(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
2013 年 9 月 6 日 (06.09.2013)

WIPO | PCT

(10) 国际公布号
WO 2013/127190 A1

(51) 国际专利分类号:
H04W 12/06 (2009.01) *H04W 12/10* (2009.01)

(21) 国际申请号: PCT/CN2012/084314

(22) 国际申请日: 2012 年 11 月 8 日 (08.11.2012)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210050881.9 2012 年 2 月 29 日 (29.02.2012) CN

(71) 申请人: **大唐移动通信设备有限公司 (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO.,LTD)** [CN/CN]; 中国北京市海淀区学院路 29 号, Beijing 100083 (CN)。

(72) 发明人: **吴鹏程 (WU, Pengcheng)**; 中国北京市海淀区学院路 29 号, Beijing 100083 (CN)。

(74) 代理人: **北京同达信恒知识产权代理有限公司 (TDIP & PARTNERS)**; 中国北京市西城区裕民路 18 号北环中心 A 座 2002, Beijing 100029 (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, BN, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, 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, RS, SE, SI, SK, SM, 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(条约第 21 条(3))。

(54) **Title**: NAS ALGORITHM TRANSMISSION METHOD AND DEVICE

(54) **发明名称** : 一种 NAS 算法的传输方法及装置

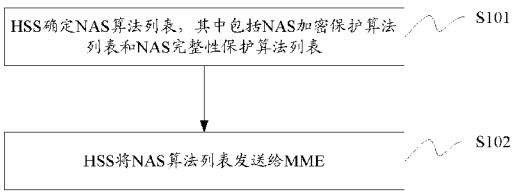

图 1 / Fig. 1

S101 AN HSS DETERMINING AN NAS ALGORITHM LIST WHICH COMPRISES AN NAS ENCRYPTION PROTECTION ALGORITHM LIST AND AN NAS INTEGRITY PROTECTION ALGORITHM LIST
S102 THE HSS SENDING THE NAS ALGORITHM LIST TO AN MME

(57) **Abstract**: Disclosed are an NAS algorithm transmission method and device, which are used to achieve the process of determining an NAS algorithm by an HSS and sending same to an MME, so that an operator can modify subscription information about the HSS according to a BOSS end, and freely configure the NAS algorithm in accordance with subscribers of different qualifications. An NAS algorithm notification method provided in the application comprises: a home subscriber server (HSS) determining an NAS algorithm list which comprises an NAS encryption protection algorithm list and an NAS integrity protection algorithm list; and the HSS sending the NAS algorithm list to a mobility management entity (MME).

(57) **摘要**: 本申请公开了一种 NAS 算法的传输方法及装置，用以实现由 HSS 确定 NAS 算法并下发该 NAS 算法给 MME 的过程，使得运营商可以根据 BOSS 端对 HSS 的签约信息进行修改，针对不同资质的用户对 NAS 算法进行灵活配置。本申请提供的一种 NAS 算法的通知方法包括：归属签约用户服务器 HSS 确定 NAS 算法列表，其中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表；HSS 将所述 NAS 算法列表发送给移动性管理实体 MME。

WO 2013/127190 A1

一种 NAS 算法的传输方法及装置

本申请要求在 2012 年 2 月 29 日提交中国专利局、申请号为 201210050881.9、发明名称为“一种 NAS 算法的传输方法及装置”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

本发明涉及通信技术领域，尤其涉及一种 NAS 算法的传输方法及装置。

背景技术

在长期演进（Long Term Evolution，LTE）网络内，移动性管理实体（Mobility Management Entity，MME）和用户设备（User Equipment，UE）之间的非接入层（Non-Access Stratum，NAS）消息传输是被完整性保护和安全保护的。MME 可以根据 UE 上报的网络能力和 MME 配置的安全算法能力以及优先级来决定使用哪种安全算法。

现有在 MME 上配置算法能力和优先级的方法，在配置数据固定的情况下不能轻易地对算法集合以及优先级做出改变。另外，在目前使用的算法中，包括演进的分组系统（Evolved Packet System，EPS）加密算法 0~EPS 加密算法 7（EEA0~EEA7；EPS Encryption Algorithm，EEA）以及 EPS 完整性保护算法 0~EPS 完整性保护算法 7（EIA0~EIA7；EPS Integrity Algorithm，EIA），每一种算法的安全保护程度以及运行效率都是不一样的，现有配置 NAS 层算法列表的方法无法满足用户对 NAS 安全算法多样性的需要。

现在 LTE 网络中，MME 选择加密保护算法和完整性保护算法主要依据 UE 上报的 UE 安全能力（UE Security Capability）和 MME 上配置的算法集合以及优先级。

在 3GPP TS 33.401 V9.4.0 协议 7.2.4.3 章节中，MME 需要能够通过配置算法列表配置加密保护算法列表和完整性保护算法列表。在建立 NAS 安全上下文的时候，MME 根据算法集合选择出优先级排列最高的 NAS 安全算法。并通过发起安全模式控制过程，将选择的算法以及 UE 支持的安全能力通过安全模式命令（Security Mode Command）消息发送给 UE。

也就是说，MME 选择算法是根据 UE 的安全能力以及网络侧配置的 NAS 安全算法集以及算法的优先级来决定的。

UE 侧的安全能力是根据 UE 本身所支持的算法，可以根据 UE 自身的安全能力决定。而网络侧配置的 NAS 安全算法集以及算法的优先级通过在 MME 上预先配置的方法实现。如果多个 UE 上报的安全能力一样，MME 选择出的算法必然是一样，不能体现出用户之间的差异性和多样性。

另外，加密保护算法 EEA0~EEA7 以及完整性保护算法 EIA0~EIA7 之间，每种算法的安全保护程度以及运行效率也都是不同的。对不同的用户来说，效率和安全程度的要求是不一样的。

综上所述，现有技术在网络侧配置 NAS 安全算法列表的方法使得运营商无法灵活地针对具体用户来灵活改变 NAS 层使用的安全算法。

发明内容

本发明实施例提供了一种 NAS 算法的传输方法及装置，用以实现由归属签约用户服务器（Home Subscriber Server，HSS）确定 NAS 算法并下发该 NAS 算法给 MME 的过程，使得运营商可以根据业务运营支撑系统（Business Operating Support System，BOSS）端对 HSS 的签约信息进行修改，针对不同资质的用户对 NAS 算法进行灵活配置。

本发明实施例提供的一种 NAS 算法的通知方法包括:

归属签约用户服务器 HSS 确定 NAS 算法列表，其中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表;

HSS 将所述 NAS 算法列表发送给移动性管理实体 MME。

本发明实施例提供的一种 NAS 算法的获取方法包括:

移动性管理实体 MME 接收归属签约用户服务器 HSS 发送的携带有 NAS 算法列表的消息，所述 NAS 算法列表中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表;

MME 从所述消息中获取 NAS 算法列表。

本发明实施例提供的一种 NAS 算法的通知装置包括:

NAS 算法列表确定单元，用于确定 NAS 算法列表，其中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表;

通知单元，用于将所述 NAS 算法列表发送给移动性管理实体 MME。

本发明实施例提供的一种 NAS 算法的获取装置包括:

消息接收单元，用于接收归属签约用户服务器 HSS 发送的携带有 NAS 算法列表的消息，所述 NAS 算法列表中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表;

获取单元，用于从所述消息中获取 NAS 算法列表。

本发明实施例中，归属签约用户服务器 HSS 确定 NAS 算法列表，其中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表；HSS 将所述 NAS 算法列表发送给移动性管理实体 MME，从而实现了由 HSS 来配置 NAS 算法列表的策略，运营商可以通过 BOSS 系统来修改 HSS 中的用户签约数据，使得 NAS 安全算法和服务质量（Quality of Service，QoS）等用户信息进行关联，针对不同用户的需求，可以选择不同特点的算法对 NAS 消息进行安全保护。

附图说明

图 1 为本发明实施例提供的一种 NAS 算法的通知方法的流程示意图;

图 2 为本发明实施例提供的一种 NAS 算法的获取方法的流程示意图;

图 3 为本发明实施例提供的鉴权信息获取过程示意图;

图 4 为本发明实施例提供的插入签约数据过程示意图;

图 5 为本发明实施例提供的插入签约数据成功过程示意图;

图 6 为本发明实施例提供的插入签约数据失败过程示意图;

图 7 为本发明实施例提供的一种 NAS 算法的通知装置的结构示意图;

图 8 为本发明实施例提供的一种 NAS 算法的获取装置的结构示意图。

具体实施方式

本发明实施例提供了一种 NAS 算法的传输方法及装置，用以实现由 HSS 确定 NAS 算法并下发该 NAS 算法给 MME 的过程，使得运营商可以根据 BOSS 端对 HSS 的签约信息进行修改，针对不同资质的用户对 NAS 算法进行灵活配置。

本发明实施例将 NAS 层算法列表由 MME 配置改变为由 HSS 下发。运营商可以根据业务运营支撑系统（Business Operating Support System，BOSS）端对 HSS 的签约信息进行修改，针对不同资质的用户对算法列表进行灵活配置。

参见图 1，本发明实施例提供的一种 NAS 算法的通知方法，包括:

S101、HSS 确定 NAS 算法列表，其中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表;

S102、HSS 将 NAS 算法列表发送给 MME。

较佳地，HSS 将 NAS 算法列表发送给 MME，包括:

HSS 通过鉴权信息获取过程或者插入签约数据过程，将 NAS 算法列表传递给 MME。

较佳地，HSS 通过鉴权信息获取过程将 NAS 算法列表传递给 MME，包括:

HSS 接收 MME 发送的鉴权信息请求（Authentication Information Request）消息;

HSS 将鉴权信息响应（Authentication Information Answer）消息发送给 MME，其中携带 NAS 算法列表。

较佳地，HSS 通过插入签约数据过程，将 NAS 算法列表传递给 MME，包括:

当签约数据更新时，HSS 向 MME 发送插入签约数据请求（Insert Subscriber Data Request）消息，其中携带 NAS 算法列表。

较佳地，NAS 算法列表中的算法，按照预设优先级从高到低的顺序排列。

相应地，参见图 2，本发明实施例提供的一种 NAS 算法的获取方法，包括:

S201、MME 接收 HSS 发送的携带有 NAS 算法列表的消息，该 NAS 算法列表中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表;

S202、MME 从该消息中获取 NAS 算法列表。

较佳地，MME 通过鉴权信息获取过程或者插入签约数据过程，接收 HSS 发送的携带有 NAS 算法列表的消息。

较佳地，MME 通过鉴权信息获取过程接收 HSS 发送的携带有 NAS 算法列表的消息，包括:

MME 向 HSS 发送鉴权信息请求（Authentication Information Request）消息;

MME 接收 HSS 发送的鉴权信息响应（Authentication Information Answer）消息，其中携带 NAS 算法列表。

较佳地，MME 通过插入签约数据过程，接收 HSS 发送的携带有 NAS 算法列表的消息，包括:

当签约数据更新时，MME 接收 HSS 发送的插入签约数据请求（Insert Subscriber Data Request）消息，其中携带 NAS 算法列表。

较佳地，NAS 算法列表中的算法，按照预设优先级从高到低的顺序排列。

较佳地，MME 获取 NAS 算法列表后，该方法还包括:

MME 从 NAS 算法列表中选择 NAS 算法，并将选择的 NAS 算法通知给 UE。

较佳地，MME 从 NAS 算法列表中选择 NAS 算法，将选择的 NAS 算法通知给 UE，包括:

MME 确定自身支持的 NAS 加密保护算法集合 A1 和 NAS 完整性保护算法集合 A2;

MME 确定 UE 支持的 NAS 加密保护算法集合 B1 和 NAS 完整性保护算法集合 B2;

MME 确定 NAS 算法列表中的 NAS 加密保护算法集合 C1 和 NAS 完整性保护算法集合 C2;

MME 确定集合 A1、B1 和 C1 的交集 D1，以及 A2、B2 和 C2 的交集 D2;

MME 将交集 D1 中的 NAS 加密保护算法和交集 D2 中的 NAS 完整性保护算法集合通知给 UE。

较佳地，该方法还包括:

当 NAS 算法列表更新时，MME 从 HSS 发送的插入签约数据请求（Insert Subscriber Data Request）消息中获取更新的 NAS 算法列表;

MME 从更新的 NAS 算法列表中重新选择 NAS 算法;

当重新选择的 NAS 算法，与现有的 NAS 算法不一致时，MME 向 UE 发送安全模式命令（Security Mode Command）消息，其中携带重新选择的 NAS 算法;

当重新选择的 NAS 算法，与现有的 NAS 算法一致时，或者当 MME 从更新的 NAS 算法列表中重新选择 NAS 算法的操作失败时，MME 向 HSS 回复插入签约数据应答（Insert Subscriber Data Answer）消息。

较佳地，MME 向 UE 发送安全模式命令（Security Mode Command）消息后，该方法还包括:

MME 接收 UE 发送的安全模式完成（Security Mode Complete）消息或者安全模式拒绝（Security Mode Reject）消息;

MME 向 HSS 回复插入签约数据应答（Insert Subscriber Data Answer）消息。

本发明实施例中，预先在 3GPP TS 29.272 协议的表 7.3.1/1 中，增加定义信息元素（Information Elements），如下面的表 7.3.1/1 所示：

				AVP Flag rules（AVP 标志规则）				
Attribute Name（特征名称）	**AVP Code（AVP 码）**	**Section defined（定义的章节）**	**Value Type（内容类型）**	**Must（必须）**	**May（可能）**	**Should not（可能不）**	**Must not（必须不）**	**May encrypted（可能加密）.**
NAS-Algorithms-Lists（NAS 算法列表）	1651	7.3.165	Grouped（聚合）	M, V				No
NAS-ciphering-algorithms-List（NAS加密保护算法列表）	1652	7.3.166	UTF8String(UTF8字符)	M, V				No
NAS-integrity-algorithms-List（NAS完整性保护算法列表）	1653	7.3.167	UTF8String(UTF8字符)	M, V				No

表 7.3.1/1: S6a/S6d 接口和 S13/S13 接口 属性值定义（S6a/S6d and S13/S13' specific Diameter AVPs）

并且，预先在 3GPP TS 29.272 增加 7.3.165 章节，描述如下：

NAS-Algorithms-Lists（NAS 算法列表）

The AVP format shall conform to（属性值类型应当遵照以下格式）:

NAS-Algorithms-Lists（NAS 算法列表）::= <AVP header（属性值 头）: 1613 10415>

{ NAS-ciphering-algorithms-List （NAS 加密保护算法列表）}

{ NAS-integrity-algorithms-List（NAS 完整性保护算法列表） }

以及，在 3GPP TS 29.272 中增加 7.3.166 章节，描述如下：

NAS-ciphering-algorithms-List （NAS 加密保护算法列表）

NAS 加密保护算法列表（NAS-ciphering-algorithms-List）由长度不大于 8 的字符串通用转换格式编码（UTF8String）字符串表示，支持的加密保护算法，0~7 分别代表 EEA0~EEA7，按优先级从高到低排列。

在 3GPP TS 29.272 增加 7.3.166 章节，描述如下：

NAS-integrity-algorithms-List（NAS 完整性保护算法列表）

NAS 完整性保护算法列表（NAS-integrity-algorithms-List）由长度不大于 8 的 UTF8String 字符串表示，支持的完整性保护算法，0~7 分别代表 EIA0~EIA7，按优先级从高到低排列。

具体的 NAS 算法列表的传输方法，可以有两种：

第一种：在 HSS 和 MME 之间的鉴权信息获取过程（Authentication Procedures）中传递 NAS 算法列表（NAS-Algorithms-Lists）。

在现有鉴权信息响应消息结构（见表 5.2.3.1.1/2）中增加 NAS 算法列表（NAS-Algorithms-Lists），如下表 5.2.3.1.1/2 所示：

Information element name（信息元素名称）	Mapping to Diameter AVP（映射到Diameter协议的AVP）	Cat.（种类）	Description（描述）
Result（原因） (See 7.4)	Result-Code / Experimental-Result（原因值/结果值）	M	This IE shall contain the result of the operation（该信息元素应当包含结果操作码）. This IE shall contain the Result-Code AVP shall be used to indicate success / errors as defined in the Diameter Base Protocol.（该信息元素应该包含结果码的属性值，被用来指示成功或者失败） The Experimental-Result AVP shall be used for S6a/S6d errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.（结果值被用来表示S6a/S6d接口的错误，该属性值应该包含制造商标识和错误码） The following errors are applicable in this case:（以下的错误码在这种情况下被使用） - User Unknown（未知用户） - Unknown EPS Subscription（未知EPS签约）
Supported Features（支持的特征） (See 3GPP TS 29.229 [9])	Supported-Features（支持的特征）	O	If present, this information element shall contain the list of features supported by the origin host.（如果出现，该信息元素需要包含来自源地址的支持的特征列表）
Authentication Info（鉴权信息） (See 7.3.17)	Authentication-Info（鉴权信息）	C	This IE shall contain the Authentication Vectors.（该信息元素需要包含鉴权向量）
NAS-Algorithms-Lists（NAS算法列表）	NAS-Algorithms-Lists（NAS算法列表）	C	This IE shall contain the NAS Algorithms Lists。（该信息元素需要包含算法列表）

表 5.2.3.1.1/2: 鉴权信息响应（Authentication Information Answer）

HSS 通过鉴权信息获取过程将 NAS 算法列表传递给 MME，如图 3 所示。

MME 向 HSS 发出鉴权信息请求（Authentication Information Request）消息，HSS 收到该消息后，将用户相关的 NAS 算法列表包含在鉴权信息响应（Authentication Information Answer）消息中发给 MME。NAS 算法列表包括 NAS 加密保护算法列表和以及 NAS 完整性保护算法列表。其中，NAS 加密保护算法列表和 NAS 完整性保护算法列表中，各算法按照优先级从

高到低排列。

第二种：在 HSS 和 MME 之间的插入签约数据过程（Insert Subscriber Data Procedure）中传递 NAS 算法列表（NAS-Algorithms-Lists）。

Information element name（信息元素名称）	Mapping to Diameter AVP（映射到Diameter协议的AVP）	Cat.（种类）	Description（描述）
IMSI（国际移动用户标识符）	User-Name（用户名）(See IETF RFC 3588 [4])	M	This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [3], clause 2.2.（这个信息元素需要包含用户的国际移动签约标识，格式参照协议3GPP TS 23.003的2.2章节。）
Supported Features（支持的特征） (See 3GPP TS 29.229 [9])	Supported-Features（支持的特征）	O	If present, this information element shall contain the list of features supported by the origin host.（如果出现，该信息元素需要包含来自源地址的支持的特征列表）
Subscription Data（签约数据） (See 7.3.2)	Subscription-Data（签约数据）	M	This Information Element shall contain the part of the subscription profile that either is to be added to the subscription profile stored in the MME or SGSN or is replacing a part of the subscription profile stored in the MME or SGSN.（该信息元素应该包含部分签约数据，该签约数据可以被MME或者SGSN保存，或者更新MME或者SGSN中保存的签约数据）
IDR Flags（IDR标志） (See 7.3.103)	IDR-Flags（IDR标志）	C	This Information Element shall contain a bit mask. See 7.3.103 for the meaning of the bits.（该信息元素应该包含一个位掩码，位掩码参见7.3.103章节）
NAS-Algorithms-Lists（NAS算法列表）	NAS-Algorithms-Lists（NAS算法列表）	C	This IE shall contain the NAS Algorithms Lists。（该信息元素需要包含算法列表）

表 5.2.2.1.1/1：插入签约数据请求（Insert Subscriber Data Request）

HSS 通过插入签约数据过程将 NAS 算法列表传递给 MME，如图 4 所示。

在签约数据改变的情况下，HSS 向 MME 发出插入签约数据请求（Insert Subscriber Data Request）消息，包含用户相关的 NAS 算法列表。NAS 算法列表包括 NAS 加密保护算法列表和以及 NAS 完整性保护算法列表。其中 NAS 加密保护算法列表和 NAS 完整性保护算法列表中，算法按照优先级从高到低排列。MME 收到插入签约数据请求后，向 HSS 回复插入签约数据应答（Insert Subscriber Data Answer）消息。

下面介绍一下本发明实施例提供的 MME 从接收到的 NAS 算法列表中选择 NAS 加密保护算法和 NAS 完整性保护算法的方法。

对于 NAS 加密保护算法和 NAS 完整性保护算法，采用相同的处理过程，下面以其中一种算法为例进行说明。

MME 需要支持尽可能多的算法集，假如算法集合为 A。

UE 通过附着请求（ATTACH REQUEST）消息或者位置区域更新请求（TRACKING AREA UPDATE REQUEST）消息，携带 UE 网络能力（UE network capability）给 MME，即将 UE 支持的算法结合通知给 MME，记为集合 B。

运营商可以根据用户资质，对每个用户设置不同的算法集和优先级，通过鉴权信息获取过程（Authentication Procedures）或者插入签约数据过程（Insert Subscriber Data Procedure）将 NAS 算法列表（NAS-Algorithms-Lists）传递给 MME，假设 NAS 算法列表中的算法集合为 C。

首先选择出算法集合 D 为 A、B、C 三者的交集，即 $D = A \cap B \cap C$。

在根据 NAS 算法列表（NAS-Algorithms-Lists）表示的优先级对计算出的 D 进行选择，选择出优先级最高的 NAS 加密保护算法或 NAS 完整性保护算法。

MME 通过安全模式控制（Security Mode Command）消息将选择的 NAS 加密保护算法和 NAS 完整性保护算法发送给 UE。

下面介绍一下本发明实施例提供的在 HSS 和 MME 之间的插入签约数据过程（Insert Subscriber Data Procedure）中传递 NAS 算法列表（NAS-Algorithms-Lists）后的处理流程。

参见图 5，插入签约数据成功的流程如下：

步骤一，当 NAS 算法列表改变的时候，HSS 向 MME 发送插入签约数据请求（Insert Subscriber Data Request）消息给 MME，消息中携带 NAS 算法列表（NAS-Algorithms-Lists）。

步骤二，MME 从插入签约数据请求中获取到 NAS 算法列表后，对 NAS 算法进行再次选择。

如果发现再次选择的 NAS 算法和 MME 与 UE 之间当前采用的 NAS 算法不一致，则 MME 向 UE 发生安全模式命令（Security Mode Command）消息，消息中携带再次选择的 NAS 算法。

如果再次选择的 NAS 算法和 MME 与 UE 之间当前采用的 NAS 算法一致，MME 和 UE 之间不再发起安全模式控制（Security mode control，SMC）过程，MME 直接向 HSS 回复插入签约数据应答（Insert Subscriber Data Answer），则插入签约数据成功。

步骤三，UE 对安全模式命令（Security Mode Command）消息进行校验，当校验成功时，UE 向 MME 发送一个安全模式完成（Security Mode Complete）消息。

步骤四，MME 对安全模式完成（Security Mode Complete）消息进行完整性保护校验和

解密，成功则 NAS 算法更新成功。MME 向 HSS 回复插入签约数据应答（Insert Subscriber Data Answer），则插入签约数据成功。

参见图 6，插入签约数据失败的流程如下：

步骤一，当 NAS 算法列表改变的时候，HSS 向 MME 发送插入签约数据请求（Insert Subscriber Data Request）消息给 MME，消息中携带更新后的 NAS 算法列表（NAS-Algorithms-Lists）。

步骤二，MME 从插入签约数据请求中获取到 NAS 算法列表后，对 NAS 算法进行再次选择。

如果发现再次选择的 NAS 算法和 MME 与 UE 之间当前采用的 NAS 算法不一致，则 MME 向 UE 发生安全模式命令（Security Mode Command）消息，消息中携带再次选择的 NAS 算法。

如果再次选择 NAS 算法的过程失败，则 MME 和 UE 之间不再发起安全模式控制（Security mode control，SMC）过程，MME 直接向 HSS 回复插入签约数据应答（Insert Subscriber Data Answer），则插入签约数据失败。

步骤三，UE 对安全模式命令（Security Mode Command）消息进行校验，若校验失败，则 UE 向 MME 发送一个安全模式拒绝（Security Mode Reject）消息。

步骤四，MME 收到安全模式拒绝（Security Mode Reject）消息后，向 HSS 回复插入签约数据应答（Insert Subscriber Data Answer），则插入签约数据失败。

参见图 7，本发明实施例提供的一种 NAS 算法的通知装置，包括：

NAS 算法列表确定单元 11，用于确定 NAS 算法列表，其中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表；

通知单元 12，用于将 NAS 算法列表发送给 MME。

较佳地，通知单元 12，具体用于：

通过鉴权信息获取过程或者插入签约数据过程，将 NAS 算法列表传递给 MME。

较佳地，通知单元 12 通过鉴权信息获取过程将 NAS 算法列表传递给 MME 时，具体用于：

接收 MME 发送的鉴权信息请求（Authentication Information Request）消息；

将鉴权信息响应（Authentication Information Answer）消息发送给 MME，其中携带 NAS 算法列表。

较佳地，通知单元 12 通过插入签约数据过程，将 NAS 算法列表传递给 MME 时，具体用于：

当签约数据更新时，向 MME 发送插入签约数据请求（Insert Subscriber Data Request）消息，其中携带 NAS 算法列表。

较佳地，NAS 算法列表中的算法，按照预设优先级从高到低的顺序排列。

较佳地，本发明实施例提供的一种 NAS 算法的通知装置，为 HSS。

参见图 8，本发明实施例提供的一种 NAS 算法的获取装置，包括:

消息接收单元 21，用于接收 HSS 发送的携带有 NAS 算法列表的消息，NAS 算法列表中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表;

获取单元 22，用于从该消息中获取 NAS 算法列表。

较佳地，消息接收单元 21，具体用于:

通过鉴权信息获取过程或者插入签约数据过程，接收 HSS 发送的携带有 NAS 算法列表的消息。

较佳地，消息接收单元 21 通过鉴权信息获取过程接收 HSS 发送的携带有 NAS 算法列表的消息时，具体用于:

向 HSS 发送鉴权信息请求（Authentication Information Request）消息;

接收 HSS 发送的鉴权信息响应（Authentication Information Answer）消息，其中携带 NAS 算法列表。

较佳地，消息接收单元 21 通过插入签约数据取过程，接收 HSS 发送的携带有 NAS 算法列表的消息时，具体用于:

当签约数据更新时，接收 HSS 发送的插入签约数据请求（Insert Subscriber Data Request）消息，其中携带 NAS 算法列表。

较佳地，NAS 算法列表中的算法，按照预设优先级从高到低的顺序排列。

较佳地，该装置还包括:

选择处理单元 23，用于在获取单元 22 从消息中获取 NAS 算法列表后，从该 NAS 算法列表中选择 NAS 算法，并将选择的 NAS 算法通知给 UE。

较佳地，选择处理单元 23，具体用于:

确定 MME 支持的 NAS 加密保护算法集合 A1 和 NAS 完整性保护算法集合 A2;

确定 UE 支持的 NAS 加密保护算法集合 B1 和 NAS 完整性保护算法集合 B2;

确定 NAS 算法列表中的 NAS 加密保护算法集合 C1 和 NAS 完整性保护算法集合 C2;

确定集合 A1、B1 和 C1 的交集 D1，以及 A2、B2 和 C2 的交集 D2;

将交集 D1 中的 NAS 加密保护算法和交集 D2 中的 NAS 完整性保护算法集合通知给 UE。

较佳地:

消息接收单元 21，还用于当 NAS 算法列表更新时，从 HSS 发送的插入签约数据请求（Insert Subscriber Data Request）消息中获取更新的 NAS 算法列表;

选择处理单元 23，还用于从更新的 NAS 算法列表中重新选择 NAS 算法；当重新选择的 NAS 算法，与现有的 NAS 算法不一致时，向 UE 发送安全模式命令（Security Mode Command）

消息，其中携带重新选择的NAS算法；当重新选择的NAS算法，与现有的NAS算法一致时，或者当从更新的NAS算法列表中重新选择NAS算法的操作失败时，向HSS回复插入签约数据应答（Insert Subscriber Data Answer）消息。

较佳地，选择处理单元23，向UE发送安全模式命令（Security Mode Command）消息后，还用于：

接收UE发送的安全模式完成（Security Mode Complete）消息或者安全模式拒绝（Security Mode Reject）消息；

向HSS回复插入签约数据应答（Insert Subscriber Data Answer）消息。

较佳地，本发明实施例提供的一种NAS算法的获取装置，为MME。

综上所述，本发明实施例，在3GPP TS 29.272 协议中增加定义信息元素NAS算法列表（NAS-Algorithms-Lists），在HSS和MME之间的鉴权信息获取过程（Authentication Procedures）中传递NAS算法列表（NAS-Algorithms-Lists）。或者，在HSS和MME之间的插入签约数据过程（Insert Subscriber Data Procedure）中传递NAS算法列表（NAS-Algorithms-Lists）。从而实现了由HSS来配置NAS算法列表的策略，运营商可以通过BOSS系统来修改HSS中的用户签约数据，使得NAS安全算法和QoS等用户信息进行关联，针对不同用户的需求，可以选择不同特点的算法对NAS消息进行安全保护。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器和光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多

个方框中指定的功能的步骤。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求

1、一种非接入层 NAS 算法的通知方法，其特征在于，该方法包括:

归属签约用户服务器 HSS 确定 NAS 算法列表，其中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表;

HSS 将所述 NAS 算法列表发送给移动性管理实体 MME。

2、根据权利要求 1 所述的方法，其特征在于，所述 HSS 将所述 NAS 算法列表发送给 MME，包括:

HSS 通过鉴权信息获取过程或者插入签约数据过程，将 NAS 算法列表传递给 MME。

3、根据权利要求 2 所述的方法，其特征在于，HSS 通过鉴权信息获取过程将 NAS 算法列表传递给 MME，包括:

HSS 接收 MME 发送的鉴权信息请求 Authentication Information Request 消息;

HSS 将鉴权信息响应 Authentication Information Answer 消息发送给 MME，其中携带所述 NAS 算法列表。

4、根据权利要求 2 所述的方法，其特征在于，HSS 通过插入签约数据过程，将 NAS 算法列表传递给 MME，包括:

当签约数据更新时，HSS 向 MME 发送插入签约数据请求 Insert Subscriber Data Request 消息，其中携带所述 NAS 算法列表。

5、根据权利要求 1-4 任一权项所述的方法，其特征在于，所述 NAS 算法列表中的算法，按照预设优先级从高到低的顺序排列。

6、一种非接入层 NAS 算法的获取方法，其特征在于，该方法包括:

移动性管理实体 MME 接收归属签约用户服务器 HSS 发送的携带有 NAS 算法列表的消息，所述 NAS 算法列表中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表;

MME 从所述消息中获取 NAS 算法列表。

7、根据权利要求 6 所述的方法，其特征在于，MME 通过鉴权信息获取过程或者插入签约数据过程，接收 HSS 发送的携带有 NAS 算法列表的消息。

8、根据权利要求 7 所述的方法，其特征在于，MME 通过鉴权信息获取过程接收 HSS 发送的携带有 NAS 算法列表的消息，包括:

MME 向 HSS 发送鉴权信息请求 Authentication Information Request 消息;

MME 接收 HSS 发送的鉴权信息响应 Authentication Information Answer 消息，其中携带所述 NAS 算法列表。

9、根据权利要求 7 所述的方法，其特征在于，MME 通过插入签约数据过程，接收 HSS 发送的携带有 NAS 算法列表的消息，包括:

当签约数据更新时，MME 接收 HSS 发送的插入签约数据请求 Insert Subscriber Data

Request 消息，其中携带所述 NAS 算法列表。

10、根据权利要求 6-9 任一权项所述的方法，其特征在于，所述 NAS 算法列表中的算法，按照预设优先级从高到低的顺序排列。

11、根据权利要求 6-9 任一权项所述的方法，其特征在于，MME 从所述消息中获取 NAS 算法列表后，该方法还包括:

MME 从所述 NAS 算法列表中选择 NAS 算法，并将选择的 NAS 算法通知给用户设备 UE。

12、根据权利要求 11 所述的方法，其特征在于，MME 从所述 NAS 算法列表中选择 NAS 算法，将选择的 NAS 算法通知给 UE，包括:

MME 确定自身支持的 NAS 加密保护算法集合 A1 和 NAS 完整性保护算法集合 A2;

MME 确定 UE 支持的 NAS 加密保护算法集合 B1 和 NAS 完整性保护算法集合 B2;

MME 确定所述 NAS 算法列表中的 NAS 加密保护算法集合 C1 和 NAS 完整性保护算法集合 C2;

MME 确定集合 A1、B1 和 C1 的交集 D1，以及 A2、B2 和 C2 的交集 D2;

MME 将交集 D1 中的 NAS 加密保护算法和交集 D2 中的 NAS 完整性保护算法集合通知给 UE。

13、根据权利要求 12 所述的方法，其特征在于，该方法还包括:

当 NAS 算法列表更新时，MME 从 HSS 发送的插入签约数据请求 Insert Subscriber Data Request 消息中获取更新的 NAS 算法列表;

MME 从更新的 NAS 算法列表中重新选择 NAS 算法;

当重新选择的 NAS 算法，与现有的 NAS 算法不一致时，MME 向 UE 发送安全模式命令 Security Mode Command 消息，其中携带重新选择的 NAS 算法;

当重新选择的 NAS 算法，与现有的 NAS 算法一致时，或者当 MME 从更新的 NAS 算法列表中重新选择 NAS 算法的操作失败时，MME 向 HSS 回复插入签约数据应答 Insert Subscriber Data Answer 消息。

14、根据权利要求 13 所述的方法，其特征在于，MME 向 UE 发送安全模式命令 Security Mode Command 消息后，该方法还包括:

MME 接收 UE 发送的安全模式完成 Security Mode Complete 消息或者安全模式拒绝 Security Mode Reject 消息;

MME 向 HSS 回复插入签约数据应答 Insert Subscriber Data Answer 消息。

15、一种非接入层 NAS 算法的通知装置，其特征在于，该装置包括:

NAS 算法列表确定单元，用于确定 NAS 算法列表，其中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表;

通知单元，用于将所述 NAS 算法列表发送给移动性管理实体 MME。

16、根据权利要求 15 所述的装置，其特征在于，所述通知单元，具体用于：

通过鉴权信息获取过程或者插入签约数据过程，将 NAS 算法列表传递给 MME。

17、根据权利要求 16 所述的装置，其特征在于，所述通知单元通过鉴权信息获取过程将 NAS 算法列表传递给 MME 时，具体用于：

接收 MME 发送的鉴权信息请求 Authentication Information Request 消息；

将鉴权信息响应 Authentication Information Answer 消息发送给 MME，其中携带所述 NAS 算法列表。

18、根据权利要求 16 所述的装置，其特征在于，所述通知单元通过插入签约数据过程，将 NAS 算法列表传递给 MME 时，具体用于：

当签约数据更新时，向 MME 发送插入签约数据请求 Insert Subscriber Data Request 消息，其中携带所述 NAS 算法列表。

19、一种非接入层 NAS 算法的获取装置，其特征在于，该装置包括：

消息接收单元，用于接收归属签约用户服务器 HSS 发送的携带有 NAS 算法列表的消息，所述 NAS 算法列表中包括 NAS 加密保护算法列表和 NAS 完整性保护算法列表；

获取单元，用于从所述消息中获取 NAS 算法列表。

20、根据权利要求 19 所述的装置，其特征在于，所述消息接收单元，具体用于：

通过鉴权信息获取过程或者插入签约数据过程，接收 HSS 发送的携带有 NAS 算法列表的消息。

21、根据权利要求 20 所述的装置，其特征在于，所述消息接收单元通过鉴权信息获取过程接收 HSS 发送的携带有 NAS 算法列表的消息时，具体用于：

向 HSS 发送鉴权信息请求 Authentication Information Request 消息；

接收 HSS 发送的鉴权信息响应 Authentication Information Answer 消息，其中携带所述 NAS 算法列表。

22、根据权利要求 20 所述的装置，其特征在于，所述消息接收单元通过插入签约数据过程，接收 HSS 发送的携带有 NAS 算法列表的消息时，具体用于：

当签约数据更新时，接收 HSS 发送的插入签约数据请求 Insert Subscriber Data Request 消息，其中携带所述 NAS 算法列表。

23、根据权利要求 19-22 任一权项所述的装置，其特征在于，该装置还包括：

选择处理单元，用于在所述获取单元从所述消息中获取 NAS 算法列表后，从所述 NAS 算法列表中选择 NAS 算法，并将选择的 NAS 算法通知给用户设备 UE。

24、根据权利要求 23 所述的装置，其特征在于，所述选择处理单元，具体用于：

确定 MME 支持的 NAS 加密保护算法集合 A1 和 NAS 完整性保护算法集合 A2；

确定 UE 支持的 NAS 加密保护算法集合 B1 和 NAS 完整性保护算法集合 B2；

确定所述NAS算法列表中的NAS加密保护算法集合C1和NAS完整性保护算法集合C2;

确定集合A1、B1和C1的交集D1，以及A2、B2和C2的交集D2;

将交集D1中的NAS加密保护算法和交集D2中的NAS完整性保护算法集合通知给UE。

25、根据权利要求24所述的装置，其特征在于，

所述消息接收单元，还用于当NAS算法列表更新时，从HSS发送的插入签约数据请求Insert Subscriber Data Request消息中获取更新的NAS算法列表;

所述选择处理单元，还用于从更新的NAS算法列表中重新选择NAS算法；当重新选择的NAS算法，与现有的NAS算法不一致时，向UE发送安全模式命令Security Mode Command消息，其中携带重新选择的NAS算法；当重新选择的NAS算法，与现有的NAS算法一致时，或者当从更新的NAS算法列表中重新选择NAS算法的操作失败时，向HSS回复插入签约数据应答Insert Subscriber Data Answer消息。

26、根据权利要求25所述的装置，其特征在于，所述选择处理单元，向UE发送安全模式命令Security Mode Command消息后，还用于:

接收UE发送的安全模式完成Security Mode Complete消息或者安全模式拒绝Security Mode Reject消息;

向HSS回复插入签约数据应答Insert Subscriber Data Answer消息。

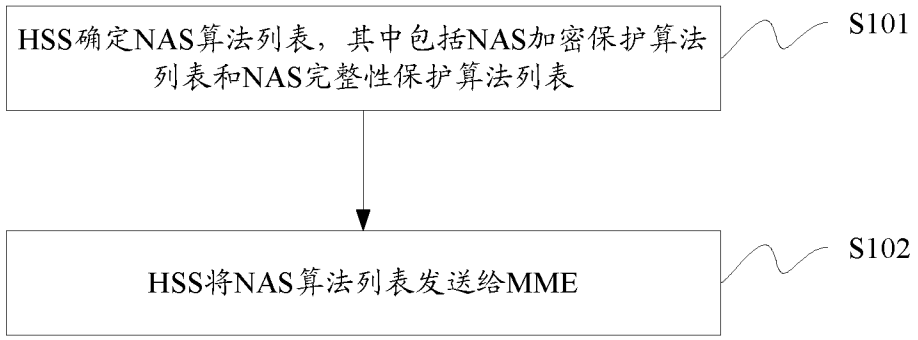
HSS确定NAS算法列表，其中包括NAS加密保护算法列表和NAS完整性保护算法列表
S101
HSS将NAS算法列表发送给MME
S102

图 1

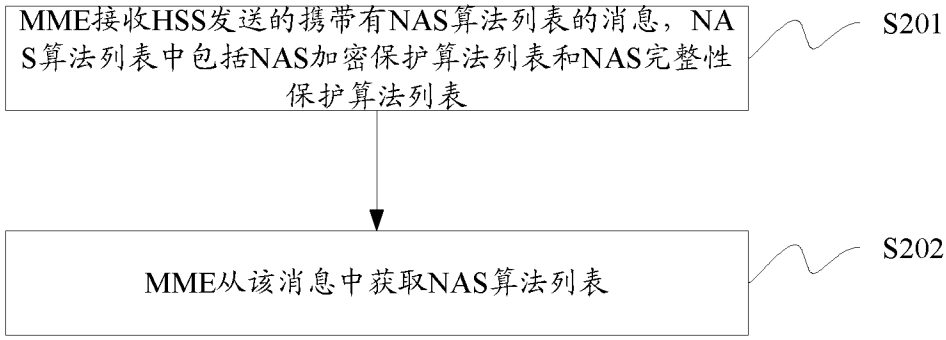
MME接收HSS发送的携带有NAS算法列表的消息，NAS算法列表中包括NAS加密保护算法列表和NAS完整性保护算法列表
S201
MME从该消息中获取NAS算法列表
S202

图 2


MME
HSS
鉴权信息请求（Authentication Information Request）
鉴权信息响应（Authentication Information Answer）

图 3


MME
HSS
插入签约数据请求（Insert Subscriber Data Request）
插入签约数据应答（Insert Subscriber Data Answer）

图 4

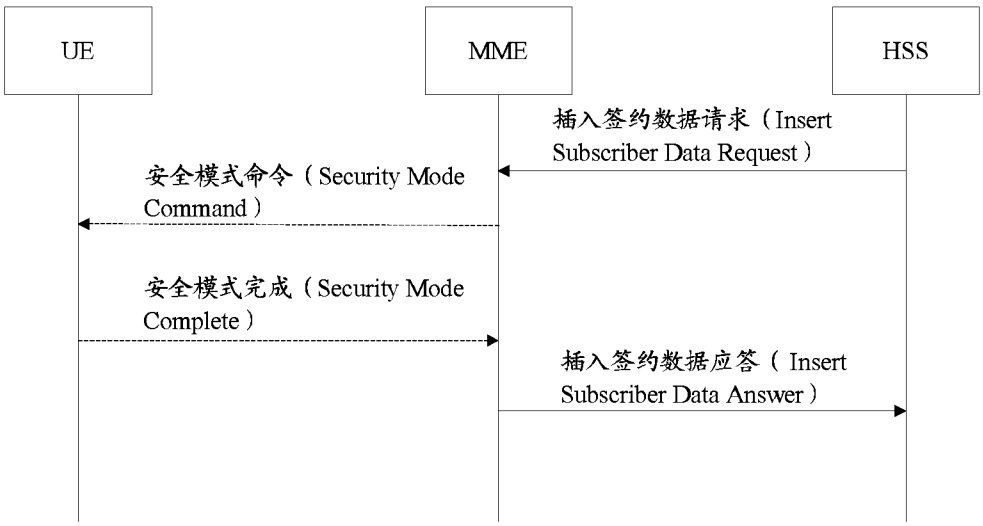
UE
MME
HSS
插入签约数据请求（Insert Subscriber Data Request）
安全模式命令（Security Mode Command）
安全模式完成（Security Mode Complete）
插入签约数据应答（Insert Subscriber Data Answer）

图 5

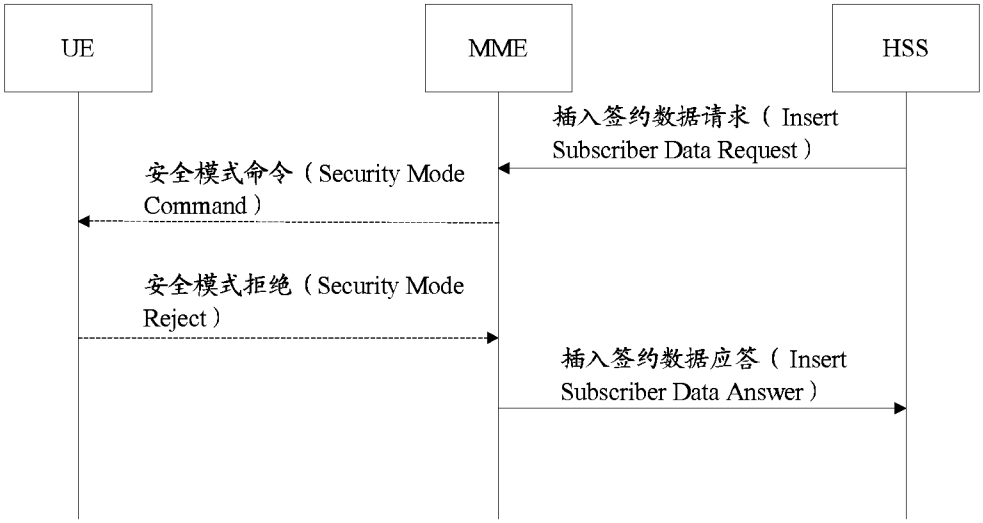
UE
MME
HSS
插入签约数据请求（ Insert Subscriber Data Request ）
安全模式命令（ Security Mode Command ）
安全模式拒绝（ Security Mode Reject ）
插入签约数据应答（ Insert Subscriber Data Answer ）

图 6

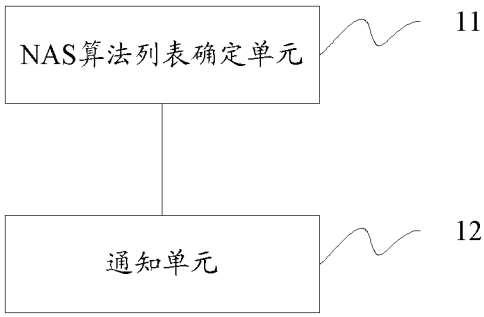
NAS算法列表确定单元
11
通知单元
12

图 7

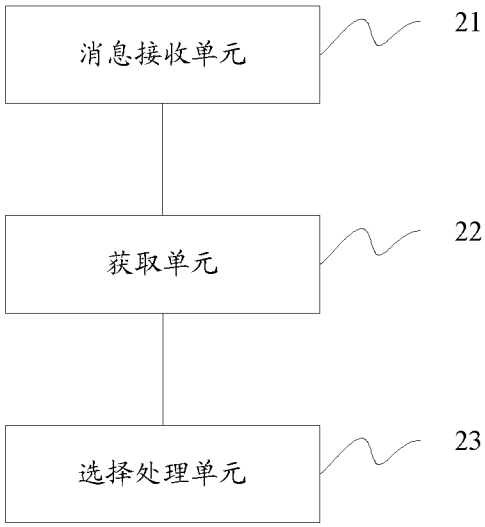

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/084314

A. CLASSIFICATION OF SUBJECT MATTER

See the 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: H04W, H04L

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)

CNABS, CNTXT: home subscriber server, non-access stratum, algorithm
VEN: HSS, NAS, algorithm

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 102595369 (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.), 18 July 2012 (18.07.2012), claims 1-28, and description, paragraphs 1-163	1-26
Y	CN 102256234 A (ACADEMY OF TELECOMMUNICATION TECHNOLOGY), 23 November 2011 (23.11.2011), see description, paragraphs 5-7, 60, 137, 138 and 157	1-26
Y	CN 101262337 A (ZTE CORP.), 10 September 2008 (10.09.2008), see description, page 2, lines 8-23, and page 9, lines 10-19	1-26
Y	CN 102083064 A (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.), 01 June 2011 (01.06.2011), see description, paragraph 38, and figures 5 and 7	1-26
Y	CN 101605324 A (HUAWEI TECHNOLOGIES CO., LTD.), 16 December 2009 (16.12.2009), see description, page 4, line 25 to page 5, line 15	1-26

☐ 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
02 February 2013 (02.02.2013)	**28 February 2013 (28.02.2013)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **JIANG, Jingjing** Telephone No.: (86-10) **62411430**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/084314

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102595369 A	18.07.2012	None	
CN 102256234 A	23.11.2011	None	
CN 101262337 A	10.09.2008	CN 101262337 B	06.06.2012
CN 102083064 A	01.06.2011	None	
CN 101605324 A	16.12.2009	CN 101605324 B	01.06.2011
		WO 2009149666 A1	17.12.2009

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2012/084314

CONTINUATION OF SECOND SHEET:

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06 (2009.01) i

H04W 12/10 (2009.01) i

国际检索报告

国际申请号
PCT/CN2012/084314

A. 主题的分类

见附加页

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:H04W,H04L

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）)

CNABS,CNTXT::归属地用户服务器，非接入层，算法

VEN:HSS, NAS, algorithm

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	CN102595369 (大唐移动通信设备有限公司) 18.7 月 2012（18.07.2012）权利要求 1-28，说明书第 1-163 段	1-26
Y	CN102256234A(电信科学技术研究院)23.11 月 2011（23.11.2011）见说明书第 5-7，60，137，138，157 段	1-26
Y	CN101262337A(中兴通讯股份有限公司)10.9 月 2008（10.09.2008）见说明书第 2 页第 8-23 行，第 9 页第 10-19 行	1-26
Y	CN102083064A(大唐移动通信设备有限公司)01.6 月 2011（01.06.2011）见说明书第 38 段以及图 5，图 7	1-26
Y	CN101605324A(华为技术有限公司)16.12 月 2009（16.12.2009）见说明书第 4 页第 25 行-第 5 页第 15 行	1-26

☐ 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	国际检索报告邮寄日期
02.2 月 2013（02.02.2013）	**28.2 月 2013 (28.02.2013)**
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	受权官员 江婧敬 电话号码：(86-10) **62411430**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2012/084314

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN102595369A	18.07.2012	无	
CN102256234A	23.11.2011	无	
CN101262337A	10.09.2008	CN101262337B	06.06.2012
CN102083064A	01.06.2011	无	
CN101605324A	16.12.2009	CN101605324B	01.06.2011
		WO2009149666A1	17.12.2009

续：第 2 页

A. 主题的分类

H04W12/06 (2009.01)i

H04W12/10 (2009.01)i