(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0026311**

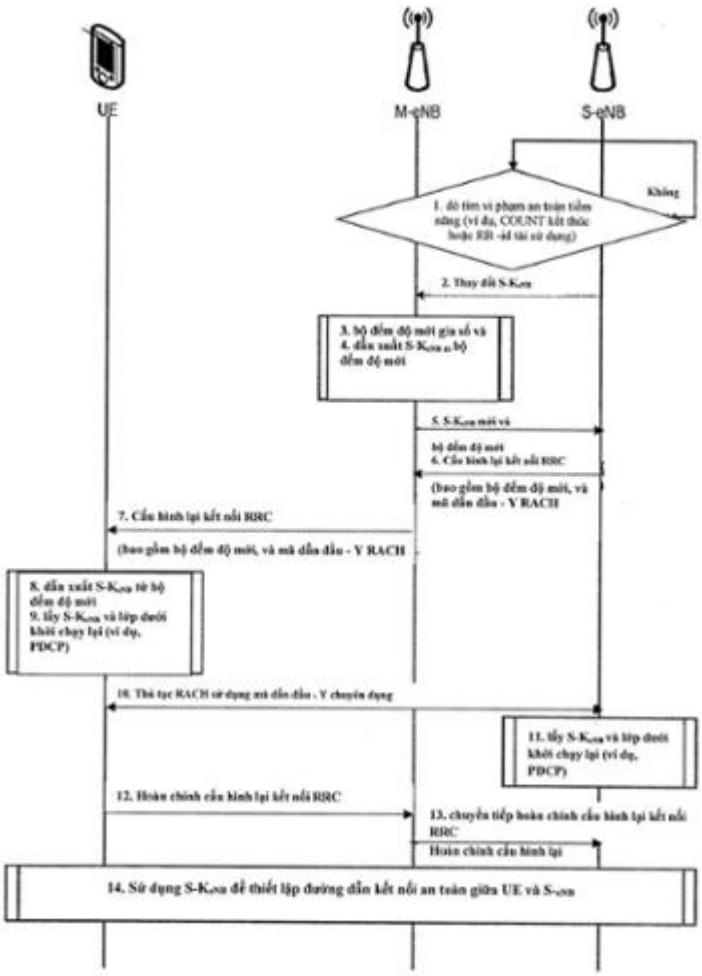
(51)[7] **H04W 12/04**; H04L 29/06

(13) **B**

(21) 1-2016-03506
(22) 03/03/2015
(86) PCT/EP2015/054400 03/03/2015
(87) WO/2015/139947 24/09/2015
(30) 14001067.9 21/03/2014 EP
(45) 25/11/2020 392
(43) 26/12/2016 345A
(73) SUN PATENT TRUST (US)
450 Lexington Avenue, 38th Floor New York, NY 10017 (US)
(72) BASU MALLICK, Prateek (DE); LOEHR, Joachim (DE).
(74) Công ty Cổ phần Hỗ trợ phát triển công nghệ Detech (DETECH)

(54) THIẾT BỊ TRẠM CƠ SỞ THỨ CẤP VÀ PHƯƠNG PHÁP TRUYỀN THÔNG

(57) Sáng chế đề cập đến phương pháp thiết lập liên kết truyền thông an toàn giữa trạm di động và trạm cơ sở thứ cấp trong hệ thống truyền thông di động. Sáng chế cũng đề xuất hệ thống truyền thông di động để thực hiện các phương pháp này, và phương tiện lưu trữ đọc được bởi máy tính mà khi máy tính đọc các chỉ dẫn được lưu trong phương tiện nói trên làm cho hệ thống truyền thông di động thực hiện phương pháp được mô tả ở đây. Cụ thể là, sáng chế đề xuất đáp lại sự vi phạm tiềm năng an toàn được báo hiệu hoặc được phát hiện, trạm cơ sở chính gia số bộ đếm độ mới để khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp; và trạm di động và trạm cơ sở thứ cấp khởi chạy lại truyền thông giữa chúng. Việc khởi chạy lại được thực hiện dưới sự điều khiển của trạm cơ sở chính và; còn bao gồm dẫn xuất khóa mật an toàn tương tự dựa trên bộ đếm độ mới được gia số này, và thiết lập liên kết truyền thông an toàn bằng cách sử dụng khóa mật an toàn tương tự, được dẫn xuất.


UE
M-eNB
S-eNB
1. đã tìm vi phạm an toàn tiềm năng (ví dụ, COUNT kết thúc hoặc RB -id tái sử dụng)
Không
2. Thay đổi S-K$_{eNB}$
3. bộ đếm độ mới gia số và
4. dẫn xuất S-K$_{eNB}$ từ bộ đếm độ mới
5. S-K$_{eNB}$ mới và
bộ đếm độ mới
6. Cấu hình lại kết nối RRC
(bao gồm bộ đếm độ mới, và mã dẫn đầu - Y RACH
7. Cấu hình lại kết nối RRC
(bao gồm bộ đếm độ mới, và mã dẫn đầu - Y RACH
8. dẫn xuất S-K$_{eNB}$ từ bộ đếm độ mới
9. lấy S-K$_{eNB}$ và lớp dưới khởi chạy lại (ví dụ, PDCP)
10. Thủ tục RACH sử dụng mã dẫn đầu - Y chuyên dụng
11. lấy S-K$_{eNB}$ và lớp dưới khởi chạy lại (ví dụ, PDCP)
12. Hoàn chỉnh cấu hình lại kết nối RRC
13. chuyển tiếp hoàn chỉnh cấu hình lại kết nối RRC
Hoàn chỉnh cấu hình lại
14. Sử dụng S-K$_{eNB}$ để thiết lập đường dẫn kết nối an toàn giữa UE và S-$_{eNB}$

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến phương pháp thiết lập liên kết truyền thông an toàn giữa trạm di động và trạm cơ sở thứ cấp trong hệ thống truyền thông di động bao gồm trạm di động, trạm cơ sở chính và thứ cấp. Sáng chế cũng đề xuất trạm di động và trạm cơ sở để tham gia và thực hiện các phương pháp được mô tả trong bản mô tả sáng chế này.

Tình trạng kỹ thuật của sáng chế

Phát triển dài hạn (LTE)

Các hệ thống di động thế hệ thứ ba (3G) dựa trên công nghệ truy nhập radio WCDMA đang được triển khai trên quy mô rộng trên toàn thế giới. Bước đầu tiên trong việc tăng cường hay phát triển công nghệ này yêu cầu đưa vào truy nhập gói đường nối xuống tốc độ cao (HSDPA - High-Speed Downlink Packet Access) và đường nối lên tăng cường, còn được gọi là truy cập gói đường nối lên tốc độ cao (HSUPA - High Speed Uplink Packet Access), đem lại một công nghệ truy nhập radio có tính tương thích cao.

Để chuẩn bị cho các nhu cầu người dùng tăng lên và để tương thích với các công nghệ truy nhập radio mới, 3GPP đưa vào một hệ thống truyền thông di động mới được gọi là hệ thống phát triển dài dạn (LTE - Long Term Evolution). LTE được thiết kế để đáp ứng các yêu cầu sóng mang đối với dữ liệu tốc độ cao và lưu lượng phương tiện cũng như sự hỗ trợ thoại dung lượng cao cho thập kỷ tới. Khả năng cung cấp tốc độ bit cao là biện pháp then chốt đối với LTE.

Văn bản xác định danh mục công việc (WI - work item) về phát triển dài hạn (LTE) liên quan đến truy nhập radio mặt đất UMTS cải tiến (UTRA -

Evolved UMTS Terrestrial Radio Access) và mạng truy nhập radio mặt đất UMTS (UTRAN - UMTS Terrestrial Radio Access Network) hiện là phiên bản 8 (LTE Rel.8). Hệ thống LTE tiêu biểu cho sự truy nhập radio dựa trên gói có hiệu quả và các mạng truy nhập radio, hệ thống này cung cấp đầy đủ các chức năng dựa trên IP độ trễ thấp và phí tổn thấp. Trong LTE, các dải thông đa truyền dẫn khả biến tỷ lệ được chỉ định là 1,4, 3,0, 5,0, 10,0, 15,0, và 20,0 MHz, để đạt được sự triển khai hệ thống một cách linh hoạt sử dụng một phổ cho trước. Trong đường nối xuống, sự truy nhập radio dựa trên dồn kênh phân tần trực giao (OFDM - Orthogonal Frequency Division Multiplexing) được sử dụng bởi tính miễn nhiễm vốn có với nhiễu đa đường (MPI - multipath interference) do tốc độ ký hiệu thấp, sự sử dụng tiền tố vòng (CP - cyclic prefix), và tính hấp dẫn của nó với các bố trí dải tần truyền khác nhau. Truy nhập radio dựa trên đa truy nhập phân tần đơn sóng mang (SC-FDMA - Single- carrier frequency division multiple access) đã được sử dụng trong đường nối lên, bởi sự cung cấp vùng phủ sóng diện tích rộng được ưu tiên hơn việc cải thiện tốc độ dữ liệu đỉnh khi xét đến công suất truyền hạn chế của thiết bị người dùng (UE - thiết bị người dùng). Nhiều công nghệ truy nhập radio gói quan trọng được sử dụng bao gồm các công nghệ truyền dẫn kênh đa đầu vào đa đầu ra (MIMO - multiple-input multiple-output), và kết cấu báo hiệu điều khiển có hiệu quả cao đạt được trong LTE Rel. 8/9 (phiên bản 8).

Cấu tạo LTE

Cấu tạo tổng thể được thể hiện trên Fig.1 và sự thể hiện chi tiết hơn được đưa ra trên Fig.2. E-UTRAN bao gồm eNodeB, cung cấp các điểm đầu cuối giao thức mặt phẳng người dùng E-UTRA (PDCP/RIC/MAC/PHY) và mặt phẳng điều khiển (RRC) cho thiết bị người dùng (UE). eNodeB (eNB) làm chủ các lớp vật lý (PHY - Physical), điều khiển truy nhập phương tiện (MAC - Medium Access Control), điều khiển liên kết radio (RIC - Radio Link Control), và giao thức điều khiển dữ liệu gói (PDCP - Packet Data

Control Protocol), các lớp này bao gồm chức năng nén phần đầu mặt phẳng người dùng và mã hóa. Nó còn đưa ra chức năng điều khiển tài nguyên radio (RRC - Radio Resource Control) tương ứng với mặt phẳng điều khiển. Nó thực hiện nhiều chức năng bao gồm quản lý tài nguyên radio, điều khiển cho phép, lập lịch, bắt buộc chất lượng dịch vụ đường nối lên thương lượng (QoS - Quality of Service), quảng bá thông tin ô, mã hóa/giải mã dữ liệu mặt phẳng người dùng và điều khiển, và nén/giải nén các phần đầu gói mặt phẳng người dùng đường nối xuống/đường nối lên. Các eNodeB được liên thông với nhau bằng giao diện X2.

Các eNodeB còn được nối kết bằng giao diện SI đến EPC (Evolved Packet Core - Lõi gói cải tiến), cụ thể hơn đến MME (Mobility Management Entity - Thực thể quản lý di động) bằng SI -MME và đến cổng nối dịch vụ (SGW - Serving Gateway) bằng SI -U. Giao diện SI hỗ trợ quan hệ nhiều-nhiều giữa các MME/các cổng nối dịch vụ và các eNodeB. SGW định tuyến và chuyển tiếp các gói dữ liệu người dùng, trong khi cũng đóng vai trò như neo di động đối với mặt phẳng người dùng trong thời gian các chuyển vùng liên eNodeB và như neo để di động giữa LTE và các công nghệ 3GPP khác (việc chuyển tiếp đầu cuối giao diện S4 và chuyển giao nghiệp vụ các hệ thống 2G/3G và PDN GW). Đối với các thiết bị người dùng ở trạng thái nghỉ, SGW tiếp nối đường truyền dữ liệu đường nối xuống và xúc phát tin nhắn khi dữ liệu đường nối xuống đến cho thiết bị người dùng. Nó quản lý và lưu trữ thiết bị người dùng, ví dụ các tham số của dịch vụ mang chuyển IP, thông tin định tuyến nội mạng. Nó còn thực hiện sao chép luồng thông tin người dùng trong trường hợp chặn hợp pháp.

MME là nút điều khiển chính đối với mạng truy nhập LTE. Nó chịu trách nhiệm theo dõi thiết bị người dùng ở chế độ nghỉ và thủ tục nhắn tin bao gồm sự truyền lại. Nó tham gia vào quy trình kích hoạt/khử kích hoạt mang chuyển và còn chịu trách nhiệm chọn SGW cho thiết bị người dùng ở gắn kết ban đầu và tại thời điểm chuyển vùng nội LTE bao gồm sự tái định vị

nút mạng lõi (CN - Core Network). Nó chịu trách nhiệm xác thực người dùng (bằng cách tương tác với HSS). Báo hiệu tầng không truy nhập (NAS - Non-Access Stratum) tiếp nối tại MME và nó còn chịu trách nhiệm sinh ra và cấp phát các danh tính tạm thời đến các thiết bị người dùng. Nó kiểm tra sự ủy quyền của thiết bị người dùng được lưu tạm thời trên mạng di động mặt đất công cộng của nhà cung cấp dịch vụ (PLMN - Public Land Mobile Network) và buộc thiết bị người dùng tuân theo các hạn chế chuyển vùng. MME là điểm tiếp nối trong mạng để bảo vệ mã hóa/tính toàn vẹn đối với báo hiệu NAS và điều khiển quản lý khóa an toàn. Chặn hợp pháp báo hiệu cũng được hỗ trợ bởi MME. MME còn cung cấp chức năng mặt phẳng điều khiển để di động giữa các mạng truy nhập LTE và 2G/3G với giao diện S3 tiếp nối tại MME từ SGSN. MME còn tiếp nối giao diện S6a đối với HSS gốc để chuyển vùng các thiết bị người dùng.

Kết cấu sóng mang thành phần trong LTE

Sóng mang thành phần đường nối xuống của hệ thống 3GPP LTE được chia nhỏ trong miền tần số thời gian được gọi là khung con. Trong 3GPP LTE mỗi khung con được chia thành hai khe đường nối xuống như được thể hiện trong Fig. 3, trong đó khe đường nối xuống thứ nhất bao gồm vùng kênh điều khiển (vùng PDCCH) trong phạm vi ký hiệu OFDM thứ nhất. Mỗi khung con bao gồm số ký hiệu OFDM đã cho trong miền thời gian (12 hoặc 14 ký hiệu OFDM trong 3GPP LTE (Phiên bản 8)), trong đó mỗi ký hiệu OFDM kéo dài trên toàn bộ dải thông của sóng mang thành phần. Do đó, mỗi ký hiệu OFDM bao gồm số ký hiệu điều biến được truyền trên sóng mang con NRB X NS™ tương ứng như cũng được thể hiện trong Fig.4.

Giả định rằng hệ thống truyền thông đa sóng mang, ví dụ, sử dụng OFDM, ví dụ như được sử dụng trong phát triển dài hạn 3 GPP (LTE), đơn vị nhỏ nhất của tài nguyên có thể được gán bởi bộ lập lịch là một "khối tài nguyên". Khối tài nguyên vật lý (PRB) được định nghĩa là N_{symb}^{DL} ký hiệu

OFDM liên tiếp trong miền thời gian (ví dụ, 7 ký hiệu OFDM) và N_{sc}^{RB} sóng mang con liên tiếp trong miền tần số như được minh họa trong Fig. 4 (ví dụ, 12 sóng mang con cho một sóng mang thành phần). Trong 3GPP LTE (Phiên bản 8), khối tài nguyên vật lý như vậy bao gồm N_{symb}^{DL} x N_{sc}^{RB} phần tử tài nguyên, tương ứng với một khe trong miền thời gian và 180 kHz trong miền tần số (nội dung chi tiết hơn về lưới tài nguyên đường nối xuống, ví dụ xem 3GPP TS 36.21 1, "Truy cập vô tuyến mặt đất toàn cầu phát triển (E-UTRA); Physical Channels and Modulation (Phiên bản 8)", phần 6.2, có sẵn tại http://www.3gpp.org và kết hợp ở đây bằng cách viện dẫn).

Một khung thứ cấp bao gồm hai khe, sao cho có 14 ký hiệu OFDM trong khung thứ cấp khi cái gọi là CP (tiền tố vòng) "thông thường" được sử dụng, và 12 ký hiệu OFDM trong khung thứ cấp khi cái gọi là CP "mở rộng" được sử dụng. Về mặt thuật ngữ, trong phần sau tài nguyên thời gian tần số tương đương với cùng N_{sc}^{RB} sóng mang con liên tục mở rộng toàn bộ khung thứ cấp được gọi là "cặp khối tài nguyên", hoặc "cặp RB" tương đương hoặc "cặp PRB".

Thuật ngữ "sóng mang thành phần chỉ đến sự kết hợp một vài khối tài nguyên trong miền tần số. Trong phiên bản tương lai của LTE, thuật ngữ "sóng mang thành phần" không còn được sử dụng; thay vì, thuật ngữ được đổi thành "khu (cell)", chỉ đến sự kết hợp của các tài nguyên đường nối xuống và các tài nguyên đường nối lên tùy chọn. Sự liên kết giữa tần số sóng mang của các tài nguyên đường nối xuống và tần số sóng mang của các tài nguyên đường nối lên được chỉ báo trong thông tin hệ thống được truyền trên các tài nguyên đường nối xuống.

Giả định tương tự cho kết cấu sóng mang thành phần cũng áp dụng cho các phiên bản về sau.

Sự gộp sóng mang trong LTE-A để hỗ trợ dải thông rộng hơn.

Phổ tần số đối với IMT cải tiến được quyết định tại Hội nghị truyền thông radio thế giới 2007 (WRC- 07- World Radiocommunication Conference

2007). Mặc dù phổ tần số tổng thể cho IMT cải tiến đã được quyết định, nhưng dải tần số khả dụng thực tế là khác nhau tương ứng với mỗi vùng hoặc quốc gia. Tuy nhiên, theo quyết định về đề cương phổ tần số khả dụng, sự chuẩn hóa về giao diện radio lại bắt đầu ở Dự án hợp tác thế hệ thứ ba (3GPP). Tại cuộc họp 3GPP TSG RAN #39 phần mô tả mục nghiên cứu về "Further Advancements for E-UTRA (LTE -Advanced)" được chấp nhận. Mục nghiên cứu bao phủ các thành phần công nghệ được xem xét đối với sự phát triển của E-UTRA, ví dụ để đáp ứng các yêu cầu về IMT cải tiến.

Dải thông mà hệ thống LTE cải tiến có khả năng hỗ trợ là 100 MHz, trong khi hệ thống LTE chỉ có thể hỗ trợ 20 MHz. Ngày nay, việc thiếu phổ tần radio trở nên nút thắt cổ chai đối với sự phát triển của mạng không dây, và kết quả là rất khó để tìm một băng phổ đủ rộng cho hệ thống LTE cải tiến. Hệ quả là, cần khẩn trương tìm ra một cách để có được một băng phổ radio rộng hơn, trong đó câu trả lời có thể là chức năng gộp sóng mang.

Trong sự gộp sóng mang, hai hoặc nhiều sóng mang thành phần (sóng mang thành phần) được gộp để hỗ trợ các dải thông truyền rộng hơn lên tới 100MHz. Một vài khu trong hệ thống LTE được gộp thành một kênh rộng hơn trong hệ thống LTE tiên tiến mà đủ rộng cho 100 MHz mặc dù các khu trong LTE theo các dải tần số khác nhau.

Toàn bộ sóng mang thành phần có thể được cấu hình tương thích với LTE Rel. 8/9, ít nhất là khi số sóng mang thành phần được gộp trong đường nối lên và trong đường nối xuống là giống nhau. Không phải toàn bộ sóng mang thành phần được gộp bởi một thiết bị người dùng có thể cần thiết tương thích với Rel. 8/9. Cơ chế hiện nay (ví dụ việc ngăn chặn) có thể được sử dụng để tránh thiết bị người dùng Rel-8/9 tạm lưu ở sóng mang thành phần.

Một thiết bị người dùng có thể đồng thời nhận hoặc truyền một hoặc nhiều sóng mang thành phần (tương ứng với nhiều khu dịch vụ) tùy thuộc vào khả năng của mình. Thiết bị người dùng LTE-A Rel. 10 với khả năng nhận và/hoặc

truyền cho sự gộp sóng mang có thể đồng thời nhận và/hoặc truyền trên nhiều khu dịch vụ, trong khi một thiết bị người dùng LTE Rel. 8/9 có thể nhận và truyền chỉ trên khu dịch vụ đơn lẻ, với điều kiện là là kết cấu sóng mang thành phần tuân thủ quy phạm Rel. 8/9

Sự gộp sóng mang được hỗ trợ đối với các sóng mang thành phần gần kề và không gần kề với mỗi sóng mang thành phần được giới hạn tối đa lên tới 110 khối tài nguyên trong miền tần số sử dụng thuật toán số 3GPP LTE (Phiên bản 8/9).

Có thể cấu hình 3GPP LTE-A (Phiên bản 10) tương thích với thiết bị người dùng để gộp số lượng các sóng mang thành phần khác nhau có nguồn gốc từ eNodeB (trạm cơ sở) tương tự và số lượng các dải thông khác nhau có thể trong đường nối lên và đường nối xuống. Số lượng sóng mang thành phần đường nối xuống mà có thể được cấu hình tùy thuộc vào khả năng gộp đường nối xuống của UE. Ngược lại, số lượng sóng mang thành phần đường nối lên mà có thể được cấu hình tùy thuộc vào khả năng gộp đường nối lên của UE. Có thể không có khả năng cấu hình một thiết bị đầu cuối di động với các sóng mang thành phần đường nối lên nhiều hơn so với các sóng mang thành phần đường nối xuống.

Trong việc triển khai TDD thông thường, một số sóng mang thành phần và dải thông của mỗi sóng mang thành phần trong đường nối lên và đường nối xuống là giống nhau. Sóng mang thành phần có nguồn gốc từ eNodeB tương tự không cần cung cấp cùng vùng phủ sóng.

Khoảng cách giữa các tần số trung tâm của các sóng mang thành phần được gộp liên tục sẽ là bội số của 300 kHz. Điều này tương thích với mành tần số 100 kHz của 3GPP LTE (Phiên bản 8/9) và đồng thời bảo tồn tính trực giao của sóng mang con với khoảng cách 15 kHz. Tùy thuộc vào kịch bản gộp, khoảng cách n x 300 kHz có thể được làm dễ dàng bằng cách chèn một số ít các sóng mang con không sử dụng giữa các sóng mang thành phần liền kề.

Bản chất của sự gộp nhiều sóng mang là chỉ bộc lộ đối với lớp MAC. Đối với cả hai đường nối lên và đường nối xuống có một thực thể HARQ được yêu cầu trong MAC đối với mỗi sóng mang thành phần được gộp. Có (trong trường hợp không có SU-MIMO đối với đường nối lên) ít nhất một khối vận chuyển cho mỗi sóng mang thành phần. Khối vận chuyển và sự truyền lại HARQ tiềm tại của nó cần được ánh xạ lên sóng mang thành phần tương tự.

Kết cấu lớp 2 với sự gộp sóng mang được kích hoạt như được thể hiện trên Fig. 5 và Fig. 6 đối với đường nối xuống và đường nối lên tương ứng.

Khi sự gộp sóng mang được cấu hình, thiết bị đầu cuối di động chỉ có một nối kết RRC với mạng. Khi thiết lập/tái thiết lập nối kết RRC, một khu nhỏ cung cấp đầu vào an toàn (một ECGI, một PCI và một ARFCN) và thông tin di động báo hiệu tầng không truy nhập (ví dụ, TAI) tương tự như trong LTE Rel. 8/9. Sau khi thiết lập/tái thiết lập nối kết RRC, sóng mang thành phần tương ứng với khu nhỏ được gọi là khu nhỏ chính đường nối xuống (Primary Cell- PCell). Luôn có một và chỉ một PCell đường nối xuống (DL PCell) và một PCell đường nối lên (UL PCell) được cấu hình cho mỗi thiết bị người dùng ở trạng thái đã kết nối. Trong bộ cấu hình của các sóng mang thành phần, các khu nhỏ khác được gọi là các khu nhỏ thứ cấp (Secondary Cells - SCells); với sóng mang của SCell là sóng mang thành phần thứ cấp đường nối xuống (DL SCC) và sóng mang thành phần thứ cấp đường nối lên (UL SCC). Các đặc trưng của đường nối xuống và đường nối lên PCell là:

- Đối với mỗi SCell việc sử dụng tài nguyên đường nối lên bởi UE, ngoài tài nguyên đường nối xuống có thể được cấu hình; Số lượng DL SCCs được cấu hình do đó luôn lớn hơn hoặc bằng số lượng UL SCCs, và không có SCell có thể được cấu hình đối với việc chỉ sử dụng tài nguyên đường nối lên.

- Đường nối lên PCell được dùng cho việc truyền thông tin điều khiển đường nối lên Lớp 1.

- Đường nối xuống PCell có thể không được khử kích hoạt, khác với SCells.

- Từ quan điểm UE, mỗi tài nguyên đường nối lên chỉ thuộc một khu nhỏ dịch vụ.

- Số lượng khu nhỏ dịch vụ mà có thể được cấu hình tùy thuộc vào khả năng gộp của UE.

- Sự tái thiết lập được kích hoạt khi PCell đường nối xuống trải qua việc giảm âm Rayleigh (RLF), không phải khi đường nối xuống SCells trải qua RLF.

- Khu nhỏ PCell đường nối xuống có thể thay đổi với việc chuyển vùng (nghĩa là với sự thay đổi khóa an toàn và quy trình RACH).

- Báo hiệu tầng không truy nhập thông tin được lấy từ đường nối xuống Pcell.

- PCell có thể chỉ được thay đổi với quy trình chuyển vùng (nghĩa là với việc thay đổi khóa an toàn và quy trình RACH).

- PCell được dùng cho việc truyền PUCCH.

Việc cấu hình và cấu hình lại sóng mang thành phần có thể được thực hiện bởi RRC. Sự kích hoạt và khử kích hoạt được thực hiện thông qua các phần tử điều khiển MAC. Khi chuyển vùng nội LTE, RRC cũng có thể thêm, loại bỏ, hoặc cấu hình lại SCells cho việc sử dụng trong cell đích. Khi thêm một SCell mới, báo hiệu RRC dành riêng được sử dụng để gửi thông tin hệ thống của SCell, thông tin này là cần thiết cho việc truyền/ nhận (tương tự như trong Rel-8/9 cho việc chuyển vùng).

Khi thiết bị người dùng được cấu hình với sự gộp sóng mang có một cặp sóng mang thành phần đường nối lên và đường nối xuống luôn kích hoạt. Sóng mang thành phần đường nối xuống của cặp này có thể cũng được gọi là 'DL sóng mang neo'. Áp dụng tương tự đối với đường nối lên.

Khi sự gộp sóng mang được cấu hình, một thiết bị người dùng có thể được lập lịch trên nhiều sóng mang thành phần đồng thời nhưng hầu như chỉ một thủ tục truy nhập ngẫu nhiên được liên tục làm việc. Sự lập lịch sóng mang chéo cho phép PDCCH của sóng mang thành phần lập lịch tài nguyên trên sóng mang thành phần khác. Vì mục đích này, trường nhận dạng sóng mang thành phần được đưa vào trong các định dạng DCI tương ứng, gọi là CIF.

Sự kết nối giữa các sóng mang thành phần đường nối lên và đường nối xuống cho phép nhận dạng sóng mang thành phần đường nối lên, sóng mang này được cấp phép áp dụng khi không có lập lịch sóng mang chéo. Sự kết nối của sóng mang thành phần đường nối xuống tới sóng mang thành phần đường nối lên không cần thiết phải là 1-1. Nói cách khác, hơn một sóng mang thành phần đường nối xuống có thể nối với cùng một sóng mang thành phần đường nối lên. Tại thời điểm này, một sóng mang thành phần đường nối xuống có thể chỉ nối với một sóng mang thành phần đường nối lên.

Tình hình triển khai khu nhỏ

Nhu cầu bùng nổ về dữ dữ liệu di động đang hướng tới sự thay đổi trong cách các nhà điều hành di động sẽ cần đáp ứng các yêu cầu đầy thách thức về dung lượng cao hơn và chất lượng kinh nghiệm người sử dụng được cải thiện (QoE). Hiện nay, hệ thống truy cập không dây thế hệ thứ tư sử dụng phát triển dài hạn (LTE) được triển khai bởi nhiều nhà điều hành trên toàn thế giới để cung cấp việc truy nhập nhanh hơn với độ trễ thấp hơn và hiệu quả hơn hệ thống 3G/3.5G.

Sự tăng trưởng lưu lượng trong tương lai được dự đoán là rất lớn do đó nhu cầu tăng cao đối với sự nén mạng hơn nữa để xử lý các yêu cầu về dung lượng, đặc biệt là trong những khu vực lưu lượng cao (những khu vực điểm nóng) tạo ra khối lượng lưu lượng cao nhất. Sự nén mạng- tăng số lượng nút mạng, nhờ đó mang chúng lại gần hơn về mặt vật lý với thiết bị đầu cuối người dùng- là chìa

khóa để cải thiện dung lượng lưu lượng và mở rộng tỷ lệ dữ liệu người dùng có thể đạt được của hệ thống truyền thông không dây.

Ngoài ra, trong việc nén trực tiếp của sự triển khai vĩ mô, sự nén mạng có thể đạt được bằng cách triển khai nút công suất thấp bổ sung một cách tương ứng các khu nhỏ dưới vùng phủ của lớp nút vĩ mô hiện có. Trong sự triển khai không đồng nhất như vậy, nút công suất thấp cung cấp dung lượng lưu lượng rất cao và thông lượng người dùng rất cao cục bộ, ví dụ ở các điểm nóng bên trong và bên ngoài. Trong khi đó, lớp vĩ mô đảm bảo khả năng dịch vụ và QoE trên toàn bộ vùng phủ sóng. Nói cách khác, lớp chứa nút công suất thấp có thể cũng được xem như là cung cấp truy nhập cục bộ, ngược lại với lớp vĩ mô che phủ vùng rộng.

Việc lắp đặt các nút công suất thấp tương ứng các khu nhỏ cũng như việc triển khai không đồng nhất có thể đạt được từ phiên bản thứ nhất của LTE. Về phương diện này, một số giải pháp được xác định trong các phiên bản của LTE gần đây (ví dụ, phiên bản-10/11). Cụ thể hơn, các phiên bản gần đây này đã đưa ra những công cụ bổ sung để xử lý nhiễu liên lớp trong việc triển khai không đồng nhất. Để tối ưu hóa hơn nữa tính năng và mang lại hoạt động tiết kiệm chi phí/năng lượng. Các khu nhỏ cần cải tiến hơn nữa và trong nhiều trường hợp cần phải tương tác với hoặc bổ sung các khu vĩ mô hiện có.

Sự tối ưu hóa như vậy sẽ được khảo sát như là một phần của việc phát triển thêm nữa đối với LTE - phiên bản 12 và tiếp theo. Cụ thể là việc tăng cường thêm liên quan đến các nút công suất thấp và triển khai không đồng nhất sẽ được xem xét dưới sự bảo trợ của hạng mục nghiên cứu Rel-12 mới (SI) có tên "Study on Small Cell Enhancements for E-UTRA and E-UTRAN". Một số hoạt động sẽ tập trung vào việc đạt được thậm chí mức độ cao hơn đối với liên kết mạng giữa các lớp vĩ mô và lớp công suất thấp, bao gồm các dạng hỗ trợ vĩ mô khác nhau đối với khả năng liên kết lớp công suất thấp và lớp kép. Khả năng liên kết kép

có nghĩa là thiết bị có sự kết nối đồng thời với cả hai lớp vĩ mô và lớp công suất thấp.

Khả năng kết nối kép

Một giải pháp đầy triển vọng cho các vấn đề mà hiện nay đang được phân tích trong các nhóm làm việc 3GPP RAN là khái niệp được gọi là khái niệm khả năng kết nối kép. Khả năng kết nối kép được sử dụng để chỉ một hoạt động mà một UE tiêu thụ tài nguyên radio được cung cấp bởi ít nhất hai nút mạng khác nhau được kết nối qua hành trình ngược phi lý tưởng.

Nói cách khác, trong khả năng kết nối kép UE được kết nối với cả hai khu lớn (eNB chủ hoặc lớn) và khu nhỏ (eNB thứ cấp hoặc nhỏ). Hơn nữa, mỗi eNB tham gia vào khả năng kết nối kép cho UE có thể đảm nhận các vai trò khác nhau. Các vai trò này không nhất thiết phụ thuộc vào loại công suất của eNB và có thể thay đổi giữa các UE.

Để sử dụng thuật ngữ phù hợp, việc tham khảo được thực hiện với phần mô tả giai đoạn 2 (3GPP R2-140906) về việc tăng cường khu nhỏ trong LTE mà các thuật ngữ dưới đây được hiểu như sau. Nhóm khu lớn, MCG, trong khả năng kết nối kép mô tả nhóm khu dịch vụ được liên kết với MeNB, bao gồm P khu và tùy chọn một hoặc nhiều S khu. eNB chủ trong khả năng kết nối kép biểu thị eNB, eNB này ít nhất tiếp nối S1 -MME. Trong khía cạnh này, thuật ngữ tải mang MCG trong khả năng kết nối kép dùng để chỉ giao thức radio chỉ nằm trong MeNB để sử dụng tài nguyên MeNB.

Tương tự, nhóm khu thứ cấp, SCG, trong khả năng kết nối kép mô tả nhóm khu dịch vụ được liên kết với SeNB bao gồm S khu đặc biệt và tùy chọn một hoặc nhiều S khu. eNB thứ cấp trong khả năng kết nối kép biểu thị eNB, eNB này cung cấp tài nguyên radio bổ sung đối với UE mà không phải là ENB chủ. Trong khía cạnh này, thuật ngữ tải mang SCG trong khả năng kết nối kép dùng để chỉ giao thức radio chỉ được đặt trong eNB thứ cấp để sử dụng tài nguyên eNB thứ cấp.

Do hạng mục nghiên cứu hiện nay mới ở giai đoạn đầu, nên chi tiết trong việc triển khai khả năng kết nối kép vẫn chưa được quyết định. Ví dụ, kết cấu khác nhau vẫn còn được phân tích một cách tích cực và, do đó, có thể ảnh hưởng đến khía cạnh hiện thực của khả năng kết nối kép. Do đó, nhiều vấn đề/chi tiết, ví dụ, sự tăng cường giao thức, vẫn mở cho việc triển khai thêm nữa.

Fig. 7 thể hiện kết cấu để làm ví dụ cho khả năng kết nối kép. Cụ thể là, kết cấu được minh họa tương ứng với những gì được hiểu hiện nay như kết cấu 1A. Trong kết cấu 1A này, S1 -U tiếp nối ở eNB chủ và ở eNB thứ cấp và S1 –MME được tiếp nối ở eNB chủ.

Cả eNB chủ và eNB thứ cấp cung cấp một cách độc lập chức năng của giao thức hội tụ dữ liệu gói (PDCP) sao cho kết cấu được minh họa 1A không cần thiết để cung cấp tải mang chia tách, nghĩa là, khi tải mang được chia tách trên eNB chủ và eNB thứ cấp.

Nhìn chung, cần hiểu rằng kết cấu khả năng kết nối kép 1A được mô tả chỉ là một trong nhiều lựa chọn cho việc thực hiện khả năng kết nối kép. Hơn nữa, khái niệm về khả năng kết nối kép ứng dụng những giả định sau đây về kết cấu:

Mỗi quyết định mức độ tải mang là ở chỗ phục vụ từng gói, chia tách mặt phẳng C/U.

Như một ví dụ báo hiệu UE RRC và dữ liệu QoS cao như VoLTE có thể được phục vụ bởi khu to, trong khi đó dữ liệu nỗ lực tốt nhất không được tải tới khu nhỏ.

Không có sự nối giữa các tải mang, do đó không có PDCP hoặc RLC thông thường được yêu cầu giữa khu lớn và khu nhỏ.

Sự phối hợp lỏng lẻo hơn giữa các nút RAN.

SeNB không có sự kết nối với S-GW, nghĩa là, các gói được chuyển tiếp bởi MeNB.

Khu nhỏ là trong suốt đối với CN.

Liên quan đến hai điểm quan trọng cuối cùng, cần lưu ý rằng cũng có thể là SeNB được kết nối trực tiếp với S-GW, nghĩa là, S1 -U ở giữa S-GW và SeNB. Về cơ bản, có ba lựa chọn khác nhau đối với ánh xạ/chia tách tải mang:

- Lựa chọn 1 : S1 -U cũng tiếp nối ở SeNB; được mô tả trong Fig. 7;

- Lựa chọn 2: S1 -U tiếp nối ở MeNB, không có chia tách tải mang trong RAN; và

- Lựa chọn 3: S1 -U tiếp nối ở MeNB, chia tách tải mang trong RAN.

Sự an toàn

Sự an toàn là đặc tính rất quan trọng của 3GPP LTE và trong 3GPP TS 33.401 : "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 12)", Version 12.10.0, section 4 ("Dự án đối tác thế hệ thứ 3; các dịch vụ nhóm đặc tả kỹ thuật và các khía cạnh hệ thống; tiến hóa kết cấu hệ thống 3GPP (SAE); kết cấu an toàn (phiên bản 12)", phiên bản 12.10.0, phần 4), có sẵn tại http://www.3gpp.org và được kết hợp trong tài liệu này bằng cách viện dẫn, định nghĩa năm nhóm đặc tính an toàn. Mỗi nhóm đặc tính an toàn này bắt gặp các uy hiếp nhất định và thực hiện các mục tiêu an toàn nhất định:

- Sự an toàn truy cập mạng (I) liên quan đến tập hợp đặc tính an toàn, tập hợp này cung cấp cho người dùng truy cập an toàn tới các dịch vụ, và trong đó đặc biệt là bảo vệ chống lại sự tấn công trên liên kết truy cập (radio).

- Sự an toàn miền mạng (II) liên quan đến tập hợp đặc tính an toàn, tập hợp này cho phép các nút trao đổi dữ liệu an toàn, dữ liệu người dùng (giữa AN và SN và trong AN), và bảo vệ chống lại sự tấn công trên mạng có dây.

- Sự an toàn miền người dùng (III) liên quan đến tập hợp đặc tính an toàn để truy cập an toàn tới các trạm di động.

- Sự an toàn miền người ứng dụng (IV) liên quan đến tập hợp đặc tính an toàn, tập hợp này cho phép các ứng dụng trong người dùng và trong miền nhà cung cấp trao đổi tin nhắn một cách an toàn.

- Chế độ hiển thị và cấu hình an toàn (V) liên quan đến tập hợp các đặc tính, tập hợp này cho phép người dùng thông báo cho bản thân người dùng xem đặc tính an toàn đang hoạt động hay không và việc sử dụng và cung cấp dịch vụ sẽ phụ thuộc vào đặc tính an toàn.

Các mục tiêu an toàn được minh họa trong Fig. 8 đối với sự tương tác giữa các đơn vị và các lớp chức năng trong LTE. Trong phần còn lại của tài liệu, phần phân tích tập trung vào sự an toàn truy cập mạng.

Sự bảo mật dữ liệu người dùng (và dữ liệu báo hiệu): mật mã hóa

Dữ liệu người dùng (và dữ liệu báo hiệu) phải được mật mã hóa. Việc bảo vệ sự bảo mật mặt phẳng người dùng sẽ được thực hiện ở lớp PDCP và là một lựa chọn nhà điều hành. Dữ liệu mặt phẳng người dùng được mật mã hóa bởi giao thức PDCP giữa UE và eNB như được xác định trong 3GPP TS 36.323: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification (Release 11)", Version 11.2.0, section 5.6 (Dự án đối tác thế hệ thứ 3; Mạng truy cập radio nhóm tham số kỹ thuật; Truy cập vô tuyến mặt đất toàn cầu phát triển (E-UTRA); Quy định giao thức hội tụ dữ liệu gói (PDCP) (Phiên bản 1 1)", Phiên bản 1 1 .2.0, phần 5.6), có sẵn tại http://www.3gpp.org và được kết hợp trong tài liệu này bằng cách viện dẫn.

Yêu cầu về việc xử lý thời hạn mặt phẳng người dùng đối với eNB

Đây là nhiệm vụ của eNB để mật mã hóa và giải mật mã gói mặt phẳng người dùng giữa điểm tham chiếu Uu và các điểm tham chiếu S1/X2 và để xử lý bảo vệ toàn vẹn cho các gói mặt phẳng người dùng đối với các điểm tham chiếu S1/X2.

1. Việc mật mã/giải mật mã dữ liệu mặt phẳng người dùng và việc xử lý toàn vẹn sẽ được tiến hành bên trong môi trường an toàn nơi các khóa liên quan được lưu trữ.

2. Việc chuyển dữ liệu người dùng qua S1 -U và X2-U sẽ được bảo vệ toàn vẹn, bảo vệ bảo mật và bảo vệ phát lại chống lại các bên không có quyền. Nếu điều này được thực hiện bằng phương tiện mật mã, khoản 12 sẽ được áp dụng ngoại trừ đối với giao diện Un giữa RN và DeNB.

Yêu cầu đối với việc xử lý thời hạn mặt phẳng điều khiển cho eNB

Nhiệm vụ của eNB là cung cấp bảo vệ sự bảo mật và bảo vệ toàn vẹn đối với các gói mặt phẳng điều khiển trên các điểm tham chiếu S1/X2.

1 . Việc mật mã hóa/giải mật mã dữ liệu mặt phẳng điều khiển và việc xử lý toàn vẹn sẽ diễn ra bên trong môi trường an toàn nơi các khóa liên quan được lưu trữ.

2. Việc chuyển dữ liệu mặt phẳng điều khiển qua S1-MME và X2-C sẽ được bảo vệ toàn vẹn, bảo vệ bảo mật và bảo vệ phát lại đối với các bên không có quyền. Nếu điều này được thực hiện bằng phương tiện mật mã, khoản 11 sẽ được áp dụng ngoại trừ đối với giao diện Un giữa RN và DeNB.

Phân cấp khóa mật EPS

Yêu cầu về EPC và E-UTRAN liên quan đến khóa mật:

a) EPC và E-UTRAN sẽ cho phép sử dụng các thuật toán mã hóa và bảo vệ toàn vẹn đối với việc bảo vệ AS và NAS có khóa mật dài 128 bit và về tương lai sử dụng các giao diện mạng sẽ được chuẩn bị để hỗ trợ khóa mật 256 bit.

b) Khóa mật được sử dụng cho việc bảo vệ UP, NAS và AS sẽ phụ thuộc vào thuật toán mà chúng được sử dụng.

Sự phân cấp khóa mật được thể hiện trong Fig. 9 bao gồm các khóa mật sau: K_{eNB}, K_{NASint}, K_{NASenc}, K_{UPenc}, K_{RRCint} và K_{RRCenc}. Trong phần tiếp theo, việc tham khảo được thực hiện đối với hàm số dẫn xuất khóa mật, KDF, được quy

định tại Mục A.7 của 3GPP TS 33.401: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 12)", Version 12.10.0, section 4, có sẵn tại http://www.3gpp.org và được kết hợp trong tài liệu này bằng cách viện dẫn.

K_{eNB} là khóa mật mật được dẫn xuất bởi ME và MME từ K_{ASME} hoặc bởi ME và eNB đích.

Khóa mật đối với lưu lượng NAS:

K_{NASint} là khóa mật mật, khóa mật này sẽ chỉ được sử dụng cho việc bảo vệ lưu lượng NAS với thuật toán toàn vẹn đặc biệt. Khóa mật này được dẫn xuất bởi ME và MME từ K_{ASME}, cũng như là một bộ nhận dạng cho thuật toán toàn vẹn bằng cách sử dụng KDF.

K_{NASenc} là khóa mật, khóa mật này sẽ chỉ được sử dụng cho việc bảo vệ lưu lượng NAS với thuật toán mã hóa đặc biệt. Khóa mật này được dẫn xuất bởi ME và MME từ K_{ASME}, cũng như là bộ nhận dạng cho thuật toán mã hóa bằng cách sử dụng KDF.

Khóa mật cho lưu lượng UP:

K_{UPenc} là khóa mật, khóa mật này sẽ chỉ được sử dụng cho việc bảo vệ lưu lượng UP với thuật toán mã hóa đặc biệt. Khóa mật này được dẫn xuất bởi ME và eNB từ K_{eNB}, cũng như là bộ nhận dạng cho thuật toán mã hóa bằng cách sử dụng KDF.

K_{UPint} là khóa mật, khóa mật này sẽ chỉ được sử dụng để bảo vệ lưu lượng UP giữa RN và DeNB với thuật toán toàn vẹn đặc biệt. Khóa mật này được dẫn xuất bởi RN và DeNB từ K_{eNB}, cũng như là một bộ nhận dạng cho thuật toán toàn vẹn bằng cách sử dụng KDF.

Khóa mật cho lưu lượng RRC:

K_{RRCint} là khóa mật, khóa mật này sẽ chỉ được sử dụng cho sự bảo vệ lưu lượng RRC với thuật toán toàn vẹn đặc biệt. K_{RRCint} được dẫn xuất bởi ME và eNB từ K_{eNB}, cũng như là một bộ nhận dạng cho thuật toán toàn vẹn bằng cách sử dụng KDF.

K_{RRCenc} là khóa mật, khóa mật này sẽ chỉ được sử dụng cho sự bảo vệ lưu lượng RRC với thuật toán mã hóa đặc biệt. K_{RRCenc} được dẫn xuất bởi ME và eNB từ K_{eNB} cũng như là một bộ nhận dạng cho thuật toán mã hóa bằng cách sử dụng KDF.

Khóa mật trung gian:

NH, đề cập đến tham số Next Hop, là khóa mật được dẫn xuất bởi ME và MME để cung cấp sự an toàn chuyển tiếp.

K_{eNB}* là khóa mật được dẫn xuất bởi ME và eNB khi thực hiện dẫn xuất khóa mật theo chiều dọc hoặc ngang.

Cụ thể là, xử lý khóa mật trong việc chuyển giao được mô tả trong phần 7.2.8 của 3GPP TS 33.401: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 12)", Version 12.10.0, có sẵn tại http://www.3gpp.org và được kết hợp trong tài liệu này bằng cách viện dẫn.

Đối với khả năng kết nối kép, S-K_{eNB} sẽ được dẫn xuất từ K_{eNB} và "tham số độ mới", tham số này được làm ví dụ là 16 bit dài.

Chuyển giao Intra-eNB (trong eNB)

Khi eNB quyết định thực hiện việc chuyển giao Intra-eNB nó sẽ dẫn xuất K_{eNB} * như trong phụ lục A.5 bằng cách sử dụng PCI đích, tần số của nó EARFCN-DL, và NH hoặc K_{eNB} hiện tại phụ thuộc vào các tiêu chí sau đây: eNB sẽ sử dụng NH để dẫn xuất K_{eNB} * nếu cặp không {NH, NCC} không được sử dụng có thể sử dụng trong eNB (điều này được đề cập như dẫn xuất khóa theo chiều dọc), mặt khác nếu không có cặp không {NH, NCC} không được sử

dụng có thể được sử dụng trong eNB, eNB sẽ dẫn xuất K_{eNB} * từ K_{eNB} hiện tại (điều này được đề cập như dẫn xuất khóa theo chiều ngang).

eNB sẽ sử dụng K_{eNB}* như K_{eNB} sau khi chuyển giao. eNB sẽ gửi NCC được sử dụng cho việc dẫn xuất K_{eNB}* đến UE trong tin nhắn mệnh lệnh HO.

Chuyển giao X2

Như trong chuyển giao Intra-eNBs, đối với chuyển giao X2 nguồn eNB sẽ thực hiện dẫn xuất khóa mật dọc trong trường hợp nó có một cặp không {NH, NCC} không được sử dụng. Nguồn eNB trước tiên sẽ phải tính toán K_{eNB}* từ PCI đích, tần số của nó EARFCN-DL, và hoặc từ K_{eNB} đang hoạt động trong trường hợp dẫn xuất khóa mật ngang hoặc từ NH trong trường hợp dẫn xuất khóa mật dọc như được mô tả trong phụ lục A.5 của 3GPP TS 33.401: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 12)", Version 12.10.0, có sẵn tại http://www.3gpp.org và được kết hợp trong tài liệu này bằng cách viện dẫn.

Tiếp theo, nguồn eNB sẽ chuyển tiếp cặp {K_{eNB}*, NCC} tới eNB đích. eNB đích sẽ sử dụng K_{eNB}* thu được một cách trực tiếp như K_{eNB} được sử dụng với UE. eNB đích sẽ kết hợp giá trị NCC thu được từ nguồn eNB với K_{eNB}. eNB đích sẽ đưa NCC thu được vào tin nhắn mệnh lệnh HO được chuẩn bị, tin nhắn này được gửi trở lại nguồn eNB trong đồ chứa trong suốt và chuyển tới UE bởi nguồn eNB.

Khi eNB đích đã hoàn thành việc báo hiệu chuyển giao với UE, nó sẽ gửi S1 PATH SWITCH REQUEST tới MME. Khi nhận S1 PATH SWITCH REQUEST, MME sẽ làm tăng giá trị được giữ cục bộ của nó NCC bằng một và tính NH mới mới được tạo ra bằng cách sử dụng K_{ASME} và giá trị được giữ cục bộ của nó NH như đầu vào của hàm số được định nghĩa trong phụ lục A.4. MME sau đó sẽ gửi cặp {NH, NCC} mới được tính tới eNB đích trong tin nhắn S1 PATH SWITCH REQUEST ACKNOWLEDGE. eNB đích sẽ lưu trữ cặp

{NH, NCC} nhận được để chuyển giao tiếp và loại bỏ cặp {NH, NCC} được lưu trữ không được sử dụng nếu có.

Làm mới KeNB

Thủ tục này dựa trên việc chuyển giao intra-khu (trong khu). Việc kết nối K_{eNB} được thực hiện trong thời gian quá trình chuyển giao đảm bảo rằng K_{eNB} được làm mới đối với RRC và UP COUNT sau thủ tục này.

Thuật toán mật mã hóa 128-bit

Đầu vào và đầu ra

Các tham số đầu vào cho thuật toán mật mã hóa là khóa mật mật mã hóa 128-bit có tên là KEY, COUNT 32-bit, nhận dạng tải mang 5-bit BEARER, hướng 1-bit của truyền dẫn, tức là DIRECTION, và chiều dài của dòng khóa mật được yêu cầu, tức là LENGTH. Bit DIRECTION sẽ là 0 đối với đường nối lên 1 đối với đường nối xuống.

Fig. 10 minh họa việc sử dụng thuật toán mật mã hóa EEA để mật mã hóa văn bản gốc bằng việc áp dụng dòng khóa mật bằng cách sử dụng đếm nhị phân từng bit đối với văn bản gốc và khóa mật dòng. Văn bản gốc có thể được khôi phục bởi việc tạo dòng khóa mật tương tự bằng cách sử dụng tham số đầu vào tương tự và áp dụng cộng nhị phân từng bit với văn bản mã hóa.

Việc sử dụng và phương thức hoạt động của thuật toán 128-EEA được xác định trong phụ lục B của 3GPP TS 33.401: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 12)", Version 12.10.0, có sẵn tại http://www.3gpp.org và được kết hợp trong tài liệu này bằng cách viện dẫn.

Tham số đầu vào thuật toán 128-bit EEA là khóa mật mật mã hóa 128-bit K_{UPenc} như KEY, nhận dạng tải mang 5-bit BEARER có giá trị được được gán như được xác định bởi PDCP, hướng truyền 1-bit DIRECTION, chiều dài của

dòng khóa mật được yêu cầu LENGTH và đặc định tải mang, thời gian và hướng phụ thuộc đầu vào 32-bit COUNT, đầu vào này tương ứng với PDCP COUNT 32-bit.

Dựa trên tham số đầu vào thuật toán tạo ra khối dòng khóa mật đầu ra được sử dụng để mật mã hóa khối văn bản gốc đầu vào PLAINTEXT để tạo ra khối văn bản mật mã hóa đầu ra CIPHERTEXT. Tham số đầu vào LENGTH sẽ chỉ ảnh hướng đến chiều dài của KEYSTREAM BLOCK, chứ không phải là bit thực tế ở trong đó.

Hạn chế của điều khiển công suất theo giải pháp kỹ thuật đã biết

Trong khả năng kết nối kép, khóa mật an toàn S-K_{eNB} được áp dụng cho sự an toàn truy cập mạng đối với trạm cơ sở thứ cấp, SeNB và có thể so sánh về tính năng của nó với khóa mật an toànK_{eNB} đối với trạm cơ sở chính, MeNB. Dẫn xuất của khóa mật an toàn này S-K_{eNB} sẽ được giải thích liên quan đến Fig. 12.

Trạm cơ sở chính, MeNB, dẫn xuất, trong bước 3, khóa mật an toàn S-K_{eNB} này cho việc truyền thông giữa thiết bị đầu cuối di động và trạm cơ sở thứ cấp từ khóa mật an toànK_{eNB} và giá trị "bộ đếm Counter". Sau đó, S-K_{eNB} được dẫn xuất được truyền bởi trạm cơ sở chính, MeNB, trong bước 4, tới trạm cơ sở thứ cấp, S_{eNB}. Sau đó, trạm cơ sở thứ cấp, dẫn xuất S_{eNB}, trong bước 5, khóa mật mật mã hóa UP S-K_{UPenc}, và khóa mật bảo vệ toàn vẹn tùy ý S-K_{UPint}, từ S-K_{eNB} này. Cụ thể là, SeNB còn dẫn xuất khóa mật toàn vẹn UP từ S-K_{eNB} này (và nếu được yêu cầu khóa mật toàn vẹn cho báo hiệu RRC và mặt phẳng người dùng và khóa mật mật mã hóa RRC). Bộ đếm này là bộ đếm mới 16 bit (hoặc có thể có chiều dài khác) và nó được gọi là “tham số độ mới".

Như đã thấy từ Fig.10, đối với phần mật mã hóa/mã hóa từ KHÓA (K_{eNB}/ S-K_{eNB}), bốn tham số đầu vào khác được quy định cho hoạt động mật mã hóa của dữ liệu. Độ an toàn dựa trên nguyên tắc rằng toàn bộ năm tham số đầu vào sẽ không giống nhau cho việc mật mã hóa tiếp theo. Nếu chúng là như thế thì

điều này biểu thị mối đe dọa an toàn tiềm năng. Tham số đầu vào COUNT, DIRECTION và LENGTH không cho phép nhiều mức độ tự do cho eNB để chọn/ thay đổi giữa các giá trị khác nhau; ví dụ, đối với việc mật mã hóa dữ liệu UL, DIRECTION phải chỉ ra "UL". Đối với mật mã hóa dữ liệu DL, DIRECTION phải chỉ ra "DL".

Vấn đề nảy sinh từ tình huống khi việc nhận dạng tải mang (nghĩa là, RB-id) được tái sử dụng như tham số đầu vào BEARER để mật mã hóa/mã hóa (ví dụ, cùng một RB-id được phân bổ cho một tải mang mới). Vấn đề tương tự nảy sinh từ tình huống mà COUNT sẽ kết thúc (cho cùng một BEARER). Trong các tình huống này, nếu KEY (K_{eNB}/S-K_{eNB}) vẫn như cũ, thì khi đó sẽ dẫn đến việc lặp lại trong tham số đầu vào. Việc lặp lại như thế trong tham số đầu đối với mật mã hóa/mã hóa biểu thị lỗ hổng an toàn mà có thể bị khai thác. Ví dụ, lỗ hổng an toàn tái sử dụng RB-id có thể được khai thác bởi kẻ tấn công một cách nhanh chóng bằng cách bổ sung ngày càng nhiều ứng dụng.

Đối với việc mật mã hóa và tính toàn vẹn giá trị COUNT được duy trì, giá trị này được thể hiện trong Fig.11. Giá trị COUNT bao gồm dãy số HFN và PDCP, SN. Chiều dài của PDCP SN được cấu hình bởi các lớp trên. PDCP SN là đặc định tải mang, điều này có nghĩa là đối với mỗi tải mang radio, PDCP SN riêng biệt được duy trì. Kích cỡ của một phần HFN trong các bit bằng 32 trừ đi chiều dài của PDCP SN. Việc kết thúc COUNT sẽ xảy ra khi số PDCP PDU được truyền vượt quá tổng chiều dài của COUNT.

Tải mang (RB-id) tái sử dụng (cùng RB-id được phân bổ cho tải mang mới) có thể xảy ra trong các tình huống sau đây: Thứ nhất, giải phóng tải mang và cùng RB-id sau đó (đặc biệt là DRB) được phân bổ cho tải mang khác. DRB-id là RB-id phân bổ cho tải mang dữ liệu (DRB). Thứ hai, khi khoảng trống DRB-id được kết thúc, nghĩa là, 29 DRB trong LTE (32 - 3 SRBs) được thiết lập và tải mang mới sẽ cần phải sử dụng một trong những DRB-id đã được sử dụng. Tổng cộng 32 tải mang có thể được cấu hình với một UE trong LTE, trong đó có

3 tải mang (và Id tương ứng) được dành riêng cho việc báo hiệu, được gọi là tải mang radio báo hiệu.

Do khả năng kết nối kép chưa được chuẩn hóa, các vấn đề được phân tích trên đây còn mới và không có giải pháp khả dụng được quy định. Tuy nhiên, dựa trên các nguyên tắc kế thừa (ví dụ, LTE Rel. 11 và trước đó) eNB tránh RB-id tái sử dụng càng nhiều càng tốt. Tuy nhiên, có thể có điểm mà theo đó tình huống (tải sử dụng RB-id hoặc kết thúc COUNT) không thể tránh được nữa.

Khi việc tránh là không thể/rất khó, MeNB có thể thực hiện chuyển giao intra-khu, việc này làm thay đổi K_{eNB} được sử dụng trong MeNB (MCG) mà còn không rõ làm thế nào để dẫn đến việc làm mới S- K_{eNB}. Khi/nếu K_{eNB} được sử dụng để làm mới S-K_{eNB}, tải mang MeNB cũng bị gián đoạn không cần thiết do việc làm mới của K_{eNB} chỉ là phương tiện làm mới S- K_{eNB} mà không được yêu cầu khác (không tái sử dụng RB-id hoặc kết thúc COUNT cho các tải mang được phục vụ trực tiếp bởi MeNB). Hơn nữa, việc chuyển giao intra-khu là thủ tục khá đắt do nó liên quan đến gián đoạn nhất định của dữ liệu người dùng không chỉ trong S_{eNB} mà còn trong MeNB. Việc gián đoạn dữ liệu người dùng đối với MeNB chỉ tải mang là không cần thiết/có thể tránh được vì điều chủ yếu là vấn đề an toàn tại S_{eNB}.

Kết quả là chuyển giao intra-khu toàn bộ tải mang cần phải được tái thiết lập và dữ liệu được chuyển tiếp giữa các nút mạng, v.v... Vì vậy điều này sẽ được tránh tốt hơn hoặc được tối ưu hóa.

Khả năng kết nối kép đưa ra kết nối nhiều hơn một eNB với UE, nghĩa là, UE tiêu thụ/sử dụng tài nguyên từ hai eNB. Cả hai tính an toàn bảo vệ báo hiệu và/hoặc dữ liệu về phía UE với các khóa tương ứng của chúng; MeNB với K_{eNB} và S_{eNB} với S-K_{eNB}.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất phương pháp cải tiến thiết lập liên kết truyền thông an toàn giữa trạm cơ sở chính và trạm cơ sở thứ cấp trong trường hợp sự vi phạm an toàn được tìm ra, qua đó tránh được những vấn đế của tình trạng kỹ thuật như được xác định trên đây.

Mục đích này được giải quyết bởi vấn đề chính của các yêu cầu bảo hộ độc lập. Các phương án có lợi được nêu trong các yêu cầu bảo hộ phụ thuộc.

Giả định rằng trạm di động trong khả năng kết nối kép và do đó được kết nối với cả trạm cơ sở chính và trạm cơ sở thứ cấp qua các liên kết truyền thông tương ứng. Như được giải thích trên đây, trong khả năng kết nối kép khóa mật an toàn S-K_{eNB} cho nhóm khu thứ cấp, SCG, (nghĩa là, cho việc truyền thông với trạm cơ sở thứ cấp) là phụ thuộc lẫn nhau vào khóa mật an toàn K_{eNB} đối với nhóm khu chính, MCG (nghĩa là, cho việc truyền thông với trạm cơ sở chính).

Trong khía cạnh này, trong trường hợp phát hiện sự vi phạm tiềm năng an toàn, mạng sẽ kích hoạt chuyển giao intra-khu nội bộ cho toàn bộ tải mang của nhóm khu chính và nhóm khu thứ cấp, qua đó việc tái thiết lập an toàn cho việc truyền thông với trạm cơ sở chính và thứ cấp.

Theo khía cạnh thứ nhất của sáng chế, trong trường hợp việc tìm ra sự vi phạm tiềm năng an toàn, sáng chế đề xuất chỉ để thiết lập lại sự an toàn cho truyền thông với trạm cơ sở thứ cấp mà không phải với trạm cơ sở chính. Đối với việc thiết lập lại sự an toàn độc lập cho việc truyền thông với trạm cơ sở thứ cấp, khóa mật an toàn mới S-K_{eNB} được dẫn xuất trên cơ sở tăng dần, và ở đây là, tham số đầu vào COUNT mới cho thuật toán mật mã hóa/mã hóa (sau đây gọi là bộ đếm độ mới). Nói cách khác, khóa mật an toàn K_{eNB} cho việc truyền thông với trạm cơ sở chính có thể được duy trì tương tự, do đó không cần thiết có chuyển giao intra-khu.

Cụ thể là, đáp lại sự vi phạm an toàn tiềm năng được tìm ra, trạm cơ sở chính gia tăng bộ đếm độ mới để khởi chạy lại truyền thông giữa trạm di động

và trạm cơ sở thứ cấp. Thuật ngữ khởi chạy lại truyền thông, trong ngữ cảnh của sáng chế, sẽ được hiểu là việc tái thiết lập lớp con PDCP, tái thiết lập lớp con RLC và cài đặt lại lớp MAC.

Trong khía cạnh này, việc khởi chạy lại truyền thông khác biệt với việc thực hiện một lệnh chuyển giao ở chỗ nó cung cấp định tuyến các đơn vị dữ liệu gói tối ưu, cụ thể là do C-RNTI không thay đổi. Quan trọng hơn, sự khởi chạy lại truyền thông được kích hoạt bởi tin nhắn khác nhau, cụ thể là tin nhắn cấu hình lại kết nối RRC, tin nhắn này không bao gồm mệnh lệnh chuyển giao (nghĩa là không có thông tin điều khiển di động).

Sự khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp dựa trên sự gia tăng bộ đếm độ mới trong đó khóa mật an toàn mới S-K_{eNB} được dẫn xuất cho việc truyền thông nêu trên dưới sự điều khiển của trạm cơ sở chính. Về khía cạnh này, trạm di động và trạm cơ sở thứ cấp có khả năng thiết lập liên kết truyền thông an toàn, sau khi tìm ra sự vi phạm tiềm năng an toàn, bằng cách sử dụng cùng khóa mật an toàn được dẫn xuất S-K_{eNB}.

Do các thủ tục nêu trên có sự khác biệt so với thủ tục hiện đang được thực hiện ngay khi phát hiện có sự vi phạm tiềm năng an toàn, một cách độc lập với tình huống nêu trên, đề xuất sau đây cải thiện sự thiết lập lại an toàn trong nhóm khu thứ cấp.

Theo khía cạnh thứ hai của sáng chế, trạm di động (nghĩa là UE) được đề xuất, trạm di động được khởi chạy lại để truyền thông với trạm cơ sở chính và trạm cơ sở thứ cấp trong hệ thống truyền thông không dây, trong đó trạm di động nhận từ trạm cơ sở chính tin nhắn cấu hình lại (ví dụ tin nhắn cấu hình lại kết nối RRC) trong đó bao gồm bộ đếm độ mới.

Chỉ với mục đích làm rõ, có thể nhấn mạnh rằng tin nhắn cấu hình lại không bao gồm mệnh lệnh chuyển giao.

Đáp lại việc nhận tin nhắn cấu hình lại, trạm di động dẫn xuất khóa mật an toàn S-K_{eNB} cho việc truyền thông với trạm cơ sở thứ cấp. Cụ thể hơn, trạm di

động dẫn xuất khóa mật an toàn S-K_{eNB} dựa trên bộ đếm độ mới được gia số có trong tin nhắn cấu hình lại.

Khóa thứ cấp S-K_{eNB}, sau này được sử dụng, bởi trạm di động, để khởi chạy lại truyền thông với trạm cơ sở thứ cấp, do đó cho phép trạm di động thiết lập liên kết truyền thông an toàn với trạm cơ sở thứ cấp.

Đáng lưu ý là, tin nhắn cấu hình lại nhận được từ trạm cơ sở chính bao gồm bộ đếm độ mới được gia số. Theo đó, trạm di động có thể dẫn xuất để kích hoạt sự khởi chạy lại truyền thông với trạm cơ sở thứ cấp. Nói cách khác, tin nhắn cấu hình lại không dành cho việc truyền thông với trạm cơ sở thứ cấp mà không có bộ đếm độ mới được gia số trong đó.

Có lợi là, trong trường hợp trạm di động nhận tin nhắn cấu hình lại dưới dạng mật mã từ trạm cơ sở chính, trạm di động có thể xác định, dựa vào phiên bản hiện tại của khóa mật an toàn K_{eNB} trong đó, ngoài bộ đếm độ mới được gia số, còn có khóa mật an toàn được dẫn xuất cho việc truyền thông với trạm cơ sở thứ cấp.

Theo phương án thứ nhất, phù hợp với khía cạnh thứ nhất của sáng chế, phương pháp được đề xuất để thiết lập liên kết truyền thông an toàn giữa trạm di động và trạm cơ sở thứ cấp trong hệ thống truyền thông di động. Hệ thống truyền thông di động bao gồm trạm di động, trạm cơ sở chính và thứ cấp. Trạm di động được khởi chạy truyền thông với trạm cơ sở chính và thứ cấp.

Trạm cơ sở chính hoặc trạm cơ sở thứ cấp tìm ra sự vi phạm tiềm năng an toàn bao gồm trạng thái mà ở đó bộ đếm chuỗi của đơn vị dữ liệu gói liên kết truyền thông được thiết lập an toàn giữa trạm di động và trạm cơ sở thứ cấp sẽ kết thúc do sự khởi chạy truyền thông giữa trạm di động và trạm cơ sở thứ cấp, và trạng thái mà sự nhận dạng liên kết truyền thông được tái sử dụng để thiết lập liên kết truyền thông an toàn với trạm cơ sở thứ cấp do sự khởi chạy truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Trong trường hợp sự vi phạm tiềm năng an toàn được phát hiện bởi trạm cơ sở thứ cấp, trạm cơ sở thứ cấp báo hiệu sự vi phạm an toàn được tìm ra với trạm cơ sở chính. Đáp lại sự vi phạm tiềm năng an toàn được báo hiệu hoặc được phát hiện, trạm cơ sở chính gia số bộ đếm độ mới để khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp; và trạm di động và trạm cơ sở thứ cấp, khởi chạy lại truyền thông giữa chúng. Sự khởi chạy lại được thực hiện dưới sự điều khiển của trạm cơ sở chính và còn bao gồm dẫn xuất khóa mật an toàn tương tự dựa trên bộ đếm độ mới được gia số này, và thiết lập liên kết truyền thông an toàn sử dụng cùng khóa mật an toàn được dẫn xuất.

Theo phương án thứ hai, phù hợp với khía cạnh thứ nhất của sáng chế, hệ thống truyền thông di động được đề xuất để thiết lập liên kết truyền thông an toàn giữa trạm di động và trạm cơ sở thứ cấp. Hệ thống truyền thông di động bao gồm trạm di động, trạm cơ sở chính và trạm cơ sở thứ cấp. Trạm di động được khởi chạy để truyền thông với trạm cơ sở chính và thứ cấp.

Trạm cơ sở chính và/hoặc trạm cơ sở thứ cấp được cấu hình để tìm ra sự vi phạm tiềm năng an toàn bao gồm: trạng thái mà ở đó bộ đếm chuỗi đối với đơn vị dữ liệu gói của liên kết truyền thông an toàn được thiết lập giữa trạm di động và trạm cơ sở thứ cấp sẽ kết thúc do sự khởi chạy truyền thông giữa trạm di động và trạm cơ sở thứ cấp, và trạng thái mà sự nhận dạng liên kết truyền thông được tái sử dụng để thiết lập liên kết truyền thông an toàn với trạm cơ sở thứ cấp do sự khởi chạy truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Trạm cơ sở thứ cấp được cấu hình, trong trường hợp tìm ra sự vi phạm tiềm năng an toàn, để báo hiệu sự vi phạm an toàn được tìm ra tới trạm cơ sở chính; trạm cơ sở chính được cấu hình để gia số, đáp lại sự vi phạm tiềm năng an toàn được báo hiệu hoặc được phát hiện, bộ đếm độ mới để khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Mô tả vắn tắt các hình vẽ

Sau đây sáng chế được mô tả chi tiết hơn với việc tham chiếu tới hình vẽ kèm theo.

Fig. 1 thể hiện kết cấu để làm ví dụ của hệ thống 3GPP LTE,

Fig. 2 thể hiện khái quát ví dụ về kết cấu E-UTRAN tổng thể của 3GPP LTE,

Fig. 3 thể hiện biên giới khung con làm ví dụ trên sóng mang thành phần đường xuống như được định nghĩa cho 3GPP LTE (phiên bản 8/9),

Fig. 4 thể hiện mạng tài nguyên đường xuống làm ví dụ của khe đường nối xuống như được định nghĩa cho 3GPP LTE (phiên bản 8/9),

Fig. 5 và Fig. 6 thể hiện cấu tạo lớp 2 trong 3GPP LTE (phiên bản 10) với sự gộp sóng mang được kích hoạt cho đường nối xuống và đường nối lên tương ứng,

Fig. 7 trình bày chi tiết kết cấu của hệ thống truyền thông di động trong khả năng kết nối kép với các eNB to và nhỏ được kết nối với mạng lõi trong 3GPP LTE (phiên bản 11),

Fig. 8 đưa ra sự tổng quát về kết cấu an toàn trong 3GPP LTE (phiên bản 12),

Fig. 9 trình bày chi tiết kết cấu khóa mật an toàn trong 3GPP LTE (phiên bản 12),

Fig. 10 minh họa thuật toán mật mã hóa/mã hóa trong 3GPP LTE (phiên bản 12),

Fig. 11 thể hiện định dạng COUNT là tham số đầu vào cho thuật toán mật mã hóa/mã hóa trong 3GPP LTE (phiên bản 11),

Fig. 12 minh họa sự dẫn xuất khóa mật an toàn trong hệ thống truyền thông không dây trong khả năng kết nối kép trong 3GPP LTE (phiên bản 12), và

Fig. 13 đến Fig. 16 minh họa dẫn xuất khóa mật an toàn theo các phương án khác nhau của sáng chế.

Mô tả chi tiết sáng chế

Trạm di động hoặc nút di động là phần tử vật lý trong mạng truyền thông. Một nút có thể có vài phần tử chức năng. Phần tử chức năng dùng để chỉ mô đun phần mềm hoặc phần cứng thực hiện và/hoặc cung cấp tập hợp định trước về chức năng cho các phần tử chức năng khác của nút hoặc mạng. Các nút có thể có một hoặc nhiều giao diện, giao diện này gắn nút vào thiết bị hoặc môi trường truyền thông, qua đó các nút có thể truyền thông. Tương tự, phần tử mạng có thể có giao diện hợp lý gắn phần tử chức năng vào thiết bị hoặc môi trường truyền thông, qua đó các phần tử có thể truyền thông với phần tử chức năng khác hoặc các nút tương ứng.

Thuật ngữ "trạm cơ sở chính" được sử dụng trong các điểm yêu cầu bảo hộ và trong phần mô tả của sáng chế được hiểu như được sử dụng trong lĩnh vực về khả năng kết nối kép của 3GPP LTE-A; do đó, các thuật ngữ khác như trạm cơ sở chính, hoặc eNB chính/lớn; hoặc trạm cơ sở phục vụ hoặc thuật ngữ bất kỳ được quyết định sau này bởi 3GPP. Tương tự, thuật ngữ "trạm cơ sở thứ cấp" được sử dụng trong yêu cầu bảo hộ và trong phần mô tả được hiểu như được sử dụng trong lĩnh vực về khả năng kết nối kép của 3GPP LTE-A; do đó, thuật ngữ khác như trạm cơ sở phụ thuộc, hoặc eNB thứ cấp/phụ thuộc hoặc thuật ngữ bất kỳ khác được quyết định sau này bởi 3GPP.

Thuật ngữ "liên kết vô tuyến" hoặc "liên kết truyền thông" được sử dụng trong các yêu cầu bảo hộ và trong phần mô tả của sáng chế được hiểu theo nghĩa rộng như việc kết nối vô tuyến giữa trạm di động và trạm cơ sở bao gồm trạm cơ sở chính hoặc trạm cơ sở thứ cấp.

Hơn nữa, thuật ngữ "khởi chạy" hoặc "khởi chạy lại" được sử dụng tương ứng trong các yêu cầu bảo hộ và trong phần mô tả của sáng chế được hiểu bao gồm thiết lập (lại) điều khiển liên kết vô tuyến, RLC, lớp con, thiết lập (lại) giao

thức hội tụ dữ liệu gói, lớp con PDCP, và cài đặt (cài đặt lại) điều khiển truy nhập trung gian, MAC, lớp. Trong khía cạnh này, đơn vị dữ liệu dịch vụ, SDU, và/hoặc đơn vị dữ liệu gói, PDU, không được truyền thành công trước sự khởi chạy lại sẽ được truyền phù hợp với sự truyền thông được khởi chạy lại, theo đó bắt buộc an toàn truy cập mạng.

Trong phần tiếp theo, một số phương án của sáng chế sẽ được giải thích chi tiết. Chỉ với mục đích làm ví dụ, hầu hết các phương án được nêu ra liên quan đến phương án truy nhập vô tuyến theo hệ thống truyền thông di động 3GPP LTE (phiên bản 8/9) và LTE-A (phiên bản 10/11), đã được phân tích từng phần trong phần Tình trạng kỹ thuật của sáng chế nêu trên. Cần lưu ý rằng sáng chế có thể được sử dụng một cách có lợi, ví dụ, trong hệ thống truyền thông di động như hệ thống truyền thông 3GPP LTE-A (phiên bản 12) như được mô tả trong phần Tình trạng kỹ thuật của sáng chế nêu trên. Các phương án này được mô tả như là các phương án thực hiện để sử dụng trong việc kết nối với và/hoặc để tăng cường chức năng được xác định trong 3GPP LTE và/hoặc LTE-A. Trong khía cạnh này, thuật ngữ về 3GPP LTE và/hoặc LTE-A được sử dụng trong toàn bộ phần mô tả. Hơn nữa, các cấu hình làm ví dụ được khai thác để trình bày đầy đủ về sáng chế.

Những giải thích này không nên được hiểu là sự giới hạn sáng chế, mà chỉ là những ví dụ về các phương án của sáng chế và để hiểu sáng chế rõ hơn. Những người có trình độ trung bình trong lĩnh vực có thể nhận ra rằng những nguyên tắc chung của sáng chế được nêu trong yêu cầu bảo hộ có thể được áp dụng cho các tình huống khác nhau và trong cách mà không được mô tả một cách rõ ràng ở đây. Một cách tương ứng, tình huống sau đây được giả định cho mục đích làm ví dụ của các phương án khác nhau sẽ không giới hạn sáng chế chỉ như vậy.

Sáng chế sẽ được mô tả với việc tham chiếu đến các hình vẽ từ Fig. 13 đến Fig. 16. Trong phần tiếp theo, tình huống khả năng kết nối kép trong môi trường

khu nhỏ được giả định đối với hệ thống truyền thông không dây. Theo khía cạnh này, trạm di động được nối với cả trạm cơ sở chính và trạm cơ sở thứ cấp một cách tương ứng qua liên kết truyền thông thứ nhất và thứ hai. Lưu ý rằng, tuy nhiên sáng chế không bị giới hạn bởi những tình huống này; ví dụ, các tình huống mà trạm di động được kết nối với trạm cơ sở chính và ít nhất cũng có thể là hai trạm cơ sở thứ cấp.

Chi tiết hơn, trạm di động được khởi chạy truyền thông với trạm cơ sở chính và trạm cơ sở thứ cấp. Trong khía cạnh này, trạm di động được cấu hình với lớp con RLC và lớp con PDCP để truyền thông với trạm cơ sở và trạm cơ sở thứ cấp tương ứng. Theo quan điểm về khía cạnh an toàn, sự khởi chạy truyền thông cũng có nghĩa là trạm di động được cung cấp với khóa mật an toàn, khóa này cho phép trạm di động thiết lập liên kết truyền thông an toàn với trạm cơ sở chính và thứ cấp.

Cụ thể là, việc khởi chạy trạm di động quy định rằng khóa mật an toàn K_{eNB} được cung cấp cho, cụ thể hơn là được dẫn xuất bởi, trạm di động để thiết lập liên kết truyền thông an toàn với trạm cơ sở chính. Từ quan điểm việc thực hiện này, khóa mật an toàn K_{eNB} có thể được sử dụng bởi trạm di động để dẫn xuất thêm nữa khóa mật an toàn cho các mục đích cụ thể, cụ thể là cho việc mật mã hóa hoặc cho sự toàn vẹn. Trong ngữ cảnh này, phần Tình trạng kỹ thuật liệt kê K_{UPint}, K_{UPenc}, K_{RRCint}, và K_{RRcenc}. Cho dù là thế nào, trạm di động có thể đảm bảo an toàn ngay khi liên kết truyền thông với trạm cơ sở chính.

Tương tự, việc khởi chạy lại của trạm di động cũng quy định rằng khóa mật an toàn S-K_{eNB} được cung cấp cho, cụ thể hơn là được dẫn xuất bởi, trạm di động cho việc truyền thông với trạm cơ sở thứ cấp. Cụ thể là, khóa mật an toàn S-K_{eNB} này được dẫn xuất từ khóa mật an toàn K_{eNB} cho việc truyền thông với trạm cơ sở chính và tham số bổ sung được gọi là bộ đếm độ mới. Nói cách khác, trên cơ sở khóa mật an toàn K_{eNB} và bộ đếm độ mới, trạm di động có khả năng

dẫn xuất khóa mật an toàn S-K_{eNB} qua đó cho phép đảm bảo an toàn ngay khi liên kết truyền thông với trạm cơ sở thứ cấp.

Đối với việc truyền thông giữa trạm di động và trạm cơ sở chính, sự vi phạm tiềm năng an toàn có thể được tìm ra. Trong số các điều kiện khác nhau, điều trở nên rõ ràng rằng sự vi phạm tiềm năng an toàn là do từ các tình huống trong đó việc thuật toán mật mã hóa/mã hóa được cung cấp với các tham số đầu vào lặp lại.

Trong ngữ cảnh sáng chế, sự vi phạm tiềm năng an toàn bao gồm trạng thái trong đó bộ đếm chuỗi đối với đơn vị dữ liệu gói, PDU, của liên kết truyền thông an toàn được thiết lập sẽ sớm kết thúc (nghĩa là, vượt quá ngưỡng xác định trước liên quan đến số lượng tối đa bộ đếm chuỗi) hoặc thực sự kết thúc (nghĩa là, vượt quá số lượng tối đa của bộ đếm chuỗi) do sự khởi chạy truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Nói cách khác, trong trường hợp bộ đếm chuỗi liên quan đến liên kết truyền thông an toàn kết thúc, tương tự liên kết truyền thông không còn an toàn do (các) số lượng chuỗi phải được tái sử dụng.

Cụ thể hơn, bộ đếm chuỗi PDU, trên cơ sở tham số COUNT được hình thành bởi số lượng chuỗi PDCP và số khung siêu (Hyper Frame Number – HFN) như được thể hiện trong Fig. 11, đầu vào đối với thuật toán mật mã hóa/mã hóa. Theo đó, sự lặp lại số lượng chuỗi PDU sẽ dẫn đến sự vi phạm tiềm năng an toàn. Do đó, sự vi phạm tiềm năng an toàn này có thể được tìm ra bằng cách dò tìm trạng thái trong đó bộ đếm chuỗi PDU kết thúc do việc khởi chạy.

Trong ngữ cảnh của sáng chế, sự vi phạm tiềm năng an toàn cũng bao gồm trạng thái mà ở đó sự nhận dạng liên kết truyền thông, cụ thể hơn, nhận dạng tải mang nguồn RB-id, được tái sử dụng (nghĩa là, sự nhận dạng liên kết truyền thông không được sử dụng trước đây đã không còn giá trị) do sự khởi chạy truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Việc tái sử dụng sự nhận dạng liên kết truyền thông có thể là kết quả của việc thiết lập liên kết truyền

thông an toàn mới. Nói cách khác, trong trường hợp đa số sự nhận dạng liên kết truyền thông khả dụng đã được sử dụng hết, thì việc thiết lập liên kết truyền thông thêm nữa là không an toàn do nó liên quan đến việc tái sử dụng sự nhận dạng liên kết truyền thông.

Cụ thể hơn, sự nhận dạng liên kết truyền thông (nghĩa là, RB-id) dưới dạng tham số BEARER còn là đầu vào đối với thuật toán mật mã hóa/mã hóa sao cho sự lặp lại của chúng cũng dẫn đến sự vi phạm tiềm năng an toàn. Do đó, sự vi phạm tiềm năng an toàn như vậy có thể được phát hiện bằng cách dò tìm trạng thái trong đó sự nhận dạng liên kết truyền thông được tái sử dụng do việc khởi chạy.

Khái quát hơn, sự vi phạm an toàn tiềm năng được phân tích trên đây liên quan đến việc truyền thông được khởi chạy duy nhất giữa trạm di động và trạm cơ sở thứ cấp. Trong khía cạnh này, truyền thông giữa trạm di động và trạm cơ sở thứ cấp nên được khởi chạy lại, việc tìm ra tình trạng dẫn đến sự vi phạm tiềm năng an toàn bắt đầu lại. Do đó, điều kiện của việc kết thúc bộ đếm chuỗi hoặc việc tái sử dụng nhận dạng liên kết truyền thông chỉ mang tính quyết định nếu chúng xuất hiện do sự khởi chạy truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Theo phương án cụ thể hơn, trạng thái mà ở đó bộ đếm chuỗi đối với PDU sắp kết thúc được phát hiện bởi trạm cơ sở thứ cấp. Cụ thể là, trạm cơ sở thứ cấp này được cung cấp vì lý do toàn vẹn với bộ đếm chuỗi đối với PDU như một phần truyền thông với trạm di động. Do đó, trạm cơ sở thứ cấp có thể phát hiện, từ khi bắt đầu việc truyền thông với trạm di động, bộ đếm chuỗi sắp kết thúc.

Trong phương án khác cụ thể hơn, trạng thái mà ở đó sự nhận dạng liên kết truyền thông sắp được tái sử dụng có thể được tìm ra bởi trạm cơ sở chính hoặc trạm cơ sở thứ cấp. Do tình huống khả năng kết nối kép yêu cầu cả hai, trạm cơ sở chính và thứ cấp được thông báo về việc thiết lập liên kết truyền thông an toàn mới giữa trạm di động và trạm cơ sở thứ cấp, cả hai trạm cơ sở có thể theo

dõi phép gán nhận dạng liên kết truyền thông và, cụ thể là, việc tái sử dụng chúng do việc khởi chạy.

Sự vi phạm tiềm năng an toàn có thể được phát hiện bởi trạm cơ sở thứ cấp, cùng trạm cơ sở thứ cấp báo hiệu sự vi phạm an toàn được phát hiện tới trạm cơ sở chính. Ngoài ra, sự vi phạm tiềm năng an toàn có thể được phát hiện bởi trạm cơ sở chính, không yêu cầu báo hiệu tới trạm cơ sở chính.

Đáp lại sự vi phạm an toàn tiềm năng được báo hiệu hoặc được phát hiện, trạm cơ sở chính ngăn chặn sự vi phạm an toàn tiềm năng tương tự bằng cách kích phát khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Cụ thể là, đối với mục đích này, trạm cơ sở chính tăng khóa mật an toàn S-K_{eNB} cho truyền thông giữa trạm di động và trạm cơ sở dựa vào bộ đếm độ mới.

Sau đó, trạm di động và trạm cơ sở thứ cấp khởi chạy lại truyền thông với nhau dưới sự điều khiển của trạm cơ sở chính, cụ thể là bởi trạm di động và trạm cơ sở thứ cấp, dẫn xuất khóa mật an toàn tương tự S-K_{eNB} trên cơ sở bộ đếm độ mới được tăng. Cụ thể là, trạm cơ sở chính kiểm soát việc dẫn xuất khóa mật an toàn tương tự S-K_{eNB} bằng cách cung cấp bộ đếm độ mới được tăng tới trạm di động và trạm cơ sở thứ cấp.

Do đó, việc đã có khởi chạy lại truyền thông trạm di động và trạm cơ sở thứ cấp có khả năng thiết lập liên kết truyền thông an toàn với nhau bằng cách khóa mật an toàn tương tự, được dẫn xuất S-K_{eNB}.

Một cách thuận lợi, trong phương án này, việc truyền thông giữa trạm di động và trạm cơ sở thứ cấp được khởi chạy lại mà không cần có trước khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở chính. Nói cách khác, để truyền thông giữa trạm di động và trạm cơ sở thứ cấp khóa mật an toàn S-K_{eNB} tương tự được dẫn xuất, việc này dựa trên bộ đếm độ mới được gia số, do đó khác nhau, và qua đó có khả năng thiết lập liên kết truyền thông an toàn giữa chúng mà không yêu cầu khởi chạy lại truyền thông với trạm cơ sở chính, vốn đã đòi hỏi việc dẫn xuất của khóa mật an toàn K_{eNB} tương ứng.

Ví dụ thứ nhất của phương án chi tiết hơn theo sáng chế

Đề cập đến Fig. 13 trong đó ví dụ thứ nhất của phương án chi tiết hơn của sáng chế được thể hiện. Phương án này minh họa phương pháp thiết lập liên kết truyền thông an toàn giữa trạm di động và trạm cơ sở thứ cấp trong hệ thống truyền thông di động bằng cách sử dụng khả năng kết nối kép. Theo đó, hệ thống truyền thông di động bao gồm trạm cơ sở chính và trạm cơ sở thứ cấp. Trạm di động được khởi chạy để truyền thông với trạm cơ sở chính và trạm cơ sở thứ cấp.

Giả sử rằng việc truyền thông giữa trạm di động và trạm cơ sở chính và thứ cấp được khởi chạy lần lượt, trạm cơ sở chính hoặc trạm cơ sở thứ cấp thực hiện, trong bước 1, hoạt động dò tìm sự vi phạm tiềm năng an toàn. Như được phân tích trên đây, sự vi phạm tiềm năng an toàn có thể được tìm ra như là trạng thái mà bộ đếm chuỗi PDU sắp kết thúc hoặc trạng thái mà sự nhận dạng liên kết truyền thông được tái sử dụng do sự khởi chạy truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Trong trường hợp ví dụ trạm cơ sở thứ cấp tìm ra trạng thái mà bộ đếm chuỗi đối với đơn vị dữ liệu gói của liên kết truyền thông an toàn được thiết lập giữa trạm di động và trạm cơ sở thứ cấp sắp kết thúc hoặc thực sự kết thúc, thì trạm cơ sở thứ cấp tương tự báo hiệu, trong bước 2, sự vi phạm an toàn được tìm ra tới trạm cơ sở chính. Do trong trường hợp thay thế, trạm cơ sở chính tương tự có thể phát hiện sự vi phạm an toàn, báo hiệu sự vi phạm an toàn được tìm ra được biểu thị tùy ý bằng các đường nét đứt.

Việc báo hiệu sự vi phạm an toàn được tìm ra bởi trạm cơ sở thứ cấp tới trạm cơ sở chính có thể tương ứng với tin nhắn yêu cầu thay việc truyền thông giữa trạm di động và trạm cơ sở thứ cấp được dựa vào khóa mật an toàn S-KeNB.

Đáp lại sự vi phạm an toàn được tìm ra hoặc được báo hiệu, trạm cơ sở chính gia số, trong bước 3, bộ đếm độ mới được duy trì cho việc truyền thông

giữa trạm di động và trạm cơ sở thứ cấp. Bộ đếm độ mới là để khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp trong đó cho phép thực thi sự an toàn truy cập mạng giữa chúng.

Sau đó, trạm cơ sở chính, trong bước 4, dẫn xuất trên cơ sở bộ đếm độ mới được gia số khóa mật an toàn S-K_{eNB} mới cho việc truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Như được phân tích trong phần mô tả trên đây, dẫn xuất của khóa mật an toàn S-K_{eNB} không chỉ dựa trên bộ đếm độ mới được gia số mà còn dựa trên khóa mật an toàn K_{eNB} cho việc truyền thông giữa trạm di động và trạm cơ sở chính, khóa mật này cũng có giá trị cho cả hai phía truyền thông.

Một cách thuận lợi, phương án này loại bỏ sự cần thiết đối với trạm cơ sở chính cần khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở chính, và do đó, loại bỏ cả sự cần thiết đối với trạm cơ sở chính cần dẫn xuất khóa mật an toàn K_{eNB} mới.

Sau khi khóa mật an toàn mới S-K_{eNB} được dẫn xuất cho việc truyền thông giữa trạm di động và trạm cơ sở thứ cấp, trạm cơ sở chính truyền, trong bước 5, khóa mật an toàn được dẫn xuất S-K_{eNB} mới này và độ mới được gia tăng tới trạm cơ sở thứ cấp. Về phần thực hiện, việc truyền khóa mật an toàn được dẫn xuất mới S-K_{eNB} và bộ đếm độ mới được gia số được thực hiện bằng cách sử dụng giao diện X2.

Sau đó, trạm cơ sở thứ cấp tạo ra, trong bước 6, tin nhắn cấu hình lại bao gồm bộ đếm độ mới được gia số để khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Trạm cơ sở thứ cấp sau đó truyền tin nhắn tương tự tới trạm cơ sở chính. Từ bên thực hiện, việc truyền tin nhắn cấu hình lại có thể tác động bằng cách lợi dụng giao diện X2.

Trong việc thực hiện phương án này, tin nhắn cấu hình lại là tin nhắn cấu hình lại kết nối RRC và bao gồm thông tin bổ sung thông thường có trong tin nhắn. Cụ thể là, tin nhắn cấu hình lại kết nối RRC bao gồm thêm mã dẫn đầu

kênh truy nhập ngẫu nhiên chuyên dụng - RACH. Với mục đích minh họa, mã dẫn đầu RACH chuyên dụng có tiêu đề là mã dẫn đầu - Y RACH.

Tin nhắn cấu hình lại, được tạo ra bởi trạm cơ sở thứ cấp, sau đó được chuyển tiếp, trong bước 7, bởi trạm cơ sở chính tới trạm di động. Mặc dù tin nhắn cấu hình lại nhận được từ trạm cơ sở chính, trạm di động có thể xác định từ nội dung của nó rằng nó được tạo ra bởi và, do đó, được kết nối với (nghĩa là, liên quan đến) truyền thông với trạm cơ sở thứ cấp và không truyền thông với trạm cơ sở chính.

Chuyên gia trong lĩnh vực kỹ thuật có thể dễ dàng lý giải từ phân tích trên đây, rằng tin nhắn cấu hình lại được chuyển tiếp bởi trạm cơ sở chính tới trạm di động được mật mã hóa bởi trạm cơ sở chính bằng cách sử dụng khóa mật an toàn K_{eNB} cho việc truyền thông giữa chúng. Trong khía cạnh này, độ an toàn có thể là bắt buộc đối với việc truyền của bộ đếm độ mới được gia số mà không làm phức tạp thêm việc thực hiện, đơn giản là do thực tế rằng phương án này không cần khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở chính.

Trong ngữ cảnh của sáng chế, việc tiếp nhận tin nhắn cấu hình lại này bởi trạm di động có thể được hiểu như là việc kích hoạt cho trạm di động để thực hiện khởi chạy lại truyền thông với trạm cơ sở thứ cấp.

Theo đó, trạm di động dẫn xuất, trong bước 8, khóa mật an toàn S-K_{eNB} để truyền thông với trạm cơ sở thứ cấp trên cơ sở của bộ đếm độ mới có trong tin nhắn cấu hình lại được chuyển tiếp. Khóa mật an toàn S-K_{eNB} này, được dẫn xuất bởi trạm di động, tương tự với khóa mật an toàn S-K_{eNB} được dẫn xuất trong bước 4 bởi trạm cơ sở chính và được truyền trong bước 5 tới trạm cơ sở thứ cấp.

Do đó, do cả hai, trạm di động và trạm cơ sở thứ cấp được cung cấp khóa mật an toàn tương tự, được dẫn xuất S-K_{eNB}, liên kết truyền thông an toàn có thể được thiết lập trên cơ sở khóa mật an toàn S-K_{eNB} này giữa trạm di động và trạm cơ sở thứ cấp.

Trong một biến thể của bước 8, trạm di động lần đầu tiên xác định liệu bộ đếm độ mới được gia số, có trong tin nhắn cấu hình lại được truyền, có khác biệt với bộ đếm độ mới trước đây có trong tin nhắn cấu hình lại được truyền trước đây hay không, và chỉ trong trường hợp khác biệt, bộ đếm độ mới được gia số, trạm di động mới dẫn xuất khóa mật an toàn tương tự S-K_{eNB}.

Sau đó, trạm di động khởi chạy lại, trong bước 9, truyền thông với trạm cơ sở thứ cấp trên cơ sở khóa mật an toàn tương tự, được dẫn xuất (xem bước 8) cho truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Về phần thực hiện, sự khởi chạy lại được thực hiện bởi trạm di động có thể bao gồm việc thiết lập lại lớp con PDCP, thiết lập lại lớp con RLC và cài đặt lại lớp MAC.

Để thực hiện phương án này trong đó tin nhắn cấu hình lại, là tin nhắn cấu hình lại kết nối RRC, bao gồm mã dẫn đầu - Y RACH chuyên dụng, mã dẫn đầu - Y RACH chuyên dụng này sau đó được sử dụng để thực hiện, trong bước 10, thủ tục RACH giữa trạm di động và trạm cơ sở thứ cấp.

Một cách thuận lợi, thủ tục RACH giữa trạm di động và trạm cơ sở thứ cấp không chỉ cập nhật định thời trước cho việc truyền thông giữa chúng mà cũng có thể được hiểu, trong ngữ cảnh của sáng chế, như là việc kích hoạt cho trạm cơ sở thứ cấp thực hiện khởi chạy lại truyền thông với trạm di động.

Trong khía cạnh này, trạm cơ sở thứ cấp khởi chạy lại, trong bước 11, truyền thông với trạm di động trên cơ sở được khóa mật an toàn tương tự, được dẫn xuất (xem bước 4 và 5) cho việc truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Về phần thực hiện, sự khởi chạy lại được thực hiện bởi trạm di động có thể bao gồm việc thiết lập lại lớp con PDCP, việc thiết lập lại lớp con RCL và cài đặt lại lớp MAC.

Sau đó, trạm di động truyền, trong bước 12, tin nhắn cấu hình lại hoàn chỉnh tới trạm cơ sở chính, trong bước 13, được chuyển tiếp bởi trạm cơ sở chính tới trạm cơ sở thứ cấp. Cụ thể là, trong phương án này, tin nhắn cấu hình

lại hoàn chỉnh được truyền bởi trạm di động sau khi trạm di động và trạm cơ sở thứ cấp cả hai đều khởi chạy lại truyền thông giữa chúng.

Điều này có thể đạt được, ví dụ, bởi trạm di động trì hoãn việc truyền tin nhắn cấu hình lại hoàn chỉnh tới trạm cơ sở chính với khoảng thời gian xác định trước. Ngoài ra, trạm di động cũng có thể giả định rằng trạm cơ sở thứ cấp khởi chạy lại trong bước 10 việc kết nối của nó nhanh hơn việc truyền và chuyển tiếp tin nhắn cấu hình lại hoàn chỉnh trong các bước 12 và 13 và ngay lập tức có thể truyền tải cùng một tin nhắn sau khi hoàn thành thủ tục RACH trong bước 10.

Người đọc có trình độ trung bình trong lĩnh vực kỹ thuật có thể dễ dàng lý giải từ phân tích trên đây, rằng tin nhắn cấu hình lại hoàn chỉnh, được chuyển tiếp bởi trạm di động tới trạm cơ sở chính, được mật mã hóa bởi trạm di động bằng cách sử dụng khóa mật an toàn K_{eNB} cho việc truyền thông giữa chúng với nhau. Trong khía cạnh này, độ an toàn có thể cũng là bắt buộc cho việc truyền tin nhắn cấu hình lại hoàn chỉnh này. Về phần thực hiện, việc truyền tin nhắn cấu hình lại hoàn chỉnh giữa trạm cơ sở trong bước 13 có thể có tác động bằng cách lợi dụng giao diện X2.

Thậm chí còn để thực hiện phương án này, đáp lại tin nhắn cấu hình lại, là tin nhắn cấu hình lại kết nối RRC, tin nhắn cấu hình lại hoàn chỉnh là tin nhắn cấu hình lại kết nối RRC.

Do đó, sau khi khởi chạy lại truyền thông trong bước 9 và 11, trạm di động và trạm cơ sở thứ cấp có khả năng thiết lập liên kết truyền thông an toàn giữa chúng với nhau bằng cách sử dụng khóa mật an toàn tương tự, được dẫn xuất S-K_{eNB}.

Một cách thuận lợi, cũng trong phương án này, việc truyền thông giữa trạm di động và trạm cơ sở thứ cấp khởi chạy lại mà không cần khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở chính trước đó. Nói cách khác, đối với việc truyền thông giữa trạm di động và trạm cơ sở thứ cấp cùng một khóa mật an toàn S-K_{eNB} được dẫn xuất dựa trên bộ đếm độ mới được gia số, và vì vậy khác

nhau, và do đó cho phép thiết lập liên kết truyền thông an toàn giữa chúng mà không yêu cầu khởi chạy lại truyền thông với trạm cơ sở chính, vốn đòi hỏi việc dẫn xuất của khóa mật an toàn tương ứng K_{eNB}.

Ví dụ thứ hai về phương án chi tiết hơn của sáng chế.

Đề cập đến Fig. 14 trong đó ví dụ thứ hai của phương án chi tiết hơn theo sáng chế được thể hiện. Phương án này cũng minh họa phương pháp thiết lập liên kết truyền thông an toàn giữa trạm di động và trạm cơ sở thứ cấp trong hệ thống truyền thông di động bằng cách sử dụng khả năng kết nối kép. Theo đó, hệ thống truyền thông di động bao gồm trạm cơ sở chính và trạm cơ sở thứ cấp. Trạm di động được khởi chạy để truyền thông với trạm cơ sở chính và trạm cơ sở thứ cấp.

Ngược lại với ví dụ thứ nhất về phương án chi tiết hơn, trong phương án này tin nhắn cấu hình lại bao gồm bộ đếm độ mới được tạo ra và được truyền trực tiếp bởi trạm cơ sở chính tới trạm di động và không yêu cầu tạo ra và truyền tin ngắn cấu hình lại tương tự tới trạm cơ sở thứ cấp và sau đó chuyển tiếp nó bởi trạm cơ sở chính tới trạm di động. Theo đó, phương án này dẫn đến việc thiết lập nhanh hơn liên kết truyền thông an toàn trong một tổng thể giữa trạm di động và trạm cơ sở thứ cấp bởi vì tin nhắn cấu hình lại chỉ được truyền một lần thay vì hai lần.

Giả sử việc truyền thông giữa trạm di động và trạm cơ sở chính và thứ cấp được lần lượt khởi chạy lại, trạm cơ sở chính hoặc trạm cơ sở thứ cấp thực hiện, trong bước 1, hoạt động dò tìm sự vi phạm tiềm năng an toàn. Như được phân tích trên đây, sự vi phạm tiềm năng an toàn có thể được phát hiện ở trạng thái mà bộ đếm chuỗi của PDU sắp kết thúc hoặc sự nhận dạng liên kết truyền thông được tái sử dụng do sự khởi chạy truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Trong trường hợp trạm cơ sở thứ cấp tìm ra, ví dụ, trạng thái mà bộ đếm chuỗi đối với đơn vị dữ liệu gói của liên kết truyền thông an toàn được thiết lập

giữa trạm di động và trạm cơ sở thứ cấp sắp kết thúc hoặc thực sự kết thúc, trạm cơ sở thứ cấp tương tự báo hiệu, trong bước 2, sự vi phạm an toàn được phát hiện tới trạm cơ sở chính. Vì trong trường hợp khác, trạm cơ sở chính tương tự có thể phát hiện sự vi phạm an toàn, việc báo hiệu sự vi phạm an toàn đã phát hiện được biểu thị tùy ý bằng đường nét đứt.

Việc báo hiệu sự vi phạm an toàn tìm được bởi trạm cơ sở thứ cấp tới trạm cơ sở chính có thể tương ứng với tin nhắn yêu cầu thay đổi khóa mật an toàn S-K_{eNB} , khóa này làm cơ sở cho việc truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Đáp lại sự vi phạm an toàn được phát hiện hoặc báo hiệu, trạm cơ sở chính gia số, trong bước 3, bộ đếm độ mới được duy trì cho việc truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Bộ đếm độ mới này là để khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp trong đó nó cho phép việc bắt buộc có sự an toàn truy cập mạng ở giữa.

Sau đó, trạm cơ sở chính, trong bước 4, dẫn xuất trên cơ sở bộ đếm độ mới được gia số khóa mật an toàn mới S-K_{eNB} để truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Như được phân tích trong phần mô tả trên đây, việc dẫn xuất của khóa mật an toàn S-K_{eNB} không chỉ dựa trên bộ đếm độ mới được gia số mà còn dựa trên khóa mật an toàn K_{eNB} để truyền thông giữa trạm di động và trạm cơ sở chính, khóa này cũng có giá trị cho cả hai bên truyền thông.

Một cách thuận lợi, phương án này loại bỏ sự cần thiết đối với trạm cơ sở chính để khởi chạy lại truyền thông này giữa trạm di động và trạm cơ sở chính, và, do đó, cũng loại bỏ sự cần thiết đối với trạm cơ sở chính để dẫn xuất khóa mật an toàn mới K_{eNB}.

Sau khi dẫn xuất khóa mật an toàn mới S-K_{eNB} để truyền thông giữa trạm di động và trạm cơ sở thứ cấp, trạm cơ sở chính tạo ra, trong bước 5, tin nhắn cấu hình lại bao gồm bộ đếm độ mới được gia số để khởi chạy lại truyền thông giữa

trạm di động và trạm cơ sở thứ cấp. Trạm cơ sở chính sau đó truyền tin nhắn tương tự tới trạm di động.

Trong phương án này, trạm di động, nhận tin nhắn cấu hình lại bao gồm bộ đếm độ mới được gia số, kết nối tin nhắn này để truyền thông với trạm cơ sở thứ cấp chỉ bởi thực tế rằng nó bao gồm bộ đếm độ mới. Tin nhắn cấu hình lại cho việc cấu hình lại truyền thông với trạm cơ sở chính không bao gồm bộ đếm độ mới. Trong khía cạnh này, trạm di động có thể nhận dạng từ nội dung tin nhắn rằng nó được kết nối với (nghĩa là, có liên quan đến) truyền thông với trạm cơ sở thứ cấp và không truyền thông với trạm cơ sở chính.

Trong việc thực hiện phương án này, tin nhắn cấu hình lại là tin nhắn cấu hình lại kết nối RRC và bao gồm thông tin bổ sung thông thường có trong tin nhắn. Cụ thể là, tin nhắn cấu hình lại kết nối RRC còn bao gồm mã dẫn đầu kênh truy nhập ngẫu nhiên chuyên dụng - RACH. Vì mục đích chỉ để minh họa, mã dẫn đầu RACH chuyên dụng có tên gọi là mã dẫn đầu - Y RACH.

Sau đó, trạm cơ sở chính truyền, trong bước 6, khóa mật an toàn mới được dẫn xuất mới S-K_{eNB} và bộ đếm độ mới được gia số tới trạm cơ sở thứ cấp. Về phần thực hiện, việc truyền khóa mật an toàn được dẫn xuất S-K_{eNB} mới và bộ đếm độ mới được gia số được thực hiện bằng cách sử dụng giao diện X2.

Người đọc có trình độ trong lĩnh vực kỹ thuật có thể dễ dàng lý giải từ phân tích trên đây, rằng tin nhắn cấu hình lại được truyền bởi trạm cơ sở chính tới trạm di động được mật mã hóa bằng trạm cơ sở chính bằng cách sử dụng khóa mật an toàn K_{eNB} cho việc truyền thông giữa chúng với nhau. Trong khía cạnh này, sự an toàn có thể là bắt buộc cho việc truyền bộ đếm độ mới được gia số mà không làm phức tạp thêm việc thực hiện, đơn giản là do thực tế rằng phương án này loại bỏ qua sự cần thiết đối với khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở chính.

Hơn nữa, từ phần mô tả trên đây, rõ ràng rằng bước 5 và 6 cũng có thể được thực hiện bởi trạm cơ sở chính theo thứ tự đảo ngược, cụ thể là tin nhắn

cấu hình lại bao gồm bộ đếm độ mới được gia số được truyền (xem bước 5) tới trạm di động sau khi, và không trước khi truyền (xem bước 6) khóa mật an toàn được dẫn xuất S-K_{eNB} mới và bộ đếm độ mới được gia số tới trạm cơ sở thứ cấp.

Trong ngữ cảnh của sáng chế, việc tiếp nhận tin nhắn cấu hình lại này bởi trạm di động có thể được hiểu như là việc kích hoạt trạm di động để thực hiện khởi chạy lại truyền thông với trạm cơ sở thứ cấp.

Theo đó, trạm di động dẫn xuất, trong bước 7, khóa mật an toàn S-K_{eNB} để truyền thông với trạm cơ sở thứ cấp trên cơ sở bộ đếm độ mới có trong tin nhắn cấu hình lại được chuyển tiếp. Khóa mật an toàn S-K_{eNB} này, được dẫn xuất bởi trạm di động, là tương tự với khóa mật an toàn S-K_{eNB} được dẫn xuất trong bước 4 bởi trạm cơ sở chính và được truyền trong bước 6 tới trạm cơ sở thứ cấp.

Do đó, do cả hai, trạm di động và trạm cơ sở thứ cấp được cung cấp với cùng một khóa mật an toàn được dẫn xuất S-K_{eNB}, liên kết truyền thông an toàn có thể được thiết lập trên cơ sở khóa mật an toàn S-K_{eNB} này giữa trạm di động và trạm cơ sở thứ cấp.

Trong sự biến đổi của bước 7, trạm di động trước tiên quyết định việc có hay không bộ đếm độ mới được gia số, có trong tin nhắn cấu hình lại được truyền, khác với bộ đếm độ mới trước đây có trong tin nhắn cấu hình lại được truyền trước đây, và chỉ trong trường hợp khác nhau, bộ đếm độ mới được gia số, thì trạm di động mới dẫn xuất khóa mật an toàn tương tự S- K_{eNB}.

Sau đó, trạm di động khởi chạy lại, trong bước 8, truyền thông với trạm cơ sở thứ cấp trên cơ sở khóa mật an toàn tương tự, được dẫn xuất (xem bước 8) để truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Về phía thực hiện, sự khởi chạy lại được thực hiện bởi trạm di động có thể bao gồm việc thiết lập lại lớp con PDCP, việc thiết lập lại lớp con RCL và cài đặt lại lớp MAC.

Để thực hiện phương án này khi tin nhắn cấu hình lại, là tin nhắn cấu hình lại kết nối RRC, bao gồm mã dẫn đầu - Y RACH chuyên dụng, mã dẫn đầu - Y

RACH chuyên dụng này sau đó được sử dụng lại để thực hiện, trong bước 9, thủ tục RACH giữa trạm di động và trạm cơ sở thứ cấp.

Một cách thuận lợi, thủ tục RACH giữa trạm di động và trạm cơ sở thứ cấp không chỉ cập nhật định thời trước cho việc truyền thông giữa chúng mà còn có thể được hiểu, trong ngữ cảnh của sáng chế, như là việc kích hoạt trạm cơ sở thứ cấp để thực hiện khởi chạy lại truyền thông với trạm di động.

Trong khía cạnh này, trạm cơ sở thứ cấp khởi chạy lại, trong bước 10, truyền thông với trạm di động trên cơ sở khóa mật an toàn tương tự, được dẫn xuất (xem các bước 4, 6 và 7) để truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Về phía thực hiện, sự khởi chạy lại được thực hiện bởi trạm di động có thể bao gồm việc thiết lập lại lớp con PDCP, việc thiết lập lại lớp con RCL và cài đặt lại lớp MAC.

Sau đó, trạm di động truyền, trong bước 11, tin nhắn cấu hình lại hoàn chỉnh tới trạm cơ sở chính, trong bước 12, được chuyển tiếp bởi trạm cơ sở chính tới trạm cơ sở thứ cấp. Cụ thể là, trong phương án này, tin nhắn cấu hình lại hoàn chỉnh được truyền bởi trạm di động sau khi trạm di động và trạm cơ sở thứ cấp cả hai đều khởi chạy lại truyền thông giữa chúng.

Điều này có thể đạt được, ví dụ, bởi trạm di động trì hoãn việc truyền tin nhắn cấu hình lại hoàn chỉnh tới trạm cơ sở chính với khoảng thời gian được xác định trước. Theo cách khác, trạm di động cũng có thể giả định rằng trạm cơ sở thứ cấp khởi chạy lại trong bước 10 sự kết nối của nó nhanh hơn việc truyền và chuyển tiếp tin nhắn cấu hình lại hoàn chỉnh trong bước 11 và 12 và có thể truyền ngay lập tức tin nhắn tương tự sau khi hoàn thành thủ tục RACH trong bước 9.

Người đọc có trình độ trung bình trong lĩnh vực kỹ thuật có thể dễ dàng lý giải từ phân tích trên đây, rằng tin nhắn cấu hình lại hoàn chỉnh, được chuyển tiếp bởi trạm di động tới trạm cơ sở chính, được mật mã hóa bởi trạm di động bằng cách sử dụng khóa mật an toàn K_{eNB} cho việc truyền thông giữa chúng với

nhau. Trong khía cạnh này, sự an toàn cũng có thể là bắt buộc cho việc truyền tin nhắn cấu hình lại hoàn chỉnh này. Về phần thực hiện, việc truyền tin nhắn cấu hình lại hoàn chỉnh giữa trạm cơ sở trong bước 13 có thể được thực hiện bằng cách sử dụng giao diện X2.

Thậm chí để thực hiện phương án này, đáp lại tin nhắn cấu hình lại, là tin nhắn cấu hình lại kết nối RRC, tin nhắn cấu hình lại hoàn chỉnh là tin nhắn cấu hình lại hoàn chỉnh kết nối RRC.

Do đó, sau khi khởi chạy lại truyền thông trong bước 8 và 10, trạm di động và trạm cơ sở thứ cấp có khả năng thiết lập liên kết truyền thông an toàn giữa chúng với nhau bằng cách sử dụng khóa mật an toàn tương tự, được dẫn xuất S-K_{eNB}.

Một cách thuận lợi, cũng trong phương án này truyền thông giữa trạm di động và trạm cơ sở thứ cấp được khởi chạy lại mà không cần có sự khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở chính trước đó. Nói cách khác, để truyền thông giữa trạm di động và trạm cơ sở thứ cấp, khóa mật an toàn S-K_{eNB} tương tự được dẫn xuất trên cơ sở bộ đếm độ mới được gia số, và do đó khác nhau và nhờ đó cho phép thiết lập liên kết truyền thông an toàn giữa chúng mà không yêu cầu khởi chạy lại truyền thông với trạm cơ sở chính, vốn đã yêu cầu sự dẫn xuất của khóa mật an toàn K_{eNB} tương ứng.

Trong việc thực hiện thay thế của phương án này, tin nhắn cấu hình lại, là tin nhắn cấu hình lại kết nối RRC, có thể bao gồm mã dẫn đầu chuyên dụng từ nhiều mã dẫn đầu được cấu hình trước, hoặc thay vào đó, có thể bao gồm thông tin chỉ dẫn mã dẫn đầu chuyên dụng từ nhiều mã dẫn đầu được cấu hình trước, cụ thể là để thực hiện thủ tục RACH giữa trạm di động và trạm cơ sở thứ cấp. Trong việc thực hiện này, trạm cơ sở chính kiểm soát cấu hình trước của nhiều mã dẫn đầu được cấu hình trước ở trạm cơ sở thứ cấp, ví dụ, bằng cách sử dụng giao diện X2.

Cụ thể hơn, việc thực hiện này giả định tình huống, để truyền thông giữa trạm di động và trạm cơ sở thứ cấp, nhiều mã dẫn đầu RACH được cấu hình trước. Cụ thể là, việc cấu hình trước mã dẫn đầu RACH có thể được xem là có lợi trong tình huống mà không chỉ một mà là đa số trạm di động muốn thiết lập liên kết truyền thông an toàn với trạm cơ sở thứ cấp này.

Trạm cơ sở thứ cấp được ưu tiên cấu hình trước với nhiều mã dẫn đầu để thực hiện thủ tục RACH giữa trạm di động và trạm cơ sở thứ cấp tương tự, trạm di động có thể được truyền/được chỉ báo mã dẫn đầu chuyên dụng từ nhiều mã dẫn đầu tới trạm di động, nghĩa là, không cần thiết yêu cầu trạm cơ sở thứ cấp để gán mã dẫn chuyên dụng cụ thể để thủ tục RACH được thực hiện. Nói cách khác, bằng cách cấu hình trước trạm cơ sở thứ cấp với nhiều mã dẫn đầu, số lượng này được giành riêng cho mục đích cụ thể của trạm cơ sở chính truyền/chỉ báo từ nhiều mã dẫn đầu chuyên dụng được sử dụng để thực hiện thủ tục RACH, mục đích cụ thể này ngăn chặn trạm cơ sở thứ cấp khỏi việc gán cho chúng với mã dẫn đầu chuyên dụng khác nhau.

Do đó, việc cấu hình trước trạm cơ sở thứ hai với nhiều mã dẫn đầu, trong số đó trạm cơ sở chính có thể truyền/chỉ báo mã dẫn đầu chuyên dụng được sử dụng để thực hiện thủ tục RACH, loại bỏ sự cần thiết đối với việc kết hợp với mã dẫn đầu chuyên dụng nào trong số mã dẫn đầu chuyên dụng của trạm cơ sở thứ cấp được truyền/chỉ báo bởi trạm cơ sở chính tới thiết bị đầu cuối di động.

Hơn nữa, sự khác biệt giữa việc truyền và chỉ báo mã dẫn đầu chuyên dụng trong tin nhắn cấu hình lại kết nối RRC bởi trạm cơ sở chính tới trạm di động có thể là hữu ích trong trường hợp số lượng mã dẫn đầu nhỏ (ví dụ, ít hơn 16 mã dẫn đầu được biểu diễn bởi 4 bit), số lượng mã dẫn đầu này được cấu hình trước để thực hiện thủ tục RACH giữa trạm di động và trạm cơ sở chính. Trong trường hợp như vậy, việc truyền hiệu suất đối với tin nhắn cấu hình lại kết nối RRC được cải thiện do yêu cầu ít bit báo hiệu.

Ví dụ thứ ba của phương án chi tiết hơn theo sáng chế.

Đề cập đến Fig. 15 trong đó ví dụ thứ ba của phương án chi tiết hơn theo sáng chế được thể hiện. Phương án này cũng minh họa phương pháp thiết lập liên kết truyền thông an toàn giữa trạm di động và trạm cơ sở thứ cấp trong hệ thống truyền thông di động sử dụng khả năng kết nối kép. Theo đó, hệ thống truyền thông di động bao gồm trạm cơ sở chính và trạm cơ sở thứ cấp. Trạm di động được khởi chạy để truyền thông với trạm cơ sở chính và trạm cơ sở thứ cấp.

Ngược lại với ví dụ thứ hai của phương án chi tiết hơn, trong phương án này tình huống được giả định là không có mã dẫn đầu chuyên dụng hoặc có thể được gán để thực hiện thủ tục RACH giữa trạm di động và trạm cơ sở thứ cấp. Tuy nhiên, cũng trong phương án này việc kích hoạt được yêu cầu để trạm cơ sở thứ cấp thực hiện đồng thời việc khởi chạy lại truyền thông với trạm di động.

Trong khía cạnh này, phương án này đề xuất việc truyền, bởi trạm di động, tin nhắn xác nhận cấu hình lại tới trạm cơ sở thứ cấp (xem bước 9). Qua đó, việc phức tạp thực hiện trong phương án này có thể giảm bớt, cụ thể là bằng cách bỏ qua việc gán mã dẫn đầu chuyên dụng tới trạm di động để thực hiện thủ tục RACH giữa nó và trạm cơ sở thứ cấp. Hơn nữa, trong phương án này thời gian xử lý việc thiết lập liên kết truyền thông an toàn giữa trạm di động và trạm cơ sở thứ cấp giảm bớt.

Giả sử rằng việc truyền thông giữa trạm di động và trạm cơ sở chính và thứ cấp được khởi chạy lại lần lượt, trạm cơ sở chính hoặc trạm cơ sở thứ cấp thực hiện, trong bước 1, hoạt động dò tìm sự vi phạm tiềm năng an toàn. Như được phân tích trên đây, sự vi phạm tiềm năng an toàn có thể được tìm ra như là trạng thái khi bộ đếm chuỗi của PDU sắp kết thúc hoặc khi sự nhận dạng liên kết truyền thông được tái sử dụng do sự khởi chạy truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Trong trường hợp trạm cơ sở thứ cấp tìm ra, ví dụ, trạng thái mà bộ đếm chuỗi đối với đơn vị dữ liệu gói của liên kết truyền thông an toàn được thiết lập

giữa trạm di động và trạm cơ sở thứ cấp sắp kết thúc hoặc thực sự kết thúc, trạm cơ sở thứ cấp tương tự báo hiệu, trong bước 2, sự vi phạm an toàn được tìm ra tới trạm cơ sở chính. Do trong trường hợp khác, trạm cơ sở chính có thể giống như thế phát hiện sự vi phạm an toàn, báo hiệu của sự vi phạm an toàn được tìm ra được chỉ báo theo một lựa chọn là đường nét đứt.

Báo hiệu sự vi phạm an toàn được tìm ra bởi trạm cơ sở thứ cấp tới trạm cơ sở chính có thể tương ứng với tin nhắn yêu cầu thay đổi khóa mật an toàn S-K_{eNB}, khóa này làm cơ sở cho việc truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Đáp lại sự vi phạm an toàn được tìm ra hoặc được báo hiệu, trạm cơ sở chính gia số, trong bước 3, bộ đếm độ mới được duy trì để truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Bộ đếm độ mới này là để khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp trong đó cho phép thực thi sự an toàn truy cập mạng giữa chúng.

Sau đó, trạm cơ sở chính, trong bước 4, dẫn xuất trên cơ sở bộ đếm độ mới được gia số khóa mật an toàn mới S-K_{eNB} để truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Như được phân tích trong phần mô tả trên đây, dẫn xuất khóa mật an toàn S-K_{eNB} không chỉ dựa trên bộ đếm độ mới được gia số mà còn dựa trên khóa mật an toàn K_{eNB} để truyền thông giữa trạm di động và trạm cơ sở chính, khóa mật này cũng có giá trị với cả hai phía truyền thông.

Một cách thuận lợi, phương án này loại bỏ sự cần thiết đối với trạm cơ sở chính để khởi chạy lại truyền thông này giữa trạm di động và trạm cơ sở chính, và, do đó, cũng loại bỏ sự cần thiết để trạm cơ sở chính dẫn xuất khóa mật an toàn mới K_{eNB}.

Sau khi dẫn xuất khóa mật an toàn mới S-K_{eNB} để truyền thông giữa trạm di động và trạm cơ sở thứ cấp, trạm cơ sở chính tạo ra, trong bước 5, tin nhắn cấu hình lại bao gồm bộ đếm độ mới được gia số để khởi chạy lại truyền thông giữa

trạm di động và trạm cơ sở thứ cấp. Trạm cơ sở chính sau đó truyền tin nhắn tương tự tới trạm di động.

Trong việc thực hiện phương án này, tin nhắn cấu hình lại là tin nhắn cấu hình lại kết nối RRC và bao gồm thông tin bổ sung thông thường có trong tin nhắn. Tuy nhiên, trong phương án này, tin nhắn cấu hình lại kết nối RRC không bao gồm mã dẫn đầu chuyên dụng để thực hiện thủ tục RACH. Như lưu ý trên đây, trong phương án này, có thể là trường hợp mà mã dẫn đầu chuyên dụng không được gán hoặc có thể không được gán.

Sau đó, trạm cơ sở chính truyền, trong bước 6, khóa mật an toàn được dẫn xuất S-K_{eNB} mới và bộ đếm độ mới được gia số tới trạm cơ sở thứ cấp. Về phía thực hiện, việc truyền khóa mật an toàn được dẫn xuất S-K_{eNB} mới và bộ đếm độ mới được gia số có thể hưởng tác động bằng cách lợi dụng giao diện X2.

Người đọc có trình độ trung bình trong lĩnh vực kỹ thuật có thể dễ dàng lý giải từ phân tích trên đây, rằng tin nhắn cấu hình lại được truyền bởi trạm cơ sở chính tới trạm di động được mật mã hóa bởi trạm cơ sở chính bằng cách lợi dụng khóa mật an toàn K_{eNB} cho việc truyền thông giữa chúng với nhau. Trong khía cạnh này, sự an toàn có thể là bắt buộc cho việc truyền bộ đếm độ mới được gia số mà không làm phức tạp thêm việc thực hiện, đơn giản là do thực tế rằng phương án này bỏ qua sự cần thiết đối với việc khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở chính.

Hơn nữa, từ phần mô tả trên đây, rõ ràng rằng bước 5 và 6 cũng có thể được thực hiện bởi trạm cơ sở chính theo thứ tự đảo ngược, cụ thể là tin nhắn cấu hình lại bao gồm bộ đếm độ mới được gia số được truyền (xem bước 5) tới trạm di động sau đó, và không trước khi truyền (xem bước 6) khóa mật an toàn được dẫn xuất S-K_{eNB} mới và bộ đếm độ mới được gia số tới trạm cơ sở thứ cấp.

Trong ngữ cảnh của sáng chế, việc tiếp nhận tin nhắn cấu hình lại này bởi trạm di động có thể được hiểu như là việc kích hoạt trạm di động để thực hiện khởi chạy lại truyền thông với trạm cơ sở thứ cấp.

Theo đó, trạm di động dẫn xuất, trong bước 7, khóa mật an toàn S-K_{eNB} để truyền thông với trạm cơ sở thứ cấp trên cơ sở bộ đếm độ mới có trong tin nhắn cấu hình lại được chuyển tiếp. Khóa mật an toàn S-K_{eNB} này, được dẫn xuất bởi trạm di động, tương tự với khóa mật an toàn S-K_{eNB} được dẫn xuất trong bước 4 bởi trạm cơ sở chính và được truyền trong bước 6 tới trạm cơ sở thứ cấp.

Do đó, do cả hai, trạm di động và trạm cơ sở thứ cấp được cung cấp khóa mật an toàn giống nhau, được dẫn xuất S-K_{eNB}, liên kết truyền thông an toàn có thể được thiết lập trên cơ sở khóa mật an toàn S-K_{eNB} này giữa trạm di động và trạm cơ sở thứ cấp.

Trong sự biến đổi của bước 7, trạm di động trước hết xác định có hay không bộ đếm độ mới được gia số, có trong tin nhắn cấu hình lại được truyền, khác biệt với bộ đếm độ mới trước đây có trong tin nhắn cấu hình lại được truyền trước đây, và chỉ trong trường hợp khác biệt, bộ đếm độ mới được gia số, trạm di động dẫn xuất khóa mật an toàn tương tự S-K_{eNB}.

Sau đó, trạm di động khởi chạy lại, trong bước 8, truyền thông với trạm cơ sở thứ cấp trên cơ sở khóa mật an toàn tương tự, được dẫn xuất (xem bước 8) để truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Về phía thực hiện, sự khởi chạy lại được thực hiện bởi trạm di động có thể bao gồm việc thiết lập lại lớp con PDCP, việc thiết lập lại lớp con RCL và cài đặt lại lớp MAC.

Sau khi kết thúc sự khởi chạy lại truyền thông với trạm cơ sở thứ cấp, trạm di động xác nhận việc kết thúc nói trên bởi việc truyền, trong bước 9, tin nhắn báo nhận cấu hình lại tới trạm cơ sở thứ cấp. Về phần thực hiện, việc truyền tin nhắn báo nhận cấu hình lại giữa trạm cơ sở trong bước 13 có thể được hỗ trợ thông qua việc lợi dụng giao diện X2.

Trong việc thực hiện phương án này, tin nhắn báo nhận cấu hình lại hỗ trợ trạm cơ sở thứ cấp dưới dạng phần tử đều khiển (Control Element - CE) điều khiển truy nhập phương tiện (MAC - Medium Access Control). Cụ thể là, việc xác nhận cấu hình lại có thể có trong việc truyền phần tử điều khiển MAC, bằng

cách sử dụng loại MAC CE cụ thể cho tin nhắn cấu hình lại, tin nhắn này được chỉ báo bằng kênh lô gic được xác định trước ID, LCID trong việc truyền trước đây.

Cụ thể là, trong việc thực hiện này, tin nhắn cấu hình lại bao gồm bộ đếm độ mới có thể được truyền và/hoặc chuyển tới trạm di động (xem bước 5) dưới đơn vị dữ liệu gói MAC, PDU. MAC PDU này có thể bao gồm trong phần đầu MAC của nó LCID được xác định trước nhận dạng loại MAC CE được sử dụng cho tin nhắn báo nhận cấu hình lại dưới dạng MAC CE. Theo đó, trạm di động ở giữa bước 5 và bước 9 cần được yêu cầu thực hiện việc truyền khác biệt với việc truyền tin nhắn báo nhận cấu hình lại, trong bước 9, trạm di động có thể sử dụng MAC CE thuộc loại khác mà được chỉ báo bởi LCID được xác định trước.

Một cách thuận lợi, tin nhắn báo nhận cấu hình lại, được truyền bởi trạm di động tới trạm cơ sở thứ cấp, có thể được hiểu, trong ngữ cảnh của sáng chế, như là việc kích hoạt trạm cơ sở thứ cấp để thực hiện khởi chạy lại truyền thông với trạm di động.

Trong khía cạnh này, trạm cơ sở thứ cấp khởi chạy lại, trong bước 10, truyền thông với trạm di động trên cơ sở khóa mật an toàn tương tự, được dẫn xuất (xem các bước 4, 6 và 7) để truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Về phía việc thực hiện, sự khởi chạy lại được thực hiện bởi trạm di động có thể bao gồm việc thiết lập lại lớp con PDCP, việc thiết lập lại lớp con RCL và cài đặt lại lớp MAC.

Do đó, sau khi khởi chạy lại truyền thông trong bước 8 và 10, trạm di động và trạm cơ sở thứ cấp có khả năng thiết lập liên kết truyền thông an toàn giữa chúng với nhau bằng cách sử dụng khóa mật an toàn tương tự, được dẫn xuất S-K_{eNB}.

Một cách thuận lợi, cũng trong phương án này truyền thông giữa trạm di động và trạm cơ sở thứ cấp được khởi chạy lại mà không cần có sự khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở chính. Nói cách khác, để truyền

thông giữa trạm di động và trạm cơ sở thứ cấp, khóa mật an toàn S-K_{eNB} tương tự được dẫn xuất dựa trên bộ đếm độ mới được gia số, do đó khác nhau, và do đó cho phép thiết lập liên kết truyền thông an toàn giữa chúng mà không yêu cầu khởi chạy lại truyền thông với trạm cơ sở chính, việc khởi chạy lại này vốn yêu cầu dẫn xuất khóa mật an toàn K_{eNB} tương ứng.

Điểm mới thực hiện phương án được minh họa trong Fig.15, bao gồm tin nhắn cấu hình lại dưới dạng MAC CE, điều này có thể dễ dàng lý giải do bỏ đi việc thực hiện thủ tục RACH, thời gian xử lý để thiết lập liên kết truyền thông an toàn giữa trạm di động và trạm cơ sở thứ cấp giảm đi khoảng từ 5 đến 15 giây so với việc thực hiện ví dụ thứ hai của phương án chi tiết hơn được thể hiện trong Fig. 14.

Ví dụ thứ tư của phương án chi tiết hơn theo sáng chế.

Đề cập đến Fig. 16 trong đó ví dụ thứ tư của phương án chi tiết hơn theo sáng chế được thể hiện. Phương án này cũng minh họa phương pháp thiết lập liên kết truyền thông an toàn giữa trạm di động và trạm cơ sở thứ cấp trong hệ thống truyền thông di động sử dụng khả năng kết nối kép. Theo đó, hệ thống truyền thông di động bao gồm trạm cơ sở chính và trạm cơ sở thứ cấp. Trạm di động được khởi chạy để truyền thông với trạm cơ sở chính và trạm cơ sở thứ cấp.

Ngược lại với các ví dụ trước đây của phương án chi tiết hơn, trong phương án này tình huống được giả định rằng không chỉ khóa mật an toàn mới S-K_{eNB} để truyền thông giữa trạm di động và trạm cơ sở thứ cấp được dẫn xuất, mà còn khóa mật an toàn được dẫn xuất S-K_{eNB} mới này dựa trên khóa mật an toàn được dẫn xuất K_{eNB}* mới để truyền thông giữa trạm di động và trạm cơ sở chính. Tuy nhiên, khóa mật an toàn được dẫn xuất K_{eNB}* mới không được sử dụng để khởi chạy lại truyền thông giữa thiết bị đầu cuối di động và trạm cơ sở chính.

Thay vào đó, khóa mật an toàn mới K_{eNB}* chỉ được duy trì trong trạm cơ sở chính và trạm di động cho mục đích dẫn xuất sau đó khóa mật an toàn mới S-K_{eNB} để truyền thông giữa thiết bị đầu cuối di động và trạm cơ sở thứ cấp.

Một cách thuận lợi, phương án này loại bỏ sự cần thiết đối với trạm di động và trạm cơ sở chính khởi chạy lại truyền thông giữa chúng với nhau. Trong khía cạnh này, cũng khóa mật an toàn K_{eNB} "cũ" được duy trì trong trạm di động và trạm cơ sở chính để việc truyền thông giữa chúng (ví dụ, để mật mã hóa truyền thông giữa trạm di động và trạm cơ sở chính).

Giả sử rằng việc truyền thông giữa trạm di động và trạm cơ sở chính và thứ cấp được khởi chạy lần lượt, trạm cơ sở chính hoặc trạm cơ sở thứ cấp thực hiện, trong bước 1, hoạt động việc dò tìm sự vi phạm tiềm năng an toàn. Như được thảo luận trên đây, sự vi phạm tiềm năng an toàn có thể được tìm ra như là ở trạng thái mà bộ đếm chuỗi của PDU sắp kết thúc hoặc sự nhận dạng liên kết truyền thông được tái sử dụng do sự khởi chạy truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Trong trường hợp trạm cơ sở thứ cấp tìm ra, ví dụ, trạng thái mà bộ đếm chuỗi đối với đơn vị dữ liệu gói của liên kết truyền thông an toàn được thiết lập giữa trạm di động và trạm cơ sở thứ cấp sắp kết thúc hoặc thực sự kết thúc, trạm cơ sở thứ cấp tương tự báo hiệu, trong bước 2, sự vi phạm an toàn được tìm ra tới trạm cơ sở chính. Do trong trường hợp khác, trạm cơ sở chính có thể phát hiện giống như thế sự vi phạm an toàn, báo hiệu sự vi phạm an toàn tìm được được chỉ báo theo một lựa chọn bằng đường đứt nét.

Việc báo hiệu sự vi phạm an toàn được tìm ra bởi trạm cơ sở thứ cấp tới trạm cơ sở chính có thể tương ứng với tin nhắn yêu cầu thay đổi khóa mật an toàn S-K_{eNB}, dựa vào khóa này để xác định việc truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Đáp lại sự vi phạm an toàn được tìm ra hoặc được báo hiệu, trạm cơ sở chính dẫn xuất, trong bước 3, khóa mật an toàn mới K_{eNB}*, khóa này có thể

được sử dụng để khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp.

Tuy nhiên, ở điểm này của phần mô tả, điều nên được làm rõ là, trong bước 3, khóa mật an toàn được dẫn xuất K_{eNB}* mới chỉ được duy trì trong trạm cơ sở chính và trạm di động để dẫn xuất khóa mật an toàn mới S-K_{eNB} để truyền thông giữa thiết bị đầu cuối di động và trạm cơ sở thứ cấp (xem các bước 9, 10 và 13). Theo đó, cũng khóa mật an toàn K_{eNB} "cũ" được duy trì trong trạm di động và trạm cơ sở chính cho việc truyền thông giữa chúng (ví dụ, để mật mã hóa truyền thông giữa trạm di động và trạm cơ sở chính).

Sau đó, trạm cơ sở chính, trong bước 4, tạo ra tin nhắn cấu hình lại bao gồm mệnh lệnh chuyển giao để truyền thông giữa trạm di động và trạm cơ sở chính. Như một phần của mệnh lệnh chuyển giao, thông tin được bao gồm trong đó cho phép (xem bước 5) trạm di động dẫn xuất khóa mật an toàn tương tự mới K_{eNB}*, khóa này có thể được sử dụng cho việc truyền thông giữa chúng và trạm cơ sở chính. Tin nhắn cấu hình lại này bao gồm mệnh lênh chuyển giao được truyền bởi trạm cơ sở chính tới trạm di động.

Trong việc thực hiện phương án này, tin nhắn cấu hình lại là tin nhắn cấu hình lại kết nối RRC bao gồm, như là mệnh lệnh chuyển giao, thông tin điều khiển di động có tên gọi là "mobilityControlInfo". Thông tin điều khiển di động bao gồm, ví dụ, bộ đếm chuỗi nhảy tiếp theo (Next hop Chaining Counter – NCC), trên cơ sở bộ đếm này trạm di động, ngay khi việc nhận tin nhắn cấu hình lại kết nối RRC có khả năng dẫn xuất giống khóa mật an toàn mới K_{eNB}* tương tự cho việc truyền thông giữa chúng và trạm cơ sở chính.

Hơn nữa, trong việc thực hiện phương án này, thông tin điều khiển di động, là mệnh lệnh chuyển giao có trong tin nhắn cấu hình lại kết nối RRC, bao gồm thêm mã dẫn đầu RACH chuyên dụng. Với mục đích minh họa, mã dẫn đầu RACH chuyên dụng có tên gọi là mã dẫn đầu - Y RACH.

Trong ngữ cảnh của sáng chế, việc tiếp nhận tin nhắn cấu hình lại này bởi trạm di động có thể được hiểu như là việc kích hoạt trạm di động dẫn xuất khóa mật an toàn K_{eNB}* để truyền thông giữa trạm di động và trạm cơ sở chính.

Trong khía cạnh này, trạm di động dẫn xuất, trong bước 5, khóa mật an toàn mới K_{eNB}* để truyền thông với trạm cơ sở chính trên cơ sở NCC có trong mệnh lệnh chuyển giao được truyền như một phần của tin nhắn cấu hình lại. Khóa mật an toàn K_{eNB}* này, được dẫn xuất bởi trạm di động, giống như khóa mật an toàn K_{eNB}* được dẫn xuất trong bước 4 bởi trạm cơ sở chính và được truyền trong bước 5 tới trạm cơ sở thứ cấp.

Tương tự như trên, tại điểm mô tả này cũng được làm rõ rằng, trong bước 5, khóa mật an toàn được dẫn xuất K_{eNB}* mới chỉ được duy trì trong trạm di động và trạm cơ sở chính để dẫn xuất khóa mật an toàn mới S-K_{eNB} để truyền thông giữa thiết bị đầu cuối di động và trạm cơ sở thứ cấp (xem các bước 9, 10 và 13). Theo đó, cũng khóa mật an toàn K_{eNB} cũ được duy trì trong trạm di động và trạm cơ sở chính cho việc truyền thông giữa chúng (ví dụ, để mật mã hóa truyền thông giữa trạm di động và trạm cơ sở chính).

Hơn nữa, điều quan trọng cần lưu ý rằng việc tiếp nhận tin nhắn cấu hình lại này bởi trạm di động không kích hoạt trạm di động để thực hiện trên cơ sở khóa mật an toàn được dẫn xuất K_{eNB}* mới khởi chạy lại truyền thông với trạm cơ sở chính. Theo đó, trạm di động không lấy khóa mật an toàn được dẫn xuất K_{eNB}* mới như K_{eNB} và không sử dụng khóa mật an toàn được dẫn xuất K_{eNB}* này (hoặc K_{eNB}) để khởi chạy lại truyền thông với trạm cơ sở chính. Với mục đích minh họa, hoạt động giả định của việc dùng khóa mật an toàn được dẫn xuất K_{eNB}* như là K_{eNB} và sử dụng chúng để khởi chạy lại truyền thông được gạch chéo, do đó chỉ báo rằng hoạt động này không được thực hiện bởi trạm di động.

Do đó, về phần thực hiện, trạm cơ sở chính không thực hiện bất kỳ hoạt động nào sau đây, cụ thể là việc thiết lập lại lớp con PDCP, việc thiết lập lại lớp

con RCL hoặc cài đặt lại lớp MAC đối với việc truyền thông giữa chúng và trạm cơ sở chính.

Điểm mới của việc thực hiện phương án này là tin nhắn cấu hình lại trong bước 4, là tin nhắn cấu hình lại kết nối RRC, bao gồm mã dẫn đầu - X RACH chuyên dụng, mã dẫn đầu - X RACH chuyên dụng này sau đó được sử dụng lại để thực hiện, trong bước 6, thủ tục RACH giữa trạm di động và trạm cơ sở thứ cấp.

Cũng trong trường hợp này, điều quan trọng cần lưu ý rằng thủ tục RACH giữa trạm di động và trạm cơ sở chính chỉ cập nhật định thời trước cho việc truyền thông giữa chúng mà không thể được hiểu như là việc kích hoạt trạm cơ sở chính để thực hiện khởi chạy lại truyền thông với trạm di động. Với mục đích minh họa, hoạt động giả định của việc dùng khóa mật an toàn được dẫn xuất K_{eNB}* như là K_{eNB} và sử dụng chúng để khởi chạy lại truyền thông được gạch chéo, do đó chỉ báo rằng hoạt động này không được thực hiện bởi trạm cơ sở chính.

Do đó, về phần thực hiện, trạm cơ sở chính không thực hiện bất kỳ hoạt động nào sau đây, cụ thể là việc thiết lập lại lớp con PDCP, việc thiết lập lại lớp con RCL hoặc cài đặt lại lớp MAC đối với truyền thông giữa chúng và trạm cơ sở chính.

Sau đó, trạm di động truyền, trong bước 7, tin nhắn cấu hình lại hoàn chỉnh tới trạm cơ sở chính. Trong việc thực hiện phương án này, đáp lại tin nhắn cấu hình lại, là tin nhắn cấu hình lại kết nối RRC trong bước 4, tin nhắn cấu hình lại hoàn chỉnh là tin nhắn cấu hình lại hoàn chỉnh kết nối RRC trong bước 7.

Một cách thuận lợi, tin nhắn cấu hình lại hoàn chỉnh, được truyền bởi trạm di động tới trạm cơ sở chính, có thể được hiểu, trong ngữ cảnh của sáng chế, như là việc kích hoạt trạm cơ sở chính để điều khiển trạm di động và trạm cơ sở thứ cấp thực hiện khởi chạy lại truyền thông giữa chúng, bao gồm dẫn xuất khóa mật an toàn tương tự S-K_{eNB} trên cơ sở bộ đếm độ mới được gia số để thiết lập

liên kết truyền thông an toàn bằng cách sử dụng khóa mật an toàn tương tự, được dẫn xuất S-K_{eNB}.

Trong khía cạnh này, trạm cơ sở chính gia số, trong bước 8, bộ đếm độ mới được duy trì để truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Bộ đếm độ mới này khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp trong đó cho phép bắt buộc có sự an toàn truy cập mạng giữa chúng.

Trong khía cạnh này, trạm cơ sở chính, trong bước 9, dẫn xuất trên cơ sở bộ đếm độ mới được gia số khóa mật an toàn mới S-K_{eNB} để truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Như được phân tích trong phần mô tả trên đây, dẫn xuất khóa mật an toàn S-K_{eNB} không chỉ dựa trên bộ đếm độ mới được gia số mà còn dựa trên khóa mật an toàn K_{eNB}*. Lưu ý rằng, trong phương án này, khóa mật an toàn được dẫn xuất mới K_{eNB}* được sử dụng bởi trạm cơ sở chính trong bước 8 thay vì khóa mật an toàn "cũ" K_{eNB} mà cả hai được duy trì trong trạm di động và trạm cơ sở chính như được phân tích trên đây.

Cụ thể là, trong bước 3 và bước 5, khóa mật an toàn được dẫn xuất mới K_{eNB}* chỉ được duy trì trong trạm di động và trạm cơ sở chính để dẫn xuất khóa mật an toàn mới S-K_{eNB} cho việc truyền thông giữa thiết bị đầu cuối di động và trạm cơ sở thứ cấp (xem các bước 9, 10 và 13) trong đó khóa mật an toàn "cũ" K_{eNB} được duy trì trong trạm di động và trạm cơ sở chính cho việc truyền thông giữa chúng (ví dụ, để mật mã hóa truyền thông giữa trạm di động và trạm cơ sở chính).

Sau khi dẫn xuất khóa mật an toàn mới S-K_{eNB} để truyền thông giữa trạm di động và trạm cơ sở thứ cấp, trạm cơ sở chính truyền, trong bước 10, khóa mật an toàn được dẫn xuất mới S-K_{eNB} này và độ mới được gia số tới trạm cơ sở thứ cấp. Về phần thực hiện, việc truyền khóa mật an toàn được dẫn xuất mới S-K_{eNB} và bộ đếm độ mới được gia số có thể được hỗ trợ thông qua việc lợi dụng giao diện X2.

Sau đó, trạm cơ sở thứ cấp tạo ra, trong bước 11, tin nhắn cấu hình lại bao gồm bộ đếm độ mới được gia số để khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Trạm cơ sở thứ cấp sau đó truyền tin nhắn giống như vậy tới trạm cơ sở chính. Về phần thực hiện, việc truyền tin nhắn cấu hình lại có thể được hỗ trợ thông qua việc lợi dụng giao diện X2.

Trong việc thực hiện phương án này, tin nhắn cấu hình lại của bước 11 là tin nhắn cấu hình lại kết nối RRC và bao gồm thông tin bổ sung thông thường có trong tin nhắn. Cụ thể là, tin nhắn cấu hình lại kết nối RRC bổ sung bao gồm mã dẫn đầu kênh truy nhập ngẫu nhiên chuyên dụng - RACH. Với mục đích minh họa, mã dẫn đầu RACH chuyên dụng có tên gọi là mã dẫn đầu - Y RACH.

Tin nhắn cấu hình lại, được tạo ra bởi trạm cơ sở thứ cấp, sau đó được chuyển tiếp, trong bước 12, bởi trạm cơ sở chính tới trạm di động. Ngay cả khi tin nhắn cấu hình lại nhận được từ trạm cơ sở chính, trạm di động có thể nhận ra từ nội dung của nó rằng nó được tạo ra, bởi và do đó, được kết nối với (nghĩa là, liên quan đến) truyền thông với trạm cơ sở thứ cấp và không truyền thông với trạm cơ sở chính.

Người đọc có trình độ trung bình trong lĩnh vực kỹ thuật có thể dễ dàng lý giải từ phân tích trên đây, rằng tin nhắn cấu hình lại được chuyển tiếp bởi trạm cơ sở chính tới trạm di động được mật mã hóa bởi trạm cơ sở chính bằng cách sử dụng khóa mật an toàn cũ K_{eNB} để truyền thông giữa chúng với nhau. Trong khía cạnh này, sự an toàn có thể là bắt buộc cho việc truyền của bộ đếm độ mới được gia số mà không làm phức tạp thêm việc thực hiện, đơn giản là do thực tế rằng phương án này bỏ qua sự cần thiết đối với việc khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở chính.

Trong ngữ cảnh của sáng chế, việc tiếp nhận tin nhắn cấu hình lại này bởi trạm di động có thể được hiểu như là việc kích hoạt trạm di động để thực hiện khởi chạy lại truyền thông với trạm cơ sở thứ cấp.

Theo đó, trạm di động dẫn xuất, trong bước 13, khóa mật an toàn S-K_{eNB} để truyền thông với trạm cơ sở thứ cấp trên cơ sở bộ đếm độ mới có trong tin nhắn cấu hình lại được chuyển tiếp. Khóa mật an toàn S-K_{eNB} này, được dẫn xuất bởi trạm di động, giống như khóa mật an toàn S-K_{eNB} dẫn xuất trong bước 4 bởi trạm cơ sở chính và được truyền trong bước 5 tới trạm cơ sở thứ cấp.

Như được phân tích trong phần mô tả trên đây, dẫn xuất khóa mật an toàn S-K_{eNB} không chỉ dựa trên bộ đếm độ mới được gia số mà còn dựa trên khóa mật an toàn K_{eNB}*. Lưu ý rằng, trong phương án này, khóa mật an toàn được dẫn xuất mới K_{eNB}* được sử dụng bởi trạm di động trong bước 13 thay vì khóa mật an toàn "cũ" K_{eNB} mà cả hai được duy trì trong trạm di động và trạm cơ sở chính như được phân tích trên đây.

Do đó, do cả hai, trạm di động và trạm cơ sở thứ cấp được cung cấp với khóa mật an toàn tương tự, được dẫn xuất S-K_{eNB}, liên kết truyền thông an toàn có thể được thiết lập trên cơ sở khóa mật an toàn S-K_{eNB} này giữa trạm di động và trạm cơ sở thứ cấp.

Trong sự biến đổi của bước 13, trạm di động trước hết xác định liệu bộ đếm độ mới được gia số, có trong tin nhắn cấu hình lại được truyền, có khác biệt với bộ đếm độ mới trước đây có trong tin nhắn cấu hình lại được truyền trước đây hay không, và chỉ trong trường hợp khác biệt, bộ đếm độ mới được gia số, trạm di động dẫn xuất khóa mật an toàn tương tự S- K_{eNB}.

Sau đó, trạm di động khởi chạy lại, trong bước 14, truyền thông với trạm cơ sở thứ cấp trên cơ sở khóa mật an toàn tương tự, được dẫn xuất (xem bước 13) để truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Về phía thực hiện, sự khởi chạy lại được thực hiện bởi trạm di động có thể bao gồm việc thiết lập lại lớp con PDCP, việc thiết lập lại lớp con RCL và cài đặt lại lớp MAC.

Điểm mới của việc thực hiện phương án này là, tin nhắn cấu hình lại, là tin nhắn cấu hình lại kết nối RRC, bao gồm mã dẫn đầu - Y RACH chuyên dụng,

mã này sau đó được sử dụng lại để thực hiện, trong bước 15, thủ tục RACH giữa trạm di động và trạm cơ sở thứ cấp.

Một cách thuận lợi, thủ tục RACH giữa trạm di động và trạm cơ sở thứ cấp không chỉ cập nhật định thời trước cho việc truyền thông giữa chúng mà còn có thể được hiểu, trong ngữ cảnh của sáng chế, như là việc kích hoạt trạm cơ sở thứ cấp thực hiện khởi chạy lại truyền thông với trạm di động.

Trong khía cạnh này, trạm cơ sở thứ cấp khởi chạy lại, trong bước 16, truyền thông với trạm di động trên cơ sở khóa mật an toàn tương tự, được dẫn xuất (xem bước 4 và 5) để truyền thông giữa trạm di động và trạm cơ sở thứ cấp. Về phía thực hiện, sự khởi chạy lại được thực hiện bởi trạm di động có thể bao gồm việc thiết lập lại lớp con PDCP, việc thiết lập lại lớp con RCL và cài đặt lại lớp MAC.

Sau đó, trạm di động truyền, trong bước 17, tin nhắn cấu hình lại hoàn chỉnh tới trạm cơ sở chính, trong bước 18, được chuyển tiếp bởi trạm cơ sở chính tới trạm cơ sở thứ cấp. Cụ thể là, trong phương án này, tin nhắn cấu hình lại hoàn chỉnh được truyền bởi trạm di động sau khi trạm di động và trạm cơ sở thứ cấp cả hai đều khởi chạy lại truyền thông giữa chúng.

Điều này có thể đạt được, ví dụ, bởi trạm di động trì hoãn việc truyền tin nhắn cấu hình lại hoàn chỉnh đến trạm cơ sở chính với khoảng thời gian được xác định trước. Ngoài ra, trạm di động cũng có thể giả định rằng trạm cơ sở thứ cấp khởi chạy lại trong bước 16 kết nối của nó nhanh hơn việc truyền và chuyển tiếp tin nhắn cấu hình lại hoàn chỉnh trong bước 17 and 18 và có thể truyền ngay lập tức tin nhắn tương tự sau khi hoàn thành thủ tục RACH trong bước 15.

Người đọc có trình độ trung bình trong lĩnh vực kỹ thuật có thể dễ dàng lý giải từ phân tích trên đây, rằng tin nhắn cấu hình lại hoàn chỉnh, được chuyển tiếp bởi trạm di động tới trạm cơ sở chính, được mật mã hóa bởi trạm di động bằng cách sử dụng khóa mật an toàn cũ K_{eNB} để truyền thông giữa chúng. Trong khía cạnh này, sự an toàn cũng có thể là bắt buộc cho việc truyền tin nhắn cấu

hình lại hoàn chỉnh này. Về phần thực hiện, việc truyền tin nhắn cấu hình lại hoàn chỉnh giữa trạm cơ sở trong bước 13 có thể được hỗ trợ thông qua giao diện X2.

Điểm mới nữa của việc thực hiện phương án này là, đáp lại tin nhắn cấu hình lại, là tin nhắn cấu hình lại kết nối RRC, tin nhắn cấu hình lại hoàn chỉnh là tin nhắn cấu hình lại hoàn chỉnh kết nối RRC.

Do đó, sau khi khởi chạy lại truyền thông trong bước 14 và 16, trạm di động và trạm cơ sở thứ cấp có khả năng thiết lập liên kết truyền thông an toàn giữa chúng với nhau bằng cách lợi dụng khóa mật an toàn tương tự, được dẫn xuất $S\text{-}K_{eNB}$.

Một cách thuận lợi, cũng trong phương án này truyền thông giữa trạm di động và trạm cơ sở thứ cấp được khởi chạy lại mà không cần có sự khởi chạy lại truyền thông giữa trạm di động và trạm cơ sở chính. Nói cách khác, để truyền thông giữa trạm di động và trạm cơ sở thứ cấp khóa mật an toàn $S\text{-}K_{eNB}$ giống như vậy được dẫn xuất, khóa này dựa trên bộ đếm độ mới được gia số, do đó khác biệt và do đó cho phép thiết lập liên kết truyền thông an toàn giữa chúng mà không yêu cầu khởi chạy lại truyền thông với trạm cơ sở chính.

Nói tóm lại, bốn ví dụ được phân tích trên đây đưa ra đối với chuyển giao intra-khu thông thường có những lợi ích như sau. Thứ nhất, liên kết truyền thông an toàn được thiết lập (nghĩa là, tải mang vô tuyến) được thiết lập trong nhóm khu to, MCG, sẽ không bị gián đoạn khi không cần thiết. Thứ hai, thời gian để thiết lập liên kết truyền thông an toàn trong trường hợp sự vi phạm an toàn tiềm năng được phát hiện bao gồm dẫn xuất (nghĩa là, làm mới) khóa mật an toàn mới $S\text{-}K_{eNB}$ sẽ nhanh hơn do dẫn xuất khóa mật an toàn $S\text{-}K_{eNB}$ sẽ không còn phụ thuộc vào việc hoàn thành chuyển giao intra-khu. Cuối cùng, hành vi/việc thực hiện đối với UE đặc thù không yêu cầu đến: trong tình trạng kỹ thuật UE/ mạng giải phóng nhóm khu thứ cấp, SCG, trong quá trình chuyển giao M_{eNB} - S_{eNB}, việc chuyển giao này cũng bao gồm chuyển giao intra-khu. Để có thể sử

dụng chuyển giao intra-khu để bắt buộc sự an toàn truy cập mạng, việc giải phóng SCG không thực hiện để làm mới S-K_{eNB} mà tự nó là một hành vi mới để chuyển giao intra-khu được biết đến một cách thông thường.

Trong Fig. 16, chuyển giao intra-khu cho việc thay đổi K_{eNB} của bước 4- 7 và thủ tục dẫn xuất S-K_{eNB} trong bước 8- 18 là hai thủ tục riêng biệt. Theo sự biến đổi của ví dụ thứ tư được mô tả trên đây của phương án chi tiết hơn, hai thủ tục được kết hợp dẫn đến UE dẫn xuất K_{eNB} và S- K_{eNB} từ K_{eNB} mới ở cùng thời điểm, cụ thể là sau khi nhận được mệnh lệnh chuyển giao intra-khu được gọi là thông tin điều khiển di động và có trong tin nhắn cấu hình lại kết nối RRC trong bước 4.

Sự biến đổi này được làm rõ dựa trên các tham số đầu vào nào UE quyết định dẫn xuất (lại) S- K_{eNB}. Trong khía cạnh này, cần lưu ý rằng tự mỗi bộ đếm chuỗi nhảy tiếp theo NCC là không đủ. Do đó, có đề xuất để cung cấp bổ sung tham số độ mới được gia số. Ngay khi dò tìm ra tham số độ mới được gia số, UE khi đó dẫn xuất (lại) S-K_{eNB} từ K_{eNB} và tham số độ mới được gia số. Trong phiên bản được đơn giản hóa khác của biến thể này, UE làm mới/dẫn xuất lại S-K_{eNB} bất cứ khi nào tham số độ mới được gửi/được chỉ báo bằng mạng mà không cần UE kiểm ra liệu các tham số độ mới nhận được có gia số so với bộ đếm độ mới nhận được trước đây hay không (nghĩa là, tham số độ mới cuối cùng được lưu trữ bởi UE, và được sử dụng cho dẫn xuất S- K_{eNB} một cách thành công). Nói tóm lại, ở đây dẫn xuất S-K_{eNB} luôn dựa trên K_{eNB} dẫn xuất gần đây nhất và tham số độ mới nhận được gần đây nhất.

Việc thực hiện phần cứng và phần mềm theo sáng chế

Phương án khác của sáng chế đề cập đến việc thực hiện các phương án khác nhau được mô tả trên đây bằng cách sử dụng phần cứng và phần mềm, hoặc chỉ phần cứng. Trong việc kết nối này, sáng chế cung cấp thiết bị người dùng (thiết bị đầu cuối di động) và eNodeB chính và thứ cấp (trạm cơ sở). Thiết

bị người dùng và trạm cơ sở được làm thích ứng để thực hiện các phương án được mô tả ở đây.

Điều còn được thừa nhận rằng các phương án khác nhau của sáng chế có thể được thi hành hoặc thực hiện bằng cách sử dụng các thiết bị máy tính (bộ xử lý). Thiết bị máy tính hoặc bộ xử lý ví dụ có thể là bộ xử lý đa năng, bộ xử lý tín hiệu số (DSP), vi mạch tích hợp đặc dụng (ASIC), mảng cổng lập trình được dạng trường (FPGA) hoặc thiết bị lô gic lập trình được khác, v.v... Ngoài ra, máy phát radio và máy thu radio và phần cứng cần thiết khác có thể được cung cấp trong các thiết bị (UE, MeNB, SeNB). Các phương án khác nhau của sáng chế có thể cũng được thực hiện hoặc thực thi bởi việc kết hợp các thiết bị này.

Hơn nữa, các phương án khác nhau của sáng chế cũng có thể được thực hiện bởi các mô đun phần mềm, các mô đun này được thực hiện bởi bộ xử lý hoặc một cách trực tiếp trong phần cứng. Ngoài ra, cũng có thể thực hiện việc kết hợp các mô đun phần mềm và phần cứng. Mô đun phần mềm có thể được lưu ở phương tiện lưu giữ bất kỳ có thể đọc được bằng máy tính, ví dụ RAM, EPROM, EEPROM, bộ nhớ flash, bộ ghi, đĩa cứng, CD-ROM, DVD, v.v.

Cần lưu ý thêm nữa rằng các dấu hiệu riêng của các phương án khác nhau theo sáng chế có thể là riêng rẽ hoặc sự kết hợp tùy ý để làm sáng chế khác.

Người có trình độ trung bình trong lĩnh vực kỹ thuật có thể lý giải rằng nhiều biến thể và/hoặc cải biến có thể được thực hiện cho sáng chế như được thể hiện trong các phương án cụ thể mà không trệch khỏi phạm vi của sáng chế như được mô tả một cách khái quát. Các phương án này, do đó, được xem xét trong tất cả các khía cạnh được minh họa và không bị hạn chế.

YÊU CẦU BẢO HỘ

1. Thiết bị trạm cơ sở thứ cấp bao gồm:

máy phát, khi hoạt động, truyền yêu cầu thay đổi của khóa mật an toàn thứ cấp tới trạm cơ sở chính khi giá trị COUNT vượt quá giá trị ngưỡng,

trong đó khóa mật an toàn thứ cấp là khóa mật an toàn cho thiết bị trạm cơ sở thứ cấp;

máy thu, khi hoạt động, nhận từ trạm cơ sở chính khóa mật an toàn thứ cấp được cập nhật, khóa mật an toàn thứ cấp được cập nhật được dẫn xuất ở trạm cơ sở chính bằng cách sử dụng bộ đếm độ mới được gia số và khóa mật an toàn đang hoạt động của trạm cơ sở chính, mà không cần làm mới khóa mật an toàn đang hoạt động của trạm cơ sở chính; và

mạch điện điều khiển, khi hoạt động, tính khóa mật mã hóa mới cho việc truyền thông với thiết bị đầu cuối di động bằng cách sử dụng khóa mật an toàn thứ cấp được cập nhật.

2. Thiết bị trạm cơ sở thứ cấp theo điểm 1, trong đó COUNT bao gồm số chuỗi giao thức hội tụ dữ liệu gói (PDCP) và số khung siêu (HFN) được chia sẻ giữa trạm cơ sở thứ cấp và thiết bị đầu cuối di động.

3. Thiết bị trạm cơ sở thứ cấp theo điểm 1, trong đó mạch điện điều khiển, khi hoạt động, thiết lập lại liên kết truyền thông với thiết bị đầu cuối di động bằng cách sử dụng khóa mật an toàn thứ cấp được cập nhật.

4. Thiết bị trạm cơ sở thứ cấp theo điểm 1, trong đó tin nhắn cấu hình lại kết nối RRC được truyền từ trạm cơ sở hoặc trạm cơ sở chính tới thiết bị đầu cuối di động sau khi trạm cơ sở chính truyền khóa mật an toàn thứ cấp được cập nhật.

5. Thiết bị trạm cơ sở thứ cấp theo điểm 1, trong đó bộ đếm độ mới là giá trị đếm để làm mới khóa mật an toàn thứ cấp.

6. Phương pháp truyền thông cho thiết bị trạm cơ sở thứ cấp, phương pháp truyền thông này bao gồm các bước:

truyền yêu cầu thay đổi của khóa mật an toàn thứ cấp tới trạm cơ sở chính khi giá trị COUNT vượt quá giá trị ngưỡng, trong đó khóa mật an toàn thứ cấp là khóa mật an toàn cho thiết bị trạm cơ sở thứ cấp;

nhận từ trạm cơ sở chính khóa mật an toàn thứ cấp được cập nhật, khóa mật an toàn thứ cấp được cập nhật được dẫn xuất ở trạm cơ sở chính bằng cách sử dụng bộ đếm độ mới được gia số và khóa mật an toàn đang hoạt động của trạm cơ sở chính, mà không cần làm mới khóa mật an toàn đang hoạt động của trạm cơ sở chính; và

tính toán khóa mật mật mã hóa mới cho việc truyền thông với thiết bị đầu cuối di động bằng cách sử dụng khóa mật an toàn thứ cấp được cập nhật.

7. Phương pháp truyền thông theo điểm 6, trong đó COUNT bao gồm số chuỗi giao thức hội tụ dữ liệu gói (PDCP) và số khung siêu (HFN) được chia sẻ giữa trạm cơ sở thứ cấp và đầu cuối di động.

8. Phương pháp truyền thông theo điểm 6, bao gồm việc thiết lập lại liên kết truyền thông với đầu cuối di động bằng cách sử dụng khóa mật an toàn thứ cấp được cập nhật.

9. Phương pháp truyền thông theo điểm 6, trong đó tin nhắn cấu hình lại kết nối RRC được truyền từ trạm cơ sở thứ cấp hoặc trạm cơ sở chính tới thiết bị đầu cuối di động sau khi trạm chính truyền khóa mật an toàn thứ cấp được cập nhật.

10. Phương pháp truyền thông theo điểm 6, trong đó bộ đếm độ mới là giá trị đếm để làm mới của khóa mật an toàn thứ cấp.

11. Thiết bị truyền thông bao gồm:

máy thu, khi hoạt động, thu bộ đếm độ mới được gia số từ trạm cơ sở chính, bộ đếm độ mới được gia số được chuẩn bị đáp lại yêu cầu thay đổi của khóa mật an toàn thứ cấp từ trạm cơ sở thứ cấp khi giá trị COUNT vượt quá giá trị ngưỡng, trong đó khóa mật an toàn thứ cấp là khóa mật an toàn cho trạm cơ sở thứ cấp; và

mạch điện điều khiển, khi hoạt động, dẫn xuất an khóa mật an toàn thứ cấp được cập nhật bằng cách sử dụng bộ đếm độ mới được gia số nhận được và khóa mật an toàn đang hoạt động của thiết bị truyền thông, tương ứng với khóa mật an toàn đang hoạt động của trạm cơ sở chính, mà không cần làm mới khóa mật an toàn đang hoạt động của thiết bị truyền thông, và sử dụng khóa mật an toàn thứ cấp được cập nhật được dẫn xuất trong liên kết truyền thông với trạm cơ sở thứ cấp.

12. Phương pháp truyền thông bao gồm các bước:

nhận bộ đếm độ mới được gia số từ trạm cơ sở chính, bộ đếm độ mới được gia số được chuẩn bị đáp lại yêu cầu thay đổi của khóa mật an toàn thứ cấp từ trạm cơ sở thứ cấp khi giá trị COUNT vượt quá giá trị ngưỡng, trong đó khóa mật an toàn thứ cấp là khóa mật an toàn cho trạm cơ sở thứ cấp;

dẫn xuất khóa mật an toàn thứ cấp được cập nhật bằng cách sử dụng bộ đếm độ mới được gia số nhận được và khóa mật an toàn đang hoạt động của thiết bị truyền thông, tương ứng với khóa mật an toàn đang hoạt động của trạm cơ sở chính, mà không cần làm mới khóa mật an toàn đang hoạt động của thiết bị truyền thông; và

sử dụng khóa mật an toàn thứ cấp được cập nhật được dẫn xuất trong liên kết truyền thông với trạm cơ sở thứ cấp.

13. Mạch tích hợp, khi hoạt động, điều khiển quy trình của thiết bị trạm cơ sở thứ cấp, quy trình này bao gồm các công đoạn:

truyền yêu cầu thay đổi của khóa mật an toàn thứ cấp tới trạm cơ sở chính khi giá trị COUNT vượt quá giá trị ngưỡng, trong đó khóa mật an toàn thứ cấp là khóa mật an toàn cho thiết bị trạm cơ sở thứ cấp;

nhận từ trạm cơ sở chính khóa mật an toàn thứ cấp được cập nhật, khóa mật an toàn thứ cấp được cập nhật được dẫn xuất tại trạm cơ sở chính bằng cách sử dụng bộ đếm độ mới được gia số và khóa mật an toàn đang hoạt động của trạm cơ sở chính, mà không cần làm mới khóa mật an toàn đang hoạt động của trạm cơ sở chính; và

tính toán khóa mật mã hóa mới để truyền thông với đầu cuối di động bằng cách sử dụng khóa mật an toàn thứ cấp được cập nhật.

14. Mạch tích hợp, khi hoạt động, điều khiển quy trình của thiết bị truyền thông, quy trình này bao gồm các công đoạn:

nhận bộ đếm độ mới được gia số từ trạm cơ sở chính, bộ đếm độ mới được gia số được chuẩn bị đáp lại yêu cầu thay đổi của khóa mật an toàn thứ cấp từ trạm cơ sở thứ cấp khi giá trị COUNT vượt quá giá trị ngưỡng, trong đó khóa mật an toàn thứ cấp là khóa mật an toàn cho trạm cơ sở thứ cấp;

dẫn xuất khóa mật an toàn thứ cấp được cập nhật bằng cách sử dụng bộ đếm độ mới được gia số nhận được và khóa mật an toàn đang hoạt động của thiết bị truyền thông, tương ứng với khóa mật an toàn đang hoạt động của trạm cơ sở chính, mà không cần làm mới khóa mật an toàn đang hoạt động của thiết bị truyền thông; và

sử dụng khóa mật an toàn thứ cấp được cập nhật được dẫn xuất trong liên kết truyền thông với trạm cơ sở thứ cấp.

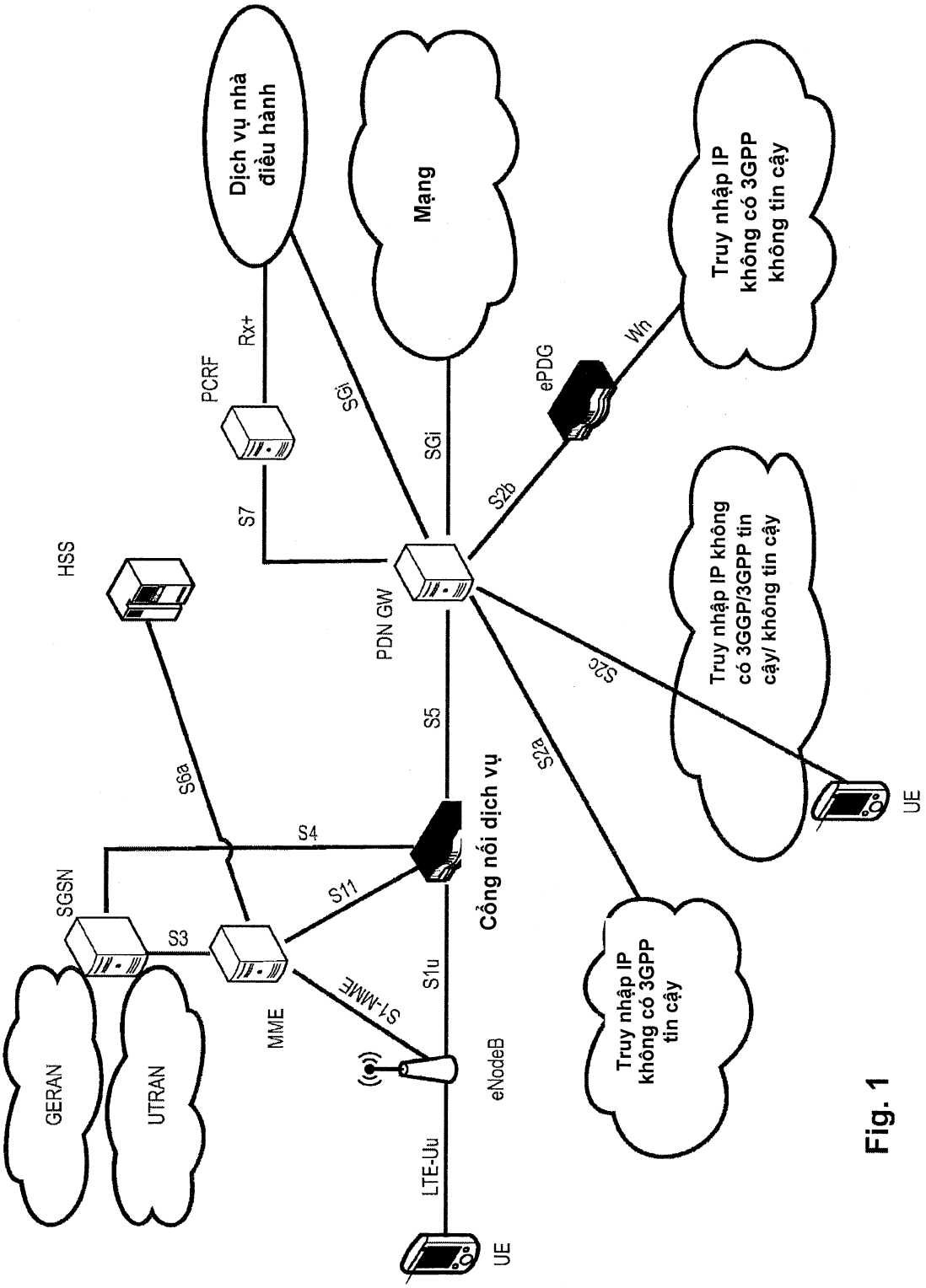

Dịch vụ nhà điều hành
Mạng
Truy nhập IP không có 3GPP không tin cậy
PCRF
Rx+
SGi
SGi
ePDG
Wn
S7
S2b
HSS
PDN GW
Truy nhập IP không có 3GGP/3GPP tin cậy/ không tin cậy
S2c
S6a
S5
S2a
S4
Cổng nối dịch vụ
UE
SGSN
S11
S3
S1u
S1-MME
MME
Truy nhập IP không có 3GPP tin cậy
GERAN
UTRAN
eNodeB
LTE-Uu
UE

Fig. 1

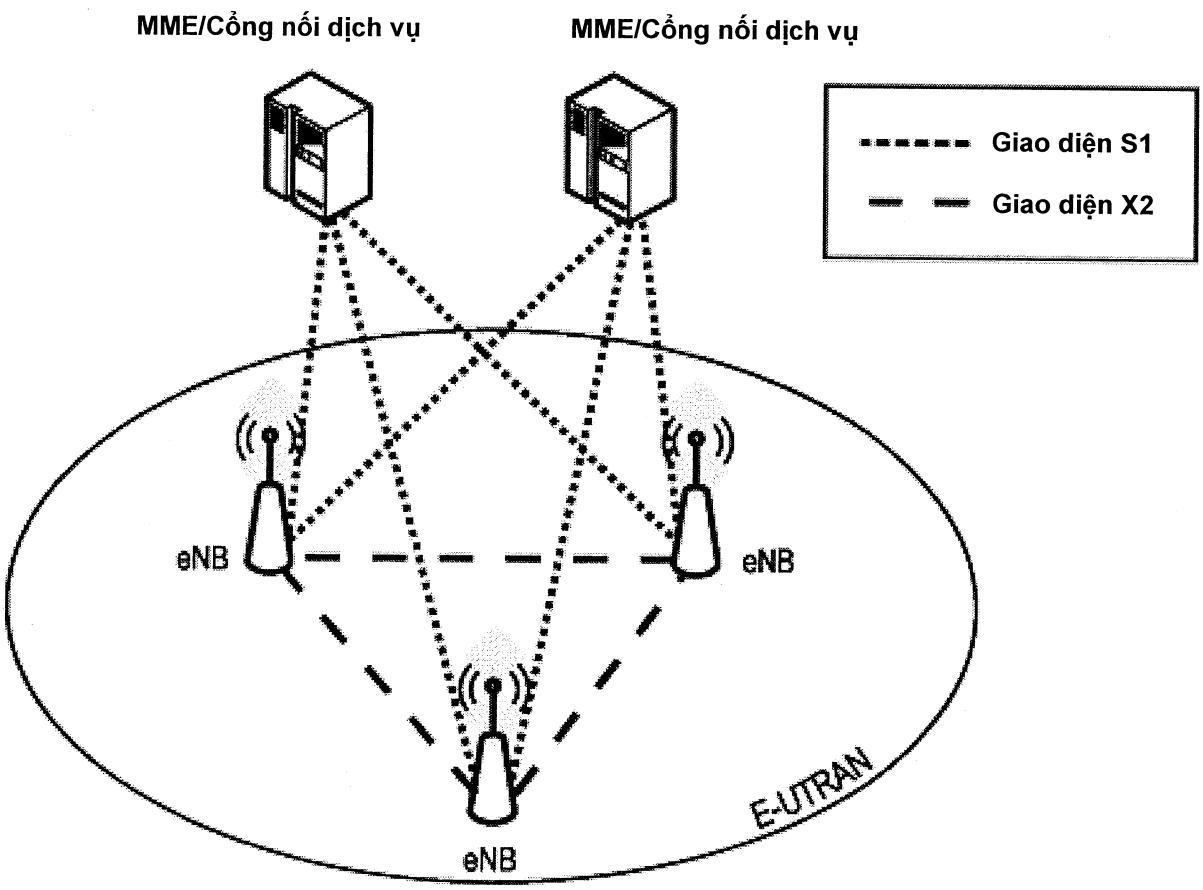

MME/Cổng nối dịch vụ
MME/Cổng nối dịch vụ
Giao diện S1
Giao diện X2
eNB
eNB
eNB
E-UTRAN

Fig. 2

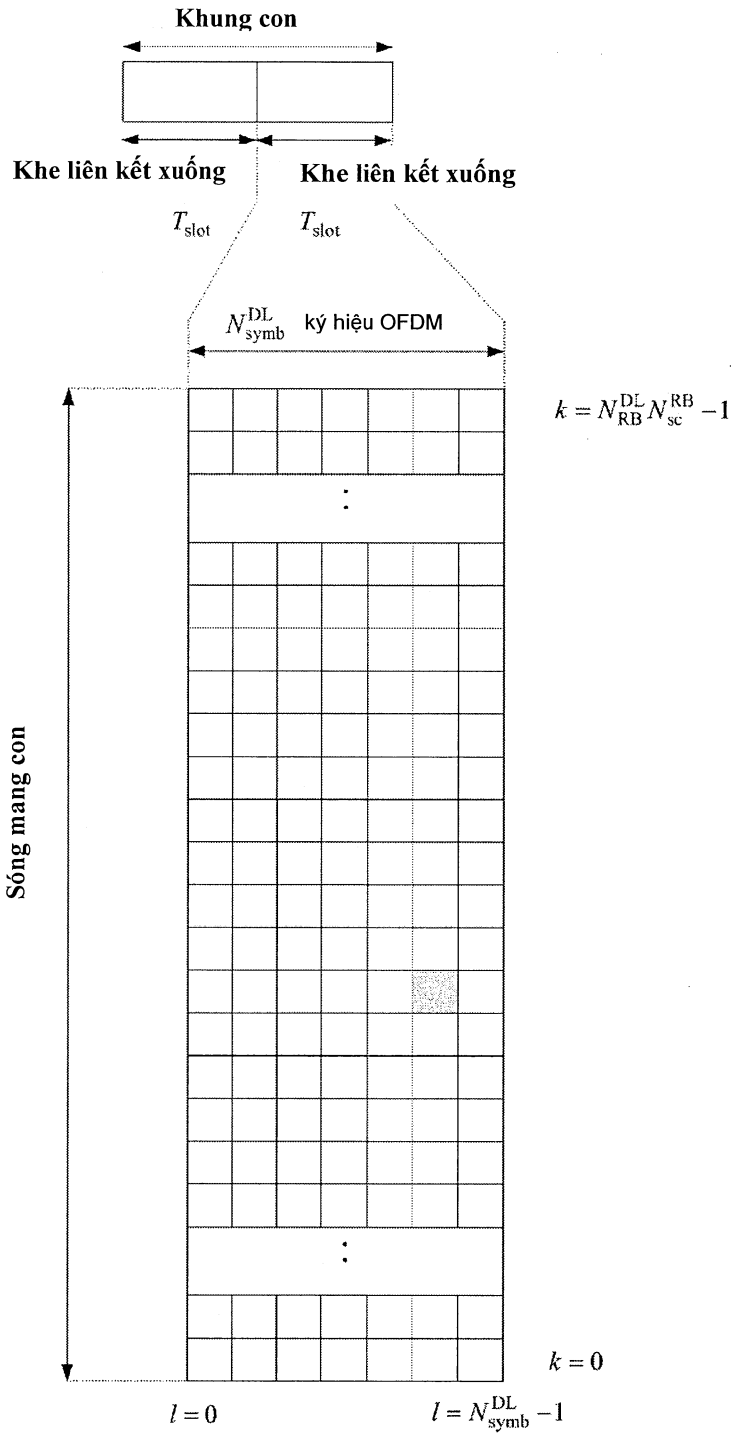

Khung con
Khe liên kết xuống
Khe liên kết xuống
T_{slot}
T_{slot}
N_{symb}^{DL} ký hiệu OFDM
$k = N_{RB}^{DL} N_{sc}^{RB} - 1$
Sóng mang con
$k = 0$
$l = 0$
$l = N_{symb}^{DL} - 1$

Fig. 3

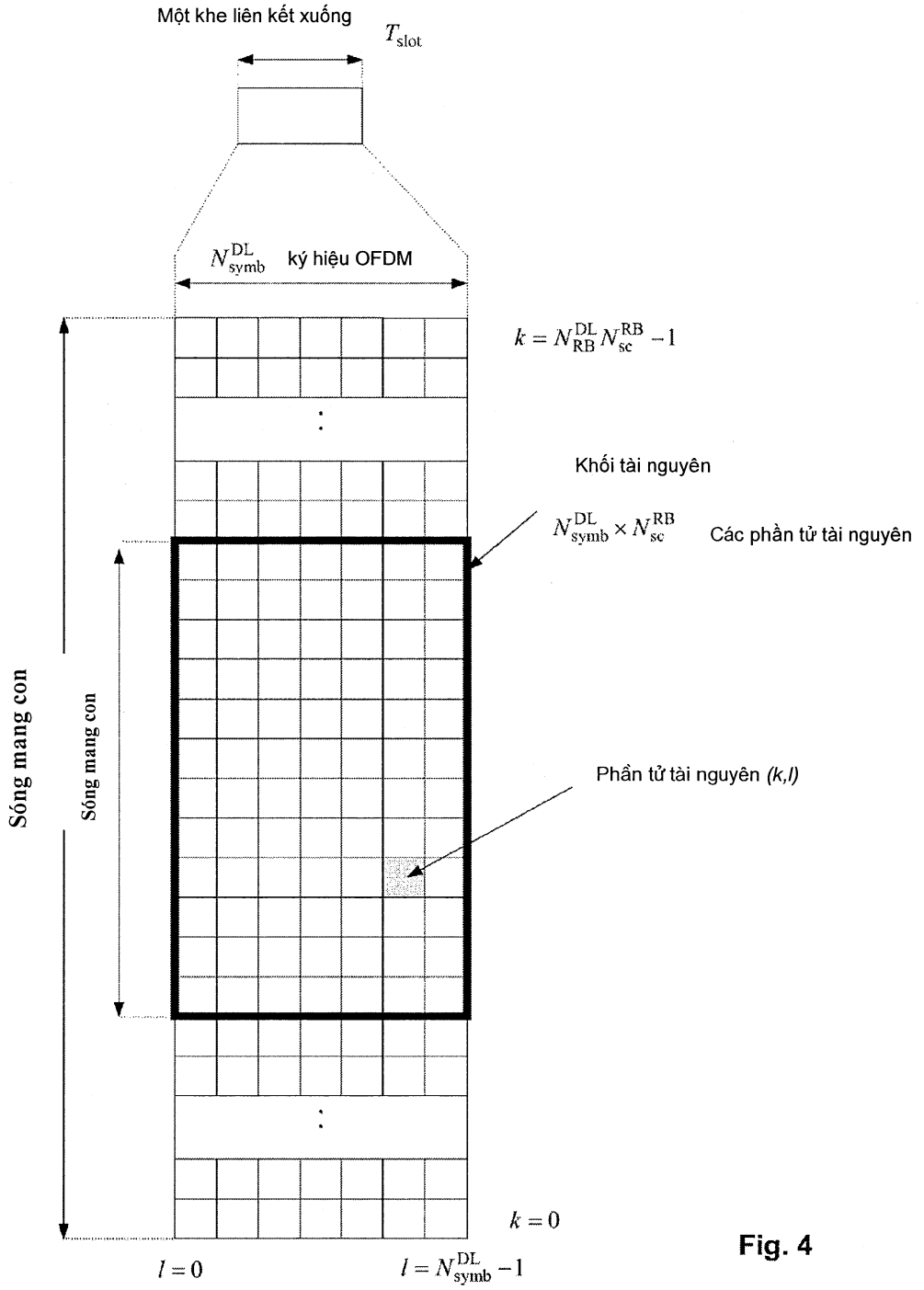

Một khe liên kết xuống
T_{slot}
N_{symb}^{DL} ký hiệu OFDM
$k = N_{RB}^{DL} N_{sc}^{RB} - 1$
Khối tài nguyên
$N_{symb}^{DL} \times N_{sc}^{RB}$ Các phần tử tài nguyên
Sóng mang con
Sóng mang con
Phần tử tài nguyên *(k,l)*
$k = 0$
$l = 0$
$l = N_{symb}^{DL} - 1$

Fig. 4

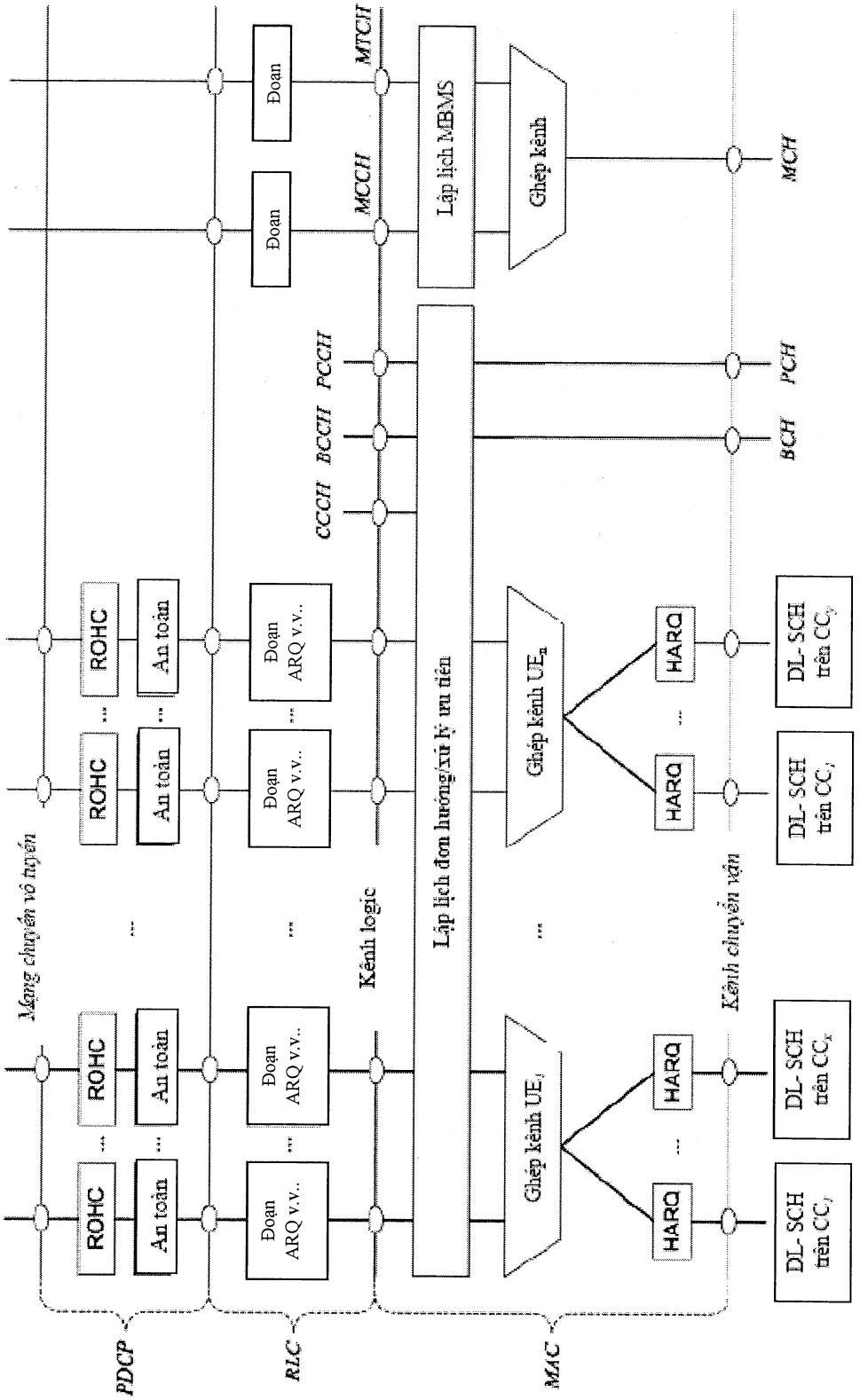

Mạng chuyển vô tuyến
ROHC
An toàn
Đoạn ARQ v.v..
Kênh logic
Lập lịch đơn hướng/xử lý ưu tiên
Ghép kênh UE$_j$
Ghép kênh UE$_n$
HARQ
DL- SCH trên CC$_j$
DL- SCH trên CC$_x$
Kênh chuyển vận
CCCH
BCCH
PCCH
MCCH
MTCH
Đoạn
Lập lịch MBMS
Ghép kênh
MCH
PCH
BCH
PDCP
RLC
MAC

Fig.5

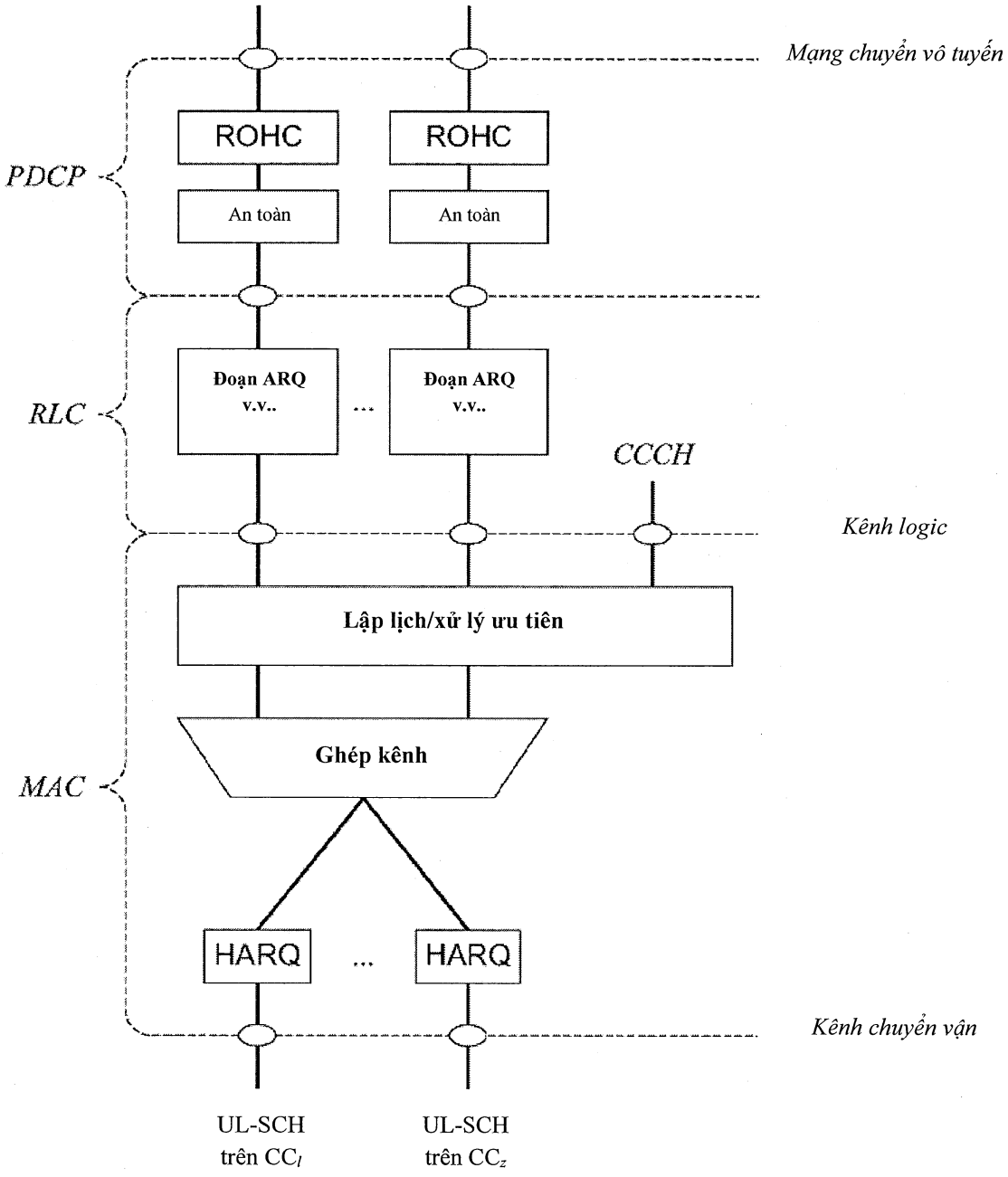

Mạng chuyển vô tuyến
PDCP
ROHC
ROHC
An toàn
An toàn
RLC
Đoạn ARQ
v.v..
...
Đoạn ARQ
v.v..
CCCH
Kênh logic
Lập lịch/xử lý ưu tiên
MAC
Ghép kênh
HARQ
...
HARQ
Kênh chuyển vận
UL-SCH
trên CC1
UL-SCH
trên CCz

Fig. 6

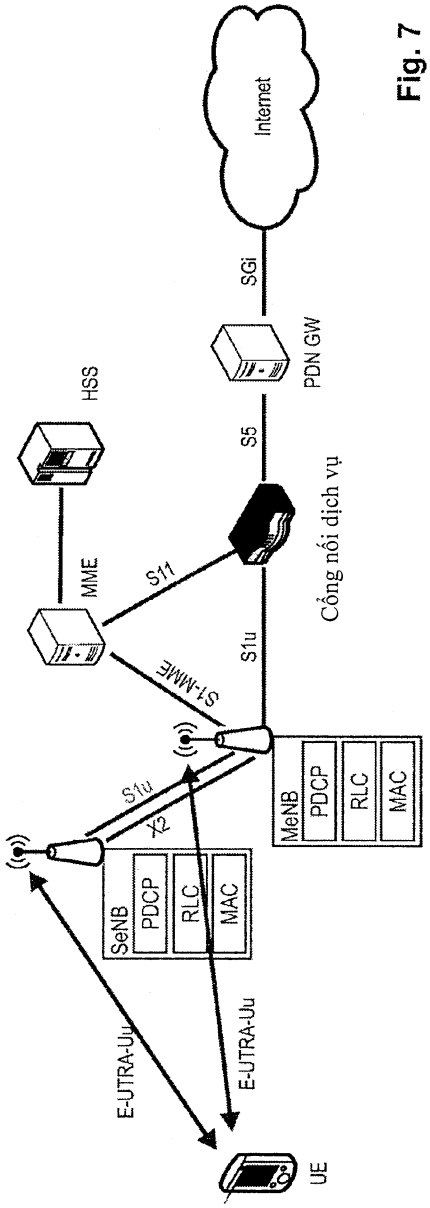

Internet
SGi
PDN GW
S5
Cổng nối dịch vụ
HSS
MME
S11
S1-MME
S1u
MeNB
PDCP
RLC
MAC
S1u
X2
SeNB
PDCP
RLC
MAC
E-UTRA-Uu
E-UTRA-Uu
UE

Fig. 7

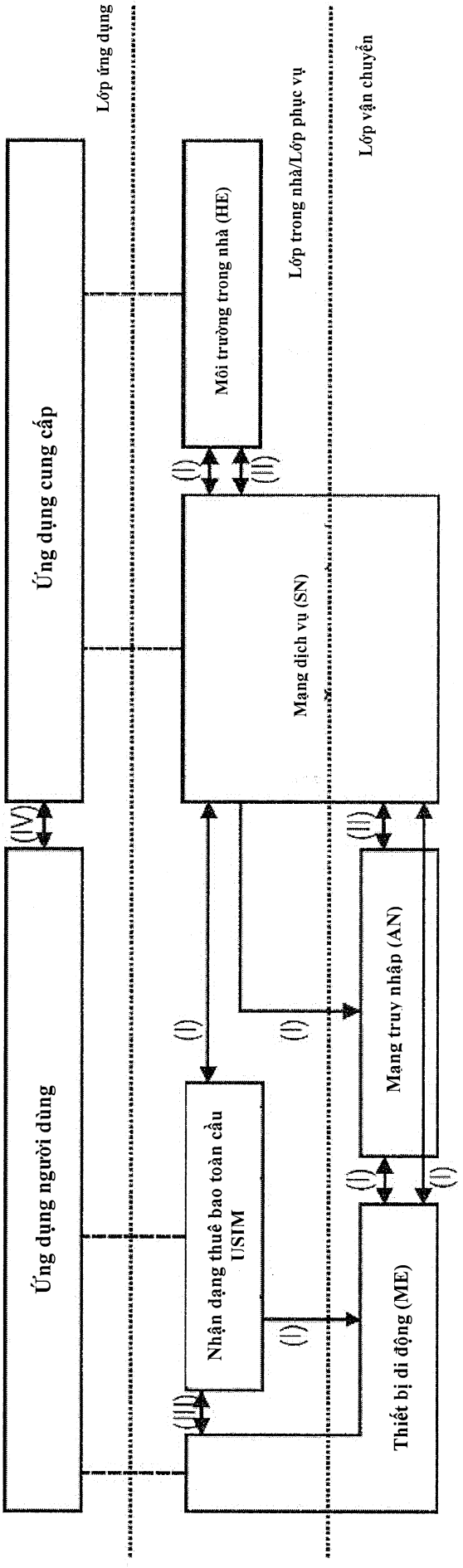

Lớp ứng dụng
Lớp trong nhà/Lớp phục vụ
Lớp vận chuyển
Ứng dụng cung cấp
Môi trường trong nhà (HE)
Mạng dịch vụ (SN)
Ứng dụng người dùng
Nhận dạng thuê bao toàn cầu USIM
Mạng truy nhập (AN)
Thiết bị di động (ME)
(I)
(II)
(III)
(IV)

Fig. 8

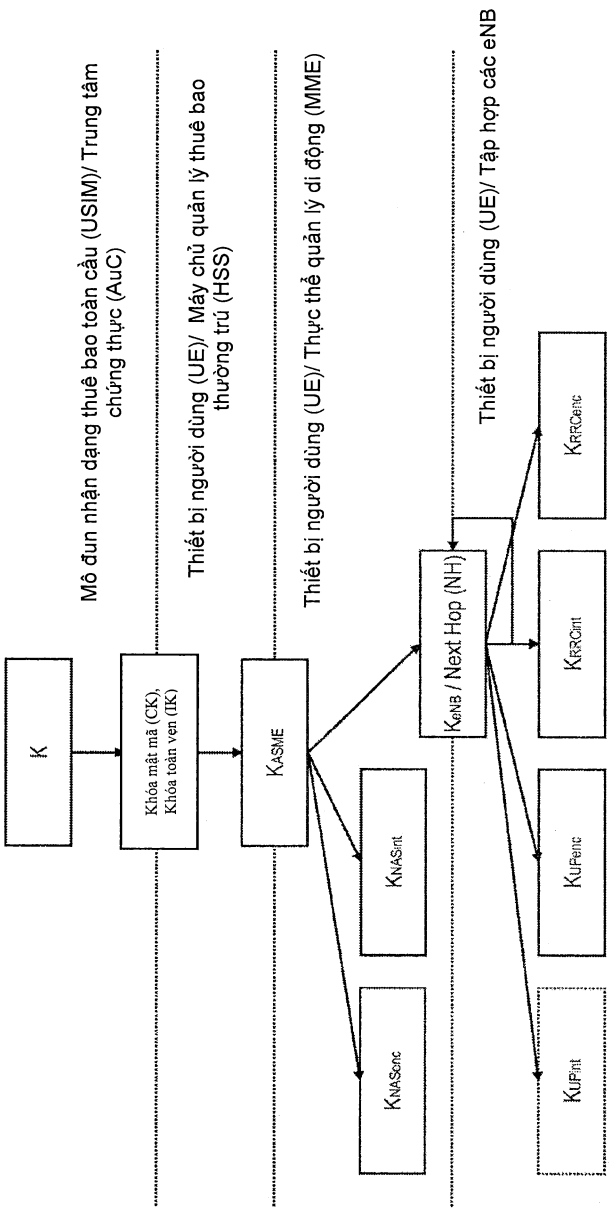

K
Khóa mật mã (CK), Khóa toàn vẹn (IK)
KASME
KNASint
KNASenc
KeNB / Next Hop (NH)
KRRCenc
KRRCint
KUPenc
KUPint
Mô đun nhận dạng thuê bao toàn cầu (USIM)/ Trung tâm chứng thực (AuC)
Thiết bị người dùng (UE)/ Máy chủ quản lý thuê bao thường trú (HSS)
Thiết bị người dùng (UE)/ Thực thể quản lý di động (MME)
Thiết bị người dùng (UE)/ Tập hợp các eNB

Fig. 9

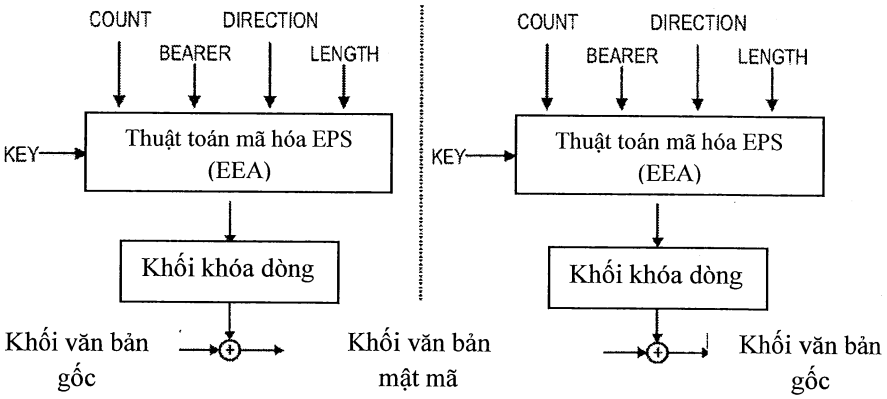


Fig. 10

Số khung siêu (HFN)	Số thứ tự PCDP (SN)

Fig. 11

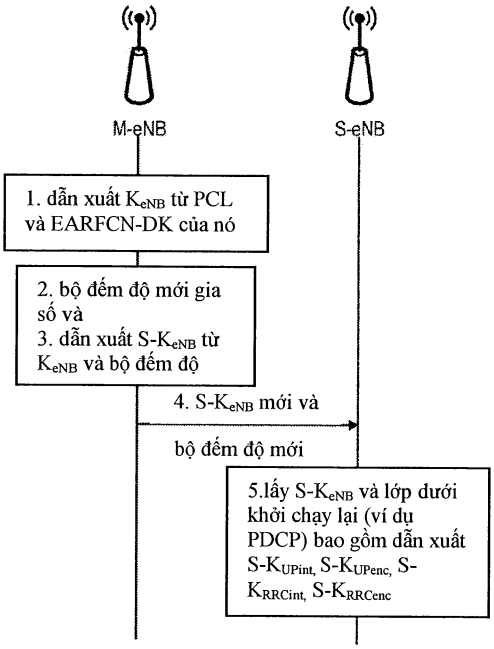

M-eNB
S-eNB
1. dẫn xuất K_{eNB} từ PCL và EARFCN-DK của nó
2. bộ đếm độ mới gia số và
3. dẫn xuất S-K_{eNB} từ K_{eNB} và bộ đếm độ
4. S-K_{eNB} mới và
bộ đếm độ mới
5.lấy S-K_{eNB} và lớp dưới khởi chạy lại (ví dụ PDCP) bao gồm dẫn xuất S-K_{UPint}, S-K_{UPenc}, S-K_{RRCint}, S-K_{RRCenc}

Fig. 12

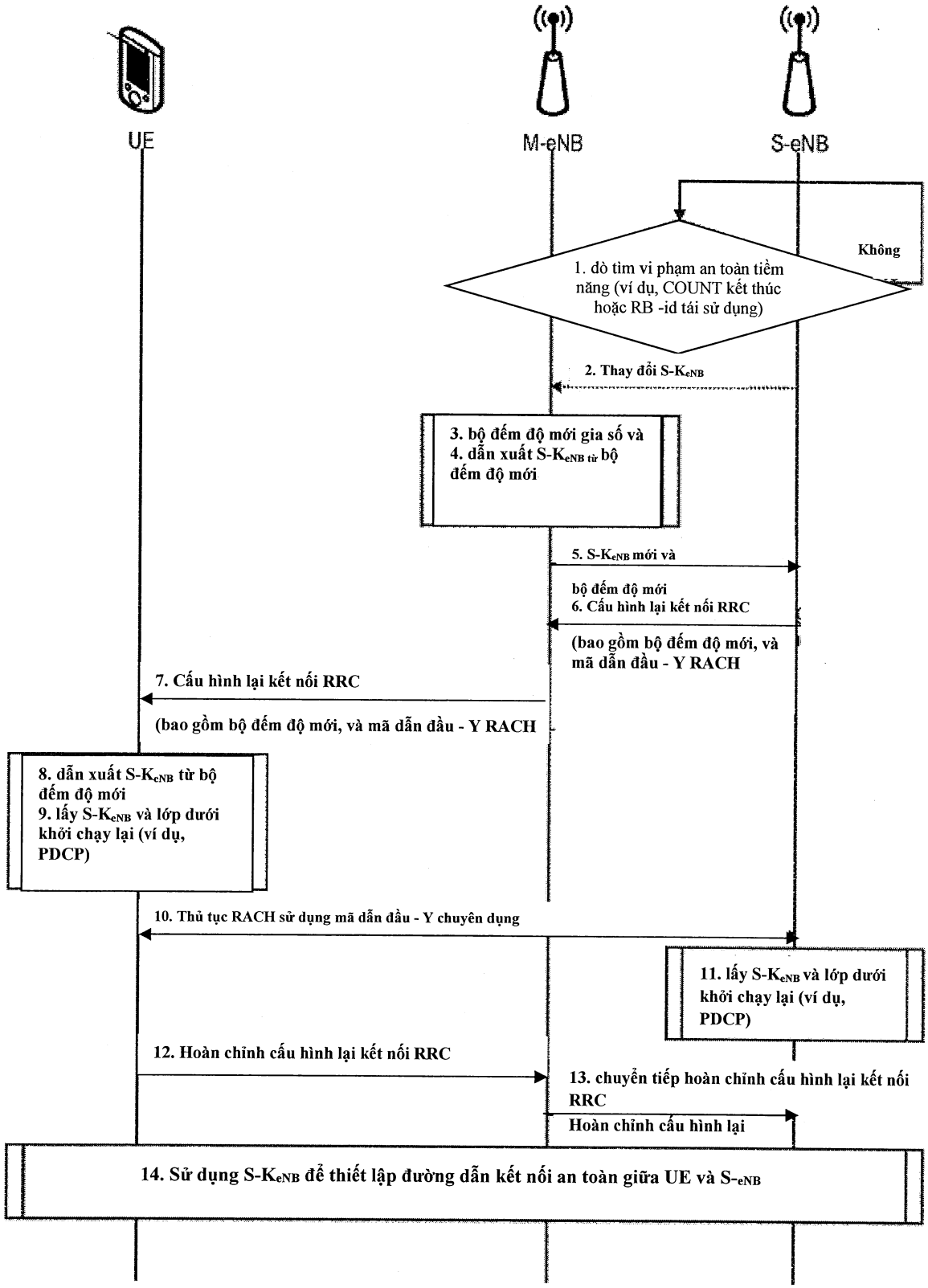

UE
M-eNB
S-eNB
1. dò tìm vi phạm an toàn tiềm năng (ví dụ, COUNT kết thúc hoặc RB -id tái sử dụng)
Không
2. Thay đổi S-KeNB
3. bộ đếm độ mới gia số và
4. dẫn xuất S-KeNB từ bộ đếm độ mới
5. S-KeNB mới và
bộ đếm độ mới
6. Cấu hình lại kết nối RRC
(bao gồm bộ đếm độ mới, và mã dẫn đầu - Y RACH
7. Cấu hình lại kết nối RRC
(bao gồm bộ đếm độ mới, và mã dẫn đầu - Y RACH
8. dẫn xuất S-KeNB từ bộ đếm độ mới
9. lấy S-KeNB và lớp dưới khởi chạy lại (ví dụ, PDCP)
10. Thủ tục RACH sử dụng mã dẫn đầu - Y chuyên dụng
11. lấy S-KeNB và lớp dưới khởi chạy lại (ví dụ, PDCP)
12. Hoàn chỉnh cấu hình lại kết nối RRC
13. chuyển tiếp hoàn chỉnh cấu hình lại kết nối RRC
Hoàn chỉnh cấu hình lại
14. Sử dụng S-KeNB để thiết lập đường dẫn kết nối an toàn giữa UE và S-eNB

Fig. 13

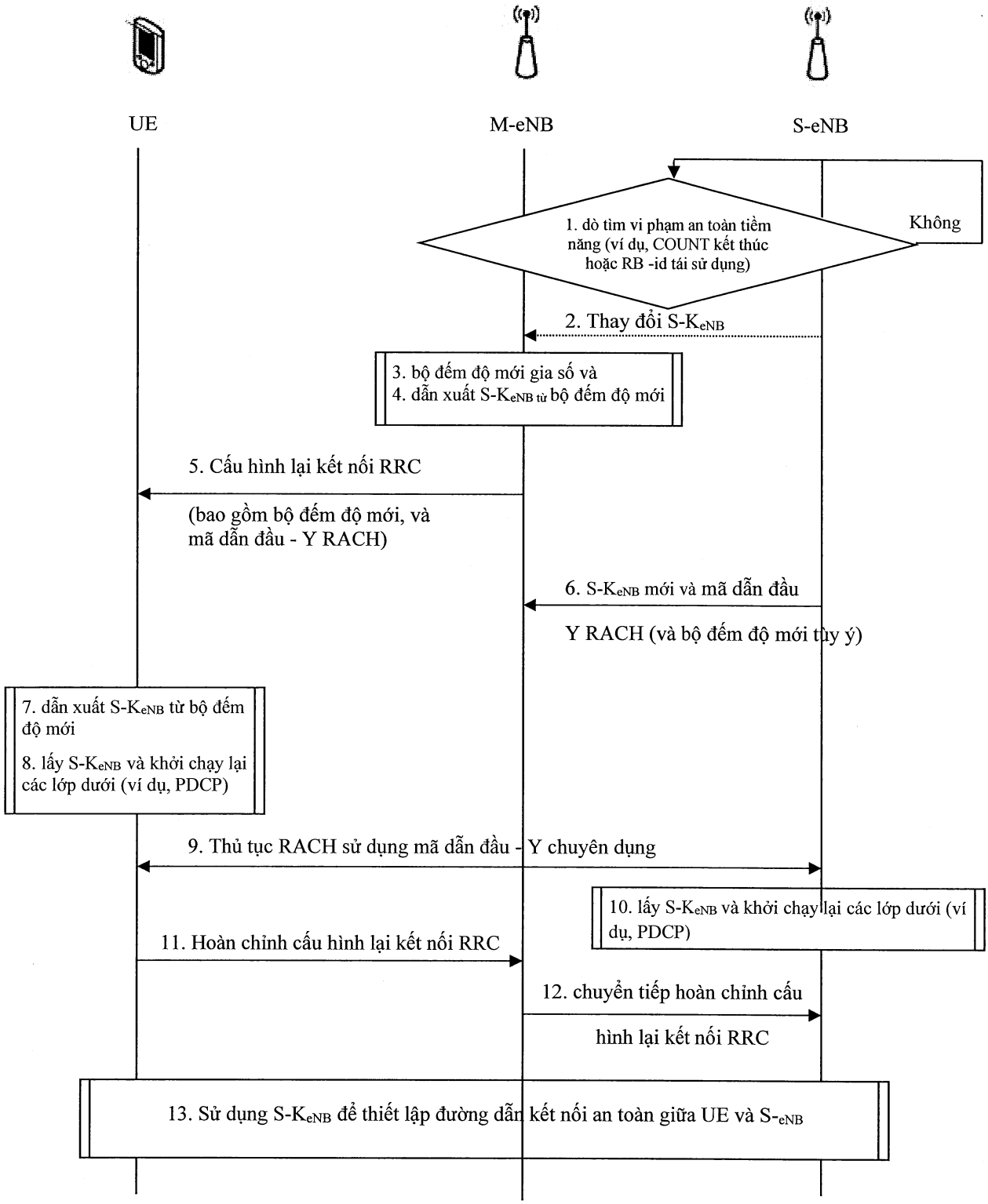

UE
M-eNB
S-eNB
1. dò tìm vi phạm an toàn tiềm năng (ví dụ, COUNT kết thúc hoặc RB -id tái sử dụng)
Không
2. Thay đổi S-KeNB
3. bộ đếm độ mới gia số và
4. dẫn xuất S-KeNB từ bộ đếm độ mới
5. Cấu hình lại kết nối RRC
(bao gồm bộ đếm độ mới, và mã dẫn đầu - Y RACH)
6. S-KeNB mới và mã dẫn đầu
Y RACH (và bộ đếm độ mới tùy ý)
7. dẫn xuất S-KeNB từ bộ đếm độ mới
8. lấy S-KeNB và khởi chạy lại các lớp dưới (ví dụ, PDCP)
9. Thủ tục RACH sử dụng mã dẫn đầu - Y chuyên dụng
10. lấy S-KeNB và khởi chạy lại các lớp dưới (ví dụ, PDCP)
11. Hoàn chỉnh cấu hình lại kết nối RRC
12. chuyển tiếp hoàn chỉnh cấu
hình lại kết nối RRC
13. Sử dụng S-KeNB để thiết lập đường dẫn kết nối an toàn giữa UE và S-eNB

FIG.14

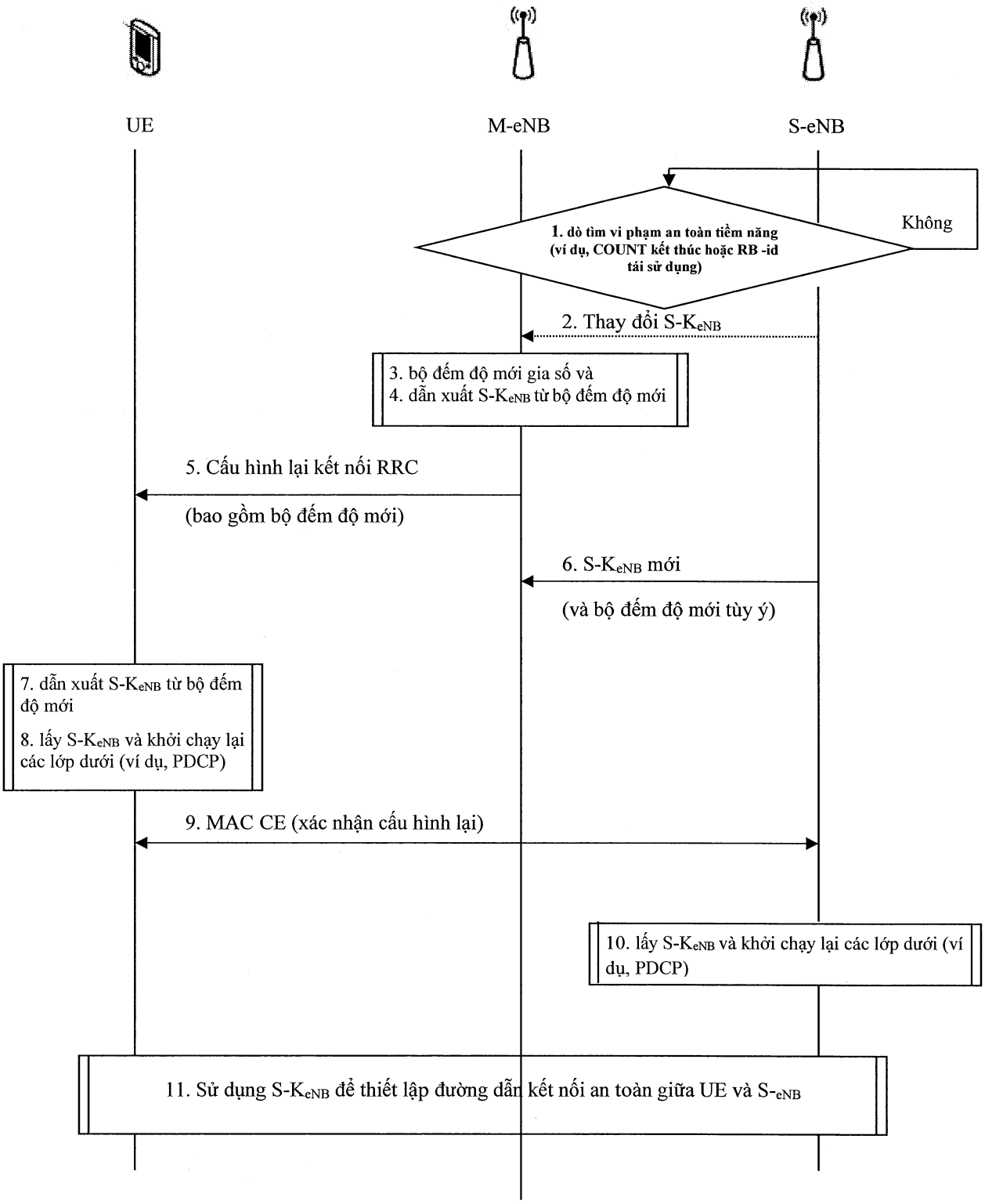

UE
M-eNB
S-eNB
1. dò tìm vi phạm an toàn tiềm năng (ví dụ, COUNT kết thúc hoặc RB -id tái sử dụng)
Không
2. Thay đổi S-KeNB
3. bộ đếm độ mới gia số và
4. dẫn xuất S-KeNB từ bộ đếm độ mới
5. Cấu hình lại kết nối RRC
(bao gồm bộ đếm độ mới)
6. S-KeNB mới
(và bộ đếm độ mới tùy ý)
7. dẫn xuất S-KeNB từ bộ đếm độ mới
8. lấy S-KeNB và khởi chạy lại các lớp dưới (ví dụ, PDCP)
9. MAC CE (xác nhận cấu hình lại)
10. lấy S-KeNB và khởi chạy lại các lớp dưới (ví dụ, PDCP)
11. Sử dụng S-KeNB để thiết lập đường dẫn kết nối an toàn giữa UE và S-eNB

FIG.15

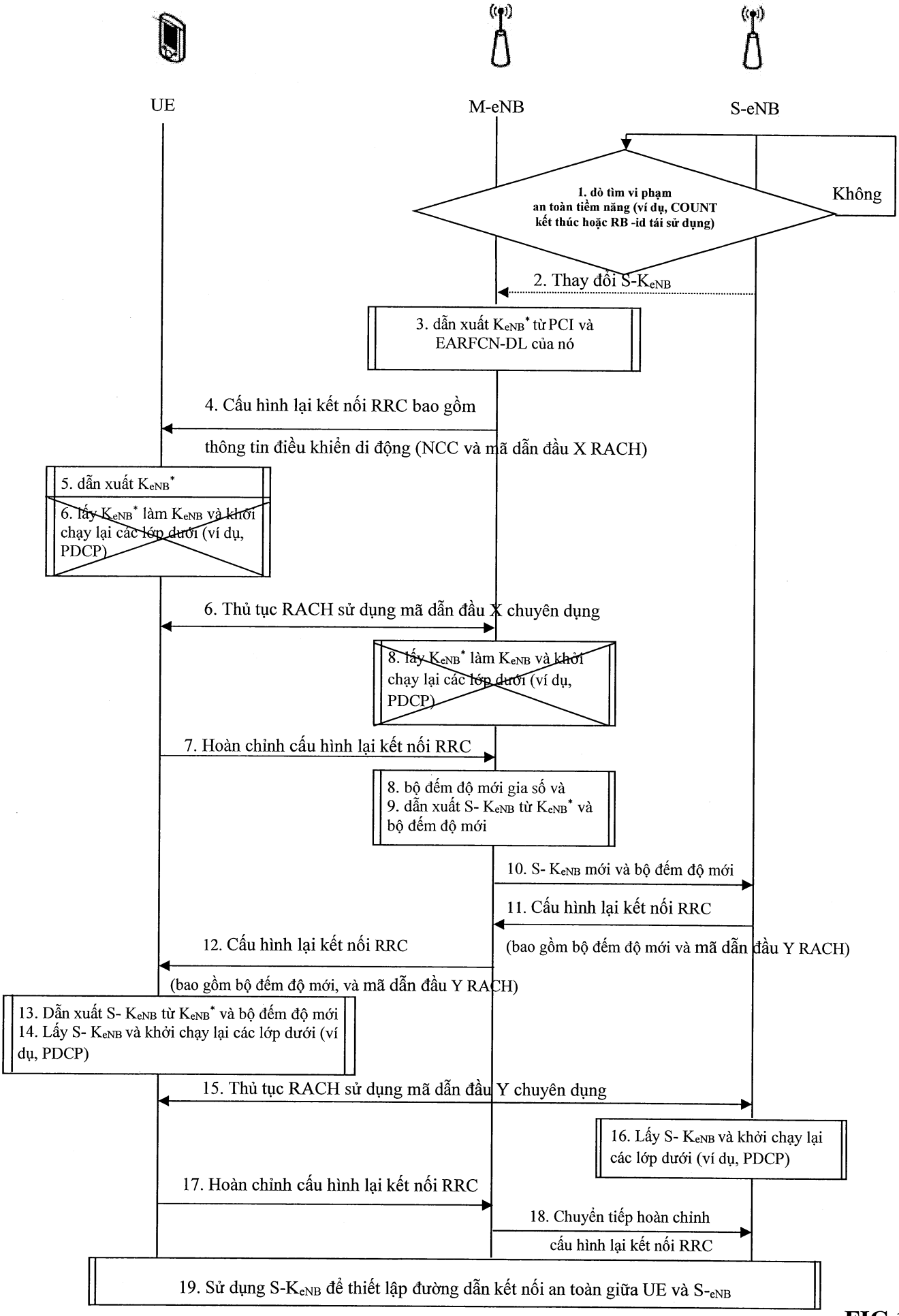

UE
M-eNB
S-eNB
1. dò tìm vi phạm an toàn tiềm năng (ví dụ, COUNT kết thúc hoặc RB -id tái sử dụng)
Không
2. Thay đổi S-KeNB
3. dẫn xuất KeNB* từ PCI và EARFCN-DL của nó
4. Cấu hình lại kết nối RRC bao gồm
thông tin điều khiển di động (NCC và mã dẫn đầu X RACH)
5. dẫn xuất KeNB*
6. lấy KeNB* làm KeNB và khởi chạy lại các lớp dưới (ví dụ, PDCP)
6. Thủ tục RACH sử dụng mã dẫn đầu X chuyên dụng
8. lấy KeNB* làm KeNB và khởi chạy lại các lớp dưới (ví dụ, PDCP)
7. Hoàn chỉnh cấu hình lại kết nối RRC
8. bộ đếm độ mới gia số và
9. dẫn xuất S- KeNB từ KeNB* và bộ đếm độ mới
10. S- KeNB mới và bộ đếm độ mới
11. Cấu hình lại kết nối RRC
(bao gồm bộ đếm độ mới và mã dẫn đầu Y RACH)
12. Cấu hình lại kết nối RRC
(bao gồm bộ đếm độ mới, và mã dẫn đầu Y RACH)
13. Dẫn xuất S- KeNB từ KeNB* và bộ đếm độ mới
14. Lấy S- KeNB và khởi chạy lại các lớp dưới (ví dụ, PDCP)
15. Thủ tục RACH sử dụng mã dẫn đầu Y chuyên dụng
16. Lấy S- KeNB và khởi chạy lại các lớp dưới (ví dụ, PDCP)
17. Hoàn chỉnh cấu hình lại kết nối RRC
18. Chuyển tiếp hoàn chỉnh
cấu hình lại kết nối RRC
19. Sử dụng S-KeNB để thiết lập đường dẫn kết nối an toàn giữa UE và S-eNB

FIG.16