(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) **1-0050701**

(51)[2020.01] **H04W 36/00**; H04W 76/19; H04W 76/18; H04W 12/04; H04W 36/12

(13) **B**

(21) 1-2021-01986
(22) 12/09/2019
(86) PCT/CN2019/105801 12/09/2019
(87) WO2020/052671 19/03/2020
(30) 201811077550.8 15/09/2018 CN
(45) 25/08/2025 449
(43) 26/07/2021 400A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, China
(72) CHEN, Chao (CN); HU, Li (CN); ZHANG, Zhongli (CN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP TRUYỀN THÔNG VÔ TUYẾN, THIẾT BỊ TRUYỀN THÔNG VÀ PHƯƠNG TIỆN LƯU TRỮ ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(21) 1-2021-01986

(57) Sáng chế đề xuất phương pháp truyền thông vô tuyến, thiết bị truyền thông và phương tiện lưu trữ đọc được bằng máy tính. Phương pháp này bao gồm các bước: Khi thủ tục chuyển giao của thiết bị đầu cuối không thành công, thiết bị đầu cuối khởi tạo thủ tục thiết lập lại. Khi trạm gốc được chọn lại bởi thiết bị đầu cuối là trạm gốc (tức là, trạm gốc đích) mà thiết bị đầu cuối được chuyển giao đến trong thủ tục chuyển giao, do khóa của trạm gốc được cập nhật trong thủ tục chuyển giao, nên trạm gốc bao gồm thông tin dẫn xuất khóa trong tin nhắn thiết lập lại sẽ được gửi đến thiết bị đầu cuối. Do đó, thiết bị đầu cuối có thể cập nhật khóa của thiết bị đầu cuối dựa trên thông tin dẫn xuất khóa, sao cho khóa của thiết bị đầu cuối có thể phù hợp với khóa của trạm gốc.

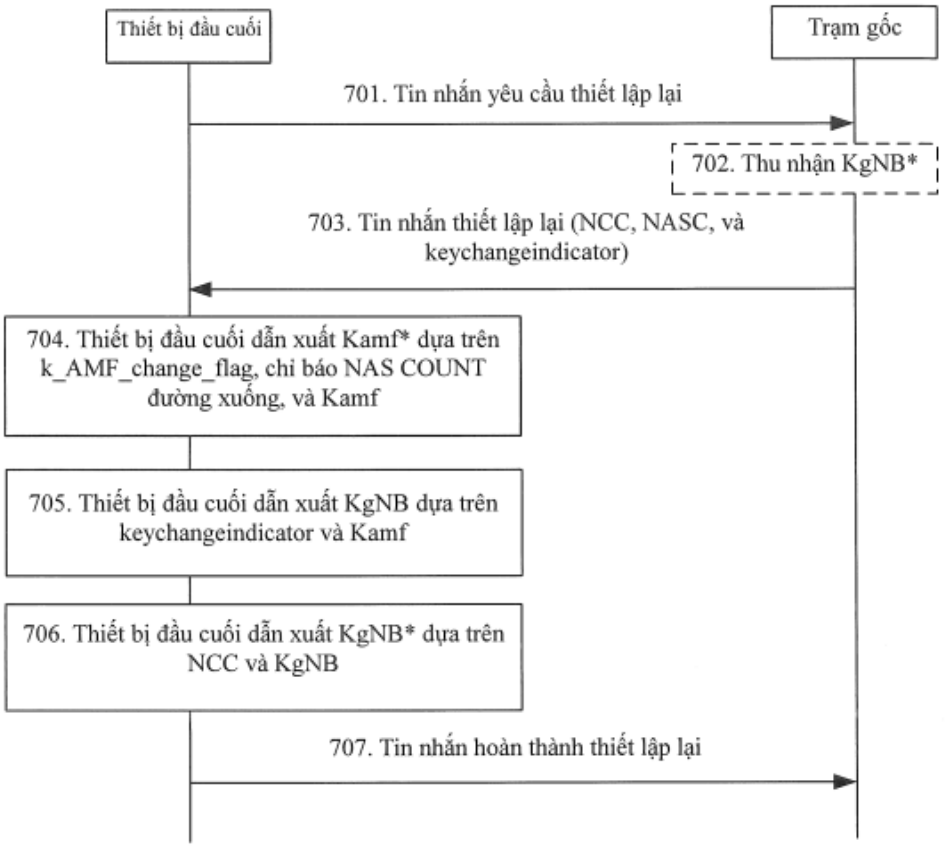

FIG. 7

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực kỹ thuật truyền thông di động, và cụ thể là đến phương pháp truyền thông vô tuyến và thiết bị.

Tình trạng kỹ thuật của sáng chế

Trong truyền thông thế hệ thứ 5 (5th generation, 5G), do các lý do như sự di chuyển của thiết bị đầu cuối, thiết bị đầu cuối cần khởi tạo thủ tục chuyển giao (handover, HO), điều này có nghĩa là, thiết bị đầu cuối cần được chuyển giao từ trạm gốc nguồn đến trạm gốc đích. Khi việc chuyển giao xảy ra, thiết bị đầu cuối có thể cần khởi tạo thủ tục thiết lập lại do một số lý do như lỗi chuyển giao hoặc lỗi tái cấu hình.

Khi thiết bị đầu cuối khởi tạo việc thiết lập lại ở trạm gốc đích trong thủ tục chuyển giao, do nhiều lý do, ví dụ, khóa trên mạng lõi đã được cập nhật trong thủ tục chuyển giao, thuật toán ở phía mạng lõi được chọn lại, hoặc khóa ở phía mạng lõi không được đồng bộ hóa với khóa ở phía trạm gốc, trường hợp trong đó ngữ cảnh bảo mật trên thiết bị đầu cuối không phù hợp với ngữ cảnh bảo mật tiếp theo ở phía mạng được phát sinh sau đó.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp truyền thông vô tuyến và thiết bị, sao cho khóa của thiết bị đầu cuối phù hợp với khóa ở phía mạng.

Theo khía cạnh thứ nhất, sáng chế đề xuất phương pháp truyền thông vô tuyến, được sử dụng trong tình huống trong đó việc chuyển giao của thiết bị đầu cuối không thành công, phương pháp này bao gồm các bước: Thiết bị đầu cuối gửi tin nhắn yêu cầu thiết lập lại đến trạm gốc, trong đó tin nhắn yêu cầu thiết lập lại được sử dụng để thiết lập lại kết nối RRC; thiết bị đầu cuối nhận tin nhắn thiết lập lại từ trạm gốc, trong đó tin nhắn thiết lập lại bao gồm bộ đếm móc nối lần nhảy tiếp theo (next hop chaining counter) NCC và thông tin dẫn xuất khóa; thiết bị đầu cuối dẫn xuất khóa tầng truy cập thứ nhất của thiết bị đầu cuối dựa trên thông tin dẫn xuất khóa; thiết bị đầu cuối dẫn xuất khóa tầng truy cập thứ hai của thiết bị đầu cuối dựa trên NCC và khóa tầng truy cập thứ nhất

của thiết bị đầu cuối; và thiết bị đầu cuối gửi tin nhắn hoàn thành thiết lập lại đến trạm gốc, trong đó tin nhắn hoàn thành thiết lập lại được bảo vệ bằng cách sử dụng khóa được dẫn xuất dựa trên khóa tầng truy cập thứ hai của thiết bị đầu cuối.

Dựa trên giải pháp này, khi thủ tục chuyển giao của thiết bị đầu cuối không thành công, thiết bị đầu cuối khởi tạo thủ tục thiết lập lại. Khi trạm gốc được chọn lại bởi thiết bị đầu cuối là trạm gốc (tức là, trạm gốc đích) mà thiết bị đầu cuối được chuyển giao đến trong thủ tục chuyển giao, do khóa của trạm gốc được cập nhật trong thủ tục chuyển giao, và thông tin dẫn xuất khóa được lưu trữ, nên trạm gốc bao gồm thông tin dẫn xuất khóa trong tin nhắn thiết lập lại sẽ được gửi đến thiết bị đầu cuối. Do đó, thiết bị đầu cuối có thể cập nhật khóa của thiết bị đầu cuối dựa trên thông tin dẫn xuất khóa, sao cho khóa của thiết bị đầu cuối có thể phù hợp với khóa ở phía mạng.

Theo một cách thực hiện khả thi, thông tin dẫn xuất khóa theo khía cạnh thứ nhất bao gồm chỉ báo thứ nhất và NASC, NASC bao gồm chỉ báo thứ hai và chỉ báo NAS COUNT đường xuống, chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập, và chỉ báo thứ hai được sử dụng để chỉ báo cập nhật khóa gốc. Việc thiết bị đầu cuối dẫn xuất khóa tầng truy cập thứ nhất của thiết bị đầu cuối dựa trên thông tin dẫn xuất khóa bao gồm: Thiết bị đầu cuối dẫn xuất khóa gốc thứ hai của thiết bị đầu cuối dựa trên chỉ báo thứ hai, chỉ báo NAS COUNT đường xuống, và khóa gốc thứ nhất của thiết bị đầu cuối; và thiết bị đầu cuối dẫn xuất khóa tầng truy cập thứ nhất của thiết bị đầu cuối dựa trên chỉ báo thứ nhất và khóa gốc thứ hai của thiết bị đầu cuối.

Tùy chọn là, NASC còn bao gồm NAS MAC thứ nhất và bộ nhận dạng của thuật toán được chọn; thiết bị đầu cuối còn có thể dẫn xuất khóa tầng không truy cập dựa trên khóa gốc thứ hai của thiết bị đầu cuối; và thiết bị đầu cuối kiểm tra NAS MAC thứ nhất dựa trên thuật toán được chọn, chỉ báo NAS COUNT đường xuống, và khóa tầng không truy cập.

Theo một cách thực hiện khả thi, chỉ báo NAS COUNT đường xuống bao gồm L1 bit thấp của NAS COUNT đường xuống, trong đó L1 là số nguyên dương, và NAS MAC thứ nhất bao gồm tất cả các bit của NAS MAC thứ hai; và việc thiết bị đầu cuối kiểm tra NAS MAC thứ nhất dựa trên thuật toán được chọn, chỉ báo NAS COUNT đường xuống, và khóa tầng không truy cập bao gồm: Thiết bị đầu cuối thu nhận NAS

COUNT đường xuống thứ hai dựa trên chỉ báo NAS COUNT đường xuống và NAS COUNT đường xuống thứ nhất của thiết bị đầu cuối; thiết bị đầu cuối tạo ra NAS MAC dựa trên khóa tầng không truy cập, thuật toán được chọn, và NAS COUNT đường xuống thứ hai; và thiết bị đầu cuối kiểm tra NAS MAC thứ nhất của NASC dựa trên NAS MAC tạo thành.

Theo một cách thực hiện khả thi khác, chỉ báo NAS COUNT đường xuống bao gồm L2 bit thấp của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm L3 bit thấp hoặc L4 bit cao của NAS MAC thứ hai, trong đó L2 là số nguyên dương, và L3 là số nguyên dương, L4 là số nguyên dương; và việc thiết bị đầu cuối kiểm tra NAS MAC thứ nhất dựa trên thuật toán được chọn, chỉ báo NAS COUNT đường xuống, và khóa tầng không truy cập bao gồm: Thiết bị đầu cuối thu nhận NAS COUNT đường xuống thứ hai dựa trên chỉ báo NAS COUNT đường xuống và NAS COUNT đường xuống thứ nhất của thiết bị đầu cuối; thiết bị đầu cuối tạo ra NAS MAC dựa trên khóa tầng không truy cập, thuật toán được chọn, và NAS COUNT đường xuống thứ hai; và thiết bị đầu cuối kiểm tra NAS MAC thứ nhất của NASC dựa trên L3 bit thấp hoặc L4 bit cao của NAS MAC tạo thành.

Theo một cách thực hiện khả thi khác, chỉ báo NAS COUNT đường xuống bao gồm tất cả các bit của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm L5 bit thấp của NAS MAC thứ hai, trong đó L5 là số nguyên dương; và việc thiết bị đầu cuối kiểm tra NAS MAC thứ nhất dựa trên thuật toán được chọn, chỉ báo NAS COUNT đường xuống, và khóa tầng không truy cập bao gồm: Thiết bị đầu cuối tạo ra NAS MAC dựa trên khóa tầng không truy cập, thuật toán được chọn, và chỉ báo NAS COUNT đường xuống của NASC; và thiết bị đầu cuối kiểm tra NAS MAC thứ nhất của NASC dựa trên L5 bit thấp của NAS MAC tạo thành.

Theo một cách thực hiện khả thi khác, thông tin dẫn xuất khóa theo khía cạnh thứ nhất bao gồm chỉ báo thứ nhất, và chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập; và việc thiết bị đầu cuối dẫn xuất khóa tầng truy cập thứ nhất của thiết bị đầu cuối dựa trên thông tin dẫn xuất khóa bao gồm: Thiết bị đầu cuối dẫn xuất khóa tầng truy cập thứ nhất của thiết bị đầu cuối dựa trên chỉ báo thứ nhất và khóa gốc thứ nhất của thiết bị đầu cuối.

Theo một cách thực hiện khả thi khác, thông tin dẫn xuất khóa theo khía cạnh thứ nhất bao gồm NASC, và NASC có thể bao gồm bộ nhận dạng của thuật toán được chọn, NAS MAC, và tương tự. Thiết bị đầu cuối kiểm tra NAS MAC và tạo ra Knas.

Theo một cách thực hiện khả thi, theo phương án bất kỳ trong số các phương án trên đây, trước khi thiết bị đầu cuối gửi tin nhắn yêu cầu thiết lập lại đến trạm gốc, phương pháp này còn bao gồm bước: Thiết bị đầu cuối nhận tin nhắn tái cấu hình điều khiển tài nguyên radiô RRC từ trạm gốc, trong đó tin nhắn tái cấu hình RRC bao gồm thông số cấu hình, NCC, và thông tin dẫn xuất khóa; và thiết bị đầu cuối thực hiện cấu hình dựa trên thông số cấu hình, trong đó cấu hình không thành công.

Theo một cách thực hiện khả thi khác, theo phương án bất kỳ trong số các phương án trên đây, trước khi thiết bị đầu cuối gửi tin nhắn yêu cầu thiết lập lại đến trạm gốc, phương pháp này còn bao gồm bước: Thiết bị đầu cuối nhận tin nhắn tái cấu hình RRC từ trạm gốc, trong đó tin nhắn tái cấu hình RRC bao gồm NCC và thông tin dẫn xuất khóa; thiết bị đầu cuối khởi động bộ định thời; thiết bị đầu cuối gửi tin nhắn hoàn thành tái cấu hình RRC đến trạm gốc; và thiết bị đầu cuối xác định rằng bộ định thời hết hiệu lực.

Theo khía cạnh thứ hai, sáng chế đề xuất phương pháp truyền thông vô tuyến, được sử dụng trong tình huống trong đó việc chuyển giao của thiết bị đầu cuối không thành công, phương pháp này bao gồm các bước: Trạm gốc nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, trong đó tin nhắn yêu cầu thiết lập lại được sử dụng để thiết lập lại kết nối RRC; trạm gốc gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn thiết lập lại bao gồm bộ đếm móc nối lần nhảy tiếp theo NCC và thông tin dẫn xuất khóa, và thông tin dẫn xuất khóa được sử dụng để chỉ báo cho thiết bị đầu cuối dẫn xuất khóa tầng truy cập; và trạm gốc nhận tin nhắn hoàn thành thiết lập lại từ thiết bị đầu cuối, trong đó tin nhắn hoàn thành thiết lập lại được bảo vệ bằng cách sử dụng khóa được dẫn xuất dựa trên khóa tầng truy cập.

Dựa trên giải pháp này, khi thủ tục chuyển giao của thiết bị đầu cuối không thành công, thiết bị đầu cuối khởi tạo thủ tục thiết lập lại. Khi trạm gốc được chọn lại bởi thiết bị đầu cuối là trạm gốc (tức là, trạm gốc đích) mà thiết bị đầu cuối được chuyển giao đến trong thủ tục chuyển giao, do khóa của trạm gốc được cập nhật trong thủ tục chuyển giao, và thông tin dẫn xuất khóa được lưu trữ, nên trạm gốc bao gồm thông tin dẫn xuất khóa trong tin nhắn thiết lập lại sẽ được gửi đến thiết bị đầu cuối. Do đó, thiết bị đầu

cuối có thể cập nhật khóa của thiết bị đầu cuối dựa trên thông tin dẫn xuất khóa, sao cho khóa của thiết bị đầu cuối có thể phù hợp với khóa ở phía mạng.

Theo một cách thực hiện khả thi, thông tin dẫn xuất khóa theo khía cạnh thứ hai bao gồm chỉ báo thứ nhất và bộ chứa tầng không truy cập NASC, NASC bao gồm chỉ báo thứ hai và chỉ báo NAS COUNT đường xuống, chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập, và chỉ báo thứ hai được sử dụng để chỉ báo cập nhật khóa gốc. Tùy chọn là, NASC còn bao gồm NAS MAC thứ nhất và bộ nhận dạng của thuật toán được chọn.

Theo một cách thực hiện khả thi, chỉ báo NAS COUNT đường xuống bao gồm L1 bit thấp của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm tất cả các bit của NAS MAC thứ hai.

Theo một cách thực hiện khả thi khác, chỉ báo NAS COUNT đường xuống bao gồm L2 bit thấp của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm L3 bit thấp hoặc L4 bit cao của NAS MAC thứ hai.

Theo một cách thực hiện khả thi khác, chỉ báo NAS COUNT đường xuống bao gồm tất cả các bit của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm L5 bit thấp của NAS MAC thứ hai.

Theo một cách thực hiện khả thi khác, thông tin dẫn xuất khóa theo khía cạnh thứ nhất bao gồm chỉ báo thứ nhất, và chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập.

Theo một cách thực hiện khả thi, trước khi trạm gốc gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trạm gốc xác định chỉ báo thứ nhất dựa trên thông số trung gian được đệm, trong đó thông số trung gian là bộ chỉ báo ngữ cảnh bảo mật mới (new security context indicator) NSCI được thu nhận bởi trạm gốc từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao, và NSCI được sử dụng để chỉ báo cho trạm gốc cập nhật khóa tầng truy cập.

Theo một cách thực hiện khả thi khác, trước khi trạm gốc nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, trạm gốc thu nhận bộ chỉ báo ngữ cảnh bảo mật mới NSCI từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển

giao, trong đó NSCI được sử dụng để chỉ báo cho trạm gốc cập nhật khóa tầng truy cập; và trạm gốc xác định và lưu trữ chỉ báo thứ nhất dựa trên NSCI; và trước khi trạm gốc gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trạm gốc thu nhận chỉ báo thứ nhất đã lưu trữ.

Theo một cách thực hiện khả thi khác, trước khi trạm gốc nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, trạm gốc thu nhận NASC từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao; và trạm gốc lưu trữ NASC; và trước khi trạm gốc gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trạm gốc thu nhận NASC đã lưu trữ.

NASC thu được dựa trên NASC được đệm, và NASC được thu nhận từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao.

Theo một cách thực hiện khả thi, theo phương án bất kỳ trong số các phương án trên đây, trước khi trạm gốc nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, phương pháp này còn bao gồm bước: Trạm gốc gửi tin nhắn tái cấu hình RRC đến thiết bị đầu cuối, trong đó tin nhắn tái cấu hình RRC bao gồm thông số cấu hình, NCC, và thông tin dẫn xuất khóa.

Theo khía cạnh thứ ba, sáng chế đề xuất thiết bị. Thiết bị này có chức năng thực thi thiết bị trong phương án phương pháp trên đây. Chức năng này có thể được thực hiện bằng phần cứng, hoặc có thể được thực hiện bằng phần cứng thực hiện phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng này.

Theo một thiết kế khả thi, thiết bị này bao gồm bộ xử lý, bộ nhớ, bus, và giao diện truyền thông. Bộ nhớ lưu trữ lệnh thực hiện được bằng máy tính. Bộ xử lý và bộ nhớ được nối bằng cách sử dụng bus. Khi thiết bị chạy, bộ xử lý thực hiện lệnh thực hiện được bằng máy tính được lưu trữ trong bộ nhớ, sao cho thiết bị thực hiện phương pháp truyền thông vô tuyến theo giải pháp bất kỳ trong số khía cạnh thứ nhất và khía cạnh thứ hai hoặc các cách thực hiện của khía cạnh thứ nhất và khía cạnh thứ hai. Ví dụ, thiết bị này có thể là thiết bị đầu cuối hoặc trạm gốc.

Theo một thiết kế khả thi khác, thiết bị này có thể là chip, ví dụ, chip trong thiết

bị đầu cuối hoặc chip trong trạm gốc. Chip bao gồm bộ phận xử lý, và tùy chọn là còn bao gồm bộ phận lưu trữ. Chip có thể được tạo cấu hình để thực hiện phương pháp truyền thông vô tuyến theo giải pháp bất kỳ trong số khía cạnh thứ nhất và khía cạnh thứ hai hoặc các cách thực hiện của khía cạnh thứ nhất và khía cạnh thứ hai.

Theo khía cạnh thứ tư, sáng chế đề xuất phương tiện lưu trữ máy tính. Phương tiện lưu trữ máy tính lưu trữ lệnh phần mềm máy tính được sử dụng bởi thiết bị đầu cuối hoặc trạm gốc. Lệnh phần mềm máy tính bao gồm chương trình được thiết kế để thực hiện khía cạnh bất kỳ trong số các khía cạnh trên đây.

Theo khía cạnh thứ năm, sáng chế đề xuất sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính bao gồm lệnh phần mềm máy tính. Lệnh phần mềm máy tính có thể được nạp bởi bộ xử lý để thực hiện thủ tục trong phương pháp truyền thông vô tuyến theo khía cạnh bất kỳ trong số các khía cạnh trên đây.

Theo khía cạnh thứ sáu, sáng chế đề xuất hệ thống. Hệ thống bao gồm thiết bị đầu cuối theo giải pháp bất kỳ trong số khía cạnh thứ nhất hoặc các cách thực hiện của khía cạnh thứ nhất, và trạm gốc theo giải pháp bất kỳ trong số khía cạnh thứ hai hoặc các cách thực hiện của khía cạnh thứ hai.

Các khía cạnh này hoặc các khía cạnh khác của sáng chế sẽ rõ ràng hơn và dễ hiểu hơn trong các phần mô tả của các phương án sau đây.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ giản lược của kiến trúc mạng khả thi theo sáng chế;

Fig.2A và Fig.2B là hình vẽ giản lược của thủ tục chuyển giao của thiết bị đầu cuối trong kỹ thuật thông thường;

Fig.3 là hình vẽ giản lược khác của thủ tục chuyển giao của thiết bị đầu cuối trong kỹ thuật thông thường;

Fig.4 là hình vẽ giản lược khác của thủ tục chuyển giao của thiết bị đầu cuối trong kỹ thuật thông thường;

Fig.5 là hình vẽ giản lược của việc dẫn xuất khóa trong 5G;

Fig.6 là hình vẽ giản lược của thủ tục thiết lập lại của thiết bị đầu cuối trong kỹ

thuật thông thường;

Fig.7 là hình vẽ giản lược của thủ tục thiết lập lại của thiết bị đầu cuối theo sáng chế;

Fig.8 là hình vẽ giản lược khác của thủ tục thiết lập lại của thiết bị đầu cuối theo sáng chế;

Fig.9 là hình vẽ giản lược khác của thủ tục thiết lập lại của thiết bị đầu cuối theo sáng chế;

Fig.10 là hình vẽ giản lược của thiết bị theo sáng chế;

Fig.11 là hình vẽ giản lược của thiết bị đầu cuối theo sáng chế; và

Fig.12 là hình vẽ giản lược của trạm gốc theo sáng chế.

Mô tả chi tiết sáng chế

Để làm cho các mục đích, các giải pháp kỹ thuật, và các ưu điểm của sáng chế rõ ràng hơn, phần sau đây còn mô tả sáng chế chi tiết có dựa vào các hình vẽ kèm theo. Phương pháp hoạt động cụ thể theo các phương án phương pháp cũng có thể được sử dụng trong phương án thiết bị hoặc phương án hệ thống. Trong các phần mô tả của sáng chế, trừ khi được nêu khác, "các" có nghĩa là hai hoặc nhiều hơn hai.

Các kiến trúc và các tình huống dịch vụ được mô tả trong sáng chế nhằm mô tả rõ ràng hơn các giải pháp kỹ thuật trong sáng chế, mà không được dự định để giới hạn các giải pháp kỹ thuật được đề xuất trong sáng chế. Người có hiểu biết trung bình trong lĩnh vực tương ứng có thể biết rằng do các kiến trúc mạng tiến hóa và tình huống dịch vụ mới xuất hiện, các giải pháp kỹ thuật được đề xuất trong sáng chế cũng có thể áp dụng được vào các vấn đề kỹ thuật tương tự.

Fig.1 là hình vẽ giản lược của kiến trúc mạng khả thi mà sáng chế có thể áp dụng vào được. Kiến trúc mạng này bao gồm ít nhất một thiết bị đầu cuối 10. Thiết bị đầu cuối 10 truyền thông với trạm gốc 20 bằng cách sử dụng giao diện radiô. Để rõ ràng, chỉ một trạm gốc và một thiết bị đầu cuối được thể hiện trên hình vẽ.

Thiết bị đầu cuối là thiết bị có chức năng của bộ thu-phát vô tuyến. Thiết bị đầu cuối có thể được triển khai trên đất liền, và bao gồm thiết bị trong nhà, thiết bị ngoài

trời, thiết bị cầm tay, hoặc thiết bị lắp trên xe. Thiết bị đầu cuối cũng có thể được triển khai trên mặt nước (ví dụ, trên tàu thủy), và cũng có thể được triển khai trong không trung (ví dụ, trong máy bay, khí cầu, hoặc vệ tinh). Thiết bị đầu cuối có thể là điện thoại di động (mobile phone), máy tính bảng (pad), máy tính có chức năng bộ thu-phát vô tuyến, thiết bị đầu cuối thực tế ảo (virtual reality, VR), thiết bị đầu cuối thực tế tăng cường (augmented reality, AR), thiết bị đầu cuối vô tuyến trong điều khiển công nghiệp (industrial control), thiết bị đầu cuối vô tuyến trong tự lái (self driving), thiết bị đầu cuối vô tuyến trong y tế từ xa (y khoa từ xa - remote medical), thiết bị đầu cuối vô tuyến trong lưới điện thông minh (smart grid), thiết bị đầu cuối vô tuyến trong an toàn vận tải (transportation safety), thiết bị đầu cuối vô tuyến trong thành phố thông minh (smart city), hoặc thiết bị đầu cuối vô tuyến trong nhà thông minh (smart home), hoặc có thể là thiết bị người dùng (user equipment, UE), hoặc tương tự.

Trạm gốc là thiết bị mà cung cấp chức năng truyền thông vô tuyến cho thiết bị đầu cuối. Ví dụ, trạm gốc bao gồm nhưng không bị giới hạn ở nút B (NodeB) thế hệ tiếp theo (g NodeB, gNB) trong 5G, nút B phát triển (evolved NodeB, eNB), bộ điều khiển mạng rađiô (radio network controller, RNC), nút B (NodeB, NB), bộ điều khiển trạm gốc (base station controller, BSC), trạm thu-phát gốc (base transceiver station, BTS), trạm gốc gia đình (ví dụ, nút B phát triển gia đình (home evolved NodeB) hoặc nút B gia đình (home NodeB), HNB), và bộ phận dải gốc (baseBand unit, BBU).

Trong ô, trạm gốc và thiết bị đầu cuối có thể truyền dữ liệu bằng cách sử dụng tài nguyên giao diện qua không trung. Tài nguyên giao diện qua không trung có thể bao gồm tài nguyên miền thời gian và tài nguyên miền tần số, và tài nguyên miền thời gian và tài nguyên miền tần số cũng có thể được gọi là các tài nguyên thời gian-tần số. Tài nguyên miền tần số có thể nằm trong khoảng tần số quy định. Khoảng tần số cũng có thể được gọi là dải (band) hoặc dải tần số, và độ rộng của tài nguyên miền tần số có thể được gọi là dải thông (bandwidth, BW).

Theo sáng chế, thực thể chức năng quản lý truy cập và di động được sử dụng chủ yếu cho việc gắn, quản lý di động, thủ tục cập nhật khu vực theo dõi, và tương tự của thiết bị đầu cuối trong mạng di động. Trong truyền thông thế hệ thứ 5 (5th generation, 5G), thực thể chức năng quản lý truy cập và di động có thể là phần tử mạng chức năng

quản lý truy cập và di động (access and mobility management function, AMF). Trong truyền thông tương lai như truyền thông thế hệ thứ 6 (6th generation, 6G), thực thể chức năng quản lý truy cập và di động có thể vẫn là phần tử mạng AMF, hoặc có thể có tên khác. Điều này không bị giới hạn ở sáng chế. Để dễ dàng mô tả, ví dụ trong đó thực thể chức năng quản lý truy cập và di động là AMF được sử dụng để mô tả trong sáng chế. Ngoài ra, trong thủ tục chuyển giao của thiết bị đầu cuối, AMF mà thiết bị đầu cuối thiết lập kết nối ban đầu được gọi là AMF nguồn, và AMF mà thiết bị đầu cuối thiết lập kết nối sau khi chuyển giao được gọi là AMF đích.

Theo sáng chế, các khóa gốc có thể bao gồm Kamf và Kamf*. Kamf được gọi là khóa gốc thứ nhất, và Kamf* được gọi là khóa gốc thứ hai. Knas có thể được gọi là khóa tầng không truy cập. Các khóa tầng truy cập có thể bao gồm KgNB, KgNB*, lần nhảy tiếp theo (next hop, NH), và tương tự. KgNB hoặc NH được gọi là khóa tầng truy cập thứ nhất, và KgNB* được gọi là khóa tầng truy cập thứ hai.

Theo sáng chế, thiết bị đầu cuối có thể nhận chỉ báo thứ nhất và chỉ báo thứ hai từ phía mạng.

Chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập (nhập lại khóa AS). Theo cách khác, cũng có thể hiểu rằng chỉ báo thứ nhất được sử dụng để chỉ báo cho thiết bị đầu cuối dẫn xuất khóa tầng truy cập dựa trên khóa gốc. Theo cách thực hiện cụ thể, keychangeindicator (bộ chỉ báo thay đổi khóa) có thể được sử dụng để thực hiện. Ví dụ, theo một cách thực hiện, nếu keychangeindicator nhận được là giá trị thiết đặt trước thứ nhất, ví dụ, "1" hoặc "true" ("đúng"), thì điều này chỉ báo rằng khóa tầng truy cập cần được cập nhật; hoặc nếu keychangeindicator nhận được là giá trị thiết đặt trước thứ hai, ví dụ, "0"hoặc "false" ("sai"), điều này chỉ báo rằng khóa tầng truy cập không cần được cập nhật. Theo một ví dụ khác, theo một cách thực hiện khác, keychangeindicator là chỉ báo thứ nhất. Cụ thể, miễn là keychangeindicator được nhận, điều này chỉ báo rằng khóa tầng truy cập cần được cập nhật, hoặc nếu keychangeindicator không được nhận, điều này chỉ báo rằng khóa tầng truy cập không cần được cập nhật.

Chỉ báo thứ hai được sử dụng để chỉ báo rằng khóa gốc được dẫn xuất ngang. Theo cách khác, cũng có thể hiểu rằng chỉ báo thứ hai được sử dụng để chỉ báo cập nhật

khóa gốc. Theo cách thực hiện cụ thể, k_AMF_change_flag có thể được sử dụng để thực hiện. Ví dụ, theo một cách thực hiện, nếu k_AMF_change_flag nhận được là giá trị thiết đặt trước thứ ba, ví dụ, "1" hoặc "đúng", điều này chỉ báo rằng khóa gốc cần được cập nhật, hoặc nếu k_AMF_change_flag nhận được là "0" hoặc "sai", điều này chỉ báo rằng khóa gốc không cần được cập nhật. Theo một ví dụ khác, theo một cách thực hiện khác, k_AMF_change_flag là chỉ báo thứ hai. Cụ thể, miễn là k_AMF_change_flag được nhận, điều này chỉ báo rằng khóa gốc cần được cập nhật, hoặc nếu k_AMF_change_flag không được nhận, điều này chỉ báo rằng khóa gốc không cần được cập nhật.

Các hình vẽ từ Fig.2A đến Fig.4 là các hình vẽ giản lược của ba thủ tục chuyển giao của thiết bị đầu cuối theo sáng chế. Các hình vẽ từ Fig.2A đến Fig.4 lần lượt tương ứng với ba trường hợp trong các thủ tục chuyển giao:

Trường hợp 1: Trong thủ tục chuyển giao, AMF nguồn cập nhật khóa gốc, điều này có nghĩa là, khóa gốc được cập nhật từ Kamf thành Kamf*.

Trường hợp 2: Trong thủ tục chuyển giao, AMF nguồn không cập nhật khóa gốc, điều này có nghĩa là, khóa gốc vẫn là Kamf, nhưng AMF đích chọn thuật toán mới.

Trường hợp 3: Trước khi chuyển giao, các khóa gốc của thiết bị đầu cuối và AMF nguồn đều được cập nhật thành Kamf, thủ tục chuyển giao được thực hiện trước khi trạm gốc nguồn và thiết bị đầu cuối dẫn xuất khóa tầng truy cập mới KgNB dựa trên Kamf, và AMF nguồn không cập nhật khóa gốc trong thủ tục chuyển giao, điều này có nghĩa là, khóa gốc vẫn là Kamf.

Cần lưu ý rằng, trong trường hợp 1 hoặc trường hợp 3, AMF đích có thể chọn thuật toán mới, hoặc có thể không chọn thuật toán mới.

Fig.2A và Fig.2B là hình vẽ giản lược của thủ tục chuyển giao của thiết bị đầu cuối trong kỹ thuật thông thường. Thiết bị đầu cuối được chuyển giao từ trạm gốc nguồn đến trạm gốc đích. Thủ tục chuyển giao được thể hiện trên Fig.2A và Fig.2B tương ứng với trường hợp 1. Thủ tục chuyển giao bao gồm các bước sau đây.

Bước 201. Trạm gốc nguồn quyết định khởi tạo việc chuyển giao.

Bước 202. Trạm gốc nguồn gửi tin nhắn đòi hỏi chuyển giao (Handover Required) đến thiết bị chức năng quản lý truy cập và di động (access and mobility management

function AMF) nguồn.

Bước 203. AMF nguồn xác định Kamf* dựa trên chính sách cục bộ.

Nếu AMF nguồn xác định, dựa trên chính sách cục bộ, rằng khóa gốc Kamf cần được cập nhật, thì AMF nguồn dẫn xuất khóa gốc được cập nhật Kamf* dựa trên Kamf và NAS COUNT đường xuống. Kamf và NAS COUNT đường xuống là nội dung mà ở trong ngữ cảnh thiết bị đầu cuối và được lưu trữ trong AMF nguồn. NAS COUNT đường xuống là thông số về làm mới.

Bước 204. AMF nguồn gửi tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối đến AMF đích.

Theo một cách thực hiện, tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối có thể là, ví dụ, tin nhắn yêu cầu Namf_Communication_CreateUEContext.

Tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối có thể bao gồm chỉ báo thứ ba (được biểu diễn bởi keyAmfDerivationInd dưới đây), chỉ báo thứ tư (được biểu diễn bởi keyAmfChangeInd dưới đây), NAS COUNT đường xuống, Kamf*, và khả năng bảo mật thiết bị đầu cuối. Tùy chọn là, tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối có thể bao gồm thuật toán gốc được sử dụng bởi thiết bị đầu cuối, tức là, thuật toán hiện được sử dụng bởi thiết bị đầu cuối.

keyAmfDerivationInd được sử dụng để chỉ báo rằng Kamf* mới được dẫn xuất. keyAmfChangeInd được sử dụng để chỉ báo rằng Kamf* không được đồng bộ hóa một cách tạm thời với trạm gốc, tức là, chỉ báo rằng khóa tầng truy cập của trạm gốc đã không được cập nhật dựa trên Kamf*. Khả năng bảo mật thiết bị đầu cuối được sử dụng để chỉ báo thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối. NAS COUNT đường xuống là thông số về làm mới.

Bước 205. AMF đích xây dựng bộ chứa NAS (NASC), và.

NASC xây dựng được có thể bao gồm k_AMF_change_flag, chỉ báo NAS_COUNT đường xuống, bộ nhận dạng của thuật toán được chọn, NAS MAC, và tương tự.

k_AMF_change_flag được tạo ra dựa trên keyAmfDerivationInd nhận được, và k_AMF_change_flag được sử dụng để chỉ báo, cho thiết bị đầu cuối, rằng Kamf* mới

được dẫn xuất. Theo cách thực hiện cụ thể, ví dụ, khi giá trị của k_AMF_change_flag là "1" hoặc "đúng", điều này chỉ báo rằng Kamf* mới được dẫn xuất, hoặc khi giá trị của k_AMF_change_flag là "0" hoặc "sai", điều này chỉ báo rằng Kamf* không phải mới được dẫn xuất.

Chỉ báo NAS COUNT đường xuống có thể là tất cả hoặc một số bit của NAS COUNT được nhận từ AMF nguồn. Thuật toán được chọn được chọn bởi AMF đích. Theo một cách thực hiện, AMF đích chọn thuật toán dựa trên khả năng bảo mật thiết bị đầu cuối và chính sách thiết đặt trước. Ví dụ, thuật toán với mức ưu tiên cao nhất có thể được chọn từ khả năng bảo mật thiết bị đầu cuối dựa trên danh sách ưu tiên thuật toán cục bộ. NAS MAC được thu nhận bởi AMF đích thông qua việc tính toán đối với NASC dựa trên thuật toán được chọn và Knas, và Knas được dẫn xuất bởi AMF đích dựa trên Kamf*. Tùy chọn là, thiết bị đầu cuối dẫn xuất Knas dựa trên Kamf, bộ nhận dạng của thuật toán được chọn, và loại thuật toán được chọn.

Bước 206. AMF đích dẫn xuất khóa tầng truy cập thứ nhất (KgNB) dựa trên Kamf*.

Bước 207. AMF đích gửi tin nhắn yêu cầu chuyển giao (HO Request) đến trạm gốc đích, trong đó tin nhắn này có thể bao gồm NASC, bộ chỉ báo ngữ cảnh bảo mật mới (New Security Context Indicator, NSCI), và {NH, bộ đếm móc nối lần nhảy tiếp theo (next hop chaining counter, NCC)}.

NSCI được tạo ra bởi AMF đích dựa trên keyAmfChangeInd, và NSCI được sử dụng để chỉ báo trạm gốc để cập nhật khóa tầng truy cập. AMF đích thiết đặt NH trong {NH, NCC} ở KgNB được tạo ra bởi AMF đích ở bước 206, và thiết đặt NCC ở 0.

Theo một cách thực hiện khác của bước 206 và bước 207, AMF đích có thể dẫn xuất NH tiếp theo dựa trên Kamf* và NH hiện hành, và sau đó cộng 1 vào NCC. Ngoài ra, tin nhắn yêu cầu chuyển giao được gửi bởi AMF đích đến trạm gốc đích bao gồm NASC, NSCI, và {NH, NCC}. NH là NH được dẫn xuất, và NCC là NCC được cập nhật. Fig.5 là hình vẽ giản lược của việc dẫn xuất khóa trong 5G.

Theo một ví dụ, nếu NCC hiện hành của AMF đích bằng 0, thì AMF đích trước tiên dẫn xuất NH (cụ thể, NH thứ nhất từ đỉnh đến đáy trên Fig.5) dựa trên Kamf* và

KgNB hiện hành, và sau đó cộng 1 vào NCC, tức là, NCC=1.

Theo một ví dụ khác, nếu NCC hiện hành của AMF đích bằng 1, thì AMF đích trước tiên dẫn xuất NH tiếp theo (tức là, NH thứ hai từ đỉnh đến đáy trên Fig.5) dựa trên Kamf* và NH hiện hành (tức là, NH tương ứng với NCC=1 trên hình vẽ, tức là, NH thứ nhất từ đỉnh đến đáy trên Fig.5), và sau đó cộng 1 vào NCC, tức là, NCC=2.

Theo một ví dụ khác, nếu NCC hiện hành của AMF đích bằng 2, thì AMF đích trước tiên dẫn xuất NH tiếp theo (tức là, NH thứ ba từ đỉnh đến đáy trên Fig.5) dựa trên Kamf* và NH hiện hành (tức là, NH tương ứng với NCC=2 trên hình vẽ, tức là, NH thứ hai từ đỉnh đến đáy trên Fig.5), và sau đó cộng 1 vào NCC, tức là, NCC=3.

Bước 208. Trạm gốc đích dẫn xuất KgNB* dựa trên NH.

Ví dụ, theo một cách thực hiện, nếu NH=KgNB, thì trạm gốc đích dẫn xuất KgNB* dựa trên KgNB. Theo một cách thực hiện cụ thể, trạm gốc đích có thể dẫn xuất KgNB* dựa trên bộ nhận dạng ô vật lý (physical cell identifier, PCI) đích, số kênh tần số radiô tuyệt đối-đường xuống (absolute radio frequency channel number-down link, ARFCN-DL) ô đích, và KgNB.

Theo một ví dụ khác, theo một cách thực hiện khác, nếu NH được dẫn xuất bởi AMF đích dựa trên Kamf* và NH hiện hành của AMF đích, thì trạm gốc đích dẫn xuất KgNB* dựa trên NH nhận được. Theo một cách thực hiện cụ thể, trạm gốc đích có thể thu được KgNB* dựa trên PCI đích, ARFCN-DL ô đích, và NH.

Tùy chọn là, trạm gốc đích có thể dẫn xuất các KgNB* mà theo sự tương ứng một-một với các ô của trạm gốc đích.

Bước 209. Trạm gốc đích gửi bộ chứa RRC đến AMF đích.

Bộ chứa RRC bao gồm tin nhắn tái cấu hình điều khiển tài nguyên radiô (radio resource control, RRC) (RRCReconfiguration), và tin nhắn bao gồm NCC, keychangeindicator, và NASC. NCC là NCC nhận được ở bước 207. NASC là NASC nhận được ở bước 207. keychangeindicator được tạo ra bởi trạm gốc đích dựa trên NSCI nhận được.

Bước 210. AMF đích gửi tin nhắn hồi đáp tạo ngữ cảnh thiết bị đầu cuối đến AMF nguồn, trong đó tin nhắn này bao gồm bộ chứa RRC.

Theo một cách thực hiện, tin nhắn hồi đáp tạo ngữ cảnh thiết bị đầu cuối có thể là tin nhắn hồi đáp Namf_Communication_CreateUEContext.

Bước 211. AMF nguồn gửi tin nhắn yêu cầu chuyển giao (Handover Request) đến trạm gốc nguồn, trong đó tin nhắn này bao gồm bộ chứa RRC.

Bước 212. Trạm gốc nguồn gửi bộ chứa RRC đến thiết bị đầu cuối. Bộ chứa RRC bao gồm tin nhắn tái cấu hình RRC (RRCReconfiguration).

Tin nhắn tái cấu hình RRC bao gồm NCC, keychangeindicator, và NASC.

Bước 213. Thiết bị đầu cuối dẫn xuất Kamf* dựa trên Kamf và NAS COUNT đường xuống.

Nếu thiết bị đầu cuối xác định, dựa trên k_AMF_change_flag trong NASC, rằng Kamf* cần được dẫn xuất, thì thiết bị đầu cuối thu nhận NAS COUNT đường xuống dựa trên chỉ báo NAS COUNT đường xuống trong NASC, và sau đó dẫn xuất Kamf* dựa trên Kamf và NAS COUNT đường xuống.

Bước 214. Thiết bị đầu cuối kiểm tra NAS MAC.

Thiết bị đầu cuối dẫn xuất Knas dựa trên Kamf*, và sau đó kiểm tra NAS MAC trong NASC bằng cách sử dụng Knas và thuật toán được chỉ báo bởi bộ nhận dạng mà là của thuật toán được chọn và có trong NASC. Cụ thể, thiết bị đầu cuối tính toán NAS MAC dựa trên Knas, thuật toán được chọn, và NASC, và sau đó so sánh NAS MAC tính toán được với NAS MAC trong NASC nhận được để xác định liệu NAS MAC tính toán được có phù hợp với NAS MAC trong NASC nhận được hay không. Nếu NAS MAC tính toán được phù hợp với NAS MAC trong NASC nhận được, thì việc kiểm tra tính toàn vẹn thành công. Nếu NAS MAC tính toán được không phù hợp với NAS MAC trong NASC nhận được, thì việc kiểm tra tính toàn vẹn không thành công.

Bước 215. Thiết bị đầu cuối dẫn xuất KgNB dựa trên Kamf*.

Nếu thiết bị đầu cuối xác định, dựa trên keychangeindicator nhận được, rằng KgNB cần được dẫn xuất, thì thiết bị đầu cuối dẫn xuất KgNB dựa trên Kamf*, và thiết đặt NCC tương ứng với KgNB ở 0.

Bước 216. Thiết bị đầu cuối so sánh NCC nhận được với NCC hiện hành của thiết

bị đầu cuối. Do các giá trị của hai NCC đều là 0, nên hai NCC là bằng nhau, và thiết bị đầu cuối dẫn xuất KgNB* dựa trên KgNB.

Cần lưu ý rằng, nếu bước 206 và bước 207 được thực hiện bởi cách khác của chúng, thì bước 215 và bước 216 được thay thế bằng cách thực hiện sau đây: Thiết bị đầu cuối xác định, dựa trên keychangeindicator, rằng KgNB cần được dẫn xuất, và thiết đặt NCC tương ứng với KgNB ở 0. Thiết bị đầu cuối trước tiên xác định liệu NCC hiện hành của thiết bị đầu cuối có giống như NCC được nhận bởi thiết bị đầu cuối hay không. Trong trường hợp này, kết quả xác định sẽ là NCC hiện hành của thiết bị đầu cuối không giống như NCC được nhận bởi thiết bị đầu cuối, và thiết bị đầu cuối dẫn xuất NH lớp tiếp theo dựa trên Kamf* và NH hiện hành, và sau đó cộng 1 vào NCC hiện hành của thiết bị đầu cuối. Sau đó, thiết bị đầu cuối tiếp tục xác định liệu NCC hiện hành của thiết bị đầu cuối có giống như NCC được nhận bởi thiết bị đầu cuối hay không, cho đến khi NCC hiện hành của thiết bị đầu cuối giống như NCC được nhận bởi thiết bị đầu cuối. Trong trường hợp này, thiết bị đầu cuối dẫn xuất KgNB* dựa trên NH hiện hành. Theo một cách thực hiện cụ thể, thiết bị đầu cuối có thể dẫn xuất KgNB* dựa trên PCI ô đích, ARFCN-DL ô đích, và NH hiện hành.

Các phần mô tả được đưa ra nhờ sử dụng các ví dụ dưới đây dựa vào Fig.5. Theo một ví dụ, nếu NCC hiện hành của thiết bị đầu cuối bằng 0, và NCC được nhận bởi thiết bị đầu cuối là 1, thì thiết bị đầu cuối trước tiên dẫn xuất NH dựa trên Kamf* và KgNB hiện hành, cộng 1 vào NCC hiện hành của thiết bị đầu cuối để thu nhận NCC=1, và sau đó dẫn xuất KgNB* dựa trên NH của thiết bị đầu cuối.

Dựa vào Fig. 5, quy trình dẫn xuất trên đây có thể được hiểu như sau: Thiết bị đầu cuối trước tiên thực hiện việc dẫn xuất dọc trên NH và cộng 1 vào NCC của thiết bị đầu cuối, cho đến khi NCC của thiết bị đầu cuối bằng NCC được nhận bởi thiết bị đầu cuối, và sau đó thiết bị đầu cuối thực hiện việc dẫn xuất ngang dựa trên NH được dẫn xuất mới nhất, để thu nhận KgNB*.

Bước 217. Thiết bị đầu cuối gửi tin nhắn hoàn thành tái cấu hình RRC (RRCReconfigurationComplete) đến trạm gốc đích.

Trong thủ tục chuyển giao trên đây của thiết bị đầu cuối, phía thiết bị đầu cuối dẫn xuất Kamf*, Knas, và KgNB* dựa trên Kamf gốc. Phía AMF đích dẫn xuất Kamf* và

Knas dựa trên Kamf gốc, và phía trạm gốc đích dẫn xuất KgNB*. Do đó, các khóa (KgNB*) được đồng bộ hóa giữa thiết bị đầu cuối và trạm gốc đích, và các khóa (Knas và Kamf*) được đồng bộ hóa giữa thiết bị đầu cuối và AMF đích.

Trong thủ tục trên đây, các lỗi thủ tục chuyển giao là như sau: Ví dụ, lỗi chuyển giao xảy ra do tin nhắn hoàn thành tái cấu hình RRC ở bước 217 không được nhận bởi phía mạng (ví dụ, thiết bị đầu cuối khởi động bộ định thời trước bước 217, và thiết bị đầu cuối không nhận tin nhắn ACK từ trạm gốc trước khi bộ định thời hết hiệu lực, mà chỉ báo rằng thiết bị đầu cuối không gửi tin nhắn hoàn thành tái cấu hình RRC), hoặc tin nhắn tái cấu hình RRC trong bộ chứa RRC được nhận bởi thiết bị đầu cuối ở bước 212 gây ra lỗi tái cấu hình thiết bị đầu cuối (ví dụ, sau bước 212, thiết bị đầu cuối thực hiện cấu hình dựa trên thông số cấu hình trong tin nhắn tái cấu hình RRC, và cấu hình không thành công) do lỗi thông số cấu hình hoặc tương tự. Trong các trường hợp này, khóa mà đã được dẫn xuất bởi thiết bị đầu cuối không được kích hoạt do lỗi. Do đó, khóa trước đó được sử dụng trong thủ tục RRC tiếp theo. Ví dụ, các khóa được sử dụng bởi thiết bị đầu cuối được lùi về Kamf và KgNB1 (ở đây, KgNB1 được dẫn xuất dựa trên Kamf).

Fig.3 là hình vẽ giản lược của thủ tục chuyển giao của thiết bị đầu cuối trong kỹ thuật thông thường. Thiết bị đầu cuối được chuyển giao từ trạm gốc nguồn đến trạm gốc đích. Thủ tục chuyển giao được thể hiện trên Fig.3 tương ứng với trường hợp 2. Thủ tục chuyển giao bao gồm các bước sau đây.

Bước 301 và bước 302 giống như bước 201 và bước 202 trong thủ tục chuyển giao được thể hiện trên Fig.2A. Tham khảo các phần mô tả trên đây.

Bước 303. AMF nguồn xác định Kamf dựa trên chính sách cục bộ.

AMF nguồn xác định không cập nhật Kamf dựa trên chính sách cục bộ. Hơn nữa, AMF nguồn còn dẫn xuất NH tiếp theo dựa trên Kamf và NH tiếp theo, và cộng 1 vào NCC.

Bước 304. AMF nguồn gửi tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối đến AMF đích.

Theo một cách thực hiện, tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối có thể là, ví dụ, tin nhắn yêu cầu Namf_Communication_CreateUEContext.

Tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối có thể bao gồm NAS COUNT đường xuống, Kamf, và khả năng bảo mật thiết bị đầu cuối. Tùy chọn là, tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối có thể bao gồm thuật toán gốc được sử dụng bởi thiết bị đầu cuối, tức là, thuật toán hiện được sử dụng bởi thiết bị đầu cuối.

Tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối có thể còn bao gồm NH và NCC mà được tạo ra bởi AMF nguồn.

Theo một cách thực hiện, tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối có thể còn bao gồm keyAmfDerivationInd, và keyAmfDerivationInd được sử dụng để chỉ báo rằng Kamf không được cập nhật. Ví dụ, khi giá trị của keyAmfDerivationInd là "0" hoặc "sai", điều này chỉ báo rằng Kamf không được cập nhật. Theo một cách thực hiện khác, nếu tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối không bao gồm keyAmfDerivationInd, thì AMF đích xác định rằng keyAmfDerivationInd không được nhận, và do đó xác định rằng Kamf không được cập nhật.

Bước 305. AMF đích xây dựng bộ chứa NAS (NASC).

NASC xây dựng được có thể bao gồm bộ nhận dạng của thuật toán được chọn, NAS MAC, và tương tự.

Thuật toán được chọn được chọn bởi AMF đích. Theo một cách thực hiện, AMF đích chọn thuật toán dựa trên khả năng bảo mật thiết bị đầu cuối và chính sách thiết đặt trước. Ví dụ, thuật toán với mức ưu tiên cao nhất có thể được chọn từ khả năng bảo mật thiết bị đầu cuối dựa trên danh sách ưu tiên thuật toán cục bộ. NAS MAC được thu nhận bởi AMF đích thông qua việc tính toán đối với NASC dựa trên thuật toán được chọn và Knas, và Knas được dẫn xuất bởi AMF đích dựa trên Kamf*. Tùy chọn là, thiết bị đầu cuối dẫn xuất Knas dựa trên Kamf, bộ nhận dạng của thuật toán được chọn, và loại thuật toán được chọn.

Theo một cách thực hiện, tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối còn bao gồm keyAmfDerivationInd, và keyAmfDerivationInd được sử dụng để chỉ báo rằng Kamf không được cập nhật. Ví dụ, khi giá trị của keyAmfDerivationInd là "0" hoặc "sai", điều này chỉ báo rằng Kamf không được cập nhật. Theo cách khác, nếu tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối không bao gồm keyAmfDerivationInd, thì AMF

đích xác định rằng Kamf không được cập nhật. Do đó, khi AMF đích xây dựng NASC, NASC có thể bao gồm k_AMF_change_flag, và giá trị của k_AMF_change_flag có thể là, ví dụ, "0" hoặc "sai", để chỉ báo rằng Kamf không được cập nhật, hoặc NASC không bao gồm k_AMF_change_flag.

Bước 306. AMF đích gửi tin nhắn yêu cầu chuyển giao (HO Request) đến trạm gốc đích, trong đó tin nhắn này có thể bao gồm NASC và {NH, NCC}.

AMF đích thiết đặt NH trong {NH, NCC} ở NH được tạo ra bởi AMF nguồn ở bước 303, và thiết đặt NCC ở NCC được tạo ra bởi AMF nguồn ở bước 303.

Bước 307. Trạm gốc đích dẫn xuất KgNB* dựa trên NH.

NH là NH được nhận bởi trạm gốc đích từ AMF đích.

Theo một cách thực hiện cụ thể, trạm gốc đích có thể thu được KgNB* dựa trên PCI đích, ARFCN-DL ô đích, và NH.

Tùy chọn là, trạm gốc đích có thể dẫn xuất các khóa KgNB* mà theo sự tương ứng một-một với các ô của trạm gốc đích.

Bước 308. Trạm gốc đích gửi bộ chứa RRC đến AMF đích.

Bộ chứa RRC bao gồm tin nhắn tái cấu hình kết nối RRC, và tin nhắn này bao gồm NCC và NASC. NCC là NCC nhận được ở bước 307. NASC là NASC nhận được ở bước 306.

Bước 309. AMF đích gửi tin nhắn hồi đáp tạo ngữ cảnh thiết bị đầu cuối đến AMF nguồn, trong đó tin nhắn này bao gồm bộ chứa RRC.

Theo một cách thực hiện, tin nhắn hồi đáp tạo ngữ cảnh thiết bị đầu cuối có thể là tin nhắn hồi đáp Namf_Communication_CreateUEContext.

Bộ chứa RRC bao gồm tin nhắn tái cấu hình kết nối RRC, và tin nhắn này bao gồm NCC và NASC.

Bước 310. AMF nguồn gửi tin nhắn yêu cầu chuyển giao (Handover Request) đến trạm gốc nguồn, trong đó tin nhắn này bao gồm bộ chứa RRC.

Bộ chứa RRC bao gồm tin nhắn tái cấu hình kết nối RRC, và tin nhắn này bao gồm NCC và NASC.

Bước 311. Trạm gốc nguồn gửi bộ chứa RRC đến thiết bị đầu cuối. Bộ chứa RRC bao gồm tin nhắn tái cấu hình RRC (RRCReconfiguration).

Bước 312. Thiết bị đầu cuối kiểm tra NAS MAC.

Thiết bị đầu cuối dẫn xuất Knas dựa trên Kamf, và sau đó kiểm tra NAS MAC trong NASC bằng cách sử dụng Knas và thuật toán được chỉ báo bởi bộ nhận dạng mà là của thuật toán được chọn và có trong NASC. Cụ thể, thiết bị đầu cuối tính toán NAS MAC dựa trên Knas, thuật toán được chọn, và NASC, và sau đó so sánh NAS MAC tính toán được với NAS MAC trong NASC nhận được để xác định liệu NAS MAC tính toán được có phù hợp với NAS MAC trong NASC nhận được hay không. Nếu NAS MAC tính toán được phù hợp với NAS MAC trong NASC nhận được, thì việc kiểm tra tính toàn vẹn thành công. Nếu NAS MAC tính toán được không phù hợp với NAS MAC trong NASC nhận được, thì việc kiểm tra tính toàn vẹn không thành công.

Bước 313. Thiết bị đầu cuối dẫn xuất KgNB* dựa trên NCC nhận được.

Cụ thể, thiết bị đầu cuối xác định liệu NCC của thiết bị đầu cuối có giống như NCC trong NASC nhận được hay không. Trong trường hợp này, NCC của thiết bị đầu cuối sẽ khác với NCC trong NASC nhận được. Do đó, thiết bị đầu cuối dẫn xuất NH dựa trên Kamf và NAS COUNT đường xuống trong NASC, và sau đó dẫn xuất KgNB* dựa trên NH. Các phần mô tả được đưa ra nhờ sử dụng các ví dụ dưới đây dựa vào Fig.5.

Theo một ví dụ, nếu NCC hiện hành của thiết bị đầu cuối bằng 0, và NCC được nhận bởi thiết bị đầu cuối là 1, thì thiết bị đầu cuối trước tiên dẫn xuất KgNB dựa trên Kamf, thiết đặt NH hiện hành của thiết bị đầu cuối ở KgNB, cộng 1 vào NCC hiện hành của thiết bị đầu cuối để thu nhận NCC=1, và sau đó dẫn xuất KgNB* dựa trên NH hiện hành.

Dựa vào Fig. 5, quy trình dẫn xuất trên đây có thể được hiểu như sau: Thiết bị đầu cuối trước tiên thực hiện việc dẫn xuất dọc trên NH và cộng 1 vào NCC của thiết bị đầu cuối, cho đến khi NCC của thiết bị đầu cuối bằng NCC được nhận bởi thiết bị đầu cuối, và sau đó thiết bị đầu cuối thực hiện việc dẫn xuất ngang dựa trên NH được dẫn xuất mới nhất, để thu nhận KgNB*.

Bước 314. Thiết bị đầu cuối gửi tin nhắn hoàn thành tái cấu hình RRC đến trạm

gốc đích.

Trong thủ tục chuyển giao trên đây của thiết bị đầu cuối, phía thiết bị đầu cuối dẫn xuất KgNB* và Knas, phía trạm gốc đích cũng dẫn xuất KgNB*, và phía AMF đích dẫn xuất Knas. Do đó, các khóa (KgNB*) được đồng bộ hóa giữa thiết bị đầu cuối và trạm gốc đích, và các khóa (Knas) được đồng bộ hóa giữa thiết bị đầu cuối và AMF đích.

Trong thủ tục trên đây, các lỗi thủ tục chuyển giao là như sau: Ví dụ, lỗi chuyển giao xảy ra do tin nhắn hoàn thành tái cấu hình RRC ở bước 314 không được nhận bởi phía mạng (ví dụ, thiết bị đầu cuối khởi động bộ định thời trước bước 314, và thiết bị đầu cuối không nhận tin nhắn ACK từ trạm gốc trước khi bộ định thời hết hiệu lực, mà chỉ báo rằng thiết bị đầu cuối không gửi tin nhắn hoàn thành tái cấu hình RRC), hoặc tin nhắn tái cấu hình RRC trong bộ chứa RRC được nhận bởi thiết bị đầu cuối ở bước 311 gây ra lỗi tái cấu hình thiết bị đầu cuối (ví dụ, sau bước 311, thiết bị đầu cuối thực hiện cấu hình dựa trên thông số cấu hình trong tin nhắn tái cấu hình RRC, và cấu hình không thành công) do lỗi thông số cấu hình hoặc tương tự. Trong các trường hợp này, khóa mà đã được dẫn xuất bởi thiết bị đầu cuối không được kích hoạt do lỗi. Do đó, khóa trước đó được sử dụng trong thủ tục RRC tiếp theo. Ví dụ, khóa được sử dụng bởi thiết bị đầu cuối được lùi về KgNB (ở đây, KgNB được dẫn xuất dựa trên Kamf).

Fig.4 là hình vẽ giản lược của thủ tục chuyển giao của thiết bị đầu cuối trong kỹ thuật thông thường. Thiết bị đầu cuối được chuyển giao từ trạm gốc nguồn đến trạm gốc đích. Thủ tục chuyển giao được thể hiện trên Fig.4 tương ứng với trường hợp 3.

Thủ tục chuyển giao bao gồm các bước sau đây.

Bước 401 và bước 402 giống như bước 201 và bước 202 trong thủ tục chuyển giao được thể hiện trên Fig.2A. Tham khảo các phần mô tả trên đây.

Bước 403. AMF nguồn xác định Kamf dựa trên chính sách cục bộ.

AMF nguồn xác định không cập nhật Kamf dựa trên chính sách cục bộ.

Hơn nữa, AMF nguồn xác định rằng trạm gốc nguồn và thiết bị đầu cuối đã không được cập nhật khóa tầng truy cập KgNB. Cụ thể, trước khi thiết bị đầu cuối thực hiện thủ tục chuyển giao, Kamf của thiết bị đầu cuối và Kamf của AMF nguồn đã được đồng bộ hóa, nhưng thiết bị đầu cuối thực hiện thủ tục chuyển giao thiết bị đầu cuối trước khi

thiết bị đầu cuối và trạm gốc nguồn cập nhật khóa tầng truy cập KgNB. Do đó, trạm gốc đích và thiết bị đầu cuối có thể được thông báo để cập nhật khóa tầng truy cập KgNB trong thủ tục chuyển giao.

Bước 404. AMF nguồn gửi tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối đến AMF đích.

Theo một cách thực hiện, tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối có thể là, ví dụ, tin nhắn yêu cầu Namf_Communication_CreateUEContext.

Tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối có thể bao gồm keyAmfChangeInd, NAS COUNT đường xuống, Kamf, và khả năng bảo mật thiết bị đầu cuối. Tùy chọn là, tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối có thể bao gồm thuật toán gốc được sử dụng bởi thiết bị đầu cuối, tức là, thuật toán hiện được sử dụng bởi thiết bị đầu cuối.

keyAmfChangeInd được sử dụng để chỉ báo rằng Kamf không được đồng bộ hóa một cách tạm thời với trạm gốc, tức là, chỉ báo rằng khóa tầng truy cập của trạm gốc đã không được cập nhật dựa trên Kamf. Khả năng bảo mật thiết bị đầu cuối được sử dụng để chỉ báo thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối. NAS COUNT đường xuống là thông số về làm mới.

Sau khi nhận tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối, AMF đích chọn thuật toán mới dựa trên khả năng bảo mật thiết bị đầu cuối và danh sách ưu tiên thuật toán cục bộ, nhưng thuật toán mới chọn được giống như thuật toán gốc của thiết bị đầu cuối, hoặc thuật toán gốc của thiết bị đầu cuối là thuật toán có mức ưu tiên cao nhất trong danh sách ưu tiên thuật toán cục bộ của AMF đích. Do đó, AMF đích không chọn thuật toán mới. Trong trường hợp này, do thuật toán của thiết bị đầu cuối không cần được cập nhật, và Kamf cũng không cần được cập nhật, nên AMF đích không xây dựng NASC.

Bước 405. AMF đích dẫn xuất khóa tầng truy cập thứ nhất (KgNB) dựa trên Kamf.

Bước 406. AMF đích gửi tin nhắn yêu cầu chuyển giao (HO Request) đến trạm gốc đích, trong đó tin nhắn này có thể bao gồm NSCI và {NH, NCC}.

NSCI được tạo ra bởi AMF đích dựa trên keyAmfChangeInd, và NSCI được sử dụng để chỉ báo trạm gốc để cập nhật khóa tầng truy cập. AMF đích thiết đặt NH trong {NH, NCC} ở KgNB được tạo ra bởi AMF đích ở bước 405, và thiết đặt NCC ở 0.

Theo một cách thực hiện khác của bước 405 và bước 406, AMF đích có thể dẫn xuất NH tiếp theo dựa trên Kamf và NH hiện hành, và sau đó cộng 1 vào NCC. Ngoài ra, NH có trong tin nhắn yêu cầu chuyển giao được gửi bởi AMF đích đến trạm gốc đích là NH được dẫn xuất, và NCC có trong tin nhắn yêu cầu chuyển giao được gửi bởi AMF đích đến trạm gốc đích là NCC đã cập nhật. Fig.5 là hình vẽ giản lược của việc dẫn xuất khóa trong 5G.

Theo một ví dụ, nếu NCC hiện hành của AMF đích bằng 0, thì AMF đích trước tiên dẫn xuất NH (cụ thể, NH thứ nhất từ đỉnh đến đáy trên hình vẽ) dựa trên Kamf và KgNB hiện hành, và sau đó cộng 1 vào NCC, tức là, NCC=1.

Theo một ví dụ khác, nếu NCC hiện hành của AMF đích bằng 1, thì AMF đích trước tiên dẫn xuất NH tiếp theo (tức là, NH thứ hai từ đỉnh đến đáy trên hình vẽ) dựa trên Kamf và NH hiện hành (tức là, NH tương ứng với NCC=1 trên hình vẽ, tức là, NH thứ nhất từ đỉnh đến đáy trên hình vẽ), và sau đó cộng 1 vào NCC, tức là, NCC=2.

Theo một ví dụ khác, nếu NCC hiện hành của AMF đích bằng 2, thì AMF đích trước tiên dẫn xuất NH tiếp theo (tức là, NH thứ ba từ đỉnh đến đáy trên hình vẽ) dựa trên Kamf và NH hiện hành (tức là, NH tương ứng với NCC=2 trên hình vẽ, tức là, NH thứ hai từ đỉnh đến đáy trên hình vẽ), và sau đó cộng 1 vào NCC, tức là, NCC=3.

Bước 407. Trạm gốc đích dẫn xuất KgNB* dựa trên NH.

Ví dụ, nếu NH=KgNB, thì trạm gốc đích dẫn xuất KgNB* dựa trên KgNB. Theo một cách thực hiện cụ thể, trạm gốc đích có thể dẫn xuất KgNB* dựa trên PCI đích, ARFCN-DL ô đích, và KgNB.

Theo một ví dụ khác, nếu NH được dẫn xuất bởi AMF đích dựa trên Kamf và NH hiện hành của AMF đích, thì trạm gốc đích dẫn xuất KgNB* dựa trên NH nhận được ở bước 407. Theo một cách thực hiện cụ thể, trạm gốc đích có thể dẫn xuất KgNB* dựa trên PCI đích, ARFCN-DL ô đích, và NH.

Tùy chọn là, trạm gốc đích có thể dẫn xuất các khóa KgNB* mà theo sự tương ứng một-một với các ô của trạm gốc đích.

Bước 408. Trạm gốc đích gửi bộ chứa RRC đến AMF đích.

Bộ chứa RRC bao gồm tin nhắn tái cấu hình kết nối RRC, và tin nhắn này bao

gồm NCC và keychangeindicator. NCC là NCC nhận được ở bước 406. keychangeindicator được tạo ra bởi trạm gốc đích dựa trên NSCI nhận được.

Bước 409. AMF đích gửi tin nhắn hồi đáp tạo ngữ cảnh thiết bị đầu cuối đến AMF nguồn, trong đó tin nhắn này bao gồm bộ chứa RRC.

Theo một cách thực hiện, tin nhắn hồi đáp tạo ngữ cảnh thiết bị đầu cuối có thể là tin nhắn hồi đáp Namf_Communication_CreateUEContext.

Bước 410. AMF nguồn gửi tin nhắn yêu cầu chuyển giao (Handover Request) đến trạm gốc nguồn, trong đó tin nhắn này bao gồm bộ chứa RRC.

Bước 411. Trạm gốc nguồn gửi bộ chứa RRC đến thiết bị đầu cuối. Bộ chứa RRC bao gồm tin nhắn tái cấu hình RRC (RRCReconfiguration).

Bước 412. Dẫn xuất KgNB dựa trên Kamf.

Nếu thiết bị đầu cuối xác định, dựa trên keychangeindicator nhận được, rằng KgNB cần được dẫn xuất, thì thiết bị đầu cuối dẫn xuất KgNB dựa trên Kamf, và thiết đặt NCC tương ứng với KgNB ở 0.

Bước 413. Thiết bị đầu cuối so sánh NCC nhận được với NCC hiện hành của thiết bị đầu cuối. Do các giá trị của hai NCC đều là 0, nên hai NCC là bằng nhau, và thiết bị đầu cuối dẫn xuất KgNB* dựa trên KgNB.

Cần lưu ý rằng, nếu bước 405 và bước 406 được thực hiện bởi cách khác của chúng, thì bước 412 và bước 413 được thay thế bằng cách thực hiện sau đây: Thiết bị đầu cuối xác định, dựa trên keychangeindicator, rằng KgNB cần được dẫn xuất, và thiết đặt NCC tương ứng với KgNB ở 0. Thiết bị đầu cuối trước tiên xác định liệu NCC hiện hành của thiết bị đầu cuối có giống như NCC được nhận bởi thiết bị đầu cuối hay không. Trong trường hợp này, kết quả xác định sẽ là NCC hiện hành của thiết bị đầu cuối không giống như NCC được nhận bởi thiết bị đầu cuối, và thiết bị đầu cuối dẫn xuất NH lớp tiếp theo dựa trên Kamf* và NH hiện hành, và sau đó cộng 1 vào NCC hiện hành của thiết bị đầu cuối. Sau đó, thiết bị đầu cuối tiếp tục xác định liệu NCC hiện hành của thiết bị đầu cuối có giống như NCC được nhận bởi thiết bị đầu cuối hay không, cho đến khi NCC hiện hành của thiết bị đầu cuối giống như NCC được nhận bởi thiết bị đầu cuối. Trong trường hợp này, thiết bị đầu cuối dẫn xuất KgNB* dựa trên NH hiện hành. Theo

một cách thực hiện cụ thể, thiết bị đầu cuối có thể dẫn xuất KgNB* dựa trên PCI ô đích, ARFCN-DL ô đích, và NH hiện hành.

Các phần mô tả được đưa ra nhờ sử dụng các ví dụ dưới đây dựa vào Fig.5. Theo một ví dụ, nếu NCC hiện hành của thiết bị đầu cuối bằng 0, và NCC được nhận bởi thiết bị đầu cuối là 1, thì thiết bị đầu cuối trước tiên dẫn xuất NH dựa trên Kamf và KgNB hiện hành, cộng 1 vào NCC hiện hành của thiết bị đầu cuối để thu nhận NCC=1, và sau đó dẫn xuất KgNB* dựa trên NH của thiết bị đầu cuối.

Dựa vào Fig. 5, quy trình dẫn xuất trên đây có thể được hiểu như sau: Thiết bị đầu cuối trước tiên thực hiện việc dẫn xuất dọc trên NH và cộng 1 vào NCC của thiết bị đầu cuối, cho đến khi NCC của thiết bị đầu cuối bằng NCC được nhận bởi thiết bị đầu cuối, và sau đó thiết bị đầu cuối thực hiện việc dẫn xuất ngang dựa trên NH mới nhất thông qua việc dẫn xuất, để thu nhận KgNB*.

Bước 414. Thiết bị đầu cuối gửi tin nhắn hoàn thành tái cấu hình RRC đến trạm gốc đích.

Trong thủ tục chuyển giao trên đây của thiết bị đầu cuối, phía thiết bị đầu cuối dẫn xuất KgNB* dựa trên Kamf gốc. Phía trạm gốc đích dẫn xuất KgNB*, sao cho các khóa (KgNB*) được đồng bộ hóa giữa thiết bị đầu cuối và trạm gốc đích.

Trong thủ tục trên đây, các lỗi thủ tục chuyển giao là như sau: Ví dụ, lỗi chuyển giao xảy ra do tin nhắn hoàn thành tái cấu hình RRC ở bước 414 không được nhận bởi phía mạng (ví dụ, thiết bị đầu cuối khởi động bộ định thời trước bước 414, và thiết bị đầu cuối không nhận tin nhắn ACK từ trạm gốc trước khi bộ định thời hết hiệu lực, mà chỉ báo rằng thiết bị đầu cuối không gửi tin nhắn hoàn thành tái cấu hình RRC), hoặc tin nhắn tái cấu hình RRC trong bộ chứa RRC được nhận bởi thiết bị đầu cuối ở bước 411 gây ra lỗi tái cấu hình thiết bị đầu cuối (ví dụ, sau bước 411, thiết bị đầu cuối thực hiện cấu hình dựa trên thông số cấu hình trong tin nhắn tái cấu hình RRC, và cấu hình không thành công) do lỗi thông số cấu hình hoặc tương tự. Trong các trường hợp này, khóa mà đã được dẫn xuất bởi thiết bị đầu cuối không được kích hoạt do lỗi. Do đó, khóa trước đó được sử dụng trong thủ tục RRC tiếp theo. Ví dụ, khóa được sử dụng bởi thiết bị đầu cuối được lùi về KgNB2 (ở đây, KgNB2 được dẫn xuất dựa trên Kamf1).

Đối với ba trường hợp được thể hiện trên các hình vẽ từ Fig.2A đến Fig.4 trên đây, khi thiết bị đầu cuối xác định rằng thủ tục chuyển giao không thành công, thiết bị đầu cuối khởi tạo thủ tục thiết lập lại, như được thể hiện trong mỗi hình vẽ trong số các hình vẽ từ Fig.7 đến Fig.9. Fig.6 là hình vẽ giản lược của thủ tục thiết lập lại của thiết bị đầu cuối trong 5G trong kỹ thuật thông thường. Thủ tục thiết lập lại giống như thủ tục thiết lập lại trong 4G. Ngoài ra, sáng chế đặc trưng cho trường hợp trong đó ô được chọn lại bởi thiết bị đầu cuối là ô của trạm gốc đích trong thủ tục chuyển giao trên đây. Sau khi thủ tục chuyển giao không thành công, khóa trên thiết bị đầu cuối không phù hợp với khóa trên trạm gốc đích. Do đó, trong thủ tục thiết lập lại, các khóa của thiết bị đầu cuối và trạm gốc đích cần được cập nhật, sao cho khóa của thiết bị đầu cuối phù hợp với khóa của trạm gốc đích.

Thủ tục này bao gồm các bước sau đây.

Bước 601. Thiết bị đầu cuối gửi tin nhắn yêu cầu thiết lập lại đến trạm gốc đích.

Tùy chọn là, tin nhắn yêu cầu thiết lập lại bao gồm thông số xác thực định danh.

Bước 602. Trạm gốc đích thu nhận KgNB*.

Tùy chọn là, khi tin nhắn yêu cầu thiết lập lại bao gồm thông số xác thực định danh, trạm gốc đích còn xác thực thiết bị đầu cuối dựa trên thông số xác thực định danh.

Nếu trạm gốc đích tạo ra KgNB* tương ứng đối với ô hiện hành ở bước 208 (hoặc bước 307, hoặc bước 407), thì trạm gốc đích thu nhận, dựa trên thông số xác thực định danh, ngữ cảnh bảo mật tương ứng với thiết bị đầu cuối, và thu nhận tương ứng KgNB*.

Nếu trạm gốc đích không tạo KgNB* tương ứng đối với ô hiện hành ở bước 208 (hoặc bước 307, hoặc bước 407), thì trạm gốc đích dẫn xuất KgNB* phụ thuộc vào việc liệu có NH mà không được sử dụng thành công trong ngữ cảnh hiện hành hay không. Nếu có NH mà không được sử dụng thành công trong ngữ cảnh hiện hành, thì trạm gốc đích dẫn xuất KgNB* dựa trên NH. Nếu không, KgNB* được dẫn xuất dựa trên KgNB hiện hành.

Tùy chọn là, trạm gốc đích dẫn xuất KgNB* dựa trên PCI đích, ARFCN-DL ô đích, và KgNB. Theo cách khác, trạm gốc đích dẫn xuất KgNB* dựa trên PCI đích, ARFCN-DL ô đích, và NH.

Bước 602 là bước tùy chọn.

Bước 603. Trạm gốc đích gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn này bao gồm NCC.

Ở bước này, NCC được mang trong tin nhắn thiết lập lại được gửi bởi trạm gốc đích đến thiết bị đầu cuối. NCC là NCC tương ứng ở bước 602.

Bước 604. Thiết bị đầu cuối dẫn xuất KgNB3 dựa trên NCC nhận được.

Bước 605. Thiết bị đầu cuối gửi tin nhắn hoàn thành thiết lập lại đến trạm gốc.

Do đó, hiện nay, trong thủ tục thiết lập lại trong 5G được thể hiện trên Fig.6, NCC được gửi đến thiết bị đầu cuối bằng cách sử dụng tin nhắn thiết lập lại ở bước 603. Do đó, có vấn đề về cách trong đó thiết bị đầu cuối cập nhật khóa. Cụ thể, trong thủ tục trên đây, khóa của thiết bị đầu cuối không phù hợp với khóa của trạm gốc.

Nguyên nhân chính của lỗi thủ tục thiết lập lại được thể hiện trên Fig.6 là tin nhắn thiết lập lại ở bước 603 mang chỉ thông số NCC, mà là không đủ. Tuy nhiên, hiện nay, trong 5G, chỉ NCC được mang trong tin nhắn thiết lập lại do thủ tục thiết lập lại trong truyền thông thế hệ thứ 4 (4th generation, 4G) vẫn được sử dụng. Trong thủ tục thiết lập lại trong 4G, chỉ NCC được mang trong tin nhắn thiết lập lại do, đối với việc chuyển giao S1 sẵn có trong 4G, thực thể quản lý di động (mobility management entity, MME) không đưa vào dấu hiệu của cách ly khóa (key isolation), và Kasme không thay đổi. Nếu MME thực hiện việc chọn lại thuật toán, thì MME thực hiện việc chọn lại thuật toán sau khi việc chuyển giao S1 được hoàn thành, thay vì thực hiện việc chọn lại thuật toán trong thủ tục chuyển giao. Ngoài ra, nếu khóa tầng truy cập và khóa gốc không được đồng bộ hóa, thì vấn đề là khóa tầng truy cập và khóa gốc không được đồng bộ hóa không được giải quyết trong thủ tục rõ ràng trong 4G. Thay vào đó, ràng buộc ngầm được sử dụng để giải quyết vấn đề này. Nói cách khác, trong 4G, chỉ NCC được mang trong tin nhắn thiết lập lại, sao cho các khóa giữa thiết bị đầu cuối và trạm gốc đích có thể là phù hợp. Tuy nhiên, trong 5G, do sự cải tiến bảo mật, cách ly khóa cần được thực hiện trong suốt quá trình chuyển giao AMF, và thuật toán mới hoặc khóa tầng truy cập đồng bộ có thể được chọn trong thủ tục chuyển giao. Do đó, NASC và keychangeindicator xuất hiện. Kết quả là, do đó không đủ để gửi chỉ NCC trong tin nhắn

thiết lập lại, và các khóa là không phù hợp.

Do đó, trong thủ tục thiết lập lại trong kỹ thuật thông thường được thể hiện trên Fig.6, khóa của thiết bị đầu cuối không phù hợp với khóa của trạm gốc. Để giải quyết vấn đề này, sáng chế đề xuất phương pháp truyền thông vô tuyến. Phương pháp truyền thông vô tuyến bao gồm thủ tục thiết lập lại của thiết bị đầu cuối, và tùy chọn là còn bao gồm thủ tục chuyển giao của thiết bị đầu cuối. Phương pháp truyền thông vô tuyến được đề xuất theo sáng chế có thể được sử dụng để giải quyết vấn đề tồn tại trong thủ tục thiết lập lại được thể hiện trên Fig.6.

Trong thủ tục thiết lập lại được đề xuất theo sáng chế, ngoài NCC, tin nhắn thiết lập lại ở bước 603 còn mang thông tin dẫn xuất khóa. Thông tin dẫn xuất khóa bao gồm các thông số cụ thể khác nhau theo các tình huống khác nhau.

Ví dụ, nếu thủ tục chuyển giao của thiết bị đầu cuối là thủ tục chuyển giao được thể hiện trên Fig.2A và Fig.2B, thì thông tin dẫn xuất khóa bao gồm NASC và keychangeindicator, trong đó NASC có thể bao gồm k_AMF_change_flag, chỉ báo NAS_COUNT đường xuống, bộ nhận dạng của thuật toán được chọn, NAS MAC, và tương tự, và keychangeindicator được sử dụng để chỉ báo cập nhật khóa tầng truy cập.

Theo một ví dụ khác, nếu thủ tục chuyển giao của thiết bị đầu cuối là thủ tục chuyển giao được thể hiện trên Fig.3, thì thông tin dẫn xuất khóa bao gồm NASC, trong đó NASC có thể bao gồm bộ nhận dạng của thuật toán được chọn, NAS MAC, và tương tự.

Theo một ví dụ khác, nếu thủ tục chuyển giao của thiết bị đầu cuối là thủ tục chuyển giao được thể hiện trên Fig.4, thì thông tin dẫn xuất khóa bao gồm keychangeindicator, trong đó keychangeindicator được sử dụng để chỉ báo cập nhật khóa tầng truy cập.

Nói cách khác, thông số được mang trong tin nhắn thiết lập lại theo sáng chế giống như thông số được mang trong tin nhắn tái cấu hình RRC trong thủ tục chuyển giao. Nếu tin nhắn tái cấu hình RRC mang NCC, NASC, và keychangeindicator, thì tin nhắn thiết lập lại trong thủ tục thiết lập lại cũng mang NCC, NASC, và keychangeindicator. Nếu tin nhắn tái cấu hình RRC mang NCC và NASC, thì tin nhắn thiết lập lại trong thủ

tục thiết lập lại cũng mang NCC và NASC. Nếu tin nhắn tái cấu hình RRC mang NCC và keychangeindicator, thì tin nhắn thiết lập lại trong thủ tục thiết lập lại cũng mang NCC và keychangeindicator.

Các trường hợp khác nhau được thể hiện trên các hình vẽ từ Fig.2A đến Fig.4 lần lượt được mô tả chi tiết dưới đây dựa vào các hình vẽ từ Fig.7 đến Fig.9.

Fig.7 là hình vẽ giản lược của thủ tục thiết lập lại theo sáng chế. Thủ tục thiết lập lại được thể hiện trên Fig.7 là thủ tục chuyển giao được thể hiện trên Fig.2A và Fig.2B. Thủ tục thiết lập lại được thể hiện trên Fig.7 có thể được thực hiện sau bước 217 trên Fig.2B sau khi lỗi chuyển giao xảy ra trong thủ tục chuyển giao trên Fig.2A và Fig.2B. Theo cách khác, thủ tục thiết lập lại được thể hiện trên Fig.7 có thể được thực hiện sau bước 212 trên Fig.2B sau khi lỗi tái cấu hình xảy ra trong thủ tục chuyển giao trên Fig.2A và Fig.2B.

Thủ tục thiết lập lại bao gồm các bước sau đây.

Bước 701 và bước 702 giống như bước 601 và bước 602 được thể hiện trên Fig.6. Tham khảo các phần mô tả trên đây.

Bước 703. Trạm gốc gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn thiết lập lại này bao gồm NCC, NASC, và keychangeindicator.

Trạm gốc là trạm gốc đích mà thiết bị đầu cuối sẽ được chuyển giao trong thủ tục chuyển giao. Cần lưu ý rằng thiết bị đầu cuối có thể được thiết lập lại trong cùng một ô của trạm gốc đích, hoặc có thể được thiết lập lại trong các ô khác nhau của trạm gốc đích. Ví dụ, trạm gốc đích mà được chuyển giao đến trên Fig.2A và Fig.2B bao gồm ô A, ô B, và ô C, và trong thủ tục chuyển giao trên Fig.2A và Fig.2B, ô mà thiết bị đầu cuối cần được chuyển giao đến là ô A của trạm gốc đích. Do đó, trong thủ tục thiết lập lại được thể hiện trên Fig.7, thiết bị đầu cuối có thể được thiết lập lại trong ô A của trạm gốc đích, tức là, có thể được thiết lập lại trong cùng một ô của trạm gốc đích, hoặc có thể được thiết lập lại trong ô B hoặc ô C của trạm gốc đích, tức là, có thể được thiết lập lại trong các ô khác nhau của trạm gốc đích.

NASC bao gồm k_AMF_change_flag và chỉ báo NAS COUNT đường xuống, và k_AMF_change_flag được sử dụng để chỉ báo cập nhật khóa gốc. Hơn nữa, NASC có

thể còn bao gồm bộ nhận dạng của thuật toán được chọn, NAS MAC, và tương tự. Chỉ báo NAS COUNT đường xuống được sử dụng để chỉ báo tất cả hoặc một số bit của NAS COUNT đường xuống.

keychangeindicator được sử dụng để chỉ báo cập nhật khóa tầng truy cập.

NASC được thu nhận bởi trạm gốc từ AMF đích ở bước 207 trên Fig.2A. keychangeindicator được tạo ra bởi trạm gốc dựa trên NSCI được gửi bởi AMF đích ở bước 207 trên Fig.2A. Thông thường, trạm gốc xây dựng trực tiếp bộ chứa RRC, và bộ chứa RRC bao gồm NASC và keychangeindicator. Sau khi gửi bộ chứa RRC, trạm gốc không cần lưu trữ NASC và keychangeindicator. Tuy nhiên, do vấn đề mất đồng bộ hóa của ngữ cảnh bảo mật khi thiết lập lại cần được giải quyết, nên trạm gốc cần lưu trữ tạm thời NASC và keychangeindicator, hoặc trạm gốc lưu trữ tạm thời NASC và NSCI, cho đến khi thủ tục chuyển giao được hoàn thành một cách thành công, tức là, tin nhắn tái cấu hình RRC được nhận thành công. Thông tin được lưu trữ bởi trạm gốc có thể được gọi là thông số trung gian. Cụ thể, thông số trung gian được lưu trữ có thể là NASC và keychangeindicator, hoặc có thể là NASC và NSCI. Cũng có thể hiểu rằng, trong quy trình chuẩn bị chuyển giao, trạm gốc thu nhận NSCI và NASC từ AMF đích, trạm gốc xác định keychangeindicator dựa trên NSCI, và sau đó trạm gốc đệm NASC và keychangeindicator, hoặc đệm NASC và NSCI. Quy trình chuẩn bị chuyển giao liên quan đến quy trình truyền ngữ cảnh trước khi phía mạng gửi tin nhắn tái cấu hình RRC đến thiết bị đầu cuối, và có thể bao gồm việc trao đổi các tin nhắn như chuyển giao được đòi hỏi, yêu cầu chuyển giao, yêu cầu tạo ngữ cảnh thiết bị đầu cuối, và hồi đáp tạo ngữ cảnh thiết bị đầu cuối. Các phần mô tả thống nhất được cung cấp ở đây, và các nội dung chi tiết không được mô tả lại trong các phương án khác sau đó.

Khi trạm gốc lưu trữ tạm thời NASC và keychangeindicator, trước khi gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trạm gốc trước tiên thu nhận NASC được đệm và keychangeindicator được đệm, và sau đó gửi tin nhắn yêu cầu thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn yêu cầu thiết lập lại bao gồm NCC, NASC và keychangeindicator.

Khi trạm gốc lưu trữ tạm thời NASC và NSCI, trước khi gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trạm gốc thu nhận NASC và NSCI, và sau đó xác định

keychangeindicator dựa trên NSCI, và gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn thiết lập lại bao gồm NCC, NASC và keychangeindicator.

Tùy chọn là, sau khi hoàn thành một cách thành công việc chuyển giao, trạm gốc xóa thông số trung gian được đệm.

Bước 704. Thiết bị đầu cuối dẫn xuất khóa gốc thứ hai (Kamf*) dựa trên k_AMF_change_flag, chỉ báo NAS COUNT đường xuống, và khóa gốc thứ nhất (Kamf) của thiết bị đầu cuối.

Cụ thể, theo một cách thực hiện, nếu thiết bị đầu cuối nhận k_AMF_change_flag, thì thiết bị đầu cuối xác định rằng khóa gốc của thiết bị đầu cuối cần được cập nhật. Theo một cách thực hiện khác, nếu thiết bị đầu cuối nhận k_AMF_change_flag, và giá trị của k_AMF_change_flag là "1" hoặc "đúng", thì thiết bị đầu cuối xác định rằng khóa gốc của thiết bị đầu cuối cần được cập nhật.

Sau khi xác định rằng khóa gốc của thiết bị đầu cuối cần được cập nhật, thiết bị đầu cuối thu nhận NAS COUNT đường xuống thứ hai dựa trên chỉ báo NAS COUNT đường xuống và NAS COUNT đường xuống thứ nhất của thiết bị đầu cuối, và sau đó thiết bị đầu cuối dẫn xuất Kamf* dựa trên NAS COUNT đường xuống thứ hai và Kamf.

Hơn nữa, sau khi dẫn xuất Kamf*, thiết bị đầu cuối còn có thể dẫn xuất Knas dựa trên Kamf* của thiết bị đầu cuối, và sau đó thiết bị đầu cuối kiểm tra NAS MAC trong NASC nhận được dựa trên thuật toán được chọn trong NASC, chỉ báo NAS COUNT đường xuống, và Knas. Phương pháp kiểm tra cụ thể giống như phương pháp kiểm tra trong thủ tục được thể hiện trên Fig.2A và Fig.2B. Tham khảo các phần mô tả trên đây.

Bước 705. Thiết bị đầu cuối dẫn xuất KgNB của thiết bị đầu cuối dựa trên keychangeindicator và Kamf*.

Cụ thể, theo một cách thực hiện, nếu thiết bị đầu cuối nhận keychangeindicator, thì thiết bị đầu cuối xác định rằng khóa tầng truy cập của thiết bị đầu cuối cần được cập nhật. Theo một cách thực hiện khác, nếu thiết bị đầu cuối nhận keychangeindicator, và giá trị của k_AMF_change_flag là "1" hoặc "đúng", thì thiết bị đầu cuối xác định rằng khóa tầng truy cập của thiết bị đầu cuối cần được cập nhật.

Sau khi xác định rằng khóa tầng truy cập của thiết bị đầu cuối cần được cập nhật,

thiết bị đầu cuối dẫn xuất khóa tầng truy cập thứ nhất (KgNB) của thiết bị đầu cuối dựa trên Kamf*.

Bước 706. Thiết bị đầu cuối dẫn xuất khóa tầng truy cập thứ hai (KgNB*) của thiết bị đầu cuối dựa trên NCC và KgNB của thiết bị đầu cuối.

Cần lưu ý rằng bước 706 cũng có thể được thực hiện theo cách sau đây: Cần lưu ý rằng, nếu bước 206 và bước 207 trong thủ tục chuyển giao được thể hiện trên Fig.2A được thực hiện bởi cách khác của chúng, thì bước 706 và bước 707 được thay thế bằng cách thực hiện sau đây: Thiết bị đầu cuối xác định, dựa trên keychangeindicator, rằng KgNB cần được dẫn xuất, và thiết đặt NCC tương ứng với KgNB ở 0. Thiết bị đầu cuối trước tiên xác định liệu NCC hiện hành của thiết bị đầu cuối có giống như NCC được nhận bởi thiết bị đầu cuối hay không. Trong trường hợp này, kết quả xác định sẽ là NCC hiện hành của thiết bị đầu cuối không giống như NCC được nhận bởi thiết bị đầu cuối, và thiết bị đầu cuối dẫn xuất NH lớp tiếp theo dựa trên Kamf* và NH hiện hành, và sau đó cộng 1 vào NCC hiện hành của thiết bị đầu cuối. Sau đó, thiết bị đầu cuối tiếp tục xác định liệu NCC hiện hành của thiết bị đầu cuối có giống như NCC được nhận bởi thiết bị đầu cuối hay không, cho đến khi NCC hiện hành của thiết bị đầu cuối giống như NCC được nhận bởi thiết bị đầu cuối. Trong trường hợp này, thiết bị đầu cuối dẫn xuất KgNB* dựa trên NH hiện hành. Theo một cách thực hiện cụ thể, thiết bị đầu cuối có thể dẫn xuất KgNB* dựa trên PCI ô đích, ARFCN-DL ô đích, và NH hiện hành.

Bước 707. Thiết bị đầu cuối gửi tin nhắn hoàn thành thiết lập lại đến trạm gốc. Tin nhắn hoàn thành thiết lập lại được bảo vệ bằng cách sử dụng khóa được dẫn xuất dựa trên khóa tầng truy cập thứ hai (KgNB*) của thiết bị đầu cuối.

"Khóa được dẫn xuất dựa trên KgNB* của thiết bị đầu cuối" bao gồm khóa nguyên vẹn và khóa mã hóa. "Bảo vệ" bao gồm bảo vệ tính toàn vẹn và bảo vệ mã hóa. Cụ thể, bảo vệ mã hóa được thực hiện trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu bằng cách sử dụng khóa mã hóa và thuật toán mã hóa. Bảo vệ tính toàn vẹn được thực hiện trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu bằng cách sử dụng khóa bảo vệ tính toàn vẹn và thuật toán bảo vệ tính toàn vẹn. Mối quan hệ liên tiếp giữa bảo vệ mã hóa và bảo vệ tính toàn vẹn không bị giới hạn trong các phương án của sáng chế. Cụ thể, bảo vệ mã hóa có thể được thực hiện trước tiên trên mặt phẳng người dùng/dữ

liệu mặt phẳng báo hiệu, và sau đó bảo vệ tính toàn vẹn được thực hiện. Theo cách khác, bảo vệ tính toàn vẹn có thể được thực hiện trước tiên trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu, và sau đó bảo vệ mã hóa được thực hiện trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu. Tất nhiên, cùng một trình tự thực hiện không thể được sử dụng cho mặt phẳng người dùng và dữ liệu mặt phẳng báo hiệu.

Ví dụ, thiết bị đầu cuối sử dụng khóa tầng truy cập thứ hai làm khóa tầng truy cập hiện hành, dẫn xuất khóa RRC dựa trên khóa tầng truy cập hiện hành, và bảo vệ tin nhắn hoàn thành thiết lập lại dựa trên khóa RRC.

Dựa trên giải pháp trên Fig.7, khi thủ tục chuyển giao của thiết bị đầu cuối không thành công, thiết bị đầu cuối khởi tạo thủ tục thiết lập lại. Khi trạm gốc được chọn lại bởi thiết bị đầu cuối là trạm gốc (tức là, trạm gốc đích) mà thiết bị đầu cuối được chuyển giao đến trong thủ tục chuyển giao, do khóa của trạm gốc được cập nhật trong thủ tục chuyển giao, và thông số trung gian được lưu trữ (ví dụ, NASC và keychangeindicator được lưu trữ, hoặc NASC và NSCI được lưu trữ), trạm gốc bao gồm thông tin dẫn xuất khóa trong tin nhắn thiết lập lại sẽ được gửi đến thiết bị đầu cuối. Do đó, thiết bị đầu cuối có thể cập nhật khóa của thiết bị đầu cuối dựa trên thông tin dẫn xuất khóa, sao cho khóa của thiết bị đầu cuối có thể phù hợp với khóa ở phía mạng.

Fig.8 là hình vẽ giản lược của thủ tục thiết lập lại theo sáng chế. Thủ tục thiết lập lại được thể hiện trên Fig.8 là thủ tục chuyển giao được thể hiện trên Fig. 3. Thủ tục thiết lập lại được thể hiện trên Fig.8 có thể được thực hiện sau bước 314 trên Fig.3 sau khi lỗi chuyển giao xảy ra trong thủ tục chuyển giao trên Fig.3. Theo cách khác, thủ tục thiết lập lại được thể hiện trên Fig.7 có thể được thực hiện sau bước 311 trên Fig.3 sau khi lỗi tái cấu hình xảy ra trong thủ tục chuyển giao trên Fig.3.

Thủ tục thiết lập lại bao gồm các bước sau đây.

Bước 801 và bước 802 giống như bước 601 và bước 602 được thể hiện trên Fig.6. Tham khảo các phần mô tả trên đây.

Bước 803. Trạm gốc gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn thiết lập lại bao gồm NCC và NASC.

Trạm gốc là trạm gốc đích mà thiết bị đầu cuối sẽ được chuyển giao trong thủ tục

chuyển giao. Cần lưu ý rằng thiết bị đầu cuối có thể được thiết lập lại trong cùng một ô của trạm gốc đích, hoặc có thể được thiết lập lại trong các ô khác nhau của trạm gốc đích. Ví dụ, trạm gốc đích mà được chuyển giao đến trên Fig.3 bao gồm ô A, ô B, và ô C, và trong thủ tục chuyển giao trên Fig.3, ô mà thiết bị đầu cuối cần được chuyển giao đến là ô A của trạm gốc đích. Do đó, trong thủ tục thiết lập lại được thể hiện trên Fig.8, thiết bị đầu cuối có thể được thiết lập lại trong ô A của trạm gốc đích, tức là, có thể được thiết lập lại trong cùng một ô của trạm gốc đích, hoặc có thể được thiết lập lại trong ô B hoặc ô C của trạm gốc đích, tức là, có thể được thiết lập lại trong các ô khác nhau của trạm gốc đích.

NASC bao gồm chỉ báo NAS COUNT đường xuống, thuật toán được chọn, NAS MAC, và tương tự. Chỉ báo NAS COUNT đường xuống được sử dụng để chỉ báo tất cả hoặc một số bit của NAS COUNT đường xuống.

Hơn nữa, sau khi nhận tin nhắn thiết lập lại, thiết bị đầu cuối có thể dẫn xuất Knas dựa trên Kamf của thiết bị đầu cuối, và sau đó thiết bị đầu cuối kiểm tra NAS MAC trong NASC nhận được dựa trên thuật toán được chọn trong NASC, chỉ báo NAS COUNT đường xuống, và Knas. Phương pháp kiểm tra cụ thể giống như phương pháp kiểm tra trong thủ tục được thể hiện trên Fig.3. Tham khảo phần mô tả trên đây.

NASC được thu nhận bởi trạm gốc từ AMF đích ở bước 306 trên Fig.3. Thông thường, trạm gốc xây dựng trực tiếp bộ chứa RRC, và bộ chứa RRC bao gồm NASC. Sau khi gửi bộ chứa RRC, trạm gốc không cần lưu trữ NASC. Tuy nhiên, do vấn đề mất đồng bộ hóa của ngữ cảnh bảo mật khi thiết lập lại cần được giải quyết, nên trạm gốc cần lưu trữ tạm thời NASC, hoặc trạm gốc lưu trữ tạm thời NASC, cho đến khi thủ tục chuyển giao được hoàn thành một cách thành công, tức là, tin nhắn tái cấu hình RRC được nhận thành công. Thông tin được lưu trữ bởi trạm gốc có thể được gọi là thông số trung gian. Cụ thể, thông số trung gian được lưu trữ có thể là NASC. Cũng có thể hiểu rằng, trong quy trình chuẩn bị chuyển giao, trạm gốc thu nhận NASC từ AMF đích, và sau đó trạm gốc đệm NASC.

Khi trạm gốc lưu trữ tạm thời NASC, trước khi gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trạm gốc trước tiên thu nhận NASC được đệm, và sau đó gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn thiết lập lại bao gồm NCC và NASC.

Bước 804. Thiết bị đầu cuối dẫn xuất khóa tầng truy cập thứ hai (KgNB*) của thiết bị đầu cuối dựa trên NCC và KgNB của thiết bị đầu cuối.

Tùy chọn là, sau khi hoàn thành một cách thành công việc chuyển giao, trạm gốc xóa thông số trung gian được đệm.

Bước 805. Thiết bị đầu cuối gửi tin nhắn hoàn thành thiết lập lại đến trạm gốc. Tin nhắn hoàn thành thiết lập lại được bảo vệ bằng cách sử dụng khóa được dẫn xuất dựa trên khóa tầng truy cập thứ hai (KgNB*) của thiết bị đầu cuối.

"Khóa được dẫn xuất dựa trên KgNB* của thiết bị đầu cuối" bao gồm khóa nguyên vẹn và khóa mã hóa. "Bảo vệ" bao gồm bảo vệ tính toàn vẹn và bảo vệ mã hóa. Cụ thể, bảo vệ mã hóa được thực hiện trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu bằng cách sử dụng khóa mã hóa và thuật toán mã hóa. Bảo vệ tính toàn vẹn được thực hiện trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu bằng cách sử dụng khóa bảo vệ tính toàn vẹn và thuật toán bảo vệ tính toàn vẹn. Mối quan hệ liên tiếp giữa bảo vệ mã hóa và bảo vệ tính toàn vẹn không bị giới hạn trong các phương án của sáng chế. Cụ thể, bảo vệ mã hóa có thể được thực hiện trước tiên trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu, và sau đó bảo vệ tính toàn vẹn được thực hiện. Theo cách khác, bảo vệ tính toàn vẹn có thể được thực hiện trước tiên trên mặt phẳng người dùng/mặt phẳng báo hiệu, và sau đó bảo vệ mã hóa được thực hiện trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu. Tất nhiên, cùng một trình tự thực hiện không thể được sử dụng cho mặt phẳng người dùng và mặt phẳng báo hiệu.

Ví dụ, thiết bị đầu cuối sử dụng khóa tầng truy cập thứ hai làm khóa tầng truy cập hiện hành, dẫn xuất khóa RRC dựa trên khóa tầng truy cập hiện hành, và bảo vệ tin nhắn hoàn thành thiết lập lại dựa trên khóa RRC.

Dựa trên giải pháp trên Fig.8, khi thủ tục chuyển giao của thiết bị đầu cuối không thành công, thiết bị đầu cuối khởi tạo thủ tục thiết lập lại. Khi trạm gốc được chọn lại bởi thiết bị đầu cuối là trạm gốc (tức là, trạm gốc đích) mà thiết bị đầu cuối được chuyển giao đến trong thủ tục chuyển giao, do khóa của trạm gốc được cập nhật trong thủ tục chuyển giao, và thông số trung gian được lưu trữ (ví dụ, NASC được lưu trữ), trạm gốc bao gồm thông tin dẫn xuất khóa trong tin nhắn thiết lập lại sẽ được gửi đến thiết bị đầu cuối. Do đó, thiết bị đầu cuối có thể cập nhật khóa của thiết bị đầu cuối dựa trên thông

tin dẫn xuất khóa, sao cho khóa của thiết bị đầu cuối có thể phù hợp với khóa ở phía mạng.

Fig.9 là hình vẽ giản lược của thủ tục thiết lập lại theo sáng chế. Thủ tục thiết lập lại được thể hiện trên Fig.9 là thủ tục chuyển giao được thể hiện trên Fig.4. Thủ tục thiết lập lại được thể hiện trên Fig.9 có thể được thực hiện sau bước 414 trên Fig.4 sau khi lỗi chuyển giao xảy ra trong thủ tục chuyển giao trên Fig.4. Theo cách khác, thủ tục thiết lập lại được thể hiện trên Fig.9 có thể được thực hiện sau bước 411 trên Fig.4 sau khi lỗi tái cấu hình xảy ra trong thủ tục chuyển giao trên Fig.4.

Thủ tục thiết lập lại bao gồm các bước sau đây.

Bước 901 và bước 902 giống như bước 601 và bước 602 được thể hiện trên Fig.9. Tham khảo các phần mô tả trên đây.

Bước 903. Trạm gốc gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn thiết lập lại bao gồm NCC và keychangeindicator.

Trạm gốc là trạm gốc đích mà thiết bị đầu cuối sẽ được chuyển giao trong thủ tục chuyển giao. Cần lưu ý rằng thiết bị đầu cuối có thể được thiết lập lại trong cùng một ô của trạm gốc đích, hoặc có thể được thiết lập lại trong các ô khác nhau của trạm gốc đích. Ví dụ, trạm gốc đích mà được chuyển giao đến trên Fig.4 bao gồm ô A, ô B, và ô C, và trong thủ tục chuyển giao trên Fig.4, ô mà thiết bị đầu cuối cần được chuyển giao đến là ô A của trạm gốc đích. Do đó, trong thủ tục thiết lập lại được thể hiện trên Fig.9, thiết bị đầu cuối có thể được thiết lập lại trong ô A của trạm gốc đích, tức là, có thể được thiết lập lại trong cùng một ô của trạm gốc đích, hoặc có thể được thiết lập lại trong ô B hoặc ô C của trạm gốc đích, tức là, có thể được thiết lập lại trong các ô khác nhau của trạm gốc đích.

keychangeindicator được sử dụng để chỉ báo cập nhật khóa tầng truy cập.

keychangeindicator được tạo ra bởi trạm gốc đích ở bước 406 trên Fig.4 dựa trên NSCI được gửi bởi AMF đích. Thông thường, sau khi gửi keychangeindicator, trạm gốc đích không cần lưu trữ keychangeindicator. Tuy nhiên, do vấn đề mất đồng bộ hóa của ngữ cảnh bảo mật khi thiết lập lại cần được giải quyết, nên trạm gốc đích cần lưu trữ tạm thời keychangeindicator, hoặc trạm gốc lưu trữ tạm thời NSCI, cho đến khi thủ tục

chuyển giao được hoàn thành một cách thành công, tức là, tin nhắn tái cấu hình RRC được nhận thành công. Thông tin được lưu trữ bởi trạm gốc có thể được gọi là thông số trung gian. Cụ thể, thông số trung gian được lưu trữ có thể là keychangeindicator hoặc NSCI. Cũng có thể hiểu rằng, trong quy trình chuẩn bị chuyển giao, trạm gốc thu nhận NSCI từ AMF đích, trạm gốc xác định keychangeindicator dựa trên NSCI, và sau đó trạm gốc đệm keychangeindicator hoặc đệm NSCI.

Khi trạm gốc lưu trữ tạm thời keychangeindicator, trước khi gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trạm gốc trước tiên thu nhận keychangeindicator được đệm, và sau đó gửi tin nhắn yêu cầu thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn yêu cầu thiết lập lại bao gồm NCC và keychangeindicator.

Khi trạm gốc lưu trữ tạm thời NSCI, trước khi gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trạm gốc thu nhận NSCI, và sau đó xác định keychangeindicator dựa trên NSCI, và gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn thiết lập lại bao gồm NCC và keychangeindicator.

Tùy chọn là, sau khi hoàn thành một cách thành công việc chuyển giao, trạm gốc xóa thông số trung gian được đệm.

Bước 904. Thiết bị đầu cuối dẫn xuất KgNB của thiết bị đầu cuối dựa trên Kamf và keychangeindicator.

Cụ thể, theo một cách thực hiện, nếu thiết bị đầu cuối nhận keychangeindicator, thì thiết bị đầu cuối xác định rằng khóa tầng truy cập của thiết bị đầu cuối cần được cập nhật. Theo một cách thực hiện khác, nếu thiết bị đầu cuối nhận keychangeindicator, và giá trị của k_AMF_change_flag là "1" hoặc "đúng", thì thiết bị đầu cuối xác định rằng khóa tầng truy cập của thiết bị đầu cuối cần được cập nhật.

Sau khi xác định rằng khóa tầng truy cập của thiết bị đầu cuối cần được cập nhật, thiết bị đầu cuối dẫn xuất khóa tầng truy cập thứ nhất (KgNB) của thiết bị đầu cuối dựa trên Kamf.

Bước 905. Thiết bị đầu cuối dẫn xuất khóa tầng truy cập thứ hai (KgNB*) của thiết bị đầu cuối dựa trên NCC và KgNB của thiết bị đầu cuối.

Đối với cách thực hiện cụ thể của bước này, tham khảo bước 413 trong thủ tục

chuyển giao được thể hiện trên Fig.4. Bước 906. Thiết bị đầu cuối gửi tin nhắn hoàn thành thiết lập lại đến trạm gốc. Tin nhắn hoàn thành thiết lập lại được bảo vệ bằng cách sử dụng khóa được dẫn xuất dựa trên khóa tầng truy cập thứ hai (KgNB*) của thiết bị đầu cuối.

"Khóa được dẫn xuất dựa trên KgNB* của thiết bị đầu cuối" bao gồm khóa nguyên vẹn và khóa mã hóa. "Bảo vệ" bao gồm bảo vệ tính toàn vẹn và bảo vệ mã hóa. Cụ thể, bảo vệ mã hóa được thực hiện trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu bằng cách sử dụng khóa mã hóa và thuật toán mã hóa. Bảo vệ tính toàn vẹn được thực hiện trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu bằng cách sử dụng khóa bảo vệ tính toàn vẹn và thuật toán bảo vệ tính toàn vẹn. Mối quan hệ liên tiếp giữa bảo vệ mã hóa và bảo vệ tính toàn vẹn không bị giới hạn trong các phương án của sáng chế. Cụ thể, bảo vệ mã hóa có thể được thực hiện trước tiên trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu, và sau đó bảo vệ tính toàn vẹn được thực hiện. Theo cách khác, bảo vệ tính toàn vẹn có thể được thực hiện trước tiên trên mặt phẳng người dùng/mặt phẳng báo hiệu, và sau đó bảo vệ mã hóa được thực hiện trên mặt phẳng người dùng/dữ liệu mặt phẳng báo hiệu. Tất nhiên, cùng một trình tự thực hiện không thể được sử dụng cho mặt phẳng người dùng và mặt phẳng báo hiệu.

Ví dụ, thiết bị đầu cuối sử dụng khóa tầng truy cập thứ hai làm khóa tầng truy cập hiện hành, dẫn xuất khóa RRC dựa trên khóa tầng truy cập hiện hành, và bảo vệ tin nhắn hoàn thành thiết lập lại dựa trên khóa RRC. Dựa trên giải pháp trên Fig.9, khi thủ tục chuyển giao của thiết bị đầu cuối không thành công, thiết bị đầu cuối khởi tạo thủ tục thiết lập lại. Khi trạm gốc được chọn lại bởi thiết bị đầu cuối là trạm gốc (tức là, trạm gốc đích) mà thiết bị đầu cuối được chuyển giao đến trong thủ tục chuyển giao, do khóa của trạm gốc được cập nhật trong thủ tục chuyển giao, và thông số trung gian được lưu trữ (ví dụ, keychangeindicator được lưu trữ, hoặc NSCI được lưu trữ), trạm gốc bao gồm thông tin dẫn xuất khóa trong tin nhắn thiết lập lại sẽ được gửi đến thiết bị đầu cuối. Do đó, thiết bị đầu cuối có thể cập nhật khóa của thiết bị đầu cuối dựa trên thông tin dẫn xuất khóa, sao cho khóa của thiết bị đầu cuối có thể phù hợp với khóa của phía mạng.

Dựa vào phương án bất kỳ trong số các phương án trên đây, nếu NASC cần được gửi đến thiết bị đầu cuối theo các phương án này, theo một quy trình thực hiện cụ thể,

NASC bao gồm chỉ báo NAS COUNT đường xuống, thuật toán được chọn, NAS MAC thứ nhất, và tương tự. Chỉ báo NAS COUNT đường xuống có thể bao gồm một số hoặc tất cả các bit của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm một số hoặc tất cả bit của NAS MAC thứ hai. NAS MAC thứ hai liên quan đến NAS MAC được tính toán bởi trạm gốc.

Theo cách thực hiện cụ thể, ít nhất các cách thực hiện sau đây được bao gồm.

Cách thực hiện 1: Chỉ báo NAS COUNT đường xuống bao gồm tất cả các bit của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm tất cả các bit của NAS MAC thứ hai.

Theo một ví dụ, NASC bao gồm các thông số sau đây: NAS COUNT đường xuống có 32 bit, ngKSI có 4 bit, và thuật toán được chọn (các thuật toán bảo mật NAS được chọn) có 6 bit, và NAS MAC thứ hai có 32 bit, trong đó có tổng cộng 74 bit.

Trong ví dụ này, chỉ báo NAS COUNT đường xuống có trong NASC mà được gửi đến thiết bị đầu cuối có 32 bit, NAS MAC thứ hai có 32 bit, thuật toán được chọn có 6 bit, và ngKSI có 4 bit.

Dựa trên cách thực hiện này, sau khi nhận NASC, thiết bị đầu cuối thu nhận các thông số như chỉ báo NAS COUNT đường xuống và NAS MAC thứ nhất trong NASC, tạo ra NAS MAC dựa trên Knas, thuật toán được chọn, và chỉ báo NAS COUNT đường xuống, và sau đó kiểm tra NAS MAC thứ nhất của NASC dựa trên NAS MAC tạo thành.

Cách thực hiện 2: Chỉ báo NAS COUNT đường xuống bao gồm một số bit (ví dụ, L1 bit thấp) của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm tất cả các bit của NAS MAC thứ hai, trong đó L1 là số nguyên dương.

Theo cách thực hiện này, NAS COUNT đường xuống bị cắt tỉa (truncated), và NAS MAC thứ hai không bị cắt tỉa.

Vẫn sử dụng ví dụ trong cách thực hiện 1, L1 được thiết đặt trước ở 5, tức là, 5 bit thấp của NAS COUNT đường xuống được thu nhận qua cắt tỉa. Trong trường hợp này, chỉ báo NAS COUNT đường xuống có trong NASC mà được gửi đến thiết bị đầu cuối có 5 bit, NAS MAC thứ nhất có 32 bit, thuật toán được chọn có 6 bit, và ngKSI có 4 bit.

Dựa trên cách thực hiện này, sau khi nhận NASC, thiết bị đầu cuối thu nhận các

thông số như chỉ báo NAS COUNT đường xuống và NAS MAC thứ nhất trong NASC, và thu nhận NAS COUNT đường xuống thứ hai dựa trên NAS COUNT đường xuống thứ nhất của thiết bị đầu cuối và chỉ báo NAS COUNT đường xuống. Sau đó, NAS MAC được tạo ra dựa trên Knas, thuật toán được chọn, và NAS COUNT đường xuống thứ hai. Thiết bị đầu cuối kiểm tra NAS MAC thứ nhất của NASC dựa trên NAS MAC tạo thành.

Cách thực hiện 3: Chỉ báo NAS COUNT đường xuống bao gồm một số bit (ví dụ, L2 bit thấp) của NAS COUNT đường xuống, NAS MAC thứ nhất bao gồm một số bit (ví dụ, L3 bit thấp hoặc L4 bit cao) của NAS MAC thứ hai, trong đó L2 là số nguyên dương, L3 là số nguyên dương, và L4 là số nguyên dương.

Theo cách thực hiện này, cả NAS COUNT đường xuống lẫn NAS MAC thứ hai đều bị cắt tỉa.

Theo một ví dụ, vẫn sử dụng ví dụ trong cách thực hiện 1, nếu L2 được thiết đặt trước ở 8, NAS MAC thứ nhất bao gồm L3 bit thấp của NAS MAC thứ hai, và L3 được thiết đặt trước ở 16, tức là, 8 bit thấp của NAS COUNT đường xuống được thu nhận qua cắt tỉa, và 16 bit thấp của NAS MAC thứ hai được thu nhận qua cắt tỉa, chỉ báo NAS COUNT đường xuống có trong NASC mà được gửi đến thiết bị đầu cuối có 8 bit, NAS MAC thứ nhất có 16 bit, thuật toán được chọn có 6 bit, và ngKSI có 4 bit.

Theo một ví dụ khác, vẫn sử dụng ví dụ trong cách thực hiện 1, nếu L2 được thiết đặt trước ở 8, NAS MAC thứ nhất bao gồm L4 bit cao của NAS MAC thứ hai, và L4 được thiết đặt trước ở 16, tức là, 8 bit thấp của NAS COUNT đường xuống được thu nhận qua cắt tỉa, và 16 bit cao của NAS MAC thứ hai được thu nhận qua cắt tỉa, chỉ báo NAS COUNT đường xuống có trong NASC mà được gửi đến thiết bị đầu cuối có 8 bit, NAS MAC thứ nhất có 16 bit, thuật toán được chọn có 6 bit, và ngKSI có 4 bit.

Dựa trên cách thực hiện này, sau khi nhận NASC, thiết bị đầu cuối thu nhận NAS COUNT đường xuống thứ hai dựa trên NAS COUNT đường xuống thứ nhất của thiết bị đầu cuối và chỉ báo NAS COUNT đường xuống. Thiết bị đầu cuối tạo ra NAS MAC dựa trên Knas, thuật toán được chọn, và NAS COUNT đường xuống thứ hai. Thiết bị đầu cuối kiểm tra NAS MAC thứ nhất của NASC dựa trên 16 bit thấp hoặc 16 bit cao của NAS MAC tạo thành.

Cách thực hiện 4: Chỉ báo NAS COUNT đường xuống bao gồm tất cả các bit của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm một số bit (ví dụ, L5 bit thấp) của NAS MAC thứ hai.

Theo cách thực hiện này, NAS MAC thứ hai bị cắt tỉa. Ví dụ, trạm gốc đích cắt tỉa NASC.

Ví dụ trong cách thực hiện 1 vẫn được sử dụng, và L5 được thiết đặt trước ở 6. Khi gửi tin nhắn thiết lập lại, trạm gốc đích cắt tỉa trực tiếp 48 bit đầu tiên của NASC có 74 bit dựa trên cách ngoài cùng bên trái. Trong trường hợp này, NAS MAC thứ hai chỉ có 6 bit còn lại. Trạm gốc đích gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn này bao gồm NASC bị cắt tỉa, chỉ báo NAS COUNT đường xuống có trong NASC có 32 bit, NAS MAC thứ nhất có 6 bit, thuật toán được chọn có 6 bit, và ngKSI có 4 bit.

Dựa trên cách thực hiện này, sau khi nhận NASC, thiết bị đầu cuối tạo ra NAS MAC dựa trên Knas, thuật toán được chọn, và chỉ báo NAS COUNT đường xuống của NASC, và sau đó kiểm tra NAS MAC thứ nhất của NASC dựa trên 6 bit thấp của NAS MAC tạo thành.

Khi bộ phận tích hợp được sử dụng, Fig.10 là sơ đồ khối ví dụ khả thi của thiết bị 1000 theo một phương án của sáng chế. Thiết bị 1000 có thể tồn tại dưới dạng phần mềm. Thiết bị 1000 có thể bao gồm bộ phận xử lý 1002 và bộ phận truyền thông 1003. Theo một cách thực hiện, bộ phận truyền thông 1003 có thể bao gồm bộ phận nhận và bộ phận gửi. Bộ phận xử lý 1002 được tạo cấu hình để điều khiển và quản lý hoạt động của thiết bị 1000. Bộ phận truyền thông 1003 được tạo cấu hình để hỗ trợ thiết bị 1000 khi truyền thông với một thực thể mạng khác. Thiết bị 1000 có thể còn bao gồm bộ phận lưu trữ 1001, được tạo cấu hình để lưu trữ mã chương trình và dữ liệu của thiết bị 1000.

Bộ phận xử lý 1002 có thể là bộ xử lý hoặc bộ điều khiển, ví dụ, bộ xử lý trung tâm (central processing unit, CPU), bộ xử lý đa năng, bộ xử lý tín hiệu số (digital signal processing, DSP), mạch tích hợp chuyên dụng (application specific integrated circuits, ASIC), mảng cổng lập trình được dạng trường (field programmable gate array, FPGA), hoặc thiết bị lôgic lập trình được khác, thiết bị lôgic tranzito, thành phần phần cứng, hoặc sự kết hợp bất kỳ của chúng. Bộ phận xử lý 1002 có thể thực thi hoặc thực hiện

các khối lôgic, các môđun, và các mạch ví dụ khác nhau được mô tả dựa vào nội dung được bộc lộ trong sáng chế. Bộ phận xử lý 1002 có thể là sự kết hợp của các bộ xử lý thực hiện chức năng tính toán, ví dụ, sự kết hợp bao gồm một hoặc nhiều bộ vi xử lý, hoặc sự kết hợp của DSP và bộ vi xử lý. Bộ phận truyền thông 1003 có thể là giao diện truyền thông, bộ thu-phát, mạch thu-phát, hoặc tương tự, trong đó giao diện truyền thông là tên chung, và có thể bao gồm các giao diện trong cách thực hiện cụ thể. Bộ phận lưu trữ 1001 có thể là bộ nhớ.

Trong ứng dụng thứ nhất, thiết bị 1000 có thể là trạm gốc theo phương án bất kỳ trong số các phương án trên đây, hoặc có thể là chip trong trạm gốc. Ví dụ, khi thiết bị 1000 là trạm gốc, bộ phận xử lý có thể là, ví dụ, bộ xử lý. Bộ phận truyền thông có thể là, ví dụ, bộ thu-phát, và bộ thu-phát bao gồm mạch tần số rađiô. Tùy chọn là, bộ phận lưu trữ có thể là, ví dụ, bộ nhớ. Ví dụ, khi thiết bị 1000 là chip trong trạm gốc, bộ phận xử lý có thể là, ví dụ, bộ xử lý, và bộ phận truyền thông có thể là, ví dụ, giao diện vào/ra, chân cắm, hoặc mạch. Bộ phận xử lý có thể thực hiện lệnh thực hiện được bằng máy tính được lưu trữ trong bộ phận lưu trữ. Tùy chọn là, bộ phận lưu trữ là bộ phận lưu trữ bên trong chip, như thanh ghi hoặc bộ nhớ cache. Theo cách khác, bộ phận lưu trữ có thể là bộ phận lưu trữ mà ở trong thiết bị mạng truy cập và nằm bên ngoài chip, như bộ nhớ chỉ đọc (read-only memory, ROM) hoặc loại thiết bị lưu trữ tĩnh khác mà có thể lưu trữ thông tin tĩnh và lệnh, hoặc bộ nhớ truy cập ngẫu nhiên (random access memory, RAM).

Cụ thể, khi bộ phận truyền thông 1003 bao gồm bộ phận gửi và bộ phận nhận, bộ phận nhận được tạo cấu hình để nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, trong đó tin nhắn yêu cầu thiết lập lại được sử dụng để thiết lập lại kết nối RRC. Bộ phận gửi được tạo cấu hình để gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn thiết lập lại bao gồm bộ đếm móc nối lần nhảy tiếp theo NCC và thông tin dẫn xuất khóa, và thông tin dẫn xuất khóa được sử dụng để chỉ báo cho thiết bị đầu cuối dẫn xuất khóa tầng truy cập. Bộ phận nhận còn được tạo cấu hình để nhận tin nhắn hoàn thành thiết lập lại từ thiết bị đầu cuối, trong đó tin nhắn hoàn thành thiết lập lại được bảo vệ bằng cách sử dụng khóa được dẫn xuất dựa trên khóa tầng truy cập.

Theo một cách thực hiện khả thi, thông tin dẫn xuất khóa bao gồm chỉ báo thứ

nhất và bộ chứa tầng không truy cập NASC, NASC bao gồm chỉ báo thứ hai và chỉ báo NAS COUNT đường xuống, chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập, và chỉ báo thứ hai được sử dụng để chỉ báo cập nhật khóa gốc.

Theo một cách thực hiện khả thi, NASC còn bao gồm NAS MAC thứ nhất và bộ nhận dạng của thuật toán được chọn.

Theo một cách thực hiện khả thi, thông tin dẫn xuất khóa bao gồm chỉ báo thứ nhất, và chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập.

Theo một cách thực hiện khả thi, bộ phận xử lý được tạo cấu hình để: trước khi bộ phận gửi gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, xác định chỉ báo thứ nhất dựa trên thông số trung gian được đệm, trong đó thông số trung gian là bộ chỉ báo ngữ cảnh bảo mật mới NSCI thu nhận được bởi thiết bị từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao, và NSCI được sử dụng để chỉ báo cho thiết bị cập nhật khóa tầng truy cập.

Theo một cách thực hiện khả thi, bộ phận nhận còn được tạo cấu hình để: trước khi nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, thu nhận bộ chỉ báo ngữ cảnh bảo mật mới NSCI từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao, trong đó NSCI được sử dụng để chỉ báo cho trạm gốc cập nhật khóa tầng truy cập.

Bộ phận xử lý được tạo cấu hình để: xác định và lưu trữ chỉ báo thứ nhất dựa trên NSCI, và thu nhận chỉ báo thứ nhất đã lưu trữ trước khi bộ phận gửi gửi tin nhắn thiết lập lại đến thiết bị đầu cuối.

Theo một cách thực hiện khả thi, bộ phận nhận còn được tạo cấu hình để: trước khi nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, thu nhận NASC từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao; và bộ phận xử lý được tạo cấu hình để: lưu trữ NASC; và thu nhận NASC đã lưu trữ trước khi bộ phận gửi gửi tin nhắn thiết lập lại đến thiết bị đầu cuối.

Theo một cách thực hiện khả thi, bộ phận gửi còn được tạo cấu hình để: trước khi bộ phận nhận nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, gửi tin nhắn tái cấu hình RRC đến thiết bị đầu cuối, trong đó tin nhắn tái cấu hình RRC bao gồm thông số

cấu hình, NCC, và thông tin dẫn xuất khóa.

Trong ứng dụng thứ hai, thiết bị 1000 có thể là thiết bị đầu cuối theo phương án bất kỳ trong số các phương án trên đây, hoặc có thể là chip trong thiết bị đầu cuối. Ví dụ, khi thiết bị 1000 có thể là thiết bị đầu cuối, bộ phận xử lý có thể là, ví dụ, bộ xử lý. Bộ phận truyền thông có thể là, ví dụ, bộ thu-phát, và bộ thu-phát bao gồm mạch tần số rađiô. Tùy chọn là, bộ phận lưu trữ có thể là, ví dụ, bộ nhớ. Ví dụ, khi thiết bị 1000 có thể là chip trong thiết bị đầu cuối, bộ phận xử lý có thể là, ví dụ, bộ xử lý, và bộ phận truyền thông có thể là, ví dụ, giao diện vào/ra, chân cắm, hoặc mạch. Tùy chọn là, bộ phận lưu trữ là bộ phận lưu trữ bên trong chip, như thanh ghi hoặc bộ nhớ cache. Theo cách khác, bộ phận lưu trữ có thể là bộ phận lưu trữ mà ở bên trong thiết bị đầu cuối và nằm ngoài chip, như ROM, loại thiết bị lưu trữ tĩnh khác mà có thể lưu trữ thông tin tĩnh và lệnh, hoặc RAM.

Cụ thể, khi bộ phận truyền thông 1003 bao gồm bộ phận gửi và bộ phận nhận, bộ phận gửi được tạo cấu hình để gửi tin nhắn yêu cầu thiết lập lại đến trạm gốc, trong đó tin nhắn yêu cầu thiết lập lại được sử dụng để thiết lập lại kết nối RRC; bộ phận nhận được tạo cấu hình để nhận tin nhắn thiết lập lại từ trạm gốc, trong đó tin nhắn thiết lập lại bao gồm bộ đếm móc nối lần nhảy tiếp theo NCC và thông tin dẫn xuất khóa; bộ phận xử lý được tạo cấu hình để: dẫn xuất khóa tầng truy cập thứ nhất của thiết bị đầu cuối dựa trên thông tin dẫn xuất khóa; và dẫn xuất khóa tầng truy cập thứ hai của thiết bị đầu cuối dựa trên NCC và khóa tầng truy cập thứ nhất của thiết bị đầu cuối; và bộ phận gửi còn được tạo cấu hình để gửi tin nhắn hoàn thành thiết lập lại đến trạm gốc, trong đó tin nhắn hoàn thành thiết lập lại được bảo vệ bằng cách sử dụng khóa được dẫn xuất dựa trên khóa tầng truy cập thứ hai của thiết bị đầu cuối.

Theo một cách thực hiện khả thi, thông tin dẫn xuất khóa bao gồm chỉ báo thứ nhất và bộ chứa tầng không truy cập NASC, NASC bao gồm chỉ báo thứ hai và chỉ báo NAS COUNT đường xuống, chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập, và chỉ báo thứ hai được sử dụng để chỉ báo cập nhật khóa gốc; và bộ phận xử lý được tạo cấu hình cụ thể để: dẫn xuất khóa gốc thứ hai của thiết bị đầu cuối dựa trên chỉ báo thứ hai, chỉ báo NAS COUNT đường xuống, và khóa gốc thứ nhất của thiết bị đầu cuối; và dẫn xuất khóa tầng truy cập thứ nhất của thiết bị đầu cuối dựa trên chỉ

báo thứ nhất và khóa gốc thứ hai của thiết bị đầu cuối.

Theo một cách thực hiện khả thi, NASC còn bao gồm NAS MAC thứ nhất và bộ nhận dạng của thuật toán được chọn, và bộ phận xử lý còn được tạo cấu hình để: dẫn xuất khóa tầng không truy cập dựa trên khóa gốc thứ hai của thiết bị đầu cuối; và kiểm tra NAS MAC thứ nhất dựa trên thuật toán được chọn, chỉ báo NAS COUNT đường xuống, và khóa tầng không truy cập.

Theo một cách thực hiện khả thi, thông tin dẫn xuất khóa bao gồm chỉ báo thứ nhất, và chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập; và bộ phận xử lý được tạo cấu hình cụ thể để dẫn xuất khóa tầng truy cập thứ nhất của thiết bị đầu cuối dựa trên chỉ báo thứ nhất và khóa gốc thứ nhất của thiết bị đầu cuối.

Theo một cách thực hiện khả thi, chỉ báo NAS COUNT đường xuống bao gồm L1 bit thấp của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm tất cả các bit của NAS MAC thứ hai; và việc thiết bị đầu cuối kiểm tra NAS MAC thứ nhất dựa trên thuật toán được chọn, chỉ báo NAS COUNT đường xuống, và khóa tầng không truy cập bao gồm: Bộ phận xử lý được tạo cấu hình cụ thể để: thu nhận NAS COUNT đường xuống thứ hai dựa trên chỉ báo NAS COUNT đường xuống và NAS COUNT đường xuống thứ nhất của thiết bị đầu cuối; tạo NAS MAC dựa trên khóa tầng không truy cập, thuật toán được chọn, và NAS COUNT đường xuống thứ hai; và kiểm tra NAS MAC thứ nhất của NASC dựa trên NAS MAC tạo thành.

Theo một cách thực hiện khả thi, chỉ báo NAS COUNT đường xuống bao gồm L2 bit thấp của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm L3 bit thấp hoặc L4 bit cao của NAS MAC thứ hai; và bộ phận xử lý được tạo cấu hình cụ thể để: thu nhận NAS COUNT đường xuống thứ hai dựa trên chỉ báo NAS COUNT đường xuống và NAS COUNT đường xuống thứ nhất của thiết bị đầu cuối; tạo NAS MAC dựa trên khóa tầng không truy cập, thuật toán được chọn, và NAS COUNT đường xuống thứ hai; và kiểm tra NAS MAC thứ nhất của NASC dựa trên L3 bit thấp hoặc L4 bit cao của NAS MAC tạo thành.

Theo một cách thực hiện khả thi, chỉ báo NAS COUNT đường xuống bao gồm tất cả các bit của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm L5 bit thấp của NAS MAC thứ hai; và bộ phận xử lý được tạo cấu hình cụ thể để: tạo NAS MAC

dựa trên khóa tầng không truy cập, thuật toán được chọn, và chỉ báo NAS COUNT đường xuống của NASC; và kiểm tra NAS MAC thứ nhất của NASC dựa trên L5 bit thấp của NAS MAC tạo thành.

Theo một cách thực hiện khả thi, bộ phận nhận còn được tạo cấu hình để: trước bộ phận gửi gửi tin nhắn yêu cầu thiết lập lại đến trạm gốc, nhận tin nhắn tái cấu hình RRC từ trạm gốc, trong đó tin nhắn tái cấu hình RRC bao gồm thông số cấu hình, NCC, và thông tin dẫn xuất khóa; và bộ phận xử lý còn được tạo cấu hình để thực hiện cấu hình dựa trên thông số cấu hình, trong đó cấu hình không thành công.

Theo một cách thực hiện khả thi, bộ phận nhận còn được tạo cấu hình để: trước khi bộ phận gửi gửi tin nhắn yêu cầu thiết lập lại đến trạm gốc, nhận tin nhắn tái cấu hình RRC từ trạm gốc, trong đó tin nhắn tái cấu hình RRC bao gồm NCC và thông tin dẫn xuất khóa; bộ phận gửi còn được tạo cấu hình để gửi tin nhắn hoàn thành tái cấu hình RRC đến trạm gốc; và bộ phận xử lý còn được tạo cấu hình để xác định rằng bộ định thời hết hiệu lực.

Khi thiết bị được thể hiện trên Fig.10 là thiết bị đầu cuối hoặc trạm gốc, đối với các hiệu quả hữu ích cụ thể của việc truyền thông vô tuyến được thực hiện bởi thiết bị này, tham khảo các phần mô tả liên quan trong các phương án phương pháp trên đây. Các nội dung chi tiết không được mô tả lại ở đây.

Fig.11 là hình vẽ giản lược được đơn giản hóa của cấu trúc thiết kế khả thi của thiết bị đầu cuối theo một phương án của sáng chế. Thiết bị đầu cuối 1100 bao gồm bộ truyền 1101, bộ nhận 1102, và bộ xử lý 1103. Bộ xử lý 1103 cũng có thể là bộ điều khiển, và được biểu diễn là "bộ điều khiển/bộ xử lý 1103" trên Fig.11. Tùy chọn là, thiết bị đầu cuối 1100 có thể còn bao gồm bộ xử lý modem 1105, và bộ xử lý modem 1105 có thể bao gồm bộ mã hóa 1106, bộ điều biến 1107, bộ giải mã 1108, và bộ giải điều biến 1109.

Theo một ví dụ, bộ truyền 1101 điều chỉnh (ví dụ, qua chuyển đổi tương tự, lọc, khuếch đại, và chuyển đổi lên (up-conversion)) mẫu được kết xuất và tạo ra tín hiệu đường lên. Tín hiệu đường lên được truyền đến trạm gốc theo các phương án trên đây bằng cách sử dụng ăng ten. Trên đường xuống, ăng ten nhận tín hiệu đường xuống được truyền bởi trạm gốc theo các phương án trên đây. Bộ nhận 1102 điều chỉnh (ví dụ, qua lọc, khuếch đại, chuyển đổi xuống (down-conversion), và số hóa) tín hiệu được nhận từ

ăng ten và cung cấp mẫu được đưa vào. Trong bộ xử lý modem 1105, bộ mã hóa 1106 nhận dữ liệu dịch vụ và tin nhắn báo hiệu mà được gửi trên đường lên, và xử lý (ví dụ, thông qua định dạng, mã hóa, và đan xen) dữ liệu dịch vụ và tin nhắn báo hiệu. Bộ điều biến 1107 còn xử lý (ví dụ, qua ánh xạ ký hiệu và điều biến) dữ liệu dịch vụ được mã hóa và tin nhắn báo hiệu được mã hóa, và cung cấp mẫu được kết xuất. Bộ giải điều biến 1109 xử lý (ví dụ, qua giải điều biến) mẫu được đưa vào và cung cấp sự ước lượng ký hiệu. Bộ giải mã 1108 xử lý (ví dụ, qua giải đan xen và giải mã) sự ước lượng ký hiệu và cung cấp dữ liệu được giải mã và tin nhắn báo hiệu được giải mã mà cần được gửi đến thiết bị đầu cuối 1100. Bộ mã hóa 1106, bộ điều biến 1107, bộ giải điều biến 1109, và bộ giải mã 1108 có thể được thực thi bởi bộ xử lý modem kết hợp 1105. Các bộ phận này thực hiện việc xử lý dựa trên kỹ thuật truy cập radiô được sử dụng trong mạng truy cập radiô. Cần lưu ý rằng khi thiết bị đầu cuối 1100 không bao gồm bộ xử lý modem 1105, các chức năng trên đây của bộ xử lý modem 1105 cũng có thể được thực hiện bởi bộ xử lý 1103.

Bộ xử lý 1103 điều khiển và quản lý hoạt động của thiết bị đầu cuối 1100, và được tạo cấu hình để thực hiện quy trình xử lý được thực hiện bởi thiết bị đầu cuối 1100 theo các phương án trên đây của sáng chế. Ví dụ, bộ xử lý 1103 được tạo cấu hình để thực hiện quy trình xử lý của thiết bị đầu cuối trong phương pháp truyền thông vô tuyến theo phương án bất kỳ trong số các phương án của sáng chế và/hoặc quy trình khác của các giải pháp kỹ thuật được mô tả trong sáng chế.

Hơn nữa, thiết bị đầu cuối 1100 có thể còn bao gồm bộ nhớ 1104, và bộ nhớ 1104 được tạo cấu hình để lưu trữ mã chương trình và dữ liệu của thiết bị đầu cuối 1100.

Fig.12 là sơ đồ cấu trúc giản lược khả thi của trạm gốc theo một phương án của sáng chế. Trạm gốc 1200 bao gồm bộ xử lý 1202 và giao diện truyền thông 1204. Bộ xử lý 1202 cũng có thể là bộ điều khiển, và được biểu diễn là "bộ điều khiển/bộ xử lý 1202" trên Fig.12. Giao diện truyền thông 1204 được tạo cấu hình để hỗ trợ trạm gốc khi truyền thông với thiết bị đầu cuối. Hơn nữa, trạm gốc 1200 có thể còn bao gồm bộ truyền/bộ nhận 1201. Bộ truyền/bộ nhận 1201 được tạo cấu hình để hỗ trợ truyền thông radiô giữa trạm gốc và thiết bị đầu cuối theo các phương án trên đây. Bộ xử lý 1202 có thể thực hiện các chức năng khác nhau được sử dụng để truyền thông với thiết bị đầu cuối. Trên

đường lên, tín hiệu đường lên từ thiết bị đầu cuối được nhận bằng cách sử dụng ăng ten, được giải điều biến (ví dụ, tín hiệu tần số cao được giải điều biến thành tín hiệu dải gốc) bởi bộ nhận 1201, và còn được xử lý bởi bộ xử lý 1202 để khôi phục dữ liệu dịch vụ và thông tin báo hiệu mà được gửi bởi thiết bị đầu cuối. Trên đường xuống, dữ liệu dịch vụ và tin nhắn báo hiệu được xử lý bởi bộ xử lý 1202, và được điều biến (ví dụ, tín hiệu dải gốc được điều biến thành tín hiệu tần số cao) bởi bộ truyền 1201, để tạo tín hiệu đường xuống, và tín hiệu đường xuống được truyền đến thiết bị đầu cuối bằng cách sử dụng ăng ten. Cần lưu ý rằng chức năng giải điều biến hoặc điều biến trên đây cũng có thể được thực hiện bởi bộ xử lý 1202.

Ví dụ, bộ xử lý 1202 còn được tạo cấu hình để thực hiện quy trình xử lý liên quan đến trạm gốc trong phương pháp truyền thông vô tuyến theo phương án bất kỳ trong số các phương án của sáng chế và/hoặc quy trình khác của các giải pháp kỹ thuật được mô tả trong sáng chế.

Hơn nữa, trạm gốc 1200 có thể còn bao gồm bộ nhớ 1203, và bộ nhớ 1203 được tạo cấu hình để lưu trữ mã chương trình và dữ liệu của trạm gốc 1200.

Có thể hiểu rằng Fig.12 thể hiện chỉ thiết kế được đơn giản hóa của trạm gốc 1200. Trong ứng dụng thực tế, trạm gốc 1200 có thể bao gồm số lượng bộ truyền, bộ nhận, bộ xử lý, bộ điều khiển, bộ nhớ, bộ phận truyền thông, và tương tự bất kỳ, và tất cả các trạm gốc mà có thể thực hiện các phương án của sáng chế đều nằm trong phạm vi bảo hộ của các phương án của sáng chế.

Tất cả hoặc một số phương án trên đây có thể được thực hiện bằng cách sử dụng phần mềm, phần cứng, phần sụn, hoặc sự kết hợp bất kỳ của chúng. Khi phần mềm được sử dụng để thực thi các phương án, tất cả hoặc một số phương án có thể được thực thi dưới dạng sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính bao gồm một hoặc nhiều lệnh máy tính. Khi các lệnh máy tính được nạp và được thực hiện trên máy tính, các thủ tục hoặc các chức năng theo các phương án của sáng chế được tạo ra toàn bộ hoặc một phần. Máy tính có thể là máy tính đa năng, máy tính chuyên dụng, mạng máy tính, hoặc thiết bị lập trình được khác. Các lệnh máy tính có thể được lưu trữ trong phương tiện lưu trữ đọc được bằng máy tính hoặc có thể được truyền từ một phương tiện lưu trữ đọc được bằng máy tính đến phương tiện lưu trữ đọc được bằng

máy tính khác. Ví dụ, các lệnh máy tính có thể được truyền từ vị trí web, máy tính, máy chủ, hoặc trung tâm dữ liệu đến vị trí web, máy tính, máy chủ, hoặc trung tâm dữ liệu khác theo cách hữu truyến (ví dụ, cáp đồng trục, cáp sợi quang, hoặc đường thuê bao số (DSL)) hoặc vô tuyến (ví dụ, hồng ngoại, rađiô, hoặc vi sóng). Phương tiện lưu trữ đọc được bằng máy tính có thể là phương tiện sử dụng được bất kỳ có thể truy cập được bằng máy tính, hoặc thiết bị lưu trữ dữ liệu, như máy chủ hoặc trung tâm dữ liệu, tích hợp một hoặc nhiều phương tiện sử dụng được. Phương tiện sử dụng được có thể là phương tiện từ tính (ví dụ, đĩa mềm, đĩa cứng, hoặc băng từ), phương tiện quang học (ví dụ, DVD), phương tiện bán dẫn (ví dụ, ổ trạng thái rắn (Solid State Disk, SSD)), hoặc tương tự.

Các bộ phận và các mạch lôgic minh họa khác nhau được mô tả trong các phương án của sáng chế có thể thực thi hoặc vận hành các chức năng được mô tả bằng cách sử dụng bộ xử lý đa năng, bộ xử lý tín hiệu số, mạch tích hợp chuyên dụng (ASIC), mảng cổng lập trình được dạng trường (FPGA) hoặc thiết bị lôgic lập trình được khác, bộ lôgic tranzito hoặc cổng riêng biệt, thành phần phần cứng riêng biệt, hoặc thiết kế với sự kết hợp bất kỳ của chúng. Bộ xử lý đa năng có thể là bộ vi xử lý. Tùy chọn là, bộ xử lý đa năng, theo cách khác, có thể là bộ xử lý thông thường bất kỳ, bộ điều khiển, bộ vi điều khiển, hoặc máy trạng thái. Bộ xử lý cũng có thể được thực thi bởi sự kết hợp của các thiết bị điện toán, như bộ xử lý tín hiệu số và bộ vi xử lý, các bộ vi xử lý, một hoặc nhiều bộ vi xử lý kết hợp với lõi bộ xử lý tín hiệu số, hoặc cấu hình tương tự khác bất kỳ.

Các bước của các phương pháp hoặc các thuật toán được mô tả trong các phương án của sáng chế có thể được nhúng trực tiếp vào phần cứng, bộ phận phần mềm được thực hiện bởi bộ xử lý, hoặc sự kết hợp của chúng. Bộ phận phần mềm có thể được lưu trữ trong bộ nhớ RAM, bộ nhớ tác động nhanh (flash memory), bộ nhớ ROM, bộ nhớ EPROM, bộ nhớ EEPROM, thanh ghi, đĩa cứng, đĩa từ tháo được, CD-ROM, hoặc phương tiện lưu trữ ở dạng khác bất kỳ trong lĩnh vực kỹ thuật này. Ví dụ, phương tiện lưu trữ có thể được nối với bộ xử lý, sao cho bộ xử lý có thể đọc thông tin từ phương tiện lưu trữ và ghi thông tin vào phương tiện lưu trữ. Tùy chọn là, phương tiện lưu trữ còn có thể được tích hợp vào bộ xử lý. Bộ xử lý và phương tiện lưu trữ có thể được bố trí trong ASIC, và ASIC có thể được bố trí trong thiết bị đầu cuối. Tùy chọn là, bộ xử lý và phương tiện lưu trữ cũng có thể được bố trí trong các thành phần khác nhau của thiết

bị đầu cuối.

Các lệnh chương trình máy tính này theo cách khác có thể được nạp vào máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác, sao cho chuỗi thao tác và bước được thực hiện trên máy tính hoặc thiết bị lập trình được khác, để tạo ra việc xử lý được thực hiện bởi máy tính. Do đó, các lệnh được thực hiện trên máy tính hoặc thiết bị lập trình được khác sẽ tạo ra các bước để thực hiện chức năng cụ thể trong một hoặc nhiều thủ tục trên các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Mặc dù sáng chế được mô tả dựa vào các dấu hiệu cụ thể và các phương án của sáng chế, nhưng rõ ràng là các sự cải biến và kết hợp khác nhau có thể được thực hiện đối với chúng mà không nằm ngoài phạm vi của sáng chế. Tương ứng, bản mô tả và các hình vẽ kèm theo chỉ là các phần mô tả ví dụ của sáng chế được xác định bởi yêu cầu bảo hộ kèm theo, và được dự định bao trùm bất kỳ hoặc tất cả các sự cải biến, thay đổi, kết hợp, hoặc tương đương nằm trong phạm vi của sáng chế. Rõ ràng là người có hiểu biết trung bình trong lĩnh vực tương ứng có thể thực hiện các sự cải biến và thay đổi khác nhau đối với sáng chế mà không nằm ngoài phạm vi của sáng chế. Sáng chế được dự định bao trùm các sự cải biến và thay đổi này của sáng chế miễn là chúng nằm trong phạm vi của yêu cầu bảo hộ của sáng chế và các kỹ thuật tương đương của chúng.

YÊU CẦU BẢO HỘ

1. Phương pháp truyền thông vô tuyến, được sử dụng trong tình huống trong đó việc chuyển giao của thiết bị đầu cuối không thành công, phương pháp này bao gồm các bước:

gửi, bởi thiết bị đầu cuối, tin nhắn yêu cầu thiết lập lại đến trạm gốc, trong đó tin nhắn yêu cầu thiết lập lại được sử dụng để thiết lập lại kết nối điều khiển tài nguyên rađiô (radio resource control, RRC);

nhận, bởi thiết bị đầu cuối, tin nhắn thiết lập lại từ trạm gốc, trong đó tin nhắn thiết lập lại bao gồm bộ đếm móc nối lần nhảy tiếp theo (next hop chaining counter, NCC) và thông tin dẫn xuất khóa; thông tin dẫn xuất khóa bao gồm chỉ báo thứ nhất và bộ chứa tầng không truy cập (non-access stratum container, NASC), NASC bao gồm chỉ báo thứ hai và chỉ báo NAS COUNT đường xuống, chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập, và chỉ báo thứ hai được sử dụng để chỉ báo cập nhật khóa gốc;

dẫn xuất, bởi thiết bị đầu cuối, khóa gốc thứ hai của thiết bị đầu cuối dựa trên chỉ báo thứ hai, chỉ báo NAS COUNT đường xuống, và khóa gốc thứ nhất của thiết bị đầu cuối; và

dẫn xuất, bởi thiết bị đầu cuối, khóa tầng truy cập thứ nhất của thiết bị đầu cuối dựa trên chỉ báo thứ nhất và khóa gốc thứ hai của thiết bị đầu cuối.

dẫn xuất, bởi thiết bị đầu cuối, khóa tầng truy cập thứ hai của thiết bị đầu cuối dựa trên NCC và khóa tầng truy cập thứ nhất của thiết bị đầu cuối; và

gửi, bởi thiết bị đầu cuối, tin nhắn hoàn thành thiết lập lại đến trạm gốc, trong đó tin nhắn hoàn thành thiết lập lại được bảo vệ bằng cách sử dụng khóa được dẫn xuất dựa trên khóa tầng truy cập thứ hai của thiết bị đầu cuối.

2. Phương pháp theo điểm 1, trong đó NASC còn bao gồm NAS MAC thứ nhất và bộ nhận dạng của thuật toán được chọn, và phương pháp này còn bao gồm bước:

dẫn xuất, bởi thiết bị đầu cuối, khóa tầng không truy cập dựa trên khóa gốc thứ hai của thiết bị đầu cuối; và

kiểm tra, bởi thiết bị đầu cuối, NAS MAC thứ nhất dựa trên thuật toán được chọn, chỉ báo NAS COUNT đường xuống, và khóa tầng không truy cập.

3. Phương pháp theo điểm 2, trong đó chỉ báo NAS COUNT đường xuống bao gồm L1 bit thấp của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm tất cả các bit của NAS MAC thứ hai, trong đó L1 là số nguyên dương; và

bước kiểm tra, bởi thiết bị đầu cuối, NAS MAC thứ nhất dựa trên thuật toán được chọn, chỉ báo NAS COUNT đường xuống, và khóa tầng không truy cập bao gồm:

thu nhận, bởi thiết bị đầu cuối, NAS COUNT đường xuống thứ hai dựa trên chỉ báo NAS COUNT đường xuống và NAS COUNT đường xuống thứ nhất của thiết bị đầu cuối;

tạo, bởi thiết bị đầu cuối, NAS MAC dựa trên khóa tầng không truy cập, thuật toán được chọn, và NAS COUNT đường xuống thứ hai; và

kiểm tra, bởi thiết bị đầu cuối, NAS MAC thứ nhất của NASC dựa trên NAS MAC tạo thành.

4. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó trước bước gửi, bởi thiết bị đầu cuối, tin nhắn yêu cầu thiết lập lại đến trạm gốc, phương pháp này còn bao gồm bước:

nhận, bởi thiết bị đầu cuối, tin nhắn tái cấu hình điều khiển tài nguyên rađiô (radio resource control, RRC) từ trạm gốc, trong đó tin nhắn tái cấu hình RRC bao gồm thông số cấu hình, NCC, và thông tin dẫn xuất khóa; và

thực hiện, bởi thiết bị đầu cuối, cấu hình dựa trên thông số cấu hình, trong đó cấu hình không thành công.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó trước bước gửi, bởi thiết bị đầu cuối, tin nhắn yêu cầu thiết lập lại đến trạm gốc, phương pháp này còn bao gồm bước:

nhận, bởi thiết bị đầu cuối, tin nhắn tái cấu hình RRC từ trạm gốc, trong đó tin nhắn tái cấu hình RRC bao gồm NCC và thông tin dẫn xuất khóa;

khởi động, bởi thiết bị đầu cuối, bộ định thời;

gửi, bởi thiết bị đầu cuối, tin nhắn hoàn thành tái cấu hình RRC đến trạm gốc; và

xác định, bởi thiết bị đầu cuối, rằng bộ định thời hết hiệu lực.

6. Phương pháp truyền thông vô tuyến, được sử dụng trong tình huống trong đó việc chuyển giao của thiết bị đầu cuối không thành công, phương pháp này bao gồm các bước:

nhận, bởi trạm gốc, tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, trong đó tin nhắn yêu cầu thiết lập lại được sử dụng để thiết lập lại kết nối RRC;

gửi, bởi trạm gốc, tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn thiết lập lại bao gồm bộ đếm móc nối lần nhảy tiếp theo (next hop chaining counter, NCC), và thông tin dẫn xuất khóa, và thông tin dẫn xuất khóa bao gồm chỉ báo thứ nhất và bộ chứa tầng không truy cập (non-access stratum container, NASC), NASC bao gồm chỉ báo thứ hai và chỉ báo NAS COUNT đường xuống, chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập, và chỉ báo thứ hai được sử dụng để chỉ báo cập nhật khóa gốc; và

nhận, bởi trạm gốc, tin nhắn hoàn thành thiết lập lại từ thiết bị đầu cuối, trong đó tin nhắn hoàn thành thiết lập lại được bảo vệ bằng cách sử dụng khóa được dẫn xuất dựa trên khóa tầng truy cập.

7. Phương pháp theo điểm 6, trong đó trước bước gửi, bởi trạm gốc, tin nhắn thiết lập lại đến thiết bị đầu cuối, phương pháp này còn bao gồm bước:

xác định, bởi trạm gốc, chỉ báo thứ nhất dựa trên thông số trung gian được đệm, trong đó thông số trung gian là bộ chỉ báo ngữ cảnh bảo mật mới (new security context indicator, NSCI) được thu nhận bởi trạm gốc từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao, và NSCI được sử dụng để chỉ báo cho trạm gốc cập nhật khóa tầng truy cập.

8. Phương pháp theo điểm 6, trong đó trước bước nhận, bởi trạm gốc, tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, phương pháp này còn bao gồm bước:

thu nhận, bởi trạm gốc, bộ chỉ báo ngữ cảnh bảo mật mới NSCI từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao, trong đó NSCI được sử dụng để chỉ báo cho trạm gốc cập nhật khóa tầng truy cập; và

xác định và lưu trữ, bởi trạm gốc, chỉ báo thứ nhất dựa trên NSCI; và

trước bước gửi, bởi trạm gốc, tin nhắn thiết lập lại đến thiết bị đầu cuối, phương pháp này còn bao gồm bước:

thu nhận, bởi trạm gốc, chỉ báo thứ nhất đã lưu trữ.

9. Phương pháp theo điểm 6, trong đó trước bước nhận, bởi trạm gốc, tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, phương pháp này còn bao gồm bước:

thu nhận và lưu trữ, bởi trạm gốc, NASC từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao; và

trước bước gửi, bởi trạm gốc, tin nhắn thiết lập lại đến thiết bị đầu cuối, phương pháp này còn bao gồm bước:

thu nhận, bởi trạm gốc, NASC đã lưu trữ.

10. Phương pháp theo điểm 6 hoặc điểm 9, trong đó trước bước nhận, bởi trạm gốc, tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, phương pháp này còn bao gồm bước:

gửi, bởi trạm gốc, tin nhắn tái cấu hình RRC đến thiết bị đầu cuối, trong đó tin nhắn tái cấu hình RRC bao gồm thông số cấu hình, NCC, và thông tin dẫn xuất khóa.

11. Thiết bị truyền thông, được sử dụng trong thiết bị đầu cuối và được sử dụng trong tình huống trong đó việc chuyển giao của thiết bị đầu cuối không thành công, thiết bị này bao gồm:

bộ phận gửi, được tạo cấu hình để gửi tin nhắn yêu cầu thiết lập lại đến trạm gốc, trong đó tin nhắn yêu cầu thiết lập lại được sử dụng để thiết lập lại kết nối RRC;

bộ phận nhận, được tạo cấu hình để nhận tin nhắn thiết lập lại từ trạm gốc, trong đó tin nhắn thiết lập lại bao gồm bộ đếm móc nối lần nhảy tiếp theo (next hop chaining counter, NCC) và thông tin dẫn xuất khóa; thông tin dẫn xuất khóa bao gồm chỉ báo thứ nhất và bộ chứa tầng không truy cập (non-access stratum container, NASC), NASC bao gồm chỉ báo thứ hai và chỉ báo NAS COUNT đường xuống, chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập, và chỉ báo thứ hai được sử dụng để chỉ báo cập nhật khóa gốc; và

bộ phận xử lý, được tạo cấu hình để:

dẫn xuất khóa gốc thứ hai của thiết bị đầu cuối dựa trên chỉ báo thứ hai, chỉ báo NAS COUNT đường xuống, và khóa gốc thứ nhất của thiết bị đầu cuối;

dẫn xuất khóa tầng truy cập thứ nhất của thiết bị đầu cuối dựa trên chỉ báo thứ nhất và khóa gốc thứ hai của thiết bị đầu cuối; và dẫn xuất khóa tầng truy cập thứ hai của thiết bị đầu cuối dựa trên NCC và khóa tầng truy cập thứ nhất của thiết bị đầu cuối, trong đó

bộ phận gửi còn được tạo cấu hình để gửi tin nhắn hoàn thành thiết lập lại đến trạm gốc, trong đó tin nhắn hoàn thành thiết lập lại được bảo vệ bằng cách sử dụng khóa được dẫn xuất dựa trên khóa tầng truy cập thứ hai của thiết bị đầu cuối.

12. Thiết bị theo điểm 11, trong đó NASC còn bao gồm NAS MAC thứ nhất và bộ nhận dạng của thuật toán được chọn, và bộ phận xử lý còn được tạo cấu hình để:

dẫn xuất khóa tầng không truy cập dựa trên khóa gốc thứ hai của thiết bị đầu cuối; và

kiểm tra NAS MAC thứ nhất dựa trên thuật toán được chọn, chỉ báo NAS COUNT đường xuống, và khóa tầng không truy cập.

13. Thiết bị theo điểm 12, trong đó chỉ báo NAS COUNT đường xuống bao gồm L1 bit thấp của NAS COUNT đường xuống, và NAS MAC thứ nhất bao gồm tất cả các bit của NAS MAC thứ hai, trong đó L1 là số nguyên dương; và

bộ phận xử lý được tạo cấu hình cụ thể để:

thu nhận NAS COUNT đường xuống thứ hai dựa trên chỉ báo NAS COUNT đường xuống và NAS COUNT đường xuống thứ nhất của thiết bị đầu cuối;

tạo NAS MAC dựa trên khóa tầng không truy cập, thuật toán được chọn, và NAS COUNT đường xuống thứ hai; và

kiểm tra NAS MAC thứ nhất của NASC dựa trên NAS MAC tạo thành.

14. Thiết bị theo điểm bất kỳ trong số các điểm từ 11 đến 13, trong đó bộ phận nhận còn được tạo cấu hình để: trước khi bộ phận gửi gửi tin nhắn yêu cầu thiết lập lại đến trạm gốc, nhận tin nhắn tái cấu hình RRC từ trạm gốc, trong đó tin nhắn tái cấu hình RRC bao gồm thông số cấu hình, NCC, và thông tin dẫn xuất khóa; và

bộ phận xử lý còn được tạo cấu hình để thực hiện cấu hình dựa trên thông số cấu hình, trong đó cấu hình không thành công.

15. Thiết bị theo điểm bất kỳ trong số các điểm từ 11 đến 13, trong đó bộ phận nhận còn được tạo cấu hình để: trước khi bộ phận gửi gửi tin nhắn yêu cầu thiết lập lại đến trạm gốc, nhận tin nhắn tái cấu hình RRC từ trạm gốc, trong đó tin nhắn tái cấu hình RRC bao gồm NCC và thông tin dẫn xuất khóa;

bộ phận gửi còn được tạo cấu hình để gửi tin nhắn hoàn thành tái cấu hình RRC đến trạm gốc; và

bộ phận xử lý còn được tạo cấu hình để: khởi động bộ định thời, và xác định rằng bộ định thời hết hiệu lực.

16. Thiết bị đầu cuối, bao gồm thiết bị theo điểm bất kỳ trong số các điểm từ 11 đến 15.

17. Thiết bị truyền thông, được sử dụng trong tình huống trong đó việc chuyển giao của thiết bị đầu cuối không thành công, thiết bị này bao gồm:

bộ phận nhận, được tạo cấu hình để nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, trong đó tin nhắn yêu cầu thiết lập lại được sử dụng để thiết lập lại kết nối RRC; và

bộ phận gửi, được tạo cấu hình để gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, trong đó tin nhắn thiết lập lại bao gồm bộ đếm móc nối lần nhảy tiếp theo (NCC) và thông tin dẫn xuất khóa, và thông tin dẫn xuất khóa bao gồm chỉ báo thứ nhất và bộ chứa tầng không truy cập (NASC), NASC bao gồm chỉ báo thứ hai và chỉ báo NAS COUNT đường xuống, chỉ báo thứ nhất được sử dụng để chỉ báo cập nhật khóa tầng truy cập, và chỉ báo thứ hai được sử dụng để chỉ báo cập nhật khóa gốc, trong đó

bộ phận nhận còn được tạo cấu hình để nhận tin nhắn hoàn thành thiết lập lại từ thiết bị đầu cuối, trong đó tin nhắn hoàn thành thiết lập lại được bảo vệ bằng cách sử dụng khóa được dẫn xuất dựa trên khóa tầng truy cập.

18. Thiết bị theo điểm 17, trong đó thiết bị này còn bao gồm bộ phận xử lý, được tạo cấu hình để: trước khi bộ phận gửi gửi tin nhắn thiết lập lại đến thiết bị đầu cuối, xác định chỉ báo thứ nhất dựa trên thông số trung gian được đệm, trong đó thông số trung gian là bộ chỉ báo ngữ cảnh bảo mật mới NSCI thu nhận được bởi thiết bị từ thực thể

chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao, và NSCI được sử dụng để chỉ báo cho thiết bị cập nhật khóa tầng truy cập.

19. Thiết bị theo điểm 17, trong đó bộ phận nhận còn được tạo cấu hình để: trước khi nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, thu nhận bộ chỉ báo ngữ cảnh bảo mật mới (NSCI) từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao, trong đó NSCI được sử dụng để chỉ báo cho trạm gốc cập nhật khóa tầng truy cập; và

thiết bị còn bao gồm bộ phận xử lý, được tạo cấu hình để: xác định và lưu trữ chỉ báo thứ nhất dựa trên NSCI; và thu nhận chỉ báo thứ nhất đã lưu trữ trước khi bộ phận gửi gửi tin nhắn thiết lập lại đến thiết bị đầu cuối.

20. Thiết bị theo điểm 17, trong đó bộ phận nhận còn được tạo cấu hình để: trước khi nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, thu nhận NASC từ thực thể chức năng quản lý truy cập và di động trong quy trình chuẩn bị chuyển giao; và

thiết bị này còn bao gồm bộ phận xử lý, được tạo cấu hình để lưu trữ NASC; và thu nhận NASC đã lưu trữ trước khi bộ phận gửi gửi tin nhắn thiết lập lại đến thiết bị đầu cuối.

21. Thiết bị theo điểm bất kỳ trong số các điểm từ 17 đến 20, trong đó bộ phận gửi còn được tạo cấu hình để: trước khi bộ phận nhận nhận tin nhắn yêu cầu thiết lập lại từ thiết bị đầu cuối, gửi tin nhắn tái cấu hình RRC đến thiết bị đầu cuối, trong đó tin nhắn tái cấu hình RRC bao gồm thông số cấu hình, NCC, và thông tin dẫn xuất khóa.

22. Thiết bị truyền thông, thiết bị này bao gồm:

bộ xử lý; và

bộ nhớ được ghép nối với bộ xử lý và có các lệnh chương trình được lưu trữ trên đó mà, khi được thực hiện bởi bộ xử lý, làm cho thiết bị này thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5.

23. Thiết bị truyền thông, thiết bị này bao gồm:

bộ xử lý; và

bộ nhớ được ghép nối với bộ xử lý và có các lệnh chương trình được lưu trữ trên

đó mà, khi được thực hiện bởi bộ xử lý, làm cho thiết bị này thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 6 đến 10.

24. Phương tiện lưu trữ đọc được bằng máy tính, bao gồm các lệnh, trong đó khi các lệnh này được chạy trên máy tính, máy tính được phép thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5.

25. Phương tiện lưu trữ đọc được bằng máy tính, bao gồm các lệnh, trong đó khi các lệnh này được chạy trên máy tính, máy tính được phép thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 6 đến 10.

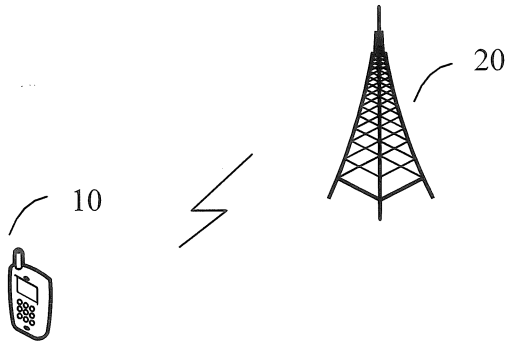
20
10

FIG. 1

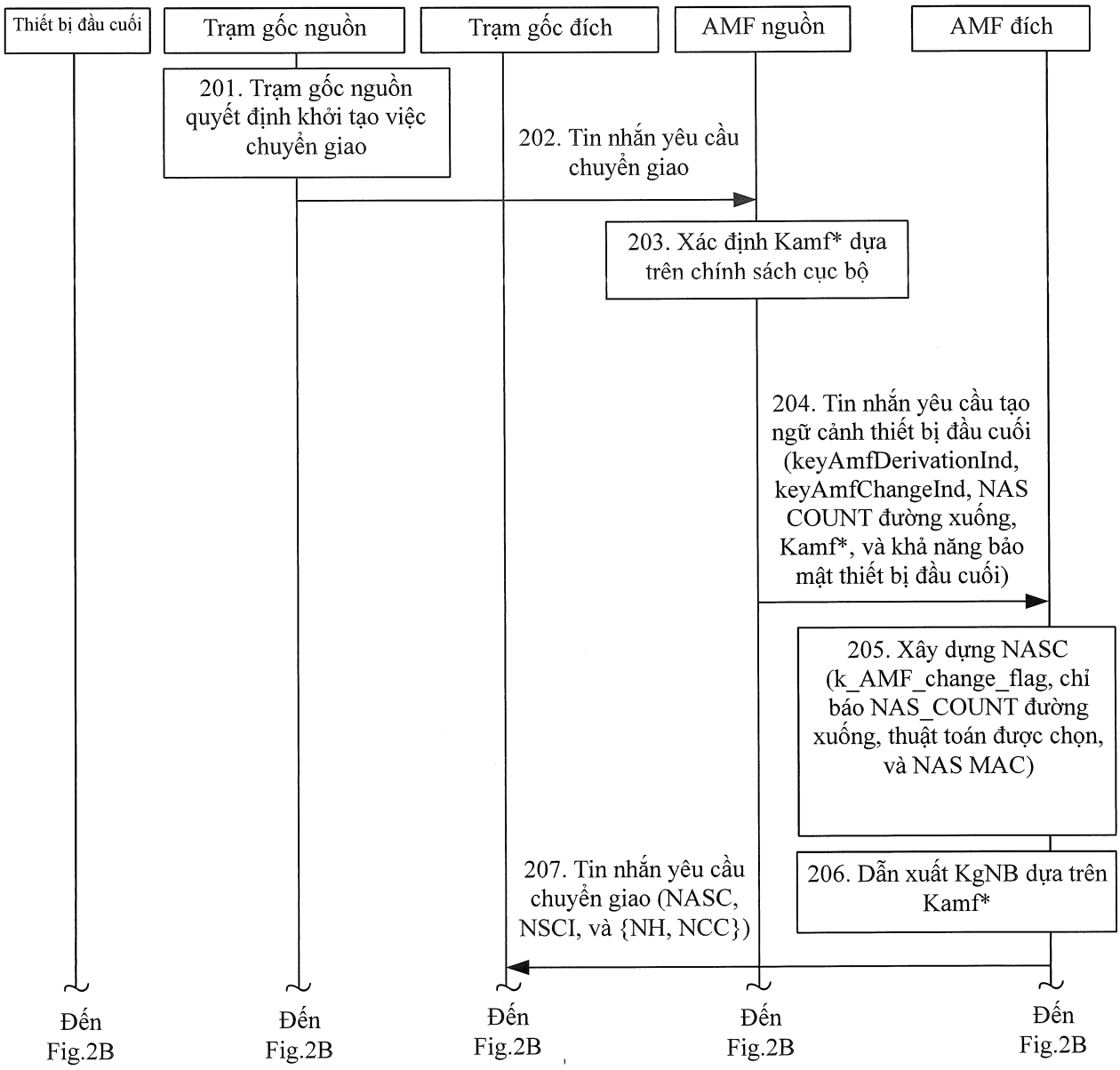
Thiết bị đầu cuối
Trạm gốc nguồn
Trạm gốc đích
AMF nguồn
AMF đích
201. Trạm gốc nguồn quyết định khởi tạo việc chuyển giao
202. Tin nhắn yêu cầu chuyển giao
203. Xác định Kamf* dựa trên chính sách cục bộ
204. Tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối (keyAmfDerivationInd, keyAmfChangeInd, NAS COUNT đường xuống, Kamf*, và khả năng bảo mật thiết bị đầu cuối)
205. Xây dựng NASC (k_AMF_change_flag, chỉ báo NAS_COUNT đường xuống, thuật toán được chọn, và NAS MAC)
206. Dẫn xuất KgNB dựa trên Kamf*
207. Tin nhắn yêu cầu chuyển giao (NASC, NSCI, và {NH, NCC})
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B

FIG. 2A

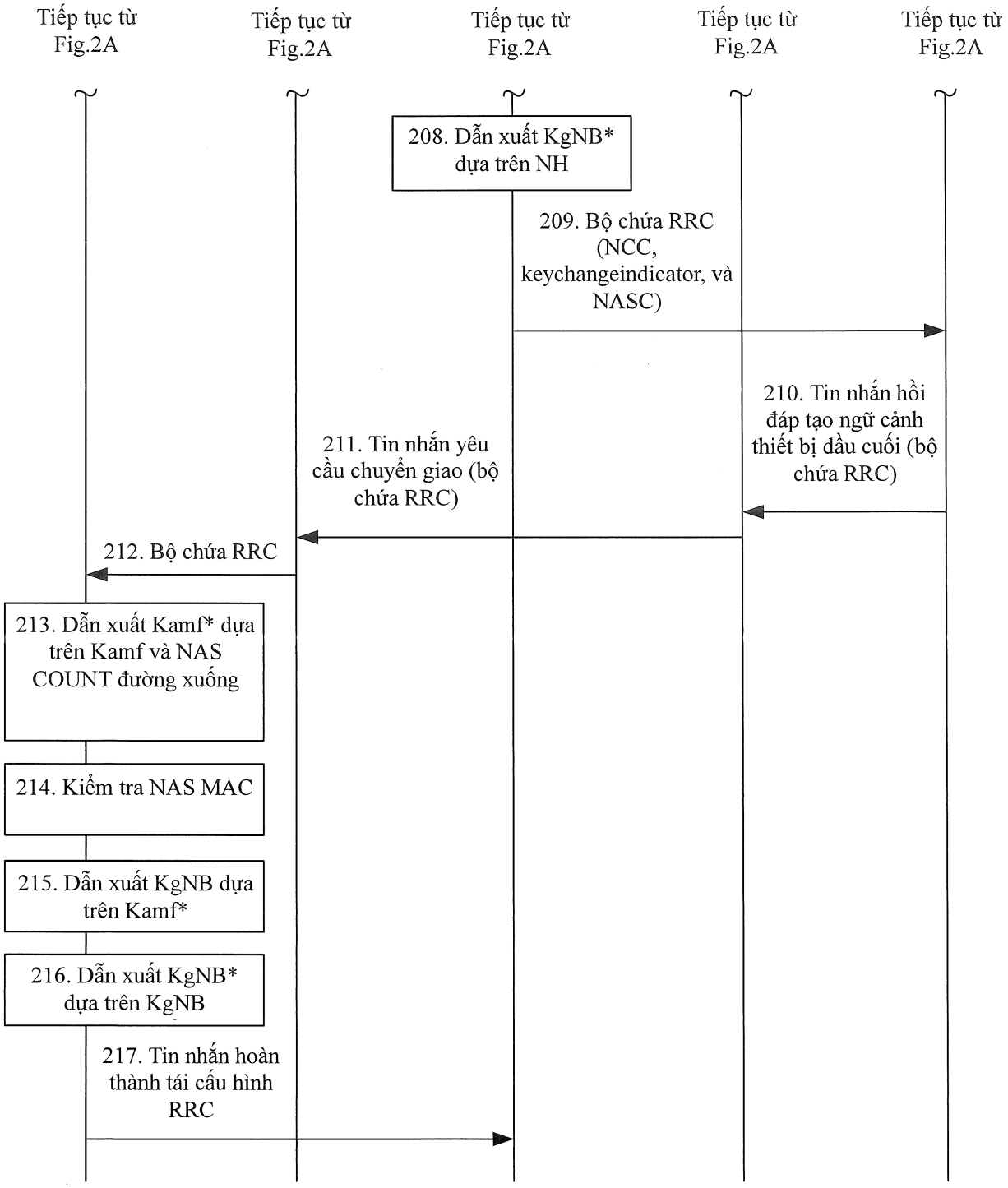
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
208. Dẫn xuất KgNB* dựa trên NH
209. Bộ chứa RRC (NCC, keychangeindicator, và NASC)
210. Tin nhắn hồi đáp tạo ngữ cảnh thiết bị đầu cuối (bộ chứa RRC)
211. Tin nhắn yêu cầu chuyển giao (bộ chứa RRC)
212. Bộ chứa RRC
213. Dẫn xuất Kamf* dựa trên Kamf và NAS COUNT đường xuống
214. Kiểm tra NAS MAC
215. Dẫn xuất KgNB dựa trên Kamf*
216. Dẫn xuất KgNB* dựa trên KgNB
217. Tin nhắn hoàn thành tái cấu hình RRC

FIG. 2B

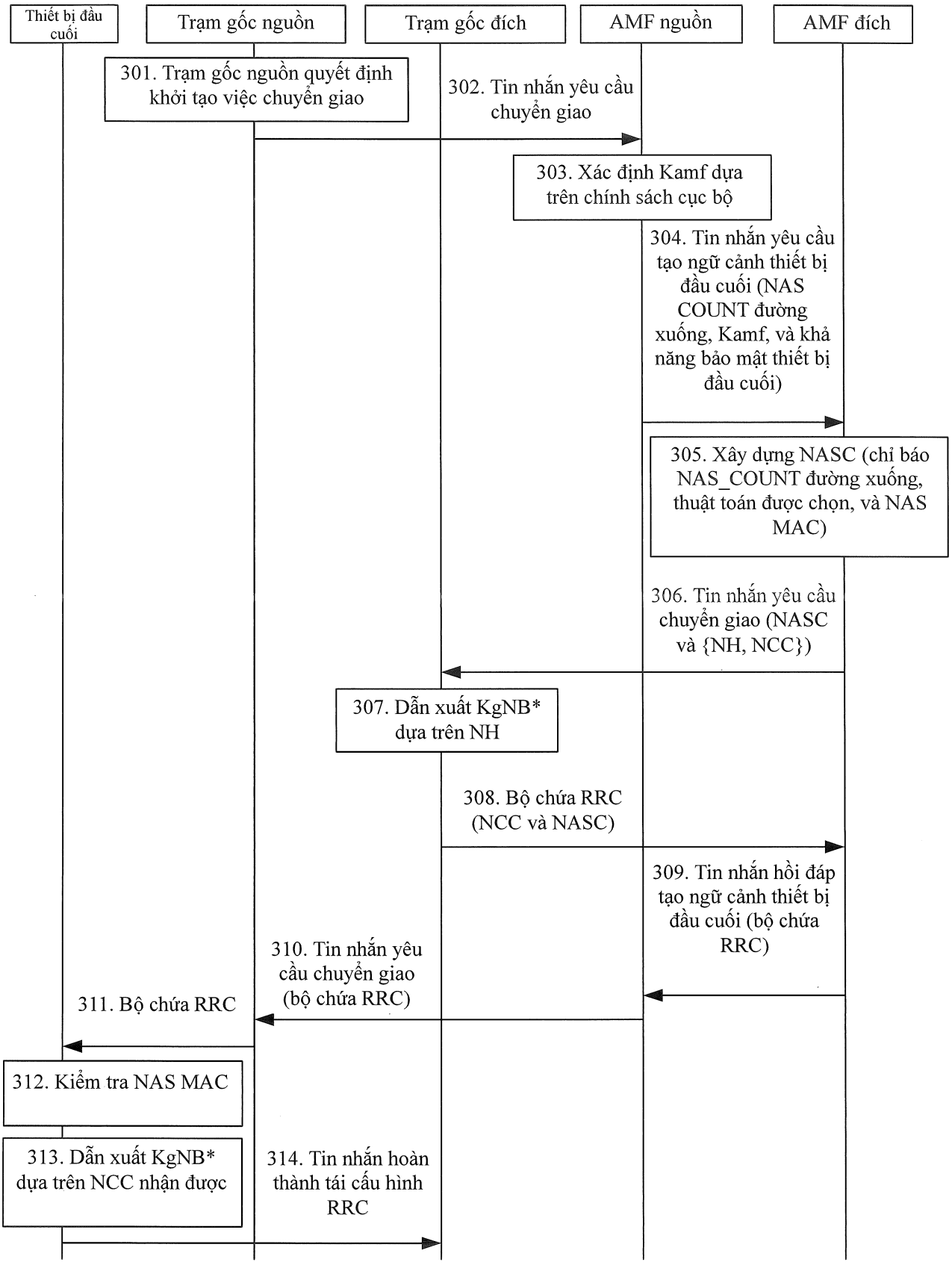
Thiết bị đầu cuối
Trạm gốc nguồn
Trạm gốc đích
AMF nguồn
AMF đích
301. Trạm gốc nguồn quyết định khởi tạo việc chuyển giao
302. Tin nhắn yêu cầu chuyển giao
303. Xác định Kamf dựa trên chính sách cục bộ
304. Tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối (NAS COUNT đường xuống, Kamf, và khả năng bảo mật thiết bị đầu cuối)
305. Xây dựng NASC (chỉ báo NAS_COUNT đường xuống, thuật toán được chọn, và NAS MAC)
306. Tin nhắn yêu cầu chuyển giao (NASC và {NH, NCC})
307. Dẫn xuất KgNB* dựa trên NH
308. Bộ chứa RRC (NCC và NASC)
309. Tin nhắn hồi đáp tạo ngữ cảnh thiết bị đầu cuối (bộ chứa RRC)
310. Tin nhắn yêu cầu chuyển giao (bộ chứa RRC)
311. Bộ chứa RRC
312. Kiểm tra NAS MAC
313. Dẫn xuất KgNB* dựa trên NCC nhận được
314. Tin nhắn hoàn thành tái cấu hình RRC

FIG. 3

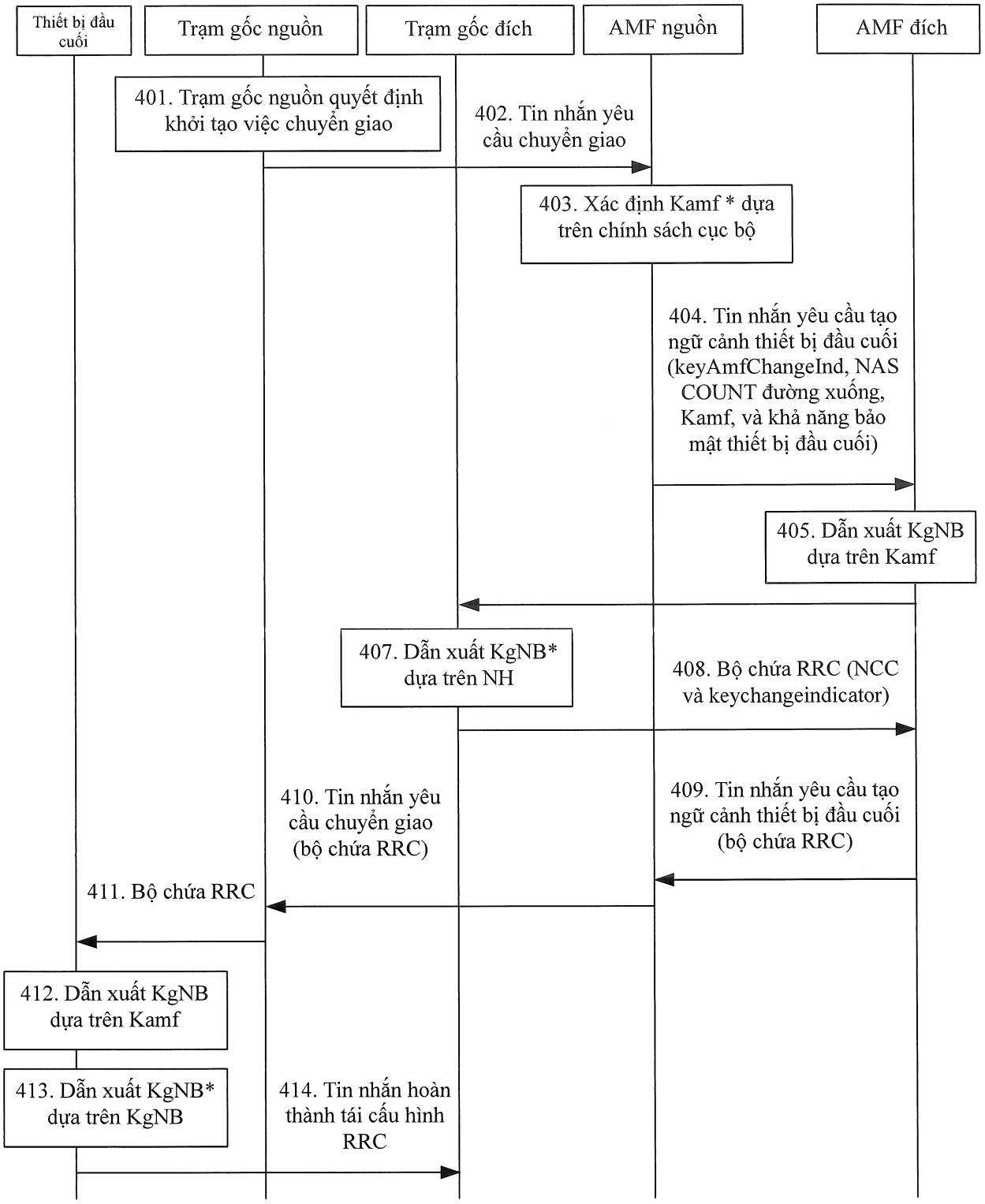
Thiết bị đầu cuối
Trạm gốc nguồn
Trạm gốc đích
AMF nguồn
AMF đích
401. Trạm gốc nguồn quyết định khởi tạo việc chuyển giao
402. Tin nhắn yêu cầu chuyển giao
403. Xác định Kamf * dựa trên chính sách cục bộ
404. Tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối (keyAmfChangeInd, NAS COUNT đường xuống, Kamf, và khả năng bảo mật thiết bị đầu cuối)
405. Dẫn xuất KgNB dựa trên Kamf
407. Dẫn xuất KgNB* dựa trên NH
408. Bộ chứa RRC (NCC và keychangeindicator)
410. Tin nhắn yêu cầu chuyển giao (bộ chứa RRC)
409. Tin nhắn yêu cầu tạo ngữ cảnh thiết bị đầu cuối (bộ chứa RRC)
411. Bộ chứa RRC
412. Dẫn xuất KgNB dựa trên Kamf
413. Dẫn xuất KgNB* dựa trên KgNB
414. Tin nhắn hoàn thành tái cấu hình RRC

FIG. 4

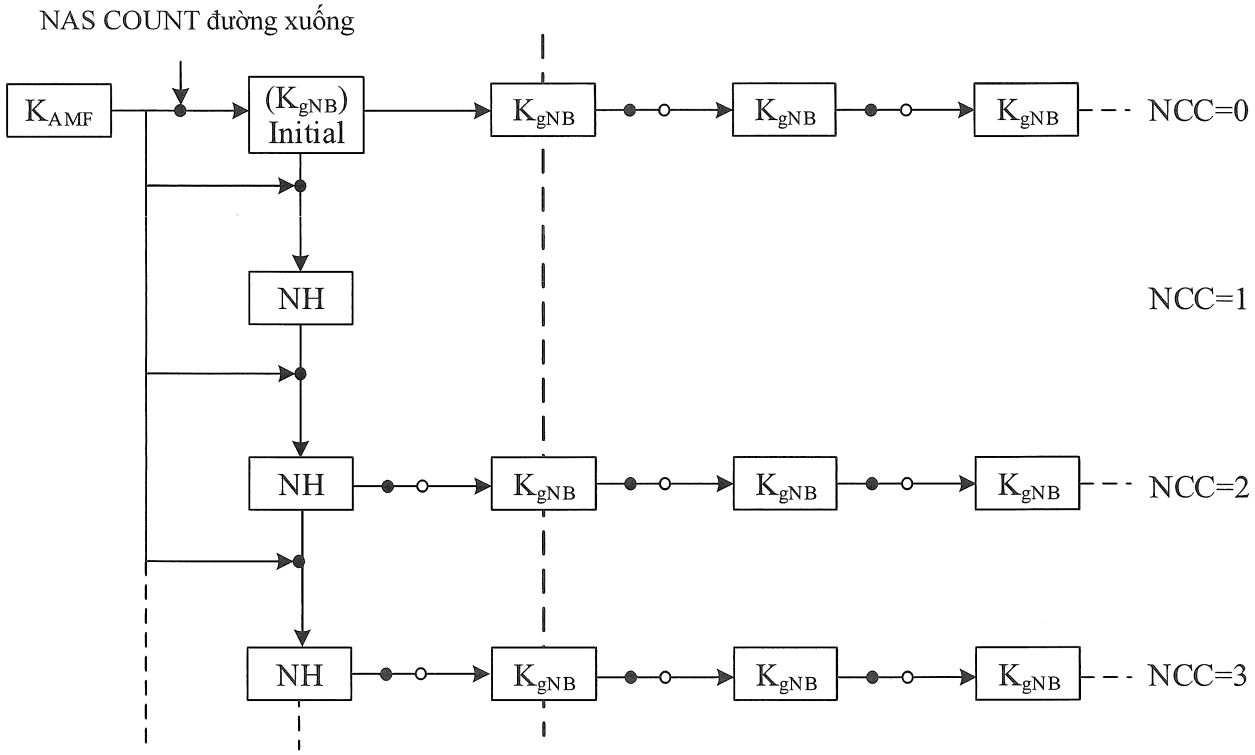
NAS COUNT đường xuống
K_{AMF}
(K_{gNB}) Initial
K_{gNB}
K_{gNB}
K_{gNB}
NCC=0
NH
NCC=1
NH
K_{gNB}
K_{gNB}
K_{gNB}
NCC=2
NH
K_{gNB}
K_{gNB}
K_{gNB}
NCC=3

FIG. 5

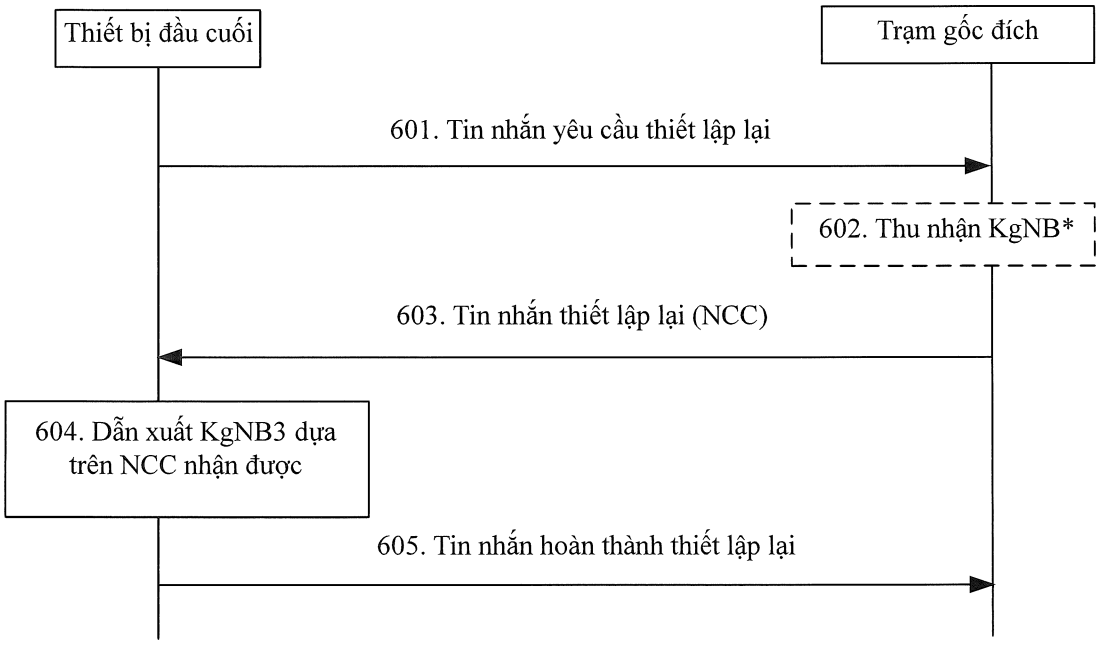
Thiết bị đầu cuối
Trạm gốc đích
601. Tin nhắn yêu cầu thiết lập lại
602. Thu nhận KgNB*
603. Tin nhắn thiết lập lại (NCC)
604. Dẫn xuất KgNB3 dựa trên NCC nhận được
605. Tin nhắn hoàn thành thiết lập lại

FIG. 6

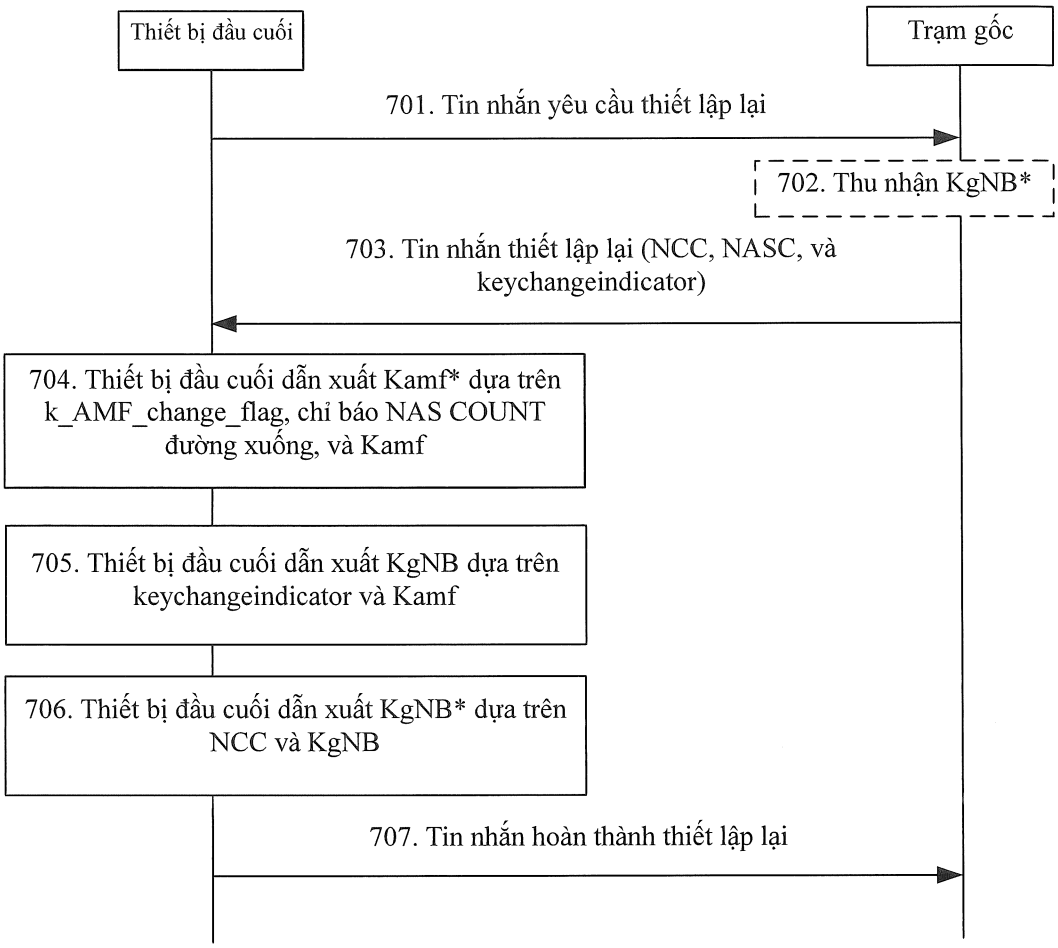
Thiết bị đầu cuối
Trạm gốc
701. Tin nhắn yêu cầu thiết lập lại
702. Thu nhận KgNB*
703. Tin nhắn thiết lập lại (NCC, NASC, và keychangeindicator)
704. Thiết bị đầu cuối dẫn xuất Kamf* dựa trên k_AMF_change_flag, chỉ báo NAS COUNT đường xuống, và Kamf
705. Thiết bị đầu cuối dẫn xuất KgNB dựa trên keychangeindicator và Kamf
706. Thiết bị đầu cuối dẫn xuất KgNB* dựa trên NCC và KgNB
707. Tin nhắn hoàn thành thiết lập lại

FIG. 7

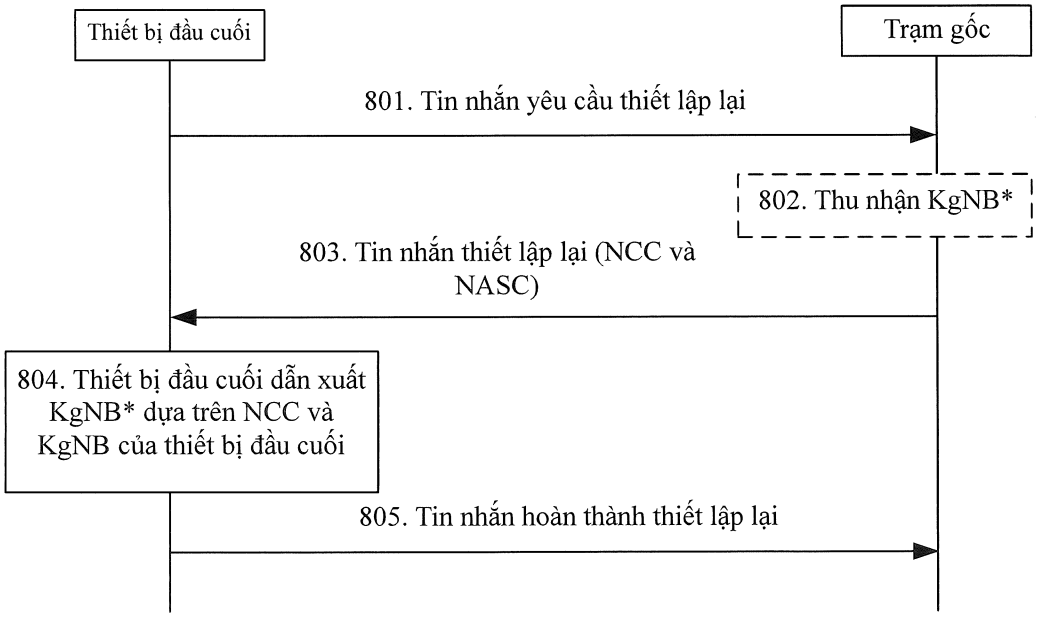
Thiết bị đầu cuối
Trạm gốc
801. Tin nhắn yêu cầu thiết lập lại
802. Thu nhận KgNB*
803. Tin nhắn thiết lập lại (NCC và NASC)
804. Thiết bị đầu cuối dẫn xuất KgNB* dựa trên NCC và KgNB của thiết bị đầu cuối
805. Tin nhắn hoàn thành thiết lập lại

FIG. 8

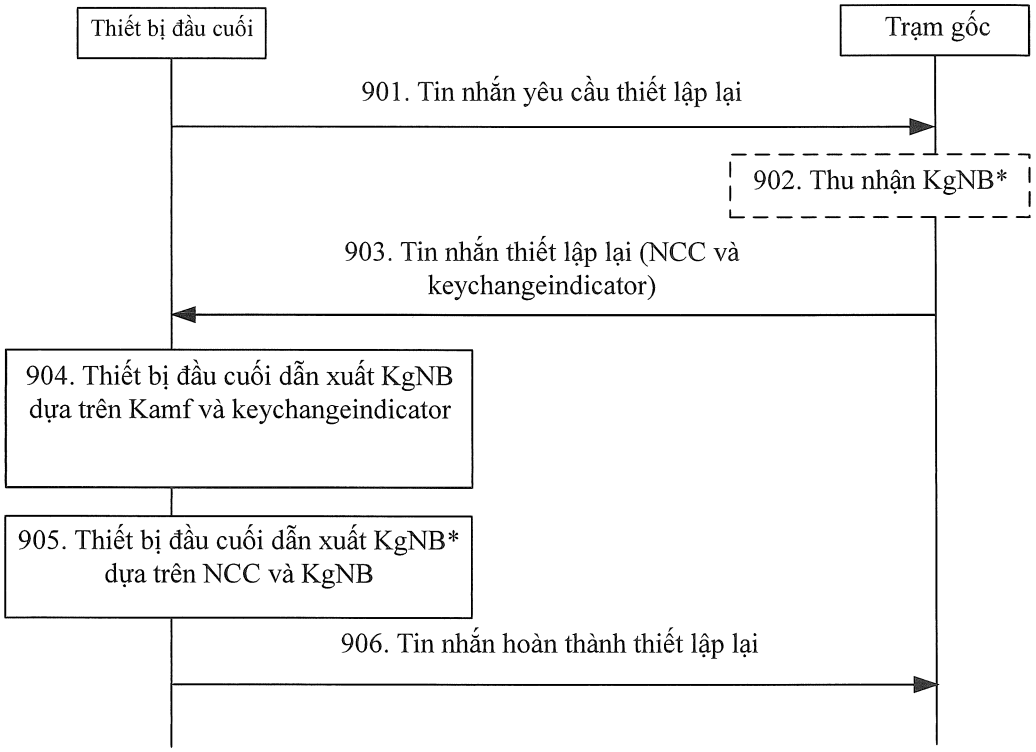
Thiết bị đầu cuối
Trạm gốc
901. Tin nhắn yêu cầu thiết lập lại
902. Thu nhận KgNB*
903. Tin nhắn thiết lập lại (NCC và keychangeindicator)
904. Thiết bị đầu cuối dẫn xuất KgNB dựa trên Kamf và keychangeindicator
905. Thiết bị đầu cuối dẫn xuất KgNB* dựa trên NCC và KgNB
906. Tin nhắn hoàn thành thiết lập lại

FIG. 9

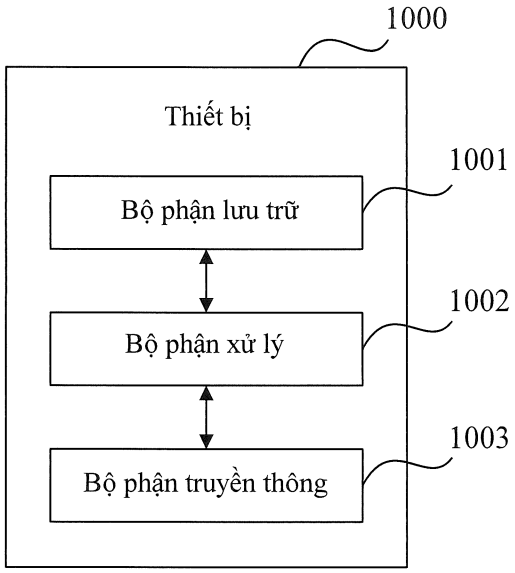
1000
Thiết bị
1001
Bộ phận lưu trữ
1002
Bộ phận xử lý
1003
Bộ phận truyền thông

FIG. 10

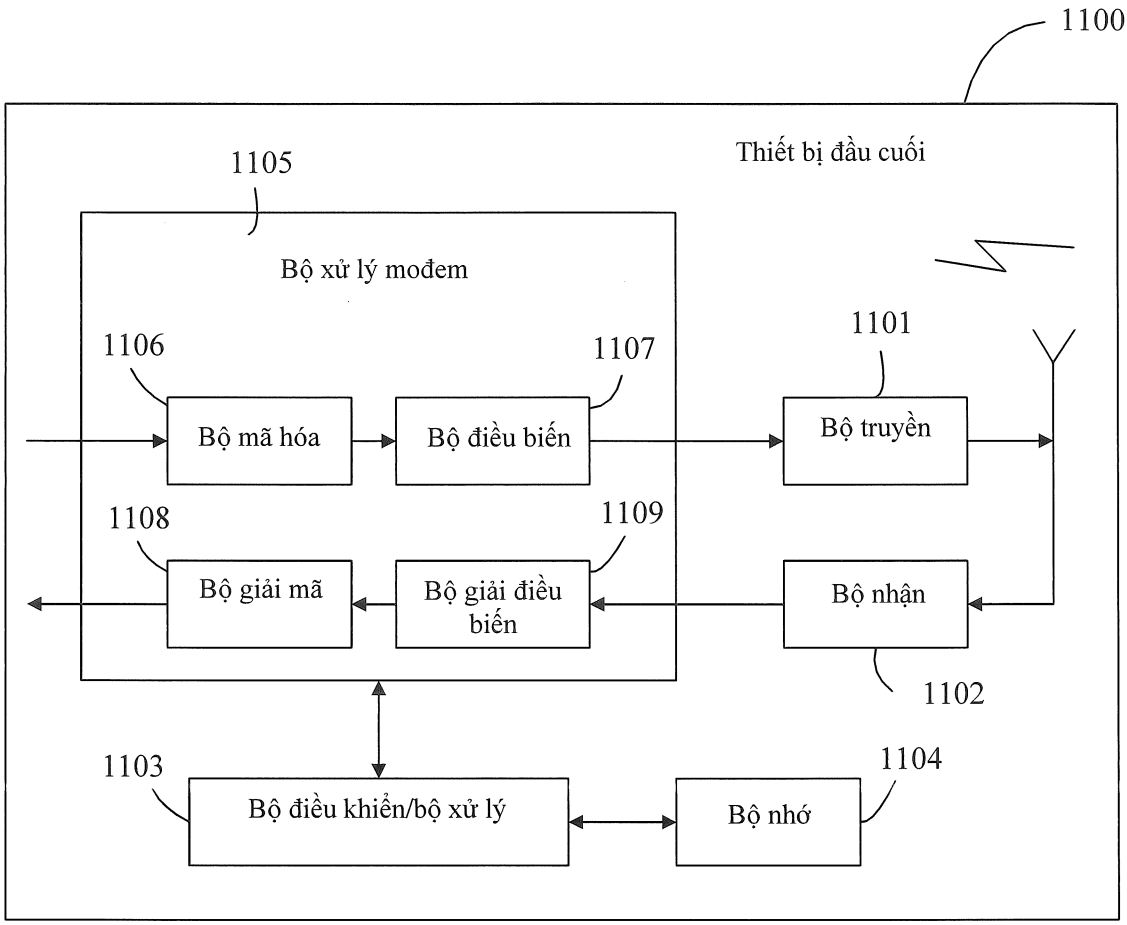
1100
Thiết bị đầu cuối
1105
Bộ xử lý modem
1106
Bộ mã hóa
1107
Bộ điều biến
1101
Bộ truyền
1108
Bộ giải mã
1109
Bộ giải điều biến
Bộ nhận
1102
1103
Bộ điều khiển/bộ xử lý
1104
Bộ nhớ

FIG. 11

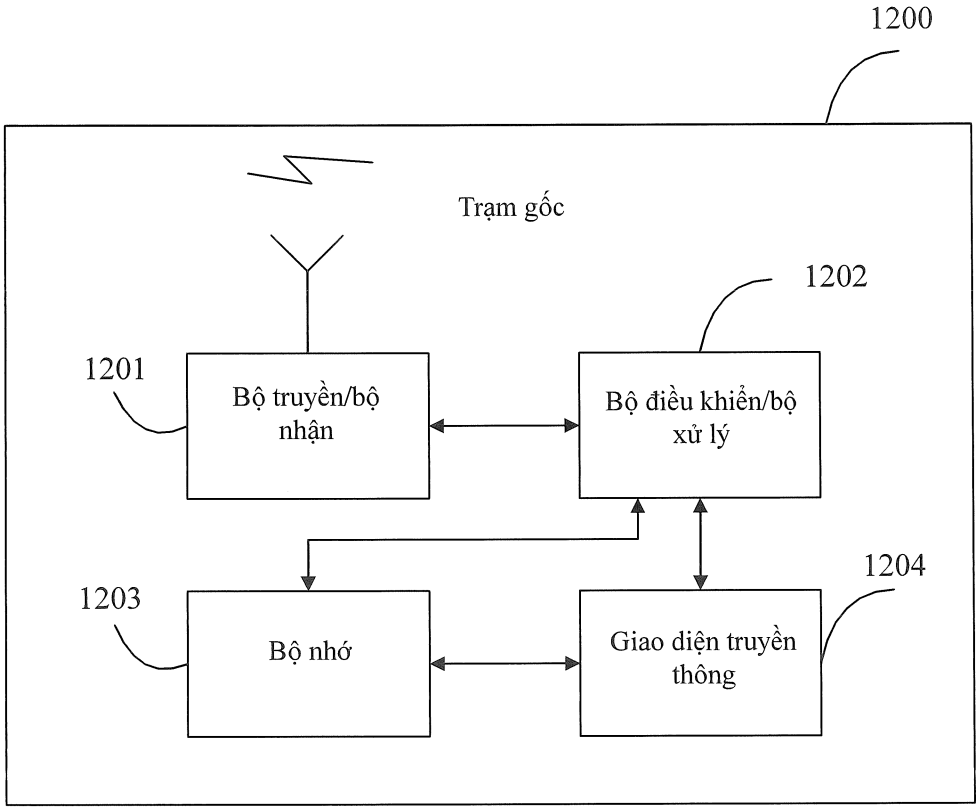
1200
Trạm gốc
1202
1201
Bộ truyền/bộ nhận
Bộ điều khiển/bộ xử lý
1204
1203
Bộ nhớ
Giao diện truyền thông

FIG. 12