

(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
2018 年 7 月 19 日 (19.07.2018)



(10) 国际公布号
WO 2018/129652 A1

- (51) 国际专利分类号:
H04W 36/08 (2009.01) *H04L 29/02* (2006.01)
H04W 36/34 (2009.01)
- (21) 国际申请号: PCT/CN2017/070744
- (22) 国际申请日: 2017 年 1 月 10 日 (10.01.2017)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: 海能达通信股份有限公司 (HYTERA COMMUNICATIONS CORPORATION LIMITED) [CN/CN]; 中国广东省深圳市南山区高新技术产业园北区北环路海能达大厦, Guangdong 518057 (CN)。
- (72) 发明人: 张祥云 (ZHANG, Xiangyun); 中国广东省深圳市南山区高新技术产业园北区北环路海能达大厦, Guangdong 518057 (CN)。
- (74) 代理人: 深圳市威世博知识产权代理事务所 (普通合伙) (CHINA WISPRO INTELLECTUAL PROPERTY LLP.); 中国广东省深圳市南山区高新区粤兴三道8号中国地质大学产学研基地中地大楼A806, Guangdong 518057 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,

(54) Title: DECRYPTION METHOD FOR CLUSTER GROUP CALL, AND USER EQUIPMENT

(54) 发明名称: 集群组呼解密方法及用户设备

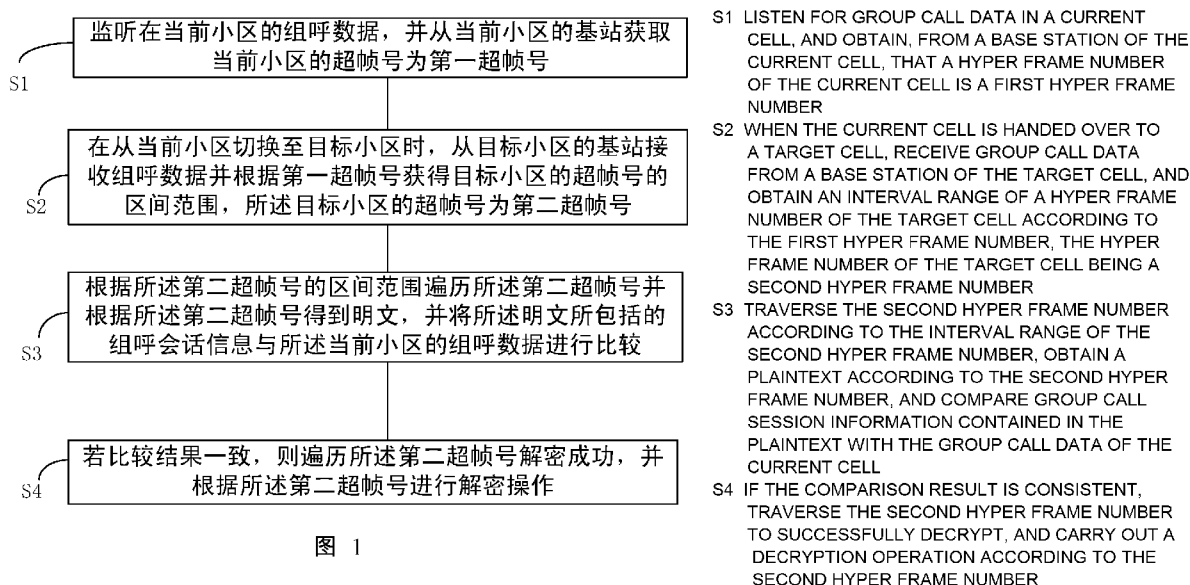


图 1

(57) Abstract: The present invention provides a decryption method for a cluster group call, and a user equipment. The method comprises: listening for group call data in a current cell, and obtaining that a hyper frame number is a first hyper frame number; when the current cell is handed over to a target cell, obtaining the group call data and obtaining an interval range of a hyper frame number of the target cell according to the first hyper frame number, the hyper frame number of the target cell being a second hyper frame number; traversing the second hyper frame number according to the interval range of the second hyper frame numbers, obtaining a plaintext, and comparing group call session information contained in the plaintext with the group call data of the current cell; and if consistent, traversing the second hyper frame number to successfully decrypt, and carrying out a decryption operation according to the second hyper frame number.

QA, RO, RS, RU, RW, SA, 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, ST, 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, KM, 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))。

(57) 摘要: 本发明提供一种集群组呼解密方法及用户设备。所述方法包括监听在当前小区的组呼数据并获取超帧号为第一超帧号; 在从当前小区切换至目标小区时, 获得组呼数据并根据第一超帧号获得目标小区的超帧号的区间范围, 目标小区的超帧号为第二超帧号; 根据第二超帧号的区间范围遍历第二超帧号并得到明文, 将明文所包括的组呼会话信息与当前小区的组呼数据进行比较; 若一致, 则遍历第二超帧号解密成功, 并根据第二超帧号进行解密操作。

集群组呼解密方法及用户设备

[1] **【技术领域】**

[2] 本发明涉及移动通信领域，特别是涉及一种集群组呼解密方法及用户设备。

[3] **【背景技术】**

[4] 组呼会话发起后，基站下各小区建立会话、应用加密参数发组呼码流，各小区配置加密参数可能不一致、加密上下文并不同步，因此当用户设备从当前小区切换至相邻的目标小区时必须获取目标小区的加密参数及状态才能解密，导致组呼业务中断时延较长。

[5] **【发明内容】**

[6] 本发明主要解决的技术问题是提供一种集群组呼解密方法及用户设备，以减小组呼业务中断时延，提高用户体验。

[7] 为解决上述技术问题，本发明采用的一个技术方案是：提供一种集群组呼解密方法，所述方法应用于用户设备，包括：

[8] 监听在当前小区的组呼数据，并从所述当前小区的基站获取所述当前小区的超帧号为第一超帧号；

[9] 在从所述当前小区切换至目标小区时，从所述目标小区的基站接收组呼数据并根据所述第一超帧号获得所述目标小区的超帧号的区间范围，所述目标小区的超帧号为第二超帧号；

[10] 根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号得到明文，并将所述明文所包括的组呼会话信息与所述当前小区的组呼数据进行比较；

[11] 若比较结果一致，则遍历所述第二超帧号解密成功，并根据所述第二超帧号进行解密操作。

[12] 其中，从所述目标小区的基站接收组呼数据并根据所述第一超帧号获得所述目标小区的超帧号的区间范围的步骤包括：

[13] 所述第二超帧号为在 $[X-M, X+N]$ 的区间范围内，其中 X 为所述第一超帧号， M

和N均为自然数;

[14] 根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号得到明文的步骤包括:

[15] 在所述 $[X-M, X+N]$ 的区间范围内改变所述第二超帧号的值, 并根据改变后的所述第二超帧号的值进行解密操作, 以得到所述明文。

[16] 其中, 遍历所述第二超帧号解密成功, 并根据所述第二超帧号进行解密操作的步骤包括:

[17] 遍历所述第二超帧号的顺序为:

[18] $X \rightarrow X-1 \rightarrow X+1 \rightarrow X-2 \rightarrow X+2 \dots \rightarrow X-M \dots \rightarrow X+N$ 。

[19] 其中, 在所述组呼数据配置为PDCP SN 5bit且包间隔20毫秒时, M和N设置为2。

[20] 其中, 所述从所述当前小区切换至目标小区的步骤包括:

[21] 发起并建立组呼会话, 以使基站在建立集群业务承载时, 新增字段以携带组呼数据的加密参数, 并且保存所述加密参数;

[22] 从所述当前小区切换至所述目标小区, 新增或复用其中一条信令携带所述当前小区会话密钥标识或直接携带所述当前小区的密钥;

[23] 接收到所述目标小区的加密组呼数据;

[24] 所述根据所述第二超帧号进行解密操作的步骤包括:

[25] 根据所述第二超帧号对所述目标小区的加密组呼数据进行解密操作。

[26] 其中, 在接收到所述目标小区的加密组呼数据的步骤之前, 所述方法进一步包括:

[27] 发送所述当前小区会话密钥标识或者所述当前小区的密钥给所述目标小区的基站, 所述目标小区的基站将所述当前小区会话密钥标识或者所述当前小区的密钥与所述目标小区的密钥进行比较;

[28] 若一致, 则从所述目标小区的基站接收到所述目标小区的加密组呼数据;

[29] 若不一致, 则从所述目标小区的基站接收到所述目标小区的加密组呼数据的同时将所述目标小区的密钥发送给所述当前小区的基站, 再由所述当前小区的基站将所述目标小区的密钥发送给所述用户设备。

- [30] 其中，所述从所述当前小区切换至目标小区的步骤包括：
- [31] 发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼加密参数，并且保存所述组呼加密参数；
- [32] 从所述目标小区的基站接收到所述目标小区的加密组呼数据。
- [33] 为解决上述技术问题，本发明采用的一个技术方案是：提供一种用户设备，所述用户设备包括：
- [34] 监听模块，用于监听用户设备在当前小区的组呼数据，并从所述当前小区的基站获取所述当前小区的超帧号为第一超帧号；
- [35] 收发模块，用于在所述用户设备从所述当前小区切换至目标小区时，从所述目标小区的基站接收组呼数据并根据所述第一超帧号获得所述目标小区的超帧号的区间范围，所述目标小区的超帧号为第二超帧号；
- [36] 处理模块，连接所述监听模块及所述收发模块，用于根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号得到明文，并将所述明文所包括的组呼会话信息与所述当前小区的组呼数据进行比较，若比较结果一致，则遍历所述第二超帧号解密成功，并根据所述第二超帧号进行解密操作。
- [37] 其中，所述第二超帧号为在 $[X-M, X+N]$ 的区间范围内，其中 X 为所述第一超帧号， M 和 N 均为自然数；在所述 $[X-M, X+N]$ 的区间范围内改变所述第二超帧号的值，所述处理模块根据改变后的所述第二超帧号的值进行解密操作，以得到所述明文。
- [38] 其中，所述处理模块遍历所述第二超帧号的顺序为：
- [39] $X \rightarrow X-1 \rightarrow X+1 \rightarrow X-2 \rightarrow X+2 \dots \rightarrow X-M \dots \rightarrow X+N$ 。
- [40] 其中，在所述组呼数据配置为PDCP SN 5bit且包间隔20毫秒时， M 和 N 设置为2。
- [41] 其中，所述用户设备还包括建立模块及密钥模块，所述用户设备在从所述当前小区切换至目标小区时，所述建立模块发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼数据的加密参数，并且保存所述加密参数；
- [42] 所述用户设备从所述当前小区切换至所述目标小区时，所述密钥模块新增或复

用其中一条信令携带所述当前小区会话密钥标识或直接携带所述当前小区的密钥；

[43] 所述收发模块接收到所述目标小区的加密组呼数据；

[44] 所述处理模块根据所述第二超帧号对所述目标小区的加密组呼数据进行解密操作。

[45] 其中，所述密钥模块还发送所述当前小区会话密钥标识或者所述当前小区的密钥给所述目标小区的基站，所述目标小区的基站将所述当前小区会话密钥标识或者所述当前小区的密钥与所述目标小区的密钥进行比较；

[46] 若一致，则所述收发模块从所述目标小区的基站接收到所述目标小区的加密组呼数据；

[47] 若不一致，则从所述目标小区的基站接收到所述目标小区的加密组呼数据的同时将所述目标小区的密钥发送给所述当前小区的基站，再由所述当前小区的基站将所述目标小区的密钥发送给所述用户设备。

[48] 其中，所述用户设备还包括建立模块，在所述用户设备从所述当前小区切换至目标小区时，所述建立模块发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼加密参数，并且保存所述组呼加密参数；

[49] 所述收发模块从所述目标小区的基站接收到所述目标小区的加密组呼数据。

[50] 为解决上述技术问题，本发明采用的一个技术方案是：提供一种用户设备，所述用户设备包括：

[51] 存储器，用于存储程序指令；

[52] 处理器，用于监听用户设备在当前小区的组呼数据，并从所述当前小区的基站获取所述当前小区的超帧号为第一超帧号；

[53] 所述处理器，还用于在所述用户设备从所述当前小区切换至目标小区时，从所述目标小区的基站接收组呼数据并根据所述第一超帧号获得所述目标小区的超帧号的区间范围，所述目标小区的超帧号为第二超帧号；

[54] 控制器，用于根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号得到明文，并将所述明文所包括的组呼会话信息与所述当前小区的组呼数据进行比较，若比较结果一致，则遍历所述第二超帧号解密成功，并根

据所述第二超帧号进行解密操作。

- [55] 其中，所述第二超帧号为在 $[X-M, X+N]$ 的区间范围内，其中 X 为所述第一超帧号， M 和 N 均为自然数；在所述 $[X-M, X+N]$ 的区间范围内改变所述第二超帧号的值，所述处理模块根据改变后的所述第二超帧号的值进行解密操作，以得到所述明文。
- [56] 其中，所述处理模块遍历所述第二超帧号的顺序为：
- [57] $X \rightarrow X-1 \rightarrow X+1 \rightarrow X-2 \rightarrow X+2 \dots \rightarrow X-M \dots \rightarrow X+N$ ；
- [58] 在所述组呼数据配置为PDCP SN 5bit且包间隔20毫秒时， M 和 N 设置为2。
- [59] 其中，所述用户设备在从所述当前小区切换至目标小区时，所述处理器发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼数据的加密参数，并且保存所述加密参数；
- [60] 所述用户设备从所述当前小区切换至所述目标小区时，所述处理器新增或复用其中一条信令携带所述当前小区会话密钥标识或直接携带所述当前小区的密钥；
- [61] 所述处理器接收到所述目标小区的加密组呼数据；
- [62] 所述控制器根据所述第二超帧号对所述目标小区的加密组呼数据进行解密操作。
- [63] 其中，所述处理器还发送所述当前小区会话密钥标识或者所述当前小区的密钥给所述目标小区的基站，所述目标小区的基站将所述当前小区会话密钥标识或者所述当前小区的密钥与所述目标小区的密钥进行比较；
- [64] 若一致，则所述处理器从所述目标小区的基站接收到所述目标小区的加密组呼数据；
- [65] 若不一致，则所述处理器从所述目标小区的基站接收到所述目标小区的加密组呼数据的同时将所述目标小区的密钥发送给所述当前小区的基站，再由所述当前小区的基站将所述目标小区的密钥发送给所述用户设备。
- [66] 其中，在所述用户设备从所述当前小区切换至目标小区时，所述处理器发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼加密参数，并且保存所述组呼加密参数；

[67] 所述处理器从所述目标小区的基站接收到所述目标小区的加密组呼数据。

[68] 本发明的有益效果是：区别于现有技术的情况，本发明所述集群组呼解密方法在用户设备从当前小区切换至目标小区时，根据用户设备在当前小区的第一超帧号推导得出目标小区的第二超帧号的合理区间范围，根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号进行遍历解密，在解密成功后根据所述第二超帧号进行解密操作，以此减小组呼业务中断时延，提高用户体验。

[69] **【附图说明】**

[70] 图1是本发明的集群组呼解密方法的流程图；

[71] 图2是图1中的具体步骤的第一实施例的流程图；

[72] 图3是图2中的具体步骤的流程图；

[73] 图4是图1中的具体步骤的第二实施例的流程图；

[74] 图5是本发明的基于集群组呼解密方法的用户设备的方框结构示意图；

[75] 图6是本发明的基于集群组呼解密方法的用户设备的硬件结构示意图。

[76] **【具体实施方式】**

[77] 下面将结合本发明实施例中的附图，对本发明所提供的各个示例性的实施例的技术方案进行清楚、完整地描述。在不冲突的情况下，下述各个实施例以及实施例中的特征可以相互组合。

[78] 请参阅图1，是本发明集群组呼解密方法的流程图。本实施例所揭示的方法应用于用户设备，该方法包括以下步骤：

[79] 步骤S1：监听在当前小区的组呼数据，并从当前小区的基站获取所述当前小区的超帧号为第一超帧号。

[80] 其中，每一基站与多个小区之间进行组呼数据传输，在本实施例中，所述当前小区与所述目标小区可以与同一个基站进行组呼数据传输，也可以与两个不同的基站进行组呼数据传输。组呼会话发起后，基站下各小区大致同步建立会话，应用加密参数发组呼码流，保证不同小区的组呼码流数目及内容相同，因此分组数据汇聚协议（Packet Data Convergence Protocol, PDCP）层的超帧号（HFN）会大致相同。

- [81] 步骤S2: 在从所述当前小区切换至目标小区时, 从所述目标小区的基站接收组呼数据并根据所述第一超帧号获得所述目标小区的超帧号的区间范围, 所述目标小区的超帧号为第二超帧号。
- [82] 其中, 所述第二超帧号为在 $[X-M, X+N]$ 的区间范围内, 其中 X 为所述第一超帧号, M 和 N 均为自然数。
- [83] 请参阅图2, 其中, 步骤S2中从所述当前小区切换至目标小区的步骤的第一实施例包括:
- [84] 步骤S21: 发起并建立组呼会话, 以使基站在建立集群业务承载时, 新增字段以携带组呼数据的加密参数, 并且保存所述加密参数。
- [85] 在作为主叫用户设备建立组呼业务时, 获取主叫用户设备标识及主叫用户所设置的区域范围信息, 并向控制装置发送请求建立呼叫的第一请求, 所述第一请求包括主叫用户设备标识、组呼业务类型和主叫用户所设置的区域范围信息。在该步骤中, 需说明的是, 主叫用户设备可为用户终端、车载终端、调度台等, 而且, 在不同控制方式的集群通信系统中, 控制装置可为控制中心或基站。
- [86] 在作为被叫用户设备接收到控制装置发送的组呼建立请求时, 所述组呼建立请求包括主叫用户设备标识、主叫用户所设置的区域范围信息、所分配的组标识和业务信道, 获取自身的位置信息, 并判断自身位置是否在所述区域范围内, 而且, 当自身位置在所述区域范围内时, 参与该组呼业务并切换到所述业务信道。在该步骤中, 需说明的是, 在不同控制方式的集群通信系统中, 组标识和业务信道可由控制中心来分配, 也可由基站来分配, 或者其中一个控制中心分配, 另一个由基站来分配。
- [87] 步骤S22: 从所述当前小区切换至所述目标小区, 新增或复用其中一条信令携带所述当前小区会话密钥标识或直接携带所述当前小区的密钥。
- [88] 其中, 会话密钥标识可使用shortMac-i。
- [89] 步骤S23: 接收到所述目标小区的加密组呼数据。
- [90] 步骤S24: 根据所述第二超帧号对所述目标小区的加密组呼数据进行解密操作。
- [91] 请参阅图3, 在步骤S22与步骤S23之间还包括步骤:

- [92] 步骤S221: 发送所述当前小区会话密钥标识或者所述当前小区的密钥给所述目标小区的基站, 所述目标小区的基站将所述当前小区会话密钥标识或者所述当前小区的密钥与所述目标小区的密钥进行比较, 判断是否一致。
- [93] 步骤S222: 若一致, 则从所述目标小区的基站接收到所述目标小区的加密组呼数据。
- [94] 步骤S223: 若不一致, 则从所述目标小区的基站接收到所述目标小区的加密组呼数据的同时将所述目标小区的密钥发送给所述当前小区的基站, 再由所述当前小区的基站将所述目标小区的密钥发送给所述用户设备。
- [95] 在所述第一实施例中, 所述用户设备以连接态从当前小区切换至目标小区。
- [96] 请参阅图4, 其中, 在步骤S2中从所述当前小区切换至目标小区的步骤的第二实施例包括:
- [97] 步骤S25: 发起并建立组呼会话, 以使基站在建立集群业务承载时, 新增字段以携带组呼加密参数, 并且保存所述组呼加密参数。
- [98] 在作为主叫用户设备建立组呼业务时, 获取主叫用户设备标识及主叫用户所设置的区域范围信息, 并向控制装置发送请求建立呼叫的第一请求, 所述第一请求包括主叫用户设备标识、组呼业务类型和主叫用户所设置的区域范围信息。在该步骤中, 需说明的是, 主叫用户设备可为用户终端、车载终端、调度台等, 而且, 在不同控制方式的集群通信系统中, 控制装置可为控制中心或基站。
- [99] 在作为被叫用户设备接收到控制装置发送的组呼建立请求时, 所述组呼建立请求包括主叫用户设备标识、主叫用户所设置的区域范围信息、所分配的组标识和业务信道, 获取自身的位置信息, 并判断自身位置是否在所述区域范围内, 而且, 当自身位置在所述区域范围内时, 参与该组呼业务并切换到所述业务信道。在该步骤中, 需说明的是, 在不同控制方式的集群通信系统中, 组标识和业务信道可由控制中心来分配, 也可由基站来分配, 或者其中一个控制中心分配, 另一个由基站来分配。
- [100] 步骤S26: 从所述目标小区的基站接收到所述目标小区的加密组呼数据。
- [101] 在所述第二实施例中, 所述用户设备以空闲态从当前小区切换至目标小区。
- [102] 步骤S3: 根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二

超帧号得到明文，并将所述明文所包括的组呼会话信息与所述当前小区的组呼数据进行比较。

[103] 其中，根据所述第二超帧号得到明文具体为：在所述 $[X-M, X+N]$ 的区间范围内改变所述第二超帧号的值，并根据改变后的所述第二超帧号的值进行解密操作，以得到所述明文。

[104] 步骤S4：若比较结果一致，则遍历所述第二超帧号解密成功，并根据所述第二超帧号进行解密操作。

[105] 其中，遍历所述第二超帧号解密成功具体为：遍历所述第二超帧号的顺序为： $X \rightarrow X-1 \rightarrow X+1 \rightarrow X-2 \rightarrow X+2 \dots \rightarrow X-M \dots \rightarrow X+N$ 。

[106] 在本实施例中，优选在所述组呼数据配置为PDCP SN 5bit且包间隔20毫秒时，M和N设置为2，其它组呼配置为1，当然越大越可靠，但是耗时相应增大。

[107] 其中，解密的输入参数为超帧号、密钥、组呼数据密文块、加密算法及其它参数，对于不同小区只有超帧号可能不同，所以固定不变参数，通过只改变超帧号值的方式进行标准的解密流程，得到明文，并将明文所包含的组呼会话信息与用户设备在当前小区的组呼上下文进行比对，如果比对结果一致，遍历超帧号解密流程结束，认为该超帧号值为有效值，此后维护此超帧号值进行解密操作。

[108] 所述集群组呼解密方法在用户设备从当前小区切换至目标小区时，根据用户设备在当前小区的第一超帧号推导得出目标小区的第二超帧号的合理区间范围，并根据所述第二超帧号进行遍历解密，以此减小组呼业务中断时延，提高用户体验。

[109] 请参阅图5，为本发明的基于集群组呼解密方法的用户设备的方框结构示意图。所述用户设备包括建立模块10、密钥模块20、监听模块30、收发模块40及处理模块50。

[110] 所述监听模块30用于监听用户设备在当前小区的组呼数据，并从所述当前小区的基站获取所述当前小区的超帧号为第一超帧号。

[111] 其中，每一基站与多个小区之间进行组呼数据传输，在本实施例中，所述当前

小区与所述目标小区可以与同一个基站进行组呼数据传输，也可以与两个不同的基站进行组呼数据传输。组呼会话发起后，基站下各小区大致同步建立会话，应用加密参数发组呼码流，保证不同小区的组呼码流数目及内容相同，因此分组数据汇聚协议（Packet Data Convergence Protocol, PDCP）层的超帧号（HFN）会大致相同。

[112] 所述收发模块40用于用户设备在从所述当前小区切换至目标小区时，从所述目标小区的基站接收组呼数据并根据所述第一超帧号获得所述目标小区的超帧号的区间范围，所述目标小区的超帧号为第二超帧号。

[113] 其中，所述第二超帧号为在 $[X-M, X+N]$ 的区间范围内，其中 X 为所述第一超帧号， M 和 N 均为自然数。

[114] 其中，从所述当前小区切换至目标小区的第一实施例包括：

[115] 所述建立模块10用于发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼数据的加密参数，并且保存所述加密参数。

[116] 在作为主叫用户设备建立组呼业务时，获取主叫用户设备标识及主叫用户所设置的区域范围信息，并向控制装置发送请求建立呼叫的第一请求，所述第一请求包括主叫用户设备标识、组呼业务类型和主叫用户所设置的区域范围信息。在该步骤中，需说明的是，主叫用户设备可为用户终端、车载终端、调度台等，而且，在不同控制方式的集群通信系统中，控制装置可为控制中心或基站。

[117] 在作为被叫用户设备接收到控制装置发送的组呼建立请求时，所述组呼建立请求包括主叫用户设备标识、主叫用户所设置的区域范围信息、所分配的组标识和业务信道，获取自身的位置信息，并判断自身位置是否在所述区域范围内，而且，当自身位置在所述区域范围内时，参与该组呼业务并切换到所述业务信道。在该步骤中，需说明的是，在不同控制方式的集群通信系统中，组标识和业务信道可由控制中心来分配，也可由基站来分配，或者其中一个控制中心分配，另一个由基站来分配。

[118] 密钥模块20用于用户设备从所述当前小区切换至所述目标小区时，新增或复用其中一条信令携带所述当前小区会话密钥标识或直接携带所述当前小区的密钥。

- [119] 其中，会话密钥标识可使用shortMac-i。
- [120] 所述收发模块40接收到所述目标小区的加密组呼数据。
- [121] 所述处理模块50用于根据所述第二超帧号对所述目标小区的加密组呼数据进行解密操作。
- [122] 所述密钥模块20还用于发送所述当前小区会话密钥标识或者所述当前小区的密钥给所述目标小区的基站，所述目标小区的基站将所述当前小区会话密钥标识或者所述当前小区的密钥与所述目标小区的密钥进行比较。
- [123] 若一致，则所述收发模块40从所述目标小区的基站接收到所述目标小区的加密组呼数据。
- [124] 若不一致，则所述收发模块40从所述目标小区的基站接收到所述目标小区的加密组呼数据的同时将所述目标小区的密钥发送给所述当前小区的基站，再由所述当前小区的基站将所述目标小区的密钥发送给所述用户设备。
- [125] 在所述第一实施例中，所述用户设备以连接态从当前小区切换至目标小区。
- [126] 其中，从所述当前小区切换至目标小区的第二实施例包括：
- [127] 所述建立模块10用于发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼加密参数，并且保存所述组呼加密参数。
- [128] 在作为主叫用户设备建立组呼业务时，获取主叫用户设备标识及主叫用户所设置的区域范围信息，并向控制装置发送请求建立呼叫的第一请求，所述第一请求包括主叫用户设备标识、组呼业务类型和主叫用户所设置的区域范围信息。在该步骤中，需说明的是，主叫用户设备可为用户终端、车载终端、调度台等，而且，在不同控制方式的集群通信系统中，控制装置可为控制中心或基站。
- [129] 在作为被叫用户设备接收到控制装置发送的组呼建立请求时，所述组呼建立请求包括主叫用户设备标识、主叫用户所设置的区域范围信息、所分配的组标识和业务信道，获取自身的位置信息，并判断自身位置是否在所述区域范围内，而且，当自身位置在所述区域范围内时，参与该组呼业务并切换到所述业务信道。在该步骤中，需说明的是，在不同控制方式的集群通信系统中，组标识和业务信道可由控制中心来分配，也可由基站来分配，或者其中一个控制中心分配，另一个由基站来分配。

- [130] 所述收发模块40用于从所述目标小区的基站接收到所述目标小区的加密组呼数据。
- [131] 在所述第二实施例中，所述用户设备以空闲态从当前小区切换至目标小区。
- [132] 所述处理模块50用于根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号得到明文，并将所述明文所包括的组呼会话信息与所述当前小区的组呼数据进行比较。
- [133] 其中，根据所述第二超帧号得到明文具体为：在所述 $[X-M, X+N]$ 的区间范围内改变所述第二超帧号的值，并根据改变后的所述第二超帧号的值进行解密操作，以得到所述明文。
- [134] 若比较结果一致，则所述处理模块50遍历所述第二超帧号解密成功，并根据所述第二超帧号进行解密操作。
- [135] 其中，遍历所述第二超帧号解密成功具体为：遍历所述第二超帧号的顺序为： $X \rightarrow X-1 \rightarrow X+1 \rightarrow X-2 \rightarrow X+2 \dots \rightarrow X-M \dots \rightarrow X+N$ 。
- [136] 在所述组呼数据配置为PDCP SN 5bit且包间隔20毫秒时，M和N设置为2，其它组呼配置为1，当然越大越可靠，但是耗时相应增大。
- [137] 其中，解密的输入参数为超帧号、密钥、组呼数据密文块、加密算法及其它参数，对于不同小区只有超帧号可能不同，所以固定不变参数，通过只改变超帧号值的方式进行标准的解密流程，得到明文，并将明文所包含的组呼会话信息与用户设备在当前小区的组呼上下文进行比对，如果比对结果一致，遍历超帧号解密流程结束，认为该超帧号值为有效值，此后维护此超帧号值进行解密操作。
- [138] 本发明实施例的用户设备的上述模块对应执行上述实施例的基于集群组呼解密的方法，具有与其相同的技术效果。
- [139] 应该理解到，上述模块的划分为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如两个模块可以集成到另一个系统中，或一些特征可以忽略，或不执行。另外，模块相互之间的连接可以通过一些接口，也可以是电性或其它形式。上述模块既可以采用软件功能框的形式实现，也可以采用例如图6所示的硬件的形式实现。

[140] 请参阅图6, 是本发明基于集群组呼解密方法的用户设备的硬件结构示意图。

所述用户设备包括存储器110、处理器120、控制器130及通信总线140。通信总线140用于处理器120调用各种数据, 存储器110用于存储程序指令。为了方便说明, 图6所示处理器120、存储器110、通信总线140及控制器130的数量均为一个。

[141] 其中, 所述存储器110将建立模块10、密钥模块20、监听模块30、收发模块40及处理模块50的所有程序指令进行存储。

[142] 所述处理器120监听用户设备在当前小区的组呼数据, 并从所述当前小区的基站获取所述当前小区的超帧号为第一超帧号。

[143] 其中, 每一基站与多个小区之间进行组呼数据传输, 在本实施例中, 所述当前小区与所述目标小区可以与同一个基站进行组呼数据传输, 也可以与两个不同的基站进行组呼数据传输。组呼会话发起后, 基站下各小区大致同步建立会话, 应用加密参数发组呼码流, 保证不同小区的组呼码流数目及内容相同, 因此分组数据汇聚协议 (Packet Data Convergence Protocol, PDCP) 层的超帧号 (HFN) 会大致相同。

[144] 所述处理器120在用户设备从所述当前小区切换至目标小区时, 从所述目标小区的基站接收组呼数据并根据所述第一超帧号获得所述目标小区的超帧号的区间范围, 所述目标小区的超帧号为第二超帧号。

[145] 其中, 所述第二超帧号为在 $[X-M, X+N]$ 的区间范围内, 其中 X 为所述第一超帧号, M 和 N 均为自然数。

[146] 其中, 用户设备从所述当前小区切换至目标小区的第一实施例包括:

[147] 处理器120发起并建立组呼会话, 以使基站在建立集群业务承载时, 新增字段以携带组呼数据的加密参数, 并且保存所述加密参数。

[148] 在作为主叫用户设备建立组呼业务时, 获取主叫用户设备标识及主叫用户所设置的区域范围信息, 并向控制装置发送请求建立呼叫的第一请求, 所述第一请求包括主叫用户设备标识、组呼业务类型和主叫用户所设置的区域范围信息。在该步骤中, 需说明的是, 主叫用户设备可为用户终端、车载终端、调度台等, 而且, 在不同控制方式的集群通信系统中, 控制装置可为控制中心或基站。

- [149] 在作为被叫用户设备接收到控制装置发送的组呼建立请求时，所述组呼建立请求包括主叫用户设备标识、主叫用户所设置的区域范围信息、所分配的组标识和业务信道，获取自身的位置信息，并判断自身位置是否在所述区域范围内，而且，当自身位置在所述区域范围内时，参与该组呼业务并切换到所述业务信道。在该步骤中，需说明的是，在不同控制方式的集群通信系统中，组标识和业务信道可由控制中心来分配，也可由基站来分配，或者其中一个控制中心分配，另一个由基站来分配。
- [150] 用户设备从所述当前小区切换至所述目标小区时，所述处理器120新增或复用其中一条信令携带所述当前小区会话密钥标识或直接携带所述当前小区的密钥。
- [151] 其中，会话密钥标识可使用shortMac-i。
- [152] 所述处理器120接收到所述目标小区的加密组呼数据。
- [153] 所述控制器130用于根据所述第二超帧号对所述目标小区的加密组呼数据进行解密操作。
- [154] 所述处理器120还发送所述当前小区会话密钥标识或者所述当前小区的密钥给所述目标小区的基站，所述目标小区的基站将所述当前小区会话密钥标识或者所述当前小区的密钥与所述目标小区的密钥进行比较。
- [155] 若一致，则所述处理器120从所述目标小区的基站接收到所述目标小区的加密组呼数据。
- [156] 若不一致，则所述处理器120从所述目标小区的基站接收到所述目标小区的加密组呼数据的同时将所述目标小区的密钥发送给所述当前小区的基站，再由所述当前小区的基站将所述目标小区的密钥发送给所述用户设备。
- [157] 在所述第一实施例中，所述用户设备以连接态从当前小区切换至目标小区。
- [158] 其中，用户设备从所述当前小区切换至目标小区的第二实施例包括：
- [159] 所述处理器120发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼加密参数，并且保存所述组呼加密参数。
- [160] 在作为主叫用户设备建立组呼业务时，获取主叫用户设备标识及主叫用户所设置的区域范围信息，并向控制装置发送请求建立呼叫的第一请求，所述第一请

求包括主叫用户设备标识、组呼业务类型和主叫用户所设置的区域范围信息。
在该步骤中，需说明的是，主叫用户设备可为用户终端、车载终端、调度台等，而且，在不同控制方式的集群通信系统中，控制装置可为控制中心或基站。

[161] 在作为被叫用户设备接收到控制装置发送的组呼建立请求时，所述组呼建立请求包括主叫用户设备标识、主叫用户所设置的区域范围信息、所分配的组标识和业务信道，获取自身的位置信息，并判断自身位置是否在所述区域范围内，而且，当自身位置在所述区域范围内时，参与该组呼业务并切换到所述业务信道。在该步骤中，需说明的是，在不同控制方式的集群通信系统中，组标识和业务信道可由控制中心来分配，也可由基站来分配，或者其中一个控制中心分配，另一个由基站来分配。

[162] 所述处理器120从所述目标小区的基站接收到所述目标小区的加密组呼数据。

[163] 在所述第二实施例中，所述用户设备以空闲态从当前小区切换至目标小区。

[164] 所述控制器130用于根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号得到明文，并将所述明文所包括的组呼会话信息与所述当前小区的组呼数据进行比较。

[165] 其中，根据所述第二超帧号得到明文具体为：在所述 $[X-M, X+N]$ 的区间范围内改变所述第二超帧号的值，并根据改变后的所述第二超帧号的值进行解密操作，以得到所述明文。

[166] 若比较结果一致，则所述控制器130遍历所述第二超帧号解密成功，并根据所述第二超帧号进行解密操作。

[167] 其中，遍历所述第二超帧号解密成功具体为：遍历所述第二超帧号的顺序为： $X \rightarrow X-1 \rightarrow X+1 \rightarrow X-2 \rightarrow X+2 \dots \rightarrow X-M \dots \rightarrow X+N$ 。

[168] 在所述组呼数据配置为PDCP SN 5bit且包间隔20毫秒时，M和N设置为2，其它组呼配置为1，当然越大越可靠，但是耗时相应增大。

[169] 其中，解密的输入参数为超帧号、密钥、组呼数据密文块、加密算法及其它参数，对于不同小区只有超帧号可能不同，所以固定不变参数，通过只改变超帧号值的方式进行标准的解密流程，得到明文，并将明文所包含的组呼会话信息与用户设备在当前小区的组呼上下文进行比对，如果比对结果一致，遍历超帧

号解密流程结束，认为该超帧号值为有效值，此后维护此超帧号值进行解密操作。

[170] 所述集群组呼解密方法在用户设备从当前小区切换至目标小区时，根据用户设备在当前小区的第一超帧号推导得出目标小区的第二超帧号的合理区间范围，根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号进行遍历解密，在解密成功后根据所述第二超帧号进行解密操作，以此减小组呼业务中断时延，提高用户体验。

[171] 以上仅为本发明的实施方式，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

权利要求书

- [权利要求 1] 一种集群组呼解密方法，其中，所述方法应用于用户设备，包括：
- 监听在当前小区的组呼数据，并从所述当前小区的基站获取所述当前小区的超帧号为第一超帧号；
- 在从所述当前小区切换至目标小区时，从所述目标小区的基站接收组呼数据并根据所述第一超帧号获得所述目标小区的超帧号的区间范围，所述目标小区的超帧号为第二超帧号；
- 根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号得到明文，并将所述明文所包括的组呼会话信息与所述当前小区的组呼数据进行比较；
- 若比较结果一致，则遍历所述第二超帧号解密成功，并根据所述第二超帧号进行解密操作。
- [权利要求 2] 根据权利要求1所述的集群组呼解密方法，其中，从所述目标小区的基站接收组呼数据并根据所述第一超帧号获得所述目标小区的超帧号的区间范围的步骤包括：
- 所述第二超帧号为在 $[X-M, X+N]$ 的区间范围内，其中 X 为所述第一超帧号， M 和 N 均为自然数；
- 根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号得到明文的步骤包括：
- 在所述 $[X-M, X+N]$ 的区间范围内改变所述第二超帧号的值，并根据改变后的所述第二超帧号的值进行解密操作，以得到所述明文。
- [权利要求 3] 根据权利要求2所述的集群组呼解密方法，其中，遍历所述第二超帧号解密成功，并根据所述第二超帧号进行解密操作的步骤包括：
- 遍历所述第二超帧号的顺序为：
- $X \rightarrow X-1 \rightarrow X+1 \rightarrow X-2 \rightarrow X+2 \dots \rightarrow X-M \dots \rightarrow X+N$ 。

- [权利要求 4] 根据权利要求2所述的集群组呼解密方法，其中，在所述组呼数据配置为PDCP SN 5bit且包间隔20毫秒时，M和N设置为2。
- [权利要求 5] 根据权利要求1所述的集群组呼解密方法，其中，所述从所述当前小区切换至目标小区的步骤包括：
发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼数据的加密参数，并且保存所述加密参数；
从所述当前小区切换至所述目标小区，新增或复用其中一条信令携带所述当前小区会话密钥标识或直接携带所述当前小区的密钥；
接收到所述目标小区的加密组呼数据；
所述根据所述第二超帧号进行解密操作的步骤包括：
根据所述第二超帧号对所述目标小区的加密组呼数据进行解密操作。
- [权利要求 6] 根据权利要求5所述的集群组呼解密方法，其中，在接收到所述目标小区的加密组呼数据的步骤之前，所述方法进一步包括：
发送所述当前小区会话密钥标识或者所述当前小区的密钥给所述目标小区的基站，所述目标小区的基站将所述当前小区会话密钥标识或者所述当前小区的密钥与所述目标小区的密钥进行比较；
若一致，则从所述目标小区的基站接收到所述目标小区的加密组呼数据；
若不一致，则从所述目标小区的基站接收到所述目标小区的加密组呼数据的同时将所述目标小区的密钥发送给所述当前小区的基站，再由所述当前小区的基站将所述目标小区的密钥发送给所述用户设备。
- [权利要求 7] 根据权利要求1所述的集群组呼解密方法，其中，所述从所述当前小区切换至目标小区的步骤包括：
发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼加密参数，并且保存所述组呼加密参数；

从所述目标小区的基站接收到所述目标小区的加密组呼数据。

[权利要求 8]

一种用户设备，其中，所述用户设备包括：

监听模块，用于监听用户设备在当前小区的组呼数据，并从所述当前小区的基站获取所述当前小区的超帧号为第一超帧号；

收发模块，用于在所述用户设备从所述当前小区切换至目标小区时，从所述目标小区的基站接收组呼数据并根据所述第一超帧号获得所述目标小区的超帧号的区间范围，所述目标小区的超帧号为第二超帧号；

处理模块，连接所述监听模块及所述收发模块，用于根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号得到明文，并将所述明文所包括的组呼会话信息与所述当前小区的组呼数据进行比较，若比较结果一致，则遍历所述第二超帧号解密成功，并根据所述第二超帧号进行解密操作。

[权利要求 9]

根据权利要求8所述的用户设备，其中，所述第二超帧号为在 $[X-M, X+N]$ 的区间范围内，其中 X 为所述第一超帧号， M 和 N 均为自然数；在所述 $[X-M, X+N]$ 的区间范围内改变所述第二超帧号的值，所述处理模块根据改变后的所述第二超帧号的值进行解密操作，以得到所述明文。

[权利要求 10]

根据权利要求9所述的用户设备，其中，所述处理模块遍历所述第二超帧号的顺序为：

$X \rightarrow X-1 \rightarrow X+1 \rightarrow X-2 \rightarrow X+2 \dots \rightarrow X-M \dots \rightarrow X+N$ 。

[权利要求 11]

根据权利要求10所述的用户设备，其中，在所述组呼数据配置为PDCP SN 5bit且包间隔20毫秒时， M 和 N 设置为2。

[权利要求 12]

根据权利要求9所述的用户设备，其中，所述用户设备还包括建立模块及密钥模块，所述用户设备在从所述当前小区切换至目标小区时，所述建立模块发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼数据的加密参数，并且保存所述加密参数；

所述用户设备从所述当前小区切换至所述目标小区时，所述密钥模块新增或复用其中一条信令携带所述当前小区会话密钥标识或直接携带所述当前小区的密钥；

所述收发模块接收到所述目标小区的加密组呼数据；

所述处理模块根据所述第二超帧号对所述目标小区的加密组呼数据进行解密操作。

[权利要求 13]

根据权利要求12所述的设备，其中，所述密钥模块还发送所述当前小区会话密钥标识或者所述当前小区的密钥给所述目标小区的基站，所述目标小区的基站将所述当前小区会话密钥标识或者所述当前小区的密钥与所述目标小区的密钥进行比较；

若一致，则所述收发模块从所述目标小区的基站接收到所述目标小区的加密组呼数据；

若不一致，则从所述目标小区的基站接收到所述目标小区的加密组呼数据的同时将所述目标小区的密钥发送给所述当前小区的基站，再由所述当前小区的基站将所述目标小区的密钥发送给所述用户设备。

[权利要求 14]

根据权利要求8所述的设备，其中，所述用户设备还包括建立模块，在所述用户设备从所述当前小区切换至目标小区时，所述建立模块发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼加密参数，并且保存所述组呼加密参数；所述收发模块从所述目标小区的基站接收到所述目标小区的加密组呼数据。

[权利要求 15]

一种用户设备，其中，所述用户设备包括：

存储器，用于存储程序指令；

处理器，用于监听用户设备在当前小区的组呼数据，并从所述当前小区的基站获取所述当前小区的超帧号为第一超帧号；

所述处理器，还用于在所述用户设备从所述当前小区切换至目标小区时，从所述目标小区的基站接收组呼数据并根据所述第一超

帧号获得所述目标小区的超帧号的区间范围，所述目标小区的超帧号为第二超帧号；

控制器，用于根据所述第二超帧号的区间范围遍历所述第二超帧号并根据所述第二超帧号得到明文，并将所述明文所包括的组呼会话信息与所述当前小区的组呼数据进行比较，若比较结果一致，则遍历所述第二超帧号解密成功，并根据所述第二超帧号进行解密操作。

[权利要求 16]

根据权利要求15所述的电子设备，其中，所述第二超帧号为在 $[X-M, X+N]$ 的区间范围内，其中 X 为所述第一超帧号， M 和 N 均为自然数；在所述 $[X-M, X+N]$ 的区间范围内改变所述第二超帧号的值，所述处理模块根据改变后的所述第二超帧号的值进行解密操作，以得到所述明文。

[权利要求 17]

根据权利要求16所述的电子设备，其中，所述处理模块遍历所述第二超帧号的顺序为：

$X \rightarrow X-1 \rightarrow X+1 \rightarrow X-2 \rightarrow X+2 \dots \rightarrow X-M \dots \rightarrow X+N$ ；

在所述组呼数据配置为PDCP SN 5bit且包间隔20毫秒时， M 和 N 设置为2。

[权利要求 18]

根据权利要求15所述的电子设备，其中，所述用户在从所述当前小区切换至目标小区时，所述处理器发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼数据的加密参数，并且保存所述加密参数；

所述用户设备从所述当前小区切换至所述目标小区时，所述处理器新增或复用其中一条信令携带所述当前小区会话密钥标识或直接携带所述当前小区的密钥；

所述处理器接收到所述目标小区的加密组呼数据；

所述控制器根据所述第二超帧号对所述目标小区的加密组呼数据进行解密操作。

[权利要求 19]

根据权利要求18所述的电子设备，其中，所述处理器还发送所述

当前小区会话密钥标识或者所述当前小区的密钥给所述目标小区的基站，所述目标小区的基站将所述当前小区会话密钥标识或者所述当前小区的密钥与所述目标小区的密钥进行比较；

若一致，则所述处理器从所述目标小区的基站接收到所述目标小区的加密组呼数据；

若不一致，则所述处理器从所述目标小区的基站接收到所述目标小区的加密组呼数据的同时将所述目标小区的密钥发送给所述当前小区的基站，再由所述当前小区的基站将所述目标小区的密钥发送给所述用户设备。

[权利要求 20]

根据权利要求15所述的设备，其中，在所述用户设备从所述当前小区切换至目标小区时，所述处理器发起并建立组呼会话，以使基站在建立集群业务承载时，新增字段以携带组呼加密参数，并且保存所述组呼加密参数；

所述处理器从所述目标小区的基站接收到所述目标小区的加密组呼数据。

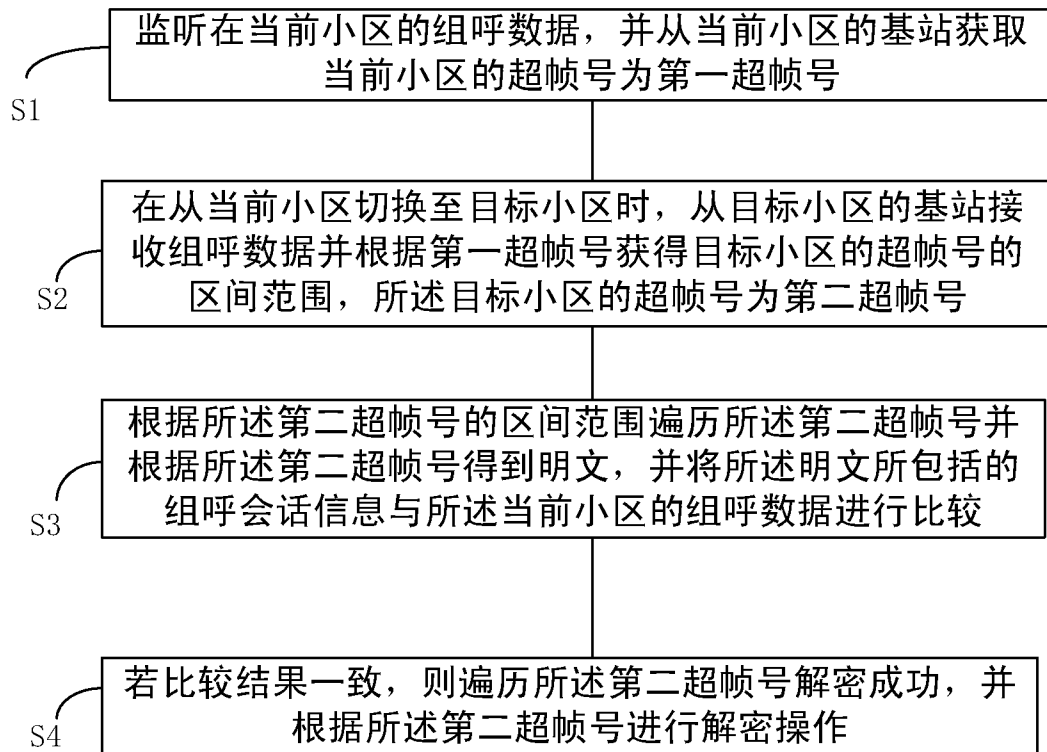


图 1

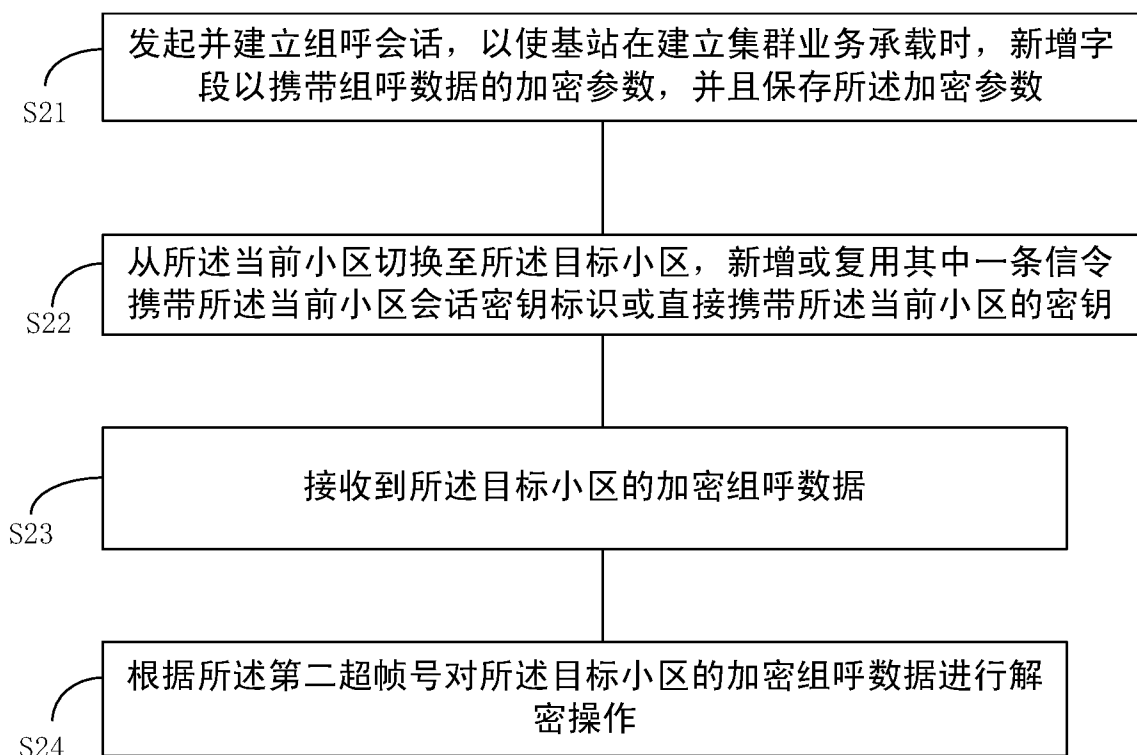


图 2

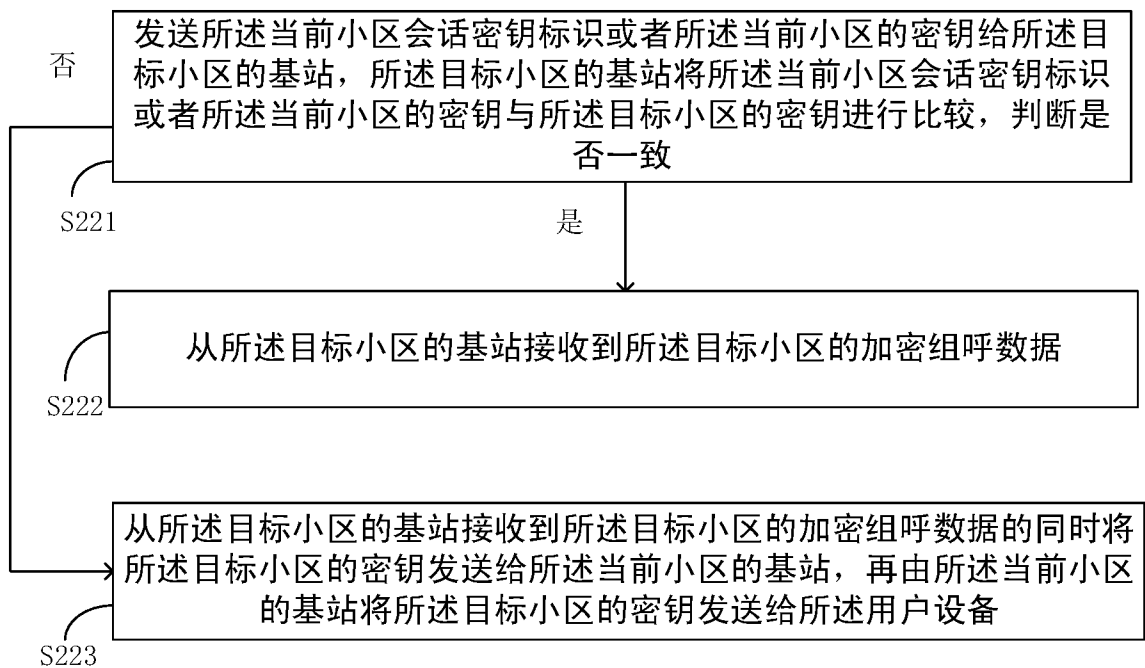


图 3

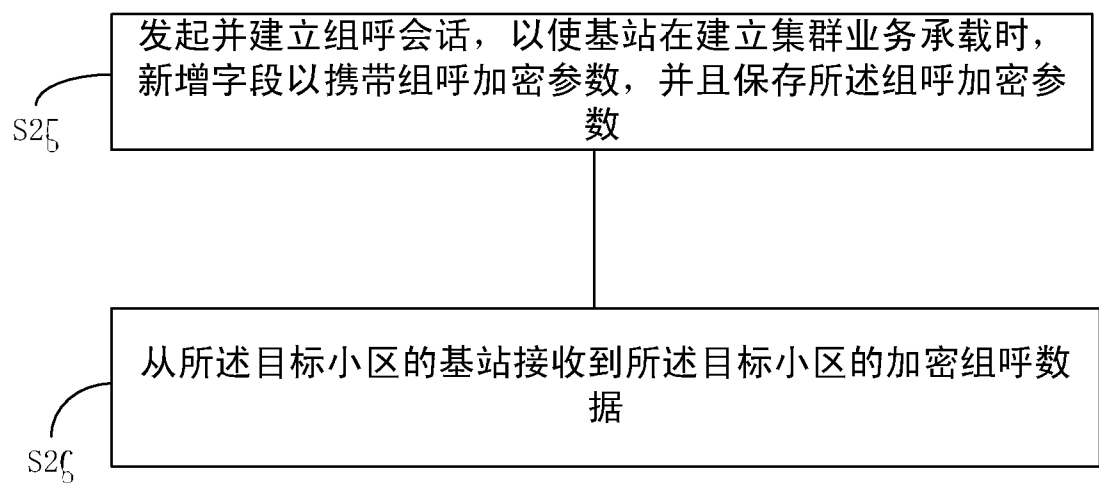


图 4

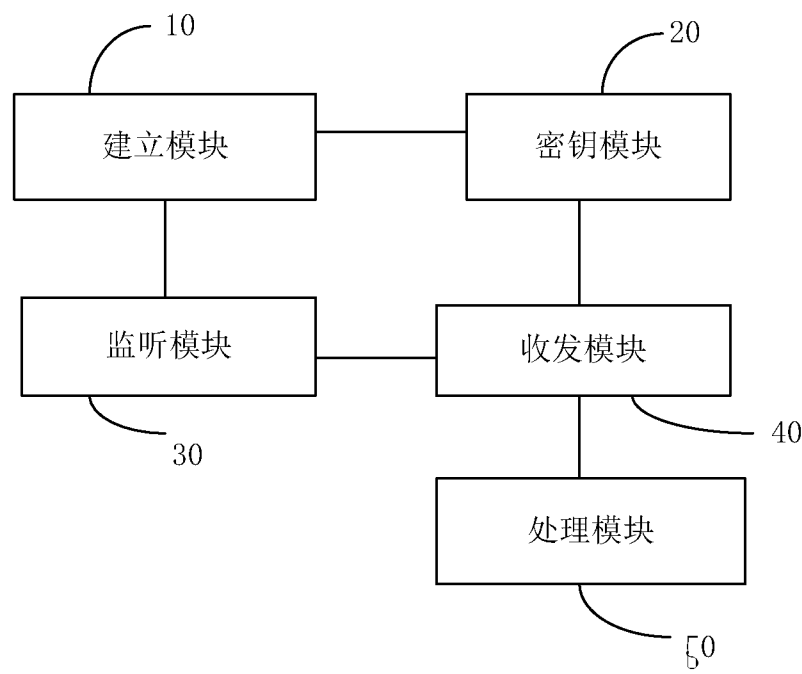


图 5

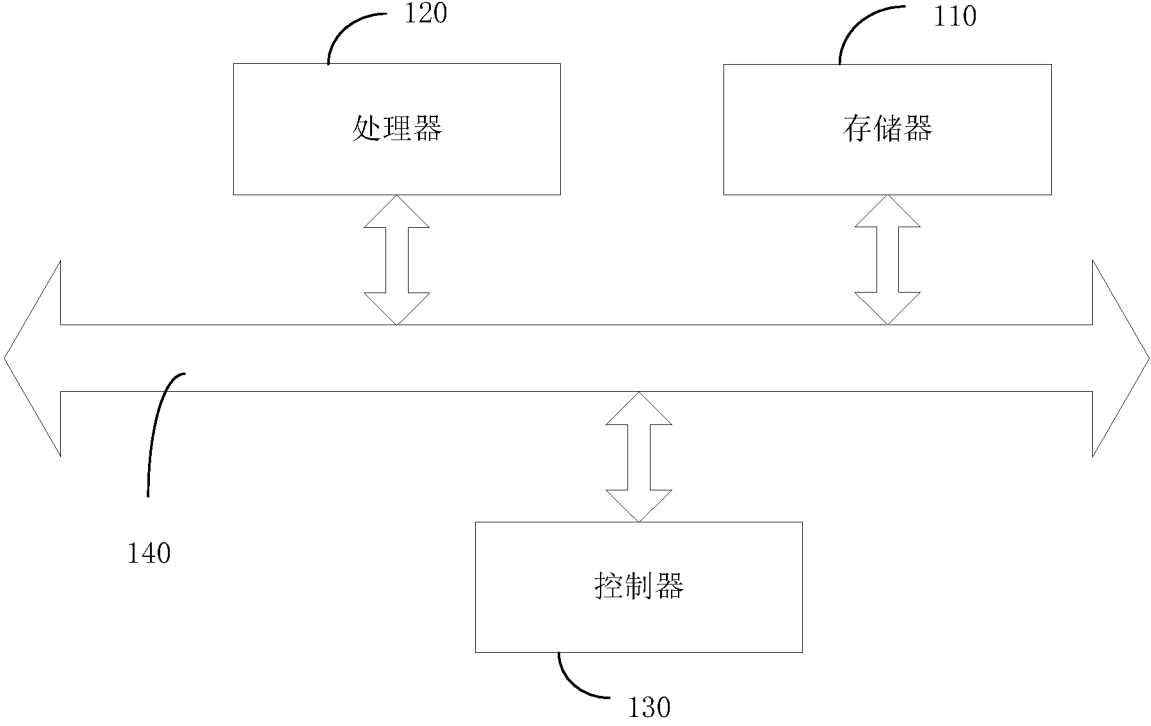


图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/070744

A. CLASSIFICATION OF SUBJECT MATTER

H04W 36/08 (2009.01) i; H04W 36/34 (2009.01) i; H04L 29/02 (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)

H04W; H04L; H04B

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)

EPODOC, WPI, CNPAT, CNKI: 集群, 组呼, 小区, 超帧, 号, 目标, 解密, 切换, 时延, cluster, group, call, cell, area, hyperframe, superframe, HFN, target, decipher, decrypt, switch+, handover, delay

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101729377 A (HUAWEI TECHNOLOGIES CO., LTD.), 09 June 2010 (09.06.2010), description, paragraphs [0040]-[0045] and [0093]-[0108], and figures 2 and 8	1-20
A	CN 104853388 A (SICHUAN UNIVERSITY), 19 August 2015 (19.08.2015), entire document	1-20
A	CN 104684030 A (POTEVIO INSTITUTE OF TECHNOLOGY CO., LTD.), 03 June 2015 (03.06.2015), entire document	1-20
A	WO 2009045160 A1 (TELEFONAKTIEBOLAGET L M ERICSSON PUBL), 09 April 2009 (09.04.2009), entire document	1-20

☐ 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 September 2017	Date of mailing of the international search report 27 September 2017
Name and mailing address of the ISA 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 CHEN, Sheng Telephone No. (86-10) 62413284

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/070744

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101729377 A	09 June 2010	None	
CN 104853388 A	19 August 2015	None	
CN 104684030 A	03 June 2015	None	
WO 2009045160 A1	09 April 2009	US 2010265912 A1	21 October 2010
		EP 2195977 A1	16 June 2010

国际检索报告

国际申请号

PCT/CN2017/070744

A. 主题的分类

H04W 36/08(2009.01)i; H04W 36/34(2009.01)i; H04L 29/02(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)

H04W; H04L; H04B

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))

EPODOC, WPI, CNPAT, CNKI; 集群, 组呼, 小区, 超帧, 号, 目标, 解密, 切换, 时延, cluster, group, call, cell, area, hyperframe, superframe, HFN, target, decipher, decrypt, switch+, handover, delay

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	CN 101729377 A (华为技术有限公司) 2010年 6月 9日 (2010 - 06 - 09) 说明书第[0040]-[0045]、[0093]-[0108]段, 图2、8	1-20
A	CN 104853388 A (四川大学) 2015年 8月 19日 (2015 - 08 - 19) 全文	1-20
A	CN 104684030 A (普天信息技术研究院有限公司) 2015年 6月 3日 (2015 - 06 - 03) 全文	1-20
A	WO 2009045160 A1 (TELEFONAKTIEBOLAGET L M ERICSSON PUBL) 2009年 4月 9日 (2009 - 04 - 09) 全文	1-20

☐ 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

2017年 9月 15日

国际检索报告邮寄日期

2017年 9月 27日

ISA/CN的名称和邮寄地址

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

陈昇

电话号码 (86-10)62413284

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2017/070744

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	101729377	A	2010年 6月 9日	无			
CN	104853388	A	2015年 8月 19日	无			
CN	104684030	A	2015年 6月 3日	无			
WO	2009045160	A1	2009年 4月 9日	US	2010265912	A1	2010年 10月 21日
				EP	2195977	A1	2010年 6月 16日

表 PCT/ISA/210 (同族专利附件) (2009年7月)