

(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
2010 年 11 月 11 日 (11.11.2010)

PCT

(10) 国际公布号
WO 2010/127592 A1

- (51) 国际专利分类号:
H04W 4/22 (2009.01) H04W 76/02 (2009.01)
- (21) 国际申请号: PCT/CN2010/072081
- (22) 国际申请日: 2010 年 4 月 22 日 (22.04.2010)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
200910083358.4 2009 年 5 月 4 日 (04.05.2009) 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): **徐建华 (XU, Jianhua)** [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)。 **甘露 (GAN, Lu)** [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)。 **张旭武 (ZHANG, Xuwu)** [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: 北京派特恩知识产权代理事务所(普通合伙) (CHINA PAT INTELLECTUAL PROPERTY OFFICE); 中国北京市海淀区知春路 113 号 0717 室, Beijing 100086 (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 (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)。
- 本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

[见续页]

(54) Title: EMERGENCY CALL-BASED SECURITY ALGORITHM NEGOTIATION METHOD AND APPARATUS

(54) 发明名称: 基于紧急呼叫的安全算法协商方法与装置

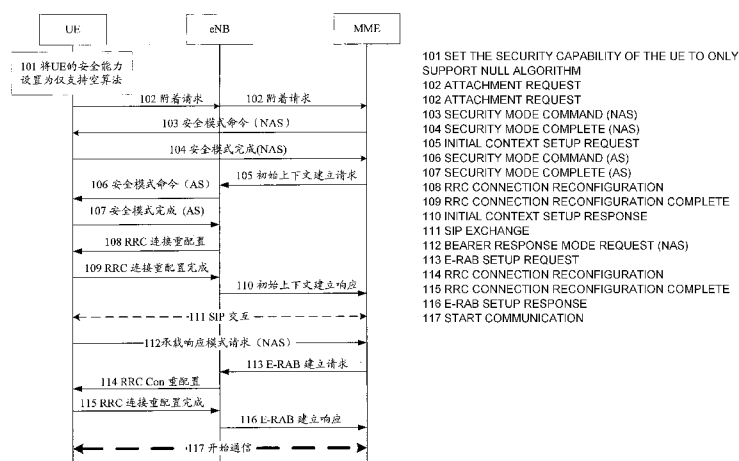


图 1 / Fig. 1

(57) Abstract: An emergency call-based security algorithm negotiation method and apparatus are disclosed. The method involves the following steps: after receiving an attachment request from a user terminal, the network side determines that the attachment request is an emergency attachment request, then sets the security capability of the user terminal to support a null algorithm only; or the network side determines that the security capability of the user terminal carried in the attachment request supports the null algorithm only, then performs non-access stratum (NAS) and access stratum (AS) security negotiation with the user terminal using the null algorithm. A mobility management entity (MME) and an evolved Node-B (eNB) can perform a security negotiation directly on the basis that the user terminal only supports the null algorithm when the NAS and AS security negotiation is performed.

[见续页]

(57) 摘要:

公开了一种基于紧急呼叫的安全算法协商方法与装置。该方法包括：网络侧接收用户终端的附着请求后，确定所述附着请求为紧急附着请求，设置所述用户终端的安全能力为仅支持空算法，或者，确定所述附着请求中所携带的所述用户终端安全能力为仅支持空算法，以空算法与所述用户终端进行非接入层及接入层的安全协商处理。移动管理实体（MME）及演进的基站（eNB）在进行非接入层及接入层的安全协商时，直接以用户终端仅支持空算法为基础进行安全协商即可。

基于紧急呼叫的安全算法协商方法与装置

技术领域

本发明涉及移动网络中的紧急呼叫技术，尤其涉及一种移动网络中基于紧急呼叫的安全算法协商方法与装置。

5 背景技术

算法生成非接入层完整性保护密钥 K_{NASint} 。移动管理实体（MME，Mobility Management）将 K_{NASenc} 及 K_{NASint} 通知用户终端（UE，User Equipment），UE 利用 MME 所通知的密钥对所接收到的非接入层消息进行安全解析。

10 供演进的基站（eNB）使用的接入层的根密钥是演进的基站密钥（Key eNB） K_{eNB} 。MME 使用 K_{ASME} 和非接入层上行计数器生成 K_{eNB} ，并将 K_{eNB} 通知 eNB。eNB 使用 K_{eNB} 及为 UE 所选择的无线资源控制（RRC，Radio Resource Control）加密算法生成 RRC 加密密钥 K_{RRCenc} ，使用 K_{eNB} 及为 UE 所选择的 RRC 完整性保护算法生成 RRC 完整性保护密钥 K_{RRCint} ，使用 K_{eNB}
15 及所选择的 UP 加密算法生成 K_{UPenc} 。

上述的非接入层及非接入层的安全协商处理是对正常呼叫设计的，对于紧急呼叫，原则上也以上述安全协商处理方式进行安全协商处理，但由于紧急呼叫是一类特殊的呼叫通信，即使用户终端处于服务受限状态，同样也支持紧急呼叫；如在不正常通信信号情况下，用户终端也支持 112 的
20 呼叫；在用户终端没有用户身份识别卡的情况下，也支持 110、119 等紧急呼叫。紧急呼叫情况下，UE 与通信网络之间如按正常的呼叫那样进行安全认证，可能会影响紧急呼叫的接通成功率。目前并没有处理紧急呼叫情况下的安全协商处理的技术方案。

发明内容

有鉴于此，本发明的主要目的在于提供一种基于紧急呼叫的安全算法协商方法与装置，能提升紧急呼叫的接入效率及接通率。

为达到上述目的，本发明的技术方案是这样实现的：

5 一种基于紧急呼叫的安全算法协商方法，包括：

网络侧接收到用户终端的附着请求后，确定所述附着请求为紧急附着请求，设置所述用户终端的安全能力为仅支持空算法；或者，网络侧确定附着请求中所携带的所述用户终端安全能力为仅支持空算法；以及

以空算法与所述用户终端进行非接入层及接入层的安全协商处理。

10 优选地，所述以空算法与所述用户终端进行非接入层的安全协商处理，具体为：

网络侧的 MME 向所述用户终端发送非接入层的安全模式命令，所述非接入层的安全模式命令中携带以空算法作为非接入层安全算法的指示信息。

15 优选地，所述以空算法与所述用户终端进行接入层的安全协商处理，具体为：

网络侧的 MME 确定演进基站 eNB 所使用的接入层的根密钥 K_{eNB} ，并与所述用户终端的安全能力信息一起通知所述 eNB；以及

20 所述 eNB 根据所述用户终端的安全能力信息确定所述用户终端仅支持空算法，向所述用户终端发送接入层的安全模式命令，所述接入层的安全模式命令中携带以空算法作为接入层安全算法的指示信息。

优选地，所述确定 eNB 所使用的接入层的根密钥 K_{eNB} ，具体为：

所述 MME 确定 UE 附着为紧急附着时，随机生成所述 eNB 使用的接入层的根密钥 K_{eNB} ，并通知所述 eNB。

25 优选地，附着请求中携带所述用户终端安全能力信息，具体为：

用户终端确定当前呼叫请求为紧急呼叫请求时，将所述附着请求中的所述用户终端的安全能力信息标识为仅支持空算法。

优选地，所述方法还包括：

源 eNB 发起基于 X2 接口的切换时，所述源 eNB 将自身所存储的所述
5 用户终端当前的安全能力信息即仅支持空算法通知目标 eNB；以及

所述目标 eNB 在切换响应消息中承载有接入层使用空算法作为安全算法的标识信息。

优选地，所述方法还包括：

源 eNB 发起基于 S1 接口的切换时，MME 将自身所存储的所述用户终
10 端当前的安全能力信息即仅支持空算法通知目标 eNB；以及

所述目标 eNB 在切换响应消息中承载有接入层使用空算法作为安全算法的标识信息。

一种基于紧急呼叫的安全算法协商装置，包括：

第一确定单元，用于确定当前呼叫请求是否为紧急呼叫请求，是时触
15 发生成单元；

生成单元，用于为所述紧急呼叫生成附着请求，并将所述附着请求中的发起呼叫的用户终端的安全能力信息标识为仅支持空算法；

发送单元，用于发送所述附着请求；

接收单元，用于接收所述发送单元所发送的附着请求；

20 第二确定单元，用于确定所述附着请求中所携带的所述用户终端安全能力信息是否为仅支持空算法，是时触发安全协商处理单元；以及

安全协商处理单元，用于以空算法与所述用户终端进行非接入层及接入层的安全协商处理。

优选地，所述安全协商处理单元包括第一发送模块，用于在所述第二
25 确定单元确定所述用户终端仅支持空算法时，向所述用户终端发送非接入

层的安全模式命令，所述非接入层的安全模式命令中携带以空算法作为非接入层安全算法的指示信息。

优选地，所述安全协商处理单元还包括：

确定模块，用于确定演进基站 eNB 所使用的接入层的根密钥 K_{eNB} ；

5 通知模块，用于将所述确定模块所确定的所述根密钥 K_{eNB} 与所述用户终端的安全能力信息一起通知所述 eNB；以及

第二发送模块，用于在所述 eNB 确定所述用户终端仅支持空算法时，向所述用户终端发送接入层的安全模式命令，所述接入层的安全模式命令中携带以空算法作为接入层安全算法的指示信息。

10 一种基于紧急呼叫的安全算法协商装置，包括：

接收单元，用于接收用户终端的附着请求；

确定单元，用于确定所述附着请求是否为紧急附着请求，是时触发设置单元；

设置单元，用于设置所述用户终端的安全能力为仅支持空算法；以及

15 安全协商处理单元，用于以空算法与所述用户终端进行非接入层及接入层的安全协商处理。

优选地，所述安全协商处理单元包括第一发送模块，用于在所述设置单元设置所述用户终端仅支持空算法时，向所述用户终端发送非接入层的安全模式命令，所述非接入层的安全模式命令中携带以空算法作为非接入层安全算法的指示信息。

20 优选地，所述安全协商处理单元还包括：

确定模块，用于确定演进基站 eNB 所使用的接入层的根密钥 K_{eNB} ；

通知模块，用于将所述确定模块所确定的所述根密钥 K_{eNB} 与所述用户终端的安全能力信息一起通知所述 eNB；以及

25 第二发送模块，用于在所述 eNB 确定所述用户终端仅支持空算法时，

向所述用户终端发送接入层的安全模式命令，所述接入层的安全模式命令中携带以空算法作为接入层安全算法的指示信息。

本发明的用户终端在确定用户当前的呼叫为紧急呼叫时，在附着请求中将用户终端的安全能力信息标识为仅支持空算法，或者，网络侧（即 MME）在接收到用户终端的紧急呼叫的附着请求后，确定当前的附着请求为紧急附着请求，将用户终端的安全能力设置为仅支持空算法，这样，MME 及 eNB 在进行非接入层及接入层的安全协商时，直接以用户终端仅支持空算法进行安全协商即可，提升了紧急呼叫的接入效率，同时也提高了紧急呼叫的呼通率。本发明实现简单且实用。

10 附图说明

图 1 为本发明基于紧急呼叫的安全算法协商方法实施例一的流程图；

图 2 为本发明基于紧急呼叫的安全算法协商方法实施例二的流程图；

图 3 为本发明基于紧急呼叫的安全算法协商方法实施例三的流程图；

图 4 为本发明基于紧急呼叫的安全算法协商方法实施例四的流程图；

15 图 5 为本发明基于紧急呼叫的安全算法协商装置实施例一的组成结构示意图；

图 6 为本发明基于紧急呼叫的安全算法协商装置实施例二的组成结构示意图。

具体实施方式

20 本发明的基本思想是：用户终端在确定用户当前的呼叫为紧急呼叫时，在附着请求中将用户终端的安全能力信息标识为仅支持空算法，或者，网络侧（即 MME）在接收到用户终端的紧急呼叫的附着请求后，确定当前的附着请求为紧急附着请求，将用户终端的安全能力设置为仅支持空算法，这样，MME 及 eNB 在进行非接入层及接入层的安全协商时，直接以用户

终端仅支持空算法进行安全协商即可，提升了紧急呼叫的接入效率，同时也提高了紧急呼叫的呼通率。本发明实现简单且实用。

为使本发明的目的、技术方案和优点更加清楚明白，以下举实施例并参照附图，对本发明进一步详细说明。

5 实施例一

图 1 为本发明基于紧急呼叫的安全算法协商方法实施例一的流程图，如图 1 所示，本示例基于紧急呼叫的安全算法协商方法包括以下步骤：

101: UE 确定当前用户所发起的呼叫请求为紧急呼叫请求时，将 UE 的安全能力设置为仅支持空算法。

10 本发明步骤 101 中，UE 一旦确定用户所请求的呼叫为紧急呼叫，即把安全能力设置为仅支持空算法，无论 UE 是否处于受限服务状态。

102: UE 向网络侧发送附着请求（Attach Req）消息，Attach Req 消息中的演进的分组系统附着类型（EPS Attach Type）项设置为演进的分组系统紧急附着（EPS Emergency Attach），其中的用户终端网络能力（UE Network
15 Capability）项中包括 UE 的安全能力（仅支持空算法）。网络侧是指 eNB 及 MME 等网元。

103: MME 根据 UE 的安全能力，选择空算法，向 UE 发起非接入层的安全模式命令（Security Mode Command），Security Mode Command 中携带以空算法作为非接入层安全算法的指示信息。MME 确定 UE 的安全能力为
20 仅支持空算法，则 MME 与 UE 之间的非接入层的消息中将不再进行加密及完整性保护处理，并通过 Security Mode Command 通知 UE 非接入层的安全算法为空算法。

104: UE 接收到 Security Mode Command 消息后，给 MME 回应安全模式完成（Security Mode Complete）消息，向 MME 确认安全模式配置生效。

25 105: MME 生成初始上下文建立请求（INITIAL CONTEXT SETUP

REQUEST) 消息, 并发送给 eNB, 消息中的用户终端安全能力 (UESecurityCapabilities) 项, 根据步骤 102 中的 Attach 请求中的 UE Network Capability 的信息填写为仅支持空算法, 根据用于传输会话初始协议 (SIP, Session initiation protocol) 信令的服务质量 (QoS, Quality of Service) 需求
5 填写演进无线接入承载待建立列表 (E-RAB to Be Setup List)。INITIAL CONTEXT SETUP REQUEST 消息中还包括 MME 为 eNB 随机生成的 eNB 所使用的接入层的根密钥 KeNB。

106: eNB 根据 UESecurityCapabilities, 确定 UE 仅支持空算法, 向 UE 发起 AS 的 Security Mode Command。Security Mode Command 中携带以空
10 算法作为接入层安全算法的指示信息。eNB 确定 UE 的安全能力为仅支持空算法, 则 eNB 与 UE 之间的接入层的消息中将不再进行加密及完整性保护处理, 通过 AS 的 Security Mode Command 通知 UE 接入层的消息所使用的安全算法为空算法。

107: UE 给 eNB 回应 AS 的 Security Mode Complete 消息。

15 108: eNB 根据 E-RAB to Be Setup List 配置相应的空口承载, 向 UE 发送 RRC 连接重配置 (RRCConnectionReconfiguration) 消息。

109: UE 根据 RRCConnectionReconfiguration 建立空口承载资源, 然后给 eNB 响应 RRC 连接重配置完成 (RRCConnectionReconfigurationComplete) 消息。

20 110: eNB 给 MME 回应初始上下文建立响应 (INITIAL CONTEXT SETUP RESPONSE) 消息。

111: UE 通过默认承载向 IP 多媒体子系统 (IMS, IP Multimedia Subsystem) 服务器发起 SIP 注册过程, 成功后向 IMS 服务器发起紧急呼叫信令流程, 流程结束后会和目标交换双方媒体面传输层地址, 协商出双方
25 使用的编解码格式等参数。

112: UE 根据协调出的编解码格式等参数, 转化为 QoS 需求, 向 MME 发起承载资源修改 (Bearer Resource Modification Request) 消息, 请求建立专用承载, 用于传输媒体流。

113: MME 根据 Bearer Resource Modification Request 消息中的 QoS 参数, 生成演进无线接入承载建立请求 (E-RAB SETUP REQUEST) 消息, 发给 eNB。

114: eNB 向 UE 发送 RRCConnectionReconfiguration 消息, 包括专用承载的资源配置。

115: UE 向 eNB 回应 RRCConnectionReconfigurationComplete 消息后, 专用承载建立成功。

116: eNB 向 MME 回应 E-RAB SETUP RESPONSE 消息。

117: 用于媒体流传输的专用承载建立成功, UE 与目标开始通话。

实施例二

图 2 为本发明基于紧急呼叫的安全算法协商方法实施例二的流程图, 如图 2 所示, 本示例基于紧急呼叫的安全算法协商方法包括以下步骤:

201: UE 向网络侧发送 Attach Req 消息, Attach Req 消息中 Eps Attach Type 项设置为 Eps Emergency Attach, 其中的 UE Network Capability 项填写为 UE 的真实安全能力, 即 UE 正常情况下的安全能力以及 UE 在受限服务情况下的安全能力。

202: MME 无视 UE 上报的安全能力, 直接将 UE 安全能力设置为仅支持空算法。

203: MME 根据 UE 安全能力, 选择空算法, 向 UE 发起 NAS 的 Security Mode Command。Security Mode Command 中携带以空算法作为非接入层安全算法的指示信息。

204: UE 给 MME 回应 Security Mode Complete 消息, 且在紧急附着场

景下 UE 不对 MME 返回的 UE 安全能力作检查。

205: MME 生成 INITIAL CONTEXT SETUP REQUEST 消息, 并发给 eNB, 消息中的 UESecurityCapabilities 填写为仅支持空算法, 根据用于传输 SIP 信令的 QoS 需求填写 E-RAB to Be Setup List。INITIAL CONTEXT
5 SETUP REQUEST 消息中还包括 MME 为 eNB 随机生成的 eNB 所使用的接入层的根密钥 KeNB。

步骤 206 至步骤 217 与前述步骤 106 至步骤 217 的实现方式完全相同, 这里不再赘述。

实施三

10 图 3 为本发明基于紧急呼叫的安全算法协商方法实施例三的流程圖, 如图 3 所示, 本示例基于紧急呼叫的安全算法协商方法包括以下步骤:

301: UE 上报测量报告, 报告中携带符合要求的目标小区 ID。

302: 源 eNB 根据目标小区 ID, 发起基于 X2 口的切换, 向目标 eNB 发送切换请求 (HANDOVER REQUEST), 请求中携带 UE Security
15 Capabilities (仅支持空算法)。

303: 目标 eNB 根据从源侧发送的 UE Security Capabilities, 选择空算法作为 AS 的安全算法。

304: 目标 eNB 根据所选的安全算法及业务参数, 生成 RRCConnectionReconfiguration 消息, RRCConnectionReconfiguration 消息中
20 包括切换相关的信元, 封装在切换请求确认 (HANDOVER REQUEST ACKNOWLEDGE) 消息中发给源 eNB。RRCConnectionReconfiguration 消息中还包括 AS 消息所使用的安全算法为空算法的指示信息。

305: 源基站从 HANDOVER REQUEST ACKNOWLEDGE 消息中提取出 RRC 消息内容, 发送给 UE。

25 306: UE 到目标小区进行接入, 发送

RRCCONNECTIONReconfigurationComplete 消息给目标 eNB

307: 目标 eNB 向 MME 发送路径变换请求 (PATH SWITCH REQUEST) 消息。

308: MME 向目标 eNB 回应路径变换请求确认 (PATH SWITCH
5 REQUEST ACKNOWLEDGE) 消息。

309: 目标 eNB 向源 eNB 发送用户终端上下文释放 (UE CONTEXT RELEASE) 消息。

310: 源 eNB 释放 UE 上下文

实施例四

10 图 4 为本发明基于紧急呼叫的安全算法协商方法实施例四的流程图，
如图 4 所示，本示例基于紧急呼叫的安全算法协商方法包括以下步骤：

401: UE 上报测量报告，报告中携带符合要求的目标小区 ID。

402: 源 eNB 根据目标小区 ID，发起基于 S1 口的切换，向 MME 发送
HANDOVER REQUIRED。

15 403: MME 上保存有仅支持空算法的 UE Security Capabilities，向目标
eNB 发送 HANDOVER REQUEST 请求，携带 UE Security Capabilities (仅
支持空算法)。

404: 目标 eNB 根据从 MME 发送的 UE Security Capabilities，选择空
算法作为 AS 的安全算法。

20 405: 目标 eNB 根据所选的算法及业务参数，生成
RRCCONNECTIONReconfiguration 消息，RRCCONNECTIONReconfiguration 消息中
包括切换相关的信元，封装在 HANDOVER REQUEST ACKNOWLEDGE 消
息中发给 MME。RRCCONNECTIONReconfiguration 消息中还包括 AS 消息所使
用的安全算法为空算法的指示信息。

25 406: MME 生成切换命令 (HANDOVER COMMAND)，携带目标 eNB

传入的 RRC 消息，发送给源 eNB。

407: 源 eNB 从 HANDOVER COMMAND 中提取出 RRC 消息内容，发送给 UE。

408 : UE 到目标小区进行接入，发送
5 RRCConnectionReconfigurationComplete 消息给目标 eNB。

409: 目标 eNB 向 MME 发送 HANDOVER NOTIFY。

410: MME 向源 eNB 发送 UE CONTEXT RELEASE COMMAND，通知其释放源 eNB 的 UE 上下文。

411: 源 eNB 发起 UE 上下文释放。

10 图 5 为本发明基于紧急呼叫的安全算法协商装置实施例一的组成结构示意图，如图 5 所示，本示例基于紧急呼叫的安全协商装置包括第一确定单元 50、生成单元 51、发送单元 52、接收单元 53、第二确定单元 54 和安全协商处理单元 55，其中，第一确定单元 50 用于确定当前呼叫请求是否为紧急呼叫请求，是时触发生成单元 51；生成单元 51 用于为所述紧急呼叫生
15 成附着请求，并将所述附着请求中的发起呼叫的用户终端的安全能力信息标识为仅支持空算法；发送单元 52 用于发送所述附着请求；接收单元 53 用于接收发送单元 52 所发送的附着请求；第二确定单元 54 用于确定所述附着请求中所携带的所述用户终端安全能力信息是否为仅支持空算法，是时触发安全协商处理单元 55；安全协商处理单元 55 用于以空算法与所述用
20 户终端进行非接入层及接入层的安全协商处理。其中，安全协商处理单元 55 包括第一发送模块，用于在第二确定单元 54 确定所述用户终端仅支持空算法时，向所述用户终端发送非接入层的安全模式命令，所述非接入层的安全模式命令中携带以空算法作为非接入层安全算法的指示信息。安全协商处理单元还包括：确定模块、通知模块和第二发送模块，确定模块用于
25 确定演进基站 eNB 所使用的接入层的根密钥 KeNB；通知模块用于将所述

确定模块所确定的所述 eNB 所使用的接入层的根密钥 KeNB 与所述用户终端的安全能力信息一起通知所述 eNB；第二发送模块用于在所述 eNB 确定所述用户终端仅支持空算法时，向所述用户终端发送接入层的安全模式命令中携带以空算法作为非接入层安全算法的指示信息。

5 本领域技术人员应当理解，本发明图 5 所示的基于紧急呼叫的安全算法协商装置是为实现图 1 所示的基于紧急呼叫的安全算法协商方法而设计的，图 5 所示装置中的各处理单元的实现功能可参照图 1 所示的方法中的相关描述而理解，各单元的功能可通过运行于处理器上的程序而实现，也可通过相应的逻辑电路而实现。

10 图 6 为本发明基于紧急呼叫的安全算法协商装置实施例二的组成结构示意图，如图 6 所示，本示例基于紧急呼叫的安全算法协商装置包括接收单元 60、确定单元 61、设置单元 62 和安全协商处理单元 63，其中，接收单元 60 用于接收用户终端的附着请求；确定单元 61 用于确定所述附着请求是否为紧急附着请求，是时触发设置单元 62；设置单元 62 用于设置所述
15 用户终端的安全能力为仅支持空算法；安全协商处理单元 63 用于以空算法与所述用户终端进行非接入层及接入层的安全协商处理。

安全协商处理单元 63 包括第一发送模块，用于在设置单元 62 设置所述用户终端仅支持空算法时，向所述用户终端发送非接入层的安全模式命令，所述非接入层的安全模式命令中携带以空算法作为非接入层安全算法
20 的指示信息。安全协商处理单元 63 还包括确定模块、通知模块和第二发送模块，其中，确定模块用于确定演进基站 eNB 所使用的接入层的根密钥 KeNB；通知模块用于将所述确定模块所确定的所述 eNB 所使用的接入层的根密钥 KeNB 与所述用户终端的安全能力信息一起通知所述 eNB；第二发送模块用于在所述 eNB 确定所述用户终端仅支持空算法时，向所述用户终端
25 发送接入层的安全模式命令，所述非接入层的安全模式命令中携带以空

算法作为非接入层安全算法的指示信息。

本领域技术人员应当理解，本发明图 6 所示的基于紧急呼叫的安全算法协商装置是为实现图 2 所示的基于紧急呼叫的安全算法协商方法而设计的，图 6 所示装置中的各处理单元的实现功能可参照图 2 所示的方法中的
5 相关描述而理解，各单元的功能可通过运行于处理器上的程序而实现，也可通过相应的逻辑电路而实现。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

权利要求书

1、一种基于紧急呼叫的安全算法协商方法，其特征在于，所述方法包括：

网络侧接收到用户终端的紧急附着请求后，允许紧急附着请求时，设置所述用户终端的安全能力为仅支持空算法；或者，网络侧确定附着请求中所携带的所述用户终端安全能力为仅支持空算法；

为所述用户终端进行非接入层及接入层的以空算法为安全算法的选择处理。

2、根据权利要求 1 所述的方法，其特征在于，所述为所述用户终端进行非接入层及接入层的以空算法为安全算法的选择处理，具体为：

网络侧的移动管理实体 MME 向所述用户终端发送非接入层的安全模式命令，所述非接入层的安全模式命令中携带以空算法作为非接入层安全算法的指示信息。

3、根据权利要求 1 所述的方法，其特征在于，所述为所述用户终端进行非接入层及接入层的以空算法为安全算法的选择处理，具体为：

网络侧的 MME 将所述用户终端的安全能力信息通知所述 eNB；

所述 eNB 根据所述用户终端的安全能力信息确定所述用户终端仅支持空算法，向所述用户终端发送接入层的安全模式命令，所述接入层的安全模式命令中携带以空算法作为接入层安全算法的指示信息。

4、根据权利要求 3 所述的方法，其特征在于，所述确定 eNB 所使用的接入层的根密钥 KeNB，具体为：

所述 MME 确定 UE 附着为紧急附着时，随机生成所述 eNB 使用的接入层的根密钥 KeNB，并通知所述 eNB。

5、根据权利要求 1 所述的方法，其特征在于，所述附着请求中携带所述用户终端安全能力信息，具体为：

所述用户终端确定当前呼叫请求为紧急呼叫请求时，将所述附着请求中的所述用户终端的安全能力信息标识为仅支持空算法。

6、根据权利要求1所述的方法，其特征在于，所述方法还包括：

源 eNB 发起基于 X2 接口的切换时，所述源 eNB 将自身所存储的所述
5 用户终端当前的安全能力信息即仅支持空算法通知目标 eNB；

所述目标 eNB 在切换响应消息中承载有接入层使用空算法作为安全算法的标识信息。

7、根据权利要求1所述的方法，其特征在于，所述方法还包括：

源 eNB 发起基于 S1 接口的切换时，MME 将自身所存储的所述用户终
10 端当前的安全能力信息即仅支持空算法通知目标 eNB；

所述目标 eNB 在切换响应消息中承载有接入层使用空算法作为安全算法的标识信息。

8、一种基于紧急呼叫的安全算法协商装置，其特征在于，所述装置包括第一确定单元、生成单元、发送单元、接收单元、第二确定单元和安全
15 协商处理单元；其中：

第一确定单元，用于在当前呼叫请求是否为紧急呼叫请求时，确定允许紧急附着请求是触发生成单元；

生成单元，用于为所述紧急呼叫生成附着请求，并将所述附着请求中的发起呼叫的用户终端的安全能力信息标识为仅支持空算法；

20 发送单元，用于发送所述附着请求；

接收单元，用于接收所述发送单元所发送的附着请求；

第二确定单元，用于确定所述附着请求中所携带的所述用户终端安全能力信息是否为仅支持空算法，是时触发安全协商处理单元；

安全协商处理单元，用于为所述用户终端进行非接入层及接入层的以
25 空算法为安全算法的选择处理。

9、根据权利要求 8 所述的装置，其特征在于，所述安全协商处理单元包括第一发送模块，用于在所述第二确定单元确定所述用户终端仅支持空算法时，向所述用户终端发送非接入层的安全模式命令，所述非接入层的安全模式命令中携带以空算法作为非接入层安全算法的指示信息。

5 10、根据权利要求 9 所述的装置，其特征在于，所述安全协商处理单元还包括确定模块、通知模块和第二发送模块；其中：

确定模块，用于确定演进基站 eNB 所使用的接入层的根密钥 KeNB；

通知模块，用于将所述确定模块所确定的所述根密钥 KeNB 与所述用户终端的安全能力信息一起通知所述 eNB；

10 第二发送模块，用于在所述 eNB 确定所述用户终端仅支持空算法时，向所述用户终端发送接入层的安全模式命令，所述接入层的安全模式命令中携带以空算法作为接入层安全算法的指示信息。

11、一种基于紧急呼叫的安全算法协商装置，其特征在于，所述装置包括接收单元、确定单元、设置单元和安全协商处理单元；其中：

15 接收单元，用于接收用户终端的附着请求；

确定单元，用于确定所述附着请求是否为紧急附着请求，是时触发设置单元；

设置单元，用于设置所述用户终端的安全能力为仅支持空算法；以及

20 安全协商处理单元，用于以空算法与所述用户终端进行非接入层及接入层的安全协商处理。

12、根据权利要求 11 所述的装置，其特征在于，所述安全协商处理单元包括第一发送模块，用于在所述设置单元设置所述用户终端仅支持空算法时，向所述用户终端发送非接入层的安全模式命令，所述非接入层的安全模式命令中携带以空算法作为非接入层安全算法的指示信息。

25 13、根据权利要求 12 所述的装置，其特征在于，所述安全协商处理单

元还包括确定模块、通知模块和第二发送模块；其中：

确定模块，用于确定演进基站 eNB 所使用的接入层的根密钥 KeNB；

通知模块，用于将所述确定模块所确定的所述根密钥 KeNB 与所述用户终端的安全能力信息一起通知所述 eNB；以及

- 5 第二发送模块，用于在所述 eNB 确定所述用户终端仅支持空算法时，向所述用户终端发送接入层的安全模式命令，所述接入层的安全模式命令中携带以空算法作为接入层安全算法的指示信息。

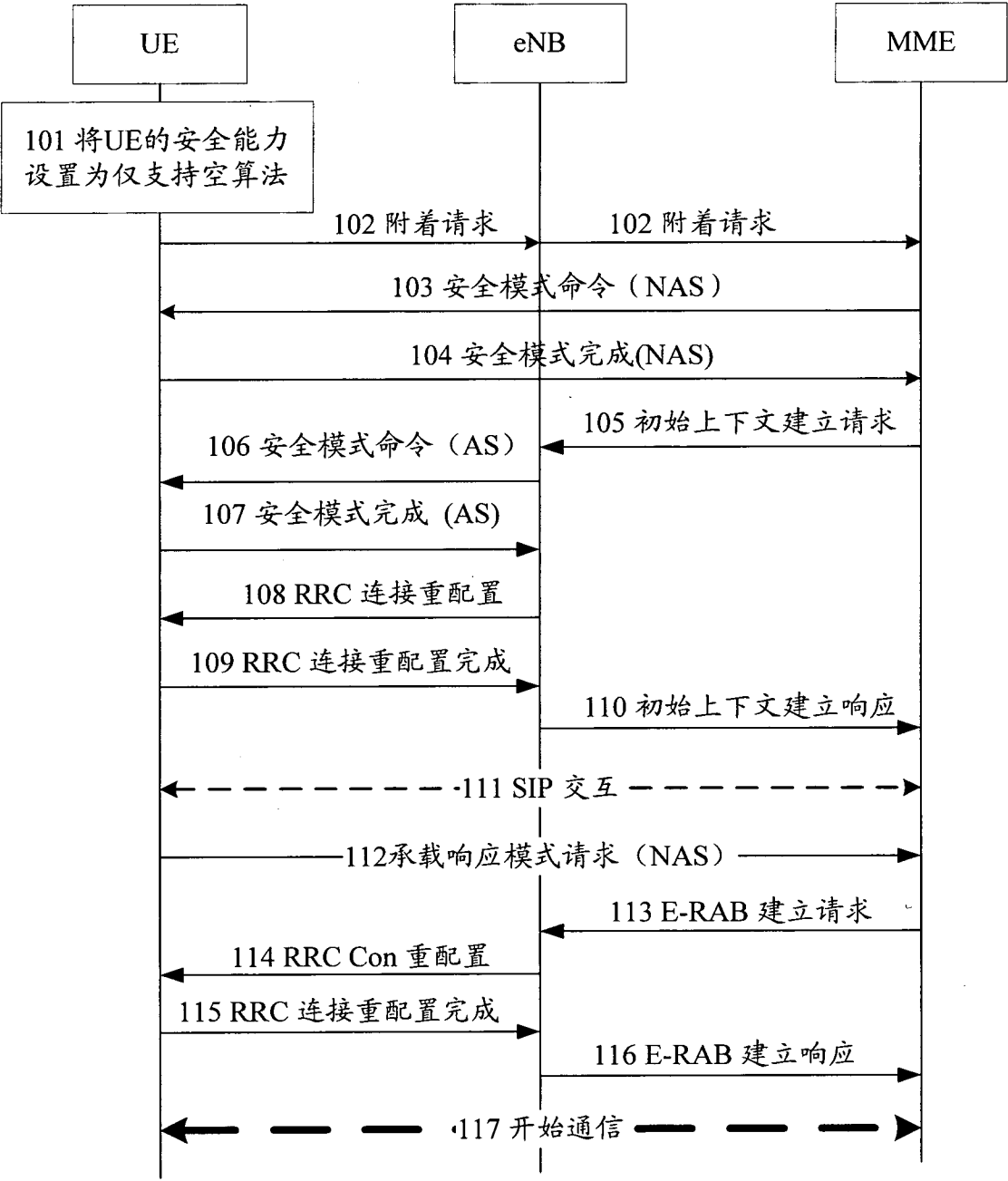


图 1

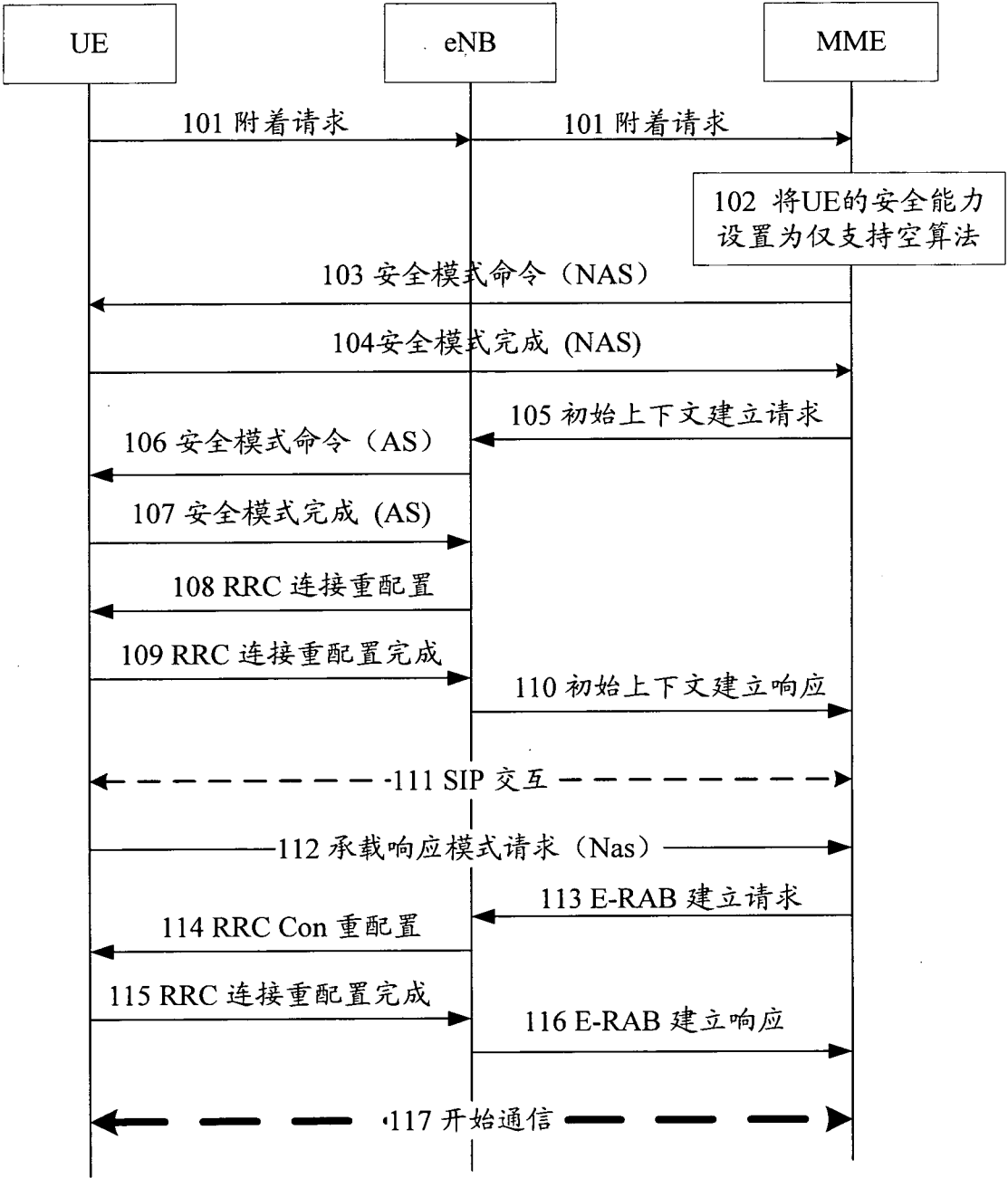


图 2

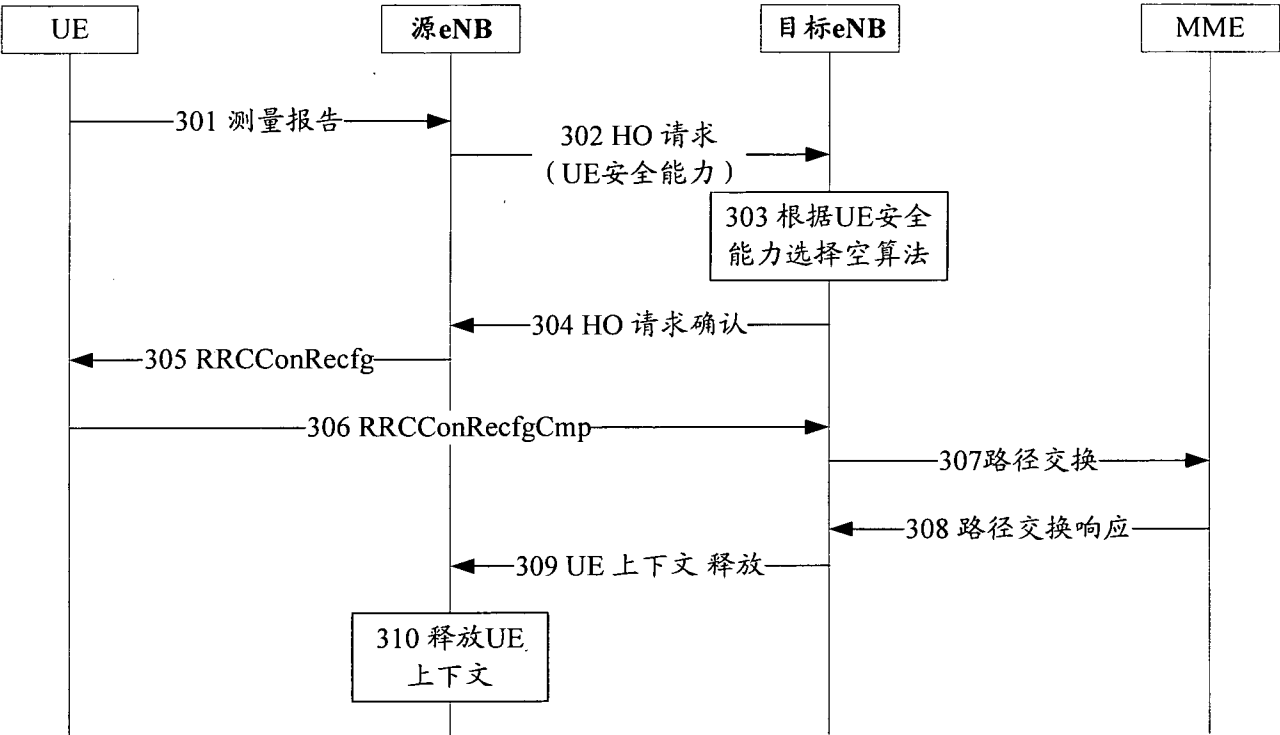


图 3

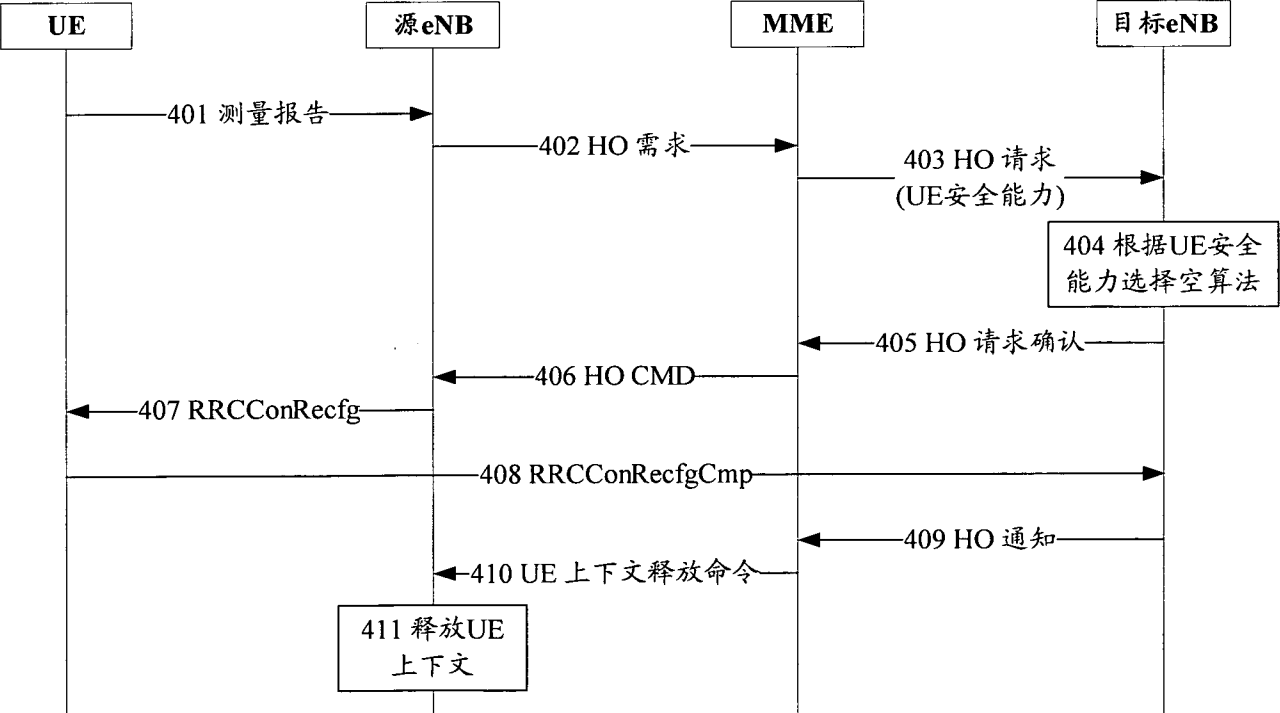


图 4

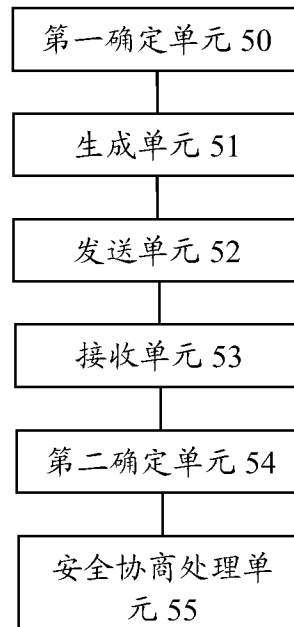


图 5



图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2010/072081

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:H04W,H04Q,H04L,H04M

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)

CNPAT; WPI; EPODOC

emergency,urgency,call,request,algorithm,receiv+,select,network,mobile,cellular,telephone,protocol,safe,estimate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN101110758A (HUAWEI TECHNOLOGIES CO LTD) 23 January 2008(23.01.2008) see the description page 6 line 16 to page 7 line 4	1
A	CN101394667A (ZTE CORP) 25 March 2009(25.03.2009) see the whole document	1-13
A	US2007060097A1 (QUALCOMM INC et al.) 15 March 2007(15.03.2007) see the whole document	1-13

☐ 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 15 July 2010(15.07.2010)	Date of mailing of the international search report 05 Aug. 2010 (05.08.2010)
---	--

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

ZHAO, Weihua

Telephone No. (86-10)62411830

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2010/072081

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101110758A	23.01.2008	WO2008011833A1	31.01.2008
		CN101317493A	03.12.2008
		US2009122793A1	14.05.2009
CN101394667A	25.03.2009	None	
US2007060097A1	15.03.2007	WO2007016695A2	08.02.2007
		WO2007016695A3	29.03.2007
		EP1911257A2	16.04.2008
		CN101273615A	24.09.2008
		KR20080054380A	17.06.2008
		JP2009505455T	05.02.2009
		CA2617783A1	08.02.2007
		TW200715789A	16.04.2007
		RU2008107997A	10.09.2009

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2010/072081

A. CLASSIFICATION OF SUBJECT MATTER

H04W 4/22(2009.01)i

H04W 76/02(2009.01)i

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

国际检索报告

国际申请号
PCT/CN2010/072081

A. 主题的分类

参见附加页

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, H04Q, H04L, H04M

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))

CNPAT; WPI; EPODOC

紧急呼叫, 算法, 协议, 空算法, 请求, 接入, 紧急, 限制, 接收, 协商, 网络, 用户, 呼叫, 请求, emergency, urgency, call, request, algorithm, receiv+, select, network, mobile, cellular, telephone, protocol, safe, estimate

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
X	CN101110758A (华为技术有限公司) 23.1 月 2008 (23.01.2008) 参见说明书第 6 页第 16 行至第 7 页第 4 行	1
A	CN101394667A (中兴通讯股份有限公司) 25.3 月 2009 (25.03.2009) 参见全文	1-13
A	US2007060097A1 (QUALCOMM INC 等) 15.3 月 2007 (15.03.2007) 参见全文	1-13

☐ 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
15.7 月 2010 (15.07.2010)

国际检索报告邮寄日期
05.8 月 2010 (05.08.2010)

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

受权官员
赵伟华
电话号码: (86-10) **62411830**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2010/072081

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN101110758A	23.01.2008	WO2008011833A1	31.01.2008
		CN101317493A	03.12.2008
		US2009122793A1	14.05.2009
CN101394667A	25.03.2009	无	
US2007060097A1	15.03.2007	WO2007016695A2	08.02.2007
		WO2007016695A3	29.03.2007
		EP1911257A2	16.04.2008
		CN101273615A	24.09.2008
		KR20080054380A	17.06.2008
		JP2009505455T	05.02.2009
		CA2617783A1	08.02.2007
		TW200715789A	16.04.2007
		RU2008107997A	10.09.2009

A. 主题的分类

H04W 4/22 (2009.01) i

H04W 76/02 (2009.01) 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