(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2007 年11 月22 日 (22.11.2007)

PCT

(10) 国际公布号
WO 2007/131415 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) *H04L 12/28* (2006.01)

(21) 国际申请号: PCT/CN2007/001329

(22) 国际申请日: 2007 年4 月23 日 (23.04.2007)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200610060542.3
2006 年4 月28 日 (28.04.2006) CN

(71) 申请人 (对除美国外的所有指定国): 华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): 丁志明(DING, Zhiming) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

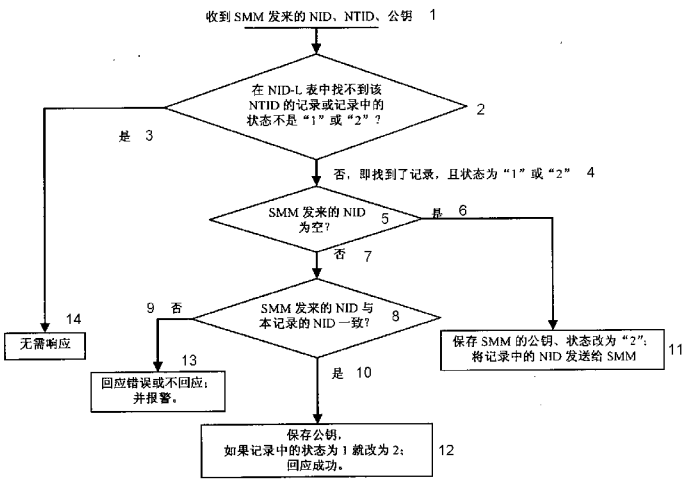
(74) 代理人: 北京集佳知识产权代理有限公司(UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建国门外大街22号赛特广场7层, Beijing 100004 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE,

[见续页]

(54) Title: SYSTEM AND METHOD TO MANAGE HOME NETWORK

(54) 发明名称: 家庭网络安全管理系统及方法



1 RECEIVING NID, NTID, PUBLIC KEY FROM SMM
2 CANNOT FIND NTID RECORD IN NID-L LIST OR STATE IN RECORD IS NOT 1 OR 2?
3 YES
4 NO, NAMELY RECORD IS FOUND, AND STATE IS 1 OR 2
5 WHETHER NID FROM SMM IS NONE?
6 YES
7 NO
8 IS NID FROM SMM CONSISTENT WITH NID IN RECORD?
9 NO
10 YES
11 STORING SMM PUBLIC KEY, CHANGING STATE TO 2, AND TRANSMITTING NID IN RECORD TO SMM
12 STORING SMM PUBLIC KEY, WHEN STATE IN RECORD IS 1, CHANGING STATE TO 2, AND ACKNOWLEDGING SUCCESS
13 ACKNOWLEDGING FALSE OR NO ACKNOWLEDGING, AND ALARMING
14 ACKNOWLEDGMENT IS NEEDLESS

(57) Abstract: A security management system of home network is provided. A home network includes a home gateway, one or more user devices connected to the home gateway, and a security management server is used for home network to provide security management service. Within the home network, there is a security management module used by user devices to provide a security management service. The user devices and the security management module have unique device identifications, and the home network has a unique network identification. By the home gateway the security management server communicates with the security management module. With the network identification and device identification, the security management server and the security management module by home network and user device registration achieve security management for home network. A security management method of home network is also provided.

[见续页]

WO 2007/131415 A1

GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国（除另有指明，要求每一种可提供的地区保护）：ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告。

所引用双字母代码及其它缩写符号，请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

(57) 摘要：

本发明实施例提供了一种家庭网络安全管理系统，所述家庭网络包括家庭网关以及与所述家庭网关连接的一个或多个用户设备；还包括用于为所述家庭网络提供安全管理服务的安全管理服务器；所述家庭网络内部设有用于为所述家庭网络内部的用户设备提供安全服务的安全管理模块；其中，所述用户设备和所述安全管理模块所在设备具有唯一的设备标识，所述家庭网络具有唯一的网络标识；所述安全管理服务器通过所述家庭网关与所述安全管理模块通信，所述安全管理服务器和安全管理模块利用所述网络标识和设备标识通过所述家庭网络的注册和所述用户设备的注册来对所述家庭网络进行安全管理。本发明实施例还提供了一种家庭网络设备安全管理方法。

家庭网络安全管理系统及方法

本申请要求于 2006 年 4 月 28 日提交中国专利局、申请号为 200610060542.3、发明名称为"家庭网络设备安全管理系统及方法"的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及家庭网络设备的安全管理技术，更具体地说，涉及一种家庭网络安全管理系统及方法。

背景技术

目前，传统的只完成接入功能的 ADSL 调制解调器即将由功能更全面的名为"HGW（Home Gateway，家庭网关）"的设备取代。如图 1 所示，家庭网关不仅可完成 ADSL 调制解调器的接入和路由功能，也集成了 LAN 交换功能，还提供防火墙、NAT、QoS、时间服务等，甚至还直接提供 VoIP 服务，而且一般都提供无线接入功能，具有无线网卡的计算机不用连线就可与之相连。

UPnP 技术论坛是由微软公司发起的研究家庭网络设备即插即用技术的组织。它研究通用即插即用（即 UPnP）通信协议，目标是任何智能家电设备包括家用信息设备使用该协议后只要接入网络就可使用，就像现在使用家电一样简单，而不需要使用者具备专门知识。这样的网络就叫 UPnP 网络。

UPnP 协议将网络实体从逻辑上分成 CP（控制点）和设备（Device）。CP 完成对设备的发现和控制，它在启动后主动查询网络上已有设备。设备实现具体应用功能，它在启动后向外宣告自己的存在，以便 CP 可以发现它，并在宣告中公布自己可以产生的事件。CP 发现设备后可以订阅它感兴趣的设备的事件，设备发生事件后就将事件发送给订阅此事件的 CP，CP 可能对设备的事件产生相应的控制。CP 可以是自动完成对设备的控制，也可以是通过人机界面完成对设备的控制。注意，UPnP 说的设备是逻辑上的实体，而不是物理设备。一个物理设备可能由一个或多个 UPnP 设备组成，也可能还包含一个 CP 实体。一个物理设备也可能只由一个 CP 组成。特殊情况下，一个物理设备可以包含多个 CP，例如计算机上的多个软件完成多种 CP 实体的功能。

UPnP 协议中也有一套安全机制，为此增加了 SC（安全控制台）实体。SC

既是 CP 也是设备，作为 CP，它能发现和控制其它设备/SC；作为设备，它能向其它 CP/SC 宣告自己并接受控制。

UPnP 安全机制考虑的是 CP/SC 对安全设备的访问和控制。UPnP 将设备分为安全设备和非安全设备。所谓安全设备，就是对其访问和控制是受限的，需要经过该设备的授权，并且在访问此设备时要对访问设备进行认证。

UPnP 设备是由一个或多个服务组成的，安全设备与非安全设备的区别在于，安全设备具有一个特殊的安全服务。通过设备的安全服务，SC 可以获得操作设备的密钥、证书、访问控制表、所有者列表等信息。UPnP 安全设备使用所有者列表、访问控制表、证书三个要素组成访问权限管理安全框架。

设备保存一份所有者列表，其中会记录哪些 CP/SC 拥有此设备，拥有此设备的 CP/SC（即所有者）对此设备有百分之百的控制权。设备的首个所有者（必然是 SC）通过 UPnP 自动发现协议（SSDP）并结合手工操作来获得对此设备的所有权。安全设备都具有初始密钥系统，为了能实现首次拥有这个操作，安全设备具有安全 ID 和初始密码（注意 SC 也是安全设备），这两者都可以直接从设备机身、其显示器、或其随机卡片获得。当设备的所有者列表为空、且被接入 UPnP 网络时，通过自动发现协议，SC 能发现此设备，通过其具有安全服务的特点确定其为安全设备，并读取设备的安全 ID 然后显示给用户。用户通过安全 ID 识别此设备并选中它，然后可以给其命名。命名以后的设备便以其名字显示而不再是安全 ID（名字保存在 SC 上）。用户可以继续输入设备的初始密码，确认后 SC 将自己的安全 ID 送给设备，设备便将此 SC 加入所有者列表，SC 便拥有了此设备。以后，可以在此 SC 上通过授权操作使其它 SC/CP 拥有此设备。

设备还保存一张访问控制表，向 CP/SC 部分授权。被部分授权的 CP/SC 并不拥有此设备，只能对此设备进行有限的访问。用户可在拥有此设备的 SC 上编辑访问控制表。当我们说设备向 CP/SC 授权时，与设备的所有者 SC 向其它 CP/SC 授权是一个意思，因为一个所有者完全拥有设备，所有者就成了设备的权力代理。

可以操作安全设备的 CP/SC 都持有表明对此设备有合法权限的证书，此证书由设备的所有者 SC 产生。

UPnP 安全机制还使用签名和加密方式保证消息的安全。设备具有初始公钥，SC 可以直接获得。安全设备的安全 ID 实际上就是基于其公钥的一个可视散列值，一般位数较短，只是用于识别，相当于名字，SC 和设备都使用完全相同的散列算法得到这个安全 ID。

UPnP 的安全机制对于有线或无线接入同样适用，当然首先是针对无线接入提出的。有线接入在物理上局限于家庭内部，认为这已经是安全的。如图 2 所示，在无线接入方面，对于非法 CP/SC 由于无法得到安全设备的授权，因此无法对安全设备进行操作，从而保证安全。同样，对于延伸到室外的有线接入，此机制一样起作用。

由前面的描述可知，UPnP 安全机制具有以下一些缺点：

（1）必须有人工干预，其所描述的拥有过程和授权过程并不是一个简单的步骤，仍需用户具备一定的专业知识，例如拥有者列表、访问控制列表等。

（2）UPnP 的安全机制使未经授权的（物理）设备不能访问受权限保护的安全设备，但不能防止非法用户访问那些非安全设备，也不能防止非 UPnP 安全设备接入到网络并经家庭网关接入到互联网，即盗用上网帐户。后者在使用无线接入时极易发生。

（3）UPnP 的设备被转移（例如转卖）前，必须人为将设备恢复到初始状态，即出厂设置和未被拥有。在未恢复初始状态就被转移的情况下（例如被盗窃），易发生帐号盗用情况，例如 VoIP 用户设备一般会将呼叫号码与设备本身关联，设备移到别处后，仍可继续使用原号码拨打 IP 电话。

发明内容

针对现有技术的上述缺陷，本发明实施例要解决现有机制中需要用户手工操作来实现设备的授权访问，且用户帐号和设备易被盗用的问题。

本发明实施例提供的家庭网络安全管理系统，所述家庭网络包括家庭网关以及与所述家庭网关连接的一个或多个用户设备；其中，

所述安全管理系统还包括用于为所述家庭网络提供安全管理服务的安全管理服务器；

所述家庭网络内部设有用于为所述用户设备提供安全服务的安全管理模块；

其中，所述用户设备和所述安全管理模块所在设备具有唯一的设备标识，所述家庭网络具有唯一的网络标识；所述安全管理服务器通过所述家庭网关与所述安全管理模块通信，所述安全管理服务器和安全管理模块通过利用所述网络标识和设备标识通过所述家庭网络的注册和所述用户设备的注册来对所述家庭网络进行安全管理。

本发明实施例提供的家庭网络安全管理方法，包括，

设置安全管理服务器，以及在家庭网络内部设置安全管理模块；

所述安全管理服务器通过所述家庭网络内部的家庭网关与所述安全管理模块通信，所述安全管理服务器和安全管理模块利用网络标识和设备标识通过所述家庭网络的注册和所述用户设备的注册来对所述家庭网络进行安全管理。

由于采取了上述技术方案，本发明实施例至少具有以下有益效果：

（1）只要用户为其设备预先向安全管理服务器申请安全服务，设备接入网络就可自动实现安全服务注册过程，实现了类似于 UPnP 安全机制中的用户手工确认过程，而这个预申请过程不需要用户理解技术问题，只需要提供有关信息。

（2）具有比 UPnP 安全机制更强的访问安全性，所有被访问设备都可以通过注册验证访问设备的合法性。

（3）由于设备注册到安全管理服务器，这样当一个设备被非法转移到另一个网络中后，就会被安全管理服务器发现。由于所设置的安全管理模块，就能够解决用户帐号和设备易被盗用的问题。

附图说明

下面将结合附图及实施例对本发明作进一步说明，附图中：

图 1 是家庭网络的组网示例图；

图 2 是现有机制的示意图；

图 3 是本发明所述系统实施例结构图；

图 4 是本发明所述方法实施例中 SMS 收到 SMM 的网络安全服务注册消息时的处理流程图；

图 5 是本发明所述方法实施例中预先申请了安全服务的非安全 CPE 首次注册安全服务的流程图；

图 6 是本发明所述方法实施例中预先申请了安全服务的安全 CPE 首次注册安全服务的流程图;

图 7 是本发明所述方法实施例中没有预先申请安全服务的非安全 CPE 首次注册安全服务的流程图;

图 8 是本发明所述方法实施例中没有预先申请安全服务的安全 CPE 首次注册安全服务的流程图;

图 9 是本发明所述方法实施例中合法设备再注册安全服务的流程图;

图 10 是本发明所述方法实施例中 SMS 发现非法设备的处理流程图;

图 11 是本发明所述方法实施例中 CPE1 访问 CPE2 的第一步：建立连接时携带 NTID;

图 12 是本发明所述方法实施例中 CPE1 访问 CPE2 的第一步：建立连接时不带 NTID;

图 13 是本发明所述方法实施例中 CPE2 鉴权 CPE1 的流程图;

图 14 是本发明所述方法实施例中用户向 SMS 取消 CPE 的安全服务的流程图;

图 15 是本发明所述方法实施例中转移设备在线确认的流程图。

具体实施方式

本发明实施例利用网络标识（NID）概念，结合唯一的设备标识（NTID），提供一种网络设备安全管理机制。NID 是由一个位于公网（即广域网）的服务器自动分配的或者用户自己指定的字符串，它唯一地标识一个局域网络。NTID 是用户家庭网络中所有设备都支持的具有统一格式并且能唯一地标识一台设备的信息串，它的格式可以是 DSL 论坛技术文献 TR069 定义的“OUI-设备序列号”格式，但不排除使用其它形式的唯一的设备标识信息，例如，家庭网关或所述安全管理模块所在设备的设备标识，广域网接入帐号，互联网域名或固定 IP 地址、用户家庭电话号码等。

如图 3 所示，本发明实施例的系统中，包括一个位于公网上的安全管理服务器（SMS）、家庭网络内部的安全管理模块（SMM）、家庭网络中的所有 CPE（Customer Premises Equipment，用户驻地设备，即用户设备）、以及另一个位于公网的自动配置服务器（ACS）。广义的说，CPE 包含了 SMM 和家庭网关。

下面将分别介绍图 3 中各个功能实体的功能。其中，SMM 可以是独立的物理设备、或者是其它设备的一个功能模块，例如是 HGW 的一个功能模块。

1、安全管理服务器

本发明实施例中，在 WAN（Wide Area Network，广域网）上布置一个安全管理服务器，简称 SMS（Security Management Server）。拥有并管理此服务器的商业实体可称之为家庭网络安全服务提供商，简称 SSP（home network Security Service Provider）。SMS 为家庭网络设备的安全管理提供服务，它具有如下主要功能:

1）接受用户申请网络安全服务。

1.1）用户申请网络安全服务时，提供 SMM 设备的 NTID。

1.2）SMS 自动生成唯一的家庭网络标识 NID（Network Identification，网络标识）和密码，或接受用户指定的 NID 和密码，确保 NID 的唯一性。

1.3）在表 NID-L（NID List，NID 列表）中生成新的记录。NID-L 的结构如表 1 所示。

表 1 - NID-L 的格式

NID	$PSW_{(NID)}$	$NTID_{(SMM)}$	$SKey_{(SMM)}$	用户姓名	用户地址	其它联系方式	状态	备注	最近注册时间

NID: 由 SMS 自动分配或用户指定的唯一性网络标识。

$PSW_{(NID)}$: NID 对应的密码，由 SMS 自动生成或用户指定。

$NTID_{(SMM)}$: 用户 SMM（见后面的描述）设备的唯一标识，由用户在申请网络安全服务时提供。

$SKey_{(SMM)}$: SMM 的加密公钥。

用户姓名: 用户的姓名，也可以增加身份证信息。

用户地址: 用户住址信息。

其它联系方式: 可以是电话号码或电子邮箱等，用于在特殊情况下与用户联系。

状态: 取值如下，

“1” - 已申请，用户的 SMM 还未向 SMS 注册过，新记录的初始值。

“2” - 应用中，用户的 SMM 已经向 SMS 注册过，但不表示设备是否在线。

"3" - 已注销，用户已取消了网络安全服务，这样的记录也可以移到另一张表，保留这样的记录备查。

最近注册时间： 最近一次 SMM 注册安全服务的时间，SMS 接受注册时记录。

备注： 其它有用信息。

2）接受用户家庭网络安全服务注册。

用户申请了网络安全服务后，其网络中的 SMM 就可以向 SMS 注册网络安全服务，以获得自己的 NID。其过程在网络安全服务注册方法中描述。

3）接受用户为其 CPE 预申请安全服务。

3.1）用户为其 CPE 预申请安全服务时，应提供其 NID、$PSW_{(NID)}$、CPE 的 NTID、安全设备的初始密码。

3.2）SMS 在表 NTID-L（NTID List，NTID 列表）中生成新的记录。NTID-L 的格式可以如表 2 所示。

表 2 - NTID-L 的格式：

$NTID_{(CPE)}$	NID	$PSW_{(CPE)}$	状态	最近一次注册时间

$NTID_{(CPE)}$： CPE 的 NTID。

NID： CPE 所属家庭网络的 NID。

$PSW_{(CPE)}$： CPE 的密码，标示于 CPE 的标签、随机卡片或说明书等资料中。对于非安全设备为空。

状态： 取值如下，

"1" - 已申请，用户预先申请了安全服务，尚未在线注册过，新记录的初始值；

"2" - 应用中，用户已在线注册了安全服务，但不表示设备当前是否在线；

"3" - 已注销，用户取消了该设备的安全服务，这样的记录也可以移到另一张表，保留这样的记录备查。

最近注册时间： 最近一次 SMM 为其注册安全服务的时间，SMS 接受注册时记录。

4）接受 CPE 注册安全服务。

只要用户申请了网络安全服务，即获得了 NID，不管用户是否已预先为其

CPE 申请了安全服务，都可以接受 CPE 安全服务注册。CPE 注册安全服务的详细过程将在后面描述。

5）将 SMM 的所有注册事件，包括 SMM 注册网络安全服务和为 CPE 注册设备安全服务生成记录保存。

2、家庭网络内部的安全管理模块

用户家庭网络内部存在一个 SMM（Security Management Module，安全管理模块），它可以是家庭网关的一部分，也可以是独立的设备。其主要功能包括:

1）记录并管理家庭网络中所有 CPE 的 NTID 及其它辅助信息。SMM 使用表 CPE-L（CPE List）管理用户设备，见表 3 所示。

表 3 - SMM 使用的 CPE-L:

$NTID_{(CPE)}$	IP 地址	状态	其它信息

$NTID_{(CPE)}$: CPE 的 NTID。

IP 地址: CPE 在线时的 IP 地址信息，若不在线，此项无定义。

状态: 用于表示 CPE 的状态，可能的取值，

"0" - 不在线;

"1" - 在线。

2）为家庭网络中的 CPE 向 SMS 注册安全服务，其注册过程将在后面描述。

3）当 SMM 不能连接到 SMS 时，能为网络中的 CPE 提供安全服务，并缓存 CPE 上线记录到表 CPE-L-UR（UR 为未向 SMS 注册之意）。其提供安全服务的方法在后面描述。CPE-L-UR 可用表 4 的格式。

表 4 - 未经 SMS 认证的 CPE 上线记录表 CPE-L-UR 的格式

$NTID_{(CPE)}$	上线时间	密码

$NTID_{(CPE)}$: CPE 的 NTID

上线时间: CPE 上电宣告自己的时间，包含年月日时分秒。

密码: 安全设备的密码，对于非安全设备为空，对于已经注册过的安全设备也可能为空。它只在安全设备首次进入用户网络是通过手工确认的时候有用，用来向 SMS 报告此信息，SMS 随后将之保存。

4）当 SMM 能连接到 SMS 时，如果存有未向 SMS 注册的 CPE 上线记录，则发送到 SMS 进行滞后的安全验证。

5）为对网络中的设备所进行的访问进行安全认证服务。

6）保存对网络中设备的访问事件。

3、CPE

为了实现本发明实施例所描述的安全服务，CPE 必须具有以下功能:

1）CPE 在接入网络时应该能宣告自己，在宣告消息中包含自己的 NTID，或者 SMM 收到宣告消息后来查询 NTID 时能反馈 NTID，所述宣告消息可以是广播消息，也可以是点对点发送的消息。这样，网络中的 SMM 在得知 CPE 上线时能得到其 NTID，为其向 SMS 注册安全服务。本实施例以 CPE 在宣告消息中携带 NTID 为例。安全设备还应该在宣告中表明自己是安全设备，SMM 也将在注册消息中包括这个标识。CPE 的宣告消息是一个广播消息，这样，CPE 就不必在一开始就要知道 SMM 的地址。CPE 不必将 SMM 的地址信息保存到永久存储器，而是在每次启动时由 SMM 通知给它。

2）CPE 收到对自己的访问时，可以通过 SMM 鉴别其是否为合法设备。详细过程在安全访问控制方法中描述。当 CPE 不能得到 SMM 的地址时，是否允许其它设备访问它由 CPE 自己决定，本发明不作规定。

3）CPE 可以将对自己的访问事件发送给 SMM 保存。

4、自动配置服务器

自动配置服务器简称 ACS（Auto-Configuration Server），也是 WAN 侧的服务器，用来实现对 CPE 的自动配置。本发明实施例中，要求它发给 SMM 的配置文件中必须有 SMS 的地址信息，以及一个证书。这样在 SMM 获得自动配置时就获得了 SMS 的地址以及能够和 SMS 进行秘密通信的密钥。

下面逐一描述本发明实施例的有关处理方法。

一、网络安全服务注册流程

1）SMM 启动时，如果还不知道 SMS 的地址，就发送请求给 ACS，向 ACS 请求配置；如果 SMM 已经知道了 SMS 的地址，则转步骤 3。

2）ACS 通过某种方式将 SMS 的地址信息、以及一个证书发送给 SMM，例如一个配置文件或通过访问 SMM 的一个数据结点进行设置。

3）SMM 获得 SMS 的地址后，向 SMS 发送网络安全服务注册消息，在注册消息中包含自己的 NTID 和 NID、加密公钥。当 SMM 还未获得 NID 时注册消息中的 NID 为空。SMS 和 SMM 之间的通信需要保证安全性，因此 SMM 需要从 SMS 获得其公钥，用其公钥加密自己发送的信息，并在注册消息中包含自己的加密公钥，之后 SMS 向 SMM 发送消息时可使用 SMM 的公钥加密。SMM 获得 SMS 的公钥应该在发送注册消息之前发生，SMM 可以直接从 SMS 获得，也可以从 SMS 的 CA 处获得，本发明不限定。

4）SMS 收到网络安全服务注册消息后，在表 NID-L 中搜索 SMM 的 NTID，如图 4 所示，

4.1)如果没有找到该 NTID 或找到该 NTID 但记录中的申请标识的值为“3”（表示 NTID 已删除），则忽略，无需发送响应报文。

4.2）如果找到该 NTID，且 SMM 发送的 NID 为空（此时记录中的申请标识应该为“1”），则保存 SMM 发送的 SMM 的公钥信息，申请标识置为“2”，回应注册成功消息并附加记录中的 NID。响应消息使用 SMM 的公钥加密（以下都是如此，不再重复）。

4.3）如果找到该 NTID，但 SMM 发送的 NID 不为空且与记录中的 NID 不一致，则报警，并回应错误或不回应（这种情况不应该发生）。

4.4）如果找到该 NTID，SMM 发送的 NID 不为空且与记录中的 NID 一致（此时记录中的申请标识应该为“2”），则回应注册成功消息。

5）SMM 收到 SMS 的响应消息，

5.1）如果是注册成功，则指示成功注册网络安全服务。如果 SMM 是首次注册，则从响应消息中取出 NID 保存。

5.2）如果是出错信息，则指示未成功注册网络安全服务。

二、CPE 安全服务注册流程

1）CPE 接入网络后，例如，用广播消息宣告自己的存在，在宣告报文中包括自己的 NTID，如果该 CPE 是限制访问的安全设备，则还包括一个表明它是安全设备的标识。

2）SMM 收到 CPE 的宣告消息后，向 SMS 发送 CPE 设备安全服务注册消息，消息中包括 NID、CPE 的 NTID、是否为安全设备的标识。消息使用 SMS

的公钥加密（以下交互消息都是加密的，不再重复）。

3）SMM 发送 CPE 注册消息之后，在 CPE-L 中检索该 CPE 的 NTID:

3.1）若 CPE-L 中存在此 CPE，则将该 CPE 添加到表 CPE-L-UR，见表 4，并将自己的地址告诉 CPE；否则，

3.2）若 CPE-L 中不存在此 CPE，则将该 CPE 添加到未确认的 CPE 列表 CPE-L-UC（UC 为未经用户确认之意）中，并标明是安全设备还是非安全设备，然后等待手工确认或 SMS 的注册结果。CPE-L-UC 的格式见表 5。

表 5 - 未经确认的 CPE 记录表 CPE-L-UC 的格式

$NTID_{(CPE)}$	安全标志

$NTID_{(CPE)}$： CPE 的 NTID

安全标志：取值如下，

0 - 非安全设备;

1 - 安全设备。

4）用户手工确认安全设备

4.1）SMM 将 CPE-L-UC 列表中的 CPE 的 NTID 或 STID（简单终端标识）显示给用户。STID 是使用某种摘要算法得到的 NTID 的摘要信息并使用 BASE64 编码然后取前 4～5 个字符。STID 不能唯一标识一台设备，但在一个家庭内难以重复，并且因为简短而易于阅读。

4.2）用户查看 CPE 的标签、随机卡片、说明书等资料，从中获得该设备的 NTID 或 STID，在 SMM 上查看显示信息，选中所要的 CPE，然后确认。安全设备则要在确认时输入 CPE 的密码。密码同样来自该设备的卡片、标签、说明书等资料。对于非安全设备确认之后转步骤 4.6。

4.3）对于安全设备的确认，SMM 将输入的密码用 CPE 的公钥加密发送给 CPE。安全 CPE 具有初始安全证书，其加密公钥可以直接读取。

4.4）CPE 收到 SMM 发来的密码信息，验证其正确性，向 SMM 回送验证结果，这个结果可能是通过或不通过。

4.5）SMM 收到 CPE 的验证结果，如果是验证不通过，则回到 4.2；否则进入 4.6。

4.6）SMM 添加该 CPE 到表 CPE-L-UR 和 CPE-L，并从表 CPE-L-UC 中

删除，然后将自己的地址告诉该 CPE。然后 SMM 等待 SMS 的响应消息，转步骤 6。

5）接步骤 2，SMS 收到设备安全服务注册消息后，检索 NID-L:

5.1）若 NID-L 中没有指定的 NID，则忽略之，不作任何响应；否则，

5.2）若 NID-L 中存在指定的 NID，SMS 根据 NTID 与 NID 检索 NTID-L:

5.2.1）如果 NTID-L 中找到与指定 NTID、NID 完全匹配的记录，说明该设备已经申请了或注册过安全服务：回应注册成功，如果注册消息指明 CPE 是安全设备，则将 NTID-L 记录中该设备的密码附加在响应消息中；如果此时记录中状态标识为“1”，则将其置为“2”。否则，

5.2.2）如果 NTID-L 中找到指定的 NTID 记录但记录中的 NID 与注册消息中的 NID 不同，则报警，回应 SMM 此 CPE 已在其它网络注册；否则，

5.2.3）如果 NTID-L 中没有指定的 NTID 记录，说明用户没有为此设备预先申请安全服务，则发消息询问 SMM 是否注册，消息中应该包括 NTID。

6）SMM 收到 SMS 对注册消息的响应消息:

6.1）注册响应消息为“注册成功”:

6.1.1）若 SMM 正在等待用户确认该 CPE，则如果 CPE 是非安全设备，直接转 6.1.1.4，否则进行下列步骤:

6.1.1.1）SMM 将 SMS 传送来的密码发送给 CPE。

6.1.1.2）CPE 验证密码的正确性，向 SMM 回送验证结果（通过或不通过）。

6.1.1.3）SMM 收到 CPE 的验证结果，如果是验证不通过，向 SMS 回送出错信息，表示预申请安全服务时出错，同时继续等待用户手工确认，即回到步骤 4；否则，

6.1.1.4）SMM 添加该 CPE 到表 CPE-L，将自己的地址告诉 CPE，并取消等待确认，即从 CPE-L-UC 中删除此 CPE。

6.1.2）若用户已手工确认过了，此时该 CPE 已经从表 CPE-L-UC 删除，并且同时加入到表 CPE-L-UR 和表 CPE-L 中，SMM 的地址也已经告诉 CPE，则将 CPE 从 CPE-L-UR 删除即可，此时 SMS 发送过来的密码被忽略。

6.1.3）或该 CPE 以前注册过，CPE 已经在表 CPE-L 中，经步骤 3.1，CPE 也出现在 CPE-L-UR 中，而且 SMM 的地址也已经告诉 CPE，则将 CPE 从

CPE-L-UR 中删除即可。

6.2）注册响应消息为“CPE 已在其它网络注册”，SMM 向用户提示设备不能应用或不提示，并将该 CPE 从所有表中删除。

6.3）注册响应消息为“询问是否注册”，说明 CPE 没有预先向 SMS 申请安全服务:

6.3.1）如果正在等待用户确认，则等待用户完成确认（见步骤 4），或者可能已经完成确认。

6.3.2）完成手工确认后，向 SMS 发送确实注册消息，并将 CPE 添加到表 CPE-L，但不从表 CPE-L-UR 中删除。对于安全设备，确实注册消息中包含该 CPE 的密码。

7）步骤 6 之后，SMM 可能向 SMS 发送确实要注册的消息或提示密码错误的消息或一直无消息。

7.1）SMS 收到 CPE 密码错误的消息，消息中包括 NID、CPE 的 NTID。SMS 给出提示，请求人工干预修正信息，同时将注册状态改为“1”。

7.2）SMS 收到“确实注册”消息，消息中包括 NID、CPE 的 NTID 和密码（对于非安全设备来说此项为空）。SMS 首先检索 NID-L:

7.2.1）若 NID-L 中没有指定的 NID，则忽略之，不作任何响应；否则，

7.2.2)若 NID-L 中存在指定的 NID,SMS 根据 NTID 与 NID 检索 NTID-L:

7.2.2.1）如果 NTID-L 中找到与指定 NTID、NID 完全匹配的记录，回应注册成功，将 SMM 发来的 CPE 的密码（对于非安全设备来说此项为空）记录到 NTID-L 中，同时将记录中标识置为“2”；否则，

7.2.2.2）如果 NTID-L 中找到指定的 NTID 记录但记录的 NID 与指定的 NID 不同，则报警，回应 SMM 此 CPE 已在其它网络注册；否则，

7.2.2.3）如果 NTID-L 中没有指定的 NTID 记录，直接添加记录，包括记录密码，回应注册成功。

8）对于步骤 5、7 中 SMM 收到 SMS 的“注册成功”消息，还有，

8.1）对于步骤 7.2.2.3 的“注册成功”消息，SMM 将 CPE 从表 CPE-L-UR 中删除。

8.2）SMM 可能需要再给 SMS 回送一个确认消息然后结束会话。

根据前面的描述，对于 CPE 申请安全服务的各种情况，可分别用交互图描述如下。

如果用户预先为非安全设备向 SSP 申请了安全服务，则 CPE 首次向 SMS 注册安全服务的过程如图 5 所示。图中在每一步骤前所标的步骤号对应于第二点的“CPE 安全服务注册流程”中所描述的各步骤，对图 6 至图 15 也同样如此。

如果用户预先为安全设备向 SSP 申请了安全服务，则 CPE 首次向 SMS 注册安全服务的过程如图 6 所示。

如果非安全设备没有预先申请安全服务，只要用户已经为其家庭网络申请了安全服务，则设备接入后可在 SMM 简单确认即可，如图 7 所示。

如果安全设备没有预先申请安全服务，只要用户已经为其家庭网络申请了安全服务，则设备接入后可通过人工确认获得 SMS 的安全服务，如图 8 所示。

对于已经成功注册过安全服务的 CPE，其再注册过程如图 9 所示。

如果一台 CPE 在其它网络成功注册过安全服务或事先被申请了安全服务，移到一个不属于它的网络中使用时，SMS 能够发现并报警，如图 10 所示。

三、没有 SMS 时的安全服务

本机制用于保证当 SMM 不能访问 SMS 时用户家庭网络仍可以正常运行。它体现在，设备首次注册时并不需要一定等待 SMS 的响应，用户可以通过手工确认使 CPE 获得 SMM 的安全服务。见前述第二点中的步骤 4。

在前述第二点中，如果 SMM 不能访问 SMS，手工确认过程可以起作用。此时，SMM 保存所有未向 SMS 注册的 CPE 的有关信息，它们存储在 CPE-L-UR 中。

当 SMM 能够访问 SMS 时，把表 CPE-L-UR 中 CPE 的 NTID 等信息送给 SMS 进行滞后注册。方法同前述第二点中一样，只是在时间上是滞后的行为。SMS 能从这种滞后的安全服务注册行为中发现非法设备，这是 SMS 在这种情况下最主要的作用。而用户不能修改 SMM 中的 CPE-L-UR 信息。

四、安全访问控制方法

1、家庭网络内部设备之间的访问

当家庭网络内部一个设备访问另一个设备时，可以先发送一个访问请求，

在访问请求中包含自己的NTID,也可以象常规那样直接开始建立连接的过程。

被访问设备收到建立连接的请求时,如果之前没有收到访问者主动发送来的 NTID，则向访问者查询其 NTID。访问者收到这种查询时，必须告知被访问者自己的NTID。

被访问者向 SMM 查询访问者的 NTID 是否合法。方法是被访问设备调用 SMM 的一个接口，SMM 检查 CPE-L 列表，如果访问设备的 NTID 在 CPE-L 中，则认为该设备合法，否则为不合法。

建立连接的过程示如图 11 和图 12 所示，其中图 11 示出的是请求建立连接时携带了 NTID 的处理流程，图 12 示出的是请求建立连接时未携带 NTID 的处理流程。

如图 13 所示，被访问设备可以对访问设备进行鉴权。设备自己保存一个访问权限表，有权访问自己的设备其NTID和认证密钥将出现在这个表中。当被访问设备发现访问者没有出现在这个表中或鉴权不通过（即图 13 中的密码检查不通过）时，向 SMM 报告此事件；用户可以通过 SMM 手工确认访问设备是否确有权限访问被访问设备。如果 SMM 确认访问设备确有权限访问被访问设备，则 SMM 从被访问者读取一个密码转发给访问者。SMM 与被访问者之间的通信是秘密传输的。SMM 与访问者之间也应该是秘密传输的。如果访问者没有证书，则 SMM 给其下发一个，否则就使用其原有的。

CPE从SMM获得证书的过程可以是这样的:CPE随机生成一个对等密钥，使用 SMM 的公钥加密传输给 SMM。SMM 使用 CPE 的对等密钥加密一个证书发给CPE。

SMM 发给 CPE 的证书可以是自己生成的，也可以从 SMS 获取。SMS 在 SMM 的请求下生成一个证书发送给 SMM。

CPE 鉴权另一个 CPE 的过程见图 13。

2、家庭网络内部设备访问外部

当家庭网络内部设备访问外部时，必然要经过 HGW（家庭网关），HGW 可采用上述相同方法验证设备合法性,并使用同样的访问权限列表来限制设备的权限,经过确认的合法设备允许穿过此网关,未被确认的合法设备不能穿过。这相当于建立了一个过滤列表，但不是事先编辑好的，而是当设备访问外部网

络时即时建立的。

3、外部设备访问家庭网络内部设备

前述家庭网络内部的设备之间的访问控制机制，同样适用于网络外部设备访问家庭网络内部设备。

用户自己的可游牧设备可以预先在 SMS 申请安全服务，或从家庭网络内部进行手工确认的安全服务注册并确实注册到 SMS。当该游牧设备从公共接入点接入网络时，它的宣告消息不会起作用，因为所处环境中没有 SMM，但这并不影响它接入互联网，因为用户设备并没有直接的与 SMM 通信。

当游牧设备访问到用户家庭网络内的某个 CPE 时，该 CPE 会询问游牧设备的 NTID，然后向 SMM 查询。后续过程与家庭网络内部的访问是一样的。

五、设备注销

用户将自己的设备转让予其他人，应该注销该设备在 SMS 上的安全服务，这样受转让人才可为该设备申请安全服务，以免该设备在另一个网络接入时 SMS 报警。注销过程如图 14 所示，其中，用户向 SMS 发送取消安全服务请求，其中带有要注销设备的 NTID，SMS 在其 NTID－L 中找到相应记录，将其状态置为“3”，然后向用户回传注销成功消息；同时，SMS 向 SMM 发送注销安全服务消息，其中带有要注销设备的 NTID，由 SMM 在其 CPE－L 中找到相应记录并将其删除。

用户也可以在家庭内部的 SMM 上进行操作，删除一个设备，然后 SMM 向 SMS 发送注销安全服务请求，其中带有要注销设备的设备标识，安全管理服务器在 NTID－L 记录表中找到相应记录，将其状态置为“3”，然后向用户回传注销成功消息。

六、在线设备转移

如图 15 所示，用户转移其设备时，也可以不用前述注销方法。接受设备的用户将设备接入其网络后，SMS 可在其报警环节发送一个消息给设备的原用户家庭网络中的 SMM，该消息中包括：新用户的户名和/或地址等信息、被转移设备的 NTID。设备原用户的 SMM 将显示：“您的设备 xxxx 出现在 xxx 家里，其地址是 xxxxx，您确认吗？”，原用户只要选择“是”即可。SMS 收到原用户的确认消息后，将 NTID-L 表中原记录的状态改为“3”，并自动生成新

的记录。

由前述优选实施例可知，本发明实施例具有以下有益效果:

（1）预申请过程不需要用户理解技术问题，只需要提供有关信息。

（2）同时兼容 UPnP 或类似的手工安全确认机制，用户根据自己的情况选择采用预申请还是自己手工确认。

（3）具有比 UPnP 安全机制更强的访问安全性，所有被访问设备都可以验证访问设备的合法性。

（4）由于设备注册到 SMS，一个设备被非法转移到另一个网络中将被 SMS 发现。只要接入网络提供商强制用户家庭网络中存在这样一个 SMM 并且可验证，例如 SMM 是家庭网关的必备模块，则本条所说效果就可得到体现。

权 利 要 求

1、一种家庭网络安全管理系统，所述家庭网络包括家庭网关以及与所述家庭网关连接的一个或多个用户设备，其特征在于，

所述安全管理系统还包括用于为所述家庭网络提供安全管理服务的安全管理服务器；

所述家庭网络内部设有用于为所述用户设备提供安全服务的安全管理模块；

其中，所述用户设备和所述安全管理模块所在设备具有唯一的设备标识，所述家庭网络具有唯一的网络标识；所述安全管理服务器通过所述家庭网关与所述安全管理模块通信，所述安全管理服务器和安全管理模块利用所述网络标识和设备标识通过所述家庭网络的注册和所述用户设备的注册来对所述家庭网络进行安全管理。

2、根据权利要求 1 所述的家庭网络安全管理系统，其特征在于，所述安全管理模块是独立的物理设备、或者是所述家庭网关的一个功能模块。

3、一种家庭网络安全管理方法，其特征在于，

设置安全管理服务器，以及在家庭网络内部设置安全管理模块；

所述安全管理服务器通过所述家庭网络内部的家庭网关与所述安全管理模块通信，所述安全管理服务器和安全管理模块利用网络标识和设备标识通过所述家庭网络的注册和所述用户设备的注册来对所述家庭网络进行安全管理。

4、根据权利要求 3 所述的方法，其特征在于，所述家庭网络的注册包括：

所述安全管理服务器接收到所述安全管理模块发送的网络安全服务注册消息，该消息中至少包含所述安全管理模块所在设备的设备标识和所述安全管理模块所述家庭网络的网络标识，查找安全管理模块的设备标识；

如果有效找到该设备标识，则进行相应家庭网络的注册。

5、根据权利要求 3 所述的方法，其特征在于，网络标识是由所述安全管理服务器自动分配或由用户指定，或者任意采用下述信息的一个作为网络标识：家庭网关或所述安全管理模块所在设备的设备标识，广域网接入帐号，互联网域名或固定 IP 地址、用户家庭电话号码。

6、根据权利要求 3 所述的方法，其特征在于，所述用户设备的注册包括：

安全管理模块获取所述用户设备的设备标识;

所述安全管理模块向所述安全管理服务器发送所述用户设备注册消息，所述注册消息中包含所述用户设备的设备标识和网络标识;

所述安全管理服务器收到所述注册消息后，查找是否有所述安全管理模块所属家庭网络的网络标识以及所述网络标识下是否有所述用户设备的设备标识，并根据查找结果向安全管理模块发送相应的响应消息;

安全管理模块根据安全管理服务器发回的响应消息作相应的处理，如果所述响应消息指示“注册成功”，则安全管理模块将所述用户设备的设备标识添加到安全管理模块的记录表中。

7、根据权利要求 6 所述的方法，其特征在于，如果用户设备首次向安全管理服务器注册，则在发给所述安全管理模块的响应消息中附加所述用户设备的密码;

安全管理模块收到该响应消息后，将安全管理服务器传送来的密码发送给用户设备;用户设备验证所述密码的正确性，并向安全管理模块发送验证结果;如果验证为通过，则安全管理模块将所述用户设备的设备标识添加到安全管理模块的记录表，并记录此设备的密码。

8、根据权利要求 6 所述的方法，其特征在于，如果所述安全管理服务器上没有所述用户设备的设备标识信息， 则安全管理模块收到安全管理服务器传送来的响应消息后，将用户设备的设备标识信息显示给用户，提示用户进行确认，当用户确认之后，安全管理模块将所述用户设备的设备标识添加到安全管理模块的记录表;

安全管理模块向安全管理服务器发送确实注册消息，安全管理服务器收到该消息后，记录所述用户设备的设备标识，并向安全管理模块回应注册成功消息。

9、根据权利要求 6 所述的方法，其特征在于如果所述安全管理服务器上没有所述用户设备的设备标识信息，则:

安全管理模块收到该响应消息后，提示用户对所述用户设备的设备标识信息进行确认;

安全管理模块收到用户输入的所述用户设备密码后，将其发送给用户设备

进行验证;

安全管理模块接收所述用户设备的验证结果，如果所述验证结果为通过，则安全管理模块将所述用户设备的设备标识添加到安全管理模块的记录表;

安全管理模块向安全管理服务器发送确实注册消息，安全管理服务器收到该消息后，记录所述用户设备的设备标识，并向安全管理模块回应注册成功消息。

10、根据权利要求 6 所述的方法，其特征在于，当安全管理模块不能访问安全管理服务器时，安全管理模块获取所述用户设备的设备标识后，

安全管理模块提示用户输入所述用户设备要求的密码对所述用户设备的设备标识信息进行确认;

安全管理模块收到用户输入的密码后，将其发送给所述用户设备进行验证并接收验证结果;

如果所述验证结果为通过，安全管理模块将所述用户设备的设备标识添加到安全管理模块的记录表。

11、根据权利要求 6 所述的方法，其特征在于，当家庭网络内部一个用户设备访问另一个用户设备，或一个家庭网络外部的用户设备访问家庭网络内部的一个用户设备时，按以下步骤进行:

由访问设备向被访问设备发送一个访问请求;

被访问设备收到该访问请求后，向访问设备查询其设备标识;

访问设备将自己的设备标识发送给被访问设备;

被访问设备将访问设备的设备标识发送给本家庭网络中的安全管理模块请求验证其合法性;

所述安全管理模块检查其记录表中是否有访问设备的设备标识，并向所述被访问设备发送相应的响应信息，如果有则为合法，否则为不合法;

当访问设备的设备标识为合法时，允许所述访问设备与之建立连接。

12、根据权利要求 6 所述的方法，其特征在于，当家庭网络内部一个用户设备访问所述家庭网络外部的设备时，按以下步骤进行:

访问设备向家庭网络外部发送报文;

家庭网关转发此报文时，如果是所述访问设备首次向家庭网络外部的设备

发送报文，则向所述访问设备查询其设备标识；

访问设备将自己的设备标识发送给家庭网关；

家庭网关将访问设备的设备标识发送给安全管理模块请求验证其合法性；

所述安全管理模块检查其第三记录表中是否有访问设备的设备标识，并向所述家庭网关发送相应的响应信息，如果有则为合法，否则为不合法；

当访问设备的设备标识为合法时，允许所述访问设备访问所述家庭网络外部的设备。

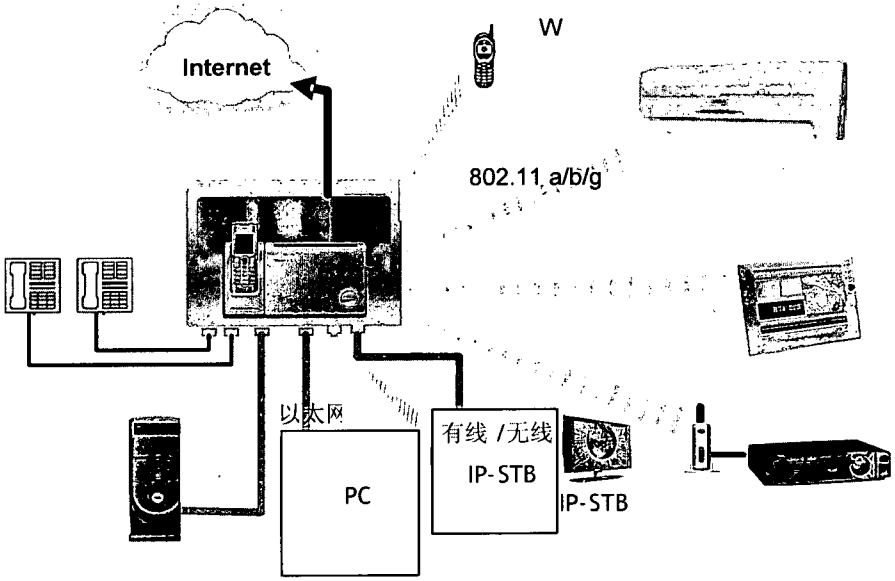

Internet
W
802.11 a/b/g
以太网
PC
有线 /无线
IP-STB
IP-STB

图 1

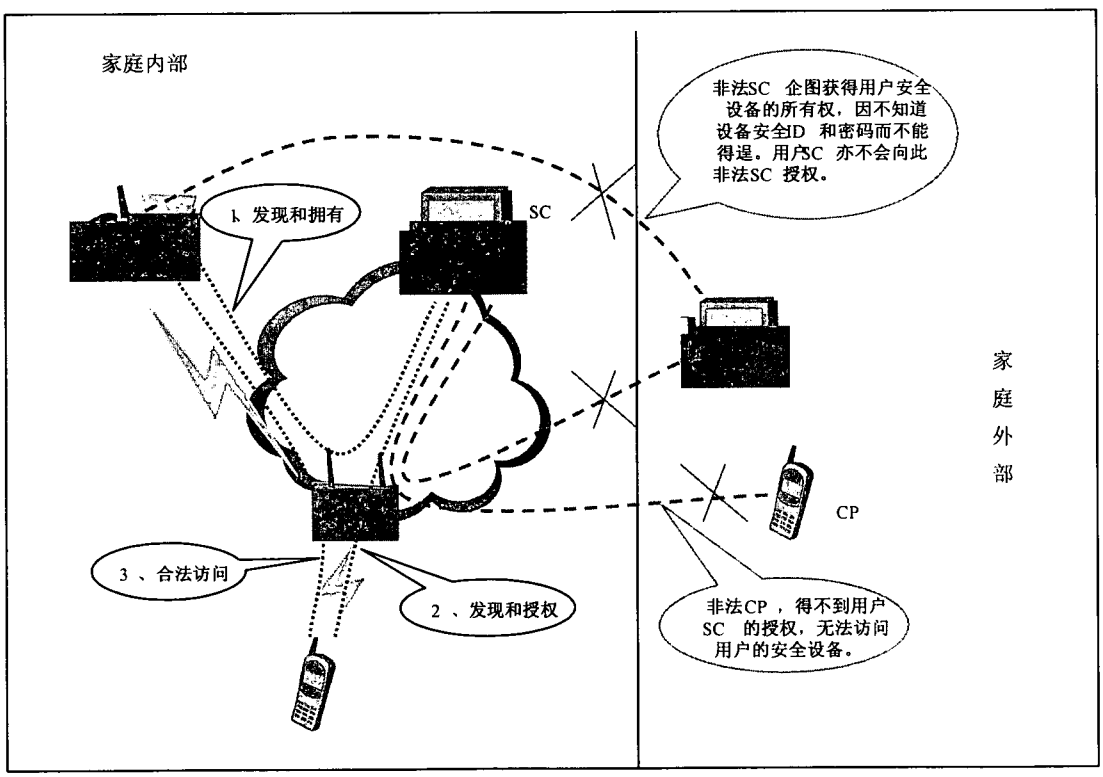

家庭内部
非法SC 企图获得用户安全设备的所有权，因不知道设备安全ID 和密码而不能得逞。用户SC 亦不会向此非法SC 授权。
1、发现和拥有
SC
家庭外部
CP
3 、合法访问
2 、发现和授权
非法CP ，得不到用户SC 的授权，无法访问用户的安全设备。

图 2

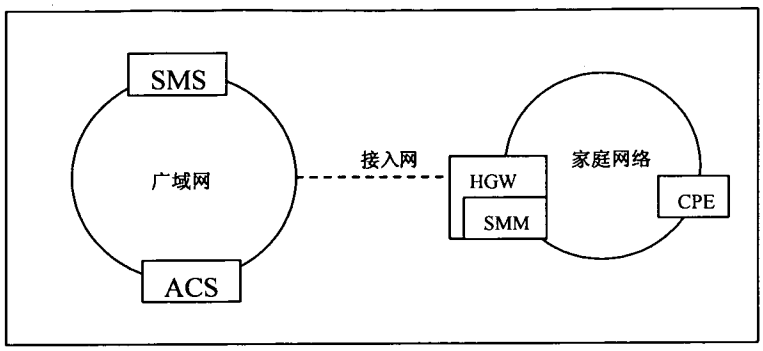

SMS
广域网
ACS
接入网
HGW
SMM
家庭网络
CPE

图 3

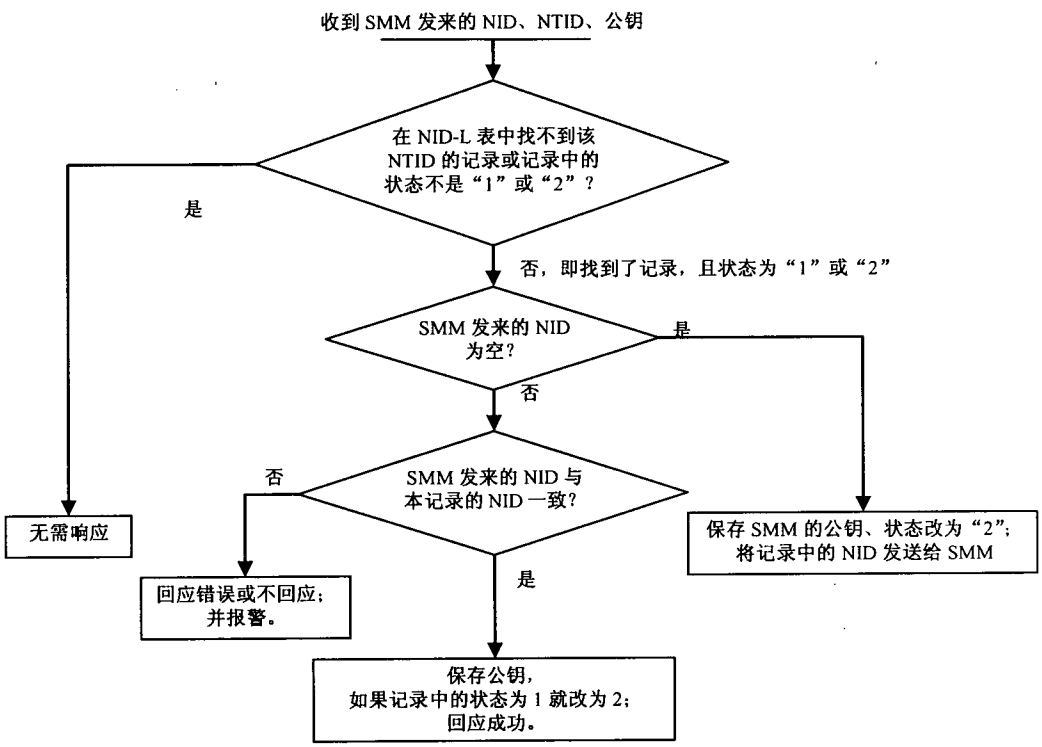

收到 SMM 发来的 NID、NTID、公钥
在 NID-L 表中找不到该 NTID 的记录或记录中的状态不是“1”或“2”？
是
否，即找到了记录，且状态为“1”或“2”
SMM 发来的 NID 为空？
是
否
SMM 发来的 NID 与本记录的 NID 一致？
否
是
无需响应
回应错误或不回应；并报警。
保存 SMM 的公钥、状态改为“2”；将记录中的 NID 发送给 SMM
保存公钥，如果记录中的状态为 1 就改为 2；回应成功。

图 4

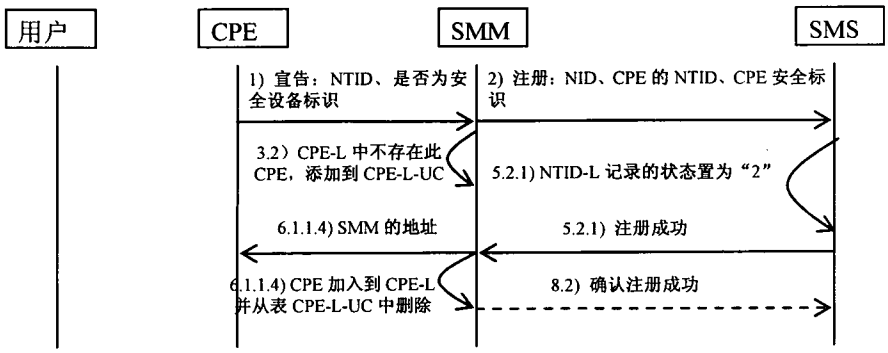

用户
CPE
SMM
SMS
1) 宣告：NTID、是否为安全设备标识
2) 注册：NID、CPE 的 NTID、CPE 安全标识
3.2) CPE-L 中不存在此 CPE，添加到 CPE-L-UC
5.2.1) NTID-L 记录的状态置为“2”
6.1.1.4) SMM 的地址
5.2.1) 注册成功
6.1.1.4) CPE 加入到 CPE-L 并从表 CPE-L-UC 中删除
8.2) 确认注册成功

图 5

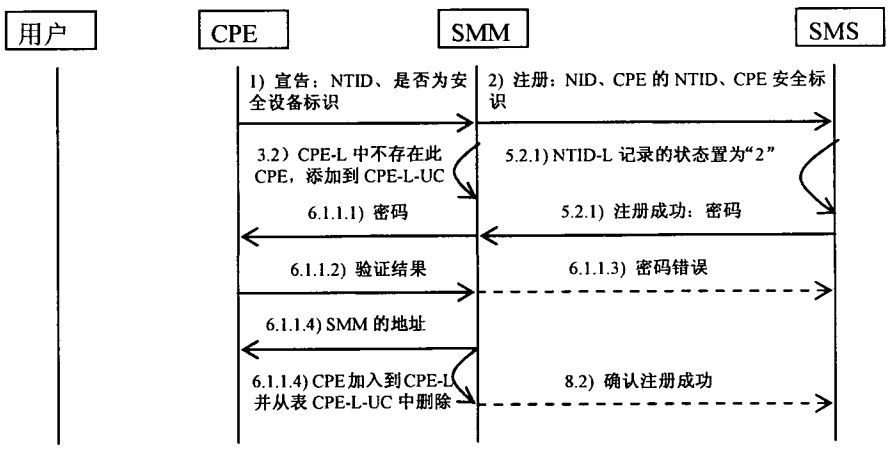

用户
CPE
SMM
SMS
1) 宣告：NTID、是否为安全设备标识
2) 注册：NID、CPE 的 NTID、CPE 安全标识
3.2) CPE-L 中不存在此 CPE，添加到 CPE-L-UC
5.2.1) NTID-L 记录的状态置为“2”
6.1.1.1) 密码
5.2.1) 注册成功：密码
6.1.1.2) 验证结果
6.1.1.3) 密码错误
6.1.1.4) SMM 的地址
6.1.1.4) CPE加入到CPE-L 并从表 CPE-L-UC 中删除
8.2) 确认注册成功

图 6

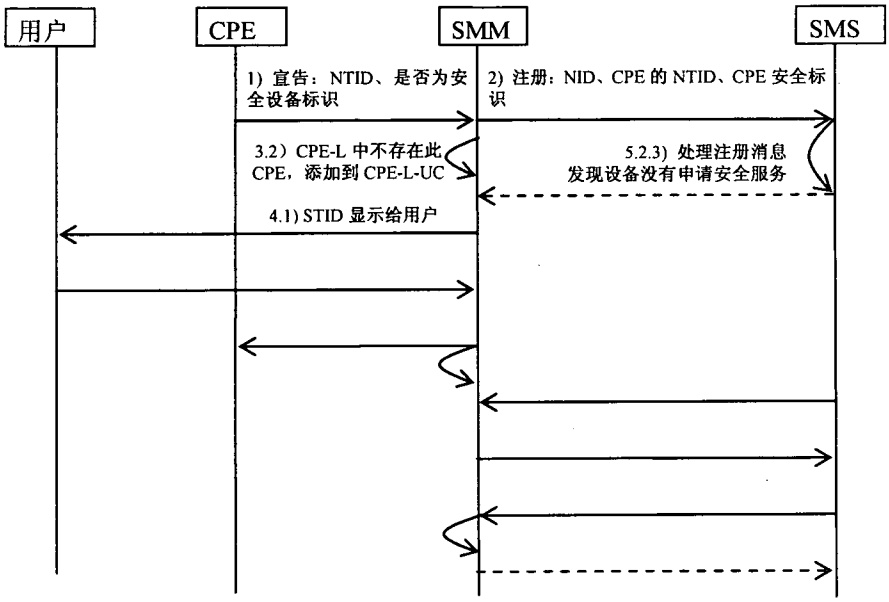

用户
CPE
SMM
SMS
1) 宣告：NTID、是否为安全设备标识
2) 注册：NID、CPE 的 NTID、CPE 安全标识
3.2) CPE-L 中不存在此 CPE，添加到 CPE-L-UC
5.2.3) 处理注册消息
发现设备没有申请安全服务
4.1) STID 显示给用户

图 7

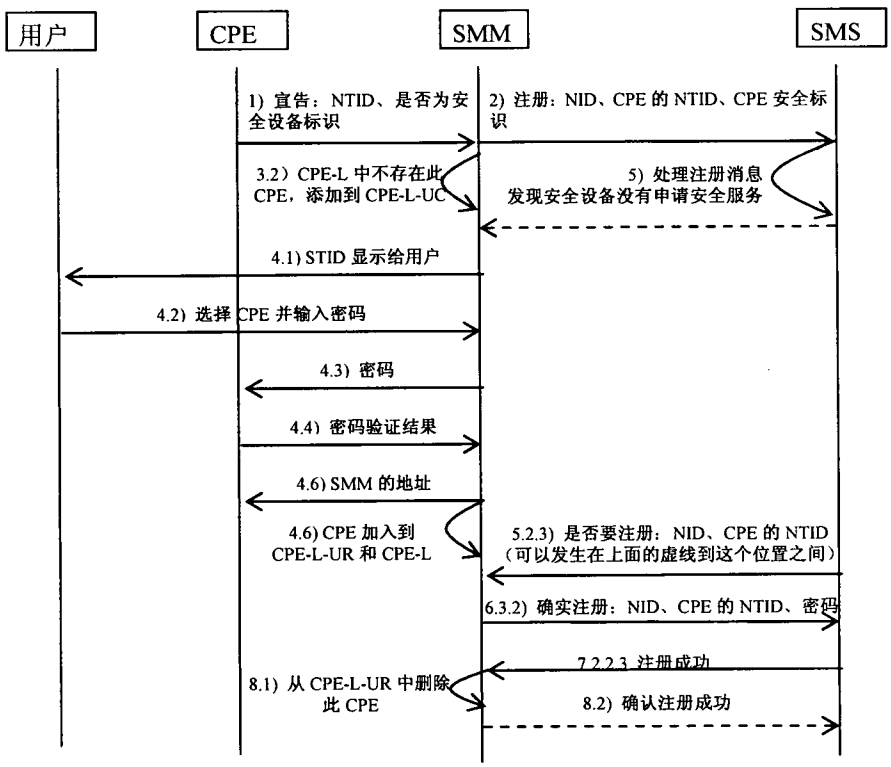

用户
CPE
SMM
SMS
1) 宣告：NTID、是否为安全设备标识
2) 注册：NID、CPE 的 NTID、CPE 安全标识
3.2) CPE-L 中不存在此 CPE，添加到 CPE-L-UC
5) 处理注册消息
发现安全设备没有申请安全服务
4.1) STID 显示给用户
4.2) 选择 CPE 并输入密码
4.3) 密码
4.4) 密码验证结果
4.6) SMM 的地址
4.6) CPE 加入到 CPE-L-UR 和 CPE-L
5.2.3) 是否要注册：NID、CPE 的 NTID
（可以发生在上面的虚线到这个位置之间）
6.3.2) 确实注册：NID、CPE 的 NTID、密码
7.2.2.3 注册成功
8.1) 从 CPE-L-UR 中删除此 CPE
8.2) 确认注册成功

图 8

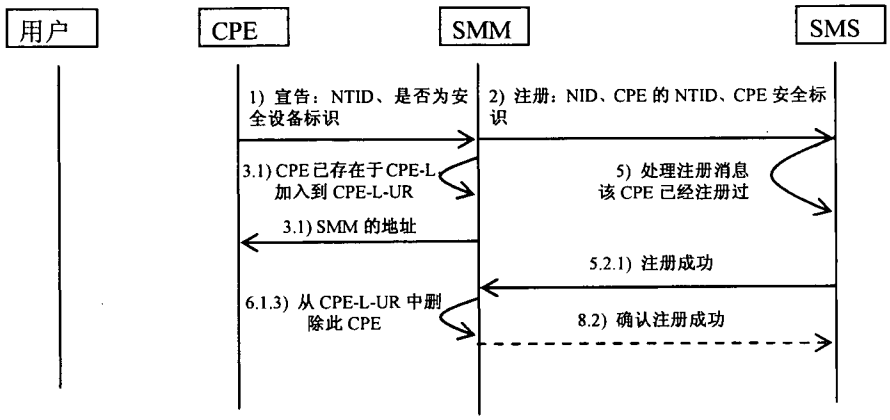

用户
CPE
SMM
SMS
1) 宣告：NTID、是否为安全设备标识
2) 注册：NID、CPE 的 NTID、CPE 安全标识
3.1) CPE 已存在于 CPE-L，加入到 CPE-L-UR
5) 处理注册消息
该 CPE 已经注册过
3.1) SMM 的地址
5.2.1) 注册成功
6.1.3) 从 CPE-L-UR 中删除此 CPE
8.2) 确认注册成功

图 9

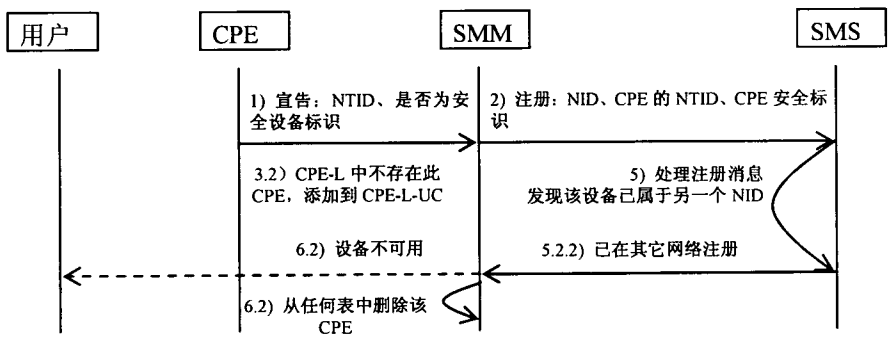

用户
CPE
SMM
SMS
1) 宣告：NTID、是否为安全设备标识
2) 注册：NID、CPE 的 NTID、CPE 安全标识
3.2) CPE-L 中不存在此 CPE，添加到 CPE-L-UC
5) 处理注册消息
发现该设备已属于另一个 NID
6.2) 设备不可用
5.2.2) 已在其它网络注册
6.2) 从任何表中删除该 CPE

图 10

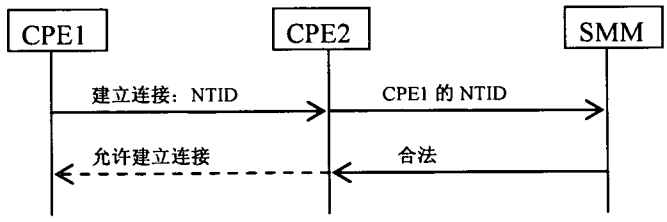

CPE1
CPE2
SMM
建立连接：NTID
CPE1 的 NTID
允许建立连接
合法

图 11

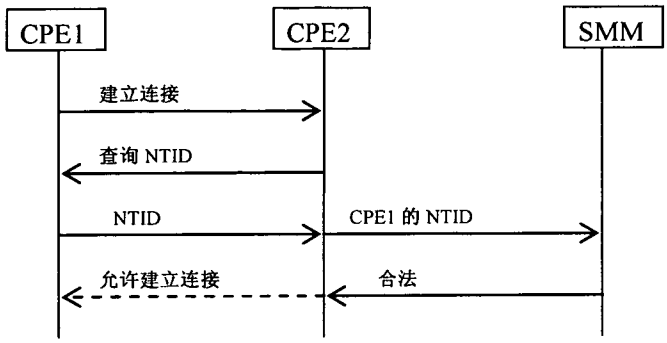

CPE1
CPE2
SMM
建立连接
查询 NTID
NTID
CPE1 的 NTID
允许建立连接
合法

图 12

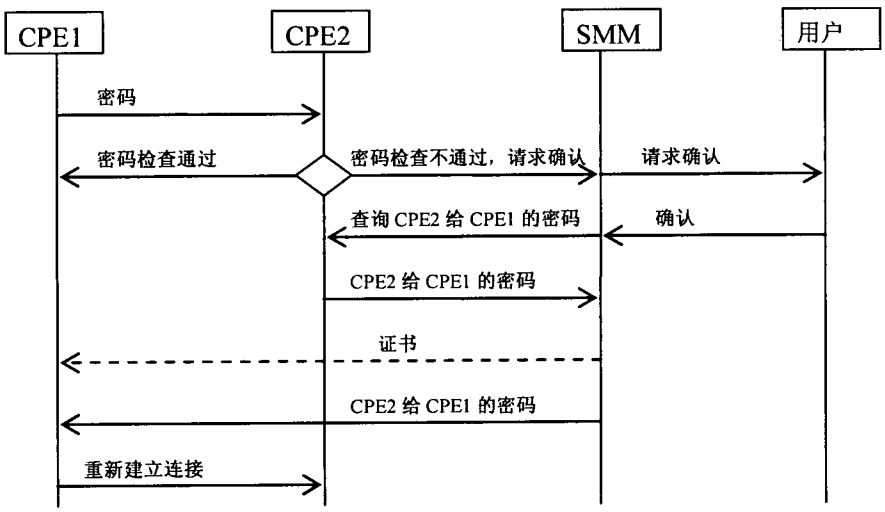

CPE1
CPE2
SMM
用户
密码
密码检查通过
密码检查不通过，请求确认
请求确认
查询 CPE2 给 CPE1 的密码
确认
CPE2 给 CPE1 的密码
证书
CPE2 给 CPE1 的密码
重新建立连接

图 13

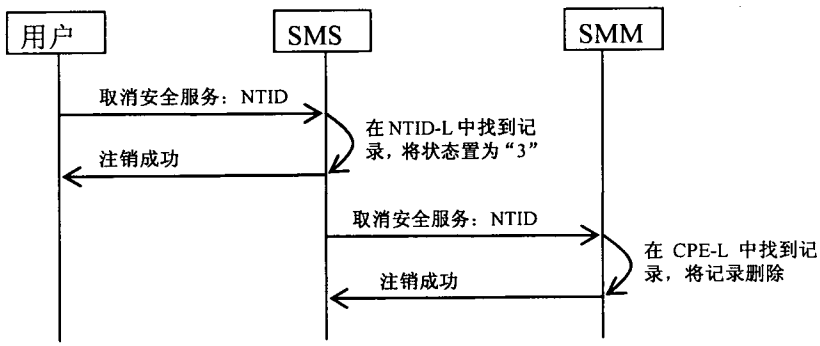

用户
SMS
SMM
取消安全服务：NTID
在 NTID-L 中找到记录，将状态置为“3”
注销成功
取消安全服务：NTID
在 CPE-L 中找到记录，将记录删除
注销成功

图 14

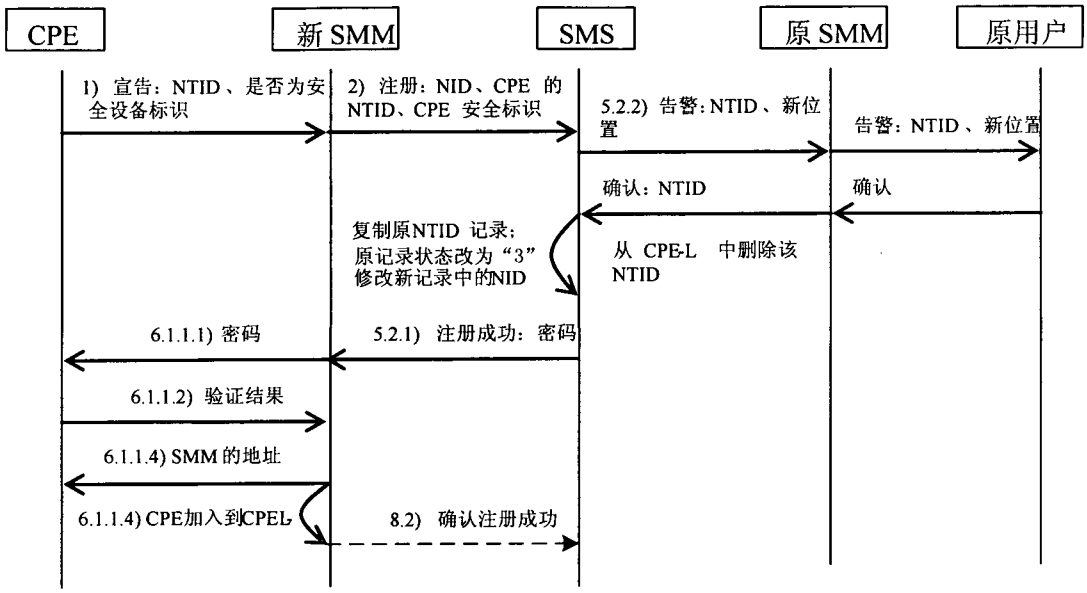

CPE
新 SMM
SMS
原 SMM
原用户
1) 宣告：NTID、是否为安全设备标识
2) 注册：NID、CPE 的 NTID、CPE 安全标识
5.2.2) 告警：NTID、新位置
告警：NTID、新位置
确认：NTID
确认
复制原NTID 记录；
原记录状态改为“3”
修改新记录中的NID
从 CPE-L 中删除该 NTID
6.1.1.1) 密码
5.2.1) 注册成功：密码
6.1.1.2) 验证结果
6.1.1.4) SMM 的地址
6.1.1.4) CPE加入到CPE-L
8.2) 确认注册成功

图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/001329

A. CLASSIFICATION OF SUBJECT MATTER

See Extra Sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[8] H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI,PAJ,EPODOC,CNKI,CNPAT: network,upnp, home, id, identif+, manag+, regist+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US2005/0086514A1(SAMSUNG ELECTRONICS CO.,LTD) 21 Apr.2005 (21.04.2005) page 1, line 2-page 3, line 30,Figs. 1-2	1-12
A	CN1481120A(LENOVO BEIJING CO., LTD)10 Mar.2004(10.03.2004) the whole document	1-12
A	CN1561136A(UT SIDAKANG COMMUNICATION CO., LTD)5 Jan.2005 (05.01.2005) the whole document	1-12

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 July 2007(04.07.2007)	**02 Aug. 2007 (02.08.2007)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer YANG, Ruili Telephone No. (86-10)82336247

Form PCT/ISA /210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/001329

CLASSIFICATION OF SUBJECT MATTER

H04L9/32 (2006.01)i

H04L12/28 (2006.01)i

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/001329

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN1750461A(LG ELECTRONIC SHENYANG CO., LTD)22 Mar.2006 (22.03.2006) the whole document	1-12
A	CN1747427A(LG ELECTRONIC TIANJIN CO., LTD)15 Mar.2006 (15.03.2006) the whole document	1-12
PX	CN1863195A(ZHONGXING COMMUNICATION CO., LTD)15 Nov.2006 (15.11.2006) page 3, line 15-page 5, line 16, Fig.2	1,3

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2007/001329

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
US2005/0086514A1	21.04.2005	EP1521423A2	06.04.2005
		JP2005117631A	28.04.2005
		CN1604552A	06.04.2005
		KR20050032856A	08.04.2005
CN1481120A	10.03.2004	NONE	
CN1561136A	05.01.2005	NONE	
CN1750461A	22.03.2006	NONE	
CN1747427A	15.03.2006	NONE	
CN1863195A	15.11.2006	NONE	

国际检索报告

国际申请号
PCT/CN2007/001329

A. 主题的分类

参见附加页

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC[8] H04L H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

WPI,PAJ,EPODOC,CNKI,CNPAT: 家庭,网络,标示,标识,标志,管理,注册,upnp, network, home, id, identif+, manag+, regist+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	US2005/0086514A1(SAMSUNG ELECTRONICS CO.,LTD) 21.4 月 2005 (21.04.2005)说明书第 2 页第 2 行至第 3 页第 30 行，附图 1-2	1-12
A	CN1481120A(联想(北京)有限公司)10.3 月 2004(10.03.2004)全文	1-12
A	CN1561136A(UT 斯达康通讯有限公司)5.1 月 2005(05.01.2005)全文	1-12
A	CN1750461A(乐金电子(沈阳)有限公司)22.3 月 2006(22.03.2006)全文	1-12
A	CN1747427A(乐金电子(天津)电器有限公司)15.3 月 2006(15.03.2006)全文	1-12
PX	CN1863195A(中兴通讯股份有限公司)15.11 月 2006(15.11.2006) 说明书第 3 页第 15 行至第 5 页第 16 行，附图 2	1，3

☐ 其余文件在 C 栏的续页中列出。 ☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
4.7 月 2007（04.07.2007）	**02.8 月 2007 (02.08.2007)**
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 杨瑞丽 电话号码：(86-10) **82336247**

主题的分类：

H04L9/32 (2006.01)i

H04L12/28 (2006.01)i

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2007/001329

检索报告中引用的专利文件	公布日期	同族专利	公布日期
US2005/0086514A1	21.04.2005	EP1521423A2	06.04.2005
		JP2005117631A	28.04.2005
		CN1604552A	06.04.2005
		KR20050032856A	08.04.2005
CN1481120A	10.03.2004	无	
CN1561136A	05.01.2005	无	
CN1750461A	22.03.2006	无	
CN1747427A	15.03.2006	无	
CN1863195A	15.11.2006	无	