(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) **1-0043641**

(51)[2020.01] **H04L 29/06**

(13) **B**

(21) 1-2020-01879
(22) 29/03/2018
(86) PCT/CN2018/081154 29/03/2018
(87) WO 2019/041802 07/03/2019
(30) 201710775263.3 31/08/2017 CN
(45) 25/02/2025 443
(43) 27/07/2020 388A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, China
(72) ZHANG, Bo (CN); GAN, Lu (CN); WU, Rong (CN); TAN, Shuaishuai (CN).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) HỆ THỐNG XÁC THỰC DỰA VÀO KIẾN TRÚC DỰA TRÊN DỊCH VỤ, PHƯƠNG PHÁP PHÁT HIỆN DỰA VÀO KIẾN TRÚC DỰA TRÊN DỊCH VỤ, PHẦN TỬ MẠNG ĐIỀU KHIỂN THỨ HAI, VÀ VẬT GHI ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(21) 1-2020-01879

(57) Sáng chế đề cập đến hệ thống xác thực và phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ. Trong phương pháp này, phần tử mạng điều khiển gửi phản hồi phát hiện đến phần tử mạng chức năng thứ nhất, trong đó phản hồi phát hiện này bao gồm thông số bảo mật được xác định và một địa chỉ truy cập hoặc mã định danh của phần tử mạng chức năng thứ hai. Phần tử mạng chức năng thứ nhất nhận phản hồi phát hiện được gửi bởi phần tử mạng điều khiển, và gửi yêu cầu truy cập đến phần tử mạng chức năng thứ hai dựa vào địa chỉ hoặc mã định danh của phần tử mạng chức năng thứ hai có trong phản hồi phát hiện này, trong đó yêu cầu truy cập này bao gồm thông số bảo mật nhận được. Phần tử mạng chức năng thứ hai nhận yêu cầu truy cập được gửi bởi phần tử mạng chức năng thứ nhất, xác minh tính chính xác của thông số bảo mật này, và xác định, dựa vào tính chính xác của thông số bảo mật, xem yêu cầu truy cập có được cấp quyền bởi phần tử mạng chức năng thứ nhất hay không. Nhờ sử dụng sáng chế, số lần truyền thông có thể được giảm bớt ở mức độ nhất định, và độ phức tạp truyền thông có thể giảm đi. Ngoài ra, sáng chế còn đề cập đến hệ thống và phương pháp xác thực dựa vào kiến trúc dựa trên dịch vụ, và phần tử mạng điều khiển. Ngoài ra, sáng chế còn đề cập đến phần tử mạng điều khiển thứ hai và vật ghi đọc được bằng máy tính.

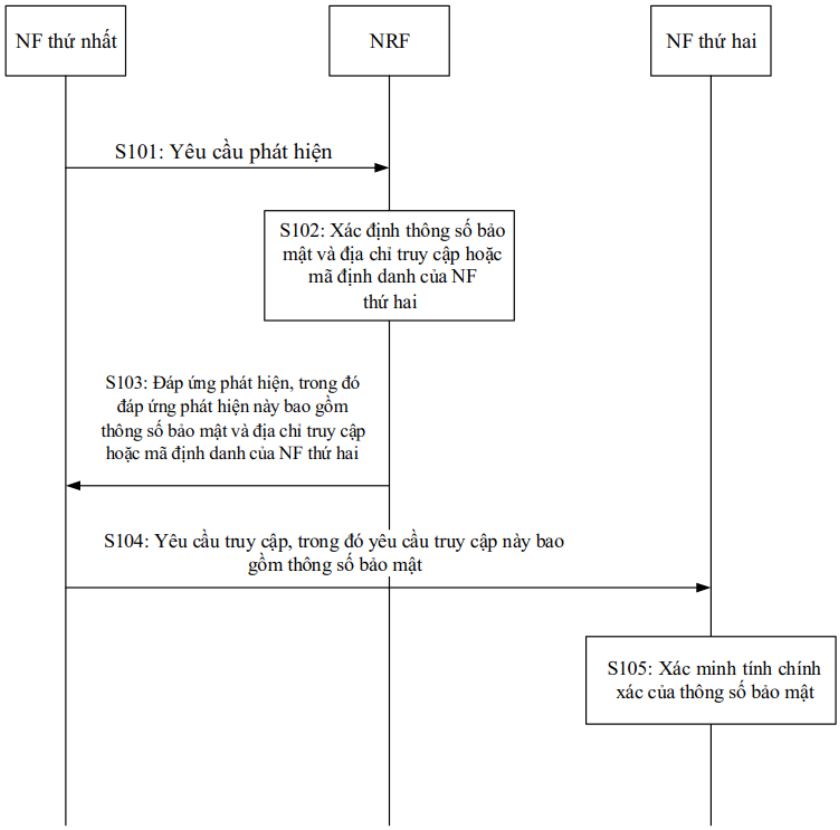

FIG.2

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ truyền thông, cụ thể là đến hệ thống xác thực dựa vào kiến trúc dựa trên dịch vụ, phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ, phần tử mạng điều khiển thứ hai, và vật ghi đọc được bằng máy tính.

Tình trạng kỹ thuật của sáng chế

Khi bàn đến kiến trúc mạng lõi của mạng 5G, giải pháp kiến trúc dựa trên dịch vụ với chức năng mạng (network function, NF) đóng vai trò trung tâm được đề xuất. Trong giải pháp kiến trúc dựa trên dịch vụ, việc chia tách và tích hợp giữa các NF được thực hiện bằng cách môđun hóa. Các NF đã chia tách được định quy mô riêng rẽ, được phát triển riêng rẽ, và được triển khai theo yêu cầu. Ngoài ra, tất cả các NF trên mặt phẳng điều khiển sử dụng các giao diện dựa trên dịch vụ để tương tác. Cùng dịch vụ có thể được gọi bởi nhiều NF, để giảm bớt việc ghép các định nghĩa giao diện giữa các NF, và cuối cùng thực hiện sự tùy biến theo yêu cầu đối với các chức năng trên toàn bộ chức năng mạng, để hỗ trợ linh hoạt các yêu cầu và kịch bản dịch vụ khác nhau.

Trong giải pháp kiến trúc dựa trên dịch vụ, phần tử mạng điều khiển chẳng hạn như thực thể chức năng kho lưu trữ (NF repository function, NRF) phần tử mạng thường cung cấp các chức năng như đăng ký dịch vụ, phát hiện và cấp quyền cho các NF, để thực hiện việc tạo cấu hình theo yêu cầu cho các NF và dịch vụ và sự liên kết giữa các NF. Ở giai đoạn phát hiện dịch vụ, theo phương pháp phát hiện khả thi hiện tại, NF thứ nhất gửi yêu cầu phát hiện đến NRF, ở đây yêu cầu phát hiện này được sử dụng để yêu cầu truy cập NF thứ hai, hoặc yêu cầu phát hiện này được sử dụng để yêu cầu thực hiện dịch vụ cụ thể. NRF xác định địa chỉ truy cập hoặc mã định danh của NF thứ hai dựa vào yêu cầu phát hiện nhận được, và gửi địa chỉ truy cập hoặc mã định danh của NF thứ

hai đến NF thứ nhất. NF thứ nhất truy cập NF thứ hai dựa vào địa chỉ truy cập hoặc mã định danh này.

Trong phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ nêu trên, để bảo đảm sự truyền thông bảo mật giữa NF thứ nhất và NF thứ hai, NRF thường tạo ra khóa bảo mật, và gửi khóa bảo mật này đến NF thứ nhất và NF thứ hai; và NF thứ nhất và NF thứ hai thực hiện xác thực bảo mật dựa vào khóa bảo mật. Tuy nhiên, trong phương pháp này, NRF được yêu cầu truyền thông với NF thứ hai, để thực hiện việc chia sẻ khóa bảo mật giữa NF thứ nhất và NF thứ hai. Điều này dẫn đến độ phức tạp truyền thông tương đối cao.

Bản chất kỹ thuật của sáng chế

Theo phương pháp và thiết bị phát hiện dựa vào kiến trúc dựa trên dịch vụ được đề xuất theo các phương án của sáng chế, trong quy trình phát hiện dịch vụ, việc xác thực của khóa bảo mật được thực hiện trực tiếp giữa NF thứ nhất và NF thứ hai, và NRF không cần truyền thông với NF thứ hai. Điều này có thể làm giảm bớt số lần truyền thông ở mức độ nhất định và giảm bớt được độ phức tạp truyền thông.

Theo khía cạnh thứ nhất, sáng chế đề xuất phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ. Phần tử mạng điều khiển xác định thông số bảo mật và gửi thông số bảo mật này đến phần tử mạng chức năng thứ nhất; phần tử mạng chức năng thứ nhất nhận thông số bảo mật được gửi bởi phần tử mạng điều khiển, và gửi thông số bảo mật này đến phần tử mạng chức năng thứ hai; và sau khi nhận thông số bảo mật được gửi bởi phần tử mạng chức năng thứ nhất, phần tử mạng chức năng thứ hai xác minh tính chính xác của thông số bảo mật này, và xác định, dựa vào tính chính xác của thông số bảo mật, xem yêu cầu truy cập có được cấp quyền bởi phần tử mạng chức năng thứ nhất hay không. Với phương pháp này, việc xác thực của khóa bảo mật được thực hiện trực tiếp giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai. Điều này làm giảm bớt số lần truyền thông giữa phần tử mạng chức năng và phần tử mạng điều khiển trong quy trình phát hiện ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Phần tử mạng chức năng thứ nhất này là phần tử mạng cần truy cập phần tử mạng chức năng khác hoặc có yêu cầu dịch vụ. Phần tử mạng chức năng thứ hai là phần tử mạng chức năng được truy cập bởi phần tử mạng chức năng thứ nhất, hoặc phần tử mạng có khả năng cung cấp dịch vụ được yêu cầu cho phần tử mạng chức năng thứ nhất.

Theo một thiết kế khả thi, phần tử mạng chức năng thứ nhất gửi yêu cầu phát hiện đến phần tử mạng điều khiển, khi xác định rằng phần tử mạng chức năng thứ nhất cần truy cập phần tử mạng chức năng khác hoặc xác định rằng phần tử mạng chức năng thứ nhất cần yêu cầu thực hiện dịch vụ. Sau khi nhận yêu cầu phát hiện được gửi bởi phần tử mạng chức năng thứ nhất, phần tử mạng điều khiển xác định, dựa vào yêu cầu phát hiện, địa chỉ truy cập hoặc mã định danh của phần tử mạng chức năng thứ hai thỏa mãn yêu cầu dịch vụ, và xác định thông số bảo mật. Phần tử mạng điều khiển này gửi phản hồi phát hiện đến phần tử mạng chức năng thứ nhất, trong đó phản hồi phát hiện này bao gồm thông số bảo mật được xác định và địa chỉ truy cập hoặc mã định danh của phần tử mạng chức năng thứ hai. Phần tử mạng chức năng thứ nhất nhận phản hồi phát hiện được gửi bởi phần tử mạng điều khiển, và gửi yêu cầu truy cập đến phần tử mạng chức năng thứ hai dựa vào địa chỉ hoặc mã định danh của phần tử mạng chức năng thứ hai có trong phản hồi phát hiện này, trong đó yêu cầu truy cập này bao gồm thông số bảo mật nhận được. Phần tử mạng chức năng thứ hai nhận yêu cầu truy cập được gửi bởi phần tử mạng chức năng thứ nhất, và thu được thông số bảo mật có trong yêu cầu truy cập này. Trong phương án thực hiện này, phần tử mạng chức năng thứ hai có thể thu được thông số bảo mật nhờ sử dụng cách báo hiệu đã có. Ngoài ra, phần tử mạng chức năng thứ hai còn cho phép phần tử mạng chức năng thứ nhất truy cập phần tử mạng chức năng thứ hai, khi xác định rằng thông số bảo mật được gửi bởi phần tử mạng chức năng thứ nhất là đúng, và có thể từ chối cho phép phần tử mạng chức năng thứ nhất truy cập phần tử mạng chức năng thứ hai, khi xác định rằng thông số bảo mật được gửi bởi phần tử mạng chức năng thứ nhất là không đúng, nhờ đó nâng cao sự bảo mật truyền thông.

Theo một thiết kế khả thi, thông số bảo mật bao gồm token thứ nhất bất đối xứng và khóa phiên thứ nhất được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai.

Phần tử mạng điều khiển tạo ra khóa phiên thứ nhất. Phần tử mạng điều khiển này thực hiện thuật toán chữ ký số đối với mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ nhất dựa vào khóa bí mật của phần tử mạng điều khiển, để tạo ra chữ ký số. Phần tử mạng điều khiển mật hóa chữ ký số, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, và khóa phiên thứ nhất dựa vào khóa công khai của phần tử mạng chức năng thứ hai, để tạo ra token thứ nhất bất đối xứng. Phần tử mạng điều khiển gửi, đến phần tử mạng chức năng thứ nhất, token thứ nhất bất đối xứng dưới dạng thông số bảo mật, và sau khi nhận token thứ nhất bất đối xứng, phần tử mạng chức năng thứ nhất gửi token thứ nhất bất đối xứng này đến phần tử mạng chức năng thứ hai. Phần tử mạng chức năng thứ hai nhận token thứ nhất bất đối xứng, giải mật token thứ nhất bất đối xứng nhờ sử dụng khóa bí mật của phần tử mạng chức năng thứ hai, thu được chữ ký số, và xác minh tính chính xác của chữ ký số nhờ sử dụng khóa công khai của phần tử mạng điều khiển và nội dung được ký. Nội dung được ký này bao gồm mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ nhất.

Ngoài ra, ngoài mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ nhất, giá trị tham số, mà phần tử mạng điều khiển thực hiện thuật toán chữ ký số đối với giá trị tham số này trong khi tạo ra chữ ký số, có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của chữ ký, giá trị nonce của chữ ký, giá trị đếm và số chuỗi. Nội dung được ký giống như giá trị tham số được sử dụng trong khi thực hiện thuật toán chữ ký số. Ngoài chữ ký số, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai và khóa phiên thứ nhất, thì giá trị tham số được mật hóa bởi phần tử mạng điều khiển trong khi tạo ra token thứ nhất

bất đối xứng có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của token-thứ nhất-bất đối xứng, giá trị nonce của token-thứ nhất-bất đối xứng, giá trị đếm và số chuỗi.

Theo thiết kế khả thi khác, thông số bảo mật bao gồm token thứ nhất đối xứng và khóa phiên thứ nhất được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai.

Phần tử mạng điều khiển tạo ra khóa phiên thứ nhất. Phần tử mạng điều khiển này thực hiện thuật toán mã xác thực thông điệp đối với mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ nhất dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra mã xác thực thông điệp. Phần tử mạng điều khiển mật hóa mã xác thực thông điệp, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, và khóa phiên thứ nhất dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra token thứ nhất đối xứng. Phần tử mạng điều khiển gửi, đến phần tử mạng chức năng thứ nhất, token thứ nhất đối xứng dưới dạng thông số bảo mật, và sau khi nhận token thứ nhất đối xứng, phần tử mạng chức năng thứ nhất gửi token thứ nhất đối xứng này đến phần tử mạng chức năng thứ hai. Phần tử mạng chức năng thứ hai nhận token thứ nhất đối xứng, giải mật token thứ nhất đối xứng nhờ sử dụng khóa đối xứng, để thu được mã xác thực thông điệp, và xác minh tính chính xác của mã xác thực thông điệp nhờ sử dụng khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai và nội dung được bảo vệ bởi mã xác thực thông điệp này. Nội dung được bảo vệ bởi mã xác thực thông điệp bao gồm mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ nhất.

Ngoài ra, ngoài mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ nhất, giá trị tham số, mà phần tử mạng điều khiển thực hiện thuật toán mã xác thực thông điệp đối với giá trị tham số này trong khi tạo ra mã xác thực thông điệp, có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của mã xác thực thông điệp, giá trị nonce của mã xác thực thông điệp, giá trị đếm và số chuỗi. Nội dung được bảo vệ bởi mã xác thực thông điệp giống như giá trị tham số được sử dụng trong khi thực hiện thuật toán mã xác thực thông điệp. Ngoài mã xác thực thông điệp, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, và khóa phiên thứ nhất, thì giá trị tham số được mật hóa bởi phần tử mạng điều khiển trong khi tạo ra token thứ nhất đối xứng có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của token-thứ nhất-đối xứng, giá trị nonce của token-thứ nhất-đối xứng, giá trị đếm và số chuỗi.

Khi phần tử mạng điều khiển tạo ra khóa phiên thứ nhất, theo phương án thực hiện khả thi, khóa phiên thứ nhất được lựa chọn ngẫu nhiên bởi phần tử mạng điều khiển. Theo phương án thực hiện khả thi khác, khóa phiên thứ nhất được tạo ra bởi phần tử mạng điều khiển nhờ thực hiện phép tạo dẫn xuất đối với mã định danh của phần tử mạng chức năng thứ nhất và mã định danh của phần tử mạng chức năng thứ hai dựa vào khóa dẫn xuất. Khóa dẫn xuất thu được bởi phần tử mạng điều khiển nhờ thực hiện phép tạo dẫn xuất khóa đối với khóa gốc được thiết lập trước, hoặc khóa dẫn xuất này là khóa được lưu bởi phần tử mạng điều khiển.

Ngoài ra, trong khi tạo ra khóa phiên thứ nhất bởi phần tử mạng điều khiển, giá trị tham số mà phép tạo dẫn xuất được thực hiện đối với giá trị tham số này có thể bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng chức năng thứ nhất,

mã định danh của phần tử mạng chức năng thứ hai, địa chỉ truy cập hoặc mã định danh của phần tử mạng chức năng thứ hai, mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và dạng tương tự. Phần tử mạng điều khiển này thực hiện phép tạo dẫn xuất đối với giá trị tham số nêu trên, và có thể còn thực hiện phép tạo dẫn xuất đối với ít nhất một giá trị trong số chu kỳ hợp lệ của khóa phiên thứ nhất, giá trị nonce của khóa phiên thứ nhất, giá trị đếm, và số chuỗi, để tạo ra khóa phiên thứ nhất.

Theo một thiết kế khả thi khác nữa, phần tử mạng chức năng thứ hai giải mật token thứ nhất đối xứng hoặc token thứ nhất bất đối xứng để còn thu được khóa phiên thứ nhất, và phần tử mạng chức năng thứ hai và phần tử mạng chức năng thứ nhất có thể chia sẻ khóa phiên thứ nhất. Phần tử mạng chức năng thứ hai và phần tử mạng chức năng thứ nhất có thể thiết lập kênh bảo mật dựa vào khóa phiên thứ nhất hoặc khóa được dẫn xuất từ khóa phiên thứ nhất.

Trong phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ được đề xuất theo phương án này của sáng chế, phần tử mạng điều khiển tạo ra token thứ nhất đối xứng hoặc token thứ nhất bất đối xứng và khóa phiên thứ nhất được sử dụng để bảo vệ toàn bộ dữ liệu được sử dụng cho việc truyền thông giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai. Điều này có thể thực hiện được việc bảo vệ bảo mật dựa trên kết nối, và thực hiện được việc xác thực bảo mật đối với thông số bảo mật giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai khi phần tử mạng điều khiển và phần tử mạng chức năng thứ hai không trao đổi thông số bảo mật. Điều này làm giảm bớt số lần truyền thông giữa phần tử mạng chức năng và phần tử mạng điều khiển trong quy trình phát hiện ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Theo một thiết kế khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai, và token thứ hai bất đối xứng được tạo ra dựa vào từng khóa phiên thứ hai.

Phần tử mạng điều khiển tạo ra khóa phiên thứ hai bảo vệ từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất. Phần tử mạng điều khiển này thực hiện, đối với từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, thuật toán chữ ký số đối với mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ hai dựa vào khóa bí mật của phần tử mạng điều khiển, để tạo ra chữ ký số. Phần tử mạng điều khiển này mật hóa, đối với từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, chữ ký số, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, mã định danh dịch vụ của dịch vụ được bảo vệ bởi khóa phiên thứ hai, và khóa phiên thứ hai dựa vào khóa công khai của phần tử mạng chức năng thứ hai, để tạo ra token thứ hai bất đối xứng của từng dịch vụ. Phần tử mạng điều khiển gửi, đến phần tử mạng chức năng thứ nhất, token thứ hai bất đối xứng tương ứng với từng dịch vụ dưới dạng thông số bảo mật, và sau khi nhận token thứ hai bất đối xứng tương ứng với từng dịch vụ, phần tử mạng chức năng thứ nhất gửi token thứ hai bất đối xứng tương ứng với dịch vụ được yêu cầu đến phần tử mạng chức năng thứ hai dựa vào dịch vụ được yêu cầu. Phần tử mạng chức năng thứ hai nhận token thứ hai bất đối xứng, giải mật token thứ hai bất đối xứng này nhờ sử dụng khóa bí mật của phần tử mạng chức năng thứ hai, thu được chữ ký số, và xác minh tính chính xác của chữ ký số nhờ sử dụng khóa công khai của phần tử mạng điều khiển và nội dung được ký. Nội dung được ký này bao gồm mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ hai.

Ngoài ra, ngoài mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ hai, giá trị tham số, mà phần tử mạng điều khiển thực hiện thuật toán chữ ký số đối với giá trị tham số này trong khi tạo ra chữ ký số, có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của chữ ký, giá trị nonce của chữ ký, giá trị đếm và số chuỗi. Nội dung được ký giống như giá trị tham số được sử dụng trong khi thực hiện thuật toán chữ ký số. Ngoài chữ ký số, mã định danh của phần tử mạng chức năng thứ

nhất, mã định danh của phần tử mạng chức năng thứ hai, và khóa phiên thứ hai, thì giá trị tham số được mật hóa bởi phần tử mạng điều khiển trong khi tạo ra token thứ hai bất đối xứng có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ token-thứ hai-bất đối xứng, giá trị nonce token-thứ hai-bất đối xứng, giá trị đếm và số chuỗi.

Theo một thiết kế khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai, và token thứ hai đối xứng được tạo ra dựa vào từng khóa phiên thứ hai.

Phần tử mạng điều khiển này tạo ra khóa phiên thứ hai bảo vệ từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất. Phần tử mạng điều khiển này thực hiện, đối với từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, thuật toán mã xác thực thông điệp đối với mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ hai dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra mã xác thực thông điệp. Phần tử mạng điều khiển mật hóa mã xác thực thông điệp, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, mã định danh dịch vụ của dịch vụ được bảo vệ bởi khóa phiên thứ hai, và khóa phiên thứ hai dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra token thứ hai đối xứng cho từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất. Phần tử mạng điều khiển gửi, đến phần tử mạng chức năng thứ nhất, token thứ hai đối xứng dưới dạng thông số bảo mật, và sau khi nhận token thứ hai đối xứng, phần tử mạng chức năng thứ nhất gửi token thứ hai đối xứng đến phần tử mạng chức năng thứ hai. Phần tử mạng chức năng thứ hai nhận token thứ hai đối xứng, giải mật token thứ hai đối xứng này nhờ sử dụng khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để thu được mã xác thực thông điệp, và xác minh tính chính xác của mã xác thực thông điệp này nhờ sử dụng khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai và nội dung được bảo vệ

bởi mã xác thực thông điệp này. Nội dung được bảo vệ bởi mã xác thực thông điệp bao gồm mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ hai.

Ngoài ra, ngoài mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ hai, giá trị tham số, mà phần tử mạng điều khiển thực hiện thuật toán mã xác thực thông điệp đối với giá trị tham số này trong khi tạo ra mã xác thực thông điệp, có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của mã xác thực thông điệp, giá trị nonce của mã xác thực thông điệp, giá trị đếm và số chuỗi. Nội dung được bảo vệ bởi mã xác thực thông điệp giống như giá trị tham số được sử dụng trong khi thực hiện thuật toán mã xác thực thông điệp. Ngoài mã xác thực thông điệp, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, và khóa phiên thứ hai, thì giá trị tham số được mật hóa bởi phần tử mạng điều khiển trong khi tạo ra token thứ hai đối xứng có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của token-thứ hai-đối xứng, giá trị nonce của token-thứ hai-đối xứng, giá trị đếm và số chuỗi.

Trong phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ được đề xuất theo phương án này của sáng chế, phần tử mạng điều khiển tạo ra khóa phiên thứ hai và token thứ hai đối với từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất. Điều này có thể thực hiện việc bảo vệ bảo mật dựa trên dịch vụ, và thực hiện việc xác thực bảo mật đối với thông số bảo mật giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai khi phần tử mạng điều khiển và phần tử mạng chức năng thứ hai không trao đổi thông số bảo mật. Điều này làm giảm bớt số lần truyền thông giữa phần tử mạng chức năng và phần tử mạng điều khiển trong quy trình phát hiện ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Theo một thiết kế khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai, và token thứ ba bất đối xứng được tạo ra dựa vào tất cả các khóa phiên thứ hai.

Phần tử mạng điều khiển tạo ra khóa phiên thứ hai bảo vệ từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất. Phần tử mạng điều khiển này thực hiện thuật toán chữ ký số đối với mã định danh của phần tử mạng chức năng thứ nhất và tất cả các khóa phiên thứ hai dựa vào khóa bí mật của phần tử mạng điều khiển, để tạo ra chữ ký số. Phần tử mạng điều khiển mật hóa chữ ký số, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, các mã định danh dịch vụ của các dịch vụ được bảo vệ bởi tất cả các khóa phiên thứ hai, và tất cả các khóa phiên thứ hai dựa vào khóa công khai của phần tử mạng chức năng thứ hai, để tạo ra token thứ ba bất đối xứng của các dịch vụ. Phần tử mạng điều khiển gửi, đến phần tử mạng chức năng thứ nhất, token thứ ba bất đối xứng dưới dạng thông số bảo mật, và sau khi nhận token thứ ba bất đối xứng, phần tử mạng chức năng thứ nhất gửi token thứ ba bất đối xứng đến phần tử mạng chức năng thứ hai. Phần tử mạng chức năng thứ hai nhận token thứ ba bất đối xứng, giải mật token thứ ba nhờ sử dụng khóa bí mật của phần tử mạng chức năng thứ hai, thu được chữ ký số, và xác minh tính chính xác của chữ ký số nhờ sử dụng khóa công khai của phần tử mạng điều khiển và nội dung được ký. Nội dung được ký này bao gồm mã định danh của phần tử mạng chức năng thứ nhất và tất cả các khóa phiên thứ hai.

Ngoài ra, ngoài mã định danh của phần tử mạng chức năng thứ nhất và tất cả các khóa phiên thứ hai, giá trị tham số, mà phần tử mạng điều khiển thực hiện thuật toán chữ ký số đối với giá trị tham số này trong khi tạo ra chữ ký số, có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của chữ ký, giá trị nonce của chữ ký, giá trị đếm và số chuỗi. Nội dung được ký giống như giá trị tham số được sử dụng trong khi thực hiện thuật toán chữ ký số. Ngoài chữ ký số, mã định danh của phần tử mạng chức

năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, và tất cả các khóa phiên thứ hai, thì giá trị tham số được mật hóa bởi phần tử mạng điều khiển trong khi tạo ra token thứ ba bất đối xứng có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một trong số chu kỳ hợp lệ của token-thứ ba-bất đối xứng, giá trị nonce của token-thứ ba-bất đối xứng, giá trị đếm và số chuỗi.

Theo một thiết kế khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai, và token thứ ba đối xứng được tạo ra dựa vào tất cả các khóa phiên thứ hai.

Phần tử mạng điều khiển tạo ra khóa phiên thứ hai bảo vệ từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất. Phần tử mạng điều khiển này thực hiện thuật toán mã xác thực thông điệp đối với mã định danh của phần tử mạng chức năng thứ nhất và tất cả các khóa phiên thứ hai dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra mã xác thực thông điệp. Phần tử mạng điều khiển mật hóa mã xác thực thông điệp, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, các mã định danh dịch vụ của các dịch vụ được bảo vệ bởi tất cả các khóa phiên thứ hai, và tất cả các khóa phiên thứ hai dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra token thứ ba đối xứng. Phần tử mạng điều khiển gửi, đến phần tử mạng chức năng thứ nhất, token thứ ba đối xứng dưới dạng thông số bảo mật, và sau khi nhận token thứ ba đối xứng, phần tử mạng chức năng thứ nhất gửi token thứ ba đối xứng đến phần tử mạng chức năng thứ hai. Phần tử mạng chức năng thứ hai nhận token thứ ba đối xứng, giải mật token thứ ba đối xứng này nhờ sử dụng khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để thu được mã xác thực thông điệp, và xác minh tính chính xác của mã xác thực thông điệp này nhờ sử dụng khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai và nội dung được bảo vệ bởi mã xác thực

thông điệp này. Nội dung được bảo vệ bởi mã xác thực thông điệp bao gồm mã định danh của phần tử mạng chức năng thứ nhất và tất cả các khóa phiên thứ hai.

Ngoài ra, ngoài mã định danh của phần tử mạng chức năng thứ nhất và tất cả các khóa phiên thứ hai, giá trị tham số, mà phần tử mạng điều khiển thực hiện thuật toán mã xác thực thông điệp đối với giá trị tham số này trong khi tạo ra mã xác thực thông điệp, có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của mã xác thực thông điệp, giá trị nonce của mã xác thực thông điệp, giá trị đếm và số chuỗi. Nội dung được bảo vệ bởi mã xác thực thông điệp giống như giá trị tham số được sử dụng trong khi thực hiện thuật toán mã xác thực thông điệp. Ngoài mã xác thực thông điệp, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, và tất cả các khóa phiên thứ hai, giá trị tham số được mật hóa bởi phần tử mạng điều khiển trong khi tạo ra token thứ ba đối xứng có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của token-thứ ba-đối xứng, giá trị nonce của token-thứ ba-đối xứng, giá trị đếm và số chuỗi.

Khi phần tử mạng điều khiển tạo ra khóa phiên thứ hai cho từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, theo phương án thực hiện khả thi, khóa phiên thứ hai được lựa chọn ngẫu nhiên bởi phần tử mạng điều khiển. Theo phương án thực hiện khả thi khác, khóa phiên thứ hai được tạo ra bởi phần tử mạng điều khiển nhờ thực hiện phép tạo dẫn xuất đối với mã định danh của phần tử mạng chức năng thứ nhất và mã định danh của phần tử mạng chức năng thứ hai dựa vào khóa dẫn xuất. Khóa dẫn xuất này thu được bởi phần tử mạng điều khiển nhờ thực hiện phép tạo dẫn xuất khóa đối với khóa gốc được thiết lập trước, hoặc khóa dẫn xuất này là khóa được lưu bởi phần tử mạng điều khiển này.

Ngoài ra, trong khi tạo ra khóa phiên thứ hai bởi phần tử mạng điều khiển, giá trị tham số mà phép tạo dẫn xuất được thực hiện đối với giá trị tham số này có thể bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, địa chỉ truy cập hoặc mã định danh của phần tử mạng chức năng thứ hai, mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và dạng tương tự. Phần tử mạng điều khiển này thực hiện phép tạo dẫn xuất đối với giá trị tham số nêu trên, và có thể còn thực hiện phép tạo dẫn xuất đối với ít nhất một giá trị trong số chu kỳ hợp lệ của khóa phiên thứ hai, giá trị nonce của khóa phiên thứ hai, giá trị đếm và số chuỗi, để tạo ra khóa phiên thứ hai.

Trong phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ được đề xuất theo phương án này của sáng chế, phần tử mạng điều khiển tạo ra khóa phiên thứ hai cho từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và bổ sung tất cả các khóa phiên thứ hai vào một token thứ ba. Điều này có thể thực hiện việc bảo vệ bảo mật dựa trên dịch vụ, và việc gửi một token đến phần tử mạng chức năng thứ hai có thể giảm bớt được độ phức tạp truyền thông.

Theo một thiết kế khả thi khác nữa, phần tử mạng chức năng thứ hai giải mật token thứ hai hoặc token thứ ba để còn thu được khóa phiên thứ hai, và phần tử mạng chức năng thứ hai và phần tử mạng chức năng thứ nhất có thể chia sẻ khóa phiên thứ hai này. Phần tử mạng chức năng thứ hai và phần tử mạng chức năng thứ nhất có thể thiết lập, đối với dịch vụ được bảo vệ bởi khóa phiên thứ hai, kênh bảo mật dựa vào khóa phiên thứ hai hoặc khóa được dẫn xuất từ khóa phiên thứ hai.

Theo một thiết kế khả thi khác nữa, thông số bảo mật bao gồm chữ ký số.

Phần tử mạng điều khiển thực hiện thuật toán chữ ký số đối với mã định danh của phần tử mạng chức năng thứ nhất dựa vào khóa bí mật của phần tử mạng điều khiển, để tạo ra chữ ký số. Phần tử mạng điều khiển gửi, đến phần tử mạng chức năng thứ nhất, chữ ký số được tạo ra dưới dạng thông số bảo mật. Sau khi nhận chữ ký số, phần tử

mạng chức năng thứ nhất gửi chữ ký số đến phần tử mạng chức năng thứ hai. Phần tử mạng chức năng thứ hai nhận chữ ký số được gửi bởi phần tử mạng chức năng thứ nhất, và xác minh tính chính xác của chữ ký số này nhờ sử dụng khóa công khai của phần tử mạng điều khiển và nội dung được ký bởi chữ ký số. Nội dung được ký bởi chữ ký số này bao gồm mã định danh của phần tử mạng chức năng thứ nhất.

Ngoài ra, ngoài mã định danh của phần tử mạng chức năng thứ nhất, giá trị tham số, mà phần tử mạng điều khiển thực hiện thuật toán chữ ký số đối với giá trị tham số này trong khi tạo ra chữ ký số, có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của chữ ký, giá trị nonce của chữ ký, giá trị đếm và số chuỗi. Nội dung được ký giống như giá trị tham số được sử dụng trong khi thực hiện thuật toán chữ ký số.

Phần tử mạng điều khiển có thể tạo ra chữ ký số dựa vào từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, để thực hiện việc xác minh cấp quyền ở mức dịch vụ.

Trong phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ được đề xuất theo phương án này của sáng chế, phần tử mạng điều khiển tạo ra chữ ký số, và khi phần tử mạng điều khiển và phần tử mạng chức năng thứ hai không trao đổi thông số bảo mật, phần tử mạng chức năng thứ hai có thể thực hiện việc xác minh cấp quyền đối với phần tử mạng chức năng thứ nhất. Điều này làm giảm bớt số lần truyền thông giữa phần tử mạng chức năng và phần tử mạng điều khiển trong quy trình phát hiện ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Theo một thiết kế khả thi khác nữa, thông số bảo mật bao gồm mã xác thực thông điệp.

Phần tử mạng điều khiển thực hiện thuật toán mã xác thực thông điệp đối với mã định danh của phần tử mạng chức năng thứ nhất dựa vào khóa đối xứng được chia sẻ

giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra mã xác thực thông điệp. Phần tử mạng điều khiển gửi, đến phần tử mạng chức năng thứ nhất, mã xác thực thông điệp được tạo ra dưới dạng thông số bảo mật. Sau khi nhận mã xác thực thông điệp, phần tử mạng chức năng thứ nhất gửi mã xác thực thông điệp đến phần tử mạng chức năng thứ hai. Phần tử mạng chức năng thứ hai nhận mã xác thực thông điệp được gửi bởi phần tử mạng chức năng thứ nhất, và xác minh tính chính xác của mã xác thực thông điệp nhờ sử dụng khóa đối xứng và nội dung được bảo vệ bởi mã xác thực thông điệp này. Nội dung được bảo vệ bởi mã xác thực thông điệp bao gồm mã định danh của phần tử mạng chức năng thứ nhất.

Ngoài ra, ngoài mã định danh của phần tử mạng chức năng thứ nhất, giá trị tham số, mà phần tử mạng điều khiển thực hiện thuật toán mã xác thực thông điệp đối với giá trị tham số này trong khi tạo ra mã xác thực thông điệp, có thể còn bao gồm một hoặc nhiều giá trị trong số mã định danh của phần tử mạng điều khiển, PLMN ID của phần tử mạng chức năng thứ nhất, PLMN ID của phần tử mạng chức năng thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và ít nhất một giá trị trong số chu kỳ hợp lệ của mã xác thực thông điệp, giá trị nonce của mã xác thực thông điệp, giá trị đếm và số chuỗi. Nội dung được bảo vệ bởi mã xác thực thông điệp giống như giá trị tham số được sử dụng trong khi thực hiện thuật toán mã xác thực thông điệp.

Phần tử mạng điều khiển có thể tạo ra mã xác thực thông điệp dựa vào từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, để thực hiện việc xác minh cấp quyền ở mức dịch vụ.

Trong phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ được đề xuất theo Phương án 4 của sáng chế, phần tử mạng điều khiển tạo ra mã xác thực thông điệp, và khi phần tử mạng điều khiển và phần tử mạng chức năng thứ hai không trao đổi thông số bảo mật, phần tử mạng chức năng thứ hai có thể thực hiện việc xác minh cấp quyền đối với phần tử mạng chức năng thứ nhất. Điều này làm giảm bớt số lần truyền thông giữa phần tử mạng chức năng và phần tử mạng điều khiển trong quy trình phát hiện ở

mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Theo một thiết kế khả thi khác nữa, khi phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai ở trong kịch bản chuyển vùng, phần tử mạng điều khiển bao gồm phần tử mạng điều khiển thuộc PLMN thứ nhất và phần tử mạng điều khiển thuộc PLMN thứ hai. Phần tử mạng điều khiển thuộc PLMN thứ nhất được tạo cấu hình để quản lý và điều khiển phần tử mạng chức năng thứ nhất, và phần tử mạng điều khiển thuộc PLMN thứ hai được tạo cấu hình để quản lý và điều khiển phần tử mạng chức năng thứ hai. Phần tử mạng điều khiển thuộc PLMN thứ hai tạo ra thông số bảo mật, và gửi thông số bảo mật này đến phần tử mạng điều khiển thuộc PLMN thứ nhất. Phần tử mạng điều khiển thuộc LMN thứ nhất nhận thông số bảo mật được gửi bởi phần tử mạng điều khiển thuộc PLMN thứ hai, và gửi thông số bảo mật nhận được này đến phần tử mạng chức năng thứ nhất, và phần tử mạng chức năng thứ nhất gửi thông số bảo mật này đến phần tử mạng chức năng thứ hai, nhờ đó thực hiện việc xác thực bảo mật của phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai trong kịch bản chuyển vùng.

Quy trình tạo ra thông số bảo mật bởi phần tử mạng điều khiển thuộc PLMN thứ hai tương tự các quy trình tạo ra thông số bảo mật trong các thiết kế nêu trên. Điểm khác biệt nằm ở chỗ ngoài giá trị tham số nêu trên, giá trị tham số được sử dụng trong khi tạo ra thông số bảo mật còn bao gồm mã nhận dạng của PLMN thứ nhất, hoặc mã nhận dạng của PLMN thứ hai, hoặc mã nhận dạng của PLMN thứ nhất và mã nhận dạng của PLMN thứ hai.

Theo một thiết kế khả thi khác nữa, nếu dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất cần được thay đổi, ví dụ, theo kịch bản trong đó dịch vụ được yêu cầu cần được xóa bỏ, hoặc dịch vụ được yêu cầu cần được sửa đổi, phần tử mạng chức năng thứ nhất, phần tử mạng điều khiển, hoặc phần tử mạng quản lý có thể khởi tạo yêu cầu thay đổi dịch vụ.

Theo phương án khả thi, khi phần tử mạng chức năng thứ nhất xác định rằng dịch vụ được yêu cầu cần được thay đổi, phần tử mạng chức năng thứ nhất tạo ra mã xác thực thông điệp hoặc chữ ký số, và gửi yêu cầu thay đổi dịch vụ đến phần tử mạng điều khiển. Yêu cầu thay đổi dịch vụ này bao gồm mã xác thực thông điệp hoặc chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ. Phần tử mạng điều khiển nhận yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng chức năng thứ nhất, và thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng chức năng thứ nhất. Nếu xác định rằng yêu cầu thay đổi dịch vụ nhận được được cấp quyền bởi phần tử mạng chức năng thứ nhất, phần tử mạng điều khiển có thể thay đổi dịch vụ được yêu cầu thay đổi bởi yêu cầu thay đổi dịch vụ.

Mã xác thực thông điệp thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ có thể được tạo ra bởi phần tử mạng chức năng thứ nhất nhờ thực hiện thuật toán mã xác thực thông điệp đối với mã định danh dịch vụ được thay đổi bởi yêu cầu thay đổi dịch vụ và mã định danh của phần tử mạng chức năng thứ nhất dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng điều khiển. Chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ có thể được tạo ra bởi phần tử mạng chức năng thứ nhất nhờ thực hiện thuật toán chữ ký số đối với mã định danh dịch vụ được thay đổi bởi yêu cầu thay đổi dịch vụ và mã định danh của phần tử mạng chức năng thứ nhất dựa vào khóa bí mật của phần tử mạng chức năng thứ nhất.

Nếu phần tử mạng chức năng thứ nhất đã truy cập phần tử mạng chức năng thứ hai, phần tử mạng chức năng thứ nhất có thể gửi thông báo thay đổi dịch vụ đến phần tử mạng chức năng thứ hai để chỉ thị cho phần tử mạng chức năng thứ hai thay đổi dịch vụ.

Theo phương án thực hiện khả thi khác, khi phần tử mạng điều khiển xác định rằng dịch vụ được yêu cầu cần được thay đổi, phần tử mạng điều khiển tạo ra MAC hoặc chữ ký số, trong đó MAC hoặc chữ ký số này có thể thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng điều khiển đến phần tử mạng

chức năng thứ nhất. Phần tử mạng điều khiển gửi yêu cầu thay đổi dịch vụ đến phần tử mạng chức năng thứ nhất, trong đó yêu cầu thay đổi dịch vụ bao gồm MAC hoặc chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ. Phần tử mạng chức năng thứ nhất nhận yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng điều khiển, và thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng điều khiển. Nếu xác định rằng yêu cầu thay đổi dịch vụ nhận được được cấp quyền bởi phần tử mạng điều khiển, phần tử mạng chức năng thứ nhất có thể thay đổi dịch vụ được yêu cầu thay đổi bởi yêu cầu thay đổi dịch vụ này.

Mã xác thực thông điệp thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ có thể được tạo ra bởi phần tử mạng điều khiển nhờ thực hiện thuật toán mã xác thực thông điệp đối với mã định danh dịch vụ được thay đổi bởi yêu cầu thay đổi dịch vụ và mã định danh của phần tử mạng chức năng thứ nhất dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng điều khiển. Chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ có thể được tạo ra bởi phần tử mạng điều khiển nhờ thực hiện thuật toán chữ ký số đối với mã định danh dịch vụ được thay đổi bởi yêu cầu thay đổi dịch vụ và mã định danh của phần tử mạng chức năng thứ nhất dựa vào khóa bí mật của phần tử mạng điều khiển.

Nếu phần tử mạng chức năng thứ nhất đã truy cập phần tử mạng chức năng thứ hai, phần tử mạng chức năng thứ nhất có thể gửi thông báo thay đổi dịch vụ đến phần tử mạng chức năng thứ hai để chỉ thị cho phần tử mạng chức năng thứ hai thay đổi dịch vụ.

Theo phương án thực hiện khả thi khác nữa, khi xác định rằng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất cần được thay đổi, phần tử mạng quản lý tạo ra MAC hoặc chữ ký số, trong đó MAC hoặc chữ ký số có thể thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng quản lý đến phần tử mạng điều khiển. Phần tử mạng quản lý này gửi yêu cầu thay đổi dịch vụ đến phần tử mạng điều khiển, trong đó yêu cầu thay đổi dịch vụ này bao gồm MAC hoặc chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ. Phần tử mạng điều khiển

nhận yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng quản lý, và thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng quản lý.

Mã xác thực thông điệp thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ có thể được tạo ra bởi phần tử mạng quản lý nhờ thực hiện thuật toán mã xác thực thông điệp đối với mã định danh dịch vụ được thay đổi bởi yêu cầu thay đổi dịch vụ và mã định danh của phần tử mạng chức năng thứ nhất dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng quản lý và phần tử mạng điều khiển. Chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ có thể được tạo ra bởi phần tử mạng quản lý nhờ thực hiện thuật toán chữ ký số đối với mã định danh dịch vụ được thay đổi bởi yêu cầu thay đổi dịch vụ và mã định danh của phần tử mạng chức năng thứ nhất dựa vào khóa bí mật của phần tử mạng quản lý.

Nếu xác định rằng phần tử mạng quản lý cấp quyền cho yêu cầu thay đổi dịch vụ được gửi, phần tử mạng điều khiển gửi thông báo thay đổi dịch vụ đến phần tử mạng chức năng thứ nhất. Phần tử mạng chức năng thứ nhất nhận thông báo thay đổi dịch vụ thứ nhất được gửi bởi phần tử mạng điều khiển, và gửi thông báo thay đổi dịch vụ đến phần tử mạng chức năng thứ hai khi xác định rằng phần tử mạng chức năng thứ nhất đã truy cập phần tử mạng chức năng thứ hai, để chỉ thị cho phần tử mạng chức năng thứ hai thay đổi dịch vụ.

Theo khía cạnh thứ hai, sáng chế đề xuất thiết bị phát hiện dựa vào kiến trúc dựa trên dịch vụ. Thiết bị phát hiện này có thể được áp dụng cho phần tử mạng điều khiển, và thiết bị phát hiện này được áp dụng cho phần tử mạng điều khiển có chức năng thực hiện phần tử mạng điều khiển theo một dấu hiệu bất kỳ trong số khía cạnh thứ nhất và các thiết kế của khía cạnh thứ nhất. Chức năng này có thể được thực hiện bởi phần cứng, hoặc có thể được thực hiện bởi phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm này bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên. Môđun này có thể là phần mềm và/hoặc phần cứng.

Theo một thiết kế khả thi, thiết bị phát hiện được áp dụng cho phần tử mạng điều khiển bao gồm bộ phận xử lý và bộ phận gửi, và có thể còn có bộ phận nhận. Bộ phận

nhận, bộ phận xử lý và bộ phận gửi có thể tương ứng với các bước chức năng được thực hiện bởi phần tử mạng điều khiển nêu trên. Các chi tiết không được mô tả lại dưới đây.

Theo thiết kế khả thi khác, thiết bị phát hiện được áp dụng cho phần tử mạng điều khiển bao gồm bộ xử lý, bộ thu phát, và bộ nhớ. Bộ nhớ được nối với bộ xử lý, và được tạo cấu hình để lưu trữ các chương trình phần mềm khác nhau và/hoặc các tập hợp lệnh. Bộ xử lý gọi các chương trình hoặc các lệnh được lưu trữ của bộ nhớ để thực hiện các bước chức năng được thực hiện bởi phần tử mạng điều khiển nêu trên, và điều khiển bộ thu phát gửi và nhận tín hiệu.

Theo khía cạnh thứ ba, sáng chế đề xuất thiết bị phát hiện dựa vào kiến trúc dựa trên dịch vụ. Thiết bị phát hiện này có thể được áp dụng cho phần tử mạng chức năng thứ nhất, và thiết bị phát hiện được áp dụng cho phần tử mạng chức năng thứ nhất có chức năng thực hiện phần tử mạng chức năng thứ nhất theo một dấu hiệu bất kỳ trong số khía cạnh thứ nhất và các thiết kế của khía cạnh thứ nhất. Chức năng này có thể được thực hiện bởi phần cứng, hoặc có thể được thực hiện bởi phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm này bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên. Môđun này có thể là phần mềm và/hoặc phần cứng.

Theo một thiết kế khả thi, thiết bị phát hiện được áp dụng cho phần tử mạng chức năng thứ nhất bao gồm bộ phận nhận và bộ phận gửi, và có thể còn có bộ phận xử lý. Bộ phận nhận, bộ phận xử lý, và bộ phận gửi có thể tương ứng với các bước chức năng được thực hiện bởi phần tử mạng chức năng thứ nhất nêu trên. Các chi tiết không được mô tả lại dưới đây.

Theo thiết kế khả thi khác, thiết bị phát hiện được áp dụng cho phần tử mạng chức năng thứ nhất bao gồm bộ xử lý, bộ thu phát, và bộ nhớ. Bộ nhớ được nối với bộ xử lý, và được tạo cấu hình để lưu trữ các chương trình phần mềm khác nhau và/hoặc các tập hợp lệnh. Bộ xử lý gọi các chương trình hoặc các lệnh được lưu trữ của bộ nhớ để thực hiện các bước chức năng được thực hiện bởi phần tử mạng chức năng thứ nhất nêu trên, và điều khiển bộ thu phát gửi và nhận tín hiệu.

Theo khía cạnh thứ tư, sáng chế đề xuất thiết bị phát hiện dựa vào kiến trúc dựa trên dịch vụ. Thiết bị phát hiện này có thể được áp dụng cho phần tử mạng chức năng thứ hai, và thiết bị phát hiện được áp dụng cho phần tử mạng chức năng thứ hai có chức năng thực hiện phần tử mạng chức năng thứ hai theo một dấu hiệu bất kỳ trong số khía cạnh thứ nhất và các thiết kế của khía cạnh thứ nhất. Chức năng này có thể được thực hiện bởi phần cứng, hoặc có thể được thực hiện bởi phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm này bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên. Môđun này có thể là phần mềm và/hoặc phần cứng.

Theo một thiết kế khả thi, thiết bị phát hiện được áp dụng cho phần tử mạng chức năng thứ hai bao gồm bộ phận nhận và bộ phận xử lý. Bộ phận nhận và bộ phận xử lý có thể tương ứng với các bước chức năng được thực hiện bởi phần tử mạng chức năng thứ hai nêu trên. Các chi tiết không được mô tả lại dưới đây.

Theo thiết kế khả thi khác, thiết bị phát hiện được áp dụng cho phần tử mạng chức năng thứ hai bao gồm bộ xử lý và bộ thu phát. Bộ nhớ được nối với bộ xử lý, và được tạo cấu hình để lưu trữ các chương trình phần mềm khác nhau và/hoặc các tập hợp lệnh. Bộ xử lý gọi các chương trình hoặc các lệnh được lưu trữ của bộ nhớ để thực hiện các bước chức năng được thực hiện bởi phần tử mạng chức năng thứ hai nêu trên, và điều khiển bộ thu phát gửi và nhận tín hiệu.

Theo khía cạnh thứ năm, sáng chế đề xuất vật ghi lưu trữ bởi máy tính. Vật ghi lưu trữ bởi máy tính lưu trữ lệnh máy tính. Khi lệnh này chạy trên máy tính, chức năng bất kỳ của phần tử mạng chức năng thứ nhất, phần tử mạng chức năng thứ hai, hoặc phần tử mạng điều khiển theo một dấu hiệu bất kỳ trong số khía cạnh thứ nhất và các thiết kế khả thi của khía cạnh thứ nhất có thể được thực hiện.

Theo khía cạnh thứ sáu, sáng chế đề xuất sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính này bao gồm chương trình máy tính. Chương trình máy tính này được sử dụng để thực hiện chức năng bất kỳ của phần tử mạng chức năng thứ nhất, phần tử mạng chức năng thứ hai, hoặc phần tử mạng điều khiển theo một dấu hiệu bất kỳ trong số khía cạnh thứ nhất và các thiết kế khả thi của khía cạnh thứ nhất.

Theo phương pháp và thiết bị phát hiện dựa vào kiến trúc dựa trên dịch vụ được đề xuất theo các phương án của sáng chế, phần tử mạng điều khiển xác định thông số bảo mật và gửi thông số bảo mật này đến phần tử mạng chức năng thứ nhất; phần tử mạng chức năng thứ nhất nhận thông số bảo mật được gửi bởi phần tử mạng điều khiển, và gửi thông số bảo mật này đến phần tử mạng chức năng thứ hai; và sau khi nhận thông số bảo mật được gửi bởi phần tử mạng chức năng thứ nhất, phần tử mạng chức năng thứ hai xác minh tính chính xác của thông số bảo mật này, và xác định, dựa vào tính chính xác của thông số bảo mật, xem yêu cầu truy cập có được cấp quyền bởi phần tử mạng chức năng thứ nhất hay không. Với phương pháp này, việc xác thực khóa bảo mật được thực hiện trực tiếp giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai. Điều này làm giảm bớt số lần truyền thông giữa phần tử mạng chức năng và phần tử mạng điều khiển trong quy trình phát hiện ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ thể hiện kiến trúc dựa trên dịch vụ theo phương án của sáng chế;

Fig.2 là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo phương án của sáng chế;

Fig.3A và Fig.3B là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo Phương án 1 của sáng chế;

Fig.4A và Fig.4B là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo Phương án 2 của sáng chế;

Fig.5A và Fig.5B là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo Phương án 3 của sáng chế;

Fig.6A và Fig.6B là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo Phương án 4 của sáng chế;

Fig.7 là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo Phương án 5 của sáng chế;

Fig.8 là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo Phương án 6 của sáng chế;

Fig.9 là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ khác theo Phương án 6 của sáng chế;

Fig.10 là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ khác nữa theo Phương án 6 của sáng chế;

Fig.11 là sơ đồ cấu trúc sơ lược của thiết bị phát hiện được áp dụng cho phần tử mạng điều khiển theo phương án của sáng chế;

Fig.12 là sơ đồ cấu trúc sơ lược của phần tử mạng điều khiển theo phương án của sáng chế;

Fig.13 là sơ đồ cấu trúc sơ lược của thiết bị phát hiện được áp dụng cho phần tử mạng chức năng thứ nhất theo phương án của sáng chế;

Fig.14 là sơ đồ cấu trúc sơ lược của phần tử mạng chức năng thứ nhất theo phương án của sáng chế;

Fig.15 là sơ đồ cấu trúc sơ lược của thiết bị phát hiện được áp dụng cho phần tử mạng chức năng thứ hai theo phương án của sáng chế; và

Fig.16 là sơ đồ cấu trúc sơ lược của phần tử mạng chức năng thứ hai theo phương án của sáng chế.

Mô tả chi tiết sáng chế

Phần dưới đây mô tả các giải pháp kỹ thuật của các phương án theo sáng chế dựa vào các hình vẽ kèm theo.

Phương pháp đăng ký được đề xuất theo các phương án của sáng chế có thể được sử dụng cho kiến trúc dựa trên dịch vụ được thể hiện trên Fig.1. Trên Fig.1, trong kiến trúc dựa trên dịch vụ trên mặt phẳng điều khiển mạng lõi, việc chia tách và tích hợp giữa các NF được thực hiện nhờ môđun hóa, và các NF sử dụng các giao diện dựa trên dịch vụ để tương tác. Ví dụ, trên Fig.1, các NF như chức năng bộc lộ mạng (network exposure

function, NEF), NRF, chức năng điều khiển chính sách (policy control function, PCF), quản lý dữ liệu thống nhất (unified data management, UDM), chức năng ứng dụng (application function, AF), chức năng máy chủ xác thực (authentication server function, AUSF), chức năng quản lý truy cập và di động (access and mobility management function, AMF), và chức năng quản lý phiên (session management function, SMF) có thể tương tác nhờ sử dụng các giao diện dựa trên dịch vụ như giao diện dựa trên dịch vụ được đưa ra bởi NEF (service-based interface exhibited by NEF, Nnef), giao diện dựa trên dịch vụ được đưa ra bởi AUSF (service-based interface exhibited by AUSF, Nausf), giao diện dựa trên dịch vụ được đưa ra bởi NRF (service-based interface exhibited by NRF, Nnrf), giao diện dựa trên dịch vụ được đưa ra bởi AMF (service-based interface exhibited by AMF, Namf), giao diện dựa trên dịch vụ được đưa ra bởi PCF (service-based interface exhibited by PCF, Npcf), giao diện dựa trên dịch vụ được đưa ra bởi SMF (service-based interface exhibited by SMF, Nsmf), giao diện dựa trên dịch vụ được đưa ra bởi UDM (service-based interface exhibited by UDM, Nudm), và giao diện dựa trên dịch vụ được đưa ra bởi AF (service-based interface exhibited by AF, Naf), và cùng dịch vụ có thể được gọi bởi nhiều NF. Điều này làm giảm bớt việc ghép các định nghĩa giao diện giữa các NF, và các NF có thể được tùy biến theo nhu cầu. Theo Fig.1, thiết bị người dùng (user equipment, UE) có thể truy cập AMF trong mạng lõi nhờ sử dụng mạng truy cập vô tuyến (Radio Access Network, RAN), hoặc có thể truy cập trực tiếp AMF này. Giao diện giữa UE và AMF là giao diện N1, và giao diện giữa RAN và AMF là giao diện N2. RAN có thể tương tác với chức năng mặt phẳng người dùng (user plane function, UPF) nhờ sử dụng giao diện N3. UPF có thể truy cập SMF trong mạng lõi nhờ sử dụng giao diện N4, và tương tác với mạng lõi này. UPF có thể còn truy cập mạng dữ liệu (data network, DN) nhờ sử dụng giao diện N6, và tương tác với DN này.

Các tên của phần tử mạng và các định nghĩa giao diện được thể hiện trên Fig.1 được trích từ các định nghĩa trong dự thảo dự án đối tác thế hệ thứ 3 (3rd Generation Partnership Project, 3GPP) và thế hệ thứ năm (5G). Hình vẽ này chỉ thể hiện tóm lược các định nghĩa giao diện giữa các thực thể chức năng mạng. Trên hình vẽ này, khối biểu

diễn định nghĩa NF cụ thể, và đường nối biểu diễn định nghĩa giao diện. Đối với các định nghĩa cụ thể, xem các định nghĩa có liên quan trong dự thảo 5G 3GPP.

Trong kiến trúc dựa trên dịch vụ nêu trên, phần tử mạng điều khiển có chức năng điều khiển phần tử mạng, như NRF, có thể thực hiện chức năng phát hiện và xác thực phần tử mạng chức năng như NF chẳng hạn. Ở giai đoạn phát hiện dịch vụ dựa vào kiến trúc dựa trên dịch vụ, nếu phần tử mạng chức năng có yêu cầu dịch vụ, và yêu cầu dịch vụ này, ví dụ, có thể là yêu cầu truy cập phần tử mạng chức năng khác hoặc có thể là yêu cầu đòi hỏi thu được dịch vụ, phần tử mạng chức năng có yêu cầu dịch vụ có thể gửi yêu cầu phát hiện đến phần tử mạng điều khiển. Sau khi nhận yêu cầu phát hiện này, phần tử mạng điều khiển có thể thực hiện chức năng phát hiện phần tử mạng chức năng, xác định phần tử mạng chức năng thỏa mãn yêu cầu dịch vụ này, và gửi địa chỉ truy cập hoặc mã định danh của phần tử mạng chức năng thỏa mãn yêu cầu dịch vụ đến phần tử mạng chức năng đã gửi yêu cầu phát hiện. Phần tử mạng chức năng gửi yêu cầu phát hiện có thể truy cập, dựa vào địa chỉ truy cập hoặc mã định danh, phần tử mạng chức năng được xác định bởi phần tử mạng điều khiển.

Có thể hiểu rằng trong khi thực hiện phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ nêu trên, phần tử mạng quản lý có thể quản lý và điều khiển phần tử mạng chức năng.

Trong các phương án của sáng chế, để dễ mô tả, phần tử mạng chức năng có yêu cầu dịch vụ được gọi là phần tử mạng chức năng thứ nhất, và phần tử mạng chức năng thỏa mãn yêu cầu dịch vụ của phần tử mạng chức năng thứ nhất được gọi là phần tử mạng chức năng thứ hai.

Phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai theo các phương án của sáng chế có thể được hiểu là các thực thể có chức năng cụ thể. Ví dụ, phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai có thể là các NF, hoặc có thể là các thực thể như các thiết bị đầu cuối, trạm cơ sở, bộ điều khiển hoặc máy chủ. Điều này không bị giới hạn ở các phương án của sáng chế. Để dễ mô tả, phần mô tả sau đây sử dụng ví dụ trong đó phần tử mạng chức năng là NF. Phần tử mạng điều

khiển theo các phương án của sáng chế có thể được hiểu là thực thể chức năng mà sở hữu thông tin đăng ký được lưu trữ và điều khiển phần tử mạng. Ví dụ, phần tử mạng điều khiển này có thể là NRF, hoặc có thể là thực thể như thiết bị đầu cuối, trạm cơ sở, bộ điều khiển hoặc máy chủ. Điều này không bị giới hạn ở các phương án của sáng chế. Để dễ mô tả, phần mô tả sau đây sử dụng ví dụ trong đó phần tử mạng điều khiển là NRF. Phần tử mạng quản lý trong các phương án của sáng chế có thể là thực thể chức năng có chức năng quản lý và điều khiển phần tử mạng. Ví dụ, phần tử mạng quản lý có thể là thực thể như phần tử mạng điều hành, quản trị và bảo trì (operation administration and maintenance, OAM) hoặc phần tử mạng quản lý lát (bộ quản lý lát - Slice manager), hoặc có thể là thực thể như thiết bị đầu cuối, trạm cơ sở, bộ điều khiển hoặc máy chủ. Điều này không bị giới hạn ở các phương án của sáng chế. Để dễ mô tả, phần mô tả sau đây sử dụng ví dụ trong đó phần tử mạng quản lý là OAM.

Trong quy trình nêu trên để phát hiện NF thứ hai dựa vào kiến trúc dựa trên dịch vụ, để bảo đảm sự truyền thông bảo mật giữa NF thứ nhất và NF thứ hai, NRF thường tạo ra khóa bảo mật, và gửi khóa bảo mật này đến NF thứ nhất và NF thứ hai; và NF thứ nhất và NF thứ hai thực hiện việc xác thực bảo mật dựa vào khóa bảo mật này. Tuy nhiên, với phương pháp này, NRF cần phải truyền thông với NF thứ hai, thực hiện việc xác thực bảo mật được thực hiện giữa NF thứ nhất và NF thứ hai dựa vào khóa bảo mật này. Việc này dẫn đến độ phức tạp truyền thông tương đối cao.

Xét vấn đề này, các phương án của sáng chế đề xuất phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ. Trong phương pháp này, NRF tạo ra thông số bảo mật và gửi thông số bảo mật này đến NF thứ nhất, việc xác thực bảo mật được thực hiện giữa NF thứ nhất và NF thứ hai dựa vào thông số bảo mật này, và NF thứ hai không cần tương tác với NRF. Điều này làm giảm bớt số lần truyền thông giữa NF và NRF trong quy trình phát hiện ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Fig.2 là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo phương án của sáng chế. Theo Fig.2, phương pháp bao gồm các bước sau.

S101: NF thứ nhất gửi yêu cầu phát hiện đến NRF.

Trong phương án này của sáng chế, khi xác định rằng NF thứ nhất cần truy cập NF khác hoặc cần yêu cầu thực hiện dịch vụ, NF thứ nhất gửi yêu cầu phát hiện đến NRF. Khi NF thứ nhất xác định rằng NF thứ nhất cần truy cập NF khác, yêu cầu phát hiện được gửi bởi NF thứ nhất đến NRF có thể bao gồm thông tin loại NF mà NF thứ nhất cần truy cập. Khi NF thứ nhất xác định rằng NF thứ nhất cần yêu cầu thực hiện dịch vụ cụ thể, yêu cầu phát hiện được gửi bởi NF thứ nhất đến NRF có thể bao gồm thông tin như thông số của dịch vụ được yêu cầu bởi NF thứ nhất.

S102: NRF nhận yêu cầu phát hiện được gửi bởi NF thứ nhất, và xác định thông số bảo mật và địa chỉ truy cập hoặc mã định danh của NF thứ hai dựa vào yêu cầu phát hiện.

Cụ thể, sau khi nhận yêu cầu phát hiện được gửi bởi NF thứ nhất, NRF có thể xác định, dựa vào thông tin có trong yêu cầu phát hiện chẳng hạn như thông tin loại NF và thông số dịch vụ, NF thỏa mãn yêu cầu dịch vụ. Trong phương án này của sáng chế, giả sử rằng NF thứ hai là NF mà NF thứ nhất cần truy cập, hoặc có thể cung cấp dịch vụ được yêu cầu bởi NF thứ nhất, cho NF thứ nhất. Sau khi xác định NF thứ hai thỏa mãn yêu cầu dịch vụ, NRF có thể xác định thông tin thông số của NF thứ hai chẳng hạn như địa chỉ truy cập của NF thứ hai hoặc mã định danh của NF thứ hai.

Trong phương án này của sáng chế, sau khi xác định địa chỉ truy cập hoặc mã định danh của NF thứ hai, NRF có thể tạo ra thông số bảo mật dựa vào thông tin thông số dịch vụ của dịch vụ được yêu cầu bởi NF thứ nhất và thông tin thông số của NF thứ hai. Thông số bảo mật này được sử dụng cho việc xác thực bảo mật giữa NF thứ nhất và NF thứ hai.

Ngoài ra, trong phương án này của sáng chế, sau khi nhận yêu cầu phát hiện được gửi bởi NF thứ nhất, NRF có thể thực hiện việc xác thực bảo mật đối với yêu cầu phát

hiện được gửi bởi NF thứ nhất, và khi xác định rằng yêu cầu phát hiện được gửi bởi NF thứ nhất là hợp lệ, thì thực hiện quy trình xác định địa chỉ truy cập hoặc mã định danh của NF thứ hai và tạo ra thông số bảo mật, nâng cao sự bảo mật của quy trình phát hiện này.

S103: NRF gửi phản hồi phát hiện đến NF thứ nhất, trong đó phản hồi phát hiện này bao gồm thông số bảo mật và địa chỉ truy cập hoặc mã định danh của NF thứ hai.

S104: NF thứ nhất gửi yêu cầu truy cập đến NF thứ hai dựa vào địa chỉ truy cập hoặc mã định danh của NF thứ hai được gửi bởi NRF, trong đó yêu cầu truy cập này bao gồm thông số bảo mật.

S105: NF thứ hai nhận yêu cầu truy cập được gửi bởi NF thứ nhất, xác minh tính chính xác của thông số bảo mật có trong yêu cầu truy cập, và xác định, dựa vào tính chính xác của thông số bảo mật, xem có cho phép NF thứ nhất truy cập NF thứ hai hay không.

Trong phương án này của sáng chế, NF thứ hai cho phép NF thứ nhất truy cập NF thứ hai, khi xác định rằng thông số bảo mật được gửi bởi NF thứ nhất là đúng, và có thể từ chối cho phép NF thứ nhất truy cập NF thứ hai, khi xác định rằng thông số bảo mật được gửi bởi NF thứ nhất là không đúng.

Trong phương án này của sáng chế, NRF tạo ra thông số bảo mật và gửi thông số bảo mật này đến NF thứ nhất, việc xác thực bảo mật được thực hiện giữa NF thứ nhất và NF thứ hai dựa vào thông số bảo mật, và NF thứ hai không cần tương tác với NRF. Điều này làm giảm bớt số lần truyền thông giữa NF và NRF trong quy trình phát hiện ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Trong các phương án của sáng chế, quy trình tạo ra và xác minh thông số bảo mật và quy trình thực hiện việc phát hiện có dựa vào các thông số bảo mật khác nhau được mô tả dưới đây có dựa vào các phương án cụ thể.

Trong phương án của sáng chế, NF thứ nhất cần yêu cầu dịch vụ và NF thứ hai có khả năng cung cấp dịch vụ này cho NF thứ nhất được sử dụng làm ví dụ để mô tả, và quy trình thực hiện để NF thứ nhất yêu cầu truy cập NF thứ hai là tương tự như vậy. Các chi tiết không được mô tả lại dưới đây.

Phương án 1

Fig.3A và Fig.3B là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo Phương án 1 của sáng chế. Theo Fig.3A và Fig.3B, phương pháp này bao gồm các bước sau.

S201: NF thứ nhất xác định rằng dịch vụ cần được yêu cầu, trong đó dịch vụ này có thể được xác định nhờ sử dụng thông số dịch vụ, và thông số dịch vụ này có thể là mã nhận dạng dịch vụ (service ID) chẳng hạn. Trong phương án dưới đây, thông số dịch vụ là ID dịch vụ được sử dụng làm ví dụ để mô tả, và quy trình thực hiện đối với thông số dịch vụ khác là tương tự như vậy. Các chi tiết không được mô tả lại dưới đây.

S202: NF thứ nhất gửi yêu cầu phát hiện đến NRF, trong đó yêu cầu phát hiện này có thể bao gồm thông tin như mã định danh của NF thứ nhất (ID_NF1) và ID dịch vụ của dịch vụ được yêu cầu bởi NF thứ nhất, và có thể còn có thông tin về loại của NF thứ hai (NF2 type) và thông tin tương tự.

Yêu cầu phát hiện trong phương án này của sáng chế có thể bao gồm các ID dịch vụ của các dịch vụ.

Ngoài ra, theo cách khác, yêu cầu phát hiện trong phương án này của sáng chế có thể không bao gồm ID dịch vụ. Nếu yêu cầu phát hiện không bao gồm ID dịch vụ, NRF có thể xác định ID dịch vụ dựa vào thông số dịch vụ được gửi bởi NF thứ nhất.

S203: NRF nhận yêu cầu phát hiện được gửi bởi NF thứ nhất, và xác định địa chỉ truy cập hoặc mã định danh của NF thứ hai (ID_NF2) và thông số bảo mật.

NRF có thể xác định NF thứ hai dựa vào ID dịch vụ có trong yêu cầu phát hiện, để xác định thêm ID_NF2.

Cụ thể, nếu yêu cầu phát hiện bao gồm loại NF2, NF thứ hai có thể được xác định dựa vào loại NF2 này, hoặc ID_NF2 có thể được xác định dựa vào ID dịch vụ và loại NF2. Tất nhiên, nếu yêu cầu phát hiện trong phương án này của sáng chế chỉ bao gồm loại NF2, theo cách khác NRF có thể xác định NF thứ hai dựa vào loại NF2.

Trong phương án này của sáng chế, sau khi nhận yêu cầu phát hiện được gửi bởi NF thứ nhất và xác định ID_NF2, NRF có thể tạo ra K_session dựa vào ID dịch vụ, ID_NF1, ID_NF2 và dạng tương tự. K_session được tạo ra có thể được sử dụng để bảo vệ toàn bộ dữ liệu được sử dụng cho việc truyền thông giữa NF thứ nhất và NF thứ hai.

Trong phương án này của sáng chế, để dễ mô tả, K_session được tạo ra bởi NRF và được sử dụng để bảo vệ toàn bộ dữ liệu được sử dụng cho việc truyền thông giữa NF thứ nhất và NF thứ hai được gọi là K_session thứ nhất.

Trong phương án này của sáng chế, K_session thứ nhất có thể được tạo ra bởi NRF. K_session thứ nhất này có thể được lựa chọn ngẫu nhiên bởi NRF. Theo cách khác, K_session thứ nhất có thể được dẫn xuất bởi NRF dựa vào khóa dẫn xuất. Ngoài ra, trong khi tạo ra K_session thứ nhất bởi NRF, giá trị tham số mà phép tạo dẫn xuất được thực hiện đối với giá trị tham số này bao gồm một hoặc nhiều giá trị trong số ID_NF1, ID_NF2, địa chỉ của NF2, mã định danh của NRF (ID_NRF), mã nhận dạng mạng di động mặt đất công cộng (Public Land Mobile Network ID, PLMN ID) của NF thứ nhất, PLMN ID của NF thứ hai, ID dịch vụ và giá trị tương tự. Ngoài giá trị tham số nêu trên, NRF có thể còn thực hiện phép tạo dẫn xuất đối với ít nhất một giá trị trong số chu kỳ (thời gian) hợp lệ K_session thứ nhất, giá trị nonce K_session thứ nhất (nonce_session), giá trị đếm, và số chuỗi, để tạo ra K_session thứ nhất. Chu kỳ hợp lệ của K_session thứ nhất có thể bao gồm thời gian bắt đầu và thời gian kết thúc, hoặc thời gian bắt đầu và thời gian hợp lệ, hoặc thời gian kết thúc. Giá trị nonce K_session thứ nhất có thể được lựa chọn ngẫu nhiên bởi NRF.

Cụ thể, nếu NF thứ nhất yêu cầu nhiều dịch vụ, trong quy trình tạo ra K_session thứ nhất, K_session thứ nhất này có thể được tạo ra dựa vào nhiều ID dịch vụ.

Khóa dẫn xuất được sử dụng để tạo ra K_session thứ nhất có thể thu được bởi NRF nhờ thực hiện phép tạo dẫn xuất khóa đối với khóa gốc được thiết lập trước, hoặc khóa dẫn xuất có thể là khóa được lưu bởi NRF.

Trong phương án này của sáng chế, NRF có thể tạo ra thẻ (token) dựa vào K_session thứ nhất, và sử dụng token được tạo ra dựa vào K_session thứ nhất và K_session thứ nhất làm thông số bảo mật được sử dụng cho việc xác thực bảo mật giữa NF thứ nhất và NF thứ hai.

Trong phương án này của sáng chế, để dễ mô tả, token được tạo ra dựa vào K_session thứ nhất được gọi là token thứ nhất.

Trong phương án này của sáng chế, theo phương án thực hiện khả thi, token thứ nhất có thể là token thứ nhất bất đối xứng, và token thứ nhất bất đối xứng này có thể được tạo ra bởi NRF dựa vào khóa công khai của NF thứ hai (PKNF2). NRF tạo ra token thứ nhất bất đối xứng dựa vào PKNF2, và trên NRF, PKNF2, khóa công khai của NRF (PKnrf), và khóa bí mật của NRF (SKnrf) cần được lưu trước. PKNF2 có thể được thiết lập trước từ đầu trên NRF, hoặc có thể được gửi bởi NF thứ hai đến NRF trong quá trình tương tác giữa NF thứ hai và NRF. NF2 cũng cần lưu trước PKnrf, PKNF2, và khóa bí mật của NF thứ hai (SKNF2). PKnrf có thể được thiết lập trước từ đầu trên NF thứ hai, hoặc có thể được gửi bởi NRF đến NRF trong quá trình tương tác giữa NF thứ hai và NRF.

Cụ thể, NRF có thể mật hóa chữ ký số (Chữ ký), ID_NF1, ID_NF2, và K_session thứ nhất dựa vào PKNF2 này. Chữ ký số có thể được tạo ra bởi NRF nhờ thực hiện thuật toán chữ ký số đối với ID_NF1 và K_session thứ nhất dựa vào SKnrf.

Ngoài ra, trong phương án này của sáng chế, ngoài các giá trị tham số nêu trên được mật hóa dựa vào PKNF2, NRF có thể còn mật hóa một hoặc nhiều thông tin trong số ID_NRF, PLMN ID của NF thứ nhất, PLMN ID của NF thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi NF thứ nhất. NRF có thể còn thực hiện thuật toán chữ ký đối với ít nhất một giá trị trong số chu kỳ (thời gian) hợp lệ của token thứ nhất bất đối xứng, giá trị nonce của token (nonce_token) thứ nhất bất đối xứng, giá trị đếm

và số chuỗi. Một cách tương tự, chữ ký số cũng có thể được tạo ra bởi NRF dựa vào SKnrf nhờ thực hiện thuật toán chữ ký số đối với một hoặc nhiều thông tin trong số ID_NRF, PLMN ID của NF thứ nhất, PLMN ID của NF thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi NF thứ nhất, ngoài các giá trị tham số nêu trên. NRF có thể còn thực hiện thuật toán chữ ký đối với ít nhất một giá trị trong số chu kỳ (thời gian) hợp lệ của chữ ký, giá trị nonce của chữ ký (nonce_sign), giá trị đếm, và số chuỗi.

Chu kỳ hợp lệ của token thứ nhất và chu kỳ hợp lệ của chữ ký có thể bao gồm thời gian bắt đầu và thời gian kết thúc, hoặc thời gian bắt đầu và thời gian hợp lệ, hoặc thời gian kết thúc. Giá trị nonce của token thứ nhất bất đối xứng và giá trị nonce của chữ ký có thể được lựa chọn ngẫu nhiên bởi NRF. Giá trị nonce của token thứ nhất bất đối xứng và giá trị nonce của chữ ký có thể giống nhau hoặc có thể khác nhau.

Theo phương án thực hiện khả thi khác, token thứ nhất có thể là token thứ nhất đối xứng. Token thứ nhất đối xứng này có thể được tạo ra bởi NRF dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai. Khi NRF tạo ra token thứ nhất đối xứng dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai, NRF và NF thứ hai cần lưu trước khóa đối xứng được chia sẻ.

Cụ thể, token thứ nhất đối xứng có thể được tạo ra bởi NRF nhờ mật hóa mã xác thực thông điệp (message Authentication code, MAC), ID_NF1, ID_NF2, và K_session thứ nhất dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai. MAC được tạo ra bởi NRF nhờ thực hiện thuật toán mã xác thực thông điệp đối với ID_NF1 và K_session thứ nhất dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai.

Ngoài ra, trong phương án này của sáng chế, ngoài các giá trị tham số nêu trên được mật hóa dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai, NRF có thể còn mật hóa một hoặc nhiều thông tin trong số ID_NRF, PLMN ID của NF thứ nhất, PLMN ID của NF thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi NF thứ nhất. NRF có thể còn thực hiện thuật toán mã xác thực thông điệp đối với ít nhất một giá trị trong số chu kỳ (thời gian) hợp lệ token thứ nhất đối xứng, giá trị nonce của token thứ nhất đối xứng (nonce_token), giá trị đếm và số chuỗi. Một cách tương tự,

MAC có thể còn được tạo ra bởi NRF dựa vào SKnrf nhờ thực hiện thuật toán mã xác thực thông điệp đối với một hoặc nhiều thông tin trong số ID_NRF, PLMN ID của NF thứ nhất, PLMN ID của NF thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi NF thứ nhất, ngoài các giá trị tham số nêu trên. NRF có thể còn thực hiện thuật toán mã xác thực thông điệp đối với ít nhất một giá trị trong số chu kỳ (thời gian) hợp lệ của MAC, giá trị nonce của MAC (nonce_mac), giá trị đếm và số chuỗi.

Chu kỳ hợp lệ của token thứ nhất và chu kỳ hợp lệ của MAC có thể bao gồm thời gian bắt đầu và thời gian kết thúc, hoặc thời gian bắt đầu và thời gian hợp lệ, hoặc thời gian kết thúc. Giá trị nonce của token thứ nhất đối xứng và giá trị nonce của MAC có thể được lựa chọn ngẫu nhiên bởi NRF. Giá trị nonce của token thứ nhất đối xứng và giá trị nonce của MAC có thể giống nhau hoặc có thể khác nhau.

S204: NRF gửi phản hồi phát hiện đến NF thứ nhất, trong đó phản hồi phát hiện này bao gồm K_session thứ nhất và token thứ nhất, và còn bao gồm ít nhất một thông tin trong số ID_NF2 và địa chỉ của NF2.

S205: NF thứ nhất nhận phản hồi phát hiện được gửi bởi NRF, và gửi yêu cầu truy cập đến NF thứ hai dựa vào ID_NF2 hoặc địa chỉ của NF2, trong đó yêu cầu truy cập này bao gồm ID_NF1 và token thứ nhất.

S206: NF thứ hai nhận yêu cầu truy cập được gửi bởi NF thứ nhất, và xác minh tính chính xác của token thứ nhất có trong yêu cầu truy cập này.

Trong phương án này của sáng chế, nếu token thứ nhất là token thứ nhất bất đối xứng được tạo ra dựa vào PKNF2, NF thứ hai giải mật token thứ nhất nhờ sử dụng SKNF2, để thu được chữ ký số, và xác minh tính chính xác của chữ ký số nhờ sử dụng PKnrf và nội dung được ký. Nội dung được ký này bao gồm các giá trị tham số mà trên đó thuật toán chữ ký số được thực hiện trong khi tạo ra token thứ nhất. Nếu xác minh rằng chữ ký số là đúng, NF thứ hai xác định rằng yêu cầu truy cập được gửi bởi NF thứ nhất được cấp quyền bởi NRF, và NF thứ nhất được phép truy cập NF thứ hai. Nếu xác minh rằng chữ ký số là không đúng, NF thứ hai xác định rằng yêu cầu truy cập được gửi

bởi NF thứ nhất không được cấp quyền bởi NRF, và NF thứ nhất không được phép truy cập NF thứ hai.

Trong phương án này của sáng chế, nếu token thứ nhất là token thứ nhất đối xứng được tạo ra dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai, NF thứ hai giải mật token thứ nhất nhờ sử dụng khóa đối xứng được chia sẻ giữa NRF và NF thứ hai, để thu được MAC, và xác minh tính chính xác của MAC này nhờ sử dụng khóa đối xứng được chia sẻ giữa NRF và NF thứ hai và nội dung được bảo vệ bởi MAC. Nội dung được bảo vệ bởi MAC này bao gồm các giá trị tham số mà trên đó thuật toán mã xác thực thông điệp được thực hiện trong khi tạo ra token thứ nhất. Nếu xác minh rằng MAC là đúng, NF thứ hai xác định rằng yêu cầu truy cập được gửi bởi NF thứ nhất được cấp quyền bởi NRF, và NF thứ nhất được phép truy cập NF thứ hai. Nếu xác minh rằng MAC là không đúng, NF thứ hai xác định rằng yêu cầu truy cập được gửi bởi NF thứ nhất không được cấp quyền bởi NRF, và NF thứ nhất không được phép truy cập NF thứ hai.

Ngoài ra, trong phương án này của sáng chế, NF thứ hai giải mật token thứ nhất để thu thêm K_session thứ nhất, và NF thứ hai và NF thứ nhất có thể chia sẻ K_session thứ nhất. NF thứ hai có thể sử dụng K_session thứ nhất để thực hiện bước S207 dưới đây. Bước S207 là tùy chọn.

S207: Khi xác định rằng yêu cầu truy cập được gửi bởi NF thứ nhất được cấp quyền bởi NRF, NF thứ hai thiết lập kênh bảo mật với NF thứ nhất dựa vào K_session thứ nhất hoặc khóa được dẫn xuất từ K_session thứ nhất.

Khóa được dẫn xuất từ K_session thứ nhất có thể thu được bằng cách thực hiện thuật toán tạo dẫn xuất khóa đối với ít nhất một giá trị trong số K_session thứ nhất, giá trị đếm thiết lập đường hầm và mã định danh phiên.

Ngoài ra, phương án này của sáng chế có thể còn có bước S208 dưới đây. Bước S208 là tùy chọn.

S208: NF thứ hai có thể gửi phản hồi truy cập đến NF thứ nhất, để thông báo NF thứ nhất về việc NF thứ nhất có truy cập thành công NF thứ hai hay không.

Trong phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ được đề xuất theo phương án 1 của sáng chế, NRF tạo ra token thứ nhất và K_session thứ nhất được sử dụng để bảo vệ toàn bộ dữ liệu được sử dụng cho việc truyền thông giữa NF thứ nhất và NF thứ hai. Điều này có thể thực hiện được việc bảo vệ bảo mật dựa trên kết nối, và thực hiện việc xác thực bảo mật đối với thông số bảo mật giữa NF thứ nhất và NF thứ hai khi NRF không trao đổi thông số bảo mật với NF thứ hai. Điều này làm giảm bớt số lần truyền thông giữa NF và NRF ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Phương án 2

Fig.4A và Fig.4B là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo Phương án 2 của sáng chế. Theo Fig.4A và Fig.4B, các bước S301 và S302 là giống như các bước S201 và S202 theo phương án 1. Các chi tiết không được mô tả lại dưới đây. Chỉ các phần khác nhau là được mô tả dưới đây.

S303: NRF nhận yêu cầu phát hiện được gửi bởi NF thứ nhất, xác định địa chỉ truy cập hoặc mã định danh của NF thứ hai (ID_NF2), và xác định thông số bảo mật.

Quy trình thực hiện để NRF xác định ID_NF2 là tương tự như trong phương án nêu trên. Các chi tiết không được mô tả lại dưới đây.

Trong phương án này của sáng chế, khi xác định K_session được chia sẻ giữa NF thứ nhất và NF thứ hai, NRF có thể tạo ra K_session riêng biệt cho các dịch vụ được yêu cầu bởi NF thứ nhất. Có thể hiểu rằng có mối hệ tương ứng một-một giữa mỗi dịch vụ và K_session, và mỗi K_session bảo vệ dịch vụ tương ứng với K_session này.

Trong phương án này của sáng chế, để dễ mô tả, mỗi K_session bảo vệ từng dịch vụ được yêu cầu bởi NF thứ nhất được gọi là K_session thứ hai.

Trong phương án này của sáng chế, NRF có thể tạo ra, dựa vào ID dịch vụ của dịch vụ được yêu cầu bởi NF thứ nhất, K_session thứ hai tương ứng với từng dịch vụ.

Cụ thể, các quy trình tạo ra các K_session thứ hai là tương tự, và chỉ các ID dịch vụ được sử dụng là khác nhau. Mỗi K_session có thể được tạo ra theo cách sau:

K_session thứ hai có thể được tạo ra bởi NRF. K_session thứ hai có thể được lựa chọn ngẫu nhiên bởi NRF. Theo cách khác, K_session thứ hai có thể được tạo ra bởi NRF nhờ thực hiện phép tạo dẫn xuất, dựa vào khóa dẫn xuất, đối với ít nhất một giá trị trong số ID_NF1, ID_NF2, và ID dịch vụ của dịch vụ được bảo vệ bởi K_session thứ hai. Khóa dẫn xuất được sử dụng để tạo ra K_session thứ hai có thể thu được bởi NRF nhờ thực hiện phép tạo dẫn xuất khóa đối với khóa gốc được thiết lập trước, hoặc khóa dẫn xuất có thể là khóa được lưu bởi NRF.

Ví dụ, giả sử rằng các dịch vụ được yêu cầu bởi NF thứ nhất bao gồm dịch vụ 1 và dịch vụ 2, mã định danh của dịch vụ 1 là ID dịch vụ 1, và mã định danh của dịch vụ 2 là ID dịch vụ 2. Trong phương án này của sáng chế, K_session thứ hai 1 và K_session thứ hai 2 có thể được tạo ra. K_session thứ hai 1 được tạo ra dựa vào ID dịch vụ 1 và bảo vệ dịch vụ 1. K_session thứ hai 2 được tạo ra dựa vào ID dịch vụ 2 và bảo vệ dịch vụ 2.

Ngoài ra, trong phương án này của sáng chế, NRF có thể tạo ra, dựa vào từng K_session thứ hai được tạo ra, token tương ứng với từng K_session thứ hai.

Trong phương án này của sáng chế, để dễ mô tả, token được tạo ra dựa vào từng K_session thứ hai và tương ứng với từng K_session thứ hai được gọi là token thứ hai.

Cụ thể, NRF có thể tạo ra token thứ hai tương ứng với từng K_session thứ hai, dựa vào từng K_session thứ hai và ID dịch vụ của dịch vụ được bảo vệ bởi K_session thứ hai này. Các quy trình tạo ra các token thứ hai là tương tự, và chỉ các K_session thứ hai được sử dụng và các ID dịch vụ của các dịch vụ được bảo vệ bởi các K_session thứ hai này là khác nhau. Ví dụ, vẫn giả sử rằng các dịch vụ được yêu cầu bởi NF thứ nhất bao gồm dịch vụ 1 và dịch vụ 2, mã định danh của dịch vụ 1 là ID dịch vụ 1, mã định danh của dịch vụ 2 là ID dịch vụ 2, K_session thứ hai 1 được tạo ra dựa vào ID dịch vụ 1 và bảo vệ dịch vụ 1 này, và K_session thứ hai 2 được tạo ra dựa vào ID dịch vụ 2 và bảo vệ dịch vụ 2 này. Do đó, trong phương án này của sáng chế, token thứ hai 1 có thể

được tạo ra dựa vào ID dịch vụ 1 và K_session thứ hai 1, và token thứ hai 2 được tạo ra dựa vào ID dịch vụ 2 và K_session thứ hai 2.

Ngoài ra, trong phương án này của sáng chế, token thứ hai có thể là token thứ hai đối xứng, hoặc có thể là token thứ hai bất đối xứng.

Theo phương án khả thi, NRF có thể mật hóa chữ ký số, ID_NF1, ID_NF2, ID dịch vụ của dịch vụ được bảo vệ bởi K_session thứ hai, và K_session thứ hai dựa vào PKNF2, để tạo ra token thứ hai bất đối xứng. Chữ ký số được tạo ra bởi NRF nhờ thực hiện thuật toán chữ ký số đối với ID_NF1 và K_session thứ hai dựa vào khóa bí mật của NRF.

Theo phương án thực hiện khả thi khác, NRF có thể mật hóa MAC, ID_NF1, ID_NF2, ID dịch vụ của dịch vụ được bảo vệ bởi K_session thứ hai, và K_session thứ hai dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai, để tạo ra token thứ hai đối xứng. MAC được tạo ra bởi NRF nhờ thực hiện thuật toán mã xác thực thông điệp đối với ID_NF1 và K_session thứ hai dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai.

Trong phương án này của sáng chế, đối với token thứ hai đối xứng hoặc token thứ hai bất đối xứng được tạo ra cho từng K_session thứ hai, phương án thực hiện tương tự phương án thực hiện tạo ra token thứ nhất đối xứng hoặc token thứ nhất bất đối xứng theo phương án 1 có thể được sử dụng, và điểm khác biệt nằm ở chỗ quá trình tạo ra ở đây cần được thực hiện dựa vào K_session thứ hai và ID dịch vụ của dịch vụ được bảo vệ bởi K_session thứ hai này. Các giá trị tham số khác có thể tương tự, và do đó các chi tiết không được mô tả lại dưới đây. Chi tiết hơn, xem các phần mô tả theo phương án 1.

S304: NRF gửi phản hồi phát hiện đến NF thứ nhất, trong đó phản hồi phát hiện này bao gồm tất cả các K_session thứ hai và tất cả các token thứ hai, và còn bao gồm ít nhất một giá trị trong số ID_NF2 và địa chỉ của NF2.

S305: NF thứ nhất nhận phản hồi phát hiện được gửi bởi NRF, và gửi yêu cầu truy cập đến NF thứ hai dựa vào ID_NF2 có trong phản hồi phát hiện, trong đó yêu cầu truy cập này bao gồm ID_NF2 và token thứ hai. Ví dụ, nếu dịch vụ được yêu cầu bởi

NF thứ nhất là dịch vụ 1, yêu cầu truy cập có thể bao gồm K_session thứ hai 1 và token thứ hai 1.

S306: NF thứ hai nhận yêu cầu truy cập được gửi bởi NF thứ nhất, và xác minh tính chính xác của token thứ hai có trong yêu cầu truy cập này.

Trong phương án này của sáng chế, quy trình thực hiện để NF thứ hai xác minh token thứ hai là tương tự việc xác minh token thứ nhất theo phương án 1, và do đó các chi tiết không được mô tả lại dưới đây.

Ngoài ra, trong phương án này của sáng chế, NF thứ hai giải mật token thứ hai để thu thêm K_session thứ hai, và NF thứ hai và NF thứ nhất có thể chia sẻ K_session thứ hai. NF thứ hai có thể sử dụng K_session thứ hai để thực hiện bước S307 dưới đây. Bước S307 là tùy chọn.

S307: Khi xác định rằng yêu cầu truy cập được gửi bởi NF thứ nhất được cấp quyền bởi NRF, NF thứ hai thiết lập, với NF thứ nhất dựa vào K_session thứ hai hoặc khóa được dẫn xuất từ K_session thứ hai, kênh bảo mật cho dịch vụ được bảo vệ bởi K_session thứ hai.

Một cách tương tự, phương án này của sáng chế có thể còn bao gồm bước dưới đây để gửi phản hồi truy cập đến NF thứ nhất:

S308: NF thứ hai gửi phản hồi truy cập đến NF thứ nhất, để thông báo NF thứ nhất về việc NF thứ nhất có truy cập thành công NF thứ hai hay không.

Bước S308 là tùy chọn.

Trong phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ được đề xuất theo phương án 2 của sáng chế, NRF tạo ra K_session thứ hai và token thứ hai đối với từng dịch vụ được yêu cầu bởi NF thứ nhất. Điều này có thể thực hiện việc bảo vệ bảo mật dựa trên dịch vụ, và thực hiện việc xác thực bảo mật đối với thông số bảo mật giữa NF thứ nhất và NF thứ hai khi NRF không trao đổi thông số bảo mật với NF thứ hai. Điều này làm giảm bớt số lần truyền thông giữa NF và NRF ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Theo phương án khả thi khác của sáng chế, NRF có thể tạo ra một token cho tất cả các K_session thứ hai, do đó khi NF thứ nhất yêu cầu nhiều dịch vụ, NRF không cần gửi nhiều token mà chỉ gửi một token đến NF thứ hai. Điều này làm giảm thêm độ phức tạp truyền thông.

Trong phương án này của sáng chế, để dễ mô tả, token được tạo ra dựa vào tất cả các K_session thứ hai có thể được gọi là token thứ ba.

Phương án 3

Fig.5A và Fig.5B là lưu đồ theo phương án thực hiện của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo Phương án 3 của sáng chế. Trên Fig.5A và Fig.5B, các bước S401 và S402 giống các bước S301 và S302 theo phương án 2, và quy trình thực hiện xác định ID_NF2 và tạo ra K_session thứ hai trong bước S303 cũng giống như quy trình xác định ID_NF2 và tạo ra K_session thứ hai theo phương án 2. Do đó, các chi tiết không được mô tả lại dưới đây. Chỉ các phần khác nhau là được mô tả dưới đây.

S403: NRF tạo ra token thứ ba dựa vào các K_session thứ hai được tạo ra.

Trong phương án này của sáng chế, token thứ ba có thể là token thứ ba đối xứng, hoặc có thể là token thứ ba bất đối xứng.

Theo phương án khả thi, trong phương án này của sáng chế, NRF có thể mật hóa chữ ký số, ID_NF1, ID_NF2, và tất cả các K_session thứ hai dựa vào PKNF2, để tạo ra token thứ ba bất đối xứng. Chữ ký số được tạo ra bởi NRF nhờ thực hiện thuật toán chữ ký số đối với ID_NF1 và tất cả các K_session thứ hai dựa vào khóa bí mật của NRF. Theo phương án thực hiện khả thi khác, theo cách khác, NRF có thể mật hóa mã xác thực thông điệp, ID_NF1, ID_NF2, và tất cả các K_session thứ hai dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai, để tạo ra token thứ ba đối xứng. Mã xác thực thông điệp này được tạo ra bởi NRF nhờ thực hiện thuật toán mã xác thực thông điệp đối với ID_NF1 và tất cả các K_session thứ hai dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai. Thông số tính toán của token thứ ba có thể còn bao gồm các ID dịch vụ của tất cả các dịch vụ được bảo vệ bởi tất cả các K_session thứ hai.

Trong phương án này của sáng chế, đối với quy trình tạo ra token thứ ba bất đối xứng hoặc token thứ ba đối xứng, phương án thực hiện tương tự như việc tạo ra token thứ hai đối xứng hoặc token thứ hai bất đối xứng theo phương án 1 có thể được sử dụng, và điểm khác biệt nằm ở chỗ quá trình tạo ra ở đây cần được thực hiện dựa vào các K_session thứ hai và tất cả ID dịch vụ của các dịch vụ được bảo vệ bởi các K_session thứ hai này. Các giá trị tham số khác có thể là tương tự, và do đó các chi tiết không được mô tả lại dưới đây. Chi tiết hơn, xem các phần mô tả theo phương án 1.

S404: NRF gửi phản hồi phát hiện đến NF thứ nhất, trong đó phản hồi phát hiện này bao gồm tất cả các K_session thứ hai và token thứ ba, và còn bao gồm ít nhất một giá trị trong số ID_NF2 và địa chỉ của NF2.

S405: NF thứ nhất nhận phản hồi phát hiện được gửi bởi NRF, và gửi yêu cầu truy cập đến NF thứ hai dựa vào ID_NF2 có trong phản hồi phát hiện này, trong đó yêu cầu truy cập bao gồm ID_NF2 và token thứ ba. Ví dụ, nếu dịch vụ được yêu cầu bởi NF thứ nhất là dịch vụ 1, yêu cầu truy cập có thể bao gồm K_session thứ hai 1 và token thứ ba.

S406: NF thứ hai nhận yêu cầu truy cập được gửi bởi NF thứ nhất, và xác minh tính chính xác của token thứ ba có trong yêu cầu truy cập này.

Trong phương án này của sáng chế, quy trình thực hiện để NF thứ hai xác minh token thứ ba là tương tự như việc xác minh token thứ nhất theo phương án 1, và do đó các chi tiết không được mô tả lại dưới đây.

Bước S407 giống như bước S307, và các chi tiết không được mô tả lại dưới đây. Bước S407 là tùy chọn.

Một cách tương tự, phương án này của sáng chế có thể còn bao gồm bước gửi phản hồi truy cập đến NF thứ nhất:

S408: NF thứ hai gửi phản hồi truy cập đến NF thứ nhất, để thông báo NF thứ nhất về việc NF thứ nhất có truy cập thành công NF thứ hai hay không.

Bước S408 là tùy chọn.

Trong phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ được đề xuất theo Phương án 3 của sáng chế, NRF tạo ra K_session thứ hai đối với từng dịch vụ được yêu cầu bởi NF thứ nhất, và bổ sung tất cả các K_session thứ hai vào một token thứ ba. Điều này có thể thực hiện việc bảo vệ bảo mật dựa trên dịch vụ, và việc gửi một token đến NF thứ hai có thể giảm bớt được độ phức tạp truyền thông.

Phương án 4

Fig.6A và Fig.6B thể hiện phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ theo Phương án 4 của sáng chế. Trên Fig.6A và Fig.6B, các bước S501 và S502 giống các bước S201 và S202 theo phương án 1. Các chi tiết không được mô tả lại dưới đây. Chỉ các phần khác nhau là được mô tả dưới đây.

S503: NRF nhận yêu cầu phát hiện được gửi bởi NF thứ nhất, và xác định ID_NF2 và thông số bảo mật.

Quy trình thực hiện để NRF xác định ID_NF2 là tương tự như trong phương án nêu trên. Các chi tiết không được mô tả lại dưới đây.

Trong phương án này của sáng chế, NRF không cần tạo ra khóa phiên được chia sẻ giữa NF thứ nhất và NF thứ hai, và có thể tạo ra thông số bảo mật riêng biệt được sử dụng để NF thứ hai thực hiện việc xác minh cấp quyền đối với NF thứ nhất.

Trong phương án này của sáng chế, thông số bảo mật được sử dụng để NF thứ hai thực hiện việc xác minh cấp quyền đối với NF thứ nhất có thể là chữ ký số hoặc MAC.

Theo phương án khả thi, thông số bảo mật được sử dụng để NF thứ hai thực hiện việc xác minh cấp quyền đối với NF thứ nhất có thể bao gồm chữ ký số, và chữ ký số này được sử dụng để NF thứ hai thực hiện việc xác minh cấp quyền đối với NF thứ nhất có thể được tạo ra bởi NRF dựa vào SKnrf. Để tạo ra chữ ký số dựa vào SKnrf bởi NRF, thì PKNF2, PKnrf và SKnrf cần được lưu trước trên NRF. PKNF2 có thể được thiết lập trước từ đầu trên NRF, hoặc có thể được gửi bởi NF thứ hai đến NRF trong quá trình tương tác giữa NF thứ hai và NRF. NF thứ hai cũng cần lưu trữ trước PKnrf. PKnrf này

có thể được thiết lập trước từ đầu trên NF thứ hai, hoặc có thể được gửi bởi NRF đến NRF trong quá trình tương tác giữa NF thứ hai và NRF.

Cụ thể, trong phương án này của sáng chế, NRF có thể thực hiện thuật toán chữ ký số đối với ID_NF1 dựa vào SKnrf. Ngoài ra, ngoài việc thực hiện thuật toán chữ ký số đối với ID_NF1, NRF có thể còn thực hiện thuật toán chữ ký số đối với một hoặc nhiều giá trị trong số ID_NRF, PLMN ID của NF thứ nhất, PLMN ID của NF thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi NF thứ nhất. NRF có thể còn thực hiện thuật toán chữ ký đối với ít nhất một giá trị trong số chu kỳ (thời gian) hợp lệ của chữ ký, giá trị nonce của chữ ký (nonce_sign), giá trị đếm và số chuỗi.

Theo phương án thực hiện khả thi khác, thông số bảo mật được sử dụng để NF thứ hai thực hiện việc xác minh cấp quyền đối với NF thứ nhất có thể bao gồm MAC, và MAC được sử dụng để NF thứ hai thực hiện việc xác minh cấp quyền đối với NF thứ nhất có thể được tạo ra bởi NRF dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai. Khi NRF tạo ra MAC dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai, NRF và NF thứ hai cần lưu trước khóa đối xứng được chia sẻ.

Cụ thể, MAC được sử dụng để NF thứ hai thực hiện việc xác minh cấp quyền đối với NF thứ nhất có thể được tạo ra bởi NRF nhờ thực hiện thuật toán mã xác thực thông điệp đối với ID_NF1 dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai.

Ngoài ra, MAC cũng có thể được tạo ra bởi NRF bằng cách thực hiện, dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai, thuật toán mã xác thực thông điệp đối với một hoặc nhiều giá trị trong số ID_NRF, PLMN ID của NF thứ nhất, PLMN ID của NF thứ hai, và mã định danh dịch vụ của dịch vụ được yêu cầu bởi NF thứ nhất, ngoài giá trị tham số nêu trên. NRF có thể còn thực hiện thuật toán mã xác thực thông điệp đối với ít nhất một giá trị trong số chu kỳ (thời gian) hợp lệ của MAC, giá trị nonce của MAC (nonce_mac), giá trị đếm và số chuỗi.

Có thể hiểu rằng chu kỳ hợp lệ của chữ ký và chu kỳ hợp lệ của MAC có thể bao gồm thời gian bắt đầu và thời gian kết thúc, hoặc thời gian bắt đầu và thời gian hợp lệ

hoặc thời gian kết thúc. Giá trị nonce của chữ ký và giá trị nonce của MAC có thể được lựa chọn ngẫu nhiên bởi NRF.

S504: NRF gửi phản hồi phát hiện đến NF thứ nhất, trong đó phản hồi phát hiện này bao gồm chữ ký số hoặc MAC, và còn bao gồm ít nhất một giá trị trong số ID_NF2 và địa chỉ của NF2.

S505: NF thứ nhất nhận phản hồi phát hiện được gửi bởi NRF, và gửi yêu cầu truy cập đến NF thứ hai dựa vào ID_NF2, trong đó yêu cầu truy cập này bao gồm ID_NF1 và chữ ký số, hoặc ID_NF1 và MAC.

Yêu cầu truy cập này có thể còn có giá trị tham số khác. Ví dụ, khi yêu cầu truy cập bao gồm ID_NF1 và chữ ký số, yêu cầu truy cập này có thể còn có ít nhất một giá trị trong số chu kỳ hợp lệ của chữ ký, giá trị nonce của chữ ký, giá trị đếm, và số chuỗi mà thuật toán chữ ký số được thực hiện đối với giá trị này. Theo cách khác, nếu yêu cầu truy cập bao gồm ID_NF1 và MAC, yêu cầu truy cập có thể còn có ít nhất một giá trị trong số chu kỳ hợp lệ của MAC, giá trị nonce của MAC, giá trị đếm, và số chuỗi mà thuật toán mã xác thực thông điệp được thực hiện đối với giá trị này.

S506: NF thứ hai nhận yêu cầu truy cập được gửi bởi NF thứ nhất, và xác minh tính chính xác của chữ ký số hoặc MAC có trong yêu cầu truy cập này.

Cụ thể, nếu thông số bảo mật bao gồm chữ ký số, NF thứ hai có thể xác minh tính chính xác của chữ ký số này dựa vào PKnrf và nội dung được ký bởi chữ ký số này, và nội dung được ký bởi chữ ký số này bao gồm ID_NF1. Nếu xác minh rằng chữ ký số là đúng, NF thứ hai xác định rằng yêu cầu truy cập được gửi bởi NF thứ nhất được cấp quyền bởi NRF, và NF thứ nhất được phép truy cập NF thứ hai. Nếu xác minh rằng chữ ký số là không đúng, NF thứ hai xác định rằng yêu cầu truy cập được gửi bởi NF thứ nhất không được cấp quyền bởi NRF, và NF thứ nhất không được phép truy cập NF thứ hai.

Nếu thông số bảo mật bao gồm MAC, NF thứ hai có thể xác minh tính chính xác của MAC này nhờ sử dụng khóa đối xứng được chia sẻ giữa NRF và NF thứ hai và nội dung được bảo vệ bởi MAC. Nội dung được bảo vệ bởi MAC bao gồm ID_NF1. Nếu

xác minh rằng MAC là đúng, NF thứ hai xác định rằng yêu cầu truy cập được gửi bởi NF thứ nhất được cấp quyền bởi NRF, và NF thứ nhất được phép truy cập NF thứ hai. Nếu xác minh rằng MAC là không đúng, NF thứ hai xác định rằng yêu cầu truy cập được gửi bởi NF thứ nhất không được cấp quyền bởi NRF, và NF thứ nhất không được phép truy cập NF thứ hai.

Theo một ví dụ khả thi, trong phương án này của sáng chế, NRF có thể tạo ra chữ ký số hoặc MAC dựa vào từng dịch vụ được yêu cầu bởi NF thứ nhất, để thực hiện việc xác minh cấp quyền ở mức dịch vụ.

Một cách tương tự, phương án này của sáng chế có thể còn bao gồm bước gửi phản hồi truy cập đến NF thứ nhất.

Trong phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ được đề xuất theo Phương án 4 của sáng chế, NRF tạo ra chữ ký số hoặc MAC, và khi NRF và NF thứ hai không trao đổi thông số bảo mật, NF thứ hai có thể thực hiện việc xác minh cấp quyền đối với NF thứ nhất. Điều này làm giảm bớt số lần truyền thông giữa NF và NRF trong quy trình phát hiện ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Phương án 5

Trong phương án này của sáng chế, nếu NRF điều khiển và quản lý NF thứ nhất thuộc PLMA thứ nhất, NRF điều khiển và quản lý NF thứ hai thuộc PLMN thứ hai, và PLMN thứ nhất khác PLMN thứ hai, thì thông số bảo mật được sử dụng để thực hiện việc xác minh cấp quyền đối với NF thứ nhất có thể được tạo ra bởi NRF thuộc PLMN thứ hai và được gửi đến NRF thuộc PLMN thứ nhất. NRF thuộc PLMN thứ nhất nhận thông số bảo mật được gửi bởi NRF thuộc PLMN thứ hai, và gửi phản hồi phát hiện đến NF thứ nhất, trong đó phản hồi phát hiện này bao gồm thông số bảo mật thu được từ NRF thuộc PLMN thứ hai. Đối với quy trình thực hiện cụ thể, xem Fig.7.

Fig.7 là lưu đồ của phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ, và áo dụng được cho kịch bản trong đó NF thứ nhất và/hoặc NF thứ hai chuyển vùng, cụ thể là kịch bản trong đó PLMA thứ nhất mà NRF điều khiển và quản lý NF thứ nhất

thuộc về và PLMA thứ hai mà NRF điều khiển và quản lý NF thứ nhất thuộc về là khác nhau. Quy trình thực hiện để NRF thuộc PLMN thứ hai tạo ra thông số bảo mật trong kịch bản này tương tự các quy trình thực hiện để tạo ra thông số bảo mật theo các phương án từ 1 đến 4. Điểm khác biệt nằm ở chỗ giá trị tham số được sử dụng bởi NRF để tạo ra thông số bảo mật còn bao gồm PLMN ID ngoài các giá trị tham số trong các phương án nêu trên.

Phương án 6

Trong phương án này của sáng chế, trong khi thực hiện các phương án nêu trên, nếu dịch vụ cần được thay đổi, ví dụ, theo kịch bản trong đó dịch vụ được yêu cầu cần được xóa bỏ, hoặc dịch vụ được yêu cầu cần được sửa đổi, các phương án thực hiện sau có thể được sử dụng.

Trong phương án thực hiện thứ nhất, NF thứ nhất khởi tạo yêu cầu thay đổi dịch vụ, và phương án thực hiện về quy trình cụ thể được thể hiện trên Fig.8.

S601: NF thứ nhất xác định rằng dịch vụ được yêu cầu cần được thay đổi, ví dụ, dịch vụ có ID dịch vụ 1 cần được xóa bỏ hoặc được sửa đổi.

Trong phương án này của sáng chế, NF thứ nhất có thể thay đổi một hoặc nhiều dịch vụ.

S602: NF thứ nhất tạo ra MAC hoặc chữ ký số, trong đó MAC hoặc chữ ký số này có thể thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ được gửi bởi NF thứ nhất đến NRF.

Cụ thể, MAC thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ có thể được tạo ra bởi NF thứ nhất nhờ thực hiện thuật toán mã xác thực thông điệp đối với ID dịch vụ của dịch vụ được yêu cầu thay đổi bởi yêu cầu thay đổi dịch vụ, chu kỳ hợp lệ của khóa đối xứng, và ID_NF1 dựa vào khóa đối xứng được chia sẻ giữa NF thứ nhất và NRF. Chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ có thể được tạo ra bởi NF thứ nhất nhờ thực hiện thuật toán chữ ký số đối với ID dịch vụ

của dịch vụ được yêu cầu thay đổi bởi yêu cầu thay đổi dịch vụ, chu kỳ hợp lệ của chữ ký số, và ID_NF1 dựa vào khóa bí mật của NF thứ nhất.

Trong phương án này của sáng chế, nếu NF thứ nhất thay đổi nhiều dịch vụ, NF thứ nhất có thể tạo ra chữ ký số hoặc MAC cho từng dịch vụ cần thay đổi, và tất nhiên, theo cách khác có thể tạo ra một chữ ký số hoặc một MAC cho nhiều dịch vụ.

S603: NF thứ nhất gửi yêu cầu thay đổi dịch vụ đến NRF, trong đó yêu cầu thay đổi dịch vụ bao gồm MAC hoặc chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ này.

S604: NRF nhận yêu cầu thay đổi dịch vụ được gửi bởi NF thứ nhất, và thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi NF thứ nhất.

Trong phương án này của sáng chế, NRF có thể thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi NF thứ nhất, dựa vào việc xác minh MAC hoặc chữ ký số.

Cụ thể, nếu thông số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ là MAC, thì NRF có thể xác minh MAC nhận được dựa vào khóa đối xứng được lưu trước được chia sẻ bởi NRF và NF thứ nhất và nội dung nhận được được bảo vệ bởi MAC. Nếu xác minh rằng MAC là đúng, NRF xác định rằng yêu cầu thay đổi dịch vụ nhận được được cấp quyền bởi NF thứ nhất, và có thể thay đổi dịch vụ được yêu cầu thay đổi bởi yêu cầu thay đổi dịch vụ. Nếu xác minh rằng MAC là không đúng, NRF xác định rằng yêu cầu thay đổi dịch vụ nhận được không được cấp quyền bởi NF thứ nhất, và có thể từ chối thay đổi dịch vụ được yêu cầu thay đổi bởi yêu cầu thay đổi dịch vụ này.

Nếu thông số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ là chữ ký số, NRF có thể xác minh chữ ký số nhận được dựa vào PKNF1 và nội dung được bảo vệ bởi chữ ký số. PKNF1 có thể được lưu trước bởi NRF, hoặc có thể thu được trong quá trình tương tác giữa NRF và NF thứ nhất. Nếu xác minh rằng chữ ký số là đúng, NRF xác định rằng yêu cầu thay đổi dịch vụ nhận được được cấp quyền bởi NF thứ nhất, và có thể thay đổi dịch vụ được yêu cầu thay đổi bởi yêu cầu thay đổi dịch vụ.

Nếu xác minh rằng chữ ký số là không đúng, NRF xác định rằng yêu cầu thay đổi dịch vụ nhận được không được cấp quyền bởi NF thứ nhất, và có thể từ chối thay đổi dịch vụ được yêu cầu thay đổi bởi yêu cầu thay đổi dịch vụ này.

Trong phương án này của sáng chế, quy trình thực hiện để NRF thay đổi dịch vụ được yêu cầu thay đổi bởi yêu cầu thay đổi dịch vụ là không bị giới hạn. Ví dụ, NF thứ nhất có thể gửi chính sách thay đổi đến NRF, và chính sách thay đổi này có thể được bảo vệ bởi chữ ký số hoặc MAC.

Theo một ví dụ khả thi, sau khi thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi NF thứ nhất, NRF có thể gửi kết quả xác minh cấp quyền đến NF thứ nhất. Tất nhiên, quy trình thực hiện này là tùy chọn.

S605: Nếu NF thứ nhất đã truy cập NF thứ hai, NF thứ nhất có thể gửi thông báo thay đổi dịch vụ đến NF thứ hai, để chỉ thị cho NF thứ hai này thay đổi dịch vụ.

Bước S605 là tùy chọn.

Trong phương án thực hiện thứ hai, NRF khởi tạo yêu cầu thay đổi dịch vụ, và thủ tục thực hiện cụ thể được thể hiện trên Fig.9.

S701: NRF xác định rằng dịch vụ được yêu cầu cần được thay đổi, ví dụ, dịch vụ có ID dịch vụ 1 cần được xóa bỏ hoặc được sửa đổi.

Trong phương án này của sáng chế, NRF có thể thay đổi một hoặc nhiều dịch vụ.

S702: NRF tạo ra MAC hoặc chữ ký số, trong đó MAC hoặc chữ ký số này có thể thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ được gửi bởi NRF đến NF thứ nhất.

Cụ thể, quy trình tạo ra MAC hoặc chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ là tương tự như quy trình tạo ra MAC hoặc chữ ký số, bởi NF thứ nhất, thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ trong phương án nêu trên. Do đó, các chi tiết không được mô tả lại dưới đây.

Trong phương án này của sáng chế, nếu NRF thay đổi nhiều dịch vụ, NRF có thể tạo ra chữ ký số hoặc MAC cho từng dịch vụ cần thay đổi, và tất nhiên, theo cách khác có thể tạo ra một chữ ký số hoặc một MAC cho nhiều dịch vụ.

S703: NRF gửi yêu cầu thay đổi dịch vụ đến NF thứ nhất, trong đó yêu cầu thay đổi dịch vụ này bao gồm MAC hoặc chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ.

S704: NF thứ nhất nhận yêu cầu thay đổi dịch vụ được gửi bởi NRF, và thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi NRF.

Quy trình thực hiện để NF thứ nhất thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi NRF là tương tự quy trình thực hiện để NRF thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi NF thứ nhất. Do đó, các chi tiết không được mô tả lại dưới đây.

Theo một ví dụ khả thi, sau khi thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi NRF, NF thứ nhất có thể gửi kết quả xác minh cấp quyền đến NRF.

S705: Sếu NF thứ nhất đã truy cập NF thứ hai, NF thứ nhất có thể gửi thông báo thay đổi dịch vụ đến NF thứ hai, để chỉ thị cho NF thứ hai thay đổi dịch vụ.

Bước S705 là tùy chọn.

Theo phương án thực hiện thứ ba, OAM khởi tạo yêu cầu thay đổi dịch vụ, và thủ tục thực hiện cụ thể được thể hiện trên Fig.10.

S801: OAM xác định rằng dịch vụ được yêu cầu bởi NF thứ nhất cần được thay đổi, ví dụ, dịch vụ có ID dịch vụ 1 cần được xóa bỏ hoặc được sửa đổi.

Trong phương án này của sáng chế, OAM này có thể thay đổi một hoặc nhiều dịch vụ được yêu cầu bởi NF thứ nhất.

S802: OAM tạo ra MAC hoặc chữ ký số, trong đó MAC hoặc chữ ký số này có thể thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ được gửi bởi OAM đến NRF.

Cụ thể, quy trình tạo ra MAC hoặc chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ tương tự quy trình tạo ra MAC hoặc chữ ký số, bởi NRF, thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ trong phương án nêu trên. Điểm khác biệt nằm ở chỗ OAM xác định MAC dựa vào khóa đối xứng được chia sẻ giữa PAM và NRF, hoặc OAM xác định chữ ký số dựa vào PKnrf. Khi OAM xác định MAC, khóa đối xứng cần được chia sẻ giữa OAM và NRF từ trước. Khi xác định chữ ký số, OAM cần lưu trước khóa công khai của OAM, khóa bí mật của OAM, và PKnrf, và NRF cần lưu trước khóa công khai của OAM. Đối với các phần tương tự, các chi tiết không được mô tả lại dưới đây.

Trong phương án này của sáng chế, nếu OAM thay đổi nhiều dịch vụ, OAM có thể tạo ra chữ ký số hoặc MAC cho từng dịch vụ cần thay đổi, và tất nhiên, theo cách khác có thể tạo ra một chữ ký số hoặc một MAC cho nhiều dịch vụ.

S803: OAM gửi yêu cầu thay đổi dịch vụ đến NRF, trong đó yêu cầu thay đổi dịch vụ bao gồm MAC hoặc chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ.

S804: NRF nhận yêu cầu thay đổi dịch vụ được gửi bởi OAM, và thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi OAM.

Trong phương án này của sáng chế, theo quy trình thực hiện để NRF thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi OAM, NRF có thể xác minh MAC dựa vào khóa đối xứng được chia sẻ giữa NRF và OAM, hoặc có thể xác minh tính chính xác của chữ ký số dựa vào khóa công khai của OAM. Quy trình khác tương tự quy trình thực hiện để NRF thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi NF thứ nhất. Do đó, các chi tiết không được mô tả lại dưới đây.

Theo một ví dụ khả thi, sau khi thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ được gửi bởi OAM, NRF có thể gửi kết quả xác minh cấp quyền đến OAM.

S805: Nếu xác định rằng OAM cấp quyền cho yêu cầu thay đổi dịch vụ được gửi, NRF gửi thông báo thay đổi dịch vụ đến NF thứ nhất.

Trong phương án này của sáng chế, để dễ mô tả, thông báo thay đổi dịch vụ được gửi bởi NRF đến NF thứ nhất được gọi là thông báo thay đổi dịch vụ thứ nhất. Thông báo thay đổi dịch vụ thứ nhất này được gửi bởi NRF khi xác định rằng yêu cầu thay đổi dịch vụ được gửi bởi OAM được cấp quyền.

S806: NF thứ nhất nhận thông báo thay đổi dịch vụ thứ nhất được gửi bởi NRF, và khi xác định rằng NF thứ nhất đã truy cập NF thứ hai, gửi thông báo thay đổi dịch vụ đến NF thứ hai, để chỉ thị cho NF thứ hai thay đổi dịch vụ.

Trong phương án này của sáng chế, để dễ mô tả, thông báo thay đổi dịch vụ được gửi bởi NF thứ nhất đến NF thứ hai có thể được gọi là thông báo thay đổi dịch vụ thứ hai. Thông báo thay đổi dịch vụ thứ hai được gửi bởi NF thứ nhất đến NF thứ hai, và được sử dụng để chỉ thị cho NF thứ hai thay đổi dịch vụ.

Phương pháp được đề xuất theo Phương án 6 của sáng chế áp dụng được cho kịch bản trong đó dịch vụ cần được thay đổi.

Trong các phương án của sáng chế, đối với các phương án nêu trên, nếu NF thứ nhất biết mã định danh của NF thứ hai, nhưng không biết địa chỉ của NF thứ hai, thì NF thứ nhất gửi yêu cầu phát hiện đến NRF, trong đó yêu cầu phát hiện này bao gồm mã định danh của NF thứ hai. NRF xác minh mã định danh của NF thứ hai, và nếu việc xác minh thành công, thì gửi địa chỉ của NF thứ hai đến NF thứ nhất. Các tham số khác là giống các tham số trong các phương án nêu trên.

Trong các phương án của sáng chế, đối với các phương án nêu trên, mã định danh của NF1 trong yêu cầu phát hiện được gửi bởi NF1 đến NRF là tùy chọn.

Trong các phương án của sáng chế, tất cả các phương án dựa trên công nghệ bất đối xứng nêu trên có thể vẫn được thực hiện dựa vào công nghệ mã nhận dạng. Khác với trong công nghệ bảo mật bất đối xứng dựa trên chứng nhận, khóa công khai PK có thể là ID, cụ thể là mã nhận dạng người dùng trong công nghệ dựa trên mã nhận dạng.

Trong các phương án của sáng chế, các phương án nêu trên trong đó MAC và chữ ký được sử dụng cho việc xác thực còn bao gồm khả năng là K_session được tạo ra dựa vào thỏa thuận khóa DH (Diffie-Hellman), cụ thể, NRF tạo ra khóa công khai PK_DH_NRF và SK_DH_NRF mà thu được thông qua thỏa thuận khóa DH, và sử dụng MAC hoặc chữ ký để bảo vệ PK_DH_NRF; Ngoài ra, NRF còn gửi PK_DH_NRF và SK_DH_NRF đến NF thứ nhất. NF thứ nhất còn gửi PK_DH_NRF đến NF thứ hai ngoài việc gửi yêu cầu truy cập như được mô tả trong các phương án nêu trên. Sau khi xác minh thành công MAC hoặc chữ ký, NF thứ hai tạo ra PK_DH_NF2 và SK_DH_NF2. NF thứ hai tạo ra K_session dựa vào PK_DH_NRF và SK_DH_NF2. NF thứ hai gửi PK_DH_NF2 đến NF thứ nhất. Trong trường hợp này, NF thứ nhất có thể tạo ra K_session dựa vào PK_DH_NF2 và SK_DH_NRF. Các định dạng của các tham số và cách tính toán K_session là tương tự như trong thủ tục thỏa thuận khóa DH cổ điển. Giao thức khóa DH là không giới hạn, và bao gồm nhưng không giới hạn ở thuật toán rời rạc và dạng tương tự.

Phần nêu trên chủ yếu mô tả các giải pháp được đề xuất theo các phương án của sáng chế về mặt tương tác giữa phần tử mạng quản lý, phần tử mạng chức năng, và phần tử mạng điều khiển. Có thể hiểu rằng, để thực hiện các chức năng nêu trên, phần tử mạng quản lý, phần tử mạng chức năng và phần tử mạng điều khiển bao gồm các cấu trúc phần cứng tương ứng và/hoặc các môđun phần mềm để thực hiện các chức năng này. Các bộ phận và các bước thuật toán trong các ví dụ được mô tả có dựa vào các phương án được mô tả trong sáng chế có thể được thực hiện dưới dạng phần cứng hoặc phần cứng và phần mềm máy tính theo các phương án của sáng chế. Việc chức năng được thực hiện bởi phần cứng hay phần cứng được điều khiển bởi phần mềm máy tính thì phụ thuộc vào các ứng dụng cụ thể và các ràng buộc về thiết kế của các giải pháp kỹ thuật này. Người có trình độ trung bình trong lĩnh vực kỹ thuật này có thể sử dụng các phương pháp khác nhau để thực hiện các chức năng được mô tả đối với từng ứng dụng cụ thể, nhưng không nên xem là phương án thực hiện này vượt quá phạm vi của các giải pháp kỹ thuật theo các phương án của sáng chế.

Trong các phương án của sáng chế, phần tử mạng chức năng thứ nhất, phần tử mạng chức năng thứ hai và phần tử mạng điều khiển có thể được phân chia thành các bộ phận chức năng theo các ví dụ về phương pháp nêu trên. Ví dụ, các bộ phận chức năng khác nhau có thể thu được nhờ phân chia theo các chức năng khác nhau, hoặc hai hoặc nhiều chức năng có thể được tích hợp thành bộ phận xử lý. Bộ phận được tích hợp này có thể được thực hiện dưới dạng phần cứng, hoặc có thể được thực hiện dưới dạng bộ phận chức năng dạng phần mềm. Cần lưu ý rằng, theo các phương án của sáng chế, việc phân chia bộ phận là ví dụ, và chỉ là sự phân chia chức năng về mặt lôgic. Trong phương án thực hiện thực tế, cách phân chia khác cũng có thể được sử dụng.

Khi dạng bộ phận chức năng dạng phần mềm được sử dụng để thực hiện sáng chế, Fig.11 là sơ đồ cấu trúc sơ lược của thiết bị phát hiện 100 dựa vào kiến trúc dựa trên dịch vụ theo phương án của sáng chế. Thiết bị phát hiện 100 dựa vào kiến trúc dựa trên dịch vụ có thể được áp dụng cho phần tử mạng điều khiển. Theo Fig.11, thiết bị phát hiện 100 được áp dụng cho phần tử mạng điều khiển có thể bao gồm bộ phận xử lý 101 và bộ phận gửi 102. Bộ phận xử lý 101 được tạo cấu hình để xác định thông số bảo mật. Bộ phận gửi 102 được tạo cấu hình để gửi phản hồi phát hiện đến phần tử mạng chức năng thứ nhất, trong đó phản hồi phát hiện này bao gồm thông số bảo mật được tạo ra bởi bộ phận xử lý 101.

Theo một ví dụ khả thi, thông số bảo mật này bao gồm token thứ nhất bất đối xứng và khóa phiên thứ nhất được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai.

Bộ phận xử lý 101 được tạo cấu hình để: tạo ra khóa phiên thứ nhất; thực hiện thuật toán chữ ký số đối với mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ nhất dựa vào khóa bí mật của phần tử mạng điều khiển, để tạo ra chữ ký số; và mật hóa chữ ký số, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, và khóa phiên thứ nhất dựa vào khóa công khai của phần tử mạng chức năng thứ hai, để tạo ra token thứ nhất bất đối xứng. Bộ phận

gửi 102 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ nhất, token thứ nhất bất đối xứng được tạo ra bởi bộ phận xử lý 101 dưới dạng thông số bảo mật.

Theo một ví dụ khả thi khác, thông số bảo mật bao gồm token thứ nhất đối xứng và khóa phiên thứ nhất được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai.

Bộ phận xử lý 101 được tạo cấu hình để: tạo ra khóa phiên thứ nhất; thực hiện thuật toán mã xác thực thông điệp đối với mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ nhất dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra mã xác thực thông điệp; và mật hóa mã xác thực thông điệp, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, và khóa phiên thứ nhất dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra token thứ nhất đối xứng. Bộ phận gửi 102 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ nhất, token thứ nhất đối xứng được tạo ra bởi bộ phận xử lý 101 dưới dạng thông số bảo mật.

Cụ thể, theo phương án thực hiện khả thi, bộ phận xử lý 101 lựa chọn ngẫu nhiên khóa phiên thứ nhất. Theo phương án thực hiện khả thi khác, bộ phận xử lý 101 thực hiện phép tạo dẫn xuất đối với mã định danh của phần tử mạng chức năng thứ nhất và mã định danh của phần tử mạng chức năng thứ hai dựa vào khóa dẫn xuất, để tạo ra khóa phiên thứ nhất. Khóa dẫn xuất này thu được bởi phần tử mạng điều khiển nhờ thực hiện phép tạo dẫn xuất khóa đối với khóa gốc được thiết lập trước, hoặc khóa dẫn xuất này là khóa được lưu bởi phần tử mạng điều khiển.

Trong phương án này của sáng chế, thiết bị phát hiện 100 được áp dụng cho phần tử mạng điều khiển tạo ra token thứ nhất đối xứng hoặc token thứ nhất bất đối xứng, và khóa phiên thứ nhất được sử dụng để bảo vệ toàn bộ dữ liệu được sử dụng cho việc truyền thông giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai. Điều này có thể thực hiện việc bảo vệ bảo mật dựa trên kết nối, và thực hiện việc xác thực bảo mật đối với thông số bảo mật giữa phần tử mạng chức năng thứ nhất và phần

tử mạng chức năng thứ hai khi phần tử mạng điều khiển và phần tử mạng chức năng thứ hai không trao đổi thông số bảo mật. Điều này làm giảm bớt số lần truyền thông giữa phần tử mạng chức năng và phần tử mạng điều khiển trong quy trình phát hiện ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai, và token thứ hai bất đối xứng được tạo ra dựa vào từng khóa phiên thứ hai.

Bộ phận xử lý 101 được tạo cấu hình để: tạo ra khóa phiên thứ hai cho từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất; thực hiện thuật toán chữ ký số đối với mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ hai dựa vào khóa bí mật của phần tử mạng điều khiển cho từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, để tạo ra chữ ký số; và mật hóa chữ ký số, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, mã định danh dịch vụ của dịch vụ được bảo vệ bởi khóa phiên thứ hai, và khóa phiên thứ hai dựa vào khóa công khai của phần tử mạng chức năng thứ hai đối với từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, để tạo ra token thứ hai bất đối xứng của từng dịch vụ. Bộ phận gửi 102 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ nhất, token thứ hai bất đối xứng tương ứng với từng dịch vụ được tạo ra bởi bộ phận xử lý 101 dưới dạng thông số bảo mật.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai, và token thứ hai đối xứng được tạo ra dựa vào từng khóa phiên thứ hai.

Phần tử mạng điều khiển tạo ra khóa phiên thứ hai bảo vệ từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất. Phần tử mạng điều khiển thực hiện, đối với từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, thuật toán mã xác thực thông điệp đối với mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ hai dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra mã xác thực thông điệp. Phần tử mạng điều khiển mật

hóa mã xác thực thông điệp, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, mã định danh dịch vụ của dịch vụ được bảo vệ bởi khóa phiên thứ hai, và khóa phiên thứ hai dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra token thứ hai đối xứng cho từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất. Bộ phận gửi 102 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ nhất, token thứ hai đối xứng được tạo ra bởi bộ phận xử lý 101 dưới dạng thông số bảo mật.

Trong phương án này của sáng chế, thiết bị phát hiện 100 được áp dụng cho phần tử mạng điều khiển tạo ra khóa phiên thứ hai và token thứ hai cho từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất. Điều này có thể thực hiện việc bảo vệ bảo mật dựa trên dịch vụ, và thực hiện việc xác thực bảo mật đối với thông số bảo mật giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai khi phần tử mạng điều khiển và phần tử mạng chức năng thứ hai không trao đổi thông số bảo mật. Điều này làm giảm bớt số lần truyền thông giữa phần tử mạng chức năng và phần tử mạng điều khiển trong quy trình phát hiện ở mức độ nhất định, và thêm nữa, có thể giảm độ phức tạp truyền thông ở mức độ nhất định.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai, và token thứ ba bất đối xứng được tạo ra dựa vào tất cả các khóa phiên thứ hai.

Bộ phận xử lý 101 được tạo cấu hình để: tạo ra khóa phiên thứ hai bảo vệ từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất; thực hiện thuật toán chữ ký số đối với mã định danh của phần tử mạng chức năng thứ nhất và tất cả các khóa phiên thứ hai dựa vào khóa bí mật của phần tử mạng điều khiển, để tạo ra chữ ký số; và mật hóa chữ ký số, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, các mã định danh dịch vụ của các dịch vụ được bảo vệ bởi tất cả các khóa phiên thứ hai, và tất cả các khóa phiên thứ hai dựa vào khóa công khai của phần tử mạng chức năng thứ hai, để tạo ra token thứ ba bất đối xứng của các

dịch vụ. Bộ phận gửi 102 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ nhất, token thứ ba bất đối xứng được tạo ra bởi bộ phận xử lý 101 dưới dạng thông số bảo mật.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai, và token thứ ba đối xứng được tạo ra dựa vào tất cả các khóa phiên thứ hai.

Bộ phận xử lý 101 được tạo cấu hình để: tạo ra khóa phiên thứ hai bảo vệ từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất; thực hiện thuật toán mã xác thực thông điệp đối với mã định danh của phần tử mạng chức năng thứ nhất và tất cả các khóa phiên thứ hai dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra mã xác thực thông điệp; và mật hóa mã xác thực thông điệp, mã định danh của phần tử mạng chức năng thứ nhất, mã định danh của phần tử mạng chức năng thứ hai, các mã định danh dịch vụ của các dịch vụ được bảo vệ bởi tất cả các khóa phiên thứ hai, và tất cả các khóa phiên thứ hai dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra token thứ ba đối xứng. Bộ phận gửi 102 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ nhất, token thứ ba đối xứng được tạo ra bởi bộ phận xử lý 101 dưới dạng thông số bảo mật.

Trong phương án này của sáng chế, thiết bị phát hiện 100 được áp dụng cho phần tử mạng điều khiển tạo ra khóa phiên thứ hai cho từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và bổ sung tất cả các khóa phiên thứ hai vào một token thứ ba. Điều này có thể thực hiện việc bảo vệ bảo mật dựa trên dịch vụ, và việc gửi một token đến phần tử mạng chức năng thứ hai có thể giảm bớt được độ phức tạp truyền thông.

Cụ thể, khi bộ phận xử lý 101 tạo ra khóa phiên thứ hai cho từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, theo phương án thực hiện khả thi, khóa phiên thứ hai được lựa chọn ngẫu nhiên bởi bộ phận xử lý 101. Theo phương án thực

hiện khả thi khác, khóa phiên thứ hai được tạo ra bởi bộ phận xử lý 101 nhờ thực hiện phép tạo dẫn xuất đối với mã định danh của phần tử mạng chức năng thứ nhất và mã định danh của phần tử mạng chức năng thứ hai dựa vào khóa dẫn xuất. Khóa dẫn xuất này thu được bởi phần tử mạng điều khiển nhờ thực hiện phép tạo dẫn xuất khóa đối với khóa gốc được thiết lập trước, hoặc khóa dẫn xuất này là khóa được lưu bởi phần tử mạng điều khiển này.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm chữ ký số.

Bộ phận xử lý 101 được tạo cấu hình để thực hiện thuật toán chữ ký số đối với mã định danh của phần tử mạng chức năng thứ nhất dựa vào khóa bí mật của phần tử mạng điều khiển, để tạo ra chữ ký số. Bộ phận gửi 102 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ nhất, chữ ký số được tạo ra bởi bộ phận xử lý 101 dưới dạng thông số bảo mật.

Bộ phận xử lý 101 có thể tạo ra chữ ký số dựa vào từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, để thực hiện việc xác minh cấp quyền ở mức dịch vụ.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm mã xác thực thông điệp.

Bộ phận xử lý 101 được tạo cấu hình để thực hiện thuật toán mã xác thực thông điệp đối với mã định danh của phần tử mạng chức năng thứ nhất dựa vào khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, để tạo ra mã xác thực thông điệp. Bộ phận gửi 102 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ nhất, mã xác thực thông điệp được tạo ra bởi bộ phận xử lý 101 dưới dạng thông số bảo mật.

Bộ phận xử lý 101 có thể tạo ra mã xác thực thông điệp dựa vào từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, để thực hiện việc xác minh cấp quyền ở mức dịch vụ.

Theo phương án thực hiện khả thi khác nữa, bộ phận xử lý 101 được tạo cấu hình để tạo ra MAC hoặc chữ ký số khi xác định rằng bộ phận gửi cần phải thay đổi dịch vụ được yêu cầu. Bộ phận gửi 102 được tạo cấu hình để gửi yêu cầu thay đổi dịch vụ đến phần tử mạng chức năng thứ nhất, trong đó yêu cầu thay đổi dịch vụ bao gồm MAC hoặc chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ và được tạo ra bởi bộ phận xử lý 101.

Theo phương án thực hiện khả thi khác nữa, thiết bị phát hiện 100 được áp dụng cho phần tử mạng điều khiển có thể còn có bộ phận nhận 103.

Theo phương án khả thi, bộ phận nhận 103 được tạo cấu hình để nhận yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng chức năng thứ nhất hoặc phần tử mạng quản lý. Yêu cầu thay đổi dịch vụ này bao gồm mã xác thực thông điệp hoặc chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ. Bộ phận xử lý 101 được tạo cấu hình để thực hiện việc xác minh cấp quyền, dựa vào yêu cầu thay đổi dịch vụ được tiếp nhận bởi bộ phận nhận 103, đối với yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng chức năng thứ nhất hoặc phần tử mạng quản lý.

Nếu dạng phần cứng được sử dụng để thực hiện sáng chế, thì bộ phận xử lý 101 có thể bộ xử lý, bộ phận gửi 102 có thể là bộ phát, và bộ phận nhận 103 có thể là bộ thu. Nếu bộ phận xử lý 101 là bộ xử lý, bộ phận gửi 102 là bộ phát, và bộ phận nhận 103 là bộ thu, thì thiết bị phát hiện 100 có thể sử dụng cấu trúc của phần tử mạng điều khiển được thể hiện trên Fig.12. Phần tử mạng điều khiển được thể hiện trên Fig.12 có thể là NRF, và NRF này có thể là NRF trong các phương án phương pháp nêu trên.

Fig.12 là sơ đồ cấu trúc sơ lược của phần tử mạng điều khiển 1000 theo phương án của sáng chế, nghĩa là sơ đồ cấu trúc sơ lược khác của thiết bị phát hiện 100. Theo Fig.12, phần tử mạng điều khiển 1000 bao gồm bộ xử lý 1001 và bộ phát 1002, và có thể còn có bộ thu 1003. Theo cách khác, bộ xử lý 1001 có thể là bộ điều khiển. Bộ xử lý 1001 được tạo cấu hình để hỗ trợ phần tử mạng điều khiển 1000 khi thực hiện các chức năng của phần tử mạng điều khiển trên các hình vẽ từ Fig.2 đến Fig.10. Bộ phát 1002 và bộ thu 1003 được tạo cấu hình để hỗ trợ chức năng gửi và nhận các thông điệp

giữa phần tử mạng điều khiển 1000 và phần tử mạng chức năng thứ nhất. Phần tử mạng điều khiển 1000 có thể còn có bộ nhớ 1004. Bộ nhớ 1004 được tạo cấu hình để ghép được với bộ xử lý 1001, và bộ nhớ 1004 lưu trữ lệnh chương trình và dữ liệu cần thiết cho phần tử mạng điều khiển 1000. Bộ xử lý 1001, bộ phát 1002, bộ thu 1003 và bộ nhớ 1004 được nối với nhau. Bộ nhớ 1004 được tạo cấu hình để lưu trữ lệnh. Bộ xử lý 1001 được tạo cấu hình để thi hành lệnh được lưu trữ trong bộ nhớ 1004, để điều khiển bộ phát 1002 và bộ thu 1003 gửi và nhận dữ liệu, và thực hiện các bước thực hiện các chức năng tương ứng bởi phần tử mạng điều khiển trong các phương pháp nêu trên.

Trong phương án này của sáng chế, đối với các khái niệm, các phần diễn giải, các phần mô tả chi tiết, và các bước khác của thiết bị phát hiện 100 được áp dụng cho phần tử mạng điều khiển và phần tử mạng điều khiển 1000 liên quan đến các giải pháp kỹ thuật được đề xuất theo các phương án của sáng chế, xem các phần mô tả về nội dung trong các phương án phương pháp nêu trên hoặc các phương án khác. Các chi tiết không được mô tả lại dưới đây.

Khi dạng bộ phận chức năng dạng phần mềm được sử dụng để thực hiện sáng chế, Fig.13 là sơ đồ cấu trúc sơ lược của thiết bị phát hiện 200 dựa vào kiến trúc dựa trên dịch vụ theo phương án của sáng chế. Thiết bị phát hiện 200 dựa vào kiến trúc dựa trên dịch vụ có thể được áp dụng cho phần tử mạng chức năng thứ nhất. Theo Fig.13, thiết bị phát hiện 200 được áp dụng cho phần tử mạng chức năng thứ nhất có thể bao gồm bộ phận nhận 201 và bộ phận gửi 202. Bộ phận nhận 201 được tạo cấu hình để nhận phản hồi phát hiện được gửi bởi phần tử mạng điều khiển, trong đó phản hồi phát hiện này bao gồm thông số bảo mật và địa chỉ truy cập hoặc mã định danh của phần tử mạng chức năng thứ hai. Bộ phận gửi 202 được tạo cấu hình để gửi yêu cầu truy cập đến phần tử mạng chức năng thứ hai dựa vào địa chỉ truy cập hoặc mã định danh được tiếp nhận bởi bộ phận nhận, trong đó yêu cầu truy cập này bao gồm thông số bảo mật được tiếp nhận bởi bộ phận nhận 201.

Theo một ví dụ khả thi, thông số bảo mật bao gồm token thứ nhất đối xứng hoặc token thứ nhất bất đối xứng, và khóa phiên thứ nhất được chia sẻ giữa phần tử mạng

chức năng thứ nhất và phần tử mạng chức năng thứ hai. Bộ phận nhận 201 được tạo cấu hình để nhận token thứ nhất đối xứng hoặc token thứ nhất bất đối xứng được gửi bởi phần tử mạng điều khiển. Bộ phận gửi 202 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ hai, token thứ nhất đối xứng hoặc token thứ nhất bất đối xứng được tiếp nhận bởi bộ phận nhận 201.

Theo một ví dụ khả thi khác, thông số bảo mật bao gồm khóa phiên thứ hai được tạo ra dựa vào mã định danh dịch vụ của từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và token thứ hai đối xứng hoặc token thứ hai bất đối xứng được tạo ra dựa vào từng khóa phiên thứ hai. Bộ phận nhận 201 được tạo cấu hình để nhận token thứ hai đối xứng hoặc token thứ hai bất đối xứng được gửi bởi phần tử mạng điều khiển. Bộ phận gửi 202 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ hai, token thứ hai đối xứng hoặc token thứ hai bất đối xứng được tiếp nhận bởi bộ phận nhận 201.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được tạo ra dựa vào mã định danh dịch vụ của từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và token thứ ba đối xứng hoặc token thứ ba bất đối xứng được tạo ra dựa vào tất cả các khóa phiên thứ hai. Bộ phận nhận 201 được tạo cấu hình để nhận token thứ ba đối xứng hoặc token thứ ba bất đối xứng được gửi bởi phần tử mạng điều khiển. Bộ phận gửi 202 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ hai, token thứ ba đối xứng hoặc token thứ ba bất đối xứng được tiếp nhận bởi bộ phận nhận 201.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm chữ ký số hoặc mã xác thực thông điệp. Bộ phận nhận 201 được tạo cấu hình để nhận chữ ký số hoặc mã xác thực thông điệp được gửi bởi phần tử mạng điều khiển. Bộ phận gửi 202 được tạo cấu hình để gửi, đến phần tử mạng chức năng thứ hai, chữ ký số hoặc mã xác thực thông điệp được tiếp nhận bởi bộ phận nhận 201.

Theo phương án thực hiện khả thi khác nữa, bộ phận nhận 201 còn được tạo cấu hình để nhận thông báo thay đổi dịch vụ thứ nhất được gửi bởi phần tử mạng điều khiển,

trong đó thông báo thay đổi dịch vụ thứ nhất được gửi bởi phần tử mạng điều khiển khi xác định rằng yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng quản lý là hợp lệ.

Theo phương án thực hiện khả thi khác nữa, bộ phận nhận 201 còn được tạo cấu hình để nhận yêu cầu thay đổi dịch vụ được gửi bởi phần tử mạng điều khiển, trong đó yêu cầu thay đổi dịch vụ bao gồm mã xác thực thông điệp hoặc chữ ký số thực hiện việc bảo vệ bảo mật đối với yêu cầu thay đổi dịch vụ. Thiết bị phát hiện 200 được áp dụng cho phần tử mạng chức năng thứ nhất còn bao gồm bộ phận xử lý 203, trong đó bộ phận xử lý 203 được tạo cấu hình để xác minh tính chính xác của mã xác thực thông điệp hoặc chữ ký số có trong yêu cầu thay đổi dịch vụ được tiếp nhận bởi bộ phận nhận 201.

Nếu dạng phần cứng được sử dụng để thực hiện sáng chế, bộ phận nhận 201 có thể là bộ thu, bộ phận gửi 202 có thể là bộ phát, và bộ phận xử lý 203 có thể bộ xử lý. Nếu bộ phận nhận 201 là bộ thu, bộ phận gửi 202 là bộ phát, và bộ phận xử lý 203 là bộ xử lý, thiết bị phát hiện 200 có thể sử dụng cấu trúc của phần tử mạng chức năng thứ nhất được thể hiện trên Fig.14. Phần tử mạng chức năng thứ nhất được thể hiện trên Fig.14 có thể là NF thứ nhất, và NF thứ nhất này có thể là NF thứ nhất trong các phương án phương pháp nêu trên.

Fig.14 là sơ đồ cấu trúc sơ lược của phần tử mạng chức năng thứ nhất 2000 theo phương án của sáng chế, nghĩa là sơ đồ cấu trúc sơ lược khác của thiết bị phát hiện 200. Theo Fig.14, phần tử mạng chức năng thứ nhất 2000 bao gồm bộ xử lý 2001 và bộ phát 2002, và có thể còn có bộ thu 2003. Theo cách khác, bộ xử lý 2001 có thể là bộ điều khiển. Bộ xử lý 2001 được tạo cấu hình để hỗ trợ phần tử mạng chức năng thứ nhất 2000 thực hiện các chức năng của phần tử mạng chức năng thứ nhất trên các hình vẽ từ Fig.2 đến Fig.10. Bộ phát 2002 và bộ thu 2003 được tạo cấu hình để hỗ trợ chức năng gửi và nhận các thông điệp giữa phần tử mạng chức năng thứ nhất 2000 và phần tử mạng điều khiển và phần tử mạng chức năng thứ hai. Phần tử mạng chức năng thứ nhất 2000 có thể còn có bộ nhớ 2004. Bộ nhớ 2004 được tạo cấu hình để ghép được với bộ xử lý 2001, và bộ nhớ 2004 lưu trữ lệnh chương trình và dữ liệu cần thiết cho phần tử mạng chức năng thứ nhất 2000. Bộ xử lý 2001, bộ phát 2002, bộ thu 2003 và bộ nhớ 2004

được nối với nhau. Bộ nhớ 2004 được tạo cấu hình để lưu trữ lệnh. Bộ xử lý 2001 được tạo cấu hình để thi hành lệnh được lưu trữ trong bộ nhớ 2004, để điều khiển bộ phát 2002 và bộ thu 2003 gửi và nhận dữ liệu, và thực hiện các bước thực hiện các chức năng tương ứng bởi phần tử mạng chức năng thứ nhất trong các phương pháp nêu trên.

Trong phương án này của sáng chế, đối với các khái niệm, các phần diễn giải, và các bước khác của thiết bị phát hiện 200 được áp dụng cho phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ nhất 2000 liên quan đến các giải pháp kỹ thuật được đề xuất theo các phương án của sáng chế, xem các phần mô tả về nội dung trong các phương án phương pháp nêu trên hoặc các phương án khác. Các chi tiết không được mô tả lại dưới đây.

Khi dạng bộ phận chức năng dạng phần mềm được sử dụng để thực hiện sáng chế, Fig.15 là sơ đồ cấu trúc sơ lược của thiết bị phát hiện 300 dựa vào kiến trúc dựa trên dịch vụ theo phương án của sáng chế. Thiết bị phát hiện 300 dựa vào kiến trúc dựa trên dịch vụ có thể được áp dụng cho phần tử mạng chức năng thứ hai. Theo Fig.15, thiết bị phát hiện 300 được áp dụng cho phần tử mạng chức năng thứ hai có thể bao gồm bộ phận nhận 301 và bộ phận xử lý 302. Bộ phận nhận 301 được tạo cấu hình để nhận yêu cầu truy cập được gửi bởi phần tử mạng chức năng thứ nhất, trong đó yêu cầu truy cập này bao gồm thông số bảo mật. Bộ phận xử lý 302 được tạo cấu hình để xác minh tính chính xác của thông số bảo mật được tiếp nhận bởi bộ phận nhận 301, và xác định, dựa vào tính chính xác của thông số bảo mật, xem yêu cầu truy cập có được cấp quyền bởi phần tử mạng chức năng thứ nhất hay không.

Theo một ví dụ khả thi, thông số bảo mật bao gồm token thứ nhất bất đối xứng và khóa phiên thứ nhất được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai. Bộ phận nhận 301 được tạo cấu hình để nhận token thứ nhất bất đối xứng được gửi bởi phần tử mạng chức năng thứ nhất. Bộ phận xử lý 302 được tạo cấu hình để giải mật, nhờ sử dụng khóa bí mật của phần tử mạng chức năng thứ hai, token thứ nhất bất đối xứng được tiếp nhận bởi bộ phận nhận 301, để thu được chữ ký số, và xác minh tính chính xác của chữ ký số nhờ sử dụng khóa công khai của phần tử

mạng điều khiển và nội dung được ký. Nội dung được ký này bao gồm mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ nhất.

Theo một ví dụ khả thi khác, thông số bảo mật bao gồm token thứ nhất đối xứng và khóa phiên thứ nhất được chia sẻ giữa phần tử mạng chức năng thứ nhất và phần tử mạng chức năng thứ hai. Bộ phận nhận 301 được tạo cấu hình để nhận token thứ nhất đối xứng được gửi bởi phần tử mạng chức năng thứ nhất. Bộ phận xử lý 302 được tạo cấu hình để giải mật, nhờ sử dụng khóa đối xứng, token thứ nhất đối xứng được tiếp nhận bởi bộ phận nhận 301, để thu được mã xác thực thông điệp, và xác minh tính chính xác của mã xác thực thông điệp nhờ sử dụng khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai và nội dung được bảo vệ bởi mã xác thực thông điệp này. Nội dung được bảo vệ bởi mã xác thực thông điệp bao gồm mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ nhất.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được tạo ra dựa vào mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và token thứ hai bất đối xứng được tạo ra dựa vào khóa phiên thứ hai. Bộ phận nhận 301 được tạo cấu hình để nhận token thứ hai bất đối xứng được gửi bởi phần tử mạng chức năng thứ nhất. Bộ phận xử lý 302 được tạo cấu hình để giải mật, nhờ sử dụng khóa bí mật của phần tử mạng chức năng thứ hai, token thứ hai bất đối xứng được tiếp nhận bởi bộ phận nhận 301, để thu được chữ ký số, và xác minh tính chính xác của chữ ký số nhờ sử dụng khóa công khai của phần tử mạng điều khiển và nội dung được ký. Nội dung được ký này bao gồm mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ hai.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được tạo ra riêng biệt dựa vào mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và token thứ hai đối xứng được tạo ra dựa vào khóa phiên thứ hai. Bộ phận nhận 301 được tạo cấu hình để nhận token thứ hai đối xứng được gửi bởi phần tử mạng chức năng thứ nhất. Bộ phận xử lý 302 được tạo cấu hình để giải mật, nhờ sử dụng khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển

và phần tử mạng chức năng thứ hai, token thứ hai đối xứng được tiếp nhận bởi bộ phận nhận 301, để thu được mã xác thực thông điệp, và xác minh tính chính xác của mã xác thực thông điệp nhờ sử dụng khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai và nội dung được bảo vệ bởi mã xác thực thông điệp này. Nội dung được bảo vệ bởi mã xác thực thông điệp bao gồm mã định danh của phần tử mạng chức năng thứ nhất và khóa phiên thứ hai.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được tạo ra dựa vào mã định danh dịch vụ của từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và token thứ ba bất đối xứng được tạo ra dựa vào tất cả các khóa phiên thứ hai. Bộ phận nhận 301 được tạo cấu hình để nhận token thứ ba bất đối xứng được gửi bởi phần tử mạng chức năng thứ nhất. Bộ phận xử lý 302 được tạo cấu hình để giải mật, nhờ sử dụng khóa bí mật của phần tử mạng chức năng thứ hai, token thứ ba được tiếp nhận bởi bộ phận nhận 301, để thu được chữ ký số, và xác minh tính chính xác của chữ ký số nhờ sử dụng khóa công khai của phần tử mạng điều khiển và nội dung được ký. Nội dung được ký này bao gồm mã định danh của phần tử mạng chức năng thứ nhất và tất cả các khóa phiên thứ hai.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm khóa phiên thứ hai được tạo ra dựa vào mã định danh dịch vụ của từng dịch vụ được yêu cầu bởi phần tử mạng chức năng thứ nhất, và token thứ ba đối xứng được tạo ra dựa vào tất cả các khóa phiên thứ hai. Bộ phận nhận 301 được tạo cấu hình để nhận token thứ ba đối xứng được gửi bởi phần tử mạng chức năng thứ nhất. Bộ phận xử lý 302 được tạo cấu hình để giải mật, nhờ sử dụng khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai, token thứ ba đối xứng được tiếp nhận bởi bộ phận nhận 301, để thu được mã xác thực thông điệp, và xác minh tính chính xác của mã xác thực thông điệp nhờ sử dụng khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai và nội dung được bảo vệ bởi mã xác thực thông điệp này. Nội dung được bảo vệ bởi mã xác thực thông điệp bao gồm mã định danh của phần tử mạng chức năng thứ nhất và tất cả các khóa phiên thứ hai.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm chữ ký số. Bộ phận nhận 301 được tạo cấu hình để nhận chữ ký số được gửi bởi phần tử mạng chức năng thứ nhất. Bộ phận xử lý 302 được tạo cấu hình để xác minh, nhờ sử dụng khóa công khai của phần tử mạng điều khiển và nội dung được ký bởi chữ ký số, tính chính xác của chữ ký số được tiếp nhận bởi bộ phận nhận 301. Nội dung được ký bởi chữ ký số bao gồm mã định danh của phần tử mạng chức năng thứ nhất.

Theo phương án thực hiện khả thi khác nữa, thông số bảo mật bao gồm mã xác thực thông điệp. Bộ phận nhận 301 được tạo cấu hình để nhận mã xác thực thông điệp được gửi bởi phần tử mạng chức năng thứ nhất. Bộ phận xử lý 302 được tạo cấu hình để xác minh tính chính xác của mã xác thực thông điệp nhờ sử dụng khóa đối xứng được chia sẻ giữa phần tử mạng điều khiển và phần tử mạng chức năng thứ hai và nội dung được bảo vệ bởi mã xác thực thông điệp, trong đó nội dung được bảo vệ bởi mã xác thực thông điệp bao gồm mã định danh của phần tử mạng chức năng thứ nhất.

Nếu dạng phần cứng được sử dụng để thực hiện sáng chế, bộ phận nhận 301 có thể là bộ thu phát, và bộ phận xử lý 302 có thể là bộ xử lý. Nếu bộ phận nhận 301 là bộ thu và bộ phận xử lý 302 là bộ xử lý, thiết bị phát hiện 300 có thể sử dụng cấu trúc của phần tử mạng chức năng thứ hai được thể hiện trên Fig.16. Phần tử mạng chức năng thứ hai được thể hiện trên Fig.16 có thể là NF thứ hai, và NF thứ hai này có thể là NF thứ hai trong các phương án phương pháp nêu trên.

Fig.16 là sơ đồ cấu trúc sơ lược của phần tử mạng chức năng thứ hai 3000 theo phương án của sáng chế, nghĩa là sơ đồ cấu trúc sơ lược khác của thiết bị phát hiện 300. Theo Fig.16, phần tử mạng chức năng thứ hai 3000 bao gồm bộ xử lý 3001 và bộ thu phát 3002. Theo cách khác, bộ xử lý 3001 có thể là bộ điều khiển. Bộ xử lý 3001 được tạo cấu hình để hỗ trợ phần tử mạng chức năng thứ hai 3000 trong việc thực hiện các chức năng của phần tử mạng chức năng thứ hai trên các hình vẽ từ Fig.2 đến Fig.10. Bộ thu phát 3002 được tạo cấu hình để hỗ trợ chức năng gửi và nhận các thông điệp giữa phần tử mạng chức năng thứ hai 3000 và phần tử mạng chức năng thứ nhất. Phần tử mạng chức năng thứ hai 3000 có thể còn có bộ nhớ 3003. Bộ nhớ 3003 được tạo cấu

hình để ghép được với bộ xử lý 3001, và bộ nhớ 3000 lưu trữ lệnh chương trình và dữ liệu cần thiết cho phần tử mạng chức năng thứ hai 3000. Bộ xử lý 3001, bộ thu phát 3002 và bộ nhớ 3003 được nối với nhau. Bộ nhớ 3003 được tạo cấu hình để lưu trữ lệnh. Bộ xử lý 3001 được tạo cấu hình để thi hành lệnh được lưu trữ trong bộ nhớ 3003, để điều khiển bộ thu phát 3002 gửi và nhận dữ liệu, và thực hiện các bước thực hiện các chức năng tương ứng bởi phần tử mạng điều khiển trong các phương pháp nêu trên.

Trong phương án này của sáng chế, đối với các khái niệm, các phần diễn giải, và các bước khác của thiết bị phát hiện 300 và phần tử mạng chức năng thứ hai 3000 liên quan đến các giải pháp kỹ thuật được đề xuất theo các phương án của sáng chế, xem các phần mô tả về nội dung trong các phương án phương pháp nêu trên hoặc các phương án khác. Các chi tiết không được mô tả lại dưới đây.

Cần lưu ý rằng bộ xử lý có liên quan nêu trên theo các phương án của sáng chế có thể là bộ xử lý trung tâm (central processing unit, CPU), bộ xử lý dùng cho mục đích chung, bộ xử lý tín hiệu số (digital signal processor, DSP), mạch tích hợp dùng cho ứng dụng cụ thể (application-specific integrated circuit, ASIC), mảng cổng lập trình được theo trường (field programmable gate array, FPGA), hoặc thiết bị lôgic lập trình được khác, thiết bị lôgic tranzito, thành phần phần cứng, hoặc sự kết hợp bất kỳ của chúng. Bộ xử lý này có thể thực hiện hoặc thi hành các khối lôgic, các môđun và các mạch làm ví dụ khác nhau được mô tả có dựa vào nội dung được mô tả trong sáng chế. Theo cách khác, bộ xử lý có thể là sự kết hợp của các bộ xử lý thực hiện chức năng tính toán, ví dụ, sự kết hợp của một hoặc nhiều bộ vi xử lý, hoặc sự kết hợp của DSP và bộ vi xử lý.

Bộ nhớ có thể được tích hợp vào bộ xử lý hoặc có thể được bố trí tách rời khỏi bộ xử lý này.

Trong phương án thực hiện, các chức năng của bộ thu và bộ phát có thể được thực hiện nhờ sử dụng mạch thu phát hoặc chip thu phát chuyên dụng. Bộ xử lý có thể được thực hiện nhờ sử dụng chip xử lý chuyên dụng, mạch xử lý, bộ xử lý hoặc chip dùng cho mục đích chung.

Theo phương án thực hiện khác, mã chương trình để thực hiện các chức năng của bộ xử lý, bộ thu, và bộ phát được lưu trữ trong bộ nhớ, và bộ xử lý dùng cho mục đích chung thi hành mã trong bộ nhớ để thực hiện các chức năng của bộ xử lý, bộ thu và bộ phát.

Theo các phương pháp được đề xuất theo các phương án của sáng chế, phương án của sáng chế còn đề xuất hệ thống truyền thông, trong đó hệ thống truyền thông này bao gồm phần tử mạng chức năng thứ nhất, phần tử mạng chức năng thứ hai và phần tử mạng điều khiển nêu trên.

Phương án của sáng chế còn đề xuất chip. Chip này được nối với bộ nhớ, và được tạo cấu hình để đọc và thi hành chương trình phần mềm được lưu trữ trong bộ nhớ, để thực hiện các chức năng của phần tử mạng chức năng thứ nhất, phần tử mạng chức năng thứ hai hoặc phần tử mạng điều khiển trong phương án nêu trên.

Phương án của sáng chế còn đề xuất vật ghi lưu trữ bởi máy tính. Vật ghi lưu trữ bởi máy tính này lưu trữ một số lệnh. Khi các lệnh này được thi hành, phương pháp phát hiện trong các phương án phương pháp nêu trên có thể được thực hiện.

Phương án của sáng chế còn đề xuất sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính này bao gồm chương trình máy tính. Chương trình máy tính này được sử dụng để thực hiện phương pháp phát hiện trong các phương án phương pháp nêu trên.

Người có trình độ trung bình trong lĩnh vực kỹ thuật này cần hiểu rằng các phương án của sáng chế có thể được đề xuất dưới dạng phương pháp, hệ thống, hoặc sản phẩm chương trình máy tính. Do đó, các phương án của sáng chế có thể sử dụng một dạng trong số các phương án chỉ có phần cứng, các phương án chỉ có phần mềm, hoặc các phương án kết hợp phần mềm và phần cứng. Ngoài ra, các phương án của sáng chế có thể sử dụng một dạng của sản phẩm chương trình máy tính được thực hiện trên một hoặc nhiều vật ghi lưu trữ đọc được bởi máy tính (bao gồm bộ nhớ dạng đĩa từ, CD-ROM, bộ nhớ quang và dạng tương tự, nhưng không giới hạn ở đó) chứa mã chương trình đọc được bởi máy tính.

Các phương án của sáng chế được mô tả dựa trên các lưu đồ và/hoặc sơ đồ khối thể hiện phương pháp, thiết bị (hệ thống), và sản phẩm chương trình máy tính theo các phương án thực hiện của sáng chế. Cần hiểu rằng các lệnh chương trình máy tính có thể được sử dụng để thực hiện từng quy trình và/hoặc từng khối trên các lưu đồ và/hoặc các sơ đồ khối và sự kết hợp của quy trình và/hoặc khối trên các lưu đồ và/hoặc các sơ đồ khối. Các lệnh chương trình máy tính này có thể được sử dụng cho máy tính dùng cho mục đích chung, máy tính chuyên dụng, bộ xử lý nhúng, hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được bất kỳ khác để tạo thành một máy, sao cho các lệnh được thực hiện bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được bất kỳ khác tạo ra thiết bị để thực hiện chức năng cụ thể trong một hoặc nhiều quy trình trên các lưu đồ và/hoặc trong một hoặc nhiều khối trên các sơ đồ khối.

Các lệnh chương trình máy tính này có thể được lưu trong bộ nhớ đọc được bởi máy tính mà có thể chỉ thị cho máy tính hoặc thiết bị xử lý dữ liệu lập trình được bất kỳ khác hoạt động theo một cách cụ thể, do đó các lệnh được lưu trong bộ nhớ đọc được bởi máy tính này tạo ra công cụ bao gồm thiết bị ra lệnh. Thiết bị ra lệnh này thực hiện chức năng cụ thể trong một hoặc nhiều quy trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trên các sơ đồ khối.

Các lệnh chương trình máy tính có thể được nạp vào máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác, sao cho dãy các hoạt động và các bước được thực hiện trên máy tính hoặc thiết bị lập trình được khác, nhờ đó tạo ra quy trình thực hiện được bằng máy tính. Do đó, các lệnh được thực hiện trên máy tính hoặc thiết bị lập trình được khác tạo ra các bước để thực hiện chức năng cụ thể trong một hoặc nhiều quy trình trên các lưu đồ và/hoặc trong một hoặc nhiều khối trên các sơ đồ khối.

YÊU CẦU BẢO HỘ

1. Hệ thống xác thực dựa vào kiến trúc dựa trên dịch vụ, trong đó hệ thống xác thực này bao gồm:

phần tử mạng điều khiển thứ hai thuộc mạng di động mặt đất công cộng (PLMN) thứ hai, trong đó phần tử mạng điều khiển thứ hai bao gồm ít nhất một bộ xử lý thứ nhất được ghép với ít nhất một bộ nhớ thứ nhất lưu trữ các lệnh và được tạo cấu hình để thực thi các lệnh để khiến cho phần tử mạng điều khiển thứ hai:

thu được thông số bảo mật bằng cách thực hiện, dựa vào khoá, thuật toán được thiết lập trước đối với mã định danh của phần tử mạng chức năng mạng (NF) thứ nhất trong hệ thống xác thực, mã định danh của phần tử mạng điều khiển thứ hai, mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng NF thứ nhất, mã định danh của PLMN thứ nhất, và mã định danh của PLMN thứ hai, trong đó thuật toán được thiết lập trước là thuật toán chữ ký số, trong đó thông số bảo mật được ký số bằng cách sử dụng thuật toán chữ ký số này, và trong đó phần tử mạng NF thứ nhất thuộc PLMN thứ nhất; và

gửi thông số bảo mật đến phần tử mạng NF thứ nhất; và

phần tử mạng NF thứ hai thuộc PLMN thứ hai, trong đó phần tử mạng NF thứ hai bao gồm ít nhất một bộ xử lý thứ hai được ghép với ít nhất một bộ nhớ thứ hai lưu trữ các lệnh và được tạo cấu hình để thực thi các lệnh để khiến cho phần tử mạng NF thứ hai:

tiếp nhận thông số bảo mật từ phần tử mạng NF thứ nhất;

xác minh tính chính xác của thông số bảo mật; và

cho phép phần tử mạng NF thứ nhất truy cập phần tử mạng NF thứ hai khi phần tử mạng NF thứ hai xác minh được rằng thông số bảo mật là chính xác.

2. Hệ thống xác thực theo điểm 1, trong đó phần tử mạng NF thứ hai còn được tạo cấu

hình để từ chối việc cho phép phần tử mạng NF thứ nhất truy cập phần tử mạng NF thứ hai khi phần tử mạng NF thứ hai xác minh được rằng thông số bảo mật là không chính xác.

3. Hệ thống xác thực theo điểm 1, trong đó phần tử mạng điều khiển thứ hai còn được tạo cấu hình để gửi thông số bảo mật đến phần tử mạng NF thứ nhất qua phần tử mạng điều khiển thứ nhất thuộc PLMN thứ nhất.

4. Hệ thống xác thực theo điểm 1, trong đó khoá là khoá bí mật của phần tử mạng điều khiển thứ hai.

5. Hệ thống xác thực theo điểm 1, trong đó khoá là khoá đối xứng được chia sẻ giữa phần tử mạng điều khiển thứ hai và phần tử mạng NF thứ hai, và trong đó thông số bảo mật là mã xác thực thông điệp.

6. Hệ thống xác thực theo điểm 1, trong đó phần tử mạng điều khiển thứ hai còn được tạo cấu hình để tiếp nhận, qua phần tử mạng điều khiển thứ nhất thuộc PLMN thứ nhất, yêu cầu phát hiện từ phần tử mạng NF thứ nhất trước khi thu được thông số bảo mật.

7. Phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ, phương pháp phát hiện này bao gồm các bước:

thu được, bởi phần tử mạng điều khiển thứ hai thuộc mạng di động mặt đất công cộng (PLMN) thứ hai, thông số bảo mật bằng cách thực hiện, dựa vào khoá, thuật toán được thiết lập trước đối với mã định danh của phần tử mạng chức năng mạng (NF) thứ nhất trong hệ thống xác thực, mã định danh của phần tử mạng điều khiển thứ hai, mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng NF thứ nhất, mã định danh của PLMN thứ nhất, và mã định danh của PLMN thứ hai, trong đó thuật toán được thiết lập trước là thuật toán chữ ký số, trong đó thông số bảo mật được ký số bằng cách sử dụng thuật toán chữ ký số này, và trong đó phần tử mạng NF thứ nhất thuộc PLMN thứ nhất;

gửi, bởi phần tử mạng điều khiển thứ hai, thông số bảo mật đến phần tử mạng NF thứ nhất;

tiếp nhận, bởi phần tử mạng NF thứ hai thuộc PLMN thứ hai, thông số bảo mật từ phần tử mạng NF thứ nhất;

xác minh, bởi phần tử mạng NF thứ hai, tính chính xác của thông số bảo mật; và

cho phép, bởi phần tử mạng NF thứ hai, phần tử mạng NF thứ nhất truy cập phần tử mạng NF thứ hai khi phần tử mạng NF thứ hai xác minh được rằng thông số bảo mật là chính xác.

8. Phương pháp phát hiện theo điểm 7, còn bao gồm bước từ chối, bởi phần tử mạng NF thứ hai, việc cho phép phần tử mạng NF thứ nhất truy cập phần tử mạng NF thứ hai khi phần tử mạng NF thứ hai xác minh được rằng thông số bảo mật là không chính xác.

9. Phương pháp phát hiện theo điểm 7, trong đó bước gửi thông số bảo mật đến phần tử mạng NF thứ nhất bao gồm bước gửi, bởi phần tử mạng điều khiển thứ hai, thông số bảo mật đến phần tử mạng NF thứ nhất qua phần tử mạng điều khiển thứ nhất thuộc PLMN thứ nhất.

10. Phương pháp phát hiện theo điểm 7, trong đó khoá là khoá bí mật của phần tử mạng điều khiển thứ hai, và trong đó thông số bảo mật là chữ ký số.

11. Phương pháp phát hiện theo điểm 7, trong đó khoá là khoá đối xứng được chia sẻ giữa phần tử mạng điều khiển thứ hai và phần tử mạng NF thứ hai, và trong đó thông số bảo mật là mã xác thực thông điệp.

12. Phương pháp phát hiện theo điểm 7, còn bao gồm bước tiếp nhận, bởi phần tử mạng điều khiển thứ hai qua phần tử mạng điều khiển thứ nhất thuộc PLMN thứ nhất, yêu cầu phát hiện từ phần tử mạng NF thứ nhất trước khi thu được thông số bảo mật.

13. Phương pháp phát hiện dựa vào kiến trúc dựa trên dịch vụ, bao gồm các bước:

thu được, bởi phần tử mạng điều khiển thứ hai thuộc mạng di động mặt đất công cộng (PLMN) thứ hai, thông số bảo mật bằng cách thực hiện, dựa vào khoá, thuật toán được thiết lập trước đối với mã định danh của phần tử mạng chức năng mạng (NF) thứ nhất trong hệ thống xác thực, mã định danh của phần tử mạng điều khiển thứ hai, mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng NF thứ nhất, mã định

danh của PLMN thứ nhất, và mã định danh của PLMN thứ hai, trong đó thuật toán được thiết lập trước là thuật toán chữ ký số, trong đó thông số bảo mật được ký số bằng cách sử dụng thuật toán chữ ký số này, và trong đó phần tử mạng NF thứ nhất thuộc PLMN thứ nhất; và

gửi, bởi phần tử mạng điều khiển thứ hai, thông số bảo mật đến phần tử mạng NF thứ nhất.

14. Phương pháp phát hiện theo điểm 13, trong đó bước gửi thông số bảo mật đến phần tử mạng NF thứ nhất bao gồm bước gửi, bởi phần tử mạng điều khiển thứ hai, thông số bảo mật đến phần tử mạng NF thứ nhất qua phần tử mạng điều khiển thứ nhất thuộc PLMN thứ nhất.

15. Phương pháp phát hiện theo điểm 13, trong đó khoá là khoá bí mật của phần tử mạng điều khiển thứ hai, và trong đó thông số bảo mật là chữ ký số.

16. Phương pháp phát hiện theo điểm 13, trong đó khoá là khoá đối xứng được chia sẻ giữa phần tử mạng điều khiển thứ hai và phần tử mạng NF thứ hai, và trong đó thông số bảo mật là mã xác thực thông điệp.

17. Phần tử mạng điều khiển thứ hai, bao gồm:

ít nhất một bộ xử lý được ghép với ít nhất một bộ nhớ lưu trữ các lệnh và được tạo cấu hình để thực thi các lệnh để khiến cho phần tử mạng điều khiển thứ hai:

thu được thông số bảo mật bằng cách thực hiện, dựa vào khoá, thuật toán được thiết lập trước đối với mã định danh của phần tử mạng chức năng mạng (NF) thứ nhất, mã định danh của phần tử mạng điều khiển thứ hai, mã định danh dịch vụ của dịch vụ được yêu cầu bởi phần tử mạng NF thứ nhất, mã định danh của mạng di động mặt đất công cộng (PLMN) thứ nhất mà phần tử mạng NF thứ nhất thuộc về, và mã định danh của PLMN thứ hai mà phần tử mạng NF thứ hai thuộc về, trong đó thuật toán được thiết lập trước là thuật toán chữ ký số, trong đó thông số bảo mật được ký số bằng cách sử dụng thuật toán chữ ký số này, và trong đó phần tử mạng NF thứ hai được tạo cấu hình để cung cấp dịch vụ được yêu cầu bởi phần tử mạng NF thứ nhất; và

gửi thông số bảo mật đến phần tử mạng NF thứ nhất.

18. Phần tử mạng điều khiển thứ hai theo điểm 17, trong đó các lệnh còn khiến cho phần tử mạng điều khiển thứ hai gửi thông số bảo mật đến phần tử mạng NF thứ nhất qua phần tử mạng điều khiển thứ nhất thuộc PLMN thứ nhất.

19. Phần tử mạng điều khiển thứ hai theo điểm 17, trong đó khoá là khoá bí mật của phần tử mạng điều khiển thứ hai, và trong đó thông số bảo mật là chữ ký số.

20. Phần tử mạng điều khiển thứ hai theo điểm 17, trong đó khoá là khoá đối xứng được chia sẻ giữa phần tử mạng điều khiển thứ hai và phần tử mạng NF thứ hai, và trong đó thông số bảo mật là mã xác thực thông điệp.

21. Vật ghi đọc được bằng máy tính, trong đó vật ghi đọc được bằng máy tính này lưu trữ các lệnh, và khi các lệnh này được thực hiện trên thiết bị, thiết bị này có khả năng thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 13 đến 16.

22. Vật ghi bao gồm sản phẩm chương trình máy tính, trong đó khi sản phẩm chương trình máy tính này thực hiện trên thiết bị, thiết bị này thực thi phương pháp theo điểm bất kỳ trong số các điểm từ 13 đến 16.

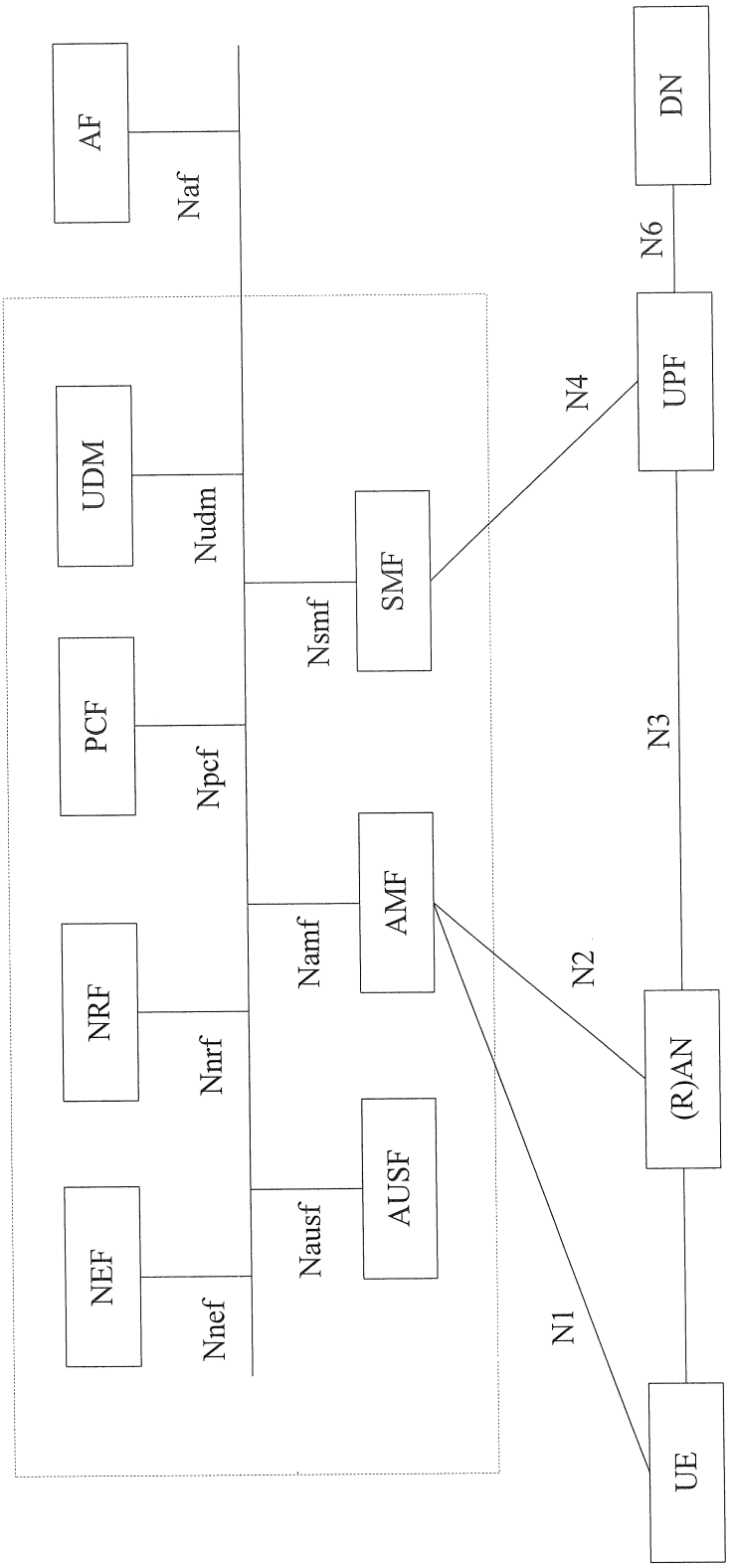
AF
Naf
UDM
Nudm
PCF
Npcf
NRF
Nnrf
NEF
Nnef
Nsmf
SMF
Namf
AMF
Nausf
AUSF
N4
UPF
N6
DN
N3
N2
(R)AN
N1
UE

FIG. 1

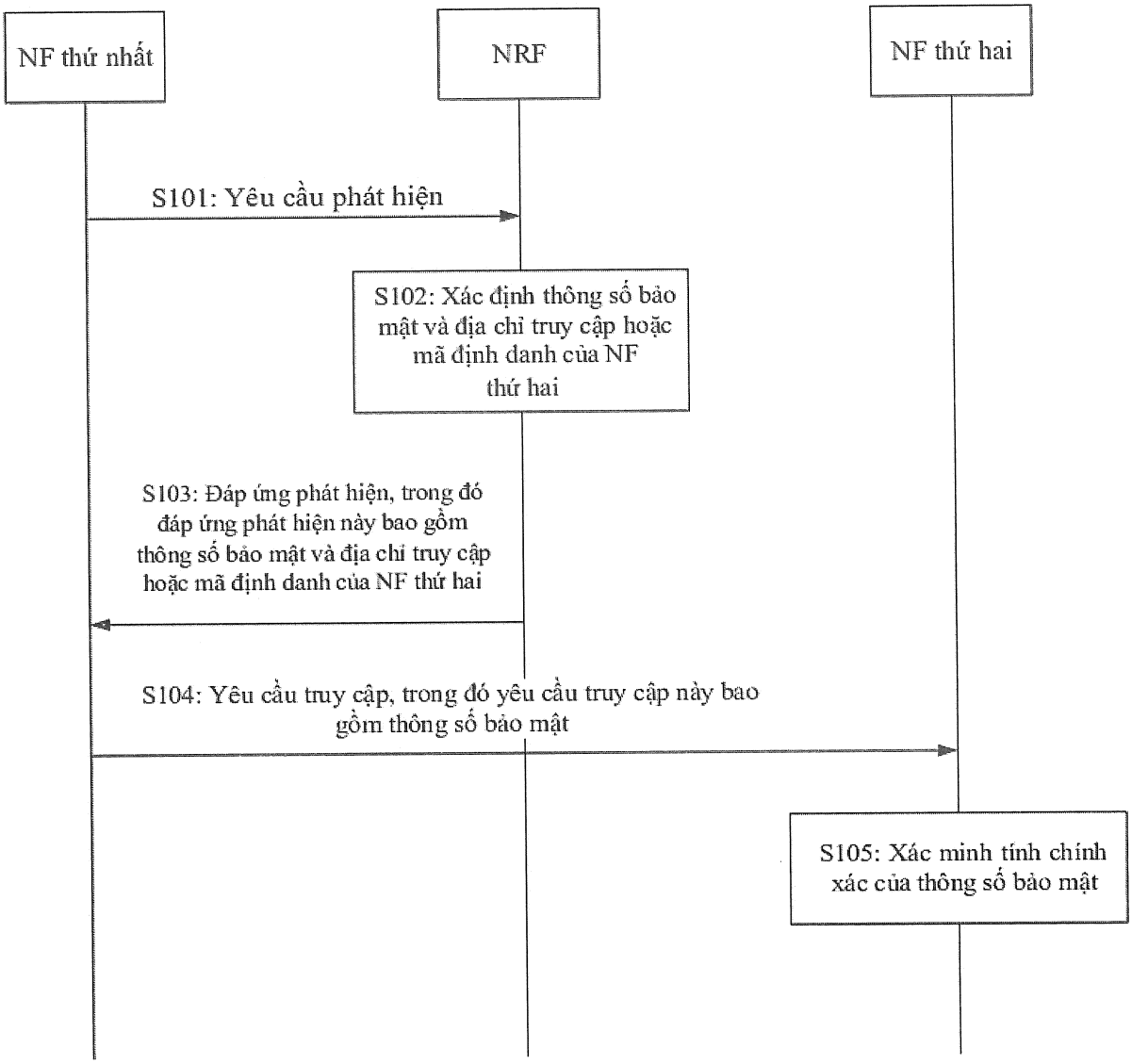
NF thứ nhất
NRF
NF thứ hai
S101: Yêu cầu phát hiện
S102: Xác định thông số bảo mật và địa chỉ truy cập hoặc mã định danh của NF thứ hai
S103: Đáp ứng phát hiện, trong đó đáp ứng phát hiện này bao gồm thông số bảo mật và địa chỉ truy cập hoặc mã định danh của NF thứ hai
S104: Yêu cầu truy cập, trong đó yêu cầu truy cập này bao gồm thông số bảo mật
S105: Xác minh tính chính xác của thông số bảo mật

FIG.2

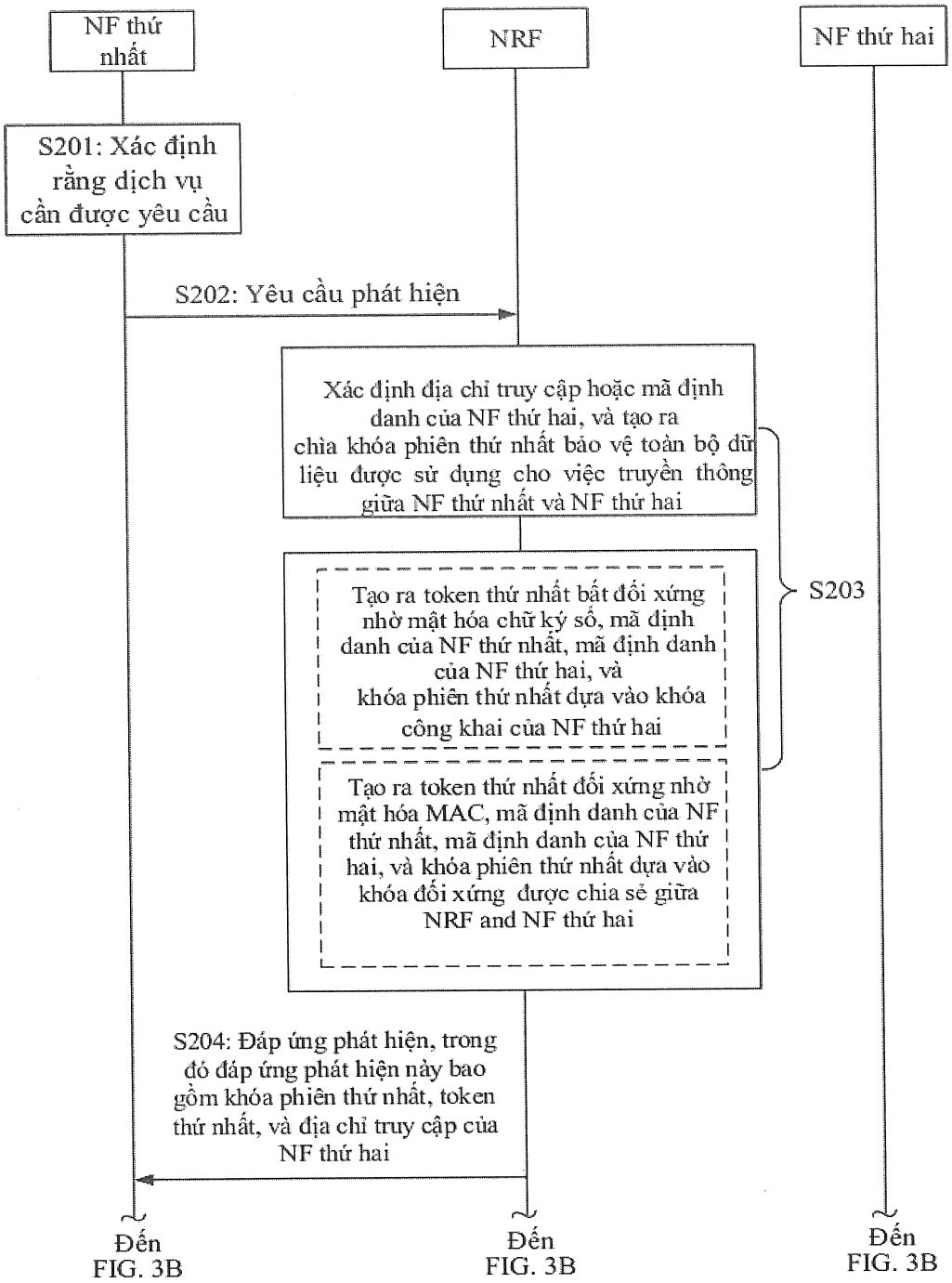
NF thứ nhất
NRF
NF thứ hai
S201: Xác định rằng dịch vụ cần được yêu cầu
S202: Yêu cầu phát hiện
Xác định địa chỉ truy cập hoặc mã định danh của NF thứ hai, và tạo ra chìa khóa phiên thứ nhất bảo vệ toàn bộ dữ liệu được sử dụng cho việc truyền thông giữa NF thứ nhất và NF thứ hai
Tạo ra token thứ nhất bất đối xứng nhờ mật hóa chữ ký số, mã định danh của NF thứ nhất, mã định danh của NF thứ hai, và khóa phiên thứ nhất dựa vào khóa công khai của NF thứ hai
Tạo ra token thứ nhất đối xứng nhờ mật hóa MAC, mã định danh của NF thứ nhất, mã định danh của NF thứ hai, và khóa phiên thứ nhất dựa vào khóa đối xứng được chia sẻ giữa NRF and NF thứ hai
S203
S204: Đáp ứng phát hiện, trong đó đáp ứng phát hiện này bao gồm khóa phiên thứ nhất, token thứ nhất, và địa chỉ truy cập của NF thứ hai
Đến FIG. 3B
Đến FIG. 3B
Đến FIG. 3B

FIG.3A

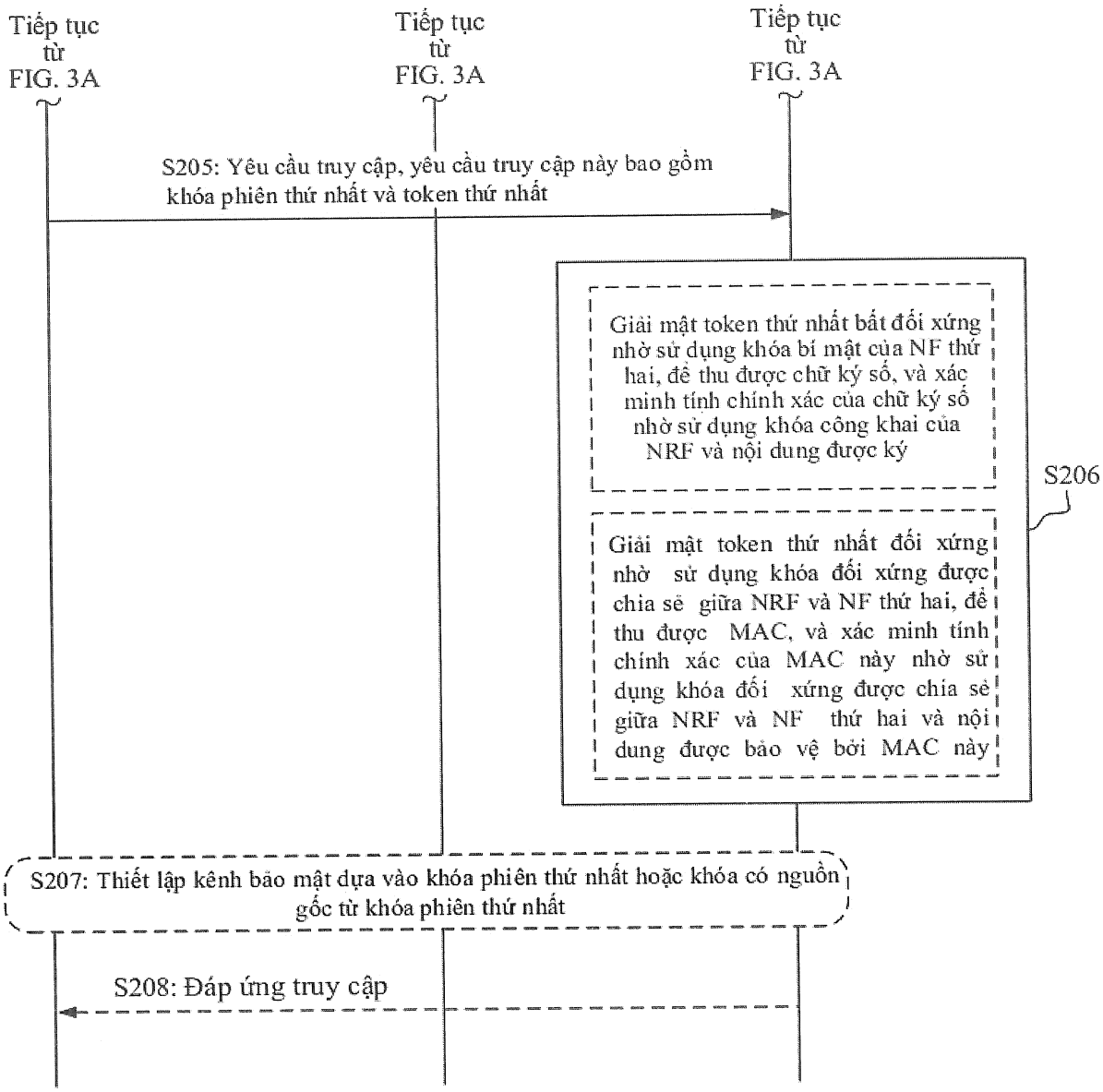
Tiếp tục từ FIG. 3A
Tiếp tục từ FIG. 3A
Tiếp tục từ FIG. 3A
S205: Yêu cầu truy cập, yêu cầu truy cập này bao gồm khóa phiên thứ nhất và token thứ nhất
Giải mật token thứ nhất bất đối xứng nhờ sử dụng khóa bí mật của NF thứ hai, để thu được chữ ký số, và xác minh tính chính xác của chữ ký số nhờ sử dụng khóa công khai của NRF và nội dung được ký
Giải mật token thứ nhất đối xứng nhờ sử dụng khóa đối xứng được chia sẻ giữa NRF và NF thứ hai, để thu được MAC, và xác minh tính chính xác của MAC này nhờ sử dụng khóa đối xứng được chia sẻ giữa NRF và NF thứ hai và nội dung được bảo vệ bởi MAC này
S206
S207: Thiết lập kênh bảo mật dựa vào khóa phiên thứ nhất hoặc khóa có nguồn gốc từ khóa phiên thứ nhất
S208: Đáp ứng truy cập

FIG.3B

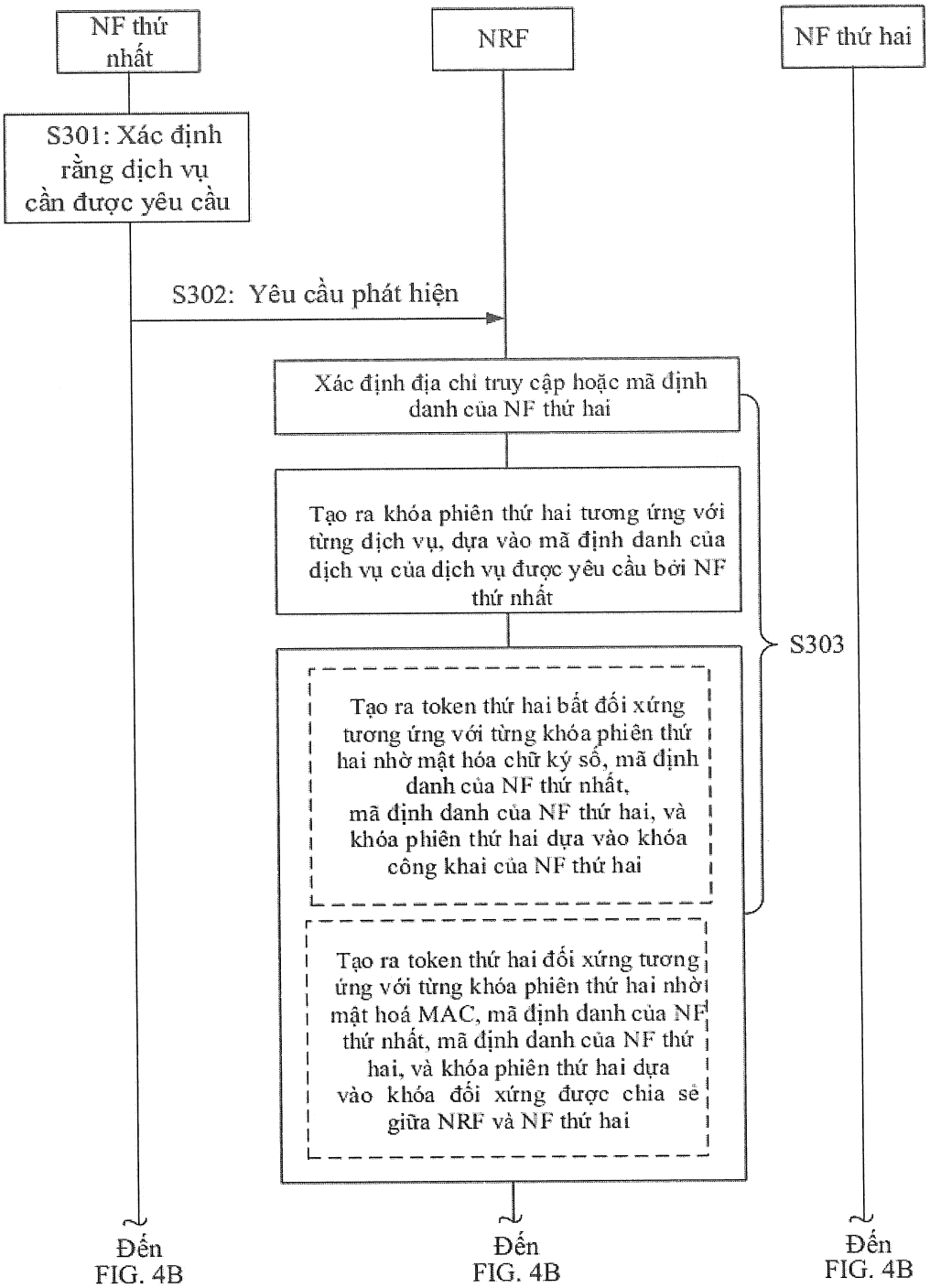
NF thứ nhất
NRF
NF thứ hai
S301: Xác định rằng dịch vụ cần được yêu cầu
S302: Yêu cầu phát hiện
Xác định địa chỉ truy cập hoặc mã định danh của NF thứ hai
Tạo ra khóa phiên thứ hai tương ứng với từng dịch vụ, dựa vào mã định danh của dịch vụ của dịch vụ được yêu cầu bởi NF thứ nhất
Tạo ra token thứ hai bất đối xứng tương ứng với từng khóa phiên thứ hai nhờ mật hóa chữ ký số, mã định danh của NF thứ nhất, mã định danh của NF thứ hai, và khóa phiên thứ hai dựa vào khóa công khai của NF thứ hai
Tạo ra token thứ hai đối xứng tương ứng với từng khóa phiên thứ hai nhờ mật hoá MAC, mã định danh của NF thứ nhất, mã định danh của NF thứ hai, và khóa phiên thứ hai dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai
S303
Đến FIG. 4B
Đến FIG. 4B
Đến FIG. 4B

FIG.4A

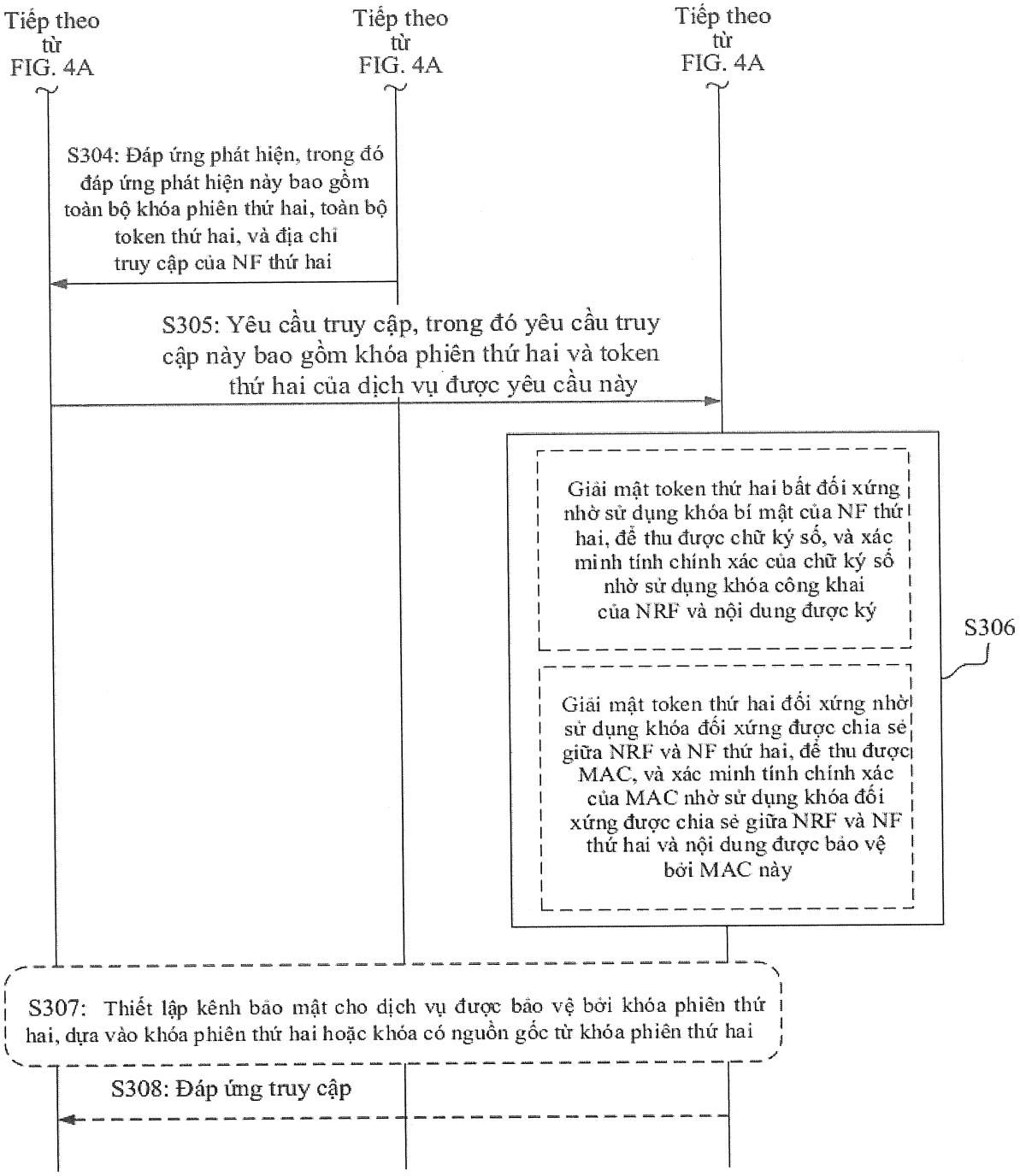
Tiếp theo từ FIG. 4A
Tiếp theo từ FIG. 4A
Tiếp theo từ FIG. 4A
S304: Đáp ứng phát hiện, trong đó đáp ứng phát hiện này bao gồm toàn bộ khóa phiên thứ hai, toàn bộ token thứ hai, và địa chỉ truy cập của NF thứ hai
S305: Yêu cầu truy cập, trong đó yêu cầu truy cập này bao gồm khóa phiên thứ hai và token thứ hai của dịch vụ được yêu cầu này
Giải mật token thứ hai bất đối xứng nhờ sử dụng khóa bí mật của NF thứ hai, để thu được chữ ký số, và xác minh tính chính xác của chữ ký số nhờ sử dụng khóa công khai của NRF và nội dung được ký
Giải mật token thứ hai đối xứng nhờ sử dụng khóa đối xứng được chia sẻ giữa NRF và NF thứ hai, để thu được MAC, và xác minh tính chính xác của MAC nhờ sử dụng khóa đối xứng được chia sẻ giữa NRF và NF thứ hai và nội dung được bảo vệ bởi MAC này
S306
S307: Thiết lập kênh bảo mật cho dịch vụ được bảo vệ bởi khóa phiên thứ hai, dựa vào khóa phiên thứ hai hoặc khóa có nguồn gốc từ khóa phiên thứ hai
S308: Đáp ứng truy cập

FIG.4B

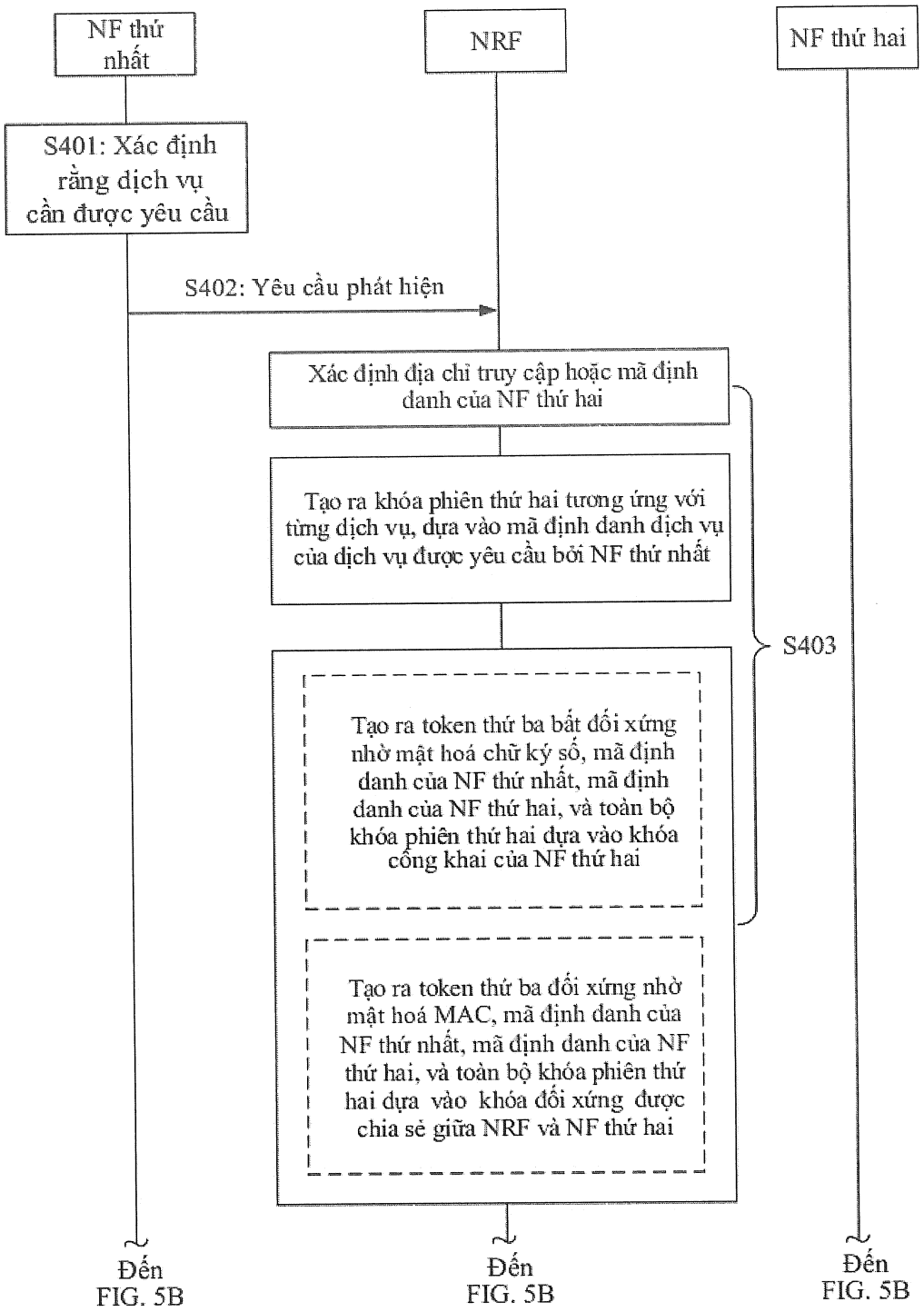
NF thứ nhất
NRF
NF thứ hai
S401: Xác định rằng dịch vụ cần được yêu cầu
S402: Yêu cầu phát hiện
Xác định địa chỉ truy cập hoặc mã định danh của NF thứ hai
Tạo ra khóa phiên thứ hai tương ứng với từng dịch vụ, dựa vào mã định danh dịch vụ của dịch vụ được yêu cầu bởi NF thứ nhất
S403
Tạo ra token thứ ba bất đối xứng nhờ mật hoá chữ ký số, mã định danh của NF thứ nhất, mã định danh của NF thứ hai, và toàn bộ khóa phiên thứ hai dựa vào khóa công khai của NF thứ hai
Tạo ra token thứ ba đối xứng nhờ mật hoá MAC, mã định danh của NF thứ nhất, mã định danh của NF thứ hai, và toàn bộ khóa phiên thứ hai dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai
Đến FIG. 5B
Đến FIG. 5B
Đến FIG. 5B

FIG.5A

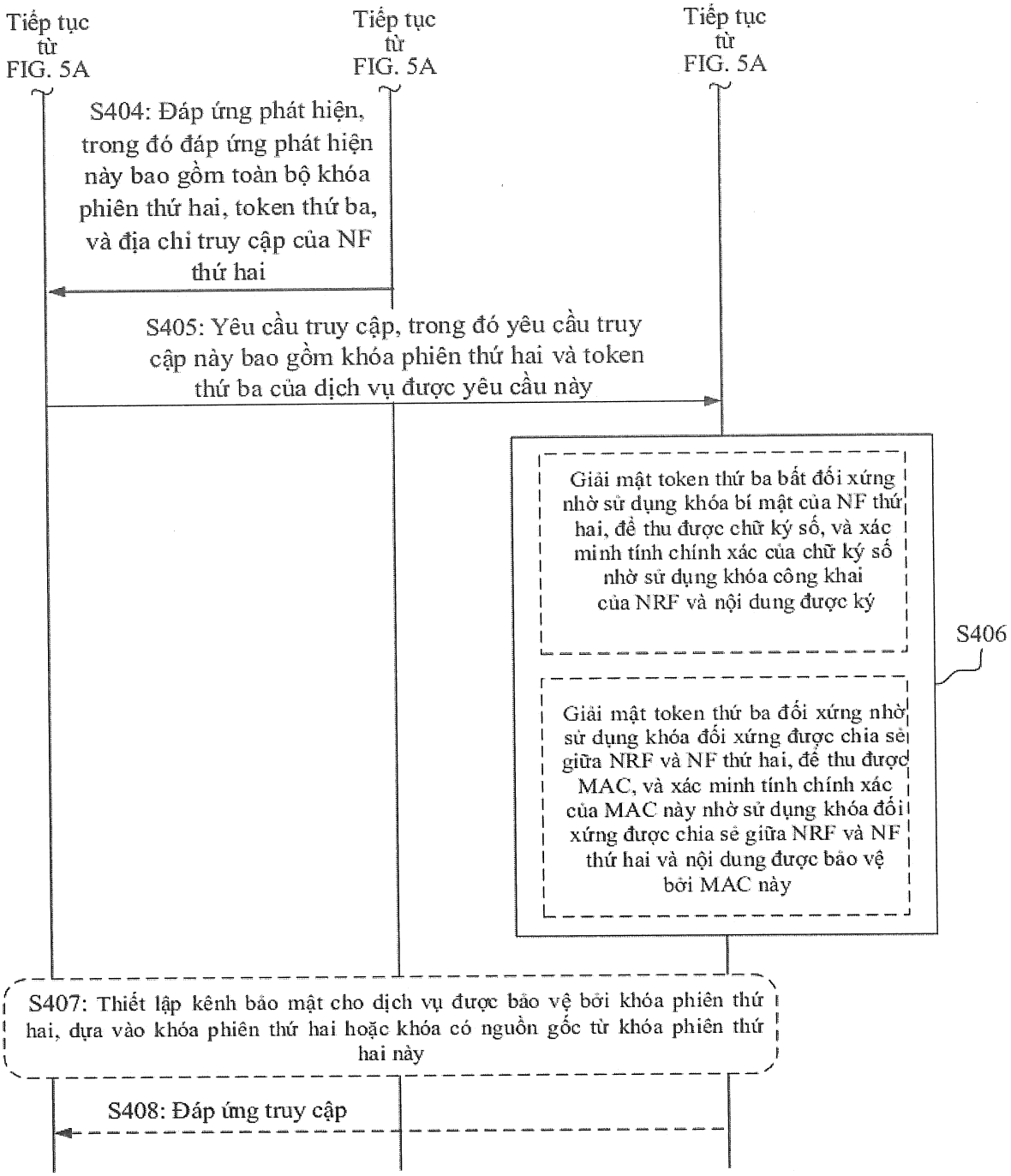
Tiếp tục từ FIG. 5A
Tiếp tục từ FIG. 5A
Tiếp tục từ FIG. 5A
S404: Đáp ứng phát hiện, trong đó đáp ứng phát hiện này bao gồm toàn bộ khóa phiên thứ hai, token thứ ba, và địa chỉ truy cập của NF thứ hai
S405: Yêu cầu truy cập, trong đó yêu cầu truy cập này bao gồm khóa phiên thứ hai và token thứ ba của dịch vụ được yêu cầu này
Giải mật token thứ ba bất đối xứng nhờ sử dụng khóa bí mật của NF thứ hai, để thu được chữ ký số, và xác minh tính chính xác của chữ ký số nhờ sử dụng khóa công khai của NRF và nội dung được ký
Giải mật token thứ ba đối xứng nhờ sử dụng khóa đối xứng được chia sẻ giữa NRF và NF thứ hai, để thu được MAC, và xác minh tính chính xác của MAC này nhờ sử dụng khóa đối xứng được chia sẻ giữa NRF và NF thứ hai và nội dung được bảo vệ bởi MAC này
S406
S407: Thiết lập kênh bảo mật cho dịch vụ được bảo vệ bởi khóa phiên thứ hai, dựa vào khóa phiên thứ hai hoặc khóa có nguồn gốc từ khóa phiên thứ hai này
S408: Đáp ứng truy cập

FIG.5B

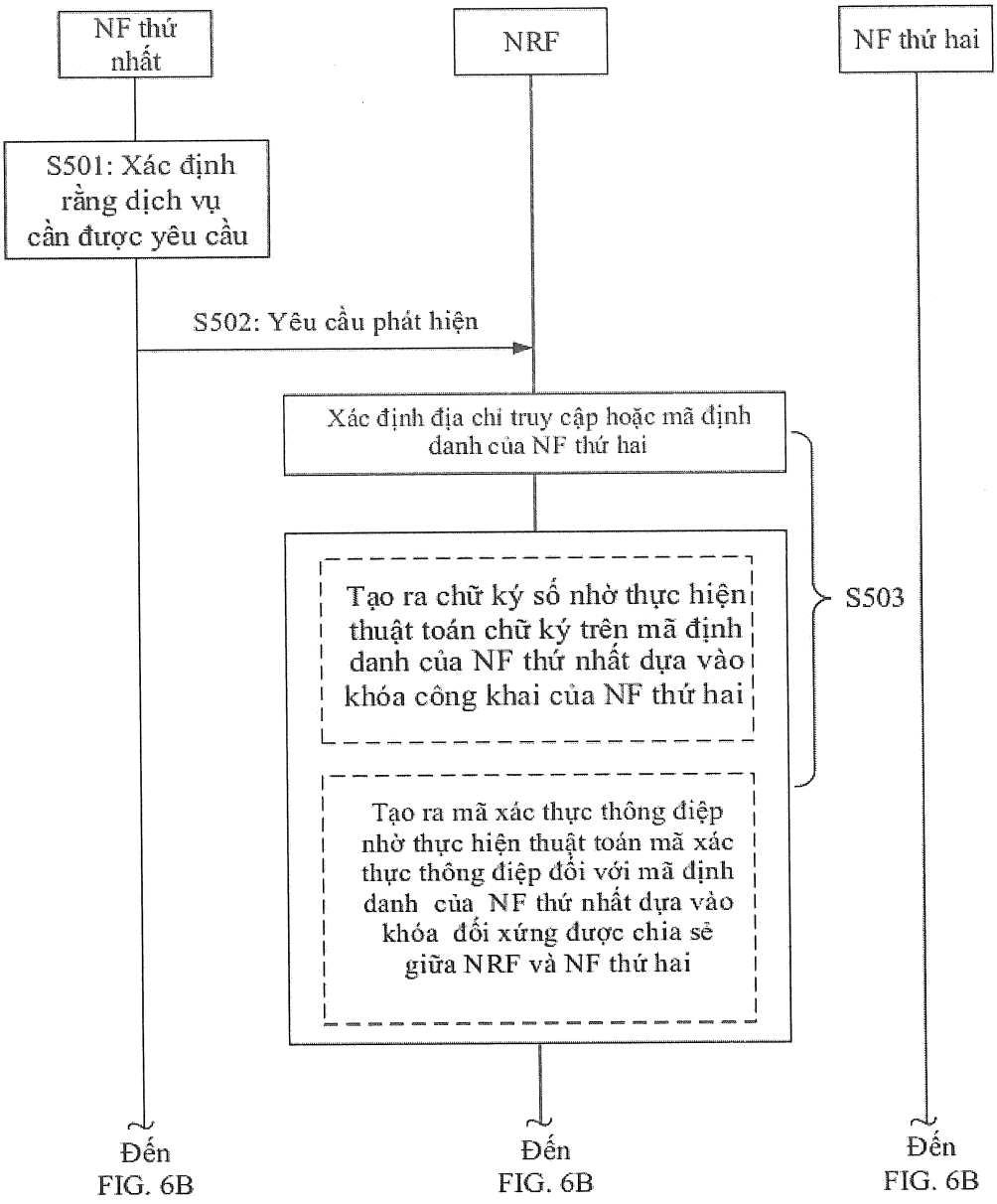
NF thứ nhất
NRF
NF thứ hai
S501: Xác định rằng dịch vụ cần được yêu cầu
S502: Yêu cầu phát hiện
Xác định địa chỉ truy cập hoặc mã định danh của NF thứ hai
Tạo ra chữ ký số nhờ thực hiện thuật toán chữ ký trên mã định danh của NF thứ nhất dựa vào khóa công khai của NF thứ hai
Tạo ra mã xác thực thông điệp nhờ thực hiện thuật toán mã xác thực thông điệp đối với mã định danh của NF thứ nhất dựa vào khóa đối xứng được chia sẻ giữa NRF và NF thứ hai
S503
Đến FIG. 6B
Đến FIG. 6B
Đến FIG. 6B

FIG.6A

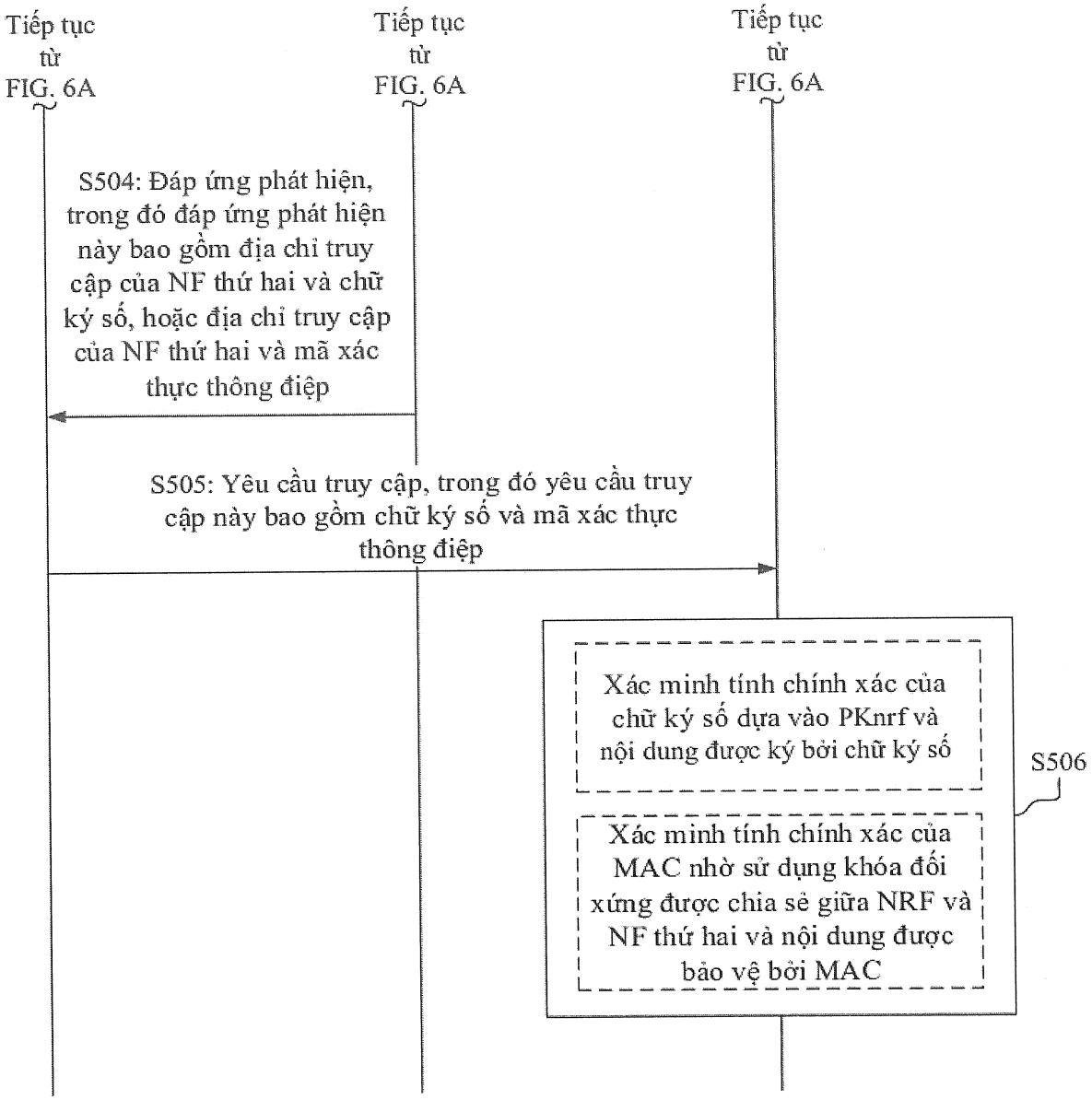
Tiếp tục từ FIG. 6A
Tiếp tục từ FIG. 6A
Tiếp tục từ FIG. 6A
S504: Đáp ứng phát hiện, trong đó đáp ứng phát hiện này bao gồm địa chỉ truy cập của NF thứ hai và chữ ký số, hoặc địa chỉ truy cập của NF thứ hai và mã xác thực thông điệp
S505: Yêu cầu truy cập, trong đó yêu cầu truy cập này bao gồm chữ ký số và mã xác thực thông điệp
Xác minh tính chính xác của chữ ký số dựa vào PKnrf và nội dung được ký bởi chữ ký số
Xác minh tính chính xác của MAC nhờ sử dụng khóa đối xứng được chia sẻ giữa NRF và NF thứ hai và nội dung được bảo vệ bởi MAC
S506

FIG.6B

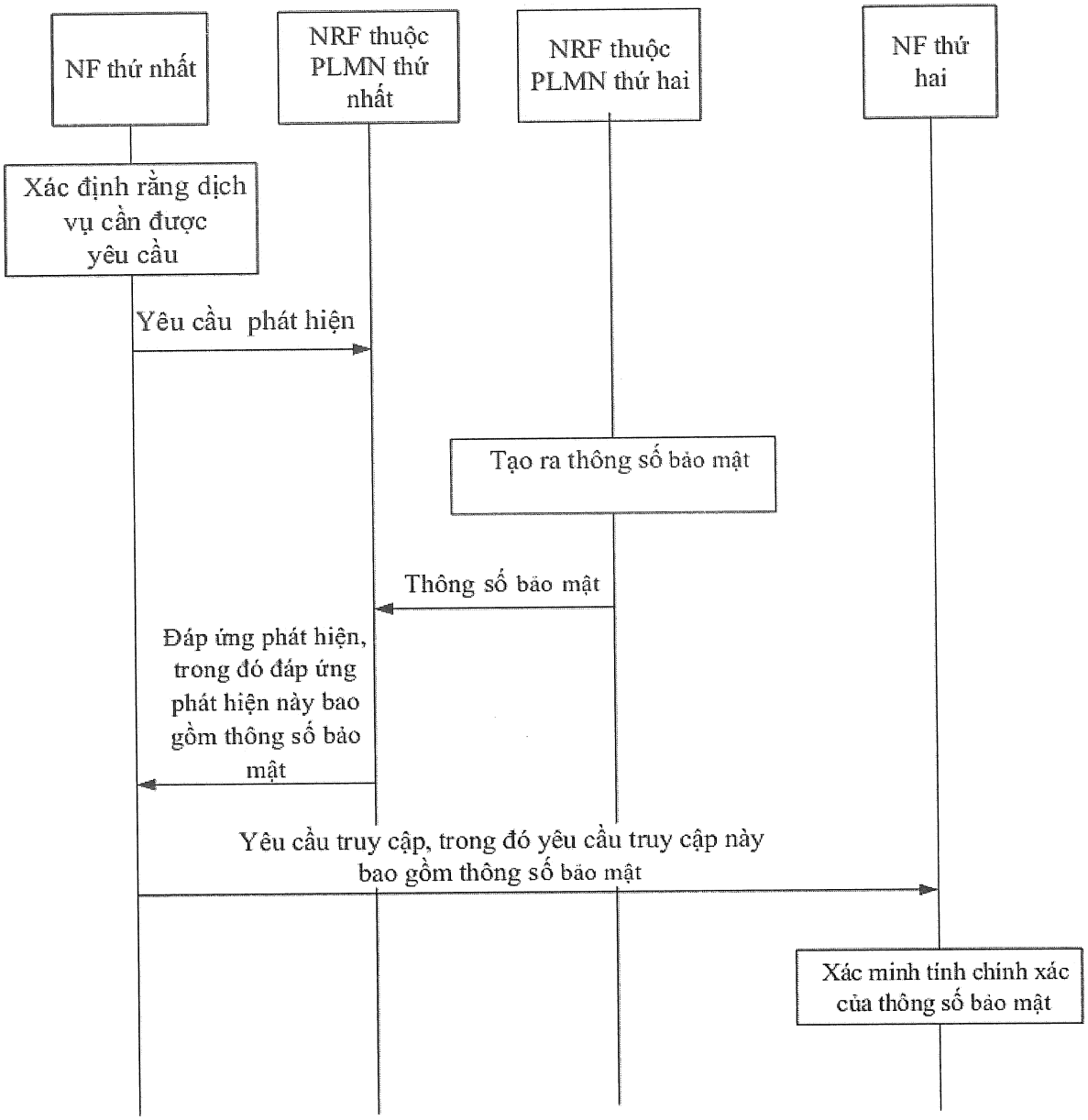
NF thứ nhất
NRF thuộc PLMN thứ nhất
NRF thuộc PLMN thứ hai
NF thứ hai
Xác định rằng dịch vụ cần được yêu cầu
Yêu cầu phát hiện
Tạo ra thông số bảo mật
Thông số bảo mật
Đáp ứng phát hiện, trong đó đáp ứng phát hiện này bao gồm thông số bảo mật
Yêu cầu truy cập, trong đó yêu cầu truy cập này bao gồm thông số bảo mật
Xác minh tính chính xác của thông số bảo mật

FIG.7

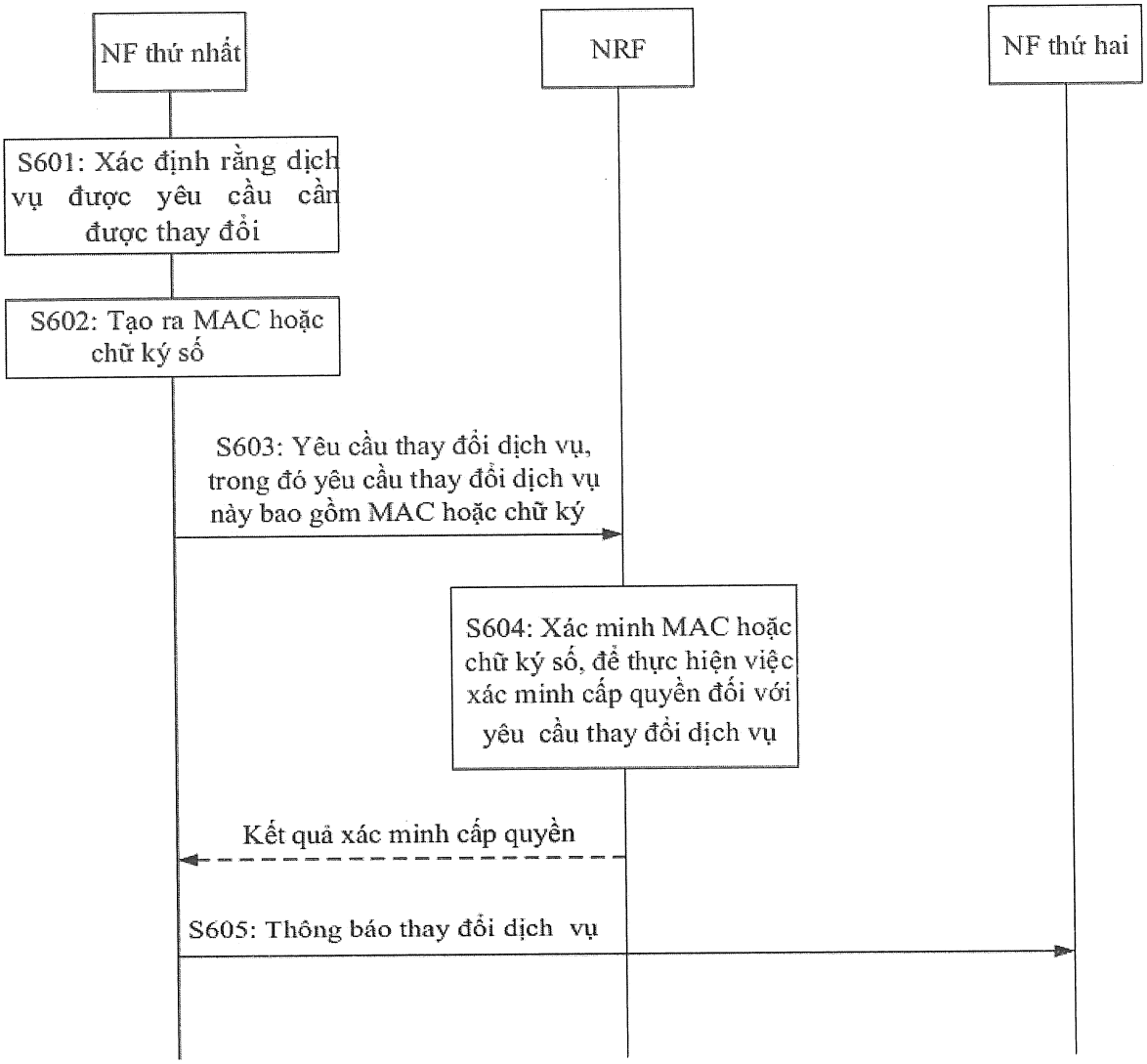
NF thứ nhất
NRF
NF thứ hai
S601: Xác định rằng dịch vụ được yêu cầu cần được thay đổi
S602: Tạo ra MAC hoặc chữ ký số
S603: Yêu cầu thay đổi dịch vụ, trong đó yêu cầu thay đổi dịch vụ này bao gồm MAC hoặc chữ ký
S604: Xác minh MAC hoặc chữ ký số, để thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ
Kết quả xác minh cấp quyền
S605: Thông báo thay đổi dịch vụ

FIG.8

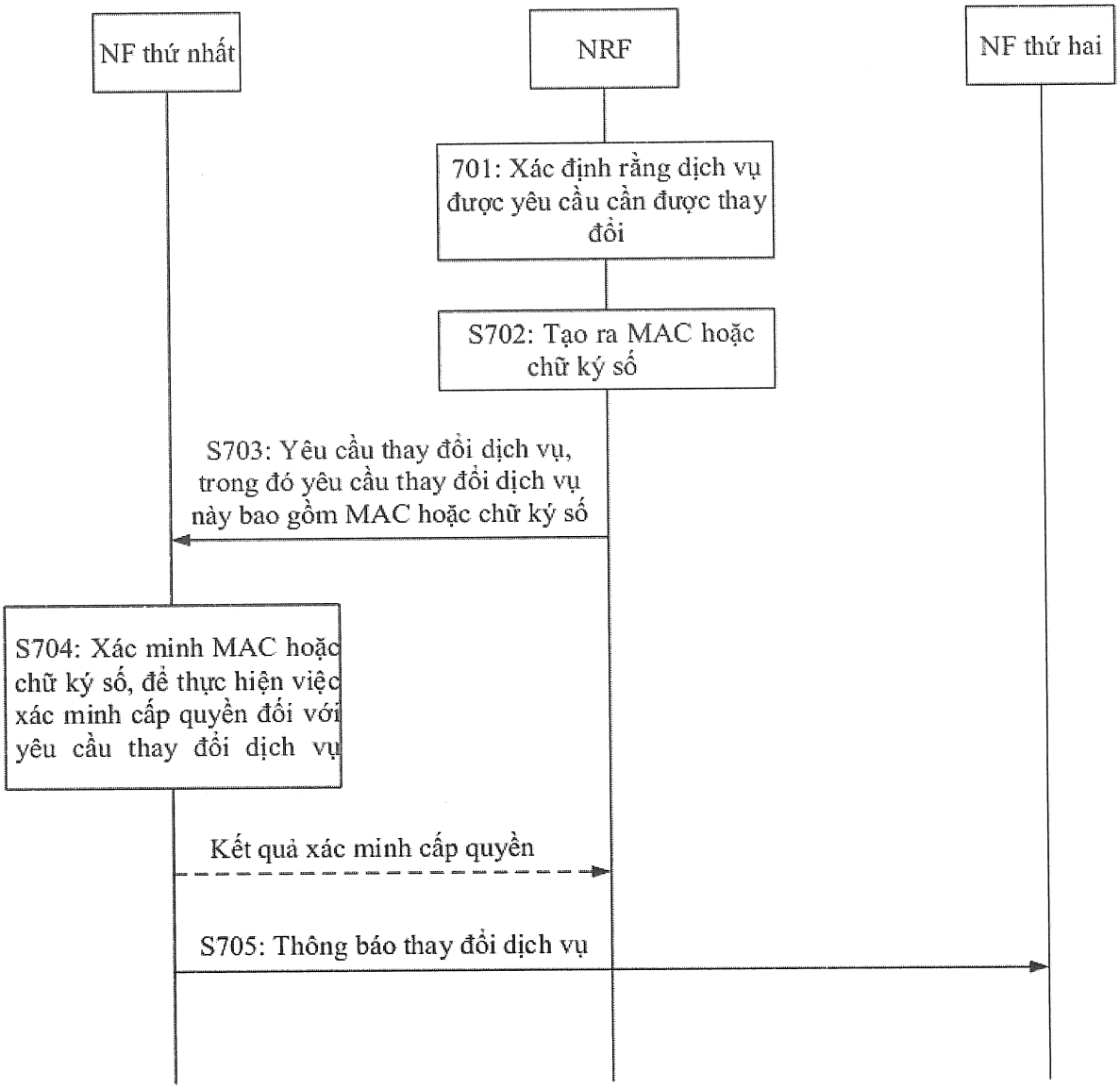
NF thứ nhất
NRF
NF thứ hai
701: Xác định rằng dịch vụ được yêu cầu cần được thay đổi
S702: Tạo ra MAC hoặc chữ ký số
S703: Yêu cầu thay đổi dịch vụ, trong đó yêu cầu thay đổi dịch vụ này bao gồm MAC hoặc chữ ký số
S704: Xác minh MAC hoặc chữ ký số, để thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ
Kết quả xác minh cấp quyền
S705: Thông báo thay đổi dịch vụ

FIG.9

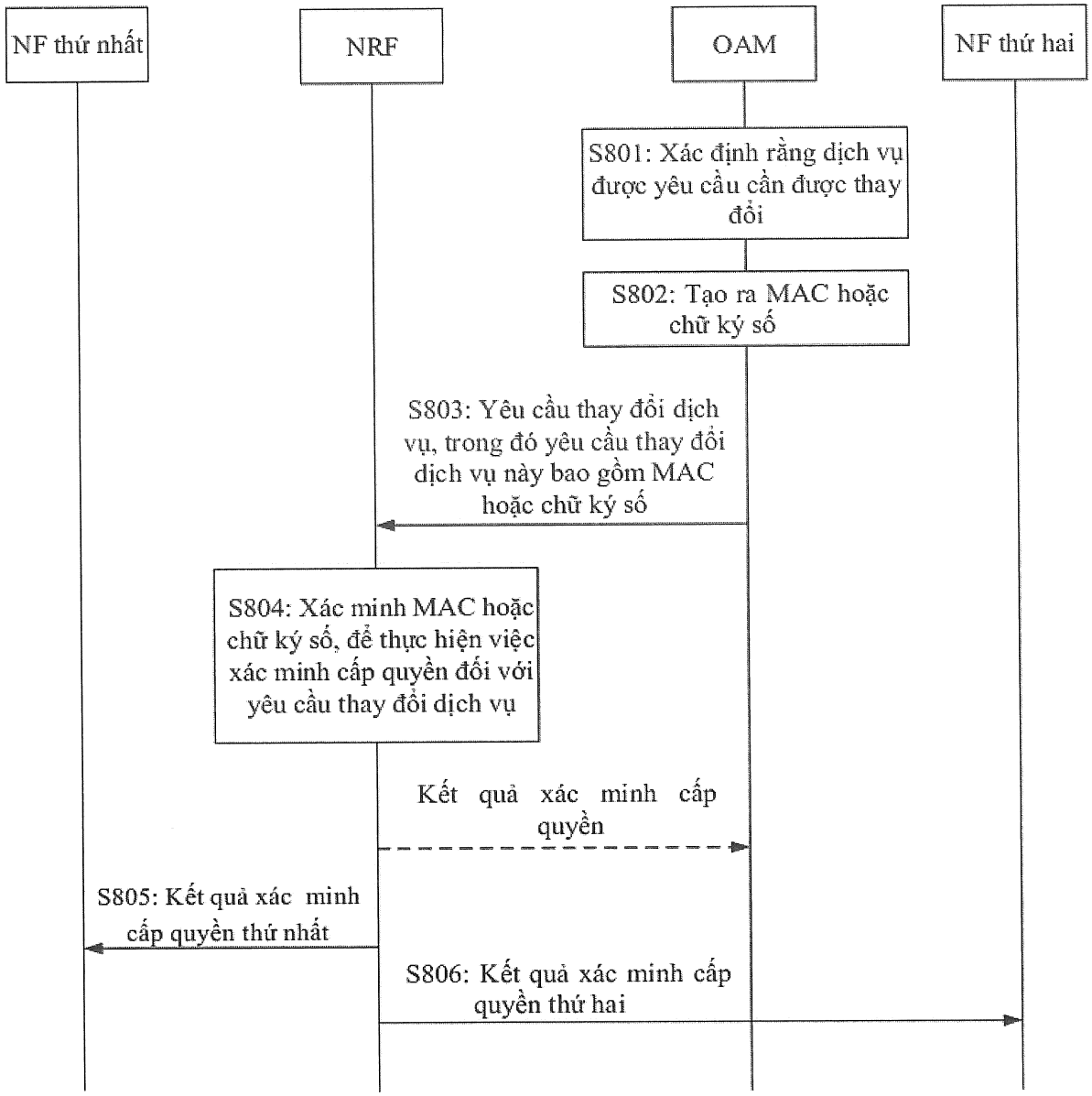
NF thứ nhất
NRF
OAM
NF thứ hai
S801: Xác định rằng dịch vụ được yêu cầu cần được thay đổi
S802: Tạo ra MAC hoặc chữ ký số
S803: Yêu cầu thay đổi dịch vụ, trong đó yêu cầu thay đổi dịch vụ này bao gồm MAC hoặc chữ ký số
S804: Xác minh MAC hoặc chữ ký số, để thực hiện việc xác minh cấp quyền đối với yêu cầu thay đổi dịch vụ
Kết quả xác minh cấp quyền
S805: Kết quả xác minh cấp quyền thứ nhất
S806: Kết quả xác minh cấp quyền thứ hai

FIG.10

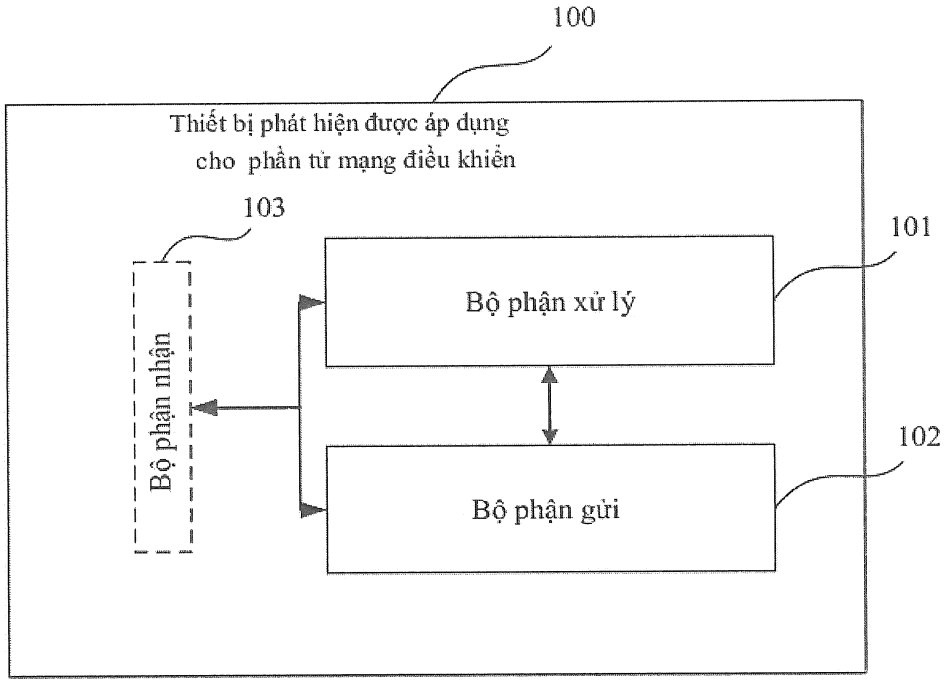
100
Thiết bị phát hiện được áp dụng
cho phần tử mạng điều khiển
103
Bộ phận nhận
101
Bộ phận xử lý
102
Bộ phận gửi

FIG.11

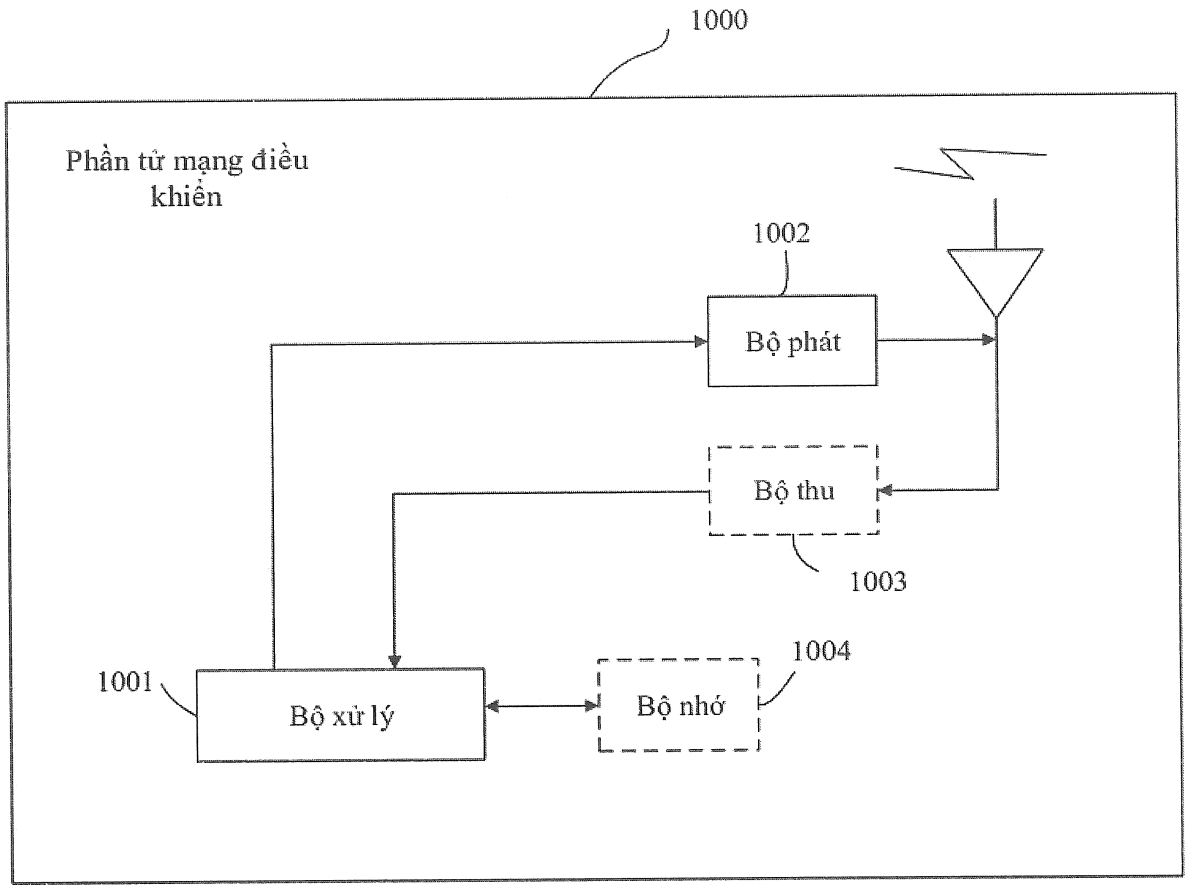
1000
Phần tử mạng điều khiển
1002
Bộ phát
Bộ thu
1003
1001
Bộ xử lý
1004
Bộ nhớ

FIG.12

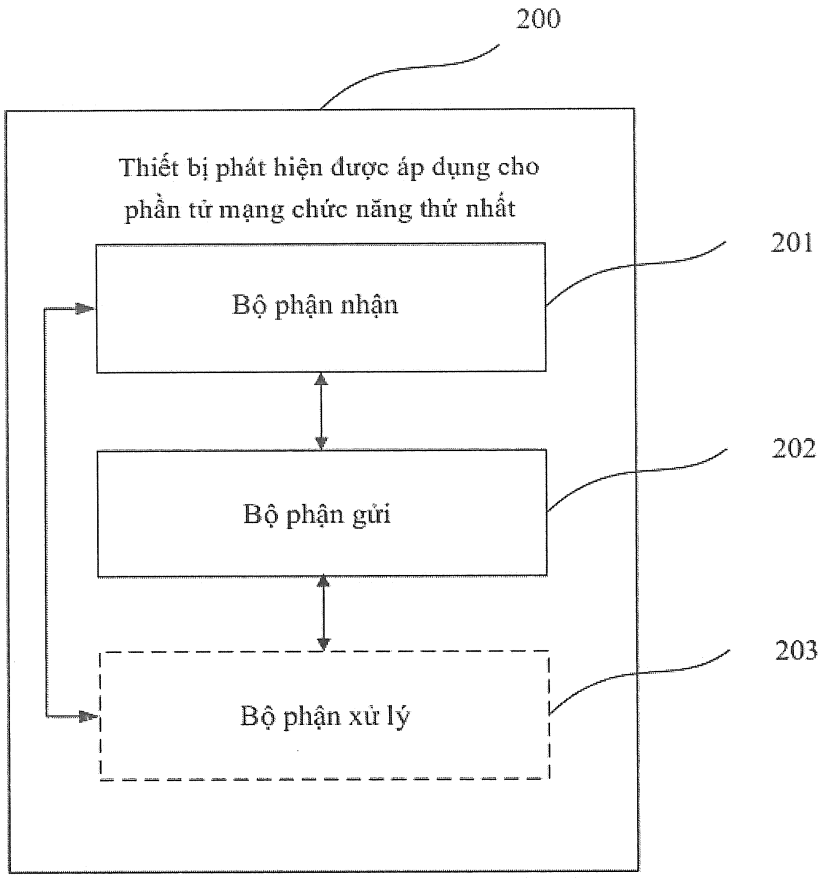
200
Thiết bị phát hiện được áp dụng cho phần tử mạng chức năng thứ nhất
201
Bộ phận nhận
202
Bộ phận gửi
203
Bộ phận xử lý

FIG.13

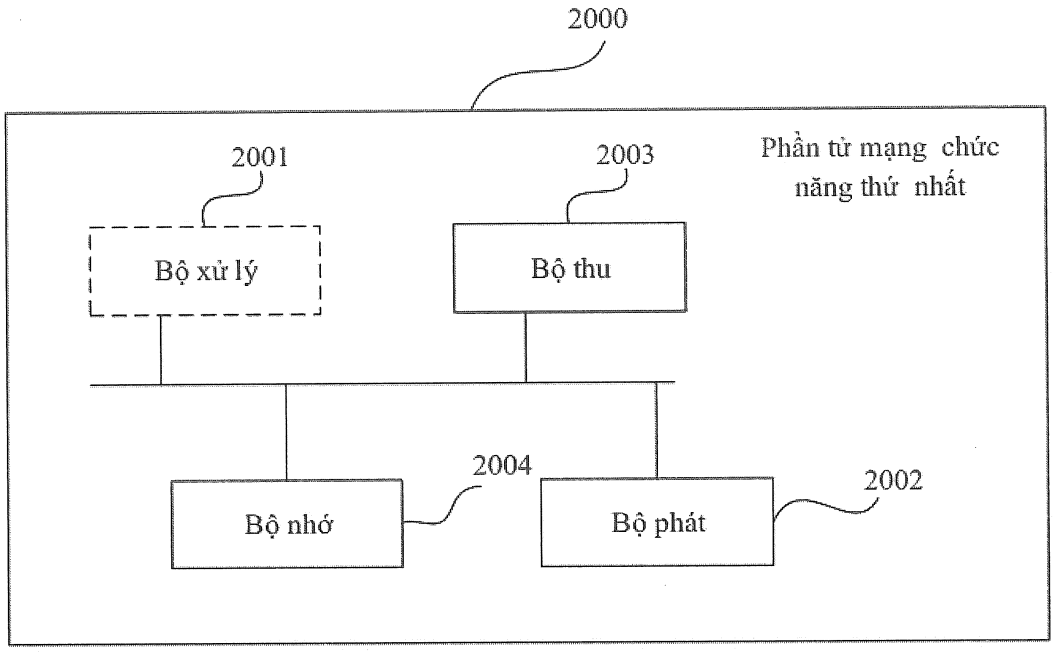
2000
2001
2003
Phần tử mạng chức năng thứ nhất
Bộ xử lý
Bộ thu
2004
2002
Bộ nhớ
Bộ phát

FIG.14

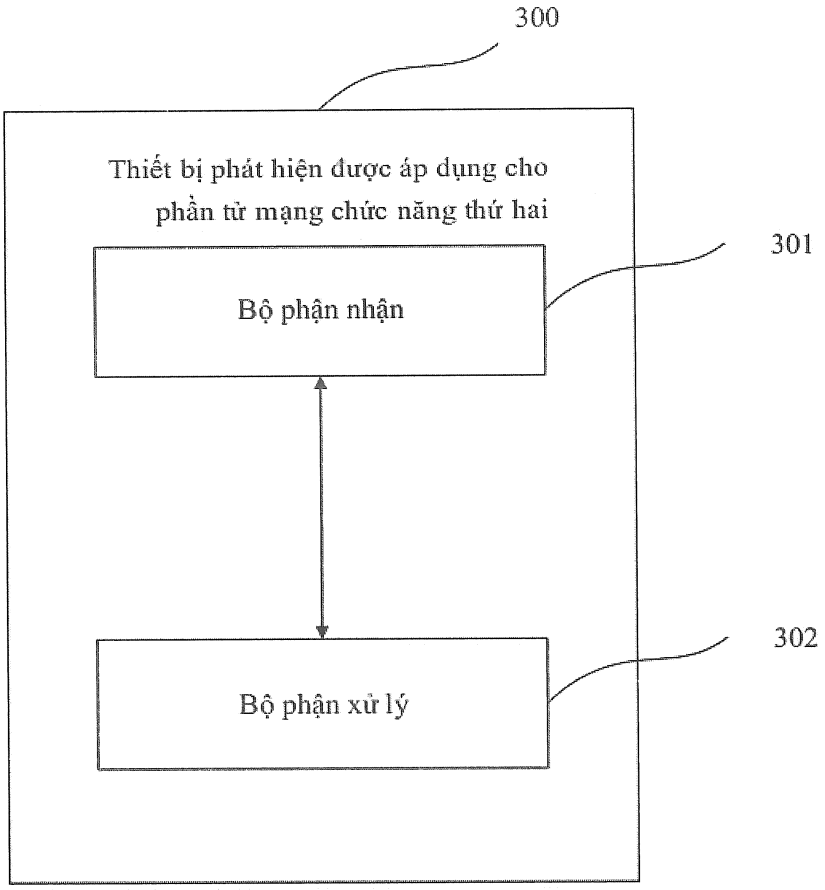
300
Thiết bị phát hiện được áp dụng cho phần tử mạng chức năng thứ hai
301
Bộ phận nhận
302
Bộ phận xử lý

FIG.15

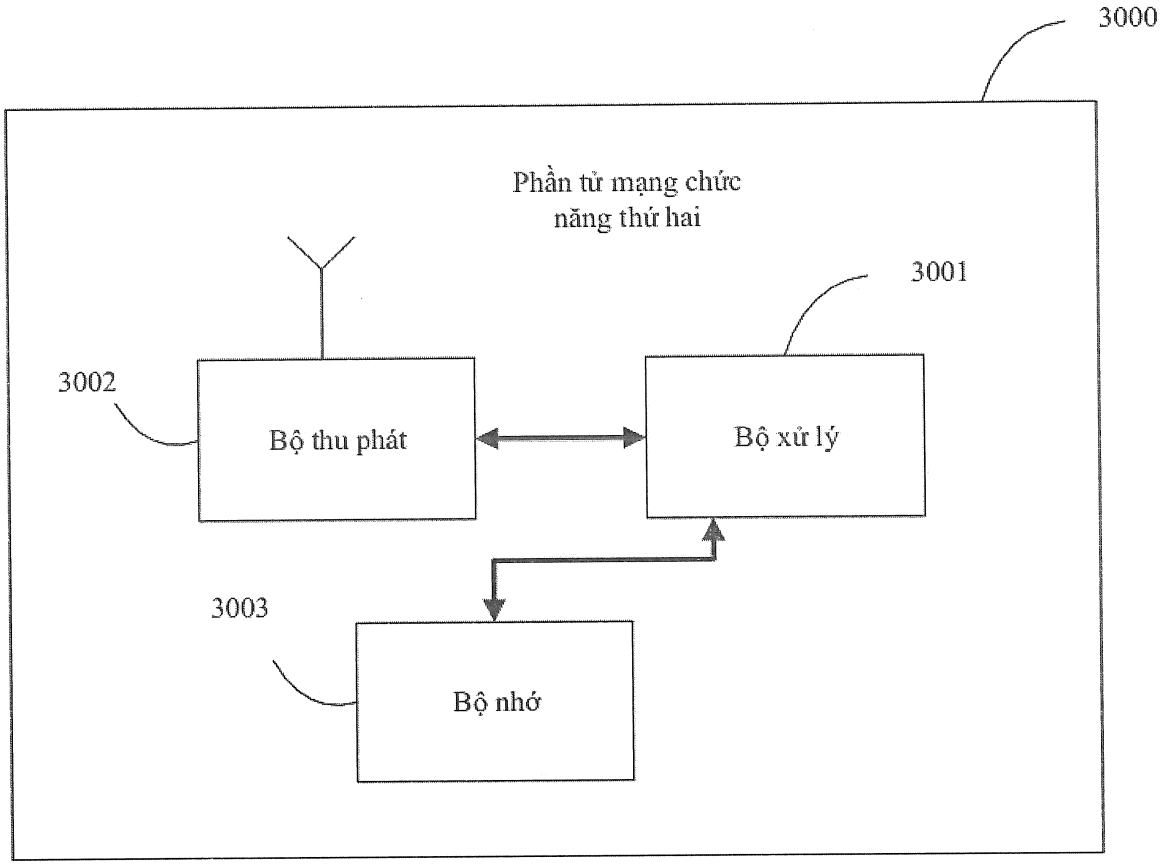
3000
Phần tử mạng chức năng thứ hai
3001
3002
Bộ thu phát
Bộ xử lý
3003
Bộ nhớ

FIG.16