得广播侧和移动侧双方既可以同时获取用户数据,又能避免一方绕过另一方的管理平台,从而导致某一方的用户数据不真实而产生的利益损失。

[0007] 为了解决上述技术问题,本发明提供一种移动终端管理系统,所述系统包括广播侧业务管理平台和移动侧业务管理平台,其中:

[0008] 所述移动侧业务管理平台,用于保存终端的移动侧身份信息;在终端请求业务密钥时,向所述广播侧业务管理平台请求所述业务密钥并且在收到后,使用所述保存的终端的移动侧身份信息加密所述业务密钥后,发送给终端;

[0009] 所述广播侧业务管理平台,用于保存终端的广播侧身份信息;在所述终端通过所述移动侧业务管理平台请求业务密钥时,用于根据所述保存的终端的广播侧身份信息加密所述业务密钥后,发送给所述移动侧业务管理平台。

[0010] 本发明所述系统,其中,所述终端的移动侧身份信息包括该终端的移动侧身份编号和其对应的密钥信息;所述终端的广播侧身份信息包括该终端的广播侧身份编号和其对应的密钥信息。

[0011] 本发明所述系统,其中,所述系统还包括被所述移动侧业务管理平台和广播侧业务管理平台管理的终端,所述终端包括存储模块、业务密钥解密模块、播放模块,其中:

[0012] 所述存储模块,用于保存该终端的移动侧身份信息和该终端的广播侧身份信息,还用于保存该终端解密后的业务密钥;

[0013] 所述业务密钥解密模块,在所述终端收到所述移动侧业务管理平台发送的加密的业务密钥后,先用保存的该终端的移动侧身份信息解密一次,再用保存的该终端的广播侧身份信息继续解密,得到业务密钥;

[0014] 所述播放模块,在收到广播网络发送的业务数据后,用所述保存的该终端解密后的业务密钥最终解密所述业务数据,播放收到的业务节目。

[0015] 本发明所述系统,其中,在所述终端的状态发生改变时,所述移动侧业务管理平台还用于发送所述终端的状态改变信息给所述广播侧业务管理平台;所述广播侧业务管理平台收到后,还用于对所述终端的状态改变信息进行确认。

[0016] 进一步地,在所述终端的状态发生改变时,所述移动侧业务管理平台、广播侧业务管理平台用于与所述终端先使用保存的该终端的身份信息互相验证可信任性后,所述移动侧业务管理平台才发送所述终端的状态改变信息给所述广播侧业务管理平台;所述广播侧业务管理平台收到后,对所述终端的状态改变信息进行确认。

[0017] 本发明还提供一种移动终端管理方法,包括如下步骤:

[0018] (1) 在广播侧业务管理平台中设置保存终端的广播侧身份信息;在移动侧业务管理平台中也设置保存所述终端的移动侧身份信息;

[0019] (2) 在所述终端通过所述移动侧业务管理平台向所述广播侧业务管理平台请求业务密钥时,所述广播侧业务管理平台根据所述保存的终端的广播侧身份信息加密所述业务密钥后,发送给所述移动侧业务管理平台;

[0020] (3) 所述移动侧业务管理平台收到后,使用所述保存的终端的移动侧身份信息加密所述业务密钥后,发送给所述终端。

[0021] 本发明所述方法,其中,步骤(1)中,在所述终端中也设置保存该终端的广播侧身份信息和该终端的移动侧身份信息。

[0022] 进一步地,所述方法还包括如下步骤:

[0023] (4) 所述终端收到所述移动侧业务管理平台发送的加密的业务密钥后,先用保存的该终端的移动侧身份信息解密一次,再用保存的该终端的广播侧身份信息继续解密,得到业务密钥后进行保存;

[0024] (5) 所述终端在收到广播网络发送的业务数据后,用所述保存的该终端解密后的业务密钥最终解密所述业务数据,播放收到的业务节目。

[0025] 本发明所述方法,其中,所述终端的移动侧身份信息包括该终端的移动侧身份编号和其对应的密钥信息;所述终端的广播侧身份信息包括该终端的广播侧身份编号和其对应的密钥信息。

[0026] 本发明所述方法,其中,步骤(1)之后,所述终端的状态发生改变时,所述移动侧业务管理平台发送所述终端的状态改变信息给所述广播侧业务管理平台;所述广播侧业务管理平台收到后,对所述终端的状态改变信息进行确认。

[0027] 进一步地,在所述终端的状态发生改变时,所述移动侧业务管理平台、广播侧业务管理平台与所述终端先使用保存的该终端的身份信息互相验证可信任性后,所述移动侧业务管理平台才发送所述终端的状态改变信息给所述广播侧业务管理平台;所述广播侧业务管理平台收到后,对所述终端的状态改变信息进行确认。

[0028] 本发明在技术上保证了移动多媒体广播业务的开展和使用,在可靠性上,要求广

播网络侧和移动网络侧必须合作才能够保证用户使用业务,从而使得双方可以分享用户数的增长带来的效益。

[0029] 进一步地,本系统还可以应用于一个广播网络管理平台 and 多个移动通信网络管理平台联合运营的情况,在广播网络侧平台唯一,而存在多个移动网络侧平台的情况下,本系统可以最大限度的降低广播网络侧的建设成本和运营成本,也降低了整个系统的复杂度。

[0030] 进一步地,本系统还可以应用于一个移动通信网络管理平台 and 多个广播网络管理平台联合运营的情况,在移动网络侧平台唯一,而存在多个广播网络管理平台的情况下,本系统可以最大限度的降低移动侧平台的建设成本和运营成本,也降低了整个系统的复杂度。

附图说明

[0031] 图 1 是本发明实施例一种移动终端管理系统结构示意图;

[0032] 图 2 是本发明实施例一种被移动侧业务管理平台和广播侧业务管理平台管理的终端结构示意图;

[0033] 图 3 是本发明实施例一种移动终端管理方法流程图。

具体实施方式

[0034] 以下结合附图和具体实施方式对本发明所述技术方案进行详细描述。

[0035] 如图 1 所示,是本发明实施例一种移动终端管理系统结构示意图,该系统包括终端 T(包括各类配合使用的卡)、广播网络 B 对应的广播侧业务管理平台 PB 和移动通信网络 A 对应的移动侧业务管理平台 PA,其中:

[0036] 移动侧业务管理平台 PA,用于保存终端 T 的移动侧身份信息;在终端 T 请求业务密钥时,向所述广播侧业务管理平台 PB 请求所述业务密钥并且在收到后,使用所述保存的终端 T 的移动侧身份信息加密所述业务密钥后,发送给终端 T;上述终端 T 的移动侧身份信息包括该终端 T 的移动侧身份编号和其对应的密钥信息;上述终端 T 的状态包括注册/注销、订购/退订(业务)、暂停/恢复(业务)等;在终端 T 的状态发生改变时,所述移动侧业务管理平台 PA 还用于发送终端 T 的状态改变信息给所述广播侧业务管理平台 PB;

[0037] 广播侧业务管理平台 PB,用于保存终端 T 的广播侧身份信息;在所述终端 T 通过所述移动侧业务管理平台 PA 请求业务密钥时,用于根据所述保存的终端 T 的广播侧身份信息加密所述业务密钥后,发送给所述移动侧业务管理平台 PA;上述终端 T 的广播侧身份信息包括该终端 T 的广播侧身份编号和其对应的密钥信息;广播侧业务管理平台 PB 收到终端 T 的状态改变信息后,还用于对所述终端 T 的状态改变信息进行确认;

[0038] 终端 T,用于保存该终端 T 的移动侧身份信息和该终端 T 的广播侧身份信息,还用于保存该终端 T 解密后的业务密钥;在所述终端 T 的状态发生改变时,用于通过移动侧业务管理平台 PA 向广播侧业务管理平台 PB 发送的终端 T 的状态改变信息进行确认;在终端 T 收到所述移动侧业务管理平台 PA 发送的加密的业务密钥后,先用保存的该终端 T 的移动侧身份信息解密一次,再用保存的该终端 T 的广播侧身份信息继续解密,得到业务密钥;在收到广播网络发送的业务数据后,用所述保存的该终端 T 解密后的业务密钥最终解密所述业务数据,播放收到的业务节目。

[0039] 如图 2 所示,是本发明实施例一种被移动侧业务管理平台和广播侧业务管理平台管理的终端结构示意图,该终端包括存储模块、业务密钥解密模块、播放模块,其中:存储模块,用于保存该终端的移动侧身份信息和该终端的广播侧身份信息,还用于保存该终端解密后的业务密钥;业务密钥解密模块,在所述终端收到所述移动侧业务管理平台发送的加密的业务密钥后,先用保存的该终端的移动侧身份信息解密一次,再用保存的该终端的广播侧身份信息继续解密,得到业务密钥;播放模块,在收到广播网络发送的业务数据后,用所述保存的该终端解密后的业务密钥最终解密所述业务数据,播放收到的业务节目。

[0040] 如图 3 所示,是本发明实施例一种移动终端管理方法流程图,包括如下步骤:

[0041] 步骤 301,在广播侧业务管理平台 PB 中设置保存终端 T 的广播侧身份信息;在移动侧业务管理平台 PA 中设置保存终端 T 的移动侧身份信息;同时,在终端 T 中也设置保存该终端 T 的广播侧身份信息和该终端 T 的移动侧身份信息;终端 T 的移动侧身份信息包括该终端 T 的移动侧身份编号和其对应的密钥信息;终端 T 的广播侧身份信息包括该终端 T 的广播侧身份编号和其对应的密钥信息;

[0042] 上述移动侧业务管理平台 PA 和广播侧业务管理平台 PB 所保存的终端 T 的身份信息是不相同的。上述终端 T 身份信息的保存可以通过预先设置的方式实现(例如制作卡时直接写入),也可以利用双向交互信道协商得出(由于 PB 和终端 T 是单向通信,所以 PB 和终端 T 需要经过 PA 进行双向交互信道协商)。上述终端 T 的移动侧身份信息和终端 T 的广播侧身份信息在终端 T 保存时,其中的身份密钥信息应该以加密的方式(不可直接读取)保存。

[0043] 在终端 T 的状态发生改变时,移动侧业务管理平台 PA 发送终端 T 状态的改变信息给所述广播侧业务管理平台 PB 进行确认。例如,终端 T 注册成功后订购某业务,终端 T 发送请求到 PA,PA 先发送给 PB 进行确认,如果 PB 返回失败响应,则 PA 直接返回拒绝响应;否则,PA 继续处理。在继续处理的过程中,如果 PA 同意终端 T 的订购请求,则返回给终端 T 成功响应,同时通知 PB,该订购请求被同意,PB 保存该订购关系,同时给 PA 返回通知响应,PA 收到响应,保存终端 T 的订购关系;如果 PA 拒绝终端 T 的订购请求,则直接返回失败的响应,同时不再通知 PB。进一步地,如果终端 T 收到的是失败的响应,则说明 PA 和 PB 没有保存终端 T 的订购关系,那么以下步骤中,该终端 T 将不会收到受到加密保护的密钥。

[0044] 在终端 T 的状态发生改变时,PA、PB 还可以与终端 T 使用终端 T 的身份信息来互相验证可信任性。例如,终端 T 发起订购请求给 PA 后,PA 转发给 PB,PB 先生成一个随机数,并用保存的 T 的身份信息加密,随后将随机数和加密信息返回给 PA,PA 将 PB 的随机数作为 T 的请求响应返回,同时用自己保存的 T 的身份信息对 PB 返回的加密信息再一次加密。T 收到第一次响应后,用自己的保存的 PB 侧的身份信息加密随机数,再用保存的 PA 侧的身份信息加密该结果,然后在第二次请求中携带第二次加密随机数的值,PA 收到后,与自己保存的计算结果进行比较,由此,PA 和 PB 可以联合验证终端 T 的可信任性。进一步地,在终端 T 的第二次请求中,还携带一个终端的随机数,PA 收到后发送给 PB,PB 用自己保存的终端 T 的身份信息进行加密计算,然后反馈给 PA,PA 收到后,也用自己保存的终端 T 的身份信息进行加密计算,在第二次响应中返回,终端 T 收到后,先用自己保存的 PB 侧的身份信息加密生成的随机数,再用 PA 侧的身份信息加密,然后与收到的加密值进行比较,由此,终端 T 可以验证 PA 和 PB 的可信任性。如果 PA、PB 与终端 T 互相验证可信任性没有通过,则以后的步

骤中, PA 或者 PB 可以拒绝终端 T 的任何请求。

[0045] 步骤 302, 在终端 T 通过所述移动侧业务管理平台 PA 向所述广播侧业务管理平台 PB 请求业务密钥时, 所述广播侧业务管理平台 PB 根据所述保存的终端 T 的广播侧身份信息加密所述业务密钥后, 发送给所述移动侧业务管理平台 PA;

[0046] 步骤 303, 移动侧业务管理平台 PA 收到后, 使用所述保存的终端 T 的移动侧身份信息加密所述业务密钥后, 发送给所述终端 T;

[0047] 例如, 当终端 T 请求密钥时, PA 会鉴权终端 T 的有效状态, 对于符合发送密钥条件的终端 T (比如该终端 T 已经在 PB 注册, 并订购了某业务时), PA 向 PB 请求终端 T 的业务密钥, PB 收到请求后, 对于符合发送密钥条件的终端 T 用自己保存的身份信息加密业务密钥, 携带在给 PA 的返回响应中, PA 收到后, 再用自己保存的与终端 T 的身份信息对已加密的业务密钥进行再一次的加密保护后才下发该业务密钥。进一步地, 对于不符合发送密钥条件的终端 T, PB 或者 PA 将会直接拒绝终端 T 的获取密钥请求。

[0048] 步骤 304, 终端 T 收到移动侧业务管理平台 PA 发送的加密的业务密钥后, 先用保存的该终端 T 的移动侧身份信息解密一次, 再用保存的该终端 T 的广播侧身份信息继续解密, 得到业务密钥后进行保存;

[0049] 步骤 305, 终端 T 在收到广播网络发送的业务数据后, 用所述保存的该终端 T 解密后的业务密钥最终解密所述业务数据, 播放收到的业务节目。

[0050] 由于解密业务密钥需要用到终端 T 的 PA 侧和 PB 侧的身份信息, 因此对于未保存 PA 侧或 PB 侧的身份信息的终端 T, 即使截获或者取得 PA 或者 PB 平台下发的受保护的密钥信息, 也将无法解出有效的业务密钥, 也就不能进一步解密收到的业务数据, 从而使用该业务。

[0051] 本方法在保证业务可以运营管理的条件下, 通过向用户终端确认两种不同的身份信息的方法, 确保双平台可以联合管理业务。这种方法很好的保证了双方运营平台对于用户数据和业务使用数据的透明性, 促进了移动多媒体广播业务的良性发展。

[0052] 本方法如前所述, 在多个内容运营商和多个移动网络运营商并存的情况下, 每一个运营商只需要建立一个自己的业务管理平台, 就可以和其它多个对应运营商合作, 节约了成本和网络复杂度, 利于业务更好的推广。

[0053] 以上所述仅为本发明的优选实施例而已, 并不用于限制本发明, 对于本领域的技术人员来说, 本发明可以有各种更改和变化。凡在本发明的精神和原则之内, 所作的任何修改、等同替换、改进等, 均应包含在本发明的保护范围之内。

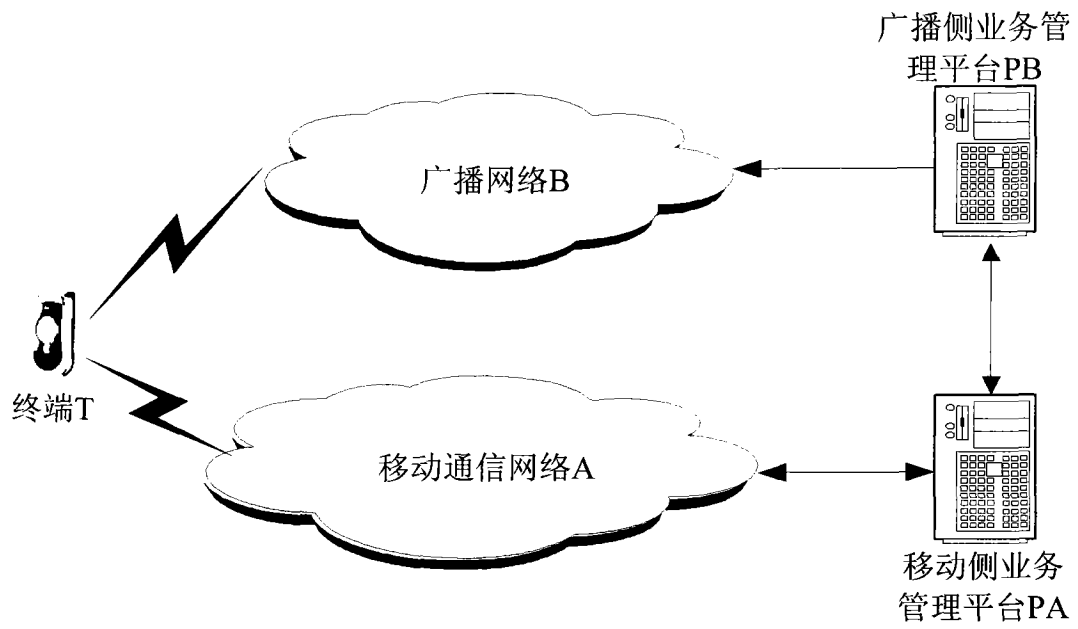


图 1

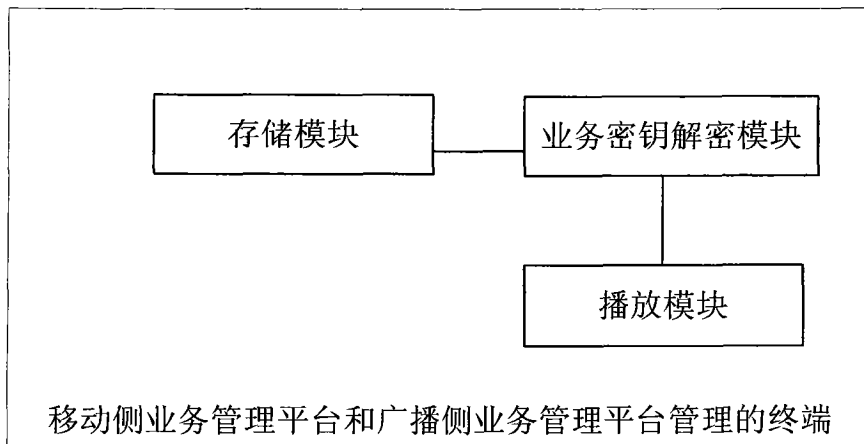


图 2

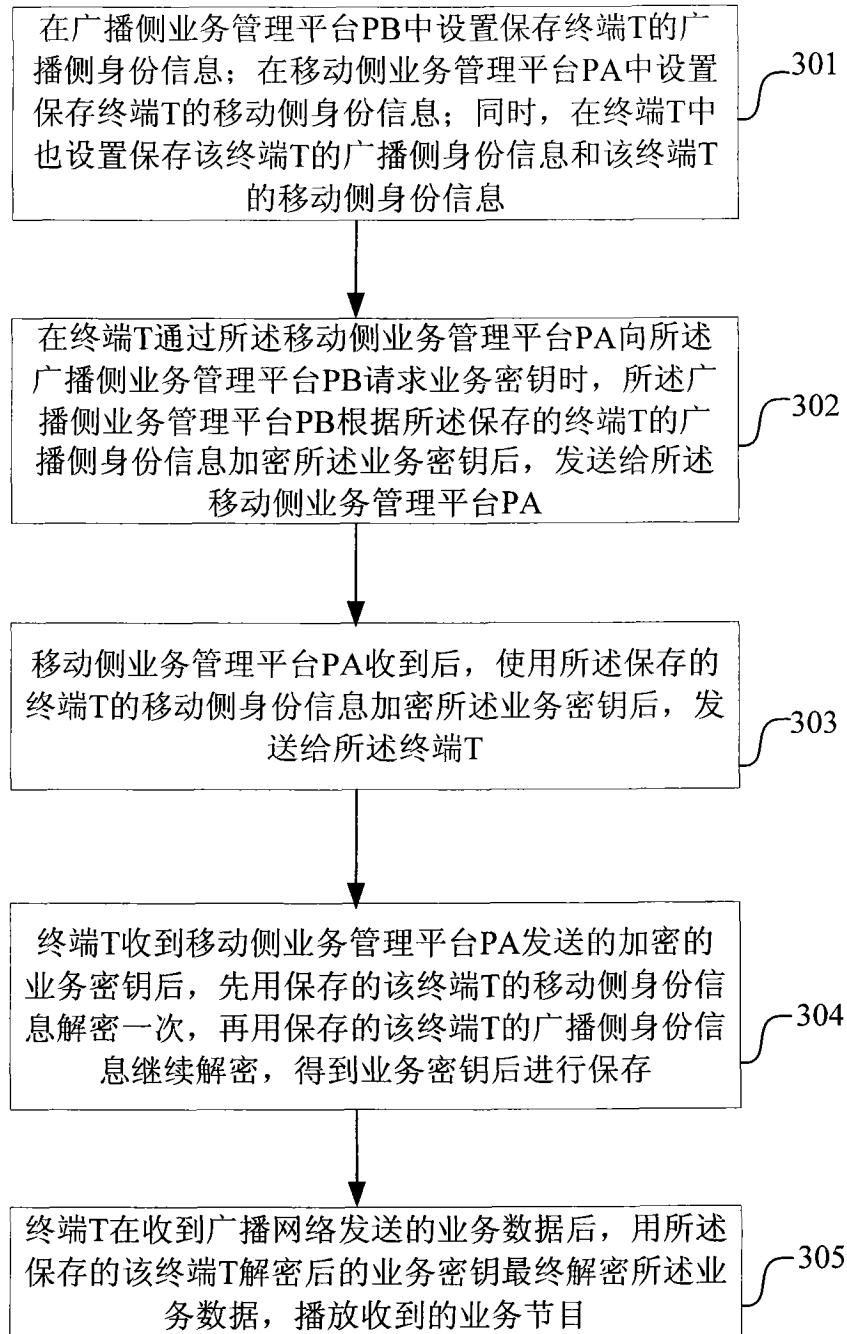


图 3