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

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

(11) **1-0050282**

(51)[2021.01] **H04W 12/041**; H04W 12/08; H04W 12/06; H04L 9/32

(13) **B**

(21) 1-2022-02091
(22) 09/10/2020
(86) PCT/US2020/055021 09/10/2020
(87) WO 2021/072223 A1 15/04/2021
(30) 62/914,335 11/10/2019 US; 17/066,014 08/10/2020 US
(45) 25/08/2025 449
(43) 25/07/2022 412A
(73) QUALCOMM INCORPORATED (US)
ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, CA 92121-1714, United States of America
(72) LEE, Soo Bum (KR); HORN, Gavin Bernard (US); AGARWAL, Ravi (US).
(74) Công ty TNHH Quốc tế D &N (D&N INTERNATIONAL CO.,LTD.)

(54) PHƯƠNG PHÁP VÀ MÁY ĐỂ TRUYỀN THÔNG KHÔNG DÂY

(21) 1-2022-02091

(57) Sáng chế đề cập đến các phương pháp, hệ thống, máy và thiết bị để truyền thông không dây. Các khóa riêng tư có thể được duy trì ở hướng lên trong mạng tại vị trí an toàn hơn. Ví dụ, khi cần chữ ký, trạm gốc có thể truyền yêu cầu ký đến chức năng ký trong mạng lõi và có thể truyền thông tin hệ thống (system information - SI) cần được bảo vệ. Chức năng ký có thể sử dụng khóa riêng tư để tạo ra chữ ký cho SI và trả lại chữ ký cho trạm gốc. Trạm gốc có thể truyền SI và chữ ký đến thiết bị người dùng (user equipment - UE) trong vùng phủ sóng của trạm gốc. Các UE có thể thu được khóa công khai tương ứng với khóa riêng tư và có thể sử dụng khóa công khai để xác minh rằng chữ ký cho SI là hợp lệ và đến từ trạm gốc. Khóa công khai, và do đó cả chữ ký, có thể tương ứng với vùng theo dõi cụ thể.

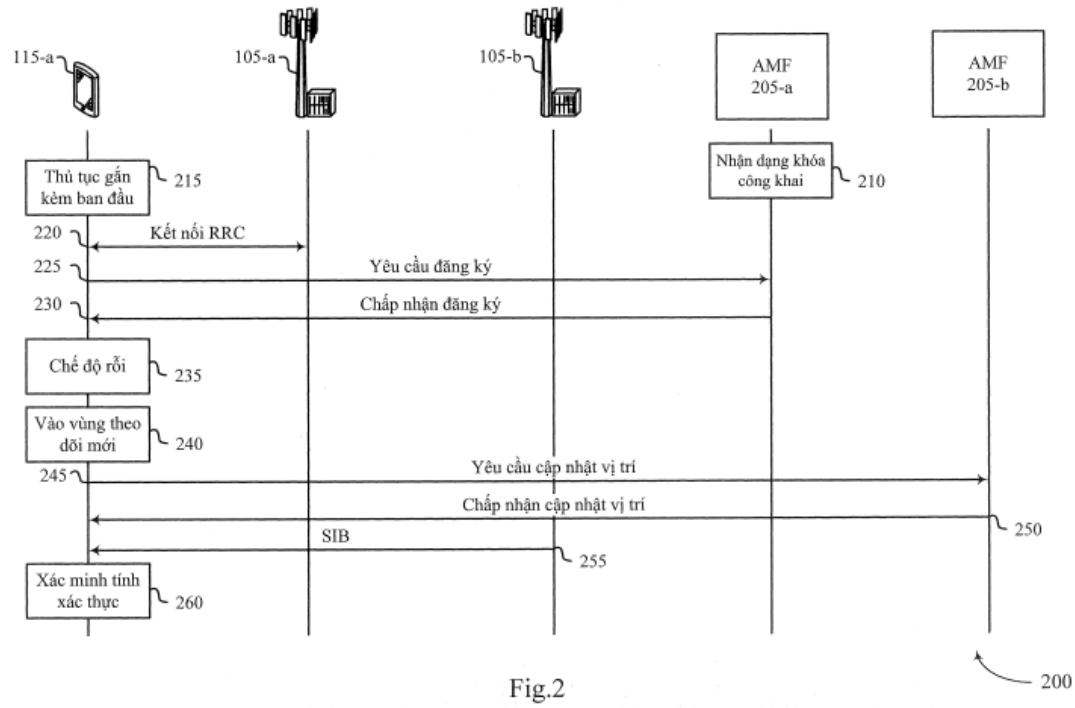


Fig.2

**Lĩnh vực kỹ thuật được đề cập**

Sáng chế đề cập đến truyền thông không dây và cụ thể hơn là đề cập đến việc bảo vệ thông tin hệ thống (system information - SI) tại chức năng mạng (network function - NF) trong mạng lõi.

**Tình trạng kỹ thuật của sáng chế**

Các hệ thống truyền thông không dây được triển khai rộng rãi để cung cấp các loại nội dung truyền thông khác nhau như thoại, viđeo, dữ liệu gói, gửi tin nhắn, phát quảng bá, và tương tự. Các hệ thống này có thể có khả năng hỗ trợ truyền thông với nhiều người dùng bằng cách dùng chung tài nguyên hệ thống sẵn có (ví dụ, thời gian, tần số, và công suất). Ví dụ về các hệ thống đa truy cập như vậy bao gồm các hệ thống thế hệ thứ tư (fourth generation - 4G) như hệ thống phát triển dài hạn (Long Term Evolution - LTE) hoặc hệ thống LTE nâng cao (LTE-Advanced - LTE-A), hoặc hệ thống LTE-A Pro, và hệ thống thế hệ thứ năm (fifth generation - 5G) mà có thể được gọi là hệ thống vô tuyến mới (New Radio - NR). Các hệ thống này có thể sử dụng các công nghệ như đa truy cập phân chia theo mã (code division multiple access - CDMA), đa truy cập phân chia theo thời gian (time division multiple access - TDMA), đa truy cập phân chia theo tần số (frequency division multiple access - FDMA), đa truy cập phân chia theo tần số trực giao (orthogonal frequency division multiple access - OFDMA), hoặc ghép kênh phân chia theo tần số trực giao trải phổ biến đổi Fourier rời rạc (discrete Fourier transform spread orthogonal frequency division multiplexing - DFT-S-OFDM). Hệ thống truyền thông đa truy cập không dây có thể bao gồm một hoặc nhiều trạm gốc hoặc một hoặc nhiều nút truy cập mạng, mỗi trạm hoặc nút hỗ trợ đồng thời việc truyền thông cho nhiều thiết bị truyền thông, mà còn có thể được gọi là thiết bị người dùng (user equipment - UE).

Trong một số hệ thống truyền thông không dây, thực thể mạng có thể sử dụng một hoặc nhiều khóa bảo mật để hỗ trợ truyền thông an toàn qua mạng (ví dụ, giữa UE và trạm gốc). Khóa bảo mật có thể được suy ra từ một số tham số hoặc hàm dẫn xuất khóa (key derivation function - KDF). Trước khi thiết lập và sử dụng các khóa bảo mật, thông tin hệ thống (SI) có thể được truyền từ trạm gốc đến UE để cung cấp cho UE thông tin về hệ thống và trạm gốc cho phép các cuộc truyền thông tiếp theo (ví dụ, như tín hiệu để

thiết lập kết nối cho các cuộc truyền thông an toàn). Tuy nhiên, SI này có thể không được bảo vệ khi được truyền đến UE (ví dụ, SI không được mã hóa), tạo cơ hội cho kẻ tấn công (attacker) có cơ hội đóng giả làm trạm gốc và cung cấp thông tin giả cho UE, ảnh hưởng đến khả năng của UE trong việc thiết lập kết nối với mạng (ví dụ, như một phần của cuộc tấn công từ chối dịch vụ (denial of service - DoS)).

**Bản chất kỹ thuật của sáng chế**

Các kỹ thuật được mô tả đề cập đến các phương pháp, hệ thống, thiết bị, và máy để hỗ trợ bảo vệ thông tin hệ thống (SI) tại chức năng mạng (NF) trong mạng lõi. Nói chung, các kỹ thuật được mô tả đề cập đến việc lưu trữ các cặp khóa riêng tư-khóa công khai tại nút mạng (ví dụ, tại NF ký được triển khai ảo trong phần mềm trong mạng lõi) mà thiết bị người dùng (UE) có thể sử dụng để xác minh chữ ký của bản tin SI (ví dụ, khối SI (SI block - SIB), SIB bảo mật, khối thông tin chính (master information block - MIB), v.v.) mà đã được truyền bởi trạm gốc. Trong một số trường hợp, trạm gốc có thể truyền yêu cầu chữ ký đến nút mạng (ví dụ, nút mạng lõi) bao gồm SI và có thể nhận đáp ứng chữ ký từ nút mạng bao gồm chữ ký đã được tạo ra dựa vào SI (ví dụ, tương ứng với cặp khóa công khai-khóa riêng tư). Sau đó, trạm gốc có thể truyền bản tin SI (ví dụ, qua bản tin được phát quảng bá) bao gồm SI và chữ ký được tạo ra. Trước khi nhận bản tin SI, UE có thể được cung cấp một hoặc nhiều khóa công khai được tạo ra bởi nút mạng qua chức năng quản lý truy cập và di động (AMF) khi đăng ký với mạng. Do đó, khi bản tin SI được phát hiện và nhận tại UE, UE có thể sử dụng các khóa công khai được cung cấp để xác minh chữ ký và xác định rằng bản tin SI nhận được đã được truyền bởi trạm gốc (ví dụ, và không phải tin tặc, kẻ tấn công, trạm gốc giả, v.v.).

Trong một số trường hợp, trạm gốc có thể truyền yêu cầu chữ ký hàng loạt đến nút mạng yêu cầu một số chữ ký cho thời gian cho trước (ví dụ, chữ ký dựa vào thời gian). Ngoài ra hoặc theo cách khác, yêu cầu chữ ký hàng loạt có thể bao gồm thông số độ mới (ví dụ, thông số truy cập gần đây (recency parameter), số khung hệ thống (system frame number - SFN), v.v.), trong đó các chữ ký được tạo ra tại nút mạng dựa vào thông số độ mới (ví dụ, chữ ký được cung cấp dựa vào SFN được yêu cầu). Trong một số trường hợp, trạm gốc có thể liên tục nhận các chữ ký được cập nhật từ nút mạng hoặc có thể yêu cầu các chữ ký mới khi các bản tin SI được thay đổi tại trạm gốc. Ngoài ra, khóa công khai có thể bao gồm mã định danh (identifier - ID) khóa tương ứng với vùng theo

dõi (ví dụ, vùng địa lý cho mạng trong đó khóa công khai là hợp lệ). Do đó, nút mạng có thể cung cấp các bộ gồm ID khóa và khóa công khai tương ứng cho UE khi UE đăng ký với mạng (ví dụ, qua bản tin chấp nhận đăng ký) để cho phép UE xác minh bản tin SI và chữ ký được phát quảng bá bởi trạm gốc cùng với ID khóa. Do đó, các bản tin chữ ký được cung cấp cho trạm gốc (ví dụ, bởi nút mạng, nút mạng lõi, NF ký, v.v.) cũng có thể mang ID khóa để cho phép trạm gốc phát quảng bá ID khóa cùng với bản tin SI và chữ ký. Trong một số trường hợp, AMF có thể được cung cấp nhiều khóa công khai tương ứng với các vùng theo dõi lân cận sao cho nếu UE vào vùng theo dõi mới, UE có thể xác minh bản tin SI mà không phải nhận các khóa công khai mới.

Sáng chế đề xuất phương pháp truyền thông không dây bởi trạm gốc. Phương pháp này có thể bao gồm bước truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI, nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI, và truyền bản tin SI bao gồm SI và chữ ký.

Sáng chế đề xuất máy để truyền thông không dây bởi trạm gốc. Máy này có thể bao gồm bộ xử lý, bộ nhớ được ghép nối với bộ xử lý, và các lệnh được lưu trữ trong bộ nhớ. Các lệnh này có thể thực thi được bởi bộ xử lý để khiến cho máy truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI, nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI, và truyền bản tin SI bao gồm SI và chữ ký.

Sáng chế đề xuất máy khác để truyền thông không dây bởi trạm gốc. Máy này có thể bao gồm phương tiện để truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI, nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI, và truyền bản tin SI bao gồm SI và chữ ký.

Sáng chế đề xuất phương tiện bất biến đọc được bằng máy tính lưu trữ mã để truyền thông không dây bởi trạm gốc. Mã này có thể bao gồm các lệnh thực thi được bởi bộ xử lý để truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI, nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI, và truyền bản tin SI bao gồm SI và chữ ký.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc truyền yêu cầu chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền yêu cầu chữ ký bao gồm SI và thông tin chính, trong đó chữ ký có thể được tạo ra dựa vào SI và thông tin chính.

Một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây còn có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền bản tin SI chỉ báo ID của khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký.

Một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây còn có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền, đến nút mạng, yêu cầu chữ ký thứ hai bao gồm SI cập nhật, nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký thứ hai được tạo ra dựa vào SI cập nhật, và truyền bản tin SI bao gồm SI cập nhật và chữ ký thứ hai.

Một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây còn có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận yêu cầu đăng ký từ UE, truyền yêu cầu đăng ký đến nút mạng cung cấp AMF, nhận, từ nút mạng, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký, và truyền đáp ứng đăng ký đến UE.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc truyền đáp ứng đăng ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền đáp ứng đăng ký bao gồm vùng theo dõi thứ nhất cho khóa công khai thứ nhất.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc truyền đáp ứng đăng ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền đáp ứng đăng ký chỉ báo khóa công khai thứ hai cho vùng theo dõi thứ hai mà có thể được định vị địa lý so với vùng theo dõi thứ nhất, khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai được truyền trong vùng theo dõi thứ hai.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc nhận yêu cầu đăng ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận yêu cầu cập nhật đăng ký di động từ UE chỉ báo rằng UE có thể đã vào vùng theo dõi mới.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc truyền yêu cầu chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền yêu cầu chữ ký để yêu cầu tập hợp chữ ký cho

phạm vi thời gian và khoảng tăng thời gian.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc nhận đáp ứng chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận đáp ứng chữ ký bao gồm tập hợp chữ ký.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc nhận đáp ứng chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận tập hợp đáp ứng chữ ký, trong đó mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều tập hợp chữ ký. Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, mỗi trong số các tập con tương ứng với khoảng tăng thời gian riêng trong phạm vi thời gian.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc truyền yêu cầu chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền yêu cầu chữ ký chỉ báo khoảng tăng khung con và yêu cầu tập hợp chữ ký tương ứng với phạm vi số khung con giữa số khung con bắt đầu và số khung con kết thúc.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc nhận đáp ứng chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận đáp ứng chữ ký bao gồm tập hợp chữ ký.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc nhận đáp ứng chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận tập hợp đáp ứng chữ ký, trong đó mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều tập hợp chữ ký. Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, mỗi trong số các tập con tương ứng với khoảng tăng khung con trong phạm vi số khung con.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc truyền yêu cầu chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền yêu cầu chữ ký bao gồm thông số truy cập gần đây.

Một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây còn có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký mà có thể được tạo ra dựa vào SI và thông số truy cập gần đây. Theo một số ví dụ về phương pháp, máy và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, thông số truy cập gần đây có thể là SFN.

Sáng chế đề xuất phương pháp truyền thông không dây bởi nút mạng. Phương pháp này có thể bao gồm bước nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI và truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI.

Sáng chế đề xuất máy để truyền thông không dây bởi nút mạng. Máy này có thể bao gồm bộ xử lý, bộ nhớ được ghép nối với bộ xử lý và các lệnh được lưu trữ trong bộ nhớ. Các lệnh này có thể thực thi được bởi bộ xử lý để khiến cho máy nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI và truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI.

Sáng chế đề xuất máy khác để truyền thông không dây bởi nút mạng. Máy này có thể bao gồm phương tiện để nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI và truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI.

Sáng chế đề xuất phương tiện bất biến đọc được bằng máy tính lưu trữ mã để truyền thông không dây bởi nút mạng. Mã này có thể bao gồm các lệnh thực thi được bởi bộ xử lý để nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI và truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc nhận yêu cầu chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận yêu cầu chữ ký bao gồm SI và thông tin chính, trong đó chữ ký có thể được tạo ra dựa vào SI và thông tin chính.

Một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây còn có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền bản tin ID khóa chỉ báo ID của khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký.

Một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy

tính được mô tả ở đây còn có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận, từ trạm gốc, yêu cầu chữ ký thứ hai bao gồm SI cập nhật, và truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký thứ hai được tạo ra dựa vào SI cập nhật.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc nhận yêu cầu chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận yêu cầu chữ ký mà yêu cầu tập hợp chữ ký cho phạm vi thời gian và khoảng tăng thời gian.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc truyền đáp ứng chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền đáp ứng chữ ký bao gồm tập hợp chữ ký. Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc truyền đáp ứng chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền tập hợp đáp ứng chữ ký, mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều tập hợp chữ ký. Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, mỗi trong số các tập con tương ứng với khoảng tăng thời gian trong phạm vi thời gian.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc nhận yêu cầu chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận yêu cầu chữ ký chỉ báo khoảng tăng khung con và yêu cầu tập hợp chữ ký tương ứng với phạm vi số khung con giữa số khung con bắt đầu và số khung con kết thúc.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc nhận đáp ứng chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận đáp ứng chữ ký bao gồm tập hợp chữ ký. Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc nhận đáp ứng chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận tập hợp đáp ứng chữ ký, trong đó mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều tập hợp chữ ký. Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, mỗi trong số các tập con tương ứng với khoảng tăng khung con trong phạm vi số khung con.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng

máy tính được mô tả ở đây, việc nhận yêu cầu chữ ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận yêu cầu chữ ký bao gồm thông số truy cập gần đây.

Một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây còn có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký mà có thể được tạo ra dựa vào SI và thông số truy cập gần đây. Theo một số ví dụ về phương pháp, máy và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, thông số truy cập gần đây có thể là SFN.

Sáng chế đề xuất phương pháp truyền thông không dây bởi UE. Phương pháp này có thể bao gồm bước truyền yêu cầu đăng ký đến nút mạng lõi, nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất, và giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai.

Sáng chế đề xuất máy để truyền thông không dây bởi UE. Máy này có thể bao gồm bộ xử lý, bộ nhớ được ghép nối với bộ xử lý, và các lệnh được lưu trữ trong bộ nhớ. Các lệnh này có thể thực thi được bởi bộ xử lý để khiến cho máy truyền yêu cầu đăng ký đến nút mạng lõi, nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất, và giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai.

Sáng chế đề xuất máy khác để truyền thông không dây bởi UE. Máy này có thể bao gồm phương tiện để truyền yêu cầu đăng ký đến nút mạng lõi, nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ

hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất, và giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai.

Sáng chế đề xuất phương tiện bất biến đọc được bằng máy tính lưu trữ mã dùng để truyền thông không dây bởi UE. Mã này có thể bao gồm các lệnh thực thi được bởi bộ xử lý để truyền yêu cầu đăng ký đến nút mạng lõi, nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất, và giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc giám sát bản tin SI có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất.

Một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây còn có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để xác minh SI thứ nhất dựa vào chữ ký thứ nhất, và thiết lập kết nối với trạm gốc trong vùng theo dõi thứ nhất dựa vào SI thứ nhất được xác minh.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc giám sát bản tin SI có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận bản tin SI bao gồm SI thứ hai và chữ ký thứ hai.

Một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây còn có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để xác minh SI thứ hai dựa vào chữ ký thứ hai, và thiết lập kết nối với trạm gốc trong vùng theo dõi thứ hai dựa vào SI thứ hai được xác minh.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc giám sát bản tin SI có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để nhận bản tin SI chỉ báo ID của khóa công khai thứ

nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất.

Theo một số ví dụ về phương pháp, máy, và phương tiện bất biến đọc được bằng máy tính được mô tả ở đây, việc truyền yêu cầu đăng ký có thể bao gồm các thao tác, dấu hiệu, phương tiện, hoặc các lệnh để truyền yêu cầu cập nhật đăng ký di động chỉ báo rằng UE có thể đã di chuyển từ vùng theo dõi thứ nhất đến vùng theo dõi thứ hai.

**Mô tả vắn tắt các hình vẽ**

Fig.1 minh họa ví dụ về hệ thống truyền thông không dây hỗ trợ bảo vệ thông tin hệ thống (SI) tại một chức năng mạng (NF) trong mạng lõi theo các khía cạnh của sáng chế.

Fig.2 minh họa ví dụ về xác thực ô hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

Fig.3 minh họa ví dụ về dòng quy trình hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

Các Fig.4 và Fig.5 thể hiện sơ đồ khối của các thiết bị hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

Fig.6 thể hiện sơ đồ khối của bộ quản lý truyền thông thiết bị người dùng (UE) hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

Fig.7 thể hiện sơ đồ của hệ thống bao gồm thiết bị hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

Các Fig.8 và Fig.9 thể hiện sơ đồ khối của các thiết bị hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

Fig.10 thể hiện sơ đồ khối của bộ quản lý truyền thông trạm gốc hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

Fig.11 thể hiện sơ đồ của hệ thống bao gồm thiết bị hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

Các Fig.12 và Fig.13 thể hiện sơ đồ khối của các thiết bị hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

Fig.14 thể hiện sơ đồ khối của bộ quản lý truyền thông mạng lõi hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

Fig.15 thể hiện sơ đồ của hệ thống bao gồm thiết bị hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

Các Fig.16 đến Fig.23 thể hiện lưu đồ minh họa phương pháp hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế.

**Mô tả chi tiết sáng chế**

Trong các hệ thống truyền thông không dây, trạm gốc có thể truyền khối thông tin hệ thống (system information block - SIB) chứa thông tin cho phép UE thiết lập kết nối với trạm gốc. SIB thông thường không được mã hóa. Kẻ tấn công có thể thay đổi thông tin hệ thống (SI) trong SIB như là một phần của cuộc tấn công từ chối dịch vụ (denial of service - DoS). Trong một số trường hợp, khóa riêng tư có thể được phân bố cho các trạm gốc và được sử dụng để tạo ra chữ ký số cho SIB. Tuy nhiên, có nhiều trạm gốc, và tin tặc đã tìm ra cách để lấy trộm khóa riêng tư từ các trạm gốc.

Như được mô tả ở đây, khóa riêng tư có thể được duy trì ở hướng lên trong mạng tại vị trí an toàn hơn. Ví dụ, khi khi cần chữ ký, trạm gốc có thể truyền yêu cầu ký đến chức năng ký trong mạng lõi và có thể truyền SI cần được bảo vệ. Chức năng ký có thể sử dụng khóa riêng tư để tạo ra chữ ký cho SI và trả lại chữ ký cho trạm gốc. Trạm gốc truyền SI và chữ ký đến các UE trong vùng phủ sóng của trạm gốc (ví dụ, qua cuộc truyền quảng bá). UE có thể thu được khóa công khai tương ứng với khóa riêng tư và có thể sử dụng khóa công khai để xác minh rằng chữ ký cho SIB là hợp lệ và đến từ trạm gốc (ví dụ, nếu không SIB sẽ bị loại). Khóa công khai, và do đó cả chữ ký, có thể tương ứng với vùng theo dõi cụ thể, và mạng có thể cung cấp cho UE nhiều khóa công khai cho các vùng theo dõi lân cận. Khi UE di chuyển từ một vùng theo dõi đến vùng theo dõi lân cận, UE cố gắng xác minh chữ ký của SIB cho vùng theo dõi đó. Nếu được xác minh, UE có thể cố gắng thiết lập kết nối với trạm gốc trong vùng theo dõi lân cận bằng cách sử dụng SIB được xác minh.

Các khía cạnh của sáng chế được mô tả ban đầu trong ngữ cảnh của các hệ thống truyền thông không dây. Ngoài ra, các khía cạnh của sáng chế được minh họa qua xác thực ô và dòng quy trình. Các khía cạnh của sáng chế còn được minh họa và mô tả dựa vào các sơ đồ máy, sơ đồ hệ thống và lưu đồ liên quan đến bảo vệ SI tại NF trong mạng lõi.

Fig.1 minh họa ví dụ về hệ thống truyền thông không dây 100 hỗ trợ bảo vệ SI tại

NF trong mạng lõi theo các khía cạnh của sáng chế. Hệ thống truyền thông không dây 100 có thể bao gồm một hoặc nhiều trạm gốc 105, một hoặc nhiều UE 115, và mạng lõi 130. Theo một số ví dụ, hệ thống truyền thông không dây 100 có thể là mạng phát triển dài hạn (Long Term Evolution - LTE), mạng LTE nâng cao (LTE-Advanced - LTE-A), mạng LTE-A Pro hoặc mạng vô tuyến mới (New Radio - NR). Theo một số ví dụ, hệ thống truyền thông không dây 100 có thể hỗ trợ truyền thông băng rộng nâng cao, truyền thông siêu tin cậy (ví dụ, cơ yếu), truyền thông độ trễ thấp, truyền thông với các thiết bị chi phí thấp và độ phức tạp thấp, hoặc kết hợp bất kỳ của chúng.

Các trạm gốc 105 có thể được phân tán trong khắp khu vực địa lý để tạo thành hệ thống truyền thông không dây 100 và có thể là các thiết bị ở các dạng khác nhau hoặc có các khả năng khác nhau. Các trạm gốc 105 và các UE 115 có thể truyền không dây qua một hoặc nhiều liên kết truyền thông 125. Mỗi trạm gốc 105 có thể cung cấp vùng phủ sóng 110 trong đó các UE 115 và trạm gốc 105 có thể thiết lập một hoặc nhiều liên kết truyền thông 125. Vùng phủ sóng 110 có thể là ví dụ về vùng địa lý trong đó trạm gốc 105 và UE 115 có thể hỗ trợ truyền thông tín hiệu theo một hoặc nhiều công nghệ truy cập vô tuyến.

Các UE 115 có thể được phân tán trong vùng phủ sóng 110 của hệ thống truyền thông không dây 100 và mỗi UE 115 có thể ở trạng thái tĩnh, hoặc di động, hoặc cả hai tại các thời điểm khác nhau. Các UE 115 có thể là các thiết bị có các dạng khác nhau hoặc có các khả năng khác nhau. Một số UE 115 làm ví dụ được minh họa trên Fig.1. Các UE 115 được mô tả ở đây có thể có khả năng truyền thông với các loại thiết bị khác nhau, như các UE 115 khác, các trạm gốc 105, hoặc thiết bị mạng (ví dụ, các nút mạng lõi, các thiết bị chuyển tiếp, các nút truy cập và backhaul tích hợp (integrated access and backhaul - IAB), hoặc thiết bị mạng khác) khác, như thể hiện trên Fig.1.

Các trạm gốc 105 có thể truyền thông với mạng lõi 130, hoặc với nhau, hoặc cả hai. Ví dụ, các trạm gốc 105 có thể giao tiếp với mạng lõi 130 qua một hoặc nhiều liên kết backhaul 120 (ví dụ, qua S1, N2, N3 hoặc giao diện khác). Các trạm gốc 105 có thể truyền thông với nhau qua các liên kết backhaul 120 (ví dụ, qua X2, Xn hoặc giao diện khác) một cách trực tiếp (ví dụ, trực tiếp giữa các trạm gốc 105) hoặc gián tiếp (ví dụ, qua mạng lõi 130), hoặc cả hai. Theo một số ví dụ, liên kết backhaul 120 có thể là hoặc bao gồm một hoặc nhiều liên kết không dây.

Một hoặc nhiều trạm gốc 105 được mô tả ở đây có thể bao gồm hoặc có thể được người có hiểu biết trung bình trong lĩnh vực kỹ thuật này gọi là trạm thu phát cơ sở, trạm gốc vô tuyến, điểm truy cập, bộ thu phát vô tuyến, nút B (NodeB-NB), nút B cải tiến (eNodeB - eNB), nút B thế hệ tiếp theo hoặc nút B giga (một trong các nút này có thể được gọi là gNB), Nút B trong nhà, eNB trong nhà hoặc một thuật ngữ khác thích hợp.

UE 115 có thể bao gồm hoặc có thể được gọi là thiết bị di động, thiết bị không dây, thiết bị từ xa, thiết bị cầm tay, hoặc thiết bị thuê bao, hoặc một thuật ngữ phù hợp khác nào đó, ở đó "thiết bị" có thể cũng được gọi là đơn vị, trạm, thiết bị đầu cuối, hoặc máy khách bên cạnh các ví dụ khác. UE 115 cũng có thể bao gồm hoặc có thể được gọi là thiết bị điện tử cá nhân như điện thoại di động, thiết bị số hỗ trợ cá nhân (personal digital assistant - PDA), máy tính bảng, máy tính xách tay hoặc máy tính cá nhân. Theo một số ví dụ, UE 115 có thể bao gồm hoặc được gọi là trạm vòng lặp cục bộ không dây (wireless local loop - WLL), thiết bị internet vạn vật kết nối (Internet of Things - IoT), thiết bị internet mọi vật kết nối (Internet of Everything - IoE), hoặc thiết bị truyền thông kiểu máy (machine type communication - MTC), cùng với các ví dụ khác, mà có thể được thực hiện trong các đối tượng khác nhau như thiết bị, xe cộ, đồng hồ đo, cùng với các ví dụ khác.

Các UE 115 được mô tả ở đây có thể truyền thông với các loại thiết bị khác nhau, như các UE 115 khác mà đôi khi có thể hoạt động như các trạm chuyển tiếp cũng như trạm gốc 105 và thiết bị mạng bao gồm các eNB hoặc gNB macro, eNB hoặc gNB ô nhỏ, hoặc trạm gốc chuyển tiếp, trong số các ví dụ khác, như thể hiện trên Fig.1.

Các UE 115 và các trạm gốc 105 có thể truyền thông không dây với nhau qua một hoặc nhiều liên kết truyền thông 125 trên một hoặc nhiều sóng mang. Thuật ngữ "sóng mang" có thể đề cập đến tập hợp tài nguyên phổ tần số vô tuyến có cấu trúc lớp vật lý xác định để hỗ trợ các liên kết truyền thông 125. Ví dụ, sóng mang được sử dụng cho liên kết truyền thông 125 có thể bao gồm một phần của dải phổ tần số vô tuyến (ví dụ, phần băng thông (bandwidth part - BWP)) được vận hành theo một hoặc nhiều kênh lớp vật lý cho công nghệ truy cập vô tuyến nhất định (ví dụ, LTE, LTE-A, LTE-A Pro, NR). Mỗi kênh lớp vật lý có thể mang tín hiệu thu được (ví dụ, tín hiệu đồng bộ hóa, thông tin hệ thống), tín hiệu điều khiển điều phối hoạt động cho sóng mang, dữ liệu người dùng, hoặc tín hiệu khác. Hệ thống truyền thông không dây 100 có thể hỗ trợ truyền thông với

UE 115 bằng cách sử dụng kỹ thuật gộp sóng mang hoặc hoạt động đa sóng mang. UE 115 có thể được tạo cấu hình với nhiều sóng mang thành phần đường xuống và một hoặc nhiều sóng mang thành phần đường lên theo cấu hình gộp sóng mang. Kỹ thuật gộp sóng mang có thể được sử dụng với cả sóng mang thành phần song công phân chia theo tần số (frequency division duplexing - FDD) và song công phân chia theo thời gian (time division duplexing - TDD).

Theo một số ví dụ (ví dụ, trong cấu hình gộp sóng mang), sóng mang có thể cũng có tín hiệu thu nhận hoặc tín hiệu điều khiển mà điều phối các hoạt động cho các sóng mang khác. Sóng mang có thể được kết hợp với kênh tần số (ví dụ, số kênh tần số vô tuyến tuyệt đối truy cập vô tuyến mặt đất của hệ thống viễn thông di động toàn cầu cải tiến (E-UTRA absolute radio frequency channel number - EARFCN)), và có thể được định vị theo raster kênh để phát hiện bởi các UE 115. Sóng mang có thể hoạt động ở chế độ độc lập trong đó sự kết nối và thu nhận ban đầu có thể được điều khiển bởi các UE 115 qua sóng mang, hoặc sóng mang có thể hoạt động ở chế độ không độc lập trong đó kết nối được neo bằng cách sử dụng sóng mang khác (ví dụ, thuộc cùng hoặc khác công nghệ truy cập vô tuyến).

Các liên kết truyền thông 125 thể hiện trong hệ thống truyền thông không dây 100 có thể bao gồm các cuộc truyền đường lên từ UE 115 đến trạm gốc 105, hoặc các cuộc truyền đường xuống, từ trạm gốc 105 đến UE 115. Các sóng mang có thể mang các cuộc truyền thông đường xuống hoặc đường lên (ví dụ, ở chế độ FDD), hoặc được tạo cấu hình để mang các cuộc truyền thông đường xuống và đường lên (ví dụ, ở chế độ TDD).

Sóng mang có thể được kết hợp với băng thông cụ thể của phổ tần số vô tuyến, và theo một số ví dụ băng thông sóng mang có thể được gọi là "băng thông hệ thống" của sóng mang hoặc hệ thống truyền thông không dây 100. Ví dụ, băng thông sóng mang có thể là một trong số các băng thông xác định cho các sóng mang của công nghệ truy cập vô tuyến cụ thể (ví dụ, 1,4, 3, 5, 10, 15, 20, 40, hoặc 80 megahec (MHz)). Các thiết bị của hệ thống truyền thông không dây 100 (ví dụ, các trạm gốc 105, các UE 115, hoặc cả hai) có thể có các cấu hình phần cứng hỗ trợ truyền thông qua băng thông sóng mang cụ thể, hoặc có thể tạo cấu hình được để hỗ trợ truyền thông qua một băng thông trong tập hợp băng thông sóng mang. Theo một số ví dụ, hệ thống truyền thông không dây 100 có thể bao gồm các trạm gốc 105 hoặc UE 115 mà hỗ trợ các cuộc truyền thông đồng thời

qua các sóng mang kết hợp với nhiều băng thông sóng mang. Theo một số ví dụ, mỗi UE 115 được phục vụ có thể được tạo cấu hình để hoạt động trên các phần (ví dụ, băng tần con, BWP) hoặc toàn bộ băng thông sóng mang.

Dạng sóng tín hiệu được truyền qua sóng mang có thể được tạo thành từ nhiều sóng mang con (ví dụ, sử dụng các kỹ thuật điều chế nhiều sóng mang (multi-carrier modulation - MCM) như ghép kênh phân chia theo tần số trực giao (orthogonal frequency division multiplexing - OFDM) hoặc OFDM trải rộng biến đổi Fourier rời rạc (discrete Fourier transform-spread-OFDM - DFT-S-OFDM). Trong hệ thống sử dụng các kỹ thuật MCM, phần tử tài nguyên có thể bao gồm một chu kỳ ký hiệu (ví dụ, thời khoảng của một ký hiệu điều chế) và một sóng mang con, ở đó chu kỳ ký hiệu và khoảng cách sóng mang con có liên quan ngược. Số lượng bit được mỗi phần tử tài nguyên mang có thể phụ thuộc vào sơ đồ điều chế (ví dụ, thứ tự của sơ đồ điều chế, tốc độ mã hóa của sơ đồ điều chế, hoặc cả hai). Do đó, UE 115 nhận được càng nhiều phần tử tài nguyên và thứ tự của sơ đồ điều chế càng cao, thì tốc độ dữ liệu cho UE 115 có thể càng cao. Tài nguyên truyền thông không dây có thể chỉ sự kết hợp của tài nguyên phổ tần số vô tuyến, tài nguyên thời gian, và tài nguyên không gian (ví dụ, các lớp hoặc chùm không gian), và việc sử dụng nhiều lớp không gian có thể làm tăng thêm tốc độ dữ liệu hoặc tính toàn vẹn dữ liệu cho các cuộc truyền với UE 115.

Khoảng cách thời gian cho các trạm gốc 105 hoặc các UE 115 có thể được biểu thị bằng bội số của đơn vị thời gian cơ bản mà có thể, ví dụ, chỉ chu kỳ lấy mẫu $T_s = 1/(\Delta f_{max} \cdot N_f)$ giây, trong đó $\Delta f_{max}$ có thể biểu diễn khoảng cách sóng mang con được hỗ trợ tối đa và $N_f$ có thể biểu diễn kích thước biến đổi Fourier rời rạc (discrete Fourier transform - DFT) được hỗ trợ tối đa. Khoảng cách thời gian của tài nguyên truyền thông có thể được tổ chức theo các khung vô tuyến mỗi khung có thời khoảng xác định (ví dụ, 10 mili giây (milliseconds - ms)). Mỗi khung vô tuyến có thể được xác định bởi số khung hệ thống (system frame number - SFN) (ví dụ, nằm trong khoảng từ 0 đến 1023).

Mỗi khung có thể bao gồm nhiều khung con hoặc khe được đánh số liên tục , và mỗi khung con hoặc khe có thể có cùng thời khoảng. Theo một số ví dụ, khung có thể được chia (ví dụ, trong miền thời gian) thành khung con, và mỗi khung con có thể được chia tiếp thành một số khe. Theo cách khác, mỗi khung có thể bao gồm số lượng khe thay đổi, và số lượng khe có thể phụ thuộc vào khoảng cách sóng mang con. Mỗi khe có

thể bao gồm một số chu kỳ ký hiệu (ví dụ, tùy thuộc vào độ dài của tiền tố vòng được thêm vào trước mỗi chu kỳ ký hiệu). Trong một số hệ thống truyền thông không dây 100, khe có thể được chia tiếp thành nhiều khe nhỏ chứa một hoặc nhiều ký hiệu. Ngoại trừ tiền tố vòng, mỗi chu kỳ ký hiệu có thể chứa một hoặc nhiều (ví dụ, $N_f$) chu kỳ lấy mẫu. Thời khoảng của chu kỳ ký hiệu có thể phụ thuộc vào khoảng cách sóng mang con hoặc dải tần số hoạt động.

Khung con, khe, khe nhỏ, hoặc ký hiệu có thể là đơn vị lập lịch nhỏ nhất (ví dụ, trong miền thời gian) của hệ thống truyền thông không dây 100 và có thể được gọi là khoảng thời gian truyền (transmission time interval - TTI). Theo một số ví dụ, thời khoảng TTI (ví dụ, số lượng chu kỳ ký hiệu trong TTI) có thể thay đổi. Ngoài ra hoặc theo cách khác, đơn vị lập lịch nhỏ nhất của hệ thống truyền thông không dây 100 có thể được chọn động (ví dụ, trong các cụm TTI rút gọn (shortened TTI - sTTI)).

Các kênh vật lý có thể được ghép kênh trên sóng mang theo các kỹ thuật khác nhau. Kênh điều khiển vật lý và kênh dữ liệu vật lý có thể được ghép kênh trên sóng mang đường xuống, ví dụ, bằng cách sử dụng một hoặc nhiều kỹ thuật trong số các kỹ thuật ghép kênh phân chia theo thời gian (time division multiplexing - TDM), các kỹ thuật ghép kênh phân chia theo tần số (frequency division multiplexing - FDM), hoặc các kỹ thuật TDM-FDM lai. Vùng điều khiển (ví dụ, tập hợp tài nguyên điều khiển (control resource set - CORESET)) cho kênh điều khiển vật lý có thể được xác định bằng số chu kỳ ký hiệu và có thể mở rộng trên băng thông hệ thống hoặc tập con của băng thông hệ thống của sóng mang. Một hoặc nhiều vùng điều khiển (ví dụ, CORESET) có thể được tạo cấu hình cho tập hợp các UE 115. Ví dụ, một hoặc nhiều UE 115 có thể giám sát hoặc tìm kiếm các vùng điều khiển cho thông tin điều khiển theo một hoặc nhiều tập hợp không gian tìm kiếm, và mỗi tập hợp không gian tìm kiếm có thể bao gồm một hoặc nhiều ứng viên kênh điều khiển trong một hoặc nhiều mức gộp được sắp xếp theo cách xếp tầng. Mức gộp cho ứng viên kênh điều khiển có thể đề cập đến số tài nguyên kênh điều khiển (ví dụ, phần tử kênh điều khiển (control channel element - CCE)) kết hợp với thông tin được mã hóa cho định dạng thông tin điều khiển có kích thước tải tin cho trước. Các tập hợp không gian tìm kiếm có thể bao gồm các tập hợp không gian tìm kiếm chung được tạo cấu hình để gửi thông tin điều khiển đến nhiều UE 115 và các tập hợp không gian tìm kiếm dành riêng cho UE để gửi thông tin điều khiển đến UE 115 cụ thể.

Mỗi trạm gốc 105 có thể cung cấp vùng phủ sóng truyền thông qua một hoặc nhiều ô, ví dụ ô marco, ô nhỏ, điểm truy cập, hoặc các loại ô khác, hoặc sự kết hợp bất kỳ của chúng. Thuật ngữ "ô" có thể chỉ thực thể truyền thông logic dùng để truyền thông với trạm gốc 105 (ví dụ, qua sóng mang) và có thể được kết hợp với mã định danh để phân biệt các ô lân cận (ví dụ, mã định danh ô vật lý (physical cell identifier-PCID), mã định danh ô ảo (virtual cell ký hiệu identifier-VCID), hoặc các mã khác). Theo một số ví dụ, ô còn có thể là vùng phủ sóng địa lý 110 hoặc một phần của vùng phủ sóng địa lý 110 (ví dụ, sectơ) mà thực thể truyền thông logic hoạt động trên đó. Các ô này có thể nằm trong phạm vi từ khu vực nhỏ (ví dụ, kết cấu, tập con của kết cấu) đến khu vực lớn phụ thuộc vào nhiều yếu tố chẳng hạn như các khả năng của trạm gốc 105. Ví dụ, ô có thể là hoặc bao gồm tòa nhà, nhóm nhỏ của tòa nhà, hoặc các không gian bên ngoài ở giữa hoặc chồng lấn với các vùng phủ sóng địa lý 110, cùng nhiều ví dụ khác.

Ô macro thường phủ sóng vùng địa lý tương đối rộng (ví dụ, bán kính vài kilômét) và có thể cho phép các UE 115 có thuê bao dịch vụ với nhà cung cấp mạng có hỗ trợ ô macro truy cập không giới hạn. Ô nhỏ có thể kết hợp với trạm gốc 105 có công suất thấp hơn so với ô macro, và ô nhỏ có thể hoạt động ở dải tần số (ví dụ, được cấp phép, được miễn cấp phép) giống hoặc khác với các ô macro. Các ô nhỏ có thể cấp quyền truy cập không giới hạn cho các UE 115 có thuê bao dịch vụ với nhà cung cấp mạng hoặc có thể cấp quyền truy cập giới hạn cho các UE 115 có liên kết với ô nhỏ (ví dụ, các UE 115 trong nhóm thuê bao kín (closed subscriber group - CSG), các UE 115 liên quan tới các người dùng trong cùng gia đình hoặc nơi công sở). Trạm gốc 105 có thể hỗ trợ một hoặc nhiều ô và có thể cũng hỗ trợ các cuộc truyền thông trên một hoặc nhiều ô nhờ sử dụng một hoặc nhiều sóng mang thành phần.

Theo một số ví dụ, sóng mang có thể hỗ trợ nhiều ô, và các ô khác nhau có thể được tạo cấu hình theo các loại giao thức khác nhau (ví dụ, MTC, IoT băng hẹp (NB-IoT), băng rộng di động nâng cao (enhanced mobile broadband - eMBB)) mà có thể cấp quyền truy cập cho các loại thiết bị khác nhau.

Theo một số ví dụ, trạm gốc 105 có thể di động và do đó cung cấp vùng phủ sóng truyền thông cho vùng phủ sóng địa lý 110 di động. Theo một số ví dụ, các vùng phủ sóng địa lý 110 khác nhau kết hợp với các công nghệ khác nhau có thể chồng lấn, nhưng các vùng phủ sóng địa lý 110 khác nhau có thể được cùng một trạm gốc 105 hỗ trợ. Theo

một số ví dụ khác, các vùng phủ sóng địa lý 110 chồng lấn kết hợp với các công nghệ khác nhau có thể được hỗ trợ bởi các trạm gốc 105 khác nhau. Hệ thống truyền thông không dây 100 có thể bao gồm, ví dụ, mạng không đồng nhất, trong đó các loại trạm gốc 105 khác nhau cung cấp vùng phủ sóng cho các vùng phủ sóng địa lý 110 khác nhau bằng cách sử dụng các công nghệ truy cập vô tuyến giống nhau hoặc khác nhau.

Hệ thống truyền thông không dây 100 có thể được tạo cấu hình để hỗ trợ truyền thông siêu tin cậy hoặc truyền thông có độ trễ thấp, hoặc các kết hợp khác nhau của chúng. Ví dụ, hệ thống truyền thông không dây 100 có thể được tạo cấu hình để hỗ trợ truyền thông siêu tin cậy có độ trễ thấp (ultra-reliable low-latency communication - URLLC) hoặc truyền thông cơ yếu. Các UE 115 có thể được thiết kế để hỗ trợ các chức năng siêu tin cậy, độ trễ thấp hoặc các chức năng then chốt (ví dụ, các chức năng cơ yếu). Truyền thông siêu tin cậy có thể bao gồm truyền thông cá nhân hoặc truyền thông nhóm và có thể được hỗ trợ bởi một hoặc nhiều dịch vụ cơ yếu, như bộ đàm cơ yếu (Mission Critical Push-To-Talk - MCPTT), video cơ yếu (Mission Critical Video - MCVideo), hoặc dữ liệu cơ yếu (Mission Critical Data - MCData). Hỗ trợ cho các chức năng cơ yếu có thể bao gồm ưu tiên các dịch vụ, và các dịch vụ cơ yếu có thể được sử dụng cho an toàn công cộng hoặc các ứng dụng thương mại nói chung. Các thuật ngữ siêu tin cậy, độ trễ thấp, cơ yếu, và độ trễ thấp siêu tin cậy có thể được sử dụng thay thế cho nhau ở đây.

Trong một số ví dụ, UE 115 cũng có thể có khả năng truyền thông trực tiếp với các UE 115 khác qua liên kết truyền thông từ thiết bị đến thiết bị (device-to-device - D2D) 135 (ví dụ, sử dụng giao thức ngang hàng (peer-to-peer - P2P) hoặc D2D). Một hoặc nhiều UE 115 sử dụng truyền thông D2D có thể nằm trong vùng phủ sóng địa lý 110 của trạm gốc 105. Các UE 115 khác trong nhóm như vậy có thể nằm ngoài vùng phủ sóng địa lý 110 của trạm gốc 105, hoặc nói cách khác không có khả năng nhận các cuộc truyền từ trạm gốc 105. Theo một số ví dụ, các nhóm UE 115 truyền thông qua truyền thông D2D có thể sử dụng hệ thống một đến nhiều (one-to-many - 1:M), trong đó mỗi UE 115 truyền đến mọi UE 115 khác trong nhóm. Theo một số ví dụ, trạm gốc 105 hỗ trợ lập lịch các tài nguyên cho truyền thông D2D. Trong các trường hợp khác, truyền thông D2D được thực hiện giữa các UE 115 mà không có sự tham gia của trạm gốc 105.

Mạng lõi 130 có thể cung cấp chức năng xác thực người dùng, cấp phép truy cập,

theo dõi, kết nối giao thức internet (internet protocol - IP), và các chức năng truy cập, định tuyến hoặc di động khác. Mạng lõi 130 có thể là lõi gói phát triển (evolved packet core - EPC) hoặc lõi 5G (5G core - 5GC), có thể bao gồm ít nhất một thực thể mặt phẳng điều khiển quản lý quyền truy cập và tính di động (ví dụ, thực thể quản lý di động (mobility management entity - MME), chức năng truy cập và quản lý di động (access and mobility management function - AMF)) và ít nhất một thực thể mặt phẳng người dùng định tuyến các gói hoặc kết nối với nhau với các mạng bên ngoài (ví dụ, cổng phục vụ (serving gateway - S-GW), cổng mạng dữ liệu gói (Packet Data Network (PDN) gateway P-GW), hoặc chức năng mặt phẳng người dùng (user plane function - UPF)). Thực thể mặt phẳng điều khiển có thể quản lý các chức năng của tầng không truy cập (non-access stratum - NAS) như tính di động, xác thực và quản lý kênh mang đối với các UE 115 do các trạm gốc 105 liên kết với mạng lõi 130 phục vụ. Các gói IP của người dùng có thể được chuyển qua thực thể mặt phẳng người dùng, có thể cung cấp phân bổ địa chỉ IP cũng như các chức năng khác. Thực thể mặt phẳng người dùng có thể được kết nối với dịch vụ IP của nhà khai thác mạng 150. Dịch vụ IP của nhà khai thác 150 có thể bao gồm dịch vụ truy cập mạng Internet, Intranet, phân hệ đa phương tiện IP (IP Multimedia Subsystem - IMS), và dịch vụ phát trực tuyến chuyển mạch gói.

Một số thiết bị mạng, như trạm gốc 105, có thể bao gồm các thành phần con như thực thể mạng truy cập, mà có thể là ví dụ về bộ điều khiển nút truy cập (access node controller - ANC). Mỗi thực thể mạng truy cập 140 có thể truyền thông với các UE 115 qua một hoặc nhiều thực thể truyền mạng truy cập 145 khác, mà có thể được gọi là đầu vô tuyến, đầu vô tuyến thông minh, hoặc điểm truyền/nhận (transmission/reception point - TRP). Mỗi thực thể truyền mạng truy cập 145 có thể bao gồm một hoặc nhiều tấm anten. Trong một số cấu hình, các chức năng khác nhau của mỗi thực thể mạng truy cập 140 hoặc trạm gốc 105 có thể được phân phối trên các thiết bị mạng khác nhau (ví dụ, các đầu vô tuyến và ANC) hoặc được hợp nhất thành thiết bị mạng duy nhất (ví dụ, trạm gốc 105).

Hệ thống truyền thông không dây 100 có thể hoạt động bằng cách sử dụng một hoặc nhiều dải tần, thường trong khoảng từ 300 megahec (MHz) đến 300 gigahec (GHz). Nói chung, vùng từ 300 MHz đến 3 GHz được biết đến là vùng tần số siêu cao (ultra-high frequency - UHF) hoặc băng tần deximet vì các bước sóng có độ dài nằm trong khoảng từ xấp xỉ một deximet đến một mét. Sóng UHF có thể bị các tòa nhà và các đặc

điểm môi trường chặn hoặc làm chuyển hướng, nhưng các sóng này có thể xuyên qua các cấu trúc đủ để ô macro cung cấp dịch vụ cho các UE 115 ở trong nhà. Việc truyền sóng UHF có thể được kết hợp với các anten nhỏ hơn và phạm vi ngắn hơn (ví dụ, nhỏ hơn 100 km) so với việc truyền nhờ sử dụng các tần số nhỏ hơn và các sóng dài hơn của phần tần số cao (high frequency - HF) hoặc tần số rất cao (very high frequency - VHF) của phổ dưới 300MHz.

Hệ thống truyền thông không dây 100 có thể sử dụng cả dải phổ tần số vô tuyến được cấp phép và được miễn cấp phép. Ví dụ, hệ thống truyền thông không dây 100 có thể sử dụng công nghệ truy cập vô tuyến hỗ trợ đăng ký (License Assisted Access - LAA), công nghệ truy cập vô tuyến LTE-được miễn cấp phép (LTE-U), hoặc công nghệ NR trong băng tần được miễn cấp phép như dải công nghiệp, khoa học, và y tế (industrial, scientific, and medical - ISM) 5 GHz. Khi hoạt động trong các dải phổ tần số vô tuyến được miễn cấp phép, các thiết bị như trạm gốc 105 và các UE 115 có thể sử dụng cảm biến sóng mang để phát hiện và tránh xung đột. Theo một số ví dụ, các hoạt động trong các băng tần được miễn cấp phép có thể dựa vào cấu hình gộp sóng mang cùng với các sóng mang thành phần hoạt động ở băng tần được cấp phép (ví dụ, LAA). Các hoạt động trong phổ được miễn cấp phép có thể bao gồm truyền đường xuống, truyền đường lên, truyền P2P, truyền D2D, trong số các ví dụ khác.

Trạm gốc 105 hoặc UE 115 có thể được trang bị nhiều anten, mà có thể được sử dụng để áp dụng các kỹ thuật như phân tập truyền, phân tập thu, các cuộc truyền thông nhiều đầu vào nhiều đầu ra (multiple-input multiple-output - MIMO), hoặc điều hướng chùm sóng. Các anten của trạm gốc 105 hoặc UE 115 có thể được đặt trong một hoặc nhiều mảng anten hoặc tấm anten, có thể hỗ trợ hoạt động MIMO hoặc truyền hoặc nhận việc điều hướng chùm sóng. Ví dụ, một hoặc nhiều anten hoặc mảng anten của trạm gốc có thể được đặt cùng vị trí ở một cụm anten, như tháp anten. Theo một số ví dụ, các anten hoặc mảng anten liên quan đến trạm gốc 105 có thể được bố trí ở các vị trí địa lý khác nhau. Trạm gốc 105 có thể có mảng anten với các hàng và cột cổng anten mà trạm gốc 105 có thể sử dụng để hỗ trợ việc điều hướng chùm sóng các cuộc truyền thông với UE 115. Tương tự, UE 115 có thể có một hoặc nhiều mảng anten mà có thể hỗ trợ các hoạt động MIMO hoặc điều hướng chùm sóng khác nhau. Ngoài ra hoặc theo cách khác, tấm anten có thể hỗ trợ việc điều hướng chùm sóng tần số vô tuyến cho tín hiệu được truyền qua cổng anten.

Kỹ thuật điều hướng chùm sóng, mà có thể cũng được gọi là lọc không gian, truyền có hướng, hoặc thu có hướng, là kỹ thuật xử lý tín hiệu mà có thể được sử dụng ở thiết bị truyền hoặc thiết bị thu (ví dụ, trạm gốc 105, UE 115) để định hình hoặc lái chùm anten (ví dụ, chùm truyền, chùm thu) cùng với đường không gian giữa thiết bị truyền và thiết bị thu. Việc điều hướng chùm sóng có thể được thực hiện bằng cách kết hợp các tín hiệu được truyền thông qua các phần tử anten của mảng anten sao cho các tín hiệu lan truyền theo các hướng cụ thể so với mảng anten trải qua sự giao thoa tăng trong khi các tín hiệu khác trải qua sự giao thoa giảm. Việc điều chỉnh tín hiệu truyền qua các phần tử anten có thể bao gồm thiết bị truyền hoặc thiết bị thu áp dụng hiệu số biên độ, lệch pha, hoặc cả hai đối với tín hiệu được truyền qua các phần tử anten kết hợp với thiết bị. Các điều chỉnh liên quan tới mỗi trong số các phần tử anten có thể được xác định bởi tập hợp trọng số điều hướng chùm sóng liên quan tới một hướng cụ thể (ví dụ, so với mảng anten của thiết bị truyền hoặc thiết bị thu, hoặc so với một hướng khác nào đó).

Mạng lõi 130 có thể bao gồm một số thực thể (ví dụ, các chức năng) như các AMF, các chức năng quản lý phiên (session management function - SMF), các chức năng mặt phẳng người dùng (user plane function - UPF), NF, và các chức năng khác. Một hoặc nhiều thực thể của mạng lõi có thể được thực hiện ảo trên phần mềm. Theo một số ví dụ, các UE 115 và các trạm gốc 105 có thể truyền thông với thực thể của mạng lõi 130 (ví dụ, MME hoặc AMF) để thiết lập kết nối an toàn cho các cuộc truyền thông. AMF có thể cung cấp các dịch vụ quản lý truy cập và di động cho các UE 115 và các trạm gốc 105. Theo một số ví dụ, AMF có thể dùng làm điểm cơ bản của các cuộc truyền thông báo hiệu mặt phẳng điều khiển với các UE 115 và các trạm gốc 105, sao cho phần lớn các cuộc truyền thông mặt phẳng điều khiển giữa các UE 115, các trạm gốc 105, và mạng lõi 130 đi qua AMF.

Theo một số ví dụ, UE 115 có thể bắt đầu quy trình kết nối với trạm gốc 105 bằng cách gửi yêu cầu gắn kèm. Dựa vào yêu cầu gắn kèm, trạm gốc 105 có thể hỗ trợ xác thực và/hoặc cấp phép cho UE 115 thông qua mạng lõi 130 (ví dụ, qua một hoặc nhiều thực thể của mạng lõi 130). Khi được xác thực, UE 115 có thể truyền thông với mạng lõi 130 dựa vào giao thức tầng không truy cập (non-access stratum - NAS) được tạo cấu hình để thiết lập và duy trì một cách an toàn khả năng kết nối giữa UE 115 và mạng lõi 130. Một hoặc nhiều nút mạng lõi (ví dụ, AMF, MME, cổng phục vụ, v.v.) có thể thông báo cho trạm gốc 105 rằng UE 115 được xác thực và cấp phép để kết nối với hệ thống

truyền thông không dây 100. Sau đó, trạm gốc 105 có thể thiết lập kết nối điều khiển tài nguyên vô tuyến (radio resource control - RRC) (ví dụ, lớp cao hơn) với UE 115 (ví dụ, dựa vào giao thức AS).

Để thiết lập kết nối RRC, trạm gốc 105 có thể tạo ra và truyền cấu hình bảo mật đến UE 115 trong suốt quá trình thực thi giao thức tầng truy cập (access stratum - AS) hoặc sau khi giao thức AS đã được thực hiện. Theo một số ví dụ, cấu hình bảo mật có thể được truyền đến UE 115 qua kênh vô tuyến bảo mật (ví dụ, kênh RRC bảo mật), mà có thể được thiết lập dựa ít nhất một phần vào khóa dùng chung liên quan tới trạm gốc 105 và UE 115. Theo một số ví dụ, khóa dùng chung có thể là khóa gNB (ví dụ, $K_{gNB}$) hoặc khóa eNB ($K_{eNB}$), mà có thể được truyền đến trạm gốc 105 bởi nút mạng lõi (ví dụ, trong khi hoặc tiếp sau quy trình thỏa thuận xác thực và khóa (authentication and key agreement-AKA)) và/hoặc được suy ra bởi UE 115.

Trạm gốc 105 có thể sau đó tạo ra bản tin mã hóa mà bao gồm phân bổ các tài nguyên và cụ thể là, mẫu dùng chung của các tài nguyên được phân bổ cho thông tin điều khiển đường lên cho UE 115. Theo một ví dụ, bản tin mã hóa có thể được mã hóa dựa vào khóa dùng chung và được cung cấp cho UE 115 qua kênh RRC bảo mật. Theo một ví dụ khác, bản tin mã hóa có thể được mã hóa trong bản tin kênh điều khiển đường xuống vật lý (physical downlink control channel - PDCCH). Bản tin PDCCH được mã hóa có thể được mã hóa bằng cách sử dụng khóa mã hóa (ví dụ, khóa công khai). Khóa mã hóa có thể được truyền từ trạm gốc 105 đến UE 115 trong khi kết nối RRC và/hoặc có thể được truyền qua kênh RRC bảo mật (ví dụ, sau khi kết nối RRC được thiết lập). Việc sử dụng kênh RRC bảo mật có thể ngăn không cho các thiết bị khác chặn khóa mã hóa, như thiết bị gây tắc nghẽn. Theo một số ví dụ, khóa mã hóa có thể là chung cho tất cả các UE 115 được kết nối với hoặc cố gắng kết nối với trạm gốc 105. Trong một số trường hợp, khóa mã hóa có thể được tạo ra ngẫu nhiên bởi trạm gốc 105 hoặc mạng lõi 130. Theo một số ví dụ, khóa mã hóa có thể được suy ra dựa vào khóa dùng chung liên quan tới trạm gốc 105 và UE 115, như $K_{gNB}$ (hoặc $K_{eNB}$).

Trong một số hệ thống truyền thông không dây 100 (ví dụ, LTE), máy chủ thuê bao trong nhà (home subscriber server - HSS) có thể tạo ra khóa thực thể quản lý an ninh truy cập (access security management entity - ASME) (ví dụ, $K_{ASME}$) và báo hiệu nó đến MME. $K_{eNB}$ ban đầu có thể sau đó được suy ra bởi MME sử dụng $K_{ASME}$. $K_{eNB}$ tiếp sau

có thể được suy ra từ khóa bước nhảy tiếp theo (next hop-NH), ở đó khóa NH có thể được suy ra từ $K_{ASME}$ và khóa NH trước đó hoặc từ $K_{ASME}$ và $K_{eNB}$ để suy ra khóa NH ban đầu. Để suy ra các khóa khác nhau (ví dụ, $K_{eNB}$, khóa NH, khóa kiểm tra tính toàn vẹn, khóa mật mã, v.v.), UE 115, trạm gốc 105, hoặc MME có thể sử dụng các hàm dẫn xuất khóa (key derivation function - KDF), trong đó mỗi KDF có thể bao gồm một số tham số nhất định của đầu vào, S, như mã chức năng (function code-FC), tham số 0 (P0), độ dài tham số 0 (L0), tham số 1 (P1), độ dài tham số 1 (L1), v.v..

Theo một số ví dụ, khi suy ra $K_{eNB}$ từ $K_{ASME}$ với NAS COUNT đường lên trong UE 115 và MME, các tham số KDF có thể bao gồm giá trị FC 0x11, giá trị P0 bằng NAS COUNT đường lên, và giá trị L0 bằng với độ dài NAS COUNT đường lên (ví dụ, 0x00 0x04). Ngoài ra, UE 115 và MME có thể sử dụng $K_{ASME}$ 256-bit làm khóa đầu vào. UE 115 và MME có thể áp dụng KDF này khi thiết lập các kênh mang vô tuyến của mạng truy cập vô tuyến mặt đất sử dụng hệ thống viễn thông di động toàn cầu cải tiến (Evolved Universal Mobile Telecommunications System Terrestrial Radio Access Network- E-UTRAN) được bảo vệ bằng mật mã và/hoặc khi thực hiện thay đổi khóa khi đang hoạt động.

Theo một số ví dụ, khi suy ra khóa NH từ $K_{ASME}$, các tham số KDF có thể bao gồm giá trị FC 0x12, giá trị P0 bằng với SYNC-input, và giá trị L0 bằng với độ dài của SYNC-input (ví dụ, 0x00 0x20). Tham số SYNC-input có thể là $K_{eNB}$ mới được suy ra để suy ra khóa NH ban đầu hoặc khóa NH trước đó cho các lần suy ra khóa NH tiếp theo. Thông qua tham số SYNC-input này, chuỗi NH có thể được tạo ra sao cho khóa NH tiếp theo có thể là mới và được suy ra từ khóa NH trước đó. Ngoài ra, UE 115 và MME có thể sử dụng $K_{ASME}$ 256-bit làm khóa đầu vào.

Trước khi thiết lập kết nối bảo mật như được mô tả ở trên (ví dụ, một khi ngữ cảnh bảo mật được thiết lập tại trạm gốc, tất cả các tín hiệu được mã hóa và bảo vệ tính toàn vẹn), trạm gốc 105 có thể truyền SIB chứa thông tin (ví dụ, SI) cho phép UE 115 thiết lập kết nối với trạm gốc 105. Thông thường, SIB chưa được mã hóa, nhưng một khi ngữ cảnh bảo mật được thiết lập tại trạm gốc 105, tất cả các tín hiệu có thể được mã hóa và bảo vệ tính toàn vẹn. Tuy nhiên, SIB không được mã hóa có thể cho phép kẻ tấn công (ví dụ, tin tặc) có thể thay đổi SI trong SIB như là một phần của cuộc tấn công DoS. Để ngăn chặn cuộc tấn công DoS, khóa riêng tư đã được phân bố cho các trạm gốc và được

sử dụng để tạo ra chữ ký số cho SIB để tăng cường bảo mật chống lại các trạm gốc giả. Ví dụ, ngay cả khi kẻ tấn công có thể làm giả SI, kẻ tấn công cũng không thể thiết lập kết nối bảo mật với UE đích 115 do việc xác thực sẽ bị lỗi (ví dụ, với truy cập ban đầu) hoặc lệnh chế độ bảo mật (security mode command - SMC) AS sẽ bị lỗi. Tuy nhiên, có nhiều trạm gốc, và tin tặc đã tìm ra cách để lấy trộm khóa riêng tư từ các trạm gốc hoặc tạo ra các loại DoS khác (ví dụ, gửi bản tin từ chối không được bảo vệ, gây tắc nghẽn, v.v.).

Trong một số trường hợp, giải pháp dựa vào mã khóa công khai có thể ngăn chặn các loại tấn công DoS khác nhau. Tuy nhiên, khóa công khai dùng chung có thể không theo tỷ lệ và/hoặc có thể khó sử dụng được cho việc bảo vệ bản tin phát quảng bá. Ngoài ra, không khóa công khai dùng chung nào có thể có sẵn trước lần đăng ký ban đầu (ví dụ, với mã định danh ẩn thuê bao (subscription concealed identifier - SUCI)) dựa vào việc không có ngữ cảnh bảo mật.

Trong một số trường hợp, đối với chế độ rỗi RRC từ góc độ bảo mật AS liên quan đến việc UE phát hiện các trạm gốc 105 lừa đảo (ví dụ, các trạm gốc 105 giả), các giải pháp khác nhau để xác minh hoặc xác thực trạm gốc 105 đã được đề xuất. Ví dụ, để xác minh SI nhờ sử dụng giải pháp chữ ký số để giảm thiểu tấn công phát lại (ví dụ, tấn công DoS), kích thước của SI được bảo vệ có thể lớn hơn do các thông số chữ ký số và dấu thời gian. Ngoài ra hoặc theo cách khác, UE 115 xác minh trạm gốc 105 với giải pháp 'Truy vấn hệ thống' có thể bao gồm UE 115 truyền thông với mạng mặc dù đang ở trạng thái hoặc chế độ rỗi RRC. Trong một số trường hợp, UE 115 có thể sử dụng giải pháp giảm thiểu đo kiểm hiện trường (minimization of drive test - MDT) để xác minh trạm gốc 105, nhưng giải pháp MDT này có thể bị động và không phải là giải pháp kiểu phòng ngừa. Do đó, UE 115 có thể kết nối với trạm gốc giả (ví dụ, ô giả) trong khi ở trạng thái rỗi RRC, dẫn đến khả năng bị tấn công DoS hoặc tấn công tính khả dụng (ví dụ, như các cảnh báo an toàn công cộng, cuộc gọi đến khẩn cấp, dịch vụ đẩy của máy chủ ứng dụng thời gian thực, dịch vụ lân cận, v.v.). Do một số dịch vụ, như hệ thống cảnh báo động đất và sóng thần (earthquake and tsunami warning system - ETWS), có thể được cung cấp cho UE 115 trong chế độ rỗi RRC qua các SIB, có thể cần thiết cân nhắc và đảm bảo rằng UE 115 nhận được các dịch vụ này, điều này sẽ không đúng nếu UE 115 đang kết nối tại trạm gốc 105 giả (ví dụ, trạm gốc lừa đảo 105, eNB lừa đảo, v.v.).

Từ góc độ tín hiệu mặt phẳng điều khiển RRC (ví dụ, các bản tin phát đơn hướng), các thủ tục có thể được thực hiện trước khi kích hoạt bảo mật AS, bao gồm thủ tục thiết lập kết nối RRC, thủ tục thu nhận định danh UE, thủ tục truyền thông tin khả năng UE, thủ tục truyền thông tin đường xuống/đường lên, v.v. Các bản tin phát đơn hướng này có thể cũng cần bảo vệ. Ví dụ, các cuộc xâm nhập (hacking) được báo cáo trên các mạng LTE đã có trên các bản tin ban đầu không được bảo vệ, như bản tin từ chối kết nối (ví dụ, các mã lỗi quản lý tính di động của hệ thống gói cải tiến (evolved packet system (EPS) mobility management - EMM)), bản tin từ chối cập nhật vùng theo dõi, v.v., mà được truyền qua giao diện không gian trước khi kích hoạt bảo mật AS.

Fig.2 minh họa ví dụ về xác thực ô 200 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Theo một số ví dụ, xác thực ô 200 có thể thực hiện các khía cạnh của hệ thống truyền thông không dây 100. Xác thực ô 200 có thể bao gồm UE 115-a, trạm gốc 105-a, và trạm gốc 105-b, đây có thể lần lượt là ví dụ về các UE 115 và các trạm gốc 105 tương ứng, như được mô tả ở trên liên quan đến Fig.1. Ngoài ra, xác thực ô 200 có thể bao gồm AMF 205-a và AMF 205-b, có thể là các chức năng được triển khai ảo trong phần mềm của mạng lõi.

Xác thực ô 200 có thể biểu diễn giải pháp dựa vào kỹ thuật mã hóa khóa công khai để xác minh hoặc xác thực xem bản tin nhận được có phải là từ trạm gốc 105 hay không. Ví dụ, chữ ký có thể được thêm vào SIB (ví dụ, SIB1, SIB bảo mật, v.v.) sao cho UE 115 đã thu nhận SIB (ví dụ, và/hoặc MIB/SIB) có thể xác minh SI. Trong một số trường hợp, AMF 205 có thể cung cấp cho UE 115 khóa công khai có thể được sử dụng để xác minh chữ ký SIB (ví dụ, chữ ký MIB/SIB) trong khi đăng ký, trong đó khóa công khai là hợp lệ trong vùng theo dõi (ví dụ, vùng vị trí địa lý cho mạng). Ngoài ra, trạm gốc 105 có thể ký SIB nhờ sử dụng khóa riêng tư gắn với khóa công khai. Do đó, khi UE 115 vào vùng theo dõi mới, UE 115 có thể thu được khóa công khai mới từ AMF 205 trong khi đăng ký (ví dụ, thông qua cập nhật đăng ký di động). Như được thể hiện, xác thực ô 200 có thể bao gồm một số thao tác cho thủ tục xác thực mã khóa công khai được mô tả ở trên.

Ở khối 210, AMF 205-a có thể được cấp trước một hoặc nhiều khóa công khai ($K\text{-}SIG_{Public}$) để phân bố cho tất cả các chỉ báo vùng theo dõi (tracking area indication - TAI) dưới sự điều khiển của AMF 205-a. Ở khối 215, UE 115-a có thể thực hiện thủ tục gắn

kèm ban đầu để kết nối với mạng (ví dụ, trạm gốc 105-a, mạng lõi, v.v.).

Ở khối 220, UE 115-a có thể thực hiện kết nối RRC để thiết lập kết nối với trạm gốc 105-a (ví dụ, thủ tục truy cập ngẫu nhiên). Ở khối 225, UE 115-a có thể truyền yêu cầu đăng ký đến AMF 205-a. Ở khối 230, để đáp lại, AMF 205-a có thể truyền bản tin chấp nhận đăng ký đến UE 115-a. Trong một số trường hợp, bản tin chấp nhận đăng ký có thể bao gồm danh sách gồm các TAI và các khóa công khai tương ứng cho các TAI (ví dụ, $K\text{-}SIG_{Public}$ thứ nhất của TAI thứ nhất (TAI-1), $K\text{-}SIG_{Public}$ thứ hai của TAI thứ hai (TAI-2), $K\text{-}SIG_{Public}$ thứ ba của TAI thứ ba (TAI-3), v.v.).

Ở khối 235, UE 115-a có thể chuyển tiếp sang chế độ rỗi (ví dụ, chế độ rỗi RRC). Trong một số trường hợp, trong khi ở chế độ rỗi, UE 115-a có thể vào vùng theo dõi mới (ví dụ, TAI-2). Theo đó, UE 115-a có thể xác minh chữ ký số (digital signature - DS) trong SIB nhận được trong khi ở trong vùng theo dõi mới nhờ sử dụng khóa công khai cho vùng theo dõi (ví dụ, $K\text{-}SIG_{Public}$ thứ hai của TAI-2) và sau đó có thể chọn lại ô truyền khóa công khai trong vùng theo dõi mới này.

Ngoài ra hoặc theo cách khác, ở khối 240, trong khi ở chế độ rỗi, UE 115-a có thể vào vùng theo dõi khác (ví dụ, TAI-4). Trong một số trường hợp, UE 115-a có thể phát hiện thấy rằng vùng theo dõi khác (TAI-4) này không ở trong danh sách các TAI mà UE 115-a đã đăng ký với mạng ở khối 225 và 230. Sau khi thực hiện chọn lại ô, UE 115-a có thể thực hiện thủ tục cập nhật vùng theo dõi (tracking area update - TAU) trước khi kết nối với ô mới trong vùng theo dõi khác (ví dụ, trạm gốc 105-b). Một khi TAU được thực hiện, UE 115-a có thể thu được khóa công khai của vùng theo dõi khác (TAI-4) và cả danh sách các TAI dưới sự điều khiển của AMF 205-b.

Ví dụ, ở khối 245, UE 115-a có thể truyền yêu cầu cập nhật vị trí (ví dụ, cập nhật đăng ký di động) đến AMF 205-b. Sau đó ở khối 250, AMF 205-b có thể truyền bản tin chấp nhận cập nhật vị trí bao gồm danh sách các TAI dưới sự điều khiển của AMF 205-b và khóa công khai tương ứng (ví dụ, $K\text{-}SIG_{Public}$ thứ tư của TAI thứ tư (TAI-4), $K\text{-}SIG_{Public}$ thứ năm của TAI thứ năm (TAI-5), $K\text{-}SIG_{Public}$ thứ sáu của TAI thứ sáu (TAI-6, v.v.).

Ở khối 255, trạm gốc 105-b có thể truyền SIB có DS. Trong một số trường hợp, trạm gốc 105-b có thể truyền SIB qua việc truyền tín hiệu RRC, cuộc truyền được phát quảng bá, v.v..

Ở khối 260, UE 115-a có thể xác minh DS trong SIB nhờ sử dụng khóa công khai ($K\text{-}SIG_{Public}$) cho TAI-4 và sau đó có thể chọn lại ô (ví dụ, trạm gốc 105-b) sau khi xác minh SIB là từ trạm gốc 105-b. Theo đó, SIB có thể được ký bởi trạm gốc 105-b (ví dụ, mạng) mà sau đó được gửi đến một hoặc nhiều UE 115 (ví dụ, bao gồm UE 115-a), và UE 115-a có thể xác minh chữ ký SIB được phát quảng bá bởi trạm gốc 105-b dựa vào khóa công khai cho vùng theo dõi gắn với trạm gốc 105-b.

Tuy nhiên, AMF 205 và tất cả các trạm gốc 105 trong vùng theo dõi có thể dùng chung cùng khóa riêng tư. Theo đó, nếu một thực thể (ví dụ, trạm gốc 105) bị xâm phạm bởi kẻ tấn công (ví dụ, tin tặc) và khóa ký (tức là, khóa riêng tư) bị tiết lộ cho kẻ tấn công, thì toàn bộ an ninh hệ thống (ví dụ, trong vùng theo dõi) có thể bị xâm phạm. Ngoài ra, nếu các trạm gốc có thể được triển khai gần hơn với người dùng/kẻ tấn công (ví dụ, do phủ sóng ngắn hơn), việc dùng chung một khóa giữa nhiều trạm gốc có thể không được mong muốn. Do đó có nhu cầu cần nhiều kỹ thuật hiệu quả hơn xác thực ô 200.

Fig.3 minh họa ví dụ về dòng quy trình 300 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Theo một số ví dụ, dòng quy trình 300 có thể thực hiện các khía cạnh của hệ thống truyền thông không dây 100. Dòng quy trình 300 có thể bao gồm UE 115-b và trạm gốc 105-c, đây có thể lần lượt là ví dụ về các UE 115 và các trạm gốc 105 tương ứng, như được mô tả ở trên liên quan đến các Fig.1 và Fig.2. Ngoài ra, dòng quy trình 300 có thể bao gồm AMF 305 và NF ký 310, đây có thể là các chức năng được triển khai ảo trong phần mềm và/hoặc phần cứng của nút mạng, như nút mạng lõi trong mạng lõi. Trong một số trường hợp, NF ký 310 có thể được đặt cùng vị trí với AMF 305 và/hoặc chức năng neo bảo mật (security anchor function - SEAF).

Ở khối 315, nút mạng có thể tạo ra một hoặc nhiều cặp khóa công khai (public key - PK)-khóa riêng tư (private key - SK). Nút mạng có thể là nút chức năng ký như NF ký 310, nút mạng truy cập vô tuyến (radio access network - RAN), nút chức năng ứng dụng (application function - AF), AMF, nút mạng lõi, hoặc nút tương tự. Trong một số trường hợp, khóa công khai có thể được gọi là khóa xác minh, và khóa riêng tư có thể được gọi là khóa ký. Ngoài ra, khóa riêng tư có thể được giữ cục bộ tại NF ký 310. Theo đó, dựa vào việc giữ các khóa riêng tư cục bộ tại NF ký 310, kẻ tấn công có thể gặp khó khăn hơn trong việc lấy được khóa riêng tư, do đó tăng cường bảo mật hệ thống. Trong

một số trường hợp, NF ký 310 có thể có nhiều cặp PK-SK với mã định danh (identifier - ID) khóa tương ứng.

Ở khối 320, NF ký 310 có thể cung cấp một hoặc nhiều PK (ví dụ, với các ID khóa tương ứng) tại (các) AMF 305 trong vùng theo dõi (ví dụ, vùng mà trong đó PK là hợp lệ). Ví dụ, AMF 305 có thể nhận một hoặc nhiều khóa công khai và ID khóa cho vùng theo dõi từ NF ký 310.

Ở khối 325, trạm gốc 105-b có thể gửi MIB và/hoặc SIB như là một phần của yêu cầu chữ ký (ví dụ, yêu cầu ký) đến mạng lõi qua NF ký 310. Ví dụ, trạm gốc 105-b có thể truyền yêu cầu chữ ký trực tiếp đến NF ký 310. Ngoài ra hoặc theo cách khác, trạm gốc 105-b có thể truyền yêu cầu chữ ký đến mạng lõi và NF ký 310 qua AMF 305. Trong một số trường hợp, yêu cầu chữ ký có thể bao gồm thông số truy cập gần đây (ví dụ, thông số độ mới). Ví dụ, thông số truy cập gần đây có thể là số khung hệ thống (system frame number - SFN) mà có thể được sử dụng làm thông số độ mới để tạo ra chữ ký. Theo đó, SFN có thể cần được cung cấp cho NF ký 310. Ví dụ, yêu cầu chữ ký và đáp ứng chữ ký có thể được chuyển tiếp đến AMF 305. Ngoài ra, yêu cầu chữ ký và đáp ứng chữ ký có thể được nhận từ AMF 305 và được chuyển tiếp đến trạm gốc 105-b. Trong một số trường hợp, chữ ký có thể được yêu cầu qua chức năng mạng lõi khác, như AMF 305, cũng như đáp ứng chữ ký.

Ở khối 330, NF ký 310 có thể ký MIB và/hoặc SIB và có thể cung cấp chữ ký cho trạm gốc 105-c (ví dụ, trực tiếp hoặc gián tiếp). Theo đó, trạm gốc 105-c có thể thêm chữ ký vào bản tin SIB (ví dụ, SIB1 hoặc SIB bảo mật khác). Trong một số trường hợp, trạm gốc 105-c có thể cung cấp thông tin chính để ký cho NF ký 310, và NF ký 310 có thể tạo ra và cung cấp chữ ký cho MIB. Theo một số ví dụ, trạm gốc 105-c có thể cung cấp cả thông tin chính và thông tin hệ thống để ký cho NF ký 310, và NF ký 310 có thể tạo ra và cung cấp một chữ ký được tạo ra cho MIB và SIB. Theo ví dụ khác, NF ký 310 có thể tạo ra và cung cấp các chữ ký riêng được tạo ra cho MIB và SIB. Ở khối 335 và 340, trạm gốc 105-c và NF ký 310 có thể truyền và nhận yêu cầu chữ ký và đáp ứng chữ ký được định tuyến qua AMF 305.

Ở khối 345, nút mạng (ví dụ, nút RAN, nút chức năng ứng dụng (application function - AF), AMF, nút mạng lõi, v.v.), như AMF 305, có thể nhận yêu cầu đăng ký từ UE 115-b. Trong một số trường hợp, AMF 305 có thể gửi đáp ứng đăng ký (ví dụ, bản

tin NAS, chấp nhận đăng ký, v.v.) đến UE 115-b mà bao gồm (các) khóa công khai và ID khóa. Ví dụ, đáp ứng đăng ký có thể bao gồm danh sách TAI mà trong dód PK là hợp lệ. Theo đó, UE 115-b có thể thu được một hoặc nhiều PK với các ID khóa gắn kèm hoặc tương ứng trong khi đăng ký. Ví dụ, nút mạng (ví dụ, AMF 305) có thể cung cấp các bộ gồm ID khóa và khóa công khai tương ứng cho UE 115-b khi UE 115-b đăng ký với mạng (ví dụ, qua đáp ứng đăng ký/bản tin chấp nhận) để cho phép UE 115-b xác minh bản tin SI và chữ ký được truyền (ví dụ, được phát quảng bá) bởi trạm gốc 105-c cùng với ID khóa. Trong một số trường hợp, đăng ký có thể là đăng ký ban đầu, cập nhật đăng ký di động (ví dụ, để vào vùng theo dõi mới), v.v..

Ở khối 350, trạm gốc 105-c có thể truyền bản tin SI bao gồm SI và chữ ký nhận được ở khối 330 hoặc 340. Trong một số trường hợp, bản tin SI có thể bao gồm ID khóa mà tương ứng với khóa công khai được sử dụng bởi UE 115-b để xác minh chữ ký. Ví dụ, các bản tin chữ ký được cung cấp cho trạm gốc 105-c (ví dụ, bởi nút mạng, NF ký, v.v.) ở khối 330 hoặc 340 cũng có thể mang ID khóa để cho phép trạm gốc 105-c phát quảng bá ID khóa cùng với SI và chữ ký. Theo đó, trạm gốc 105-c có thể phát quảng bá SIB1 bao gồm chữ ký được tạo ra dựa vào thông tin hệ thống. Theo một số ví dụ, trạm gốc 105-c có thể phát quảng bá bản tin MIB bao gồm chữ ký được tạo ra dựa vào thông tin chính. Theo một số ví dụ, trạm gốc 105-c có thể phát quảng bá bản tin MIB/SIB kết hợp bao gồm chữ ký được tạo ra dựa vào thông tin chính và thông tin hệ thống. Theo một số ví dụ, trạm gốc 105-c có thể phát quảng bá bản tin MIB/SIB kết hợp bao gồm chữ ký thứ nhất được tạo ra dựa vào thông tin chính và chữ ký thứ hai được tạo ra dựa vào thông tin hệ thống.

Ở khối 355, UE 115-b có thể xác minh chữ ký trong bản tin SI (ví dụ, chữ ký MIB/SIB) nhờ sử dụng PK (ví dụ, nhận được trong khi đăng ký ở khối 345) gắn với vùng theo dõi được chỉ báo với bản tin SI (ví dụ, khóa xác minh). Theo đó, nếu chữ ký được xác minh (ví dụ, UE 115-b xác định trạm gốc 105-c đã truyền bản tin SI), UE 115-b có thể sử dụng thông tin hệ thống có trong bản tin SIB (và/hoặc thông tin chính nhận được trong bản tin MIB/SIB kết hợp hoặc bản tin MIB riêng bao gồm chữ ký được tạo ra nhờ sử dụng thông tin chính theo các kỹ thuật được mô tả ở đây) có thể đồng bộ hóa và thiết lập kết nối với trạm gốc 105-c (ví dụ, ô trên trạm gốc 105-c). Ví dụ, UE 115-b có thể đọc SIB1 được phát quảng bá và xác minh chữ ký SIB1 trước khi thiết lập kết nối an toàn với trạm gốc 105-c cho các cuộc truyền thông tiếp theo.

Trong một số trường hợp, trạm gốc 105-c có thể yêu cầu các chữ ký hàng loạt. Theo một số ví dụ (ví dụ, yêu cầu chữ ký dựa vào thời gian), trạm gốc 105-c có thể yêu cầu *N* chữ ký cho khoảng cách thời gian cho trước (ví dụ, từ T1 đến T2 với khoảng cách T_int). Ví dụ, trạm gốc 105-c có thể yêu cầu các chữ ký từ thời gian thứ nhất (ví dụ, T1, khung hoặc khung con thứ nhất, v.v.) đến thời gian thứ hai (ví dụ, T2, khung hoặc khung con thứ hai, v.v.) với khoảng cách thời gian (ví dụ, T_int, khoảng tăng khung hoặc khung con, v.v.). Theo đó, NF ký 310 có thể tạo ra các chữ ký cho T1, T1+T_int, T1+2*T_int, v.v., cho tới khi đến T2. Ngoài ra hoặc theo cách khác, khi sử dụng thông số truy cập gần đây (ví dụ, SFN, thông số độ mới), cho yêu cầu chữ ký hàng loạt, trạm gốc 105-c có thể yêu cầu các chữ ký từ SFN_start đến SFN_end với khoảng cách nhất định (ví dụ, SFN_int). Ví dụ, nếu các chữ ký được yêu cầu cho SFN thứ nhất (SFN1) đến SFN thứ 999 (SFN999) với khoảng cách hai (2), NF ký 310 có thể tạo ra 500 chữ ký (ví dụ, cho SFN 1, 3, 5…, đến 999). UE 115-b có thể cố gắng xác minh chữ ký của bản tin SIB nhận được cho số khung hệ thống nằm trong phạm vi số khung con nhờ sử dụng khóa công khai nhận được và số khung con cho bản tin SIB để xác định xem bản tin SIB nhận được có bao gồm thông tin hệ thống thật hay không.

Ngoài ra hoặc theo cách khác, trạm gốc 105-c có thể đăng ký dịch vụ chữ ký với NF ký 310. Ví dụ, NF ký 310 có thể cung cấp các chữ ký mới cho trạm gốc đăng ký 105 định kỳ. Trong một số trường hợp, khi bản tin SI thay đổi (ví dụ, MIB và/hoặc SIB bị thay đổi bởi trạm gốc 105 hoặc thực thể khác), trạm gốc 105-c có thể cập nhật việc đăng ký hoặc yêu cầu đăng ký mới bằng việc cung cấp bản tin SI mới (ví dụ, MIB/SIB mới). Các bản tin SI có thể không thay đổi thường xuyên và tương đối tĩnh. Ngoài ra, yêu cầu chữ ký hàng loạt có thể được thực hiện dựa vào đăng ký. Theo đó, chữ ký có thể không được gửi trong cuộc truyền đáp ứng chữ ký hàng loạt mà có thể được truyền bất cứ khi nào chữ ký được tạo ra dựa vào việc đăng ký.

Trong một số trường hợp, AMF 305 có thể cung cấp cho UE 115-b các PK của một hoặc nhiều vùng theo dõi lân cận. Ngoài ra, AMF 305 sau đó có thể cung cấp các PK này cho UE 115-b trong khi đăng ký như được mô tả ở khối 345. Theo một ví dụ, trong khi đăng ký, AMF 305 có thể cung cấp cho UE 115-b ít nhất một PK của vùng theo dõi phục vụ, và một hoặc nhiều PK của một hoặc nhiều vùng theo dõi lân cận. Do đó, khi UE 115-b di chuyển từ vùng theo dõi phục vụ sang vùng theo dõi lân cận, UE 115-b có thể xác minh bản tin SI (ví dụ, MIB/SIB) nhận được trong vùng theo dõi lân

cận nhờ sử dụng khóa nhận được trước đó từ AMF 305. Ngoài ra hoặc theo cách khác, nếu AMF 305 không lưu trữ các PK của các vùng theo dõi lân cận và cung cấp chúng cho UE 115-b, UE 115-b có thể không xác minh chữ ký trong khi di chuyển đến vùng theo dõi lân cận. Theo đó, kẻ tấn công sau đó có thể có khả năng khai thác việc không có khả năng xác minh chữ ký này của vùng theo dõi lân cận (ví dụ, bằng việc duy trì phát quảng bá vùng theo dõi mới trong SIB (ví dụ, SIB1) để bắt đầu cuộc tấn công DoS tại UE 115-b).

Fig.4 thể hiện sơ đồ khối 400 của thiết bị 405 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Thiết bị 405 có thể là ví dụ về UE 115 theo các khía cạnh được mô tả ở đây. Thiết bị 405 có thể bao gồm bộ thu 410, bộ quản lý truyền thông UE 415 và bộ phát 420. Thiết bị 405 cũng có thể bao gồm bộ xử lý. Mỗi trong số các thành phần này có thể truyền thông với nhau (ví dụ, qua một hoặc nhiều bus).

Bộ thu 410 có thể nhận thông tin như gói, dữ liệu người dùng, hoặc thông tin điều khiển gắn với các kênh thông tin khác nhau (ví dụ, kênh điều khiển, kênh dữ liệu, và thông tin liên quan đến bảo vệ SI tại NF trong mạng lõi, v.v.) Thông tin có thể được truyền đến các thành phần khác của thiết bị 405. Bộ thu 410 có thể là ví dụ về bộ thu phát 720 theo các khía cạnh được mô tả liên quan đến Fig.7. Bộ thu 410 có thể sử dụng một anten hoặc bộ anten.

Bộ quản lý truyền thông UE 415 có thể truyền yêu cầu đăng ký đến nút mạng lõi (ví dụ, AMF). Ngoài ra, bộ quản lý truyền thông UE 415 có thể nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất. Sau đó, bộ quản lý truyền thông UE 415 có thể giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai. Bộ quản lý truyền thông UE 415 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông UE 710 được mô tả ở đây.

Dựa vào các hoạt động thực hiện bởi bộ quản lý truyền thông UE 415 như được mô tả ở đây, UE 115 có thể giảm độ trễ khi chuyển từ một vùng theo dõi sang vùng theo dõi khác. Ví dụ, bằng việc tạo nhiều chữ ký (ví dụ, chữ ký thứ nhất và chữ ký thứ hai)

cho các cặp khóa công khai-khóa riêng tư và các vùng theo dõi gắn kèm, nếu UE 115 di chuyển từ một vùng theo dõi đến vùng theo dõi tiếp theo, UE 115 có thể xác minh chữ ký cho vùng theo dõi tiếp theo ngay lập tức thay vì chờ nhận khóa công khai cho vùng theo dõi tiếp theo và sau đó tạo ra chữ ký. Ngoài ra, bằng việc tạo ra nhiều chữ ký ngay lập tức, UE 115 có thể loại bỏ để không xảy ra cuộc tấn công DoS bất kỳ trong khi có các chữ ký được nạp trước trong khi di chuyển từ vùng theo dõi này sang vùng theo dõi khác mà tại đó kẻ tấn công có thể có khả năng cố gắng duy trì phát quảng bá các vùng theo dõi mới trong SIB. Do đó, với các chữ ký được nạp trước trong kịch bản di động này, UE 115 có thể xác minh hoặc nhận dạng xem SIB có thật hay không trước khi bị kẹt vào một vòng vô tận với các vùng theo dõi mới được truyền đến UE 115 (ví dụ, cuộc tấn công DoS).

Bộ quản lý truyền thông UE 415, hoặc các thành phần con của nó, có thể được thực thi trong phần cứng, mã (ví dụ, phần mềm hoặc firmware) được thực thi bởi bộ xử lý, hoặc kết hợp bất kỳ của chúng. Nếu được thực hiện bằng mã do bộ xử lý thực thi, các chức năng của bộ quản lý truyền thông UE 415, hoặc các thành phần con của nó có thể được thực thi bởi bộ xử lý đa dụng, bộ xử lý tín hiệu số (digital signal processor - DSP), mạch tích hợp chuyên dụng (application-specific integrated circuit - ASIC), mảng cổng lập trình được theo trường (field programmable gate array - FPGA) hoặc các thiết bị logic lập trình được khác, cổng rời rạc hoặc mạch logic bán dẫn, các thành phần phần cứng rời rạc, hoặc dạng kết hợp bất kỳ của chúng được thiết kế để thực hiện các chức năng mô tả trong sáng chế.

Bộ quản lý truyền thông UE 415, hoặc các thành phần con của nó có thể được định vị vật lý ở các vị trí khác nhau, bao gồm việc được phân bổ sao cho các phần của các chức năng được thực hiện ở các vị trí vật lý khác nhau bởi một hoặc nhiều thành phần vật lý. Theo một số ví dụ, bộ quản lý truyền thông UE 415, hoặc các thành phần con của nó, có thể là thành phần riêng và khác biệt theo các khía cạnh khác nhau của sáng chế. Theo một số ví dụ, bộ quản lý truyền thông UE 415, hoặc các thành phần con của nó có thể được kết hợp với một hoặc nhiều thành phần phần cứng khác, bao gồm nhưng không bị giới hạn ở thành phần đầu ra/ đầu vào (I/O), bộ thu phát, máy chủ mạng, thiết bị điện toán khác, một hoặc nhiều thành phần khác được mô tả trong sáng chế, hoặc sự kết hợp của chúng theo các khía cạnh khác nhau của sáng chế.

Bộ phát 420 có thể truyền các tín hiệu được tạo ra bởi các thành phần khác của thiết bị 405. Theo một số ví dụ, bộ phát 420 có thể được đặt cùng vị trí với bộ thu 410 trong mođun thu phát. Ví dụ, bộ phát 420 có thể là ví dụ của bộ thu phát 720 theo các khía cạnh được mô tả dựa vào Fig.7. Bộ phát 420 có thể sử dụng một anten hoặc bộ anten.

Fig.5 thể hiện sơ đồ khối 500 của thiết bị 505 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Thiết bị 505 có thể là ví dụ về các khía cạnh của thiết bị 405, hoặc UE 115 như được mô tả ở đây. Thiết bị 505 có thể bao gồm bộ thu 510, bộ quản lý truyền thông UE 515 và bộ phát 535. Thiết bị 505 cũng có thể bao gồm bộ xử lý. Mỗi trong số các thành phần này có thể truyền thông với nhau (ví dụ, qua một hoặc nhiều bus).

Bộ thu 510 có thể nhận thông tin như gói, dữ liệu người dùng, hoặc thông tin điều khiển gắn với các kênh thông tin khác nhau (ví dụ, kênh điều khiển, kênh dữ liệu, và thông tin liên quan đến bảo vệ SI tại NF trong mạng lõi, v.v.) Thông tin có thể được truyền đến các thành phần khác của thiết bị 505. Bộ thu 510 có thể là ví dụ về các khía cạnh của bộ thu phát 720 được mô tả liên quan đến Fig.7. Bộ thu 510 có thể sử dụng một anten hoặc bộ anten.

Bộ quản lý truyền thông UE 515 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông UE 415 như được mô tả ở đây. Bộ quản lý truyền thông UE 515 có thể bao gồm thành phần yêu cầu đăng ký 520, thành phần đáp ứng đăng ký 525, và thành phần giám sát bản tin SI 530. Bộ quản lý truyền thông UE 515 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông UE 710 được mô tả ở đây.

Thành phần yêu cầu đăng ký 520 có thể truyền yêu cầu đăng ký đến nút mạng lõi (ví dụ, AMF).

Thành phần đáp ứng đăng ký 525 có thể nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất.

Thành phần giám sát bản tin SI 530 có thể giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai.

Dựa vào việc nhận đáp ứng đăng ký và tạo ra nhiều chữ ký, bộ xử lý của UE 115 (ví dụ, điều khiển bộ thu 510, bộ phát 535, hoặc bộ thu phát 720 như được mô tả liên quan đến Fig.7) có thể ngăn không cho UE 115 tiêu tốn năng lượng pin không cần thiết bằng việc bị mắc kẹt trong cuộc tấn công DoS như được mô tả ở trên. Ngoài ra, bộ xử lý của UE 115 có thể giảm hao tổn báo hiệu bằng việc nhận đáp ứng đăng ký và tạo ra nhiều chữ ký thay vì tạo ra một chữ ký trên mỗi đáp ứng đăng ký, trong đó mỗi đáp ứng đăng ký được truyền và xử lý bởi bộ xử lý của UE 115.

Bộ phát 535 có thể truyền các tín hiệu được tạo ra bởi các thành phần khác của thiết bị 505. Theo một số ví dụ, bộ phát 535 có thể được đặt cùng vị trí với bộ thu 510 trong mođun thu phát. Ví dụ, bộ phát 535 có thể là ví dụ về các khía cạnh của bộ thu phát 720 được mô tả dựa vào Fig.7. Bộ phát 535 có thể sử dụng một anten hoặc bộ anten.

Fig.6 thể hiện sơ đồ khối 600 của bộ quản lý truyền thông UE 605 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Bộ quản lý truyền thông UE 605 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông UE 415, bộ quản lý truyền thông UE 515, hoặc bộ quản lý truyền thông UE 710 được mô tả ở đây. Bộ quản lý truyền thông UE 605 có thể bao gồm thành phần yêu cầu đăng ký 610, thành phần đáp ứng đăng ký 615, thành phần giám sát bản tin SI 620, và thành phần xác minh SI 625. Mỗi trong số các mođun này có thể truyền thông, trực tiếp hoặc gián tiếp, với nhau (ví dụ, qua một hoặc nhiều bus).

Thành phần yêu cầu đăng ký 610 có thể truyền yêu cầu đăng ký đến nút mạng lõi (ví dụ, AMF). Theo một số ví dụ, thành phần yêu cầu đăng ký 610 có thể truyền yêu cầu cập nhật đăng ký di động chỉ báo rằng UE đã di chuyển từ vùng theo dõi thứ nhất đến vùng theo dõi thứ hai.

Thành phần đáp ứng đăng ký 615 có thể nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất.

Thành phần giám sát bản tin SI 620 có thể giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai. Theo một số ví dụ, thành phần giám sát bản tin SI 620 có thể nhận bản tin SI chỉ báo một mã định danh (ví

dụ, ID khóa) của khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất.

Thành phần xác minh SI 625 có thể nhận bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất và có thể xác minh SI thứ nhất dựa vào chữ ký thứ nhất. Theo một số ví dụ, thành phần xác minh SI 625 có thể thiết lập kết nối với trạm gốc trong vùng theo dõi thứ nhất dựa vào SI thứ nhất được xác minh. Ngoài ra hoặc theo cách khác, thành phần xác minh SI 625 có thể nhận bản tin SI bao gồm SI thứ hai và chữ ký thứ hai và có thể xác minh SI thứ hai dựa vào chữ ký thứ hai. Theo đó, thành phần xác minh SI 625 có thể thiết lập kết nối với trạm gốc trong vùng theo dõi thứ hai dựa vào SI thứ hai được xác minh.

Fig.7 thể hiện sơ đồ của hệ thống 700 bao gồm thiết bị 705 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Thiết bị 705 có thể là ví dụ về hoặc bao gồm các thành phần của thiết bị 405, thiết bị 505, hoặc UE 115 như được mô tả ở đây. Thiết bị 705 có thể bao gồm các thành phần cho các cuộc truyền thông thoại và dữ liệu hai chiều bao gồm các thành phần để truyền và nhận các cuộc truyền thông, bao gồm bộ quản lý truyền thông UE 710, bộ điều khiển đầu vào/đầu ra (Input/Ouput - I/O) 715, bộ thu phát 720, anten 725, bộ nhớ 730, và bộ xử lý 740. Các thành phần này có thể truyền thông điện tử qua một hoặc nhiều bus (ví dụ, bus 745).

Bộ quản lý truyền thông UE 710 có thể truyền yêu cầu đăng ký đến nút mạng lõi (ví dụ, AMF). Ngoài ra, bộ quản lý truyền thông UE 710 có thể nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất. Sau đó, bộ quản lý truyền thông UE 710 có thể giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai.

Bộ điều khiển I/O 715 có thể quản lý các tín hiệu đầu vào và đầu ra cho thiết bị 705. Bộ điều khiển I/O 715 có thể còn quản lý các thiết bị ngoại vi không được tích hợp vào thiết bị 705. Trong một số trường hợp, bộ điều khiển I/O 715 có thể biểu diễn kết nối hoặc cổng vật lý với thiết bị ngoại vi bên ngoài. Trong một số trường hợp, bộ điều khiển I/O 715 có thể sử dụng hệ điều hành như iOS®, ANDROID®, MS-DOS®, MS-

WINDOWS®, OS/2®, UNIX®, LINUX®, hoặc một hệ điều hành đã biết khác. Trong các trường hợp khác, bộ điều khiển I/O 715 có thể biểu diễn hoặc tương tác với modem, bàn phím, chuột, màn hình cảm ứng, hoặc thiết bị tương tự. Trong một số trường hợp, bộ điều khiển I/O 715 có thể được cài đặt như là một phần của bộ xử lý. Trong một số trường hợp, người dùng có thể tương tác với thiết bị 705 qua bộ điều khiển I/O 715 hoặc qua các thành phần phần cứng được điều khiển bởi bộ điều khiển I/O 715.

Bộ thu phát 720 có thể truyền thông hai chiều, qua một hoặc nhiều anten, các liên kết có dây hoặc không dây như được mô tả ở trên. Ví dụ, bộ thu phát 720 có thể biểu diễn bộ thu phát không dây và có thể truyền thông hai chiều với một bộ thu phát không dây khác. Bộ thu phát 720 cũng có thể bao gồm modem để điều chế các gói và cung cấp các gói đã điều chế đến các anten để truyền, và giải điều chế các gói thu được từ các anten.

Trong một số trường hợp, thiết bị không dây có thể bao gồm một anten 725. Tuy nhiên, trong một số trường hợp thiết bị này có thể có nhiều hơn một anten 725, có khả năng truyền hoặc thu đồng thời nhiều tín hiệu truyền không dây.

Bộ nhớ 730 có thể bao gồm bộ nhớ truy cập ngẫu nhiên (random - access memory - RAM) và bộ nhớ chỉ đọc (read-only memory - ROM). Bộ nhớ 730 có thể lưu trữ mã đọc được bằng máy tính và thực thi được bằng máy tính 735 bao gồm các lệnh mà, khi được thực thi, khiến cho bộ xử lý thực hiện các chức năng khác nhau được mô tả ở đây. Trong một số trường hợp, bộ nhớ 730 có thể chứa, trong số các thành phần khác, hệ thống I/O cơ bản (basic input/output system - BIOS) mà có thể điều khiển thao tác phần cứng hoặc phần mềm cơ bản như tương tác với các thành phần hoặc thiết bị ngoại vi.

Bộ xử lý 740 có thể bao gồm thiết bị phần cứng thông minh (ví dụ, bộ xử lý đa dụng, DSP, bộ xử lý trung tâm (central processing unit - CPU), bộ vi điều khiển, ASIC, FPGA, thiết bị logic lập trình được, thành phần cổng rời rạc hoặc logic bán dẫn, thành phần phần cứng rời rạc, hoặc kết hợp bất kỳ của chúng). Trong một số trường hợp, bộ xử lý 740 có thể được tạo cấu hình để vận hành mảng bộ nhớ bằng cách sử dụng bộ điều khiển bộ nhớ. Trong các trường hợp khác, bộ điều khiển bộ nhớ có thể được tích hợp vào bộ xử lý 740. Bộ xử lý 740 có thể được tạo cấu hình để thực thi các lệnh đọc được bằng máy tính lưu trữ trong bộ nhớ (ví dụ, bộ nhớ 730) để khiến cho thiết bị 705 thực hiện các chức năng khác nhau (ví dụ, các chức năng hoặc tác vụ hỗ trợ bảo vệ SI tại NF trong

mạng lõi).

Mã 735 có thể bao gồm các lệnh để thực thi các khía cạnh của sáng chế, bao gồm các lệnh hỗ trợ truyền thông không dây. Mã 735 có thể được lưu trữ trong phương tiện bất biến đọc được bằng máy tính như bộ nhớ hệ thống hoặc loại bộ nhớ khác. Trong một số trường hợp, mã 735 có thể không được thực thi trực tiếp bởi bộ xử lý 740 nhưng có thể khiến cho máy tính (ví dụ, khi được biên soạn và thực thi) thực hiện các chức năng được mô tả ở đây.

Fig.8 thể hiện sơ đồ khối 800 của thiết bị 805 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Thiết bị 805 có thể là ví dụ về các khía cạnh của trạm gốc 105 như được mô tả ở đây. Thiết bị 805 có thể bao gồm bộ thu 810, bộ quản lý truyền thông trạm gốc 815 và bộ phát 820. Thiết bị 805 cũng có thể bao gồm bộ xử lý. Mỗi trong số các thành phần này có thể truyền thông với nhau (ví dụ, qua một hoặc nhiều bus).

Bộ thu 810 có thể nhận thông tin như gói, dữ liệu người dùng, hoặc thông tin điều khiển gắn với các kênh thông tin khác nhau (ví dụ, kênh điều khiển, kênh dữ liệu, và thông tin liên quan đến bảo vệ SI tại NF trong mạng lõi, v.v.) Thông tin có thể được truyền đến các thành phần khác của thiết bị 805. Bộ thu 810 có thể là ví dụ các khía cạnh của bộ thu phát 1120 được mô tả liên quan đến Fig.11. Bộ thu 810 có thể sử dụng một anten hoặc bộ anten.

Bộ quản lý truyền thông trạm gốc 815 có thể truyền, đến nút mạng (ví dụ, NF ký, nút RAN, nút AF, AMF, nút mạng lõi, hoặc tương tự), yêu cầu chữ ký bao gồm SI. Trong một số trường hợp, bộ quản lý truyền thông trạm gốc 815 có thể nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI. Ngoài ra, bộ quản lý truyền thông trạm gốc 815 có thể truyền (ví dụ, phát quảng bá) bản tin SI bao gồm SI và chữ ký. Bộ quản lý truyền thông trạm gốc 815 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông trạm gốc 1110 được mô tả ở đây.

Dựa vào các hoạt động thực hiện bởi bộ quản lý truyền thông trạm gốc 815 như được mô tả ở đây, trạm gốc 105 có thể tăng cường bảo mật trong hệ thống bằng cách truy hồi các đáp ứng chữ ký từ nút mạng (ví dụ, NF ký). Ví dụ, các đáp ứng chữ ký có thể bao gồm các chữ ký được tạo ra tại nút mạng thay vì nhận khóa riêng tư và ký chính bản tin SI. Nhờ tách việc tạo chữ ký ra khỏi sự kiểm soát của trạm gốc 105, trạm gốc 105

có thể không bị khai thác bởi kẻ tấn công bởi vì trạm gốc 105 không có bản ghi của các khóa riêng tư lưu trữ trong trạm gốc 105.

Bộ quản lý truyền thông trạm gốc 815, hoặc các thành phần con của nó, có thể được thực thi trong phần cứng, mã (ví dụ, phần mềm hoặc firmware) được thực thi bởi bộ xử lý, hoặc kết hợp bất kỳ của chúng. Nếu được thực hiện bằng mã do bộ xử lý thực thi, các chức năng của bộ quản lý truyền thông trạm gốc 815, hoặc các thành phần con của nó có thể được thực thi bởi bộ xử lý đa dụng, bộ xử lý tín hiệu số (digital signal processor - DSP), mạch tích hợp chuyên dụng (ASIC), mảng cổng lập trình được theo trường (field programmable gate array - FPGA) hoặc các thiết bị logic lập trình được khác, cổng rời rạc hoặc mạch logic tranzito, các thành phần phần cứng rời rạc, hoặc kết hợp bất kỳ giữa chúng được thiết kế để thực hiện các chức năng được mô tả trong sáng chế.

Bộ quản lý truyền thông trạm gốc 815, hoặc các thành phần con của nó có thể được định vị vật lý ở các vị trí khác nhau, bao gồm việc được phân bổ sao cho các phần của các chức năng được thực hiện ở các vị trí vật lý khác nhau bởi một hoặc nhiều thành phần vật lý. Theo một số ví dụ, bộ quản lý truyền thông trạm gốc 815, hoặc các thành phần con của nó, có thể là thành phần riêng và khác biệt theo các khía cạnh khác nhau của sáng chế. Theo một số ví dụ, bộ quản lý truyền thông trạm gốc 815, hoặc các thành phần con của nó có thể được kết hợp với một hoặc nhiều thành phần phần cứng khác, bao gồm nhưng không bị giới hạn ở thành phần I/O, bộ thu phát, máy chủ mạng, thiết bị điện toán khác, một hoặc nhiều thành phần khác được mô tả trong sáng chế, hoặc sự kết hợp của chúng theo khía cạnh khác nhau của sáng chế.

Bộ phát 820 có thể truyền các tín hiệu được tạo ra bởi các thành phần khác của thiết bị 805. Theo một số ví dụ, bộ phát 820 có thể được đặt cùng vị trí với bộ thu 810 trong mođun thu phát. Ví dụ, bộ phát 820 có thể là ví dụ về các khía cạnh của bộ thu phát 1120 được mô tả dựa vào Fig.11. Bộ phát 820 có thể sử dụng một anten hoặc bộ anten.

Fig.9 thể hiện sơ đồ khối 900 của thiết bị 905 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Thiết bị 905 có thể là ví dụ về các khía cạnh của thiết bị 805, hoặc trạm gốc 105 như được mô tả ở đây. Thiết bị 905 có thể bao gồm bộ thu 910, bộ quản lý truyền thông trạm gốc 915 và bộ phát 935. Thiết bị 905 cũng có thể bao gồm bộ xử lý. Mỗi trong số các thành phần này có thể truyền thông với nhau (ví dụ,

qua một hoặc nhiều bus).

Bộ thu 910 có thể nhận thông tin như gói, dữ liệu người dùng, hoặc thông tin điều khiển gắn với các kênh thông tin khác nhau (ví dụ, kênh điều khiển, kênh dữ liệu, và thông tin liên quan đến bảo vệ SI tại NF trong mạng lõi, v.v.) Thông tin có thể được truyền đến các thành phần khác của thiết bị 905. Bộ thu 910 có thể là ví dụ về các khía cạnh của bộ thu phát 1120 được mô tả liên quan đến Fig.11. Bộ thu 910 có thể sử dụng một anten hoặc bộ anten.

Bộ quản lý truyền thông trạm gốc 915 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông trạm gốc 815 như được mô tả ở đây. Bộ quản lý truyền thông trạm gốc 915 có thể bao gồm bộ phát yêu cầu chữ ký 920, bộ thu đáp ứng chữ ký 925, và bộ phát bản tin SI 930. Bộ quản lý truyền thông trạm gốc 915 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông trạm gốc 1110 được mô tả ở đây.

Bộ phát yêu cầu chữ ký 920 có thể truyền, đến nút mạng (ví dụ, nút RAN, nút AF, AMF, nút mạng lõi, NF ký, hoặc tương tự), yêu cầu chữ ký bao gồm SI.

Bộ thu đáp ứng chữ ký 925 có thể nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI.

Bộ phát bản tin SI 930 có thể truyền (ví dụ, phát quảng bá) bản tin SI bao gồm SI và chữ ký.

Bộ phát 935 có thể truyền các tín hiệu được tạo ra bởi các thành phần khác của thiết bị 905. Theo một số ví dụ, bộ phát 935 có thể được đặt cùng vị trí với bộ thu 910 trong mođun thu phát. Ví dụ, bộ phát 935 có thể là ví dụ về các khía cạnh của bộ thu phát 1120 được mô tả dựa vào Fig.11. Bộ phát 935 có thể sử dụng một anten hoặc bộ anten.

Fig.10 thể hiện sơ đồ khối 1000 của bộ quản lý truyền thông trạm gốc 1005 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Bộ quản lý truyền thông trạm gốc 1005 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông trạm gốc 815, bộ quản lý truyền thông trạm gốc 915, hoặc bộ quản lý truyền thông trạm gốc 1110 được mô tả ở đây. Bộ quản lý truyền thông trạm gốc 1005 có thể bao gồm bộ phát yêu cầu chữ ký 1010, bộ thu đáp ứng chữ ký 1015, bộ phát bản tin SI 1020, thành phần cập nhật SI 1025, thành phần vùng theo dõi 1030, thành phần yêu cầu chữ ký hàng loạt 1035, và thành phần độ mới chữ ký 1040. Mỗi trong số các mođun này có thể truyền

thông, trực tiếp hoặc gián tiếp, với nhau (ví dụ, qua một hoặc nhiều bus).

Bộ phát yêu cầu chữ ký 1010 có thể truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI. Theo một số ví dụ, bộ phát yêu cầu chữ ký 1010 có thể truyền yêu cầu chữ ký bao gồm SI và thông tin chính (ví dụ, MIB/SIB), trong đó chữ ký được tạo ra dựa vào SI và thông tin chính. Ngoài ra hoặc theo cách khác, bộ phát yêu cầu chữ ký 1010 có thể truyền yêu cầu chữ ký để yêu cầu một tập hợp chữ ký (ví dụ, yêu cầu chữ ký hàng loạt) cho một phạm vi thời gian và khoảng tăng thời gian.

Bộ thu đáp ứng chữ ký 1015 có thể nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI. Theo một số ví dụ, bộ thu đáp ứng chữ ký 1015 có thể nhận đáp ứng chữ ký bao gồm tập hợp chữ ký. Ngoài ra hoặc theo cách khác, bộ thu đáp ứng chữ ký 1015 có thể nhận tập hợp đáp ứng chữ ký, mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều tập hợp chữ ký, trong đó mỗi trong số các tập con tương ứng với khoảng tăng thời gian riêng trong phạm vi thời gian.

Bộ phát bản tin SI 1020 có thể truyền bản tin SI bao gồm SI và chữ ký. Theo một số ví dụ, bộ phát bản tin SI 1020 có thể truyền bản tin SI chỉ báo mã định danh của khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký.

Thành phần cập nhật SI 1025 có thể truyền, đến nút mạng, yêu cầu chữ ký thứ hai bao gồm SI cập nhật và có thể nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký thứ hai được tạo ra dựa vào SI cập nhật. Theo một số ví dụ, thành phần cập nhật SI 1025 có thể truyền bản tin SI bao gồm SI cập nhật và chữ ký thứ hai.

Thành phần vùng theo dõi 1030 có thể nhận yêu cầu đăng ký từ UE và có thể truyền yêu cầu đăng ký đến nút mạng mà cung cấp AMF. Theo một số ví dụ, thành phần vùng theo dõi 1030 có thể nhận, từ nút mạng, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký và có thể truyền đáp ứng đăng ký đến UE. Theo một số ví dụ, thành phần vùng theo dõi 1030 có thể truyền đáp ứng đăng ký bao gồm vùng theo dõi thứ nhất cho khóa công khai thứ nhất. Sau đó, thành phần vùng theo dõi 1030 có thể truyền đáp ứng đăng ký chỉ báo khóa công khai thứ hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất, khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai được truyền trong vùng theo dõi thứ hai. Theo một số ví dụ, thành phần vùng theo dõi 1030 có thể nhận yêu cầu cập nhật đăng ký di động từ UE chỉ báo rằng UE

đã vào vùng theo dõi mới.

Thành phần yêu cầu chữ ký hàng loạt 1035 có thể truyền yêu cầu chữ ký chỉ báo khoảng tăng khung con và yêu cầu một tập hợp chữ ký tương ứng với phạm vi số khung con giữa số khung con bắt đầu và số khung con kết thúc. Theo một số ví dụ, thành phần yêu cầu chữ ký hàng loạt 1035 có thể nhận đáp ứng chữ ký bao gồm tập hợp chữ ký. Ngoài ra hoặc theo cách khác, thành phần yêu cầu chữ ký hàng loạt 1035 có thể nhận tập hợp đáp ứng chữ ký, mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều tập hợp chữ ký. Trong một số trường hợp, mỗi trong số các tập con có thể tương ứng với khoảng tăng khung con riêng trong phạm vi số khung con.

Thành phần độ mới chữ ký 1040 có thể truyền yêu cầu chữ ký bao gồm thông số truy cập gần đây. Ngoài ra, thành phần độ mới chữ ký 1040 có thể nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký mà được tạo ra dựa vào SI và thông số truy cập gần đây. Trong một số trường hợp, thông số truy cập gần đây có thể là SFN.

Fig.11 thể hiện sơ đồ của hệ thống 1100 bao gồm thiết bị 1105 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Thiết bị 1105 có thể là ví dụ về hoặc bao gồm các thành phần của thiết bị 805, thiết bị 905, hoặc trạm gốc 105 như được mô tả ở đây. Thiết bị 1105 có thể bao gồm các thành phần để truyền thông giọng nói và dữ liệu hai chiều bao gồm các thành phần để truyền và thu các cuộc truyền thông, bao gồm bộ quản lý truyền thông trạm gốc 1110, bộ quản lý truyền thông mạng 1115, bộ thu phát 1120, anten 1125, bộ nhớ 1130, bộ xử lý 1140, và bộ quản lý truyền thông liên trạm 1145. Các thành phần này có thể truyền thông điện tử qua một hoặc nhiều bus (ví dụ, bus 1150).

Bộ quản lý truyền thông trạm gốc 1110 có thể truyền, đến nút mạng (ví dụ, nút mạng lõi, NF ký), yêu cầu chữ ký bao gồm SI. Trong một số trường hợp, bộ quản lý truyền thông trạm gốc 1110 có thể nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI. Ngoài ra, bộ quản lý truyền thông trạm gốc 1110 có thể truyền bản tin SI bao gồm SI và chữ ký.

Bộ quản lý truyền thông mạng 1115 có thể quản lý truyền thông với mạng lõi (ví dụ, qua một hoặc nhiều liên kết backhaul có dây). Ví dụ, bộ quản lý truyền thông mạng 1115 có thể quản lý việc truyền các cuộc truyền dữ liệu cho thiết bị máy khách, ví dụ như một hoặc nhiều UE 115.

Bộ thu phát 1120 có thể truyền thông hai chiều, qua một hoặc nhiều anten, các liên kết có dây hoặc không dây như được mô tả ở trên. Ví dụ, bộ thu phát 1120 có thể biểu diễn bộ thu phát không dây và có thể truyền thông hai chiều với một bộ thu phát không dây khác. Bộ thu phát 1120 cũng có thể bao gồm mođem để điều chế các gói và cung cấp các gói đã điều chế đến các anten để truyền, và giải điều chế các gói thu được từ các anten.

Trong một số trường hợp, thiết bị không dây có thể bao gồm một anten 1125. Tuy nhiên, trong một số trường hợp thiết bị này có thể có nhiều hơn một anten 1125, có khả năng truyền hoặc thu đồng thời nhiều cuộc truyền không dây.

Bộ nhớ 1130 có thể bao gồm RAM, ROM, hoặc kết hợp của chúng. Bộ nhớ 1130 có thể lưu trữ mã đọc được bằng máy tính 1135 bao gồm các lệnh mà, khi được thực thi bởi bộ xử lý (ví dụ, bộ xử lý 1140) khiến cho thiết bị thực hiện các chức năng khác nhau được mô tả ở đây. Trong một số trường hợp, bộ nhớ 1130 có thể chứa, trong số các thành phần khác, BIOS mà có thể điều khiển thao tác phần cứng hoặc phần mềm cơ bản như tương tác với các thành phần hoặc thiết bị ngoại vi.

Bộ xử lý 1140 có thể bao gồm thiết bị phần cứng thông minh, (ví dụ bộ xử lý đa dụng, DSP, CPU, bộ vi điều khiển, ASIC, FPGA, thiết bị logic lập trình được, bộ phận cổng rời rạc hoặc logic bán dẫn, bộ phận phần cứng rời rạc, hoặc sự kết hợp bất kỳ của chúng). Trong một số trường hợp, bộ xử lý 1140 có thể được tạo cấu hình để vận hành mảng bộ nhớ bằng cách sử dụng bộ điều khiển bộ nhớ. Trong một số trường hợp, bộ điều khiển bộ nhớ có thể được tích hợp vào bộ xử lý 1140. Bộ xử lý 1140 có thể được tạo cấu hình để thực thi các lệnh đọc được bằng máy tính lưu trữ trong bộ nhớ (ví dụ, bộ nhớ 1130) để khiến cho thiết bị 1105 thực hiện các chức năng khác nhau (ví dụ, các chức năng hoặc tác vụ hỗ trợ bảo vệ SI tại NF trong mạng lõi).

Bộ quản lý truyền thông liên trạm 1145 có thể quản lý truyền thông với các trạm gốc 105 khác và có thể bao gồm bộ điều khiển hoặc bộ lập lịch để điều khiển truyền thông với các UE 115 phối hợp với các trạm gốc 105 khác. Ví dụ, bộ quản lý truyền thông liên trạm 1145 có thể điều phối lập lịch đối với các cuộc truyền đến UE 115 với một số kỹ thuật giảm nhiễu khác nhau như điều hướng chùm sóng hoặc truyền chung. Theo một số ví dụ, bộ quản lý truyền thông liên trạm 1145 có thể cung cấp giao diện X2 trong công nghệ mạng truyền thông không dây LTE/LTE-A để cung cấp truyền thông

giữa các trạm gốc 105.

Mã 1135 có thể bao gồm các lệnh để thực thi các khía cạnh của sáng chế, bao gồm các lệnh hỗ trợ truyền thông không dây. Mã 1135 có thể được lưu trữ trong phương tiện bất biến đọc được bằng máy tính như bộ nhớ hệ thống hoặc loại bộ nhớ khác. Trong một số trường hợp, mã 1135 có thể không được thực thi trực tiếp bởi bộ xử lý 1140 nhưng có thể khiến cho máy tính (ví dụ, khi được biên soạn và thực thi) thực hiện các chức năng được mô tả ở đây.

Fig.12 thể hiện sơ đồ khối 1200 của thiết bị 1205 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Thiết bị 1205 có thể là ví dụ về các khía cạnh của nút mạng (ví dụ, thực thể mạng, như nút mạng lõi) theo như được mô tả ở đây. Thiết bị 1205 có thể bao gồm bộ thu 1210, bộ quản lý truyền thông mạng 1215 và bộ phát 1220. Thiết bị 1205 cũng có thể bao gồm bộ xử lý. Mỗi trong số các thành phần này có thể truyền thông với nhau (ví dụ, qua một hoặc nhiều bus).

Bộ thu 1210 có thể nhận thông tin như gói, dữ liệu người dùng, hoặc thông tin điều khiển gắn với các kênh thông tin khác nhau (ví dụ, kênh điều khiển, kênh dữ liệu, và thông tin liên quan đến bảo vệ SI tại NF trong mạng lõi, v.v.) Thông tin có thể được truyền đến các thành phần khác của thiết bị 1205. Bộ thu 1210 có thể là ví dụ về các khía cạnh của bộ thu phát 1520 được mô tả liên quan đến Fig.15. Bộ thu 1210 có thể sử dụng một anten hoặc bộ anten.

Bộ quản lý truyền thông mạng 1215 có thể nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI. Ngoài ra, bộ quản lý truyền thông mạng 1215 có thể truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI. Bộ quản lý truyền thông mạng 1215 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông mạng 1510 được mô tả ở đây.

Dựa vào các hoạt động thực hiện bởi bộ quản lý truyền thông mạng 1215 như được mô tả ở đây, một hoặc nhiều chức năng trong mạng lõi (ví dụ, NF ký, AMF, v.v.) có thể tăng cường bảo mật trong hệ thống. Ví dụ, các chức năng của mạng lõi có thể lưu trữ thông tin khóa riêng tư ở hướng lên cao hơn so với trạm gốc 105, mà tại đó kẻ tấn công ít có khả năng có thể xâm nhập vào mạng lõi để lấy được thông tin khóa riêng tư. Theo đó, các chức năng của mạng lõi có thể ngăn các loại tấn công DoS khác nhau bằng việc lưu trữ thông tin khóa riêng tư và truyền chữ ký được tạo ra dựa vào thông tin khóa

riêng tư và bản tin SI.

Bộ quản lý truyền thông mạng 1215, hoặc các thành phần con của nó, có thể được thực thi trong phần cứng, mã (ví dụ, phần mềm hoặc firmware) được thực thi bởi bộ xử lý, hoặc kết hợp bất kỳ của chúng. Nếu được thực hiện bằng mã do bộ xử lý thực thi, các chức năng của bộ quản lý truyền thông mạng 1215, hoặc các thành phần con của nó có thể được thực thi bởi bộ xử lý đa dụng, bộ xử lý tín hiệu số (digital signal processor - DSP), mạch tích hợp chuyên dụng (ASIC), mảng cổng lập trình được theo trường (field programmable gate array - FPGA) hoặc các thiết bị logic lập trình được khác, cổng rời rạc hoặc mạch logic tranzito, các thành phần phần cứng rời rạc, hoặc kết hợp bất kỳ giữa chúng được thiết kế để thực hiện các chức năng được mô tả trong sáng chế.

Bộ quản lý truyền thông mạng 1215, hoặc các thành phần con của nó có thể được định vị vật lý ở các vị trí khác nhau, bao gồm việc được phân bổ sao cho các phần của các chức năng được thực hiện ở các vị trí vật lý khác nhau bởi một hoặc nhiều thành phần vật lý. Theo một số ví dụ, bộ quản lý truyền thông mạng 1215, hoặc các thành phần con của nó, có thể là thành phần riêng và khác biệt theo các khía cạnh khác nhau của sáng chế. Theo một số ví dụ, bộ quản lý truyền thông mạng 1215, hoặc các thành phần con của nó có thể được kết hợp với một hoặc nhiều thành phần phần cứng khác, bao gồm nhưng không bị giới hạn ở thành phần I/O, bộ thu phát, máy chủ mạng, thiết bị điện toán khác, một hoặc nhiều thành phần khác được mô tả trong sáng chế, hoặc sự kết hợp của chúng theo khía cạnh khác nhau của sáng chế.

Bộ phát 1220 có thể truyền các tín hiệu được tạo ra bởi các thành phần khác của thiết bị 1205. Theo một số ví dụ, bộ phát 1220 có thể được đặt cùng vị trí với bộ thu 1210 trong mođun thu phát. Ví dụ, bộ phát 1220 có thể là ví dụ về các khía cạnh của bộ thu phát 1520 được mô tả dựa vào Fig.15. Bộ phát 1220 có thể sử dụng một anten hoặc bộ anten.

Fig.13 thể hiện sơ đồ khối 1300 của thiết bị 1305 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Thiết bị 1305 có thể là ví dụ về các khía cạnh của thiết bị 1205 hoặc thực thể mạng như được mô tả ở đây. Thiết bị 1305 có thể bao gồm bộ thu 1310, bộ quản lý truyền thông mạng 1315 và bộ phát 1330. Thiết bị 1305 cũng có thể bao gồm bộ xử lý. Mỗi trong số các thành phần này có thể truyền thông với nhau (ví dụ, qua một hoặc nhiều bus).

Bộ thu 1310 có thể nhận thông tin như gói, dữ liệu người dùng, hoặc thông tin điều khiển gắn với các kênh thông tin khác nhau (ví dụ, kênh điều khiển, kênh dữ liệu, và thông tin liên quan đến bảo vệ SI tại NF trong mạng lõi, v.v.) Thông tin có thể được truyền đến các thành phần khác của thiết bị 1305. Bộ thu 1310 có thể là ví dụ về các khía cạnh của bộ thu phát 1520 được mô tả liên quan đến Fig.15. Bộ thu 1310 có thể sử dụng một anten hoặc bộ anten.

Bộ quản lý truyền thông mạng 1315 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông mạng 1215 như được mô tả ở đây. Bộ quản lý truyền thông mạng 1315 có thể bao gồm bộ thu yêu cầu chữ ký 1320 và bộ phát đáp ứng chữ ký 1325. Bộ quản lý truyền thông mạng 1315 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông mạng 1510 được mô tả ở đây.

Bộ thu yêu cầu chữ ký 1320 có thể nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI.

Bộ phát đáp ứng chữ ký 1325 có thể truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI.

Bộ phát 1330 có thể truyền các tín hiệu được tạo ra bởi các thành phần khác của thiết bị 1305. Theo một số ví dụ, bộ phát 1330 có thể được đặt cùng vị trí với bộ thu 1310 trong mođun thu phát. Ví dụ, bộ phát 1330 có thể là ví dụ về các khía cạnh của bộ thu phát 1520 được mô tả dựa vào Fig.15. Bộ phát 1330 có thể sử dụng một anten hoặc bộ anten.

Fig.14 thể hiện sơ đồ khối 1400 của bộ quản lý truyền thông mạng 1405 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Bộ quản lý truyền thông mạng 1405 có thể là ví dụ về các khía cạnh của bộ quản lý truyền thông mạng 1215, bộ quản lý truyền thông mạng 1315, hoặc bộ quản lý truyền thông mạng 1510 được mô tả ở đây. Bộ quản lý truyền thông mạng 1405 có thể bao gồm bộ thu yêu cầu chữ ký 1410, bộ phát đáp ứng chữ ký 1415, thành phần chữ ký hàng loạt 1420, và mã định danh độ mới chữ ký 1425. Mỗi trong số các mođun này có thể truyền thông, trực tiếp hoặc gián tiếp, với nhau (ví dụ, qua một hoặc nhiều bus).

Bộ thu yêu cầu chữ ký 1410 có thể nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI. Theo một số ví dụ, bộ thu yêu cầu chữ ký 1410 có thể nhận yêu cầu chữ ký bao gồm SI và thông tin chính (ví dụ, MIB/SIB), trong đó chữ ký được tạo ra dựa vào SI và thông tin chính. Ngoài ra hoặc theo cách khác, bộ thu yêu cầu chữ ký 1410 có thể nhận, từ trạm

gốc, yêu cầu chữ ký thứ hai bao gồm SI cập nhật.

Bộ phát đáp ứng chữ ký 1415 có thể truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI. Theo một số ví dụ, bộ phát đáp ứng chữ ký 1415 có thể truyền bản tin mã định danh khóa chỉ báo mã định danh (ví dụ, ID khóa) của khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký. Theo một số ví dụ, bộ phát đáp ứng chữ ký 1415 có thể truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký thứ hai được tạo ra dựa vào SI cập nhật.

Thành phần chữ ký hàng loạt 1420 có thể nhận yêu cầu chữ ký mà yêu cầu một tập hợp chữ ký cho một phạm vi thời gian và khoảng tăng thời gian và có thể truyền đáp ứng chữ ký bao gồm tập hợp chữ ký. Ngoài ra hoặc theo cách khác, thành phần chữ ký hàng loạt 1420 có thể truyền tập hợp đáp ứng chữ ký, mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều tập hợp chữ ký, trong đó mỗi trong số các tập con tương ứng với khoảng tăng thời gian riêng trong phạm vi thời gian.

Theo một số ví dụ, thành phần chữ ký hàng loạt 1420 có thể nhận yêu cầu chữ ký chỉ báo khoảng tăng khung con và yêu cầu một tập hợp chữ ký tương ứng với phạm vi số khung con giữa số khung con bắt đầu và số khung con kết thúc và có thể nhận đáp ứng chữ ký bao gồm tập hợp chữ ký. Ngoài ra hoặc theo cách khác, thành phần chữ ký hàng loạt 1420 có thể nhận tập hợp đáp ứng chữ ký, mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều tập hợp chữ ký, trong đó mỗi trong số các tập con tương ứng với khoảng tăng khung con riêng trong phạm vi số khung con.

Mã định danh độ mới chữ ký 1425 có thể nhận yêu cầu chữ ký bao gồm thông số truy cập gần đây. Theo một số ví dụ, mã định danh độ mới chữ ký 1425 có thể truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký mà được tạo ra dựa vào SI và thông số truy cập gần đây. Trong một số trường hợp, thông số truy cập gần đây có thể là SFN.

Fig.15 thể hiện sơ đồ của hệ thống 1500 bao gồm thiết bị 1505 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Thiết bị 1505 có thể là ví dụ về hoặc bao gồm các thành phần của thiết bị 1205, thiết bị 1305, hoặc thực thể mạng như được mô tả ở đây. Thiết bị 1505 có thể bao gồm các thành phần cho các cuộc truyền thông thoại và dữ liệu hai chiều bao gồm các thành phần để truyền và nhận các cuộc truyền thông, bao gồm bộ quản lý truyền thông mạng 1510, bộ điều khiển đầu vào/đầu ra (Input/Ouput - I/O) 1515, bộ thu phát 1520, anten 1525, bộ nhớ 1530, và bộ xử lý 1535.

Các thành phần này có thể truyền thông điện tử qua một hoặc nhiều bus (ví dụ, bus 1545).

Bộ quản lý truyền thông mạng 1510 có thể nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI và truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI.

Bộ điều khiển I/O 1515 có thể quản lý các tín hiệu đầu vào và đầu ra cho thiết bị 1505. Bộ điều khiển I/O 1515 có thể còn quản lý các thiết bị ngoại vi không được tích hợp vào thiết bị 1505. Trong một số trường hợp, bộ điều khiển I/O 1515 có thể biểu diễn kết nối hoặc cổng vật lý với thiết bị ngoại vi. Trong một số trường hợp, bộ điều khiển I/O 1515 có thể sử dụng hệ điều hành như iOS®, vàROID®, MS-DOS®, MS-WINDOWS®, OS/2®, UNIX®, LINUX® hoặc hệ điều hành đã biết khác. Trong các trường hợp khác, bộ điều khiển I/O 1515 có thể biểu diễn hoặc tương tác với mođem, bàn phím, chuột, màn hình cảm ứng, hoặc thiết bị tương tự. Trong một số trường hợp, bộ điều khiển I/O 1515 có thể được cài đặt như là một phần của bộ xử lý. Trong một số trường hợp, người dùng có thể tương tác với thiết bị 1505 qua bộ điều khiển I/O 1515 hoặc qua các thành phần phần cứng được điều khiển bởi bộ điều khiển I/O 1515.

Bộ thu phát 1520 có thể truyền thông hai chiều, qua một hoặc nhiều anten, các liên kết có dây hoặc không dây như được mô tả ở trên. Ví dụ, bộ thu phát 1520 có thể biểu diễn bộ thu phát không dây và có thể truyền thông hai chiều với một bộ thu phát không dây khác. Bộ thu phát 1520 cũng có thể bao gồm mođem để điều chế các gói và cung cấp các gói đã điều chế đến các anten để truyền, và giải điều chế các gói thu được từ các anten.

Trong một số trường hợp, thiết bị không dây có thể bao gồm một anten 1525. Tuy nhiên, trong một số trường hợp thiết bị này có thể có nhiều hơn một anten 1525, có khả năng truyền hoặc thu đồng thời nhiều cuộc truyền không dây.

Bộ nhớ 1530 có thể bao gồm RAM và ROM. Bộ nhớ 1530 có thể lưu trữ mã đọc được bằng máy tính và thực thi được bằng máy tính 1540 chứa các lệnh mà, khi được thực thi, khiến cho bộ xử lý thực hiện các chức năng khác nhau được mô tả ở đây. Trong một số trường hợp, bộ nhớ 1530 có thể chứa, trong số các thành phần khác, BIOS mà có thể điều khiển thao tác phần cứng hoặc phần mềm cơ bản như tương tác với các thành phần hoặc thiết bị ngoại vi.

Bộ xử lý 1535 có thể bao gồm thiết bị phần cứng thông minh, (ví dụ bộ xử lý đa

năng, DSP, CPU, bộ vi điều khiển, ASIC, FPGA, thiết bị logic lập trình được, bộ phận cổng rời rạc hoặc logic bán dẫn, bộ phận phần cứng rời rạc, hoặc sự kết hợp bất kỳ của chúng). Trong một số trường hợp, bộ xử lý 1535 có thể được tạo cấu hình để vận hành mảng bộ nhớ bằng cách sử dụng bộ điều khiển bộ nhớ. Trong các trường hợp khác, bộ điều khiển bộ nhớ có thể được tích hợp vào bộ xử lý 1535. Bộ xử lý 1535 có thể được tạo cấu hình để thực thi các lệnh đọc được bằng máy tính lưu trữ trong bộ nhớ (ví dụ, bộ nhớ 1530) để khiến cho thiết bị 1505 thực hiện các chức năng khác nhau (ví dụ, các chức năng hoặc tác vụ hỗ trợ bảo vệ SI tại NF trong mạng lõi).

Mã 1540 có thể bao gồm các lệnh để thực thi các khía cạnh của sáng chế, bao gồm các lệnh hỗ trợ truyền thông không dây. Mã 1540 có thể được lưu trữ trong phương tiện bất biến đọc được bằng máy tính như bộ nhớ hệ thống hoặc loại bộ nhớ khác. Trong một số trường hợp, mã 1540 có thể không được thực thi trực tiếp bởi bộ xử lý 1535 nhưng có thể khiến cho máy tính (ví dụ, khi được biên soạn và thực thi) thực hiện các chức năng được mô tả ở đây.

Fig.16 thể hiện lưu đồ minh họa phương pháp 1600 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Các thao tác của phương pháp 1600 có thể được thực hiện bởi trạm gốc 105 hoặc các thành phần của nó như mô tả ở đây. Ví dụ, các thao tác của phương pháp 1600 có thể được thực hiện bởi bộ quản lý truyền thông trạm gốc như được mô tả liên quan đến các từ Fig.8 đến Fig.11. Theo một số ví dụ, trạm gốc có thể thực thi một tập lệnh để điều khiển các phần tử chức năng của trạm gốc để thực hiện các chức năng mô tả dưới đây. Ngoài ra hoặc theo cách khác, trạm gốc có thể thực hiện các khía cạnh của các chức năng được mô tả dưới đây bằng cách sử dụng phần cứng chuyên dụng.

Ở khối 1605, trạm gốc có thể truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI. Các thao tác ở khối 1605 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1605 có thể được thực hiện bởi bộ phát yêu cầu chữ ký như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1610, trạm gốc có thể nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI. Các thao tác ở khối 1610 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1610 có thể được thực hiện bởi bộ thu đáp ứng chữ ký như được mô tả liên quan đến các Fig.8

đến Fig.11.

Ở khối 1615, trạm gốc có thể truyền bản tin SI bao gồm SI và chữ ký. Các thao tác ở khối 1615 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1615 có thể được thực hiện bởi bộ phát bản tin SI như được mô tả liên quan đến các Fig.8 đến Fig.11.

Fig.17 thể hiện lưu đồ minh họa phương pháp 1700 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Các thao tác của phương pháp 1700 có thể được thực hiện bởi trạm gốc 105 hoặc các thành phần của nó như mô tả ở đây. Ví dụ, các thao tác của phương pháp 1700 có thể được thực hiện bởi bộ quản lý truyền thông trạm gốc như được mô tả liên quan đến các Fig.8 đến Fig.11. Theo một số ví dụ, trạm gốc có thể thực thi một tập lệnh để điều khiển các phần tử chức năng của trạm gốc để thực hiện các chức năng mô tả dưới đây. Ngoài ra hoặc theo cách khác, trạm gốc có thể thực hiện các khía cạnh của các chức năng được mô tả dưới đây bằng cách sử dụng phần cứng chuyên dụng.

Ở khối 1705, trạm gốc có thể truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI. Các thao tác ở khối 1705 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1705 có thể được thực hiện bởi bộ phát yêu cầu chữ ký như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1710, trạm gốc có thể truyền yêu cầu chữ ký bao gồm SI và thông tin chính, trong đó chữ ký được tạo ra dựa vào SI và thông tin chính. Các thao tác ở khối 1710 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1710 có thể được thực hiện bởi bộ phát yêu cầu chữ ký như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1715, trạm gốc có thể nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI. Các thao tác ở khối 1715 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1715 có thể được thực hiện bởi bộ thu đáp ứng chữ ký như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1720, trạm gốc có thể truyền bản tin SI bao gồm SI và chữ ký. Các thao tác ở khối 1720 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1720 có thể được thực hiện bởi bộ phát

bản tin SI như được mô tả liên quan đến các Fig.8 đến Fig.11.

Fig.18 thể hiện lưu đồ minh họa phương pháp 1800 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Các thao tác của phương pháp 1800 có thể được thực hiện bởi trạm gốc 105 hoặc các thành phần của nó như mô tả ở đây. Ví dụ, các thao tác của phương pháp 1800 có thể được thực hiện bởi bộ quản lý truyền thông trạm gốc như được mô tả liên quan đến các Fig.8 đến Fig.11. Theo một số ví dụ, trạm gốc có thể thực thi một tập lệnh để điều khiển các phần tử chức năng của trạm gốc để thực hiện các chức năng mô tả dưới đây. Ngoài ra hoặc theo cách khác, trạm gốc có thể thực hiện các khía cạnh của các chức năng được mô tả dưới đây bằng cách sử dụng phần cứng chuyên dụng.

Ở khối 1805, trạm gốc có thể truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI. Các thao tác ở khối 1805 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1805 có thể được thực hiện bởi bộ phát yêu cầu chữ ký như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1810, trạm gốc có thể nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI. Các thao tác ở khối 1810 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1810 có thể được thực hiện bởi bộ thu đáp ứng chữ ký như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1815, trạm gốc có thể truyền bản tin SI bao gồm SI và chữ ký. Các thao tác ở khối 1815 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1815 có thể được thực hiện bởi bộ phát bản tin SI như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1820, trạm gốc có thể truyền bản tin SI chỉ báo mã định danh của khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký. Các thao tác ở khối 1820 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1820 có thể được thực hiện bởi bộ phát bản tin SI như được mô tả liên quan đến các Fig.8 đến Fig.11.

Fig.19 thể hiện lưu đồ minh họa phương pháp 1900 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Các thao tác của phương pháp 1900 có thể được thực hiện bởi trạm gốc 105 hoặc các thành phần của nó như mô tả ở đây. Ví dụ, các

thao tác của phương pháp 1900 có thể được thực hiện bởi bộ quản lý truyền thông trạm gốc như được mô tả liên quan đến các Fig.8 đến Fig.11. Theo một số ví dụ, trạm gốc có thể thực thi một tập lệnh để điều khiển các phần tử chức năng của trạm gốc để thực hiện các chức năng mô tả dưới đây. Ngoài ra hoặc theo cách khác, trạm gốc có thể thực hiện các khía cạnh của các chức năng được mô tả dưới đây bằng cách sử dụng phần cứng chuyên dụng.

Ở khối 1905, trạm gốc có thể truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI. Các thao tác ở khối 1905 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1905 có thể được thực hiện bởi bộ phát yêu cầu chữ ký như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1910, trạm gốc có thể nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI. Các thao tác ở khối 1910 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1910 có thể được thực hiện bởi bộ thu đáp ứng chữ ký như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1915, trạm gốc có thể nhận yêu cầu đăng ký từ UE. Các thao tác ở khối 1915 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1915 có thể được thực hiện bởi thành phần vùng theo dõi như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1920, trạm gốc có thể truyền yêu cầu đăng ký đến nút mạng (ví dụ, nút mạng lõi) mà cung cấp chức năng quản lý truy cập và di động (AMF). Các thao tác ở khối 1920 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1920 có thể được thực hiện bởi thành phần vùng theo dõi như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1925, trạm gốc có thể nhận, từ nút mạng, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký. Các thao tác ở khối 1925 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1925 có thể được thực hiện bởi thành phần vùng theo dõi như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1930, trạm gốc có thể truyền đáp ứng đăng ký đến UE. Các thao tác ở khối 1930 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ,

các khía cạnh của các thao tác ở khối 1930 có thể được thực hiện bởi thành phần vùng theo dõi như được mô tả liên quan đến các Fig.8 đến Fig.11.

Ở khối 1935, trạm gốc có thể truyền bản tin SI bao gồm SI và chữ ký. Các thao tác ở khối 1935 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 1935 có thể được thực hiện bởi bộ phát bản tin SI như được mô tả liên quan đến các Fig.8 đến Fig.11.

Fig.20 thể hiện lưu đồ minh họa phương pháp 2000 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Các thao tác của phương pháp 2000 có thể được thực hiện bởi thực thể mạng hoặc các thành phần của nó như mô tả ở đây. Ví dụ, các thao tác của phương pháp 2000 có thể được thực hiện bởi bộ quản lý truyền thông mạng như được mô tả liên quan đến các Fig.12 đến Fig.15. Theo một số ví dụ, thực thể mạng có thể thực thi một tập lệnh để điều khiển các phần tử chức năng của thực thể mạng để thực hiện các chức năng mô tả dưới đây. Ngoài ra hoặc theo cách khác, thực thể mạng có thể thực hiện các khía cạnh của các chức năng được mô tả dưới đây bằng cách sử dụng phần cứng chuyên dụng.

Ở khối 2005, thực thể mạng có thể nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI. Các thao tác ở khối 2005 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2005 có thể được thực hiện bởi bộ thu yêu cầu chữ ký như được mô tả liên quan đến các Fig.12 đến Fig.15.

Ở khối 2010, thực thể mạng có thể truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI. Các thao tác ở khối 2010 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2010 có thể được thực hiện bởi bộ phát đáp ứng chữ ký như được mô tả liên quan đến các Fig.12 đến Fig.15.

Fig.21 thể hiện lưu đồ minh họa phương pháp 2100 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Các thao tác của phương pháp 2100 có thể được thực hiện bởi thực thể mạng hoặc các thành phần của nó như mô tả ở đây. Ví dụ, các thao tác của phương pháp 2100 có thể được thực hiện bởi bộ quản lý truyền thông mạng như được mô tả liên quan đến các Fig.12 đến Fig.15. Theo một số ví dụ, thực thể mạng có thể thực thi một tập lệnh để điều khiển các phần tử chức năng của thực thể mạng để thực hiện các chức năng mô tả dưới đây. Ngoài ra hoặc theo cách khác, thực thể

mạng có thể thực hiện các khía cạnh của các chức năng được mô tả dưới đây bằng cách sử dụng phần cứng chuyên dụng.

Ở khối 2105, thực thể mạng có thể nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI. Các thao tác ở khối 2105 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2105 có thể được thực hiện bởi bộ thu yêu cầu chữ ký như được mô tả liên quan đến các Fig.12 đến Fig.15.

Ở khối 2110, thực thể mạng có thể truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI. Các thao tác ở khối 2110 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2110 có thể được thực hiện bởi bộ phát đáp ứng chữ ký như được mô tả liên quan đến các Fig.12 đến Fig.15.

Ở khối 2115, thực thể mạng có thể nhận, từ trạm gốc, yêu cầu chữ ký thứ hai bao gồm SI cập nhật. Các thao tác ở khối 2115 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2115 có thể được thực hiện bởi bộ thu yêu cầu chữ ký như được mô tả liên quan đến các Fig.12 đến Fig.15.

Ở khối 2120, thực thể mạng có thể truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký thứ hai được tạo ra dựa vào SI cập nhật. Các thao tác ở khối 2120 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2120 có thể được thực hiện bởi bộ phát đáp ứng chữ ký như được mô tả liên quan đến các Fig.12 đến Fig.15.

Fig.22 thể hiện lưu đồ minh họa phương pháp 2200 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Các thao tác của phương pháp 2200 có thể được thực hiện bởi UE 115 hoặc các thành phần của nó như mô tả ở đây. Ví dụ, các thao tác của phương pháp 2200 có thể được thực hiện bởi bộ quản lý truyền thông UE như được mô tả liên quan đến các Fig.4 đến Fig.7. Theo một số ví dụ, UE có thể thực thi một tập lệnh để điều khiển các phần tử chức năng của UE để thực hiện các chức năng mô tả dưới đây. Ngoài ra hoặc theo cách khác, UE có thể thực hiện các khía cạnh của các chức năng được mô tả dưới đây bằng cách sử dụng phần cứng chuyên dụng.

Ở khối 2205, UE có thể truyền yêu cầu đăng ký đến nút mạng lõi. Các thao tác ở khối 2205 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví

dụ, các khía cạnh của các thao tác ở khối 2205 có thể được thực hiện bởi thành phần yêu cầu đăng ký như được mô tả liên quan đến các Fig.4 đến Fig.7.

Ở khối 2210, UE có thể nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất. Các thao tác ở khối 2210 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2210 có thể được thực hiện bởi thành phần đáp ứng đăng ký như được mô tả liên quan đến các Fig.4 đến Fig.7.

Ở khối 2215, UE có thể giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai. Các thao tác ở khối 2215 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2215 có thể được thực hiện bởi thành phần giám sát bản tin SI như được mô tả liên quan đến các Fig.4 đến Fig.7.

Fig.23 thể hiện lưu đồ minh họa phương pháp 2300 hỗ trợ bảo vệ SI tại NF trong mạng lõi theo các khía cạnh của sáng chế. Các thao tác của phương pháp 2300 có thể được thực hiện bởi UE 115 hoặc các thành phần của nó như mô tả ở đây. Ví dụ, các thao tác của phương pháp 2300 có thể được thực hiện bởi bộ quản lý truyền thông UE như được mô tả liên quan đến các Fig.4 đến Fig.7. Theo một số ví dụ, UE có thể thực thi một tập lệnh để điều khiển các phần tử chức năng của UE để thực hiện các chức năng mô tả dưới đây. Ngoài ra hoặc theo cách khác, UE có thể thực hiện các khía cạnh của các chức năng được mô tả dưới đây bằng cách sử dụng phần cứng chuyên dụng.

Ở khối 2305, UE có thể truyền yêu cầu đăng ký đến nút mạng lõi. Các thao tác ở khối 2305 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2305 có thể được thực hiện bởi thành phần yêu cầu đăng ký như được mô tả liên quan đến các Fig.4 đến Fig.7.

Ở khối 2310, UE có thể nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai cho vùng theo dõi thứ

hai mà được định vị địa lý so với vùng theo dõi thứ nhất. Các thao tác ở khối 2310 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2310 có thể được thực hiện bởi thành phần đáp ứng đăng ký như được mô tả liên quan đến các Fig.4 đến Fig.7.

Ở khối 2315, UE có thể giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai. Các thao tác ở khối 2315 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2315 có thể được thực hiện bởi thành phần giám sát bản tin SI như được mô tả liên quan đến các Fig.4 đến Fig.7.

Ở khối 2320, UE có thể truyền yêu cầu cập nhật đăng ký di động chỉ báo rằng UE đã di chuyển từ vùng theo dõi thứ nhất đến vùng theo dõi thứ hai. Các thao tác ở khối 2320 có thể được thực hiện theo các phương pháp được mô tả ở đây. Theo một số ví dụ, các khía cạnh của các thao tác ở khối 2320 có thể được thực hiện bởi thành phần yêu cầu đăng ký như được mô tả liên quan đến các Fig.4 đến Fig.7.

Cần lưu ý rằng các phương pháp được mô tả ở đây mô tả các phương án thực hiện có thể có, và các hoạt động và các bước có thể được sắp xếp lại hoặc theo cách khác được sửa đổi và các phương án thực hiện khác có thể được thực hiện. Hơn nữa, các khía cạnh của hai hay nhiều phương pháp này có thể được kết hợp.

Mặc dù các khía cạnh của hệ thống LTE, LTE-A, LTE-A Pro, hoặc NR có thể được mô tả cho mục đích minh họa, và thuật ngữ LTE, LTE-A, LTE-A Pro, hoặc NR có thể được sử dụng ở hầu hết phần mô tả, nhưng các kỹ thuật được mô tả ở đây là có thể áp dụng được ngoài các mạng LTE, LTE-A, LTE-A Pro, hoặc NR. Ví dụ, các kỹ thuật được mô tả có thể ứng dụng cho nhiều hệ thống truyền thông không dây khác như siêu băng rộng di động (Ultra Mobile Broadband - UMB), các chuẩn 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20 của Viện kỹ sư điện và điện tử (Institute of Electrical và Electronics Engineers - IEEE), Flash-OFDM, cũng như các hệ thống và công nghệ vô tuyến khác không được đề cập rõ ràng ở đây.

Các thông tin và tín hiệu mô tả trong bản mô tả này có thể được thể hiện bằng cách sử dụng công nghệ và kỹ thuật bất kỳ trong số nhiều công nghệ và kỹ thuật khác nhau. Ví dụ, dữ liệu, lệnh, chỉ lệnh, thông tin, tín hiệu, bit, ký hiệu, và chip mà có thể được mô tả trong suốt phần mô tả có thể được thể hiện bằng điện áp, dòng điện, sóng

điện từ, các từ trường hoặc hạt từ, các trường hoặc hạt quang học, hoặc dạng kết hợp bất kỳ của chúng.

Các khối và thành phần minh họa khác nhau được mô tả liên quan đến nội dung được bộc lộ ở đây có thể được thực thi hoặc thực hiện bởi bộ xử lý đa năng, DSP, ASIC, CPU, FPGA hoặc thiết bị logic lập trình được khác, cổng rời rạc hoặc logic tranzito, thành phần phần cứng rời rạc, hoặc kết hợp bất kỳ của chúng được thiết kế để thực hiện các chức năng được mô tả ở đây. Bộ xử lý đa dụng có thể là bộ vi xử lý, nhưng theo cách khác, bộ xử lý có thể là bộ xử lý, bộ điều khiển, bộ vi điều khiển, hoặc máy trạng thái bất kỳ. Bộ xử lý cũng có thể được thực hiện dưới dạng kết hợp của các thiết bị điện toán (ví dụ, kết hợp DSP và bộ vi xử lý, nhiều bộ vi xử lý, một hoặc nhiều bộ vi xử lý kết hợp với lõi DSP, hoặc bất kỳ cấu hình khác như vậy).

Các chức năng mô tả ở đây có thể được thực hiện bằng phần cứng, phần mềm được thực thi bởi bộ xử lý, firmware, hoặc dạng kết hợp bất kỳ của chúng. Nếu được thực hiện bằng phần mềm thực thi bởi bộ xử lý, các chức năng có thể được lưu trữ hoặc được truyền dưới dạng một hoặc nhiều lệnh hoặc mã trên phương tiện đọc được bằng máy tính. Các ví dụ và phương án khác đều nằm trong phạm vi của sáng chế và các điểm yêu cầu bảo hộ kèm theo. Ví dụ, do bản chất của phần mềm, nên các chức năng được mô tả trong đây có thể được thực hiện bằng cách sử dụng phần mềm thực thi bởi bộ xử lý, phần cứng, firmware, dây kết nối cứng, hoặc kết hợp bất kỳ của chúng. Các dấu hiệu thực hiện các chức năng cũng có thể được định vị vật lý ở các vị trí khác nhau, bao gồm được phân bổ sao cho các phần chức năng được thực hiện tại các vị trí vật lý khác nhau.

Phương tiện đọc được bằng máy tính bao gồm cả phương tiện lưu trữ máy tính bất biến và phương tiện truyền thông bao gồm phương tiện bất kỳ mà hỗ trợ việc chuyển chương trình máy tính từ nơi này đến nơi khác. Phương tiện lưu trữ bất biến có thể là phương tiện có sẵn bất kỳ mà có thể được truy cập bởi máy tính đa dụng hoặc chuyên dụng. Ví dụ, và không giới hạn ở ví dụ này, phương tiện bất biến đọc được bằng máy tính có thể bao gồm RAM, ROM, bộ nhớ chỉ đọc lập trình được xóa được bằng điện (electrically erasable programmable read-only memory - EEPROM), bộ nhớ flash, CD-ROM hoặc bộ nhớ đĩa quang khác, bộ nhớ đĩa từ khác hoặc các thiết bị lưu trữ từ khác, hoặc phương tiện bất biến khác bất kỳ mà có thể được sử dụng để mang hoặc lưu trữ phương tiện mang mã chương trình mong muốn dưới dạng các lệnh hoặc các cấu trúc dữ

liệu và mà có thể được truy cập bởi máy tính đa năng hoặc chuyên dụng, hoặc bộ xử lý đa năng hoặc chuyên dụng. Ngoài ra, mọi dạng kết nối được gọi theo cách thích hợp là phương tiện đọc được bằng máy tính. Ví dụ, nếu phần mềm được truyền từ trang web, máy chủ hoặc nguồn từ xa khác nhờ sử dụng cáp đồng trục, cáp sợi quang, cặp dây xoắn, đường dây thuê bao số (digital subscriber line - DSL), hoặc các công nghệ không dây như hồng ngoại, sóng vô tuyến, vi sóng, thì cáp đồng trục, cáp sợi quang, cặp dây xoắn, DSL, hoặc các công nghệ không dây như hồng ngoại, sóng vô tuyến, vi sóng này được bao hàm trong định nghĩa về phương tiện đọc được bằng máy tính. Đĩa từ và đĩa quang, như mô tả ở đây, bao gồm đĩa CD, đĩa laze, đĩa quang, đĩa số đa năng (digital versatile disc - DVD), đĩa mềm và đĩa blu-ray trong đó các đĩa từ thường tái tạo dữ liệu bằng từ tính, còn các đĩa quang tái tạo lại dữ liệu theo phương pháp quang học bằng tia laze. Dạng kết hợp của các loại nêu trên cũng được bao gồm trong phạm vi của phương tiện đọc được bằng máy tính.

Như được sử dụng ở đây, bao gồm trong các yêu cầu bảo hộ, "hoặc" như được sử dụng trong danh sách các mục (ví dụ, danh sách các mục bắt đầu bằng cụm từ như "ít nhất một trong số" hoặc "một hoặc nhiều trong số") chỉ danh sách bao quát sao cho, ví dụ, danh sách gồm ít nhất một trong số A, B, hoặc C có nghĩa là A hoặc B hoặc C hoặc AB hoặc AC hoặc BC hoặc ABC (tức là, A và B và C). Ngoài ra, như được sử dụng ở đây, cụm từ "dựa vào" không nên được hiểu là tham chiếu đến một tập hợp điều kiện đóng. Ví dụ, bước minh họa mà được mô tả là "dựa vào điều kiện A" có thể được dựa vào cả điều kiện A và điều kiện B mà không nằm ngoài phạm vi của sáng chế. Nói cách khác, như được sử dụng ở đây, cụm từ "dựa vào" phải được hiểu theo cách giống với cụm từ "dựa ít nhất một phần vào."

Trong các hình vẽ kèm theo, các bộ phận hoặc dấu hiệu tương tự có thể có cùng một nhãn tham chiếu. Hơn nữa, các thành phần khác nhau thuộc cùng một loại có thể được phân biệt bằng cách đặt sau nhãn chuẩn một nét gạch ngang và nhãn thứ hai để phân biệt giữa các thành phần tương tự. Nếu chỉ nhãn tham chiếu thứ nhất được sử dụng trong bản mô tả, thì sự mô tả đó có thể áp dụng được cho thành phần bất kỳ trong các thành phần tương tự có cùng nhãn tham chiếu thứ nhất bất kể có nhãn tham chiếu thứ hai hoặc nhãn tham chiếu tiếp sau khác.

Phần mô tả được nêu trong bản mô tả này, dựa vào các hình vẽ kèm theo, mô tả

các cấu hình ví dụ và không đại diện cho tất cả các ví dụ mà có thể được thực thi hoặc nằm trong phạm vi yêu cầu bảo hộ. Thuật ngữ "ví dụ" được sử dụng trong bản mô tả này nghĩa là "dùng làm ví dụ, trường hợp hoặc minh họa," và không phải là "được ưu tiên" hoặc "có lợi so với các ví dụ khác." Phần mô tả chi tiết bao gồm các chi tiết cụ thể nhằm mục đích giúp hiểu được các kỹ thuật được mô tả. Tuy nhiên, các kỹ thuật này có thể được thực hiện mà không cần các chi tiết cụ thể này. Trong một số trường hợp, các cấu trúc và thiết bị đã biết được thể hiện ở dạng sơ đồ khối để tránh làm khó hiểu các khái niệm của các ví dụ được mô tả.

Phần mô tả ở đây được đưa ra để cho phép người có hiểu biết trung bình trong lĩnh vực này thực hành hoặc sử dụng sáng chế. Các cải biến khác nhau đối với sáng chế sẽ là hiển nhiên với người có hiểu biết trung bình trong lĩnh vực, và các nguyên lý chung được xác định ở đây có thể được áp dụng cho các phương án biến đổi khác mà không nằm ngoài phạm vi của sáng chế. Do đó, sáng chế không bị hạn chế ở các ví dụ và phương án được mô tả ở đây mà phải được hiểu ở phạm vi rộng nhất theo các nguyên lý và dấu hiệu mới được bộc lộ ở đây.

## YÊU CẦU BẢO HỘ

1. Phương pháp truyền thông không dây bởi trạm gốc, phương pháp này bao gồm các bước:

truyền, từ trạm gốc đến nút mạng trước khi cung cấp khối thông tin hệ thống bao gồm thông tin hệ thống đến thiết bị người dùng (user equipment – UE), yêu cầu chữ ký bao gồm thông tin hệ thống, trong đó yêu cầu chữ ký chỉ báo khoảng tăng khung con và yêu cầu nhiều chữ ký tương ứng với phạm vi số khung con giữa số khung con bắt đầu và số khung con kết thúc;

nhận, bởi trạm gốc từ nút mạng và để đáp lại yêu cầu chữ ký, nhiều đáp ứng chữ ký mà mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều trong số nhiều chữ ký, trong đó mỗi trong số các tập con tương ứng với khoảng tăng khung con riêng trong phạm vi số khung con, trong đó đáp ứng chữ ký thứ nhất trong số nhiều đáp ứng chữ ký bao gồm chữ ký thứ nhất trong số nhiều chữ ký mà được tạo ra bởi nút mạng dựa vào khóa riêng tư thứ nhất được duy trì tại nút mạng, chữ ký thứ nhất để xác thực thông tin hệ thống, trong đó khóa riêng tư thứ nhất là không được biết với trạm gốc và đáp ứng chữ ký thứ nhất còn bao gồm mã định danh của khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất;

truyền, từ trạm gốc tới UE và để đáp lại việc nhận nhiều đáp ứng chữ ký bao gồm đáp ứng chữ ký thứ nhất, bản tin thông tin hệ thống bao gồm khối thông tin hệ thống bao gồm thông tin hệ thống, chữ ký thứ nhất và mã định danh của khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất; và

truyền thông với UE qua kết nối được thiết lập bằng cách sử dụng thông tin hệ thống được bao gồm trong khối thông tin hệ thống.

2. Phương pháp theo điểm 1, trong đó bước truyền yêu cầu chữ ký bao gồm:

truyền yêu cầu chữ ký bao gồm thông tin hệ thống và thông tin chính, trong đó chữ ký thứ nhất được tạo ra dựa ít nhất một phần vào thông tin hệ thống và thông tin chính.

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

truyền, đến nút mạng, yêu cầu chữ ký thứ hai bao gồm thông tin hệ thống cập nhật;

nhận, từ nút mạng, đáp ứng chữ ký thứ hai bao gồm chữ ký thứ hai được tạo ra dựa ít nhất một phần vào thông tin hệ thống cập nhật; và

truyền bản tin thông tin hệ thống thứ hai bao gồm thông tin hệ thống cập nhật và chữ ký thứ hai.

4. Phương pháp theo điểm 1, phương pháp này còn bao gồm các bước:

nhận yêu cầu đăng ký từ UE;

truyền yêu cầu đăng ký đến nút mạng cung cấp chức năng quản lý truy cập và di động (access and mobility management function - AMF);

nhận, từ nút mạng, đáp ứng đăng ký bao gồm khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất; và

truyền đáp ứng đăng ký đến UE.

5. Phương pháp theo điểm 4, trong đó bước truyền đáp ứng đăng ký bao gồm:

truyền đáp ứng đăng ký bao gồm vùng theo dõi thứ nhất cho khóa công khai.

6. Phương pháp theo điểm 5, trong đó bước truyền đáp ứng đăng ký bao gồm:

truyền đáp ứng đăng ký chỉ báo khóa công khai thứ hai cho vùng theo dõi thứ hai được định vị địa lý so với vùng theo dõi thứ nhất, khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho thông tin hệ thống thứ hai được truyền trong vùng theo dõi thứ hai.

7. Phương pháp theo điểm 4, trong đó bước nhận yêu cầu đăng ký bao gồm:

nhận yêu cầu cập nhật đăng ký di động từ UE chỉ báo rằng UE đã vào vùng theo dõi mới.

8. Phương pháp theo điểm 1, phương pháp này còn bao gồm bước:

truyền yêu cầu chữ ký thứ hai để yêu cầu nhiều chữ ký thứ hai cho phạm vi thời gian và khoảng tăng thời gian.

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

nhận đáp ứng chữ ký thứ hai bao gồm nhiều chữ ký thứ hai.

10. Phương pháp theo điểm 8, phương pháp này còn bao gồm:

nhận nhiều đáp ứng chữ ký thứ hai mà mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều trong số nhiều chữ ký thứ hai.

11. Phương pháp theo điểm 10, trong đó mỗi trong số các tập con của một hoặc nhiều trong số nhiều chữ ký thứ hai tương ứng với khoảng tăng thời gian riêng trong phạm vi thời gian.

12. Phương pháp theo điểm 1, trong đó bước truyền yêu cầu chữ ký bao gồm:

truyền yêu cầu chữ ký bao gồm thông số truy cập gần đây.

13. Phương pháp theo điểm 12, phương pháp này còn bao gồm bước:

nhận, từ nút mạng, đáp ứng chữ ký thứ nhất bao gồm chữ ký thứ nhất được tạo ra dựa ít nhất một phần vào thông tin hệ thống và thông số truy cập gần đây.

14. Phương pháp theo điểm 12, trong đó thông số truy cập gần đây là số khung hệ thống.

15. Phương pháp truyền thông không dây bởi nút mạng, phương pháp này bao gồm các bước:

nhận, bởi nút mạng từ trạm gốc, trước khi khối thông tin hệ thống bao gồm thông tin hệ thống được cung cấp đến thiết bị người dùng (UE), yêu cầu chữ ký bao gồm thông tin hệ thống, trong đó yêu cầu chữ ký chỉ báo khoảng tăng khung con và yêu cầu nhiều chữ ký tương ứng với phạm vi số khung con giữa số khung con bắt đầu và số khung con kết thúc; và

truyền, từ nút mạng đến trạm gốc và để đáp lại yêu cầu chữ ký, nhiều đáp ứng chữ ký mà mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều trong số nhiều chữ ký, trong đó mỗi trong số các tập con tương ứng với khoảng tăng khung con riêng trong phạm vi số khung con, trong đó đáp ứng chữ ký thứ nhất trong số nhiều đáp ứng chữ ký bao gồm chữ ký thứ nhất trong số nhiều chữ ký mà được tạo ra bởi nút mạng dựa vào khóa riêng tư thứ nhất được duy trì tại nút mạng, chữ ký thứ nhất để xác thực thông tin hệ thống được bao gồm trong khối thông tin hệ thống, trong đó khóa riêng tư thứ nhất là

không được biết với trạm gốc và đáp ứng chữ ký thứ nhất còn bao gồm mã định danh của khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất.

16. Phương pháp theo điểm 15, trong đó bước nhận yêu cầu chữ ký bao gồm:

nhận yêu cầu chữ ký bao gồm thông tin hệ thống và thông tin chính, trong đó chữ ký thứ nhất được tạo ra dựa ít nhất một phần vào thông tin hệ thống và thông tin chính.

17. Phương pháp theo điểm 15, phương pháp này còn bao gồm bước:

nhận, từ trạm gốc, yêu cầu chữ ký thứ hai bao gồm thông tin hệ thống cập nhật; và

truyền, đến trạm gốc, đáp ứng chữ ký thứ hai bao gồm chữ ký thứ hai được tạo ra dựa ít nhất một phần vào thông tin hệ thống cập nhật.

18. Phương pháp theo điểm 15, trong đó bước nhận yêu cầu chữ ký bao gồm:

nhận yêu cầu chữ ký yêu cầu nhiều chữ ký thứ hai cho phạm vi thời gian và khoảng tăng thời gian.

19. Phương pháp theo điểm 18, phương pháp này còn bao gồm:

truyền đáp ứng chữ ký thứ hai bao gồm nhiều chữ ký thứ hai.

20. Phương pháp theo điểm 18, phương pháp này còn bao gồm:

truyền nhiều đáp ứng chữ ký thứ hai mà mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều trong số nhiều chữ ký thứ hai.

21. Phương pháp theo điểm 20, trong đó mỗi trong số các tập con của một hoặc nhiều trong số nhiều chữ ký thứ hai tương ứng với khoảng tăng thời gian riêng trong phạm vi thời gian.

22. Phương pháp theo điểm 15, trong đó nút mạng là nút mạng lõi, nút mạng truy cập vô tuyến (radio access network - RAN), nút chức năng ứng dụng, hoặc nút chức năng ký.

23. Máy để truyền thông không dây bởi trạm gốc, máy này bao gồm:

phương tiện để truyền, từ trạm gốc đến nút mạng trước khi cung cấp khối thông

tin hệ thống bao gồm thông tin hệ thống tới thiết bị người dùng (UE), yêu cầu chữ ký bao gồm thông tin hệ thống, trong đó yêu cầu chữ ký chỉ báo khoảng tăng khung con và yêu cầu nhiều chữ ký tương ứng với phạm vi số khung con giữa số khung con bắt đầu và số khung con kết thúc;

phương tiện để nhận, bởi trạm gốc từ nút mạng và để đáp lại yêu cầu chữ ký, nhiều đáp ứng chữ ký mà mỗi đáp ứng chữ ký bao gồm tập con của một hoặc nhiều trong số nhiều chữ ký, trong đó mỗi trong số các tập con tương ứng với khoảng tăng khung con riêng trong phạm vi số khung con, trong đó đáp ứng chữ ký thứ nhất trong số nhiều đáp ứng chữ ký bao gồm chữ ký thứ nhất trong số nhiều chữ ký mà được tạo ra bởi nút mạng dựa vào khóa riêng tư thứ nhất được duy trì tại nút mạng, chữ ký thứ nhất để xác thực thông tin hệ thống, trong đó khóa riêng tư thứ nhất là không được biết tới trạm gốc và đáp ứng chữ ký thứ nhất còn bao gồm mã định danh của khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất;

phương tiện để truyền, từ trạm gốc đến UE và để đáp lại việc nhận nhiều đáp ứng chữ ký bao gồm đáp ứng chữ ký thứ nhất, bản tin thông tin hệ thống bao gồm khối thông tin hệ thống bao gồm thông tin hệ thống, chữ ký thứ nhất và mã định danh của khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất; và

phương tiện để truyền thông với UE qua kết nối được thiết lập bằng cách sử dụng thông tin hệ thống được bao gồm trong khối thông tin hệ thống.

24. Máy để truyền thông không dây bởi trạm gốc, máy này bao gồm:

bộ xử lý;

bộ nhớ được ghép nối với bộ xử lý; và

các lệnh được lưu trữ trong bộ nhớ và thực thi được bởi bộ xử lý để khiến cho máy thực hiện các phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 14.

25. Máy để truyền thông không dây bởi nút mạng, máy này bao gồm:

bộ xử lý;

bộ nhớ được ghép nối với bộ xử lý; và

các lệnh được lưu trữ trong bộ nhớ và thực thi được bởi bộ xử lý để khiến cho máy thực hiện các phương pháp theo điểm bất kỳ trong số các điểm từ 15 đến 22.

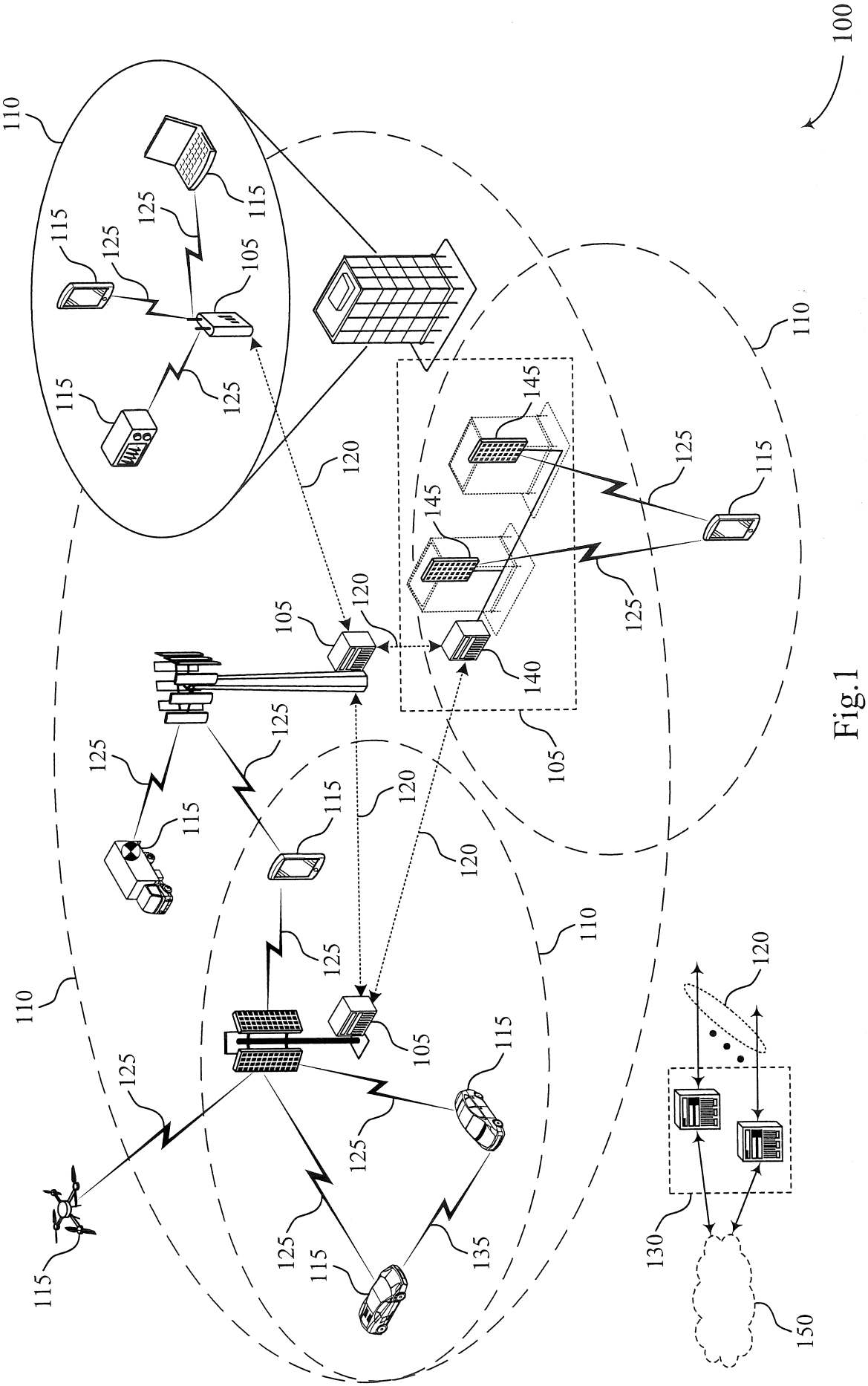


Fig.1

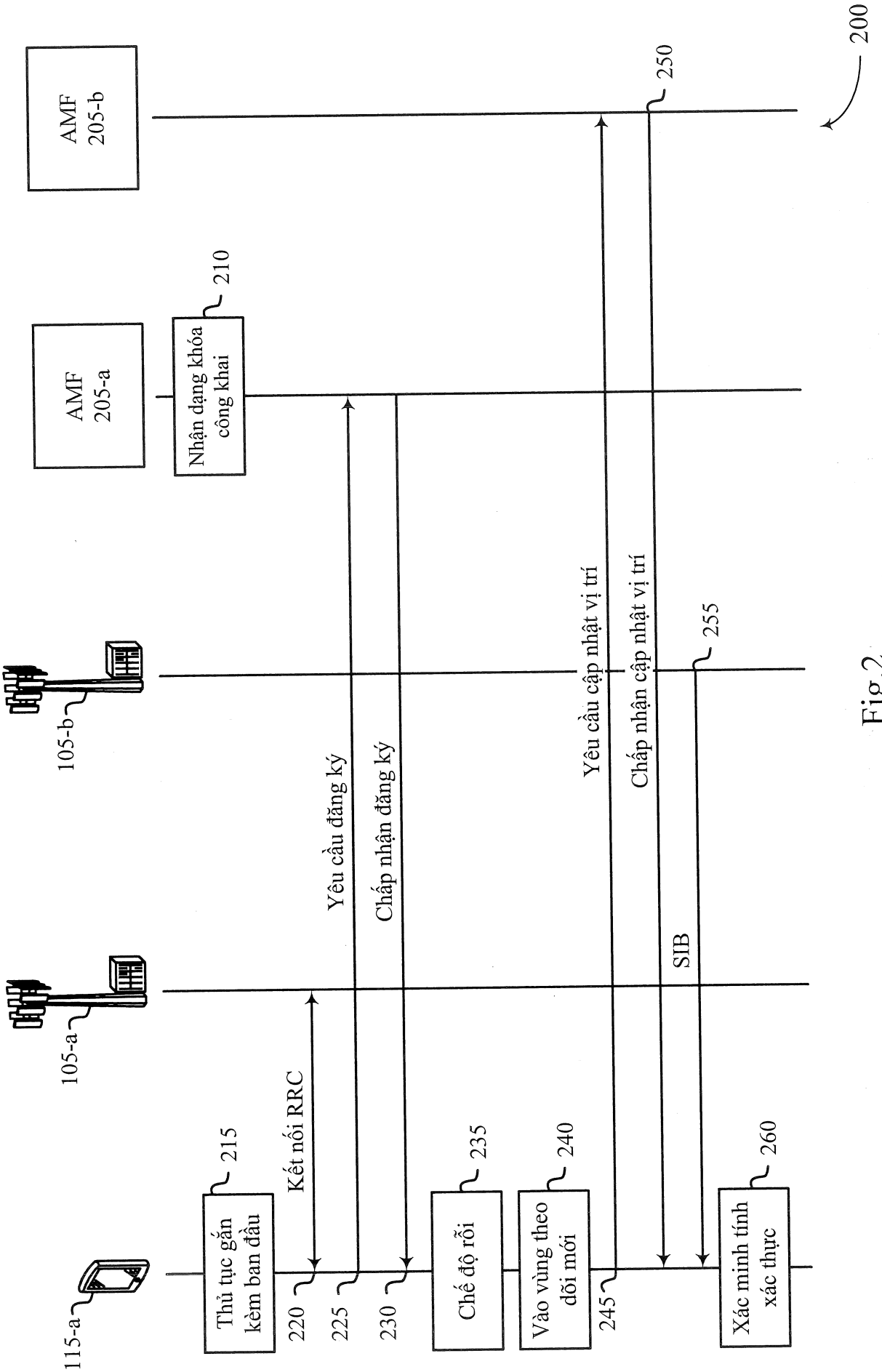
200
AMF 205-b
AMF 205-a
Nhận dạng khóa công khai
210
250
105-b
105-a
115-a
Thủ tục gắn kèm ban đầu
215
Kết nối RRC
220
Yêu cầu đăng ký
225
Chấp nhận đăng ký
230
Chế độ rỗi
235
Vào vùng theo dõi mới
240
Yêu cầu cập nhật vị trí
245
Chấp nhận cập nhật vị trí
255
SIB
Xác minh tính xác thực
260

Fig.2

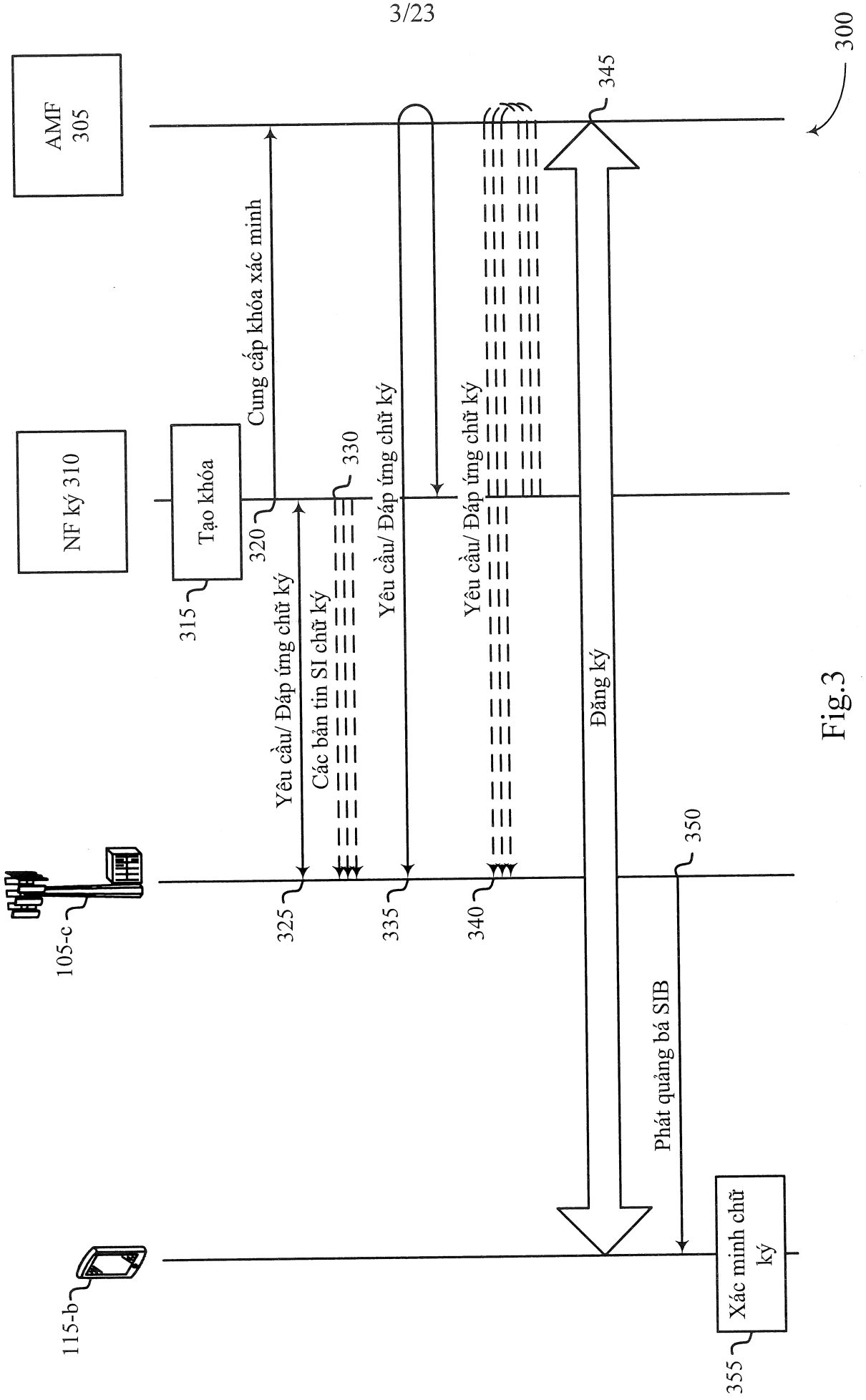
300
AMF 305
NF ký 310
105-c
115-b
Tạo khóa
315
320
330
345
350
355
325
335
340
Cung cấp khóa xác minh
Yêu cầu/ Đáp ứng chữ ký
Các bản tin SI chữ ký
Yêu cầu/ Đáp ứng chữ ký
Yêu cầu/ Đáp ứng chữ ký
Đăng ký
Phát quảng bá SIB
Xác minh chữ ký

Fig.3

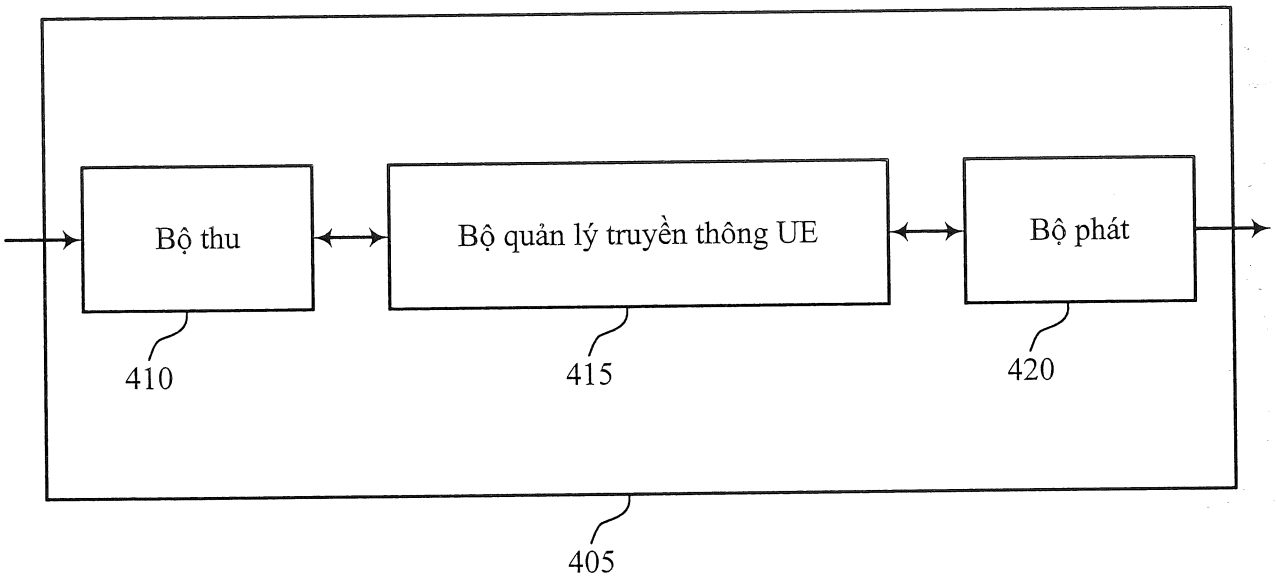


Fig.4

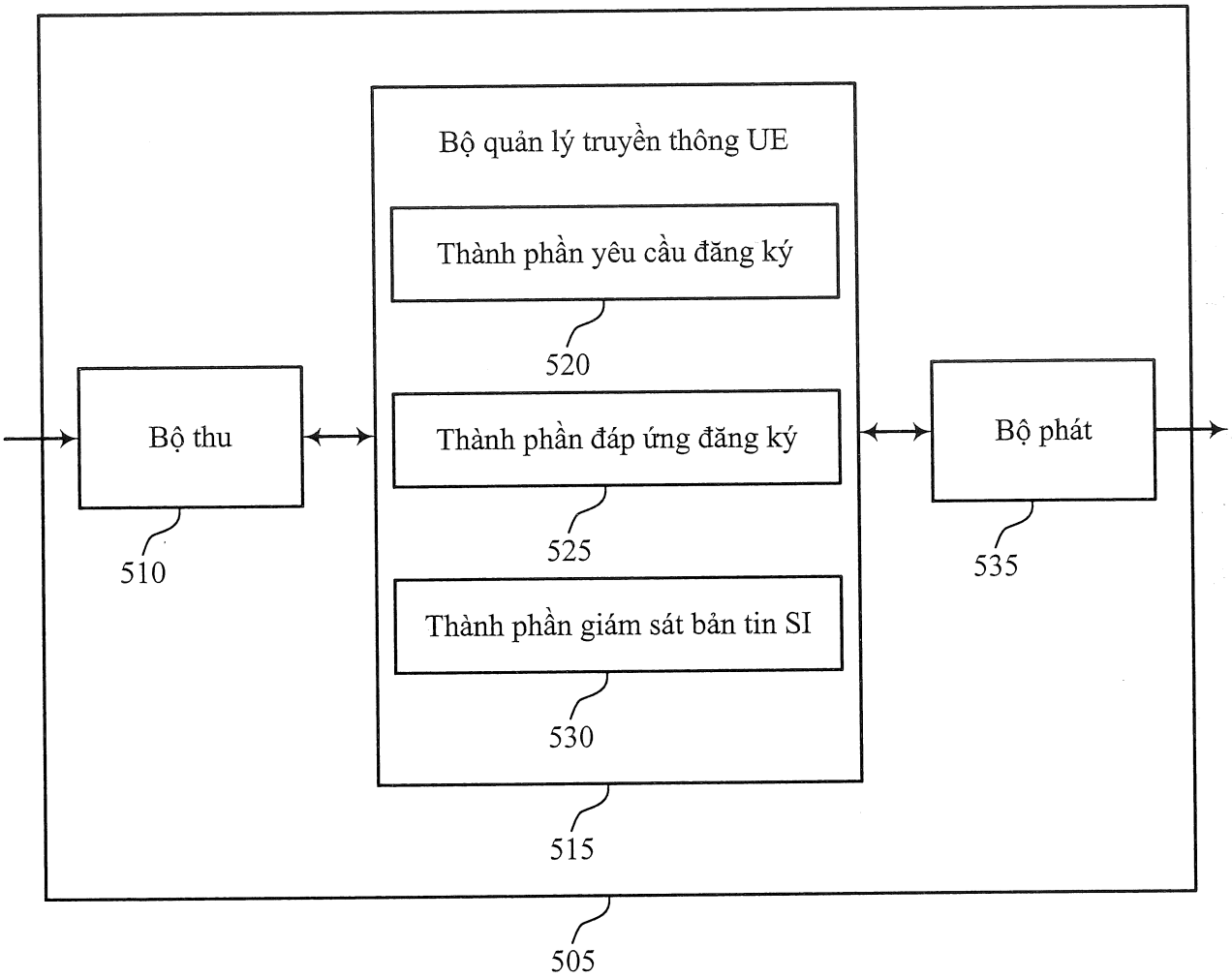
Bộ quản lý truyền thông UE
Thành phần yêu cầu đăng ký
520
Bộ thu
Thành phần đáp ứng đăng ký
Bộ phát
525
510
535
Thành phần giám sát bản tin SI
530
515
505
500

Fig.5

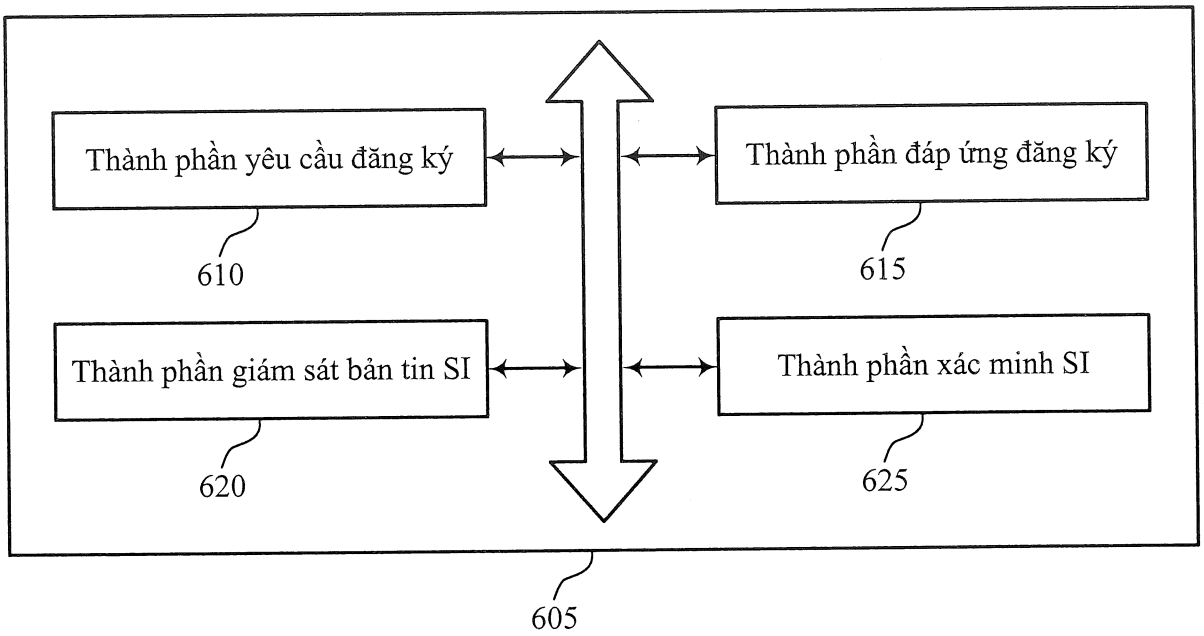
Thành phần yêu cầu đăng ký
610
Thành phần đáp ứng đăng ký
615
Thành phần giám sát bản tin SI
620
Thành phần xác minh SI
625
605
600

Fig.6

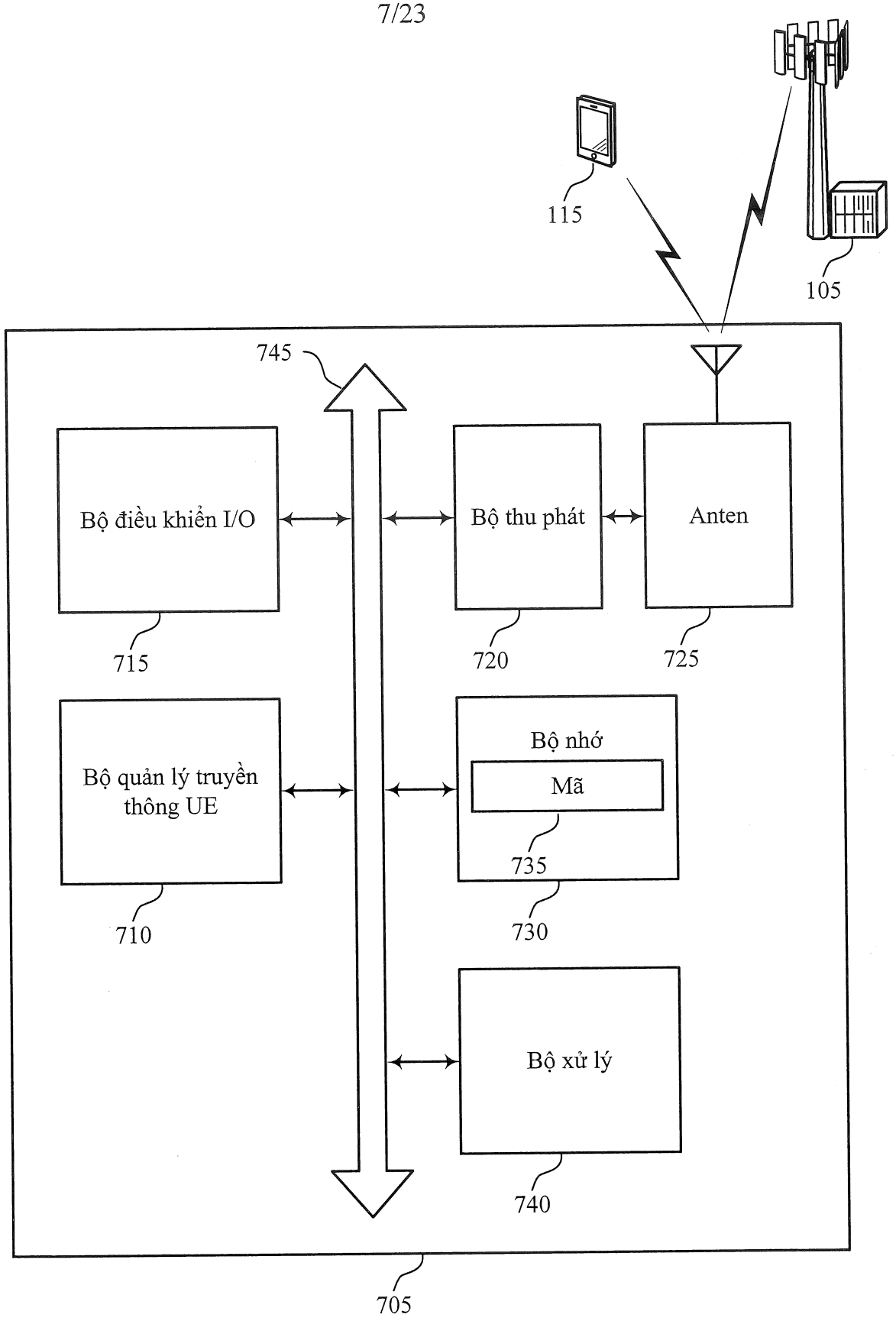
115
105
745
Bộ điều khiển I/O
Bộ thu phát
Anten
715
720
725
Bộ quản lý truyền thông UE
Bộ nhớ
Mã
735
710
730
Bộ xử lý
740
705
700

Fig.7

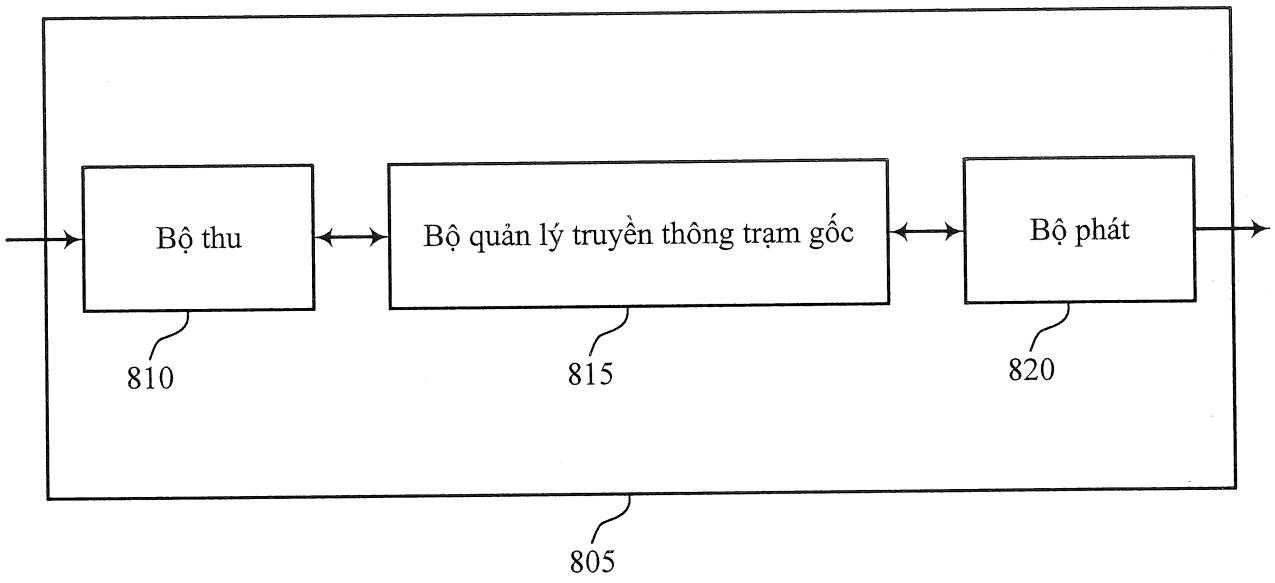
Bộ thu
Bộ quản lý truyền thông trạm gốc
Bộ phát
810
815
820
805
800

Fig.8

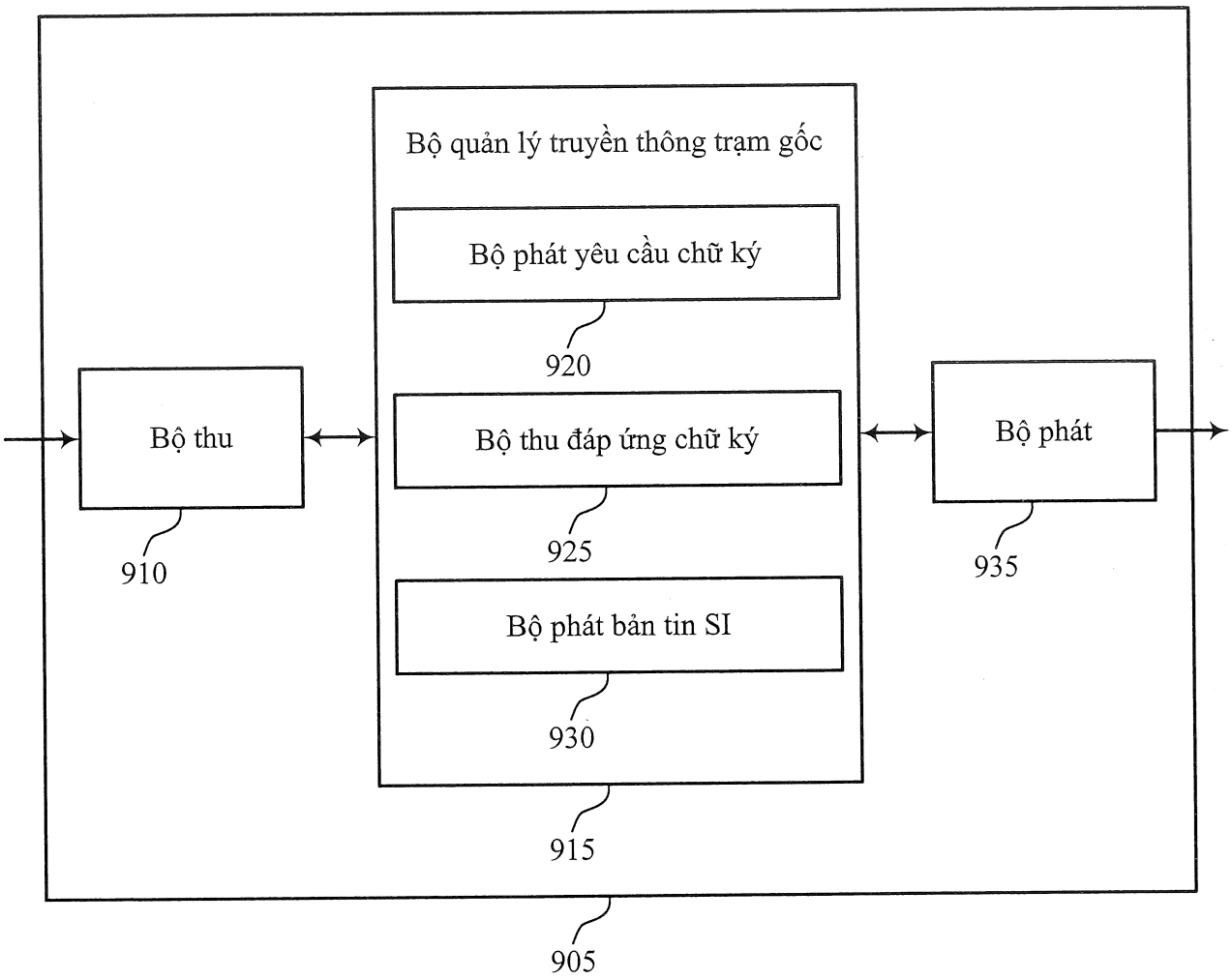
Bộ quản lý truyền thông trạm gốc
Bộ phát yêu cầu chữ ký
920
Bộ thu
Bộ thu đáp ứng chữ ký
Bộ phát
910
925
935
Bộ phát bản tin SI
930
915
905
900

Fig.9

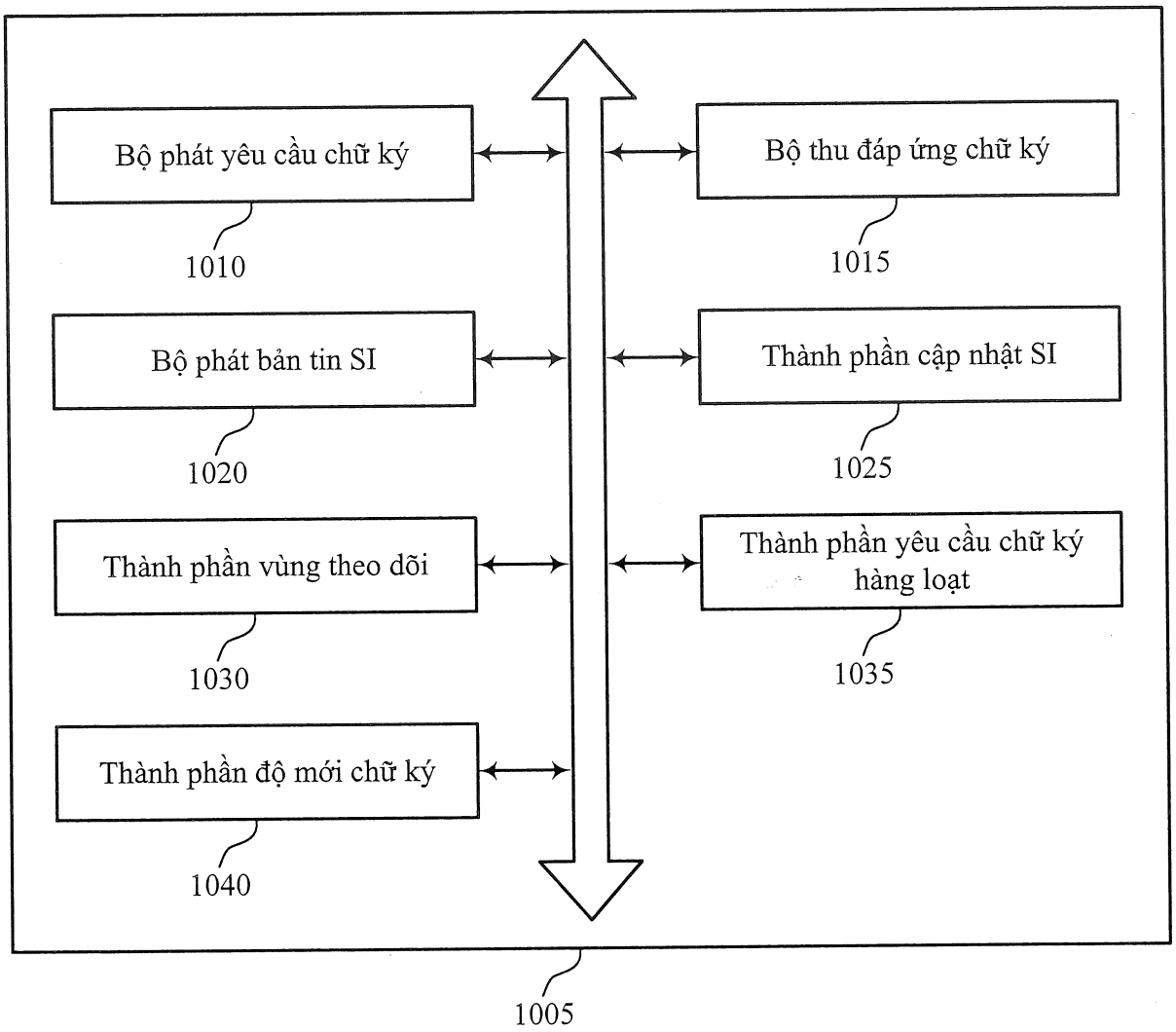
Bộ phát yêu cầu chữ ký
1010
Bộ thu đáp ứng chữ ký
1015
Bộ phát bản tin SI
1020
Thành phần cập nhật SI
1025
Thành phần vùng theo dõi
1030
Thành phần yêu cầu chữ ký hàng loạt
1035
Thành phần độ mới chữ ký
1040
1005
1000

Fig.10

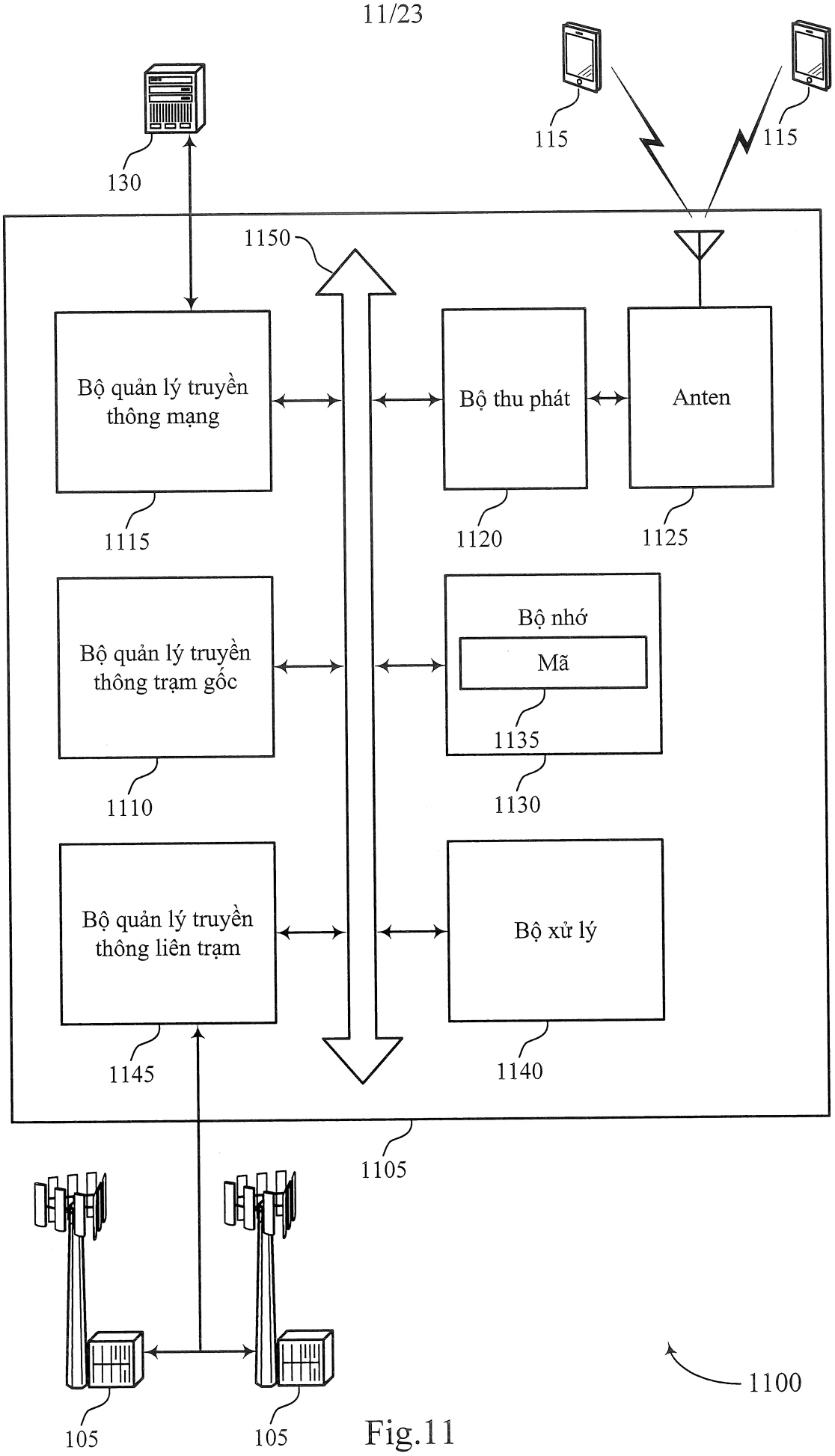
130
115
115
1150
Bộ quản lý truyền thông mạng
Bộ thu phát
Anten
1115
1120
1125
Bộ quản lý truyền thông trạm gốc
Bộ nhớ
Mã
1135
1110
1130
Bộ quản lý truyền thông liên trạm
Bộ xử lý
1145
1140
1105
105
105
1100

Fig.11

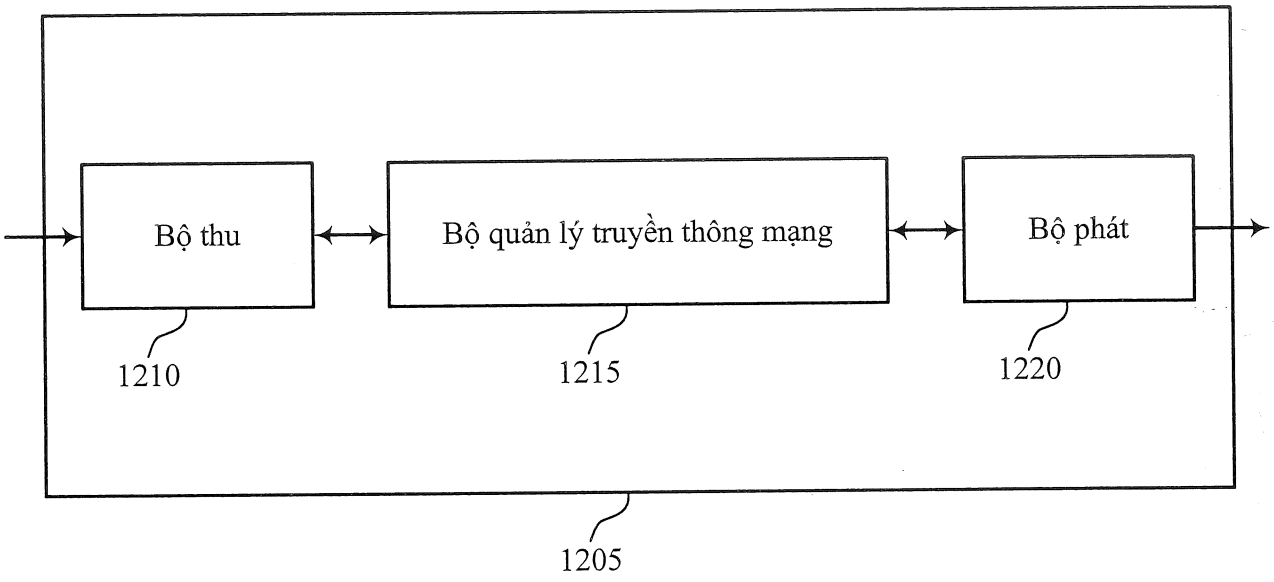
Bộ thu
Bộ quản lý truyền thông mạng
Bộ phát
1210
1215
1220
1205
1200

Fig.12

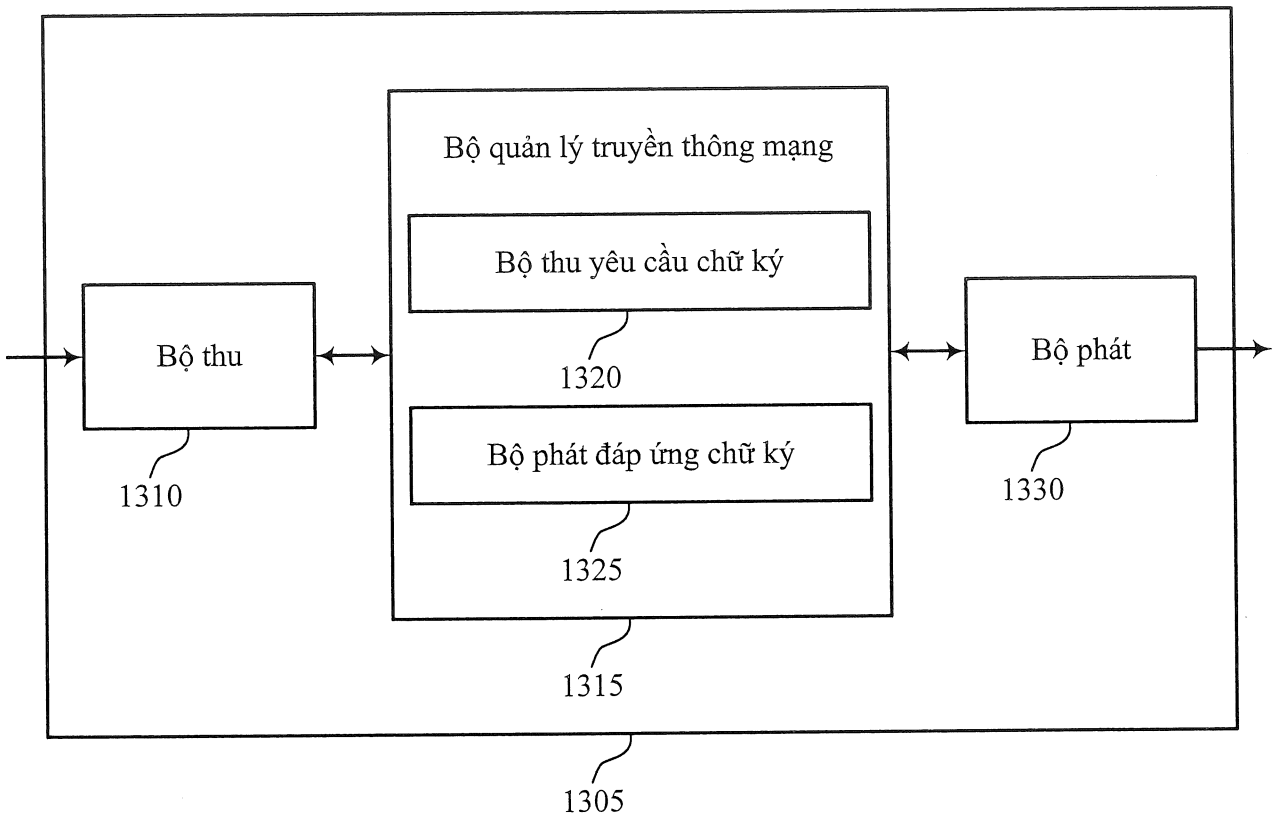
Bộ quản lý truyền thông mạng
Bộ thu yêu cầu chữ ký
Bộ thu
Bộ phát
Bộ phát đáp ứng chữ ký
1320
1310
1330
1325
1315
1305
1300

Fig.13

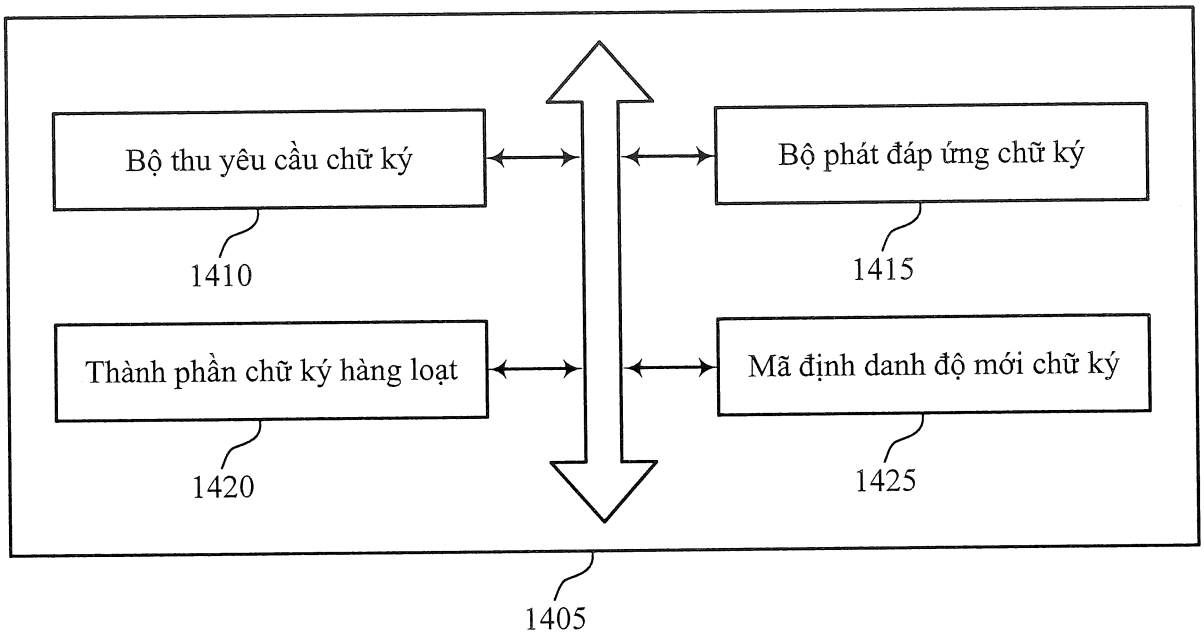
Bộ thu yêu cầu chữ ký
1410
Bộ phát đáp ứng chữ ký
1415
Thành phần chữ ký hàng loạt
1420
Mã định danh độ mới chữ ký
1425
1405
1400

Fig.14

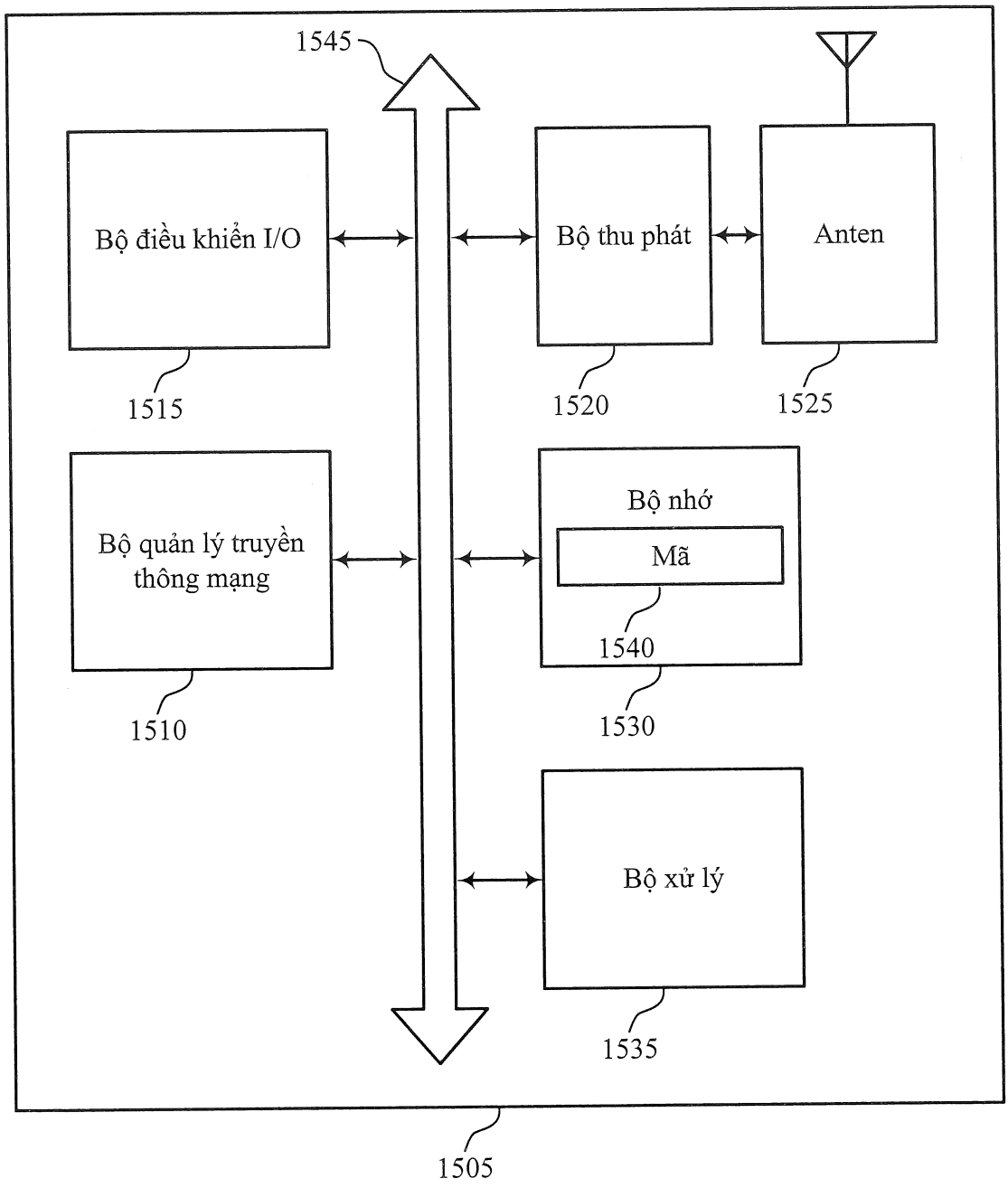
1545
Bộ điều khiển I/O
Bộ thu phát
Anten
1515
1520
1525
Bộ quản lý truyền thông mạng
Bộ nhớ
Mã
1540
1510
1530
Bộ xử lý
1535
1505
1500

Fig.15

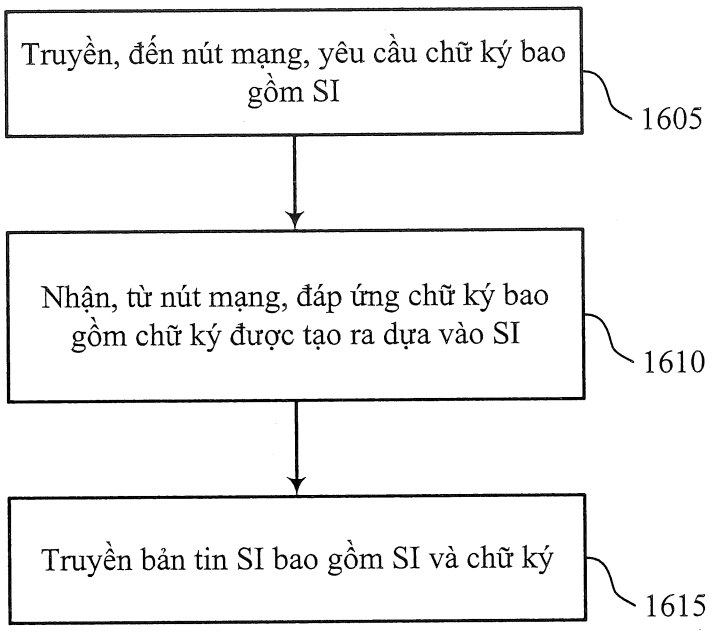
Truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI
1605
Nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI
1610
Truyền bản tin SI bao gồm SI và chữ ký
1615
1600

Fig.16

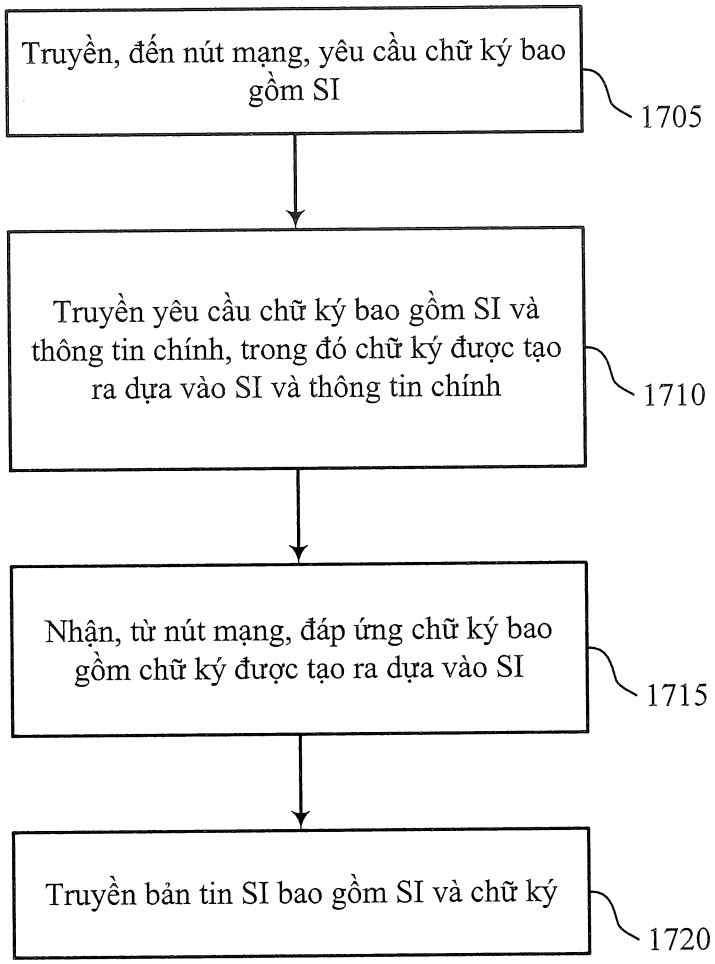
Truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI
1705
Truyền yêu cầu chữ ký bao gồm SI và thông tin chính, trong đó chữ ký được tạo ra dựa vào SI và thông tin chính
1710
Nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI
1715
Truyền bản tin SI bao gồm SI và chữ ký
1720
1700

Fig.17

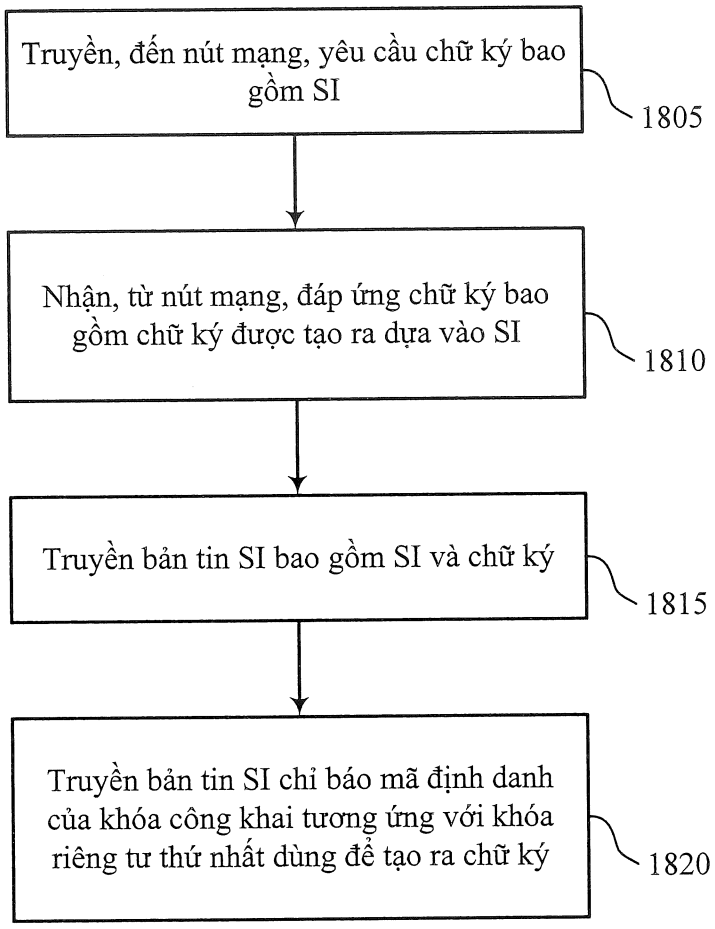
Truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI
1805
Nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI
1810
Truyền bản tin SI bao gồm SI và chữ ký
1815
Truyền bản tin SI chỉ báo mã định danh của khóa công khai tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký
1820
1800

Fig.18

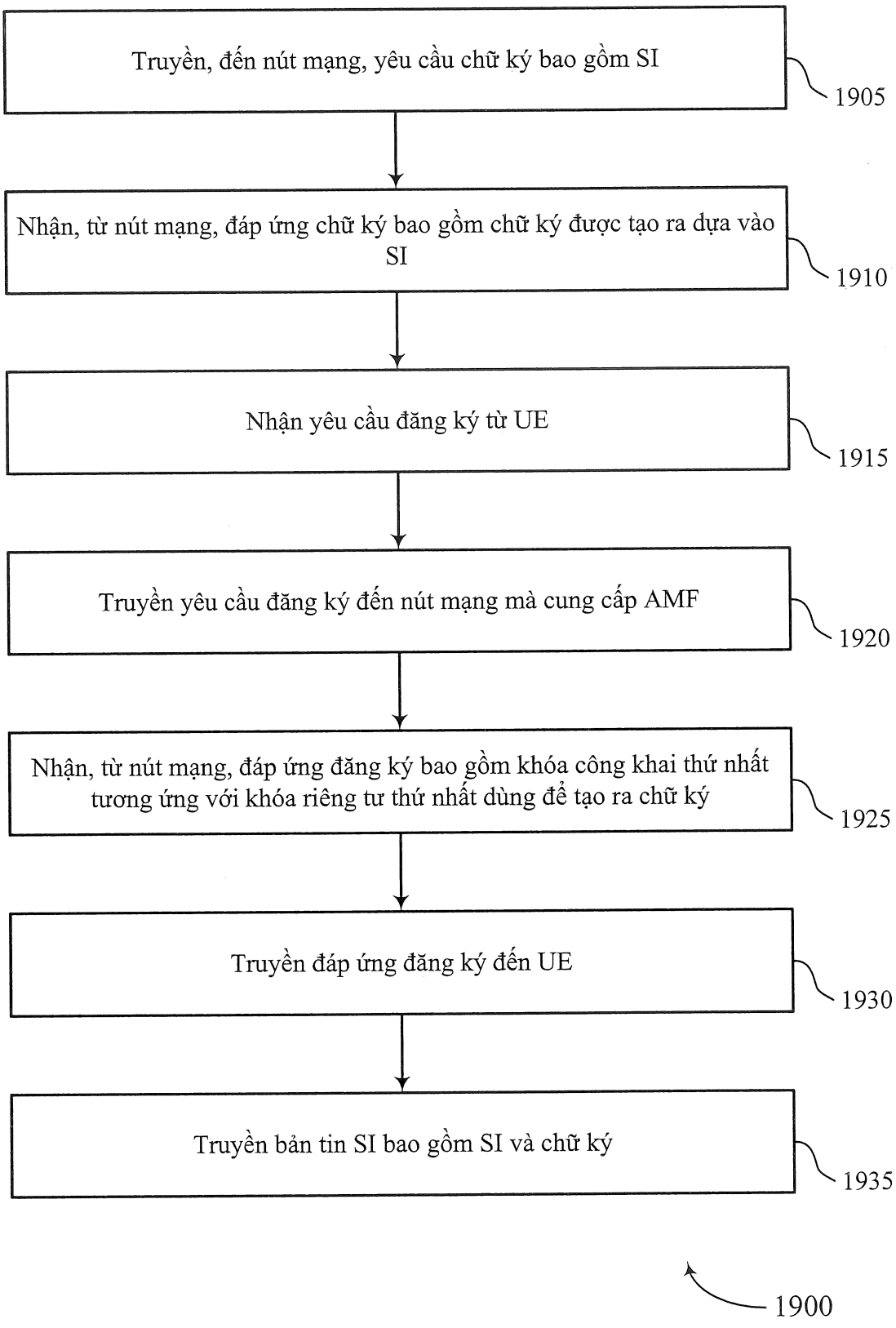
Truyền, đến nút mạng, yêu cầu chữ ký bao gồm SI
1905
Nhận, từ nút mạng, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI
1910
Nhận yêu cầu đăng ký từ UE
1915
Truyền yêu cầu đăng ký đến nút mạng mà cung cấp AMF
1920
Nhận, từ nút mạng, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký
1925
Truyền đáp ứng đăng ký đến UE
1930
Truyền bản tin SI bao gồm SI và chữ ký
1935
1900

Fig.19

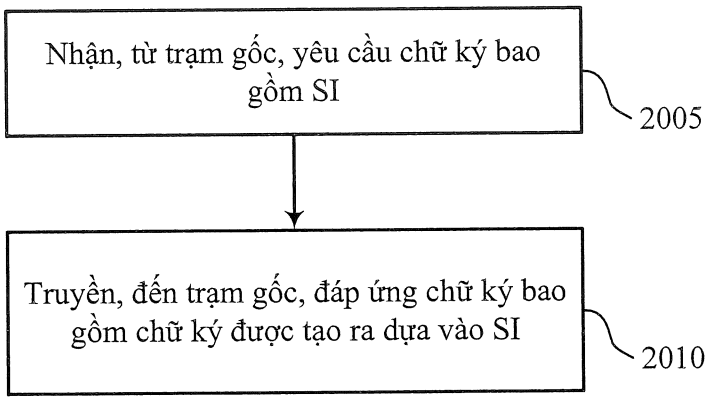
Nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI
2005
Truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI
2010
2000

Fig.20

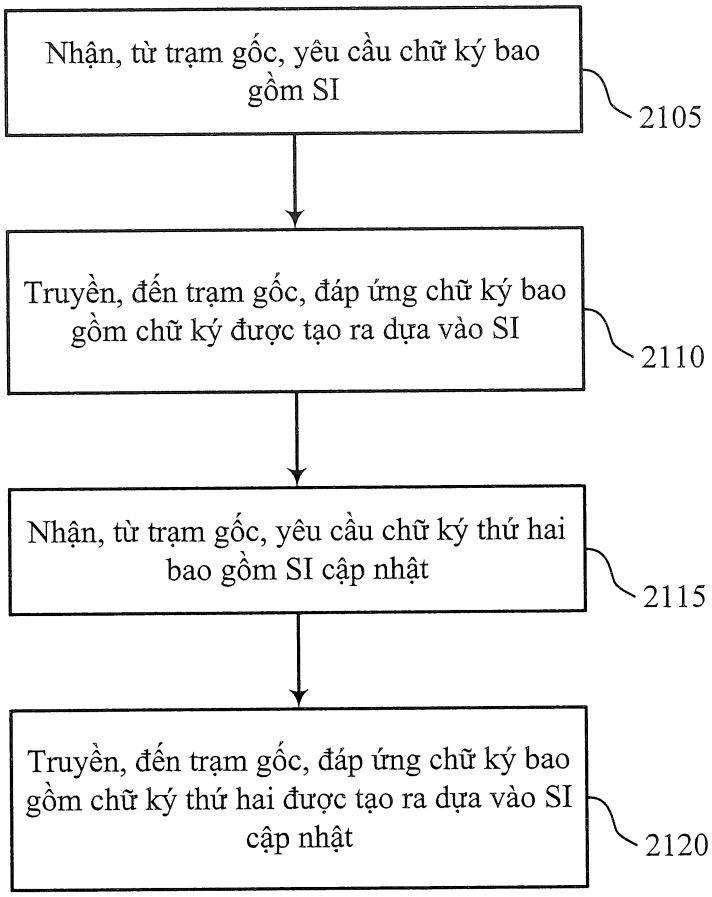
Nhận, từ trạm gốc, yêu cầu chữ ký bao gồm SI
2105
Truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký được tạo ra dựa vào SI
2110
Nhận, từ trạm gốc, yêu cầu chữ ký thứ hai bao gồm SI cập nhật
2115
Truyền, đến trạm gốc, đáp ứng chữ ký bao gồm chữ ký thứ hai được tạo ra dựa vào SI cập nhật
2120
2100

Fig.21

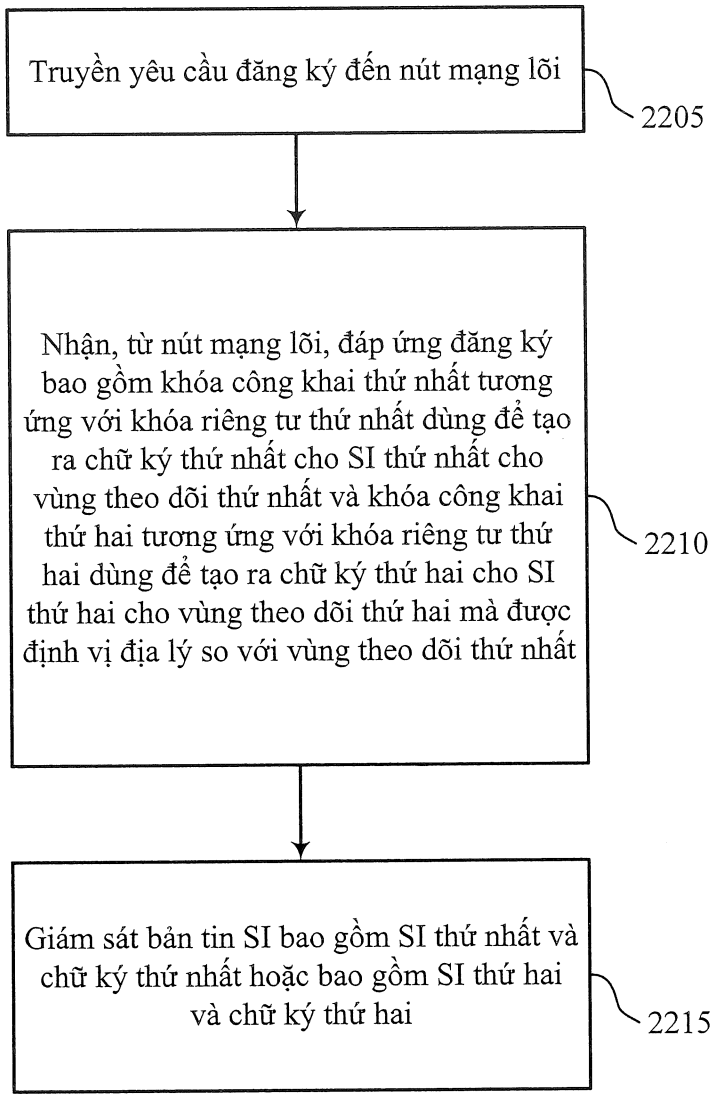
Truyền yêu cầu đăng ký đến nút mạng lõi
2205
Nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất
2210
Giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai
2215
2200

Fig.22

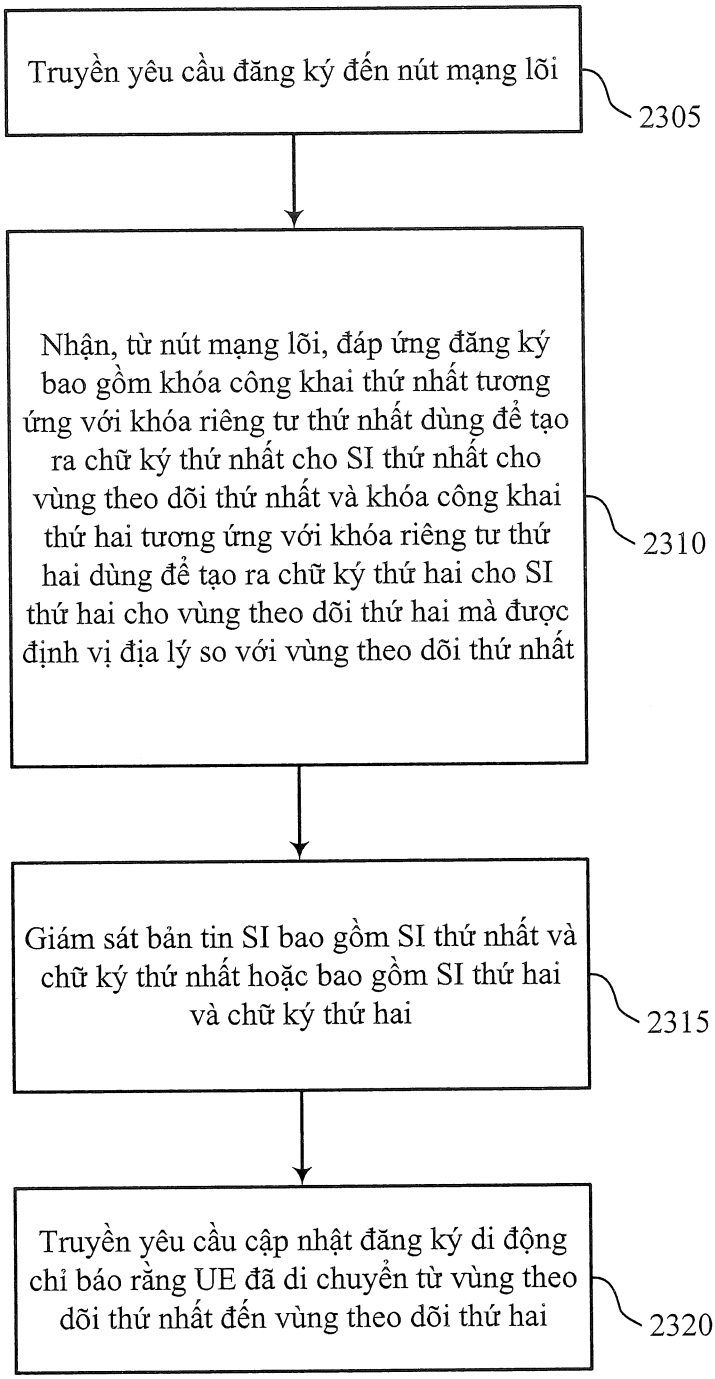
Truyền yêu cầu đăng ký đến nút mạng lõi
2305
Nhận, từ nút mạng lõi, đáp ứng đăng ký bao gồm khóa công khai thứ nhất tương ứng với khóa riêng tư thứ nhất dùng để tạo ra chữ ký thứ nhất cho SI thứ nhất cho vùng theo dõi thứ nhất và khóa công khai thứ hai tương ứng với khóa riêng tư thứ hai dùng để tạo ra chữ ký thứ hai cho SI thứ hai cho vùng theo dõi thứ hai mà được định vị địa lý so với vùng theo dõi thứ nhất
2310
Giám sát bản tin SI bao gồm SI thứ nhất và chữ ký thứ nhất hoặc bao gồm SI thứ hai và chữ ký thứ hai
2315
Truyền yêu cầu cập nhật đăng ký di động chỉ báo rằng UE đã di chuyển từ vùng theo dõi thứ nhất đến vùng theo dõi thứ hai
2320
2300

Fig.23