in the above-mentioned LTE network, the E-UTRAN connects cellular IoT (CIoT) UEs to a CN and ultimately to services available through a PDN or other data network. However, in currently proposed implementations, there are security concerns for CIoT UEs in NB-IoT networks, for example, during operations such as radio link recovery.

Summary

Illustrative embodiments provide techniques for providing secure radio link recovery for user equipment in a communication system.

In an embodiment, the present disclosure provides a method comprising: in a communication system, in response to a radio link failure between a user equipment and a source access node of the communication system during a data transfer operation over a control plane; recovering the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is enabled via a mobility management node of the communication system using a non-access stratum security context previously established between the user equipment and the mobility management node.

In an embodiment, the present disclosure provides an apparatus comprising: in a communication system, in response to a radio link failure between a user equipment and a source access node of the communication system during a data transfer operation over a control plane; a network node in the communication system configured to function as a mobility management entity, and further configured to enable recovering the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is enabled via the mobility management entity using a non-access stratum security context previously established between the user equipment and the mobility management entity.

In an embodiment, the present disclosure provides a method comprising: in a communication system, in response to a radio link failure between a user equipment and a source access node of the communication system during a data transfer operation over a control plane; recovering the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is initiated by the user equipment by sending a message to a mobility management node of the communication system through the target access node using a non-access stratum security context previously established between the user equipment and the mobility management node.

In an embodiment, the present disclosure provides an apparatus comprising: in a communication system, in response to a radio link failure between a user equipment and a source access node of the communication system during a data transfer operation over a control plane; the user equipment configured to enable recovery of the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is initiated by the user equipment by sending a message to a mobility management node of the communication system through the target access node using a non-access stratum security context previously established between the user equipment and the mobility management node.

In an embodiment, the present disclosure provides an article of manufacture comprising a non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to perform the method according to the first aspect or the third aspect.

In one embodiment, a method comprises, in response to a radio link failure between given user equipment and a source access node of a communication system during a data transfer operation over a control plane, recovering the radio link for the given user equipment through a target access node of the communication system. The radio link recovery is enabled via a mobility management node of the communication system using a non-access stratum security context previously established between the given user equipment and the mobility management node.

In another embodiment, a method comprises, in response to a radio link failure between given user equipment and a source access node of a communication system during a data transfer operation over a control plane, recovering the radio link for the given user equipment through a target access node of the communication system. The radio link recovery is initiated by the given user equipment by sending a message to a mobility management node of the communication system through the target access node using a non-access stratum security context previously established between the given user equipment and the mobility management node.

In an aspect, there is provided a method for recovering a radio link, the method comprising:

establishing, in a communication system, a non-access stratum security context between user equipment and a mobility management node of the communication system; and

receiving a first message indicating a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, wherein at least a portion of the first message is protected using a cryptographic key created within the non-access stratum security context previously established between the user equipment and the mobility management node;

verifying, using the mobility management node, the user equipment using the cryptographic key;

initiating, via the mobility management node, within the non-access stratum security context previously established between the user equipment and the mobility management node, a radio link for the user equipment through a target access node of the communication system by initiating set up of a signaling interface with the target access node and sending a second message to the user equipment through the target access node; and retrieving, by the mobility management node, buffered data associated with the data transfer over the control plane .

In an aspect, there is provided an apparatus configured for recovering a radio link, the apparatus comprising: a network node comprising a processor and memory, the network node being configured to function as a mobility management node of a communication system and to be in communication with user equipment and one or more access nodes of the communication system, wherein the network node is further configured to at least:

establish, in the communication system, a non-access stratum security context between the user equipment and the network node; and

receive a first message indicating a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, wherein at least a portion of the first message is protected using a cryptographic key created within the non-access stratum security context previously established between the user equipment and the mobility management node;

verify the user equipment using the cryptographic key;

initiate within the non-access stratum security context previously established between the user equipment and the network node, a radio link for the user equipment through a target access node of the communication system by initiating set up of a signaling interface with the target access node and sending a second message to the user equipment through the target access node; and

retrieve buffered data associated with the data transfer over the control plane.

In an aspect, there is provided a method for recovering a radio link, the method comprising:

establishing, between user equipment and a mobility management node of a communication system, a non-access stratum security context; and

in response to a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, sending a first message from the user equipment to the mobility management node of the communication system through a target access node using the non-access stratum security context previously established between the user equipment and the mobility management node, the first message indicating that the radio link failure has occurred, , at least a portion of the first message being protected using a cryptographic key created within the non-access stratum security context previously established between the user equipment and the mobility management node, and

after the mobility management node verifies the user equipment using the cryptographic key and initiates setup of a signaling interface with the target access node, receiving, from the target access node, a second message acknowledging the radio link failure

.

In an embodiment, there is provided an apparatus configured for recovering a radio link, the apparatus comprising:

a processor and a memory storing program codes, wherein the memory and program codes are configured, with the processor, to cause the apparatus to at least:

establish, between the apparatus and a mobility management node of a communication system, a non-access security context; and

in response to a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, send a first message from the apparatus to the mobility management node of the communication system through a target access node using the non-access stratum security context previously established between the apparatus and the mobility management node, the first message indicating that the radio link failure has occurred, at least a portion of the first message being protected using a cryptographic key created within the non-access stratum security context previously established between the user equipment and the mobility management node, and

after the mobility management node verifies the user equipment using the

cryptographic key and initiates setup of a signaling interface with the target access node, receive, from the target access node, a second message acknowledging the radio link failure.

In an embodiment, there is provideda method for recovering a radio link, the method comprising: establishing, in a communication system, a non-access stratum security context between user equipment and a mobility management node of the communication system;

receiving, at the mobility management node, within the non-access stratum security context previously established between the user equipment and the mobility management node of the communication system, a first message from the user equipment via a target access node of the communication system, the first message being protected using a cryptographic key associated with the non-access stratum security context previously established between the user equipment and the mobility management node;

verifying the user equipment using the cryptographic key;n an instance in which the first message received from the user equipment indicates a radio link failure has occurred between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, recovering, initiating via the mobility management node,

set up of a signaling interface with the target access node;

sending a second message to the user equipment via the target access node, the second message acknowledging the radio link failure; and retrieving buffered data associated with the data transfer over the control plane,

wherein the non-access stratum message is integrity protected using an integrity key associated with the non-access stratum security context previously established between the user equipment and the mobility management node.

In an aspect, there is provided an apparatus for recovering a radio link, the apparatus comprising:

one or more processors; and

one or more memories storing program instructions which, when executed by the one or more processors, cause the apparatus at least to:

establish, in a communication system, a non-access stratum security context between user equipment and the apparatus;

receive, at the apparatus, within the non-access stratum security context previously established between the user equipment and the apparatus, a first message from the user equipment via a target access node of the communication system, the first message

being protected using a cryptographic key associated with the non-access stratum security context previously established between the user equipment and the mobility management node; verify the user equipment using the cryptographic key;

in an instance in which the first message received from the user equipment indicates a radio link failure has occurred between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, initiate set up of a signaling interface with the target access node;

send a second message to the user equipment via the target access node of the communication system, the second message acknowledging the radio link failure and retrieve buffered data associated with the data transfer over the control plane.

wherein the non-access stratum message is integrity protected using an integrity key associated with the non-access stratum security context previously established between the user equipment and the apparatus.

In an aspect, there is provided a non-transitory computer-readable storage medium for recovering a radio link, the non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to:establish, in a communication system, a non-access stratum security context between user equipment and a mobility management node of the communication system;

receive, at the mobility management node, within the non-access stratum security context previously established between the user equipment and the mobility management node of the communication system, a first message from the user equipment via a target access node of the communication system, the first message being protected using a cryptographic key associated with the non-access stratum security context previously established between the user equipment and the mobility management node; verify the user equipment using the cryptographic key;

in an instance in which the first message received from the user equipment indicates a radio link failure has occurred between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, initiate set up of a signaling interface with the target access node;

send a second message to the user equipment via the target access node of the communication system, and

retrieve buffered data associated with the data transfer over the control plan .

In an aspect, there is provided a method for recovering a radio link, the method

comprising:

establishing, between user equipment and a mobility management node of a communication system, via a source access node of the communication system, a non-access stratum security context; in an instance in which a radio link failure occurs between the user equipment and the source access node of the communication system during a data transfer operation over a control plane, initiating recovery of the radio link for the user equipment, through a target access node of the communication system, by sending a first message from the user equipment to the mobility management node of the communication system through the target access node, the non-access stratum message indicating that the radio link failure has occurred,

wherein the first message is protected using a cryptographic key associated with the non-access stratum security context previously established between the user equipment and the mobility management node;

after the mobility management node verifies the user equipment using the cryptographic key and initiates set up of a signaling interface with the target access node, receiving, from the target access node, a second message acknowledging the radio link failure.

In an aspect, there is provided an apparatus for recovering a radio link, the apparatus comprising: one or more processors; and

one or more memories storing program instructions which, when executed by the one or more processors, cause the apparatus at least to:

establish, between the apparatus and a mobility management node of a communication system, via a source access node of the communication system, a non-access stratum security context;

in an instance in which a radio link failure occurs between the apparatus and the source access node of the communication system during a data transfer operation over a control plane, send a first message to the mobility management node of the communication system through the target access node, the first message indicating that the radio link failure has occurred, at least a portion of the first message being protected using a cryptographic key created within or associated with the non-access stratum security context previously established between the user equipment and the mobility management node; and

after the mobility management node verifies the user equipment using the cryptographic key and initiates set up of a signaling interface with the target access node, receive, from the target access node, a second message acknowledging the radio link failure.

In an aspect, there is provided a non-transitory computer-readable storage medium for recovering a radio link, the non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to:

establish, between user equipment and a mobility management node of a communication system, via a source access node of the communication system, a non-access stratum security context;

in an instance in which a radio link failure occurs between the user equipment and the source access node of the communication system during a data transfer operation over a control plane, send a first message from the user equipment to the mobility management node of the communication system through a target access node of the communication system, the first message indicating that the radio link failure has occurred, at least a portion of the first message being protected using a cryptographic key created within or associated with the non-access stratum security context previously established between the user equipment and the mobility management node; and

after the mobility management node verifies the user equipment using the cryptographic key and initiates set up of a signaling interface with the target access node, receive, from the target access node, a second message acknowledging the radio link failure.In an aspect, method comprising:

in a communication system, in response to a radio link failure between a user equipment and a source access node of the communication system during a data transfer operation over a control plane, recovering the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is enabled via a mobility management node of the communication system using a non-access stratum security context previously established between the user equipment and the mobility management node, wherein recovering the radio link further comprises receiving, at the mobility management node, a first message from the user equipment, wherein the first message indicates that the user equipment has experienced the radio link failure with the source access node, and is protected using a cryptographic key created from the non-access stratum security context between the user equipment and the mobility management node, and wherein said recovering the radio link further comprises:

verifying, at the mobility management node, the user equipment using the cryptographic key;

initiating, at the mobility management node, set up of a signaling interface with the target access node;

sending, from the mobility management node, a second message to the user equipment through the target access node; and

retrieving, by the mobility management node, buffered data associated with the data transfer from the source access node. Advantageously, in illustrative embodiments, secure radio link recovery is achieved with no new context set up to protect the link between the given user equipment and the target access node, only the non-access stratum security context between the given user equipment and the mobility management node and its related cryptographic keys are used. For the sake of key separation, new keys may be computed using existing non-access stratum security parameters or non-access stratum message counts either in the uplink or in the downlink. In an aspect, there is provided an apparatus comprising:

a network node in a communication system, the network node being configured to function as a mobility management entity, wherein the network node is configured to establish a non-access stratum security context between a user equipment and the mobility management entity, and, in response to a radio link failure occurring between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, enable recovering the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is enabled via the mobility management entity using the non-access stratum security context previously established between the user equipment and the mobility management entity,

wherein the mobility management node is configured to enable recovering the radio link in response to the mobility management node receiving, from the user equipment, a first message indicating that the user equipment has experienced the radio link failure with the source access node, the first message being protected using a cryptographic key created from the non-access stratum security context between the user equipment and the mobility management node, and wherein said enabling recovery of the radio link further comprises:

verifying, at the mobility management node, the user equipment using the cryptographic key;

initiating, at the mobility management node, set up of a signaling interface with the target access node;

sending, from the mobility management node, a second message to the user

equipment through the target access node; and

retrieving, by the mobility management node, buffered data associated with the data transfer from the source access node. In aspect, there is provided a method comprising:

in a communication system, establishing, between a user equipment and a mobility management node of the communication system, a non-access stratum security context; and

in response to a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, recovering the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is initiated by the user equipment by sending a first message to the mobility management node of the communication system through the target access node using the non-access stratum security context previously established between the user equipment and the mobility management node, wherein the first message indicates that the user equipment has experienced the radio link failure with the source access node and is protected using a cryptographic key created from the non-access stratum security context between the user equipment and the mobility management node, and wherein said recovering the radio link further comprises:

receiving, at the user equipment, from the mobility management node, through the target access node of the communication system, a second message providing an acknowledgement of the radio link failure by the target access node, the second message being received within the non-access stratum security context previously established between the user equipment and the mobility management node for data transfer operations over said control plane. In an aspect, there is provided an apparatus comprising:

a user equipment configured for communication with a mobility management node of a communication system, the user equipment being configured to:

establish, between a user equipment and a mobility management node of the communication system, a non-access stratum security context; and

in response to a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, enable recovery of the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is initiated by the user equipment by sending a first message to the mobility management node of the communication system through the target access node using the non-access stratum security

context previously established between the user equipment and the mobility management node, wherein the first message indicates that the user equipment has experienced the radio link failure with the source access node and is protected using a cryptographic key created from the non-access stratum security context between the user equipment and the mobility management node, and wherein said enabling recovery of the radio link further comprises:

receiving, at the user equipment, from the mobility management node, through the target access node of the communication system, a second message providing an acknowledgement of the radio link failure by the target access node, the second message being received within the non-access stratum security context previously established between the user equipment and the mobility management node for data transfer operations over said control plane.

CLAIMS

What is claimed is:

1. A method for recovering a radio link, the method comprising:

establishing, in a communication system, a non-access stratum security context between user equipment and a mobility management node of the communication system; and

receiving a first message indicating a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, wherein at least a portion of the first message is protected using a cryptographic key created within the non-access stratum security context previously established between the user equipment and the mobility management node;

verifying, using the mobility management node, the user equipment using the cryptographic key;

initiating, via the mobility management node, within the non-access stratum security context previously established between the user equipment and the mobility management node, a radio link for the user equipment through a target access node of the communication system by initiating set up of a signaling interface with the target access node and sending a second message to the user equipment through the target access node; and

retrieving, by the mobility management node, buffered data associated with the data transfer over the control plane.

2. The method of claim 1, wherein the communication system comprises a Narrow Band Internet of Things (NB-IoT) network, and further wherein the user equipment comprises cellular IoT (CIoT) user equipment.

3. The method of claim 1, wherein the cryptographic key comprises an integrity key previously created in association with the non-access stratum security context previously established between the user equipment and the mobility management node.

4. The method of claim 1, wherein the cryptographic key is derived using an uplink message count or a downlink message count.

5. A non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to perform the method of claim 1.

6. An apparatus configured for recovering a radio link, the apparatus comprising:

a network node comprising a processor and memory, the network node being configured to function as a mobility management node of a communication system and to be in communication with user equipment and one or more access nodes of the communication system, wherein the network node is further configured to at least:

establish, in the communication system, a non-access stratum security context between the user equipment and the network node;

receive a first message indicating a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, wherein at least a portion of the first message is protected using a cryptographic key created within the non-access stratum security context previously established between the user equipment and the mobility management node;

verify the user equipment using the cryptographic key;

initiate, within the non-access stratum security context previously established between the user equipment and the network node, a radio link for the user equipment through a target access node of the communication system by initiating set up of a signaling interface with the target access node and sending a second message to the user equipment through the target access node; and

retrieve buffered data associated with the data transfer over the control plane.

7. The apparatus of claim 6, wherein the communication system comprises a Narrow Band Internet of Things (NB-IoT) network, and further wherein the user equipment comprises cellular IoT (CIoT) user equipment.

8. The apparatus of claim 6, wherein the cryptographic key comprises an integrity key previously created in association with the non-access stratum security context previously established between the user equipment and the mobility management node.

9. The apparatus of claim 6, wherein the cryptographic key is derived using an uplink message count or a downlink message count.

10. A method for recovering a radio link, the method comprising:

establishing, between user equipment and a mobility management node of a communication system, a non-access stratum security context; and

in response to a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, sending a first message from the user equipment to the mobility management node of the communication system through a target access node using the non-access stratum security context previously established between the user equipment and the mobility management node, the first message indicating that the radio link failure has occurred, at least a portion of the first message being protected using a cryptographic key created within the non-access stratum security context previously established between the user equipment and the mobility management node; and

after the mobility management node verifies the user equipment using the cryptographic key and initiates setup of a signaling interface with the target access node, receiving, from the target access node, a second message acknowledging the radio link failure.

11. The method of claim 10, wherein the communication system comprises a Narrow Band Internet of Things (NB-IoT) network, and further wherein the user equipment comprises cellular IoT (CIoT) user equipment.

12. The method of claim 10, wherein the cryptographic key comprises an integrity key previously created in association with the non-access stratum security context previously established between the user equipment and the mobility management node.

13. The method of claim 10, wherein the cryptographic key is derived using an uplink message count or a downlink message count.

14. The method of claim 10, wherein at least one of the first message and the second message is integrity protected using the cryptographic key previously created in association with the non-access stratum security context previously established between the user

equipment and the mobility management node, or at least a portion of the first message or the second message is encrypted using the cryptographic key previously created in association with the non-access stratum security context previously established between the user equipment and the mobility management node.

15. A non-transitory computer-readable storage medium having embodied therein executable program code that, when executed by a processor, causes the processor to perform the method of claim 10.

16. An apparatus configured for recovering a radio link, the apparatus comprising:

a processor; and

a memory storing program codes, wherein the memory and program codes are configured, with the processor, to cause the apparatus to at least:

establish, between the apparatus and a mobility management node of a communication system, a non-access security context; and

in response to a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, send a first message from the user equipment to the mobility management node of the communication system through a target access node using the non-access stratum security context previously established between the user equipment and the mobility management node, the first message indicating that the radio link failure has occurred, at least a portion of the first message being protected using a cryptographic key created within the non-access stratum security context previously established between the user equipment and the mobility management node; and

after the mobility management node verifies the user equipment using the cryptographic key and initiates setup of a signaling interface with the target access node, receive, from the target access node, a second message acknowledging the radio link failure.

17. The apparatus of claim 16, wherein the communication system comprises a Narrow Band Internet of Things (NB-IoT) network, and further wherein the user equipment comprises cellular IoT (CIoT) user equipment.

18. The apparatus of claim 16, wherein the cryptographic key comprises an integrity key previously created in association with the non-access stratum security context previously established between the user equipment and the mobility management node.

19. The apparatus of claim 16, wherein the cryptographic key is derived using an uplink message count or a downlink message count.

20. The apparatus of claim 16, wherein at least one of the first message and the second message is integrity protected using the cryptographic key previously created in association with the non-access stratum security context previously established between the user equipment and the mobility management node, or at least a portion of the first message or the second message is encrypted using the cryptographic key previously created in association with the non-access stratum security context previously established between the user equipment and the mobility management node.

21. A method for recovering a radio link, the method comprising:

establishing, in a communication system, a non-access stratum security context between user equipment and a mobility management node of the communication system;

receiving, at the mobility management node, within the non-access stratum security context previously established between the user equipment and the mobility management node of the communication system, a first message from the user equipment via a target access node of the communication system, the first message being protected using a cryptographic key associated with the non-access stratum security context previously established between the user equipment and the mobility management node;

verifying the user equipment using the cryptographic key;

in an instance in which the first message received from the user equipment indicates a radio link failure has occurred between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, initiating, via the mobility management node, set up of a signaling interface with the target access node;

sending a second message to the user equipment via the target access node, the second message acknowledging the radio link failure; and

retrieving buffered data associated with the data transfer over the control plane.

22. The method of claim 21, wherein the cryptographic key is generated using at least an uplink message count or a downlink message count.

23. The method of claim 21, wherein the second message comprises data associated with the data transfer.

24. The method of claim 23, wherein the data is at least one of previous buffered data and new data.

25. The method of claim 23, wherein the data is encrypted by an encryption key created during establishment of the non-access stratum security context previously established between the user equipment and the mobility management node.

26. The method of claim 25, wherein the encryption key comprises a non-access stratum encryption key.

27. The method of claim 21, further comprising:

retrieving, by the mobility management node, buffered data associated with the data transfer from the source access node.

28. The method of claim 21, wherein the radio link failure is detected by the user equipment.

29. The method of claim 21, wherein the radio link failure is detected by the source access node.

30. The method of claim 21, wherein the communication system comprises a Narrow Band Internet of Things (NB-IoT) network, and further wherein the user equipment comprises cellular IoT (CIoT) user equipment.

31. The method of claim 21, wherein the source access node and the target access node each comprise a base station distinct from the mobility management node of the communication system.

32. The method of claim 31, wherein the first message comprises a radio resource control connection re-establishment request from the user equipment and is received from the user equipment via the target access node, and wherein the first message comprises a request that the mobility management node authenticates the radio resource control connection re-establishment request from the user equipment based at least upon at least a non-access stratum count.

33. The method of claim 31, further comprising:

in an instance in which the mobility management node receives the first message comprising said radio resource control connection re-establishment request and said request that the mobility management node authenticates the radio resource connection re-establishment request, authenticating, using the mobility management node, the radio resource control connection re-establishment request received from the user equipment based on at least one of: the non-access stratum count, an identifier associated with the target access node, or the integrity key associated with the non-access stratum security context previously established between the user equipment and the mobility management node.

34. The method of claim 21, wherein the target access node is a different access node than the source access node.

35. An apparatus for recovering a radio link, the apparatus comprising:

one or more processors; and

one or more memories storing program instructions which, when executed by the one or more processors, cause the apparatus at least to:

establish, in a communication system, a non-access stratum security context between user equipment and the apparatus;

receive, at the apparatus, within the non-access stratum security context previously established between the user equipment and the apparatus, a first message from the user equipment via a target access node of the communication system , the first message being protected using a cryptographic key associated with the non-access stratum security context previously established between the user equipment and the mobility management node;

verify the user equipment using the cryptographic key;

in an instance in which the first message received from the user equipment indicates a radio link failure has occurred between the user equipment and a source access

node of the communication system during a data transfer operation over a control plane, initiate set up of a signaling interface with the target access node;

send a second message to the user equipment via the target access node of the communication system, the second message acknowledging the radio link failure; and

retrieve buffered data associated with the data transfer over the control plane.

36. The apparatus of claim 35, wherein the integrity key is generated using at least an uplink message count or a downlink message count.

37. The apparatus of claim 35, wherein the second message comprises data associated with the data transfer.

38. The apparatus of claim 37, wherein the data is at least one of previous buffered data or new data.

39. The apparatus of claim 37, wherein the data is encrypted by the cryptographic key created during establishment of the non-access stratum security context previously established between the user equipment and the apparatus.

40. The apparatus of claim 39, wherein the cryptographic key comprises a non-access stratum encryption key.

41. The apparatus of claim 35, wherein the radio link failure is detected by the user equipment.

42. The apparatus of claim 35, wherein the radio link failure is detected by the source access node.

43. The apparatus of claim 35, wherein the communication system comprises a Narrow Band Internet of Things (NB-IoT) network, and further wherein the user equipment comprises cellular IoT (CIoT) user equipment.

44. The apparatus of claim 35, wherein the source access node and the target access node each comprise a base station distinct from the apparatus.

45. The apparatus of claim 31, wherein the first message comprises a radio resource control connection re-establishment request from the user equipment and is received from the user equipment via the target access node, and wherein the first message comprises a request that the apparatus authenticates the radio resource control connection re-establishment request from the user equipment based at least upon at least a non-access stratum count.

46. The apparatus of claim 45, further comprising:

in an instance in which the apparatus receives the first message comprising said radio resource control connection re-establishment request and said request that the apparatus authenticates the radio resource connection re-establishment request, authenticating the radio resource control connection re-establishment request received from the user equipment based on at least one of: the non-access stratum count, an identifier associated with the target access node, or the integrity key associated with the non-access stratum security context previously established between the user equipment and the apparatus.

47. The apparatus of claim 35, wherein the target access node is a different access node than the source access node.

48. A non-transitory computer-readable storage medium for recovering a radio link, the non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to:

establish, in a communication system, a non-access stratum security context between user equipment and a mobility management node of the communication system;

receive, at the mobility management node, within the non-access stratum security context previously established between the user equipment and the mobility management node of the communication system, a first message from the user equipment via a target access node of the communication system, the first message being protected using a cryptographic key associated with the non-access stratum security context previously established between the user equipment and the mobility management node;

verify the user equipment using the cryptographic key;

in an instance in which the first message received from the user equipment indicates a radio link failure has occurred between the user equipment and a source access node of the

communication system during a data transfer operation over a control plane, initiate set up of a signaling interface with the target access node;

send a second message to the user equipment via the target access node of the communication system; and

retrieve buffered data associated with the data transfer over the control plane.

49. A method for recovering a radio link, the method comprising:

establishing, between user equipment and a mobility management node of a communication system, via a source access node of the communication system, a non-access stratum security context;

in an instance in which a radio link failure occurs between the user equipment and the source access node of the communication system during a data transfer operation over a control plane, initiating recovery of the radio link for the user equipment, through a target access node of the communication system, by sending a first message from the user equipment to the mobility management node of the communication system through the target access node, the first message indicating that the radio link failure has occurred, wherein the first message is protected using a cryptographic key associated with the non-access stratum security context previously established between the user equipment and the mobility management node;

after the mobility management node verifies the user equipment using the cryptographic key and initiates set up of a signaling interface with the target access node, receiving, from the target access node, a second message acknowledging the radio link failure.

50. The method of claim 49, further comprising:

including at least a non-access stratum count in the first message.

51. The method of claim 49, wherein the first message comprises a radio resource control connection re-establishment request.

52. The method of claim 49, wherein the first message comprises a request that the mobility management node authenticate the radio resource control connection re-establishment request.

53. The method of claim 49, wherein the target access node is a different access node than the source access node.

54. The method of claim 49, wherein the communication system comprises a Narrow Band Internet of Things (NB-IoT) network, wherein the apparatus comprises cellular IoT (CIoT) user equipment.

55. An apparatus for recovering a radio link, the apparatus comprising:

one or more processors; and

one or more memories storing program instructions which, when executed by the one or more processors, cause the apparatus at least to:

establish, between the apparatus and a mobility management node of a communication system, via a source access node of the communication system, a non-access stratum security context;

in an instance in which a radio link failure occurs between the apparatus and the source access node of the communication system during a data transfer operation over a control plane, send a first message to the mobility management node of the communication system through the target access node, the first message indicating that the radio link failure has occurred, at least a portion of the first message being protected using a cryptographic key created within or associated with the non-access stratum security context previously established between the user equipment and the mobility management node; and

after the mobility management node verifies the user equipment using the cryptographic key and initiates set up of a signaling interface with the target access node, receive, from the target access node, a second message acknowledging the radio link failure.

56. The apparatus of claim 55, wherein the program instructions, when executed by the one or more processors, further cause the apparatus at least to:

include at least a non-access stratum count in the first message.

57. The apparatus of claim 55, wherein the first message comprises a radio resource control connection re-establishment request.

58. The apparatus of claim 55, wherein the first message comprises a request that the mobility management node authenticate the radio resource control connection re-establishment request.

59. The apparatus of claim 55, wherein the target access node is a different access node than the source access node.

60. The apparatus of claim 55, wherein the communication system comprises a Narrow Band Internet of Things (NB-IoT) network, wherein the apparatus comprises cellular IoT (CIoT) user equipment.

61. A non-transitory computer-readable storage medium for recovering a radio link, the non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to:

establish, between user equipment and a mobility management node of a communication system, via a source access node of the communication system, a non-access stratum security context;

in an instance in which a radio link failure occurs between the user equipment and the source access node of the communication system during a data transfer operation over a control plane, send a first message from the user equipment to the mobility management node of the communication system through a target access node of the communication system, the first message indicating that the radio link failure has occurred, at least a portion of the first message being protected using a cryptographic key created within or associated with the non-access stratum security context previously established between the user equipment and the mobility management node; and

after the mobility management node verifies the user equipment using the cryptographic key and initiates set up of a signaling interface with the target access node, receive, from the target access node, a second message acknowledging the radio link failure.

62. A method comprising:

in a communication system, in response to a radio link failure between a user equipment and a source access node of the communication system during a data transfer operation over a control plane, recovering the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is enabled

via a mobility management node of the communication system using a non-access stratum security context previously established between the user equipment and the mobility management node, wherein recovering the radio link further comprises receiving, at the mobility management node, a first message from the user equipment, wherein the first message indicates that the user equipment has experienced the radio link failure with the source access node, and is protected using a cryptographic key created from the non-access stratum security context between the user equipment and the mobility management node, and wherein said recovering the radio link further comprises:

verifying, at the mobility management node, the user equipment using the cryptographic key;

initiating, at the mobility management node, set up of a signaling interface with the target access node;

sending, from the mobility management node, a second message to the user equipment through the target access node; and

retrieving, by the mobility management node, buffered data associated with the data transfer from the source access node.

63. The method of claim 62, wherein the communication system comprises a Narrow Band Internet of Things (NB-IoT) network, and further wherein the user equipment comprises cellular IoT (CIoT) user equipment.

64. An article of manufacture comprising a non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to perform the method of claim 62.

65. An apparatus comprising:

a network node in a communication system, the network node being configured to function as a mobility management entity, wherein the network node is configured to establish a non-access stratum security context between a user equipment and the mobility management entity, and, in response to a radio link failure occurring between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, enable recovering the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is

enabled via the mobility management entity using the non-access stratum security context previously established between the user equipment and the mobility management entity,

wherein the mobility management node is configured to enable recovering the radio link in response to the mobility management node receiving, from the user equipment, a first message indicating that the user equipment has experienced the radio link failure with the source access node, the first message being protected using a cryptographic key created from the non-access stratum security context between the user equipment and the mobility management node, and wherein said enabling recovery of the radio link further comprises:

verifying, at the mobility management node, the user equipment using the cryptographic key;

initiating, at the mobility management node, set up of a signaling interface with the target access node;

sending, from the mobility management node, a second message to the user equipment through the target access node; and

retrieving, by the mobility management node, buffered data associated with the data transfer from the source access node.

66. A method comprising:

in a communication system, establishing, between a user equipment and a mobility management node of the communication system, a non-access stratum security context; and

in response to a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, recovering the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is initiated by the user equipment by sending a first message to the mobility management node of the communication system through the target access node using the non-access stratum security context previously established between the user equipment and the mobility management node, wherein the first message indicates that the user equipment has experienced the radio link failure with the source access node and is protected using a cryptographic key created from the non-access stratum security context between the user equipment and the mobility management node, and wherein said recovering the radio link further comprises:

receiving, at the user equipment, from the mobility management node, through the target access node of the communication system, a second message providing an acknowledgement of the radio link failure by the target access node, the second message

being received within the non-access stratum security context previously established between the user equipment and the mobility management node for data transfer operations over said control plane.

67. An article of manufacture comprising a non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to perform the method of claim 66.

68. An apparatus comprising:

a user equipment configured for communication with a mobility management node of a communication system, the user equipment being configured to:

establish, between a user equipment and a mobility management node of the communication system, a non-access stratum security context; and

in response to a radio link failure between the user equipment and a source access node of the communication system during a data transfer operation over a control plane, enable recovery of the radio link for the user equipment through a target access node of the communication system, wherein the radio link recovery is initiated by the user equipment by sending a first message to the mobility management node of the communication system through the target access node using the non-access stratum security context previously established between the user equipment and the mobility management node, wherein the first message indicates that the user equipment has experienced the radio link failure with the source access node and is protected using a cryptographic key created from the non-access stratum security context between the user equipment and the mobility management node, and wherein said enabling recovery of the radio link further comprises:

receiving, at the user equipment, from the mobility management node, through the target access node of the communication system, a second message providing an acknowledgement of the radio link failure by the target access node, the second message being received within the non-access stratum security context previously established between the user equipment and the mobility management node for data transfer operations over said control plane.