

(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



(10) 国际公布号

WO 2011/026341 A1

(43) 国际公布日

2011 年 3 月 10 日 (10.03.2011)

PCT

- (51) 国际专利分类号:
H04L 12/56 (2006.01)
- (21) 国际申请号: PCT/CN2010/072593
- (22) 国际申请日: 2010 年 5 月 11 日 (11.05.2010)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
200910189928.8 2009 年 9 月 1 日 (01.09.2009) CN
- (71) 申请人 (对除美国外的所有指定国): **中兴通讯股份有限公司 (ZTE CORPORATION)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
- (72) 发明人: 及
- (75) 发明人/申请人 (仅对美国): **钮远 (NIU, Yuan)** [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
金仁康 (JIN, Renkang) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
井惟栋 (JING, Weidong) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
- (74) 代理人: 北京安信方达知识产权代理有限公司 (AFD CHINA INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市海淀区学清路 8 号 B 座 1601A, Beijing 100192 (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, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, 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, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: MOBILE IP SERVICE ACCESS METHOD AND SYSTEM

(54) 发明名称: 一种移动 IP 业务的接入方法和系统

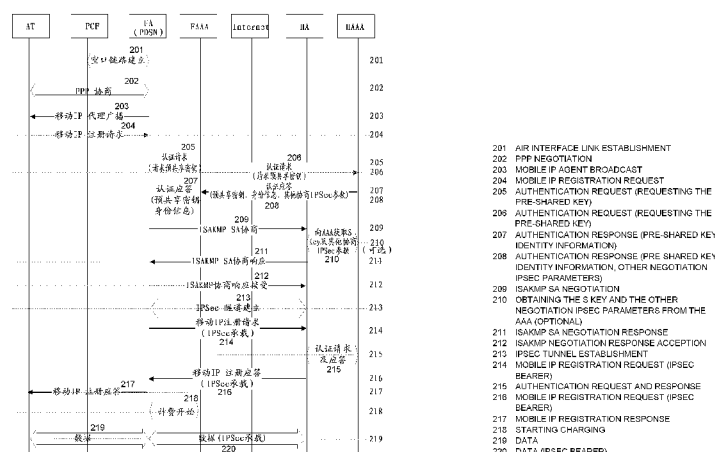


图 2 / Fig. 2

(57) Abstract: Disclosed is a mobile internet protocol (IP) access method. The method includes the following step: during the procedure that a foreign agent (FA) or a packet data service node (PDSN) negotiates with a home agent (HA) to establish an Internet protocol safety tunnel, i.e. IPSec tunnel, an authentication/authorization/accounting server (AAA) distributes negotiation IPSec parameters or a profile ID (profileID) corresponding to the negotiation IPSec parameters to the FA or the PDSN. Disclosed is also a mobile IP access system.

(57) 摘要: 本发明提供了一种移动 IP 接入方法, 包括, 在外地代理 FA 或分组数据服务节点 PDSN 与家乡代理 HA 协商建立 Internet 协议安全隧道即 IPSec 隧道的过程中, 鉴权授权计费服务器 AAA 下发协商 IPSec 参数或协商 IPSec 参数所对应的属性标识 profile ID 至所述 FA 或所述 PDSN。本发明还提供一种移动 IP 接入系统。

WO 2011/026341 A1



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种移动 IP 业务的接入方法和系统

技术领域

本发明涉及通信领域，尤其涉及 CDMA2000 系统中移动网络互连协议（Internet Protocol，IP）业务接入时方法和系统。

背景技术

移动 IP 业务相较于简单 IP 业务为用户提供了更大范围的不间断业务，在 CDMA2000、全球微波接入互通技术（World Interoperability for Microwave Access，Wimax）以及下一代演进网络中都得到了广泛的应用。

移动 IP 业务在核心网侧主要网元包括外地代理（Foreign Agent，FA）、归属代理（Home Agent，HA）和鉴权授权计费服务器（Authentication Authorization Accounting，AAA）。移动 IP 通过 FA 和 HA 接入网络，并通过 FA 和 HA 与网络进行信令和数据业务的交互，保证移动 IP 业务的安全性通过保证 FA 和 HA 之间信令和数据业务的安全性来实现。

在第三代合作伙伴计划 2 (3rd Generation Partnership Project 2, 3gpp2) 协议中，FA 与 HA 之间的信令和数据业务的安全性通常采用两种方法来保证：

第一种方法是采用 FA 与 HA 之间的认证扩展，即在 FA 上配置 HA 列表及相关参数，在 HA 上配置 FA 列表及相关参数。此方法的缺点是列表及相关参数需要手工配置，对于复杂的组网环境，操作维护工作不够方便。特别是移动 IP 业务国际漫游的场景，每次配置 FA 时需要了解全球所有互通 HA 的配置并且在全球的 HA 上增加新增 FA 的配置，实际可操作性较差。

第二种方法采用 Internet 协议安全（Internet Protocol Security，IPSec）隧道，即由 AAA 下发因特网密钥交换协议（Internet Key Exchange，IPSec IKE）协商需要的预共享密钥。

在某些 CDMA2000 系统中，分组数据服务节点（Packet Data Service Node，PDSN）在移动 IP 用户接入时具有 FA 同样的功能，在第二种方法中，

FA 可以用 PDSN 替换。

和第一种方法相比，第二种采用 IPSec 隧道的安全性更高，现有的采用 IPSec 隧道的移动 IP 接入方法包括以下步骤，如图 1 所示：

步骤 101、分组控制功能 (Packet Control Function, PCF) 与 FA 或 PDSN 建立空口链路；

步骤 102、访问终端与 FA 或 PDSN 协商 PPP， FA 或 PDSN 发送代理广播至访问终端；

步骤 103、访问终端通过代理广播获取移动 IP 相关信息；

步骤 104、访问终端向 FA 或 PDSN 发起移动 IP 注册；

步骤 105 至 108，FA 或 PDSN 与 AAA 交互，获取认证信息，包括预共享密码和 KeyID，同时下发 HA 地址给 FA 或 PDSN；

步骤 109，FA 或 PDSN 读取本地配置的其他协商 IPSec 参数，根据 FA 下发的认证信息，向 HA 进行 ISAKMP SA 协商，携带提议的 ISAKMP SA 信息、密钥材料以及 KeyID；

步骤 110，HA 根据 KeyID 还原出 FA 地址，向 AAA 获取生成 IPSec 预共享密钥的 S Key 并保存在本地；

步骤 111~112，HA 读取本地预先配置的其他协商 IPSec 参数，与 FA 或 PDSN 协商建立 ISAKMP SA；

步骤 113 ， PDSN/FA、HA 协商建立 IPSec SA；

步骤 114~117，完成 MIP 注册，PDSN/FA 与 HA 之间信令由 IPSec 隧道承载；

步骤 118， FA 通知 AAA 计费开始；

步骤 119，移动 IP 接入完成，访问终端开始数据业务， FA 与 HA 之间数据由 IPSec 隧道承载。

现有的采用 IPSec 隧道的移动 IP 接入方法有以下问题:

问题一, IKE 协商两端的 IPSec 安全关联, 除了预共享密钥还需要配置若干协商参数, 如 FA 与 HA 之间 IPSec 的传输模式、隧道模式下隧道两端的地址、安全类型、具体的加密认证算法等, 这些参数仍需要手工配置在 FA 和 HA 上, 可操作性较差;

问题二, 3gpp2 协议对 IKE 协商作了若干约束, 如 ISAKMP (Internet Security Association and Key Management Protocol, 因特网安全协定和密钥管理协议) 的主版本和副版本、选择符等, 统一了标准, 但是扩展性不好。如目前主流 IKE 已经有 V1.0 和 V2.0 的版本, 而 3gpp2 还是停留在 0 版本, 不同的系统、不同的版本在实际对接存在问题。

发明内容

本发明提供了一种移动 IP 业务的接入方法及系统, 可以提高系统的可用性, 同时满足运营商多样化安全策略需求。

为解决上述问题, 本发明提供了一种移动 IP 接入方法, 包括, 在外地代理 FA 或分组数据服务节点 PDSN 与家乡代理 HA 协商建立 Internet 协议安全隧道即 IPSec 隧道的过程中, 鉴权授权计费服务器 AAA 下发协商 IPSec 参数或协商 IPSec 参数所对应的属性标识 profileID 至所述 FA 或所述 PDSN。

上述方法还包括, 在外地代理 FA 或分组数据服务节点 PDSN 与家乡代理 HA 协商建立 Internet 协议安全隧道即 IPSec 隧道的过程中, 所述 AAA 下发协商 IPSec 参数或协商 IPSec 参数所对应的属性标识 profileID 至所述 HA。

其中, 所述 FA 或 PDSN 与所述 HA 协商建立所述 IPSec 隧道的过程包含:

A1、所述 FA 或 PDSN 向所述 AAA 发送认证请求;

A2、所述 AAA 将认证应答下发至所述 FA 或 PDSN, 所述认证应答中包含所述协商 IPSec 参数或所述协商 IPSec 参数所对应的 profileID;

A3、所述 FA 或 PDSN 根据所述 AAA 下发的认证应答, 发送协商请求

至所述 HA;

A4、所述 HA 接收所述协商请求,从本地或者从所述 AAA 获取所述协商 IPsec 参数或协商 IPsec 参数所对应的 profileID,所述 FA 或所述 PDSN 与所述 HA 协商建立 IPsec 隧道。

其中,所述认证应答中还包括预共享密钥和身份信息;

所述协商请求为所述 FA 或 PDSN 根据所述协商 IPsec 参数发起的 ISAKMP SA 建立的协商请求,所述 ISAKMP SA 建立的协商请求中携带提议建立的 ISAKMP SA 信息、密钥材料以及身份信息;

所述步骤 A4 中,所述 HA 收到所述协商请求后,从本地或从所述 AAA 获取所述协商 IPsec 参数,所述 FA 或所述 PDSN 与所述 HA 协商建立 IPsec 隧道的步骤包括:

所述 HA 收到所述 ISAKMP SA 建立的协商请求后,根据其中的所述身份信息还原所述 FA 或 PDSN 的地址,从本地获取 S Key 和所述协商 IPsec 参数,或者,从所述 AAA 获取所述 S Key 和所述协商 IPsec 参数;

所述 HA 根据所述身份信息以及所述 S Key,生成 IPsec 的预共享密钥;

所述 HA 与所述 FA 或 PDSN 交互,从而建立所述 FA 或 PDSN 与所述 HA 之间的 IPsec 隧道。

其中,所述认证应答中还包括预共享密钥和身份信息;

所述步骤 A3 中还包括,所述 FA 或 PDSN 根据所述协商 IPsec 参数所对应 profileID 在本地获取所述协商 IPsec 参数;

所述步骤 A3 中:所述协商请求为所述 FA 或 PDSN 根据所述本地获取的协商 IPsec 参数发起的 ISAKMP SA 建立的协商请求,所述 ISAKMP SA 建立的协商请求中携带提议建立的 ISAKMP SA 信息、密钥材料以及身份信息;

所述步骤 A4 中,所述 HA 收到所述协商请求后,从本地或者从所述 AAA 获取协商 IPsec 参数所对应的 profileID,所述 FA 或所述 PDSN 与所述 HA 协商建立 IPsec 隧道的步骤包括:

所述 HA 收到所述 ISAKMP SA 建立的协商请求后, 根据其中的所述身份信息还原所述 FA 或 PDSN 的地址, 从本地获取 S Key 和所述协商 IPSec 参数对应的 profileID, 或者, 从所述 AAA 获取所述 S Key 和协商 IPSec 参数对应的 profileID;

所述 HA 根据所述身份信息以及 S Key, 生成 IPSec 的预共享密钥;

所述 HA 与所述 FA 或 PDSN 交互, 从而建立所述 FA 或 PDSN 与所述 HA 之间的 IPSec 隧道。

其中, 所述协商 IPSec 参数或协商 IPSec 参数所对应的 profileID 是与访问终端的安全等级对应的协商 IPSec 参数或协商 IPSec 参数所对应的 profileID。

其中, 所述访问终端的安全等级由运营商或用户预先设定。

本发明还提供一种支持移动 IP 接入的鉴权授权计费服务器, 所述鉴权授权计费服务器设置为, 在外地代理 FA 或分组数据服务节点 PDSN 和家乡代理 HA 之间协商建立 IPSec 隧道的过程中, 下发协商 IPSec 参数或协商 IPSec 参数所对应的属性标识 profileID 至所述 FA 或者所述 PDSN。

其中, 所述鉴权授权计费服务器还设置为, 在所述 FA 或所述 PDSN 和所述 HA 之间协商建立 IPSec 隧道的过程中, 下发所述协商 IPSec 参数或协商 IPSec 参数所对应的 profileID 至所述 HA。

其中, 所述鉴权授权计费服务器是设置为: 根据访问终端的安全等级选择对应的协商 IPSec 参数或协商 IPSec 参数所对应的 profileID 后下发所述协商 IPSec 参数或协商 IPSec 参数所对应的 profileID。

本发明还提供一种支持移动 IP 接入的外地代理 FA 或分组数据服务节点 PDSN, 其中:

所述 FA 或 PDSN 设置为, 在和家乡 HA 之间协商建立 IPSec 隧道的过程中, 从所述 AAA 获取协商 IPSec 参数; 或者, 从所述 AAA 获取协商 IPSec 参数所对应的 profileID, 根据所述 profileID 得到协商 IPSec 参数。

本发明还提供一种支持移动 IP 接入的家乡代理 HA，其中，

所述 HA 设置为：在和外地代理 FA 或分组数据服务节点 PDSN 之间协商建立 IPsec 隧道的过程中，从鉴权授权计费服务器 AAA 获取协商 IPsec 参数或协商 IPsec 参数所对应的属性标识 profileID。

本发明还提供一种移动 IP 接入系统，包括：外地代理 FA 或分组数据服务节点 PDSN、以及鉴权授权计费服务器 AAA，其中，

所述 AAA 设置为，在外地代理 FA 或分组数据服务节点 PDSN 和家乡代理 HA 之间协商建立 IPsec 隧道的过程中，下发所述协商 IPsec 参数或协商 IPsec 参数所对应的属性标识 profileID 至所述 FA 或者所述 PDSN；

所述 FA 或 PDSN 设置为，在和所述 HA 之间协商建立 IPsec 隧道的过程中，从所述 AAA 获取协商 IPsec 参数；或者，从所述 AAA 获取协商 IPsec 参数所对应的 profileID，根据所述 profileID 得到协商 IPsec 参数。

其中，所述系统还包括家乡代理 HA，所述 AAA 还设置为，在所述 FA 或所述 PDSN 和所述 HA 之间协商建立 IPsec 隧道的过程中，下发协商 IPsec 参数或协商 IPsec 参数所对应的属性标识 profileID 至所述 HA；

所述 HA 设置为，在和所述 FA 或所述 PDSN 之间协商建立 IPsec 隧道的过程中，从所述 AAA 获取所述协商 IPsec 参数或协商 IPsec 参数所对应的 profileID。

其中，所述 AAA 是设置为：根据访问终端的安全等级选择对应的协商 IPsec 参数或协商 IPsec 参数所对应的 profileID 后下发所述协商 IPsec 参数或协商 IPsec 参数所对应的 profileID。

与现有技术相比，本发明的有益效果在于：本发明选择并下发协商 IPsec 参数或协商 IPsec 参数所对应的 profileID 至 FA 和 HA，或 PDSN 和 HA，避免了在上述网元上手工配置协商 IPsec 参数，简化了系统配置，提高了系统的可用性，同时，由于 FA 和 HA，或 PDSN 和 HA 上的协商参数统一下发，协议版本相同，避免了不同版本造成的对接困难。而且，本发明还可由运营商预先设定访问终端的安全级别，不同安全级别的访问终端对应不同的认证应答，不同的认证应答对应不同级别的安全策略，满足了运营商安全策略多

样化的需求。

附图概述

图 1 示例性地描述了现有的 CDMA2000 系统移动 IP 接入流程；

图 2 示例性地描述了本发明的 CDMA2000 系统移动 IP 接入流程；

图 3 示例性地描述了本发明的 CDMA2000 系统移动 IP 接入方法多样化安全策略的一种实施例；

图 4 示例性地描述了本发明的系统结构图。

本发明的较佳实施方式

下面对照附图并结合具体实施方式对本发明进行进一步详细说明。

实施例一：

如图 2 所示，本例的 CDMA2000 系统移动 IP 的接入系统，其 CDMA2000 系统移动 IP 接入方法，包括以下处理步骤：

步骤 201，PCF（Packet Control Function，分组控制功能子系统）与 FA 建立空口链路；

步骤 202，访问终端与所述 FA 协商 PPP（Point to Point Protocol，点对点联机协议），FA 发送代理广播至所述访问终端；

步骤 203，访问终端通过代理广播获取移动 IP 相关信息；

步骤 204，访问终端向 FA 发起移动 IP 注册；

步骤 205，FA 向 FAAA 发送认证请求，同时请求预共享密码；

AAA 包括 HAAA（Home Authentication Authorization Accounting 归属鉴权授权计费服务器）和 FAAA（Foreign Authentication Authorization Accounting 外地鉴权授权计费服务器），其中，HAAA 为用于选择和下发协商 IPSec 参数；FAAA 用于中转 FA 与 HAAA 之间的认证请求和应答。

步骤 206, FAAA 将认证请求转至 HAAA;

步骤 207, HAAA 根据访问终端的安全级别, 选择并下发不同的认证应答至 FAAA, 认证应答包含协商 IPSec 参数、预共享密钥、身份信息等;

访问终端的安全级别由用户或运营商预先设定, 不同安全级别的访问终端可对应不同的认证应答, 不同的认证应答对应不同级别的安全策略。

协商 IPSec 参数包括 IKE 版本号、IKE 协商的身份类型、IKE 协商的交换类型、IPSec 模式、加密算法、认证算法、IPSec 隧道两端地址、选择符、ISAKMP SA 的生命期、DH 交换群、密钥长度、IPSec 协议发展后续引入的参数。

步骤 208, FAAA 将认证应答转发至 FA;

AAA 下发协商 IPSec 参数等至 FA, 避免了在 FA 上手工配置各种参数, 简化了系统配置, 提高了系统的可用性。

步骤 209, FA 根据 AAA 下发的协商 IPSec 参数, 发送 ISAKMP SA 建立的协商请求至 HA, ISAKMP SA 建立的协商请求中携带提议建立的 ISAKMP SA 信息、密钥材料以及身份信息;

步骤 210, HA 根据收到 ISAKMP SA 建立的协商请求后, 根据其中的身份信息还原 FA 地址, 并发送 S Key 和协商 IPSec 获取请求至 AAA, AAA 下发 S Key 和所述协商 IPSec 参数至 HA, HA 根据身份信息以及 S Key 生成 IPSec 的预共享密钥, 并将信息保存在本地; 若本地已保存 S Key 和所述协商 IPSec 参数, 则直接读取本地保存的信息, 跳过步骤 210。

HA 与 FA 上的预共享密码, 用来加密在 IPSec 隧道内传输的数据和信令。

AAA 下发协商 IPSec 参数等至 HA, 避免了在 HA 上手工配置各种参数, 简化了系统配置, 提高了系统的可用性。协商 IPSec 参数在 AAA 统一配置, 然后下发到 FA 与 HA, 可以保证下发的协商 IPsec 参数与 HA、FA 的版本一致且与 FA、HA 的支持能力相符, 提高了系统的扩展性能。

步骤 211, HA 发送 ISAKMP SA 协商请求响应至所述 FA;

步骤 212, FA 收到 ISAKMP SA 协商请求响应后, 发送已接收响应至

所述 HA, ISAKMP SA 建立;

步骤 213, ISAKMP SA 建立后, FA 与 HA 建立 IPSec SA; IPSec SA 建立后, FA 与 HA 之间建立 IPSec 隧道。

步骤 214~步骤 217, 访问终端完成移动 IP 注册, FA 与 HA 之间的信令由 IPSec 隧道承载;

步骤 218, FA 通知 AAA 计费开始;

步骤 219, 移动 IP 接入完成, 访问终端开始数据业务, FA 与 HA 之间数据由所述 IPSec 隧道承载。

现有技术存在安全策略单一, 无法满足运营商订制安全策略的需求, 运营商在建设移动 IP 网络时可能会提出若干的订制要求, 如区分帐号实施 FA 与 HA 之间的 IPSec、区分运营商内部网络和其他运营商网络实施不同的 IPSec 策略等, 目前的架构无法满足运营商的需求。

本发明中, 访问终端的安全级别由运营商预先设定, 不同安全级别的访问终端对应不同的认证应答, 不同的认证应答对应不同级别的安全策略, 满足了运营商安全策略多样化的需求。

本实施例选择并下发协商 IPSec 参数至 FA 和 HA, 避免了在上述网元上手工配置协商 IPSec 参数, 简化了系统配置, 提高了系统的可用性; 同时, 由于 FA 和 HA 上的协商参数统一下发, 协议版本相同, 避免了不同版本造成的对接困难; 另一方面, 对不同安全等级提供不同的协商 IPSec 参数, 即提供了不同的安全策略, 可以满足运营商多样化安全策略需求。

实施例二:

如图 3 所示, 本发明的 CDMA2000 系统移动 IP 接入方法的实施例二中, 多样化安全策略包含以下步骤:

步骤 301, 访问终端接入 CDMA2000 系统, PCF 与所述 FA 建立空口链路; 访问终端与所述 FA 协商 PPP, FA 发送代理广播至访问终端; 访问终端通过代理广播获取移动 IP 相关信息; 访问终端发起移动 IP 注册; FA 向

AAA 发送认证请求，同时请求预共享密码；

步骤 302，AAA 根据访问终端的安全级别，提供不同的协商 IPSec 参数，即提供不同等级的安全策略，下发至 FA；

安全策略体现在不同的协商 IPSec 参数中，例如，协商 IPSec 参数中有 IPSec 隧道两端地址，高级别安全策略提供特殊 HA 地址以及机密级别的其他协商 IPSec 参数，低级别安全策略则按通用算法，如轮循算法选择 HA 地址以及仅提供认证服务的其他协商 IPSec 参数。

步骤 303，FA 与 HA 按照不同的协商 IPSec 参数，建立不同安全级别的 IPSec 隧道；

步骤 304，访问终端的信令和数据在 FA 与 HA 之间的 IPSec 隧道传输。

高安全级别的访问终端和低安全级别的访问终端，在不同安全级别的 IPSec 隧道上传输信令和数据，达到不同安全级别的保障。

实施例三：

本实施例中，为减少 FA/PDSN 与 AAA，以及 HA 和 PDSN 之间交互的信息，AAA 只下发协商 IPSec 参数所对应的属性标识(profileID)，FA/PDSN，HA 根据协商 IPSec 参数所对应的 profileID 获取协商 IPSec 参数，在 FA/PDSN，HA 本地保存 profileID 与协商 IPSec 参数的对应关系，与实施例一的不同之处主要在于，步骤 207~步骤 210 有另一种实施方法：

步骤 207a，HAAA 根据访问终端安全级别，选择并下发认证应答至 FAAA，认证应答中包含协商 IPSec 参数所对应的 profileID、预共享密钥、身份信息等；

步骤 208a，FAAA 将认证应答转发至 FA；

步骤 209a，FA 根据协商 IPSec 参数所对应的 profileID 在本地获取协商 IPSec 参数，FA 根据协商 IPSec 参数信息，发送 ISAKMP SA 建立的协商请求至所述 HA，ISAKMP SA 建立的协商请求中携带提议建立的 ISAKMP SA 信息、密钥材料以及身份信息；

步骤 210a, HA 根据收到 ISAKMP SA 建立的协商请求后, 根据其中的身份信息还原 FA 地址, 并发送 S Key 和协商 IPsec 所对应 profileID 获取请求至 AAA, AAA 下发 S Key 和协商 IPsec 参数的 profileID 至 HA, HA 根据身份信息以及 S Key 生成 IPsec 的预共享密钥, 并将信息 (包括 S Key 和协商 IPsec 参数) 保存在本地; 在后续接入时, 可以使用已保存的信息。

若本地已保存所述 S Key 和所述协商 IPsec 参数所对应的 profileID, 则直接读取本地保存的信息, 跳过步骤 210a。

AAA 下发 profileID 至 FA 和 HA, 由 FA 和 HA 根据 profileID 在本地获取协商 IPsec 参数, 避免了在 FA 和 HA 上手动配置参数, 同时也节约了 HA 和 FA 之间的通信量。

实施例四:

如图 4 所示, 本发明的一种 CDMA2000 系统移动 IP 的接入系统地实施例中, 包括归属代理、外地代理和鉴权授权计费服务器, 用于协商建立承载信令和数据的 IPsec 隧道, 在归属代理和外地代理之间协商建立 IPsec 隧道的过程中, 鉴权授权计费服务器选择并下发协商 IPsec 参数或协商 IPsec 参数所对应的 profileID 至外地代理和归属代理。

本发明提供一种支持移动 IP 接入的鉴权授权计费服务器, 所述鉴权授权计费服务器设置为, 在外地代理 FA 或分组数据服务节点 PDSN 和家乡代理 HA 之间协商建立 IPsec 隧道的过程中, 下发协商 IPsec 参数或协商 IPsec 参数所对应的属性标识 profileID 至所述 FA 或者所述 PDSN。

其中, 所述鉴权授权计费服务器还设置为, 在所述 FA 或所述 PDSN 和所述 HA 之间协商建立 IPsec 隧道的过程中, 下发所述协商 IPsec 参数或协商 IPsec 参数所对应的属性标识 profileID 至所述 HA。

其中, 所述鉴权授权计费服务器是设置为: 根据访问终端的安全等级选择对应的协商 IPsec 参数或协商 IPsec 参数所对应的 profileID 后下发所述协

商 IPSec 参数或协商 IPSec 参数所对应的 profileID。

本发明还提供一种支持移动 IP 接入的外地代理 FA 或分组数据服务节点 PDSN，其中：

所述 FA 或 PDSN 设置为，在和家乡 HA 之间协商建立 IPSec 隧道的过程中，从所述 AAA 获取协商 IPSec 参数；或者，从所述 AAA 获取协商 IPSec 参数所对应的 profileID，根据所述 profileID 得到协商 IPSec 参数。

本发明还提供一种支持移动 IP 接入的家乡代理 HA，其中，

所述 HA 设置为：在和外地代理 FA 或分组数据服务节点 PDSN 之间协商建立 IPSec 隧道的过程中，从鉴权授权计费服务器 AAA 获取协商 IPSec 参数或协商 IPSec 参数所对应的属性标识 profileID。

本发明还提供一种移动 IP 接入系统，包括上述提到的外地代理 FA 或分组数据服务节点 PDSN，鉴权授权计费服务器 AAA，和家乡代理 HA。

本发明不限于 CDMA2000 系统。

以上内容是结合具体的优选实施方式对本发明所作的进一步详细说明，但这只是为便于理解而举的实例，不应认为本发明的具体实施只局限于这些说明。对于本发明所属技术领域的普通技术人员来说，在不脱离本发明构思的前提下，可以做出各种可能的等同改变或替换，这些改变或替换都应属于本发明的保护范围。例如，某些 CDMA2000 系统中，PDSN (Packet Data Service Node 分组数据服务节点)在移动 IP 用户接入时具有 FA 同样的功能，所以在上述各实施例中，FA 可以用 PDSN 替换。

工业实用性

本发明选择并下发协商 IPSec 参数或协商 IPSec 参数所对应的 profileID 至 FA 和 HA，或 PDSN 和 HA，避免了在上述网元上手工配置协商 IPSec 参数，简化了系统配置，提高了系统的可用性，同时，由于 FA 和 HA，或 PDSN 和 HA 上的协商参数统一下发，协议版本相同，避免了不同版本造成的对接困难。

权 利 要 求 书

1、一种移动 IP 接入方法，包括，在外地代理 FA 或分组数据服务节点 PDSN 与家乡代理 HA 协商建立 Internet 协议安全隧道即 IPSec 隧道的过程中，鉴权授权计费服务器 AAA 下发协商 IPSec 参数或协商 IPSec 参数所对应的属性标识 profileID 至所述 FA 或所述 PDSN。

2、如权利要求 1 所述的接入方法，其特征在于，所述方法还包括，在外地代理 FA 或分组数据服务节点 PDSN 与家乡代理 HA 协商建立 Internet 协议安全隧道即 IPSec 隧道的过程中，所述 AAA 下发协商 IPSec 参数或协商 IPSec 参数所对应的属性标识 profileID 至所述 HA。

3、如权利要求 1 所述的接入方法，其中，所述 FA 或 PDSN 与所述 HA 协商建立所述 IPSec 隧道的过程包含：

A1、所述 FA 或 PDSN 向所述 AAA 发送认证请求；

A2、所述 AAA 将认证应答下发至所述 FA 或 PDSN，所述认证应答中包含所述协商 IPSec 参数或所述协商 IPSec 参数所对应的 profileID；

A3、所述 FA 或 PDSN 根据所述 AAA 下发的认证应答，发送协商请求至所述 HA；

A4、所述 HA 接收所述协商请求，从本地或者从所述 AAA 获取所述协商 IPSec 参数或协商 IPSec 参数所对应的 profileID，所述 FA 或所述 PDSN 与所述 HA 协商建立 IPSec 隧道。

4、如权利要求 3 所述的接入方法，其中，

所述认证应答中还包括预共享密钥和身份信息；

所述协商请求为所述 FA 或 PDSN 根据所述协商 IPSec 参数发起的 ISAKMP SA 建立的协商请求，所述 ISAKMP SA 建立的协商请求中携带提议建立的 ISAKMP SA 信息、密钥材料以及身份信息；

所述步骤 A4 中，所述 HA 收到所述协商请求后，从本地或从所述 AAA 获取所述协商 IPSec 参数，所述 FA 或所述 PDSN 与所述 HA 协商建立 IPSec

隧道的步骤包括:

所述 HA 收到所述 ISAKMP SA 建立的协商请求后, 根据其中的所述身份信息还原所述 FA 或 PDSN 的地址, 从本地获取 S Key 和所述协商 IPSec 参数, 或者, 从所述 AAA 获取所述 S Key 和所述协商 IPSec 参数;

所述 HA 根据所述身份信息以及所述 S Key, 生成 IPSec 的预共享密钥;

所述 HA 与所述 FA 或 PDSN 交互, 从而建立所述 FA 或 PDSN 与所述 HA 之间的 IPSec 隧道。

5、如权利要求 3 所述的接入方法, 其中,

所述认证应答中还包括预共享密钥和身份信息;

所述步骤 A3 中还包括, 所述 FA 或 PDSN 根据所述协商 IPSec 参数所对应 profileID 在本地获取所述协商 IPSec 参数;

所述步骤 A3 中: 所述协商请求为所述 FA 或 PDSN 根据所述本地获取的协商 IPSec 参数发起的 ISAKMP SA 建立的协商请求, 所述 ISAKMP SA 建立的协商请求中携带提议建立的 ISAKMP SA 信息、密钥材料以及身份信息;

所述步骤 A4 中, 所述 HA 收到所述协商请求后, 从本地或者从所述 AAA 获取协商 IPSec 参数所对应的 profileID, 所述 FA 或所述 PDSN 与所述 HA 协商建立 IPSec 隧道的步骤包括:

所述 HA 收到所述 ISAKMP SA 建立的协商请求后, 根据其中的所述身份信息还原所述 FA 或 PDSN 的地址, 从本地获取 S Key 和所述协商 IPSec 参数对应的 profileID, 或者, 从所述 AAA 获取所述 S Key 和协商 IPSec 参数对应的 profileID;

所述 HA 根据所述身份信息以及 S Key, 生成 IPSec 的预共享密钥;

所述 HA 与所述 FA 或 PDSN 交互, 从而建立所述 FA 或 PDSN 与所述 HA 之间的 IPSec 隧道。

6、如权利要求 1 至 5 任一所述的接入方法, 其中, 所述协商 IPSec 参数或协商 IPSec 参数所对应的 profileID 是与访问终端的安全等级对应的协商

IPSec 参数或协商 IPSec 参数所对应的 profileID。

7、如权利要求 6 所述的接入方法，其中，所述访问终端的安全等级由运营商或用户预先设定。

8、一种支持移动 IP 接入的鉴权授权计费服务器，所述鉴权授权计费服务器设置为，在外地代理 FA 或分组数据服务节点 PDSN 和家乡代理 HA 之间协商建立 IPSec 隧道的过程中，下发协商 IPSec 参数或协商 IPSec 参数所对应的属性标识 profileID 至所述 FA 或者所述 PDSN。

9、如权利要求 8 所述的鉴权授权计费服务器，其中，所述鉴权授权计费服务器还设置为，在所述 FA 或所述 PDSN 和所述 HA 之间协商建立 IPSec 隧道的过程中，下发所述协商 IPSec 参数或协商 IPSec 参数所对应的 profileID 至所述 HA。

10、如权利要求 8 或 9 所述的鉴权授权计费服务器，其中，所述鉴权授权计费服务器是设置为：根据访问终端的安全等级选择对应的协商 IPSec 参数或协商 IPSec 参数所对应的 profileID 后下发所述协商 IPSec 参数或协商 IPSec 参数所对应的 profileID。

11、一种支持移动 IP 接入的外地代理 FA 或分组数据服务节点 PDSN，其中：

所述 FA 或 PDSN 设置为，在和家乡 HA 之间协商建立 IPSec 隧道的过程中，从所述 AAA 获取协商 IPSec 参数；或者，从所述 AAA 获取协商 IPSec 参数所对应的 profileID，根据所述 profileID 得到协商 IPSec 参数。

12、一种支持移动 IP 接入的家乡代理 HA，其中，

所述 HA 设置为：在和外地代理 FA 或分组数据服务节点 PDSN 之间协商建立 IPSec 隧道的过程中，从鉴权授权计费服务器 AAA 获取协商 IPSec 参数或协商 IPSec 参数所对应的属性标识 profileID。

13、一种移动 IP 接入系统，包括：外地代理 FA 或分组数据服务节点 PDSN、以及鉴权授权计费服务器 AAA，其中，

所述 AAA 设置为，在外地代理 FA 或分组数据服务节点 PDSN 和家乡代

理 HA 之间协商建立 IPSec 隧道的过程中, 下发所述协商 IPSec 参数或协商 IPSec 参数所对应的属性标识 profileID 至所述 FA 或者所述 PDSN;

所述 FA 或 PDSN 设置为, 在和所述 HA 之间协商建立 IPSec 隧道的过程中, 从所述 AAA 获取协商 IPSec 参数; 或者, 从所述 AAA 获取协商 IPSec 参数所对应的 profileID, 根据所述 profileID 得到协商 IPSec 参数。

14、如权利要求 13 所述的接入系统, 其中, 所述系统还包括家乡代理 HA, 其中:

所述 AAA 还设置为, 在所述 FA 或所述 PDSN 和所述 HA 之间协商建立 IPSec 隧道的过程中, 下发协商 IPSec 参数或协商 IPSec 参数所对应的属性标识 profileID 至所述 HA;

所述 HA 设置为, 在和所述 FA 或所述 PDSN 之间协商建立 IPSec 隧道的过程中, 从所述 AAA 获取所述协商 IPSec 参数或协商 IPSec 参数所对应的 profileID。

15、如权利要求 13 或 14 所述的接入系统, 其中,

所述 AAA 是设置为: 根据访问终端的安全等级选择对应的协商 IPSec 参数或协商 IPSec 参数所对应的 profileID 后下发所述协商 IPSec 参数或协商 IPSec 参数所对应的 profileID。

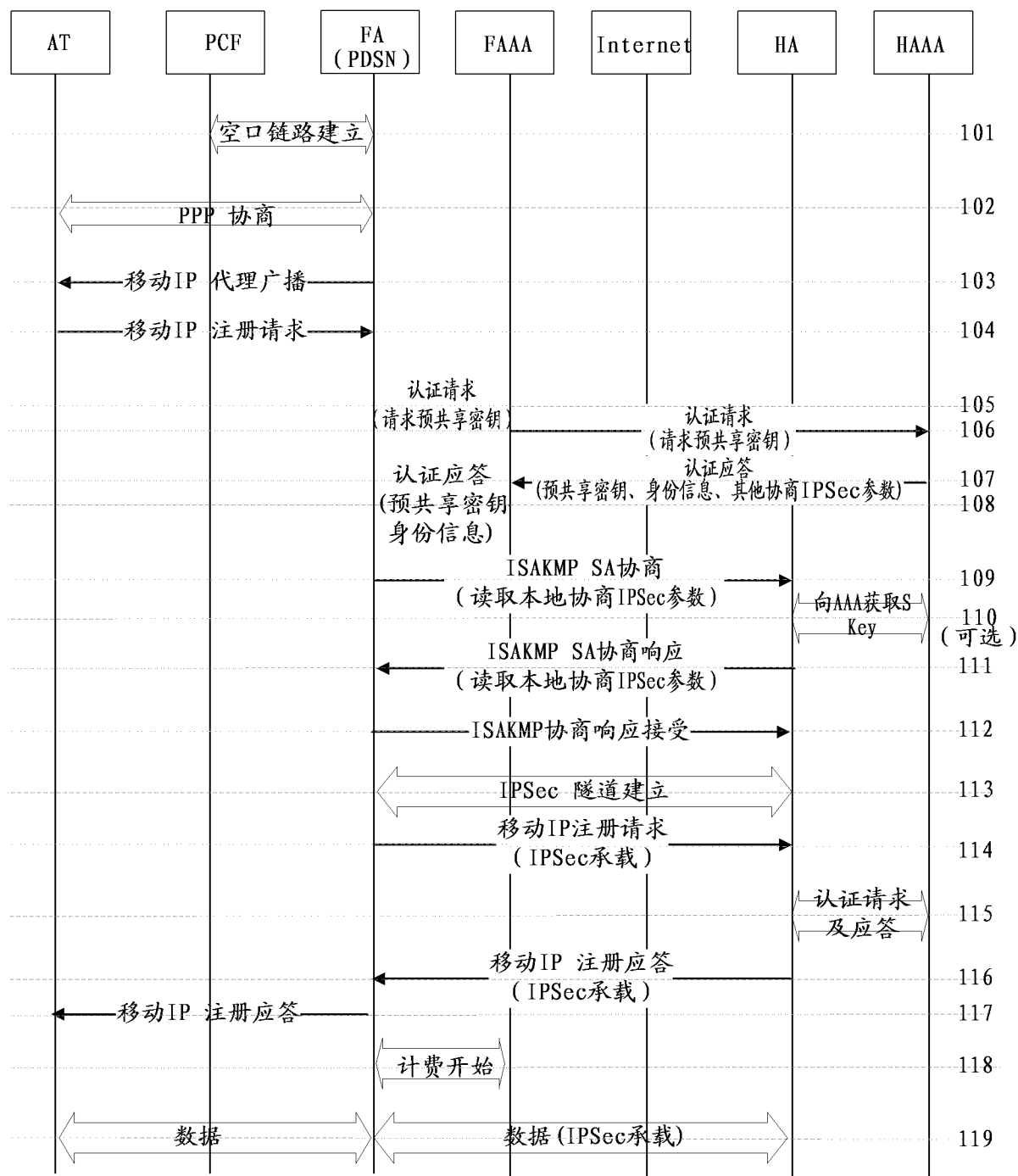


图 1

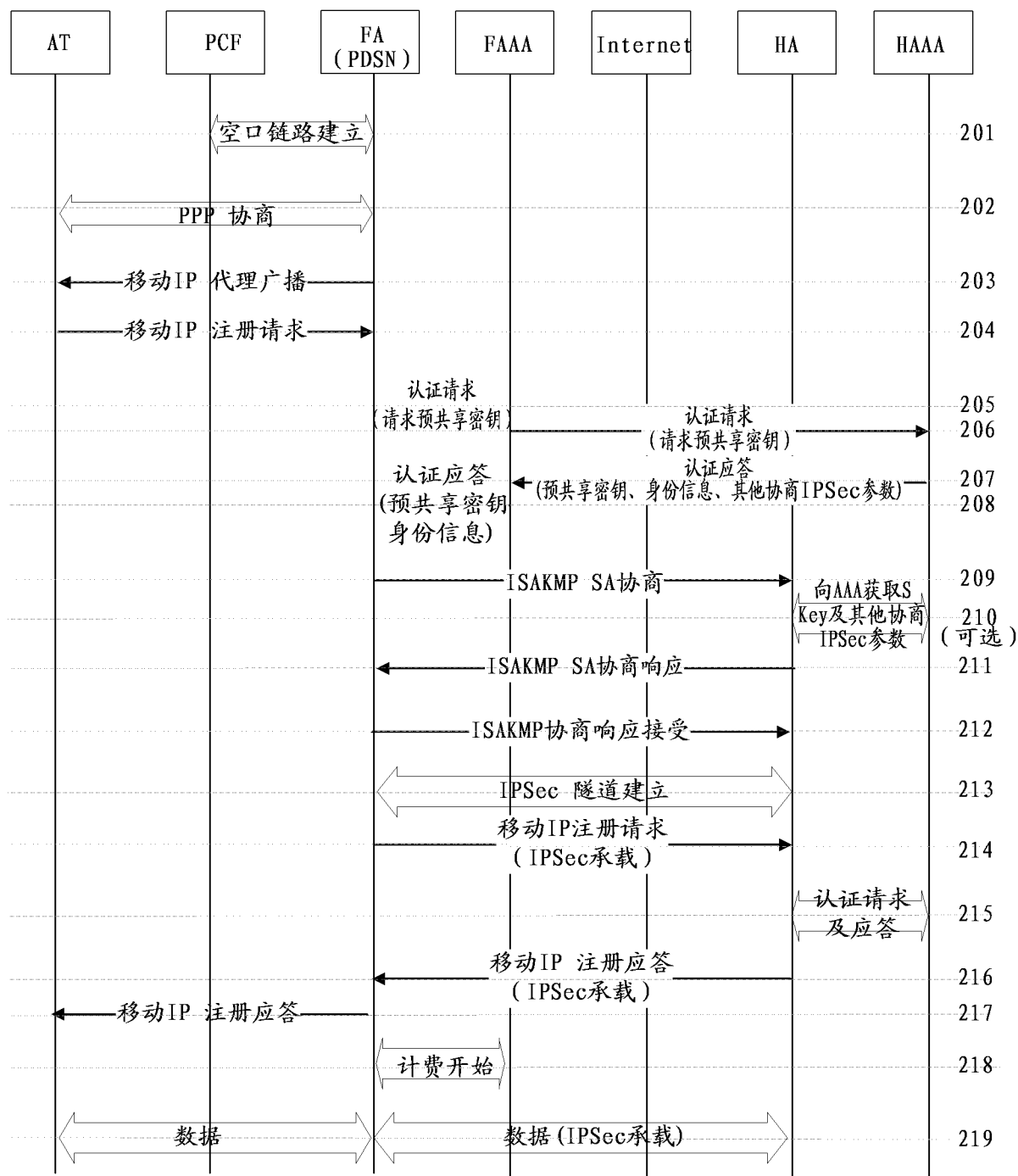


图 2

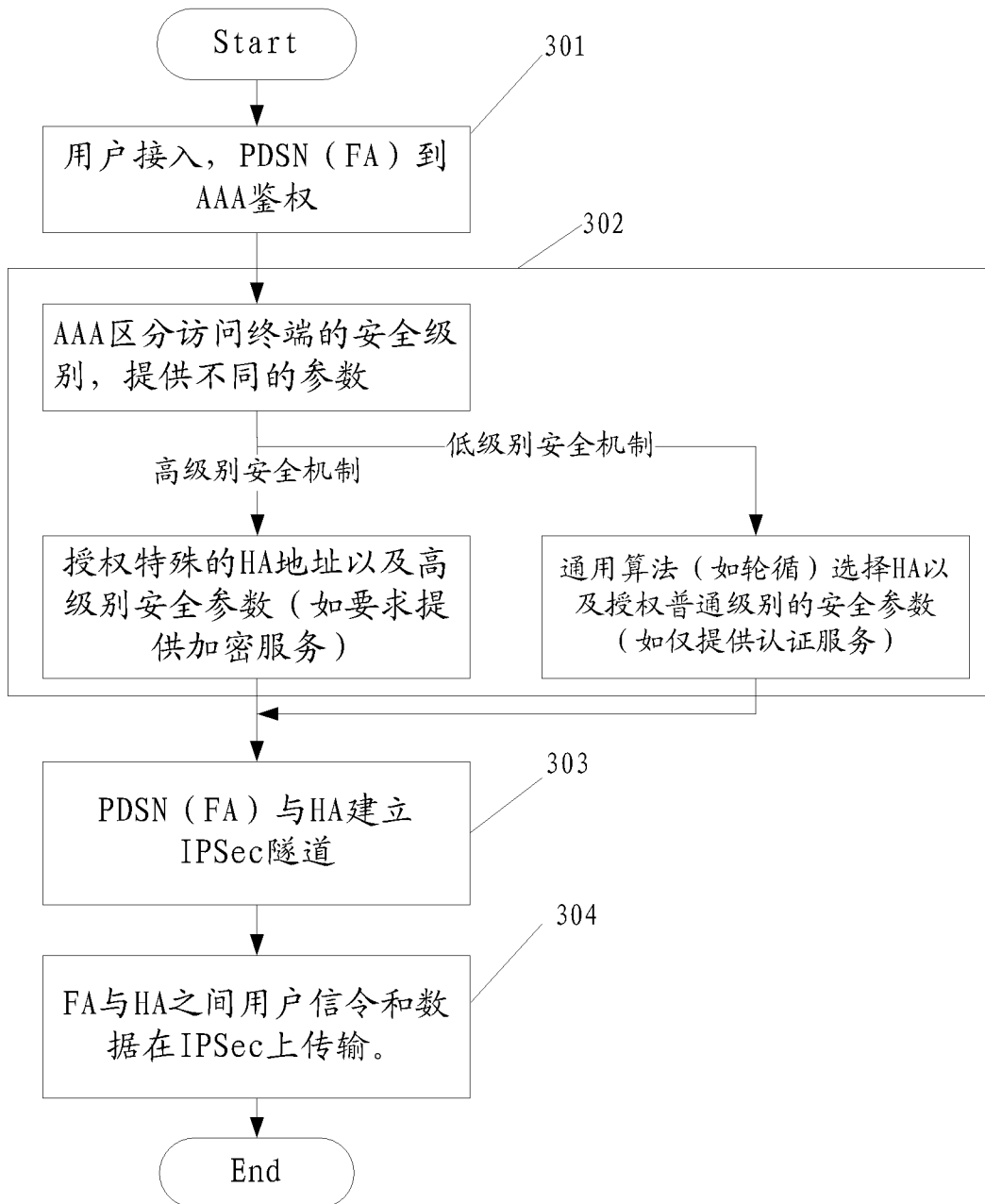


图 3

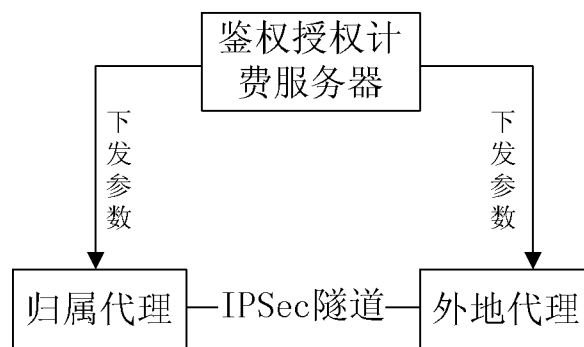


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2010/072593

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/56 (2006.01) i

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: H04L, H04W, G06F

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)

CNKI, CPRSABS, CNTXT, WPI, EPODOC, IEEE: Internet protocol security, IP security, protocol security, security tunnel, establish, construct, policy, strategy, parameter, configure, collocate, setting, setup, automatic, manual, authentication, authorization, accounting, AAA, server, agent, foreign agent, FA, home agent, HA, packet data service node, PDSN, profile ID

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN101656961A (ZTE CORP) 24 Feb. 2010 (24.02.2010), the whole document	1-15
A	CN1905452A (CHINA TELECOM CO LTD) 31 Jan. 2007 (31.01.2007), the description page 1 line 16 to page 2 line 12, page 3 line 16 to page 4 line 11, figures 1-6	1-15
A	US2007136590A1 (ELECTRONICS&TELECOM RES INST) 14 Jun. 2007 (14.06.2007), the whole document	1-15

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

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 29 Jul. 2010 (29.07.2010)	Date of mailing of the international search report 19 Aug. 2010 (19.08.2010)
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 TANG Wensen Telephone No. (86-10)62411230

International application No.
PCT/CN2010/072593

Form PCT/ISA /210 (patent family annex) (July 2009)

A. 主题的分类		
H04L 12/56 (2006.01) i		
按照国际专利分类(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: H04L, H04W, G06F		
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))		
CNKI, CPRSABS, CNTXT: IPSec IP 安全 协议安全 安全隧道 安全通道 建立 构建 策略 参数 配置 设置 自动 手动 认证 鉴权 授权 计费 AAA 服务器 代理 外地代理 FA 家乡代理 本地代理 HA 分组数据服务节点 PDSN 属性标识 profile ID		
WPI, EPODOC, IEEE: Internet protocol security, IP security, protocol security, security tunnel, establish, construct, policy, strategy, parameter, configure, collocate, setting, setup, automatic, manual, authentication, authorization, accounting, AAA, server, agent, foreign agent, FA, home agent, HA, packet data service node, PDSN, profile ID		
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
PX	CN101656961A (中兴通讯股份有限公司) 24.2 月 2010 (24.02.2010), 全文	1~15
A	CN1905452A (中国电信股份有限公司) 31.1 月 2007 (31.01.2007), 说明书第 1 页第 16 行至第 2 页第 12 行、第 3 页第 16 行至第 4 页第 11 行, 图 1~6	1~15
A	US2007136590A1 (ELECTRONICS&TELECOM RES INST) 14.6 月 2007 (14.06.2007), 全文	1~15
☐ 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(如具体说明的) “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 29.7 月 2010 (29.07.2010)		国际检索报告邮寄日期 19.8 月 2010 (19.08.2010)
ISA/CN 的名称和邮寄地址: 中华人民共和国国家知识产权局 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号: (86-10)62019451		授权官员 唐文森 电话号码: (86-10) 62411230

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2010/072593

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN101656961A	24.02.2010	无	
CN1905452A	31.01.2007	CN100596069C	24.03.2010
US2007136590A1	14.06.2007	KR20070061619A	14.06.2007
		KR100753820B1	31.08.2007