(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103067333 A
(43)申请公布日 2013.04.24

(21)申请号 201110316790.0

(22)申请日 2011.10.18

(71)申请人 华为终端有限公司
地址 518129 广东省深圳市龙岗区坂田华为基地 B 区 2 号楼

(72)发明人 刘琛

(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.
H04L 29/06(2006.01)
H04L 29/12(2006.01)
H04N 21/6334(2011.01)

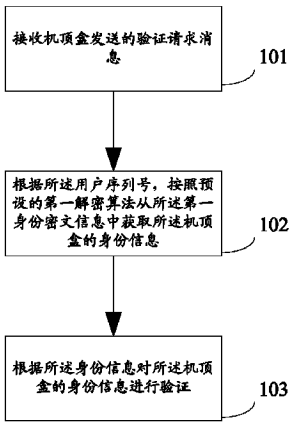
权利要求书2页 说明书10页 附图7页

(54)发明名称

验证机顶盒接入身份的方法和认证服务器

(57)摘要

本发明实施例公开了一种验证机顶盒接入身份的方法和认证服务器，涉及通信技术领域，能够通过机顶盒中的加密算法对身份信息进行加密，并能够更新所述加密算法。本发明的方法包括：接收机顶盒发送的验证请求消息，所述验证请求消息中携带所述机顶盒的第一身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第一身份密文信息是所述机顶盒根据所述机顶盒的身份信息通过第一加密算法计算生成的；根据所述用户序列号，按照预设的第一解密算法从所述第一身份密文信息中获取所述机顶盒的身份信息；根据所述软件版本信息对所述机顶盒的身份信息进行验证。用于验证机顶盒接入身份。



CN 103067333 A

1. 一种验证机顶盒接入身份的方法，其特征在于，包括：

接收机顶盒发送的验证请求消息，所述验证请求消息中携带所述机顶盒的第一身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第一身份密文信息是所述机顶盒根据所述机顶盒的身份信息通过第一加密算法计算生成的；

根据所述用户序列号，按照预设的第一解密算法从所述第一身份密文信息中获取所述机顶盒的身份信息；

根据所述软件版本信息对所述机顶盒的身份信息进行验证。

2. 根据权利要求 1 所述的验证机顶盒接入身份的方法，其特征在于，所述接收机顶盒发送的验证请求消息的步骤包括：

接收所述机顶盒通过动态主机分配协议服务器发送的验证请求消息。

3. 根据权利要求 1 所述的验证机顶盒接入身份的方法，其特征在于，所述方法还包括：

若验证通过，则向所述动态主机分配协议服务器发送验证成功指示信息，所述验证成功指示信息用于指示所述动态主机分配协议服务器为所述机顶盒分配 IP 地址。

4. 根据权利要求 3 所述的验证机顶盒接入身份的方法，其特征在于，所述方法还包括：

更新所述第一解密算法。

5. 根据权利要求 4 所述的验证机顶盒接入身份的方法，其特征在于，所述更新所述第一解密算法包括：

接收解密算法更新指示消息，所述解密算法更新指示消息中包含第二解密算法；

从所述解密算法更新指示消息中获取所述第二解密算法，以便于接收所述机顶盒下次发送的认证请求消息后，采用所述第二解密算法从第二身份密文信息中获取所述机顶盒的身份信息，其中，所述第二身份密文信息是所述机顶盒根据所述机顶盒的身份信息通过第二加密算法计算生成的。

6. 根据权利要求 1 至 5 任一项所述的验证机顶盒接入身份的方法，其特征在于，所述机顶盒的身份信息还包括所述机顶盒通过所述第一加密算法计算所述第一身份密文，或所述机顶盒通过所述第二加密算法计算所述第二身份密文时的时间戳信息。

7. 一种验证机顶盒接入身份的认证服务器，其特征在于，包括：

第一接收模块，用于接收机顶盒发送的验证请求消息，所述验证请求消息中携带所述机顶盒的第一身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第一身份密文是所述机顶盒根据所述机顶盒的身份信息通过第一加密算法计算生成的；

解密模块，用于根据所述用户序列号，按照预设的第一解密算法从所述第一身份密文信息中获取所述机顶盒的身份信息；

检测模块，用于根据所述软件版本信息对所述机顶盒的身份信息进行验证。

8. 根据权利要求 7 所述的验证机顶盒接入身份的认证服务器，其特征在于，所述装置还包括：

第三发送模块，用于若验证通过，向所述动态主机分配协议服务器发送验证成功指示信息，所述验证成功指示信息用于指示所述动态主机分配协议服务器为所述机顶盒分配 IP 地址。

9. 根据权利要求 8 所述的验证机顶盒接入身份的认证服务器，其特征在于，所述装置还包括：

第一更新模块，用于更新所述第一解密算法。

10. 根据权利要求 9 所述的验证机顶盒接入身份的认证服务器，其特征在于，所述第一更新模块包括：

接收单元，用于接收解密算法更新指示消息，所述解密算法更新指示消息中包含第二解密算法；

读取单元，用于从所述解密算法更新指示消息中获取所述第二解密算法，以便于接收所述机顶盒下次发送的认证请求消息后，采用所述第二解密算法从第二身份密文信息中获取所述机顶盒的身份信息；

所述机顶盒下次发送的认证请求消息中携带所述机顶盒的第二身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第二身份密文信息是所述机顶盒根据所述机顶盒的身份信息通过第二加密算法计算生成的。

11. 根据权利要求 7 至 10 任一项所述的验证机顶盒接入身份的认证服务器，其特征在于，所述机顶盒的身份信息还包括所述机顶盒通过所述第一加密算法计算所述第一身份密文，或所述机顶盒通过所述第二加密算法计算所述第二身份密文时的时间戳信息。

12. 一种机顶盒，其特征在于，包括：

填加模块，用于将验证请求消息填加在动态主机分配协议服务器的可选项信息中；

第一发送模块，用于发送所述可选项信息；

第三接收模块，用于在所述可选项信息通过验证后，接收所述动态主机分配协议服务器为所述机顶盒分配的 IP 地址；

第四发送模块，用于在所述机顶盒获取所述 IP 地址后，向广播电视网发送业务请求。

13. 根据权利要求 12 所述的机顶盒，其特征在于，还包括：

加密模块，用于将所述机顶盒的身份信息通过第一加密算法进行加密，生成第一身份密文信息。

14. 根据权利要求 12 所述的机顶盒，其特征在于，还包括：所述验证请求消息中携带所述机顶盒的第一身份密文信息、机顶盒的软件版本信息、和用户序列号。

15. 根据权利要求 12 所述的机顶盒，其特征在于，还包括：

第七接收模块，用于接收升级服务器发送的升级数据；

第二更新模块，用于根据所述升级数据更新加密算法和软件版本。

验证机顶盒接入身份的方法和认证服务器

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种验证机顶盒接入身份的方法和认证服务器。

背景技术

[0002] 随着通信技术的日益发展，数字电视得到迅速推广，使用数字电视的用户也逐渐增多。其中，机顶盒（数字视频变换盒）是使用数字电视所需的设备之一。然而，机顶盒的接入身份盗用现象层出不穷，为维护消费者及制造商的权益，现有技术提供了一些验证机顶盒接入身份的方案。现在主要使用的验证机顶盒接入身份的方案为摘要验证方案。

[0003] 摘要验证方案具体为：机顶盒将用户序列号和口令等验证信息发送至认证服务器；认证服务器检测验证信息正确后，向机顶盒发送挑战消息；机顶盒接收到认证服务器发来的挑战消息后，向认证服务器发送验证响应消息；认证服务器根据接收到的验证信息，通过摘要算法计算生成摘要，并将摘要与相应的应用服务器进行匹配；认证服务器根据匹配的结果选择应用服务器，认证服务器将用户的序列号和登录令牌发送至所选择的应用服务器；认证服务器向机顶盒发送登录成功的消息，登录成功的消息中包含登录令牌，其中，登录成功的消息中包含的登录令牌与认证服务器发送给应用服务器的登录令牌相同；机顶盒向应用服务器发送请求消息，请求消息包括用户的序列号和登录令牌，其中，请求消息中包括的登录令牌与认证服务器向机顶盒发送的登录令牌相同；应用服务器接收到机顶盒发来的请求消息后，将认证服务器发来的用户序列号和登录令牌与请求消息中的用户序列号和登录令牌进行匹配，若两者相同，则向机顶盒发送业务数据，机顶盒开始向用户提供业务服务；正常结束业务服务后，机顶盒向认证服务器和应用服务器发送登出请求，认证服务器和应用服务器删除之前的登录令牌。

[0004] 在实现上述发明的过程中，发明人发现现有技术中至少存在如下问题：

[0005] 该方案对身份进行认证的过程中使用摘要算法生成摘要，所述摘要算法的输入在摘要信息发送前的网络交换报文中都有与之对应的明文信息，摘要算法容易被窃取，从而降低了接入身份认证的准确性。并且摘要算法无法更新，一旦被破解，真正用户的接入身份就会被一直盗用，降低了接入身份认证的安全性。

发明内容

[0006] 本发明的实施例提供一种验证机顶盒接入身份的方法和认证服务器，能够提高机顶盒接入身份的认证安全性。

[0007] 为达到上述目的，本发明的实施例采用如下技术方案：

[0008] 一方面，本发明的实施例提供一种验证机顶盒接入身份的方法，包括：

[0009] 接收机顶盒发送的验证请求消息，所述验证请求消息中携带所述机顶盒的第一身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第一身份密文信息是所述机顶盒根据所述机顶盒的身份信息通过第一加密算法计算生成的；

[0010] 根据所述用户序列号，按照预设的第一解密算法从所述第一身份密文信息中获取所述机顶盒的身份信息；

[0011] 根据所述软件版本信息对所述机顶盒的身份信息进行验证。

[0012] 另一方面，本发明的实施例提供一种验证机顶盒接入身份的认证服务器，包括：

[0013] 第一接收模块，用于接收机顶盒发送的验证请求消息，所述验证请求消息中携带所述机顶盒的第一身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第一身份密文信息是所述机顶盒根据所述机顶盒的身份信息通过第一加密算法计算生成的；

[0014] 解密模块，用于根据所述用户序列号，按照预设的第一解密算法从所述第一身份密文信息中获取所述机顶盒的身份信息；

[0015] 检测模块，用于根据所述软件版本信息对所述机顶盒的身份信息进行验证。

[0016] 一种机顶盒，其特征在于，包括：

[0017] 填加模块，用于将所述验证请求消息填加在所述动态主机分配协议服务器的可选项信息中；

[0018] 第一发送模块，用于发送所述可选项信息；

[0019] 第三接收模块，用于接收所述动态主机分配协议服务器为所述机顶盒分配的 IP 地址；

[0020] 第四发送模块，用于向广播电视网发送业务请求。

[0021] 本发明实施例提供的方法和系统，能够通过机顶盒中的所述加密算法，产生所述身份密文信息，随所述验证请求消息发送到所述认证服务器，所述认证服务器通过所述解密算法从密文中获取身份信息并加以验证。同时，机顶盒能够从广播电视网中接收到升级服务器通过应用服务器下发至所述广播电视网中的新的加密算法，所述解密算法也能够随之进行相应的更新，从而使得整个发明方案能够使用新的加密算法和解密算法进行以上身份信息的认证程。与现有技术相比，本发明实施例能够提高验证机顶盒接入身份认证的准确性，并且能够更新验证接入身份所使用的加密算法和解密算法，从而提高了接入身份认证的安全性。

附图说明

[0022] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图；

[0023] 图 1 为本发明实施例 1 提供的验证机顶盒接入身份的方法的流程图；

[0024] 图 2 为本发明实施例 2 提供的验证机顶盒接入身份的方法的具体实例的流程图；

[0025] 图 3 为本发明实施例 3 提供的验证机顶盒接入身份的方法的具体实例的流程图；

[0026] 图 4 为本发明实施例 4 提供的验证机顶盒接入身份的装置的结构示意图；

[0027] 图 5 为本发明实施例 5、实施例 6、实施例 7 提供的验证机顶盒接入身份的装置的具体实例的结构示意图；

[0028] 图 6 为本发明实施例 7 提供的验证机顶盒接入身份的装置的具体实例的结构示意图；

[0029] 图 7 为本发明实施例 8 提供的验证机顶盒接入身份的系统的结构图。

具体实施方式

[0030] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

[0031] 为使本发明技术方案的优点更加清楚，下面结合附图和实施例对本发明作详细说明。

[0032] 实施例 1

[0033] 本发明实施例提供一种验证机顶盒接入身份的方法，如图 1 所示，该方法包括 ：

[0034] 步骤 101，接收机顶盒发送的验证请求消息。

[0035] 其中，所述验证请求消息中携带所述机顶盒的第一身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第一身份密文是所述机顶盒根据所述机顶盒的身份信息通过第一加密算法计算生成的，所述机顶盒的身份信息包含机顶盒序列号和 MAC 地址。

[0036] 步骤 102，根据所述用户序列号，按照预设的第一解密算法从所述第一身份密文信息中获取所述机顶盒的身份信息。

[0037] 步骤 103，根据所述身份信息对所述机顶盒的身份信息进行验证。

[0038] 本发明实施例提供的方法，能够通过机顶盒中的所述加密算法，产生所述身份密文信息，并随所述验证请求消息发送到所述认证服务器，所述认证服务器接收到所述验证请求消息后，通过所述解密算法从所述身份密文信息中获取所述身份信息并加以验证。与现有技术相比，本发明实施例提供的验证机顶盒接入身份的方法，机顶盒发送的验证请求消息中的身份信息是经过加密的，因此，能够提高验证机顶盒接入身份认证的准确性，并且能够更新验证接入身份所使用的加密算法和解密算法，从而提高了接入身份认证的安全性。

[0039] 实施例 2

[0040] 本发明实施例提供一种验证机顶盒接入身份的方法，如图 2 所示，该方法包括 ：

[0041] 步骤 201，将所述机顶盒的身份信息通过第一加密算法进行加密，生成第一身份密文信息。

[0042] 其中所述机顶盒的所述身份信息包含机顶盒序列号和 MAC 地址。

[0043] 具体的，本实施例中，使用的是具有回传功能的机顶盒，在机顶盒的内部储存器中存有加密程序，例如 ：在用于充当内部储存器的闪存芯片中存储有 96Byte 的数据，这组数据是对验证请求消息进行加密的密钥，并且该加密程序具备传输数据、接收 IP 地址信息和接收升级数据并根据升级数据跟新加密算法的功能。

[0044] 具体的，本实施例中，将所述机顶盒的身份信息通过第一加密算法进行加密的加密方式可以有多种，例如 ：将机顶盒序列号、MAC 地址通过 DES(Data Encryption Standard，数据加密标准）算法进行加密形成密文，其密钥即为储存于闪存芯片中的前 7 个 Byte 的数据。在通过 DES 算法进行加密形成密文时，为了进一步增加第一身份密文的保密性，也可以将时间戳信息纳入加密计算过程。DES 算法为本领域所熟知，在此不再赘述。

[0045] 步骤 202，将所述验证请求消息填加在所述动态主机分配协议服务器的可选项信息中。

[0046] 其中，所述验证请求消息包括软件版本信息、用户序列号、第一身份密文信息和时间戳信息。

[0047] 其中，所述时间戳信息为所述机顶盒通过所述第一加密算法计算所述第一身份密文时的时间戳信息。

[0048] 具体的，本实施例中，机顶盒可以将所述软件版本信息、所述用户序列号和所述第一身份密文加入到发往动态主机分配协议服务器的报文中的 Option60 字段，之后将所述报文通过 IP 网络发送给动态主机分配协议服务器。

[0049] 步骤 203，动态主机分配协议服务器接收所述可选项信息。

[0050] 其中，用于进行验证的所述可选项信息包括所述软件版本信息、所述用户序列号和所述第一身份密文信息。

[0051] 步骤 204，动态主机分配协议服务器提取所述可选项信息中的所述验证请求消息，并将所述验证请求消息发送至认证服务器。

[0052] 具体的，本实施例中，动态主机分配协议服务器接收到机顶盒发送至 IP 网络中的报文后，提取报文中的 Option60 字段所对应的可选项信息，并将所述验证请求消息发送至认证服务器。所述可选项信息包括所述软件版本信息、所述用户序列号和所述第一身份密文信息。

[0053] 步骤 205，认证服务器接收所述验证请求消息。

[0054] 步骤 206，认证服务器根据所述验证请求消息中的用户序列号通过所述第一解密算法对所述第一身份密文信息进行解密，获得所述机顶盒序列号和所述 MAC 地址。

[0055] 具体的，本实施例中，所述认证服务器可以使用密钥根据所述用户序列号通过与第一加密算法所对应第一解密算法的对所述第一身份密文信息进行解密。

[0056] 步骤 207，认证服务器根据所述验证请求消息中的软件版本信息验证所述第一解密算法获得所述机顶盒序列号和所述 MAC 地址是否正确。

[0057] 具体的，本实施例中，认证服务器通过第一解密算法对第一身份密文信息进行解密后得到机顶盒序列号和 MAC 地址（若在步骤 201 中将时间戳信息纳入加密计算过程，则解密后还应得到机顶盒的时间戳信息），针对不同的软件版本，对解密后所得到的数据进行验证，若验证结果正确，则执行步骤 208，通知或指示动态主机分配协议服务器其设备接入合法，并且给接入设备分配 IP 地址，若验证结果不正确，则说明其设备接入不合法，流程结束。

[0058] 步骤 208，认证服务器向所述动态主机分配协议服务器发送验证成功指示信息。

[0059] 步骤 209，动态主机分配协议服务器为所述机顶盒分配 IP 地址。

[0060] 所述动态主机分配协议服务器在接收到验证成功指示信息后，为所述机顶盒分配 IP 地址。从而使机顶盒获得 IP 地址，获得 IP 地址的机顶盒可以直接向广播电视网发送业务请求。

[0061] 步骤 210，机顶盒接收到被分配的 IP 地址，向广播电视网发送业务请求。

[0062] 其中，所述机顶盒的身份信息还包括所述机顶盒通过所述第一加密算法计算所述第一身份密文，或所述机顶盒通过所述第二加密算法计算所述第二身份密文时的时间戳信

息。

[0063] 本发明实施例提供的方法，能够通过机顶盒中的所述加密算法，产生所述身份密文信息，并随所述验证请求消息发送到所述认证服务器，所述认证服务器接收到所述验证请求消息后，通过所述解密算法从所述身份密文信息中获取所述身份信息并加以验证。与现有技术相比，本发明实施例提供的验证机顶盒接入身份的方法，机顶盒发送的验证请求消息中的身份信息是经过加密的，因此，能够提高验证机顶盒接入身份认证的准确性，并且能够更新验证接入身份所使用的加密算法和解密算法，从而提高了接入身份认证的安全性。

[0064] 实施例 3

[0065] 本发明实施例提供一种验证机顶盒接入身份的方法，如图 3 所示，该方法包括：

[0066] 步骤 301，升级服务器发送升级请求至应用服务器。

[0067] 为了进一步提高机顶盒接入身份验证的准确性，可以对认证服务器的解密算法和机顶盒的解密算法进行更新，首先，由升级服务器发送升级请求至应用服务器。

[0068] 步骤 302，应用服务器发送确认信息至升级服务器。

[0069] 具体的，本实施例中，应用服务器在接收到升级服务器发送的升级请求后，反馈确认信息至升级服务器。

[0070] 步骤 303，认证服务器接收升级服务器发送的解密算法更新指示消息。

[0071] 其中，所述解密算法更新指示消息中包含第二解密算法。

[0072] 具体的，本实施例中，升级服务器向认证服务器发送解密算法更新指示消息，以配合对于机顶盒的加密算法的更新。

[0073] 步骤 304，认证服务器从所述解密算法更新指示消息中获取所述第二解密算法。

[0074] 其中，认证服务器从所述解密算法更新指示消息中获取所述第二解密算法，以便在接收所述机顶盒下次发送的认证请求消息后，能够采用所述第二解密算法从第二身份密文信息中获取所述机顶盒的身份信息，至此所述认证服务器的解密算法更新完毕。从而，更新了认证服务器验证接入身份所使用的解密算法，提高了接入身份认证的安全性。

[0075] 具体的，本实施例中，认证服务器接收应用服务器发送的解密算法更新指示消息后，即可采用与新解密算法与密钥进行解密。其中，新解密算法可以是已经预存在认证服务器中的解密算法；也可以是未预存在认证服务器中，由认证服务器通过 IP 网络接收到的解密算法。

[0076] 步骤 305，升级服务器发送升级数据至应用服务器。所述升级数据包括第二加密算法。

[0077] 具体的，本实施例中，升级服务器将采用 3DES 加密算法的机顶盒加密程序数据发送给应用服务器。其中，3DES 加密算法的密钥是机顶盒生产时存储在闪存芯片中的 96 个 Byte 数据的前 21 个 Byte 数据，每 7 个 Byte 为一组密钥，共三组。

[0078] 步骤 306，应用服务器发送升级数据至所述广播电视网中。

[0079] 具体的，在本实施例中，广播电视网是采用条件接收模式进行信息认证的，安全性较高，提高了接入身份认证的安全性。所述条件接收模式为本领域所熟知，在此不再赘述。

[0080] 步骤 307，机顶盒从广播电视网接收升级数据。

[0081] 步骤 308，机顶盒根据所述升级数据更新加密算法和软件版本。

[0082] 其中，所述机顶盒下次发送的认证请求消息中携带所述机顶盒的第二身份密文信息、机顶盒的软件版本信息、用户序列号和时间戳信息，所述第二身份密文信息是所述机顶盒根据所述机顶盒的身份信息通过第二加密算法计算生成的。从而，更新了机顶盒在验证接入身份地过程中所使用的加密算法，提高了接入身份认证的安全性。

[0083] 其中，所述时间戳信息为所述机顶盒通过所述第二加密算法计算所述第二身份密文时的时间戳信息。

[0084] 其中，所述机顶盒的身份信息还包括所述机顶盒通过所述第一加密算法计算所述第一身份密文，或所述机顶盒通过所述第二加密算法计算所述第二身份密文时的时间戳信息。

[0085] 具体的，本实施例中，机顶盒接收到了下发的升级数据后，对其合法性后进行验证，若确认该升级数据合法，则机顶盒根据所述升级数据更新加密算法和软件版本，更新完成后机顶盒将采用新的 3DES 加密算法与密钥对机顶盒序列号与 MAC 地址进行加密。若确认该升级数据不合法，则删除所述升级数据。

[0086] 本发明实施例提供的方法，能够通过机顶盒从广播电视网中接收到所述升级服务器通过所述应用服务器下发至所述广播电视网中的新的加密算法。同时，所述认证服务器中的所述解密算法也能够随之进行相应的更新，从而使得整个发明方案能够使用新的加密算法和解密算法进行以上验证机顶盒接入身份的过程。与现有技术相比，本发明实施例能够更新验证接入身份所使用的加密算法和解密算法，从而提高了接入身份认证的安全性。

[0087] 实施例 4

[0088] 本发明实施例提供一种验证机顶盒接入身份的认证服务器，如图 4 所示，该装置包括 ：第一接收模块 401、解密模块 402、检测模块 403。

[0089] 其中，第一接收模块 401，用于接收机顶盒发送的验证请求消息。

[0090] 其中，所述验证请求消息中携带所述机顶盒的第一身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第一身份密文是所述机顶盒根据所述机顶盒的身份信息通过第一加密算法计算生成的，所述机顶盒的身份信息包含机顶盒序列号和 MAC 地址 ；

[0091] 解密模块 402，用于根据所述用户序列号，按照预设的第一解密算法从所述第一身份密文信息中获取所述机顶盒的身份信息 ；

[0092] 检测模块 403，用于根据所述身份信息对所述机顶盒的身份信息进行验证。

[0093] 本发明实施例提供的验证机顶盒接入身份的认证服务器，接收机顶盒发送的验证请求消息，所述验证请求消息中包含机顶盒通过加密算法产生的身份密文信息，第一接收模块接收到所述验证请求消息后，解密模块通过所述解密算法从所述身份密文信息中获取所述身份信息，检测模块加以验证。与现有技术相比，本发明实施例能够提高验证机顶盒接入身份认证的准确性，并且能够更新验证接入身份所使用的加密算法和解密算法，从而提高了接入身份认证的安全性。

[0094] 实施例 5

[0095] 本发明实施例提供一种机顶盒，如图 5 所示，包括 ：加密模块 404、填加模块 405、第一发送模块 406、第三接收模块 412、第四发送模块 413。

[0096] 其中，加密模块 404，用于将所述机顶盒的身份信息通过第一加密算法进行加密，生成第一身份密文信息。

[0097] 其中所述机顶盒的所述身份信息包含机顶盒序列号和 MAC 地址。

[0098] 填加模块 405，用于将验证请求消息填加在动态主机分配协议服务器的可选项信息中。

[0099] 其中，所述验证请求消息包括软件版本信息、用户序列号、所述第一身份密文信息和时间戳信息。

[0100] 其中，所述时间戳信息为所述机顶盒通过所述第一加密算法计算所述第一身份密文时的时间戳信息。

[0101] 第一发送模块 406，用于发送所述可选项信息至认证服务器。

[0102] 其中，所述认证服务器根据所述用户序列号，按照预设的第一解密算法从所述第一身份密文信息中获取所述机顶盒的身份信息，并对所述机顶盒的身份信息进行验证。

[0103] 第三接收模块 412，用于在所述可选项信息通过验证后，接收所述动态主机分配协议服务器为所述机顶盒分配的 IP 地址。

[0104] 所述动态主机分配协议服务器在接收到验证成功指示信息后，为所述机顶盒分配 IP 地址。从而使机顶盒获得 IP 地址，获得 IP 地址的机顶盒可以直接向广播电视网发送业务请求。

[0105] 第四发送模块 413，用于在所述机顶盒获取所述 IP 地址后，向广播电视网发送业务请求。

[0106] 本发明实施例提供的机顶盒，能够通过机顶盒加密模块中的加密算法，产生身份密文信息，通过填加模块将所述验证请求消息填加在动态主机分配协议服务器的可选项信息中，之后，所述可选项信息通过第一发送模块发送到认证服务器。与现有技术相比，本发明实施例能够提高验证机顶盒接入身份认证的准确性，从而提高了接入身份认证的安全性。

[0107] 进一步可选地，如图 5 所示，该机顶盒还包括 ：第七接收模块 602、第二更新模块 603。

[0108] 其中，第七接收模块 602，用于接收升级服务器发送的升级数据。

[0109] 第二更新模块 603，用于根据所述升级数据更新加密算法和软件版本。

[0110] 实施例 6

[0111] 本发明实施例提供一种验证机顶盒接入身份的动态主机分配协议服务器，如图 5 所示，包括 ：第二接收模块 407、第一提取模块 408、第二发送模块 409、分配模块 411。

[0112] 第二接收模块 407，用于接收机顶盒发送的所述可选项信息。

[0113] 其中，所述可选项信息包含所述验证请求消息中的软件版本信息、用户序列号和所述第一身份密文信息。

[0114] 第一提取模块 408，用于提取所述可选项信息中的所述验证请求消息。

[0115] 第二发送模块 409，用于发送所述验证请求消息至认证服务器。

[0116] 分配模块 411，用于为所述机顶盒分配 IP 地址。

[0117] 所述动态主机分配协议服务器在接收到验证成功指示信息后，为所述机顶盒分配 IP 地址。从而使机顶盒获得 IP 地址，获得 IP 地址的机顶盒可以直接向广播电视网发送业务请求。

[0118] 本发明实施例提供的动态主机分配协议服务器，能够通过第二接收模块接收机顶

盒发送的可选项信息，通过第一提取模块提取可选项信息中的所述验证请求消息，之后并将所述可选项信息通过第二发送模块发送至认证服务器，同时能够通过分配模块为机顶盒分配 IP 地址。与现有技术相比，本发明实施例能够提高验证机顶盒接入身份认证的准确性，从而提高了接入身份认证的安全性。

[0119] 实施例 7

[0120] 本发明实施例提供另一种验证机顶盒接入身份的认证服务器，如图 5 所示，该装置包括 :第一接收模块 401、解密模块 402、检测模块 403、第三发送模块 410。

[0121] 第一接收模块 401，用于接收动态主机分配协议服务器发送的所述验证请求消息。

[0122] 其中，所述验证请求消息中携带所述机顶盒的第一身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第一身份密文是所述机顶盒根据所述机顶盒的身份信息通过第一加密算法计算生成的，所述机顶盒的身份信息包含机顶盒序列号、和 MAC 地址。

[0123] 解密模块 402，用于根据所述用户序列号，按照预设的第一解密算法从所述第一身份密文信息中获取所述机顶盒的身份信息。

[0124] 进一步的，在认证服务器从所述解密算法更新指示消息中获取所述第二解密算法后，能够采用所述第二解密算法从第二身份密文信息中获取所述机顶盒的身份信息，至此解密模块 402 能够采用新的解密算法。从而，更新了认证服务器验证接入身份所使用的解密算法，提高了接入身份认证的安全性。

[0125] 检测模块 403，用于根据所述软件版本信息对所述机顶盒的身份信息进行验证。

[0126] 第三发送模块 410，用于若验证通过，向所述动态主机分配协议服务器发送验证成功指示信息。

[0127] 其中，所述验证成功指示信息用于指示所述动态主机分配协议服务器为所述机顶盒分配 IP 地址，从而使获得 IP 地址的机顶盒可以直接向广播电视网发送业务请求。

[0128] 本发明实施例提供的认证服务器，能够通过认证服务器第一接收模块接收所述验证请求消息，通过解密模块使用解密算法从身份密文信息中获取所述身份信息，检测模块加以验证，之后通过第三发送模块向所述动态主机分配协议服务器发送验证成功指示信息。从而使得整个发明方案能够使用新的解密算法进行以上验证机顶盒接入身份的过程。与现有技术相比，本发明实施例能够提高验证机顶盒接入身份认证的准确性，从而提高了接入身份认证的安全性。

[0129] 进一步可选的，如图 6 所示，该验证机顶盒接入身份的认证服务器还包括 :第一更新模块 601。其中，所述第一更新模块 601 包括 :接收单元 6011、读取单元 6012。

[0130] 其中，第一更新模块 601，用于更新所述第一解密算法。

[0131] 接收单元 6011，用于接收升级服务器发送的解密算法更新指示消息，所述解密算法更新指示消息中包含第二解密算法。

[0132] 具体的，本实施例中，升级服务器发送更新指示消息至认证服务器。

[0133] 读取单元 6012，用于从所述解密算法更新指示消息中获取所述第二解密算法，以便于接收所述机顶盒下次发送的认证请求消息后，采用所述第二解密算法从第二身份密文信息中获取所述机顶盒的身份信息。

[0134] 具体的，本实施例中，认证服务器接收应用服务器发送的解密算法更新指示消息后，即可采用与新解密算法与密钥进行解密。其中，新解密算法可以是已经预存在认证服务

器中的解密算法；也可以是未预存在认证服务器中，由认证服务器通过 IP 网络接收到的解密算法。

[0135] 其中，所述机顶盒下次发送的认证请求消息中携带所述机顶盒的第二身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第二身份密文信息是所述机顶盒根据所述机顶盒的身份信息通过第二加密算法计算生成的。并且，所述第二加密算法是所述机顶盒从广播电视网中接收到的。进一步的，所述第二加密算法是升级服务器通过应用服务器下发至所述广播电视网中的。

[0136] 具体的，在本实施例中，如图 6 所示，所述升级服务器包括：

[0137] 第五发送模块，用于发送升级请求至应用服务器。

[0138] 具体的，本实施例中，升级服务器发送升级请求至应用服务器。

[0139] 第五接收模块，用于接收应用服务器发送的确认信息。

[0140] 具体的，本实施例中，升级服务器通过第四接收模块接收应用服务器发送的确认信息。

[0141] 当升级服务器接收到应用服务器发送的确认信息后，向认证服务器发送更新指示消息以更新解密算法，并且向应用服务器发送升级数据。

[0142] 第七发送模块，用于发送更新指示消息至认证服务器。

[0143] 第八发送模块，用于发送升级数据至应用服务器。所述升级数据包括第二加密算法。

[0144] 具体的，本实施例中，升级服务器将采用 3DES 加密算法的机顶盒加密程序数据发送给应用服务器。其中，3DES 加密算法的密钥是机顶盒生产时存储在闪存芯片中的 96 个 Byte 数据的前 21 个 Byte 数据，每 7 个 Byte 为一组密钥，共三组。

[0145] 其中，如图 6 所示，所述应用服务器包括：

[0146] 第四接收模块，用于接收升级请求。

[0147] 第六发送模块，用于发送确认信息至升级服务器。

[0148] 具体的，本实施例中，应用服务器在接收到升级服务器发送的升级请求后，发送确认信息至升级服务器。

[0149] 第六接收模块，用于接收升级服务器发送的更新指示消息。

[0150] 其中，所述解密算法更新指示消息中包含第二解密算法。

[0151] 具体的，本实施例中，认证服务器接收升级服务器发送的解密算法更新指示消息，以配合对于机顶盒的加密算法的更新。

[0152] 第九发送模块，用于发送升级数据至所述广播电视网中。

[0153] 具体的，本实施例中，应用服务器通过第七发送模块发送升级数据至广播电视网。

[0154] 本发明实施例提供的认证服务器，能够通过第一更新模块更新认证服务器中的解密算法，从而使得整个发明方案能够使用新的解密算法进行以上验证机顶盒接入身份的过程。与现有技术相比，本发明实施例能够更新验证接入身份所使用的解密算法，从而提高了接入身份认证的安全性。

[0155] 实施例 8

[0156] 本发明实施例提供一种验证机顶盒接入身份的系统，如图 7 所示，该系统包括：机顶盒 701、认证服务器 702、动态主机分配协议服务器 703。

[0157] 其中，机顶盒 701，用于将所述第一身份密文信息、机顶盒的软件版本信息、和用户序列号填加在所述动态主机分配协议服务器的可选项信息中，向动态主机分配协议服务器发送验证请求消息。所述验证请求消息中携带所述机顶盒的第一身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第一身份密文信息是所述机顶盒根据所述机顶盒的身份信息通过第一加密算法计算生成的，所述机顶盒的身份信息包含机顶盒序列号和 MAC 地址；

[0158] 认证服务器 702，用于接收动态主机分配协议服务器发送的可选项信息，从所述可选项信息中获取所述第一身份密文信息、所述机顶盒的软件版本信息、和所述用户序列号，根据所述用户序列号，按照预设的第一解密算法从所述第一身份密文信息中获取所述机顶盒的身份信息；根据所述软件版本信息对所述机顶盒的身份信息进行验证，若验证通过，则向所述动态主机分配协议服务器发送验证成功指示信息，所述验证成功指示信息用于指示所述动态主机分配协议服务器为所述机顶盒分配 IP 地址；

[0159] 所述认证服务器 702，还用于从所述解密算法更新指示消息中获取所述第二解密算法，以便于接收所述机顶盒下次发送的认证请求消息后，采用所述第二解密算法从第二身份密文信息中获取所述机顶盒的身份信息，所述机顶盒下次发送的认证请求消息中携带所述机顶盒的第二身份密文信息、机顶盒的软件版本信息、和用户序列号，所述第二身份密文信息是所述机顶盒根据所述机顶盒的身份信息通过第二加密算法计算生成的。

[0160] 动态主机分配协议服务器 703，用于接收所述机顶盒发送的验证请求消息，并从所述验证请求消息中获取所述可选项信息，并将所述可选项信息发送给所述认证服务器。

[0161] 进一步可选的，还包括：升级服务器 704，用于向所述认证服务器发送解密算法更新指示消息，所述解密算法更新指示消息中包含第二解密算法；

[0162] 本发明实施例提供的系统，机顶盒通过加密算法，产生身份密文信息，随验证请求消息发送到认证服务器，所述认证服务器通过解密算法从密文中获取身份信息并加以验证。同时，机顶盒能够从广播电视网中接收到升级服务器通过应用服务器下发至所述广播电视网中的新的加密算法，所述解密算法也能够随之进行相应的更新，从而使得整个发明方案能够使用新的加密算法和解密算法进行以上身份信息的认证程。与现有技术相比，本发明实施例能够提高验证机顶盒接入身份认证的准确性，并且能够更新验证接入身份所使用的加密算法和解密算法，从而提高了接入身份认证的安全性。

[0163] 本领域普通技术人员可以理解实现上述实施例装置中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各装置的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体 (Read-Only Memory，ROM) 或随机存储记忆体 (Random Access Memory，RAM) 等。

[0164] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

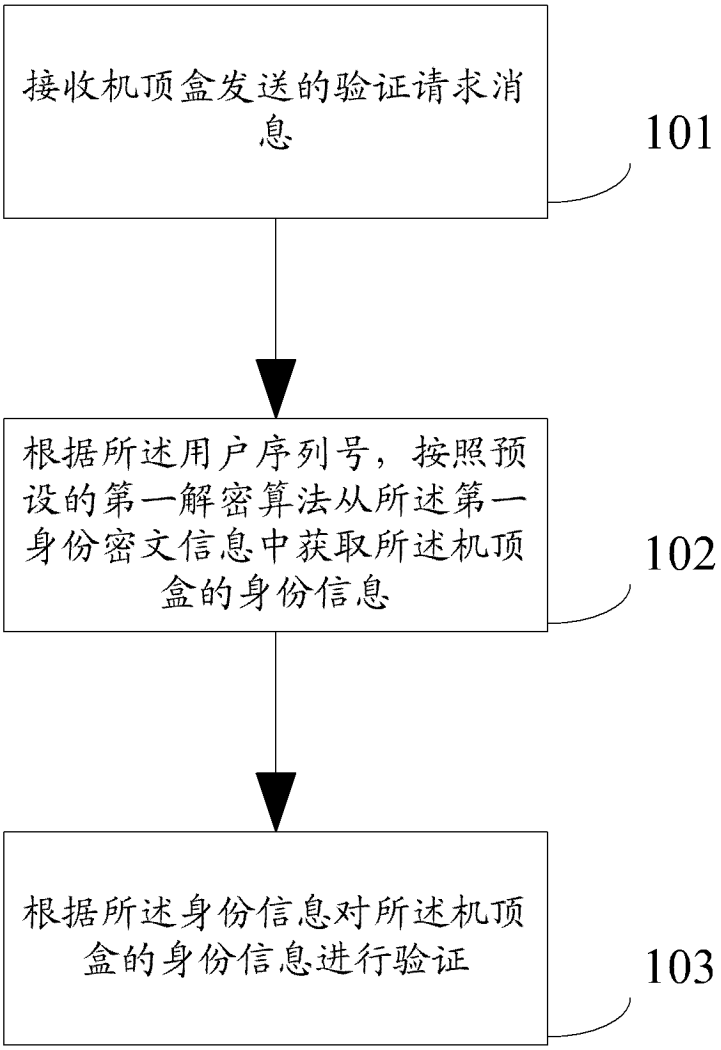

接收机顶盒发送的验证请求消息
101
根据所述用户序列号，按照预设的第一解密算法从所述第一身份密文信息中获取所述机顶盒的身份信息
102
根据所述身份信息对所述机顶盒的身份信息进行验证
103

图 1

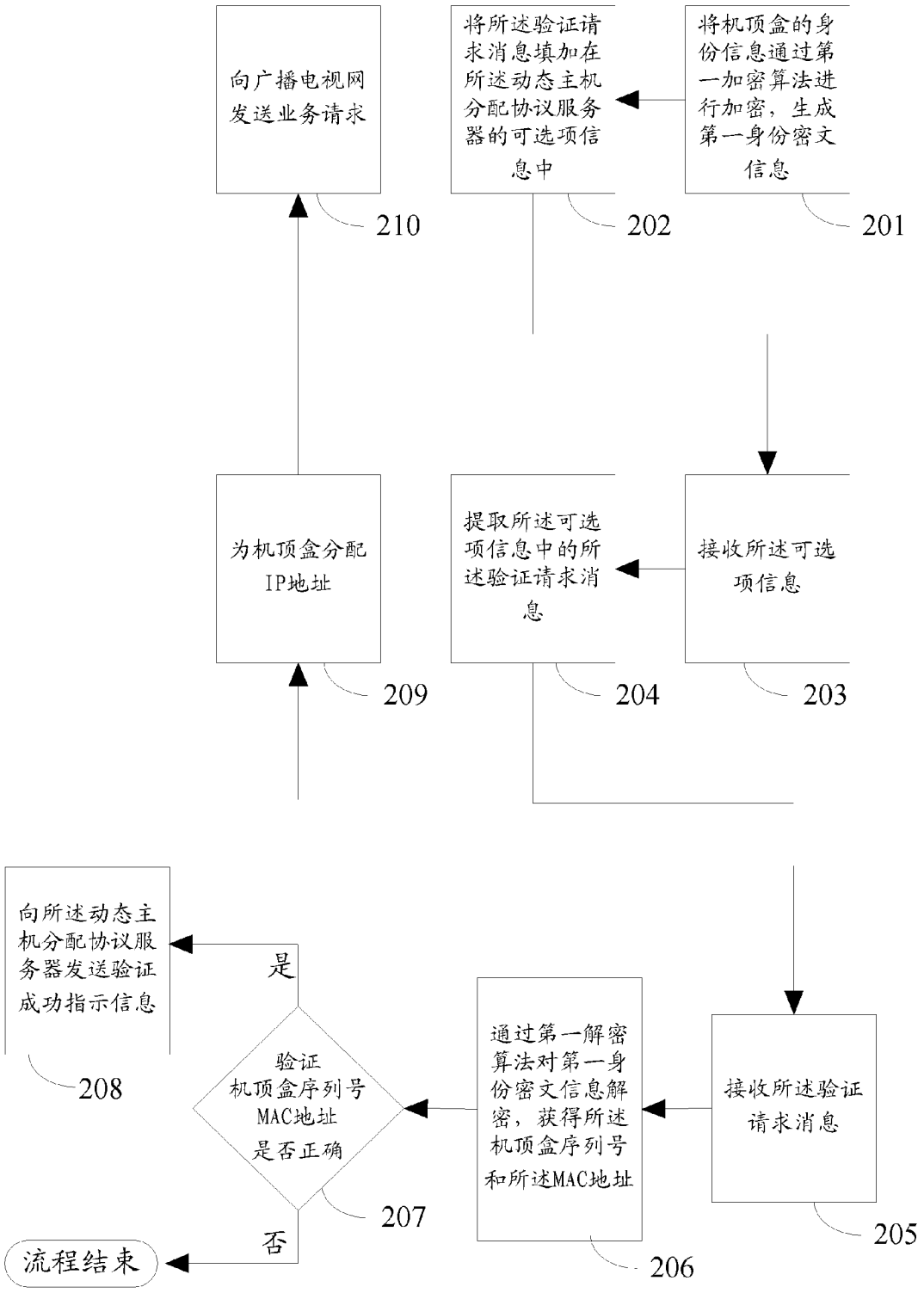

将机顶盒的身份信息通过第一加密算法进行加密，生成第一身份密文信息
201
将所述验证请求消息填加在所述动态主机分配协议服务器的可选项信息中
202
向广播电视网发送业务请求
210
接收所述可选项信息
203
提取所述可选项信息中的所述验证请求消息
204
为机顶盒分配IP地址
209
接收所述验证请求消息
205
通过第一解密算法对第一身份密文信息解密，获得所述机顶盒序列号和所述MAC地址
206
验证机顶盒序列号MAC地址是否正确
207
是
否
向所述动态主机分配协议服务器发送验证成功指示信息
208
流程结束

图 2

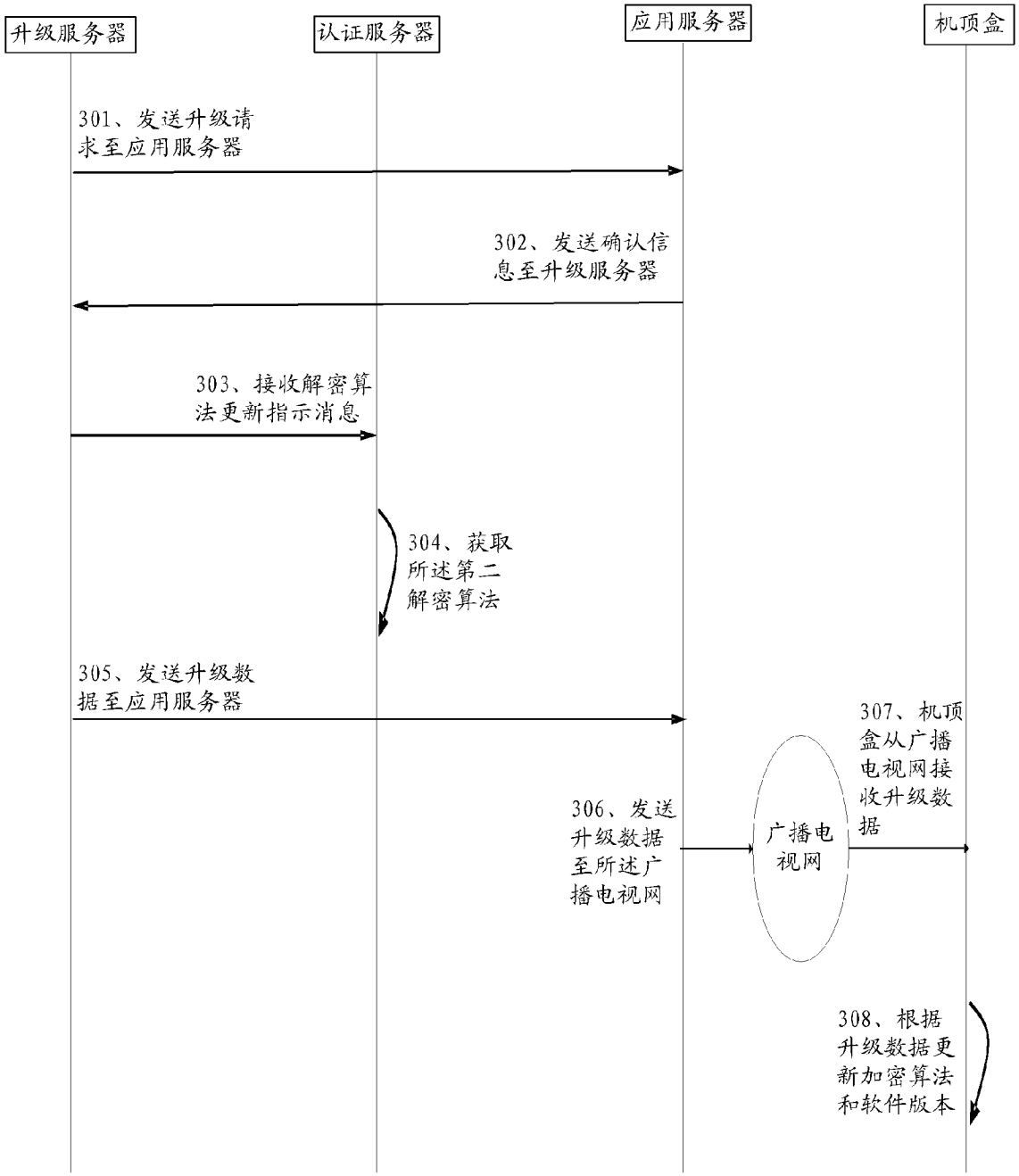

升级服务器
认证服务器
应用服务器
机顶盒
301、发送升级请求至应用服务器
302、发送确认信息至升级服务器
303、接收解密算法更新指示消息
304、获取所述第二解密算法
305、发送升级数据至应用服务器
306、发送升级数据至所述广播电视网
广播电视网
307、机顶盒从广播电视网接收升级数据
308、根据升级数据更新加密算法和软件版本

图 3

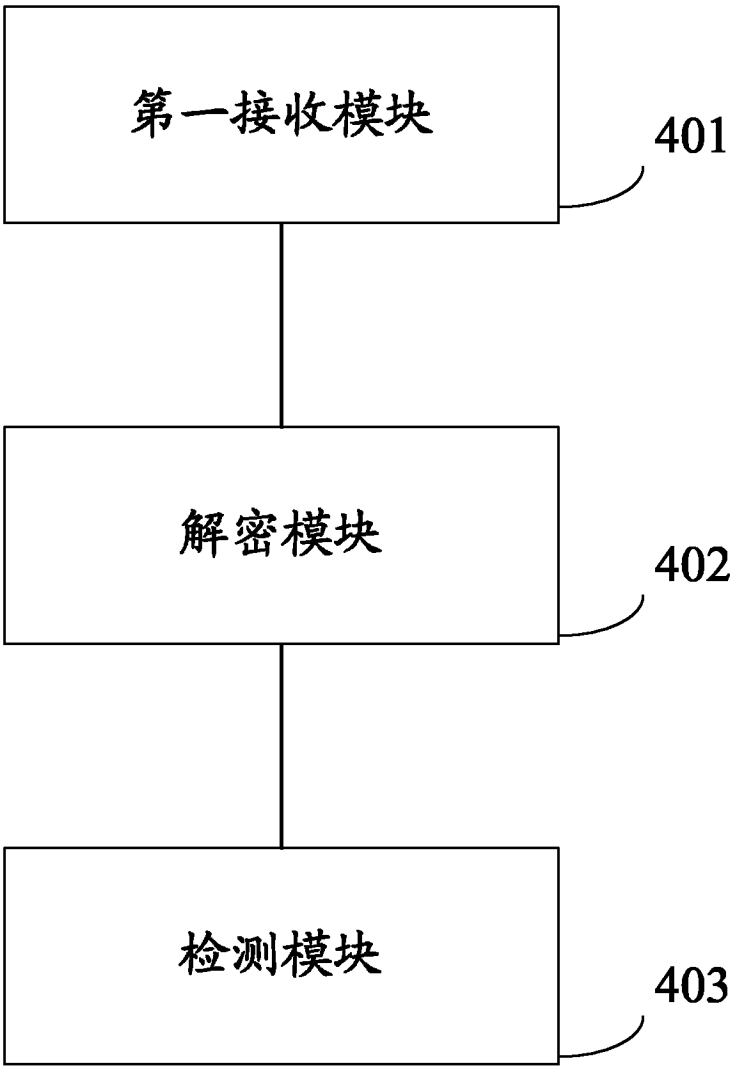


图 4

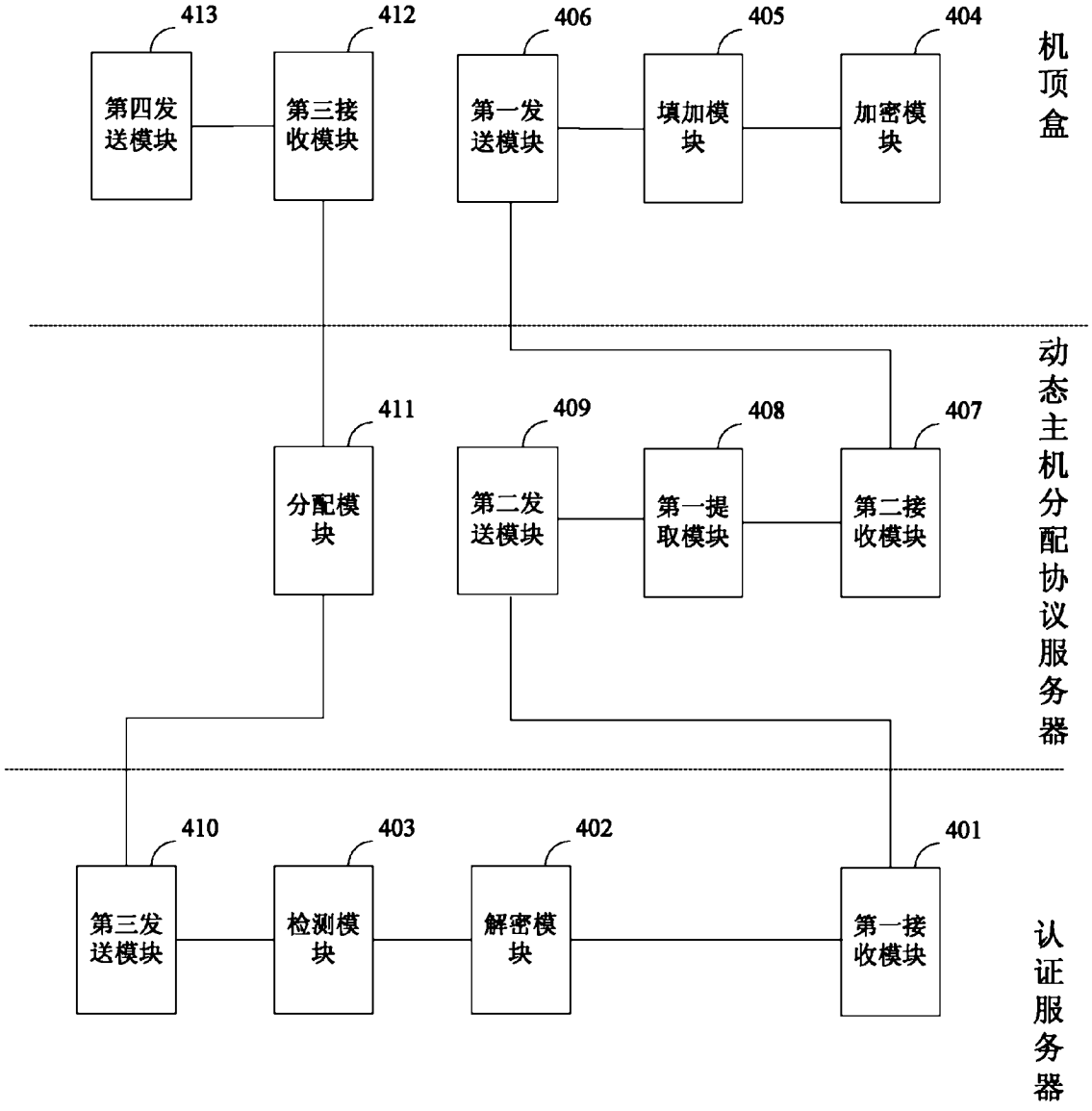

413
412
406
405
404
第四发送模块
第三接收模块
第一发送模块
填加模块
加密模块
机顶盒
411
409
408
407
分配模块
第二发送模块
第一提取模块
第二接收模块
动态主机分配协议服务器
410
403
402
401
第三发送模块
检测模块
解密模块
第一接收模块
认证服务器

图 5

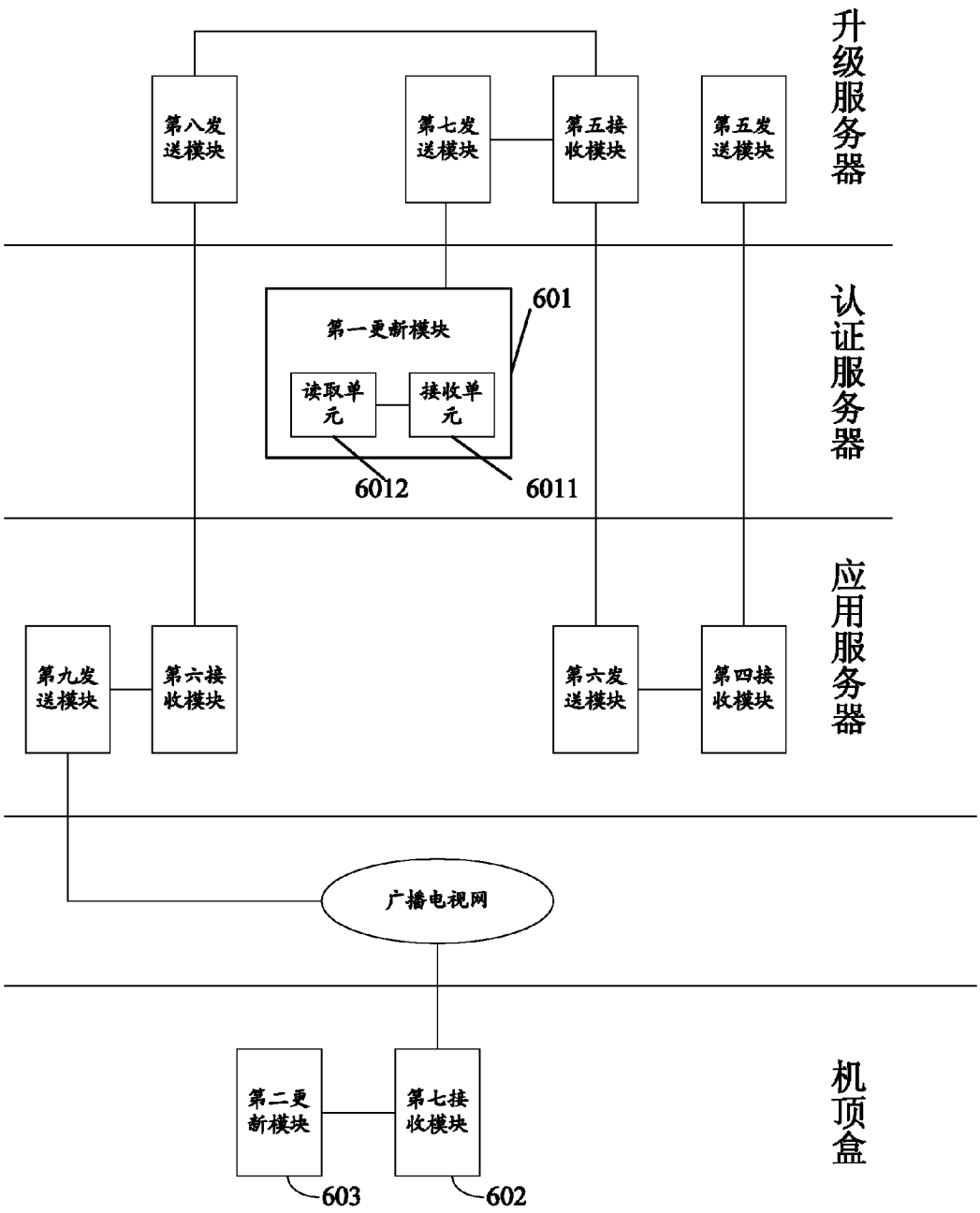

升级服务器
第八发送模块
第七发送模块
第五接收模块
第五发送模块
认证服务器
第一更新模块
601
读取单元
接收单元
6012
6011
应用服务器
第九发送模块
第六接收模块
第六发送模块
第四接收模块
广播电视网
机顶盒
第二更新模块
第七接收模块
603
602

图 6

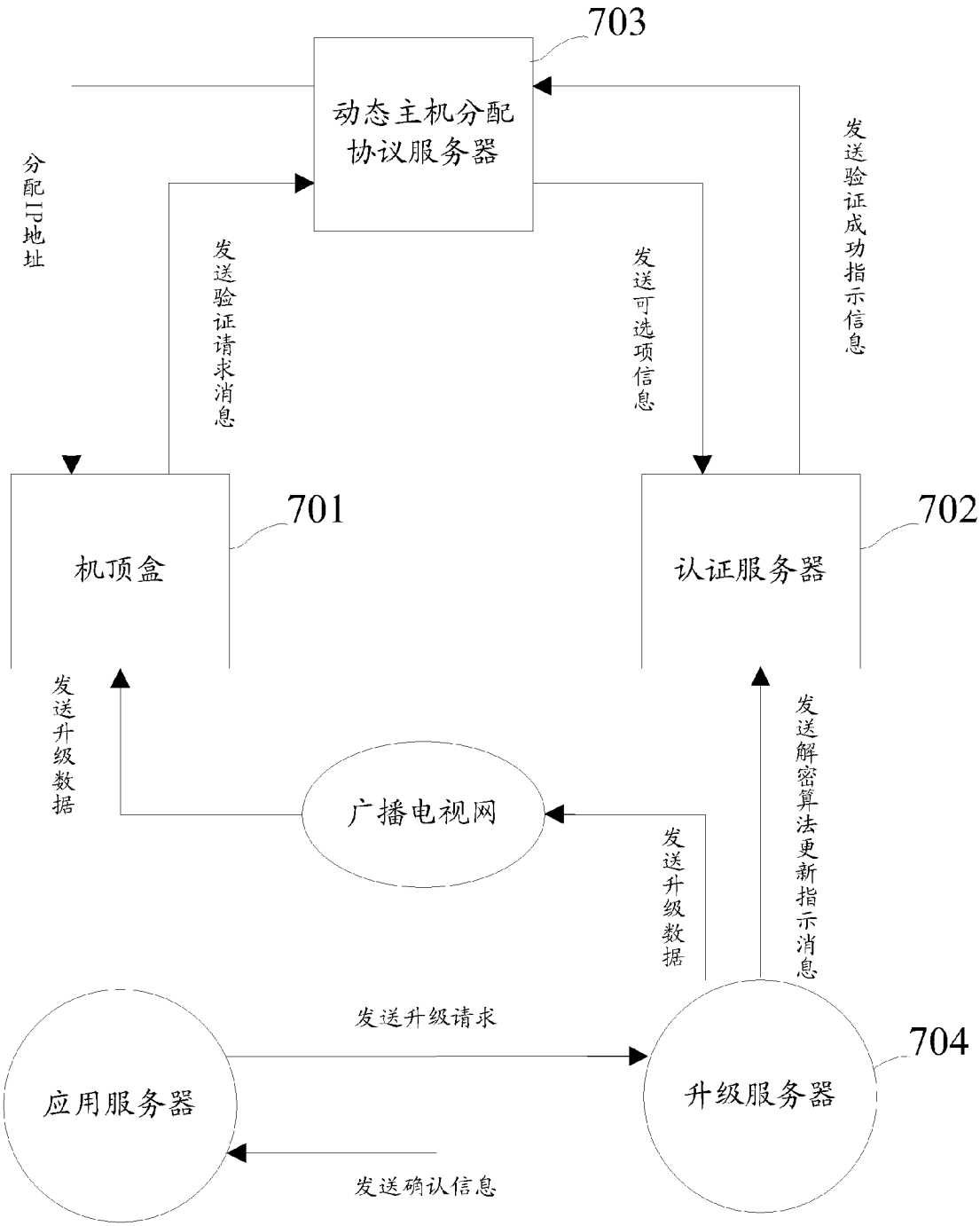

703
动态主机分配协议服务器
分配IP地址
发送验证请求消息
发送可选项信息
发送验证成功指示信息
701
机顶盒
702
认证服务器
发送升级数据
广播电视网
发送升级数据
发送解密算法更新指示消息
发送升级请求
704
应用服务器
升级服务器
发送确认信息

图 7