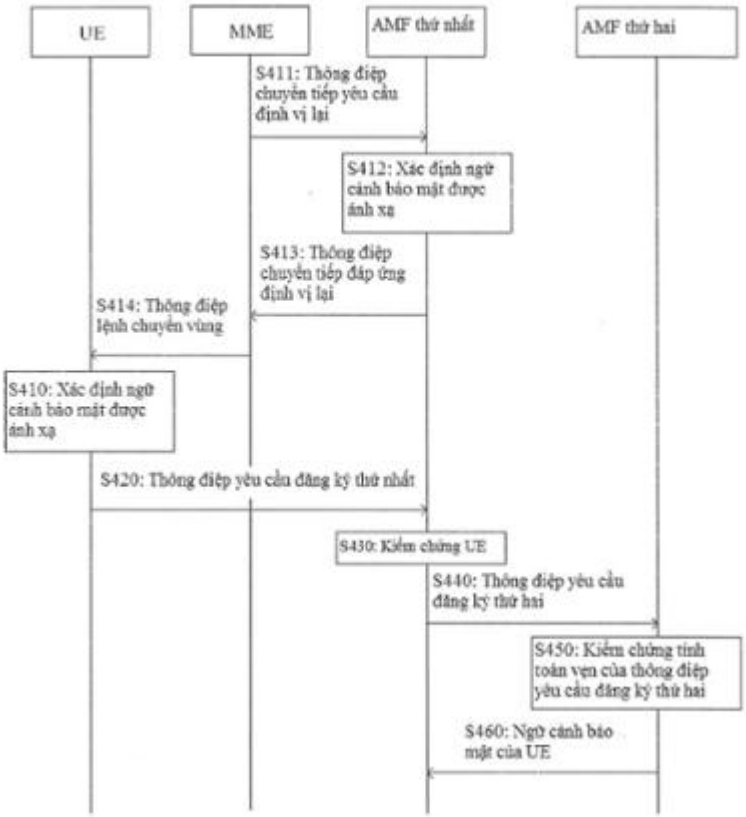
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0041404**
(51)[2020.01] **H04W 12/10**
(13) **B**

(21) 1-2021-08330
(22) 11/05/2020
(86) PCT/CN2020/089621 11/05/2020
(87) WO2020/238595 03/12/2020
(30) 201910470895.8 31/05/2019 CN
(45) 25/10/2024 439
(43) 25/02/2022 407
(73) HONOR DEVICE CO., LTD. (CN)
Suite 3401, Unit A, Building 6, Shum Yip Sky Park, No. 8089, Hongli West Road, Xiangmihu Street, Futian District, Shenzhen, Guangdong 518040, China
(72) LI, Fei (CN); ZHANG, Bo (CN).
(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ THU THẬP NGỮ CẢNH BẢO MẬT, VÀ HỆ THỐNG TRUYỀN THÔNG

(57) Sáng chế đề cập đến phương pháp thu thập ngữ cảnh bảo mật. Sau khi thiết bị người dùng (user equipment, UE) được chuyển vùng từ hệ thống truyền thông 4G đến hệ thống truyền thông 5G, chức năng quản lý di động và truy nhập thứ nhất (access and mobility management function, AMF) thứ nhất cấp dịch vụ quản lý di động và truy nhập cho UE trong hệ thống 5G có thể thu được ngữ cảnh bảo mật của UE từ AMF thứ hai trong hệ thống truyền thông 5G theo phương pháp. Phương pháp bao gồm: UE truyền thông điệp yêu cầu đăng ký thứ nhất đến AMF thứ nhất, trong đó thông điệp yêu cầu đăng ký thứ nhất mang thông điệp yêu cầu đăng ký thứ hai. AMF thứ nhất truyền thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai, trong đó thông điệp yêu cầu đăng ký thứ hai được bảo vệ tính toàn vẹn nhờ sử dụng ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai. Sau khi kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ hai trả về ngữ cảnh bảo mật của UE cho AMF thứ nhất. Phương pháp này có thể cải thiện khả năng mà AMF thứ nhất thu được thành công ngữ cảnh bảo mật của UE từ AMF thứ hai.


UE
MME
AMF thứ nhất
AMF thứ hai
S411: Thông điệp chuyển tiếp yêu cầu định vị lại
S412: Xác định ngữ cảnh bảo mật được ánh xạ
S413: Thông điệp chuyển tiếp đáp ứng định vị lại
S414: Thông điệp lệnh chuyển vùng
S410: Xác định ngữ cảnh bảo mật được ánh xạ
S420: Thông điệp yêu cầu đăng ký thứ nhất
S430: Kiểm chứng UE
S440: Thông điệp yêu cầu đăng ký thứ hai
S450: Kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai
S460: Ngữ cảnh bảo mật của UE

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực truyền thông, và cụ thể hơn, đến phương pháp và thiết bị thu thập ngữ cảnh bảo mật, và hệ thống truyền thông.

Tình trạng kỹ thuật của sáng chế

Trong kịch bản truyền thông thế hệ thứ 5 (5th generation, 5G), do chuyển động của thiết bị người dùng (user equipment, UE), thiết bị mạng phục vụ UE thay đổi. Trong kịch bản chuyển vùng khả thi, UE được chuyển vùng từ hệ thống truyền thông thế hệ thứ 4 (4th generation, 4G) sang hệ thống truyền thông 5G. Trong kịch bản chuyển vùng này, UE được chuyển vùng từ thiết bị mạng truy nhập 4G sang thiết bị mạng truy nhập 5G, và từ thiết bị mạng lõi 4G sang thiết bị mạng lõi 5G. Chuyển vùng giữa các thiết bị mạng lõi bao gồm chuyển vùng giữa các phần tử mạng lõi cung cấp dịch vụ quản lý di động cho UE, nói cách khác, chuyển vùng từ thực thể quản lý di động (mobility management entity, MME) trong hệ thống truyền thông 4G đến chức năng quản lý di động và truy nhập (access and mobility management function, AMF) trong hệ thống truyền thông 5G.

Trong kịch bản hiện tại trong đó UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, bên cạnh AMF (AMF thứ nhất) được chọn bởi MME, hệ thống truyền thông 5G còn bao gồm AMF (AMF thứ hai) mà lưu trữ ngữ cảnh bảo mật của UE. Trong trường hợp này, cách thức AMF thứ nhất thu được ngữ cảnh bảo mật của UE từ AMF thứ hai trở thành vấn đề cấp thiết cần được giải quyết.

Bản chất kỹ thuật của sáng chế

Sáng chế đề cập đến phương pháp và thiết bị thu thập ngữ cảnh bảo mật, và hệ thống truyền thông. Thông điệp yêu cầu đăng ký thứ hai được gửi bởi AMF thứ nhất đến AMF thứ hai được bảo vệ tính toàn vẹn dựa trên ngữ cảnh bảo mật

nguyên gốc giữa UE và AMF thứ hai, sao cho AMF thứ hai có thể kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai dựa trên ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai, để cải thiện khả năng AMF thứ hai kiểm chứng thành công thông điệp yêu cầu đăng ký thứ hai. Nếu kiểm chứng thành công, AMF thứ nhất có thể thu được thành công ngữ cảnh bảo mật của UE từ AMF thứ hai.

Khía cạnh thứ nhất đề cập đến phương pháp thu thập ngữ cảnh bảo mật. Phương pháp bao gồm: AMF thứ nhất nhận thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE, trong đó thông điệp yêu cầu đăng ký thứ nhất mang thông điệp yêu cầu đăng ký thứ hai, thông điệp yêu cầu đăng ký thứ hai được bảo vệ tính toàn vẹn nhờ sử dụng ngữ cảnh bảo mật thứ nhất, ngữ cảnh bảo mật thứ nhất là ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai, và AMF thứ nhất là AMF cấp dịch vụ quản lý di động và truy nhập cho UE sau khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G. AMF thứ nhất truyền thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai. AMF thứ hai kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai. Nếu AMF thứ hai kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ hai truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, ngữ cảnh bảo mật của UE được lưu trữ bởi UE và AMF thứ hai trước khi chuyển vùng. Sau khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, AMF thứ nhất cấp dịch vụ quản lý di động và truy nhập cho UE. AMF thứ nhất cần thu được ngữ cảnh bảo mật của UE từ AMF thứ hai. Cụ thể là, sau khi nhận lệnh chuyển vùng, UE có thể thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư dựa trên ngữ cảnh bảo mật được lưu trữ nguyên gốc giữa UE và AMF thứ hai, tạo thông điệp yêu cầu đăng ký thứ hai, bổ sung thông điệp yêu cầu đăng ký thứ hai vào thông điệp yêu cầu đăng ký thứ nhất, và truyền thông điệp yêu cầu đăng ký thứ nhất đến AMF thứ nhất. Theo cách này, AMF thứ nhất có thể chuyển tiếp thông điệp

yêu cầu đăng ký thứ hai đến AMF thứ hai, và AMF thứ hai có thể kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai. Sau khi kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ hai có thể trả về ngữ cảnh bảo mật của UE cho AMF thứ nhất. Điều này có thể cải thiện khả năng mà AMF thứ nhất thu được thành công ngữ cảnh bảo mật của UE từ AMF thứ hai.

Dựa vào khía cạnh thứ nhất, theo một số triển khai của khía cạnh thứ nhất, ngữ cảnh bảo mật của UE bao gồm: ngữ cảnh bảo mật thứ nhất, hoặc ngữ cảnh bảo mật thứ hai thu được dựa trên ngữ cảnh bảo mật thứ nhất.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, ngữ cảnh bảo mật của UE có thể là ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai. Theo cách khác, khi AMF thứ hai thực hiện dẫn xuất khóa và tạo khóa mới, ngữ cảnh bảo mật của UE có thể là ngữ cảnh bảo mật thứ hai được tạo qua dẫn xuất khóa dựa trên ngữ cảnh bảo mật thứ nhất.

Dựa vào khía cạnh thứ nhất, theo một số triển khai của khía cạnh thứ nhất, that AMF thứ nhất truyền thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai bao gồm: AMF thứ nhất truyền yêu cầu gọi dịch vụ truyền ngữ cảnh UE đến AMF thứ hai, trong đó yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang thông điệp yêu cầu đăng ký thứ hai.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, thông điệp yêu cầu đăng ký thứ hai được gửi bởi AMF thứ nhất đến AMF thứ hai có thể được mang trong yêu cầu gọi dịch vụ truyền ngữ cảnh UE được gửi bởi AMF thứ nhất to AMF thứ hai.

Dựa vào khía cạnh thứ nhất, theo một số triển khai của khía cạnh thứ nhất, that AMF thứ hai truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất bao gồm: AMF thứ hai truyền thông điệp đáp ứng thứ nhất đến AMF thứ nhất, trong đó thông điệp đáp ứng thứ nhất mang ngữ cảnh bảo mật của UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, khi trả về ngữ cảnh bảo mật của UE cho AMF thứ nhất, AMF thứ hai có thể truyền thông điệp đáp ứng thứ nhất mang ngữ cảnh bảo mật của UE đến AMF thứ nhất.

Dựa vào khía cạnh thứ nhất, theo một số triển khai của khía cạnh thứ nhất, phương pháp còn bao gồm: Khi AMF thứ nhất nhận thông điệp chỉ báo rằng AMF thứ hai không kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ nhất tiếp tục sử dụng ngữ cảnh bảo mật được ánh xạ, or khởi tạo xác thực ban đầu đến UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, khi AMF thứ nhất không thu được ngữ cảnh bảo mật của UE từ AMF thứ hai, AMF thứ nhất có thể tiếp tục sử dụng ngữ cảnh bảo mật được ánh xạ được tạo qua thương lượng với UE; hoặc AMF thứ nhất có thể khởi tạo xác thực ban đầu đến UE để tạo ngữ cảnh bảo mật giữa AMF thứ nhất và UE.

Dựa vào khía cạnh thứ nhất, theo một số triển khai của khía cạnh thứ nhất, ngữ cảnh bảo mật được ánh xạ thu được dựa trên ngữ cảnh bảo mật giữa MME và UE, và MME là phần tử mạng trong hệ thống truyền thông 4G.

Trong phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, ngữ cảnh bảo mật được ánh xạ là ngữ cảnh bảo mật được tạo bởi UE và AMF thứ nhất riêng rẽ qua dẫn xuất dựa trên ngữ cảnh bảo mật giữa UE và MME.

Dựa vào khía cạnh thứ nhất, theo một số triển khai của khía cạnh thứ nhất, that AMF thứ hai kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai bao gồm: AMF thứ hai kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai dựa trên ngữ cảnh bảo mật nguyên gốc giữa AMF thứ hai và UE.

Khía cạnh thứ hai đề cập đến phương pháp thu thập ngữ cảnh bảo mật. Phương pháp bao gồm: AMF thứ hai nhận thông điệp yêu cầu đăng ký thứ hai được gửi bởi AMF thứ nhất, trong đó thông điệp yêu cầu đăng ký thứ hai được bảo vệ tính toàn vẹn using ngữ cảnh bảo mật thứ nhất, ngữ cảnh bảo mật thứ nhất là ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai, và AMF thứ nhất là AMF cấp dịch vụ quản lý di động và truy nhập cho UE sau khi UE được chuyển vùng từ hệ thống truyền thông 4G đến hệ thống truyền thông 5G. AMF thứ hai kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai. Nếu AMF thứ hai kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu

đăng ký thứ hai, AMF thứ hai truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, ngữ cảnh bảo mật của UE được lưu trữ bởi UE và AMF thứ hai trước khi chuyển vùng. Sau khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, AMF thứ nhất cấp dịch vụ quản lý di động và truy nhập cho UE. AMF thứ nhất cần thu được ngữ cảnh bảo mật của UE từ AMF thứ hai. Cụ thể là, sau khi nhận lệnh chuyển vùng, UE có thể thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư dựa trên ngữ cảnh bảo mật được lưu trữ nguyên gốc giữa UE và AMF thứ hai, và sau đó tạo thông điệp yêu cầu đăng ký thứ hai. UE bổ sung thông điệp yêu cầu đăng ký thứ hai vào thông điệp yêu cầu đăng ký thứ nhất được truyền đến AMF thứ nhất. Theo cách này, AMF thứ nhất có thể chuyển tiếp thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai, và AMF thứ hai có thể kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai. Sau khi kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ hai truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất. Điều này có thể cải thiện khả năng mà AMF thứ nhất thu được thành công ngữ cảnh bảo mật của UE từ AMF thứ hai.

Dựa vào khía cạnh thứ hai, theo một số triển khai của khía cạnh thứ hai, ngữ cảnh bảo mật của UE bao gồm: ngữ cảnh bảo mật thứ nhất, hoặc ngữ cảnh bảo mật thứ hai được tạo qua dẫn xuất khóa dựa trên ngữ cảnh bảo mật thứ nhất.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, ngữ cảnh bảo mật của UE có thể là ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai. Theo cách khác, khi AMF thứ hai thực hiện dẫn xuất khóa và tạo khóa mới, ngữ cảnh bảo mật của UE có thể là ngữ cảnh bảo mật thứ hai được tạo qua dẫn xuất khóa dựa trên ngữ cảnh bảo mật thứ nhất.

Dựa vào khía cạnh thứ hai, theo một số triển khai của khía cạnh thứ hai, việc AMF thứ hai nhận thông điệp yêu cầu đăng ký thứ hai được gửi bởi AMF thứ nhất bao gồm: AMF thứ hai nhận yêu cầu gọi dịch vụ truyền ngữ cảnh UE

được gửi bởi AMF thứ nhất, trong đó yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang thông điệp yêu cầu đăng ký thứ hai.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, thông điệp yêu cầu đăng ký thứ hai được gửi bởi AMF thứ nhất đến AMF thứ hai có thể được mang trong yêu cầu gọi dịch vụ truyền ngữ cảnh UE được gửi bởi AMF thứ nhất đến AMF thứ hai.

Dựa vào khía cạnh thứ hai, theo một số triển khai của khía cạnh thứ hai, việc AMF thứ hai truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất bao gồm: AMF thứ hai truyền thông điệp đáp ứng thứ nhất đến AMF thứ nhất, trong đó thông điệp đáp ứng thứ nhất mang ngữ cảnh bảo mật của UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, khi trả về ngữ cảnh bảo mật của UE cho AMF thứ nhất, AMF thứ hai có thể truyền thông điệp đáp ứng thứ nhất mang ngữ cảnh bảo mật của UE đến AMF thứ nhất.

Dựa vào khía cạnh thứ hai, theo một số triển khai của khía cạnh thứ hai, việc AMF thứ hai kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai bao gồm: AMF thứ hai kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai dựa trên ngữ cảnh bảo mật thứ nhất.

Khía cạnh thứ ba đề cập đến phương pháp thu thập ngữ cảnh bảo mật. Phương pháp bao gồm: UE xác định thông điệp yêu cầu đăng ký thứ hai, và thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ hai, trong đó thông điệp yêu cầu đăng ký thứ hai được bảo vệ tính toàn vẹn nhờ sử dụng ngữ cảnh bảo mật thứ nhất, và ngữ cảnh bảo mật thứ nhất là ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai. UE truyền thông điệp yêu cầu đăng ký thứ nhất đến AMF thứ nhất, trong đó thông điệp yêu cầu đăng ký thứ nhất mang thông điệp yêu cầu đăng ký thứ hai, và AMF thứ nhất là AMF cấp dịch vụ quản lý di động và truy nhập cho UE sau khi UE được chuyển vùng từ hệ thống truyền thông 4G đến hệ thống truyền thông 5G.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, ngữ cảnh bảo mật của UE được lưu trữ bởi UE và AMF thứ

hai trước khi chuyển vùng. Sau khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, AMF thứ nhất cấp dịch vụ quản lý di động và truy nhập cho UE. AMF thứ nhất cần thu được ngữ cảnh bảo mật của UE từ AMF thứ hai. Cụ thể là, sau khi nhận lệnh chuyển vùng, UE có thể thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư dựa trên ngữ cảnh bảo mật được lưu trữ nguyên gốc giữa UE và AMF thứ hai, và sau đó tạo thông điệp yêu cầu đăng ký thứ hai. UE bổ sung thông điệp yêu cầu đăng ký thứ hai vào thông điệp yêu cầu đăng ký thứ nhất được truyền đến AMF thứ nhất. Theo cách này, AMF thứ nhất có thể chuyển tiếp thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai, và AMF thứ hai có thể kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai. Sau khi kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ hai có thể trả về ngữ cảnh bảo mật của UE cho AMF thứ nhất. Điều này có thể cải thiện khả năng mà AMF thứ nhất thu được thành công ngữ cảnh bảo mật của UE từ AMF thứ hai.

Dựa vào khía cạnh thứ ba, theo một số triển khai của khía cạnh thứ ba, phương pháp còn bao gồm: nếu thông điệp lệnh chế độ bảo mật tầng không truy nhập (non-access stratum security mode command, NAS SMC) được gửi bởi AMF thứ nhất được nhận, kiểm chứng tính toàn vẹn của NAS SMC; và nếu kiểm chứng thành công, gửi thông điệp hoàn thành chế độ bảo mật tầng không truy nhập đến AMF thứ nhất.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, nếu UE nhận thông điệp NAS SMC được gửi bởi AMF thứ nhất, và UE kiểm chứng thành công thông điệp NAS SMC, UE truyền thông điệp hoàn thành chế độ bảo mật tầng không truy nhập đến AMF thứ nhất.

Khía cạnh thứ tư đề cập đến phương pháp thu thập ngữ cảnh bảo mật. Phương pháp bao gồm: AMF thứ nhất nhận thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE, trong đó thông điệp yêu cầu đăng ký thứ nhất mang thông điệp yêu cầu đăng ký thứ hai, thông điệp yêu cầu đăng ký thứ hai được bảo vệ tính toàn vẹn nhờ sử dụng ngữ cảnh bảo mật thứ nhất, ngữ cảnh bảo mật thứ nhất là ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai, và AMF

thứ nhất là AMF cấp dịch vụ quản lý di động và truy nhập cho UE sau khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G. AMF thứ nhất truyền thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai. Nếu AMF thứ hai kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ nhất nhận ngữ cảnh bảo mật của UE được gửi bởi AMF thứ hai.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, ngữ cảnh bảo mật của UE được lưu trữ bởi UE và AMF thứ hai trước khi chuyển vùng. Sau khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, AMF thứ nhất cấp dịch vụ quản lý di động và truy nhập cho UE. AMF thứ nhất cần thu được ngữ cảnh bảo mật của UE từ AMF thứ hai. Cụ thể là, sau khi nhận lệnh chuyển vùng, UE có thể thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư dựa trên ngữ cảnh bảo mật được lưu trữ nguyên gốc giữa UE và AMF thứ hai, và sau đó tạo thông điệp yêu cầu đăng ký thứ hai. UE bổ sung thông điệp yêu cầu đăng ký thứ hai vào thông điệp yêu cầu đăng ký thứ nhất được truyền đến AMF thứ nhất. Theo cách này, AMF thứ nhất có thể chuyển tiếp thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai, và AMF thứ hai có thể kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai. Sau khi kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ hai có thể trả về ngữ cảnh bảo mật của UE cho AMF thứ nhất. Điều này có thể cải thiện khả năng mà AMF thứ nhất thu được thành công ngữ cảnh bảo mật của UE từ AMF thứ hai.

Dựa vào khía cạnh thứ tư, theo một số triển khai của khía cạnh thứ tư, ngữ cảnh bảo mật của UE bao gồm: ngữ cảnh bảo mật thứ nhất, hoặc ngữ cảnh bảo mật thứ hai được tạo qua dẫn xuất khóa dựa trên ngữ cảnh bảo mật thứ nhất.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, ngữ cảnh bảo mật của UE có thể là ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai. Theo cách khác, khi AMF thứ hai thực hiện dẫn xuất khóa and tạo khóa mới, ngữ cảnh bảo mật của UE có thể là ngữ cảnh bảo mật

thứ hai được tạo qua dẫn xuất khóa dựa trên ngữ cảnh bảo mật thứ nhất.

Dựa vào khía cạnh thứ tư, theo một số triển khai của khía cạnh thứ tư, việc AMF thứ nhất truyền thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai bao gồm: AMF thứ nhất truyền yêu cầu gọi dịch vụ truyền ngữ cảnh UE đến AMF thứ hai, trong đó yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang thông điệp yêu cầu đăng ký thứ hai.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, thông điệp yêu cầu đăng ký thứ hai được gửi bởi AMF thứ nhất đến AMF thứ hai có thể được mang trong yêu cầu gọi dịch vụ truyền ngữ cảnh UE được gửi bởi AMF thứ nhất đến AMF thứ hai.

Dựa vào khía cạnh thứ tư, theo một số triển khai của khía cạnh thứ tư, việc AMF thứ nhất nhận ngữ cảnh bảo mật của UE được gửi bởi AMF thứ hai bao gồm: AMF thứ nhất nhận thông điệp đáp ứng thứ nhất được gửi bởi AMF thứ hai, trong đó thông điệp đáp ứng thứ nhất mang ngữ cảnh bảo mật của UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, khi trả về ngữ cảnh bảo mật của UE cho AMF thứ nhất, AMF thứ hai có thể truyền thông điệp đáp ứng thứ nhất mang ngữ cảnh bảo mật của UE đến AMF thứ nhất.

Dựa vào khía cạnh thứ tư, theo một số triển khai của khía cạnh thứ tư, phương pháp còn bao gồm: Khi AMF thứ nhất nhận thông điệp chỉ báo rằng AMF thứ hai không kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ nhất tiếp tục sử dụng ngữ cảnh bảo mật được ánh xạ, hoặc khởi tạo xác thực ban đầu đến UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, khi AMF thứ nhất không thu được ngữ cảnh bảo mật của UE từ AMF thứ hai, AMF thứ nhất có thể tiếp tục sử dụng ngữ cảnh bảo mật được ánh xạ được tạo qua thương lượng với UE; hoặc AMF thứ nhất có thể khởi tạo xác thực ban đầu đến UE để tạo ngữ cảnh bảo mật giữa AMF thứ nhất and UE.

Dựa vào khía cạnh thứ tư, theo một số triển khai của khía cạnh thứ tư, ngữ cảnh bảo mật được ánh xạ thu được dựa trên ngữ cảnh bảo mật giữa thực thể quản lý di động (mobility management entity, MME) và UE, và MME là phần

tử mạng trong hệ thống truyền thông 4G.

Trong phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, ngữ cảnh bảo mật được ánh xạ là ngữ cảnh bảo mật được tạo bởi UE và AMF thứ nhất riêng rẽ qua dẫn xuất dựa trên ngữ cảnh bảo mật giữa UE và MME.

Khía cạnh thứ năm đề cập đến phương pháp thu thập ngữ cảnh bảo mật. Phương pháp bao gồm: AMF thứ nhất truyền yêu cầu gọi dịch vụ truyền ngữ cảnh UE đến AMF thứ hai, trong đó yêu cầu gọi dịch vụ truyền ngữ cảnh UE được sử dụng để thu được ngữ cảnh bảo mật của UE, yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang thông tin chỉ báo, thông tin chỉ báo được sử dụng để chỉ báo rằng UE được kiểm chứng, và AMF thứ nhất là AMF cấp dịch vụ quản lý di động và truy nhập cho UE sau khi UE được chuyển vùng từ hệ thống truyền thông 4G đến hệ thống truyền thông 5G. AMF thứ nhất nhận thông điệp đáp ứng thứ hai được gửi bởi AMF thứ hai, trong đó thông điệp đáp ứng thứ hai mang ngữ cảnh bảo mật của UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, yêu cầu gọi dịch vụ truyền ngữ cảnh UE được gửi bởi AMF thứ nhất đến AMF thứ hai mang thông tin chỉ báo chỉ báo rằng UE được kiểm chứng. Điều này có thể tránh việc AMF thứ hai không kiểm chứng UE đó và không truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất, và cải thiện khả năng rằng AMF thứ nhất thu được thành công ngữ cảnh bảo mật của UE từ AMF thứ hai.

Dựa vào khía cạnh thứ năm, theo một số triển khai của khía cạnh thứ năm, that thông tin chỉ báo được sử dụng để chỉ báo rằng UE được kiểm chứng bao gồm: Thông tin chỉ báo được sử dụng để chỉ báo rằng tính toàn vẹn của thông điệp yêu cầu đăng ký được kiểm chứng thành công, trong đó thông điệp yêu cầu đăng ký được nhận bởi AMF thứ nhất từ UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, thông tin chỉ báo, được gửi bởi AMF thứ nhất đến AMF thứ hai, chỉ báo rằng UE được kiểm chứng có thể được sử dụng bởi AMF thứ nhất để thông báo AMF thứ hai rằng tính toàn vẹn của thông điệp yêu cầu đăng ký được gửi bởi UE được kiểm chứng thành công. Điều này đề cập đến giải pháp tùy chọn

linh hoạt để chỉ báo rằng UE được kiểm chứng.

Dựa vào khía cạnh thứ năm, theo một số triển khai của khía cạnh thứ năm, trước khi AMF thứ nhất truyền yêu cầu gọi dịch vụ truyền ngữ cảnh UE đến AMF thứ hai, phương pháp còn bao gồm: AMF thứ nhất kiểm chứng thành công bảo vệ tính toàn vẹn cho thông điệp yêu cầu đăng ký, trong đó thông điệp yêu cầu đăng ký được nhận bởi AMF thứ nhất từ UE; và/hoặc AMF thứ nhất xác định rằng thông điệp yêu cầu đăng ký là thông điệp yêu cầu đăng ký được gửi bởi UE sau khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, AMF thứ nhất xác định, dựa trên kết quả chỉ báo rằng thông điệp yêu cầu đăng ký được kiểm chứng thành công và/hoặc dựa trên việc thông điệp yêu cầu đăng ký được nhận là thông điệp yêu cầu đăng ký được gửi bởi UE sau khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, rằng yêu cầu gọi dịch vụ truyền ngữ cảnh UE có thể được truyền đến AMF thứ hai.

Dựa vào khía cạnh thứ năm, theo một số triển khai của khía cạnh thứ năm, yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang định danh của UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, để AMF thứ hai có thể biết rằng AMF thứ nhất cần thu được ngữ cảnh bảo mật của UE, AMF thứ nhất bổ sung định danh của UE vào yêu cầu gọi dịch vụ truyền ngữ cảnh.

Dựa vào khía cạnh thứ năm, theo một số triển khai của khía cạnh thứ năm, yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang số đếm tầng không truy nhập liên kết lên (uplink non-access stratum count, UL NAS COUNT) của UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, để AMF thứ hai có thể biết về UL NAS COUNT, AMF thứ nhất có thể bổ sung UL NAS COUNT vào yêu cầu gọi dịch vụ truyền ngữ cảnh.

Dựa vào khía cạnh thứ năm, theo một số triển khai của khía cạnh thứ năm, việc yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang UL NAS COUNT bao gồm: yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang thông điệp yêu cầu đăng ký văn

bản thuần túy, trong đó thông điệp yêu cầu đăng ký văn bản thuần túy bao gồm UL NAS COUNT, và thông điệp yêu cầu đăng ký được nhận bởi AMF thứ nhất từ UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, việc yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang UL NAS COUNT có thể được triển khai bằng cách mang thông điệp yêu cầu đăng ký văn bản thuần túy trong yêu cầu gọi dịch vụ truyền ngữ cảnh UE, trong đó thông điệp yêu cầu đăng ký văn bản thuần túy bao gồm UL NAS COUNT. Điều này đề cập đến giải pháp tùy chọn linh hoạt để AMF thứ nhất để truyền UL NAS COUNT đến AMF thứ hai.

Khía cạnh thứ sáu đề cập đến phương pháp thu thập ngữ cảnh bảo mật. Phương pháp bao gồm: AMF thứ hai nhận yêu cầu gọi dịch vụ truyền ngữ cảnh UE được gửi bởi AMF thứ nhất, trong đó yêu cầu gọi dịch vụ truyền ngữ cảnh UE được sử dụng để thu được ngữ cảnh bảo mật của UE, yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang thông tin chỉ báo, thông tin chỉ báo được sử dụng để chỉ báo rằng UE được kiểm chứng, và AMF thứ nhất là AMF cấp dịch vụ quản lý di động và truy nhập cho UE sau khi UE được chuyển vùng từ hệ thống truyền thông 4G đến hệ thống truyền thông 5G. AMF thứ hai truyền thông điệp đáp ứng thứ hai đến AMF thứ nhất, trong đó thông điệp đáp ứng thứ hai mang ngữ cảnh bảo mật của UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, yêu cầu gọi dịch vụ truyền ngữ cảnh UE được gửi bởi AMF thứ nhất và được nhận bởi AMF thứ hai mang thông tin chỉ báo chỉ báo rằng UE được kiểm chứng. Dựa trên thông tin chỉ báo, AMF thứ hai không cần kiểm chứng UE. Điều này có thể tránh việc AMF thứ hai không kiểm chứng UE và không truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất, và cải thiện khả năng rằng AMF thứ nhất thu được thành công ngữ cảnh bảo mật của UE từ AMF thứ hai.

Dựa vào khía cạnh thứ sáu, theo một số triển khai của khía cạnh thứ sáu, việc thông tin chỉ báo được sử dụng để chỉ báo rằng UE được kiểm chứng bao gồm: Thông tin chỉ báo được sử dụng để chỉ báo rằng tính toàn vẹn của thông điệp yêu cầu đăng ký được kiểm chứng thành công, trong đó thông điệp yêu

cầu đăng ký được nhận bởi AMF thứ nhất từ UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, thông tin chỉ báo, được gửi bởi AMF thứ nhất và được nhận bởi AMF thứ hai, chỉ báo rằng UE được kiểm chứng có thể được sử dụng bởi AMF thứ nhất để thông báo AMF thứ hai mà tính toàn vẹn của thông điệp yêu cầu đăng ký được gửi bởi UE được kiểm chứng thành công. Điều này đề cập đến giải pháp tùy chọn linh hoạt để chỉ báo rằng UE được kiểm chứng.

Dựa vào khía cạnh thứ sáu, theo một số triển khai của khía cạnh thứ sáu, yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang định danh của UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, dựa trên định danh của UE được mang trong yêu cầu gọi dịch vụ truyền ngữ cảnh, AMF thứ hai có thể xác định rằng AMF thứ nhất cần thu được ngữ cảnh bảo mật của UE.

Dựa vào khía cạnh thứ sáu, theo một số triển khai của khía cạnh thứ sáu, yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang UL NAS COUNT của UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, AMF thứ hai có thể biết UL NAS COUNT dựa trên UL NAS COUNT được mang trong yêu cầu gọi dịch vụ truyền ngữ cảnh.

Dựa vào khía cạnh thứ sáu, theo một số triển khai của khía cạnh thứ sáu, việc yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang UL NAS COUNT bao gồm: yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang thông điệp yêu cầu đăng ký văn bản thuần túy, trong đó thông điệp yêu cầu đăng ký văn bản thuần túy bao gồm UL NAS COUNT, và thông điệp yêu cầu đăng ký được nhận bởi AMF thứ nhất từ UE.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, việc yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang UL NAS COUNT có thể được triển khai bằng cách mang thông điệp yêu cầu đăng ký văn bản thuần túy trong yêu cầu gọi dịch vụ truyền ngữ cảnh UE, trong đó thông điệp yêu cầu đăng ký văn bản thuần túy bao gồm UL NAS COUNT. Điều này đề cập đến giải pháp tùy chọn linh hoạt để AMF thứ nhất có thể truyền UL NAS COUNT đến AMF thứ hai.

Dựa vào khía cạnh thứ sáu, theo một số triển khai của khía cạnh thứ sáu, phương pháp còn bao gồm: AMF thứ hai thực hiện dẫn xuất khóa dựa trên UL NAS COUNT.

Theo phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế, AMF thứ hai có thể thực hiện dẫn xuất khóa dựa trên UL NAS COUNT được nhận.

Khía cạnh thứ bảy đề cập đến hệ thống truyền thông. Hệ thống truyền thông bao gồm AMF thứ nhất và AMF thứ hai mà có thể được tạo cấu hình để thực hiện các hoạt động được thực hiện bởi AMF thứ nhất và AMF thứ hai theo trường hợp bất kỳ trong khía cạnh thứ nhất hoặc các triển khai khả thi của khía cạnh thứ nhất. Cụ thể là, thiết bị truyền thông có thể bao gồm thành phần (phương tiện) tương ứng được tạo cấu hình để thực hiện các bước hoặc các chức năng được mô tả theo trường hợp bất kỳ trong khía cạnh thứ nhất hoặc các triển khai khả thi của khía cạnh thứ nhất, và thành phần có thể là AMF thứ nhất và AMF thứ hai theo khía cạnh thứ nhất, hoặc các chip hoặc các môđun chức năng bên trong AMF thứ nhất và AMF thứ hai theo khía cạnh thứ nhất. Các bước hoặc các chức năng có thể được triển khai bằng cách phần mềm, phần cứng, hoặc kết hợp của phần cứng và phần mềm.

Khía cạnh thứ tám đề cập đến thiết bị thu thập ngữ cảnh bảo mật. Thiết bị có thể được tạo cấu hình để thực hiện hoạt động được thực hiện bởi AMF thứ nhất theo trường hợp bất kỳ trong khía cạnh thứ năm, khía cạnh thứ tư, các cách triển khai khả thi của khía cạnh thứ năm, hoặc các triển khai khả thi của khía cạnh thứ tư. Cụ thể là, thiết bị thu thập ngữ cảnh bảo mật có thể bao gồm thành phần (phương tiện) tương ứng được tạo cấu hình để thực hiện các bước hoặc các chức năng được mô tả theo trường hợp bất kỳ trong khía cạnh thứ năm, khía cạnh thứ tư, các cách triển khai khả thi của khía cạnh thứ nhất, hoặc các triển khai khả thi của khía cạnh thứ tư, và thành phần có thể là AMF thứ nhất theo các khía cạnh thứ tư và thứ năm, hoặc chip hoặc môđun chức năng bên trong AMF thứ nhất theo các khía cạnh thứ tư và thứ năm. Các bước hoặc các chức năng có thể được triển khai bằng cách phần mềm, phần cứng, hoặc kết hợp của phần cứng và phần mềm.

Khía cạnh thứ chín đề cập thiết bị thu thập ngữ cảnh bảo mật. Thiết bị có thể được tạo cấu hình để thực hiện hoạt động được thực hiện bởi AMF thứ hai theo trường hợp bất kỳ trong khía cạnh thứ hai, khía cạnh thứ sáu, các cách triển khai khả thi của khía cạnh thứ hai, hoặc các triển khai khả thi của khía cạnh thứ sáu. Cụ thể là, thiết bị thu thập ngữ cảnh bảo mật có thể bao gồm thành phần (phương tiện) tương ứng được tạo cấu hình để thực hiện các bước hoặc các chức năng được mô tả theo trường hợp bất kỳ trong khía cạnh thứ hai, khía cạnh thứ sáu, các cách triển khai khả thi của khía cạnh thứ hai, hoặc các triển khai khả thi của khía cạnh thứ sáu, và thành phần có thể là AMF thứ hai theo các khía cạnh thứ hai và thứ sáu, hoặc chip hoặc môđun chức năng trong AMF thứ hai theo các khía cạnh thứ hai và thứ sáu. Các bước hoặc các chức năng có thể được triển khai bằng cách phần mềm, phần cứng, hoặc kết hợp của phần cứng và phần mềm.

Khía cạnh thứ mười đề cập đến thiết bị thu thập ngữ cảnh bảo mật. Thiết bị có thể được tạo cấu hình để thực hiện hoạt động được thực hiện bởi UE theo khía cạnh thứ ba. Cụ thể là, thiết bị thu thập ngữ cảnh bảo mật có thể bao gồm thành phần (phương tiện) tương ứng được tạo cấu hình để thực hiện các bước hoặc các chức năng được mô tả in khía cạnh thứ ba, và thành phần có thể là UE theo khía cạnh thứ ba, hoặc chip hoặc môđun chức năng trong UE theo khía cạnh thứ ba. Các bước hoặc các chức năng có thể được triển khai bằng cách phần mềm, phần cứng, hoặc kết hợp của phần cứng và phần mềm.

Khía cạnh thứ mười một đề cập đến bộ phận truyền thông, bao gồm bộ xử lý, bộ thu phát, và bộ nhớ. Bộ nhớ được tạo cấu hình để lưu trữ chương trình máy tính. Bộ thu phát được tạo cấu hình để thực hiện các bước gửi và nhận trong phương pháp thu thập ngữ cảnh bảo mật theo triển khai khả thi bất kỳ theo các khía cạnh từ thứ nhất đến thứ năm. Bộ xử lý được tạo cấu hình để gọi chương trình máy tính từ bộ nhớ và chạy chương trình máy tính, để thiết bị truyền thông có thể thực hiện phương pháp thu thập ngữ cảnh bảo mật theo triển khai khả thi bất kỳ theo các khía cạnh từ thứ nhất đến thứ sáu.

Một cách tùy chọn, có một hoặc nhiều bộ xử lý và một hoặc nhiều bộ nhớ.

Một cách tùy chọn, bộ nhớ có thể được tích hợp với bộ xử lý, hoặc bộ nhớ

và bộ xử lý có thể được đặt riêng rẽ.

Một cách tùy chọn, bộ thu phát bao gồm bộ phát (transmitter) và bộ thu (receiver).

Khía cạnh thứ mười hai đề cập đến hệ thống. Hệ thống bao gồm các thiết bị thu thập ngữ cảnh bảo mật theo khía cạnh thứ tám và khía cạnh thứ chín.

Khía cạnh thứ mười ba đề cập đến sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính bao gồm chương trình máy tính (cũng có thể được gọi là mã hoặc lệnh). Khi chương trình máy tính được chạy, máy tính có thể thực hiện phương pháp theo triển khai khả thi bất kỳ theo các khía cạnh từ thứ nhất đến thứ sáu.

Khía cạnh thứ mười bốn đề cập đến vật ghi máy tính đọc được. Vật ghi máy tính đọc được lưu trữ chương trình máy tính (cũng có thể được gọi là mã hoặc lệnh). Khi chương trình máy tính được chạy trên máy tính, máy tính có thể thực hiện phương pháp theo triển khai khả thi bất kỳ theo các khía cạnh từ thứ nhất đến thứ sáu.

Khía cạnh thứ mười năm đề cập đến hệ thống chip, bao gồm bộ nhớ và bộ xử lý. Bộ nhớ được tạo cấu hình để lưu trữ chương trình máy tính. Bộ xử lý được tạo cấu hình để gọi chương trình máy tính từ bộ nhớ và chạy chương trình máy tính, sao cho thiết bị truyền thông trên đó hệ thống chip được cài đặt thực hiện phương pháp theo triển khai khả thi bất kỳ theo các khía cạnh từ thứ nhất đến thứ sáu.

Mô tả vắn tắt các hình vẽ

Fig.1 là kiến trúc mạng có thể áp dụng cho các phương án thực hiện sáng chế;

Fig.2 là lưu đồ chuyển vùng giữa các hệ thống truyền thông;

Fig.3 là sơ đồ của phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế;

Fig.4 là sơ đồ của phương pháp thu thập ngữ cảnh bảo mật khác theo phương án thực hiện sáng chế;

Fig.5 là sơ đồ của thiết bị thu thập ngữ cảnh bảo mật 50 theo phương án

thực hiện sáng chế;

Fig.6 là sơ đồ cấu trúc của UE 60 theo phương án thực hiện sáng chế;

Fig.7 là sơ đồ của thiết bị thu thập ngữ cảnh bảo mật 70 theo phương án thực hiện sáng chế;

Fig.8 là sơ đồ cấu trúc của AMF thứ nhất 80 theo phương án thực hiện sáng chế;

Fig.9 là sơ đồ của thiết bị thu thập ngữ cảnh bảo mật 90 theo phương án thực hiện sáng chế; và

Fig.10 là sơ đồ cấu trúc của AMF thứ hai 100 theo phương án thực hiện sáng chế.

Mô tả chi tiết sáng chế

Phần sau mô tả các giải pháp kỹ thuật của sáng chế dựa vào các hình vẽ đi kèm.

Các giải pháp kỹ thuật của các phương án thực hiện sáng chế có thể được áp dụng cho các hệ thống truyền thông khác nhau, chẳng hạn hệ thống truyền thông di động toàn cầu (global system for mobile communications, GSM), hệ thống đa truy nhập phân chia mã (code division multiple access, CDMA), hệ thống CDMA băng rộng (wideband code division multiple access, WCDMA), hệ thống dịch vụ vô tuyến gói tổng hợp (general packet radio service, GPRS), hệ thống tiến hóa dài hạn (long term evolution, LTE), hệ thống song công phân chia tần số LTE (frequency division duplex, FDD), hệ thống song công phân chia thời gian LTE (time division duplex, TDD), hệ thống viễn thông di động toàn cầu (universal mobile telecommunication system, UMTS), hệ thống truyền liên tác toàn cầu truy nhập vi sóng (worldwide interoperability for microwave access, WiMAX), hệ thống thế hệ thứ 5 (5th generation, 5G) tương lai, hoặc hệ thống vô tuyến mới (new radio, NR).

Fig.1 là kiến trúc mạng có thể áp dụng cho các phương án thực hiện sáng chế. Như được thể hiện trên Fig.1, phần sau mô tả riêng rẽ các thành phần trong kiến trúc mạng.

1. Thiết bị người dùng (user equipment, UE) 110 có thể bao gồm các thiết

bị cầm tay khác nhau, các thiết bị lắp trong xe, các thiết bị đeo được, và các thiết bị tính toán có chức năng truyền thông không dây, hoặc các thiết bị xử lý khác được kết nối với modem không dây, và các dạng khác nhau của các thiết bị đầu cuối, các trạm di động (mobile station, MS), các thiết bị đầu cuối (terminal), máy khách phần mềm, và tương tự. Chẳng hạn, UE 110 có thể là đồng hồ đo nước, đồng hồ đo điện, hoặc bộ cảm biến.

2. Phần tử mạng truy nhập (vô tuyến) (radio access network, (R)AN) 120 được tạo cấu hình để tạo chức năng truy nhập mạng cho các UE được cấp quyền trong khu vực cụ thể, và có thể sử dụng các đường hầm truyền có chất lượng khác nhau dựa trên các mức, các yêu cầu dịch vụ, và tương tự của các UE.

Phần tử (R)AN có thể quản lý các tài nguyên vô tuyến và cấp dịch vụ truy nhập cho UE, để chuyển tiếp tín hiệu điều khiển và dữ liệu UE giữa UE và mạng lõi. Phần tử (R)AN cũng có thể được hiểu là trạm cơ sở trong mạng đã biết.

3. Phần tử mạng mặt phẳng người dùng 130 được sử dụng để định tuyến và chuyển tiếp gói, xử lý chất lượng dịch vụ (quality of service, QoS) của dữ liệu mặt phẳng người dùng, và tương tự.

Trong hệ thống truyền thông 5G, phần tử mạng mặt phẳng người dùng có thể là phần tử mạng thực hiện chức năng mặt phẳng người dùng (user plane function, UPF). Trong hệ thống truyền thông tương lai, phần tử mạng mặt phẳng người dùng có thể vẫn là phần tử mạng thực hiện UPF, hoặc có thể có tên khác. Điều này không bị giới hạn ở sáng chế.

4. Phần tử mạng dữ liệu 140 được tạo cấu hình để tạo mạng để truyền dữ liệu.

Trong hệ thống truyền thông 5G, phần tử mạng dữ liệu có thể là phần tử mạng dữ liệu (data network, DN). Trong hệ thống truyền thông tương lai, phần tử mạng dữ liệu có thể vẫn là phần tử DN, hoặc có thể có tên khác. Điều này không bị giới hạn ở sáng chế.

5. Phần tử mạng quản lý truy nhập và di động 150 chủ yếu được tạo cấu hình để thực hiện quản lý di động, quản lý truy nhập, và tương tự. Phần tử

mạng quản lý truy nhập và di động 150 có thể được tạo cấu hình để thực hiện các chức năng, chẳng hạn, ngăn xen theo luật và ủy quyền/xác thực truy nhập, khác ngoài quản lý phiên ở các chức năng của thực thể quản lý di động (mobility management entity, MME).

Trong hệ thống truyền thông 5G, phần tử mạng quản lý truy nhập và di động có thể là chức năng quản lý truy nhập và di động (access and mobility management function, AMF). Trong hệ thống truyền thông tương lai, thiết bị quản lý truy nhập và di động có thể vẫn là AMF, hoặc có thể có tên khác. Điều này không bị giới hạn ở sáng chế.

6. Phần tử mạng quản lý phiên 160 chủ yếu được tạo cấu hình để quản lý phiên, gán và quản lý địa chỉ giao thức internet (internet protocol, IP) của UE, chọn điểm cuối mà có thể quản lý giao diện UPF và giao diện chức năng tính cước và điều khiển chính sách, thông báo dữ liệu liên kết xuống, và tương tự.

Trong hệ thống truyền thông 5G, phần tử mạng quản lý phiên có thể là phần tử mạng thực hiện chức năng quản lý phiên (session management function, SMF). Trong hệ thống truyền thông tương lai, phần tử mạng quản lý phiên có thể vẫn là phần tử mạng SMF, hoặc có thể có tên khác. Điều này không bị giới hạn ở sáng chế.

7. Phần tử mạng điều khiển chính sách 170 được tạo cấu hình để hướng dẫn khuôn khổ chính sách thống nhất hành vi mạng, và cung cấp thông tin luật lệ chính sách cho phần tử mạng thực hiện chức năng mặt phẳng điều khiển (chẳng hạn, phần tử mạng AMF hoặc SMF), và tương tự.

Trong hệ thống truyền thông 4G, phần tử mạng điều khiển chính sách có thể là phần tử mạng thực hiện chức năng chính sách và các quy tắc tính cước (policy and charging rules function, PCRF). Trong hệ thống truyền thông 5G, phần tử mạng điều khiển chính sách có thể là phần tử mạng thực hiện chức năng điều khiển chính sách (policy control function, PCF). Trong hệ thống truyền thông tương lai, phần tử mạng điều khiển chính sách có thể vẫn là phần tử mạng thực hiện PCF, hoặc có thể có tên khác. Điều này không bị giới hạn ở sáng chế.

8. Máy chủ xác thực 180 được tạo cấu hình để xác thực dịch vụ, tạo khóa để

thực hiện xác thực hai chiều cho UE, và hỗ trợ khung xác thực thống nhất.

Trong hệ thống truyền thông 5G, máy chủ xác thực có thể là phần tử mạng thực hiện chức năng máy chủ xác thực (authentication server function, AUSF). Trong hệ thống truyền thông tương lai, phần tử mạng thực hiện AUSF vẫn có thể là phần tử mạng thực hiện AUSF, hoặc có thể có tên khác. Điều này không bị giới hạn ở sáng chế.

9. Phần tử mạng quản lý dữ liệu 190 được tạo cấu hình để xử lý định danh UE, thực hiện xác thực truy nhập, đăng ký, và quản lý di động, và tương tự.

Trong hệ thống truyền thông 5G, phần tử mạng quản lý dữ liệu có thể là phần tử mạng quản lý dữ liệu thống nhất (unified data management, UDM). Trong hệ thống truyền thông 4G, phần tử mạng quản lý dữ liệu có thể là phần tử mạng máy chủ thuê bao thường trú (home subscriber server, HSS). Trong hệ thống truyền thông tương lai, phần tử mạng UDM vẫn có thể là phần tử mạng UDM, hoặc có thể có tên khác. Điều này không bị giới hạn ở sáng chế.

10. Phần tử mạng ứng dụng 1100 được tạo cấu hình để thực hiện định tuyến dữ liệu bị ảnh hưởng ứng dụng, truy nhập phần tử mạng thực hiện chức năng công khai mạng, tương tác với khung chính sách để thực hiện điều khiển chính sách, và tương tự.

Trong hệ thống truyền thông 5G, phần tử mạng ứng dụng có thể là phần tử mạng thực hiện chức năng ứng dụng (application function, AF). Trong hệ thống truyền thông tương lai, phần tử mạng ứng dụng có thể vẫn là phần tử mạng thực hiện AF, hoặc có thể có tên khác. Điều này không bị giới hạn ở sáng chế.

11. Phần tử mạng lưu trữ mạng được tạo cấu hình để duy trì thông tin thời gian thực của tất cả các dịch vụ chức năng mạng trong mạng.

Trong hệ thống truyền thông 5G, phần tử mạng lưu trữ mạng có thể là phần tử mạng thực hiện chức năng lưu trữ mạng (network repository function, NRF). Trong hệ thống truyền thông tương lai, phần tử mạng lưu trữ mạng có thể vẫn là phần tử mạng NRF, hoặc có thể có tên khác. Điều này không bị giới hạn ở sáng chế.

Có thể hiểu rằng các phần tử mạng hoặc các chức năng nêu trên có thể là các phần tử mạng trong thiết bị phần cứng, các chức năng phần mềm chạy trên

phần cứng dành riêng, hoặc các chức năng ảo hóa được khởi tạo trên nền tảng (chẳng hạn, nền tảng đám mây). Để dễ mô tả, sáng chế được mô tả dưới đây nhờ sử dụng ví dụ trong đó thiết bị quản lý truy nhập và di động là AMF, phần tử mạng quản lý dữ liệu là phần tử mạng UDM, phần tử mạng quản lý phiên là phần tử mạng SMF, và phần tử mạng mặt phẳng người dùng là phần tử mạng UPF.

Để dễ mô tả, theo các phương án thực hiện sáng chế, phương pháp thiết lập phiên được mô tả nhờ sử dụng ví dụ trong đó thiết bị là thực thể AMF hoặc thực thể UDM. Đối với phương pháp triển khai trong đó thiết bị là chip trong thực thể AMF hoặc chip trong thực thể UDM, tham khảo các phần mô tả cụ thể về phương pháp thiết lập phiên trong đó thiết bị là thực thể AMF hoặc thực thể UDM. Các chi tiết không được lặp lại.

Trong kiến trúc mạng được thể hiện trên Fig.1, UE được kết nối với AMF qua giao diện N1, (R)AN được kết nối với AMF qua giao diện N2, và (R)AN được kết nối với UPF qua giao diện N3. Các UPF được nối với nhau qua giao diện N9, và UPF được liên kết với DN qua giao diện N6. SMF điều khiển UPF qua giao diện N4. AMF được kết nối với SMF qua giao diện N11. AMF thu được dữ liệu thuê bao của UE từ khối UDM qua giao diện N8. SMF thu được dữ liệu thuê bao của UE từ khối UDM qua giao diện N10.

Cần hiểu rằng kiến trúc mạng nêu trên được áp dụng cho các phương án thực hiện sáng chế chỉ là ví dụ, và kiến trúc mạng có thể áp dụng cho các phương án thực hiện sáng chế không bị giới hạn ở đó. Kiến trúc mạng bất kỳ có thể thực hiện các chức năng của các phần tử mạng nêu trên có thể áp dụng cho các phương án thực hiện sáng chế.

Chẳng hạn, trong một số kiến trúc mạng, các phần tử mạng thực hiện chức năng mạng và các thực thể, chẳng hạn AMF, phần tử mạng thực hiện SMF, phần tử mạng thực hiện PCF, phần tử mạng thực hiện BSF, và phần tử mạng thực hiện UDM đều được gọi là các phần tử mạng thực hiện chức năng mạng (network function, NF). Theo cách khác, trong một số kiến trúc mạng khác, tập hợp phần tử mạng, chẳng hạn, AMF, phần tử mạng SMF, phần tử mạng PCF, phần tử mạng BSF, và phần tử mạng UDM có thể được gọi là phần tử mạng

thực hiện chức năng mặt phẳng điều khiển.

UE theo các phương án thực hiện sáng chế có thể là thiết bị đầu cuối truy nhập, khối thuê bao, trạm thuê bao, trạm di động, bảng điều khiển di động, trạm chuyển tiếp, trạm từ xa, thiết bị đầu cuối từ xa, thiết bị di động, thiết bị đầu cuối người dùng, bộ phận đầu cuối (terminal equipment), thiết bị đầu cuối (terminal), thiết bị truyền thông không dây, đại diện người dùng, thiết bị người dùng, hoặc tương tự. UE có thể theo cách khác là điện thoại tế bào, điện thoại không dây, điện thoại giao thức khởi tạo phiên (session initiation protocol, SIP), trạm vòng cục bộ không dây (wireless local loop, WLL), thiết bị hỗ trợ số cá nhân (personal digital assistant, PDA), thiết bị cầm tay có chức năng truyền thông không dây, thiết bị điện toán, thiết bị xử lý khác được kết nối với modem không dây, thiết bị lắp trong xe, thiết bị đeo được, UE trong mạng 5G tương lai, UE trong mạng di động mặt đất công cộng (public land mobile network, PLMN) tiến hóa tương lai, hoặc tương tự. Điều này không bị giới hạn ở các phương án thực hiện sáng chế.

Thiết bị mạng theo các phương án thực hiện sáng chế có thể là thiết bị bất kỳ có chức năng thu phát không dây và được tạo cấu hình để truyền thông với UE. Thiết bị bao gồm nhưng không bị giới hạn ở nút B tiến hóa (evolved Node B, eNB), bộ điều khiển mạng vô tuyến (radio network controller, RNC), nút B (Node B, NB), bộ điều khiển trạm cơ sở (base station controller, BSC), trạm thu phát cơ sở (base transceiver station, BTS), trạm cơ sở thường trú (chẳng hạn, nút B tiến hóa thường trú, hoặc nút B thường trú (home Node B, HNB)), khối băng cơ sở (baseBand unit, BBU), điểm truy nhập (access point, AP) trong hệ thống không dây (wireless fidelity, WIFI), nút chuyển tiếp không dây, nút backhaul không dây, điểm truyền (transmission point, TP), điểm thu phát (transmission and reception point, TRP), hoặc tương tự. Theo cách khác, thiết bị có thể là gNB hoặc điểm phát (TRP hoặc TP) trong hệ thống 5G, chẳng hạn hệ thống NR, có thể là một panen anten hoặc nhóm (bao gồm các panen anten) panen anten của trạm cơ sở trong hệ thống 5G, hoặc có thể là nút mạng, chẳng hạn khối băng cơ sở (baseband unit, BBU) hoặc khối phân tán (distributed unit, DU), tạo thành gNB hoặc TP.

Theo một số triển khai, gNB có thể bao gồm khối tập trung (centralized unit, CU) và DU. gNB có thể còn bao gồm khối anten hoạt động (active antenna unit, AAU). CU triển khai một số chức năng của gNB, và DU triển khai một số chức năng của gNB. Chẳng hạn, CU chịu trách nhiệm xử lý giao thức và dịch vụ phi thời gian thực, và triển khai các chức năng của lớp điều khiển tài nguyên vô tuyến (radio resource control, RRC) layer và lớp giao thức hội tụ dữ liệu gói (packet data convergence protocol, PDCP). DU chịu trách nhiệm xử lý giao thức lớp vật lý và dịch vụ thời gian thực, và triển khai các chức năng của lớp điều khiển liên kết vô tuyến (radio link control, RLC), lớp điều khiển truy nhập phương tiện (media access control, MAC), và lớp vật lý (physical, PHY). AAU triển khai một số chức năng xử lý lớp vật lý, xử lý tần số vô tuyến, và chức năng liên quan đến anten hoạt động. Thông tin ở lớp RRC dần dần được biến đổi thành thông tin ở lớp PHY, hoặc được biến đổi từ thông tin ở lớp PHY. Do vậy, trong kiến trúc này, báo hiệu lớp cao hơn, chẳng hạn, báo hiệu lớp RRC cũng có thể được xem xét như là được gửi bởi DU hoặc được gửi bởi DU và AAU. Có thể hiểu rằng thiết bị mạng có thể là thiết bị bao gồm một hoặc nhiều nút CU, nút DU, và nút AAU. Ngoài ra, CU có thể là thiết bị mạng trong mạng truy nhập (radio access network, RAN), hoặc có thể là thiết bị mạng trong mạng lõi (core network, CN). Điều này không bị giới hạn ở sáng chế.

Theo các phương án thực hiện sáng chế, UE hoặc thiết bị mạng bao gồm lớp phần cứng, lớp hệ điều hành chạy phía trên lớp phần cứng, và lớp ứng dụng chạy phía trên lớp hệ điều hành. Lớp phần cứng bao gồm phần cứng chẳng hạn khối xử lý trung tâm (central processing unit, CPU), khối quản lý bộ nhớ (memory management unit, MMU), và bộ nhớ (cũng được gọi là bộ nhớ chính). Hệ điều hành có thể là một hoặc nhiều loại của hệ điều hành máy tính mà thực hiện xử lý dịch vụ nhờ sử dụng tiến trình (process), chẳng hạn, hệ điều hành Linux, hệ điều hành Unix, hệ điều hành Android, hệ điều hành iOS, hoặc hệ điều hành Windows. Lớp ứng dụng bao gồm các ứng dụng, chẳng hạn, bộ trình duyệt, sổ địa chỉ, phần mềm xử lý từ, và phần mềm truyền thông tức thời. Ngoài ra, cấu trúc cụ thể của thực thể để thực hiện phương pháp theo các phương án thực hiện sáng chế không bị giới hạn cụ thể theo các phương án

thực hiện sáng chế, giả sử rằng mã ghi chương trình của phương pháp theo các phương án thực hiện sáng chế có thể được vận hành để thực hiện truyền thông theo phương pháp theo các phương án thực hiện sáng chế. Chẳng hạn, thực thể để thực hiện phương pháp theo các phương án thực hiện sáng chế có thể là UE hoặc thiết bị mạng, hoặc có thể là mô đun chức năng có thể gọi và thực thi chương trình trong UE hoặc thiết bị mạng.

Ngoài ra, các khía cạnh hoặc các dấu hiệu của sáng chế có thể được triển khai dưới dạng phương pháp, thiết bị hoặc sản phẩm sử dụng công nghệ lập trình và/hoặc kỹ thuật chuẩn. Cụm từ "sản phẩm" được sử dụng theo sáng chế bao gồm chương trình máy tính có thể được truy nhập từ thành phần máy tính đọc được bất kỳ, kênh mang hoặc phương tiện. Chẳng hạn, phương tiện máy tính đọc được có thể bao gồm mà không bị giới hạn ở: thành phần lưu trữ từ tính (chẳng hạn, đĩa cứng, đĩa mềm hoặc băng từ), đĩa quang (chẳng hạn, đĩa compac (compact disc, CD) hoặc đĩa đa dụng số (digital versatile disc, DVD)), thẻ thông minh, và thành phần bộ nhớ nhanh (chẳng hạn, bộ nhớ chỉ đọc lập trình được xóa được (erasable programmable read-only memory, EPROM), thẻ, gậy, hoặc ổ khóa). Ngoài ra, các phương tiện lưu trữ khác nhau được mô tả trong bản mô tả có thể chỉ báo một hoặc nhiều thiết bị và/hoặc phương tiện máy đọc được khác mà được tạo cấu hình để lưu trữ thông tin. Cụm từ "phương tiện lưu trữ máy đọc được" có thể bao gồm mà không bị giới hạn ở kênh vô tuyến, và các phương tiện khác có thể lưu trữ, chứa, và/hoặc mang lệnh và/hoặc dữ liệu.

Các phương án thực hiện sáng chế chủ yếu đề cập đến thực thể quản lý di động (mobility management entity, MME) khi kiến trúc mạng được thể hiện trên Fig.1 là kiến trúc mạng 4G, và AMF và UE khi kiến trúc mạng được thể hiện trên Fig.1 là kiến trúc mạng 5G. Đối với AMF, sáng chế đề cập đến AMF thứ nhất và AMF thứ hai. Cụ thể là, AMF thứ nhất theo sáng chế là AMF mà được chọn, từ hệ thống truyền thông 5G trong tiến trình trong đó UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, cho UE bởi MME trong hệ thống truyền thông 4G để cấp dịch vụ mạng lõi cho UE. AMF thứ hai theo sáng chế là AMF, khác ngoài AMF thứ nhất trong hệ thống

truyền thông 5G trong tiến trình trong đó UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, mà lưu trữ ngữ cảnh bảo mật của UE.

Cần hiểu rằng "thứ nhất" và "thứ hai" theo sáng chế chỉ được sử dụng để phân biệt, và không được hiểu như là giới hạn bất kỳ ở sáng chế. Chẳng hạn, AMF thứ nhất và AMF thứ hai chỉ được sử dụng để phân biệt giữa các AMF khác nhau.

Để dễ hiểu phương pháp thu thập ngữ cảnh bảo mật theo các phương án thực hiện sáng chế, phần sau mô tả vắn tắt, dựa vào Fig.2, tiến trình trong đó UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G. Fig.2 là lưu đồ chuyển vùng giữa các hệ thống truyền thông. Lưu đồ bao gồm UE, MME, AMF thứ nhất, và AMF thứ hai.

Chuyển vùng giữa các hệ thống truyền thông bao gồm các bước sau.

S210: MME truyền thông điệp yêu cầu chuyển tiếp định vị lại (forward relocation request) đến AMF thứ nhất.

Cụ thể là, MME trong hệ thống truyền thông 4G biết rằng UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, và cần chọn, cho UE, AMF thứ nhất từ hệ thống truyền thông 5G để tiếp tục cấp dịch vụ quản lý truy nhập và di động cho UE. Khi UE truy nhập hệ thống truyền thông 4G, UE và MME thu được cùng khóa K_{ASME}. Khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, MME chọn AMF thứ nhất và truyền K_{ASME} và tham số bước nhảy tiếp theo (next hop, NH) đến AMF thứ nhất. Nói cách khác, thông điệp chuyển tiếp yêu cầu định vị lại mang các tham số, chẳng hạn, K_{ASME} và NH.

Theo phương án thực hiện sáng chế, cách MME nhận biết chuyển vùng giữa các hệ thống không bị giới hạn. Để biết chi tiết, tham khảo các phần mô tả thủ tục chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G trong giao thức hiện tại. Chẳng hạn, trạm cơ sở trong hệ thống truyền thông 4G có thể gửi yêu cầu chuyển vùng đến MME, sao cho MME biết rằng UE cần được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G.

Ngoài ra, theo phương án thực hiện sáng chế, cách thức MME chọn AMF

thứ nhất không bị giới hạn. Để biết chi tiết, tham khảo các phần mô tả trong giao thức hiện tại. Chẳng hạn, MME lưu trữ ít nhất một AMF được tạo cấu hình bởi người vận hành. Khi MME biết rằng UE cần được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, MME chọn AMF thứ nhất từ ít nhất một AMF.

S220: AMF thứ nhất xác định ngữ cảnh bảo mật được ánh xạ (mapped).

Cụ thể là, AMF thứ nhất dẫn xuất ngữ cảnh bảo mật được ánh xạ dựa trên các tham số, chẳng hạn K_{ASME} và NH, được mang trong thông điệp yêu cầu định vị lại được nhận. Ngữ cảnh bảo mật được ánh xạ được bao gồm trong ngữ cảnh được ánh xạ của UE. Cần hiểu rằng ngữ cảnh được ánh xạ theo sáng chế là ngữ cảnh bảo mật của UE được dẫn xuất bởi AMF thứ nhất và UE một cách riêng rẽ dựa trên ngữ cảnh được tạo qua thương lượng giữa UE và MME trong hệ thống truyền thông 4G. Đối với cách thức dẫn xuất ngữ cảnh bảo mật của UE dựa trên ngữ cảnh 4G, tham khảo các mô tả trong giao thức hiện tại, và tiến trình này không bị giới hạn theo sáng chế. Ngữ cảnh bảo mật được ánh xạ thu được bởi AMF thứ nhất và UE riêng rẽ dựa trên ngữ cảnh bảo mật giữa MME và UE. Ngoài ra, theo sáng chế, ngữ cảnh được thương lượng giữa UE và MME trong hệ thống truyền thông 4G bao gồm ngữ cảnh bảo mật giữa UE và MME, và có thể cũng được gọi là ngữ cảnh 4G của UE để phân biệt. Tương tự, theo sáng chế, trước khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, ngữ cảnh bảo mật của UE mà được lưu trữ trong UE và AMF thứ hai là ngữ cảnh được thương lượng giữa UE và AMF thứ hai trong hệ thống truyền thông 5G, bao gồm ngữ cảnh bảo mật giữa UE và AMF thứ hai, và có thể cũng được gọi là ngữ cảnh 5G của UE để phân biệt.

Để dễ mô tả, dưới đây, ngữ cảnh bảo mật thu được bởi AMF thứ nhất và UE riêng rẽ qua dẫn xuất dựa trên ngữ cảnh bảo mật giữa MME và UE được gọi là ngữ cảnh bảo mật được ánh xạ, và ngữ cảnh bảo mật giữa AMF thứ hai và UE được gọi là ngữ cảnh bảo mật nguyên gốc (native).

Cần hiểu thêm rằng phương án thực hiện sáng chế chủ yếu đề cập đến việc gửi ngữ cảnh bảo mật của UE bởi AMF thứ hai đến AMF thứ nhất. Ngữ cảnh bảo mật của UE là một phần ngữ cảnh của UE, và có thể được truyền cùng với

ngữ cảnh của UE. Do vậy, để dễ mô tả, theo phương án thực hiện sáng chế, gửi ngữ cảnh bảo mật của UE bởi AMF thứ hai đến AMF thứ nhất có thể được mô tả như là gửi ngữ cảnh của UE hoặc gửi ngữ cảnh bảo mật của UE. Điều này chỉ được sử dụng để dễ mô tả, và không giới hạn bất kỳ ở phạm vi bảo hộ của các phương án thực hiện sáng chế.

Việc AMF thứ nhất dẫn xuất ngữ cảnh bảo mật được ánh xạ của UE dựa trên các tham số, chẳng hạn, K_{ASME} và NH, được mang trong thông điệp yêu cầu định vị lại được nhận bao gồm việc AMF thứ nhất dẫn xuất khóa K_{AMF1} dựa trên K_{ASME} và NH.

Chẳng hạn, sau khi nhận K_{ASME} và NH, AMF thứ nhất có thể tính toán khóa K_{AMF1} nhờ sử dụng công thức dẫn xuất định trước. Công thức dẫn xuất là: K_{AMF1} = HMAC – SHA – 256 (Key, FC||P0||L0), trong đó FC = 0x76, P0 = giá trị NH, L0 = chiều dài của giá trị NH (tức là, 0x00 0x20), và KEY = K_{ASME}. AMF thứ nhất tính toán khóa bảo vệ tính toàn vẹn $K_{NASint1}$ và khóa bảo vệ tính bảo mật $K_{NASenc1}$ dựa trên khóa K_{AMF1} và thuật toán bảo mật được thương lượng với UE, trong đó K_{AMF1}, $K_{NASint1}$, và $K_{NASenc1}$ được bao gồm trong ngữ cảnh bảo mật của UE. K_{AMF1}, $K_{NASint1}$, và $K_{NASenc1}$ được dẫn xuất dựa trên K_{ASME} và NH, và K_{ASME} và NH là ngữ cảnh bảo mật giữa UE và MME. Do vậy, K_{AMF1}, $K_{NASint1}$, và $K_{NASenc1}$ được gọi là ngữ cảnh bảo mật được ánh xạ của UE.

S230: AMF thứ nhất truyền thông điệp chuyển tiếp đáp ứng định vị lại (forward relocation response) đến MME.

Cụ thể là, sau khi xác định ngữ cảnh bảo mật được ánh xạ, AMF thứ nhất truyền thông điệp chuyển tiếp đáp ứng định vị lại đến MME. Thông điệp chuyển tiếp đáp ứng định vị lại được sử dụng để thông báo MME rằng AMF thứ nhất có thể được sử dụng làm AMF cung cấp dịch vụ quản lý truy nhập và di động cho UE trong hệ thống truyền thông 5G khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G.

S240: MME truyền thông điệp lệnh chuyển vùng (handover command) đến UE.

Sau khi nhận thông điệp chuyển tiếp đáp ứng phân phối lại được gửi bởi AMF thứ nhất, MME biết rằng AMF thứ nhất có thể cấp dịch vụ quản lý truy

nhập và di động cho UE. Trong trường hợp này, MME truyền chuyển vùng thông điệp lệnh đến UE, sao cho UE biết rằng UE có thể được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G.

S250: UE xác định ngữ cảnh bảo mật được ánh xạ.

Sau khi nhận thông điệp lệnh chuyển vùng, UE tính toán, nhờ sử dụng công thức dẫn xuất định trước, khóa K_{AMF1} dựa trên khóa K_{ASME} và NH được lưu trữ trong UE. Đối với quá trình dẫn xuất cụ thể, tham khảo bước S220 nêu trên, và chi tiết không được mô tả lại ở đây.

Sau bbước S250, UE và AMF thứ nhất thu được khóa tương tự K_{AMF1}, và khóa K_{AMF1} có thể lần lượt được sử dụng để dẫn xuất khóa khác.

Chẳng hạn, UE và AMF thứ nhất thu được cùng khóa K_{AMF1}. Sau đó, dựa trên K_{AMF1} và thuật toán bảo vệ tính toàn vẹn tầng không truy nhập (non-access stratum, NAS) và thuật toán bảo vệ tính bảo mật được thương lượng giữa UE và AMF thứ nhất, UE và AMF thứ nhất tạo khóa bảo vệ tính toàn vẹn $K_{NASint1}$ và khóa bảo vệ tính bảo mật $K_{NASenc1}$ được sử dụng để bảo vệ thông điệp NAS (chẳng hạn, thông điệp yêu cầu đăng ký). Cụ thể là, $K_{NASint1}$ và $K_{NASenc1}$ được tính toán như sau:

$K_{NASint1}$ = HMAC – SHA – 256 (KEY, S), trong đó S = $FC||P0_1||L0_1||P1_1||L1_1$, FC = 0x69, $P0_1$ = bộ phân biệt loại thuật toán (algorithm type distinguisher), $L0_1$ = chiều dài của bộ phân biệt loại thuật toán (length of algorithm type distinguisher) (tức là, 0x00 0x01), $P1_1$ = định danh thuật toán (algorithm identity), $L1_1$ = chiều dài của định danh thuật toán (length of algorithm identity) (tức là, 0x00 0x01), và KEY = K_{AMF1}.

$K_{NASenc1}$ = HMAC – SHA – 256 (KEY, S), trong đó S = FC||P0||L0||P1||L1, FC = 0x69, P0 = bộ phân biệt loại thuật toán, L0 = chiều dài của bộ phân biệt loại thuật toán (tức là, 0x00 0x01), P1 = định danh thuật toán, L1 = chiều dài của định danh thuật toán (tức là, 0x00 0x01), và KEY = K_{AMF1}.

Bộ phân biệt loại thuật toán và định danh thuật toán để tính toán $K_{NASint1}$ khác với bộ phân biệt và định danh để tính toán $K_{NASenc1}$.

Sau khi hoàn thành chuyển vùng, UE khởi tạo đăng ký di động, nói cách khác, thực hiện bước S260. UE truyền thông điệp yêu cầu đăng ký (registration

request) đến AMF thứ nhất, và UE thực hiện bảo vệ bảo mật trên thông điệp yêu cầu đăng ký nhờ sử dụng ngữ cảnh bảo mật được ánh xạ được tạo qua dẫn xuất dựa trên K_{AMF1} được tạo trước đó. Bảo vệ bảo mật bao gồm bảo vệ mật mã hóa và/hoặc bảo vệ tính toàn vẹn.

Cần hiểu rằng thông điệp được gửi bởi UE đến thiết bị mạng lõi có thể được chuyển tiếp bởi thiết bị mạng truy nhập. Do chức năng của thiết bị truy nhập không bị giới hạn theo phương án thực hiện sáng chế, thiết bị mạng truy nhập có thể chuyển tiếp thông điệp giữa UE và AMF thứ nhất. Để ngắn gọn, theo sáng chế, việc chuyển tiếp thông điệp giữa UE và AMF thứ nhất được mô tả như là việc UE truyền thông điệp yêu cầu đăng ký đến AMF thứ nhất và MME truyền thông điệp đến UE. Thông điệp yêu cầu đăng ký được gửi bởi UE còn bao gồm định danh UE tạm thời duy nhất toàn cục (globally unique temporary user equipment identity, GUTI) trong ngữ cảnh được ánh xạ, và GUTI được sử dụng bởi thiết bị mạng truy nhập để xác định chuyển tiếp thông điệp yêu cầu đăng ký đến AMF thứ nhất. Do GUTI được bao gồm trong ngữ cảnh được ánh xạ, GUTI có thể được gọi là GUTI được ánh xạ.

Một cách tùy chọn, khi UE truyền thông điệp yêu cầu đăng ký đến AMF thứ nhất, UE lưu trữ ngữ cảnh bảo mật của UE giữa UE và AMF khác (AMF thứ hai) và định danh UE tạm thời duy nhất toàn cục thế hệ thứ 5 (5th generation globally unique temporary user equipment identity, 5G-GUTI) của UE. Do vậy, UE bổ sung 5G-GUTI vào thông điệp yêu cầu đăng ký.

Cần hiểu rằng phương án thực hiện sáng chế chủ yếu liên quan đến tiến trình trong đó AMF thứ nhất thu được thành công ngữ cảnh bảo mật của UE từ AMF thứ hai. Do vậy, theo sáng chế, trường hợp sau chủ yếu được xem xét: Khi UE truyền thông điệp yêu cầu đăng ký đến AMF thứ nhất, UE lưu trữ ngữ cảnh bảo mật UE được thương lượng giữa UE và AMF thứ hai cũng như 5G-GUTI.

Cần hiểu thêm rằng nguyên nhân tại sao ngữ cảnh bảo mật và 5G-GUTI của UE được lưu trữ bởi UE và AMF thứ hai không bị giới hạn theo phương án thực hiện sáng chế, và có thể được xác định trong giao thức hiện tại. Chẳng hạn, trước khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống

truyền thông 5G, UE được chuyển vùng từ hệ thống truyền thông mạng 5G sang hệ thống truyền thông 4G. Theo cách khác, UE hỗ trợ kết nối kép truy nhập hệ thống truyền thông 5G qua kết nối phi 3GPP, và truy nhập hệ thống truyền thông 4G qua kết nối 3GPP cùng lúc. Theo cách này, UE ở chế độ kết nối được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G.

Cần hiểu rằng khi ngữ cảnh bảo mật của UE nằm giữa AMF thứ hai và UE tồn tại trên AMF thứ hai, AMF thứ nhất cần thu được ngữ cảnh bảo mật của UE từ AMF thứ hai. Cụ thể là, việc AMF thứ nhất thu được ngữ cảnh bảo mật của UE từ AMF thứ hai được xác định dựa trên 5G-GUTI được mang trong thông điệp yêu cầu đăng ký được nhận từ UE. 5G-GUTI được tạo cấu hình bởi AMF thứ hai cho UE và có thể được sử dụng để nhận diện UE và AMF thứ hai. Như được nêu trong giao thức, khi ngữ cảnh bảo mật của UE tồn tại trong hệ thống truyền thông 5G, ngữ cảnh bảo mật của UE thay vì ngữ cảnh bảo mật được ánh xạ được xác định qua thương lượng giữa AMF thứ nhất và UE được ưu tiên sử dụng, do ngữ cảnh bảo mật được ánh xạ thu được qua ánh xạ dựa trên ngữ cảnh bảo mật của UE giữa UE và MME trong hệ thống truyền thông 4G. Nói cách khác, thủ tục được thể hiện trên Fig.2 còn bao gồm S270 trong đó AMF thứ nhất khởi tạo yêu cầu gọi dịch vụ truyền ngữ cảnh UE (Namf_Communication_UEContextTransfer).

Cụ thể là, AMF thứ nhất nhận thông điệp yêu cầu đăng ký được gửi bởi UE, và khởi tạo yêu cầu gọi dịch vụ truyền ngữ cảnh UE đến AMF thứ hai dựa trên the 5G-GUTI được mang trong thông điệp yêu cầu đăng ký. yêu cầu gọi dịch vụ truyền ngữ cảnh UE mang thông điệp yêu cầu đăng ký.

Cần hiểu rằng thông điệp yêu cầu đăng ký được bảo vệ bảo mật dựa trên ngữ cảnh bảo mật được ánh xạ giữa UE và AMF thứ nhất, và AMF thứ hai xác định, dựa trên kết quả kiểm chứng thông điệp yêu cầu đăng ký, liệu có trả về ngữ cảnh bảo mật của UE cho AMF thứ nhất hay không. Nói cách khác, S290 được thực hiện. AMF thứ hai kiểm chứng thông điệp yêu cầu đăng ký.

Theo triển khai khả thi, AMF thứ hai không kiểm chứng thông điệp yêu cầu đăng ký. Trong trường hợp này, AMF thứ hai không trả về ngữ cảnh bảo mật

của UE cho AMF thứ nhất. Kết quả là, AMF thứ nhất không thu được ngữ cảnh bảo mật của UE từ AMF thứ hai, và AMF thứ nhất không thể ưu tiên sử dụng ngữ cảnh bảo mật của UE. Điều này không tuân thủ theo giao thức.

Theo triển khai khả thi khác, AMF thứ hai kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký. Trong trường hợp này, AMF thứ hai trả về ngữ cảnh bảo mật của UE cho AMF thứ nhất, và thực hiện S291 trong đó AMF thứ hai truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất. Một cách tùy chọn, việc AMF thứ hai truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất có thể được mô tả như là việc AMF thứ hai truyền ngữ cảnh của UE đến AMF thứ nhất. Ngữ cảnh của UE bao gồm ngữ cảnh bảo mật của UE được xác định qua thương lượng giữa AMF thứ hai và UE, và ngữ cảnh bảo mật của UE bao gồm khóa K_{AMF2}, số đếm tầng không truy nhập (non-access stratum count, NAS COUNT), và tương tự.

Một cách tùy chọn, trước khi truyền ngữ cảnh bảo mật của UE, AMF thứ hai có thể thực hiện dẫn xuất khóa trên khóa K_{AMF2} theo chính sách nội bộ. Nếu AMF thứ hai đã thực hiện dẫn xuất khóa trên K_{AMF2}, AMF thứ hai truyền, đến AMF thứ nhất, khóa K_{AMF2}' thu được sau khi dẫn xuất và thông tin chỉ báo dẫn xuất được sử dụng để chỉ báo rằng AMF thứ hai đã thực hiện dẫn xuất khóa trên K_{AMF2}.

Theo triển khai khả thi, dẫn xuất khóa theo sáng chế có thể là dẫn xuất khóa ngang.

Chẳng hạn, cách thức thực hiện dẫn xuất khóa ngang trên K_{AMF2} để tạo K_{AMF2}' như sau:

K_{AMF2}'=HMAC–SHA–256 (Key, S);

FC = 0x72;

P0 = 0x01;

L0 = chiều dài của P0 (tức là, 0x00 0x01);

P1 = NAS COUNT liên kết lên;

L1 = chiều dài của P1 (tức là, 0x00 0x04);

KEY = K_{AMF2};

S=FC||P0||L0||P1||L1.

Theo triển khai khả thi khác, việc dẫn xuất khóa theo sáng chế có thể là cách thức dẫn xuất khóa được thỏa hiệp giữa các phần tử mạng khác nhau. Chẳng hạn, AMF thứ nhất và AMF thứ hai thỏa hiệp trên cách thức dẫn xuất khóa định trước. Giả sử rằng ngữ cảnh bảo mật của UE mà được gửi bởi AMF thứ hai đến AMF thứ nhất bao gồm thông tin chỉ báo dẫn xuất, AMF thứ nhất có thể xác định rằng khóa trong ngữ cảnh bảo mật được nhận của UE thu được bởi AMF thứ hai bằng cách thực hiện dẫn xuất khóa theo cách dẫn xuất khóa định trước.

Tương tự, sau khi nhận thông tin chỉ báo dẫn xuất, AMF thứ nhất cũng truyền thông tin chỉ báo dẫn xuất đến UE, để chỉ báo UE thực hiện dẫn xuất khóa trên khóa K_{AMF2} để thu được khóa K_{AMF2}', sao cho UE và phía mạng thỏa thuận trên khóa. Cần hiểu rằng UE nhận định danh khóa chỉ báo khóa K_{AMF2}, và do vậy có thể xác định thực hiện dẫn xuất khóa trên khóa K_{AMF2} thay cho K_{AMF}. Định danh khóa không được cải thiện theo sáng chế. Do vậy, định danh khóa không được mô tả chi tiết ở đây.

Có thể được biết, từ tiến trình chuyển vùng UE từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G trên Fig.2, việc khi AMF thứ hai không kiểm chứng UE, AMF thứ nhất không thể thu được ngữ cảnh bảo mật của UE từ AMF thứ hai. Để tránh gặp sự cố khi thu thập ngữ cảnh bảo mật của UE, phương án thực hiện sáng chế đề cập đến phương pháp thu thập ngữ cảnh bảo mật. Khi AMF thứ nhất thu được ngữ cảnh bảo mật của UE từ AMF thứ hai, ngữ cảnh bảo mật mang thông tin chỉ báo. Thông tin chỉ báo chỉ báo rằng UE đã được kiểm chứng thành công. Dựa trên thông tin chỉ báo, AMF thứ hai không cần kiểm chứng UE, nhưng trả về trực tiếp ngữ cảnh bảo mật của UE. Điều này có thể tránh khả năng gặp sự cố thu được ngữ cảnh bảo mật của UE.

Cần hiểu rằng việc kiểm chứng UE theo sáng chế nghĩa là kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký được gửi bởi UE, chẳng hạn, giải mật mã thông điệp yêu cầu đăng ký và/hoặc kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký. Do giả sử rằng tính toàn vẹn của thông điệp yêu cầu đăng ký được kiểm chứng thành công chính là việc thông điệp yêu cầu đăng ký được giải mật mã thành công, theo phương án thực hiện sáng chế, việc UE

được kiểm chứng thành công được mô tả như là việc tính toàn vẹn của thông điệp yêu cầu đăng ký được kiểm chứng thành công.

Dựa vào Fig.3, phần sau mô tả chi tiết phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế. Fig.3 là sơ đồ của phương pháp thu thập ngữ cảnh bảo mật theo phương án thực hiện sáng chế. Sơ đồ bao gồm UE, MME, AMF thứ nhất, và AMF thứ hai.

Phương pháp thu thập ngữ cảnh bảo mật bao gồm các bước sau.

S310: AMF thứ nhất truyền thông điệp yêu cầu thứ hai đến AMF thứ hai.

Thông điệp yêu cầu thứ hai được sử dụng để yêu cầu thu được ngữ cảnh bảo mật của UE. Thông điệp yêu cầu thứ hai mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo rằng UE được kiểm chứng.

Một cách tùy chọn, thông tin chỉ báo có thể được gọi là giá trị nguyên nhân (value).

Cụ thể là, việc AMF thứ nhất xác định rằng UE được kiểm chứng chủ yếu xác định liệu thông điệp yêu cầu đăng ký được nhận từ UE thỏa mãn điều kiện định trước. Cần hiểu rằng, trước khi AMF thứ nhất truyền thông điệp yêu cầu thứ hai đến AMF thứ hai, thủ tục phương pháp được thể hiện trên Fig.3 còn bao gồm các bước từ S311 đến S316.

S311: MME truyền thông điệp chuyển tiếp yêu cầu định vị lại đến AMF thứ nhất. Bước này tương tự với bước S210 trên Fig.2, và chi tiết không được mô tả lại ở đây.

S312: AMF thứ nhất xác định ngữ cảnh bảo mật được ánh xạ. Bước này tương tự với bước S220 trên Fig.2, và chi tiết không được mô tả lại ở đây.

S313: AMF thứ nhất truyền thông điệp đáp ứng chuyển tiếp định vị lại đến MME. Bước này tương tự với bước S230 trên Fig.2, và chi tiết không được mô tả lại ở đây.

S314: MME truyền thông điệp lệnh chuyển vùng đến UE. Bước này tương tự với bước S240 trên Fig.2, và chi tiết không được mô tả lại ở đây.

S315: UE xác định ngữ cảnh bảo mật được ánh xạ. Bước này tương tự với bước S250 trên Fig.2, và chi tiết không được mô tả lại ở đây.

S316: UE truyền thông điệp yêu cầu đăng ký đến AMF thứ nhất. Bước này

tương tự với bước S260 trên Fig.2, và chi tiết không được mô tả lại ở đây.

Ngoài ra, việc AMF thứ nhất xác định rằng thông điệp yêu cầu đăng ký thỏa mãn điều kiện định trước bao gồm:

AMF thứ nhất kiểm chứng thành công bảo vệ tính toàn vẹn cho thông điệp yêu cầu đăng ký; hoặc

AMF thứ nhất xác định rằng thông điệp yêu cầu đăng ký là thông điệp yêu cầu đăng ký được gửi bởi UE sau khi UE được chuyển vùng từ hệ thống truyền thông 4G đến hệ thống truyền thông 5G. Chẳng hạn, trước khi nhận thông điệp yêu cầu đăng ký được gửi bởi UE, AMF thứ nhất nhận thông điệp chuyển tiếp yêu cầu định vị lại được gửi bởi MME. Do vậy, AMF thứ nhất có thể biết rằng thông điệp yêu cầu đăng ký đang được nhận là thông điệp yêu cầu đăng ký được nhận từ UE trong thủ tục chuyển vùng.

Cụ thể là, việc AMF thứ nhất kiểm chứng thành công bảo vệ tính toàn vẹn cho thông điệp yêu cầu đăng ký có thể cũng được gọi là AMF thứ nhất kiểm chứng thành công UE. Nói cách khác, thủ tục phương pháp được thể hiện trên Fig.3 còn bao gồm bước S317 trong đó AMF thứ nhất kiểm chứng UE.

Theo triển khai khả thi, thông điệp yêu cầu thứ hai là yêu cầu gọi dịch vụ truyền ngữ cảnh UE (Namf_Communication_UEContextTransfer) được khởi tạo bởi AMF thứ nhất được thể hiện trên Fig.2. Khác với yêu cầu gọi dịch vụ truyền ngữ cảnh UE được thể hiện trên Fig.2, yêu cầu gọi dịch vụ truyền ngữ cảnh UE theo phương án thực hiện sáng chế bao gồm phần tử thông tin mới được bổ sung (information element, IE), tức là, thông tin chỉ báo.

Theo triển khai khả thi khác, thông điệp yêu cầu thứ hai là thông điệp yêu cầu thứ hai khả thi khác được gửi bởi AMF thứ nhất đến AMF thứ hai và được sử dụng để thu được ngữ cảnh bảo mật của UE.

Cần hiểu rằng dạng cụ thể của thông điệp yêu cầu thứ hai không bị giới hạn theo sáng chế. Thông tin chỉ báo có thể được bổ sung vào báo hiệu hiện có giữa AMF thứ nhất và AMF thứ hai, hoặc có thể được bổ sung vào báo hiệu mới được bổ sung giữa AMF thứ nhất và AMF thứ hai.

Theo triển khai khả thi khác, theo phương án thực hiện sáng chế, bị giới hạn riêng việc AMF thứ nhất cần gửi thông tin chỉ báo đến AMF thứ hai trước khi

gửi yêu cầu gọi dịch vụ truyền ngữ cảnh UE đến AMF thứ hai. Nói cách khác, AMF thứ nhất có thể trực tiếp truyền thông tin chỉ báo đến AMF thứ hai, mà không bổ sung thông tin chỉ báo vào thông điệp yêu cầu thứ hai. Triển khai khả thi này không được thể hiện trên Fig.3.

Cần hiểu thêm rằng cách thức thông tin chỉ báo sẽ chỉ báo cụ thể rằng UE được kiểm chứng không bị giới hạn theo sáng chế. Theo triển khai khả thi, thông tin chỉ báo có thể là 5G-GUTI của UE. Trong trường hợp này, 5G-GUTI có thể được sử dụng để nhận diện UE và chỉ báo rằng UE được kiểm chứng. Theo triển khai này, chức năng chỉ báo mới được bổ sung vào IE hiện tại, và AMF thứ hai có thể được thông báo, theo cách định trước, rằng 5G-GUTI có chức năng mới. Theo triển khai khả thi khác, thông tin chỉ báo có thể là ít nhất một bit mới được thêm vào, và giá trị của bit được gán bằng 1, để chỉ báo rằng UE được kiểm chứng. Các cách triển khai khả thi nêu trên chỉ là ví dụ để mô tả, và không giới hạn bất kỳ ở phạm vi bảo hộ của sáng chế.

Theo triển khai khả thi, thông tin chỉ báo chỉ báo tường minh rằng UE được kiểm chứng. Theo cách khác, Theo triển khai khả thi khác, thông tin chỉ báo ngầm chỉ báo rằng UE được kiểm chứng. Chẳng hạn, thông tin chỉ báo chỉ báo rằng tính toàn vẹn của thông điệp yêu cầu đăng ký được nhận bởi AMF thứ nhất từ UE được kiểm chứng thành công.

Ngoài ra, để AMF thứ hai có thể xác định rằng AMF thứ nhất cần thu được ngữ cảnh bảo mật của UE, thông điệp yêu cầu thứ hai còn cần mang định danh của UE.

Theo triển khai khả thi, định danh của UE có thể là 5G-GUTI nêu trên.

Theo triển khai khả thi khác, định danh của UE có thể là định danh thuê bao dài hạn (subscriber permanent identity, SUPI).

Cần hiểu rằng, nếu AMF thứ nhất xác định, sau khi nhận 5G-GUTI của UE từ UE, rằng ngữ cảnh bảo mật của UE cần thu được từ AMF thứ hai, AMF thứ nhất có thể chọn tiếp tục bổ sung 5G-GUTI của UE, SUPI của UE, hoặc cả 5G-GUTI lẫn SUPI của UE vào thông điệp yêu cầu thứ hai.

Một cách tùy chọn, để AMF thứ hai có thể thu được số đếm tầng không truy nhập liên kết lên (uplink non-access stratum count, UL NAS COUNT) của UE,

Theo triển khai khả thi, thông điệp yêu cầu thứ hai mang thông điệp yêu cầu đăng ký văn bản thuần túy, trong đó thông điệp yêu cầu đăng ký văn bản thuần túy bao gồm UL NAS COUNT; hoặc theo triển khai khả thi, thông điệp yêu cầu thứ hai mang UL NAS COUNT.

Ngoài ra, sau khi nhận thông điệp yêu cầu thứ hai được gửi bởi AMF thứ nhất, AMF thứ hai biết, dựa trên thông tin chỉ báo, rằng UE được kiểm chứng. Trong trường hợp này, AMF thứ hai không cần kiểm chứng UE, nói cách khác, thực hiện bước S320 trong đó AMF thứ hai xác định rằng UE không cần được kiểm chứng.

S330: AMF thứ hai truyền thông điệp đáp ứng thứ hai đến AMF thứ nhất.

Thông điệp đáp ứng thứ hai mang ngữ cảnh bảo mật của UE.

Theo phương án thực hiện sáng chế, AMF thứ hai không cần kiểm chứng UE. Sau khi nhận thông điệp yêu cầu thứ hai được gửi bởi AMF thứ nhất, AMF thứ hai trực tiếp trả về ngữ cảnh bảo mật của UE đến AMF thứ nhất. Điều này tránh trường hợp trong đó AMF thứ nhất không thu được ngữ cảnh bảo mật của UE do AMF thứ hai không kiểm chứng UE.

Một cách tùy chọn, khi thông điệp yêu cầu thứ hai mang thông điệp yêu cầu đăng ký văn bản thuần túy, hoặc thông điệp yêu cầu thứ hai mang UL NAS COUNT, AMF thứ hai có thể thu được UL NAS COUNT. Chẳng hạn, do thông điệp yêu cầu đăng ký văn bản thuần túy là thông điệp yêu cầu đăng ký mà trên đó không thực hiện bảo vệ bảo mật, AMF thứ hai không cần kiểm chứng thông điệp yêu cầu đăng ký văn bản thuần túy, và có thể thu được trực tiếp UL NAS COUNT từ thông điệp yêu cầu đăng ký văn bản thuần túy.

Ngoài ra, AMF thứ hai có thể thực hiện dẫn xuất khóa trên khóa thứ nhất trong ngữ cảnh bảo mật của UE dựa trên UL NAS COUNT. Trong trường hợp này, khóa trong ngữ cảnh bảo mật của UE được trả về bởi AMF thứ hai cho AMF thứ nhất là khóa thứ hai thu được bằng cách thực hiện dẫn xuất khóa trên khóa thứ nhất.

Cụ thể là, khi khóa trong ngữ cảnh bảo mật của UE được gửi bởi AMF thứ hai đến AMF thứ nhất là khóa thứ hai, AMF thứ hai còn cần gửi dẫn xuất khóa thông tin chỉ báo đến AMF thứ nhất, để chỉ báo rằng khóa thứ hai là khóa thu

được qua dẫn xuất khóa.

Cần hiểu rằng thủ tục sau khi AMF thứ nhất thu được ngữ cảnh bảo mật của UE giống như thủ tục sau khi AMF thứ nhất thu được ngữ cảnh bảo mật của UE trong thủ tục hiện tại chuyển vùng UE từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G. Để biết chi tiết, tham khảo thủ tục hiện tại. Chi tiết không được mô tả lại ở đây.

Trong phương pháp thu thập ngữ cảnh bảo mật được thể hiện trên Fig.3, thông điệp yêu cầu thứ hai được gửi bởi AMF thứ nhất đến AMF thứ hai mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo rằng UE được kiểm chứng. Do vậy, AMF thứ hai có thể xác định, dựa trên thông tin chỉ báo, rằng UE được kiểm chứng, và không cần kiểm chứng UE. Sau khi nhận thông điệp yêu cầu thứ hai mang thông tin chỉ báo, AMF thứ hai trả về trực tiếp ngữ cảnh bảo mật của UE cho AMF thứ nhất. Điều này tránh trường hợp trong đó AMF thứ nhất không thu được ngữ cảnh bảo mật của UE do AMF thứ hai không kiểm chứng UE. Sáng chế còn đề cập đến phương pháp thu thập ngữ cảnh bảo mật khác trong đó AMF thứ hai kiểm chứng UE. Tuy nhiên, phương pháp có thể cải thiện khả năng mà AMF thứ hai kiểm chứng thành công UE, nhờ đó cải thiện khả năng mà AMF thứ nhất thu được thành công ngữ cảnh bảo mật của UE từ AMF thứ hai.

Phần sau mô tả chi tiết phương pháp thu thập ngữ cảnh bảo mật dựa vào Fig.4. Fig.4 là sơ đồ của phương pháp thu thập ngữ cảnh bảo mật khác theo phương án thực hiện sáng chế. Sơ đồ bao gồm UE, MME, AMF thứ nhất, và AMF thứ hai.

Phương pháp thu thập ngữ cảnh bảo mật bao gồm các bước sau.

S410: UE xác định thông điệp yêu cầu đăng ký thứ nhất.

Thông điệp yêu cầu đăng ký thứ nhất mang thông điệp yêu cầu đăng ký thứ hai. Thông điệp yêu cầu đăng ký thứ hai được bảo vệ tính toàn vẹn nhờ sử dụng ngữ cảnh bảo mật thứ nhất, và ngữ cảnh bảo mật thứ nhất là ngữ cảnh bảo mật nguyên gốc (native) giữa UE và AMF thứ hai.

Cụ thể là, việc UE xác định thông điệp yêu cầu đăng ký thứ nhất chủ yếu xác định thông điệp yêu cầu đăng ký thứ hai. Thông điệp yêu cầu đăng ký thứ

hai là thông điệp thu được sau khi UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư nhờ sử dụng ngữ cảnh bảo mật nguyên gốc. Thông điệp yêu cầu đăng ký thứ tư bao gồm GUTI, thông tin định danh khóa (ngKSI), và UL NAS COUNT nằm trong ngữ cảnh của UE giữa UE và AMF thứ hai. Để dễ phân biệt, GUTI có thể được gọi là GUTI nguyên thủy, và định danh khóa có thể được gọi là định danh khóa nguyên thủy.

Một cách tùy chọn, thông điệp yêu cầu đăng ký thứ tư có thể có vài trường hợp khả thi sau:

Trường hợp 1:

Thông điệp yêu cầu đăng ký thứ tư là thông điệp được tạo bởi UE dựa trên GUTI nguyên gốc, định danh khóa nguyên gốc, và UL NAS COUNT. Trong trường hợp 1, thông điệp yêu cầu đăng ký thứ tư có thể cũng được gọi là thông điệp thứ tư hoặc có thể có tên khả thi khác. Tên của thông điệp không bị giới hạn theo phương án thực hiện sáng chế.

Cần hiểu rằng thông điệp yêu cầu đăng ký thứ tư được tạo bởi UE dựa trên ngữ cảnh của UE nằm giữa UE và AMF thứ hai có thể theo cách khác ở dạng khác. Chẳng hạn, bên cạnh GUTI nguyên gốc, định danh khóa nguyên gốc, và UL NAS COUNT, thông điệp yêu cầu đăng ký thứ tư được tạo bởi UE còn bao gồm phần tử thông tin (information element, IE) khác.

Trong trường hợp 1, việc UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư dựa trên ngữ cảnh bảo mật thứ nhất bao gồm: UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư dựa trên ngữ cảnh bảo mật thứ nhất, và tạo MAC thứ nhất. Do vậy, mang thông điệp yêu cầu đăng ký thứ hai trong thông điệp yêu cầu đăng ký thứ nhất cũng có thể được hiểu là mang MAC thứ nhất và thông điệp yêu cầu đăng ký thứ tư trong thông điệp yêu cầu đăng ký thứ nhất.

Ngoài ra, trong trường hợp 1, việc UE xác định thông điệp yêu cầu đăng ký thứ nhất bao gồm các bước sau:

Bước 1:

UE tạo thông điệp yêu cầu đăng ký thứ tư.

Bước 2:

UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư dựa trên ngữ cảnh bảo mật giữa UE và AMF thứ hai, và tạo MAC thứ nhất.

Bước 3:

UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ ba và thông điệp yêu cầu đăng ký thứ hai (RR2) dựa trên ngữ cảnh bảo mật được ánh xạ giữa UE và AMF thứ nhất, và tạo MAC thứ năm. Thông điệp yêu cầu đăng ký thứ ba là thông điệp yêu cầu đăng ký được gửi bởi UE đến AMF thứ nhất trong thủ tục phương pháp S260 được thể hiện trên Fig.2. Cụ thể là, thông điệp yêu cầu đăng ký thứ ba bao gồm GUTI và thông tin định danh khóa nằm trong ngữ cảnh được ánh xạ giữa UE và AMF thứ nhất. Để dễ phân biệt, GUTI có thể được gọi là GUTI được ánh xạ, và định danh khóa có thể được gọi là định danh khóa được ánh xạ.

Trong trường hợp này, thông điệp yêu cầu đăng ký thứ nhất bao gồm thông điệp yêu cầu đăng ký thứ tư (RR4), thông điệp yêu cầu đăng ký thứ ba (RR3), MAC thứ năm (MAC5), và MAC thứ nhất (MAC1). MAC1 là giá trị MAC thu được bằng cách thực hiện bảo vệ tính toàn vẹn trên RR4 nhờ sử dụng ngữ cảnh bảo mật nguyên gốc. MAC5 là giá trị MAC thu được bằng cách thực hiện bảo vệ tính toàn vẹn trên RR3 và RR2 nhờ sử dụng ngữ cảnh bảo mật được ánh xạ (hoặc MAC5 là giá trị MAC thu được bằng cách thực hiện bảo vệ tính toàn vẹn trên RR3, RR4, và MAC1 nhờ sử dụng ngữ cảnh bảo mật được ánh xạ). Cũng có thể hiểu rằng thông điệp yêu cầu đăng ký thứ nhất là thông điệp trên đó bảo vệ tính toàn vẹn được thực hiện tuần tự dựa trên ngữ cảnh bảo mật nguyên gốc và ngữ cảnh bảo mật được ánh xạ.

Trường hợp 2:

Thông điệp yêu cầu đăng ký thứ tư là thông điệp yêu cầu đăng ký thu được sau khi UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ ba dựa trên ngữ cảnh bảo mật được ánh xạ.

Trong trường hợp 2, việc UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư dựa trên ngữ cảnh bảo mật thứ nhất bao gồm: UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư dựa trên ngữ cảnh bảo mật thứ nhất, và tạo MAC thứ nhất. Do vậy, mang thông điệp yêu cầu

đăng ký thứ hai trong thông điệp yêu cầu đăng ký thứ nhất có thể cũng được hiểu là mang MAC thứ nhất và thông điệp yêu cầu đăng ký thứ tư trong thông điệp yêu cầu đăng ký thứ nhất.

Ngoài ra, trong trường hợp 2, việc UE xác định thông điệp yêu cầu đăng ký thứ nhất bao gồm các bước sau:

Bước 1:

UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ ba dựa trên ngữ cảnh bảo mật được ánh xạ giữa UE và AMF thứ nhất, và tạo MAC thứ ba.

Bước 2:

UE thực hiện, dựa trên ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai, bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ ba trên đó bảo vệ tính toàn vẹn được thực hiện dựa trên ngữ cảnh bảo mật được ánh xạ ở bước 1, và tạo MAC thứ nhất.

Trong trường hợp này, thông điệp yêu cầu đăng ký thứ nhất bao gồm thông điệp yêu cầu đăng ký thứ ba (RR3), MAC thứ ba (MAC3), và MAC thứ nhất (MAC1). MAC3 là giá trị MAC thu được bằng cách thực hiện bảo vệ tính toàn vẹn trên RR3 nhờ sử dụng ngữ cảnh bảo mật được ánh xạ. MAC1 là giá trị MAC thu được bằng cách thực hiện bảo vệ tính toàn vẹn trên RR3 và MAC3 nhờ sử dụng ngữ cảnh bảo mật nguyên gốc. Cũng có thể hiểu rằng thông điệp yêu cầu đăng ký thứ nhất là thông điệp trên đó bảo vệ tính toàn vẹn được thực hiện tuần tự dựa trên ngữ cảnh bảo mật được ánh xạ và ngữ cảnh bảo mật nguyên gốc.

Trường hợp 3:

Thông điệp yêu cầu đăng ký thứ tư là thông điệp yêu cầu đăng ký thứ ba. Thông điệp yêu cầu đăng ký thứ ba là thông điệp yêu cầu đăng ký được gửi bởi UE đến AMF thứ nhất ở thủ tục phương pháp S260 được thể hiện trên Fig.2.

Trong trường hợp 3, việc UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư dựa trên ngữ cảnh bảo mật thứ nhất bao gồm: UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ tư dựa trên ngữ cảnh bảo mật thứ nhất, và tạo MAC thứ nhất. Do vậy, việc mang thông điệp

yêu cầu đăng ký thứ hai trong thông điệp yêu cầu đăng ký thứ nhất có thể cũng được hiểu là mang MAC thứ nhất và thông điệp yêu cầu đăng ký thứ tư in thông điệp yêu cầu đăng ký thứ nhất.

Ngoài ra, trong trường hợp 3, việc UE xác định thông điệp yêu cầu đăng ký thứ nhất bao gồm các bước sau:

Bước 1:

UE thực hiện bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ ba dựa trên ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai, và tạo MAC thứ nhất.

Bước 2:

UE thực hiện, dựa trên ngữ cảnh bảo mật được ánh xạ giữa UE và AMF thứ nhất, bảo vệ tính toàn vẹn trên thông điệp yêu cầu đăng ký thứ ba trên đó bảo vệ tính toàn vẹn được thực hiện dựa trên ngữ cảnh bảo mật nguyên gốc ở bước 1, và tạo MAC thứ tư.

Trong trường hợp này, thông điệp yêu cầu đăng ký thứ nhất bao gồm thông điệp yêu cầu đăng ký thứ ba (RR3), MAC thứ nhất (MAC1), và MAC thứ tư (MAC4). MAC1 là giá trị MAC thu được bằng cách thực hiện bảo vệ tính toàn vẹn trên RR3 nhờ sử dụng ngữ cảnh bảo mật nguyên gốc. MAC4 là giá trị MAC thu được bằng cách thực hiện bảo vệ tính toàn vẹn trên RR3 và MAC1 nhờ sử dụng ngữ cảnh bảo mật được ánh xạ. Cũng có thể được hiểu là thông điệp yêu cầu đăng ký thứ nhất là thông điệp trên đó bảo vệ tính toàn vẹn được thực hiện tuần tự dựa trên ngữ cảnh bảo mật nguyên gốc và ngữ cảnh bảo mật được ánh xạ.

Cần hiểu rằng, trong trường hợp 1, AMF thứ nhất có thể xác định, dựa trên cả GUITI được ánh xạ lẫn GUTI nguyên gốc được mang trong thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE, để truyền thông điệp yêu cầu đăng ký thứ hai được bảo vệ tính toàn vẹn nhờ sử dụng ngữ cảnh bảo mật nguyên gốc đến AMF thứ hai.

Cần hiểu thêm rằng trường hợp 1 đến trường hợp 3 nêu trên chỉ là các ví dụ để mô tả các trường hợp khả thi của thông điệp yêu cầu đăng ký thứ hai và cách thức UE xác định thông điệp yêu cầu đăng ký thứ nhất. Dạng khả thi

không được mô tả khác của yêu cầu đăng ký thứ hai cũng nằm trong phạm vi bảo hộ của sáng chế. Chẳng hạn, thông điệp yêu cầu đăng ký thứ tư là thông điệp khả thi khác được tạo bởi UE dựa trên ngữ cảnh nguyên gốc.

S420: UE truyền thông điệp yêu cầu đăng ký thứ nhất đến AMF thứ nhất.

Cụ thể là, UE truyền thông điệp yêu cầu đăng ký thứ nhất được xác định ở bước S410 đến AMF thứ nhất.

Cần hiểu rằng thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE đến AMF thứ nhất có thể được chuyển tiếp bởi thiết bị mạng truy nhập. Chức năng của thiết bị mạng truy nhập không bị giới hạn theo sáng chế. Do vậy, việc thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE đến AMF thứ nhất có thể được chuyển tiếp bởi thiết bị mạng truy nhập được mô tả trực tiếp như là việc UE truyền thông điệp yêu cầu đăng ký thứ nhất đến AMF thứ nhất.

Cần hiểu thêm rằng, trước khi UE truyền thông điệp yêu cầu đăng ký thứ nhất đến AMF thứ nhất, UE cần xác định ngữ cảnh bảo mật được ánh xạ. Do vậy, trước khi UE truyền thông điệp yêu cầu đăng ký thứ nhất đến AMF thứ nhất, thủ tục phương pháp được thể hiện trên Fig.4 còn bao gồm các bước từ S411 đến S414.

S411: MME truyền thông điệp chuyển tiếp yêu cầu định vị lại đến AMF thứ nhất. Bước này tương tự với S210 trên Fig.2, và chi tiết không được mô tả lại ở đây.

S412: AMF thứ nhất xác định ngữ cảnh bảo mật được ánh xạ. Bước này tương tự với S220 trên Fig.2, và chi tiết không được mô tả lại ở đây.

S413: AMF thứ nhất truyền thông điệp đáp ứng chuyển tiếp định vị lại đến MME. Bước này tương tự với S230 trên Fig.2, và chi tiết không được mô tả lại ở đây.

S414: MME truyền thông điệp lệnh chuyển vùng đến UE. Bước này tương tự với S240 trên Fig.2, và chi tiết không được mô tả lại ở đây.

Cụ thể là, sau khi nhận thông điệp lệnh chuyển vùng, UE dẫn xuất ngữ cảnh bảo mật được ánh xạ. Ngoài ra, UE thực hiện bảo vệ bảo mật trên thông điệp yêu cầu đăng ký thứ nhất nhờ sử dụng ngữ cảnh bảo mật nguyên gốc và ngữ cảnh bảo mật được ánh xạ.

S430: AMF thứ nhất kiểm chứng UE.

Cụ thể là, việc AMF thứ nhất xác định rằng UE được kiểm chứng chủ yếu xác định liệu thông điệp yêu cầu đăng ký thứ nhất được nhận từ UE thỏa mãn điều kiện định trước. Việc AMF thứ nhất xác định việc thông điệp yêu cầu đăng ký thứ nhất thỏa mãn điều kiện định trước bao gồm:

AMF thứ nhất kiểm chứng thành công bảo vệ tính toàn vẹn cho thông điệp yêu cầu đăng ký thứ nhất dựa trên ngữ cảnh bảo mật được ánh xạ; hoặc

AMF thứ nhất xác định rằng thông điệp yêu cầu đăng ký thứ nhất là thông điệp yêu cầu đăng ký được gửi bởi UE sau khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G. Chẳng hạn, trước khi nhận thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE, AMF thứ nhất nhận thông điệp chuyển tiếp yêu cầu định vị lại được gửi bởi MME. Do vậy, AMF thứ nhất có thể biết rằng thông điệp yêu cầu đăng ký thứ nhất đang được nhận là thông điệp yêu cầu đăng ký được nhận từ UE trong thủ tục chuyển vùng.

Sau khi kiểm chứng rằng UE được kiểm chứng, AMF thứ nhất truyền thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai, trong đó thông điệp yêu cầu đăng ký thứ hai được sử dụng bởi AMF thứ hai để kiểm chứng UE. Nói cách khác, thủ tục phương pháp được thể hiện trên Fig.4 còn bao gồm bước S440 trong đó AMF thứ nhất truyền thông điệp yêu cầu thứ hai đến AMF thứ hai.

Một cách tùy chọn, thông điệp yêu cầu đăng ký thứ hai được mang trong thông điệp yêu cầu thứ nhất, và được gửi bởi AMF thứ nhất đến AMF thứ hai.

Theo triển khai khả thi, thông điệp yêu cầu thứ nhất là yêu cầu gọi dịch vụ truyền ngữ cảnh UE (Namf_Communication_UEContextTransfer) được khởi tạo bởi AMF thứ nhất được thể hiện trên Fig.2. Khác với yêu cầu gọi dịch vụ truyền ngữ cảnh UE được thể hiện trên Fig.2, yêu cầu gọi dịch vụ truyền ngữ cảnh UE theo phương án thực hiện sáng chế bao gồm IE mới được bổ sung, tức là, MAC thứ nhất.

Theo triển khai khả thi khác, thông điệp yêu cầu thứ nhất là thông điệp yêu cầu thứ nhất khả thi khác được gửi bởi AMF thứ nhất đến AMF thứ hai và được sử dụng để thu được ngữ cảnh bảo mật của UE.

Cần hiểu rằng dạng cụ thể của thông điệp yêu cầu thứ nhất không bị giới hạn in sáng chế. MAC thứ nhất có thể được bổ sung vào báo hiệu hiện có giữa AMF thứ nhất và AMF thứ hai, hoặc có thể được bổ sung vào báo hiệu mới được bổ sung giữa AMF thứ nhất và AMF thứ hai.

Ngoài ra, để AMF thứ hai có thể xác định rằng AMF thứ nhất cần thu được ngữ cảnh bảo mật của UE, thông điệp yêu cầu thứ nhất còn mang định danh của UE. Cụ thể là, định danh của UE được bao gồm trong thông điệp yêu cầu đăng ký thứ hai được gửi bởi AMF thứ nhất đến AMF thứ hai.

Theo triển khai khả thi, định danh của UE có thể là GUTI được ánh xạ.

Theo triển khai khả thi, định danh của UE có thể là GUTI nguyên gốc.

Theo triển khai khả thi khác, định danh của UE có thể là SUPI.

Cần hiểu rằng, nếu AMF thứ nhất xác định, sau khi nhận GUTI được ánh xạ của UE từ UE, rằng ngữ cảnh bảo mật của UE cần thu được từ AMF thứ hai, AMF thứ nhất có thể chọn tiếp tục bổ sung GUTI được ánh xạ của UE, SUPI của UE, hoặc cả GUTI được ánh xạ và SUPI của UE vào thông điệp yêu cầu thứ nhất.

Cần hiểu thêm rằng, khi thông điệp yêu cầu đăng ký thứ nhất được nhận bởi AMF thứ nhất là thông điệp yêu cầu đăng ký thứ nhất được thể hiện trong trường hợp 1 ở bước S410, thông điệp yêu cầu đăng ký thứ nhất mang thông điệp yêu cầu đăng ký thứ hai, và thông điệp yêu cầu đăng ký thứ hai bao gồm GUTI nguyên gốc. Trong trường hợp này, AMF thứ nhất có thể chọn bổ sung GUTI nguyên gốc của UE vào thông điệp yêu cầu thứ nhất.

Ngoài ra, thông điệp yêu cầu đăng ký thứ hai còn bao gồm UL NAS COUNT của UE, sao cho AMF thứ hai có thể nhận UL NAS COUNT của UE.

Ngoài ra, sau khi nhận thông điệp yêu cầu thứ nhất được gửi bởi AMF thứ nhất, AMF thứ hai xác định, dựa trên kết quả kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, liệu UE được kiểm chứng. Cụ thể là, AMF thứ hai thực hiện bước S450, nói cách khác, kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai.

AMF thứ hai kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai dựa trên ngữ cảnh bảo mật giữa AMF thứ hai và UE. Chẳng hạn, AMF thứ

hai tạo MAC thứ hai dựa trên ngữ cảnh bảo mật được lưu trữ nguyên gốc, và so sánh MAC thứ nhất với MAC thứ hai. Khi MAC thứ nhất bằng MAC thứ hai, AMF thứ hai kiểm chứng thành công UE, và xác định rằng UE được kiểm chứng. Trong trường hợp này, AMF thứ hai truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất.

Cần hiểu rằng MAC thứ nhất là MAC được tạo bởi UE dựa trên ngữ cảnh bảo mật của UE được thỏa hiệp giữa UE và AMF thứ hai, và MAC thứ hai là MAC được tạo bởi AMF thứ hai dựa trên ngữ cảnh bảo mật của UE được thỏa hiệp giữa UE và AMF thứ hai. Do vậy, có xác suất cao là MAC thứ nhất bằng MAC thứ hai. Trong trường hợp này, AMF thứ hai có thể kiểm chứng thành công UE, và trả về ngữ cảnh bảo mật của UE cho AMF thứ nhất, trừ khi AMF thứ hai không kiểm chứng UE do sự kiện có xác suất thấp, chẳng hạn, sai số truyền. So với thủ tục phương pháp được thể hiện trên Fig.2, phương pháp thu thập ngữ cảnh bảo mật được thể hiện trên Fig.4 cải thiện khả năng là AMF thứ nhất thu được thành công ngữ cảnh bảo mật của UE từ AMF thứ hai.

Sau khi kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ hai thực hiện S460, nói cách khác, truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất.

Một cách tùy chọn, ngữ cảnh bảo mật của UE được mang trong thông điệp đáp ứng thứ nhất.

Ngoài ra, nếu ngữ cảnh bảo mật của UE được bao gồm trong ngữ cảnh của UE, AMF thứ hai có thể truyền ngữ cảnh của UE đến AMF thứ nhất.

Một cách tùy chọn, AMF thứ hai can thực hiện dẫn xuất khóa trên khóa thứ nhất trong ngữ cảnh bảo mật của UE dựa trên UL NAS COUNT. Trong trường hợp này, khóa trong ngữ cảnh bảo mật của UE được trả về bởi AMF thứ hai cho AMF thứ nhất là khóa thứ hai thu được bằng cách thực hiện dẫn xuất khóa trên khóa thứ nhất. Theo phương án thực hiện sáng chế, ngữ cảnh bảo mật của UE bao gồm khóa thứ hai được tạo qua dẫn xuất khóa có thể được gọi là ngữ cảnh bảo mật thứ hai. Nói cách khác, ngữ cảnh bảo mật của UE được gửi bởi AMF thứ hai đến AMF thứ nhất có thể không thực hiện dẫn xuất khóa, có thể là ngữ cảnh bảo mật của UE nằm giữa AMF thứ hai và UE và được lưu trữ

nguyên gốc trong AMF thứ hai, hoặc có thể là ngữ cảnh bảo mật thứ hai khi AMF thứ hai thực hiện, theo chính sách cục bộ, dẫn xuất khóa trên khóa trong ngữ cảnh bảo mật được lưu trữ nguyên gốc của UE giữa AMF thứ hai và UE, để tạo khóa được dẫn xuất.

Cụ thể là, khi khóa trong ngữ cảnh bảo mật của UE được gửi bởi AMF thứ hai đến AMF thứ nhất là khóa thứ hai, AMF thứ hai còn cần gửi thông tin chỉ báo dẫn xuất khóa đến AMF thứ nhất, để chỉ báo rằng khóa thứ hai là khóa thu được qua dẫn xuất khóa.

Cần hiểu rằng thủ tục sau khi AMF thứ nhất thu được ngữ cảnh bảo mật của UE giống như thủ tục sau khi AMF thứ nhất thu được ngữ cảnh bảo mật của UE trong thủ tục hiện tại chuyển vùng UE từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G. Để biết chi tiết, tham khảo thủ tục hiện tại. Chi tiết không được mô tả lại ở đây.

Chẳng hạn, UE và AMF thứ nhất lần lượt thỏa hiệp để sử dụng ngữ cảnh bảo mật nguyên gốc. Cụ thể là, AMF thứ nhất truyền thông điệp NAS SMC (non-access stratum secure mode command, NAS SMC) đến UE, và UE kiểm chứng tính toàn vẹn của thông điệp NAS SMC. Sau khi UE kiểm chứng thành công thông điệp NAS SMC, UE truyền thông điệp hoàn thành chế độ bảo mật tầng không truy nhập (non-access layer security mode complete) đến AMF thứ nhất.

Theo triển khai khả thi, khi AMF thứ hai không kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ hai truyền thông tin chỉ báo sự cố đến AMF thứ nhất, để thông báo AMF thứ nhất rằng AMF thứ hai không kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai.

Ngoài ra, sau khi AMF thứ nhất nhận thông tin chỉ báo sự cố chỉ báo rằng AMF thứ hai không kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, AMF thứ nhất xác định, theo chính sách nội bộ, rằng AMF thứ nhất có thể tiếp tục sử dụng ngữ cảnh bảo mật được ánh xạ, hoặc AMF thứ nhất xác định khởi tạo xác thực ban đầu đến UE theo chính sách nội bộ, và tạo ngữ cảnh bảo mật mới giữa AMF thứ nhất và UE.

Cần hiểu rằng các số thứ tự của các tiến trình nêu trên không phải là các

trình tự thực thi theo các phương án thực hiện phương pháp nêu trên. Các trình tự thực thi của các tiến trình nên được xác định dựa trên các chức năng và lôgic bên trong của các tiến trình, và không nên được hiểu như là giới hạn bất kỳ ở các tiến trình triển khai của các phương án thực hiện sáng chế.

Phương pháp thu thập các ngữ cảnh bảo mật theo các phương án thực hiện sáng chế được mô tả chi tiết nêu trên dựa vào Fig.3 và Fig.4. Phần sau mô tả chi tiết các thiết bị thu thập ngữ cảnh bảo mật theo các phương án thực hiện sáng chế dựa vào các hình vẽ từ Fig.5 đến Fig.10.

Fig.5 là sơ đồ của thiết bị thu thập ngữ cảnh bảo mật 50 theo sáng chế. Như được thể hiện trên Fig.5, thiết bị 50 bao gồm khối gửi 510, khối xử lý 520, và khối nhận 530.

Khối gửi 510 được tạo cấu hình để gửi thông điệp yêu cầu đăng ký thứ nhất đến AMF thứ nhất.

Khối xử lý 520 được tạo cấu hình để xác định thông điệp yêu cầu đăng ký thứ nhất.

Khối nhận 530 được tạo cấu hình để nhận thông điệp lệnh chuyển vùng được gửi bởi MME.

Thiết bị 50 hoàn toàn tương ứng với UE theo các phương án thực hiện phương pháp. Thiết bị 50 có thể là UE theo các phương án thực hiện phương pháp, hoặc chip hoặc môđun chức năng bên trong UE theo các phương án thực hiện phương pháp. Các khối tương ứng của thiết bị 50 được tạo cấu hình để thực hiện các bước tương ứng được thực hiện bởi UE theo các phương án thực hiện phương pháp được thể hiện trên Fig.3 và Fig.4.

Khối gửi 510 của thiết bị 50 thực hiện bước gửi được thực hiện bởi UE theo các phương án thực hiện phương pháp. Chẳng hạn, khối gửi 510 thực hiện bước S316 gửi thông điệp yêu cầu đăng ký đến AMF thứ nhất trên Fig.3 và bước S420 gửi thông điệp yêu cầu đăng ký thứ nhất đến AMF thứ nhất trên Fig.4.

Khối xử lý 520 thực hiện bước được triển khai hoặc xử lý bên trong UE theo các phương án thực hiện phương pháp. Chẳng hạn, khối xử lý 520 thực hiện bước S315 xác định ngữ cảnh bảo mật được ánh xạ trên Fig.3 và bước

S410 xác định thông điệp yêu cầu đăng ký thứ nhất trên Fig.4.

Khối nhận 530 thực hiện bước nhận được thực hiện bởi UE theo các phương án thực hiện phương pháp. Chẳng hạn, khối nhận 530 thực hiện bước S314 nhận thông điệp lệnh chuyển vùng được gửi bởi MME trên Fig.3 và bước S414 nhận thông điệp lệnh chuyển vùng được gửi bởi MME trên Fig.4.

Khối gửi 510 và khối nhận 530 được thể hiện trên thiết bị 50 có thể tạo khối thu phát đều có chức năng nhận và gửi. Khối xử lý 520 có thể là bộ xử lý. Khối gửi 510 có thể là bộ truyền, và khối nhận 530 có thể là bộ nhận. Bộ nhận và bộ truyền có thể được tích hợp để tạo bộ thu phát.

Fig.6 là sơ đồ cấu trúc của UE 60 có thể áp dụng cho phương án thực hiện sáng chế. UE 60 có thể được áp dụng cho hệ thống được thể hiện trên Fig.1. Để dễ mô tả, Fig.6 thể hiện chỉ các thành phần chính của UE. Như được thể hiện trên Fig.6, UE 60 bao gồm bộ xử lý (tương ứng với khối xử lý 520 trên Fig.5), bộ nhớ, mạch điều khiển, anten, và bộ phận nhập/xuất (input/output, I/O) (tương ứng với khối gửi 510 và khối nhận 530 trên Fig.5). Bộ xử lý được tạo cấu hình để điều khiển anten và bộ phận I/O để truyền và nhận tín hiệu. Bộ nhớ được tạo cấu hình để lưu trữ chương trình máy tính. Bộ xử lý được tạo cấu hình để gọi chương trình máy tính từ bộ nhớ và chạy chương trình máy tính, để thực hiện thủ tục và/hoặc hoạt động tương ứng được thực hiện bởi UE ở các phương pháp thu thập ngữ cảnh bảo mật theo sáng chế. Chi tiết không được mô tả lại ở đây.

Người có hiểu biết trung bình trong lĩnh vực có thể hiểu rằng, để dễ mô tả, Fig.6 thể hiện chỉ một bộ nhớ và chỉ một bộ xử lý. UE thực có thể có các bộ xử lý và các bộ nhớ. Bộ nhớ có thể cũng được gọi là phương tiện lưu trữ, thiết bị lưu trữ, hoặc tương tự. Điều này không bị giới hạn ở phương án thực hiện sáng chế.

Fig.7 là sơ đồ của thiết bị thu thập ngữ cảnh bảo mật 70 theo sáng chế. Như được thể hiện trên Fig.7, thiết bị 70 bao gồm khối nhận 710, khối xử lý 720, và khối gửi 730.

Khối nhận 710 được tạo cấu hình để nhận thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE, trong đó thông điệp yêu cầu đăng ký thứ nhất mang

thông điệp yêu cầu đăng ký thứ hai, thông điệp yêu cầu đăng ký thứ hai được bảo vệ tính toàn vẹn nhờ sử dụng ngữ cảnh bảo mật thứ nhất, ngữ cảnh bảo mật thứ nhất là ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai, và AMF thứ nhất là AMF cấp dịch vụ quản lý di động và truy nhập cho UE sau khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G.

Khối xử lý 720 được tạo cấu hình để xác định ngữ cảnh bảo mật được ánh xạ.

Khối gửi 730 được tạo cấu hình để gửi thông điệp yêu cầu đăng ký thứ hai to AMF thứ hai.

Thiết bị 70 hoàn toàn tương ứng với AMF thứ nhất theo các phương án thực hiện phương pháp. Thiết bị 70 có thể là AMF thứ nhất theo các phương án thực hiện phương pháp, hoặc chip hoặc môđun chức năng bên trong AMF thứ nhất theo các phương án thực hiện phương pháp. Các khối tương ứng của thiết bị 70 được tạo cấu hình để thực hiện các bước tương ứng được thực hiện bởi AMF thứ nhất theo các phương án thực hiện phương pháp được thể hiện trên Fig.3 và Fig.4.

Khối nhận 710 của thiết bị 70 thực hiện bước nhận được thực hiện bởi AMF thứ nhất theo các phương án thực hiện phương pháp. Chẳng hạn, khối nhận 710 thực hiện bước S311 nhận thông điệp chuyển tiếp yêu cầu định vị lại được gửi bởi MME trên Fig.3, bước S411 nhận thông điệp chuyển tiếp yêu cầu định vị lại được gửi bởi MME trên Fig.4, bước S316 nhận thông điệp yêu cầu đăng ký được gửi bởi UE trên Fig.3, bước S420 nhận thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE trên Fig.3, bước S330 nhận thông điệp đáp ứng thứ hai được gửi bởi AMF thứ hai trên Fig.3, và bước S460 nhận ngữ cảnh bảo mật của UE được gửi bởi AMF thứ hai trên Fig.4.

Khối xử lý 720 thực hiện bước được triển khai hoặc xử lý bên trong AMF thứ nhất theo các phương án thực hiện phương pháp. Chẳng hạn, khối xử lý 720 thực hiện bước S312 xác định ngữ cảnh bảo mật được ánh xạ trên Fig.3, bước S412 xác định ngữ cảnh bảo mật được ánh xạ trên Fig.4, bước S317 kiểm chứng UE trên Fig.3, và bước S430 kiểm chứng UE trên Fig.4.

Khối gửi 730 thực hiện bước gửi được thực hiện bởi AMF thứ nhất theo các

phương án thực hiện phương pháp. Chẳng hạn, khối gửi 730 thực hiện bước S313 gửi thông điệp chuyển tiếp đáp ứng định vị lại đến MME trên Fig.3, bước S413 gửi thông điệp chuyển tiếp đáp ứng định vị lại đến MME trên Fig.4, bước S310 gửi thông điệp yêu cầu thứ hai đến AMF thứ hai trên Fig.3, và bước S440 gửi thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai trên Fig.4.

Khối nhận 710 và khối gửi 730 có thể tạo thành khối thu phát có cả chức năng thu và phát. Khối xử lý 720 có thể là bộ xử lý. Khối gửi 730 có thể là bộ phát. Khối nhận 710 có thể là bộ thu. Bộ thu và bộ phát có thể được tích hợp để tạo bộ thu phát.

Như được thể hiện trên Fig.8, phương án thực hiện sáng chế còn đề cập đến AMF thứ nhất 80. AMF thứ nhất 80 bao gồm bộ xử lý 810, bộ nhớ 820, và bộ thu phát 830. Bộ nhớ 820 lưu trữ lệnh hoặc chương trình, và bộ xử lý 830 được tạo cấu hình để thực thi lệnh hoặc chương trình được lưu trữ trong bộ nhớ 820. Khi lệnh hoặc chương trình được lưu trữ trong bộ nhớ 820 được thực thi, bộ thu phát 830 được tạo cấu hình để thực hiện các hoạt động được thực hiện bởi khối nhận 710 và khối gửi 730 trong thiết bị 70 được thể hiện trên Fig.7.

Fig.9 là sơ đồ của thiết bị thu thập ngữ cảnh bảo mật 90 theo sáng chế. Như được thể hiện trên Fig.9, thiết bị 90 bao gồm khối nhận 910, khối xử lý 920, và khối gửi 930.

Khối nhận 910 được tạo cấu hình để nhận thông điệp yêu cầu đăng ký thứ hai được gửi bởi AMF thứ nhất, trong đó thông điệp yêu cầu đăng ký thứ hai được bảo vệ tính toàn vẹn nhờ sử dụng ngữ cảnh bảo mật thứ nhất, và ngữ cảnh bảo mật thứ nhất là ngữ cảnh bảo mật nguyên gốc giữa UE và AMF thứ hai.

Khối xử lý 920 được tạo cấu hình để kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai.

Khối gửi 930 được tạo cấu hình để: khi khối xử lý 920 kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai, truyền ngữ cảnh bảo mật của UE đến AMF thứ nhất.

Thiết bị 90 hoàn toàn tương ứng với AMF thứ hai theo các phương án thực hiện phương pháp. Thiết bị 90 có thể là AMF thứ hai theo các phương án thực hiện phương pháp, hoặc chip hoặc môđun chức năng bên trong AMF thứ hai

theo các phương án thực hiện phương pháp. Các khối tương ứng của thiết bị 90 được tạo cấu hình để thực hiện các bước tương ứng được thực hiện bởi AMF thứ hai theo các phương án thực hiện phương pháp được thể hiện trên Fig.3 và Fig.4.

Khối nhận 910 của thiết bị 90 thực hiện bước nhận được thực hiện bởi AMF thứ hai theo các phương án thực hiện phương pháp. Chẳng hạn, khối nhận 910 thực hiện bước S310 nhận thông điệp yêu cầu thứ hai được gửi bởi AMF thứ nhất trên Fig.3 và bước S440 nhận thông điệp yêu cầu đăng ký thứ hai được gửi bởi AMF thứ nhất trên Fig.4.

Khối xử lý 920 thực hiện bước được triển khai hoặc xử lý bên trong AMF thứ hai theo các phương án thực hiện phương pháp. Chẳng hạn, khối xử lý 920 thực hiện bước S320 xác định rằng UE không cần được kiểm chứng trên Fig.3 và bước S450 kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai trên Fig.4.

Khối gửi 930 thực hiện bước gửi được thực hiện bởi AMF thứ hai theo các phương án thực hiện phương pháp. Chẳng hạn, khối gửi 930 thực hiện bước S330 gửi thông điệp đáp ứng thứ hai đến AMF thứ nhất trên Fig.3 và bước S460 gửi ngữ cảnh bảo mật của UE đến AMF thứ nhất trên Fig.4.

Khối nhận 910 và khối gửi 930 có thể tạo khối thu phát có cả chức năng thu và phát. Khối xử lý 920 có thể là bộ xử lý. Khối gửi 930 có thể là bộ phát, và khối nhận 910 có thể là bộ thu. Bộ thu và bộ phát có thể được tích hợp để tạo bộ thu phát.

Như được thể hiện trên Fig.10, phương án thực hiện sáng chế còn đề cập đến AMF thứ hai 100. AMF thứ hai 100 bao gồm bộ xử lý 1010, bộ nhớ 1020, và bộ thu phát 1030. Bộ nhớ 1020 lưu trữ lệnh hoặc chương trình, và bộ xử lý 1030 được tạo cấu hình để thực thi lệnh hoặc chương trình được lưu trữ trong bộ nhớ 1020. Khi lệnh hoặc chương trình được lưu trữ trong bộ nhớ 1020 được thực thi, bộ thu phát 1030 được tạo cấu hình để thực hiện các hoạt động được thực hiện bởi khối nhận 910 và khối gửi 930 trên thiết bị 90 được thể hiện trên Fig.9.

Phương án thực hiện sáng chế còn đề cập đến phương tiện lưu trữ máy tính

đọc được. Phương tiện lưu trữ máy tính đọc được lưu trữ lệnh. Khi lệnh được chạy trên máy tính, máy tính có thể thực hiện các bước được thực hiện bởi AMF thứ nhất trong các phương pháp được thể hiện trên Fig.3 và Fig.4.

Phương án thực hiện sáng chế còn đề cập đến phương tiện lưu trữ máy tính đọc được. Phương tiện lưu trữ máy tính đọc được lưu trữ lệnh. Khi lệnh được chạy trên máy tính, máy tính có thể thực hiện các bước được thực hiện bởi AMF thứ hai ở các phương pháp được thể hiện trên Fig.3 và Fig.4.

Phương án thực hiện sáng chế còn đề cập đến sản phẩm chương trình máy tính bao gồm lệnh. Khi sản phẩm chương trình máy tính chạy trên máy tính, máy tính có thể thực hiện các bước được thực hiện bởi AMF thứ nhất trong các phương pháp được thể hiện trên Fig.3 và Fig.4.

Phương án thực hiện sáng chế còn đề cập đến sản phẩm chương trình máy tính bao gồm lệnh. Khi sản phẩm chương trình máy tính chạy trên máy tính, máy tính có thể thực hiện các bước được thực hiện bởi AMF thứ hai trong các phương pháp được thể hiện trên Fig.3 và Fig.4.

Phương án thực hiện sáng chế còn đề cập đến chip, bao gồm bộ xử lý. Bộ xử lý được tạo cấu hình để đọc chương trình máy tính được lưu trữ trong bộ nhớ và chạy chương trình máy tính, để thực hiện hoạt động và/hoặc thủ tục tương ứng được thực hiện bởi AMF thứ hai trong các phương pháp thu thập ngữ cảnh bảo mật theo sáng chế. Một cách tùy chọn, chip còn bao gồm bộ nhớ. Bộ nhớ được kết nối với bộ xử lý qua mạch hoặc cáp. Bộ xử lý được tạo cấu hình để đọc chương trình máy tính từ bộ nhớ và thực thi chương trình máy tính. Một cách tùy chọn, chip còn bao gồm giao diện truyền thông. Bộ xử lý được kết nối với giao diện truyền thông. Giao diện truyền thông được tạo cấu hình để nhận dữ liệu và/hoặc thông tin cần được xử lý. Bộ xử lý thu được dữ liệu và/hoặc thông tin từ giao diện truyền thông, và xử lý dữ liệu và/hoặc thông tin. Giao diện truyền thông có thể là giao diện I/O.

Sáng chế còn đề cập đến chip, bao gồm bộ xử lý. Bộ xử lý được tạo cấu hình để gọi chương trình máy tính được lưu trữ trong bộ nhớ và chạy chương trình máy tính, để thực hiện hoạt động và/hoặc thủ tục tương ứng được thực hiện bởi AMF thứ nhất trong các phương pháp thu thập ngữ cảnh bảo mật theo

sáng chế. Một cách tùy chọn, chip còn bao gồm bộ nhớ. Bộ nhớ được kết nối với bộ xử lý qua mạch hoặc cáp. Bộ xử lý được tạo cấu hình để đọc chương trình máy tính từ bộ nhớ và thực thi chương trình máy tính. Một cách tùy chọn, chip còn bao gồm giao diện truyền thông. Bộ xử lý được kết nối với giao diện truyền thông. Giao diện truyền thông được tạo cấu hình để nhận dữ liệu và/hoặc thông tin cần được xử lý. Bộ xử lý thu được dữ liệu và/hoặc thông tin từ giao diện truyền thông, và xử lý dữ liệu và/hoặc thông tin. Giao diện truyền thông có thể là giao diện I/O.

Người có hiểu biết trung bình trong lĩnh vực có thể hiểu rằng, cùng với các ví dụ được mô tả theo các phương án thực hiện được nêu trong bản mô tả, các khối và các bước thuật toán có thể được triển khai bằng cách phần cứng điện tử hoặc kết hợp của phần mềm máy tính và phần cứng điện tử. Liệu các chức năng có được thực hiện bằng phần cứng hoặc phần mềm tùy thuộc vào các ứng dụng cụ thể và các ràng buộc thiết kế của các giải pháp kỹ thuật. Người có hiểu biết trung bình trong lĩnh vực có thể sử dụng các phương pháp khác nhau để thực hiện các chức năng được mô tả cho mỗi ứng dụng cụ thể, nhưng không nên xem xét rằng việc triển khai vượt quá phạm vi của sáng chế.

Người có hiểu biết trung bình trong lĩnh vực có thể hiểu rõ rằng, để mô tả ngắn gọn và thuận tiện, đối với các quá trình làm việc chi tiết của hệ thống, thiết bị, và khối nêu trên, tham khảo các quá trình tương ứng ở các phương án thực hiện phương pháp nêu trên, và chi tiết không được mô tả lại ở đây.

Theo vài phương án thực hiện sáng chế, cần hiểu rằng hệ thống, thiết bị, và phương pháp được bộc lộ có thể được triển khai theo các cách khác. Chẳng hạn, thiết bị được mô tả theo phương án thực hiện chỉ là ví dụ. Chẳng hạn, việc phân chia thành các khối chỉ là phân chia chức năng lôgic và có thể là phân chia khác khi triển khai thực. Chẳng hạn, các khối và các thành phần có thể được kết hợp hoặc tích hợp vào hệ thống khác, hoặc một số dấu hiệu có thể bị bỏ qua hoặc không được thực hiện. Ngoài ra, các ghép nối qua lại được hiển thị hoặc đề cập hoặc các ghép nối trực tiếp hoặc các kết nối truyền thông có thể được triển khai nhờ sử dụng một số giao diện. Các ghép nối gián tiếp hoặc các kết nối truyền thông giữa các thiết bị hoặc các khối có thể được triển khai ở dạng

điện, cơ khí, hoặc các dạng khác.

Các khối được mô tả dưới dạng các phần riêng rẽ có thể hoặc không thể riêng rẽ về mặt vật lý, và các phần được hiển thị dưới dạng các khối có thể hoặc không thể là các khối vật lý, có thể được đặt ở một vị trí, hoặc có thể được phân tán trên các khối mạng. Một số hoặc tất cả các khối có thể được chọn dựa trên các yêu cầu thực để đạt được các mục đích của các giải pháp của các phương án thực hiện.

Ngoài ra, các khối chức năng theo các phương án thực hiện sáng chế có thể được tích hợp vào một khối xử lý, hoặc mỗi khối trong các khối có thể tồn tại độc lập về mặt vật lý, hoặc hai hoặc nhiều khối được tích hợp vào một khối.

Khi các chức năng được triển khai ở dạng khối chức năng phần mềm và được bán hoặc sử dụng làm sản phẩm độc lập, các chức năng có thể được lưu trữ trong phương tiện lưu trữ máy tính đọc được. Dựa trên hiểu biết này, các giải pháp kỹ thuật của sáng chế chủ yếu, hoặc một phần góp phần vào giải pháp kỹ thuật đã biết, hoặc một số giải pháp kỹ thuật có thể được triển khai ở dạng sản phẩm phần mềm. Sản phẩm phần mềm được lưu trữ trong phương tiện lưu trữ, và bao gồm vài lệnh để ra lệnh máy tính (có thể là máy tính cá nhân, máy chủ, thiết bị mạng, hoặc tương tự) thực hiện tất cả hoặc một số bước của các phương pháp được mô tả theo các phương án thực hiện sáng chế. Phương tiện lưu trữ nêu trên bao gồm: phương tiện bất kỳ có thể lưu trữ mã chương trình, chẳng hạn ổ nhớ nhanh USB, đĩa cứng tháo được, bộ nhớ chỉ đọc (Read-Only Memory, ROM), bộ nhớ truy nhập ngẫu nhiên ((R)ANdom Access Memory, RAM), đĩa từ, hoặc đĩa quang.

Ngoài ra, cụm từ "và/hoặc" theo sáng chế mô tả chỉ mối quan hệ liên kết để mô tả các đối tượng liên kết và biểu diễn việc ba mối quan hệ có thể tồn tại. Chẳng hạn, A và/hoặc B có thể là ba trường hợp sau: Chỉ có A, có cả A lẫn B, và chỉ có B. Ngoài ra, ký tự "/" trong bản mô tả thường chỉ báo mối quan hệ "hoặc" giữa các đối tượng liên kết. Cụm từ "ít nhất một" theo sáng chế có thể là "một" và "hai hoặc lớn hơn". Chẳng hạn, ít nhất một trong A, B, và C có thể là: Chỉ có A, chỉ có B, chỉ có C, có cả A lẫn B, và có cả A lẫn C, có C và B, và có A, B, và C.

Các phần mô tả nêu trên chỉ là các triển khai cụ thể của sáng chế, mà không nhằm giới hạn phạm vi bảo hộ của sáng chế. Biến thể hoặc thay thế bất kỳ dễ được đoán ra bởi người có hiểu biết trung bình trong lĩnh vực trong phạm vi kỹ thuật được bộc lộ theo sáng chế sẽ nằm trong phạm vi bảo hộ của sáng chế. Do vậy, phạm vi bảo hộ của sáng chế sẽ phụ thuộc vào phạm vi bảo hộ của các điểm yêu cầu bảo hộ.

YÊU CẦU BẢO HỘ

1. Phương pháp thu thập ngữ cảnh bảo mật bao gồm các bước:

nhận, bởi chức năng quản lý truy nhập và di động (access and mobility management function, AMF) thứ nhất, thông điệp yêu cầu đăng ký thứ nhất được gửi bởi thiết bị người dùng (user equipment, UE);

kiểm chứng, bởi AMF thứ nhất, tính toàn vẹn của thông điệp yêu cầu đăng ký thứ nhất;

gửi, bởi AMF thứ nhất, thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai khi AMF thứ nhất kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ nhất, trong đó thông điệp yêu cầu đăng ký thứ hai mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo rằng UE được kiểm chứng; và

nhận, bởi AMF thứ nhất, ngữ cảnh bảo mật của UE được gửi bởi AMF thứ hai dựa trên thông điệp yêu cầu đăng ký thứ hai.

2. Phương pháp theo điểm 1, trong đó bảo vệ bảo mật được thực hiện trên thông điệp yêu cầu đăng ký thứ nhất bằng cách sử dụng ngữ cảnh bảo mật được ánh xạ.

3. Phương pháp theo điểm 2, trong đó bảo vệ bảo mật bao gồm bảo vệ mật mã hóa và/hoặc bảo vệ tính toàn vẹn.

4. Phương pháp theo điểm 2, trong đó ngữ cảnh bảo mật được ánh xạ được dẫn xuất bởi UE dựa trên ngữ cảnh bảo mật giữa thực thể quản lý di động (mobility management entity, MME) và UE.

5. Phương pháp theo điểm 2, trong đó:

ngữ cảnh bảo mật được ánh xạ được dẫn xuất bởi UE dựa trên khóa K_{AMF1}.

6. Phương pháp theo điểm 1, trong đó:

ngữ cảnh bảo mật của UE là ngữ cảnh bảo mật nguyên gốc.

7. Phương pháp theo điểm 1, trong đó thông điệp yêu cầu đăng ký thứ nhất được gửi sau khi UE hoàn thành thủ tục chuyển vùng.

8. Phương pháp theo điểm 1, trong đó thông điệp yêu cầu đăng ký thứ nhất là thông điệp yêu cầu đăng ký.

9. Phương pháp theo điểm 1, trong đó thông điệp yêu cầu đăng ký thứ nhất bao gồm định danh UE tạm thời duy nhất toàn cục (unique temporary user equipment identity, GUTI) của UE.

10. Phương pháp theo điểm 9, trong đó 5G GUTI được tạo cấu hình bởi AMF thứ hai cho UE, và được sử dụng để nhận diện UE và AMF thứ hai.

11. Phương pháp theo điểm 1, trong đó thông điệp yêu cầu đăng ký thứ hai bao gồm 5G GUTI hoặc định danh thuê bao lâu dài (subscriber permanent identity, SUPI) của UE.

12. Phương pháp theo điểm 1, trong đó AMF thứ hai không cần kiểm chứng UE.

13. Phương pháp theo điểm 1, trong đó việc thông tin chỉ báo được sử dụng để chỉ báo rằng UE được kiểm chứng cụ thể bao gồm việc thông tin chỉ báo được sử dụng để chỉ báo rằng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ nhất được nhận bởi AMF thứ nhất từ UE được kiểm chứng thành công.

14. Phương pháp theo điểm 1, trong đó AMF thứ hai là AMF lưu lại ngữ cảnh bảo mật của UE khác ngoài AMF thứ nhất trong hệ thống truyền thông 5G trong quá trình trong đó UE được chuyển vùng từ hệ thống truyền thông 4G đến hệ thống truyền thông 5G.

15. Phương pháp theo điểm 1, trong đó AMF thứ nhất là AMF được chọn bởi

MME trong hệ thống truyền thông 4G cho UE từ hệ thống truyền thông 5G để cung cấp dịch vụ mạng lõi cho UE trong quá trình trong đó UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G.

16. Phương pháp theo điểm 1, trong đó hoạt động nhận, bởi AMF thứ nhất, ngữ cảnh bảo mật của UE được gửi bởi AMF thứ hai dựa trên thông điệp yêu cầu đăng ký thứ hai cụ thể bao gồm bước:

nhận, bởi AMF thứ nhất, ngữ cảnh của UE được gửi bởi AMF thứ hai dựa trên thông điệp yêu cầu đăng ký thứ hai, trong đó ngữ cảnh của UE bao gồm ngữ cảnh bảo mật của UE được xác định qua thương lượng giữa AMF thứ hai và UE, và ngữ cảnh bảo mật của UE bao gồm khóa K_{AMF2} và số đếm tầng không truy nhập (non-access stratum count, NAS COUNT).

17. Phương pháp theo điểm 9, trong đó nguyên nhân tại sao ngữ cảnh bảo mật và 5G GUTI của UE được lưu trữ giữa UE và AMF thứ hai bao gồm: trước khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G, UE được chuyển vùng từ hệ thống truyền thông mạng 5G sang hệ thống truyền thông 4G; hoặc UE hỗ trợ kết nối kép (dual connectivity, DC) truy nhập hệ thống truyền thông 5G qua kết nối phi 3GPP, truy nhập hệ thống truyền thông 4G qua kết nối 3GPP, và được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G trong chế độ được kết nối.

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

khi AMF thứ nhất không kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ nhất, tiếp tục, bởi AMF thứ nhất, để sử dụng ngữ cảnh bảo mật được ánh xạ được tạo qua thương lượng giữa AMF thứ nhất và UE, hoặc khởi tạo, bởi AMF thứ nhất, xác thực ban đầu đến UE để tạo ngữ cảnh bảo mật giữa AMF thứ nhất và UE.

19. Phương pháp theo điểm 1, trong đó phương pháp còn bao gồm các bước: khi AMF thứ nhất không kiểm chứng tính toàn vẹn của thông điệp yêu cầu

đăng ký thứ nhất, không tiếp nhận, bởi AMF thứ nhất, ngữ cảnh bảo mật của UE được gửi bởi AMF thứ hai.

20. Phương pháp theo điểm 1, trong đó hoạt động nhận, bởi AMF thứ nhất, ngữ cảnh bảo mật của UE được gửi bởi AMF thứ hai dựa trên thông điệp yêu cầu đăng ký thứ hai cụ thể bao gồm bước:

nhận, bởi AMF thứ nhất, ngữ cảnh bảo mật của UE được xác định bởi AMF thứ hai dựa trên 5G GUTI trong thông điệp yêu cầu đăng ký thứ hai.

21. Phương pháp theo điểm 2, trong đó việc ngữ cảnh bảo mật được ánh xạ được dẫn xuất bởi UE dựa trên khóa K_{AMF1} cụ thể bao gồm:

UE dẫn xuất khóa K_{AMF1} dựa trên khóa được lưu lại K_{ASME}, tham số bước nhảy tiếp theo NH, và công thức định trước, trong đó công thức định trước là:

K_{AMF1} = HMAC-SHA-256 (Key, FC||P0||L0), trong đó FC = 0x76, P0 = giá trị NH, L0 = chiều dài của giá trị NH, và KEY = K_{ASME}.

22. Phương pháp theo điểm 1, trong đó trước khi nhận, bởi AMF thứ nhất, thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE, phương pháp còn bao gồm bước:

nhận, bởi AMF thứ nhất, yêu cầu chuyển tiếp định vị lại thứ nhất từ MME, trong đó yêu cầu chuyển tiếp định vị lại thứ nhất bao gồm ngữ cảnh bảo mật giữa UE và MME;

xác định, bởi AMF thứ nhất, ngữ cảnh bảo mật được ánh xạ dựa trên ngữ cảnh bảo mật giữa UE và MME;

gửi, bởi AMF thứ nhất, thông điệp đáp ứng chuyển tiếp định vị lại đến MME;

gửi, bởi MME, thông điệp lệnh chuyển vùng đến UE; và

xác định, bởi UE, ngữ cảnh bảo mật được ánh xạ.

23. Phương pháp theo điểm 22, trong đó phương pháp còn bao gồm bước:

yêu cầu chuyển tiếp định vị lại thứ nhất bao gồm khóa K_{ASME} và tham số

bước nhảy tiếp theo NH; và

dẫn xuất, bởi AMF thứ nhất, khóa K_{AMF1} dựa trên K_{ASME} và NH.

24. Phương pháp theo điểm 23, trong đó hoạt động dẫn xuất, bởi AMF thứ nhất, khóa K_{AMF1} dựa trên K_{ASME} và NH cụ thể bao gồm:

sau khi AMF thứ nhất nhận K_{ASME} và NH, dẫn xuất, bởi AMF thứ nhất, K_{AMF1} dựa trên công thức định trước, trong đó công thức định trước là:

K_{AMF1} = HMAC-SHA-256 (Key, FC||P0||L0), trong đó FC = 0x76, P0 = giá trị NH, L0 = chiều dài của giá trị NH, và KEY = K_{ASME}.

25. Phương pháp theo điểm 24, trong đó phương pháp còn bao gồm bước:

tính toán, bởi AMF thứ nhất, khóa bảo vệ tính toàn vẹn $K_{NASint1}$ và khóa bảo vệ tính riêng tư $K_{NASenc1}$ dựa trên K_{ASME} và thuật toán bảo mật được thương lượng với UE.

26. Phương pháp theo điểm 24, trong đó phương pháp còn bao gồm bước:

tạo, bởi UE dựa trên khóa K_{AMF1} và thuật toán bảo vệ tính toàn vẹn tầng không truy nhập (non-access stratum, NAS) và thuật toán bảo vệ tính riêng tư được thương lượng giữa UE và AMF thứ nhất, khóa bảo vệ tính toàn vẹn $K_{NASint1}$ và khóa bảo vệ tính riêng tư $K_{NASenc1}$ được sử dụng để bảo vệ thông điệp NAS.

27. Phương pháp theo điểm 26, trong đó phương pháp còn bao gồm:

công thức để tính toán khóa bảo vệ tính toàn vẹn $K_{NASint1}$ bao gồm: $K_{NASint1}$ = HMAC-SHA-256 (KEY,S), trong đó S = FC| $|P0_1$ | $|L0_1$ | $|P1_1|$ $|L1_1$, FC = 0x69, $P0_1$ = bộ phân loại thuật toán, $L0_1$= chiều dài của bộ phân loại thuật toán, $P1_1$= định danh thuật toán, $L1_1$ = chiều dài của định danh thuật toán, và KEY = K_{AMF1}.

28. Phương pháp theo điểm 27, trong đó phương pháp còn bao gồm:

công thức để tính toán the khóa bảo vệ tính riêng tư $K_{NASenc1}$ bao gồm:

$K_{NASenc1}$ = HMAC-SHA-256 (KEY, S), trong đó S = FC| |P0| |L0| |P1| |L1, FC = 0x69, P0 = bộ phân loại thuật toán, L0 = chiều dài của bộ phân loại thuật toán, P1 = định danh thuật toán, L1 = chiều dài của định danh thuật toán, và KEY = K_{AMF1}.

29. Phương pháp theo điểm 22, trong đó thông điệp đáp ứng chuyển tiếp định vị lại được sử dụng để thông báo MME rằng AMF thứ nhất là AMF cung cấp dịch vụ quản lý truy nhập và di động cho UE trong hệ thống truyền thông 5G khi UE được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G.

30. Phương pháp thu thập ngữ cảnh bảo mật bao gồm các bước:

nhận, bởi AMF thứ hai, thông điệp yêu cầu đăng ký thứ hai được gửi bởi AMF thứ nhất, trong đó thông điệp yêu cầu đăng ký thứ hai mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo rằng UE được kiểm chứng; và

sau khi AMF thứ hai nhận thông điệp đăng ký thứ hai, gửi, bởi AMF thứ hai, ngữ cảnh bảo mật của UE đến AMF thứ nhất,

trong đó thông điệp yêu cầu đăng ký thứ hai được gửi khi AMF thứ nhất kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ nhất, và thông điệp đăng ký thứ nhất được gửi bởi UE đến AMF thứ nhất.

31. Phương pháp theo điểm 30, trong đó thông điệp yêu cầu đăng ký thứ hai bao gồm 5G GUTI hoặc SUPI của UE.

32. Phương pháp theo điểm 30, trong đó trước khi AMF thứ hai gửi ngữ cảnh bảo mật của UE đến AMF thứ nhất, AMF thứ hai xác định ngữ cảnh bảo mật của UE dựa trên 5G GUTI trong thông điệp yêu cầu đăng ký thứ hai.

33. Phương pháp theo điểm 30, trong đó AMF thứ hai không cần kiểm chứng UE.

34. Phương pháp theo điểm 31, trong đó nguyên nhân tại sao ngữ cảnh bảo mật và 5G GUTI của UE được lưu trữ giữa UE và AMF thứ hai bao gồm: trước khi UE được chuyển vùng từ hệ thống truyền thông 4G đến hệ thống truyền thông 5G, UE được chuyển vùng từ hệ thống truyền thông mạng 5G đến hệ thống truyền thông 4G; hoặc UE hỗ trợ DC truy nhập hệ thống truyền thông 5G qua kết nối phi 3GPP, truy nhập hệ thống truyền thông 4G qua kết nối 3GPP, và được chuyển vùng từ hệ thống truyền thông 4G sang hệ thống truyền thông 5G trong chế độ được kết nối.

35. Hệ thống truyền thông bao gồm AMF thứ nhất và AMF thứ hai, trong đó:

AMF thứ nhất được tạo cấu hình để:

nhận thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE;

kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ nhất;

khi AMF thứ nhất kiểm chứng thành công tính toàn vẹn của thông điệp yêu cầu đăng ký thứ nhất, gửi thông điệp yêu cầu đăng ký thứ hai đến AMF thứ hai, trong đó thông điệp yêu cầu đăng ký thứ hai mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo rằng UE được kiểm chứng; và

AMF thứ hai được tạo cấu hình để:

nhận thông điệp yêu cầu đăng ký thứ hai; và

gửi ngữ cảnh bảo mật của UE đến AMF thứ nhất dựa trên thông điệp yêu cầu đăng ký thứ hai.

36. Hệ thống theo điểm 35, trong đó trước khi AMF thứ nhất nhận thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE, AMF thứ nhất còn được tạo cấu hình để:

nhận yêu cầu chuyển tiếp định vị lại thứ nhất từ MME, trong đó yêu cầu chuyển tiếp định vị lại thứ nhất bao gồm ngữ cảnh bảo mật giữa UE và MME;

xác định ngữ cảnh bảo mật được ánh xạ dựa trên ngữ cảnh bảo mật giữa UE và MME; và

gửi thông điệp đáp ứng chuyển tiếp định vị lại đến MME.

37. Hệ thống theo điểm 36, trong đó yêu cầu chuyển tiếp định vị lại thứ nhất bao gồm khóa K_{ASME} và tham số bước nhảy tiếp theo NH, và AMF thứ nhất còn được tạo cấu hình để:

dẫn xuất khóa K_{AMF1} dựa trên K_{ASME} và NH.

38. Hệ thống theo điểm 37, trong đó AMF thứ nhất được tạo cấu hình cụ thể để:

sau khi AMF thứ nhất nhận K_{ASME} và NH, dẫn xuất K_{AMF1} dựa trên công thức định trước, trong đó công thức định trước là:

K_{AMF1} = HMAC-SHA-256 (Key, FC||P0||L0), trong đó FC = 0x76, P0 = giá trị NH, L0 = chiều dài của giá trị NH, và KEY = K_{ASME}.

39. Hệ thống theo điểm 38, trong đó AMF thứ nhất còn được tạo cấu hình để:

tính toán khóa bảo vệ tính toàn vẹn $K_{NASint1}$ và khóa bảo vệ tính riêng tư $K_{NASenc1}$ dựa trên K_{ASME} và thuật toán bảo mật được thương lượng với UE.

40. Hệ thống theo điểm 36, trong đó thông điệp đáp ứng chuyển tiếp định vị lại được sử dụng để thông báo MME rằng AMF thứ nhất là AMF cung cấp dịch vụ quản lý truy nhập và di động cho UE trong hệ thống truyền thông 5G khi UE được chuyển vùng từ hệ thống truyền thông 4G đến hệ thống truyền thông 5G.

41. Hệ thống theo điểm 35, trong đó thông điệp yêu cầu đăng ký thứ nhất là thông điệp yêu cầu đăng ký.

42. Hệ thống theo điểm 35, trong đó trước khi AMF thứ nhất nhận thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE, AMF thứ nhất còn được tạo cấu hình để:

nhận thông điệp yêu cầu đăng ký thứ nhất được gửi bởi UE sau khi UE hoàn thành thủ tục chuyển vùng.

43. Hệ thống theo điểm 35, trong đó thông điệp yêu cầu đăng ký thứ nhất bao

gồm 5G GUTI của UE.

44. Hệ thống theo điểm 43, trong đó 5G GUTI được tạo cấu hình bởi AMF thứ hai cho UE, và được sử dụng để nhận diện UE và AMF thứ hai.

45. Hệ thống theo điểm 43, trong đó nguyên nhân tại sao ngữ cảnh bảo mật và 5G GUTI của UE được lưu trữ giữa UE và AMF thứ hai bao gồm: trước khi UE được chuyển vùng từ hệ thống truyền thông 4G đến hệ thống truyền thông 5G, UE được chuyển vùng từ hệ thống truyền thông mạng 5G đến hệ thống truyền thông 4G; hoặc UE hỗ trợ DC truy nhập hệ thống truyền thông 5G qua kết nối phi 3GPP, truy nhập hệ thống truyền thông 4G qua kết nối 3GPP, và được chuyển vùng từ hệ thống truyền thông 4G đến hệ thống truyền thông 5G trong chế độ được kết nối.

46. Hệ thống theo điểm 35, trong đó thông điệp yêu cầu đăng ký thứ hai bao gồm 5G GUTI hoặc SUPI của UE.

47. Hệ thống theo điểm 35, trong đó AMF thứ hai còn được tạo cấu hình để:

xác định ngữ cảnh bảo mật của UE dựa trên 5G GUTI trong thông điệp yêu cầu đăng ký thứ hai khi AMF thứ hai nhận thông điệp yêu cầu đăng ký thứ hai.

48. Hệ thống theo điểm 35, trong đó AMF thứ hai không cần kiểm chứng UE.

49. Thiết bị thu thập ngữ cảnh bảo mật, trong đó thiết bị được áp dụng cho hệ thống mạng, hệ thống mạng bao gồm AMF thứ nhất và AMF thứ hai, và thiết bị bao gồm bộ xử lý, mạch giao diện, bộ nhớ, và buýt hệ thống; và

bộ nhớ được tạo cấu hình để lưu trữ các lệnh máy tính thực thi được, và bộ xử lý thực thi các lệnh máy tính thực thi được lưu trữ trong bộ nhớ để thiết bị có thể thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 34.

50. Thiết bị mạng thu thập ngữ cảnh bảo mật, bao gồm bộ xử lý và bộ nhớ, trong đó bộ nhớ được tạo cấu hình để lưu trữ chương trình máy tính, và bộ xử lý thực thi các lệnh máy tính thực thi được lưu trữ trong bộ nhớ để thiết bị mạng có thể thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 29.

51. Thiết bị mạng thu thập ngữ cảnh bảo mật, bao gồm bộ xử lý và bộ nhớ, trong đó bộ nhớ được tạo cấu hình để lưu trữ chương trình máy tính, và bộ xử lý thực thi các lệnh máy tính thực thi được lưu trữ trong bộ nhớ để thiết bị mạng có thể thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 30 đến 34.

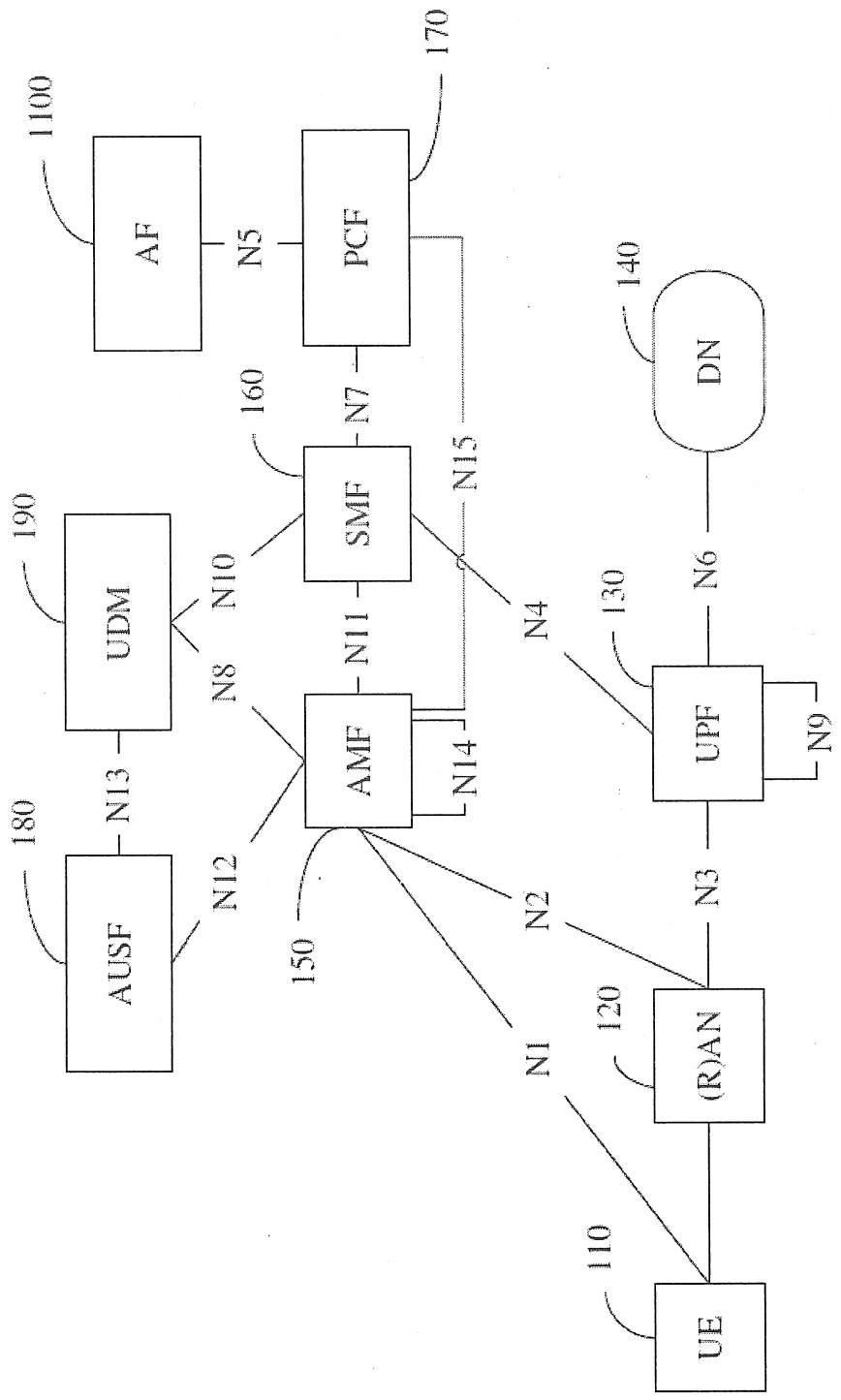

1100
AF
N5
PCF
170
160
N7
SMF
N15
190
UDM
N10
N11
N4
140
DN
N6
130
UPF
N9
N8
AMF
N14
180
N13
AUSF
N12
150
N2
N3
120
(R)AN
N1
110
UE

Fig.1

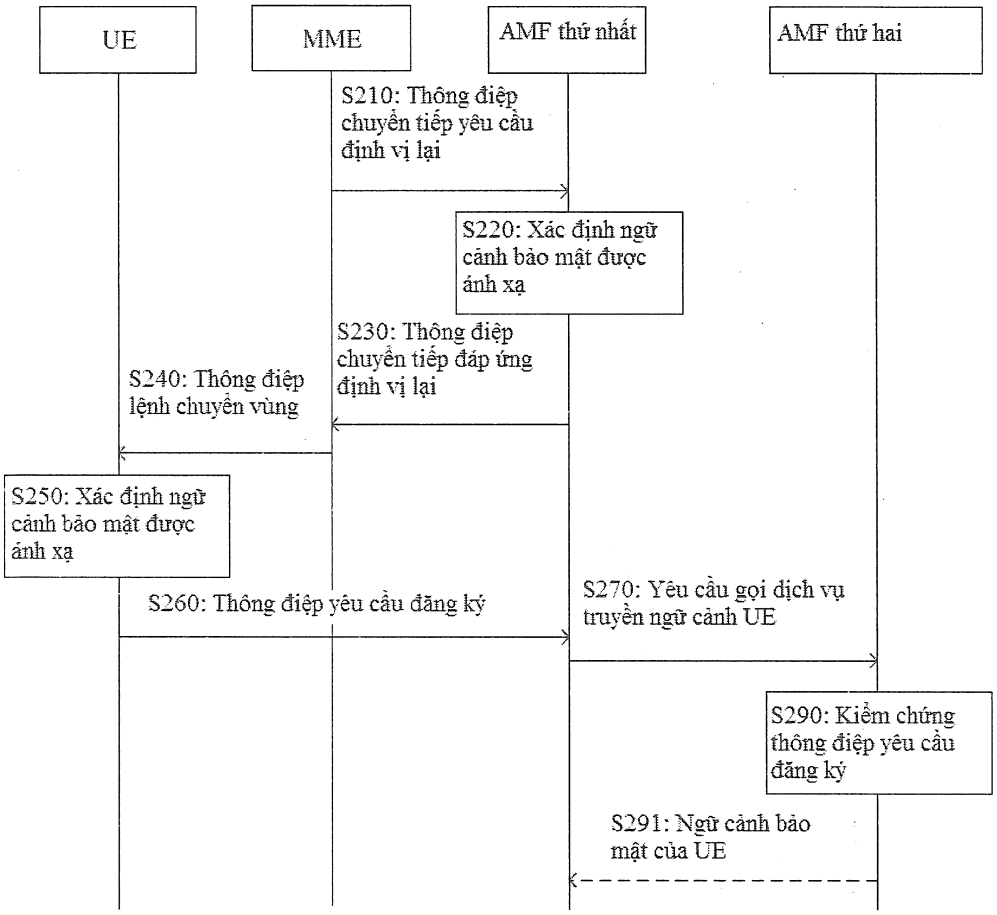

UE
MME
AMF thứ nhất
AMF thứ hai
S210: Thông điệp chuyển tiếp yêu cầu định vị lại
S220: Xác định ngữ cảnh bảo mật được ánh xạ
S230: Thông điệp chuyển tiếp đáp ứng định vị lại
S240: Thông điệp lệnh chuyển vùng
S250: Xác định ngữ cảnh bảo mật được ánh xạ
S260: Thông điệp yêu cầu đăng ký
S270: Yêu cầu gọi dịch vụ truyền ngữ cảnh UE
S290: Kiểm chứng thông điệp yêu cầu đăng ký
S291: Ngữ cảnh bảo mật của UE

Fig.2

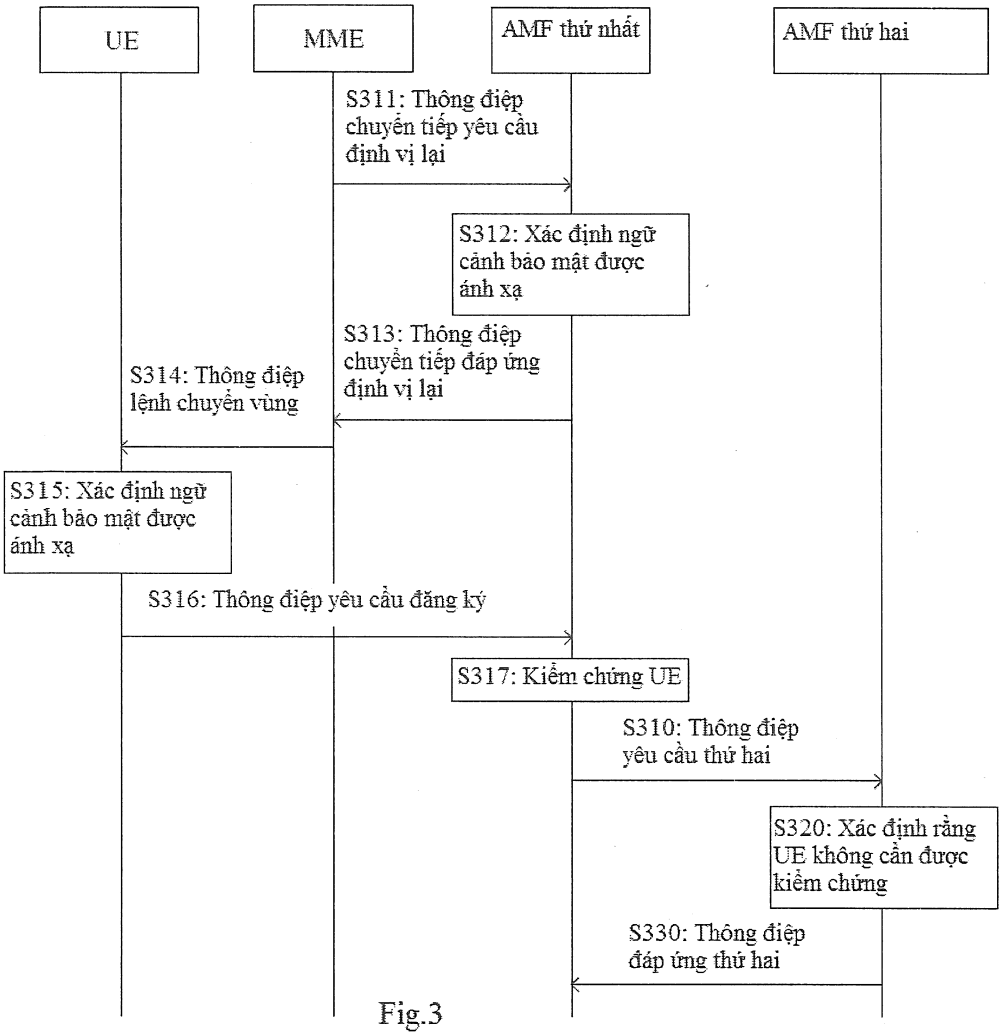

UE
MME
AMF thứ nhất
AMF thứ hai
S311: Thông điệp chuyển tiếp yêu cầu định vị lại
S312: Xác định ngữ cảnh bảo mật được ánh xạ
S313: Thông điệp chuyển tiếp đáp ứng định vị lại
S314: Thông điệp lệnh chuyển vùng
S315: Xác định ngữ cảnh bảo mật được ánh xạ
S316: Thông điệp yêu cầu đăng ký
S317: Kiểm chứng UE
S310: Thông điệp yêu cầu thứ hai
S320: Xác định rằng UE không cần được kiểm chứng
S330: Thông điệp đáp ứng thứ hai

Fig.3

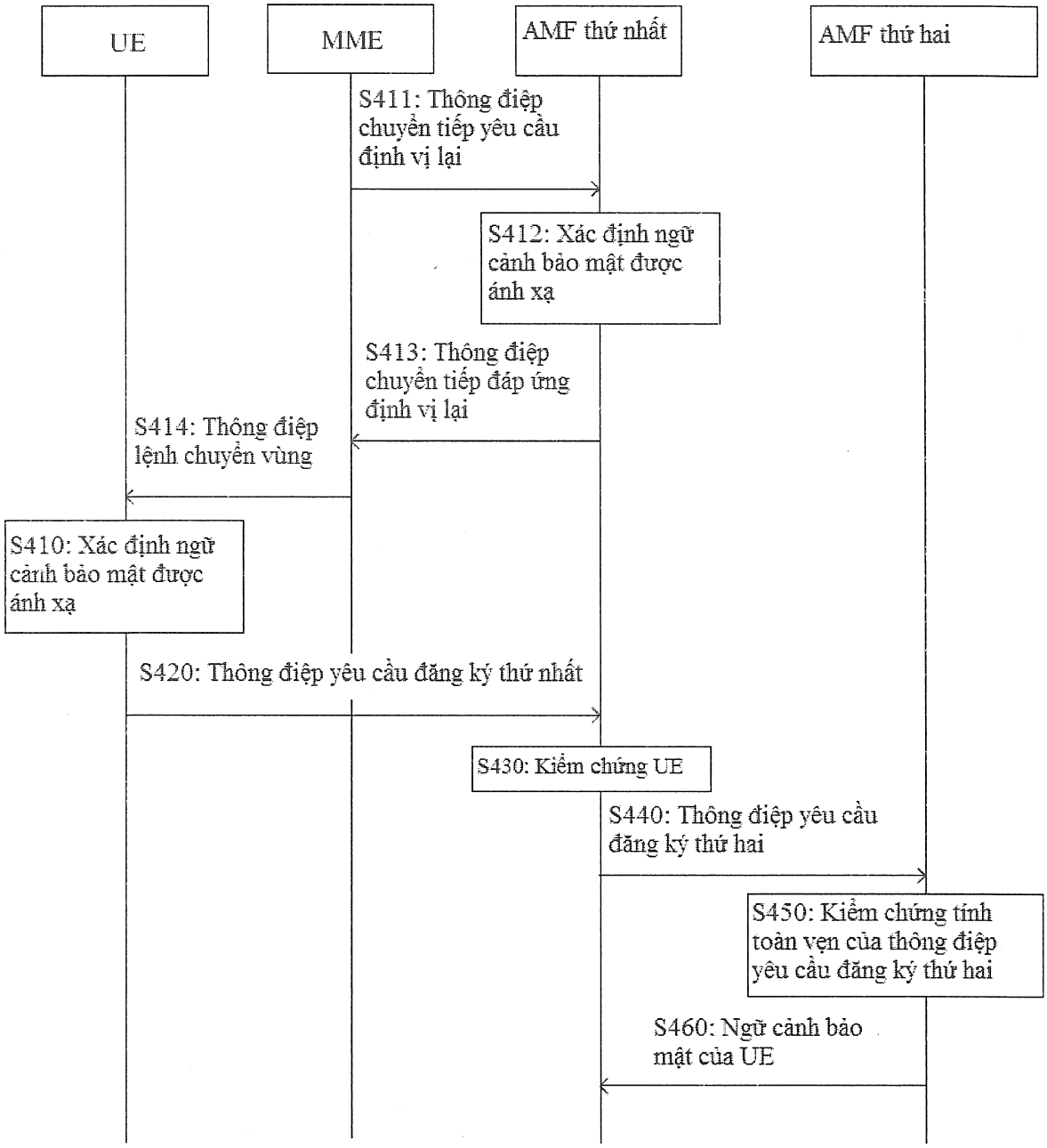

UE
MME
AMF thứ nhất
AMF thứ hai
S411: Thông điệp chuyển tiếp yêu cầu định vị lại
S412: Xác định ngữ cảnh bảo mật được ánh xạ
S413: Thông điệp chuyển tiếp đáp ứng định vị lại
S414: Thông điệp lệnh chuyển vùng
S410: Xác định ngữ cảnh bảo mật được ánh xạ
S420: Thông điệp yêu cầu đăng ký thứ nhất
S430: Kiểm chứng UE
S440: Thông điệp yêu cầu đăng ký thứ hai
S450: Kiểm chứng tính toàn vẹn của thông điệp yêu cầu đăng ký thứ hai
S460: Ngữ cảnh bảo mật của UE

Fig.4

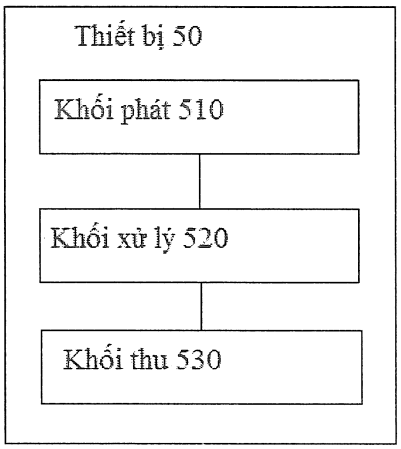

Thiết bị 50
Khối phát 510
Khối xử lý 520
Khối thu 530

Fig.5

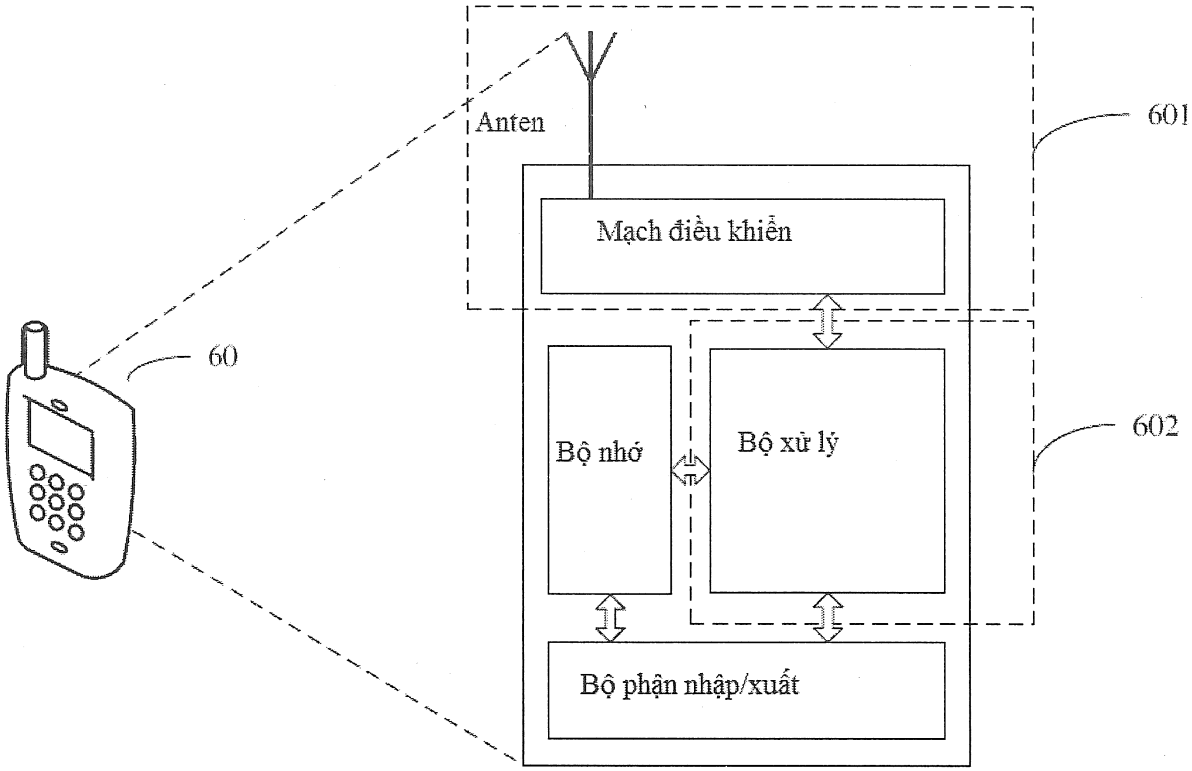

Anten
601
Mạch điều khiển
60
Bộ nhớ
Bộ xử lý
602
Bộ phận nhập/xuất

Fig.6

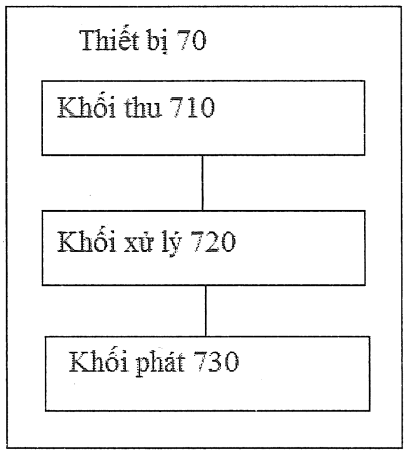


Fig.7

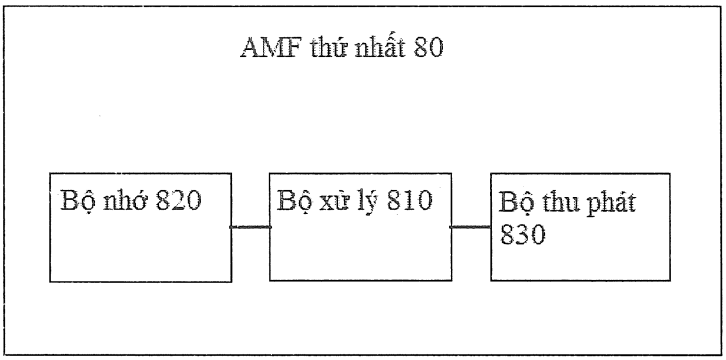


Fig.8

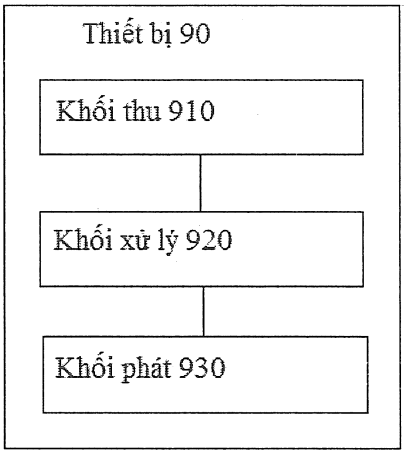


Fig.9

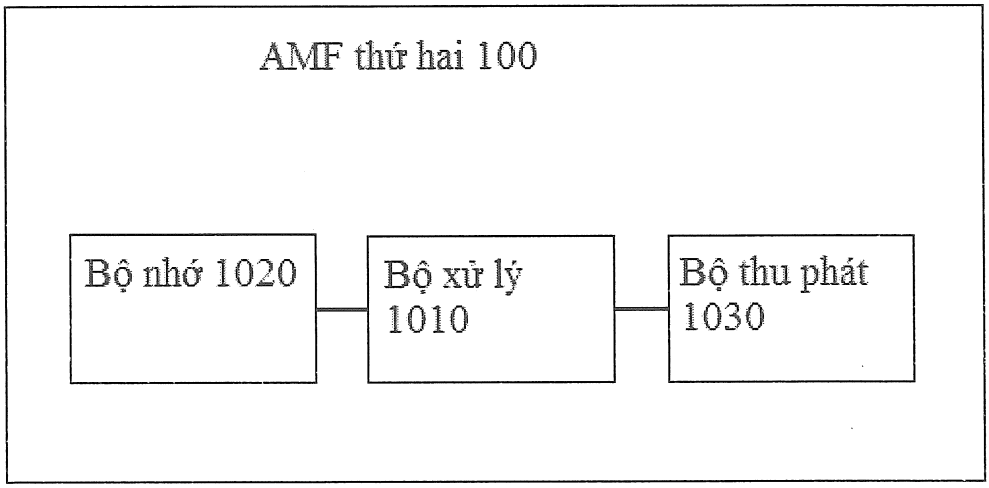


Fig.10