(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105323231 B
(45)授权公告日 2019.04.23

(21)申请号 201410375477.8

(22)申请日 2014.07.31

(65)同一申请的已公布的文献号
申请公布号 CN 105323231 A

(43)申请公布日 2016.02.10

(73)专利权人 中兴通讯股份有限公司
地址 518057 广东省深圳市南山区科技南路55号

(72)发明人 魏铮 佟志新 韩成延

(74)专利代理机构 北京康信知识产权代理有限责任公司 11240
代理人 余刚 梁丽超

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

(56)对比文件
CN 101001252 A,2007.07.18,
CN 1599485 A,2005.03.23,
CN 101883346 A,2010.11.10,
CN 101128061 A,2008.02.20,
CN 102487502 A,2012.06.06,

审查员 叶坚

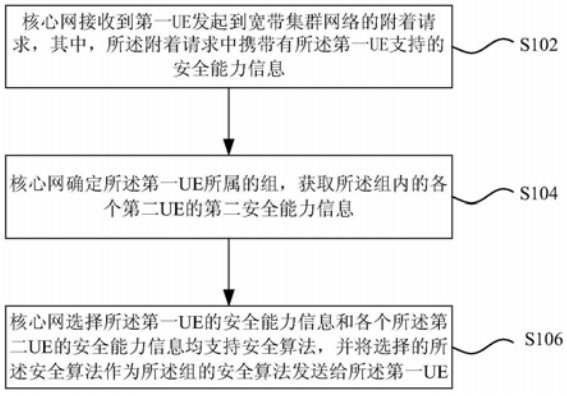
权利要求书2页 说明书6页 附图3页

(54)发明名称

安全算法选择方法、装置及系统

(57)摘要

本发明公开了一种安全算法选择方法、装置及系统。其中，该方法包括：核心网接收到第一终端UE发起到宽带集群网络的附着请求，其中，所述附着请求中携带有所述UE支持的第一安全能力信息；所述核心网确定所述第一UE所属的组，获取所述组内的各个第二UE的安全能力信息；所述核心网选择所述第一UE的安全能力信息和所述各个第二UE的安全能力信息均支持安全算法，并将选择的所述安全算法作为所述组的安全算法发送给所述第一UE。



CN 105323231 B

1.一种安全算法选择方法,其特征在于,包括:

核心网接收到第一UE发起到宽带集群网络的附着请求,其中,所述附着请求中携带有所述第一UE支持的第一安全能力信息;

所述核心网确定所述第一UE所属的组,获取所述组内的各个第二UE的安全能力信息;

所述核心网选择所述第一UE的安全能力信息和各个所述第二UE的安全能力信息均支持安全算法,并将选择的所述安全算法作为所述组的安全算法发送给所述第一UE。

2.根据权利要求1所述的方法,其特征在于,所述方法还包括:

所述核心网确定选择的所述安全算法与保存的所述组的安全算法不相同,则将所述组的安全算法更新为选择的所述安全算法,并将选择的所述安全算法为所述组的安全算法发送给所述组内的各个所述第二UE。

3.根据权利要求2所述的方法,其特征在于,将选择的所述安全算法为所述组的安全算法发送给所述组内的各个所述第二UE,包括:所述核心网向各个所述第二UE发送组信息更新消息,所述组信息更新消息中携带选择的所述安全算法。

4.根据权利要求1所述的方法,其特征在于,核心网接收到第一UE发起到宽带集群网络的附着请求之后,所述方法还包括:所述核心网保存所述第一UE的安全能力信息。

5.根据权利要求1所述的方法,其特征在于,所述核心网选择所述第一UE的安全能力信息和各个所述第二UE的安全能力信息均支持安全算法,包括:所述核心网根据所述第一U E安全能力信息判断所述第一UE是否支持当前所述组的安全算法,如果是,则选择当前所述组的安全算法,否则,取所述第一UE安全能力信息与各个所述第二UE的安全能力信息的交集,选择所述交集支持的一个安全算法。

6.根据权利要求1至5中任一项所述的方法,其特征在于,所述方法还包括:

所述核心网在发起所述组的组呼业务时,将选择的所述安全算法及对应的密钥通知到基站,指示所述基站在进行所述组呼业务传递时,使用所述安全算法及密钥对信令和业务数据进行加密。

7.一种安全算法选择装置,其特征在于,包括:

接收模块,用于第一UE发起到宽带集群网络的附着请求,其中,所述附着请求中携带有所述第一UE支持的安全能力信息;

获取模块,用于确定所述第一UE所属的组,获取所述组内的各个第二UE的安全能力信息;

选择模块,用于选择所述第一UE安全能力信息和各个所述第二UE的安全能力信息均支持安全算法;

发送模块,用于将选择的所述安全算法作为所述组的安全算法发送给所述第一UE。

8.根据权利要求7所述的装置,其特征在于,所述装置还包括:

判断模块,用于判断选择的所述安全算法与保存的所述组的安全算法是否相同,如果不同,则触发更新模块;

所述更新模块,用于将所述组的安全算法更新为选择的所述安全算法,并将选择的所述安全算法发送给所述组内的各个所述第二UE。

9.根据权利要求7所述的装置,其特征在于,所述装置还包括:存储模块,用于保存所述第一UE的安全能力信息。

10.根据权利要求7所述的装置，其特征在于，所述选择模块包括：

判断单元，用于根据所述第一UE的安全能力信息判断所述第一UE是否支持当前所述组的安全算法；

选择单元，用于在所述判断单元的判断结果为是的情况下，选择当前所述组的安全算法，以及在所述判断单元的判断结果为否的情况下，取所述第一UE的安全能力信息与各个所述第二UE的安全能力信息的交集，选择所述交集支持的一个安全算法。

11.根据权利要求7至10中任一项所述的装置，其特征在于，所述装置还包括：

通知模块，用于在发起所述组的组呼业务时，将选择的所述安全算法及对应的密钥通知到基站，指示所述基站在进行所述组呼业务传递时，使用所述安全算法及密钥对信令和业务数据进行加密。

12.一种安全算法选择系统，其特征在于，包括：核心网和基站，其中，

所述核心网包括权利要求11所述的装置；

所述基站，用于按照所述核心网通知的组的安全算法及对应的密钥，在进行所述组的组呼业务传递时，使用所述安全算法及密钥对信令和业务数据进行加密。

安全算法选择方法、装置及系统

技术领域

[0001] 本发明涉及通信领域，具体而言，涉及一种安全算法选择方法、装置及系统。

背景技术

[0002] 在LTE系统中，为保证数据业务的安全性要求，协议中定义了一套安全加密的机制，即终端在附着时上报终端(UE)支持的安全加密的算法到核心网，核心网接收后将UE的安全能力信息以及其计算的根密钥信息传给基站，基站接收后根据UE的能力和基站支持能力为当前终端业务选择一套安全加密算法，并以核心网传递过来的根密钥计算一套密钥，用于后续业务数据的加密。

[0003] 宽带集群系统中，为节省空口资源和无线资源控制(Radio Resource Control，RRC)连接数据，对于组呼的集群业务引入了共享信道的概念，即一个组呼业务在一个小区下仅分配一套物理资源连接供集群组呼呼叫中组内的多个用户共享，即一份业务的数据由多个终端来接收。由于是同一份数据，则其对应的安全算法和密钥只可能是一套，组内多个终端的安全能力是有差异的，该套安全算法和密钥可能不能保证组内所有终端都支持，从而无法保证组内所有终端都能成功接收业务数据。

[0004] 针对相关技术中在集群业务时不能组内保证所有终端都能成功接收业务数据的问题，目前尚未提出有效的解决方案。

发明内容

[0005] 针对相关技术中在集群业务时不能组内保证所有终端都能成功接收业务数据的问题，本发明提供了一种安全算法选择方法、装置及系统，以至少解决上述问题。

[0006] 根据本发明的一个方面，提供了一种安全算法选择方法，包括：核心网接收到第一终端UE发起到宽带集群网络的附着请求，其中，所述附着请求中携带有所述UE支持的第一安全能力信息；所述核心网确定所述第一UE所属的组，获取所述组内的各个第二UE的安全能力信息；所述核心网选择所述第一UE的安全能力信息和所述各个第二UE的安全能力信息均支持安全算法，并将选择的所述安全算法作为所述组的安全算法发送给所述第一UE。

[0007] 可选地，所述方法还包括：所述核心网确定选择的所述安全算法与保存的所述组的安全算法不相同，则将所述组的安全算法更新为选择的所述安全算法，并将选择的所述安全算法为所述组的安全算法发送给所述组内的各个所述第二UE。

[0008] 可选地，将选择的所述安全算法为所述组的安全算法发送给所述组内的各个所述第二UE，包括：所述核心网向各个所述第二UE发送组信息更新消息，所述组信息更新消息中携带选择的所述安全算法。

[0009] 可选地，核心网接收到第一用户终端UE发起到宽带集群网络的附着请求之后，所述方法还包括：所述核心网保存所述第一UE的安全能力信息。

[0010] 可选地，所述核心网选择所述第一UE的安全能力信息和所述各个第二UE的安全能力信息均支持安全算法，包括：所述核心网根据所述第一UE安全能力信息判断所述第一UE

是否支持当前所述组的安全算法，如果是，则选择当前所述组的安全算法，否则，取所述第一UE安全能力信息与所述各个第二UE的安全能力信息的交集，选择所述交集支持的一个安全算法。

[0011] 可选地，所述方法还包括：所述核心网在发起所述组的组呼业务时，将选择的所述安全算法及对应的密钥通知到基站，指示所述基站在进行所述组呼业务传递时，使用所述安全算法及密钥对信令和业务数据进行加密。

[0012] 根据本发明的另一个方面，提供了一种安全算法选择装置，包括：接收模块，用于第一终端UE发起到宽带集群网络的附着请求，其中，所述附着请求中携带有所述第一UE支持的安全能力信息；获取模块，用于确定所述第一UE所属的组，获取所述组内的各个第二UE的安全能力信息；选择模块，用于选择所述第一UE安全能力信息和所述各个第二UE的安全能力信息均支持安全算法；发送模块，用于将选择的所述安全算法作为所述组的安全算法发送给所述第一UE。

[0013] 可选地，所述装置还包括：判断模块，用于判断选择的所述安全算法与保存的所述组的安全算法是否相同，如果不同，则触发更新模块；所述更新模块，用于将所述组的安全算法更新为选择的所述安全算法，并将选择的所述安全算法发送给所述组内的各个所述第二UE。

[0014] 可选地，所述装置还包括：存储模块，用于保存所述第一UE的安全能力信息。

[0015] 可选地，所述选择模块包括：判断单元，用于根据所述第一UE的安全能力信息判断所述第一UE是否支持当前所述组的安全算法；选择单元，用于在所述判断单元的判断结果为是的情况下，选择当前所述组的安全算法，以及在所述判断单元的判断结果为否的情况下，取所述第一UE的安全能力信息与各个所述第二UE的安全能力信息的交集，选择所述交集支持的一个安全算法。

[0016] 可选地，所述装置还包括：通知模块，用于在发起所述组的组呼业务时，将选择的所述安全算法及对应的密钥通知到基站，指示所述基站在进行所述组呼业务传递时，使用所述安全算法及密钥对信令和业务数据进行加密。

[0017] 根据本发明的又一个方面，提供了一种安全算法选择系统，包括：核心网和基站，其中，所述核心网包括上述的安全算法选择装置；所述基站，用于按照所述核心网通知的组的安全算法及对应的密钥，在进行所述组的组呼业务传递时，使用所述安全算法及密钥对信令和业务数据进行加密。

[0018] 通过本发明，核心网在接收到UE发起到宽带集群网络的附着请求时，选择所述UE所属组的所有UE都支持的安全算法作为所述组的安全算法发送给所述UE，解决了相关技术中在集群业务时不能组内保证所有终端都能成功接收业务数据的问题，进而使得组内的所有UE都能成功接收业务数据，保证了集群业务的可靠性。

附图说明

[0019] 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

[0020] 图1是根据本发明实施例的安全算法选择方法的流程图；

[0021] 图2是根据本发明实施例的安全算法选择装置的结构示意图；

[0022] 图3是根据本发明实施例的安全算法选择系统的结构示意图；

[0023] 图4是实施例一的信令流程图；

[0024] 图5是实施例二的流程图。

具体实施方式

[0025] 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0026] 由于一个组呼业务在一个小区下只会建立一套无线资源连接供多个终端用户共享，对于加密算法的选择上可以由核心网直接配置一套加密算法分别通知基站和终端，这样如果配置的算法终端不支持那么这个终端将无法接收组内的业务数据。针对相关技术中的上述问题，本发明实施例提供了一种解决方案，在本发明实施例中，核心网根据组内各终端的安全能力情况，选择组内所有终端都支持的安全加密算法。

[0027] 根据本发明实施例，提供了一种安全算法选择方法。

[0028] 图1为根据本发明实施例的安全算法选择方法的流程图，如图1所示，该方法主要包括以下步骤S102-S106。

[0029] 步骤S102，核心网接收到第一UE发起到宽带集群网络的附着请求，其中，所述附着请求中携带有所述第一UE支持的安全能力信息。

[0030] 步骤S104，核心网确定所述第一UE所属的组，获取所述组内的各个第二UE的安全能力信息。

[0031] 在本发明可选实施例中，核心网可以保存每个业务组内的终端的标识信息以及安全能力信息，比如IMSI等，因此，可选地，核心网在接收到上述附着请求后，可以将该UE的标识信息以及安全能力信息保存到该UE所属的组中。

[0032] 在本发明可选实施例中，终端在附着时携带自身的能力信息，包括终端的安全能力信息，比如终端支持的安全加密算法等，核心网保存每个终端支持的安全能力信息。

[0033] 步骤S106，核心网选择所述第一UE的安全能力信息和各个所述第二UE的安全能力信息均支持安全算法，并将选择的所述安全算法作为所述组的安全算法发送给所述第一UE。

[0034] 终端附着成功后，核心网将选择的安全算法作为组对应的安全算法，发起终端所属的组信息更新的流程，将终端所属的组信息以及组相关的配置信息下发给终端，包括组对应的安全算法等信息。核心网在生成组更新消息里组对应的安全算法信息时，需要遍历组所包含的所有已附着终端支持的安全能力，取所有终端支持安全能力的交集，即选定所有终端均支持的安全算法下发给终端。

[0035] 在本发明可选实施例中，在步骤S106之后，所述方法还可以包括：所述核心网确定选择的所述安全算法与保存的所述组的安全算法不相同，则将所述组的安全算法更新为选择的所述安全算法，并将选择的所述安全算法作为所述组的安全算法发送给所述组内的各个所述第二UE。例如，所述核心网可以向各个所述第二UE发送组信息更新消息，所述组信息更新消息中携带选择的所述安全算法。

[0036] 在本发明可选实施例中，在步骤S106中，所述核心网在选择所述第一UE的安全能力信息和各个所述第二UE的安全能力信息均支持安全算法时，可以先根据所述第一安全能

力信息判断所述第一UE是否支持当前所述组的安全算法，如果是，则选择当前所述组的安全算法，否则，取所述第一UE的安全能力信息与各个所述第二UE的安全能力信息的交集，选择所述交集支持的一个安全算法。

[0037] 在本发明实施例中，当有新的终端附着时，如果终端所在的组计算出来的安全算法有变化，需要给组内其他已附着的终端重新发送组信息更新消息，以更新终端内保存的组所对应的安全算法。

[0038] 在本发明可选实施例中，核心网在发起组呼业务建立时，可以通过组信息更新消息通知到终端的组对应的安全算法和密钥通知到基站，指示所述基站在进行所述组呼业务传递时，使用所述安全算法及密钥对信令和业务数据进行加密。

[0039] 在本发明实施例中，第一UE所属的组可能为多个，则对于每个组，分别执行上述步骤S104和步骤S106。

[0040] 通过本发明实施例提供的上述方法，为业务组选择的安全算法为组内所有终端都支持的安全算法，从而可以保证组内的所有终端都可以成功接收到业务数据。

[0041] 根据本发明实施例，还提供一种安全算法选择装置，可以用于实现上述方法。

[0042] 图2为根据本发明实施例的安全算法选择装置的结构示意图，如图2所示，该装置主要包括：接收模块22，用于第一终端UE发起到宽带集群网络的附着请求，其中，所述附着请求中携带有所述第一UE支持的安全能力信息；获取模块24，用于确定所述第一UE所属的组，获取所述组内的各个第二UE的安全能力信息；选择模块26，用于选择所述第一UE的安全能力信息和各个所述第二UE的安全能力信息均支持安全算法；发送模块28，用于将选择的所述安全算法作为所述组的安全算法发送给所述第一UE。

[0043] 可选地，所述装置还可以包括：判断模块，用于判断选择的所述安全算法与保存的所述组的安全算法是否相同，如果不同，则触发更新模块；所述更新模块，用于将所述组的安全算法更新为选择的所述安全算法，并将选择的所述安全算法作为所述组的安全算法发送给所述组内的各个所述第二UE。

[0044] 可选地，所述装置还可以包括：存储模块，用于保存所述第一UE的安全能力信息。

[0045] 可选地，所述选择模块可以包括：判断单元，用于根据所述第一UE的安全能力信息判断所述第一UE是否支持当前所述组的安全算法；选择单元，用于在所述判断单元的判断结果为是的情况下，选择当前所述组的安全算法，以及在所述判断单元的判断结果为否的情况下，取所述第一UE的安全能力信息与各个所述第二UE的安全能力信息的交集，选择所述交集支持的一个安全算法。

[0046] 可选地，所述装置还可以包括：通知模块，用于在发起所述组的组呼业务时，将选择的所述安全算法及对应的密钥通知到基站，指示所述基站在进行所述组呼业务传递时，使用所述安全算法及密钥对信令和业务数据进行加密。

[0047] 根据本发明实施例，还提供了一种安全算法选择系统。

[0048] 图3为根据本发明实施例的安全算法选择系统的结构示意图，如图3所示，该系统包括：核心网32和基站34。其中，所述核心网32可以包括上述各个实施方式的安全算法选择装置；所述基站34，用于按照所述核心网通知的组的安全算法及对应的密钥，在进行所述组的组呼业务传递时，使用所述安全算法及密钥对信令和业务数据进行加密。

[0049] 下面通过具体实施例对本发明实施例提供的技术方案进行说明。

[0050] 实施例一

[0051] 本实施例以UE所属的组为一个业务组为例进行说明。

[0052] 图4为本实施例中组对应的安全算法选择的信令流程图，如图4所示，主要包括以下步骤：

[0053] 步骤401，UE1期望使用宽带集群业务，发起到宽带集群网络的附着流程，先建立与eNodeB的RRC连接，在附着消息里携带UE1支持的能力信息到核心网，包括支持的安全算法等，核心网保存UE1的能力信息。

[0054] 步骤402，核心网检索配置信息，确定UE1所属的组，并循环获取组内已登记的每个用户，在此实施例中假设UE1是组内第一个登记的用户，则核心网直接选取UE1上报的支持安全算法中的一个算法，作为组内用户所使用的安全算法，发起组信息更新流程，将组相关内容以及组对应的安全算法下发到UE1，并保存组对应的新的安全算法。

[0055] 步骤403，UE2期望使用宽带集群业务，发起到宽带集群网络的附着流程，先建立与eNodeB的RRC连接，在附着消息里携带UE2支持的能力信息到核心网，包括支持的安全算法等，核心网保存UE2的能力信息。

[0056] 步骤404，核心网检索配置信息，确定UE2所属的组，并循环获取组内已登记的每个用户，假设UE2所属的组中还有其他用户已经完成登记，比如UE1，则核心网会根据组内已登记的用户，包括UE1和UE2所支持的安全能力取交集后，选取一种安全算法作为组内用户所使用的安全算法，发起组信息更新流程，将组相关内容以及组对应的安全算法下发到UE2，并保存组对应的新安全算法。

[0057] 步骤405，核心网判决组内新计算得到的安全算法与之前组内保存的安全算法不一致，发起组更新的流程，将新的安全算法通知到组内其他用户，比如UE1。

[0058] 步骤406，UE2发起集群组呼业务的建立，建立RRC连接和集群的共享承载。

[0059] 步骤407，核心网将当前业务的组安全算法等信息通知给eNodeB，在进行组呼业务传递时，eNodeB使用这套安全算法对信令进行完保，对信令和业务数据进行加密。

[0060] 步骤408，如果UE1不在UE2所在的小区，UE1在接受到UE1发起组呼业务的寻呼后，回复寻呼响应，eNodeB和UE1开始建立集群共享信道的业务承载。

[0061] 步骤409，核心网将当前业务的组安全算法等信息通知给eNodeB，在进行组呼业务传递时，eNodeB使用这套安全算法对信令进行完保，对信令和业务数据进行加密。

[0062] 实施例二

[0063] 本实施例以UE所属的组为多个为例，对核心网进行安全算法选择的处理逻辑进行描述。

[0064] 图5为本实施例中核心网进行安全算法选择的流程图，如图5所示，主要包括以下步骤：

[0065] 步骤501，核心网接收到新的UE附着消息后，保存UE的能力信息，包括安全能力信息。

[0066] 步骤502，核心网检索UE所属的所有组信息以及组目前使用的安全算法。

[0067] 步骤503，逐个遍历UE所属的组，对于每个组需要判断组当前使用的安全算法是否在UE支持的安全能力集内，如果在，则组保持原有安全算法，如果不在，需要取组内所有UE包括新增UE的所有能力信息，取交集以确定当前的组对应的安全算法，并保存；

[0068] 步骤504，核心网对新附着的UE发起组更新流程，将UE所属所有组的安全算法等参数带给UE。

[0069] 步骤505，判断组对应的安全加密算法是否有变动，如果有改变，则执行步骤506，否则，结束安全加密算法选择流程。

[0070] 步骤506，对组内其他UE重新发起组更新流程，将新的安全算法通知到组内其他UE。

[0071] 从以上的描述中，可以看出，本发明实施例中，核心网在接收到UE发起到宽带集群网络的附着请求时，选择所述UE所属组的所有UE都支持的安全算法发送给所述UE，解决了相关技术中在集群业务时不能组内保证所有终端都能成功接收业务数据的问题，进而使得组内的所有UE都能成功接收业务数据，保证了集群业务的可靠性。

[0072] 显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

[0073] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

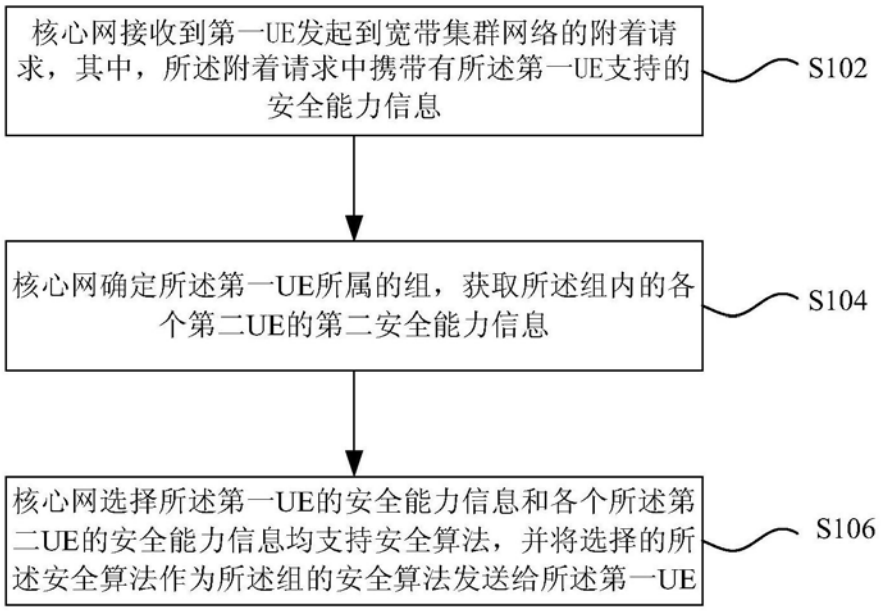

核心网接收到第一UE发起到宽带集群网络的附着请求，其中，所述附着请求中携带有所述第一UE支持的安全能力信息
S102
核心网确定所述第一UE所属的组，获取所述组内的各个第二UE的第二安全能力信息
S104
核心网选择所述第一UE的安全能力信息和各个所述第二UE的安全能力信息均支持安全算法，并将选择的所述安全算法作为所述组的安全算法发送给所述第一UE
S106

图1


接收模块22
获取模块24
选择模块26
发送模块28

图2

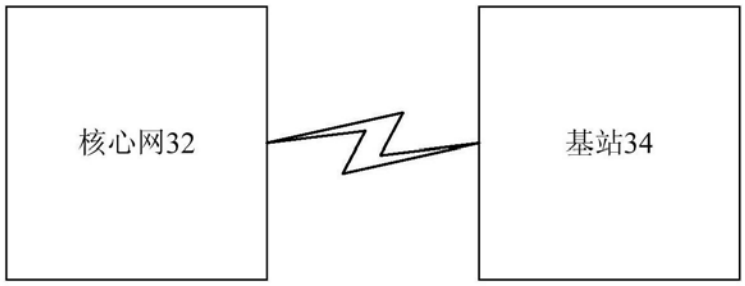

核心网32
基站34

图3

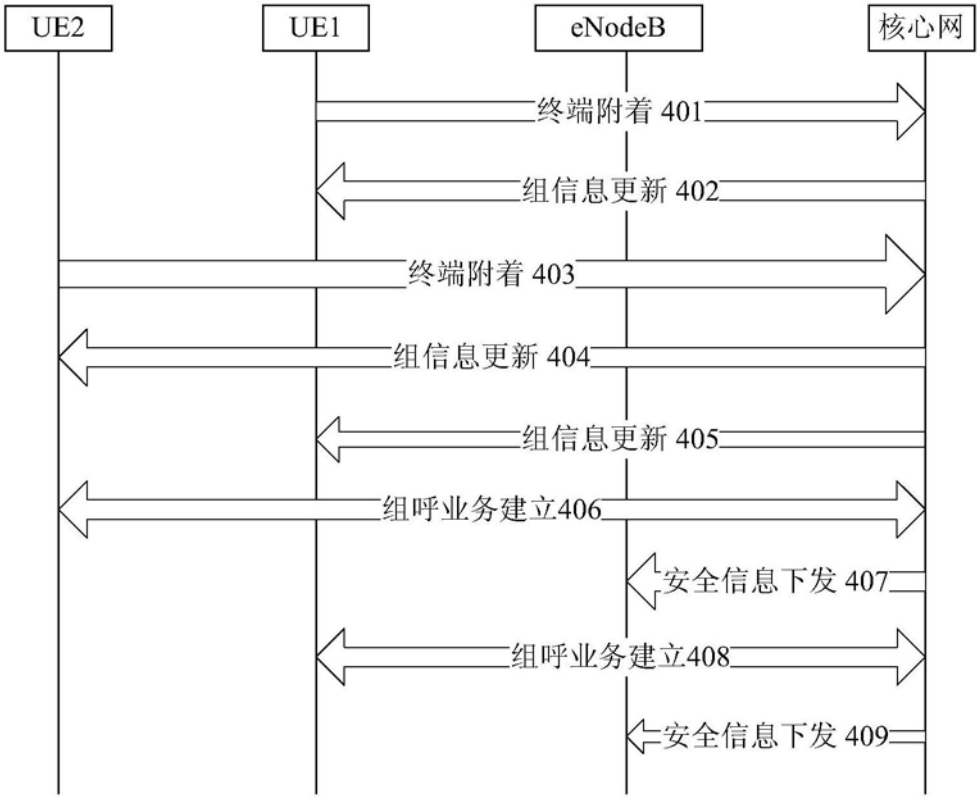

UE2
UE1
eNodeB
核心网
终端附着 401
组信息更新 402
终端附着 403
组信息更新 404
组信息更新 405
组呼业务建立406
安全信息下发 407
组呼业务建立408
安全信息下发 409

图4

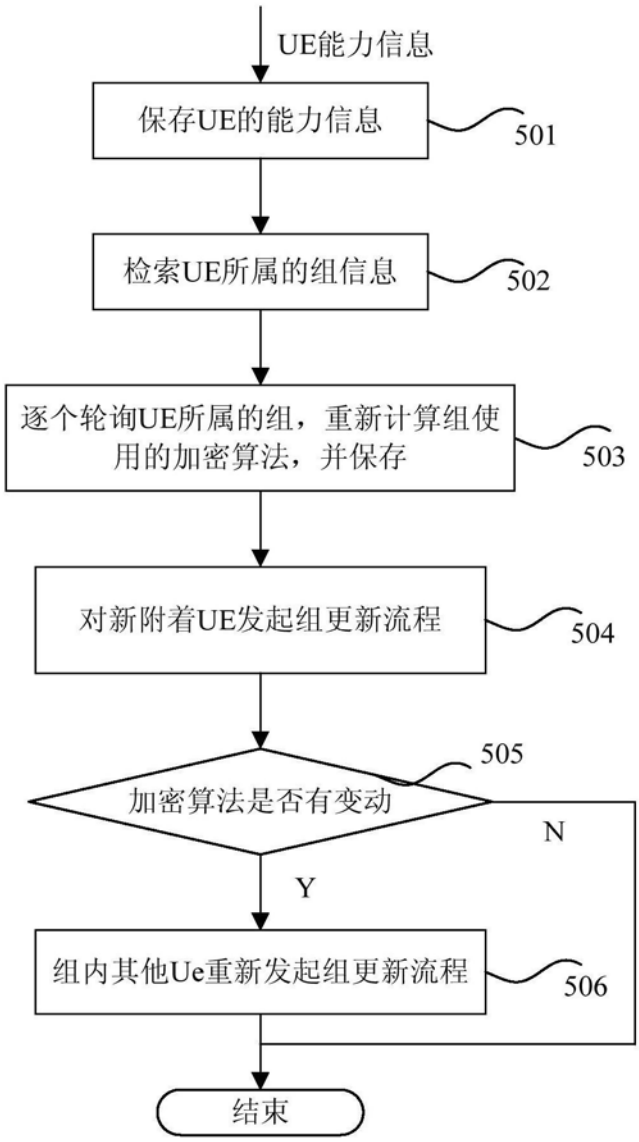

UE能力信息
保存UE的能力信息
501
检索UE所属的组信息
502
逐个轮询UE所属的组，重新计算组使用的加密算法，并保存
503
对新附着UE发起组更新流程
504
505
加密算法是否有变动
N
Y
组内其他Ue重新发起组更新流程
506
结束

图5