[0001] METHOD AND APPARATUS FOR DATA SECURITY AND AUTOMATIC REPEAT REQUEST IMPLEMENTATION IN A WIRELESS COMMUNICATION SYSTEM

[0002] FIELD OF INVENTION

[0003] The present invention is related to wireless communication systems. More particularly, the present invention is related to a method and apparatus for data security and automatic repeat request (ARQ) implementation in a wireless communication system.

[0004] BACKGROUND

[0005] The third generation partnership project (3GPP) has initiated a long term evolution (LTE) project to bring new technology, new network architecture and configuration, and new applications and services to a wireless cellular network in order to provide improved spectral efficiency, reduced latency, faster user experiences, and richer applications and services with less cost.

[0006] In the wireless communication network, user data privacy and user data accuracy are always the main concerns. The data privacy and accuracy concerns are addressed by data block encryption, (i.e., ciphering for both user data and control messages), and implementation of ARQ protocol on the data path to recover lost or inaccurate data.

[0007] Figure 1 shows a conventional third generation (3G) universal terrestrial radio access network (UTRAN) 100. The UTRAN 100 includes a user equipment (UE) 110, a Node-B 120 and a radio network controller (RNC) 130. In the UTRAN 100, security procedural entities 112, 132, (i.e., cipher entities), are located in the UE 110 and the RNC 130, along with outer ARQ entities 114, 134, (i.e., radio link control (RLC) acknowledged mode (AM) entities). Both the cipher entities 112, 132 and the outer ARQ entities 114, 134 use RLC packet data unit (PDU) sequence numbers (SNs) as an input for the data block encryption/decryption and for ARQ operation.

[0008] In LTE, the architecture of the UTRAN 100 will be changed. The RNC 130 no longer exists. An evolved Node-B (eNode-B) will assume medium access control (MAC) and some radio resource control (RRC) functionalities. Original RLC sub-layer and the data security, (or ciphering), entity in the RNC 130 will have to be re-located in LTE to maintain the necessary data encryption and data ARQ functionalities. Given this new LTE network architecture, the issue is where the outer ARQ entities and the data security entities shall be located and how the two formerly co-located entities cooperate to work in the LTE system.

[0009] Figure 2 shows a proposed LTE network 200 with respect to outer ARQ entities. The LTE network 200 includes a UE 210, an eNode-B 220 and an access gateway (aGW) 230. In the proposed LTE network 200, outer ARQ entities 212 and 222 are located in the UE 210 and the eNode-B 220, respectively. Placing the outer ARQ entity 222 in the eNode-B 220 would be optimal with respect to retransmission delay, retransmission PDU size, simple protocol complexity, low buffering requirements and possible hybrid ARQ (H-ARQ) and outer ARQ interaction. However, this approach does not have a user data security process in mind.

[0010] It would be optimal to place user data security entities in the UE 210 and the aGW 230, which is a network anchor node, for the following reasons. First, the security parameters of the UE 210 (or user), (such as UE security credentials, encryption key sets, or the like), may be kept in a safer place, (i.e., aGW 230), where the interaction of UE authentication with a home subscriber server (HSS) is administered. Second, user data may be protected all the way from the aGW 230 to the UE 210 without requiring an additional scheme to achieve at least the same level of security as in the conventional UTRAN 100. Third, eNode-B physical protection may be simplified, thus increasing the total system security protection and the system cost effectiveness, and simplifying the eNodeB functionality. Forth, inter-Node-B handover and inter-aGW handover would be easier from less security context transfer, (between eNode-Bs if the data security entity is located on an eNode-

B). However, the drawback on this approach is that the outer ARQ is not taken into consideration.

[0011] Simply putting the data security entities in the eNode-B 220 or putting outer ARQ entities in the aGW 230 will not meet LTE security requirements and data retransmission performance requirements. Therefore, it would be desirable to provide an architecture and operational scheme which provides the best possible performances with respect to the data security functionality and the outer ARQ functionality for the new LTE network architecture.

[0012] SUMMARY

[0013] The present invention is related to a method and apparatus for implementing data security and ARQ in a wireless communication system. Cipher entities are included in a wireless transmit/receive unit (WTRU) and an aGW, and outer ARQ, (or RLC), entities are included in the WTRU and an eNode-B. Each cipher entity is located on top of an outer ARQ entity. The cipher entities cipher and decipher a data block by using a generic SN assigned to the data block. The outer ARQ entities may segment the ciphered data block to multiple PDUs, may concatenate multiple ciphered data blocks to a PDU, or may generate one PDU from one data block. The outer ARQ entities may segment or re-segment the PDU when a transmission failure occurs.

[0014] BRIEF DESCRIPTION OF THE DRAWINGS

[0015] Figure 1 shows a conventional 3G UTRAN.

[0016] Figure 2 shows a proposed LTE network architecture with respect to outer ARQ entities.

[0017] Figure 3 shows a wireless communication system configured in accordance with the present invention.

[0018] Figure 4 shows a ciphered data block configured in accordance with the present invention.

[0019] Figures 5A and 5B show two exemplary segmented PDUs in accordance with the present invention.

[0020] Figure 6 shows an exemplary concatenated PDU in accordance with the present invention.

[0021] Figure 7 shows an exemplary PDU generated by one-to-one mapping in accordance with the present invention.

[0022] Figure 8 is a flow diagram of a process for segmentation and re-segmentation operation between a WTRU and an eNode-B in accordance with the present invention.

[0023] DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0024] When referred to hereafter, the terminology "WTRU" includes but is not limited to a user equipment (UE), a mobile station, a fixed or mobile subscriber unit, a pager, a personal data assistant (PDA), a cellular telephone, a computer, or any other type of user device capable of operating in a wireless environment. When referred to hereafter, the terminology "eNode-B" includes but is not limited to a base station, a Node-B, a site controller, an access point (AP) or any other type of interfacing device in a wireless environment.

[0025] The features of the present invention may be incorporated into an integrated circuit (IC) or be configured in a circuit comprising a multitude of interconnecting components.

[0026] Figure 3 shows a wireless communication system 300 configured in accordance with the present invention. The system 300 includes a WTRU 310, an eNode-B 320 and an aGW 330. The WTRU 310 includes an RRC/non-access stratum (NAS) entity 312, a packet data convergence protocol (PDCP) entity 314, a cipher entity 316, an outer ARQ, (or RLC), entity 318 and a user application layer 319. The eNode-B 320 includes an outer ARQ entity 322. The aGW 330, (may also be referred to as an evolved global packet radio services (GPRS) service node (eGSN)), includes an NAS entity 332, a PDCP entity 334, a cipher entity 336 and a user application layer 338.

[0027] In accordance with the present invention, cipher entities 316 and 336 reside in the WTRU 310 and the aGW 330, respectively, and outer ARQ entities 318 and 322 reside in the WTRU 310 and the eNode-B 320, respectively. The order of ciphering operation and the outer ARQ operation is changed from the conventional system such that data block ciphering is performed before data block segmentation or concatenation by the outer ARQ entities 318 and 322. This means that the cipher entities 316 and 336 are located on top of the outer ARQ entities 318 and 322. The cipher entities 316 and 336 may be directly invoked by the RRC/NAS entity 312 and the NAS entity 332, respectively, on a control plane (C-plane) through the PDCP entities 314 and 334, or by the PDCP entities 314, 334, (under the user application layers 319, 338), on a user plane (U-plane).

[0028] The cipher entities 316, 336 perform data security functionality by encrypting and decrypting a data block, (i.e., control message from the RRC/NAS entity 312 or the NAS entity 332 through the PDCP entity 314, 334 or a user service data unit (SDU) from the PDCP entity 314, 334). The cipher entities 316, 336 use a generic SN for data encryption and decryption. The generic SN is a sequence number used for ciphering and deciphering the data block. The generic SN for each data block is preferably used together with other ciphering parameters, (such as a ciphering key, bearer-ID, etc.), to encrypt and decrypt the data block.

[0029] Figure 4 shows a ciphered data block 400 configured in accordance with the present invention. The ciphered data block 400 includes a generic SN 402 and a ciphered data portion 404. A data block is ciphered by the cipher entity 316, 336 using a generic SN 402. The generic SN 402 is left unencrypted.

[0030] The generic SN 402 may be allocated by a higher layer entity, (such as the NAS entity 312, 332 or the PDCP entity 314, 334). Alternatively, the generic SN 402 may be derived by the cipher entity 316, 336 with a seed, such as a required transmission sequence numbers known at the WTRU 310 and the aGW 330, (e.g., a PDCP SN for U-plane data, an RRC message SN or

a NAS message SN for C-plane data). The advantage of this scheme is that the generic SN 402 may be used for multiple H-ARQ and/or outer ARQ transmissions, which results in reducing signaling overhead.

[0031] The outer ARQ entity 318, 322 generates a PDU from the ciphered data block 400 and performs ARQ operation. The outer ARQ entity 318, 322 may segment the ciphered data block 400 into a number of outer ARQ PDUs. When a ciphered data block size exceeds a PDU size, the ciphered data block 400 is segmented into multiple blocks. The outer ARQ entity 318, 322 may assign an ARQ SN for each of the PDUs. The ARQ SN is a sequence number used for transmission feedback, (i.e., a positive acknowledgement (ACK) or a negative acknowledgement (NACK)), and retransmission of failed PDUs between two outer ARQ entities 318, 322.

[0032] Figures 5A and 5B show two exemplary segmented PDUs 510, 520 in accordance with the present invention. In this example, a ciphered data block is segmented into two ciphered data parts 518, 528 which are included in two PDUs 510, 520, respectively. The generic SN 516 may be included only in the first PDU 510 and the generic SN 526 may be omitted in the subsequent PDUs 520 to avoid repeated transmission of the generic SN. An SN field 515, 525 is a 1-bit indicator field in preceding the generic SN 516, 526 to indicate whether a generic SN 516, 526 is following or not. The extension field 513, 523 after the ARQ SN 512, 522 indicates whether a segment header 514, 524 is following or not. The segment header 514, 524 comprises a length indicator (LI) and a segment extension indicator (SE). The LI indicates the last position of the ciphered data part in the PDU, as shown in Figure 5B. The SE indicates whether another segment header is following or not. The segment header 514, 524 is optional and may be omitted when there is no padding, as shown in Figure 5A, or the ciphered data block has a fixed size.

[0033] Alternatively, the outer ARQ entity 318, 322 may concatenate several data blocks into one PDU. When a ciphered data block size is smaller

than a PDU size, multiple ciphered data blocks may be concatenated in one PDU.

[0034] Figure 6 shows an exemplary concatenated PDU 600 in accordance with the present invention. An optional ARQ SN 602 may be assigned by the outer ARQ entity 318, 322 to the PDU 600. The concatenated PDU 600 is generated from multiple ciphered data blocks and includes multiple segment headers 604a-604n. Each segment header 604a-604n indicates the ending position of the corresponding ciphered data blocks 608a-608n in the PDU 600. A different generic SN is used for each of the data blocks and the generic SNs 606a-606n are included in the PDU 600. The extension field 603 after the ARQ SN 602 indicates whether a segment header 604a is following or not. If the concatenation always supports in-sequence concatenated SDUs, the generic sequence number may only be included in the first concatenated SDU.

[0035] Alternatively, the outer ARQ entity 318, 322 may generate one PDU from one ciphered data block, (i.e., one-to-one mapping). When the ciphered data block size is close or same to the PDU size, the outer ARQ entity 318, 322 may generate one PDU from one data block. The one-to-one mapping may occur by coincidence or by configuration. If the one-to-one mapping is configured, the generic SN used by the cipher entity 316, 336 may include an ARQ SN, (either in higher or lower order bit positions in the generic SN). In this case, the generic SN is called a common SN. The common SN is a sequence number as a generic SN, but it embeds an ARQ SN. The common SN may be used when by configuration one data block is carried by one PDU. Since the ARQ SN is embedded in the common SN, the outer ARQ entity does not need to allocate another ARQ SN and a processing overhead is reduced.

[0036] Figure 7 shows an exemplary PDU 700 generated by one-to-one mapping. The PDU 700 includes a common SN 702 which embeds an ARQ SN 701. The segment header 704 indicates the last position of the ciphered data block 706. The data block size may be fixed, (by configuration), or may be flexible. The segment header 704 may be omitted if padding is zero or the size

of the data block is fixed. An FX field 703 is a 1-bit indicator field following the common SN 702, indicating whether a segment header 704 is following or not.

[0037] A receiving side outer ARQ entity checks the ARQ SN for ACK or NACK. The transmission status feedback flows between the WTRU 310 and the eNode-B 320 to ensure the guaranteed data service at the shortest possible time. All correctly received PDUs are then passed to a reassembly process to form the original ciphered data block, each associated with a unique ciphering sequence number. The generic SN, (or common SN), is used for data deciphering by the cipher entity 314, 334.

[0038] Figure 8 is a flow diagram of a process 800 for segmentation and re-segmentation operation between a WTRU 310 and an eNode-B 320 of the wireless communication system 300 of Figure 3 in accordance with the present invention. The WTRU 310 and the eNode-B 320 implement an H-ARQ for transmission of a PDU. At a transmitting node, (either the WTRU 310 or the eNode-B 320), an outer ARQ entity 318, 322 generates at least one PDU from at least one ciphered data block and transmits the PDU(s) to a receiving node (step 802). The PDU(s) may be generated by segmenting one data block, by concatenating multiple data blocks, or may be generated from one data block by one-to-one mapping. The receiving node checks whether the PDU is successfully received and sends an ACK or a NACK to the transmitting node (step 804).

[0039] Upon receiving feedback indicating H-ARQ transmission failure, (including H-ARQ retransmissions), of one or more segments, the transmitting node may resend the data block. The data block may be retransmitted as long as retransmission criteria is met, (i.e., maximum delay or latency, or maximum number of retransmissions is not exceeded). The assigned physical resources, channel quality and/or available transmission power may result in a different allowable transport format combination (TFC) subset requiring different segment sizes for retransmitting the data block.

[0040] In resending the data block, the transmitting node has three options. The outer ARQ entity 318, 322 may segment or re-segment the data block or PDU for retransmission and increments a segmentation version identifier for this data block identified by the generic SN (step 806). If the data block was not segmented previously, (i.e., the data block was generated by one-to-one mapping), the outer ARQ entity 318, 322 may segment the data block for retransmission. If the data block was segmented previously, the outer ARQ entity 318, 322 may re-segment the data block or PDU to different segment sizes and potentially different number of segments. Upon reception of a new segmentation version identifier, in the case of data block re-segmentation, the receiving node discards previously received segments of the data block or PDU with an old segmentation version identifier(s) (step 812). Optionally, in the case of data block re-segmentation, upon performing re-segmentation and setting a new segmentation version identifier, the transmitting node may terminate H-ARQ process for the old segments.

[0041] Alternatively, the outer ARQ entity 318, 322 of the transmitting node may choose not to re-segment the data block, but retransmit only the H-ARQ failed segment(s) of the previous transmission (step 808). In this case, the segmentation version identifier is not incremented so that the receiving node does not discard successfully received segments of the previous transmission of the data block or PDU.

[0042] If the previously transmitted PDU is generated by concatenating multiple data blocks, depending on assigned physical resources, channel quality, and/or available transmission power, the transmitting node may separate the previous PDU into multiple sub-PDUs, each including one or more data blocks without segmenting the data blocks (step 810). Since the data blocks are not segmented and the receiving node can unambiguously determine lost and duplicate data block from the generic SN, it is not necessary to coordinate transmissions between the transmitting node and the receiving node with a segmentation version identifier.

[0043] Embodiments.

[0044] 1. A wireless communication system for implementing data security and ARQ.

[0045] 2. The system of embodiment 1 comprising a WTRU, a Node-B and an aGW.

[0046] 3. The system of embodiment 2 wherein the WTRU comprises a first cipher entity for ciphering an uplink data block for transmission and deciphering a downlink data block ciphered by an aGW.

[0047] 4. The system of embodiment 3 wherein the WTRU comprises a first outer ARQ entity for performing ARQ operation for transmission of the uplink data block ciphered by the first cipher entity, and the reception of the downlink data block between the WTRU and the Node-B.

[0048] 5. The system as in any of the embodiments 2-4, wherein the Node-B comprises a second outer ARQ entity for performing ARQ operation for reception of an uplink data block and transmission of a downlink data block between the WTRU and the Node-B.

[0049] 6. The system as in any of the embodiments 2-5, wherein the aGW comprises a second cipher entity for ciphering the downlink data block for transmission to the WTRU and deciphering the uplink data block ciphered by the first cipher entity.

[0050] 7. The system of embodiment 6, wherein the first cipher entity and the second cipher entity use a generic SN to cipher and decipher the uplink data block and the downlink data block.

[0051] 8. The system as in any of the embodiments 6-7, wherein the first cipher entity and the second cipher entity derive the generic SN from a seed.

[0052] 9. The system of embodiment 8, wherein the seed is a required transmission sequence number known at the aGW and the WTRU.

[0053] 10. The system of embodiment 9, wherein the required transmission sequence number is one of a PDCP SN and a higher layer message SN.

[0054] 11. The system as in any of the embodiments 7-10, wherein the generic SN is assigned by a higher layer entity.

[0055] 12. The system of embodiment 11, wherein the higher layer entity is one of an RRC entity, an NAS entity and a PDCP entity.

[0056] 13. The system as in any of the embodiments 5-12, wherein the first outer ARQ entity and the second outer ARQ entity segment one data block to multiple PDUs.

[0057] 14. The system of embodiment 13, wherein the first outer ARQ entity and the second outer ARQ entity assign an ARQ SN to each of the PDUs.

[0058] 15. The system of embodiment 13, wherein the first outer ARQ entity and the second outer ARQ entity attach the generic SN only to a first PDU.

[0059] 16. The system as in any of the embodiments 13-15, wherein the first outer ARQ entity and the second outer ARQ entity attach a segment header to each of the PDUs.

[0060] 17. The system as in any of the embodiments 13-15, wherein the first outer ARQ entity and the second outer ARQ entity attach a segment header only to a PDU which includes padding.

[0061] 18. The system as in any of the embodiments 13-17, wherein the first outer ARQ entity and the second outer ARQ entity are configured to segment one of the data block and the PDUs to multiple sub-level PDUs in smaller size than previous PDUs when transmission failure of at least one the previous PDUs occurs and increase a segmentation version identifier.

[0062] 19. The system of embodiment 18, wherein an H-ARQ process for the previous PDUs is terminated.

[0063] 20. The system as in any of the embodiments 18-19, wherein the first outer ARQ entity and the second outer ARQ entity are configured to resend only a failed PDU.

[0064] 21. The system as in any of the embodiments 5-12, wherein the first outer ARQ entity and the second outer ARQ entity concatenate multiple data blocks to one PDU.

[0065] 22. The system of embodiment 21, wherein the first outer ARQ entity and the second outer ARQ entity attach a segment header to the PDU.

[0066] 23. The system as in any of the embodiments 21-22, wherein the first outer ARQ entity and the second outer ARQ entity attach a segment header only if the PDU includes padding.

[0067] 24. The system as in any of the embodiments 21-23, wherein the first outer ARQ entity and the second outer ARQ entity are configured to separate the PDU to multiple sub-PDUs when transmission failure of the PDU occurs, each sub-PDU including at least one data block.

[0068] 25. The system as in any of the embodiments 5-12, wherein the first outer ARQ entity and the second outer ARQ entity generate one PDU from one data block.

[0069] 26. The system of embodiment 25, wherein an ARQ SN is embedded in the generic SN.

[0070] 27. The system as in any of the embodiments 25-26, wherein the first outer ARQ entity and the second outer ARQ entity generate one PDU from one data block by configuration.

[0071] 28. The system as in any of the embodiments 25-27, wherein a size of the uplink data block and the downlink data block is fixed.

[0072] 29. The system as in any of the embodiments 25-27, wherein a size of the uplink data block and the downlink data block is flexible.

[0073] 30. The system as in any of the embodiments 25-28, wherein the first outer ARQ entity and the second outer ARQ entity are configured to segment one of the data block and the PDU to multiple sub-level PDUs when transmission failure of the PDU occurs and increase a segmentation version identifier.

[0074] 31. The system of embodiment 30, wherein an H-ARQ process for the previous PDU is terminated.

[0075] 32. A method for implementing data security and ARQ in a wireless communication system including a WTRU, a Node-B and an aGW.

[0076] 33. The method of embodiment 32 comprising the step of ciphering a data block.

[0077] 34. The method of embodiment 33 comprising the step of generating at least one PDU from the ciphered data block.

[0078] 35. The method of embodiment 34 comprising the step of assigning an ARQ SN to the PDU.

[0079] 36. The method as in any of the embodiments 34-35, comprising the step of transmitting the PDU.

[0080] 37. The method as in any of the embodiments 33-36, further comprising the step of assigning a generic SN to the data block, the data block being ciphered by using the generic SN.

[0081] 38. The method of embodiment 37, wherein the generic SN is derived from a seed.

[0082] 39. The method of embodiment 38, wherein the seed is a required transmission sequence number known at the aGW and the WTRU.

[0083] 40. The method of embodiment 39, wherein the required transmission sequence number is one of a PDCP sequence number, an RRC message sequence number and an NAS message sequence number.

[0084] 41. The method of embodiment 37, wherein the generic SN is assigned by a higher layer entity.

[0085] 42. The method as in any of the embodiments 34-41, wherein one ciphered data block is segmented to multiple PDUs.

[0086] 43. The method as in any of the embodiments 37-42, wherein the generic SN is attached only to a first PDU.

[0087] 44. The method as in any of the embodiments 34-43, wherein a segment header is attached to each of the PDUs.

[0088] 45. The method as in any of the embodiments 34-43, wherein a segment header is attached only to a PDU which includes padding.

[0089] 46. The method as in any of the embodiments 34-45, further comprising the step of re-segmenting one of the ciphered data block and the PDUs to multiple sub-level PDUs in smaller size than previous PDUs when transmission of at least one previous PDU fails.

[0090] 47. The method of embodiment 46, comprising the step of incrementing a segmentation version identifier.

[0091] 48. The method as in any of the embodiments 46-47, comprising the step of retransmitting the multiple PDUs.

[0092] 49. The method as in any of the embodiments 46-48, further comprising the step of terminating an H-ARQ process for the previous PDUs.

[0093] 50. The method as in any of the embodiments 46-49, further comprising the step of retransmitting a failed PDU when transmission of at least one previous PDU fails.

[0094] 51. The method as in any of the embodiments 34-45, wherein multiple ciphered data blocks are concatenated to one PDU.

[0095] 52. The method of embodiment 51, wherein a segment header is attached to the PDU.

[0096] 53. The method of embodiment 52, wherein a segment header is attached only if the PDU includes padding.

[0097] 54. The method as in any of the embodiments 51-53, further comprising the step of separating the PDU to multiple sub-PDUs when transmission of the PDU fails, each sub-PDU including at least one data block.

[0098] 55. The method of embodiment 54 further comprising the step of retransmitting the sub-PDUs.

[0099] 56. The method as in any of the embodiments 34-45, wherein one PDU is generated from one ciphered data block.

[00100] 57. The method of embodiment 56, wherein an ARQ SN is embedded in the generic SN.

[00101] 58. The method as in any of the embodiments 56-57, wherein a size of the data block is fixed.

[00102] 59. The method as in any of the embodiments 56-57, wherein a size of the data block is flexible.

[00103] 60. The method as in any of the embodiments 56-59, further comprising the step of segmenting one of the ciphered data block and the PDU to multiple sub-level PDUs when transmission of the PDU fails.

[00104] 61. The method of embodiment 60, comprising the step of incrementing a segmentation version identifier.

[00105] 62. The method as in any of the embodiments 60-61, further comprising the step of retransmitting the multiple PDUs.

[00106] 63. The method as in any of the embodiments 56-62, further comprising the step of terminating an H-ARQ process for the previous PDU.

[00107] 64. A WTRU for implementing data security and ARQ in a wireless communication system including a Node-B and an aGW.

[00108] 65. The WTRU of embodiment 64 comprising a cipher entity for ciphering an uplink data block for transmission and deciphering a downlink data block ciphered by the aGW.

[00109] 66. The WTRU of embodiment 65 comprising an outer ARQ entity for performing ARQ operation for transmission of the ciphered uplink data block and reception of the downlink data block between the WTRU and the Node-B.

[00110] 67. The WTRU as in any of the embodiments 65-66, wherein the cipher entity uses a generic SN to cipher the uplink data block.

[00111] 68. The WTRU of embodiment 67, wherein the cipher entity derives the generic SN from a seed.

[00112] 69. The WTRU of embodiment 68, wherein the seed is a required transmission sequence number known at the aGW and the WTRU.

[00113] 70. The WTRU of embodiment 69, wherein the required transmission sequence number is one of a PDCP SN, an RRC message SN and an NAS message SN.

[00114] 71. The WTRU of embodiment 67, wherein the generic SN is assigned by a higher layer entity.

[00115] 72. The WTRU of embodiment 71, wherein the higher layer entity is one of an RRC entity, an NAS entity, and a PDCP entity.

[00116] 73. The WTRU as in any of the embodiments 66-72, wherein the outer ARQ entity segments the uplink data block to multiple PDUs.

[00117] 74. The WTRU of embodiment 73, wherein the outer ARQ entity assigns an ARQ SN to each of the PDUs.

[00118] 75. The WTRU as in any of the embodiments 67-74, wherein the outer ARQ entity attaches the generic SN only to a first PDU.

[00119] 76. The WTRU as in any of the embodiments 73-75, wherein the outer ARQ entity attaches a segment header to each of the PDUs.

[00120] 77. The WTRU as in any of the embodiments 73-75, wherein the outer ARQ entity attaches a segment header only to a PDU which includes padding.

[00121] 78. The WTRU as in any of the embodiments 73-77, wherein the outer ARQ entity is configured to segment one of the uplink data block and the PDUs to multiple sub-level PDUs in smaller size than previous PDUs when transmission of at least one previous PDU fails, and configured to increase a segmentation version identifier.

[00122] 79. The WTRU as in any of the embodiments 73-78, wherein an H-ARQ process for the previous PDUs is terminated.

[00123] 80. The WTRU as in any of the embodiments 78-79, wherein the outer ARQ entity is configured to resend only a failed PDU.

[00124] 81. The WTRU as in any of the embodiments 66-72, wherein the outer ARQ entity concatenates multiple ciphered uplink data blocks to one PDU.

[00125] 82. The WTRU of embodiment 81, wherein the outer ARQ entity attaches a segment header to the PDU.

[00126] 83. The WTRU as in any of the embodiments 81-82, wherein the outer ARQ entity attaches a segment header only if the PDU includes padding.

[00127] 84. The WTRU as in any of the embodiments 81-83, wherein the outer ARQ entity is configured to separate the PDU to multiple sub-PDUs when transmission of the PDU fails, each sub-PDU including at least one ciphered uplink data block.

[00128] 85. The WTRU as in any of the embodiments 66-72, wherein the outer ARQ entity generates one PDU from one ciphered uplink data block.

[00129] 86. The WTRU of embodiment 85, wherein an ARQ SN is embedded in the generic SN.

[00130] 87. The WTRU as in any of the embodiments 85-86, wherein a size of the uplink data block is fixed.

[00131] 88. The WTRU as in any of the embodiments 85-86, wherein a size of the uplink data block is flexible.

[00132] 89. The WTRU as in any of the embodiments 85-88, wherein the outer ARQ entity is configured to segment one of the ciphered uplink data block and the PDU to multiple sub-level PDUs when transmission of the PDU fails, and increase a segmentation version identifier.

[00133] 90. The WTRU as in any of the embodiments 85-89, wherein an H-ARQ process for the previous PDU is terminated.

[00134] 91. A PDU for implementing data security and ARQ.

[00135] 92. The PDU of embodiment 91 comprising an ARQ SN for identifying a segment of a data block.

[00136] 93. The PDU of embodiment 92 comprising an extension for indicating whether a segment header is following.

[00137] 94. The PDU as in any of the embodiments 92-93, a generic SN used for ciphering the data block.

[00138] 95. The PDU of embodiment 94, comprising at least one data portion ciphered by using the generic SN.

[00139] 96. The PDU as in any of the embodiments 92-95, further comprising at least one segment header, the segment header including a length indicator for indicating an end point of corresponding data portion and

a segment extension for indicating whether another segment header is following.

[00140] 97. The PDU as in any of the embodiments 92-96, further comprising padding.

[00141] 98. The PDU as in any of the embodiments 92-97, wherein the ARQ SN is embedded in the generic SN.

[00142] Although the features and elements of the present invention are described in the preferred embodiments in particular combinations, each feature or element can be used alone without the other features and elements of the preferred embodiments or in various combinations with or without other features and elements of the present invention. The methods or flow charts provided in the present invention may be implemented in a computer program, software, or firmware tangibly embodied in a computer-readable storage medium for execution by a general purpose computer or a processor. Examples of computer-readable storage mediums include a read only memory (ROM), a random access memory (RAM), a register, cache memory, semiconductor memory devices, magnetic media such as internal hard disks and removable disks, magneto-optical media, and optical media such as CD-ROM disks, and digital versatile disks (DVDs).

[00143] Suitable processors include, by way of example, a general purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs) circuits, any other type of integrated circuit (IC), and/or a state machine.

[00144] A processor in association with software may be used to implement a radio frequency transceiver for use in a wireless transmit receive unit (WTRU), user equipment (UE), terminal, base station, radio network controller (RNC), or any host computer. The WTRU may be used in conjunction with modules, implemented in hardware and/or software, such as

a camera, a video camera module, a videophone, a speakerphone, a vibration device, a speaker, a microphone, a television transceiver, a hands free headset, a keyboard, a Bluetooth® module, a frequency modulated (FM) radio unit, a liquid crystal display (LCD) display unit, an organic light-emitting diode (OLED) display unit, a digital music player, a media player, a video game player module, an Internet browser, and/or any wireless local area network (WLAN) module.

Claims

1. A method, implemented by a wireless transmit/receive unit (WTRU) for implementing data security and automatic repeat request (ARQ), the method comprising:

assigning a generic sequence number (SN) to a data block in a layer above a radio link control (RLC) layer;

ciphering the data block using the SN in the layer above the RLC layer;

generating at least one protocol data unit (PDU) from the ciphered data block, wherein the generating the at least one PDU includes at least one of segmenting or concatenating the ciphered data block;

assigning an ARQ SN to the at least one PDU;

transmitting the at least one PDU to an evolved Node B (eNB); and

transmitting ARQ retransmissions of the at least one PDU to an eNB.

2. The method of claim 1 wherein the generic SN is derived from a seed.

3. The method of claim 2 wherein the seed is a required transmission sequence number known at the WTRU.

4. The method of claim 3 wherein the required transmission sequence number is one of a packet data convergence protocol (PDCP) sequence number, a radio resource control (RRC) message sequence number and a non-access stratum (NAS) message sequence number.

5. The method of claim 1 wherein the generic SN is assigned by a higher layer entity.

6. The method of claim 1 wherein the ciphered data block is segmented into multiple PDUs.

7. The method of claim 6 wherein the generic SN is attached only to a first PDU.

8. The method of claim 6 wherein a segment header is attached to each of the PDUs.

9. The method of claim 6 wherein a segment header is attached only to a PDU which includes padding.

10. The method of claim 6 further comprising:

re-segmenting one of the ciphered data block or the PDUs to multiple sub-level PDUs in smaller size than previous PDUs when transmission of at least one previous PDU fails;

incrementing a segmentation version identifier; and

retransmitting the multiple PDUs.

11. The method of claim 10 further comprising:

terminating a hybrid automatic repeat request (H-ARQ) process for the previous PDUs.

12. The method of claim 6 further comprising:

retransmitting a failed PDU when transmission of at least one previous PDU fails.

13. The method of claim 1 wherein multiple ciphered data blocks are concatenated to one PDU.

14. The method of claim 13 wherein a segment header is attached to the PDU.

15. The method of claim 13 wherein a segment header is attached only if the PDU includes padding.

16. The method of claim 13 further comprising:

separating the PDU to multiple sub-PDUs when transmission of the PDU fails, each sub-PDU including at least one data block; and

retransmitting the sub-PDUs.

17. The method of claim 1 wherein one PDU is generated from one ciphered data block.

18. The method of claim 17 wherein an ARQ SN is embedded in the generic SN.

19. The method of claim 17 wherein a size of the data block is fixed.

20. The method of claim 17 wherein a size of the data block is flexible.

21. The method of claim 17 further comprising:

segmenting one of the ciphered data block or the PDU to multiple sub-level PDUs when transmission of the PDU fails;

incrementing a segmentation version identifier; and

retransmitting the multiple PDUs.

22. The method of claim 21 further comprising:

terminating a hybrid automatic repeat request (H-ARQ) process for the previous PDU.

23. A wireless transmit/receive unit (WTRU) for implementing data security and automatic repeat request (ARQ), the WTRU comprising:

a cipher entity configured to assign a generic sequence number (SN) to a data block in a layer above a radio link control (RLC) layer;

the cipher entity configured to cipher an uplink data block for transmission and decipher a ciphered downlink data block using the generic SN in the layer above the RLC layer; and

an automatic repeat request (ARQ) entity configured to perform an ARQ operation for transmission of the ciphered uplink data block and reception of the downlink data block, wherein ARQ retransmissions of the uplink data block use the ARQ SN.

24. The WTRU of claim 23 wherein the cipher entity derives the generic SN from a seed.

25. The WTRU of claim 24 wherein the seed is a required transmission sequence number known at the WTRU.

26. The WTRU of claim 25 wherein the required transmission sequence number is one of a packet data convergence protocol (PDCP) sequence number, a radio resource control (RRC) message sequence number and a non-access stratum (NAS) message sequence number.

27. The WTRU of claim 23 wherein the generic SN is assigned by a higher layer entity.

28. The WTRU of claim 27 wherein the higher layer entity is one of a radio resource control (RRC) entity, a non access stratum (NAS) entity, and a packet data convergence protocol (PDCP) entity.

29. The WTRU of claim 23 wherein the ARQ entity segments the uplink data block to multiple protocol data units (PDUs).

30. The WTRU of claim 29 wherein the ARQ entity assigns an ARQ SN to each of the PDUs.

31. The WTRU of claim 29 wherein the ARQ entity attaches the generic SN only to a first PDU.

32. The WTRU of claim 29 wherein the ARQ entity attaches a segment header to each of the PDUs.

33. The WTRU of claim 29 wherein the ARQ entity attaches a segment header only to a PDU which includes padding.

34. The WTRU of claim 29 wherein the ARQ entity is configured to segment one of the uplink data block and the PDUs to multiple sub-level PDUs in smaller size than previous PDUs when transmission of at least one previous PDU fails, and configured to increase a segmentation version identifier.

35. The WTRU of claim 34 wherein a hybrid automatic repeat request (H-ARQ) process for the previous PDUs is terminated.

36. The WTRU of claim 29 wherein the ARQ entity is configured to resend only a failed PDU.

37. The WTRU of claim 23 wherein the ARQ entity concatenates multiple ciphered uplink data blocks into one protocol data unit (PDU).

38. The WTRU of claim 37 wherein the ARQ entity attaches a segment header to the PDU.

39. The WTRU of claim 37 wherein the ARQ entity attaches a segment header only if the PDU includes padding.

40. The WTRU of claim 37 wherein the ARQ entity is configured to separate the PDU to multiple sub-PDUs when transmission of the PDU fails, each sub-PDU including at least one ciphered uplink data block.

41. The WTRU of claim 23 wherein the ARQ entity generates one protocol data unit (PDU) from one ciphered uplink data block.

42. The WTRU of claim 41 wherein an ARQ SN is embedded in the generic SN.

43. The WTRU of claim 42 wherein a size of the uplink data block is fixed.

44. The WTRU of claim 42 wherein a size of the uplink data block is flexible.

45. The WTRU of claim 41 wherein the ARQ entity is configured to segment one of the ciphered uplink data block or the PDU to multiple sub-level PDUs when transmission of the PDU fails, and increase a segmentation version identifier.

46. The WTRU of claim 45 wherein a hybrid automatic repeat request (H-ARQ) process for the previous PDU is terminated.