SUMMARY OF THE INVENTION

~~One object~~Embodiments of the invention ~~is to~~ 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.

~~The object is solved by the subject matter of the independent claims. Advantageous embodiments are subject to the dependent claims.~~

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 when a COUNT is about to wrap up; a receiver, which, in operation, receives from a master base station an updated secondary security key for the secondary base station, the updated secondary security key being derived by using an incremented freshness counter and a 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 when a COUNT is about to wrap up; receiving from a master base station an updated secondary security key for the secondary base station, the updated secondary security key being derived by using an incremented freshness counter and a 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; 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; 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; 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; 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; and control circuitry, which, in operation, derives 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 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 preset 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; 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; 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 when a COUNT is about to wrap up; receiving from a master base station an updated secondary security key for a secondary base station, the updated secondary security key being derived by using an incremented freshness counter and a 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 eighth 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; 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; 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; 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; 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 ~~a first aspect~~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

different message, namely an RRC connection reconfiguration message which does not include a handover command (i.e. without mobility control information).

The re-initialization of the communication between the mobile station and the secondary base station is based on the incremented freshness counter in that a new security key S-K_{eNB} is derived for the communication there between under the control of the master base station. In this respect, the mobile station and the secondary base station are capable of establishing the secure communication link, after detection of the potential security breach, using the same, derived security key S-K_{eNB}.

As the above procedure is so different from what is presently carried out upon detection of a potential security breach, independently from the above, the following suggested improving the re-establishment of security within a secondary cell group.

According to ~~a second aspect~~ another embodiment of the invention, a mobile station (i.e. UE) is suggested, the mobile station being initialized for communication with a master and a secondary base station in a wireless communication system, wherein the mobile station receives from the master base station a reconfiguration message (for example an RRC connection reconfiguration message) which includes a freshness counter.

For clarification purposes only, it shall be emphasized that the reconfiguration message does not include a handover command.

In response to receipt of the reconfiguration message, the mobile station derives a security key S-K_{eNB} for the communication with the secondary base station. More particularly, the mobile station derives the security key S-K_{eNB} based on the incremented freshness counter included in the re-configuration message.

The secondary key S-K_{eNB}, is subsequently used, by the mobile station, for re-initializing the communication with the secondary base station, thereby enabling the mobile station to establish a secure communication link with the secondary base station.

Notably, the re-configuration message received from the master base station includes the incremented freshness counter. Accordingly, the mobile station can derive that it is to trigger re-initialization of the communication with the secondary base station. In other words, should the re-configuration message not be for the communication with the secondary base station no incremented freshness counter would be included therein.

CLAIMS

1. A secondary base station apparatus comprising:

a transmitter, which, in operation, transmits a change request of a secondary security key when a COUNT is about to wrap up;

a receiver, which, in operation, receives from a master base station an updated secondary security key for the secondary base station, the updated secondary security key being derived by using an incremented freshness counter and a 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 when a COUNT is about to wrap up;

receiving from a master base station an updated secondary security key for the secondary base station, the updated secondary security key being derived by using an incremented freshness counter and a 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;

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; 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;

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; 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; and

control circuitry, which, in operation, derives 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 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;
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; 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 when a COUNT is about to wrap up;
receiving from a master base station an updated secondary security key for a secondary base station, the updated secondary security key being derived by using an incremented freshness counter and a 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;

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; 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;

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; 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.

CLAIMS

1. A method for establishing a secure communication link between a mobile station and a secondary base station in a mobile communication system comprising the mobile station, a master and the secondary base station, the mobile station being initialized for communication with the master and the secondary base station,

detecting, by the master or by the secondary base station, a potential security breach including:

- a condition where a sequence counter of packet data units of an established secure communication link between the mobile station and the secondary base station is to wrap-up since initialization of the communication between the mobile station and the secondary base station, and
- a condition where a communication link identification is to be reused for establishing the secure communication link with the secondary base station since initialization of the communication between the mobile station and the secondary base station;

and, in case the potential security breach is detected by the secondary base station, signaling the detected security breach to the master base station;

incrementing, by the master base station, in response to the detected or signaled potential security breach, a freshness counter for re-initializing the communication between the mobile station and the secondary base station; and

re-initializing, by the mobile station and by the secondary base station, the communication there between, the re-initializing step being performed under the control of the master base station and further includes deriving a same security key based on said incremented freshness counter, and establishing the secure communication link utilizing the same, derived security key.

2. The method according to claim 1, wherein the re-initialization step is performed by the mobile station and by the secondary base station without re-initializing the communication between the mobile station and the master base station.

3. The method according to claim 1 or 2, wherein the secondary base station performs the step of detecting the condition where the sequence counter is to wrap-up, and

wherein either the master or the secondary base station performs the step of detecting the condition where a communication link identification is to be reused.

4. The method according to one of claims 1 – 3, wherein the step of re-initializing the communication between the mobile station and the secondary base station further includes:

deriving, by the master base station, a security key based on the incremented freshness counter for the communication between the mobile station and the secondary base station, and transmitting said derived security key and the incremented freshness counter to the secondary base station;

generating, by the secondary base station, a re-configuration message for re-initializing the communication between the mobile station and the secondary base station including the incremented freshness counter and transmitting the re-configuration message to the master base station;

forwarding, by the master base station, the re-configuration message including the incremented freshness counter to the mobile station; and

deriving, by the mobile station, a same security key based on the freshness counter included in the forwarded re-configuration message for establishing on the basis of the same, derived security key the secure communication link between the mobile station and the secondary base station.

5. The method according to one of claims 1 – 3, wherein the step of re-initializing the communication between the mobile station and the secondary base station further includes:

generating and transmitting, by the master base station, a re-configuration message for re-initializing the communication between the mobile station and the secondary base station including the incremented freshness counter to the mobile station;

deriving, by the master base station, a security key based on the incremented freshness counter for the communication between the mobile station and the secondary base station, and transmitting, by the master base station, said derived security key to the secondary base station;

deriving, by the mobile station, a same security key based on the freshness counter included in the transmitted re-configuration message for establishing on the basis of the same, derived security key the secure communication link between the mobile station and the secondary base station; and

wherein the step of deriving and transmitting said derived security key to the secondary base station is performed, by the master base station, before or after the step of transmitting the re-configuration message including the incremented freshness counter to the mobile station is performed by the master base station.

6. The method according to claim 5, wherein the master base station additionally transmits the incremented freshness counter to the secondary base station.

7. The method according to one of claims 4 – 6 , wherein the step of deriving, by the mobile station, a same security key based on the incremented freshness counter included in the transmitted re-configuration message, further includes:

determining, by the mobile station, whether the incremented freshness counter, included in the transmitted re-configuration message, differs from a previous freshness counter included in a previously transmitted re-configuration message, and only in case of a different, incremented freshness counter, performing the step of deriving the same security key by the mobile station.

8. The method according to one of claims 4 – 7, further comprising the step of transmitting, by the mobile station, a re-configuration complete message to the master or to the secondary base station; and, in case the re-configuration complete message is transmitted by the mobile station to the master base station, the step of forwarding, by the master base station, said re-configuration complete message to the secondary base station.

9. The method according to claim 8, wherein the step of transmitting, and forwarding the reconfiguration complete message is performed after the step of re-initializing, by the mobile station and the secondary base station the communication there between.

10. The method according to one of claims 4 – 9, wherein the re-configuration message, generated by the master or the secondary base station, further includes a dedicated preamble or indicates a dedicated preamble from among a plurality of pre-configured preambles for performing a Random Access CHannel, RACH, procedure between

the mobile station and the secondary base station; and the method further includes the step of:

performing between the mobile station and the secondary base station the RACH procedure utilizing the dedicated preamble included in the re-configuration message or utilizing the indicated dedicated preamble from the plurality of pre-configured preambles, respectively.

11. The method according to claim 10, wherein the step of performing the RACH procedure is performed between the mobile station and the secondary base station after the step of re-initializing, by the mobile station, the communication with the secondary base station, and before the step of re-initializing, by secondary base station, the communication with the mobile station.

12. The method according to claim 10 or 11, wherein the plurality of pre-configured preambles, from among which the re-configuration message indicates the dedicated preamble to be used for performing the RACH procedure, are pre-configured using an X2 interface between the master and the secondary base station.

13. The method according to one of claims 4 – 12, wherein the step of transmitting and/or forwarding the re-configuration message is performed by signaling a corresponding Radio Resource Control, RRC, connection reconfiguration message, and, in case of a re-configuration complete message, the step of transmitting and/or forwarding the re-configuration complete message is performed by signaling a corresponding RRC connection reconfiguration complete message.

14. The method according to one of claims 4 – 9, wherein the method further includes the step of:

transmitting, by the mobile station, in response to the re-configuration message including a freshness counter, a re-configuration acknowledge message to the secondary base station in form of a Medium Access Control, MAC, Control Element, CE.

15. The method according to claim 14, wherein the step of transmitting the re-configuration acknowledge message is performed before the step of re-initializing, by the secondary base station, the communication with the mobile station.

16. The method according to claim 14 or 15, wherein the re-configuration message including the freshness counter is transmitted and/or forwarded to the mobile station in form of MAC packet data unit, PDU, including in its MAC header a pre-defined Logical Channel ID, LCID, and wherein the LCID identifies the type of the MAC CE for the re-configuration acknowledge message.

17. A mobile communication system for establishing a secure communication link between a mobile station and a secondary base station, the mobile communication system comprising the mobile station, a master and the secondary base station, the mobile station being initialized for communication with the master and the secondary base station, wherein:

the master and/or the secondary base station are configured to detect a potential security breach including:

- *a condition where a sequence counter of packet data units of an established* secure communication link between the mobile station and the secondary base station is to wrap-up since initialization of the communication between the mobile station and the secondary base station, and
- a condition where a communication link identification is to be reused for establishing the secure communication link with the secondary base station since initialization of the communication between the mobile station and the secondary base station;

the secondary base station is configured to, in case of detecting the potential security breach, signal the detected security breach to the master base station;

the master base station is configured to increment in response to the detected or signaled potential security breach, a freshness counter for re-initializing the communication between the mobile station and the secondary base station; and

the mobile station and the secondary base station are further configured to re-initialize the communication there between, the re-initialization being performed under the control of the master base station and includes deriving a same security key based on said incremented freshness counter, and establishing the secure communication link utilizing the same, derived security key.

18. The mobile communication system according to claim 17, wherein the mobile station and the secondary base station are configured to re-initialize, under the control of the master base station, the communication there between without re-initializing the communication between the mobile station and the master base station.

19. The mobile communication system according to claim 17 or 18, wherein the secondary base station is configured to detect the condition where the sequence counter is to wrap-up, and wherein either the master or the secondary base station are configured to detect the condition where a communication link identification is to be reused.

20. The mobile communication system according to one of claims 17 – 19, wherein:

the master base station is configured to derive a security key based on the incremented freshness counter for the communication between the mobile station and the secondary base station, and to transmit said derived security key and the incremented freshness counter to the secondary base station;

the secondary base station is configured to generate a re-configuration message for the communication between the mobile station and the secondary base station including the incremented freshness counter and to transmit the re-configuration message to the master base station;

the master base station is configured to forward the re-configuration message including the incremented freshness counter to the mobile station; and

the mobile station is configured to derive a same security key based on the freshness counter included in the forwarded re-configuration message for establishing on the basis of the same, derived security key the secure communication link between the mobile station and the secondary base station.

21. The mobile communication system according to one of claims 17 – 19, wherein:

the master base station is configured to generate and to transmit a re-configuration message including the incremented freshness counter to the mobile station;

the master base station is configured to derive a security key based on the incremented freshness counter for the communication between the mobile station

and the secondary base station, and to transmit said derived security key to the secondary base station;

the mobile station is configured to derive a same security key based on the freshness counter included in the transmitted re-configuration message for establishing on the basis of the same, derived security key the secure communication link between the mobile station and the secondary base station; and

wherein the master base station is configured to derive and to transmit said derived security key to the secondary base station before or after transmitting the re-configuration message including the incremented freshness counter to the mobile station.

22. The mobile communication system according to claim 21, wherein the master base station is configured to additionally transmit the incremented freshness counter to the secondary base station.

23. The mobile communication system according to on of claims 20 - 22, wherein:

the mobile station is configured to determine whether the incremented freshness counter, included in the transmitted re-configuration message, differs from a previous freshness counter included in a previously transmitted re-configuration message, and only in case of a different, incremented freshness counter, to derive the same security key by the mobile station.

24. The mobile communication system according to one of claims 20 – 23, wherein the mobile station is configured to transmit a re-configuration complete message to the master or to the secondary base station; and

the master base station is configured to forward the re-configuration complete message to the secondary base station, in case the re-configuration complete message is transmitted by the mobile station to the master base station.

25. The mobile communication system according to claim 24, wherein mobile station and the master base station are configured to transmit and to forward the reconfiguration complete message after re-initializing, by the mobile station and the secondary base station the communication there between.

26. The mobile communication system according to one of claims 20 – 25, wherein master or the secondary base station are configured to generated the re-configuration message further including a dedicated preamble or indicating a dedicated preamble from among a plurality of pre-configured preambles for performing a Random Access CHannel, RACH, procedure between the mobile station and the secondary base station; and

the mobile station and the secondary base station are configured to perform the RACH procedure utilizing the dedicated preamble included in the re-configuration message or utilizing the indicated dedicated preamble from the plurality of pre-configured preambles, respectively.

27. The mobile communication system according to claim 26, wherein the mobile station and the secondary base station are configured to perform the RACH procedure there between after the mobile station re-initializes the communication with the secondary base station, and before the secondary base station re-initializes the communication with the mobile station.

28. The mobile communication system according to claim 26 or 27, wherein the master and the secondary base station are configured to pre-configure the plurality of pre-configured preambles, from among which the re-configuration message indicates the dedicated preamble to be used for performing the RACH procedure, using an X2 interface.

29. The mobile communication system according to one of claims 20 – 28, wherein the master and the secondary base station are configured to transmit and/or to forwarding the re-configuration message by signaling a corresponding Radio Resource Control, RRC, connection reconfiguration message, and,

in case of a re-configuration complete message, the mobile station and the master base station are configured to transmit and/or to forward the re-configuration complete message, by signaling a corresponding RRC connection reconfiguration complete message.

30. The mobile communication system according to one of claims 20 – 28, wherein:

the mobile station is configured to transmit, in response to the re-configuration message including a freshness counter, a re-configuration acknowledge message to

the secondary base station in form of a Medium Access Control, MAC, Control Element, CE.

31. The mobile communication system according to claim 30, wherein the mobile station is configured to transmit the re-configuration acknowledge message before the secondary base station re-initializing the communication with the mobile station.

32. The mobile communication system according to claim 30 or 31, wherein master base station is configured to transmit and/or to forward the re-configuration message including the freshness counter to the mobile station in form of MAC packet data unit, PDU, including in its MAC header a pre-defined Logical Channel ID, LCID, and wherein the LCID identifies the type of the MAC CE for the re-configuration acknowledge message.

33. A computer readable medium storing instruction that, when executed in connection with a mobile communication system comprising a mobile station, a master and a secondary base station, the mobile station being initialized for communication with the master and the secondary base station,

cause the mobile communication system to establish a secure communication link between the mobile station and the secondary base station, by performing the steps of:

detecting, by the master or by the secondary base station, a potential security breach including:

- a condition where a sequence counter of packet data units of an established secure communication link between the mobile station and the secondary base station is to wrap-up since initialization of the communication between the mobile station and the secondary base station, and
- a condition where a communication link identification is to be reused for establishing the secure communication link with the secondary base station since initialization of the communication between the mobile station and the secondary base station;

and, in case the potential security breach is detected by the secondary base station, signaling the detected security breach to the master base station;

incrementing, by the master base station, in response to the detected or signaled potential security breach, a freshness counter for re-initializing the communication between the mobile station and the secondary base station; and

re-initializing, by the mobile station and by the secondary base station, the communication there between, the re-initializing step being performed under the control of the master base station and further includes deriving a same security key based on said incremented freshness counter, and establishing the secure communication link utilizing the same, derived security key.