SUMMARY OF THE INVENTION

Embodiments of the invention provide an improved method for establishing a secure communication link between a master base station and a secondary base station in case of a detected security breach, thereby avoiding the problems of the prior art as identified above.

According to a first aspect of the present invention, there is provided a secondary base station apparatus comprising: a transmitter, which, in operation, transmits a change request of a secondary security key to a master base station when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base station apparatus; a receiver, which, in operation, receives from the master base station an updated secondary security key, the updated secondary security key being derived at the master base station by using an incremented freshness counter and a currently active security key of the master base station, without refreshing the currently active security key of the master base station; and control circuitry, which, in operation, computes a new encryption key for communication with a mobile terminal by using the updated secondary security key.

According to a second aspect of the present invention, there is provided a communication method for a secondary base station apparatus, the communication method comprising: transmitting a change request of a secondary security key to a master base station when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base station apparatus; receiving from the master base station an updated secondary security key, the updated secondary security key being derived at the master base station by using an incremented freshness counter and a currently active security key of the master base station without refreshing the currently active security key of the master base station; and computing a new encryption key for communication with a mobile terminal by using the updated secondary security key.

According to a third aspect of the present invention, there is provided a master base station apparatus comprising: a receiver, which, in operation, receives from a secondary base station a change request of a secondary security key when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base station; control circuitry, which, in operation, increments a freshness counter and derives an updated secondary security key for the secondary base station by using the incremented freshness counter and a currently active security key of the master base station apparatus without refreshing the currently active security key of the master base station

apparatus; and a transmitter, which, in operation, transmits the updated secondary security key to the secondary base station.

According to a fourth aspect of the present invention, there is provided a communication method for a master base station apparatus, the communication method comprising: receiving from a secondary base station a change request of a secondary security key when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base station; incrementing a freshness counter and deriving an updated secondary security key for the secondary base station by using the incremented freshness counter and a currently active security key of the master base station apparatus without refreshing the currently active security key of the master base station apparatus; and transmitting the updated secondary security key to the secondary base station.

According to a fifth aspect of the present invention, there is provided a mobile terminal apparatus comprising: a receiver, which, in operation, receives an incremented freshness counter prepared by a master base station that receives a change request of a secondary security key from a secondary base station, wherein the secondary security key is a security key for the secondary base station; and control circuitry, which, in operation, derives an updated secondary security key by using the received incremented freshness counter and a currently active security key of the master base station without refreshing the currently active security key of the master base station, and re-establishes a communication link with the secondary base station by using the derived updated secondary security key.

According to a sixth aspect of the present invention, there is provided a communication method for a mobile terminal apparatus, the communication method comprising: receiving an incremented freshness counter prepared by a master base station that receives a change request of a secondary security key from a secondary base station, wherein the secondary security key is a security key for the secondary base station; deriving an updated secondary security key for the secondary base station by using the received incremented freshness counter and a currently active security key of the master base station without refreshing the currently active security key of the master base station; and re-establishing a communication link with the secondary base station by using the derived updated secondary security key.

According to a seventh aspect of the present invention, there is provided an integrated circuit comprising: circuitry, which, in operation, controls: transmitting a change request of a secondary security key to a master base station when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base

station; receiving from the master base station an updated secondary security key, the updated secondary security key being derived at the master base station by using an incremented freshness counter and a currently active security key of the master base station, without refreshing the currently active security key of the master base station; and computing a new encryption key for communication with a mobile terminal by using the updated secondary security key; and at least one output coupled to the circuitry, which, in operation, outputs data.

According to an eight aspect of the present invention, there is provided an integrated circuit comprising: circuitry, which, in operation, controls: receiving from a secondary base station a change request of a secondary security key when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base station; incrementing a freshness counter and deriving an updated secondary security key for the secondary base station by using the incremented freshness counter and a currently active security key of the master base station without refreshing the currently active security key of the master base station; and transmitting the updated secondary security key to the secondary base station; and at least one output coupled to the circuitry, which, in operation, outputs data.

According to a ninth aspect of the present invention, there is provided an integrated circuit comprising: circuitry, which, in operation, controls: receiving an incremented freshness counter prepared by a master base station that receives a change request of a secondary security key from a secondary base station, wherein the secondary security key is a security key for the secondary base station; deriving an updated secondary security key for the secondary base station by using the received incremented freshness counter and a currently active security key of the master base station without refreshing the currently active security key of the master base station; and re-establishing a communication link with the secondary base station by using the derived updated secondary security key; and at least one output coupled to the circuitry, which, in operation, outputs data.

It is assumed that the mobile station is in dual connectivity and thus connected to both a master base station and a secondary base station via respective communication links. As explained above, in dual connectivity the security key S-K_{eNB} for the Secondary Cell Group, SCG, (i.e. for communication with the secondary base station) is inter-dependent on the security key K_{eNB} for the Master Cell Group, MCG (i.e. for communication with the master base station).

In this respect, in case of the detection of a potential security breach, the network would trigger a intra-cell handover for all bearers of the master and the secondary cell group thereby re-establishing security for the communication with the master and the secondary base station.

According to an embodiment of the invention, in case of the detection of a potential security breach it is proposed to only re-establish security for the communication with the secondary base station and not with the master base station. For an independent re-establishment of security for the communication with the secondary base station, a new security key S-K_{eNB} is derived on the basis of a incremented, hence, new COUNT input parameter to the ciphering/encryption algorithm (henceforth: freshness counter). In other words, the security key K_{eNB} for the communication with the master base station can remain the same, such that no intra-cell handover becomes necessary.

Specifically, in response to a detected potential security breach, the master base station increments the freshness counter for re-initializing the communication between the mobile station and the secondary base station. The term re-initializing of communication shall, in the context of the invention, be understood as re-establishing the PDCP sub-layer, re-establishing the RLC sub-layer and resetting the MAC layer.

In this respect, the re-initializing of communication differs from the execution of a handover command in that it provides for an optimized routing of packet data units, namely since the C-RNTI does not change. More importantly, the re-initialization of communication is triggered by a

CLAIMS:

1. A secondary base station apparatus comprising:

a transmitter, which, in operation, transmits a change request of a secondary security key to a master base station when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base station apparatus;

a receiver, which, in operation, receives from the master base station an updated secondary security key, the updated secondary security key being derived at the master base station by using an incremented freshness counter and a currently active security key of the master base station, without refreshing the currently active security key of the master base station; and

control circuitry, which, in operation, computes a new encryption key for communication with a mobile terminal by using the updated secondary security key.

2. The secondary base station apparatus according to claim 1, wherein the COUNT is composed of a packet data convergence protocol, PDCP, sequence number and a hyper frame number, HFN, that is shared between the secondary base station and the mobile terminal.

3. The secondary base station apparatus according to claim 1, wherein the transmitter determines that the COUNT is about to wrap up when a value of the COUNT exceeds a threshold value.

4. The secondary base station apparatus according to claim 1, wherein the currently active security key of the master base station is not updated in response to the change request.

5. The secondary base station apparatus according to claim 1, wherein the control circuitry, in operation, re-establishes a communication link with the mobile terminal by using the updated secondary security key.

6. The secondary base station apparatus according to claim 1, wherein RRCConnectionReconfiguration message is transmitted from the master base station or the secondary base station to the mobile terminal after the master base station transmits the updated secondary security key.

7. The secondary base station apparatus according to claim 1, wherein the freshness counter is a counter value for refresh of the secondary security key.

8. A communication method for a secondary base station apparatus, the communication method comprising:

transmitting a change request of a secondary security key to a master base station when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base station apparatus;

receiving from the master base station an updated secondary security key, the updated secondary security key being derived at the master base station by using an incremented freshness counter and a currently active security key of the master base station without refreshing the currently active security key of the master base station; and

computing a new encryption key for communication with a mobile terminal by using the updated secondary security key.

9. A master base station apparatus comprising:

a receiver, which, in operation, receives from a secondary base station a change request of a secondary security key when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base station;

control circuitry, which, in operation, increments a freshness counter and derives an updated secondary security key for the secondary base station by using the incremented freshness counter and a currently active security key of the master base station apparatus without refreshing the currently active security key of the master base station apparatus; and

a transmitter, which, in operation, transmits the updated secondary security key to the secondary base station.

10. The master base station apparatus according to claim 9, wherein the COUNT is composed of a packet data convergence protocol, PDCP, sequence number and a hyper frame number, HFN, that is shared between the secondary base station and a mobile terminal.

11. The master base station apparatus according to claim 9, wherein the COUNT is determined to be about to wrap up, by the secondary base station, when a value of the COUNT exceeds a threshold value.

12. The master base station apparatus according to claim 9, wherein the currently active security key of the master base station apparatus is not updated in response to the change request.

13. The master base station apparatus according to claim 9, wherein the transmitter, in operation, transmits RRCConnectionReconfiguration message to the mobile terminal after deriving the updated secondary security key.

14. The master base station apparatus according to claim 9, wherein the freshness counter is a counter value for refresh of the secondary security key.

15. A communication method for a master base station apparatus, the communication method comprising:

receiving from a secondary base station a change request of a secondary security key when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base station;

incrementing a freshness counter and deriving an updated secondary security key for the secondary base station by using the incremented freshness counter and a currently active security key of the master base station apparatus without refreshing the currently active security key of the master base station apparatus; and

transmitting the updated secondary security key to the secondary base station.

16. A mobile terminal apparatus comprising:

a receiver, which, in operation, receives an incremented freshness counter prepared by a master base station that receives a change request of a secondary security key from a secondary base station, wherein the secondary security key is a security key for the secondary base station; and

control circuitry, which, in operation, derives an updated secondary security key by using the received incremented freshness counter and a currently active security key of the master base station without refreshing the currently active security key of the master base station, and re-establishes a communication link with the secondary base station by using the derived updated secondary security key.

17. The mobile terminal apparatus according to claim 16, wherein the secondary base station transmits the change request of the secondary security key to the master base station when a COUNT is about to wrap up, the COUNT being composed of a packet data convergence protocol, PDCP, sequence number and a hyper frame number, HFN, that is shared between the secondary base station and the mobile terminal apparatus.

18. The mobile terminal apparatus according to claim 16, wherein the freshness counter is incremented by the master base station after it is determined by the secondary base station that the COUNT is about to wrap up.

19. The mobile terminal apparatus according to claim 16, wherein the COUNT is determined to be about to wrap up when a value of the COUNT exceeds a threshold value.

20. The mobile terminal apparatus according to claim 16, wherein the receiver, in operation, receives RRCConnectionReconfiguration message from the master base station or the secondary base station, and the incremented freshness count is included in the RRCConnectionReconfiguration message.

21. The mobile terminal apparatus according to claim 16, wherein the currently active security key of the master base station is not updated in response to the change request.

22. The mobile terminal apparatus according to claim 16, wherein the freshness counter is a counter value for refresh of the secondary security key.

23. The mobile terminal apparatus according to claim 16, further comprising:

a transmitter, which, in operation, transmits RRCConnectionReconfigurationComplete message after the updated secondary security key is derived.

24. A communication method for a mobile terminal apparatus, the communication method comprising:

receiving an incremented freshness counter prepared by a master base station that receives a change request of a secondary security key from a secondary base station, wherein the secondary security key is a security key for the secondary base station;

deriving an updated secondary security key for the secondary base station by using the received incremented freshness counter and a currently active security key of the master base station without refreshing the currently active security key of the master base station; and

re-establishing a communication link with the secondary base station by using the derived updated secondary security key.

25. An integrated circuit comprising:

circuitry, which, in operation, controls:

transmitting a change request of a secondary security key to a master base station when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base station;

receiving from the master base station an updated secondary security key, the updated secondary security key being derived at the master base station by using an incremented freshness counter and a currently active security key of the master base station, without refreshing the currently active security key of the master base station; and

computing a new encryption key for communication with a mobile terminal by using the updated secondary security key; and

at least one output coupled to the circuitry, which, in operation, outputs data.

26. An integrated circuit comprising:

circuitry, which, in operation, controls:

receiving from a secondary base station a change request of a secondary security key when a COUNT is about to wrap up, wherein the COUNT is a sequence counter and the secondary security key is a security key for the secondary base station;

incrementing a freshness counter and deriving an updated secondary security key for the secondary base station by using the incremented freshness counter and a currently active security key of the master base station without refreshing the currently active security key of the master base station; and

transmitting the updated secondary security key to the secondary base station; and

at least one output coupled to the circuitry, which, in operation, outputs data.

27. An integrated circuit comprising:

circuitry, which, in operation, controls:

receiving an incremented freshness counter prepared by a master base station that receives a change request of a secondary security key from a secondary base station, wherein the secondary security key is a security key for

the secondary base station;

deriving an updated secondary security key for the secondary base station by using the received incremented freshness counter and a currently active security key of the master base station without refreshing the currently active security key of the master base station; and

re-establishing a communication link with the secondary base station by using the derived updated secondary security key; and

at least one output coupled to the circuitry, which, in operation, outputs data.