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

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

(11) **1-0045200**

(51)[2020.01] **H04L 9/08**

(13) **B**

(21) 1-2020-04527
(22) 07/01/2019
(86) PCT/CN2019/070709 07/01/2019
(87) WO2019/134704 11/07/2019
(30) 201810016762.9 08/01/2018 CN
(45) 25/04/2025 445
(43) 25/11/2020 392A
(71) 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 T&G (TGVN)

(54) PHƯƠNG PHÁP CẬP NHẬT KHÓA VÀ THIẾT BỊ MẠNG LÕI

(21) 1-2020-04527

(57) Các phương án của sáng chế đề xuất phương pháp cập nhật khóa, thiết bị mạng lõi, thiết bị truyền thông và phương tiện lưu trữ đọc được bằng máy tính, liên quan đến lĩnh vực công nghệ truyền thông, và có thể giải quyết vấn đề là việc cập nhật của khóa NAS (non-access stratum - tầng không truy cập) trong quy trình xử lý trong đó nút AMF (access and mobility management function - chức năng quản lý truy cập và tính di động) thực hiện việc tái xác thực trên đầu cuối bằng cách sử dụng một công nghệ truy cập làm ảnh hưởng việc truyền thông thông thường mà được thực hiện giữa đầu cuối và nút AMF bằng cách sử dụng công nghệ truy cập khác. Theo phương pháp này, hệ thống truyền thông bao gồm đầu cuối và thiết bị mạng lõi, đầu cuối truy cập thiết bị mạng lõi bằng cách sử dụng đồng thời cả công nghệ truy cập thứ nhất và công nghệ truy cập thứ hai, và phương pháp này bao gồm các bước: thực hiện, bởi thiết bị mạng lõi, việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất; và nếu điều kiện kích hoạt được đáp ứng, cập nhật, bởi thiết bị mạng lõi, khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai.

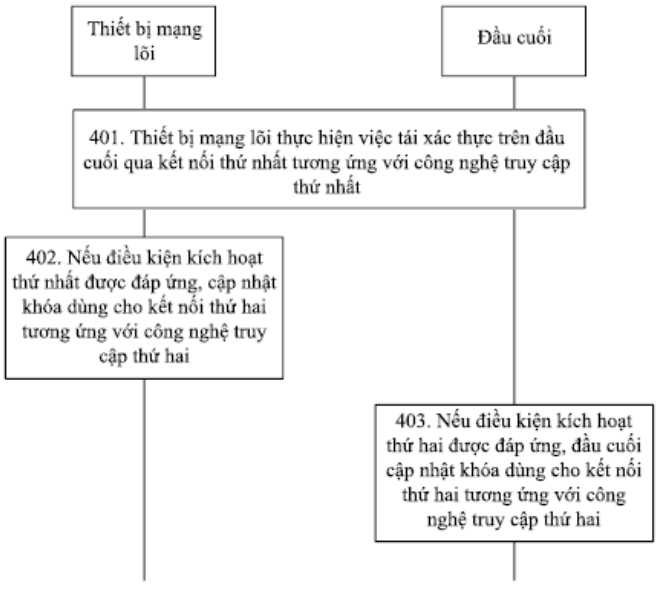

FIG. 4

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ truyền thông, và cụ thể là, sáng chế đề cập đến phương pháp cập nhật khóa, thiết bị mạng lõi, thiết bị truyền thông và phương tiện lưu trữ đọc được bằng máy tính.

Tình trạng kỹ thuật của sáng chế

Trong hệ thống thế hệ thứ năm (5th generation, viết tắt là 5G), đầu cuối có thể truy cập nút chức năng quản lý truy cập và tính di động (access and mobility management function, viết tắt là AMF) bằng cách sử dụng đồng thời cả công nghệ truy cập dự án đối tác thế hệ thứ ba (3rd generation partnership project, viết tắt là 3GPP) và công nghệ truy cập không phải 3GPP (non-3GPP). Khi đầu cuối truy cập nút AMF bằng cách sử dụng đồng thời cả công nghệ truy cập 3GPP và công nghệ truy cập không phải 3GPP, nút AMF duy trì máy trạng thái quản lý đăng ký (registration management, viết tắt là RM) và máy trạng thái quản lý kết nối (connection management, viết tắt là CM) dùng cho công nghệ truy cập 3GPP và công nghệ truy cập không phải 3GPP một cách tương ứng.

Máy trạng thái quản lý đăng ký tương ứng với trạng thái RM (RM state), và trạng thái RM bao gồm trạng thái đăng ký RM (RM-registration state) và trạng thái bỏ đăng ký RM (RM-deregistration state). Máy trạng thái quản lý kết nối tương ứng với trạng thái CM (CM state), và trạng thái CM bao gồm trạng thái được kết nối CM (CM-connected state) và trạng thái nghỉ CM (CM-idle state). Sau khi đi vào trạng thái được kết nối từ trạng thái nghỉ, đầu cuối có thể khởi tạo thủ tục đăng ký. Sau khi hoàn thành thủ tục đăng ký, đầu cuối có thể chuyển đổi từ trạng thái bỏ đăng ký sang trạng thái đăng ký. Trong trường hợp này, đầu cuối có thông tin ngữ cảnh bảo mật chẳng hạn như khóa tầng không truy cập (non-access stratum, viết tắt là NAS) và thuật toán bảo mật. Khi đầu cuối quay lại trạng thái nghỉ hoặc trạng thái bỏ đăng ký, đầu cuối vẫn có khóa NAS và thuật toán bảo mật.

Mặc dù nút AMF có thể duy trì riêng rẽ máy trạng thái dùng cho công nghệ truy

cập 3GPP và máy trạng thái dùng cho công nghệ truy cập không phải 3GPP, đầu cuối và nút AMF có thể chia sẻ tập hợp các khóa NAS khi truyền thông bằng cách sử dụng hai công nghệ truy cập. Khi nút AMF cần thực hiện việc tái xác thực trên đầu cuối bằng cách sử dụng một trong số các công nghệ truy cập, quy trình tái xác thực liên quan đến việc cập nhật khóa NAS. Tuy nhiên, khi đầu cuối và nút AMF truyền thông bằng cách sử dụng công nghệ truy cập khác, đầu cuối và AMF vẫn cần sử dụng khóa NAS được chia sẻ, hoặc đầu cuối và nút AMF đang truyền thông bằng cách sử dụng khóa NAS được chia sẻ. Trong trường hợp này, việc cập nhật khóa NAS trong quá trình trong đó nút AMF thực hiện việc tái xác thực trên đầu cuối bằng cách sử dụng một công nghệ truy cập có thể làm ảnh hưởng việc truyền thông thông thường mà được thực hiện giữa đầu cuối và nút AMF bằng cách sử dụng công nghệ truy cập khác.

Bản chất kỹ thuật của sáng chế

Các phương án của sáng chế đề xuất phương pháp cập nhật khóa, thiết bị mạng lõi, thiết bị truyền thông và phương tiện lưu trữ đọc được bằng máy tính, để giải quyết vấn đề là việc cập nhật của khóa NAS trong quy trình xử lý trong đó nút AMF thực hiện việc tái xác thực trên đầu cuối bằng cách sử dụng một công nghệ truy cập làm ảnh hưởng việc truyền thông thông thường mà được thực hiện giữa đầu cuối và nút AMF bằng cách sử dụng công nghệ truy cập khác.

Theo khía cạnh thứ nhất, phương án của sáng chế đề xuất phương pháp cập nhật khóa, được áp dụng cho hệ thống truyền thông. Hệ thống truyền thông bao gồm đầu cuối và thiết bị mạng lõi. Đầu cuối truy cập thiết bị mạng lõi bằng cách sử dụng đồng thời cả công nghệ truy cập thứ nhất và công nghệ truy cập thứ hai. Phương pháp này bao gồm các bước: thực hiện, bởi thiết bị mạng lõi, việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất; và nếu điều kiện kích hoạt được đáp ứng, cập nhật, bởi thiết bị mạng lõi, khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai. Theo phương pháp này, thiết bị mạng lõi có thể thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, và khóa dùng cho kết nối thứ nhất có thể được cập nhật trong quy trình tái xác thực. Khi điều kiện kích hoạt thứ nhất được đáp ứng, thiết bị mạng lõi có thể cập nhật khóa dùng cho kết nối thứ hai. Khi điều kiện kích

hoạt thứ hai được đáp ứng, đầu cuối có thể cập nhật khóa dùng cho kết nối thứ hai. Theo cách này, khi đầu cuối truy cập nút AMF bằng cách sử dụng nhiều công nghệ truy cập, việc tái xác thực có thể được thực hiện trên đầu cuối qua kết nối thứ nhất với tiền đề là việc truyền thông thông thường mà được thực hiện giữa đầu cuối và nút AMF qua kết nối thứ hai không bị ảnh hưởng, và các khóa của hai kết nối được cập nhật.

Trong thiết kế khả thi, điều kiện kích hoạt là trạng thái của kết nối thứ hai, và trạng thái của kết nối thứ hai là trạng thái được kết nối hoặc trạng thái nghỉ.

Theo phương pháp, nếu xác định rằng việc tái xác thực cần được thực hiện trên đầu cuối qua kết nối thứ nhất, thiết bị mạng lõi còn cần xác định trạng thái của kết nối thứ hai, thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất chỉ khi kết nối thứ hai ở trạng thái nghỉ, và cập nhật các khóa dùng cho kết nối thứ nhất và kết nối thứ hai. Do kết nối thứ hai ở trạng thái nghỉ, quy trình cập nhật khóa không làm ảnh hưởng sự sử dụng bình thường của kết nối thứ hai bởi đầu cuối và thiết bị mạng lõi.

Trong thiết kế khả thi, điều kiện kích hoạt là kết nối thứ hai ở trạng thái nghỉ; và nếu thiết bị mạng lõi xác định để thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, và kết nối thứ hai ở trạng thái được kết nối, thiết bị mạng lõi gửi tin nhắn thứ nhất tới đầu cuối qua kết nối thứ nhất, trong đó tin nhắn thứ nhất được sử dụng để lệnh đầu cuối hoãn việc sử dụng kết nối thứ nhất. Theo phương pháp, nếu đầu cuối tiếp tục gửi tin nhắn NAS tới thiết bị mạng lõi qua kết nối thứ nhất, số đếm NAS có thể vòng lại (wrap around). Trong trường hợp này, đầu cuối được thông báo kịp thời để hoãn việc sử dụng kết nối thứ nhất.

Trong thiết kế khả thi, điều kiện kích hoạt là kết nối thứ hai ở trạng thái nghỉ; và thiết bị mạng lõi thu được ký hiệu nhận dạng khóa thứ nhất trong quá trình thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, trong đó ký hiệu nhận dạng khóa thứ nhất được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ nhất.

Trong thiết kế khả thi, sau khi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất, thiết bị mạng lõi có thể gửi thông tin lệnh tới đầu cuối qua kết nối thứ nhất, trong đó thông tin lệnh được sử dụng để lệnh đầu cuối cập nhật khóa tương ứng với kết nối thứ hai. Theo phương pháp, sau khi cập nhật khóa tương ứng với kết nối thứ hai, thiết bị mạng lõi lệnh đầu cuối kịp thời

để cập nhật khóa dùng cho kết nối thứ hai. Do đó, có thể được đảm bảo rằng thiết bị mạng lõi và đầu cuối thực hiện việc bảo vệ bảo mật trên tin nhắn bằng cách sử dụng cùng khóa khi truyền tin nhắn sau đó qua kết nối thứ hai.

Một cách tùy ý, thông tin lệnh có thể là ký hiệu nhận dạng khóa thứ nhất. Sau khi thu ký hiệu nhận dạng khóa thứ nhất, đầu cuối có thể cập nhật khóa dùng cho kết nối thứ hai tới khóa được nhận dạng bởi ký hiệu nhận dạng khóa thứ nhất.

Trong thiết kế khả thi, điều kiện kích hoạt là kết nối thứ hai ở trạng thái được kết nối; và phương pháp cập nhật, bởi thiết bị mạng lõi, khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai là: hoãn, bởi thiết bị mạng lõi, sử dụng kết nối thứ hai; và sau đó cập nhật, bởi thiết bị mạng lõi, khóa dùng cho kết nối thứ hai. Theo phương pháp, thiết bị mạng lõi hoãn việc sử dụng kết nối thứ hai, và sau đó cập nhật khóa dùng cho kết nối thứ hai. Điều này có thể tránh được việc thủ tục cập nhật khóa làm ảnh hưởng việc truyền thông thông thường mà được thực hiện bởi thiết bị mạng lõi qua kết nối thứ hai.

Trong thiết kế khả thi, trong quy trình xử lý trong đó thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, thiết bị mạng lõi có thể thu được ký hiệu nhận dạng khóa thứ nhất, và giữ lại ký hiệu nhận dạng khóa thứ hai và khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật, trong đó ký hiệu nhận dạng khóa thứ nhất được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ nhất, và ký hiệu nhận dạng khóa thứ hai được sử dụng để nhận dạng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật.

Trong thiết kế khả thi, sau khi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất, thiết bị mạng lõi có thể bắt đầu bộ định thời.

Trong thiết kế khả thi, điều kiện kích hoạt là:

thiết bị mạng lõi thu, trước khi bộ định thời kết thúc, tin nhắn thứ hai mà được gửi bởi đầu cuối qua kết nối thứ hai, và việc xác thực bảo mật mà được thực hiện bởi thiết bị mạng lõi trên tin nhắn thứ hai bằng cách sử dụng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật thành công;

bộ định thời kết thúc, và thiết bị mạng lõi không thu, trước khi bộ định thời kết

thúc, tin nhắn thứ hai mà được gửi bởi đầu cuối qua kết nối thứ hai;

sau khi bộ định thời kết thúc, thiết bị mạng lõi thu tin nhắn thứ hai mà được gửi bởi đầu cuối qua kết nối thứ hai và mà trên đó việc bảo vệ bảo mật không được thực hiện; hoặc

sau khi bộ định thời kết thúc, thiết bị mạng lõi thu tin nhắn thứ hai mà được gửi bởi đầu cuối qua kết nối thứ hai, và việc xác thực bảo mật mà được thực hiện bởi thiết bị mạng lõi trên tin nhắn thứ hai bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai thành công.

Trong thiết kế khả thi, thiết bị mạng lõi có thể gửi tin nhắn thứ ba tới đầu cuối qua kết nối thứ nhất, trong đó tin nhắn thứ ba bao gồm ký hiệu nhận dạng khóa thứ nhất, ký hiệu nhận dạng khóa thứ hai, hoặc thông tin lệnh, và thông tin lệnh được sử dụng để lệnh đầu cuối bắt đầu bộ định thời. Theo phương pháp, khi thiết bị mạng lõi xác định rằng việc tái xác thực cần được thực hiện qua kết nối thứ nhất, nếu kết nối thứ hai ở trạng thái được kết nối, thiết bị mạng lõi có thể thực hiện trực tiếp việc tái xác thực trên đầu cuối qua kết nối thứ nhất; trong quy trình tái xác thực, khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật có thể được giữ lại. Theo cách này, ngay cả khi thiết bị mạng lõi cập nhật khóa dùng cho kết nối thứ nhất bằng cách thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, khi thiết bị mạng lõi và đầu cuối truyền thông với nhau qua kết nối thứ hai, khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật có thể vẫn được sử dụng, và việc truyền thông thông thường qua kết nối thứ hai không bị ảnh hưởng. Ngoài ra, theo phương pháp, kết nối thứ nhất và kết nối thứ hai được tách riêng. Khi thực hiện việc xác thực trên đầu cuối qua kết nối thứ nhất, thiết bị mạng lõi không cần phát hiện trạng thái của kết nối thứ hai. Sau khi bộ định thời kết thúc, cả thiết bị mạng lõi và đầu cuối có thể chủ động cập nhật khóa dùng cho kết nối thứ hai, nhờ đó làm giảm các phí tổn tương tác báo hiệu giữa thiết bị mạng lõi và đầu cuối và đơn giản hóa việc thực hiện.

Trong thiết kế khả thi, sau khi thiết bị mạng lõi cập nhật khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai, thiết bị mạng lõi có thể xóa khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật và ký hiệu nhận dạng khóa thứ hai.

Trong thiết kế khả thi, nếu kết nối thứ hai ở trạng thái được kết nối, sau khi thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất, thiết bị mạng lõi có thể thiết đặt dấu thứ nhất, trong đó dấu thứ nhất được sử dụng để đánh dấu rằng thiết bị mạng lõi đã tái xác thực đầu cuối qua kết nối thứ nhất, hoặc được sử dụng để lệnh cập nhật khóa dùng cho kết nối thứ hai.

Trong thiết kế khả thi, điều kiện kích hoạt là kết nối thứ hai được chuyển đổi sang trạng thái nghỉ, và thiết bị mạng lõi xác định rằng dấu thứ nhất tồn tại.

Trong thiết kế khả thi, điều kiện kích hoạt là thiết bị mạng lõi xác định rằng dấu thứ nhất tồn tại; và phương pháp cập nhật, bởi thiết bị mạng lõi, khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai bao gồm bước: nếu kết nối thứ hai ở trạng thái được kết nối, hoãn, bởi thiết bị mạng lõi, sử dụng kết nối thứ hai; và sau đó cập nhật, bởi thiết bị mạng lõi, khóa dùng cho kết nối thứ hai.

Trong thiết kế khả thi, sau khi thiết bị mạng lõi cập nhật khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai, thiết bị mạng lõi có thể thu được ký hiệu nhận dạng khóa thứ ba, trong đó ký hiệu nhận dạng khóa thứ ba được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ nhất và khóa được cập nhật dùng cho kết nối thứ hai; và sau đó thiết bị mạng lõi gửi ký hiệu nhận dạng khóa thứ ba tới đầu cuối.

Trong thiết kế khả thi, sau khi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất, thiết bị mạng lõi gửi thông tin lệnh tới đầu cuối mà ở đó thông tin lệnh được sử dụng để lệnh đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Trong thiết kế khả thi, điều kiện kích hoạt là thiết bị mạng lõi xác định rằng dấu thứ hai tồn tại, và kết nối thứ hai ở trạng thái nghỉ; và sau khi thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, thiết bị mạng lõi có thể thiết đặt dấu thứ hai, trong đó dấu thứ hai được sử dụng để lệnh cập nhật khóa dùng cho kết nối thứ hai.

Theo khía cạnh thứ hai, phương án của sáng chế đề xuất phương pháp cập nhật khóa, được áp dụng cho hệ thống truyền thông. Hệ thống truyền thông bao gồm đầu cuối và thiết bị mạng lõi. Đầu cuối truy cập thiết bị mạng lõi bằng cách sử dụng đồng thời cả

công nghệ truy cập thứ nhất và công nghệ truy cập thứ hai. Phương pháp này bao gồm các bước: thực hiện, bởi đầu cuối, việc tái xác thực qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất; và nếu điều kiện kích hoạt được đáp ứng, cập nhật, bởi đầu cuối khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai. Theo phương pháp, đầu cuối cập nhật khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai chỉ khi điều kiện kích hoạt được đáp ứng, sao cho việc tái xác thực có thể được thực hiện trên đầu cuối qua kết nối thứ nhất với tiền đề là việc truyền thông thông thường mà được thực hiện giữa đầu cuối và nút AMF qua kết nối thứ hai không bị ảnh hưởng.

Trong thiết kế khả thi, điều kiện kích hoạt là trạng thái của kết nối thứ hai là trạng thái nghỉ.

Trong thiết kế khả thi, bước thực hiện, bởi đầu cuối, việc tái xác thực qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất bao gồm bước: trong quá trình thực hiện việc tái xác thực qua kết nối thứ nhất, giữ lại, bởi đầu cuối ký hiệu nhận dạng khóa và khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật, trong đó ký hiệu nhận dạng khóa được sử dụng để nhận dạng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật.

Trong thiết kế khả thi, điều kiện kích hoạt là bộ định thời kết thúc; và sau khi thực hiện việc tái xác thực qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất, đầu cuối có thể bắt đầu bộ định thời.

Trong thiết kế khả thi, sau khi bắt đầu bộ định thời bởi đầu cuối, phương pháp này còn bao gồm bước: trước khi bộ định thời kết thúc, gửi, bởi đầu cuối, tin nhắn tới thiết bị mạng lõi qua kết nối thứ hai, trong đó việc bảo vệ bảo mật được thực hiện trên tin nhắn bằng cách sử dụng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật; sau khi bộ định thời kết thúc, gửi, bởi đầu cuối, tin nhắn tới thiết bị mạng lõi qua kết nối thứ hai, trong đó việc bảo vệ bảo mật không được thực hiện trên tin nhắn; hoặc sau khi bộ định thời kết thúc, gửi, bởi đầu cuối, tin nhắn tới thiết bị mạng lõi qua kết nối thứ hai, trong đó việc bảo vệ bảo mật được thực hiện trên tin nhắn bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai.

Trong thiết kế khả thi, sau khi cập nhật, bởi đầu cuối, khóa dùng cho kết nối thứ

hai tương ứng với công nghệ truy cập thứ hai, phương pháp này còn bao gồm bước: xóa, bởi đầu cuối, khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật và ký hiệu nhận dạng khóa.

Theo khía cạnh thứ ba, phương án của sáng chế đề xuất thiết bị, và thiết bị này có chức năng thực hiện các thao tác của thiết bị mạng lõi trong thiết kế phương pháp nêu trên. Chức năng có thể được thực hiện bởi phần cứng, hoặc có thể được thực hiện bởi phần cứng bằng cách thực hiện phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên. Ví dụ, thiết bị này có thể là thiết bị mạng lõi, hoặc có thể là chip trong thiết bị mạng lõi.

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

Theo khía cạnh thứ tư, phương án của sáng chế đề xuất thiết bị, và thiết bị này có chức năng thực hiện các thao tác của đầu cuối trong thiết kế phương pháp nêu trên. Chức năng có thể được thực hiện bởi phần cứng, hoặc có thể được thực hiện bởi phần cứng bằng cách thực hiện phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên. Ví dụ, thiết bị này có thể là đầu cuối hoặc có thể là chip trong đầu cuối.

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

Theo khía cạnh thứ năm, phương án của sáng chế đề xuất hệ thống truyền thông,

trong đó hệ thống này bao gồm đầu cuối và thiết bị mạng lõi được mô tả trong các khía cạnh nêu trên. Một cách tùy ý, hệ thống có thể còn bao gồm trạm gốc, nút N3IWF, và đầu cuối và thiết bị mạng lõi được mô tả trong các khía cạnh nêu trên.

Theo khía cạnh thứ sáu, phương án của sáng chế đề xuất phương tiện lưu trữ bằng máy tính, được tạo cấu hình để lưu trữ các lệnh phần mềm máy tính được sử dụng bởi thiết bị mạng lõi nêu trên. Phương tiện lưu trữ bằng máy tính chứa chương trình được thiết kế để thực hiện khía cạnh thứ nhất.

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

Theo khía cạnh thứ tám, phương án của sáng chế đề xuất sản phẩm chương trình máy tính bao gồm lệnh. Khi sản phẩm chương trình máy tính được chạy trên máy tính, máy tính được cho phép để thực hiện phương pháp được mô tả theo khía cạnh thứ nhất.

Theo khía cạnh thứ chín, phương án của sáng chế đề xuất sản phẩm chương trình máy tính bao gồm lệnh. Khi sản phẩm chương trình máy tính được chạy trên máy tính, máy tính được cho phép để thực hiện phương pháp được mô tả theo khía cạnh thứ hai.

Theo khía cạnh thứ mười, phương án của sáng chế đề xuất hệ thống chip, được áp dụng cho thiết bị mạng lõi. Hệ thống chip 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 tuyến. Ít nhất một bộ nhớ lưu trữ lệnh. Lệnh được thực hiện bởi bộ xử lý để thực hiện các hoạt động của thiết bị mạng lõi theo phương pháp được mô tả theo khía cạnh thứ nhất.

Theo khía cạnh thứ mười một, phương án của sáng chế đề xuất hệ thống chip, được áp dụng cho đầu cuối. Hệ thống chip 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 tuyến. Ít nhất một bộ nhớ lưu trữ lệnh. Lệnh được thực hiện bởi bộ xử lý để thực hiện các hoạt động của đầu cuối theo phương pháp được mô tả theo khía cạnh thứ hai.

Theo phương pháp được đề xuất trong các phương án của sáng chế, thiết bị mạng lõi có thể thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, và khóa dùng

cho kết nối thứ nhất có thể được cập nhật trong quy trình tái xác thực. Khi điều kiện kích hoạt thứ nhất được đáp ứng, thiết bị mạng lõi có thể cập nhật khóa dùng cho kết nối thứ hai. Khi điều kiện kích hoạt thứ hai được đáp ứng, đầu cuối có thể cập nhật khóa dùng cho kết nối thứ hai. Theo cách này, khi đầu cuối truy cập nút AMF bằng cách sử dụng nhiều công nghệ truy cập, việc tái xác thực có thể được thực hiện trên đầu cuối qua kết nối thứ nhất với tiền đề là việc truyền thông thông thường mà được thực hiện giữa đầu cuối và nút AMF qua kết nối thứ hai không bị ảnh hưởng, và các khóa của hai kết nối được cập nhật.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ giản lược của cấu trúc mạng khả thi theo phương án của sáng chế;

Fig.2 là sơ đồ giản lược của cấu trúc mạng khả thi khác theo phương án của sáng chế;

Fig.3 là sơ đồ giản lược của cấu trúc khóa theo phương án của sáng chế;

Fig.4 là lưu đồ của phương pháp tạo khóa theo phương án của sáng chế;

Fig.5 là lưu đồ của phương pháp tạo khóa khác theo phương án của sáng chế;

Fig.6 là lưu đồ của phương pháp tạo khóa khác theo phương án của sáng chế;

Fig.7 là lưu đồ của phương pháp tạo khóa khác theo phương án của sáng chế;

Fig.8 là lưu đồ của phương pháp tạo khóa khác theo phương án của sáng chế;

Fig.9 là lưu đồ của phương pháp tạo khóa khác theo phương án của sáng chế;

Fig.10 là lưu đồ của phương pháp tạo khóa khác theo phương án của sáng chế;

Fig.11 là lưu đồ của phương pháp tạo khóa khác theo phương án của sáng chế;

Fig.12 là lưu đồ của phương pháp tạo khóa khác theo phương án của sáng chế;

Fig.13 là lưu đồ của phương pháp tạo khóa khác theo phương án của sáng chế;

Fig.14 là sơ đồ cấu trúc giản lược của thiết bị theo phương án của sáng chế;

Fig.15 là sơ đồ cấu trúc giản lược của thiết bị mạng lõi theo phương án của sáng chế;

Fig.16 là sơ đồ cấu trúc giản lược của thiết bị khác theo phương án của sáng chế; và

Fig.17 là sơ đồ cấu trúc giản lược của thiết bị theo phương án của sáng chế.

Mô tả chi tiết sáng chế

Phần sau đây còn mô tả chi tiết sáng chế này có dựa trên các hình vẽ kèm theo. Phương pháp hoạt động cụ thể theo các phương án của phương pháp có thể cũng được áp dụng cho phương án của thiết bị hoặc phương án của hệ thống. Trong phần mô tả sáng chế, trừ khi có quy định khác, "nhiều" có nghĩa là hai hoặc nhiều hơn hai.

Các cấu trúc hệ thống và các kịch bản dịch vụ được mô tả trong sáng chế này có mục đích mô tả rõ hơn các giải pháp kỹ thuật trong sáng chế này, nhưng không có mục đích giới hạn các giải pháp kỹ thuật được đề xuất trong sáng chế này. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể nhận biết rằng do các cấu trúc hệ thống phát triển và kịch bản dịch vụ mới xuất hiện, các giải pháp kỹ thuật được đề xuất trong sáng chế này áp dụng được cho vấn đề kỹ thuật tương tự.

Cần chú ý rằng, trong sáng chế này, thuật ngữ "ví dụ" hoặc "theo ví dụ" được sử dụng để thể hiện việc đưa ra ví dụ, sự minh họa, hoặc sự mô tả. Phương án hoặc sơ đồ thiết kế bất kỳ được mô tả là "ví dụ" hoặc "theo ví dụ" trong sáng chế này cần được giải thích là ưu tiên hơn hoặc có nhiều ưu điểm hơn phương án hoặc sơ đồ thiết kế khác. Chính xác là, việc sử dụng thuật ngữ "ví dụ" hoặc "theo ví dụ" hoặc tương tự có mục đích thể hiện mô hình tương ứng theo cách cụ thể.

Các phương án của sáng chế có thể được áp dụng cho hệ thống truyền thông mà hỗ trợ đầu cuối trong việc truy cập mạng bằng cách sử dụng ít nhất hai công nghệ truy cập. Ví dụ, hệ thống truyền thông có thể là hệ thống truyền thông không dây thế hệ tiếp theo, ví dụ, hệ thống truyền thông 5G. Fig.1 là sơ đồ giản lược của cấu trúc mạng khả thi theo sáng chế này. Cấu trúc mạng này bao gồm các phần sau đây:

Nút AMF: nút AMF là phần tử mạng chịu trách nhiệm quản lý tính di động, và có thể được tạo cấu hình để thực hiện các chức năng ngoài quản lý phiên trong các chức năng thực thể quản lý tính di động (mobility management entity, viết tắt là MME), ví dụ, các chức năng chẳng hạn như ngăn chặn hợp pháp và cấp quyền truy cập.

Nút chức năng quản lý phiên (session management function, viết tắt là SMF): nút SMF được tạo cấu hình để cấp phát tài nguyên phiên tới mặt phẳng người dùng.

Nút chức năng máy chủ xác thực (authentication server function, viết tắt là

AUSF): khi thực hiện việc xác thực trên đầu cuối, AUSF chịu trách nhiệm xác nhận và truyền thông số cần được xác thực và thực hiện việc xác thực độ tin cậy của đầu cuối. Các chức năng chính bao gồm thu yêu cầu xác thực được gửi bởi nút chức năng neo bảo mật (security anchor function, viết tắt là SEAF) và lựa chọn phương pháp xác thực. Khi phương pháp xác thực chấp nhận khóa và xác thực giao thức xác thực mở rộng được (extensible authentication protocol authentication and key agreement, viết tắt là EAP-AKA') được sử dụng, nút AUSF có thể hoàn thành việc xác thực được thực hiện bởi phía mạng trên đầu cuối.

Nút SEAF: nút SEAF có thể là một phần của nút AMF, hoặc có thể là phần tử mạng độc lập. Nút SEAF chịu trách nhiệm chính trong việc khởi tạo yêu cầu xác thực tới AUSF, và hoàn thành việc xác thực được thực hiện bởi phía mạng trên đầu cuối trong quá trình xác thực chấp nhận khóa và xác thực hệ thống gói tin cải tiến (evolved packet system authentication and key agreement, viết tắt là EPS-AKA*).

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

Mạng dữ liệu (data network, viết tắt là DN): DN là mạng được sử dụng để cung cấp dữ liệu bên ngoài, ví dụ, mạng Internet (Internet).

Nút mạng truy cập (rađio) ((radio) access network, viết tắt là (R)AN): (R)AN có thể sử dụng các công nghệ truy cập khác nhau. Hiện nay, có hai loại công nghệ truy cập rađio: công nghệ truy cập 3GPP (ví dụ, công nghệ truy cập rađio được sử dụng trong hệ thống 3G, 4G, hoặc 5G) và công nghệ truy cập không phải 3GPP. Công nghệ truy cập 3GPP là công nghệ truy cập mà tuân theo đặc tả kỹ thuật tiêu chuẩn 3GPP. Mạng truy cập sử dụng công nghệ truy cập 3GPP là mạng truy cập rađio (RAN), và thiết bị truy cập mạng trong hệ thống 5G là trạm gốc nút thế hệ tiếp theo (next generation node base-station, viết tắt là gNB). Công nghệ truy cập không phải 3GPP là công nghệ truy cập mà không tuân theo đặc tả kỹ thuật tiêu chuẩn 3GPP, ví dụ, công nghệ giao diện không khí được thể hiện bởi điểm truy cập (access point, viết tắt là AP) WiFi.

Đầu cuối: đầu cuối trong sáng chế này là thiết bị có các chức năng thu và gửi không dây, và có thể được triển khai trên mặt đất, bao gồm trong nhà hoặc ngoài trời,

cầm tay, hoặc trên xe. Nó có thể cũng được triển khai trên mặt nước (chẳng hạn như tàu thuyền) hoặc trong không khí (chẳng hạn như máy bay, khinh khí cầu, và vệ tinh). Đầu cuối có thể bao gồm các loại khác nhau của thiết bị người dùng (user equipment, viết tắt là UE), điện thoại di động (mobile phone), máy tính bảng (pad), các máy tính có các chức năng thu và gửi không dây, các cạc dữ liệu không dây, các thiết bị đầu cuối thực tế ảo (virtual reality, viết tắt là VR), các thiết bị đầu cuối thực tế tăng cường (augmented reality, viết tắt là AR), các thiết bị đầu cuối truyền thông kiểu máy (machine type communication, viết tắt là MTC), các thiết bị đầu cuối trong điều khiển công nghiệp (industrial control), các thiết bị đầu cuối trong việc tự lái (self driving), các thiết bị đầu cuối trong y tế từ xa (remote medical), các thiết bị đầu cuối trong lưới điện thông minh (smart grid), các thiết bị đầu cuối trong an toàn giao thông (transportation safety), các thiết bị đầu cuối trong thành phố thông minh (smart city), các thiết bị mang theo được (chẳng hạn như đồng hồ thông minh, vòng đeo thông minh, và máy đo bước), và tương tự. Trong các hệ thống sử dụng các công nghệ truy cập rađio khác nhau, tên của các đầu cuối có các chức năng truyền thông không dây tương tự có thể khác nhau. Chỉ với mục đích mô tả dễ dàng hơn, trong các phương án của sáng chế, thiết bị nêu trên có các chức năng truyền thông thu và gửi không dây được gọi chung là các đầu cuối.

Đặc biệt là, đầu cuối trong sáng chế này lưu trữ khóa dài hạn và chức năng liên quan. Khi thực hiện việc xác thực hai chiều với nút mạng lõi (ví dụ, nút AMF, nút AUSF, hoặc nút SEAF), đầu cuối có thể xác nhận độ tin cậy của mạng bằng cách sử dụng cặp khóa dài hạn và chức năng liên quan.

Thiết bị mạng truy cập: thiết bị truy cập mạng trong các phương án của sáng chế là thiết bị mà cung cấp chức năng truyền thông không dây cho đầu cuối. Ví dụ, thiết bị truy cập mạng có thể là trạm gốc (base station, viết tắt là BS), và trạm gốc có thể bao gồm các dạng khác nhau trong số trạm gốc macrô, trạm gốc micrô, trạm gốc chuyển tiếp, điểm truy cập, và tương tự. Trong các hệ thống sử dụng các công nghệ truy cập rađio khác nhau, tên của các thiết bị có chức năng trạm gốc có thể khác nhau. Ví dụ, trong hệ thống 5G, thiết bị là trạm gốc nút thế hệ tiếp theo, mà có thể được thể hiện là gNB. Trong hệ thống phát triển dài hạn (long term evolution, viết tắt là LTE), thiết bị là nút B cải tiến (evolved NodeB, viết tắt là eNB hoặc eNodeB). Trong hệ thống truyền thông

thế hệ thứ ba (3rd generation, viết tắt là 3G), thiết bị là nút B (Node B), và v.v.. Để mô tả dễ dàng hơn, trong các phương án của sáng chế, thiết bị nêu trên mà cung cấp chức năng truyền thông mạng cho đầu cuối được gọi chung là các thiết bị truy cập mạng.

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

Nút chức năng lưu trữ mạng (network repository function, viết tắt là NRF): nút NRF được tạo cấu hình để tìm kiếm phần tử mạng cụ thể và duy trì chức năng mạng (network function, viết tắt là NF).

Nút chức năng điều khiển chính sách (policy control function, viết tắt là PCF): nút PCF lưu trữ quy tắc chất lượng dịch vụ (quality of service, viết tắt là QoS) cuối cùng. Trạm gốc có thể cấp phát tài nguyên thích hợp tới kênh truyền mặt phẳng người dùng dựa vào quy tắc QoS được cung cấp bởi nút SMF.

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

Nút chức năng ứng dụng (application function, viết tắt là AF): nút AF có thể nằm bên trong DN, và thuộc về phần tử mạng chức năng được triển khai trong bên thứ ba. Phần tử mạng này được sử dụng chủ yếu để thông báo nút PCF của yêu cầu dịch vụ cuối cùng của công ty bên thứ ba cho ứng dụng. Nút PCF có thể tạo quy tắc QoS tương ứng dựa vào yêu cầu dịch vụ, để đảm bảo rằng dịch vụ được cung cấp bởi mạng đáp ứng yêu cầu được đề xuất bởi bên thứ ba.

Trong các phương án của sáng chế, đầu cuối có thể truy cập nút AMF bằng cách sử dụng ít nhất hai công nghệ truy cập. Ví dụ, ít nhất hai công nghệ truy cập bao gồm công nghệ truy cập 3GPP và công nghệ truy cập không phải 3GPP. Các phương án của sáng chế còn đề xuất sơ đồ giản lược của cấu trúc mạng khả thi, như được thể hiện trên Fig.2. Cấu trúc mạng bao gồm nút AMF, nút AUSF, nút SMF, nút UPF, nút UDM (hoặc nút chức năng lưu trữ và xử lý đáng tin cậy sự xác thực (authentication credential storage and processing function, viết tắt là APRF)), đầu cuối và nút chức năng liên kết mạng không phải 3GPP (non-3GPP interworking function, viết tắt là N3IWF).

Đối với nút AMF, nút AUSF, nút SMF, nút UPF, nút UDM, và đầu cuối đề cập

đến 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 đầu cuối trong việc truy cập nút AMF bằng cách sử dụng công nghệ truy cập không phải 3GPP.

Dựa trên cấu trúc mạng được thể hiện trên Fig.2, đầu cuối có thể truy cập nút AMF bằng cách sử dụng đồng thời cả công nghệ truy cập 3GPP và công nghệ truy cập không phải 3GPP. Thiết bị truy cập mạng trong công nghệ truy cập 3GPP có thể là trạm gốc trong mạng 5G, trạm gốc trong mạng 4G, hoặc trạm gốc được sử dụng trong mạng viễn thông trong tương lai. Công nghệ truy cập không phải 3GPP có thể là mạng công nghệ truy cập được sử dụng bởi mạng không phải viễn thông, chẳng hạn như mạng WiFi hoặc mạng cố định. Công nghệ truy cập 3GPP được thể hiện đơn giản là 3GPP, và công nghệ truy cập không phải 3GPP được thể hiện đơn giản là không phải 3GPP. Tuyến 1 trên Fig.2 là tuyến mà trên đó đầu cuối truy cập nút AMF bằng cách sử dụng công nghệ truy cập 3GPP, và tuyến 2 là tuyến mà trên đó đầu cuối truy cập nút AMF bằng cách sử dụng công nghệ truy cập không phải 3GPP. Đầu cuối có thể truy cập nút AMF bằng cách sử dụng cổng tương ứng với công nghệ truy cập tương ứng, thực thể chức năng được triển khai liên kết với cổng, hoặc thực thể có chức năng cổng. Cổng tương ứng với công nghệ không phải 3GPP có thể là nút N3IWF, hoặc có thể là cổng được sử dụng khi đầu cuối truy cập nút AMF bằng cách sử dụng mạng cố định công nghệ truy cập, ví dụ, BNG (cổng mạng băng rộng, cổng mạng cố định). Thực thể có chức năng cổng là đầu cuối ngang hàng được kết nối với nút AMF, ví dụ, đầu cuối khác của giao diện N2 trong mạng 5G và đầu cuối khác của giao diện S1 trong mạng 4G.

Khi đầu cuối truy cập nút AMF bằng cách sử dụng đồng thời cả 3GPP và công nghệ truy cập không phải 3GPP, nếu đầu cuối cần gửi tin nhắn NAS tới nút AMF, trong cách thực hiện khả thi, tin nhắn NAS có thể được phân chia thành ít nhất hai khối tin nhắn. Một số khối tin nhắn được truyền bằng cách sử dụng công nghệ truy cập 3GPP, và một số khối tin nhắn khác được truyền bằng cách sử dụng công nghệ truy cập không phải 3GPP. Ví dụ, tin nhắn NAS có thể được phân chia thành năm khối tin nhắn: 1, 2, 3, 4, và 5. Khối tin nhắn 2 và 4 được truyền bằng cách sử dụng công nghệ truy cập 3GPP, và khối tin nhắn 1, 3, và 5 được truyền bằng cách sử dụng công nghệ truy cập không phải 3GPP. Theo cách thực hiện khả thi khác, đầu cuối có thể truyền toàn bộ tin nhắn

NAS bằng cách sử dụng công nghệ truy cập 3GPP, và truyền toàn bộ tin nhắn NAS khác bằng cách sử dụng công nghệ truy cập không phải 3GPP.

Đầu tiên, các thuật ngữ liên quan đến các phương án của sáng chế được giải thích.

(1) Trạng thái RM

RM được sử dụng để điều khiển đầu cuối và mạng. Trạng thái RM bao gồm hai trạng thái: trạng thái đăng ký và trạng thái bỏ đăng ký.

Khi đầu cuối ở trạng thái bỏ đăng ký, đầu cuối có thể cố gắng đi vào trạng thái đăng ký bằng cách gửi thủ tục đăng ký tới thiết bị mạng lõi (ví dụ, nút AMF). Sau khi thu tin nhắn chấp nhận đăng ký (registration accept) được phản hồi bởi nút AMF, đầu cuối đi vào trạng thái đăng ký. Khi đầu cuối được tắt nguồn hoặc bị lỗi đăng ký, đầu cuối quay lại trạng thái bỏ đăng ký.

Khi đầu cuối ở trạng thái đăng ký, nút AMF có thông tin vị trí, thông tin định tuyến, và thông tin ngữ cảnh bảo mật của đầu cuối và đầu cuối có thông tin ngữ cảnh bảo mật.

Khi đầu cuối ở trạng thái bỏ đăng ký, nút AMF không có thông tin vị trí mà cũng không có thông tin định tuyến của đầu cuối và cả nút AMF và đầu cuối có thông tin ngữ cảnh bảo mật. Thông tin ngữ cảnh bảo mật bao gồm khóa NAS và thuật toán liên quan. Nếu đầu cuối quay lại từ trạng thái đăng ký sang trạng thái bỏ đăng ký, đầu cuối không chỉ lưu trữ thông tin ngữ cảnh bảo mật, mà còn lưu trữ thông tin nhận dạng tạm thời được cấp phát bởi nút AMF trong suốt quá trình đăng ký trước đó, sao cho đầu cuối có thể không khởi tạo thủ tục xác thực khi đầu cuối đăng ký lại với mạng, nhờ đó làm giảm trễ trong việc truy cập mạng.

(2) Trạng thái CM

Trạng thái CM bao gồm trạng thái được kết nối và trạng thái nghỉ.

Khi đầu cuối ở trạng thái được kết nối, có kết nối truyền thông giữa đầu cuối và mạng, nghĩa là, dữ liệu đang được trao đổi giữa đầu cuối và nút AMF.

Khi đầu cuối ở trạng thái nghỉ, không có kết nối truyền thông giữa đầu cuối và mạng, nghĩa là, không có dữ liệu đang được trao đổi giữa đầu cuối và nút AMF.

(3) Chuyển đổi trạng thái

Khi đầu cuối chưa truy cập mạng, đầu cuối ở trạng thái nghỉ và trạng thái bỏ đăng

ký. Trong trường hợp này, không có thông tin ngữ cảnh bảo mật giữa đầu cuối và nút AMF. Đầu cuối đầu tiên chuyển đổi từ trạng thái nghỉ sang trạng thái được kết nối, và sau đó đầu cuối có thể khởi tạo thủ tục đăng ký, và chuyển đổi từ trạng thái bỏ đăng ký sang trạng thái đăng ký. Trong trường hợp này, đầu cuối có khóa NAS và thuật toán bảo mật. Nếu đầu cuối không cần trao đổi dữ liệu với mạng sau đó, đầu cuối có thể quay lại trạng thái nghỉ, và đầu cuối vẫn trong trạng thái đăng ký sau khi quay lại trạng thái nghỉ.

Khi đầu cuối quay lại từ trạng thái được kết nối sang trạng thái nghỉ, thông tin ngữ cảnh bảo mật được lưu trữ bởi đầu cuối là khóa NAS và thuật toán bảo mật. Khi đầu cuối quay lại từ trạng thái đăng ký sang trạng thái không đăng ký, đầu cuối lưu trữ khóa NAS, thuật toán bảo mật, và thông tin nhận dạng tạm thời được cấp phát bởi AMF trong suốt quá trình đăng ký trước đó.

Cần chú ý rằng việc chuyển đổi trạng thái trong sáng chế này có nghĩa là trạng thái CM của đầu cuối trong thiết bị mạng lõi quay lại từ một trạng thái sang trạng thái khác. Ví dụ, chuyển đổi từ trạng thái được kết nối sang trạng thái nghỉ có nghĩa là trạng thái CM của đầu cuối trong thiết bị mạng lõi quay lại từ trạng thái được kết nối sang trạng thái nghỉ. Ví dụ, khi đầu cuối gửi tin nhắn yêu cầu đăng ký tới thiết bị mạng lõi, đầu cuối ở trạng thái được kết nối. Sau khi thiết bị mạng lõi gửi tin nhắn hoàn thành đăng ký tới đầu cuối nếu đầu cuối không gửi ngay tin nhắn tới thiết bị mạng lõi, hoặc đầu cuối không gửi tin nhắn tới thiết bị mạng lõi trong khoảng thời gian cụ thể được điều khiển bởi bộ định thời, đầu cuối quay lại trạng thái nghỉ.

Ngoài ra, thời gian được sử dụng cho thao tác "chuyển đổi" không giới hạn trong các phương án của sáng chế. Cụ thể là, thời gian được yêu cầu để chuyển đổi kết nối thứ hai từ trạng thái được kết nối sang trạng thái nghỉ có thể được điều khiển bởi bộ định thời, hoặc có thể được điều khiển bởi thủ tục chuyển đổi. Điều này không giới hạn trong sáng chế này.

(4) Công nghệ truy cập thứ nhất và công nghệ truy cập thứ hai

Đầu cuối hỗ trợ việc truy cập mạng bằng cách sử dụng đồng thời cả công nghệ truy cập thứ nhất và công nghệ truy cập thứ hai. Công nghệ truy cập thứ nhất là công nghệ truy cập 3GPP, và công nghệ truy cập thứ hai là công nghệ truy cập không phải 3GPP. Như một sự lựa chọn, công nghệ truy cập thứ nhất là công nghệ truy cập không

phải 3GPP, và công nghệ truy cập thứ hai là công nghệ truy cập 3GPP. Tất nhiên, sáng chế này không giới hạn ở đó. Công nghệ truy cập thứ nhất và công nghệ truy cập thứ hai có thể là công nghệ truy cập khác như một sự lựa chọn được hỗ trợ khi đầu cuối truyền thông với thiết bị mạng lõi.

Kết nối thứ nhất là kết nối mà qua đó đầu cuối truy cập thiết bị mạng lõi thứ nhất bằng cách sử dụng công nghệ truy cập thứ nhất.

Kết nối thứ hai là kết nối mà qua đó đầu cuối truy cập thiết bị mạng lõi thứ hai bằng cách sử dụng công nghệ truy cập thứ hai.

Đầu cuối sử dụng kết nối thứ nhất và kết nối thứ hai cùng là đầu cuối nhưng thiết bị mạng lõi thứ nhất và thiết bị mạng lõi thứ hai có thể giống hoặc khác nhau. Theo sáng chế này, ví dụ trong đó đầu cuối hỗ trợ việc truy cập cùng thiết bị mạng lõi bằng cách sử dụng cả kết nối thứ nhất và kết nối thứ hai được sử dụng đồng thời.

Ngoài ra, kết nối thứ nhất và kết nối thứ hai trong sáng chế này có thể là kết nối trực tiếp hoặc kết nối gián tiếp giữa đầu cuối và thiết bị mạng lõi. Ví dụ, kết nối thứ hai là kết nối mà qua đó đầu cuối truy cập cổng thiết bị bằng cách sử dụng công nghệ truy cập thứ hai, và truy cập phần tử mạng của mạng lõi bằng cách sử dụng thiết bị cổng. Fig.2 được sử dụng làm ví dụ. Đầu cuối có thể truy cập nút AMF bằng cách sử dụng công nghệ truy cập 3GPP. Kết nối thứ nhất có thể được hiểu là tuyến truyền thông giữa đầu cuối và nút AMF khi đầu cuối sử dụng công nghệ truy cập 3GPP, nghĩa là, tuyến 1. Như một sự lựa chọn, đầu cuối có thể truy cập nút AMF bằng cách sử dụng công nghệ truy cập không phải 3GPP. Khi đầu cuối truy cập nút AMF bằng cách sử dụng công nghệ truy cập không phải 3GPP, đầu cuối không truyền thông trực tiếp với nút AMF, nhưng truyền thông với nút AMF bằng cách sử dụng nút N3IWF. Kết nối thứ hai là kết nối giữa đầu cuối và nút N3IWF và kết nối giữa nút N3IWF và nút AMF, và có thể cũng được hiểu là tuyến 2.

(5) Việc tái xác thực

Việc tái xác thực có nghĩa là: khi thiết bị mạng lõi nhận thấy rằng loại thông số sắp không sẵn có, ví dụ, số đếm NAS sắp vòng lại, hoặc điều kiện kích hoạt được đáp ứng dựa vào yêu cầu cấu hình của người thao tác, thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối. Trong quy trình xử lý trong đó thiết bị mạng lõi thực hiện việc

tái xác thực trên thiết bị đầu cuối mạng lõi trao đổi tin nhắn với đầu cuối. Đầu cuối so sánh thông số cần được xác nhận được cung cấp bởi mạng lõi với thông số khác được tạo ra bởi đầu cuối và thiết bị mạng lõi so sánh thông số cần được xác nhận được cung cấp bởi đầu cuối với thông số khác được tạo ra bởi thiết bị mạng lõi. Nếu thông số cần được xác nhận được cung cấp bởi thiết bị mạng lõi giống như thông số được tạo ra bởi đầu cuối hoặc nếu thông số cần được xác nhận được cung cấp bởi đầu cuối giống như thông số được tạo ra bởi thiết bị mạng lõi, việc xác nhận xác thực được thực hiện giữa đầu cuối và thiết bị mạng lõi thành công.

Ví dụ, thủ tục xác nhận xác thực có thể là thủ tục 5G AKA trong mạng 5G, thủ tục EAP-AKA', hoặc thủ tục EPS AKA trong mạng LTE.

Một cách tùy ý, thủ tục tái xác thực trong các phương án của sáng chế có thể bao gồm thủ tục xác nhận xác thực và thủ tục kích hoạt khóa. Cụ thể là, trong thủ tục xác nhận xác thực, thiết bị mạng lõi và đầu cuối có thể xác nhận xem thông tin cần xác nhận được gửi bởi thiết bị còn lại có chính xác hay không. Trong thủ tục kích hoạt khóa, thiết bị mạng lõi gửi tin nhắn lệnh chế độ bảo mật NAS (security mode command, viết tắt là SMC) tới đầu cuối và thu tin nhắn hoàn thành chế độ bảo mật NAS (security mode complete, viết tắt là SMP) từ đầu cuối.

(6) Thiết bị mạng lõi

Thiết bị mạng lõi là thiết bị trong mạng 3GPP khác với thiết bị truy cập mạng. Thiết bị mạng lõi có thể là nút AMF, nút SMF, hoặc có thể là mạng thiết bị chẳng hạn như nút SEAF, nút AUSF, hoặc nút UDM.

Thiết bị mạng lõi không giới hạn tới thiết bị mà xác nhận đầu cuối, ví dụ, nút AUSF trong mạng 5G. Như một sự lựa chọn, thiết bị mạng lõi có thể là thiết bị tham gia vào thủ tục xác thực, ví dụ, thiết bị (ví dụ, nút AMF) được tạo cấu hình để chuyển tiếp tin nhắn trong thủ tục xác thực. Một cách tùy ý, thiết bị mạng lõi có thể còn có chức năng độc lập, ví dụ, chức năng SEAF, được triển khai cùng với thiết bị mạng lõi.

Ngoài ra, thiết bị mạng lõi mà khởi tạo thủ tục tái xác thực tới đầu cuối có thể giống hoặc khác với thiết bị mạng lõi mà thực hiện việc xác nhận xác thực trên đầu cuối. Sự xác nhận xác thực có nghĩa là thiết bị mạng lõi xác nhận xem thông tin cần được xác thực được gửi bởi đầu cuối có chính xác hay không. Ví dụ, trong kịch bản 5G AKA,

thiết bị mạng lõi mà khởi tạo thủ tục tái xác thực là nút AMF, hoặc là nút SEAF được triển khai cùng với nút AMF. Trong kịch bản này, thiết bị mạng lõi mà khởi tạo thủ tục tái xác thực có thể là nút AMF, và thiết bị mạng lõi mà thực hiện việc xác nhận xác thực trên đầu cuối là nút SEAF trong nút AMF. Trong trường hợp này, có thể được xem xét rằng thiết bị mạng lõi mà khởi tạo thủ tục tái xác thực tới đầu cuối giống như thiết bị mạng lõi mà thực hiện việc xác nhận xác thực trên đầu cuối và cả hai đều là nút AMF. Trong kịch bản này, nếu nút SEAF không được triển khai cùng với nút AMF, nghĩa là, nút SEAF cũng là thiết bị mạng lõi độc lập, thiết bị mạng lõi mà khởi tạo thủ tục tái xác thực tới đầu cuối khác với thiết bị mà thực hiện việc xác nhận xác thực trên đầu cuối.

Theo ví dụ khác, trong kịch bản 5G EAP-AKA', thiết bị mạng lõi mà khởi tạo thủ tục tái xác thực có thể là nút AMF, và thiết bị mà thực hiện việc xác nhận xác thực trên đầu cuối là nút AUSF. Trong trường hợp này, thiết bị mạng lõi mà khởi tạo thủ tục tái xác thực tới đầu cuối khác với thiết bị mạng lõi mà thực hiện việc xác nhận xác thực trên đầu cuối.

(7) Khóa

Cả khóa dùng cho kết nối thứ nhất và khóa dùng cho kết nối thứ hai là khóa NAS. Khóa NAS bao gồm khóa mật mã và khóa bảo vệ tính toàn vẹn. Khóa dùng cho kết nối thứ nhất được sử dụng để thực hiện việc bảo vệ bảo mật trên tin nhắn mà được truyền giữa đầu cuối và thiết bị mạng lõi qua kết nối thứ nhất, và khóa dùng cho kết nối thứ hai được sử dụng để thực hiện việc bảo vệ bảo mật trên tin nhắn mà được truyền giữa đầu cuối và thiết bị mạng lõi qua kết nối thứ hai.

Cấu trúc khóa trong các phương án của sáng chế được thể hiện trên Fig.3. Trên Fig.3, khóa lớp phía trên có thể được sử dụng làm thông số tạo của khóa lớp phía dưới. Một cách tùy ý, trong quy trình tái xác thực, khóa dùng cho kết nối thứ nhất và khóa khác được sử dụng để thu nhận kết nối thứ nhất có thể được tạo ra. Ví dụ, trên Fig.3, tất cả các khóa ngoại trừ khóa lớp thứ nhất, K, được cập nhật trong quy trình tái xác thực. Ví dụ, khóa dùng cho kết nối thứ nhất có thể là KNASint, KNASenc, KRRCint, KRRCenc, KUPint, KUPenc, và tương tự.

Một cách tùy ý, nếu khóa cũ cần được giữ lại trong quy trình cập nhật khóa, khóa cũ được giữ lại có thể là ít nhất một trong số KNASint, KNASenc, KgNB, NH, KRRCint,

KRRCenc, KUPint, KUPenc, hoặc KN3IWF. Một cách tùy ý, KAMF, KSEAF, hoặc KAUSF cũng được giữ lại.

Dựa trên các hình vẽ từ Fig.1 đến Fig.3, phương án của sáng chế đề xuất phương pháp cập nhật khóa, được áp dụng cho hệ thống truyền thông. Hệ thống truyền thông bao gồm thiết bị mạng lõi và đầu cuối. Đầu cuối truy cập thiết bị mạng lõi bằng cách sử dụng đồng thời cả công nghệ truy cập thứ nhất và công nghệ truy cập thứ hai. Như được thể hiện trên Fig.4, phương pháp này bao gồm các bước sau đây.

Bước 401. Thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất; một cách tương ứng, đầu cuối thực hiện việc tái xác thực trên thiết bị mạng lõi qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất.

Trong quy trình xử lý trong đó thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, cả thiết bị mạng lõi và đầu cuối có thể cập nhật khóa dùng cho kết nối thứ nhất. Ví dụ, thiết bị mạng lõi và thiết bị đầu cuối có thể tạo các khóa mới dùng cho kết nối thứ nhất, ví dụ, các khóa chẳng hạn như KAUSF, KSEAF, KAMF, KNASint, hoặc KNASenc.

Một cách tùy ý, trong quy trình xử lý trong đó thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, thiết bị mạng lõi có thể còn thu được ký hiệu nhận dạng khóa thứ nhất, trong đó ký hiệu nhận dạng khóa thứ nhất được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ nhất. Khi nút mạng lõi là nút AMF, có ba phương pháp sau đây để thu nhận ký hiệu nhận dạng khóa thứ nhất bởi nút AMF:

Cách 1: nút AMF tạo ra ký hiệu nhận dạng khóa thứ nhất.

Cách 2: nút AMF thu được ký hiệu nhận dạng khóa thứ nhất từ thiết bị mạng lõi khác. Ví dụ, ký hiệu nhận dạng khóa thứ nhất thu được từ nút SEAF.

Cách 3: nút AMF thu được, từ thiết bị mạng lõi khác, thông tin được sử dụng để tạo ra ký hiệu nhận dạng khóa thứ nhất, và sau đó tạo ra ký hiệu nhận dạng khóa thứ nhất dựa vào thông tin được sử dụng để tạo ra ký hiệu nhận dạng khóa thứ nhất.

Một cách tùy ý, trong quy trình tái xác thực, thiết bị mạng lõi có thể gửi ký hiệu nhận dạng khóa thứ nhất tới đầu cuối.

Có thể được hiểu rằng sau khi thu ký hiệu nhận dạng khóa thứ nhất, đầu cuối có

thể cập nhật khóa dùng cho kết nối thứ nhất tới khóa được nhận dạng bởi ký hiệu nhận dạng khóa thứ nhất.

Bước 402. Nếu điều kiện kích hoạt thứ nhất được đáp ứng, thiết bị mạng lõi cập nhật khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai.

Một cách tùy ý, điều kiện kích hoạt thứ nhất có thể là trạng thái của kết nối thứ hai, và trạng thái của kết nối thứ hai có thể là trạng thái nghỉ hoặc trạng thái được kết nối.

Một cách tùy ý, điều kiện kích hoạt thứ nhất có thể tùy chọn là kết nối thứ hai ở trạng thái bỏ đăng ký. Nếu thiết bị mạng lõi xác định rằng kết nối thứ hai ở trạng thái bỏ đăng ký, điều này chỉ báo rằng thiết bị mạng lõi và đầu cuối hiện nay không sử dụng kết nối thứ hai. Trong trường hợp này, không có quy trình tái xác thực được thực hiện trên đầu cuối mà cũng không có quy trình cập nhật khóa dùng cho kết nối thứ hai nào làm ảnh hưởng việc sử dụng của kết nối thứ hai bởi thiết bị mạng lõi và đầu cuối.

Bước 403. Nếu điều kiện kích hoạt thứ hai được đáp ứng, đầu cuối cập nhật khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai.

Theo phương pháp được đề xuất theo phương án này của sáng chế, thiết bị mạng lõi có thể thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, và khóa dùng cho kết nối thứ nhất có thể được cập nhật trong quy trình tái xác thực. Khi điều kiện kích hoạt thứ nhất được đáp ứng, thiết bị mạng lõi có thể cập nhật khóa dùng cho kết nối thứ hai. Khi điều kiện kích hoạt thứ hai được đáp ứng, đầu cuối có thể cập nhật khóa dùng cho kết nối thứ hai. Theo cách này, khi đầu cuối truy cập nút AMF bằng cách sử dụng nhiều công nghệ truy cập, việc tái xác thực có thể được thực hiện trên đầu cuối qua kết nối thứ nhất với tiền đề là việc truyền thông thông thường mà được thực hiện giữa đầu cuối và nút AMF qua kết nối thứ hai không bị ảnh hưởng, và các khóa của hai kết nối được cập nhật.

Có thể được hiểu rằng đầu cuối hoặc thiết bị mạng lõi có thể thực hiện một số hoặc tất cả các bước trong phương án nêu trên. Các bước hoặc các hoạt động này chỉ là các ví dụ. Trong các phương án của sáng chế, các hoạt động khác hoặc các sự thay đổi của các hoạt động khác nhau có thể còn được thực hiện. Ngoài ra, các bước có thể được thực hiện theo trình tự khác với các bước được thể hiện trong phương án nêu trên, và có

khả năng là không phải tất cả các hoạt động trong phương án nêu trên cần được thực hiện.

Dựa trên phương án được thể hiện trên Fig.4, trong kịch bản thực hiện khả thi, điều kiện kích hoạt thứ nhất là kết nối thứ hai ở trạng thái nghỉ. Nếu thiết bị mạng lõi xác định rằng thiết bị mạng lõi cần thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, nhưng kết nối thứ hai ở trạng thái được kết nối tại thời điểm này, như được thể hiện trên Fig.5, phương pháp này bao gồm bước 501 đến bước 505.

501. Thiết bị mạng lõi gửi tin nhắn thứ nhất tới đầu cuối qua kết nối thứ nhất, trong đó tin nhắn thứ nhất được sử dụng để lệnh đầu cuối hoãn việc sử dụng kết nối thứ nhất. Một cách tương ứng, đầu cuối thu tin nhắn thứ nhất từ thiết bị mạng lõi qua kết nối thứ nhất.

Có thể được hiểu rằng, khi kết nối thứ hai ở trạng thái được kết nối, để tránh sự ảnh hưởng của quy trình tái xác thực trên truyền thông mà được thực hiện giữa đầu cuối và thiết bị mạng lõi qua kết nối thứ hai, việc tái xác thực trên đầu cuối qua kết nối thứ nhất có thể được hoãn. Sau khi kết nối thứ hai được chuyển đổi từ trạng thái được kết nối sang trạng thái nghỉ, việc tái xác thực được thực hiện trên đầu cuối qua kết nối thứ nhất. Do các lý do chẳng hạn như số đếm NAS được sử dụng bởi đầu cuối sắp vòng lại, thiết bị mạng lõi cần thực hiện việc tái xác thực trên đầu cuối. Nếu đầu cuối tiếp tục gửi tin nhắn NAS tới thiết bị mạng lõi qua kết nối thứ nhất, số đếm NAS có thể vòng lại. Trong trường hợp này, thiết bị mạng lõi có thể lệnh đầu cuối hoãn việc sử dụng kết nối thứ nhất. Một cách tùy ý, nếu ngữ cảnh bảo mật của kết nối thứ nhất có thể còn được sử dụng một lần, thiết bị mạng lõi có thể lệnh đầu cuối gửi, tới thiết bị mạng lõi chỉ qua qua kết nối thứ nhất hoặc kết nối thứ hai, tin nhắn NAS được bảo vệ bằng cách sử dụng ngữ cảnh bảo mật của kết nối thứ nhất hiện có, trước khi việc tái xác thực được thực hiện.

Bước 502. Sau khi kết nối thứ hai được chuyển đổi từ trạng thái được kết nối sang trạng thái nghỉ, thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất. Một cách tương ứng, đầu cuối thực hiện việc tái xác thực qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất.

Một cách tùy ý, sau khi kết nối thứ hai được chuyển đổi từ trạng thái được kết nối sang trạng thái nghỉ, nếu kết nối thứ nhất vẫn trong trạng thái được kết nối, phương pháp của bước 502 được thực hiện.

Một cách tùy ý, sau khi kết nối thứ hai được chuyển đổi từ trạng thái được kết nối sang trạng thái nghỉ, nếu kết nối thứ nhất ở trạng thái nghỉ, thiết bị mạng lõi có thể thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất hoặc kết nối thứ hai tương ứng với công nghệ truy cập thứ hai. Có thể được hiểu rằng do cả hai kết nối ở trong trạng thái nghỉ, đầu cuối có thể truy cập lại mạng bằng cách sử dụng mỗi kết nối. Khi trường hợp này xảy ra, có thể được xem xét rằng kết nối thứ hai trở thành kết nối thứ nhất theo phương án này của sáng chế, và kết nối thứ nhất ban đầu trở thành kết nối thứ hai.

Một cách tùy ý, trong quá trình thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, thiết bị mạng lõi có thể còn cập nhật khóa dùng cho kết nối thứ hai, và thu được ký hiệu nhận dạng khóa thứ ba, trong đó ký hiệu nhận dạng khóa thứ ba được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ hai. Cần chú ý rằng nếu kết nối thứ nhất và kết nối thứ hai chia sẻ tập hợp các khóa NAS, ký hiệu nhận dạng khóa thứ ba giống như ký hiệu nhận dạng khóa thứ nhất, hoặc có thể được hiểu rằng thiết bị mạng lõi không cần thu nhận ký hiệu nhận dạng khóa thứ ba, và ký hiệu nhận dạng khóa thứ nhất có thể còn được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ hai.

Theo cách thực hiện khả thi khác, sau khi phát hiện rằng kết nối thứ hai quay lại trạng thái nghỉ, đầu cuối có thể gửi tin nhắn tới thiết bị mạng lõi qua kết nối thứ nhất hoặc kết nối thứ hai, để kích hoạt thiết bị mạng lõi để khởi tạo việc tái xác thực trên đầu cuối. Theo cách thực hiện khả thi khác nữa, khi kết nối thứ nhất ở trạng thái nghỉ, sau khi đầu cuối thu tin nhắn cuối cùng của thủ tục qua kết nối thứ hai, và trước khi kết nối thứ hai được chuyển đổi sang trạng thái nghỉ, đầu cuối có thể gửi tin nhắn tới thiết bị mạng lõi, để kích hoạt thiết bị mạng lõi để thực hiện việc tái xác thực trên thiết bị đầu cuối qua kết nối thứ hai. Trong trường hợp này, có thể được xem xét rằng kết nối thứ hai trở thành kết nối thứ nhất trong sáng chế này, và kết nối thứ nhất ban đầu trở thành kết nối thứ hai.

Như một sự lựa chọn, khóa dùng cho kết nối thứ hai có thể được cập nhật sau khi thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, nghĩa là, bước 503 có thể còn được thực hiện sau bước 502.

Bước 503. Thiết bị mạng lõi cập nhật khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai.

Đặc biệt là, nếu kết nối thứ hai ở trạng thái nghỉ, thiết bị mạng lõi có thể cập nhật khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai sau khi tái xác thực.

Một cách tùy ý, thiết bị mạng lõi có thể còn thu được ký hiệu nhận dạng khóa thứ ba.

Bước 504. Thiết bị mạng lõi gửi thông tin lệnh thứ nhất tới đầu cuối qua kết nối thứ nhất.

Kết nối thứ nhất được sử dụng để lệnh đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Một cách tùy ý, thông tin lệnh thứ nhất có thể là ký hiệu nhận dạng khóa thứ nhất hoặc ký hiệu nhận dạng khóa thứ hai. Như một sự lựa chọn, thông tin lệnh thứ nhất có thể là ký hiệu nhận dạng khóa thứ nhất và ký hiệu nhận dạng khóa thứ hai.

Bước 505. Đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Có thể được hiểu rằng điều kiện kích hoạt thứ hai là đầu cuối thu thông tin lệnh thứ nhất từ thiết bị mạng lõi qua kết nối thứ nhất.

Một cách tùy ý, nếu thông tin lệnh thứ nhất là ký hiệu nhận dạng khóa thứ nhất, đầu cuối có thể cập nhật khóa dùng cho kết nối thứ hai cho khóa được chỉ báo bởi ký hiệu nhận dạng khóa thứ nhất; hoặc nếu thông tin lệnh thứ nhất là ký hiệu nhận dạng khóa thứ hai, đầu cuối có thể cập nhật khóa dùng cho kết nối thứ hai cho khóa được chỉ báo bởi ký hiệu nhận dạng khóa thứ hai.

Cần chú ý rằng theo phương án bất kỳ của sáng chế, nếu thiết bị mạng lõi lệnh, bằng cách gửi ký hiệu nhận dạng khóa tới đầu cuối đầu cuối để cập nhật khóa dùng cho kết nối thứ hai, đầu cuối có thể cập nhật khóa dùng cho kết nối thứ hai cho khóa được chỉ báo bởi ký hiệu nhận dạng khóa được gửi bởi thiết bị mạng lõi.

Theo phương pháp cập nhật khóa được đề xuất theo phương án này của sáng chế,

nếu xác định rằng việc tái xác thực cần được thực hiện trên đầu cuối qua kết nối thứ nhất, thiết bị mạng lõi còn cần xác định trạng thái của kết nối thứ hai, thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất chỉ khi kết nối thứ hai ở trạng thái nghỉ, và cập nhật các khóa dùng cho kết nối thứ nhất và kết nối thứ hai. Do kết nối thứ hai ở trạng thái nghỉ, quy trình cập nhật khóa không làm ảnh hưởng sự sử dụng bình thường của kết nối thứ hai bởi đầu cuối và thiết bị mạng lõi.

Có thể được hiểu rằng đầu cuối hoặc thiết bị mạng lõi có thể thực hiện một số hoặc tất cả các bước trong phương án nêu trên. Các bước hoặc các hoạt động này chỉ là các ví dụ. Trong các phương án của sáng chế, các hoạt động khác hoặc các sự thay đổi của các hoạt động khác nhau có thể còn được thực hiện. Ngoài ra, các bước có thể được thực hiện theo trình tự khác với các bước được thể hiện trong phương án nêu trên, và có khả năng là không phải tất cả các hoạt động trong phương án nêu trên cần được thực hiện.

Dựa trên phương pháp được thể hiện trên Fig.4, một cách tùy ý, theo kịch bản thực hiện khả thi khác, điều kiện kích hoạt thứ nhất là kết nối thứ hai ở trạng thái được kết nối. Khi thiết bị mạng lõi xác định rằng thiết bị mạng lõi cần thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, nếu kết nối thứ hai ở trạng thái được kết nối, thiết bị mạng lõi có thể hoãn việc sử dụng kết nối thứ hai, và sau đó thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, để cập nhật các khóa dùng cho kết nối thứ nhất và kết nối thứ hai.

Một cách tùy ý, theo kịch bản thực hiện khả thi khác, bộ định thời có thể được tạo cấu hình trước cho nút AMF và đầu cuối. Sau khi thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất và cập nhật khóa dùng cho kết nối thứ nhất, nếu kết nối thứ hai ở trạng thái được kết nối, thiết bị mạng lõi và đầu cuối có thể bắt đầu bộ định thời. Sau khi mạng lõi và đầu cuối xác định rằng bộ định thời kết thúc, khóa cũ dùng cho kết nối thứ hai không thể được sử dụng. Như một sự lựa chọn,

sau khi thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất và cập nhật khóa dùng cho kết nối thứ nhất, nếu kết nối thứ hai ở trạng thái được kết nối, thiết bị mạng lõi bắt đầu bộ định thời sau khi việc tái xác thực được hoàn thành; và đầu cuối bắt đầu tự động bộ định thời. Sau khi mạng lõi xác định rằng bộ định thời

kết thúc, khóa cũ dùng cho kết nối thứ hai không thể còn được sử dụng. Tương tự, sau khi xác định rằng bộ định thời kết thúc, đầu cuối không thể còn sử dụng khóa cũ dùng cho kết nối thứ hai. Như một sự lựa chọn,

trong quy trình xử lý trong đó thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, hoặc sau khi hoàn thành việc tái xác thực, thiết bị mạng lõi gửi ký hiệu nhận dạng khóa thứ nhất tới đầu cuối và sau đó mỗi trong số thiết bị mạng lõi và đầu cuối thiết đặt thông tin dấu, để đánh dấu rằng nếu kết nối thứ hai được chuyển đổi sang trạng thái nghỉ, thiết bị mạng lõi và đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Dựa trên Fig.4, một cách tùy ý, theo kịch bản thực hiện khả thi khác, điều kiện kích hoạt thứ nhất là bộ định thời hoặc thông tin dấu. Như được thể hiện trên Fig.6, phương pháp bao gồm các bước sau đây.

Bước 601. Thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất. Một cách tương ứng, đầu cuối thực hiện việc tái xác thực trên thiết bị mạng lõi qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất.

Một cách tùy ý, trong quy trình xử lý trong đó thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, thiết bị mạng lõi thu được ký hiệu nhận dạng khóa thứ nhất, và giữ ký hiệu nhận dạng khóa thứ hai và khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật, trong đó ký hiệu nhận dạng khóa thứ nhất được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ nhất, và ký hiệu nhận dạng khóa thứ hai được sử dụng để nhận dạng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật.

Một cách tương ứng, trong quá trình thực hiện việc tái xác thực qua kết nối thứ nhất, đầu cuối giữ ký hiệu nhận dạng khóa thứ hai và khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật, trong đó ký hiệu nhận dạng khóa thứ hai được sử dụng để nhận dạng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật.

Cần chú ý rằng, theo phương án này của sáng chế, khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật là khóa cũ dùng cho kết nối thứ hai, và khóa được cập nhật dùng cho kết nối thứ hai là khóa mới dùng cho kết nối thứ hai. Khóa mới dùng

cho kết nối thứ hai liên quan đến khóa được tạo ra trong quy trình tái xác thực của thiết bị đầu cuối qua kết nối thứ nhất.

Bước 602. Thiết bị mạng lõi bắt đầu bộ định thời.

Giá trị mà làm cho bộ định thời kết thúc có thể là giá trị của bộ định thời đang được sử dụng, ví dụ, giá trị của bộ định thời liên quan đến công nghệ truy cập không phải 3GPP, ví dụ, giá trị của bộ định thời bỏ đăng ký (deregistration timer), hoặc có thể là giá trị của bộ định thời liên quan đến công nghệ truy cập 3GPP, ví dụ, giá trị của bộ định thời cập nhật theo chu kỳ (periodic registration timer). Khi bắt đầu bộ định thời, thiết bị mạng lõi có thể sử dụng trực tiếp giá trị của bộ định thời mà đang đếm xuống, có thể thiết đặt giá trị nhỏ hơn giá trị của bộ định thời mà đang đếm xuống, hoặc có thể thiết đặt giá trị không liên quan đến giá trị của bộ định thời hiện có. Như một sự lựa chọn, người thao tác có thể tạo cấu hình trước giá trị mà tại đó bộ định thời kết thúc, sao cho giá trị mà tại đó bộ định thời kết thúc thể hiện thời khoảng hợp lệ của khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật, nghĩa là, thời khoảng, mà khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật, có thể vẫn được sử dụng.

Bước 603. Thiết bị mạng lõi gửi tin nhắn thứ hai tới đầu cuối qua kết nối thứ nhất. Một cách tương ứng, đầu cuối thu tin nhắn thứ hai.

Một cách tùy ý, tin nhắn thứ hai mang thông tin lệnh, và thông tin lệnh được sử dụng để lệnh đầu cuối bắt đầu bộ định thời. Một cách tùy ý, tin nhắn thứ hai có thể là tin nhắn NAS SMC.

Một cách tùy ý, tin nhắn thứ hai còn mang ký hiệu nhận dạng khóa thứ nhất hoặc ký hiệu nhận dạng khóa thứ hai.

Bước 604. Đầu cuối bắt đầu bộ định thời.

Một cách tùy ý, nếu tin nhắn thứ hai được thu bởi đầu cuối mang ký hiệu nhận dạng khóa thứ nhất hoặc ký hiệu nhận dạng khóa thứ hai, đầu cuối có thể xác định rằng khóa dùng cho kết nối thứ hai cần được cập nhật, và sau đó bắt đầu bộ định thời; hoặc nếu tin nhắn thứ hai được thu bởi đầu cuối mang thông tin lệnh, đầu cuối có thể bắt đầu bộ định thời theo thông tin lệnh.

Một cách tùy ý, giá trị mà tại đó bộ định thời được bắt đầu bởi đầu cuối kết thúc có thể giống hoặc khác với giá trị mà tại đó bộ định thời được bắt đầu bởi thiết bị mạng

lõi kết thúc. Nếu các giá trị khác nhau, giá trị mà tại đó bộ định thời được bắt đầu bởi đầu cuối kết thúc có thể là nhỏ hơn giá trị mà tại đó bộ định thời được bắt đầu bởi thiết bị mạng lõi kết thúc. Giá trị mà tại đó bộ định thời được bắt đầu bởi đầu cuối kết thúc có thể là giá trị của bộ định thời đang được sử dụng, ví dụ, giá trị của bộ định thời liên quan đến công nghệ truy cập không phải 3GPP, ví dụ, giá trị của bộ định thời bỏ đăng ký (deregistration timer), hoặc có thể là giá trị của bộ định thời liên quan đến công nghệ truy cập 3GPP, ví dụ, giá trị của bộ định thời cập nhật theo chu kỳ (periodic registration timer). Khi bắt đầu bộ định thời, thiết bị mạng lõi có thể sử dụng trực tiếp giá trị của bộ định thời mà đang đếm xuống, có thể thiết đặt giá trị nhỏ hơn giá trị của bộ định thời mà đang đếm xuống, hoặc có thể thiết đặt giá trị không liên quan đến giá trị của bộ định thời hiện có. Như một sự lựa chọn, người thao tác có thể tạo cấu hình trước giá trị mà tại đó bộ định thời kết thúc, sao cho giá trị mà tại đó bộ định thời kết thúc thể hiện thời khoảng hợp lệ của khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật, nghĩa là, thời khoảng, mà khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật, có thể vẫn được sử dụng.

Bước 605. Nếu điều kiện kích hoạt thứ hai được đáp ứng, đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Một cách tùy ý, điều kiện kích hoạt thứ hai có thể là bộ định thời của đầu cuối kết thúc. Sau khi bộ định thời kết thúc, đầu cuối có thể loại bỏ khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật, hoặc đầu cuối cập nhật, dựa vào khóa mới được tạo ra trong quy trình tái xác thực, khóa được sử dụng dùng cho kết nối thứ hai. Ví dụ, khóa tầng NAS được tạo mới trong quy trình tái xác thực được sử dụng làm khóa mới, hoặc khóa tầng NAS mới thu được bằng cách sử dụng khóa được tạo mới trong quy trình tái xác thực, ví dụ, Kamf.

Cần chú ý rằng trình tự thực hiện của bước 605 và bước 606 không giới hạn trong sáng chế này. Bước 605 có thể được thực hiện trước khi bước 606, hoặc có thể được thực hiện sau bước 606 và bước 607. Trên Fig.6, bước 605 được thực hiện đầu tiên được sử dụng làm ví dụ.

Bước 606. Đầu cuối gửi tin nhắn thứ ba tới thiết bị mạng lõi qua kết nối thứ hai. Một cách tương ứng, thiết bị mạng lõi thu tin nhắn thứ ba từ đầu cuối qua kết nối thứ

hai.

Tin nhắn thứ ba là tin nhắn NAS, và có thể là, ví dụ, tin nhắn yêu cầu đăng ký hoặc tin nhắn yêu cầu thiết lập phiên. Có ít nhất một vài trường hợp sau đây trong đó đầu cuối gửi tin nhắn thứ ba tới thiết bị mạng lõi qua kết nối thứ hai:

Trường hợp 1: trước khi bộ định thời kết thúc, đầu cuối gửi tin nhắn thứ ba tới thiết bị mạng lõi qua kết nối thứ hai, trong đó việc bảo vệ bảo mật được thực hiện trên tin nhắn thứ ba bằng cách sử dụng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật.

Trường hợp 2: sau khi bộ định thời kết thúc, đầu cuối gửi tin nhắn thứ ba tới thiết bị mạng lõi qua kết nối thứ hai, trong đó việc bảo vệ bảo mật không được thực hiện trên tin nhắn thứ ba. Có thể được hiểu rằng, trong trường hợp này, nếu bộ định thời kết thúc, đầu cuối có thể không chủ động cập nhật khóa dùng cho kết nối thứ hai. Một cách tùy ý, đầu cuối có thể gửi tin nhắn thứ ba qua kết nối thứ hai, và sau đó thực hiện bước 607. Sau bước 607, thiết bị mạng lõi có thể gửi, tới đầu cuối qua kết nối thứ hai, tin nhắn được sử dụng để cập nhật và kích hoạt khóa mới. Ví dụ, tin nhắn mang thông tin lệnh dùng để lệnh đầu cuối cập nhật khóa dùng cho kết nối thứ hai hoặc ký hiệu nhận dạng khóa thứ ba, và sau đó đầu cuối thực hiện bước 605. Tương ứng với trường hợp này, điều kiện kích hoạt thứ hai trong bước 605 là đầu cuối thu thông tin lệnh hoặc ký hiệu nhận dạng khóa thứ ba. Như một sự lựa chọn, trong trường hợp này, đầu cuối có thể cập nhật khóa dùng cho kết nối thứ hai sau khi gửi tin nhắn thứ ba tới thiết bị mạng lõi, nghĩa là, điều kiện kích hoạt thứ hai là bộ định thời của đầu cuối kết thúc, nghĩa là, đầu cuối thực hiện bước 605 sau bước 606.

Trường hợp 3: sau khi bộ định thời kết thúc, đầu cuối gửi tin nhắn thứ ba tới thiết bị mạng lõi qua kết nối thứ hai, trong đó việc bảo vệ bảo mật được thực hiện trên tin nhắn thứ ba bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai.

Một cách tùy ý, trong trường hợp 3, sau khi bộ định thời kết thúc, đầu cuối có thể chủ động cập nhật khóa dùng cho kết nối thứ hai, nghĩa là, bước 605 được thực hiện sau bước 606. Tương ứng với trường hợp này, điều kiện kích hoạt thứ hai trong bước 605 là bộ định thời của đầu cuối kết thúc.

Bước 607. Nếu điều kiện kích hoạt thứ nhất được đáp ứng, thiết bị mạng lõi cập

nhật khóa dùng cho kết nối thứ hai.

Tương ứng với ba trường hợp trong bước 605, cũng có ba loại điều kiện kích hoạt thứ nhất:

Tương ứng với trường hợp 1, loại thứ nhất của điều kiện kích hoạt là: thiết bị mạng lõi thu, trước khi bộ định thời kết thúc, tin nhắn thứ ba mà được gửi bởi đầu cuối qua kết nối thứ hai, và việc xác thực bảo mật mà được thực hiện bởi thiết bị mạng lõi trên tin nhắn thứ ba bằng cách sử dụng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật thành công.

Một cách tùy ý, trong trường hợp này, đầu cuối không cập nhật khóa dùng cho kết nối thứ hai trước khi gửi tin nhắn thứ ba tới thiết bị mạng lõi. Do đó, sau khi cập nhật khóa dùng cho kết nối thứ hai, thiết bị mạng lõi có thể lệnh đầu cuối cập nhật khóa dùng cho kết nối thứ hai, ví dụ, cập nhật khóa dùng cho kết nối thứ hai trong thủ tục kích hoạt khóa sau đó, ví dụ, quy trình NAS SMC.

Một cách tùy ý, trong quy trình xử lý trong đó thiết bị mạng lõi xử lý tin nhắn thứ ba, bộ định thời kết thúc, và thiết bị mạng lõi có thể gửi tin nhắn sự cố tới đầu cuối. Tin nhắn sự cố có thể mang giá trị nguyên nhân sự cố, và giá trị nguyên nhân được sử dụng để thông báo đầu cuối rằng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật kết thúc.

Một cách tùy ý, trong quy trình xử lý trong đó thiết bị mạng lõi xử lý tin nhắn thứ ba, nếu bộ định thời kết thúc, việc bảo vệ bảo mật có thể được thực hiện, bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai, trên tin nhắn được gửi sau đó bởi thiết bị mạng lõi tới đầu cuối. Do đầu cuối cập nhật khóa dùng cho kết nối thứ hai sau khi bộ định thời của đầu cuối kết thúc, đầu cuối có thể thực hiện, bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai, việc xác thực bảo mật trên tin nhắn được thu qua kết nối thứ hai sau khi bộ định thời kết thúc.

Tương ứng với trường hợp 2, loại thứ hai của điều kiện kích hoạt là: sau khi bộ định thời kết thúc, thiết bị mạng lõi thu tin nhắn thứ ba mà được gửi bởi đầu cuối qua kết nối thứ hai và trên đó việc bảo vệ bảo mật không được thực hiện. Trong trường hợp này, thiết bị mạng lõi cho phép khóa được cập nhật dùng cho kết nối thứ hai trong thủ tục kích hoạt khóa sau đó, ví dụ, thủ tục NAS SMC.

Tương ứng với trường hợp 3, loại thứ ba của điều kiện kích hoạt là: sau khi bộ định thời kết thúc, thiết bị mạng lõi thu tin nhắn thứ ba mà được gửi bởi đầu cuối qua kết nối thứ hai, trong đó việc bảo vệ bảo mật được thực hiện trên tin nhắn thứ ba bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai. Một cách tương ứng, thiết bị mạng lõi thực hiện việc xác thực bảo mật trên tin nhắn thứ ba bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai.

Một cách tùy ý, loại thứ tư của điều kiện kích hoạt còn bao gồm: bộ định thời kết thúc, và thiết bị mạng lõi không thu, trước khi bộ định thời kết thúc, tin nhắn thứ ba mà được gửi bởi đầu cuối qua kết nối thứ hai.

Đối với loại thứ tư của điều kiện kích hoạt, nghĩa là, đầu cuối không gửi tin nhắn thứ ba tới thiết bị mạng lõi từ thời điểm khi bộ định thời của thiết bị mạng lõi được bắt đầu tới thời điểm khi bộ định thời của mạng lõi kết thúc, thiết bị mạng lõi loại bỏ khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật, sau khi bộ định thời của thiết bị mạng lõi kết thúc. Một cách tùy ý, thiết bị mạng lõi còn cập nhật khóa dùng cho kết nối thứ hai. Một cách tùy ý, thiết bị mạng lõi lệnh đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Một cách tùy ý, sau khi bộ định thời kết thúc, kết nối thứ hai không quay lại ngay trạng thái nghỉ. Trong khoảng thời gian từ thời điểm khi bộ định thời kết thúc đến thời điểm khi kết nối thứ hai quay lại trạng thái nghỉ, nếu đầu cuối gửi tin nhắn yêu cầu đăng ký tới thiết bị mạng lõi, thiết bị mạng lõi có thể thực hiện việc tái xác thực trên đầu cuối.

Cần chú ý rằng, trước khi bộ định thời kết thúc, nếu thiết bị mạng lõi đã cập nhật khóa dùng cho kết nối thứ hai, thiết bị mạng lõi có thể đóng bộ định thời. Tương tự, nếu đầu cuối cập nhật khóa dùng cho kết nối thứ hai trước khi bộ định thời kết thúc, đầu cuối có thể cũng đóng bộ định thời.

Bước 608. Thiết bị mạng lõi xóa khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật và ký hiệu nhận dạng khóa thứ hai.

Có thể được hiểu rằng, trong bước 607, sau khi cập nhật khóa dùng cho kết nối thứ hai, thiết bị mạng lõi có thể thực hiện bước 608.

Bước 609. Đầu cuối xóa khóa dùng cho kết nối thứ hai trước khi cập nhật và ký hiệu nhận dạng khóa thứ hai.

Có thể được hiểu rằng, trong bước 605, sau khi cập nhật khóa dùng cho kết nối thứ hai, đầu cuối có thể thực hiện bước 609.

Theo phương pháp cập nhật khóa được đề xuất theo phương án này của sáng chế, khi mạng lõi xác định rằng mạng lõi cần thực hiện việc tái xác thực qua kết nối thứ nhất, nếu kết nối thứ hai ở trạng thái được kết nối, thiết bị mạng lõi có thể thực hiện trực tiếp việc tái xác thực trên đầu cuối qua kết nối thứ nhất, và có thể giữ lại khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật trong quy trình tái xác thực. Theo cách này, ngay cả khi thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, và cập nhật khóa dùng cho kết nối thứ nhất, khi thiết bị mạng lõi và đầu cuối truyền thông với nhau qua kết nối thứ hai, khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật có thể vẫn được sử dụng, và việc truyền thông thông thường qua kết nối thứ hai không bị ảnh hưởng. Ngoài ra, theo phương pháp, kết nối thứ nhất và kết nối thứ hai được tách riêng. Khi thực hiện việc xác thực trên đầu cuối qua kết nối thứ nhất, thiết bị mạng lõi không cần phát hiện trạng thái của kết nối thứ hai. Sau khi bộ định thời kết thúc, cả thiết bị mạng lõi và đầu cuối có thể chủ động cập nhật khóa dùng cho kết nối thứ hai, nhờ đó làm giảm các phí tổn tương tác báo hiệu giữa thiết bị mạng lõi và đầu cuối và đơn giản hóa việc thực hiện.

Có thể được hiểu rằng đầu cuối hoặc thiết bị mạng lõi có thể thực hiện một số hoặc tất cả các bước trong phương án nêu trên. Các bước hoặc các hoạt động này chỉ là các ví dụ. Trong các phương án của sáng chế, các hoạt động khác hoặc các sự thay đổi của các hoạt động khác nhau có thể còn được thực hiện. Ngoài ra, các bước có thể được thực hiện theo trình tự khác với các bước được thể hiện trong phương án nêu trên, và có khả năng là không phải tất cả các hoạt động trong phương án nêu trên cần được thực hiện.

Một cách tùy ý, có dựa trên Fig.4, theo kịch bản thực hiện khả thi khác, khi mạng lõi xác định rằng mạng lõi cần thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, như được thể hiện trên Fig.7, phương pháp này bao gồm các bước sau đây.

Bước 701. Thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất; một cách tương ứng, đầu cuối thực hiện việc tái xác thực trên thiết bị mạng lõi qua kết nối thứ nhất tương ứng với công

nghệ truy cập thứ nhất.

Bước 702. Thiết bị mạng lõi thiết đặt dấu thứ nhất. Một cách tùy ý, kết nối thứ hai ở trạng thái được kết nối.

Dấu thứ nhất được sử dụng để đánh dấu rằng thiết bị mạng lõi đã thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, hoặc được sử dụng để lệnh cập nhật khóa dùng cho kết nối thứ hai.

Cần chú ý rằng, nếu dấu thứ nhất được sử dụng để đánh dấu rằng thiết bị mạng lõi đã thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, nó cũng đánh dấu ngầm định rằng thiết bị mạng lõi cần cập nhật khóa dùng cho kết nối thứ hai.

Bước 703. Nếu điều kiện kích hoạt thứ nhất được đáp ứng, thiết bị mạng lõi cập nhật khóa dùng cho kết nối thứ hai.

Một cách tùy ý, trong quy trình xử lý trong đó thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, kết nối thứ hai có thể quay lại trạng thái nghỉ. Dựa vào điều này, điều kiện kích hoạt thứ nhất là kết nối thứ hai ở trạng thái nghỉ, và thiết bị mạng lõi xác định rằng dấu thứ nhất tồn tại.

Như một sự lựa chọn, sau khi thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất và kết nối thứ hai vẫn trong trạng thái được kết nối, điều kiện kích hoạt thứ nhất trong trường hợp này là thiết bị mạng lõi xác định rằng dấu thứ nhất tồn tại, và phương pháp cập nhật khóa tương ứng dùng cho kết nối thứ hai bởi thiết bị mạng lõi là: nếu kết nối thứ hai ở trạng thái được kết nối, đầu tiên hoãn, bởi thiết bị mạng lõi, sử dụng kết nối thứ hai, và sau đó cập nhật khóa dùng cho kết nối thứ hai. Như một sự lựa chọn, trước khi phản hồi đầu cuối bằng tin nhắn qua kết nối thứ hai, thiết bị mạng lõi đầu tiên trao đổi thủ tục kích hoạt và cập nhật khóa với thiết bị đầu cuối để cập nhật khóa dùng cho kết nối thứ hai. Sau đó thiết bị mạng lõi gửi tin nhắn phản hồi tới đầu cuối. Ví dụ, khóa dùng cho kết nối thứ hai được cập nhật trong thủ tục NAS SMC.

Cần chú ý rằng, nếu kết nối thứ hai quay lại trạng thái nghỉ trong quy trình xử lý trong đó thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, thiết bị mạng lõi có thể cập nhật khóa dùng cho kết nối thứ hai khi thiết bị mạng lõi thu lại tin nhắn NAS, ví dụ, tin nhắn yêu cầu đăng ký, mà được gửi bởi đầu cuối qua kết nối thứ hai, và thiết bị mạng lõi xác định rằng dấu thứ nhất tồn tại. Ví dụ, khóa dùng cho kết

nối thứ hai được cập nhật bằng cách trao đổi thủ tục kích hoạt và cập nhật khóa với thiết bị đầu cuối.

Một cách tùy ý, thiết bị mạng lõi có thể xác định, dựa vào thông tin ký hiệu nhận dạng khóa được mang trong tin nhắn được gửi bởi thiết bị đầu cuối, tập hợp cụ thể của các khóa được sử dụng bởi thiết bị đầu cuối. Trong trường hợp này, thiết bị mạng lõi xác định các khóa dựa vào ký hiệu nhận dạng khóa, và xác nhận, bằng cách sử dụng các khóa tương ứng với ký hiệu nhận dạng khóa, tin nhắn được gửi bởi đầu cuối. Sau khi xác nhận thành công, tập hợp các khóa được sử dụng làm các khóa được cập nhật dùng cho kết nối thứ hai.

Có thể được hiểu rằng: sau khi cập nhật khóa dùng cho kết nối thứ hai, thiết bị mạng lõi có thể tiếp tục lại việc sử dụng kết nối thứ hai; và khi gửi sau đó tin nhắn NAS qua kết nối thứ hai, thiết bị mạng lõi có thể thực hiện việc bảo vệ tính toàn vẹn trên tin nhắn NAS bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai.

Bước 704. Thiết bị mạng lõi thu được ký hiệu nhận dạng khóa thứ ba.

Ký hiệu nhận dạng khóa thứ ba được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ hai.

Một cách tùy ý, nếu kết nối thứ nhất và kết nối thứ hai chia sẻ tập hợp các khóa NAS, thiết bị mạng lõi có thể không thu được ký hiệu nhận dạng khóa thứ nhất trong quy trình tái xác thực, nhưng thu được ký hiệu nhận dạng khóa thứ ba sau khi cập nhật khóa dùng cho kết nối thứ hai. Trong trường hợp này, ký hiệu nhận dạng khóa thứ ba có thể được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ nhất và khóa được cập nhật dùng cho kết nối thứ hai.

Một cách tùy ý, nếu kết nối thứ nhất và kết nối thứ hai chia sẻ tập hợp các khóa NAS, thiết bị mạng lõi có thể không thu được ký hiệu nhận dạng khóa thứ ba, nhưng sử dụng trực tiếp ký hiệu nhận dạng khóa thứ nhất thu được trong quy trình tái xác thực. Nói cách khác, ký hiệu nhận dạng khóa thứ nhất thu được trong quy trình tái xác thực có thể được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ nhất và khóa được cập nhật dùng cho kết nối thứ hai.

Bước 705. Thiết bị mạng lõi gửi ký hiệu nhận dạng khóa thứ ba tới đầu cuối. Một cách tương ứng, đầu cuối thu ký hiệu nhận dạng khóa thứ ba từ thiết bị mạng lõi.

Cần chú ý rằng, sau khi thiết bị mạng lõi cập nhật khóa dùng cho kết nối thứ hai, nếu kết nối thứ hai ở trạng thái được kết nối, thiết bị mạng lõi có thể gửi ký hiệu nhận dạng khóa thứ ba tới đầu cuối qua kết nối thứ hai, trong đó việc bảo vệ tính toàn vẹn được thực hiện trên ký hiệu nhận dạng khóa thứ ba bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai; nếu kết nối thứ hai ở trạng thái nghỉ, thiết bị mạng lõi có thể gửi ký hiệu nhận dạng khóa thứ ba tới đầu cuối qua kết nối thứ nhất, và việc bảo vệ tính toàn vẹn được thực hiện trên ký hiệu nhận dạng khóa thứ ba bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ nhất.

Một cách tùy ý, nếu kết nối thứ nhất và kết nối thứ hai chia sẻ tập hợp các khóa NAS, và thiết bị mạng lõi không thu được ký hiệu nhận dạng khóa thứ ba, thiết bị mạng lõi có thể gửi ký hiệu nhận dạng khóa thứ nhất tới đầu cuối.

Một cách tùy ý, thiết bị mạng lõi có thể còn gửi, tới đầu cuối ít nhất một thông số được sử dụng để cập nhật khóa dùng cho kết nối thứ hai, ví dụ, thuật toán mật mã hóa và thuật toán bảo vệ tính toàn vẹn mà được lựa chọn khi thiết bị mạng lõi cập nhật khóa dùng cho kết nối thứ hai, và loại công nghệ truy cập.

Bước 706. Đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Có thể được hiểu rằng trong trường hợp này, điều kiện kích hoạt thứ hai là đầu cuối thu ký hiệu nhận dạng khóa thứ ba từ thiết bị mạng lõi.

Một cách tùy ý, ký hiệu nhận dạng khóa thứ ba có thể được mang trong tin nhắn NAS. Nếu đầu cuối thu ký hiệu nhận dạng khóa thứ ba qua kết nối thứ hai, đầu cuối có thể cập nhật khóa dùng cho kết nối thứ hai dựa vào ký hiệu nhận dạng khóa thứ ba, nghĩa là, cập nhật khóa dùng cho kết nối thứ hai tới khóa được nhận dạng bởi ký hiệu nhận dạng khóa thứ ba, và thực hiện việc xác nhận bảo vệ tính toàn vẹn trên tin nhắn NAS bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai. Sau khi xác nhận thành công, khóa được cập nhật dùng cho kết nối thứ hai trở nên hợp lệ. Nếu đầu cuối thu ký hiệu nhận dạng khóa thứ ba qua kết nối thứ nhất, đầu cuối có thể thực hiện việc xác nhận bảo vệ tính toàn vẹn trên tin nhắn NAS bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai, và cập nhật khóa dùng cho kết nối thứ hai sau khi xác nhận thành công.

Theo phương pháp tạo khóa được đề xuất theo phương án này của sáng chế, bất kể việc kết nối thứ hai có ở trạng thái nghỉ hay không, thiết bị mạng lõi có thể đầu tiên

cập nhật khóa dùng cho kết nối thứ nhất. Sau khi khóa dùng cho kết nối thứ nhất được cập nhật, nếu kết nối thứ hai quay lại trạng thái nghỉ, khóa dùng cho kết nối thứ hai có thể được cập nhật sau khi đầu cuối gửi tin nhắn yêu cầu đăng ký tới thiết bị mạng lõi qua kết nối thứ hai lần tiếp theo. Nếu kết nối thứ hai vẫn trong trạng thái được kết nối, để tránh việc thiết bị mạng lõi và đầu cuối thực hiện việc bảo vệ bảo mật vẫn bằng cách sử dụng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật khi truyền tin nhắn với nhau qua kết nối thứ hai và do đó việc xác thực bảo mật trên tin nhắn bị lỗi, thiết bị mạng lõi có thể hoãn việc sử dụng kết nối thứ hai, nghĩa là, đầu tiên hoãn việc trao đổi tin nhắn NAS mà được thực hiện giữa thiết bị mạng lõi và đầu cuối qua kết nối thứ hai, và sau đó cập nhật khóa dùng cho kết nối thứ hai. Sau khi cập nhật, việc trao đổi tin nhắn NAS được thực hiện giữa thiết bị mạng lõi và đầu cuối có thể được tiếp tục lại qua kết nối thứ hai. Trong trường hợp này, việc bảo vệ bảo mật được thực hiện trên tin nhắn NAS bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai. Sau khi thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, sự cố xác thực bảo mật trên tin nhắn mà được truyền qua kết nối thứ hai được tránh.

Có thể được hiểu rằng đầu cuối hoặc thiết bị mạng lõi có thể thực hiện một số hoặc tất cả các bước trong phương án nêu trên. Các bước hoặc các hoạt động này chỉ là các ví dụ. Trong các phương án của sáng chế, các hoạt động khác hoặc các sự thay đổi của các hoạt động khác nhau có thể còn được thực hiện. Ngoài ra, các bước có thể được thực hiện theo trình tự khác với các bước được thể hiện trong phương án nêu trên, và có khả năng là không phải tất cả các hoạt động trong phương án nêu trên cần được thực hiện.

Dựa trên Fig.4, trong kịch bản thực hiện khả thi trước, khi mạng lõi xác định rằng mạng lõi cần thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, nếu kết nối thứ hai ở trạng thái được kết nối, phương án của sáng chế còn đề xuất cách thực hiện khả thi khác. Như được thể hiện trên Fig.8, phương pháp này bao gồm các bước sau đây.

Bước 801. Thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất; một cách tương ứng, đầu cuối thực hiện việc tái xác thực trên thiết bị mạng lõi qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất.

Bước 802. Thiết bị mạng lõi gửi thông tin lệnh thứ hai tới đầu cuối qua kết nối thứ nhất. Một cách tương ứng, đầu cuối thu thông tin lệnh thứ hai từ thiết bị mạng lõi.

Thông tin lệnh thứ hai được sử dụng để lệnh đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Theo phương pháp thực hiện này, cơ hội cập nhật khóa dùng cho kết nối thứ hai không bị giới hạn. Cụ thể là, việc xem thiết bị đầu cuối cập nhật khóa ngay sau khi thu thông tin lệnh thứ hai hay cập nhật khóa sau một khoảng thời gian sau khi thu thông tin lệnh thứ hai không bị giới hạn. Phương pháp này nhấn mạng rằng đầu cuối thực hiện thao tác cập nhật khóa dùng cho kết nối thứ hai sau khi thu thông tin lệnh thứ hai.

Bước 803. Thiết bị mạng lõi thiết đặt dấu thứ hai.

Dấu thứ hai được sử dụng để lệnh cập nhật khóa dùng cho kết nối thứ hai.

Cần chú ý rằng trình tự thực hiện của bước 802 và bước 803 không giới hạn trong sáng chế này. Hai bước có thể được thực hiện đồng thời, hoặc một trong số hai bước được thực hiện đầu tiên.

Bước 804. Đầu cuối thiết đặt dấu thứ ba.

Dấu thứ ba được sử dụng để lệnh cập nhật khóa dùng cho kết nối thứ hai.

Bước 805. Nếu thiết bị mạng lõi xác định rằng dấu thứ hai tồn tại và kết nối thứ hai được chuyển đổi sang trạng thái nghỉ, thiết bị mạng lõi cập nhật khóa dùng cho kết nối thứ hai.

Có thể được hiểu rằng, trong trường hợp này, điều kiện kích hoạt thứ nhất là thiết bị mạng lõi xác định rằng dấu thứ hai tồn tại, và kết nối thứ hai được chuyển đổi sang trạng thái nghỉ.

Bước 806. Nếu đầu cuối xác định rằng dấu thứ ba tồn tại, và kết nối thứ hai được chuyển đổi sang trạng thái nghỉ, đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Có thể được hiểu rằng trong trường hợp này, điều kiện kích hoạt thứ hai là đầu cuối xác định rằng dấu thứ ba tồn tại, và kết nối thứ hai được chuyển đổi sang trạng thái nghỉ.

Một cách tùy ý, đầu cuối có thể không thiết đặt dấu thứ ba. Sau khi cập nhật khóa dùng cho kết nối thứ hai, thiết bị mạng lõi có thể gửi thông tin lệnh tới đầu cuối để lệnh đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Như một sự lựa chọn, sau khi kết nối thứ hai được chuyển đổi sang trạng thái nghỉ, đầu cuối có thể không cập nhật khóa dùng cho kết nối thứ hai một cách tạm thời. Khi đầu cuối cần gửi tin nhắn tới thiết bị mạng lõi qua kết nối thứ hai, nếu được xác định rằng dấu thứ ba tồn tại, đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Có thể được hiểu rằng sau khi đầu cuối cập nhật khóa dùng cho kết nối thứ hai, việc bảo vệ tính toàn vẹn có thể được thực hiện, bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai, trên tin nhắn NAS mà được gửi bởi đầu cuối tới thiết bị mạng lõi qua kết nối thứ hai.

Theo phương pháp cập nhật khóa được đề xuất theo phương án này của sáng chế, khi thiết bị mạng lõi xác định rằng thiết bị mạng lõi cần thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, nếu kết nối thứ hai ở trạng thái được kết nối, thiết bị mạng lõi có thể thực hiện đầu tiên việc tái xác thực trên đầu cuối qua kết nối thứ nhất. Sau khi tái xác thực, thiết bị mạng lõi có thể thiết đặt dấu thứ hai, và đầu cuối có thể thiết đặt dấu thứ ba. Sau khi kết nối thứ hai được chuyển đổi sang trạng thái nghỉ, cả thiết bị mạng lõi và đầu cuối có thể cập nhật khóa dùng cho kết nối thứ hai dựa vào các dấu được thiết đặt bởi thiết bị mạng lõi và đầu cuối, nhờ đó làm giảm phí tổn báo hiệu được tạo ra trong quy trình cập nhật khóa dùng cho kết nối thứ hai.

Có thể được hiểu rằng đầu cuối hoặc thiết bị mạng lõi có thể thực hiện một số hoặc tất cả các bước trong phương án nêu trên. Các bước hoặc các hoạt động này chỉ là các ví dụ. Trong các phương án của sáng chế, các hoạt động khác hoặc các sự thay đổi của các hoạt động khác nhau có thể còn được thực hiện. Ngoài ra, các bước có thể được thực hiện theo trình tự khác với các bước được thể hiện trong phương án nêu trên, và có khả năng là không phải tất cả các hoạt động trong phương án nêu trên cần được thực hiện.

Phương pháp tạo khóa được đề xuất trong các phương án của sáng chế được mô tả dưới đây có dựa trên kịch bản cụ thể. Dựa trên Fig.4 và Fig.6, trong kịch bản thực hiện tương ứng với Fig.6, như được thể hiện trên Fig.9, phương pháp này bao gồm cụ thể các bước sau đây.

Bước 901. Đầu cuối gửi tin nhắn NAS tới nút AMF qua kết nối thứ nhất. Một cách tương ứng, nút AMF thu tin nhắn NAS qua kết nối thứ nhất.

Ví dụ, tin nhắn NAS có thể là tin nhắn yêu cầu đăng ký, tin nhắn yêu cầu dịch vụ, hoặc tin nhắn yêu cầu thiết lập phiên PDU, hoặc có thể là tin nhắn NAS khác. Điều này không giới hạn trong sáng chế này.

Tin nhắn NAS mang ký hiệu nhận dạng khóa được sử dụng để nhận dạng khóa dùng cho kết nối thứ nhất, và tin nhắn NAS được bảo vệ bằng cách sử dụng khóa dùng cho kết nối thứ nhất.

Bước 902. Nút AMF thực hiện xác nhận tính toàn vẹn trên tin nhắn NAS, trong đó việc xác nhận thành công, và xác định rằng nút AMF cần thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất.

Nút AMF xác định khóa dùng cho kết nối thứ nhất dựa vào ký hiệu nhận dạng khóa được mang trong tin nhắn NAS. Sau khi xác nhận tính toàn vẹn của tin nhắn NAS bằng cách sử dụng khóa dùng cho kết nối thứ nhất mà được xác định dựa vào ký hiệu nhận dạng khóa, trong đó việc xác nhận thành công, nút AMF có thể xác định xem việc tái xác thực có cần được thực hiện trên đầu cuối hay không. Ví dụ, khi xác định rằng số đếm NAS được sử dụng bởi đầu cuối sắp vòng lại, nút AMF xác định rằng việc tái xác thực cần được thực hiện trên đầu cuối. Như một sự lựa chọn, nút AMF có thể xác định, dựa vào thông tin tạo cấu hình của người thao tác, xem việc tái xác thực có cần được thực hiện trên đầu cuối hay không. Tất nhiên, sáng chế này không giới hạn ở hai phương pháp được liệt kê để xác định xem việc tái xác thực có cần được thực hiện trên đầu cuối hay không.

Bước 903. Nút AMF khởi tạo việc tái xác thực trên đầu cuối qua kết nối thứ nhất. Một cách tương ứng, đầu cuối thực hiện việc tái xác thực qua kết nối thứ nhất.

Việc tái xác thực bao gồm thủ tục xác nhận xác thực và thủ tục kích hoạt khóa.

Bước 904. Nút AMF cập nhật khóa tương ứng với kết nối thứ nhất, và thu được ký hiệu nhận dạng khóa thứ nhất.

Ký hiệu nhận dạng khóa thứ nhất có thể thu được trong quá trình xác thực, và ký hiệu nhận dạng khóa thứ nhất được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ nhất.

Cần chú ý rằng, nếu kết nối thứ nhất và kết nối thứ hai sử dụng các khóa khác nhau, sau khi cập nhật khóa dùng cho kết nối thứ nhất, nút AMF có thể xóa khóa dùng

cho kết nối thứ nhất mà được sử dụng trước khi cập nhật, và giữ lại khóa dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa thứ hai, trong đó ký hiệu nhận dạng khóa thứ hai được sử dụng để nhận dạng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật; hoặc

nếu kết nối thứ nhất và kết nối thứ hai chia sẻ tập hợp các khóa, khi nút AMF cập nhật khóa dùng cho kết nối thứ nhất, một cách tùy ý, nút AMF vẫn cần giữ, dùng cho kết nối thứ hai, khóa dùng cho kết nối thứ nhất mà được sử dụng trước khi cập nhật và ký hiệu nhận dạng khóa thứ hai. Ký hiệu nhận dạng khóa thứ hai được sử dụng để nhận dạng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật. Có thể được hiểu rằng, khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật giống như khóa dùng cho kết nối thứ nhất mà được sử dụng trước khi cập nhật. Đặc biệt là, nếu kết nối thứ hai ở trạng thái được kết nối, trong phương pháp trong đó nút AMF thiết đặt thông tin nhận dạng hoặc giá trị bộ định thời, nút AMF vẫn cần giữ, dùng cho kết nối thứ hai, khóa dùng cho kết nối thứ nhất mà được sử dụng trước khi cập nhật và ký hiệu nhận dạng khóa thứ hai.

Bước 905. Nút AMF gửi tin nhắn NAS SMC tới đầu cuối qua kết nối thứ nhất. Một cách tương ứng, đầu cuối thu tin nhắn NAS SMC từ nút AMF qua kết nối thứ nhất.

Tin nhắn NAS SMC tương đương với tin nhắn thứ hai trong bước 603. Một cách tùy ý, tin nhắn NAS SMC mang ký hiệu nhận dạng khóa thứ nhất, ký hiệu nhận dạng khóa thứ hai, hoặc thông tin chỉ báo, trong đó thông tin chỉ báo được sử dụng để chỉ báo đầu cuối để bắt đầu bộ định thời.

Một cách tùy ý, nếu tin nhắn NAS SMC được thu bởi đầu cuối mang thông tin lệnh mà được sử dụng để lệnh đầu cuối bắt đầu bộ định thời, đầu cuối bắt đầu bộ định thời. Như một sự lựa chọn, nếu đầu cuối xác định rằng được thu tin nhắn NAS SMC mang ký hiệu nhận dạng khóa thứ nhất hoặc ký hiệu nhận dạng khóa thứ hai, đầu cuối có thể bắt đầu bộ định thời.

Như một sự lựa chọn, khi phương pháp dùng cho bộ định thời được sử dụng, ngay cả khi tin nhắn NAS SMC không mang ký hiệu nhận dạng khóa thứ nhất, ký hiệu nhận dạng khóa thứ hai, hoặc thông tin lệnh, đầu cuối có thể bắt đầu bộ định thời sau khi xác nhận rằng việc bảo vệ tính toàn vẹn của NAS SMC chính xác hoặc sau khi gửi

tin nhắn NAS SMP. Việc bắt đầu bộ định thời có thể được thực hiện bởi đầu cuối trong thời gian cực kỳ ngắn sau khi đầu cuối xác nhận rằng việc bảo vệ tính toàn vẹn của tin nhắn NAS SMC chính xác hoặc sau khi đầu cuối gửi tin nhắn NAS SMP. Ví dụ, bộ định thời được bắt đầu ngay sau khi tin nhắn NAS SMC được xác nhận, hoặc được bắt đầu ngay sau khi NAS SMP được gửi. Theo phương pháp này, ký hiệu nhận dạng khóa thứ nhất đã được truyền tới đầu cuối trong thủ tục xác thực.

Cần chú ý rằng nút AMF có thể tùy chọn bắt đầu bộ định thời trước khi thực hiện bước 905, hoặc bắt đầu bộ định thời sau bước 908.

Giá trị mà làm cho bộ định thời kết thúc là thời khoảng hợp lệ của khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật. Ví dụ, được giả thiết rằng kết nối thứ nhất và kết nối thứ hai chia sẻ tập hợp các khóa. Trước khi bộ định thời kết thúc, khóa dùng cho kết nối thứ nhất mà được sử dụng trước khi cập nhật có thể vẫn được sử dụng bởi kết nối thứ hai; sau khi bộ định thời kết thúc, khóa dùng cho kết nối thứ nhất mà được sử dụng trước khi cập nhật không thể được sử dụng để thực hiện việc bảo vệ bảo mật trên tin nhắn mà được truyền giữa nút AMF và đầu cuối qua kết nối thứ hai.

Bước 906. Đầu cuối cập nhật khóa dùng cho kết nối thứ nhất.

Có thể được hiểu rằng, trong quy trình tái xác thực, đầu cuối thu tin nhắn NAS SMC từ nút AMF qua kết nối thứ nhất, và cập nhật khóa tương ứng với kết nối thứ nhất.

Sau khi cập nhật khóa dùng cho kết nối thứ nhất, đầu cuối có thể xóa khóa dùng cho kết nối thứ nhất mà được sử dụng trước khi cập nhật, và giữ lại khóa dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa thứ hai. Việc xóa khóa dùng cho kết nối thứ nhất mà được sử dụng trước khi cập nhật có nghĩa là khóa không thể được sử dụng lại bởi kết nối thứ nhất. Thao tác này chỉ liên quan đến kết nối thứ nhất và không liên quan đến kết nối thứ hai.

Bước 907. Đầu cuối gửi tin nhắn NAS SMP tới nút AMF qua kết nối thứ nhất. Một cách tương ứng, nút AMF thu tin nhắn NAS SMP.

Nút NAS SMP thực hiện việc bảo vệ tính toàn vẹn bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ nhất.

Cần chú ý rằng bước 904 tới bước 907 có thể cũng được hiểu là quy trình xử lý trong đó thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất.

Bước 908. Nút AMF gửi tin nhắn hoàn thành tới đầu cuối qua kết nối thứ nhất; một cách tương ứng, đầu cuối thu tin nhắn hoàn thành từ nút AMF.

Tin nhắn hoàn thành là tin nhắn phản hồi của tin nhắn NAS trong bước 901. Ví dụ, nếu tin nhắn NAS trong bước 901 là tin nhắn yêu cầu đăng ký, tin nhắn NAS là tin nhắn hoàn thành đăng ký.

Bước 909. Đầu cuối gửi tin nhắn NAS tới nút AMF qua kết nối thứ hai. Một cách tương ứng, nút AMF thu tin nhắn NAS qua kết nối thứ hai.

Tin nhắn NAS mang ký hiệu nhận dạng khóa thứ hai, và tin nhắn NAS được bảo vệ bằng cách sử dụng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật.

Một cách tùy ý, tin nhắn NAS còn mang ký hiệu nhận dạng khóa thứ nhất.

Tương tự, tin nhắn NAS có thể tùy chọn là tin nhắn yêu cầu đăng ký, tin nhắn yêu cầu dịch vụ, hoặc tin nhắn yêu cầu thiết lập phiên PDU. Tất nhiên, sáng chế này không giới hạn ở đó.

Tin nhắn NAS tương đương với tin nhắn thứ ba trong bước 606. Đối với trường hợp trong đó đầu cuối gửi tin nhắn NAS tới nút AMF qua kết nối thứ hai, đề cập đến phần mô tả trên bước 606. Các chi tiết không được mô tả lại ở đây.

Bước 910. Nút AMF cập nhật khóa dùng cho kết nối thứ hai.

Nút AMF có thể cập nhật khóa dùng cho kết nối thứ hai chỉ khi điều kiện kích hoạt thứ nhất được đáp ứng. Để mô tả điều kiện kích hoạt thứ nhất, xem phần mô tả liên quan của bước 607. Các chi tiết không được mô tả lại ở đây.

Một cách tùy ý, nút AMF có thể thu được ký hiệu nhận dạng khóa thứ ba tương ứng với khóa được cập nhật dùng cho kết nối thứ hai, trong đó ký hiệu nhận dạng khóa thứ ba được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ hai. Như một sự lựa chọn, nếu kết nối thứ nhất và kết nối thứ hai chia sẻ tập hợp các khóa NAS, nút AMF có thể không tạo ký hiệu nhận dạng khóa thứ ba, nhưng sử dụng ký hiệu nhận dạng khóa thứ nhất để nhận dạng khóa được cập nhật dùng cho kết nối thứ nhất và khóa được cập nhật dùng cho kết nối thứ hai.

Cần chú ý rằng sau khi cập nhật khóa dùng cho kết nối thứ hai, nút AMF có thể xóa khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật và ký hiệu nhận

dạng khóa được sử dụng để nhận dạng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật. Như một sự lựa chọn, nút AMF có thể lựa chọn, dựa vào các điều kiện kích hoạt khác nhau, để xóa khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật và ký hiệu nhận dạng khóa được sử dụng để nhận dạng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật, trước khi khóa dùng cho kết nối thứ hai được cập nhật.

Bước 911. Nút AMF gửi tin nhắn NAS SMC tới đầu cuối qua kết nối thứ hai. Một cách tương ứng, đầu cuối thu tin nhắn NAS SMC từ nút AMF qua kết nối thứ hai.

Nếu kết nối thứ nhất và kết nối thứ hai chia sẻ tập hợp các khóa, tin nhắn NAS SMC mang ký hiệu nhận dạng khóa thứ nhất.

Một cách tùy ý, nếu kết nối thứ nhất và kết nối thứ hai sử dụng các khóa khác nhau, tin nhắn NAS SMC mang ký hiệu nhận dạng khóa thứ ba.

Bước 912. Đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Một cách tùy ý, sau khi thu tin nhắn NAS SMC, đầu cuối cập nhật khóa dùng cho kết nối thứ hai. Một cách tùy ý, khóa dùng cho kết nối thứ hai có thể được cập nhật dựa vào ký hiệu nhận dạng khóa thứ nhất hoặc ký hiệu nhận dạng khóa thứ ba được mang trong tin nhắn NAS SMC.

Một cách tùy ý, sau khi đầu cuối bắt đầu bộ định thời, nếu bộ định thời của đầu cuối không kết thúc, đầu cuối dừng bộ định thời sau khi cập nhật khóa dùng cho kết nối thứ hai.

Sau khi cập nhật khóa dùng cho kết nối thứ hai, đầu cuối có thể xóa khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật và ký hiệu nhận dạng khóa được sử dụng để nhận dạng khóa dùng cho kết nối thứ hai mà được sử dụng trước khi cập nhật.

Bước 913. Đầu cuối gửi tin nhắn NAS SMP tới nút AMF qua kết nối thứ hai. Một cách tương ứng, nút AMF thu tin nhắn NAS SMP qua kết nối thứ hai.

Việc bảo vệ tính toàn vẹn của tin nhắn NAS SMP được thực hiện dựa vào khóa được cập nhật.

Một cách tùy ý, sau khi thiết bị mạng lõi bắt đầu bộ định thời, nếu bộ định thời của thiết bị mạng lõi không kết thúc, thiết bị mạng lõi dừng bộ định thời sau khi cập

nhật khóa dùng cho kết nối thứ hai.

Bước 914. Nút AMF gửi tin nhắn hoàn thành tới đầu cuối qua kết nối thứ hai. Một cách tương ứng, đầu cuối thu tin nhắn hoàn thành qua kết nối thứ hai.

Tin nhắn hoàn thành là tin nhắn phản hồi của tin nhắn NAS trong bước 901. Ví dụ, nếu tin nhắn NAS trong bước 901 là tin nhắn yêu cầu đăng ký, tin nhắn hoàn thành là tin nhắn hoàn thành đăng ký.

Có thể được hiểu rằng đầu cuối hoặc thiết bị mạng lõi có thể thực hiện một số hoặc tất cả các bước trong phương án nêu trên. Các bước hoặc các hoạt động này chỉ là các ví dụ. Trong các phương án của sáng chế, các hoạt động khác hoặc các sự thay đổi của các hoạt động khác nhau có thể còn được thực hiện. Ngoài ra, các bước có thể được thực hiện theo trình tự khác với các bước được thể hiện trong phương án nêu trên, và có khả năng là không phải tất cả các hoạt động trong phương án nêu trên cần được thực hiện.

Một cách tùy ý, trong kịch bản thực hiện tương ứng với Fig.5, khi nút AMF xác định rằng nút AMF cần thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, nút AMF cần xác định trạng thái của kết nối thứ hai, và có thể thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất chỉ khi trạng thái của kết nối thứ hai là trạng thái nghỉ. Như được thể hiện trên Fig.10, phương pháp bao gồm bước 1001 tới bước 1012.

Bước 1001 tới bước 1002 giống như bước 901 tới bước 902, và các chi tiết không được mô tả lại ở đây.

Bước 1003. Nút AMF xác định trạng thái của kết nối thứ hai.

Khi nút AMF xác định rằng nút AMF cần thực hiện việc tái xác thực trên đầu cuối, phương pháp tái xác thực được sử dụng khi kết nối thứ hai ở trạng thái được kết nối khác với phương pháp xác thực được sử dụng khi kết nối thứ hai ở trạng thái nghỉ hoặc trạng thái không đăng ký. Do đó, nút AMF cần xác định xem kết nối thứ hai có ở trạng thái được kết nối hay không.

Một cách tùy ý, ví dụ, đầu cuối hỗ trợ việc truy cập nút AMF bằng cách sử dụng đồng thời cả công nghệ truy cập 3GPP và công nghệ truy cập không phải 3GPP. Nút AMF có thể đầu tiên xác định xem đầu cuối có truy cập nút AMF bằng cách sử dụng đồng thời cả công nghệ truy cập 3GPP và công nghệ truy cập không phải 3GPP hay

không. Nếu đầu cuối truy cập nút AMF bằng cách sử dụng đồng thời cả công nghệ truy cập 3GPP và công nghệ truy cập không phải 3GPP, điều này chỉ báo rằng kết nối thứ hai tồn tại giữa nút AMF và đầu cuối và sau đó việc xem kết nối thứ hai của đầu cuối có ở trạng thái được kết nối hay không được xác định.

Để xác định nhanh xem kết nối thứ hai có ở trạng thái được kết nối hay không, nút AMF có thể đầu tiên xác định xem kết nối thứ hai của đầu cuối có ở trạng thái đăng ký hay không. Nếu xác định rằng kết nối thứ hai của đầu cuối ở trạng thái bỏ đăng ký, nút AMF có thể xác định rằng kết nối thứ hai của đầu cuối không thể ở trong trạng thái được kết nối. Nếu xác định rằng kết nối thứ hai của đầu cuối ở trạng thái đăng ký, nút AMF còn xác định xem kết nối thứ hai của đầu cuối có ở trạng thái được kết nối hay không.

Có ít nhất ba phương pháp sau đây dùng cho nút AMF để xác định xem đầu cuối có truy cập nút AMF bằng cách sử dụng đồng thời hai công nghệ truy cập hay không:

(1) Tin nhắn NAS trong bước 1001 mang thông tin chỉ báo được sử dụng để chỉ báo rằng kết nối thứ hai của đầu cuối ở trạng thái đăng ký, và nút AMF có thể xác định, dựa vào thông tin chỉ báo, rằng kết nối thứ hai của đầu cuối ở trạng thái đăng ký, nghĩa là, đầu cuối truy cập nút AMF bằng cách sử dụng hai công nghệ truy cập.

Theo phương pháp này, nút AMF có thể xác định trực tiếp trạng thái của kết nối thứ hai của đầu cuối dựa vào thông tin chỉ báo thu được. Điều này là thuận lợi và nhanh chóng, và nút AMF không cần thực hiện truy vấn khác.

(2) Nút AMF xác định, bằng cách truy vấn máy trạng thái của đầu cuối mà được duy trì bởi nút AMF, rằng đầu cuối vẫn có trạng thái đăng ký khác kết hợp với công nghệ truy cập khác ngoài công nghệ truy cập tương ứng với kết nối thứ nhất.

Theo phương pháp này, nút AMF có thể xác định trạng thái của kết nối thứ hai bằng cách sử dụng hoạt động truy vấn đơn giản, và đầu cuối không cần bổ sung thêm, tới tin nhắn NAS, thông tin chỉ báo được sử dụng để chỉ báo trạng thái của kết nối thứ hai.

(3) Nút AMF lưu trữ thông tin lệnh được sử dụng để lệnh đầu cuối sử dụng đồng thời hai công nghệ truy cập để truy cập.

Ví dụ, khi đầu cuối đã truy cập nút AMF bằng cách sử dụng công nghệ truy cập

(ví dụ, công nghệ truy cập 3GPP), nếu nút AMF xác định rằng đầu cuối truy cập thành công nút AMF bằng cách sử dụng công nghệ truy cập khác (ví dụ, công nghệ truy cập không phải 3GPP), nút AMF có thể thiết đặt ký hiệu nhận dạng trong ngữ cảnh của đầu cuối. Ký hiệu nhận dạng được sử dụng để chỉ báo số lượng các công nghệ truy cập bằng cách sử dụng đầu cuối mà hiện đang truy cập nút AMF. Ví dụ, khi ký hiệu nhận dạng bằng 0, nó chỉ báo rằng đầu cuối truy cập nút AMF bằng cách sử dụng một công nghệ truy cập. Khi ký hiệu nhận dạng bằng 1, nó chỉ báo rằng đầu cuối truy cập nút AMF bằng cách sử dụng đồng thời hai công nghệ truy cập, hoặc chỉ báo rằng đầu cuối ở trong trạng thái đăng ký kép. Trạng thái đăng ký kép là trạng thái trong đó đầu cuối đăng ký với nút AMF bằng cách sử dụng hai công nghệ truy cập.

Theo ví dụ khác, nút AMF có thể thiết đặt thông tin chỉ báo cho tệp được chia sẻ bởi hai công nghệ truy cập, để chỉ báo rằng nội dung trong tệp được chia sẻ được chia sẻ bởi hai công nghệ truy cập. Trước khi nội dung trong tệp được xóa hoặc được thay đổi, cần được xác định xem nội dung trong tệp có đang được sử dụng hay không. Nội dung trong tệp có thể là khóa NAS và thuật toán bảo mật liên quan được chia sẻ bởi hai công nghệ truy cập. Nút AMF có thể xác định, dựa vào thông tin chỉ báo tương ứng với tệp, rằng đầu cuối truy cập nút AMF bằng cách sử dụng đồng thời hai công nghệ truy cập.

Ngoài ra, có ít nhất ba cách thực hiện khả thi sau đây dùng cho nút AMF để xác định xem kết nối thứ hai của đầu cuối có ở trạng thái được kết nối hay không:

(1) Nút AMF xác định rằng nút AMF đang truyền thông với đầu cuối qua kết nối thứ hai.

Ví dụ, nút AMF đang gửi tin nhắn NAS tới đầu cuối qua kết nối thứ hai, hoặc nút AMF đang tìm gọi đầu cuối qua kết nối thứ hai.

(2) Nút AMF xác định, bằng cách truy vấn máy trạng thái của đầu cuối mà được duy trì bởi nút AMF, rằng kết nối thứ hai của đầu cuối ở trạng thái được kết nối.

(3) Nút AMF xác định, bằng cách sử dụng thông tin chỉ báo được lưu trữ trong nút AMF, rằng kết nối thứ hai của đầu cuối ở trạng thái được kết nối.

Ví dụ, nếu nút AMF tìm kiếm ký hiệu nhận dạng mà được lưu trữ bởi nút AMF và chỉ báo rằng đầu cuối ở trong trạng thái đăng ký kép hoặc trạng thái được kết nối kép,

ví dụ, tìm kiếm ký hiệu nhận dạng mà bằng 1, nút AMF xác định rằng kết nối thứ hai của đầu cuối ở trạng thái được kết nối.

Theo ví dụ khác, nếu nút AMF nhận thấy rằng thông tin chỉ báo tương ứng với tệp được lưu trữ trong nút AMF chỉ báo rằng nội dung trong tệp được chia sẻ bởi hai công nghệ truy cập, và nội dung trong tệp không thể thay đổi, điều này chỉ báo rằng nội dung trong tệp đang được sử dụng bởi kết nối thứ hai, và nút AMF có thể còn xác định rằng kết nối thứ hai của đầu cuối ở trạng thái được kết nối.

Theo phương án này, ví dụ trong đó trạng thái của kết nối thứ hai là trạng thái được kết nối được sử dụng để mô tả.

Bước 1004. Nút AMF gửi tin nhắn từ chối hoặc tin nhắn chấp nhận tới đầu cuối qua kết nối thứ nhất.

Tin nhắn thứ nhất trong bước 501 có thể là tin nhắn từ chối hoặc tin nhắn chấp nhận trong bước này. Tin nhắn từ chối chỉ báo rằng nút AMF từ chối tin nhắn NAS được gửi bởi đầu cuối trong bước 1001, ví dụ, từ chối tin nhắn yêu cầu đăng ký được gửi bởi đầu cuối. Một cách tùy ý, tin nhắn từ chối mang giá trị nguyên nhân, và giá trị nguyên nhân được sử dụng để thông báo đầu cuối rằng nguyên nhân từ chối là kết nối thứ hai ở trạng thái được kết nối. Trong trường hợp này, việc tái xác thực không thể được thực hiện trên đầu cuối. Một cách tùy ý, giá trị nguyên nhân còn được sử dụng để chỉ báo rằng xác nhận tính toàn vẹn được thực hiện bởi nút AMF trên tin nhắn NAS được gửi bởi đầu cuối trong bước 1101 thành công.

Một cách tùy ý, nếu số đếm NAS tương ứng với kết nối thứ nhất không vòng lại một cách tạm thời, nút AMF còn cho phép đầu cuối tiếp tục gửi số lượng được định rõ của tin nhắn NAS, hoặc đầu cuối gửi tin nhắn đăng ký theo chu kỳ tới nút AMF qua kết nối thứ nhất, nút AMF có thể gửi tin nhắn chấp nhận tới đầu cuối qua kết nối thứ nhất.

Tin nhắn chấp nhận mang thông tin bit cờ tái xác thực, và thông tin bit cờ tái xác thực được sử dụng để thông báo đầu cuối rằng việc tái xác thực cần được thực hiện trên đầu cuối. Tuy nhiên, do kết nối thứ hai ở trạng thái được kết nối, việc tái xác thực không thể được khởi tạo một cách tạm thời. Sau khi đầu cuối thu bit cờ tái xác thực, thao tác của đầu cuối bị giới hạn. Ví dụ, việc tái xác thực ký hiệu nhận dạng có thể được sử dụng để lệnh đầu cuối hoãn việc sử dụng kết nối thứ nhất, hoặc đầu cuối có thể gửi dữ liệu

mặt phẳng người dùng chỉ qua qua kết nối thứ nhất, hoặc đầu cuối có thể gửi số lượng được định rõ (ví dụ, một) của tin nhắn NAS chỉ qua qua kết nối thứ nhất (mà có nghĩa là ngữ cảnh bảo mật của kết nối thứ nhất có thể còn được sử dụng một lần), hoặc đầu cuối có thể gửi, chỉ qua qua kết nối thứ nhất, tin nhắn yêu cầu đăng ký mà trên đó việc bảo vệ tính toàn vẹn không được thực hiện.

Thông tin bit cờ tái xác thực có thể tùy chọn là thông tin bộ định thời. Nếu việc tái xác thực không được thực hiện trên đầu cuối trước khi bộ định thời kết thúc, nút AMF khiến đầu cuối có trạng thái bỏ đăng ký. Một cách tùy ý, nút AMF xóa tất cả ngữ cảnh bảo mật của đầu cuối sao cho đầu cuối cần thực hiện việc tái xác thực khi truy cập mạng lần tiếp theo.

Bước 1005. Đầu cuối xác định rằng kết nối thứ hai được chuyển đổi sang trạng thái nghỉ.

Bước 1006. Đầu cuối gửi tin nhắn NAS tới nút AMF bằng cách sử dụng kết nối bất kỳ. Một cách tương ứng, nút AMF thu tin nhắn NAS. Kết nối để gửi tin nhắn NAS trở thành kết nối thứ nhất trong sáng chế.

Một cách tùy ý, tin nhắn NAS có thể là tin nhắn yêu cầu đăng ký.

Nếu đầu cuối thu tin nhắn từ chối trong bước 1004, đầu cuối có thể gửi tin nhắn NAS tới nút AMF bằng cách sử dụng kết nối bất kỳ.

Nếu đầu cuối thu tin nhắn chấp nhận trong bước 1004, và bit cờ tái xác thực chỉ báo rằng đầu cuối có thể gửi số lượng được định rõ của các tin nhắn NAS qua kết nối thứ nhất, đầu cuối có thể gửi, tới nút AMF qua kết nối thứ nhất, một tin nhắn NAS mà trên đó việc bảo vệ tính toàn vẹn được thực hiện. Nếu bit cờ tái xác thực chỉ báo rằng đầu cuối có thể gửi tin nhắn yêu cầu đăng ký mà trên đó việc bảo vệ bảo mật không được thực hiện, đầu cuối có thể gửi, tới thiết bị mạng lõi qua kết nối thứ nhất hoặc kết nối thứ hai, tin nhắn yêu cầu đăng ký mà trên đó việc bảo vệ bảo mật không được thực hiện.

Có thể được hiểu rằng nếu nút AMF thu tin nhắn NAS mà trên đó việc bảo vệ tính toàn vẹn được thực hiện, nút AMF thực hiện đầu tiên việc xác nhận bảo vệ tính toàn vẹn trên tin nhắn NAS.

Bước 1005 và bước 1006 là các bước tùy chọn, nghĩa là, sau bước 1004, bước

1007 có thể được thực hiện trực tiếp.

Bước 1007. Nút AMF xác định rằng kết nối thứ hai ở trạng thái nghỉ.

Đối với phương pháp xác định trạng thái của kết nối thứ hai bởi nút AMF, xem phần mô tả liên quan của bước 1003. Các chi tiết không được mô tả lại ở đây.

Bước 1008. Nút AMF thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất.

Một cách tùy ý, nếu đầu cuối gửi tin nhắn NAS tới nút AMF qua kết nối thứ hai trong bước 1006, nút AMF có thể thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ hai trong bước này. Phần mô tả sau đây sử dụng ví dụ trong đó nút AMF thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất.

Một cách tùy ý, trong bước này, nút AMF có thể cập nhật khóa dùng cho kết nối thứ nhất và khóa dùng cho kết nối thứ hai, và đầu cuối có thể cập nhật khóa dùng cho kết nối thứ nhất. Một cách tùy ý, nếu kết nối thứ nhất và kết nối thứ hai chia sẻ tập hợp các khóa NAS, nút AMF có thể thu được ký hiệu nhận dạng khóa thứ nhất trong quá trình thực hiện việc tái xác thực trên đầu cuối mà ở đó ký hiệu nhận dạng khóa thứ nhất được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ nhất và khóa được cập nhật dùng cho kết nối thứ hai.

Như một sự lựa chọn, nếu kết nối thứ nhất và kết nối thứ hai sử dụng riêng rẽ các khóa NAS khác nhau, nút AMF có thể thu được ký hiệu nhận dạng khóa thứ nhất trong quá trình thực hiện việc tái xác thực trên đầu cuối. Một cách tùy ý, nút AMF có thể còn thu được ký hiệu nhận dạng khóa thứ ba. Trong trường hợp này, ký hiệu nhận dạng khóa thứ nhất được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ nhất, và ký hiệu nhận dạng khóa thứ ba được sử dụng để chỉ báo khóa được cập nhật dùng cho kết nối thứ hai.

Bước 1009. Nút AMF gửi tin nhắn NAS SMC tới đầu cuối. Một cách tương ứng, đầu cuối thu tin nhắn NAS SMC.

Một cách tùy ý, tin nhắn NAS SMC có thể mang thông tin lệnh thứ nhất trong bước 504.

Thông tin lệnh thứ nhất được sử dụng để lệnh đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Một cách tùy ý, thông tin lệnh thứ nhất có thể là ký hiệu nhận dạng khóa thứ nhất hoặc ký hiệu nhận dạng khóa thứ hai. Như một sự lựa chọn, thông tin lệnh thứ nhất có thể là ký hiệu nhận dạng khóa thứ nhất và ký hiệu nhận dạng khóa thứ hai.

Việc bảo vệ tính toàn vẹn có thể được thực hiện trên tin nhắn NAS SMC bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ nhất, và đầu cuối có thể thực hiện việc xác nhận bảo vệ tính toàn vẹn trên tin nhắn NAS SMC bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ nhất.

Bước 1010. Đầu cuối cập nhật khóa dùng cho kết nối thứ hai dựa vào thông tin lệnh thứ nhất.

Bước 1011. Đầu cuối gửi tin nhắn NAS SMP tới nút AMF qua kết nối thứ nhất; một cách tương ứng, nút AMF thu tin nhắn NAS SMP qua kết nối thứ nhất.

Việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMP bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ nhất.

Một cách tùy ý, đầu cuối có thể còn gửi tin nhắn NAS SMP tới nút AMF qua kết nối thứ hai. Trong trường hợp này, việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMP bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai.

Bước 1012. Nút AMF gửi tin nhắn hoàn thành tới đầu cuối qua kết nối thứ nhất. Một cách tương ứng, đầu cuối thu tin nhắn hoàn thành từ nút AMF qua kết nối thứ nhất.

Tin nhắn hoàn thành là tin nhắn phản hồi của tin nhắn NAS trong bước 1001. Ví dụ, nếu tin nhắn NAS trong bước 1001 là tin nhắn yêu cầu đăng ký, tin nhắn hoàn thành là tin nhắn hoàn thành đăng ký.

Có thể được hiểu rằng nếu đầu cuối gửi sau đó tin nhắn NAS tới đầu cuối qua kết nối thứ hai, việc bảo vệ tính toàn vẹn có thể được thực hiện trên tin nhắn NAS bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai.

Có thể được hiểu rằng đầu cuối hoặc thiết bị mạng lõi có thể thực hiện một số hoặc tất cả các bước trong phương án nêu trên. Các bước hoặc các hoạt động này chỉ là các ví dụ. Trong các phương án của sáng chế, các hoạt động khác hoặc các sự thay đổi của các hoạt động khác nhau có thể còn được thực hiện. Ngoài ra, các bước có thể được thực hiện theo trình tự khác với các bước được thể hiện trong phương án nêu trên, và có khả năng là không phải tất cả các hoạt động trong phương án nêu trên cần được thực

hiện.

Một cách tùy ý, trong các kịch bản thực hiện tương ứng với Fig.7 và Fig.8, khi nút AMF xác định rằng nút AMF cần thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, nếu nhánh thứ hai ở trạng thái được kết nối, thiết bị mạng lõi có thể thực hiện đầu tiên việc tái xác thực trên đầu cuối qua kết nối thứ nhất. Như được thể hiện trên Fig.11, phương pháp này bao gồm bước 1101 tới bước 1115.

Bước 1101 tới bước 1103 giống như bước 1001 tới bước 1003, và các chi tiết không được mô tả lại ở đây.

Bước 1104. Nút AMF thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất.

Cả nút AMF và đầu cuối có thể cập nhật khóa dùng cho kết nối thứ nhất trong quy trình tái xác thực.

Bước 1105. Nút AMF gửi tin nhắn NAS SMC tới đầu cuối qua kết nối thứ nhất. Một cách tương ứng, đầu cuối thu tin nhắn NAS SMC từ nút AMF qua kết nối thứ nhất.

Việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMC bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ nhất, và đầu cuối có thể thực hiện việc xác nhận bảo vệ tính toàn vẹn trên tin nhắn NAS SMC bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ nhất.

Một cách tùy ý, tin nhắn NAS SMC mang thông tin lệnh thứ hai trong bước 802, trong đó thông tin lệnh thứ hai được sử dụng để lệnh đầu cuối cập nhật khóa dùng cho kết nối thứ hai, hoặc thông tin lệnh thứ hai có thể được sử dụng để lệnh đầu cuối không cập nhật khóa dùng cho kết nối thứ hai.

Bước 1106. Đầu cuối gửi tin nhắn NAS SMP tới nút AMF qua kết nối thứ nhất.

Bước 1107. Nút AMF thiết đặt dấu thứ nhất.

Dấu thứ nhất được sử dụng để đánh dấu rằng thiết bị mạng lõi đã thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất, hoặc được sử dụng để lệnh cập nhật khóa dùng cho kết nối thứ hai.

Bước 1108. Đầu cuối thiết đặt dấu thứ hai.

Dấu thứ hai được sử dụng để lệnh cập nhật khóa dùng cho kết nối thứ hai.

Một cách tùy ý, bước 1108 cần được thực hiện chỉ khi thông tin lệnh thứ hai được

thu bởi đầu cuối được sử dụng để lệnh đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Bước 1109. Nút AMF gửi tin nhắn chấp nhận đăng ký tới đầu cuối qua kết nối thứ nhất. Một cách tương ứng, đầu cuối thu tin nhắn chấp nhận đăng ký từ nút AMF qua kết nối thứ nhất.

Bước 1110. Đầu cuối xác định rằng kết nối thứ hai được chuyển đổi sang trạng thái nghỉ. Nếu xác định rằng dấu thứ ba tồn tại, đầu cuối cập nhật khóa dùng cho kết nối thứ hai.

Một cách tùy ý, nếu đầu cuối không thiết đặt dấu thứ ba, bước 1111 cần được thực hiện khi kết nối thứ hai được chuyển đổi sang trạng thái nghỉ.

Bước 1111. Nút AMF xác định rằng kết nối thứ hai được chuyển đổi sang trạng thái nghỉ. Nếu xác định rằng dấu thứ nhất tồn tại, nút AMF cập nhật khóa dùng cho kết nối thứ hai.

Một cách tùy ý, nếu kết nối thứ hai vẫn trong trạng thái được kết nối, nút AMF có thể hoãn việc sử dụng kết nối thứ hai. Như một sự lựa chọn, khi xử lý tin nhắn NAS mà được gửi bởi đầu cuối qua kết nối thứ hai, nếu nút AMF tìm kiếm dấu thứ nhất, nút AMF có thể hoãn việc sử dụng kết nối thứ hai, sau đó cập nhật khóa dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ hai, và gửi tin nhắn NAS SMC tới đầu cuối qua kết nối thứ hai. Tin nhắn NAS SMC mang ký hiệu nhận dạng khóa được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ hai, sao cho đầu cuối có thể cập nhật khóa dùng cho kết nối thứ hai dựa vào ký hiệu nhận dạng khóa. Có thể được hiểu rằng, sau khi cả nút AMF và đầu cuối cập nhật khóa dùng cho kết nối thứ hai, nút AMF có thể tiếp tục lại việc sử dụng kết nối thứ hai, và thực hiện, bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai, việc bảo vệ tính toàn vẹn trên tin nhắn NAS được truyền qua kết nối thứ hai.

Bước 1112. Đầu cuối gửi tin nhắn yêu cầu đăng ký tới nút AMF qua kết nối thứ hai. Một cách tương ứng, nút AMF thu tin nhắn yêu cầu đăng ký từ đầu cuối qua kết nối thứ hai.

Việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn yêu cầu đăng ký bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai.

Bước 1113. Nút AMF gửi tin nhắn NAS SMC tới đầu cuối qua kết nối thứ hai.

Một cách tương ứng, đầu cuối thu tin nhắn NAS SMC từ nút AMF qua kết nối thứ hai.

Tin nhắn NAS SMC mang ký hiệu nhận dạng khóa được sử dụng để nhận dạng khóa được cập nhật dùng cho kết nối thứ hai. Một cách tùy ý, tin nhắn NAS SMC có thể còn mang ít nhất một thông số được sử dụng để cập nhật khóa dùng cho kết nối thứ hai.

Bước 1114. Đầu cuối gửi tin nhắn NAS SMP tới nút AMF qua kết nối thứ hai. Một cách tương ứng, nút AMF thu tin nhắn NAS SMP từ đầu cuối qua kết nối thứ hai.

Việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMP bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai.

Bước 1115. Nút AMF phản hồi tới đầu cuối bằng tin nhắn chấp nhận đăng ký qua kết nối thứ hai. Một cách tương ứng, đầu cuối thu tin nhắn chấp nhận đăng ký từ nút AMF qua kết nối thứ hai.

Việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn chấp nhận đăng ký bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ hai.

Có thể được hiểu rằng đầu cuối hoặc thiết bị mạng lõi có thể thực hiện một số hoặc tất cả các bước trong phương án nêu trên. Các bước hoặc các hoạt động này chỉ là các ví dụ. Trong các phương án của sáng chế, các hoạt động khác hoặc các sự thay đổi của các hoạt động khác nhau có thể còn được thực hiện. Ngoài ra, các bước có thể được thực hiện theo trình tự khác với các bước được thể hiện trong phương án nêu trên, và có khả năng là không phải tất cả các hoạt động trong phương án nêu trên cần được thực hiện.

Theo kịch bản thực hiện khả thi khác, điều kiện kích hoạt việc cập nhật khóa dùng cho kết nối thứ hai liên quan đến bộ định thời và trạng thái của kết nối thứ hai. Như được thể hiện trên Fig.12, phương pháp này bao gồm bước 1201 tới bước 1212.

Trong bước 1201 tới bước 1208, đầu cuối truyền thông với thiết bị mạng lõi qua kết nối thứ nhất.

Bước 1201. Đầu cuối gửi tin nhắn yêu cầu đăng ký tới thiết bị mạng lõi qua kết nối thứ nhất; một cách tương ứng, nút AMF thu tin nhắn yêu cầu đăng ký.

Một cách tùy ý, tin nhắn yêu cầu đăng ký có thể tùy chọn là tin nhắn NAS trong bước 901. Xem chi tiết tại phần mô tả liên quan của bước 901. Các chi tiết không được mô tả lại ở đây.

Bước 1202. Thiết bị mạng lõi kích hoạt việc tái xác thực.

Bước 1203. Thiết bị mạng lõi và đầu cuối thực hiện thủ tục tái xác thực.

Bước 1204. Thiết bị mạng lõi gửi tin nhắn NAS SMC tới đầu cuối. Một cách tương ứng, đầu cuối thu tin nhắn NAS SMC.

Bước 1205. Đầu cuối kích hoạt khóa mới dùng cho kết nối thứ nhất, và bắt đầu bộ định thời.

Đầu cuối kích hoạt khóa mới dùng cho kết nối thứ nhất có nghĩa là khóa dùng cho kết nối thứ nhất đã được cập nhật, và sau đó đầu cuối thực hiện việc bảo vệ bảo mật bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ nhất, trên tin nhắn NAS mà được gửi bởi đầu cuối sau đó tới thiết bị mạng lõi qua kết nối thứ nhất.

Bước 1206. Đầu cuối gửi tin nhắn NAS SMP tới thiết bị mạng lõi. Một cách tương ứng, đầu cuối thu tin nhắn NAS SMP từ thiết bị mạng lõi.

Bước 1207. Thiết bị mạng lõi kích hoạt khóa mới dùng cho kết nối thứ nhất, và bắt đầu bộ định thời.

Thiết bị mạng lõi kích hoạt khóa mới dùng cho kết nối thứ nhất có nghĩa là khóa dùng cho kết nối thứ nhất đã được cập nhật, và sau đó thiết bị mạng lõi thực hiện việc bảo vệ bảo mật, bằng cách sử dụng khóa được cập nhật dùng cho kết nối thứ nhất, trên tin nhắn NAS mà được gửi bởi thiết bị mạng lõi sau đó tới đầu cuối qua kết nối thứ nhất.

Bước 1208. Thiết bị mạng lõi gửi tin nhắn hoàn thành đăng ký tới đầu cuối. Một cách tương ứng, đầu cuối thu tin nhắn hoàn thành đăng ký.

Trong bước 1209 tới bước 1212, đầu cuối truyền thông với thiết bị mạng lõi qua kết nối thứ hai.

Bước 1209. Trước khi bộ định thời kết thúc, nếu kết nối thứ hai ở trạng thái nghỉ, đầu cuối xóa khóa cũ dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa cũ, cho phép khóa mới dùng cho kết nối thứ hai, và dừng bộ định thời.

Nếu kết nối thứ nhất và kết nối thứ hai chia sẻ tập hợp các khóa, khóa mới dùng cho kết nối thứ hai giống như khóa mới dùng cho kết nối thứ nhất. Ký hiệu nhận dạng khóa thứ nhất được sử dụng để chỉ báo khóa mới dùng cho kết nối thứ nhất và khóa mới dùng cho kết nối thứ hai.

Một cách tùy ý, trước khi bộ định thời kết thúc, nếu kết nối thứ hai ở trạng thái

được kết nối, đầu cuối có thể vẫn sử dụng khóa cũ dùng cho kết nối thứ hai.

Bước 1210. Đầu cuối gửi tin nhắn yêu cầu đăng ký tới thiết bị mạng lõi. Một cách tương ứng, thiết bị mạng lõi thu tin nhắn yêu cầu đăng ký.

Việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn yêu cầu đăng ký bằng cách sử dụng khóa mới dùng cho kết nối thứ hai, và tin nhắn yêu cầu đăng ký mang ký hiệu nhận dạng khóa thứ nhất.

Bước 1211. Thiết bị mạng lõi xác định, dựa vào ký hiệu nhận dạng khóa thứ nhất, để cho phép khóa mới dùng cho kết nối thứ hai, xóa khóa cũ dùng cho kết nối thứ hai, và dừng bộ định thời.

Sau khi thu tin nhắn yêu cầu đăng ký, thiết bị mạng lõi có thể xác định, dựa vào ký hiệu nhận dạng khóa thứ nhất, rằng khóa mới dùng cho kết nối thứ hai giống như khóa mới dùng cho kết nối thứ nhất, và còn thực hiện xác nhận tính toàn vẹn trên tin nhắn yêu cầu đăng ký bằng cách sử dụng khóa mới dùng cho kết nối thứ hai. Sau khi xác nhận thành công, thiết bị mạng lõi xóa khóa cũ dùng cho kết nối thứ hai, và dừng bộ định thời.

Bước 1212. Thiết bị mạng lõi gửi tin nhắn hoàn thành đăng ký tới đầu cuối; một cách tương ứng, đầu cuối thu tin nhắn hoàn thành đăng ký từ thiết bị mạng lõi.

Việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn hoàn thành đăng ký bằng cách sử dụng khóa mới dùng cho kết nối thứ hai.

Theo cách thực hiện khả thi khác, như được thể hiện trên Fig.13, điều kiện kích hoạt việc cập nhật khóa dùng cho kết nối thứ hai không liên quan đến trạng thái của kết nối thứ hai. Như được thể hiện trên Fig.13, phương pháp bao gồm bước 1301 tới bước 1314.

Bước 1301 tới bước 1308 giống như bước 1201 tới bước 1208, và các chi tiết không được mô tả lại ở đây.

Trong bước 1309 tới bước 1314, đầu cuối truyền thông với thiết bị mạng lõi qua kết nối thứ hai.

Bước 1309. Trước khi bộ định thời kết thúc, đầu cuối xác định sử dụng khóa cũ dùng cho kết nối thứ hai.

Ký hiệu nhận dạng khóa thứ hai được sử dụng để nhận dạng khóa cũ dùng cho

kết nối thứ hai. Có thể được hiểu rằng, theo phương án này của sáng chế, khóa mới là khóa được cập nhật, và khóa cũ là khóa mà được sử dụng trước khi cập nhật. Khi kết nối thứ nhất và kết nối thứ hai chia sẻ tập hợp các khóa, khóa cũ dùng cho kết nối thứ hai giống như khóa trước khi kết nối thứ nhất được sử dụng cho việc tái xác thực.

Bước 1310. Đầu cuối gửi, tới thiết bị mạng lõi, tin nhắn yêu cầu đăng ký mà trên đó việc bảo vệ tính toàn vẹn được thực hiện bằng cách sử dụng khóa cũ dùng cho kết nối thứ hai, trong đó tin nhắn yêu cầu đăng ký mang ký hiệu nhận dạng khóa thứ hai. Một cách tương ứng, thiết bị mạng lõi thu tin nhắn yêu cầu đăng ký.

Bước 1311. Thiết bị mạng lõi xác định, dựa vào ký hiệu nhận dạng khóa thứ hai, khóa cũ dùng cho kết nối thứ hai, và thực hiện xác nhận tính toàn vẹn trên tin nhắn yêu cầu đăng ký bằng cách sử dụng khóa cũ dùng cho kết nối thứ hai.

Bước 1312. Thiết bị mạng lõi gửi tin nhắn hoàn thành đăng ký tới đầu cuối.

Bước 1313. Sau khi bộ định thời kết thúc, đầu cuối xóa khóa cũ dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa thứ hai.

Bước 1314. Sau khi bộ định thời kết thúc, thiết bị mạng lõi xóa khóa cũ dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa thứ hai.

Sau khi xóa khóa cũ dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa thứ hai, đầu cuối và thiết bị mạng lõi có thể sử dụng khóa mới dùng cho kết nối thứ nhất làm khóa mới dùng cho kết nối thứ hai.

Một cách tùy ý, theo phương pháp thủ tục trên Fig.13, trước khi các bộ định thời của đầu cuối và thiết bị mạng lõi kết thúc, nếu thiết bị mạng lõi kích hoạt lại thủ tục tái xác thực, các bộ định thời của đầu cuối và thiết bị mạng lõi có thể tiếp tục thực hiện việc định thời. Sau khi các bộ định thời kết thúc, bước 1313 và bước 1314 được thực hiện. Như một sự lựa chọn, đầu cuối và thiết bị mạng lõi có thể bắt đầu lại việc định thời, và sau khi bộ định thời kết thúc, thực hiện bước 1313 và bước 1314.

Phần trên đây mô tả chủ yếu các giải pháp được đề xuất trong các phương án của sáng chế từ phối cảnh của sự tương tác giữa thiết bị mạng lõi và đầu cuối. Có thể được hiểu rằng để thực hiện các chức năng nêu trên, đầu cuối và thiết bị mạng lõi bao gồm các cấu trúc phần cứng và/hoặc các môđun phần mềm tương ứng để thực hiện các chức năng. Dựa trên các bộ phận và các bước thuật toán trong các ví dụ được mô tả trong các

phương án được bộc lộ trong sáng chế này, các phương án của sáng chế có thể được thực hiện theo dạng phần cứng hoặc dạng kết hợp của phần cứng và phần mềm máy tính. Việc xem chức năng được thực hiện bởi phần cứng hay phần cứng được điều khiển bởi phần mềm máy tính phụ thuộc vào các ứng dụng cụ thể và các hạn chế thiết kế của các giải pháp kỹ thuật. Người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể sử dụng các phương pháp khác nhau để thực hiện được mô tả các chức năng cho mỗi ứng dụng cụ thể, nhưng không được xem rằng việc thực hiện trệch khỏi phạm vi của các giải pháp kỹ thuật trong các phương án của sáng chế.

Theo các phương án của sáng chế, việc phân chia thành các bộ phận chức năng có thể được thực hiện trên đầu cuối và thiết bị mạng lõi dựa vào các ví dụ phương pháp nêu trên. Ví dụ, mỗi bộ phận chức năng có thể thu được qua việc phân chia dựa vào chức năng tương ứng, hoặc hai hoặc nhiều chức năng có thể được tích hợp thành một bộ phận xử lý. Bộ phận được tích hợp có thể được thực hiện theo dạng phần cứng, hoặc có thể được thực hiện theo dạng bộ phận chức năng phần mềm. Cần chú ý rằng, trong các phương án của sáng chế, việc phân chia thành các bộ phận được sử dụng làm ví dụ, và chỉ là việc phân chia chức năng lôgic. Trong sự thực hiện thực tế, cách phân chia khác có thể được sử dụng.

Khi bộ phận được tích hợp được sử dụng, Fig.14 là sơ đồ khối giản lược của thiết bị theo phương án của sáng chế. Thiết bị này có thể tồn tại theo dạng phần mềm, hoặc có thể là thiết bị mạng lõi, hoặc có thể là chip trong thiết bị mạng lõi. Thiết bị 1400 bao gồm bộ phận xử lý 1402 và bộ phận truyền thông 1403. Bộ phận xử lý 1402 được tạo cấu hình để điều khiển và quản lý thao tác của thiết bị 1400. Ví dụ, bộ phận xử lý 1402 được tạo cấu hình để hỗ trợ thiết bị 1400 trong việc thực hiện các bước 401 và 402 trên Fig.4, các bước 502 và 503 trên Fig.5, các bước 601, 602, 607, và 608 trên Fig.6, các bước 701, 702, 703, và 704 trên Fig.7, các bước 801, 803, và 805 trên Fig.8, các bước 902, 903, 904, và 910 trên Fig.9, các bước 1002, 1003, 1005, 1007, và 1008 trên Fig.10, và các bước 1102, 1103, 1104, 1107, và 1112 trên Fig.11, các bước 1202, 1203, 1207, và 1211 trên Fig.12, các bước 1302, 1303, 1307, 1311, và 1314 trên Fig.13, và/hoặc quy trình khác của công nghệ được mô tả trong bản mô tả này. Bộ phận truyền thông 1403 được tạo cấu hình để hỗ trợ truyền thông giữa thiết bị 1400 và phần tử mạng khác (ví

dụ, đầu cuối). Ví dụ, bộ phận truyền thông 1403 có thể hỗ trợ thiết bị 1400 trong việc thực hiện các bước 501 và 504 trên Fig.5, bước 603 trên Fig.6, bước 705 trên Fig.7, bước 802 trên Fig.8, các bước 905, 908, 911, và 914 trên Fig.9, các bước 1004, 1009, và 1014 trên Fig.10, các bước 1105, 1109, 1113, và 1115 trên Fig.11, các bước 1204, 1208, và 1212 trên Fig.12, và các bước 1304, 1308, và 1312 trên Fig.13. Thiết bị 1400 có thể còn bao gồm bộ phận lưu trữ 1401, được tạo cấu hình để lưu trữ mã chương trình và dữ liệu của thiết bị 1400.

Bộ phận xử lý 1402 có thể là bộ xử lý hoặc bộ điều khiển, chẳng hạn như bộ phận xử lý trung tâm (Central Processing Unit, viết tắt là CPU), bộ xử lý đa năng, bộ xử lý tín hiệu số (Digital Signal Processor, viết tắt là DSP), mạch tích hợp chuyên dụng (Application-Specific Integrated Circuit, viết tắt là ASIC), mảng cổng khả trình dạng trường (Field Programmable Gate Array, viết tắt là FPGA), hoặc thiết bị lôgic khả trình khác, thiết bị lôgic tranzito, thành phần phần cứng, hoặc dạng kết hợp của chúng. Bộ điều khiển/bộ xử lý có thể thực hiện hoặc tiến hành các ví dụ khác nhau của các khối lôgic, các môđun, và các mạch được mô tả có dựa trên nội dung được bộc lộ trong sáng chế. Bộ xử lý có thể là dạng kết hợp của các bộ xử lý mà thực hiện chức năng tính toán, ví dụ, dạng kết hợp của một hoặc nhiều bộ vi xử lý, hoặc dạng kết hợp của DSP và bộ vi xử lý. Bộ phận truyền thông 1403 có thể là giao diện truyền thông, và giao diện truyền thông là thuật ngữ chung. Trong sự thực hiện cụ thể, giao diện truyền thông có thể bao gồm nhiều giao diện, và có thể bao gồm, ví dụ, giao diện giữa các thiết bị truy cập mạng, giao diện giữa thiết bị truy cập mạng và thiết bị mạng lõi, và/hoặc giao diện khác. Bộ phận lưu trữ 1401 có thể là bộ nhớ.

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

Fig.15 thể hiện sơ đồ cấu trúc giản lược khả thi của thiết bị mạng lõi theo phương án của 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 ý, thiết bị mạng lõi 1500 có thể còn bao gồm bus 1504. Giao diện truyền thông 1503, bộ xử lý 1502, và bộ nhớ 1501

có thể được kết nối với nhau bằng cách sử dụng bus 1504. Bus 1504 có thể là PCI bus, EISA bus, hoặc tương tự. Bus 1504 có thể được phân loại thành bus địa chỉ, bus dữ liệu, bus điều khiển, và tương tự. Để thể hiện dễ dàng hơn, chỉ một đường nét đậm được sử dụng để thể hiện bus trên Fig.15, nhưng điều này không có nghĩa là chỉ có một bus hoặc chỉ có một loại bus.

Khi bộ phận được tích hợp được sử dụng, Fig.16 thể hiện sơ đồ khối giản lược của thiết bị khác theo phương án của sáng chế. Thiết bị 1600 có thể tồn tại theo dạng phần mềm, hoặc có thể là đầu cuối hoặc có thể là chip trong đầu cuối. Thiết bị 1600 bao gồm: bộ phận xử lý 1602 và bộ phận truyền thông 1603. Bộ phận xử lý 1602 được tạo cấu hình để điều khiển và quản lý thao tác của thiết bị 1600. Ví dụ, bộ phận xử lý 1602 được tạo cấu hình để hỗ trợ thiết bị 1600 trong việc thực hiện các bước 401 và 403 trên Fig.4, bước 505 trên Fig.5, các bước 604, 605, và 609 trên Fig.6, bước 706 trên Fig.7, và các bước 801, 804, và 806 trên Fig.8, các bước 903, 906, và 912 trên Fig.9, các bước 1008 và 1010 trên Fig.10, các bước 1104, 1108, và 1110 trên Fig.11, các bước 1205 và 1209 trên Fig.12, và các bước 1305, 1309, và 1313 trên Fig.13, và/hoặc quy trình khác của công nghệ được mô tả trong bản mô tả này. Bộ phận truyền thông 1603 được tạo cấu hình để hỗ trợ truyền thông giữa thiết bị 1600 và phần tử mạng khác (chẳng hạn như thiết bị mạng lõi và nút N3IWF). Ví dụ, bộ phận truyền thông 1603 được tạo cấu hình để hỗ trợ thiết bị 1600 trong việc thực hiện bước 606 trên Fig.6, các bước 901, 907, 909, và 913 trên Fig.9, các bước 1001, 1006, và 1011 trên Fig.10, các bước 1101, 1106, 1111, và 1114 trên Fig.11, các bước 1201, 1206, và 1210 trên Fig.12, và các bước 1301, 1306, và 1310 trên Fig.13. Thiết bị 1600 có thể còn bao gồm bộ phận lưu trữ 1601, được tạo cấu hình để lưu trữ mã chương trình và dữ liệu của thiết bị 1600.

Bộ phận xử lý 1602 có thể là bộ xử lý hoặc bộ điều khiển, chẳng hạn như bộ phận xử lý trung tâm (Central Processing Unit, viết tắt là CPU), bộ xử lý đa năng, bộ xử lý tín hiệu số (Digital Signal Processor, viết tắt là DSP), mạch tích hợp chuyên dụng (Application-Specific Integrated Circuit, viết tắt là ASIC), mảng cổng khả trình dạng trường (Field Programmable Gate Array, viết tắt là FPGA), hoặc thiết bị lôgic khả trình khác, thiết bị lôgic tranzito, thành phần phần cứng, hoặc dạng kết hợp của chúng. Bộ điều khiển/bộ xử lý có thể thực hiện hoặc tiến hành các ví dụ khác nhau của các khối

lôgic, các môđun, và các mạch được mô tả có dựa trên nội dung được bộc lộ trong sáng chế này. Bộ xử lý có thể là dạng kết hợp của các bộ xử lý mà thực hiện chức năng tính toán, ví dụ, dạng kết hợp của một hoặc nhiều bộ vi xử lý, hoặc dạng kết hợp của DSP và bộ vi xử lý. Bộ phận truyền thông 1603 có thể là bộ thu phát, mạch thu phát, giao diện truyền thông, hoặc tương tự. Bộ phận lưu trữ 1601 có thể là bộ nhớ.

Khi bộ phận xử lý 1602 là bộ xử lý, bộ phận truyền thông 1603 là bộ thu phát, và bộ phận lưu trữ 1601 là bộ nhớ, thiết bị 1600 theo phương án này của sáng chế có thể là đầu cuối được thể hiện trên Fig.17.

Fig.17 là sơ đồ giản lược được đơn giản hóa của cấu trúc thiết kế khả thi của đầu cuối trong phương án của sáng chế. Đầu cuối 1700 bao gồm bộ truyền 1701, bộ thu 1702, và bộ xử lý 1703. Bộ xử lý 1703 có thể tùy chọn là bộ điều khiển, và được thể hiện là "bộ điều khiển/bộ xử lý 1703" trên Fig.17. Một cách tùy ý, đầu cuối 1700 có thể còn bao gồm bộ xử lý môđem 1705, và bộ xử lý môđem 1705 có thể bao gồm bộ mã hóa 1706, bộ điều biến 1707, bộ giải mã 1708, và bộ giải điều biến 1709.

Theo một ví dụ, bộ truyền 1701 điều chỉnh (ví dụ, qua chuyển đổi tương tự, lọc, khuếch đại, và chuyển đổi lên) mẫu đầu ra và tạo ra tín hiệu đường lên. Tín hiệu đường lên được truyền bởi anten tới trạm gốc trong các phương án nêu trên. Trong đường xuống, anten thu tín hiệu đường xuống được truyền bởi trạm gốc trong các phương án nêu trên. Bộ thu 1702 điều chỉnh (chẳng hạn như qua lọc, khuếch đại, chuyển đổi xuống, và số hóa) tín hiệu được thu từ anten và tạo ra mẫu đầu vào. Trong bộ xử lý môđem 1705, bộ mã hóa 1706 thu dữ liệu dịch vụ và tin nhắn báo hiệu cần được gửi trong đường lên, và xử lý (chẳng hạn như qua định dạng, mã hóa, và đan xen) dữ liệu dịch vụ và tin nhắn báo hiệu. Bộ điều biến 1707 còn xử lý (chẳng hạn như qua ánh xạ và điều biến ký hiệu) dữ liệu dịch vụ được mã hóa và tin nhắn báo hiệu, và tạo ra mẫu đầu ra. Bộ giải điều biến 1709 xử lý (chẳng hạn như qua giải điều biến) mẫu đầu vào và cung cấp sự ước tính ký hiệu. Bộ giải mã 1708 xử lý (chẳng hạn như qua bỏ đan xen và giải mã) ước tính ký hiệu và tạo ra dữ liệu được giải mã và tin nhắn báo hiệu mà được gửi tới đầu cuối 1700. Bộ mã hóa 1706, bộ điều biến 1707, bộ giải điều biến 1709, và bộ giải mã 1708 có thể được thực hiện bởi bộ xử lý môđem được kết hợp 1705. Các bộ phận này thực hiện xử lý dựa vào công nghệ truy cập rađio (ví dụ, công nghệ truy cập của LTE hoặc

hệ thống cải tiến khác) được sử dụng bởi mạng truy cập rađio. Cần chú ý rằng khi đầu cuối 1700 không bao gồm bộ xử lý môđem 1705, các chức năng nêu trên của bộ xử lý môđem 1705 có thể tùy chọn được hoàn thành bởi bộ xử lý 1703.

Bộ xử lý 1703 điều khiển và quản lý các thao tác của đầu cuối 1700 và được tạo cấu hình để thực hiện xử lý các thủ tục được thực hiện bởi đầu cuối 1700 trong các phương án của sáng chế. Ví dụ, bộ xử lý 1703 còn được tạo cấu hình để thực hiện xử lý xử lý của đầu cuối theo các phương pháp được thể hiện trên các hình vẽ từ Fig.4 đến Fig.13 và/hoặc quy trình khác của các giải pháp kỹ thuật được mô tả trong sáng chế này.

Ngoài ra, đầu cuối 1700 có thể còn bao gồm bộ nhớ 1704, trong đó bộ nhớ 1704 được tạo cấu hình để lưu trữ mã chương trình và dữ liệu của đầu cuối 1700.

Phương pháp hoặc các bước thuật toán được mô tả theo dạng kết hợp với nội dung được bộc lộ trong sáng chế này có thể được thực hiện bởi phần cứng, hoặc có thể được thực hiện bởi bộ xử lý bằng cách thực hiện lệnh phần mềm. Lệnh phần mềm có thể bao gồm môđun phần mềm tương ứng. Môđun phần mềm có thể được lưu trữ trong bộ nhớ truy cập ngẫu nhiên (Random Access Memory, viết tắt là RAM), bộ nhớ chớp, bộ nhớ chỉ đọc (Read Only Memory, viết tắt là ROM), bộ nhớ chỉ đọc khả trình xóa được (Erasable Programmable ROM, viết tắt là EPROM), bộ nhớ chỉ đọc khả trình xóa được bằng điện (Electrically EPROM, viết tắt là EEPROM), thanh ghi, ổ đĩa cứng, ổ đĩa cứng di động, bộ nhớ chỉ đọc dạng đĩa nén (CD-ROM), hoặc dạng khác bất kỳ của phương tiện lưu trữ đã biết trong giải pháp kỹ thuật. Ví dụ, phương tiện lưu trữ được ghép nối với bộ xử lý, sao cho bộ xử lý có thể đọc thông tin từ phương tiện lưu trữ hoặc ghi thông tin vào trong phương tiện lưu trữ. Tất nhiên, phương tiện lưu trữ có thể là thành phần của bộ xử lý. Bộ xử lý và phương tiện lưu trữ có thể nằm trong ASIC. Ngoài ra, ASIC có thể nằm trong thiết bị mạng lõi hoặc đầu cuối. Tất nhiên, bộ xử lý và phương tiện lưu trữ có thể tồn tại trong thiết bị mạng lõi hoặc đầu cuối như các thành phần riêng rẽ.

Trong một vài phương án được đề xuất trong sáng chế này, cần được hiểu rằng hệ thống, thiết bị, và phương pháp được bộc lộ có thể được thực hiện theo các cách khác. Ví dụ, các phương án của thiết bị được mô tả chỉ là các ví dụ. Ví dụ, việc phân chia bộ phận chỉ là việc phân chia chức năng lôgic và có thể là sự phân chia khác trong sự thực

hiện thực tế. Ví dụ, nhiều bộ phận hoặc thành phần có thể được kết hợp hoặc được tích hợp vào trong hệ thống khác, hoặc một số dấu đặc tính có thể được bỏ qua hoặc không được thực hiện. Ngoài ra, các sự ghép nối chung được hiển thị hoặc được bàn luận hoặc các sự ghép nối trực tiếp hoặc các kết nối truyền thông có thể được thực hiện qua một số giao diện. Các sự ghép nối gián tiếp hoặc các kết nối truyền thông giữa thiết bị hoặc các bộ phận có thể được thực hiện theo dạng ghép nối về điện hoặc dạng khác.

Các bộ phận được mô tả là các phần riêng rẽ có thể hoặc có thể không được tách rời về mặt vật lý, và các phần được hiển thị là các bộ phận có thể hoặc có thể không phải là các bộ phận vật lý, có thể nằm tại một vị trí, hoặc có thể được phân bố trên nhiều thiết bị mạng. Một số hoặc tất cả của các bộ phận có thể được lựa chọn dựa vào các yêu cầu thực tế để đạt được các mục đích của các giải pháp của các phương án.

Ngoài ra, các bộ phận chức năng trong các phương án của sáng chế có thể được tích hợp thành một bộ phận xử lý, hoặc mỗi bộ phận chức năng có thể tồn tại độc lập, hoặc hai hoặc nhiều bộ phận được tích hợp thành một bộ phận. Bộ phận được tích hợp có thể được thực hiện theo dạng phần cứng, hoặc có thể được thực hiện theo dạng phần cứng ngoài bộ phận chức năng phần mềm.

Dựa vào các phần mô tả trên đây của các sự thực hiện, người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể hiểu rõ rằng sáng chế này có thể được thực hiện bởi phần mềm ngoài phần cứng cần thiết thông thường hoặc chỉ bởi phần cứng. Hầu hết các trường hợp là thực hiện bởi phần mềm. Dựa vào cách hiểu này, các giải pháp kỹ thuật của sáng chế là cần thiết hoặc đóng góp một phần vào giải pháp kỹ thuật đã biết có thể được thực hiện theo dạng sản phẩm phần mềm. Sản phẩm phần mềm được lưu trữ trong phương tiện lưu trữ đọc được, chẳng hạn như đĩa mềm, ổ đĩa cứng hoặc đĩa quang của máy tính, và bao gồm một vài lệnh dùng để ra lệnh cho thiết bị máy tính (mà có thể là máy tính cá nhân, máy chủ, thiết bị mạng, hoặc tương tự) thực hiện các phương pháp được mô tả trong các phương án của sáng chế.

Các phần mô tả trên đây chỉ là các sự thực hiện cụ thể của sáng chế, nhưng không có mục đích giới hạn phạm vi bảo hộ của sáng chế. Sự thay đổi hoặc thay thế bất kỳ trong phạm vi kỹ thuật được bộc lộ trong sáng chế này sẽ nằm trong phạm vi bảo hộ của sáng chế. Do đó, phạm vi bảo hộ của sáng chế sẽ là phạm vi bảo hộ của bộ yêu cầu bảo

hộ.

YÊU CẦU BẢO HỘ

1. Phương pháp cập nhật khóa, được áp dụng cho hệ thống truyền thông, trong đó hệ thống truyền thông này bao gồm thiết bị mạng lõi, có kết nối thứ nhất tương ứng với công nghệ truy cập dự án đối tác thế hệ thứ ba (3rd reneration partnership project, 3GPP) và kết nối thứ hai tương ứng với công nghệ truy cập không phải 3GPP giữa thiết bị mạng lõi và đầu cuối, kết nối thứ nhất và kết nối thứ hai chia sẻ khóa thứ nhất, và khóa thứ nhất có ký hiệu nhận dạng khóa thứ nhất mà nhận dạng khóa thứ nhất, và phương pháp này bao gồm các bước:

cập nhật, bởi thiết bị mạng lõi, khóa thứ nhất để thu nhận khóa được cập nhật dùng cho kết nối thứ nhất và thu nhận ký hiệu nhận dạng khóa thứ hai, trong đó ký hiệu nhận dạng khóa thứ hai nhận dạng khóa được cập nhật;

đáp lại việc xác định rằng kết nối thứ hai ở trạng thái được kết nối, giữ lại, bởi thiết bị mạng lõi, khóa thứ nhất dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa thứ nhất; và

tiếp tục, bởi thiết bị mạng lõi trước khi cập nhật khóa thứ nhất dùng cho kết nối thứ hai, sử dụng khóa thứ nhất dùng cho kết nối thứ hai khi thiết bị mạng lõi truyền thông với đầu cuối qua kết nối thứ hai.

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

gửi, bởi thiết bị mạng lõi, tin nhắn lệnh chế độ bảo mật (security mode command, SMC) tầng không truy cập (non-access stratum, NAS) (NAS SMC) thứ nhất đến đầu cuối qua kết nối thứ nhất; và trong đó tin nhắn NAS SMC thứ nhất bao gồm ký hiệu nhận dạng khóa thứ hai; và

thu, bởi thiết bị mạng lõi, tin nhắn hoàn thành chế độ bảo mật (security mode completion, SMP) NAS (NAS SMP) thứ nhất từ đầu cuối qua kết nối thứ nhất, trong đó việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMP thứ nhất dựa trên khóa được cập nhật.

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

cập nhật, bởi thiết bị mạng lõi, khóa thứ nhất dùng cho kết nối thứ hai bằng cách sử dụng khóa được cập nhật; và

sau khi cập nhật khóa thứ nhất dùng cho kết nối thứ hai, sử dụng, bởi thiết bị mạng lõi, khóa được cập nhật dùng cho kết nối thứ hai khi thiết bị mạng lõi truyền thông với đầu cuối qua kết nối thứ hai.

4. Phương pháp theo điểm 3, trong đó phương pháp này còn bao gồm bước:

gửi, bởi thiết bị mạng lõi, tin nhắn NAS SMC thứ hai đến đầu cuối qua kết nối thứ hai, trong đó tin nhắn NAS SMC thứ hai bao gồm ký hiệu nhận dạng khóa thứ hai; và

thu, bởi thiết bị mạng lõi, tin nhắn NAS SMP thứ hai từ đầu cuối qua kết nối thứ hai, trong đó việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMP thứ hai dựa trên khóa được cập nhật.

5. Phương pháp theo điểm 3, trong đó phương pháp này còn bao gồm bước:

sau bước cập nhật khóa thứ nhất dùng cho kết nối thứ hai, xóa, bởi thiết bị mạng lõi, khóa thứ nhất và ký hiệu nhận dạng khóa thứ nhất.

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

trước khi cập nhật khóa thứ nhất để thu nhận khóa được cập nhật dùng cho kết nối thứ nhất, xác định, bởi thiết bị mạng lõi theo thông tin cấu hình của nhà điều hành hoặc số đếm NAS (NAS COUNT) được sử dụng bởi đầu cuối mà sắp vòng lại (wrap around), rằng đầu cuối cần được tái xác thực.

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

xác định, bởi thiết bị mạng lõi, trạng thái của kết nối thứ hai.

8. Phương pháp cập nhật khóa, được áp dụng cho hệ thống truyền thông, trong đó hệ thống truyền thông bao gồm đầu cuối, có kết nối thứ nhất tương ứng với công nghệ truy cập dự án đối tác thế hệ thứ ba (3rd generation partnership project, 3GPP) và kết nối thứ hai tương ứng với công nghệ truy cập không phải 3GPP giữa đầu cuối và thiết bị mạng lõi, kết nối thứ nhất và kết nối thứ hai chia sẻ khóa thứ nhất, và khóa thứ nhất có ký hiệu nhận dạng khóa thứ nhất mà nhận dạng khóa thứ nhất, và phương pháp này bao gồm các bước:

thu, bởi đầu cuối, tin nhắn lệnh chế độ bảo mật (SMC) tầng không truy cập (NAS) (NAS SMC) thứ nhất từ thiết bị mạng lõi qua kết nối thứ nhất, trong đó tin nhắn NAS SMC thứ nhất bao gồm ký hiệu nhận dạng khóa thứ hai;

cập nhật, bởi đầu cuối, khóa thứ nhất để thu nhận khóa được cập nhật dùng cho kết nối thứ nhất, trong đó khóa được cập nhật được nhận dạng bởi ký hiệu nhận dạng khóa thứ hai;

gửi, bởi đầu cuối, tin nhắn hoàn thành chế độ bảo mật (SMP) NAS (NAS SMP) thứ nhất đến thiết bị mạng lõi qua kết nối thứ nhất, trong đó việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMP thứ nhất dựa trên khóa được cập nhật;

thu, bởi đầu cuối, tin nhắn NAS SMC thứ hai từ thiết bị mạng lõi qua kết nối thứ hai, trong đó tin nhắn NAS SMC thứ hai bao gồm ký hiệu nhận dạng khóa thứ hai;

cập nhật, bởi đầu cuối, khóa thứ nhất dùng cho kết nối thứ hai bằng cách sử dụng khóa được cập nhật; và

gửi, bởi đầu cuối, tin nhắn NAS SMP thứ hai đến thiết bị mạng lõi qua kết nối thứ hai, trong đó việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMP thứ hai dựa trên khóa được cập nhật.

9. Phương pháp theo điểm 8, trong đó phương pháp này còn bao gồm bước:

sau khi cập nhật khóa thứ nhất dùng cho kết nối thứ hai bằng cách sử dụng khóa được cập nhật, xóa, bởi đầu cuối, khóa thứ nhất và ký hiệu nhận dạng khóa thứ nhất.

10. Phương pháp theo điểm 8, trong đó, trước khi cập nhật khóa thứ nhất dùng cho kết nối thứ hai, tiếp tục sử dụng khóa thứ nhất dùng cho kết nối thứ hai khi đầu cuối truyền thông với thiết bị mạng lõi qua kết nối thứ hai.

11. Thiết bị truyền thông, được áp dụng cho hệ thống truyền thông, trong đó hệ thống truyền thông bao gồm thiết bị này, có kết nối thứ nhất tương ứng với công nghệ truy cập 3GPP và kết nối thứ hai tương ứng với công nghệ truy cập không phải 3GPP giữa thiết bị này và đầu cuối, kết nối thứ nhất và kết nối thứ hai chia sẻ khóa thứ nhất, và khóa thứ nhất có ký hiệu nhận dạng khóa thứ nhất mà nhận dạng khóa thứ nhất, và thiết bị này bao gồm:

ít nhất một bộ xử lý; và

bộ nhớ được ghép nối với ít nhất một bộ xử lý và có các lệnh chương trình được lưu trữ trên đó mà, khi được thực hiện bởi ít nhất một bộ xử lý, khiến cho thiết bị:

cập nhật khóa thứ nhất để thu nhận khóa được cập nhật dùng cho kết nối thứ nhất và thu nhận ký hiệu nhận dạng khóa thứ hai, trong đó ký hiệu nhận dạng khóa

thứ hai nhận dạng khóa được cập nhật;

đáp lại việc xác định rằng kết nối thứ hai ở trạng thái được kết nối, giữ lại khóa thứ nhất dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa thứ nhất; và

trước khi cập nhật khóa thứ nhất dùng cho kết nối thứ hai, tiếp tục sử dụng khóa thứ nhất dùng cho kết nối thứ hai khi thiết bị truyền thông với đầu cuối qua kết nối thứ hai.

12. Thiết bị theo điểm 11, trong đó các lệnh chương trình được lưu trữ trên đó mà, khi được thực hiện bởi ít nhất một bộ xử lý, khiến cho thiết bị:

gửi tin nhắn lệnh chế độ bảo mật (SMC) tầng không truy cập (NAS) (NAS SMC) thứ nhất đến đầu cuối qua kết nối thứ nhất; và trong đó tin nhắn NAS SMC thứ nhất bao gồm ký hiệu nhận dạng khóa thứ hai; và

thu tin nhắn hoàn thành chế độ bảo mật (SMP) NAS (NAS SMP) thứ nhất từ đầu cuối qua kết nối thứ nhất, trong đó việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMP thứ nhất dựa trên khóa được cập nhật.

13. Thiết bị theo điểm 11, trong đó các lệnh chương trình được lưu trữ trên đó mà, khi được thực hiện bởi ít nhất một bộ xử lý, khiến cho thiết bị:

cập nhật khóa thứ nhất dùng cho kết nối thứ hai bằng cách sử dụng khóa được cập nhật; và

sau khi cập nhật khóa thứ nhất dùng cho kết nối thứ hai, sử dụng khóa được cập nhật dùng cho kết nối thứ hai khi thiết bị truyền thông với đầu cuối qua kết nối thứ hai.

14. Thiết bị theo điểm 13, trong đó các lệnh chương trình được lưu trữ trên đó mà, khi được thực hiện bởi ít nhất một bộ xử lý, khiến cho thiết bị:

gửi tin nhắn NAS SMC thứ hai đến đầu cuối qua kết nối thứ hai, trong đó tin nhắn NAS SMC thứ hai bao gồm ký hiệu nhận dạng khóa thứ hai; và

thu tin nhắn NAS SMP thứ hai từ đầu cuối qua kết nối thứ hai, trong đó việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMP thứ hai dựa trên khóa được cập nhật.

15. Thiết bị theo điểm 13, trong đó các lệnh chương trình được lưu trữ trên đó mà, khi được thực hiện bởi ít nhất một bộ xử lý, khiến cho thiết bị:

sau khi cập nhật khóa thứ nhất dùng cho kết nối thứ hai, xóa khóa thứ nhất và ký

hiệu nhận dạng khóa thứ nhất.

16. Thiết bị theo điểm 11, trong đó các lệnh chương trình được lưu trữ trên đó mà, khi được thực hiện bởi ít nhất một bộ xử lý, khiến cho thiết bị:

trước khi cập nhật khóa thứ nhất để thu nhận khóa được cập nhật dùng cho kết nối thứ nhất, xác định, theo thông tin cấu hình của nhà điều hành hoặc số đếm NAS (NAS COUNT) được sử dụng bởi đầu cuối mà sắp vòng lại, rằng đầu cuối cần được tái xác thực.

17. Thiết bị theo điểm 11, trong đó các lệnh chương trình được lưu trữ trên đó mà, khi được thực hiện bởi ít nhất một bộ xử lý, khiến cho thiết bị:

xác định trạng thái của kết nối thứ hai.

18. Thiết bị truyền thông, được áp dụng cho hệ thống truyền thông, trong đó hệ thống truyền thông bao gồm thiết bị này, có kết nối thứ nhất tương ứng với công nghệ truy cập dự án đối tác thế hệ thứ ba (3rd generation partnership project, 3GPP) và kết nối thứ hai tương ứng với công nghệ truy cập không phải 3GPP giữa thiết bị này và thiết bị mạng lõi, và kết nối thứ nhất và kết nối thứ hai chia sẻ khóa thứ nhất, và khóa thứ nhất có ký hiệu nhận dạng khóa thứ nhất mà nhận dạng khóa thứ nhất, và thiết bị này bao gồm:

ít nhất một bộ xử lý; và

bộ nhớ được ghép nối với ít nhất một bộ xử lý và có các lệnh chương trình được lưu trữ trên đó mà, khi được thực hiện bởi ít nhất một bộ xử lý, khiến cho thiết bị:

thu tin nhắn lệnh chế độ bảo mật (SMC) tầng không truy cập (NAS) (NAS SMC) thứ nhất từ thiết bị mạng lõi qua kết nối thứ nhất, trong đó tin nhắn NAS SMC thứ nhất bao gồm ký hiệu nhận dạng khóa thứ hai;

cập nhật khóa thứ nhất để thu nhận khóa được cập nhật dùng cho kết nối thứ nhất; trong đó khóa được cập nhật được nhận dạng bởi ký hiệu nhận dạng khóa thứ hai;

gửi tin nhắn hoàn thành chế độ bảo mật (SMP) NAS (NAS SMP) thứ nhất đến thiết bị mạng lõi qua kết nối thứ nhất, trong đó việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMP thứ nhất dựa trên khóa được cập nhật;

thu tin nhắn NAS SMC thứ hai từ thiết bị mạng lõi qua kết nối thứ hai, trong đó tin nhắn NAS SMC thứ hai bao gồm ký hiệu nhận dạng khóa thứ hai;

cập nhật khóa thứ nhất dùng cho kết nối thứ hai bằng cách sử dụng khóa được cập nhật; và

gửi tin nhắn NAS SMP thứ hai đến thiết bị mạng lõi qua kết nối thứ hai, trong đó việc bảo vệ tính toàn vẹn được thực hiện trên tin nhắn NAS SMP thứ hai dựa trên khóa được cập nhật.

19. Thiết bị theo điểm 18, trong đó các lệnh chương trình được lưu trữ trên đó mà, khi được thực hiện bởi ít nhất một bộ xử lý, khiến cho thiết bị:

sau khi cập nhật khóa thứ nhất dùng cho kết nối thứ hai bằng cách sử dụng khóa được cập nhật, xóa khóa thứ nhất và ký hiệu nhận dạng khóa thứ nhất.

20. Thiết bị theo điểm 18, trong đó các lệnh chương trình được lưu trữ trên đó mà, khi được thực hiện bởi ít nhất một bộ xử lý, khiến cho thiết bị, trước khi cập nhật khóa thứ nhất dùng cho kết nối thứ hai, tiếp tục sử dụng khóa thứ nhất dùng cho kết nối thứ hai khi thiết bị truyền thông với thiết bị mạng lõi qua kết nối thứ hai.

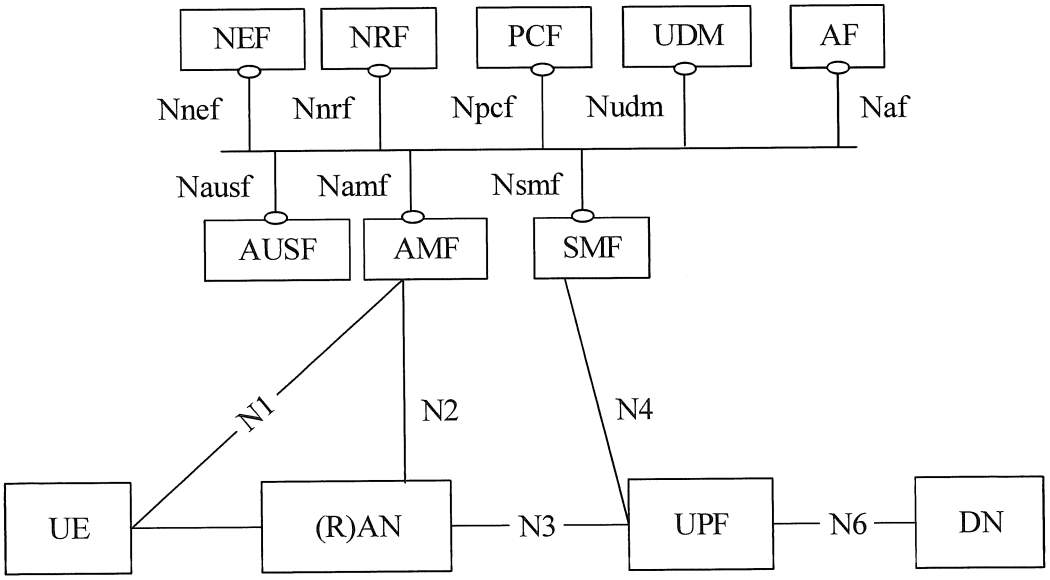
NEF
NRF
PCF
UDM
AF
Nnef
Nnrf
Npcf
Nudm
Naf
Nausf
Namf
Nsmf
AUSF
AMF
SMF
N1
N2
N4
UE
(R)AN
N3
UPF
N6
DN

FIG. 1

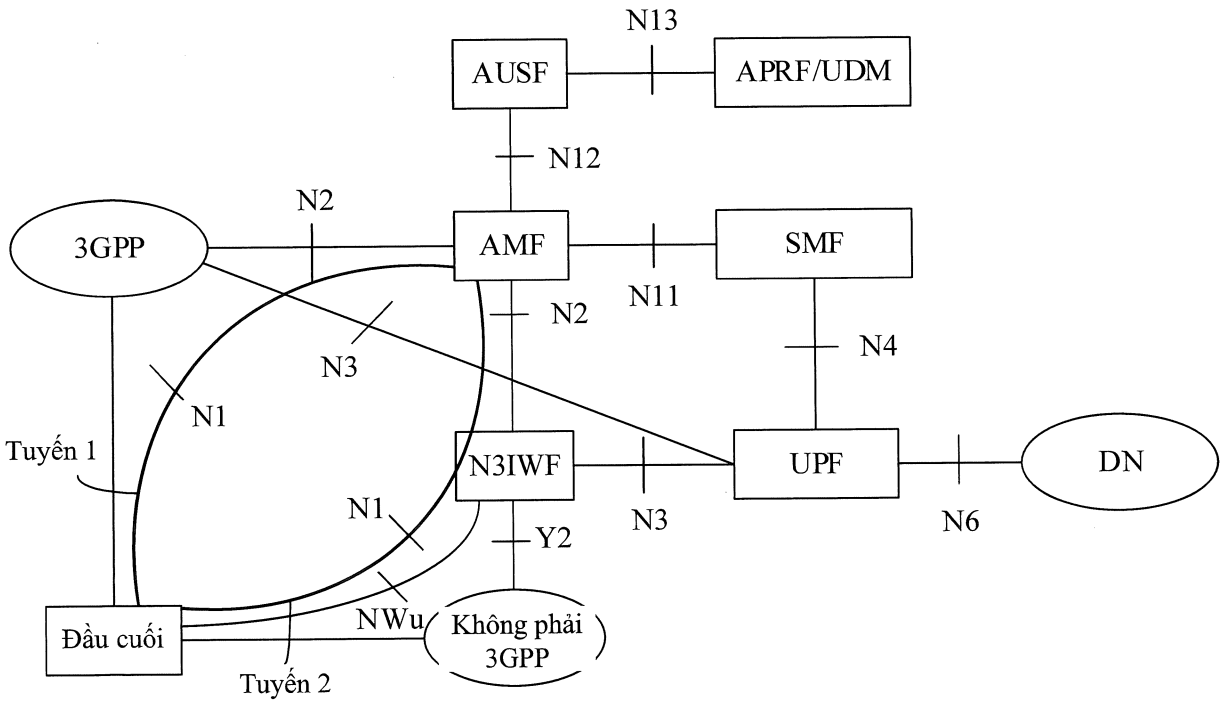
N13
AUSF
APRF/UDM
N12
N2
3GPP
AMF
SMF
N11
N2
N4
N3
N1
Tuyến 1
N3IWF
UPF
DN
N1
N3
N6
Y2
NWu
Đầu cuối
Không phải 3GPP
Tuyến 2

FIG. 2

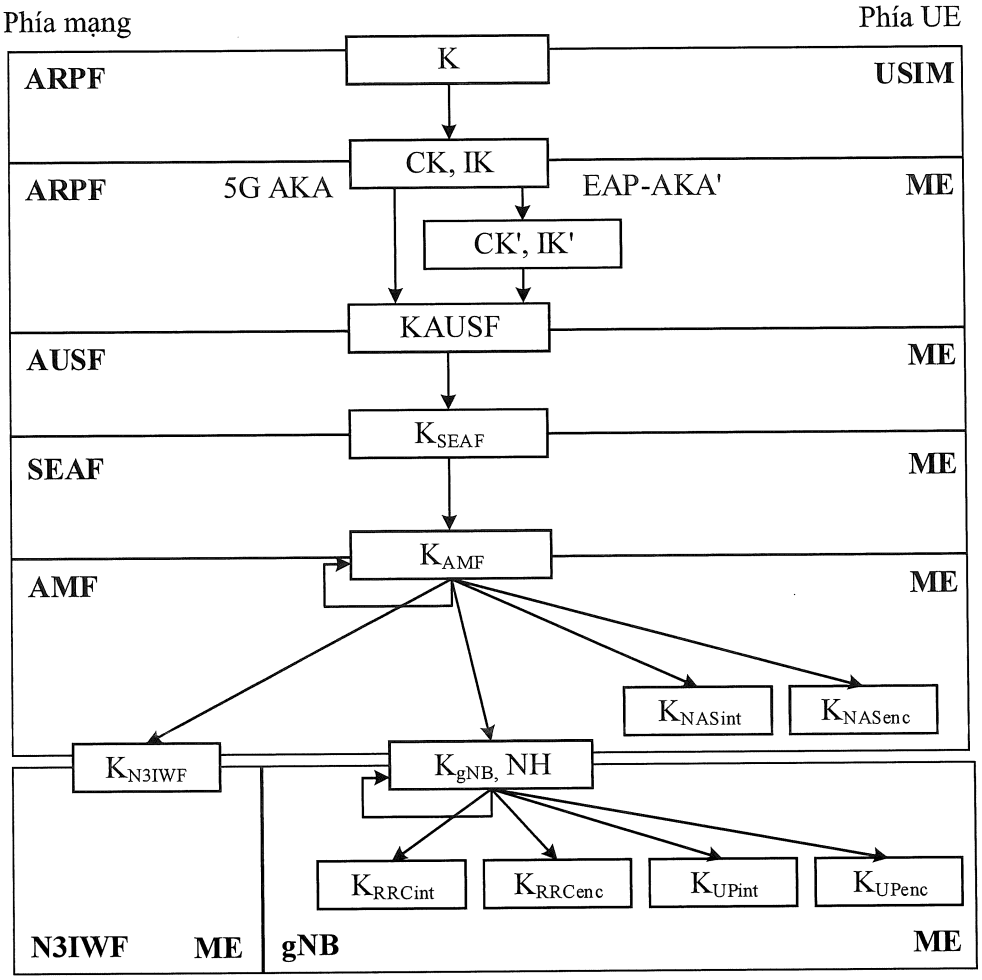
Phía mạng
Phía UE
ARPF
K
USIM
ARPF
5G AKA
CK, IK
EAP-AKA'
ME
CK', IK'
KAUSF
AUSF
ME
K_SEAF
SEAF
ME
K_AMF
AMF
ME
K_NASint
K_NASenc
K_N3IWF
K_gNB, NH
K_RRCint
K_RRCenc
K_UPint
K_UPenc
N3IWF
ME
gNB
ME

FIG. 3

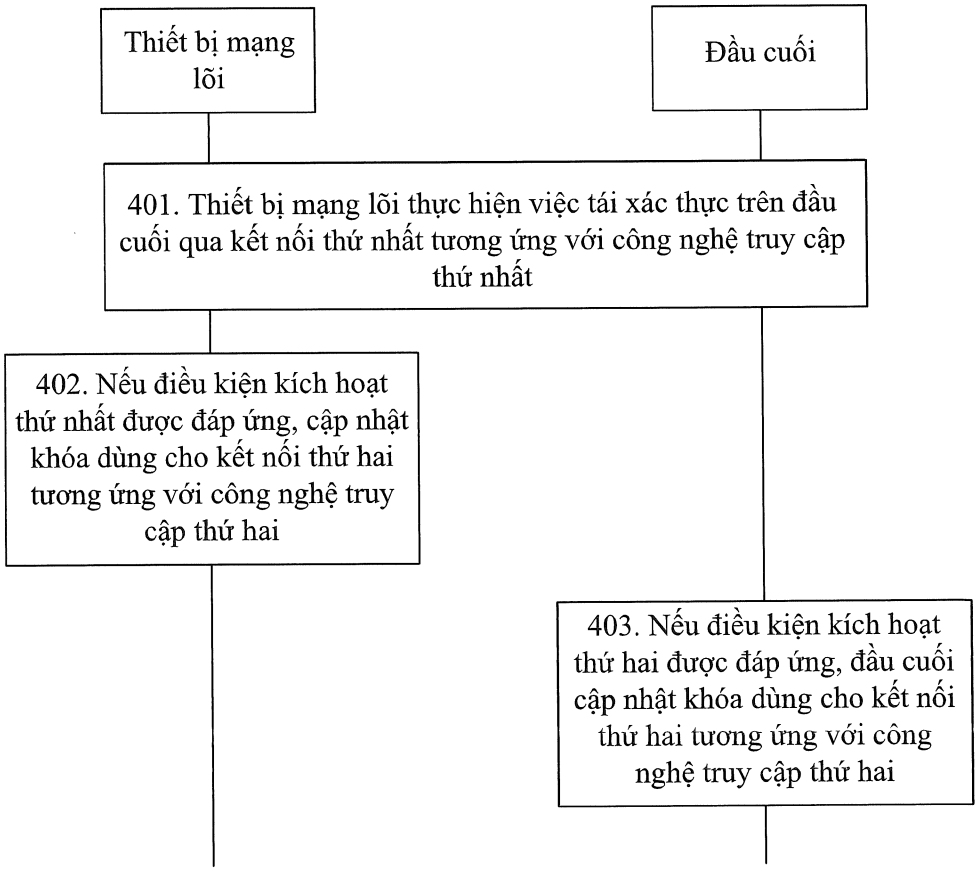
Thiết bị mạng lõi
Đầu cuối
401. Thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất
402. Nếu điều kiện kích hoạt thứ nhất được đáp ứng, cập nhật khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai
403. Nếu điều kiện kích hoạt thứ hai được đáp ứng, đầu cuối cập nhật khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai

FIG. 4

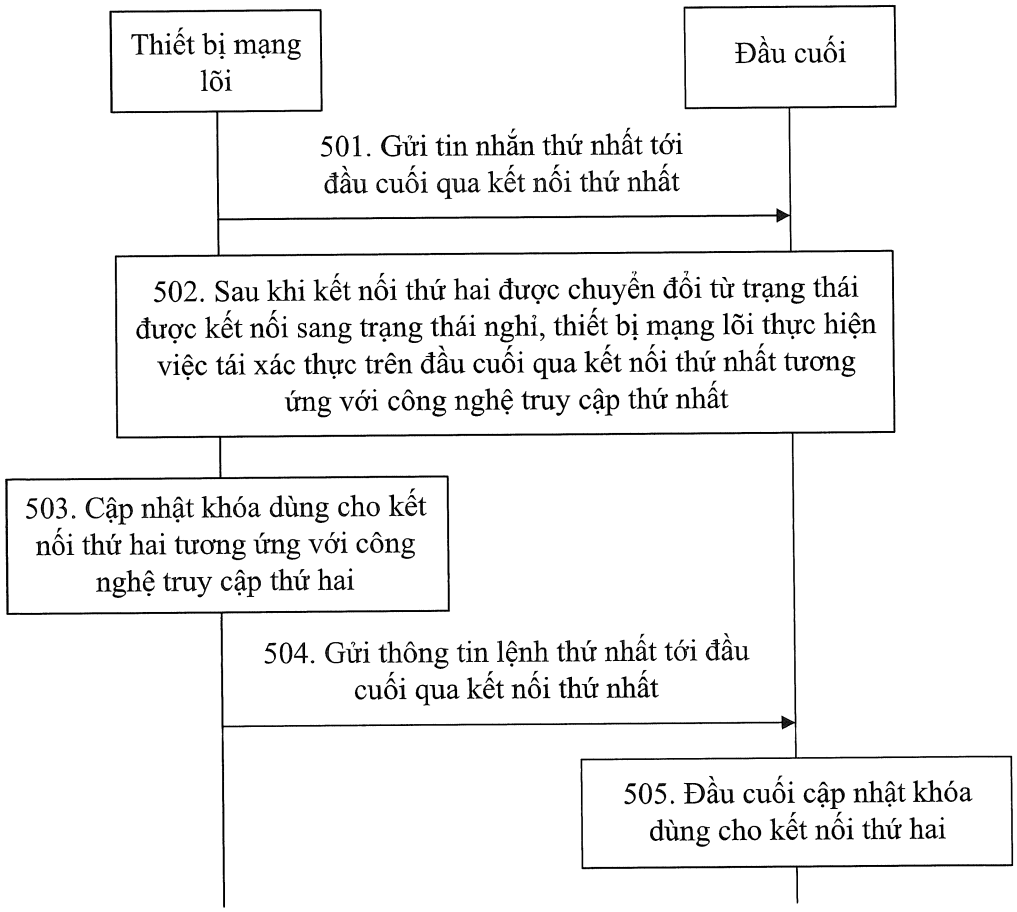
Thiết bị mạng lõi
Đầu cuối
501. Gửi tin nhắn thứ nhất tới đầu cuối qua kết nối thứ nhất
502. Sau khi kết nối thứ hai được chuyển đổi từ trạng thái được kết nối sang trạng thái nghỉ, thiết bị mạng lõi thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất
503. Cập nhật khóa dùng cho kết nối thứ hai tương ứng với công nghệ truy cập thứ hai
504. Gửi thông tin lệnh thứ nhất tới đầu cuối qua kết nối thứ nhất
505. Đầu cuối cập nhật khóa dùng cho kết nối thứ hai

FIG. 5

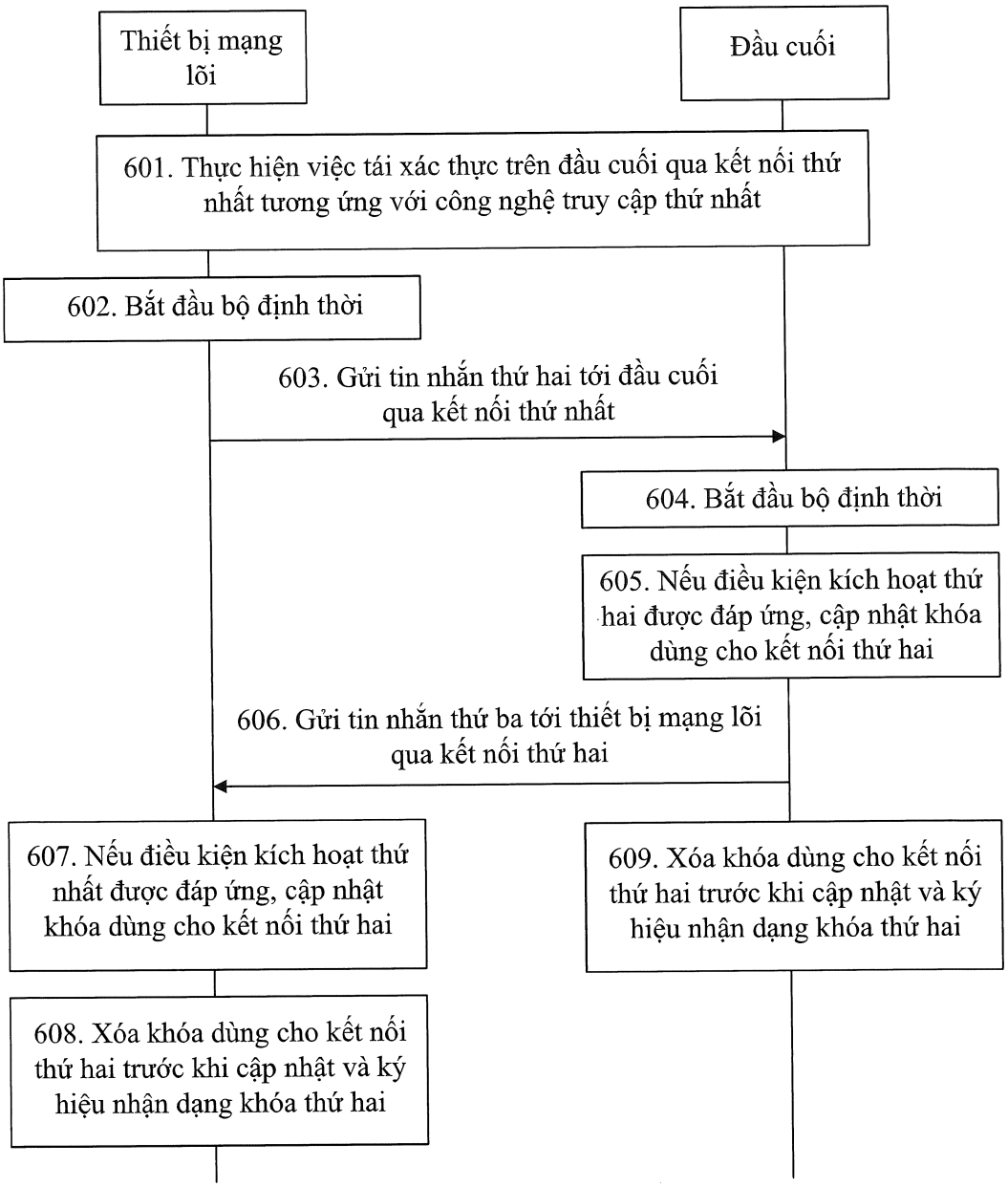
Thiết bị mạng lõi
Đầu cuối
601. Thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất
602. Bắt đầu bộ định thời
603. Gửi tin nhắn thứ hai tới đầu cuối qua kết nối thứ nhất
604. Bắt đầu bộ định thời
605. Nếu điều kiện kích hoạt thứ hai được đáp ứng, cập nhật khóa dùng cho kết nối thứ hai
606. Gửi tin nhắn thứ ba tới thiết bị mạng lõi qua kết nối thứ hai
607. Nếu điều kiện kích hoạt thứ nhất được đáp ứng, cập nhật khóa dùng cho kết nối thứ hai
609. Xóa khóa dùng cho kết nối thứ hai trước khi cập nhật và ký hiệu nhận dạng khóa thứ hai
608. Xóa khóa dùng cho kết nối thứ hai trước khi cập nhật và ký hiệu nhận dạng khóa thứ hai

FIG. 6

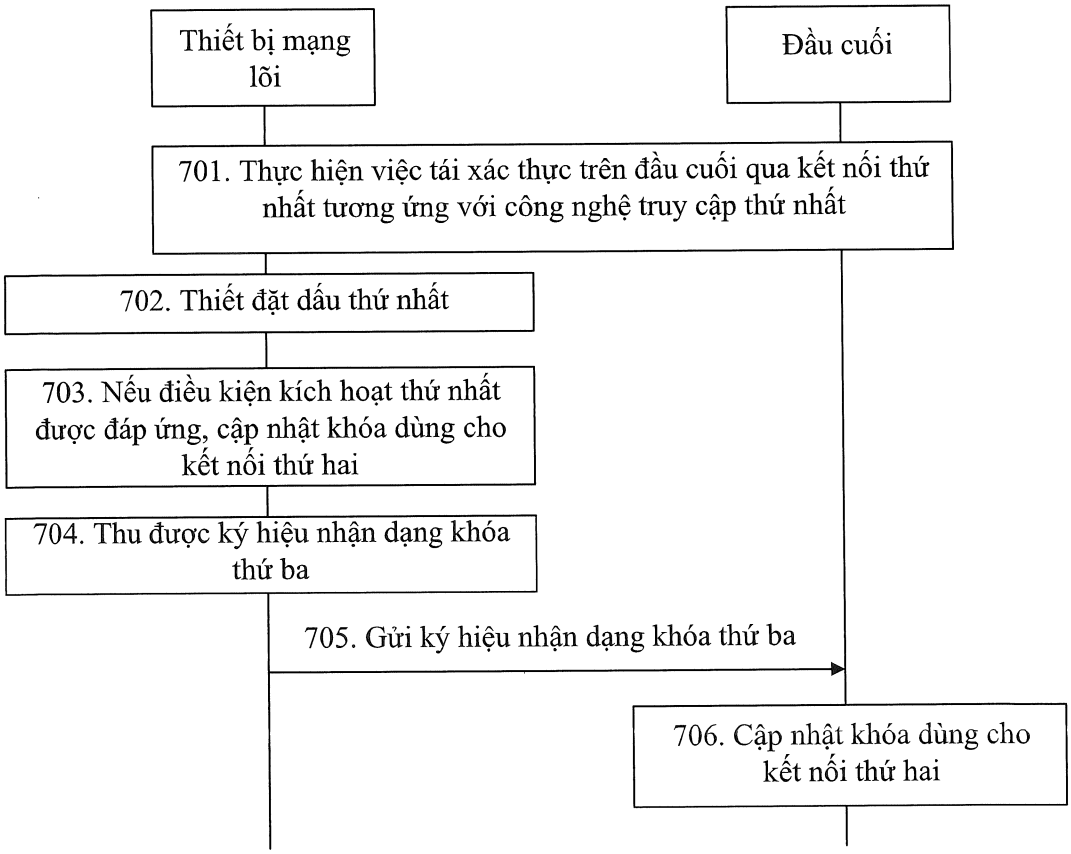
Thiết bị mạng lõi
Đầu cuối
701. Thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất
702. Thiết đặt dấu thứ nhất
703. Nếu điều kiện kích hoạt thứ nhất được đáp ứng, cập nhật khóa dùng cho kết nối thứ hai
704. Thu được ký hiệu nhận dạng khóa thứ ba
705. Gửi ký hiệu nhận dạng khóa thứ ba
706. Cập nhật khóa dùng cho kết nối thứ hai

FIG. 7

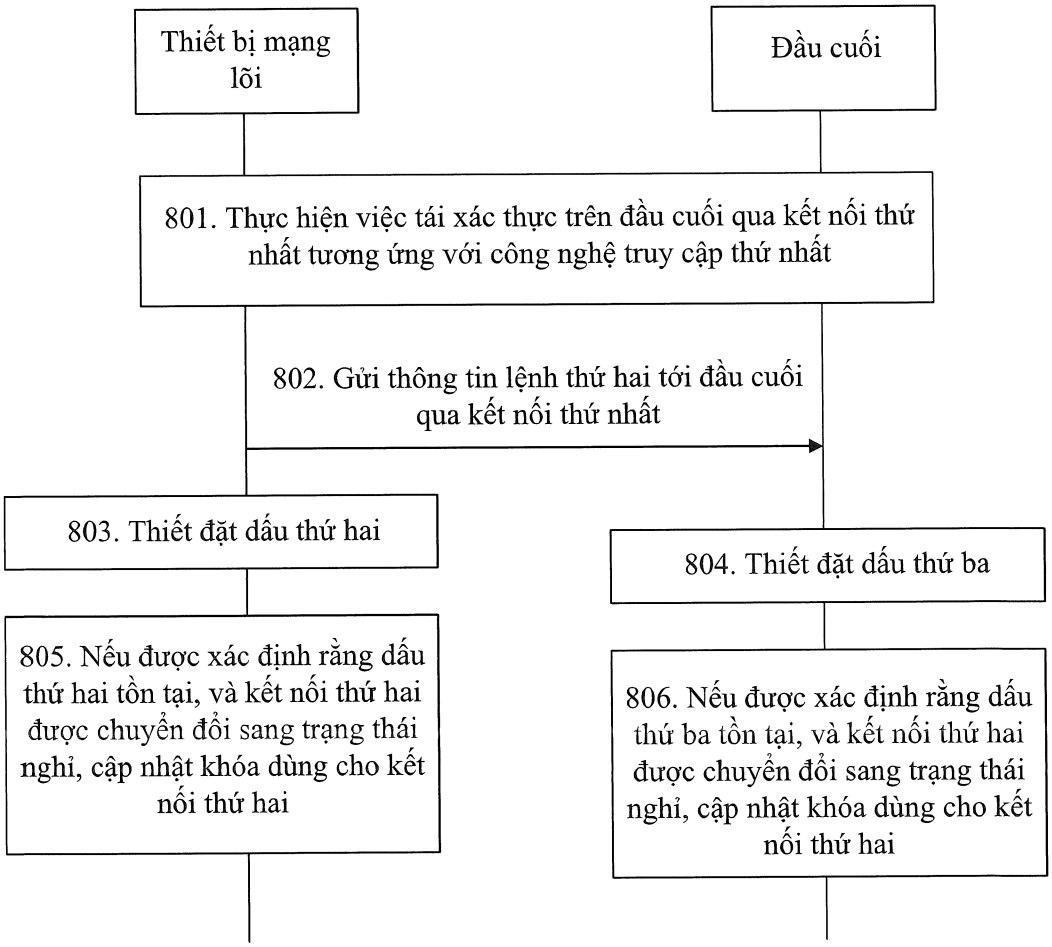
Thiết bị mạng lõi
Đầu cuối
801. Thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất tương ứng với công nghệ truy cập thứ nhất
802. Gửi thông tin lệnh thứ hai tới đầu cuối qua kết nối thứ nhất
803. Thiết đặt dấu thứ hai
804. Thiết đặt dấu thứ ba
805. Nếu được xác định rằng dấu thứ hai tồn tại, và kết nối thứ hai được chuyển đổi sang trạng thái nghỉ, cập nhật khóa dùng cho kết nối thứ hai
806. Nếu được xác định rằng dấu thứ ba tồn tại, và kết nối thứ hai được chuyển đổi sang trạng thái nghỉ, cập nhật khóa dùng cho kết nối thứ hai

FIG. 8

8/15

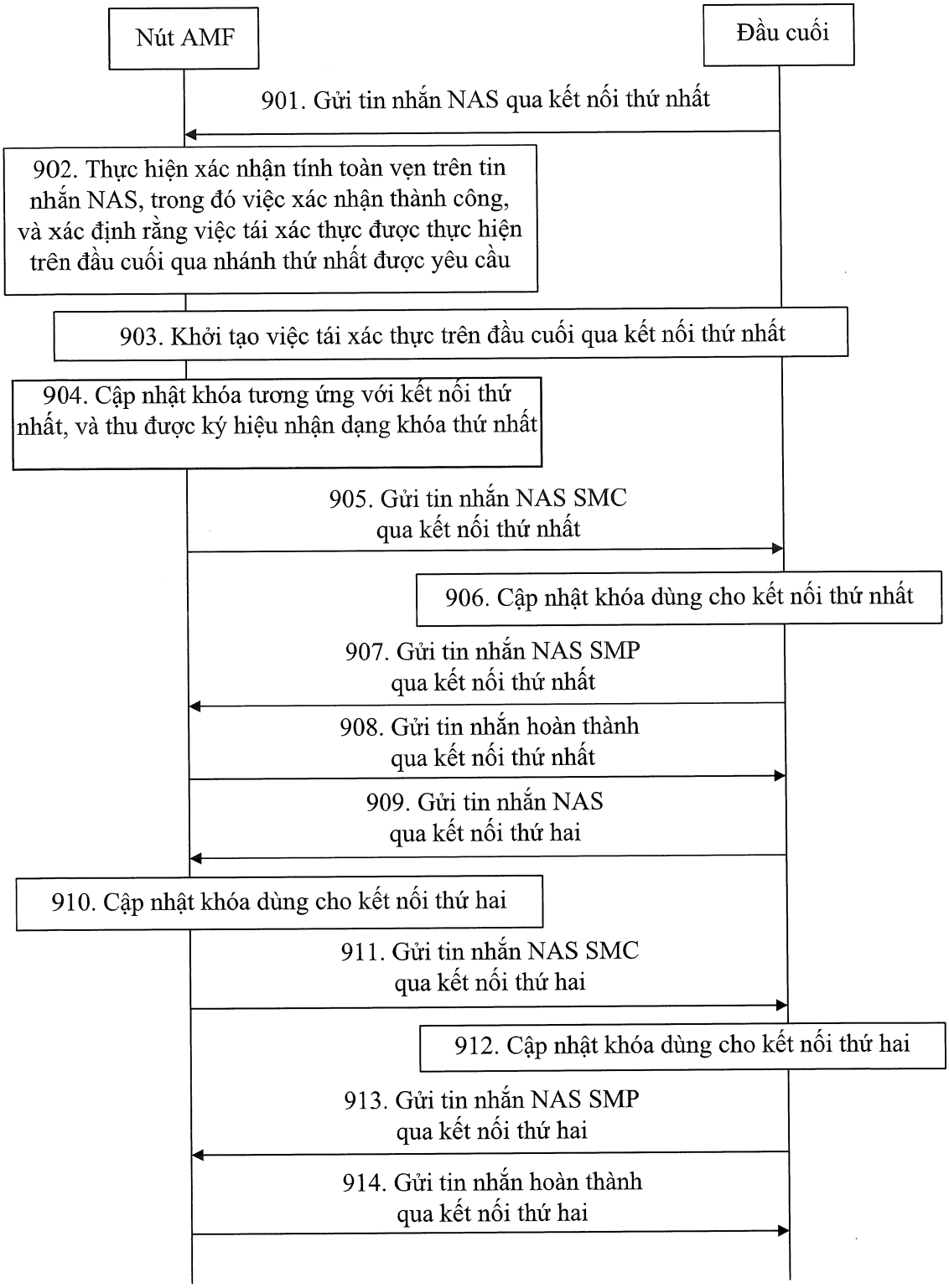
Nút AMF
Đầu cuối
901. Gửi tin nhắn NAS qua kết nối thứ nhất
902. Thực hiện xác nhận tính toàn vẹn trên tin nhắn NAS, trong đó việc xác nhận thành công, và xác định rằng việc tái xác thực được thực hiện trên đầu cuối qua nhánh thứ nhất được yêu cầu
903. Khởi tạo việc tái xác thực trên đầu cuối qua kết nối thứ nhất
904. Cập nhật khóa tương ứng với kết nối thứ nhất, và thu được ký hiệu nhận dạng khóa thứ nhất
905. Gửi tin nhắn NAS SMC qua kết nối thứ nhất
906. Cập nhật khóa dùng cho kết nối thứ nhất
907. Gửi tin nhắn NAS SMP qua kết nối thứ nhất
908. Gửi tin nhắn hoàn thành qua kết nối thứ nhất
909. Gửi tin nhắn NAS qua kết nối thứ hai
910. Cập nhật khóa dùng cho kết nối thứ hai
911. Gửi tin nhắn NAS SMC qua kết nối thứ hai
912. Cập nhật khóa dùng cho kết nối thứ hai
913. Gửi tin nhắn NAS SMP qua kết nối thứ hai
914. Gửi tin nhắn hoàn thành qua kết nối thứ hai

FIG. 9

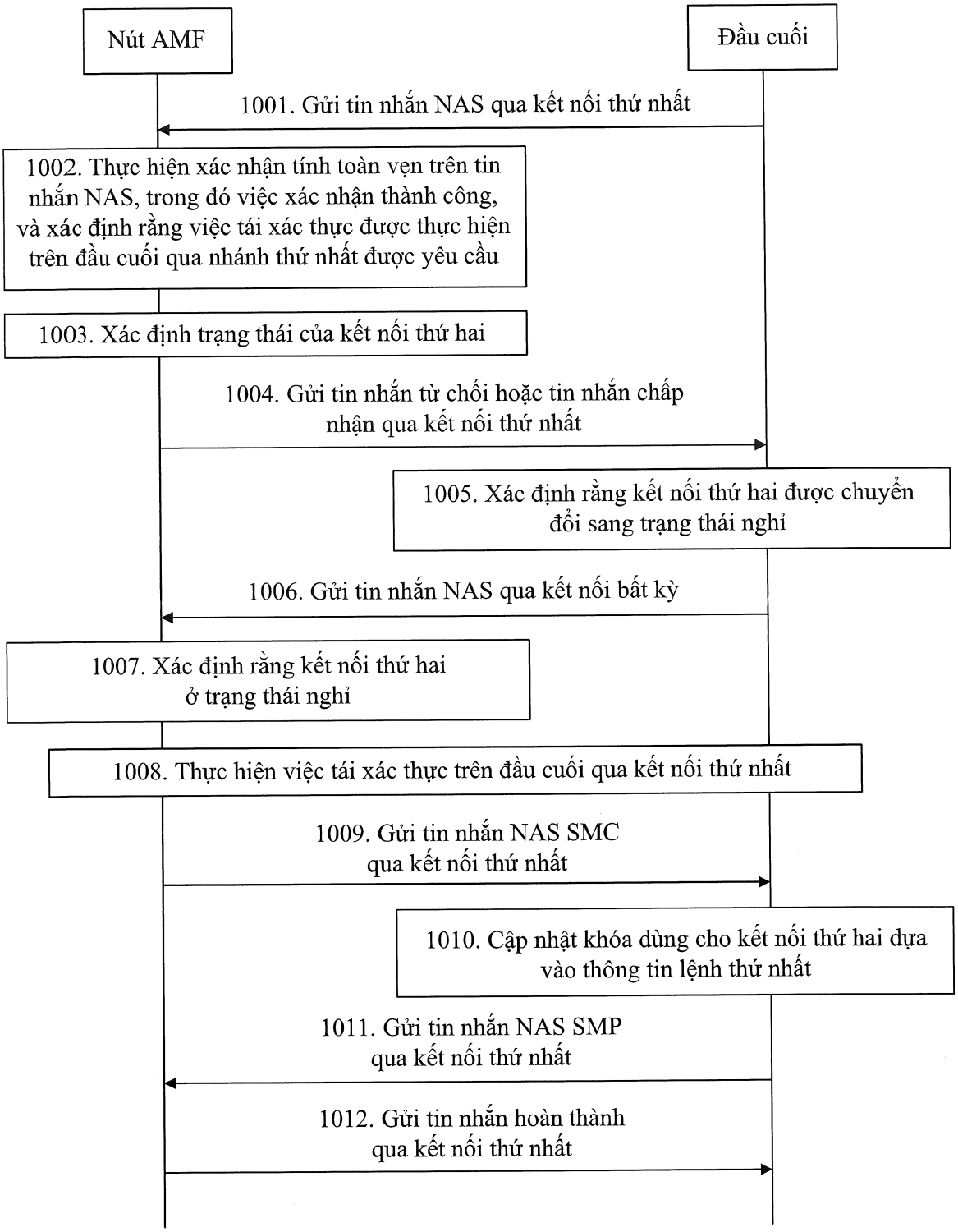
Nút AMF
Đầu cuối
1001. Gửi tin nhắn NAS qua kết nối thứ nhất
1002. Thực hiện xác nhận tính toàn vẹn trên tin nhắn NAS, trong đó việc xác nhận thành công, và xác định rằng việc tái xác thực được thực hiện trên đầu cuối qua nhánh thứ nhất được yêu cầu
1003. Xác định trạng thái của kết nối thứ hai
1004. Gửi tin nhắn từ chối hoặc tin nhắn chấp nhận qua kết nối thứ nhất
1005. Xác định rằng kết nối thứ hai được chuyển đổi sang trạng thái nghỉ
1006. Gửi tin nhắn NAS qua kết nối bất kỳ
1007. Xác định rằng kết nối thứ hai ở trạng thái nghỉ
1008. Thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất
1009. Gửi tin nhắn NAS SMC qua kết nối thứ nhất
1010. Cập nhật khóa dùng cho kết nối thứ hai dựa vào thông tin lệnh thứ nhất
1011. Gửi tin nhắn NAS SMP qua kết nối thứ nhất
1012. Gửi tin nhắn hoàn thành qua kết nối thứ nhất

FIG. 10

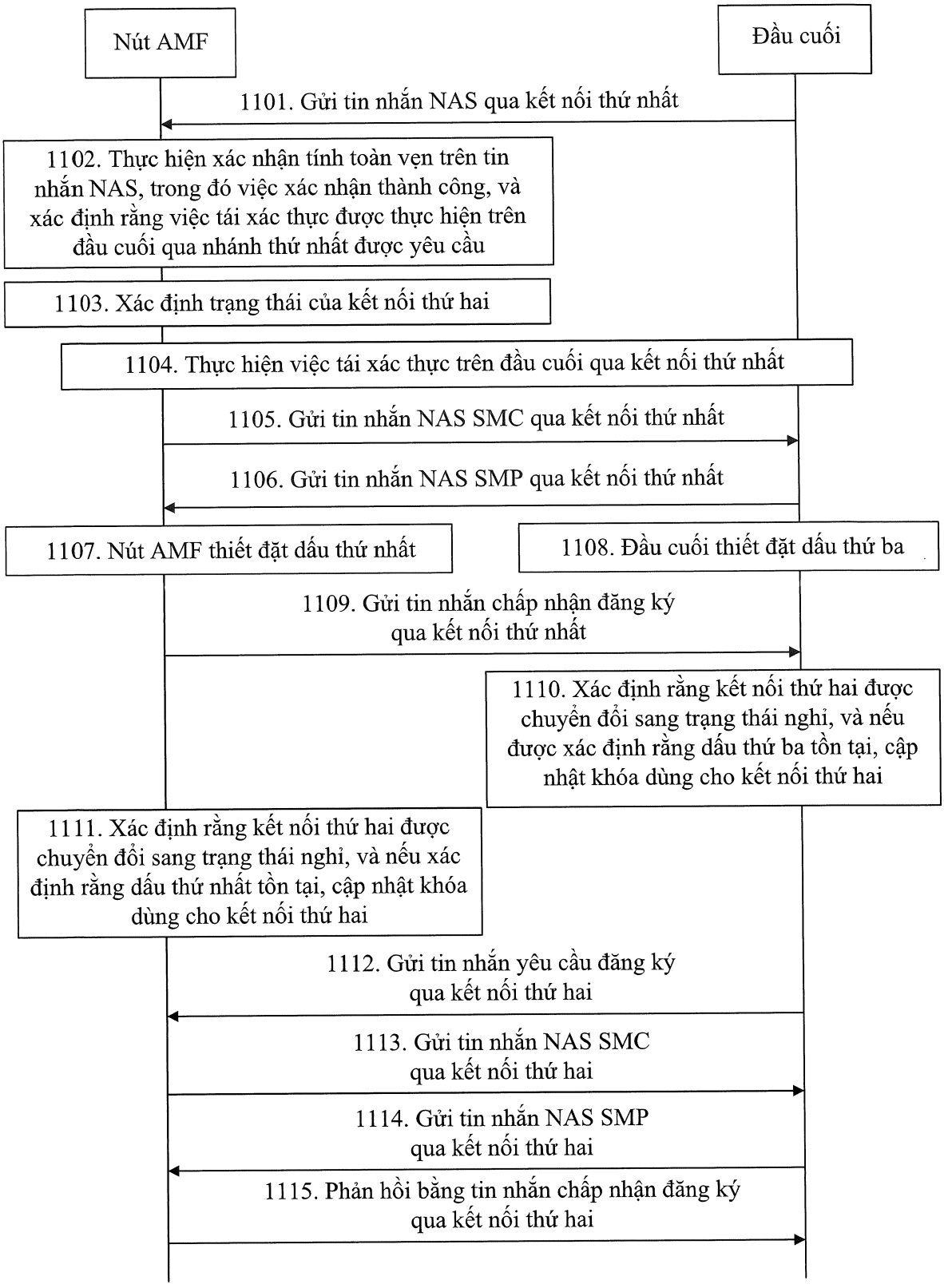
Nút AMF
Đầu cuối
1101. Gửi tin nhắn NAS qua kết nối thứ nhất
1102. Thực hiện xác nhận tính toàn vẹn trên tin nhắn NAS, trong đó việc xác nhận thành công, và xác định rằng việc tái xác thực được thực hiện trên đầu cuối qua nhánh thứ nhất được yêu cầu
1103. Xác định trạng thái của kết nối thứ hai
1104. Thực hiện việc tái xác thực trên đầu cuối qua kết nối thứ nhất
1105. Gửi tin nhắn NAS SMC qua kết nối thứ nhất
1106. Gửi tin nhắn NAS SMP qua kết nối thứ nhất
1107. Nút AMF thiết đặt dấu thứ nhất
1108. Đầu cuối thiết đặt dấu thứ ba
1109. Gửi tin nhắn chấp nhận đăng ký qua kết nối thứ nhất
1110. Xác định rằng kết nối thứ hai được chuyển đổi sang trạng thái nghỉ, và nếu được xác định rằng dấu thứ ba tồn tại, cập nhật khóa dùng cho kết nối thứ hai
1111. Xác định rằng kết nối thứ hai được chuyển đổi sang trạng thái nghỉ, và nếu xác định rằng dấu thứ nhất tồn tại, cập nhật khóa dùng cho kết nối thứ hai
1112. Gửi tin nhắn yêu cầu đăng ký qua kết nối thứ hai
1113. Gửi tin nhắn NAS SMC qua kết nối thứ hai
1114. Gửi tin nhắn NAS SMP qua kết nối thứ hai
1115. Phản hồi bằng tin nhắn chấp nhận đăng ký qua kết nối thứ hai

FIG. 11

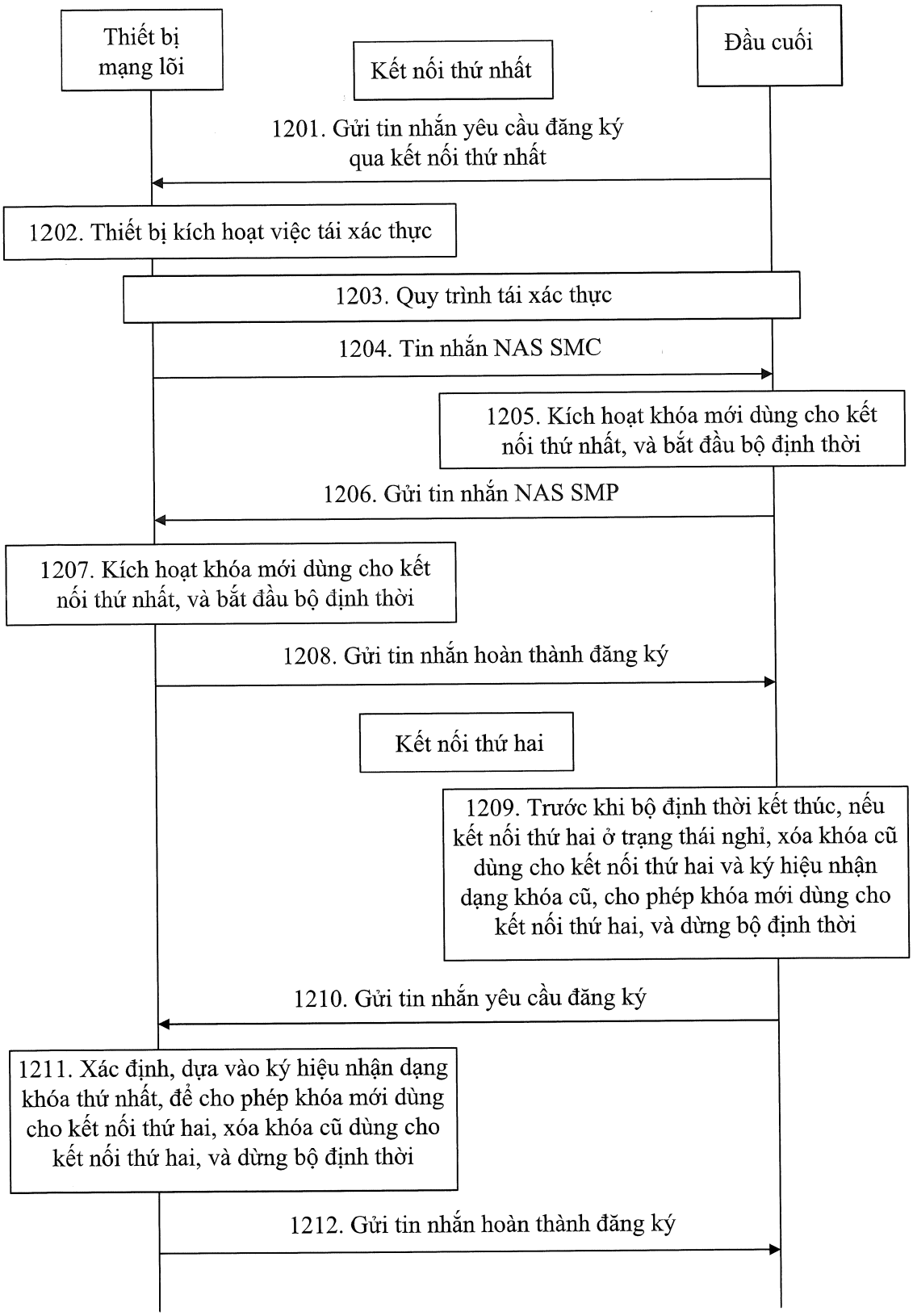
Thiết bị mạng lõi
Kết nối thứ nhất
Đầu cuối
1201. Gửi tin nhắn yêu cầu đăng ký qua kết nối thứ nhất
1202. Thiết bị kích hoạt việc tái xác thực
1203. Quy trình tái xác thực
1204. Tin nhắn NAS SMC
1205. Kích hoạt khóa mới dùng cho kết nối thứ nhất, và bắt đầu bộ định thời
1206. Gửi tin nhắn NAS SMP
1207. Kích hoạt khóa mới dùng cho kết nối thứ nhất, và bắt đầu bộ định thời
1208. Gửi tin nhắn hoàn thành đăng ký
Kết nối thứ hai
1209. Trước khi bộ định thời kết thúc, nếu kết nối thứ hai ở trạng thái nghỉ, xóa khóa cũ dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa cũ, cho phép khóa mới dùng cho kết nối thứ hai, và dừng bộ định thời
1210. Gửi tin nhắn yêu cầu đăng ký
1211. Xác định, dựa vào ký hiệu nhận dạng khóa thứ nhất, để cho phép khóa mới dùng cho kết nối thứ hai, xóa khóa cũ dùng cho kết nối thứ hai, và dừng bộ định thời
1212. Gửi tin nhắn hoàn thành đăng ký

FIG. 12

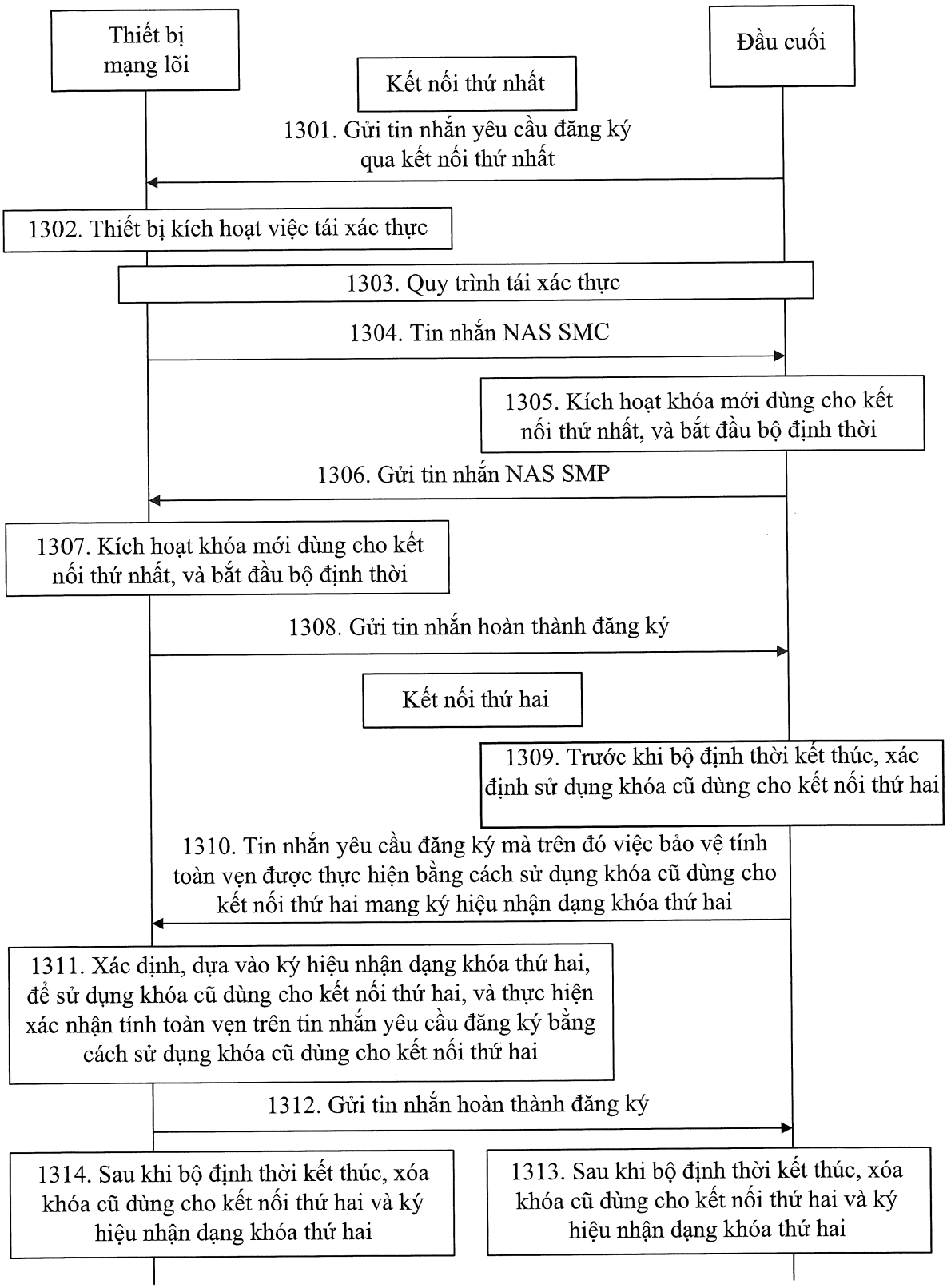
Thiết bị mạng lõi
Đầu cuối
Kết nối thứ nhất
1301. Gửi tin nhắn yêu cầu đăng ký qua kết nối thứ nhất
1302. Thiết bị kích hoạt việc tái xác thực
1303. Quy trình tái xác thực
1304. Tin nhắn NAS SMC
1305. Kích hoạt khóa mới dùng cho kết nối thứ nhất, và bắt đầu bộ định thời
1306. Gửi tin nhắn NAS SMP
1307. Kích hoạt khóa mới dùng cho kết nối thứ nhất, và bắt đầu bộ định thời
1308. Gửi tin nhắn hoàn thành đăng ký
Kết nối thứ hai
1309. Trước khi bộ định thời kết thúc, xác định sử dụng khóa cũ dùng cho kết nối thứ hai
1310. Tin nhắn yêu cầu đăng ký mà trên đó việc bảo vệ tính toàn vẹn được thực hiện bằng cách sử dụng khóa cũ dùng cho kết nối thứ hai mang ký hiệu nhận dạng khóa thứ hai
1311. Xác định, dựa vào ký hiệu nhận dạng khóa thứ hai, để sử dụng khóa cũ dùng cho kết nối thứ hai, và thực hiện xác nhận tính toàn vẹn trên tin nhắn yêu cầu đăng ký bằng cách sử dụng khóa cũ dùng cho kết nối thứ hai
1312. Gửi tin nhắn hoàn thành đăng ký
1314. Sau khi bộ định thời kết thúc, xóa khóa cũ dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa thứ hai
1313. Sau khi bộ định thời kết thúc, xóa khóa cũ dùng cho kết nối thứ hai và ký hiệu nhận dạng khóa thứ hai

FIG. 13

13/15

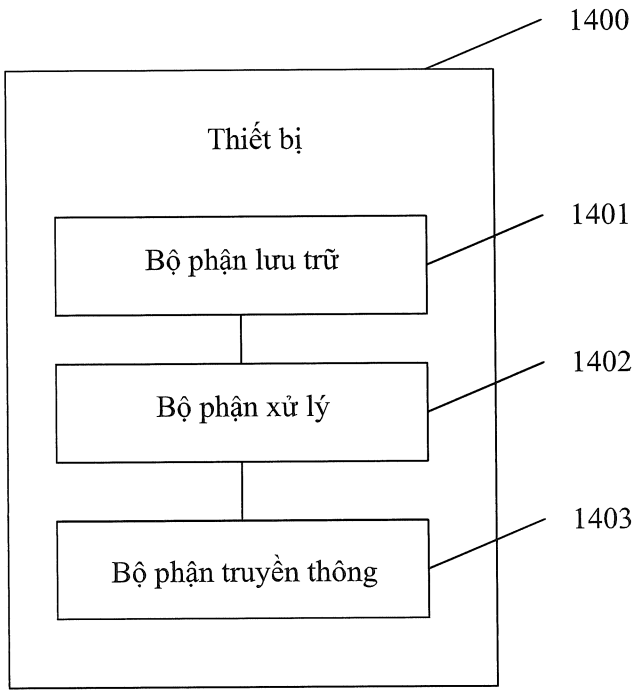

FIG. 14

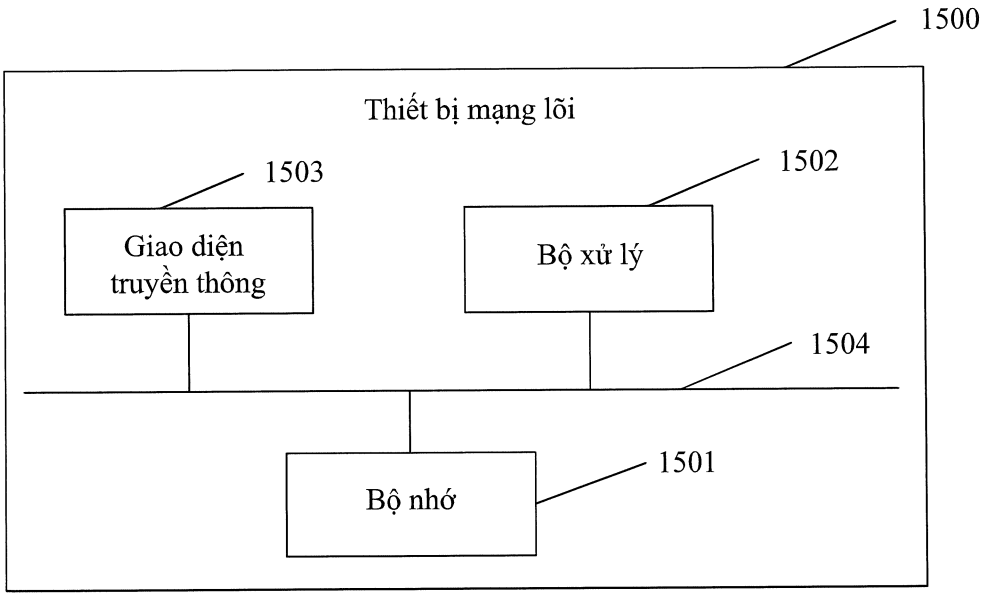

FIG. 15

14/15

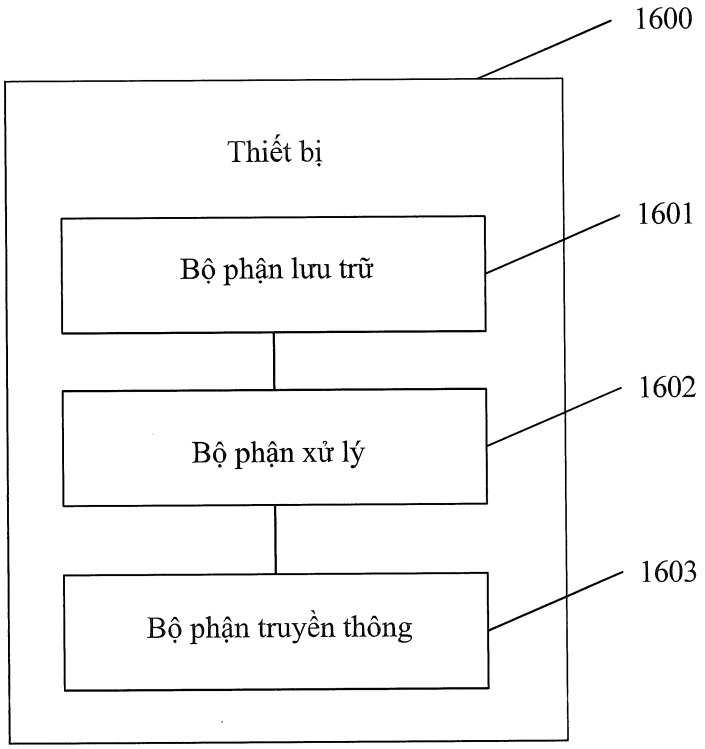
1600
Thiết bị
1601
Bộ phận lưu trữ
1602
Bộ phận xử lý
1603
Bộ phận truyền thông

FIG. 16

15/15

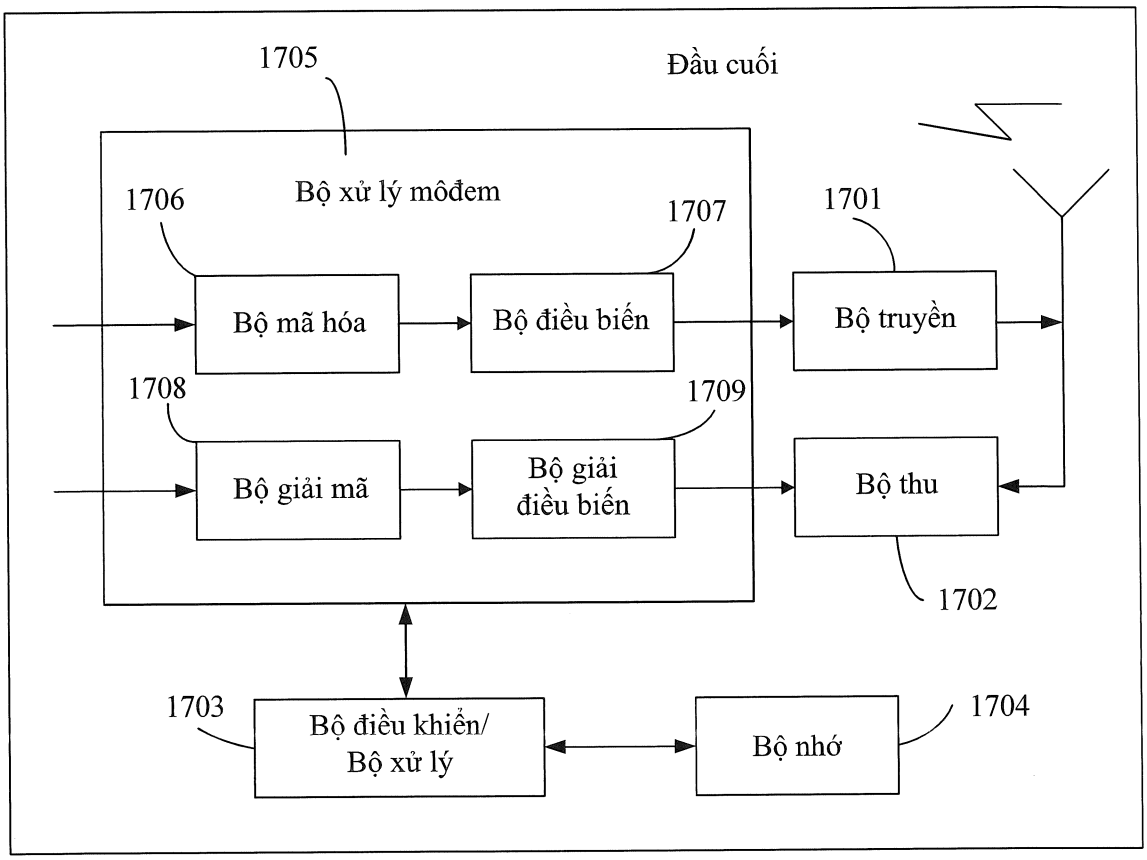
1705
Đầu cuối
Bộ xử lý môđem
1706
1707
1701
Bộ mã hóa
Bộ điều biến
Bộ truyền
1708
1709
Bộ giải mã
Bộ giải điều biến
Bộ thu
1702
1703
Bộ điều khiển/ Bộ xử lý
Bộ nhớ
1704

FIG. 17