(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 101437223 B
(45)授权公告日 2011.11.02

(21)申请号 200710187239.4

(22)申请日 2007.11.16

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 陈璟

(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.
H04W 12/02(2006.01)
H04W 12/06(2006.01)

(56)对比文件
US 2007/0054668 A1,2007.03.08, 全文.
CN 1905452 A,2007.01.31, 全文.
US 2006/0005025 A1, 全文.
WO 2007/057732 A1,2007.05.24, 说明书第1页第4段,第4页第2段至第6页第1段,附图1-3.
C. Kaufman, Ed..Internet Key Exchange (IKEv2) Protocol.IETF RFC4306.2005,5,31.

审查员 孙丽丽

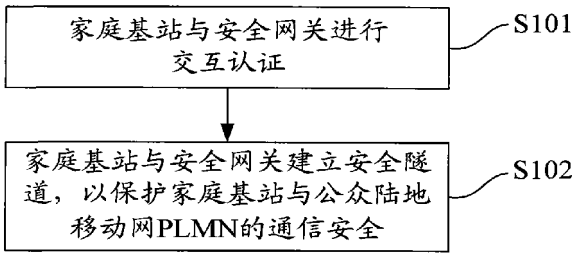
权利要求书 3 页 说明书 8 页 附图 5 页

(54)发明名称

一种家庭基站接入的方法、系统和装置

(57)摘要

本发明公开了一种家庭基站接入的方法,包括以下步骤:家庭基站与安全网关进行交互认证;所述家庭基站与所述安全网关建立安全隧道,以保护所述家庭基站与公众陆地移动网PLMN网络的通信安全。通过本发明实施例,家庭基站与PLMN网络的安全网关进行交互认证,并建立安全隧道,从而提供了一种为家庭基站和PLMN的OAM域和Service域之间的通信提供安全保护的机制,确保了家庭基站和PLMN网络的通信安全。



CN 101437223 B

1. 一种家庭基站接入的方法，其特征在于，包括以下步骤：

家庭基站与安全网关进行交互认证；

所述家庭基站与所述安全网关建立安全隧道，以保护所述家庭基站与公众陆地移动网 PLMN 网络的通信安全；

所述安全网关包括：运行和维护 OAM 域的安全网关，所述家庭基站与所述安全网关建立安全隧道具体包括：所述家庭基站与所述 OAM 域的安全网关进行安全关联协商建立安全隧道，以保护所述家庭基站与所述 OAM 域的通信安全；

所述家庭基站与所述 OAM 域的安全网关进行安全关联协商建立安全隧道之后还包括所述家庭基站与所述 OAM 域的安全网关共享密钥；

所述安全网关还包括服务域的安全网关，所述家庭基站与所述安全网关建立安全隧道还包括：所述家庭基站与所述服务域的安全网关根据所述共享密钥建立安全隧道，以保护所述家庭基站与所述服务域的通信安全。

2. 如权利要求 1 所述家庭基站接入的方法，其特征在于，在所述家庭基站与所述服务域的安全网关根据所述共享密钥建立安全隧道之前，还包括：

所述家庭基站将所述共享密钥的标识符发送给所述服务域的安全网关；

所述服务域的安全网关根据所述标识符获取所述共享密钥。

3. 如权利要求 1 至 2 任意一项所述家庭基站接入的方法，其特征在于，所述安全隧道为：因特网协议安全 IPsec 隧道或安全传输层 TLS 隧道。

4. 如权利要求 1 所述家庭基站接入的方法，其特征在于，所述安全隧道为 IPsec 安全隧道，

在所述家庭基站与所述安全网关建立安全隧道的过程中，还包括：

所述家庭基站获取所述家庭基站在 OAM 域和服务域的 IP 地址；

所述家庭基站和安全网关将所述 IPsec 安全隧道与所述 OAM 域和服务域的 IP 地址进行绑定，以保护所述家庭基站与所述 OAM 域和所述服务域的通信安全。

5. 如权利要求 1 所述家庭基站接入的方法，其特征在于，所述安全隧道包括 IPsec 安全隧道，

在所述家庭基站与所述安全网关建立安全隧道的过程中或之后，还包括：

所述家庭基站获取所述家庭基站在所述 OAM 域的 IP 地址；

所述家庭基站和安全网关将所述 IPsec 安全隧道与所述 OAM 域的 IP 地址进行绑定，以保护所述家庭基站与所述 OAM 的通信安全。

6. 如权利要求 5 所述家庭基站接入的方法，其特征在于，在所述家庭基站和安全网关将所述 IPsec 安全隧道与所述 OAM 域的 IP 地址进行绑定之后，还包括：

所述家庭基站获取所述家庭基站在服务域的 IP 地址；

所述家庭基站和安全网关将所述 IPsec 安全隧道与所述服务域的 IP 地址进行绑定，以保护所述家庭基站与所述服务域的通信安全。

7. 如权利要求 6 所述家庭基站接入的方法，其特征在于，在所述家庭基站获取所述家庭基站在服务域的 IP 地址之后，还包括：所述家庭基站和所述安全网关根据所述服务域的 IP 地址进行安全关联协商建立另一 IPsec 隧道，以保护所述家庭基站与所述服务域的通信安全。

8. 如权利要求 6 所述家庭基站接入的方法，其特征在于，在所述家庭基站和安全网关将所述 IPsec 安全隧道与所述 OAM 域的 IP 地址进行绑定之后，还包括：

如果所述家庭基站在所述服务域的 IP 地址与在所述 OAM 域的 IP 地址相同，则所述家庭基站和安全网关将所述 IPsec 安全隧道与所述 OAM 域的 IP 地址进行绑定，以保护所述家庭基站与所述服务域的通信安全；或者，

所述家庭基站和所述安全网关根据所述 OAM 域的 IP 地址进行安全关联协商建立另一 IPsec 隧道，以保护所述家庭基站与所述服务域的通信安全。

9. 如权利要求 1 所述家庭基站接入的方法，其特征在于，在所述家庭基站与所述安全网关建立安全隧道之后，还包括：所述家庭基站在所述安全隧道上与所述 PLMN 网络进行交互认证。

10. 一种家庭基站接入的系统，包括安全网关，其特征在于，还包括：家庭基站，用于与所述安全网关进行交互认证，建立安全隧道，以保护所述家庭基站与 PLMN 的通信安全；

所述安全网关包括运行和维护 OAM 域的安全网关，所述家庭基站与所述安全网关建立安全隧道具体包括：所述家庭基站与 OAM 域的安全网关进行安全关联协商建立安全隧道，以保护所述家庭基站与所述 OAM 域的通信安全；所述家庭基站与所述 OAM 域的安全网关进行安全关联协商建立安全隧道之后还包括所述家庭基站与所述 OAM 域的安全网关共享密钥；

所述安全网关还包括服务域的安全网关，所述家庭基站与所述安全网关建立安全隧道还包括：所述家庭基站与所述服务域的安全网关根据所述共享密钥建立安全隧道，以保护所述家庭基站与所述服务域的通信安全。

11. 如权利要求 10 所述家庭基站接入的系统，其特征在于，所述家庭基站包括：

认证模块，用于与所述安全网关进行交互认证；

建立模块，与所述认证模块连接，用于在所述认证模块认证后，建立安全隧道，以保护所述家庭基站与 PLMN 的通信安全。

12. 一种家庭基站，其特征在于，包括：

认证模块，用于与安全网关进行交互认证；

建立模块，与所述认证模块连接，用于在所述认证模块认证后，建立安全隧道，以保护所述家庭基站与 PLMN 的通信安全；

所述建立模块还包括：运行和维护 OAM 域建立子模块，用于所述家庭基站与所述 OAM 域的安全网关进行安全关联协商建立安全隧道，以保护所述家庭基站与所述 OAM 域的通信安全；

服务域建立子模块，用于在所述 OAM 域建立子模块与所述 OAM 域的安全网关建立安全隧道之后，根据所述家庭基站与所述 OAM 域的安全网关共享的秘密信息与所述服务域的安全网关建立安全隧道；或者，与所述服务域的安全网关进行安全关联协商建立安全隧道，以保护所述家庭基站与所述服务域的通信安全。

13. 如权利要求 12 所述家庭基站，其特征在于，还包括：

IP 地址获取模块，与所述建立模块连接，用于在所述建立模块建立 IPsec 安全隧道时或建立 IPsec 安全隧道之后，获取所述家庭基站在 OAM 域和服务域的 IP 地址中的一种或两种；

绑定模块，与所述 IP 地址获取模块连接，用于将所述 IPsec 安全隧道与所述 IP 地址获取模块获取的 IP 地址进行绑定，以保护所述家庭基站与所述 OAM 域和所述服务域的通信安全。

14. 如权利要求 13 所述家庭基站，其特征在于，所述绑定模块将所述 IPsec 安全隧道与所述 IP 地址获取模块获取的 IP 地址进行绑定具体为：

将所述 IPsec 安全隧道与所述 IP 地址获取模块获取的所述家庭基站在 OAM 域和服务域的 IP 地址进行绑定；或者，

将所述 IPsec 安全隧道与所述 IP 地址获取模块获取的所述家庭基站在 OAM 域的 IP 地址进行绑定，再将所述 IPsec 安全隧道与所述 IP 地址获取模块获取的所述家庭基站在服务域的 IP 地址进行绑定。

15. 如权利要求 14 所述家庭基站，其特征在于，所述建立模块还包括：隧道新建子模块，用于在所述绑定模块将所述 IPsec 安全隧道与所述家庭基站在 OAM 域的 IP 地址进行绑定之后，根据所述 IP 地址获取模块获取的所述家庭基站在服务域的 IP 地址与所述安全网关进行安全关联协商建立另一 IPsec 隧道，以保护所述家庭基站与所述服务域的通信安全。

一种家庭基站接入的方法、系统和装置

技术领域

[0001] 本发明涉及网络通信技术领域，特别涉及一种家庭基站接入的方法、系统和装置。

[0002] 背景技术

[0003] 在目前的移动通信网络中，对于网络节点的布置，一般来说，都是由运营商事先规划好，根据规划的内容来完成网络的布置。在网络中，在同一位置区域中的所有用户共享小区的资源，当高速率或高带宽的业务接入之后，有可能会对其他用户的接入造成影响。

[0004] 随着 Internet 的发展以及各种无线业务的广泛应用，用户对于无线网络提出了高速、便捷、低成本等方面的需求。另一方面，从运营商的角度来看，需要充分地利用现有网络的资源，扩大容量，减少成本，更好地为用户提供服务。

[0005] HB(Home Base-station，家庭基站）的提出，充分的满足了上面的需求和网络的发展需求。家庭基站是一种家用的微型基站，移动用户可以在家庭、办公场所等热点覆盖区域布置这种基站，通过 Internet 接入移动通信网络，来获得无线通信服务。家庭基站的引入，解决了无线数据业务中空口资源的瓶颈问题，使得用户可以享用到高速率、高带宽的网络服务。另一方面，家庭基站通过 Internet 接入，节省了移动运营商的传输费用，提高了移动网络的容量。而且，家庭基站主要应用在家庭个人使用，办公场所等热点区域，以及边远地区的盲点覆盖，提高了移动网络的覆盖率，优化了网络的质量。家庭基站需要和 PLMN(Public Land Mobile Network，公众陆地移动网）网络的 OAM(Operation And Maintenance，运行和维护）域和 Service（服务）域进行通信。家庭基站通过 Internet 等不可信的网络和这两个域进行通信，无法确保家庭基站和 PLMN 网络的通信安全，因此需要有一种机制为家庭基站和 PLMN 的这两个域之间的通信提供安全保护。

[0006] 在实现本发明的过程中，发明人发现现有技术至少存在以下问题：没有为家庭基站和 PLMN 的 OAM 域和 Service 域之间的通信提供安全保护的机制，无法保证家庭基站和 PLMN 网络的通信安全。

[0007] 发明内容

[0008] 本发明实施例提供一种家庭基站接入的方法、系统和装置，以实现保护家庭基站和 PLMN 网络之间的通信安全。

[0009] 为达到上述目的，本发明实施例一方面提供一种家庭基站接入的方法，包括以下步骤：家庭基站与安全网关进行交互认证；所述家庭基站与所述安全网关建立安全隧道，以保护所述家庭基站与公众陆地移动网 PLMN 的通信 安全；

[0010] 所述安全网关包括：运行和维护 OAM 域的安全网关，所述家庭基站与所述安全网关建立安全隧道具体包括：所述家庭基站与所述 OAM 域的安全网关进行安全关联协商建立安全隧道，以保护所述家庭基站与所述 OAM 域的通信安全；所述家庭基站与所述 OAM 域的安全网关进行安全关联协商建立安全隧道之后还包括所述家庭基站与所述 OAM 域的安全网关共享密钥；所述安全网关还包括服务域的安全网关，所述家庭基站与所述安全网关建立安全隧道还包括：所述家庭基站与所述服务域的安全网关根据所述共享密钥建立安全隧道，以保护所述家庭基站与所述服务域的通信安全。

[0011] 另一方面，本发明实施例还提供一种家庭基站接入的系统，包括安全网关，还包括：家庭基站，用于与所述安全网关进行交互认证，建立安全隧道，以保护所述家庭基站与PLMN的通信安全；所述安全网关包括运行和维护OAM域的安全网关，所述家庭基站与所述安全网关建立安全隧道具体包括：所述家庭基站与OAM域的安全网关进行安全关联协商建立安全隧道，以保护所述家庭基站与所述OAM域的通信安全；所述家庭基站与所述OAM域的安全网关进行安全关联协商建立安全隧道之后还包括所述家庭基站与所述OAM域的安全网关共享密钥；所述安全网关还包括服务域的安全网关，所述家庭基站与所述安全网关建立安全隧道还包括：所述家庭基站与所述服务域的安全网关根据所述共享密钥建立安全隧道，以保护所述家庭基站与所述服务域的通信安全。

[0012] 再一方面，本发明实施例还提供一种家庭基站，包括：认证模块，用于与安全网关进行交互认证；建立模块，与所述认证模块连接，用于在所述认证模块认证后，建立安全隧道，以保护所述家庭基站与PLMN的通信安全；

[0013] 所述建立模块还包括：运行和维护OAM域建立子模块，用于所述家庭基站与所述OAM域的安全网关进行安全关联协商建立安全隧道，以保护所述家庭基站与所述OAM域的通信安全；

[0014] 服务域建立子模块，用于在所述OAM域建立子模块与所述OAM域的安全网关建立安全隧道之后，根据所述家庭基站与所述OAM域的安全网关共享的秘密信息与所述服务域的安全网关建立安全隧道；或者，与所述服务域的安全网关进行安全关联协商建立安全隧道，以保护所述家庭基站与所述服务域的通信安全。

[0015] 与现有技术相比，本发明实施例具有以下优点：通过在家庭基站和PLMN的安全网关之间建立安全隧道，为家庭基站和PLMN网络之间的通信提供了安全保护。

[0016] 附图说明

[0017] 图1为本发明实施例家庭基站接入的方法的流程图；

[0018] 图2为本发明家庭基站接入的方法实施例一的流程图；

[0019] 图3为本发明家庭基站接入的方法实施例三的流程图；

[0020] 图4为本发明家庭基站接入的方法实施例四的流程图；

[0021] 图5为本发明实施例家庭基站接入的系统的结构图。

[0022] 具体实施方式

[0023] 本发明实施例提供了一种家庭基站接入的方法，通过在家庭基站和PLMN网络之间建立的安全隧道来保护家庭基站和PLMN网络之间的通信安全。家庭基站和PLMN之间建立的安全隧道可以是一条或者多条，这些安全隧道可能在一个安全网关上建立，也可能在多个安全网关上建立。

[0024] 如图1所示，为本发明实施例家庭基站接入的方法的流程图，具体包括以下步骤：

[0025] 步骤S101，家庭基站与安全网关进行交互认证。家庭基站和安全网关之间可以采用基于EAP(Extensible Authentication Protocol，可扩展认证协议)的方式、基于预共享密钥的方式、基于证书的方式等完成家庭基站和安全网关之间的交互认证。

[0026] 步骤S102，家庭基站与安全网关建立安全隧道，以保护所述家庭基站与公众陆地移动网PLMN的通信安全。家庭基站和PLMN之间可以建立一条或者多条安全隧道。该安全隧道可以是IPsec(Internet Protocol security，因特网协议安全)安全隧道，也可以是

TLS(Transport Layer Security,传输层安全)安全隧道。当PLMN网络的OAM域的安全网关和Service(服务)域的安全网关为不同的安全网关时,家庭基站可以与OAM域的安全网关和Service域的安全网关分别建立安全隧道,以保护家庭基站与OAM域和Service域的通信安全。当PLMN网络的OAM域的安全网关和Service域的安全网关为相同的安全网关时,家庭基站可以与该安全网关建立一条安全隧道,以同时保护家庭基站与OAM域和Service域的通信安全;或者,家庭基站与该安全网关分别建立两条安全隧道,以分别保护家庭基站与OAM域的通信安全和家庭基站与Service域的通信安全。

[0027] 优选地,在家庭基站与安全网关建立安全隧道之后,家庭基站在建立的安全隧道上和PLMN网络再次进行交互认证。

[0028] 上述家庭基站接入的方法中,家庭基站与PLMN网络的安全网关进行交互认证,并建立安全隧道,从而提供了一种为家庭基站和PLMN的OAM域和Service域之间的通信提供安全保护的机制,确保了家庭基站和PLMN网络的通信安全。

[0029] 如图2所示,为本发明家庭基站接入的方法实施例一的流程图,本发明家庭基站接入的方法实施例一描述的场景为:家庭基站与PLMN网络的OAM域的安全网关SGo(Security Gateway,安全网关)和PLMN网络的Service域的安全网关SGs之间分别建立安全隧道,并利用这些安全隧道来保护家庭基站和PLMN网络之间的通信。具体包括以下步骤:

[0030] 步骤S201,HB获取OAM域的安全网关SGo的IP地址;

[0031] 步骤S202,HB和OAM域的安全网关进行IKE_SA_INIT交换。HB发送其支持的安全关联信息(Sai1)、DH交换值(KEi)和nonce(随机数)(Ni)给SGo。

[0032] 步骤S203,SGo选择IKE(Internet Key Exchange,因特网密钥交换)SA(Security Association,安全关联)的安全关联,将选择结果发送给HB。并将DH交换值(KEr)、nonce(Nr)也一起发送给HB。这一步结束后,SGo和HB协商完成IKE SA。

[0033] 步骤S204,HB和SGo开始进行IPsec安全关联的协商。在安全关联协商的过程中,HB和SGo利用EAP(Extensible Authentication Protocol,可扩展认证协议)AKA(Authentication and Key Agreement,认证和密钥协商)/SIM(Subscriber Identity Modular,客户身份模块)进行交互认证。HB发送HB的身份,即ID(Identifier,标识)of HB,该HB的身份是根据HB中插入的USIM(Universal Mobile Telecommunications System Subscriber IdentificationModule,通用移动通信系统)卡中的IMSI(International Mobile SubscriberIdentification number,国际移动用户识别码)推导出来的NAI(Network AccessIdentifier,网络接入标识符)格式的身份、证书请求(请求SG的证书)、内网IP地址请求CP(Configuration Payload,配置负载),HB支持的安全关联信息(SAi2)和策略选择符(TSi,TSr)。其中,CP用于请求SG给该HB分配的OAM域的内网IP地址,是可选参数。这条消息中不携带AUTH(Authentication,鉴权)字段以指示SGo需要执行EAP认证。

[0034] 步骤S205,SGo将HB的身份发送给AAA(Authentication AuthorizationAccounting,认证、授权、计费)服务器。

[0035] 步骤S206,AAA服务器和存储HB相关信息的存储服务器交互以获得HB的认证向量。HB的profile(签约信息)可能也同时发送给AAA服务器。

[0036] 步骤 S207，AAA 服务器发送 EAP AKA/SIM Challenge 给 SGo。

[0037] 步骤 S208，SGo 将 EAP AKA/SIM Challenge 发送给 HB。SGo 的身份 IDr、SG 的证书和 SG 利用证书计算的 AUTH 载荷也一起发送给 HB。

[0038] 步骤 S209，HB 生成相应的 EAP 响应消息，发送给 SGo。

[0039] 步骤 S210，SGo 将 EAP 响应消息转发给 AAA 服务器。

[0040] 步骤 S211，AAA 服务器对 EAP 响应消息进行验证。验证成功后，发送 EHBsuccess 消息。并将相应的密钥素材发送给 SGo。

[0041] 步骤 S212，SGo 将 HB 的身份等信息发送给 AAA 服务器，AAA 服务器根据 HB 的 profile 进行授权检查。

[0042] 步骤 S213，SGo 转发 EAP success 消息给 HB。这一步结束后，SGo 和 HB 共享了密钥素材 key material，完成了 SG 和 HB 之间的交互认证。

[0043] 步骤 S214，HB 发送 IKE 消息，其中携带 AUTH 载荷。AUTH 载荷使用共享密钥计算。

[0044] 步骤 S215，SGo 发送 IKE 消息，其中携带 AUTH 载荷（使用共享密钥计算）、选择的 IPsec SA(SAr2)、选择的策略选择符 (TSi 和 TSr)。如果 HB 请求了内网 IP 地址，则 SG 回应 CP 载荷，其中 CP 载荷中携带 HB 的内网 IP 地址。

[0045] 步骤 S216，SGo 与 HB 进行交互，删除 SGo 和 HB 间共享的旧的 IKE SA。后续如果 HB 和 SGo 之间需要建立更多的安全隧道，则 HB 和 SGo 之间利用 CREATE CHILD SA 交换来建立更多的 IPsec 安全隧道以保护有不同安全需求的信息。

[0046] 步骤 S217，HB 和 OAM 域的设备之间可能执行应用层的安全机制。

[0047] 步骤 S218，HB 和 EMS(Element Management System，网元管理系统）通 信，从 EMS 中获取配置数据等信息。HB 获得其在 Service 域的 IP 地址和 Service 域的安全网关的地址。

[0048] 步骤 S219，HB 和服务域的安全网关 SGs 进行 IKE 交换。HB 发送其支持的安全关联信息 (SAi1)、DH 交换值 (KEi) 和 nonce(Ni) 给 SGs。

[0049] 步骤 S220，SGs 选择 IKE SA 的安全关联，将选择结果发送给 HB。DH 交换值 (KEr)、nonce(Nr) 也一起发送给 HB。这一步结束后，SGs 和 HB 协商完成 IKE SA。

[0050] 步骤 S221，HB 开始进行 IKE 第二阶段的协商。HB 发送其身份给 SGs。这个身份有特殊的身份格式，SGs 根据这个身份的特殊格式，可以寻址到位于 OAM 域的 AAA 服务器，并可以根据这个特殊的身份，获得和 HB 相同的密钥。这个身份格式可以是 RAND@HBServiceDomainAUTH.operator.com。HB 利用在 OAM 域认证时生成的 CK(Cryptographic Key，加密密钥）/IK(Integrality Key，完整性密钥）计算出密钥 K = (CK‖IK，IP of SGs，...)，然后利用密钥 K 计算 AUTH。

[0051] 步骤 S222，SGs 根据 ID 的特殊格式，寻址到对应的 AAA 服务器，并向 AAA 服务器请求密钥 K。AAA 服务器利用和 HB 相同的方法计算出密钥 K = (CK‖IK，IP of SGs，...)。并将密钥 K 发送给 SGs。其中，SGs 可能需要将 HB 计算 K 时的 SGs 的 IP 地址告诉 AAA。

[0052] 步骤 S223，SGs 利用密钥 K 验证 AUTH 的正确性，并完成 IPsec SA 的协商。回复消息中的 AUTH 也使用密钥 K 计算。如果需要更多的安全隧道来保护不同的信息，如对信令和数据采用不同的安全保护，那么 SGs 可以和 HB 进行 CREATE CHILD SA 交换来建立更多的 IPsec 安全隧道。

[0053] 在本实施例中，家庭基站和 SGo 之间的安全关联建立采用了 EAP-AKA 的方式进行认证，但是，家庭基站和 SGo 之间的安全关联建立也可以采用其他的方式建立，如 EAP-SIM 的方式、基于预共享密钥的方式、基于证书的方式等。

[0054] 本发明家庭基站接入的方法实施例二描述的场景为：家庭基站与 PLMN 网络的 OAM 域的安全网关 SGo 和 PLMN 网络的 Service 域的安全网关 SGs 之间分别建立安全隧道，并利用这些安全隧道来保护家庭基站和 PLMN 网络之间的 通信。下面以建立 IPsec 隧道为例介绍，介绍本发明实施例二。

[0055] 实施例二的步骤 1 ～ 17 与实施例一的步骤 S201 ～步骤 S217 相同；

[0056] 步骤 18，家庭基站和 Service 域的安全网关 SGs 重新执行步骤 S201 ～步骤 S216 中描述的步骤以建立家庭基站和 SGs 之间的 IPsec 隧道。如果家庭基站和 Service 域的安全网关之间需要更多的安全隧道来保护不同的信息，如对信令和数据采用不同的安全保护，那么 SGs 可以和 AP 进行 CREATE CHILD SA 交换，以建立更多的 IPsec 安全隧道。

[0057] 在本发明实施例中，家庭基站和 SGo/SGs 之间的安全关联建立采用了 EAP-AKA 的方式进行认证，但是，家庭基站和 SGo/SGs 之间的安全关联建立也可以采用其他的方式建立，如 EAP-SIM 的方式、基于预共享密钥的方式、基于证书的方式等。并且家庭基站和 SGo 之间建立安全关联的方式可以和家庭基站与 SGs 之间建立安全关联的方式不同。

[0058] 如图 3 所示，为本发明家庭基站接入的方法实施例三的流程图，本发明家庭基站接入的方法实施例三描述的场景为：PLMN 网络的 OAM 域的安全网关和 PLMN 网络的 Service 域的安全网关是同一个安全网关 SG。家庭基站和这个安全网关建立安全隧道，并利用这些安全隧道来保护家庭基站和 PLMN 网络之间的通信。具体包括以下步骤：

[0059] 步骤 S301，HB 获取 SG 的 IP 地址；

[0060] 步骤 S302，HB 和 SG 进行 IKE_SA_INIT 交换。HB 发送其支持的安全关联信息 (SAi1)、DH 交换值 (KEi) 和 nonce(Ni) 给 SG。

[0061] 步骤 S303，SG 选择 IKE SA 的安全关联，将选择结果发送给 HB。并将 DH 交换值 (KEr)、nonce(Nr) 也一起发送给 HB。这一步结束后，SG 和 HB 协商完成 IKE SA。

[0062] 步骤 S304，HB 和 SG 开始进行 IPsec 安全关联的协商。在安全关联的协商过程中，HB 和 SG 利用 EAP AKA/SIM 进行交互认证。HB 发送 HB 的身份，即 ID ofHB，根据 HB 中插入的 USIM 卡中的 IMSI 推导出来 NAI 格式的身份、证书请求 (CERT REQUEST，用于请求 SG 的证书)、内网 IP 地址请求 (CP，用于请求 SG 给该 HB 分配 OAM 域的内网 IP 地址，可选)、HB 支持的安全关联信息 (SAi2) 和策略选择符 (TSi，TSr)。这条消息中不携带 AUTH 字段以指示 SG 需要进行 EAP 认证。

[0063] 步骤 S305，SG 将 HB 的身份发送给 AAA 服务器。

[0064] 步骤 S306，AAA 服务器和存储 HB 相关信息的存储服务器交互以获得 HB 的认证向量。HB 的 profile 可能也发送给 AAA 服务器。

[0065] 步骤 S307，AAA 服务器发送 EAP AKA/SIM Challenge 给 SG。

[0066] 步骤 S308，SG 将 EAP AKA/SIM Challenge 发送给 HB。SG 的身份 IDr、SG 的证书和 SG 利用证书计算的 AUTH 载荷也一起发送给 HB。

[0067] 步骤 S309，HB 生成相应的 EAP 响应消息，发送给 SG。

[0068] 步骤 S310，SG 将 EAP 响应消息转发给 AAA 服务器。

[0069] 步骤S311，AAA服务器对EAP响应消息进行验证。在验证成功后，发送EAP success消息。并将相应的密钥素材发送给SG。

[0070] 步骤S312，SG将HB的身份等信息发送给AAA服务器，AAA服务器根据HB的profile进行授权检查。

[0071] 步骤S313，SG转发EAP success消息给HB。这一步结束后，SG和HB共享了密钥素材key material，完成了SG和HB之间的交互认证。

[0072] 步骤S314，HB发送IKE消息，其中携带AUTH载荷。AUTH载荷使用共享密钥计算。

[0073] 步骤S315，SG发送IKE消息，其中携带AUTH载荷（使用共享密钥计算）、选择的IPsec SA(SAr2)、选择的策略选择符(TSi和TSr)。如果HB请求了内网IP地址，则SG回应CP载荷，其中CP载荷中携带HB的内网IP地址。

[0074] 步骤S316，SG和HB进行交互，删除SG和HB间共享的旧的IKE SA。后续如果HB和SG需要更多的安全关联以保护HB和OAM间不同性质的通信，HB和SG可以通过CREATE CHILD SA交换建立多条IPsec安全隧道。

[0075] 步骤S317，HB和EMS通信，从EMS中获取配置数据等信息。HB获得该HB在Service域的IP地址，若HB在Service域和OAM域的IP地址相同，则HB不需要再次获得IP地址。

[0076] 步骤S318，HB和Service域进行通信。这时HB可能需要建立一个新的IPsec安全关联用于Service域。HB和SG之间执行CREATE CHILD SA交换，HB发送IKE消息请求生成一个IPsec SA。HB也可以在这条消息中携带CP载荷请求获得HB在Service域的IP地址。若HB在Service域和OAM域的IP地址相同，则HB不需要再次获得IP地址。

[0077] 步骤S319，SG完成IPsec SA的协商，并发送相应IKE消息通知HB该SG选定的IPsec SA。HB可能需要在安全网关之间建立多条IPsec关联以保护不同性质的通信，这时，HB和SG之间可以通过CREATE CHILD SA交换建立多条IPsec关联。

[0078] 在本实施例中，家庭基站和SG之间的安全关联建立采用了EAP-AKA的方式进行认证，但是，家庭基站和SGo之间的安全关联建立也可以采用其他的方式建立，如EHB-SIM的方式、基于预共享密钥的方式、基于证书的方式等。

[0079] 如图4所示，为本发明家庭基站接入的方法实施例四的流程图，本发明家庭基站接入的方法实施例四描述的场景为：PLMN网络的OAM域的安全网关和PLMN网络的Service域的安全网关是同一个安全网关SG。家庭基站和这个安全网关建立安全隧道，并利用这些安全隧道来保护家庭基站和PLMN网络之间的通信。具体包括以下步骤：

[0080] 步骤S401，HB和安全网关建立安全隧道。HB和安全网关间利用IKEv2承载EAP的方式进行交互认证，交互认证后，HB和安全网关间建立好一条IPsec安全隧道。

[0081] 步骤S402，将建立的IPsec安全隧道与HB的IP地址进行绑定。在协商安全关联时，HB利用IKEv2协议中的CP载荷请求两个IP地址：HB在OAM域的IP地址和HB在Service域的IP地址。HB和安全网关间建立的IPsec安全隧道和这两个IP地址绑定；或者，

[0082] 在协商安全关联时，HB利用IKEv2协议中的CP载荷请求该HB在OAM域的IP地址。HB和安全网关间建立的IPsec安全隧道与该HB在OAM域的IP地址绑定。然后HB请求该HB在Service域的IP地址，将HB和安全网关间建立的IPsec安全隧道与该HB在Service域的IP地址进行绑定；或者，

[0083] HB 在 OAM 域和 Service 域使用相同的 IP 地址，这样 HB 仅需要利用 IKEv2 中的 CP 载荷请求该相同的 IP 地址，并将 HB 和安全网关间建立的 IPsec 安全隧道与该 IP 地址绑定即可。上述为在 HB 与安全网关进行安全关联协商的过程中，即在 IPsec 安全隧道的建立过程中，HB 获取该 HB 在 OAM 域和服务域的 IP 地址，也可以在 IPsec 安全隧道建立之后，HB 再获取该 HB 在 OAM 域和服务域的 IP 地址，然后将该 IP 地址与建立的 IPsec 安全隧道进行绑定。

[0084] 步骤 S403，通过建立的 IPsec 安全隧道保护 HB 与 OAM 域的通信和 HB 与 Service 域的通信。

[0085] 上述实施例一～四中描述的方案大都采用了 EAP-AKA 的方式作为建立安全隧道时，HB 和安全网关交互认证的方法。在这种情况下，HB 和 PLMN 网络在建立安全隧道的过程中就完成了 HB 和 PLMN 网络的交互认证。但是，在某些情况下，HB 和 PLMN 网络可能还需要再做进一步的认证，即 HB 首先和 PLMN 网络进行交互认证，建立安全隧道，然后 HB 和 PLMN 网络再次进行交互认证。在这种场景下，AP 和安全网关之间可以采用实施例一到实施例四的方法，以基于 EAP 的方式、基于预共享密钥的方式、基于证书的方式完成 HB 和安全网关间的交互认证，并完成安全隧道的建立。然后 HB 再在建立的安全隧道上和 PLMN 网络执行交互认证。

[0086] 如图 5 所示，为本发明实施例家庭基站接入的系统的结构图，包括安全网关 1，还包括 ：家庭基站 2，用于与安全网关 1 进行交互认证，建立安全隧道，以保护家庭基站 2 与 PLMN 的通信安全。

[0087] 其中，家庭基站 2 包括 ：认证模块 21，用于与安全网关 1 进行交互认证 ；

[0088] 建立模块 22，与认证模块 21 连接，用于在认证模块 21 认证后，建立安全隧道，以保护家庭基站 2 与 PLMN 的通信安全。

[0089] 其中，建立模块 22 包括 ：OAM 域建立子模块 221，用于与 OAM 域的安全网关进行安全关联协商建立安全隧道，以保护家庭基站 2 与 OAM 域的通信安全。

[0090] 其中，建立模块 22 还包括 ：服务域建立子模块 222，用于在 OAM 域建立子模块 221 与 OAM 域的安全网关建立安全隧道之后，根据家庭基站 2 与 AAA 服务器共享的秘密信息与服务域的安全网关建立安全隧道 ；或者，与服务域的安全网关进行安全关联协商建立安全隧道，以保护家庭基站 2 与服务域的通信安全。

[0091] 其中，家庭基站 2 还包括 ：IP 地址获取模块 23，与建立模块 22 连接，用于在建立模块 22 建立 IPsec 安全隧道之后，获取家庭基站 2 在 OAM 域和服务域的 IP 地址中的一种或两种 ；

[0092] 绑定模块 24，与 IP 地址获取模块 23 连接，用于将 IPsec 安全隧道与 IP 地址获取模块 23 获取的 IP 地址进行绑定，以保护家庭基站与 OAM 域和服务域的通信安全。

[0093] 其中，绑定模块 24 将 IPsec 安全隧道与 IP 地址获取模块 23 获取的 IP 地址进行绑定具体为 ：将 IPsec 安全隧道与 IP 地址获取模块 23 获取的家庭基站 2 在 OAM 域和服务域的 IP 地址进行绑定 ；或者，

[0094] 将所述 IPsec 安全隧道与 IP 地址获取模块 23 获取的家庭基站 2 在 OAM 域的 IP 地址进行绑定，再将 IPsec 安全隧道与 IP 地址获取模块 23 获取的家庭基站 2 在服务域的 IP 地址进行绑定。

[0095] 其中，建立模块 22 还包括：隧道新建子模块 223，用于在绑定模块 24 将 IPsec 安全隧道与家庭基站 2 在 OAM 域的 IP 地址进行绑定之后，根据 IP 地址获取模块 23 获取的家庭基站 2 在服务域的 IP 地址与安全网关 1 进行安全关联协商建立另一 IPsec 隧道，以保护家庭基站 2 与服务域的通信安全。

[0096] 上述家庭基站接入的系统，家庭基站 2 与 PLMN 网络的安全网关 1 进行交互认证，并建立安全隧道，从而提供了一种为家庭基站 2 和 PLMN 的 OAM 域和 Service 域之间的通信提供安全保护的机制，确保了家庭基站 2 和 PLMN 网络的通信安全。

[0097] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算 机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

[0098] 以上公开的仅为本发明的几个具体实施例，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。

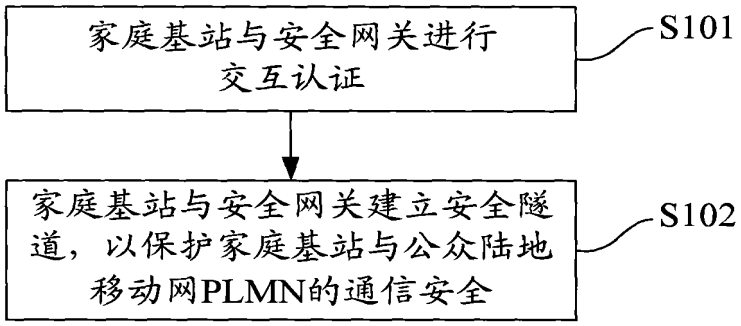

家庭基站与安全网关进行交互认证
S101
家庭基站与安全网关建立安全隧道，以保护家庭基站与公众陆地移动网PLMN的通信安全
S102

图 1

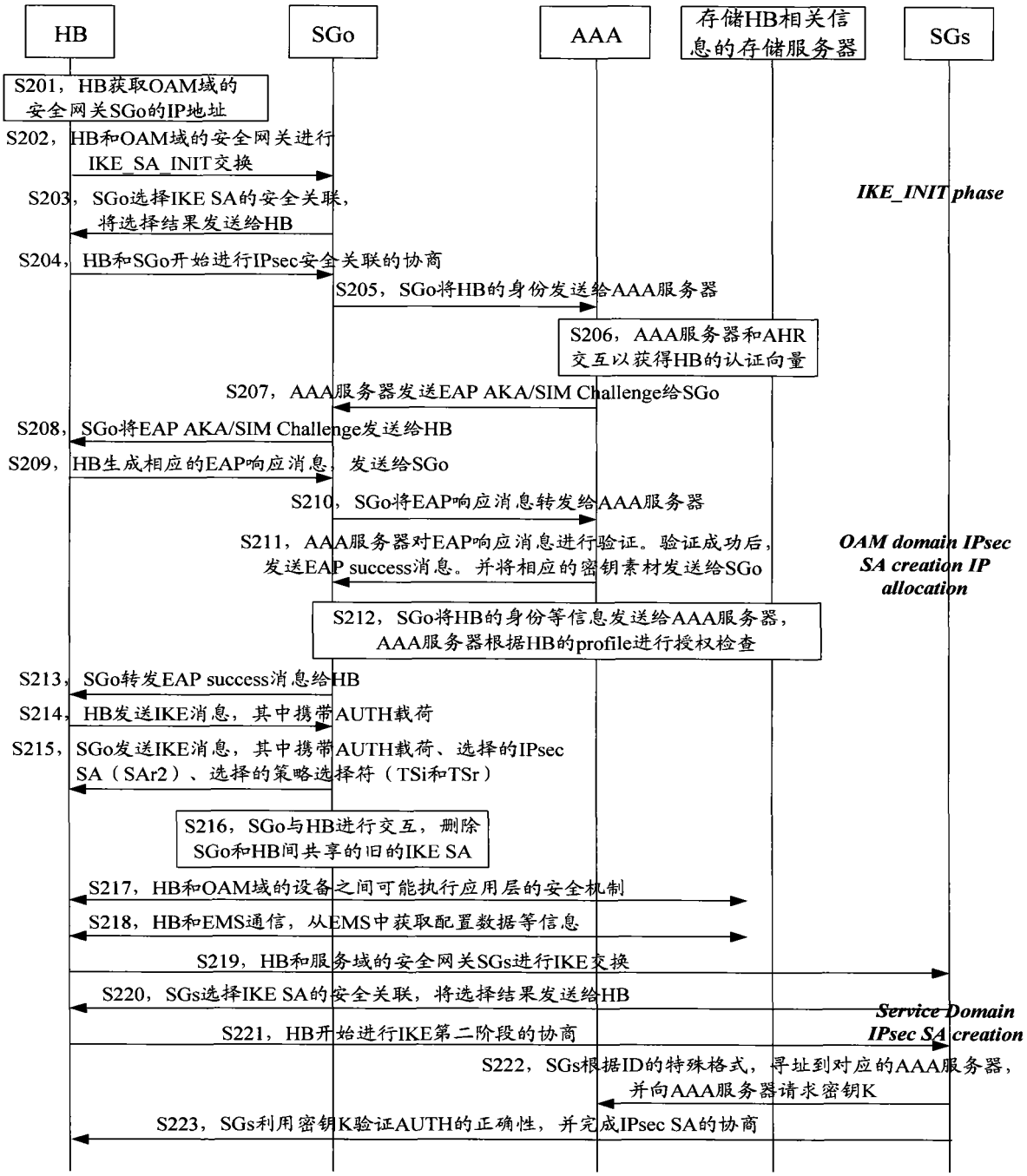

HB
SGo
AAA
存储HB相关信息的存储服务器
SGs
S201，HB获取OAM域的安全网关SGo的IP地址
S202，HB和OAM域的安全网关进行IKE_SA_INIT交换
S203，SGo选择IKE SA的安全关联，将选择结果发送给HB
IKE_INIT phase
S204，HB和SGo开始进行IPsec安全关联的协商
S205，SGo将HB的身份发送给AAA服务器
S206，AAA服务器和AHR交互以获得HB的认证向量
S207，AAA服务器发送EAP AKA/SIM Challenge给SGo
S208，SGo将EAP AKA/SIM Challenge发送给HB
S209，HB生成相应的EAP响应消息，发送给SGo
S210，SGo将EAP响应消息转发给AAA服务器
S211，AAA服务器对EAP响应消息进行验证。验证成功后，发送EAP success消息。并将相应的密钥素材发送给SGo
OAM domain IPsec SA creation IP allocation
S212，SGo将HB的身份等信息发送给AAA服务器，AAA服务器根据HB的profile进行授权检查
S213，SGo转发EAP success消息给HB
S214，HB发送IKE消息，其中携带AUTH载荷
S215，SGo发送IKE消息，其中携带AUTH载荷、选择的IPsec SA（SAr2）、选择的策略选择符（TSi和TSr）
S216，SGo与HB进行交互，删除SGo和HB间共享的旧的IKE SA
S217，HB和OAM域的设备之间可能执行应用层的安全机制
S218，HB和EMS通信，从EMS中获取配置数据等信息
S219，HB和服务域的安全网关SGs进行IKE交换
S220，SGs选择IKE SA的安全关联，将选择结果发送给HB
Service Domain IPsec SA creation
S221，HB开始进行IKE第二阶段的协商
S222，SGs根据ID的特殊格式，寻址到对应的AAA服务器，并向AAA服务器请求密钥K
S223，SGs利用密钥K验证AUTH的正确性，并完成IPsec SA的协商

图 2

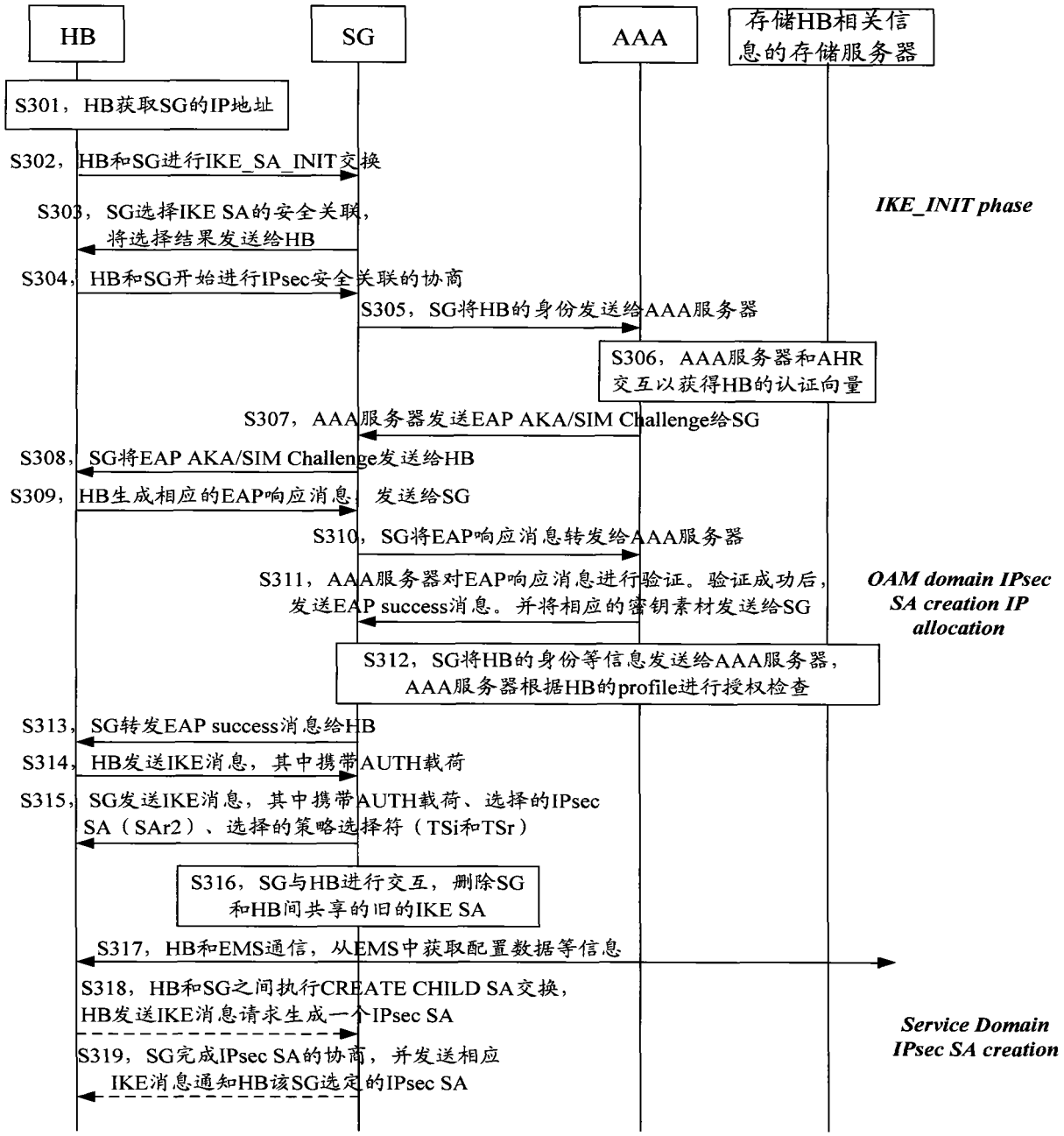

HB
SG
AAA
存储HB相关信息的存储服务器
S301，HB获取SG的IP地址
S302，HB和SG进行IKE_SA_INIT交换
S303，SG选择IKE SA的安全关联，将选择结果发送给HB
IKE_INIT phase
S304，HB和SG开始进行IPsec安全关联的协商
S305，SG将HB的身份发送给AAA服务器
S306，AAA服务器和AHR交互以获得HB的认证向量
S307，AAA服务器发送EAP AKA/SIM Challenge给SG
S308，SG将EAP AKA/SIM Challenge发送给HB
S309，HB生成相应的EAP响应消息，发送给SG
S310，SG将EAP响应消息转发给AAA服务器
S311，AAA服务器对EAP响应消息进行验证。验证成功后，发送EAP success消息。并将相应的密钥素材发送给SG
OAM domain IPsec SA creation IP allocation
S312，SG将HB的身份等信息发送给AAA服务器，AAA服务器根据HB的profile进行授权检查
S313，SG转发EAP success消息给HB
S314，HB发送IKE消息，其中携带AUTH载荷
S315，SG发送IKE消息，其中携带AUTH载荷、选择的IPsec SA（SAr2）、选择的策略选择符（TSi和TSr）
S316，SG与HB进行交互，删除SG和HB间共享的旧的IKE SA
S317，HB和EMS通信，从EMS中获取配置数据等信息
S318，HB和SG之间执行CREATE CHILD SA交换，HB发送IKE消息请求生成一个IPsec SA
S319，SG完成IPsec SA的协商，并发送相应IKE消息通知HB该SG选定的IPsec SA
Service Domain IPsec SA creation

图 3

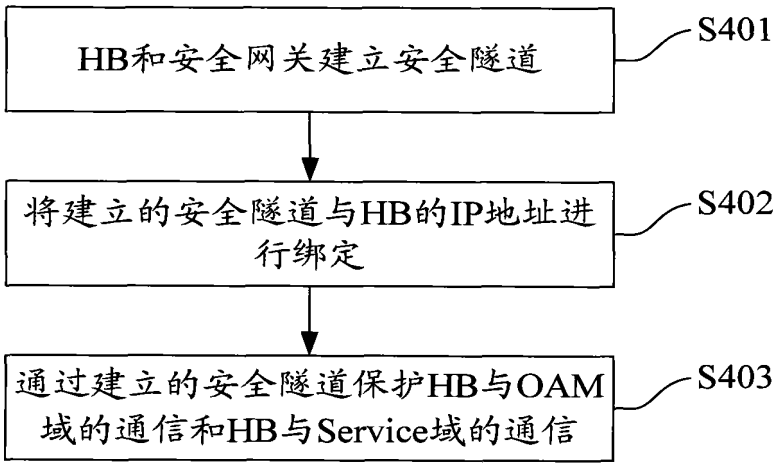

HB和安全网关建立安全隧道
S401
将建立的安全隧道与HB的IP地址进行绑定
S402
通过建立的安全隧道保护HB与OAM域的通信和HB与Service域的通信
S403

图 4

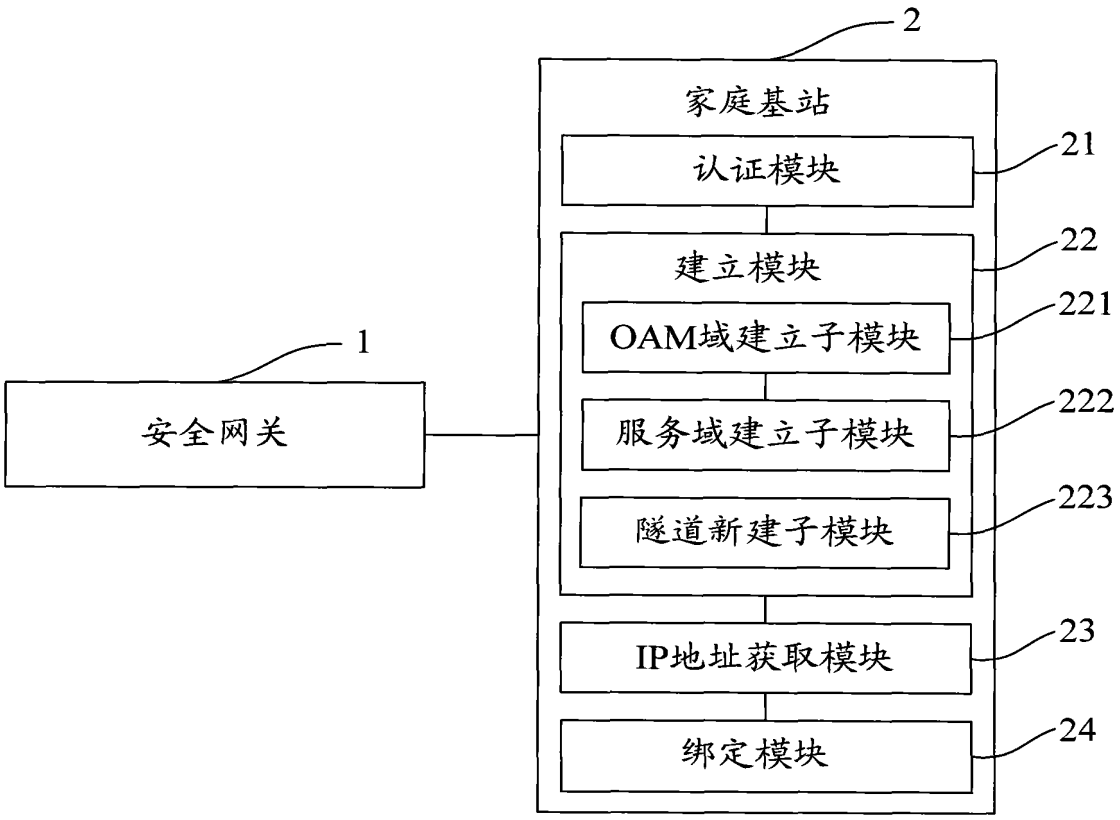

2
家庭基站
认证模块
21
建立模块
22
OAM域建立子模块
221
服务域建立子模块
222
隧道新建子模块
223
IP地址获取模块
23
绑定模块
24
1
安全网关

图 5