



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

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

(11)



1-0041909

(51)^{2020.01} H04W 12/08

(13) B

(21) 1-2020-03322

(22) 31/10/2018

(86) PCT/CN2018/112897 31/10/2018

(87) WO2019/096002 23/05/2019

(30) 201711148926.5 17/11/2017 CN

(45) 25/12/2024 441

(43) 25/08/2020 389

(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)

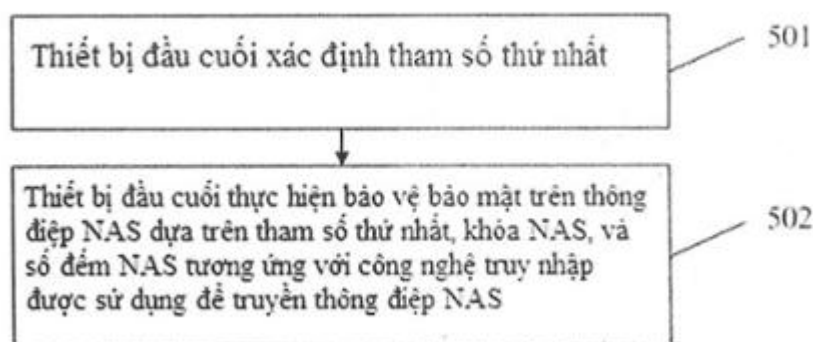
Huawei Administration Building, Bantian, Longgang District Shenzhen, Guangdong
518129, China

(72) LI, He (CN); CHEN, Jing (CN).

(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) PHƯƠNG PHÁP BẢO VỆ BẢO MẬT, THIẾT BỊ TRUYỀN THÔNG, VẬT GHI
MÁY TÍNH ĐỌC ĐƯỢC VÀ HỆ THỐNG TRUYỀN THÔNG

(57) Sáng chế đề cập đến lĩnh vực công nghệ truyền thông không dây. Các phương án thực hiện sáng chế đề xuất phương pháp bảo vệ bảo mật, thiết bị truyền thông, vật lưu trữ máy tính đọc được và hệ thống, để triển khai bảo vệ bảo mật cho các liên kết kết nối tầng không truy nhập (non-access stratum, NAS). Phương pháp theo sáng chế bao gồm các bước: xác định, bằng thiết bị, giá trị của tham số thứ nhất, trong đó giá trị của tham số thứ nhất được sử dụng để chỉ báo công nghệ truy nhập được sử dụng để truyền thông điệp NAS; và sau đó thực hiện, bằng thiết bị, bảo vệ bảo mật trên thông điệp NAS dựa trên tham số thứ nhất, khóa NAS, và số đếm NAS tương ứng với công nghệ truy nhập được sử dụng để truyền thông điệp NAS. Sáng chế có thể áp dụng cho quá trình thực hiện bảo vệ bảo mật trên thông điệp NAS.



Lĩnh vực kỹ thuật của sáng chế

Sáng chế đề cập đến lĩnh vực công nghệ truyền thông không dây, và cụ thể là, đến phương pháp bảo vệ bảo mật, thiết bị truyền thông, vật lưu trữ máy tính đọc được và hệ thống.

Tình trạng kỹ thuật của sáng chế

Trong hệ thống thế hệ thứ 5 (5th generation, 5G), thiết bị đầu cuối có thể truy nhập nút chức năng quản lý truy nhập và di động (access and mobility management function, AMF) chỉ qua công nghệ truy nhập dự án hợp tác thế hệ thứ 3 (3rd generation partnership project, 3GPP), hoặc chỉ qua công nghệ truy nhập phi 3GPP, hoặc qua cả công nghệ truy nhập 3GPP và công nghệ truy nhập phi 3GPP. Khi thiết bị đầu cuối truy nhập nút AMF qua cả công nghệ truy nhập 3GPP lẫn công nghệ truy nhập phi 3GPP, cùng lúc có hai liên kết kết nối tầng không truy nhập (non-access stratum, NAS) giữa thiết bị đầu cuối và nút AMF. Nếu thiết bị đầu cuối sử dụng một tập của các khóa NAS và một tập của các số đếm NASs (non-access stratum count, NAS count) để bảo vệ riêng rẽ hai liên kết kết nối, trường hợp sau có thể xảy ra: Nút AMF trước hết nhận được số đếm NAS tương đối nhỏ được truyền qua một liên kết, và sau đó nhận được số đếm NAS tương đối lớn được truyền qua liên kết còn lại. Kết quả là, xảy ra tấn công phát lại, dẫn đến vấn đề bảo mật dữ liệu tương đối kém cho phiên truyền liên kết kết nối NAS giữa thiết bị đầu cuối và nút AMF. Do vậy, khi có các liên kết kết nối NAS giữa thiết bị đầu cuối và nút AMF, cách thức thực hiện bảo vệ bảo mật trên các liên kết kết nối NAS là vấn đề cấp bách cần được giải quyết.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp bảo vệ bảo mật, thiết bị truyền thông, vật lưu trữ máy tính đọc được và hệ thống, để triển khai bảo vệ bảo mật cho các liên kết kết nối NAS.

Để đạt được các mục đích nêu trên, các vấn đề kỹ thuật sau được nêu theo các phương án thực hiện sáng chế:

Phương án thực hiện sáng chế đề xuất phương pháp bảo vệ bảo mật. Phương pháp bao gồm các bước: xác định, bởi thiết bị đầu cuối, tham số thứ nhất, và sau đó thực hiện bảo vệ bảo mật trên thông điệp NAS dựa trên tham số thứ nhất, khóa NAS, và số đếm NAS tương ứng với công nghệ truy nhập được sử dụng để truyền thông điệp NAS. Tham số thứ nhất là tham số đầu vào được sử dụng khi thiết bị đầu cuối thực hiện bảo vệ bảo mật trên thông điệp NAS, và được sử dụng để chỉ báo công nghệ truy nhập được sử dụng để truyền thông điệp NAS. Thiết bị đầu cuối có thể hỗ trợ ít nhất hai công nghệ truy nhập, và có thể duy trì riêng rẽ số đếm NAS tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập.

Chẳng hạn, ít nhất hai công nghệ truy nhập được hỗ trợ bởi thiết bị đầu cuối có thể bao gồm công nghệ truy nhập 3GPP và công nghệ truy nhập khác nhau mà có thể chia sẻ thiết bị mạng lõi mạng 3GPP tương tự với công nghệ truy nhập 3GPP. Công nghệ truy nhập khác nhau có thể là, chẳng hạn, công nghệ truy nhập phi 3GPP hoặc công nghệ truy nhập mạng cố định.

Một cách tùy chọn, tham số thứ nhất có thể còn được sử dụng để chỉ báo đường truyền được sử dụng bởi thiết bị đầu cuối để truyền thông điệp NAS, và thiết bị đầu cuối có thể duy trì riêng rẽ số đếm NAS tương ứng cho mỗi đường truyền được sử dụng để truyền các thông điệp NAS.

Tham số thứ nhất có thể là tham số đầu vào mới được thêm vào trong quá trình mã hóa/giải mật mã hoặc quá trình bảo vệ tính toàn vẹn, chẳng hạn, tham số ACCESS. Bit của tham số ACCESS có thể được gán bằng các giá trị khác nhau để biểu diễn các công nghệ truy nhập khác nhau. Chẳng hạn, nếu tham số thứ nhất bằng 00, chỉ báo rằng công nghệ truy nhập 3GPP được sử dụng; hoặc nếu tham số thứ nhất bằng 01, chỉ báo rằng công nghệ truy nhập phi 3GPP được sử dụng. Theo cách khác, tham số thứ nhất có thể là tất cả hoặc một số bit của tham số đầu vào COUNT hiện có trong quá trình mã hóa/giải mật mã hoặc quá trình bảo vệ tính toàn vẹn, hoặc tham số thứ nhất có thể là tất cả hoặc một số bit của tham số đầu vào BEARER hiện có trong quá trình mã hóa/giải mật mã hoặc

quá trình bảo vệ tính toàn vẹn.

Khóa NAS là chung cho ít nhất hai công nghệ truy nhập được hỗ trợ bởi thiết bị đầu cuối.

Theo phương pháp này, thiết bị đầu cuối có thể duy trì riêng rẽ các số đếm NAS tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập. Thiết bị đầu cuối không sử dụng cùng tập hợp các số đếm NAS khi truyền các thông điệp NAS qua các công nghệ truy nhập khác nhau. Thay vào đó, thiết bị đầu cuối thực hiện bảo vệ bảo mật trên thông điệp NAS bằng cách sử dụng số đếm NAS được duy trì cho công nghệ truy nhập tương ứng. Điều này có thể tránh vấn đề tấn công phát lại mà xảy ra khi thiết bị mạng lỗi trước hết nhận được số đếm NAS tương đối nhỏ được truyền bằng một liên kết, và sau đó nhận số đếm NAS tương đối lớn được truyền bằng liên kết khác. Ngoài ra, theo sáng chế, tham số thứ nhất được sử dụng để phân biệt các công nghệ truy nhập khác nhau còn được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS. Do vậy, thậm chí nếu khóa NAS tương tự và số đếm NAS tương tự được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS được truyền qua các công nghệ truy nhập khác nhau, các kết quả bảo vệ bảo mật của thông điệp NAS là khác nhau, giảm khả năng xuất hiện tấn công phát lại, nhờ đó triển khai bảo vệ bảo mật cho các liên kết kết nối NAS.

Theo thiết kế khả thi, ít nhất hai công nghệ truy nhập bao gồm công nghệ truy nhập thứ nhất. Nếu công nghệ truy nhập được sử dụng để truyền thông điệp NAS là công nghệ truy nhập thứ nhất, trước khi thiết bị đầu cuối xác định tham số thứ nhất, thiết bị đầu cuối có thể xác định số đếm NAS liên kết lên thứ nhất tương ứng với công nghệ truy nhập thứ nhất, và sau đó thiết bị đầu cuối gửi thông điệp thứ nhất đến thiết bị mạng lõi, trong đó bảo vệ bảo mật được thực hiện trên thông điệp thứ nhất bằng cách sử dụng số đếm NAS liên kết lên thứ nhất và khóa NAS, và thông điệp thứ nhất mang một số hoặc tất cả các bit của số đếm NAS liên kết lên thứ nhất.

Chẳng hạn, công nghệ truy nhập thứ nhất có thể là công nghệ truy nhập phi 3GPP.

Theo triển khai khả thi, giá trị bắt đầu của số đếm NAS liên kết lên thứ nhất

bằng 0, trong đó một số hoặc tất cả các bit của số đếm NAS liên kết lên thứ nhất bằng 0. Theo cách khác, số đếm NAS liên kết lên thứ nhất là số ngẫu nhiên. Cụ thể là, một số hoặc tất cả các bit trong số đếm NAS liên kết lên thứ nhất là các số ngẫu nhiên. Chẳng hạn, phần số trình tự hoặc phần tràn NAS của số đếm NAS liên kết lên thứ nhất là số ngẫu nhiên. Trong trường hợp này, phần còn lại bằng 0. Theo cách khác, ít nhất hai công nghệ truy nhập còn bao gồm công nghệ truy nhập thứ hai, và số đếm NAS liên kết lên thứ nhất là số đếm NAS liên kết lên (uplink, UL) tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS liên kết lên thứ nhất là số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối. Theo cách khác, ít nhất hai công nghệ truy nhập còn bao gồm công nghệ truy nhập thứ hai, và số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối. Theo cách khác, số đếm NAS liên kết lên thứ nhất là số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS liên kết lên thứ nhất là số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối. Theo cách khác, số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối.

Theo thiết kế khả thi khác, ít nhất hai công nghệ truy nhập bao gồm công nghệ truy nhập thứ nhất và công nghệ truy nhập thứ hai. Nếu công nghệ truy nhập được sử dụng để truyền thông điệp NAS là công nghệ truy nhập thứ nhất,

trước khi thiết bị đầu cuối xác định tham số thứ nhất, thiết bị đầu cuối có thể gửi thông điệp thứ nhất đến thiết bị mạng lõi, trong đó bảo vệ bảo mật được thực hiện trên thông điệp thứ nhất bằng khóa NAS và số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai, và thông điệp thứ nhất mang một số hoặc tất cả các bit của số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai.

Công nghệ truy nhập thứ hai là công nghệ truy nhập 3GPP. Một cách tùy chọn, tiền đề để triển khai thiết kế này là việc thiết bị đầu cuối đã được truy nhập thiết bị mạng lõi qua công nghệ truy nhập 3GPP.

Theo thiết kế khả thi, thông điệp thứ nhất có thể mang thông tin chỉ báo thứ nhất, và thông tin chỉ báo thứ nhất được sử dụng để chỉ báo công nghệ truy nhập tương ứng với một số hoặc tất cả các bit của số đếm NAS UL được mang trong thông điệp thứ nhất. Một cách tùy chọn, thông tin chỉ báo thứ nhất có thể còn được sử dụng để chỉ báo đường truyền tương ứng với một số hoặc tất cả các bit của số đếm NAS UL được mang trong thông điệp thứ nhất.

Theo thiết kế khả thi, thiết bị đầu cuối nhận thông điệp thứ hai từ thiết bị mạng lõi, trong đó thông điệp thứ hai bao gồm một hoặc cả hai số đếm NAS UL thứ hai và số đếm NAS liên kết xuống (Downlink, DL) thứ nhất tương ứng với công nghệ truy nhập thứ nhất.

Một cách tùy chọn, thông điệp thứ hai có thể bao gồm số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập thứ nhất. Theo cách khác, thông điệp thứ hai bao gồm cả số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập thứ nhất.

Một cách tùy chọn, số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập thứ nhất là tương tự.

Theo triển khai khả thi, giá trị bắt đầu của số đếm NAS UL thứ hai bằng 0, trong đó tất cả hoặc một số bit của số đếm NAS UL thứ hai bằng 0. Theo cách khác, số đếm NAS UL thứ hai là số ngẫu nhiên. Cụ thể là, một số hoặc tất cả các bit trong số đếm NAS UL thứ hai là các số ngẫu nhiên. Chẳng hạn, phần số trình tự hoặc phần tràn NAS của số đếm NAS UL thứ hai là số ngẫu nhiên. Trong trường hợp này, phần còn lại bằng 0. Theo cách khác, số đếm NAS UL thứ hai là số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ

bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS UL thứ hai là số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS UL thứ hai là số đếm NAS liên kết lên thứ nhất; hoặc số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS liên kết lên thứ nhất.

Theo thiết kế khả thi, giá trị bắt đầu của số đếm NAS DL thứ nhất bằng 0, trong đó tất cả hoặc một số bit của số đếm NAS DL thứ nhất bằng 0. Theo cách khác, số đếm NAS DL thứ nhất là số ngẫu nhiên. Cụ thể là, một số hoặc tất cả các bit trong số đếm NAS DL thứ nhất là các số ngẫu nhiên. Chẳng hạn, phần số trình tự hoặc phần tràn NAS của số đếm NAS DL thứ nhất là số ngẫu nhiên. Trong trường hợp này, phần còn lại bằng 0. Theo cách khác, số đếm NAS DL thứ nhất là số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS DL thứ nhất là số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai

và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi.

Theo thiết kế khả thi, thông điệp thứ hai mang thông tin chỉ báo thứ hai, và thông tin chỉ báo thứ hai được sử dụng để chỉ báo công nghệ truy nhập tương ứng với số đếm NAS DL thứ nhất được mang trong thông điệp thứ hai. Một cách tùy chọn, thông điệp thứ hai có thể còn mang thông tin chỉ báo được sử dụng để chỉ báo số đếm NAS UL thứ hai được mang trong thông điệp thứ hai.

Một cách tùy chọn, thông tin chỉ báo thứ hai được sử dụng để chỉ báo đường truyền tương ứng với số đếm NAS DL thứ nhất được mang trong thông điệp thứ hai. Một cách tùy chọn, thông điệp thứ hai có thể còn mang thông tin chỉ báo mà được sử dụng để chỉ báo đường truyền tương ứng với số đếm NAS UL thứ hai được mang trong thông điệp thứ hai.

Theo khía cạnh thứ hai, phương án thực hiện sáng chế đề xuất phương pháp bảo vệ bảo mật. Phương pháp bao gồm bước:

xác định, bởi thiết bị mạng lõi, tham số thứ nhất; sau đó thực hiện, bởi thiết bị mạng lõi, bảo vệ bảo mật trên thông điệp NAS dựa trên tham số thứ nhất, khóa NAS, và số đếm NAS tương ứng với công nghệ truy nhập được sử dụng để truyền thông điệp NAS. Tham số thứ nhất được sử dụng để chỉ báo công nghệ truy nhập được sử dụng để truyền thông điệp NAS. Thiết bị mạng lõi có thể duy trì riêng rẽ số đếm NAS tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập được hỗ trợ bởi thiết bị đầu cuối.

Chẳng hạn, ít nhất hai công nghệ truy nhập được hỗ trợ bởi thiết bị đầu cuối có thể bao gồm công nghệ truy nhập 3GPP và công nghệ truy nhập khác nhau. Công nghệ truy nhập khác nhau có thể là, chẳng hạn, công nghệ truy nhập phi 3GPP hoặc công nghệ truy nhập mạng cố định.

Một cách tùy chọn, tham số thứ nhất có thể còn được sử dụng để chỉ báo đường truyền được sử dụng bởi thiết bị mạng lõi để truyền thông điệp NAS, và

thiết bị mạng lõi có thể duy trì riêng rẽ số đếm NAS tương ứng cho mỗi đường truyền được sử dụng để truyền các thông điệp NAS.

Tham số thứ nhất có thể là tham số đầu vào mới được thêm vào trong quá trình mã hóa/giải mã hoặc quá trình bảo vệ tính toàn vẹn, chẳng hạn, tham số ACCESS. Bit của tham số ACCESS có thể được gán bằng các giá trị khác nhau để biểu diễn các công nghệ truy nhập khác nhau. Chẳng hạn, nếu tham số thứ nhất bằng 00, công nghệ truy nhập 3GPP được sử dụng; hoặc nếu tham số thứ nhất bằng 01, công nghệ truy nhập phi 3GPP được sử dụng. Theo cách khác, tham số thứ nhất có thể còn là tất cả hoặc một số bit của tham số đầu vào COUNT hiện có trong quá trình mã hóa/giải mã hoặc quá trình bảo vệ tính toàn vẹn. Theo cách khác, tham số thứ nhất có thể là tất cả hoặc một số bit của tham số đầu vào BEARER hiện có trong quá trình mã hóa/giải mã hoặc quá trình bảo vệ tính toàn vẹn.

Khóa NAS là chung cho ít nhất hai công nghệ truy nhập được hỗ trợ bởi thiết bị đầu cuối.

Theo phương pháp này, thiết bị mạng lõi có thể duy trì riêng rẽ các số đếm NAS tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập. Thiết bị đầu cuối không sử dụng một tập hợp các số đếm NAS khi truyền thông điệp NAS bằng các công nghệ truy nhập khác nhau. Thay vào đó, thiết bị mạng lõi thực hiện bảo vệ bảo mật trên thông điệp NAS bằng số đếm NAS được duy trì cho công nghệ truy nhập tương ứng. Điều này có thể tránh vấn đề tấn công phát lại mà xảy ra khi thiết bị đầu cuối trước hết nhận số đếm NAS tương đối nhỏ được truyền bằng một liên kết, và sau đó nhận số đếm NAS tương đối lớn được truyền bằng liên kết khác. Ngoài ra, theo sáng chế, tham số thứ nhất được sử dụng để phân biệt các công nghệ truy nhập khác nhau còn được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS. Do vậy, thậm chí nếu khóa NAS tương tự và số đếm NAS tương tự được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS được truyền qua các công nghệ truy nhập khác nhau, các kết quả bảo vệ bảo mật của thông điệp NAS là khác nhau, giảm khả năng xuất hiện tấn công phát lại, nhờ đó triển khai bảo vệ bảo mật cho các liên kết kết nối NAS.

Theo thiết kế khả thi, ít nhất hai công nghệ truy nhập bao gồm công nghệ truy nhập thứ nhất. Nếu công nghệ truy nhập được sử dụng để truyền thông điệp NAS là công nghệ truy nhập thứ nhất, trước khi thiết bị mạng lõi xác định tham số thứ nhất, thiết bị mạng lõi có thể nhận thông điệp thứ nhất, trong đó bảo vệ bảo mật được thực hiện trên thông điệp thứ nhất bằng khóa NAS và số đếm NAS liên kết lên thứ nhất tương ứng với công nghệ truy nhập thứ nhất, và thông điệp thứ nhất mang số đếm NAS liên kết lên thứ nhất.

Chẳng hạn, công nghệ truy nhập thứ nhất có thể là công nghệ truy nhập phi 3GPP.

Theo triển khai khả thi, giá trị bắt đầu của số đếm NAS liên kết lên thứ nhất bằng 0, trong đó một số hoặc tất cả các bit của số đếm NAS liên kết lên thứ nhất bằng 0. Theo cách khác, số đếm NAS liên kết lên thứ nhất là số ngẫu nhiên. Cụ thể là, một số hoặc tất cả các bit trong số đếm NAS liên kết lên thứ nhất là các số ngẫu nhiên. Chẳng hạn, phần số trình tự hoặc phần tràn NAS của số đếm NAS liên kết lên thứ nhất là số ngẫu nhiên. Trong trường hợp này, phần còn lại bằng 0. Theo cách khác, ít nhất hai công nghệ truy nhập còn bao gồm công nghệ truy nhập thứ hai, và số đếm NAS liên kết lên thứ nhất là số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS liên kết lên thứ nhất là số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối. Theo cách khác, ít nhất hai công nghệ truy nhập còn bao gồm công nghệ truy nhập thứ hai, và số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối. Theo cách khác, số đếm NAS liên kết lên thứ nhất là số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS liên kết lên thứ nhất là số đếm NAS

UL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối. Theo cách khác, số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối.

Theo thiết kế khả thi khác, ít nhất hai công nghệ truy nhập bao gồm công nghệ truy nhập thứ nhất và công nghệ truy nhập thứ hai. Nếu công nghệ truy nhập được sử dụng để truyền thông điệp NAS là công nghệ truy nhập thứ nhất, trước khi thiết bị mạng lõi xác định tham số thứ nhất, thiết bị mạng lõi có thể nhận thông điệp thứ nhất, trong đó bảo vệ bảo mật được thực hiện trên thông điệp thứ nhất bằng khóa NAS và số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai, và thông điệp thứ nhất mang một số hoặc tất cả các bit của số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai.

Công nghệ truy nhập thứ hai là công nghệ truy nhập 3GPP. Một cách tùy chọn, tiền đề để triển khai thiết kế này là việc thiết bị đầu cuối đã được truy nhập thiết bị mạng lõi bằng công nghệ truy nhập 3GPP.

Theo thiết kế khả thi, thông điệp thứ nhất mang thông tin chỉ báo thứ nhất, và thông tin chỉ báo thứ nhất được sử dụng để chỉ báo công nghệ truy nhập tương ứng với một số hoặc tất cả các bit của số đếm NAS UL được mang trong thông điệp thứ nhất. Một cách tùy chọn, thông tin chỉ báo thứ nhất có thể còn được sử dụng để chỉ báo đường truyền tương ứng với một số hoặc tất cả các bit của số đếm NAS UL được mang trong thông điệp thứ nhất.

Theo thiết kế khả thi, sau khi thiết bị mạng lõi nhận thông điệp thứ nhất từ thiết bị đầu cuối, thiết bị mạng lõi kiểm chứng, theo số đếm NAS UL tương ứng với công nghệ truy nhập được chỉ báo bởi thông tin chỉ báo thứ nhất, một số hoặc tất cả các bit của số đếm NAS được mang trong thông điệp thứ nhất.

Theo phương án thực hiện sáng chế, thiết bị mạng lõi có thể độc lập duy trì số đếm NAS của công nghệ truy nhập 3GPP và số đếm NAS của công nghệ truy nhập phi 3GPP, và còn kiểm chứng số đếm NAS UL được nhận theo số đếm

NAS UL được duy trì bởi thiết bị mạng lõi, nhờ đó giảm khả năng xuất hiện tấn công phát lại.

Theo thiết kế khả thi, thiết bị mạng lõi xác định một hoặc cả hai số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập thứ nhất, và sau đó thiết bị mạng lõi gửi thông điệp thứ hai đến thiết bị đầu cuối, trong đó thông điệp thứ hai bao gồm một hoặc cả hai số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập thứ nhất.

Một cách tùy chọn, thông điệp thứ hai có thể bao gồm số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập thứ nhất. Theo cách khác, thông điệp thứ hai bao gồm cả số đếm NAS UL thứ hai lẫn số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập thứ nhất.

Một cách tùy chọn, số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập thứ nhất là tương tự.

Theo triển khai khả thi, giá trị bắt đầu của số đếm NAS UL thứ hai bằng 0, trong đó tất cả hoặc một số bit của số đếm NAS UL thứ hai bằng 0. Theo cách khác, số đếm NAS UL thứ hai là số ngẫu nhiên. Cụ thể là, một số hoặc tất cả các bit trong số đếm NAS UL thứ hai là các số ngẫu nhiên. Chẳng hạn, phần số trình tự hoặc phần tràn NAS của số đếm NAS UL thứ hai là số ngẫu nhiên. Trong trường hợp này, phần còn lại bằng 0. Theo cách khác, số đếm NAS UL thứ hai là số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS UL thứ hai là số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS

DL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS UL thứ hai là số đếm NAS liên kết lên thứ nhất; hoặc số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS liên kết lên thứ nhất.

Theo triển khai khả thi, giá trị bắt đầu của số đếm NAS DL thứ nhất bằng 0, trong đó tất cả hoặc một số bit của số đếm NAS DL thứ nhất bằng 0. Theo cách khác, số đếm NAS DL thứ nhất là số ngẫu nhiên. Cụ thể là, một số hoặc tất cả các bit in số đếm NAS DL thứ nhất là các số ngẫu nhiên. Chẳng hạn, phần số trình tự hoặc phần tràn NAS của số đếm NAS DL thứ nhất là số ngẫu nhiên. Trong trường hợp này, phần còn lại bằng 0. Theo cách khác, số đếm NAS DL thứ nhất là số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS DL thứ nhất là số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi.

Theo thiết kế khả thi, thông điệp thứ hai mang thông tin chỉ báo thứ hai, và thông tin chỉ báo thứ hai được sử dụng để chỉ báo công nghệ truy nhập tương ứng với số đếm NAS DL thứ nhất được mang trong thông điệp thứ hai. Một cách tùy chọn, thông điệp thứ hai có thể còn mang thông tin chỉ báo được sử dụng để chỉ báo số đếm NAS UL thứ hai được mang trong thông điệp thứ hai.

Một cách tùy chọn, thông tin chỉ báo thứ hai được sử dụng để chỉ báo đường truyền tương ứng với số đếm NAS DL thứ nhất được mang trong thông điệp thứ hai. Một cách tùy chọn, thông điệp thứ hai có thể còn mang thông tin chỉ báo mà được sử dụng để chỉ báo đường truyền tương ứng với số đếm NAS UL thứ hai được mang trong thông điệp thứ hai.

Theo khía cạnh thứ ba, phương án thực hiện sáng chế đề xuất thiết bị, và thiết bị có chức năng triển khai các hoạt động của thiết bị đầu cuối theo triển khai phương pháp nêu trên. Chức năng có thể được triển khai bằng phần cứng, hoặc có thể được triển khai bằng phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên. Chẳng hạn, thiết bị có thể là thiết bị đầu cuối, hoặc có thể là vi mạch trong thiết bị đầu cuối.

Theo thiết kế khả thi, thiết bị là thiết bị đầu cuối, và thiết bị đầu cuối bao gồm bộ xử lý. Bộ xử lý được tạo cấu hình để hỗ trợ thiết bị đầu cuối khi thực hiện chức năng tương ứng ở phương pháp nêu trên. Ngoài ra, thiết bị đầu cuối có thể còn bao gồm bộ truyền và bộ nhận, trong đó bộ truyền và bộ nhận được tạo cấu hình để hỗ trợ truyền thông giữa thiết bị đầu cuối và thiết bị mạng lõi. Ngoài ra, thiết bị đầu cuối có thể còn bao gồm bộ nhớ, và bộ nhớ được tạo cấu hình để ghép nối với bộ xử lý, và lưu trữ lệnh chương trình cần thiết và dữ liệu cần cho thiết bị đầu cuối.

Theo khía cạnh thứ tư, phương án thực hiện sáng chế đề xuất thiết bị, và thiết bị có chức năng triển khai các hoạt động của thiết bị mạng lõi theo triển khai phương pháp nêu trên. Chức năng có thể được triển khai bằng phần cứng, hoặc có thể được triển khai bằng phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên. Chẳng hạn, thiết bị có thể là thiết bị mạng lõi, hoặc có thể là vi mạch trong thiết bị mạng lõi.

Theo thiết kế khả thi, thiết bị là thiết bị mạng lõi, và thiết bị mạng lõi bao gồm bộ xử lý. Bộ xử lý được tạo cấu hình để hỗ trợ thiết bị mạng lõi khi thực hiện chức năng tương ứng ở phương pháp nêu trên. Ngoài ra, thiết bị mạng lõi có thể còn bao gồm bộ truyền và bộ nhận, trong đó bộ truyền và bộ nhận được

tạo cấu hình để hỗ trợ truyền thông giữa thiết bị mạng lõi và thiết bị đầu cuối. Ngoài ra, thiết bị mạng lõi có thể còn bao gồm bộ nhớ, và bộ nhớ được tạo cấu hình để ghép nối với bộ xử lý, và lưu trữ lệnh chương trình và dữ liệu cần cho thiết bị đầu cuối.

Theo khía cạnh thứ năm, phương án thực hiện sáng chế đề xuất hệ thống truyền thông, trong đó hệ thống bao gồm thiết bị đầu cuối và thiết bị mạng lõi được mô tả theo các khía cạnh nêu trên. Một cách tùy chọn, hệ thống có thể còn bao gồm trạm cơ sở, nút N3IWF, và thiết bị đầu cuối và thiết bị mạng lõi được mô tả theo các khía cạnh nêu trên.

Theo khía cạnh thứ sáu, phương án thực hiện sáng chế đề xuất vật lưu trữ máy tính, được tạo cấu hình để lưu trữ lệnh phần mềm máy tính được sử dụng thiết bị đầu cuối nêu trên, trong đó lệnh phần mềm máy tính bao gồm chương trình được thiết kế thực thi khía cạnh thứ nhất.

Theo khía cạnh thứ bảy, phương án thực hiện sáng chế đề xuất vật lưu trữ máy tính, được tạo cấu hình để lưu trữ lệnh phần mềm máy tính được sử dụng bằng thiết bị mạng lõi nêu trên. Lệnh phần mềm máy tính bao gồm chương trình được thiết kế thực thi khía cạnh thứ hai.

Theo khía cạnh thứ tám, phương án thực hiện sáng chế đề xuất sản phẩm chương trình máy tính bao gồm lệnh. Khi máy tính chạy lệnh, máy tính có thể thực hiện phương pháp in khía cạnh thứ nhất.

Theo khía cạnh thứ chín, phương án thực hiện sáng chế đề xuất sản phẩm chương trình máy tính bao gồm lệnh. Khi máy tính chạy lệnh, máy tính có thể thực hiện phương pháp in khía cạnh thứ hai.

Theo khía cạnh thứ mười, phương án thực hiện sáng chế đề xuất hệ thống vi mạch được áp dụng cho thiết bị đầu cuối, trong đó hệ thống vi mạch bao gồm ít nhất một bộ xử lý, bộ nhớ, và mạch thu phát. Bộ nhớ, mạch thu phát, và ít nhất một bộ xử lý được kết nối với nhau qua các đường truyền. Ít nhất một bộ nhớ lưu trữ lệnh. Lệnh này được thực thi bởi bộ xử lý, để thực thi các hoạt động của thiết bị đầu cuối ở phương pháp được mô tả trong khía cạnh thứ nhất.

Theo khía cạnh thứ mười một, phương án thực hiện sáng chế đề xuất hệ thống vi mạch được áp dụng cho thiết bị mạng lõi, trong đó hệ thống vi mạch bao gồm

ít nhất một bộ xử lý, bộ nhớ, và mạch thu phát. Bộ nhớ, mạch thu phát, và ít nhất một bộ xử lý được kết nối với nhau qua các đường truyền. Ít nhất một bộ nhớ lưu trữ lệnh. Lệnh này được thực thi bởi bộ xử lý, để thực thi các hoạt động của thiết bị mạng lõi ở phương pháp được mô tả trong khía cạnh thứ hai.

Theo phương pháp bảo vệ bảo mật theo các phương án thực hiện sáng chế, thiết bị đầu cuối có thể duy trì riêng rẽ số đếm NAS tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập. Thiết bị đầu cuối không sử dụng một tập hợp các số đếm NAS khi truyền thông điệp NAS qua các công nghệ truy nhập khác nhau. Thay vào đó, thiết bị đầu cuối thực hiện bảo vệ bảo mật trên thông điệp NAS bằng số đếm NAS được duy trì cho công nghệ truy nhập tương ứng. Điều này có thể tránh vấn đề tấn công phát lại mà xảy ra khi thiết bị mạng lõi trước hết nhận số đếm NAS tương đối nhỏ được truyền bằng một liên kết, và sau đó nhận số đếm NAS tương đối lớn được truyền qua liên kết khác. Ngoài ra, theo sáng chế, tham số thứ nhất được sử dụng để phân biệt các công nghệ truy nhập khác nhau còn được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS. Do vậy, thậm chí nếu khóa NAS tương tự và số đếm NAS tương tự được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS được truyền qua các công nghệ truy nhập khác nhau, các kết quả bảo vệ bảo mật của thông điệp NAS là khác nhau, giảm khả năng xuất hiện tấn công phát lại, nhờ đó triển khai bảo vệ bảo mật cho các liên kết kết nối NAS.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ của kiến trúc mạng khả thi theo phương án thực hiện sáng chế;

Fig.2 là sơ đồ của kiến trúc mạng khả thi khác theo phương án thực hiện sáng chế;

Fig.3 là ví dụ của sơ đồ của phương pháp mật mã hóa và giải mật mã theo phương án thực hiện sáng chế;

Fig.4 là ví dụ của sơ đồ của phương pháp bảo vệ tính toàn vẹn theo phương án thực hiện sáng chế;

Fig.5 là lưu đồ của phương pháp bảo vệ bảo mật theo phương án thực hiện sáng chế;

Fig.6 là ví dụ của sơ đồ của phương pháp mật mã hóa và giải mật mã khác theo phương án thực hiện sáng chế;

Fig.7 là ví dụ của sơ đồ của phương pháp mật mã hóa và giải mật mã khác nữa theo phương án thực hiện sáng chế;

Fig.8 là ví dụ của sơ đồ của phương pháp mật mã hóa và giải mật mã khác nữa theo phương án thực hiện sáng chế;

Fig.9 là lưu đồ của phương pháp bảo vệ bảo mật khác theo phương án thực hiện sáng chế;

Fig.10 là lưu đồ của phương pháp bảo vệ bảo mật khác nữa theo phương án thực hiện sáng chế;

Fig.11A và Fig.11B là lưu đồ của phương pháp bảo vệ bảo mật khác nữa theo phương án thực hiện sáng chế;

Fig.12 là sơ đồ cấu trúc của thiết bị theo phương án thực hiện sáng chế;

Fig.13 là sơ đồ cấu trúc của thiết bị đầu cuối theo phương án thực hiện sáng chế;

Fig.14 là sơ đồ cấu trúc của thiết bị khác theo phương án thực hiện sáng chế; và

Fig.15 là sơ đồ cấu trúc của thiết bị mạng lõi theo phương án thực hiện sáng chế.

Mô tả chi tiết sáng chế

Phần sau còn mô tả chi tiết sáng chế dựa vào các hình vẽ đi kèm. Phương pháp hoạt động cụ thể ở các phương án thực hiện phương pháp có thể cũng được áp dụng cho phương án thực hiện của thiết bị hoặc phương án thực hiện của hệ thống. Trong các phần mô tả của sáng chế, trừ khi có thông báo khác, “các” nghĩa là hai hoặc nhiều hơn hai.

Kiến trúc hệ thống và kịch bản dịch vụ được mô tả trong sáng chế nhằm mô tả rõ ràng hơn các giải pháp kỹ thuật theo sáng chế, mà không nhằm giới hạn các giải pháp kỹ thuật theo sáng chế. Người có hiểu biết trung bình trong lĩnh vực có thể biết rằng khi kiến trúc hệ thống tiến hóa và kịch bản dịch vụ mới phát triển, các giải pháp kỹ thuật theo sáng chế cũng áp dụng được cho vấn đề kỹ thuật

tương tự.

Nên lưu ý rằng, theo sáng chế, cụm từ chẳng hạn “ví dụ” hoặc “chẳng hạn” được sử dụng làm ví dụ để nêu minh họa, hoặc phần mô tả. Phương án thực hiện hoặc giải pháp thiết kế bất kỳ được mô tả như là “ví dụ” hoặc “chẳng hạn” theo sáng chế sẽ không nên được giải thích như là được ưu tiên hơn hoặc có nhiều lợi thế hơn so với phương án thực hiện hoặc giải pháp thiết kế khác. Chính xác là, việc sử dụng từ “ví dụ”, hoặc “chẳng hạn”, hoặc tương tự nhằm nêu khái niệm liên quan theo cách cụ thể.

Các phương án thực hiện sáng chế có thể được áp dụng cho hệ thống truyền thông không dây thế hệ mới, chẳng hạn, hệ thống truyền thông 5G. Fig.1 thể hiện sơ đồ của kiến trúc mạng khả thi theo sáng chế. Kiến trúc mạng bao gồm các phần sau.

Nút AMF là phần tử mạng chịu trách nhiệm quản lý di động, và có thể được tạo cấu hình để triển khai chức năng khác ngoài quản lý phiên trong các chức năng thực thể quản lý di động (mobility management entity, MME), chẳng hạn, chức năng chẳng hạn can thiệp hợp pháp hoặc ủy quyền truy nhập.

Nút chức năng quản lý phiên (session management function, SMF) được tạo cấu hình để phân phối tài nguyên phiên đến mặt phẳng người dùng.

Nút chức năng máy chủ xác thực (authentication server function, AUSF) chịu trách nhiệm: khi nút AUSF thực hiện xác thực trên thiết bị đầu cuối, kiểm chứng và truyền tham số cần được xác thực, và tính chân thực xác thực của thiết bị đầu cuối. Các chức năng chính bao gồm: nhận yêu cầu xác thực được gửi bởi nút chức năng neo bảo mật (security anchor function, SEAF), và lựa chọn phương pháp xác thực. Khi phương pháp giao thức xác thực mở rộng cho phương pháp xác thực thỏa thuận khóa và xác thực thể hệ thứ ba (extensible authentication protocol authentication and key agreement, EAP-AKA') được sử dụng, nút AUSF có thể hoàn thành xác thực từ phía mạng đến thiết bị đầu cuối.

Nút SEAF có thể là một phần của nút AMF, hoặc có thể là phần tử mạng độc lập, và chịu trách nhiệm khởi tạo yêu cầu xác thực đến nút AUSF và hoàn thành xác thực từ phía mạng đến thiết bị đầu cuối trong quá trình xác thực của xác thực hệ thống gói tiến hóa và thỏa thuận khóa (evolved packet system authentication

and key agreement, EPS-AKA*).

Nút chức năng mặt phẳng người dùng (user plane function, UPF) là nút nguồn của dữ liệu mặt phẳng người dùng, và được tạo cấu hình để kết nối với mạng bên ngoài.

Mạng dữ liệu (Data Network, DN) là mạng được sử dụng để cấp dữ liệu bên ngoài, chẳng hạn, mạng Internet (Internet).

Nút mạng truy nhập (vô tuyến) ((radio) access network, (R)AN) có thể sử dụng các công nghệ truy nhập khác nhau. Hiện tại, có hai loại công nghệ truy nhập vô tuyến: công nghệ truy nhập 3GPP (chẳng hạn, công nghệ truy nhập vô tuyến được sử dụng trong hệ thống 3G, 4G, hoặc 5G) và công nghệ truy nhập phi 3GPP. Công nghệ truy nhập 3GPP là công nghệ truy nhập mà tuân theo đặc tả chuẩn 3GPP. Công nghệ truy nhập bằng cách sử dụng công nghệ truy nhập 3GPP là RAN. Thiết bị mạng truy nhập trong hệ thống 5G được gọi là trạm cơ sở nút thế hệ tiếp theo (next generation node base station, gNB). Công nghệ truy nhập phi 3GPP là công nghệ truy nhập mà không tuân theo đặc tả chuẩn 3GPP, chẳng hạn, công nghệ vô tuyến được biểu diễn bởi điểm truy nhập (access point, AP) WiFi.

Thiết bị đầu cuối theo sáng chế là thiết bị có các chức năng truyền và nhận không dây. Thiết bị đầu cuối có thể được khai triển trên mặt đất, chẳng hạn, thiết bị trong nhà, thiết bị ngoài trời, thiết bị cầm tay, hoặc thiết bị trong xe; hoặc có thể được khai triển trên mặt nước (chẳng hạn, trên tàu hỏa); hoặc có thể được khai triển trong không khí (chẳng hạn, trên máy bay, khinh khí cầu, hoặc vệ tinh). Thiết bị đầu cuối có thể bao gồm các loại khác nhau của thiết bị người dùng (user equipment, UE), điện thoại di động, các máy tính bảng (pad), máy tính có các chức năng truyền và nhận không dây, các thẻ dữ liệu không dây, 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 truyền thông loại máy (machine type communication, MTC), thiết bị đầu cuối trong điều khiển công nghiệp, thiết bị đầu cuối xe tự lái, thiết bị đầu cuối y tế từ xa, thiết bị đầu cuối lưới thông minh, các thiết bị đầu cuối trong an toàn giao thông, thiết bị đầu cuối ở thành phố thông minh, thiết bị đeo được (chẳng hạn băng đồng hồ thông minh, băng đeo thông

minh, và máy đếm bước), và tương tự. Các thiết bị đầu cuối có các chức năng truyền thông không dây tương tự có thể có các tên khác nhau trong các hệ thống trong đó các công nghệ truy nhập vô tuyến khác nhau được sử dụng. Để dễ mô tả, theo các phương án thực hiện sáng chế, các thiết bị nêu trên có các chức năng truyền thông nhận và truyền không dây được gọi chung là các thiết bị đầu cuối.

Cụ thể là, thiết bị đầu cuối theo sáng chế lưu trữ khóa dài hạn và chức năng liên quan. Khi thực hiện xác thực hai chiều có nút mạng lõi (chẳng hạn nút AMF, nút AUSF, và nút SEAF), thiết bị đầu cuối có thể kiểm chứng tính chân thực của mạng bằng khóa dài hạn và chức năng liên quan.

Thiết bị mạng truy nhập theo các phương án thực hiện sáng chế là thiết bị cấp chức năng truyền thông không dây cho thiết bị đầu cuối. Chẳng hạn, thiết bị mạng truy nhập có thể là trạm cơ sở (Base Station, BS), và BS có thể bao gồm các dạng khác nhau của các BS lớn, các BS nhỏ, các trạm chuyển tiếp, các AP, và tương tự. Các thiết bị có các chức năng của BS có thể có các tên khác trong các hệ thống trong đó các công nghệ truy nhập không dây khác nhau được sử dụng. Chẳng hạn, trong hệ thống 5G, thiết bị có các chức năng của BS được gọi là BS nút thế hệ mới, và có thể được biểu diễn như là gNB; trong hệ thống tiến hóa dài hạn (Long Term Evolution, LTE), thiết bị có các chức năng của BS được gọi là nút B tiến hóa (evolved NodeB, eNB hoặc eNodeB); trong hệ thống truyền thông thế hệ thứ 3 (3rd Generation, 3G), thiết bị có các chức năng của BS được gọi là nút B (Node B). Để dễ mô tả, theo các phương án thực hiện sáng chế, các thiết bị nêu trên mà cấp chức năng truyền thông không dây cho thiết bị đầu cuối được gọi chung là các thiết bị mạng truy nhập.

Nút chức năng lộ diện mạng (network exposure function, NEF) chủ yếu được tạo cấu hình để tương tác với bên thứ ba, sao cho bên thứ ba có thể tương tác gián tiếp với phần tử mạng trong một số mạng 3GPP.

Nút chức năng kho lưu trữ mạng (network function repository function, NRF) được tạo cấu hình để khám phá phần tử giữa các mạng và bảo trì chức năng mạng (network function, NF).

Nút chức năng điều khiển chính sách (policy control function, PCF) lưu trữ quy tắc chất lượng dịch vụ (quality of service, QoS) mới nhất. BS có thể phân

phối tài nguyên thích hợp đến kênh truyền mặt phẳng người dùng theo quy tắc QoS được cấp cho nút SMF.

Nút quản lý dữ liệu thống nhất (unified data management, UDM) được tạo cấu hình để lưu trữ thông tin thuê bao của người dùng.

Nút chức năng ứng dụng (application function, AF) có thể được đặt bên trong DN, và là phần tử mạng chức năng được khai triển ở bên thứ ba. Phần tử mạng này chủ yếu được tạo cấu hình để thông báo cho nút PCF về yêu cầu dịch vụ mới nhất của doanh nghiệp bên thứ ba cho ứng dụng. Nút PCF có thể tạo quy tắc QoS tương ứng dựa trên yêu cầu dịch vụ, để đảm bảo rằng dịch vụ được cấp bởi mạng thỏa mãn yêu cầu được nêu bởi bên thứ ba.

Theo các phương án thực hiện sáng chế, thiết bị đầu cuối có thể truy nhập nút AMF bằng ít nhất hai công nghệ truy nhập. Việc ít nhất hai công nghệ truy nhập bao gồm công nghệ truy nhập 3GPP và công nghệ truy nhập phi 3GPP được sử dụng làm ví dụ. Phương án thực hiện sáng chế còn đề xuất sơ đồ của kiến trúc mạng khả thi. Như được thể hiện trên Fig.2, kiến trúc mạng bao gồm nút AMF, nút AUSF, nút SMF, nút UPF, nút UDM (hoặc nút chức năng xử lý và kho lưu trữ ủy nhiệm xác thực (authentication credential repository and processing function, APRF)), thiết bị đầu cuối, và nút chức năng liên kết làm việc phi (phi 3GPP interworking function, N3IWF).

Đối với nút AMF, nút AUSF, nút SMF, nút UPF, nút UDM, và thiết bị đầu cuối, tham khảo phần mô tả trên Fig.1. Các chi tiết không được mô tả lại ở đây.

Nút N3IWF được tạo cấu hình để hỗ trợ thiết bị đầu cuối khi truy nhập nút AMF bằng công nghệ truy nhập phi 3GPP.

Dựa vào kiến trúc mạng được thể hiện trên Fig.2, thiết bị đầu cuối có thể truy nhập nút AMF qua cả công nghệ truy nhập 3GPP lẫn công nghệ truy nhập phi 3GPP. Công nghệ truy nhập 3GPP có thể được biểu diễn đơn giản là 3GPP, và công nghệ truy nhập phi 3GPP có thể được biểu diễn đơn giản là phi 3GPP. Tuyến 1 trên Fig.2 là tuyến mà trên đó thiết bị đầu cuối truy nhập nút AMF qua 3GPP, và tuyến 2 là tuyến mà trên đó thiết bị đầu cuối truy nhập nút AMF qua phi 3GPP, nói cách khác, thiết bị đầu cuối có thể truy nhập nút AMF qua nút N3IWF. Khi thiết bị đầu cuối truy nhập nút AMF qua cả 3GPP lẫn phi 3GPP, nếu thiết bị đầu

cuối cần gửi thông điệp NAS đến nút AMF, theo triển khai khả thi, thông điệp NAS có thể được tách thành ít nhất hai khối thông điệp, trong đó một phần của các khối thông điệp được truyền qua 3GPP, và phần còn lại của các khối thông điệp được truyền qua phi 3GPP. Chẳng hạn, thông điệp NAS có thể được phân chia thành khối thông điệp 1, khối thông điệp 2, khối thông điệp 3, khối thông điệp 4, và khối thông điệp 5. Các khối thông điệp 2 và 4 được truyền qua 3GPP, và các khối thông điệp 1, 3, và 5 được truyền qua phi 3GPP. Theo triển khai khả thi khác, thiết bị đầu cuối có thể truyền toàn bộ thông điệp NAS qua 3GPP, và truyền toàn bộ thông điệp NAS khác qua phi 3GPP.

Trước hết, các cụm từ liên quan đến các phương án thực hiện sáng chế được giải thích.

(1) số đếm NAS

Số đếm NAS bao gồm 24 bit bao gồm phần tràn NAS 16-bit và số trình tự 8-bit.

Giá trị bắt đầu của số đếm NAS bằng 0. Số đếm NAS UL được tăng lên 1 mỗi lần thiết bị đầu cuối gửi một thông điệp NAS đến thiết bị mạng lõi, và số đếm NAS DL được tăng lên 1 mỗi lần thiết bị mạng lõi gửi một thông điệp NAS đến thiết bị đầu cuối. Sau khi hoàn thành quá trình xác thực từ thiết bị đầu cuối đến thiết bị mạng lõi, cả số đếm NAS UL lẫn số đếm NAS DL được gán bằng 0.

Một cách tùy chọn, có hai phương pháp duy trì số đếm NAS:

Phương pháp 1: Sau khi thông điệp NAS được gửi, số đếm NAS lưu trữ được tăng lên 1 và được lưu trữ; và khi thông điệp NAS cần được gửi lần tới, bảo vệ bảo mật được thực hiện trên thông điệp NAS bằng số đếm NAS lưu trữ.

Phương pháp 2: Sau khi thông điệp NAS được gửi, khi thông điệp NAS cần được gửi lần tới, số đếm NAS lưu trữ được tăng lên 1 để thu được số đếm NAS mới, và bảo vệ bảo mật được thực hiện trên thông điệp NAS bằng số đếm NAS mới.

Sau khi nhận thông điệp NAS, thiết bị đầu cuối và thiết bị mạng lõi có thể kiểm chứng liệu số đếm NAS được nhận được sử dụng lại, cụ thể là, kiểm chứng liệu số đếm NAS được mang trong thông điệp NAS lớn hơn số đếm NAS được nhận trước đó. Chẳng hạn, nếu nút AMF nhận số đếm NAS UL từ thiết bị đầu

cuối, số đếm NAS UL được nhận có thể được so sánh với số đếm NAS được nhận trước đó UL. Nếu số đếm NAS UL được nhận lớn hơn số đếm NAS được nhận trước đó UL, kiểm chứng bảo mật được thực hiện trên thông điệp NAS thành công.

Khi mật mã hóa và giải mật mã, và bảo vệ tính toàn vẹn được thực hiện bằng số đếm NAS, số đếm NAS được đệm vào 32 bit, nói cách khác, 8 bit được đệm ở phía trước của số đếm NAS 24 bit ban đầu, trong đó 8 bit được đệm có thể đều là 0.

(2) Mật mã hóa và giải mật mã

Fig.3 thể hiện quá trình mật mã hóa và giải mật mã thông điệp NAS.

Ở đây, khóa này có thể là khóa NAS.

COUNT được sử dụng cho mật mã hóa và giải mật mã bao gồm 32 bit, trong đó 8 bit đầu bằng 0, 16 bit giữa là phần tràn NAS, và 8 bit cuối là số trình tự.

Thông tin kênh mang (BEARER) bao gồm 5 bit, và 5 bit toàn 0.

Hướng truyền dữ liệu (DIRECTION) được sử dụng để chỉ báo UL hoặc DL. Khi mật mã hóa và giải mật mã được thực hiện trên thông điệp NAS UL, DIRECTION chỉ báo UL. Khi mật mã hóa và giải mật mã được thực hiện trên thông điệp NAS DL, DIRECTION chỉ báo DL.

Độ dài (LENGTH) được sử dụng để chỉ báo độ dài dữ liệu của thông điệp NAS cần được mật mã hóa hoặc giải mật mã.

Thuật toán mật mã hóa hệ thống gói tiến hóa (evolved packet system encryption algorithm, EEA) có thể được gọi là thuật toán mật mã hóa EPS, và là thuật toán được sử dụng để mật mã hóa và giải mật mã thông điệp NAS.

Quá trình mật mã hóa như sau: thực hiện xử lý EEA trên các tham số đầu vào (KEY, COUNT, BEARER, DIRECTION, và LENGTH), để thu được dòng khóa (keystream); và thực hiện phép cộng modulo 2 trên dòng khóa và văn bản gốc (thông điệp NAS), để thu được văn bản mã hóa (ciphertext). Quá trình giải mật mã như sau: thực hiện xử lý EEA trên các tham số đầu vào nêu trên, để thu được dòng khóa; và thực hiện phép cộng modulo 2 trên dòng khóa và văn bản mật mã hóa, để khôi phục văn bản gốc.

(3) Bảo vệ tính toàn vẹn

Fig.4 thể hiện quá trình thực hiện bảo vệ tính toàn vẹn và kiểm chứng bảo vệ tính toàn vẹn trên thông điệp NAS.

Thông điệp (MESSAGE) là thông điệp mà trên đó bảo vệ tính toàn vẹn cần được thực hiện, và có thể cụ thể là thông điệp NAS.

Thuật toán toàn vẹn hệ thống gói tiến hóa (evolved packet system integrity algorithm, EPS integrity algorithm) được thể hiện trên Fig.4.

Phương pháp bảo vệ tính toàn vẹn như sau: Đầu truyền thực hiện xử lý EIA trên các tham số đầu vào (KEY, COUNT, MESSAGE, BEARER, và DIRECTION) để thu được mã xác thực thông điệp mong đợi cho tính toàn vẹn (message authentication code integrity, MAC-I) hoặc NAS-MAC. Phương pháp kiểm chứng bảo vệ tính toàn vẹn như sau: thực hiện xử lý EIA trên các tham số đầu vào (KEY, COUNT, MESSAGE, BEARER, và DIRECTION), để thu được mã xác thực thông điệp mong đợi cho tính toàn vẹn (expected message authentication code integrity, XMAC-I) hoặc XNAS-MAC; so sánh tiếp XMAC-I với MAC-I; và nếu XMAC-I nhất quán với MAC-I, xác định rằng kiểm chứng bảo vệ tính toàn vẹn thành công.

Phần sau mô tả chi tiết các giải pháp kỹ thuật theo sáng chế.

Dựa trên các kiến trúc mạng trên Fig.1 và Fig.2, phương án thực hiện sáng chế đề xuất phương pháp bảo vệ bảo mật. Ở phương pháp này, đối với quá trình mật mã hóa, giải mật mã, và bảo vệ tính toàn vẹn, tham khảo các phần mô tả trên Fig.3 và Fig.4. Như được thể hiện trên Fig.5, phương pháp chủ yếu bao gồm bước 501 và bước 502.

Bước 501: Thiết bị đầu cuối xác định tham số thứ nhất.

Tham số thứ nhất là tham số đầu vào được sử dụng khi thiết bị đầu cuối thực hiện bảo vệ bảo mật trên thông điệp NAS, và tham số thứ nhất được sử dụng để chỉ báo công nghệ truy nhập được sử dụng để truyền thông điệp NAS. Thiết bị đầu cuối có thể hỗ trợ ít nhất hai công nghệ truy nhập, và có thể duy trì riêng rẽ số đếm NAS tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập. Chẳng hạn, ít nhất hai công nghệ truy nhập bao gồm công nghệ truy nhập 3GPP và công nghệ truy nhập khác nhau mà có thể chia sẻ thiết bị mạng lõi mạng 3GPP tương tự với công nghệ truy nhập 3GPP, chẳng hạn, công nghệ truy nhập phi

3GPP hoặc công nghệ truy nhập mạng cố định. Một cách tùy chọn, việc tham số thứ nhất chỉ báo công nghệ truy nhập được sử dụng để truyền thông điệp NAS có thể nên được hiểu rằng tham số thứ nhất được sử dụng để chỉ báo đường truyền được sử dụng bởi thiết bị đầu cuối để truyền thông điệp NAS. Chẳng hạn, thiết bị đầu cuối và nút AMF có thể duy trì riêng rẽ số đếm NAS tương ứng cho mỗi đường truyền mà không phân biệt các công nghệ truy nhập. Nếu đường truyền được sử dụng để truyền thông điệp NAS là tuyến 1, số đếm NAS tương ứng với tuyến 1 được sử dụng. Nếu đường truyền được sử dụng để truyền thông điệp NAS là tuyến 2, số đếm NAS tương ứng với tuyến 2 được sử dụng. Có thể hiểu rằng đường truyền tương ứng với công nghệ truy nhập. Chẳng hạn, dựa vào Fig.2, công nghệ truy nhập được sử dụng khi dữ liệu được truyền trên tuyến 1 là công nghệ truy nhập 3GPP, và công nghệ truy nhập được sử dụng khi dữ liệu được truyền trên tuyến 2 là công nghệ truy nhập phi 3GPP.

Tham số thứ nhất có thể là tham số đầu vào mới được thêm vào trong quá trình mật mã hóa và giải mật mã hoặc quá trình bảo vệ tính toàn vẹn. Tham số này bao gồm số lượng bit định trước. Một cách tùy chọn, các công nghệ truy nhập khác nhau có thể được biểu diễn bằng cách gán cho các bit bằng các giá trị khác nhau.

Theo triển khai khả thi thứ nhất, như được thể hiện trên Fig.6, tham số thứ nhất có thể là tham số ACCESS. Chẳng hạn, nếu tham số thứ nhất bằng 00, chỉ báo rằng công nghệ truy nhập 3GPP được sử dụng; nếu tham số thứ nhất bằng 01, chỉ báo rằng công nghệ truy nhập phi 3GPP được sử dụng. Theo cách khác, 001 biểu diễn công nghệ truy nhập 3GPP, 010 biểu diễn công nghệ WiFi, và 011 biểu diễn công nghệ mạng cố định.

Theo cách khác, 001 có thể được sử dụng để biểu diễn công nghệ truy nhập được sử dụng thứ nhất, 010 có thể được sử dụng để biểu diễn công nghệ truy nhập được sử dụng thứ hai, và 011 có thể được sử dụng để biểu diễn công nghệ truy nhập được sử dụng thứ ba. Nói cách khác, mỗi lần công nghệ truy nhập được sử dụng được chuyển đổi, tham số thứ nhất được tăng lên 1 cho đến khi các bit của tham số thứ nhất đều là 1, và sau đó tham số thứ nhất có thể được đếm lại từ 000. Chẳng hạn, nếu các bit của tham số thứ nhất đều được đổi sang 1 sau khi

thiết bị đầu cuối chuyển đổi công nghệ truy nhập được sử dụng nhiều lần, khi thiết bị đầu cuối cần chuyển đổi công nghệ truy nhập được sử dụng từ công nghệ truy nhập thứ nhất sang công nghệ truy nhập thứ hai, tham số thứ nhất được tạo cho công nghệ truy nhập thứ hai bằng 001. Một cách tùy chọn, ở phương pháp này, công nghệ truy nhập thứ nhất, công nghệ truy nhập thứ hai, và công nghệ truy nhập thứ ba có thể là cùng công nghệ. Nói cách khác, khi công nghệ truy nhập được tận dụng lại, tham số thứ nhất được tăng lên 1 cho đến khi các bit của tham số thứ nhất đều là 1, và sau đó tham số thứ nhất có thể được đếm lại từ 000.

Một cách tùy chọn, mỗi lần tham số này COUNT trong các tham số đầu vào được đặt lại bằng 0 hoặc số chuỗi NAS được đặt lại bằng 0, tham số thứ nhất có thể cũng được tăng lên 1.

Một cách tùy chọn, khi các bit của tham số thứ nhất đều bằng 1, khóa NAS được sử dụng khi thông điệp NAS được truyền cho lần tiếp theo cần được cập nhật.

Theo triển khai khả thi thứ hai, như được thể hiện trên Fig.7, tất cả hoặc một số bit của tham số này COUNT trong các tham số đầu vào có thể được sử dụng để chỉ báo công nghệ truy nhập được sử dụng để truyền thông điệp NAS. Chẳng hạn, nếu COUNT bao gồm 8 bit đệm toàn 0 và số đếm NAS, tham số thứ nhất có thể là một số hoặc tất cả các bit của cả 8 bit. Chẳng hạn, 3 bit đầu có thể được chọn để chỉ báo công nghệ truy nhập được sử dụng để truyền thông điệp NAS. Đối với cách thức phân biệt các công nghệ truy nhập khác nhau bằng các giá trị bit, tham khảo các phần mô tả liên quan theo triển khai thứ nhất.

Theo triển khai khả thi thứ ba, như được thể hiện trên Fig.8, tham số này BEARER trong các tham số đầu vào có thể được sử dụng để chỉ báo công nghệ truy nhập được sử dụng để truyền thông điệp NAS, hoặc để chỉ báo tuyến truy nhập được sử dụng để truyền thông điệp NAS, trong đó tham số thứ nhất có thể là một số hoặc tất cả các bit của BEARER. Chẳng hạn, 3 bit đầu có thể được chọn để chỉ báo công nghệ truy nhập được sử dụng để truyền thông điệp NAS. Đối với cách thức phân biệt các công nghệ truy nhập khác nhau bằng các giá trị bit, tham khảo các phần mô tả liên quan theo triển khai thứ nhất.

Theo triển khai khả thi thứ tư, số lượng bit của COUNT có thể được tăng lên,

và tham số thứ nhất là một số bit của COUNT. Chẳng hạn, COUNT được mở rộng từ 32 bit sang 64 bit (COUNT 64-bit được làm thích ứng với khóa có độ dài 256 bit). Một phần của COUNT mở rộng được sử dụng để chỉ báo công nghệ truy nhập. Chẳng hạn, ba bit được dành riêng để chỉ báo công nghệ truy nhập, trong đó 000 biểu diễn công nghệ truy nhập 3GPP, 001 biểu diễn công nghệ truy nhập WiFi, và 010 biểu diễn công nghệ truy nhập mạng cố định.

Theo triển khai khả thi thứ năm, tham số thứ nhất có thể là số đếm NAS, và bit của số đếm NAS có thể được loại bỏ. Số lượng bit được loại bỏ được sử dụng để chỉ báo công nghệ truy nhập.

Một cách tùy chọn, số lượng bit định trước của phần tràn NAS trong số đếm NAS hiện có được loại bỏ, và số lượng bit được loại bỏ được sử dụng để chỉ báo công nghệ truy nhập. Chẳng hạn, nếu một bit được loại bỏ, chỉ báo rằng công nghệ truy nhập là công nghệ truy nhập 3GPP; nếu hai bit được loại bỏ, chỉ báo rằng công nghệ truy nhập là công nghệ truy nhập WiFi; nếu ba bit được loại bỏ, chỉ báo rằng công nghệ truy nhập là công nghệ truy nhập mạng cố định.

Theo cách khác, số lượng bit định trước của phần số trình tự của số đếm NAS hiện có được loại bỏ, và số lượng bit được loại bỏ được sử dụng để chỉ báo công nghệ truy nhập. Chẳng hạn, nếu một bit được loại bỏ, chỉ báo rằng công nghệ truy nhập là công nghệ truy nhập 3GPP; nếu hai bit được loại bỏ, chỉ báo rằng công nghệ truy nhập là công nghệ truy nhập WiFi; nếu ba bit được loại bỏ, chỉ báo rằng công nghệ truy nhập là công nghệ truy nhập mạng cố định.

Một cách tùy chọn, tham số thứ nhất tương ứng với mỗi công nghệ truy nhập có thể được tiền cấu hình trong thiết bị đầu cuối. Sau khi xác định công nghệ truy nhập được sử dụng để truyền thông điệp NAS, thiết bị đầu cuối có thể tìm kiếm tham số thứ nhất tương ứng dựa trên công nghệ truy nhập được sử dụng để truyền thông điệp NAS; hoặc sau khi xác định công nghệ truy nhập được sử dụng để truyền thông điệp NAS, thiết bị đầu cuối tạo tham số thứ nhất dựa trên công nghệ truy nhập được sử dụng để truyền thông điệp NAS.

Nên lưu ý rằng, khi tham số thứ nhất là số đếm NAS hoặc tham số thứ nhất là một số bit của số đếm NAS, thiết bị đầu cuối duy trì các số đếm NAS khác nhau cho các công nghệ truy nhập được hỗ trợ khác nhau. Trong các trường hợp

khác, thiết bị đầu cuối có thể duy trì số đếm NAS tương tự hoặc số đếm NAS khác nhau cho các công nghệ truy nhập được hỗ trợ khác nhau.

Thiết bị đầu cuối có thể độc lập xác định tham số thứ nhất, và thông báo nút AMF về tham số thứ nhất. Theo cách khác, nút AMF xác định tham số thứ nhất, và thông báo thiết bị đầu cuối về tham số thứ nhất. Theo cách khác, tham số thứ nhất có thể được tiền cấu hình trong thiết bị đầu cuối và nút AMF. Chẳng hạn, nếu tham số thứ nhất được xác định bởi nút AMF, thiết bị đầu cuối có thể nhận tham số thứ nhất từ nút AMF. Nếu tham số thứ nhất là một số bit trong số đếm NAS, sau khi nhận tham số thứ nhất, thiết bị đầu cuối có thể thay thế, bằng tham số thứ nhất, các bit được xác định trong số đếm NAS được lưu trữ bởi thiết bị đầu cuối. Theo cách khác, nếu tham số thứ nhất là một số bit trong BEARER, thiết bị đầu cuối có thể thay thế các bit được xác định trong BEARER bằng tham số thứ nhất.

Bước 502: Thiết bị đầu cuối thực hiện bảo vệ bảo mật trên thông điệp NAS dựa trên tham số thứ nhất, khóa NAS, và số đếm NAS tương ứng với công nghệ truy nhập được sử dụng để truyền thông điệp NAS.

Số đếm NAS có thể là tham số có chức năng ngăn ngừa tấn công phát lại thông điệp NAS. Khóa NAS là khóa NAS được chia sẻ bởi ít nhất hai công nghệ truy nhập mà có thể được hỗ trợ bởi thiết bị đầu cuối.

Việc thiết bị đầu cuối thực hiện bảo vệ bảo mật trên thông điệp NAS chỉ báo: mật mã hóa thông điệp NAS cần được truyền đến thiết bị mạng lõi, giải mật mã thông điệp NAS được nhận, và thực hiện bảo vệ tính toàn vẹn trên thông điệp NAS cần được truyền đến thiết bị mạng lõi, hoặc thực hiện kiểm chứng bảo vệ tính toàn vẹn trên thông điệp NAS được nhận. Một cách tương ứng, khóa được sử dụng để thực hiện bảo vệ bảo mật trên thông điệp NAS có thể là khóa mật mã hóa và khóa bảo vệ tính toàn vẹn. Theo phương án thực hiện sáng chế, khóa mật mã hóa và khóa bảo vệ tính toàn vẹn được gọi chung là các khóa NAS. Trình tự thực thi mật mã hóa, giải mật mã, bảo vệ tính toàn vẹn sản xuất, và kiểm chứng bảo vệ tính toàn vẹn không bị giới hạn ở phương án thực hiện sáng chế.

Có thể hiểu rằng thiết bị đầu cuối có thể duy trì số đếm NAS tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập. Nếu thiết bị đầu cuối truyền

thông điệp NAS bằng công nghệ truy nhập 3GPP, bảo vệ bảo mật được thực hiện trên thông điệp NAS bằng tham số thứ nhất tương ứng với công nghệ truy nhập 3GPP, số đếm NAS UL được duy trì bởi thiết bị đầu cuối cho công nghệ truy nhập 3GPP, và khóa NAS.

Tương ứng với ba triển khai của tham số thứ nhất, các phương pháp mật mã hóa thông điệp NAS được thể hiện riêng rẽ trên Fig.6, Fig.7, và Fig.8.

Tương ứng với triển khai thứ nhất nêu trên, dựa vào Fig.4, tham số đầu vào được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS có thể cũng là truy nhập.

Tương ứng với triển khai thứ hai nêu trên, dựa vào Fig.4, COUNT trong tham số đầu vào được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS bao gồm tham số thứ nhất.

Tương ứng với triển khai thứ ba nêu trên, dựa vào Fig.4, BEARER trong tham số đầu vào được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS bao gồm tham số thứ nhất.

Một cách tùy chọn, nếu thiết bị đầu cuối nhận thông điệp NAS, thiết bị đầu cuối có thể xác định tham số thứ nhất tương ứng với công nghệ truy nhập được sử dụng để truyền thông điệp NAS, để giải mật mã và/hoặc thực hiện kiểm chứng bảo vệ tính toàn vẹn trên thông điệp NAS bằng số đếm NAS DL được mang trong thông điệp NAS, tham số thứ nhất tương ứng với công nghệ truy nhập được sử dụng để truyền thông điệp NAS, và khóa NAS.

Theo phương pháp bảo vệ bảo mật theo phương án thực hiện sáng chế, thiết bị đầu cuối có thể duy trì riêng rẽ số đếm NAS tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập. Thiết bị đầu cuối không sử dụng một tập hợp của các số đếm NAS khi truyền thông điệp NAS bằng các công nghệ truy nhập khác nhau. Thay vào đó, thiết bị đầu cuối thực hiện bảo vệ bảo mật trên thông điệp NAS bằng số đếm NAS được duy trì cho công nghệ truy nhập tương ứng. Điều này có thể tránh vấn đề tấn công phát lại mà xảy ra khi thiết bị mạng lỗi nhận trước số đếm NAS tương đối nhỏ được truyền bằng liên kết, và nhận sau số đếm NAS tương đối lớn được truyền bằng liên kết khác. Theo sáng chế, tham số thứ nhất được sử dụng để phân biệt các công nghệ truy nhập khác

nhau còn được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS. Do vậy, mặc dù khóa NAS tương tự và số đếm NAS tương tự được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS được truyền bằng các công nghệ truy nhập khác nhau, các kết quả bảo vệ bảo mật của thông điệp NAS là khác nhau, giảm khả năng xuất hiện tấn công phát lại, nhờ đó triển khai bảo vệ bảo mật cho các liên kết kết nối NAS.

Tương ứng với phương án thực hiện trên Fig.5, phương pháp thực hiện bảo vệ bảo mật trên thông điệp NAS bởi thiết bị mạng lõi còn được đề xuất theo triển khai khác của phương án thực hiện sáng chế. Thiết bị mạng lõi có thể là nút AMF, nút SEAF, nút MME, nút tham gia vào quá trình xác thực của thiết bị đầu cuối, hoặc nút khác liên quan đến tạo khóa và lưu trữ khóa. Theo phương án thực hiện sáng chế, việc thiết bị mạng lõi là nút AMF được sử dụng làm ví dụ. Như được thể hiện trên Fig.9, phương pháp bao gồm các bước sau.

Bước 901: Nút AMF xác định tham số thứ nhất.

Tham số thứ nhất được sử dụng để chỉ báo công nghệ truy nhập được sử dụng để truyền thông điệp NAS. Nút AMF có thể duy trì riêng rẽ số đếm NAS tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập được hỗ trợ bởi thiết bị đầu cuối.

Phương pháp xác định tham số thứ nhất bởi nút AMF giống như phương pháp xác định tham số thứ nhất bởi thiết bị đầu cuối ở bước 501 trên Fig.5, và có thể thực hiện tham khảo mô tả liên quan ở bước 501.

Bước 902: Nút AMF thực hiện bảo vệ bảo mật trên thông điệp NAS dựa trên tham số thứ nhất, khóa NAS, và số đếm NAS tương ứng với công nghệ truy nhập được sử dụng để truyền thông điệp NAS.

Số đếm NAS có thể là tham số có chức năng ngăn ngừa tấn công phát lại thông điệp NAS.

Việc nút AMF thực hiện bảo vệ bảo mật trên thông điệp NAS có thể là: mật mã hóa thông điệp NAS cần được truyền đến thiết bị đầu cuối, giải mật mã thông điệp NAS được nhận, và thực hiện bảo vệ tính toàn vẹn trên thông điệp NAS cần được truyền đến thiết bị đầu cuối, hoặc thực hiện kiểm chứng bảo vệ tính toàn vẹn trên thông điệp NAS được nhận.

Phương pháp thực hiện bảo vệ bảo mật trên thông điệp NAS bằng nút AMF giống như phương pháp thực hiện bảo vệ bảo mật trên thông điệp NAS bởi thiết bị đầu cuối ở bước 502, và có thể tham khảo mô tả liên quan ở bước 502.

Theo phương pháp bảo vệ bảo mật theo phương án thực hiện sáng chế, thiết bị mạng lõi có thể duy trì riêng rẽ số đếm NAS tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập. Thiết bị đầu cuối không sử dụng một tập hợp của các số đếm NAS khi truyền thông điệp NAS bằng các công nghệ truy nhập khác nhau. Thay vào đó, thiết bị đầu cuối thực hiện bảo vệ bảo mật trên thông điệp NAS bằng số đếm NAS được duy trì cho công nghệ truy nhập tương ứng. Điều này có thể tránh vấn đề tấn công phát lại mà xảy ra khi thiết bị mạng lõi nhận trước số đếm NAS tương đối nhỏ được truyền bằng một liên kết, và sau đó nhận số đếm NAS tương đối lớn được truyền bằng liên kết khác. Theo sáng chế, tham số thứ nhất được sử dụng để phân biệt các công nghệ truy nhập khác nhau còn được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS. Do vậy, mặc dù khóa NAS tương tự và số đếm NAS tương tự được sử dụng khi bảo vệ bảo mật được thực hiện trên thông điệp NAS được truyền bằng các công nghệ truy nhập khác nhau, các kết quả bảo vệ bảo mật của thông điệp NAS là khác nhau, giảm khả năng xuất hiện tấn công phát lại, nhờ đó triển khai bảo vệ bảo mật cho các liên kết kết nối NAS.

Một cách tùy chọn, nếu công nghệ truy nhập được sử dụng để truyền thông điệp NAS là công nghệ truy nhập thứ nhất, trước các thủ tục trên Fig.5 và Fig.9, như được thể hiện trên Fig.10, phương pháp có thể còn bao gồm bước 1001 đến bước 1007.

Bước 1001: Thiết bị đầu cuối xác định số đếm NAS liên kết lên thứ nhất tương ứng với công nghệ truy nhập thứ nhất.

Số đếm NAS liên kết lên thứ nhất bằng 0, và cụ thể là, tất cả hoặc một số bit của số đếm NAS liên kết lên thứ nhất bằng 0.

Theo cách khác, số đếm NAS liên kết lên thứ nhất là số ngẫu nhiên. Cụ thể là, một số hoặc tất cả các bit trong số đếm NAS liên kết lên thứ nhất là các số ngẫu nhiên. Chẳng hạn, phần số trình tự hoặc phần tràn NAS của số đếm NAS liên kết lên thứ nhất là số ngẫu nhiên. Trong trường hợp này, phần còn lại bằng

0.

Theo cách khác, ít nhất hai công nghệ truy nhập còn bao gồm công nghệ truy nhập thứ hai, và số đếm NAS liên kết lên thứ nhất là số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS liên kết lên thứ nhất là số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối.

Theo cách khác, ít nhất hai công nghệ truy nhập còn bao gồm a công nghệ truy nhập thứ hai, và số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối.

Theo cách khác, số đếm NAS liên kết lên thứ nhất là số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS liên kết lên thứ nhất là số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối.

Theo cách khác, số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị đầu cuối.

Một cách tùy chọn, công nghệ truy nhập thứ nhất và công nghệ truy nhập thứ hai có thể riêng rẽ là công nghệ truy nhập 3GPP, công nghệ truy nhập phi 3GPP, công nghệ truy nhập mạng cố định, công nghệ khác có thể được sử dụng để truy nhập thiết bị mạng lõi, hoặc công nghệ bất kỳ mà có thể chia sẻ thiết bị mạng lõi mạng 3GPP với công nghệ truy nhập 3GPP. Theo phương án thực hiện sáng chế, ví dụ trong đó công nghệ truy nhập thứ nhất là công nghệ truy nhập phi 3GPP,

và công nghệ truy nhập thứ hai là công nghệ truy nhập 3GPP được sử dụng để mô tả.

Có thể hiểu rằng, trước khi thiết bị đầu cuối gửi thông điệp NAS đến nút AMF qua công nghệ truy nhập phi 3GPP, thiết bị đầu cuối cần xác định số đếm NAS liên kết lên thứ nhất được mang khi thông điệp NAS được truyền qua công nghệ truy nhập phi 3GPP.

Nếu thiết bị đầu cuối truy nhập nút AMF bằng cách sử dụng công nghệ truy nhập phi 3GPP lần thứ nhất, số đếm NAS liên kết lên thứ nhất tương ứng với công nghệ truy nhập phi 3GPP có thể được gán bằng 0 hoặc số ngẫu nhiên. Theo cách khác, khi thiết bị đầu cuối đã được truy nhập nút AMF qua công nghệ truy nhập 3GPP, nếu phương pháp duy trì số đếm NAS là phương pháp 1 được nêu trên (sau khi thông điệp NAS được gửi, số đếm NAS được sử dụng trong thông điệp NAS được tăng lên 1 và được lưu trữ; và khi thông điệp NAS cần được gửi cho lần tiếp theo, bảo vệ bảo mật được thực hiện trên thông điệp NAS bằng số đếm NAS lưu trữ), có thể được xác định rằng số đếm NAS liên kết lên thứ nhất là số đếm NAS UL tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập 3GPP và thiết bị đầu cuối không thể xác định số đếm NAS UL được sử dụng bằng thông điệp NAS trước đó, số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi thiết bị đầu cuối được chọn, và bảo vệ bảo mật được thực hiện trên thông điệp NAS. Nếu phương pháp duy trì số đếm NAS là phương pháp 2 được nêu trên (sau khi thông điệp NAS được gửi, khi thông điệp NAS cần được gửi cho lần tiếp theo, số đếm NAS lưu trữ được tăng lên 1 để xác định số đếm NAS mới, và bảo vệ bảo mật được thực hiện trên thông điệp NAS bằng số đếm NAS mới), có thể được xác định rằng số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi thiết bị đầu cuối. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập 3GPP và thiết bị đầu cuối không thể xác định số đếm NAS UL được sử dụng bằng thông điệp NAS trước đó, số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi thiết bị đầu cuối được

chọn và được tăng lên 1, và bảo vệ bảo mật được thực hiện trên thông điệp NAS bằng số đếm NAS UL được tăng lên 1.

Khi thiết bị đầu cuối đã được truy nhập nút AMF qua công nghệ truy nhập phi 3GPP, nếu phương pháp duy trì số đếm NAS là phương pháp 1 nêu trên, có thể được xác định rằng số đếm NAS liên kết lên thứ nhất là số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi thiết bị đầu cuối; hoặc nếu phương pháp duy trì số đếm NAS là phương pháp 2 nêu trên, có thể được xác định rằng số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi thiết bị đầu cuối.

Bước 1002: Thiết bị đầu cuối gửi thông điệp thứ nhất đến nút AMF, trong đó thông điệp thứ nhất mang một số hoặc tất cả các bit của số đếm NAS liên kết lên thứ nhất.

Bảo vệ bảo mật được thực hiện trên thông điệp thứ nhất bằng số đếm NAS liên kết lên thứ nhất và khóa NAS. Một cách tùy chọn, thông điệp thứ nhất có thể mang COUNT UL thứ nhất 24 bit, hoặc có thể mang chỉ một số bit của COUNT UL thứ nhất, chẳng hạn, chỉ mang 4 hoặc 8 bit cuối cùng của số đếm NAS liên kết lên thứ nhất.

Theo triển khai khả thi khác, nếu thiết bị đầu cuối truy nhập, trong lần đầu, nút AMF qua công nghệ truy nhập phi 3GPP, và thiết bị đầu cuối đã được truy nhập nút AMF qua công nghệ truy nhập 3GPP, thiết bị đầu cuối có thể tạm thời không xác định số đếm NAS liên kết lên thứ nhất, và thực hiện bảo vệ bảo mật trước hết trên thông điệp thứ nhất bằng số đếm NAS tương ứng với công nghệ truy nhập phi 3GPP, nói cách khác, bước 1001 và bước 1002 có thể được thay thế bằng bước 1003.

Bước 1003: Thiết bị đầu cuối gửi thông điệp thứ nhất đến nút AMF, trong đó thông điệp thứ nhất mang một số hoặc tất cả các bit của số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai.

Bảo vệ bảo mật được thực hiện trên thông điệp thứ nhất bằng khóa NAS và số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai.

Số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai và được mang

trong thông điệp thứ nhất là một số hoặc tất cả các bit của số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối, hoặc là một số hoặc tất cả các bit của số đếm NAS mới UL thu được sau số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối được tăng lên 1. Nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS UL tương ứng với công nghệ truy nhập thứ hai ở bước này là số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị đầu cuối.

Nên lưu ý rằng, một cách tùy chọn, thông điệp thứ nhất ở bước 1002 và ở bước 1003 đều bao gồm thông tin chỉ báo thứ nhất, trong đó thông tin chỉ báo thứ nhất được sử dụng để chỉ báo công nghệ truy nhập tương ứng với một số hoặc tất cả các bit của số đếm NAS UL được mang trong thông điệp thứ nhất, hoặc thông tin chỉ báo thứ nhất được sử dụng để chỉ báo đường truyền tương ứng với một số hoặc tất cả các bit của số đếm NAS được mang trong thông điệp thứ nhất. Chẳng hạn, thông tin chỉ báo thứ nhất được mang trong thông điệp thứ nhất ở bước 1002 chỉ báo công nghệ truy nhập phi 3GPP, và thông tin chỉ báo thứ nhất được mang trong thông điệp thứ nhất ở bước 1003 chỉ báo công nghệ truy nhập 3GPP. Lấy ví dụ khác, thông tin chỉ báo thứ nhất được mang trong thông điệp thứ nhất ở bước 1002 chỉ báo truy nhập nút AMF qua tuyến 1, và thông tin chỉ báo thứ nhất được mang trong thông điệp thứ nhất ở bước 1003 chỉ báo truy nhập nút AMF qua tuyến 2.

Các bước sau có thể được thực hiện tiếp sau bước 1002 hoặc bước 1003.

Bước 1004: Nút AMF nhận thông điệp thứ nhất.

Bước 1005: Nút AMF kiểm chứng, dựa trên số đếm NAS UL tương ứng với công nghệ truy nhập được chỉ báo bởi thông tin chỉ báo thứ nhất, số đếm NAS được mang trong thông điệp thứ nhất.

Thông tin chỉ báo có thể là chỉ báo tường minh, hoặc có thể là thông báo ngầm. Chẳng hạn, thông tin loại truy nhập có thể là thông tin chỉ báo loại truy nhập (chẳng hạn loại truy nhập của loại công nghệ truy nhập vô tuyến (Random Access Technology, RAT)) mà được chỉ báo ngầm trong thông điệp N2, hoặc là thông tin chỉ báo loại truy nhập mà được bổ sung trong thông điệp NAS. Nút

AMF có thể xác định loại truy nhập dựa trên nguồn của thông điệp thứ nhất khi không có thông tin chỉ báo loại truy nhập. Chẳng hạn, nếu địa chỉ nguồn của thông điệp là BS, loại truy nhập là truy nhập 3GPP; nếu địa chỉ nguồn của thông điệp là nút N3IWF, loại truy nhập là truy nhập phi 3GPP; nếu địa chỉ nguồn của thông điệp là thiết bị được kết nối với mạng cố định, loại truy nhập là truy nhập mạng cố định.

Khi thông tin chỉ báo thứ nhất chỉ báo công nghệ truy nhập phi 3GPP, nếu thông điệp thứ nhất mang số đếm NAS thứ nhất hoàn chỉnh và nút AMF xác định rằng thiết bị đầu cuối đã truy nhập nút AMF, nút AMF xác định liệu số đếm NAS thứ nhất lớn hơn số đếm NAS được nhận trước đó UL tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bằng nút AMF. Nếu số đếm NAS thứ nhất lớn hơn số đếm NAS được nhận trước đó UL, kiểm chứng thành công; hoặc nếu số đếm NAS thứ nhất nhỏ hơn số đếm NAS được nhận trước đó UL, việc xác thực thất bại, truy nhập của thiết bị đầu cuối bị từ chối, và thiết bị đầu cuối được thông báo về nguyên nhân thất bại. Một cách tùy chọn, nếu nút AMF xác định rằng thiết bị đầu cuối đã không truy nhập nút AMF bằng công nghệ truy nhập phi 3GPP, nút AMF lưu trữ số đếm NAS thứ nhất dưới dạng số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP, hoặc nút AMF xác định rằng số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP bằng 0. Nếu thông điệp thứ nhất mang một phần số đếm NAS thứ nhất, nút AMF trước hết khôi phục toàn bộ số đếm NAS thứ nhất, và sau đó kiểm chứng hoặc lưu lại số đếm NAS thứ nhất theo phương pháp nêu trên để xử lý số đếm NAS thứ nhất.

Khi thông tin chỉ báo thứ nhất chỉ báo công nghệ truy nhập 3GPP, nếu thông điệp thứ nhất mang toàn bộ số đếm NAS tương ứng với công nghệ truy nhập 3GPP, nút AMF xác định liệu số đếm NAS thứ nhất lớn hơn số đếm NAS được nhận trước đó UL tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bằng nút AMF. Nếu số đếm NAS thứ nhất lớn hơn số đếm NAS được nhận trước đó UL, kiểm chứng thành công; hoặc nếu số đếm NAS thứ nhất nhỏ hơn số đếm NAS được nhận trước đó UL, việc xác thực thất bại. Nếu thông điệp thứ nhất mang một phần số đếm NAS tương ứng với công nghệ truy nhập 3GPP, nút AMF trước hết khôi phục toàn bộ số đếm NAS, và sau đó kiểm chứng toàn bộ COUNT

được khôi phục bằng phương pháp nêu trên để kiểm chứng số đếm NAS.

Bước 1006: Nút AMF xác định một hoặc cả hai số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập thứ nhất.

Số đếm NAS UL thứ hai bằng 0, và cụ thể là, tất cả hoặc một số bit của số đếm NAS UL thứ hai bằng 0. Theo cách khác, số đếm NAS UL thứ hai là số ngẫu nhiên. Cụ thể là, một số hoặc tất cả các bit in số đếm NAS UL thứ hai là các số ngẫu nhiên. Chẳng hạn, phần số trình tự hoặc phần tràn NAS của số đếm NAS UL thứ hai là số ngẫu nhiên. Trong trường hợp này, phần còn lại bằng 0. Theo cách khác, số đếm NAS UL thứ hai là số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS UL thứ hai là số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS UL thứ hai là số đếm NAS liên kết lên thứ nhất; hoặc số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS liên kết lên thứ nhất.

Một cách tùy chọn, nếu thông điệp thứ nhất được nhận bằng nút AMF mang số đếm NAS liên kết lên thứ nhất, nút AMF có thể xác định rằng số đếm NAS UL thứ hai là số đếm NAS liên kết lên thứ nhất, hoặc việc số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS liên kết lên thứ nhất.

Theo cách khác, nếu thông điệp thứ nhất được nhận bằng nút AMF mang số

đếm NAS liên kết lên thứ nhất, chỉ báo rằng thiết bị đầu cuối đã xác định số đếm NAS tương ứng với công nghệ truy nhập phi 3GPP, và nút AMF có thể không xác định số đếm NAS thứ hai.

Số đếm NAS DL thứ nhất bằng 0, và cụ thể là, tất cả hoặc một số bit của số đếm NAS DL thứ nhất bằng 0.

Theo cách khác, số đếm NAS DL thứ nhất là số ngẫu nhiên. Cụ thể là, một số hoặc tất cả các bit trong số đếm NAS DL thứ nhất là các số ngẫu nhiên. Chẳng hạn, phần số trình tự hoặc phần tràn NAS của số đếm NAS liên kết lên thứ nhất là số ngẫu nhiên. Trong trường hợp này, phần còn lại bằng 0. Theo cách khác, số đếm NAS DL thứ nhất là số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS DL thứ nhất là số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ hai, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ hai và được lưu trữ bởi thiết bị mạng lõi. Theo cách khác, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi. Nếu thiết bị mạng lõi lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập thứ nhất, số đếm NAS DL thứ nhất là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập thứ nhất và được lưu trữ bởi thiết bị mạng lõi.

Một cách tùy chọn, nếu thông điệp thứ nhất được nhận bằng nút AMF mang số đếm NAS tương ứng với công nghệ truy nhập thứ hai, số đếm NAS UL thứ hai được xác định bằng nút AMF có thể giống như số đếm NAS DL thứ nhất.

Bước 1007: Nút AMF gửi thông điệp thứ hai đến thiết bị đầu cuối, trong đó thông điệp thứ hai bao gồm một hoặc cả hai số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập thứ nhất.

Một cách tương ứng, thiết bị đầu cuối nhận thông điệp thứ hai.

Một cách tùy chọn, thông điệp thứ hai mang thông tin chỉ báo thứ hai, và thông tin chỉ báo thứ hai được sử dụng để chỉ báo công nghệ truy nhập tương ứng với số đếm NAS DL thứ nhất được mang trong thông điệp thứ hai. Một cách tùy chọn, thông điệp thứ hai có thể còn mang thông tin chỉ báo được sử dụng để chỉ báo số đếm NAS UL thứ hai được mang trong thông điệp thứ hai. Một cách tùy chọn, thông tin chỉ báo thứ hai được sử dụng để chỉ báo đường truyền tương ứng với số đếm NAS DL thứ nhất được mang trong thông điệp thứ hai. Một cách tùy chọn, thông điệp thứ hai có thể còn mang thông tin chỉ báo mà được sử dụng để chỉ báo đường truyền tương ứng với số đếm NAS UL thứ hai được mang trong thông điệp thứ hai. Có thể hiểu rằng, do thông điệp thứ hai mang số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập thứ nhất, thông tin chỉ báo thứ hai được sử dụng để chỉ báo công nghệ truy nhập thứ nhất. Chẳng hạn, nếu công nghệ truy nhập thứ nhất là công nghệ truy nhập 3GPP, thông tin chỉ báo thứ hai được sử dụng để chỉ báo công nghệ truy nhập 3GPP; nếu công nghệ truy nhập thứ nhất là công nghệ truy nhập phi 3GPP, thông tin chỉ báo thứ hai được sử dụng để chỉ báo công nghệ truy nhập phi 3GPP.

Có thể hiểu rằng, sau khi nhận thông điệp thứ hai, thiết bị đầu cuối có thể lưu lại một hoặc cả hai số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất được mang trong thông điệp thứ hai. Khi thông điệp NAS UL cần được gửi qua mạng phi 3GPP lần tiếp theo, bảo vệ bảo mật có thể được thực hiện trên thông điệp NAS dựa trên số đếm NAS UL thứ hai. Theo cách khác, sau khi nhận thông điệp NAS DL, số đếm NAS DL trong thông điệp NAS được nhận DL có thể được kiểm chứng dựa trên số đếm NAS DL thứ nhất.

Dựa vào kịch bản cụ thể, phần sau mô tả phương pháp bảo vệ bảo mật được mô tả trong các phương án thực hiện nêu trên. Phương án thực hiện sáng chế có thể được áp dụng cho kịch bản trong đó thiết bị đầu cuối đã được truy nhập nút AMF bằng công nghệ truy nhập 3GPP, và sau đó thiết bị đầu cuối truy nhập nút AMF tương tự bằng công nghệ truy nhập phi 3GPP. Fig.11A và Fig.11B thể hiện quá trình đăng ký trong đó thiết bị đầu cuối truy nhập nút AMF bằng công nghệ truy nhập phi 3GPP. Phương pháp bao gồm các bước sau.

Bước 1101: Thiết bị đầu cuối truy nhập mạng phi 3GPP không tín nhiệm.

Chẳng hạn, thiết bị đầu cuối truy nhập mạng WiFi không thể được tín nhiệm trực tiếp.

Ở bước này, thiết bị đầu cuối truy nhập mạng phi 3GPP không tín nhiệm, và thiết bị đầu cuối đã được xác thực bởi mạng 3GPP và có ngữ cảnh bảo mật NAS. Ngữ cảnh bảo mật NAS bao gồm khóa NAS, ID khóa, và số đếm NAS tương ứng với công nghệ truy nhập 3GPP. Một cách tùy chọn, ngữ cảnh NAS còn bao gồm số đếm NAS tương ứng với công nghệ truy nhập phi 3GPP. Nếu thiết bị đầu cuối đã truy nhập nút AMF qua công nghệ truy nhập phi 3GPP, số đếm NAS tương ứng với công nghệ truy nhập phi 3GPP khác 0. Nếu thiết bị đầu cuối đã không truy nhập nút AMF qua công nghệ truy nhập phi 3GPP, số đếm NAS tương ứng với công nghệ truy nhập phi 3GPP bằng 0.

Khóa NAS có thể là một hoặc cả hai khóa mật mã hóa và khóa bảo vệ tính toàn vẹn.

Bước 1102: Thiết bị đầu cuối trao đổi thông điệp liên kết bảo mật giao thức trao đổi khóa Internet ban đầu (internet key exchange protocol security association initial, IKE_SA_INIT) với nút N3IWF.

Thông điệp IKE_SA_INIT mang tài liệu khóa, và tài liệu khóa là thông tin được sử dụng để thực hiện bảo vệ bảo mật trên thông điệp được truyền giữa thiết bị đầu cuối và nút N3IWF. Sau khi thiết bị đầu cuối trao đổi thông điệp IKE_SA_INIT với nút N3IWF, thiết bị đầu cuối và nút N3IWF có thể tạo khóa tương tự, và khóa này được sử dụng để thực hiện bảo vệ bảo mật trên thông điệp được truyền tuần tự bởi thiết bị đầu cuối và nút N3IWF.

Bước 1103: Thiết bị đầu cuối gửi thông điệp yêu cầu xác thực giao thức trao đổi khóa Internet (Internet key exchange protocol authentication request, IKE_AUTH_Req) đến nút N3IWF.

Một cách tương ứng, nút N3IWF nhận thông điệp IKE_AUTH_Req.

Bước 1104: Nút N3IWF gửi thông điệp đáp ứng xác thực giao thức trao đổi khóa Internet (internet key exchange protocol authentication response, IKE_AUTH_Res) đến thiết bị đầu cuối.

Một cách tương ứng, thiết bị đầu cuối nhận thông điệp IKE_AUTH_Res.

Thông điệp IKE_AUTH_Res mang thông điệp khởi động 5G của thông điệp

yêu cầu thể hệ thứ năm giao thức xác thực mở rộng được (extensible authentication protocol_5th generation_request, EAP_5G_Req), và thông điệp EAP_5G_Req được sử dụng để yêu cầu thiết bị đầu cuối khởi tạo thủ tục giao thức xác thực mở rộng được (extensible authentication protocol, EAP).

Bước 1105: Thiết bị đầu cuối xác định số đếm NAS liên kết lên thứ nhất.

Số đếm NAS liên kết lên thứ nhất là COUNT được sử dụng để thực hiện bảo vệ bảo mật trên thông điệp NAS được gửi bởi thiết bị đầu cuối đến nút AMF.

Có hai cách triển khai bước này.

Theo triển khai thứ nhất, thiết bị đầu cuối xác định số đếm NAS liên kết lên thứ nhất dựa trên số đếm NAS UL tương ứng với công nghệ truy nhập 3GPP.

Do thiết bị đầu cuối đã truy nhập nút AMF qua công nghệ truy nhập 3GPP, thiết bị đầu cuối đã lưu trữ số đếm NAS tương ứng với công nghệ truy nhập 3GPP. Nếu phương pháp duy trì số đếm NAS là phương pháp 1 nêu trên, có thể xác định rằng số đếm NAS liên kết lên thứ nhất là số đếm NAS UL tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi thiết bị đầu cuối (nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập 3GPP, số đếm NAS liên kết lên thứ nhất là số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi thiết bị đầu cuối). Nếu phương pháp duy trì số đếm NAS là phương pháp 2 nêu trên, có thể xác định rằng số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi thiết bị đầu cuối (nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP, số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi thiết bị đầu cuối).

Theo triển khai thứ hai, thiết bị đầu cuối tạo số đếm NAS tương ứng với công nghệ truy nhập phi 3GPP, và sử dụng, làm số đếm NAS liên kết lên thứ nhất, số đếm NAS tương ứng với công nghệ truy nhập phi 3GPP.

Cụ thể là, số đếm NAS liên kết lên thứ nhất có thể bằng 0, hoặc có thể là số ngẫu nhiên.

Nếu số đếm NAS liên kết lên thứ nhất bằng 0, tất cả hoặc một số bit của số

đếm NAS liên kết lên thứ nhất bằng 0. Nếu số đếm NAS liên kết lên thứ nhất là số ngẫu nhiên, một số hoặc tất cả các bit trong số đếm NAS liên kết lên thứ nhất là các số ngẫu nhiên. Chẳng hạn, 8 bit cuối (phần số trình tự) của số đếm NAS liên kết lên thứ nhất là các số ngẫu nhiên, hoặc phần tràn NAS là số ngẫu nhiên, và phần còn lại bằng 0.

Một cách tùy chọn, nếu thiết bị đầu cuối đã truy nhập nút AMF qua công nghệ truy nhập phi 3GPP, thiết bị đầu cuối có thể xác định rằng số đếm NAS liên kết lên thứ nhất là số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi thiết bị đầu cuối (nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP, số đếm NAS liên kết lên thứ nhất là số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi thiết bị đầu cuối), hoặc thiết bị đầu cuối có thể xác định rằng số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi thiết bị đầu cuối (nếu thiết bị đầu cuối lưu trữ ít nhất hai số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP, số đếm NAS liên kết lên thứ nhất là tổng của 1 và số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi thiết bị đầu cuối).

Một cách tùy chọn, nếu số đếm NAS liên kết lên thứ nhất được xác định trong triển khai thứ hai, trong quá trình đăng ký trong đó thiết bị đầu cuối truy nhập nút AMF bằng công nghệ truy nhập phi 3GPP, thiết bị đầu cuối không gửi thông điệp NAS bằng công nghệ truy nhập 3GPP.

Một cách tùy chọn, thiết bị đầu cuối có thể thiết lập tiếp bộ chỉ báo. Bộ chỉ báo tương đương với thông tin chỉ báo thứ nhất theo phương án thực hiện tương ứng với Fig.10, và được sử dụng để chỉ báo liệu số đếm NAS liên kết lên thứ nhất tương ứng với công nghệ truy nhập 3GPP hoặc công nghệ truy nhập phi 3GPP. Có thể hiểu rằng, nếu thiết bị đầu cuối xác định số đếm NAS liên kết lên thứ nhất theo triển khai thứ nhất nêu trên, bộ chỉ báo chỉ báo công nghệ truy nhập 3GPP; hoặc nếu thiết bị đầu cuối xác định số đếm NAS liên kết lên thứ nhất theo triển khai thứ hai nêu trên, bộ chỉ báo chỉ báo công nghệ truy nhập phi 3GPP.

Bước 1106: Thiết bị đầu cuối gửi thông điệp IKE_AUTH_Req đến nút

N3IWF.

Một cách tương ứng, nút N3IWF nhận thông điệp IKE_AUTH_Req.

Thông điệp IKE_AUTH Req bao gồm khối dữ liệu giao thức (protocol data unit, PDU) NAS và EAP để vận chuyển thông điệp NAS 5G (thông điệp NAS 5G tương ứng với thông điệp EAP_5G_ReS), hoặc thông điệp NAS 5G. NAS PDU bao gồm thông điệp yêu cầu đăng ký. Thông điệp yêu cầu đăng ký được sử dụng bởi thiết bị đầu cuối để đăng ký với nút AMF qua công nghệ truy nhập 3GPP. Một cách tùy chọn, thông điệp thứ nhất theo phương án thực hiện nêu trên có thể là thông điệp yêu cầu đăng ký.

Một cách tùy chọn, bảo vệ tính toàn vẹn có thể được thực hiện trên thông điệp yêu cầu đăng ký bằng số đếm NAS liên kết lên thứ nhất, và thông điệp yêu cầu đăng ký bao gồm thông tin chỉ báo thứ nhất và số đếm NAS liên kết lên thứ nhất. Một cách tùy chọn, thông điệp yêu cầu đăng ký còn bao gồm ID khóa và ID tạm thời của thiết bị đầu cuối.

Bước 1107: Nút N3IWF lựa chọn nút AMF.

Đối với phương pháp lựa chọn nút AMF bằng nút N3IWF, tham khảo giải pháp kỹ thuật đã biết.

Bước 1108: Nút N3IWF chuyển tiếp thông điệp yêu cầu đăng ký đến nút AMF.

Một cách tương ứng, nút AMF nhận thông điệp yêu cầu đăng ký.

Bước 1109: Nút AMF kiểm chứng thông điệp yêu cầu đăng ký.

Việc kiểm chứng được thực hiện trên thông điệp yêu cầu đăng ký bằng nút AMF bao gồm kiểm chứng bảo vệ tính toàn vẹn được thực hiện trên thông điệp yêu cầu đăng ký và kiểm chứng được thực hiện trên số đếm NAS liên kết lên thứ nhất được mang trong thông điệp yêu cầu đăng ký. Việc nút AMF kiểm chứng số đếm NAS liên kết lên thứ nhất được mang trong thông điệp yêu cầu đăng ký tương ứng với bước 1005 nêu trên.

Nút AMF có thể tạo khóa bảo vệ tính toàn vẹn dựa trên ID tạm thời và ID khóa trong thông điệp yêu cầu đăng ký, và thực hiện kiểm chứng bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký dựa trên khóa bảo vệ tính toàn vẹn.

Nếu công nghệ truy nhập tương ứng với thông điệp NAS UL thứ nhất và được

chỉ báo bởi thông tin chỉ báo thứ nhất là công nghệ truy nhập 3GPP, nút AMF kiểm chứng liệu số đếm NAS liên kết lên thứ nhất lớn hơn số đếm NAS được nhận trước đó tương ứng với công nghệ truy nhập 3GPP. Nếu số đếm NAS liên kết lên thứ nhất lớn hơn số đếm NAS được nhận trước đó, kiểm chứng thành công; hoặc nếu số đếm NAS liên kết lên thứ nhất không lớn hơn số đếm NAS được nhận trước đó, kiểm chứng thất bại.

Nếu công nghệ truy nhập tương ứng với thông điệp NAS UL thứ nhất và được chỉ báo bởi thông tin chỉ báo thứ nhất là công nghệ truy nhập phi 3GPP, và thiết bị đầu cuối đã không truy nhập nút AMF qua công nghệ truy nhập phi 3GPP, nút AMF lưu trữ số đếm NAS thứ nhất làm số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP, hoặc nút AMF xác định rằng số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP bằng 0. Thiết bị đầu cuối đã truy nhập nút AMF qua công nghệ truy nhập phi 3GPP. Nút AMF kiểm chứng liệu số đếm NAS liên kết lên thứ nhất lớn hơn số đếm NAS được nhận trước đó tương ứng với công nghệ truy nhập phi 3GPP. Nếu số đếm NAS liên kết lên thứ nhất lớn hơn số đếm NAS được nhận trước đó, kiểm chứng thành công; hoặc nếu số đếm NAS liên kết lên thứ nhất không lớn hơn số đếm NAS được nhận trước đó, kiểm chứng thất bại.

Bước 1110: Nút AMF tạo khóa Kn3iwf cho nút N3IWF.

Khóa Kn3iwf được sử dụng để xác thực hai chiều giữa nút AMF và thiết bị đầu cuối.

Bước 1111: Nút AMF xác định một hoặc cả hai số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập phi 3GPP.

Một cách tùy chọn, nếu công nghệ truy nhập được chỉ báo bởi thông tin chỉ báo thứ nhất là công nghệ truy nhập 3GPP, chỉ báo rằng thiết bị đầu cuối không xác định số đếm NAS cho công nghệ truy nhập phi 3GPP, và nút AMF có thể xác định số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập phi 3GPP. Nếu công nghệ truy nhập được chỉ báo bởi thông tin chỉ báo thứ nhất là công nghệ truy nhập phi 3GPP, chỉ báo rằng thiết bị đầu cuối xác định số đếm NAS UL cho công nghệ truy nhập phi 3GPP, và nút AMF cần xác định chỉ số đếm NAS DL thứ nhất tương ứng với công nghệ phi 3GPP,

hoặc nút AMF xác định số đếm NAS DL thứ nhất và xác định lại số đếm NAS UL của công nghệ truy nhập phi 3GPP.

Cụ thể là, số đếm NAS UL thứ hai bằng 0, hoặc số đếm NAS UL thứ hai là số ngẫu nhiên.

Nếu số đếm NAS UL thứ hai bằng 0, tất cả hoặc một số bit của số đếm NAS UL thứ hai bằng 0. Nếu số đếm NAS UL thứ hai là số ngẫu nhiên, một số hoặc tất cả các bit trong số đếm NAS UL thứ hai là các số ngẫu nhiên. Chẳng hạn, 8 bit cuối (phần số trình tự) của số đếm NAS UL thứ hai là các số ngẫu nhiên, hoặc phần tràn NAS là số ngẫu nhiên, và phần còn lại bằng 0. Một cách tùy chọn, nếu số đếm NAS UL thứ hai là số ngẫu nhiên, số đếm NAS UL thứ hai cần lớn hơn số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi nút AMF (nếu nút AMF lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP, số đếm NAS UL thứ hai cần lớn hơn số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi nút AMF).

Số đếm NAS UL thứ hai có thể là số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi nút AMF (nếu nút AMF lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP, số đếm NAS UL thứ hai là số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi thiết bị đầu cuối). Theo cách khác, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi nút AMF (nếu nút AMF lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi thiết bị đầu cuối). Theo cách khác, số đếm NAS UL thứ hai có thể là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi nút AMF (nếu nút AMF lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập phi 3GPP, số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi thiết bị đầu cuối). Theo cách khác, số đếm NAS UL thứ hai là số đếm NAS liên kết lên thứ nhất; hoặc số đếm NAS UL thứ hai là tổng của 1 và số đếm NAS liên kết lên thứ nhất.

Một cách tùy chọn, số đếm NAS DL thứ nhất có thể giống như số đếm NAS UL thứ hai.

Cụ thể là, số đếm NAS DL thứ nhất có thể bằng 0, hoặc có thể là số ngẫu nhiên.

Nếu số đếm NAS DL thứ nhất bằng 0, tất cả hoặc một số bit của số đếm NAS DL thứ nhất bằng 0. Nếu số đếm NAS DL thứ nhất là số ngẫu nhiên, một số hoặc tất cả các bit trong số đếm NAS DL thứ nhất là các số ngẫu nhiên. Chẳng hạn, 8 bit cuối (phần số trình tự) của số đếm NAS DL thứ nhất là các số ngẫu nhiên, hoặc phần tràn NAS là số ngẫu nhiên, và phần còn lại bằng 0. Một cách tùy chọn, nếu số đếm NAS DL thứ nhất là số ngẫu nhiên, số đếm NAS DL thứ nhất cần lớn hơn số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi nút AMF.

Theo cách khác, số đếm NAS DL thứ nhất có thể là số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi nút AMF (nếu nút AMF lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP, số đếm NAS DL thứ nhất có thể còn là số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi nút AMF). Theo cách khác, số đếm NAS DL thứ nhất có thể là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi nút AMF (nếu nút AMF lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP, số đếm NAS DL thứ nhất có thể còn là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi nút AMF). Theo cách khác, số đếm NAS DL thứ nhất có thể là tổng của 1 và số đếm NAS DL tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi nút AMF (nếu nút AMF lưu trữ ít nhất hai số đếm NAS DL tương ứng với công nghệ truy nhập phi 3GPP, số đếm NAS DL thứ nhất có thể còn là tổng của 1 và số đếm NAS DL lớn nhất tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi nút AMF).

Nên lưu ý rằng nút AMF có thể chứa một hoặc cả hai số đếm NAS UL thứ hai được tạo và số đếm NAS thứ nhất DL được tạo. Nút AMF có thể duy trì số đếm NAS UL và số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP, và có thể duy trì tiếp số đếm NAS UL và số đếm NAS DL tương ứng với công nghệ

truy nhập phi 3GPP. Nếu nút AMF tạo số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất, nút AMF lưu trữ số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất. Nếu nút AMF tạo chỉ số đếm NAS DL thứ nhất, nút AMF lưu trữ số đếm NAS DL thứ nhất. Trong trường hợp này, số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP và được duy trì bởi thiết bị đầu cuối là số đếm NAS liên kết lên thứ nhất.

Có thể hiểu rằng nút AMF duy trì riêng rẽ tập hợp các số đếm NAS cho mỗi công nghệ trong công nghệ truy nhập 3GPP và công nghệ truy nhập phi 3GPP, nói cách khác, các độ lớn của các số đếm NAS được duy trì bởi nút AMF cho công nghệ truy nhập 3GPP và các độ lớn của các số đếm NAS được duy trì bởi nút AMF cho công nghệ truy nhập phi 3GPP không ảnh hưởng nhau. Khi nhận thông điệp NAS UL, nút AMF có thể xác định, dựa trên thông tin bit trong thông điệp NAS UL hoặc thông tin trong thông điệp N2, công nghệ truy nhập hoặc đường truyền được sử dụng bởi thiết bị đầu cuối để truyền thông điệp NAS UL. Nếu công nghệ truy nhập được sử dụng là công nghệ truy nhập 3GPP, số đếm NAS UL được mang trong thông điệp NAS UL có thể được so sánh với số đếm NAS UL lớn nhất được duy trì cho công nghệ truy nhập 3GPP. Nếu công nghệ truy nhập được sử dụng là công nghệ truy nhập phi 3GPP, số đếm NAS UL được mang trong thông điệp NAS UL có thể được so sánh với số đếm NAS UL lớn nhất được duy trì cho công nghệ truy nhập phi 3GPP, để ngăn ngừa tấn công phát lại.

Bước 1112: Nút AMF gửi thông điệp lệnh chế độ bảo mật NAS (security mode command, SMC) đến thiết bị đầu cuối bằng nút N3IWF.

Một cách tương ứng, thiết bị đầu cuối nhận thông điệp NAS SMC.

Thông điệp thứ hai theo phương án thực hiện nêu trên có thể là thông điệp NAS SMC.

Thông điệp NAS SMC mang một hoặc cả hai số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất. Có thể hiểu rằng nếu nút AMF xác định chỉ số đếm NAS DL thứ nhất, thông điệp NAS SMC mang số đếm NAS DL thứ nhất. Nếu nút AMF xác định số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất, thông điệp NAS SMC mang số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất.

Một cách tùy chọn, nếu thông điệp NAS mang chỉ số đếm NAS DL thứ nhất, thông điệp NAS có thể còn mang thông tin chỉ báo được sử dụng để ra lệnh thiết bị đầu cuối tiếp tục sử dụng số đếm NAS UL được xác định bởi thiết bị đầu cuối.

Một cách tùy chọn, thông điệp NAS SMC còn bao gồm thông tin chỉ báo thứ hai, và thông tin chỉ báo thứ hai được sử dụng để chỉ báo công nghệ truy nhập hoặc đường truyền tương ứng với số đếm NAS được mang trong thông điệp NAS SMC. Trong kịch bản của phương án thực hiện, công nghệ truy nhập được chỉ báo bởi thông tin chỉ báo thứ hai là công nghệ truy nhập phi 3GPP.

Bước 1113: Thiết bị đầu cuối xác định, dựa trên thông điệp NAS SMC, số đếm NAS UL và số đếm NAS DL tương ứng với công nghệ truy nhập phi 3GPP.

Thiết bị đầu cuối có thể duy trì riêng rẽ tập hợp các số đếm NAS cho mỗi công nghệ trong công nghệ truy nhập 3GPP và công nghệ truy nhập phi 3GPP. Trong kịch bản của phương án thực hiện, thiết bị đầu cuối đã số đếm NAS lưu trữ UL và số đếm NAS DL tương ứng với công nghệ truy nhập 3GPP, và thiết bị đầu cuối có thể xác định tiếp, dựa trên thông điệp NAS SMC được nhận ở bước này, số đếm NAS UL và số đếm NAS DL được duy trì cho phi 3GPP.

Một cách tùy chọn, nếu thông điệp NAS SMC bao gồm chỉ số đếm NAS DL thứ nhất, thiết bị đầu cuối xác định rằng số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP vẫn là số đếm NAS liên kết lên thứ nhất, và số đếm NAS DL tương ứng với công nghệ truy nhập phi 3GPP là số đếm NAS DL thứ nhất. Nếu thông điệp NAS SMC bao gồm số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất, thiết bị đầu cuối có thể xác định rằng số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP là số đếm NAS UL thứ hai, và số đếm NAS DL tương ứng với công nghệ truy nhập phi 3GPP là số đếm NAS DL thứ nhất.

Có thể hiểu rằng khi nhận thông điệp NAS DL, thiết bị đầu cuối có thể xác định, dựa trên thông tin bit trong thông điệp NAS DL, công nghệ truy nhập hoặc đường truyền được sử dụng bởi thiết bị đầu cuối để truyền thông điệp NAS DL. Nếu công nghệ truy nhập được sử dụng là công nghệ truy nhập 3GPP, số đếm NAS DL được mang trong thông điệp NAS DL có thể được so sánh với số đếm NAS DL lớn nhất được duy trì cho công nghệ truy nhập 3GPP. Nếu công nghệ

truy nhập được sử dụng là công nghệ truy nhập phi 3GPP, số đếm NAS DL được mang trong thông điệp NAS DL có thể được so sánh với số đếm NAS DL lớn nhất được duy trì cho công nghệ truy nhập phi 3GPP, để ngăn ngừa tấn công phát lại.

Bước 1114: Thiết bị đầu cuối gửi thông điệp hoàn thành chế độ bảo mật NAS (security mode complete, SMP) đến nút AMF bằng nút N3IWF.

Một cách tương ứng, nút AMF nhận thông điệp NAS SMP.

Một cách tùy chọn, thông điệp NAS ở bước 502 có thể là thông điệp NAS SMP ở bước này.

Thiết bị đầu cuối có thể thực hiện bảo vệ tính toàn vẹn trên thông điệp NAS SMP bằng tham số thứ nhất, số đếm NAS UL, và khóa NAS. Tham số thứ nhất được sử dụng để chỉ báo rằng công nghệ truy nhập được sử dụng để truyền thông điệp NAS SMP là công nghệ truy nhập phi 3GPP, hoặc được sử dụng để chỉ báo rằng đường truyền được sử dụng để truyền thông điệp NAS SMP là tuyến 2 trên Fig.2. Số đếm NAS UL là số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP và được xác định bởi thiết bị đầu cuối ở bước 1113, hoặc số đếm NAS UL tương ứng với tuyến 2. Thông điệp NAS SMP mang số đếm NAS UL.

Có thể hiểu rằng sau khi nhận thông điệp NAS SMP, nút AMF có thể kiểm chứng liệu số đếm NAS UL được mang trong thông điệp NAS SMP lớn hơn số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi nút AMF, hoặc liệu số đếm NAS UL được mang trong thông điệp NAS SMP lớn hơn số đếm NAS UL tương ứng với tuyến 2. Nếu số đếm NAS UL được mang trong thông điệp NAS SMP lớn hơn số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi nút AMF, hoặc số đếm NAS UL được mang trong thông điệp NAS SMP lớn hơn số đếm NAS UL tương ứng với tuyến 2, có thể xác định, dựa trên thông tin bit trong thông điệp NAS, rằng công nghệ truy nhập được sử dụng để truyền thông điệp NAS SMP là công nghệ truy nhập phi 3GPP, để xác định tham số thứ nhất tương ứng với công nghệ truy nhập phi 3GPP, và sau đó thực hiện kiểm chứng toàn vẹn trên thông điệp NAS SMP dựa trên tham số thứ nhất, khóa NAS, và số đếm NAS UL được mang trong thông điệp NAS SMP. Nếu kiểm chứng thành công, bước 1115 được thực hiện. Một

cách tùy chọn, nếu AMF lưu trữ các số đếm NAS UL, có thể kiểm chứng liệu số đếm NAS UL được mang trong thông điệp NAS SMP lớn hơn số đếm NAS UL lớn nhất tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi nút AMF.

Bước 1115: Nút AMF gửi thông điệp N2 đến nút N3IWF. Thông điệp N2 mang khóa Kn3iwf và thông điệp hoàn thành đăng ký.

Một cách tương ứng, nút N3IWF nhận thông điệp N2.

Bước 1116: Nút N3IWF gửi thông điệp EAP-5G-Success đến thiết bị đầu cuối.

Một cách tương ứng, thiết bị đầu cuối nhận thông điệp EAP-5G-Success.

Bước 1117: Thiết bị đầu cuối và nút N3IWF hoàn thành tính toán tham số xác thực bằng Kn3iwf.

Bước 1118: Kết nối bảo mật giao thức Internet (Internet protocol security, IPsec) được thiết lập giữa thiết bị đầu cuối và nút N3IWF.

Bước 1119: Nút N3IWF gửi thông điệp hoàn thành đăng ký đến thiết bị đầu cuối.

Theo phương pháp theo phương án thực hiện sáng chế, thiết bị đầu cuối có thể truy nhập mạng qua công nghệ truy nhập phi 3GPP, và có thể độc lập duy trì số đếm NAS của công nghệ truy nhập 3GPP và số đếm NAS của công nghệ truy nhập phi 3GPP, nhờ đó giảm khả năng xuất hiện tấn công phát lại.

Theo triển khai khả thi theo phương án thực hiện sáng chế, ngữ cảnh bảo mật của thiết bị đầu cuối có thể được gắn với thông tin nhà khai thác. Chẳng hạn, thông tin nhà khai thác có thể là ID PLMN. Sau khi thiết bị đầu cuối truy nhập mạng bằng công nghệ truy nhập 3GPP do nhà khai thác A cung cấp, khi thiết bị đầu cuối thực thi thủ tục tương ứng với Fig.11A và Fig.11B, có thể được xác định liệu nút N3IWF tương ứng với công nghệ truy nhập phi 3GPP vẫn là nhà khai thác A. Nếu nút N3IWF vẫn là nhà khai thác A, thủ tục tương ứng với Fig.11A và Fig.11B có thể được tiếp tục.

Theo triển khai khả thi khác, ngữ cảnh bảo mật của thiết bị đầu cuối ở phía công nghệ truy nhập phi 3GPP có thể được gắn với thông tin khác chẳng hạn thông tin thuê bao và thông tin khu vực vị trí. Chẳng hạn, thiết bị đầu cuối di

chuyển từ khoảng phủ sóng của BS A đến khoảng phủ sóng của BS B, khoảng phủ sóng của BS A hỗ trợ công nghệ truy nhập phi 3GPP C, và BS B hỗ trợ công nghệ truy nhập phi 3GPP D. Nếu thiết bị đầu cuối truy nhập mạng qua công nghệ truy nhập phi 3GPP C, khi thiết bị đầu cuối di chuyển từ khoảng phủ sóng của BS A đến khoảng phủ sóng của BS B, nếu thông tin thuê bao của thiết bị đầu cuối chỉ báo rằng thiết bị đầu cuối không có quyền sử dụng công nghệ truy nhập phi 3GPP D, thiết bị đầu cuối không thể truy nhập mạng qua công nghệ truy nhập phi 3GPP D.

Một cách tùy chọn, theo phương án thực hiện nêu trên, nút AMF có thể xác định, dựa trên thông tin chỉ báo thứ nhất, công nghệ truy nhập được sử dụng để truyền thông điệp NAS. Phương án thực hiện sáng chế còn đề xuất ba phương pháp xác định công nghệ truy nhập được sử dụng để truyền thông điệp N2 hoặc thông điệp NAS sau khi nút AMF nhận thông điệp N2.

Phương pháp 1: Nút AMF có thể xác định, dựa trên nguồn của thông điệp N2, công nghệ truy nhập được sử dụng để truyền thông điệp N2. Chẳng hạn, nút AMF xác định nguồn của thông điệp dựa trên thông tin địa chỉ nguồn (chẳng hạn, địa chỉ IP), và xác định thêm, dựa trên nguồn của thông điệp, công nghệ truy nhập được sử dụng để truyền thông điệp. Nếu thông điệp N2 đến từ thiết bị qua công nghệ truy nhập 3GPP, chẳng hạn, BS, xác định rằng số đếm NAS tương ứng với công nghệ truy nhập 3GPP có thể được sử dụng. Nói cách khác, nút AMF có thể kiểm chứng, bằng số đếm NAS UL tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi nút AMF, số đếm NAS UL được mang trong thông điệp N2. Nếu thông điệp N2 đến từ thiết bị qua công nghệ truy nhập phi 3GPP, chẳng hạn, nút N3IWF, xác định rằng số đếm NAS tương ứng với công nghệ truy nhập phi 3GPP có thể được sử dụng. Nói cách khác, nút AMF có thể kiểm chứng, bằng số đếm NAS UL tương ứng với công nghệ truy nhập phi 3GPP và được lưu trữ bởi nút AMF, số đếm NAS UL được mang trong thông điệp N2.

Phương pháp 2: Thiết bị đầu cuối có thể thông báo nút AMF về nguồn của thông điệp N2 một cách tường minh. Chẳng hạn, thông điệp N2 có thể mang bit mà được sử dụng để chỉ báo công nghệ truy nhập. Chẳng hạn, 0 biểu diễn công nghệ truy nhập 3GPP, và 1 biểu diễn công nghệ truy nhập phi 3GPP. Theo cách

khác, thông điệp N2 có thể mang chuỗi kỹ tự, chẳng hạn, “NR” biểu diễn công nghệ truy nhập 3GPP, và “wifi” biểu diễn công nghệ truy nhập phi 3GPP.

Phương pháp 3: Nút AMF xác định, dựa trên thông tin loại truy nhập trong thông điệp N2, công nghệ truy nhập được sử dụng để truyền thông điệp N2. Chẳng hạn, thông tin loại truy nhập là thông tin loại RAT (loại truy nhập). Nếu thông điệp N2 đến từ thiết bị sử dụng công nghệ truy nhập 3GPP, chẳng hạn, BS, chỉ báo loại truy nhập trong thông điệp N2 là truy nhập 3GPP, sao cho xác định rằng số đếm NAS tương ứng với công nghệ truy nhập 3GPP có thể được sử dụng. Nói cách khác, nút AMF có thể kiểm chứng, bằng số đếm NAS UL tương ứng với công nghệ truy nhập 3GPP và được lưu trữ bởi nút AMF, số đếm NAS UL được mang trong thông điệp N2.

So sánh với giải pháp kỹ thuật đã biết trong đó nút AMF không phân biệt các công nghệ truy nhập được sử dụng bằng các thông điệp được nhận, theo hai cách nêu trên theo phương án thực hiện sáng chế, nút AMF có thể xác định công nghệ truy nhập được sử dụng bằng thông điệp được nhận, để chọn số đếm NAS tương ứng với công nghệ truy nhập được sử dụng bằng thông điệp được nhận.

Một cách tùy chọn, theo triển khai khác theo phương án thực hiện sáng chế, dựa vào thủ tục phương pháp tương ứng với Fig.11A và Fig.11B, nếu nút AMF xác định số đếm NAS UL thứ hai và số đếm NAS DL thứ nhất tương ứng với công nghệ truy nhập phi 3GPP ở bước 1111, nút AMF có thể cập nhật tiếp khóa NAS. Phương án thực hiện sáng chế đề xuất bốn phương pháp cập nhật khóa NAS.

Phương pháp 1: Tạo Kamf mới (new Kamf, nKamf) bằng Kamf cũ (old Kamf, oKamf), và sau khi nút AMF tạo nKamf, tạo khóa NAS mới dựa trên nKamf.

Ở đây, Kamf là khóa gốc của nút AMF.

Ở đây, $nKamf = KDF(oKamf, \text{tham số độ mới})$. Tham số độ mới có thể là số đếm NAS UL được nhận trước đó bằng nút AMF, COUNT, tham số được gửi bởi thiết bị đầu cuối đến nút AMF, hoặc tham số được thỏa hiệp giữa thiết bị đầu cuối và nút AMF.

Phương pháp 2: Tạo nKamf bằng Kseaf, và sau khi nút AMF tạo nKamf, tạo

khóa NAS mới dựa trên $nKamf$.

Ở đây, $Kseaf$ là khóa gốc của nút AMF.

Ở đây, $nKamf = KDF(Kamf, \text{tham số độ mới})$. Tham số độ mới có thể là số đếm NAS UL được nhận trước đó bằng nút AMF, hoặc có thể là giá trị bộ đếm. Chẳng hạn, giá trị bắt đầu của giá trị bộ đếm bằng 0, và mỗi lần nút AMF tạo khóa NAS, giá trị bộ đếm được tăng lên 1, để chỉ báo rằng nút AMF tạo khóa mới.

Phương pháp 3: Nút AMF có thể tạo khóa NAS mới dựa trên $oKamf$ và thuật toán.

Ở đây, $nKamf = KDF(oKamf, ID \text{ thuật toán}, \text{thuật toán được chọn}, \text{và tham số khác})$, và ID thuật toán là ID của thuật toán được lựa chọn bởi nút AMF. Thuật toán được chọn là thuật toán được sử dụng bởi thiết bị đầu cuối và nút AMF để thực hiện bảo vệ bảo mật trên thông điệp NAS.

Tham số khác là tham số được sử dụng để chỉ báo công nghệ truy nhập. Cụ thể là, tham số khác có thể ở dạng bit hoặc ở dạng ID. Chẳng hạn, có thể xác định rằng tham số khác tương ứng với công nghệ truy nhập 3GPP bằng 0x01, tham số khác tương ứng với công nghệ truy nhập phi 3GPP bằng 0x10, và tham số khác tương ứng với công nghệ truy nhập mạng cố định bằng 0x11.

Tham số khác có thể theo cách khác là giá trị bộ đếm. Chẳng hạn, giá trị bắt đầu của giá trị bộ đếm bằng 0, và mỗi lần nút AMF tạo khóa NAS, giá trị bộ đếm được tăng lên 1, để chỉ báo rằng nút AMF tạo khóa mới.

Phương pháp 4: Tạo khóa NAS mới dựa trên khóa NAS cũ.

khóa NAS mới = (khóa NAS cũ, giá trị bộ đếm). Chẳng hạn, giá trị bắt đầu của giá trị bộ đếm bằng 0, và mỗi lần nút AMF tạo khóa NAS, giá trị bộ đếm được tăng lên 1, để chỉ báo rằng nút AMF tạo khóa mới.

Nên lưu ý rằng nếu nút AMF tạo khóa NAS mới, nút AMF có thể ra lệnh, bằng thông điệp NAS SMC theo phương án thực hiện tương ứng với Fig.11A và Fig.11B, thiết bị đầu cuối cập nhật khóa theo tường minh. Sau khi nhận lệnh cập nhật khóa, thiết bị đầu cuối có thể cập nhật khóa bằng một trong bốn phương pháp nêu trên. Phương pháp cập nhật hóa bởi thiết bị đầu cuối giống như phương pháp cập nhật khóa NAS bởi nút AMF, và phương pháp cập nhật khóa NAS được

tiền cấu hình trong cả nút AMF và thiết bị đầu cuối.

Một cách tùy chọn, khi nút AMF và thiết bị đầu cuối thay đổi công nghệ truy nhập được sử dụng, khóa NAS có thể được cập nhật. Theo cách khác, khóa NAS có thể được cập nhật khi trường hợp sử dụng các công nghệ truy nhập được chuyển đổi sang trường hợp sử dụng chỉ một công nghệ truy nhập, hoặc khi số lượng công nghệ truy nhập được sử dụng đồng thời được giảm.

Theo phương pháp này, khóa được cập nhật. Thậm chí nếu kẻ tấn công thu được khóa NAS được sử dụng khi nút AMF truyền thông với thiết bị đầu cuối bằng các công nghệ truy nhập, kẻ tấn công không thể thu được văn bản gốc được sử dụng khi thiết bị đầu cuối lần lượt truyền thông với nút AMF bằng một công nghệ truy nhập, nhờ đó cải thiện độ bảo mật.

Nên lưu ý rằng, theo các phương án thực hiện sáng chế, ví dụ trong đó công nghệ truy nhập thứ nhất là công nghệ truy nhập phi 3GPP và công nghệ truy nhập thứ hai là công nghệ truy nhập 3GPP được sử dụng để mô tả. Theo cách khác, trong ứng dụng thực, công nghệ truy nhập thứ nhất có thể là công nghệ truy nhập 3GPP, và công nghệ truy nhập thứ hai có thể là công nghệ truy nhập phi 3GPP. Phương pháp theo các phương án thực hiện nêu trên có thể được sử dụng khi công nghệ truy nhập thứ nhất và công nghệ truy nhập thứ hai một cách lần lượt là hai công nghệ truy nhập khác nhau được hỗ trợ bởi thiết bị đầu cuối, hoặc phương pháp theo các phương án thực hiện nêu trên có thể được sử dụng khi thiết bị đầu cuối truy nhập thiết bị mạng lõi bằng các công nghệ truy nhập.

Chẳng hạn, nếu công nghệ truy nhập thứ nhất là công nghệ truy nhập mạng cố định và công nghệ truy nhập thứ hai là công nghệ truy nhập phi 3GPP, phương pháp triển khai giống như phương pháp được mô tả trong các phương án thực hiện nêu trên. Phương án thực hiện tương ứng với Fig.11A và Fig.11B có thể được áp dụng cho kịch bản trong đó thiết bị đầu cuối đã truy nhập nút AMF bằng công nghệ truy nhập 3GPP, và sau đó truy nhập nút AMF tương tự bằng công nghệ truy nhập mạng cố định. Thủ tục trên Fig.11A và Fig.11B có thể được thay thế bằng quá trình đăng ký trong đó thiết bị đầu cuối truy nhập nút AMF bằng công nghệ truy nhập mạng cố định. Phương pháp bảo vệ bảo mật trong quá trình đăng ký giống như phương pháp bảo vệ bảo mật được mô tả trong phương án

thực hiện trên Fig.11A và Fig.11B và trong đó thiết bị đầu cuối truy nhập nút AMF bằng công nghệ truy nhập phi 3GPP.

Phần trên mô tả chủ yếu các giải pháp theo các phương án thực hiện sáng chế từ khía cạnh tương tác giữa các phần tử mạng khác nhau. Có thể hiểu rằng để triển khai các chức năng nêu trên, thiết bị đầu cuối và thiết bị mạng lõi bao gồm các cấu trúc phần cứng tương ứng và/hoặc các môđun phần mềm để thực hiện các chức năng. Dựa vào các ví dụ được mô tả trong các phương án thực hiện được bộc lộ theo sáng chế, các khối và các bước thuật toán có thể được triển khai bằng phần cứng hoặc tổ hợp của phần cứng và phần mềm máy tính theo các phương án thực hiện sáng chế. Liệu chức năng được triển khai theo cách thức phần cứng hoặc theo cách thức điều khiển phần cứng bằng phần mềm máy tính tùy thuộc vào ứng dụng cụ thể và điều kiện ràng buộc thiết kế của các giải pháp kỹ thuật. Đối với mỗi ứng dụng cụ thể, người có hiểu biết trung bình trong lĩnh vực có thể sử dụng các phương pháp khác nhau để triển khai các chức năng được mô tả, nhưng không nên xem là việc triển khai vượt quá phạm vi của các giải pháp kỹ thuật theo các phương án thực hiện sáng chế.

Theo các phương án thực hiện sáng chế, việc phân chia khối chức năng có thể được thực hiện trên thiết bị đầu cuối và thiết bị mạng lõi dựa trên các ví dụ phương pháp nêu trên. Chẳng hạn, mỗi khối chức năng có thể thu được qua phân chia dựa trên chức năng tương ứng, hoặc hai hoặc nhiều khối có thể được tích hợp vào một khối xử lý. Khối được tích hợp có thể được triển khai ở dạng phần cứng, hoặc có thể được triển khai ở dạng khối chức năng phần mềm. Nên lưu ý rằng việc phân chia khối theo các phương án thực hiện sáng chế là ví dụ, và chỉ là phân chia chức năng logic và có thể là phân chia khác khi triển khai thực.

Khi khối tích hợp được sử dụng, Fig.12 thể hiện sơ đồ khối của thiết bị 1200 theo phương án thực hiện sáng chế. Thiết bị 1200 có thể ở dạng phần mềm, hoặc có thể là thiết bị đầu cuối, hoặc có thể là vi mạch trong thiết bị đầu cuối. Thiết bị 1200 bao gồm khối xử lý 1202 và khối truyền thông 1203. Khối xử lý 1202 được tạo cấu hình để điều khiển và quản lý hoạt động của thiết bị 1200. Chẳng hạn, khối xử lý 1202 được tạo cấu hình để hỗ trợ thiết bị 1200 khi thực hiện bước 501 và bước 502 trên Fig.5, bước 1001 trên Fig.10, bước 1101, bước 1105, bước

1113, bước 1117, và bước 1118 trên Fig.11A và Fig.11B, và/hoặc quá trình khác của công nghệ được mô tả trong bản mô tả. Khối truyền thông 1203 được tạo cấu hình để hỗ trợ truyền thông giữa thiết bị 1200 và phần tử mạng khác (chẳng hạn thiết bị mạng lõi và nút N3IWF). Chẳng hạn, khối truyền thông 1203 được tạo cấu hình để hỗ trợ thiết bị 1200 khi thực hiện bước 1002, bước 1003, và bước 1007 trên Fig.10, và bước 1102, bước 1103, bước 1104, bước 1106, bước 1112, bước 1114, bước 1116, và bước 1119 trên Fig.11A và Fig.11B. Thiết bị 1200 có thể còn bao gồm khối lưu trữ 1201, được tạo cấu hình để lưu trữ mã chương trình và dữ liệu của thiết bị 1200.

Khối xử lý 1202 có thể là bộ xử lý hoặc bộ điều khiển, chẳng hạn, khối xử lý trung tâm (Central Processing Unit, CPU), bộ xử lý đa năng, bộ xử lý tín hiệu số (Digital Signal Processor, DSP), mạch tích hợp ứng dụng cụ thể (Application-Specific Integrated Circuit, ASIC), mảng cổng dạng trường lập trình được (Field Programmable Gate Array, FPGA) hoặc thiết bị logic lập trình được (programmable logic device, PLD) khác, thiết bị logic tranzito, linh kiện phần cứng, hoặc tổ hợp bất kỳ của nó. Khối xử lý 1202 có thể triển khai hoặc thực thi các ví dụ khác nhau của các khối logic, các môđun, và các mạch được mô tả dựa vào nội dung được bộc lộ theo sáng chế. Theo cách khác, bộ xử lý có thể là tổ hợp để triển khai chức năng tính toán, chẳng hạn, tổ hợp của một hoặc nhiều bộ vi xử lý hoặc tổ hợp của DSP và bộ vi xử lý. Khối truyền thông 1203 có thể là bộ thu phát, mạch thu phát, giao diện truyền thông, hoặc tương tự. Khối lưu trữ 1201 có thể là bộ nhớ.

Khi khối xử lý 1202 là bộ xử lý, khối truyền thông 1203 là bộ thu phát, và khối lưu trữ 1201 là bộ nhớ, thiết bị 1200 theo phương án thực hiện sáng chế có thể là thiết bị đầu cuối được thể hiện trên Fig.13.

Fig.13 thể hiện sơ đồ được đơn giản hóa của kiến trúc thiết kế khả thi của thiết bị đầu cuối 1300 liên quan theo phương án thực hiện sáng chế. Thiết bị đầu cuối 1300 bao gồm bộ truyền 1301, bộ nhận 1302, và bộ xử lý 1303. Bộ xử lý 1303 có thể theo cách khác là bộ điều khiển, và được chỉ bảo là “bộ điều khiển/bộ xử lý 1303” trên Fig.13. Một cách tùy chọn, thiết bị đầu cuối 1300 có thể còn bao gồm bộ xử lý modem 1305, và bộ xử lý modem 1305 có thể bao gồm bộ mã

hóa 1306, bộ điều biến 1307, bộ giải mã 1308, và bộ giải điều biến 1309.

Trong ví dụ, bộ truyền 1301 điều chỉnh (chẳng hạn, qua biến đổi tương tự, lọc, khuếch đại, và biến đổi lên) mẫu đầu ra và tạo tín hiệu UL. Tín hiệu UL được truyền đến BS theo các phương án thực hiện nêu trên bằng anten. Trên DL, anten nhận tín hiệu DL được truyền bằng BS theo phương án thực hiện nêu trên. Bộ nhận 1302 điều chỉnh (chẳng hạn, qua lọc, khuếch đại, biến đổi xuống, và số hóa) tín hiệu được nhận từ anten và cấp mẫu đầu vào. Trong bộ xử lý modem 1305, bộ mã hóa 1306 nhận dữ liệu dịch vụ và thông điệp báo hiệu cần được gửi trên UL, và xử lý (chẳng hạn, qua định dạng, mã hóa, và đan xen) dữ liệu dịch vụ và thông điệp báo hiệu. Bộ điều biến 1307 xử lý tiếp (chẳng hạn, qua ánh xạ ký hiệu và điều biến) dữ liệu dịch vụ được mã hóa và thông điệp báo hiệu được mã hóa, và cấp mẫu đầu ra. Bộ giải điều biến 1309 xử lý (chẳng hạn, qua giải điều biến) mẫu đầu vào và tạo ước tính ký hiệu. Bộ giải mã 1308 xử lý (chẳng hạn, qua bỏ đan xen và giải mã) ước tính ký hiệu và cấp dữ liệu được giải mã và thông điệp báo hiệu được giải mã cần được gửi đến thiết bị đầu cuối 1300. Bộ mã hóa 1306, bộ điều biến 1307, bộ giải điều biến 1309, và bộ giải mã 1308 có thể được triển khai bằng modem bộ xử lý được tích hợp 1305. Các hồi thực hiện xử lý dựa trên công nghệ truy nhập vô tuyến (chẳng hạn, các công nghệ truy nhập của LTE và hệ thống tiến hóa khác) được sử dụng trong RAN. Nên lưu ý rằng khi thiết bị đầu cuối 1300 không bao gồm bộ xử lý modem 1305, các chức năng nêu trên của bộ xử lý modem 1305 có thể theo cách khác được triển khai bởi bộ xử lý 1303.

Bộ xử lý 1303 điều khiển và quản lý hoạt động của thiết bị đầu cuối 1300, và được tạo cấu hình để thực thi xử lý được thực hiện bởi thiết bị đầu cuối 1300 theo các phương án thực hiện nêu trên của sáng chế. Chẳng hạn, bộ xử lý 1303 còn được tạo cấu hình để thực thi quá trình xử lý liên quan đến thiết bị đầu cuối ở phương pháp được thể hiện trên Fig.5, Fig.10, và Fig.11A và Fig.11B, và/hoặc quá trình khác của các giải pháp kỹ thuật được mô tả trong sáng chế.

Ngoài ra, thiết bị đầu cuối 1300 có thể còn bao gồm bộ nhớ 1304, và bộ nhớ 1304 được tạo cấu hình để lưu trữ mã chương trình và dữ liệu được sử dụng cho thiết bị đầu cuối 1300.

Khi khối tích hợp được sử dụng, Fig.14 thể hiện sơ đồ khối của thiết bị 1400 khác theo phương án thực hiện sáng chế. Thiết bị có thể tồn tại ở dạng phần mềm, hoặc có thể là thiết bị mạng lõi, hoặc có thể là vi mạch trong thiết bị mạng lõi. Thiết bị 1400 bao gồm khối xử lý 1402 và khối truyền thông 1403. Khối xử lý 1402 được tạo cấu hình để điều khiển và quản lý hoạt động của thiết bị 1400. Chẳng hạn, khối xử lý 1402 được tạo cấu hình để hỗ trợ thiết bị 1400 khi thực hiện bước 901 và bước 902 trên Fig.9, bước 1004 đến bước 1006 trên Fig.10, bước 1109 đến bước 1111 trên Fig.11A và Fig.11B, và/hoặc quá trình khác của công nghệ được mô tả trong bản mô tả. Khối truyền thông 1403 được tạo cấu hình để hỗ trợ truyền thông giữa thiết bị 1400 và phân tử mạng khác (chẳng hạn thiết bị đầu cuối hoặc nút N3IWF). Chẳng hạn, khối truyền thông 1403 được tạo cấu hình để hỗ trợ thiết bị 1400 khi thực hiện bước 1001, bước 1002, và bước 1007 trên Fig.10, và bước 1108, bước 1112, bước 1114, và bước 1115 trên Fig.11A và Fig.11B. Thiết bị 1400 có thể còn bao gồm khối lưu trữ 1401, được tạo cấu hình để lưu trữ mã chương trình và dữ liệu của thiết bị 1400.

Khối xử lý 1402 có thể là bộ xử lý hoặc bộ điều khiển, chẳng hạn, CPU, bộ xử lý đa năng, DSP, ASIC, FPGA hoặc PLD khác, thiết bị logic tranzito, linh kiện phần cứng, hoặc tổ hợp bất kỳ của nó. Khối xử lý 1402 có thể triển khai hoặc thực thi các khối logic ví dụ khác nhau, các môđun, và các mạch được mô tả dựa vào nội dung được bộc lộ theo sáng chế. Theo cách khác, bộ xử lý có thể là tổ hợp để triển khai chức năng tính toán, chẳng hạn, tổ hợp của một hoặc nhiều bộ vi xử lý hoặc tổ hợp của DSP và bộ vi xử lý. Khối truyền thông 1403 có thể là giao diện truyền thông. Giao diện truyền thông là tên chung. Theo triển khai cụ thể, giao diện truyền thông có thể bao gồm các giao diện. Chẳng hạn, giao diện truyền thông có thể bao gồm giao diện giữa thiết bị mạng lõi và thiết bị đầu cuối, và giao diện giữa thiết bị mạng lõi và nút N3IWF, và/hoặc giao diện khác. Khối lưu trữ 1401 có thể là bộ nhớ.

Khi khối xử lý 1402 là bộ xử lý, khối truyền thông 1403 là giao diện truyền thông, và khối lưu trữ 1401 là bộ nhớ, cấu trúc của thiết bị 1400 theo phương án thực hiện sáng chế có thể là cấu trúc của thiết bị mạng được thể hiện trên Fig.15.

Fig.15 thể hiện sơ đồ cấu trúc khả thi của thiết bị mạng lõi theo phương án

thực hiện sáng chế.

Như được thể hiện trên Fig.15, thiết bị mạng lõi 1500 bao gồm bộ xử lý 1502, giao diện truyền thông 1503, và bộ nhớ 1501. Một cách tùy chọn, thiết bị mạng lõi 1500 có thể còn bao gồm đường truyền 1504. Giao diện truyền thông 1503, bộ xử lý 1502, và bộ nhớ 1501 có thể be được kết nối với nhau bằng đường truyền 1504. Đường truyền 1504 có thể là đường truyền PCI, đường truyền EISA, hoặc tương tự. Đường truyền 1504 có thể được phân loại thành đường truyền địa chỉ, đường truyền dữ liệu, đường truyền điều khiển, và tương tự. Để dễ chỉ báo, đường truyền được chỉ báo bằng chỉ một đường nét đậm trên Fig.15. Tuy nhiên, it không chỉ báo rằng chỉ có một đường truyền hoặc chỉ một loại đường truyền.

Các phương pháp hoặc các bước thuật toán được mô tả dựa vào nội dung được bộc lộ theo sáng chế có thể được triển khai theo cách thức phần cứng, hoặc có thể được triển khai theo cách thức thực thi lệnh phần mềm bằng bộ xử lý. Lệnh phần mềm có thể bao gồm phần mềm môđun tương ứng. Phần mềm môđun có thể be được lưu trữ trong bộ nhớ truy nhập ngẫu nhiên (Random Access Memory, RAM), bộ nhớ nhanh, bộ nhớ chỉ đọc (Read-Only Memory, ROM), ROM lập trình được xóa được (Erasable Programmable ROM, EPROM), EPROM bằng điện (Electrically EPROM, EEPROM), thanh ghi, đĩa cứng, đĩa cứng tháo được, đĩa CD-ROM, hoặc vật lưu trữ theo các dạng khác bất kỳ đã biết theo giải pháp kỹ thuật. Vật lưu trữ được sử dụng làm ví dụ được ghép nối với bộ xử lý, sao cho bộ xử lý có thể đọc thông tin từ vật lưu trữ, và có thể viết thông tin vào vật lưu trữ. Chắc chắn là, vật lưu trữ có thể là thành phần của bộ xử lý. Bộ xử lý và vật lưu trữ có thể được đặt trong ASIC. Ngoài ra, ASIC có thể được đặt trong thiết bị giao diện mạng lõi. Chắc chắn là, bộ xử lý và vật lưu trữ có thể tồn tại ở thiết bị giao diện mạng lõi như là các thành phần riêng rẽ.

Theo một số phương án thực hiện sáng chế, nên hiểu rằng hệ thống, thiết bị, và phương pháp được bộc lộ có thể được triển khai theo các cách khác. Chẳng hạn, thiết bị được mô tả theo phương án thực hiện chỉ là ví dụ. Chẳng hạn, việc phân chia khối chỉ là phân chia chức năng logic và có thể là phân chia khác khi triển khai thực. Chẳng hạn, các khối hoặc thành phần có thể được kết hợp hoặc

tích hợp vào hệ thống khác, hoặc một số dấu hiệu có thể được bỏ qua hoặc không được thực hiện. Ngoài ra, các ghép nối lẫn nhau được đề cập hoặc hiển thị hoặc các ghép nối trực tiếp hoặc các kết nối truyền thông có thể được triển khai qua một số giao diện. Các ghép nối gián tiếp hoặc các kết nối truyền thông giữa các thiết bị hoặc các khối có thể được triển khai ở các dạng điện tử hoặc dạng khác.

Các khối được mô tả như là các phần riêng rẽ có thể hoặc không thể riêng rẽ về mặt vật lý. Các phần được hiển thị dưới dạng khác khối có thể hoặc không thể là các khối vật lý, nói cách khác, có thể được đặt ở một vị trí, hoặc có thể được phân tán các thiết bị mạng. Một số hoặc tất cả các khối có thể được lựa chọn theo các nhu cầu thực để đạt được các mục đích của các giải pháp theo các phương án thực hiện.

Ngoài ra, các khối chức năng theo các phương án thực hiện sáng chế có thể được tích hợp vào một khối xử lý, hoặc mỗi khối của các khối chức năng có thể tồn tại độc lập, hoặc hai hoặc nhiều khối được tích hợp vào một khối. Khối được tích hợp có thể được triển khai ở dạng phần cứng, hoặc có thể được triển khai ở dạng phần cứng bên cạnh khối chức năng phần mềm.

Dựa trên các phần mô tả nêu trên của các triển khai, người có hiểu biết trung bình trong lĩnh vực có thể hiểu rõ ràng rằng sáng chế có thể được triển khai bằng phần mềm bên cạnh phần cứng đa năng cần thiết hoặc chắc chắn là chỉ bằng phần cứng. Trong một số trường hợp, triển khai bằng phần mềm được ưu tiên. Dựa trên hiểu biết này, các giải pháp kỹ thuật của sáng chế chủ yếu hoặc một phần đóng góp vào giải pháp kỹ thuật đã biết có thể được triển khai ở dạng sản phẩm phần mềm. Sản phẩm phần mềm máy tính được lưu trữ trong vật lưu trữ đọc được, chẳng hạn đĩa mềm, đĩa cứng, hoặc đĩa quang của máy tính, và bao gồm vài lệnh để ra lệnh thiết bị máy tính (có thể là máy tính cá nhân, máy chủ, hoặc thiết bị mạng) thực hiện phương pháp được mô tả trong các phương án thực hiện sáng chế.

Các phần mô tả nêu trên chỉ là các phương án thực hiện cụ thể sáng chế, mà không nhằm giới hạn phạm vi bảo hộ của sáng chế. Biến thể hoặc thay thế bất kỳ được bộc lộ theo sáng chế sẽ nằm trong phạm vi bảo hộ của sáng chế. Do vậy, phạm vi bảo hộ của sáng chế sẽ phụ thuộc vào phạm vi bảo hộ của các điểm yêu

cầu bảo hộ.

YÊU CẦU BẢO HỘ

1. Phương pháp bảo vệ bảo mật bao gồm các bước:

xác định (501, 901), bằng thiết bị, giá trị của tham số thứ nhất, trong đó giá trị của tham số thứ nhất là công nghệ truy nhập được sử dụng để truyền thông điệp tầng không truy nhập (non-access stratum, NAS) và tham số thứ nhất là tham số đầu vào được sử dụng khi thực hiện bảo vệ bảo mật trên thông điệp NAS; và

thực hiện (502, 902), bằng thiết bị, bảo vệ bảo mật trên thông điệp NAS dựa trên tham số thứ nhất, khóa NAS, và số đếm NAS (NAS COUNT) tương ứng với công nghệ truy nhập được sử dụng để truyền thông điệp NAS.

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

xác định, bằng thiết bị, công nghệ truy nhập được sử dụng để truyền thông điệp NAS trước khi xác định giá trị của tham số thứ nhất.

3. Phương pháp theo điểm 1 hoặc 2, trong đó tham số thứ nhất là kênh mang (BEARER).

4. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó công nghệ truy nhập được sử dụng để truyền thông điệp NAS là công nghệ truy nhập 3GPP và giá trị của tham số thứ nhất được gán bằng giá trị thứ nhất.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó công nghệ truy nhập được sử dụng để truyền thông điệp NAS là công nghệ truy nhập phi 3GPP và giá trị của tham số thứ nhất được gán bằng giá trị thứ hai.

6. Thiết bị bảo vệ bảo mật bao gồm:

phương tiện xác định giá trị của tham số thứ nhất, trong đó giá trị của tham số thứ nhất là công nghệ truy nhập được sử dụng để truyền thông điệp NAS và tham số thứ nhất là tham số đầu vào được sử dụng khi thực hiện bảo vệ bảo mật trên thông điệp NAS; và

phương tiện thực hiện bảo vệ bảo mật trên thông điệp NAS dựa trên tham số thứ nhất, khóa NAS, và NAS COUNT tương ứng với công nghệ truy nhập được sử dụng để truyền thông điệp NAS.

7. Thiết bị theo điểm 6, trong đó thiết bị còn bao gồm:

phương tiện xác định công nghệ truy nhập được sử dụng để truyền thông

điệp NAS trước khi xác định giá trị của tham số thứ nhất.

8. Thiết bị theo điểm 6 hoặc 7, trong đó tham số thứ nhất là BEARER.

9. Thiết bị theo điểm bất kỳ trong số các điểm từ 6 đến 8, trong đó công nghệ truy nhập được sử dụng để truyền thông điệp NAS là công nghệ truy nhập 3GPP và giá trị của tham số thứ nhất được gán bằng giá trị thứ nhất.

10. Thiết bị theo điểm bất kỳ trong số các điểm từ 6 đến 8, trong đó công nghệ truy nhập được sử dụng để truyền thông điệp NAS là công nghệ truy nhập phi 3GPP và giá trị của tham số thứ nhất được gán bằng giá trị thứ hai.

11. Thiết bị theo điểm bất kỳ trong số các điểm từ 6 đến 10, trong đó thiết bị là thiết bị đầu cuối hoặc chip trong thiết bị đầu cuối.

12. Thiết bị theo điểm 11, trong đó thiết bị đầu cuối hỗ trợ ít nhất hai công nghệ truy nhập và duy trì riêng rẽ NAS COUNT tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập.

13. Thiết bị theo điểm bất kỳ trong số các điểm từ 6 đến 10, trong đó thiết bị là thiết bị mạng lõi hoặc chip trong thiết bị mạng lõi.

14. Thiết bị theo điểm 13, trong đó thiết bị duy trì riêng rẽ NAS COUNT tương ứng cho mỗi công nghệ trong ít nhất hai công nghệ truy nhập.

15. Vật ghi máy tính đọc được bao gồm các lệnh mà, khi được thực thi bằng máy tính, khiến máy tính thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5.

1/10

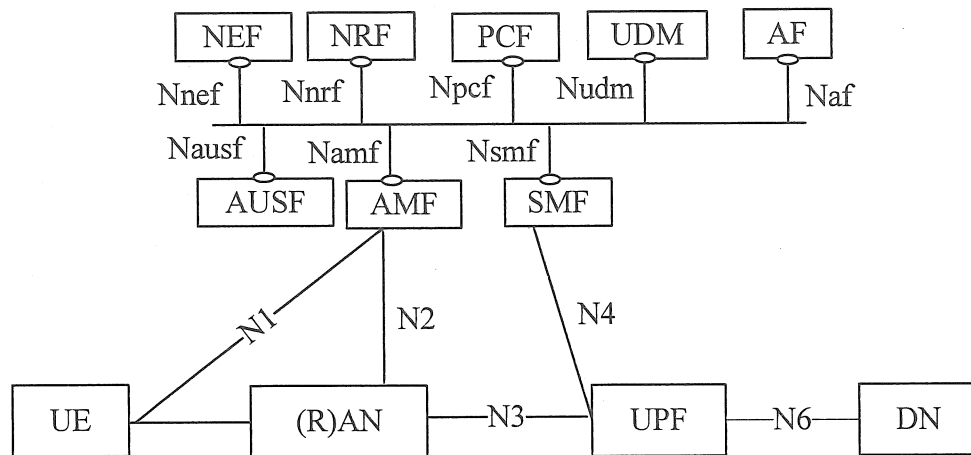


Fig.1

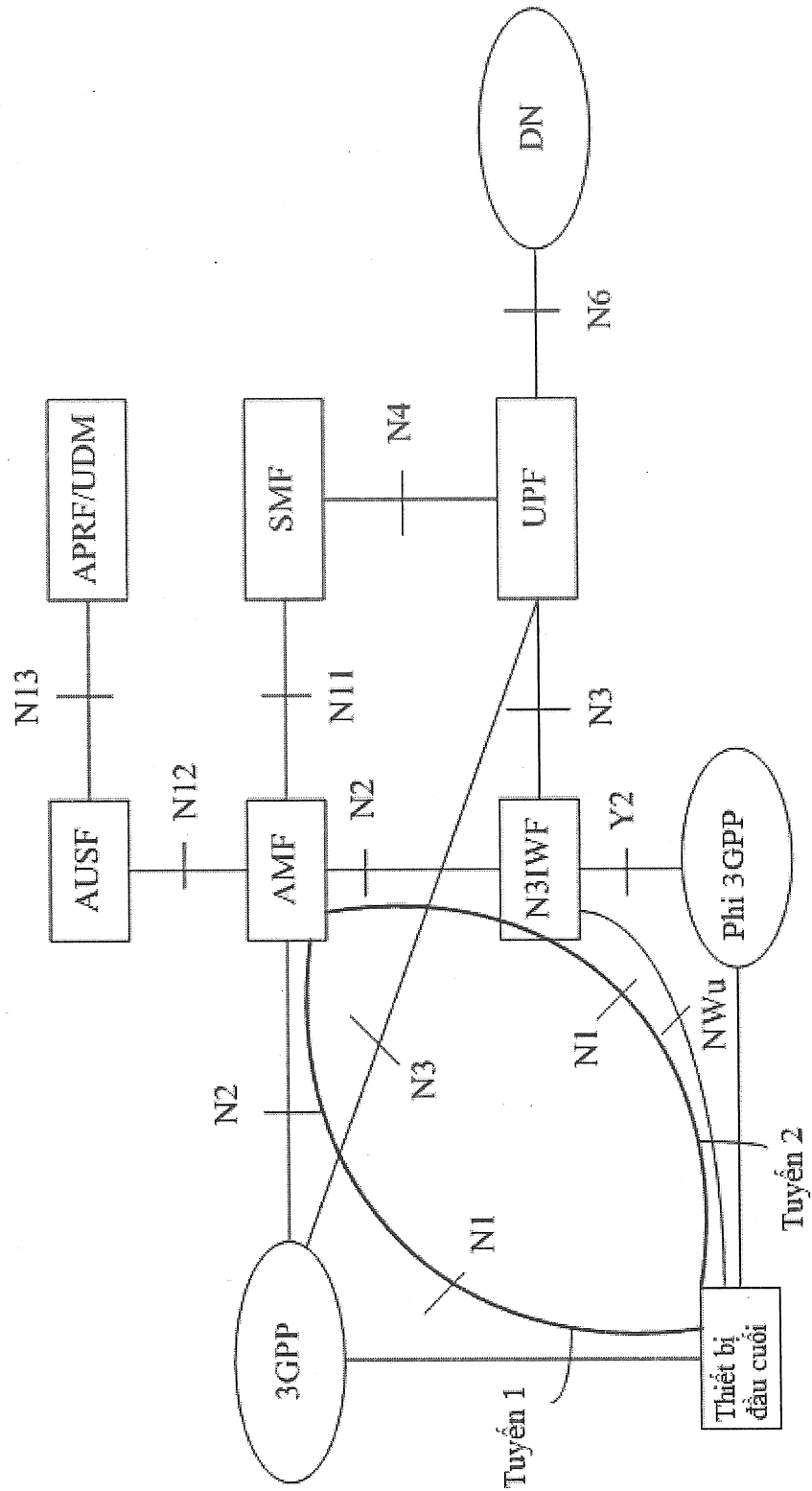


Fig. 2

3/10

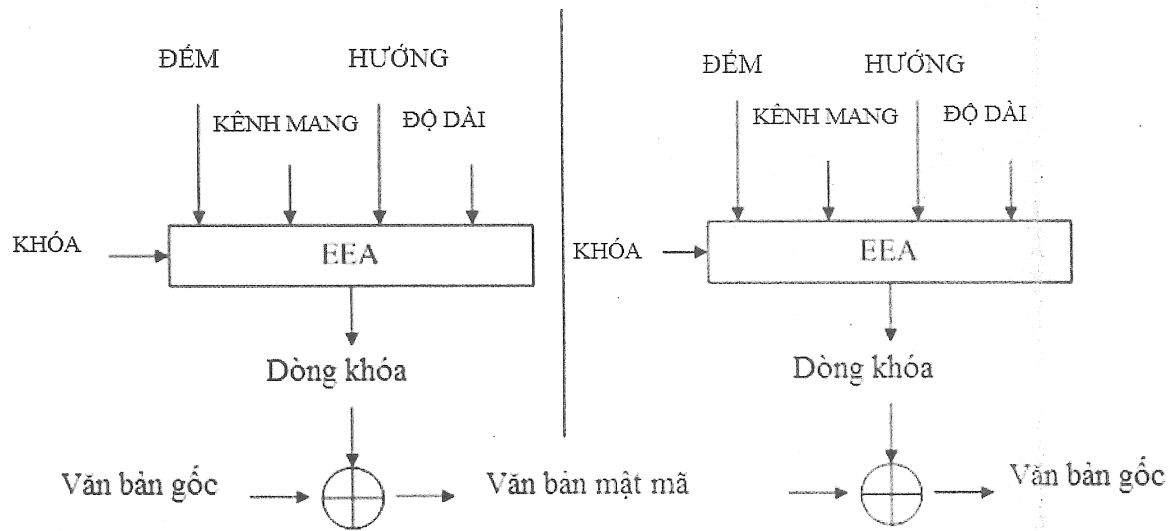


Fig.3

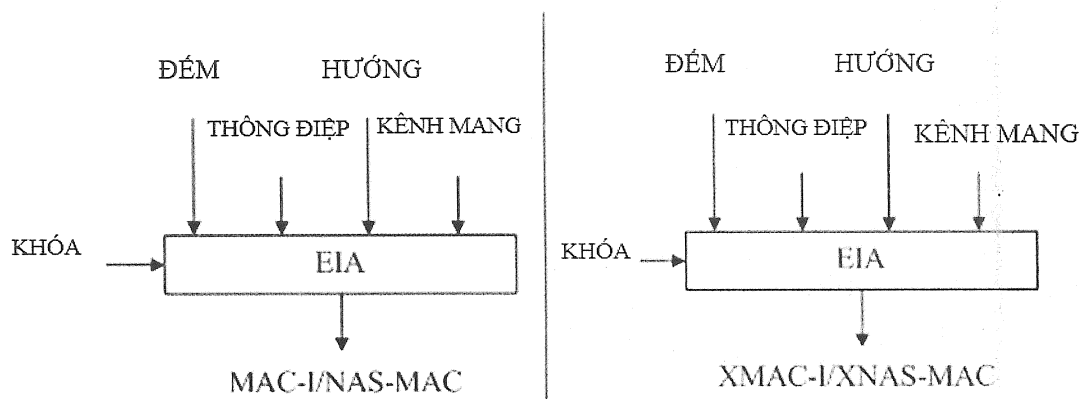


Fig.4

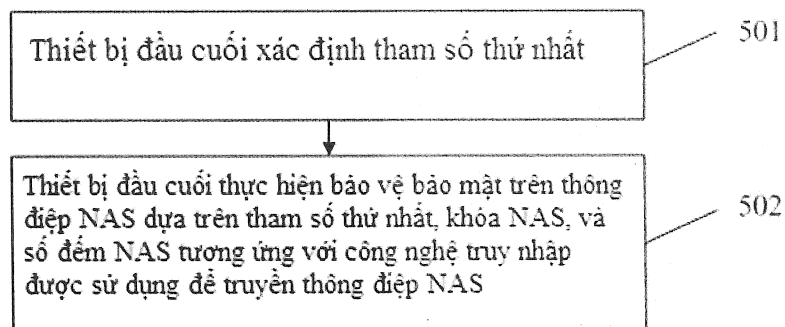
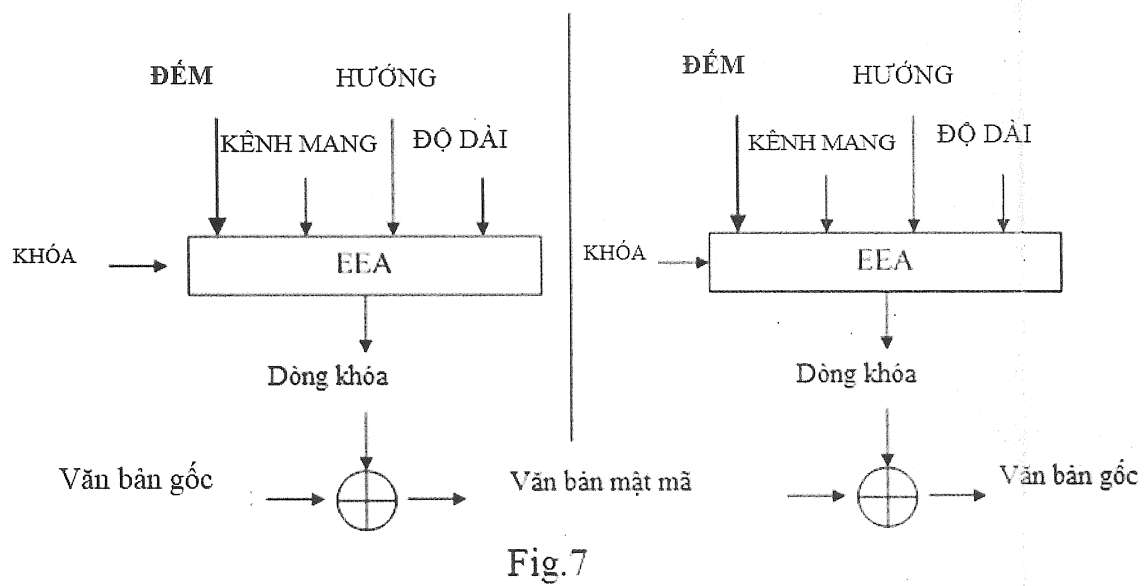
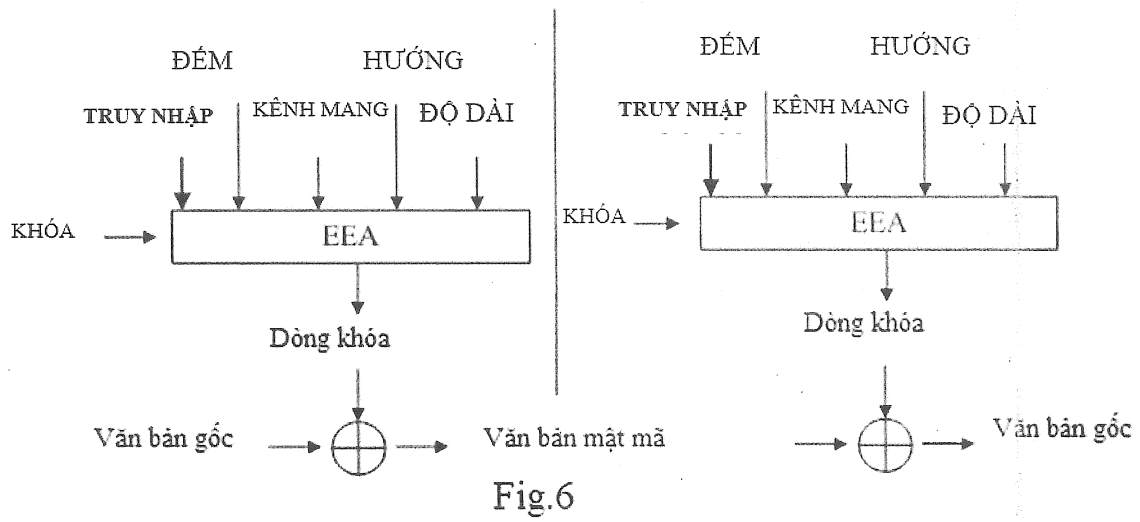


Fig.5

4/10



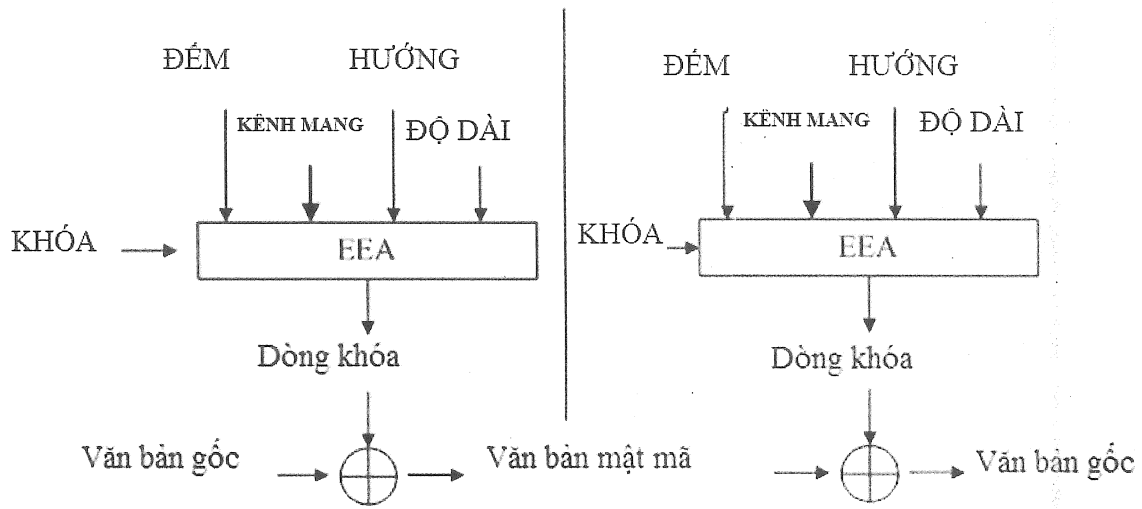


Fig.8

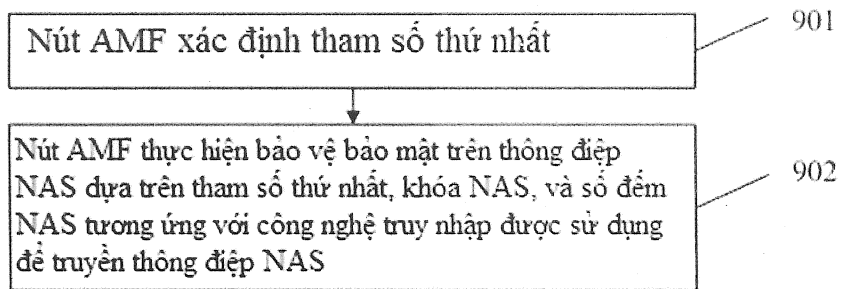


Fig.9

6/10

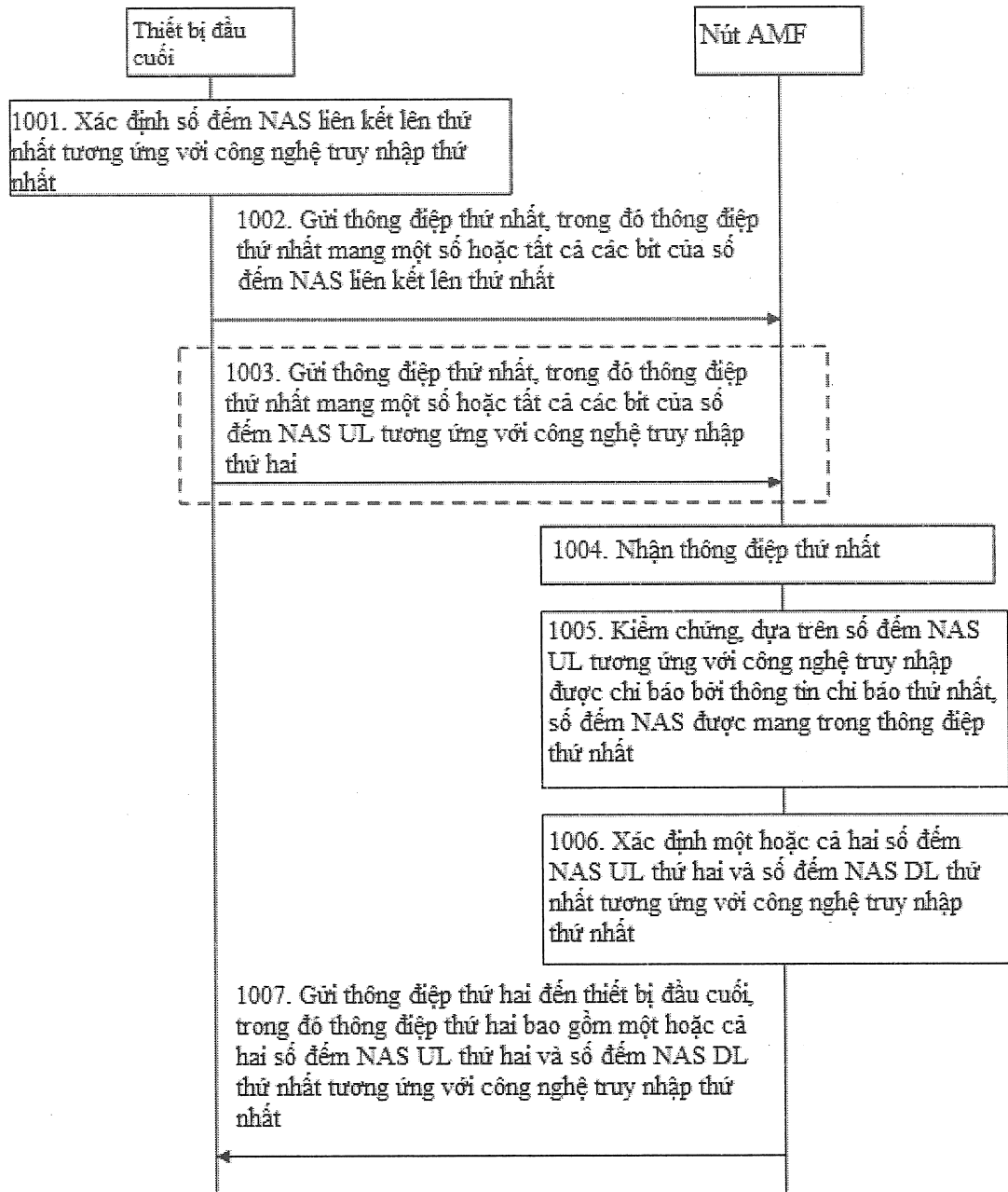


Fig.10

7/10

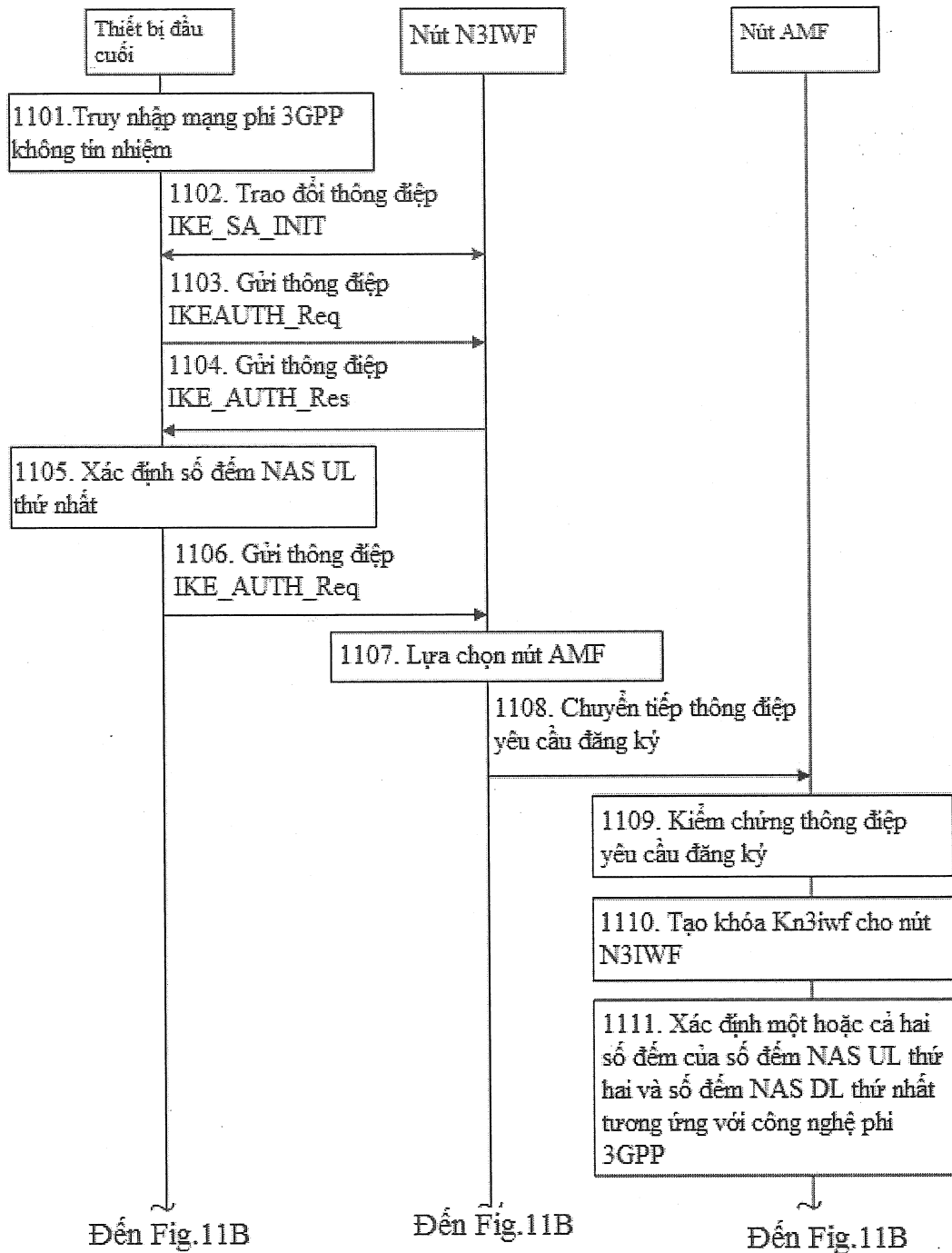


Fig.11A

8/10

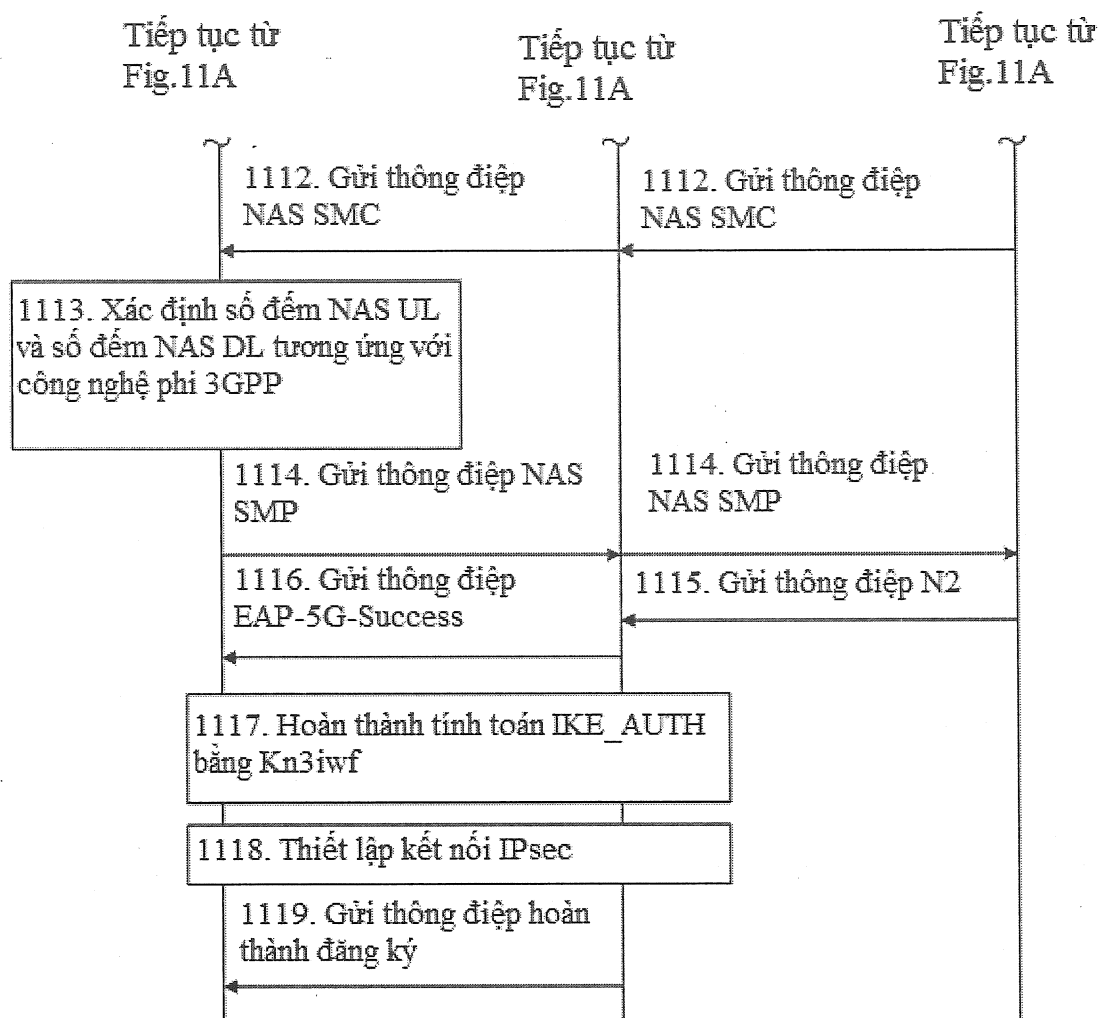


Fig. 11B

9/10

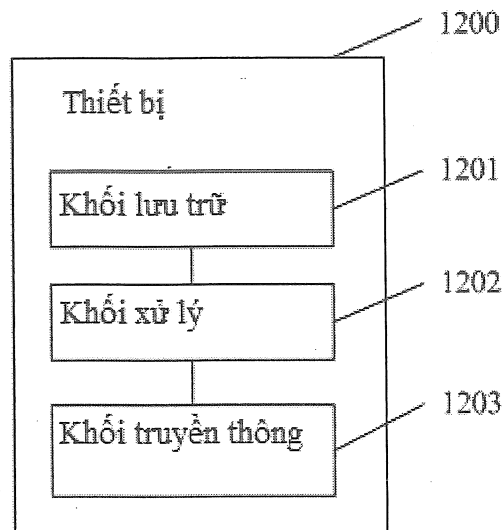


Fig.12

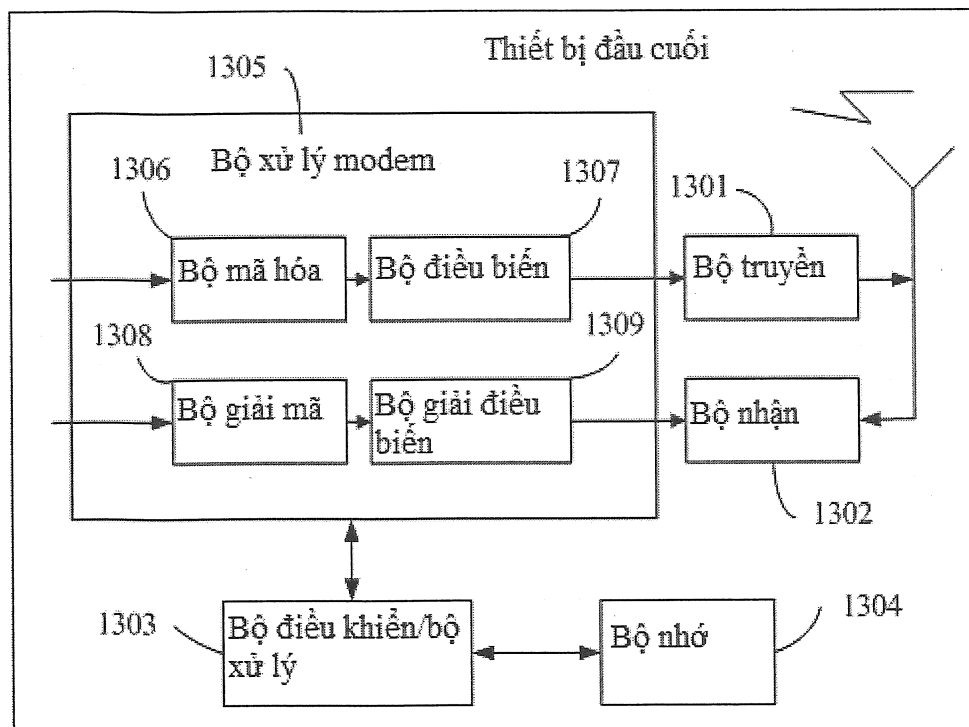


Fig.13

10/10

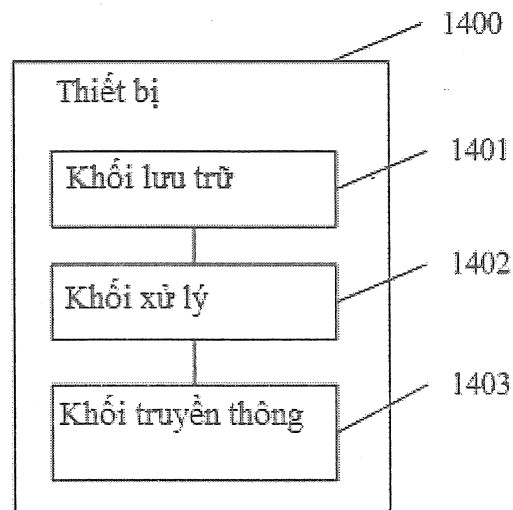


Fig.14

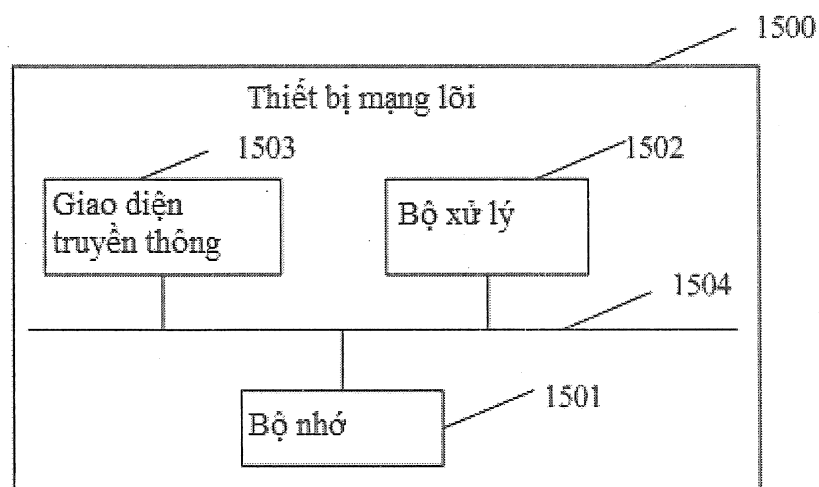


Fig.15