(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
2009 年4 月23 日 (23.04.2009)

PCT

(10) 国际公布号
WO 2009/049447 A1

(51) 国际专利分类号:
H04Q 7/28 (2006.01)

(21) 国际申请号: PCT/CN2007/003321

(22) 国际申请日: 2007 年11 月23 日 (23.11.2007)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200710123860.4
2007 年10 月15 日 (15.10.2007) 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）: **王彦(WANG, Yan)** [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: **北京康信知识产权代理有限责任公司(KANGXIN PARTNERS, P.C.)**; 中国北京市海淀区知春路甲48号盈都大厦A座16层余刚, Beijing 100098 (CN)。

(81) 指定国（除另有指明，要求每一种可提供的国家保护）: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM,

［见续页］

(54) **Title:** PTT DISPATCHING SYSTEM AND A REMOTE-DESTROYING KEY METHOD THEREOF

(54) **发明名称:** 集群调度系统及其密钥遥毁方法

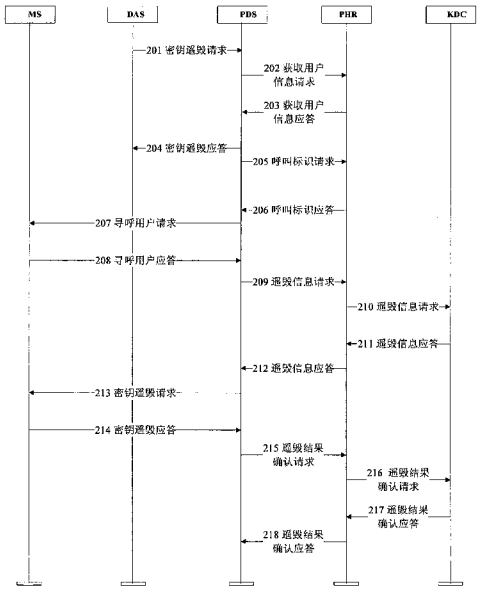

图 2 / FIG. 2

201 REMOTE-DESTROYING KEY REQUEST
202 REQUEST FOR OBTAINING USER INFORMATION
203 RESPONDENCE FOR OBTAINING USER INFORMATION
204 REMOTE-DESTROYING KEY RESPONDENCE
205 CALL INDENTIFICATION REQUEST
206 CALL INDENTIFICATION RESPONDENCE
207 PAGING USER REQUEST
208 PAGING USER RESPONDENCE
209 REMOTE-DESTROYING INFORMATION REQUEST
210 REMOTE-DESTROYING INFORMATION REQUEST
211 REMOTE-DESTROYING INFORMATION RESPONDENCE
212 REMOTE-DESTROYING INFORMATION RESPONDENCE
213 REMOTE-DESTROYING KEY REQUEST
214 REMOTE-DESTROYING KEY RESPONDENCE
215 REQUEST OF REMOTE-DESTROYING RESULT ACKNOWLEDGE
216 REQUEST OF REMOTE-DESTROYING RESULT ACKNOWLEDGE
217 RESPONDENCE OF REMOTE-DESTROYING RESULT ACKNOWLEDGE
218 RESPONDENCE OF REMOTE-DESTROYING RESULT ACKNOWLEDGE

(57) Abstract: A remote-destroying key method in a PTT dispatching system is provided in the present invention, in which the PTT dispatching system performs encryption call management to a PTT terminal equipped encryption module and includes the following steps: A1. the PTT dispatching system initiating a remote-dispatching key request to certain PTT terminal; B1. obtaining a call information corresponding with the PTT terminal according to the remote-destroying key request so as to establish a call channel with the PTT terminal; C1. generating a remote-destroying key instruction to destroy the encryption module of the PTT terminal; D1. sending the remote-destroying key instruction to the PTT terminal so as to destroy the encryption module. A PTT dispatching system for realizing remote-destroying key of a terminal is also provided in the present invention. In the present invention, the encryption module of the terminal could be destroyed instantly, which insures real time privacy of an encryption call.

［见续页］

WO 2009/049447 A1

TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

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

本国际公布：

— 包括国际检索报告。

(57) 摘要：

本发明公开了一种集群调度系统的密钥遥毁方法，该集群调度系统对配备加密模块的集群终端进行加密呼叫管理，包括以下步骤：A1、集群调度系统发起对某集群终端的密钥遥毁请求；B1、根据密钥遥毁请求获取与该集群终端对应的呼叫信息以建立起与该集群终端的呼叫信道；C1、生成用于销毁该集群终端的加密模块的密钥遥毁指令；D1、发送所述密钥遥毁指令至集群终端以销毁其加密模块。本发明同时公开了一种可实现终端密钥遥毁的集群调度系统。本发明能够实现对终端加密模块的即时销毁，确保了加密呼叫的实时私密性。

集群调度系统及其密钥遥毁方法

技术领域

本发明涉及集群通信系统领域，具体涉及一种集群调度系统及其密钥遥毁方法。

背景技术

集群通信系统诞生于20世纪70年代，最早的集群通信系统是模拟系统，数字集群技术从20世纪90年代中期在全球范围内兴起，90年代末期在中国出现数字集群网络。数字集群通信技术具有通信信道利用率高，系统容量大的优点，因此得到了更广泛的应用。

集群技术最主要的两项业务是调度和组呼。集群业务的调度功能是指对一定数量的终端同时发起呼叫，让这些终端同时参与到一个呼叫中；集群业务的组呼功能是指在一个通讯终端上呼叫群组号码，可以将群组内所有终端同时呼入一个呼叫中，从而达到多人同时通话的效果。以上终端可以是有线终端也可以是无线终端。

而在具体的应用中，军方和保密单位往往有对部分终端的集群呼叫进行加密的需求，即没有加密权限的终端即使处在该群组中，也不能加入呼叫，这样才能很好地保证呼叫的私密性。因此，需要在加密呼叫的终端上必须配备加密模块，负责对呼叫密钥进行加密和解密。出于安全性要求，如果发现某个终端已经不能再参与加密呼叫了，调度控制端也可以主动发起密钥遥毁，将终端的加密模块销毁。

但是在目前的技术中，还没有调度控制端主动发起密钥遥毁，将终端的加密模块销毁的技术，这会大大影响呼叫的安全性。

发明内容

本发明的主要目的就是解决现有技术中的问题，提供一种集群调度系统及其密钥遥毁方法，能从调度控制端主动发起对集群终端的密钥遥毁，从而增强集群呼叫的安全性。

为实现上述目的，本发明采用以下技术方案：

一种集群调度系统的密钥遥毁方法，该集群调度系统对配备加密模块的集群终端进行加密呼叫管理，包括以下步骤：

A1、集群调度系统发起对某集群终端的密钥遥毁请求；

B1、根据密钥遥毁请求获取与该集群终端对应的呼叫信息以建立起与该集群终端的呼叫信道；

C1、生成用于销毁该集群终端的加密模块的密钥遥毁指令；

D1、发送所述密钥遥毁指令至集群终端以销毁其加密模块。

优选地：

所述密钥遥毁请求携带集群终端号码信息。

还包括以下步骤：

E1、所述集群终端接收到密钥遥毁指令后，对自身加密模块运行遥毁指令。

集群调度系统包括调度台服务器、集群调度服务器和集群鉴权服务器，所述步骤 B1 包括以下子步骤：

B11、所述集群调度服务器响应所述调度台服务器发起的对某集群终端的密钥遥毁请求并发出呼叫信息获取请求，所述集群鉴权服务器响应所述呼叫信息获取请求并返回与该集群终端相对应的呼叫信息；

B12、所述集群调度服务器根据所述呼叫信息建立与该集群终端的呼叫信道。

所述呼叫信息包括用户信息和呼叫标识，所述用户信息包括全球移动用户标识和用户当前位置信息，所述步骤 B11 包括如下子步骤：

B111、所述集群调度服务器向集群鉴权服务器请求用户信息；

B112、所述集群调度服务器得到所述集群鉴权服务器返回的用户信息后先向所述调度台服务器返回密钥遥回应答，然后向集群鉴权服务器请求呼

叫标识;

B113、所述集群鉴权服务器向集群调度服务器返回呼叫标识。

所述集群调度系统还包括密钥分发中心,所述步骤 C1 包括如下子步骤:

C11、所述集群调度服务器通过集群鉴权服务器向密钥分发中心发送密钥遥毁指令获取请求;

C12、所述密钥分发中心响应遥毁指令获取请求产生密钥遥毁指令,并通过集群鉴权服务器返送至调度服务器。

在所述步骤 E1 之后还包括以下步骤:

F1、所述集群终端向集群调度系统返回密钥遥毁成功或失败的结果;

G1、所述集群调度系统根据集群终端返回的所述结果进行调度端处理。

所述步骤 G1 包括如下子步骤:

G11、所述集群调度服务器接收集群终端的密钥遥毁结果,并通过集群鉴权服务器向密钥分发中心发送结果确认请求;

G12、密钥分发中心响应结果确认请求,并根据密钥遥毁结果确定是否更新加密用户列表;

G13、密钥分发中心通过集群鉴权服务器向集群调度服务器返回结果确认应答。

为实现上述目的,本发明还采用以下技术方案:

一种可实现终端密钥遥毁的集群调度系统,包括调度台服务器、调度系统服务器和密钥分发中心,所述调度台服务器用于发起对某集群终端的密钥遥毁请求;所述调度系统服务器用于根据密钥遥毁请求获取查询与该集群终端对应的呼叫信息以建立起与该集群终端的呼叫信道;所述密钥分发中心用于生成用于销毁该集群终端的加密模块的密钥遥毁指令,所述调度系统服务器将密钥遥毁指令发送至所述集群终端。

所述调度系统服务器包括集群调度服务器和集群鉴权服务器,所述集群调度服务器用于根据密钥遥毁请求发出对某集群终端的呼叫信息获取请求,

并接收集群鉴权服务器返回的呼叫信息，并根据呼叫信息建立呼叫信道；所述集群调度服务器通过集群鉴权服务器向密钥分发中心发送密钥遥毁指令获取请求；所述密钥分发中心通过集群鉴权服务器将密钥遥毁指令返送至调度服务器。

本发明的有益效果是:

由于本发明能由集群调度系统主动对不能再参与加密呼叫的集群终端实施密钥遥毁，集群终端受控响应集群调度系统的密钥遥毁指令销毁其所配备的加密模块。如果调度控制端的集群调度系统发现某个终端已经不能再参与加密呼叫了，不再只是由用户终端负责处理自身的加密模块，集群调度系统也可以主动发起密钥销毁指令将集群终端的加密模块销毁，因此，这种密钥遥毁的方式大大增强了集群通信中，集群调度系统对集群终端的加密呼叫管理能力，提高了加密呼叫的安全性。

附图说明

图 1 为本发明实施例所应用的集群通信系统网络框架图;

图 2 为本发明实施例的密钥遥毁方法流程图。

本发明的特征及优点将通过实施例结合附图进行详细说明。

具体实施方式

本发明中，当集群调度系统管理的某个集群终端不能再参与加密呼叫时，调度控制端的集群调度系统能主动发起对该终端的密钥遥毁，下发指令将其自身配备的加密模块销毁，从而实现加密呼叫的安全管理。

请参考图 1，本实施例所应用的集群通信系统包括调度服务子系统 DSS(Dispatching Service System)、密钥分发中心 KDC（Key Distribution Center）、基站子系统 BSS(Base Station Subsystem)、交换子系统 MSS(Mobile Switch Subsystem)、集群终端等逻辑功能模块。其中，调度服务子系统和密钥分发中心组成了本发明的集群调度系统。集群终端通过空中接口和基站子系统相连，调度服务子系统与密钥分发中心则分别通过基站子系统与集群终端连接。

调度服务子系统包括调度系统服务器、调度台服务器，其中，调度系统服务器又包括集群调度服务器 PDS(PTT Dispatch Server)和集群鉴权服务器 PHR(PTT Home Register)，主要负责完成集群调度业务。

集群调度服务器是集群呼叫的总控制点，完成集群调度呼叫的处理，包括鉴别集群用户、建立各种集群呼叫如私密呼叫和群组呼叫、判断集群 PTT 请求等。此外，集群调度服务器还接收反向链路来的集群语音数据，根据呼叫的性质再分发到对应的前向链路。

集群鉴权服务器完成数据库管理和配置功能，为集群用户提供群组注册、群组成员注册，并提供集群成员的本地信息以及集群成员的业务权限记录，完成呼叫统计和计费功能。

密钥分发中心主要是完成密钥的生成、维护和分发的功能。

本实施例中，调度台服务器是集群调度系统的密钥遥毁请求发起端，负责向集群调度服务器主动发起对某终端的密钥遥毁请求。

集群调度服务器是集群呼叫的总控制点，它根据密钥遥毁请求发出集群鉴权服务器呼叫信息获取请求，接收集群鉴权服务器返回的呼叫信息，并根据其中的用户信息和呼叫标识建立呼叫信道，其中的用户信息包括全球移动用户标识和用户当前位置信息。集群调度服务器还负责在建立起呼叫信道之后，向密钥分发中心发送密钥遥毁指令获取请求，并在接收到密钥遥毁指令后发送给集群终端。在集群终端作出响应之后，集群调度服务器接收集群终端返回的密钥遥毁结果，进一步向密钥分发中心发送结果确认请求，并在密钥分发中心进行相应处理之后，接收其返回的结果确认应答。

集群鉴权服务器负责处理来自集群调度服务器的呼叫信息获取请求，查询并返回含用户信息和呼叫标识的呼叫信息至集群调度服务器；在呼叫信道建立之后，负责转发来自集群调度服务器的密钥遥毁指令获取请求至密钥分发中心，并将密钥分发中心给出的密钥遥毁指令返回至调度服务器；此外，它还负责转发来自集群调度服务器的结果确认请求至密钥分发中心，并将密钥分发中心的结果确认应答返回至集群调度服务器。

密钥分发中心负责接收集群调度服务器遥毁指令获取请求，根据遥毁指令获取请求生成遥毁指令，并通过集群鉴权服务器发送至调度服务器；负责接收结果确认请求，根据遥毁结果确定是否更新加密用户列表，并向集群调

度服务器返回结果确认应答。

基站子系统主要完成各种集群业务，数据业务和普通电话业务的无线接入功能。基站子系统由基站收发信机 BTS（Base Transceiver System ）、基站控制器 BSC（Base Station Controller）以及调度控制器 PDC 共同构成。其中基站收发信机完成基带信号的调制与解调、射频信号收发等功能，基站控制器完成无线资源的分配、呼叫处理、功率控制以及支持终端的各类切换，调度控制器则完成无线资源的分配、调度呼叫控制、功率控制、支持集群终端的在不同覆盖区下的各类切换、汇集和分发集群语音数据流。

交换子系统主要完成电话互联业务、普通电话呼叫业务和部分增值业务。交换子系统由移动交换中心 MSC（Mobile Switching Center）和归属位置寄存器 HLR（Home Location Register）等组成。

请参见图 2，集群通信系统中，由集群调度系统自调度控制端主动发起和完成终端密钥遥毁的流程如下：

步骤 201：调度控制端的调度台服务器 DAS 主动向集群调度服务器 PDS 发起对某集群终端的密钥遥毁请求，请求中携带终端的号码信息；

步骤 202：集群调度服务器 PDS 收到该请求后，向集群鉴权服务器 PHR 请求获取用户信息，包括全球移动用户标识 IMSI 和用户的当前位置信息；

步骤 203：集群鉴权服务器 PHR 给集群调度服务器 PDS 回用户信息应答；

步骤 204：集群调度服务器 PDS 收到后给先调度台服务器 DAS 回密钥遥毁应答；

步骤 205：集群调度服务器 PDS 然后向集群鉴权服务器 PHR 请求用户的呼叫标识 GID；

步骤 206：集群鉴权服务器 PHR 生成用户的呼叫标识 GID,向集群调度服务器 PDS 回应答；

步骤 207：集群调度服务器 PDS 利用获得的呼叫标识 GID 和用户信息对终端发起寻呼，建立业务信道；

步骤 208: 集群终端回集群调度服务器 PDS 寻呼应答;

步骤 209: 集群调度服务器 PDS 向集群鉴权服务器 PHR 发起遥毁信息请求，即请求获取对集群终端加密模块的遥毁指令;

步骤 210: 集群鉴权服务器 PHR 向密钥分发中心 KDC 转发该遥毁信息请求;

步骤 211: 密钥分发中心 KDC 生成对终端加密模块的遥毁指令，向集群鉴权服务器 PHR 回遥毁信息应答;

步骤 212: 集群鉴权服务器 PHR 向集群调度服务器 PDS 转发遥毁信息应答;

步骤 213: 集群调度服务器 PDS 收到应答后，向终端发起密钥遥毁请求，请求中携带终端加密模块的遥毁指令;

步骤 214: 终端收到密钥遥毁请求后，利用请求中携带的遥毁指令将自己的加密模块销毁，然后给集群调度服务器 PDS 回遥毁是否成功的应答;

步骤 215: 集群调度服务器 PDS 向集群鉴权服务器 PHR 发送遥毁结果确认请求;

步骤 216: 集群鉴权服务器 PHR 向密钥分发中心 KDC 转发遥毁结果确认请求;

步骤 217: 密钥分发中心 KDC 收到请求后，根据遥毁结果是否成功实时更新所维护的用户密钥和用户加密状态，然后回集群鉴权服务器 PHR 遥毁结果确认应答;

步骤 218: 集群鉴权服务器 PHR 向集群调度服务器 PDS 转发遥毁结果确认应答。

本发明能够实现对终端加密模块的即时销毁，确保了加密呼叫的实时私密性。当然，除了加密呼叫管理业务，本发明所应用的集群通信系统还可为用户提供集群系统的各种集群业务，也可为用户提供传统的普通电话业务、短消息业务和数据业务。

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，

不能认定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，还可以做出若干简单推演或替换，都应当视为属于本发明的保护范围。

权 利 要 求 书

1. 一种集群调度系统的密钥遥毁方法，该集群调度系统对配备加密模块的集群终端进行加密呼叫管理，其特征在于包括以下步骤：

A1、集群调度系统发起对某集群终端的密钥遥毁请求；

B1、根据密钥遥毁请求获取与该集群终端对应的呼叫信息以建立起与该集群终端的呼叫信道；

C1、生成用于销毁该集群终端的加密模块的密钥遥毁指令；

D1、发送所述密钥遥毁指令至集群终端以销毁其加密模块。

2. 如权利要求 1 所述的集群调度系统的密钥遥毁方法，其特征在于，所述密钥遥毁请求携带集群终端号码信息。

3. 如权利要求 1 所述的集群调度系统的密钥遥毁方法，其特征在于还包括以下步骤：

E1、所述集群终端接收到密钥遥毁指令后，对自身加密模块运行遥毁指令。

4. 如权利要求 1 所述的集群调度系统的密钥遥毁方法，其特征在于，集群调度系统包括调度台服务器、集群调度服务器和集群鉴权服务器，所述步骤 B1 包括以下子步骤：

B11、所述集群调度服务器响应所述调度台服务器发起的对某集群终端的密钥遥毁请求并发出呼叫信息获取请求，所述集群鉴权服务器响应所述呼叫信息获取请求并返回与该集群终端相对应的呼叫信息；

B12、所述集群调度服务器根据所述呼叫信息建立与该集群终端的呼叫信道。

5. 如权利要求 4 所述的集群调度系统的密钥遥毁方法，其特征在于，所述呼叫信息包括用户信息和呼叫标识，所述用户信息包括全球移动用户标识和用户当前位置信息，所述步骤 B11 包括如下子步骤：

B111、所述集群调度服务器向集群鉴权服务器请求用户信息；

B112、所述集群调度服务器得到所述集群鉴权服务器返回的用户信息后先向所述调度台服务器返回密钥遥回应答，然后向集群鉴权服务器请求呼叫标识；

B113、所述集群鉴权服务器向集群调度服务器返回呼叫标识。

6. 如权利要求 4 所述的集群调度系统的密钥遥毁方法，其特征在于，所述集群调度系统还包括密钥分发中心，所述步骤 C1 包括如下子步骤：

C11、所述集群调度服务器通过集群鉴权服务器向密钥分发中心发送密钥遥毁指令获取请求；

C12、所述密钥分发中心响应遥毁指令获取请求产生密钥遥毁指令，并通过集群鉴权服务器返送至调度服务器。

7. 如权利要求 3 所述的集群调度系统的密钥遥毁方法，其特征在于，在所述步骤 E1 之后还包括以下步骤：

F1、所述集群终端向集群调度系统返回密钥遥毁成功或失败的结果；

G1、所述集群调度系统根据集群终端返回的所述结果进行调度端处理。

8. 如权利要求 7 所述的集群调度系统的密钥遥毁方法，其特征在于，所述步骤 G1 包括如下子步骤：

G11、所述集群调度服务器接收集群终端的密钥遥毁结果，并通过集群鉴权服务器向密钥分发中心发送结果确认请求；

G12、密钥分发中心响应结果确认请求，并根据密钥遥毁结果确定是否更新加密用户列表；

G13、密钥分发中心通过集群鉴权服务器向集群调度服务器返回结果确认应答。

9. 一种可实现终端密钥遥毁的集群调度系统，其特征在于，包括调度台服务器、调度系统服务器和密钥分发中心，所述调度台服务器用于发起对某集群终端的密钥遥毁请求；所述调度系统服务器用于根据密钥遥毁请求获取查询与该集群终端对应的呼叫信息以建立起与该集群终端的呼叫信道；所述密钥分发中心用于生成用于销毁该集群终端的加

密模块的密钥遥毁指令，所述调度系统服务器将密钥遥毁指令发送至所述集群终端。

10. 如权利要求 9 所述的集群调度系统，其特征在于，所述调度系统服务器包括集群调度服务器和集群鉴权服务器，所述集群调度服务器用于根据密钥遥毁请求发出对某集群终端的呼叫信息获取请求，并接收集群鉴权服务器返回的呼叫信息，并根据呼叫信息建立呼叫信道；所述集群调度服务器通过集群鉴权服务器向密钥分发中心发送密钥遥毁指令获取请求；所述密钥分发中心通过集群鉴权服务器将密钥遥毁指令返送至调度服务器。

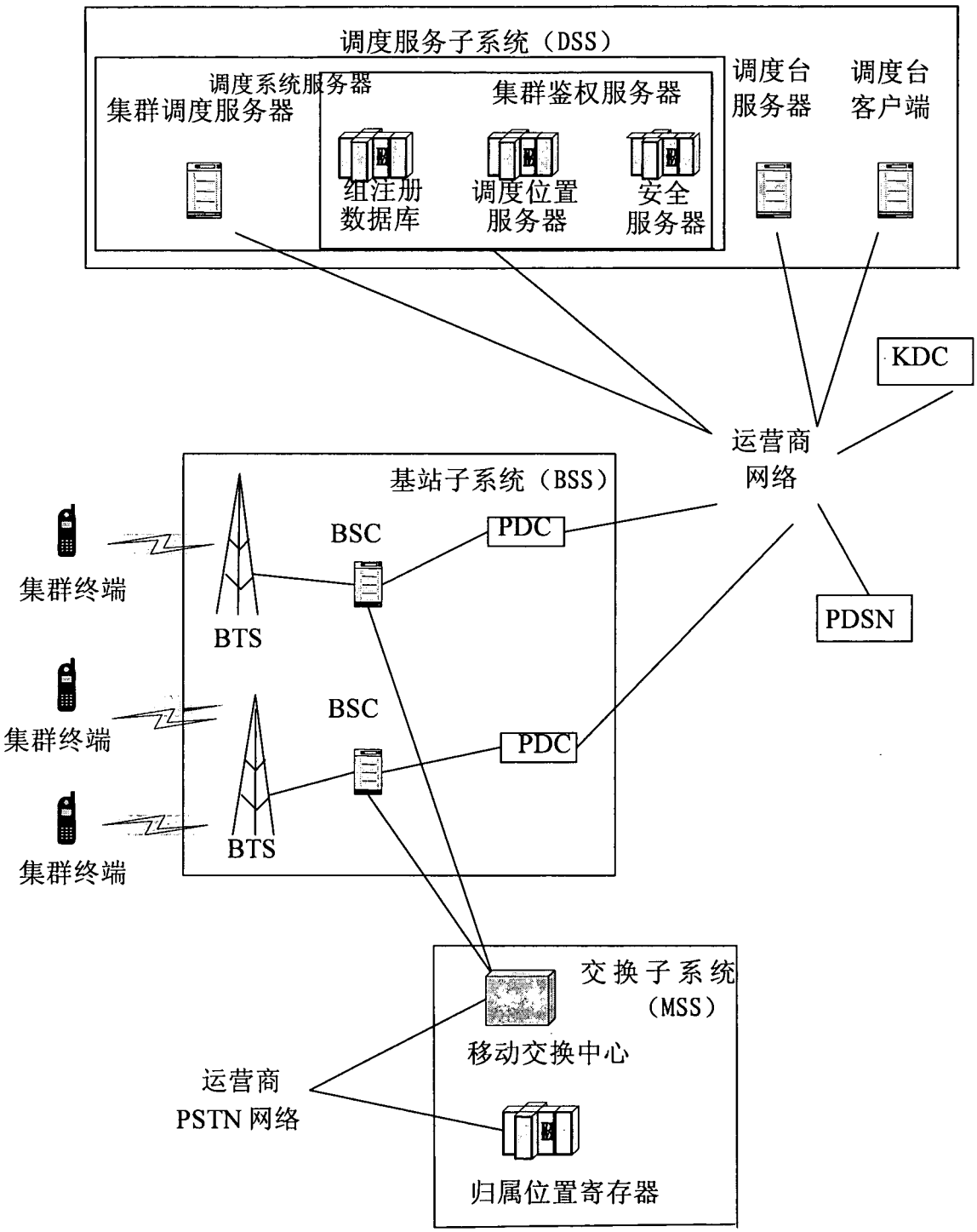
调度服务子系统（DSS）
调度系统服务器
集群调度服务器
集群鉴权服务器
组注册数据库
调度位置服务器
安全服务器
调度台服务器
调度台客户端
KDC
运营商网络
基站子系统（BSS）
BSC
PDC
BTS
集群终端
PDSN
交换子系统（MSS）
移动交换中心
运营商PSTN网络
归属位置寄存器

图 1

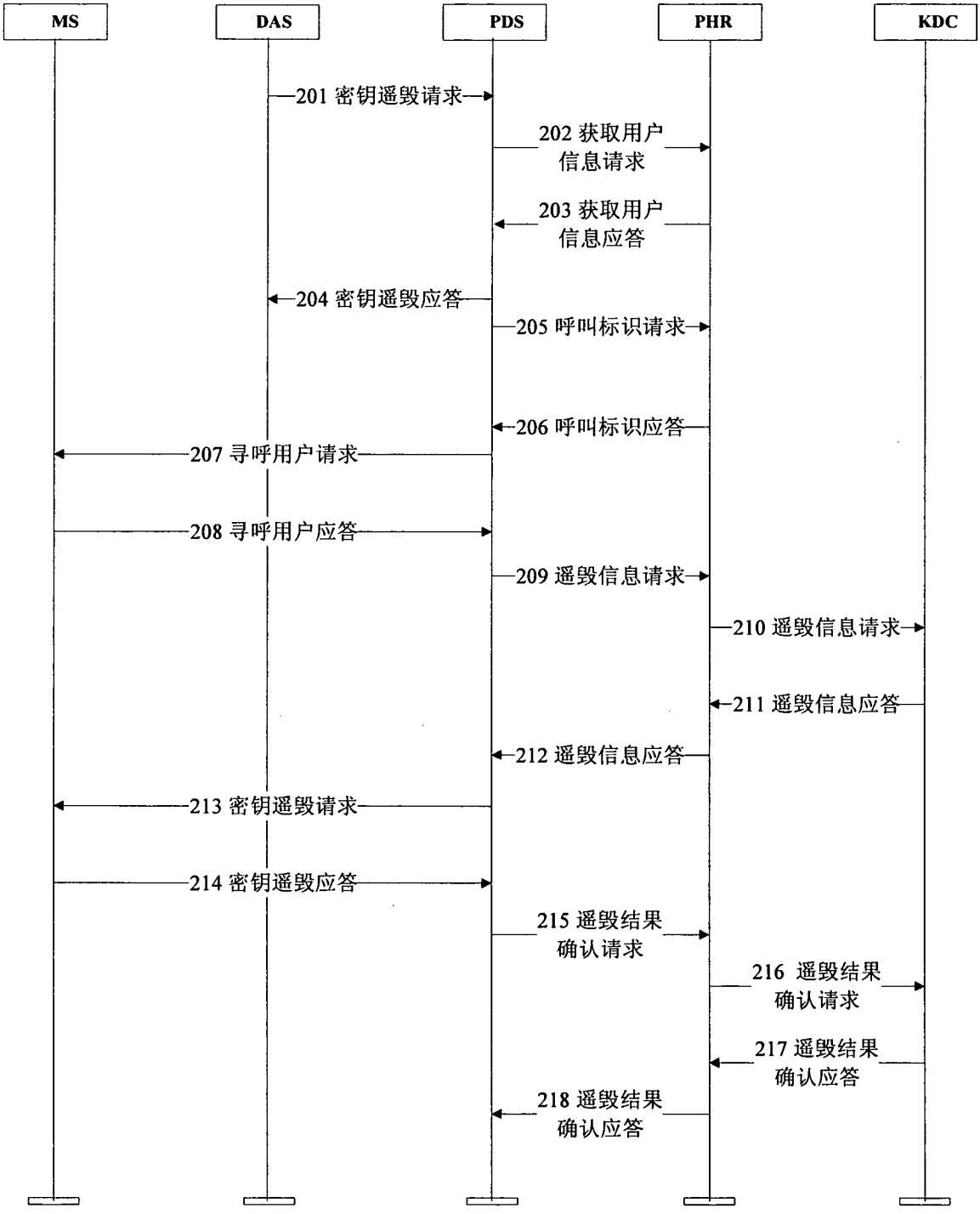
MS
DAS
PDS
PHR
KDC
201 密钥遥毁请求
202 获取用户信息请求
203 获取用户信息应答
204 密钥遥毁应答
205 呼叫标识请求
206 呼叫标识应答
207 寻呼用户请求
208 寻呼用户应答
209 遥毁信息请求
210 遥毁信息请求
211 遥毁信息应答
212 遥毁信息应答
213 密钥遥毁请求
214 密钥遥毁应答
215 遥毁结果确认请求
216 遥毁结果确认请求
217 遥毁结果确认应答
218 遥毁结果确认应答

图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/003321

A. CLASSIFICATION OF SUBJECT MATTER

H04Q7/28 (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: H04Q7/-, H04M9/-, H04L12/-

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

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

WPI,EPODOC,PAJ, CPRS, CNKI: PTT/dispatch/trunk, call, channel, key/encrypt/password, instrument/information/request, remote

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN101022608A (ZTE COMMUNICATION CO LTD) 22 Aug. 2007 (22.08.2007) the whole document	1-10
A	RU2307475C1 (DEFENCE MIN RES TEST INST 16) 27 Sept. 2007 (27.09.2007) the whole document	1-10
A	US2006121927A1 (SAMSUNG ELECTRONICS CO LTD) 08 Jun. 2006 (08.06.2006) the whole document	1-10

☐ 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
10 Jul. 2008 (10.07.2008)	**24 Jul. 2008 (24.07.2008)**
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 WANG, Chunyan Telephone No. (86-10)62411355

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2007/003321

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101022608 A	22.08.2007	None	
RU2307475C1	27.09.2007	None	
US2006121927A1	08.06.2006	KR20060064212A	13.06.2006
		KR100626218B1	21.09.2006

国际检索报告

国际申请号
PCT/CN2007/003321

A. 主题的分类

H04Q7/28 (2006.01) i

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04Q7/-, H04M9/-, H04L12/-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI,EPODOC,PAJ: PTT/dispatch/trunk, call, channel, key/encrypt/password, instrument/information/request, remote;

CPRS,CNKI: 集群/调度, 呼叫, 信道, 指令/命令, 加密/密码/密钥, 信息/请求,鉴权, 遥控/远端

C. 相关文件

类　型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN101022608A (中兴通讯股份有限公司) 22.8 月 2007 (22.08.2007)　全文	1-10
A	RU2307475C1 (DEFENCE MIN RES TEST INST 16) 27.9 月 2007 (27.09.2007) 全文	1-10
A	US2006121927A1 (三星电子株式会社) 08.6 月 2006 (08.06.2006) 全文	1-10

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

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

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

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

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

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

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
10.7 月 2008 (10.07.2008)	**24.7 月 2008 (24.07.2008)**
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号：　(86-10)62019451	受权官员 王春艳 电话号码：(86-10) **62411355**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2007/003321

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101022608 A	22.08.2007	无	
RU2307475C1	27.09.2007	无	
US2006121927A1	08.06.2006	KR20060064212A	13.06.2006
		KR100626218B1	21.09.2006