(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 101247508 B
(45)授权公告日 2011.05.11

(21)申请号 200810101540.3

(22)申请日 2008.03.07

(73)专利权人 盛志凡
地址 100032 北京市西城区复兴门外大街 2 号
专利权人 李慧镝
易鹏
王幼君
王同洋
刘达

(72)发明人 王军 盛志凡 李慧镝 易鹏 王幼君 王同洋 刘达

(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健

(51)Int.Cl.
H04N 21/266(2011.01)
H04N 21/254(2011.01)
H04N 21/4623(2011.01)

审查员 张冰青

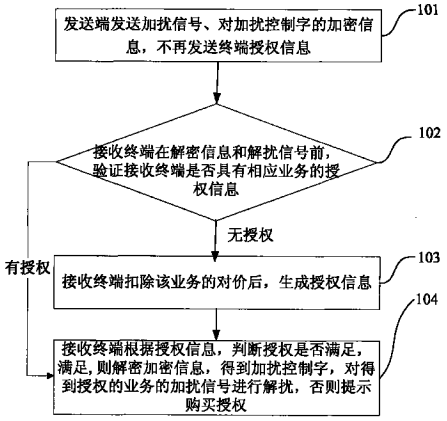
权利要求书 2 页 说明书 5 页 附图 2 页

(54)发明名称

有条件接收系统中终端实现业务授权的方法

(57)摘要

本发明公开了一种有条件接收系统中终端实现业务授权的方法，用于在没有发送端授权的情况下收看业务。步骤 A：发送端发送加扰信号、对加扰控制字的加密信息，不再发送终端授权信息；步骤 B：接收终端在解密信息和解扰信号前，验证接收终端是否具有相应业务的授权信息，无授权，则进入步骤 C；有授权，则进入步骤 D；步骤 C：接收终端扣除该业务的对价后，生成授权信息；步骤 D：接收终端根据授权信息判断授权是否满足，满足则，解密所述的加密信息，得到所述加扰控制字，对得到授权的业务的加扰信号进行解扰，否则提示购买授权。本发明能在窄带广播系统中实现有条件接收；有利于用户更加灵活的接收和订购窄带广播业务。



CN 101247508 B

1. 一种有条件接收系统中终端实现业务授权的方法，其特征在于，包括如下步骤：

步骤 A：发送端发送加扰信号、对加扰控制字的加密信息，与信号对应的各种业务和业务费率的信息，不再发送终端授权信息；

步骤 B：接收终端在解密信息和解扰信号前，验证接收终端是否具有相应业务的授权信息，无授权，则进入步骤 C；有授权，则进入步骤 D；

步骤 C：接收终端扣除该业务的对价后，生成授权信息；

步骤 D：接收终端根据授权信息判断授权是否满足，满足，则解密所述的加密信息，得到所述加扰控制字，对得到授权的业务的加扰信号进行解扰；否则提示购买授权。

2. 如权利要求 1 所述的方法，其特征在于，

步骤 C 具体为：用户通过接收终端定购相应的业务；接收终端根据用户购买业务的费率信息计算费用，并从接收终端的电子钱包中扣除该费用后，生成授权信息。

3. 如权利要求 1 所述的方法，其特征在于，

步骤 C 具体为：接收终端扣除该业务的授权标识后，生成授权信息。

4. 如权利要求 1 所述的方法，其特征在于，所述对加扰控制字的加密信息包括：

授权控制信息包含利用业务密钥 SK 对加扰控制字加密处理的密文；

授权管理信息包含利用用户个人分配密钥对业务密钥 SK 加密处理的密文，不包括终端授权信息。

5. 如权利要求 2 所述的方法，其特征在于，所述与信号对应的各种业务和业务费率的信息对所有接收终端是相同的。

6. 如权利要求 2 所述的方法，其特征在于，接收终端将接收到的所述与信号对应的各种业务和业务费率的信息存储于接收终端，在步骤 C 中调用存储的费率信息进行计算；或在步骤 C 中调用步骤 A 中下发的费率信息。

7. 如权利要求 1 或 2 或 3 所述的方法，其特征在于，所述授权信息包括用户使用业务的方式信息。

8. 如权利要求 7 所述的方法，其特征在于，所述用户使用业务的方式为一段时间内用户使用业务的权限、或用户使用业务的时长或次数。

9. 如权利要求 2 所述的方法，其特征在于，所述各种业务和 / 或业务费率的信息通过

a 发送端下传业务和 / 或业务费率信息的密文，接收终端进行解密，或

b 发送端同时下传业务和 / 或业务费率信息的明文和消息验证码，接收终端进行消息验证码验证，或

c 发送端同时下传业务和 / 或业务费率信息的密文和消息验证码，接收终端进行解密和消息验证码验证，来保证业务和 / 或业务费率信息的完整性。

10. 如权利要求 2 或 9 所述的方法，其特征在于，所述各种业务和 / 或业务费率的信息通过逻辑广播信道

a 电子服务指南，或

b 授权控制信息，或

c 授权管理信息，下传。

11. 如权利要求 2 所述的方法，其特征在于，所述与信号对应的各种业务和业务费率的信息作为一个整体信息一起下发，或者将业务信息和业务费率信息分别作为一个整体信息

下发。

有条件接收系统中终端实现业务授权的方法

技术领域

[0001] 本发明涉及有条件接收技术，尤其涉及广播领域的有条件接收系统中实现终端业务授权的方法。

背景技术

[0002] 有条件接收 (CA，Conditional Access) 系统是开展付费电视、广播服务的核心技术，就是保证合法的用户（称之为授权者）能够接收音、视频节目和数据服务业务，而对于非法用户则无法获取相关信号。付费服务有条件接收是由两个相互独立的关键部分，即对信号的加解扰和接收控制信息加解密组成，其中解扰、解密无疑是一个对安全性要求很高的信息处理过程。

[0003] 有条件接收经历了两代的发展，第一代的特征是以设备为基础，一般用于模拟系统。为了实现有线电视的有效收费，在发送端将模拟信号进行加扰，使普通电视机无法收看，只有安装了解扰器的用户接收终端才能正常收看。这样的系统可以通过发送端的寻址来控制单个用户的解扰器开关。系统可实现全频段加扰和频道加扰，实现的方法通常是采用视频倒相、水平同步重叠、垂直同步重叠、数字随机视频行抖动等技术，该种方式下通常会对信号产生损耗。

[0004] 第二代的基本原理是采用加扰控制字 (CW，Control Word) 加密传输的方法，用户接收终端利用智能卡解密。由于采用的是数字技术，对信号没有损耗，系统的保密性、可靠性均大大提高。对传输流的加扰，有些系统如数字电视广播 (DVB，Digital Video Broadcasting) 已有标准；对控制字的加密算法一般采用 RSA（由 Rivest、Shamir、Adleman 所提出）以及 3DES（数据加密标准，Data Encryption Standard) 算法，对加密体制，不同系统差别很大，其技术大体有两种：一种是以爱迪德系统为代表的密码循环体制，另一种是以 NDS 系统为代表的利用专有算法来进行保护。

[0005] 在第一代有条件接收系统中，由于系统的密钥体系依赖于设备及解扰器，信号比较容易破解和复制。而第二代，由于加密系统、密钥体系与设备是分开的，依靠智能卡提供加、解密的安全性来保障系统的安全，破解难度有所提高。

[0006] 同时，在第二代有条件接收系统的密钥体系设计中，不同的接收终端使用不同的密钥，并且因为不同接收终端定制的节目各不相同，所以发送端需要为每个接收终端，生成不同的授权控制信息。这样的设计虽然在系统安全性上有所加强，但是付出的代价是授权控制信息随着用户的增加而大幅上升，加重了发送端的负载，占用了大量的带宽，降低了系统的效率。在用户数量巨大，同时系统带宽有限的条件下，如无线广播系统，第二代有条件接收系统的方案是不适应此类系统要求的。另外，目前收看各个节目需要提前获得授权，不能根据用户需要立刻开通相应的节目，给用户的使用带来不便利。

发明内容

[0007] 本发明提供一种有条件接收系统中实现终端业务授权的方法，用以解决现有技术

中因不能克服在授权控制信息的管理过程中，随着用户数量的增加而大幅度加重发送端的负载、占用大量的带宽的困难，不能在窄带广播中实现有条件接受业务和不能及时开通相应业务的问题。

[0008] 本发明提供了一种有条件接收系统中实现终端业务授权的方法，包括如下步骤：

[0009] 步骤 A：发送端发送加扰信号、对加扰控制字的加密信息，不再发送终端授权信息；

[0010] 步骤 B：接收终端在解密信息和解扰信号前，验证接收终端是否具有相应业务的授权信息，无授权，则进入步骤 C；有授权，则进入步骤 D；

[0011] 步骤 C：接收终端扣除该业务的对价后，生成授权信息；

[0012] 步骤 D：接收终端根据授权信息，解密所述的加密信息，得到所述加扰控制字，对得到授权的业务的加扰信号进行解扰。

[0013] 较佳的，所述步骤 A：发送端还发送与信号对应的各种业务和业务费率的信息；步骤 C 具体为：用户通过接收终端定购相应的业务；接收终端根据用户购买业务的费率信息计算费用，并从接收终端的电子钱包中扣除该费用后，生成授权信息。

[0014] 较佳的，步骤 C 具体为：接收终端扣除该业务的授权标识后，生成授权信息。

[0015] 较佳的，所述对加扰控制字的加密信息包括：

[0016] 授权控制信息包含利用业务密钥 SK 对加扰控制字加密处理的密文；

[0017] 授权管理信息包含利用用户个人分配密钥对业务密钥 SK 加密处理的密文，不包括终端授权信息。

[0018] 较佳的，所述与信号对应的各种业务和业务费率的信息对所有接收终端是相同的。

[0019] 较佳的，接收终端将接收到的所述与信号对应的各种业务和业务费率的信息存储于接收终端，在步骤 C 中调用存储的费率信息进行计算；或在步骤 C 中调用步骤 A 中下发的费率信息。

[0020] 较佳的，所述授权信息包括用户使用业务的方式信息，还可以包括用户使用业务方式对应的价格、用户身份信息；所述用户使用业务的方式可以为一段时间内用户使用业务的权限、或用户使用业务的时长或次数。

[0021] 较佳的，所述业务和 / 或业务费率信息通过

[0022] a 发送端下传业务和 / 或业务费率信息的密文，接收终端进行解密，或

[0023] b 发送端同时下传业务和 / 或业务费率信息的明文和消息验证码，接收终端进行消息验证码验证，或

[0024] c 发送端同时下传业务和 / 或业务费率信息的密文和消息验证码，接收终端进行解密和消息验证码验证，来保证费率信息的完整性。

[0025] 较佳的，所述业务和 / 或业务费率信息通过逻辑广播信道 a 电子服务指南，或 b 授权控制信息，或 c 授权管理信息，下传。

[0026] 较佳的，所述与信号对应的各种业务和业务费率的信息作为一个整体信息一起下发，或者将业务信息和业务费率信息分别作为一个整体信息下发。

[0027] 发送端不再发送与用户相关的授权控制信息，减少了大量带宽占用的问题本使得本发明更始于在窄带广播系统中实现有条件接收；同时通过终端用户自己订阅需要的业务

信号，不再受控于发送端统一控制，有利于用户更加灵活的接收和订购窄带广播业务，享受更加良好的用户体验和服务质量；同时也有利于服务提供商更大范围的推广广播业务，发展用户数量和促进接收终端的大面积普及。

[0028] 本发明有益效果如下：

[0029] 由于窄带广播系统存在带宽有限的不足，因此虽然潜在用户数量巨大，但是现有技术并不能克服在授权控制信息的管理过程中，随着用户的增加而大幅度加重发送端的负载、占用大量的带宽、系统效率低下的事实。

[0030] 由于在本发明中，使用电子钱包进行业务购买和终端自授权，从而解决了现有技术对每一用户采用不同的信息管理发送所需的带宽，同时将现有技术中通过发送端来对用户进行管理的方式，变化为对用户的管理主要建立在接收终端一侧，从接收终端一侧安全性的提高来满足有条件接收的安全性要求，从而解决了因对用户的管理造成的带宽占用问题，实现了对数量巨大的窄带广播用户的有条件接收服务。同时，本发明将安全性的管理转移至接收终端一侧，因此实质上不仅仍旧能够满足有条件接受的安全性要求，而且本发明中对终端的管理更加灵活方便，用户使用相关业务时也更加便捷。另外，也能够更加方便的利用技术的进步不断提高对有条件接收的安全性。

附图说明

[0031] 图 1 为实施例中有条件接收系统中终端实现业务授权的方法示意图；

[0032] 图 2 为实施例中所述使用电子钱包通过用户交互购买业务实现终端自授权流程示意图；

具体实施方式

[0033] 下面结合附图对本发明的具体实施方式进行说明。

[0034] 图 1 为有条件接收系统中终端实现业务授权的方法示意图，如图所示，实施步骤为：

[0035] 步骤 101、发送端发送加扰信号、对加扰控制字的加密信息，不再发送终端授权信息，其中，加密信息包括授权控制信息 (Entitlement Control Message，ECM) 和授权管理信息 (Entitlement Management Message，EMM)；

[0036] 步骤 102、接收终端在解密信息和解扰信号前，验证接收终端是否具有相应业务的授权信息，无授权，则进入步骤 103；有授权，则进入步骤 104；

[0037] 步骤 103、接收终端扣除该业务的对价后，生成授权信息；

[0038] 步骤 104、接收终端根据授权信息判断是否满足授权，满足，则解密所述的加密信息，得到所述加扰控制字，对得到授权的业务的加扰信号进行解扰；否则，提示购买授权。

[0039] 由实施中可见，必须实现终端自授权，才能收看相应业务。

[0040] 在发送端发送的数据中共涉及三种数据，一是加扰后的码流，二是加密信息，包括授权控制信息 (ECM) 和授权管理信息 (EMM)，三是与信号对应的各种业务和业务费率的信息，不再发送终端授权信息。其中加扰后的码流就是利用加扰控制字对传输的码流进行加扰；授权控制信息 (ECM) 包含利用业务密钥 SK 对加扰控制字加密处理的密文，与用户信息无关，对所有的接收终端都是相同的，ECM 占用的下传带宽不随用户数量的增加而变化；授

权管理信息(EMM)包含利用用户个人分配密钥对业务密钥SK加密处理的密文,不包括终端授权信息,与用户信息相关,EMM占用的下传带宽随用户数量的增加而增加;与信号对应的各种业务和业务费率的信息对所有接收终端是相同的,与用户信息无关,其占用的下传带宽不随用户数量的增加而变化,业务可以是频道或其组合,也可以是一段播放的节目或其组合,当然也可以是频道和节目的组合,业务费率信息是业务使用方式的费率,例如可以是每个频道一段时间内的费用,如包月费、季度费、年费等,也可以是使用每一频道一次的费用或使用该业务每分钟/小时等的费用,为方便开展业务也可以是将几个频道组合起来,例如体育频道和影视频道各种使用方式的费率,在此不一一列举。通过上述变化发送端发送的数据与用户信息关联性大幅度减少,占用的下传带宽也可以大幅度减少。

[0041] 与信号对应的各种业务和业务费率的信息通过逻辑广播信道电子服务指南(Electronic Service Guide,ESG)或授权控制信息ECM或授权管理信息EMM,向接收终端下传。当然,可以将业务信息和业务费率信息作为一个整体信息一起下发,也可以将业务信息和业务费率信息分别作为一个整体信息各自分别通过逻辑广播信道下发。

[0042] 与信号对应的各种业务和/或业务费率的信息的下传需要保证数据的完整性。有三种方式保证信息完整性,一是只下传信息的密文,接收终端收到后进行对应的解密;二是同时下传信息的明文和消息验证码(MAC),接收终端收到后进行消息码验证;三是同时下传信息的密文和消息验证码(MAC),接收终端收到后进行解密和消息码验证。

[0043] 接收终端接收到上述数据,可以将接收到的与信号对应的各种业务和业务费率的信息存储于接收终端,在扣除业务对价时直接调用,以便减少接收终端的信息处理量,当然,也可以不存储,在需要调用时直接从下传的数据中解析出来,但是这样会增加接收终端的信息处理量。

[0044] 接收终端在解密信息和解扰信号前,验证接收终端是否具有相应业务的授权信息,如果没有,接收终端扣除该业务的对价后,生成授权信息。接收终端通过与用户交互,由用户确定其购买的业务和使用业务方式,并根据业务的费率信息确定需要扣除的对价,扣除的对价可以为电子货币形式,从接收终端的电子钱包中扣除;扣除的对价也可以是该业务的授权标识,例如标识可以观看2小时影视的授权码。在扣除对价后,生成对该业务的授权信息。授权信息可以包括用户使用业务的方式信息,具体根据用户购买业务的使用方式来确定,还可以包括用户使用业务方式对应的价格、用户身份信息;用户使用业务的方式可以为一段时间内用户使用业务的权限(如某一个月、季度、年度内)、或用户使用业务的时长或次数。

[0045] 接收终端根据授权信息判断是否满足授权,满足,则解密所述的加密信息,得到所述加扰控制字,对得到授权的业务的加扰信号进行解扰;否则,提示购买授权。如生成的授权信息为某一段时间内的权限,则判断是否超出该时间范围;如生成的授权信息为时长或使用次数,则判断时长或使用次数是否用完,具体实现可以为记录使用的时长或使用次数,并与授权信息进行比较,当然,也可以是根据使用情况,更新授权信息。具体的判断方法在此不一一列举,只要能够判断授权是否满足均可。

[0046] 下面结合图2详细描述通过用户交互确定购买业务并使用电子钱包扣除费用实现终端授权,用户进行购买业务时,可以提供多种购买启动方式,如:主动购买,用户进入购买界面,选择需要购买的业务和使用方式,进行购买授权;或者是查看某一频道时,验证是

否具有授权，无授权则提供购买界面，由用户选择购买。具体实施步骤为：

[0047] 步骤 401、接收终端在验证解密、解扰数据所属业务的授权信息失败后，发起用户交互购买业务授权过程；

[0048] 步骤 402，终端应用获取业务和业务费率信息，通过用户界面向用户显示业务包括的内容，使用方式和收费费率等数据；

[0049] 步骤 403，用户通过用户界面选择订购中意的业务和使用方式，终端应用会将用户的选择情况传递给终端；

[0050] 步骤 404、根据用户的选择情况和对应的费率信息，计算用户购买业务所需费用，并向电子钱包模块发送扣减费用的命令；

[0051] 步骤 405、电子钱包模块响应命令，实施扣减费用动作并返回消息，如果扣减失败，同时返回失败原因；

[0052] 步骤 406、接收到扣减成功消息后，生成对该业务的授权信息；接收到扣减失败消息后，通过用户界面提示用户失败原因。

[0053] 授权信息包括用户使用一种或多种业务的权限、或用户使用业务的时长或次数以及用户购买业务的价格、和 / 或用户身份信息，具体根据用户选择的发送端发送的业务和业务费率信息决定。

[0054] 生成业务的授权信息所扣减的费用从接收终端的电子钱包中扣除，这样可以更好的保证安全性。

[0055] 通过用户交互可以由用户方便的购买自己需要的业务，比如可以分别购买自己喜欢收看的体育节目或影视节目，这时只需要用户购买此两类业务并支付相应的费用即可获得授权信息进行收看，而不必支付自己不喜欢收看的其他节目的费用。

[0056] 由上述实施可知，本发明能在窄带广播系统中实现有条件接收，解决了现在有条件接收方式下授权控制信息与用户相关需要占用大量带宽的问题；并进一步通过在终端实现业务购买和终端自授权，为窄带广播系统的运营带来方便；有利于用户更加灵活的接收和订购窄带广播业务，享受更加良好的用户体验和服务质量；同时也有利于服务提供商更大范围的推广广播业务，发展用户数量和促进接收终端的大面积普及。

[0057] 本发明的精神在于，在有条件接收的安全体系上，实现终端的业务购买和终端自授权，不再依靠通过发送端进行控制，满足有条件接收的授权安全要求，从而节省了对终端控制所带来的巨大带宽消耗，也因此使得有条件接收能够在窄带广播系统中运用。显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若对本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

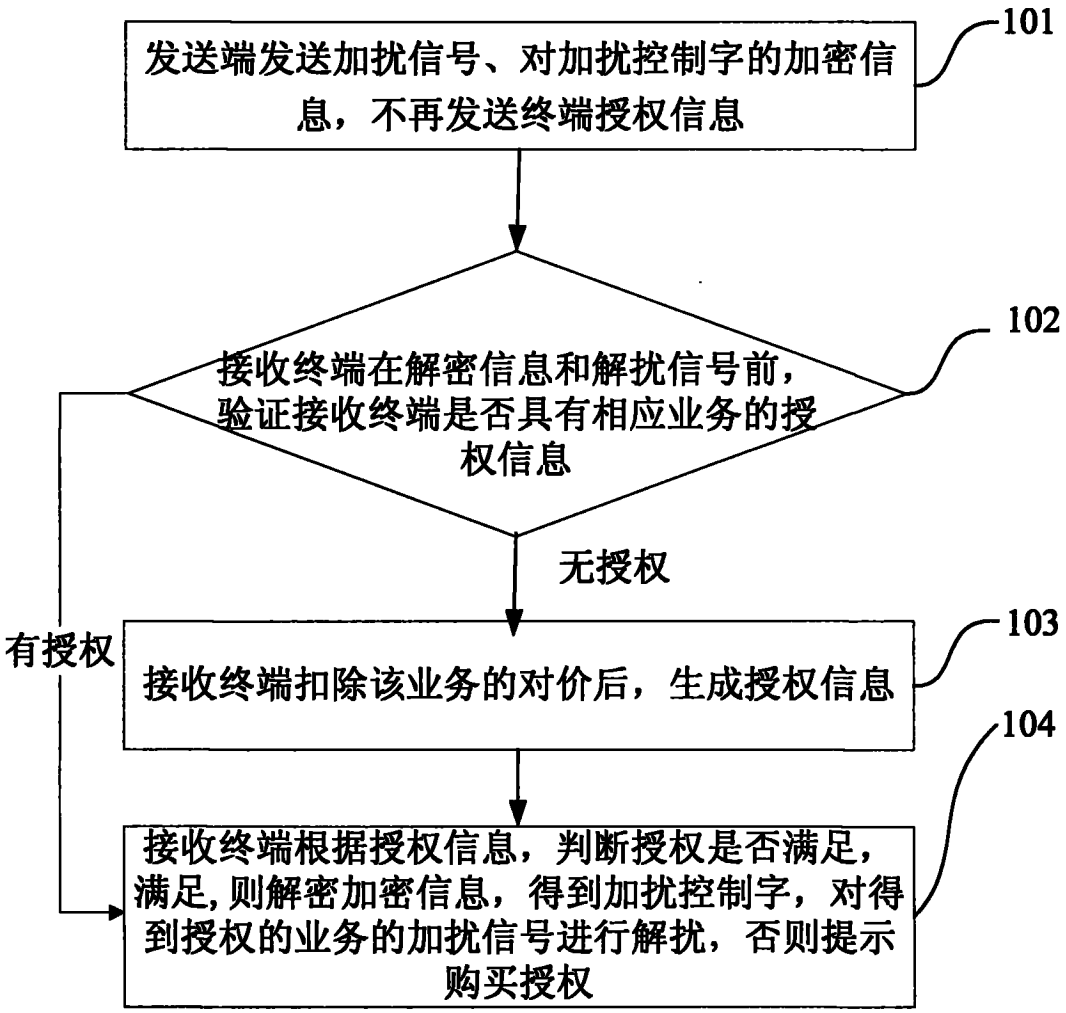

发送端发送加扰信号、对加扰控制字的加密信息，不再发送终端授权信息
101
接收终端在解密信息和解扰信号前，验证接收终端是否具有相应业务的授权信息
102
无授权
有授权
接收终端扣除该业务的对价后，生成授权信息
103
接收终端根据授权信息，判断授权是否满足，满足，则解密加密信息，得到加扰控制字，对得到授权的业务的加扰信号进行解扰，否则提示购买授权
104

图 1

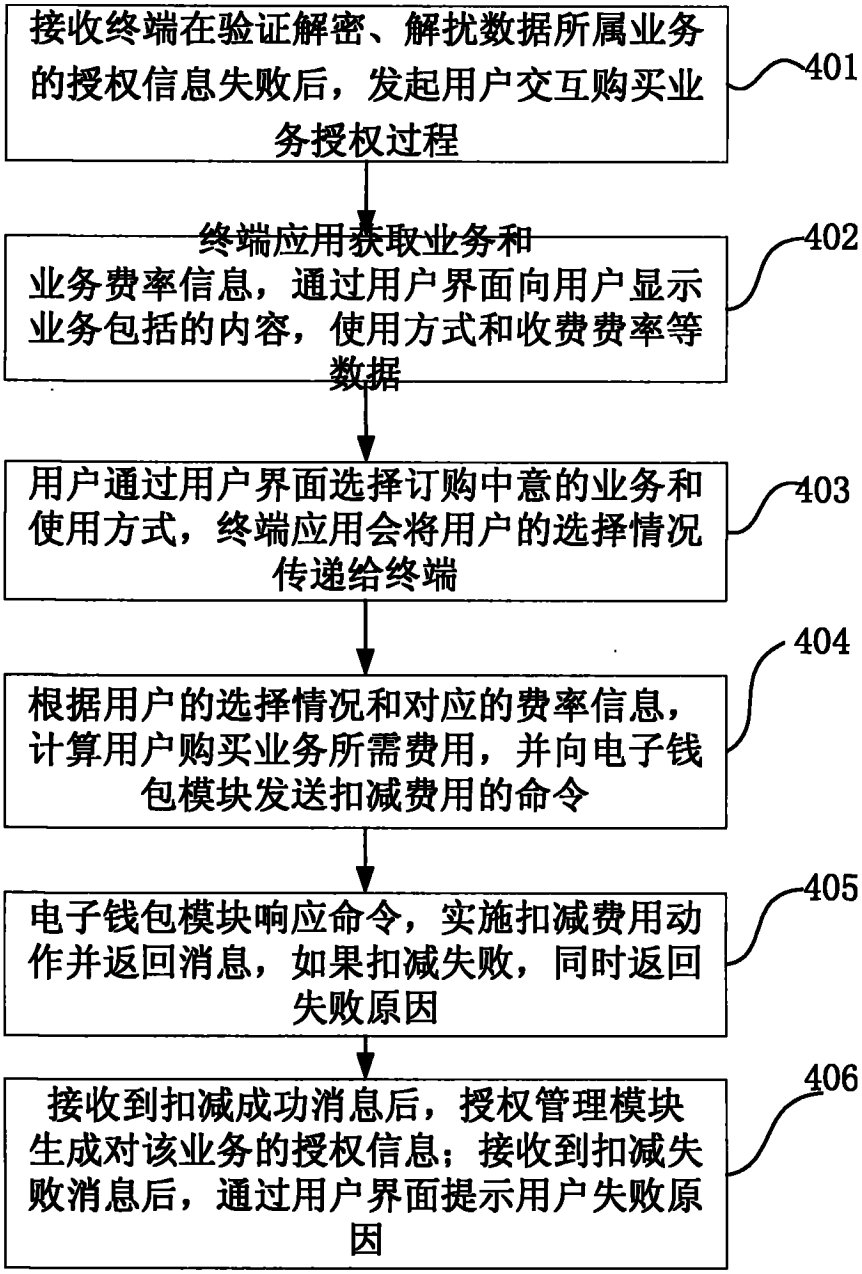

接收终端在验证解密、解扰数据所属业务的授权信息失败后，发起用户交互购买业务授权过程
401
终端应用获取业务和业务费率信息，通过用户界面向用户显示业务包括的内容，使用方式和收费费率等数据
402
用户通过用户界面选择订购中意的业务和使用方式，终端应用会将用户的选择情况传递给终端
403
根据用户的选择情况和对应的费率信息，计算用户购买业务所需费用，并向电子钱包模块发送扣减费用的命令
404
电子钱包模块响应命令，实施扣减费用动作并返回消息，如果扣减失败，同时返回失败原因
405
接收到扣减成功消息后，授权管理模块生成对该业务的授权信息；接收到扣减失败消息后，通过用户界面提示用户失败原因
406

图 2