



(12) 发明专利

(10) 授权公告号 CN 101282254 B

(45) 授权公告日 2011.06.01

(21) 申请号 200710087550.1

(56) 对比文件

(22) 申请日 2007.04.02

CN 1863195 A, 2006.11.15,

(73) 专利权人 华为技术有限公司

审查员 高雪峰

地址 518129 广东省深圳市龙岗区坂田华为
总部办公楼

专利权人 北京邮电大学

(72) 发明人 李超 辛阳 刘云 陈进

(74) 专利代理机构 北京挺立专利事务所 11265

代理人 皋吉甫

(51) Int. Cl.

H04L 12/28 (2006.01)

H04L 12/24 (2006.01)

H04L 29/06 (2006.01)

H04L 9/32 (2006.01)

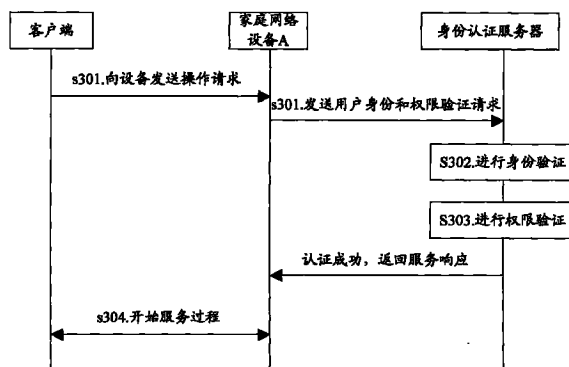
权利要求书 2 页 说明书 9 页 附图 5 页

(54) 发明名称

家庭网络设备管理方法、系统及装置

(57) 摘要

本发明提供了一种家庭网络设备管理方法,包括以下步骤:接收家庭网络用户访问家庭网络设备的访问请求;根据访问请求中包含的家庭网络用户的属性,以及家庭网络用户访问的家庭设备的属性,验证该家庭网络用户对家庭网络设备的使用权限;再根据使用权限,控制家庭网络用户对家庭网络设备的使用。本发明还提供了一种家庭网络设备管理系统及装置。本发明通过对家庭网络中的设备及业务进行属性及权限设置,能够为家庭网络管理员管理设备提供方便;并且明确家庭网络设备的安全级别及家庭网络用户的使用权限,有利于家庭网络的安全管理。



1. 一种家庭网络设备的访问控制方法,其特征在于,包括以下步骤:

预先设置家庭网络用户和所述家庭网络设备的属性,及家庭网络用户对家庭网络设备的使用权限;

接收家庭网络用户访问家庭网络设备的访问请求;

根据所述访问请求中包含的所述家庭网络用户的属性,以及被所述家庭网络用户访问的家庭设备的属性,验证所述家庭网络用户对所述家庭网络设备的使用权限,其中,所述验证家庭网络用户对家庭网络设备的使用权限之前进一步包括:根据所述访问请求中包含的所述家庭网络用户的身份信息进行身份验证,确定所述家庭网络用户的身份信息合法;

根据所述使用权限,控制所述家庭网络用户对所述家庭网络设备的使用。

2. 如权利要求1所述家庭网络设备的访问控制方法,其特征在于,所述家庭网络设备的属性根据家庭网络设备的安全需求设置。

3. 如权利要求2所述家庭网络设备的访问控制方法,其特征在于,所述家庭网络设备的属性根据安全需求由低到高的顺序为:公共服务性设备、公共信息性设备、私人服务性设备、私人信息性设备。

4. 如权利要求1所述家庭网络设备的访问控制方法,其特征在于,所述家庭网络用户的属性根据家庭网络用户的权限需求设置。

5. 如权利要求1所述家庭网络设备的访问控制方法,其特征在于,还包括权限变更流程:

接收第一家庭网络用户更改第二家庭网络用户权限的更改权限请求;

对所述第一家庭网络用户进行身份验证及权限验证;

确认所述第一家庭网络用户有权限修改所述第二家庭网络用户的相应权限后,按照所述第一家庭网络用户的更改权限请求对所述第二家庭网络用户的权限进行修改。

6. 如权利要求1所述家庭网络设备的访问控制方法,其特征在于,还包括权限申请和权限注销流程:

接收所述家庭网络用户发出的申请或注销其它家庭网络用户权限的请求;

对所述家庭网络用户进行身份验证及权限验证;

确认所述家庭网络用户有权限申请或注销其它成员相应权限后,执行所述家庭网络用户对其它家庭网络用户权限申请或权限注销的请求。

7. 一种家庭网络设备管理系统,包括家庭网络设备和身份认证服务器,其特征在于,所述身份认证服务器包括权限设置单元、权限验证单元和身份验证单元;

所述权限设置单元,用于预先设置家庭网络用户和所述家庭网络设备的属性,及家庭网络用户对家庭网络设备的使用权限;

所述权限验证单元,用于根据接收到访问请求的所述家庭网络设备发送的对发起所述访问请求的所述家庭网络用户进行验证的操作请求,及所述权限设置单元预先设置的使用权限验证发起所述访问请求的所述家庭网络用户是否具有相应的使用权限;

所述身份验证单元,用于对发起所述访问请求的所述家庭网络用户的身份信息进行验证。

8. 如权利要求7所述家庭网络设备管理系统,其特征在于,根据所述权限设置单元的设置,所述家庭网络设备分为:公共服务性设备、公共信息性设备、私人服务性设备、私人信

息性设备。

9. 一种用于家庭网络设备管理的身份认证服务器,其特征在于,包括权限设置单元、权限验证单元和身份验证单元,

所述权限设置单元,用于预先设置家庭网络用户和家庭网络设备的属性,及所述家庭网络用户对所述家庭网络设备的使用权限;

所述权限验证单元,用于根据接收到访问请求的所述家庭网络设备发送的对发起所述访问请求的所述网络用户进行验证的操作请求,及所述权限设置单元预先设置的使用权限验证发起所述访问请求的所述家庭网络用户是否具有相应的使用权限;

所述身份验证单元,用于对发起所述访问请求的所述家庭网络用户的身份信息进行验证。

10. 如权利要求9所述用于家庭网络设备管理的身份认证服务器,其特征在于,根据所述权限设置单元的设置,所述家庭网络设备分为:公共服务性设备、公共信息性设备、私人服务性设备、私人信息性设备。

家庭网络设备管理方法、系统及装置

技术领域

[0001] 本发明涉及家庭网络控制管理技术领域,尤其涉及一种家庭网络设备管理方法、系统及装置。

背景技术

[0002] 家庭网络概念最初由家电和 IT 行业提出,主要为了满足用户对于家用电器设备的控制、安防等需求,包括基于 Intel 的家庭数字媒体和 Microsoft 的媒体中心操作系统等。随着宽带互联网络的发展,运营商开始关注家庭网络,但是不同于家电行业和 IT 行业对于家庭网络和家庭网关的认识,电信运营商不再将家庭网络停留在家庭范围内的网络互连,而是将家庭网络作为电信网络的延伸。

[0003] 从家庭网络的发展来看,家庭网络是一个不断扩展的概念,不同的行业对家庭网络有着不同的理解,相应的,也形成了各自的标准化组织或论坛。总体而言,家庭网络在概念和范畴上涉及四个方面的内容:

[0004] (1) 面向家庭网络内部互联

[0005] 家庭网络内部互联主要指通过各种互联网设备和网络技术,将家庭网络的各个设备连接在一起。内部互联涉及两个层面,一个是网络连接,重点是家庭联网技术,例如以太网、PLC(Power Line Communication,电力线联网)、Wifi(Wireless Fidelity,无线保真)、蓝牙等;另外一个内部设备控制,例如通过UPnP(Universal Plug and Play,通用即插即用)相关标准进行内部设备控制。

[0006] (2) 面向家庭内部信息共享和协同工作

[0007] 家庭内部信息共享和协同主要指在家庭内部共享内容和设备能力。例如,通过多媒体信息共享,可以在电视机上播放存储在 PC 机上的影视节目,可以通过电视浏览数码相机拍摄的照片等。信息共享和协作主要在应用层上,通过信息共享和协同,可以在家庭范围内建立一个基于家庭网络的应用环境,将原来孤立的家庭设备连接起来,构成无缝集成的家庭媒体、办公和信息中心。

[0008] (3) 面向公网提供公共网络连接和宽带业务应用

[0009] 家庭网络面向公网的连接和宽带服务主要是通过家庭网关将家庭网络和外部 Internet 宽带网络连接起来,包括两个层面的内容,一个是配合家庭网络需求进行的宽带接入控制,特别是对于 QoS(Quality of Server,服务质量)、安全(包括防攻击和防病毒),以及内部 NAT(Network Address Translation,网地址转换)和穿透等问题,需要一个涉及家庭内部网络和宽带接入网络的统一解决方案;另一个是以家庭为目标开展业务,包括宽带业务和通信业务。与传统的通信业务和宽带业务不同,基于家庭网络环境的业务具有新的特点,包括多终端、多种呈现和操作方式、融合通信等。

[0010] (4) 面向家庭网络业务平台

[0011] 面向家庭网络的业务平台以满足家庭网络业务需求为核心,提供面向家庭网络的业务管理和业务开发平台,涉及三个层面:第一个层面是对家庭网络设备进行自动配置和

管理；第二个层面是对家庭网络的业务配置和策略管理；第三个层面是向外部应用提供家庭网络的开放接口，使得外部应用能够利用家庭网络的平台能力，包括设备能力、自动配置能力、策略管理能力等开发基于家庭网络的业务应用。

[0012] 由图 1 所示的家庭网络一般模型可以看到，根据所处位置及作用不同，家庭网络实体可以分为 7 种，包括：远程用户、远程终端、应用服务器、家庭安全网关、家庭应用服务器、家庭用户、家庭设备。家庭网络内部各实体之间通过有线或无线的方式连接，并通过家庭安全网关与公共网络相连接。这些实体之间的相互联系包括：远程用户和远程终端、远程终端和家庭安全网关、远程终端和家庭应用服务器、远程终端和家庭设备、应用服务器和家庭安全网关、应用服务器和家庭应用服务器、应用服务器和家庭设备、家庭安全网关和家庭设备、家庭应用服务器和家庭设备、家庭设备和家庭用户、家庭设备和其它家庭设备、家庭安全网关和家庭应用服务器之间的联系。

[0013] 其中，家庭设备根据功能不同分成 3 类：A 类家庭设备、B 类家庭设备和 C 类家庭设备。A 类家庭设备具有控制功能，例如：电脑、机顶盒等；B 类家庭设备具有桥接功能，例如：交换机 (switch) 和集线器 (hub) 等；C 类家庭设备为其它家庭设备提供特定服务，例如：数字电视、冰箱等，其中，C 类家庭设备没有通信接口直接连接家庭网络，需要通过 B 类家庭设备连接到家庭网络。

[0014] 从安全角度来看由于家庭成员的不同会有很多种家庭环境，例如：单身家庭、夫妻家庭、三口之家等。由于成员在家庭中的身份不同往往要求对不同设备有不同的使用权限。

[0015] 而现有的这种设备分类方法只是从功能上对家庭设备进行分类，但是用这种简单的分类方法进行分类往往不是很严谨的，属于某类设备的设备可能同时有另一类型设备的功能。而且这种分类没有为家庭网络管理员管理设备提供方便：没有明确设备的安全级别及其用户的业务权限，不利于家庭网络的安全管理。

[0016] 发明内容

[0017] 本发明实施例提供一种家庭网络设备管理方法、系统及装置，便于家庭网络的安全管理。

[0018] 本发明实施例提供了家庭网络设备的访问控制方法，包括以下步骤：

[0019] 预先设置家庭网络用户和所述家庭网络设备的属性，及家庭网络用户对家庭网络设备的使用权限；

[0020] 接收家庭网络用户访问家庭网络设备的访问请求；

[0021] 根据所述访问请求中包含的所述家庭网络用户的属性，以及被所述家庭网络用户访问的家庭设备的属性，验证所述家庭网络用户对所述家庭网络设备的使用权限，其中，所述验证家庭网络用户对家庭网络设备的使用权限之前进一步包括：根据所述访问请求中包含的所述家庭网络用户的身份信息进行身份验证，确定所述家庭网络用户的身份信息合法；

[0022] 根据所述使用权限，控制所述家庭网络用户对所述家庭网络设备的使用。

[0023] 本发明实施例还提供了一种家庭网络设备管理系统，包括家庭网络设备和身份认证服务器，所述身份认证服务器包括权限设置单元、权限验证单元和身份验证单元；

[0024] 所述权限设置单元，用于预先设置家庭网络用户和所述家庭网络设备的属性，及家庭网络用户对家庭网络设备的使用权限；

[0025] 所述权限验证单元,用于根据接收到访问请求的所述家庭网络设备发送的对发起所述访问请求的所述家庭网络用户进行验证的操作请求,及所述权限设置单元预先设置的使用权限验证发起所述访问请求的所述家庭网络用户是否具有相应的使用权限;

[0026] 所述身份验证单元,用于对发起所述访问请求的所述家庭网络用户的身份信息进行验证。

[0027] 本发明实施例还提供了一种用于家庭网络设备管理的身份认证服务器,包括权限设置单元、权限验证单元和身份验证单元,

[0028] 所述权限设置单元,用于预先设置家庭网络用户和家庭网络设备的属性,及所述家庭网络用户对所述家庭网络设备的使用权限;

[0029] 所述权限验证单元,用于根据接收到访问请求的所述家庭网络设备发送的对发起所述访问请求的所述网络用户进行验证的操作请求,及所述权限设置单元预先设置的使用权限验证发起所述访问请求的所述家庭网络用户是否具有相应的使用权限;

[0030] 所述身份验证单元,用于对发起所述访问请求的所述家庭网络用户的身份信息进行验证。

[0031] 本发明实施例通过对家庭网络用户和家庭网络设备进行分权分级,能够为家庭网络管理员管理设备提供方便;并且明确家庭网络设备的安全级别及其家庭网络用户对家庭网络设备的使用权限,有利于家庭网络的安全管理。

[0032] 附图说明

[0033] 图 1 是现有技术中家庭网络一般模型结构图;

[0034] 图 2 是本发明实施例中家庭网络设备业务管理方法流程图;

[0035] 图 3 是本发明实施例中客户端和家庭网络设备 A 的交互过程图;

[0036] 图 4 是本发明实施例中客户端与家庭网络设备 A 交互后和家庭网络设备 B 的交互过程图;

[0037] 图 5 是本发明实施例中家庭网络用户权限变更流程图;

[0038] 图 6 是本发明实施例中家庭网络用户权限申请或权限取消流程图;

[0039] 图 7 是本发明实施例中家庭网络设备业务管理系统图。

[0040] 具体实施方式

[0041] 为了保护网络资源不被未经授权使用,确保只有经过授权的用户才能访问家庭网络设备、存储的信息、信息流、服务和应用程序等,需要加强对家庭网络设备的安全管理。本发明公开一种家庭网络设备业务管理方法,其一实施例如图 2 所示,包括以下步骤:

[0042] S201、根据安全需求设置家庭网络设备的属性,并根据权限需求设置家庭网络用户的属性。

[0043] 家庭网络设备包括:提供信息类服务的家庭网络设备,如电脑、监视器等;提供服务类的家庭网络设备,如冰箱、微波炉等。显然,存储信息的家庭网络设备对安全的需求度要高于仅提供单一服务的家庭网络设备。家庭网络用户主要是比较固定的家庭成员,还有临时的家庭访客,出于家庭网络中信息的安全或者其它方面因素考虑,要求不同的家庭成员有不同的操作权限。

[0044] 在一般家庭网络中,将家庭网络设备分为公用设备和私人设备。其中,公用设备包括电话、电视、收音机、冰箱等;私人设备包括个人电脑、游戏终端等。上述私人设备和公用

设备不固定,可以根据设备在家庭网络中的使用情况来区分。

[0045] 根据安全需求的不同可以进一步将家庭网络设备设置为公共服务性设备、私人服务性设备、公共信息性设备、私人信息性设备;而根据权限需求的不同可以设置家庭网络用户为管理员、普通用户及临时访客等。

[0046] S202、根据预设的属性设置家庭网络用户对家庭网络设备的使用权限。

[0047] 在分别设置家庭网络设备 & 家庭网络用户的属性后,还需要设置家庭网络用户对家庭网络设备的使用权限。结合步骤 S201 中的属性设置,具体设置可实现如下:对于公共服务性设备,由于不存储信息而且一般不会对造成威胁,为所有家庭成员提供同样的服务,例如照明灯,音响,该类设备的安全级别最低,一般不需要家庭网络用户进行身份及权限验证就可以使用,因此可以为所有的家庭网络用户配置相同的使用权限;公共信息性设备,可以存储信息或者提供信息服务,例如可视电话、电视、传真机、监视器等,该类设备的安全级别中等,需要对用户身份及权限进行认证,因此为不同属性的用户配置不同的使用权限;私人服务性设备,不存储信息,仅私人可以使用,或者不存储信息,但是对某些用户相对比较危险,例如儿童或者老人操作起来可能存在威胁的冰箱、微波炉等,该类设备的安全级别较高,需要对用户身份及权限进行认证,因此为特定用户才配置使用权限;私人信息性设备,可以存储信息为私人提供服务,例如个人电脑、游戏终端等,该类设备的安全级别最高,需要对用户进行身份及权限验证,因此为特定用户才配置使用权限,而且不同属性的用户需配置不同的使用权限。

[0048] S203、家庭网络用户需要使用家庭网络设备时,验证该家庭网络用户是否具有相应的使用权限,如果是,则允许该家庭网络用户对家庭网络设备进行相应操作。

[0049] 经过步骤 S202 的使用权限设置后,家庭网络用户在使用家庭网络设备时则必须经过身份验证及权限验证。其中,身份验证是指通过身份信息的比对确认家庭网络用户的身份,具体可以根据家庭网络安全需要而定,一般可以采用的认证方法有:用户口令认证、智能卡认证、生物特征认证等;而权限验证是指通过预先设置的权限列表确认家庭网络用户对家庭网络设备的使用权限。在确认家庭网络用户的身份信息正确并具有对家庭网络设备的相应使用权限后,该家庭网络用户即可以对家庭网络设备进行相应操作。

[0050] 针对上述本发明实施例中对家庭网络设备 & 家庭网络用户的属性设置,及家庭网络用户对家庭网络设备使用权限的设置,下面以一具体设置实例进一步加以阐述。结合现有的家庭网络设备 A、B、C 分类,将每类设备进行二次划分,即细分为公共服务类设备,公共信息类设备、私人服务类设备、私人信息类设备。由此家庭设备被分为 12 类。

[0051] 在经过设备分类之后,以一般的三口之家为例来设置不同设备和不同用户之间的权限关系,用表 1 表示如下。

[0052] 表 1:设备分类及用户之间的权限关系

[0053]

设备类型 用户		公共服务类			公共信息类			私人服务类			私人信息类		
		A	B	C	A	B	C	A	B	C	A	B	C
管理员 (父母)	使用	Y	Y	Y	Y	Y	Y	Y*	Y*	Y*	Y*	Y*	Y*
	控制	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
其它用户 (小孩)	使用	N	N	Y	Y	Y	Y	N	Y*	Y*	Y*	Y*	Y*
	控制	N	N	Y	N	N	N	N	N	N	N	N	N
临时用户 (访客)	使用	N	Y	Y	?	?	?	?	?	?	?	?	?
	控制	N	N	Y	N	N	N	N	N	N	N	N	N

[0054] 表 1 中, Y 表示相对应的用户具有该设备使用或者控制权限, N 表示不具有对应的权限, ? 表示权限根据临时用户对设备业务的需求及管理员的认可后具有使用或者控制权, 所述私人服务或者信息类设备所对应的 Y* 是指仅该设备业务的服务对象具有使用权。

[0055] 这里对家庭网络中的用户进行了划分, 便于从用户角度来看表 1。

[0056] 父母一般是作为家庭网络管理员, 对设备使用权限进行管理, 比如将数字电视, 电脑的开放时间进行限制、禁止小孩对某些危险设备的使用权等; 当家庭中出现临时访客时也需要对访客的设备使用权限进行限制。因此, 网络管理员对家庭网络中所有设备具有控制权, 对所有公共设备和为管理员服务的私人设备也都具有使用权。

[0057] 家庭中的小孩就是家庭网络中除了管理员之外的固定家庭用户, 对于公共设备中的 A 类设备不具有控制和使用权, 因为 A 类设备是具有控制功能的设备, 需要避免不合理的操作出现以造成不必要的损失。此外, 该类用户对某些设备的使用时间也是受限制的, 例如电视、个人电脑的网络连接时间都是由网络管理员预先设置的。

[0058] 临时访客的权限级别需要由管理员进行临时分配, 不同身份的临时用户一般权限级别也会不同, 但是一般都没有设备的控制权。表 1 中唯一所有用户都具有控制和使用权的公共服务类设备中的 C 类设备, 因为其不存储信息也不会造成其它威胁。

[0059] 再从设备的安全级别来看表 1: 显然信息类设备对用户开放的程度比服务类的要低, 即信息类设备安全级别高于服务类设备。因为信息类设备中一般都存储着有用信息, 仅网络管理员对这些设备才具有控制权, 而其它用户只具有使用权或者部分使用权。私人设备比公共设备的安全级别高, 由于私人信息类设备可能存储着需要保密的私人信息, 私人服务设备一般仅允许设备所属者使用。A 类设备安全级别高于 B 和 C 类, 因为可以用来控制其它设备, 一般仅网络管理员才能对 A 类设备进行操作控制。

[0060] 本发明实施例中, 在安装家庭网络时要对家庭网络设备中关于家庭网络用户的属性以及相应的使用权限进行初始化, 并且在连接到家庭网络后对家庭网络设备进行属性设置。具体过程可按如下步骤进行:

[0061] 在安装配置家庭网络时, 家庭网关可以将现有用户分为三类: 管理员、一般家庭成员和临时访客, 并且按照 A、B、C 类中公共服务类、公共信息类、私人服务类、私人信息类设

备的权限表（如表 1 所示）来对各类用户权限进行初始化。

[0062] 在家庭网络安装完成后，家庭网络中的所有设备需要和家庭网关进行初始化连接，并且由家庭网关对这些设备进行分类，一类家庭网络用户对于同一类家庭网络设备拥有相同的使用权限。

[0063] 本发明家庭成员权限的初始化过程在家庭网络安装完成后要对家庭网络用户的使用权限进行初始分配，并对相应的私人信息设备的使用权限进行调整。具体过程如下：

[0064] 在完成家庭网络设备的初始化后，给家庭网络用户分配一个管理员权限，管理员权限可以向其它家庭网络用户赋予相应的管理员或者一般家庭成员权限，并对经常性的访客赋予相应的临时访客权限。

[0065] 管理员可以在对家庭网络用户的使用权限进行分类分配的基础上，对家庭网络用户的私人信息类设备权限进行调整，以便使家庭网络用户只拥有对自己的私人信息类设备的使用权。

[0066] 本发明实施例中的家庭设备的使用流程中，由于对家庭网络用户的使用权限和家庭网络设备分类进行了详细的划分，所以在家庭网络用户登录到家庭网络后，如果验证到家庭网络用户对某一类家庭网络设备拥有使用权限，那么该家庭网络用户就可以对这一类家庭网络设备拥有相应的使用权限。具体过程如图 3 所示，包括以下步骤：

[0067] 步骤 s301，家庭网络用户通过客户端向家庭网络设备 A 发出服务请求，请求中包含家庭网络用户的用户名、申请的服务信息，如服务名称或唯一标识。

[0068] 步骤 s302，家庭网络设备 A 在接收到家庭网络用户的服务请求后，向身份认证服务器发送对家庭网络进行相应验证的请求。

[0069] 步骤 s303，身份认证服务器对家庭网络用户的身份进行验证。

[0070] 步骤 s304，在身份验证通过并且家庭网络用户信息得到确认后，身份认证服务器要对该家庭网络用户所申请的相关操作权限进行验证。

[0071] 步骤 s305，服务器对家庭用户的权限验证通过后，通知家庭网络设备 A 该家庭网络用户有权进行相应的操作。

[0072] 步骤 s306，家庭网络用户对家庭网络设备进行相应的操作。

[0073] 如果家庭网络用户在对家庭网络设备 A 访问完毕后要再对家庭网络设备 B 进行访问，因为家庭网络用户已经在对家庭网络设备 A 进行操作前已经进行过身份验证，所以在这里不需要再对该家庭网络用户的身份进行验证，具体步骤如图 4 所示，包括以下步骤：

[0074] 步骤 s401，家庭网络用户通过客户端向家庭网络设备 B 发送操作请求。

[0075] 步骤 s402，家庭网络设备 B 向身份认证服务器发送家庭网络用户身份和权限验证请求。

[0076] 步骤 s403，验证该家庭网络用户对家庭网络设备 B 的请求和对家庭网络设备 A 的请求是否相同，如果相同，则转步骤 s404，否则，转步骤 s405。

[0077] 步骤 s404，身份认证服务器向家庭网关来查证家庭网络设备 B 和家庭网络设备 A 是否属于同一类型家庭网络设备，如属于同一类家庭网络设备（不包括私人信息类家庭网络设备）则家庭网络用户可以对家庭网络设备 B 进行同样的操作，转步骤 s406，否则，转步骤 s405。

[0078] 步骤 s405，验证权限，如果家庭网络用户对设备 B 申请的服务和对设备 A 申请的操

作不相同,或申请服务虽然相同,但是家庭网络设备 A 和家庭网络设备 B 不属于同一类家庭网络设备,则身份认证服务器需要对家庭网络用户的相应的操作权限重新进行验证,如果拥有相应的权限就允许家庭网络用户对家庭网络设备 B 进行相应的操作,如果家庭网络用户没有权限对家庭网络设备 B 进行请求的操作,则给出拒绝提示。

[0079] 步骤 s406,家庭网络用户对家庭设备进行相应的操作。

[0080] 本发明家庭成员权限变更流程中,作为家庭成员或临时访客的家庭网络用户可以向管理员申请获得某个设备的使用权或控制权,管理员也可以取消家庭成员和临时访客对家庭网络设备的使用权或控制权。具体如图 5 所示,包括以下步骤:

[0081] 步骤 s501,家庭网络用户向管理员申请某一家家庭网络设备或者某一类家庭网络设备的使用权限,或者是管理员认为应该取消家庭网络用户的某些权限;管理员批准申请后,使用本身的管理员身份通过客户端登陆家庭网关,并向家庭网关发出更改家庭网络用户相应权限的请求。

[0082] 步骤 s502,家庭网关在接收到某个家庭网络用户以管理员身份发送的相应操作请求后,向身份认证服务器发送该家庭网络用户的身份和权限验证请求。

[0083] 步骤 s503,身份认证服务器对该家庭网络用户进行身份验证,如果身份信息验证通过则转步骤 s504。

[0084] 步骤 s504,查看该家庭网络用户是否具有管理员权限以修改其它成员的相应权限,如果该家庭网络用户拥有对其它家庭网络用户的修改权限,就转步骤 s505;如果该家庭网络用户没有权限对其它家庭网络用户的权限进行相应的操作,则给出拒绝提示。

[0085] 步骤 s505,身份认证服务器向家庭网关返回一个允许修改的响应。

[0086] 步骤 s506,家庭网关开始进行相应家庭网络用户权限的修改。

[0087] 步骤 s507,通知身份认证服务器进行相应的修改操作。

[0088] 步骤 s508,将管理员修改后的家庭网络用户权限存储在身份认证服务器的权限列表里,此时权限经过修改的家庭网络用户就拥有了或者失去了对某些家庭网络设备的操作权限。

[0089] 步骤 s509,如果在身份认证服务器的权限列表存储成功,身份认证服务器向家庭网关返回存储成功信息。

[0090] 步骤 s510,家庭网关向管理员客户端返回家庭网络用户权限修改成功信息。

[0091] 本发明实施例中的家庭网络用户的权限申请和权限注销流程中,家庭成员或临时访客可以向管理员申请获得相应的家庭成员或临时访客的身份,管理员也可以取消家庭成员或临时访客的相应身份。具体过程如图 6 所示,包括以下步骤:

[0092] 步骤 s601,家庭网络用户向管理员申请获得相应的家庭成员或临时访客的身份,或者是管理员认为应该取消家庭网络用户的相应身份;管理员批准申请后,使用本身的管理员身份通过客户端登陆家庭网关,并向家庭网关发出添加或取消家庭网络用户的请求。

[0093] 步骤 s602,家庭网关在接收到某个家庭网络用户以管理员身份发起的相应操作请求后,向身份认证服务器发送该家庭网络用户的身份及权限验证请求。

[0094] 步骤 s603,身份认证服务器对该家庭网络用户进行身份验证,如果身份信息验证通过则转步骤 s604。

[0095] 步骤 s604,查看该家庭网络用户是否有权限修改其它家庭网络用户相应权限,如

果该家庭网络用户拥有对其它家庭网络用户的修改权限,则转步骤 s605;如果家庭网络用户没有权限对其它家庭网络用户的权限进行相应的操作,则给出拒绝提示。

[0096] 步骤 s605,身份认证服务器向家庭网关返回一个允许修改的响应。

[0097] 步骤 s606,家庭网关开始进行添加或删除相应家庭网络用户权限。

[0098] 步骤 s607,通知身份认证服务器进行相应家庭网络用户权限的添加或删除。

[0099] 步骤 s608,将用户添加到身份认证服务器并赋予相应的权限,此时该新家庭网络用户就拥有相应的权限;或管理员将某个家庭网络用户取消,那么该家庭网络用户就从身份认证服务器中被删除。

[0100] 步骤 s609,如果在身份认证服务器的权限列表存储成功,身份认证服务器向家庭网关返回存储成功信息。

[0101] 步骤 s610,家庭网关向管理员客户端返回家庭网络用户添加或取消成功信息。

[0102] 上述本发明家庭网络设备管理方法的实施例,通过对家庭网络设备及用户进行分权分级,而家庭网络用户在需要对家庭网络设备进行操作时,需要经过身份认证服务器的身份信息验证及权限验证,以确定身份信息是否正确并进一步验证是否具有相应的操作权限,从而方便管理员对家庭网络进行管理,使家庭网络设备的安全级别及用户权限更为明确,有利于家庭网络的安全管理。

[0103] 本发明还公开一种家庭网络设备管理系统,其一实施例如图 7 所示,包括客户端 100、家庭网络设备 200 和身份认证服务器 300,身份认证服务器 300 包括权限设置单元 301、身份验证单元 302、权限验证单元 303 和权限列表存储单元 304。权限设置单元 301 用于预先设置家庭网络用户对家庭网络设备的使用权限,并以列表形式存入权限列表存储单元 304;身份验证单元 302 用于对家庭网络用户进行身份验证,确认家庭网络用户的身份信息是否正确;权限验证单元 303 用于根据家庭网络设备 200 向身份认证设备 300 发送的认证请求,及权限列表存储单元 304 存储的使用权限列表为家庭网络用户进行权限验证;权限列表存储单元 304,用于存储所述使用权限列表。

[0104] 下面以一具体应用实例对上述本发明家庭网络设备管理系统进一步加以阐述。继续如图 7 所示,首先由身份认证服务器 300 中的权限设置单元 301 完成家庭网络用户及家庭网络设备的属性设置,并为家庭网络用户设置使用权限,并将设置后的使用权限以列表形式存入身份认证服务器 300 的权限列表存储单元 304 中;家庭网络用户需要使用家庭网络设备 200 时,通过客户端 100 向家庭网络设备 200 发起操作请求,请求中包括家庭网络用户的用户名、申请的操作信息;家庭网络设置 200 在收到用户的操作请求后,通过身份认证服务器 300 对用户进行身份及权限验证,具体包括:通过身份验证单元 302 根据预先存储的信息判断发起操作请求的家庭网络用户身份信息是否符合,在身份验证单元 302 认证通过后,由权限验证单元 303 根据权限列表存储单元 304 中的权限列表信息验证该家庭网络用户是否有权限进行操作,如果验证通过,则允许家庭网络用户对家庭网络设备 200 进行相应操作。另外,家庭网络用户还可以向管理员申请通过客户端 100 对身份认证服务器 300 中的权限设置单元 301 进行操作,进行权限变更、申请及注销,权限设置单元 301 在进行相应的权限修改后将结果存入权限列表存储单元 304 中。

[0105] 上述本发明家庭网络设备管理系统的实施例,在家庭网络设备管理中,首先由身份认证服务器的权限设置单元对家庭网络设备及用户进行分权分级管理,然后在用户需要

对家庭网络设备进行操作时再由身份验证单元及权限验证单元对用户的身份信息及权限进行验证,以确定是否具有相应的操作权限;从而通过对家庭网络设备及用户进行分权分级,为家庭网络管理员对设备进行管理提供方便,并使家庭网络设备的安全级别及其用户权限更为明确,有利于家庭网络的安全管理。

[0106] 本发明还公开一种用于家庭网络设备管理的身份认证服务器,其一实施例如图 7 中身份认证服务器 300 所示,其包括权限设置单元 301、身份验证单元 302、权限验证单元 303 和权限列表存储单元 304。权限设置单元 301 用于预先设置家庭网络用户对家庭网络设备的使用权限,并以列表形式存入权限列表存储单元 304;身份验证单元 302 用于对家庭网络用户进行身份验证,确认家庭网络用户的身份信息是否正确;权限验证单元 303 用于根据家庭网络设备 200 向身份认证设备 300 发送的认证请求,及权限列表存储单元 304 存储的使用权限列表为家庭网络用户进行权限验证;权限列表存储单元 304,用于存储所述使用权限列表。

[0107] 以上公开的仅为本发明的具体实施例,但是,本发明并非局限于此,任何本领域的技术人员能思之的变化都应落入本发明的保护范围。

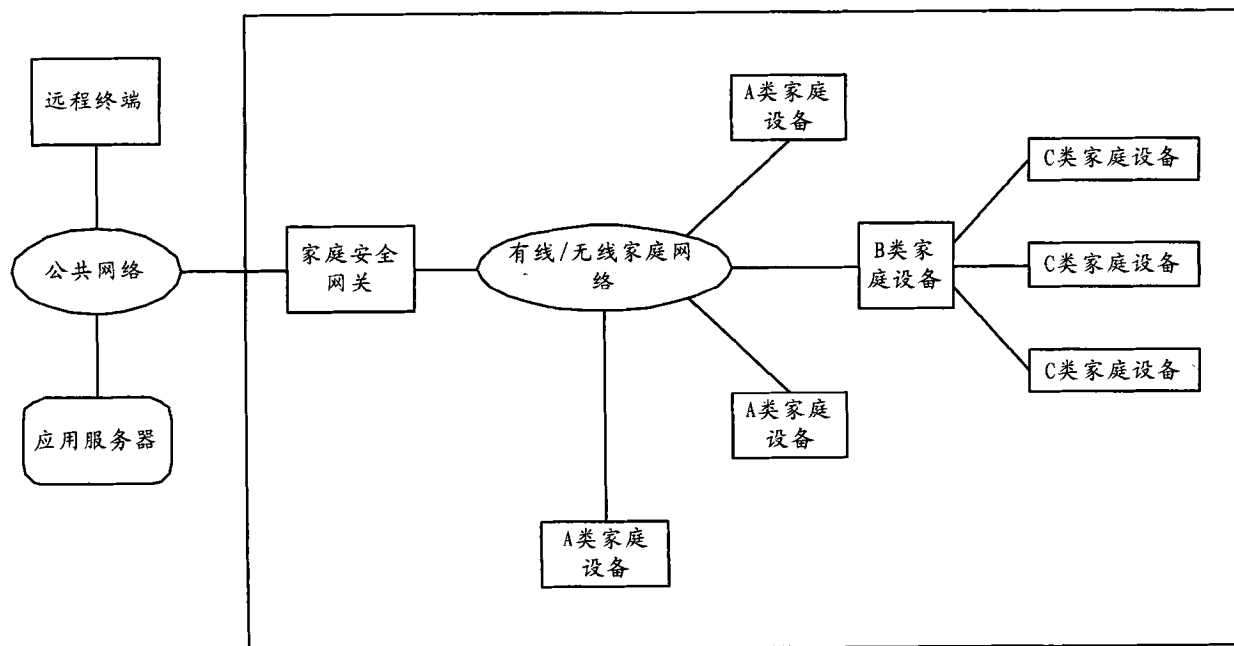


图 1

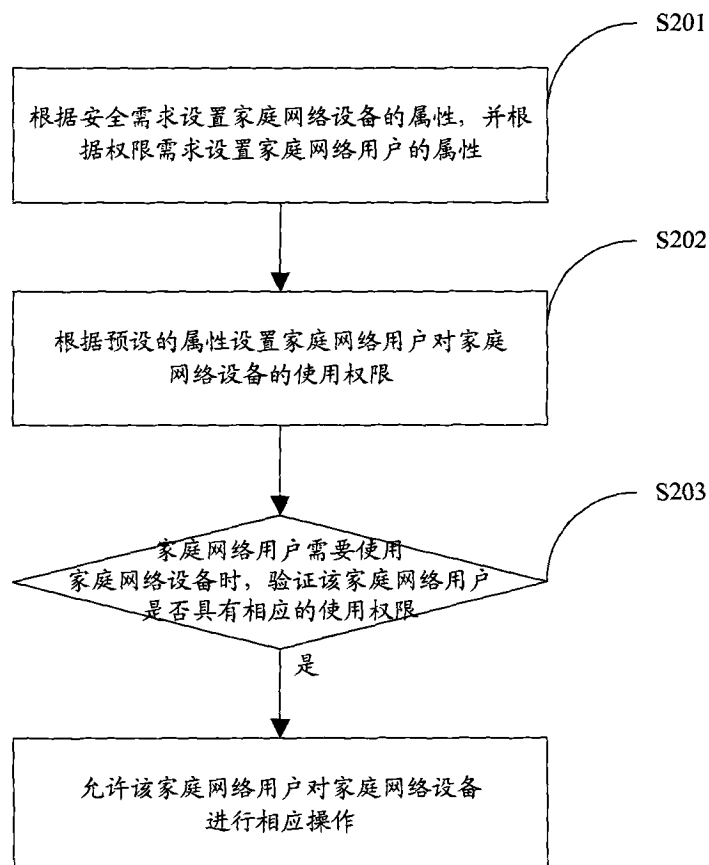


图 2

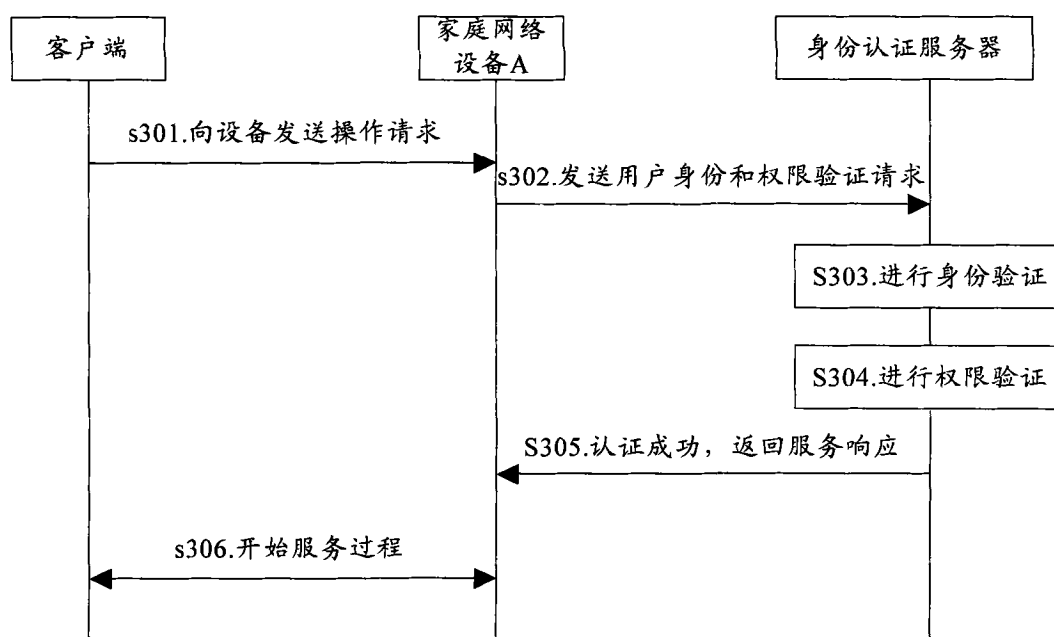


图 3

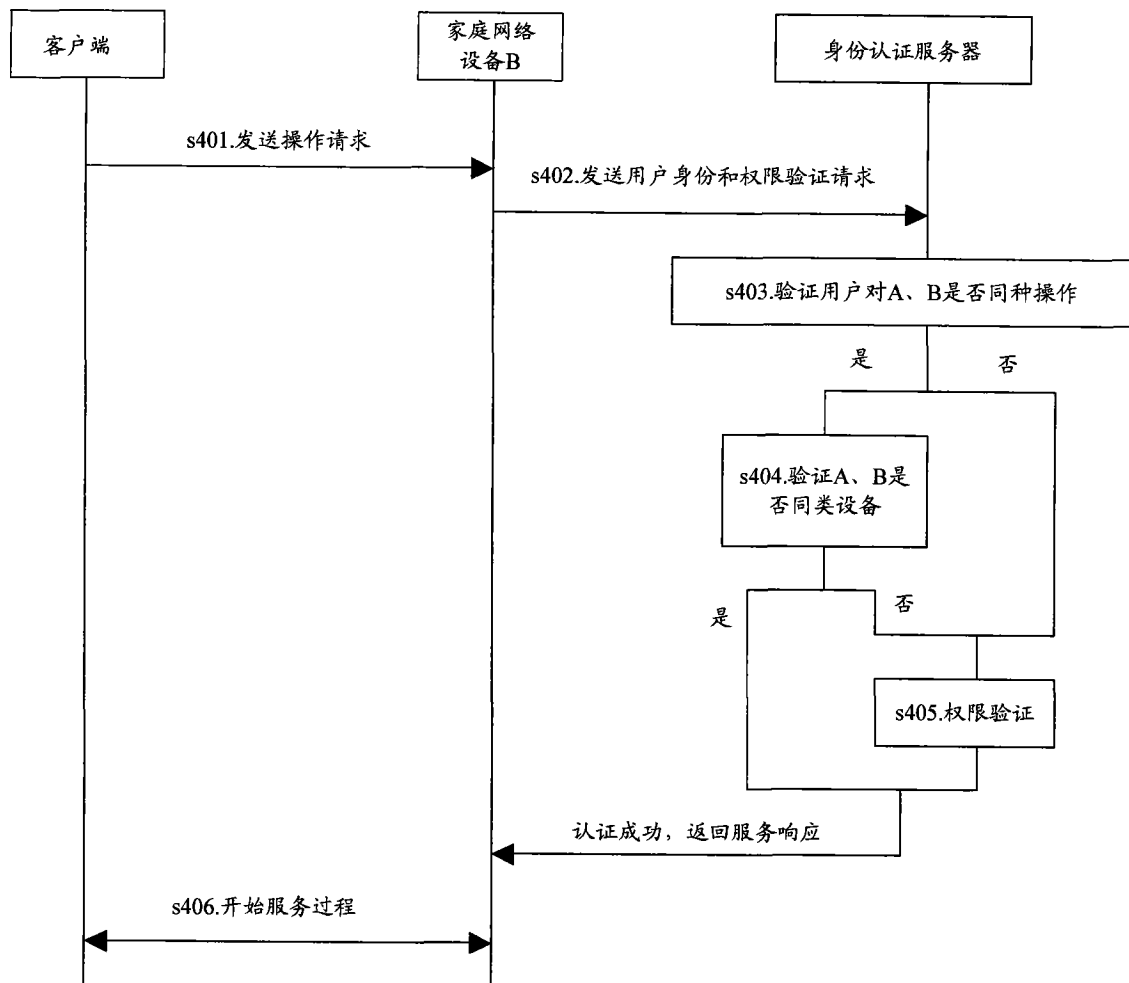


图 4

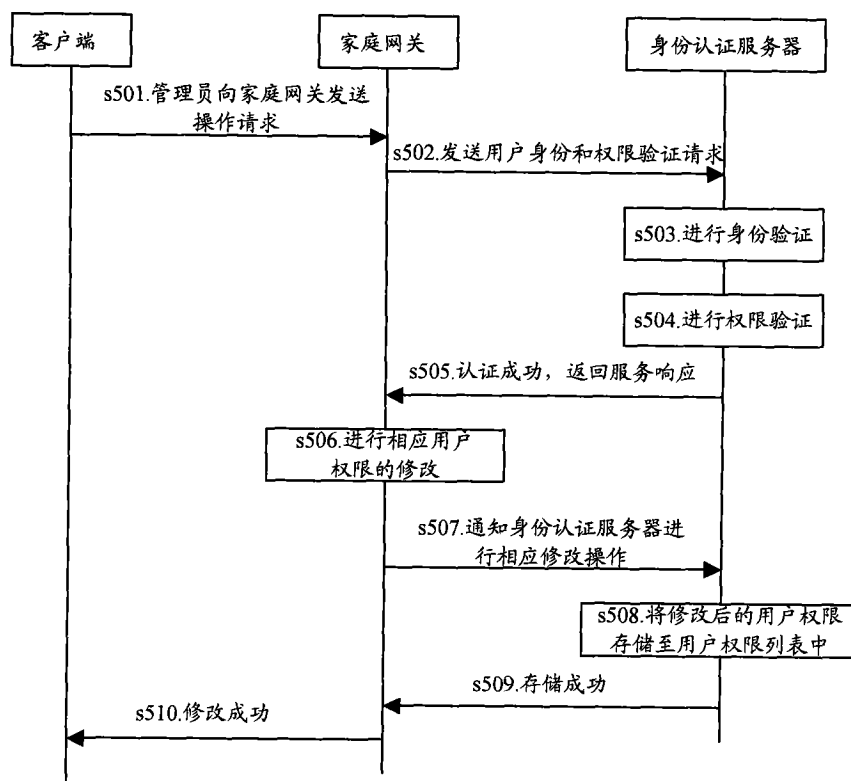


图 5

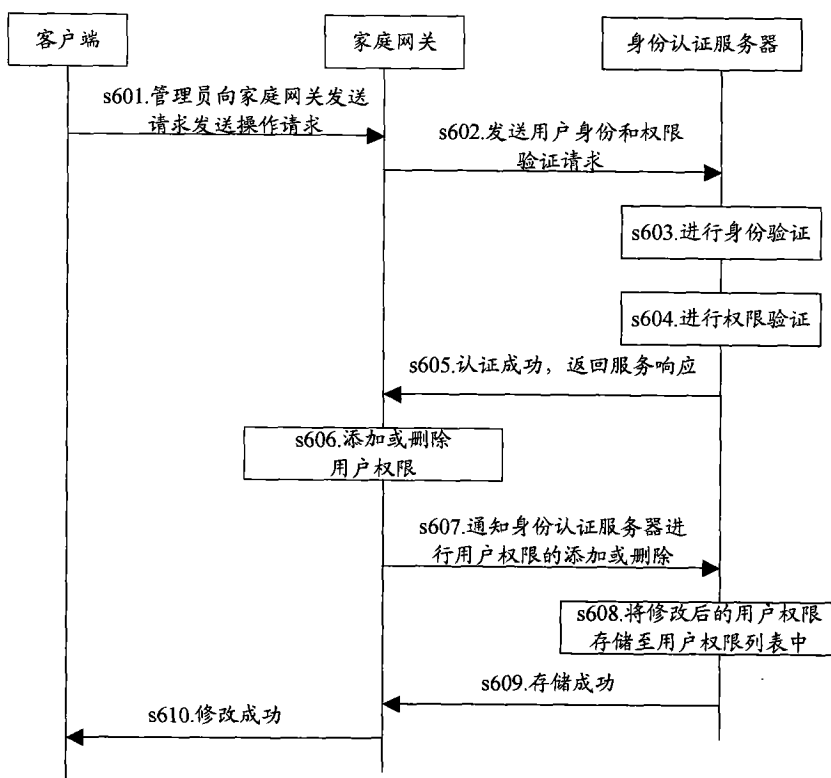


图 6

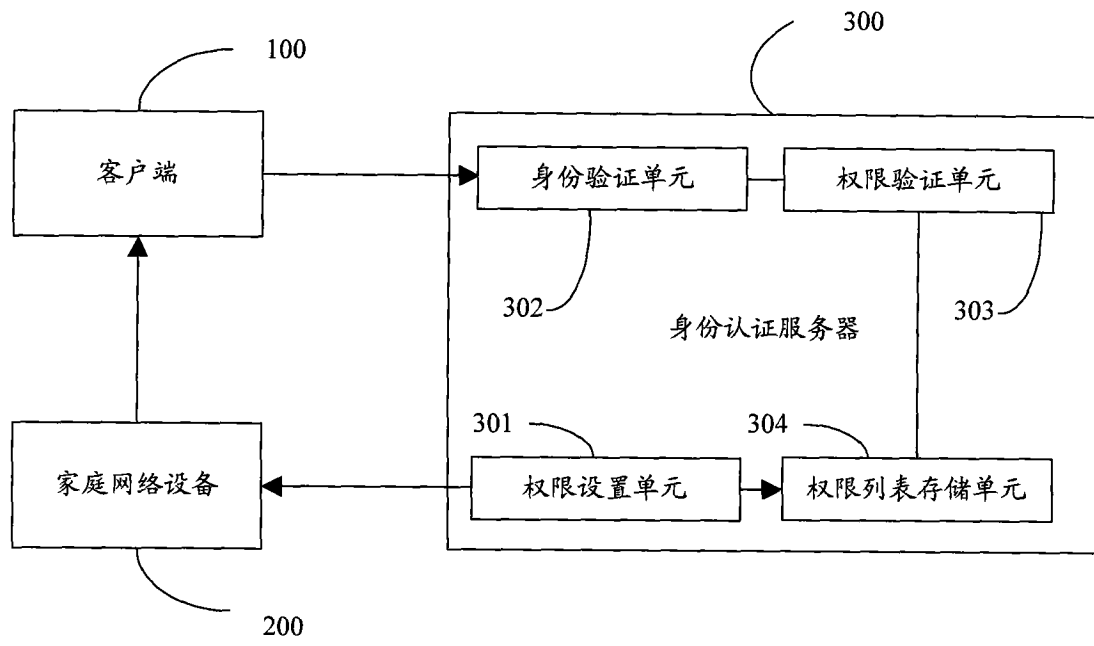


图 7