(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) **1-0044254**

(51)[2020.01] **G06F 21/60**; G06F 21/62; H04W 12/02; H04L 29/08; H04W 12/00; G06F 16/955; H04L 29/06

(13) **B**

(21) 1-2020-05082
(22) 15/02/2019
(86) PCT/EP2019/053784 15/02/2019
(87) WO2019/158681 22/08/2019
(30) 18382092.7 16/02/2018 EP
(45) 25/03/2025 444
(43) 25/12/2020 393A
(71) TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (SE)
SE-164 83 Stockholm, Sweden
(72) SAARINEN, Pasi (SE); MARTINEZ DE LA CRUZ, Pablo (ES); DE-GREGORIO-RODRIGUEZ, Jesus-Angel (ES); JOST, Christine (DE).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP TRUYỀN THÔNG VÀ THIẾT BỊ MẠNG

(21) 1-2020-05082

(57) Sáng chế đề cập đến thiết bị mạng (300, 400) được tạo cấu hình cho sự sử dụng trong một trong nhiều miền mạng lõi khác nhau của hệ thống truyền thông không dây (10). Thiết bị mạng (300, 400) được tạo cấu hình để nhận thông điệp (60) mà đã, hoặc là để, được truyền giữa các miền mạng lõi khác nhau. Thiết bị mạng (300, 400) cũng được tạo cấu hình để áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn của nội dung của trường trong thông điệp theo chính sách bảo vệ (80). Chính sách bảo vệ (80) gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ. Thiết bị mạng (300, 400) cũng được tạo cấu hình để gửi chuyển tiếp thông điệp (60), với sự bảo vệ an toàn liên miền được áp dụng hoặc được loại bỏ đối với một hoặc nhiều đoạn, về phía đích của thông điệp (60). Sáng chế cũng đề cập đến phương pháp truyền thông được thực hiện bởi thiết bị mạng, và phương tiện lưu trữ đọc được bởi máy tính.

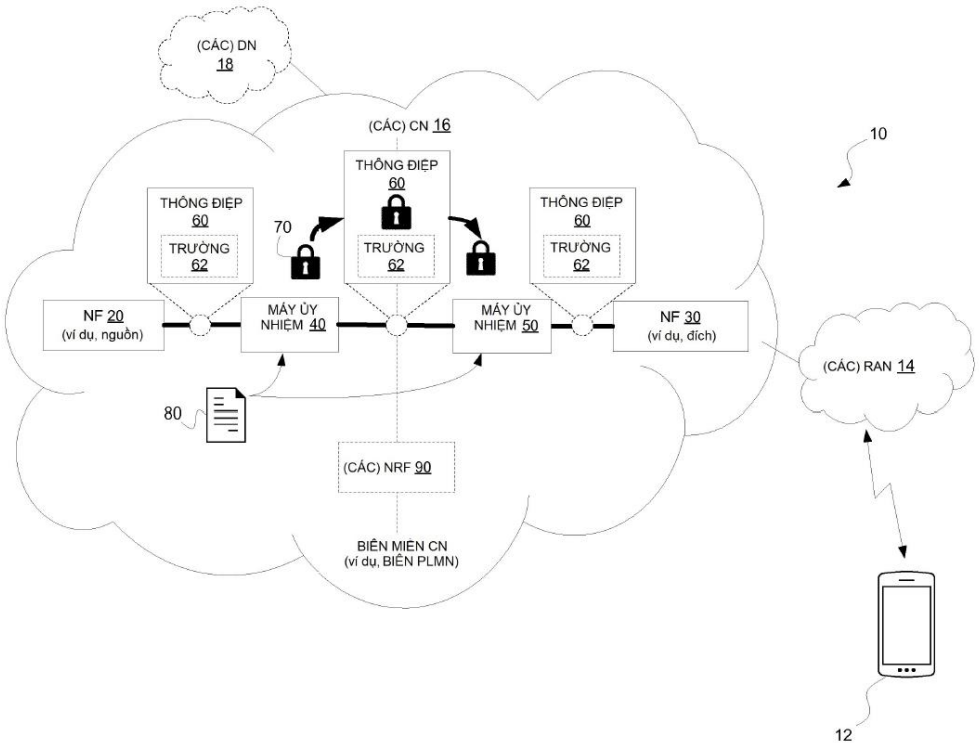

FIG. 1

Lĩnh vực kỹ thuật được đề cập

Sáng chế nói chung là đề cập đến hệ thống truyền thông không dây, và nói riêng hơn là đề cập đến việc bảo vệ thông điệp được truyền giữa các miền mạng lõi khác nhau của hệ thống truyền thông không dây.

Tình trạng kỹ thuật của sáng chế

Miền mạng phục vụ của người dùng gồm có thiết bị mạng lõi và các chức năng mà là cục bộ đối với điểm truy nhập của người dùng. Miền mạng thường trú (home network) của người dùng gồm có thiết bị mạng lõi và các chức năng mà không phụ thuộc vào địa điểm của điểm truy nhập của người dùng. Miền mạng thường trú của người dùng có thể chẳng hạn quản lý thông tin thuê bao và/hoặc các dịch vụ đặc trưng thường trú (home-specific service) của người dùng. Khi miền mạng phục vụ của người dùng khác với miền mạng thường trú của người dùng, miền mạng phục vụ và miền mạng thường trú truyền thông với nhau, ví dụ, cho sự xác thực người dùng, cho các dịch vụ/dữ liệu đặc trưng người dùng, v.v.. Trong các phiên bản này và các phiên bản khác, sự truyền thông giữa các miền mạng lõi khác nhau sẽ được bảo vệ (ví dụ, với sự bảo vệ bảo mật (confidentiality) và/hoặc toàn vẹn (integrity)), để bảo đảm sự truyền thông không được kiểm tra hoặc được sửa đổi bởi các bên không được phép.

Một số ngữ cảnh làm phức tạp sự bảo vệ của sự truyền thông liên miền. Thứ nhất, nhà cung cấp trao đổi liên mạng mà hỗ trợ sự kết nối lẫn nhau giữa các miền mạng lõi khác nhau có thể trên thực tế cần đọc và/hoặc sửa đổi một số trong sự truyền thông để đưa ra các dịch vụ có giá trị nhất định cho các nhà vận hành mạng. Thứ hai, việc bảo đảm sự bảo vệ thích đáng của sự truyền thông liên miền khi đối mặt với các định dạng truyền thông tiến hóa đe dọa áp đặt tổng phí (overhead) vận hành và quản trị không thực tế.

Bản chất kỹ thuật của sáng chế

Một số phương án ở đây khai thác chính sách bảo vệ cho sự bảo vệ an toàn liên miền (inter-domain security protection) của thông điệp được truyền giữa các miền mạng

lõi khác nhau của hệ thống truyền thông không dây. Chính sách bảo vệ có thể chỉ báo một hoặc nhiều đoạn (portion) nào của thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ, ví dụ, sao cho sự bảo vệ có thể được áp dụng hoặc được loại bỏ theo cách chọn lọc đối với chỉ các đoạn nhất định của thông điệp. Trên thực tế, trong một số phương án, chính sách bảo vệ gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung của trường trong thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ. Theo cách này, sự bảo vệ có thể được áp dụng hoặc được loại bỏ theo cách chọn lọc đối với (các) đoạn nhất định của nội dung của trường đã cho, hơn là so với toàn bộ nội dung của trường.

Như một sự lựa chọn hoặc ngoài ra, trong một số phương án, chính sách bảo vệ cho sự bảo vệ an toàn liên miền của thông điệp có thể được nhận và/hoặc được cập nhật theo cách động. Ví dụ, trong một phương án, chính sách bảo vệ có thể áp dụng được cho thông điệp nhất định (ví dụ, của loại đặc trưng) có thể được tìm ra và/hoặc được lấy ra theo cách động đáp lại việc nhận thông điệp. Trong phương án khác, chính sách bảo vệ có thể áp dụng được cho thông điệp nhất định có thể được gồm có trong hoặc nếu không thì được kết hợp với chính thông điệp.

Sự bảo vệ an toàn liên miền chọn lọc của các đoạn nhất định của thông điệp (ví dụ, một hoặc nhiều đoạn của nội dung của trường nhất định) theo một số phương án ở đây có thể theo cách thuận lợi làm cho nhà cung cấp trao đổi liên mạng có thể đọc và/hoặc sửa đổi thông điệp khi cần để đưa ra các dịch vụ cho các nhà vận hành mạng. Như một sự lựa chọn hoặc ngoài ra, khả năng cập nhật và/hoặc sự nhận động của chính sách bảo vệ theo một số phương án có thể cung cấp theo cách thuận lợi sự bảo vệ linh hoạt mà tiến hóa cùng với các sự thay đổi định dạng thông điệp (ví dụ, có thể quy cho sự tiến hóa của các chức năng mạng trong mạng lõi), trong khi giảm thiểu hoặc ít nhất giảm tổng phí vận hành và/hoặc quản trị mà sẽ nếu không thì được đòi hỏi cho tính linh hoạt như vậy.

Nói riêng hơn, các phương án ở đây gồm có phương pháp được thực hiện bởi thiết bị mạng (network equipment) trong một trong nhiều miền mạng lõi khác nhau của hệ thống truyền thông không dây. Phương pháp có thể bao gồm bước nhận thông điệp mà đã, hoặc là để, được truyền giữa các miền mạng lõi khác nhau. Phương pháp có thể cũng bao gồm bước áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ

an toàn liên miền khỏi, một hoặc nhiều đoạn của thông điệp (ví dụ, một hoặc nhiều đoạn của nội dung của trường trong thông điệp) theo chính sách bảo vệ. Trong một số phương án, chính sách bảo vệ chỉ báo một hoặc nhiều đoạn nào của thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ. Ví dụ, trong một phương án, chính sách bảo vệ gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung của trường trong thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ. Trong một số phương án, thiết bị mạng có thể thu được chính sách bảo vệ nhờ nhận chính sách bảo vệ, ví dụ, theo cách động đáp lại yêu cầu tìm ra (discovery request). Trong một số phương án, phương pháp còn bao gồm bước gửi chuyển tiếp thông điệp, với sự bảo vệ an toàn liên miền được áp dụng hoặc được loại bỏ đối với một hoặc nhiều đoạn, về phía đích (destination) của thông điệp.

Trong một số phương án, thông điệp là thông điệp Giao thức chuyển tải siêu văn bản (Hypertext Transfer Protocol, HTTP) và trường là trường HTTP. Ví dụ, trong một số phương án, thông điệp HTTP là thông điệp yêu cầu HTTP và trường là trường đường (path field), và trong đó nội dung của trường đường là Phần tử nhận dạng tài nguyên đồng nhất (Uniform Resource Identifier, URI) yêu cầu.

Trong một số phương án, thông tin gồm có một hoặc nhiều biểu thức thông thường (regular expression) mà chỉ báo một hoặc nhiều đoạn. Như một sự lựa chọn hoặc ngoài ra, trong một số phương án, thông tin gồm có một hoặc nhiều Con trỏ (Pointer) Ký hiệu đối tượng JavaScript (JavaScript Object Notation, JSON), mà chỉ báo một hoặc nhiều đoạn.

Trong một số phương án, chính sách bảo vệ còn chỉ báo, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ. Trong trường hợp này, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ có thể bao gồm sự bảo vệ bảo mật và/hoặc sự bảo vệ toàn vẹn.

Trong một số phương án, chính sách bảo vệ được gồm có trong thông điệp. Trong các phương án này và các phương án khác, phương pháp có thể còn bao gồm bước nhận chính sách bảo vệ từ thiết bị mạng trong đường mà thông điệp đi từ nguồn (source) của thông điệp đến đích của thông điệp. Trong các phương án khác, phương pháp có thể còn bao gồm bước, đáp lại việc nhận thông điệp, truyền yêu cầu tìm ra đến chức năng kho

mạng (network repository function, NRF) yêu cầu sự tìm ra của chính sách bảo vệ để bảo vệ thông điệp, và nhận chính sách bảo vệ đáp lại yêu cầu tìm ra.

Các phương án ở đây cũng gồm có phương pháp được thực hiện bởi thiết bị mạng để tạo thuận lợi cho sự bảo vệ của thông điệp được truyền giữa các miền mạng lõi khác nhau của hệ thống truyền thông không dây. Phương pháp có thể bao gồm bước thu được chính sách bảo vệ. Trong một số phương án, chính sách bảo vệ chỉ báo một hoặc nhiều đoạn nào của thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ. Ví dụ, trong một phương án, chính sách bảo vệ gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung của trường trong thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ. Bất kể, phương pháp có thể cũng bao gồm bước truyền chính sách bảo vệ. Chẳng hạn, trong một số phương án, phương pháp bao gồm bước truyền chính sách bảo vệ đến thiết bị mạng, trong một các miền mạng lõi khác nhau, được tạo cấu hình để áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn theo chính sách bảo vệ.

Trong một số phương án, phương pháp được thực hiện bởi thiết bị mạng mà thi hành chức năng kho mạng (network repository function, NRF). Trong trường hợp này, phương pháp có thể còn bao gồm bước nhận yêu cầu tìm ra yêu cầu sự tìm ra của chính sách bảo vệ để bảo vệ thông điệp, và truyền chính sách bảo vệ đáp lại yêu cầu tìm ra. Trong các phương án khác, phương pháp có thể được thực hiện bởi thiết bị mạng trong đường mà thông điệp đi từ nguồn của thông điệp đến đích của thông điệp. Trong các phương án này và các phương án khác, chính sách bảo vệ có thể được gồm có trong thông điệp.

Trong một số phương án, thông điệp là thông điệp Giao thức chuyển tải siêu văn bản (Hypertext Transfer Protocol, HTTP) và trường là trường HTTP. Ví dụ, trong một số phương án, thông điệp HTTP là thông điệp yêu cầu HTTP và trường là trường đường, và trong đó nội dung của trường đường là Phần tử nhận dạng tài nguyên đồng nhất (Uniform Resource Identifier, URI) yêu cầu.

Trong một số phương án, thông tin gồm có một hoặc nhiều biểu thức thông thường mà chỉ báo một hoặc nhiều đoạn. Như một sự lựa chọn hoặc ngoài ra, trong một

số phương án, thông tin gồm có một hoặc nhiều Con trỏ Ký hiệu đối tượng JavaScript (JavaScript Object Notation, JSON), mà chỉ báo một hoặc nhiều đoạn.

Trong một số phương án, chính sách bảo vệ còn chỉ báo, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ. Trong trường hợp này, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ có thể bao gồm sự bảo vệ bảo mật và/hoặc sự bảo vệ toàn vẹn.

Các phương án ở đây cũng gồm có máy, các chương trình máy tính, và các bộ mang (ví dụ, các phương tiện không chuyển tiếp đọc được bởi máy tính) tương ứng. Ví dụ, các phương án ở đây cũng gồm có thiết bị mạng được tạo cấu hình cho sự sử dụng trong một trong nhiều miền mạng lõi khác nhau của hệ thống truyền thông không dây. Thiết bị mạng bao gồm hệ mạch truyền thông và hệ mạch xử lý. Hệ mạch xử lý có thể được tạo cấu hình để để nhận, qua hệ mạch truyền thông, thông điệp mà đã, hoặc là để, được truyền giữa các miền mạng lõi khác nhau. Hệ mạch xử lý có thể cũng được tạo cấu hình để áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn của nội dung của trường trong thông điệp theo chính sách bảo vệ mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ. Hệ mạch xử lý có thể còn được tạo cấu hình để gửi chuyển tiếp thông điệp, với sự bảo vệ an toàn liên miền được áp dụng hoặc được loại bỏ đối với một hoặc nhiều đoạn, về phía đích của thông điệp qua hệ mạch truyền thông.

Các phương án còn gồm có thiết bị mạng bao gồm hệ mạch truyền thông và hệ mạch xử lý. Hệ mạch xử lý được tạo cấu hình để thu được chính sách bảo vệ mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung của trường trong thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ, trong đó thông điệp là để được truyền giữa các miền mạng lõi khác nhau của hệ thống truyền thông không dây. Hệ mạch xử lý cũng được tạo cấu hình để truyền chính sách bảo vệ qua hệ mạch truyền thông.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ khối của hệ thống truyền thông không dây theo một số phương án.

Fig.2A là sơ đồ khối của trường trong thông điệp đối với đó sự bảo vệ an toàn liên miền được áp dụng theo một số phương án.

Fig.2B là sơ đồ khối của nội dung ví dụ của trường trong thông điệp đối với đó sự bảo vệ an toàn liên miền được áp dụng theo một số phương án.

Fig.3 là sơ đồ tiến trình cuộc gọi của quy trình cho một hoặc nhiều máy ủy nhiệm (proxy) để thu được chính sách bảo vệ theo một số phương án.

Fig.4 là sơ đồ tiến trình cuộc gọi của quy trình cho một hoặc nhiều máy ủy nhiệm để thu được chính sách bảo vệ theo các phương án khác.

Fig.5 là sơ đồ tiến trình logic của phương pháp được thực hiện bởi thiết bị mạng theo một số phương án.

Fig.6 là sơ đồ tiến trình logic của phương pháp được thực hiện bởi thiết bị mạng theo các phương án khác.

Fig.7 là sơ đồ khối của hệ thống truyền thông không dây theo một số phương án.

Fig.8 là sơ đồ tiến trình cuộc gọi của quy trình để bảo vệ thông điệp truyền giữa các miền mạng lõi theo một số phương án.

Fig.9A là sơ đồ khối của thiết bị mạng theo một số phương án.

Fig.9B là sơ đồ khối của thiết bị mạng theo các phương án khác.

Fig.10A là sơ đồ khối của thiết bị mạng theo các phương án vẫn còn khác.

Fig.10B là sơ đồ khối của thiết bị mạng theo các phương án khác nữa.

Mô tả chi tiết sáng chế

Fig.1 thể hiện hệ thống truyền thông không dây 10 theo một số phương án. Hệ thống 10 gồm có một hoặc nhiều mạng truy nhập rađio (radio access network, RAN) 14 mà kết nối theo cách không dây các thiết bị không dây (wireless device) 12 với một hoặc nhiều mạng lõi (core network, CN) 16, ví dụ, của một hoặc nhiều mạng di động mặt đất công cộng (public land mobile network, PLMN). (Các) CN 16 đến lượt kết nối các thiết bị không dây 12 với một hoặc nhiều mạng dữ liệu 18, ví dụ, Internet, mạng điện thoại chuyển mạch công cộng (public switched telephone network, PSTN), v.v..

(Các) CN 16 trong một số phương án có kiến trúc dựa trên dịch vụ mà tác dụng đòn bẩy đối với các sự tương tác dựa trên dịch vụ giữa các chức năng mạng (network function, NF) CN, hai trong số chúng được thể hiện như các NF 20, 30. Mỗi NF 20, 30 có thể được thi hành bởi thiết bị mạng hoặc là như phần tử mạng trên phần cứng được

dành riêng, như phiên bản phần mềm chạy trên phần cứng được dành riêng, hoặc là như chức năng được ảo hóa được tạo phiên bản trên nền tảng thích hợp, ví dụ, trên cơ sở hạ tầng đám mây. Tại đó hệ thống 10 là hệ thống 5G, chẳng hạn, các NF trong mặt phẳng điều khiển có thể gồm có chức năng quản lý truy nhập và tính di động (access and mobility management function, AMF), chức năng quản lý phiên (session management function, SMF), chức năng điều khiển chính sách (policy control function, PCF), chức năng máy chủ xác thực (authentication server function, AUSF), chức năng quản lý dữ liệu thống nhất (unified data management, UDM), v.v..

NF có thể cung cấp các dịch vụ của nó cho các NF được phép khác mà tiêu dùng các dịch vụ đó. NF có thể bằng cách đó đảm nhiệm vai trò nhà cung cấp như nhà cung cấp của dịch vụ (nhà cung cấp dịch vụ NF) và/hoặc vai trò người tiêu dùng như người tiêu dùng của dịch vụ (người tiêu dùng dịch vụ NF). Trong một ví dụ, NF 20 vận hành như người tiêu dùng dịch vụ NF để tiêu dùng các dịch vụ được cung cấp bởi NF 30 như nhà cung cấp dịch vụ NF. Bất kể, như một phần của, hoặc để cho, nhà cung cấp dịch vụ NF cung cấp các dịch vụ của nó cho người tiêu dùng dịch vụ NF, các NF 20, 30 trao đổi sự truyền thông ở dạng của các thông điệp. Trong một số phương án, tuy nhiên, các NF 20, 30 ở trong các PLMN khác nhau. Trong các phương án này và các phương án khác, sau đó, các thông điệp này phải được truyền giữa các miền mạng lõi khác nhau.

Fig.1 thể hiện là các máy ủy nhiệm (proxy) 40, 50 tạo thuận lợi cho sự gửi thông điệp liên miền (inter-domain messaging). Mỗi máy ủy nhiệm 40, 50 được tạo cấu hình như máy ủy nhiệm cho miền mạng lõi tương ứng. Tại đó các NF 20, 30 ở trong các PLMN khác nhau, chẳng hạn, các máy ủy nhiệm 40, 50 có thể là các máy ủy nhiệm mép (ví dụ, ở dạng của các máy ủy nhiệm bảo vệ mép an toàn, security edge protection proxy, SEPP) ở mép của PLMN tương ứng. Mỗi máy ủy nhiệm 40, 50 chặn các thông điệp (ví dụ, ở lớp ứng dụng) mà đang đến với và/hoặc đang đi ra từ miền đó, ví dụ, để kiểm tra và/hoặc lọc các thông điệp (ví dụ, cho sự ác ý), để thực hiện sự cân bằng tải, hoặc tương tự. Các máy ủy nhiệm 40, 50 trong một số phương án giấu tôpô của miền mạng lõi tương ứng của chúng. Các máy ủy nhiệm 40, 50 cũng bảo vệ các thông điệp được truyền giữa các miền mạng lõi.

Nói riêng hơn về vấn đề này, Fig.1 thể hiện như ví dụ là NF 20 là nguồn của thông điệp 60 (ví dụ, thông điệp lớp ứng dụng) để được truyền đến NF 30 như đích của thông điệp 60. Với các NF 20, 30 trong các miền mạng lõi khác nhau, máy ủy nhiệm 40 nhận (ví dụ, chặn) thông điệp 60 trước khi thông điệp 60 được truyền qua biên miền mạng lõi. Máy ủy nhiệm 40 áp dụng sự bảo vệ an toàn liên miền 70 đối với thông điệp 60. Tại đó sự bảo vệ 70 gồm có sự bảo vệ bảo mật, ví dụ, sự áp dụng của sự bảo vệ 70 có thể bao hàm sự mật mã hóa. Như một sự lựa chọn hoặc ngoài ra, tại đó sự bảo vệ 70 gồm có sự bảo vệ toàn vẹn, sự áp dụng của sự bảo vệ 70 có thể bao hàm sự bổ sung của kiểm tra tổng (checksum), Mã xác thực thông điệp (Message Authentication Code, MAC), chữ ký, hoặc thông tin khác để phát hiện sự can thiệp thông điệp. Trong sự kiện bất kỳ, máy ủy nhiệm 40 sau đó gửi chuyển tiếp thông điệp 60, với sự bảo vệ 70 được áp dụng, về phía NF 30 như đích 30 của thông điệp. Máy ủy nhiệm 50 nhận (ví dụ, chặn) thông điệp 60 đến với miền mạng lõi của NF 30. Máy ủy nhiệm 50 loại bỏ sự bảo vệ an toàn liên miền 70 (ví dụ, nhờ thực hiện sự giải mật mã và/hoặc sự xác nhận và loại bỏ kiểm tra tổng). Máy ủy nhiệm 50 sau đó gửi chuyển tiếp thông điệp 60 về phía NF 30 như đích 30 của thông điệp.

Theo một số phương án, sự bảo vệ an toàn liên miền 70 được áp dụng đối với một hoặc nhiều đoạn hoặc phần của thông điệp 60, ví dụ, sao cho sự bảo vệ có thể được áp dụng theo cách chọn lọc đối với chỉ các đoạn nhất định của thông điệp 60 hơn là so với phải được áp dụng đối với toàn bộ thông điệp 60. Trên thực tế, trong một số phương án, sự bảo vệ 70 được áp dụng đối với một hoặc nhiều đoạn của nội dung của trường 62 nhất định trong thông điệp 60. Trường 62 về vấn đề này có thể được định nghĩa trước (ví dụ, dựa trên giao thức theo đó thông điệp 60 được tạo ra) như có nội dung của loại và/hoặc mục đích nhất định. Trường 62 trong một số phương án có thể cũng được tham chiếu đến như phần tử hoặc phần tử thông tin. Theo cách này, sự bảo vệ có thể được áp dụng theo cách chọn lọc đối với (các) đoạn nhất định của nội dung của trường đã cho, hơn là so với toàn bộ nội dung của trường.

Fig.2A thể hiện ví dụ. Như được thể hiện trên Fig.2A, nội dung của trường 62 có nhiều đoạn 62A, 62B, và 62C. Tất cả các đoạn này có thể có cùng loại và/hoặc mục đích để sao cho cùng nhau tạo thành nội dung của trường. Nhưng sự bảo vệ 70 có thể được

áp dụng theo cách chọn lọc đối với đoạn 62B, đối với sự loại trừ của các đoạn 62A và 62C. Trong một số phương án, ví dụ, máy ủy nhiệm 50 trích đoạn 62B từ trường 62 và áp dụng sự bảo vệ 70 theo cách chọn lọc đối với đoạn 62B được trích (ví dụ, nhờ mật mã hóa theo cách chọn lọc đoạn 62B và/hoặc tạo ra kiểm tra tổng theo cách chọn lọc cho đoạn 62B). Các đoạn 62A và 62C có thể vẫn không được bảo vệ. Máy ủy nhiệm 60 vào lúc nhận thông điệp 60 có thể đến lượt trích đoạn 62B từ trường 62 và loại bỏ sự bảo vệ 70 theo cách chọn lọc từ đoạn 62B được trích (ví dụ, nhờ giải mật mã theo cách chọn lọc đoạn 62B và/hoặc xác nhận và loại bỏ kiểm tra tổng cho đoạn 62B).

Fig.2B minh họa ví dụ đặc trưng của nội dung của trường trong một số phương án tại đó thông điệp 60 là thông điệp Giao thức chuyển tải siêu văn bản (HyperText Transfer Protocol, HTTP) và trường 62 là trường HTTP (ví dụ, thân hoặc một phần của thân của thông điệp HTTP, hoặc trường trong phần đầu hoặc phần đầu giả (pseudo) HTTP). Như được thể hiện, thông điệp 60 là yêu cầu GET HTTP (LẤY HTTP) và trường 62 là trường PATH (ĐƯỜNG). Nội dung của trường PATH là Phần tử nhận dạng tài nguyên đồng nhất (Uniform Resource Identifier, URI) yêu cầu. Trong trường hợp này, sau đó, sự bảo vệ 70 có thể được áp dụng đối với một hoặc nhiều đoạn của URI yêu cầu trong trường PATH. Thực vậy, nội dung của trường PATH (cụ thể là, URI yêu cầu) trong ví dụ này chứa nhiều đoạn 62A, 62B, và 62C, với sự bảo vệ 70 được áp dụng theo cách chọn lọc đối với chỉ đoạn 62B của URI yêu cầu. Đoạn 62B trong ví dụ này gồm có phần tử nhận dạng thuê bao ở dạng của Phần tử nhận dạng thuê bao di động quốc tế (International Mobile Subscriber Identifier, IMSI). Các đoạn 62A và 62C khác có thể vẫn không được bảo vệ.

Sự bảo vệ an toàn liên miền chọn lọc của các đoạn nhất định của thông điệp 60 (ví dụ, một hoặc nhiều đoạn của nội dung của trường 62) theo một số phương án có thể bảo hộ theo cách thuận lợi các đoạn nhất định đó chống lại sự can thiệp và/hoặc sự kiểm tra không được phép, trong khi cùng một lúc làm cho các thực thể có khả năng đọc và/hoặc sửa đổi các phần khác. Ví dụ, nhà cung cấp trao đổi liên mạng mà cung cấp sự kết nối giữa các miền mạng lõi khác nhau có thể đọc và/hoặc sửa đổi các đoạn không được bảo vệ khi cần để đưa ra các dịch vụ cho các nhà vận hành mạng. Độ chi tiết của sự bảo vệ bởi vậy có thể được điều chỉnh hẹp đối với độ chi tiết của nội dung (ví dụ,

nhạy cảm) trên thực tế cần sự bảo vệ. Điều này tránh sự bảo vệ quá rộng mà gây nguy hiểm cho sự sử dụng nội dung khác của các thực thể khác và/hoặc có thể tăng theo cách không cần thiết các tài nguyên truyền thông hoặc công suất xử lý.

Đáng chú ý, một số phương án ở đây khai thác chính sách bảo vệ 80 để hiện thực hóa sự bảo vệ an toàn liên miền chọn lọc này của các đoạn nhất định của thông điệp 60 (ví dụ, một hoặc nhiều đoạn của nội dung của trường 62). Chính sách bảo vệ 80 gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của thông điệp 60 mà sự bảo vệ an toàn liên miền 70 là để được áp dụng (ví dụ, bởi máy ủy nhiệm 40) hoặc được loại bỏ (ví dụ, bởi máy ủy nhiệm 50). Trong một số phương án, sau đó, thông tin này chỉ báo đối với một hoặc nhiều đoạn nào của nội dung của trường 62 mà sự bảo vệ an toàn liên miền 70 là để được áp dụng hoặc được loại bỏ. Lưu ý là thông tin có thể chỉ báo theo cách có hiệu quả đối với một hoặc nhiều đoạn nào mà sự bảo vệ 70 là để được áp dụng/được loại bỏ, hoặc là theo cách rõ ràng nhờ chỉ báo (các) đoạn đối với đó sự bảo vệ 70 là để được áp dụng/được loại bỏ hoặc là theo cách ngầm nhờ chỉ báo (các) đoạn đối với đó sự bảo vệ 70 là *không* để được áp dụng/được loại bỏ. Chính sách bảo vệ 80 trong một phương án cũng chỉ báo, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền 70 để được áp dụng hoặc được loại bỏ (ví dụ, sự bảo vệ bảo mật và/hoặc toàn vẹn).

Ví dụ, trong một số phương án, thông tin trong chính sách bảo vệ 80 gồm có một hoặc nhiều biểu thức thông thường mà chỉ báo một hoặc nhiều đoạn. Biểu thức thông thường về vấn đề này có thể là trình tự của các ký tự mà định nghĩa mẫu tìm kiếm. Mẫu tìm kiếm có thể đến lượt được sử dụng bởi các thuật toán tìm kiếm để tìm mẫu nhất định của các ký tự trong thông điệp 60 (ví dụ, trong nội dung của trường).

Chẳng hạn, biểu thức thông thường có thể sử dụng được để tìm đoạn 62B trên Fig.2B (ví dụ, IMSI) có thể là "^/udm-sdm/v1/([^/?#]+)/nssai$". Trong ví dụ này, ký tự dấu mũ (cụ thể là, ^) và ký tự dấu đô la (cụ thể là, $) là các neo mà không “tiêu dùng” (consume) các ký tự bất kỳ, mà thay vào đó buộc mẫu vào phần bắt đầu và phần kết thúc của chuỗi được tìm kiếm. Các ký tự ([^/?#]+) trong biểu thức thông thường bắt giữ mẫu con hoặc nhóm con bất kỳ mà gồm có một hoặc nhiều sự xuất hiện của ký tự bất kỳ ngoại trừ ký tự gạch chéo lên (/), ký tự dấu chấm hỏi (?), và ký tự dấu thăng (#). Mẫu

con hoặc nhóm con được bắt giữ này được đưa ra từ thuật toán tìm kiếm. Do đó, việc phân tách nội dung của trường sử dụng biểu thức thông thường cung cấp mẫu con "imsi-214050123456789". Sự bảo vệ 70 có thể bởi vậy được áp dụng theo cách chọn lọc đối với chỉ mẫu con này, đối với sự loại trừ của các đoạn 62A và 62C khác của nội dung của trường.

Đương nhiên, biểu thức thông thường chỉ là một cách để chỉ báo đoạn như được sử dụng ở đây. Chính sách bảo vệ 80 có thể gồm có loại bất kỳ của biểu thức, mẫu, cú pháp, ngôn ngữ, dấu phân cách, con trỏ, quy tắc, hoặc thông tin khác mà chỉ báo một hoặc nhiều đoạn. Ví dụ, trong một số phương án, thông tin có thể là thông tin bất kỳ mà chỉ báo mẫu, dấu hiệu (token), hoặc chuỗi con bên trong chuỗi rộng hơn. Trong ví dụ trên Fig.2B, chẳng hạn, thông tin có thể như một sự lựa chọn chỉ báo đoạn 62B như phân đoạn đường thứ ba trong nội dung của trường; nghĩa là, mẫu con hoặc nhóm con của các ký tự xuất hiện giữa các dấu hiệu hoặc dấu phân cách thứ ba và thứ tư ở dạng của gạch chéo lên (/). Trong các phương án vẫn còn khác, thông tin có thể gồm có một hoặc nhiều phạm vi của các byte trong trường 62, và/hoặc một hoặc nhiều phạm vi của các bit trong trường 62, mà chỉ báo một hoặc nhiều đoạn.

Trong các phương án khác nữa, thông tin trong chính sách bảo vệ 80 gồm có một hoặc nhiều Con trỏ Ký hiệu đối tượng JavaScript (JavaScript Object Notation, JSON), mà chỉ báo một hoặc nhiều đoạn. Con trỏ JSON (ví dụ, như được định nghĩa trong RFC 6901) là cú pháp chuỗi để nhận dạng trị số đặc trưng trong tài liệu JSON. Con trỏ JSON có thể được biểu thị trong các trị số chuỗi JSON và/hoặc các phần tử nhận dạng phân mảnh URI. Con trỏ JSON nói riêng là chuỗi Unicode chứa trình tự của không (zero) hoặc nhiều dấu hiệu tham chiếu hơn. Mỗi dấu hiệu được đặt tiền tố bởi ký tự gạch chéo lên '/'. Trong các phương án này và các phương án khác, sau đó, chính sách bảo vệ 80 như ví dụ có thể chỉ báo một hoặc nhiều đoạn của nội dung trong thân hoặc trọng tải của thông điệp HTML, tại đó thân hoặc trọng tải đó gồm có tài liệu JSON.

Bất kể bản chất riêng của thông tin trong chính sách bảo vệ 80, các ví dụ này minh họa là chính sách bảo vệ 80 trong một số phương án chỉ báo (các) đoạn (đối với đó sự bảo vệ 70 là để được áp dụng hoặc được loại bỏ) với thông tin mà bất khả tri đối với, không phụ thuộc vào, và/hoặc có thể áp dụng được theo cách tổng quát đối với bất

kỳ của nội dung trường/thông điệp cơ bản (underlying) hoặc giao thức truyền của thông điệp. Chính sách bảo vệ 80 có thể chẳng hạn có khả năng chỉ báo (các) đoạn bất kỳ của nội dung trong trường 62 với cùng loại chung của thông tin (ví dụ, biểu thức thông thường), bất kể loại, kết cấu, hoặc định dạng của nội dung của trường. Nghĩa là, trong một phiên bản thông tin có thể được tạo thành (ví dụ, như biểu thức thông thường riêng) để chỉ báo đoạn nhất định của nội dung trong trường 62 dựa trên nội dung có loại hoặc định dạng nhất định (ví dụ, IMSI), nhưng trong phiên bản khác thông tin có thể được tạo thành (ví dụ, như biểu thức thông thường khác nhau) để chỉ báo đoạn khác nhau của nội dung trong trường 62 dựa trên nội dung có loại hoặc định dạng khác nhau (ví dụ, phần tử nhận dạng ô). Nhưng thông tin trong cả hai phiên bản có cùng đặc điểm chung (ví dụ, cả hai là các biểu thức thông thường), để sao cho theo cách phổ biến làm cho các máy ủy nhiệm 40, 50 có thể nhận dạng (các) đoạn bất kỳ mà không quan tâm đến việc liệu hoặc cách thức loại, kết cấu, hoặc định dạng của nội dung cơ bản tiến hóa. Do đó, việc tạo cấu hình các máy ủy nhiệm 40, 50 để hiểu hoặc xử lý theo cách tổng quát các biểu thức thông thường hoặc thông tin khác trong chính sách bảo vệ 80 trang bị đủ cho các máy ủy nhiệm 40, 50 để áp dụng hoặc loại bỏ theo cách chọn lọc sự bảo vệ 70 đối với đoạn bất kỳ của nội dung trong thông điệp 60 hoặc trường 62, ngay cả không có việc các máy ủy nhiệm 40, 50 được tạo cấu hình để hiểu nội dung đó theo cách đặc trưng hơn. Trong ví dụ trên Fig.2B, sau đó, máy ủy nhiệm cần hiểu theo cách đơn giản cách thức để xử lý biểu thức thông thường để bảo vệ đoạn 62B, mà không phải hiểu theo cách đặc trưng hơn cách thức để nhận dạng IMSI. Điều này có nghĩa các máy ủy nhiệm 40, 50 có thể vẫn không biết gì về cách thức nội dung cơ bản đó thay đổi hoặc tiến hóa (ví dụ, về mặt dạng hoặc kết cấu của nó), như đáp lại sự đưa vào của các thực thể (ví dụ, các chức năng mạng) và/hoặc các dịch vụ (ví dụ, được biểu diễn bởi các URI HTTP của chúng) mới đối với hệ thống 10. Trong một số phương án, sau đó, nó là thông tin trong chính sách bảo vệ 80 (ví dụ, các biểu thức thông thường) mà thay đổi hoặc tiến hóa theo cách động để giải thích cho các sự thay đổi hoặc sự tiến hóa đối với nội dung cơ bản của thông điệp 60 (ví dụ, về mặt kết cấu hoặc định dạng của nó), hơn là so với sự cấu hình chung của các máy ủy nhiệm để nhận dạng (các) đoạn sử dụng loại thông tin đó.

Như một sự lựa chọn hoặc ngoài ra đối với các phương án ở trên, chính sách bảo vệ 80 cho sự bảo vệ an toàn liên miền 70 của thông điệp 60 có thể được nhận và/hoặc

được cập nhật theo cách động bởi máy ủy nhiệm 40 hoặc 50. Sự lấy ra và/hoặc được cập nhật động của chính sách 80 có thể giải thích cho các sự thay đổi hoặc sự tiến hóa đối với nội dung của thông điệp 60. Cách này, sự cấu hình của chính máy ủy nhiệm 40 hoặc 50 không cần được cập nhật (theo cách thủ công) để giải thích cho sự thay đổi hoặc sự tiến hóa như vậy. Theo một số phương án, điều này có thể cung cấp theo cách thuận lợi sự bảo vệ linh hoạt mà tiến hóa cùng với các sự thay đổi định dạng thông điệp (ví dụ, có thể quy cho sự tiến hóa của các chức năng mạng hoặc dịch vụ trong mạng lõi), trong khi giảm thiểu hoặc ít nhất giảm tổng phí vận hành và/hoặc quản trị mà sẽ nếu không thì được đòi hỏi cho tính linh hoạt như vậy.

Fig.3 ví dụ minh họa một số phương án tại đó máy ủy nhiệm 40 và/hoặc 50 tìm ra theo cách động chính sách bảo vệ 80 từ một hoặc nhiều chức năng kho mạng (network repository function, NRF) 90, ví dụ, đáp lại việc nhận thông điệp 60. Như được thể hiện, NF 20 như nguồn của thông điệp 60 truyền thông điệp 60, mà được chặn bởi hoặc nếu không thì được nhận bởi máy ủy nhiệm 40 (Bước 1). Đáp lại việc nhận thông điệp 60, máy ủy nhiệm 40 truyền yêu cầu tìm ra 92 đến dịch vụ tìm ra (trong miền mạng lõi của nó) yêu cầu sự tìm ra của chính sách bảo vệ 80 để bảo vệ thông điệp 60 (Bước 2). Dịch vụ tìm ra được thể hiện ở đây như được thi hành bởi chức năng kho mạng (network repository function, NRF) 90A nhưng trong các phương án khác có thể được thi hành bởi chức năng độc lập được cùng định vị với NRF hoặc bởi các chức năng hoặc thiết bị mạng khác. Bất kể, máy ủy nhiệm 40 nhận chính sách bảo vệ 80 đáp lại yêu cầu tìm ra (Bước 3). Máy ủy nhiệm 40 áp dụng sự bảo vệ đối với một hoặc nhiều đoạn của thông điệp 60 (ví dụ, một hoặc nhiều đoạn của nội dung của trường 62) được xác định theo chính sách bảo vệ 80 và truyền thông điệp 60 được bảo vệ qua biên miền mạng lõi đến máy ủy nhiệm 50 (Bước 4). Đáp lại việc nhận thông điệp 60, máy ủy nhiệm 50 đến lượt truyền yêu cầu tìm ra 94 đến dịch vụ tìm ra (trong miền mạng lõi của nó), được thể hiện như được thi hành bởi NRF 90B (Bước 5). Đáp lại yêu cầu tìm ra, máy ủy nhiệm 50 nhận chính sách bảo vệ 80 từ dịch vụ tìm ra (Bước 6). Máy ủy nhiệm 50 loại bỏ sự bảo vệ khỏi một hoặc nhiều đoạn của thông điệp 60 (ví dụ, một hoặc nhiều đoạn của nội dung của trường 62) được xác định theo chính sách bảo vệ 80 và truyền thông điệp 60 (không được bảo vệ) về phía NF 30 như đích của thông điệp (Bước 7).

Mặc dù không được thể hiện, trong một số phương án, nguồn và/hoặc đích của thông điệp cung cấp chính sách bảo vệ 80 có thể áp dụng được cho thông điệp 60 cho dịch vụ tìm ra trong một hoặc nhiều trong các miền mạng lõi, ví dụ, cho sự tìm ra muộn hơn của chính sách 80 đó như được thể hiện trên Fig.3. Ví dụ, tại đó NF 30 là NF nhà cung cấp mà cung cấp dịch vụ cho NF 20 như NF người tiêu dùng, và thông điệp 60 là thông điệp mà NF 20 gửi đến NF 30 để tiêu dùng dịch vụ đó, NF 30 như NF nhà cung cấp trong một số phương án cung cấp hồ sơ dịch vụ của nó cho NRF 90B (ví dụ, như một phần của sự đăng ký ban đầu hoặc sự cập nhật đăng ký), gồm có chính sách bảo vệ 80 có thể áp dụng được cho một hoặc nhiều thông điệp được sử dụng để tiêu dùng dịch vụ được cung cấp bởi NF 30. NRF 90B có thể đến lượt phân phối hoặc nếu không thì cung cấp hồ sơ dịch vụ hoặc ít nhất chính sách bảo vệ 80 cho NRF 90A, cho sự tìm ra muộn hơn bởi các NF người tiêu dùng tiềm năng.

Trong các phương án khác nữa, tuy nhiên, máy ủy nhiệm 40 và/hoặc 50 có thể thuê bao để nhận theo cách chủ động các chính sách bảo vệ mới hoặc được cập nhật từ NRF 90A và/hoặc 90B. Trong các phương án này và các phương án khác, máy ủy nhiệm 40 và/hoặc 50 có thể lưu trữ (ví dụ, nhớ đệm (cache)) các chính sách bảo vệ được nhận trong dự đoán sự sử dụng muộn hơn để bảo vệ các thông điệp được truyền giữa các miền mạng lõi.

Fig.4 ngược lại thể hiện các phương án khác tại đó máy ủy nhiệm 40 và/hoặc 50 nhận chính sách bảo vệ 80 từ thiết bị hoặc các chức năng mạng trong đường mà thông điệp 60 đi từ nguồn đến đích của thông điệp 60. Nói riêng, Fig.4 thể hiện là NF 20 như nguồn thông điệp truyền thông điệp 60 với chính sách bảo vệ 80 được nhúng hoặc nếu không thì được gồm có trong chính thông điệp 60 (ví dụ, trong phần đầu của thông điệp) (Bước 1). Theo cách này, máy ủy nhiệm 40 nhận chính sách bảo vệ 80 từ nguồn của thông điệp 60. Máy ủy nhiệm 40 sau đó truyền thông điệp 60 được bảo vệ qua biên miền mạng lõi, lần nữa với chính sách bảo vệ 80 được gồm có trong thông điệp 80 (Bước 2). Máy ủy nhiệm 50 do đó nhận chính sách bảo vệ 80 từ máy ủy nhiệm 40 trong miền mạng lõi khác nhau. Máy ủy nhiệm 50 có thể sau đó loại bỏ sự bảo vệ của thông điệp 60 và gửi chuyển tiếp nó về phía NF 30 như đích (Bước 3).

Xét thấy các sự biến đổi và các sự sửa đổi ở trên, thiết bị mạng trong một số phương án nói chung là thực hiện phương pháp 100 được thể hiện trên Fig.5. Thiết bị mạng có thể được tạo cấu hình như máy ủy nhiệm cho một trong nhiều miền mạng lõi khác nhau của hệ thống truyền thông không dây 10. Ví dụ, phương pháp 100 có thể được thực hiện bởi thiết bị mạng được tạo cấu hình như máy ủy nhiệm 40 hoặc máy ủy nhiệm 50. Phương pháp 100 như được thể hiện gồm có bước nhận thông điệp 60 mà đã, hoặc là để, được truyền giữa các miền mạng lõi khác nhau (Khối 110). Phương pháp 100 có thể cũng gồm có bước nhận chính sách bảo vệ 80 mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của thông điệp 60 (ví dụ, một hoặc nhiều đoạn của nội dung của trường 62 trong thông điệp 60) mà sự bảo vệ an toàn liên miền 70 là để được áp dụng hoặc được loại bỏ (Khối 120). Phương pháp 100 có thể còn gồm có bước áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn theo chính sách bảo vệ 80 (Khối 130). Phương pháp 100 trong một số phương án có thể cũng gồm có bước gửi chuyển tiếp thông điệp 60, với sự bảo vệ an toàn liên miền được áp dụng hoặc được loại bỏ đối với một hoặc nhiều đoạn, về phía đích của thông điệp 60 (Khối 140).

Trong một số phương án, phương pháp còn bao gồm bước, đáp lại việc nhận thông điệp 60, truyền yêu cầu tìm ra đến chức năng kho mạng (network repository function, NRF) yêu cầu sự tìm ra của chính sách bảo vệ 80 để bảo vệ thông điệp 60, và nhận chính sách bảo vệ đáp lại yêu cầu tìm ra. Như một sự lựa chọn, phương pháp có thể bao gồm bước nhận chính sách bảo vệ 80 từ thiết bị mạng trong đường mà thông điệp đi từ nguồn của thông điệp đến đích của thông điệp.

Cũng xét thấy các sự biến đổi và các sự sửa đổi ở trên, thiết bị mạng trong các phương án khác nói chung là thực hiện phương pháp 200 được thể hiện trên Fig.6 để tạo thuận lợi cho sự bảo vệ của thông điệp 60 được truyền giữa các miền mạng lõi khác nhau của hệ thống truyền thông không dây 10. Phương pháp 200 có thể được thực hiện ví dụ bởi thiết bị mạng thi hành NF 20, máy ủy nhiệm 40, máy ủy nhiệm 50, NF 30, hoặc (các) NRF 90. Phương pháp 200 như được thể hiện về vấn đề này gồm có bước thu được chính sách bảo vệ 80 mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của thông điệp 60 (ví dụ, một hoặc nhiều đoạn của nội dung của trường 62 trong thông điệp 60) mà sự bảo vệ an toàn liên miền 70 là để được áp dụng hoặc được loại bỏ

(Khối 210). Phương pháp 200 có thể cũng gồm có bước truyền chính sách bảo vệ 80 (Khối 220).

Ví dụ, trong một số phương án, việc truyền chính sách bảo vệ bao gồm truyền chính sách bảo vệ đến thiết bị mạng được tạo cấu hình, như một máy ủy nhiệm của các miền mạng lõi khác nhau, để áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn theo chính sách bảo vệ.

Như một sự lựa chọn hoặc ngoài ra, phương pháp có thể được thực hiện bởi thiết bị mạng mà thi hành chức năng kho mạng (network repository function, NRF) và có thể còn bao gồm nhận yêu cầu tìm ra yêu cầu sự tìm ra của chính sách bảo vệ để bảo vệ thông điệp, và truyền chính sách bảo vệ đáp lại yêu cầu tìm ra.

Như một sự lựa chọn, phương pháp có thể được thực hiện bởi thiết bị mạng trong đường mà thông điệp đi từ nguồn của thông điệp đến đích của thông điệp (ví dụ, bởi NF 20, máy ủy nhiệm 40, máy ủy nhiệm 50, hoặc NF 30).

Một số phương án sẽ tiếp đây được thảo luận với sự liên quan riêng đối với có thể áp dụng được của chúng vào các thời điểm đối với 5G.

3GPP đang tiếp tục làm việc 5G, và Mạng lõi được kết hợp của nó (5GC) mà cung cấp các dịch vụ cho các người dùng kết nối, từ sự xác thực đối với sự chỉ định địa chỉ IP và sự định tuyến của các gói. Tuy nhiên, mạng lõi 5G khác nhau đáng kể với các thế hệ trước.

Một trong các sự thay đổi trong kiến trúc 5G là để thi hành kiến trúc được gọi là Kiến trúc dựa trên dịch vụ (Service-Based Architecture, SBA). Trong kiến trúc mới này, số lượng của các giao diện trong mạng lõi (gồm có các giao diện chuyển vùng) được thay đổi từ các giao diện lập trình ứng dụng (application programming interface, API) dựa trên web, kiểu viễn thông kế thừa đến hiện đại. Các chi tiết của các API này đang hiện thời được tiếp tục làm việc ở nhóm SA2 3GPP, trong tài liệu kiến trúc mạng lõi 5G 23.501 và 23.502, cũng như trong các nhóm CT 3GPP.

Có vài sự lựa chọn để phát triển và thi hành kiến trúc dựa trên dịch vụ. Trong vài khả năng, nhóm CT4 3GPP đã lựa chọn kiến trúc dựa trên mô hình kiến trúc Chuyển tải trạng thái đại diện (Representational State Transfer, REST). Trong mô hình này, các thực thể (các dịch vụ, các chức năng mạng, v.v.) khác nhau trong hệ thống 5G tương tác với nhau nhờ gọi ra các hành động trên cái được gọi là "tài nguyên" (resource), mà được

nhận dạng trong HTTP bởi Phần tử nhận dạng tài nguyên đồng nhất (Uniform Resource Identifier, URI). Sau đó, các hành động khác nhau để được gọi ra trong các thực thể hệ thống khác nhau được định nghĩa bởi các câu lệnh chuẩn HTTP khác nhau (ví dụ, GET, POST, PUT, DELETE, v.v.…), trong khi các thông điệp HTTP chuyển các đại diện của các tài nguyên bị ảnh hưởng trong trọng tải HTTP. Các đại diện này có thể được định dạng trong các ngôn ngữ lập mã dữ liệu khác nhau (ví dụ JSON).

Mạng lõi 5G có thể theo các sự đòi hỏi này: Giao thức chính: HTTP/2; Giao thức vận tải: TCP; Kiểu thiết kế API RESTful; Định dạng nối tiếp hóa dữ liệu: JSON; Các sự tương tác được khởi đầu máy chủ: "*Web-hook*"; và Ngôn ngữ định nghĩa giao diện: OpenAPI 3.0.0 (trước đây được biết đến như "Swagger").

Các chức năng mạng khác nhau trong Mạng lõi 5G bộc lộ các dịch vụ của chúng qua Giao diện lập trình ứng dụng (Application Programming Interface, API). API này định nghĩa các tài nguyên HTTP (Các phần tử nhận dạng tài nguyên đa năng, Universal Resource Identifier, URI), các sự vận hành được cho phép (GET, POST, PUT,…) và định dạng của dữ liệu được vận tải trong trọng tải thông điệp (thân thông điệp).

Trừ khi thông tin về các nhà cung cấp dịch vụ NF được tạo cấu hình theo cách cục bộ trên các người tiêu dùng dịch vụ NF tương ứng (đây có thể là trường hợp nếu dịch vụ NF hoặc NF được kỳ vọng ở trong cùng PLMN như NF người yêu cầu), các người tiêu dùng dịch vụ NF tìm ra và lựa chọn các nhà sản xuất dịch vụ NF theo cách động sử dụng Chức năng kho mạng (Network Repository Function, NRF). NRF là chức năng logic mà được sử dụng để duy trì hồ sơ NF của các phiên bản khả dụng của các nhà sản xuất dịch vụ NF và các dịch vụ được hỗ trợ của chúng, nhận Các yêu cầu tìm ra dịch vụ NF từ các người tiêu dùng dịch vụ NF, và cung cấp thông tin của các phiên bản khả dụng của các nhà sản xuất dịch vụ NF tương ứng cho người tiêu dùng dịch vụ NF yêu cầu.

Để làm cho có thể truy nhập đối với loại NF hoặc dịch vụ NF được yêu cầu, NF người yêu cầu khởi đầu sự tìm ra NF hoặc dịch vụ NF nhờ cung cấp loại của NF hoặc dịch vụ đặc trưng mà nó đang cố gắng để tìm ra (ví dụ chức năng quản lý phiên (session management function, SMF), chức năng tính cước chính sách (policy charging function, PCF), thiết bị người dùng (user equipment, UE), Báo cáo địa điểm) và các tham số dịch vụ khác (ví dụ thông tin liên quan đến sự tạo lát) cho NRF. Phụ thuộc vào mô hình định

tuyến thông điệp được chọn, NRF có thể cung cấp địa chỉ IP hoặc tên miền hoàn toàn hợp lệ (fully qualified domain name, FQDN) hoặc phần tử nhận dạng của các dịch vụ và/hoặc (các) phiên bản NF có liên quan cho NF người yêu cầu. Dựa trên thông tin đó, NF người yêu cầu có thể lựa chọn một phiên bản NF đặc trưng hoặc phiên bản NF mà có năng lực để cung cấp Dịch vụ NF riêng (ví dụ, phiên bản của PCF mà có thể cung cấp Sự cho phép chính sách).

Trong các trường hợp của sự chuyển vùng (nghĩa là, khi người dùng đang truy nhập mạng khác với mạng thường trú của anh ấy hoặc của cô ấy, tại đó người dùng có sự thuê bao của anh ấy/của cô ấy), sự truyền thông có thể được bảo vệ (ví dụ, bằng mật mã) giữa mạng tạm trú (visited network) và mạng thường trú, để bảo đảm là thông tin được gửi qua các mạng kết nối lẫn nhau không được kiểm tra hoặc được sửa đổi bởi các bên không được phép. Nhiệm vụ này được hoàn thành bởi phần tử mạng được gọi là SEPP (Security Edge Protection Proxy, Máy ủy nhiệm bảo vệ mép an toàn). Có thể có vSEPP (SEPP trong mạng tạm trú) và hSEPP (SEPP trong mạng thường trú) mà truyền thông qua giao diện N32.

Sự bảo vệ của sự truyền thông giữa các SEPP có thể là ở lớp ứng dụng. Trong một số phương án, sự bảo vệ toàn vẹn áp dụng đối với tất cả các thuộc tính được chuyển tải qua giao diện N32. Như một sự lựa chọn hoặc ngoài ra, một hoặc nhiều trong các thuộc tính sau đây có thể được bảo vệ bảo mật khi được gửi qua giao diện N32: Các vectơ xác thực; Tài liệu bằng mật mã (Cryptographic material); dữ liệu Địa điểm, ví dụ ID ô và ID ô vật lý; hoặc phần tử nhận dạng vĩnh cửu thuê bao (subscriber permanent identifier, SUPI) như Phần tử nhận dạng thuê bao di động quốc tế (International Mobile Subscriber Identifier, IMSI).

Như một phần của các chức năng của SEPP, một trong số chúng là để bảo vệ thông tin được gửi trên các trường khác nhau mà hợp thành các thông điệp HTTP. Các trường HTTP này có thể là, ví dụ, URI yêu cầu HTTP, các phần đầu HTTP, và các phần khác nhau của thân HTTP (hoặc trọng tải).

Sự kết nối giữa hai PLMN thường được hoàn thành qua các nhà cung cấp được gọi là các nhà cung cấp IPX. Ngoài sự kết nối thực tế, các nhà cung cấp IPX cũng thường đưa ra các dịch vụ bổ sung cho các nhà vận hành. Một số trong các dịch vụ này được dựa trên việc đọc và/hoặc thay đổi các trường trong các thông điệp được gửi giữa các

PLMN. Vì thế nó có thể mong muốn là các đoạn hoặc các trường thông điệp nhất định trên thực tế không được bảo vệ bằng mật mã khi được gửi qua giao diện N32 giữa vSEPP và hSEPP.

Tóm tắt, SEPP sẽ bảo vệ (mật mã hóa và/hoặc bảo vệ toàn vẹn) một số trong các trường hoặc các đoạn thông tin trong các thông điệp được gửi trên N32, và một số phần khác của các thông điệp mà SEPP sẽ để lại không được bảo vệ, ví dụ, để hiện thực hóa các dịch vụ bổ sung được cung cấp bởi các nhà cung cấp IPX.

Tuy nhiên, nếu loại mới của thông điệp được gửi qua N32 mà đã không được định nghĩa ở sự triển khai (roll-out) hoặc sự cập nhật cuối cùng của SEPP, thì các phần của thông điệp mà cần được bảo vệ không được biết theo cách rõ ràng đối với SEPP. Nó có thể mong muốn nữa là SEPP có năng lực để cung cấp các dịch vụ của nó mà không đòi hỏi sự nâng cấp phần mềm như kết quả của sự tiến hóa chức năng thông thường của Các chức năng mạng khác nhau trong Mạng lõi.

Một số phương án ở đây cung cấp theo cách thuận lợi chính sách mà định nghĩa các phần nào của thông điệp cần được bảo vệ, và chúng phải được bảo vệ theo cách nào (sự bảo mật, sự toàn vẹn). Trong một hoặc nhiều phương án, chính sách này được biểu thị trong ngôn ngữ hoặc "mặt nạ" (mask) mà là (sự so khớp mẫu) có thể áp dụng được cho các loại mới của các thông điệp. Theo cách này, chính sách có thể được biểu thị theo cách động và không cần để được biết ở sự triển khai hoặc sự cập nhật cuối cùng của SEPP. Các phương án ở đây cũng gồm có các luồng để báo cho SEPP về chính sách có thể áp dụng được cho thông điệp đặc trưng. Các phương án bằng cách đó cung cấp cách động và linh hoạt để bảo vệ theo cách chọn lọc các phần của các thông điệp được gửi trên N32, theo cách như vậy mà các thực thể thực hiện sự bảo vệ như vậy (sự mật mã hóa và/hoặc sự bảo vệ toàn vẹn) không phụ thuộc vào sự cấu hình tĩnh và không cần được thay đổi khi các thực thể (Các chức năng mạng) mới và các dịch vụ mới (được biểu diễn bởi các URI HTTP của chúng) được bổ sung đối với hệ thống.

Một số phương án cho phép sự áp dụng của cơ chế an toàn mà không làm ảnh hưởng đến thiết kế (API) của các dịch vụ giữa các PLMN thường trú (home) và tạm trú (visited). Ngoài ra hoặc như một sự lựa chọn, một số phương án cho phép sự bảo vệ (sự mật mã hóa và/hoặc sự bảo vệ toàn vẹn) của các phần tử thông tin nhạy cảm (như các nhận dạng người dùng, như là IMSI) được tìm trong các thông điệp HTTP trong lưu

lượng 5G được vận tải giữa các nhà vận hành mạng theo cách linh hoạt, không bị ràng buộc với sự định nghĩa hiện thời của các API dịch vụ, và được chuẩn bị cho sự đưa vào của các chức năng mạng, các dịch vụ và các API mới trong sự tiến hóa thêm nữa của Mạng lõi 5G.

Hai biến thể được thảo luận ở dưới cho các ví dụ của các luồng báo hiệu để báo cho SEPP về chính sách cho thông điệp đặc trưng. Fig.7 thể hiện ngữ cảnh ví dụ để thảo luận các biến thể 1 và 2.

Trong biến thể 1, SEPP truy vấn (query) NRF cho thông tin chính sách bảo vệ có thể áp dụng được. Như được thể hiện, chức năng mạng NF1 trong PLMN1 dự định để gửi thông điệp đến chức năng mạng NF2 trong PLMN2. Thông điệp được định tuyến qua SEPP1 và SEPP2 trong PLMN1 và PLMN2. Khi SEPP1 nhận thông điệp, nó kiểm tra liệu nó đã lưu trữ chính sách bảo vệ cho loại này của thông điệp mà chưa hết hạn. Nếu không có chính sách bảo vệ như vậy là khả dụng, thì SEPP1 truy vấn NRF trong PLMN1 (NRF1 được gọi).

Nếu NRF1 đã được truy vấn bởi SEPP1 về các chính sách bảo vệ có thể áp dụng được đối với thông điệp đặc trưng, thì NRF1 gửi các chính sách bảo vệ khả dụng đến SEPP1. NRF1 có thể cần truy vấn NRF2, NRF trong PLMN2. NRF1 có thể đã nhận các chính sách bảo vệ từ NF1 lúc đăng ký. NRF2 có thể đã nhận các chính sách bảo vệ từ NF2 lúc đăng ký.

Trước khi gửi chuyển tiếp thông điệp đến SEPP2, SEPP1 thực hiện sự bảo vệ (ví dụ, sự bảo vệ bằng mật mã) của thông điệp theo chính sách được nhận từ NRF1 và/hoặc NRF2. SEPP1 có thể gồm có chính sách bảo vệ trong thông điệp mà nó gửi chuyển tiếp. Lưu ý là SEPP "gửi chuyển tiếp" (forwarding) có thể sửa đổi thông điệp hoặc thậm chí đóng gói nó trong thông điệp khác.

Khi nhận thông điệp từ SEPP1, SEPP2 giải mật mã các phần được mật mã hóa của thông điệp và kiểm tra sự toàn vẹn của các phần được bảo vệ toàn vẹn của thông điệp. SEPP2 có thể sử dụng chính sách bảo vệ được nhận từ SEPP1 hoặc truy vấn NRF1 và/hoặc NRF2 như được đòi hỏi để lấy thông tin chính sách bảo vệ.

SEPP2 gửi chuyển tiếp thông điệp đến NF2.

Trong biến thể 2, ngược lại, NF mà gửi thông điệp (NF1) gồm có chính sách bảo vệ trong thông điệp. NF có thể đã nhận chính sách trong sự tìm ra dịch vụ (nếu nó là

người tiêu dùng dịch vụ) hoặc trong sự đăng ký dịch vụ (nếu nó là nhà sản xuất dịch vụ).

Nói riêng hơn về vấn đề này, chức năng mạng NF1 thực hiện sự tìm ra dịch vụ hoặc sự đăng ký dịch vụ ở NRF1, NRF trong PLMN của nó. Như một phần của sự tìm ra hoặc sự đăng ký ở trên, NRF1 có thể gồm có các chính sách bảo vệ của các loại thông điệp mà NF1 có thể gửi trong khi tiêu dùng hoặc sản xuất dịch vụ. Cho trường hợp của sự tìm ra, NRF1 có thể đã nhận chính sách bảo vệ từ NRF2.

Trong khi tiêu dùng hoặc sản xuất dịch vụ, NF1 dự định để gửi thông điệp đến NF2. Thông điệp được định tuyến qua SEPP1 và SEPP2. Trong thông điệp, NF1 gồm có chính sách bảo vệ mà là có thể áp dụng được cho thông điệp này. NF1 có thể đã nhận chính sách từ NRF1 hoặc NRF2, nhưng chính sách có thể như một sự lựa chọn bắt nguồn từ chính NF1.

Trước khi gửi chuyển tiếp thông điệp đến SEPP2, SEPP1 thực hiện sự bảo vệ của thông điệp theo chính sách được nhận từ NF1. Để bảo đảm là SEPP2 có năng lực để lấy ra thông điệp gốc, SEPP1 có thể gồm có thông tin mà cho phép SEPP2 biết các phần nào đã được bảo vệ. Điều này có thể ví dụ được giải quyết bởi SEPP1 gồm có chính sách bảo vệ trong thông điệp mà nó gửi chuyển tiếp. Một lần nữa lưu ý là SEPP "gửi chuyển tiếp" có thể sửa đổi thông điệp hoặc thậm chí đóng gói nó trong thông điệp khác.

Khi nhận thông điệp từ SEPP1, SEPP2 giải mật mã các phần được mật mã hóa của thông điệp và kiểm tra sự toàn vẹn của các phần được bảo vệ sự toàn vẹn của thông điệp. Ví dụ, SEPP2 có thể sử dụng chính sách bảo vệ được nhận từ SEPP1.

SEPP2 gửi chuyển tiếp thông điệp đến NF2.

Chính sách bảo vệ như được thảo luận trong các ví dụ này mô tả các phần tử nào của thông điệp sẽ được mật mã hóa và các phần tử nào sẽ được bảo vệ toàn vẹn. Chính sách có thể mô tả theo cách rõ ràng các phần tử nào sẽ được bảo vệ (được mật mã hóa và/hoặc được bảo vệ toàn vẹn), hoặc nó có thể mô tả theo cách rõ ràng các phần tử nào sẽ *không* được bảo vệ (không được mật mã hóa và/hoặc không được bảo vệ toàn vẹn).

Một trong các sự hiện thực hóa tiềm năng của chính sách bảo vệ được phác thảo ở dưới. Chính sách bảo vệ có thể được định nghĩa cho tất cả các thông điệp được gửi và được nhận bởi NF. Các thông điệp có thể là hoặc các yêu cầu HTTP hoặc các sự đáp lại HTTP.

Chính sách bảo vệ trong một số phương án bao gồm một hoặc nhiều quy tắc bảo vệ. Mỗi quy tắc bảo vệ gồm: (1) loại thông điệp mà quy tắc là có thể áp dụng được đối với, gồm có chẳng hạn yêu cầu HTTP, sự đáp lại HTTP, hoặc cả hai; (2) thực thể thông điệp mà quy tắc là có thể áp dụng được đối với, mà có thể là chẳng hạn URI-Yêu cầu, phần đầu giả HTTP, phần đầu HTTP, hoặc thân HTTP; và (3) sự vận hành so khớp và thay thế. Phụ thuộc vào thực thể thông điệp, sự vận hành có thể được biểu diễn bởi biểu thức thông thường, Con trỏ JSON (RFC 6901) đối với phần tử trong kết cấu JSON và sự thay thế của nó, hoặc biểu thức khác bất kỳ.

Trong một số phương án, quy tắc bảo vệ sẽ tồn tại trong chính sách bảo vệ cho mọi mục của mọi thông điệp mà đòi hỏi được bảo vệ.

Trong sự truyền thông giữa hai NF, chính sách bảo vệ đơn có thể được sử dụng trong một số phương án. Chính sách bảo vệ này có thể được định nghĩa bởi NF cung cấp dịch vụ (nghĩa là NF được gọi). Chính sách bảo vệ có thể là áp dụng được đối với các thông điệp được gửi và được nhận bởi NF. Chính sách bảo vệ cho NF có thể được lưu trữ trong NRF được định vị trong PLMN của NF cung cấp dịch vụ.

Chính sách bảo vệ có thể được sử dụng cho sự truyền thông NF với vài PLMN, nhưng nó có thể cũng có thể định nghĩa các chính sách bảo vệ theo cách riêng lẻ cho mỗi PLMN mà NF tương tác với.

Chính sách bảo vệ cho các NF trong PLMN đã cho có thể là chung đối với tất cả các người tiêu dùng dịch vụ NF mà NF cung cấp dịch vụ tương tác với.

SEPP, khi mật mã hóa thông điệp được gửi đến NF, sẽ lặp lại qua các quy tắc bảo vệ của chính sách bảo vệ cho NF đó. Cho mọi quy tắc chính sách, nếu loại thông điệp của quy tắc so khớp loại thông điệp của thông điệp, thì nó sẽ áp dụng sự vận hành so khớp và thay thế tương ứng qua thực thể thông điệp được xác định bởi quy tắc.

SEPP, khi giải mật mã thông điệp được nhận từ SEPP khác sẽ lặp lại qua các quy tắc bảo vệ của chính sách bảo vệ cho NF nhận. Cho mọi quy tắc chính sách, nếu loại thông điệp của quy tắc so khớp loại thông điệp của thông điệp, thì nó sẽ áp dụng sự vận hành so khớp và thay thế đảo qua thực thể thông điệp được xác định bởi quy tắc.

Quy trình mật mã hóa và giải mật mã kết thúc khi tất cả các quy tắc bảo vệ của chính sách bảo vệ đã được đánh giá.

Phụ thuộc vào biến thể có thể áp dụng được, chính sách bảo vệ có thể áp dụng được có thể hoặc là được cung cấp cho SEPP (bởi NF hoặc SEPP trong PLMN khác) hoặc là được tra cứu bởi SEPP trong NRF.

Trong một số phương án, chính sách bảo vệ có thể được cung cấp cục bộ cho NF và trong NRF. Cho trường hợp sau, chính sách bảo vệ có thể được đăng ký trong NRF cho mỗi NF. Điều này có thể được hoàn thành bởi NF như một phần của quy trình đăng ký của nó với NRF, hoặc bởi cơ chế khác nhau, như việc cung cấp Vận hành và Bảo dưỡng (Operations and Maintenance, O&M). Trong cả hai trường hợp, mục tiêu là để ngăn SEPP khỏi đòi hỏi sự nâng cấp khi các NF mới hoặc các sự thay đổi trong chính sách bảo vệ của các NF hiện có được triển khai.

Ví dụ cụ thể cho Biến thể 2 được thể hiện trên Fig.8. Trong ví dụ này, chức năng mạng trong PLMN tạm trú (ví dụ chức năng truy nhập và tính di động, access and mobility function, AMF) cần gửi yêu cầu HTTP đến chức năng mạng trong PLMN thường trú (ví dụ, chức năng quản lý dữ liệu thống nhất, unified data management, UDM), để lấy ra dữ liệu thuê bao của người dùng riêng. Dữ liệu thuê bao có thể là phần nhỏ của hồ sơ thuê bao, như dữ liệu được đòi hỏi để lựa chọn "lát" (slice) riêng của Mạng lõi 5G.

Để tìm hiểu URI của UDM (mà được định vị trong PLMN thường trú), AMF truy vấn NRF cục bộ, nhờ phát ra thông điệp yêu cầu tìm ra. Thông điệp yêu cầu tìm ra gồm có các tiêu chuẩn tìm kiếm như loại chức năng mạng được đòi hỏi (UDM trong trường hợp này), hoặc dịch vụ đặc trưng ("nudm-sdm", trong trường hợp này). NRF trong vPLMN đến lượt gửi chuyển tiếp yêu cầu tìm ra đến NRF trong hPLMN, và như kết quả danh sách của các chức năng mạng UDM khả dụng (các điểm cuối URI) trong hPLMN được trả về đối với vAMF.

Như một phần của các hồ sơ được trả về của các phiên bản UDM khả dụng, thông tin hồ sơ gồm có các tham số chỉ báo các URI khả dụng khác nhau trong mỗi dịch vụ. Thông tin hồ sơ cũng gồm có chính sách bảo vệ 80 mà gồm có thông tin về nơi trong các URI này có thông tin nhạy cảm mà cần được bảo vệ. Xem xét ví dụ:

GET http://www.homeoperator.com/nudm-sdm/v1/{SUPI}/nssai

Trong trường hợp này, AMF có thể sử dụng URI này khi nó cần lấy ra Thông tin giúp đỡ lựa chọn lát mạng (Network Slice Selection Assistance Information, NSSAI) của

người dùng đã cho được lưu trữ trong UDM trong mạng thường trú của anh ấy/của cô ấy. Trong cú pháp ở trên, thành phần {SUPI} biểu diễn biến để được thay thế bởi nhận dạng người dùng thực, như, ví dụ:

GET http://www.homeoperator.com/nudm-sdm/v1/imsi-214050123456789/nssai

Yêu cầu HTTP được định tuyến từ AMF đến SEPP trong mạng tạm trú (vSEPP), và AMF gồm có chính sách bảo vệ 80 trong phần đầu HTTP đặc trưng, gồm có thông tin được nhận từ NRF về các phần của URI mà cần được bảo vệ bởi vì chúng chứa thông tin nhạy cảm.

vSEPP nhận thông điệp HTTP. vSEPP xác định SEPP trong hPLMN (hSEPP), tại đó thông tin này cần được gửi, và kiểm tra sự thỏa thuận chuyển vùng có liên quan để tìm ra được các khóa mật mã hóa thích hợp để được sử dụng để bảo vệ các thông điệp giữa các SEPP. vSEPP cũng trích phần đầu HTTP đặc trưng được gửi bởi AMF, và xử lý URI theo đó, vì vậy các phần URI nhạy cảm có thể được mật mã hóa sử dụng các khóa được tìm. Phần đầu HTTP có thể chỉ báo, ví dụ, biểu thức thông thường sau đây (từ ví dụ URL ở trên): "^/udm-sdm/v1/([^/?#]+)/nssai$". Điều này cho phép tìm sự so khớp hoàn toàn, tại đó nhóm bên trong thứ 1: "([^/?#]+)" là tập hợp của các ký tự tại đó trị số {supi} được kỳ vọng để được tìm.

hSEPP nhận thông điệp HTTP, và hoàn thành sự vận hành đảo. Nó xác định PLMN mà đang gửi thông điệp, để kiểm tra các sự thỏa thuận chuyển vùng có thể áp dụng được, và xác định các khóa mật mã hóa đúng. Sau đó, nó kiểm tra phần đầu HTTP đặc trưng và xác định các phần của URI mà chịu sự bảo vệ (được mật mã hóa), và nó giải mật mã chúng, và thay thế chúng bởi phiên bản không được mật mã hóa. hSEPP cũng loại bỏ phần đầu HTPP mà đã chỉ báo các phần của URI mà đã được mật mã hóa.

Sau đó, hSEPP gửi chuyển tiếp thông điệp HTTP đến phiên bản UDM trong HPLMN. Thông điệp này giống hệt với thông điệp được bắt nguồn bởi vAMF, và bởi vậy sự mật mã hóa/sự giải mật mã được hoàn thành giữa SEPPS, của các thành phần URI nhất định là trong suốt đối với sự truyền thông vAMF -> hUDM.

Mặc dù các phương án đã được lấy làm ví dụ trong ngữ cảnh để truyền thông điệp 60 giữa các miền mạng lõi mà lấy dạng của các mạng lõi trong các PLMN khác nhau, các phương án ở đây có thể mở rộng được đến loại bất kỳ của các miền mạng lõi.

Trên thực tế, trong một số phương án, các miền mạng lõi là các miền khác nhau trong cùng mạng lõi.

Lưu ý thêm nữa là các phương án ở đây có thể sử dụng giao thức truyền thông bất kỳ trong một hoặc nhiều giao thức truyền thông được biết đến trong lĩnh vực hoặc mà có thể được phát triển, như IEEE 802.xx, Đa truy nhập phân chia mã (Code Division Multiple Access, CDMA), CDMA băng rộng (Wideband CDMA, WCDMA), Hệ thống viễn thông di động toàn cầu (Global System for Mobile telecommunications, GSM), Tiến hóa dài hạn (Long Term Evolution, LTE), WiMax, Rađio mới (New Radio, NR), hoặc tương tự. Do đó, mặc dù đôi khi được mô tả ở đây trong ngữ cảnh của 5G, các nguyên lý và các khái niệm được thảo luận ở đây là có thể áp dụng được đối với các hệ thống 4G và các hệ thống khác.

Thiết bị không dây (wireless device) như được sử dụng ở đây là thiết bị loại bất kỳ có khả năng truyền thông với nút rađio khác theo cách không dây qua các tín hiệu rađio. Thiết bị không dây có thể bởi vậy tham chiếu đến thiết bị người dùng (user equipment, UE), trạm di động, máy tính xách tay (laptop), điện thoại thông minh, thiết bị máy đến máy (machine-to-machine, M2M), thiết bị truyền thông loại máy (machine-type communications, MTC), thiết bị Vạn vật kết nối Internet (Internet of Things, IoT) băng hẹp, v.v.. Mà nói, mặc dù thiết bị không dây có thể được tham chiếu đến như UE, sẽ cần lưu ý là thiết bị không dây không nhất thiết có "người dùng" (user) trong ý nghĩa của người cá nhân sở hữu và/hoặc vận hành thiết bị. Thiết bị không dây có thể cũng được tham chiếu đến như thiết bị truyền thông không dây, thiết bị rađio, thiết bị truyền thông rađio, thiết bị đầu cuối không dây, hoặc theo cách đơn giản là thiết bị đầu cuối – trừ khi ngữ cảnh chỉ báo theo cách khác, sự sử dụng của thuật ngữ bất kỳ trong các thuật ngữ này được dự định để gồm có các thiết bị hoặc các UE thiết bị đến thiết bị, các thiết bị hoặc các thiết bị loại máy có khả năng truyền thông máy đến máy, các cảm biến được trang bị với thiết bị không dây, các máy tính để bàn được làm cho có thể không dây, các thiết bị đầu cuối di động, các điện thoại thông minh, được trang bị được nhúng vào máy tính xách tay (laptop-embedded equipped, LEE), thiết bị được lắp vào máy tính xách tay (laptop-mounted equipment, LME), các khóa điện tử (dongle) USB, thiết bị đặt tại nhà riêng khách hàng (customer-premises equipment, CPE) không dây, v.v.. Trong thảo luận ở đây, các thuật ngữ thiết bị máy đến máy (machine-to-machine, M2M), thiết bị truyền

thông loại máy (machine-type communication, MTC), cảm biến không dây, và cảm biến có thể cũng được sử dụng. Cần hiểu là các thiết bị này có thể là các UE, nhưng có thể nói chung là được tạo cấu hình để truyền và/hoặc nhận dữ liệu mà không có sự tương tác con người trực tiếp.

Trong kịch bản IOT, thiết bị không dây như được mô tả ở đây có thể là, hoặc có thể được bao gồm trong, máy hoặc thiết bị mà thực hiện sự giám sát hoặc các sự đo, và truyền các kết quả của các sự đo giám sát như vậy đến thiết bị khác hoặc mạng. Các ví dụ riêng của các máy như vậy là các máy đo công suất, máy móc công nghiệp, hoặc các dụng cụ gia đình hoặc cá nhân, ví dụ các thiết bị làm lạnh, các ti vi, các thiết bị có thể mang được cá nhân như các đồng hồ v.v.. Trong các kịch bản khác, thiết bị truyền thông không dây như được mô tả ở đây có thể được bao gồm trong xe cộ và có thể thực hiện sự giám sát và/hoặc việc báo cáo của trạng thái vận hành của xe cộ hoặc các chức năng khác được kết hợp với xe cộ.

Như được sử dụng ở đây, "thiết bị mạng" (network equipment) tham chiếu đến thiết bị có khả năng, được tạo cấu hình, được sắp đặt và/hoặc có thể vận hành được để truyền thông theo cách trực tiếp hoặc theo cách gián tiếp với thiết bị không dây và/hoặc với thiết bị khác trong mạng truyền thông không dây mà làm cho có thể và/hoặc cung cấp sự truy nhập không dây đối với thiết bị không dây. Các ví dụ của thiết bị mạng gồm có, nhưng không được giới hạn vào, thiết bị mạng lõi trong mạng lõi (ví dụ, thiết bị mà thi hành AMF hoặc SMF).

Lưu ý là thiết bị mạng như được mô tả ở trên có thể thực hiện sự xử lý bất kỳ trong sự xử lý ở đây nhờ thi hành các phương tiện hoặc các bộ phận chức năng bất kỳ. Trong một phương án, ví dụ, thiết bị mạng bao gồm các mạch hoặc hệ mạch tương ứng được tạo cấu hình để thực hiện các bước được thể hiện trên Fig.5. Các mạch hoặc hệ mạch về vấn đề này có thể bao gồm các mạch được dành riêng để thực hiện sự xử lý chức năng nhất định và/hoặc một hoặc nhiều bộ vi xử lý kết hợp với bộ nhớ. Trong các phương án mà dùng bộ nhớ, mà có thể bao gồm một hoặc vài loại của bộ nhớ như bộ nhớ chỉ đọc (read-only memory, ROM), bộ nhớ truy nhập ngẫu nhiên, bộ nhớ cache, các thiết bị nhớ tác động nhanh, các thiết bị lưu trữ quang, v.v., bộ nhớ lưu trữ mã chương trình mà, khi được thực thi bởi một hoặc nhiều bộ xử lý, thực hiện các kỹ thuật được mô tả ở đây.

Fig.9A minh họa thiết bị mạng 300 phù hợp với một hoặc nhiều phương án. Như được thể hiện, thiết bị mạng 300 gồm có hệ mạch xử lý 310 và hệ mạch truyền thông 320. Hệ mạch truyền thông 320 được tạo cấu hình để truyền và/hoặc nhận thông tin đến và/hoặc từ một hoặc nhiều nút khác, ví dụ, qua công nghệ truyền thông bất kỳ. Hệ mạch xử lý 310 được tạo cấu hình để thực hiện sự xử lý được mô tả ở trên, ví dụ, trên Fig.5, như nhờ thực thi các lệnh được lưu trữ trong bộ nhớ 330. Hệ mạch xử lý 310 về vấn đề này có thể thi hành các phương tiện, các bộ phận, hoặc các môđun chức năng nhất định.

Fig.9B minh họa thiết bị mạng 400 phù hợp với một hoặc nhiều phương án khác. Như được thể hiện, thiết bị mạng 400 thi hành các phương tiện, các bộ phận, hoặc các môđun chức năng khác nhau, ví dụ, qua hệ mạch xử lý 410 trên Fig.9A và/hoặc qua mã phần mềm. Các phương tiện, các bộ phận, hoặc các môđun chức năng này, ví dụ, để thi hành phương pháp trên Fig.5, gồm có chẳng hạn bộ phận hoặc môđun nhận 410 để nhận thông điệp 60 mà đã, hoặc là để, được truyền giữa các miền mạng lõi khác nhau, và để nhận chính sách bảo vệ 80 mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của thông điệp 60 (ví dụ, một hoặc nhiều đoạn của nội dung của trường 62 trong thông điệp 60) mà sự bảo vệ an toàn liên miền 70 là để được áp dụng hoặc được loại bỏ. Cũng được gồm có có thể là bộ phận hoặc môđun bảo vệ 420 để áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn theo chính sách bảo vệ 80. Còn được gồm có trong một số phương án có thể là bộ phận hoặc môđun gửi chuyển tiếp 430 để gửi chuyển tiếp thông điệp 60, với sự bảo vệ an toàn liên miền được áp dụng hoặc được loại bỏ đối với một hoặc nhiều đoạn, về phía đích của thông điệp 60.

Cũng lưu ý là thiết bị mạng khác như được mô tả ở trên có thể thực hiện sự xử lý bất kỳ trong sự xử lý ở đây nhờ thi hành các phương tiện hoặc các bộ phận chức năng bất kỳ. Trong một phương án, ví dụ, thiết bị mạng bao gồm các mạch hoặc hệ mạch tương ứng được tạo cấu hình để thực hiện các bước được thể hiện trên Fig.6. Các mạch hoặc hệ mạch về vấn đề này có thể bao gồm các mạch được dành riêng để thực hiện sự xử lý chức năng nhất định và/hoặc một hoặc nhiều bộ vi xử lý kết hợp với bộ nhớ. Trong các phương án mà dùng bộ nhớ, mà có thể bao gồm một hoặc vài loại của bộ nhớ như bộ nhớ chỉ đọc (read-only memory, ROM), bộ nhớ truy nhập ngẫu nhiên, bộ nhớ cache, các thiết bị nhớ tác động nhanh, các thiết bị lưu trữ quang, v.v., bộ nhớ lưu trữ mã

chương trình mà, khi được thực thi bởi một hoặc nhiều bộ xử lý, thực hiện các kỹ thuật được mô tả ở đây.

Fig.10A minh họa thiết bị mạng 500 phù hợp với một hoặc nhiều phương án. Như được thể hiện, thiết bị mạng 500 gồm có hệ mạch xử lý 510 và hệ mạch truyền thông 520. Hệ mạch truyền thông 520 được tạo cấu hình để truyền và/hoặc nhận thông tin đến và/hoặc từ một hoặc nhiều nút khác, ví dụ, qua công nghệ truyền thông bất kỳ. Hệ mạch xử lý 510 được tạo cấu hình để thực hiện sự xử lý được mô tả ở trên, ví dụ, trên Fig.6, như nhờ thực thi các lệnh được lưu trữ trong bộ nhớ 530. Hệ mạch xử lý 510 về vấn đề này có thể thi hành các phương tiện, các bộ phận, hoặc các môđun chức năng nhất định.

Fig.10B minh họa thiết bị mạng 600 phù hợp với một hoặc nhiều phương án khác. Như được thể hiện, thiết bị mạng 600 thi hành các phương tiện, các bộ phận, hoặc các môđun chức năng khác nhau, ví dụ, qua hệ mạch xử lý 610 trên Fig.10A và/hoặc qua mã phần mềm. Các phương tiện, các bộ phận, hoặc các môđun chức năng này, ví dụ, để thi hành phương pháp trên Fig.6, gồm có chẳng hạn bộ phận hoặc môđun thu được 410 để thu được chính sách bảo vệ 80 mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của thông điệp 60 (ví dụ, một hoặc nhiều đoạn của nội dung của trường 62 trong thông điệp 60) mà sự bảo vệ an toàn liên miền 70 là để được áp dụng hoặc được loại bỏ. Còn được gồm có có thể là bộ phận hoặc môđun truyền 420 để truyền chính sách bảo vệ 80.

Những người có hiểu biết trung bình trong lĩnh vực sẽ cũng hiểu rõ là các phương án ở đây còn gồm có các chương trình máy tính tương ứng.

Chương trình máy tính bao gồm các lệnh mà, khi được thực thi trên ít nhất một bộ xử lý của thiết bị mạng, làm cho thiết bị mạng thực hiện sự xử lý bất kỳ trong sự xử lý tương ứng được mô tả ở trên. Chương trình máy tính về vấn đề này có thể bao gồm một hoặc nhiều môđun mã tương ứng với các phương tiện hoặc các bộ phận được mô tả ở trên.

Các phương án còn gồm có bộ mang chứa chương trình máy tính như vậy. Bộ mang này có thể bao gồm một trong tín hiệu điện tử, tín hiệu quang, tín hiệu radio, hoặc phương tiện lưu trữ đọc được bởi máy tính.

Về vấn đề này, các phương án ở đây cũng gồm có phương tiện không chuyển tiếp đọc được (lưu trữ hoặc ghi) bởi máy tính mà đã lưu trữ trên đó các lệnh mà, khi được thực thi bởi bộ xử lý của thiết bị mạng, làm cho thiết bị mạng thực hiện như được mô tả ở trên.

Xét thấy ở trên, một số phương án sẽ được đánh số ở dưới như các ví dụ.

Phương án 1. Phương pháp được thực hiện bởi thiết bị mạng được tạo cấu hình như máy ủy nhiệm cho một trong nhiều miền mạng lõi khác nhau của hệ thống truyền thông không dây, phương pháp này bao gồm các bước: nhận thông điệp mà đã, hoặc là để, được truyền giữa các miền mạng lõi khác nhau; nhận chính sách bảo vệ mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung của trường trong thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ; áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn theo chính sách bảo vệ; và gửi chuyển tiếp thông điệp, với sự bảo vệ an toàn liên miền được áp dụng hoặc được loại bỏ đối với một hoặc nhiều đoạn, về phía đích của thông điệp.

Phương án 2. Phương pháp theo phương án 1, trong đó thông tin gồm có một hoặc nhiều biểu thức thông thường mà chỉ báo một hoặc nhiều đoạn.

Phương án 3. Phương pháp theo phương án 1, trong đó thông tin gồm có một hoặc nhiều Con trỏ Ký hiệu đối tượng JavaScript (JavaScript Object Notation, JSON), mà chỉ báo một hoặc nhiều đoạn.

Phương án 4. Phương pháp theo phương án 1, trong đó thông tin gồm có một hoặc nhiều phạm vi của các byte trong trường, và/hoặc một hoặc nhiều phạm vi của các bit trong trường, mà chỉ báo một hoặc nhiều đoạn.

Phương án 5. Phương pháp theo phương án 1, trong đó thông tin gồm có một hoặc nhiều mẫu tìm kiếm, một hoặc nhiều dấu hiệu, và/hoặc một hoặc nhiều chuỗi con, mà chỉ báo một hoặc nhiều đoạn.

Phương án 6. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 5, phương pháp này còn bao gồm bước trích một hoặc nhiều đoạn của nội dung của trường để áp dụng hoặc loại bỏ sự bảo vệ an toàn liên miền, nhờ phân tách nội dung sử dụng thông tin được gồm có trong chính sách bảo vệ.

Phương án 7. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 6, trong đó chính sách bảo vệ còn chỉ báo, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ.

Phương án 8. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 7, trong đó, cho mỗi trong một hoặc nhiều đoạn, sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ bao gồm sự bảo vệ bảo mật và/hoặc sự bảo vệ toàn vẹn.

Phương án 9. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 8, trong đó thông điệp là thông điệp Giao thức chuyển tải siêu văn bản (Hypertext Transfer Protocol, HTTP) và trường là trường HTTP.

Phương án 10. Phương pháp theo phương án 9, trong đó thông điệp HTTP là thông điệp yêu cầu HTTP và trường là trường đường, và trong đó nội dung của trường đường là Phần tử nhận dạng tài nguyên đồng nhất (Uniform Resource Identifier, URI) yêu cầu.

Phương án 11. Phương pháp theo phương án 9, trong đó trường là trường của phần đầu HTTP hoặc phần đầu giả HTTP.

Phương án 12. Phương pháp theo phương án 9, trong đó trường là thân, hoặc một phần của thân, của thông điệp HTTP.

Phương án 13. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 12, phương pháp này còn bao gồm bước truyền yêu cầu tìm ra đến dịch vụ tìm ra yêu cầu sự tìm ra của chính sách bảo vệ để bảo vệ thông điệp, và nhận chính sách bảo vệ đáp lại yêu cầu tìm ra.

Phương án 14. Phương pháp theo phương án 13, phương pháp này bao gồm bước truyền yêu cầu tìm ra đáp lại việc nhận thông điệp.

Phương án 15. Phương pháp theo phương án bất kỳ trong các phương án từ 13 đến 14, trong đó dịch vụ tìm ra được thi hành bởi chức năng kho mạng (network repository function, NRF).

Phương án 16. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 12, phương pháp này bao gồm bước nhận chính sách bảo vệ từ thiết bị mạng trong đường mà thông điệp đi từ nguồn của thông điệp đến đích của thông điệp.

Phương án 17. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 12 và 16, phương pháp này bao gồm bước nhận chính sách bảo vệ từ hoặc là nguồn của thông điệp hoặc là đích của thông điệp.

Phương án 18. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 12 và 16, phương pháp này bao gồm bước nhận chính sách bảo vệ từ thiết bị mạng khác từ đó thông điệp được nhận, trong đó thiết bị mạng khác cũng được tạo cấu hình như máy ủy nhiệm giữa các miền mạng lõi khác nhau.

Phương án 19. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 12 và từ 16 đến 18, trong đó chính sách bảo vệ được gồm có trong thông điệp.

Phương án 20. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 12 và từ 16 đến 19, trong đó chính sách bảo vệ được gồm có trong phần đầu của thông điệp.

Phương án 21. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 20, trong đó thông điệp là thông điệp lớp ứng dụng, trong đó trường là trường lớp ứng dụng, trong đó nội dung của trường bao gồm thông tin lớp ứng dụng, và trong đó sự bảo vệ an toàn liên miền bao gồm sự bảo vệ lớp ứng dụng.

Phương án 22. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 21, trong đó thiết bị mạng được tạo cấu hình như Máy ủy nhiệm bảo vệ mép an toàn (Security Edge Protection Proxy, SEPP).

Phương án 23. Phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 22, trong đó các miền mạng lõi bao gồm các mạng lõi của các mạng di động mặt đất công cộng (public land mobile network, PLMN) khác nhau.

Phương án 24. Phương pháp được thực hiện bởi thiết bị mạng để tạo thuận lợi cho sự bảo vệ của thông điệp được truyền giữa các miền mạng lõi khác nhau của hệ thống truyền thông không dây, phương pháp này bao gồm các bước: thu được chính sách bảo vệ mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung của trường trong thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ; và truyền chính sách bảo vệ.

Phương án 25. Phương pháp theo phương án 24, trong đó thông tin gồm có một hoặc nhiều biểu thức thông thường mà chỉ báo một hoặc nhiều đoạn.

Phương án 26. Phương pháp theo phương án 24, trong đó thông tin gồm có một hoặc nhiều Con trỏ Ký hiệu đối tượng JavaScript (JavaScript Object Notation, JSON), mà chỉ báo một hoặc nhiều đoạn.

Phương án 27. Phương pháp theo phương án 24, trong đó thông tin gồm có một hoặc nhiều phạm vi của các byte trong trường, và/hoặc một hoặc nhiều phạm vi của các bit trong trường, mà chỉ báo một hoặc nhiều đoạn.

Phương án 28. Phương pháp theo phương án 24, trong đó thông tin gồm có một hoặc nhiều mẫu tìm kiếm, một hoặc nhiều dấu hiệu, và/hoặc một hoặc nhiều chuỗi con, mà chỉ báo một hoặc nhiều đoạn.

Phương án 29. Phương pháp theo phương án bất kỳ trong các phương án từ 24 đến 28, trong đó chính sách bảo vệ còn chỉ báo, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ.

Phương án 30. Phương pháp theo phương án bất kỳ trong các phương án từ 24 đến 29, trong đó, cho mỗi trong một hoặc nhiều đoạn, sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ bao gồm sự bảo vệ bảo mật và/hoặc sự bảo vệ toàn vẹn.

Phương án 31. Phương pháp theo phương án bất kỳ trong các phương án từ 24 đến 30, trong đó thông điệp là thông điệp Giao thức chuyển tải siêu văn bản (Hypertext Transfer Protocol, HTTP) và trường là trường HTTP.

Phương án 32. Phương pháp theo phương án 31, trong đó thông điệp HTTP là thông điệp yêu cầu HTTP và trường là trường đường, và trong đó nội dung của trường đường là Phần tử nhận dạng tài nguyên đồng nhất (Uniform Resource Identifier, URI) yêu cầu.

Phương án 33. Phương pháp theo phương án 31, trong đó trường là trường của phần đầu HTTP hoặc phần đầu giả HTTP.

Phương án 34. Phương pháp theo phương án 31, trong đó trường là phần thân của thông điệp HTTP.

Phương án 35. Phương pháp theo phương án bất kỳ trong các phương án từ 24 đến 34, trong đó bước truyền chính sách bảo vệ bao gồm truyền chính sách bảo vệ đến thiết bị mạng được tạo cấu hình, như một máy ủy nhiệm của các miền mạng lõi khác nhau, để áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn theo chính sách bảo vệ.

Phương án 36. Phương pháp theo phương án bất kỳ trong các phương án từ 24 đến 35, phương pháp này còn bao gồm bước nhận yêu cầu tìm ra yêu cầu sự tìm ra của chính sách bảo vệ để bảo vệ thông điệp, và truyền chính sách bảo vệ đáp lại yêu cầu tìm ra.

Phương án 37. Phương pháp theo phương án 36, trong đó phương pháp được thực hiện bởi thiết bị mạng mà thi hành chức năng kho mạng (network repository function, NRF).

Phương án 38. Phương pháp theo phương án bất kỳ trong các phương án từ 24 đến 35, trong đó phương pháp được thực hiện bởi thiết bị mạng trong đường mà thông điệp đi từ nguồn của thông điệp đến đích của thông điệp.

Phương án 39. Phương pháp theo phương án bất kỳ trong các phương án từ 24 đến 35 và 38, trong đó phương pháp được thực hiện bởi thiết bị mạng mà là nguồn của thông điệp hoặc đích của thông điệp.

Phương án 40. Phương pháp theo phương án bất kỳ trong các phương án từ 24 đến 35 và 38, trong đó phương pháp được thực hiện bởi thiết bị mạng được tạo cấu hình như máy ủy nhiệm giữa các miền mạng lõi khác nhau.

Phương án 41. Phương pháp theo phương án bất kỳ trong các phương án từ 24 đến 35 và từ 38 đến 40, trong đó bước truyền chính sách bảo vệ bao gồm truyền thông điệp với chính sách bảo vệ được gồm có trong thông điệp.

Phương án 42. Phương pháp theo phương án bất kỳ trong các phương án từ 24 đến 41, trong đó thông điệp là thông điệp lớp ứng dụng, trong đó trường là trường lớp ứng dụng, trong đó nội dung của trường bao gồm thông tin lớp ứng dụng, và trong đó sự bảo vệ an toàn liên miền bao gồm sự bảo vệ lớp ứng dụng.

Phương án 43. Phương pháp theo phương án bất kỳ trong các phương án từ 24 đến 42, trong đó các miền mạng lõi bao gồm các mạng lõi của các mạng di động mặt đất công cộng (public land mobile network, PLMN) khác nhau.

Phương án 44. Thiết bị mạng được tạo cấu hình như máy ủy nhiệm cho một trong nhiều miền mạng lõi khác nhau của hệ thống truyền thông không dây. Thiết bị mạng được tạo cấu hình để: nhận thông điệp mà đã, hoặc là để, được truyền giữa các miền mạng lõi khác nhau; nhận chính sách bảo vệ mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung của trường trong thông điệp mà sự bảo vệ an toàn

liên miền là để được áp dụng hoặc được loại bỏ; áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn theo chính sách bảo vệ; và gửi chuyển tiếp thông điệp, với sự bảo vệ an toàn liên miền được áp dụng hoặc được loại bỏ đối với một hoặc nhiều đoạn, về phía đích của thông điệp.

Phương án 45. Thiết bị mạng theo phương án 44, trong đó thông tin gồm có một hoặc nhiều biểu thức thông thường mà chỉ báo một hoặc nhiều đoạn.

Phương án 46. Thiết bị mạng theo phương án 44, trong đó thông tin gồm có một hoặc nhiều Con trỏ Ký hiệu đối tượng JavaScript (JavaScript Object Notation, JSON), mà chỉ báo một hoặc nhiều đoạn.

Phương án 47. Thiết bị mạng theo phương án 44, trong đó thông tin gồm có một hoặc nhiều phạm vi của các byte trong trường, và/hoặc một hoặc nhiều phạm vi của các bit trong trường, mà chỉ báo một hoặc nhiều đoạn.

Phương án 48. Thiết bị mạng theo phương án 44, trong đó thông tin gồm có một hoặc nhiều mẫu tìm kiếm, một hoặc nhiều dấu hiệu, và/hoặc một hoặc nhiều chuỗi con, mà chỉ báo một hoặc nhiều đoạn.

Phương án 49. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 48, còn bao gồm trích một hoặc nhiều đoạn của nội dung của trường để áp dụng hoặc loại bỏ sự bảo vệ an toàn liên miền, nhờ phân tách nội dung sử dụng thông tin được gồm có trong chính sách bảo vệ.

Phương án 50. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 49, trong đó chính sách bảo vệ còn chỉ báo, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ.

Phương án 51. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 50, trong đó, cho mỗi trong một hoặc nhiều đoạn, sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ bao gồm sự bảo vệ bảo mật và/hoặc sự bảo vệ toàn vẹn.

Phương án 52. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 51, trong đó thông điệp là thông điệp Giao thức chuyển tải siêu văn bản (Hypertext Transfer Protocol, HTTP) và trường là trường HTTP.

Phương án 53. Thiết bị mạng theo phương án 52, trong đó thông điệp HTTP là thông điệp yêu cầu HTTP và trường là trường đường, và trong đó nội dung của trường

đường là Phần tử nhận dạng tài nguyên đồng nhất (Uniform Resource Identifier, URI) yêu cầu.

Phương án 54. Thiết bị mạng theo phương án 52, trong đó trường là trường của phần đầu HTTP hoặc phần đầu giả HTTP.

Phương án 55. Thiết bị mạng theo phương án 52, trong đó trường là thân, hoặc một phần của thân, của thông điệp HTTP.

Phương án 56. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 55, còn bao gồm truyền yêu cầu tìm ra đến dịch vụ tìm ra yêu cầu sự tìm ra của chính sách bảo vệ để bảo vệ thông điệp, và nhận chính sách bảo vệ đáp lại yêu cầu tìm ra.

Phương án 57. Thiết bị mạng theo phương án 56, bao gồm truyền yêu cầu tìm ra đáp lại việc nhận thông điệp.

Phương án 58. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 56 đến 57, trong đó dịch vụ tìm ra được thi hành bởi chức năng kho mạng (network repository function, NRF).

Phương án 59. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 55, bao gồm nhận chính sách bảo vệ từ thiết bị mạng trong đường mà thông điệp đi từ nguồn của thông điệp đến đích của thông điệp.

Phương án 60. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 55 và 59, bao gồm nhận chính sách bảo vệ từ hoặc là nguồn của thông điệp hoặc là đích của thông điệp.

Phương án 61. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 55 và 59, bao gồm nhận chính sách bảo vệ từ thiết bị mạng khác từ đó thông điệp được nhận, trong đó thiết bị mạng khác cũng được tạo cấu hình như máy ủy nhiệm giữa các miền mạng lõi khác nhau.

Phương án 62. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 55 và từ 59 đến 61, trong đó chính sách bảo vệ được gồm có trong thông điệp.

Phương án 63. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 55 và từ 59 đến 62, trong đó chính sách bảo vệ được gồm có trong phần đầu của thông điệp.

Phương án 64. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 63, trong đó thông điệp là thông điệp lớp ứng dụng, trong đó trường là trường lớp ứng dụng, trong đó nội dung của trường bao gồm thông tin lớp ứng dụng, và trong đó sự bảo vệ an toàn liên miền bao gồm sự bảo vệ lớp ứng dụng.

Phương án 65. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 64, trong đó thiết bị mạng được tạo cấu hình như Máy ủy nhiệm bảo vệ mép an toàn (Security Edge Protection Proxy, SEPP).

Phương án 66. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 44 đến 65, trong đó các miền mạng lõi bao gồm các mạng lõi của các mạng di động mặt đất công cộng (public land mobile network, PLMN) khác nhau.

Phương án 67. Thiết bị mạng để tạo thuận lợi cho sự bảo vệ của thông điệp được truyền giữa các miền mạng lõi khác nhau của hệ thống truyền thông không dây. Thiết bị mạng được tạo cấu hình để: thu được chính sách bảo vệ mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung của trường trong thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ; và truyền chính sách bảo vệ.

Phương án 68. Thiết bị mạng theo phương án 67, trong đó thông tin gồm có một hoặc nhiều biểu thức thông thường mà chỉ báo một hoặc nhiều đoạn.

Phương án 69. Thiết bị mạng theo phương án 67, trong đó thông tin gồm có một hoặc nhiều Con trỏ Ký hiệu đối tượng JavaScript (JavaScript Object Notation, JSON), mà chỉ báo một hoặc nhiều đoạn.

Phương án 70. Thiết bị mạng theo phương án 67, trong đó thông tin gồm có một hoặc nhiều phạm vi của các byte trong trường, và/hoặc một hoặc nhiều phạm vi của các bit trong trường, mà chỉ báo một hoặc nhiều đoạn.

Phương án 71. Thiết bị mạng theo phương án 67, trong đó thông tin gồm có một hoặc nhiều mẫu tìm kiếm, một hoặc nhiều dấu hiệu, và/hoặc một hoặc nhiều chuỗi con, mà chỉ báo một hoặc nhiều đoạn.

Phương án 72. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 67 đến 71, trong đó chính sách bảo vệ còn chỉ báo, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ.

Phương án 73. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 67 đến 72, trong đó, cho mỗi trong một hoặc nhiều đoạn, sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ bao gồm sự bảo vệ bảo mật và/hoặc sự bảo vệ toàn vẹn.

Phương án 74. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 67 đến 75, trong đó thông điệp là thông điệp Giao thức chuyển tải siêu văn bản (Hypertext Transfer Protocol, HTTP) và trường là trường HTTP.

Phương án 75. Thiết bị mạng theo phương án 74, trong đó thông điệp HTTP là thông điệp yêu cầu HTTP và trường là trường đường, và trong đó nội dung của trường đường là Phần tử nhận dạng tài nguyên đồng nhất (Uniform Resource Identifier, URI) yêu cầu.

Phương án 76. Thiết bị mạng theo phương án 74, trong đó trường là trường của phần đầu HTTP hoặc phần đầu giả HTTP.

Phương án 77. Thiết bị mạng theo phương án 74, trong đó trường là phần thân của thông điệp HTTP.

Phương án 78. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 67 đến 77, trong đó việc truyền chính sách bảo vệ bao gồm truyền chính sách bảo vệ đến thiết bị mạng được tạo cấu hình, như một máy ủy nhiệm của các miền mạng lõi khác nhau, để áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn theo chính sách bảo vệ.

Phương án 79. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 67 đến 78, còn bao gồm nhận yêu cầu tìm ra yêu cầu sự tìm ra của chính sách bảo vệ để bảo vệ thông điệp, và truyền chính sách bảo vệ đáp lại yêu cầu tìm ra.

Phương án 80. Thiết bị mạng theo phương án 79, trong đó phương pháp được thực hiện bởi thiết bị mạng mà thi hành chức năng kho mạng (network repository function, NRF).

Phương án 81. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 67 đến 78, trong đó phương pháp được thực hiện bởi thiết bị mạng trong đường mà thông điệp đi từ nguồn của thông điệp đến đích của thông điệp.

Phương án 82. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 67 đến 78 và 81, trong đó phương pháp được thực hiện bởi thiết bị mạng mà là nguồn của thông điệp hoặc đích của thông điệp.

Phương án 83. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 67 đến 78 và 81, trong đó phương pháp được thực hiện bởi thiết bị mạng được tạo cấu hình như máy ủy nhiệm giữa các miền mạng lõi khác nhau.

Phương án 84. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 67 đến 78 và từ 81 đến 83, trong đó việc truyền chính sách bảo vệ bao gồm truyền thông điệp với chính sách bảo vệ được gồm có trong thông điệp.

Phương án 85. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 67 đến 84, trong đó thông điệp là thông điệp lớp ứng dụng, trong đó trường là trường lớp ứng dụng, trong đó nội dung của trường bao gồm thông tin lớp ứng dụng, và trong đó sự bảo vệ an toàn liên miền bao gồm sự bảo vệ lớp ứng dụng.

Phương án 86. Thiết bị mạng theo phương án bất kỳ trong các phương án từ 67 đến 85, trong đó các miền mạng lõi bao gồm các mạng lõi của các mạng di động mặt đất công cộng (public land mobile network, PLMN) khác nhau.

Phương án 87. Thiết bị mạng được tạo cấu hình như máy ủy nhiệm cho một trong nhiều miền mạng lõi khác nhau của hệ thống truyền thông không dây. Thiết bị mạng bao gồm hệ mạch truyền thông và hệ mạch xử lý trong đó thiết bị mạng được tạo cấu hình để nhận thông điệp mà đã, hoặc là để, được truyền giữa các miền mạng lõi khác nhau; nhận chính sách bảo vệ mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung của trường trong thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ; áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn theo chính sách bảo vệ; và gửi chuyển tiếp thông điệp, với sự bảo vệ an toàn liên miền được áp dụng hoặc được loại bỏ đối với một hoặc nhiều đoạn, về phía đích của thông điệp.

Phương án 88. Thiết bị mạng theo phương án 87, được tạo cấu hình để thực hiện phương pháp theo phương án bất kỳ trong các phương án từ 2 đến 23.

Phương án 89. Thiết bị mạng để tạo thuận lợi cho sự bảo vệ của thông điệp được truyền giữa các miền mạng lõi khác nhau của hệ thống truyền thông không dây. Thiết bị mạng bao gồm hệ mạch truyền thông và hệ mạch xử lý trong đó thiết bị mạng được tạo cấu hình để thu được chính sách bảo vệ mà gồm có thông tin chỉ báo đối với một

hoặc nhiều đoạn nào của nội dung của trường trong thông điệp mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ; và truyền chính sách bảo vệ.

Phương án 90. Thiết bị mạng theo phương án 89, được tạo cấu hình để thực hiện phương pháp theo phương án bất kỳ trong các phương án từ 25 đến 43.

Phương án 91. Chương trình máy tính bao gồm các lệnh mà, khi được thực thi bởi ít nhất một bộ xử lý của thiết bị mạng, làm cho thiết bị thiết bị mạng thực hiện phương pháp theo phương án bất kỳ trong các phương án từ 1 đến 343.

Phương án 92. Bộ mang chứa chương trình máy tính theo phương án 91, trong đó bộ mang là một trong tín hiệu điện tử, tín hiệu quang, tín hiệu rađio, hoặc phương tiện lưu trữ đọc được bởi máy tính.

YÊU CẦU BẢO HỘ

1. Phương pháp truyền thông được thực hiện bởi thiết bị mạng, phương pháp này bao gồm các bước:

nhận thông điệp mà đã, hoặc là để, được truyền;

áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn của nội dung của trường trong thông điệp theo chính sách bảo vệ mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ, trong đó thông tin bao gồm một hoặc nhiều con trỏ Ký hiệu đối tượng JavaScript (JavaScript Object Notation, JSON) mà chỉ báo một hoặc các đoạn mà đối với đó sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ; và

gửi chuyển tiếp thông điệp, với sự bảo vệ an toàn liên miền được áp dụng hoặc được loại bỏ đối với một hoặc nhiều đoạn, về phía đích của thông điệp, trong đó

chính sách bảo vệ còn chỉ báo, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ, và trong đó, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ bao gồm sự bảo vệ bảo mật và/hoặc sự bảo vệ toàn vẹn.

2. Phương pháp theo điểm 1, trong đó thông điệp là thông điệp Giao thức chuyển tải siêu văn bản (Hypertext Transfer Protocol, HTTP) và trường là trường HTTP.

3. Phương pháp theo điểm 2, trong đó thông điệp HTTP là thông điệp yêu cầu HTTP và trường là trường đường, và trong đó nội dung của trường đường là Phần tử nhận dạng tài nguyên đồng nhất (Uniform Resource Identifier, URI) yêu cầu.

4. Phương pháp theo điểm 1, trong đó thông tin gồm có một hoặc nhiều biểu thức thông thường mà chỉ báo một hoặc nhiều đoạn.

5. Phương pháp theo điểm 1, trong đó chính sách bảo vệ được gồm có trong thông điệp.

6. Phương pháp theo điểm 1, còn bao gồm bước, đáp lại việc nhận thông điệp, truyền yêu cầu tìm ra đến chức năng kho mạng (network repository function, NRF), yêu cầu sự

tìm ra của chính sách bảo vệ để bảo vệ thông điệp, và nhận chính sách bảo vệ đáp lại yêu cầu tìm ra.

7. Phương pháp theo điểm 1, còn bao gồm bước nhận chính sách bảo vệ từ thiết bị mạng trong đường mà thông điệp đi từ nguồn của thông điệp đến đích của thông điệp.

8. Phương pháp theo điểm 1, trong đó phương pháp được thực hiện bởi Máy ủy nhiệm bảo vệ mép an toàn (Security Edge Protection Proxy, SEPP).

9. Phương pháp theo điểm 8, trong đó SEPP bao gồm SEPP trong mạng tạm trú, vSEPP, và SEPP trong mạng thường trú, hSEPP.

10. Thiết bị mạng, trong đó thiết bị mạng này bao gồm:

hệ mạch truyền thông; và

hệ mạch xử lý được kết nối với hệ mạch truyền thông, trong đó thiết bị mạng được tạo cấu hình để:

nhận, qua hệ mạch truyền thông, thông điệp mà đã, hoặc là để, được truyền;

áp dụng sự bảo vệ an toàn liên miền đối với, hoặc loại bỏ sự bảo vệ an toàn liên miền khỏi, một hoặc nhiều đoạn của nội dung của trường trong thông điệp theo chính sách bảo vệ mà gồm có thông tin chỉ báo đối với một hoặc nhiều đoạn nào của nội dung mà sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ, trong đó thông tin bao gồm một hoặc nhiều con trỏ Ký hiệu đối tượng JavaScript (JavaScript Object Notation, JSON) mà chỉ báo một hoặc các đoạn mà đối với đó sự bảo vệ an toàn liên miền là để được áp dụng hoặc được loại bỏ; và

gửi chuyển tiếp thông điệp, với sự bảo vệ an toàn liên miền được áp dụng hoặc được loại bỏ đối với một hoặc nhiều đoạn, về phía đích của thông điệp qua hệ mạch truyền thông, trong đó

chính sách bảo vệ còn chỉ báo, cho mỗi trong một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ, và trong đó, cho mỗi trong

một hoặc nhiều đoạn, loại của sự bảo vệ an toàn liên miền để được áp dụng hoặc được loại bỏ bao gồm sự bảo vệ bảo mật và/hoặc sự bảo vệ toàn vẹn.

11. Thiết bị mạng theo điểm 10, trong đó thông điệp là thông điệp Giao thức chuyển tải siêu văn bản (Hypertext Transfer Protocol, HTTP) và trường là trường HTTP.

12. Thiết bị mạng theo điểm 11, trong đó thông điệp HTTP là thông điệp yêu cầu HTTP và trường là trường đường, và trong đó nội dung của trường đường là Phần tử nhận dạng tài nguyên đồng nhất (Uniform Resource Identifier, URI) yêu cầu.

13. Thiết bị mạng theo điểm 10, trong đó thông tin gồm có một hoặc nhiều biểu thức thông thường mà chỉ báo một hoặc nhiều đoạn.

14. Thiết bị mạng theo điểm 10, trong đó chính sách bảo vệ được gồm có trong thông điệp.

15. Thiết bị mạng theo điểm 10, trong đó hệ mạch xử lý còn được tạo cấu hình để, đáp lại việc nhận thông điệp, truyền yêu cầu tìm ra đến chức năng kho mạng (network repository function, NRF), yêu cầu sự tìm ra của chính sách bảo vệ để bảo vệ thông điệp, và nhận chính sách bảo vệ đáp lại yêu cầu tìm ra.

16. Thiết bị mạng theo điểm 10, trong đó hệ mạch xử lý còn được tạo cấu hình để nhận chính sách bảo vệ từ thiết bị mạng trong đường mà thông điệp đi từ nguồn của thông điệp đến đích của thông điệp.

17. Thiết bị mạng theo điểm 10, trong đó thiết bị mạng là Máy ủy nhiệm bảo vệ mép an toàn (Security Edge Protection Proxy, SEPP).

18. Thiết bị mạng theo điểm 17, trong đó SEPP bao gồm SEPP trong mạng tạm trú và vSEPP trong mạng thường trú, hSEPP.

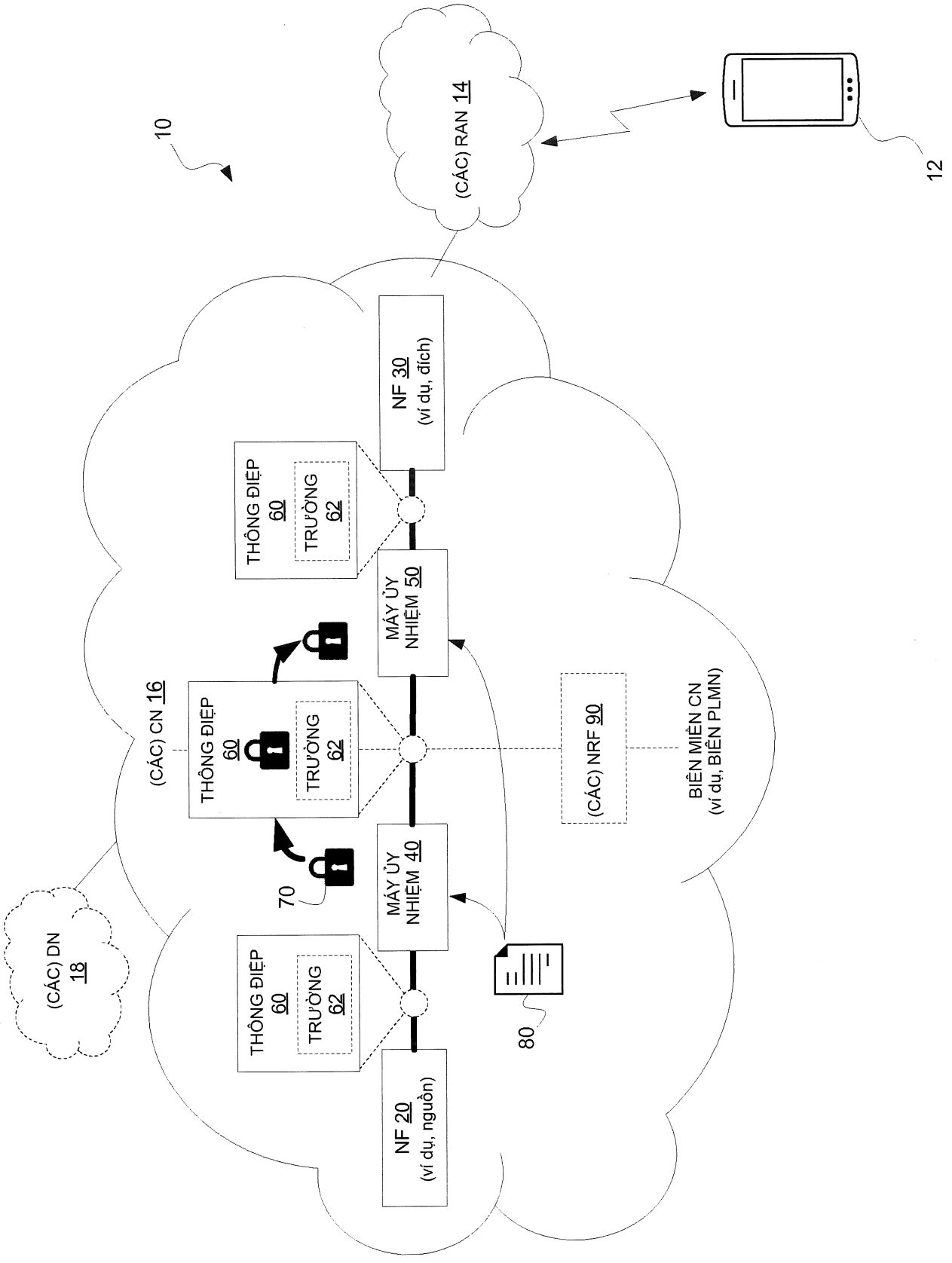
10
(CÁC) RAN 14
12
(CÁC) CN 16
(CÁC) DN 18
NF 30 (ví dụ, đích)
NF 20 (ví dụ, nguồn)
MÁY ỦY NHIỆM 50
MÁY ỦY NHIỆM 40
THÔNG ĐIỆP 60
TRƯỜNG 62
70
80
(CÁC) NRF 90
BIÊN MIỀN CN (ví dụ, BIÊN PLMN)

FIG. 1

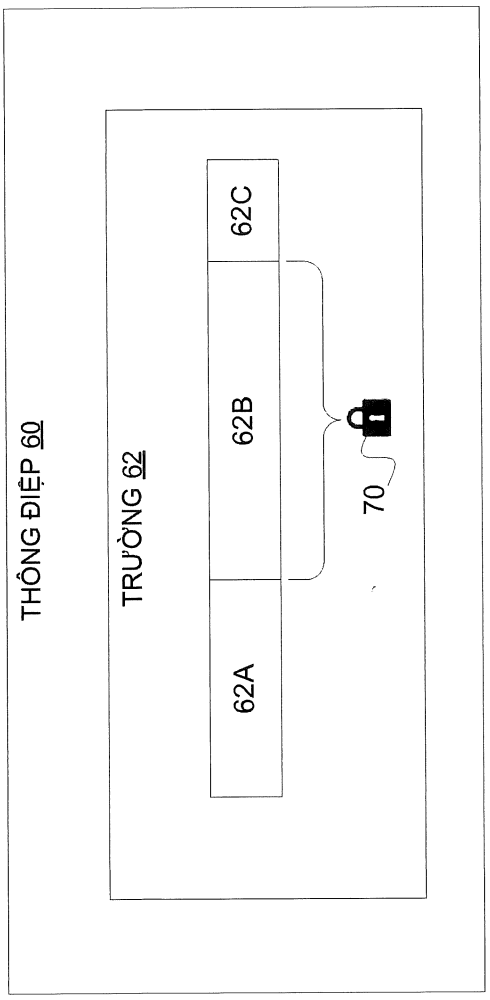
THÔNG ĐIỆP 60
TRƯỜNG 62
62A
62B
62C
70

FIG. 2A

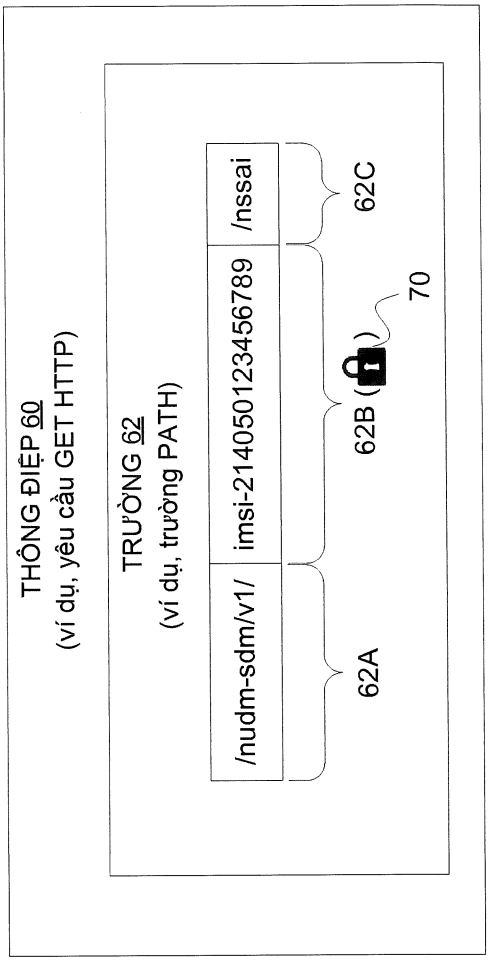
THÔNG ĐIỆP 60
(ví dụ, yêu cầu GET HTTP)
TRƯỜNG 62
(ví dụ, trường PATH)
/nudm-sdm/v1/
imsi-214050123456789
/nssai
62A
62B
62C
70

FIG. 2B

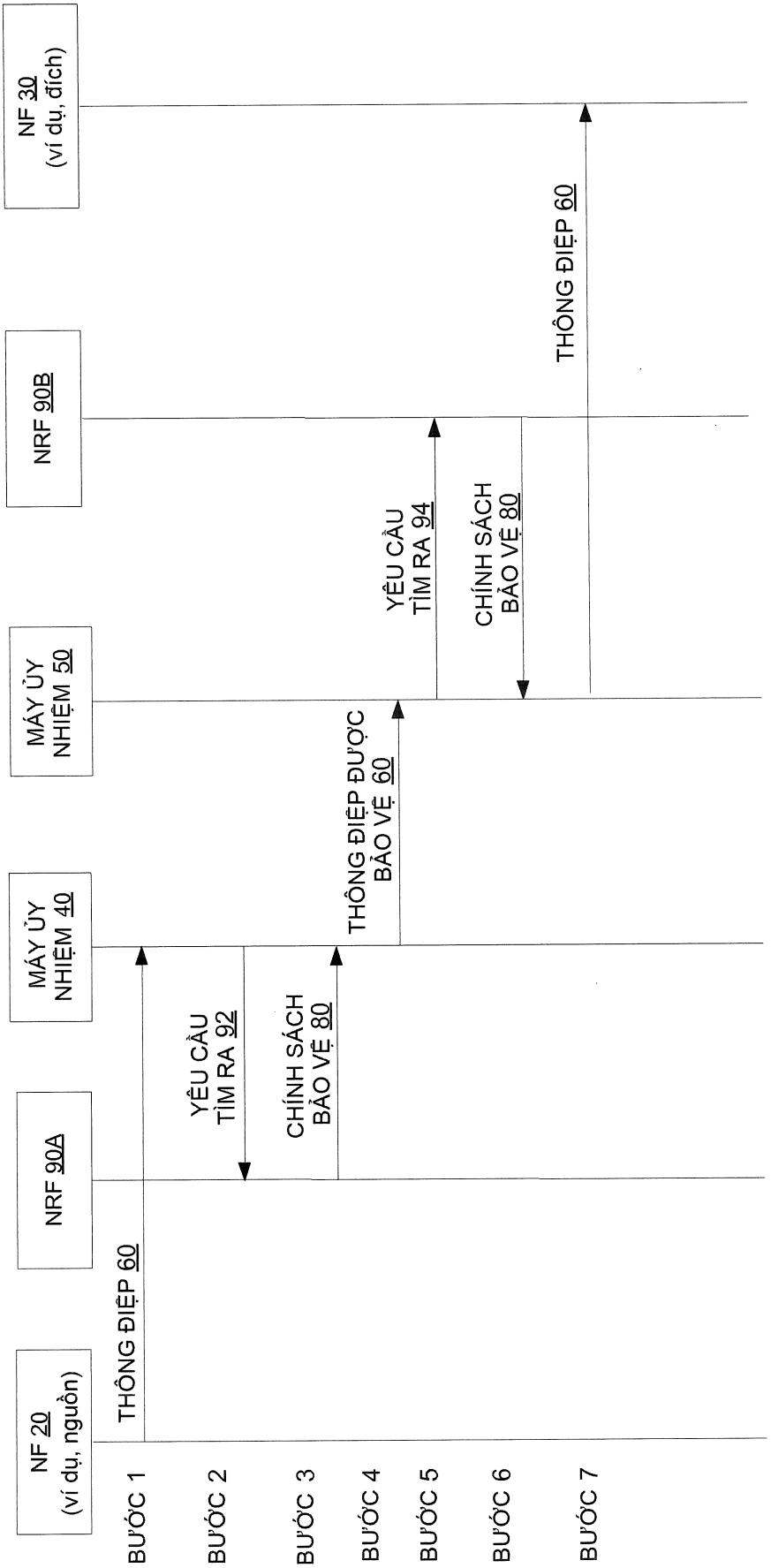
NF 20
(ví dụ, nguồn)
NRF 90A
MÁY ỦY
NHIỆM 40
MÁY ỦY
NHIỆM 50
NRF 90B
NF 30
(ví dụ, đích)
BƯỚC 1
BƯỚC 2
BƯỚC 3
BƯỚC 4
BƯỚC 5
BƯỚC 6
BƯỚC 7
THÔNG ĐIỆP 60
YÊU CẦU
TÌM RA 92
CHÍNH SÁCH
BẢO VỆ 80
THÔNG ĐIỆP ĐƯỢC
BẢO VỆ 60
YÊU CẦU
TÌM RA 94
CHÍNH SÁCH
BẢO VỆ 80
THÔNG ĐIỆP 60

FIG. 3

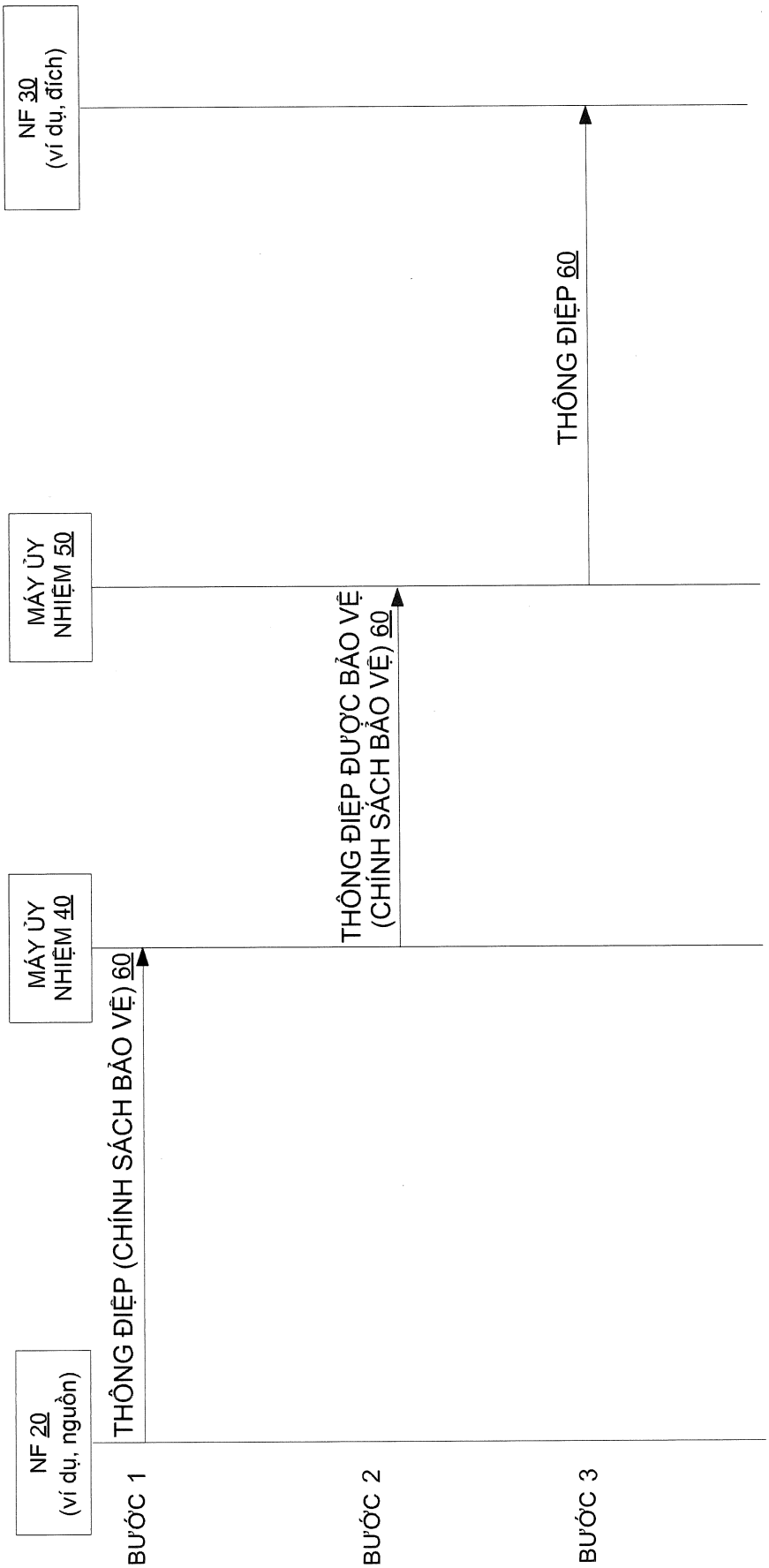
NF 20
(ví dụ, nguồn)
MÁY ỦY NHIỆM 40
MÁY ỦY NHIỆM 50
NF 30
(ví dụ, đích)
BƯỚC 1
BƯỚC 2
BƯỚC 3
THÔNG ĐIỆP (CHÍNH SÁCH BẢO VỆ) 60
THÔNG ĐIỆP ĐƯỢC BẢO VỆ (CHÍNH SÁCH BẢO VỆ) 60
THÔNG ĐIỆP 60

FIG. 4

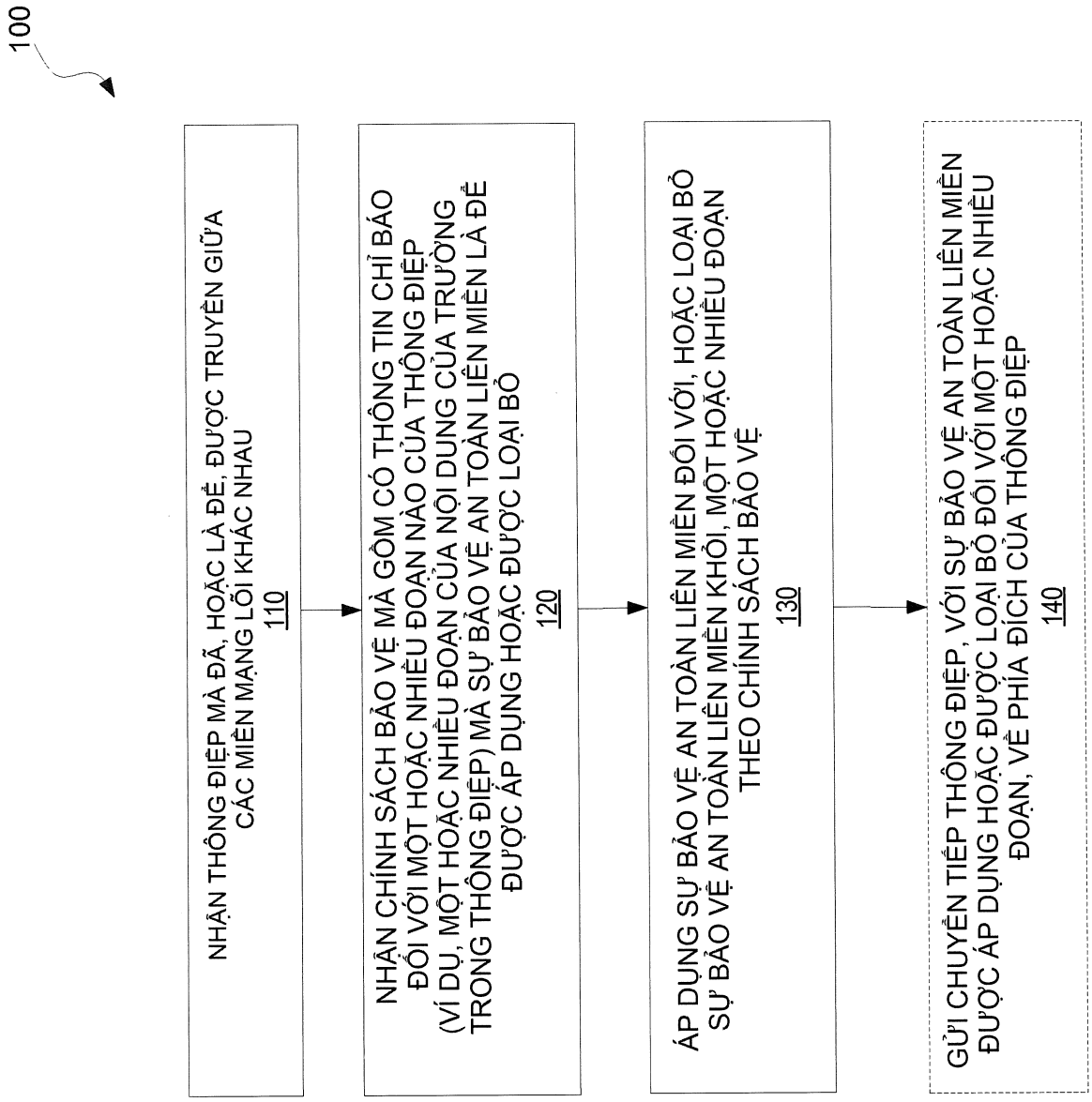
100
NHẬN THÔNG ĐIỆP MÀ ĐÃ, HOẶC LÀ ĐỂ, ĐƯỢC TRUYỀN GIỮA CÁC MIỀN MẠNG LỖI KHÁC NHAU
110
NHẬN CHÍNH SÁCH BẢO VỆ MÀ GỒM CÓ THÔNG TIN CHỈ BÁO ĐỐI VỚI MỘT HOẶC NHIỀU ĐOẠN NÀO CỦA THÔNG ĐIỆP (VÍ DỤ, MỘT HOẶC NHIỀU ĐOẠN CỦA NỘI DUNG CỦA TRƯỜNG TRONG THÔNG ĐIỆP) MÀ SỰ BẢO VỆ AN TOÀN LIÊN MIỀN LÀ ĐỂ ĐƯỢC ÁP DỤNG HOẶC ĐƯỢC LOẠI BỎ
120
ÁP DỤNG SỰ BẢO VỆ AN TOÀN LIÊN MIỀN ĐỐI VỚI, HOẶC LOẠI BỎ SỰ BẢO VỆ AN TOÀN LIÊN MIỀN KHỎI, MỘT HOẶC NHIỀU ĐOẠN THEO CHÍNH SÁCH BẢO VỆ
130
GỬI CHUYỂN TIẾP THÔNG ĐIỆP, VỚI SỰ BẢO VỆ AN TOÀN LIÊN MIỀN ĐƯỢC ÁP DỤNG HOẶC ĐƯỢC LOẠI BỎ ĐỐI VỚI MỘT HOẶC NHIỀU ĐOẠN, VỀ PHÍA ĐÍCH CỦA THÔNG ĐIỆP
140

FIG. 5

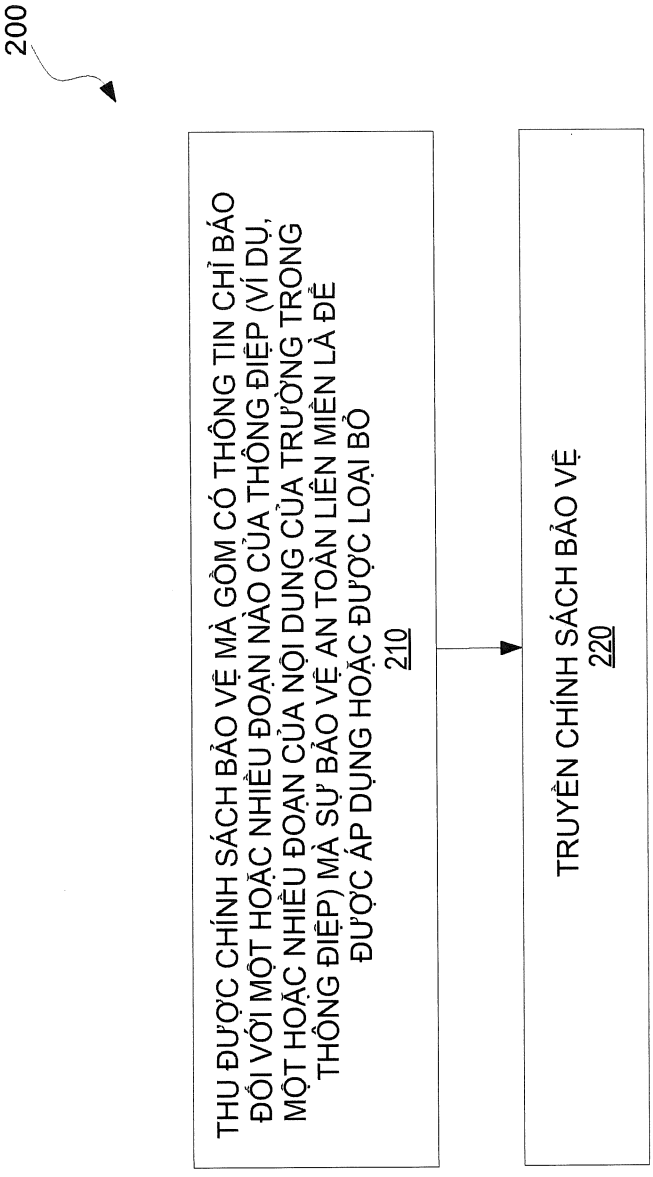
200
THU ĐƯỢC CHÍNH SÁCH BẢO VỆ MÀ GỒM CÓ THÔNG TIN CHỈ BÁO ĐỐI VỚI MỘT HOẶC NHIỀU ĐOẠN NÀO CỦA THÔNG ĐIỆP (VÍ DỤ, MỘT HOẶC NHIỀU ĐOẠN CỦA NỘI DUNG CỦA TRƯỜNG TRONG THÔNG ĐIỆP) MÀ SỰ BẢO VỆ AN TOÀN LIÊN MIỀN LÀ ĐỂ ĐƯỢC ÁP DỤNG HOẶC ĐƯỢC LOẠI BỎ
210
TRUYỀN CHÍNH SÁCH BẢO VỆ
220

FIG. 6

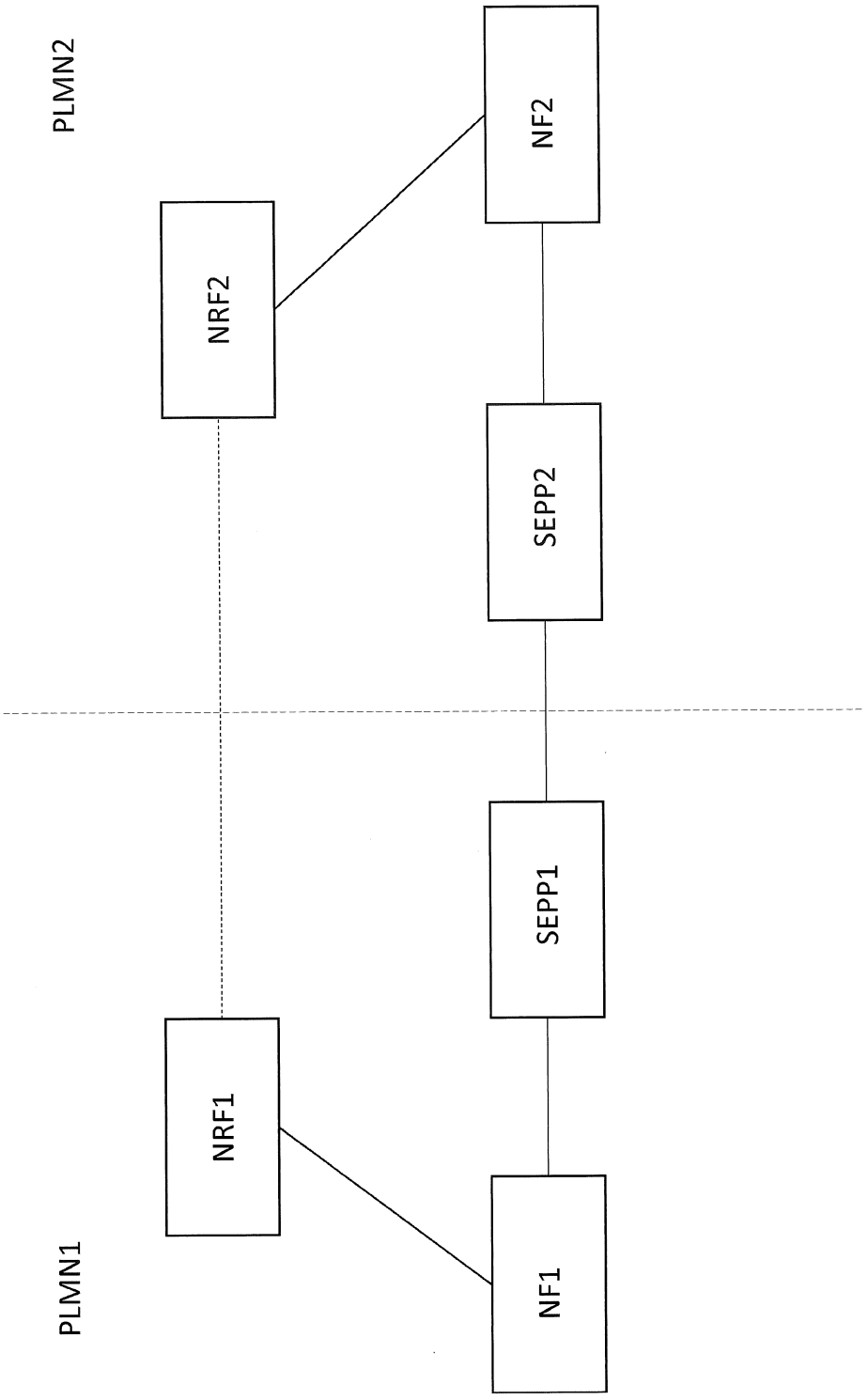

FIG. 7

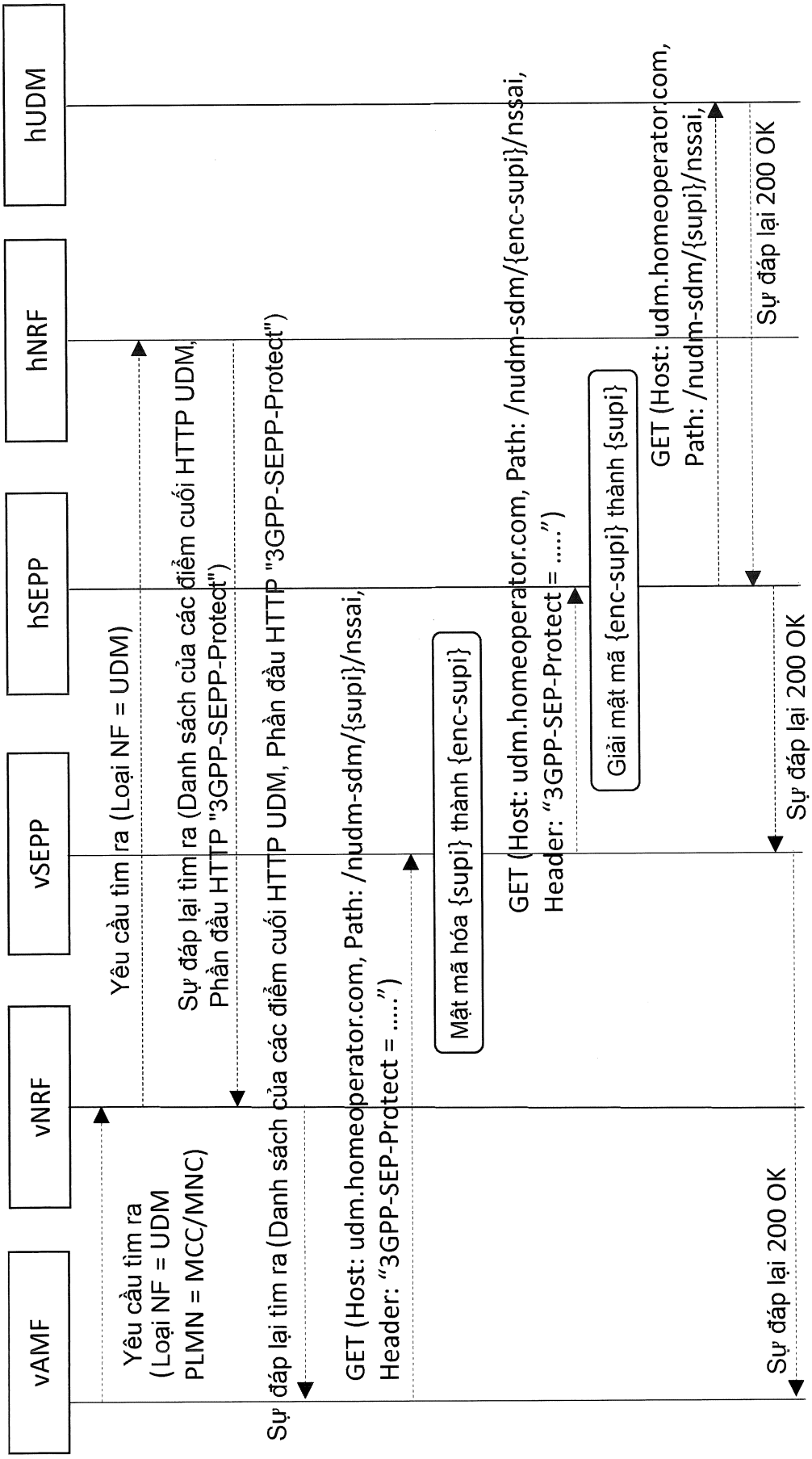
vAMF
vNRF
vSEPP
hSEPP
hNRF
hUDM
Yêu cầu tìm ra
(Loại NF = UDM
PLMN = MCC/MNC)
Yêu cầu tìm ra (Loại NF = UDM)
Sự đáp lại tìm ra (Danh sách của các điểm cuối HTTP UDM,
Phần đầu HTTP "3GPP-SEPP-Protect")
Sự đáp lại tìm ra (Danh sách của các điểm cuối HTTP UDM, Phần đầu HTTP "3GPP-SEPP-Protect")
GET (Host: udm.homeoperator.com, Path: /nudm-sdm/{supi}/nssai,
Header: "3GPP-SEP-Protect = ...")
Mật mã hóa {supi} thành {enc-supi}
GET (Host: udm.homeoperator.com, Path: /nudm-sdm/{enc-supi}/nssai,
Header: "3GPP-SEP-Protect = ...")
Giải mật mã {enc-supi} thành {supi}
GET (Host: udm.homeoperator.com,
Path: /nudm-sdm/{supi}/nssai,
Sự đáp lại 200 OK
Sự đáp lại 200 OK
Sự đáp lại 200 OK

FIG. 8

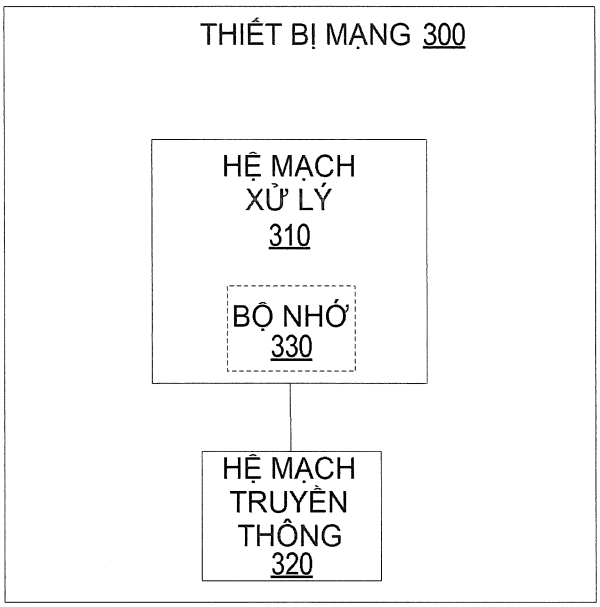
THIẾT BỊ MẠNG 300
HỆ MẠCH XỬ LÝ 310
BỘ NHỚ 330
HỆ MẠCH TRUYỀN THÔNG 320

FIG. 9A

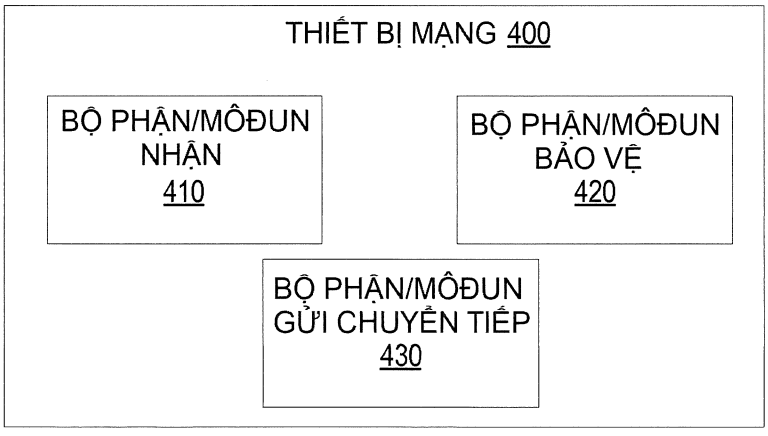
THIẾT BỊ MẠNG 400
BỘ PHẬN/MÔĐUN NHẬN 410
BỘ PHẬN/MÔĐUN BẢO VỆ 420
BỘ PHẬN/MÔĐUN GỬI CHUYỂN TIẾP 430

FIG. 9B

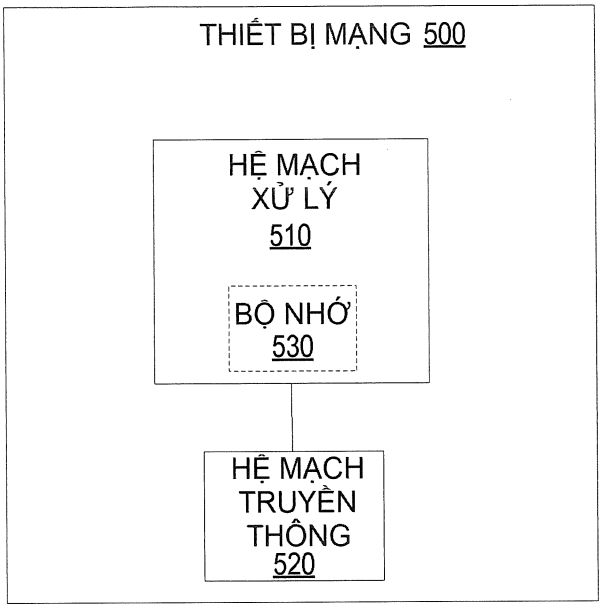

FIG. 10A

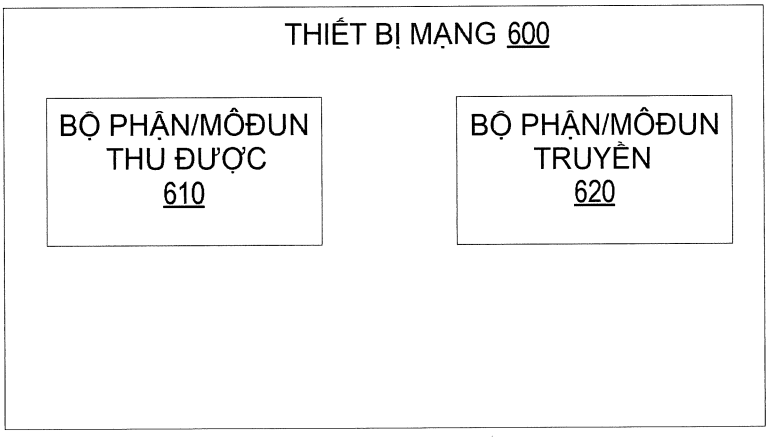

FIG. 10B