(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) **1-0041884**

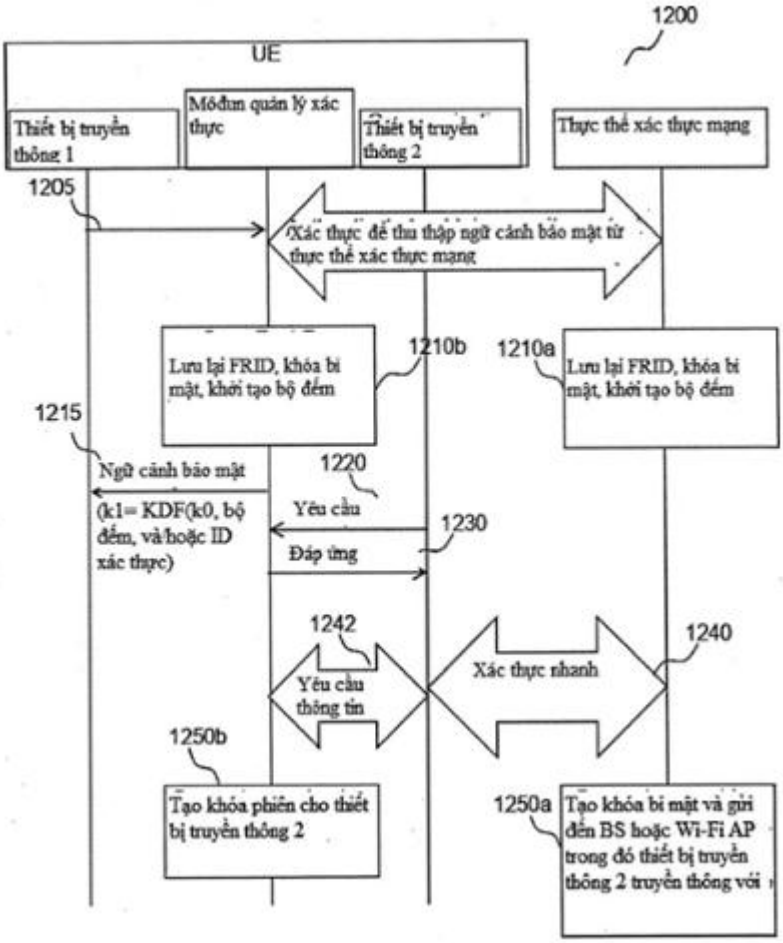
(51)[8] **H04W 12/06**; H04W 84/04; H04W 88/06; H04W 36/00

(13) **B**

(21) 1-2019-00666
(22) 28/03/2017
(86) PCT/SG2017/050163 28/03/2017
(87) WO2018/013052 18/01/2018
(30) 10201605752P 13/07/2016 SG
(45) 25/12/2024 441
(43) 25/04/2019 373A
(73) HUAWEI INTERNATIONAL PTE. LTD. (SG)
51, Changi Business Park Central 2, #07-08, The Signature Singapore 486066, Singapore
(72) WANG, Haiguang (CN); LI, Lichun (CN); KANG, Xin (CN); SHI, Jie (CN).
(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) PHƯƠNG PHÁP CHO THIẾT BỊ NGƯỜI DÙNG TRUYỀN THÔNG VỚI MẠNG LÕI VÀ THIẾT BỊ TRUYỀN THÔNG VÀ THIẾT BỊ NGƯỜI DÙNG ĐỂ TRUYỀN THÔNG TRỰC TIẾP VỚI MẠNG LÕI VÀ VẬT LƯU TRỮ MÁY TÍNH ĐỌC ĐƯỢC BẤT BIẾN

(57) Sáng chế đề xuất thiết bị người dùng (User Equipment - UE) để truyền thông trực tiếp với mạng lõi (core network - CN) bao gồm: thiết bị truyền thông thứ nhất; thiết bị truyền thông thứ hai; môđun quản lý xác thực; bộ xử lý; vật lưu trữ; các lệnh được lưu trữ trên vật lưu trữ và thực thi được bởi bộ xử lý: thực hiện xác thực thứ nhất với CN để thu thập ngữ cảnh bảo mật; truyền ngữ cảnh bảo mật từ môđun quản lý xác thực đến ít nhất một trong các thiết bị truyền thông thứ nhất và thứ hai; và thực hiện xác thực thứ hai cho một trong các thiết bị truyền thông thứ nhất và thứ hai với CN bằng cách sử dụng ngữ cảnh bảo mật từ môđun quản lý xác thực để thiết lập kết nối với CN.


1200
UE
Thiết bị truyền thông 1
Môđun quản lý xác thực
Thiết bị truyền thông 2
Thực thể xác thực mạng
1205
Xác thực để thu thập ngữ cảnh bảo mật từ thực thể xác thực mạng
Lưu lại FRID, khóa bí mật, khởi tạo bộ đếm
1210b
1210a
Lưu lại FRID, khóa bí mật, khởi tạo bộ đếm
1215
Ngữ cảnh bảo mật
(k1= KDF(k0, bộ đếm, và/hoặc ID xác thực)
1220
Yêu cầu
1230
Đáp ứng
1242
Yêu cầu thông tin
Xác thực nhanh
1240
1250b
Tạo khóa phiên cho thiết bị truyền thông 2
1250a
Tạo khóa bí mật và gửi đến BS hoặc Wi-Fi AP trong đó thiết bị truyền thông 2 truyền thông với

Lĩnh vực kỹ thuật đã được đề cập

Sáng chế đề cập đến phương pháp và hệ thống, khung làm việc xác thực thống nhất để xác thực cộng tác các thiết bị di động để truy nhập mạng lõi. Cụ thể là, sáng chế đề cập đến phương pháp và hệ thống, khung làm việc xác thực thống nhất để xác thực cộng tác giữa thiết bị di động và mạng lõi.

Tình trạng kỹ thuật của sáng chế

Trong vài năm qua, số người dùng điện thoại thông minh tăng nhanh và nhiều người dùng điện thoại di động truy nhập mạng Internet qua mạng tế bào di động. Tuy nhiên, công nghệ tế bào hiện tại chẳng hạn đa truy nhập phân chia mã băng rộng (Wideband Code Division Multiple Access – WCDMA) hoặc tiến hóa dài hạn (Long Term Evolution – LTE) không thể đáp ứng sự tăng trưởng nhanh chóng của lưu lượng Internet di động. Để thỏa mãn yêu cầu từ những người dùng di động, nhà cung cấp dịch vụ truyền thông (communications service provider – CSP) cũng được biết đến là telco hoặc các nhà vận hành viễn thông đã khai triển tiềm năng của công nghệ Wi-Fi để bù lại việc hết dung lượng.

Trong mạng tế bào, công nghệ Wi-Fi không phải là công nghệ tự nhiên. Do vậy, để tích hợp công nghệ Wi-Fi trong mạng tế bào được định nghĩa bởi 3GPP, vài đặc tả đã được định nghĩa, gồm bảo mật, bởi 3GPP. Fig.1 thể hiện kiến trúc mạng tích hợp công nghệ truy nhập Wi-Fi, gồm Wi-Fi đáng tin cậy và không đáng tin cậy. Trong phần mô tả này, truy nhập Wi-Fi tin

cậy là các trường hợp trong đó điểm truy nhập (Access Point – AP) cho thiết bị người dùng (User Equipment – UE) để kết nối với được khai triển bởi chính các nhà vận hành viễn thông. Truy nhập Wi-Fi không tin cậy là các trường hợp trong đó AP được khai triển bởi các bên thứ ba khác ngoài các nhà vận hành viễn thông.

Thông thường, để đảm bảo rằng các thiết bị và các mạng là thật, bước thứ nhất để UE truy nhập mạng xác thực lẫn nhau với mạng. Với mạng 3GPP, xác thực khóa chia sẻ trước dựa trên môđun danh tính thuê bao toàn cầu (Universe Subscriber Identity Module – USIM) được đưa vào sử dụng. Cặp khóa chia sẻ được lưu giữ ở cả UE lẫn phía mạng. Ở phía UE, chứng nhận được bảo quản trong thẻ USIM, vốn là thiết bị độc lập được nhúng vào UE. Ở phía mạng, các chứng nhận được bảo quản trong hệ thống thuê bao thường trú (Home Subscriber System – HSS). Trong quá trình xác thực, các vectơ xác thực hoặc các khóa phiên chủ được dẫn xuất từ các chứng nhận được lưu giữ. UE và mạng sử dụng vectơ xác thực để xác thực với nhau.

Với khung làm việc tích hợp 3GPP hiện tại và Wi-Fi, UE xác thực với mạng nhờ các chứng nhận được lưu giữ trong USIM. Tuy nhiên, các giao thức tạo khóa và xác thực được sử dụng bởi công nghệ LTE và Wi-Fi là khác nhau. Với công nghệ LTE, UE và máy chủ thực thể quản lý di động (Mobility Management Entity – MME) của mạng sử dụng các giao thức thỏa thuận khóa và xác thực hệ thống gói tiến hóa (Evolved Packet System Authentication and Key Agreement – EPS-AKA) để xác thực lẫn nhau. Nói cách khác, với công nghệ Wi-Fi, UE và máy chủ xác thực, ủy quyền và tính cước (Authentication, Authorization, và Accounting – AAA) của mạng sử dụng các giao thức EAP-AKA hoặc giao thức xác thực khả mở (Extensible Authentication Protocol – EAP-AKA') để xác thực lẫn nhau. Dựa trên khung làm việc hiện tại, cùng một UE phải sử dụng hai giao thức khác nhau để xác thực với cùng một mạng. Từ khía cạnh quản lý mạng, điều này

không tối ưu và không chỉ làm phức tạp công việc thiết kế và triển khai, mà còn gây lãng phí tài nguyên mạng và tăng chi phí vận hành.

Do vậy, các chuyên gia trong lĩnh vực đang cố gắng để cung cấp phương pháp xác thực tốt hơn cho mạng không đồng bộ.

Bản chất kỹ thuật của sáng chế

Các vấn đề nêu trên và các vấn đề khác được giải quyết và cải tiến trong lĩnh vực được thực hiện bởi các hệ thống và các phương pháp được cung cấp bởi các phương án thực hiện theo sáng chế. Ưu điểm thứ nhất của các phương án thực hiện của các hệ thống và các phương pháp theo sáng chế là việc các thiết bị truyền thông trong UE có thể chia sẻ ngữ cảnh bảo mật để xác thực với CN. Điều này làm giảm các bước cho UE để xác thực với CN khi một trong các thiết bị truyền thông đã thực hiện trước đó xác thực đủ với CN. Ưu điểm thứ hai của các phương án thực hiện của các hệ thống và các phương pháp theo sáng chế chính là việc tiến trình xác thực được cải thiện khi số lần tương tác được yêu cầu giữa UE và mạng lõi (core network – CN) được giảm đáng kể.

Các ưu điểm nêu trên được đề xuất bởi các phương án thực hiện của hệ thống và phương pháp của khung làm việc xác thực cho UE có ít nhất hai thiết bị truyền thông để xác thực với thực thể xác thực mạng của CN.

Khía cạnh sáng chế đề cập đến UE để truyền thông trực tiếp với CN theo cách thức sau. UE bao gồm thiết bị truyền thông thứ nhất, thiết bị truyền thông thứ hai, môđun quản lý xác thực, bộ xử lý, vật lưu trữ, các lệnh được lưu trữ trên vật lưu trữ và thực thi được bởi bộ xử lý để: thực hiện xác thực thứ nhất với CN để thu thập ngữ cảnh bảo mật, truyền ngữ cảnh bảo mật từ môđun quản lý xác thực đến ít nhất một trong các thiết bị truyền thông thứ nhất và thứ hai, và thực hiện xác thực thứ hai cho một trong các thiết bị truyền thông thứ nhất và thứ hai với CN bằng cách sử dụng ngữ cảnh bảo mật từ môđun quản lý xác thực để thiết lập kết nối với

CN. Theo phương án thực hiện sáng chế, lệnh còn bao gồm lệnh để thực hiện xác thực thứ hai bởi thiết bị truyền thông thứ nhất với CN bằng cách sử dụng ngữ cảnh bảo mật thu được, đáp lại việc ngắt kết nối giữa thiết bị truyền thông thứ nhất và CN.

Theo phương án thực hiện sáng chế, môđun quản lý mạng có thể là "máy trạm" như trong khung làm việc xác thực dựa trên EAP, vốn là thực thể đã biết để quản lý xác thực ở phía thiết bị đầu cuối.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất với CN để thu thập ngữ cảnh bảo mật bao gồm các lệnh để ra lệnh thiết bị truyền thông thứ nhất: truyền yêu cầu để FRID đến môđun quản lý xác thực; và tiếp nhận đáp ứng từ môđun quản lý xác thực.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất với CN để thu thập ngữ cảnh bảo mật bao gồm các lệnh để ra lệnh thiết bị truyền thông thứ nhất: truyền/chuyển tiếp yêu cầu đến môđun quản lý xác thực để kích hoạt thủ tục xác thực; và nhận ngữ cảnh bảo mật từ môđun quản lý xác thực.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất với CN để thu thập ngữ cảnh bảo mật bao gồm các lệnh để, đáp ứng việc tiếp nhận yêu cầu từ thiết bị truyền thông thứ nhất, ra lệnh môđun quản lý xác thực: truy xuất danh tính (ID của UE); tạo và truyền yêu cầu bao gồm ID của UE đến CN; và nhận thông điệp AKA-thử thách bao gồm số ngẫu nhiên (random number – RAND) và thẻ xác thực mạng (network authentication token – AUTN), FRID (FRID) và mã xác thực thông điệp (message authentication code – MAC) được tạo bởi CN.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất với CN để thu thập ngữ cảnh bảo mật bao gồm các lệnh để, đáp ứng việc nhận thông điệp AKA - thách thức, ra lệnh môđun quản lý xác thực: kiểm chứng tính hợp lệ của MAC bằng cách sử dụng khóa (IK) được cấp trước đó cho thiết bị truyền thông thứ nhất; đáp ứng việc MAC hợp lệ, tính

toán vectơ xác thực bằng cách sử dụng thuật toán để thu thập các tham số chẳng hạn $AUTN_{UE}$, RES, và K_{ASME}; và xác định liệu $AUTN_{UE}$ bằng AUTN.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất với CN để thu thập ngữ cảnh bảo mật bao gồm các lệnh để, đáp ứng $AUTN_{UE}$ bằng AUTN, ra lệnh môđun quản lý xác thực: tạo khóa bí mật thứ nhất, k0; thiết lập ngữ cảnh bảo mật bao gồm FRID, k0, và bộ đếm; tạo khóa bí mật thứ hai, k1, cho thiết bị truyền thông thứ nhất. Theo phương án thực hiện, khóa bí mật thứ nhất được tạo bằng cách sử dụng các chức năng dẫn xuất khóa (key derivation function – KDF) với đầu vào bao gồm ID của UE và RAND (hoặc NONCE được nhận từ mạng) trong khi khóa bí mật thứ hai được tạo bằng cách sử dụng các KDF với đầu vào bao gồm k0 và bộ đếm. Theo phương án thực hiện, khóa bí mật thứ hai, k1, được tạo bằng cách sử dụng các KDF với đầu vào bao gồm k0 và RAND (hoặc NONCE được nhận từ mạng).

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất với CN để thu thập ngữ cảnh bảo mật còn bao gồm các lệnh để ra lệnh môđun quản lý xác thực: tạo và truyền thông điệp đáp ứng AKA đến CN, thông điệp đáp ứng AKA bao gồm RES.

Theo phương án thực hiện sáng chế, lệnh để truyền ngữ cảnh bảo mật từ môđun quản lý xác thực đến ít nhất một trong các thiết bị truyền thông thứ nhất và thứ hai bao gồm các lệnh để ra lệnh môđun quản lý xác thực: nhận yêu cầu xác thực từ thiết bị truyền thông thứ hai; và tạo và truyền đáp ứng đến thiết bị truyền thông thứ hai chứa FRID.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ hai cho một trong các thiết bị truyền thông thứ nhất và thứ hai với CN bao gồm các lệnh để ra lệnh thiết bị truyền thông thứ hai: tạo và truyền yêu cầu đến CN chứa ID của UE, FRID và một cách tùy chọn, cờ, cờ này bao gồm chỉ báo rằng FRID không thuộc thiết bị truyền thông thứ hai; nhận thông điệp

yêu cầu xác thực lại AKA từ CN, thông điệp yêu cầu xác thực lại AKA bao gồm bộ đếm, nonce, FRID mới và MAC; kiểm chứng độ chuẩn của MAC và độ mới của bộ đếm; đáp ứng việc MAC hợp lệ, truyền FRID mới làm ID mới xác thực lại nhanh đến môđun quản lý xác thực và cập nhật bộ đếm cục bộ với giá trị bộ đếm nhận được cộng 1; truyền đáp ứng xác thực lại AKA đến CN, thông điệp đáp ứng xác thực lại AKA bao gồm bộ đếm được cập nhật; nhận thông điệp kết quả từ CN chỉ báo rằng xác thực là thành công; tạo các khóa để truy nhập tế bào hoặc phi tế bào; và truyền và nhận dữ liệu với CN bằng cách sử dụng các khóa. Theo phương án thực hiện, bộ đếm nhận được được xem là mới nếu giá trị này không nhỏ hơn bộ đếm được lưu trữ bởi UE. Theo phương án thực hiện khác, độ chuẩn của MAC được xác định tạo MAC với bộ đếm, nonce và FRID mới bằng cách sử dụng SK và so sánh MAC được tạo với MAC được nhận từ CN. Theo phương án thực hiện khác, môđun quản lý xác thực tạo ngữ cảnh bảo mật mới cho thiết bị truyền thông thứ hai nếu FRID không thuộc thiết bị truyền thông thứ hai.

Theo khía cạnh khác của sáng chế, UE để truyền thông trực tiếp với CN được đề xuất theo cách thức sau. UE bao gồm thiết bị truyền thông thứ nhất, thiết bị truyền thông thứ hai, môđun quản lý xác thực, bộ xử lý, vật lưu trữ, các lệnh được lưu trữ trên vật lưu trữ và thực thi được bởi bộ xử lý: thực hiện xác thực thứ nhất bởi thiết bị truyền thông thứ nhất với CN để thu thập ngữ cảnh bảo mật cho thiết bị truyền thông thứ nhất; truyền một phần ngữ cảnh bảo mật từ môđun quản lý xác thực đến thiết bị truyền thông thứ hai; và thực hiện xác thực thứ hai bởi thiết bị truyền thông thứ hai với CN bằng cách sử dụng ngữ cảnh bảo mật từ môđun quản lý xác thực. Theo phương án thực hiện, các lệnh còn bao gồm lệnh để thực hiện xác thực thứ hai bởi thiết bị truyền thông thứ nhất với CN bằng cách sử dụng ngữ cảnh bảo mật thu được.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ

nhất bởi thiết bị truyền thông thứ nhất với CN để thu thập ngữ cảnh bảo mật cho thiết bị truyền thông thứ nhất bao gồm các lệnh để ra lệnh thiết bị truyền thông thứ nhất: truyền yêu cầu để FRID đến môđun quản lý xác thực; tiếp nhận đáp ứng từ môđun quản lý xác thực.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất bởi thiết bị truyền thông thứ nhất với CN để thu thập ngữ cảnh bảo mật cho thiết bị truyền thông thứ nhất bao gồm các lệnh để, đáp ứng lệnh đáp ứng từ môđun quản lý xác thực không chứa FRID, ra lệnh thiết bị truyền thông thứ nhất: truy xuất danh tính (ID của UE); tạo và truyền yêu cầu bao gồm ID của UE đến CN; nhận thông điệp AKA-thử thách bao gồm RAND và AUTN, FRID và MAC được tạo bởi CN.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất bởi thiết bị truyền thông thứ nhất với CN để thu thập ngữ cảnh bảo mật cho thiết bị truyền thông thứ nhất bao gồm các lệnh để, đáp ứng việc nhận thông điệp AKA - thách thức, ra lệnh thiết bị truyền thông thứ nhất: kiểm chứng tính hợp lệ của MAC bằng cách sử dụng IK được cấp trước đó cho thiết bị truyền thông thứ nhất; đáp ứng việc MAC hợp lệ, tính toán vectơ xác thực bằng cách sử dụng thuật toán AKA để thu thập $AUTN_{UE}$, RES, và khóa, theo một phương án thực hiện, khóa này là K_{ASME}; xác định liệu $AUTN_{UE}$ bằng AUTN; và đáp ứng $AUTN_{UE}$ bằng AUTN, dẫn xuất các khóa bí mật để truy nhập tế bào hoặc truy nhập phi tế bào.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất bởi thiết bị truyền thông thứ nhất với CN để thu thập ngữ cảnh bảo mật cho thiết bị truyền thông thứ nhất còn bao gồm các lệnh để ra lệnh thiết bị truyền thông thứ nhất: truyền ngữ cảnh bảo mật đến môđun quản lý xác thực, ngữ cảnh bảo mật bao gồm FRID, các khóa bí mật, và bộ đếm; và tạo và truyền thông điệp đáp ứng AKA đến CN, thông điệp đáp ứng AKA bao gồm RES. Theo phương án thực hiện, các khóa bí mật được dẫn xuất bằng cách sử dụng các KDF với đầu vào bao gồm ID của UE và RAND.

Theo phương án thực hiện sáng chế, lệnh để truyền ngữ cảnh bảo mật từ môđun quản lý xác thực đến thiết bị truyền thông thứ hai bao gồm các lệnh để ra lệnh môđun quản lý xác thực: nhận yêu cầu cho FRID từ thiết bị truyền thông thứ hai; và tạo và truyền đáp ứng đến thiết bị truyền thông thứ hai chứa FRID.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ hai bởi thiết bị truyền thông thứ hai với CN bằng cách sử dụng ngữ cảnh bảo mật từ thiết bị truyền thông thứ nhất bao gồm các lệnh để, đáp ứng việc nhận FRID từ môđun quản lý xác thực, ra lệnh thiết bị truyền thông thứ hai: tạo và truyền yêu cầu đến CN chứa ID của UE, FRID và cờ, cờ bao gồm chỉ báo rằng FRID không thuộc thiết bị truyền thông thứ hai; nhận thông điệp yêu cầu xác thực lại AKA từ CN, thông điệp yêu cầu xác thực lại AKA bao gồm bộ đếm, nonce, FRID mới và MAC; kiểm chứng độ chuẩn của MAC và độ mới của bộ đếm; đáp ứng việc MAC hợp lệ, truyền FRID mới làm ID mới xác thực lại nhanh đến môđun quản lý xác thực và cập nhật bộ đếm cục bộ với giá trị bộ đếm nhận được cộng 1; truyền đáp ứng xác thực lại AKA đến CN, thông điệp đáp ứng xác thực lại AKA bao gồm bộ đếm được cập nhật; nhận thông điệp kết quả từ CN chỉ báo rằng xác thực là thành công; tạo các khóa để truy nhập tế bào hoặc phi tế bào; và truyền và nhận dữ liệu với CN bằng cách sử dụng các khóa. Theo phương án thực hiện, bộ đếm nhận được được xem là mới nếu giá trị này không nhỏ hơn bộ đếm được lưu trữ bởi UE. Theo phương án thực hiện, độ chuẩn của MAC được xác định tạo MAC với bộ đếm, nonce và FRID mới sử dụng SK và so sánh MAC được tạo với MAC được nhận từ CN.

Theo khía cạnh khác của sáng chế, UE để truyền thông trực tiếp với CN được đề xuất theo cách thức sau. UE bao gồm thiết bị truyền thông thứ nhất, thiết bị truyền thông thứ hai, bộ xử lý, vật lưu trữ, các lệnh được lưu trữ trên vật lưu trữ và thực thi được bởi bộ xử lý: thực hiện xác thực thứ nhất bởi thiết bị truyền thông thứ nhất với CN để thu thập ngữ cảnh bảo

mật cho thiết bị truyền thông thứ nhất; truyền ngữ cảnh bảo mật từ thiết bị truyền thông thứ nhất đến thiết bị truyền thông thứ hai; và thực hiện xác thực thứ hai bởi thiết bị truyền thông thứ hai với CN bằng cách sử dụng ngữ cảnh bảo mật từ thiết bị truyền thông thứ nhất. Theo phương án thực hiện, các lệnh còn bao gồm lệnh thực hiện xác thực thứ hai bởi thiết bị truyền thông thứ nhất với CN bằng cách sử dụng ngữ cảnh bảo mật thu được, đáp lại việc ngắt kết nối giữa thiết bị truyền thông thứ nhất và CN.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất bởi thiết bị truyền thông thứ nhất với CN để thu thập ngữ cảnh bảo mật cho thiết bị truyền thông thứ nhất bao gồm các lệnh để ra lệnh thiết bị truyền thông thứ nhất: truyền yêu cầu để FRID đến thiết bị truyền thông thứ hai; tiếp nhận đáp ứng từ thiết bị truyền thông thứ hai.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất bởi thiết bị truyền thông thứ nhất với CN để thu thập ngữ cảnh bảo mật cho thiết bị truyền thông thứ nhất bao gồm các lệnh để, đáp ứng lệnh đáp ứng từ thiết bị truyền thông thứ hai không chứa FRID, ra lệnh thiết bị truyền thông thứ nhất: truy xuất danh tính (ID của UE); tạo và truyền yêu cầu bao gồm ID của UE đến CN; nhận thông điệp AKA-thử thách bao gồm RAND và AUTN, FRID và MAC được tạo bởi CN; kiểm chứng tính hợp lệ của MAC bằng cách sử dụng IK được cấp trước đó cho thiết bị truyền thông thứ nhất; đáp ứng việc MAC hợp lệ, tính toán vectơ xác thực bằng cách sử dụng thuật toán AKA để thu thập $AUTN_{UE}$, RES, và K_{ASME}; xác định liệu $AUTN_{UE}$ có bằng AUTN hay không, đáp ứng AUTNUE bằng AUTN, dẫn xuất các khóa bí mật để truy nhập tế bào hoặc truy nhập phi tế bào; lưu trữ ngữ cảnh bảo mật bao gồm FRID, các khóa bí mật, và bộ đếm; và tạo và truyền thông điệp đáp ứng AKA đến CN, thông điệp đáp ứng AKA bao gồm RES. Theo phương án thực hiện, các khóa bí mật được dẫn xuất bằng cách sử dụng các KDF với đầu vào bao gồm ID của UE và RAND.

Theo phương án thực hiện sáng chế, lệnh để truyền ngữ cảnh bảo mật từ thiết bị truyền thông thứ nhất đến thiết bị truyền thông thứ hai bao gồm các lệnh để ra lệnh thiết bị truyền thông thứ nhất: nhận yêu cầu cho FRID từ thiết bị truyền thông thứ hai; và tạo và truyền đáp ứng đến thiết bị truyền thông thứ hai chứa FRID.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ hai bởi thiết bị truyền thông thứ hai với CN bằng cách sử dụng ngữ cảnh bảo mật từ thiết bị truyền thông thứ nhất bao gồm các lệnh để, đáp ứng việc nhận FRID từ thiết bị truyền thông thứ nhất, ra lệnh thiết bị truyền thông thứ hai: tạo và truyền yêu cầu đến CN chứa ID của UE, FRID và cờ, cờ bao gồm chỉ báo rằng FRID không thuộc thiết bị truyền thông thứ hai; nhận thông điệp yêu cầu xác thực lại AKA từ CN, thông điệp yêu cầu xác thực lại AKA bao gồm bộ đếm, nonce, FRID mới và MAC; kiểm chứng độ chuẩn của MAC và độ mới của bộ đếm; đáp ứng việc MAC hợp lệ, lưu trữ FRID mới làm ID mới xác thực lại nhanh trong ngữ cảnh bảo mật và cập nhật bộ đếm cục bộ với giá trị bộ đếm nhận được cộng 1; truyền đáp ứng xác thực lại AKA đến CN, thông điệp đáp ứng xác thực lại AKA bao gồm bộ đếm được cập nhật; nhận thông điệp kết quả từ CN chỉ báo rằng xác thực là thành công; tạo các khóa để truy nhập tế bào hoặc phi tế bào; và truyền và nhận dữ liệu với CN bằng cách sử dụng các khóa. Theo phương án thực hiện, bộ đếm nhận được được xem là mới nếu giá trị này không nhỏ hơn bộ đếm được lưu trữ bởi UE. Theo phương án thực hiện, độ chuẩn của MAC được xác định tạo MAC với bộ đếm, nonce và FRID mới sử dụng SK và so sánh MAC được tạo với MAC được nhận từ CN.

Theo khía cạnh khác của sáng chế, phương pháp xác thực cho UE có thiết bị truyền thông thứ nhất và thiết bị truyền thông thứ hai để xác thực với thực thể xác thực mạng của CN được đề xuất theo cách thức sau. Phương pháp xác thực trước hết xác thực giữa thiết bị truyền thông thứ nhất và thực thể mạng qua tiến trình xác thực thứ nhất để thu thập ngữ cảnh

bảo mật. Lần lượt, phương pháp xác thực truyền thông tin ngữ cảnh bảo mật đến thiết bị truyền thông thứ hai. Do vậy, phương pháp xác thực xác thực giữa thiết bị truyền thông thứ hai và thực thể xác thực mạng qua tiến trình xác thực thứ hai, thiết bị truyền thông thứ hai xác thực với thực thể xác thực mạng sử dụng ngữ cảnh bảo mật từ thiết bị truyền thông thứ nhất. Theo phương án thực hiện sáng chế, đáp lại việc ngắt kết nối giữa thiết bị truyền thông thứ nhất và CN, xác thực giữa thiết bị truyền thông thứ nhất và thực thể mạng qua tiến trình xác thực thứ hai bằng cách sử dụng một phần của ngữ cảnh bảo mật.

Theo khía cạnh khác của sáng chế, khung làm việc xác thực cho UE có ít nhất hai thiết bị truyền thông để xác thực với thực thể xác thực mạng của CN được đề xuất theo cách thức sau. Khung làm việc xác thực thực hiện xác thực thứ nhất bằng thiết bị truyền thông thứ nhất của UE với thực thể xác thực mạng để thu thập ngữ cảnh bảo mật cho thiết bị truyền thông thứ nhất. Lần lượt, ngữ cảnh bảo mật được truyền đến thiết bị truyền thông thứ hai. Sau đó, thiết bị truyền thông thứ hai thực hiện xác thực thứ hai với CN bằng cách sử dụng ngữ cảnh bảo mật từ thiết bị truyền thông thứ nhất. Theo phương án thực hiện sáng chế, đáp lại việc ngắt kết nối giữa thiết bị truyền thông thứ nhất và CN, thực hiện xác thực thứ hai bởi thiết bị truyền thông thứ nhất với CN bằng cách sử dụng ngữ cảnh bảo mật thu được.

Theo khía cạnh khác của sáng chế, thực thể xác thực mạng trong CN để xác thực với UE được đề xuất theo cách thức sau. Thực thể xác thực mạng bao gồm bộ xử lý, vật lưu trữ, và các lệnh được lưu trữ trên vật lưu trữ và thực thi được bởi bộ xử lý: thực hiện xác thực thứ nhất với thiết bị truyền thông thứ nhất của UE để tạo ngữ cảnh bảo mật qua thủ tục xác thực với thiết bị truyền thông thứ nhất; và thực hiện xác thực thứ hai với thiết bị truyền thông thứ hai của UE dựa trên ngữ cảnh bảo mật được thiết lập qua thủ tục xác thực với thiết bị truyền thông thứ nhất của UE.

Theo khía cạnh khác của sáng chế, thực thể xác thực mạng có thể là

máy chủ xác thực trong khung làm việc xác thực dựa trên EAP. Trong một số đặc tả, cũng được biết đến như là khối xác thực (Authentication Unit – AU) hoặc khối xác thực mặt phẳng điều khiển (Control Plane Authentication Unit – CP-AU).

Theo phương án thực hiện sáng chế, thực thể xác thực mạng thiết lập ngữ cảnh bảo mật thông qua xác thực với môđun quản lý xác thực qua thiết bị truyền thông thứ nhất hoặc thứ hai ở phía UE. Ngữ cảnh bảo mật ở thực thể xác thực mạng gồm ít nhất ID của UE, bộ đếm và khóa bí mật, được ký hiệu là k0. Thực thể xác thực mạng suy ra khóa bí mật dựa trên k0 và truyền khóa, được ký hiệu là k1, đến BS hoặc Wi-Fi AP mà qua đó UE và thực thể xác thực mạng xác thực với nhau. Theo phương án thực hiện, khóa bí mật thứ nhất được tạo bằng cách sử dụng các KDF với đầu vào bao gồm ID của UE và RAND (hoặc NONCE được nhận từ mạng) trong đó khóa bí mật thứ hai được tạo bằng cách sử dụng các KDF với đầu vào bao gồm k0 và bộ đếm. Theo phương án thực hiện, khóa bí mật thứ hai, k1, được tạo bằng cách sử dụng KDF với đầu vào bao gồm k0 và RAND (hoặc NONCE được nhận từ mạng). Theo phương án thực hiện, khóa bí mật thứ nhất được lưu trữ trên thực thể xác thực mạng và khóa bí mật thứ hai được truyền đến thực thể mạng chẳng hạn BS hoặc Wi-Fi AP.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất với thiết bị truyền thông thứ nhất của UE để tạo ngữ cảnh bảo mật cho thiết bị truyền thông thứ nhất bao gồm các lệnh để: nhận thông điệp yêu cầu chứa ID của UE từ UE qua BS hoặc Wi-Fi AP; tạo và truyền Yêu cầu dữ liệu xác thực đến HSS, yêu cầu dữ liệu xác thực gồm ID của UE, SN ID, và loại mạng; nhận đáp ứng dữ liệu xác thực từ HSS, đáp ứng dữ liệu xác thực bao gồm RAND, AUTN, XRES, IK, và CK; tạo FRID. Theo phương án thực hiện, FRID được tạo bởi kết hợp ID của UE với RAND. Theo phương án thực hiện khác, FRID được tạo bởi kết hợp ID của UE với số định trước dựa trên loại của thiết bị truyền thông thực hiện yêu cầu.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất với thiết bị truyền thông thứ nhất của UE để tạo ngữ cảnh bảo mật cho thiết bị truyền thông thứ nhất còn bao gồm các lệnh: tạo và truyền Thông điệp AKA-thách thức chứa FRID, RAND, AUTH, và MAC đến BS hoặc Wi-Fi AP tùy thuộc vào thiết bị nào của thiết bị truyền thông khởi tạo tiến trình xác thực, trong đó MAC được tạo bằng cách sử dụng IK với các tham số đầu vào của MAC gồm FRID, RAND, AUTH, và có thể được biểu diễn theo cách thức sau, $MAC = MAC_{IK}(FRID||RAND||AUTH)$.

Theo phương án thực hiện sáng chế, lệnh để thực hiện xác thực thứ nhất với thiết bị truyền thông thứ nhất của UE để tạo ngữ cảnh bảo mật cho thiết bị truyền thông thứ nhất còn bao gồm các lệnh để: nhận đáp ứng AKA từ UE bao gồm RES; xác định liệu RES bằng XRES; đáp ứng RES bằng XRES, suy ra khóa bí mật, k0, cho thiết bị truyền thông thứ nhất; và lưu trữ ngữ cảnh bảo mật bao gồm FRID, k0, và bộ đếm. Theo phương án thực hiện, khóa bí mật được suy ra bằng cách sử dụng KDF với các đầu vào của các KDF gồm ID của UE và RAND.

Mô tả vắn tắt các hình vẽ

Các ưu điểm nêu trên và các dấu hiệu theo sáng chế được mô tả trong phần mô tả chi tiết sau và được thể hiện trong các hình vẽ sau:

Fig.1 là hình vẽ minh họa kiến trúc mạng tích hợp công nghệ truy nhập Wi-Fi, gồm cả Wi-Fi đáng tin cậy và không đáng tin cậy;

Fig.2 là hình vẽ minh họa sơ đồ định thời của thủ tục của giao thức EPS-AKA trong mạng 4G trong đó UE thực hiện xác thực lẫn nhau với mạng để truy nhập mạng qua công nghệ LTE;

Fig.3 là hình vẽ minh họa sơ đồ định thời của thủ tục của giao thức EAP-AKA trong mạng 4G trong đó UE thực hiện xác thực lẫn nhau với mạng để truy nhập mạng qua công nghệ Wi-Fi;

Fig.4 là hình vẽ minh họa sơ đồ định thời của thủ tục của cơ cấu xác lại nhanh để tăng tốc xác thực được trình bày trong đặc tả 3GPP 33.402;

Fig.5 là hình vẽ minh họa khung làm việc xác thực thống nhất cho các công nghệ truy nhập 5G và Wi-Fi theo phương án thực hiện sáng chế;

Fig.6 là hình vẽ minh họa tiến trình trên thủ tục cho hai thực thể/thiết bị truyền thông bằng cách sử dụng thông tin xác thực chia sẻ để xác thực với CN theo phương án thực hiện sáng chế;

Fig.7 là hình vẽ minh họa sơ đồ định thời trên thủ tục cho hai thực thể/thiết bị truyền thông bằng cách sử dụng thông tin xác thực chia sẻ để xác thực với CN theo phương án thực hiện sáng chế;

Fig.8 là hình vẽ minh họa tiến trình được thực hiện bởi thiết bị truyền thông thứ nhất theo tiến trình 600 và sơ đồ định thời 700 theo phương án thực hiện sáng chế;

Fig.9 là hình vẽ minh họa tiến trình được thực hiện bởi thiết bị truyền thông 2 theo tiến trình 600 và sơ đồ định thời 700 theo phương án thực hiện sáng chế;

Fig.10 là hình vẽ minh họa tiến trình được thực hiện bởi thực thể xác thực mạng theo tiến trình 600 và sơ đồ định thời 700 theo phương án thực hiện sáng chế;

Fig.10A là hình vẽ minh họa tiến trình thay thế được thực hiện bởi thực thể xác thực mạng theo tiến trình 600 và sơ đồ định thời 700 theo phương án thực hiện sáng chế;

Fig.11 là hình vẽ minh họa tiến trình trên thủ tục cho hai thực thể/thiết bị truyền thông bằng cách sử dụng thông tin xác thực chia sẻ thông qua môđun quản lý xác thực để xác thực với CN theo phương án thực hiện sáng chế;

Fig.12 là hình vẽ minh họa sơ đồ định thời trên thủ tục cho hai thực thể/thiết bị truyền thông bằng cách sử dụng thông tin xác thực chia sẻ thông

qua môđun quản lý xác thực để xác thực với CN như được thể hiện trên Fig.11 theo phương án thực hiện sáng chế;

Fig.12A là hình vẽ minh họa sơ đồ định thời biến thể trên thủ tục cho hai thực thể/thiết bị truyền thông bằng cách sử dụng thông tin xác thực chia sẻ thông qua môđun quản lý xác thực để xác thực với CN như được thể hiện trên Fig. 11 theo phương án thực hiện sáng chế;

Fig.13 là hình vẽ minh họa tiến trình được thực hiện bởi một trong các thiết bị truyền thông 1 và 2 theo tiến trình 1100 và sơ đồ định thời 1200 theo phương án thực hiện sáng chế;

Fig.14 là hình vẽ minh họa tiến trình được thực hiện bởi môđun quản lý xác thực theo tiến trình 1100 và sơ đồ định thời 1200 theo phương án thực hiện sáng chế;

Fig.15 là hình vẽ minh họa sơ đồ định thời của thủ tục xác thực theo phần thứ nhất của khung làm việc xác thực đồng nhất theo phương án thực hiện sáng chế;

Fig.16 là hình vẽ minh họa tiến trình được thực hiện bởi một trong các thiết bị truyền thông 1 và 2 theo sơ đồ định thời 1500 theo phương án thực hiện sáng chế;

Fig.17 là hình vẽ minh họa tiến trình được thực hiện bởi thực thể xác thực mạng theo sơ đồ định thời 1500 theo phương án thực hiện sáng chế;

Fig.18 là hình vẽ minh họa tiến trình được thực hiện bởi HSS theo sơ đồ định thời 1500 theo phương án thực hiện sáng chế;

Fig.19 là hình vẽ minh họa sơ đồ định thời của thủ tục xác thực lại nhanh theo phần ths hai của khung làm việc xác thực đồng nhất theo phương án thực hiện sáng chế;

Fig.20 là hình vẽ minh họa tiến trình được thực hiện bởi một trong các thiết bị truyền thông 1 và 2 theo sơ đồ định thời 1900 theo phương án thực hiện sáng chế;

Fig.21 là hình vẽ minh họa tiến trình được thực hiện bởi thực thể xác thực mạng theo sơ đồ định thời 1900 theo phương án thực hiện sáng chế; và

Fig.22 là hình vẽ minh họa phương án thực hiện thể hiện nhiều phép xác thực cộng tác theo phương án thực hiện sáng chế;

Fig.23 là hình vẽ minh họa phương án thực hiện thể hiện nhiều công nghệ truy nhập;

Fig.24 là hình vẽ thể hiện thủ tục chi tiết cho UE với hai công nghệ truy nhập khác nhau để thiết lập ngữ cảnh bảo mật với khung làm việc xác thực đồng nhất.

Mô tả chi tiết sáng chế

Sáng chế đề cập đến phương pháp và hệ thống, khung làm việc xác thực đồng nhất để xác thực cộng tác các thiết bị di động để truy nhập CN. Một cách cụ thể, sáng chế đề cập đến phương pháp và hệ thống, khung làm việc xác thực thống nhất để xác thực cộng tác giữa thiết bị di động và CN.

Theo sáng chế, đề xuất việc giải pháp xác thực mới mà tối ưu hóa khung làm việc xác thực cho mạng truyền thông khi các công nghệ truy nhập khác nhau chẳng hạn 5G và Wi-Fi được sử dụng trong mạng truyền thông thế hệ tiếp theo.

Để hiểu rõ hơn giải pháp xác thực mới, tổng quan ngắn gọn của phương pháp xác thực hiện tại sẽ được mô tả trước.

Fig.2 minh họa sơ đồ định thời 200 của thủ tục của giao thức EPS-AKA trong mạng 4G trong đó UE thực hiện xác thực lẫn nhau với mạng để truy nhập mạng qua công nghệ LTE. Sơ đồ định thời 200 bắt đầu với 210 trong đó UE truyền yêu cầu đính kèm đến MME. Yêu cầu đính kèm bao gồm ID truy nhập của UE.

Khi tiếp nhận yêu cầu đính kèm từ UE, MME truyền yêu cầu dữ liệu xác thực đến HSS ở bước 220. Yêu cầu dữ liệu xác thực gồm ID truy nhập, danh tính mạng phục vụ (Serving Network Identity – SN ID), và loại mạng.

Đáp ứng việc nhận yêu cầu dữ liệu xác thực từ MME, HSS định vị khóa (K) được liên kết với ID truy nhập trong cơ sở dữ liệu HSS, và tính toán vectơ xác thực bằng cách sử dụng thuật toán EPS AKA ở bước 230. Vectơ xác thực gồm RAND, AUTN, K_{AMSE} và XRES. Sau đó HSS tạo và truyền đáp ứng dữ liệu xác thực với các vectơ xác thực đến MME ở bước 240.

Ở bước 250, MME tạo và truyền yêu cầu xác thực người dùng đến UE. Yêu cầu xác thực người dùng gồm RAND, và thẻ xác thực AUTN được suy ra từ vectơ xác thực.

Khi nhận RAND và AUTN, UE tính toán $AUTN_{UE}$ và sau đó xác thực CN bằng cách kiểm chứng liệu $AUTN_{UE}$ có bằng AUTN ở bước 260 hay không. Nếu $AUTN_{UE}$ bằng AUTN, UE truyền đáp ứng xác thực người dùng đến MME ở bước 270. Đáp ứng xác thực người dùng gồm RES.

Khi nhận đáp ứng xác thực người dùng, MME xác thực UE bằng cách so sánh RES và XRES ở bước 280. Nếu RES bằng XRES, xác thực là thành công và MME cấp quyền UE truy nhập vào cổng nối. Sơ đồ định thời 200 kết thúc sau bước 280.

Fig.3 minh họa sơ đồ định thời 300 của thủ tục của giao thức EAP-AKA/EAP-AKA' trong mạng 4G trong đó UE thực hiện xác thực lẫn nhau với mạng để truy nhập mạng qua công nghệ Wi-Fi. Sơ đồ định thời 300 bắt đầu với bước 310 trong đó UE liên kết với AP phi 3GPP chẳng hạn Wi-Fi AP. Sau khi UE liên kết với Wi-Fi AP, Wi-Fi AP truyền yêu cầu danh tính đến UE ở bước 315. Khi nhận yêu cầu, UE truy xuất danh tính và truyền danh tính đến Wi-Fi AP ở bước 320. Đáp ứng việc nhận danh tính từ UE, Wi-Fi AP truyền danh tính đến máy chủ AAA ở bước 325.

Ở bước 330, AAA truyền yêu cầu cho vectơ AKA đến HSS. Đáp ứng việc tiếp nhận yêu cầu từ AAA, HSS định vị khóa (K) được liên kết với

danh tính trong cơ sở dữ liệu HSS, và tính toán vectơ xác thực bằng cách sử dụng thuật toán EAP AKA ở bước 335. Vectơ xác thực gồm RAND, AUTN, K_{AMSE} và XRES. Sau đó HSS tạo và truyền các vectơ xác thực đến AAA ở bước 340.

Sau khi AAA nhận vectơ xác thực từ HSS, AAA tạo và truyền thông điệp thách thức đến Wi-Fi AP ở bước 345. Wi-Fi AP đáp ứng việc nhận thông điệp thách thức, truyềns thông điệp thách thức đến UE ở bước 350.

Ở bước 355, UE xác thực mạng dựa trên thông điệp thách thức. Cụ thể là, UE tính toán $AUTN_{UE}$ và sau đó xác thực CN bằng cách kiểm chứng liệu $AUTN_{UE}$ bằng AUTN. Nếu $AUTN_{UE}$ bằng AUTN, UE truyền thông điệp đáp ứng đến Wi-Fi AP ở bước 360. Đáp ứng xác thực người dùng gồm RES.

Đáp ứng việc nhận thông điệp đáp ứng từ UE, Wi-Fi AP truyền thông điệp đáp ứng đến máy chủ AAA ở bước 365. Khi nhận thông điệp đáp ứng, AAA xác thực UE bằng cách so sánh RES và XRES ở bước 370. Nếu RES bằng XRES, xác thực thành công và AAA sẽ truyền thông với HSS để truy xuất và đăng ký tiểu sử ở bước 375. AAA cũng sẽ cấp quyền UE truy nhập vào các cổng nối khi xác thực thành công ở bước 370.

Sau đó AAA tạo và truyền thông điệp thành công đến Wi-Fi AP ở bước 380. Wi-Fi AP đáp ứng việc nhận thông điệp thành công từ AAA, truyền thông điệp thành công đến UE ở bước 385. Sơ đồ định thời 300 kết thúc sau bước 385.

Fig.4 minh họa sơ đồ định thời 400 của thủ tục của cơ cấu xác thực lại nhanh để tăng tốc xác thực được trình báy trong đặc tả 3GPP 33.402 phiên bản 13.0.0. Sơ đồ định thời 400 bắt đầu với bước 410 trong đó UE liên kết với AP phi 3GPP chẳng hạn Wi-Fi AP. Sau khi UE liên kết với Wi-Fi AP, Wi-Fi AP truyền yêu cầu danh tính đến UE ở bước 415. Khi nhận yêu cầu, UE truy xuất danh tính của nó và truyền danh tính đến Wi-Fi AP ở bước

420. Đáp ứng việc nhận danh tính từ UE, Wi-Fi AP truyền danh tính đến máy chủ AAA ở bước 425.

Ở bước 445, AAA tạo và truyền thông điệp xác thực lại đến Wi-Fi AP. Wi-Fi AP đáp ứng việc nhận thông điệp xác thực lại, truyền thông điệp xác thực lại đến UE ở bước 450. Thông điệp xác thực lại gồm BỘ ĐẾM, NONCE_S (được mật mã hóa), NEXT_REAUTH_ID (được mật mã hóa), MAC. Đây là phương pháp đã được biết và các chi tiết khác có thể được thấy trong phần 5.4 của RFC4187.

Ở bước 460, UE truyền thông điệp đáp ứng đến Wi-Fi AP. Thông điệp đáp ứng gồm BỘ ĐẾM với cùng giá trị (được mật mã hóa) và MAC.

Đáp ứng việc nhận thông điệp đáp ứng từ UE, Wi-Fi AP truyền thông điệp đáp ứng đến máy chủ AAA ở bước 465. Khi nhận thông điệp đáp ứng, AAA tạo và truyền thông điệp thông báo đến Wi-Fi AP ở bước 470. Thông điệp thông báo gồm BỘ ĐẾM với cùng giá trị (được mật mã hóa) và MAC.

Wi-Fi AP đáp ứng việc nhận thông điệp thông báo, truyền thông điệp thông báo đến UE ở bước 475. Ở bước 480, UE tạo và truyền thông điệp đáp ứng thứ hai đến Wi-Fi AP đáp ứng việc nhận thông điệp thông báo.

Wi-Fi AP đáp ứng việc nhận thông điệp đáp ứng thứ hai, truyền thông điệp đáp ứng thứ hai đến UE ở bước 485.

Sau đó AAA tạo và truyền thông điệp thành công đến Wi-Fi AP ở bước 490. Wi-Fi AP đáp ứng việc nhận thông điệp thành công từ AAA, truyềns thông điệp thành công to UE ở bước 495. Sơ đồ định thời 400 kết thúc sau bước 495.

So sánh xác thực lại nhanh như được thể hiện trên Fig.4 với thủ tục xác thực đầy đủ EAP-AKA' thông thường như được thể hiện trên Fig. 3, máy chủ AAA không cần lấy các vectơ xác thực từ HSS. Do vậy, thủ tục xác thực lại nhanh hiệu quả hơn xác thực đầy đủ EAP-AKA' thông thường. Chuyên gia trong lĩnh vực sẽ ghi nhận rằng luồng tiến trình như được mô

tả trên đây dựa vào các hình vẽ Fig.2 đến Fig.4 là các tiến trình hiện tại. Ở đây, phần mô tả nêu trên không nhằm vét cạn.

Với nền sau, quay trở lại sáng chế. Theo sáng chế, giả sử rằng trong mạng truyền thông không dây thế hệ tiếp theo chẳng hạn mạng truyền thông thế hệ thứ 5 (5G), cả công nghệ tế bào lẫn Wi-Fi, có thể sử dụng cùng giao thức xác thực, EAP-AKA', thay cho EPS-AKA và EAP-AKA' như trong mạng 4G. Tuy nhiên, lưu ý rằng sáng chế không bị giới hạn ở việc sử dụng chỉ một giao thức xác thực.

Ngoài ra, ở phía mạng, chỉ một thực thể xác thực, máy chủ AAA, có thể được sử dụng thay cho việc có các thực thể xác thực riêng rẽ, tức là MME và AAA, trong mạng 4G. Theo cách khác, MME và AAA có thể được quản lý bởi máy chủ xác thực.

Dựa trên cấu hình này, đề xuất phương pháp và hệ thống cho các công nghệ truy nhập khác nhau để chia sẻ các kết quả xác thực. Cụ thể là, sau khi một công nghệ truy nhập của UE xác thực thành công với máy chủ AAA, UE thu thập FRID. Công nghệ truy nhập thứ hai có thể thu thập FRID và thực hiện xác thực nhanh với máy chủ AAA, thay cho việc thực hiện xác thực đầy đủ làm các công nghệ hiện tại.

Nhằm mục đích sáng chế, UE thường chẳng hạn là thiết bị di động chứa nhiều hơn một công nghệ truy nhập. LTE và Wi-Fi đại diện hai công nghệ truy nhập không dây thông thường. Hai công nghệ truy nhập cũng dần hợp nhất. Trong các mạng 4G, hai công nghệ truy nhập xác thực với mạng bằng cùng chứng nhận được bảo quản trong USIM và HSS một cách lần lượt, nhưng các giao thức xác thực cơ bản và các thực thể xác thực vẫn khác nhau. Thực thể tế bào và thực thể Wi-Fi không nói với nhau. Thay vào đó, môđun quản lý được đề xuất để xác nhận việc sử dụng một trong công nghệ truy nhập.

Fig.5 minh họa khung làm việc xác thực thống nhất cho các công nghệ truy nhập 5G và Wi-Fi. Với khung làm việc được đề xuất, độc lập với công

nghệ truy nhập, chỉ một giao thức xác thực, EAP-AKA', được sử dụng để xác thực, và chỉ có một thực thể xác thực ở phía mạng, tức là, máy chủ AAA.

Với khung làm việc xác thực mới được đề xuất, các phương pháp được đề xuất cho các công nghệ truy nhập khác nhau thuộc cùng UE chia sẻ thông tin xác thực sao cho thủ tục xác thực có thể còn được tối ưu hóa. Theo sáng chế, các phương pháp khác nhau được đề xuất. Phương pháp thứ nhất chính là việc UE với một công nghệ truy nhập không dây lấy thông tin xác thực nhanh trực tiếp từ các thiết bị còn lại với công nghệ truy nhập khác. Phương pháp thứ hai liên quan đến môđun độc lập chẳng hạn môđun quản lý xác thực để quản lý thông tin xác thực chẳng hạn FRID. Điều này cho phép UE thu thập thông tin xác thực từ môđun quản lý xác thực.

Về cơ bản, khung làm việc xác thực đồng nhất gồm hai phần 510 và 520. Phần thứ nhất 510 gắn liền với công nghệ truy nhập thứ nhất trong UE xác thực với CN để thu thập ngữ cảnh bảo mật cụ thể. Phần thứ hai gắn với công nghệ truy nhập thứ hai trong UE thu thập một phần ngữ cảnh bảo mật được thiết lập qua công nghệ truy nhập thứ nhất để xác thực với CN. Trong phần minh họa như được thể hiện trên Fig. 5, công nghệ truy nhập thứ nhất là công nghệ truy nhập Wi-Fi trong khi công nghệ truy nhập thứ hai là công nghệ tế bào. Tuy nhiên, chuyên gia trong lĩnh vực sẽ ghi nhận rằng các công nghệ truy nhập thứ nhất và thứ hai trao đổi được mà không xa rời sáng chế. Nói cách khác, Fig.5 có thể được chỉnh sửa sao cho công nghệ truy nhập thứ nhất là công nghệ tế bào trong khi công nghệ truy nhập thứ hai là công nghệ truy nhập Wi-Fi mà không xa rời sáng chế.

Lưu ý rằng các UE và CN đã được biết đến rộng rãi. Do vậy, để ngắn gọn, hệ điều hành, các cấu hình, các cấu trúc, các cơ cấu, v.v. bị bỏ qua. Một cách quan trọng, phương pháp và hệ thống theo sáng chế được đề xuất dưới dạng các lệnh được lưu trữ trên vật lưu trữ và thực thi được bởi các bộ xử lý của UE và các CN.

UE với hai môđun truyền thông

Ở phương pháp thứ nhất của khung làm việc xác thực đồng nhất, hai thực thể/thiết bị truyền thông trong cùng UE chia sẻ thông tin xác thực, gồm FRID và các khóa bí mật liên quan, với nhau một cách trực tiếp. Thủ tục cho hai thực thể/thiết bị truyền thông sử dụng xác thực chia sẻ sẽ được mô tả dưới đây dựa vào Fig.6.

Fig.6 minh họa tiến trình 600 trên thủ tục cho hai thực thể/thiết bị truyền thông bằng cách sử dụng thông tin xác thực chia sẻ để xác thực với CN. Tiến trình 600 bắt đầu bằng bước 605 trong đó thiết bị truyền thông 1 xác thực với thực thể xác thực mạng của CN để thu thập ngữ cảnh bảo mật. Một cách cụ thể, thiết bị truyền thông 1 của UE xác thực với thực thể xác thực mạng của CN và nếu thành công, thực thể xác thực mạng tạo ngữ cảnh bảo mật. Trong ví dụ này, thực thể xác thực mạng có thể là máy chủ AAA, MME hoặc môđun quản lý bảo mật độc lập, có thể cùng vị trí với các máy chủ AAA và MMEs. Ngữ cảnh bảo mật có thể gồm RFID, các khóa bí mật, và bộ đếm. Sau đó thông điệp xác thực được truyền đến thiết bị truyền thông 1. Chuyên gia trong lĩnh vực sẽ ghi nhận rằng thiết bị truyền thông 1 có thể tạo ngữ cảnh bảo mật thay thế mà không xa rời sáng chế. Bước 605 gắn với phần thứ nhất của khung làm việc xác thực đồng nhất. Các chi tiết sau của bước 605 sẽ được mô tả dưới đây dựa vào Fig.15.

Ở bước 610, thiết bị truyền thông 2 muốn xác thực với CN. Tuy nhiên, trước khi xác thực với CN, thiết bị truyền thông 2 truyền yêu cầu đến thiết bị truyền thông 1 để thu thập FRID.

Ở bước 615, khi nhận FRID từ thiết bị truyền thông 1, thiết bị truyền thông 2 sử dụng FRID để xác thực với CN sau. Một cách cụ thể, thiết bị truyền thông 2 bắt đầu thủ tục xác thực lại nhanh với CN. Thủ tục xác thực lại nhanh bắt đầu với thiết bị truyền thông 2 tạo và truyền thông điệp đến thực thể xác thực. Thông điệp gồm FRID, và một cách tùy chọn, cũng gồm

cờ để chỉ báo rằng FRID không thuộc thiết bị truyền thông hiện tại và việc thiết bị truyền thông hiện tại thu thập FRID từ thiết bị khác trong cùng UE. Bằng cách trích rút cờ từ thông điệp, thực thể xác thực ở phía mạng xác định hành động thích hợp khi xử lý ngữ cảnh bảo mật. Chẳng hạn, nếu cờ chỉ báo rằng FRID thuộc thiết bị truyền thông, thì máy chủ có thể đơn giản cập nhật ngữ cảnh bảo mật. Nếu cờ chỉ báo rằng FRID không thuộc thiết bị truyền thông, thực thể xác thực có thể tạo ngữ cảnh bảo mật mới.

Thực thể xác thực mạng có thể yêu cầu thêm thông tin từ thiết bị truyền thông 2 trong quá trình xác thực. Do vậy, thiết bị truyền thông 2 có thể yêu cầu thông tin cụ thể từ thiết bị truyền thông 1. Chẳng hạn, sau khi nhận thông điệp xác thực nhanh lại được nhúng trong yêu cầu EAP-AKA' từ thực thể xác thực mạng, thiết bị truyền thông 2 có thể gửi thông điệp xác thực nhanh lại đến thiết bị truyền thông 1. Sau đó, thiết bị truyền thông 1 sẽ tạo đáp ứng xác thực lại nhanh và truyền đáp ứng xác thực nhanh đến thiết bị truyền thông 2. Sau đó, thiết bị truyền thông 2 truyền thông điệp đáp ứng xác thực nhanh đến thực thể xác thực mạng ở phía mạng. Thực thể xác thực mạng xác thực thiết bị truyền thông 2 với thông điệp đáp ứng xác thực nhanh. Ngoài ra, các thông điệp khác chẳng hạn thông điệp thông báo và thành công có thể được trao đổi giữa thiết bị thứ hai và các thực thể xác thực ở phía mạng. Các chi tiết sau của bước 615 sẽ được mô tả dưới đây dựa vào Fig.16.

Ở bước 620, nếu thực thể xác thực mạng xác định rằng FRID không thuộc thiết bị truyền thông 2 và xác thực với thiết bị truyền thông 2 là thành công, thực thể xác thực mạng tạo ngữ cảnh bảo mật cho thiết bị truyền thông 2. Ngữ cảnh bảo mật gồm ít nhất khóa phiên chủ. Ngữ cảnh bảo mật được truyền đến thiết bị truyền thông 2. Theo cách khác, khóa phiên chủ có thể được tạo bởi thiết bị truyền thông 1 và được truyền đến thiết bị truyền thông 2. Các bước 610, 615 và 620 gắn với phần thứ hai của khung làm việc xác thực đồng nhất. Tiến trình 600 kết thúc sau bước 620.

Fig.7 minh họa sơ đồ định thời 700 trên thủ tục cho hai thực thể/thiết bị truyền thông bằng cách sử dụng thông tin xác thực chia sẻ để xác thực với CN như được thể hiện trên Fig.6. Sơ đồ định thời 700 bắt đầu với bước 705 trong đó thiết bị truyền thông 1 xác thực với thực thể xác thực mạng của CN để thu thập ngữ cảnh bảo mật. Giống với bước 605 trong tiến trình 600, thiết bị truyền thông 1 của UE xác thực với thực thể xác thực mạng của CN và nếu thành công, thực thể xác thực mạng tạo ngữ cảnh bảo mật. Trong ví dụ này, thực thể xác thực mạng có thể là máy chủ AAA, máy chủ MME hoặc môđun quản lý bảo mật trong hoặc ngoài các máy chủ AAA và MME. Ngữ cảnh bảo mật có thể gồm FRID, các khóa bí mật, và bộ đếm. Sau đó, thông điệp gồm FRID, bộ đếm và thông tin khác được truyền đến thiết bị truyền thông 1. Chuyên gia trong lĩnh vực sẽ ghi nhận rằng thiết bị truyền thông 1 có thể tạo ngữ cảnh bảo mật thay vào đó mà không xa rời sáng chế. Các chi tiết sau của bước 705 sẽ được mô tả dưới đây dựa vào Fig.15.

Sau khi xác thực thành công ở bước 705, thực thể xác thực mạng lưu lại FRID, các khóa bí mật, và khởi tạo bộ đếm ở bước 710a. Một cách tương tự, ở đầu UE, thiết bị truyền thông 1 cũng lưu lại FRID, các khóa bí mật, và khởi tạo bộ đếm ở bước 710b. Các bước 705, 710a và 710b gắn với phần thứ nhất của khung làm việc xác thực đồng nhất.

Ở bước 715, thiết bị truyền thông 2 muốn xác thực với CN. Để làm vậy, thiết bị truyền thông 2 truyền yêu cầu đến thiết bị truyền thông 1 để thu thập FRID. Đáp ứng yêu cầu from thiết bị truyền thông 2, thiết bị truyền thông truyền đáp ứng chứa FRID đến thiết bị truyền thông 1 ở bước 720.

Ở bước 730, khi nhận FRID từ thiết bị truyền thông 1, thiết bị truyền thông 2 sử dụng FRID để xác thực với CN. Một cách cụ thể, thiết bị truyền thông 2 bắt đầu thủ tục xác thực lại nhanh với thực thể xác thực mạng của CN. Thủ tục xác thực lại nhanh bắt đầu với thiết bị truyền thông 2 tạo và truyền thông điệp đến thực thể xác thực. Thông điệp gồm FRID và cờ để

chỉ báo FRID không thuộc thiết bị truyền thông hiện tại và việc thiết bị truyền thông hiện tại thu thập FRID từ thiết bị khác trong cùng UE. Bằng cách trích rút cờ từ thông điệp, thực thể xác thực ở phía mạng xác định hành động thích hợp khi xử lý ngữ cảnh bảo mật. Chẳng hạn, nếu cờ chỉ báo rằng FRID thuộc thiết bị truyền thông, thì máy chủ có thể chỉ đơn giản ngữ cảnh bảo mật. Nếu cờ chỉ báo rằng FRID không thuộc thiết bị truyền thông, thực thể xác thực có thể tạo ngữ cảnh bảo mật mới.

Trong suốt bước 730, thực thể xác thực mạng có thể yêu cầu thông tin khác từ thiết bị truyền thông 2. Do vậy, thiết bị truyền thông 2 có thể yêu cầu thông tin cụ thể từ thiết bị truyền thông 1 ở bước 732. Chẳng hạn, sau khi nhận thông điệp xác thực nhanh lại được nhúng trong yêu cầu EAP-AKA' từ thực thể xác thực mạng, thiết bị truyền thông 2 có thể gửi thông điệp xác thực nhanh lại đến thiết bị truyền thông 1. Sau đó, thiết bị truyền thông 1 sẽ tạo đáp ứng xác thực lại nhanh và truyền đáp ứng xác thực nhanh đến thiết bị truyền thông 2. Sau đó thiết bị truyền thông 2 truyền thông điệp đáp ứng xác thực nhanh đến thực thể xác thực mạng ở phía mạng. Thực thể xác thực mạng xác thực thiết bị truyền thông 2 với thông điệp đáp ứng xác thực nhanh. Ngoài ra, các thông điệp khác chẳng hạn thông điệp thông báo và thành công có thể được trao đổi giữa thiết bị thứ hai và các thực thể xác thực ở phía mạng. Các chi tiết sau của bước 615 sẽ được mô tả dưới đây dựa vào Fig.16.

Ở bước 740a, nếu thực thể xác thực mạng xác định rằng FRID không thuộc thiết bị truyền thông 2 và xác thực với thiết bị truyền thông 2 là thành công, thực thể xác thực mạng tạo ngữ cảnh bảo mật cho thiết bị truyền thông 2. Ngữ cảnh bảo mật gồm ít nhất khóa phiên chủ. Thông điệp xác thực gồm RFID mới, bộ đếm và các nonce được truyền đến thiết bị truyền thông 2 để dẫn xuất ngữ cảnh bảo mật. Theo cách khác, khóa phiên chủ có thể được tạo bởi thiết bị truyền thông 1 và được truyền đến thiết bị truyền thông 2 ở bước 740b. Các bước 730, 732, 740a và 740b gắn với phần thứ

hai của khung làm việc xác thực đồng nhất. Sơ đồ định thời 700 kết thúc sau bước 740a hoặc 740b.

Fig.8 minh họa tiến trình 800 được thực hiện bởi thiết bị truyền thông 1 theo tiến trình 600 và sơ đồ định thời 700. Tiến trình 800 bắt đầu với bước 805 bằng cách truyền yêu cầu cho FRID đến thiết bị truyền thông thứ hai của UE. Ở bước 810, thiết bị truyền thông thứ nhất nhận đáp ứng từ thiết bị truyền thông thứ hai. Nếu đáp ứng chứa FRID, thiết bị truyền thông chuyển sang bước 820. Nếu đáp ứng không chứa FRID, thiết bị truyền thông chuyển sang bước 830.

Ở bước 820, thiết bị truyền thông thứ nhất tiếp tục với phần thứ hai của khung làm việc xác thực đồng nhất. Ở bước 830, thiết bị truyền thông thứ nhất chuyển sang phần thứ nhất của khung làm việc xác thực đồng nhất. Tiến trình 800 kết thúc sau bước 820 hoặc 830.

Fig.9 minh họa tiến trình 900 được thực hiện bởi thiết bị truyền thông 2 theo tiến trình 600 và sơ đồ định thời 700. Tiến trình 900 bắt đầu với bước 905 bằng cách nhận yêu cầu FRID từ thiết bị truyền thông 1 of UE.

Ở bước 910, thiết bị truyền thông 2 tạo và truyền đáp ứng chứa FRID, khóa bí mật và bộ đếm. Nếu thiết bị truyền thông 2 không có FRID, thiết bị truyền thông 2 tạo và truyền đáp ứng chỉ báo rằng không có FRID.

Tiến trình 900 kết thúc sau bước 910.

Fig.10 minh họa tiến trình 1000 được thực hiện bởi thực thể xác thực mạng theo tiến trình 600 và sơ đồ định thời 700. Tiến trình 1000 bắt đầu với bước 1005 bằng cách nhận yêu cầu từ UE. Ở bước 1010, thực thể xác thực mạng xác định liệu yêu cầu dành cho xác thực hoặc xác thực nhanh. Nếu yêu cầu dành cho xác thực, tiến trình 1000 chuyển sang bước 1015. Nếu yêu cầu là để xác thực nhanh, tiến trình 1000 chuyển sang bước 1040.

Ở bước 1015, đáp ứng việc nhận yêu cầu để xác thực, thực thể xác thực mạng xác thực với UE. Nếu xác thực thành công, tiến trình 1000 chuyển sang bước 1020. Ngược lại, tiến trình 1000 kết thúc.

Ở bước 1020, thực thể xác thực mạng tạo ngữ cảnh bảo mật. Ngữ cảnh bảo mật có thể gồm FRID, khóa bí mật, và bộ đếm. Khóa bí mật khác được suy ra từ ngữ cảnh bảo mật và được truyền đến thực thể mạng chẳng hạn Wi-Fi AP hoặc BS được định nghĩa bởi công nghệ 3GPP, hoặc các công nghệ khác ở bước 1025. Bản sao của ngữ cảnh bảo mật được lưu lại trong cơ sở dữ liệu của thực thể xác thực mạng ở bước 1030. Khóa bí mật, được ký hiệu là k1, được truyền đến BS hoặc Wi-Fi AP được suy ra từ khóa bí mật, được ký hiệu là k0, của ngữ cảnh bảo mật với chức năng KDF. Các tham số chẳng hạn FRID hoặc bộ đếm, hoặc RAND, hoặc nonce được truyền đến UE, cũng có thể được lấy làm đầu vào của hàm KDF khi suy ra k1.

Ở bước 1040, thực thể xác thực mạng khởi tạo thủ tục xác thực lại nhanh từ UE bằng cách xác định trước liệu thông điệp chứa cờ ở gốc của FRID. Sau đó thực thể xác thực mạng xác định gốc của FRID.

Nếu cờ chỉ báo rằng gốc của FRID thuộc thiết bị truyền thông, thì thực thể xác thực mạng chuyển sang bước 1045 để cập nhật đơn giản ngữ cảnh truyền thông chẳng hạn bộ đếm trong ngữ cảnh bảo mật. Nếu cờ chỉ báo rằng gốc của FRID không thuộc thiết bị truyền thông, thực thể xác thực mạng chuyển sang bước 1050.

Ở bước 1050, thực thể xác thực mạng tạo ngữ cảnh bảo mật mới cho thiết bị truyền thông mới giống bước 1020 và truyền các khóa hoặc các khóa được suy ra thêm từ ngữ cảnh bảo mật đến các thực thể mạng chẳng hạn Wi-Fi AP hoặc BS được định nghĩa bởi 3GPP. Theo cách khác, ngữ cảnh bảo mật có thể được truyền ở bước 1060 cùng với khóa phiên chủ được tạo ở bước 1055.

Ở bước 1055, thực thể xác thực mạng tiếp tục với thủ tục xác thực lại nhanh. Nếu xác thực thành công, thực thể xác thực mạng tạo khóa phiên chủ. Khóa phiên chủ có thể được bao gồm trong ngữ cảnh bảo mật. Theo cách khác, ngữ cảnh bảo mật không thể bao gồm khóa phiên chủ. Thay vào

đó, khóa phiên chủ có thể được tạo bởi thiết bị truyền thông mà sở hữu FRID và được truyền đến thiết bị truyền thông mới. Ngữ cảnh bảo mật cũng được lưu lại trong cơ sở dữ liệu của thực thể xác thực mạng.

Ở bước 1060, thực thể xác thực mạng truyền Thông điệp xác thực lại nhanh đến UE chứa ngữ cảnh bảo mật. Các chi tiết khác trên thủ tục để xác thực nhanh sẽ được mô tả dưới đây dựa vào Fig.16. Tiến trình 1000 kết thúc sau bước 1060.

Fig.10A minh họa tiến trình 1000A khác được thực hiện bởi thực thể xác thực mạng theo tiến trình 600 và sơ đồ định thời 700. Cụ thể là, thủ tục xác thực lại nhanh không xem xét liệu FRID có phải từ nguồn ban đầu hay không và tiếp tục ngay với việc cập nhật ngữ cảnh bảo mật. Tiến trình xác thực của tiến trình 1000A giống tiến trình xác thực của tiến trình 1000.

Tiến trình 1000A bắt đầu với bước 1005A bằng cách nhận yêu cầu từ UE. Ở bước 1010A, thực thể xác thực mạng xác định liệu yêu cầu dành cho xác thực hoặc xác thực nhanh. Nếu yêu cầu dành cho xác thực, tiến trình 1000A chuyển sang bước 1015A. Nếu yêu cầu là để xác thực nhanh, tiến trình 1000A chuyển sang bước 1045A.

Ở bước 1015A, đáp ứng việc nhận yêu cầu để xác thực, thực thể xác thực mạng xác thực với UE. Nếu xác thực thành công, tiến trình 1000A chuyển sang bước 1020A. Ngược lại, tiến trình 1000A kết thúc.

Ở bước 1020A, thực thể xác thực mạng tạo ngữ cảnh bảo mật. Ngữ cảnh bảo mật có thể gồm FRID, các khóa bí mật, và bộ đếm. Khóa bí mật khác được suy ra từ ngữ cảnh bảo mật và được truyền đến thực thể mạng chẳng hạn Wi-Fi AP hoặc BS được định nghĩa bởi công nghệ 3GPP, hoặc các công nghệ khác ở bước 1025A. Bản sao của ngữ cảnh bảo mật được lưu lại trong cơ sở dữ liệu của thực thể xác thực mạng ở bước 1030A. Khóa bí mật, được ký hiệu là k1, được truyền đến BS hoặc Wi-Fi AP được suy ra từ khóa bí mật, được ký hiệu là k0, của ngữ cảnh bảo mật với hàm KDF.

Các tham số chẳng hạn FRID hoặc bộ đếm, hoặc RAND, hoặc nonce được truyền đến UE cũng có thể lấy làm đầu vào của hàm KDF khi suy ra k1.

Ở bước 1045A, thực thể xác thực mạng cập nhật ngữ cảnh truyền thông chẳng hạn bộ đếm trong ngữ cảnh bảo mật.

Ở bước 1050A, thực thể xác thực mạng tiếp tục với thủ tục xác thực lại nhanh. Nếu xác thực thành công, thực thể xác thực mạng tạo khóa phiên chủ.

Sau đó, khóa phiên chủ được truyền đến các thực thể mạng chẳng hạn Wi-Fi AP hoặc BS được định nghĩa bởi 3GPP ở bước 1055A. Tiến trình 1000A kết thúc sau bước 1055A.

UE với hai mô đun truyền thông và môđun quản lý xác thực dành riêng

Ở phương pháp thứ hai của khung làm việc xác thực đồng nhất, hai thực thể/thiết bị truyền thông trong cùng UE chia sẻ thông tin xác thực, gồm FRID và các khóa bí mật liên quan, qua môđun quản lý xác thực. Cụ thể là, trong UE, môđun riêng rẽ được đề xuất để quản lý thông tin xác thực từ các thiết bị truyền thông khác nhau. Sau khi nhận FRID từ thực thể xác thực mạng, thiết bị truyền thông còn đưa qua FRID, các khóa bí mật được suy ra (tùy chọn), và bộ đếm v.v., đến môđun quản lý xác thực. Thủ tục cho hai thực thể/thiết bị truyền thông bằng cách sử dụng xác thực chia sẻ qua môđun quản lý xác thực sẽ được mô tả dưới đây dựa vào Fig.11.

Fig.11 minh họa tiến trình 1100 trên thủ tục cho hai thực thể/thiết bị truyền thông bằng cách sử dụng thông tin xác thực chia sẻ qua môđun quản lý xác thực để xác thực với CN. Tiến trình 1100 bắt đầu với bước 1105 trong đó thiết bị truyền thông 1 xác thực với thực thể xác thực mạng của CN để thu thập ngữ cảnh bảo mật. Một cách cụ thể, thiết bị truyền thông 1 của UE xác thực với thực thể xác thực mạng của CN và nếu thành công, thực thể xác thực mạng tạo ngữ cảnh bảo mật. Trong ví dụ này, thực thể xác thực mạng có thể máy chủ AAA, máy chủ MME hoặc môđun quản lý mà quản lý các máy chủ AAA và MME. Thực thể xác thực mạng cũng có

thể là thực thể chức năng độc lập. Ngữ cảnh bảo mật có thể gồm FRID, các khóa bí mật, và bộ đếm. Sau đó, ngữ cảnh bảo mật được truyền đến thiết bị truyền thông 1. Chuyên gia trong lĩnh vực sẽ ghi nhận rằng thiết bị truyền thông 1 có thể tạo ngữ cảnh bảo mật thay thế mà không xa rời sáng chế. Bước 1105 gắn với phần thứ nhất của khung làm việc xác thực đồng nhất. Các chi tiết sau của bước 1105 sẽ được mô tả dưới đây dựa vào Fig.15.

Ở bước 1110, thiết bị truyền thông 1 truyền ngữ cảnh bảo mật đến môđun quản lý xác thực. Theo phương án thực hiện khác, môđun quản lý xác thực có thể tự thiết lập ngữ cảnh bảo mật thông qua trao đổi thông điệp xác thực với thực thể xác thực mạng ở phía mạng. Môđun quản lý xác thực có thể là môđun độc lập, có thể là phần cứng hoặc phần mềm, và được phát triển để quản lý thông tin xác thực từ các thiết bị truyền thông khác nhau trong cùng UE. Khi nhận ngữ cảnh bảo mật từ thiết bị truyền thông 1, môđun quản lý xác thực lưu lại bản sao của thông tin ngữ cảnh bảo mật.

Ở bước 1115, thiết bị truyền thông 2 muốn xác thực với CN. Tuy nhiên, trước khi xác thực với CN, thiết bị truyền thông 2 truyền yêu cầu đến môđun quản lý xác thực để thu thập FRID. Theo cách khác, thiết bị truyền thông 2 có thể kích hoạt môđun quản lý xác thực để bắt đầu thủ tục xác thực.

Ở bước 1120, khi nhận FRID từ môđun quản lý xác thực, thiết bị truyền thông 2 sử dụng FRID để xác thực với CN. Một cách cụ thể, thiết bị truyền thông 2 bắt đầu thủ tục xác thực lại nhanh với CN. Thủ tục xác thực lại nhanh bắt đầu với thiết bị truyền thông 2 hoặc môđun quản lý xác thực tạo và truyền thông điệp đến thực thể xác thực. Thông điệp gồm FRID và cờ để chỉ báo FRID không thuộc thiết bị truyền thông hiện tại và thiết bị truyền thông hiện tại thu thập FRID từ thiết bị khác trong cùng UE. Bằng cách trích rút cờ từ thông điệp, thực thể xác thực ở phía mạng xác định hành động thích hợp khi xử lý ngữ cảnh bảo mật. Chẳng hạn, nếu cờ chỉ báo rằng FRID thuộc thiết bị truyền thông, thì máy chủ có thể chỉ cập nhật ngữ

cảnh bảo mật. Nếu cờ chỉ báo rằng FRID không thuộc thiết bị truyền thông, thực thể xác thực có thể tạo ngữ cảnh bảo mật mới.

Thực thể xác thực mạng có thể yêu cầu thông tin khác từ thiết bị truyền thông 2 trong quá trình xác thực. Do vậy, thiết bị truyền thông 2 có thể yêu cầu thông tin cụ thể từ môđun quản lý xác thực. Chẳng hạn, sau khi nhận thông điệp xác thực nhanh lại được nhúng trong yêu cầu EAP-AKA' từ thực thể xác thực mạng, thiết bị truyền thông 2 có thể gửi thông điệp xác thực nhanh lại đến môđun quản lý xác thực. Sau đó môđun quản lý xác thực sẽ tạo đáp ứng xác thực lại nhanh và truyền đáp ứng xác thực nhanh đến thiết bị truyền thông 2. Sau đó, thiết bị truyền thông 2 truyền thông điệp đáp ứng xác thực nhanh đến thực thể xác thực mạng ở phía mạng. Thực thể xác thực mạng xác thực thiết bị truyền thông 2 với thông điệp đáp ứng xác thực nhanh. Ngoài ra, các thông điệp khác chẳng hạn thông điệp thông báo và thành công có thể được trao đổi giữa các thiết bị truyền thông hoặc môđun quản lý xác thực và các thực thể xác thực ở phía mạng. Các chi tiết sau của bước 1120 sẽ được mô tả dưới đây dựa vào Fig.16.

Ở bước 1125, nếu thực thể xác thực mạng xác định rằng FRID không thuộc thiết bị truyền thông 2 và xác thực với thiết bị truyền thông 2 là thành công, thực thể xác thực mạng tạo ngữ cảnh bảo mật cho thiết bị truyền thông 2. Ngữ cảnh bảo mật gồm ít nhất khóa phiên chủ. Khóa phiên chủ có thể được tạo bởi môđun quản lý xác thực và được truyền đến thiết bị truyền thông 2. Các bước 1115, 1120 và 1125 gắn với phần thứ hai của khung làm việc xác thực đồng nhất. Tiến trình 1100 kết thúc sau bước 1125.

Fig.12 minh họa sơ đồ định thời 1200 trên thủ tục cho hai thực thể/thiết bị truyền thông bằng cách sử dụng thông tin xác thực chia sẻ qua môđun quản lý xác thực để xác thực với CN như được thể hiện trên Fig.11. Sơ đồ định thời 1200 bắt đầu với bước 1205 trong đó thiết bị truyền thông 1 xác thực với thực thể xác thực mạng của CN để thiết lập ngữ cảnh bảo mật. Giống với bước 1105 trong tiến trình 1100, thiết bị truyền thông 1 của UE

xác thực với thực thể xác thực mạng của CN và nếu thành công, thực thể xác thực mạng tạo ngữ cảnh bảo mật. Trong ví dụ này, thực thể xác thực mạng có thể là máy chủ AAA, máy chủ MME hoặc môđun quản lý mà quản lý các máy chủ AAA và MME. Ngữ cảnh bảo mật có thể gồm FRID, các khóa bí mật, và bộ đếm. Chuyên gia trong lĩnh vực sẽ ghi nhận rằng thiết bị truyền thông 1 có thể tạo ngữ cảnh bảo mật thay vào đó mà không xa rời sáng chế. Các chi tiết sau của bước 1205 sẽ được mô tả dưới đây dựa vào Fig.15.

Sau khi xác thực thành công ở bước 1205, thực thể xác thực mạng lưu lại FRID, các khóa bí mật, và khởi tạo bộ đếm ở bước 1210a. Một cách tương tự, ở đầu UE, thiết bị truyền thông 1 cũng lưu lại FRID, các khóa bí mật, và khởi tạo bộ đếm ở bước 1210b. Các bước 1205, 1210a và 1210b gắn với phần thứ nhất của khung làm việc xác thực đồng nhất.

Ở bước 1215, thiết bị truyền thông 1 truyền ngữ cảnh bảo mật đến môđun quản lý xác thực. Môđun quản lý xác thực có thể là môđun độc lập, có thể là phần cứng hoặc phần mềm, và được phát triển để quản lý thông tin xác thực từ các thiết bị truyền thông khác nhau trong cùng UE. Khi nhận ngữ cảnh bảo mật từ thiết bị truyền thông 1, môđun quản lý xác thực lưu lại bản sao của thông tin ngữ cảnh bảo mật.

Ở bước 1220, thiết bị truyền thông 2 muốn xác thực với CN. Để làm vậy, thiết bị truyền thông 2 truyền yêu cầu đến môđun quản lý xác thực để thu thập FRID. Đáp ứng yêu cầu từ thiết bị truyền thông 2, môđun quản lý xác thực truyền đáp ứng chứa FRID đến thiết bị truyền thông 1 ở bước 1230.

Ở bước 1240, khi nhận FRID từ môđun quản lý xác thực, thiết bị truyền thông 2 sử dụng FRID để xác thực với CN. Một cách cụ thể, thiết bị truyền thông 2 bắt đầu thủ tục xác thực lại nhanh với thực thể xác thực mạng của CN. Thủ tục xác thực lại nhanh bắt đầu với thiết bị truyền thông 2 tạo và truyền thông điệp đến thực thể xác thực. Thông điệp gồm FRID và cờ để

chỉ báo FRID không thuộc thiết bị truyền thông hiện tại và rằng thiết bị truyền thông hiện tại thu thập FRID từ thiết bị khác trong cùng UE. Bằng cách trích rút cờ từ thông điệp, thực thể xác thực ở phía mạng xác định hành động thích hợp khi xử lý ngữ cảnh bảo mật. Chẳng hạn, nếu cờ chỉ báo rằng FRID thuộc thiết bị truyền thông, thì máy chủ có thể chỉ cập nhật ngữ cảnh bảo mật. Nếu cờ chỉ báo rằng FRID không thuộc thiết bị truyền thông, thực thể xác thực có thể tạo ngữ cảnh bảo mật mới.

Trong bước 1240, thực thể xác thực mạng có thể yêu cầu thông tin khác từ thiết bị truyền thông 2. Do vậy, thiết bị truyền thông 2 có thể yêu cầu thông tin cụ thể từ môđun quản lý xác thực ở bước 1442. Chẳng hạn, sau khi nhận thông điệp xác thực nhanh lại được nhúng trong yêu cầu EAP-AKA' từ thực thể xác thực mạng, thiết bị truyền thông 2 có thể gửi thông điệp xác thực nhanh lại đến môđun quản lý xác thực. Sau đó môđun quản lý xác thực sẽ tạo đáp ứng xác thực lại nhanh và truyền đáp ứng xác thực nhanh đến thiết bị truyền thông 2. Sau đó, thiết bị truyền thông 2 truyền thông điệp đáp ứng xác thực nhanh đến thực thể xác thực mạng ở phía mạng. Thực thể xác thực mạng xác thực thiết bị truyền thông 2 với thông điệp đáp ứng xác thực nhanh. Ngoài ra, các thông điệp khác chẳng hạn thông điệp thông báo và thành công có thể được trao đổi giữa thiết bị truyền thông 2 và thực thể xác thực ở phía mạng. Các chi tiết sau của các bước 1240 và 1242 sẽ được mô tả dưới đây dựa vào Fig.16.

Ở bước 1250a, nếu thực thể xác thực mạng xác định rằng FRID không thuộc thiết bị truyền thông 2 và xác thực với thiết bị truyền thông 2 là thành công, thực thể xác thực mạng tạo ngữ cảnh bảo mật cho thiết bị truyền thông 2. Khóa phiên chủ cũng được tạo và được bao gồm trong ngữ cảnh bảo mật. Ngữ cảnh bảo mật được truyền đến thực thể mạng chẳng hạn Wi-Fi AP hoặc BS được định nghĩa bởi công nghệ 3GPP, hoặc các công nghệ khác. Thực thể mạng sẽ còn truyền ngữ cảnh bảo mật không có khóa phiên chủ đến môđun quản lý xác thực. Theo cách khác, khóa phiên chủ có thể

được tạo bởi môđun quản lý xác thực và được truyền đến thiết bị truyền thông 2 ở bước 1250b. Các bước 1240, 1242, 1250a và 1250b gắn với phần thứ hai của khung làm việc xác thực đồng nhất. Theo tiến trình khác trong đó ngữ cảnh bảo mật được chia sẻ bởi các thiết bị truyền thông, ngữ cảnh bảo mật mới sẽ không được tạo. thay vào đó, chỉ khóa phiên chủ được tạo và được truyền đến thực thể mạng.

Sơ đồ định thời 1200 kết thúc sau bước 1250a hoặc 1250b.

Fig.12A minh họa chỉnh sửa cho sơ đồ định thời 1200. Cụ thể là, các bước từ 1205 đến 1215 trong sơ đồ định thời 1200 sẽ được cải biến theo cách thức sau. Ở bước 1205, thay cho thiết bị truyền thông 1 xác thực với thực thể xác thực mạng của CN để thiết lập ngữ cảnh bảo mật, thiết bị truyền thông 1 kích hoạt môđun quản lý xác thực để xác thực với thực thể xác thực mạng của CN để thiết lập ngữ cảnh bảo mật. Cụ thể là, thiết bị truyền thông 1 truyền yêu cầu xác thực đến môđun quản lý xác thực để xác thực với thực thể xác thực mạng của CN để thiết lập ngữ cảnh bảo mật. Đáp ứng việc nhận lệnh kích hoạt từ thiết bị truyền thông 1, môđun quản lý xác thực của UE xác thực với thực thể xác thực mạng của CN và nếu thành công, thực thể xác thực mạng tạo ngữ cảnh bảo mật. Ngữ cảnh bảo mật có thể gồm FRID, các khóa bí mật, và bộ đếm. Chuyên gia trong lĩnh vực sẽ ghi nhận rằng môđun quản lý xác thực có thể tạo ngữ cảnh bảo mật thay vào đó mà không xa rời sáng chế.

Sau khi xác thực thành công ở bước 1205, thực thể xác thực mạng lưu lại FRID, các khóa bí mật, và khởi tạo bộ đếm ở bước 1210a. Một cách tương tự, ở đầu UE, môđun quản lý xác thực cũng lưu lại FRID, các khóa bí mật, và khởi tạo bộ đếm ở bước 1210b. Thực thể xác thực mạng và môđun quản lý xác thực dẫn xuất các khóa mới dựa trên các khóa bí mật được thiết lập sau thủ tục xác thực. Theo một phương án thực hiện, nếu các khóa bí mật được thiết lập sau khi xác thực là k0, thì môđun xác thực và thực thể xác thực mạng còn dẫn xuất khóa mới, k1, bằng cách sử dụng

KDF. Cụ thể là, k1 có thể được suy ra bằng cách sử dụng khóa bí mật và bộ đếm và được biểu diễn theo cách thức sau, k1 = KDF(k0, bộ đếm). Theo phương án thực hiện khác, môđun quản lý xác thực và thực thể xác thực mạng có thể suy ra k1 bằng cách sử dụng các khóa bí mật và FRID và được biểu diễn theo cách thức sau, k1 = KDF(k0, FRID). Khóa bí mật, k0, được giữ trong môđun quản lý xác thực và thực thể xác thực mạng trong khi k1 được bao gồm trong ngữ cảnh bảo mật và được truyền đến các thiết bị truyền thông bởi môđun quản lý xác thực. k1 cũng được bao gồm trong ngữ cảnh bảo mật được truyền đến BS hoặc Wi-Fi AP bởi thực thể xác thực mạng. Môđun quản lý xác thực có thể là máy trạm như được định nghĩa trong khung làm việc EAP và thực thể xác thực mạng có thể là máy chủ xác thực trong khung làm việc EAP hoặc khối xác thực được gọi là CP-AU trong các đặc tả 3GPP chẳng hạn trong TR 23.799. Để tránh nghi ngờ, các khóa bí mật được tạo bởi thực thể xác thực mạng và môđun quản lý xác thực một cách riêng rẽ.

Ở bước 1215, môđun quản lý xác thực truyền ngữ cảnh bảo mật đến thiết bị truyền thông 1. Khi nhận ngữ cảnh bảo mật từ môđun quản lý xác thực, thiết bị truyền thông 1 lưu lại bản sao của thông tin ngữ cảnh bảo mật. Phần còn lại của các bước từ 1220 đến 1250 vẫn không đổi.

Fig.13 minh họa tiến trình 1300 được thực hiện bởi một trong các thiết bị truyền thông 1 và 2 theo tiến trình 1100 và sơ đồ định thời 1200 trên Fig.12 hoặc Fig.12A. Tiến trình 1300 bắt đầu với bước 1305 bằng cách truyền yêu cầu FRID đến môđun quản lý xác thực của UE. Ở bước 1310, thiết bị truyền thông nhận đáp ứng từ môđun quản lý xác thực. Nếu đáp ứng chứa FRID, thiết bị truyền thông chuyển sang bước 1320. Nếu đáp ứng không chứa FRID, thiết bị truyền thông chuyển sang bước 1330.

Ở bước 1320, thiết bị truyền thông chuyển sang phần thứ hai của khung làm việc xác thực đồng nhất. Ở bước 1330, thiết bị truyền thông chuyển sang phần thứ nhất của khung làm việc xác thực đồng nhất. Một cách cụ

thể, thiết bị truyền thông xác thực với thực thể xác thực mạng để thu thập ngữ cảnh bảo mật trực tiếp như được minh họa trên Fig.12 hoặc gián tiếp qua môđun quản lý xác thực như được minh họa trên Fig.12A. Tiến trình 1300 kết thúc sau bước 1320 hoặc 1330.

Fig.14 minh họa tiến trình 1400 được thực hiện bởi môđun quản lý xác thực theo tiến trình 1100 và sơ đồ định thời 1200 trên Fig.12 hoặc Fig.12A. Tiến trình 1400 bắt đầu với bước 1405 bằng cách nhận thông điệp từ thiết bị truyền thông của UE. Sau đó, tiến trình 1400 xác định liệu thông điệp là yêu cầu FRID hoặc yêu cầu để kích hoạt môđun quản lý xác thực để xác thực với thực thể xác thực mạng của CN để thiết lập ngữ cảnh bảo mật ở bước 1410. Nếu thông điệp là yêu cầu FRID từ thiết bị truyền thông của UE, tiến trình 1400 chuyển sang bước 1415. Nếu thông điệp là yêu cầu kích hoạt môđun quản lý xác thực để xác thực với thực thể xác thực mạng của CN để thiết lập ngữ cảnh bảo mật, tiến trình 1400 chuyển sang bước 1420.

Ở bước 1415, môđun quản lý xác thực tạo và truyền đáp ứng chứa FRID, khóa bí mật và bộ đếm. Nếu môđun quản lý xác thực không có FRID, môđun quản lý xác thực tạo và truyền đáp ứng chỉ báo rằng nó không có FRID.

Ở bước 1420, tiến trình 1400 chuyển sang phần thứ nhất của khung làm việc xác thực đồng nhất. Các chi tiết khác phần thứ nhất của khung làm việc xác thực đồng nhất sẽ được mô tả dưới đây.

Tiến trình 1400 kết thúc sau bước 1420.

Tiến trình được thực hiện bởi thực thể xác thực mạng theo tiến trình 1100 và sơ đồ định thời 1200 giống với tiến trình 1000.

Quay lại tập trung vào các thủ tục xác thực và xác thực lại nhanh.

Xác thực cộng tác

Fig.15 minh họa sơ đồ định thời 1500 của thủ tục xác thực theo phần thứ nhất của khung làm việc xác thực đồng nhất. Việc xác thực dựa trên

thủ tục xác thực lại nhanh AKA. Quan trọng lưu ý rằng có thể có một chút khác biệt trong thủ tục xác thực và điều này phụ thuộc vào các thiết bị truyền thông trong UE. Các điểm khác biệt chinhgs sẽ được nêu bật trong phần mô tả dưới đây dựa vào sơ đồ định thời 1500.

Sơ đồ định thời 1500 bắt đầu với 1505 trong đó UE thiết lập kết nối với BS của mạng truy nhập tế bào (nếu thiết bị truyền thông là công nghệ tế bào) chẳng hạn mạng truy nhập 3GPP hoặc Wi-Fi AP (nếu thiết bị truyền thông là thực thể Wi-Fi). Theo cách khác, Wi-Fi AP có thể là cổng nối dữ liệu gói tiến hóa (Evolved Packet Data Gateway – ePDG) hoặc cổng nói/máy trung gian truy nhập WLAN đáng tin cậy (Trusted WLAN Access Gateway/Proxy – TWAG/TWAP).

Ở bước 1510, đáp ứng thiết lập kết nối, UE yêu cầu truy nhập vào mạng truy nhập 3GPP bằng cách gửi yêu cầu chứa ID của UE đến BS (nếu thiết bị truyền thông là thực thể công nghệ tế bào). Trong trường hợp mà trong đó thiết bị truyền thông của UE là thực thể Wi-Fi, Wi-Fi AP khởi tạo tiến trình xác thực AKA bằng cách gửi UE thông điệp yêu cầu. Khi đáp ứng, thực thể Wi-Fi của UE đáp ứng lại Wi-Fi AP thông điệp đáp ứng với ID của UE trong thông điệp.

Ở bước 1515, BS chuyển tiếp thông điệp yêu cầu đế thực thể xác thực mạng. Một cách tương tự, Wi-Fi AP chuyển tiếp thông điệp đáp ứng ở dạng thông điệp yêu cầu đến thực thể xác thực mạng.

Ở bước 1520, thực thể xác thực mạng truyền các thông điệp yêu cầu dữ liệu xác thực đến HSS để thu thập dữ liệu xác thực của UE. Thông điệp yêu cầu dữ liệu xác thực chứa ID của UE.

Khi nhận thông điệp yêu cầu dữ liệu xác thực từ thực thể xác thực mạng, HSS định vị khóa, K, theo ID của UE, và tính toán vectơ xác thực bằng cách sử dụng thuật toán AKA. Sau đó HSS gửi đáp ứng dữ liệu xác thực với các vectơ xác thực đến thực thể xác thực mạng ở bước 1525. Đáp ứng dữ liệu xác thực chứa vectơ xác thực. Vectơ xác thực chứa RAND, AUTN

được sử dụng để xác thực mạng đến môđun danh tính, phần kết quả mong đợi (XRES), khóa phiên 128-bit để kiểm tra tính toàn vẹn (IK), và khóa phiên 128-bit để mạt mã hóa (CK). Tiến trình tạo vectơ xác thực được biết và sẽ bị bỏ qua cho ngắn gọn.

Ở bước 1530, thực thể xác thực mạng truyền thông điệp AKA-thách thức chứa FRID, RAND, AUTH, SN ID, và loại mạng và MAC đến BS hoặc Wi-Fi AP tùy thuộc vào thiết bị nào của thiết bị truyền thông khởi tạo tiến trình xác thực. FRID có thể được tạo bởi thực thể xác thực mạng bằng cách kết hợp ID của UE với RAND. Theo cách khác, FRID có thể được tạo bởi kết hợp ID của UE với số định trước dựa trên loại của thiết bị truyền thông thực hiện yêu cầu. Chẳng hạn, nếu thiết bị truyền thông là thực thể Wi-Fi, số định trước là 01 và nếu thiết bị truyền thông là thực thể tế bào, số định trước là 02. Chuyên gia trong lĩnh vực sẽ ghi nhận rằng các phương pháp khác tạo FRID có thể được triển khai mà không xa rời sáng chế. MAC được tạo bằng cách sử dụng IK với đầu vào là RAND, AUTH và FRID. Tiến trình chính xác tạo MAC được biết đến và sẽ bị bỏ qua cho ngắn gọn.

Ở bước 1535, BS chuyển tiếp thông điệp AKA - thách thức đến UE trong khi Wi-Fi AP chuyển tiếp thông điệp AKA - thách thức đến UE.

Ở bước 1540, UE xác thực thực thể xác thực mạng bằng cách trước hết kiểm chứng thông điệp AKA - thách thức dựa trên MAC và lần lượt, sau khi kiểm chứng thành công tính chân thực của thông điệp AKA - thách thức, chạy thuật toán AKA bằng cách sử dụng RAND và AUTH. UE còn dẫn xuất các khóa để truy nhập tế bào hoặc truy nhập phi tế bào. UE lưu trữ FRID, dẫn xuất các khóa để xác thực nhanh, và khởi tạo bộ đếm để xác thực nhanh. Các chi tiết khác trên UE tạo khóa để xác thực nhanh sẽ được mô tả dưới đây dựa vào Fig.16.

Lưu ý rằng các khóa để truy nhập tế bào gồm khóa để mật mã hóa lưu lượng giữa UE và BS và khóa để bảo vệ tính toàn vẹn của lưu lượng này. Ngoài ra, các khóa để xác thực nhanh gồm khóa mật mã hóa để mật mã

hóa một số dữ liệu trong suốt quá trình xác thực lại, và khóa xác thực để tạo MAC.

Lưu ý rằng các khóa để truy nhập phi tế bào gồm khóa để mật mã hóa lưu lượng giữa UE và cổng nối và khóa để bảo vệ tính toàn vẹn của lưu lượng này. Ngoài ra, các khóa để xác thực nhanh gồm khóa mật mã để mật mã hóa một số dữ liệu trong quá trình xác thực lại, và khóa xác thực để tạo MAC.

Ở bước 1545, UE gửi thông điệp đáp ứng thách thức AKA đến BS. Trong trường hợp liên quan thực thể Wi-Fi, UE truyền thông điệp đáp ứng thách thức AKA đến cổng nối. Thông điệp đáp ứng thách thức AKA chứa RES và MAC được tạo bởi UE.

Ở bước 1550, BS hoặc Wi-Fi AP chuyển tiếp thông điệp đáp ứng thách thức AKA đến thực thể xác thực mạng.

Ở bước 1555, thực thể xác thực mạng xác thực UE bằng cách kiểm chứng thông điệp AKA-thách thức nhận được. Một cách cụ thể, thực thể xác thực mạng kiểm chứng thông điệp bằng cách kiểm tra liệu RES và MAC trong thông điệp nhận được là đúng. Sau đó, thực thể xác thực mạng dẫn xuất các khóa để truy nhập tế bào hoặc truy nhập phi tế bào, và lưu trữ FRID. Các khóa được dẫn xuất bằng cách sử dụng các KDF, vốn là các hàm giả ngẫu nhiên. Các đầu vào của các KDF gồm ID của UE và RAND. Lần lượt, thực thể xác thực mạng khởi tạo bộ đếm để xác thực nhanh.

Ở bước 1560, thực thể xác thực mạng truyền thông điệp thành công đến BS hoặc Wi-Fi AP mà xác thực thành công và các khóa để truy nhập tế bào hoặc phi tế bào của UE. Khi nhận thông điệp thành công và các khóa, BS hoặc Wi-Fi AP truyền thông điệp thành công và các khóa đến UE ở bước 1565. Sơ đồ định thời 1500 kết thúc sau bước 1565. Trong trường hợp trong đó việc xác thực được yêu cầu bởi môđun quản lý xác thực nhân danh thiết bị bất kỳ trong thiết bị truyền thông, thực thể xác thực mạng và môđun quản lý xác thực còn suy ra các khóa mới dựa trên các khóa bí mật

được thiết lập sau thủ tục xác thực. Theo một phương án thực hiện, nếu các khóa bí mật được thiết lập sau khi xác thực bằng k0, thì môđun xác thực và thực thể xác thực mạng còn dẫn xuất khóa mới, k1, bằng cách sử dụng KDF. Một cách cụ thể k1 có thể được dẫn xuất bằng cách sử dụng khóa bí mật và bộ đếm và được biểu diễn theo cách thức sau, k1 = KDF(k0, bộ đếm). Theo phương án thực hiện khác, môđun quản lý xác thực và thực thể xác thực mạng có thể dẫn xuất k1 bằng cách sử dụng các khóa bí mật và FRID và được biểu diễn theo cách thức sau, k1 = KDF(k0, FRID). Khóa bí mật, k0, được giữ trong môđun quản lý xác thực và thực thể xác thực mạng trong khi k1 được bao gồm trong ngữ cảnh bảo mật và được truyền đến các thiết bị truyền thông bởi môđun quản lý xác thực. k1 cũng được bao gồm trong ngữ cảnh bảo mật được truyền đến BS hoặc Wi-Fi AP bởi thực thể xác thực mạng. Môđun quản lý xác thực có thể là máy trạm như được định nghĩa trong trong khung làm việc EAP và thực thể xác thực mạng có thể là máy chủ xác thực trong khung làm việc EAP hoặc khối xác thực được đặt tên là CP-AU trong các đặc tả 3GPP chẳng hạn trong TR 23.799.

Fig.16 minh họa luồng tiến trình 1600 được thực hiện bởi UE theo phần thứ nhất của khung làm việc xác thực đồng nhất như được mô tả dựa vào sơ đồ định thời 1500. Tiến trình 1600 bắt đầu với bước 1605 bằng cách thiết lập liên kết với BS của mạng truy nhập tế bào (nếu thiết bị truyền thông là thực thể tế bào) chẳng hạn mạng truy nhập 3GPP hoặc Wi-Fi AP (nếu thiết bị truyền thông là thực thể Wi-Fi). Theo cách khác, Wi-Fi AP có thể là ePDG hoặc TWAG/TWAP.

Ở bước 1610, UE truy xuất danh tính của nó (ID của UE) và lần lượt tạo và truyền yêu cầu bao gồm ID của UE. Yêu cầu được truyền đến BS (nếu thiết bị truyền thông là thực thể công nghệ tế bào). Đến lượt, BS chuyển tiếp yêu cầu thông điệp đến thực thể xác thực mạng. Trong trường hợp trong đó thiết bị truyền thông của UE là thực thể Wi-Fi, Wi-Fi AP khởi

tạo tiến trình xác thực AKA bằng cách gửi UE thông điệp yêu cầu. Đáp lại, thực thể Wi-Fi của UE đáp ứng Wi-Fi AP với thông điệp đáp ứng với ID của UE trong thông điệp. Sau đó Wi-Fi AP chuyển tiếp thông điệp đáp ứng làm thông điệp yêu cầu đến thực thể xác thực mạng.

Ở bước 1615, UE nhận thông điệp AKA-thách thức. Thông điệp AKA - thách thức gồm RAND và AUTN được tạo bởi HSS. Thông điệp AKA - thách thức cũng chứa FRID và MAC được tạo bởi thực thể xác thực mạng.

Ở bước 1620, UE kiểm chứng MAC bằng cách sử dụng khóa của nó (IK). Lưu ý rằng UE đã được đăng ký với HSS vả cả UE lẫn HSS có cùng khóa. Để kiểm chứng MAC, UE tạo MAC với FRID, RAND và AUTN bằng cách sử dụng hàm tạo MAC tương tự được sử dụng bởi thực thể xác thực mạng với IK. Một ví dụ về hàm tạo MAC là mã xác thực thông điệp băm (Hash Message Authentication Code – HMAC) được tạo khóa. Nếu MAC là hợp lệ, bước 1620 tiếp tục tính toán vectơ xác thực bằng cách sử dụng thuật toán AKA 1690. Các tham số đầu vào cho thuật toán AKA gồm IK, RAND, SN ID, và SQN. Các tham số đầu ra từ thuật toán AKA KDF gồm $AUTN_{UE}$, RES, và K_{ASME}.

Ở bước 1625, UE xác thực với thực thể xác thực mạng bằng cách kiểm chứng liệu $AUTN_{UE}$ bằng AUTN. Nếu $AUTN_{UE}$ không bằng AUTN, tiến trình 1700 kết thúc. Nếu $AUTN_{UE}$ bằng AUTN, tiến trình 1600 chuyển sang bước 1630.

Ở bước 1630, UE dẫn xuất khóa bí mậts để truy nhập tế bào hoặc truy nhập phi tế bào. Các khóa được dẫn xuất bằng cách sử dụng KDF, vốn là các hàm giả ngẫu nhiên. Các đầu vào của các KDF gồm ID của UE và RAND. Chuyên gia trong lĩnh vực sẽ ghi nhận rằng đầu vào khác chẳng hạn khóa gốc của UE có thể được bao gồm làm đầu vào của KDF để tạo khóa bí mật mà không xa rời sáng chế. UE lưu trữ ngữ cảnh bảo mật bao gồm FRID, các khóa bí mật để xác thực nhanh, và khởi tạo bộ đếm để xác thực nhanh. Trong trường hợp trong đó môđun quản lý xác thực là khả

dụng, ngữ cảnh bảo mật được lưu trữ trên môđun quản lý xác thực. Nếu môđun quản lý xác thực không khả dụng, ngữ cảnh bảo mật được lưu trữ trên thiết bị truyền thông thứ nhất hoặc thứ hai. Trong trường hợp trong đó việc xác thực được yêu cầu bởi môđun quản lý xác thực nhân danh một trong thiết bị truyền thông, bước 1630 được chỉnh sửa sao cho môđun quản lý xác thực còn dẫn xuất các khóa mới dựa trên các khóa bí mật được thiết lập. Theo một phương án thực hiện, nếu các khóa bí mật được thiết lập sau khi xác thực là k0, thì môđun quản lý xác thực còn dẫn xuất khóa mới, k1, bằng cách sử dụng KDF cho thiết bị truyền thông. Một cách cụ thể, k1 có thể được dẫn xuất bằng cách sử dụng khóa bí mật và bộ đếm và được biểu diễn theo cách thức sau, k1 = KDF(k0, bộ đếm). Theo phương án thực hiện khác, môđun quản lý xác thực có thể dẫn xuất k1 bằng cách sử dụng các khóa bí mật và FRID và được biểu diễn theo cách thức sau, k1 = KDF(k0, FRID). Khóa bí mật, k0, được giữ môđun quản lý xác thực trong khi k1 được bao gồm trong ngữ cảnh bảo mật và được truyền đến các thiết bị truyền thông bởi môđun quản lý xác thực. Môđun quản lý xác thực có thể là máy trạm như được định nghĩa trong khung làm việc EAP.

Ở bước 1635, UE tạo và truyền thông điệp đáp ứng AKA đến thực thể xác thực mạng. Thông điệp đáp ứng AKA gồm RES được xác định ở bước 1620. Tiến trình 1600 kết thúc sau bước 1635.

Fig.17 minh họa luồng tiến trình 1700 được thực hiện bởi thực thể xác thực mạng trong CN theo phần thứ nhất của khung làm việc xác thực đồng nhất như được mô tả dựa vào sơ đồ định thời 1500. Tiến trình 1700 bắt đầu với bước 1705 bằng cách nhận thông điệp yêu cầu từ UE qua BS hoặc Wi-Fi AP.

Ở bước 1710, thực thể xác thực mạng tạo và truyền yêu cầu dữ liệu xác thực đến HSS dựa trên thông tin được nhận từ UE. Thông tin khác chẳng hạn SN ID và loại mạng có thể được truy xuất bởi MME dựa trên yêu cầu

được nhận từ UE. Yêu cầu dữ liệu xác thực gồm ID của UE, SN ID, và loại mạng.

Ở bước 1715, thực thể xác thực mạng nhận đáp ứng dữ liệu xác thực từ HSS. Đáp ứng dữ liệu xác thực chứa RAND, AUTN, XRES, IK, và CK (cũng có thể được biết đến là K_{ASME}).

Ở bước 1718, thực thể xác thực mạng tạo FRID bằng cách kết hợp ID của UE với RAND. Theo cách khác, FRID có thể được tạo bởi kết hợp ID của UE với số định trước dựa trên loại của thiết bị truyền thông thực hiện yêu cầu. Chẳng hạn, nếu thiết bị truyền thông là thực thể Wi-Fi, số định trước là 01, nếu thiết bị truyền thông là thực thể tế bào, số định trước là 02, và nếu yêu cầu từ môđun quản lý xác thực, số định trước là 03. Chuyên gia trong lĩnh vực sẽ ghi nhận rằng các phương pháp khác tạo FRID có thể được triển khai mà không xa rời sáng chế.

Ở bước 1720, thực thể xác thực mạng tạo và truyền thông điệp AKA-thách thức chứa FRID, RAND, AUTH, và MAC) đến BS hoặc Wi-Fi AP tùy thuộc vào thiết bị nào của thiết bị truyền thông khởi tạo tiến trình xác thực. MAC được tạo bằng cách sử dụng IK. Các tham số đầu vào của MAC gồm FRID, RAND, AUTH, và có thể được biểu diễn theo cách thức sau,

$MAC = MAC_{IK}(FRID||RAND||AUTH)$

Ở bước 1725, thực thể xác thực mạng nhận đáp ứng AKA từ UE. Đáp lại, thực thể xác thực mạng xác định liệu RES (từ đáp ứng AKA) bằng XRES (từ đáp ứng dữ liệu xác thực). Nếu RES không bằng XRES, tiến trình 1700 kết thúc. Nếu RES bằng XRES, tiến trình 1700 chuyển sang bước 1730.

Ở bước 1730, thực thể xác thực mạng cấp cho UE truy nhập vào các cổng nối ở bước 1730. Một cách cụ thể, thực thể xác thực mạng gửi thông điệp đến các cổng nối để cấp quyền truy nhập vào UE. Ngoài ra, thực thể xác thực mạng dẫn xuất các khóa bí mật để truy nhập tế bào hoặc truy nhập phi tế bào. Các khóa được dẫn xuất bằng cách sử dụng KDF, vốn là các

hàm giả ngẫu nhiên. Các đầu vào của các KDF gồm ID của UE và RAND. Chuyên gia trong lĩnh vực sẽ ghi nhận rằng đầu vào khác chẳng hạn khóa gốc của UE có thể được bao gồm làm đầu vào của KDF để tạo khóa bí mật mà không xa rời sáng chế. Thực thể xác thực mạng lưu trữ ngữ cảnh bảo mật bao gồm FRID, các khóa bí mật để xác thực nhanh, và khởi tạo bộ đếm để xác thực nhanh. Thực thể xác thực mạng cũng tạo và truyền thông điệp thành công đến UE qua BS hoặc Wi-Fi AP chỉ báo rằng xác thực là thành công. Tiến trình 1700 kết thúc sau bước 1730.

Trong trường hợp trong đó việc xác thực được yêu cầu bởi môđun quản lý xác thực nhân danh thiết bị bất kỳ của thiết bị truyền thông, bước 1730 có thể được chỉnh sửa sao cho thực thể xác thực mạng còn dẫn xuất các khóa mới dựa trên các khóa bí mật được thiết lập cho thiết bị truyền thông. Theo một phương án thực hiện, nếu các khóa bí mật được thiết lập sau khi xác thực là k0, thì thực thể xác thực mạng còn dẫn xuất khóa mới, k1, bằng cách sử dụng KDF. Một cách cụ thể, k1 có thể được suy ra bằng cách sử dụng khóa bí mật và bộ đếm và được biểu diễn theo cách thức sau, k1 = KDF(k0, bộ đếm). Theo phương án thực hiện khác, thực thể xác thực mạng có thể suy ra k1 bằng cách sử dụng các khóa bí mật và FRID và được biểu diễn theo cách thức sau, k1 = KDF(k0, FRID). Các khóa bí mật, k0 và k1, được giữ trong thực thể xác thực mạng và được bao gồm trong ngữ cảnh bảo mật được truyền đến BS hoặc Wi-Fi AP bởi thực thể xác thực mạng. Thực thể xác thực mạng có thể là máy chủ xác thực trong khung làm việc EAP hoặc khối xác thực được đặt tên là CP-AU trong các đặc tả 3GPP chẳng hạn trong TR 23.799.

Fig.18 minh họa luồng tiến trình 1800 được thực hiện bởi HSS trong CN theo phần thứ nhất của khung làm việc xác thực đồng nhất như được mô tả dựa vào sơ đồ định thời 1500. Tiến trình 1800 bắt đầu với bước 1805 bằng cách nhận yêu cầu dữ liệu xác thực từ thực thể xác thực mạng.

Ở bước 1810, HSS tạo đáp ứng dữ liệu xác thực bằng cách sử dụng thuật toán AKA 1890 để thu thập vectơ xác thực. Các tham số đầu vào cho thuật toán AKA gồm IK, RAND, SN ID, SQN. Các tham số đầu ra cho thuật toán AKA gồm AUTN, XRES, và khóa phiên 128-bit để mật mã hóa (CK) (cũng được biết là K_{ASME}). RAND là số ngẫu nhiên được suy ra bởi HSS. Đáp ứng dữ liệu xác thực chứa RAND, AUTN, XRES, IK, và CK.

Sau đó, đáp ứng dữ liệu xác thực được truyền đến thực thể xác thực mạng ở bước 1815. Tiến trình 1800 kết thúc sau bước 1815.

Fig.19 minh họa sơ đồ định thời 1900 của thủ tục xác thực lại nhanh theo phần thứ hai của khung làm việc xác thực đồng nhất. Xác thực nhanh dựa trên thủ tục xác thực lại nhanh AKA. Quan trọng lưu ý rằng có thể có các khác biệt nhỏ trong thủ tục xác thực lại nhanh và điều này phụ thuộc vào các thiết bị truyền thông trong UE. Các khác biệt chính sẽ được làm nổi bật trong phần mô tả sau dựa vào sơ đồ định thời 1900.

Sơ đồ định thời 1900 bắt đầu với 1905 trong đó UE thiết lập kết nối với BS của mạng truy nhập 3GPP (nếu thiết bị truyền thông là thực thể tế bào) hoặc Wi-Fi AP (nếu thiết bị truyền thông là thực thể Wi-Fi). Wi-Fi AP có thể là ePDG hoặc TWAG/TWAP.

Ở bước 1910, đáp ứng thiết lập kết nối, UE yêu cầu truy nhập vào mạng truy nhập tế bào bằng cách gửi yêu cầu chứa ID của UE, FRID và cờ đến BS (nếu thiết bị truyền thông là thực thể tế bào). Trong trường hợp trong đó thiết bị truyền thông của UE là thực thể Wi-Fi, Wi-Fi AP khởi tạo tiến trình xác thực AKA bằng cách gửi cho UE thông điệp yêu cầu. Đáp ứng, thực thể Wi-Fi của UE đáp ứng Wi-Fi AP bằng thông điệp đáp ứng chứa ID của UE, FRID và cờ.

Ở bước 1915, BS chuyển tiếp thông điệp yêu cầu đến thực thể xác thực mạng. Trong trường hợp của Wi-Fi AP, Wi-Fi AP truyền thông điệp đáp ứng dưới dạng thông điệp yêu cầu đến thực thể xác thực mạng. Wi-Fi AP

cũng thông báo thực thể xác thực mạng về loại truy nhập (truy nhập tế bào hoặc truy nhập phi tế bào).

Ở bước 1920, thực thể xác thực mạng trả lời BS hoặc Wi-Fi AP bằng yêu cầu xác thực lại AKA bằng bốn trường (*bộ đếm, *nonce, *new-re-auth-ID, MAC) trong đó. Các trường có dấu "*" nghĩa là trường được mật mã hóa bằng khóa mật mã cho xác thực lại nhanh AKA. *bộ đếm là giá trị của bộ đếm để xác thực lại nhanh AKA. Thực thể xác thực mạng và UE tăng giá trị lên ít nhất 1 sau mỗi lần xác thực lại. Điều này cho phép UE kiểm tra độ mới của thông điệp. *nonce là số ngẫu nhiên được chọn bởi thực thể xác thực mạng. *new-re-auth-ID là FRID để xác thực lại tiếp theo. MAC là mã xác thực thông điệp để kiểm chứng bộ tạo thông điệp.

Ở bước 1930, BS hoặc Wi-Fi AP chuyển tiếp yêu cầu xác thực lại AKA đến UE.

Ở bước 1940, UE xác thực thực thể xác thực mạng bằng cách kiểm chứng độ chuẩn của MAC và độ mới của bộ đếm. Sau đó UE lưu trữ Re-auth-ID mới là FRID mới. UE còn cập nhật bộ đếm cục bộ với giá trị của bộ đếm nhận được cộng 1 và dẫn xuất các khóa để truy nhập tế bào hoặc phi tế bào, tùy thuộc vào loại của các thiết bị truyền thông.

Các khóa để truy nhập tế bào gồm khóa để mật mã hóa lưu lượng giữa UE và BS và khóa để bảo vệ tính toàn vẹn của lưu lượng này. Ngoài ra, các khóa để truy nhập phi tế bào gồm khóa để mật mã hóa lưu lượng giữa UE và Wi-Fi AP và khóa để bảo vệ tính toàn vẹn của lưu lượng này. Bộ đếm nhận được được xem là mới nếu và chỉ nếu giá trị của nó không nhỏ hơn bộ đếm được lưu trữ bởi UE.

Ở bước 1945, UE truyền đáp ứng xác thực lại AKA BS hoặc Wi-Fi AP chứa hai trường (*bộ đếm và MAC). Giá trị của bộ đếm nên giống với giá trị của bộ đếm nhận được.

Ở bước 1950, BS hoặc Wi-Wi AP chuyển tiếp đáp ứng xác thực lại AKA đến thực thể xác thực mạng.

Ở bước 1955, thực thể xác thực mạng xác thực UE bằng cách kiểm chứng MAC của thông điệp đáp ứng xác thực lại AKA nhận được và giá trị của bộ đếm. Thực thể xác thực mạng dẫn xuất các khóa để truy nhập phi tế bào hoặc tế bào và lưu trữ FRID mới. Sau đó, thực thể xác thực mạng tăng bộ đếm lên 1. Giá trị của bộ đếm nhận được nên giống giá trị của bộ đếm của thực thể xác thực mạng.

Ở bước 1960, thực thể xác thực mạng thông báo BS hoặc Wi-Fi AP về kết quả xác thực lại nhanh. Nếu xác thực thành công, kết quả sẽ chứa các khóa cho truy nhập phi tế bào hoặc tế bào của UE. Ở bước 1665, BS hoặc Wi-Fi AP chuyển tiếp các kết quả đến UE.

Fig.20 minh họa luồng tiến trình 2000 được thực hiện bởi thiết bị UE theo phần thứ hai của khung làm việc xác thực đồng nhất như được mô tả dựa vào sơ đồ định thời 1900. Tiến trình 2000 bắt đầu với bước 2005 by thiết lập kết nối với BS của mạng truy nhập 3GPP (nếu thiết bị truyền thông là thực thể tế bào) hoặc Wi-Fi AP (nếu thiết bị truyền thông là thực thể Wi-Fi).

Ở bước 2010, đáp ứng thiết lập kết nối, UE yêu cầu truy nhập vào mạng truy nhập tế bào bằng cách gửi yêu cầu chứa ID của UE, FRID và cờ đến BS (nếu thiết bị truyền thông là thực thể tế bào). Lần lượt, BS chuyển tiếp thông điệp yêu cầu đến thực thể xác thực mạng. Trong trường hợp trong đó thiết bị truyền thông của UE là thực thể Wi-Fi, Wi-Fi AP khởi tạo tiến trình xác thực AKA bằng cách gửi UE thông điệp yêu cầu. Đáp ứng, thực thể Wi-Fi của UE đáp ứng Wi-Fi AP với thông điệp đáp ứng chứa ID của UE, FRID và cờ. Lần lượt, Wi-Fi AP chuyển tiếp thông điệp đáp ứng ở dạng thông điệp yêu cầu đến thực thể xác thực mạng. Cờ chứa chỉ báo rằng FRID không thuộc thiết bị truyền thông yêu cầu truy nhập.

Ở bước 2015, UE nhận thông điệp yêu cầu xác thực lại AKA từ thực thể xác thực mạng. Thông điệp yêu cầu xác thực lại AKA gồm *bộ đếm, *nonce, *FRID mới và MAC.

Ở bước 2018, UE xác thực thực thể xác thực mạng bằng cách kiểm chứng độ chuẩn của MAC và độ mới của bộ đếm. Bộ đếm nhận được được xem là mới nếu và chỉ nếu giá trị của nó không nhỏ hơn bộ đếm được lưu trữ bởi UE. Độ chuẩn của MAC được xác định theo cách thức sau. UE giải mật mã *bộ đếm, *nonce và *FRID mới từ thông điệp yêu cầu xác thực lại AKA. Sau đó UE kiểm chứng MAC bằng cách tạo MAC với bộ đếm được giải mã, nonce và FRID mới bằng cách sử dụng hàm tạo MAC tương tự được sử dụng bởi thực thể xác thực mạng với SK. Nếu MAC là hợp lệ, bước 2018 tiếp tục với việc lưu trữ FRID mới làm FRID mới trong ngữ cảnh bảo mật. UE còn cập nhật bộ đếm cục bộ với giá trị của bộ đếm nhận được cộng 1. Trong trường hợp trong đó môđun quản lý xác thực là khả dụng, ngữ cảnh bảo mật được lưu trữ trên môđun quản lý xác thực. Nếu môđun quản lý xác thực không khả dụng, ngữ cảnh bảo mật được lưu trữ trên thiết bị truyền thông thứ nhất hoặc thứ hai.

Ở bước 2020, UE xác định các khóa để truy nhập tế bào hoặc phi tế bào, tùy thuộc vào loại của các thiết bị truyền thông. Các khóa để truy nhập tế bào gồm khóa để mật mã hóa lưu lượng giữa UE và BS và khóa để bảo vệ tính toàn vẹn của lưu lượng này. Ngoài ra, các khóa để truy nhập phi tế bào gồm khóa để mật mã hóa lưu lượng giữa UE và Wi-Fi AP và khóa để bảo vệ tính toàn vẹn của lưu lượng này.

Ở bước 2025, UE truyền thông điệp đáp ứng xác thực lại AKA đến thực thể xác thực mạng qua BS hoặc Wi-Wi AP chứa hai trường (*bộ đếm và MAC). Giá trị của bộ đếm nên giống như giá trị của bộ đếm nhận được. Theo cách khác, đáp ứng xác thực lại AKA có thể chứa chỉ bộ đếm có hoặc không có mật mã hóa mà không xa rời sáng chế.

Ở bước 2030, UE nhận thông điệp kết quả từ thực thể xác thực mạng qua BS hoặc Wi-Fi AP. Thông điệp kết quả sẽ chỉ báo liệu có xác thực thành công. Nếu xác thực thành công, tiến trình 2000 chuyển sang 2035 và

chuyển sang truyền và nhận dữ liệu với CN bằng cách sử dụng các khóa được dẫn xuất ở bước 2020. Tiến trình 2000 kết thúc sau bước 2035.

Fig.21 minh họa luồng tiến trình 2200 được thực hiện bởi thực thể xác thực mạng trong CN theo phần thứ hai của khung làm việc xác thực đồng nhất như được mô tả dựa vào sơ đồ định thời 1900. Tiến trình 2100 bắt đầu với bước 2205 bằng cách nhận thông điệp yêu cầu từ BS (nếu thiết bị truyền thông là thực thể tế bào) hoặc Wi-Fi AP (nếu thiết bị truyền thông là thực thể Wi-Fi). Thông điệp yêu cầu chứa ID của UE, FRID và cờ.

Ở bước 2110, thực thể xác thực mạng truy xuất ngữ cảnh bảo mật được liên kết với ID của UE từ cơ sở dữ liệu của nó. Ngữ cảnh bảo mật bao gồm FRID, các khóa bí mật (SK), và bộ đếm. Sau đó, thực thể xác thực mạng xác định liệu FRID từ thông điệp yêu cầu có giống hệt FRID được lưu trữ trong cơ sở dữ liệu. Tiến trình 2100 kết thúc nếu FRID từ thông điệp yêu cầu không giống hệt FRID được lưu trữ trong cơ sở dữ liệu. Nếu FRID từ thông điệp yêu cầu giống hệt FRID được lưu trữ trong cơ sở dữ liệu, tiến trình 2100 chuyển sang bước 2115

Ở bước 2115, thực thể xác thực mạng tạo FRID mới cho thủ tục xác thực lại tiếp theo bằng cách kết hợp ID của UE với RAND. Bộ đếm cũng được tăng lên 1. Thực thể xác thực mạng và UE tăng giá trị lên ít nhất 1 sau mỗi lần xác thực lại. Điều này cho phép UE kiểm tra độ mới của thông điệp. FRID mới và bộ đếm được cập nhật cho ngữ cảnh bảo mật được liên kết với ID của UE. Nonce vốn là RAND được chọn bởi thực thể xác thực mạng cũng được cập nhật cho ngữ cảnh bảo mật được liên kết với ID của UE.

Ở bước 2120, thực thể xác thực mạng tạo và truyền yêu cầu xác thực lại AKA với *bộ đếm, *nonce, *FRID mới và MAC. Trường này với dấu "*" nghĩa là trường này được mật mã hóa bằng khóa mật mã để xác thực lại nhanh AKA. MAC được tạo bằng cách sử dụng SK. Các tham số đầu

vào của MAC gồm bộ đếm, nonce, FRID mới, và có thể được biểu diễn theo cách thức sau,

$MAC = MAC_{SK}$(bộ đếm||nouce||FRID mới)

Ở bước 2125, thực thể xác thực mạng nhận Thông điệp đáp ứng xác thực lại AKA. Đáp ứng lại, thực thể xác thực mạng xác thực UE bằng cách kiểm chứng MAC của thông điệp đáp ứng xác thực lại AKA nhận được và giá trị của bộ đếm. Giá trị của bộ đếm nhận được sẽ giống như giá trị của bộ đếm của thực thể xác thực mạng. Tiến trình 2100 kết thúc nếu xác thực không hợp lệ. Nếu xác thực là hợp lệ, tiến trình 2100 chuyển sang bước 2130.

Ở bước 2130, thực thể xác thực mạng dẫn xuất các khóa để truy nhập tế bào hoặc phi tế bào. Tiến trình này giống bước 2020 của tiến trình 2000.

Ở bước 2135, thực thể xác thực mạng lưu trữ bộ đếm được tăng và FRID mới trong ngữ cảnh bảo mật được liên kết với ID của UE.

Ở bước 2140, thực thể xác thực mạng tạo và truyền thông điệp kết quả đến BS hoặc Wi-Fi AP để thông báo UE về kết quả xác thực nhanh. Thông điệp kết quả sẽ chứa các khóa để truy nhập tế bào hoặc phi tế bào của UE. Lưu ý rằng thông điệp kết quả không được truyền trực tiếp đến UE. Thay vào đó, nếu các khóa khả dụng trong thông điệp kết quả, thực thể mạng sẽ loại bỏ các khóa khỏi thông điệp kết quả và chỉ đơn giản chỉ báo rằng xác thực thành công đến UE. Tiến trình 2100 kết thúc sau bước 2140.

Nhiều phiên xác thực lại cộng tác của truy nhập không đồng nhất

Fig.22 minh họa các phiên xác thực cộng tác theo phương án thực hiện. Thiết bị truyền thông thứ nhất của UE bắt đầu với thiết lập kết nối với cổng nối tế bào chẳng hạn cổng nối 3GPP hoặc cổng phi tế bào chẳng hạn Wi-Fi AP qua phần thứ nhất của khung làm việc xác thực đồng nhất ở bước 2205.

Ở bước 2210, UE xác thực với thực thể xác thực mạng và thực hiện xác thực đầy đủ qua phần thứ nhất để xác thực lẫn nhau.

Ở bước 2215, thiết bị truyền thông thứ hai của UE thiết lập kết nối với cổng nối tế bào chẳng hạn cổng nối 3GPP hoặc cổng nối phi tế bào chẳng hạn Wi-Fi AP qua phần thứ hai của khung làm việc xác thực đồng nhất.

Ở bước 2220, UE xác thực với thực thể xác thực mạng và thực hiện xác thực lại qua phần thứ hai để xác thực lẫn nhau.

Ở bước 2225, nếu thiết bị truyền thông thứ nhất của UE mất kết nối với cổng nối, thiết bị truyền thông thứ nhất của UE thiết lập lại kết nối ở bước 2230. Ở bước 2235, UE thiết lập kết nối với cổng nối bằng cách sử dụng phần thứ nhất hoặc thứ hai hai của khung làm việc xác thực đồng nhất. Cổng nối này có thể là cổng nối tương tự ở bước 2205. Theo cách khác, cổng nối này có thể là cổng nối khác cổng nối ở bước 2205.

Lưu ý rằng UE và thực thể xác thực mạng có thể thực hiện nhiều phiên xác thực nhanh sau khi xác thực đầy đủ. Ngoài ra, các thiết bị truyền thông thứ nhất và thứ hai của UE có thể chia sẻ một tập FRID, các khóa xác thực lại nhanh và bộ đếm. Theo cách khác, cả UE lẫn máy chủ xác thực có thể tạo hai tập FRID, các khóa xác thực lại nhanh và bộ đếm trong suốt hoặc sau khi xác thực đầy đủ. Một tập dành cho thiết bị truyền thông thứ nhất, và tập còn lại dành cho thiết bị truyền thông thứ hai. UE và thực thể xác thực mạng sẽ lưu trữ và duy trì hai tập sau khi tạo chúng.

Hình dung rằng khung làm việc xác thực đồng nhất có thể được áp dụng trong phiên truyền thông giữa UE di động với mạng có các công nghệ truy nhập khác nhau, chẳng hạn, các mạng 5G. Khung làm việc xác thực đồng nhất cho phép quản lý xác thực nhanh và xác thực đồng nhất cho các mạng di động với truy nhập không đồng nhất. Điều này đơn giản hóa quản lý xác thực, cho phép chuyển vùng nhanh giữa các kỹ thuật truy nhập không đồng nhất, và cải thiện trải nghiệm người dùng. Cũng giảm tải công việc của HSS.

Fig.23 minh họa phương án thực hiện thể hiện nhiều công nghệ truy nhập. Hệ thống mạng thế hệ tiếp theo sẽ hỗ trợ nhiều công nghệ truy nhập, gồm vô tuyến thế hệ tiếp theo, các công nghệ truy nhập Wi-Fi, và bluetooth v.v.. Nhiều UE hỗ trợ công nghệ đa truy nhập và UE có thể thiết lập nhiều kết nối đồng thời đến mạng với cùng các chứng nhận 3GPP. Do SA2 đã đề xuất khung làm việc xác thực đồng nhất và cấu trúc ngữ cảnh bảo mật đã được định nghĩa ở phía mạng. Cấu trúc ngữ cảnh bảo mật chưa được định nghĩa cho UE. Do vậy, trong đề xuất này, cấu trúc ngữ cảnh bảo mật được đề xuất ở phía UE với khung làm việc xác thực đồng nhất và cấu trúc ngữ cảnh bảo mật phía mạng được xem xét.

Với hệ thống 5G, thông thường UE có thể kết nối với mạng bằng nhiều kết nối đồng thời. Các kết nối khác nhau có thể cư trú trên các công nghệ truy nhập khác nhau. Tuy nhiên, công nghệ truy nhập khác có thể xác thực với mạng bằng các chứng nhận 3GPP giống nhau. Trong các kịch bản này, cách UE xác thực với mạng và cách dẫn xuất ngữ cảnh bảo mật cho mỗi công nghệ truy nhập cần được nghiên cứu.

Trong phần này, công nghệ truy nhập khác chia sẻ cùng máy trạm ở phía UE được đề xuất. Máy trạm chịu trách nhiệm xác thực cho các công nghệ chia sẻ khác nhau.

Khi máy trạm thực hiện xác thực lẫn nhau với khối xác thực ở phía mạng (CP-AU), nếu ngữ cảnh bảo mật đã không được thiết lập ở máy trạm, thì UE thiết lập ngữ cảnh bảo mật trong máy trạm.

Nếu bên nhận đã có một ngữ cảnh bảo mật được thiết lập, thì UE có thể sử dụng ngữ cảnh bảo mật hiện tại để xác thực lẫn nhau với thực thể xác thực mạng. Nếu xác thực thành công, cả máy trạm lẫn CP-AU cập nhật ngữ cảnh bảo mật.

Các máy trạm truyền ngữ cảnh bảo mật được dẫn xuất đến công nghệ truy nhập liên quan để bảo vệ các phiên truyền thông.

Fig.24

Fig.24 thể hiện thủ tục chi tiết cho UE với hai công nghệ truy nhập khác nhau để thiết lập ngữ cảnh bảo mật với khung làm việc xác thực đồng nhất và phương pháp dẫn xuất ngữ cảnh bảo mật được nêu trên:

Thiết bị với công nghệ truy nhập 1 trong UE gửi yêu cầu đến máy trạm để xác thực.

Xác thực máy trạm với CP-AU trong CN, trong quá trình đó máy trạm và CP-AU truyền thông với bộ nhớ đáng tin cậy tính toán và chứng nhận kho để lần lượt xác thực các vectơ (2a và 2b).

Máy trạm và CP-AU thiết lập ngữ cảnh bảo mật xác thực với cả CP-AU lẫn máy trạm (3a và 3b)

Máy trạm và CP-AU truyền ngữ cảnh bảo mật đến thiết bị liên quan ở phía UE và mạng truy nhập ở phía mạng.

Cả hai thiết bị và AN đã cài đặt ngữ cảnh bảo mật và sử dụng chúng để bảo vệ dữ liệu/báo hiệu.

Thiết bị với công nghệ truy nhập 1 trong UE gửi yêu cầu đến máy trạm để xác thực.

Xác thực máy trạm với CP-AU trong CN. Thủ tục xác thực tận dụng lại ngữ cảnh bảo mật được thiết lập qua xác thực cho công nghệ truy nhập thứ nhất.

Máy trạm và CP-AU cập nhật ngữ cảnh bảo mật xác thực.

Máy trạm và CP-AU truyền ngữ cảnh bảo mật đến thiết bị liên quan (thiết bị có công nghệ truy nhập 2) ở phía UE và mạng truy nhập ở phía truy nhập.

Cả hai thiết bị và AN đã cài đặt ngữ cảnh bảo mật và sử dụng chúng để bảo vệ dữ liệu/báo hiệu.

Phần trên là phần mô tả các phương án thực hiện của phương pháp và hệ thống của khung làm việc xác thực thống nhất để xác thực cộng tác giữa thiết bị di động và CN. Thấy trước rằng chuyên gia trong lĩnh vực có thể

và sẽ thiết kế phương pháp và hệ thống thay thế dựa trên sáng chế mà vi phạm sáng chế sẽ được đề xuất trong các điểm yêu cầu bảo hộ dưới đây.

YÊU CẦU BẢO HỘ

1. Phương pháp truyền thông để thiết bị người dùng (user equipment, UE) truyền thông với mạng lõi, trong đó phương pháp bao gồm các bước:

xác thực, bằng mạng lõi, bộ phận truyền thông thứ nhất của UE, trong đó bộ phận truyền thông thứ nhất của UE được liên kết với công nghệ truy nhập thứ nhất;

tạo, bằng mạng lõi, ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất của UE khi xác thực thành công, trong đó ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất bao gồm định danh xác thực lại nhanh;

nhận, bằng mạng lõi, yêu cầu xác thực từ bộ phận truyền thông thứ hai của UE qua công nghệ truy nhập thứ hai;

xác định, bằng mạng lõi, liệu yêu cầu xác thực bao gồm định danh xác thực lại nhanh; và

khởi tạo, bằng mạng lõi, thủ tục xác thực lại nhanh đáp lại xác định yêu cầu bao gồm định danh xác thực lại nhanh,

trong đó hoạt động khởi tạo thủ tục xác thực lại nhanh bao gồm bước:

cập nhật, bằng mạng lõi, ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất của UE.

2. Phương pháp theo điểm 1, trong đó bước cập nhật ngữ cảnh bảo mật bao gồm bước cập nhật, bằng mạng lõi, bộ đếm trong ngữ cảnh bảo mật.

3. Phương pháp theo điểm 2, trong đó công nghệ truy nhập thứ nhất là công nghệ truy nhập 3GPP, và công nghệ truy nhập thứ hai là công nghệ truy nhập phi 3GPP.

4. Phương pháp theo điểm 2, trong đó công nghệ truy nhập thứ nhất là công nghệ truy nhập phi 3GPP, và công nghệ truy nhập thứ hai là công nghệ truy nhập 3GPP.

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

truyền, bằng mạng lõi, ngữ cảnh bảo mật được cập nhật đến mạng truy nhập sau cho mạng truy nhập sử dụng ngữ cảnh bảo mật được cập nhật để

bảo vệ báo hiệu.

6. Phương pháp truyền thông để UE truyền thông với mạng lõi, trong đó phương pháp bao gồm các bước:

tạo, bởi UE, ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất của UE đáp lại xác thực thành công bộ phận truyền thông thứ nhất, trong đó bộ phận truyền thông thứ nhất được liên kết với công nghệ truy nhập thứ nhất, và trong đó ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất bao gồm định danh xác thực lại nhanh;

gửi, bởi UE, yêu cầu đến mạng lõi qua công nghệ truy nhập thứ hai, trong đó yêu cầu bao gồm ID xác thực lại nhanh; và

cập nhật, bởi UE, ngữ cảnh bảo mật khi bộ phận truyền thông thứ nhất của UE được xác thực thành công.

7. Phương pháp theo điểm 6, trong đó hoạt động cập nhật ngữ cảnh bảo mật bao gồm cập nhật, bởi UE, bộ đếm trong ngữ cảnh bảo mật.

8. Phương pháp theo điểm 7, trong đó công nghệ truy nhập thứ nhất là công nghệ truy nhập 3GPP, và công nghệ truy nhập thứ hai là công nghệ truy nhập phi 3GPP.

9. Phương pháp theo điểm 7, trong đó công nghệ truy nhập thứ nhất là công nghệ truy nhập phi 3GPP, và công nghệ truy nhập thứ hai là công nghệ truy nhập 3GPP.

10. Thiết bị truyền thông bao gồm:

ít nhất một bộ nhớ để lưu trữ các lệnh; và

ít nhất một bộ xử lý được ghép nối với ít nhất một bộ nhớ, và để thực thi các lệnh được lưu trữ để:

xác thực bộ phận truyền thông thứ nhất của UE, trong đó bộ phận truyền thông thứ nhất của UE được liên kết với công nghệ truy nhập thứ nhất;

tạo ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất của UE khi xác thực thành công, trong đó ngữ cảnh bảo mật của bộ phận truyền thông

thứ nhất bao gồm định danh xác thực lại nhanh;

nhận yêu cầu xác thực từ bộ phận truyền thông thứ hai của UE qua công nghệ truy nhập thứ hai;

xác định liệu yêu cầu này có để xác thực lại nhanh hay không; và

khởi tạo thủ tục xác thực lại nhanh đáp lại xác định yêu cầu bao gồm ID xác thực lại nhanh, trong đó thủ tục bao gồm cập nhật ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất của UE.

11. Thiết bị theo điểm 10, trong đó khi cập nhật ngữ cảnh bảo mật, ít nhất một bộ xử lý còn thực thi các lệnh được lưu trữ để cập nhật bộ đếm trong ngữ cảnh bảo mật.

12. Thiết bị theo điểm 11, trong đó công nghệ truy nhập thứ nhất là công nghệ truy nhập 3GPP, và công nghệ truy nhập thứ hai là công nghệ truy nhập phi 3GPP.

13. Thiết bị theo điểm 11, trong đó công nghệ truy nhập thứ nhất là công nghệ truy nhập phi 3GPP, và công nghệ truy nhập thứ hai là công nghệ truy nhập 3GPP.

14. Thiết bị theo điểm 12, trong đó bộ xử lý còn thực thi các lệnh được lưu trữ để truyền ngữ cảnh bảo mật được cập nhật đến mạng truy nhập sau cho mạng truy nhập sử dụng ngữ cảnh bảo mật được cập nhật để bảo vệ báo hiệu.

15. Thiết bị người dùng (user equipment, UE) để truyền thông trực tiếp với mạng lõi, trong đó UE bao gồm:

ít nhất một bộ nhớ để lưu trữ các lệnh; và

ít nhất một bộ xử lý được ghép nối với ít nhất một bộ nhớ, và để thực thi các lệnh được lưu trữ để:

tạo ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất của UE đáp lại việc xác thực thành công bộ phận truyền thông thứ nhất, trong đó bộ phận truyền thông thứ nhất được liên kết với công nghệ truy nhập thứ nhất, và trong đó ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất bao gồm

định danh xác thực lại nhanh;

gửi yêu cầu đến mạng lõi qua công nghệ truy nhập thứ hai, trong đó yêu cầu bao gồm ID xác thực lại nhanh; và

cập nhật ngữ cảnh bảo mật khi bộ phận truyền thông thứ nhất của UE được xác thực thành công.

16. Thiết bị người dùng theo điểm 15, trong đó khi cập nhật ngữ cảnh bảo mật, ít nhất một bộ xử lý còn thực thi các lệnh được lưu trữ để:

cập nhật bộ đếm trong ngữ cảnh bảo mật.

17. Thiết bị người dùng theo điểm 16, trong đó công nghệ truy nhập thứ nhất là công nghệ truy nhập 3GPP, và công nghệ truy nhập thứ hai là công nghệ truy nhập phi 3GPP.

18. Thiết bị người dùng theo điểm 16, trong đó công nghệ truy nhập thứ nhất là công nghệ truy nhập phi 3GPP, và công nghệ truy nhập thứ hai là công nghệ truy nhập 3GPP.

19. Vật ghi máy tính đọc được bất biến bao gồm các lệnh bộ xử lý thực thi được, mà khi được thực thi bởi ít nhất một bộ xử lý, khiến ít nhất một bộ xử lý thực hiện các bước sau:

tạo ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất đáp lại việc xác thực thành công bộ phận truyền thông thứ nhất trong đó ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất bao gồm định danh xác thực lại nhanh;

nhận yêu cầu xác thực từ bộ phận truyền thông thứ hai của UE qua công nghệ truy nhập thứ hai;

xác thực yêu cầu bằng cách sử dụng ngữ cảnh bảo mật, trong đó bảo mật được thiết lập khi UE được xác thực thành công qua công nghệ truy nhập thứ nhất;

xác định liệu yêu cầu này có để xác thực lại nhanh hay không; và

khởi tạo thủ tục xác thực lại nhanh đáp lại xác định rằng yêu cầu bao gồm ID xác thực lại nhanh, trong đó thủ tục xác thực lại nhanh bao gồm

cập nhật ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất của UE.

20. Vật ghi máy tính đọc được bất biến bao gồm các lệnh bộ xử lý thực thi được, mà khi được thực thi bởi ít nhất một bộ xử lý, khiến ít nhất một bộ xử lý thực hiện các bước sau:

tạo ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất của UE khi bộ phận truyền thông thứ nhất được xác thực thành công, trong đó bộ phận truyền thông thứ nhất được liên kết với công nghệ truy nhập thứ nhất, và trong đó ngữ cảnh bảo mật của bộ phận truyền thông thứ nhất bao gồm định danh xác thực lại nhanh;

gửi yêu cầu đến mạng lõi qua công nghệ truy nhập thứ hai, trong đó yêu cầu bao gồm ID xác thực lại nhanh; và

cập nhật ngữ cảnh bảo mật khi bộ phận truyền thông thứ nhất được xác thực thành công.

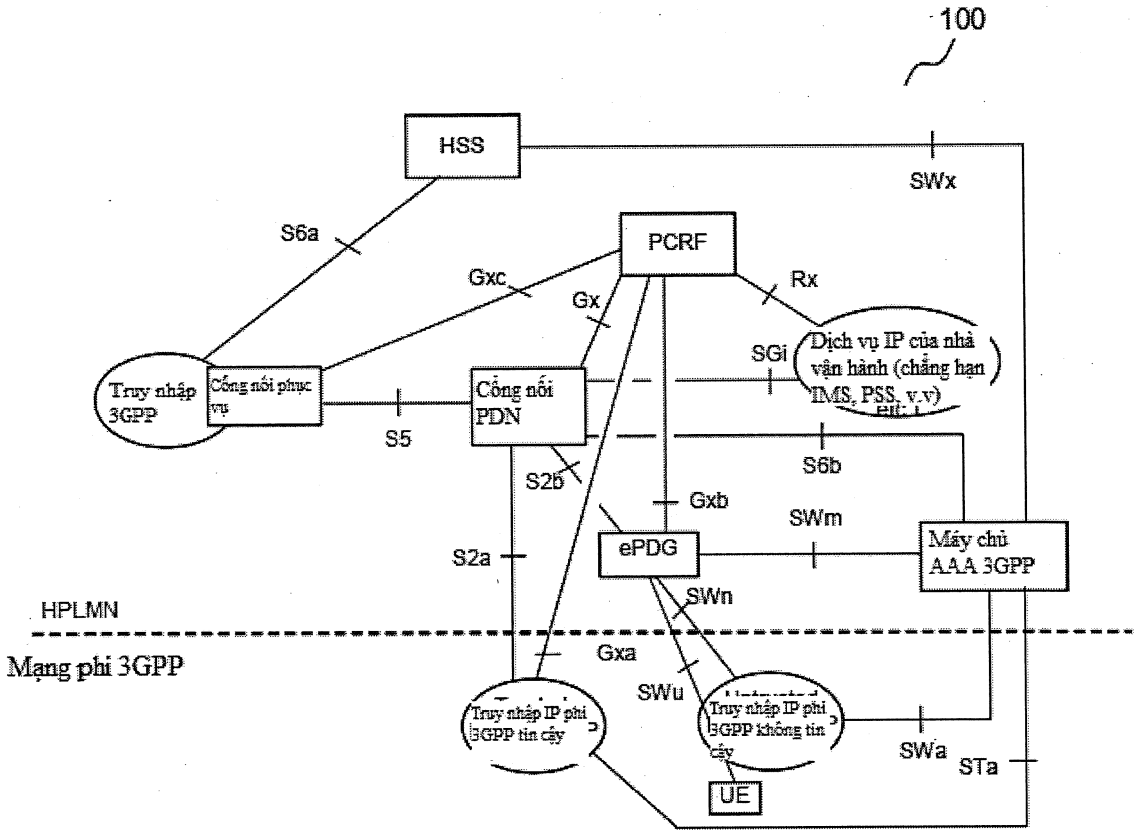

100
HSS
SWx
S6a
PCRF
Gxc
Gx
Rx
SGi
Dịch vụ IP của nhà vận hành (chẳng hạn IMS, PSS, v.v)
Truy nhập 3GPP
Cổng nối phục vụ
Cổng nối PDN
S5
S2b
S6b
Gxb
SWm
S2a
ePDG
Máy chủ AAA 3GPP
SWn
HPLMN
Mạng phi 3GPP
Gxa
SWu
Truy nhập IP phi 3GPP tin cậy
Truy nhập IP phi 3GPP không tin cậy
SWa
STa
UE

Fig.1

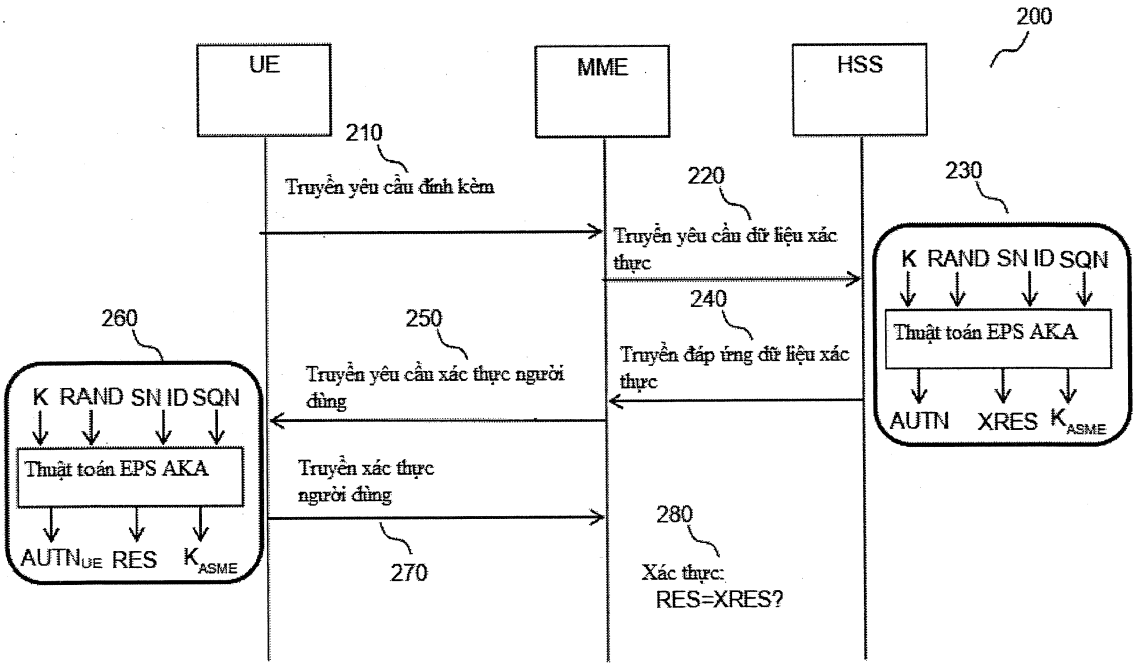

200
UE
MME
HSS
210
Truyền yêu cầu đính kèm
220
Truyền yêu cầu dữ liệu xác thực
230
K RAND SN ID SQN
Thuật toán EPS AKA
AUTN XRES K_{ASME}
240
Truyền đáp ứng dữ liệu xác thực
250
Truyền yêu cầu xác thực người dùng
260
K RAND SN ID SQN
Thuật toán EPS AKA
$AUTN_{UE}$ RES K_{ASME}
Truyền xác thực người dùng
270
280
Xác thực:
RES=XRES?

Fig.2

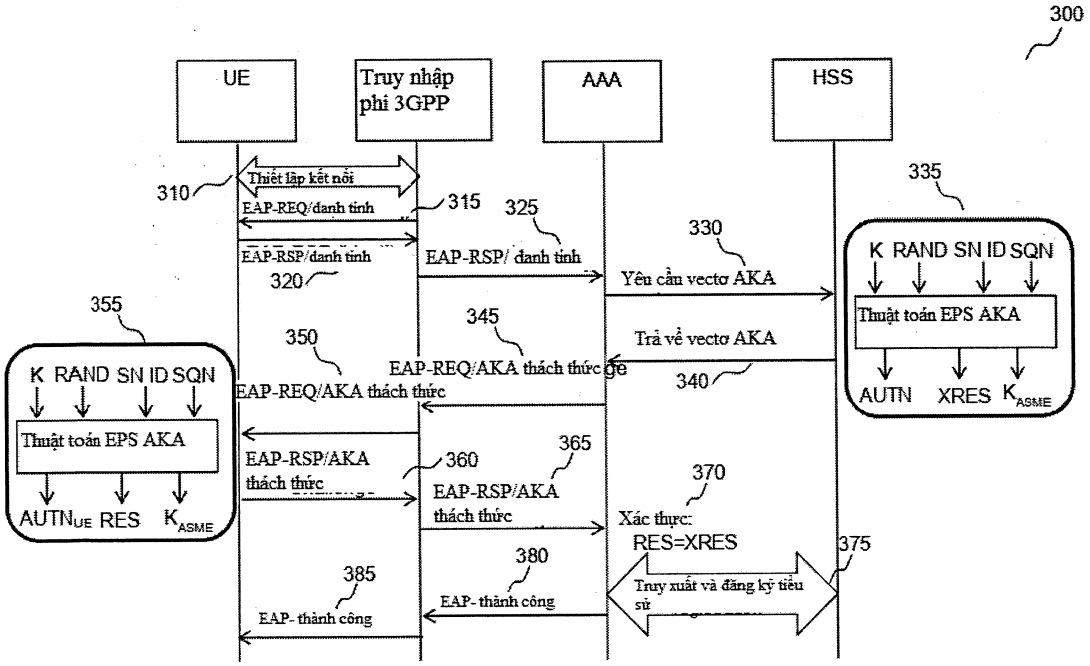

300
UE
Truy nhập phi 3GPP
AAA
HSS
310
Thiết lập kết nối
EAP-REQ/danh tính
315
325
330
335
EAP-RSP/danh tính
EAP-RSP/ danh tính
Yêu cầu vectơ AKA
320
K RAND SN ID SQN
Thuật toán EPS AKA
AUTN XRES K_{ASME}
355
345
Trả về vectơ AKA
350
EAP-REQ/AKA thách thức
EAP-REQ/AKA thách thức
340
K RAND SN ID SQN
Thuật toán EPS AKA
$AUTN_{UE}$ RES K_{ASME}
EAP-RSP/AKA thách thức
360
365
EAP-RSP/AKA thách thức
370
Xác thực:
RES=XRES
375
380
385
Truy xuất và đăng ký tiểu sử
EAP- thành công
EAP- thành công

Fig.3

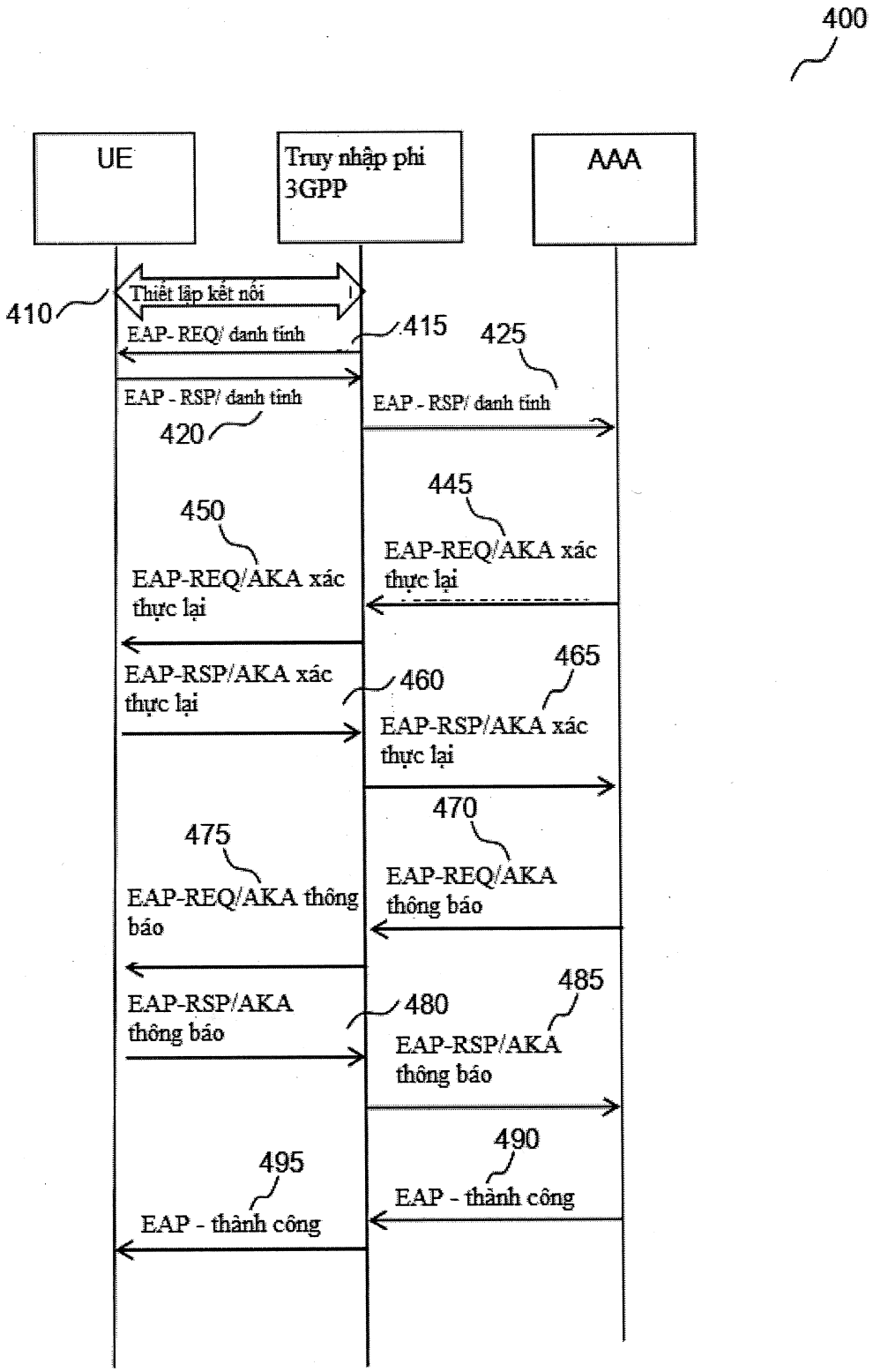

400
UE
Truy nhập phi 3GPP
AAA
410
Thiết lập kết nối
EAP- REQ/ danh tính
415
425
EAP - RSP/ danh tính
EAP - RSP/ danh tính
420
445
450
EAP-REQ/AKA xác thực lại
EAP-REQ/AKA xác thực lại
465
EAP-RSP/AKA xác thực lại
460
EAP-RSP/AKA xác thực lại
470
475
EAP-REQ/AKA thông báo
EAP-REQ/AKA thông báo
485
EAP-RSP/AKA thông báo
480
EAP-RSP/AKA thông báo
490
495
EAP - thành công
EAP - thành công

Fig.4

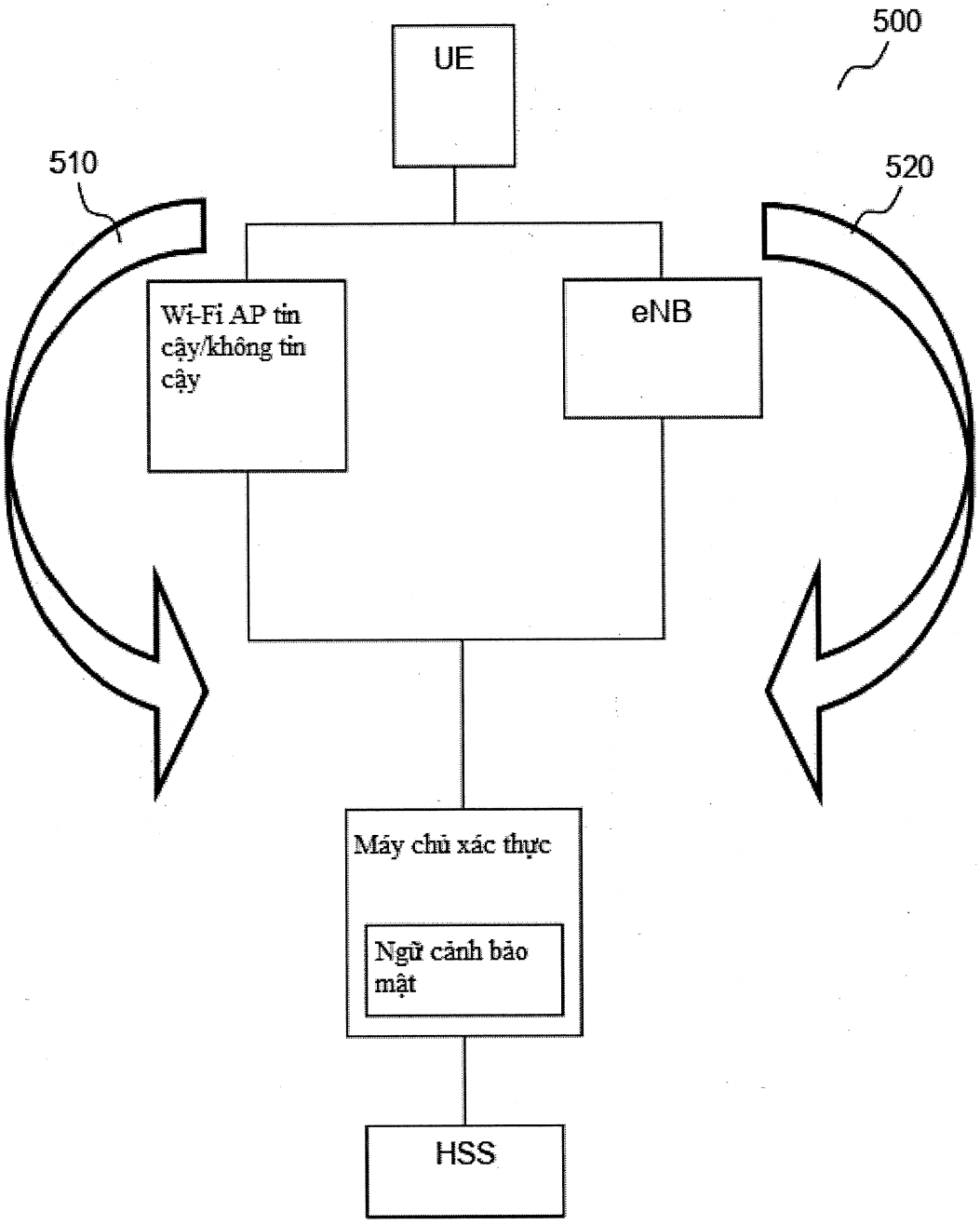

500
UE
510
520
Wi-Fi AP tin cậy/không tin cậy
eNB
Máy chủ xác thực
Ngữ cảnh bảo mật
HSS

Fig.5

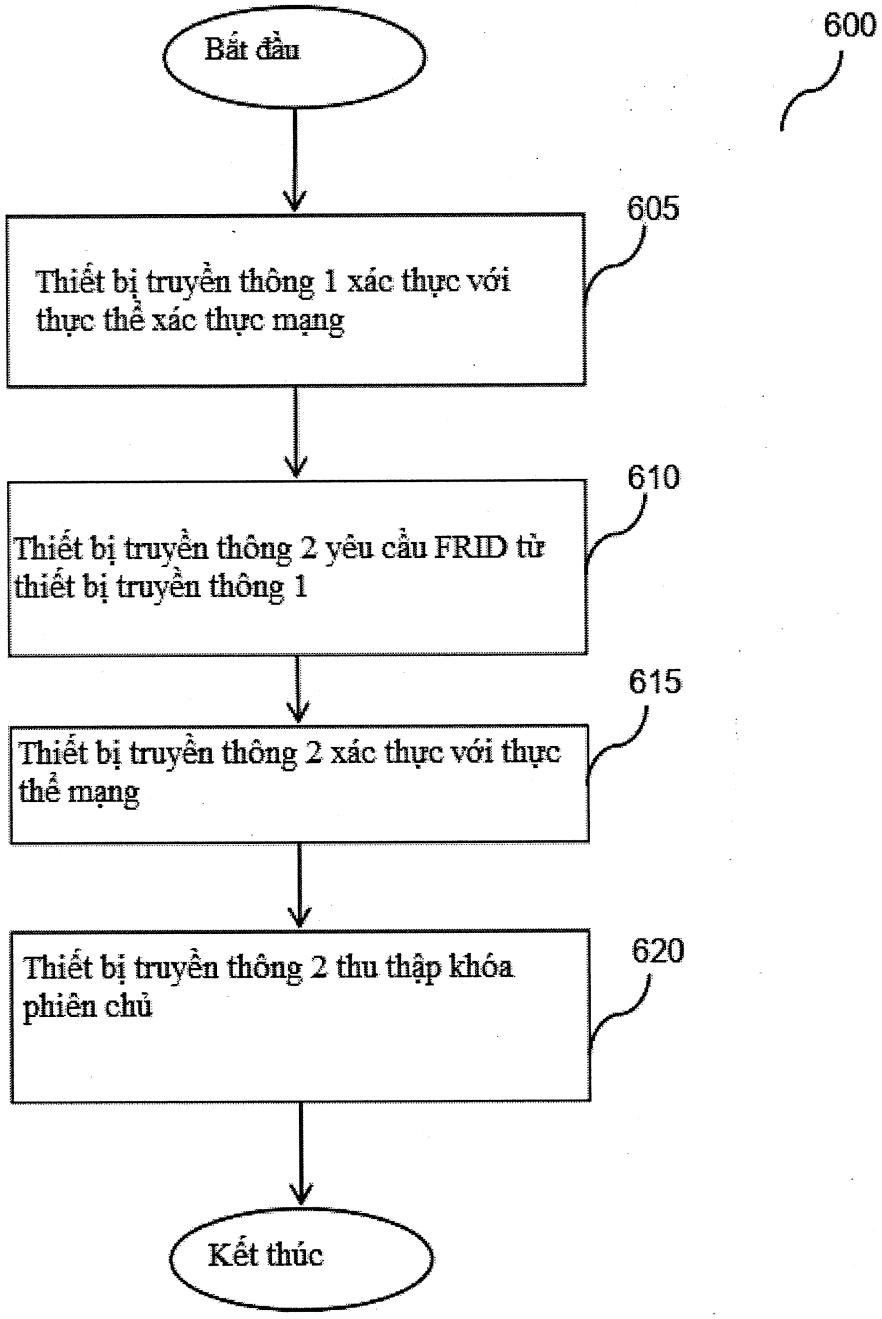

600
Bắt đầu
605
Thiết bị truyền thông 1 xác thực với thực thể xác thực mạng
610
Thiết bị truyền thông 2 yêu cầu FRID từ thiết bị truyền thông 1
615
Thiết bị truyền thông 2 xác thực với thực thể mạng
620
Thiết bị truyền thông 2 thu thập khóa phiên chủ
Kết thúc

Fig.6

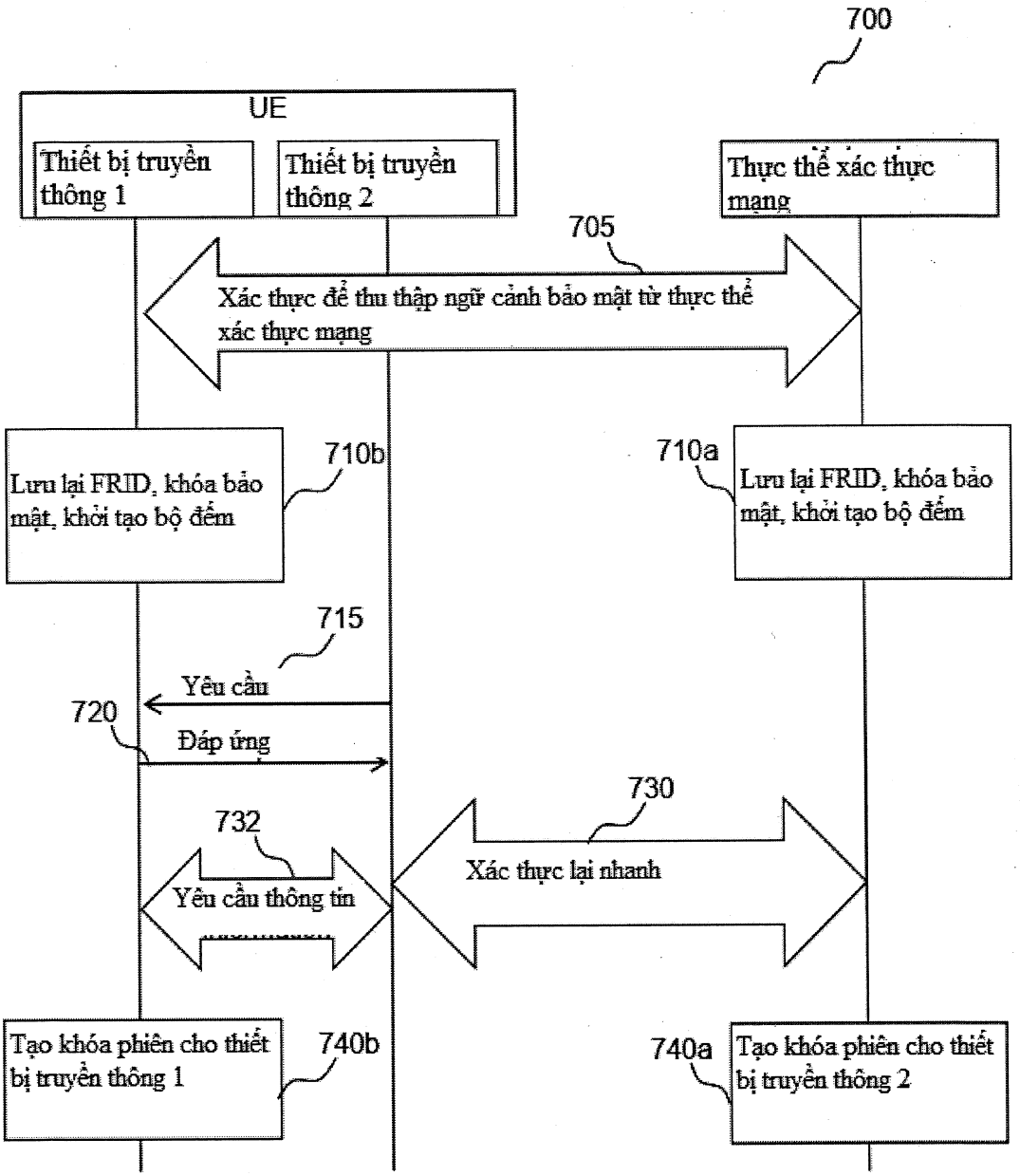

700
UE
Thiết bị truyền thông 1
Thiết bị truyền thông 2
Thực thể xác thực mạng
705
Xác thực để thu thập ngữ cảnh bảo mật từ thực thể xác thực mạng
Lưu lại FRID, khóa bảo mật, khởi tạo bộ đếm
710b
710a
Lưu lại FRID, khóa bảo mật, khởi tạo bộ đếm
715
Yêu cầu
720
Đáp ứng
730
732
Xác thực lại nhanh
Yêu cầu thông tin
Tạo khóa phiên cho thiết bị truyền thông 1
740b
740a
Tạo khóa phiên cho thiết bị truyền thông 2

Fig.7

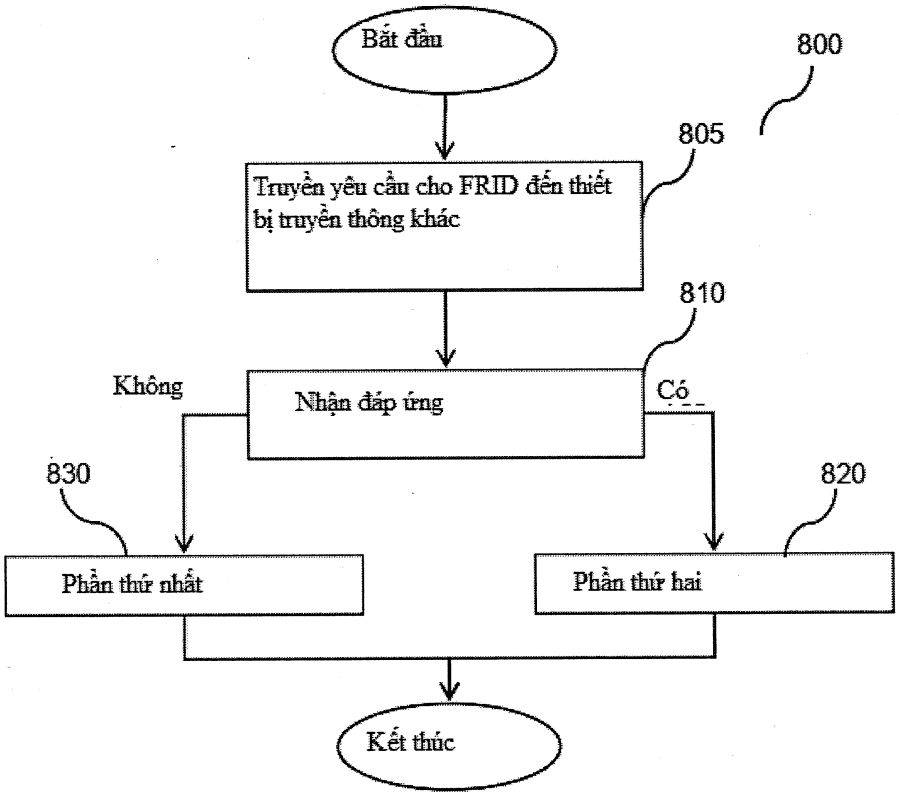

Bắt đầu
800
805
Truyền yêu cầu cho FRID đến thiết bị truyền thông khác
810
Không
Nhận đáp ứng
Có
830
820
Phần thứ nhất
Phần thứ hai
Kết thúc

Fig.8

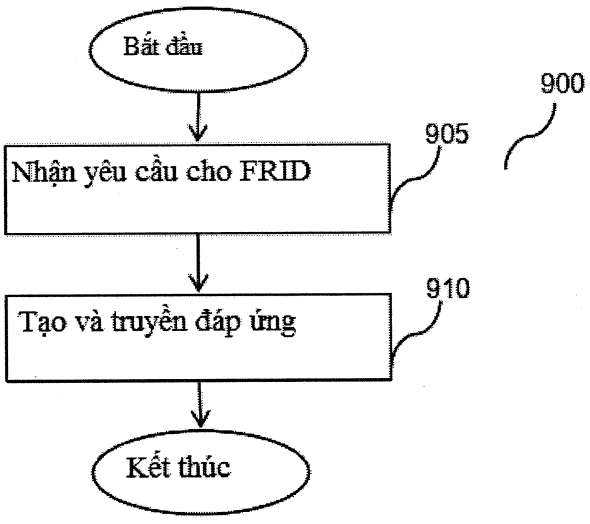

Bắt đầu
900
905
Nhận yêu cầu cho FRID
910
Tạo và truyền đáp ứng
Kết thúc

Fig.9

9/25

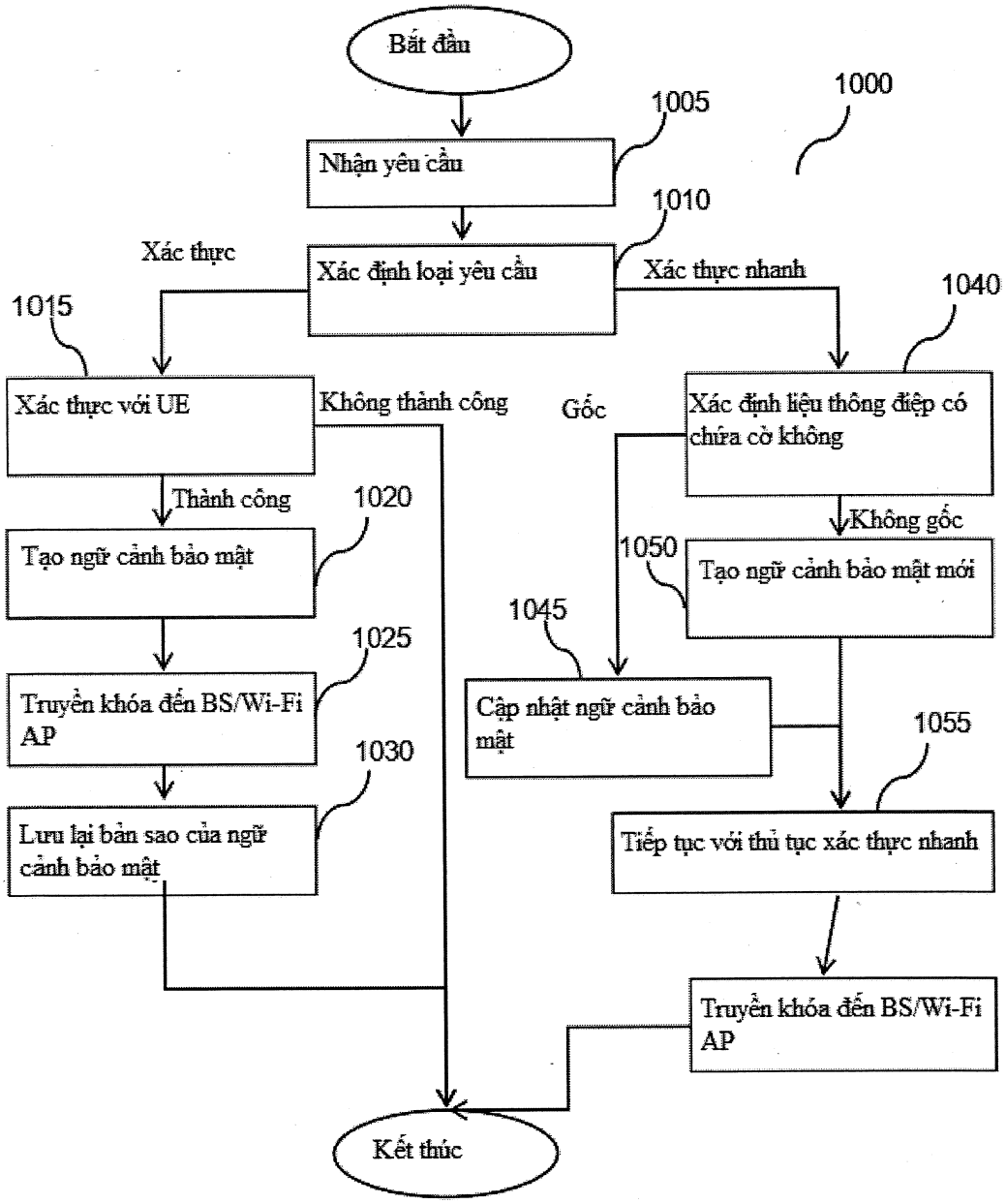

Bắt đầu
1000
1005
Nhận yêu cầu
1010
Xác thực
Xác định loại yêu cầu
Xác thực nhanh
1040
1015
Xác thực với UE
Không thành công
Gốc
Xác định liệu thông điệp có chứa cờ không
Thành công
1020
Không gốc
Tạo ngữ cảnh bảo mật
1050
Tạo ngữ cảnh bảo mật mới
1045
1025
Truyền khóa đến BS/Wi-Fi AP
Cập nhật ngữ cảnh bảo mật
1055
1030
Lưu lại bản sao của ngữ cảnh bảo mật
Tiếp tục với thủ tục xác thực nhanh
Truyền khóa đến BS/Wi-Fi AP
Kết thúc

Fig.10

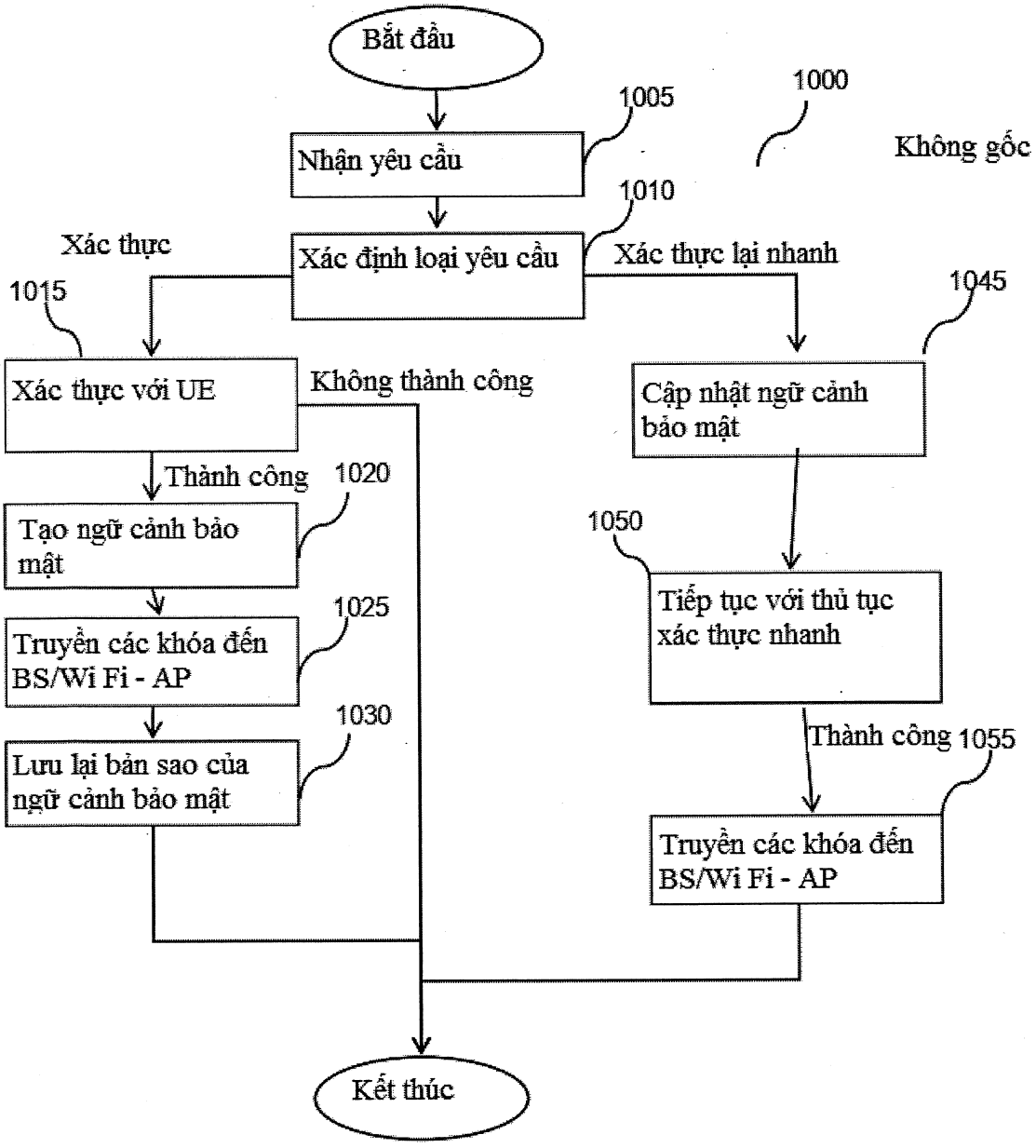

Bắt đầu
1000
1005
Nhận yêu cầu
Không gốc
1010
Xác thực
Xác định loại yêu cầu
Xác thực lại nhanh
1015
1045
Xác thực với UE
Không thành công
Cập nhật ngữ cảnh bảo mật
Thành công
1020
Tạo ngữ cảnh bảo mật
1050
Tiếp tục với thủ tục xác thực nhanh
1025
Truyền các khóa đến BS/Wi Fi - AP
1030
Thành công
1055
Lưu lại bản sao của ngữ cảnh bảo mật
Truyền các khóa đến BS/Wi Fi - AP
Kết thúc

Fig.10A

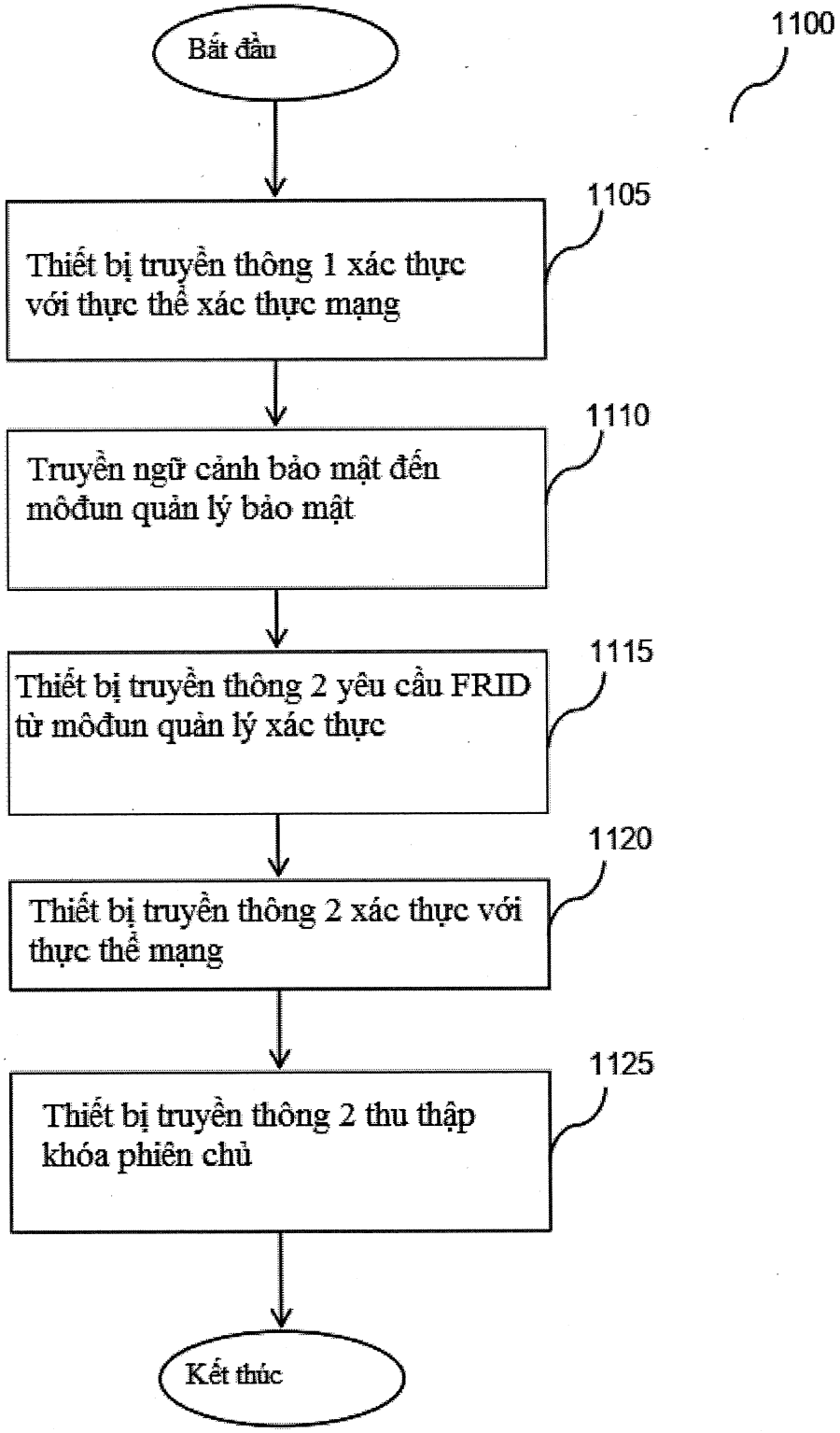

1100
Bắt đầu
1105
Thiết bị truyền thông 1 xác thực với thực thể xác thực mạng
1110
Truyền ngữ cảnh bảo mật đến môđun quản lý bảo mật
1115
Thiết bị truyền thông 2 yêu cầu FRID từ môđun quản lý xác thực
1120
Thiết bị truyền thông 2 xác thực với thực thể mạng
1125
Thiết bị truyền thông 2 thu thập khóa phiên chủ
Kết thúc

Fig.11

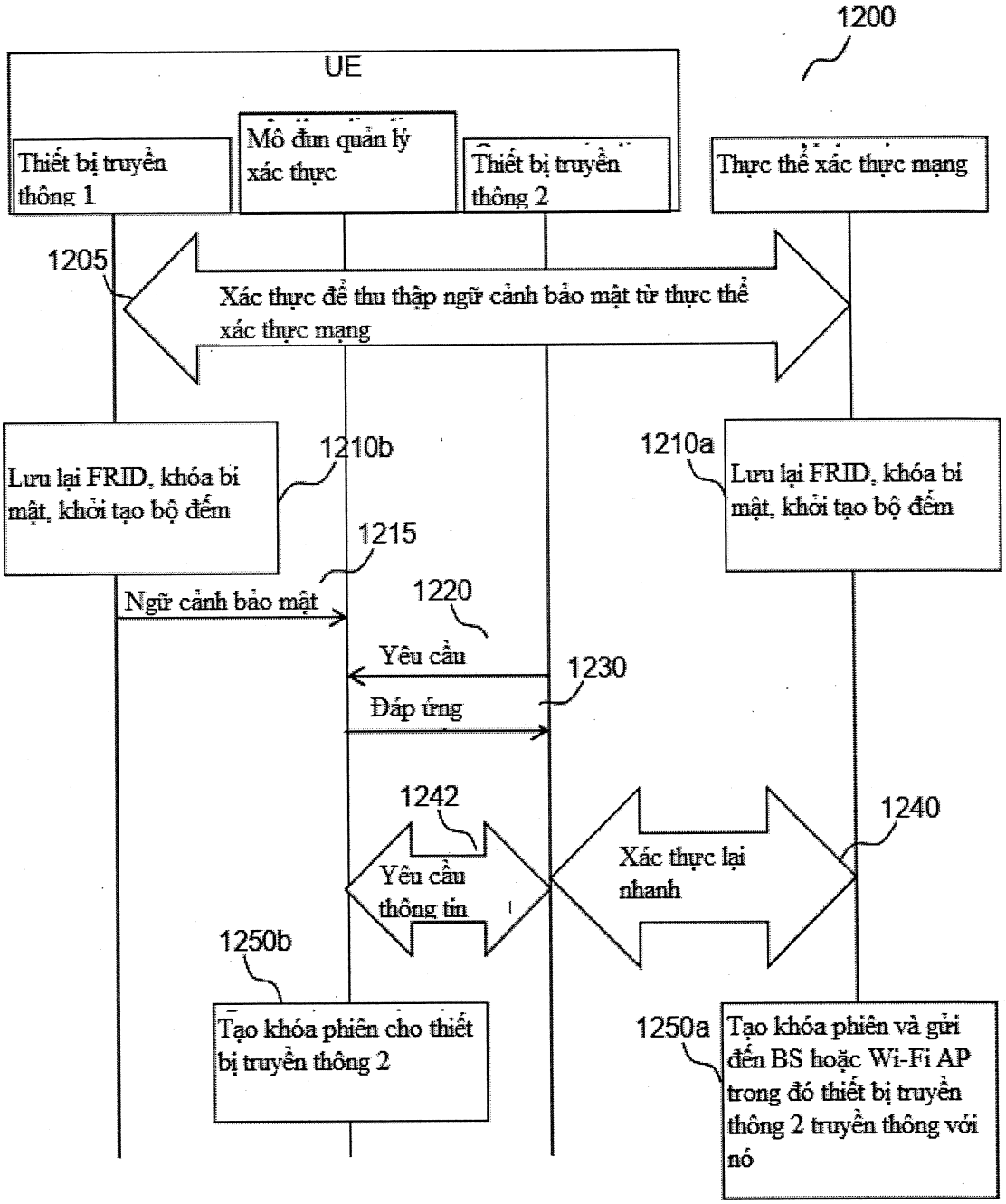

1200
UE
Thiết bị truyền thông 1
Mô đun quản lý xác thực
Thiết bị truyền thông 2
Thực thể xác thực mạng
1205
Xác thực để thu thập ngữ cảnh bảo mật từ thực thể xác thực mạng
1210b
Lưu lại FRID, khóa bí mật, khởi tạo bộ đếm
1210a
Lưu lại FRID, khóa bí mật, khởi tạo bộ đếm
1215
Ngữ cảnh bảo mật
1220
Yêu cầu
1230
Đáp ứng
1242
Yêu cầu thông tin
1240
Xác thực lại nhanh
1250b
Tạo khóa phiên cho thiết bị truyền thông 2
1250a
Tạo khóa phiên và gửi đến BS hoặc Wi-Fi AP trong đó thiết bị truyền thông 2 truyền thông với nó

Fig.12

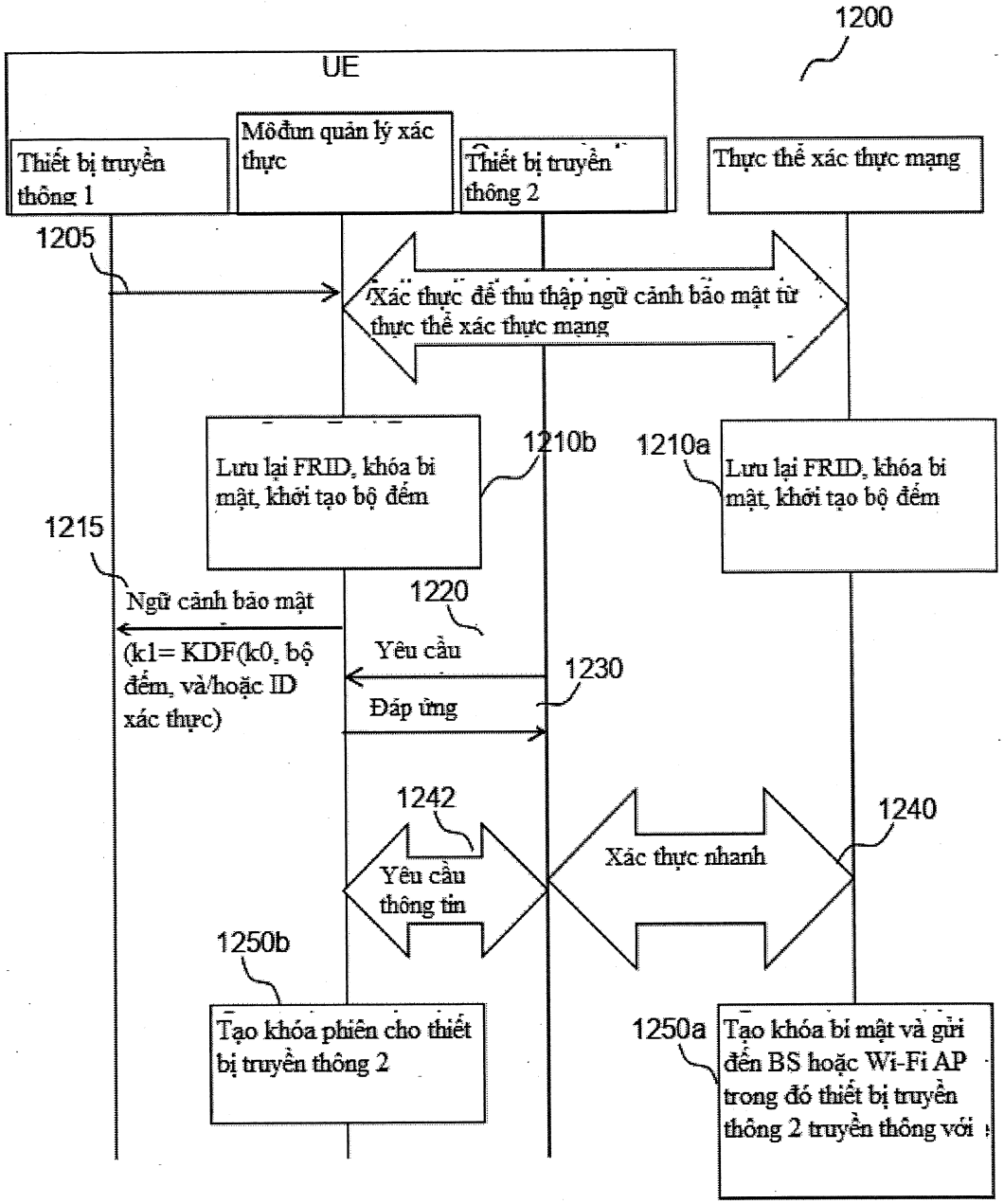

1200
UE
Thiết bị truyền thông 1
Môđun quản lý xác thực
Thiết bị truyền thông 2
Thực thể xác thực mạng
1205
Xác thực để thu thập ngữ cảnh bảo mật từ thực thể xác thực mạng
Lưu lại FRID, khóa bí mật, khởi tạo bộ đếm
1210b
1210a
Lưu lại FRID, khóa bí mật, khởi tạo bộ đếm
1215
Ngữ cảnh bảo mật
(k1= KDF(k0, bộ đếm, và/hoặc ID xác thực)
1220
Yêu cầu
1230
Đáp ứng
1242
Yêu cầu thông tin
Xác thực nhanh
1240
1250b
Tạo khóa phiên cho thiết bị truyền thông 2
1250a
Tạo khóa bí mật và gửi đến BS hoặc Wi-Fi AP trong đó thiết bị truyền thông 2 truyền thông với

Fig.12A

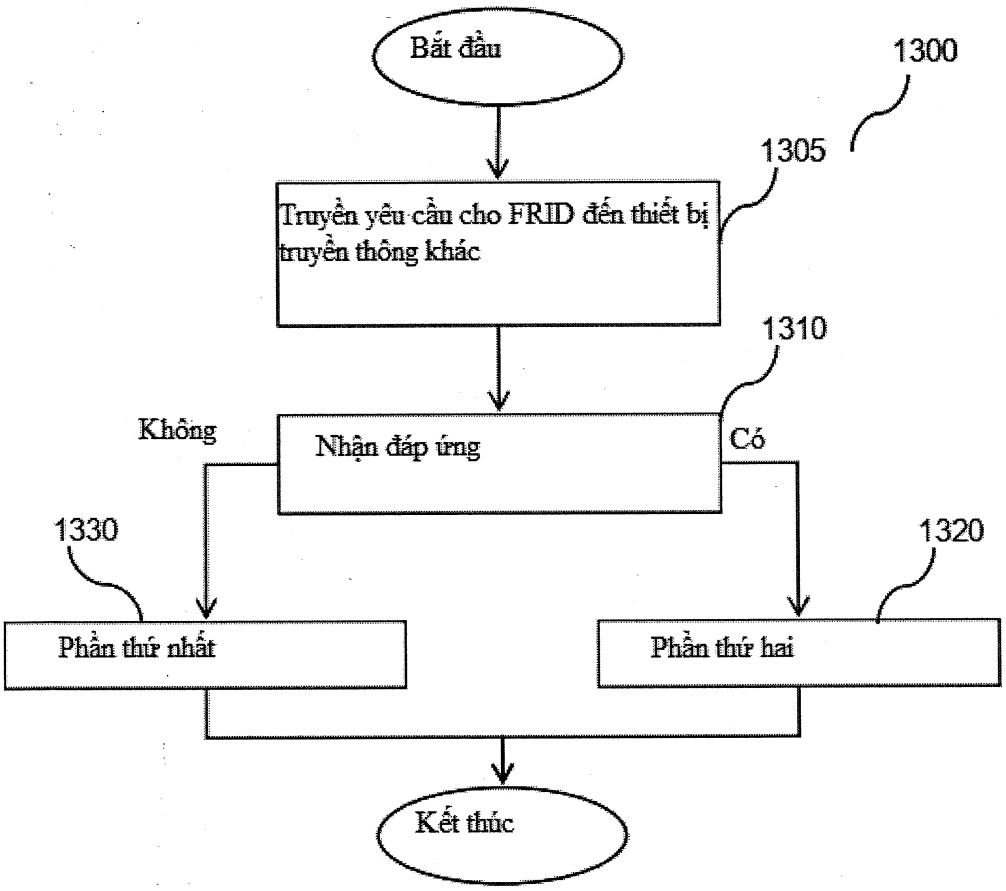

Bắt đầu
1300
1305
Truyền yêu cầu cho FRID đến thiết bị truyền thông khác
1310
Không
Nhận đáp ứng
Có
1330
1320
Phần thứ nhất
Phần thứ hai
Kết thúc

Fig.13

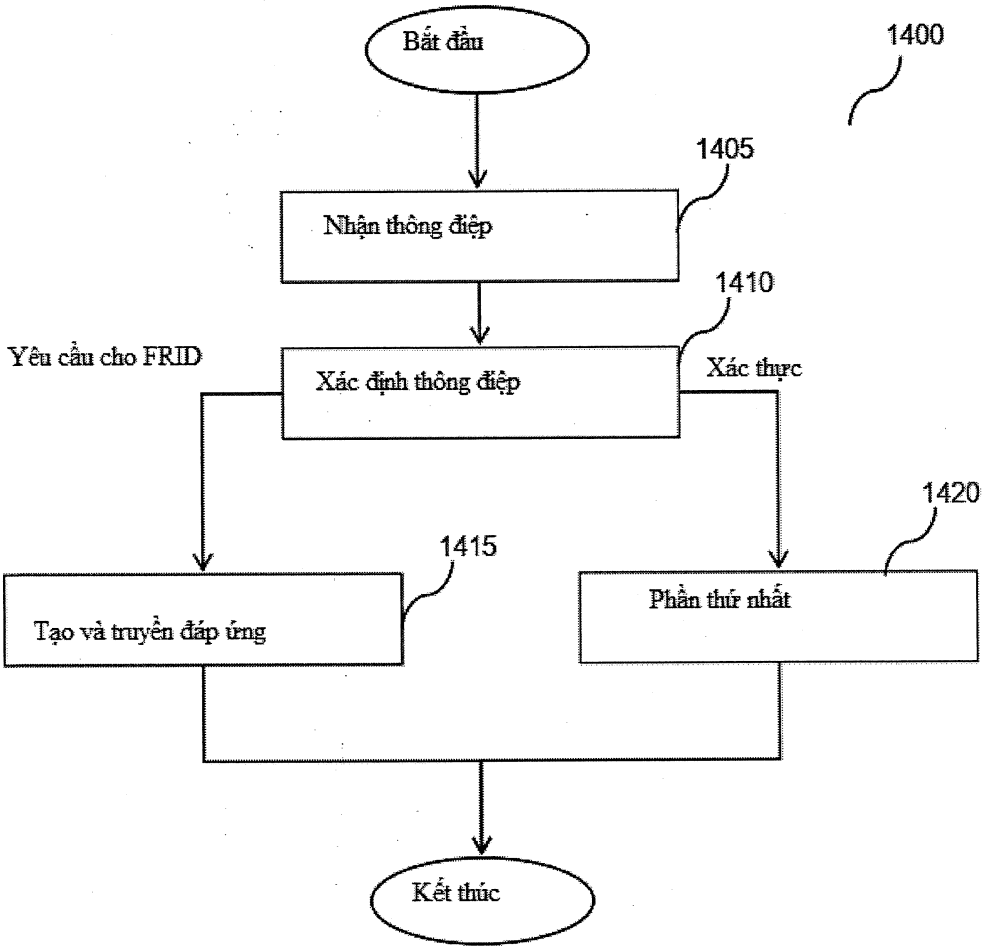

Bắt đầu
1400
1405
Nhận thông điệp
1410
Yêu cầu cho FRID
Xác định thông điệp
Xác thực
1420
1415
Tạo và truyền đáp ứng
Phần thứ nhất
Kết thúc

Fig.14

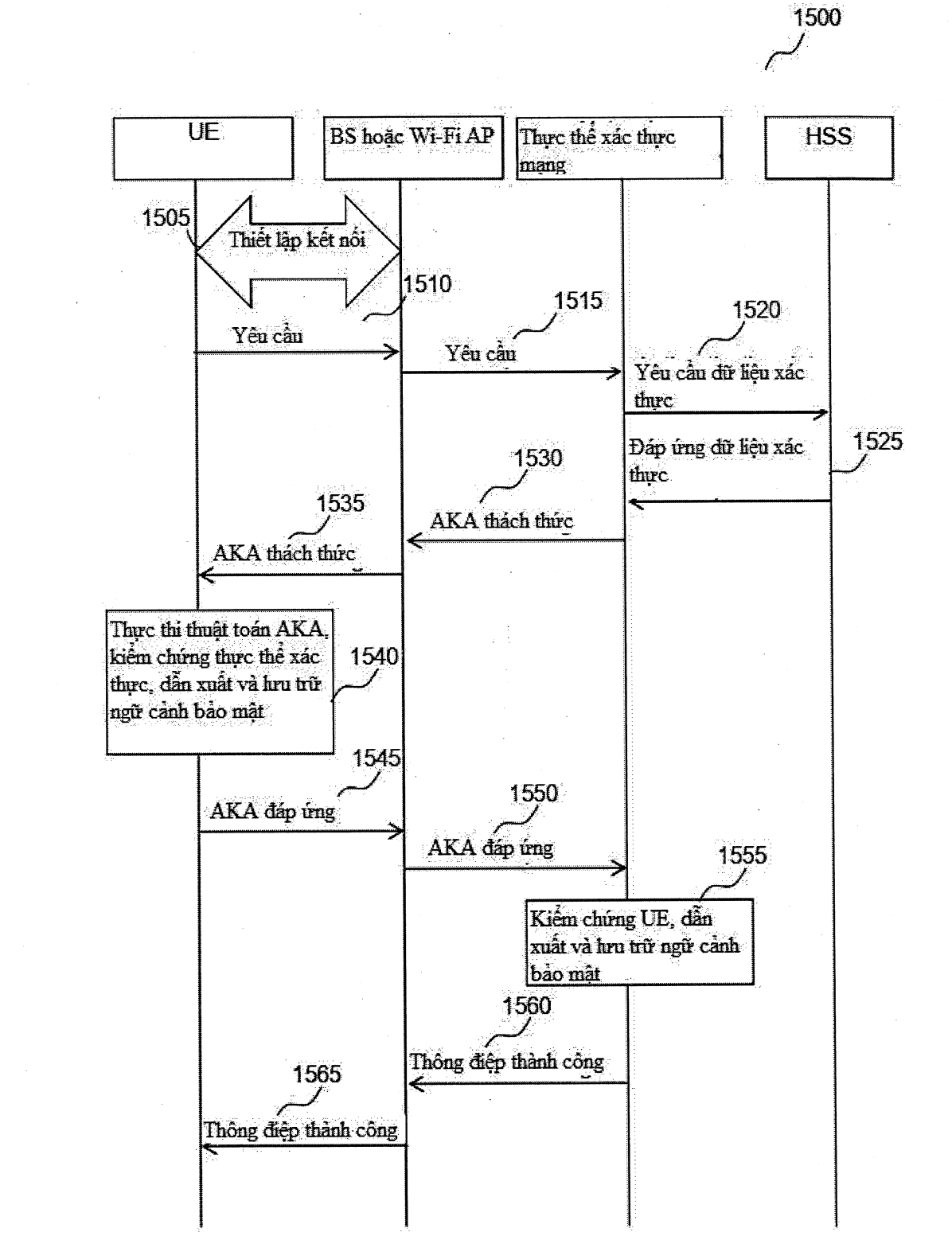

1500
UE
BS hoặc Wi-Fi AP
Thực thể xác thực mạng
HSS
1505
Thiết lập kết nối
1510
Yêu cầu
1515
Yêu cầu
1520
Yêu cầu dữ liệu xác thực
Đáp ứng dữ liệu xác thực
1525
1530
AKA thách thức
1535
AKA thách thức
Thực thi thuật toán AKA, kiểm chứng thực thể xác thực, dẫn xuất và lưu trữ ngữ cảnh bảo mật
1540
1545
AKA đáp ứng
1550
AKA đáp ứng
1555
Kiểm chứng UE, dẫn xuất và lưu trữ ngữ cảnh bảo mật
1560
Thông điệp thành công
1565
Thông điệp thành công

Fig.15

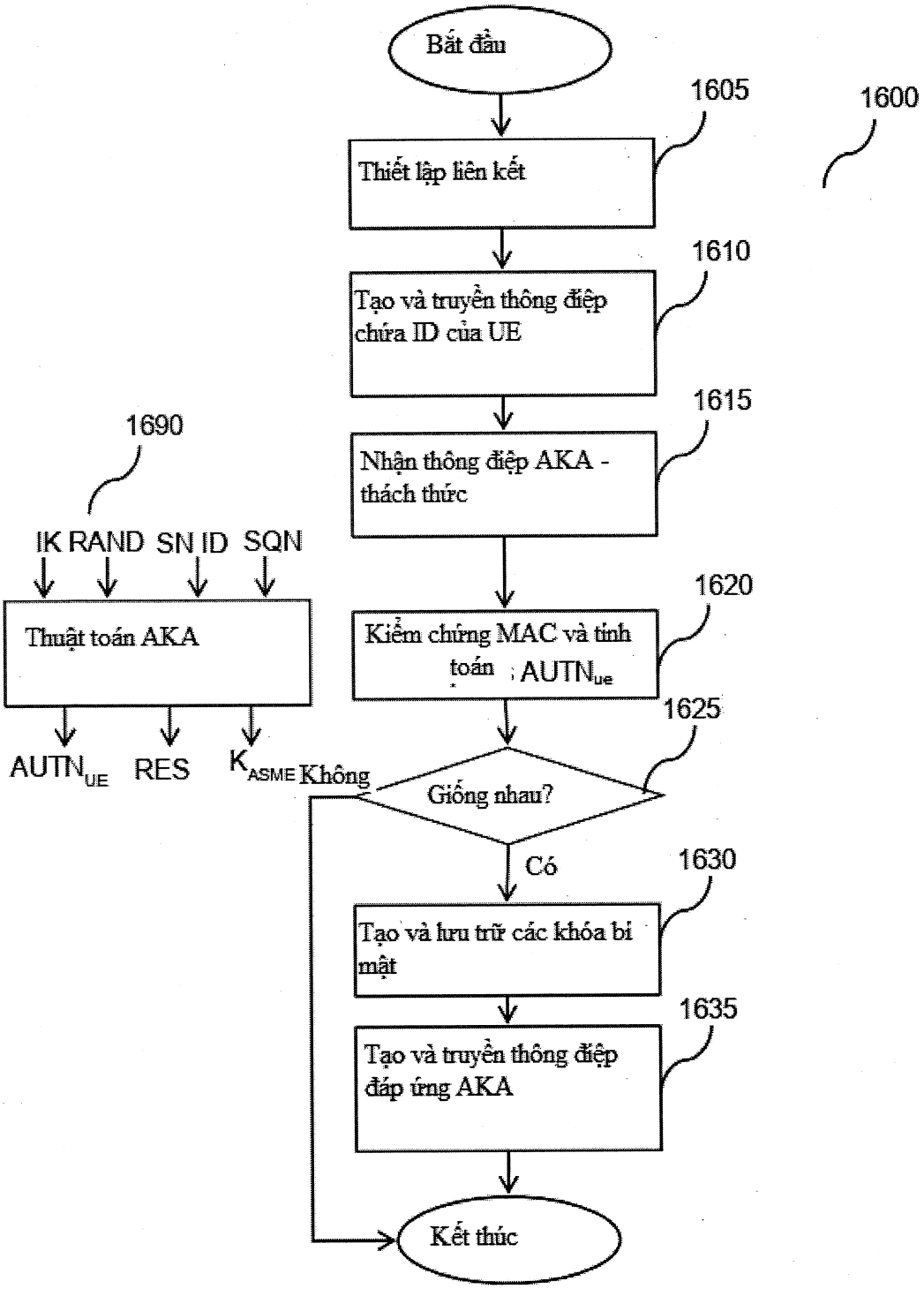

Bắt đầu
1605
1600
Thiết lập liên kết
1610
Tạo và truyền thông điệp chứa ID của UE
1615
Nhận thông điệp AKA - thách thức
1690
IK RAND SN ID SQN
Thuật toán AKA
AUTN$_{UE}$ RES K$_{ASME}$
1620
Kiểm chứng MAC và tính toán ; AUTN$_{ue}$
1625
Giống nhau?
Không
Có
1630
Tạo và lưu trữ các khóa bí mật
1635
Tạo và truyền thông điệp đáp ứng AKA
Kết thúc

Fig.16

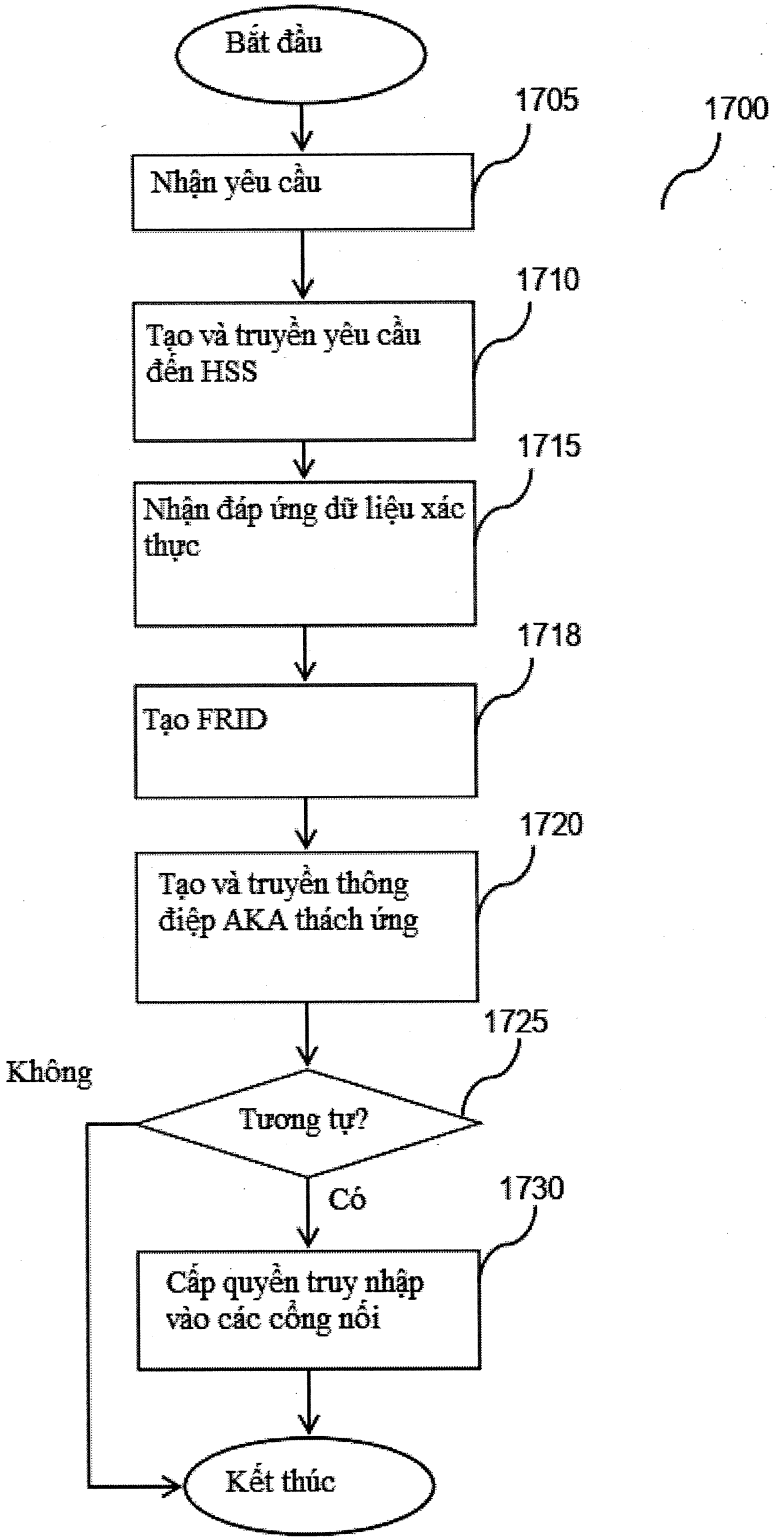

Bắt đầu
1705
1700
Nhận yêu cầu
1710
Tạo và truyền yêu cầu đến HSS
1715
Nhận đáp ứng dữ liệu xác thực
1718
Tạo FRID
1720
Tạo và truyền thông điệp AKA thách ứng
1725
Không
Tương tự?
Có
1730
Cấp quyền truy nhập vào các cổng nối
Kết thúc

Fig.17

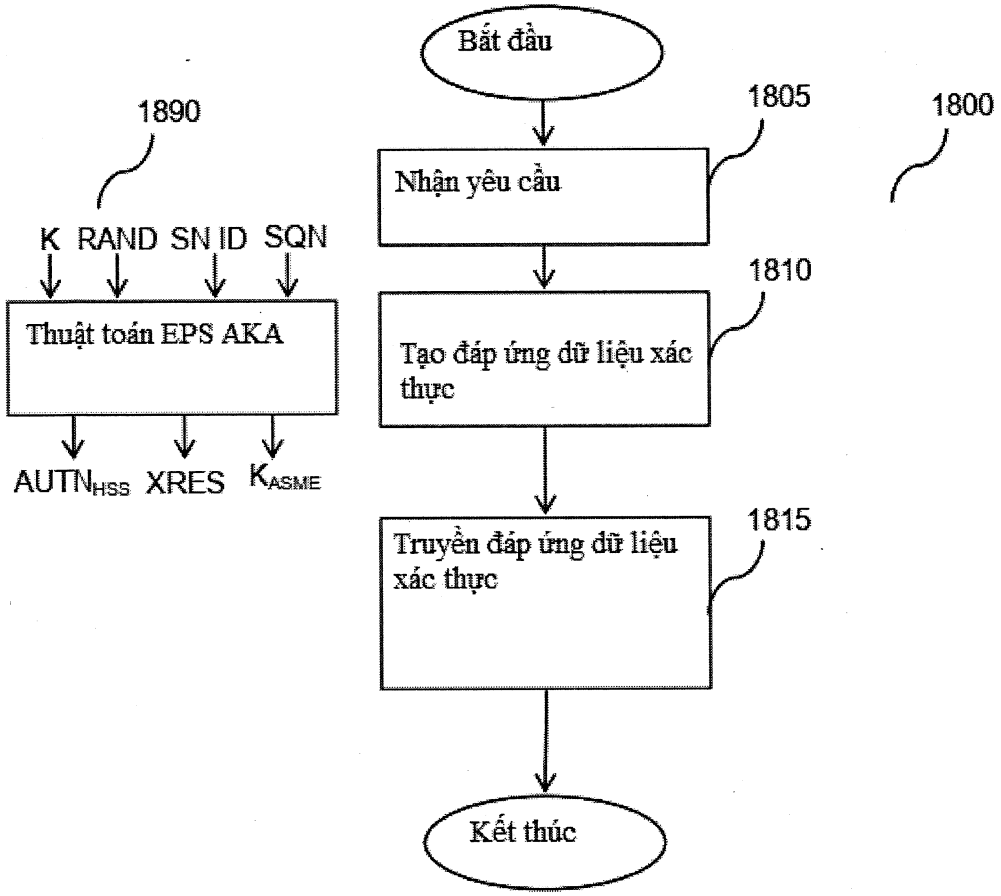

Bắt đầu
1805
1800
1890
Nhận yêu cầu
K RAND SN ID SQN
1810
Thuật toán EPS AKA
Tạo đáp ứng dữ liệu xác thực
AUTN$_{HSS}$ XRES K$_{ASME}$
1815
Truyền đáp ứng dữ liệu xác thực
Kết thúc

Fig.18

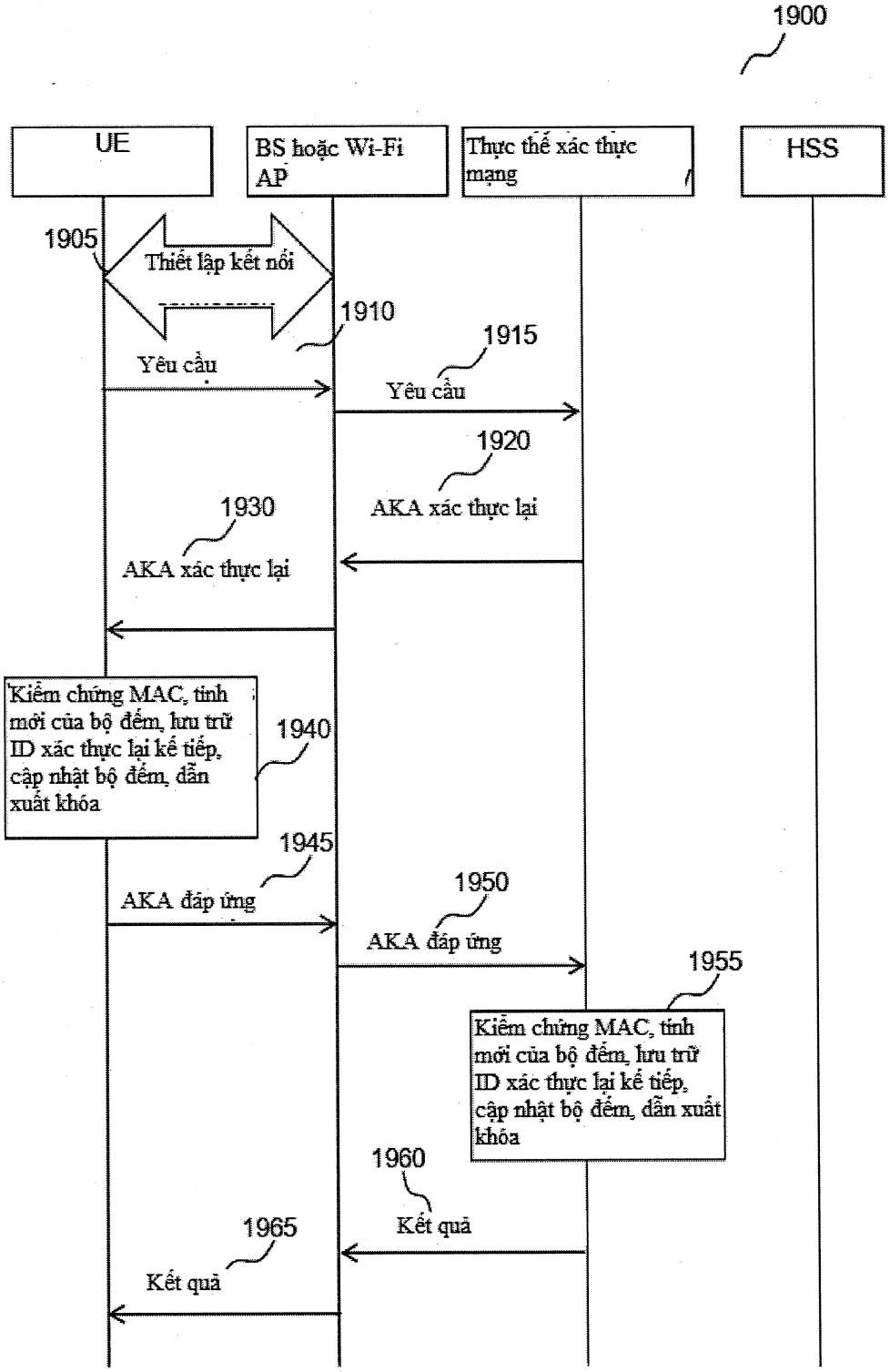

1900
UE
BS hoặc Wi-Fi AP
Thực thể xác thực mạng
HSS
1905
Thiết lập kết nối
1910
Yêu cầu
1915
Yêu cầu
1920
AKA xác thực lại
1930
AKA xác thực lại
Kiểm chứng MAC, tính mới của bộ đếm, lưu trữ ID xác thực lại kế tiếp, cập nhật bộ đếm, dẫn xuất khóa
1940
1945
AKA đáp ứng
1950
AKA đáp ứng
1955
Kiểm chứng MAC, tính mới của bộ đếm, lưu trữ ID xác thực lại kế tiếp, cập nhật bộ đếm, dẫn xuất khóa
1960
Kết quả
1965
Kết quả

Fig.19

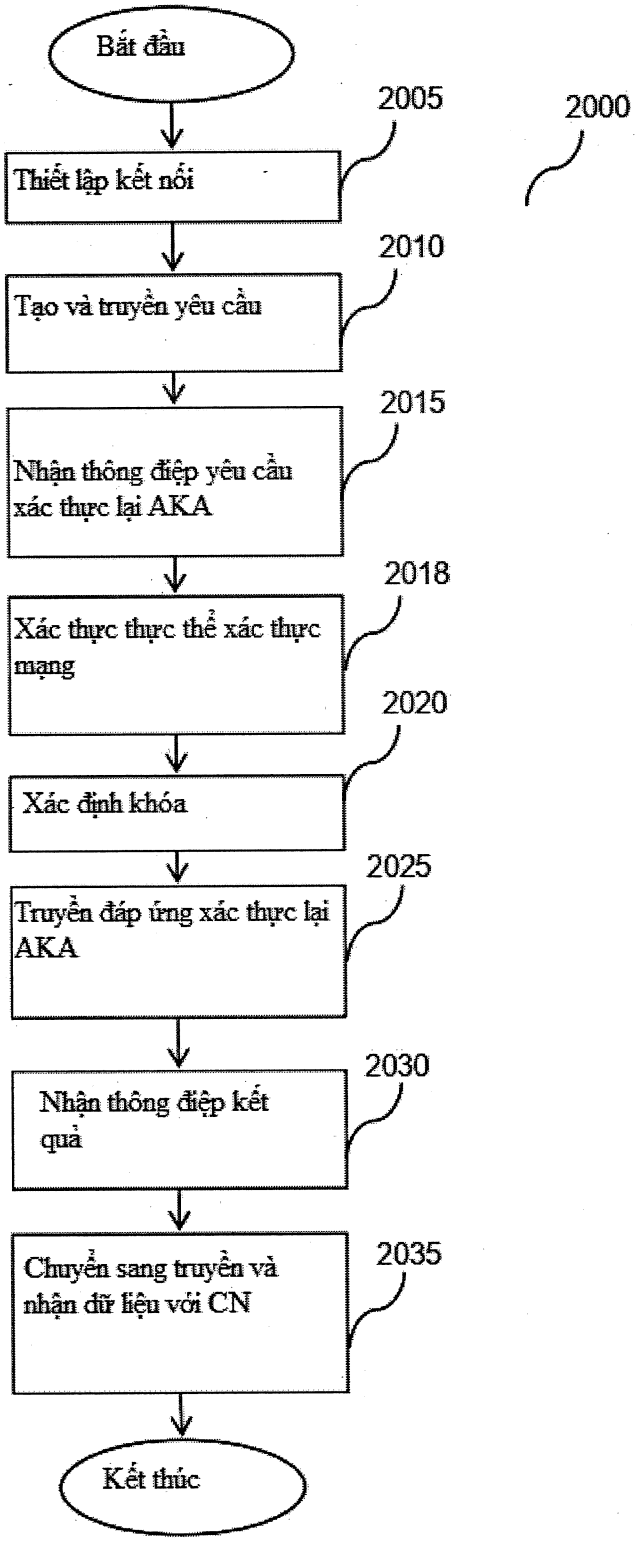

Bắt đầu
2005
2000
Thiết lập kết nối
2010
Tạo và truyền yêu cầu
2015
Nhận thông điệp yêu cầu xác thực lại AKA
2018
Xác thực thực thể xác thực mạng
2020
Xác định khóa
2025
Truyền đáp ứng xác thực lại AKA
2030
Nhận thông điệp kết quả
2035
Chuyển sang truyền và nhận dữ liệu với CN
Kết thúc

Fig.20

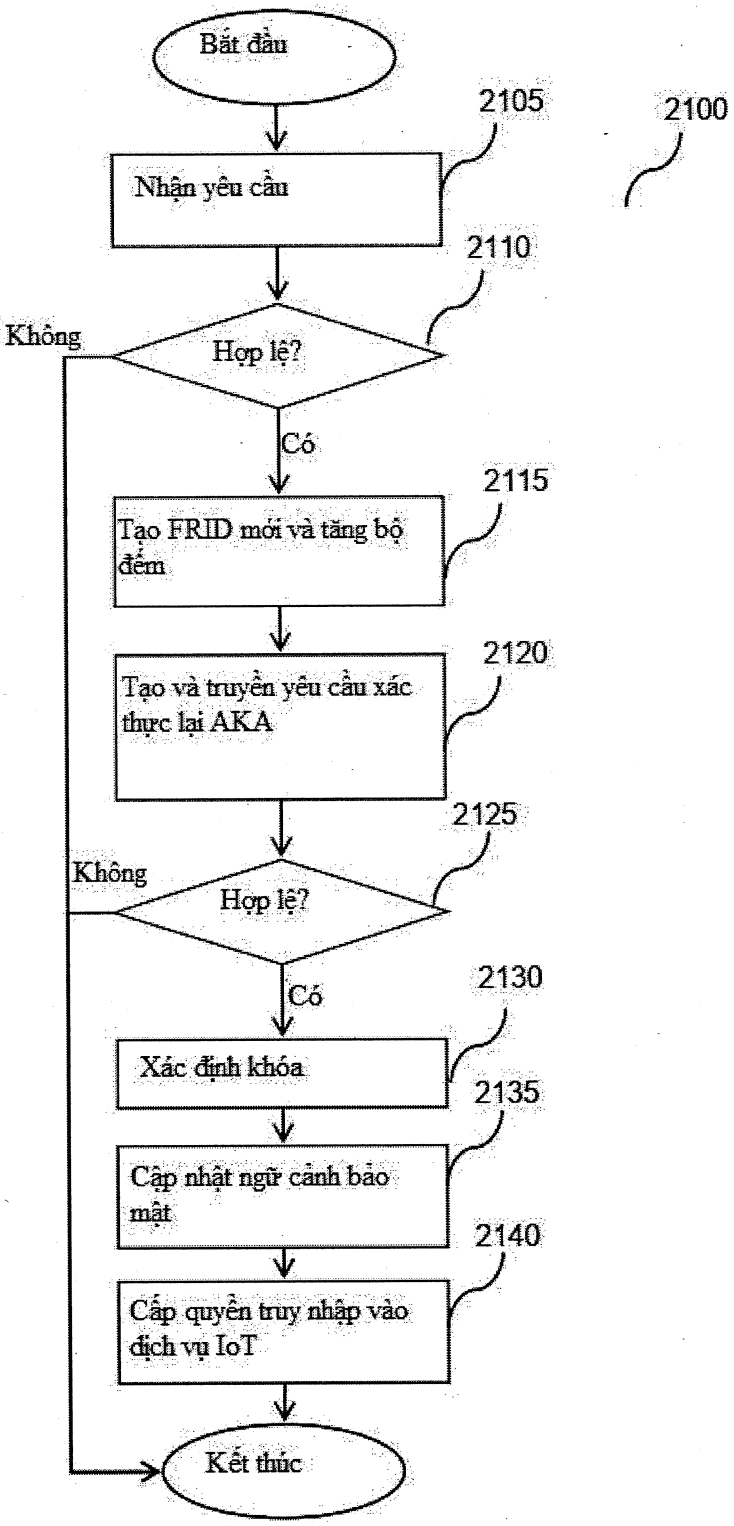

Bắt đầu
2105
2100
Nhận yêu cầu
2110
Không
Hợp lệ?
Có
2115
Tạo FRID mới và tăng bộ đếm
2120
Tạo và truyền yêu cầu xác thực lại AKA
2125
Không
Hợp lệ?
Có
2130
Xác định khóa
2135
Cập nhật ngữ cảnh bảo mật
2140
Cấp quyền truy nhập vào dịch vụ IoT
Kết thúc

Fig.21

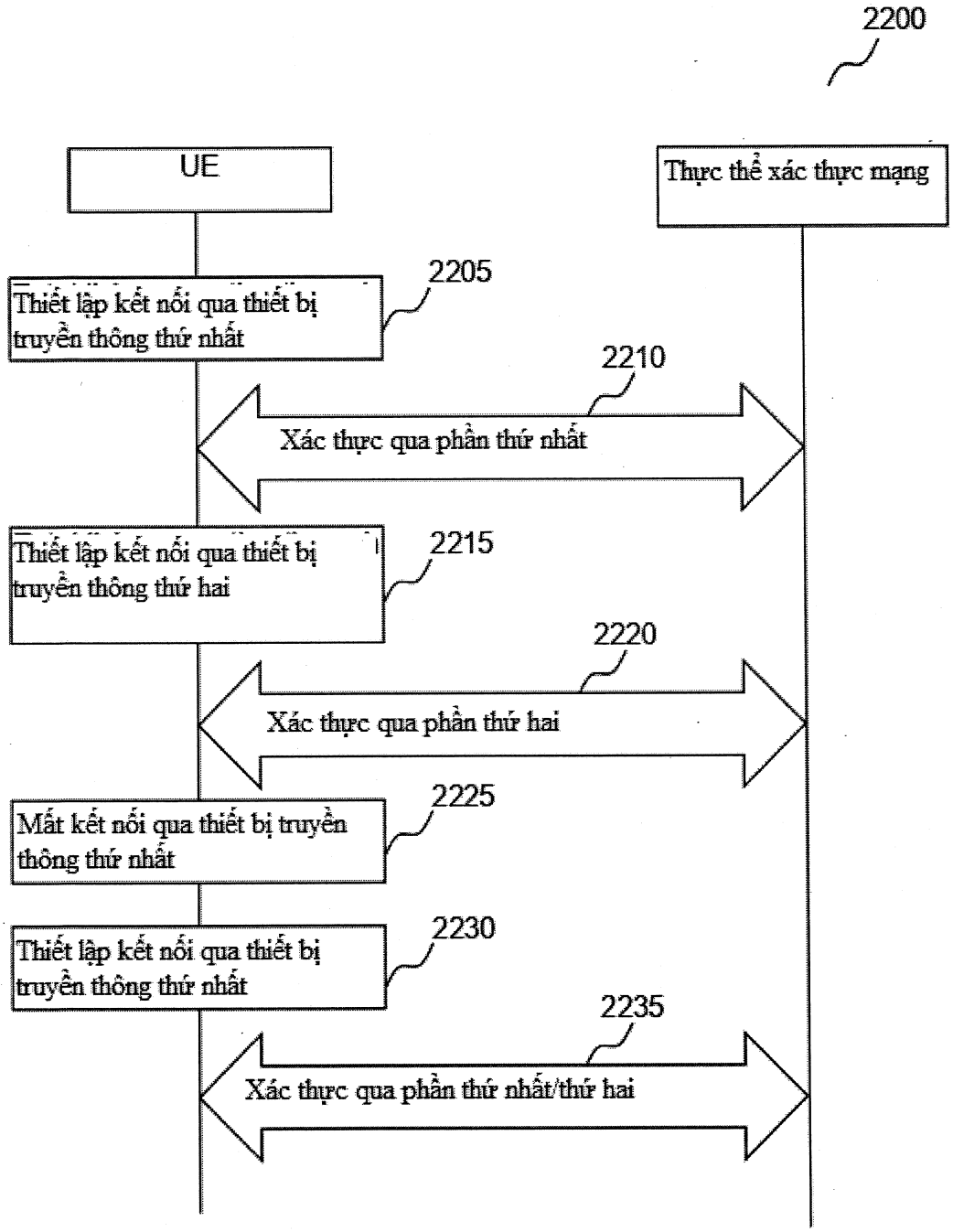

2200
UE
Thực thể xác thực mạng
2205
Thiết lập kết nối qua thiết bị truyền thông thứ nhất
2210
Xác thực qua phần thứ nhất
2215
Thiết lập kết nối qua thiết bị truyền thông thứ hai
2220
Xác thực qua phần thứ hai
2225
Mất kết nối qua thiết bị truyền thông thứ nhất
2230
Thiết lập kết nối qua thiết bị truyền thông thứ nhất
2235
Xác thực qua phần thứ nhất/thứ hai

Fig.22

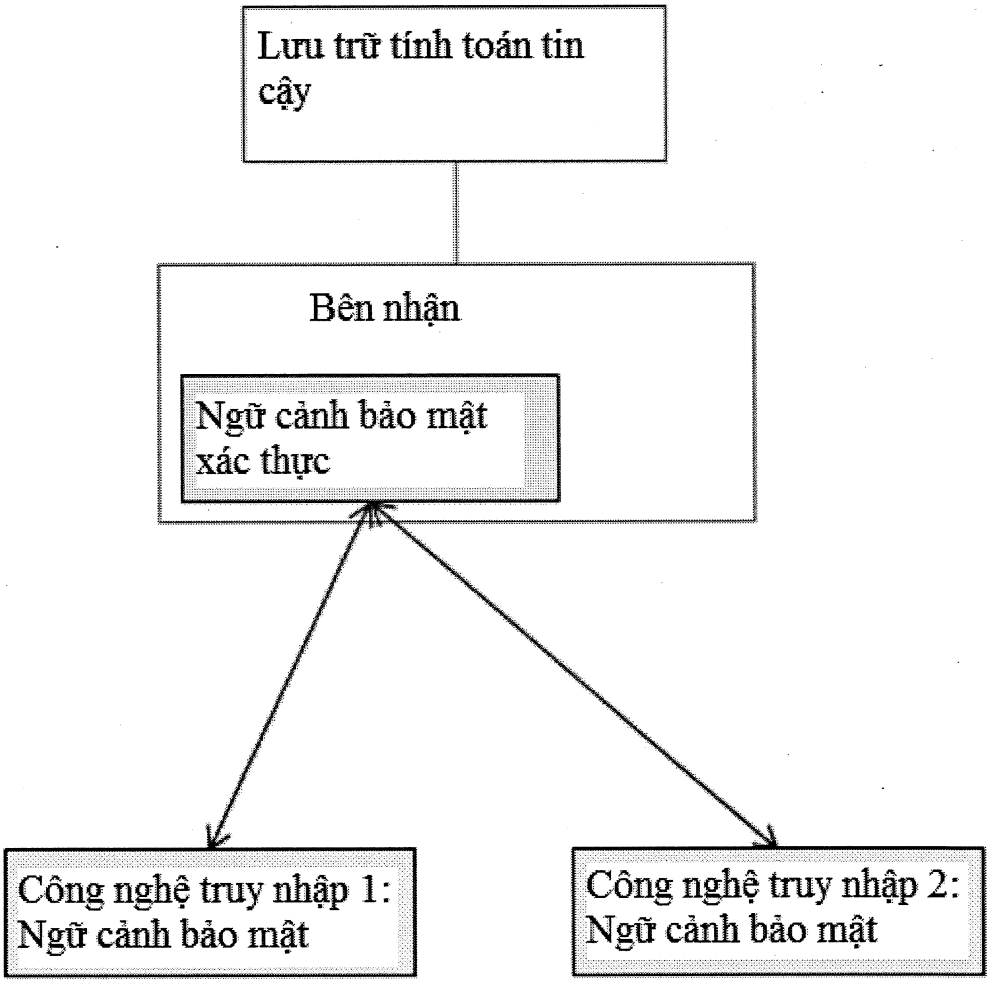

Lưu trữ tính toán tin cậy
Bên nhận
Ngữ cảnh bảo mật xác thực
Công nghệ truy nhập 1: Ngữ cảnh bảo mật
Công nghệ truy nhập 2: Ngữ cảnh bảo mật

Fig.23

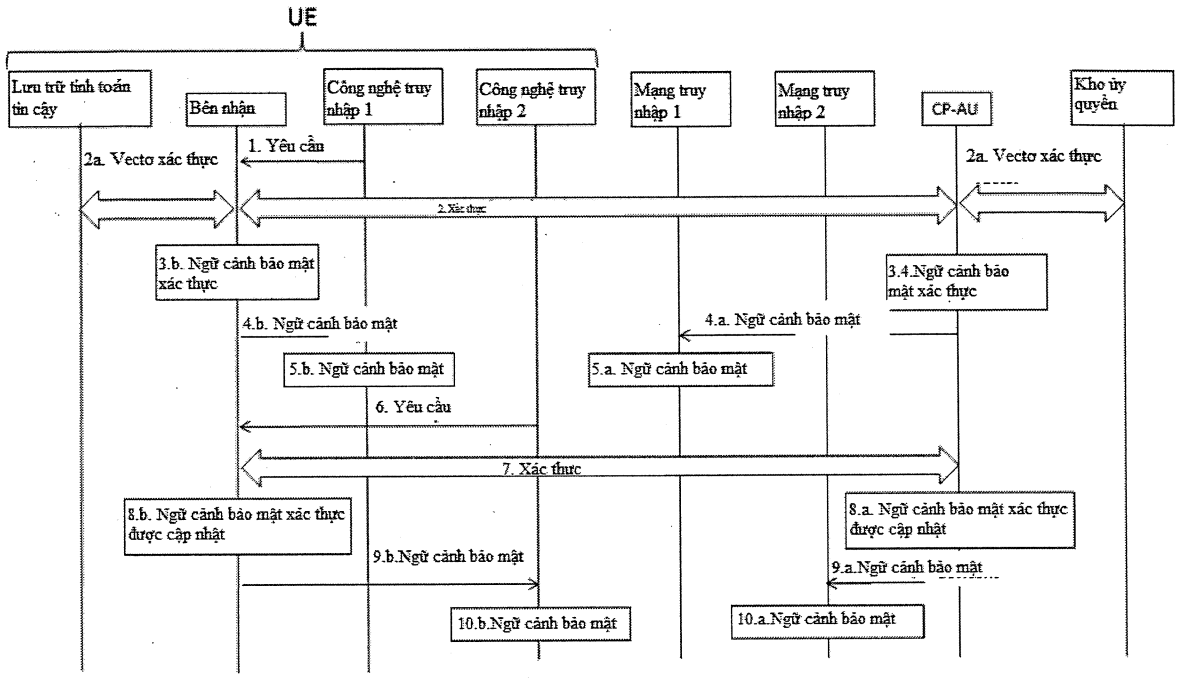

UE
Lưu trữ tính toán tin cậy
Bên nhận
Công nghệ truy nhập 1
Công nghệ truy nhập 2
Mạng truy nhập 1
Mạng truy nhập 2
CP-AU
Kho ủy quyền
1. Yêu cầu
2a. Vectơ xác thực
2a. Vectơ xác thực
2. Xác thực
3.b. Ngữ cảnh bảo mật xác thực
3.4.Ngữ cảnh bảo mật xác thực
4.b. Ngữ cảnh bảo mật
4.a. Ngữ cảnh bảo mật
5.b. Ngữ cảnh bảo mật
5.a. Ngữ cảnh bảo mật
6. Yêu cầu
7. Xác thực
8.b. Ngữ cảnh bảo mật xác thực được cập nhật
8.a. Ngữ cảnh bảo mật xác thực được cập nhật
9.b.Ngữ cảnh bảo mật
9.a.Ngữ cảnh bảo mật
10.b.Ngữ cảnh bảo mật
10.a.Ngữ cảnh bảo mật

Fig.24