

RADIO LINK RECOVERY FOR USER EQUIPMENT

Cross-Reference to Related Application

The present application claims priority to the U.S. Provisional Patent Application
5 identified as U.S. Serial No. 62/488,179 filed April 21, 2017 and entitled "Cellular Internet of
Things (CIoT) UE Radio Link Recovery Using NAS Keys," the disclosure of which is
incorporated by reference herein in its entirety.

Field

10 The field relates generally to communication systems, and more particularly, but not
exclusively, to security within such systems.

Background

This section introduces aspects that may be helpful to facilitating a better understanding
15 of the inventions. Accordingly, the statements of this section are to be read in this light and
are not to be understood as admissions about what is in the prior art or what is not in the prior
art.

Fourth generation (4G) wireless mobile telecommunications technology, also known as
Long Term Evolution (LTE) technology, was designed to provide high capacity mobile
20 multimedia with high data rates particularly for human interaction. Next generation or fifth
generation (5G) technology is intended to be used not only for human interaction, but also for
machine type communications in so-called Internet of Things (IoT) networks.

In an LTE example communication system, user equipment (UE) such as a mobile
device communicates over an air interface with a base station referred to as an evolved Node
25 B (eNB). The eNB is illustratively part of an access network of the system such as, for example,
an Evolved Universal Terrestrial Radio Access Network (E-UTRAN). The eNB provides
access for the UE to a Core Network (CN), which then provides access for the UE to a data
network such as a packet data network (e.g., PDN such as the Internet).

Narrow-Band IoT (NB-IoT) is a low power wide area network (LPWAN) radio
30 technology developed to enable connection of a wide range of devices (e.g., mobile devices,
sensors, smart meters, etc.) and services using a cellular communication network. For example,

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.

5

Summary

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

10 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
15 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
20 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.

Advantageously, in illustrative embodiments, secure radio link recovery is achieved
25 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.

Further embodiments are provided in the form of non-transitory computer-readable storage medium having embodied therein executable program code that when executed by a processor causes the processor to perform the above steps. Still further embodiments comprise apparatus with a processor and a memory configured to perform the above steps.

5 These and other features and advantages of embodiments described herein will become more apparent from the accompanying drawings and the following detailed description.

Brief Description of the Drawings

FIGS. 1A and 1B show a communication system in which radio link recovery is
10 implemented in an illustrative embodiment.

FIG. 2 shows a more detailed view of example user equipment and mobility management entity elements in an illustrative embodiment.

FIG. 3 shows a message flow for a radio link recovery process in an illustrative embodiment.

15 FIG. 4 shows a flow diagram of a radio link recovery process in an illustrative embodiment.

FIGS. 5A and 5B show a key computation and message flow for a radio link recovery process in another illustrative embodiment.

Detailed Description

Embodiments will be illustrated herein in conjunction with example communication systems and associated techniques for radio link recovery for user equipment. It should be understood, however, that the scope of the claims is not limited to particular types of communication systems and/or processes disclosed. Embodiments can be implemented in a
25 wide variety of other types of communication systems, using alternative processes and operations. For example, although illustrated in the context of wireless cellular systems utilizing 3GPP system elements such as an LTE Evolved Packet Core (EPC), the disclosed embodiments can be adapted in a straightforward manner to a variety of other types of communication systems including, but not limited to, WiMAX systems and Wi-Fi systems.
30 Also, while illustrative embodiments are particularly well suited for implementation in NB-IoT

networks, embodiments may be implemented in other networks wherein secure radio link recovery would be desired or needed.

Various illustrative embodiments are now described with reference to the drawings, wherein like reference numbers are used to refer to like elements throughout. In the following
5 description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of one or more illustrative embodiments. It may be evident, however, that such illustrative embodiment(s) may be practiced without these specific details, or with functionally similar or equivalent substitutions.

As illustratively used herein, Non-Access Stratum (NAS) is a functional layer of a
10 communication network that provides non-radio signaling for certain control plane functionalities between the UE and the Core Network (CN), transparent to the Radio Access Network (RAN). Such functionalities include, but are not limited to, mobility management, authentication, etc. Compare the NAS functional layer to the Access Stratum (AS), which is the functional layer below NAS that provides functionalities between the UE and the RAN
15 including, but not limited to, data transport over a wireless connection and radio resource management.

Support of radio link recovery and mobility for NB-IoT UEs using a CIoT optimization solution is under consideration by relevant standards bodies. This optimization solution for data transfer over an NAS layer is also referred to as Data Over NAS (DoNAS). Some
20 proposals include the use a Radio Resource Control (RRC) connection re-establishment procedure to allow context fetch and data forwarding from a serving (or source) eNB to a target eNB in a mobility scenario, similar to the active mode hand-over scenario of conventional practice. However, such proposals may pose a security risk that should be addressed to reduce potential harm from malicious actors.

More particularly, the UE's use of a Radio Resource Control (RRC) connection re-establishment procedure for a CIoT control plane optimization (DoNAS) may be vulnerable to attack, since the RRC connection of the CIoT UE to the eNB is not security protected. Various aspects of the following discussion may be illuminated by reference to TS23.401, Rel. 14, 2016-12, § 5.3.4B.2, TS 24.301, TS 33.401, each of which are incorporated by reference in
30 their entireties.

At least one current proposal for CIoT control plane optimization strategy includes a single short data packet strategy. However, it is realized herein that such a strategy may be compromised in terms of security. A threat analysis demonstrates that unless the UE-eNB link is protected, it is vulnerable to attacks. The following observations result from such a threat analysis:

(i) If the UE has a large amount of data to send or receive, the UE may have an access stratum (AS) context established with an eNB and a NAS context established with a Mobility Management Entity (MME). In such cases, the RRC messages should be protected. Without such context and protection, maintaining sustained connection of the UE with the eNB may not be possible, e.g., the UE connection can be hijacked or closed by an attacker UE. The eNB may also be subject to attacks with spurious data and/or control packets in the uplink (UL).

(ii) In some current proposals, it is not clear how mobility (e.g., handover of the UE from a serving or source eNB to a target eNB) is achieved without establishing an AS context in a reliable manner. Thus, for reliable X2 or S1 handover, an AS context needs to be established.

(iii) Without an AS security context in a serving or source eNB and target eNB, attack scenarios exist on the downlink (DL) and UL for a DoNAS UE and to its S1 Application Protocol (S1AP) link.

In various illustrative embodiments, one or more of the aforementioned security risks may be mitigated by enabling security for radio link recovery by protecting the link between the UE and the eNB utilizing the NAS context between the UE and an MME element (node) of the CN, and NAS keys associated with that context.

Before describing such secure radio link recovery processes according to illustrative embodiments, an illustrative communication system in which such processes may be implemented is described in connection with FIGS. 1A and 1B.

FIG. 1A shows a communication system 100 comprising user equipment (UE) 102 that communicates via an air interface 103 with an evolved Node B (eNB) 104. In this illustrative embodiment, the communication system 100 comprises a wireless cellular system, and more particularly, an LTE system. The communication system 100 illustrates at least part of an NB-IoT network.

The user equipment 102 may be a mobile station, and such a mobile station may comprise, by way of example, a mobile telephone, a computer, a sensor, a smart meter, or any other type of communication device. The term “user equipment” as used herein is therefore intended to be construed broadly, so as to encompass a variety of different types of mobile stations, subscriber stations or, more generally, communication devices, including examples such as a combination of a data card inserted in a communication device. Such communication devices are also intended to encompass devices commonly referred to as access terminals. In this illustrative embodiment, UE 102 is considered a CIoT UE.

The eNB 104 is illustratively part of an access network of the communication system 100. Such a radio access network may comprise, for example, an E-UTRAN having a plurality of base stations and one or more associated radio network controllers (RNCs). The base stations and RNCs are logically separate entities, but in a given embodiment may be implemented in the same physical network element, such as, for example, a base station router or femto cellular access point. The eNB may, more generally, be referred to as an access node.

While FIG. 1A illustrates 4G network nomenclature, it is to be understood that communication 100 may be a 5G network or a hybrid 4G/5G network. Thus, the access point referred to as an eNB in the 4G network, is referred to as a gNB in a 5G network. The access node (e.g., gNB/eNB) is illustratively part of a radio access network of the communication system. While the 4G network utilizes an E-UTRAN as the radio access network, in a 5G network, the access network is referred to as a 5G System and is described in 5G Technical Specification (TS) 23.501, V0.4.0, entitled “Technical Specification Group Services and System Aspects; System Architecture for the 5G System,” the disclosure of which is incorporated by reference herein in its entirety. In general, the access node (e.g., gNB/eNB) provides access for the UE to a CN, which then provides access for the UE to other UEs and/or a data network such as a packet data network (e.g., Internet). In this illustrative embodiment, a CIoT UE may access CIoT services via the data packet network.

The eNB 104 in this illustrative embodiment is operatively coupled to a Mobility Management Entity (MME) 106. MME 106 is one example of what is referred to as a “mobility management entity element,” “mobility management entity function” or, more generally, a “mobility management node.” A mobility management node, as used herein, is the element

or function in the communication system that enables, among other network operations, radio link recovery operations with the UE (through an eNB). The eNB 104 is also operatively coupled to a Serving Gateway (SGW) 108, which is operatively coupled to a Packet Data Network (PDN) Gateway (PGW) 110. PGW 110 is operatively coupled to a Packet Data
5 Network, e.g., Internet 112. MME 106 is also operatively coupled to SGW 108. MME 106 and SGW 108 are considered part of the CN. In some embodiments, PGW 110 is also considered part of the CN.

It is to be appreciated that this particular arrangement of system elements is an example only, and other types and arrangements of additional or alternative elements can be used to
10 implement a communication system in other embodiments. For example, in other embodiments, the system 100 may comprise authentication elements, as well as other elements not expressly shown herein.

Accordingly, the FIG. 1A arrangement is just one example configuration of a wireless cellular system, and numerous alternative configurations of system elements may be used. For
15 example, although only single UE, eNB, MME, SGW and PGW elements are shown in the FIG. 1A embodiment, this is for simplicity and clarity of description only. A given alternative embodiment may of course include larger numbers of such system elements, functions and/or nodes, as well as additional or alternative elements, functions and/or nodes of a type commonly associated with conventional system implementations.

It is also to be noted that while FIG. 1A illustrates system elements, functions and/or nodes as singular functional blocks, the various subnetworks that make up a 5G network are partitioned into so-called network slices. Network slices (network partitions) comprise a series of function sets (i.e., function chains) for each corresponding service type using network function virtualization (NFV) on a common physical infrastructure. The network slices are
25 instantiated as needed for a given service, e.g., enhanced mobile broadband (eMBB) service, massive IoT service, and mission-critical IoT service. A network slice or function set is thus instantiated when an instance of that network slice or function set is created. In some embodiments, this involves installing or otherwise running the network slice or function set on one or more host devices of the underlying physical infrastructure. UE 102 accesses one or
30 more of these services through the CN via eNB 104.

As mentioned above, a radio link failure may occur whereby the UE 102 loses connection with eNB 104 for a variety of typical reasons. In such a case, as depicted in FIG. 1B, when UE 102 loses connection with eNB 104 (depicted as Source eNB), it may re-establish connection (air interface 103) with eNB 114 (depicted as Target eNB) in accordance with radio link recovery processes according to illustrative embodiments.

It is to be appreciated that the communication system 100 illustrated in FIGS. 1A and 1B has both eNB 104 and eNB 114 being operatively coupled to the same MME 106 and SGW 108. However, in alternative embodiments, eNB 104 and eNB 114 can each be operatively coupled with different MMEs and/or different SGWs. As will also be explained below, eNB 104 and eNB 114 can actually be the same eNB.

When UE 102 loses connection with source eNB 104 and seeks to re-establish connection with target eNB 114, illustrative embodiments provide for a secure radio link recovery operation for UE 102 using the existing NAS security context and keys established between UE 102 and MME 106.

FIG. 2 shows a more detailed view of UE 102 and MME 106 in an illustrative embodiment. The UE 102 comprises a processor 200 coupled to a memory 202 and interface circuitry 204. The processor 200 of the UE 102 includes a recovery processing module 210 that may be implemented at least in part in the form of software executed by the processor. By “recovery processing,” it is meant to refer to processing steps (operations, processes, executed instructions, etc.) associated with radio link recovery according to one or more illustrative embodiments. More specifically, the recovery processing module 210 performs the user equipment operations of the radio link recovery processes described in conjunction with subsequent figures and otherwise herein. The memory 202 of the UE 102 includes a recovery storage module 212 that stores data generated during radio link recovery operations with the MME 106 through the target eNB 114.

The MME 106 comprises a processor 220 coupled to a memory 222 and interface circuitry 224. The processor 220 of the MME 106 includes a recovery processing module 230 that may be implemented at least in part in the form of software executed by the processor. The recovery processing module 230 performs the MME operations in the context of the radio link recovery processes between the UE and the target eNB described in conjunction with

subsequent figures and otherwise herein. The memory 222 of the MME 106 includes a recovery storage module 232 that stores data generated during radio link recovery operations with the UE 102 through the target eNB 114.

The processors 200 and 220 of the respective UE 102 and MME 106 may comprise, for example, microprocessors, application-specific integrated circuits (ASICs), digital signal processors (DSPs) or other types of processing devices, as well as portions or combinations of such elements.

The memories 202 and 222 of the respective UE 102 and MME 106 may be used to store one or more software programs that are executed by the respective processors 200 and 220 to implement at least a portion of the functionality described herein. For example, radio link recovery operations and other functionality as described in conjunction with subsequent figures and otherwise herein may be implemented in a straightforward manner using software code executed by processors 200 and 220.

A given one of the memories 202 or 222 may therefore be viewed as an example of what is more generally referred to herein as a computer program product or still more generally as a processor-readable (or computer-readable) storage medium that has executable program code embodied therein. Other examples of processor-readable storage media may include disks or other types of magnetic or optical media, in any combination. Illustrative embodiments can include articles of manufacture comprising such computer program products or other processor-readable storage media.

The memory 202 or 222 may more particularly comprise, for example, an electronic random access memory (RAM) such as static RAM (SRAM), dynamic RAM (DRAM) or other types of volatile or non-volatile electronic memory. The latter may include, for example, non-volatile memories such as flash memory, magnetic RAM (MRAM), phase-change RAM (PCRAM) or ferroelectric RAM (FRAM). The term "memory" as used herein is intended to be broadly construed, and may additionally or alternatively encompass, for example, a read-only memory (ROM), a disk-based memory, or other type of storage device, as well as portions or combinations of such devices.

The interface circuitries 204 and 224 of the respective UE 102 and MME 106 illustratively comprise transceivers or other communication hardware or firmware that allows

the associated system elements to communicate with one another in the manner described herein.

It is apparent from FIG. 2 that UE 102 is configured for communication with MME 106 and vice-versa via their respective interface circuitries 204 and 224. The UE 102 communicates with the MME 106 via eNB 114. This communication involves UE 102 sending data to the MME 106 via eNB 114 and the MME 106 sending data to the UE 102 via eNB 114. However, in alternative embodiments, other network elements may be operatively coupled between the UE and MME. The term “data” as used herein is intended to be construed broadly, so as to encompass any type of information that may be sent between user equipment and a core network via a base station element including, but not limited to, radio link recovery data, control data, audio, video, multimedia, data from any sensor device, etc.

It is to be appreciated that the particular arrangement of components shown in FIG. 2 is an example only, and numerous alternative configurations may be used in other embodiments. For example, the user equipment and mobility management entity can be configured to incorporate additional or alternative components and to support other communication protocols.

Other system elements, such as eNB 104, eNB 114, SGW 108, and PGW 110, may each also be configured to include components such as a processor, memory and network interface. These elements need not be implemented on separate stand-alone processing platforms, but could instead, for example, represent different functional portions of a single common processing platform. Such a processing platform may additionally comprise at least portions of an eNB and an associated RNC.

Illustrative embodiments provide radio link recovery for a CIoT UE (e.g., UE 102) that loses connection with a serving or source eNB (e.g., eNB 104) and seeks to re-establish connection with a target eNB (e.g., eNB 114). More particularly, as will be further explained below, illustrative embodiments use existing NAS keys and NAS context between the UE and MME (e.g., MME 106). A temporary AS context in the eNB may be created, in a radio link failure (RLF) scenario in a source eNB 104, until the UE 102 sends an NAS message directly to the MME 106 through a target eNB 114. Certain other embodiments may use alternate keys computed from the existing NAS context parameters or NAS message counts between the UE

and the MME to re-establish connection with a target eNB for key separation between regular NAS messages and radio link recovery procedures.

Note that in some embodiments the target eNB 114 may be the same as the source eNB 104, i.e., the UE seeks to re-establish a connection with the same eNB with which the UE lost
5 connection. In such case, that same eNB is a serving or source access node and then a target access node.

The MME 106 retrieves buffered packets at source eNB 104. The MME 106 sets up a new S1AP with target eNB 114 and sends further packets (including retrieved packets from source eNB 104). S1AP is the S1 Application Protocol which serves as the E-UTRAN radio
10 network layer signalling protocol for the S1 interface. S1AP supports the functions of S1 interface by signalling procedures defined in 3GPP TS 36.413, the disclosure of which is incorporated by reference herein in its entirety.

Advantageously, in accordance with illustrative embodiments, there is no other key computation other than one set of NAS keys. The MME 106 verifies the NAS message
15 indicating RLF using the regular NAS integrity key, K_{NASint} . NAS security context establishment and key generation, including but not limited to NAS integrity key K_{NASint} and NAS encryption key K_{NASenc} , are described in 3GPP TS 24.301 and 3GPP TS 33.401, the disclosures of which are incorporated by reference herein in their entireties. Radio link recovery procedure and key computation are specified in 3GPP TS 36.300, 3GPP TS 36.413
20 and 3GPP TS 33.401, the disclosures of which are incorporated by reference herein in their entireties.

An illustrative radio link recovery embodiment is described in FIG. 3. More particularly, FIG. 3 shows a message flow for a radio link recovery process for user equipment. It is to be appreciated that the system elements, functions and/or nodes shown in FIG. 3 (UE,
25 eNB (Source), eNB (Target), and MME) correspond to similarly labeled system elements, functions and/or nodes in FIGS. 1A, 1B, and 2. The numbered steps below correspond to the numbers of the message flow in FIG. 3.

1. An CIoT UE 102 (note that "CIoT" may also be referred to as "NBIoT" in the figures and elsewhere herein) seeking to perform control plane (CP) data transfer establishes an NAS
30 link (security context) with MME 106 for data transfer either in the UL or DL. MME 106 sets

up a S1AP path to a Source eNB 104 for packet transfer. Note that Source eNB 104 does not have any additional context for the UE 102.

2. During the data transfer, the UE 102 detects a Radio Link Failure (RLF). Additionally or alternatively, the RLF can be detected by the eNB 104 in some cases.

5 2a. If the eNB 104 detected the RLF, eNB 104 may proactively send the yet to be sent packet data units (PDUs associated with the data transfer mentioned in step 1) for the UE 102 in its buffer to the MME 106, reporting the RLF with the UE 102 indicated in the S1AP.

3/3a. When the UE 102 detects an RLF, the UE 102 selects a target eNB 114 (note again that this could be the same eNB as Source eNB 104), sends an NAS message to report
10 that it encountered an RLF. The NAS message is protected using the regular NAS integrity key K_{NASint} created as part of the NAS security context with the MME 106 mentioned in step 1.

4. The MME 106 verifies the NAS message using the regular K_{NASint} .

5. If the integrity check passes, the MME 106 retrieves unsent residual packets from
15 Source eNB 104 for the UE 102. If the Source eNB 104 had proactively send the residual data in step 2a, this packet transfer is not needed in this step. The MME 106 cancels the S1AP context and path to the Source eNB 104.

6a/6b. The MME 106 sends a new S1AP context set up to the target eNB 114. The MME 106 sends a NAS RLF acknowledgement to the UE 102, along with fresh data, via target
20 eNB 114. The NAS message is integrity protected using the same regular K_{NASint} and data is encrypted using NAS encryption key K_{NASenc} (both created as part of the NAS security context with the MME 106 mentioned in step 1).

Many advantages are realized from radio link recovery techniques according to illustrative embodiments. For example, some of these advantages include, but are not limited
25 to:

i) There is no new context set up to protect the link between the UE 102 and the target eNB 114, only the NAS context between the UE 102 and the MME 106, and NAS keys are used. If key separation from regular NAS messages is desired during radio link recovery, alternate keys may be computed from the current NAS context.

ii) Assumption is that for CIoT UEs, RLF (RRC Connection Re-establishment Request) is processed by an eNB protected by NAS context parameters. A CIoT UE, if it encounters an RLF, either sends a NAS message to the MME (indicating RLF) since they only have a NAS context or sends an RRC Connection Re-establishment Request message to the target eNB protected by the NAS context parameters.

iii) Since the NAS message or RRC Connection Re-establishment Request message is protected, neither attacks using these messages, nor path switch to another eNB, are possible.

iv) In case only NAS messages are used, changes at the existing elements, functions and/or nodes of the network are very minimal, i.e., two NAS messages between the UE 102 and the MME 106 to report and acknowledge back an RLF, two S1AP messages between the MME 106 and an eNB for buffer packet retrieval and S1AP path change.

v) The UE 102 uses only NAS context in the entire operation.

vi) The MME 106 does not need to transfer an NAS algorithm or identifier to other nodes.

Accordingly, in general, in response to a radio link failure between given user equipment (e.g., UE 102) and a source access node (e.g., eNB 104) of a communication system during a data transfer operation over a control plane, the process recovers the radio link for the given user equipment through a target access node (e.g., eNB 114) of the communication system. The radio link recovery is enabled via a mobility management node (e.g., MME 106) of the communication system using a NAS security context previously established between the given user equipment and the mobility management node.

For example, as illustrated in FIG. 4, a radio link recovery process according to an illustrative embodiment comprises the following steps.

Step 400 receives, at the mobility management node, a first NAS message from the given user equipment. The first NAS message indicates that the given user equipment has experienced an RLF with the source access node, and is protected using a cryptographic key (e.g., NAS integrity key K_{NASint}) created during previous establishment of the NAS security context between the given user equipment and the mobility management node.

Step 402 verifies, at the mobility management node, the given user equipment using the cryptographic key (K_{NASint}).

Step 404 initiates, at the mobility management node, set up of a signaling interface (e.g., SIAP) with the target access node.

Step 406 sends, from the mobility management node, a second NAS message to the given user equipment through the target access node. The second NAS message indicates an acknowledgment of the RLF, and is protected using the cryptographic key (K_{NASint}) created during previous establishment of the NAS security context between the given user equipment and the mobility management node. The second NAS message contains data associated with the data transfer. The data is previous buffered data and/or new data. The data is encrypted using another cryptographic key (NAS encryption key K_{NASenc}) created during previous establishment of the NAS security context between the given user equipment and the mobility management node.

Also in certain embodiments, for the sake of key separation between different procedures, alternate keys may be computed using NAS context parameters along with uplink message counts or downlink message counts.

In this alternate key embodiment, the NBIoT UE uses another key ' K_{RLFint} ' to protect the uplink NAS message to the MME which reports the RLF. As shown in the key derivation function (KDF) in FIG. 5A, the key calculation uses NAS Uplink Count parameter and K_{NASint} along with the current K_{ASME} . Since the NAS uplink count is included in every uplink NAS message, the receiver can use the count value in the received message to calculate the integrity key K_{RLFint} and avoid any mis-synchronization of message counts in radio link failure situations. This can help in proper security and count verification of the radio link failure message where multiple messages may be transmitted during unsteady radio conditions. It is possible to use 'NAS downlink count' also by the MME 106 in a downlink message for better synchronization during RLF occasions.

Thus, the message flow shown in FIG. 5B is the same as that shown in FIG. 3 for steps 1, 2, 2a, 3a, 5, 6a and 6b, but with respect to steps 3 and 4, instead of the regular key K_{NASint} , the UE 102 uses K_{RLFint} (e.g., derived as shown in FIG. 5A) to integrity protect the message to report the RLF.

It is to be appreciated that the naming of network elements mentioned herein are for illustrative purposes only. As such, none of the specific names or acronyms given to these network elements herein are intended to limit embodiments in any manner.

As indicated previously, the embodiments are not limited to the LTE context and the disclosed techniques can be adapted in a straightforward manner to a wide variety of other communication system contexts including, but not limited to, other 3GPP systems and non-3GPP systems.

The processor, memory, controller and other components of a user equipment or base station element of a communication system as disclosed herein may include well-known circuitry suitably modified to implement at least a portion of the radio link recovery functionality described above.

As mentioned above, embodiments may be implemented in the form of articles of manufacture each comprising one or more software programs that are executed by processing circuitry of user equipment, base stations or other elements of a communication system. Conventional aspects of such circuitry are well known to those skilled in the art and therefore will not be described in detail herein.

Also, embodiments may be implemented in one or more ASICs, FPGAs or other types of integrated circuit devices, in any combination. Such integrated circuit devices, as well as portions or combinations thereof, are examples of "circuitry" as that term is used herein.

A wide variety of other arrangements of hardware and associated software or firmware may be used in implementing the illustrative embodiments.

It should therefore again be emphasized that the various embodiments described herein are presented by way of illustrative example only, and should not be construed as limiting the scope of the claims. For example, alternative embodiments can utilize different communication system configurations, user equipment configurations, base station configurations, radio link recovery processes, messaging protocols and message formats than those described above in the context of the illustrative embodiments. These and numerous other alternative embodiments within the scope of the appended claims will be readily apparent to those skilled in the art.