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

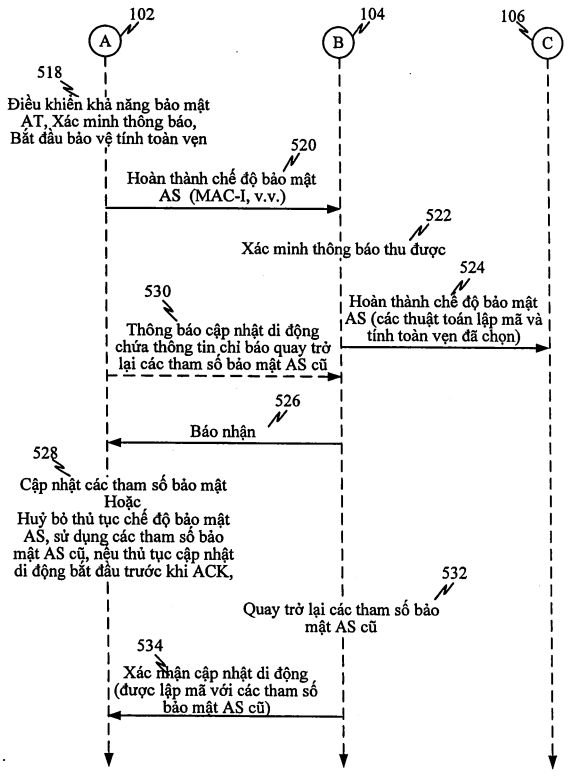
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)** (11) **1-0020952**
CỤC SỞ HỮU TRÍ TUỆ

(51)[7] **H04W 36/00**, H04L 29/06, H04W 12/04 (13) **B**

(21) 1-2013-00172 (22) 17.06.2011
(86) PCT/US2011/040964 17.06.2011 (87) WO2011/160073 22.12.2011
(30) 61/356,464 18.06.2010 US
13/162,313 16.06.2011 US
(45) 27.05.2019 374 (43) 27.05.2013 302
(73) QUALCOMM INCORPORATED (US)
Attn: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121, United States of America
(72) PATIL, Kiran KishanRao (IN), SANKA, Suresh (IN), HSU, Liangchi (US), GHOLMIEH, Aziz (US)
(74) Công ty TNHH Quốc tế D & N (D&N INTERNATIONAL CO.,LTD.)

(54) ĐẦU CUỐI TRUY NHẬP VÀ PHƯƠNG PHÁP VẬN HÀNH Ở ĐẦU CUỐI TRUY NHẬP

(57) Sáng chế đề cập đến phương pháp và thiết bị đồng bộ hoá các tham số bảo mật giữa các đầu cuối truy nhập và mạng không dây. Đầu cuối truy nhập và thực thể mạng có thể điều khiển thủ tục chế độ bảo mật, trong đó đầu cuối truy nhập truyền thông báo hoàn thành chế độ bảo mật đến thực thể mạng. Ngay khi thu được thông báo hoàn thành chế độ bảo mật, thực thể mạng có thể cập nhật các tham số bảo mật mới. Đầu cuối truy nhập có thể khởi đầu thủ tục di động trong khi thủ tục chế độ bảo mật đang diễn ra và do đó có thể huỷ bỏ thủ tục chế độ bảo mật và quay trở lại các tham số bảo mật cũ. Đầu cuối truy nhập có thể truyền đến thực thể mạng thông báo cập nhật di động chứa thông tin chỉ báo trạng thái dành riêng được làm thích ứng để báo cho thực thể mạng biết rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ. Đáp lại thông báo cập nhật di động, thực thể mạng có thể quay trở lại các tham số bảo mật cũ.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến thiết bị và hệ thống truyền thông không dây, và cụ thể hơn là kỹ thuật đồng bộ hoá các cấu hình bảo mật giữa các đầu cuối truy nhập và các thực thể mạng.

Tình trạng kỹ thuật của sáng chế

Bảo mật là một đặc điểm quan trọng của hệ thống truyền thông không dây. Bảo mật trong một số hệ thống truyền thông không dây thường có thể bao gồm hai đặc điểm: "Toàn vẹn dữ liệu" và "Lập mã". "Toàn vẹn dữ liệu" là đặc điểm đảm bảo rằng không mạng lừa đảo nào có khả năng truyền các thông báo báo hiệu không cần thiết với ý định gây ra, hoặc thực sự gây ra ảnh hưởng không mong muốn nào đến cuộc gọi đi. "Lập mã" là đặc điểm đảm bảo rằng tất cả các thông báo báo hiệu và dữ liệu được lập mã qua giao diện không gian để ngăn không cho bên thứ ba nghe lén các thông báo này. Trong một số hệ thống truyền thông không dây, như hệ thống viễn thông di động đa năng (UMTS - Universal Mobile Telecommunication System), bảo vệ tính toàn vẹn là bắt buộc trong khi lập mã là tuỳ ý. Bảo vệ tính toàn vẹn có thể chỉ được thực hiện trên các sóng mang vô tuyến báo hiệu, còn lập mã có thể được thực hiện trên các sóng mang vô tuyến báo hiệu cũng như các sóng mang vô tuyến dữ liệu.

Trong mạng không dây thông thường, đầu cuối truy nhập (AT- Access Terminal) thường dàn xếp với mạng không dây để thiết lập các tham số bảo mật, như các khoá mã hoá dùng cho việc mã hoá (hoặc lập mã) các tín hiệu truyền thông giữa đầu cuối truy nhập và các thành phần mạng. Các tham số bảo mật như vậy có thể được cập nhật và/hoặc thay đổi một cách ngẫu nhiên để đảm bảo bí mật của dữ liệu truyền giữa đầu cuối truy nhập và các thành phần mạng.

Ví dụ về một phương pháp thông thường để khởi tạo hoặc cập nhật các tham số bảo mật giữa đầu cuối truy nhập và mạng không dây thường bao gồm đầu cuối truy nhập thu lệnh chế độ bảo mật từ mạng không dây và cập nhật các tham số bảo mật của nó dựa vào lệnh chế độ bảo mật thu được. Sau khi đầu cuối truy nhập cập nhật các tham số bảo mật của nó, và trước khi cài đặt các tham số bảo mật mới, đầu

cuối truy nhập gửi thông báo hoàn thành chế độ bảo mật đến mạng không dây. Ngay khi thu được thông báo hoàn thành chế độ bảo mật, mạng không dây sẽ khởi đầu sử dụng các tham số bảo mật mới để bảo vệ thông báo liên kết xuống bất kỳ sau đó truyền đến đầu cuối truy nhập.

Tuy nhiên, đầu cuối truy nhập sẽ không khởi đầu sử dụng các tham số bảo mật mới để bảo vệ thông báo liên kết lên bất kỳ truyền đến mạng không dây cho đến khi thu được thông báo báo nhận từ mạng không dây đáp lại thông báo hoàn thành chế độ bảo mật truyền từ đầu cuối truy nhập. Nói cách khác, đầu cuối truy nhập sẽ không sử dụng các tham số bảo mật mới cho các thông báo truyền từ đầu cuối truy nhập đến mạng không dây cho đến khi đầu cuối truy nhập thu được từ mạng không dây thông báo báo nhận rằng thông báo hoàn thành chế độ bảo mật đã được thu và xác thực.

Do đó, có cửa sổ thời gian nhỏ giữa thời điểm thủ tục chế độ bảo mật hoàn thành ở mạng không dây (ví dụ, khi thông báo hoàn thành chế độ bảo mật thu được ở mạng không dây) và thời điểm thủ tục chế độ bảo mật được hoàn thành ở đầu cuối truy nhập (ví dụ, khi báo nhận thu được ở đầu cuối truy nhập và các tham số bảo mật được cập nhật). Vì cửa sổ thời gian này, mạng không dây có thể được cập nhật ở các tham số bảo mật mới, trong khi đầu cuối truy nhập giữ nguyên các tham số bảo mật cũ. Ví dụ, đầu cuối truy nhập thông thường thường được làm thích ứng để huỷ bỏ thủ tục chế độ bảo mật khi một số thủ tục khác được khởi tạo, như thủ tục di động chẳng hạn.

Trong trường hợp mạng không dây được cập nhật ở các tham số bảo mật mới, nhưng đầu cuối truy nhập vẫn tiếp tục với các tham số bảo mật cũ, thì kết nối không dây giữa hai thành phần này thường bị lỗi, làm cho cuộc gọi bị rơi và dẫn đến sự không hài lòng của người sử dụng đầu cuối truy nhập. Do đó, có thể có lợi nếu cung cấp phương pháp và thiết bị để tránh tình trạng mạng không dây được cập nhật ở các tham số bảo mật mới trong khi đầu cuối truy nhập vẫn tiếp tục với các tham số bảo mật cũ và/hoặc để đồng bộ hoá các tham số bảo mật khi xảy ra tình trạng này.

Bản chất kỹ thuật của sáng chế

Các dấu hiệu khác nhau tạo điều kiện thuận lợi cho việc đồng bộ hoá các tham số bảo mật giữa đầu cuối truy nhập và mạng truy nhập. Một dấu hiệu cho phép các đầu cuối truy nhập được làm thích ứng để tạo điều kiện thuận lợi cho việc đồng

bộ hoá này. Theo một hoặc nhiều phương án, đầu cuối truy nhập (AT) có thể có giao diện truyền thông không dây ghép nối với mạch xử lý. Giao diện truyền thông không dây này có thể được làm thích ứng để tạo điều kiện thuận lợi cho việc truyền thông không dây của đầu cuối truy nhập.

Theo ít nhất một ứng dụng, mạch xử lý có thể được làm thích ứng để điều khiển thủ tục chế độ bảo mật để tạo cấu hình lại các tham số bảo mật của đầu cuối truy nhập. Trong khi thủ tục chế độ bảo mật tiến hành, mạch xử lý có thể khởi đầu thủ tục di động. Mạch xử lý còn có thể huỷ bỏ thủ tục chế độ bảo mật và quay trở lại các tham số bảo mật cũ do khởi đầu thủ tục di động. Thông báo cập nhật di động có thể được truyền từ mạch xử lý qua giao diện truyền thông không dây, trong đó thông báo cập nhật di động này chứa thông tin chỉ báo trạng thái bảo mật dành riêng được làm thích ứng để chỉ ra rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

Theo ít nhất một ứng dụng khác, mạch xử lý có thể được làm thích ứng để điều khiển thủ tục chế độ bảo mật để tạo cấu hình lại các tham số bảo mật của đầu cuối truy nhập. Trong khi thủ tục chế độ bảo mật tiến hành, mạch xử lý có thể khởi đầu thủ tục di động, bao gồm truyền thông báo cập nhật di động. Mạch xử lý còn có thể huỷ bỏ thủ tục chế độ bảo mật và quay trở lại các tham số bảo mật cũ do khởi đầu thủ tục di động. Mạch xử lý có thể thu thông báo xác nhận cập nhật di động đáp lại thông báo cập nhật di động qua giao diện truyền thông không dây. Nếu không có khả năng giải mã thông báo xác nhận cập nhật di động bằng cách sử dụng các tham số bảo mật cũ, thì mạch xử lý có thể chuyển sang các tham số bảo mật mới.

Theo ít nhất một ứng dụng khác, mạch xử lý có thể được làm thích ứng để điều khiển thủ tục chế độ bảo mật bao gồm truyền thông báo hoàn thành chế độ bảo mật đến mạng truy nhập qua giao diện truyền thông không dây. Đáp lại thông báo hoàn thành chế độ bảo mật, mạch xử lý có thể thu thông báo báo nhận qua giao diện truyền thông không dây. Mạch xử lý có thể cập nhật các tham số bảo mật mới, và truyền thông báo báo nhận khác đến mạng truy nhập qua giao diện truyền thông không dây, trong đó thông báo báo nhận khác này được làm thích ứng để chỉ ra rằng đầu cuối truy nhập đã cập nhật ở các tham số bảo mật mới.

Phương pháp vận hành trong đầu cuối truy nhập cũng được đề xuất theo một dấu hiệu để tạo điều kiện thuận lợi cho việc đồng bộ hoá các tham số bảo mật giữa

đầu cuối truy nhập và mạng truy nhập. Theo ít nhất một ứng dụng của các phương pháp này, thủ tục chế độ bảo mật có thể được thực hiện để tạo cấu hình lại các tham số bảo mật của đầu cuối truy nhập. Thủ tục di động có thể được khởi tạo trong khi thủ tục chế độ bảo mật tiến hành. Thủ tục chế độ bảo mật có thể được huỷ bỏ do khởi đầu thủ tục cập nhật di động và đầu cuối truy nhập có thể quay trở lại các tham số bảo mật cũ. Thông báo cập nhật di động có thể được truyền, trong đó thông báo cập nhật di động này chứa chỉ báo trạng thái dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

Theo ít nhất một ứng dụng khác, thủ tục chế độ bảo mật có thể được thực hiện để tạo cấu hình lại các tham số bảo mật của đầu cuối truy nhập. Thủ tục di động có thể được khởi tạo trong khi thủ tục chế độ bảo mật tiến hành, bao gồm truyền thông báo cập nhật di động. Thủ tục chế độ bảo mật có thể được huỷ bỏ do khởi đầu thủ tục cập nhật di động và đầu cuối truy nhập có thể quay trở lại các tham số bảo mật cũ. Thông báo xác nhận cập nhật di động có thể thu được đáp lại thông báo cập nhật di động. Đầu cuối truy nhập có thể được chuyển sang các tham số bảo mật mới nếu đầu cuối truy nhập không thể giải mã thông báo xác nhận cập nhật di động khi sử dụng các tham số bảo mật cũ.

Theo một hoặc nhiều ứng dụng khác, các phương pháp này có thể bao gồm bước điều khiển thủ tục chế độ bảo mật gồm truyền thông báo hoàn thành chế độ bảo mật đến mạng truy nhập. Đáp lại thông báo hoàn thành chế độ bảo mật, thu thông báo báo nhận. Đầu cuối truy nhập có thể được cập nhật ở các tham số bảo mật mới. Thông báo báo nhận khác có thể được truyền đến mạng truy nhập, trong đó thông báo báo nhận khác này được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã được cập nhật ở các tham số bảo mật mới.

Dấu hiệu khác cho phép các thực thể mạng được làm thích ứng để tạo điều kiện thuận lợi cho việc đồng bộ hoá các tham số bảo mật giữa đầu cuối truy nhập và mạng truy nhập. Các thực thể mạng này có thể có giao diện truyền thông ghép nối với mạch xử lý. Theo ít nhất một ứng dụng, mạch xử lý có thể được làm thích ứng để thu thông báo hoàn thành chế độ bảo mật từ đầu cuối truy nhập qua giao diện truyền thông. Đáp lại thông báo hoàn thành chế độ bảo mật, mạch xử lý có thể cập nhật ở các tham số bảo mật mới. Mạch xử lý còn có thể thu thông báo cập nhật di động từ đầu cuối truy nhập qua giao diện truyền thông. Thông báo cập nhật di động có thể

chứa thông tin chỉ báo trạng thái bảo mật dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ. Đáp lại thông báo cập nhật di động thu được, mạch xử lý có thể quay trở lại các tham số bảo mật cũ.

Theo ít nhất một ứng dụng khác, mạch xử lý có thể được làm thích ứng để thu thông báo hoàn thành chế độ bảo mật từ đầu cuối truy nhập qua giao diện truyền thông. Đáp lại thông báo hoàn thành chế độ bảo mật, mạch xử lý có thể cập nhật ở các tham số bảo mật mới. Mạch xử lý có thể thu thông báo cập nhật di động từ đầu cuối truy nhập, và có thể truyền thông báo xác nhận cập nhật di động đến đầu cuối truy nhập đáp lại thông báo cập nhật di động. Nếu không thu được thông tin đáp lại thông báo xác nhận cập nhật di động từ đầu cuối truy nhập, mạch xử lý có thể quay trở lại các tham số bảo mật cũ và có thể truyền lại thông báo xác nhận cập nhật di động đến đầu cuối truy nhập bằng cách sử dụng các tham số bảo mật cũ để lập mã thông báo.

Theo một hoặc nhiều ứng dụng khác nữa, mạch xử lý có thể được làm thích ứng để thu thông báo hoàn thành chế độ bảo mật từ đầu cuối truy nhập qua giao diện truyền thông. Mạch xử lý có thể truyền thông báo báo nhận đáp lại thông báo hoàn thành chế độ bảo mật. Mạch xử lý có thể thu thông báo báo nhận khác từ đầu cuối truy nhập chỉ báo rằng đầu cuối truy nhập đã cập nhật ở các tham số bảo mật mới. Đáp lại thông báo báo nhận khác, mạch xử lý có thể cập nhật ở các tham số bảo mật mới.

Các thao tác phương pháp ở thực thể mạng cũng được đề xuất theo một dấu hiệu để tạo điều kiện thuận lợi cho việc đồng bộ hoá các tham số bảo mật giữa đầu cuối truy nhập và mạng truy nhập. Theo ít nhất một ứng dụng của phương pháp này, thông báo hoàn thành chế độ bảo mật có thể thu được từ đầu cuối truy nhập. Đáp lại thông báo hoàn thành chế độ bảo mật, thực thể mạng có thể được cập nhật ở các tham số bảo mật mới. Thông báo cập nhật di động có thể thu được từ đầu cuối truy nhập, trong đó thông báo cập nhật di động chứa chỉ báo trạng thái bảo mật dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ. Đáp lại thông báo cập nhật di động, thực thể mạng có thể quay trở lại các tham số bảo mật cũ.

Theo ít nhất một ứng dụng của phương pháp này, thông báo hoàn thành chế độ bảo mật có thể thu được từ đầu cuối truy nhập. Đáp lại thông báo hoàn thành chế

độ bảo mật, thực thể mạng có thể được cập nhật ở các tham số bảo mật mới. Thông báo cập nhật di động có thể thu được từ đầu cuối truy nhập, và thông báo xác nhận cập nhật di động có thể được truyền đến đầu cuối truy nhập đáp lại thông báo cập nhật di động thu được. Nếu không thu được thông tin đáp lại thông báo xác nhận cập nhật di động từ đầu cuối truy nhập, thì thực thể mạng có thể quay trở lại các tham số bảo mật cũ và thông báo xác nhận cập nhật di động có thể được truyền lại đến đầu cuối truy nhập bằng cách sử dụng các tham số bảo mật cũ để lập mã thông báo xác nhận cập nhật di động.

Theo một hoặc nhiều ứng dụng khác nữa, thông báo hoàn thành chế độ bảo mật có thể thu được từ đầu cuối truy nhập. Thông báo báo nhận có thể được truyền đáp lại thông báo hoàn thành chế độ bảo mật. Thông báo báo nhận khác có thể thu được từ đầu cuối truy nhập cho biết rằng đầu cuối truy nhập đã cập nhật ở các tham số bảo mật mới. Đáp lại thông báo báo nhận khác này, thực thể mạng có thể được cập nhật ở các tham số bảo mật mới.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ khối minh họa môi trường mạng, trong đó các dấu hiệu khác nhau có thể được sử dụng theo ít nhất một ví dụ.

Fig.2 minh họa phân cấp khóa thông thường có thể được cài đặt trong mạng truyền thông không dây thông thường.

Fig.3 minh họa ngăn xếp giao thức làm ví dụ có thể được cài đặt trong thiết bị truyền thông vận hành trong mạng chuyển gói.

Fig.4 là sơ đồ khối minh họa hệ thống mạng, trong đó các khoá bảo mật khác nhau đã được minh họa trên Fig. 2 và Fig.3 có thể được tạo lập.

Fig.5 (bao gồm Fig.5A và Fig.5B) là lưu đồ minh họa một ví dụ về thao tác đồng bộ hoá tham số bảo mật, trong đó đầu cuối truy nhập chỉ báo cho mạng truy nhập biết rằng thủ tục chế độ bảo mật đã được huỷ bỏ ở đầu cuối truy nhập.

Fig.6 là lưu đồ minh họa ví dụ về thao tác đồng bộ hoá tham số bảo mật ở đầu cuối truy nhập khi các tham số bảo mật ở mạng truy nhập được cập nhật và các tham số bảo mật ở đầu cuối truy nhập không được cập nhật.

Fig.7 là lưu đồ minh họa ví dụ về thao tác đồng bộ hoá tham số bảo mật của đầu cuối truy nhập, mạng truy nhập và mạng lõi để tạo điều kiện thuận lợi cho việc

cập nhật các tham số bảo mật tại mạng truy nhập chỉ sau khi các tham số bảo mật được cập nhật ở đầu cuối truy nhập.

Fig.8 là lưu đồ minh họa ví dụ về thao tác đồng bộ hoá tham số bảo mật ở mạng truy nhập khi các tham số bảo mật của mạng truy nhập được cập nhật và các tham số bảo mật của đầu cuối truy nhập không được cập nhật.

Fig.9 là sơ đồ khối minh họa các thành phần lựa chọn của đầu cuối truy nhập theo ít nhất một phương án.

Fig.10 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở đầu cuối truy nhập để chỉ báo cho mạng truy nhập khi đầu cuối truy nhập quay trở lại các tham số bảo mật cũ.

Fig.11 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở đầu cuối truy nhập để xác định trạng thái của các tham số bảo mật ở mạng truy nhập để truyền thông với đầu cuối truy nhập.

Fig.12 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở đầu cuối truy nhập để chỉ báo cho mạng truy nhập khi đầu cuối truy nhập được cập nhật ở các tham số bảo mật mới.

Fig.13 là sơ đồ khối minh họa các thành phần lựa chọn của thực thể mạng theo ít nhất một phương án.

Fig.14 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở thực thể mạng để xác định rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

Fig.15 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở thực thể mạng để xác định rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

Fig.16 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở thực thể mạng để cập nhật từ các tham số bảo mật cũ sang các tham số bảo mật mới sau khi đầu cuối truy nhập đã cập nhật các tham số bảo mật mới.

Mô tả chi tiết sáng chế

Trong phần mô tả sau, các chi tiết cụ thể được cung cấp để giúp hiểu rõ các ứng dụng được mô tả. Tuy nhiên, người có hiểu biết trung bình về lĩnh vực kỹ thuật này sẽ hiểu rằng các ứng dụng khác nhau có thể được thực hiện mà không cần đến các chi tiết cụ thể này. Ví dụ, các mạch có thể được thể hiện bằng sơ đồ khối để không làm cho các ứng dụng khó hiểu ở những chi tiết không cần thiết. Trong trường

hợp khác, các mạch, các cấu trúc và các kỹ thuật đã biết có thể được thể hiện chi tiết để giúp hiểu rõ các ứng dụng được mô tả.

Thuật ngữ "làm ví dụ" được sử dụng ở đây có nghĩa là "dùng làm ví dụ, trường hợp hoặc minh họa." Khía cạnh hoặc thiết kế bất kỳ được mô tả ở đây "làm ví dụ" không nhất thiết phải hiểu là được ưu tiên hoặc có lợi hơn các phương án hoặc ứng dụng khác. Tương tự, thuật ngữ "các phương án" không đòi hỏi tất cả các phương án phải có dấu hiệu, ưu điểm hoặc chế độ làm việc được bàn luận. Thuật ngữ "đầu cuối truy nhập" như được sử dụng ở đây được hiểu theo nghĩa rộng. Ví dụ, "đầu cuối truy nhập" có thể bao gồm phương tiện người dùng và/hoặc thiết bị thuê bao, như máy điện thoại di động, máy nhắn tin, môđem không dây, thiết bị trợ giúp số cá nhân, thiết bị quản lý thông tin cá nhân (PIM - Personal Information Manager), máy nghe nhạc cá nhân, máy tính cầm tay, máy tính xách tay, và/hoặc thiết bị truyền thông di động/tính toán khác truyền thông, ít nhất một phần, qua mạng không dây hoặc mạng chia ô.

Tổng quan

Một hoặc nhiều dấu hiệu tạo điều kiện thuận lợi và/hoặc đồng bộ hoá các tham số bảo mật giữa đầu cuối truy nhập và một hoặc nhiều thực thể của mạng không dây. Theo một dấu hiệu, đầu cuối truy nhập (AT) có thể chỉ báo cho thực thể mạng biết rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ. Ví dụ, đầu cuối truy nhập có thể truyền chỉ báo với thông báo cập nhật di động để báo cho thực thể mạng biết về việc quay trở lại này. Theo một ví dụ khác, đầu cuối truy nhập có thể truyền thông báo đến thực thể mạng để báo cho thực thể mạng biết rằng đầu cuối truy nhập đã cập nhật thành công ở các tham số bảo mật mới.

Theo một dấu hiệu, đầu cuối truy nhập có thể xác định rằng thực thể mạng đã cập nhật ở các tham số bảo mật mới và do vậy có thể cập nhật các tham số bảo mật riêng của nó. Ví dụ, sau khi huỷ bỏ thủ tục chế độ bảo mật để cập nhật ở các tham số bảo mật mới, đầu cuối truy nhập có thể xác định rằng nó không thể giải mã thông báo thu được từ thực thể mạng. Đáp lại thất bại, đầu cuối truy nhập có thể cập nhật ở các tham số bảo mật mới và thử giải mã thông báo thu được bằng cách sử dụng các tham số bảo mật mới. Nếu đầu cuối truy nhập thành công trong việc giải mã thông báo thu được với các tham số bảo mật mới, thì đầu cuối truy nhập có thể tiếp tục sử dụng các tham số bảo mật mới.

Theo một dấu hiệu, thực thể mạng có thể xác định rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ và do đó có thể trở lại các tham số bảo mật riêng của nó. Ví dụ, sau khi cập nhật ở các tham số bảo mật mới, thực thể mạng có thể truyền đến đầu cuối truy nhập thông báo được lập mã theo các tham số bảo mật mới. Nếu thực thể mạng không thu được thông tin đáp lại thông báo đã truyền, thì thực thể mạng có thể quay trở lại các tham số bảo mật cũ và truyền thông báo bằng cách sử dụng các tham số bảo mật cũ để lập mã thông báo. Nếu thực thể mạng thu được thông tin đáp lại thông báo đã truyền bằng cách sử dụng các tham số bảo mật cũ, thì thực thể mạng có thể tiếp tục sử dụng các tham số bảo mật cũ.

Môi trường mạng làm ví dụ

Fig.1 là sơ đồ khối minh họa môi trường mạng, trong đó các dấu hiệu khác nhau có thể được sử dụng theo ít nhất một ví dụ. Đầu cuối truy nhập 102 có thể được làm thích ứng để truyền thông không dây với mạng truy nhập 104 ghép nối truyền thông với mạng lõi 106.

Nói chung, mạng truy nhập 104 bao gồm thiết bị vô tuyến được làm thích ứng để cho phép các đầu cuối truy nhập 102 truy nhập mạng, trong khi mạng lõi 106 có khả năng chuyển mạch và định tuyến để kết nối với mạng chuyển mạch (ví dụ, mạng điện thoại chuyển mạch công cộng (PTSN - Public Switched Telephone Network)/mạng dịch vụ số tích hợp (ISDN - Integrated Services Digital Network) 108) hoặc kết nối với mạng chuyển gói (ví dụ, internet 110). Mạng lõi 106 còn tạo điều kiện thuận lợi cho các dịch vụ quản lý và xác thực di động và vị trí thuê bao. Trong một số ví dụ, như được minh họa trên Fig.1, mạng lõi 106 có thể là mạng tương thích hệ thống viễn thông di động đa năng (UMTS - Universal Mobile Telecommunication System) hoặc mạng tương thích hệ truyền thông di động toàn cầu (GSM - Global System for Mobile Communications).

Mạng truy nhập 104 có thể bao gồm một hoặc nhiều nút truy nhập 112 (ví dụ, trạm cơ sở, nút B, v.v.) và bộ điều khiển mạng vô tuyến (RNC - Radio Network Controller) 114. Mỗi nút truy nhập 112 thường gắn với một ô, hoặc cung, bao gồm vùng địa lý phủ sóng thu và truyền. Các ô, hoặc các cung, có thể xếp chồng lên nhau. Bộ điều khiển mạng vô tuyến (RNC) 114 có thể được làm thích ứng để điều khiển các nút truy nhập 112 kết nối truyền thông với nó. Bộ điều khiển mạng vô tuyến (RNC) 114 còn có thể được làm thích ứng để thực hiện quản lý tài nguyên vô tuyến,

một số chức năng quản lý di động, và có thể là điểm mà việc mã hoá được thực hiện trước khi dữ liệu người dùng được truyền đến và từ đầu cuối truy nhập 102. Bộ điều khiển mạng vô tuyến (RNC) 114 ghép nối truyền thông với mạng lõi 106 qua nút hỗ trợ dịch vụ vô tuyến gói đa năng (GPRS - General Packet Radio Service) (SGSN) phục vụ 116 cho các cuộc gọi chuyển gói và qua trung tâm chuyển mạch di động (MSC - Mobile Switching Center) 118, trung tâm này có thể có thanh ghi vị trí khách (VLR - Visitor Location Register), cho các cuộc gọi chuyển mạch. Thanh ghi vị trí gốc (HLR - Home Location Register) và trung tâm xác thực (AuC - Authentication Center) 120 có thể được dùng để xác thực các đầu cuối truy nhập trước khi cung cấp các dịch vụ truyền thông qua mạng lõi 106. Lưu ý rằng, trong các kiểu mạng khác, các chức năng của HLR/AuC 120 và các thành phần khác (như MSC/VLR 118) có thể được thực hiện bởi các thực thể mạng tương đương khác. Ví dụ, trong mạng phát triển dài hạn (LTE - Long Term Evolution), một số hoặc tất cả các chức năng của HLR/AuC 120 có thể được thực hiện bởi máy chủ thuê bao gốc (HSS - Home Subscriber Server). Mạng lõi 106 còn có thể bao gồm thực thể quản lý di động (MME - Mobile Management Entity) thực hiện việc kích hoạt/khử hoạt kênh thông cao của các đầu cuối truy nhập, hỗ trợ việc xác thực các đầu cuối truy nhập, và/hoặc thực hiện các thủ tục theo dõi và/hoặc nhắn tin đầu cuối truy nhập (bao gồm việc truyền lại) cho các đầu cuối truy nhập ghép nối với mạng lõi.

Khi đầu cuối truy nhập 102 thử kết nối với mạng truy nhập 104, đầu cuối truy nhập 102 được xác thực ban đầu để xác minh nhận dạng của đầu cuối truy nhập 102. Đầu cuối truy nhập 102 cũng xác thực mạng để xác minh rằng nó kết nối với mạng truy nhập 104 được phép sử dụng. Việc dàn xếp thường diễn ra giữa đầu cuối truy nhập 102 và mạng truy nhập 104 và/hoặc mạng lõi 106 để thiết lập các tham số bảo mật, như các khoá mã hoá dùng cho việc mã hoá các tín hiệu truyền thông giữa đầu cuối truy nhập 102 và các thành phần mạng (ví dụ, mạng truy nhập 104 và/hoặc mạng lõi 106). Các tham số bảo mật này có thể được cập nhật và/hoặc thay đổi ngẫu nhiên để đảm bảo bí mật của dữ liệu truyền giữa đầu cuối truy nhập 102 và các thành phần mạng.

Fig.2 minh họa phân cấp khóa thông thường 200 có thể được thực thi để thiết lập các tham số bảo mật (ví dụ, các khoá mã hoá) dùng cho việc mã hoá các tín hiệu truyền thông giữa đầu cuối truy nhập 102 và các thành phần mạng (ví dụ, mạng truy

nhập 104 và/hoặc mạng lõi 106). Ở đây, môđun nhận dạng thuê bao toàn cầu (USIM - Universal Subscriber Identity Module) trong đầu cuối truy nhập 102, và mạng lõi 106 (ví dụ, trung tâm xác thực (HLR/AuC 120 trên Fig.1)) sử dụng khoá chính K 202 để tạo ra khoá mật mã (CK - Cipher Key) 204 và khoá toàn vẹn (IK – Integrity Key) 206. Khoá mật mã (CK) 204 và khoá toàn vẹn (IK) 206 có thể được sử dụng bởi thiết bị truyền thông và mạng lõi 106 (ví dụ, thanh ghi vị trí gốc (HLR)) để tạo ra khoá của Thực thể quản lý bảo mật truy nhập K_ASME (Access Security Management Entity Key)208. Việc kích hoạt bảo mật của đầu cuối truy nhập 102 có thể được thực hiện qua thủ tục xác thực và thoả thuận khóa (AKA - Authentication và Key Agreement), thủ tục cấu hình chế độ bảo mật tầng không truy nhập (NAS SMC - Non-Access Stratum Security Mode Configuration) và thủ tục cấu hình chế độ bảo mật tầng truy nhập (AS SMC - Access Stratum Security mode Configuration). AKA được sử dụng để suy ra khoá K_ASME 208, khoá này sẽ được dùng làm khoá cơ sở để tính các khoá NAS (tầng không truy nhập) 210 và 212 và các khoá AS (tầng truy nhập) 214, 216, 218 và 220. Đầu cuối truy nhập 102 và mạng lõi 106 có thể sử dụng K_ASME 208 để tạo ra một hoặc nhiều khoá bảo mật này.

Các mạng chuyển gói có thể được tạo dựng theo nhiều lớp giao thức phân cấp, trong đó các lớp giao thức thấp hơn cung cấp dịch vụ cho các lớp cao hơn và mỗi lớp chịu trách nhiệm về các nhiệm vụ khác nhau. Ví dụ, Fig.3 minh họa ngăn xếp giao thức làm ví dụ có thể được thực thi trong thiết bị truyền thông vận hành trong mạng chuyển gói. Trong ví dụ này, ngăn xếp giao thức 302 bao gồm lớp vật lý (PHY Physical) 304, lớp điều khiển truy nhập phương tiện (MAC - Media Access Control) 306, lớp điều khiển liên kết vô tuyến (RLC - Radio Link Control) 308, lớp giao thức hội tụ dữ liệu gói (PDCP - Packet Data Convergence Protocol) 310, lớp điều khiển tài nguyên vô tuyến (RRC - Radio Resource Control) 312, lớp tầng không truy nhập (NAS - Non-Access Stratum) 314, và lớp ứng dụng (APP - Application) 316.

Các lớp bên dưới lớp NAS 314 thường được gọi là lớp tầng truy nhập (AS - Access Stratum) 318. Lớp RLC 308 có thể gồm một hoặc nhiều kênh 320. Lớp RRC 312 có thể thực hiện các chế độ giám sát khác nhau đối với đầu cuối truy nhập, bao gồm trạng thái kết nối và trạng thái rỗi. Lớp tầng không truy nhập (NAS) 314 có thể duy trì ngữ cảnh quản lý di động, ngữ cảnh dữ liệu gói của thiết bị truyền thông

và/hoặc các địa chỉ IP của nó. Lưu ý rằng các lớp khác có thể có mặt trong ngăn xếp giao thức 302 (ví dụ, bên trên, bên dưới và/hoặc ở giữa các lớp được minh họa), nhưng được bỏ qua vì mục đích minh họa.

Theo các hình vẽ từ Fig.1 đến Fig. 3, các kênh thông cao vô tuyến/phiên 322 có thể được thiết lập, ví dụ ở lớp RRC 312 và/hoặc lớp NAS 314. Do đó, lớp NAS 314 có thể được sử dụng bởi đầu cuối truy nhập 102 và mạng lõi 106 để tạo ra các khoá bảo mật K_NAS-enc 210 và K_NAS-int 212 được thể hiện trên Fig.2. Tương tự, lớp RRC 312 có thể được sử dụng bởi đầu cuối truy nhập 102 và mạng truy nhập 104 (ví dụ, RNC 114) để tạo ra các khoá bảo mật tầng truy nhập (AS) K_UP-enc 216, K_RRC-enc 218, và K_RRC-int 220. Mặc dù các khoá bảo mật K_UP-enc 216, K_RRC-enc 218 và K_RRC-int 220 có thể được tạo ra ở lớp RRC 312, nhưng các khoá này có thể được sử dụng bởi lớp PDCP 310 để đảm bảo bảo mật báo hiệu và/hoặc truyền thông người dùng/dữ liệu. Ví dụ, khoá K_UP-enc 216 có thể được sử dụng bởi lớp PDCP 310 để đảm bảo bảo mật truyền thông mặt phẳng người dùng/dữ liệu (UP - user/data plane), trong khi các khoá K_RRC-enc 218 và K_RRC-int 220 có thể được sử dụng để đảm bảo bảo mật truyền thông báo hiệu (tức là, điều khiển) ở lớp PDCP 310.

Khi suy ra các khoá bảo mật này, được sử dụng cho thuật toán lập mã và thuật toán toàn vẹn, cả AS (User plane và RRC) và NAS đều cần mã nhận dạng thuật toán riêng được cung cấp dưới dạng một trong số các đầu vào. Ở mức AS, các thuật toán sẽ dùng được cung cấp bởi lệnh chế độ bảo mật điều khiển tài nguyên vô tuyến (RRC).

Fig.4 là sơ đồ khối minh họa hệ thống mạng, trong đó các khoá bảo mật khác nhau được minh họa trên Fig.2 và Fig.3 có thể được tạo ra. Ở đây, đầu cuối truy nhập 402 có thể cài đặt ngăn xếp truyền thông gồm nhiều lớp khác nhau (ví dụ, APP, NAS, RRC, RLC, MAC, và PHY). Mạng truy nhập 404 có thể cung cấp kết nối không dây cho đầu cuối truy nhập 402 để nó có thể truyền thông với mạng. Trung tâm xác thực (AuC) 406 và đầu cuối truy nhập 402 có thể đều biết hoặc truy nhập được khoá gốc (K) có thể dùng để tạo ra hoặc thu được khoá mật mã (CK) và/hoặc khoá toàn vẹn (IK). Tiếp đó, đầu cuối truy nhập 402 và/hoặc thanh ghi vị trí gốc (HLR) 408 có thể sử dụng khoá mật mã (CK) và/hoặc khoá toàn vẹn (IK) để tạo ra khoá thực thể quản lý bảo mật truy nhập K_ASME. Nhờ sử dụng khoá K_ASME,

đầu cuối truy nhập 402 và thực thể quản lý di động (MME) 410 có thể tạo ra các khoá K_NAS-enc và K_NAS-int. Đầu cuối truy nhập 402 và MME 410 cũng có thể tạo ra khoá riêng của mạng truy nhập K_eNB/NH. Khi sử dụng khoá riêng của mạng truy nhập K_eNB/NH này, đầu cuối truy nhập 402 và mạng truy nhập 404 có thể tạo ra các khoá K_UP-enc và K_RRC-enc và K_RRC-int.

Chi tiết về quá trình suy ra các khoá này được cung cấp trong tài liệu có tên là 3GPP STD-T63-33.401 "System Architecture Evolution (SAE): Security Architecture" (được gọi là 3GPP TS 33.401) Release 8.

Quay trở lại Fig.1, đầu cuối truy nhập 102 thường được làm thích ứng để thay đổi giữa các ô (ví dụ, các nút truy nhập 112) mà nó kết nối thực. Ví dụ, khi đầu cuối truy nhập 102 đi qua một vùng địa lý, các ô khác (ví dụ, các nút truy nhập 112) có thể cung cấp kết nối tốt hơn (ví dụ, tín hiệu mạnh hơn). Do đó đầu cuối truy nhập 102 có thể chuyển từ một ô (ví dụ, nút truy nhập 112) sang ô khác (ví dụ, nút truy nhập 112). Trong các mạng thông thường, sự di chuyển như vậy của đầu cuối truy nhập 102 đòi hỏi thay đổi từ một ô (ví dụ, nút truy nhập 112) sang ô khác (ví dụ, nút truy nhập 112) có thể dẫn đến việc huỷ bỏ cập nhật các tham số bảo mật đang diễn ra bất kỳ (ví dụ, cập nhật ở các tham số bảo mật tầng truy nhập K_UP-enc, K_RRC-enc và/hoặc K_RRC-int). Ví dụ, do sự di chuyển của đầu cuối truy nhập 102, thủ tục di động có thể được khởi tạo, dẫn đến việc huỷ bỏ thủ tục chế độ bảo mật đang diễn ra. Ví dụ và không nhằm mục đích giới hạn phạm vi, thủ tục di động có thể bao gồm các vấn đề chọn lại ô, lỗi không thể khôi phục điều khiển liên kết vô tuyến (RLC), mất dịch vụ, v.v.. Do vậy, một số ví dụ không giới hạn phạm vi về các thông báo cập nhật di động có thể truyền trong thủ tục di động có thể bao gồm thông báo chọn lại ô, thông báo lỗi không thể khôi phục điều khiển liên kết vô tuyến (RLC), thông báo mất dịch vụ, v.v..

Trong trường hợp thủ tục chế độ bảo mật đang diễn ra bị huỷ bỏ, có khả năng là các tham số bảo mật được cập nhật ở mạng truy nhập 104, nhưng không được cập nhật ở đầu cuối truy nhập 102, như sẽ được mô tả chi tiết hơn dưới đây. Kết quả là các tham số bảo mật được cập nhật ở mạng truy nhập 104 nhưng không được cập nhật ở đầu cuối truy nhập 102, lỗi giải mã thông báo/dữ liệu cố định và mất kết nối giữa đầu cuối truy nhập 102 và mạng truy nhập 104 có thể xảy ra (dẫn đến các cuộc gọi bị rơi chẳng hạn).

Theo một dấu hiệu, khi đầu cuối truy nhập 102 khởi đầu thủ tục di động (ví dụ, chọn lại nút truy nhập 112) sau khi mạng truy nhập 104 đã cập nhật ở các tham số bảo mật mới, đầu cuối truy nhập 102 có thể được làm thích ứng để truyền chỉ báo đến mạng truy nhập 104 báo cho mạng truy nhập 104 biết rằng đầu cuối truy nhập 102 đã quay trở lại các tham số bảo mật cũ. Ví dụ, đầu cuối truy nhập 102 có thể gộp chỉ báo với thông báo cập nhật di động truyền đến mạng truy nhập 104.

Theo dấu hiệu khác, mạng truy nhập 104 có thể được làm thích ứng để chuyển mạch quay trở lại các tham số bảo mật cũ khi đầu cuối truy nhập 102 không đáp lại thông báo xác nhận cập nhật di động được mã hoá theo các tham số bảo mật mới từ mạng truy nhập 104. Tức là, sau khi mạng truy nhập 104 đã truyền thông báo xác nhận cập nhật di động đến đầu cuối truy nhập 102 một số lần cụ thể mà không thu được thông báo đáp từ đầu cuối truy nhập 102, mạng truy nhập 104 có thể quay trở lại các tham số bảo mật cũ và truyền thông báo xác nhận cập nhật di động được mã hoá theo các tham số bảo mật cũ. Nếu đầu cuối truy nhập 102 đáp lại thông báo xác nhận cập nhật di động được mã hoá theo các tham số bảo mật cũ, thì mạng truy nhập 104 biết rằng việc cập nhật các tham số bảo mật không thành công và mạng truy nhập 104 tiếp tục sử dụng các tham số bảo mật cũ.

Theo dấu hiệu khác, mạng truy nhập 104 có thể được làm thích ứng để cập nhật các tham số bảo mật chỉ sau khi thu được thông báo báo nhận bổ sung từ đầu cuối truy nhập 102. Tức là, sau khi thông báo xác nhận cập nhật di động được truyền từ mạng truy nhập 104 đến đầu cuối truy nhập 102, mạng truy nhập 104 có thể đợi thông báo báo nhận khác từ đầu cuối truy nhập 102 trước khi mạng truy nhập 104 cập nhật các tham số bảo mật. Theo cách này, nếu đầu cuối truy nhập 102 đã huỷ bỏ việc cập nhật các tham số bảo mật, thì mạng truy nhập 104 sẽ không vô tình cập nhật các tham số bảo mật của nó sớm.

Theo dấu hiệu khác nữa, đầu cuối truy nhập 102 có thể được làm thích ứng để nhận dạng thất bại của nó trong việc giải mã thông báo xác nhận cập nhật di động từ mạng truy nhập 104 sau khi nó truyền một số lần cụ thể. Nếu đầu cuối truy nhập 102 không thể giải mã thông báo sau một số lần cụ thể, thì đầu cuối truy nhập 102 có thể được làm thích ứng để chuyển mạch sang các tham số bảo mật mới và thử giải mã thông báo xác nhận cập nhật di động bằng cách sử dụng các tham số mới. Nếu đầu cuối truy nhập 102 thành công trong việc giải mã thông báo xác nhận cập nhật di

động bằng cách sử dụng các tham số mới, thì từ thời điểm này đầu cuối truy nhập 102 có thể tiếp tục chuyển sang sử dụng các tham số bảo mật mới khi truyền thông với mạng truy nhập 104.

Các thủ tục để đồng bộ hoá các tham số bảo mật giữa các đầu cuối truy nhập và các mạng truy nhập làm ví dụ

Fig.5 (bao gồm Fig.5A và Fig.5B) là lưu đồ minh họa một ví dụ về thao tác đồng bộ hoá tham số bảo mật bởi mạng truy nhập khi các tham số bảo mật của mạng truy nhập được cập nhật và các tham số bảo mật của đầu cuối truy nhập không được cập nhật. Mặc dù, ví dụ được minh họa trên Fig.5, cũng như các ví dụ trên các hình vẽ từ Fig.6 đến Fig.8, hướng đến các ứng dụng liên quan đến thủ tục chế độ bảo mật tầng truy nhập (AS) để khởi tạo và cập nhật các tham số bảo mật tầng truy nhập, nhưng các dấu hiệu được mô tả ở đây có thể được thực hiện trong các thủ tục chế độ bảo mật khác, như các thủ tục chế độ bảo mật tầng không truy nhập (NAS). Đầu cuối truy nhập 102, mạng truy nhập 104 và mạng lõi 106 trên Fig.1 được sử dụng cho mục đích minh họa.

Trước tiên, đầu cuối truy nhập 102 có thể thiết lập kết nối điều khiển tài nguyên vô tuyến (RRC) 502 với mạng truy nhập 104. Thông báo truyền từ đầu cuối truy nhập 102 đến mạng truy nhập 104 khi kết nối điều khiển tài nguyên vô tuyến (RRC) được thiết lập có thể chứa thông tin khả năng bảo mật của đầu cuối truy nhập. Thông tin khả năng bảo mật của đầu cuối truy nhập được làm thích ứng để báo cho mạng truy nhập 104 biết về các thuật toán lập mã (hoặc mã hoá) và các thuật toán toàn vẹn được hỗ trợ bởi đầu cuối truy nhập 102. Thông tin khả năng bảo mật còn có thể tuỳ ý bao gồm thông báo dấu hiệu hạng chỉ báo các thuật toán bảo mật GSM được hỗ trợ bởi đầu cuối truy nhập 102 (ví dụ, các dấu hiệu hạng GSM 2 và 3) và/hoặc các giá trị START cho miền dịch vụ chuyển mạch và miền dịch vụ chuyển gói. Thông tin từ thông báo thiết lập kết nối điều khiển tài nguyên vô tuyến (RRC) có thể được lưu trữ 504 trong mạng truy nhập 104.

Tiếp đó, đầu cuối truy nhập 102 có thể truyền thông báo chuyển tải trực tiếp mở đầu 506 đến mạng lõi 106. Thông báo chuyển tải trực tiếp mở đầu 506 có thể bao gồm, ngoài các thông tin khác, thông tin nhận dạng người dùng và ký hiệu nhận dạng bộ khoá (KSI - Key Set Identifier) được cấp phát bởi miền dịch vụ chuyển mạch hoặc miền dịch vụ chuyển gói tại bước xác thực sau cùng đối với mạng lõi 106

này. Theo ít nhất một ứng dụng, thông báo chuyển tải trực tiếp mở đầu có thể bao gồm thông báo lớp 3 (L3 - layer 3), như yêu cầu cập nhật vị trí, yêu cầu dịch vụ CM, yêu cầu cập nhật vùng định tuyến, yêu cầu gắn kết, thông báo đáp nhắn tin hoặc thông báo L3 khác. Thông báo chuyển tải trực tiếp mở đầu có thể được truyền, ví dụ, đến thanh ghi vị trí khách (VLR) đối với miền dịch vụ chuyển mạch của mạng lõi 106 hoặc nút hỗ trợ GPRS (SGSN) đối với miền dịch vụ chuyển gói của mạng lõi 106.

Việc xác thực đầu cuối truy nhập 102 và tạo ra các khoá bảo mật mới (ví dụ, khoá toàn vẹn (IK), khoá mật mã (CK)) có thể được thực hiện giữa đầu cuối truy nhập 102 và mạng lõi 106 bằng cách sử dụng thủ tục xác thực và thoả thuận khoá (AKA) 508. Trong thủ tục xác thực và thoả thuận khoá 508, ký hiệu nhận dạng bộ khóa mới (KSI) có thể tuỳ ý được cấp phát.

Sau thủ tục xác thực và thoả thuận khoá, các khoá bảo mật mới (ví dụ, khoá toàn vẹn (IK) và khoá mật mã (CK) có thể được sử dụng để tính các khóa tầng truy nhập (AS). Ví dụ, mạng lõi 106 có thể quyết định thuật toán lập mã và thuật toán toàn vẹn sẽ được sử dụng theo thứ tự ưu tiên ở 510. Mạng lõi 106 có thể truyền thông báo lệnh chế độ bảo mật tầng truy nhập (AS) 512 đến mạng truy nhập 104. Thông báo lệnh chế độ bảo mật tầng truy nhập (AS) 512 có thể được truyền theo giao thức phần ứng dụng mạng truy nhập vô tuyến (RANAP - Radio Access Network Application Part), và có thể được chuyển đến bộ điều khiển mạng vô tuyến (RNC) của mạng truy nhập 104. Thông báo lệnh chế độ bảo mật 512 này có thể bao gồm danh mục các thuật toán toàn vẹn được phép theo thứ tự ưu tiên, và khoá toàn vẹn (IK) sẽ được sử dụng. Nếu thủ tục lập mã cần được khởi tạo, thì thông báo lệnh chế độ bảo mật 512 còn có thể chứa danh mục các thuật toán lập mã được phép theo thứ tự ưu tiên, và khoá mật mã (CK) sẽ được sử dụng. Nếu thủ tục xác thực và thoả thuận khoá (AKA) được thực hiện, thì điều này sẽ được chỉ báo cho mạng truy nhập 104 để cho các giá trị START sẽ được thiết lập lại khi các khoá mới được khởi tạo để sử dụng.

Mạng truy nhập 104 (ví dụ, bộ điều khiển mạng vô tuyến (RNC)) quyết định những thuật toán nào (ví dụ, thuật toán toàn vẹn, thuật toán lập mã) cần sử dụng, tạo lập giá trị ngẫu nhiên RAND, và bắt đầu bảo vệ tính toàn vẹn ở bước 514. Tiếp đó, mạng truy nhập 104 có thể tạo ra thông báo điều khiển tài nguyên vô tuyến (RRC)

516 bao gồm thông báo lệnh chế độ bảo mật tầng truy nhập (AS), và truyền thông báo đến đầu cuối truy nhập 102. Thông báo lệnh chế độ bảo mật AS 516 có thể chứa thông tin khả năng bảo mật của đầu cuối truy nhập 102, thuật toán toàn vẹn và giá trị ngẫu nhiên RAND cần được sử dụng. Nếu thủ tục lập mã được khởi động, thì thông báo 516 còn có thể bao gồm thuật toán lập mã cần được sử dụng. Thông tin khác cũng có thể có. Vì đầu cuối truy nhập 102 có thể có hai bộ khoá mật mã và khoá toàn vẹn, nên mạng có thể chỉ báo bộ khoá nào sẽ được sử dụng. Trước khi truyền thông báo lệnh chế độ bảo mật AS 516 đến đầu cuối truy nhập 102, mạng truy nhập 104 tạo ra mã xác thực thông báo về tính toàn vẹn (MAC-I Message Authentication Code for Integrity) và gắn kèm thông tin này vào thông báo lệnh chế độ bảo mật AS 516.

Theo Fig.5B, đầu cuối truy nhập 102 thu thông báo lệnh chế độ bảo mật AS, xác minh rằng khả năng bảo mật giống như khả năng được truyền trong thông báo thiết lập kết nối điều khiển tài nguyên vô tuyến (RRC) và xác minh thông báo này bằng cách so sánh MAC-I với XMAC-I được tạo ra ở bước 518. Đầu cuối truy nhập 102 có thể tính XMAC-I trong thông báo thu được bằng cách sử dụng ít nhất là thuật toán toàn vẹn đã được chỉ báo và tham số giá trị ngẫu nhiên RAND thu được. Nếu tất cả các bước kiểm tra đều thành công, thì đầu cuối truy nhập 102 truyền thông báo hoàn thành chế độ bảo mật tầng truy nhập (AS) 520 có chứa MAC-I. Nếu các bước kiểm tra không thành công thì thông báo từ chối chế độ bảo mật sẽ được truyền đi.

Khi thu được thông báo hoàn thành chế độ bảo mật AS, mạng truy nhập 104 xác minh tính toàn vẹn của thông báo này bằng cách tạo ra XMAC-I và so sánh nó với MAC-I chứa trong thông báo hoàn thành chế độ bảo mật AS 522. Thông báo hoàn thành chế độ bảo mật AS 524 được truyền từ mạng truy nhập 104 đến mạng lõi 106 dưới dạng thông báo phần ứng dụng mạng truy nhập vô tuyến (RANAP) chỉ báo các thuật toán được chọn cho tính toàn vẹn và lập mã. Thông báo báo nhận 526 được truyền từ mạng truy nhập 104 đến đầu cuối truy nhập 102 để báo nhận thu được thông báo hoàn thành chế độ bảo mật AS. Theo ít nhất một số ứng dụng, thông báo báo nhận 526 có thể là báo nhận L2.

Thông báo hoàn thành chế độ bảo mật AS (ví dụ, 520) từ đầu cuối truy nhập 102 đến mạng truy nhập 104 khởi động thủ tục bảo vệ toàn vẹn liên kết xuống, tức là, các thông báo liên kết xuống tiếp theo truyền đến đầu cuối truy nhập 102 được bảo vệ toàn vẹn bằng cách sử dụng các tham số bảo mật mới. Tuy nhiên, việc bảo vệ

toàn vẹn liên kết lên không khởi đầu cho đến khi đầu cuối truy nhập 102 thu được thông báo báo nhận ở bước 526 từ mạng truy nhập 104, sau đó đầu cuối truy nhập 102 cập nhật các tham số bảo mật của nó ở bước 528. Nói cách khác, đầu cuối truy nhập 102 sẽ không sử dụng các tham số bảo mật tầng truy nhập (AS) mới cho các thông báo truyền từ đầu cuối truy nhập 102 đến mạng truy nhập 104 cho đến khi đầu cuối truy nhập 102 thu được từ mạng truy nhập 104 thông tin báo nhận là thông báo hoàn thành chế độ bảo mật tầng truy nhập (AS) đã được thu và xác thực.

Có một cửa sổ thời gian nhỏ giữa thời điểm mà thủ tục chế độ bảo mật tầng truy nhập (AS) được hoàn thành ở mạng truy nhập 104 (ví dụ, khi thông báo hoàn thành chế độ bảo mật tầng truy nhập (AS) 520 thu được ở mạng truy nhập 104) và thời điểm mà thủ tục chế độ bảo mật AS được hoàn thành ở đầu cuối truy nhập 102 (ví dụ, khi thông báo báo nhận 526 thu được bởi đầu cuối truy nhập 102 và các tham số bảo mật tầng truy nhập (AS) được cập nhật ở bước 528). Vì cửa sổ thời gian này, nên có thể để cho mạng truy nhập 104 cập nhật ở các tham số bảo mật tầng truy nhập (AS) mới, trong khi đầu cuối truy nhập 102 vẫn giữ nguyên ở các tham số bảo mật tầng truy nhập (AS) cũ.

Ví dụ, đầu cuối truy nhập 102 thường được làm thích ứng để huỷ bỏ thủ tục chế độ bảo mật tầng truy nhập (AS) khi thủ tục di động được khởi tạo, như khi thông báo cập nhật di động được truyền từ đầu cuối truy nhập 102 đến mạng truy nhập 104. Do đó, đầu cuối truy nhập 102 có thể khởi đầu thủ tục di động, bao gồm tạo ra và truyền thông báo cập nhật di động 530 sau khi thông báo hoàn thành chế độ bảo mật tầng truy nhập (AS) 520 được truyền đến mạng truy nhập 104, và trước khi thu được báo nhận 526 và/hoặc cập nhật cho đầu cuối truy nhập các tham số bảo mật. Do thủ tục di động được khởi tạo, nên đầu cuối truy nhập 102 huỷ bỏ thủ tục chế độ bảo mật và quay trở lại các tham số bảo mật tầng truy nhập (AS) cũ 528. Đầu cuối truy nhập 102 có thể thu được báo nhận 526 sau khi thủ tục di động được khởi tạo, nhưng đầu cuối truy nhập 102 đã huỷ bỏ thủ tục chế độ bảo mật tầng truy nhập (AS) và do đó, không được cập nhật ở các tham số bảo mật tầng truy nhập (AS) mới, không được biết ở mạng truy nhập 104.

Theo ứng dụng được thể hiện trên Fig.5B, thông báo cập nhật di động 530 chứa chỉ báo để báo cho mạng truy nhập 104 biết rằng đầu cuối truy nhập 102 đã huỷ bỏ thủ tục chế độ bảo mật AS và quay trở lại các tham số bảo mật AS cũ. Theo ít

nhất một số ứng dụng, chỉ báo có thể bao gồm phần tử thông tin (IE - Information Element) mới trong thông báo cập nhật di động. Theo một số ứng dụng, chỉ báo có thể bao gồm một hoặc nhiều bit của thông báo cập nhật di động.

Ngay khi thu được thông báo cập nhật di động có chứa chỉ báo, mạng truy nhập 104 quay trở lại các tham số bảo mật tầng truy nhập (AS) cũ 532. Mạng truy nhập 104 có thể tạo ra và truyền đến đầu cuối truy nhập 102 thông báo xác nhận cập nhật di động 534 được lập mã bằng cách sử dụng các tham số bảo mật AS cũ.

Theo dấu hiệu khác, đầu cuối truy nhập 102 có thể được làm thích ứng để điều chỉnh các tham số bảo mật mới khi đầu cuối truy nhập 102 coi là mạng truy nhập 104 đang vận hành với các tham số bảo mật mới trong khi đầu cuối truy nhập 102 vận hành với các tham số bảo mật cũ. Fig.6 là lưu đồ minh họa ví dụ về thao tác đồng bộ hoá tham số bảo mật bởi đầu cuối truy nhập khi các tham số bảo mật ở mạng truy nhập được cập nhật và các tham số bảo mật ở đầu cuối truy nhập không được cập nhật. Các bước được thể hiện trên Fig.6 tương ứng với các bước tiếp theo tất cả các bước được mô tả và thể hiện trên Fig.5A. Tức là, Fig.6 dự định thể hiện các bước tiếp theo sau khi các bước trên Fig.5A hoàn tất.

Như nêu trên đối với Fig.5B, khi nhận thông báo lệnh chế độ bảo mật tầng truy nhập (AS), đầu cuối truy nhập 102 xác minh khả năng bảo mật là giống như khả năng bảo mật được truyền trong thông báo thiết lập kết nối điều khiển tài nguyên vô tuyến (RRC), tính toán XMAC-I và xác minh tính toàn vẹn của thông báo lệnh chế độ bảo mật AS bằng cách so sánh MAC-I thu được với XMAC-I được tạo ra 602. Nếu tất cả các bước kiểm tra đều thành công, thì đầu cuối truy nhập 102 truyền thông báo hoàn thành chế độ bảo mật tầng truy nhập (AS) 604 có chứa MAC-I. Nếu kiểm tra không thành công thì thông báo từ chối chế độ bảo mật tầng truy nhập (AS) có thể được truyền. Khi thu được thông báo hoàn thành chế độ bảo mật AS, mạng truy nhập 104 xác minh tính toàn vẹn của thông báo này ở bước 606, và truyền thông báo hoàn thành chế độ bảo mật AS 608 đến mạng lõi 106 chỉ báo các thuật toán mã hoá và toàn vẹn đã được chọn.

Như nêu trên, trong một số trường hợp, mạng truy nhập 104 có thể cập nhật ở các tham số bảo mật tầng truy nhập (AS) mới trong khi đầu cuối truy nhập 102 không cập nhật được ở các tham số bảo mật AS mới. Ví dụ, sau khi truyền thông báo hoàn thành chế độ bảo mật AS 604 đến mạng truy nhập 104, và trước khi thu báo

nhận và/hoặc cập nhật các tham số bảo mật tầng truy nhập (AS), đầu cuối truy nhập 102 có thể khởi đầu thủ tục di động trong đó đầu cuối truy nhập 102 tạo ra và truyền thông báo cập nhật di động 610 đến mạng truy nhập 104. Đáp lại việc khởi đầu thủ tục di động, đầu cuối truy nhập 102 huỷ bỏ thủ tục chế độ bảo mật và quay trở lại các tham số bảo mật tầng truy nhập (AS) cũ 612. Đầu cuối truy nhập 102 có thể thu thông báo báo nhận 614 sau khi khởi đầu thủ tục di động, nhưng đầu cuối truy nhập 102 đã huỷ bỏ thủ tục chế độ bảo mật tầng truy nhập (AS) và do đó, không cập nhật ở các tham số bảo mật tầng truy nhập (AS) mới, không được biết đến ở mạng truy nhập 104.

Trong những trường hợp như vậy, thông báo cập nhật di động được truyền ở bước 610 thường không được mã hoá, dẫn đến mạng truy nhập 104 có thể thu và xử lý thông báo cập nhật di động ngay cả khi đầu cuối truy nhập 102 đang vận hành với các tham số bảo mật tầng truy nhập (AS) cũ. Trong ứng dụng được thể hiện trên Fig.6, mạng truy nhập 104 thu thông báo cập nhật di động 610 và đáp lại bằng thông tin xác nhận cập nhật di động 616 được lập mã với các tham số bảo mật AS mới, và do đó không thể giải mã được ở đầu cuối truy nhập 102 đang sử dụng các tham số bảo mật AS cũ. Khi mạng truy nhập 104 không thu được thông báo đáp lại thông báo xác nhận cập nhật di động, mạng truy nhập 104 truyền lại thông tin xác nhận cập nhật di động. Đầu cuối truy nhập 102 có thể được làm thích ứng để theo dõi số lần nó thu và không giải mã được thông báo xác nhận cập nhật di động. Sau một số lần thử định trước (N), đầu cuối truy nhập 102 có thể chuyển sang các tham số bảo mật AS mới 618. Sau khi chuyển sang các tham số bảo mật AS mới, đầu cuối truy nhập 102 có thể thử giải mã thông báo xác nhận cập nhật di động bằng cách sử dụng các tham số bảo mật AS mới. Nếu thành công, thì đầu cuối truy nhập 102 sẽ tiếp tục sử dụng các tham số bảo mật AS mới từ thời điểm này trở đi.

Theo dấu hiệu khác, mạng truy nhập 104 có thể được làm thích ứng để hoàn thành thủ tục chế độ bảo mật và cập nhật các tham số bảo mật của nó chỉ sau khi thu được thông báo báo nhận cuối cùng từ đầu cuối truy nhập 102. Fig.7 là lưu đồ minh họa ví dụ về thao tác đồng bộ hoá tham số bảo mật của đầu cuối truy nhập 102, mạng truy nhập 104 và mạng lõi 106 để tạo điều kiện thuận lợi cho việc cập nhật các tham số bảo mật ở mạng truy nhập 104 chỉ sau khi các tham số bảo mật được cập nhật ở đầu cuối truy nhập 102. Các bước được thể hiện trên Fig.7 tương ứng với các bước

tiếp theo tất cả các bước được mô tả và thể hiện trên Fig.5A. Tức là, Fig.7 dự định thể hiện các bước tiếp theo các bước trên Fig.5A hoàn tất.

Như nêu trên đối với Fig.5B, khi thu được thông báo lệnh chế độ bảo mật tầng truy nhập (AS), đầu cuối truy nhập 102 xác minh khả năng bảo mật có giống như khả năng bảo mật được truyền trong thông báo thiết lập kết nối điều khiển tài nguyên vô tuyến (RRC) hay không, tính toán XMAC-I và xác minh tính toàn vẹn của thông báo bằng cách so sánh MAC-I thu được với XMAC-I được tạo ra 702. Nếu tất cả các bước kiểm tra thành công, thì đầu cuối truy nhập 102 truyền thông báo hoàn thành chế độ bảo mật tầng truy nhập (AS) 704 có chứa MAC-I. Nếu các bước kiểm tra không thành công thì thông báo từ chối chế độ bảo mật AS có thể được truyền. Khi thu được thông báo hoàn thành chế độ bảo mật AS, mạng truy nhập 104 xác minh tính toàn vẹn của thông báo ở bước 706, và truyền thông báo hoàn thành chế độ bảo mật AS 708 đến mạng lõi 106 chỉ báo các thuật toán mã hoá và toàn vẹn đã được chọn.

Trong ứng dụng được thể hiện trên Fig.7, mạng truy nhập 104 không hoàn thành thủ tục chế độ bảo mật AS ngay khi thu và xác minh thông báo hoàn thành chế độ bảo mật AS. Tức là, mạng truy nhập 104 được làm thích ứng để không cập nhật các tham số bảo mật AS mới ngay khi thu và xác minh thông báo hoàn thành chế độ bảo mật AS 704. Thay vì vậy, mạng truy nhập 104 gửi thông báo báo nhận 710 đến đầu cuối truy nhập 102. Thông báo báo nhận 710 có thể là thông báo báo nhận L2. Đáp lại việc thu được thông báo báo nhận 710, đầu cuối truy nhập 102 cập nhật các tham số bảo mật AS mới 712. Đầu cuối truy nhập 102 có thể gửi thông báo báo nhận 714 đến mạng truy nhập 104. Ví dụ, đầu cuối truy nhập 102 có thể truyền thông báo báo nhận L3 đến mạng truy nhập 104 để chỉ báo rằng nó đã cập nhật các tham số bảo mật AS mới. Tiếp đó, mạng truy nhập 104 cập nhật các tham số bảo mật AS mới 716 đáp lại việc thu được thông báo báo nhận 714 từ đầu cuối truy nhập 102.

Theo ứng dụng trên Fig.7, nếu đầu cuối truy nhập 102 huỷ bỏ thủ tục chế độ bảo mật tầng truy nhập (AS) (khởi đầu thủ tục di động chẳng hạn) sau khi truyền thông báo hoàn thành chế độ bảo mật AS 704 đến mạng truy nhập 104, nhưng trước khi cập nhật các tham số bảo mật mới, thì mạng truy nhập 104 sẽ không thu được thông báo báo nhận 714 và sẽ không cập nhật các tham số bảo mật AS mới. Nói cách khác, nếu đầu cuối truy nhập 102 huỷ bỏ thủ tục chế độ bảo mật AS trước khi hoàn

thành thủ tục này (ví dụ, trước khi cập nhật các tham số bảo mật AS mới), thì thông báo báo nhận 714 sẽ không được truyền và mạng truy nhập 104 sẽ không được cập nhật các tham số bảo mật AS mới.

Theo dấu hiệu khác, mạng truy nhập 104 có thể được làm thích ứng để quay trở lại các tham số bảo mật cũ khi mạng truy nhập 104 coi là đầu cuối truy nhập 102 đang vận hành với các tham số bảo mật cũ trong khi mạng truy nhập 104 đang vận hành với các tham số bảo mật mới. Fig.8 là lưu đồ minh họa ví dụ về thao tác đồng bộ hoá tham số bảo mật của mạng truy nhập khi các tham số bảo mật của mạng truy nhập được cập nhật và các tham số bảo mật của đầu cuối truy nhập không được cập nhật. Các bước được thể hiện trên Fig.8 tương ứng với các bước tiếp theo tất cả các bước được mô tả và thể hiện trên Fig.5A. Tức là, Fig.8 dự định thể hiện các bước tiếp theo sau khi các bước trên Fig.5A hoàn tất.

Như nêu trên đối với Fig.5B, khi thu được thông báo lệnh chế độ bảo mật tầng truy nhập (AS), đầu cuối truy nhập 102 xác minh khả năng bảo mật có giống khả năng bảo mật được truyền trong thông báo thiết lập kết nối RRC hay không, tính toán XMAC-I, và xác minh tính toàn vẹn của thông báo lệnh chế độ bảo mật AS bằng cách so sánh MAC-I thu được với XMAC-I được tạo ra 802. Nếu tất cả các bước kiểm tra thành công, thì đầu cuối truy nhập 102 truyền thông báo hoàn thành chế độ bảo mật tầng truy nhập (AS) 804 chứa MAC-I. Nếu các bước kiểm tra không thành công thì thông báo từ chối chế độ bảo mật AS có thể được truyền. Khi thu được thông báo hoàn thành chế độ bảo mật AS 804 này, mạng truy nhập 104 xác minh tính toàn vẹn của thông báo 806, và truyền thông báo hoàn thành chế độ bảo mật AS 808 đến mạng lõi 106 chỉ báo các thuật toán mã hoá và toàn vẹn đã được chọn.

Như nêu trên, trong một số trường hợp, mạng truy nhập 104 có thể cập nhật các tham số bảo mật AS mới trong khi đầu cuối truy nhập 102 không cập nhật được các tham số bảo mật AS mới. Ví dụ, sau khi truyền thông báo hoàn thành chế độ bảo mật AS 804 đến mạng truy nhập 104, và trước khi thu được thông báo báo nhận và/hoặc cập nhật đầu cuối truy nhập ở các tham số bảo mật AS mới, đầu cuối truy nhập 102 có thể khởi đầu thủ tục di động, bao gồm tạo ra và truyền thông báo cập nhật di động 810. Do khởi đầu thủ tục di động, đầu cuối truy nhập 102 huỷ bỏ thủ tục chế độ bảo mật AS và quay trở lại các tham số bảo mật AS cũ 812. Đầu cuối truy

nhập 102 có thể thu thông báo báo nhận 814 sau khi khởi đầu thủ tục di động, nhưng đầu cuối truy nhập 102 đã huỷ bỏ thủ tục chế độ bảo mật AS, và do đó sẽ không cập nhật các tham số bảo mật AS mới, không được biết đến ở mạng truy nhập 104.

Trong những trường hợp như vậy, thông báo cập nhật di động 810 thường không được mã hoá, để cho mạng truy nhập 104 có thể thu và xử lý thông báo cập nhật di động 810 ngay cả khi đầu cuối truy nhập 102 đang vận hành với các tham số bảo mật AS cũ. Tuy nhiên, khi mạng truy nhập 104 truyền thông báo xác nhận cập nhật di động 816, thì thông báo 816 được lập mã với các tham số bảo mật AS mới, và do đó không thể giải mã được ở đầu cuối truy nhập 102.

Trong ứng dụng được thể hiện trên Fig.8, mạng truy nhập 104 có thể được làm thích ứng để truyền thông báo xác nhận cập nhật di động 816 một hoặc nhiều lần. Sau khi mạng truy nhập 104 đã truyền thông báo đến đầu cuối truy nhập 102 một số lần định trước mà không thu được thông báo đáp từ đầu cuối truy nhập 102, mạng truy nhập có thể được làm thích ứng để quay trở lại các tham số bảo mật AS cũ 518 và truyền lại thông báo xác nhận cập nhật di động 820 bằng cách sử dụng các tham số bảo mật AS cũ. Nếu mạng truy nhập 104 thu thông báo đáp lại thông báo xác nhận cập nhật di động được truyền bằng cách sử dụng các tham số bảo mật AS cũ, thì mạng truy nhập 104 có thể tiếp tục sử dụng các tham số bảo mật AS cũ.

Đầu cuối truy nhập làm ví dụ

Fig.9 là sơ đồ khối minh họa các thành phần chọn lọc của đầu cuối truy nhập 900 theo ít nhất một phương án. Đầu cuối truy nhập 900 thường bao gồm mạch xử lý 902 ghép nối với phương tiện nhớ 904 và giao diện truyền thông không dây 906.

Mạch xử lý 902 được bố trí để tiếp nhận, xử lý và/hoặc truyền dữ liệu, điều khiển truy nhập và lưu trữ dữ liệu, đưa ra các lệnh, và điều khiển các thao tác cần thiết khác. Mạch xử lý 902 có thể bao gồm mạch được tạo cấu hình để thực thi chương trình cần thiết được cung cấp bởi phương tiện thích hợp theo ít nhất một phương án. Ví dụ, mạch xử lý 902 có thể được thực hiện dưới dạng một hoặc nhiều bộ xử lý, bộ điều khiển, nhiều bộ xử lý và/hoặc cấu trúc khác được tạo cấu hình để thi hành các lệnh khả thi trong đó, ví dụ, các lệnh phần mềm và/hoặc phần sụn, và/hoặc mạch phần cứng. Các phương án của mạch xử lý 902 có thể bao gồm bộ xử lý đa năng, bộ xử lý tín hiệu số (DSP - Digital Signal Processor), mạch tích hợp chuyên dụng (ASIC - Application Specific Integrated Circuit), mảng cửa lập trình

được bằng trường (FPGA - Field Programmable Gate Array) hoặc thành phần logic lập trình được khác, mạng cửa rời rạc hoặc mạch logic tranzito, các thành phần phần cứng rời rạc hoặc tổ hợp bất kỳ của chúng được thiết kế để thực hiện các chức năng được mô tả ở đây. Bộ xử lý đa năng có thể là bộ vi xử lý, nhưng theo cách khác, bộ xử lý có thể là bộ xử lý thông thường, bộ điều khiển, bộ vi điều khiển hoặc máy trạng thái bất kỳ. Bộ xử lý còn có thể được thực hiện dưới dạng tổ hợp của các thiết bị tính toán, ví dụ, tổ hợp của DSP và bộ vi xử lý, các bộ vi xử lý, một hoặc nhiều bộ vi xử lý phối hợp với lõi DSP, hoặc cấu hình tương tự bất kỳ khác. Các ví dụ như vậy về mạch xử lý 902 chỉ để minh họa và cấu hình thích hợp khác trong phạm vi của sáng chế cũng được dự tính.

Mạch xử lý 902 có thể bao gồm môđun chỉ báo và/hoặc xác định các tham số bảo mật 908. Môđun chỉ báo và/hoặc xác định các tham số bảo mật 908 có thể bao gồm mạch và/hoặc chương trình được làm thích ứng để thực hiện các thủ tục chỉ báo các tham số bảo mật và/hoặc các thủ tục xác định các tham số bảo mật.

Phương tiện nhớ 904 có thể là một hoặc nhiều thiết bị lưu trữ chương trình và/hoặc dữ liệu, như các mã hoặc các lệnh khả thi của bộ xử lý (ví dụ, phần mềm, phần sụn), dữ liệu điện tử, cơ sở dữ liệu, hoặc thông tin số khác. Phương tiện nhớ 904 có thể là phương tiện khả dụng bất kỳ có thể được truy nhập bởi bộ xử lý đa năng hoặc chuyên dụng. Để làm ví dụ và không giới hạn phạm vi của sáng chế, phương tiện nhớ 904 có thể bao gồm bộ nhớ chỉ đọc (ví dụ, bộ nhớ chỉ đọc (ROM - Read Only Memory), bộ nhớ chỉ đọc lập trình được bằng điện (EPROM - Electrically Programmable ROM), bộ nhớ chỉ đọc lập trình được xóa được bằng điện (EEPROM - Electrically Erasable Programmable ROM)), bộ nhớ truy nhập ngẫu nhiên (RAM - Random Access Memory), phương tiện nhớ đĩa từ, phương tiện nhớ quang, thiết bị nhớ tác động nhanh, và/hoặc vật ghi đọc được bằng máy tính bền vững khác dùng để lưu trữ thông tin. Phương tiện nhớ 904 có thể ghép nối với mạch xử lý 902 sao cho mạch xử lý 902 có thể đọc thông tin từ, và ghi thông tin vào, phương tiện nhớ 904. Theo cách khác, phương tiện nhớ 904 có thể liền khối với mạch xử lý 902.

Phương tiện nhớ 904 có thể chứa các thao tác chỉ báo tham số bảo mật và/hoặc các thao tác xác định tham số bảo mật 910, theo một hoặc nhiều phương án. Các thao tác chỉ báo tham số bảo mật và/hoặc các thao tác xác định tham số bảo mật

910 có thể được thực hiện bởi mạch xử lý 902 trong, ví dụ, môđun chỉ báo và/hoặc xác định các tham số bảo mật 908. Trong một số ứng dụng, các thao tác chỉ báo tham số bảo mật có thể bao gồm các thao tác có thể được thực hiện bởi mạch xử lý 902 để chỉ báo trạng thái của các tham số bảo mật của đầu cuối truy nhập 900 cho mạng truy nhập, như bằng cách gộp thông tin chỉ báo trong thông báo cập nhật di động để đầu cuối truy nhập 900 quay trở lại các tham số bảo mật cũ và/hoặc truyền thông báo chỉ báo rằng đầu cuối truy nhập 900 đã cập nhật thành công các tham số bảo mật mới. Trong một số ứng dụng, các thao tác xác định tham số bảo mật có thể bao gồm các thao tác có thể được thực hiện bởi mạch xử lý 902 để xác định trạng thái của các tham số bảo mật tại mạng truy nhập để truyền thông với đầu cuối truy nhập 900, như xác định thất bại của nó đối với việc giải mã thông báo xác nhận cập nhật di động thu được từ mạng truy nhập.

Giao diện truyền thông 906 được tạo cấu hình để tạo điều kiện thuận lợi cho việc truyền thông không dây của đầu cuối truy nhập 900. Ví dụ, giao diện truyền thông 906 có thể được tạo cấu hình để truyền thông thông tin hai chiều với mạng truy nhập và/hoặc các đầu cuối truy nhập khác. Mạch truyền thông 906 có thể được ghép nối với anten (không được thể hiện) và có thể bao gồm mạch thu phát không dây, gồm ít nhất một bộ truyền 912 và/hoặc ít nhất một bộ thu 914 (ví dụ, một hoặc nhiều chuỗi bộ truyền/bộ thu).

Theo một hoặc nhiều dấu hiệu của đầu cuối truy nhập 900, mạch xử lý 902 có thể được làm thích ứng để thực hiện một số bất kỳ hoặc tất cả các quy trình, các chức năng, các bước và/hoặc các thường trình liên quan đến các đầu cuối truy nhập khác nhau được mô tả trên đây dựa vào các hình vẽ từ Fig.1 đến Fig.8 (ví dụ, đầu cuối truy nhập 102 và/hoặc 402). Như được sử dụng ở đây, thuật ngữ "được làm thích ứng" liên quan đến mạch xử lý 902 có thể được dùng để chỉ mạch xử lý 902 là một hoặc nhiều mạch xử lý được tạo cấu hình, sử dụng, thi hành hoặc lập trình để thực hiện quy trình, chức năng, bước và/hoặc thường trình cụ thể theo các dấu hiệu khác nhau được mô tả ở đây.

Fig.10 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở đầu cuối truy nhập, như đầu cuối truy nhập 900, để chỉ báo cho mạng truy nhập khi đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ. Theo cả Fig.9 và Fig.10, đầu cuối truy nhập 900 có thể điều khiển thủ tục chế độ bảo mật ở bước 1002. Ví dụ mạch xử

lý 902 có thể truyền thông với mạng truy nhập qua giao diện truyền thông 906 để điều khiển thủ tục chế độ bảo mật. Trong thủ tục chế độ bảo mật, mạch xử lý 902 có thể tạo ra và truyền thông báo hoàn thành chế độ bảo mật đến mạng truy nhập. Theo ít nhất một số ứng dụng, thủ tục chế độ bảo mật có thể bao gồm thủ tục chế độ bảo mật tầng truy nhập (AS), trong đó mạch xử lý 902 tạo ra và truyền thông báo hoàn thành chế độ bảo mật tầng truy nhập (AS). Mạch xử lý 902 có thể truyền thông báo hoàn thành chế độ bảo mật AS bằng cách sử dụng lớp điều khiển tài nguyên vô tuyến (RRC) của ngăn xếp giao thức để truyền thông với mạng truy nhập.

Ở bước 1004, sau khi đầu cuối truy nhập 900 truyền thông báo hoàn thành chế độ bảo mật đến mạng truy nhập, thủ tục di động có thể được khởi tạo trong khi thủ tục chế độ bảo mật vẫn hoạt động. Ví dụ, do sự di động của đầu cuối truy nhập 900, mạch xử lý 902 có thể khởi đầu thủ tục di động. Ví dụ về thủ tục di động có thể bao gồm chọn lại ô, lỗi không thể khôi phục điều khiển liên kết vô tuyến (RLC), đầu cuối truy nhập mất dịch vụ, v.v..

Đáp lại việc khởi đầu thủ tục di động trước khi cập nhật các tham số bảo mật của nó (ví dụ, trước khi thu báo nhận của thông báo hoàn thành chế độ bảo mật hoặc trước khi cập nhật đáp lại báo nhận), đầu cuối truy nhập 900 huỷ bỏ thủ tục chế độ bảo mật đang diễn ra và quay trở lại các tham số bảo mật cũ ở bước 1006. Ví dụ, mạch xử lý 902 có thể huỷ bỏ thủ tục chế độ bảo mật đang diễn ra và quay trở lại sử dụng các tham số bảo mật cũ (ví dụ, các tham số bảo mật tầng truy nhập (AS) cũ) đáp lại việc khởi đầu thủ tục di động.

Ở bước 1008, đầu cuối truy nhập 900 có thể tạo ra và truyền thông báo cập nhật di động đến mạng truy nhập. Thông báo cập nhật di động chứa chỉ báo được làm thích ứng để báo cho mạng truy nhập biết rằng đầu cuối truy nhập 900 đã quay trở lại các tham số bảo mật cũ. Ví dụ, mạch xử lý 902 có thể được làm thích ứng để tạo ra thông báo cập nhật di động với phần tử thông tin (IE) chỉ báo rằng đầu cuối truy nhập 900 đã quay trở lại các tham số bảo mật cũ do huỷ bỏ thủ tục chế độ bảo mật đang diễn ra. Theo ít nhất một ứng dụng, môđun chỉ báo và/hoặc xác định các tham số bảo mật 908 có thể bao gồm môđun chỉ báo tham số bảo mật được làm thích ứng để thực thi các thao tác chỉ báo tham số bảo mật 910 lưu trữ trong phương tiện nhớ 904 để tạo ra thông báo cập nhật di động với phần tử thông tin (IE) bao gồm chỉ

báo trạng thái bảo mật dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập 900 đã quay trở lại các tham số bảo mật cũ.

Mạch xử lý 902 có thể truyền thông báo cập nhật di động đã được tạo ra có chứa thông tin chỉ báo đến mạng truy nhập qua giao diện truyền thông 906. Thông báo cập nhật di động có thể được truyền bởi mạch xử lý 902 dưới dạng thông báo điều khiển tài nguyên vô tuyến (RRC) tại lớp điều khiển tài nguyên vô tuyến (RRC) của ngăn xếp giao thức. Theo ít nhất một số ứng dụng, thông báo cập nhật di động được truyền bởi mạch xử lý 902 có thể không được lập mã (tức là, có thể không mã hoá) để cho mạng truy nhập có thể thu và xử lý thông báo mà không cần biết các tham số bảo mật hiện được thực hiện bởi đầu cuối truy nhập 900. Thông báo cập nhật di động có thể bao gồm thông báo bất kỳ do sự di chuyển của đầu cuối truy nhập 900 gây ra như, ví dụ, thông báo chọn lại ô, thông báo không thể khôi phục điều khiển liên kết vô tuyến (RLC), thông báo mất dịch vụ, v.v..

Đầu cuối truy nhập 900 có thể thu, đáp lại thông báo cập nhật di động, thông báo xác nhận cập nhật di động được lập mã theo các tham số bảo mật cũ. Ví dụ, mạch xử lý 902 có thể thu thông báo xác nhận cập nhật di động qua giao diện truyền thông 906. Thông báo xác nhận cập nhật di động thu được được lập mã theo các tham số bảo mật cũ và có thể được giải mã bởi mạch xử lý 902 bằng cách sử dụng các tham số bảo mật cũ theo thuật toán được thoả thuận.

Fig.11 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở đầu cuối truy nhập, như đầu cuối truy nhập 900, để xác định trạng thái của các tham số bảo mật tại mạng truy nhập để truyền thông với đầu cuối truy nhập. Theo cả Fig.9 và Fig.11, đầu cuối truy nhập 900 có thể điều khiển thủ tục chế độ bảo mật ở bước 1102. Ví dụ mạch xử lý 902 có thể truyền thông với mạng truy nhập qua giao diện truyền thông 906 để điều khiển thủ tục chế độ bảo mật. Trong thủ tục chế độ bảo mật, mạch xử lý 902 có thể tạo ra và truyền thông báo hoàn thành chế độ bảo mật đến mạng truy nhập. Mạch xử lý 902 có thể truyền thông báo hoàn thành chế độ bảo mật dưới dạng thông báo điều khiển tài nguyên vô tuyến (RRC) đến mạng truy nhập.

Ở bước 1104, sau khi đầu cuối truy nhập 900 truyền thông báo hoàn thành chế độ bảo mật đến mạng truy nhập, thủ tục cập nhật di động có thể được khởi tạo trong khi thủ tục chế độ bảo mật vẫn hoạt động. Ví dụ, do sự di chuyển của đầu cuối truy nhập 900, mạch xử lý 902 có thể khởi đầu thủ tục di động. Ví dụ về thủ tục di động

có thể bao gồm chọn lại ô, lỗi không thể khôi phục điều khiển liên kết vô tuyến (RLC), đầu cuối truy nhập mất dịch vụ, v.v.. Trong thủ tục di động, đầu cuối truy nhập 900 truyền thông báo cập nhật di động đến mạng truy nhập.

Đáp lại việc khởi đầu thủ tục di động, và trước khi cập nhật các tham số bảo mật của nó (ví dụ, trước khi thu thông báo báo nhận L2 hoặc trước khi cập nhật đáp lại thông báo báo nhận L2), đầu cuối truy nhập 900 huỷ bỏ thủ tục chế độ bảo mật đang diễn ra và quay trở lại các tham số bảo mật cũ ở bước 1106. Ví dụ, mạch xử lý 902 có thể huỷ bỏ thủ tục chế độ bảo mật đang hoạt động và quay trở lại sử dụng các tham số bảo mật cũ do khởi đầu thủ tục di động.

Đáp lại thông báo cập nhật di động được truyền đến mạng truy nhập trong thủ tục di động, đầu cuối truy nhập 900 thu thông báo xác nhận cập nhật di động từ mạng truy nhập ở bước 1108. Ví dụ, mạch xử lý 902 có thể thu thông báo xác nhận cập nhật di động qua giao diện truyền thông 906. Ở bước 1110, mạch xử lý 902 thử giải mã thông báo xác nhận cập nhật di động bằng cách sử dụng các tham số bảo mật cũ. Ví dụ, mạch xử lý 902 có thể bao gồm môđun xác định các tham số bảo mật 908 được làm thích ứng để thực thi các thao tác xác định tham số bảo mật 910 lưu trữ trong phương tiện nhớ 904. Nếu mạch xử lý 902 có khả năng giải mã thông báo xác nhận cập nhật di động, thì đầu cuối truy nhập gửi thông báo đáp đến mạng truy nhập ở bước 1112. Trong trường hợp này, thông báo đáp có thể được lập mã bằng cách sử dụng các tham số bảo mật cũ.

Tuy nhiên, nếu mạch xử lý 902 (ví dụ, môđun xác định các tham số bảo mật 908) không thể giải mã thông báo xác nhận cập nhật di động, thì mạch xử lý 902 có thể chuyển sang các tham số bảo mật mới ở bước 1114 và có thể thử giải mã thông báo xác nhận cập nhật di động bằng cách sử dụng các tham số bảo mật mới. Theo ít nhất một ứng dụng, mạch xử lý 902 (ví dụ, môđun xác định các tham số bảo mật 908) có thể được làm thích ứng để chuyển sang các tham số bảo mật mới sau một số lần định trước thất bại trong việc thử giải mã thông báo xác nhận cập nhật di động (ví dụ, một hoặc nhiều lần thử).

Nếu mạch xử lý 902 thành công trong việc giải mã thông báo xác nhận cập nhật di động bằng cách sử dụng các tham số bảo mật mới, thì mạch xử lý 902 có thể được làm thích ứng để tiếp tục sử dụng các tham số bảo mật mới ở bước 1118. Mạch xử lý 902 có thể truyền thông báo đáp đến mạng truy nhập qua giao diện truyền

thông 906 bằng cách sử dụng các tham số bảo mật mới ở bước 1112. Nếu mạch xử lý 902 không thành công trong việc giải mã thông báo xác nhận cập nhật di động bằng cách sử dụng các tham số bảo mật mới, thì cuộc gọi có thể thất bại.

Fig.12 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở đầu cuối truy nhập, như đầu cuối truy nhập 900, để chỉ báo cho mạng truy nhập khi đầu cuối truy nhập đã cập nhật các tham số bảo mật mới. Theo cả Fig. 9 và Fig.12, đầu cuối truy nhập 900 đang điều khiển thủ tục chế độ bảo mật có thể tạo ra và truyền thông báo hoàn thành chế độ bảo mật đến mạng truy nhập ở bước 1202. Ví dụ mạch xử lý 902 (ví dụ, môđun chỉ báo tham số bảo mật 908) có thể tạo ra và truyền thông báo hoàn thành chế độ bảo mật qua giao diện truyền thông 906. Mạch xử lý 902 có thể truyền thông báo hoàn thành chế độ bảo mật dưới dạng thông báo điều khiển tài nguyên vô tuyến (RRC) đến mạng truy nhập.

Ở bước 1204, mạch xử lý 902 có thể thu qua giao diện truyền thông 906 thông báo báo nhận từ mạng truy nhập. Thông báo báo nhận thu được đáp lại thông báo hoàn thành chế độ bảo mật và có thể bao gồm cuộc truyền L2. Thông báo báo nhận có thể chỉ báo cho mạch xử lý 902 rằng thông báo hoàn thành chế độ bảo mật được thu thành công bởi mạng truy nhập. Đáp lại việc thu được thông báo báo nhận, mạch xử lý 902 cập nhật các tham số bảo mật của đầu cuối truy nhập 900 ở các tham số bảo mật mới tại bước 1206.

Sau khi đầu cuối truy nhập 900 được cập nhật ở các tham số bảo mật mới, mạch xử lý 902 truyền thông tin chỉ báo đến mạng truy nhập ở bước 908 để báo cho mạng truy nhập biết rằng đầu cuối truy nhập 900 đã cập nhật thành công các tham số bảo mật mới. Ví dụ, mạch xử lý 902 (ví dụ, môđun chỉ báo tham số bảo mật 908) có thể tạo ra và truyền thông báo báo nhận L3 đến mạng truy nhập qua giao diện truyền thông 906 để chỉ báo rằng đầu cuối truy nhập 900 đã cập nhật thành công ở các tham số bảo mật mới.

Thực thể mạng làm ví dụ

Fig.13 là sơ đồ khối minh họa các thành phần chọn lọc của thực thể mạng 1300 theo ít nhất một phương án. Theo ít nhất một số ứng dụng, thực thể mạng 1300 có thể bao gồm bộ điều khiển mạng vô tuyến (RNC) của mạng truy nhập, như RNC 114 trên Fig.1. Thực thể mạng 1300 thường bao gồm mạch xử lý 1302 ghép nối với phương tiện nhớ 1304 và giao diện truyền thông 1306.

Mạch xử lý 1302 được bố trí để tiếp nhận, xử lý và/hoặc truyền dữ liệu, điều khiển truy nhập và lưu trữ dữ liệu, đưa ra các lệnh, và điều khiển các thao tác cần thiết khác. Mạch xử lý 1302 có thể bao gồm mạch được tạo cấu hình để thực thi chương trình cần thiết được cung cấp bởi phương tiện thích hợp theo ít nhất một phương án. Ví dụ, mạch xử lý 1302 có thể được thực hiện dưới dạng một hoặc nhiều bộ xử lý, bộ điều khiển, nhiều bộ xử lý và/hoặc cấu trúc khác được tạo cấu hình để thực thi các lệnh khả thi trong đó, ví dụ, các lệnh phần mềm và/hoặc phần sụn, và/hoặc mạch phần cứng. Các phương án của mạch xử lý 1302 có thể bao gồm bộ xử lý đa năng, bộ xử lý tín hiệu số (DSP), mạch tích hợp chuyên dụng (ASIC), mảng cửa lập trình được bằng trường (FPGA) hoặc thành phần logic lập trình được khác, mạch cửa rời rạc hoặc mạch logic tranzito, các thành phần phần cứng rời rạc hoặc tổ hợp bất kỳ của chúng được thiết kế để thực hiện các chức năng được mô tả ở đây. Bộ xử lý đa năng có thể là bộ vi xử lý, nhưng theo cách khác, bộ xử lý có thể là bộ xử lý thông thường, bộ điều khiển, bộ vi điều khiển hoặc máy trạng thái bất kỳ. Bộ xử lý còn có thể được thực hiện dưới dạng tổ hợp của các thiết bị tính toán, ví dụ, tổ hợp của DSP và bộ vi xử lý, các bộ vi xử lý, một hoặc nhiều bộ vi xử lý phối hợp với lõi DSP, hoặc cấu hình tương tự bất kỳ khác. Các ví dụ như vậy về mạch xử lý 1302 chỉ để minh họa và cấu hình thích hợp khác trong phạm vi của sáng chế cũng được dự tính.

Mạch xử lý 1302 có thể bao gồm môđun quay trở lại và/hoặc cập nhật các tham số bảo mật 1308. Môđun quay trở lại và/hoặc cập nhật các tham số bảo mật 1308 có thể bao gồm mạch và/hoặc chương trình được làm thích ứng để thực hiện các thủ tục quay trở lại các tham số bảo mật cũ và/hoặc thủ tục cập nhật các tham số bảo mật mới, theo các ứng dụng khác nhau.

Phương tiện nhớ 1304 có thể là một hoặc nhiều thiết bị để lưu trữ chương trình và/hoặc dữ liệu, như mã hoặc lệnh có thể thực hiện bằng bộ xử lý (ví dụ, phần mềm, phần sụn), dữ liệu điện tử, cơ sở dữ liệu, hoặc thông tin số khác. Phương tiện nhớ 1304 có thể là phương tiện khả dụng bất kỳ có thể được truy nhập bởi bộ xử lý đa năng hoặc chuyên dụng. Ví dụ và không giới hạn phạm vi của sáng chế, phương tiện nhớ 1304 có thể bao gồm bộ nhớ chỉ đọc (ví dụ, ROM, EPROM, EEPROM), bộ nhớ truy nhập ngẫu nhiên (RAM), phương tiện nhớ đĩa từ, phương tiện nhớ quang, thiết bị nhớ tác động nhanh, và/hoặc vật ghi đọc được bằng máy tính bền vững khác

dùng để lưu trữ thông tin. Phương tiện nhớ 1304 có thể ghép nối với mạch xử lý 1302 sao cho mạch xử lý 1302 có thể đọc thông tin từ, và ghi thông tin vào, phương tiện nhớ 1304. Theo cách khác, phương tiện nhớ 1304 có thể liền khối với mạch xử lý 1302.

Phương tiện nhớ 1304 có thể chứa các thao tác quay trở lại và/hoặc cập nhật các tham số bảo mật 1310, theo một hoặc nhiều phương án. Các thao tác quay trở lại và/hoặc cập nhật các tham số bảo mật 1310 có thể được thực hiện bởi mạch xử lý 1302 trong, ví dụ, môđun quay trở lại và/hoặc cập nhật các tham số bảo mật 1308. Trong một số ứng dụng, các thao tác quay trở lại các tham số bảo mật có thể bao gồm các thao tác có thể được thực hiện bởi mạch xử lý 1302 để xác định có quay trở lại các tham số bảo mật cũ hay không và tiến hành quay trở lại các tham số bảo mật cũ. Trong một số ứng dụng, các thao tác cập nhật các tham số bảo mật có thể bao gồm các thao tác có thể được thực hiện bởi mạch xử lý 1302 để cập nhật các tham số bảo mật.

Giao diện truyền thông 1306 được tạo cấu hình để tạo điều kiện thuận lợi cho việc truyền thông không dây của thực thể mạng 1300. Ví dụ, giao diện truyền thông 1306 có thể được tạo cấu hình để truyền thông thông tin hai chiều với một hoặc nhiều đầu cuối truy nhập và/hoặc các thực thể mạng khác. Mạch truyền thông 1306 có thể ghép nối với anten (không được thể hiện) và có thể bao gồm mạch thu phát không dây, gồm ít nhất một bộ truyền 1312 và/hoặc ít nhất một bộ thu 1314 (ví dụ, một hoặc nhiều chuỗi truyền/thu).

Theo một hoặc nhiều dấu hiệu của thực thể mạng 1300, mạch xử lý 1302 có thể được làm thích ứng để thực hiện một số bất kỳ hoặc tất cả các quy trình, chức năng, bước và/hoặc thường trình liên quan đến một hoặc nhiều thực thể trong số các thực thể mạng khác nhau đã được mô tả dựa vào các hình vẽ từ Fig.1 đến Fig. 8 (ví dụ, thực thể của mạng truy nhập 104, như nút truy nhập 112 và/hoặc bộ điều khiển mạng vô tuyến (RNC) 114, hoặc thực thể của mạng lõi 106, như nút hỗ trợ GPRS phục vụ (SGSN) 116 và/hoặc trung tâm chuyển mạch di động (MSC) 118). Như được sử dụng ở đây, thuật ngữ "được làm thích ứng" liên quan đến mạch xử lý 1302 có thể được dùng để chỉ mạch xử lý 1302 là một hoặc nhiều mạch được tạo cấu hình, sử dụng, thực thi hoặc lập trình để thực hiện quy trình, chức năng, bước và/hoặc thường trình cụ thể theo các dấu hiệu khác nhau được mô tả ở đây.

Fig.14 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở thực thể mạng, như thực thể mạng 1300, để xác định rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ. Theo cả hai hình vẽ Fig.13 và Fig.14, thực thể mạng 1300 có thể thu thông báo hoàn thành chế độ bảo mật từ đầu cuối truy nhập ở bước 1402. Ví dụ, mạch xử lý 1302 có thể thu thông báo hoàn thành chế độ bảo mật qua giao diện truyền thông 1306. Theo ít nhất một số ứng dụng, thông báo hoàn thành chế độ bảo mật có thể bao gồm thông báo hoàn thành chế độ bảo mật tầng truy nhập (AS). Thông báo hoàn thành chế độ bảo mật AS có thể được thu qua giao diện truyền thông 1306 tại lớp điều khiển tài nguyên vô tuyến (RRC) của ngăn xếp giao thức.

Đáp lại thông báo hoàn thành chế độ bảo mật thu được từ đầu cuối truy nhập, thực thể mạng 1300 có thể cập nhật các tham số bảo mật mới dùng cho truyền thông giữa thực thể mạng 1300 và đầu cuối truy nhập ở bước 1404. Theo ít nhất một ứng dụng, mạch xử lý 1302 có thể được làm thích ứng để cập nhật các tham số bảo mật liên quan đến đầu cuối truy nhập ở các tham số bảo mật mới đáp lại việc thu được thông báo hoàn thành chế độ bảo mật. Theo các ứng dụng trong đó thông báo hoàn thành chế độ bảo mật bao gồm thông báo hoàn thành chế độ bảo mật AS, các tham số bảo mật mới có thể bao gồm các tham số bảo mật tầng truy nhập (AS) mới. Mạch xử lý 1302 có thể được làm thích ứng để giữ lại các tham số bảo mật cũ trong khoảng thời gian định trước sau khi cập nhật ở các tham số bảo mật mới. Ví dụ, mạch xử lý 1302 có thể lưu trữ các tham số bảo mật cũ ở phương tiện nhớ 1304 trong một khoảng thời gian (ví dụ, cho đến khi tín hiệu truyền thông thu được từ đầu cuối truy nhập sử dụng các tham số bảo mật mới).

Ở bước 1406, thực thể mạng 1300 có thể thu thông báo cập nhật di động từ đầu cuối truy nhập, trong đó thông báo cập nhật di động chứa thông tin chỉ báo trạng thái bảo mật dành riêng được làm thích ứng để chỉ báo cho thực thể mạng 1300 biết rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ. Ví dụ, mạch xử lý 1302 có thể thu thông báo cập nhật di động qua giao diện truyền thông 1306. Thông báo cập nhật di động có thể thu được dưới dạng thông báo điều khiển tài nguyên vô tuyến (RRC). Theo ít nhất một ứng dụng, thông báo cập nhật di động không được lập mã, và có thể được đọc bởi mạch xử lý 1302 mà không cần phải giải mã thông báo trước. Thông báo cập nhật di động có thể bao gồm thông báo được truyền bởi đầu cuối truy nhập do di chuyển. Ví dụ và không giới hạn phạm vi, thông báo cập nhật di

động có thể bao gồm thông báo chọn lại ô, thông báo không thể khôi phục điều khiển liên kết vô tuyến (RLC), thông báo mất dịch vụ, v.v..

Trong một số ứng dụng, chỉ báo trạng thái dành riêng nằm trong thông báo cập nhật di động có thể bao gồm phần tử thông tin (IE) được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ. Trong một số ứng dụng, chỉ báo trạng thái dành riêng nằm trong thông báo cập nhật di động có thể bao gồm một hoặc nhiều bit được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

Ở bước 1408, thực thể mạng 1300 quay trở lại các tham số bảo mật cũ. Ví dụ, mạch xử lý 1302 có thể quay trở lại các tham số bảo mật cũ đáp lại thông báo cập nhật di động thu được có chứa chỉ báo trạng thái bảo mật dành riêng. Trong một số ứng dụng, môđun quay trở lại và/hoặc cập nhật các tham số bảo mật 1308 có thể thực thi các thao tác quay trở lại và/hoặc cập nhật các tham số bảo mật 1310 ngay khi thu được chỉ báo trạng thái bảo mật dành riêng báo cho thực thể mạng 1300 biết rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ. Là một phần của các thao tác quay trở lại và/hoặc cập nhật các tham số bảo mật 1310, môđun quay trở lại và/hoặc cập nhật các tham số bảo mật 1308 có thể duy trì sự liên kết giữa đầu cuối truy nhập và các tham số bảo mật cũ có khả năng thay thế các tham số bảo mật mới với các tham số bảo mật trước đó (hoặc cũ). Theo cách này, mạch xử lý 1302 có thể sử dụng các tham số bảo mật cũ cho việc truyền thông sau đó với đầu cuối truy nhập.

Đáp lại thông báo cập nhật di động thu được, thực thể mạng 1300 có thể truyền thông báo xác nhận cập nhật di động đến đầu cuối truy nhập ở bước 1410 để báo nhận thu được thông báo cập nhật di động. Thông báo xác nhận cập nhật di động có thể được lập mã theo các tham số bảo mật cũ. Theo ít nhất một số ứng dụng, mạch xử lý 1302 có thể tạo ra thông báo xác nhận cập nhật di động và có thể lập mã thông báo xác nhận cập nhật di động theo các tham số bảo mật cũ. Mạch xử lý 1302 có thể truyền thông báo xác nhận cập nhật di động đã được lập mã đến đầu cuối truy nhập qua giao diện truyền thông 1306.

Fig.15 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở thực thể mạng, như thực thể mạng 1300, để xác định rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ. Theo cả hai Fig.13 và Fig.15, thực thể mạng 1300 có thể thu thông báo hoàn thành chế độ bảo mật từ đầu cuối truy nhập ở bước 1502. Ví dụ,

mạch xử lý 1302 có thể thu thông báo hoàn thành chế độ bảo mật qua giao diện truyền thông 1306.

Đáp lại thông báo hoàn thành chế độ bảo mật thu được từ đầu cuối truy nhập, thực thể mạng 1300 có thể cập nhật ở các tham số bảo mật mới dùng cho truyền thông giữa thực thể mạng 1300 và đầu cuối truy nhập ở bước 1504. Theo ít nhất một ứng dụng, mạch xử lý 1302 có thể được làm thích ứng để cập nhật các tham số bảo mật liên quan đến đầu cuối truy nhập ở các tham số bảo mật mới đáp lại việc thu được thông báo hoàn thành chế độ bảo mật. Mạch xử lý 1302 có thể được làm thích ứng để giữ lại các tham số bảo mật cũ trong một khoảng thời gian xác định sau khi cập nhật các tham số bảo mật mới. Ví dụ, mạch xử lý 1302 có thể lưu trữ các tham số bảo mật cũ trong phương tiện nhớ 1304 trong một khoảng thời gian (cho đến khi thu được tín hiệu truyền thông từ đầu cuối truy nhập sử dụng các tham số bảo mật mới chẳng hạn).

Ở bước 1506, thực thể mạng 1300 có thể thu thông báo cập nhật di động từ đầu cuối truy nhập. Ví dụ, mạch xử lý 1302 có thể thu thông báo cập nhật di động qua giao diện truyền thông 1306. Thông báo cập nhật di động có thể thu được dưới dạng thông báo điều khiển tài nguyên vô tuyến (RRC). Theo ít nhất một ứng dụng, thông báo cập nhật di động không được lập mã, và có thể được đọc bởi mạch xử lý 1302 mà không cần giải mã thông báo trước.

Đáp lại thông báo cập nhật di động thu được, thực thể mạng 1300 tạo ra và truyền thông báo xác nhận cập nhật di động ở bước 1508. Ví dụ, mạch xử lý 1302 có thể tạo ra thông báo xác nhận cập nhật di động và có thể lập mã thông báo theo các tham số bảo mật mới. Tiếp đó, mạch xử lý 1302 có thể truyền thông báo xác nhận cập nhật di động đã được lập mã qua giao diện truyền thông 1306 đến đầu cuối truy nhập.

Ở bước 1510, thực thể mạng 1300 xác định xem thông báo đáp lại thông báo xác nhận cập nhật di động có thu được từ đầu cuối truy nhập hay không. Ví dụ, mạch xử lý 1302 có thể giám sát các tín hiệu truyền thông thu được qua giao diện truyền thông 1306 để tìm thông báo đáp lại thông báo xác nhận cập nhật di động. Theo ít nhất một số ứng dụng, các thao tác quay trở lại và/hoặc cập nhật các tham số bảo mật 1310 có thể khiến cho môđun quay trở lại và/hoặc cập nhật các tham số bảo mật

1308 giám sát thông báo đáp thu được. Nếu thu được thông báo đáp, mạch xử lý 1302 có thể tiếp tục sử dụng các tham số bảo mật mới.

Nếu không thu được thông báo đáp, thì môđun quay trở lại và/hoặc cập nhật các tham số bảo mật 1308 có thể quay trở lại các tham số bảo mật cũ ở bước 1512 để xác định xem đầu cuối truy nhập hiện đang sử dụng các tham số bảo mật cũ hay không. Trong một số ứng dụng, mạch xử lý 1302 (ví dụ, các thao tác quay trở lại và/hoặc cập nhật các tham số bảo mật 1310) có thể được làm thích ứng để truyền lại thông báo xác nhận cập nhật di động sau khi không thu được thông báo đáp, và đợi thông báo đáp khác để truyền lại thông báo xác nhận cập nhật di động. Nếu không thu được thông báo đáp sau một số lần định trước truyền thông báo xác nhận cập nhật di động, mạch xử lý 1302 (ví dụ, các thao tác quay trở lại và/hoặc cập nhật các tham số bảo mật 1310) có thể được làm thích ứng để quay trở lại các tham số bảo mật cũ để xác định đầu cuối truy nhập có sử dụng các tham số bảo mật cũ hay không.

Khi sử dụng các tham số bảo mật cũ, thực thể mạng 1300 tạo ra và truyền thông báo xác nhận cập nhật di động khác ở bước 1514. Trong một số ứng dụng, mạch xử lý 1302 có thể tạo ra thông báo xác nhận cập nhật di động và có thể lập mã thông báo. Khác với các thông báo xác nhận cập nhật di động trước đây được lập mã theo các tham số bảo mật mới, thông báo xác nhận cập nhật di động này được lập mã theo các tham số bảo mật cũ. Tiếp đó, mạch xử lý 1302 có thể truyền thông báo xác nhận cập nhật di động đã được lập mã qua giao diện truyền thông 1306 đến đầu cuối truy nhập.

Ở bước 1516, thực thể mạng 1300 xác định thông báo đáp lại thông báo xác nhận cập nhật di động được lập mã theo các tham số bảo mật cũ có thu được từ đầu cuối truy nhập hay không. Ví dụ, mạch xử lý 1302 có thể giám sát các tín hiệu truyền thông thu được qua giao diện truyền thông 1306 để tìm thông báo đáp lại thông báo xác nhận cập nhật di động. Nếu thu được thông báo đáp lại thông báo xác nhận cập nhật di động được lập mã theo các tham số bảo mật cũ, thì môđun quay trở lại và/hoặc cập nhật các tham số bảo mật 1308 có thể xác định rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ, và có thể làm cho thực thể mạng 1300 tiếp tục sử dụng các tham số bảo mật cũ ở bước 1518. Nếu không thu được thông báo

đáp lại thông báo xác nhận cập nhật di động được lập mã theo các tham số bảo mật cũ, thì mạch xử lý 1302 có thể làm cho cuộc gọi bị thất bại với đầu cuối truy nhập.

Fig.16 là lưu đồ minh họa một ví dụ của phương pháp vận hành ở thực thể mạng, như thực thể mạng 1300, để cập nhật từ các tham số bảo mật cũ sang các tham số bảo mật mới sau khi đầu cuối truy nhập đã cập nhật các tham số bảo mật mới. Theo cả Fig. 13 và Fig.16, thực thể mạng 1300 có thể thu thông báo hoàn thành chế độ bảo mật từ đầu cuối truy nhập ở bước 1602. Ví dụ, mạch xử lý 1302 có thể thu thông báo hoàn thành chế độ bảo mật qua giao diện truyền thông 1306.

Đáp lại thông báo hoàn thành chế độ bảo mật, thực thể mạng 1300 truyền thông báo báo nhận đến đầu cuối truy nhập ở bước 1604. Thông báo báo nhận có thể bao gồm tín hiệu truyền L2 được làm thích ứng để chỉ báo cho đầu cuối truy nhập rằng thông báo hoàn thành chế độ bảo mật đã được thu và xác minh thành công bởi thực thể mạng. Theo ít nhất một ứng dụng, mạch xử lý 1302 có thể tạo ra và truyền thông báo báo nhận đến đầu cuối truy nhập qua giao diện truyền thông 1306.

Ở bước 1606, thực thể mạng 1300 thu thông báo báo nhận từ đầu cuối truy nhập. Thông báo báo nhận thu được có thể bao gồm thông báo báo nhận L3 được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã cập nhật thành công ở các tham số bảo mật mới. Theo ít nhất một ứng dụng, mạch xử lý 1302 (ví dụ, môđun quay trở lại và/hoặc cập nhật các tham số bảo mật 1308) có thể thu thông báo báo nhận L3 qua giao diện truyền thông 1306.

Đáp lại việc thu được thông báo báo nhận từ đầu cuối truy nhập, thực thể mạng 1300 có thể cập nhật các tham số bảo mật mới dùng cho truyền thông giữa thực thể mạng 1300 và đầu cuối truy nhập ở bước 1608. Ví dụ, mạch xử lý 1302 (ví dụ, môđun quay trở lại và/hoặc cập nhật các tham số bảo mật 1308) có thể cập nhật các tham số bảo mật liên quan đến đầu cuối truy nhập ở các tham số bảo mật mới đáp lại việc thu được thông báo báo nhận được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã cập nhật ở các tham số bảo mật mới. Mạch xử lý 1302 có thể sử dụng các tham số bảo mật mới để truyền thông sau đó với đầu cuối truy nhập.

Một hoặc nhiều thành phần, bước, dấu hiệu và/hoặc chức năng được minh họa trên các hình vẽ Fig.1, Fig.2, Fig.3, Fig.4, Fig.5, Fig.6, Fig.7, Fig.8, Fig.9, Fig.10, Fig.11, Fig.12, Fig.13, Fig.14, Fig.15 và/hoặc Fig.16 có thể được sắp xếp lại và/hoặc kết hợp vào một thành phần, bước, dấu hiệu hoặc chức năng duy nhất hoặc được

thực hiện trong một số thành phần, bước hoặc chức năng. Các phần tử, thành phần, bước và/hoặc chức năng khác cũng có thể được bổ sung mà không đi trệch khỏi phạm vi của sáng chế. Thiết bị, các cơ cấu và/hoặc các thành phần được minh họa trên Fig.1, Fig.4, Fig.9 và/hoặc Fig.13 có thể được tạo cấu hình để thực hiện một hoặc nhiều phương pháp, dấu hiệu, hoặc bước được mô tả dựa vào Fig.2, Fig.3, Fig.5, Fig.6, Fig.7, Fig.8, Fig.10, Fig.11, Fig.12, Fig.14, Fig.15, và/hoặc Fig.16. Các thuật toán mới được mô tả ở đây cũng có thể được thực hiện hiệu quả trong phần mềm và/hoặc được nhúng trong phần cứng.

Ngoài ra, cần lưu ý rằng ít nhất một số ứng dụng được mô tả dưới dạng quy trình được minh họa dưới dạng giản đồ luồng, lưu đồ, sơ đồ cấu trúc hoặc sơ đồ khối. Mặc dù lưu đồ có thể mô tả các thao tác dưới dạng quy trình tuần tự, nhiều thao tác này có thể được thực hiện song song hoặc đồng thời. Ngoài ra, thứ tự của các thao tác có thể được sắp xếp lại. Quy trình kết thúc khi các thao tác của nó hoàn tất. Quy trình có thể tương ứng với phương pháp, chức năng, thủ tục, thường trình con, chương trình con, v.v.. Khi quy trình tương ứng với chức năng, sự kết thúc của nó tương ứng với sự trở về của chức năng quay trở lại chức năng gọi ra hoặc chức năng chính.

Hơn nữa, các phương án có thể được thực hiện bằng phần cứng, phần mềm, phần sụn, phần trung, vi mã, hoặc tổ hợp bất kỳ của chúng. Khi được thực hiện trong phần mềm, phần sụn, phần trung hoặc vi mã, mã chương trình hoặc các đoạn mã để thực hiện các nhiệm vụ cần thiết chúng có thể được lưu trữ trong vật ghi đọc được bằng máy, như phương tiện nhớ hoặc (các) bộ nhớ khác. Đoạn mã có thể biểu diễn thủ tục, chức năng, chương trình con, chương trình, thường trình, thường trình con, môđun, gói phần mềm, lớp, hoặc tổ hợp bất kỳ của các lệnh, các cấu trúc dữ liệu hoặc các câu lệnh chương trình. Đoạn mã có thể được ghép nối với đoạn mã khác hoặc mạch phần cứng bằng cách chuyển tiếp và/hoặc thu thông tin, dữ liệu, đối số, tham số, hoặc nội dung bộ nhớ. Thông tin, đối số, tham số, dữ liệu, v.v.. có thể được chuyển, chuyển tiếp hoặc truyền bằng cách sử dụng phương tiện thích hợp bất kỳ bao gồm dùng chung bộ nhớ, chuyển thông báo, chuyển thẻ bài, truyền qua mạng, v.v..

Thuật ngữ "vật ghi đọc được bằng máy", "vật ghi đọc được bằng máy tính", và/hoặc "vật ghi đọc được bằng bộ xử lý" có thể bao gồm, nhưng không chỉ giới hạn

ở thiết bị nhớ xách tay hoặc cố định, thiết bị nhớ quang, và các vật ghi bền vững khác nhau có khả năng lưu trữ, chứa hoặc mang (các) lệnh và/hoặc dữ liệu. Do vậy, các phương pháp khác nhau được mô tả ở đây có thể được thực hiện một phần hoặc toàn bộ bởi các lệnh và/hoặc dữ liệu có thể được lưu trữ trong "vật ghi đọc được bằng máy", "vật ghi đọc được bằng máy tính", và/hoặc "vật ghi đọc được bằng bộ xử lý" và được thực thi bởi một hoặc nhiều bộ xử lý, máy và/hoặc thiết bị.

Các phương pháp hoặc các thuật toán được mô tả với các ví dụ đề xuất ở đây có thể được thực hiện trực tiếp trong phần cứng, môđun phần mềm thi hành được bằng bộ xử lý, hoặc tổ hợp cả hai loại này, dưới dạng khối xử lý, các lệnh chương trình, hoặc các hướng dẫn khác, và có thể chứa trong một thiết bị hoặc phân tán trong nhiều thiết bị. Môđun phần mềm có thể thường trú trong bộ nhớ RAM, bộ nhớ tác động nhanh, bộ nhớ ROM, bộ nhớ EPROM, bộ nhớ EEPROM, thanh ghi, đĩa cứng, đĩa tháo lắp được, CD-ROM, hoặc dạng bất kỳ khác của phương tiện nhớ bền vững đã biết trong lĩnh vực kỹ thuật này. Phương tiện nhớ có thể ghép nối với bộ xử lý sao cho bộ xử lý có thể đọc thông tin từ, và ghi thông tin vào, phương tiện nhớ. Theo cách khác, phương tiện nhớ có thể liền khối với bộ xử lý.

Người có hiểu biết trung bình về lĩnh vực kỹ thuật này còn cần hiểu rằng các khối, các môđun, các mạch và các bước thuật toán logic khác nhau được mô tả với các phương pháp đề xuất ở đây có thể được thực hiện dưới dạng phần cứng điện tử, phần mềm máy tính, hoặc tổ hợp cả hai. Để minh họa rõ khả năng hoán đổi của phần cứng và phần mềm, các thành phần, các khối, các môđun, các mạch và các bước minh họa khác nhau được mô tả chung trên đây về chức năng của chúng. Chức năng này được thực hiện dưới dạng phần cứng hay phần mềm tuỳ thuộc vào ứng dụng và các ràng buộc thiết kế cụ thể được đặt ra trong toàn hệ thống.

Các dấu hiệu khác nhau của sáng chế được mô tả ở đây có thể được thực hiện trong các hệ thống khác nhau mà không đi trệch khỏi phạm vi của sáng chế. Cần lưu ý rằng các phương án nêu trên chỉ để làm ví dụ và không được hiểu là giới hạn phạm vi của sáng chế. Phần mô tả của các phương án này dự định để minh họa, và không giới hạn phạm vi của sáng chế. Như vậy, các nguyên lý được đề xuất có thể dễ dàng được áp dụng cho các loại thiết bị khác nhau và nhiều thay đổi, cải biến và sửa đổi sẽ trở nên rõ ràng với người có hiểu biết trung bình về lĩnh vực kỹ thuật này.

YÊU CẦU BẢO HỘ

1. Đầu cuối truy nhập bao gồm:

giao diện truyền thông không dây được làm thích ứng để tạo điều kiện thuận lợi cho việc truyền thông không dây; và

mạch xử lý ghép nối với giao diện truyền thông không dây, mạch xử lý này được làm thích ứng để:

điều khiển thủ tục chế độ bảo mật để tạo cấu hình lại các tham số bảo mật của đầu cuối truy nhập;

khởi đầu thủ tục di động trong khi thủ tục chế độ bảo mật đang diễn ra;

huỷ bỏ thủ tục chế độ bảo mật và quay trở lại các tham số bảo mật cũ do khởi đầu thủ tục di động; và

truyền thông báo cập nhật di động qua giao diện truyền thông không dây, thông báo cập nhật di động này chứa thông tin chỉ báo trạng thái bảo mật dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

2. Đầu cuối truy nhập theo điểm 1, trong đó thủ tục chế độ bảo mật bao gồm thủ tục chế độ bảo mật tầng truy nhập để tạo cấu hình lại các tham số bảo mật tầng truy nhập của đầu cuối truy nhập.

3. Đầu cuối truy nhập theo điểm 2, trong đó mạch xử lý được làm thích ứng để điều khiển thủ tục chế độ bảo mật tầng truy nhập bằng cách sử dụng lớp điều khiển tài nguyên vô tuyến (RRC- Radio Resource Control) của ngăn xếp giao thức.

4. Đầu cuối truy nhập theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó mạch xử lý còn được làm thích ứng để:

tạo ra và truyền thông báo hoàn thành chế độ bảo mật đến mạng truy nhập qua giao diện truyền thông không dây là một phần của thủ tục chế độ bảo mật.

5. Đầu cuối truy nhập theo điểm bất kỳ trong số các điểm từ 1 đến 4, trong đó thủ tục di động bao gồm thủ tục cập nhật ô.

6. Đầu cuối truy nhập theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó thông báo cập nhật di động bao gồm một trong số thông báo chọn lại ô, thông báo lỗi không thể khôi phục điều khiển liên kết vô tuyến (RLC - Radio Link Control), hoặc thông báo mất dịch vụ.

7. Đầu cuối truy nhập theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó thông báo cập nhật di động bao gồm thông báo điều khiển tài nguyên vô tuyến (RRC).

8. Đầu cuối truy nhập theo điểm bất kỳ trong số các điểm từ 1 đến 7, trong đó chỉ báo trạng thái bảo mật dành riêng bao gồm phần tử thông tin (IE - Information Element) của thông báo cập nhật di động.

9. Đầu cuối truy nhập theo điểm bất kỳ trong số các điểm từ 1 đến 7, trong đó chỉ báo trạng thái bảo mật dành riêng bao gồm một hoặc nhiều bit của thông báo cập nhật di động.

10. Đầu cuối truy nhập theo điểm bất kỳ trong số các điểm từ 1 đến 9, trong đó mạch xử lý được làm thích ứng để huỷ bỏ thủ tục chế độ bảo mật và quay trở lại các tham số bảo mật cũ khi thông báo báo nhận không thu được từ mạng truy nhập trước khi thủ tục di động được khởi đầu.

11. Đầu cuối truy nhập theo điểm bất kỳ trong số các điểm từ 1 đến 10, trong đó mạch xử lý còn được làm thích ứng để:

thu thông báo xác nhận cập nhật di động từ mạng truy nhập, trong đó thông báo xác nhận cập nhật di động này được lập mã theo các tham số bảo mật cũ.

12. Phương pháp vận hành ở đầu cuối truy nhập bao gồm các bước:

điều khiển thủ tục chế độ bảo mật để tạo cấu hình lại các tham số bảo mật của đầu cuối truy nhập;

khởi đầu thủ tục di động trong khi thủ tục chế độ bảo mật đang diễn ra;

huỷ bỏ thủ tục chế độ bảo mật và quay trở lại các tham số bảo mật cũ do khởi đầu thủ tục di động; và

truyền thông báo cập nhật di động chứa chỉ báo trạng thái dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

13. Phương pháp theo điểm 12, trong đó bước điều khiển thủ tục chế độ bảo mật bao gồm:

điều khiển thủ tục chế độ bảo mật tầng truy nhập để tạo cấu hình lại các tham số bảo mật tầng truy nhập của đầu cuối truy nhập.

14. Phương pháp theo điểm 13, trong đó bước điều khiển thủ tục chế độ bảo mật tầng truy nhập bao gồm:

điều khiển thủ tục chế độ bảo mật tầng truy nhập bằng cách sử dụng lớp điều khiển tài nguyên vô tuyến (RRC) của ngăn xếp giao thức.

15. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 14, trong đó bước điều khiển thủ tục chế độ bảo mật bao gồm:

tạo ra và truyền thông báo hoàn thành chế độ bảo mật đến mạng truy nhập.

16. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 15, trong đó:

bước khởi đầu thủ tục di động bao gồm khởi đầu thủ tục cập nhật ô; và

bước truyền thông báo cập nhật di động bao gồm truyền thông báo cập nhật ô.

17. Phương pháp theo điểm 16, trong đó bước truyền thông báo cập nhật ô bao gồm:

truyền một trong số thông báo chọn lại ô, thông báo lỗi không thể khôi phục điều khiển liên kết vô tuyến (RLC), hoặc thông báo mất dịch vụ.

18. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 17, trong đó bước truyền thông báo cập nhật di động bao gồm:

truyền thông báo cập nhật di động đến mạng truy nhập dưới dạng thông báo điều khiển tài nguyên vô tuyến (RRC).

19. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 18, trong đó bước truyền thông báo cập nhật di động chứa thông tin chỉ báo trạng thái dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ bao gồm:

truyền thông báo cập nhật di động chứa phần tử thông tin (IE) được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

20. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 18, trong đó bước truyền thông báo cập nhật di động chứa thông tin chỉ báo trạng thái dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ bao gồm:

truyền thông báo cập nhật di động chứa một hoặc nhiều bit được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

21. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 20, trong đó phương pháp này còn bao gồm bước:

huỷ bỏ thủ tục chế độ bảo mật và quay trở lại các tham số bảo mật cũ khi không thu được thông báo báo nhận từ mạng truy nhập trước khi thủ tục di động được khởi đầu.

22. Đầu cuối truy nhập bao gồm:

phương tiện điều khiển thủ tục chế độ bảo mật để tạo cấu hình lại các tham số bảo mật của đầu cuối truy nhập;

phương tiện khởi đầu thủ tục di động trong khi thủ tục chế độ bảo mật đang diễn ra;

phương tiện huỷ bỏ thủ tục chế độ bảo mật và quay trở lại các tham số bảo mật cũ do khởi đầu thủ tục di động; và

phương tiện truyền thông báo cập nhật di động chứa chỉ báo trạng thái dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

23. Vật ghi đọc được bằng bộ xử lý chứa các lệnh vận hành ở đầu cuối truy nhập, khi được thực thi bởi bộ xử lý sẽ khiến cho bộ xử lý thực hiện các thao tác bao gồm:

điều khiển thủ tục chế độ bảo mật để tạo cấu hình lại các tham số bảo mật của đầu cuối truy nhập;

khởi đầu thủ tục di động trong khi thủ tục chế độ bảo mật đang diễn ra;

huỷ bỏ thủ tục chế độ bảo mật và quay trở lại các tham số bảo mật cũ do khởi đầu thủ tục di động; và

truyền thông báo cập nhật di động chứa chỉ báo trạng thái dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

24. Thực thể mạng bao gồm:

giao diện truyền thông; và

mạch xử lý ghép nối với giao diện truyền thông, mạch xử lý này được làm thích ứng để:

thu thông báo hoàn thành chế độ bảo mật từ đầu cuối truy nhập;

cập nhật các tham số bảo mật mới đáp lại thông báo hoàn thành chế độ bảo mật;

thu thông báo cập nhật di động từ đầu cuối truy nhập, thông báo cập nhật di động này chứa chỉ báo trạng thái bảo mật dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ; và

quay trở lại các tham số bảo mật cũ đáp lại thông báo cập nhật di động thu được.

25. Thực thể mạng theo điểm 24, trong đó:

thông báo hoàn thành chế độ bảo mật bao gồm thông báo hoàn thành chế độ bảo mật tầng truy nhập;

các tham số bảo mật mới bao gồm các tham số bảo mật tầng truy nhập mới; và

các tham số bảo mật cũ bao gồm các tham số bảo mật tầng truy nhập cũ.

26. Thực thể mạng theo điểm 25, trong đó thông báo hoàn thành chế độ bảo mật tầng truy nhập được thu ở lớp điều khiển tài nguyên vô tuyến (RRC) của ngăn xếp giao thức.

27. Thực thể mạng theo điểm bất kỳ trong số các điểm từ 24 đến 26, trong đó thông báo cập nhật di động bao gồm một trong số thông báo chọn lại ô, thông báo lỗi không thể khôi phục điều khiển liên kết vô tuyến (RLC), hoặc thông báo mất dịch vụ.

28. Thực thể mạng theo điểm bất kỳ trong số các điểm từ 24 đến 27, trong đó thông báo cập nhật di động được thu dưới dạng thông báo điều khiển tài nguyên vô tuyến (RRC).

29. Thực thể mạng theo điểm bất kỳ trong số các điểm từ 24 đến 28, trong đó chỉ báo trạng thái bảo mật dành riêng bao gồm phần tử thông tin (IE) của thông báo cập nhật di động thu được.

30. Thực thể mạng theo điểm bất kỳ trong số các điểm từ 24 đến 28, trong đó chỉ báo trạng thái bảo mật dành riêng bao gồm một hoặc nhiều bit của thông báo cập nhật di động thu được.

31. Thực thể mạng theo điểm bất kỳ trong số các điểm từ 24 đến 30, trong đó mạch xử lý còn được làm thích ứng để:

truyền thông báo xác nhận cập nhật di động đến đầu cuối truy nhập, trong đó thông báo xác nhận cập nhật di động này được lập mã theo các tham số bảo mật cũ.

32. Thực thể mạng theo điểm bất kỳ trong số các điểm từ 24 đến 31, trong đó thực thể mạng bao gồm bộ điều khiển mạng vô tuyến (RNC - Radio Network Controller).

33. Phương pháp vận hành ở thực thể mạng bao gồm các bước:

thu thông báo hoàn thành chế độ bảo mật từ đầu cuối truy nhập;

cập nhật ở các tham số bảo mật mới đáp lại thông báo hoàn thành chế độ bảo mật;

thu thông báo cập nhật di động từ đầu cuối truy nhập, thông báo cập nhật di động này chứa thông tin chỉ báo trạng thái bảo mật dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ; và

quay trở lại các tham số bảo mật cũ đáp lại thông báo cập nhật di động thu được.

34. Phương pháp theo điểm 33, trong đó bước thu thông báo hoàn thành chế độ bảo mật bao gồm:

thu thông báo hoàn thành chế độ bảo mật tầng truy nhập.

35. Phương pháp theo điểm 34, trong đó bước thu thông báo hoàn thành chế độ bảo mật tầng truy nhập bao gồm:

thu thông báo hoàn thành chế độ bảo mật tầng truy nhập ở lớp điều khiển tài nguyên vô tuyến (RRC) của ngăn xếp giao thức.

36. Phương pháp theo điểm bất kỳ trong số các điểm từ 33 đến 35, trong đó bước thu thông báo cập nhật di động bao gồm:

thu thông báo cập nhật ô.

37. Phương pháp theo điểm 36, trong đó bước thu thông báo cập nhật ô bao gồm:

thu một trong số thông báo chọn lại ô, thông báo lỗi không thể khôi phục điều khiển liên kết vô tuyến (RLC), hoặc thông báo mất dịch vụ.

38. Phương pháp theo điểm bất kỳ trong số các điểm từ 33 đến 37, trong đó bước thu thông báo cập nhật di động bao gồm:

thu thông báo điều khiển tài nguyên vô tuyến (RRC).

39. Phương pháp theo điểm bất kỳ trong số các điểm từ 33 đến 38, trong đó bước thu thông báo cập nhật di động chứa thông tin chỉ báo trạng thái bảo mật dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ bao gồm:

thu thông báo cập nhật di động chứa phần tử thông tin (IE) được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

40. Phương pháp theo điểm bất kỳ trong số các điểm từ 33 đến 38, trong đó bước thu thông báo cập nhật di động chứa thông tin chỉ báo trạng thái bảo mật dành riêng

được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ bao gồm:

thu thông báo cập nhật di động chứa một hoặc nhiều bit được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ.

41. Phương pháp theo điểm bất kỳ trong số các điểm từ 33 đến 40, trong đó phương pháp này còn bao gồm bước:

truyền thông báo xác nhận cập nhật di động đến đầu cuối truy nhập, trong đó thông báo xác nhận cập nhật di động này được lập mã theo các tham số bảo mật cũ.

42. Thực thể mạng bao gồm:

phương tiện thu thông báo hoàn thành chế độ bảo mật từ đầu cuối truy nhập;

phương tiện cập nhật ở các tham số bảo mật mới đáp lại thông báo hoàn thành chế độ bảo mật;

phương tiện thu thông báo cập nhật di động từ đầu cuối truy nhập, thông báo cập nhật di động này chứa thông tin chỉ báo trạng thái bảo mật dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ; và

phương tiện quay trở lại các tham số bảo mật cũ đáp lại thông báo cập nhật di động thu được.

43. Vật ghi đọc được bằng bộ xử lý chứa các lệnh vận hành ở thực thể mạng, khi được thực thi bởi bộ xử lý sẽ khiến cho bộ xử lý thực hiện các thao tác bao gồm:

thu thông báo hoàn thành chế độ bảo mật từ đầu cuối truy nhập;

cập nhật ở các tham số bảo mật mới đáp lại thông báo hoàn thành chế độ bảo mật;

thu thông báo cập nhật di động từ đầu cuối truy nhập, thông báo cập nhật di động này chứa thông tin chỉ báo trạng thái bảo mật dành riêng được làm thích ứng để chỉ báo rằng đầu cuối truy nhập đã quay trở lại các tham số bảo mật cũ; và

quay trở lại các tham số bảo mật cũ đáp lại thông báo cập nhật di động thu được.

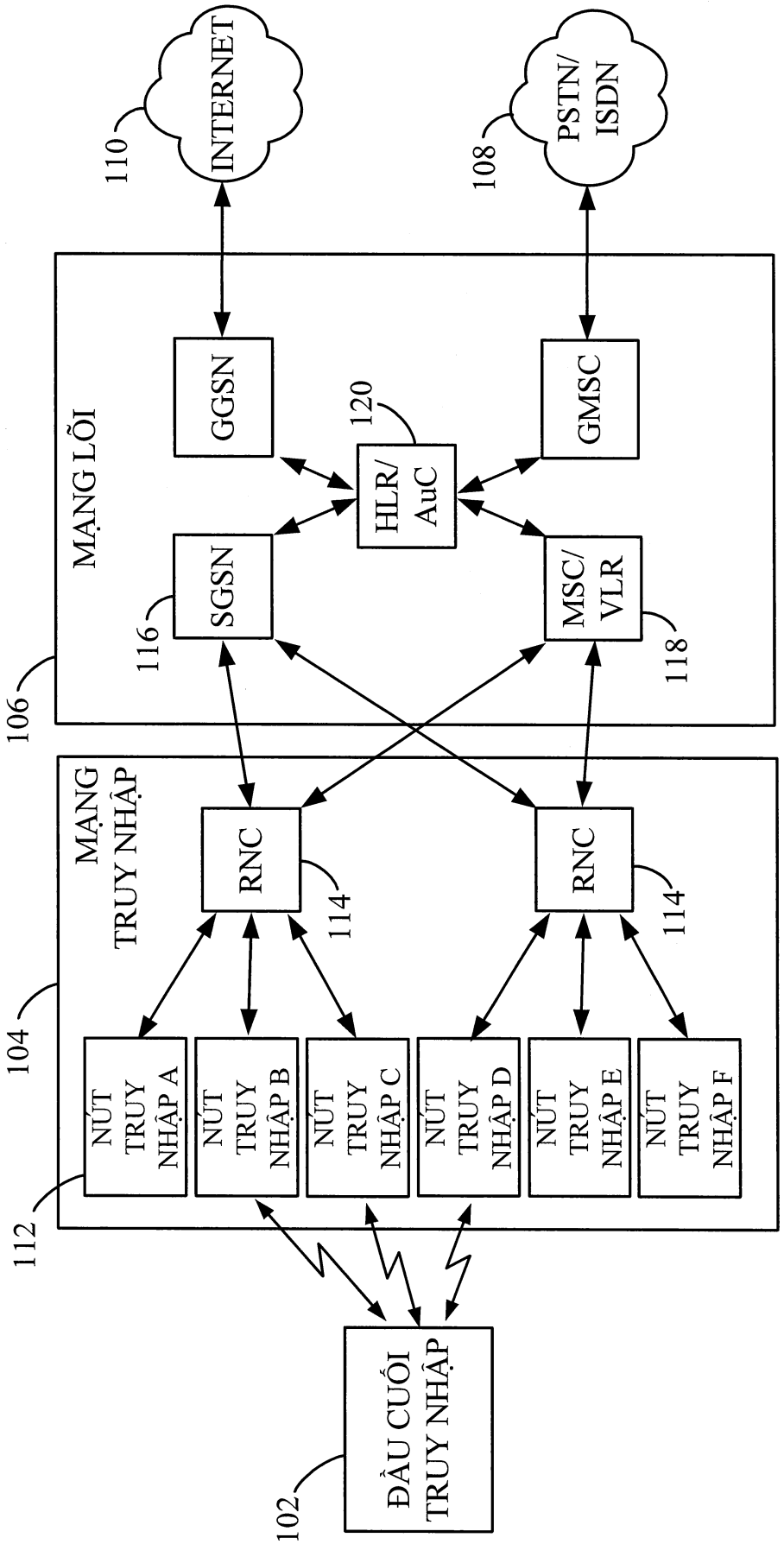

INTERNET
110
PSTN/
ISDN
108
MẠNG LÕI
106
GGSN
120
HLR/
AuC
GMSC
SGSN
116
MSC/
VLR
118
MẠNG
TRUY NHẬP
104
RNC
114
RNC
114
NÚT
TRUY
NHẬP A
NÚT
TRUY
NHẬP B
NÚT
TRUY
NHẬP C
NÚT
TRUY
NHẬP D
NÚT
TRUY
NHẬP E
NÚT
TRUY
NHẬP F
112
ĐẦU CUỐI
TRUY NHẬP
102

FIG.1

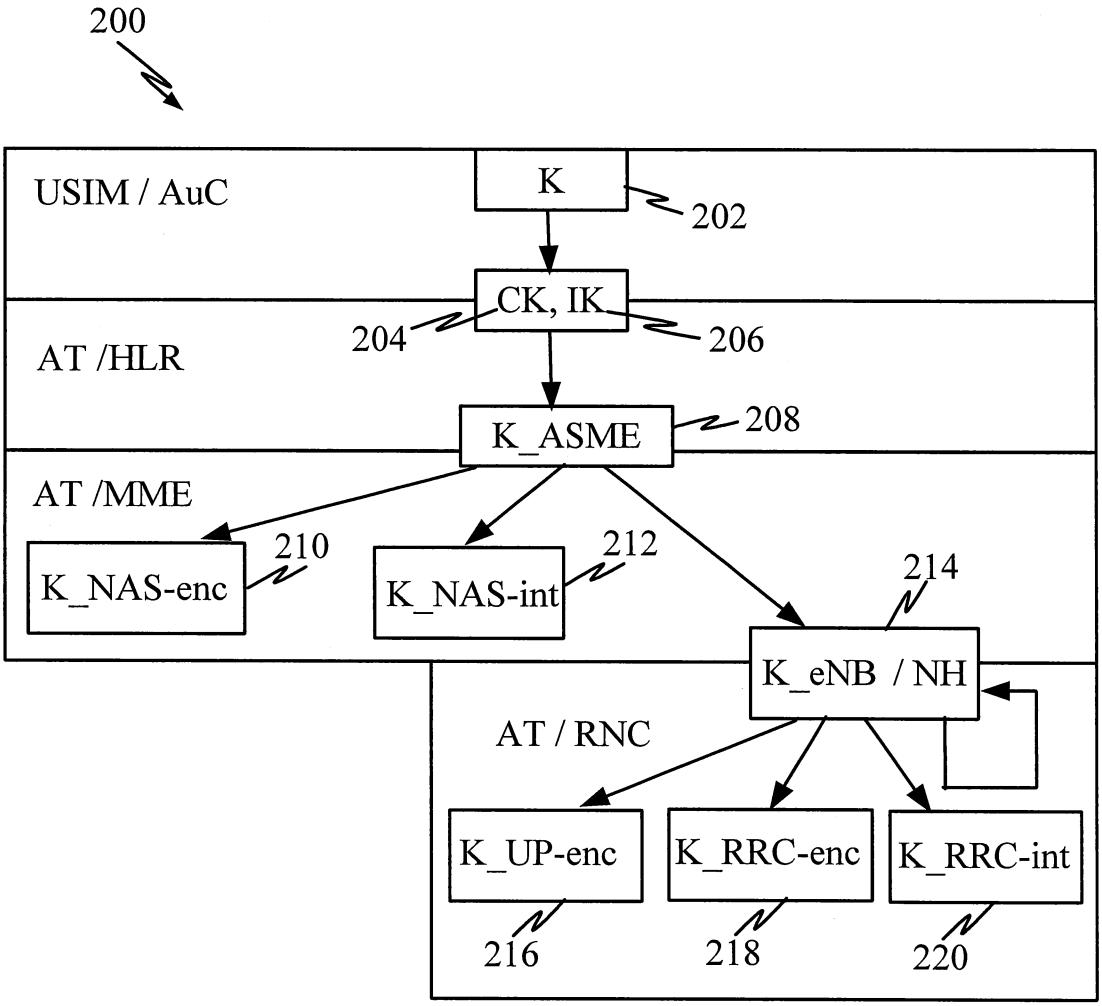

200
USIM / AuC
K
202
CK, IK
204
206
AT /HLR
K_ASME
208
AT /MME
K_NAS-enc
210
K_NAS-int
212
214
K_eNB / NH
AT / RNC
K_UP-enc
K_RRC-enc
K_RRC-int
216
218
220

FIG.2

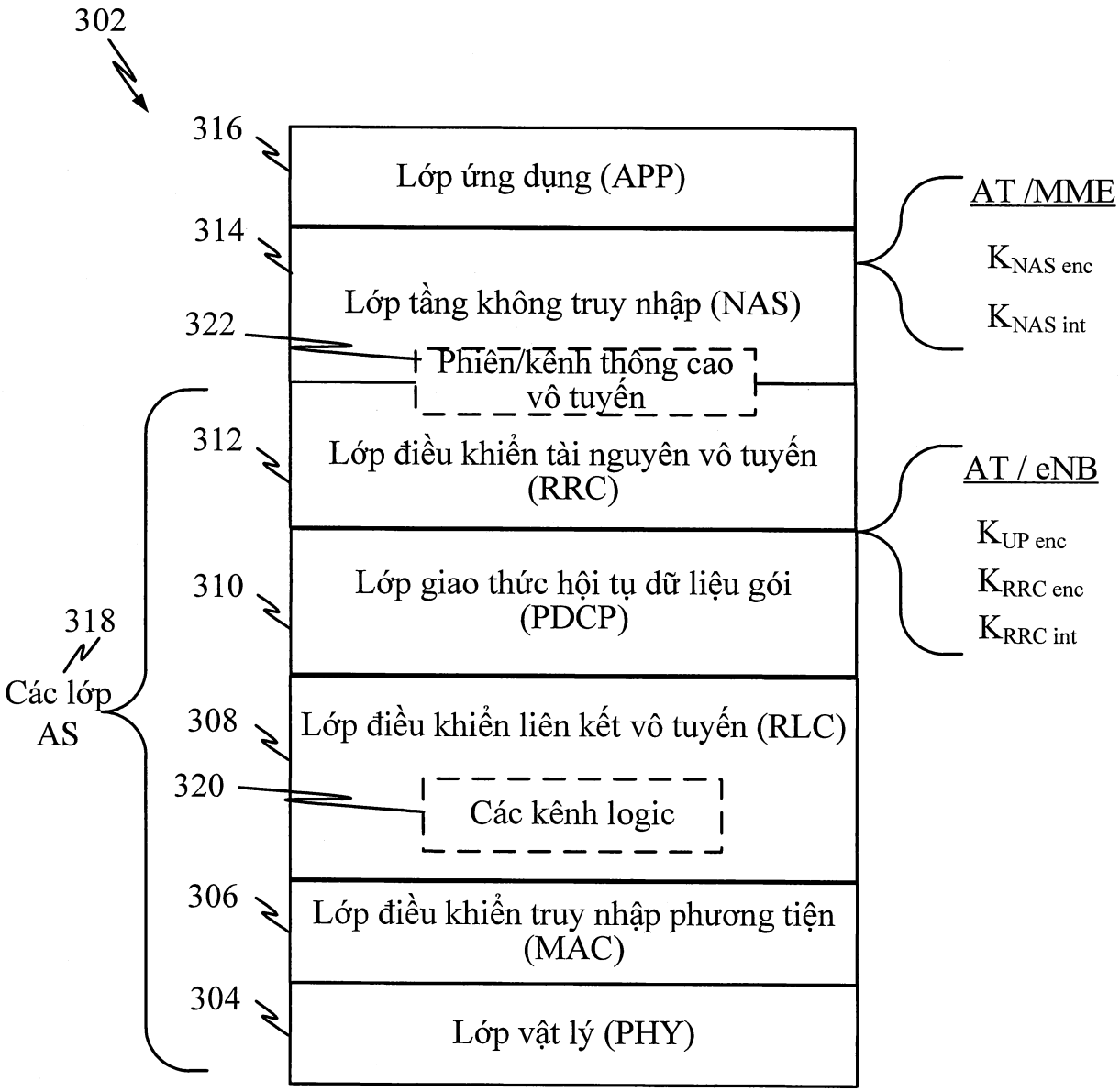

302
316
Lớp ứng dụng (APP)
314
Lớp tầng không truy nhập (NAS)
322
Phiên/kênh thông cao vô tuyến
312
Lớp điều khiển tài nguyên vô tuyến (RRC)
310
Lớp giao thức hội tụ dữ liệu gói (PDCP)
308
Lớp điều khiển liên kết vô tuyến (RLC)
320
Các kênh logic
306
Lớp điều khiển truy nhập phương tiện (MAC)
304
Lớp vật lý (PHY)
318
Các lớp AS
AT /MME
K NAS enc
K NAS int
AT / eNB
K UP enc
K RRC enc
K RRC int

FIG.3

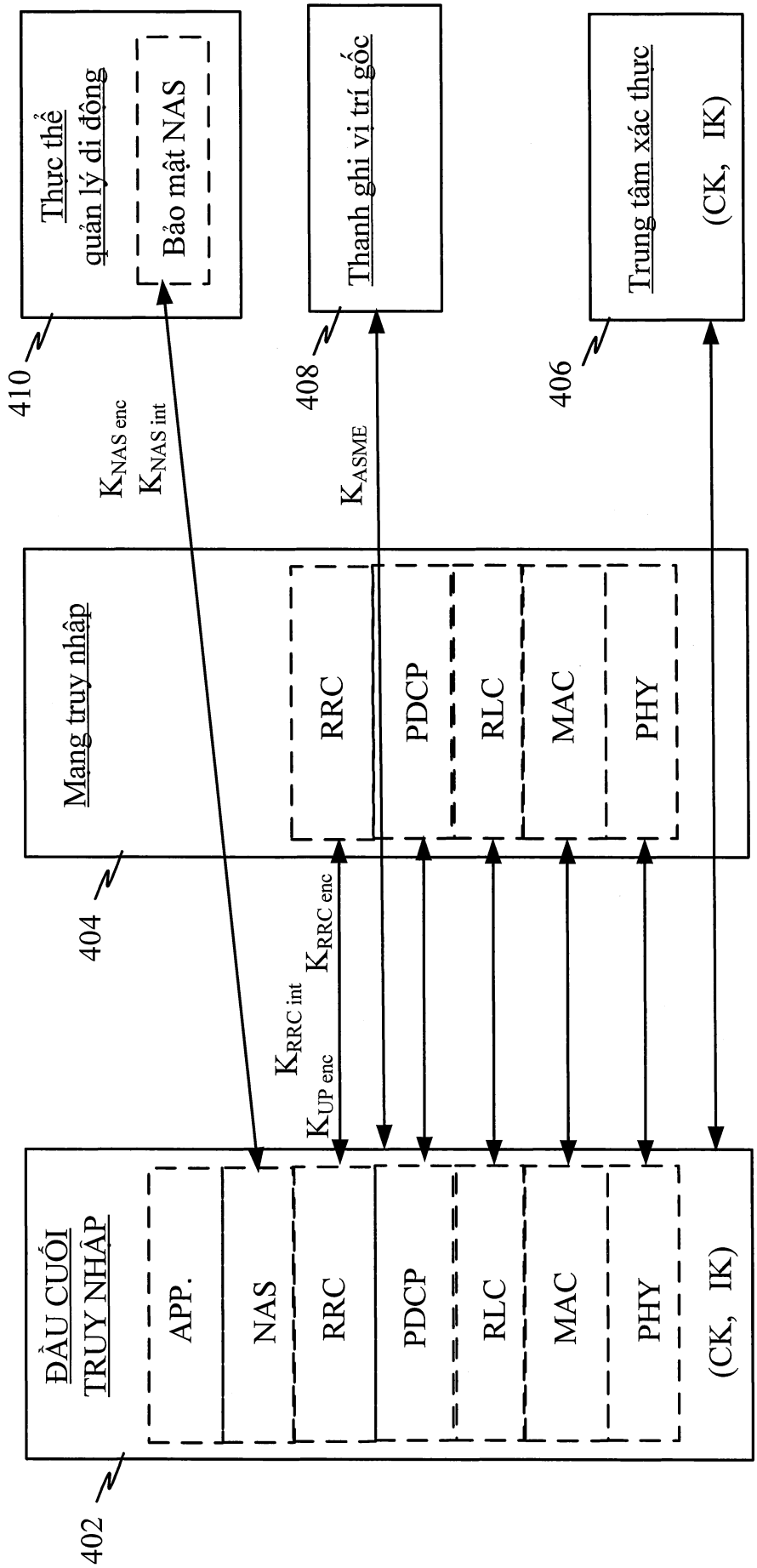

Thực thể quản lý di động
Bảo mật NAS
Thanh ghi vị trí gốc
Trung tâm xác thực
(CK, IK)
410
408
406
$K_{NAS\ enc}$
$K_{NAS\ int}$
K_{ASME}
Mạng truy nhập
RRC
PDCP
RLC
MAC
PHY
404
$K_{RRC\ int}$
$K_{RRC\ enc}$
$K_{UP\ enc}$
ĐẦU CUỐI TRUY NHẬP
APP.
NAS
RRC
PDCP
RLC
MAC
PHY
(CK, IK)
402

FIG.4

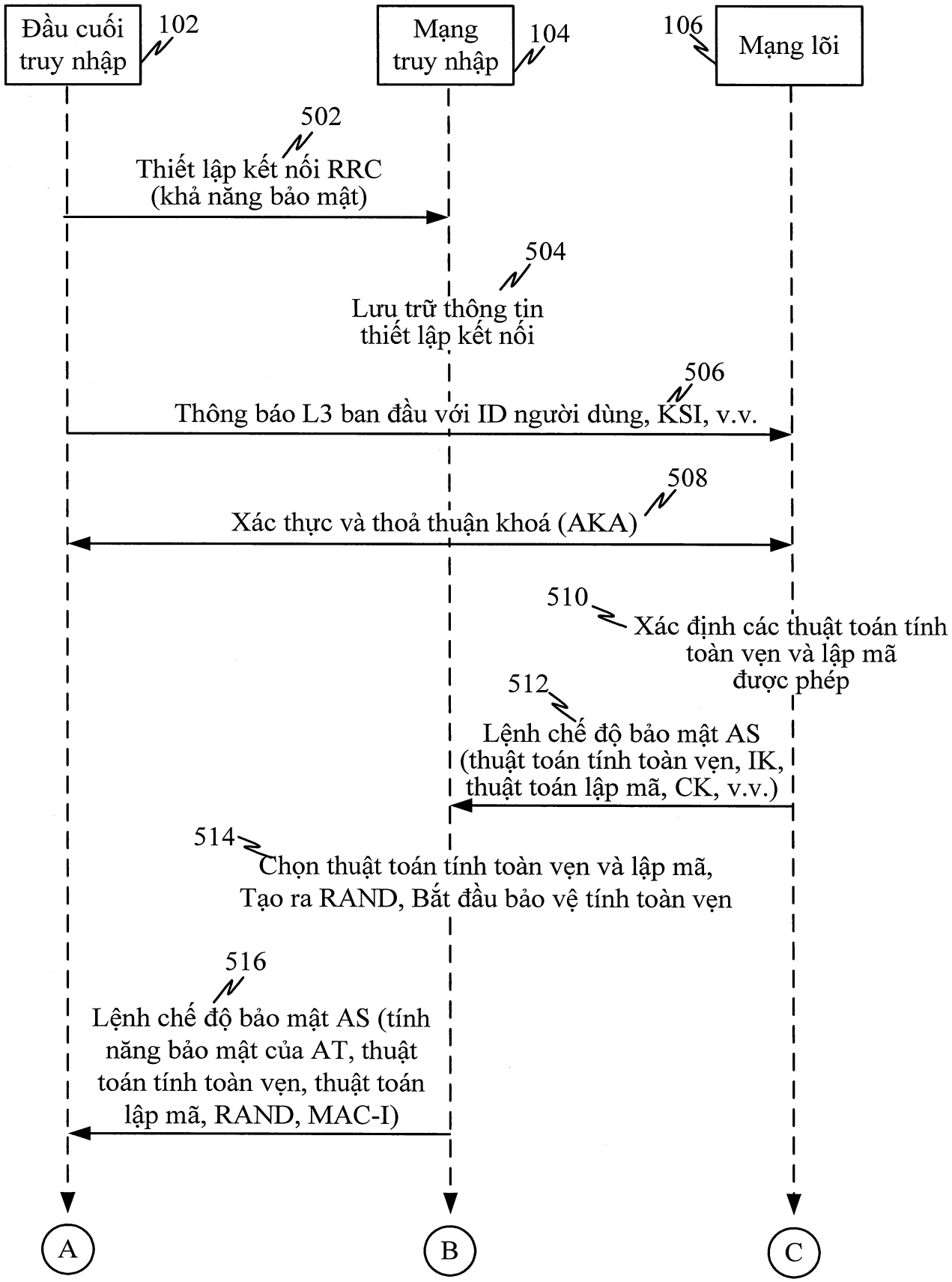

Đầu cuối truy nhập
102
Mạng truy nhập
104
106
Mạng lõi
502
Thiết lập kết nối RRC (khả năng bảo mật)
504
Lưu trữ thông tin thiết lập kết nối
506
Thông báo L3 ban đầu với ID người dùng, KSI, v.v.
508
Xác thực và thoả thuận khoá (AKA)
510
Xác định các thuật toán tính toàn vẹn và lập mã được phép
512
Lệnh chế độ bảo mật AS (thuật toán tính toàn vẹn, IK, thuật toán lập mã, CK, v.v.)
514
Chọn thuật toán tính toàn vẹn và lập mã, Tạo ra RAND, Bắt đầu bảo vệ tính toàn vẹn
516
Lệnh chế độ bảo mật AS (tính năng bảo mật của AT, thuật toán tính toàn vẹn, thuật toán lập mã, RAND, MAC-I)
A
B
C

FIG.5A

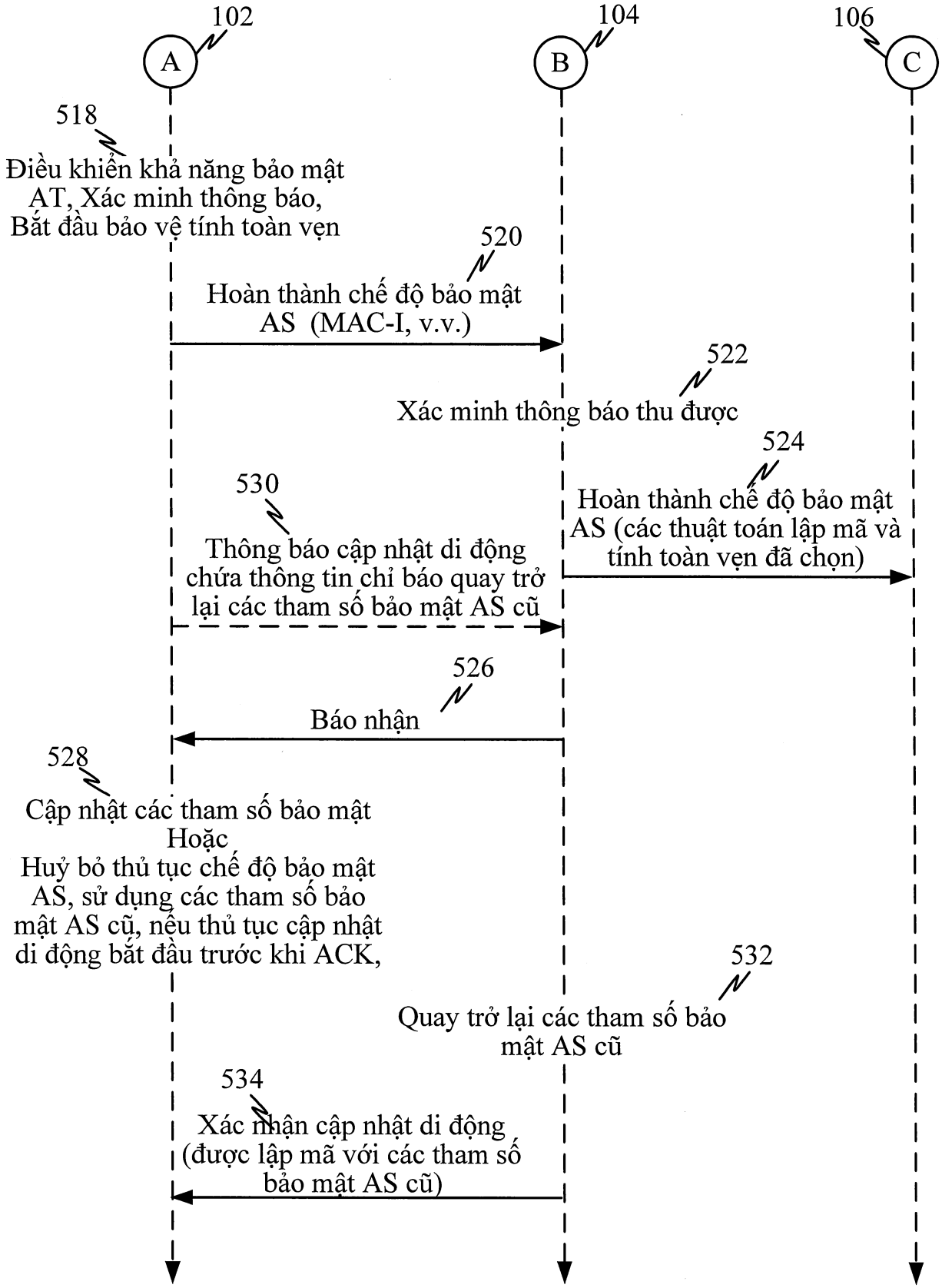

102
104
106
A
B
C
518
Điều khiển khả năng bảo mật AT, Xác minh thông báo, Bắt đầu bảo vệ tính toàn vẹn
520
Hoàn thành chế độ bảo mật AS (MAC-I, v.v.)
522
Xác minh thông báo thu được
524
Hoàn thành chế độ bảo mật AS (các thuật toán lập mã và tính toàn vẹn đã chọn)
530
Thông báo cập nhật di động chứa thông tin chỉ báo quay trở lại các tham số bảo mật AS cũ
526
Báo nhận
528
Cập nhật các tham số bảo mật
Hoặc
Huỷ bỏ thủ tục chế độ bảo mật AS, sử dụng các tham số bảo mật AS cũ, nếu thủ tục cập nhật di động bắt đầu trước khi ACK,
532
Quay trở lại các tham số bảo mật AS cũ
534
Xác nhận cập nhật di động (được lập mã với các tham số bảo mật AS cũ)

FIG.5B

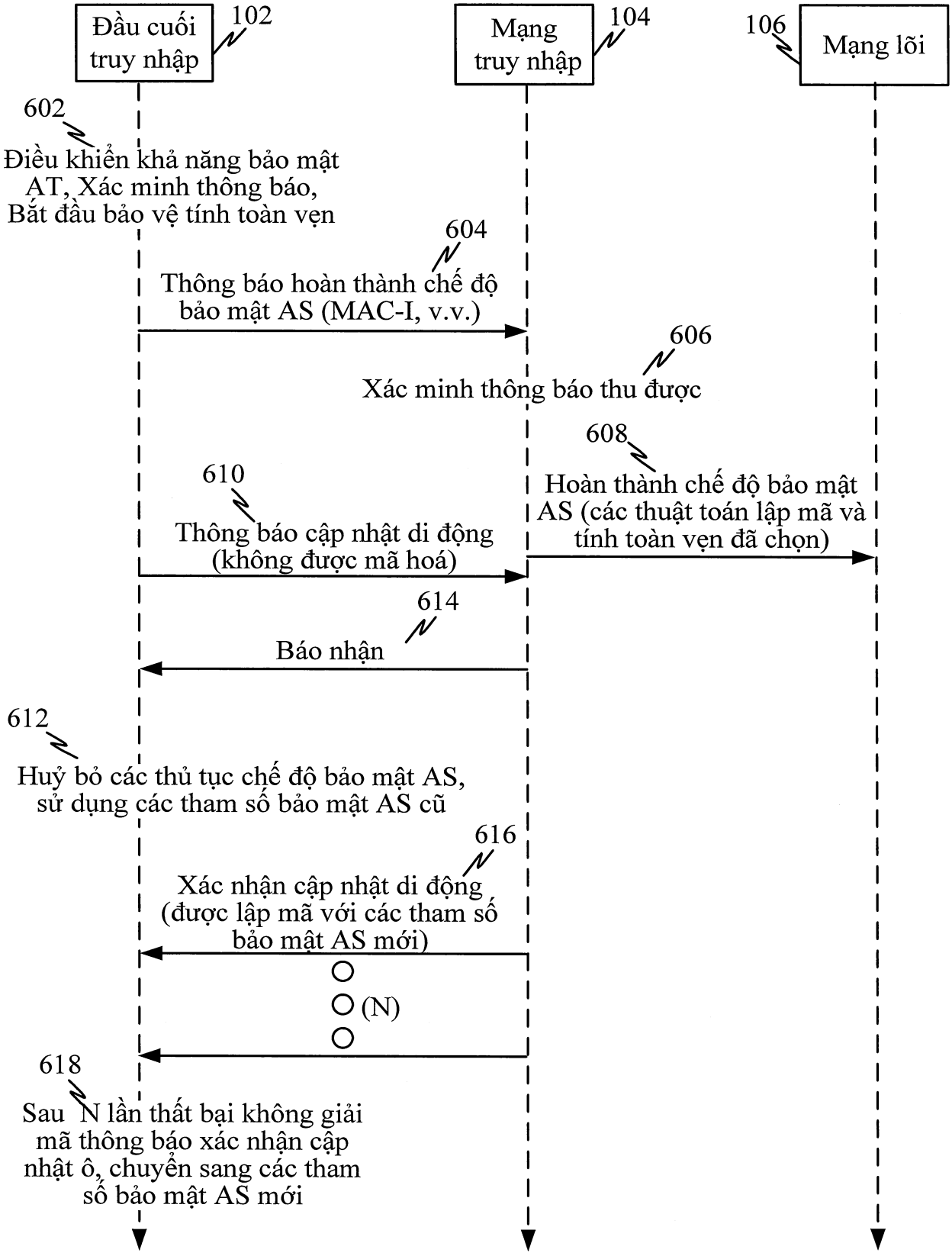

Đầu cuối truy nhập
102
Mạng truy nhập
104
106
Mạng lõi
602
Điều khiển khả năng bảo mật AT, Xác minh thông báo, Bắt đầu bảo vệ tính toàn vẹn
604
Thông báo hoàn thành chế độ bảo mật AS (MAC-I, v.v.)
606
Xác minh thông báo thu được
608
Hoàn thành chế độ bảo mật AS (các thuật toán lập mã và tính toàn vẹn đã chọn)
610
Thông báo cập nhật di động (không được mã hoá)
614
Báo nhận
612
Huỷ bỏ các thủ tục chế độ bảo mật AS, sử dụng các tham số bảo mật AS cũ
616
Xác nhận cập nhật di động (được lập mã với các tham số bảo mật AS mới)
(N)
618
Sau N lần thất bại không giải mã thông báo xác nhận cập nhật ô, chuyển sang các tham số bảo mật AS mới

FIG.6

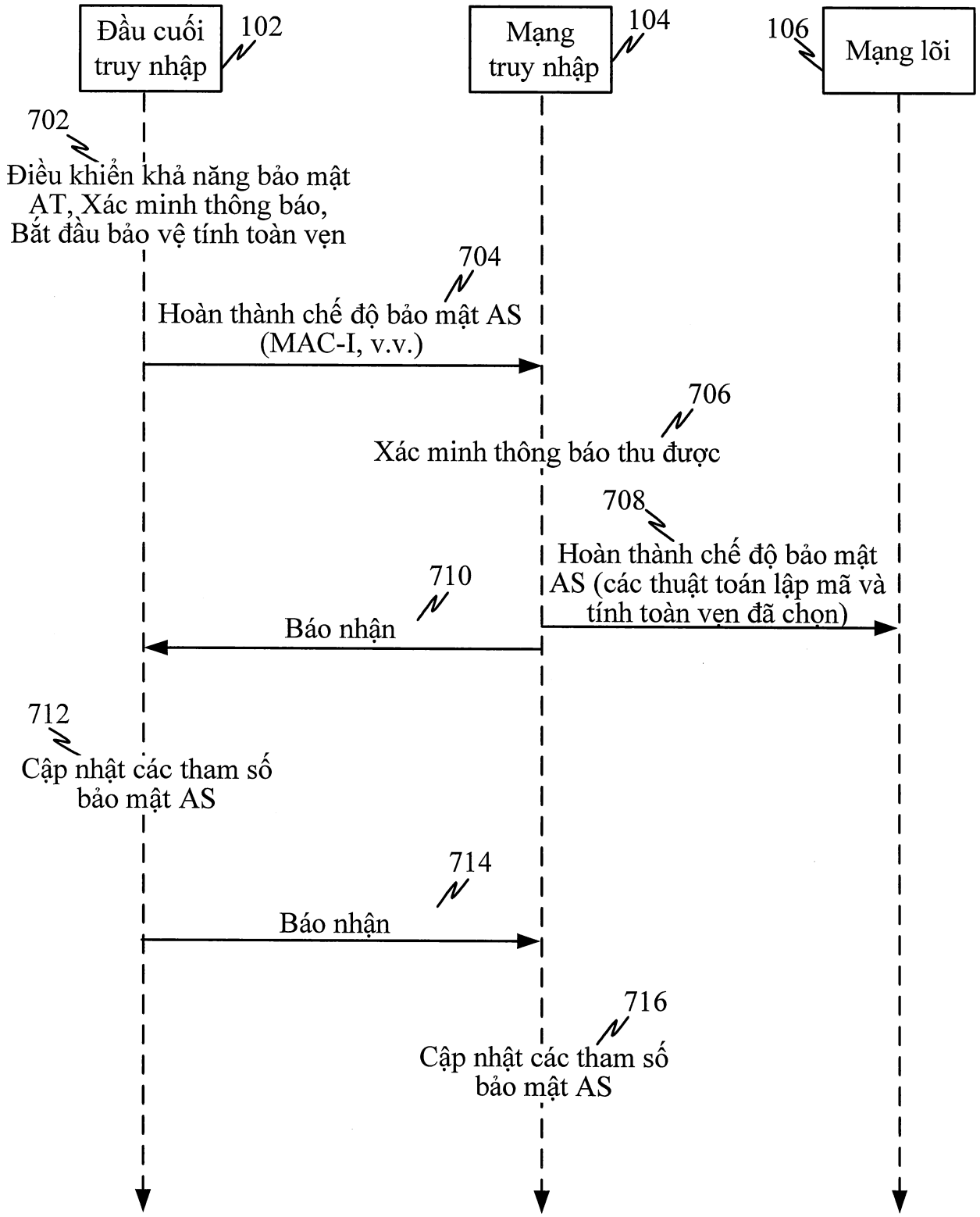

Đầu cuối truy nhập
102
Mạng truy nhập
104
106
Mạng lõi
702
Điều khiển khả năng bảo mật AT, Xác minh thông báo, Bắt đầu bảo vệ tính toàn vẹn
704
Hoàn thành chế độ bảo mật AS (MAC-I, v.v.)
706
Xác minh thông báo thu được
708
Hoàn thành chế độ bảo mật AS (các thuật toán lập mã và tính toàn vẹn đã chọn)
710
Báo nhận
712
Cập nhật các tham số bảo mật AS
714
Báo nhận
716
Cập nhật các tham số bảo mật AS

FIG.7

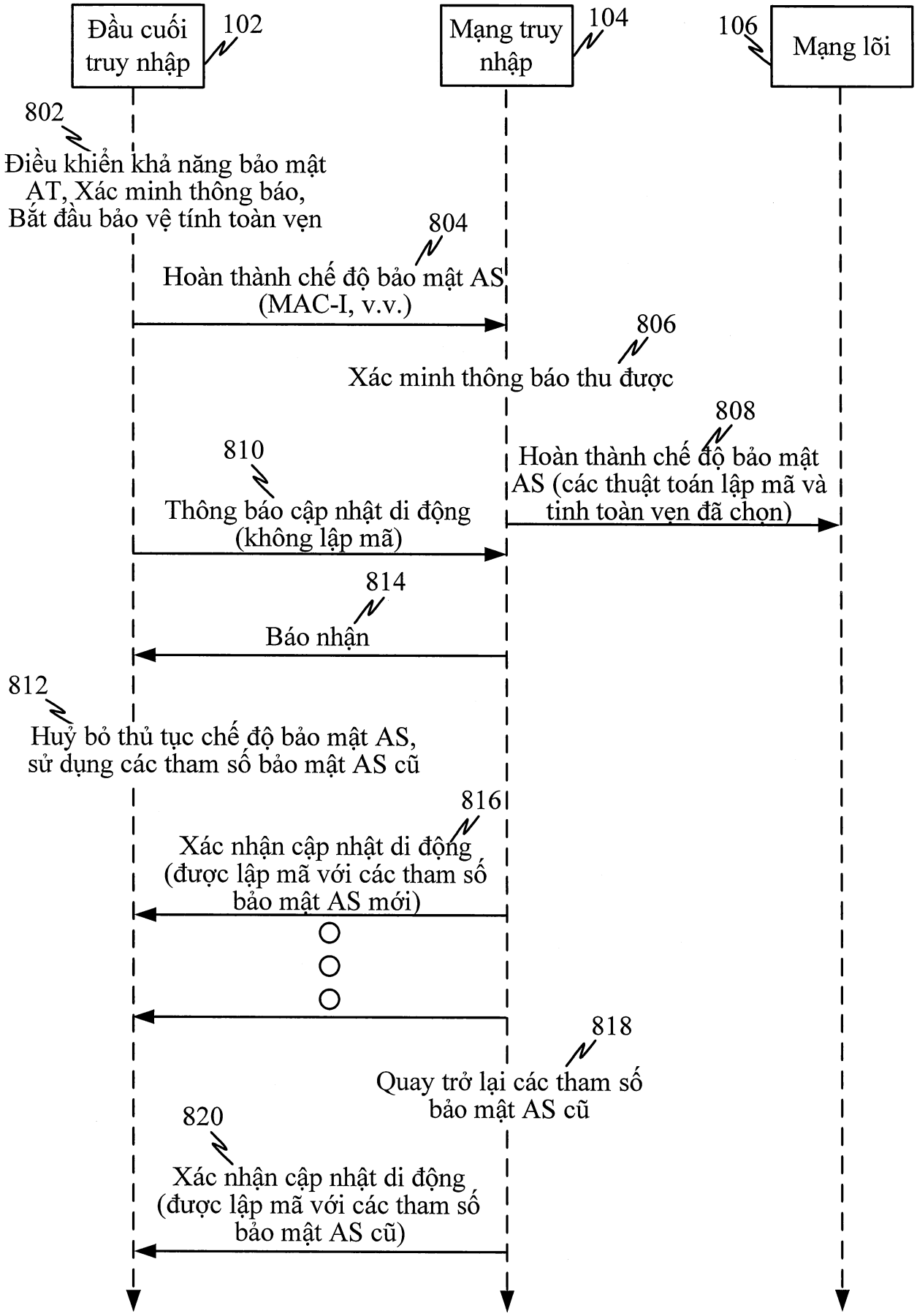

Đầu cuối truy nhập
102
Mạng truy nhập
104
106
Mạng lõi
802
Điều khiển khả năng bảo mật AT, Xác minh thông báo, Bắt đầu bảo vệ tính toàn vẹn
804
Hoàn thành chế độ bảo mật AS (MAC-I, v.v.)
806
Xác minh thông báo thu được
808
Hoàn thành chế độ bảo mật AS (các thuật toán lập mã và tính toàn vẹn đã chọn)
810
Thông báo cập nhật di động (không lập mã)
814
Báo nhận
812
Huỷ bỏ thủ tục chế độ bảo mật AS, sử dụng các tham số bảo mật AS cũ
816
Xác nhận cập nhật di động (được lập mã với các tham số bảo mật AS mới)
818
Quay trở lại các tham số bảo mật AS cũ
820
Xác nhận cập nhật di động (được lập mã với các tham số bảo mật AS cũ)

FIG.8

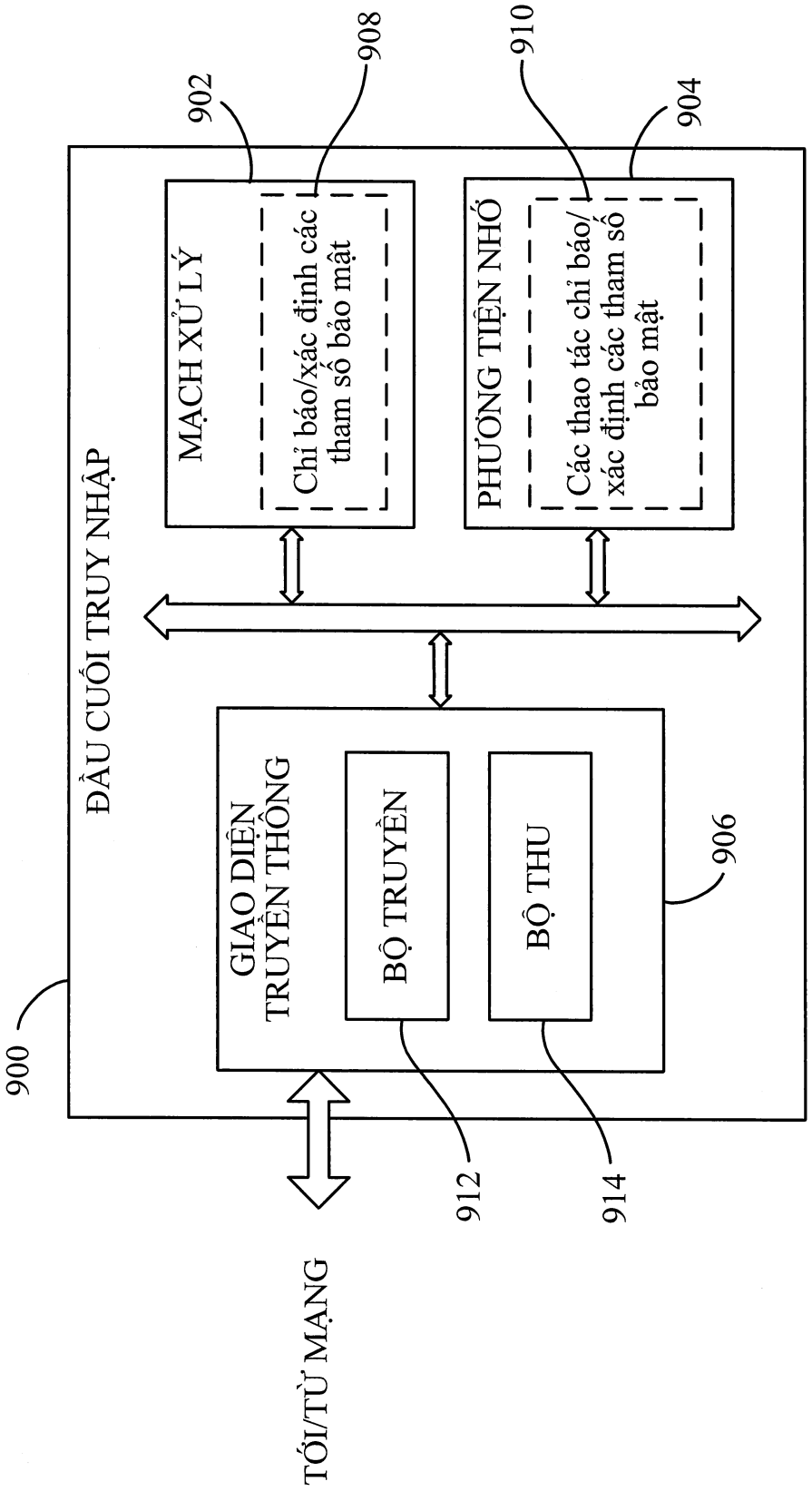

ĐẦU CUỐI TRUY NHẬP
MẠCH XỬ LÝ
Chỉ báo/xác định các tham số bảo mật
PHƯƠNG TIỆN NHỚ
Các thao tác chỉ báo/ xác định các tham số bảo mật
GIAO DIỆN TRUYỀN THÔNG
BỘ TRUYỀN
BỘ THU
TỚI/TỪ MẠNG
900
902
904
906
908
910
912
914

FIG.9

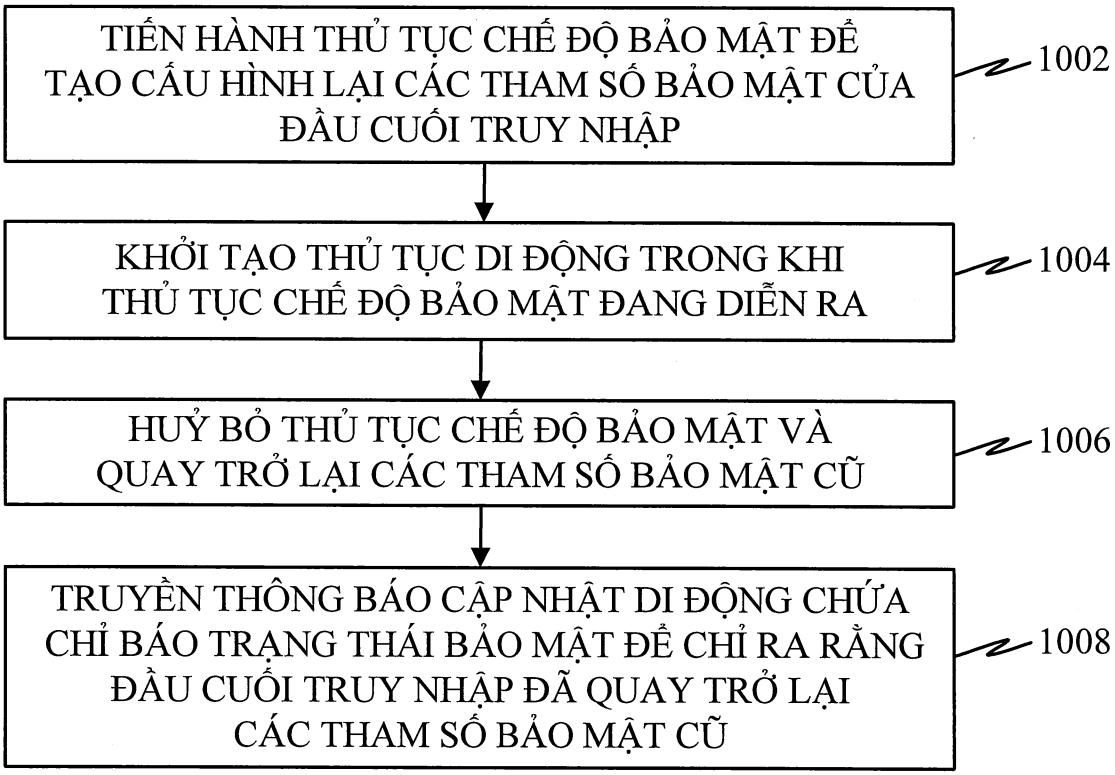

TIẾN HÀNH THỦ TỤC CHẾ ĐỘ BẢO MẬT ĐỂ TẠO CẤU HÌNH LẠI CÁC THAM SỐ BẢO MẬT CỦA ĐẦU CUỐI TRUY NHẬP
1002
KHỞI TẠO THỦ TỤC DI ĐỘNG TRONG KHI THỦ TỤC CHẾ ĐỘ BẢO MẬT ĐANG DIỄN RA
1004
HUỶ BỎ THỦ TỤC CHẾ ĐỘ BẢO MẬT VÀ QUAY TRỞ LẠI CÁC THAM SỐ BẢO MẬT CŨ
1006
TRUYỀN THÔNG BÁO CẬP NHẬT DI ĐỘNG CHỨA CHỈ BÁO TRẠNG THÁI BẢO MẬT ĐỂ CHỈ RA RẰNG ĐẦU CUỐI TRUY NHẬP ĐÃ QUAY TRỞ LẠI CÁC THAM SỐ BẢO MẬT CŨ
1008

FIG.10

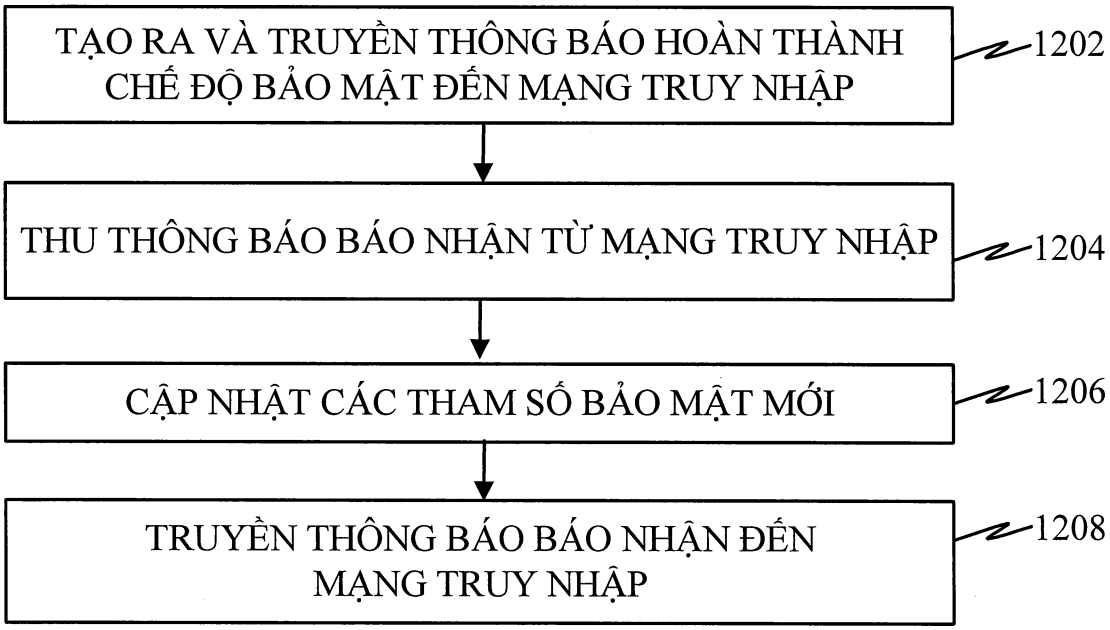

TẠO RA VÀ TRUYỀN THÔNG BÁO HOÀN THÀNH CHẾ ĐỘ BẢO MẬT ĐẾN MẠNG TRUY NHẬP
1202
THU THÔNG BÁO BÁO NHẬN TỪ MẠNG TRUY NHẬP
1204
CẬP NHẬT CÁC THAM SỐ BẢO MẬT MỚI
1206
TRUYỀN THÔNG BÁO BÁO NHẬN ĐẾN MẠNG TRUY NHẬP
1208

FIG.12

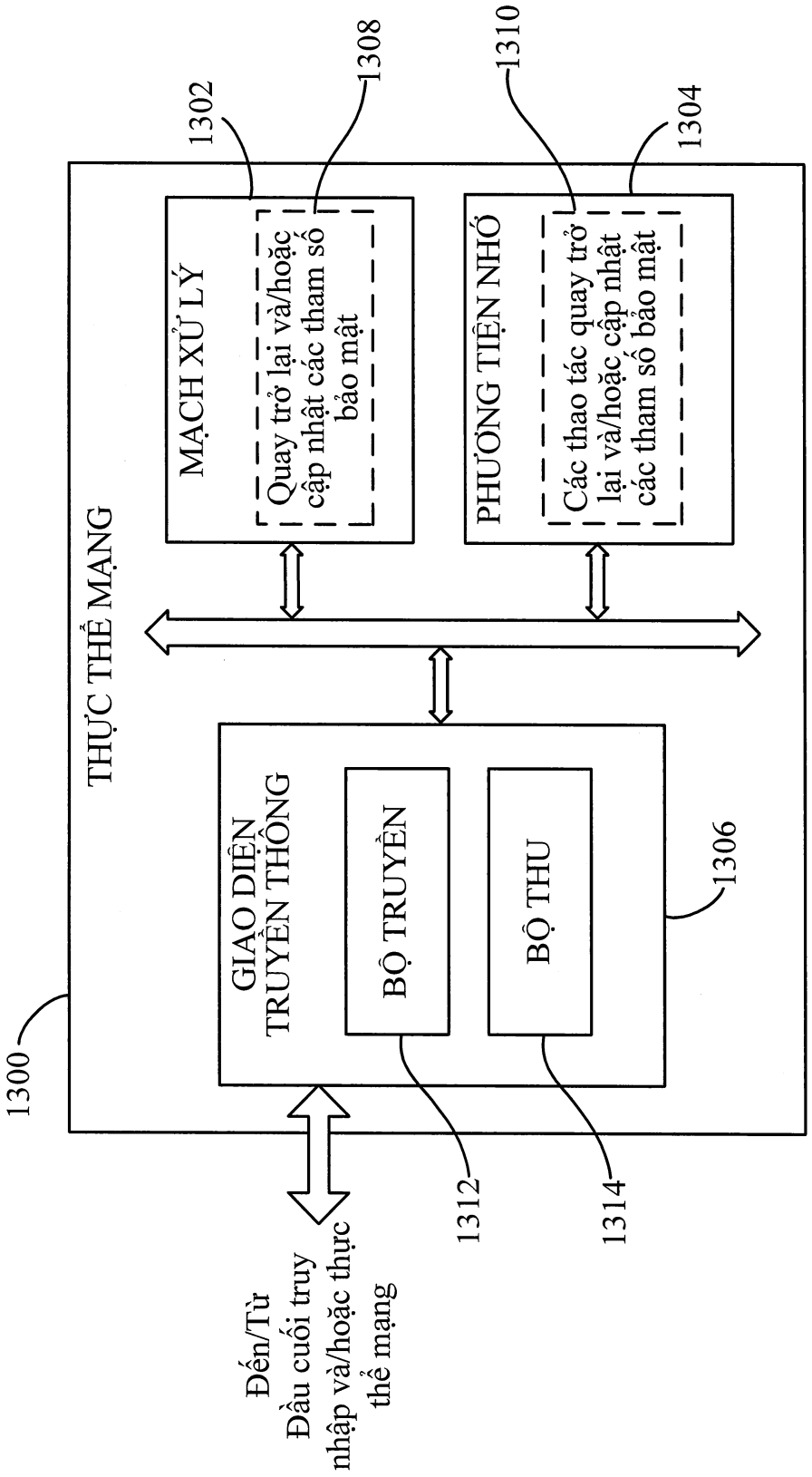

1300
THỰC THỂ MẠNG
1302
MẠCH XỬ LÝ
Quay trở lại và/hoặc cập nhật các tham số bảo mật
1308
1310
PHƯƠNG TIỆN NHỚ
Các thao tác quay trở lại và/hoặc cập nhật các tham số bảo mật
1304
GIAO DIỆN TRUYỀN THÔNG
BỘ TRUYỀN
BỘ THU
1306
1312
1314
Đến/Từ Đầu cuối truy nhập và/hoặc thực thể mạng

FIG.13

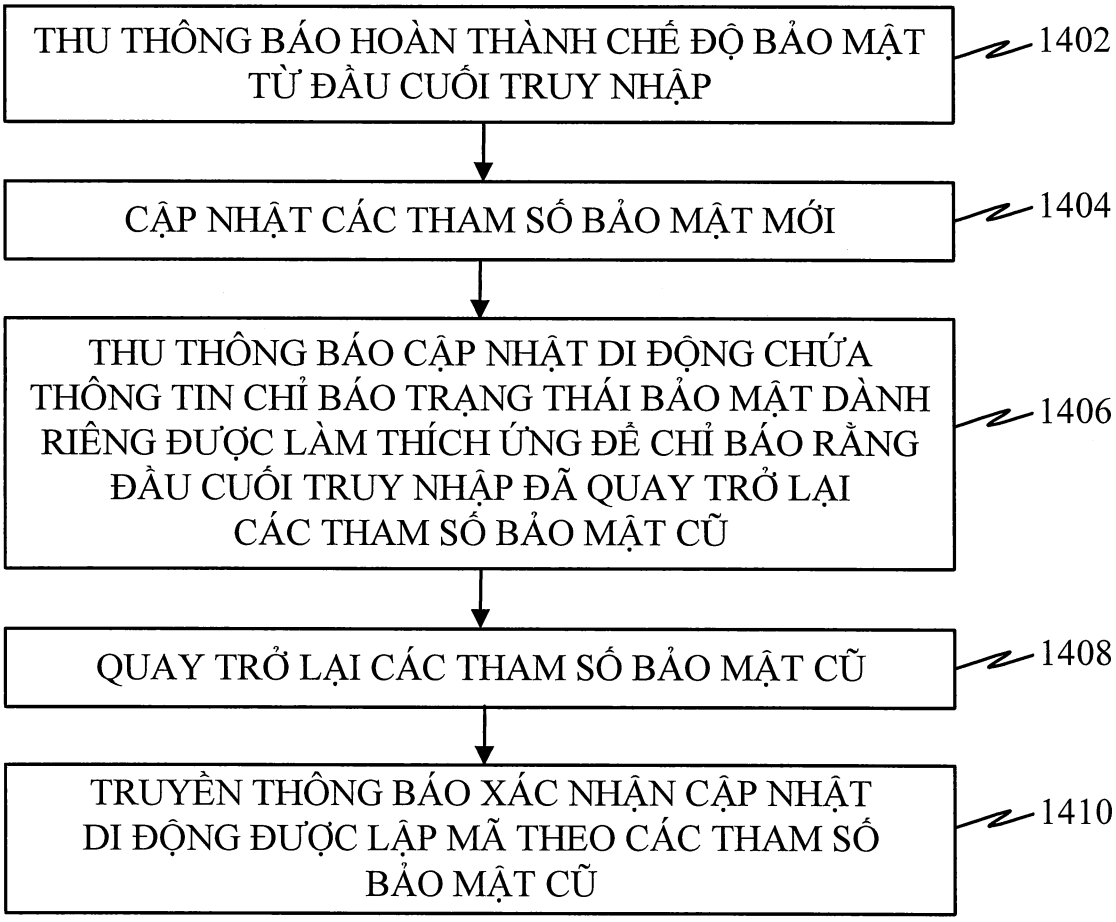

THU THÔNG BÁO HOÀN THÀNH CHẾ ĐỘ BẢO MẬT TỪ ĐẦU CUỐI TRUY NHẬP
1402
CẬP NHẬT CÁC THAM SỐ BẢO MẬT MỚI
1404
THU THÔNG BÁO CẬP NHẬT DI ĐỘNG CHỨA THÔNG TIN CHỈ BÁO TRẠNG THÁI BẢO MẬT DÀNH RIÊNG ĐƯỢC LÀM THÍCH ỨNG ĐỂ CHỈ BÁO RẰNG ĐẦU CUỐI TRUY NHẬP ĐÃ QUAY TRỞ LẠI CÁC THAM SỐ BẢO MẬT CŨ
1406
QUAY TRỞ LẠI CÁC THAM SỐ BẢO MẬT CŨ
1408
TRUYỀN THÔNG BÁO XÁC NHẬN CẬP NHẬT DI ĐỘNG ĐƯỢC LẬP MÃ THEO CÁC THAM SỐ BẢO MẬT CŨ
1410

FIG.14

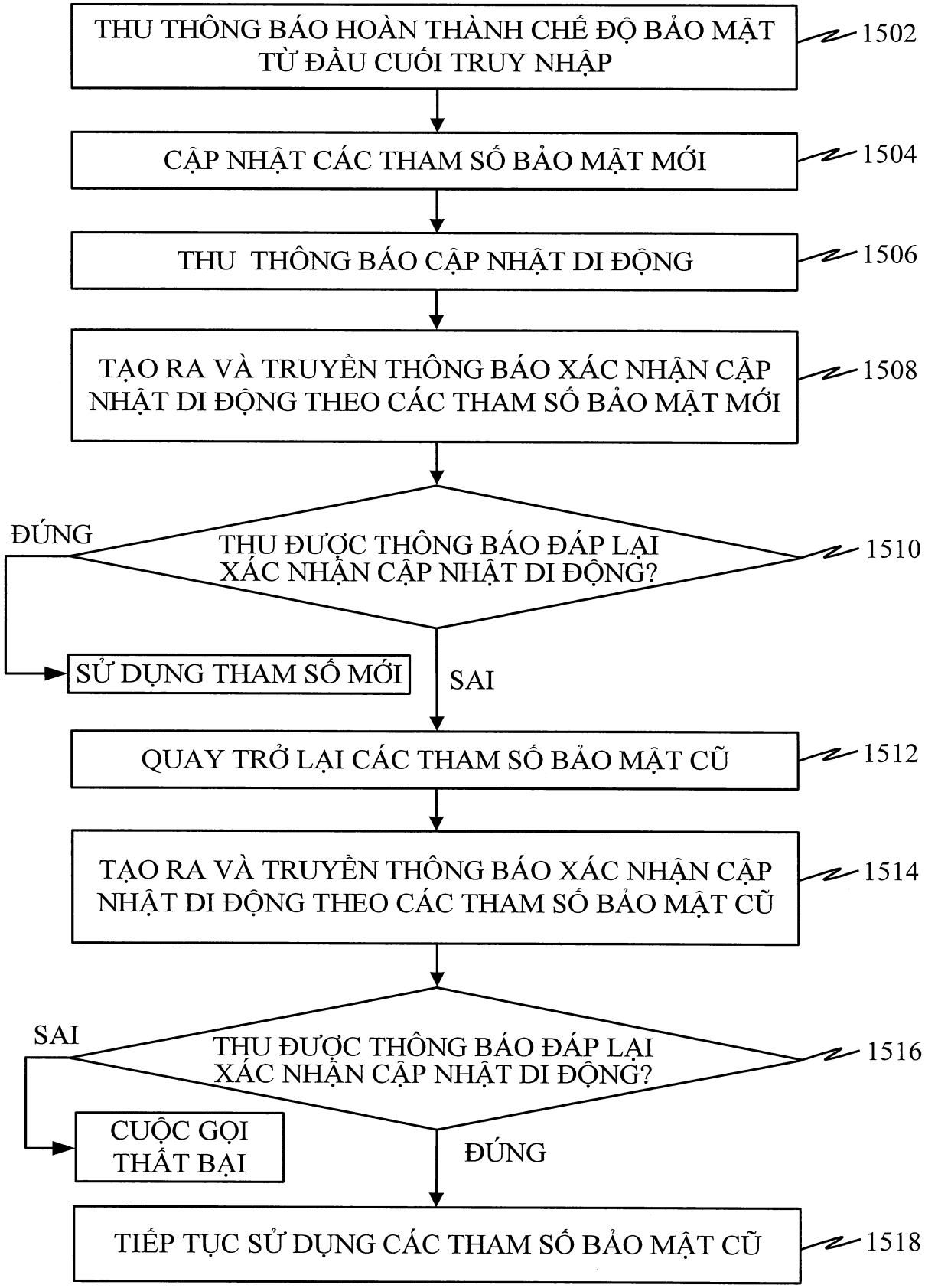

THU THÔNG BÁO HOÀN THÀNH CHẾ ĐỘ BẢO MẬT TỪ ĐẦU CUỐI TRUY NHẬP
1502
CẬP NHẬT CÁC THAM SỐ BẢO MẬT MỚI
1504
THU THÔNG BÁO CẬP NHẬT DI ĐỘNG
1506
TẠO RA VÀ TRUYỀN THÔNG BÁO XÁC NHẬN CẬP NHẬT DI ĐỘNG THEO CÁC THAM SỐ BẢO MẬT MỚI
1508
ĐÚNG
THU ĐƯỢC THÔNG BÁO ĐÁP LẠI XÁC NHẬN CẬP NHẬT DI ĐỘNG?
1510
SỬ DỤNG THAM SỐ MỚI
SAI
QUAY TRỞ LẠI CÁC THAM SỐ BẢO MẬT CŨ
1512
TẠO RA VÀ TRUYỀN THÔNG BÁO XÁC NHẬN CẬP NHẬT DI ĐỘNG THEO CÁC THAM SỐ BẢO MẬT CŨ
1514
SAI
THU ĐƯỢC THÔNG BÁO ĐÁP LẠI XÁC NHẬN CẬP NHẬT DI ĐỘNG?
1516
CUỘC GỌI THẤT BẠI
ĐÚNG
TIẾP TỤC SỬ DỤNG CÁC THAM SỐ BẢO MẬT CŨ
1518

FIG.15

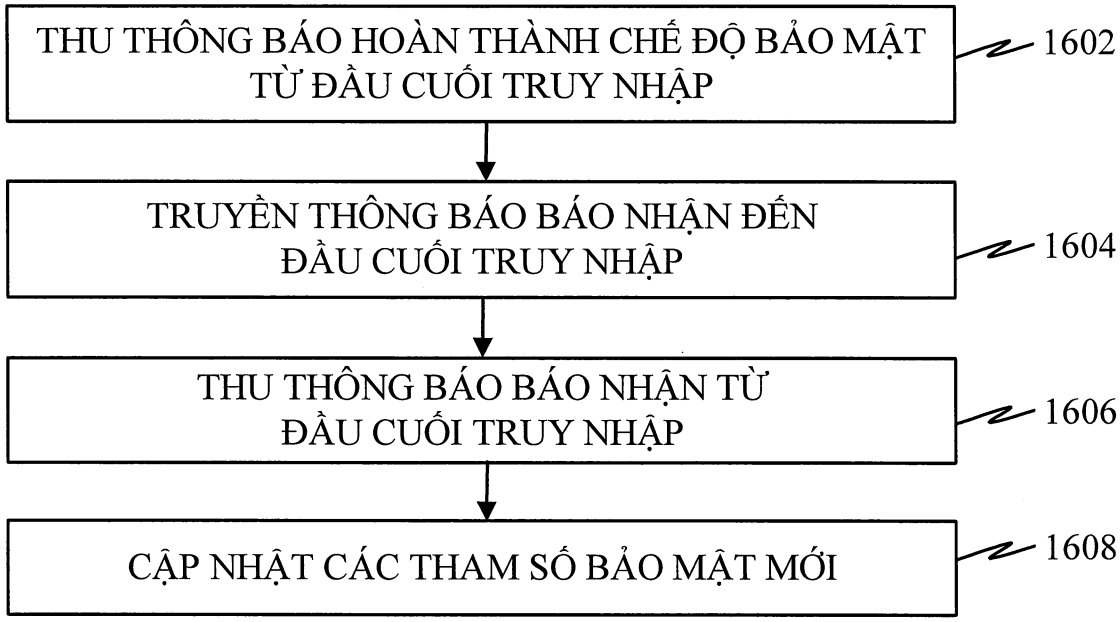

THU THÔNG BÁO HOÀN THÀNH CHẾ ĐỘ BẢO MẬT TỪ ĐẦU CUỐI TRUY NHẬP
1602
TRUYỀN THÔNG BÁO BÁO NHẬN ĐẾN ĐẦU CUỐI TRUY NHẬP
1604
THU THÔNG BÁO BÁO NHẬN TỪ ĐẦU CUỐI TRUY NHẬP
1606
CẬP NHẬT CÁC THAM SỐ BẢO MẬT MỚI
1608

FIG.16