SIGNALING WITH OPAQUE UE IDENTITIES

[0001] The present application claims priority to provisional U.S. Application Serial No. 60/771,974, filed February 10, 2006, entitled "OBSCURING TEMPORARY USER EQUIPMENT IDENTITIES," and provisional U.S. Application Serial No. 60/786,463, entitled "DOWNLINK DATA SCHEDULING WITH OPAQUE UE IDENTITIES IN E-UTRAN," filed March 27, 2006, both assigned to the assignee hereof and incorporated herein by reference.

BACKGROUND

I. Field

[0002] The present disclosure relates generally to communication, and more specifically to techniques for sending signaling with temporary identities.

II. Background

[0003] Wireless communication networks are widely deployed to provide various communication services such as voice, video, packet data, messaging, broadcast, etc. A wireless communication network may include many Node Bs (or base stations) that may communicate with many user equipments (UEs). The UEs may be assigned various identifiers or identities (IDs) used to uniquely identify these UEs for various purposes. In certain instances, the UE IDs may be sent over the air in the clear without any ciphering. This may make it possible for an eavesdropper or attacker to mount a linkability attack by monitoring a communication channel for messages and determining which messages are directed to the same UE over time. The linkability attack may be able to link messages to specific UEs but may not be able to determine the true identities of the UEs. The linkability attack may be used to track the locations of the UEs and may also be the basis of other more severe security attacks. For example, the attacker may be able to determine which UE ID is assigned to a particular UE by initiating a call to that UE and observing which UE IDs are used at approximately the same time.

[0004] There is therefore a need in the art for techniques to combat linkability attacks without imposing excessive computational burdens at the UEs and network entities.

SUMMARY

[0005] Techniques for deriving temporary IDs used to address specific UEs in a wireless communication network are described herein. The temporary IDs may be used for various types of messages sent to the UEs in the clear without ciphering via common channels. The techniques may be used to improve security, e.g., to foil linkability attacks.

[0006] In an aspect, at a network entity (e.g., a Node B), a first ID assigned to a UE and additional information such as, e.g., a salt value and/or shared secret data for the UE, may be transformed to obtain a second ID for the UE. The first ID may be a long UE ID that may be assigned to the UE by any network entity. The salt value is a non-static value that may be selected in any manner. The shared secret data may be any data that is known by both the UE and the network entity. The shared secret data may be agreed upon or determined in a separate operation, e.g., provisioning with the user's home network at the time of subscription. The first ID and/or the shared secret data may also be updated, e.g., whenever a signaling message is sent to the UE. A signaling message directed to the UE may be generated based on the second ID and may include signaling information, the second ID, the salt value, etc. The signaling message may also include a flag that may be set if loss of synchronization of the first ID is detected. The signaling message may be a scheduling message, a paging message, or some other message and may be sent via a common channel shared by the UE and other UEs. If the signaling message is a scheduling message, then a data transmission may be sent to the UE based on scheduling information included in the scheduling message.

[0007] In another aspect, at the UE, a message may be received via the common channel. The first ID and additional information such as, e.g., a salt value obtained from the received message and/or shared secret data for the UE, may be transformed to obtain the second ID, which may be used to determine whether the received message is intended for the UE. The received message may be matched based on a previous first ID or a current first ID depending on the flag (if sent) in the received message. If the received message is a scheduling message intended for the UE, then scheduling

information may be obtained from the received message, and the corresponding data transmission may be processed based on the scheduling information. The first ID and/or the shared secret data may be updated, e.g., whenever a signaling message intended for the UE is received. A re-synchronization mechanism may be used to ensure synchronization of the first ID and/or the shared secret data at the UE and the network entity.

[0008] Various aspects and features of the disclosure are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. 1 shows a wireless communication network.

[0010] FIG. 2 shows transmissions of scheduling messages and data.

[0011] FIG. 3 shows a process for receiving and using MAC IDs.

[0012] FIG. 4 shows a process for sending scheduling messages and data to a UE.

[0013] FIG. 5 shows a process for receiving scheduling messages and data at a UE.

[0014] FIG. 6 shows a process for receiving scheduling messages and data and updating a long UE ID.

[0015] FIG. 7 shows a process for receiving scheduling messages and data and updating a long UE ID and shared secret data.

[0016] FIG. 8 shows a process for receiving scheduling messages and data and updating a long UE ID and shared secret data based on a previous ID flag.

[0017] FIGS. 9A and 9B show operation of a re-synchronization mechanism.

[0018] FIG. 10 shows a process for sending signaling messages and data to a UE.

[0019] FIG. 11 shows an apparatus for sending signaling messages and data to a UE.

[0020] FIG. 12 shows a process for receiving signaling messages and data at a UE.

[0021] FIG. 13 shows an apparatus for receiving signaling messages and data at a UE.

[0022] FIG. 14 shows a block diagram of a UE, a Node B, and a system controller.

DETAILED DESCRIPTION

[0023] The techniques described herein may be used for various wireless communication networks such as Code Division Multiple Access (CDMA) networks, Time Division Multiple Access (TDMA) networks, Frequency Division Multiple Access (FDMA) networks, Orthogonal FDMA (OFDMA) networks, Single-Carrier

FDMA (SC-FDMA) networks, etc. The terms "networks" and "systems" are often used interchangeably. A CDMA network may implement a radio technology such as Universal Terrestrial Radio Access (UTRA), Evolved UTRA (E-UTRA), cdma2000, etc. UTRA includes Wideband-CDMA (W-CDMA) and Low Chip Rate (LCR). cdma2000 covers IS-2000, IS-95 and IS-856 standards. A TDMA network may implement a radio technology such as Global System for Mobile Communications (GSM). An OFDMA network may implement a radio technology such as Long Term Evolution (LTE), IEEE 802.20, Flash-OFDM®, etc. UTRA, E-UTRA, GSM and LTE are described in documents from an organization named "3rd Generation Partnership Project" (3GPP). cdma2000 is described in documents from an organization named "3rd Generation Partnership Project 2" (3GPP2). These various radio technologies and standards are known in the art. For clarity, certain aspects of the techniques are described below for LTE, and 3GPP terminology is used in much of the description below.

[0024] **FIG. 1** shows a wireless communication network 100 that includes an Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and a core network 140. The E-UTRAN includes multiple Node Bs 110 and a system controller 130. A Node B is generally a fixed station that communicates with the UEs and may also be referred to as an evolved Node B (eNode B), a base station, an access point, etc. Each Node B 110 provides communication coverage for a particular geographic area and supports communication for the UEs located within the coverage area. The term "cell" can refer to a Node B and/or its coverage area depending on the context in which the term is used. System controller 130 may couple to Node Bs 110 and provide coordination and control for these Node Bs. System controller 130 may be a single network entity or a collection of network entities, e.g., an Access Gateway (AGW), a Radio Network Controller (RNC), etc. System controller 130 may also originate and terminate messages for certain protocols and applications. Core network 140 may include various network entities that support various functions such as packet routing, user registration, mobility management, etc.

[0025] UEs 120 may be dispersed throughout network 100, and each UE may be stationary or mobile. A UE may also be referred to as a mobile station, a terminal, an access terminal, a subscriber unit, a station, etc. A UE may be a cellular phone, a personal digital assistant (PDA), a wireless device, a handheld device, a wireless

modem, a laptop computer, etc. A UE may communicate with one or more Node Bs on the downlink and/or uplink at any given moment. The downlink (or forward link) refers to the communication link from the Node Bs to the UEs, and the uplink (or reverse link) refers to the communication link from the UEs to the Node Bs.

[0026] A UE may have a variety of IDs used to identify the UE for various purposes. These UE IDs may have different context or scope (e.g., cell, paging area, etc.) and/or different life spans (e.g., temporary or permanent). For example, the UE may be assigned (i) a long UE ID that may have wide scope and/or long life span and (ii) one or more short UE IDs that may have more narrow scope and/or shorter life span. The UE IDs may be used for various purposes such as to direct scheduling messages, resource assignment messages, paging messages, and/or other messages to the UE.

[0027] **FIG. 2** shows example transmissions of scheduling messages and data on the downlink. The transmission timeline may be partitioned into transmission time intervals (TTIs). A TTI may have a predetermined time duration, e.g., 2 milliseconds (ms), and may be the smallest unit of time in which a UE may be scheduled and served.

[0028] In the example shown in FIG. 2, a Node B serves one UE in each TTI. The Node B may send a scheduling message for a scheduled UE on a control channel and may send a data block to this UE on a data channel some predetermined amount of time later. A scheduling message may also be referred to as a scheduling block, a scheduling word, a packet format, etc. A data block may also be referred to as a packet, a frame, etc. The scheduling messages sent on the control channel may be addressed to specific UEs based on Medium Access Control IDs (MAC IDs) assigned to these UEs. In general, different types of UE IDs may be used for different applications (e.g., scheduling information, paging, etc.) and/or different layers (e.g., MAC layer, physical layer, etc.). MAC ID is one type of UE ID that is commonly used for signaling. Each UE that might receive data on the data channel may process the control channel in each TTI to determine whether a scheduling message has been sent to that UE. Each UE may match the scheduling messages received on the control channel with its MAC ID to determine whether any scheduling message is intended for that UE. A UE that is scheduled in a given TTI may process the data channel to recover the data block sent to the UE.

[0029] In the example shown in FIG. 2, UE 1 is scheduled in TTI n, UE 3 is scheduled in TTI $n+1$, UE 2 is scheduled in TTIs $n+2$ and $n+3$, and UE 1 is

scheduled in TTI $n+4$. UE 1 receives scheduling messages in TTIs n and $n+4$ and processes the data channel in these TTIs to recover the data blocks sent to UE 1. UEs 2 and 3 similarly process the control and data channels to recover the scheduling messages and data blocks in their scheduled TTIs.

[0030] In the design shown in FIG. 2, the Node B may schedule individual UEs using the control channel and may send data to the scheduled UEs on the data channel. All UEs may receive the control channel. When a scheduling message indicates that a corresponding data block is intended for a particular UE, that UE knows to demodulate the data block from the data channel.

[0031] The MAC IDs may be assigned to the UEs by their serving Node Bs or some other network entities and may be used to identify these UEs for scheduling messages and other purposes. A MAC ID for a given UE may be valid for as long as the UE remains in an active state and is located in or sufficiently near the coverage area of its serving Node B. Since scheduling messages may be sent frequently, the MAC IDs should be as short as possible in order to reduce overhead of the control channel. The MAC IDs may be 16 bits long or may be of other lengths.

[0032] **FIG. 3** shows a process 300 performed by a UE to receive assignments of MAC IDs and to use the MAC IDs. The UE receives an assignment of MAC ID *a* from cell A, e.g., when the UE becomes active in cell A (block 312). While the UE remains active and in cell A, the UE monitors the control channel for scheduling messages addressed to MAC ID *a* (block 314). If a scheduling message is sent for MAC ID *a*, as determined in block 316, then the UE processes the data channel based on the information in the scheduling message (block 318). If the UE is not handed over to another cell, as determined in block 320, then the UE continues to monitor the control channel for scheduling messages addressed to MAC ID *a* (block 314).

[0033] Upon leaving cell A and being handed over to a new cell B, the UE receives an assignment of MAC ID *b* from cell B (block 322). The UE may then monitor the control channel for scheduling messages addressed to MAC ID *b* and receive data from the new cell B (not shown in FIG. 3). The UE may relinquish MAC ID *a* upon being handed over to cell B (block 324). Alternatively, the UE may retain MAC ID *a* until cell A is removed from a switching set maintained for the UE, which may occur at any time after the handover (also block 324). In any case, MAC ID *a* may be de-allocated from the UE and assigned to another UE in cell A.

[0034] In the design shown in FIG. 3, each cell may assign MAC IDs to UEs within that cell without coordination with other cells. A given MAC ID may be used in different cells to refer to different UEs. A MAC ID for a UE may be exchanged between cells (e.g., for handover of the UE) and may then be coupled with a cell ID as a disambiguation measure to uniquely identity the UE.

[0035] A MAC ID may act only as a "cookie" and may be used only for matching to allow a UE to recognize which scheduling messages are addressed to the UE. The UE may not need to be explicitly informed of its MAC ID in every scheduling message. Rather, the UE may need only sufficient information to allow it to answer the question "is this message for me or another UE?"

[0036] The MAC IDs may be used as temporary IDs that are not readily linked to permanent IDs of the UEs. However, a privacy threat may potentially exist if an eavesdropper or attacker can monitor the downlink and determine which transmissions address the same UE. For example, the attacker may monitor the control channel and determine that the messages sent in TTIs n and $n+4$ are both destined for UE 1 but may not know the true identity of UE 1. This type of attack is referred to as a linkability attack and may give rise to other related vulnerabilities. For example, the attacker may try to determine which MAC ID is assigned to a particular UE by simply initiating a packet data service to that UE and observing which MAC IDs have scheduled data at approximately the right time.

[0037] The scheduling messages may be ciphered to combat linkability attacks. However, ciphering the scheduling messages may impose excessive deciphering burden on the UEs, especially when each UE is required to decipher each scheduling message to determine whether that message is intended for that UE. It is desirable to secure the UE IDs without imposing this full deciphering burden.

[0038] In an aspect, a short UE ID may be derived for a UE based on a long UE ID assigned to the UE and may be used to address a message to the UE. In general, the long UE ID may be any ID assigned to the UE by any network entity and may have any life span. For example, the long UE ID may be (i) an ID assigned by a Node B such as a Cell Radio Network Temporary Identifier (C-RNTI), a MAC ID, etc., (ii) an ID assigned by the core network but known to the E-UTRAN, such as a Temporary Mobile Subscriber Identity (TMSI), a Packet TMSI (P-TMSI), etc., or (iii) some other ID or combination of IDs. The long UE ID may be assigned to the UE using a secure protocol

and sent over the air with ciphering. The short UE ID may be used to uniquely identify the UE for a particular application, e.g., scheduling, and may be of a suitable length. Different short UE IDs may be generated in a deterministic manner based on the same long UE ID and used for different messages addressed to the UE. The short UE IDs may be used in place of the MAC IDs for message matching.

[0039] In general, a short UE ID may be generated from a long UE ID based on any transform function such as an irreversible function that makes it difficult to determine the long UE ID from the short UE ID. For example, the transform function may be a cryptographic/secure hash function that maps a message (e.g., the long UE ID) to a digest (e.g., the short UE ID) and has cryptographic properties so that (i) the function between the message and its digest is irreversible and (ii) the likelihood of two messages mapping to the same digest is very small. The output of the hash function may be referred to as a digest, a signature, a hashed value, etc.

[0040] A short UE ID may be generated further based on a salt value σ, which is a non-static value that may be selected in any manner. Different salt values may be used with a single long UE ID to generate different short UE IDs for different signaling messages. This may be effective in combating correlation attacks and improving security.

[0041] In one design, a cryptographic/secure hash function is used as the transform function. The hash function is parameterized by the salt value σ and is denoted as H_σ. The hash function receives a long UE ID R_x and the salt value σ and provides a short UE ID denoted as $H_\sigma(R_x)$. The hash function should have the following properties:

- Knowing the salt value σ and the short UE ID $H_\sigma(R_x)$, it should be computationally infeasible to determine the long UE ID R_x,
- When the long UE ID R_x and the salt value σ are known, computing the short UE ID $H_\sigma(R_x)$ should be computationally easy, and
- For values of R_x in a range from which the long UE IDs are taken, the value $H_\sigma(R_x)$ should be, for each value of σ, in a range used for the short UE IDs.

[0042] The hash function H_σ may be defined based on any parameterized cryptographic hash function known in the art. One well-known example of a parameterized cryptographic hash function is a UNIX function 'crypt()'. Cryptographic hash functions such as SHA-1 (Secure Hash Algorithm), SHA-2 (which includes SHA-

224, SHA-256, SHA-384 and SHA-512), MD-4 (Message Digest), MD-5, or other secure hash algorithms known in the art may be used in a parameterized form. The salt value σ is a parameter that may be revealed without compromising the security of the hash function. The short UE ID $H_\sigma(R_x)$ and the salt value σ may be sent in a message directed to the UE assigned with the long UE ID R_x. The salt value σ, and thus the short UE ID, may change for different messages.

[0043] **FIG. 4** shows a process 400 performed by a network entity (e.g., a Node B or a system controller) for sending scheduling messages and data to a UE. A long UE ID is assigned to the UE, e.g., via secure signaling (block 412). In general, the long UE ID may be assigned by any network entity at any time and may have any life span. In each scheduling interval, e.g., each TTI, a determination is made whether the UE is scheduled for data transmission (block 414). If the UE is scheduled, then a short UE ID is generated based on the long UE ID and a salt value σ (block 416). A scheduling message addressed to the UE is generated based on scheduling information, the short UE ID, and the salt value (block 418). The scheduling message is sent via a common channel to the UE (block 420). Data is sent to the UE in accordance with the scheduling information in the scheduling message (block 422). The process then returns to block 414 for the next scheduling interval.

[0044] **FIG. 5** shows a process 500 performed by a UE for receiving scheduling messages and data. An assignment of a long UE ID is received, e.g., via secure signaling (block 512). In each scheduling interval, e.g., each TTI, a scheduling message is received from a common channel, and a short UE ID and a salt value σ are obtained from the received message (block 514). A short UE ID is also generated based on the long UE ID and the salt value σ obtained from the received message (block 516). The locally generated short UE ID is compared to the received short UE ID to determine whether the scheduling message is intended for the UE (block 518). If the two short UE IDs match, as determined in block 520, then the scheduling message is intended for the UE, and a corresponding data block is received and processed based on the scheduling information in the received message (block 522). After block 522 and also if the two short UE IDs do not match in block 520, the process returns to block 514 for the next scheduling interval.

[0045] The salt value σ may change with each scheduling message. In this case, an attacker may not be able to aggregate information for a given UE by monitoring the scheduling messages.

[0046] If the number of possible long UE IDs is sufficiently small, then an attacker may attempt to mount an exhaustion attack as follows. The attacker may generate a list of all possible long UE IDs, which may be denoted as $\{R_1, R_2, ..., R_K\}$, where K is the number of long UE IDs in the list. Upon seeing a scheduling message with salt value σ and short UE ID z, the attacker may generate all possible values of the form $H_\sigma(R_k)$, for R_1 through R_K, and may note the values of R_k for which $H_\sigma(R_k) = z$. This may produce multiple candidates for the long UE ID of the UE receiving the data. However, over time, the long UE IDs that are actually in use may appear over and over in candidate lists. This may allow the attacker to build a list of long UE IDs that are apparently in use. Once a "live" long UE ID is determined, the attacker may use the same algorithm as the UE to monitor scheduling messages (e.g., as shown in FIG. 5) and accumulate information intended for the UE.

[0047] Long UE IDs of a sufficiently large size may render an exhaustion attack computationally infeasible. For long UE IDs of L bits, an exhaustion attack may perform 2^L computations of the hash function for each salt value σ. The long UE ID size may be selected based on the desired degree of security, the expected life span of the long UE IDs, etc. If the life span of a long UE ID is sufficiently brief, then the exhaustion attack may succeed too late. By the time the attacker has processed a number of scheduling messages and determined that a given long UE ID is in use in a cell, the UE with that long UE ID may have already been assigned a new long UE ID by the E-UTRAN. The E-UTRAN may thus compensate for any security weakness through frequent assignments of new long UE IDs to the UEs via secure signaling.

[0048] In another aspect, a short UE ID may be derived for a UE based on a long UE ID assigned to the UE, shared secret data known to the UE and the E-UTRAN, and possibly a salt value σ. The shared secret data may be exchanged securely between the UE and the E-UTRAN, e.g., at the start of a call, during handover, etc. The shared secret data may be of any length (e.g., very long) since it may be sent over the air just once. Once established, the shared secret data may remain unchanged at the UE, e.g., for as long as the UE remains in a connected state or for some other duration.

Alternatively, the shared secret data may be updated by a hash function, as described below.

[0049] A transform function may receive the long UE ID, the shared secret data, and the salt value σ and generate a short UE ID. The shared secret data may act as another input to the transform function. The salt value σ and the short UE ID may be sent in a message whereas the shared secret data is not sent in the message. The use of the shared secret data to generate the short UE ID may thwart exhaustion attacks on the long UE IDs.

[0050] In yet another aspect, a long UE ID for a UE may be updated, e.g., whenever a short UE ID is generated. In general, the long UE ID may be updated based on any information, e.g., the current long UE ID, the shared secret data, the salt value σ, etc. The long UE ID may be updated based on a transform function F, which may be a hash function or some other function.

[0051] **FIG. 6** shows a process 600 performed by a UE for receiving scheduling messages and data and updating a long UE ID. An assignment of a long UE ID is received (block 612). In each scheduling interval, a scheduling message is received from a common channel, and a short UE ID and a salt value σ are obtained from the received message (block 614). A short UE ID is also generated based on the current long UE ID, the salt value σ obtained from the received message, and shared secret data for the UE (block 616). The locally generated short UE ID is compared to the received short UE ID to determine whether the scheduling message is intended for the UE (block 618). If the two short UE IDs match, as determined in block 620, then a corresponding data block is received and processed based on scheduling information in the received message (block 622). The long UE ID may also be updated based on the current long UE ID, the shared secret data, the salt value σ, and/or other information (block 624). After block 624 and also if the two short UE IDs do not match in block 620, the process returns to block 614 for the next scheduling interval.

[0052] The E-UTRAN may autonomously update the long UE ID for the UE whenever a scheduling message is sent to the UE. Similarly, the UE may autonomously update its long UE ID whenever a scheduling message intended for the UE is received from the E-UTRAN. If the long UE ID is updated separately by the E-UTRAN and UE, then the E-UTRAN and UE may have different values of the long UE ID in certain failure cases. For example, if a scheduling message is lost over the air, without the E-

UTRAN's knowledge, then the UE may not update its long UE ID as the E-UTRAN will expect. As another example, if the UE receives a scheduling message correctly but an acknowledgement (ACK) of that message is lost in transmission, then the UE may update its long UE ID but the E-UTRAN may not be informed. In both cases, the long UE ID maintained by the E-UTRAN may not match the long UE ID maintained by the UE. This de-synchronization may result in the E-UTRAN being unable to contact the UE using the long UE ID. A re-synchronization mechanism may be employed to ensure that the E-UTRAN and UE have the same long UE ID even in failure cases, as described below.

[0053] In yet another aspect, a long UE ID and shared secret data for a UE may be updated, e.g., whenever a short UE ID is generated. The long UE ID may be updated based on transform function F, and the shared secret data may be updated based on transform function G, each of which may be a hash function or some other function. Alternatively, the long UE ID and shared secret data may be jointly updated based on a common transform function. In any case, continually changing the shared secret data may offer additional measure of protection in cases where, for example, the shared secret data is short enough for exhaustion attacks to be feasible over a long term but within what would otherwise be the life span of the shared secret data.

[0054] **FIG. 7** shows a process 700 performed by a UE for receiving scheduling messages and data sent and updating a long UE ID and shared secret data. Process 700 includes blocks 712 through 722 that correspond to blocks 612 through 622, respectively, in FIG. 6. If the locally generated short UE ID matches the received short UE ID obtained from a received message, as determined in block 720, then the long UE ID and shared secret data may be updated based on the current long UE ID, the current shared secret data, a salt value σ obtained from the received message, and/or other information (block 722). A synchronization mechanism may be employed to ensure synchronization of the long UE ID and shared secret data between the UE and the E-UTRAN.

[0055] If the long UE ID and/or shared secret data are updated after each scheduling message, then the E-UTRAN should have (i) a reliable way of determining whether the UE received the scheduling message and hence performed the update or (ii) a reliable low-overhead recovery mechanism for situations where the update was not performed by the UE. Either (i) or (ii) may be achieved based on an ACK sent by the UE for the

scheduling message and/or an ACK sent by the UE for a data block associated with the scheduling message. Each ACK may be sent via dedicated signaling or embedded within an uplink message, e.g., a channel quality indicator (CQI) message. If the E-UTRAN receives an ACK for a data block, then the E-UTRAN may assume that the UE received the scheduling message and updated its long UE ID. In general, the UE may convey an ACK or some other information explicitly or implicitly and in any manner to indicate to the E-UTRAN that the UE has received the scheduling message.

[0056] If the E-UTRAN does not receive an ACK for a scheduling message sent to the UE, then there are two possibilities:

- The UE did not received the scheduling message and hence did not update its long UE ID and/or shared secret data, or
- The UE received the scheduling message, updated its long UE ID and/or shared secret data, and sent an ACK, which was lost.

In either case, the E-UTRAN may not know whether the UE has updated its long UE ID and/or shared secret data. The E-UTRAN may detect loss of synchronization if it does not receive an ACK from the UE for the scheduling message sent to the UE.

[0057] In one design, the E-UTRAN may assign a new long UE ID and/or new shared secret data to the UE whenever loss of synchronization is detected. The E-UTRAN may send the new long UE ID and/or new shared secret data via secure signaling and addressed to the UE by a stable ID such as a TMSI or P-TMSI.

[0058] In another design, a re-synchronization mechanism may be employed to recover synchronization whenever the E-UTRAN does not know whether the UE has updated its long UE ID and/or shared secret data. If loss of synchronization is detected, then the E-UTRAN may use the previous long UE ID and shared secret data to address the UE. The E-UTRAN may send a scheduling message with a "previous ID" flag set to '1' to indicate that the previous long UE ID and shared secret data are being used for the message. When the UE receives the scheduling message with the flag set, the UE may perform matching using both its previous and current long UE IDs and shared secret data. If there is a match, then the UE may update its long UE ID and shared secret data based on the long UE ID and shared secret data that produced the match.

[0059] **FIG. 8** shows a process 800 performed by a UE for receiving scheduling messages and data and updating a long UE ID and shared secret data based on a

previous ID flag. In each scheduling interval, a scheduling message is received from a common channel, and a previous ID flag in the received message is examined (block 812). If the flag is set, as determined in block 814, then whether the received message is for the UE is determined based on the previous long UE ID and the previous shared secret data for the UE (block 820). Block 820 may include blocks 616 and 618 in FIG. 6. If a match occurs and the received message is for the UE, as determined in block 822, then the long UE ID and/or shared secret data may be updated based on the previous long UE ID and/or the previous shared secret data (block 824). Otherwise, if a match does not occur in block 822 and also if the previous ID flag is not set in block 814, then whether the received message is for the UE is determined based on the current long UE ID and the current shared secret data (block 830). If a match occurs and the received message is for the UE, as determined in block 832, then the long UE ID and/or shared secret data may be updated based on the current long UE ID and/or the current shared secret data (block 834). After blocks 824 and 834, a corresponding data block is received and processed based on scheduling information in the received message (block 826). After block 826 and also if there is no match in block 832, the process returns to block 812 for the next scheduling interval.

[0060] **FIG. 9A** shows operation of the re-synchronization mechanism for a case in which a scheduling message does not reach the UE. The E-UTRAN and UE each begin with a previous long UE ID (PID) of R_0 and a current long UE ID (CID) of R_1 for the UE. The E-UTRAN sends a scheduling message with the current long UE ID of R_1 to the UE and updates the long UE ID as PID' = R_1 and CID' = R_2. The scheduling message is lost in transmission. The UE does not know that it should update its long UE ID and continues to use PID = R_0 and CID = R_1. The E-UTRAN does not receive an ACK from the UE and sends the next scheduling message for the UE using the previous long UE ID of R_1 and setting the previous ID flag.

[0061] The UE receives the scheduling message and, because the flag is set, checks the received message with the previous long UE ID of R_0, which does not match. The UE then checks the received message with the current long UE ID of R_1, which matches. The UE then recognizes that its current long UE ID of R_1 is equal to the previous long UE ID of R_1 at the E-UTRAN. The UE then updates its long UE ID once as PID = R_1 and CID = R_2 to match the updating by the E-UTRAN for the missed scheduling message. The UE further updates its long UE ID as PID = R_2 and CID = R_3

to match the updating by the E-UTRAN for the current scheduling message. The UE sends an ACK for the scheduling message. The E-UTRAN receives the ACK and updates the long UE ID as PID' = R_2 and CID' = R_3. The E-UTRAN recognizes that the UE has properly updated its long UE ID based on the received ACK and sends the next scheduling message for the UE using the current long UE ID of R_3 and with the previous ID flag cleared. The UE and E-UTRAN are now synchronized with the current long UE ID of R_3.

[0062] **FIG. 9B** shows operation of the re-synchronization mechanism for a case in which an ACK from the UE is lost en-route to the E-UTRAN. The E-UTRAN and UE each begin with a previous long UE ID of R_0 and a current long UE ID of R_1 for the UE. The E-UTRAN sends a scheduling message with the current long UE ID of R_1 to the UE and updates the long UE ID as PID' = R_1 and CID' = R_2. The UE receives the scheduling message, sends an ACK, and updates its long UE ID as PID = R_1 and CID = R_2. The ACK is lost, and the E-UTRAN does not know whether or not the UE has received the scheduling message and updated the long UE ID. The E-UTRAN sends the next scheduling message for the UE using the previous long UE ID of R_1 and setting the previous ID flag.

[0063] The UE receives the scheduling message and, because the flag is set, checks the received message with the previous long UE ID of R_1, which matches. The UE then recognizes that its previous long UE ID of R_1 is equal to the previous long UE ID of R_1 at the E-UTRAN. The UE then updates its long UE ID once as PID = R_2 and CID = R_3 to match the updating by the E-UTRAN for the current scheduling message. The UE sends an ACK for the scheduling message. The E-UTRAN receives the ACK and updates the long UE ID as PID = R_2 and CID = R_3. The E-UTRAN recognizes that the UE has properly updated its long UE ID based on the received ACK and sends the next scheduling message for the UE using the current long UE ID of R_3 and with the previous ID flag cleared. The UE and E-UTRAN are now synchronized with the current long UE ID of R_3.

[0064] In another design, the E-UTRAN updates the long UE ID and/or shared secret data for each scheduling message sent to the UE. The UE attempts to match a received message based on one or more long UE IDs. For example, the UE may attempt to match the received message based on the current long UE ID, then the previous long UE ID, then the future long UE ID, etc. Upon detecting a match, the UE

knows the current long UE ID at the E-UTRAN and synchronizes its long UE ID with that of the E-UTRAN.

[0065] The salt value σ may be selected to avoid collisions. A collision may occur when two long UE IDs R_x and R_y assigned to two UEs x and y are hashed to the same short UE ID, or $H_\sigma(R_x) = H_\sigma(R_y)$. If a scheduling message is sent for UE x with this short UE ID, then UEs x and y may each detect the scheduling message as being directed to that UE and may assume that the corresponding data block is intended for the UE. This presents no problem for UE x, which receives the intended data block. However, UE y may receive a spurious data block, which if ciphered may produce random deciphered data. In any case, the spurious data block may be out of place in a data stream for UE y, and the resulting effect may depend on the particular behavior of the application receiving the data stream.

[0066] In general, impact due to collisions of long UE IDs may be dependent on the type of signaling being sent with the long UE IDs, the application behavior, etc. In some situations, collisions may be acceptable, e.g., when the data scheduled for the UE can only be understood by the intended recipient. Nevertheless, the E-UTRAN may attempt to prevent collisions in order to avoid possible adverse effects. Collisions may be avoided in various manners.

[0067] In one design for avoiding collisions, a Node B (or some other network entity) selects salt values known to have no collisions. The Node B may maintain a set of all long UE IDs assigned or assignable to the UEs within its coverage. For each possible salt value σ, the Node B may generate a set of short UE IDs based on the set of long UE IDs and that salt value. The Node B may scan the set of short UE IDs for duplicates and may reject this salt value if duplicates are detected. In general, a salt value that causes a collision for certain long UE IDs may still be used for other long UE IDs. However, in order to simplify implementation, the Node B may maintain a list of salt values that result in no duplicates over the entire set of long UE IDs. The salt values in this list may be selected for use. Collisions may also be avoided in other manners.

[0068] In general, a short UE ID may be generated based on any piece or pieces of information. For example, the short UE ID may be generated based on only the long UE ID, the long UE ID and the salt value, the long UE ID and the shared secret data,

only the shared secret data, the shared secret data and the salt value, or a combination of the long UE ID, the salt value, and the shared secret data.

[0069] In general, any information may be updated by the E-UTRAN and UE. For example, only the salt value, only the long UE ID, only the shared secret data, the salt value and the long UE ID, the salt value and the shared secret data, the long UE ID and the shared secret data, or a combination of the salt value, the long UE ID, and the shared secret data may be updated. The updating may be performed after each scheduling message, after each time interval of a predetermined duration, etc.

[0070] For clarity, the use of short UE IDs for scheduling messages has been described above. The short UE IDs may also be used for other signaling messages such as paging messages, resource assignment messages, etc. For example, a short UE ID may be generated for a paging message directed to a specific UE. The short UE ID may be sent on a paging indicator channel to inform the UE that a paging message is sent on a paging channel to the UE. The short UE ID may also be sent with the paging message to address the message to the UE.

[0071] **FIG. 10** shows a process 1000 performed by a network entity in a wireless communication network to send signaling messages and data to the UEs. The network entity may be a Node B, a system controller, etc., depending on the signaling messages being sent.

[0072] A first ID assigned to a UE and additional information such as, e.g., a salt value and/or shared secret data for the UE, may be transformed to obtain a second ID for the UE (block 1012). The first ID may be a long UE ID that may be assigned to the UE by any network entity. The first ID may be assigned to the UE by the same network entity that sends signaling messages to the UE or by another network entity. The first ID may be applicable in a single cell or across multiple cells. The first ID, the salt value, and/or the shared secret data may be transformed based on an irreversible function, a hash function, or some other function to obtain the second ID. The salt value may be changed each time the first ID is transformed and may be selected to avoid collisions among a plurality of first IDs assigned to a plurality of UEs. Other types of additional information (e.g., time information such as a frame number) may also be used with the first ID to generate the second ID. The first ID and/or the shared secret data may be updated, e.g., whenever a scheduling message is sent to the UE

(block 1014). A previous first ID may be used if loss of synchronization of the first ID is detected, and a current first ID may be used if loss of synchronization is not detected.

[0073] A signaling message directed to the UE may be generated based on the second ID (block 1016). The signaling message may be a scheduling message, a paging message, or some other message and may include signaling information, the second ID, the salt value, etc. The signaling message may also include a flag that may be set if loss of synchronization of the first ID is detected. The signaling message may be sent via a common channel shared by the UE and other UEs (block 1018). If the signaling message is a scheduling message, then a data transmission may be sent based on scheduling information in the scheduling message (block 1020).

[0074] **FIG. 11** shows an apparatus 1100 for sending signaling messages and data to the UEs. Apparatus 1100 includes means for transforming a first ID assigned to a UE and additional information such as, e.g., a salt value and/or shared secret data for the UE, to obtain a second ID for the UE (module 1112), means for updating the first ID and/or the shared secret data, e.g., whenever a scheduling message is sent to the UE (module 1114), means for generating a signaling message directed to the UE based on the second ID (module 1116), means for sending the signaling message via a common channel shared by the UE and other UEs (module 1118), and means for sending a data transmission based on scheduling information in the signaling message (module 1120). Modules 1112 to 1120 may comprise processors, electronics devices, hardware devices, electronics components, logical circuits, memories, etc., or any combination thereof.

[0075] **FIG. 12** shows a process 1200 performed by a UE to receive signaling messages and data from a wireless communication network. A message may be received via a common channel shared by a plurality of UEs (block 1212). A first ID assigned to the UE and additional information such as, e.g., a salt value obtained from the received message and/or shared secret data for the UE, may be transformed to obtain a second ID for the UE (block 1214). The first ID may be assigned to the UE by the same network entity that sent the received message. Alternatively, the first ID may be assigned to the UE by one network entity, and the received message may be sent by another network entity.

[0076] Whether the received message is intended for the UE may be determined based on the second ID (block 1216). A previous first ID and/or a current first ID may be transformed depending on a flag in the received message. For example, the previous

first ID may be transformed to obtain a previous second ID, which may be used to determine whether the received message is intended for the UE. If the received message does not match with the previous second ID, then the current first ID may be transformed to obtain a current second ID, which may be used to determine whether the received message is intended for the UE. Matching may also be attempted with the current first ID and then with the previous first ID. For message matching, a third ID may be obtained from the received message and compared to the second ID to determine whether the received message is intended for the UE. The message matching may also be performed in other manners. The first ID and/or the shared secret data may be updated, e.g., if the received message is intended for the UE (block 1218).

[0077] If the received message is a scheduling message intended for the UE, then scheduling information may be obtained from the received message (block 1220). A data transmission may be processed based on the scheduling information (block 1222).

[0078] **FIG. 13** shows an apparatus 1300 for receiving signaling messages and data. Apparatus 1300 includes means for receiving a message via a common channel shared by a plurality of UEs (module 1312), means for transforming a first ID assigned to a UE and additional information such as, e.g., a salt value obtained from the received message and/or shared secret data for the UE, to obtain a second ID for the UE (module 1314), means for determining whether the received message is intended for the UE based on the second ID (module 1316), means for updating the first ID and/or the shared secret data, e.g., if the received message is intended for the UE (module 1318), means for obtaining scheduling information from the received message if it is a scheduling message intended for the UE (module 1320), and means for processing a data transmission based on the scheduling information (module 1322). Modules 1312 to 1322 may comprise processors, electronics devices, hardware devices, electronics components, logical circuits, memories, etc., or any combination thereof.

[0079] **FIG. 14** shows a block diagram of a design of a UE 120, a Node B 110, and system controller 130 in FIG. 1. On the uplink, data and signaling to be sent by UE 120 are processed (e.g., formatted, encoded, and interleaved) by an encoder 1422 and further processed (e.g., modulated, channelized, and scrambled) by a modulator (MOD) 1424 to generate output chips. A transmitter (TMTR) 1432 then conditions (e.g., converts to analog, filters, amplifies, and frequency upconverts) the output chips and generates an uplink signal, which is transmitted via an antenna 1434. On the downlink, antenna 1434

receives a downlink signal transmitted by Node B 110. A receiver (RCVR) 1436 conditions (e.g., filters, amplifies, frequency downconverts, and digitizes) the received signal from antenna 1434 and provides samples. A demodulator (DEMOD) 1426 processes (e.g., descrambles, channelizes, and demodulates) the samples and provides symbol estimates. A decoder 1428 further processes (e.g., deinterleaves and decodes) the symbol estimates and provides decoded data. Encoder 1422, modulator 1424, demodulator 1426, and decoder 1428 may be implemented by a modem processor 1420. These units may perform processing in accordance with the radio technology (e.g., LTE, W-CDMA, etc.) implemented by the wireless communication network.

[0080] A controller/processor 1440 directs the operation at UE 120. Controller/processor 1440 may perform process 500 in FIG. 5, process 600 in FIG. 6, process 700 in FIG. 7, process 800 in FIG. 8, process 1200 in FIG. 12 and/or other processes for the techniques described herein. A memory 1442 stores program codes and data for UE 120 and may also store long and short UE IDs for UE 120.

[0081] FIG. 14 also shows a design of Node B 110 and system controller 130. Node B 110 includes a controller/processor 1450 that performs various functions for communication with the UEs, a memory 1452 that stores program codes and data for Node B 110, and a transceiver 1454 that supports radio communication with the UEs. Controller/processor 1450 may perform process 1000 in FIG. 10 and/or other processes for the techniques described herein. Memory 1452 may store long and short UE IDs for the UEs served by Node B 110, or NB UE IDs. System controller 130 includes a controller/processor 1460 that performs various functions to support communication for the UEs and a memory 1462 that stores program codes and data for system controller 130. Controller/processor 1460 may perform process 1000 in FIG. 10 and/or other processes for the techniques described herein. Memory 1462 may store long and short UE IDs for the UEs served by system controller 130, or SC UE IDs.

[0082] The techniques described herein may be implemented by various means. For example, these techniques may be implemented in hardware, firmware, software, or a combination thereof. For a hardware implementation, the processing units used to perform the techniques at a given entity (e.g., a UE, a Node B, a system controller, etc.) may be implemented within one or more application specific integrated circuits (ASICs), digital signal processors (DSPs), digital signal processing devices (DSPDs), programmable logic devices (PLDs), field programmable gate arrays (FPGAs),

processors, controllers, micro-controllers, microprocessors, electronic devices, other electronic units designed to perform the functions described herein, a computer, or a combination thereof.

[0083] For a firmware and/or software implementation, the techniques may be implemented with modules (e.g., procedures, functions, etc.) that perform the functions described herein. The firmware and/or software codes may be stored in a memory (e.g., memory 1442, 1452 or 1462 in FIG. 14) and executed by a processor (e.g., processor 1440, 1450 or 1460). The memory may be implemented within the processor or external to the processor.

[0084] The previous description of the disclosure is provided to enable any person skilled in the art to make or use the disclosure. Various modifications to the disclosure will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other variations without departing from the spirit or scope of the disclosure. Thus, the disclosure is not intended to be limited to the examples described herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

CLAIMS

1. An apparatus comprising:

means for transforming a first identifier (ID) assigned to a user equipment (UE) and additional information to obtain a second ID for the UE;

means for generating a signaling message directed to the UE based on the second ID; and

means for sending the signaling message via a common channel shared by the UE and other UEs.

2. The apparatus of claim 1, wherein the additional information comprises shared secret data for the UE, and wherein the means for transforming the first ID comprises means for transforming the first ID and the shared secret data for the UE to obtain the second ID.

3. A computer-readable medium including instructions stored thereon, comprising:

a first instruction set for transforming a first identifier (ID) assigned to a user equipment (UE) and additional information to obtain a second ID for the UE;

a second instruction set for generating a signaling message directed to the UE based on the second ID; and

a third instruction set for sending the signaling message via a common channel shared by the UE and other UEs.

4. The computer-readable medium of claim 3, wherein the additional information comprises shared secret data for the UE, and wherein the first instruction set is for transforming the first ID and the shared secret data for the UE to obtain the second ID.

5. An apparatus comprising:

a processor configured to receive a message via a common channel shared by a plurality of user equipments (UEs), to transform a first identifier (ID) assigned to a UE and additional information to obtain a second ID for the UE, and to determine whether the received message is intended for the UE based on the second ID; and

a memory coupled to the processor.

6. The apparatus of claim 5, wherein the processor is configured to receive an assignment of the first ID from a first network entity and to receive the message from a second network entity.

7. The apparatus of claim 5, wherein the processor is configured to receive an assignment of the first ID and the message from a single network entity.

8. The apparatus of claim 5, wherein the additional information comprises a salt value, and wherein the processor is configured to obtain the salt value from the received message and to hash the first ID and the salt value to obtain the second ID.

9. The apparatus of claim 5, wherein the additional information comprises shared secret data for the UE, and wherein the processor is configured to transform the first ID and the shared secret data for the UE to obtain the second ID.

10. The apparatus of claim 5, wherein the additional information comprises a salt value and shared secret data for the UE, and wherein the processor is configured to obtain the salt value from the received message and to transform the first ID, the shared secret data for the UE, and the salt value to obtain the second ID.

11. The apparatus of claim 9, wherein the processor is configured to update the first ID, or the shared secret data, or both the first ID and the shared secret data.

12. The apparatus of claim 9, wherein the processor is configured to update the first ID, or the shared secret data, or both the first ID and the shared secret data after each reception of a message intended for the UE.

13. The apparatus of claim 11, wherein the processor is configured to transform a previous first ID or a current first ID based on a flag in the received message.

14. The apparatus of claim 11, wherein the processor is configured to transform a previous first ID and the additional information to obtain a previous second ID and to determine whether the received message is intended for the UE based on the previous second ID and, if the received message does not match with the previous second ID, to transform a current first ID and the additional information to obtain a current second ID and to determine whether the received message is intended for the UE based on the current second ID.

15. The apparatus of claim 11, wherein the processor is configured to transform a current first ID and the additional information to obtain a current second ID and to determine whether the received message is intended for the UE based on the current second ID and, if the received message does not match with the current second ID, to transform a previous first ID and the additional information to obtain a previous second ID and to determine whether the received message is intended for the UE based on the previous second ID.

16. The apparatus of claim 5, wherein the processor is configured to obtain a third ID from the received message and to compare the second ID to the third ID to determine whether the received message is intended for the UE.

17. The apparatus of claim 5, wherein the processor is configured to determine that the received message is intended for the UE, to obtain scheduling information from the received message, and to process a data transmission based on the scheduling information.

18. A method comprising:

receiving a message via a common channel shared by a plurality of user equipments (UEs);

transforming a first identifier (ID) assigned to a UE and additional information to obtain a second ID for the UE; and

determining whether the received message is intended for the UE based on the second ID.

19. The method of claim 18, wherein the additional information comprises shared secret data for the UE, and wherein the transforming the first ID comprises transforming the first ID and the shared secret data for the UE to obtain the second ID.

20. The method of claim 18, wherein the additional information comprises a salt value and shared secret data for the UE, and wherein the transforming the first ID comprises transforming the first ID, the shared secret data for the UE, and the salt value from the received message to obtain the second ID.

21. The method of claim 19, further comprising:

updating the first ID, or the shared secret data, or both the first ID and the shared secret data.

22. An apparatus comprising:

means for receiving a message via a common channel shared by a plurality of user equipments (UEs);

means for transforming a first identifier (ID) assigned to a UE and additional information to obtain a second ID for the UE; and

means for determining whether the received message is intended for the UE based on the second ID.

23. The apparatus of claim 22, wherein the additional information comprises shared secret data for the UE, and wherein the means for transforming the first ID comprises means for transforming the first ID and the shared secret data for the UE to obtain the second ID.