(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) **1-0021467**

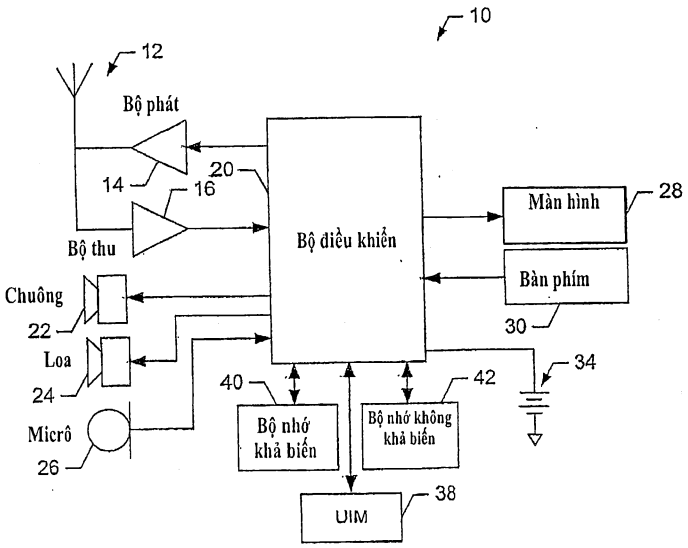
(51)[7] **H04L 29/06**

(13) **B**

(21) 1-2010-02636
(22) 30.03.2009
(86) PCT/IB2009/005129 30.03.2009
(87) WO2009/122260 08.10.2009
(30) 61/042,478 04.04.2008 US
61/043,857 10.04.2008 US
(45) 26.08.2019 377
(43) 25.07.2011 280
(73) Nokia Technologies OY (FI)
Karaportti 3, FI-02610 Espoo, Finland
(72) FORSBERG, Dan, Lars, Anders (FI), NIEMI, Pentti, Valtteri (FI), BLOMMAERT, Marc (BE)
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ THỰC HIỆN PHÂN TÁCH MẬT MÃ NHIỀU CHẶNG CHO VIỆC CHUYỂN GIAO

(57) Sáng chế đề cập đến phương pháp và thiết bị và vật ghi thực hiện phân tách khóa mật mã cho việc chuyển giao. Phương pháp được đề xuất bao gồm bước tính toán khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất được lưu từ trước. Phương pháp này cũng bao gồm bước tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào khóa tính toán được. Phương pháp này còn bao gồm bước gửi xác nhận chuyển đổi đường dẫn bao gồm giá trị trung gian thứ hai tới điểm truy cập đích. Phương pháp này có thể còn bao gồm bước nhận thông báo chuyển đổi đường dẫn bao gồm chỉ báo mã nhận diện tế bào và tính toán khóa mã hóa dựa vào chỉ báo mã nhận diện tế bào. Phương pháp này có thể còn bao gồm bước lưu giá trị trung gian thứ hai. Việc tính toán khóa có thể còn bao gồm tính toán khóa sau khi chuyển giao kết nối radio. Sáng chế cũng đề cập đến các thiết bị phân tách khóa mật mã cho việc chuyển giao và vật ghi.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến công nghệ truyền thông vô tuyến và, cụ thể hơn là đề cập tới thiết bị và phương pháp thực hiện phân tách khóa mật mã sau chuyển giao.

Tình trạng kỹ thuật của sáng chế

Các công nghệ hiện tại và các công nghệ trong tương lai tiếp tục tạo sự thuận tiện cho việc dễ dàng truyền thông tin và tiện lợi cho người sử dụng. Để tạo ra sự truyền thông dễ dàng hơn hoặc nhanh hơn cũng như tiện lợi hơn, các nhà cung cấp dịch vụ công nghiệp truyền thông viễn thông đang phát triển các cải tiến cho các mạng hiện hành. Ví dụ, hệ thống viễn thông di động toàn cầu cải tiến (Universal Mobile Telecommunications System-UMTS) mạng truy cập rađio vệ tinh (Evolved Universal Terrestrial Radio Access Network - E-UTRAN) hiện đang được phát triển. E-UTRAN, cũng được biết là công nghệ tiến hóa dài hạn (Long Term Evolution - LTE) hoặc 3.9G, nhằm mục đích nâng cấp các công nghệ trước đó bằng cách cải thiện hiệu suất, giảm giá thành, cải thiện các dịch vụ, tạo ra các cơ hội sử dụng phổ mới và giúp tích hợp tốt hơn với các chuẩn mở khác.

Một ưu điểm của E-UTRAN tiếp tục được chia sẻ với các tiêu chuẩn viễn thông khác trước đó là người sử dụng được phép truy cập mạng áp dụng các tiêu chuẩn này trong khi vẫn duy trì tính di động. Do đó, ví dụ, người sử dụng có các thiết bị đầu cuối di động được trang bị để truyền thông theo các tiêu chuẩn này có thể di chuyển qua các khoảng cách rất lớn trong khi vẫn duy trì truyền thông với mạng. Theo đó, hiện tại điểm truy cập hoặc trạm cơ sở đều bao phủ mạng cho vùng (hoặc tế bào) cụ thể, để chuyển tiếp truyền thông với thiết bị đầu cuối di động cụ thể tới trạm cơ sở lân cận khi người sử dụng thiết bị đầu cuối di động cụ thể thoát khỏi vùng phủ sóng của trạm cơ sở hoặc nếu không có thể được phục vụ hiệu quả hơn bởi trạm cơ sở lân cận. Quy trình này thường được đề cập đến là việc chuyển giao.

Một vấn đề tồn tại với việc chuyển giao trong E-UTRAN và các mạng truyền thông di động khác là vấn đề phân tách khóa mật mã giữa các điểm truy cập rađio. Theo đó, các thiết bị đầu cuối di động có thể truyền thông dữ liệu đã mã hóa qua các điểm truy cập rađio

hoặc các trạm cơ sở (được gọi là "các nút B cải tiến" hoặc "các eNB" trong E-UTRAN) sử dụng khóa mật mã đã biết cho thiết bị đầu cuối di động và điểm truy cập hoặc trạm cơ sở. Trong khi chuyển giao, khóa mật mã được sử dụng bởi thiết bị đầu cuối di động và nút B cải tiến hiện đang phục vụ của nó hoặc dạng phái sinh của khóa mật mã có thể được truyền thông với nút B cải tiến đích mà thiết bị đầu cuối di động được chuyển giao vào đó. Sau đó, nút B cải tiến đích có thể sử dụng khóa mật mã thu được từ nút B cải tiến trước đó. Do đó, các nút B cải tiến trước đó đã phục vụ thiết bị đầu cuối di động có thể biết hoặc theo cách khác có thể tính toán khóa mật mã hiện được sử dụng bởi thiết bị đầu cuối di động và nút B cải tiến phục vụ của nó và giải mã dữ liệu được truyền thông giữa thiết bị đầu cuối di động và nút B cải tiến hiện đang phục vụ, do đó dẫn đến mất tính bảo mật phân tách khóa mật mã.

Do đó, cần phát triển giao thức chuyển giao có thể tạo ra mức độ bảo mật cho việc phân tách khóa mật mã sao cho các nút B cải tiến trước đó có thể không có khả năng tạo ra khóa mật mã được sử dụng bởi thiết bị đầu cuối di động và nút B cải tiến hiện tại. Ngoài ra, còn mong muốn giao thức chuyển giao không đòi hỏi tài nguyên tốn thêm để xử lý hoặc truyền dữ liệu đáng kể đầu bởi thiết bị đầu cuối di động, nút B cải tiến, nút hỗ trợ dịch vụ radio gói chung (General Packet Radio Service Support Node - SGSN) (còn được gọi là "thực thể quản lý di động (Mobile Management Entity - MME)" trong E-UTRAN), hoặc cổng phục vụ (Serving Gateway - S-GW), sao cho việc chuyển giao và việc khôi phục truyền thông tiếp theo không bị trễ đáng kể.

Bản chất kỹ thuật của sáng chế

Sáng chế đề cập đến phương pháp và thiết bị và vật ghi thực hiện phân tách khóa mật mã cho các chuyển giao. Theo đó, các phương án của sáng chế đề xuất việc phân tách khóa mật mã sau hai lần chuyển giao (còn được gọi là hai 'chặng') bằng cách tạo cấu hình SGSN, còn được đề cập tới ở đây là MME, để tạo ra điểm truy cập đích với giá trị khóa trung gian nằm trong thông báo xác nhận chuyển đổi đường dẫn. Theo đó, các điểm truy cập đích có thể thu khóa sử dụng hàm tạo khóa mà sử dụng giá trị trung gian làm thông số đầu vào để thu khóa mà phân tách mật mã với khóa được sử dụng bởi điểm truy cập nguồn. Một số phương án của sáng chế còn gửi lệnh chuyển giao tới các thiết bị người sử dụng bao gồm chỉ báo loại chuyển giao, như, ví dụ, xem liệu chuyển giao có là chuyển giao liên

điểm truy cập hay chuyển giao nội điểm truy cập. Theo đó, theo nhiều phương án của sáng chế, các thiết bị người sử dụng được tạo cấu hình để xác định loại chuyển giao dựa trên chỉ báo được chứa trong lệnh chuyển giao và thực hiện tạo ra khóa dựa vào loại chuyển giao. Một số phương án của sáng chế còn sử dụng khóa trung gian và/hoặc các khóa được tạo ra từ khóa trung gian để bảo vệ thông báo chuyển đổi đường dẫn sao cho chỉ có các điểm truy cập radio nguồn và đích có khả năng gửi thông báo chuyển đổi đường dẫn hợp lệ và do đó giảm được rủi ro cho điểm truy cập radio ngẫu nhiên bất kỳ mà gửi các thông báo chuyển đổi đường dẫn sai. Các phương án của sáng chế có thể còn thực hiện phân tách khóa mật mã trong khi giảm hoặc giảm tới mức tối thiểu tài nguyên tốn thêm được yêu cầu của các thực thể mạng trong khi xử lý chuyển giao cũng như giảm hoặc giảm đến mức tối thiểu trễ trong chuyển giao.

Theo một phương án ví dụ, sáng chế đề xuất phương pháp bao gồm bước tính toán, đáp lại việc chuyển giao của thiết bị người sử dụng từ điểm truy cập nguồn tới điểm truy cập đích, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất được lưu từ trước. Phương pháp theo phương án này còn bao gồm bước tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào khóa tính toán được. Phương pháp theo phương án này còn bao gồm bước gửi xác nhận chuyển đổi đường dẫn bao gồm giá trị trung gian thứ hai tới điểm truy cập đích để sử dụng trong lần chuyển giao tiếp theo của thiết bị người sử dụng. Phương pháp theo phương án này có thể còn bao gồm bước nhận thông báo chuyển đổi đường dẫn bao gồm chỉ báo của mã nhận diện mạng tế bào và tính toán khóa mã hóa dựa vào mã nhận diện tế bào. Phương pháp theo phương án này có thể còn bao gồm bước lưu giá trị trung gian thứ hai. Theo một số phương án, bước tính toán khóa có thể còn bao gồm tính toán khóa sau chuyển giao liên kết radio.

Theo một phương án ví dụ khác, phương pháp được đề xuất bao gồm bước nhận lệnh chuyển giao từ điểm truy cập nguồn. Phương pháp theo phương án này còn bao gồm bước tính toán, đáp lại việc nhận lệnh chuyển giao, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất. Phương pháp theo phương án này còn bao gồm bước tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào giá trị trung gian thứ nhất. Giá trị trung gian thứ hai có thể được sử dụng để tính toán một hoặc nhiều khóa trong lần chuyển giao tiếp theo.

Theo phương án ví dụ khác, thiết bị được đề xuất. Thiết bị này có thể bao gồm bộ xử lý và bộ nhớ lưu các thực thi được mà khi được thực thi khiến cho thiết bị tính toán, đáp lại việc chuyển giao của thiết bị người sử dụng từ điểm truy cập nguồn tới điểm truy cập đích, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất được lưu từ trước. Các lệnh thực thi được khi được thực thi cũng có thể khiến cho thiết bị tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào khóa tính toán được. Các lệnh thực thi được khi được thực thi có thể còn khiến cho thiết bị gửi xác nhận chuyển đổi đường dẫn bao gồm giá trị trung gian thứ hai tới điểm truy cập đích để sử dụng trong lần chuyển giao tiếp theo của thiết bị người sử dụng.

Theo phương án ví dụ khác, thiết bị được đề xuất. Thiết bị này có thể bao gồm bộ xử lý và bộ nhớ lưu các thực thi được mà khi được thực thi khiến cho thiết bị nhận lệnh chuyển giao từ điểm truy cập nguồn. Các lệnh thực thi được khi được thực thi có thể còn khiến cho thiết bị tính toán, đáp lại việc nhận lệnh chuyển giao, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất. Các lệnh thực thi được khi được thực thi có thể còn khiến cho thiết bị tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào giá trị trung gian thứ nhất. Giá trị trung gian thứ hai có thể được sử dụng để tính toán một hoặc nhiều khóa trong lần chuyển giao tiếp theo.

Theo một phương án ví dụ khác, sáng chế đề xuất sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính có thể bao gồm ít nhất một vật ghi đọc được bằng máy tính có lưu trong đó các lệnh chương trình đọc được bằng máy tính. Các lệnh chương trình đọc được bằng máy tính có thể bao gồm nhiều lệnh chương trình. Mặc dù trong phần bản chất kỹ thuật này, các lệnh chương trình được sắp xếp, nhưng cần hiểu rằng phần bản chất kỹ thuật này chỉ nhằm mục đích ví dụ và thứ tự chỉ đơn thuần là tóm tắt sản phẩm chương trình máy tính. Thứ tự ví dụ không làm giới hạn việc ứng dụng các lệnh chương trình máy tính kết hợp. Lệnh chương trình thứ nhất có thể được tạo cấu hình để tính toán, đáp lại việc chuyển giao của thiết bị người sử dụng từ điểm truy cập nguồn tới điểm truy cập đích, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất được lưu từ trước. Lệnh chương trình thứ hai có thể được tạo cấu hình để tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào khóa tính toán được. Lệnh chương trình thứ ba có thể được tạo cấu hình để gửi xác

nhận chuyển đổi đường dẫn bao gồm giá trị trung gian thứ hai tới điểm truy cập đích để sử dụng trong lần chuyển giao tiếp theo của thiết bị người sử dụng.

Theo một phương án ví dụ khác, sáng chế đề xuất sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính này có thể bao gồm ít nhất một vật ghi đọc được bằng máy tính có lưu trong đó các lệnh chương trình đọc được bằng máy tính. Các lệnh chương trình đọc được bằng máy tính có thể bao gồm nhiều lệnh chương trình. Mặc dù trong phần bản chất kỹ thuật của sáng chế, các lệnh chương trình được thể hiện theo thứ tự, nhưng cần hiểu rằng phần bản chất kỹ thuật của sáng chế chỉ nhằm mục đích ví dụ và thứ tự này chỉ đơn thuần để minh họa bản chất kỹ thuật của sản phẩm chương trình máy tính. Ví dụ thứ này không làm giới hạn việc ứng dụng các lệnh chương trình máy tính liên quan. Lệnh chương trình thứ nhất có thể được tạo cấu hình để nhận lệnh chuyển giao từ điểm truy cập nguồn. Lệnh chương trình máy tính thứ hai có thể được tạo cấu hình để tính toán, đáp lại việc nhận lệnh chuyển giao, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất. Lệnh chương trình thứ ba có thể được tạo cấu hình để tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào giá trị trung gian thứ nhất. Giá trị trung gian thứ hai có thể được sử dụng để tính toán một hoặc nhiều khóa trong lần chuyển giao tiếp theo.

Theo phương án ví dụ khác, sáng chế đề xuất thiết bị bao gồm các phương tiện tính toán, đáp lại việc chuyển giao của thiết bị người sử dụng từ điểm truy cập nguồn tới điểm truy cập đích, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất được lưu. Thiết bị theo phương án này còn bao gồm các phương tiện tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào khóa tính toán được. Thiết bị theo phương án này còn bao gồm các phương tiện gửi xác nhận chuyển đổi đường dẫn bao gồm giá trị trung gian thứ hai tới điểm truy cập đích để sử dụng trong lần chuyển giao tiếp theo của thiết bị người sử dụng.

Theo phương án ví dụ khác, sáng chế đề xuất thiết bị bao gồm các phương tiện nhận lệnh chuyển giao từ điểm truy cập nguồn. Thiết bị theo phương án này còn bao gồm các phương tiện tính toán, đáp lại việc nhận lệnh chuyển giao, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất. Thiết bị theo phương án này còn bao gồm các phương tiện tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào giá trị trung gian thứ nhất. Giá trị trung gian thứ hai có thể được sử dụng để tính toán một hoặc nhiều khóa trong lần chuyển giao tiếp theo.

Phần bản chất kỹ thuật của sáng chế nêu trên chỉ đơn thuần nhằm mục đích tóm lược một vài phương án ví dụ của sáng chế để cung cấp hiểu biết cơ bản về một số khía cạnh của sáng chế. Theo đó, cần hiểu rằng các phương án ví dụ được mô tả ở trên chỉ đơn thuần là các ví dụ và không được hiểu là làm hẹp phạm vi hoặc mục đích của sáng chế theo cách bất kỳ nào. Cần hiểu rằng phạm vi của sáng chế bao hàm nhiều phương án có thể thực hiện, một vài trong chúng sẽ được mô tả chi tiết hơn bên dưới, ngoài những phương án đã được tóm tắt ở đây.

Mô tả vắn tắt các hình vẽ

Do đó sáng chế được mô tả theo các thuật ngữ chung, có dựa vào các hình vẽ kèm theo, các hình vẽ này không nhất thiết phải được vẽ theo tỷ lệ, trong đó:

Fig.1 là sơ đồ khối của thiết bị đầu cuối di động theo phương án ví dụ của sáng chế;

Fig.2 là sơ đồ khối của hệ thống truyền thông vô tuyến theo phương án ví dụ của sáng chế;

Fig.3 là giản đồ thể hiện hệ thống thực hiện phân tách khóa mật mã cho các chuyển giao theo phương án ví dụ của sáng chế;

Fig.4 là giản đồ điều khiển của các tín hiệu truyền thông được truyền giữa các thực thể của phương án ví dụ trên Fig.3 trong quy trình chuyển giao theo phương án ví dụ của sáng chế;

Fig.5 là lưu đồ thể hiện phương pháp ví dụ để thực hiện phân tách khóa mật mã cho các lần chuyển giao theo phương án ví dụ của sáng chế; và

Fig.6 là lưu đồ thể hiện phương pháp ví dụ khác của việc thực hiện phân tách khóa mật mã cho các lần chuyển giao theo phương án ví dụ của sáng chế.

Mô tả chi tiết sáng chế

Các phương án của sáng chế sẽ được mô tả chi tiết hơn sau đây nhờ tham chiếu đến các hình vẽ kèm theo, trong đó một số, nhưng không phải là tất cả các phương án của sáng chế được mô tả. Thực chất, sáng chế có thể được áp dụng theo nhiều dạng khác nhau và không được hiểu là bị giới hạn ở các phương án được mô tả ở đây; thực ra các phương án

này được thực hiện trong phần mô tả này nhằm đáp ứng các yêu cầu pháp lý. Các số chỉ dẫn giống nhau biểu thị các thành phần giống nhau trong suốt bản mô tả.

Fig.1 minh họa sơ đồ khối của thiết bị đầu cuối di động 10 mà có lợi nhờ các phương án của sáng chế. Tuy nhiên, cần hiểu rằng, điện thoại di động như được minh họa và được mô tả ở đây chỉ đơn thuần minh họa cho một loại thiết bị đầu cuối di động mà có lợi nhờ các phương án của sáng chế, và do đó, không nên bị coi là giới hạn phạm vi theo các phương án của sáng chế. Mặc dù một phương án của thiết bị đầu cuối di động 10 được minh họa và sẽ được mô tả ở dưới đây nhằm mục đích ví dụ, các loại khác nhau của các thiết bị đầu cuối di động, như các thiết bị trợ giúp kỹ thuật số cá nhân (Portable Digital Assistants - PDA), các máy nhắn tin, các máy tính di động, các ti vi di động, các thiết bị chơi điện tử, các máy tính xách tay, các camera, các máy quay viđeo, các hệ thống định vị toàn cầu (Global Positioning System - GPS) và các loại hệ thống truyền thông giọng nói và văn bản khác, có thể sẵn sàng áp dụng theo các phương án của sáng chế. Ngoài ra, các thiết bị không phải là các thiết bị di động cũng có thể dễ dàng áp dụng các phương án của sáng chế.

Hệ thống và phương pháp theo các phương án của sáng chế sẽ được mô tả ở dưới cùng với các ứng dụng truyền thông di động. Tuy nhiên, cần hiểu rằng hệ thống và phương pháp theo các phương án của sáng chế cũng có thể được sử dụng cùng với nhiều ứng dụng khác, cả trong ngành và ngoài ngành công nghiệp truyền thông di động.

Thiết bị đầu cuối di động 10 theo một phương án bao gồm anten 12 (hoặc nhiều anten) liên kết theo cách có thể hoạt động được với bộ phát 14 và bộ thu 16. Thiết bị di động có thể là thiết bị đầu cuối 10 còn bao gồm bộ điều khiển 20 hoặc thành phần xử lý khác lần lượt cung cấp các tín hiệu tới và nhận các tín hiệu từ bộ phát 14 và bộ thu 16. Các tín hiệu có thể bao gồm thông tin báo hiệu theo tiêu chuẩn giao diện vô tuyến của hệ thống mạng tế bào có thể ứng dụng được, và giọng nói của người sử dụng, dữ liệu nhận được và/hoặc dữ liệu được tạo ra bởi người sử dụng. Theo đó, thiết bị đầu cuối di động 10 có thể vận hành với một hoặc nhiều tiêu chuẩn giao diện vô tuyến, các giao thức truyền thông, các loại điều biến, và các loại truy cập. Theo cách minh họa, thiết bị đầu cuối di động 10 có thể vận hành theo giao thức bất kỳ trong số các giao thức truyền thông thế hệ thứ nhất, thứ hai, thứ ba và/hoặc thứ tư hoặc tương tự. Ví dụ, thiết bị đầu cuối di động 10 có thể vận hành

theo các giao thức truyền thông vô tuyến thế hệ hai (2G) IS-136 (đa truy cập phân chia thời gian (Time Division Multiple Access - TDMA)), Hệ thống truyền thông di động toàn cầu (Global System for Mobile communications - GSM), và IS-95 (đa truy cập phân chia mã (Code Division Multiple Access - CDMA)), hoặc với các giao thức truyền thông vô tuyến thế hệ ba (3G), như hệ thống viễn thông di động toàn cầu (Universal Mobile Telecommunications System-UMTS), CDMA2000, đa truy cập phân chia mã băng rộng (Wideband Code Division Multiple Access - WCDMA) và đa truy cập phân chia mã đồng bộ - phân chia thời gian (Time Division-Synchronous Code Division Multiple Access - TD-SCDMA), LTE hoặc E-UTRAN, với các giao thức truyền thông vô tuyến thế hệ thứ tư (4G) hoặc tương tự.

Cần hiểu rằng bộ điều khiển 20 theo một phương án bao gồm mạch được mong muốn để áp dụng các chức năng audio và logic của thiết bị đầu cuối di động 10. Ví dụ, bộ điều khiển 20 có thể bao gồm thiết bị xử lý tín hiệu số, thiết bị vi xử lý, và các bộ chuyển đổi từ dạng tương tự thành dạng số khác, các bộ chuyển đổi từ dạng số thành dạng tương tự, và các mạch trợ giúp khác. Các chức năng điều khiển và xử lý tín hiệu của thiết bị đầu cuối di động 10 có thể được cấp phát giữa các thiết bị này theo các khả năng tương ứng của chúng. Do đó, bộ điều khiển 20 cũng có thể có chức năng mã hóa chập và đan xen tin nhắn và dữ liệu trước khi điều biến và truyền. Bộ điều khiển 20 có thể còn bao gồm bộ mã hóa giọng nói bên trong, và có thể bao gồm môđem dữ liệu bên trong. Ngoài ra, bộ điều khiển 20 có thể có chức năng vận hành một hoặc nhiều chương trình phần mềm, có thể được lưu trong bộ nhớ. Ví dụ, bộ điều khiển 20 có thể vận hành chương trình kết nối, như trình duyệt Web thông thường. Chương trình kết nối sau đó có thể cho phép thiết bị đầu cuối di động 10 truyền và nhận nội dung Web, như nội dung dựa trên vị trí và/hoặc nội dung trang web khác, ví dụ theo giao thức ứng dụng không dây (Wireless Application Protocol - WAP), giao thức truyền siêu văn bản (Hypertext Transfer Protocol - HTTP) và/hoặc tương tự.

Thiết bị đầu cuối di động 10 cũng có thể bao gồm giao diện người sử dụng bao gồm thiết bị đầu ra như tai nghe hoặc loa thông thường 24, chuông 22, micrô 26, màn hình hiển thị 28, và giao diện đầu vào của người sử dụng, tất cả chúng được kết nối với bộ điều khiển 20. Giao diện đầu vào của người sử dụng, cho phép thiết bị đầu cuối di động 10 nhận dữ liệu, có thể bao gồm số thiết bị bất kỳ cho phép thiết bị đầu cuối di động 10 nhận dữ liệu,

như bàn phím 30, màn hình chạm (không được thể hiện) hoặc các thiết bị đầu vào khác. Trong các phương án bao gồm bàn phím 30, bàn phím 30 có thể bao gồm các số thông thường (0-9) và các phím liên quan (#, *), và các phím khác được sử dụng để vận hành thiết bị đầu cuối di động 10. Theo cách khác, bàn phím 30 có thể bao gồm bố trí bàn phím QWERTY thông thường. Bàn phím 30 cũng có thể bao gồm các phím mềm khác với các chức năng kết hợp. Ngoài ra, hoặc theo cách khác, thiết bị đầu cuối di động 10 có thể bao gồm thiết bị giao diện như cần điều khiển hoặc giao diện đầu vào người sử dụng khác. Thiết bị đầu cuối di động 10 có thể còn bao gồm pin 34, như gói pin rung, để cấp nguồn cho các mạch điện khác nhau cần thiết để vận hành thiết bị đầu cuối di động 10, cũng như tạo ra dao động cơ học làm tín hiệu ra có thể phát hiện được.

Thiết bị đầu cuối di động 10 có thể còn bao gồm môđun nhận diện người sử dụng (User Identity Module - UIM) 38. Theo một phương án, UIM 38 bao gồm thiết bị nhớ có bộ xử lý được tạo ra trong đó. UIM 38 có thể còn bao gồm, ví dụ, môđun nhận diện thuê bao (Subscriber Identity Module - SIM), thẻ mạch tích hợp vạn năng (Universal Integrated Circuit Card - UICC), môđun nhận diện thuê bao vạn năng (Universal Subscriber Identity Module - USIM), môđun nhận diện người sử dụng tháo rời được (Removable User Identity Module - R-UIM), v.v.. UIM 38 có thể lưu thông tin các thành phần liên quan tới thuê bao di động. Bên cạnh UIM 38, thiết bị đầu cuối di động 10 có thể được trang bị bộ nhớ. Ví dụ, thiết bị đầu cuối di động 10 có thể bao gồm bộ nhớ xóa được 40, như bộ nhớ truy cập ngẫu nhiên (Random Access Memory - RAM) có thể tháo ra được bao gồm vùng đệm để lưu trữ tạm thời dữ liệu. Thiết bị đầu cuối di động 10 cũng có thể bao gồm bộ nhớ không xóa được 42 khác, có thể được nhúng và/hoặc có thể được loại bỏ. Bộ nhớ không xóa được 42 có thể còn hoặc theo cách khác còn bao gồm EEPROM, bộ nhớ flash hoặc tương tự. Các bộ nhớ có thể lưu các thông tin và dữ liệu bất kỳ, được sử dụng bởi thiết bị đầu cuối di động 10 để áp dụng các chức năng của thiết bị đầu cuối di động 10. Ví dụ, các bộ nhớ có thể bao gồm mã nhận diện, như mã nhận diện thiết bị di động quốc tế (International Mobile Equipment Identification - IMEI), có khả năng nhận diện duy nhất thiết bị đầu cuối di động 10.

Trên Fig.2, sơ đồ khối của hệ thống truyền thông vô tuyến có lợi nhờ các phương án của sáng chế. Hệ thống của phương án được minh họa bao gồm nhiều thiết bị mạng. Như được thể hiện, mỗi trong số một hoặc nhiều thiết bị đầu cuối di động 10 có thể bao gồm

anten 12 để truyền các tín hiệu tới và nhận các tín hiệu từ vị trí cơ sở hoặc trạm cơ sở (Base Station - BS) 44. Trong khi BS có thể bao gồm của một hoặc nhiều tế bào, tham chiếu tới BS thường đề cập tới cả BS và tế bào của BS. Trạm cơ sở 44 có thể là một phần của một hoặc nhiều mạng tế bào hoặc mạng di động mà mỗi trong số chúng bao gồm các thành phần được yêu cầu để vận hành mạng, như trung tâm chuyển mạch di động (Mobile Switching Center - MSC) 46. Mạng di động cũng có thể còn được đề cập đến là Trạm cơ sở/MSC/chức năng liên mạng (Base Station/MSC/Interworking Function - BMI). Trong khi vận hành, MSC 46 theo một phương án có khả năng định tuyến các cuộc gọi tới và từ thiết bị đầu cuối di động 10 khi thiết bị đầu cuối di động 10 tạo và nhận các cuộc gọi. MSC 46 cũng có thể tạo ra kết nối tới các đường dây cố định khi thiết bị đầu cuối di động 10 tham gia vào cuộc gọi. Ngoài ra, MSC 46 có thể điều khiển việc chuyển tiếp các tin nhắn tới và từ thiết bị đầu cuối di động 10, và cũng có thể điều khiển việc chuyển tiếp các tin nhắn từ thiết bị đầu cuối di động 10 tới và từ trung tâm nhắn tin. Cần hiểu rằng, mặc dù MSC 46 được thể hiện trong hệ thống trên Fig.2, nhưng MSC 46 chỉ đơn thuần là thiết bị mạng ví dụ và các phương án của sáng chế không bị giới hạn ở việc sử dụng trong mạng sử dụng MSC.

MSC 46 có thể được nối với mạng dữ liệu, như mạng diện cục bộ (Local Area Network-LAN), mạng diện đô thị (Metropolitan Area Network - MAN)), và/hoặc mạng diện rộng (Wide Area Network-WAN). MSC 46 có thể được liên kết trực tiếp tới mạng dữ liệu. Tuy nhiên, theo một phương án, MSC 46 được nối với thiết bị cổng (GTW) 48, và GTW 48 được nối với WAN, như Internet 50. Đến lượt nó, các thiết bị như các thành phần xử lý (tức là, các máy tính cá nhân, máy tính chủ hoặc tương tự) có thể được nối với thiết bị đầu cuối di động 10 thông qua Internet 50. Ví dụ, như giải thích sau đây, các thành phần xử lý có thể bao gồm một hoặc nhiều thành phần xử lý được kết hợp với hệ thống tính toán 52 (hai hệ thống được thể hiện trên Fig.2), máy chủ gốc 54 (một hệ thống được thể hiện trên Fig.2) hoặc tương tự, như được mô tả bên dưới.

BS 44 cũng có thể được kết nối với nút trợ giúp (SGSN) dịch vụ rađio gói chung (General Packet Radio Service - GPRS) 56. SGSN 56 theo một phương án có khả năng thực hiện các chức năng tương tự với MSC 46 cho các dịch vụ chuyển mạch gói. SGSN 56, giống như MSC 46, có thể được kết nối với mạng dữ liệu, như Internet 50. SGSN 56 có thể

được kết nối trực tiếp với mạng dữ liệu. Tuy nhiên, theo phương án khác, SGSN 56 được kết nối với mạng lõi chuyển mạch gói, như mạng lõi GPRS 58. Mạng lõi chuyển mạch gói theo phương án này sau đó sẽ được kết nối với GTW 48 khác, như nút trợ giúp GPRS (Gateway GPRS Support Node - GGSN) cổng 60, và GGSN 60 được kết nối với Internet 50. Bên cạnh GGSN 60, mạng lõi chuyển mạch gói cũng có thể được kết nối với GTW 48. Cũng vậy, GGSN 60 có thể được kết nối với trung tâm nhắn tin. Theo đó, GGSN 60 và SGSN 56, giống như MSC 46, có thể điều khiển việc chuyển tiếp các tin nhắn, như các tin nhắn dịch vụ nhắn tin đa phương tiện (Multimedia Messaging Service - MMS). GGSN 60 và SGSN 56 cũng có thể điều khiển việc chuyển tiếp các tin nhắn cho thiết bị đầu cuối di động 10 tới và từ trung tâm nhắn tin.

Ngoài ra, bằng cách kết hợp SGSN 56 với mạng lõi GPRS 58 và GGSN 60, các thiết bị như hệ thống tính toán 52 và/hoặc máy chủ gốc 54 có thể được kết nối với thiết bị đầu cuối di động 10 thông qua Internet 50, SGSN 56 và GGSN 60. Theo đó, các thiết bị như hệ thống tính toán 52 và/hoặc máy chủ gốc 54 có thể truyền thông với thiết bị đầu cuối di động 10 thông qua SGSN 56, mạng lõi GPRS 58 và GGSN 60. Bằng cách kết nối trực tiếp hoặc gián tiếp các thiết bị đầu cuối di động 10 và các thiết bị khác (tức là, hệ thống tính toán 52, máy chủ gốc 54, v.v.) với Internet 50, các thiết bị đầu cuối di động 10 có thể truyền thông với các thiết bị khác và với nhau, như theo giao thức truyền siêu văn bản (Hypertext Transfer Protocol - HTTP) và/hoặc tương tự, nhờ đó thực hiện các chức năng khác nhau của các thiết bị đầu cuối di động 10.

Mặc dù không phải mọi thành phần của mọi mạng di động có thể được thể hiện và được mô tả ở đây, cần hiểu rằng thiết bị đầu cuối di động 10 có thể được kết nối với một hoặc nhiều trong số bất kỳ của các mạng khác nhau qua BS 44. Theo đó, mạng (các mạng) có thể trợ giúp truyền thông theo một giao thức bất kỳ hoặc hoặc nhiều giao thức trong số các giao thức truyền thông di động thế hệ thứ nhất (1G), thế hệ thứ hai (2G), 2.5G, thế hệ ba (3G), 3.9G, thế hệ thứ tư (4G) hoặc tương tự. Ví dụ, một hoặc nhiều mạng (các mạng) có thể trợ giúp truyền thông theo các giao thức truyền thông vô tuyến 2G IS-136 (TDMA), GSM, và IS-95 (CDMA). Cũng vậy, ví dụ, một hoặc nhiều mạng (các mạng) có thể trợ giúp truyền thông theo các giao thức truyền thông vô tuyến 2.5G GPRS, môi trường GSM dữ liệu tăng cường (Enhanced Data GSM Environment - EDGE), hoặc tương tự. Hơn nữa,

ví dụ, một hoặc nhiều mạng (các mạng) có thể trợ giúp truyền thông theo các giao thức truyền thông vô tuyến 3G như mạng hệ thống điện thoại di động toàn cầu (Universal Mobile Telephone System - USTM) sử dụng công nghệ truy cập rađio đa truy cập phân chia mã băng rộng (Wideband Code Division Multiple Access - WCDMA). Ngoài ra, ví dụ, một hoặc nhiều mạng (các mạng) có thể trợ giúp truyền thông theo các giao thức truyền thông vô tuyến 3.9G như E-UTRAN. Một số AMPS băng hẹp (NAMPS), cũng như hệ thống truyền thông truy cập tổng cộng (Total Access Communication System - TACS), mạng (các mạng) cũng có thể cơ lợi nhờ các phương án của sáng chế, như các thiết bị đầu cuối di động chế độ kép hoặc chế độ cao hơn (tức là, các điện thoại số/tương tự hoặc TDMA/CDMA/tương tự).

Thiết bị đầu cuối di động 10 có thể còn được kết nối với một hoặc nhiều điểm truy cập không dây (AP) 62. Các AP 62 có thể bao gồm các điểm truy cập được tạo cấu hình để truyền thông với thiết bị đầu cuối di động 10 theo các kỹ thuật như, ví dụ, tần số rađio (Radio Frequency - RF), hồng ngoại (Infrared - IrDA) hoặc kỹ thuật bất kỳ trong số các kỹ thuật nối mạng không dây, bao gồm các kỹ thuật LAN không dây (WLAN) như IEEE 802.11 (tức là, 802.11a, 802.11b, 802.11g, 802.11n, v.v.), các kỹ thuật tương tác toàn cầu với truy cập vi ba (Worldwide Interoperability for Microwave Access - WiMAX) như IEEE 802.16, và/hoặc các kỹ thuật mạng vô tuyến diện cá nhân (Personal Area Network - WPAN) như IEEE 802.15, BlueTooth (BT), băng siêu rộng (Ultra Wideband - UWB) và/hoặc tương tự. Các AP 62 có thể được kết nối với Internet 50. Giống với MSC 46, các AP 62 có thể được gắn trực tiếp với Internet 50. Tuy nhiên, theo một phương án, các AP 62 được gắn gián tiếp với Internet 50 thông qua GTW 48. Ngoài ra, theo một phương án, BS 44 có thể được coi làm AP 62 khác. Như có thể thấy, bằng cách nối trực tiếp hoặc gián tiếp các thiết bị đầu cuối di động 10 và hệ thống tính toán 52, máy chủ gốc 54, và/hoặc số thiết bị khác bất kỳ, vào Internet 50, các thiết bị đầu cuối di động 10 có thể truyền thông với thiết bị, hệ thống máy tính khác, v.v., để nhờ đó thực hiện các chức năng khác nhau của các thiết bị đầu cuối di động 10, như để truyền dữ liệu, nội dung hoặc tương tự tới, và/hoặc nhận nội dung, dữ liệu hoặc tương tự, từ hệ thống tính toán 52. 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 thay đổi cho nhau để đề cập tới dữ liệu có khả năng được truyền, nhận và/hoặc được

lưu theo các phương án của sáng chế. Do đó, việc sử dụng của thuật ngữ bất kỳ nào trong các thuật ngữ này không được coi là làm giới hạn mục đích và phạm vi của sáng chế.

Mặc dù không được thể hiện trên Fig.2, nhưng ngoài ra hoặc theo cách khác với việc kết nối thiết bị đầu cuối di động 10 vào các hệ thống tính toán 52 qua Internet 50, thiết bị đầu cuối di động 10 và hệ thống tính toán 52 có thể được kết nối với thiết bị khác và truyền thông theo, ví dụ, RF, BT, IrDA hoặc kỹ thuật truyền thông hữu tuyến hoặc truyền thông vô tuyến bất kỳ, bao gồm các kỹ thuật LAN, WLAN, WiMAX, UWB và/hoặc tương tự. Một hoặc nhiều hệ thống trong các hệ thống tính toán 52, có thể hoặc theo cách khác, còn bao gồm bộ nhớ tháo ra được có khả năng lưu trữ nội dung, nhờ đó có thể được truyền tới thiết bị đầu cuối di động 10. Hơn nữa, thiết bị đầu cuối di động 10 có thể được kết nối với một hoặc nhiều thiết bị điện tử, như các máy in, các máy chiếu kỹ thuật số và/hoặc các thiết bị thu, tạo và/hoặc lưu đa phương tiện khác (tức là, các thiết bị đầu cuối khác). Giống như các hệ thống tính toán 52, thiết bị đầu cuối di động 10 có thể được tạo cấu hình để truyền thông với các thiết bị điện tử di động theo các kỹ thuật như, ví dụ, RF, BT, IrDA hoặc số bất kỳ trong các kỹ thuật truyền thông hữu tuyến hoặc truyền thông vô tuyến khác nhau, bao gồm các kỹ thuật bus nối tiếp vạn năng (Universal Serial Bus - USB), LAN, WLAN, WiMAX, UWB và/hoặc tương tự.

Theo một phương án ví dụ, nội dung hoặc dữ liệu có thể được truyền thông qua hệ thống trên Fig.2 giữa thiết bị đầu cuối di động, có thể tương tự như thiết bị đầu cuối di động 10 trên Fig.1 và mạng thiết bị của hệ thống trên Fig.2 theo thứ tự để thực hiện các ứng dụng để thiết lập truyền thông giữa thiết bị đầu cuối di động 10 và các thiết bị đầu cuối di động khác, ví dụ, thông qua hệ thống trên Fig.2. Như vậy, cần hiểu rằng hệ thống trên Fig.2 không nhất thiết phải được dùng cho sự truyền thông giữa các thiết bị đầu cuối di động hoặc giữa mạng thiết bị và thiết bị đầu cuối di động, mà Fig.2 chỉ đơn thuần được cung cấp nhằm mục đích ví dụ.

Phương án ví dụ của sáng chế sẽ được mô tả với sự tham khảo đến Fig.3, trong đó các thành phần cụ thể của hệ thống để thực hiện việc phục hồi lỗi chuyển giao được thể hiện. Hệ thống trên Fig.3 thể hiện phương án cụ thể của mạng như mạng chung được thể hiện trên Fig.2, trừ việc Fig.3 thể hiện sơ đồ khối chung của E-UTRAN. Như vậy, kết hợp với Fig.3, thiết bị người sử dụng (User Equipment - UE) 70 có thể là ví dụ theo một phương án

của thiết bị đầu cuối di động 10 trên Fig.1 và nút B cải tiến nguồn 72 và nút B cải tiến đích 74 có thể là ví dụ về các phương án của cả BS 44 hoặc AP 62 trên Fig.2. Theo đó, mặc dù thuật ngữ "nút B cải tiến" sẽ được sử dụng thường xuyên, nhưng nút B cải tiến chỉ đơn thuần là một phương án của điểm truy cập và thuật ngữ "điểm truy cập" có thể bao hàm các điểm truy cập, các trạm cơ sở, và các nút B cải tiến. Do đó, mặc dù các phương án của sáng chế được thảo luận liên quan đến các chuẩn E-UTRAN, nhưng các phương án của sáng chế cũng không bị giới hạn và có thể được sử dụng với giao thức truyền thông bất kỳ. Ngoài ra, hệ thống trên Fig.3, cũng có thể được sử dụng kết hợp với nhiều thiết bị khác, cả di động và cố định và do đó, các phương án của sáng chế không bị giới hạn ở ứng dụng trên các thiết bị như thiết bị đầu cuối di động 10 trên Fig.1 hoặc mạng các thiết bị trên Fig.2.

Fig.3 thể hiện sơ đồ hệ thống thực hiện phân tách khóa mật mã cho các lần chuyển giao theo phương án ví dụ của sáng chế. Hệ thống này bao gồm E-UTRAN 76 có thể bao gồm, trong số các bộ phận khác, nhiều nút B cải tiến truyền thông với lõi gói cải tiến (Evolved Packet Core - EPC) 78 có thể bao gồm một hoặc nhiều thực thể quản lý di động (Mobility Management Entities - MME) 80 và một hoặc nhiều cổng phát triển kiến trúc hệ thống (System Architecture Evolution - SAE). Các nút B cải tiến (bao gồm nút B cải tiến nguồn 72 và nút B cải tiến đích 74) có thể là các nút B cải tiến (tức là, các eNB) và cũng có thể truyền thông với UE 70 và các UE khác.

Các nút B cải tiến có thể cung cấp các điểm kết thúc của giao thức mặt phẳng người sử dụng truy cập rađio vệ tinh hệ thống truyền thông viễn thông di động toàn cầu cải tiến (Evolved Universal Mobile Telecommunication System Terrestrial Radio Access - E-UTRA) và các điểm kết thúc của giao thức (điều khiển nguồn rađio (Radio Resource Control - RRC)) của mặt phẳng điều khiển cho UE 70. Các nút B cải tiến có thể cung cấp chức năng như quản lý tài nguyên radio, điều khiển kênh mang rađio, điều khiển đăng ký radio, điều khiển tính linh động liên kết, cấp phát động tài nguyên cho các UE trong cả đường lên và đường xuống, việc lựa chọn của MME 80 tại phần gắn kèm UE, việc nén và mã hóa phần đầu giao thức Internet (Internet Protocol - IP), việc lập lịch nhắn tin và thông tin phát rộng, định tuyến dữ liệu, đo đạc và báo cáo đo để tạo cấu hình tính di động, và tương tự.

MME 80 có thể chứa các chức năng như phân phối tin nhắn tới các nút B cải tiến tương ứng, điều khiển bảo mật, điều khiển trạng thái không tải, điều khiển bộ phận kênh mang SAE, mã hóa và bảo vệ tính toàn vẹn của việc lập tín hiệu phổ không truy cập (Non-Access Stratum - NAS), và tương tự. Mặc dù được đề cập tới ở đây là "MME" theo tiêu chuẩn E-UTRAN, nhưng cần hiểu rằng các phương án của sáng chế không bị giới hạn ở sự vận hành theo tiêu chuẩn E-UTRAN và MME 80 cũng có thể là các thực thể có thể vận hành được với các tiêu chuẩn mạng khác. Theo đó, MME 80 có thể là, ví dụ, SGSN 56 của hệ thống trên Fig.2. Cổng SAE có thể chứa các chức năng như dừng và chuyển mạch các gói cụ thể để nhắn tin và trợ giúp của tính linh động UE. Theo phương án ví dụ, EPC 78 có thể đề xuất liên kết tới mạng như Internet.

Như được thể hiện trên Fig.3, mỗi điểm truy cập, như, ví dụ, nút B cải tiến, có thể bao gồm bộ xử lý 88 được tạo cấu hình để thực hiện các chức năng được kết hợp với từng điểm truy cập tương ứng. Các chức năng này có thể là, ví dụ, được kết hợp với các lệnh được lưu mà khi được thực thi bởi bộ xử lý 88, thực hiện các chức năng được kết hợp với các lệnh tương ứng. Bộ xử lý như những bộ được mô tả ở trên có thể được áp dụng theo nhiều cách. Ví dụ, bộ xử lý 88 có thể được áp dụng là bộ xử lý, bộ đồng xử lý, bộ điều khiển hoặc các phương tiện xử lý khác hoặc các thiết bị bao gồm các mạch tích hợp như, ví dụ, mạch tích hợp chuyên dụng (Application Specific Integrated Circuit - ASIC), mảng cổng lập trình được bằng trường (Field Programmable Gate Array - FPGA) và/hoặc phần cứng được lập trình và/hoặc thành phần phần mềm được tạo cấu hình hoặc được lập trình thích hợp khác.

Theo phương án ví dụ, mỗi một trong số các nút B cải tiến cũng có thể bao gồm thành phần quản lý chuyển giao 90. Thành phần quản lý chuyển giao 90 có thể là thiết bị hoặc phương tiện bất kỳ được dùng trong hoặc phần cứng, hoặc sản phẩm chương trình máy tính, hoặc tổ hợp của phần cứng và phần mềm và có thể được ứng dụng làm hoặc theo cách khác được điều khiển bởi bộ xử lý 88. Thành phần quản lý chuyển giao 90 có thể được tạo cấu hình để xác định xem liệu có yêu cầu chuyển giao với một nút B cải tiến khác dựa vào, ví dụ, các báo cáo đo nhận được từ UE 70 hay không. Theo đó, ví dụ, nếu các báo cáo đo nhận được tại nút B cải tiến nguồn 72 chỉ báo sự hiện diện của điều kiện mà với nó việc chuyển giao được mong muốn (tức là, mức tín hiệu thấp), nút B cải tiến nguồn 72 có thể gửi yêu cầu chuyển giao tới nút B đích cải tiến 74. Theo phương án ví dụ của sáng chế,

thành phần quản lý chuyển giao 90 có thể được tạo cấu hình để bao gồm yêu cầu chuyển giao, khóa mật mã có thể được sử dụng để hỗ trợ truyền thông với UE 70. Theo đó, thành phần quản lý chuyển giao 90 có thể được tạo cấu hình để nhận diện các khóa mật mã nhận được từ thiết bị mạng di động, như, ví dụ nút B cải tiến khác hoặc MME 80, để truyền thông với UE 70 và/hoặc để sử dụng các thông số nhận được từ mạng thiết bị khác để thu hoặc theo cách khác là tính toán các khóa mật mã để sử dụng trong truyền thông với UE 70.

Thành phần quản lý chuyển giao 90 có thể còn được tạo cấu hình để truyền thông với MME 80. Theo đó, thành phần quản lý chuyển giao 90 có thể được tạo cấu hình để nhận thông báo yêu cầu cài đặt thuộc tính ban đầu từ MME 80. Thông báo yêu cầu cài đặt thuộc tính có thể bao gồm một hoặc nhiều khóa mã hóa, khóa mã hóa có thể hỗ trợ truyền thông với UE 70, như các thông số. Thông báo yêu cầu cài đặt thuộc tính có thể còn bao gồm một hoặc nhiều thông số có thể được sử dụng bởi thành phần quản lý chuyển giao để tính toán các khóa mật mã bổ sung. Thành phần quản lý chuyển giao 90 có thể còn được tạo cấu hình để truyền yêu cầu chuyển đổi đường dẫn tới MME 80 cũng như nhận từ MME 80 thông báo xác nhận chuyển đổi đường dẫn có thể bao gồm một hoặc nhiều thông số có thể được sử dụng để thu khóa mật mã. Trong nhiều phương án, thành phần quản lý chuyển giao 90 có thể còn được tạo cấu hình để bảo vệ thông báo chuyển đổi đường dẫn với khóa trung gian và/hoặc các khóa bất kỳ thu được từ khóa trung gian. Việc bảo vệ này có thể đạt được qua bất kỳ một trong trong nhiều phương tiện, như, ví dụ, thông qua kiểm tra tổng thể việc bảo vệ tính toán vẹn (integrity protection checksum) qua thông báo chuyển đổi đường dẫn hoặc thông qua mã thông báo (token) xác thực được tính toán dựa trên khóa trung gian và/hoặc các khóa thu được từ khóa trung gian và một số thành phần bổ sung khác có thể nằm trong thông báo chuyển đổi đường dẫn và/hoặc được chia sẻ giữa điểm truy cập radio đích và thực thể quản lý di động (MME).

Thành phần quản lý chuyển giao 90 có thể còn được tạo cấu hình để truyền thông các tin nhắn liên quan tới việc chuyển giao với UE 70. Theo đó, thành phần quản lý chuyển giao 90 của nút B cải tiến nguồn 72 có thể được tạo cấu hình để gửi lệnh chuyển giao tới UE 70, như đáp lại quyết định chuyển giao được tạo ra dựa vào các báo cáo đo nhận được từ UE 70. Lệnh chuyển giao có thể bao gồm bộ chỉ báo xem liệu việc chuyển giao có phải

là chuyển giao liên nút B cải tiến hay không. Theo một phương án ví dụ, bộ chỉ báo này có thể đơn giản chỉ là bộ chỉ báo cờ 1 bit trong đó UE 70 có thể xác định xem liệu việc chuyển giao là chuyển giao trong nút B cải tiến hay là liên nút B cải tiến dựa vào việc liệu cờ 1 bit có được thiết đặt hay không. Theo các phương án khác, các phương tiện chỉ báo khác có thể được sử dụng, như, ví dụ truyền thông số bổ sung với tin nhắn lệnh chuyển giao.

MME 80 có thể bao gồm bộ xử lý 82, bộ điều khiển chuyển giao 84, và bộ nhớ 86. Bộ xử lý 82 có thể được áp dụng làm bộ xử lý, bộ đồng xử lý, bộ điều khiển hoặc các phương tiện xử ký khác hoặc các thiết bị khác bao gồm các mạch tích hợp như, ví dụ, mạch tích hợp chuyên dụng (application specific intergrated Circuit – ASIC), mảng cổng lập trình trường được bằng trường (Field Programmable Gate Array - FPGA) và/hoặc phần cứng được tạo cấu hình hoặc lập trình và/hoặc sản phẩm chương trình máy tính thích hợp khác. Bộ điều khiển chuyển giao 84 có thể là thiết bị hoặc phương tiện bất kỳ được sử dụng trong hoặc là phần cứng, một hoặc nhiều sản phẩm chương trình máy tính, hoặc kết hợp của phần cứng và phần mềm và có thể được sử dụng hoặc theo cách khác được điều khiển bởi bộ xử lý 82. Bộ điều khiển chuyển giao 84 có thể được tạo cấu hình để truyền thông với các nút B cải tiến và quản lý việc chuyển giao của UE 70. Bộ điều khiển chuyển giao 84 có thể còn được tạo cấu hình để truyền thông với cổng SAE phục vụ. Theo đó, bộ điều khiển chuyển giao 84 có thể được tạo cấu hình để gửi các yêu cầu cập nhật U-Plane đến cổng phục vụ và nhận phản hồi cập nhật U-Plane từ cổng phục vụ.

Theo một phương án ví dụ, bộ điều khiển chuyển giao 84 có thể được tạo cấu hình để tính toán các khóa mật mã cũng như các giá trị trung gian có thể được sử dụng bởi các nút B cải tiến cho việc thu các khóa mật mã bổ sung. Bộ điều khiển chuyển giao 84 có thể được tạo cấu hình để lưu một hoặc nhiều khóa mật mã này và các giá trị trung gian trong bộ nhớ 86. Bộ điều khiển chuyển giao 84 có thể được tạo cấu hình để gửi thông báo yêu cầu cài đặt thuộc tính ban đầu tới nút B cải tiến nguồn 72. Thông báo yêu cầu cài đặt thuộc tính có thể bao gồm một hoặc nhiều giá trị khóa mật mã làm các thông số mà có thể hỗ trợ truyền thông của nút B cải tiến với UE 70. Thông báo yêu cầu cài đặt thuộc tính có thể còn hoặc theo cách khác bao gồm một hoặc nhiều giá trị trung gian làm các thông số có thể được sử dụng bởi nút B cải tiến để tính toán các khóa mật mã bổ sung. Bộ điều khiển chuyển giao 84 có thể còn được tạo cấu hình để nhận yêu cầu chuyển đổi đường dẫn từ nút

B cải tiến cũng như để gửi tới nút B cải tiến thông báo xác nhận chuyển đổi đường dẫn có thể bao gồm một hoặc nhiều thông số có thể được sử dụng bởi việc nhận nút B cải tiến để tạo ra các khóa mật mã. Theo nhiều phương án, bộ điều khiển chuyển giao 84 có thể được tạo cấu hình để kiểm tra thông báo chuyển đổi đường dẫn nhận được để đảm bảo rằng thông báo chuyển đổi đường dẫn nhận được từ nút B cải tiến có hiệu lực. Việc kiểm tra này ví dụ có thể dựa vào một hoặc nhiều khóa, như, ví dụ, khóa trung gian và/hoặc một hoặc nhiều khóa thu được từ khóa trung gian.

Theo phương án ví dụ, UE 70 có thể bao gồm bộ xử lý 92, bộ phận quản lý chuyển giao 94, và bộ nhớ 86. Bộ xử lý 92 có thể được sử dụng làm bộ xử lý, bộ đồng xử lý, bộ điều khiển hoặc các phương tiện xử lý khác hoặc các thiết bị bao gồm các mạch tích hợp như, ví dụ, mạch tích hợp chuyên dụng (Application Specific Intergrated Circuit - ASIC), mảng cổng lập trình được bằng trường (Field Programmable Gate Array - FPGA) và/hoặc phần cứng được tạo cấu hình hoặc được lập trình và/hoặc các thành phần phần mềm thích hợp khác. Theo nhiều phương án, bộ xử lý 92 có thể là bộ điều khiển 20 của thiết bị đầu cuối di động 10. Bộ phận quản lý chuyển giao 94 có thể là thiết bị và phương tiện bất kỳ được sử dụng trong cả phần cứng, một hoặc nhiều sản phẩm chương trình máy tính, hoặc tổng hợp của phần cứng và phần mềm và có thể được sử dụng làm hoặc theo cách khác được điều khiển bởi bộ xử lý 92. Trong nhiều phương án, bộ nhớ 96 có thể là bộ nhớ xóa được 40 hoặc bộ nhớ không xóa được 42 của thiết bị đầu cuối di động 10.

Bộ phận quản lý chuyển giao 94 có thể được tạo cấu hình để truyền thông với nút B cải tiến nguồn 72 và nút B cải tiến đích 74 và tính toán các khóa mật mã để được sử dụng trong truyền thông với các nút B cải tiến để hỗ trợ việc chuyển giao UE 70 từ nút B cải tiến nguồn 72 tới nút B cải tiến đích 74. Bộ phận quản lý chuyển giao có thể được tạo cấu hình để gửi các báo cáo đo tới và nhận lệnh chuyển giao từ nút B cải tiến nguồn 72. Trong nhiều phương án, lệnh chuyển giao nhận được có thể bao gồm bộ chỉ báo liệu xem việc chuyển giao có phải là chuyển giao liên nút B cải tiến hay không. Sau đó, bộ phận quản lý chuyển giao 94 có thể được tạo cấu hình để thu khóa mật mã dựa vào bộ chỉ báo nhận được. Theo đó, các phương án của sáng chế được bộc lộ ở đây có thể thực hiện quy trình thu khóa nếu chuyển giao là chuyển giao liên nút B cải tiến và quy trình thu khóa khác nếu chuyển giao là chuyển giao trong nút B cải tiến.

Trong trường hợp lỗi kết nối rađio (Radio Link Failure - RLF), bộ phận quản lý chuyển giao 94 có thể còn được tạo cấu hình để nhận thông báo tái cấu hình điều khiển nguồn tài nguyên rađio (Radio Resource Control - RRC). Thông báo RRC có thể bao gồm bộ chỉ báo để xem liệu tế bào mà UE được kết nối vào đó là khác với nút B cải tiến mà từ đó UE được kết nối từ trước hay không. Theo đó, bộ phận quản lý chuyển giao 94 có thể được tạo cấu hình để xác định liệu xem UE có được kết nối vào nút B cải tiến mới hay không theo lỗi kết nối rađio và thực hiện thu khóa trung gian dựa vào việc xác định này.

Fig.4 là lưu đồ điều khiển các tín hiệu truyền thông được truyền giữa các thực thể của phương án ví dụ trên Fig.3 cũng như các bước được thực hiện bởi các thực thể trong quy trình chuyển giao nút B cải tiến theo phương án ví dụ của sáng chế. Các bước 400-404 bao gồm các bước khởi đầu có thể xuất hiện theo sự kết nối ban đầu và/hoặc chuyển tiếp từ trạng thái không tải sang trạng thái kích hoạt, trong đó không có thông báo chuyển đổi đường dẫn. Các bước khởi tạo này có thể hoạt động để tạo ra các khóa trung gian và/hoặc các giá trị khác có thể được sử dụng để thu các khóa mã hóa và bảo vệ tính toàn vẹn và để được sử dụng sau lần chuyển giao tiếp theo để thu các khóa trung gian mới. Tại bước 400, MME có thể tính toán tùy ý khóa trung gian KeNB nếu MME không truy cập vào khóa, như khóa tính toán được trước đó và được lưu trong bộ nhớ. Việc tính toán này có thể được thực hiện sử dụng hàm thu khóa bất kỳ đã biết bởi cả MME và UE. Hàm thu khóa có thể sử dụng khóa KASME và số chuỗi liên kết lên (Sequence Number - SN) NAS làm các thông số đầu vào. KASME là một phần của thuộc tính bảo mật và được biết bởi cả MME và UE sau khi xác thực thuê bao hoặc sau khi nhận được một số thuộc tính bảo mật sau công nghệ chuyển giao liên radio, do đó khởi tạo được thuộc tính bảo mật. Một cách tương tự, SN liên kết lên NAS là một phần của cùng một thuộc tính bảo mật và được biết bởi cả MME và UE. Theo đó, SN liên kết lên NAS có thể được xác định từ thông báo yêu cầu dịch vụ khi chuyển tiếp từ trạng thái không tải sang trạng thái kích hoạt và/hoặc đặt lại giá trị 0 sau khi xác thực hoặc được khởi tạo sau khi chuyển giao (handover - HO) từ chuyển giao liên RAT. Bước 400 có thể còn bao gồm bước tính toán giá trị trung gian có thể được sử dụng bởi các nút B cải tiến để thu các khóa. Giá trị trung gian này, được nhận diện là Next-Hop-KeNB1 trên Fig.4, có thể được tính toán theo hàm thu khóa bất kỳ được biết bởi cả MME và UE. Hàm thu khóa có thể sử dụng các giá trị của KASME và KeNB làm các thông số

đầu vào. Sau đó, MME có thể gửi thông báo yêu cầu cài đặt thuộc tính ban đầu, có thể bao gồm các giá trị của KeNB và Next-Hop-KeNB1 tới nút B cải tiến nguồn tại bước 402. Tại bước 404, UE có thể còn tính toán giá trị của KeNB nếu UE không truy cập vào khóa, như khóa tính toán được và được lưu từ trước trong bộ nhớ. Bước 404 có thể còn bao gồm việc tính toán UE tính toán giá trị Next-Hop-KeNB1 sử dụng cùng một hàm thu khóa và các thông số đầu vào khi MME được sử dụng trong bước 400. Theo đó, KeNB là khóa có thể được sử dụng để hỗ trợ truyền thông giữa UE và nút B cải tiến nguồn. Next-Hop-KeNB1 là thông số trung gian có thể được sử dụng để thu giá trị của khóa được sử dụng để hỗ trợ sự truyền thông giữa UE và nút B cải tiến đích tiếp theo việc chuyển giao. Mặc dù không được minh họa, nhưng bước 404 có thể còn bao gồm việc thu RRC UE và các khóa UP từ giá trị của KeNB và/hoặc từ giá trị khóa tiếp theo được thu từ KeNB này bởi hàm thu khóa được xác định trước.

Bước 406 thể hiện bước thứ nhất có thể được thực hiện để khởi đầu việc chuyển giao của UE từ nút B cải tiến nguồn tới nút B cải tiến đích. Theo đó, UE có thể gửi các báo cáo đo tới nút B cải tiến nguồn tại bước 406. Sau đó, nút B cải tiến nguồn có thể thực hiện quyết định chuyển giao tại bước 408 dựa vào các báo cáo đo. Ví dụ, nút B cải tiến nguồn có thể quyết định chuyển giao UE nếu các báo cáo đo chỉ ra rằng UE có thể nhận tín hiệu mạnh hơn hoặc theo cách khác là tín hiệu tin cậy hơn từ một nút B cải tiến khác. Bước 408 có thể còn bao gồm việc tính toán khóa mật mã KeNB* sử dụng hàm thu khóa bất kỳ đã biết bởi UE. Hàm thu khóa có thể sử dụng giá trị trung gian Next-Hop-KeNB1 (giá trị trung gian này có thể được tạo ra trước đó tới nút B cải tiến nguồn trong yêu cầu thiết lập thông số ban đầu, như trong bước 402, và/hoặc trong thông báo xác nhận chuyển đổi đường dẫn, như trong bước 430), cũng như Cell-ID hoặc ID tế bào vật lý, ID này là chỉ báo nhận diện của tế bào đích được chọn, làm các thông số đầu vào. Tuy nhiên, theo một phương án khác, hàm thu khóa có thể không sử dụng chỉ báo bất kỳ của tế bào đích được chọn làm thông số đầu vào. Theo phương án thay thế này, hàm thu khóa có thể chỉ phụ thuộc vào giá trị trung gian Next-Hop-KeNB1 hoặc có thể sử dụng giá trị trung gian Next-Hop-KeNB1 kết hợp với một hoặc nhiều giá trị đã biết khác làm các thông số đầu vào. Bước 410 có thể bao gồm nút B cải tiến nguồn gửi yêu cầu chuyển giao bao gồm giá trị của

KeNB* làm thông số cho nút B cải tiến đích. Theo đó, KeNB* là khóa có thể được sử dụng để hỗ trợ truyền thông giữa UE và nút B cải tiến đích.

Bước 414 có thể bao gồm nút B cải tiến đích xác nhận yêu cầu chuyển giao tới nút B cải tiến nguồn. Sau đó, nút B cải tiến nguồn có thể gửi lệnh chuyển giao tới UE tại bước 416. Lệnh chuyển giao này có thể bao gồm chỉ báo kiểu chuyển giao xác định xem liệu chuyển giao có phải là chuyển giao liên nút B cải tiến hay không. Theo một số phương án, quy trình thu khóa có thể khác với các quy trình được bộc lộ ở đây cho các chuyển giao trong nút B cải tiến. Theo đó, UE có thể sử dụng chỉ báo kiểu chuyển giao để xác định quy trình thu khóa thích hợp. Trong các phương án trong đó chỉ báo nhận diện tế bào đích được sử dụng cho các hàm thu khóa và Cell-ID được sử dụng ngoài ID tế bào vật lý, lệnh chuyển giao có thể còn bao gồm chỉ báo của Cell-ID đích.

Sau đó, UE có thể tính toán các giá trị cho KeNB* và Next-Hop-KeNB2 tại bước 418. UE có thể tính toán KeNB* sử dụng cùng một hàm thu khóa và các thông số đầu vào được sử dụng bởi nút B cải tiến nguồn tại bước 408. Next-Hop-KeNB2 là giá trị trung gian được tính toán sử dụng cùng một hàm thu khóa làm Next-Hop-KeNB1 có thể được sử dụng để tính toán khóa (các khóa) trung gian trong lần chuyển giao tiếp theo. Theo đó, Next-Hop-KeNB2 có thể được lưu bởi UE để sử dụng trong quy trình chuyển giao tiếp theo từ nút B cải tiến đích tới nút B cải tiến thứ ba. Tại bước 420, UE có thể gửi thông báo xác nhận chuyển giao tới nút B cải tiến đích.

Sau đó, nút B cải tiến đích có thể gửi thông báo chuyển đổi đường dẫn tới MME tại bước 422. Theo các phương án, như được minh họa trên Fig.4, trong đó chỉ báo nhận diện của tế bào đích được sử dụng cho các chức năng thu khóa và ID tế bào vật lý được sử dụng hơn là Cell-ID, thông báo chuyển đổi đường dẫn có thể bao gồm chỉ báo của ID tế bào vật lý sao cho ID tế bào vật lý có thể được xác định bởi MME từ thông báo chuyển đổi đường dẫn. Trong các phương án khác, trong đó không có chỉ báo của tế bào đích được sử dụng cho hàm thu khóa trong các bước 408, 418, và 426, thông báo chuyển đổi đường dẫn không bao gồm chỉ báo của ID tế bào vật lý. Trong nhiều phương án, thông báo chuyển đổi đường dẫn có thể còn bao gồm khóa chữ ký hoặc các phương tiện khác để cho phép MME xác thực rằng thông báo chuyển đổi đường dẫn được gửi từ nút B cải tiến hợp lệ. Khóa chữ ký này có thể là, ví dụ, giá trị trung gian, như Next-Hop-KeNB1, và/hoặc các khóa được thu

từ giá trị trung gian. Nút B cải tiến đích có thể xác định xem có gửi thông báo chuyển đổi đường dẫn dựa vào tình huống chuyển giao hay không.

Theo một số phương án, nút B cải tiến đích có thể gửi thông báo chuyển đổi đường dẫn của bước 422 nếu chuyển giao là chuyển giao liên nút B cải tiến, như tình huống chuyển giao được minh họa trên Fig.4. Trong tình huống khác, không được minh họa trên Fig.4, chuyển giao có thể là chuyển giao liên tế bào nhưng vẫn là chuyển giao, trong đó các nút B cải tiến nguồn và đích là giống nhau (còn được đề cập đến là chuyển giao trong eNB, liên tế bào). Trong tình huống khác, không được minh họa trên Fig.4, chuyển giao có thể là chuyển giao trong tế bào. Theo đó, trong một phương án khác, nút B cải tiến đích có thể được tạo cấu hình để gửi thông báo chuyển đổi đường dẫn tại bước 422 đến tất cả các chuyển giao liên tế bào, tức là, cả các chuyển giao trong eNB và liên eNB, các chuyển giao liên tế bào. Theo phương án này, MME có thể được tạo cấu hình để phân biệt các chuyển giao liên tế bào với các chuyển giao trong tế bào, như, ví dụ, dựa vào Cell-ID thay đổi. Theo phương án khác nữa, nút B cải tiến đích có thể được tạo cấu hình để gửi thông báo chuyển đổi đường dẫn tại bước 422 ngay cả cho các chuyển giao trong tế bào. Theo phương án này, MME có thể được tạo cấu hình để phân biệt việc tái truyền thông báo chuyển đổi đường dẫn với các thông báo chuyển đổi đường dẫn liên tế bào.

Bước 424 có thể bao gồm MME gửi yêu cầu cập nhật U-Plane tới cổng phục vụ. Bước 426 có thể bao gồm việc MME tính toán giá trị của KeNB* sử dụng cùng một hàm thu khóa và các thông số đầu vào được sử dụng bởi nút B cải tiến nguồn tại bước 408. Bước 426 có thể còn bao gồm việc MME tính toán Next-Hop-KeNB2 sử dụng cùng một hàm thu khóa khi được sử dụng bởi UE tại bước 418 dựa vào các giá trị của KASME và KeNB*. Sau đó MME có thể lưu Next-Hop-KeNB2 trong bộ nhớ. Sau đó, cổng phục vụ có thể gửi phản hồi cập nhật U-Plane tới MME tại bước 428. Bước 430 có thể bao gồm việc MME gửi xác nhận chuyển đổi đường dẫn tới nút B cải tiến đích. Xác nhận chuyển đổi đường dẫn có thể bao gồm giá trị Next-Hop-KeNB2 làm thông số.

Sau đó, nút B cải tiến đích có thể lưu giá trị Next-Hop-KeNB2 trong bộ nhớ tại bước 432. Theo đó, Next-Hop-KeNB2 có thể được sử dụng bởi nút B cải tiến đích làm thông số trung gian để tính toán KeNB* trong lần chuyển giao tiếp theo. Sau đó, nút B cải tiến đích có thể gửi thông báo tới nút B cải tiến nguồn tại bước 434 giải phóng nút B cải tiến nguồn.

Fig.5 và Fig.6 là các 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 các lưu đồ, và các tổ hợp của các khối trong các lưu đồ, có thể được ứng dụng bởi các phương tiện khác nhau, như phần cứng, phần sụn, và/hoặc sản phẩm chương trình máy tính bao gồm một hoặc nhiều lệnh chương trình máy tính. Ví dụ, một hoặc nhiều quy trình được mô tả ở trên có thể được áp dụng bởi sản phẩm chương trình máy tính bao gồm các lệnh chương trình máy tính. Theo đó, các lệnh chương trình máy tính áp dụng quy trình được mô tả ở trên có thể được lưu bởi thiết bị nhớ của thiết bị đầu cuối di động và được thực hiện bởi bộ xử lý trong thiết bị đầu cuối di động và/hoặc bộ xử lý của thực thể mạng khác, như, ví dụ, SGSN hoặc MME. Có thể thấy rằng, các lệnh chương trình máy tính bất kỳ có thể được tải lên máy tính hoặc thiết bị có thể lập trình được khác (tức là, phần cứng) để tạo ra máy, mà các lệnh được lưu trong bộ nhớ thực hiện trên máy tính hoặc thiết bị có thể lập trình được khác tạo ra các phương tiện áp dụng các chức năng được chỉ ra trong (các) khối hoặc bước (các) bước của các lưu đồ. Các lệnh chương trình máy tính này cũng có thể được lưu trong bộ nhớ đọc được bằng máy tính có thể điều khiển máy tính hoặc thiết bị có thể lập trình được khác để hoạt động theo cách cụ thể sao cho các lệnh được lưu trong bộ nhớ đọc được bằng máy tính tạo ra vật phẩm sản xuất bao gồm các phương tiện ra lệnh áp dụng chức năng được chỉ ra trong (các) khối hoặc (các) bước của các lưu đồ. Các lệnh chương trình máy tính cũng có thể được tải lên trên máy tính hoặc thiết bị có thể lập trình được khác để làm cho chuỗi các bước vận hành được thực hiện trên máy tính hoặc thiết bị có thể lập trình được khác để tạo ra quy trình được thực hiện bởi máy tính mà các lệnh được lưu trong bộ nhớ thực hiện trên máy tính hoặc thiết bị có thể lập trình được khác tạo ra các bước áp dụng các chức năng được chỉ ra trong (các) khối hoặc (các) bước của các lưu đồ.

Theo đó, các khối hoặc các bước của các lưu đồ trợ giúp các tổ hợp của các phương tiện thực hiện các chức năng cụ thể, các tổ hợp của các bước để thực hiện các chức năng cụ thể và sản phẩm chương trình máy tính bao gồm các lệnh chương trình để thực hiện các chức năng cụ thể. Cần hiểu rằng một hoặc nhiều khối hoặc các bước của các lưu đồ, và các tổ hợp của các khối hoặc các bước trong các lưu đồ, có thể được ứng dụng bởi hệ máy tính dựa trên phần cứng mục đích chuyên dụng thực hiện các chức năng hoặc bước cụ thể, hoặc các tổ hợp của phần cứng mục đích chuyên dụng và các lệnh máy tính.

Fig.5 minh họa phương pháp theo một phương án của sáng chế để thực hiện phân tách khóa mật mã cho các chuyển giao, minh họa các bước có thể xuất hiện tại cổng tạo tín hiệu, như, ví dụ, SGSN hoặc thực thể quản lý di động (Mobility Management Entity - MME), trong quy trình việc chuyển giao. Theo đó, một phương án của phương pháp được minh họa trên Fig.5 bao gồm việc MME tính toán KeNB và Next-Hop-KeNB1 tại bước 500. Sau đó, MME có thể gửi yêu cầu cài đặt thông số ban đầu có thể bao gồm KeNB và Next-Hop-KeNB1 tới điểm truy cập phục vụ, như nút B cải tiến phục vụ, tại bước 510. Cần hiểu rằng các bước 500 và 510 bao gồm các bước khởi tạo tùy chọn có thể xuất hiện sau kết nối ban đầu và/hoặc chuyển tiếp từ trạng thái không tải sang trạng thái kích hoạt trong đó không có thông báo chuyển đổi đường dẫn. Các bước khởi tạo này có thể hoạt động để tạo ra các khóa trung gian và/hoặc các giá trị khác có thể được sử dụng để thu khóa mã hóa và khóa bảo vệ tính toàn vẹn cần được sử dụng sau lần chuyển giao tiếp theo để thu các khóa trung gian mới. Theo đó, trong nhiều tình huống, các bước 500 và 510 có thể không xuất hiện. Yêu cầu cài đặt thông số này có thể bao gồm các giá trị của KeNB và Next-Hop-KeNB1 làm các thông số. Tại bước 520, MME có thể nhận yêu cầu chuyển đổi đường dẫn từ điểm truy cập đích, như nút B cải tiến đích. Trong nhiều phương án, MME cũng có thể xác nhận thông báo chuyển đổi đường dẫn dựa trên Next-Hop-KeNB1 khóa và/hoặc các khóa được thu từ Next-Hop-KeNB1 tại bước 530. Trong nhiều phương án, yêu cầu chuyển đổi đường dẫn cũng có thể bao gồm ID tế bào đích vật lý. Sau đó, MME có thể gửi yêu cầu cập nhật U-Plane tới cổng phục vụ đáp lại yêu cầu chuyển đổi đường dẫn tại bước 540. Bước 550 có thể bao gồm việc MME tính toán KeNB* và Next-Hop-KeNB2. Sau đó, MME có thể lưu giá trị Next-Hop-KeNB2 trong bộ nhớ. Bước 560 có thể bao gồm việc MME nhận đáp ứng cập nhật U-Plane từ cổng phục vụ. MME có thể còn gửi xác nhận chuyển đổi đường dẫn bao gồm giá trị Next-Hop-KeNB2 tới nút B cải tiến đích tại bước 570.

Fig.6 minh họa phương pháp thực hiện phân tách khóa mật mã cho các chuyển giao theo phương án ví dụ khác của sáng chế. Theo đó, Fig.6 minh họa các bước có thể xuất hiện tại UE trong khi xử lý chuyển giao. Phương pháp này có thể bao gồm bước tính toán KeNB tại bước 600. Sau đó, UE có thể tính toán Next-Hop-KeNB1 tại bước 610 và gửi các báo cáo đo tới điểm truy cập nguồn, như nút B cải tiến nguồn, tại bước 620. Bước 630 có

thể bao gồm việc UE nhận lệnh chuyển giao từ điểm truy cập nguồn, như nút B cải tiến nguồn. Sau đó, UE có thể tính toán KeNB* và Next-Hop-KeNB2 tại bước 640. Sau đó, UE có thể thu RRC và các khóa UP từ giá trị tính toán được của KeNB*. Bước 650 có thể bao gồm việc UE gửi thông báo xác nhận chuyển giao tới điểm truy cập đích, như nút B cải tiến đích.

Các chức năng mô tả ở trên có thể được thực hiện theo nhiều cách. Ví dụ, các phương tiện thích hợp bất kỳ để thực hiện mỗi một trong các chức năng được mô tả ở trên có thể được áp dụng để thực hiện sáng chế. Theo một phương án, tất cả hoặc một phần các thành phần của sáng chế thường vận hành dưới sự điều khiển của sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính để thực hiện các phương pháp theo các phương án của sáng chế bao gồm vật ghi đọc được bằng máy tính, như vật ghi không khả biến, và các phần mã chương trình đọc được bằng máy tính, như chuỗi của các lệnh máy tính, được lưu trong vật ghi đọc được bằng máy tính.

Theo đó, các phương án của sáng chế đề xuất phân tách mật mã các khóa trung gian cho các chuyển giao sau hai chuyển giao (còn gọi là 'các chặng') bằng cách tạo cấu hình cổng báo hiệu hoặc thực thể quản lý tính di động, như MME, để tạo ra điểm truy cập đích với thông số Next-Hop-KeNB nằm trong vị trí xác nhận/đáp ứng cập nhật hoặc thông báo xác nhận/đáp ứng cập nhật ràng buộc, như, ví dụ, thông báo xác nhận chuyển đổi đường dẫn. Theo đó, việc thu khóa sử dụng hàm thu khóa sử dụng cả KASME và Next-Hop-KeNB làm các thông số đầu vào có thể làm cho khóa phân tách mật mã với KeNB được sử dụng bởi điểm truy cập nguồn. Ít nhất một số phương án của sáng chế việc thực hiện phân tách khóa mật mã sau hai lần chuyển giao do thông báo xác nhận chuyển đổi đường dẫn được đề xuất sau chuyển giao kết nối radio và do đó điểm truy cập nguồn cung cấp các giá trị khóa được sử dụng bởi điểm truy cập đích. Tuy nhiên, sau lần chuyển giao bổ sung, điểm truy cập nguồn có thể không tính toán các khóa mà điểm truy cập đích sử dụng để chuẩn bị chuyển giao tới điểm truy cập đích tiếp theo làm các giá trị được sử dụng bởi điểm truy cập đích được tạo ra bởi MME trong thông báo xác nhận chuyển đổi đường dẫn.

Ngoài ra, các phương án của sáng chế có thể đề xuất phân tách khóa mật mã cho các chuyển giao với ảnh hưởng tối thiểu tới các thực thể mạng liên quan đến tài nguyên tốn thêm. Theo một số phương án, MME thực hiện việc thu khóa bổ sung cho mỗi lần chuyển

giao và lưu Next-Hop-KeNB hiện tại sao cho nó có thể sử dụng giá trị Next-Hop-KeNB hiện tại trong hàm thu khóa để tạo ra KeNB mới và Next-Hop-KeNB mới. UE, theo nhiều phương án, thực hiện sự tính toán bổ sung để thu giá trị trung gian trước khi tính toán các giá trị KeNB*.

Nhiều biến thể và các phương án khác của sáng chế là hiển nhiên với người có hiểu biết trung bình trong lĩnh vực kỹ thuật nhờ phần bộc lộ của phần mô tả nêu trên và các hình vẽ kèm theo. Mặc dù các phương án của sáng chế được mô tả kết hợp với tiêu chuẩn E-UTRAN, nhưng các phương án của sáng chế có thể được áp dụng với các mạng và các giao thức truyền thông khác. Do đó, cần hiểu rằng sáng chế không bị giới hạn ở các phương án cụ thể được bộc lộ và các biến thể và các phương án khác nhằm mục đích được bao hàm trong phạm vi của bộ yêu cầu bảo hộ kèm theo. Ngoài ra, mặc dù phần mô tả nêu trên và các hình vẽ kèm theo mô tả các phương án ví dụ trong ngữ cảnh của các tổ hợp ví dụ cụ thể của các thành phần và/hoặc các chức năng, nhưng cần hiểu rằng các tổ hợp của các thành phần và/hoặc các chức năng khác có thể được tạo ra bởi các phương án thay thế mà không trệch khỏi phạm vi của bộ yêu cầu bảo hộ dưới đây. Theo đó, ví dụ, các tổ hợp của các thành phần và/hoặc các chức năng khác với các tổ hợp được mô tả cụ thể ở trên cũng có thể có mặt trong một số điểm yêu cầu bảo hộ kèm theo. Mặc dù các thuật ngữ cụ thể được sử dụng ở đây, nhưng chúng được sử dụng theo nghĩa chung và chỉ nhằm mục đích mô tả mà không giới hạn sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp thực hiện phân tách mật mã nhiều chặng (multi-hop) cho việc chuyển giao bao gồm các bước:

tính toán, đáp lại việc chuyển giao của thiết bị người sử dụng từ điểm truy cập nguồn tới điểm truy cập đích, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất được lưu từ trước;

tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào khóa tính toán được; và

gửi thông báo xác nhận chuyển đổi đường dẫn bao gồm giá trị trung gian thứ hai tới điểm truy cập đích để sử dụng trong lần chuyển giao tiếp theo của thiết bị người sử dụng.

2. Phương pháp theo điểm 1, trong đó phương pháp này còn bao gồm các bước:

nhận thông báo chuyển đổi đường dẫn từ điểm truy cập đích; và

trong đó bước tính toán khóa bao gồm việc tính toán khóa đáp lại việc nhận thông báo chuyển đổi đường dẫn.

3. Phương pháp theo điểm 2, trong đó:

bước nhận thông báo chuyển đổi đường dẫn còn bao gồm việc nhận thông báo chuyển đổi đường dẫn bao gồm chỉ báo của mã nhận diện mạng tế bào; và trong đó:

bước tính toán khóa bao gồm việc tính toán khóa dựa ít nhất một phần vào mã nhận diện mạng tế bào và giá trị trung gian thứ nhất được lưu từ trước.

4. Phương pháp theo điểm 2, trong đó:

bước nhận thông báo chuyển đổi đường dẫn còn bao gồm việc nhận thông báo chuyển đổi đường dẫn được bảo vệ bởi điểm truy cập đích dựa ít nhất một phần vào giá trị trung gian thứ nhất; và bước này còn bao gồm việc:

xác nhận thông báo chuyển đổi đường dẫn dựa ít nhất một phần vào giá trị trung gian thứ nhất trước khi tính toán khóa.

5. Phương pháp theo điểm bất kỳ trong số các điểm nêu trên, trong đó bước tính toán giá trị trung gian thứ hai bao gồm việc tính toán giá trị trung gian thứ hai dựa ít nhất một phần

vào khóa tính toán được, giá trị trung gian thứ nhất, và K_{ASME}, trong đó K_{ASME} là một phần của ngữ cảnh bảo mật.

6. Phương pháp theo điểm bất kỳ trong số các điểm nêu trên, trong đó bước tính toán khóa bao gồm việc tính toán khóa sau khi chuyển giao kết nối radio đối với thiết bị người sử dụng.

7. Phương pháp theo điểm bất kỳ trong số các điểm nêu trên, trong đó bước tính toán giá trị trung gian thứ hai bao gồm việc thực thể quản lý di động tính toán giá trị trung gian thứ hai.

8. Phương pháp thực hiện phân tách mật mã nhiều chặng cho việc chuyển giao bao gồm các bước:

nhận lệnh chuyển giao từ điểm truy cập nguồn;

tính toán, đáp lại việc nhận lệnh chuyển giao, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất; và

tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào giá trị trung gian thứ nhất, trong đó giá trị trung gian thứ hai để được sử dụng để tính toán một hoặc nhiều khóa trong lần chuyển giao tiếp theo.

9. Phương pháp theo điểm 8, trong đó lệnh chuyển giao còn bao gồm chỉ báo mã nhận diện mạng tế bào; và trong đó:

bước tính toán khóa bao gồm việc tính toán khóa dựa ít nhất một phần vào mã nhận diện mạng tế bào và giá trị trung gian thứ nhất.

10. Phương pháp theo điểm 8 hoặc 9, trong đó bước tính toán giá trị trung gian thứ hai bao gồm việc tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào khóa tính toán được, giá trị trung gian thứ nhất, và K_{ASME}, trong đó K_{ASME} là một phần của ngữ cảnh bảo mật.

11. Phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 10, trong đó lệnh chuyển giao chỉ báo việc chuyển giao của thiết bị người sử dụng từ điểm truy cập nguồn đến điểm truy cập đích.

12. Phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 11, trong đó khóa tính toán được được sử dụng để hỗ trợ sự truyền thông với điểm truy cập đích sau chuyển giao.

13. Phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 12, trong đó phương pháp này còn bao gồm bước lưu giá trị trung gian thứ hai trong bộ nhớ.

14. Phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 13, trong đó bước tính toán giá trị trung gian thứ hai bao gồm việc tính toán giá trị trung gian thứ hai với bộ phận quản lý chuyển giao.

15. Vật ghi bao gồm mã chương trình thực thi được bởi máy tính được ghi trên đó, mã thực thi được bởi máy tính được làm tương thích để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 7.

16. Vật ghi bao gồm mã chương trình thực thi được bởi máy tính được ghi trên đó, mã thực thi được bởi máy tính được làm tương thích để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 14.

17. Thiết bị thực hiện phân tách mật mã nhiều chặng cho việc chuyển giao bao gồm:

phương tiện tính toán, đáp lại việc chuyển giao của thiết bị người sử dụng từ điểm truy cập nguồn đến điểm truy cập đích, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất được lưu từ trước;

phương tiện tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào khóa tính toán được; và

phương tiện gửi thông báo xác nhận chuyển đổi đường dẫn bao gồm giá trị trung gian thứ hai tới điểm truy cập đích để sử dụng trong lần chuyển giao tiếp theo của thiết bị người sử dụng.

18. Thiết bị theo điểm 17, trong đó thiết bị này còn được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 2 đến 7.

19. Thiết bị thực hiện phân tách mật mã nhiều chặng cho việc chuyển giao bao gồm:

phương tiện nhận lệnh chuyển giao từ điểm truy cập nguồn;

phương tiện tính toán, đáp lại việc nhận lệnh chuyển giao, khóa dựa ít nhất một phần vào giá trị trung gian thứ nhất; và

phương tiện tính toán giá trị trung gian thứ hai dựa ít nhất một phần vào giá trị trung gian thứ nhất, trong đó giá trị trung gian thứ hai để được sử để tính toán một hoặc nhiều khóa trong lần chuyển giao tiếp theo.

20. Thiết bị theo điểm 19, trong đó thiết bị này còn được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ điểm 9 đến 14.

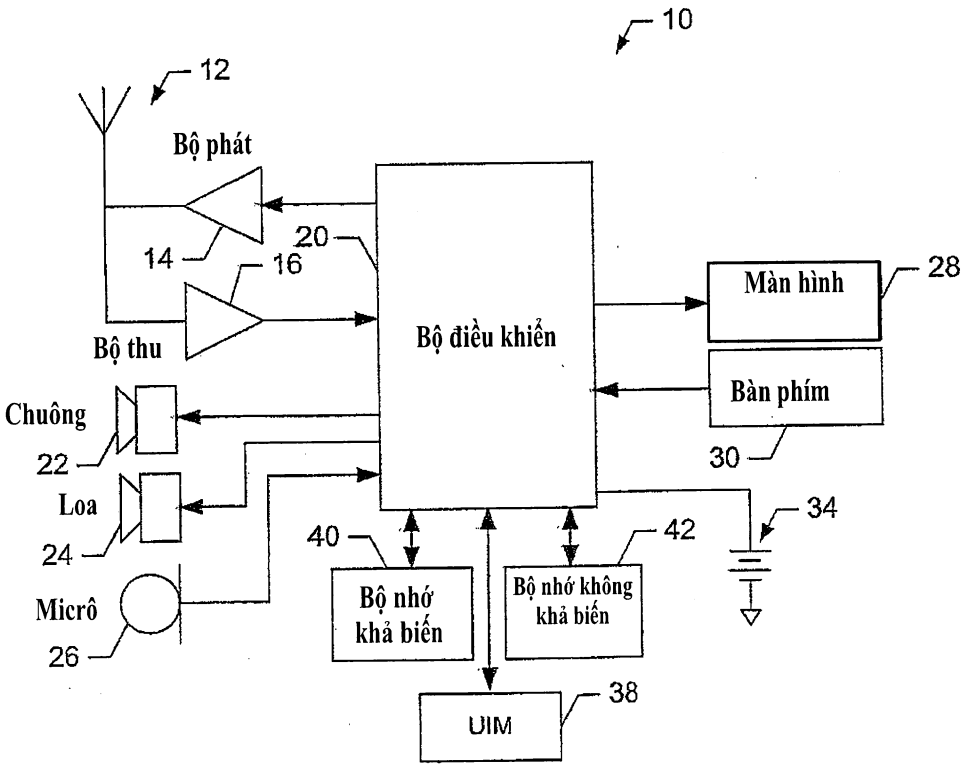

10
12
Bộ phát
14
16
20
Bộ thu
Bộ điều khiển
Màn hình
28
Bàn phím
30
Chuông
22
Loa
24
Micrô
26
40
Bộ nhớ khả biến
Bộ nhớ không khả biến
42
34
UIM
38

FIG. 1.

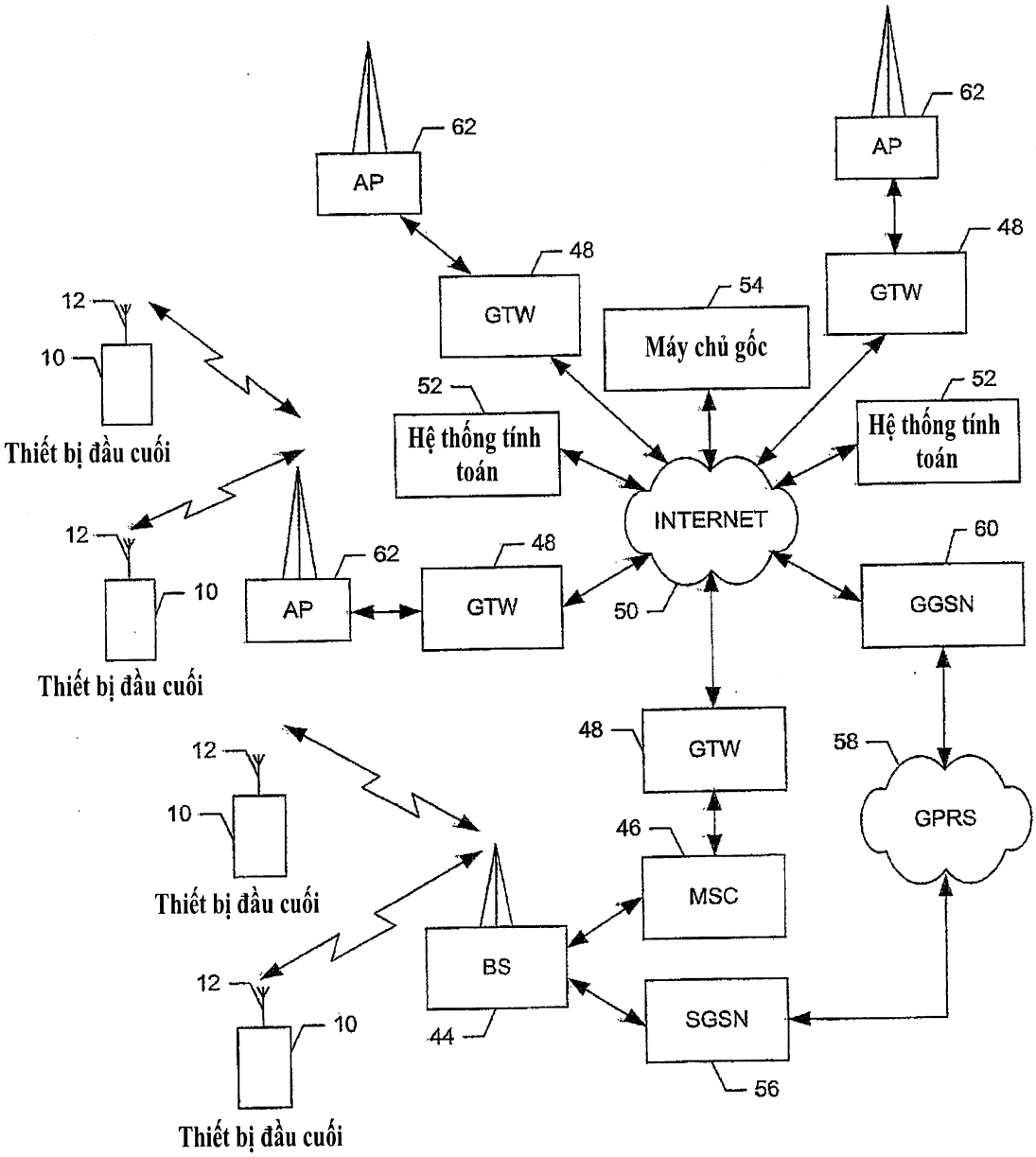

AP
62
AP
62
48
GTW
48
GTW
54
Máy chủ gốc
12
10
Thiết bị đầu cuối
52
Hệ thống tính toán
52
Hệ thống tính toán
INTERNET
12
10
Thiết bị đầu cuối
AP
62
48
GTW
50
60
GGSN
48
GTW
58
GPRS
12
10
Thiết bị đầu cuối
46
MSC
BS
12
10
Thiết bị đầu cuối
44
SGSN
56

FIG. 2.

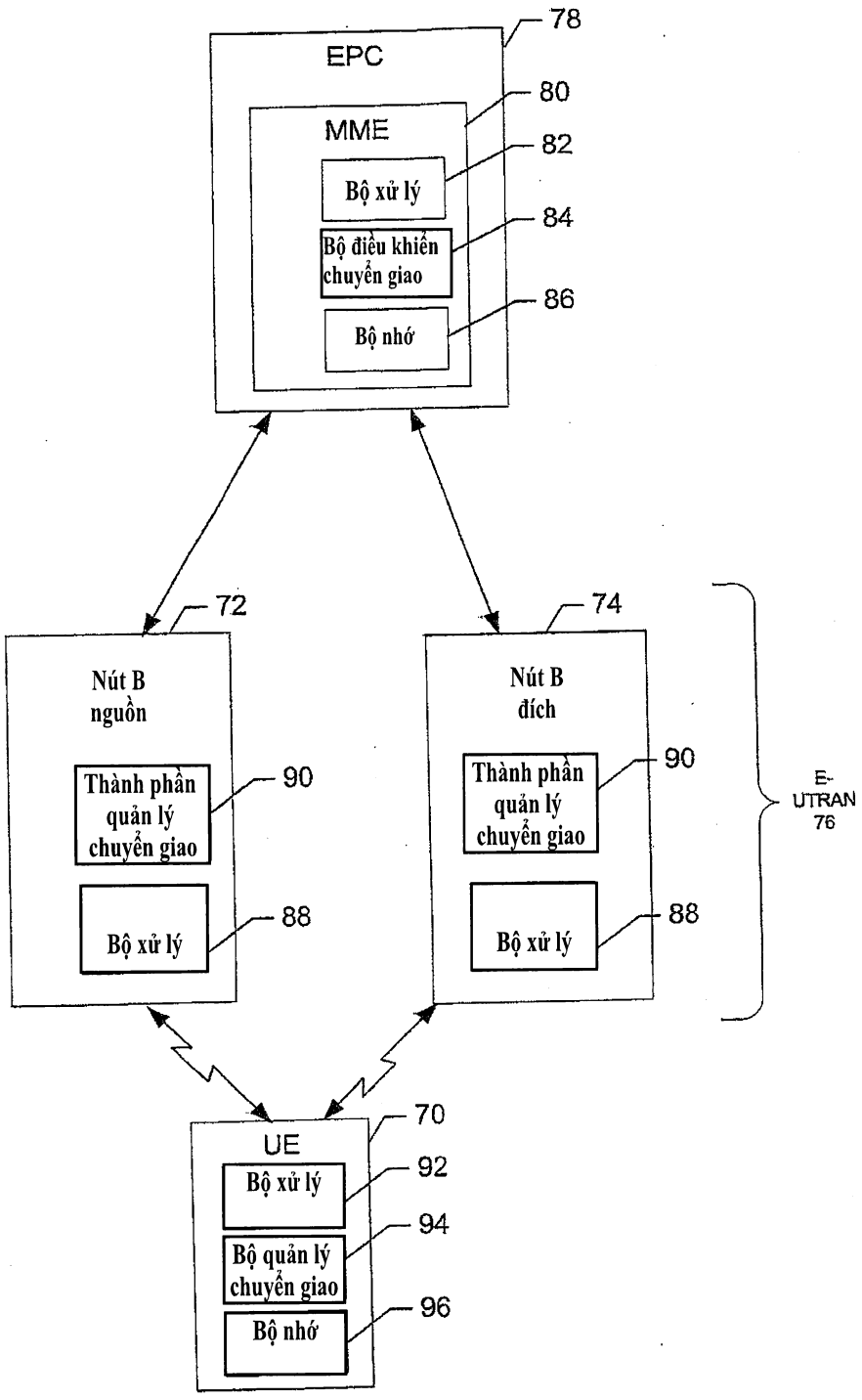

78
EPC
80
MME
82
Bộ xử lý
84
Bộ điều khiển chuyển giao
86
Bộ nhớ
72
Nút B nguồn
90
Thành phần quản lý chuyển giao
88
Bộ xử lý
74
Nút B đích
90
Thành phần quản lý chuyển giao
88
Bộ xử lý
E-UTRAN 76
70
UE
92
Bộ xử lý
94
Bộ quản lý chuyển giao
96
Bộ nhớ

FIG. 3.

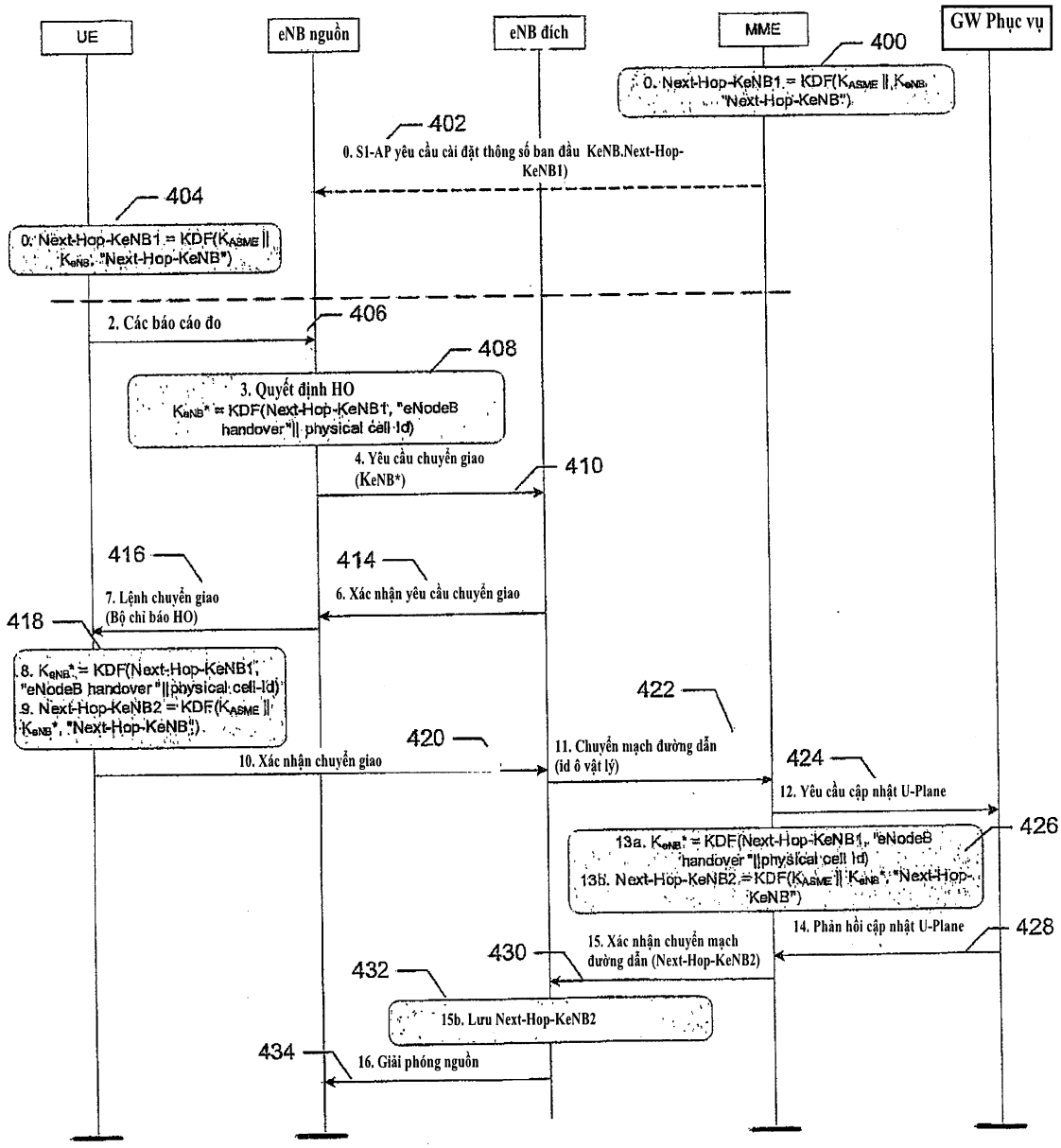

UE
eNB nguồn
eNB đích
MME
GW Phục vụ
400
0. Next-Hop-KeNB1 = KDF(KASME || KeNB, "Next-Hop-KeNB")
402
0. S1-AP yêu cầu cài đặt thông số ban đầu KeNB.Next-Hop-KeNB1)
404
0. Next-Hop-KeNB1 = KDF(KASME || KeNB, "Next-Hop-KeNB")
2. Các báo cáo đo
406
408
3. Quyết định HO
KeNB* = KDF(Next-Hop-KeNB1, "eNodeB handover"|| physical cell Id)
4. Yêu cầu chuyển giao (KeNB*)
410
416
7. Lệnh chuyển giao (Bộ chỉ báo HO)
414
6. Xác nhận yêu cầu chuyển giao
418
8. KeNB* = KDF(Next-Hop-KeNB1, "eNodeB handover"||physical cell Id)
9. Next-Hop-KeNB2 = KDF(KASME || KeNB*, "Next-Hop-KeNB")
422
420
10. Xác nhận chuyển giao
11. Chuyển mạch đường dẫn (id ô vật lý)
424
12. Yêu cầu cập nhật U-Plane
426
13a. KeNB* = KDF(Next-Hop-KeNB1, "eNodeB handover"||physical cell Id)
13b. Next-Hop-KeNB2 = KDF(KASME || KeNB*, "Next-Hop-KeNB")
14. Phản hồi cập nhật U-Plane
428
15. Xác nhận chuyển mạch đường dẫn (Next-Hop-KeNB2)
430
432
15b. Lưu Next-Hop-KeNB2
434
16. Giải phóng nguồn

FIG. 4.

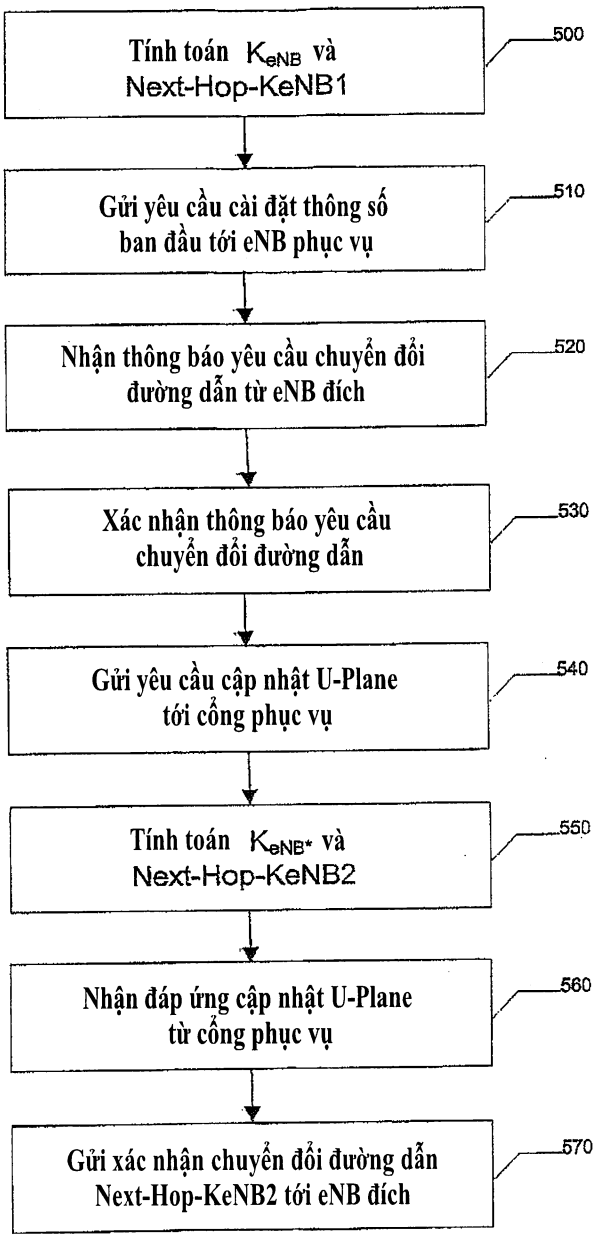

Tính toán K_{eNB} và Next-Hop-KeNB1
500
Gửi yêu cầu cài đặt thông số ban đầu tới eNB phục vụ
510
Nhận thông báo yêu cầu chuyển đổi đường dẫn từ eNB đích
520
Xác nhận thông báo yêu cầu chuyển đổi đường dẫn
530
Gửi yêu cầu cập nhật U-Plane tới cổng phục vụ
540
Tính toán K_{eNB*} và Next-Hop-KeNB2
550
Nhận đáp ứng cập nhật U-Plane từ cổng phục vụ
560
Gửi xác nhận chuyển đổi đường dẫn Next-Hop-KeNB2 tới eNB đích
570

FIG. 5.

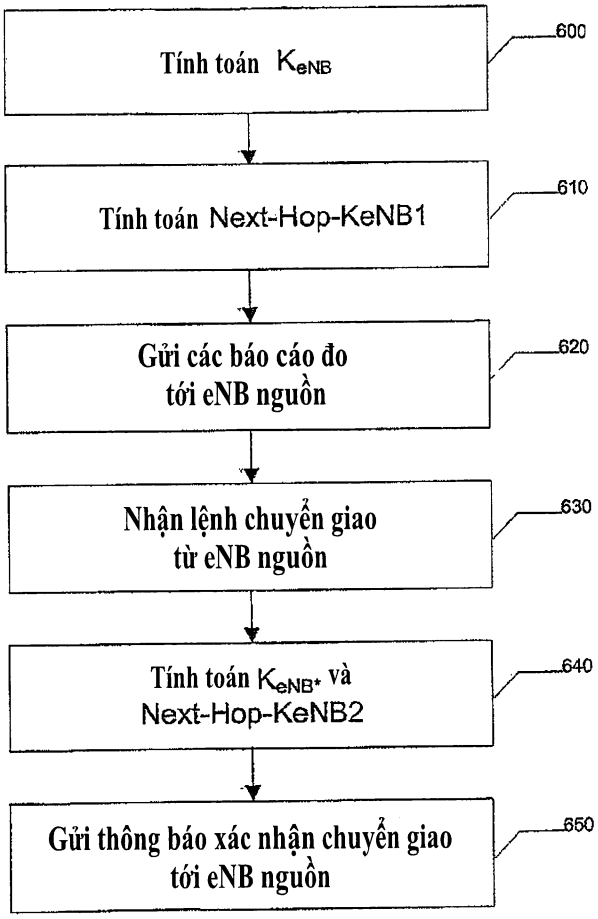

Tính toán K_{eNB}
600
Tính toán Next-Hop-KeNB1
610
Gửi các báo cáo đo tới eNB nguồn
620
Nhận lệnh chuyển giao từ eNB nguồn
630
Tính toán K_{eNB^*} và Next-Hop-KeNB2
640
Gửi thông báo xác nhận chuyển giao tới eNB nguồn
650

FIG. 6.