(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) **1-0020404**

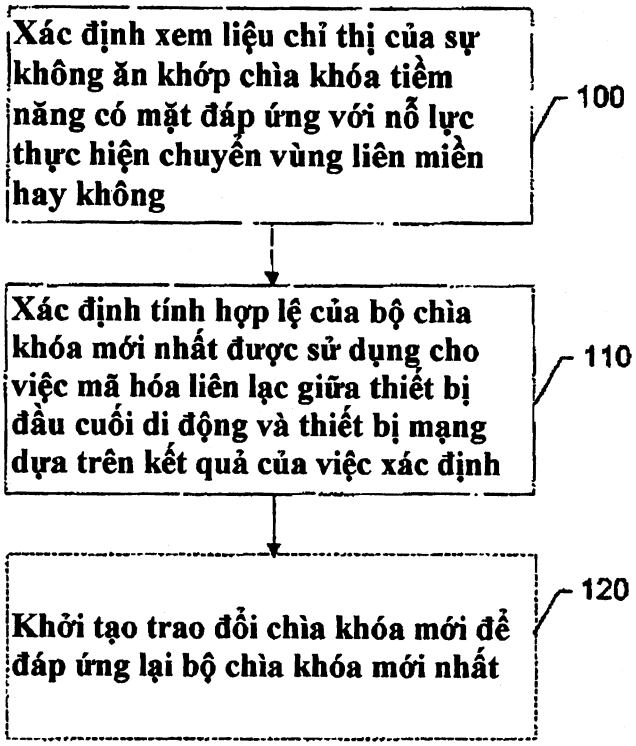
(51)[7] **H04W 12/04**, 36/14

(13) **B**

(21) 1-2012-00381
(22) 28.07.2010
(86) PCT/IB2010/053440 28.07.2010
(87) WO2011/039655 07.04.2011
(30) 61/246,723 29.09.2009 US
(45) 25.02.2019 371
(43) 25.10.2012 295
(73) Nokia Technologies OY (FI)
Karaportti 3, FI-02610 Espoo, Finland
(72) Steven FRANKLIN (GB), Stuart GEARY (GB), Keiichi KUBOTA (JP)
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) THIẾT BỊ VÀ PHƯƠNG PHÁP XÁC ĐỊNH TÍNH HIỆU LỰC CỦA BỘ KHÓA

(57) Sáng chế đề cập đến phương pháp và thiết bị cho phép xử lý khóa để chuyển giao giữa các miền khác nhau có thể bao gồm bước xác định xem liệu chỉ báo sự không ăn khớp tiềm tàng của khóa có hiện diện đáp lại nỗ lực để thực hiện chuyển giao giữa miền thứ nhất và miền thứ hai và xác định tính hiệu lực của bộ khóa mới nhất được sử dụng để mã hóa truyền thông giữa thiết bị đầu cuối di động và thiết bị mạng dựa vào kết quả xác định.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến công nghệ truyền thông trong các môi trường công nghệ đa truy cập rađio (radio access technology - RAT) và/hoặc các môi trường đơn RAT và, cụ thể hơn là, đề cập đến thiết bị và phương pháp cho phép xử lý khóa cho tính di động liên miền (tức là tính liên tục của cuộc gọi thoại rađio đơn (single radio voice call continuity - SR-VCC)).

Tình trạng kỹ thuật của sáng chế

Kỷ nguyên truyền thông hiện đại đã tạo ra sự mở rộng không ngừng của các mạng hữu tuyến và vô tuyến. Các mạng máy tính, các mạng ti vi và các mạng điện thoại đã trải qua việc mở rộng về công nghệ chưa từng có và được tiếp sức bởi nhu cầu không ngừng của người sử dụng. Các công nghệ nối mạng hữu truyến và vô tuyến đã giải quyết được các vấn đề liên quan tới nhu cầu của khách hàng, trong khi tạo ra tính linh hoạt và khả năng truyền thông tin tức thời cao hơn.

Các công nghệ nối mạng hiện tại và trong tương lai tiếp tục tạo thuận tiện cho việc truyền thông tin và tạo thuận tiện cho người sử dụng. Độ thuận tiện của việc truyền thông tin và sự thuận tiện cho người sử dụng ngày càng tăng này hiện được thực hiện bởi khả năng tăng cường để tạo ra các truyền thông di động với giá thành tương đối rẻ. Do đó các thiết bị truyền thông di động có mặt khắp nơi trên thế giới hiện tại. Cùng với sự mở rộng nhanh chóng công nghệ truyền thông di động, xuất hiện sự mở rộng nhanh chóng trong các dịch vụ được yêu cầu và được tạo ra thông qua các thiết bị truyền thông di động.

Qua lịch sử truyền thông di động, có nhiều thế hệ hệ thống được phát triển để cho phép sử dụng các thiết bị truyền thông này. Các thế hệ thứ nhất của các hệ thống này đôi khi được phát triển một cách độc lập và, ít nhất ban đầu là không cần thiết phải hoạt động phối hợp với các hệ thống khác. Tuy nhiên, sự phối hợp giữa các nhà phát triển hệ thống truyền thông bắt đầu được áp dụng sao cho các công nghệ mới có thể được phép phối hợp với các công nghệ khác để tăng toàn bộ dung lượng. Do đó, thiết bị đầu cuối di động vận hành được trong các hệ thống thế hệ hai (ví dụ, 2G) như hệ thống truyền thông di động toàn cầu (Global System for

Mobile communications - GSM) hoặc IS-95, thay thế các hệ thống thế hệ thứ nhất, trong một số trường hợp có thể sử dụng được khi phối hợp với các hệ thống thế hệ mới hơn như các hệ thống thế hệ thứ ba (ví dụ, 3G) và các hệ thống khác hiện đang được phát triển (ví dụ, mạng truy cập vô tuyến mặt đất vạn năng cải tiến (Evolved Universal Terrestrial Radio Access Network - E-UTRAN)).

Khả năng của thiết bị đầu cuối di động cụ thể để truy cập nhiều hệ thống hoặc truyền thông thông qua các công nghệ đa truy cập radio (đa RAT) là đôi khi được gọi là "đa truy cập radio" (multi-radio-access - MRA). Thiết bị đầu cuối có khả năng MRA do đó có thể được phép truyền giữa các RAT khác nhau (ví dụ, mạng truy cập vô tuyến mặt đất vạn năng (Universal Terrestrial Radio Access Network - UTRAN), mạng truy cập vô tuyến mặt đất vạn năng lan truyền (E-UTRAN), mạng truy cập vô tuyến EDGE GSM (GSM EDGE Radio Access Network - GERAN), truy cập gói tốc độ cao (High Speed Packet Access - HSPA)). Mục đích của việc truyền tất nhiên là để duy trì tính liên tục truyền thông qua mỗi lần truyền. Dự án đối tác thế hệ thứ ba (Third Generation Partnership Project - 3 GPP) định nghĩa các đặc tả khác nhau để cố gắng tiêu chuẩn hóa các khía cạnh của các cơ chế được sử dụng để đạt được mục đích này cũng như các mục đích khác. Một đề xuất của các tiêu chuẩn 3GPP tạo ra cho việc chuyển giao qua phiên giọng nói qua E-UTRAN tới GERAN như là cuộc gọi thoại được chuyển mạch kênh (circuit switched - CS) (ví dụ, chuyển giao từ kết nối được chuyển mạch gói (packet switched - PS) tới kết nối CS). Nói cách khác, ví dụ, SR-VCC tạo ra cơ chế mà nhờ đó chuyển giao từ cuộc gọi thoại qua giao thức Internet (Voice over Internet Protocol - VoIP) qua kênh mang dữ liệu tới cuộc gọi thoại truyền thống qua kênh mang CS. Tuy nhiên, SR-VCC cũng có khả năng vận hành trong môi trường RAT đơn. Ví dụ, thiết bị có thể được chuyển giao từ HSPA tới UTRAN, trong đó HSPA là một phần của UTRAN.

Ngoài ra, các tình huống chuyển giao liên miền khác ngoài SR-VCC là cũng có thể.

Một nguyên tắc hoặc mục đích của việc áp dụng các tiêu chuẩn liên quan tới các giải pháp là để loại bỏ hoặc khắc phục các tác động trên mạng truy cập đích (ví dụ, GERAN). Cụ thể, liên quan tới SR-VCC từ E-UTRAN về phía mạng đích phiên bản trước 8, có thể mong muốn sử dụng đích trung tâm chuyển mạch di động (mobile switching center - MSC) và các nút hệ thống trạm cơ sở (base station system - BSS) được triển khai không yêu cầu các thay

đổi về cơ bản cho các nút này để hỗ trợ giải pháp SR-VCC. Tuy nhiên, trong một số trường hợp, các vấn đề có thể xuất hiện do thực tế là mạng và thiết bị người sử dụng (user equipment - UE) được chuyển giao có thể có nhiều khái niệm khác nhau khi chuyển giao thành công. Ví dụ, trong mỗi tình huống chuyển giao SR-VCC khác nhau, UE có thể xem xét việc hoàn thành chuyển giao và sau đó gửi tin nhắn chỉ báo tới mạng. Mạng thông thường xem xét việc hoàn thành chuyển giao sau khi nhận tin nhắn được gửi bởi UE. Do đó, với sự khác biệt các điều kiện xác định hoàn thành chuyển giao được thiết lập, có thể có khả năng cho một phía lưu trữ bộ khóa CS mới và ở phía còn lại bố trí bộ khóa CS mới và thay vào đó là duy trì bộ khóa CS được lưu trữ trước đó. Tình huống này có thể xuất hiện, ví dụ, trong trường hợp chuyển giao thất bại. Cụ thể hơn, nếu UE thực hiện truyền (ví dụ, tin nhắn hoàn thành chuyển giao) mà không được nhận bởi mạng, UE sẽ lưu trữ bộ khóa CS mới, nhưng mạng sẽ vẫn giữ bộ khóa CS cũ.

Sự không ăn khớp của bộ khóa thường được xử lý bằng việc kiểm tra sự ăn khớp của mã nhận diện bộ khóa (key set identity - KSI) hoặc số chuỗi khóa mã hóa (ciphering key sequence number - CKSN) trong mạng và tại UE tại kết nối CS và/hoặc PS kế tiếp, trong đó sự không ăn khớp sẽ kích khởi trao đổi khóa mới (ví dụ, thông qua quy trình xác thực và thỏa thuận khóa (authentication and key agreement - AKA)). Thất bại có thể xuất hiện khi bộ khóa được ánh xạ mới có mã nhận diện được ánh xạ giống với bộ khóa được lưu trữ hiện đang tồn tại. Cụ thể, ví dụ, nếu không biết bộ khóa nào trong hai bộ khóa có thể được lưu trữ theo mã nhận diện bộ khóa trong mạng và tại UE, thì sự không ăn khớp của các bộ khóa có thể là điều kiện rất quan trọng tạo ra lỗi kết nối hoặc auđio bị mã hóa kém. Ví dụ nêu trên chỉ đơn thuần là tình huống trong đó sự không ăn khớp của khóa có thể tạo ra chuyển giao giữa các miền cụ thể khác nhau liên quan đến SR-VCC. Tuy nhiên, cần hiểu rằng các vấn đề tương tự liên quan tới sự không ăn khớp của khóa có thể xuất hiện liên quan tới các chuyển giao liên miền khác cũng như không nhất thiết liên quan đến SR-VCC hoặc MRA.

Do đó, mong muốn có các thay đổi cho các quy trình xử lý khóa cho các chuyển giao liên miền.

Bản chất kỹ thuật của sáng chế

Phương pháp, thiết bị và sản phẩm chương trình máy tính được đề xuất có thể cho phép thay đổi để chuyển giao liên miền trong các môi trường đa RAT hoặc đơn RAT. Theo đó, ví dụ, nhiều phương án của sáng chế có thể tạo ra cơ chế mà nhờ đó loại bỏ được các tình huống, trong đó gặp phải sự không ăn khớp trong các bộ khóa theo thứ tự để, ví dụ, hỗ trợ giải pháp SR-VCC.

Theo một phương án làm ví dụ, sáng chế đề xuất phương pháp cho phép xử lý khóa để chuyển giao giữa các miền khác nhau. Phương pháp này có thể bao gồm bước xác định xem liệu chỉ báo sự không ăn khớp tiềm tàng của khóa có hiện diện đáp ứng nỗ lực để thực hiện chuyển giao giữa miền thứ nhất và miền thứ hai hay không, và xác định tính hiệu lực của bộ khóa mới nhất được sử dụng để mã hóa truyền thông giữa thiết bị đầu cuối di động và thiết bị mạng dựa vào kết quả của bước xác định.

Theo một phương án làm ví dụ khác, sáng chế đề xuất thiết bị để cho phép quản lý khóa để chuyển giao giữa các miền khác nhau. Thiết bị này có thể bao gồm ít nhất một bộ xử lý và ít nhất một bộ nhớ bao gồm mã chương trình máy tính. Ít nhất một bộ nhớ và mã chương trình máy tính có thể được cấu hình để, với ít nhất một bộ xử lý, làm cho thiết bị thực hiện ít nhất việc xác định xem liệu chỉ báo sự không ăn khớp tiềm tàng của khóa có hiện diện đáp lại nỗ lực để thực hiện chuyển giao giữa miền thứ nhất và miền thứ hai hay không, và xác định tính hiệu lực của bộ chìa khóa mới nhất được sử dụng để mã hóa truyền thông giữa thiết bị đầu cuối di động và thiết bị mạng dựa vào kết quả của việc xác định.

Theo một phương án thực hiện làm ví dụ khác, sáng chế đề xuất sản phẩm chương trình máy tính để cho phép xử lý khóa để chuyển giao giữa các miền khác nhau. Sản phẩm chương trình máy tính bao gồm ít nhất một vật ghi đọc được bằng máy tính có các lệnh mã chương trình đọc được bởi máy tính được lưu ở đó. Các lệnh mã chương trình đọc được bởi máy tính có thể bao gồm các lệnh mã chương trình để xác định xem liệu chỉ báo sự không ăn khớp tiềm tàng của chìa có hiện diện đáp lại nỗ lực thực hiện chuyển giao giữa miền thứ nhất và miền thứ hai hay không, và xác định tính hiệu lực của bộ chìa khóa mới nhất được sử dụng để mã hóa truyền thông giữa thiết bị đầu cuối di động và thiết bị mạng dựa trên kết quả của việc xác định.

Mô tả vắn tắt các hình vẽ

Do đó, sáng chế được mô tả theo nghĩa chung, có tham khảo tới các hình vẽ kèm theo, các hình vẽ này không nhất thiết phải được vẽ theo cùng một tỷ lệ và trong đó:

Fig.1 giản đồ khối sơ lược của hệ thống truyền thông vô tuyến theo phương án ví dụ của sáng chế;

Fig.2 là hình vẽ minh họa giản đồ khối của thiết bị cho phép xử lý khóa cho việc chuyển giao giữa các miền khác nhau theo phương án ví dụ của sáng chế;

Fig.3 là hình vẽ minh họa giản đồ khối của thiết bị cho phép xử lý khóa để chuyển giao giữa các miền khác nhau theo phương án ví dụ của sáng chế; và

Fig.4 là lưu đồ theo phương pháp ví dụ cho phép xử lý khóa để chuyển giao giữa các miền khác nhau theo phương án ví dụ của sáng chế.

Mô tả chi tiết sáng chế

Một số phương án của sáng chế sẽ được mô tả chi tiết hơn dưới đây với sự tham khảo tới các hình vẽ kèm theo, trong đó một số, nhưng không phải là tất cả các phương án của sáng chế được thể hiện. Thực sự là, các phương án khác nhau của sáng chế có thể được áp dụng trong nhiều dạng khác nhau và không bị coi là giới hạn các phương án được chỉ ra ở đây; hơn nữa, các phương án này được tạo ra sao cho phần bộc lộ này sẽ thỏa mãn các nhu cầu pháp lý. Các số chỉ dẫn tương tự biểu thị các thành phần tương tự. Như được sử dụng ở đây, các thuật ngữ "dữ liệu", "nội dung", "thông tin" và các thuật ngữ tương tự có thể được sử dụng hoán đổi cho nhau để cập đến khả năng dữ liệu được truyền, nhận và/hoặc lưu trữ theo các phương án của sáng chế.

Hơn nữa, thuật ngữ "ví dụ", như được sử dụng ở đây, không được tạo ra để đề cập đến vấn đề về bản chất mà chỉ đơn thuần là minh họa của một ví dụ. Do đó, việc sử dụng các thuật ngữ này không làm giới hạn mục đích và phạm vi của các phương án của sáng chế.

Ngoài ra, như được sử dụng ở đây, thuật ngữ 'mạch' đề cập đến (a) các ứng dụng mạch chỉ có phần cứng (ví dụ, các ứng dụng trong mạch tương tự và/hoặc mạch kỹ thuật số); (b) tổ hợp của các mạch và (các) sản phẩm chương trình máy tính bao gồm các lệnh phần mềm và/hoặc phần sụn được lưu trữ trên một hoặc nhiều bộ nhớ đọc được bằng máy tính làm việc cùng nhau khiến cho thiết bị thực hiện một hoặc nhiều chức năng được mô tả ở đây; và (c) các

mạch, như, ví dụ, (các) bộ vi xử lý hoặc phần của (các) bộ vi xử lý) yêu cầu phần mềm hoặc phần sụn để vận hành thậm chí nếu phần mềm hoặc phần sụn không có mặt về phương diện vật lý. Định nghĩa 'mạch' này áp dụng cho tất cả cách sử dụng của thuật ngữ này ở đây, bao gồm việc sử dụng trong yêu cầu bảo hộ bất kỳ. Theo ví dụ khác, như được sử dụng ở đây, thuật ngữ 'mạch' cũng bao gồm ứng dụng bao gồm một hoặc nhiều bộ xử lý và/hoặc (các) phần của chúng và phần mềm và/hoặc phần sụn kèm theo. Theo ví dụ khác, thuật ngữ 'mạch' được sử dụng ở đây cũng bao gồm, ví dụ, mạch tích hợp băng cơ sở hoặc mạch tích hợp bộ xử lý các ứng dụng cho điện thoại di động hoặc mạch tích hợp tương tự trong máy chủ, thiết bị mạng dạng ô, thiết bị mạng khác, và/hoặc thiết bị tính toán khác.

Như được xác định ở đây, "vật ghi đọc được bằng máy tính" là vật ghi vật lý (ví dụ, thiết bị lưu trữ khả biến hoặc bất khả biến), có thể khác biệt với "môi trường truyền đọc được bằng máy tính" là tín hiệu điện từ.

Trái với tình trạng kỹ thuật nêu trên, ví dụ trong đó một phương án của sáng chế có khả năng áp dụng sẽ được mô tả dưới đây liên quan tới việc chuyển giao theo giải pháp SR-VCC. Tuy nhiên, cần hiểu rằng các phương án của sáng chế cũng mở rộng tới các giải pháp liên miền khác và không bị giới hạn ở SR-VCC. Hơn nữa, mặc dù chuyển giao từ miền PS tới miền CS được mô tả một cách cụ thể trong một ví dụ, các phương án cũng áp dụng cho các chuyển giao từ miền CS tới miền PS. Do đó, các ví dụ được minh họa ở đây không nên được coi là giới hạn về áp dụng các phương án của sáng chế. Do đó, việc xử lý các khóa được ánh xạ giữa các miền khác nhau (ví dụ, miền PS tới miền CS hoặc các chuyển giao làm ví dụ khác) có thể được cải thiện bởi các phương án của sáng chế. Thông thường, ví dụ, khi thực hiện các chuyển giao SR-VCC, việc mã hóa được duy trì khi chuyển mạch từ miền PS tới miền CS bằng cách ánh xạ các khóa CS mới từ các khóa PS đang sử dụng tại thời điểm chuyển giao. Các khóa CS được tạo ra được xem xét là "mới" do ánh xạ tạo ra việc sử dụng của giá trị NONCE. Khi các khóa CS được tạo ra và SR-VCC hoàn thành các chuyển giao một cách thành công, thì thiết bị người sử dụng (UE) như điện thoại di động hoặc thiết bị đầu cuối di động khác có thể lưu trữ các khóa CS được tạo ra mới để sử dụng trong các kết nối CS sau này. Mạng cũng có thể lưu trữ các khóa để sử dụng sau này để hỗ trợ các kết nối CS với UE. Mã nhận diện của bộ khóa CS mới (ví dụ, KSI hoặc CKSN) được sao chép một cách trực tiếp từ nhận diện bộ khóa PS.

Theo đó, nếu thất bại chuyển giao như mô tả ở trên, thì một phía có thể lưu trữ bộ khóa CS mới, trong khi phía còn lại có thể không, nhờ đó tạo ra sự không ăn khớp của khóa.

Một số phương án của sáng chế có thể tạo ra quy trình xử lý khóa có thể loại bỏ sự không ăn khớp của khóa khi thất bại chuyển giao SR-VCC. Theo đó, ví dụ, một số phương án của sáng chế có thể tạo ra cho quy trình xử lý khóa thực hiện việc làm bất hiệu lực của các khóa trong các tình huống, trong đó nó có thể xác định rằng các điều kiện hiện tại đề xuất việc không ăn khớp của khóa là có thể. Theo đó, các phương án của sáng chế có thể tạo ra cho mạng và các quy trình xử lý khóa phía UE có thể loại bỏ các tình huống không ăn khớp của khóa.

Fig.1, một phương án ví dụ của sáng chế, minh họa giản đồ khối sơ lược của hệ thống truyền thông vô tuyến theo phương án ví dụ của sáng chế. Sau đây, dựa vào Fig.1, minh họa một loại hệ thống có lợi từ các phương án của sáng chế. Hệ thống có thể bao gồm nhiều thiết bị mạng và một hoặc nhiều thiết bị đầu cuối di động (ví dụ, thiết bị người sử dụng (UE) 10). Các thiết bị đầu cuối di động có thể là các ví dụ khác nhau của thiết bị truyền thông di động như các thiết bị hỗ trợ kỹ thuật số (portable digital assistant - PDA), các máy nhắn tin, các ti vi di động, các thiết bị chơi điện tử, các máy tính xách tay, các điện thoại di động, các máy quay, các thiết bị ghi viđeo, các thiết bị chơi auđio/viđeo, các rađio, các thiết bị hệ thống định vị toàn cầu (global positioning system - GPS) hoặc tổ hợp bất kỳ của các thiết bị nêu trên và các loại khác của thiết bị truyền thông thoại và ký tự. Tuy nhiên, cần hiểu rằng thiết bị đầu cuối di động như được minh họa và dưới đây gọi được mô tả chỉ nhằm mục đích minh họa một loại bộ phận có lợi từ các phương án của sáng chế và do đó không được coi là giới hạn phạm vi của các phương án của sáng chế.

Theo một phương án làm ví dụ, UE 10 có thể có ăngten (hoặc nhiều ăngten) để truyền các tín hiệu tới và nhận các tín hiệu từ nút mạng như vị trí cơ sở, trạm cơ sở, điểm truy cập, nút B hoặc e-nút B. Theo phương án ví dụ, UE 10 có thể ban đầu truyền thông với nút nguồn 20 (ví dụ, nút B tăng cường của E-UTRAN) và có thể trong quy trình được chuyển giao đến nút đích 30 (ví dụ, trạm cơ sở (base station - BS) của GERAN). Tuy nhiên, cần hiểu rằng nút đích 30 và nút nguồn 20 có thể tương ứng với các trạm cơ sở hoặc điểm truy cập khác tương

ứng với các tình huống chuyển giao liên miền khác (ví dụ, miền PS tới miền CS hoặc miền CS tới miền PS, v.v.).

Trong quy trình chuyển giao, tin nhắn yêu cầu chuyển giao được sử dụng để khởi tạo việc chuyển giao có thể được mong đợi để nhận diện của nút nguồn 20. Do đó, trung tâm chuyển mạch di động (MSC) 32 được kết hợp với nút đích có thể nhận nhận diện từ nút nguồn 20 kết hợp với yêu cầu chuyển giao. MSC 32 có thể có khả năng định tuyến các cuộc gọi tới và từ UE 10 khi UE 10 tạo và nhận các cuộc gọi trong khi truyền thông với nút đích 30. Do đó, MSC 32 có thể tạo ra kết nối tới các đường trung kế cố định khi UE 10 tham gia vào cuộc gọi. Ngoài ra, MSC 32 có thể có khả năng điều khiển việc chuyển tiếp các tin nhắn tới và từ UE 10 và cũng có thể điều khiển việc chuyển tiếp các tin nhắn cho UE 10 tới và từ trung tâm nhắn tin. MSC 32 có thể được kết nối với mạng dữ liệu, như mạng cục bộ (local area network - LAN), mạng diện đô thị (metropolitan area network - MAN), và/hoặc mạng diện rộng (wide area network - WAN) (ví dụ, các hệ thống phụ đa phương tiện giao thức Internet (Internet Protocol Multimedia Subsystem - IMS) dự án đối tác thế hệ ba (Third Generation Partnership Project - 3GPP) 40. Nút nguồn 20 cũng có thể được kết nối với 3GPP IMS 40 thông qua một hoặc nhiều thiết bị cổng như GW 22. GW 22 có thể thể hiện cổng phục vụ (S-GW) và/hoặc cổng mạng dữ liệu gói (packet data network gateway - PDN GW). S-GW có thể định tuyến và chuyển tiếp các gói dữ liệu người sử dụng, trong khi cũng hoạt động như là neo (anchor) di động cho mặt phẳng người sử dụng trong các chuyển giao nằm trong E-UTRAN hoặc giữa E-UTRAN và các RAT khác (ví dụ, GERAN). PDN GW có thể tạo ra kết nối cho UE 10 tới các mạng dữ liệu gói ngoại vi bằng cách trở thành điểm đi ra và đi vào của lưu lượng cho UE 10.

Nút đích 30 trong ví dụ này cũng được kết nối với nút hỗ trợ (SGSN) dịch vụ vô tuyến gói tổng hợp (General Packet Radio Service - GPRS) 34. SGSN 34 có thể có khả năng thực thi các chức năng tương tự với MSC 32 cho các dịch vụ chuyển mạch gói. SGSN 34 có thể được kết nối với thành phần quản lý tính di động (mobility management element - MME) 36 cũng có thể truyền thông với MSC 32 và nút nguồn 20 và GW 22. MME 36, ngoài các khả năng khác, có thể đáp ứng các quy trình theo dõi và nhắn tin UE chế độ rỗi. MME 36 cũng có thể quản lý việc chọn GW cho việc gắn UE và chuyển giao các quy trình và có thể quản lý việc xác thực người sử dụng. Do đó, trong một số trường hợp, mạng (ví dụ, MSC 32, SGSN 34

hoặc MME 36) cũng quản lý việc tạo và/hoặc lưu trữ các khóa và ánh xạ các khóa giữa miền PS và miền CS. Tuy nhiên, cần thấy rằng thực thể mạng khác với MME 36, MSC 32, SGSN 34 hoặc thực thế khác theo cách khác cũng có thể có khả năng tạo và/hoặc lưu trữ các khóa và ánh xạ các khóa.

Ví dụ, trong tình huống mà trong đó chuyển giao được yêu cầu, MME 36 có thể phối hợp chuyển giao UE 10 từ nút nguồn 20 tới nút đích 30. Như một phần của quy trình chuyển giao, MSC 32 có thể cung cấp bộ khóa CS mới cho UE 10, có thể được tạo ra cho UE 10 thông qua SGSN 34. MME 36 có thể sử dụng các quy trình được mô tả trong các đặc điểm kỹ thuật 3GPP TS-33.102 V.x.y và TS-33.401 V.x.y để xử lý việc ánh xạ các bộ khóa giữa miền PS và miền CS. Sau khi bộ khóa CS mới được tạo, MSC 32 có thể lưu trữ bộ khóa CS mới tại chỗ. UE 10 sau đó có thể tạo bộ khóa CS mới từ khóa PS và NONCE. Sau khi tạo bộ khóa CS mới, UE 10 cũng có thể lưu trữ bộ khóa CS mới, ví dụ, bên trong (U)SIM (thuê bao nhận diện môđun UMTS) của UE 10. Các quy trình này là tương tự với các quy trình truyền thống. Tuy nhiên, các phương án của sáng chế có thể còn áp dụng thiết bị xử lý khóa trong tình huống thất bại hoạt động chuyển giao liên miền (ví dụ, thất bại chuyển giao).

Fig.2 và Fig.3 minh họa các giản đồ khối của thiết bị có lợi từ các phương án của sáng chế. Tuy nhiên, cần hiểu rằng, thiết bị như được minh họa và dưới đây được mô tả chỉ nhằm mục đích minh họa một thiết bị có thể có lợi từ các phương án của sáng chế và, do đó, không bị coi là giới hạn phạm vi của các phương án của sáng chế. Theo một phương án ví dụ, thiết bị trên Fig.2 có thể được áp dụng trên thiết bị đầu cuối di động (ví dụ, UE 10) khả năng truyền thông với thiết bị khác thông qua mạng. Theo phương án khác, thiết bị trên Fig.3 có thể được áp dụng tại thiết bị mạng (ví dụ, MSC 32) được tạo cấu hình để quản lý hoặc theo cách khác tham gia vào việc phối hợp của các chuyển giao liên miền. Tuy nhiên, không phải tất cả các hệ thống đều áp dụng các phương án của sáng chế như được mô tả một cách cần thiết ở đây. Hơn nữa, các cấu trúc khác cho các thiết bị sử dụng các phương án của sáng chế cũng có thể được tạo ra và các cấu trúc này có thể bao gồm nhiều hoặc ít các thành phần hơn số thành phần được thể hiện trên Fig.2 và Fig.3. Do đó, nhiều phương án có thể bao gồm nhiều hoặc ít hơn tất cả các thiết bị được minh hoạ và/hoặc được mô tả ở đây. Hơn nữa, trong nhiều phương án, mặc dù các bộ phận hoặc các thành phần được thể hiện truyền thông với nhau, dưới đây gọi là các

thiết bị hoặc các thành phần nên được xem là có khả năng áp dụng trong cùng một bộ phận hoặc thành phần và do đó, các bộ phận hoặc các thành phần được thể hiện trong truyền thông theo cách khác sẽ được hiểu là các phần của cùng một bộ phận hoặc thành phần.

Dựa vào Fig.2, thiết bị 50 để xử lý khóa sau khi thất bại chuyển giao liên miền được tạo ra. Thiết bị 50 có thể áp dụng trong hoặc được sử dụng làm thiết bị đầu cuối di động (ví dụ, UE 10 trên Fig.1). Thiết bị 50 có thể bao gồm hoặc theo cách khác truyền thông với bộ xử lý 70, giao diện người sử dụng 72, giao diện truyền thông 74 và thiết bị lưu trữ 76. Thiết bị lưu trữ 76 có thể chứa, ví dụ, một hoặc nhiều bộ nhớ khả biến và/hoặc bất khả biến. Theo nghĩa khác, ví dụ, thiết bị lưu trữ 76 có thể là thiết bị lưu trữ điện tử (ví dụ, vật ghi đọc được bằng máy tính) bao gồm các cổng được tạo cấu hình để lưu trữ dữ liệu (ví dụ, các bit) có thể được truy hồi bởi máy (ví dụ, thiết bị tính toán). Thiết bị lưu trữ 76 có thể được tạo cấu hình để lưu trữ thông tin, dữ liệu, ứng dụng, các lệnh hoặc tương tự cho phép thiết bị thực hiện các chức năng khác nhau theo các phương án ví dụ của sáng chế. Ví dụ, thiết bị lưu trữ 76 có thể được tạo cấu hình để đệm dữ liệu đầu vào để xử lý bởi bộ xử lý 70. Ngoài ra hoặc theo cách khác, thiết bị lưu trữ 76 có thể được tạo cấu hình để lưu trữ các lệnh để thực thi bởi bộ xử lý 70.

Bộ xử lý 70 có thể được áp dụng trong nhiều cách. Ví dụ, bộ xử lý 70 có thể được áp dụng làm một hoặc nhiều phương tiện xử lý khác nhau như bộ đồng xử lý, bộ vi xử lý, bộ điều khiển, bộ xử lý tín hiệu số (DSP), thành phần xử lý có hoặc không có DSP kèm theo hoặc các thiết bị xử lý khác bao gồm các mạch tích hợp như, ví dụ, mạch tích hợp chuyên dụng (application specific integrated circuit - ASIC, mạng cổng trường lập trình được bằng trường (field programmable gate array - FPGA), bộ vi điều khiển (microcontroller unit - MCU), bộ tăng tốc phần cứng, chip máy tính chuyên dụng hoặc tương tự. Theo phương án ví dụ, bộ xử lý 70 có thể được tạo cấu hình để thực thi các lệnh được lưu trữ trong thiết bị lưu trữ 76 hoặc có thể truy cập được bởi bộ xử lý 70. Theo cách khác hoặc ngoài ra, bộ xử lý 70 có thể được tạo cấu hình để thực hiện chức năng được mã hóa cứng. Do đó, dù có được tạo cấu hình bởi các thiết bị phần cứng hoặc phần mềm hoặc bởi tổ hợp của chúng hay không, bộ xử lý 70 có thể biểu diễn thực thể (ví dụ, theo cách vật lý được áp dụng trong mạch) có khả năng thực hiện các bước theo các phương án của sáng chế trong khi được tạo cấu hình một cách tương ứng. Do đó, ví dụ, khi bộ xử lý 70 được áp dụng làm ASIC, FPGA hoặc tương tự, bộ xử lý 70 có thể

được tạo cấu hình phần cứng một cách cụ thể để thực hiện các bước được mô tả ở đây. Theo cách khác, như một ví dụ khác, khi bộ xử lý 70 được áp dụng làm bộ phận thực thi của các lệnh phần mềm, các lệnh có thể tạo cấu hình một cách cụ thể cho bộ xử lý 70 để thực thi các thuật toán và/hoặc các bước được mô tả ở đây khi các lệnh được thực thi. Tuy nhiên, trong nhiều trường hợp, bộ xử lý 70 có thể là bộ xử lý của thiết bị cụ thể (ví dụ, thiết bị đầu cuối di động hoặc thiết bị mạng) được làm phù hợp để áp dụng các phương án của sáng chế bởi cấu hình tiếp theo của bộ xử lý 70 nhờ các lệnh để thực hiện các thuật toán và/hoặc các bước được mô tả ở đây. Ngoài các thành phần khác, bộ xử lý 70 có thể chứa đồng hồ, đơn vị logic số học (arithmetic logic unit - ALU) và các cổng logic được tạo cấu hình để hỗ trợ hoạt động của bộ xử lý 70.

Trong khi đó, giao diện truyền thông 74 có thể là phương tiện bất kỳ như thiết bị hoặc mạch được áp dụng trong cả phần cứng, phần mềm hoặc kết hợp của phần cứng và phần mềm được tạo cấu hình để nhận và/hoặc truyền dữ liệu từ/tới mạng và/hoặc bộ phận hoặc môđun bất kỳ khác truyền thông với thiết bị. Theo đó, giao diện truyền thông 74, ví dụ có thể có (nhiều) ăngten và phần cứng và/hoặc phần mềm hỗ trợ để cho phép truyền thông với mạng truyền thông vô tuyến. Trong một số môi trường, giao diện truyền thông 74 có thể thay đổi hoặc cũng hỗ trợ truyền thông hữu tuyến. Do đó, ví dụ, giao diện truyền thông 74 có thể bao gồm mođem truyền thông và/hoặc phần cứng/phần mềm khác để hỗ trợ sự truyền thông thông qua cáp, đường thuê bao số (digital subscriber line - DSL), bus nối tiếp vạn năng (universal serial bus - USB) hoặc các cơ chế khác.

Giao diện người sử dụng 72 có thể truyền thông với bộ xử lý 70 để nhận chỉ báo của đầu vào người sử dụng tại giao diện người sử dụng 72 và/hoặc để cung cấp tín hiệu nghe được, trực quan, cơ học hoặc đầu ra khác tới người sử dụng. Do đó, giao diện người sử dụng 72 có thể bao gồm, ví dụ, bàn phím, chuột, cần điều chỉnh, màn hình hiển thị, màn hình chạm, các phím mềm, micô, loa hoặc các cơ chế đầu vào/đầu ra khác. Theo phương án ví dụ, trong đó thiết bị được áp dụng làm máy chủ hoặc các thiết bị mạng khác, giao diện người sử dụng 72 có thể bị hạn chế hoặc bị loại bỏ.

Tuy nhiên, theo phương án trong đó thiết bị được áp dụng trong thiết bị truyền thông (ví dụ, thiết bị đầu cuối di động 10), giao diện người sử dụng 72, ngoài các bộ phận hoặc các

thành phần khác, có thể bao gồm bất kỳ hoặc tất cả loa, micrô, màn hình hiển thị và bàn phím hoặc tương tự. Theo đó, ví dụ, bộ xử lý 70 có thể bao gồm mạch giao diện người sử dụng được tạo cấu hình để điều khiển ít nhất một số chức năng của một hoặc nhiều thành phần của giao diện người sử dụng, như, ví dụ, loa, chuông, micrô, màn hình hiển thị, và/hoặc tương tự. Bộ xử lý 70 và/hoặc mạch giao diện người sử dụng bao gồm bộ xử lý 70 có thể được tạo cấu hình để điều khiển một hoặc nhiều chức năng của một hoặc nhiều thành phần của giao diện người sử dụng qua các lệnh chương trình máy tính (ví dụ, phần mềm và/hoặc phần sụn) được lưu trữ trên bộ nhớ truy cập được bởi bộ xử lý 70 (ví dụ, thiết bị lưu trữ 76, và/hoặc tương tự).

Theo một phương án làm ví dụ, bộ xử lý 70, bao gồm hoặc theo cách khác, có thể được áp dụng điều khiển bộ phát hiện điều kiện không ăn khớp 80 và bộ quản lý tính hiệu lực của khóa 82. Bộ phát hiện điều kiện không ăn khớp 80 theo phương án này có thể còn bao gồm hoặc theo cách khác được áp dụng như bộ phát hiện thất bại chuyển giao UE 84. Bộ phát hiện điều kiện không ăn khớp 80, bộ quản lý tính hiệu lực của khóa 82 và bộ phát hiện thất bại chuyển giao UE 84, mỗi bộ có thể là các phương tiện bất kỳ như thiết bị hoặc mạch vận hành theo phần mềm hoặc theo cách khác được áp dụng trong phần cứng hoặc tổ hợp của phần cứng và phần mềm (ví dụ, bộ xử lý 70 vận hành dưới điều khiển của phần mềm, bộ xử lý 70 được áp dụng như là ASIC hoặc FPGA được tạo cấu hình một cách cụ thể để thực hiện các bước được mô tả ở đây hoặc tổ hợp của chúng) nhờ đó tạo cấu hình cho thiết bị hoặc mạch để thực thi các chức năng tương ứng của bộ phát hiện điều kiện không ăn khớp 80, bộ quản lý tính hiệu lực của khóa 82 và bộ phát hiện thất bại chuyển giao UE 84, một cách tương ứng, như được mô tả ở đây. Do đó, trong các ví dụ, trong đó phần mềm được sử dụng, thiết bị hoặc mạch (ví dụ, bộ xử lý 70 trong một ví dụ) thực thi phần mềm tạo thành kết cấu được kết hợp với các phương tiện này.

Bộ phát hiện điều kiện không ăn khớp 80, từ khía cạnh của UE 10, có thể được tạo cấu hình để xác định xem liệu các điều kiện có tồn tại, các điều kiện mà có thể là các bộ chỉ báo về sự không ăn khớp giữa UE 10 và MSC 32 xét về các bộ khóa CS được lưu trữ ở đó. Theo đó, ví dụ, bộ phát hiện điều kiện không ăn khớp 80 có thể được tạo cấu hình để quản lý lưu lượng tin nhắn và hoạt động của UE 10 đáp lại việc tạo ra khóa CS mới khi hoạt động chuyển giao liên miền theo thứ tự để xác định xem liệu có gặp các chỉ báo của điều kiện không ăn khớp

tiềm tàng của khóa hay không. Đáp lại việc gặp phải các chỉ báo của điều kiện không ăn khớp tiềm tàng của khóa, bộ phát hiện điều kiện không ăn khớp 80 theo một phương án ví dụ được tạo cấu hình để thông báo hoặc theo cách khác thông báo cho bộ quản lý tính hiệu lực của khóa 82.

Bộ phát hiện thất bại chuyển giao UE 84 có thể được tạo cấu hình để phát hiện chỉ báo cụ thể có thể phát hiện được tại UE 10 để chỉ báo thất bại chuyển giao hoặc theo cách khác là thất bại hoạt động chuyển giao liên miền từ khía cạnh UE. Cụ thể, ví dụ, bộ phát hiện thất bại chuyển giao UE 84 có thể được tạo cấu hình để xác định xem liệu mạng có xác nhận việc hoàn thành chuyển giao hay không (ví dụ, tin nhắn hoàn thành chuyển giao). Thất bại để nhận xác nhận bất kỳ sự hoàn thành chuyển giao có thể chỉ báo thất bại chuyển giao. Ngoài ra hoặc theo cách khác, bộ phát hiện thất bại chuyển giao UE 84 có thể được tạo cấu hình để xác đinh xem liệu UE 10 có đạt được việc đồng bộ Lớp 1 (ví dụ, LI sync) hay không. Thất bại của UE10 để đạt được LI sync cũng có thể là chỉ báo thất bại chuyển giao. Ngoài ra hoặc theo cách khác, bộ phát hiện thất bại chuyển giao UE 84 có thể được tạo cấu hình để xác định xem liệu lệnh chuyển giao nhận được có chứa các cấu hình hiệu lực hay không. Việc phát hiện cấu hình không hiệu lực bất kỳ và/hoặc cấu hình không được hỗ trợ bất kỳ cũng là chỉ báo thất bại chuyển giao. Ngoài ra hoặc theo cách khác, bộ phát hiện thất bại chuyển giao UE 84 có thể được tạo cấu hình để xác định xem liệu các UE 10 có thực hiện dự phòng thất bại chuyển giao (handover failure fallback) hay không, do đó nỗ lực nên là chỉ báo thất bại chuyển giao. Các bộ chỉ báo tiềm tàng khác của thất bại chuyển giao, theo cách khác hoặc ngoài ra, có thể được phát hiện bởi bộ phát hiện thất bại chuyển giao UE 84.

Bộ phát hiện thất bại chuyển giao UE 84 có thể được tạo cấu hình để, đại diện cho bộ phát hiện điều kiện không ăn khớp 80, thông báo hoặc theo cách khác thông báo cho bộ quản lý tính hiệu lực của khóa 82 về sự tồn tại của các chỉ báo điều kiện không ăn khớp tiềm tàng của khóa đáp lại việc việc xác định chỉ báo bất kỳ của các chỉ báo được mô tả ở trên là chỉ báo thất bại chuyển giao. Bộ quản lý tính hiệu lực của khóa 82 sau đó có thể thay đổi hoạt động tại UE 10 như được mô tả ở dưới. Tuy nhiên, trong các tính huống mà trong đó bộ phát hiện điều kiện không ăn khớp 80 (hoặc bộ phát hiện thất bại chuyển giao UE 84) không tạo tín hiệu điều

kiện không ăn khớp tiềm tàng của khóa, UE 10 có thể lưu trữ bộ khóa mới được tạo ra theo các quy trình chuyển giao liên miền thông thường.

Đáp lại việc nhận chỉ báo từ bộ phát hiện điều kiện không ăn khớp 80 (hoặc bộ phát hiện thất bại chuyển giao UE 84) về điều kiện không ăn khớp tiềm tàng của khóa đã gặp phải, bộ quản lý tính hiệu lực của khóa 82 có thể được tạo cấu hình để thực hiện việc làm bất hiệu lực bộ khóa mới nhận được trong (U)SIM. Việc làm bất hiệu lực bộ khóa mới có thể bao gồm hoặc dẫn đến việc xóa bộ khóa này hoặc chỉ định chỉ báo được gắn vào hoặc được kết hợp với bộ khóa để chỉ báo trạng thái hiệu lực của bộ khóa. Bộ khóa mới có thể có các bộ khóa ăn khớp khác được sử dụng trong quá khứ. Theo đó, các bộ khóa khác với bộ khóa nhận diện (KSI hoặc CKSN) ăn khớp các khóa được ánh xạ được kết hợp với bước chuyển giao liên miền mà có thể bị nhầm lẫn trong kết nối kế tiếp có thể cũng bị làm mất hiệu lực bởi bộ quản lý tính hiệu lực của khóa 82. Đáp lại việc làm bất hiệu lực các khóa được ánh xạ bởi bộ quản lý tính hiệu lực của khóa 82, việc trao đổi khóa mới có thể bị ép (ví dụ, thông qua quy trình AKA). Bằng cách ép việc trao đổi khóa mới theo cách được điều khiển, như được mô tả ở trên, trong các tình huống mà gặp phải điều kiện không ăn khớp tiềm tàng của khóa trong đó, bộ quản lý tính hiệu lực của khóa 82 có thể quản lý tính hiệu lực của khóa tại UE 10 theo cách tương tự để ngăn cản hoặc ít nhất về cơ bản giảm khả năng gặp phải thất bại trong sự truyền thông hoặc hệ quả liên quan đến sự không ăn khớp của khóa mà không được giải quyết một cách chủ động (ví dụ, thông qua quy trình AKA). Đáp lại việc bộ khóa mới được chỉ báo tại phía UE 10 như được làm bất hoạt bởi bộ quản lý tính hiệu lực của khóa 82, bộ quản lý tính hiệu lực của khóa 82 có thể được xem xét đáp lại quyết định rằng phía mạng đã không thể nhận được xác nhận việc chuyển giao thành công và lưu trữ một cách phù hợp cùng một bộ khóa mới (ví dụ, nhờ các chỉ báo sự không ăn khớp tiềm tàng của khóa được phát hiện bởi bộ phát hiện thất bại chuyển giao UE 84) bằng cách làm bất hiệu lực bộ khóa mới tại phía UE 10. Đáp lại bộ khóa mới được làm bất hiệu lực tại phía UE 10, bộ khóa hiệu lực mới nhất có thể được giữ lại để sử dụng cho tới khi bộ khóa mới có thể được cung cấp.

Theo đó, mặc dù việc không có khả năng cố hữu hiện tại đảm bảo sự đồng bộ của việc lưu trữ các khóa được ánh xạ ở cả phía mạng lẫn phía UE khi SR-VCC hoặc chuyển giao liên miền khác thất bại, thiết bị 50 có thể được tạo cấu hình để làm giảm khả năng không ăn khớp

của khóa liên quan tới các hệ quả truyền thông nhờ việc quản lý tính hiệu lực của bộ khóa dựa vào các chỉ báo sự không ăn khớp tiềm tàng của khóa. Các chỉ báo sự không ăn khớp tiềm tàng của khóa có thể được phát hiện dựa vào hoạt động của UE 10 và các tin nhắn nhận được tại UE 10 liên quan tới việc xác nhận chuyển giao thành công thông qua hoạt động chuyển giao liên miền.

Dựa vào Fig.3, thiết bị 50' để xử lý khóa sau khi thất bại thao tác chuyển giao liên miền được tạo ra. Thiết bị 50' có thể bao gồm hoặc theo cách khác truyền thông với bộ xử lý 70', giao diện truyền thông 74' và thiết bị lưu trữ 76'. Do đó, thiết bị 50' có thể tương tự với thiết bị 50 trên Fig.2, chỉ khác là nó được làm phù hợp để sử dụng tại thiết bị mạng thay cho tại UE 10. Do đó, ví dụ, thiết bị 50' có thể không nhất thiết có giao diện người sử dụng. Tuy nhiên, bộ xử lý 70', giao diện truyền thông 74' và thiết bị lưu trữ 76' có thể có chức năng tương tự với các bộ phận tương ứng của thiết bị 50 trên Fig.2.

Theo phương án ví dụ, bao gồm hoặc theo cách khác, bộ xử lý 70' có thể được áp dụng để bao gồm hoặc theo cách khác điều khiển bộ phát hiện điều kiện không ăn khớp 80' và bộ quản lý tính hiệu lực của khóa 82'. Bộ phát hiện điều kiện không ăn khớp 80' và bộ quản lý tính hiệu lực của khóa 82' theo phương án này lần lượt có thể tương tự với bộ phát hiện điều kiện không ăn khớp 80 và bộ quản lý tính hiệu lực của khóa 82, trên Fig.2 chỉ khác là các thành phần này vận hành từ một khía cạnh khác (ví dụ, khía cạnh mạng).

Theo một phương án làm ví dụ, bộ phát hiện điều kiện không ăn khớp 80', bao gồm hoặc theo cách khác, có thể còn được áp dụng làm bộ phát hiện thất bại chuyển giao mạng 86 cũng có thể tương tự như bộ phát hiện thất bại chuyển giao UE 84 trên Fig.2 chỉ khác là bộ này vận hành từ khía cạnh của thiết bị mạng hơn là khía cạnh của UE. Sự vận hành của bộ phát hiện thất bại chuyển giao mạng 86 sẽ được mô tả trong chi tiết hơn bên dưới.

Bộ phát hiện điều kiện không ăn khớp 80', bộ quản lý tính hiệu lực của khóa 82' và bộ phát hiện thất bại chuyển giao mạng 86, mỗi bộ có thể là các phương tiện bất kỳ như thiết bị hoặc mạch vận hành theo phần mềm hoặc theo cách khác được áp dụng trong phần cứng hoặc tổ hợp của phần cứng và phần mềm (ví dụ, bộ xử lý 70' vận hành dưới sự điều khiển của phần mềm, bộ xử lý 70' được áp dụng làm ASIC hoặc FPGA được tạo cấu hình đặc biệt để thực hiện các bước được mô tả ở đây hoặc tổ hợp của chúng) nhờ đó tạo cấu hình thiết bị hoặc

mạch để thực thi các chức năng tương ứng lần lượt của bộ phát hiện điều kiện không ăn khớp 80', bộ quản lý tính hiệu lực của khóa 82' và bộ phát hiện thất bại chuyển giao mạng 86, như được mô tả ở đây. Do đó, trong ví dụ trong đó phần mềm được áp dụng, thiết bị hoặc mạch (ví dụ, bộ xử lý 70' theo một ví dụ) thực thi phần mềm tạo thành kết cấu được kết hợp với các phương tiện này.

Bộ phát hiện điều kiện không ăn khớp 80' có thể được tạo cấu hình để xác định, từ khía cạnh mạng, xem liệu các điều kiện có tồn tại hay không, các điều kiện này có thể là các bộ chỉ báo sự không ăn khớp có thể xảy ra giữa UE 10 và MSC 32 xét về các bộ khóa CS được lưu trữ ở đó. Theo đó, ví dụ, bộ phát hiện điều kiện không ăn khớp 80' có thể được tạo cấu hình để quản lý lưu lượng tin nhắn và hoạt động của mạng đáp lại việc tạo khóa CS mới tới UE 10 trong suốt thao tác chuyển giao liên miền theo thứ tự để xác định xem liệu có gặp phải các chỉ báo điều kiện không ăn khớp tiềm tàng của khóa hay không. Đáp lại việc gặp phải các chỉ báo của điều kiện không ăn khớp tiềm tàng của khóa, bộ phát hiện điều kiện không ăn khớp 80' theo phương án ví dụ được tạo cấu hình để thông báo hoặc theo cách khác thông báo cho bộ quản lý tính hiệu lực của khóa 82'.

Bộ phát hiện thất bại chuyển giao mạng 86 có thể được tạo cấu hình để phát hiện chỉ báo cụ thể có thể phát hiện được tại mạng (ví dụ, tại MSC 32, MME 36 hoặc SGSN 34) để chỉ báo thất bại chuyển giao hoặc theo cách khác thất bại thao tác chuyển giao liên miền từ khía cạnh UE. Cụ thể, ví dụ, bộ phát hiện thất bại chuyển giao mạng 86 có thể được tạo cấu hình để xác định xem liệu mạng có nhận được chỉ báo hoàn thành chuyển giao (ví dụ, tin nhắn hoàn thành chuyển giao) từ UE 10 hay không. Thất bại cho việc nhận chỉ báo hoàn thành chuyển giao có thể là chỉ báo thất bại chuyển giao. Ngoài ra hoặc theo cách khác, bộ phát hiện thất bại chuyển giao mạng 86 có thể được tạo cấu hình để xác định xem liệu có đạt được sự đồng bộ của Lớp 1 (LI sync) hay không. Thất bại trong việc đạt được LI sync có thể cũng là chỉ báo thất bại chuyển giao. Các bộ chỉ báo thất bại chuyển giao tiềm tàng khác, theo cách khác hoặc ngoài ra, có thể được phát hiện bởi bộ phát hiện thất bại chuyển giao mạng 86.

Bộ phát hiện thất bại chuyển giao mạng 86 có thể được tạo cấu hình để, nhân danh cho bộ phát hiện điều kiện không ăn khớp 80', thông báo hoặc theo cách khác thông báo cho bộ quản lý tính hiệu lực của khóa 82' sự tồn tại của các chỉ báo điều kiện không ăn khớp tiềm

tàng của khóa đáp lại việc xác định chỉ báo bất kỳ trong số các chỉ báo được mô tả ở trên vốn là chỉ báo thất bại chuyển giao. Bộ quản lý tính hiệu lực của khóa 82' sau đó có thể thay đổi hoạt động tại mạng (ví dụ, tại MSC 32, MME 36 hoặc SGSN 34) như được mô tả bên dưới. Tuy nhiên, trong các tình huống mà trong đó bộ phát hiện điều kiện không ăn khớp 80' (hoặc bộ phát hiện thất bại chuyển giao mạng 86) không tạo tín hiệu điều kiện không ăn khớp tiềm tàng của khóa, MSC 32 có thể lưu trữ bộ khóa CS mới được tạo ra cho UE 10 theo các quy trình hoạt động chuyển giao liên miền thông thường.

Đáp lại việc nhận chỉ báo từ bộ phát hiện điều kiện không ăn khớp 80' (hoặc bộ phát hiện thất bại chuyển giao mạng 86) về việc gặp phải điều kiện không ăn khớp tiềm tàng của khóa, bộ quản lý tính hiệu lực của khóa 82' có thể được tạo cấu hình để điều khiển việc làm bất hiệu lực bộ khóa mới. Việc làm bất hiệu lực bộ khóa mới có thể bao gồm hoặc dẫn đến việc xóa bộ khóa này hoặc chỉ định chỉ báo được kết nối với hoặc được kết hợp với bộ khóa để chỉ báo trạng thái hiệu lực của bộ khóa. Đáp lại việc làm bất hiệu lực các khóa được ánh xạ bởi bộ quản lý tính hiệu lực của khóa 82', việc trao đổi khóa mới có thể được ép (ví dụ, thông qua quy trình AKA). Bằng cách ép trao đổi khóa mới theo cách được điều khiển, như được mô tả ở trên, trong các tình huống, trong đó gặp phải điều kiện không ăn khớp tiềm tàng của khóa, bộ quản lý tính hiệu lực của khóa 82' có thể quản lý tính hiệu lực của khóa tại mạng theo cách giống như để ngăn ngừa hoặc ít nhất về cơ bản là làm giảm sự hiệu lực của việc gặp phải thất bại truyền thông hoặc các hệ quả liên quan đến việc không ăn khớp của khóa mà không được giải quyết một cách chủ động (ví dụ, thông qua quy trình AKA).

Đáp lại việc bộ khóa mới được chỉ báo tại phía mạng khi bị làm bất hiệu lực bởi bộ quản lý tính hiệu lực của khóa 82', bộ quản lý tính hiệu lực của khóa 82' có thể được xem xét để đáp lại việc xác định rằng phía UE 10 cũng không thể nhận và lưu trữ cùng một bộ khóa mới một cách phù hợp (ví dụ, nhờ các chỉ báo sự không ăn khớp tiềm tàng của khóa được phát hiện bởi bộ phát hiện thất bại chuyển giao mạng 86) bằng cách làm bất hiệu lực bộ khóa mới tại phía mạng. Đáp lại việc bộ khóa mới được làm bất hiệu lực tại phía mạng (ví dụ, bởi MSC 32, MME 36 hoặc SGSN 34), bộ khóa hiệu lực mới nhất có thể được giữ lại để sử dụng cho tới khi bộ khóa mới có thể được tạo ra.

Theo đó, mặc dù việc không có khả năng cố hữu hiện tại đảm bảo việc đồng bộ của các khóa được ánh xạ được lưu trữ trong cả phía mạng và phía UE khi thất bại chuyển giao liên miền, thiết bị 50' có thể được tạo cấu hình để làm giảm sự hiệu lực của việc không ăn khớp của sự phức tạp truyền thông liên quan tới khóa bằng cách quản lý tính hiệu lực của bộ khóa dựa vào các chỉ báo sự không ăn khớp tiềm tàng của khóa. Các chỉ báo sự không ăn khớp tiềm tàng của khóa có thể được phát hiện dựa vào hoạt động của mạng và các tin nhắn nhận được tại mạng liên quan tới việc xác định chuyển giao thành công thông qua hoạt động chuyển giao liên miền.

Fig.4 là lưu đồ của hệ thống, phương pháp và sản phẩm chương trình theo các phương án ví dụ của sáng chế. Cần hiểu rằng, mỗi khối hoặc bước của lưu đồ và tổ hợp của các khối trong lưu đồ, có thể được áp dụng bởi các phương tiện khác nhau, như phần cứng, phần sụn, bộ xử lý, mạch và/hoặc bộ phận khác được kết hợp với việc thực thi phần mềm chứa một hoặc nhiều lệnh chương trình máy tính. Ví dụ, một hoặc nhiều thủ tục trong các thủ tục được mô tả ở trên có thể được áp dụng bởi các lệnh chương trình máy tính. Theo đó, các lệnh chương trình máy tính áp dụng các thủ tục được mô tả ở trên có thể được lưu trữ bởi thiết bị lưu trữ của thiết bị áp dụng phương án của sáng chế và được thực thi bởi bộ xử lý trong thiết bị. Cần hiểu rằng, các lệnh chương trình máy tính bất kỳ này có thể được tải lên trên máy tính hoặc thiết bị lập trình được khác (ví dụ, phần cứng) để tạo ra cỗ máy, sao cho máy tính được tạo ra hoặc thiết bị lập trình được khác bao gồm các phương tiện để thực thi các chức năng được chỉ rõ trong (các) khối hoặc (các) bước của lưu đồ. Các lệnh chương trình máy tính này cũng có thể được lưu trữ trong bộ nhớ đọc được bằng máy tính (trái với môi trường truyền đọc được bằng máy tính như sóng mang hoặc tín hiệu điện từ) có thể điều khiển máy tính hoặc thiết bị lập trình được khác thực hiện chức năng theo cách cụ thể, sao cho các lệnh được lưu trữ trong bộ nhớ đọc được bằng máy tính tạo ra vật phẩm để thực thi các chức năng được chỉ rõ trong (các) khối hoặc (các) bước của lưu đồ. Các lệnh chương trình máy tính cũng được tải lên trên máy tính hoặc thiết bị lập trình được khác để thực hiện chuỗi các bước vận hành để thực thi trên máy tính hoặc thiết bị lập trình được khác để tạo quy trình thực thi trên máy tính sao cho các lệnh thực hiện thi máy tính hoặc thiết bị lập trình được khác tạo ra các bước để thực thi các chức năng được chỉ rõ trong (các) khối hoặc (các) bước của lưu đồ.

Theo đó, các khối hoặc các bước của lưu đồ hỗ trợ tổ hợp của các phương tiện để thực hiện các chức năng cụ thể, tổ hợp của các bước để thực thi các chức năng cụ thể và các phương tiện lệnh chương trình để thực hiện các chức năng cụ thể. Cũng cần hiểu rằng, một hoặc nhiều khối hoặc các bước của lưu đồ và tổ hợp của các khối hoặc các bước trong lưu đồ, có thể được áp dụng bởi các hệ thống máy tính dựa vào phần cứng chuyên dụng thực thi các chức năng hoặc các bước cụ thể hoặc tổ hợp của phần cứng chuyên dụng và các lệnh máy tính.

Theo đó, một phương án của phương pháp để xử lý khóa sau khi thất bại chuyển giao tiềm tàng theo một phương án ví dụ, như được thể hiện trên Fig.4 bao gồm việc xác định xem liệu chỉ báo sự không ăn khớp tiềm tàng của khóa có hiện diện đáp lại nỗ lực thực hiện chuyển giao giữa miền thứ nhất (ví dụ, miền PS) và miền thứ hai (miền khác) (ví dụ, miền CS) tại bước 100. Phương pháp có thể còn bao gồm bước xác định tính hiệu lực của bộ khóa mới nhất (ví dụ, bộ khóa CS) được sử dụng để mã hóa truyền thông giữa thiết bị đầu cuối di động và thiết bị mạng dựa vào kết quả xác định tại bước 110.

Theo nhiều phương án, phương pháp có thể bao gồm các bước tùy chọn bổ sung, ví dụ về chúng được thể hiện bởi các đường đứt trên Fig.4. Do đó, ví dụ, phương pháp có thể còn bao gồm bước khởi tạo việc trao đổi khóa mới đáp lại việc làm bất hoạt bộ khóa mới nhất tại bước 120.

Trong nhiều phương án, các hạng mục cụ thể của các bước nêu trên có thể được biến đổi hoặc được khuếch đại như được mô tả ở dưới. Các cải biến hoặc các khuếch đại cho các bước nêu trên có thể được thực hiện theo thứ tự hoặc tổ hợp bất kỳ. Theo đó, ví dụ, việc xác định xem liệu chỉ báo sự không ăn khớp tiềm tàng của khóa có mặt hay không có thể bao gồm việc xác định xem liệu xác nhận từ thiết bị mạng của tin nhắn hoàn thành chuyển giao được gửi bởi thiết bị đầu cuối di động có được nhận tại thiết bị đầu cuối di động hay không. Ngoài ra hoặc theo cách khác, việc xác định xem liệu chỉ báo sự không ăn khớp tiềm tàng của khóa có mặt hay không có bao gồm xác định xem liệu việc đồng bộ lớp 1 có được xác định hay không. Theo lựa chọn khác hoặc lựa chọn bổ sung, việc xác định xem liệu chỉ báo sự không ăn khớp tiềm tàng của khóa là có mặt hay không có thể bao gồm việc xác định xem liệu thiết bị đầu cuối di động có thực hiện dự phòng thất bại chuyển giao hay không, theo phương án khác, việc xác định xem liệu chỉ báo sự không ăn khớp tiềm tàng của khóa có mặt hay không có thể

bao gồm việc xác định xem liệu lệnh chuyển giao nhận được có chứa cấu hình hiệu lực hay không. Theo một số phương án, việc xác định xem liệu chỉ báo sự không ăn khớp tiềm tàng của khóa có mặt hay không có thể bao gồm việc xác định xem liệu tin nhắn hoàn thành chuyển giao có nhận được từ thiết bị đầu cuối di động tại thiết bị mạng hay không. Theo một phương án ví dụ, việc xác định tính hiệu lực của bộ khóa mới nhất có thể bao gồm việc làm mất hiệu lực bộ khóa mới nhất, tại thiết bị mạng hoặc tại thiết bị đầu cuối di động, đáp lại sự hiện diện của chỉ báo sự không ăn khớp tiềm tàng của khóa.

Theo phương án ví dụ, thiết bị để thực hiện phương pháp trên Fig.4 ở trên có thể bao gồm một hoặc nhiều bộ xử lý (ví dụ, bộ xử lý 70 hoặc 70') được tạo cấu hình để thực hiện một số hoặc mỗi bước (100-120) được mô tả ở trên. Bộ xử lý ví dụ có thể được tạo cấu hình để thực hiện các bước (100-120) bằng việc thực hiện các chức năng logic được thực thi bởi phần cứng, thực thi các lệnh được lưu trữ hoặc thực thi các thuật toán để thực hiện mỗi một trong số các bước.

Theo cách khác, thiết bị có thể bao gồm các phương tiện để thực hiện mỗi bước trong số các bước được mô tả ở trên. Theo đó, theo phương án ví dụ, các ví dụ về các phương tiện để thực hiện các bước 100-120 có thể bao gồm, ví dụ, bộ xử lý 70 hoặc 70', bộ phát hiện tương ứng trong số bộ phát hiện điều kiện không ăn khớp 80 hoặc 80', bộ quản lý tính hiệu lực của khóa 82 hoặc 82', bộ phát hiện thất bại chuyển giao UE 84, bộ phát hiện thất bại chuyển giao mạng 86, và/hoặc thiết bị hoặc mạch để thực thi các lệnh hoặc thực thi thuật toán để xử lý thông tin như mô tả ở trên.

Ví dụ về thiết bị theo phương án ví dụ có thể bao gồm ít nhất một bộ xử lý và ít nhất một bộ nhớ chứa mã chương trình máy tính. Ít nhất một bộ nhớ và mã chương trình máy tính có thể được tạo cấu hình để, với ít nhất một bộ xử lý, khiến cho thiết bị thực hiện các bước 100-120 (có hoặc không có các cải biến mô tả ở trên). Ví dụ về sản phẩm chương trình máy tính theo phương án ví dụ có thể bao gồm ít nhất một vật ghi đọc được bằng máy tính có các phần mã chương trình thực thi được bằng máy tính được lưu trữ ở đó. Các phần mã chương trình thực hiện được bởi máy tính có thể bao gồm các lệnh mã chương trình để thực hiện bước 100-120 (có hoặc không có các thay đổi ở trên). Nhiều thay đổi và các phương án khác của sáng chế được chỉ ra ở đây sẽ là hiển nhiên với người có hiểu biết trung bình trong lĩnh vực,

trong đó sáng chế có lợi từ các chỉ dẫn được chỉ ra trong phần mô tả nêu trên và các hình vẽ được kết hợp. Do đó, cần hiểu rằng sáng chế không bị giới hạn ở các phương án cụ thể được bộc lộ và các cải biến và các phương án khác nhằm mục đích nằm trong phạm vi của các điểm yêu cầu bảo hộ kèm theo. Hơn nữa, mặc dù các phần mô tả trên và các hình vẽ được kết hợp mô tả các phương án ví dụ trong ngữ cảnh của tổ hợp các thành phần và/hoặc các chức năng ví dụ nhất định, cần hiểu rằng tổ hợp các thành phần và/hoặc các chức năng khác nhau có thể được tạo ra bởi các phương án thay thế mà không trệch khỏi mục đích và phạm vi của các yêu cầu bảo hộ kèm theo. Ví dụ, tổ hợp các thành phần và/hoặc các chức năng khác nhau khác được mô tả cụ thể ở trên cũng được thực hiện như được chỉ ra trong một số điểm yêu cầu bảo hộ kèm theo. Mặc dù các thuật ngữ chung được sử dụng ở đây, nhưng các thuật ngữ này được sử dụng theo nghĩa chung và nghĩa mô tả và không nhằm mục đích giới hạn sáng chế.

YÊU CẦU BẢO HỘ

1. Thiết bị xác định tính hiệu lực của bộ khóa, thiết bị này bao gồm:

ít nhất một bộ xử lý và ít nhất một bộ nhớ chứa mã chương trình máy tính được tạo cấu hình để, với bộ xử lý, khiến cho thiết bị ít nhất:

xác định xem liệu sự không ăn khớp tiềm tàng của khóa có tồn tại không, đáp lại nỗ lực thực hiện chuyển giao giữa miền thứ nhất và miền thứ hai, trong đó sự tồn tại của sự không ăn khớp tiềm tàng của khóa được xác định bởi ít nhất một trong số việc kiểm tra xem liệu có nhận được xác nhận đối với tin nhắn kết thúc chuyển giao hay không; và kiểm tra xem liệu đồng bộ hóa lớp 1 có xảy ra hay không; và

xác định tính hiệu lực của bộ khóa mới nhất được sử dụng để mã hóa truyền thông giữa thiết bị đầu cuối di động và thiết bị mạng, dựa vào kết quả xác định trên.

2. Thiết bị theo điểm 1, trong đó trong bộ nhớ và mã chương trình máy tính còn được tạo cấu hình để, với bộ xử lý, khiến cho thiết bị khởi tạo việc thay đổi khóa mới đáp lại việc mất hiệu lực của bộ khóa mới nhất.

3. Thiết bị theo điểm 1, trong đó sự tồn tại của sự không ăn khớp tiềm tàng của khóa còn được xác định bởi ít nhất việc kiểm tra xem liệu thiết bị đầu cuối di động có thực hiện dự phòng thất bại chuyển giao hay không.

4. Thiết bị theo điểm 1, trong đó sự tồn tại của sự không ăn khớp tiềm tàng của khóa còn được xác định bởi ít nhất việc kiểm tra xem liệu lệnh chuyển giao nhận được bao gồm các cấu hình hiệu lực hay không.

5. Thiết bị theo điểm 1, trong đó sự tồn tại của sự không ăn khớp tiềm tàng của khóa còn được xác định bởi ít nhất việc kiểm tra xem liệu có nhận được tin nhắn kết thúc chuyển giao từ thiết bị đầu cuối di động tại thiết bị mạng hay không.

6. Thiết bị theo điểm 1, trong đó bộ nhớ và mã chương trình máy tính được tạo cấu hình để, với bộ xử lý, khiến cho thiết bị xác định tính hiệu lực của bộ khóa mới nhất bằng cách làm mất hiệu lực bộ khóa mới nhất, tại thiết bị mạng hoặc tại thiết bị đầu cuối di động, đáp lại sự tồn tại của chỉ báo không ăn khớp tiềm tàng của khóa.

7. Thiết bị theo điểm 1, trong đó thiết bị là thiết bị đầu cuối di động và còn bao gồm mạch giao diện người sử dụng được tạo cấu hình để hỗ trợ người sử dụng điều khiển ít nhất một số chức năng của thiết bị đầu cuối di động.

8. Phương pháp xác định tính hiệu lực của bộ khóa, phương pháp này bao gồm các bước:

xác định xem liệu sự không ăn khớp tiềm tàng của khóa có tồn tại hay không, đáp lại nỗ lực thực hiện chuyển giao giữa miền thứ nhất và miền thứ hai, trong đó sự tồn tại của sự không ăn khớp tiềm tàng của khóa được xác định bởi ít nhất một trong số việc kiểm tra xem liệu có nhận được xác nhận đối với tin nhắn kết thúc chuyển giao hay không; và kiểm tra xem liệu đồng bộ hóa lớp 1 có xảy ra hay không; và

xác định tính hiệu lực của bộ khóa mới nhất được sử dụng để mã hóa truyền thông giữa thiết bị đầu cuối di động và thiết bị mạng, dựa vào kết quả xác định trên.

9. Phương pháp theo điểm 8, trong đó phương pháp này còn bao gồm bước khởi tạo việc thay đổi khóa mới đáp lại việc mất hiệu lực của bộ khóa mới nhất.

10. Phương pháp theo điểm 8, trong đó sự tồn tại của sự không ăn khớp tiềm tàng của khóa còn được xác định bởi ít nhất việc kiểm tra xem liệu thiết bị đầu cuối di động có thực hiện dự phòng thất bại chuyển giao không.

11. Phương pháp theo điểm 8, trong đó sự tồn tại của sự không ăn khớp tiềm tàng của khóa còn được xác định bởi ít nhất việc kiểm tra xem liệu lệnh chuyển giao nhận được bao gồm các cấu hình hiệu lực hay không.

12. Phương pháp theo điểm 8, trong đó sự tồn tại của sự không ăn khớp tiềm tàng của khóa còn được xác định bởi ít nhất việc kiểm tra xem liệu có nhận được tin nhắn kết thúc chuyển giao từ thiết bị đầu cuối di động tại thiết bị mạng hay không.

13. Phương pháp theo điểm 8, trong đó việc xác định tính hiệu lực của bộ khóa mới nhất bao gồm việc làm mất hiệu lực bộ khóa mới nhất, tại thiết bị mạng hoặc tại thiết bị đầu cuối di động, đáp lại sự tồn tại của chỉ báo không ăn khớp tiềm tàng của khóa.

14. Vật ghi đọc được bằng máy tính bất khả biến chứa mã chương trình máy tính, mã chương trình máy tính được thực thi bởi ít nhất một bộ xử lý để vận hành các thao tác bao gồm:

xác định xem liệu sự không ăn khớp tiềm tàng của khóa có tồn tại hay không, đáp lại nỗ lực thực hiện chuyển giao giữa miền thứ nhất và miền thứ hai, trong đó sự tồn tại của sự không ăn khớp tiềm tàng của khóa được xác định bởi ít nhất một trong việc kiểm tra xem liệu có nhận được xác nhận đối với tin nhắn kết thúc chuyển giao hay không; và kiểm tra xem liệu đồng bộ hóa lớp 1 có xảy ra hay không; và

xác định tính hiệu lực của bộ khóa mới nhất được sử dụng để mã hóa truyền thông giữa thiết bị đầu cuối di động và thiết bị mạng, dựa vào kết quả xác định trên.

15. Vật ghi đọc được bằng máy tính bất khả biến theo điểm 14, trong đó vật ghi còn khởi tạo việc thay đổi khóa mới đáp lại việc mất hiệu lực của bộ khóa mới nhất.

16. Vật ghi đọc được bằng máy tính bất khả biến theo điểm 14, trong đó vật ghi còn làm mất hiệu lực bộ khóa mới nhất, tại thiết bị mạng hoặc tại thiết bị đầu cuối di động, đáp lại sự tồn tại của chỉ báo không ăn khớp tiềm tàng của khóa.

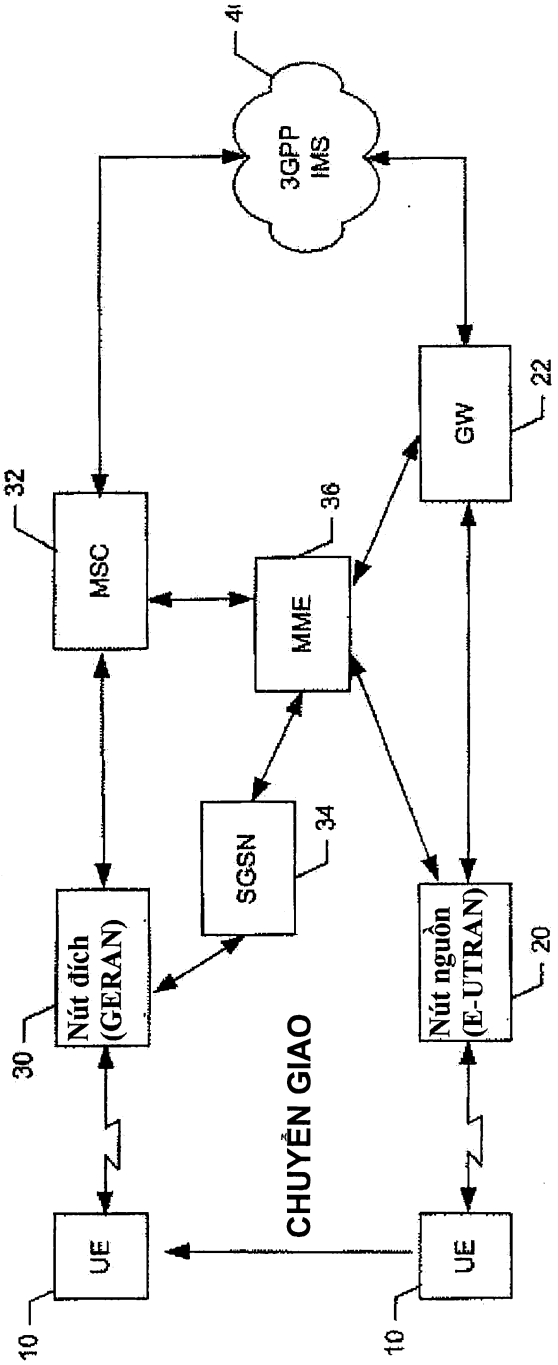

41
3GPP IMS
22
GW
32
MSC
36
MME
34
SGSN
Nút đích (GERAN)
30
Nút nguồn (E-UTRAN)
20
CHUYỂN GIAO
UE
10
UE
10

FIG. 1.

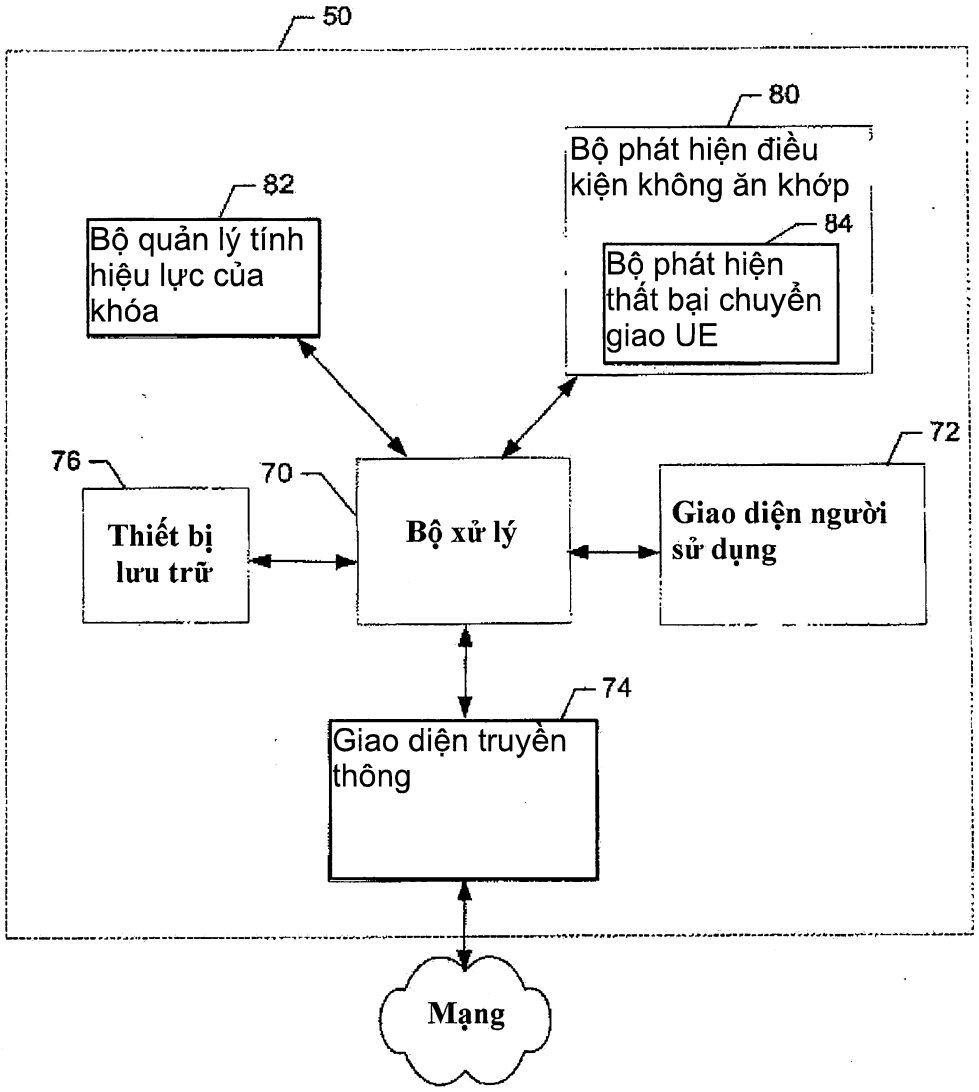

50
80
Bộ phát hiện điều kiện không ăn khớp
82
Bộ quản lý tính hiệu lực của khóa
84
Bộ phát hiện thất bại chuyển giao UE
76
70
72
Thiết bị lưu trữ
Bộ xử lý
Giao diện người sử dụng
74
Giao diện truyền thông
Mạng

FIG. 2.

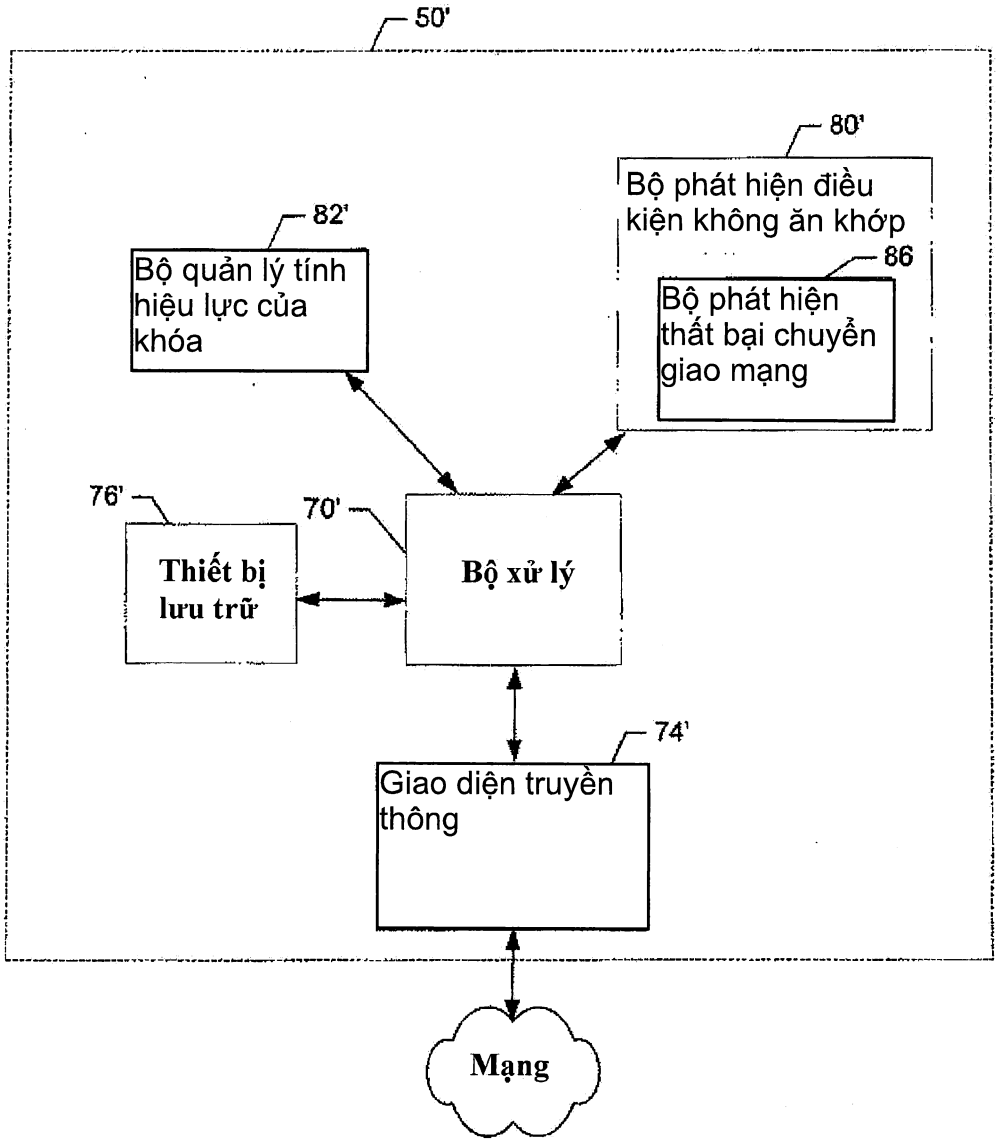

50'
80'
Bộ phát hiện điều kiện không ăn khớp
82'
Bộ quản lý tính hiệu lực của khóa
86
Bộ phát hiện thất bại chuyển giao mạng
76'
70'
Thiết bị lưu trữ
Bộ xử lý
74'
Giao diện truyền thông
Mạng

FIG. 3.

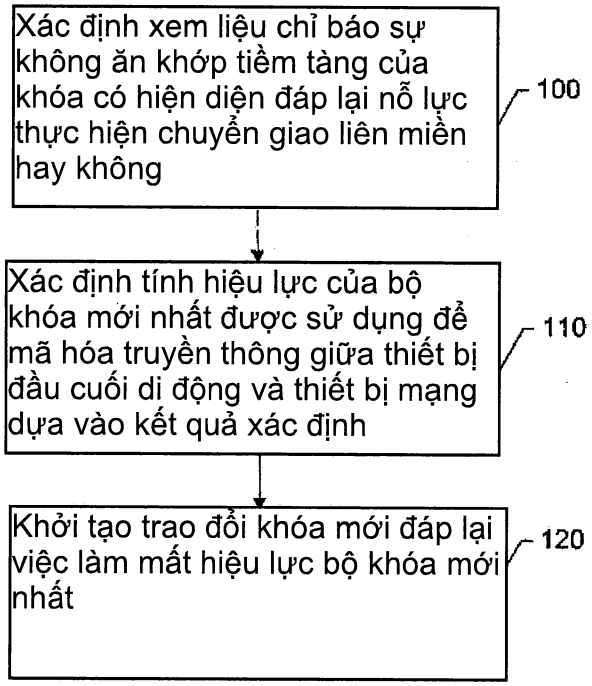

Xác định xem liệu chỉ báo sự không ăn khớp tiềm tàng của khóa có hiện diện đáp lại nỗ lực thực hiện chuyển giao liên miền hay không
100
Xác định tính hiệu lực của bộ khóa mới nhất được sử dụng để mã hóa truyền thông giữa thiết bị đầu cuối di động và thiết bị mạng dựa vào kết quả xác định
110
Khởi tạo trao đổi khóa mới đáp lại việc làm mất hiệu lực bộ khóa mới nhất
120

FIG. 4.