(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) **1-0039192**

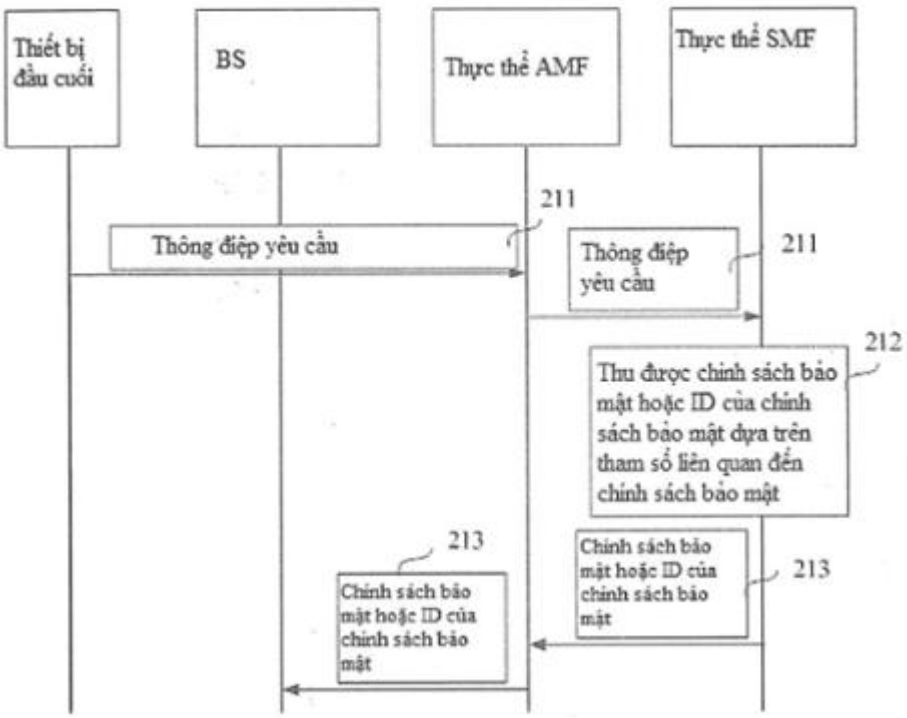
(51)[2019.01] **H04W 12/02**

(13) **B**

(21) 1-2019-06535
(22) 31/07/2017
(86) PCT/CN2017/095348 31/07/2017
(87) WO2018/201630 08/11/2018
(30) PCT/CN2017/083362 05/05/2017 CN
(45) 25/03/2024 432
(43) 30/01/2020 382A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District Shenzhen, Guangdong 518129, China
(72) LI, He (CN); CHEN, Jing (CN); HU, Li (CN).
(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) HỆ THỐNG TRUYỀN THÔNG, THỰC THỂ THỰC HIỆN CHỨC NĂNG QUẢN LÝ PHIÊN, VÀ VẬT LƯU TRỮ MÁY TÍNH ĐỌC ĐƯỢC

(57) Sáng chế đề xuất hệ thống truyền thông, phương pháp truyền thông, thực thể chức năng quản lý phiên (session management function, SMF), trạm cơ sở (base station, BS), thiết bị đầu cuối và vật lưu trữ máy tính đọc được. Hệ thống truyền thông bao gồm thực thể SMF và BS; thực thể SMF được tạo cấu hình để: nhận thông điệp yêu cầu, trong đó thông điệp yêu cầu bao gồm tham số liên quan của chính sách bảo mật; thu được chính sách bảo mật dựa trên tham số liên quan của chính sách bảo mật; và gửi chính sách bảo mật đến BS, trong đó chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối; BS được tạo cấu hình để: nhận chính sách bảo mật được gửi bởi thực thể SMF; và kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng khi chính sách bảo mật được nhận bởi BS bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn và thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.


Thiết bị đầu cuối
BS
Thực thể AMF
Thực thể SMF
211
Thông điệp yêu cầu
Thông điệp yêu cầu
211
212
Thu được chính sách bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật
213
Chính sách bảo mật hoặc ID của chính sách bảo mật
213
Chính sách bảo mật hoặc ID của chính sách bảo mật

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ truyền thông không dây, và cụ thể là, đến hệ thống, phương pháp truyền thông, thực thể chức năng quản lý phiên, trạm cơ sở (base station, BS), thiết bị đầu cuối và vật lưu trữ máy tính đọc được.

Tình trạng kỹ thuật của sáng chế

Trong hệ thống tiến hóa dài hạn (Long Term Evolution, LTE), thiết bị đầu cuối và BS thực hiện các hoạt động bảo mật chẳng hạn mật mã hóa/giải mã và bảo vệ tính toàn vẹn, để bảo vệ mật mã hóa và bảo vệ tính toàn vẹn cho báo hiệu. Do các thiết bị đầu cuối khác nhau có các dung lượng bảo mật khác nhau, chẳng hạn, hỗ trợ các thuật toán mật mã hóa hoặc các thuật báo bảo vệ tính toàn vẹn khác nhau, trước khi bảo vệ mật mã hóa và bảo vệ tính toàn vẹn được thực hiện ở tầng truy nhập (Access Stratum, AS), tập các thuật toán bảo mật cần được thương lượng giữa thiết bị đầu cuối và BS. Quá trình thương lượng các thuật toán bảo mật bao gồm các bước sau:

1. Thiết bị đầu cuối gửi yêu cầu đính kèm đến thực thể quản lý di động (Mobility Management Entity, MME) bằng cách sử dụng BS. Yêu cầu đính kèm mang thuật toán được hỗ trợ bởi thiết bị đầu cuối.

2. BS lựa chọn, dựa trên thuật toán được tiền tạo cấu hình được phép bởi mạng phục vụ để sử dụng và kết hợp với thuật toán mà được hỗ trợ bởi thiết bị đầu cuối và được chuyển tiếp bởi MME, thuật toán bảo mật được hỗ trợ bởi mạng phục vụ. Thuật toán bảo mật bao gồm thuật toán mật mã hóa và thuật toán bảo vệ tính toàn vẹn. BS tạo khóa mật mã hóa AS dựa trên thuật toán mật mã hóa được lựa chọn và tạo khóa bảo vệ tính toàn vẹn dựa trên thuật toán bảo vệ tính toàn vẹn. Thuật toán bảo mật được hỗ trợ bởi mạng phục vụ và được lựa chọn bởi BS là cả thuật toán bảo mật của mặt phẳng người dùng lẫn thuật toán bảo mật được áp dụng cho mặt phẳng báo hiệu.

toán bảo mật được áp dụng cho mặt phẳng báo hiệu.

3. Bằng cách sử dụng thủ tục lệnh chế độ bảo mật (Security mode command, SMC) AS, thiết bị đầu cuối áp dụng thuật toán bảo mật được lựa chọn bởi BS cho mặt phẳng người dùng và mặt phẳng báo hiệu. Chẳng hạn, thuật toán mật mã hóa và thuật toán bảo vệ tính toàn vẹn được lựa chọn bởi BS được mang trong SMC AS và được gửi đến thiết bị đầu cuối.

Theo giải pháp kỹ thuật đã biết, thuật toán bảo mật được áp dụng cho cả mặt phẳng người dùng lẫn mặt phẳng báo hiệu được xác định bằng cách sử dụng thủ tục SMC AS, và thuật toán bảo mật bao gồm thuật toán mật mã hóa và thuật toán bảo vệ tính toàn vẹn. Giải pháp thương lượng của thuật toán bảo mật này tương đối cố định. Chẳng hạn, tập các thuật toán bảo mật giống nhau áp dụng được cho mặt phẳng người dùng và mặt phẳng báo hiệu và không thể được tách rời. Trong ví dụ khác, thuật toán mật mã hóa và thuật toán bảo vệ tính toàn vẹn cần được xác định cùng lúc và không thể được tách rời. Do vậy, thuật toán thương lượng bảo mật tương đối cố định, và không thể làm thích ứng với các kịch bản ứng dụng thay đổi được và linh hoạt.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp truyền thông, thiết bị liên quan, và vật lưu trữ, để làm thích ứng với giải pháp trong đó thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng có thể được thương lượng linh hoạt và độc lập.

Theo khía cạnh thứ nhất, phương án thực hiện sáng chế đề xuất phương pháp truyền thông, bao gồm: thu được, bởi BS, chính sách bảo mật, trong đó chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối; và khi thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo BS để kích hoạt bảo vệ tính toàn vẹn thiết bị đầu cuối, gửi, bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối. Theo cách này, liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối có thể được lựa chọn linh hoạt dựa trên chính sách bảo mật. Ngoài ra, chỉ khi bảo vệ tính toàn vẹn được kích hoạt cho thiết bị đầu cuối, BS gửi thuật toán bảo

vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối. Một mặt, do thuật toán bảo mật mặt phẳng người dùng được thương lượng độc lập, tính linh hoạt của việc xác định riêng rẽ thuật toán bảo mật mặt phẳng người dùng và thuật toán bảo mật mặt phẳng báo hiệu được cải thiện. Nói theo cách khác, do thông tin chỉ báo bảo vệ tính toàn vẹn được thêm vào, tính linh hoạt trong việc xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích của thiết bị đầu cuối được cải thiện.

Một cách tùy chọn, thông tin chỉ báo bảo vệ tính toàn vẹn là bộ nhận dạng (identifier, ID) của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Tức là, nếu được xác định rằng chính sách bảo mật mang ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng, có thể xác định được rằng BS kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối. Chính sách bảo mật theo phương án thực hiện có thể mang một hoặc nhiều ID của các thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng (có thể được gọi là danh sách thuật toán). Thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được mang trong chính sách bảo mật theo phương án thực hiện có thể được xác định dựa trên ít nhất một trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS. Nói theo cách khác, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được mang trong chính sách bảo mật là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ.

Một cách tùy chọn, việc thu được, bởi BS, chính sách bảo mật có thể là việc nhận, bởi BS, chính sách bảo mật từ phần tử mạng khác, hoặc có thể là việc xác định, bởi BS, chính sách bảo mật từ ít nhất một chính sách bảo mật được lưu trữ trước trên BS. Chính sách bảo mật được lưu trữ trước ở phía BS cũng có thể là chính sách bảo mật được tiền tạo cấu hình ở phía BS. BS thu được, theo nhiều cách, chính sách bảo mật từ ít nhất một chính sách bảo mật được lưu trữ trước trên BS. Chẳng hạn, chính sách bảo mật tương ứng với ID của thiết bị đầu cuối và được lưu trữ trên BS có thể được xác định dựa trên phép tương ứng giữa ID của thiết bị đầu cuối và chính sách bảo mật được lưu trữ trước trên BS.

Trong ví dụ khác, chính sách bảo mật tương ứng với ID phiên và được lưu trữ trên BS có thể được xác định dựa trên phép tương ứng giữa ID phiên và chính sách bảo mật được lưu trữ trước trên BS. Giải pháp này có thể giống như giải pháp thu được chính sách bảo mật bởi thực thể chức năng quản lý phiên (Session Management Function, SMF). Các chi tiết không được mô tả ở đây.

Một cách tùy chọn, việc gửi, bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối bao gồm: gửi, bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối bằng cách sử dụng báo hiệu điều khiển tài nguyên vô tuyến (Radio Resource control, RRC). Giải pháp theo phương án thực hiện sáng chế được triển khai bằng cách tận dụng lại báo hiệu RRC theo giải pháp kỹ thuật đã biết, sao cho thực hiện tương thích tốt hơn với giải pháp kỹ thuật đã biết, và chỉnh sửa giải pháp kỹ thuật đã biết là tương đối nhỏ.

Theo triển khai tùy chọn trong đó BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối, BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích đến thiết bị đầu cuối, và thiết bị đầu cuối cũng xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích nhận được làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Tức là, BS gửi thuật toán bảo vệ tính toàn vẹn đến thiết bị đầu cuối, và thuật toán bảo vệ tính toàn vẹn là cả thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng.

Một cách tùy chọn, trước khi gửi, bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối, phương pháp còn bao gồm: xác định, bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS. Theo cách này, cả khả năng bảo mật của thiết bị đầu cuối và khả năng bảo mật của BS có thể được xem xét, sao cho thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích được xác định so khớp với cả khả năng bảo mật của thiết bị đầu cuối lẫn khả năng bảo mật của BS.

Một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng

được phép bởi BS là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, sao chho thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích tốt hơn ở phía BS có thể được lựa chọn. Theo cách khác, một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, sao cho thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích tốt hơn ở phía thiết bị đầu cuối có thể được lựa chọn.

Một cách tùy chọn, chính sách bảo mật còn bao gồm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, và the xác định, bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS bao gồm: xác định, bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ. Theo cách này, cả khả năng bảo mật của thiết bị đầu cuối và khả năng bảo mật của BS có thể được xem xét, và trạng thái thực của mạng phục vụ cũng được xem xét. Do vậy, một mặt, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích được xác định có thể so khớp khả năng bảo mật của thiết bị đầu cuối và khả năng bảo mật của BS; Nói theo cách khác, so khớp tốt hơn trạng thái thực của mạng phục vụ.

Một cách tùy chọn, khi chính sách bảo mật còn bao gồm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, BS cũng có thể xác định thuật toán, được bao gồm trong chính sách bảo mật, khác ngoài thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Chẳng hạn, một thuật toán có thể được xác định từ thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS như là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích.

Một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, sao cho thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích tốt hơn dựa trên mạng phục vụ có thể được lựa chọn.

Một cách tùy chọn, phương pháp còn bao gồm: khi chính sách bảo mật còn bao gồm thông tin chỉ báo mật mã hóa, và thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS để kích hoạt bảo vệ mật mã hóa cho thiết bị đầu cuối, gửi, bởi BS, thuật toán mật mã hóa mặt phẳng người dùng đích đến thiết bị đầu cuối; hoặc khi chính sách bảo mật còn bao gồm độ dài khóa, gửi, bởi BS, độ dài khóa đến thiết bị đầu cuối; hoặc khi chính sách bảo mật còn bao gồm thông tin chỉ báo D - H, và thông tin chỉ báo D - H được sử dụng để chỉ báo BS để kích hoạt D-H cho thiết bị đầu cuối, gửi, bởi BS, khóa liên quan D-H đến thiết bị đầu cuối. Theo cách này, thông tin bất kỳ trong chính sách bảo mật có thể được chỉ báo linh hoạt hơn, sao cho chính sách bảo mật cuối cùng được xác định được làm thích ứng hơn với kịch bản ứng dụng phức tạp.

Một cách tùy chọn, trước khi gửi, bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối, phương pháp còn bao gồm: nhận, bởi BS, chất lượng dịch vụ (quality of service, QoS) của phiên hiện tại của thiết bị đầu cuối từ thực thể SMF, và phân phối, bởi BS, kênh mang vô tuyến dữ liệu (data radio bearer, DRB) đích đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS.

Để tiết kiệm tài nguyên, một cách tùy chọn, việc phân phối, bởi BS, DRB đích đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS bao gồm: khi ít nhất một DRB lịch sử thỏa mãn điều kiện thứ nhất tồn tại trên BS, xác định, bởi BS, một trong ít nhất một DRB lịch sử thỏa mãn điều kiện thứ nhất làm DRB đích, trong đó QoS được hỗ trợ bởi mỗi DRB của ít nhất một DRB lịch sử thỏa mãn điều kiện thứ nhất giống như QoS của phiên hiện tại, và chính sách bảo mật giống như chính sách bảo mật được hỗ trợ bởi mỗi DRB.

Một cách tùy chọn, điều kiện thứ nhất bao gồm việc QoS của hai DRB là

giống nhau, và các chính sách bảo mật của hai DRB là giống nhau.

Để tiết kiệm tài nguyên, theo giải pháp tùy chọn khác, việc phân phối, bởi BS, DRB đích đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS bao gồm: khi DRB lịch sử không thỏa mãn điều kiện thứ nhất tồn tại trên BS, nhưng ít nhất một DRB lịch sử thỏa mãn điều kiện thứ hai tồn tại trên BS, cập nhật, bởi BS, một DRB lịch sử của ít nhất một DRB lịch sử thỏa mãn điều kiện thứ hai, và xác định DRB lịch sử làm DRB đích, trong đó QoS được hỗ trợ bởi mỗi DRB của ít nhất một DRB lịch sử thỏa mãn điều kiện thứ hai giống như QoS của phiên hiện tại, và chính sách bảo mật so khớp chính sách bảo mật được hỗ trợ bởi mỗi DRB; hoặc QoS được hỗ trợ bởi mỗi DRB của ít nhất một DRB lịch sử thỏa mãn điều kiện thứ hai so khớp QoS của phiên hiện tại, và chính sách bảo mật giống như chính sách bảo mật được hỗ trợ bởi mỗi DRB; hoặc QoS được hỗ trợ bởi mỗi DRB của ít nhất một DRB lịch sử thỏa mãn điều kiện thứ hai so khớp QoS của phiên hiện tại, và chính sách bảo mật so khớp chính sách bảo mật được hỗ trợ bởi mỗi DRB.

Một cách tùy chọn, điều kiện thứ hai bao gồm việc QoS của hai DRB so khớp nhau, và các chính sách bảo mật của hai DRB là giống nhau. Theo cách khác, một cách tùy chọn, điều kiện thứ hai bao gồm việc QoS của hai DRB là giống nhau, và các chính sách bảo mật của hai DRB so khớp nhau. Theo cách khác, một cách tùy chọn, điều kiện thứ hai bao gồm việc QoS của hai DRB so khớp nhau, và các chính sách bảo mật của hai DRB so khớp nhau.

Để lựa chọn DRB đích thích hợp, theo giải pháp tùy chọn khác, việc phân phối, bởi BS, DRB đích đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS bao gồm: khi DRB lịch sử không thỏa mãn điều kiện thứ nhất tồn tại trên BS, và ít nhất một DRB lịch sử không thỏa mãn điều kiện thứ hai tồn tại trên BS, tạo, bởi BS, DRB đích cho thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật and QoS.

Để lựa chọn DRB đích thích hợp, theo giải pháp tùy chọn khác, việc phân phối, bởi BS, DRB đích đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS bao gồm: khi DRB lịch sử không thỏa mãn điều kiện thứ nhất tồn tại trên BS, tạo, bởi BS, DRB đích đối với thiết bị đầu cuối dựa trên ít

nhất một trong chính sách bảo mật và QoS.

Để lựa chọn DRB đích thích hợp, theo giải pháp tùy chọn khác, việc phân phối, bởi BS, DRB đích đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS bao gồm: tạo, bởi BS, DRB đích cho thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS.

Một cách tùy chọn, việc thu được, bởi BS, chính sách bảo mật bao gồm: nhận, bởi BS, chính sách bảo mật từ thực thể SMF; hoặc nhận, bởi BS, ID của chính sách bảo mật từ thực thể SMF, và thu được chính sách bảo mật dựa trên ID của chính sách bảo mật.

Một cách tùy chọn, theo phương án thực hiện sáng chế, phương pháp còn bao gồm: thu được, bởi BS, thuật toán bảo mật mặt phẳng báo hiệu được hỗ trợ bởi thiết bị đầu cuối; xác định, bởi BS, thuật toán bảo mật mặt phẳng báo hiệu đích dựa trên mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo mật mặt phẳng báo hiệu được phép bởi BS; và thêm, bởi BS, thuật toán bảo mật mặt phẳng báo hiệu đích đến SMC AS, và gửi SMC AS đến thiết bị đầu cuối. Theo cách này, thuật toán mặt phẳng báo hiệu và thuật toán bảo mật mặt phẳng người dùng có thể được tách rời, sao cho thuật toán bảo mật mặt phẳng người dùng và mặt phẳng báo hiệu thuật toán bảo mật được thương lượng riêng rẽ, để tạo cơ sở để linh hoạt hơn xác định thuật toán bảo mật mặt phẳng người dùng.

Một cách tùy chọn, khi xác định kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Một cách tùy chọn, khi xác định kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, BS kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Một cách tùy chọn, khi BS xác định không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng tạm thời, hoặc BS hiện tại không thể xác định liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Một cách tùy chọn, khi BS xác định không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng tạm thời, hoặc BS hiện tại không thể xác định liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, BS không kích hoạt bảo

vệ mật mã hóa mặt phẳng người dùng.

"Tạm thời" nghĩa là có chu kỳ thời gian. Việc bảo vệ tính toàn vẹn mặt phẳng người dùng không được kích hoạt tạm thời nghĩa là bảo vệ tính toàn vẹn mặt phẳng người dùng không được kích hoạt trong một chu kỳ thời gian, nhưng bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt trong chu kỳ thời gian khác. Việc bảo vệ mật mã hóa mặt phẳng người dùng không được kích hoạt tạm thời nghĩa là bảo vệ mật mã hóa mặt phẳng người dùng không được kích hoạt trong một chu kỳ thời gian, nhưng bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt trong chu kỳ thời gian khác.

Theo triển khai tùy chọn, quy định rằng trong mạng mà sau khi SMC AS được nhận, bảo vệ mật mã hóa mặt phẳng người dùng có thể được kích hoạt, nhưng liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng được thông báo cho thiết bị đầu cuối bằng cách sử dụng thông điệp tái cấu hình RRC. Trong trường hợp này, thiết bị đầu cuối không thể xác định liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Theo triển khai tùy chọn khác, quy định rằng trong mạng mà sau khi SMC AS được nhận, chỉ bảo mật mặt phẳng báo hiệu được kích hoạt (bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc bảo vệ mật mã hóa mặt phẳng báo hiệu được kích hoạt), nhưng liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng được thông báo cho thiết bị đầu cuối bằng cách sử dụng thông điệp tái cấu hình RRC. Trong trường hợp này, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng không thể được xác định.

Một cách tùy chọn, việc không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bao gồm: khi liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng không thể được xác định hoặc được xác định không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng tạm thời, tạo khóa bảo vệ tính toàn vẹn mặt phẳng người dùng nhưng không thực hiện bảo vệ tính toàn vẹn mặt phẳng người dùng bằng cách sử dụng khóa bảo vệ tính toàn vẹn mặt phẳng người dùng; và khi được xác định kích hoạt bảo vệ tính toàn vẹn mặt phẳng người

dùng, thực hiện bảo vệ tính toàn vẹn mặt phẳng người dùng bằng cách sử dụng khóa bảo vệ tính toàn vẹn mặt phẳng người dùng. Theo triển khai này, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng thu được trước khi khóa bảo vệ tính toàn vẹn mặt phẳng người dùng được tạo, chẳng hạn, mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn cũng có thể được sử dụng làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng.

Một cách tùy chọn, việc không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bao gồm: khi được xác định kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, tạo khóa bảo vệ tính toàn vẹn mặt phẳng người dùng, và thực hiện bảo vệ tính toàn vẹn mặt phẳng người dùng bằng cách sử dụng khóa bảo vệ tính toàn vẹn mặt phẳng người dùng. Tức là, khi liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng không thể được xác định hoặc được xác định không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng tạm thời, khóa bảo vệ tính toàn vẹn mặt phẳng người dùng không thể được tạo khi bảo vệ tính toàn vẹn mặt phẳng người dùng không được kích hoạt. Một cách tương ứng, chẳng hạn, đối với thiết bị đầu cuối và BS, nếu xác định được rằng thiết bị đầu cuối và BS luông không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng (chẳng hạn, có thể là điều kiện định trước), khóa bảo vệ tính toàn vẹn mặt phẳng người dùng không thể được tạo.

Một cách tùy chọn, việc không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng bao gồm: khi liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng không thể được xác định hoặc được xác định không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng tạm thời, tạo khóa mật mã hóa mặt phẳng người dùng, nhưng không thực hiện bảo vệ mật mã hóa mặt phẳng người dùng bằng cách sử dụng khóa mật mã hóa mặt phẳng người dùng; và khi được xác định kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, thực hiện bảo vệ mật mã hóa mặt phẳng người dùng bằng cách sử dụng khóa mật mã hóa mặt phẳng người dùng. Theo triển khai này, thuật toán mật mã hóa mặt phẳng người dùng thu được trước khi khóa mật mã hóa mặt phẳng người dùng được tạo, chẳng hạn, mặt phẳng báo hiệu thuật toán mật mã hóa cũng có thể được sử dụng làm thuật toán mật mã hóa mặt phẳng người dùng. Một cách tùy chọn, việc không

kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng bao gồm: khi được xác định kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, tạo khóa mật mã hóa mặt phẳng người dùng, và thực hiện bảo vệ mật mã hóa mặt phẳng người dùng bằng cách sử dụng khóa mật mã hóa mặt phẳng người dùng. Tức là, khi liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng không thể được xác định hoặc được xác định không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng tạm thời, khóa mật mã hóa mặt phẳng người dùng không thể được tạo. Một cách tương ứng, chẳng hạn, đối với thiết bị đầu cuối và BS, nếu xác định được rằng thiết bị đầu cuối và BS luôn không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng (chẳng hạn, có thể là điều kiện định trước), khóa mật mã hóa mặt phẳng người dùng không thể được tạo.

Một cách tùy chọn, BS thu được thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa, và xác định, dựa trên thông tin chỉ báo bảo vệ tính toàn vẹn thu được, liệu có kích hoạt bảo vệ tính toàn vẹn, hoặc xác định, dựa trên thông tin chỉ báo mật mã hóa, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, và thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Một cách tùy chọn, có nhiều cách thu được thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa bởi BS. Chẳng hạn, BS tạo thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa thông qua việc xác định hoặc nhận ít nhất một trong thông tin chỉ báo bảo vệ tính toàn vẹn và thông tin chỉ báo mật mã hóa được gửi bởi phần tử mạng khác. Phần tử mạng khác có thể là thực thể SMF.

Một cách tùy chọn, BS có thể gửi ít nhất một trong thông tin chỉ báo bảo vệ tính toàn vẹn và thông tin chỉ báo mật mã hóa đến thiết bị đầu cuối, sao cho thiết bị đầu cuối xác định liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và/hoặc liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Theo cách khác, thiết bị đầu cuối xác định liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và/hoặc liệu có kích hoạt bảo vệ bảo vệ mật

mã hóa người dùng.

Một cách tùy chọn, thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể là thông tin bit hoặc ID của thuật toán. Chẳng hạn, thông tin chỉ báo bảo vệ tính toàn vẹn là ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Trong ví dụ khác, thông tin chỉ báo mật mã hóa là ID của thuật toán bảo vệ mật mã hóa mặt phẳng người dùng đích. Trong ví dụ khác, thông tin 1 bit được sử dụng để chỉ báo thông tin chỉ báo bảo vệ tính toàn vẹn hoặc thông tin chỉ báo mật mã hóa. Trong ví dụ khác, thông tin 2 bit được sử dụng để chỉ báo thông tin chỉ báo bảo vệ tính toàn vẹn và thông tin chỉ báo mật mã hóa. Theo khía cạnh thứ hai, phương án thực hiện sáng chế đề xuất phương pháp truyền thông, bao gồm: nhận, bởi thực thể SMF, thông điệp yêu cầu, trong đó thông điệp yêu cầu bao gồm tham số liên quan đến chính sách bảo mật; thu được, bởi thực thể SMF, chính sách bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật; và gửi, bởi thực thể SMF, chính sách bảo mật hoặc ID của chính sách bảo mật đến BS, trong đó chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối. Một mặt, do thuật toán bảo mật mặt phẳng người dùng được thương lượng độc lập, tính linh hoạt của việc xác định riêng rẽ thuật toán bảo mật mặt phẳng người dùng và thuật toán bảo mật mặt phẳng báo hiệu được cải thiện. Nói theo cách khác, do thông tin chỉ báo bảo vệ tính toàn vẹn được thêm vào, tính linh hoạt trong việc xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích của thiết bị đầu cuối được cải thiện.

Một cách tùy chọn, thông tin chỉ báo bảo vệ tính toàn vẹn là ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Tức là, nếu xác định được rằng chính sách bảo mật mang ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng, có thể xác định được rằng BS kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối. Chính sách bảo mật theo phương án thực hiện có thể mang một hoặc nhiều ID của các thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng (có thể được gọi là danh sách thuật toán). Thuật toán bảo vệ tính

toàn vẹn mặt phẳng người dùng được mang trong chính sách bảo mật theo phương án thực hiện có thể được xác định dựa trên ít nhất một trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS. Nói theo cách khác, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được mang trong chính sách bảo mật là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ.

Một cách tùy chọn, tham số liên quan đến chính sách bảo mật bao gồm ít nhất một trong ID của thiết bị đầu cuối, tên mạng dữ liệu (data network name, DNN) của thiết bị đầu cuối, ID của lát của thiết bị đầu cuối, QoS của thiết bị đầu cuối, và ID phiên của thiết bị đầu cuối. Theo cách này, chính sách bảo mật có thể được tạo thành dựa trên các ID khác nhau từ các khía cạnh khác nhau hoặc ở các độ chi tiết khác nhau, và điều này linh hoạt hơn.

Một cách tùy chọn, việc thu được, bởi thực thể SMF, chính sách bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật bao gồm: khi tham số liên quan đến chính sách bảo mật bao gồm ID của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên ID của thiết bị đầu cuối và mối quan hệ liên kết giữa ID của thiết bị đầu cuối và chính sách bảo mật. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của thiết bị đầu cuối, sao cho các thiết bị đầu cuối khác nhau có thể tương ứng với các chính sách bảo mật khác nhau.

Theo triển khai tùy chọn khác, việc thu được, bởi thực thể SMF, chính sách bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật bao gồm: khi tham số liên quan đến chính sách bảo mật bao gồm ID của lát của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên ID của lát của thiết bị đầu cuối và mối quan hệ liên kết giữa ID của lát và chính sách bảo mật. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của lát, sao cho thiết bị đầu cuối truy nhập các lát khác nhau có thể tương ứng với các chính sách bảo mật khác nhau.

Theo triển khai tùy chọn khác, việc thu được, bởi thực thể SMF, chính sách

bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật bao gồm: khi tham số liên quan đến chính sách bảo mật bao gồm ID phiên của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên ID phiên của thiết bị đầu cuối và mối quan hệ liên kết giữa ID phiên và chính sách bảo mật. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của phiên, sao cho thiết bị đầu cuối khởi tạo các phiên khác nhau có thể tương ứng với các chính sách bảo mật khác nhau.

Theo triển khai tùy chọn khác, việc thu được, bởi thực thể SMF, chính sách bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật bao gồm: khi tham số liên quan đến chính sách bảo mật bao gồm QoS của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên QoS của thiết bị đầu cuối. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của QoS, sao cho thiết bị đầu cuối khởi tạo các QoS khác nhau có thể tương ứng với các chính sách bảo mật khác nhau.

Một cách tùy chọn, chính sách bảo mật còn bao gồm ít nhất một của nội dung sau: thông tin chỉ báo mật mã hóa, trong đó thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS để kích hoạt bảo vệ mật mã hóa cho thiết bị đầu cuối; độ dài khóa; thông tin chỉ báo D - H, trong đó thông tin chỉ báo D - H được sử dụng để chỉ báo BS để kích hoạt D-H cho thiết bị đầu cuối; và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ. Theo cách này, thông tin bất kỳ trong chính sách bảo mật có thể được chỉ báo linh hoạt hơn, sao cho chính sách bảo mật cuối cùng được xác định được làm thích ứng hơn với kịch bản ứng dụng phức tạp.

Một cách tùy chọn, thực thể SMF gửi thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa đến BS. Thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, và thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo liệu có kích hoạt bảo vệ mật mã hóa. Một cách tùy chọn, thực thể SMF xác định liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và/hoặc liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng theo các cách triển khai. Dựa vào các phương án thực hiện tiếp theo, hoặc dựa vào triển khai trong đó

BS xác định liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và/hoặc liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, và các chi tiết không được mô tả lại ở đây.

Theo khía cạnh thứ ba, phương án thực hiện sáng chế đề xuất BS, trong đó BS bao gồm bộ nhớ, bộ thu phát, và bộ xử lý; bộ nhớ được tạo cấu hình để lưu trữ lệnh; bộ xử lý được tạo cấu hình để thực thi lệnh được lưu trữ trong bộ nhớ và điều khiển bộ thu phát để thực hiện nhận tín hiệu và gửi tín hiệu; và khi bộ xử lý thực thi lệnh được lưu trữ trong bộ nhớ, BS được tạo cấu hình để thực hiện phương pháp theo trường hợp bất kỳ của khía cạnh thứ nhất hoặc các triển khai của khía cạnh thứ nhất.

Theo khía cạnh thứ tư, phương án thực hiện sáng chế đề xuất thực thể SMF, trong đó thực thể SMF bao gồm bộ nhớ, bộ thu phát, và bộ xử lý; bộ nhớ được tạo cấu hình để lưu trữ lệnh; bộ xử lý được tạo cấu hình để thực thi lệnh được lưu trữ trong bộ nhớ và điều khiển bộ thu phát để thực hiện nhận tín hiệu và gửi tín hiệu; và khi bộ xử lý thực thi lệnh được lưu trữ trong bộ nhớ, thực thể SMF được tạo cấu hình để thực hiện phương pháp theo trường hợp bất kỳ của khía cạnh thứ hai hoặc các triển khai của khía cạnh thứ hai.

Theo khía cạnh thứ năm, phương án thực hiện sáng chế đề xuất BS, được tạo cấu hình để triển khai phương pháp theo trường hợp bất kỳ của khía cạnh thứ nhất hoặc các triển khai của khía cạnh thứ nhất, và bao gồm các môđun chức năng tương ứng, được tạo cấu hình riêng rẽ để triển khai các bước ở phương pháp nêu trên.

Theo khía cạnh thứ sáu, phương án thực hiện sáng chế đề xuất thực thể SMF, được tạo cấu hình để triển khai phương pháp theo trường hợp bất kỳ của khía cạnh thứ hai hoặc các triển khai của khía cạnh thứ hai, và bao gồm các môđun chức năng tương ứng, được tạo cấu hình riêng rẽ để triển khai các bước ở phương pháp nêu trên.

Theo khía cạnh thứ bảy, phương án thực hiện sáng chế đề xuất vật lưu trữ máy tính, trong đó vật lưu trữ máy tính lưu trữ lệnh; và khi lệnh chạy trên máy tính, máy tính thực hiệns phương pháp theo trường hợp bất kỳ của khía cạnh thứ nhất hoặc các triển khai khả thi của khía cạnh thứ nhất.

Theo khía cạnh thứ tám, phương án thực hiện sáng chế đề xuất vật lưu trữ máy tính, trong đó vật lưu trữ máy tính lưu trữ lệnh; và khi lệnh chạy trên máy tính, máy tính thực hiện phương pháp theo trường hợp bất kỳ của khía cạnh thứ hai hoặc các triển khai khả thi của khía cạnh thứ hai.

Theo khía cạnh thứ chín, phương án thực hiện sáng chế đề xuất sản phẩm chương trình máy tính bao gồm lệnh, và khi sản phẩm chương trình máy tính chạy trên máy tính, máy tính thực hiện phương pháp theo trường hợp bất kỳ của khía cạnh thứ nhất hoặc các triển khai khả thi của khía cạnh thứ nhất.

Theo khía cạnh thứ mười, phương án thực hiện sáng chế đề xuất sản phẩm chương trình máy tính bao gồm lệnh, và khi sản phẩm chương trình máy tính chạy trên máy tính, máy tính thực hiện phương pháp theo trường hợp bất kỳ của khía cạnh thứ hai hoặc các triển khai khả thi của khía cạnh thứ hai.

Theo các phương án thực hiện sáng chế, chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối. BS thu được chính sách bảo mật. Khi thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo BS để kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối, BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối. Theo cách này, liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối có thể được lựa chọn linh hoạt dựa trên chính sách bảo mật. Ngoài ra, chỉ khi bảo vệ tính toàn vẹn được kích hoạt cho thiết bị đầu cuối, BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối. Một mặt, do thuật toán bảo mật mặt phẳng người dùng được thương lượng độc lập, tính linh hoạt của việc xác định riêng rẽ thuật toán bảo mật mặt phẳng người dùng và thuật toán bảo mật mặt phẳng báo hiệu được cải thiện. Nói theo cách khác, do thông tin chỉ báo bảo vệ tính toàn vẹn được thêm vào, tính linh hoạt trong việc xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích của thiết bị đầu cuối được cải thiện.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ của kiến trúc hệ thống mà phương án thực hiện sáng chế áp

dụng được;

Fig.2 là lưu đồ của phương pháp truyền thông theo phương án thực hiện sáng chế;

Fig.2a là lưu đồ của phương pháp truyền thông khác theo phương án thực hiện sáng chế;

Fig.2b là lưu đồ của phương pháp truyền thông khác theo phương án thực hiện sáng chế;

Fig.3 là sơ đồ cấu trúc của BS theo phương án thực hiện sáng chế;

Fig.4 là sơ đồ cấu trúc của thiết bị đầu cuối theo phương án thực hiện sáng chế;

Fig.5 là sơ đồ cấu trúc của BS khác theo phương án thực hiện sáng chế; và

Fig.6 là sơ đồ cấu trúc của thiết bị đầu cuối khác theo phương án thực hiện sáng chế.

Mô tả chi tiết sáng chế

Fig.1 thể hiện ví dụ của sơ đồ của kiến trúc hệ thống mà các phương án thực hiện sáng chế áp dụng được. Như được thể hiện trên Fig.1, kiến trúc hệ thống 5G bao gồm thiết bị đầu cuối 101. Thiết bị đầu cuối 101 có thể truyền thông với một hoặc nhiều mạng lõi (core network, CN) bằng cách sử dụng mạng truy nhập vô tuyến (Radio Access Network, RAN). Thiết bị đầu cuối có thể đề cập đến thiết bị người dùng (User Equipment, UE), thiết bị đầu cuối truy nhập, khối thuê bao, trạm thuê bao, trạm di động, bảng điều khiển di động, trạm từ xa, thiết bị đầu cuối từ xa, thiết bị di động, thiết bị đầu cuối người dùng, thiết bị đầu cuối, thiết bị truyền thông không dây, đại lý người dùng, hoặc thiết bị người dùng. Thiết bị đầu cuối truy nhập có thể là điện thoại tế bào, điện thoại không dây, điện thoại giao thức khởi tạo phiên (Session Initiation Protocol, SIP), trạm vòng cục bộ không dây (Wireless Local Loop, WLL), thiết bị hỗ trợ số cá nhân (Personal Digital Assistant, PDA), thiết bị cầm tay có chức năng truyền thông không dây, thiết bị tính toán hoặc thiết bị xử lý khác được kết nối với modem không dây, thiết bị trong xe, thiết bị đeo tay, thiết bị đầu cuối trong mạng 5G tương lai, hoặc tương tự.

BS 102 được kết nối với thiết bị đầu cuối 101. Một cách tùy chọn, BS 102 có thể là 5G NodeB (generation NodeB, gNB), có thể là eNB tiến hóa, hoặc có thể là BS mới chẳng hạn LTE NodeB eNB, 3G NodeB NB, hoặc 5G NodeB tiến hóa, và có thể được viết dưới dạng (R)AN theo tiếng Anh. BS 102 có thể là thiết bị được tạo cấu hình để truyền thông với thiết bị đầu cuối. Chẳng hạn, BS 102 có thể trạm thu phát cơ sở (Base Transceiver Station, BTS) trong hệ thống GSM hoặc CDMA, có thể là nút B (NodeB, NB) trong hệ thống WCDMA, có thể là NodeB tiến hóa (Evolved NodeB, eNB hoặc eNodeB) trong hệ thống LTE, hoặc có thể là BS 5G. Theo cách khác, thiết bị mạng có thể là nút chuyển tiếp, AP, thiết bị trong xe, thiết bị đeo tay, thiết bị phía mạng trong mạng 5G tương lai, thiết bị mạng trong mạng PLMN tiến hóa tương lai, hoặc tương tự.

Thực thể SMF 103 có thể là chức năng được tách từ MME trong LTE, và có thể chịu trách nhiệm chính để thiết lập phiên người dùng, và chỉ sau khi phiên người dùng được thiết lập, dữ liệu có thể được nhận và truyền. MME trong hệ thống LTE là phần tử mạng chịu trách nhiệm cho bảo mật, quản lý di động, và quản lý phiên ở phía CN. Bảo mật nghĩa là thiết bị đầu cuối 101 cần thực hiện xác thực lẫn nhau với mạng khi thiết bị đầu cuối 101 truy nhập mạng ban đầu. Sau khi xác thực lẫn nhau, thiết bị đầu cuối 101 và CN tạo khóa. Sau khi khóa được tạo, thiết bị đầu cuối 101 và MME thực hiện thương lượng thuật toán, tức là, thương lượng khả năng bảo mật. Quản lý di động là để ghi nhận thông tin vị trí của thiết bị đầu cuối 101, và lựa chọn thiết bị phần tử mạng mặt phẳng người dùng thích hợp cho thiết bị đầu cuối 101 dựa trên thông tin vị trí của thiết bị đầu cuối 101. Quản lý phiên sẽ chịu trách nhiệm thiết lập liên kết mặt phẳng người dùng của thiết bị đầu cuối 101. Thiết bị đầu cuối 101 có thể truy nhập mạng chỉ sau khi liên kết mặt phẳng dữ liệu của người dùng được thiết lập.

Thực thể chức năng mặt phẳng người dùng (User Plane Function, UPF) 104 có thể là tổ hợp của cổng nối phục vụ (Serving Gateway, S-GW) và cổng nối mạng dữ liệu công khai (Public Data Network Gateway, P-GW) trong hệ thống LTE, là phần tử mạng chức năng mặt phẳng người dùng của thiết bị đầu cuối 101, và chịu trách nhiệm chính để kết nối với mạng ngoài.

Mạng dành riêng (Dedicated Network, DN) 105 có thể là mạng cấp dịch vụ cho thiết bị đầu cuối 101. Chẳng hạn, một số DN có thể cấp chức năng truy nhập mạng cho thiết bị đầu cuối 101, và một số DN có thể bố trí chức năng thông điệp SMS cho thiết bị đầu cuối 101. Chức năng điều khiển chính sách (Policy Control Function, PCF) 106 còn được bao gồm.

Thực thể chức năng máy chủ xác thực (Authentication Server Function, AUSF) 107 tương tác với chức năng xử lý và kho lưu trữ ủy nhiệm xác thực (Authentication Credential Repository and Processing Function, ARPF) và kết thúc yêu cầu xác thực từ SEAF. Thực thể AUSF 107 cũng là chức năng được tách từ máy chủ thuê bao tại gia (Home Subscriber Server, HSS) trong hệ thống LTE. AUSF 107 có thể là phần tử mạng độc lập. HSS trong hệ thống LTE có thể lưu trữ thông tin thuê bao của người dùng và khóa dài hạn của người dùng.

ARPF có thể được tích hợp vào thực thể quản lý dữ liệu người dùng (User Data Management, UDM) 108 như là một phần của UDM. ARPF được tách từ HSS trong LTE, và chủ yếu được sử dụng để lưu trữ khóa dài hạn. Việc xử lý liên quan đến khóa dài hạn cũng được hoàn thành ở đây.

Chức năng của thực thể chức năng quản lý di động và truy nhập (Access and Mobility Management Function, AMF) 109 là để quản lý vấn đề truy nhập của thiết bị đầu cuối 101, và còn quản lý tính di động của thiết bị đầu cuối 101. Chức năng này có thể là chức năng mô đun quản lý di động (Mobility Management, MM) trong MME trong LTE, và còn bao gồm chức anwng quản lý truy nhập. Chức năng chọn lát (Lát select Function, SSF) 110 còn được bao gồm.

Thực thể chức năng neo bảo mật (Security anchor function, SEAF) 111 chịu trách nhiệm cho các chức năng xác thực của thiết bị đầu cuối 101 và phía mạng, và lưu trữ khóa neo sau khi xác thực thành công.

Thực thể chức năng quản lý ngữ cảnh bảo mật (Security Context Management Function, SCMF) 112 thu được khóa từ SEAF 111 và còn dẫn xuất khóa khoác, và là chức năng được tách từ MME. Trong tình huống thực, SEAF 111 và SCMF 112 có thể còn được kết hợp thành một thực thể chức năng xác thực (Authentication function, AUF) riêng rẽ. Như được thể hiện trên

Fig.1, SEAF 111 và SCMF 112 được kết hợp thành AMF 109 để tạo một phần tử mạng.

Fig.1 còn thể hiện các triển khai khả thi của giao diện trong mỗi phần tử mạng, chẳng hạn, giao diện NG2 giữa BS 102 và thực thể AMF 109, và giao diện NG9 giữa BS 102 và thực thể UPF 104. Các chi tiết không được mô tả ở đây.

Fig.2 thể hiện ví dụ của lưu đồ của phương pháp truyền thông theo phương án thực hiện sáng chế.

Dựa trên nội dung nêu trên, phương án thực hiện sáng chế đề xuất phương pháp truyền thông. Như được thể hiện trên Fig.2, phương pháp bao gồm các bước sau.

Bước 201: BS thu được thuật toán bảo mật mặt phẳng báo hiệu được hỗ trợ bởi thiết bị đầu cuối. Một cách tùy chọn, có nhiều cách thu được mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối. Mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối ít nhất bao gồm ít nhất một thuật toán mật mã hóa mặt phẳng báo hiệu và ít nhất một thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu. Chẳng hạn, mặt phẳng báo hiệu thuật toán bảo mật được nhận từ AMF. Trong ví dụ khác, mặt phẳng báo hiệu thuật toán bảo mật thu được trực tiếp từ thiết bị đầu cuối bằng cách sử dụng thông điệp báo hiệu hoặc được tiền tạo cấu hình trên BS.

Theo phương án thực hiện sáng chế, giải pháp được nêu để triển khai bước 201. Cụ thể là, thiết bị đầu cuối gửi thông điệp tầng không truy nhập (Non-Access Stratum, NAS) đến BS. Thông điệp NAS là thông điệp mặt phẳng báo hiệu được trao đổi giữa thiết bị đầu cuối và CN, chẳng hạn, yêu cầu đính kèm LTE (yêu cầu đính kèm) hoặc yêu cầu đăng ký 5G. Theo phương án thực hiện, thông điệp yêu cầu đăng ký 5G được sử dụng làm ví dụ để mô tả, và xử lý tương tự có thể được thực hiện cho thông điệp NAS khác ở bước tương tự. Thiết bị đầu cuối gửi yêu cầu đăng ký đến BS. Yêu cầu đăng ký mang mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối.

Một cách tùy chọn, trong ví dụ nêu trên, yêu cầu đăng ký có thể cũng mang thuật toán bảo mật mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối.

Thuật toán bảo mật mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối có thể bao gồm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối. Hai thuật toán bất kỳ của mặt phẳng báo hiệu thuật toán mật mã hóa được hỗ trợ bởi thiết bị đầu cuối, mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn được hỗ trợ bởi thiết bị đầu cuối, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối có thể giống hoặc khác nhau. Theo giải pháp tùy chọn, thiết bị đầu cuối có thể báo cáo riêng rẽ mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn được hỗ trợ bởi thiết bị đầu cuối, mặt phẳng báo hiệu thuật toán mật mã hóa được hỗ trợ bởi thiết bị đầu cuối, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối. Theo cách khác, nếu ít nhất hai trong bốn thuật toán giống nhau, thiết bị đầu cuối có thể báo cáo một trong hai thuật toán giống nhau. Chẳng hạn, nếu mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn được hỗ trợ bởi thiết bị đầu cuối giống như thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, thiết bị đầu cuối báo cáo chỉ một thuật toán tương tự tương ứng với mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối. Nếu mặt phẳng báo hiệu thuật toán mật mã hóa được hỗ trợ bởi thiết bị đầu cuối giống như thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, thiết bị đầu cuối báo cáo chỉ một thuật toán tương tự tương ứng với mặt phẳng báo hiệu thuật toán mật mã hóa được hỗ trợ bởi thiết bị đầu cuối và thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối.

Theo triển khai tùy chọn khác, nếu mặt phẳng báo hiệu thuật toán mật mã hóa được hỗ trợ bởi thiết bị đầu cuối, mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn được hỗ trợ bởi thiết bị đầu cuối, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối đều giống nhau, thiết bị

đầu cuối có thể báo cáo chỉ một thuật toán để chỉ báo bốn thuật toán. Chẳng hạn, các thuật toán được báo cáo bởi thiết bị đầu cuối là EEA 1, EEA 2, EIA 1, và EIA 2. Sau đó, EEA 1 và EEA 2 có thể được lựa chọn làm cả mặt phẳng báo hiệu thuật toán mật mã hóa lẫn thuật toán mật mã hóa mặt phẳng người dùng. Một cách tương tự, EIA 1 và EIA 2 có thể được lựa chọn làm cả mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng.

Trong ví dụ khác, các thuật toán được báo cáo bởi thiết bị đầu cuối là EEA 11, EEA 12, EIA 11, EIA 12, EEA 21, EEA 23, EIA 21, và EIA 22. Sau đó, EEA 11 và EEA 12 có thể được lựa chọn làm mặt phẳng báo hiệu thuật toán mật mã hóa. EEA 21 và EEA 23 có thể được lựa chọn làm thuật toán mật mã hóa mặt phẳng người dùng. EIA 11 và EIA 12 có thể được lựa chọn làm mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn. EIA 21 và EIA 22 có thể được lựa chọn làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Trong ví dụ khác, các thuật toán được báo cáo bởi thiết bị đầu cuối là EEA 11, EEA 12, EIA 1, EIA 2, EEA 21, EEA 23, EIA 21, và EIA 22. Sau đó, EEA 11 và EEA 12 có thể được lựa chọn làm mặt phẳng báo hiệu thuật toán mật mã hóa. EEA 21 và EEA 23 có thể được lựa chọn làm thuật toán mật mã hóa mặt phẳng người dùng. EIA 1 và EIA 2 có thể được lựa chọn làm cả mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn lẫn thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Trong ví dụ khác, các thuật toán được báo cáo bởi thiết bị đầu cuối là EEA 1, EEA 2, EIA 11, EIA 12, EIA 21, và EIA 22. Sau đó, EEA 1 và EEA 2 có thể được lựa chọn làm mặt phẳng báo hiệu thuật toán mật mã hóa và thuật toán mật mã hóa mặt phẳng người dùng. EIA 11 và EIA 12 có thể được lựa chọn làm mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn. EIA 21 và EIA 22 có thể được lựa chọn làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng.

Theo khía cạnh khác, theo giải pháp triển khai tùy chọn, thiết bị đầu cuối có thể báo cáo, bằng cách sử dụng các đoạn báo hiệu, mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán mật mã

hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, trong đó một đoạn báo hiệu bao gồm một thuật toán. Theo giải pháp tùy chọn khác, mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối được báo cáo bằng cách sử dụng một hoặc nhiều đoạn báo hiệu, trong đó một đoạn báo hiệu bao gồm một hoặc nhiều thuật toán. Khi một đoạn báo hiệu bao gồm các thuật toán, một số trường có thể được định trước trong báo hiệu, và các trường này được sử dụng để mang các thuật toán tương ứng. Chẳng hạn, trường thứ nhất, trường thứ hai, và trường thứ ba được thiết lập liên tục. Trường thứ nhất được định trước để đặt mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối. Trường thứ hai được định trước để đặt thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối. Trường thứ ba được định trước để đặt thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối. Theo cách khác, khi ba thuật toán là giống nhau, chỉ một thuật toán được báo cáo trong một đoạn báo hiệu, và phần tử mạng khác xem xét mặt định rằng thuật toán này là mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối. Chẳng hạn, các khả năng bảo mật được báo cáo bởi thiết bị đầu cuối là EEA 1, EEA 2, EIA 1, và EIA 2. Sau đó, EEA 1 và EEA 2 có thể được lựa chọn làm cả mặt phẳng báo hiệu thuật toán mật mã hóa lẫn thuật toán mật mã hóa mặt phẳng người dùng. Một cách tương tự, EIA 1 và EIA 2 có thể được lựa chọn làm cả mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn lẫn thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Trong ví dụ khác, các khả năng bảo mật được báo cáo bởi UE là EEA 11, EEA 12, EIA 11, EIA 12, EEA 21, EEA 23, EIA 21, và EIA 22. Sau đó, EEA 11 và EEA 12 có thể được lựa chọn làm mặt phẳng báo hiệu thuật toán mật mã hóa. EEA 21 và EEA 23 có thể được lựa chọn làm thuật toán mật mã hóa mặt phẳng người dùng. EIA 11 và EIA 12 có thể được lựa chọn làm mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn. EIA 21 và EIA 22 có thể

được lựa chọn làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Trong ví dụ khác, các khả năng bảo mật được báo cáo bởi UE là EEA 11, EEA 12, EIA 1, EIA 2, EEA 21, EEA 23, EIA 21, và EIA 22. Sau đó, EEA 11 và EEA 12 có thể được lựa chọn làm mặt phẳng báo hiệu thuật toán mật mã hóa. EEA 21 và EEA 23 có thể được lựa chọn làm thuật toán mật mã hóa mặt phẳng người dùng. EIA 1 và EIA 2 có thể được lựa chọn làm cả mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng.

Một cách tùy chọn, BS chuyển tiếp yêu cầu đăng ký đến AMF. Một cách tùy chọn, AMF gửi thông điệp chấp nhận đăng ký thứ nhất (Registration Accept) đến BS sau khi AMF thực hiện xác thực lẫn nhau với BS và thực hiện thủ tục đăng ký khác với phần tử CN khác, chẳng hạn SEAF, AUSF, SMF, PCF, hoặc UDM. BS chuyển tiếp thông điệp chấp nhận đăng ký thứ nhất nhận được đến thiết bị đầu cuối. Việc chuyển tiếp nghĩa là thông điệp không bị thay đổi. Tuy nhiên, tham số bổ sung được thêm vào vào thông điệp do các giao diện mang thông điệp có các chức năng khác nhau, để triển khai chức năng truyền thông điệp. Chẳng hạn, thông điệp chấp nhận đăng ký thứ nhất được gửi đến BS qua giao diện N2. Bên cạnh thông điệp chấp nhận đăng ký thứ nhất, giao diện N2 có thông tin mà BS cần biết. BS chuyển tiếp thông điệp chấp nhận đăng ký thứ nhất đến UE bằng cách sử dụng thông điệp RRC. Bên cạnh thông điệp đăng ký thứ nhất, thông điệp RRC có thể bao gồm ít nhất thông tin khác mà UE cần biết, hoặc thông tin mà có thể được sử dụng để tìm thấy UE. Theo cách khác, thông điệp chấp nhận đăng ký thứ nhất được biến đổi ở mức độ nào đó, chẳng hạn, việc chuyển đổi định dạng được thực hiện dựa trên các giao diện khác nhau, và thông điệp chấp nhận đăng ký thứ nhất được chuyển đổi được chuyển tiếp đến thiết bị đầu cuối. Ở bước này, nếu giao diện giữa AMF và BS là NG2, thông điệp chấp nhận đăng ký thứ nhất được mang bằng cách sử dụng thông điệp NG2. Thông điệp chấp nhận đăng ký thứ nhất còn mang khóa cơ sở (Kan) được tạo bởi AMF hoặc SEAF cho BS, và mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ và được báo cáo bởi thiết bị đầu cuối. Một cách tùy chọn, thông điệp yêu cầu đăng ký có thể được đặt trong phần

chứa NAS, và khóa cơ sở (Kan) và khả năng bảo mật của thiết bị đầu cuối có thể được đặt trong phần chứa NAS hoặc có thể được đặt ngoài phần chứa NAS.

Bước 202: BS xác định thuật toán bảo mật mặt phẳng báo hiệu đích dựa trên mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo mật mặt phẳng báo hiệu được phép bởi BS.

Ở bước 202, một cách tùy chọn, BS có thể tiền cấu hình mặt phẳng báo hiệu thuật toán bảo mật được phép bởi BS. Một cách tùy chọn, thuật toán được bao gồm trong mặt phẳng báo hiệu thuật toán bảo mật được phép bởi BS được sắp xếp dựa trên độ ưu tiên, chẳng hạn, được sắp xếp dựa trên độ ưu tiên nhà khai thác hoặc dựa trên cấu hình môi trường thực cục bộ. Một cách tùy chọn, mặt phẳng báo hiệu thuật toán bảo mật được phép bởi BS có thể được tạo cấu hình cho BS bằng cách sử dụng thiết bị quản lý mạng, hoặc có thể được tạo cấu hình trong quá trình cài đặt môi trường phần mềm trong khi thiết lập BS, hoặc có thể được tạo cấu hình theo cách thức khác.

Ở bước 202, triển khai khả thi như sau: BS lựa chọn, dựa trên mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và mặt phẳng báo hiệu thuật toán bảo mật được phép bởi BS và được sắp xếp dựa trên độ ưu tiên, thuật toán bảo mật mặt phẳng báo hiệu mà được hỗ trợ bởi thiết bị đầu cuối và có độ ưu tiên cao nhất, như là thuật toán bảo mật mặt phẳng báo hiệu đích. Thuật toán bảo mật mặt phẳng báo hiệu đích có thể bao gồm một thuật toán mật mã hóa và/hoặc một thuật toán bảo vệ tính toàn vẹn.

Một triển khai cụ thể khả thi như sau: BS lựa chọn tập tất cả các thuật toán tồn tại trong mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và cũng tồn tại trong mặt phẳng báo hiệu thuật toán bảo mật được phép bởi BS, và lựa chọn thuật toán có độ ưu tiên tương đối cao trong mặt phẳng báo hiệu thuật toán bảo mật được phép bởi BS từ tập các thuật toán, như là thuật toán bảo mật mặt phẳng báo hiệu đích.

Nên lưu ý ở đây rằng mặt phẳng báo hiệu thuật toán bảo mật được phép bởi BS và thuật toán bảo mật mặt phẳng người dùng được phép bởi BS có thể được tạo cấu hình hoặc được tiền tạo cấu hình cho BS dựa trên ít nhất độ ưu tiên nhà khai thác. Mặt phẳng báo hiệu thuật toán bảo mật được phép bởi BS bao gồm ít

nhất một thuật toán mật mã hóa mặt phẳng báo hiệu được phép bởi BS và/hoặc ít nhất một thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu được phép bởi BS. Thuật toán bảo mật mặt phẳng người dùng được phép bởi BS bao gồm ít nhất một thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS và/hoặc ít nhất một thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS. Ngoài ra, ít nhất một thuật toán mật mã hóa mặt phẳng báo hiệu được phép bởi BS và/hoặc ít nhất một thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu được phép bởi BS trong mặt phẳng báo hiệu thuật toán bảo mật được phép bởi BS được sắp xếp dựa trên độ ưu tiên, và việc sắp xếp độ ưu tiên có thể được xác định bởi nhà khai thác. Thuật toán bảo mật mặt phẳng người dùng được phép bởi BS có thể hoặc không thể được sắp xếp dựa trên độ ưu tiên. Khi thuật toán bảo mật mặt phẳng người dùng được phép bởi BS giống như mặt phẳng báo hiệu thuật toán bảo mật được phép bởi BS, và độ ưu tiên của thuật toán bảo mật mặt phẳng người dùng được phép bởi BS giống như độ ưu tiên của mặt phẳng báo hiệu thuật toán bảo mật được phép bởi BS, BS có thể lưu trữ chỉ một tập các thuật toán được sắp xếp dựa trên độ ưu tiên, tức là, lưu trữ thuật toán bảo mật mặt phẳng người dùng được phép bởi BS và được sắp xếp dựa trên độ ưu tiên, hoặc thuật toán bảo mật mặt phẳng báo hiệu được phép bởi BS và được sắp xếp dựa trên độ ưu tiên.

Một cách tùy chọn, BS tạo chỉ khóa liên quan mặt phẳng báo hiệu dựa trên thuật toán bảo mật mặt phẳng báo hiệu đích, chẳng hạn, khóa bảo vệ tính toàn vẹn mặt phẳng báo hiệu và khóa mật mã hóa mặt phẳng báo hiệu. Khóa liên quan mặt phẳng báo hiệu là, chẳng hạn, khóa liên quan RRC, và cụ thể là khóa bảo vệ tính toàn vẹn RRC (Krrc-int) và khóa mật mã hóa RRC (Krrc-enc). BS có thể tạo khóa dựa trên khóa cơ sở (Kan). Kan thu được bởi BS từ phần tử CN, chẳng hạn AMF hoặc AUSF.

Bước 203: BS thêm thuật toán bảo mật mặt phẳng báo hiệu đích vào SMC AS, và gửi SMC AS đến thiết bị đầu cuối.

Một cách tùy chọn, ở bước 203, BS có thể gửi SMC AS đến thiết bị đầu cuối theo các cách triển khai. SMC AS bao gồm thông tin chỉ báo của thuật toán bảo mật mặt phẳng báo hiệu đích, chẳng hạn, ID của thuật toán bảo mật

mặt phẳng báo hiệu đích.

Ngoài ra, BS có thể còn thêm mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối vào SMC AS. Một cách tùy chọn, bảo vệ tính toàn vẹn có thể được thực hiện trên SMC AS bằng cách sử dụng mặt phẳng báo hiệu khóa bảo vệ tính toàn vẹn được tạo bởi BS.

Một cách tùy chọn, sau khi nhận SMC AS, thiết bị đầu cuối xác định thuật toán bảo mật mặt phẳng báo hiệu đích dựa trên thông tin chỉ báo của thuật toán bảo mật mặt phẳng báo hiệu đích, và tạo khóa liên quan mặt phẳng báo hiệu (phương pháp tạo khóa liên quan mặt phẳng báo hiệu bởi thiết bị đầu cuối giống như phương pháp tạo khóa liên quan mặt phẳng báo hiệu bởi BS), và kiểm tra bảo vệ tính toàn vẹn trên SMC AS dựa trên khóa bảo vệ tính toàn vẹn mặt phẳng báo hiệu. Nếu xác định được rằng bảo vệ tính toàn vẹn trên SMC AS đạt tiêu chuẩn, được xác định rằng mặt phẳng báo hiệu khóa bảo vệ tính toàn vẹn ở phía thiết bị đầu cuối giống như mặt phẳng báo hiệu khóa bảo vệ tính toàn vẹn được sử dụng bởi BS cho SMC AS. Một cách tùy chọn, sau bước 203, phương pháp còn bao gồm bước 204: Thiết bị đầu cuối gửi SMP AS đến BS.

Một cách tùy chọn, thiết bị đầu cuối có thể thực hiện mã hóa và/hoặc bảo vệ tính toàn vẹn trên AS SMP bằng cách sử dụng khóa liên quan mặt phẳng báo hiệu được tạo. Một cách tùy chọn, sau khi BS kiểm tra việc bảo vệ mật mã hóa và bảo vệ tính toàn vẹn trên thông điệp AS SMP là đúng, BS chuyển tiếp thông tin chấp nhận đăng ký thứ nhất nhận được đến thiết bị đầu cuối, hoặc biến đổi thông điệp chấp nhận đăng ký thứ nhất ở mức độ nào đó, chẳng hạn, thực hiện biến đổi định dạng trên thông điệp chấp nhận đăng ký thứ nhất dựa trên các giao diện khác nhau để thu được thông điệp chấp nhận đăng ký thứ hai, và gửi thông tin chấp nhận đăng ký thứ hai đến thiết bị đầu cuối. Sau đó, một cách tùy chọn, thiết bị đầu cuối trả về hoàn thành đăng ký cho AMF.

Dựa trên ví dụ nêu trên, có thể biết rằng theo phương án thực hiện sáng chế, chỉ mục đích thương lượng thuật toán bảo mật mặt phẳng báo hiệu đích bởi BS và thiết bị đầu cuối được triển khai bằng cách sử dụng thủ tục SMC AS, và mặt phẳng báo hiệu thuật toán bảo mật và thuật toán bảo mật mặt phẳng người dùng

được tách rời. Mặt phẳng báo hiệu thuật toán bảo mật và thuật toán bảo mật mặt phẳng người dùng có thể được xác định riêng rẽ, nhờ đó cải thiện độ linh hoạt truyền thông.

Ngoài ra, trong ví dụ nêu trên, giải pháp tùy chọn như sau: Thiết bị đầu cuối báo cáo, bằng cách gửi yêu cầu đăng ký, mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối. Một cách tùy chọn, thiết bị đầu cuối cũng có thể thêm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối vào yêu cầu đăng ký để báo cáo. Đối với giải pháp báo cáo tùy chọn cụ thể, tham khảo phương án thực hiện nêu trên, và các chi tiết không được mô tả lại ở đây.

Một cách tùy chọn, mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối cũng có thể được phân loại thành thuật toán bảo mật mặt phẳng báo hiệu được hỗ trợ bởi thiết bị đầu cuối trên NAS và thuật toán bảo mật mặt phẳng báo hiệu được hỗ trợ bởi thiết bị đầu cuối trên AS. Mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối trên AS cũng có thể được gọi là thuật toán bảo mật mặt phẳng báo hiệu được hỗ trợ bởi thiết bị đầu cuối ở lớp RRC. Khi báo cáo mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, thiết bị đầu cuối có thể thêm thông tin chỉ báo vào mỗi thuật toán bảo mật. Theo cách khác, một số trường có thể được định trước, và cách thức đặt thuật toán tương ứng trong trường tương ứng được sử dụng để nhận diện liệu mỗi thuật toán bảo mật có thuộc mặt phẳng báo hiệu hoặc mặt phẳng người dùng hoặc thuộc NAS hoặc AS. Chẳng hạn, trường được định trước để đặt mặt phẳng báo hiệu thuật toán bảo mật, và trường khác được định trước để đặt thuật toán bảo mật mặt phẳng người dùng. Trong ví dụ khác, trường được định trước để đặt thuật toán bảo mật trên NAS, và trường khác được định trước để đặt thuật toán bảo mật trên AS. Theo cách khác, thiết bị đầu cuối báo cáo tất cả các thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối cho AMF, và AMF thay cho thiết bị đầu cuối phân biệt liệu các

thuật toán bảo mật có thuộc mặt phẳng báo hiệu hoặc mặt phẳng người dùng. Theo cách khác, AMF chuyển tiếp thuật toán bảo mật đến BS, và BS thực hiện phân biệt.

Một cách tương ứng, khi AMF gửi thông điệp chấp nhận đăng ký thứ nhất đến BS, tất cả các thuật toán bảo mật được báo cáo bởi thiết bị đầu cuối có thể được gửi đến BS, chẳng hạn mặt phẳng báo hiệu thuật toán bảo mật, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối. Theo cách khác, chỉ mặt phẳng báo hiệu thuật toán bảo mật mà được hỗ trợ bởi thiết bị đầu cuối và được yêu cầu bởi BS để thương lượng thuật toán bảo mật mặt phẳng báo hiệu đích được gửi đến BS. Theo cách khác, chỉ mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối ở lớp RRC được truyền.

Để tương thích với giải pháp kỹ thuật đã biết, Một cách tùy chọn, BS có thể thêm, vào thông điệp SMC AS, thông tin chỉ báo để chỉ thương lượng thuật toán bảo mật mặt phẳng báo hiệu đích. Sau khi thiết bị đầu cuối phân tích cú pháp thông điệp SMC AS và tháy rằng có thông tin chỉ báo để chỉ thương lượng thuật toán bảo mật mặt phẳng báo hiệu đích, thiết bị đầu cuối tạo khóa liên quan mặt phẳng báo hiệu chỉ dựa trên thuật toán bảo mật mặt phẳng báo hiệu đích được xác định. Theo cách này, chỉ một tập các thuật toán bảo mật mặt phẳng báo hiệu đích được thương lượng giữa thiết bị đầu cuối và BS. Nếu thiết bị đầu cuối thấy rằng thông tin chỉ báo để chỉ thương lượng thuật toán bảo mật mặt phẳng báo hiệu đích không tồn tại sau khi phân tích cú pháp thông tin SMC AS, thiết bị đầu cuối xác định thuật toán bảo mật mặt phẳng báo hiệu đích được xác định như là thuật toán bảo mật đích, và thuật toán bảo mật đích được sử dụng để tạo khóa liên quan mặt phẳng báo hiệu và khóa liên quan mặt phẳng người dùng. Khóa liên quan mặt phẳng người dùng bao gồm khóa mật mã hóa mặt phẳng người dùng và khóa bảo vệ tính toàn vẹn mặt phẳng người dùng. Khóa liên quan mặt phẳng báo hiệu bao gồm khóa mật mã hóa mặt phẳng báo hiệu và khóa bảo vệ tính toàn vẹn mặt phẳng báo hiệu. Theo cách này, một tập của các thuật toán bảo mật mặt phẳng báo hiệu đích và một tập

của các thuật toán bảo mật đích mặt phẳng người dùng được thương lượng giữa thiết bị đầu cuối và BS.

Một cách tùy chọn, để tương thích được với giải pháp kỹ thuật đã biết, BS có thể thêm, vào thông tin SMC AS, thông tin chỉ báo được sử dụng để chỉ báo để thương thượng thuật toán bảo mật mặt phẳng báo hiệu đích và/hoặc thông tin chỉ báo được sử dụng để chỉ báo để thương thượng khóa liên quan mặt phẳng người dùng. Chẳng hạn, một bit được thêm vào, và bit có thể được thêm mới hoặc thu được bằng cách tận dụng lại bit hiện tại. Chẳng hạn, nếu bit này là 0, chỉ báo rằng chỉ thuật toán bảo mật mặt phẳng báo hiệu đích sẽ được thương lượng; hoặc nếu bit này bằng 1, chỉ báo rằng cả thuật toán bảo mật mặt phẳng báo hiệu đích lẫn khóa liên quan mặt phẳng người dùng sẽ được thương lượng.

Theo phương án thực hiện sáng chế, thuật toán bảo mật mặt phẳng báo hiệu đích bao gồm thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích và thuật toán mật mã hóa mặt phẳng báo hiệu đích. Một cách tùy chọn, hai thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích khác nhau và thuật toán mật mã hóa mặt phẳng báo hiệu đích có thể được thương lượng bằng cách sử dụng thủ tục SMC AS, hoặc một thuật toán bảo mật mặt phẳng báo hiệu đích được thương lượng và được sử dụng làm cả thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích lẫn thuật toán mật mã hóa mặt phẳng báo hiệu đích.

Theo giải pháp triển khai tùy chọn khác, ít nhất một của thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích và thuật toán mật mã hóa mặt phẳng báo hiệu đích có thể được thương lượng bằng cách sử dụng thủ tục SMC AS, và thuật toán bảo mật mặt phẳng báo hiệu đích còn lại có thể được thương lượng bằng cách sử dụng thủ tục khác.

Một cách tùy chọn, thuật toán bảo mật mặt phẳng báo hiệu đích được thương lượng bởi BS và thiết bị đầu cuối có thể được chỉ báo bằng cách sử dụng ID của thuật toán. Theo giải pháp triển khai tùy chọn, bất kể liệu thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích giống như hoặc khác với thuật toán mật mã hóa mặt phẳng báo hiệu đích, thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích và thuật toán mật mã hóa mặt phẳng báo hiệu đích

được chỉ báo bằng cách sử dụng các ID của hai thuật toán. Theo giải pháp triển khai tùy chọn khác, nếu thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích giống như thuật toán mật mã hóa mặt phẳng báo hiệu đích, ID của một thuật toán có thể được sử dụng để chỉ báo thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích và thuật toán mật mã hóa mặt phẳng báo hiệu đích; và nếu thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích khác với thuật toán mật mã hóa mặt phẳng báo hiệu đích, các ID của hai thuật toán được sử dụng để chỉ báo thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích và thuật toán mật mã hóa mặt phẳng báo hiệu đích.

Theo giải pháp tùy chọn khác, phương án thực hiện sáng chế bao gồm thuật toán bảo mật mặt phẳng báo hiệu đích và thuật toán bảo mật đích mặt phẳng người dùng. Theo giải pháp triển khai tùy chọn, bất kể liệu thuật toán bảo mật mặt phẳng báo hiệu đích giống như hoặc khác với thuật toán bảo mật đích mặt phẳng người dùng, thuật toán bảo mật mặt phẳng báo hiệu đích and thuật toán bảo mật đích mặt phẳng người dùng được chỉ báo bằng cách sử dụng các ID của hai tập thuật toán. Theo giải pháp triển khai tùy chọn khác, nếu thuật toán bảo mật mặt phẳng báo hiệu đích giống như thuật toán bảo mật đích mặt phẳng người dùng, các ID của một tập thuật toán có thể được sử dụng để chỉ báo thuật toán bảo mật mặt phẳng báo hiệu đích và thuật toán bảo mật đích mặt phẳng người dùng; và nếu thuật toán bảo mật mặt phẳng báo hiệu đích khác với thuật toán bảo mật đích mặt phẳng người dùng, các ID của hai tập các thuật toán được sử dụng để chỉ báo thuật toán bảo mật mặt phẳng báo hiệu đích và thuật toán bảo mật đích mặt phẳng người dùng. Các ID của một tập của các thuật toán tương ứng với thuật toán bảo mật mặt phẳng báo hiệu đích bao gồm ID của ít nhất một thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích và ID của ít nhất một thuật toán mật mã hóa mặt phẳng báo hiệu đích. Theo ví dụ nêu trên, trong các ID của một tập của các thuật toán tương ứng với thuật toán bảo mật mặt phẳng báo hiệu đích, ID của một thuật toán hoặc các ID của hai thuật toán có thể được sử dụng để biểu diễn thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích và thuật toán mật mã hóa mặt phẳng báo hiệu đích. Một cách tương ứng, các ID của một tập của các thuật toán tương ứng với thuật toán

bảo mật đích mặt phẳng người dùng bao gồm ID của ít nhất một thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích và ID của ít nhất một thuật toán mật mã hóa mặt phẳng người dùng đích. Theo ví dụ nêu trên, trong các ID của một tập của các thuật toán tương ứng với thuật toán bảo mật đích mặt phẳng người dùng, ID của một thuật toán hoặc các ID của hai thuật toán có thể được sử dụng để biểu diễn thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích và thuật toán mật mã hóa mặt phẳng người dùng đích.

Fig.2a thể hiện ví dụ của lưu đồ phương pháp truyền thông khác theo phương án thực hiện sáng chế.

Dựa trên mô tả nêu trên, phương án thực hiện sáng chế đề xuất phương pháp truyền thông khác. Như được thể hiện trên Fig.2a, phương pháp bao gồm các bước sau.

Một cách tùy chọn, bước 211: thực thể SMF nhận thông điệp yêu cầu, trong đó thông điệp yêu cầu có thể bao gồm ID của thiết bị đầu cuối. Một cách tùy chọn, thông điệp yêu cầu được nhận bởi thực thể SMF có thể bao gồm các loại, chẳng hạn yêu cầu đăng ký, yêu cầu dịch vụ, hoặc yêu cầu thiết lập phiên. Yêu cầu thiết lập phiên cũng có thể được gọi là yêu cầu thiết lập phiên PDU.

Một cách tùy chọn, nếu thông điệp yêu cầu là yêu cầu dịch vụ, yêu cầu dịch vụ có thể trước hết được gửi bởi thiết bị đầu cuối đến BS, BS chuyển tiếp yêu cầu dịch vụ đến AMF, và sau đó AMF trực tiếp chuyển tiếp yêu cầu dịch vụ. Chuyển tiếp nghĩa là gửi thông điệp đến AMF mà không thay đổi nội dung của thông điệp ban đầu. Khi thông điệp được gửi đến AMF, tham số khác có thể được thêm dựa trên hệ số chẳng hạn giao diện, hoặc thông điệp được biến đổi dựa trên thông tin giao diện và sau đó được gửi đến SMF. Nếu giao diện giữa BS và AMF là giao diện N2, và giao diện giữa AMF và SMF là N11, yêu cầu dịch vụ được chuyển tiếp bởi BS đến AMF là yêu cầu mà so khớp the giao diện N2, và yêu cầu dịch vụ được chuyển tiếp bởi AMF đến SMF là yêu cầu mà so khớp giao diện N11. Yêu cầu dịch vụ là yêu cầu NAS. Một cách tùy chọn, thông điệp yêu cầu có thể theo cách khác là yêu cầu đăng ký.

Một cách tùy chọn, nếu thông điệp yêu cầu là yêu cầu thiết lập phiên, yêu cầu thiết lập phiên có thể trước hết được gửi bởi thiết bị đầu cuối đến AMF, và

sau đó AMF trực tiếp chuyển tiếp yêu cầu thiết lập phiên. Chuyển tiếp nghĩa là gửi thông điệp đến AMF mà không thay đổi nội dung của thông điệp ban đầu. Khi thông điệp được gửi đến AMF, tham số khác có thể được thêm dựa trên hệ số chẳng hạn giao diện, hoặc thông điệp được biến đổi dựa trên thông tin giao diện và sau đó được gửi đến SMF.

Một cách tùy chọn, trước khi thiết bị đầu cuối gửi yêu cầu thiết lập phiên, thiết bị đầu cuối có thể ở trạng thái ngắt kết nối phiên. Một cách tùy chọn, thiết bị đầu cuối và BS có thể thực hiện lại thủ tục đăng ký ở bước nêu trên, tức là, thiết bị đầu cuối có thể gửi yêu cầu đăng ký đến BS, để thực hiện đăng ký thiết bị đầu cuối, và thương lượng lại thuật toán bảo mật mặt phẳng báo hiệu đích giữa thiết bị đầu cuối và BS trong SMC AS và AS SMP trong thủ tục đăng ký.

Ở bước nêu trên, ID của thiết bị đầu cuối có thể bao gồm một hoặc nhiều trong số IMSI, IMEI, hoặc danh tính tạm thời.

Bước 212: Thực thể SMF thu được chính sách bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật.

Bước 213: Thực thể SMF gửi chính sách bảo mật hoặc ID của chính sách bảo mật đến BS, trong đó chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối.

Một cách tùy chọn, SMF hoặc phần tử mạng khác được kết nối với SMF lưu trữ phép tương ứng giữa chính sách bảo mật và ID của chính sách bảo mật. Trong trường hợp này, chính sách bảo mật hoàn toàn được tiền tạo cấu hình trên SMF, BS, UE, hoặc phần tử mạng khác được kết nối với SMF. Chẳng hạn, chính sách bảo mật được tạo cấu hình dựa trên dịch vụ cụ thể, chẳng hạn chính sách bảo mật của dịch vụ thoại VoIP. Chẳng hạn, chính sách bảo mật được tạo cấu hình dựa trên nhà cung cấp dịch vụ, chẳng hạn nhà máy nước. Có nhiều cơ sở cấu hình, không được liệt kê lần lượt ở đây. Sau khi SMF xác định chính sách bảo mật cho thiết bị đầu cuối bằng cách sử dụng ID hoặc tham số khác của thiết bị đầu cuối, ID của chính sách bảo mật tương ứng với chính sách bảo mật có thể thu được. SMF truyền ID của chính sách bảo mật đến BS, và BS có thể thực hiện bảo vệ bảo mật mặt phẳng người dùng dựa trên chính sách bảo

mật tương ứng với ID của chính sách bảo mật. Chẳng hạn, phép tương ứng giữa chính sách bảo mật và ID của chính sách bảo mật được tiền tạo cấu hình trên SMF, và SMF xác định ID của chính sách bảo mật dựa trên nội dung trong thông điệp yêu cầu dịch vụ, chẳng hạn, ID của thiết bị đầu cuối. Trong ví dụ khác, nếu phép tương ứng giữa chính sách bảo mật và ID của chính sách bảo mật được tiền tạo cấu hình trên PCF, SMF cần thu được ID của chính sách bảo mật từ PDC. Trong ví dụ khác, cả SMF lẫn PCF có ID được tiền cấu hình của chính sách bảo mật, và ID của chính sách bảo mật được tiền tạo cấu hình trên PCF có thể bao gồm ID của chính sách bảo mật được tạo cấu hình trên SMF, tức là, SMF truyền ID của chính sách bảo mật thu được từ PCF đến BS.

Theo triển khai tùy chọn, thực thể SMF gửi ngay chính sách bảo mật or ID của chính sách bảo mật đến BS. Chẳng hạn, thực thể SMF gửi chính sách bảo mật tương ứng với ID của thiết bị đầu cuối đến BS dựa trên ID của thiết bị đầu cuối và mối quan hệ định trước giữa thiết bị đầu cuối và ID của chính sách bảo mật. Chính sách bảo mật định trước có thể được định trước trên SMF, hoặc có thể được định trước trên PCF hoặc phần tử mạng khác. Chính sách bảo mật định trước và ID của chính sách bảo mật có thể được định trước trên SMF, hoặc có thể được định trước trên PCF hoặc phần tử mạng khác. Theo triển khai tùy chọn khác, sau khi thực thể SMF nhận thông điệp yêu cầu, và trước khi thực thể SMF gửi chính sách bảo mật hoặc ID của chính sách bảo mật đến BS dựa trên thông điệp yêu cầu, phương pháp còn bao gồm việc thực thể SMF thu được chính sách bảo mật dựa trên thông điệp yêu cầu. Theo triển khai tùy chọn khác, sau khi thực thể SMF nhận thông điệp yêu cầu, và trước khi thực thể SMF gửi chính sách bảo mật hoặc ID của chính sách bảo mật đến BS dựa trên thông điệp yêu cầu, phương pháp còn bao gồm việc SMF thu được ID của chính sách bảo mật dựa trên chính sách bảo mật.

Theo khía cạnh khác, một cách tùy chọn, chính sách bảo mật được nhận diện bởi ID của chính sách bảo mật hoặc chính sách bảo mật được gửi bởi thực thể SMF đến BS có thể là chính sách bảo mật được tạo trước đó, hoặc có thể là chính sách bảo mật mới được tạo.

Ở bước 213, thực thể SMF gửi chính sách bảo mật hoặc ID của chính sách

bảo mật đến BS ở nhiều dạng. Chẳng hạn, thực thể SMF có thể tạo chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật. Chẳng hạn, chính sách bảo mật có thể được tạo dựa trên ID của thiết bị đầu cuối hoặc ID phiên, hoặc một số quy tắc tạo có thể được định trước, hoặc tất cả các chính sách bảo mật có thể được tiền cấu hình.

Một cách tùy chọn, BS có thể gửi, dựa trên một số thông tin được mang trong thông điệp yêu cầu, chính sách bảo mật hoặc ID của chính sách bảo mật that áp dụng được cho thiết bị đầu cuối hoặc thông điệp yêu cầu hiện tại của thiết bị đầu cuối. Một cách tùy chọn, tham số liên quan đến chính sách bảo mật bao gồm ít nhất một trong ID của thiết bị đầu cuối, DNN của thiết bị đầu cuối, ID của lát của thiết bị đầu cuối, QoS của thiết bị đầu cuối, và ID phiên của thiết bị đầu cuối. Một cách tùy chọn, tham số liên quan đến chính sách bảo mật bao gồm ít nhất một trong ID của thiết bị đầu cuối, DNN của thiết bị đầu cuối, ID của lát của thiết bị đầu cuối, QoS của thiết bị đầu cuối, ID phiên của thiết bị đầu cuối, và ID luồng của thiết bị đầu cuối.

Mối quan hệ liên kết theo phương án thực hiện sáng chế có thể bao gồm phép tương ứng, hoặc có thể bao gồm một số quy tắc, hoặc có thể bao gồm mối quan hệ giữa một số tương quan. Chẳng hạn, phép tương ứng giữa tham số liên quan và chính sách bảo mật có thể được định trước, và sau đó chính sách bảo mật tương ứng với tham số liên quan được tìm thấy. Chẳng hạn, chính sách bảo mật tương ứng với ID của lát được xác định dựa trên ID của lát. Trong ví dụ khác, chính sách bảo mật tương ứng với ID phiên được xác định dựa trên ID phiên. Trong ví dụ khác, chính sách bảo mật tương ứng với ID phiên và ID của lát được xác định dựa trên mối quan hệ liên kết trong số ID phiên, ID của lát, và chính sách bảo mật.

Theo triển khai tùy chọn khác, tham số liên quan đến chính sách bảo mật bao gồm ID của thiết bị đầu cuối, và thực thể SMF thu được chính sách bảo mật dựa trên ID của thiết bị đầu cuối và mối quan hệ liên kết giữa ID của thiết bị đầu cuối và chính sách bảo mật. Chẳng hạn, phép tương ứng giữa thiết bị đầu cuối và chính sách bảo mật có thể được lưu trữ trên SMF hoặc phần tử mạng khác được kết nối với SMF. Chẳng hạn, có phép tương ứng giữa thiết bị

đầu cuối và chính sách bảo mật. Chẳng hạn, trong dữ liệu thuê bao người dùng, có phép tương ứng giữa IMSI và chính sách bảo mật. Do vậy, các chính sách bảo mật khác nhau có thể được thiết lập cho các thiết bị đầu cuối khác nhau dựa trên một số yêu cầu hiệu năng dịch vụ của các thiết bị đầu cuối và tương tự.

Trong ví dụ khác, mối quan hệ liên kết giữa ID của thiết bị đầu cuối và chính sách bảo mật có thể được định trước. Chẳng hạn, ID của thiết bị đầu cuối được liên kết với các chính sách bảo mật, và sau đó một chính sách bảo mật có thể được lựa chọn từ các chính sách bảo mật được liên kết với ID của thiết bị đầu cuối, hoặc chính sách bảo mật có thể còn được xác định dựa trên tham số khác, trong tham số liên quan, khác với ID của thiết bị đầu cuối. Chẳng hạn, một chính sách bảo mật được liên kết với ID phiên được lựa chọn từ các chính sách bảo mật được liên kết với ID của thiết bị đầu cuối cùng với ID phiên. Trong ví dụ khác, ID luồng của QoS được xác định dựa trên QoS, và sau đó chính sách bảo mật của QoS tương ứng được xác định dựa trên ID luồng của QoS.

Chẳng hạn, thiết bị đầu cuối của Internet vạn vật (Internet of Things, IoT) chỉ chịu trách nhiệm để đọc và gửi dữ liệu đồng hồ đo nước, tức là, gửi dữ liệu của đồng hồ đo nước đến nhà máy nước hàng tháng vào một ngày cố định. Do vậy, chính sách bảo mật của thiết bị đầu cuối được cố định, ID của thiết bị đầu cuối có thể được thiết lập để tương ứng với một chính sách bảo mật, và một cách tùy chọn, chính sách bảo mật có thể thu được từ dữ liệu thuê bao người dùng được lưu trữ trên UDM.

Để mô tả rõ ràng hơn phương án thực hiện sáng chế, phần sau còn mô tả chi tiết vài ví dụ gửi chính sách bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan. Để hiểu chi tiết, tham khảo cách triển khai a1, cách triển khai a2, cách triển khai a3, và cách triển khai a4 sau.

Cách triển khai a1

ID của lát của thiết bị đầu cuối là thông tin về lát được truy nhập bởi thiết bị đầu cuối trong kịch bản ứng dụng 5G, và được sử dụng để chỉ báo lát mà thiết bị đầu cuối sẽ truy nhập.

Tham số liên quan đến chính sách bảo mật bao gồm ID của lát của thiết bị đầu cuối, và thực thể SMF thu được chính sách bảo mật dựa trên ID của lát của thiết bị đầu cuối và mối quan hệ liên kết giữa ID của lát và chính sách bảo mật. Cụ thể là, một thiết bị đầu cuối có thể tương ứng với ID của ít nhất một lát. Chẳng hạn, thiết bị đầu cuối có thể truy nhập các lát khác nhau, và dữ liệu mặt phẳng người dùng của thiết bị đầu cuối có thể tương ứng với các chính sách bảo mật khác nhau trong các lát khác nhau.

Thiết bị đầu cuối thêm thông tin hỗ trợ chọn lát (network slice selection assistance information, NSSAI) vào thông điệp SR hoặc yêu cầu thiết lập phiên PDU (yêu cầu thiết lập phiên). SMF thu được chính sách bảo mật tương ứng với NSSAI. Nếu chính sách bảo mật của lát tương ứng với NSSAI là duy nhất, chính sách bảo mật thu được bởi thiết bị đầu cuối khi truy nhập lát là duy nhất. Nếu thông tin NSSAI bao gồm ít nhất một lát, lát cần được lựa chọn dựa trên chính sách bảo mật của lát hiện được truy nhập bởi thiết bị đầu cuối (các chính sách bảo mật của các lát khác nhau có thể khác nhau). Nếu chính sách bảo mật của lát hiện tại là duy nhất sau khi lát được truy nhập được xác định, chính sách bảo mật thu được bởi thiết bị đầu cuối khi truy nhập lát là duy nhất. Nếu chính sách bảo mật của lát hiện tại không phải là duy nhất, thiết bị đầu cuối cần cần xác định thêm chính sách bảo mật dựa trên thông tin khác. Có nhiều cách triển khai trong đó thiết bị đầu cuối cần xác định thêm chính sách bảo mật dựa trên thông tin khác. Chẳng hạn, thiết bị đầu cuối thực hiện chọn dựa trên ít nhất một ID, trong tham số liên quan, khác với ID của lát, chẳng hạn, bằng cách sử dụng ID của thiết bị đầu cuối hoặc ID phiên.

Cách triển khai a2

ID phiên của thiết bị đầu cuối là ID phiên tương ứng với phiên tương ứng với thông điệp yêu cầu hiện tại của thiết bị đầu cuối. Chẳng hạn, việc thiết bị đầu cuối thực hiện dịch vụ Internet (internet) (chẳng hạn duyệt trang web, xem video, và trò chuyện sử dụng WeChat) là phiên. Thiết bị đầu cuối truy nhập intranet của công tu trong đó đặt thiết bị đầu cuối, và sử dụng dịch vụ của riêng công ty (chẳng hạn, công ty thỏa mãn), và đây là phiên khác. Thiết bị đầu cuối truy nhập mạng thực hiện cuộc gọi VoIP, và đây là phiên khác. Ở đây, ID phiên

của dịch vụ truy nhập Internet (internet) có thể được gán bằng 1; ID phiên của intranet của công ty là 2; và ID phiên của cuộc gọ VoIP là 3.

Tham số liên quan đến chính sách bảo mật bao gồm ID phiên của thiết bị đầu cuối, và thực thể SMF thu được chính sách bảo mật dựa trên ID phiên của thiết bị đầu cuối và mối quan hệ liên kết giữa ID phiên và chính sách bảo mật. Theo cách này, đối với cùng thiết bị đầu cuối, khi thiết bị đầu cuối khởi tạo các phiên khác nhau, các chính sách bảo mật khác nhau có thể được lựa chọn cho các phiên khác nhau.

Chẳng hạn, có thiết bị đầu cuối bình thường, và thiết bị đầu cuối kích hoạt chỉ các dịch vụ thực hiện gọi và gửi thông điệp SMS. Hai dịch vụ này lần lượt thuộc hai phiên. Do vậy, QoS và các chính sách bảo mật là khác nhau tùy thuộc vào các phiên khác nhau. Đối với dịch vụ thực hiện cuộc gọi, bảo vệ tính toàn vẹn mặt phẳng người dùng không cần được kích hoạt, và trộn khóa không được yêu cầu. thuật toán mật mã hóa mặt phẳng người dùng 128-bit được sử dụng, và độ dài khóa mật mã hóa mặt phẳng người dùng bằng 128 bit. Đối với dịch vụ thông điệp SMS, bảo vệ tính toàn vẹn mặt phẳng người dùng cần được kích hoạt, và việc trộn khóa được yêu cầu. Thuật toán mật mã hóa mặt phẳng người dùng 128-bit được sử dụng, khóa mật mã hóa mặt phẳng người dùng 128-bit được sử dụng, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng 256-bit được sử dụng, và khóa bảo vệ tính toàn vẹn mặt phẳng người dùng 256-bit được sử dụng.

Chẳng hạn, dịch vụ tương ứng với ID phiên là dịch vụ độ trễ siêu thấp. Để đảm bảo độ trễ thấp, chính sách bảo mật cần sử dụng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng và thuật toán mật mã hóa mặt phẳng người dùng mà có mức độ bảo mật tương đối thấp, chẳng hạn thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng 128-bit và thuật toán mật mã hóa mặt phẳng người dùng, và khóa bảo vệ tính toàn vẹn mặt phẳng người dùng 128-bit và khóa mật mã hóa mặt phẳng người dùng; hoặc không thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng nào hoặc thuật toán mật mã hóa mặt phẳng người dùng được kích hoạt. Trong ví dụ khác, dịch vụ tương ứng với ID phiên là dịch vụ có yêu cầu độ tin cậy cao. Sau đó, không chỉ khóa mật mã hóa mặt

phẳng người dùng được yêu cầu để bảo vệ mật mã hóa, mà còn khóa bảo vệ tính toàn vẹn mặt phẳng người dùng được yêu cầu để bảo vệ tính toàn vẹn. Ngoài ra, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng và thuật toán mật mã hóa mặt phẳng người dùng mà có mức độ bảo mật tương đối cao, chẳng hạn thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng 256-bit và thuật toán mật mã hóa mặt phẳng người dùng, và khóa toàn vẹn mặt phẳng người dùng 256-bit và khóa mật mã hóa mặt phẳng người dùng cần được lựa chọn. Trong ví dụ khác, dịch vụ tương ứng với ID phiên là dịch vụ chung, chẳng hạn dịch vụ thoại. Sau đó, chỉ bảo vệ khóa mật mã hóa mặt phẳng người dùng có thể được yêu cầu, và bảo vệ tính toàn vẹn mặt phẳng người dùng không được yêu cầu. Ngoài ra, thuật toán mật mã hóa mặt phẳng người dùng 256-bit có thể được yêu cầu, nhưng khóa mật mã hóa mặt phẳng người dùng 128-bit là đủ. Có thể biết rằng, theo phương án thực hiện sáng chế, các chính sách bảo mật khác nhau có thể được lựa chọn tùy thuộc vào các dịch vụ khác nhau, để thỏa mãn yêu cầu động của bảo mật mặt phẳng người dùng.

Cách triển khai a3

Sau khi truy nhập lát, thiết bị đầu cuối có thể khởi tạo các phiên. Do vậy, ID của một lát có thể tương ứng với các ID phiên. Phép tương ứng được mô tả ở đây là phép tương ứng lôgic. Trong ứng dụng thực, điều này không nhất thiết có nghĩa là phép tương ứng giữa ID phiên và ID của lát có thể được xác định.

Thực thể SMF thu được chính sách bảo mật tương ứng với ID của lát và ID phiên dựa trên mối quan hệ liên kết trong số ID của thiết bị đầu cuối, ID của lát, ID phiên, và chính sách bảo mật. Theo cách này, việc phân chia độ chi tiết mịn hơn có thể thu được, và chính sách bảo mật được lựa chọn riêng rẽ cho các phiên khác nhau được khởi tạo trong cùng lát được truy nhập bởi thiết bị đầu cuối tương tự.

Cách triển khai a4

Một cách tùy chọn, thực thể SMF thu được chính sách bảo mật của thiết bị đầu cuối dựa trên mối quan hệ liên kết giữa ID luồng và chính sách bảo mật. Theo cách này, việc phân chia độ chi tiết mịn hơn có thể thu được, và chính sách bảo mật được lựa chọn riêng rẽ dựa trên nội dung cụ thể của cùng phiên

được khởi tạo trong cùng mạng được truy nhập bởi cùng thiết bị đầu cuối.

Chẳng hạn, thiết bị đầu cuối hỗ trợ dịch vụ truy nhập Internet. Do vậy, luồng dữ liệu truy nhập Internet có thể là duyệt trang web hoặc có thể là xem viđêo. Đối với thiết bị đầu cuối này, dịch vụ truy nhập Internet thuộc phiên 1. Sau đó, việc duyệt trang web là luồng 1, và xem viđêo là luồng 2. SMF thiết lập QoS cho luồng 1 khi thấy rằng không có QoS hỗ trợ luồng 1. Luồng 2 có cùng trường hợp. Nếu SMF thấy rằng QoS của cả luồng 1 lẫn luồng 2 là khả dụng, SMF gửi ngay QoS đến BS.

Cách triển khai a4

Tham số liên quan đến chính sách bảo mật bao gồm QoS của thiết bị đầu cuối, và thực thể SMF thu được chính sách bảo mật dựa trên QoS của thiết bị đầu cuối. Một cách tùy chọn, một số QoS tương ứng với ID của thiết bị đầu cuối có thể thu được dựa trên ID của thiết bị đầu cuối mà được bao gồm trong thông điệp yêu cầu. Chẳng hạn, QoS là việc thiết bị đầu cuối đòi hỏi độ trễ thấp, bảo mật cao, và tương tự. Sau đó, tập các chính sách bảo mật được thiết lập cho thiết bị đầu cuối dựa trên QoS. Theo phương án thực hiện sáng chế, chính sách bảo mật có thể được tiền tạo cấu hình trên SMF hoặc PCF, hoặc QoS tương ứng với DNN có thể thu được từ UPF và/hoặc UDM, và sau đó chính sách bảo mật thu được dựa trên QoS. QoS mặc định được nhập vào trên UDM ở thời điểm thuê bao. UPF có thể biết về QoS động từ cuộc gọi xử lý mạng ngoài hoặc thông điệp SMS, hoặc có thể biết về QoS động từ PCF, hoặc có thể tiền cấu hình QoS động.

Một cách tùy chọn, tham số liên quan đến chính sách bảo mật bao gồm DNN của thiết bị đầu cuối, và tập các chính sách bảo mật được thiết lập tương ứng dựa trên DNN. Chẳng hạn, DNN là Youku. Có nhiều dịch vụ viđêo trong mạng Youku, và do vậy chính sách bảo mật được thiết lập cho thiết bị đầu cuối có thể có độ trễ thấp hơn. Trong ví dụ khác, DNN là website liên quan tài chính, và do vậy chính sách bảo mật được thiết lập cho thiết bị đầu cuối cần có bảo mật cao hơn.

Ngoài ra, QoS tương ứng với DNN có thể thu được dựa trên DNN từ phần tử CN chẳng hạn PCF/UPF hoặc UDM. QoS mang chính sách bảo mật, hoặc

chính sách bảo mật được thiết lập sau đó dựa trên QoS. QoS thu được từ PCF là thông tin QoS động, và QoS thu được từ UDM là thông tin QoS mặc định ở thời điểm thuê bao người dùng.

Một cách tùy chọn, SMF có thể thu được thông tin từ UDM bằng cách gửi yêu cầu dữ liệu thuê bao đến UDM, và nhận đáp ứng dữ liệu thuê bao từ UDM. SMF có thể thu được thông tin từ PCF bằng cách sử dụng thông tin chỉnh sửa phiên PDU-CAN. SMF có thể thu được thông tin từ UPF bằng cách gửi yêu cầu chỉnh sửa/thiết lập phiên đến UPF và nhận đáp ứng chỉnh sửa/thiết lập phiên từ UDM.

Theo cách triển khai a4, QoS có thể được nhận diện bằng cách sử dụng ID bởi luồng QoS, có thể được gọi là ID luồng QoS (QoS Flow ID, QFI). Theo phương án thực hiện sáng chế, tiểu sử QoS (Tiểu sử QoS) được nhận diện bằng cách sử dụng QFI.

QoS có thể bao các tham số, chẳng hạn bộ chỉ báo (5G QoS indicator, 5QI). 5QI được sử dụng để nhận diện các đặc tính hiệu năng, mà có thể bao gồm một hoặc nhiều trong số loại tài nguyên (tốc độ bit luồng được đảm bảo (Guaranteed flow bit rate, GBR) hoặc phi GBR), mức độ trễ gói, và tỷ lệ lỗi bit, và có thể còn bao gồm tham số khác. 5QI là tham số cơ bản được sử dụng bởi phần tử mạng để phân phối tài nguyên đến QoS.

QoS có thể còn bao gồm độ ưu tiên giữ lại và phân phối (allocation and retention priority, ARP), và độ ưu tiên có thể được nhận diện bởi từ 1 đến 15, chỉ báo độ ưu tiên yêu cầu tài nguyên bởi QoS và liệu việc thiết lập của DRB có thể bị loại bỏ do giới hạn tài nguyên.

QoS có thể còn bao gồm hai tham số, được sử dụng để định nghĩa liệu tài nguyên (chẳng hạn, DRB) tương ứng với QoS khác có thể bị chiếm trước hoặc liệu DRB được thiết lập cho QoS có thể bị chiếm trước bởi QoS khác.

Một cách tùy chọn, đối với nội dung dữ liệu có GBR, QoS có thể còn bao gồm: GBR, có thể được sử dụng cho liên kết lên (uplink, UL) và liên kết xuống (downlink, DL). Nội dung dữ liệu có GBR có thể là phiên hoặc luồng, và dữ liệu GBR có mức dịch vụ tương ứng. Các mức dịch vụ khác nhau cũng có thể tương ứng với QoS khác nhau. Dữ liệu phi GBR tương ứng với mức dịch vụ

mặc định. Chẳng hạn, đối với nhà khai thác, cần đảm bảo thực hiện cuộc gọi. Do vậy, thực hiện cuộc gọi có đảm bảo GBR. Đối với dịch vụ thông điệp SMS bình thường, tức là, phi GBR, độ trễ nhỏ sẽ không phải là vấn đề. Ngoài ra, chẳng hạn, nếu dịch vụ của nhà khai thác được mang đến cho trò chơi Tencent, luồng dịch vụ phi GBR của trò chơi Tencent trở thành GBR.

Một cách tùy chọn, QoS còn bao gồm tốc độ bit luồng lớn nhất (Maximum Flow Bit Rate, MFBR), và tất cả các luồng của một phiên cộng dồn và không thể vượt quá tốc độ này. Khi tốc độ được vượt quá, tham khảo ARP để xác định liệu có từ chối thiết lập hoặc chiếm trước tài nguyên khác.

Một cách tùy chọn, QoS còn bao gồm điều khiển thông báo. Thiết lập này là bật hoặc tắt. Nếu DRB không thể được thiết lập cho QoS, cần xác định, dựa trên bật/tắt điều khiển thông báo, liệu có thông báo cho thiết bị đầu cuối hay không.

Một cách tùy chọn, chính sách bảo mật còn bao gồm ít nhất một của nội dung sau: thông tin chỉ báo mật mã hóa, trong đó thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS để kích hoạt bảo vệ mật mã hóa cho thiết bị đầu cuối; độ dài khóa; thông tin chỉ báo D - H, trong đó thông tin chỉ báo D - H được sử dụng để chỉ báo BS để kích hoạt D-H cho thiết bị đầu cuối; và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ. Tức là, chính sách bảo mật có thể còn bao gồm một hoặc nhiều trong số: liệu có kích hoạt mật mã hóa mặt phẳng người dùng, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, liệu có sử dụng thuật toán mật mã hóa/giải mật mã hóa 128-bit hoặc 256-bit, liệu có sử dụng độ dài khóa 128-bit hoặc 256-bit, và liệu có kích hoạt việc trộn khóa. Một số ví dụ cụ thể được nêu. Chẳng hạn, các bit được sử dụng để chỉ báo nội dung được bao gồm trong chính sách bảo mật. Chẳng hạn, chuỗi bit 0000000 chỉ báo không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, và không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Do cả hai đều không được kích hoạt, tất cả đều 0. Trong ví dụ khác, chuỗi bit 1010100 chỉ báo để kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng nhưng không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, để sử dụng thuật toán mật mã hóa 128-bit, và không kích hoạt trộn

khóa. Nên lưu ý rằng chỉ các ví dụ được nêu, và tất cả các ví dụ tuân theo quy tắc này được đề cập đến theo sáng chế. Theo phương án thực hiện sáng chế, việc trộn khóa đề cập đến D-H, và D-H là thuật toán trộn khóa.

Một cách tùy chọn, khi thực thể SMF xác định rằng thông tin chỉ báo mật mã hóa cần được kích hoạt trong chính sách bảo mật của thiết bị đầu cuối, chính sách bảo mật có thể còn bao gồm thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ. Theo cách khác, thuật toán mật mã hóa mặt phẳng người dùng được phép xuất hiện trong chính sách bảo mật nghĩa là mật mã hóa mặt phẳng người dùng cần được kích hoạt. Một cách tùy chọn, mạng phục vụ là mạng cấp dịch vụ cho thiết bị đầu cuối.

Một cách tùy chọn, chính sách bảo mật có thể bao gồm độ dài khóa của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng, hoặc có thể bao gồm độ dài khóa của thuật toán mật mã hóa mặt phẳng người dùng. Theo cách khác, thuật toán mật mã hóa mặt phẳng người dùng được phép xuất hiện trong chính sách bảo mật và thuật toán là 256 bit, chỉ báo rằng độ dài khóa 256 bit được sử dụng.

Một cách tùy chọn, trước khi BS thu được chính sách bảo mật, phương pháp còn bao gồm việc BS gửi thông tin chỉ báo độ ưu tiên thứ nhất đến thực thể AMF. Thông tin chỉ báo độ ưu tiên thứ nhất được sử dụng để chỉ báo rằng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS không được sắp xếp dựa trên độ ưu tiên.

Một cách tùy chọn, AMF chuyển tiếp thông tin chỉ báo độ ưu tiên thứ nhất đến SMF. Do vậy, sau khi thu được thông tin chỉ báo độ ưu tiên thứ nhất, SMF biết rằng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS không được sắp xếp dựa trên độ ưu tiên. Do vậy, SMF thực hiện sắp xếp độ ưu tiên trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, hoặc thực hiện sắp xếp độ ưu tiên trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối. Thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối thu được từ AMF.

Theo triển khai tùy chọn khác, nếu SMF không thu được thông tin chỉ báo

độ ưu tiên thứ nhất, hoặc SMF nhận biết, theo cách khác, rằng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS được sắp xếp dựa trên độ ưu tiên, một cách tùy chọn SMF không thực hiện sắp xếp độ ưu tiên trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ. Một cách tùy chọn, sắp xếp độ ưu tiên có thể được thực hiện trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ dựa trên nhiều yếu tố, chẳng hạn, dựa trên các yếu tố chẳng hạn độ ưu tiên nhà khai thác hiện tại và môi trường mạng phục vụ cục bộ.

Một cách tùy chọn, trước khi BS thu được chính sách bảo mật, phương pháp còn bao gồm việc BS gửi thông tin chỉ báo độ ưu tiên thứ hai đến thực thể AMF. Thông tin chỉ báo độ ưu tiên thứ hai được sử dụng để chỉ báo liệu mật mã hóa mặt phẳng người dùng được phép bởi BS không được sắp xếp dựa trên độ ưu tiên.

Một cách tùy chọn, AMF chuyển tiếp thông tin chỉ báo độ ưu tiên thứ hai đến SMF. Do vậy, sau khi thu được thông tin chỉ báo độ ưu tiên thứ hai, SMF nhận biết rằng thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS không được sắp xếp dựa trên độ ưu tiên. Do vậy, SMF thực hiện sắp xếp độ ưu tiên trên thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ, hoặc thực hiện sắp xếp độ ưu tiên trên thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối. Thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối thu được từ AMF.

Theo triển khai tùy chọn khác, nếu SMF không thu được thông tin chỉ báo độ ưu tiên thứ hai, hoặc SMF nhận biết, theo cách khác, rằng thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS được sắp xếp dựa trên độ ưu tiên, một cách tùy chọn SMF không thực hiện sắp xếp độ ưu tiên trên thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ. Một cách tùy chọn, sắp xếp độ ưu tiên có thể được thực hiện trên thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ dựa trên nhiều yếu tố, chẳng hạn, dựa trên các yếu tố chẳng hạn độ ưu tiên nhà khai thác hiện tại và môi trường mạng phục vụ cục bộ.

Trong ví dụ nêu trên, độ ưu tiên của thuật toán mật mã hóa mặt phẳng người

dùng và độ ưu tiên của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được mô tả riêng rẽ. Theo triển khai tùy chọn khác, một đoạn thông tin chỉ báo được sử dụng để chỉ báo các độ ưu tiên của cả thuật toán mật mã hóa mặt phẳng người dùng và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng.

Một cách tùy chọn, trước khi BS thu được chính sách bảo mật, phương pháp còn bao gồm việc BS gửi thông tin chỉ báo độ ưu tiên thứ ba đến thực thể AMF. Thông tin chỉ báo độ ưu tiên thứ ba được sử dụng để chỉ báo rằng cả thuật toán mật mã hóa mặt phẳng người dùng lẫn thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS không được sắp xếp dựa trên độ ưu tiên. Thuật toán mật mã hóa mặt phẳng người dùng và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng có thể giống hoặc khác nhau.

Một cách tùy chọn, AMF chuyển tiếp thông tin chỉ báo độ ưu tiên thứ ba đến SMF. Do vậy, sau khi thu được thông tin chỉ báo độ ưu tiên thứ ba, SMF nhận biết rằng thuật toán mật mã hóa mặt phẳng người dùng và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng mà được phép bởi BS không được sắp xếp dựa trên độ ưu tiên. Do vậy, SMF thực hiện sắp xếp độ ưu tiên trên thuật toán mật mã hóa mặt phẳng người dùng và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ hoặc thực hiện sắp xếp độ ưu tiên trên thuật toán mật mã hóa mặt phẳng người dùng và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối. Thuật toán mật mã hóa mặt phẳng người dùng và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối thu được từ AMF.

Theo triển khai tùy chọn khác, nếu SMF không thu được thông tin chỉ báo độ ưu tiên thứ ba, hoặc SMF nhận biết, theo các cách khác, rằng thuật toán mật mã hóa mặt phẳng người dùng và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng mà được phép bởi BS được sắp xếp dựa trên độ ưu tiên. Một cách tùy chọn, SMF không thực hiện sắp xếp độ ưu tiên trên thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ. Một cách tùy chọn, sắp xếp độ ưu tiên có thể được thực hiện, dựa trên nhiều yếu tố, trên thuật toán mật mã hóa mặt phẳng người dùng và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, chẳng hạn, dựa trên các yếu tố chẳng

hạn độ ưu tiên nhà khai thác hiện tại và môi trường mạng cục bộ.

Fig.2b thể hiện ví dụ của lưu đồ phương pháp truyền thông khác theo phương án thực hiện sáng chế.

Dựa trên nội dung nêu trên, phương án thực hiện sáng chế đề xuất phương pháp truyền thông. Như được thể hiện trên Fig.2b, phương pháp bao gồm các bước sau.

Bước 221: BS thu được chính sách bảo mật, trong đó chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối.

Giống với nội dung nêu trên, một cách tùy chọn, chính sách bảo mật có thể còn bao gồm thuật toán mật mã hóa mặt phẳng người dùng được phép, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, và thông tin chỉ báo chỉ báo liệu có kích hoạt việc trộn khóa. Một cách tùy chọn, thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ có thể bao gồm kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng và thông tin độ dài khóa. Chẳng hạn, khi thuật toán mật mã hóa mặt phẳng người dùng là 256 bit, khóa 256-bit được sử dụng. Một cách tùy chọn, nếu thuật toán mật mã hóa trống xuất hiện trong thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ, BS được phép không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Một cách tùy chọn, nếu thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ xuất hiện trong chính sách bảo mật, BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Một cách tùy chọn, độ dài khóa được xác định dựa trên thông tin bit của thuật toán tính toàn vẹn, tức là, thuật toán tính toàn vẹn 256-bit sử dụng khóa 256-bit. Một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép không có thuật toán trống. Nếu thuật toán bảo vệ tính toàn vẹn không xuất hiện trong chính sách bảo mật, bảo vệ tính toàn vẹn không được kích hoạt. Một cách tùy chọn, BS cũng có thể được thông báo về thông tin độ dài khóa bằng cách sử dụng thông tin khác, chẳng hạn, bằng cách sử dụng thông tin bit.

Bước 222: Khi thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo BS để kích

hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối, BS xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích.

Bước 223: BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối. Đối với cách thức BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối, tham khảo nội dung nêu trên, và các chi tiết không được mô tả lại ở đây.

Một cách tùy chọn, các thủ tục SMC AS và AS SMP nêu trên có thể còn được bao gồm giữa bước 221 và bước 223, và được sử dụng để thương lượng lại thuật toán bảo mật mặt phẳng báo hiệu đích giữa BS và thiết bị đầu cuối. Cụ thể là, bước 201 đến bước 204 có thể được thêm giữa bước 221 và bước 223.

Một cách tùy chọn, việc BS thu được chính sách bảo mật bao gồm: BS nhận chính sách bảo mật từ thực thể SMF. Theo cách khác, một cách tùy chọn, BS lưu trữ trước chính sách bảo mật, và sau đó BS nhận ID của chính sách bảo mật từ thực thể SMF và thu được chính sách bảo mật dựa trên ID của chính sách bảo mật.

Một cách tùy chọn, lớp giao thức hệ thống thư mục (Directory System Protocol, SDAP) có thể được định nghĩa trên BS để ánh xạ QoS đến lớp giao thức hội tụ dữ liệu gói (Packet Data Convergence Protocol, PDCP). Mỗi lớp PDCP tương ứng với một DRB. Do vậy, mức bảo vệ được định nghĩa trước cần được phân chia thêm ở phía RAN. Nếu bảo mật vẫn được thực hiện ở lớp PDCP, mật mã hóa và giải mã mặt phẳng người dùng và bảo vệ tính toàn vẹn vẫn được hoàn thành ở lớp PDCP. Do một lớp PDCP tương ứng với một DRB, chỉ xử lý bảo mật mức DRB có thể được thực hiện ở phía RAN. Nếu xử lý bảo mật một phần hoặc bảo mật có thể được di chuyển lên đến lớp SDAP, xử lý bảo mật mức luồng QoS có thể được triển khai. Bảo mật một phần nghĩa là nếu chỉ bảo vệ tính toàn vẹn mặt phẳng người dùng dựa trên độ chi tiết luồng, chỉ xử lý bảo mật liên quan đến bảo vệ tính toàn vẹn cần được đặt ở lớp SDAP. Nếu xử lý mật mã hóa và giải mã mặt phẳng người dùng và bảo vệ tính toàn vẹn dựa trên độ chi tiết luồng, chúng đều cần được hoàn thành ở lớp SDAP. Do vậy, điều kiện tiên quyết để xử lý bảo mật dựa trên mức độ chi tiết luồng là việc bảo mật hoặc bảo mật một phần được triển khai ở lớp SDAP.

Chẳng hạn, có bốn luồng dịch vụ (luồng IP) và ba luồng QoS trong một phiên. Ánh xạ mức NAS chỉ báo xử lý QoS lần thứ nhất. Luồng IP được ánh xạ dưới dạng luồng QoS, được biểu diễn bởi QFI. Có thể thấy rằng luồng IP 1 và luồng IP 4 được đặt ở QFI 1, và mỗi luồng trong các luồng khác trong một QFI riêng rẽ. Ở lớp SDAP, lớp SDAP ánh xạ các QFI của các luồng khác nhau đến các lớp PDCP khác nhau. Có thể thấy rằng QFI 1 và QFI 2 được đặt ở một thực thể PDCP, chỉ báo rằng QFI 1 và QFI 2 được truyền bằng cách sử dụng một DRB. (Một thực thể PDCP tương ứng với một kênh mang DRB), và QFI-3 được đặt trên thực thể PDCP 2 khác, vốn là DRB khác.

Một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên. Theo cách khác, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên. Sắp xếp độ ưu tiên có thể được thực hiện, dựa trên độ ưu tiên nhà khai thác cục bộ, môi trường cục bộ, hoặc tương tự, trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS có thể được tiền tạo cấu hình trên BS. Sắp xếp độ ưu tiên có thể được thực hiện, dựa trên nội dung thuê bao truy nhập mạng của thiết bị đầu cuối, độ ưu tiên của thiết bị đầu cuối, và/hoặc tương tự, trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và có thể được thực hiện bởi thiết bị đầu cuối ở thời điểm thuê bao hoặc mua nhiều dịch vụ hơn. Một cách tùy chọn, chính sách bảo mật có thể bao gồm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối.

Một cách tùy chọn, ở bước 222, theo giải pháp triển khai tùy chọn, chính sách bảo mật bao gồm ít nhất một thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. BS trực tiếp xác định một thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng trong ít nhất một thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được bao gồm trong chính sách bảo mật, như là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Theo giải pháp tùy chọn khác, việc

BS xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích bao gồm: BS xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS.

BS có thể xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích theo vài cách triển khai tùy chọn. Chẳng hạn, BS xác định ít nhất một thuật toán mà thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, và xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích trong ít nhất một thuật toán. Một cách tùy chọn, nếu thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, thuật toán có độ ưu tiên tương đối cao hoặc độ ưu tiên cao nhất trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS được xác định từ ít nhất một thuật toán làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Một cách tùy chọn, nếu thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, BS xác định thuật toán có độ ưu tiên tương đối cao hoặc độ ưu tiên cao nhất trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, từ ít nhất một thuật toán làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích.

Một cách tùy chọn, chính sách bảo mật còn bao gồm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ. Một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên. Một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ có thể được tiền tạo cấu hình trên SMF. Độ ưu tiên của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ có thể được sắp xếp dựa trên các yếu tố

chẳng hạn độ ưu tiên nhà khai thác và/hoặc môi trường cục bộ. Một cách tùy chọn, việc BS xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS bao gồm các bước sau: BS xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ. Cụ thể là, khi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ được sắp xếp dựa trên độ ưu tiên, thực hiện lựa chọn bằng cách sử dụng sắp xếp độ ưu tiên được phép bởi mạng phục vụ làm điều kiện sơ cấp hoặc bằng cách sử dụng sắp xếp độ ưu tiên được phép bởi BS làm điều kiện sơ cấp. Việc sử dụng sắp xếp độ ưu tiên nào tùy thuộc vào chính sách của nhà khai thác cục bộ hoặc thông tin khác. Chẳng hạn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng hiện tại được phép bởi BS được cập nhật hiện tại, và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ được cập nhật lâu rồi. Do vậy, sắp xếp độ ưu tiên của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS được sử dụng làm điều kiện sơ cấp. Trong ví dụ khác, sắp xếp độ ưu tiên của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS được sử dụng mặc định làm điều kiện sơ cấp. Nếu thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ không được sắp xếp dựa trên độ ưu tiên, sắp xếp độ ưu tiên của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS được sử dụng làm điều kiện sơ cấp.

BS có thể xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích theo vài cách triển khai tùy chọn. Chẳng hạn, BS xác định ít nhất một thuật toán mà thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, mà cũng thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, và mà cũng thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, và xác định

thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích từ ít nhất một thuật toán. Một cách tùy chọn, nếu thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, thuật toán với độ ưu tiên tương đối cao hoặc độ ưu tiên cao nhất trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS được xác định từ ít nhất một thuật toán làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Một cách tùy chọn, nếu thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, BS xác định thuật toán với độ ưu tiên tương đối cao hoặc độ ưu tiên cao nhất trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, từ ít nhất một thuật toán làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Một cách tùy chọn, nếu thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, BS xác định thuật toán với độ ưu tiên tương đối cao hoặc độ ưu tiên cao nhất trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, từ ít nhất một thuật toán làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Một cách tùy chọn, mạng theo phương án thực hiện sáng chế có thể bao gồm mạng 5G hoặc mạng tiến hóa từ mạng 5G.

Một cách tùy chọn, phương pháp còn bao gồm bước sau: Khi chính sách bảo mật còn bao gồm thông tin chỉ báo mật mã hóa, và thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS để kích hoạt bảo vệ mật mã hóa cho thiết bị đầu cuối, BS gửi thuật toán mật mã hóa mặt phẳng người dùng đích đến thiết bị đầu cuối.

Dựa trên nội dung nêu trên, phần sau mô tả quá trình phương pháp trong đó BS và thiết bị đầu cuối còn cần để thương lượng thuật toán mật mã hóa mặt phẳng người dùng đích.

Một cách tùy chọn, thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS là thuật toán mật mã hóa mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên. Theo cách khác, thuật toán mật mã hóa mặt phẳng người dùng

được hỗ trợ bởi thiết bị đầu cuối là thuật toán mật mã hóa mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên. Sắp xếp độ ưu tiên có thể được thực hiện, dựa trên ít nhất độ ưu tiên nhà khai thác, trên thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, và thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS có thể được sắp xếp bởi nhà khai thác trong khi xây dựng mạng và có thể được tiền tạo cấu hình trên BS. Sắp xếp độ ưu tiên có thể được thực hiện, dựa trên độ ưu tiên nhà khai thác, trên thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối có thể được sắp xếp bởi người dùng trong khi thuê bao truy nhập mạng. Một cách tùy chọn, chính sách bảo mật có thể bao gồm thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối.

Một cách tùy chọn, giải pháp triển khai tùy chọn còn được bao gồm. Chính sách bảo mật bao gồm ít nhất một thuật toán mật mã hóa mặt phẳng người dùng, và BS xác định ngay một thuật toán mật mã hóa mặt phẳng người dùng trong ít nhất một thuật toán mật mã hóa mặt phẳng người dùng được bao gồm trong chính sách bảo mật, làm thuật toán mật mã hóa mặt phẳng người dùng đích. Theo giải pháp tùy chọn khác, BS xác định thuật toán mật mã hóa mặt phẳng người dùng đích dựa trên thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối and thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS.

BS có thể xác định thuật toán mật mã hóa mặt phẳng người dùng đích theo vài cách triển khai tùy chọn. Chẳng hạn, BS xác định ít nhất một thuật toán mà thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, và xác định thuật toán mật mã hóa mặt phẳng người dùng đích từ ít nhất một thuật toán. Một cách tùy chọn, nếu thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS là thuật toán mật mã hóa mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, thuật toán với độ ưu tiên tương đối cao hoặc độ ưu tiên cao nhất trong thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS được xác định, làm thuật toán mật mã hóa mặt phẳng người dùng

đích, từ ít nhất một thuật toán that thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS. Một cách tùy chọn, nếu thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối là thuật toán mật mã hóa mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, BS xác định thuật toán với độ ưu tiên tương đối cao hoặc độ ưu tiên cao nhất trong thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, làm thuật toán mật mã hóa mặt phẳng người dùng đích từ ít nhất một thuật toán mà thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS.

Một cách tùy chọn, chính sách bảo mật còn bao gồm thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ. Một cách tùy chọn, thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ là thuật toán mật mã hóa mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên. Một cách tùy chọn, thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ có thể được tiền tạo cấu hình trên SMF. Độ ưu tiên của thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ có thể được sắp xếp dựa trên ít nhất độ ưu tiên nhà khai thác. Một cách tùy chọn, việc BS xác định thuật toán mật mã hóa mặt phẳng người dùng đích dựa trên thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS bao gồm bước sau: BS xác định thuật toán mật mã hóa mặt phẳng người dùng đích dựa trên thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ. Cụ thể là, khi thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ được sắp xếp dựa trên độ ưu tiên, thực hiện lựa chọn bằng cách sử dụng sắp xếp độ ưu tiên được phép bởi mạng phục vụ làm điều kiện sơ cấp. Nếu thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ không được sắp xếp dựa trên độ ưu tiên, độ ưu tiên của thuật toán bảo mật mặt phẳng

người dùng được phép bởi BS được sử dụng làm điều kiện sơ cấp.

BS có thể xác định thuật toán mật mã hóa mặt phẳng người dùng đích theo vài cách triển khai tùy chọn. Chẳng hạn, BS xác định ít nhất một thuật toán mà thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, và mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ, và xác định thuật toán mật mã hóa mặt phẳng người dùng đích từ ít nhất một thuật toán that thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, và mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ. Một cách tùy chọn, nếu thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS là thuật toán mật mã hóa mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, thuật toán có độ ưu tiên tương đối cao hoặc độ ưu tiên cao nhất trong thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS được xác định làm thuật toán mật mã hóa mặt phẳng người dùng đích từ ít nhất một thuật toán mà thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, và mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ. Một cách tùy chọn, nếu thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối là thuật toán mật mã hóa mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, BS xác định thuật toán có độ ưu tiên tương đối cao hoặc độ ưu tiên cao nhất trong thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, làm thuật toán mật mã hóa mặt phẳng người dùng đích từ ít nhất một thuật toán mà thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, và mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ. Một cách tùy chọn, nếu thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ là thuật toán mật mã hóa mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, BS xác định thuật toán với độ ưu tiên tương

đối cao hoặc độ ưu tiên cao nhất trong thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ, làm thuật toán mật mã hóa mặt phẳng người dùng đích từ ít nhất một thuật toán mà thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, và mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ.

Một cách tùy chọn, khi chính sách bảo mật còn bao gồm độ dài khóa, BS gửi độ dài khóa đến thiết bị đầu cuối. Độ dài khóa bao gồm độ dài khóa bảo vệ tính toàn vẹn mặt phẳng người dùng và độ dài khóa mật mã hóa mặt phẳng người dùng. Một cách tùy chọn, theo phương án thực hiện sáng chế, khi gửi thông tin chẳng hạn thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích, thuật toán mật mã hóa mặt phẳng người dùng đích, và độ dài khóa đến thiết bị đầu cuối, BS có thể sử dụng một đoạn báo hiệu chẳng hạn yêu cầu tái cấu hình RRC, hoặc sử dụng các đoạn thông tin.

Theo triển khai tùy chọn, nếu yêu cầu tái cấu hình RRC được sử dụng để gửi, có thể có nhiều cách gửi. Chẳng hạn, thông điệp tái cấu hình RRC có thể được sử dụng. Thông điệp tái cấu hình RRC có thể bao gồm ít nhất một trong thuật toán mật mã hóa mặt phẳng người dùng đích, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích, độ dài khóa mật mã hóa mặt phẳng người dùng, độ dài khóa bảo vệ tính toàn vẹn mặt phẳng người dùng, chính sách trộn khóa (cũng có thể được gọi là D-H), thông tin chỉ báo kích hoạt hoặc vô hiệu hóa, DRB-1 (thông tin QoS), DRB-2 (thông tin QoS), và tham số khác.

Theo triển khai tùy chọn, nếu tính toàn vẹn mặt phẳng người dùng không được kích hoạt, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích không được truyền. Khi chính thuật toán có thể chỉ báo độ dài khóa, thông tin chỉ báo của độ dài khóa có thể không được mang. Khi BS không hỗ trợ hoặc không cần kích hoạt chính sách trộn khóa, chính sách trộn khóa không cần được truyền. Theo phương pháp này, chính sách bảo mật không được truyền trên mỗi DRB. Do vậy, phương pháp này áp dụng được cho trường hợp trong đó tất cả các DRB sử dụng cùng khả năng bảo mật. Ngoài ra, chính sách bảo mật đích có thể được tạo cấu hình cho tất cả các DRB qua một quá trình chọn.

Theo triển khai tùy chọn khác, thông điệp tái cấu hình RRC có thể bao gồm: tham số tái cấu hình;

DRB-1 (thuật toán mật mã hóa bảo mật mặt phẳng người dùng đích -1, [thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích-1], [độ dài khóa mật mã hóa mặt phẳng người dùng-1], [độ dài khóa bảo vệ tính toàn vẹn mặt phẳng người dùng-1], [chính sách trộn khóa], tham số QoS, tham số khác); và

DRB-2 (thuật toán mật mã hóa bảo mật mặt phẳng người dùng đích -2, [thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích-2], [độ dài khóa mật mã hóa mặt phẳng người dùng-2], [độ dài khóa bảo vệ tính toàn vẹn mặt phẳng người dùng-2], [chính sách trộn khóa], tham số QoS, tham số khác), tham số khác).

Thông điệp tái cấu hình RRC chỉ thể hiện hai trường hợp ví dụ: DRB-1 và DRB-2. Định dạng được mang trong thông điệp tái cấu hình RRC có thể giống định dạng trong ví dụ nêu trên, và tất cả hoặc một số mục tham số có thể được mang. Chẳng hạn, các tham số được bao gồm trong [] trong ví dụ nêu trên có thể được mang hoặc không thể được mang. Theo cách này, chính sách bảo mật đích có thể được tạo cấu hình cho mỗi DRB, và chính sách bảo mật đích của mỗi DRB có thể giống nhau, hoặc chính sách bảo mật đích của mỗi DRB có thể khác nhau.

Hai phương pháp nêu trên cũng có thể được sử dụng cùng nhau, tức là, một số chính sách bảo mật đích có thể được chia sẻ bởi tất cả các DRB, và chính sách bảo mật khác nhau tùy thuộc vào các DRB khác nhau. Chẳng hạn, thông điệp tái cấu hình RRC bao gồm:

thuật toán mật mã hóa bảo mật mặt phẳng người dùng đích;

DRB-1 ([thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích-1], [độ dài khóa mật mã hóa mặt phẳng người dùng-1], [độ dài khóa bảo vệ tính toàn vẹn mặt phẳng người dùng-1], [chính sách trộn khóa], tham số QoS, tham số khác);

DRB-2 (, [thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích-2], [độ dài khóa mật mã hóa mặt phẳng người dùng-2], [độ dài khóa bảo vệ tính toàn vẹn mặt phẳng người dùng-2], [chính sách trộn khóa], tham số QoS, tham

số khác); và

tham số khác.

Một cách tùy chọn, trước khi BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối, phương pháp còn bao gồm việc BS nhận QoS của phiên hiện tại của thiết bị đầu cuối từ thực thể SMF. Một cách tùy chọn, QoS của phiên hiện tại và chính sách bảo mật có thể được gửi bằng cách sử dụng một thông điệp hoặc có thể được gửi riêng rẽ bằng cách sử dụng các thông điệp. Một cách tùy chọn, BS còn nhận, từ AMF, một số thông tin cơ bản được sử dụng để tạo khóa, chẳng hạn, khóa cơ sở được sử dụng để tạo khóa bảo vệ tính toàn vẹn mặt phẳng người dùng và khóa cơ sở được sử dụng để tạo khóa mật mã hóa mặt phẳng người dùng.

Một cách tùy chọn, BS phân phối DRB đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS, và DRB được phân phối bởi BS. BS phân phối, dựa trên ít nhất QoS, DRB đến dữ liệu được truyền đến thiết bị đầu cuối. Trong 5G, trong một DRB, có thể có các luồng dữ liệu tương ứng với các loại QoS.

Một cách tùy chọn, một DRB có thể tương ứng với các đoạn QoS. DRB đích được phân phối đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS.

Một cách tùy chọn, khi DRB lịch sử không thỏa mãn điều kiện thứ nhất tồn tại trên BS, và không có ít nhất một DRB lịch sử thỏa mãn điều kiện thứ hai trên BS, BS thiết lập DRB đích cho thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS.

Một cách tùy chọn, khi DRB lịch sử không thỏa mãn điều kiện thứ nhất tồn tại trên BS, BS thiết lập DRB đích cho thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS.

Một cách tùy chọn, BS thiết lập DRB đích cho thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS.

Một cách tùy chọn, DRB lịch sử được thiết lập trước đó có thể được lựa chọn làm DRB đích cho thiết bị đầu cuối, hoặc DRB có thể mới được thiết lập làm DRB đích.

Theo triển khai tùy chọn, một trong DRB lịch sử có thể được lựa chọn trước làm DRB đích cho thiết bị đầu cuối, và nếu DRB đích không thể được lựa chọn từ DRB lịch sử, DRB mới được thiết lập cho thiết bị đầu cuối làm DRB đích.

Theo cách khác, dựa trên một số quy tắc định trước, trước hết được xác định liệu thiết bị đầu cuối có được phép sử dụng DRB lịch sử hay không. Nếu thiết bị đầu cuối được phép, một trong các DRB lịch sử có thể được lựa chọn trước làm DRB đích cho thiết bị đầu cuối. Nếu DRB đích không thể được lựa chọn từ DRB lịch sử, DRB mới được thiết lập cho thiết bị đầu cuối và được sử dụng trực tiếp làm DRB đích. Để mô tả chi tiết hơn giải pháp nêu trên, phần sau sử dụng vài ví dụ chi tiết để mô tả.

Cách triển khai b1

Khi ít nhất một DRB lịch sử thỏa mãn điều kiện thứ nhất tồn tại trên BS, DRB đích là một trong ít nhất một DRB lịch sử thỏa mãn điều kiện thứ nhất. QoS được hỗ trợ bởi mỗi DRB của ít nhất một DRB lịch sử thỏa mãn điều kiện thứ nhất giống như QoS của phiên hiện tại, và chính sách bảo mật giống như chính sách bảo mật được hỗ trợ bởi mỗi DRB.

Một cách tùy chọn, điều kiện thứ nhất bao gồm việc QoS được hỗ trợ giống như QoS của phiên hiện tại, và việc chính sách bảo mật thu được ở bước 221 giống như chính sách bảo mật được hỗ trợ.

Thông tin về việc sử dụng lại DRB có thể được triển khai bằng cách gửi thông điệp. Chẳng hạn, thông điệp được truyền đến thiết bị đầu cuối lần đầu là: thông điệp tái cấu hình RRC (thuật toán mật mã hóa mặt phẳng người dùng đích-1, DRB-1 (thông tin QoS-1), DRB-2 (thông tin QoS-2), tham số khác); thông điệp được truyền đến thiết bị đầu cuối trong lần thứ hai là: thông điệp tái cấu hình RRC (thuật toán mật mã hóa mặt phẳng người dùng hiện tại-1, DRB-1 (thông tin QoS-1), DRB-2 (thông tin QoS-2), DRB-3 (thuật toán mật mã hóa mặt phẳng người dùng hiện tại-2, thông tin QoS-2/3/4), tham số khác)). Theo cách này, chính sách bảo mật của DRB-2 được chỉnh sửa để đạt được mục đích tận dụng lại QoS. Có thể nhận biết từ ví dụ này rằng mục đích sử dụng DRB lịch sử làm DRB đích đạt được bằng cách gửi báo hiệu.

Trong ví dụ khác, để đạt được mục đích tận dụng lại DRB lịch sử, thông

điệp được truyền đến thiết bị đầu cuối trong lần thứ nhất là: thông điệp tái cấu hình RRC (thuật toán mật mã hóa mặt phẳng người dùng đích-1, DRB-1 (thông tin QoS-1), DRB-2 (thông tin QoS-2), tham số khác)); thông điệp được truyền đến thiết bị đầu cuối trong lần thứ hai là: thông điệp tái cấu hình RRC (thuật toán mật mã hóa mặt phẳng người dùng hiện tại-1, DRB-1 (thông tin QoS-1), DRB-2 (thuật toán mật mã hóa mặt phẳng người dùng hiện tại-2, thông tin QoS-2), tham số khác)). Theo cách này, chính sách bảo mật của DRB-2 được chỉnh sửa để đạt được mục đích sử dụng lại QoS.

Cách triển khai b2

Khi DRB lịch sử không thỏa mãn điều kiện thứ nhất tồn tại trên BS, nhưng ít nhất một DRB lịch sử thỏa mãn điều kiện thứ hai tồn tại trên BS, DRB đích là DRB thu được sau khi một trong ít nhất một DRB lịch sử thỏa mãn điều kiện thứ hai được cập nhật dựa trên chính sách bảo mật. QoS được hỗ trợ bởi mỗi DRB của ít nhất một DRB lịch sử thỏa mãn điều kiện thứ hai giống như QoS của phiên hiện tại, và chính sách bảo mật so khớp chính sách bảo mật được hỗ trợ bởi mỗi DRB; hoặc QoS được hỗ trợ bởi mỗi DRB của ít nhất một DRB lịch sử thỏa mãn điều kiện thứ hai so khớp QoS của phiên hiện tại, và chính sách bảo mật giống như chính sách bảo mật được hỗ trợ bởi mỗi DRB; hoặc QoS được hỗ trợ bởi mỗi DRB của ít nhất một DRB lịch sử thỏa mãn điều kiện thứ hai so khớp QoS của phiên hiện tại, và chính sách bảo mật so khớp chính sách bảo mật được hỗ trợ bởi mỗi DRB.

Một cách tùy chọn, điều kiện thứ hai bao gồm việc QoS được hỗ trợ so khớp QoS của phiên hiện tại, và việc chính sách bảo mật thu được giống như chính sách bảo mật được hỗ trợ. Theo cách khác, một cách tùy chọn, điều kiện thứ hai bao gồm việc QoS được hỗ trợ giống như QoS của phiên hiện tại, và chính sách bảo mật thu được so khớp chính sách bảo mật được hỗ trợ. Theo cách khác, một cách tùy chọn, điều kiện thứ hai bao gồm việc QoS được hỗ trợ so khớp QoS của phiên hiện tại, và chính sách bảo mật thu được so khớp chính sách bảo mật được hỗ trợ.

Tức là, các chính sách bảo mật tương ứng và QoS của DRB lịch sử được tìm thấy và DRB đích không hoàn toàn giống như mà hơi khác nhau. Chẳng

hạn, khác biệt giữa các yêu cầu băng thông trong khoảng định trước, sao cho DRB lịch sử có thể được sử dụng để chỉnh sửa ít nhất. Chẳng hạn, mối quan hệ giữa DRB thỏa mãn điều kiện thứ hai và DRB đích có thể thỏa mãn vấn đề sau: Bảo vệ mật mã hóa mặt phẳng người dùng mà không bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt cho DRB thỏa mãn điều kiện thứ hai; bảo vệ mật mã hóa mặt phẳng người dùng và bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt cho DRB đích; và thuật toán mật mã hóa mặt phẳng người dùng đích của DRB thỏa mãn điều kiện thứ hai giống như thuật toán mật mã hóa mặt phẳng người dùng đích của DRB đích. Trong trường hợp này, do tài nguyên của BS được giới hạn, DRB mới không thể được thiết lập; hoặc BS được thiết lập để tận dụng lại DRB lịch sử. Do vậy, BS gửi thông điệp tái cấu hình RRC trong nhiều lần và kích hoạt bảo vệ tính toàn vẹn.

Phương án thực hiện sáng chế đề xuất cách triển khai khả thi: Chẳng hạn, thông điệp được truyền bởi BS đến thiết bị đầu cuối trong lần thứ nhất là: thông điệp tái cấu hình RRC (thuật toán mật mã hóa mặt phẳng người dùng đích, DRB-1 (thông tin QoS-1), DRB-2 (thông tin QoS-2), tham số khác)); thông điệp được truyền bởi BS đến thiết bị đầu cuối trong lần thứ hai là: thông điệp tái cấu hình RRC (thuật toán mật mã hóa mặt phẳng người dùng hiện tại, DRB-1 (thông tin QoS-1), DRB-2 (thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích, thông tin QoS-2, thông tin QoS-3), tham số khác)). Theo cách này, tài nguyên của DRB-2 có thể được tận dụng lại. Chắc chắn là, có các cách triển khai cụ thể, và chỉ các ví dụ được nêu ở đây.

Cách triển khai b3

DRB được thiết lập trực tiếp dựa trên ít nhất một trong chính sách bảo mật hoặc QoS.

Cách triển khai b4

BS tiền cấu hình mối quan hệ liên kết giữa DRB, QoS, và chính sách bảo mật, và thiết lập ID tương ứng cho mỗi mối quan hệ liên kết, chẳng hạn, ID tiểu sử thuê bao cho công nghệ truy nhập vô tuyến (radio access technology, RAT)/độ ưu tiên tần số (Subscriber Profile ID for RAT/Frequency Priority, SPID). Tức là, bất kể cơ sở của một hoặc nhiều trong số ID phiên, IMSI, DNN,

và NSSAI, hoặc liệu việc tìm kiếm có được thực hiện trên UDM, UPF, và PCF, SMF thu được một SPID. Sau đó, SMF phát SPID đến RAN, và RAN có thể tìm thấy chính sách QoS định trước và chính sách bảo mật bằng cách sử dụng SPID. Trong trường hợp này, SMF không cần phát chính sách bảo mật bất kỳ, mà chỉ SPID. Sau đó, RAN có thể xác định DRB được sử dụng dựa trên SPID, và DRB được sử dụng thỏa mãn chính sách QoS và chính sách bảo mật.

Một cách tùy chọn, việc BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối bao gồm việc BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối bằng cách sử dụng báo hiệu RRC. Một cách tùy chọn, báo hiệu RRC bao gồm yêu cầu tái cấu hình RRC.

Một cách tùy chọn, nếu chính sách bảo mật chỉ báo rằng BS và thiết bị đầu cuối cần thương lượng thuật toán mật mã hóa mặt phẳng người dùng đích, BS còn cần gửi thuật toán mật mã hóa mặt phẳng người dùng đích đến thiết bị đầu cuối. Một cách tùy chọn, BS còn cần gửi độ dài khóa đến thiết bị đầu cuối. Nếu chính sách bảo mật chỉ báo rằng BS và thiết bị đầu cuối cần thương lượng thuật toán mật mã hóa mặt phẳng người dùng đích, độ dài khóa có thể bao gồm độ dài khóa mật mã hóa mặt phẳng người dùng. Nếu thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo BS kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối, độ dài khóa có thể bao gồm độ dài khóa bảo vệ tính toàn vẹn mặt phẳng người dùng. Một hoặc nhiều trong số thuật toán tính toàn vẹn mặt phẳng người dùng đích, thuật toán mật mã hóa mặt phẳng người dùng đích, độ dài khóa, và QoS có thể được gửi đến thiết bị đầu cuối bằng cách sử dụng một đoạn báo hiệu, chẳng hạn, yêu cầu tái cấu hình RRC.

Một cách tùy chọn, khi chính sách bảo mật còn bao gồm thông tin chỉ báo D - H, và thông tin chỉ báo D - H được sử dụng để chỉ báo BS để kích hoạt D-H cho thiết bị đầu cuối, BS gửi khóa liên quan D-H đến thiết bị đầu cuối. Ví dụ sau mô tả chi tiết quá trình trao đổi báo hiệu giữa BS và thiết bị đầu cuối nếu thông tin chỉ báo D - H được sử dụng để chỉ báo BS để kích hoạt D-H cho thiết bị đầu cuối.

Nếu chính sách trộn khóa được kích hoạt, BS lựa chọn, dựa trên khả năng

D-H được báo cáo bởi UE và khả năng D-H được phép bởi BS, khả năng D-H được phép bởi BS và có độ ưu tiên cao nhất. Ngoài ra, BS tạo khóa công khai P1 và khóa riêng tư B1 dựa trên khả năng D-H được lựa chọn. BS gửi khóa công khai P1 và khả năng D-H được lựa chọn đến thiết bị đầu cuối, chẳng hạn, có thể sử dụng thông điệp tái cấu hình RRC. Thiết bị đầu cuối tạo khóa công khai P2 và khóa riêng tư B2 dựa trên khả năng D-H được lựa chọn, và tạo khóa Kdh bằng cách sử dụng khóa riêng tư B2 và khóa công khai P1. Sau đó, Kdh và Kan được sử dụng cho việc trộn khóa. Phương pháp trộn có thể là New-Kan = KDF(Kdh, Kan, và tham số khác). Hàm dẫn xuất khóa (key derivation function, KDF) là hàm tạo khóa, chẳng hạn, thuật toán băm 256, và tham số khác có thể là tham số độ mới, chẳng hạn, PDCP COUNT. Kdh và Kan có thể được sử dụng trực tiếp để trộn khóa mà không sử dụng tham số khác. Sau khi trộn khóa, khóa mặt phẳng người dùng mới được tạo dựa trên New-Kan và thuật toán bảo mật đích mặt phẳng người dùng. Ngoài ra, khóa mặt phẳng người dùng mới được sử dụng để bảo vệ thông điệp tái cấu hình RRC, và sau đó thông điệp tái cấu hình RRC được gửi đến BS. Thông điệp tái cấu hình RRC bao gồm khóa công khai P2. Sau khi thu được khóa công khai P2, BS tạo New-Kan dựa trên khóa công khai P2 và khóa riêng tư B1 bằng cách sử dụng phương pháp tương tự như thiết bị đầu cuối, và còn sử dụng phương pháp tương tự như thiết bị đầu cuối để có khóa mặt phẳng người dùng mới. Ngoài ra, khóa mặt phẳng người dùng mới được sử dụng để kiểm chứng thông điệp tái cấu hình RRC. Nếu kiểm chứng thành công, BS bắt đầu kích hoạt khóa mặt phẳng người dùng mới.

Theo triển khai tùy chọn của phương án thực hiện được thể hiện trên Fig.2a hoặc Fig.2b, sau bước 213 trên Fig.2b, phương pháp còn bao gồm bước sau: BS nhận chính sách bảo mật hoặc ID của chính sách bảo mật, và BS có thể chọn một thuật toán bảo vệ mật mã hóa tính toàn vẹn người dùng trong chính sách bảo mật làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên thông tin được nêu trong chính sách bảo mật. Chính sách bảo mật có thể bao gồm một hoặc nhiều thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Theo cách khác, BS không thể sử dụng thuật toán bảo vệ tính toàn vẹn

mặt phẳng người dùng trong chính sách bảo mật làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Theo cách khác, khi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng trong chính sách bảo mật không trong danh sách của các thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, BS không sử dụng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng trong chính sách bảo mật làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Ngoài ra, một cách tùy chọn, khi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng trong chính sách bảo mật không được sử dụng làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích, nếu BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, BS có thể lựa chọn một trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng khác với thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng trong chính sách bảo mật làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Chẳng hạn, BS có thể lựa chọn một trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Trong ví dụ khác, nếu chính sách bảo mật được tiền tạo cấu hình trên BS, và BS không nhận chính sách bảo mật được phát bởi phần tử mạng khác, BS có thể lựa chọn thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên chính sách bảo mật được tiền tạo cấu hình trên BS. Chẳng hạn, chính sách bảo mật được tiền tạo cấu hình có thể bao gồm một hoặc nhiều thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng, và BS lựa chọn một thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng từ chính sách bảo mật được tiền tạo cấu hình làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Đối với nhiều cách triển khai khác, tham khảo nội dung nêu trên.

Một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng trong chính sách bảo mật có thể là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được bao gồm trong chính sách bảo mật được mô tả trong nội dung nêu trên và được phép bởi mạng phục vụ, hoặc có thể được xác định bởi thực thể SMF dựa trên ít nhất một trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán bảo vệ tính

toàn vẹn mặt phẳng người dùng được phép bởi BS. Chẳng hạn, thực thể SMF có thể xác định thuật toán thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Trong ví dụ khác, thực thể SMF có thể xác định thuật toán thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, mà cũng thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, và mà cũng thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích.

Chính sách bảo mật có thể bao gồm thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu, tức là, chính sách bảo mật có thể bao gồm thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Chẳng hạn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được bao gồm trong chính sách bảo mật cũng là thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu, tức là, thuật toán bảo vệ tính toàn vẹn được bao gồm trong chính sách bảo mật được sử dụng cho cả bảo vệ tính toàn vẹn mặt phẳng người dùng lẫn bảo vệ tính toàn vẹn mặt phẳng báo hiệu.

Chuyên gia trong lĩnh vực có thể biết rằng có nhiều cách triển khai lựa chọn thuật toán mật mã hóa mặt phẳng người dùng đích, thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích, và thuật toán mật mã hóa mặt phẳng báo hiệu đích bởi BS. Tham khảo phần mô tả giải pháp lựa chọn thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Phần sau mô tả vắn tắt vài cách triển khai.

Theo triển khai tùy chọn của phương án thực hiện được thể hiện trên Fig.2a hoặc Fig.2b, sau bước 213 trên Fig.2b, phương pháp còn bao gồm các bước sau: BS nhận chính sách bảo mật hoặc ID của chính sách bảo mật, và BS có thể lựa chọn một thuật toán mật mã hóa mặt phẳng người dùng trong chính sách bảo mật làm thuật toán mật mã hóa mặt phẳng người dùng đích dựa trên thông tin được nêu trong chính sách bảo mật. Chính sách bảo mật có thể bao gồm một hoặc nhiều thuật toán mật mã hóa mặt phẳng người dùng. Theo cách khác, BS

không thể sử dụng thuật toán mật mã hóa mặt phẳng người dùng trong chính sách bảo mật làm thuật toán mật mã hóa mặt phẳng người dùng đích. Theo cách khác, khi thuật toán mật mã hóa mặt phẳng người dùng trong chính sách bảo mật không trong danh sách các thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, BS không sử dụng thuật toán mật mã hóa mặt phẳng người dùng trong chính sách bảo mật làm thuật toán mật mã hóa mặt phẳng người dùng đích. Ngoài ra, một cách tùy chọn, khi thuật toán mật mã hóa mặt phẳng người dùng trong chính sách bảo mật không được sử dụng làm thuật toán mật mã hóa mặt phẳng người dùng đích, nếu BS kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, BS có thể lựa chọn một trong thuật toán mật mã hóa mặt phẳng người dùng khác với thuật toán mật mã hóa mặt phẳng người dùng trong chính sách bảo mật làm thuật toán mật mã hóa mặt phẳng người dùng đích. Chẳng hạn, BS có thể lựa chọn một trong thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS làm thuật toán mật mã hóa mặt phẳng người dùng đích. Đối với nhiều cách triển khai khác, tham khảo nội dung nêu trên.

Một cách tùy chọn, thuật toán mật mã hóa mặt phẳng người dùng trong chính sách bảo mật có thể là thuật toán mật mã hóa mặt phẳng người dùng được bao gồm trong chính sách bảo mật được mô tả trong nội dung nêu trên và được phép bởi mạng phục vụ, hoặc có thể được xác định bởi thực thể SMF dựa trên ít nhất một trong thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ, thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS. Chẳng hạn, thực thể SMF có thể xác định thuật toán thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, làm thuật toán mật mã hóa mặt phẳng người dùng đích. Trong ví dụ khác, thực thể SMF có thể xác định thuật toán thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, và mà cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi mạng phục vụ, làm thuật toán

mật mã hóa mặt phẳng người dùng đích.

Chính sách bảo mật có thể bao gồm thuật toán mật mã hóa mặt phẳng báo hiệu, tức là, chính sách bảo mật có thể bao gồm thuật toán mật mã hóa mặt phẳng báo hiệu và/hoặc thuật toán mật mã hóa mặt phẳng người dùng. Chẳng hạn, thuật toán mật mã hóa mặt phẳng người dùng được bao gồm trong chính sách bảo mật cũng là thuật toán mật mã hóa mặt phẳng báo hiệu, tức là, thuật toán mật mã hóa được bao gồm trong chính sách bảo mật được sử dụng cho cả bảo vệ mật mã hóa mặt phẳng người dùng lẫn bảo vệ mật mã hóa mặt phẳng báo hiệu.

Một cách tùy chọn, theo cách triển khai của phương án thực hiện được thể hiện trên Fig.2a, phương pháp được thể hiện trên Fig.2a còn bao gồm việc thiết bị đầu cuối thu được thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Cụ thể là, hai cách thức sau có thể được sử dụng:

Cách thức 1: Thiết bị đầu cuối nhận thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích được gửi bởi BS. Chẳng hạn, ở bước 223 trên Fig.2b, BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối, và một cách tương ứng, thiết bị đầu cuối nhận thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích được gửi bởi BS.

Cách thức 2: Thiết bị đầu cuối xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Chẳng hạn, thiết bị đầu cuối vẫn sử dụng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích được sử dụng trước đó. Trong ví dụ khác, thiết bị đầu cuối xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích (thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích có thể được gửi bởi BS đến thiết bị đầu cuối) làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Theo cách này, tính linh hoạt trong việc xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích bởi thiết bị đầu cuối có thể được cải thiện.

Ngoài ra, thiết bị đầu cuối có thể còn xác định thuật toán mật mã hóa mặt phẳng người dùng đích. Chẳng hạn, thiết bị đầu cuối vẫn sử dụng thuật toán mật mã hóa mặt phẳng người dùng đích được sử dụng trước đó. Trong ví dụ khác, thiết bị đầu cuối xác định thuật toán mật mã hóa mặt phẳng báo hiệu đích

làm thuật toán mật mã hóa mặt phẳng người dùng đích.

Theo cách triển khai của phương án thực hiện được thể hiện trên Fig.2, phương pháp được thể hiện trên Fig.2 còn bao gồm việc BS xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích và/hoặc thuật toán mật mã hóa mặt phẳng người dùng đích. Chẳng hạn, thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích trong thuật toán bảo vệ mặt phẳng đích được xác định ở bước 202 cũng có thể được sử dụng làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích, và thuật toán mật mã hóa mặt phẳng báo hiệu đích trong thuật toán bảo vệ mặt phẳng đích được xác định ở bước 202 cũng có thể được sử dụng làm thuật toán mật mã hóa mặt phẳng người dùng đích.

Một cách tùy chọn, theo cách triển khai của các phương án thực hiện được thể hiện trên Fig.2, Fig.2a, và Fig.2b, phương pháp còn bao gồm các bước sau:

BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc thiết bị đầu cuối và BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc thiết bị đầu cuối kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Phần sau mô tả bằng cách sử dụng BS làm ví dụ để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng hoặc kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Chẳng hạn, khi điều kiện để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bởi BS được thỏa mãn, BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Điều kiện để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bởi BS có thể như sau: BS nhận thông điệp mặt phẳng người dùng định trước thứ nhất, chẳng hạn thông điệp chấp nhận thiết lập phiên; hoặc BS nhận thông tin mặt phẳng người dùng, chẳng hạn ID phiên hoặc tiểu sử QoS, trong đó thông tin mặt phẳng người dùng có thể được định trước thông tin mặt phẳng người dùng, chẳng hạn ID phiên định trước hoặc tiểu sử QoS định trước, và ID phiên định trước có thể là ID phiên cụ thể; hoặc BS đang phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối hoặc phân phối lại tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, chẳng hạn, BS nhận thông điệp yêu cầu phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, và nếu BS đang

phân phối lại tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, và tham số vận hành mạng thỏa mãn điều kiện cho phép mạng định trước, BS có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc chính sách bảo mật được nhận bởi BS bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc BS nhận loại dịch vụ phiên định trước. Chẳng hạn, chính sách bảo mật được tiền tạo cấu hình có thể bao gồm mối quan hệ liên kết giữa loại dịch vụ phiên định trước và kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Bảo vệ tính toàn vẹn mặt phẳng người dùng có thể được kích hoạt khi loại dịch vụ phiên định trước được nhận.

Khi điều kiện để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bởi BS được thỏa mãn, đối với vài cách triển khai cụ thể trong đó BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, tham khảo cách triển khai c1-a1 đến cách triển khai c1-a7 sau.

Cách triển khai c1-a1

Chẳng hạn, khi nhận thông điệp mặt phẳng người dùng định trước thứ nhất trong chu kỳ thời gian định trước, BS có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, và thông điệp mặt phẳng người dùng định trước thứ nhất có thể là thông điệp chấp nhận thiết lập phiên.

Chẳng hạn, nếu BS nhận thông điệp chấp nhận thiết lập phiên (cũng có thể được gọi là hoàn thành thiết lập phiên) trong chu kỳ thời gian định trước, chỉ báo rằng BS đang trong thủ tục thiết lập phiên, và để cải thiện bảo mật báo hiệu mặt phẳng người dùng, bảo vệ tính toàn vẹn mặt phẳng người dùng có thể được kích hoạt.

Cách triển khai c1-a2

Khi nhận thông tin mặt phẳng người dùng trong chu kỳ thời gian định trước, BS có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, và thông tin mặt phẳng người dùng có thể là ID phiên hoặc tiểu sử QoS định trước.

Chẳng hạn, nếu BS nhận ID phiên bất kỳ hoặc tiểu sử QoS bất kỳ (một cách tùy chọn, có thể được nhận từ giao diện N2, hoặc có thể thu được trực tiếp từ

phía thiết bị đầu cuối) trong chu kỳ thời gian định trước, BS hiện đang trong thủ tục thiết lập phiên và kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Một cách tùy chọn, bảo vệ mặt phẳng báo hiệu cũng có thể được kích hoạt.

Một cách tùy chọn, kích hoạt bảo vệ mặt phẳng báo hiệu có thể là ít nhất một trong kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu và kích hoạt bảo vệ mật mã hóa mặt phẳng báo hiệu. Phần mô tả trong đoạn này áp dụng được nêu theo tất cả các phương án thực hiện sáng chế, và không được nêu thêm ở nội dung sau.

Cách triển khai c1-a3

Khi nhận thông tin mặt phẳng người dùng định trước trong chu kỳ thời gian định trước, BS có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Thông tin mặt phẳng người dùng định trước có thể là ID phiên định trước hoặc tiểu sử QoS định trước. Mối quan hệ liên kết giữa thông tin mặt phẳng người dùng định trước và liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng được thiết lập trước trên BS, và mối quan hệ liên kết giữa thông tin mặt phẳng người dùng định trước và liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng có thể được sử dụng làm một phần của chính sách bảo mật được tiền tạo cấu hình trên BS.

Chẳng hạn, mối quan hệ liên kết giữa liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và ID phiên được thiết lập. Do vậy, nếu BS nhận ID phiên định trước trong chu kỳ thời gian định trước, BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. ID phiên định trước tương ứng với kích hoạt của bảo vệ tính toàn vẹn mặt phẳng người dùng trong mối quan hệ liên kết giữa liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và ID phiên.

Trong ví dụ khác, mối quan hệ liên kết giữa liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và tiểu sử QoS được thiết lập. Do vậy, nếu BS nhận tiểu sử QoS định trước trong chu kỳ thời gian định trước, BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. ID phiên định trước tương ứng với việc kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng trong mối quan hệ liên kết giữa liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và ID phiên.

Ngoài ra, mối quan hệ liên kết giữa liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và ID phiên có thể được định trước trên BS, or BS có thể nhận mối quan hệ liên kết được cập nhật được gửi bởi phần tử mạng khác. Một cách tùy chọn, BS có thể xác định, dựa trên mối quan hệ liên kết định trước và mối quan hệ liên kết được cập nhật, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Chẳng hạn, khi bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt trong lần thứ nhất, liệu có kích hoạt bảo vệ tính toàn vẹn người dùng có thể được xác định dựa trên mối quan hệ liên kết định trước. Khi mối quan hệ liên kết được cập nhật tồn tại sau đó, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng hay không cũng có thể được xác định chỉ dựa trên mối quan hệ liên kết mới nhất. Việc xác định toàn diện có thể còn được thực hiện kết hợp với mối quan hệ liên kết định trước cụ thể, mối quan hệ liên kết được cập nhật, và trạng thái tải mạng. Chẳng hạn, nếu BS phân phối lại tài nguyên tới phiên do quá tải, bảo vệ tính toàn vẹn mặt phẳng người dùng ban đầu được kích hoạt cho phiên được vô hiệu hóa trong quá trình phân phối lại tài nguyên đến phiên.

Cách triển khai c1-a4

Nếu BS đang phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối hoặc phân phối lại tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, BS có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Chẳng hạn, khi BS nhận, trong chu kỳ thời gian định trước, thông điệp yêu cầu phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, BS phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối hoặc phân phối lại tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, và thủ tục liên quan đến báo hiệu mặt phẳng người dùng. Để cỉa thiện bảo mật của báo hiệu mặt phẳng người dùng, bảo vệ tính toàn vẹn mặt phẳng người dùng có thể được kích hoạt.

Cách triển khai c1-a5

Nếu BS đang phân phối lại tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, và tham số vận hành mạng thỏa mãn điều kiện cho phép mạng định trước, BS có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Tham số vận hành mạng bao gồm lượng tải mạng và/hoặc tỷ lệ tổn hao gói.

Nên lưu ý rằng, trong quá trình phân phối lại tài nguyên đến phiên bởi BS, hai cách triển khai tùy chọn sau có thể được sử dụng:

Cách thức 1: Giải pháp bảo mật mặt phẳng người dùng tương ứng với tài nguyên trước đó được phân phối đến phiên của thiết bị đầu cuối vẫn được sử dụng. Chẳng hạn, tài nguyên trước đó được phân phối đến phiên của thiết bị đầu cuối tương ứng với kích hoạt của bảo vệ tính toàn vẹn mặt phẳng người dùng, và tài nguyên được phân phối lại tương ứng với phiên của thiết bị đầu cuối cũng tương ứng với kích hoạt của bảo vệ tính toàn vẹn mặt phẳng người dùng.

Cách thức 2: Giải pháp bảo mật mặt phẳng người dùng tương ứng với tài nguyên được phân phối lại tương ứng với phiên được xác định lại dựa trên trạng thái của BS. Chẳng hạn, trạng thái của BS thể hiện rằng tỷ lệ tổn hao gói của phiên quá cao. Do bảo vệ tính toàn vẹn mặt phẳng người dùng có thể tăng tỷ lệ tổn hao gói, bảo vệ tính toàn vẹn mặt phẳng người dùng được vô hiệu hóa trong quá trình phân phối lại tài nguyên đến phiên. Trong ví dụ khác, nếu BS phân phối lại tài nguyên đến phiên do quá tải, trong quá trình phân phối lại tài nguyên đến phiên, bảo vệ tính toàn vẹn mặt phẳng người dùng ban đầu được kích hoạt cho phiên được vô hiệu hóa.

Rõ ràng, hai cách triển khai tùy chọn nêu trên có thể được kết hợp. Chẳng hạn, nếu BS phân phối lại tài nguyên đến phiên, và trạng thái của BS là bình thường, bảo vệ tính toàn vẹn mặt phẳng người dùng được giữ kích hoạt; hoặc nếu trạng thái của BS là không bình thường, chẳng hạn, BS phân phối lại tài nguyên đến phiên do quá tải, bảo vệ tính toàn vẹn mặt phẳng người dùng được vô hiệu hóa nếu bảo vệ tính toàn vẹn mặt phẳng người dùng ban đầu được kích hoạt cho phiên. Trong ví dụ khác, tỷ lệ tổn hao gói của phiên quá cao, và do vậy tài nguyên được phân phối lại cho phiên. Do bảo vệ tính toàn vẹn mặt phẳng người dùng có thể tăng tỷ lệ tổn hao gói, bảo vệ tính toàn vẹn mặt phẳng người dùng được vô hiệu hóa. Một cách tùy chọn, trường hợp này có thể được tiền tạo cấu hình trên BS như là một phần chính sách bảo mật (chính sách bảo mật được tiền tạo cấu hình trên BS cũng có thể là chính sách bảo mật được tiền tạo cấu hình trên BS trong nội dung nêu trên).

Cách triển khai c1-a6

Nếu chính sách bảo mật được nhận bởi BS bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, BS có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Một cách tùy chọn, thông tin chỉ báo bảo vệ tính toàn vẹn có thể là ID của thuật toán bảo vệ tính toàn vẹn, bit thông tin chỉ báo, hoặc thông tin định trước. Chẳng hạn, thông tin chỉ báo bảo vệ tính toàn vẹn có thể được gửi bởi thực thể SMF. Khi xác định rằng điều kiện bảo vệ tính toàn vẹn mặt phẳng người dùng của thực thể SMF được thỏa mãn, thực thể SMF gửi thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Có thể có nhiều cách triển khai trong đó thực thể SMF xác định rằng điều kiện bảo vệ tính toàn vẹn mặt phẳng người dùng của thực thể SMF được thỏa mãn, hoặc tham khảo cách triển khai của BS được mô tả trong cách triển khai c1-a1 đến cách triển khai c1-a5.

Cách triển khai c1-a7

Chính sách bảo mật có thể được tiền tạo cấu hình trên BS, và chính sách bảo mật được tiền tạo cấu hình có thể bao gồm mối quan hệ liên kết giữa loại dịch vụ phiên định trước và kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Điều kiện kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bởi BS có thể là việc chính sách bảo mật được tiền tạo cấu hình trên BS bao gồm loại dịch vụ phiên định trước. Chẳng hạn, chính sách bảo mật được tiền tạo cấu hình có thể bao gồm mối quan hệ liên kết giữa loại dịch vụ phiên định trước và kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Khi loại dịch vụ phiên định trước được nhận, bảo vệ tính toàn vẹn mặt phẳng người dùng có thể được kích hoạt. Một cách tùy chọn, nếu BS không nhận chính sách bảo mật được gửi bởi phần tử mạng, chính sách bảo mật được tiền tạo cấu hình trên BS có thể được sử dụng.

Chẳng hạn, chính sách bảo mật được tiền tạo cấu hình trên BS có thể được xác định trong chiều của dữ liệu mặt phẳng người dùng (chẳng hạn, loại dịch vụ). Chẳng hạn, được xác định trong chính sách bảo mật được tiền tạo cấu hình trên BS rằng bảo vệ tính toàn vẹn mặt phẳng người dùng không được kích hoạt

cho thủ tục tương ứng với dịch vụ VoIP. Do vậy, khi xác định rằng phiên hiện tại tương ứng với dịch vụ VoIP, BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Ngoài ra, chính sách bảo mật có thể được tiền tạo cấu hình trên BS, hoặc chính sách bảo mật được cập nhật được gửi bởi phần tử mạng khác và được nhận bởi BS. Một cách tùy chọn, BS có thể xác định, dựa trên chính sách bảo mật được tiền tạo cấu hình và chính sách bảo mật được cập nhật, liệu có kích hoạt bảo vệ tính toàn vẹn người dùng. Chẳng hạn, khi bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt trong lần thứ nhất, liệu có kích hoạt bảo vệ tính toàn vẹn người dùng có thể được xác định dựa trên chính sách bảo mật được tiền tạo cấu hình. Khi chính sách bảo mật được cập nhật tồn tại sau đó, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng cũng có thể được xác định chỉ dựa trên chính sách bảo mật mới nhất. Việc xác định toàn diện có thể còn được thực hiện kết hợp với chính sách bảo mật được tiền tạo cấu hình cụ thể, chính sách bảo mật được cập nhật, và trạng thái tải mạng. Chẳng hạn, nếu BS phân phối lại tài nguyên đến phiên do quá tải, bảo vệ tính toàn vẹn mặt phẳng người dùng ban đầu được kích hoạt cho phiên được vô hiệu hóa trong quá trình phân phối lại tài nguyên đến phiên.

Ngoài ra, một cách tùy chọn, phương pháp còn bao gồm việc BS gửi thông tin chỉ báo bảo vệ tính toàn vẹn đến thiết bị đầu cuối, trong đó thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo đến kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Thông tin chỉ báo bảo vệ tính toàn vẹn có thể là thông tin chỉ báo bảo vệ tính toàn vẹn được bao gồm trong chính sách bảo mật được nhận bởi BS.

Một cách tùy chọn, theo cách triển khai khác của phương án thực hiệns được thể hiện trên Fig.2, Fig.2a, và Fig.2b, phương pháp còn bao gồm các bước sau:

BS kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng; hoặc thiết bị đầu cuối và BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc thiết bị đầu cuối kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Chẳng hạn, khi điều kiện để kích hoạt bảo vệ mật mã hóa mặt phẳng người

dùng bởi BS được thỏa mãn, BS kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Điều kiện để kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng bởi BS có thể như sau: BS nhận thông điệp mặt phẳng người dùng định trước thứ nhất, chẳng hạn thông điệp chấp nhận thiết lập phiên; hoặc BS nhận thông tin mặt phẳng người dùng, chẳng hạn ID phiên hoặc tiểu sử QoS. Thông tin mặt phẳng người dùng có thể được định trước thông tin mặt phẳng người dùng, chẳng hạn ID phiên định trước hoặc tiểu sử QoS định trước, và ID phiên định trước có thể là ID phiên cụ thể; hoặc BS đang phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối hoặc phân phối lại tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, chẳng hạn, BS nhận thông điệp yêu cầu phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối; hoặc chính sách bảo mật được nhận bởi BS bao gồm thông tin chỉ báo mật mã hóa, và thông tin chỉ báo mật mã hóa chỉ báo để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc BS nhận loại dịch vụ phiên định trước. Chẳng hạn, chính sách bảo mật được tiền tạo cấu hình có thể bao gồm mối quan hệ liên kết giữa loại dịch vụ phiên định trước và kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Bảo vệ mật mã hóa mặt phẳng người dùng có thể được kích hoạt khi loại dịch vụ phiên định trước được nhận; hoặc bảo vệ mật mã hóa mặt phẳng người dùng có thể được kích hoạt khi bảo vệ mặt phẳng báo hiệu được kích hoạt.

Ngoài ra, một cách tùy chọn, phương pháp còn bao gồm việc BS gửi thông tin chỉ báo mật mã hóa đến thiết bị đầu cuối. Thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Thông tin chỉ báo mật mã hóa có thể là thông tin chỉ báo mật mã hóa được bao gồm trong chính sách bảo mật được nhận bởi BS.

Khi điều kiện để kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng bởi BS được thỏa mãn, đối với vài cách triển khai cụ thể trong đó BS kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, tham khảo cách triển khai c1-b1 đến cách triển khai c1-b8 sau.

Cách triển khai c1-b1

Chẳng hạn, khi nhận thông điệp mặt phẳng người dùng định trước thứ nhất

trong chu kỳ thời gian định trước, BS có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, và thông điệp mặt phẳng người dùng định trước thứ nhất có thể là thông điệp chấp nhận thiết lập phiên.

Chẳng hạn, nếu BS nhận thông điệp chấp nhận thiết lập phiên (cũng có thể được gọi là hoàn thành thiết lập phiên) trong chu kỳ thời gian định trước, chỉ báo rằng BS đang trong thủ tục thiết lập phiên, và để cải thiện bảo mật báo hiệu mặt phẳng người dùng, bảo vệ mật mã hóa mặt phẳng người dùng có thể được kích hoạt.

Cách triển khai c1-b2

Khi nhận thông tin mặt phẳng người dùng trong chu kỳ thời gian định trước, BS có thể kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, và thông tin mặt phẳng người dùng có thể là ID phiên hoặc tiểu sử QoS định trước.

Chẳng hạn, nếu BS nhận ID phiên bất kỳ hoặc tiểu sử QoS bất kỳ (Một cách tùy chọn, có thể được nhận từ giao diện N2, hoặc có thể thu được ngay từ phía thiết bị đầu cuối) trong chu kỳ thời gian định trước, BS đang trong thủ tục thiết lập phiên và kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Một cách tùy chọn, bảo vệ mặt phẳng báo hiệu cũng có thể được kích hoạt.

Một cách tùy chọn, kích hoạt bảo vệ mặt phẳng báo hiệu có thể là ít nhất một của kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu và kích hoạt bảo vệ mật mã hóa mặt phẳng báo hiệu. Phần mô tả trong đoạn này áp dụng được cho tất cả các phương án thực hiện sáng chế, và không được nêu thêm trong nội dung sau.

Cách triển khai c1-b3

Khi nhận thông tin mặt phẳng người dùng định trước trong chu kỳ thời gian định trước, BS có thể kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Thông tin mặt phẳng người dùng định trước có thể là ID phiên định trước hoặc tiểu sử QoS định trước. Mối quan hệ liên kết giữa thông tin mặt phẳng người dùng định trước và liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng được định trước trên BS, và mối quan hệ liên kết giữa thông tin mặt phẳng người dùng định trước và liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng có thể được sử dụng làm một phần chính sách bảo mật được tiền tạo cấu

hình trên BS.

Chẳng hạn, mối quan hệ liên kết giữa liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng và ID phiên được thiết lập. Do vậy, nếu BS nhận ID phiên định trước trong chu kỳ thời gian định trước, BS kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. ID phiên định trước tương ứng với kích hoạt của bảo vệ mật mã hóa mặt phẳng người dùng trong mối quan hệ liên kết giữa liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng và ID phiên.

Trong ví dụ khác, mối quan hệ liên kết giữa liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng và tiểu sử QoS được thiết lập. Do vậy, nếu BS nhận tiểu sử QoS định trước trong chu kỳ thời gian định trước, BS kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Tiểu sử QoS định trước tương ứng với kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng trong mối quan hệ liên kết giữa liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng và ID phiên.

Ngoài ra, mối quan hệ liên kết giữa liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng và ID phiên có thể được định trước trên BS, hoặc BS có thể nhận mối quan hệ liên kết được cập nhật được gửi bởi phần tử mạng khác. Một cách tùy chọn, BS có thể xác định, dựa trên mối quan hệ liên kết định trước và mối quan hệ liên kết được cập nhật, liệu có kích hoạt bảo vệ mật mã hóa người dùng. Chẳng hạn, khi bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt trong lần thứ nhất, liệu có kích hoạt bảo vệ mật mã hóa người dùng có thể được xác định dựa trên mối quan hệ liên kết định trước. Khi mối quan hệ liên kết được cập nhật tồn tại tiếp theo, liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng cũng có thể được xác định chỉ dựa trên mối quan hệ liên kết mới nhất. Việc xác định toàn diện có thể còn được thực hiện kết hợp với mối quan hệ liên kết định trước cụ thể, mối quan hệ liên kết được cập nhật, và trạng thái tải mạng. Chẳng hạn, nếu BS phân phối lại tài nguyên đến phiên do quá tải, bảo vệ mật mã hóa mặt phẳng người dùng ban đầu được kích hoạt cho phiên được vô hiệu hóa trong quá trình phân phối lại tài nguyên đến phiên.

Cách triển khai c1-b4

Nếu BS đang phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu

cuối hoặc phân phối lại tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, BS có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Chẳng hạn, khi BS nhận, trong chu kỳ thời gian định trước, thông điệp yêu cầu phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, BS phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối hoặc phân phối lại tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, và thủ tục này liên quan đến báo hiệu mặt phẳng người dùng. Để cải thiện bảo mật của báo hiệu mặt phẳng người dùng, bảo vệ mật mã hóa mặt phẳng người dùng có thể được kích hoạt.

Cách triển khai c1-b5

Nếu BS đang phân phối lại tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, và tham số vận hành mạng thỏa mãn điều kiện cho phép mạng định trước, BS có thể kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Tham số vận hành mạng bao gồm lượng tải mạng và/hoặc tỷ lệ tổn hao gói.

Nên lưu ý rằng, trong quá trình phân phối lại tài nguyên đến phiên bởi BS, hai cách triển khai tùy chọn sau có thể được sử dụng:

Cách 1: Giải pháp bảo mật mặt phẳng người dùng tương ứng với tài nguyên trước đó được phân phối đến phiên của thiết bị đầu cuối vẫn được sử dụng. Chẳng hạn, tài nguyên trước đó được phân phối đến phiên của thiết bị đầu cuối tương ứng với kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, và tài nguyên được phân phối lại tương ứng với phiên của thiết bị đầu cuối cũng tương ứng với kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Cách 2: giải pháp bảo mật mặt phẳng người dùng tương ứng với tài nguyên được phân phối lại tương ứng với phiên được xác định lại dựa trên trạng thái của BS. Chẳng hạn, trạng thái của BS thể hiện rằng tỷ lệ tổn hao gói của phiên là quá cao. Do bảo vệ mật mã hóa mặt phẳng người dùng có thể tăng tỷ lệ tổn hao gói, bảo vệ mật mã hóa mặt phẳng người dùng được vô hiệu hóa trong quá trình phân phối lại tài nguyên đến phiên. Trong ví dụ khác, nếu BS phân phối lại tài nguyên đến phiên do quá tải, trong quá trình phân phối lại tài nguyên đến phiên, bảo vệ mật mã hóa mặt phẳng người dùng ban đầu được kích hoạt cho phiên được vô hiệu hóa.

Rõ ràng, hai cách triển khai sau có thể được kết hợp. Chẳng hạn, nếu BS phân phối lại tài nguyên đến phiên, và trạng thái của BS là bình thường, bảo vệ mật mã hóa mặt phẳng người dùng được giữ kích hoạt; hoặc nếu trạng thái của BS là không bình thường, chẳng hạn, BS phân phối lại tài nguyên đến phiên do quá tải, bảo vệ mật mã hóa mặt phẳng người dùng được vô hiệu hóa nếu bảo vệ mật mã hóa mặt phẳng người dùng ban đầu được kích hoạt cho phiên. Trong ví dụ khác, tỷ lệ tổn hao gói của phiên quá cao, và do vậy tài nguyên được phân phối lại cho phiên. Do bảo vệ mật mã hóa mặt phẳng người dùng có thể tăng tỷ lệ tổn hao gói, bảo vệ mật mã hóa mặt phẳng người dùng được vô hiệu hóa. Một cách tùy chọn, trường hợp này có thể được tiền tạo cấu hình trên BS như là một phần chính sách bảo mật (chính sách bảo mật được tiền tạo cấu hình trên BS cũng có thể là chính sách bảo mật được tiền tạo cấu hình trên BS trong nội dung nêu trên).

Cách triển khai c1-b6

Nếu chính sách bảo mật được nhận bởi BS bao gồm thông tin chỉ báo bảo vệ mật mã hóa, và thông tin chỉ báo bảo vệ mật mã hóa chỉ báo để kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, BS có thể kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Một cách tùy chọn, thông tin chỉ báo bảo vệ mật mã hóa có thể là ID của thuật toán mật mã hóa, bit thông tin chỉ báo, hoặc thông tin định trước. Chẳng hạn, thông tin chỉ báo bảo vệ mật mã hóa có thể được gửi bởi thực thể SMF. Khi xác định rằng điều kiện bảo vệ mật mã hóa mặt phẳng người dùng của thực thể SMF được thỏa mãn, thực thể SMF gửi thông tin chỉ báo bảo vệ mật mã hóa chỉ báo để kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Có thể có nhiều cách triển khai trong đó thực thể SMF xác định rằng điều kiện bảo vệ mật mã hóa mặt phẳng người dùng của thực thể SMF được thỏa mãn, hoặc tham khảo cách triển khai của BS được mô tả trong cách triển khai c1-b1 đến cách triển khai c1-b5.

Cách triển khai c1-b7

Chính sách bảo mật có thể được tiền tạo cấu hình trên BS, và chính sách bảo mật được tiền tạo cấu hình có thể bao gồm mối quan hệ liên kết giữa loại dịch vụ phiên định trước và kích hoạt bảo vệ mật mã hóa mặt phẳng người

dùng. Điều kiện kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng bởi BS có thể là loại dịch vụ phiên định trước được bao gồm trong chính sách bảo mật được tiền tạo cấu hình trên BS. Chẳng hạn, chính sách bảo mật được tiền tạo cấu hình có thể bao gồm mối quan hệ liên kết giữa loại dịch vụ phiên định trước và kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Khi loại dịch vụ phiên định trước được nhận, bảo vệ mật mã hóa mặt phẳng người dùng có thể được kích hoạt. Một cách tùy chọn, nếu BS không nhận chính sách bảo mật được gửi bởi phần tử mạng, chính sách bảo mật được tiền tạo cấu hình trên BS có thể được sử dụng.

Chẳng hạn, chính sách bảo mật được tiền tạo cấu hình trên BS có thể được xác định theo chiều của dữ liệu mặt phẳng người dùng (chẳng hạn, loại dịch vụ). Chẳng hạn, được xác định trong chính sách bảo mật được tiền tạo cấu hình trên BS mà bảo vệ mật mã hóa mặt phẳng người dùng không được kích hoạt đối với thủ tục tương ứng với dịch vụ VoIP. Do vậy, khi xác định rằng phiên hiện tại tương ứng với dịch vụ VoIP, BS không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Ngoài ra, chính sách bảo mật có thể được tiền tạo cấu hình trên BS, hoặc có thể là chính sách bảo mật cập nhật được gửi bởi phần tử mạng khác và được nhận bởi BS. Một cách tùy chọn, BS có thể xác định, dựa trên chính sách bảo mật được tiền tạo cấu hình và chính sách bảo mật được cập nhật, liệu có kích hoạt bảo vệ mật mã hóa người dùng. Chẳng hạn, khi bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt trong lần thứ nhất, liệu có kích hoạt bảo vệ mật mã hóa người dùng có thể được xác định dựa trên chính sách bảo mật được tiền tạo cấu hình. Khi chính sách bảo mật cập nhật tồn tại tiếp theo, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng cũng có thể được xác định chỉ dựa trên chính sách bảo mật mới nhất. Việc xác định toàn diện có thể còn được thực hiện kết hợp với chính sách bảo mật được tiền tạo cấu hình cụ thể, chính sách bảo mật cập nhật, và trạng thái tải mạng. Chẳng hạn, nếu BS phân phối lại tài nguyên đến phiên do quá tải, bảo vệ mật mã hóa mặt phẳng người dùng ban đầu được kích hoạt cho phiên được vô hiệu hóa trong quá trình phân phối lại tài nguyên đến phiên.

Cách triển khai c1-b8

Khi kích hoạt bảo vệ mặt phẳng báo hiệu (kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc bảo vệ mật mã hóa mặt phẳng báo hiệu), BS cũng có thể kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Chẳng hạn, theo cách triển khai được thể hiện trên Fig.2, sau bước 202, cách triển khai tùy chọn còn được bao gồm: Khi kích hoạt bảo vệ mặt phẳng báo hiệu, BS cũng kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Theo triển khai này, nếu thiết bị đầu cuối và BS có thể bảo vệ mặt phẳng báo hiệu, và do việc không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và bảo vệ mật mã hóa mặt phẳng người dùng, khi bảo vệ tính toàn vẹn mặt phẳng người dùng và bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt, trạng thái kích hoạt bảo vệ mặt phẳng báo hiệu có thể được duy trì. Theo triển khai này, BS có thể gửi thông tin chỉ báo bảo vệ tính toàn vẹn và thông tin chỉ báo mật mã hóa đến thiết bị đầu cuối. Theo cách này, một mặt, thiết bị đầu cuối có thể duy trì trạng thái được kích hoạt của bảo vệ mặt phẳng báo hiệu hiện tại (chẳng hạn, nếu thiết bị đầu cuối kích hoạt trước đó bảo vệ tính toàn vẹn mặt phẳng báo hiệu mà không bảo vệ mật mã hóa mặt phẳng báo hiệu, trạng thái của kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu mà không bảo vệ mật mã hóa mặt phẳng báo hiệu được duy trì). Nói theo cách khác, thiết bị đầu cuối kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng dựa trên thông tin chỉ báo bảo vệ tính toàn vẹn, và kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng dựa trên thông tin chỉ báo mật mã hóa.

Theo triển khai tùy chọn khác, nếu thiết bị đầu cuối và BS có thể bảo vệ mặt phẳng báo hiệu, và kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng mà không bảo vệ tính toàn vẹn mặt phẳng người dùng, khi bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt, BS có thể gửi, đến thiết bị đầu cuối, chỉ thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Một mặt, thiết bị đầu cuối có thể duy trì trạng thái được kích hoạt của bảo vệ mặt phẳng báo hiệu hiện tại (chẳng hạn, nếu thiết bị đầu cuối kích hoạt trước đó bảo vệ tính toàn vẹn mặt phẳng báo hiệu mà không bảo vệ mật mã hóa mặt phẳng báo hiệu, trạng thái của kích hoạt bảo

vệ tính toàn vẹn mặt phẳng báo hiệu mà không bảo vệ mật mã hóa mặt phẳng báo hiệu được duy trì). Nói theo cách khác, thiết bị đầu cuối kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng dựa trên thông tin chỉ báo bảo vệ tính toàn vẹn, và liên tục kích hoạt bảo vệ mật mã hóa. Theo triển khai tùy chọn khác, thông tin chỉ báo mật mã hóa có thể được truyền lại để chỉ báo để kích hoạt liên tục bảo vệ tính toàn vẹn mặt phẳng người dùng.

Phần sau mô tả bằng cách sử dụng thiết bị đầu cuối làm ví dụ để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng hoặc kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Khi điều kiện kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bởi thiết bị đầu cuối được thỏa mãn, thiết bị đầu cuối kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Điều kiện để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bởi thiết bị đầu cuối có thể như sau: Thiết bị đầu cuối nhận thông tin chỉ báo bảo vệ tính toàn vẹn được gửi bởi BS, và thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo đến kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc thiết bị đầu cuối gửi thông điệp mặt phẳng người dùng định trước thứ hai, chẳng hạn, thông điệp yêu cầu thiết lập phiên.

Khi điều kiện để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bởi thiết bị đầu cuối được thỏa mãn, đối với vài cách triển khai cụ thể trong đó thiết bị đầu cuối kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, tham khảo cách triển khai c1-c1 và cách triển khai c1-c2 sau.

Cách triển khai c1-c1

Theo triển khai tùy chọn của phương án thực hiệns được thể hiện trên Fig.2a và Fig.2b, sau bước 211, phương pháp còn bao gồm việc BS gửi thông tin chỉ báo bảo vệ tính toàn vẹn đến thiết bị đầu cuối, trong đó thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Thông tin chỉ báo bảo vệ tính toàn vẹn có thể là thông tin chỉ báo bảo vệ tính toàn vẹn được bao gồm trong chính sách bảo mật thu được bởi BS ở bước 221 trên Fig.2b, hoặc có thể được xác định bởi BS theo cách bất kỳ trong các cách triển khai nêu trên từ c1-a1 đến c1-a7.

Khi thiết bị đầu cuối nhận thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo để kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, thiết bị đầu cuối có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Cách triển khai c1-c2

Chẳng hạn, thiết bị đầu cuối gửi thông điệp yêu cầu thiết lập phiên trong chu kỳ thời gian định trước, và thiết bị đầu cuối đang trong thủ tục thiết lập phiên. Trong trường hợp này, để cải thiện bảo mật mặt phẳng người dùng, thiết bị đầu cuối có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Ngoài ra, một cách tùy chọn, nếu thiết bị đầu cuối sử dụng cách triển khai c1-c2, và thiết bị đầu cuối còn nhận thông tin chỉ báo bảo vệ tính toàn vẹn, nếu có xung đột giữa cách triển khai c1-c2 và thông tin chỉ báo bảo vệ tính toàn vẹn, thiết bị đầu cuối xác định, dựa trên thông tin chỉ báo bảo vệ tính toàn vẹn được nhận, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Theo triển khai tùy chọn của các phương án thực hiện được thể hiện trên Fig.2a và Fig.2b, sau bước 211, phương pháp còn bao gồm việc BS gửi thông tin chỉ báo mật mã hóa đến thiết bị đầu cuối, trong đó thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Thông tin chỉ báo mật mã hóa có thể là thông tin chỉ báo mật mã hóa được bao gồm trong chính sách bảo mật thu được bởi BS ở bước 221 trên Fig.2b, hoặc có thể được xác định bởi BS theo một trong của các cách triển khai nêu trên từ c1-a1 đến c1-a7.

Chẳng hạn, khi thiết bị đầu cuối nhận thông tin chỉ báo mật mã hóa, và thông tin chỉ báo mật mã hóa chỉ báo để kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, thiết bị đầu cuối có thể kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Chẳng hạn, khi gửi thông điệp mặt phẳng người dùng định trước thứ hai trong chu kỳ thời gian định trước, thiết bị đầu cuối có thể kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Chẳng hạn, thiết bị đầu cuối gửi thông điệp yêu cầu thiết lập phiên trong chu kỳ thời gian định trước, và thiết bị đầu cuối đang trong thủ tục thiết lập phiên. Trong trường hợp này, để cải thiện bảo mật mặt

phẳng người dùng, thiết bị đầu cuối có thể kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Ngoài ra, một cách tùy chọn, nếu thiết bị đầu cuối sử dụng cách triển khai c1-c2, và thiết bị đầu cuối còn nhận thông tin chỉ báo mật mã hóa, nếu có xung đột giữa cách triển khai c1-c2 và thông tin chỉ báo mật mã hóa, thiết bị đầu cuối xác định, dựa trên thông tin chỉ báo mật mã hóa được nhận, liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Trong ví dụ khác, khi kích hoạt bảo vệ mặt phẳng báo hiệu (kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc bảo vệ mật mã hóa mặt phẳng báo hiệu), thiết bị đầu cuối cũng có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Chẳng hạn, theo cách triển khai được thể hiện trên Fig.2, giữa bước 203 và bước 204, phương pháp còn bao gồm việc khi kích hoạt bảo vệ mặt phẳng báo hiệu, BS cũng có thể kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Thiết bị đầu cuối có thể xác định, dựa trên việc liệu có gửi thông điệp mặt phẳng người dùng định trước thứ hai trong chu kỳ thời gian định trước, liệu có kích hoạt bảo vệ mặt phẳng báo hiệu (bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc bảo vệ mật mã hóa mặt phẳng báo hiệu). Thông điệp mặt phẳng báo hiệu định trước thứ hai có thể bao gồm yêu cầu đăng ký hoặc yêu cầu dịch vụ. Cụ thể là, nếu được xác định, dựa trên thủ tục hiện tại, rằng thiết bị đầu cuối đang khởi tạo yêu cầu đăng ký (hoặc yêu cầu dịch vụ), được xác định rằng thủ tục hiện tại là thủ tục đăng ký (hoặc thủ tục dịch vụ). Do thông tin phân phối tài nguyên mặt phẳng người dùng không được nhận trong thủ tục, thiết bị đầu cuối có thể kích hoạt bảo vệ mặt phẳng báo hiệu.

Ngoài ra, một cách tùy chọn, thiết bị đầu cuối có thể xác định, dựa trên thông tin chỉ báo bảo vệ tính toàn vẹn mặt phẳng báo hiệu nhận được, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu, và có thể xác định, dựa trên thông tin chỉ báo mật mã hóa mặt phẳng báo hiệu nhận được, liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng báo hiệu. Ít nhất một trong mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn và mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa được nhận bởi thiết bị đầu cuối cũng có thể được gửi bởi phần tử

mạng khác đến BS, và sau đó được chuyển tiếp bởi BS đến thiết bị đầu cuối. Phần tử mạng khác có thể là, chẳng hạn, thực thể SMF.

Một cách tùy chọn, theo cách triển khai của các phương án thực hiện được thể hiện trên Fig.2, Fig.2a, và Fig.2b, phương pháp còn bao gồm bước sau:

BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc thiết bị đầu cuối và BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Phần sau sử dụng ví dụ trong đó BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng để mô tả.

Khi điều kiện không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bởi BS được thỏa mãn, BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Điều kiện để không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bởi BS có thể như sau: BS nhận thông điệp mặt phẳng báo hiệu định trước thứ nhất, chẳng hạn thông điệp hoàn thành yêu cầu đăng ký hoặc thông điệp hoàn thành yêu cầu dịch vụ; hoặc BS không nhận thông tin mặt phẳng người dùng hoặc thông tin mặt phẳng người dùng định trước chẳng hạn ID phiên, tiểu sử QoS, ID phiên định trước, hoặc tiểu sử QoS định trước trong chu kỳ thời gian định trước; hoặc BS không nhận, trong chu kỳ thời gian định trước, thông điệp yêu cầu phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối hoặc phân phối lại tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, chẳng hạn thông điệp yêu cầu phân phối tài nguyên; hoặc thông tin chỉ báo bảo vệ tính toàn vẹn được bao gồm trong chính sách bảo mật được nhận bởi BS chỉ báo không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc loại dịch vụ phiên không phải là loại dịch vụ phiên định trước, chẳng hạn, chính sách bảo mật được tiền tạo cấu hình có thể bao gồm mối quan hệ liên kết giữa loại dịch vụ phiên định trước và kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, và bảo vệ tính toàn vẹn mặt phẳng người dùng không thể được kích hoạt khi loại dịch vụ phiên định trước không được nhận.

Chẳng hạn, khi điều kiện mặc định thiết lập trước chỉ báo rằng BS luôn không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, khóa bảo vệ tính toàn vẹn mặt phẳng người dùng không được tạo.

Một cách tùy chọn, theo cách triển khai của các phương án thực hiện được thể hiện trên Fig.2, Fig.2a, và Fig.2b, phương pháp còn bao gồm các bước sau:

BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc thiết bị đầu cuối và BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Phần sau sử dụng ví dụ trong đó BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng để mô tả.

Khi điều kiện cho không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng bởi BS được thỏa mãn, BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Điều kiện để không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng bởi BS có thể như sau: BS nhận thông điệp mặt phẳng báo hiệu định trước thứ nhất, chẳng hạn thông điệp hoàn thành yêu cầu đăng ký hoặc thông điệp hoàn thành yêu cầu dịch vụ; hoặc BS không nhận thông tin mặt phẳng người dùng hoặc thông tin mặt phẳng người dùng định trước chẳng hạn ID phiên, tiểu sử QoS, ID phiên định trước, hoặc tiểu sử QoS định trước trong chu kỳ thời gian định trước; hoặc BS không nhận, trong chu kỳ thời gian định trước, thông điệp yêu cầu phân phối tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối hoặc phân phối lại tài nguyên mặt phẳng người dùng đến thiết bị đầu cuối, chẳng hạn thông điệp yêu cầu phân phối tài nguyên; hoặc thông tin chỉ báo bảo vệ mật mã hóa được bao gồm trong chính sách bảo mật được nhận bởi BS chỉ báo không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc loại dịch vụ phiên khôngа loại dịch vụ phiên định trước, chẳng hạn, chính sách bảo mật được tiền tạo cấu hình có thể bao gồm mối quan hệ liên kết giữa loại dịch vụ phiên định trước và kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Chẳng hạn, khi điều kiện mặc định thiết lập trước chỉ báo rằng BS luôn không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, khóa mật mã hóa mặt phẳng người dùng không được tạo.

Phần sau sử dụng ví dụ trong đó thiết bị đầu cuối không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng để mô tả.

Khi điều kiện không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bởi thiết bị đầu cuối được thỏa mãn, thiết bị đầu cuối không kích hoạt bảo vệ

tính toàn vẹn mặt phẳng người dùng.

Điều kiện để không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bởi thiết bị đầu cuối có thể như sau: Thiết bị đầu cuối không gửi thông điệp mặt phẳng người dùng định trước thứ hai trong chu kỳ thời gian định trước, chẳng hạn thông điệp yêu cầu thiết lập phiên; hoặc thiết bị đầu cuối nhận thông tin chỉ báo bảo vệ tính toàn vẹn được gửi bởi BS, và thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc thiết bị đầu cuối nhận thông điệp mặt phẳng báo hiệu định trước thứ nhất trong chu kỳ thời gian định trước, chẳng hạn thông điệp hoàn thành yêu cầu đăng ký hoặc thông điệp hoàn thành yêu cầu dịch vụ.

Chẳng hạn, khi điều kiện mặc định thiết lập trước chỉ báo rằng thiết bị đầu cuối luôn không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, khóa bảo vệ tính toàn vẹn mặt phẳng người dùng không được tạo.

Chẳng hạn, khi điều kiện mặc định thiết lập trước chỉ báo rằng BS luôn không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, khóa mật mã hóa mặt phẳng người dùng không được tạo.

Phần sau sử dụng ví dụ trong đó thiết bị đầu cuối không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng để mô tả.

Khi điều kiện để không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng bởi thiết bị đầu cuối được thỏa mãn, thiết bị đầu cuối không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Điều kiện để không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng bởi thiết bị đầu cuối có thể như sau: Thiết bị đầu cuối không gửi thông điệp mặt phẳng người dùng định trước thứ hai trong chu kỳ thời gian định trước, chẳng hạn thông điệp yêu cầu thiết lập phiên; hoặc thiết bị đầu cuối nhận thông tin chỉ báo bảo vệ mật mã hóa được gửi bởi BS, và thông tin chỉ báo bảo vệ mật mã hóa chỉ báo không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Chẳng hạn, khi điều kiện mặc định thiết lập trước chỉ báo rằng thiết bị đầu cuối luôn không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, khóa mật mã hóa mặt phẳng người dùng không được tạo.

Có nhiều cách triển khai trong đó thiết bị đầu cuối hoặc BS không kích hoạt

bảo vệ tính toàn vẹn mặt phẳng người dùng như sau:

Cách 1 không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng: Việc thiết bị đầu cuối hoặc BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng có thể là tạo khóa bảo vệ tính toàn vẹn mặt phẳng người dùng, nhưng không thực hiện bảo vệ tính toàn vẹn mặt phẳng người dùng bằng cách sử dụng khóa bảo vệ tính toàn vẹn mặt phẳng người dùng. Tức là, khi bảo vệ tính toàn vẹn mặt phẳng người dùng không được kích hoạt, khóa bảo vệ tính toàn vẹn mặt phẳng người dùng có thể trước hết được tạo, nhưng khóa bảo vệ tính toàn vẹn mặt phẳng người dùng không được sử dụng; sau đó, khi bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt, khóa bảo vệ tính toàn vẹn mặt phẳng người dùng được sử dụng để thực hiện bảo vệ tính toàn vẹn mặt phẳng người dùng.

Ở cách 1 không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng thu được trước khi thiết bị đầu cuối tạo khóa bảo vệ tính toàn vẹn mặt phẳng người dùng. Chẳng hạn, thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu có thể được sử dụng làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng.

Cách 2 không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng: Việc thiết bị đầu cuối hoặc BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng có thể là tạo khóa bảo vệ tính toàn vẹn mặt phẳng người dùng, và thực hiện bảo vệ tính toàn vẹn mặt phẳng người dùng bằng cách sử dụng khóa bảo vệ tính toàn vẹn mặt phẳng người dùng. Tức là, khi liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng không thể được xác định hoặc được xác định không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, khóa bảo vệ tính toàn vẹn mặt phẳng người dùng không thể được tạo, và khóa bảo vệ tính toàn vẹn mặt phẳng người dùng được tạo khi bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt.

Một cách tương ứng, chẳng hạn, đối với thiết bị đầu cuối và BS, nếu xác định được rằng thiết bị đầu cuối và BS luôn không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng (chẳng hạn, có thể là điều kiện định trước), khóa bảo vệ tính toàn vẹn mặt phẳng người dùng không thể được tạo.

Các cách triển khai trong đó BS và thiết bị đầu cuối không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng có thể giống hoặc có thể khác. Chẳng hạn, cả BS lẫn thiết bị đầu cuối sử dụng cách 1 không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng; hoặc thiết bị đầu cuối sử dụng cách 1 không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, và BS sử dụng cách 2 không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Có nhiều cách triển khai trong đó thiết bị đầu cuối hoặc BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, như sau:

Cách 1 không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng: Việc thiết bị đầu cuối hoặc BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bao gồm tạo khóa bảo vệ mật mã hóa mặt phẳng người dùng, nhưng không thực hiện bảo vệ mật mã hóa mặt phẳng người dùng bằng cách sử dụng khóa bảo vệ mật mã hóa mặt phẳng người dùng. Tức là, khi bảo vệ mật mã hóa mặt phẳng người dùng không được kích hoạt, khóa bảo vệ mật mã hóa mặt phẳng người dùng có thể trước hết được tạo, nhưng không được sử dụng; và khi bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt, bảo vệ mật mã hóa mặt phẳng người dùng được thực hiện bằng cách sử dụng khóa bảo vệ mật mã hóa mặt phẳng người dùng.

Theo cách 1 không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, thuật toán mật mã hóa mặt phẳng người dùng thu được trước khi thiết bị đầu cuối tạo khóa bảo vệ mật mã hóa mặt phẳng người dùng. Chẳng hạn, thuật toán mật mã hóa mặt phẳng báo hiệu có thể được sử dụng làm thuật toán mật mã hóa mặt phẳng người dùng.

Cách 2 không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng: Việc thiết bị đầu cuối hoặc BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng bao gồm bước tạo khóa bảo vệ mật mã hóa mặt phẳng người dùng khi bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt, và thực hiện bảo vệ mật mã hóa mặt phẳng người dùng bằng cách sử dụng khóa bảo vệ mật mã hóa mặt phẳng người dùng. Tức là, khi liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng không thể được xác định hoặc được xác định không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, khóa bảo vệ mật mã hóa

mặt phẳng người dùng không thể được tạo, và khóa mật mã hóa mặt phẳng người dùng được tạo khi bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt.

Một cách tương ứng, chẳng hạn, đối với thiết bị đầu cuối và BS, nếu xác định được rằng thiết bị đầu cuối và BS luôn luôn không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng (chẳng hạn, có thể là điều kiện định trước), khóa bảo vệ mật mã hóa mặt phẳng người dùng không thể được tạo.

Các cách triển khai trong đó BS và thiết bị đầu cuối không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng có thể giống nhau hoặc có thể khác nhau. Chẳng hạn, cả BS lẫn thiết bị đầu cuối sử dụng cách 1 không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng; hoặc thiết bị đầu cuối sử dụng cách 1 không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, và BS sử dụng cách 2 không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Ngoài ra, có nhiều cách triển khai trong đó BS và thiết bị đầu cuối kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Chẳng hạn, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng có thể được xác định dựa trên quy định thiết lập trước. Quy định thiết lập trước có thể là việc thiết bị đầu cuối kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng sau khi nhận SMC AS, tức là, thỏa mãn điều kiện bảo vệ mật mã hóa mặt phẳng người dùng của BS bao gồm nhận SMC AS. Dựa trên ví dụ này, chẳng hạn, thỏa mãn điều kiện bảo vệ tính toàn vẹn mặt phẳng người dùng của thiết bị đầu cuối bao gồm việc thiết bị đầu cuối nhận thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Tức là, thiết bị đầu cuối kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng sau khi nhận SMC AS, và liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng yêu cầu BS thông báo thiết bị đầu cuối bằng cách gửi thông tin chỉ báo bảo vệ tính toàn vẹn. Trong trường hợp này, thiết bị đầu cuối không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng khi không nhận thông tin chỉ báo bảo vệ tính toàn vẹn. Ngoài ra, khi thiết bị đầu cuối nhận thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, thiết bị đầu cuối kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Nói theo cách khác, thiết bị đầu cuối

không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng trong một chu kỳ thời gian, mà có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng trong chu kỳ thời gian khác. Tức là, thiết bị đầu cuối không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng tạm thời. Điều này khác với trường hợp trong đó thiết bị đầu cuối luôn không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. BS và thiết bị đầu cuối có thể còn xác định, dựa trên quy định thiết lập trước, liệu có kích hoạt bảo vệ mặt phẳng báo hiệu (bao gồm bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc bảo vệ mật mã hóa mặt phẳng báo hiệu), và quy định thiết lập trước có thể là việc thiết bị đầu cuối kích hoạt bảo vệ mặt phẳng báo hiệu sau khi nhận SMC AS.

Trong ví dụ khác, khi kích hoạt bảo vệ mặt phẳng báo hiệu (kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc bảo vệ mật mã hóa mặt phẳng báo hiệu), thiết bị đầu cuối hoặc BS kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Tức là, thỏa mãn điều kiện bảo vệ mật mã hóa mặt phẳng người dùng của BS bao gồm kích hoạt bảo vệ mặt phẳng báo hiệu. Nói theo cách khác, bảo vệ mật mã hóa mặt phẳng người dùng có thể được kích hoạt cùng với bảo vệ mặt phẳng báo hiệu, và kích hoạt hoặc vô hiệu hóa bảo vệ tính toàn vẹn mặt phẳng người dùng tùy thuộc liệu điều kiện bảo vệ tính toàn vẹn mặt phẳng người dùng của BS được thỏa mãn. Chẳng hạn, sau khi nhận chấp nhận đăng ký hoặc chấp nhận yêu cầu dịch vụ, BS có thể kích hoạt bảo vệ mặt phẳng báo hiệu (kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc bảo vệ mật mã hóa mặt phẳng báo hiệu), kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, nhưng không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Ngoài ra, theo triển khai này, thông tin chỉ báo mật mã hóa không hrteer được thiết lập.

Chẳng hạn, sau bước 203 trên Fig.2, tức là, sau khi BS gửi SMC AS đến thiết bị đầu cuối, thiết bị đầu cuối kích hoạt bảo vệ mặt phẳng báo hiệu nhưng không bảo vệ mặt phẳng người dùng, và có thể tạo khóa mặt phẳng báo hiệu (khóa bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc khóa bảo vệ mật mã hóa mặt phẳng báo hiệu) và khóa mặt phẳng người dùng (khóa bảo vệ tính toàn vẹn mặt phẳng người dùng và/hoặc khóa bảo vệ mật mã hóa mặt phẳng người dùng). Tuy nhiên, chỉ khóa mặt phẳng báo hiệu được sử dụng để bảo vệ, và

khóa mặt phẳng người dùng có thể được lưu trữ. Khóa mặt phẳng người dùng được sử dụng khi bảo vệ mặt phẳng người dùng được kích hoạt.

Trong ví dụ khác, sau bước 203 trên Fig.2, tức là, sau khi BS gửi SMC AS đến thiết bị đầu cuối, thiết bị đầu cuối kích hoạt bảo vệ mặt phẳng báo hiệu, kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, và không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, và có thể tạo khóa mặt phẳng báo hiệu (khóa bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc khóa bảo vệ mật mã hóa mặt phẳng báo hiệu), khóa mật mã hóa mặt phẳng người dùng, và khóa bảo vệ tính toàn vẹn mặt phẳng người dùng. Tuy nhiên, chỉ khóa mặt phẳng báo hiệu và khóa mật mã hóa mặt phẳng người dùng được sử dụng để bảo vệ. Khóa bảo vệ tính toàn vẹn mặt phẳng người dùng có thể được lưu trữ. Khi bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt, khóa bảo vệ tính toàn vẹn mặt phẳng người dùng được sử dụng để thực hiện bảo vệ tính toàn vẹn.

Trong ví dụ khác, sau bước 203 trên Fig.2, tức là, sau khi BS gửi SMC AS đến thiết bị đầu cuối, thiết bị đầu cuối kích hoạt bảo vệ mặt phẳng báo hiệu mà không phải bảo vệ mặt phẳng người dùng, có thể tạo khóa mặt phẳng báo hiệu (khóa bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc khóa bảo vệ mật mã hóa mặt phẳng báo hiệu) và sử dụng khóa mặt phẳng báo hiệu để bảo vệ, và không tạo khóa mặt phẳng người dùng (khóa bảo vệ tính toàn vẹn mặt phẳng người dùng và/hoặc khóa bảo vệ mật mã hóa mặt phẳng người dùng). Trong ví dụ khác, khi thông điệp yêu cầu ở bước 211 trên Fig.2b là yêu cầu thiết lập phiên, sau bước 211, BS gửi SMC AS hoặc thông điệp tái cấu hình RRC đến thiết bị đầu cuối, và sau khi nhận SMC AS hoặc thông điệp tái cấu hình RRC, thiết bị đầu cuối sử dụng khóa mặt phẳng người dùng để thực hiện bảo vệ bảo mật mặt phẳng người dùng.

Trong ví dụ khác, sau bước 203 trên Fig.2, tức là, sau khi BS gửi SMC AS đến thiết bị đầu cuối, thiết bị đầu cuối kích hoạt bảo vệ mặt phẳng báo hiệu và bảo vệ mật mã hóa mặt phẳng người dùng, không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, có thể tạo khóa mặt phẳng báo hiệu (khóa bảo vệ tính toàn vẹn mặt phẳng báo hiệu và/hoặc khóa bảo vệ mật mã hóa mặt phẳng báo hiệu) và sử dụng khóa mặt phẳng báo hiệu để bảo vệ, và có thể tạo khóa

mật mã hóa mặt phẳng người dùng và sử dụng khóa mật mã hóa mặt phẳng người dùng để bảo vệ, nhưng không tạo khóa bảo vệ tính toàn vẹn mặt phẳng người dùng. Trong ví dụ khác, khi thông điệp yêu cầu ở bước 211 trên Fig.2b là yêu cầu thiết lập phiên, sau bước 211, BS gửi SMC AS hoặc thông điệp tái cấu hình RRC đến thiết bị đầu cuối, và sau khi nhận SMC AS hoặc thông điệp tái cấu hình RRC, thiết bị đầu cuối tạo khóa bảo vệ tính toàn vẹn mặt phẳng người dùng và sử dụng khóa bảo vệ tính toàn vẹn mặt phẳng người dùng để thực hiện bảo vệ bảo mật mặt phẳng người dùng.

Thiết bị đầu cuối có thể xác định, dựa trên thông tin chỉ báo bảo vệ tính toàn vẹn được nhận được gửi bởi BS, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, hoặc thiết bị đầu cuối cũng có thể xác định kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng hoặc không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, được mô tả sau đây bằng cách sử dụng cách triển khai c1 và cách triển khai c2. Ngoài ra, một cách tùy chọn, để tiết kiệm tài nguyên, nếu thiết bị đầu cuối xác định không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng có thể không được gửi. Tức là, theo cách triển khai tùy chọn này, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng trống không thể được gửi, mà nếu thiết bị đầu cuối không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, thuật toán mật mã hóa mặt phẳng người dùng trống được gửi.

Nên lưu ý rằng theo các phương án thực hiện nêu trên và các cách triển khai triển khai tùy chọn của các phương án thực hiện, ít nhất một trong thông tin chỉ báo bảo vệ tính toàn vẹn, thông tin chỉ báo mật mã hóa, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn, và mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa được gửi bởi BS đến thiết bị đầu cuối có thể được mang trong thông điệp định trước. Chẳng hạn, trường được định trước trong thông điệp định trước, và trường định trước mang ít nhất một trong thông tin chỉ báo bảo vệ tính toàn vẹn, thông tin chỉ báo mật mã hóa, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn, và mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa. Thông điệp định trước có thể là SMC AS hoặc yêu cầu tái cấu hình RRC. Chẳng hạn, thông tin chỉ báo bảo vệ tính toàn vẹn được gửi đến thiết bị đầu

cuối ở dạng ID của thuật toán được thể hiện trên cách triển khai sau c1-1 (b7).

Nên lưu ý rằng, theo các phương án thực hiện nêu trên và các cách triển khai tùy chọn khác nhau của phương án thực hiệns, ít nhất một trong thông tin chỉ báo bảo vệ tính toàn vẹn, thông tin chỉ báo mật mã hóa, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn, và mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa that are được nhận bởi BS có thể được mang trong chính sách bảo mật, và c1-1 (b2) đến c1-1 (b7) có thể được sử dụng cụ thể.

Phần sau mô tả các cách biểu diễn khác nhau của thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa.

Cách triển khai c1-1 (b1)

Ít nhất một trong thông tin chỉ báo bảo vệ tính toàn vẹn, thông tin chỉ báo mật mã hóa, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn, và mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa có thể được biểu diễn bằng cách thiết lập ID phiên trong trường định trước. Chẳng hạn, khi BS không nhận ID phiên, ID phiên trong trường định trước trong thông điệp định trước được gửi đến thiết bị đầu cuối được gán bằng 0, chỉ báo rằng chỉ bảo vệ mặt phẳng báo hiệu được kích hoạt, bảo vệ tính toàn vẹn mặt phẳng người dùng không được kích hoạt, và mật mã hóa mặt phẳng người dùng không được kích hoạt. Khi ID phiên trong trường định trước trong thông điệp định trước được nhận bởi thiết bị đầu cuối bằng 0, có thể xác định được rằng chỉ bảo vệ mặt phẳng báo hiệu được kích hoạt (bảo vệ tính toàn vẹn mặt phẳng báo hiệu được kích hoạt và/hoặc bảo vệ mật mã hóa mặt phẳng báo hiệu được kích hoạt), thông tin chỉ báo bảo vệ tính toàn vẹn mặt phẳng người dùng không được kích hoạt, và thông tin chỉ báo mật mã hóa mặt phẳng người dùng không được kích hoạt.

Ngoài ra, kích hoạt bảo vệ mặt phẳng báo hiệu có thể là kích hoạt ít nhất một trong bảo vệ tính toàn vẹn mặt phẳng báo hiệu và bảo vệ mật mã hóa mặt phẳng báo hiệu. Cụ thể là, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu, bảo vệ mật mã hóa mặt phẳng báo hiệu, hoặc bảo vệ tính toàn vẹn mặt phẳng báo hiệu và bảo vệ mật mã hóa mặt phẳng báo hiệu có thể được xác định dựa trên quy tắc định trước hoặc tương tự. Chẳng hạn, bảo vệ tính toàn vẹn mặt phẳng báo hiệu và bảo vệ mật mã hóa mặt phẳng báo hiệu được kích hoạt mặc

định trong quy tắc định trước. Nội dung sau giống nội dung trong đoạn này không được lặp lại dưới đây.

Trong ví dụ khác, khi nhận ID phiên, BS có thể thiết lập ID phiên trong trường định trước trong thông điệp định trước được gửi đến thiết bị đầu cuối, về ID phiên hiện tại. Nếu thiết bị đầu cuối nhận thông điệp định trước được gửi bởi BS, trường định trước trong thông điệp định trước bao gồm ID phiên, và ID phiên là ID phiên hiện tại, thiết bị đầu cuối mặc định kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng và bảo vệ tính toàn vẹn mặt phẳng người dùng. Một cách tùy chọn, thuật toán mật mã hóa được lựa chọn bởi BS cho mặt phẳng báo hiệu cũng có thể được sử dụng cho mặt phẳng người dùng, tức là, thuật toán mật mã hóa được lựa chọn bởi BS là thuật toán mật mã hóa mặt phẳng báo hiệu và thuật toán mật mã hóa mặt phẳng người dùng. Một cách tương tự, thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu được lựa chọn được sử dụng làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Ngoài ra, nếu thiết bị đầu cuối nhận thông điệp định trước được gửi bởi BS, trường định trước trong thông điệp định trước bao gồm ID phiên, và ID phiên không trống, thiết bị đầu cuối có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và/hoặc bảo vệ mật mã hóa mặt phẳng người dùng. Cụ thể là, liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, bảo vệ tính toàn vẹn mặt phẳng người dùng, hoặc bảo vệ mật mã hóa mặt phẳng người dùng và bảo vệ tính toàn vẹn mặt phẳng người dùng có thể được xác định bằng cách tham khảo quy tắc định trước hoặc phần mô tả theo phương án thực hiện khác của sáng chế.

Theo triển khai tùy chọn khác, ít nhất một trong thông tin chỉ báo bảo vệ tính toàn vẹn, thông tin chỉ báo mật mã hóa, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn, và mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa có thể được chỉ báo bằng cách thiết lập thông tin liên quan của QoS trong trường định trước trong thông điệp định trước, chẳng hạn, thiết lập giá trị QFI. Cách sử dụng giá trị QFI có thể giống như cách sử dụng ID phiên. Chẳng hạn, khi BS không nhận QFI, QFI trong trường định trước trong thông điệp định trước được gửi đến thiết bị đầu cuối được gán bằng 0, chỉ báo rằng chỉ bảo vệ mặt phẳng báo hiệu được kích hoạt, thông tin chỉ báo bảo vệ tính toàn vẹn mặt

phẳng người dùng không được kích hoạt, và thông tin chỉ báo mật mã hóa mặt phẳng người dùng không được kích hoạt. Khi QFI trong trường định trước được nhận bởi thiết bị đầu cuối bằng 0, có thể xác định được rằng chỉ bảo vệ mặt phẳng báo hiệu được kích hoạt, thông tin chỉ báo bảo vệ tính toàn vẹn mặt phẳng người dùng không được kích hoạt, và thông tin chỉ báo mật mã hóa mặt phẳng người dùng không được kích hoạt.

Cách triển khai c1-1 (b2)

Thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể được biểu diễn bằng cách sử dụng thông tin bit trong trường định trước trong thông điệp định trước hoặc chính sách bảo mật, chẳng hạn, trường định trước có thể bao gồm một đoạn thông tin bit.

Chẳng hạn, trong trường hợp mặc định, bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt, và bảo vệ tính toàn vẹn mặt phẳng người dùng không được kích hoạt. Sau đó, một đoạn thông tin bit trong trường định trước là thông tin chỉ báo bảo vệ tính toàn vẹn. Vị trí bit 1 trong trường định trước có thể chỉ báo kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Vị trí bit 0 trong trường định trước có thể chỉ báo việc không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Trong ví dụ khác, trong trường hợp mặc định, bảo vệ mật mã hóa mặt phẳng người dùng không được kích hoạt, và bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt. Sau đó, một đoạn thông tin bit trong trường định trước là thông tin chỉ báo mật mã hóa. Cụ thể là, vị trí bit 1 trong trường định trước có thể chỉ báo kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng, và vị trí bit 0 trong trường định trước có thể chỉ báo việc không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Trong ví dụ khác, trong trường hợp mặc định, bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt, và bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt. Sau đó, một đoạn thông tin bit trong trường định trước là thông tin chỉ báo bảo vệ tính toàn vẹn và thông tin chỉ báo mật mã hóa. Vị trí bit 1 trong trường định trước có thể chỉ báo kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Vị

trí bit 0 trong trường định trước có thể chỉ báo việc không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và việc không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Cách triển khai c1-1 (b3)

Thông tin chỉ báo bảo vệ tính toàn vẹn và thông tin chỉ báo mật mã hóa có thể được biểu diễn bởi thông tin bit trong trường định trước trong thông điệp định trước hoặc chính sách bảo mật. Chẳng hạn, trường định trước có thể bao gồm hai đoạn thông tin bit. Một đoạn thông tin bit chỉ báo liệu mật mã hóa mặt phẳng người dùng cần được kích hoạt hoặc vô hiệu hóa. Đoạn còn lại của thông tin bit chỉ báo liệu bảo vệ tính toàn vẹn mặt phẳng người dùng cần được kích hoạt hoặc vô hiệu hóa. Tức là, một đoạn thông tin bit là thông tin chỉ báo mật mã hóa, và đoạn còn lại của thông tin bit là thông tin chỉ báo bảo vệ tính toàn vẹn. Chẳng hạn, thông tin bit tương ứng với thông tin chỉ báo mật mã hóa trong trường định trước được gán bằng 1, chỉ báo kích hoạt của bảo vệ mật mã hóa mặt phẳng người dùng. Thông tin bit tương ứng với thông tin chỉ báo bảo vệ tính toàn vẹn trong trường định trước được gán bằng 1, chỉ báo rằng thiết bị đầu cuối kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng. Thông tin bit tương ứng với thông tin chỉ báo mật mã hóa trong trường định trước được gán bằng 0, chỉ báo việc không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. Thông tin bit tương ứng với thông tin chỉ báo bảo vệ tính toàn vẹn trong trường định trước được gán bằng 0, chỉ báo rằng thiết bị đầu cuối không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Cách triển khai c1-1 (b4)

Thông tin chỉ báo bảo vệ tính toàn vẹn và thông tin chỉ báo mật mã hóa có thể được biểu diễn bởi thông tin bit trong trường định trước trong thông điệp định trước hoặc chính sách bảo mật. Chẳng hạn, trường định trước có thể bao gồm bốn đoạn thông tin bit. Một đoạn thông tin bit trong trường định trước chỉ báo liệu bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt. Chẳng hạn, thông tin bit được gán bằng 1, chỉ báo rằng bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt, và thông tin bit được gán bằng 0, chỉ báo rằng bảo vệ mật mã hóa mặt phẳng người dùng không được kích hoạt. Một đoạn thông

tin bit trong trường định trước chỉ báo liệu độ dài khóa bảo vệ mật mã hóa mặt phẳng người dùng bằng 128 bit hoặc 256 bit. Chẳng hạn, thông tin bit được gán bằng 1, chỉ báo rằng độ dài khóa bảo vệ mật mã hóa mặt phẳng người dùng bằng 128 bit, và thông tin bit được gán bằng 0, chỉ báo rằng độ dài khóa bảo vệ mật mã hóa mặt phẳng người dùng bằng 256 bit. Một đoạn thông tin bit trong trường định trước chỉ báo liệu độ dài khóa bảo vệ tính toàn vẹn mặt phẳng người dùng bằng 128 bit hoặc 256 bit. Thông tin bit được gán bằng 1, chỉ báo rằng độ dài khóa bảo vệ tính toàn vẹn mặt phẳng người dùng bằng 128 bit, tức là, giá trị MAC 32-bit được tạo. Thông tin bit được gán bằng 0, chỉ báo rằng độ dài khóa bảo vệ tính toàn vẹn mặt phẳng người dùng bằng 256 bit, tức là, giá trị MAC 64-bit được tạo. Một đoạn thông tin bit trong trường định trước chỉ báo liệu bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt. Chẳng hạn, thông tin bit được gán bằng 1, chỉ báo rằng bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt, và thông tin bit được gán bằng 0, chỉ báo rằng bảo vệ tính toàn vẹn mặt phẳng người dùng không được kích hoạt.

Thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể là các ví dụ được thể hiện trên cách triển khai c1-1 (b2) nêu trên, cách triển khai c1-1 (b3), và cách triển khai c1-1 (b4), và có thể là thông tin bit. Theo cách khác, thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể được gọi là thông tin chuyển đổi.

Ngoài ra, nội dung cụ thể của thông tin chuyển đổi có thể được kết hợp với phương pháp cụ thể. Chẳng hạn, nếu bảo vệ mật mã hóa mặt phẳng người dùng và bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt, và ngoài ra, nếu được xác định trong quy tắc định trước rằng bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt mặc định nhưng bảo vệ tính toàn vẹn mặt phẳng người dùng cần được xác định linh hoạt, chỉ thông tin chỉ báo 1 bit có thể được mang trong trường định trước, và thông tin chỉ báo 1 bit được sử dụng để chỉ báo liệu bảo vệ tính toàn vẹn mặt phẳng người dùng cần được kích hoạt. Ngoài ra, được xác dịnh trong quy tắc định trước rằng bảo vệ mật mã hóa mặt phẳng người dùng hoặc bảo vệ tính toàn vẹn mặt phẳng người dùng không được kích hoạt trước khi thông tin chỉ báo bảo vệ tính toàn vẹn và thông tin chỉ báo mật

mã hóa được nhận, 2-bit thông tin chỉ báo có thể được mang trong trường định trước, và lần lượt được sử dụng để chỉ báo liệu có kích hoạt bảo vệ mật mã hóa người dùng và liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Cách triển khai c1-1 (b5)

Thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể là ID của thuật toán. Trong trường hợp này, thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể được mang trong trường định trước trong thông điệp định trước hoặc chính sách bảo mật, hoặc có thể được mang trong chính sách bảo mật. Nói theo cách khác, BS gửi ID của thuật toán đến thiết bị đầu cuối, ID của thuật toán được sử dụng để chỉ báo thuật toán, và ID của thuật toán cũng là thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa.

Theo triển khai tùy chọn, SMC AS được truyền bởi BS mang, chẳng hạn, các số EIA và EEA trong mạng LTE, và các số EIA và EEA biểu diễn thuật toán bảo vệ tính toàn vẹn và thuật toán mật mã hóa được lựa chọn. Các số EIA và EEA có thể được mang để biểu diễn thông tin chỉ báo bảo vệ tính toàn vẹn, thông tin chỉ báo mật mã hóa, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn, và mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa. Chẳng hạn, số EIA chỉ báo rằng bảo vệ tính toàn vẹn được kích hoạt.

Theo triển khai tùy chọn khác, ID của thuật toán có thể được mở rộng sang bốn trường định trước, lần lượt là EIA-RRC, EEA-RRC, EIA-UP, và EEA-UP. Thuật toán được lựa chọn được đặt ở vị trí tương ứng để biểu diễn phương pháp thương lượng hiện tại. Chẳng hạn, BS lựa chọn EIA-RRC = 3 và EEA-RRC = 2, và sau đó thông tin chỉ báo bảo vệ tính toàn vẹn, thông tin chỉ báo mật mã hóa, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn, và mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa có thể là (EIA-RRC = 3, EEA-RRC = 2, EIA-UP = 0, EEA-UP = 0). Do vậy, sau khi nhận thông tin, thiết bị đầu cuối kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu do EIA-RRC khác 0, kích hoạt bảo vệ mật mã hóa mặt phẳng báo hiệu do EEA-RRC khác 0, không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng do EIA-UP bằng 0, hoặc không kích hoạt bảo vệ mật mã hóa mặt phẳng người

dùng do EEA-UP bằng 0.

Ngoài ra, theo triển khai này, ID của thuật toán có thể không chỉ chỉ báo thông tin chỉ báo bảo vệ tính toàn vẹn và thông tin chỉ báo mật mã hóa, mà còn chỉ báo thuật toán. Tức là, trong trường hợp trong đó phương án thực hiện được sử dụng, khi ID của thuật toán được gửi, tất cả các thuật toán (chẳng hạn, thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích, thuật toán mật mã hóa mặt phẳng báo hiệu đích, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích, và thuật toán mật mã hóa mặt phẳng người dùng đích), thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo mật mã hóa có thể được chỉ báo.

Chẳng hạn, EIA-RRC = 3 có thể còn chỉ báo thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu. Trong ví dụ khác, EEA-RRC = 2 có thể còn chỉ báo bảo vệ mật mã hóa mặt phẳng báo hiệu thuật toán, và EIA-UP = 0 có thể còn chỉ báo thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Trong ví dụ khác, EEA-UP = 0 có thể còn chỉ báo bảo vệ mật mã hóa mặt phẳng người dùng thuật toán.

Theo triển khai tùy chọn của phương án thực hiện được thể hiện trên Fig.2a hoặc Fig.2b, thông tin chỉ báo bảo vệ tính toàn vẹn có thể là ID của thuật toán. Chẳng hạn, khi BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng cho thiết bị đầu cuối, thông tin chỉ báo bảo vệ tính toàn vẹn có thể là ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích.

Một cách tùy chọn, khi BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng cho thiết bị đầu cuối, thông tin chỉ báo bảo vệ tính toàn vẹn có thể là ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng định trước, hoặc không thể mang thông tin về thuật toán bảo vệ tính toàn vẹn bất kỳ. Tức là, ID của thuật toán bảo vệ tính toàn vẹn bất kỳ hoặc ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng định trước không được gửi, nghĩa là thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo không kích hoạt bảo vệ tính toàn vẹn. Chẳng hạn, giả sử rằng ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng định trước là X123. Nếu thông tin chỉ báo bảo vệ tính toàn vẹn được nhận bởi thiết bị đầu cuối là X123, thiết bị đầu cuối không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Theo triển khai tùy chọn của phương án thực hiện được thể hiện trên Fig.2a hoặc Fig.2b, BS có thể còn gửi thông tin chỉ báo mật mã hóa đến thiết bị đầu cuối, trong đó thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng cho thiết bị đầu cuối. Khi BS kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng cho thiết bị đầu cuối, thông tin chỉ báo mật mã hóa có thể là ID của thuật toán. Chẳng hạn, thông tin chỉ báo mật mã hóa là ID của thuật toán mật mã hóa mặt phẳng người dùng đích.

Một cách tùy chọn, khi BS không kích hoạt bảo vệ mật mã hóa cho thiết bị đầu cuối, thông tin chỉ báo mật mã hóa có thể là ID của thuật toán mật mã hóa mặt phẳng người dùng định trước hoặc thuật toán mật mã hóa trống. Tức là, ID của thuật toán mật mã hóa bất kỳ không được gửi hoặc thuật toán mật mã hóa trống hoặc ID của thuật toán mật mã hóa mặt phẳng người dùng định trước được gửi, nghĩa là thông tin chỉ báo mật mã hóa chỉ báo không kích hoạt bảo vệ mật mã hóa. Chẳng hạn, giả sử rằng ID của thuật toán mật mã hóa mặt phẳng người dùng định trước là X321. Nếu thông tin chỉ báo bảo vệ mật mã hóa được nhận bởi thiết bị đầu cuối là X321, thiết bị đầu cuối không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Theo triển khai tùy chọn khác của phương án thực hiện được thể hiện trên Fig.2, Fig.2a, hoặc Fig.2b, BS có thể còn gửi thông tin chỉ báo bảo vệ tính toàn vẹn mặt phẳng báo hiệu đến thiết bị đầu cuối, trong đó mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu cho thiết bị đầu cuối. Khi BS kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu cho thiết bị đầu cuối, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn có thể là ID của thuật toán. Chẳng hạn, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn là ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích.

Một cách tùy chọn, khi BS không kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu cho thiết bị đầu cuối, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn có thể là ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu định trước, hoặc có thể là thông tin không mang thuật toán bảo vệ tính toàn vẹn

bất kỳ. Chẳng hạn, giả sử rằng ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu định trước là X456. Nếu mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn được nhận bởi thiết bị đầu cuối là X456, thiết bị đầu cuối không kích hoạt bảo vệ tính toàn vẹn mặt phẳng báo hiệu.

Theo triển khai tùy chọn khác của phương án thực hiện được thể hiện trên Fig.2, Fig.2a, hoặc Fig.2b, BS có thể còn gửi thông tin chỉ báo mật mã hóa mặt phẳng báo hiệu đến thiết bị đầu cuối, trong đó mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ mật mã hóa mặt phẳng báo hiệu cho thiết bị đầu cuối. Khi BS kích hoạt bảo vệ mật mã hóa mặt phẳng báo hiệu cho thiết bị đầu cuối, mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa có thể là ID của thuật toán. Chẳng hạn, mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa là ID của thuật toán mật mã hóa mặt phẳng báo hiệu đích.

Một cách tùy chọn, khi BS không kích hoạt bảo vệ mật mã hóa mặt phẳng báo hiệu cho thiết bị đầu cuối, mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa có thể là ID của thuật toán mật mã hóa mặt phẳng báo hiệu định trước hoặc thuật toán mật mã hóa trống. Chẳng hạn, giả sử rằng ID của thuật toán mật mã hóa mặt phẳng báo hiệu định trước thuật toán là X654. Nếu mặt phẳng báo hiệu thông tin chỉ báo bảo vệ mật mã hóa được nhận bởi thiết bị đầu cuối là X654, thiết bị đầu cuối không kích hoạt bảo vệ mật mã hóa mặt phẳng báo hiệu.

Cách triển khai c1-1 (b6)

Thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể là ID phiên và thông tin 4-bit trong trường định trước trong thông điệp định trước hoặc chính sách bảo mật. Do vậy, thiết bị đầu cuối cần kích hoạt bảo mật mặt phẳng người dùng tương ứng của ID phiên dựa trên thông tin bit. Chẳng hạn, thiết bị đầu cuối có các ID phiên. Sau đó, các giải pháp bảo mật mặt phẳng người dùng tương ứng với các ID phiên có thể khác nhau. Chẳng hạn, một ID phiên tương ứng với kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng. ID phiên khác có thể tương ứng với việc không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Cách triển khai c1-1 (b7)

Thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể là ID phiên và ID của thuật toán trong trường định trước trong thông điệp định trước hoặc chính sách bảo mật.

Có thể được nhận biết từ phương án thực hiện nêu trên rằng, theo cách triển khai nêu trên, cách triển khai tương ứng với ID của thuật toán và thông tin 4-bit tương đối linh hoạt, do liệu bảo vệ mật mã hóa mặt phẳng người dùng được kích hoạt và liệu bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt có thể được xác định không. Có thể nhận biết dựa trên phương án thực hiện nêu trên rằng, thuật toán mặt phẳng báo hiệu được thương lượng có thể được sử dụng lại làm thông tin bit (tức là, thuật toán áp dụng được cho mặt phẳng báo hiệu cũng áp dụng được cho mặt phẳng người dùng, chẳng hạn, thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu đích được xác định cũng được sử dụng làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích, và thuật toán mật mã hóa mặt phẳng báo hiệu đích được xác định cũng được sử dụng làm thuật toán mật mã hóa mặt phẳng người dùng đích). Ngoài ra, ID của thuật toán có thể triển khai sự khác biệt giữa mặt phẳng báo hiệu thuật toán và thuật toán bảo mật mặt phẳng người dùng, chẳng hạn, sự khác biệt giữa mặt phẳng báo hiệu thuật toán mật mã hóa và thuật toán mật mã hóa mặt phẳng người dùng, và sự khác biệt giữa mặt phẳng báo hiệu thuật toán bảo vệ tính toàn vẹn và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng.

Thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể được mang trong thông điệp yêu cầu cấu hình lại RRC và được gửi bởi BS đến thiết bị đầu cuối. Trong trường hợp này, nếu thiết bị đầu cuối hiện tại đã kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng nhưng không bảo vệ tính toàn vẹn mặt phẳng người dùng, nhưng thiết bị đầu cuối hiện tại xác định kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, Một cách tùy chọn, thông điệp yêu cầu cấu hình lại RRC có thể chỉ truyền thông tin chỉ báo bảo vệ tính toàn vẹn.

BS có thể tạo và gửi thông tin chỉ báo bảo vệ tính toàn vẹn đến thiết bị đầu cuối. Theo triển khai tùy chọn khác, sau khi nhận thông tin chỉ báo bảo vệ tính

toàn vẹn và thông tin chỉ báo mật mã hóa, BS tạo thông tin chỉ báo mới (thông tin chỉ báo mới có thể bao gồm chỉ thông tin chỉ báo bảo vệ tính toàn vẹn), và còn thêm thông tin chỉ báo mới vào yêu cầu tái cấu hình RRC. Do thông tin chỉ báo bảo vệ tính toàn vẹn và thông tin chỉ báo mật mã hóa có thể đến từ giao diện N2 và giao diện có thể thay đổi sau khi chúng được gửi, BS còn cần thực hiện, dựa trên định dạng trong thông điệp yêu cầu cấu hình lại RRC, một số xử lý tương ứng trên thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa mà được mang.

Theo cách trong đó BS gửi thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa, BS có thể trực tiếp chuyển tiếp thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa đến thiết bị đầu cuối.

Theo cách khác trong đó BS gửi thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa, dựa trên thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa là ID của thuật toán, trong trường hợp này, BS có thể xác định ID của thuật toán đích tương ứng dựa trên (chẳng hạn, được nhận bởi BS hoặc thu được thông qua xác định bởi BS) thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa thu được, và gửi ID của thuật toán đích tương ứng đến thiết bị đầu cuối. Chẳng hạn, khi kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, BS xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích, và gửi ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối. Khi nhận ID của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích, thiết bị đầu cuối có thể kích hoạt thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng, và thực hiện bảo vệ tính toàn vẹn mặt phẳng người dùng bằng cách sử dụng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích.

Thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể được mang trong thông điệp yêu cầu tái cấu hình RRC và được gửi bởi BS đến thiết bị đầu cuối. Một cách tùy chọn, khi thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa là ID của thuật toán, thông điệp RRC có thể mang ID của thuật toán.

Chẳng hạn, khi thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa là ID của thuật toán, thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể là danh sách thuật toán. Một cách tùy chọn, nếu thuật toán trong danh sách thuật toán tương ứng với thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa là thuật toán bảo vệ tính toàn vẹn, và thuật toán bảo vệ tính toàn vẹn không phải là thuật toán trống, và nếu BS xác định rằng có không có giao cắt giữa thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, và danh sách thuật toán tương ứng với thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa, BS có thể lựa chọn một thuật toán thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Nếu thuật toán trong danh sách thuật toán tương ứng với thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa là thuật toán trống, BS không chọn thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích, có thể được hiểu như là không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Ngoài ra, một cách tùy chọn, nếu thuật toán trong danh sách thuật toán tương ứng với thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa là thuật toán mật mã hóa, và thuật toán mật mã hóa không phải là thuật toán mật mã hóa trống, và nếu BS xác định rằng không có giao cắt giữa thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, và danh sách thuật toán tương ứng với thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa, BS có thể lựa chọn một thuật toán mà thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, như là thuật toán mật mã hóa mặt phẳng người dùng đích. Nếu thuật toán trong danh sách thuật toán tương ứng với thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa là thuật toán mật mã hóa trống, BS có thể lựa

chọn thuật toán mật mã hóa trống làm thuật toán mật mã hóa mặt phẳng người dùng đích, có thể được hiểu như là việc không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Trong ví dụ khác, khi thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa là ID của thuật toán, thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể là danh sách thuật toán, và thuật toán có thể được lựa chọn từ danh sách thuật toán. Nếu thuật toán được lựa chọn là thuật toán bảo vệ tính toàn vẹn, và thuật toán bảo vệ tính toàn vẹn được lựa chọn là thuật toán bảo vệ tính toàn vẹn định trước, Một cách tùy chọn, trước khi chuyển tiếp thuật toán bảo vệ tính toàn vẹn được lựa chọn đến thiết bị đầu cuối, BS kiểm tra liệu thuật toán bảo vệ tính toàn vẹn được lựa chọn là thuật toán thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS. Nếu có, thuật toán bảo vệ tính toàn vẹn được lựa chọn được gửi đến thiết bị đầu cuối làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích.

Nói theo cách khác, nếu thuật toán bảo vệ tính toàn vẹn được lựa chọn không thỏa mãn điều kiện thuật toán thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, và thuật toán bảo vệ tính toàn vẹn được lựa chọn không phải là thuật toán trống, BS cần chọn thuật toán thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, làm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích, và gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối. Nói theo cách khác, nếu thuật toán bảo vệ tính toàn vẹn được lựa chọn không thỏa mãn điều kiện thuật toán thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, và thuật toán bảo vệ tính toàn vẹn được lựa chọn là thuật toán trống, BS không lựa chọn thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích,

có thể được hiểu như là không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

Ngoài ra, nói theo cách khác, một cách tùy chọn, nếu thuật toán được lựa chọn là thuật toán mật mã hóa, và thuật toán mật mã hóa được lựa chọn là thuật toán mật mã hóa định trước, Một cách tùy chọn, trước khi chuyển tiếp thuật toán mật mã hóa được lựa chọn đến thiết bị đầu cuối, BS kiểm tra liệu thuật toán mật mã hóa được lựa chọn có phải là thuật toán thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS. Nếu có, thuật toán mật mã hóa được lựa chọn được gửi đến thiết bị đầu cuối làm thuật toán mật mã hóa mặt phẳng người dùng đích.

Nói theo cách khác, nếu thuật toán mật mã hóa được lựa chọn không thỏa mãn điều kiện thuật toán thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, và thuật toán mật mã hóa được lựa chọn không phải là thuật toán trống, BS cần lựa chọn thuật toán thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, làm thuật toán mật mã hóa mặt phẳng người dùng đích, và gửi thuật toán mật mã hóa mặt phẳng người dùng đích đến thiết bị đầu cuối. Nói theo cách khác, nếu thuật toán mật mã hóa được lựa chọn không thỏa mãn điều kiện thuật toán thuộc thuật toán mật mã hóa mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và cũng thuộc thuật toán mật mã hóa mặt phẳng người dùng được phép bởi BS, và thuật toán mật mã hóa được lựa chọn là thuật toán trống, BS không chọn thuật toán mật mã hóa mặt phẳng người dùng đích, có thể được hiểu như là không kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

Theo phương án thực hiện sáng chế, thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc thông tin chỉ báo mật mã hóa có thể được mang trong SMC AS và được gửi đến thiết bị đầu cuối bởi BS. Một cách tùy chọn, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn và/hoặc mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa có thể cũng được mang trong SMC AS và được gửi đến thiết bị

đầu cuối bởi BS.

Theo triển khai tùy chọn, trước khi thiết bị đầu cuối kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, thiết bị đầu cuối có thể kiểm chứng bảo vệ tính toàn vẹn của SMC AS. Một cách tùy chọn, BS thực hiện bảo vệ tính toàn vẹn trên SMC AS bằng cách sử dụng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Một cách tùy chọn, sau khi xác định dựa trên chính sách bảo mật mà bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt, BS có thể thực hiện bảo vệ tính toàn vẹn trên SMC AS bằng cách sử dụng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Một cách tùy chọn, thiết bị đầu cuối kiểm chứng, bằng cách sử dụng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng, liệu bảo vệ tính toàn vẹn trên SMC AS là đúng. Chẳng hạn, sau khi thấy rằng bảo vệ tính toàn vẹn mặt phẳng người dùng được kích hoạt, thiết bị đầu cuối sử dụng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng để kiểm chứng liệu bảo vệ tính toàn vẹn trên SMC AS là đúng, và không loại trừ việc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng là thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu AS đang được sử dụng. Ngoài ra, BS nhận thông điệp kết thúc chế độ bảo mật AS được trả về bởi thiết bị đầu cuối. Một cách tùy chọn, BS kiểm chứng bảo vệ tính toàn vẹn trên thông điệp kết thúc chế độ bảo mật AS bằng cách sử dụng thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng. Một cách tùy chọn, sau khi thấy rằng thông điệp kết thúc chế độ bảo mật AS mang tham số bảo vệ tính toàn vẹn MAC-I, BS kiểm chứng bảo vệ tính toàn vẹn trên thông điệp kết thúc chế độ bảo mật AS, và không loại trừ việc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng là thuật toán bảo vệ tính toàn vẹn mặt phẳng báo hiệu AS đang được sử dụng. Một cách tùy chọn, sau khi nhận thông điệp kết thúc chế độ bảo mật, BS Một cách tương ứng kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng (chẳng hạn, thông tin chỉ báo tính toàn vẹn và thông tin chỉ báo mật mã hóa chỉ báo để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng và không kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, và BS có thể kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng nhưng không bảo vệ mật mã hóa mặt phẳng người dùng sau khi nhận thông điệp kết thúc chế độ bảo mật). Ngoài ra, một cách tùy chọn, sau khi một cách

tương ứng kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, BS có thể gửi thông điệp yêu cầu tái cấu hình RRC đến thiết bị đầu cuối, và ngoài ra, một cách tùy chọn, thiết bị đầu cuối trả về thông điệp hoàn thành tái cấu hình RRC cho BS.

Theo triển khai tùy chọn khác, trong trường hợp kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng, thông tin chỉ báo bảo vệ tính toàn vẹn có thể được mang trong SMC AS, và sau đó SMC AS được mang trong thông điệp yêu cầu tái cấu hình RRC và được gửi đến thiết bị đầu cuối bởi BS. Một cách tùy chọn, ít nhất một trong thông tin chỉ báo mật mã hóa, mặt phẳng báo hiệu thông tin chỉ báo bảo vệ tính toàn vẹn, và mặt phẳng báo hiệu thông tin chỉ báo mật mã hóa cũng có thể được mang trong SMC AS, và sau đó SMC AS được mang trong thông điệp yêu cầu tái cấu hình RRC và được gửi đến thiết bị đầu cuối bởi BS.

Fig.3 thể hiện ví dụ về sơ đồ cấu trúc của BS theo sáng chế.

Dựa trên khái niệm tương tự, sáng chế đề xuất BS 300, được tạo cấu hình để thực thi giải pháp theo một trong các phương pháp nêu trên. Như được thể hiện trên Fig.3, BS 300 bao gồm bộ xử lý 301, bộ thu phát 302, bộ nhớ 303, và giao diện truyền thông 304. Bộ xử lý 301, bộ thu phát 302, bộ nhớ 303, và giao diện truyền thông 304 được kết nối với nhau bằng cách sử dụng đường truyền 305.

Đường truyền 305 có thể là đường truyền liên kết thành phần ngoại vi (peripheral component interconnect, PCI), đường truyền kiến trúc chuẩn công nghiệp mở rộng (extended industry standard architecture, EISA), hoặc tương tự. Đường truyền có thể được phân loại thành đường truyền địa chỉ, đường truyền dữ liệu, đường truyền điều khiển, hoặc tương tự. Để dễ chỉ báo, đường truyền được chỉ báo bằng cách sử dụng duy nhất một đường nét đậm trên Fig.3. Tuy nhiên, không chỉ báo rằng chỉ có một đường truyền hoặc một loại đường truyền.

Bộ nhớ 303 có thể bao gồm bộ nhớ khả biến, chẳng hạn, bộ nhớ truy nhập ngẫu nhiên (random access memory, RAM), và cũng có thể bao gồm bộ nhớ bất biến, chẳng hạn, bộ nhớ nhanh, ổ đĩa cứng (hard disk drive, HDD), hoặc ổ

trạng thái rắn (solid-state drive, SSD); hoặc bộ nhớ 303 có thể bao gồm tổ hợp của các loại bộ nhớ này.

Giao diện truyền thông 304 có thể là giao diện truyền thông hữu tuyến, giao diện truyền thông không dây, hoặc tổ hợp của nó. Giao diện truyền thông hữu tuyến có thể là, chẳng hạn, giao diện Ethernet. Giao diện Ethernet có thể là giao diện quang học, giao diện điện, hoặc tổ hợp của nó. Giao diện truyền thông không dây có thể là giao diện WLAN.

Bộ xử lý 301 có thể là khối xử lý trung tâm (central processing unit, CPU), bộ xử lý mạng (network processor, NP), hoặc tổ hợp của CPU và NP. Bộ xử lý 301 có thể còn bao gồm vi mạch phần cứng. Vi mạch phần cứng có thể là mạch tích hợp ứng dụng cụ thể (application-specific integrated circuit, ASIC), thiết bị lôgic lập trình được (programmable logic device, PLD), hoặc tổ hợp của nó. PLD có thể là PLD phức (complex PLD, CPLD), mảng cổng dạng trường lập trình được (field-programmable gate array, FPGA), lôgic mảng chung (generic array logic, GAL), hoặc tổ hợp bất kỳ của nó.

Một cách tùy chọn, bộ nhớ 303 có thể còn được tạo cấu hình để lưu trữ lệnh chương trình. Bằng cách gọi lệnh chương trình được lưu trữ trong bộ nhớ 303, bộ xử lý 301 có thể thực hiện một hoặc nhiều bước hoặc cách triển khai tùy chọn theo các phương án thực hiện được thể hiện trên các giải pháp nêu trên, sao cho BS 300 triển khai chức năng của BS theo các phương pháp nêu trên.

Bộ xử lý 301 được tạo cấu hình để thực thi lệnh được lưu trữ trong bộ nhớ và điều khiển bộ thu phát 302 để thực hiện nhận tín hiệu và gửi tín hiệu. Khi bộ xử lý 301 thực thi lệnh được lưu trữ trong bộ nhớ, BS 300 có thể được tạo cấu hình để thực thi giải pháp sau.

Bộ xử lý 301 được tạo cấu hình để thu được chính sách bảo mật, trong đó chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối; và khi thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo BS để kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối, xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích. Bộ thu phát 302 được tạo cấu hình để gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người

dùng đích đến thiết bị đầu cuối. Theo cách này, liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối có thể được lựa chọn linh hoạt dựa trên chính sách bảo mật. Ngoài ra, chỉ khi bảo vệ tính toàn vẹn được kích hoạt cho thiết bị đầu cuối, BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối. Một mặt, do thuật toán bảo mật mặt phẳng người dùng được thương lượng độc lập, tính linh hoạt của việc xác định riêng rẽ thuật toán bảo mật mặt phẳng người dùng và thuật toán bảo mật mặt phẳng báo hiệu được cải thiện. Nói theo cách khác, do thông tin chỉ báo bảo vệ tính toàn vẹn được thêm vào, tính linh hoạt trong việc xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích của thiết bị đầu cuối được cải thiện.

Một cách tùy chọn, bộ thu phát 302 được tạo cấu hình để gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối bằng cách sử dụng báo hiệu RRC. Giải pháp theo phương án thực hiện sáng chế được triển khai bằng cách tận dụng lại báo hiệu RRC theo giải pháp kỹ thuật đã biết, sao cho tương thích tốt hơn với giải pháp kỹ thuật đã biết được triển khai, và chỉnh sửa với giải pháp kỹ thuật đã biết là tương đối nhỏ. Đối với cách triển khai tùy chọn cụ thể, tham khảo nội dung nêu trên, và các chi tiết không được mô tả lại ở đây.

Một cách tùy chọn, bộ xử lý 301 được tạo cấu hình cụ thể để xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS.

Một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, hoặc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên.

Một cách tùy chọn, chính sách bảo mật còn bao gồm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ. Bộ xử lý 301 được tạo cấu hình để xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được

phép bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ.

Một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên.

Một cách tùy chọn, bộ xử lý 301 còn được tạo cấu hình để: khi chính sách bảo mật còn bao gồm thông tin chỉ báo mật mã hóa, và thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS để kích hoạt bảo vệ mật mã hóa cho thiết bị đầu cuối, gửi thuật toán mật mã hóa mặt phẳng người dùng đích đến thiết bị đầu cuối bằng cách sử dụng bộ thu phát 302; hoặc khi chính sách bảo mật còn bao gồm độ dài khóa, gửi độ dài khóa đến thiết bị đầu cuối bằng cách sử dụng bộ thu phát 302; hoặc khi chính sách bảo mật còn bao gồm thông tin chỉ báo D - H, và thông tin chỉ báo D - H được sử dụng để chỉ báo BS kích hoạt D-H cho thiết bị đầu cuối, gửi khóa liên quan D-H đến thiết bị đầu cuối bằng cách sử dụng bộ thu phát 302.

Một cách tùy chọn, bộ thu phát 302 được tạo cấu hình cụ thể để nhận QoS của phiên hiện tại của thiết bị đầu cuối từ thực thể SMF, và bộ xử lý 301 còn được tạo cấu hình để phân phối DRB đích đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS.

Đối với cách phân phối cụ thể, bởi bộ xử lý 301, DRB đích đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS, dựa vào nội dung ở phương pháp nêu trên theo các phương án thực hiện. Các chi tiết không được mô tả lại ở đây.

Theo giải pháp triển khai tùy chọn, bộ xử lý 301 được tạo cấu hình để thiết lập DRB đích cho thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS.

Một cách tùy chọn, bộ thu phát 302 được tạo cấu hình để nhận chính sách bảo mật từ thực thể SMF; hoặc nhận ID của chính sách bảo mật từ thực thể SMF, và thu được chính sách bảo mật dựa trên ID của chính sách bảo mật.

Một cách tùy chọn, bộ xử lý 301 còn được tạo cấu hình để: thu được thuật

toán bảo mật mặt phẳng báo hiệu được hỗ trợ bởi thiết bị đầu cuối; và xác định thuật toán bảo mật mặt phẳng báo hiệu đích dựa trên mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo mật mặt phẳng báo hiệu được phép bởi BS; và bộ thu phát 302 còn được tạo cấu hình để thêm thuật toán bảo mật mặt phẳng báo hiệu đích vào SMC AS và gửi SMC AS đến thiết bị đầu cuối.

Fig.4 thể hiện ví dụ về sơ đồ cấu trúc của thực thể SMF theo sáng chế.

Dựa trên khái niệm tương tự, sáng chế đề xuất thực thể SMF 400, được tạo cấu hình để thực thi giải pháp theo một trong các phương pháp nêu trên. Như được thể hiện trên Fig.4, thực thể SMF 400 bao gồm bộ xử lý 401, bộ thu phát 402, bộ nhớ 403, và giao diện truyền thông 404. Bộ xử lý 401, bộ thu phát 402, bộ nhớ 403, và giao diện truyền thông 404 được kết nối với nhau bằng cách sử dụng đường truyền 405.

Đường truyền 405 có thể là đường truyền PCI, đường truyền kiến trúc chuẩn công nghiệp mở rộng (extended industry standard architecture, EISA), hoặc tương tự. Đường truyền có thể được phân loại thành đường truyền địa chỉ, đường truyền dữ liệu, đường truyền điều khiển, hoặc tương tự. Để dễ chỉ báo, đường truyền được chỉ báo bằng cách sử dụng chỉ một đường nét đậm trên Fig.4. Tuy nhiên, không chỉ báo rằng chỉ có một đường truyền hoặc chỉ một loại đường truyền.

Bộ nhớ 403 có thể bao gồm bộ nhớ bất biến, chẳng hạn, RAM, và may cũng bao gồm bộ nhớ bất biến, chẳng hạn, bộ nhớ nhanh, HDD, hoặc SSD; hoặc bộ nhớ 403 có thể bao gồm tổ hợp của các loại bộ nhớ này.

Giao diện truyền thông 404 có thể là giao diện truyền thông hữu tuyến, giao diện truyền thông không dây, hoặc tổ hợp của nó. Giao diện truyền thông hữu tuyến có thể là, chẳng hạn, giao diện Ethernet. Giao diện Ethernet có thể là giao diện quang học, giao diện điện, hoặc tổ hợp của nó. Giao diện truyền thông không dây có thể là giao diện WLAN.

Bộ xử lý 401 có thể là CPU, NP, hoặc tổ hợp của CPU và NP. Bộ xử lý 401 có thể còn bao gồm vi mạch phần cứng. Vi mạch phần cứng có thể là ASIC, PLD, hoặc tổ hợp của nó. PLD có thể là CPLD, FPGA, GAL, hoặc tổ hợp bất

kỳ của nó.

Một cách tùy chọn, bộ nhớ 403 có thể còn được tạo cấu hình để lưu trữ lệnh chương trình. Bằng cách gọi lệnh chương trình được lưu trữ trong bộ nhớ 403, bộ xử lý 401 có thể thực hiện một hoặc nhiều bước hoặc cách triển khai tùy chọn theo các phương án thực hiện được thể hiện trên các giải pháp nêu trên, sao cho thực thể SMF 400 triển khai chức năng của thực thể SMF theo các phương pháp nêu trên.

Bộ xử lý 401 được tạo cấu hình để thực thi lệnh được lưu trữ trong bộ nhớ và điều khiển bộ thu phát 402 để thực hiện nhận tín hiệu và gửi tín hiệu. Khi bộ xử lý 401 thực thi lệnh được lưu trữ trong bộ nhớ, thực thể SMF 400 có thể được tạo cấu hình để thực thi giải pháp sau.

Bộ thu phát 402 được tạo cấu hình để nhận thông điệp yêu cầu, trong đó thông điệp yêu cầu bao gồm tham số liên quan đến chính sách bảo mật, và gửi chính sách bảo mật hoặc ID của chính sách bảo mật đến BS. Bộ xử lý 401 được tạo cấu hình để thu được chính sách bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật. Chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối. Một mặt, do thuật toán bảo mật mặt phẳng người dùng được thương lượng độc lập, tính linh hoạt của việc xác định riêng rẽ thuật toán bảo mật mặt phẳng người dùng và thuật toán bảo mật mặt phẳng báo hiệu được cải thiện. Nói theo cách khác, do thông tin chỉ báo bảo vệ tính toàn vẹn được thêm vào, tính linh hoạt trong việc xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích của thiết bị đầu cuối được cải thiện.

Theo giải pháp triển khai tùy chọn, tham số liên quan đến chính sách bảo mật bao gồm ít nhất một trong ID của thiết bị đầu cuối, DNN của thiết bị đầu cuối, ID của lát của thiết bị đầu cuối, QoS của thiết bị đầu cuối, và ID phiên của thiết bị đầu cuối. Theo cách này, chính sách bảo mật có thể được tạo thành dựa trên các ID khác nhau từ các khía cạnh khác nhau hoặc ở các độ chi tiết khác nhau, và điều này linh hoạt hơn.

Một cách tùy chọn, bộ xử lý 401 được tạo cấu hình để: khi tham số liên

quan đến chính sách bảo mật bao gồm ID của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên ID của thiết bị đầu cuối và mối quan hệ liên kết giữa ID của thiết bị đầu cuối và chính sách bảo mật. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của thiết bị đầu cuối, sao cho các thiết bị đầu cuối khác nhau có thể tương ứng với các chính sách bảo mật khác nhau.

Theo triển khai tùy chọn khác, bộ xử lý 401 được tạo cấu hình để: khi tham số liên quan đến chính sách bảo mật bao gồm ID của lát của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên ID của lát của thiết bị đầu cuối và mối quan hệ liên kết giữa ID của lát và chính sách bảo mật. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của lát, sao cho thiết bị đầu cuối truy nhập các lát khác nhau có thể tương ứng với các chính sách bảo mật khác nhau.

Theo triển khai tùy chọn khác, bộ xử lý 401 được tạo cấu hình để: khi tham số liên quan đến chính sách bảo mật bao gồm ID phiên của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên ID phiên của thiết bị đầu cuối và mối quan hệ liên kết giữa ID phiên và chính sách bảo mật. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của phiên, sao cho thiết bị đầu cuối khởi tạo các phiên khác nhau có thể tương ứng với các chính sách bảo mật khác nhau.

Theo triển khai tùy chọn khác, bộ xử lý 401 được tạo cấu hình để: khi tham số liên quan đến chính sách bảo mật bao gồm QoS của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên QoS của thiết bị đầu cuối. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của QoS, sao cho thiết bị đầu cuối khởi tạo các QoS khác nhau có thể tương ứng với các chính sách bảo mật khác nhau.

Một cách tùy chọn, chính sách bảo mật còn bao gồm ít nhất một của nội dung sau: thông tin chỉ báo mật mã hóa, trong đó thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS để kích hoạt bảo vệ mật mã hóa cho thiết bị đầu cuối; độ dài khóa; thông tin chỉ báo D - H, trong đó thông tin chỉ báo D - H được sử dụng để chỉ báo BS kích hoạt D-H cho thiết bị đầu cuối; và thuật toán

bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ. Theo cách này, thông tin bất kỳ trong chính sách bảo mật có thể được chỉ báo linh hoạt hơn, sao cho chính sách bảo mật cuối cùng được xác định được làm thích ứng hơn với kịch bản ứng dụng phức tạp.

Fig.5 thể hiện ví dụ của sơ đồ cấu trúc của BS theo phương án thực hiện sáng chế.

Dựa trên khái niệm tương tự, phương án thực hiện sáng chế đề xuất BS, được tạo cấu hình để thực thi giải pháp theo một trong các thủ tục phương pháp nêu trên. Như được thể hiện trên Fig.5, BS 500 bao gồm khối nhận 501, khối xử lý 502, và khối gửi 503.

Khối xử lý 502 được tạo cấu hình để thu được chính sách bảo mật, trong đó chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối; và khi thông tin chỉ báo bảo vệ tính toàn vẹn chỉ báo BS kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối, gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối bằng cách sử dụng khối gửi 503. Khối gửi 503 được tạo cấu hình để gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối. Theo cách này, liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối có thể được lựa chọn linh hoạt dựa trên chính sách bảo mật. Ngoài ra, chỉ khi bảo vệ tính toàn vẹn được kích hoạt cho thiết bị đầu cuối, BS gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối. Một mặt, do thuật toán bảo mật mặt phẳng người dùng được thương lượng độc lập, tính linh hoạt của việc xác định riêng rẽ thuật toán bảo mật mặt phẳng người dùng và thuật toán bảo mật mặt phẳng báo hiệu được cải thiện. Nói theo cách khác, do thông tin chỉ báo bảo vệ tính toàn vẹn được thêm vào, tính linh hoạt trong việc xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích của thiết bị đầu cuối được cải thiện.

Một cách tùy chọn, khối gửi 503 được tạo cấu hình để gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối bằng cách sử dụng báo hiệu RRC. Giải pháp theo phương án thực hiện sáng chế được triển

khai bằng cách tận dụng lại báo hiệu RRC theo giải pháp kỹ thuật đã biết, sao cho tương thích tốt hơn với giải pháp kỹ thuật đã biết được triển khai, và chỉnh sửa với giải pháp kỹ thuật đã biết tương đối nhỏ. Đối với cách triển khai tùy chọn cụ thể, tham khảo nội dung nêu trên, và các chi tiết không được mô tả lại ở đây.

Một cách tùy chọn, trước khi gửi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích đến thiết bị đầu cuối bằng cách sử dụng khối gửi 503, khối xử lý 502 còn được tạo cấu hình để xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS.

Một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên, hoặc thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên.

Một cách tùy chọn, chính sách bảo mật còn bao gồm thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ. Khối xử lý 502 được tạo cấu hình để xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích dựa trên thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ.

Một cách tùy chọn, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ là thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được sắp xếp dựa trên độ ưu tiên.

Một cách tùy chọn, khối xử lý 502 còn được tạo cấu hình để: khi chính sách bảo mật còn bao gồm thông tin chỉ báo mật mã hóa, và thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS để kích hoạt bảo vệ mật mã hóa cho thiết bị đầu cuối, gửi thuật toán mật mã hóa mặt phẳng người dùng đích đến thiết bị đầu cuối bằng cách sử dụng khối gửi 503; hoặc khi chính sách bảo mật còn bao

gồm độ dài khóa, gửi độ dài khóa đến thiết bị đầu cuối bằng cách sử dụng khối gửi 503; hoặc khi chính sách bảo mật còn bao gồm thông tin chỉ báo D - H, và thông tin chỉ báo D - H được sử dụng để chỉ báo BS kích hoạt D-H cho thiết bị đầu cuối, gửi khóa liên quan D-H đến thiết bị đầu cuối bằng cách sử dụng khối gửi 503.

Một cách tùy chọn, trước khi thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích được gửi đến thiết bị đầu cuối bằng cách sử dụng khối gửi 503, khối nhận 501 được tạo cấu hình để nhận QoS của phiên hiện tại của thiết bị đầu cuối từ thực thể SMF; và khối xử lý 502 còn được tạo cấu hình để phân phối DRB đích đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS.

Khối xử lý 502 còn được tạo cấu hình để phân phối DRB đích đến thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS. Đối với cách cụ thể, tham khảo nội dung trong phương pháp nêu trên theo các phương án thực hiện. Các chi tiết không được mô tả lại ở đây.

Theo giải pháp triển khai tùy chọn, khối xử lý 502 được tạo cấu hình để thiết lập DRB đích cho thiết bị đầu cuối dựa trên ít nhất một trong chính sách bảo mật và QoS.

Một cách tùy chọn, khối nhận 501 được tạo cấu hình để nhận chính sách bảo mật từ thực thể SMF; hoặc nhận ID của chính sách bảo mật từ thực thể SMF và thu được chính sách bảo mật dựa trên ID của chính sách bảo mật.

Một cách tùy chọn, khối xử lý 502 còn được tạo cấu hình để: thu được thuật toán bảo mật mặt phẳng báo hiệu được hỗ trợ bởi thiết bị đầu cuối; và xác định thuật toán bảo mật mặt phẳng báo hiệu đích dựa trên mặt phẳng báo hiệu thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo mật mặt phẳng báo hiệu được phép bởi BS; và khối gửi 503 còn được tạo cấu hình để thêm thuật toán bảo mật mặt phẳng báo hiệu đích vào SMC AS và gửi SMC AS đến thiết bị đầu cuối.

Nên hiểu rằng việc phân chia các khối nêu trên chỉ là phân chia chức năng lôgic. Theo cách triển khai thực, tất cả hoặc một số khối có thể được tích hợp vào một thực thể vật lý, hoặc có thể riêng rẽ về mặt vật lý. Theo phương án

thực hiện sáng chế, khối nhận 501 và khối gửi 503 có thể được triển khai bởi bộ thu phát 302, và khối xử lý 502 có thể được triển khai bởi bộ xử lý 301. Như được thể hiện trên Fig.3, BS 300 có thể bao gồm bộ xử lý 301, bộ thu phát 302, và bộ nhớ 303. Bộ nhớ 303 có thể được tạo cấu hình để lưu trữ mã được sử dụng khi bộ xử lý 301 thực thi giải pháp, và mã có thể được cài đặt trước bởi chương trình/mã khi BS 300 được vận chuyển từ nhà máy.

Fig.6 thể hiện ví dụ của sơ đồ cấu trúc của thực thể SMF theo phương án thực hiện sáng chế.

Dựa trên khái niệm tương tự, phương án thực hiện sáng chế đề xuất thực thể SMF, được tạo cấu hình để thực thi giải pháp theo một trong các thủ tục phương pháp nêu trên. Như được thể hiện trên Fig.6, thực thể SMF 600 bao gồm khối nhận 601 và khối xử lý 602. Một cách tùy chọn, thực thể SMF 600 còn bao gồm khối gửi 603.

Khối nhận 601 được tạo cấu hình để nhận thông điệp yêu cầu, trong đó thông điệp yêu cầu bao gồm tham số liên quan đến chính sách bảo mật, và gửi chính sách bảo mật hoặc ID của chính sách bảo mật đến BS. Khối xử lý 602 được tạo cấu hình để thu được chính sách bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật. Chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối. Một mặt, do thuật toán bảo mật mặt phẳng người dùng được thương lượng độc lập, tính linh hoạt của việc xác định riêng rẽ thuật toán bảo mật mặt phẳng người dùng và thuật toán bảo mật mặt phẳng báo hiệu được cải thiện. Nói theo cách khác, do thông tin chỉ báo bảo vệ tính toàn vẹn được thêm vào, tính linh hoạt trong việc xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích của thiết bị đầu cuối được cải thiện.

Theo giải pháp triển khai tùy chọn, tham số liên quan đến chính sách bảo mật bao gồm ít nhất một trong ID của thiết bị đầu cuối, DNN của thiết bị đầu cuối, ID của lát của thiết bị đầu cuối, QoS của thiết bị đầu cuối, và ID phiên của thiết bị đầu cuối. Theo cách này, chính sách bảo mật có thể được tạo thành dựa trên các ID khác nhau từ các khía cạnh khác nhau hoặc ở các độ chi tiết

khác nhau, và điều này linh hoạt hơn.

Một cách tùy chọn, khối xử lý 602 được tạo cấu hình để: khi tham số liên quan đến chính sách bảo mật bao gồm ID của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên ID của thiết bị đầu cuối và mối quan hệ liên kết giữa ID của thiết bị đầu cuối và chính sách bảo mật. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của thiết bị đầu cuối, sao cho các thiết bị đầu cuối khác có thể tương ứng với các chính sách bảo mật khác nhau.

Theo triển khai tùy chọn khác, khối xử lý 602 được tạo cấu hình để: khi tham số liên quan đến chính sách bảo mật bao gồm ID của lát của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên ID của lát của thiết bị đầu cuối và mối quan hệ liên kết giữa ID của lát và chính sách bảo mật. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của lát, sao cho thiết bị đầu cuối truy nhập các lát khác nhau có thể tương ứng với các chính sách bảo mật khác nhau.

Theo triển khai tùy chọn khác, khối xử lý 602 được tạo cấu hình để: khi tham số liên quan đến chính sách bảo mật bao gồm ID phiên của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên ID phiên của thiết bị đầu cuối và mối quan hệ liên kết giữa ID phiên và chính sách bảo mật. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của phiên, sao cho thiết bị đầu cuối khởi tạo các phiên khác nhau có thể tương ứng với các chính sách bảo mật khác nhau.

Theo triển khai tùy chọn khác, khối xử lý 602 được tạo cấu hình để: khi tham số liên quan đến chính sách bảo mật bao gồm QoS của thiết bị đầu cuối, thu được, bởi thực thể SMF, chính sách bảo mật dựa trên QoS của thiết bị đầu cuối. Theo cách này, chính sách bảo mật có thể được xác định ở độ chi tiết của QoS, sao cho thiết bị đầu cuối khởi tạo các QoS khác nhau có thể tương ứng với các chính sách bảo mật khác nhau.

Một cách tùy chọn, chính sách bảo mật còn bao gồm ít nhất một của nội dung sau: thông tin chỉ báo mật mã hóa, trong đó thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS để kích hoạt bảo vệ mật mã hóa cho thiết bị đầu

cuối; độ dài khóa; thông tin chỉ báo D - H, trong đó thông tin chỉ báo D - H được sử dụng để chỉ báo BS kích hoạt D-H cho thiết bị đầu cuối; và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ. Theo cách này, thông tin bất kỳ trong chính sách bảo mật có thể được chỉ báo linh hoạt hơn, sao cho chính sách bảo mật cuối cùng được xác định được làm thích ứng hơn với kịch bản ứng dụng phức tạp.

Nên hiểu rằng việc phân chia các khối nêu trên chỉ là phân chia chức năng lôgic. Theo cách triển khai thực, tất cả hoặc một số khối có thể được tích hợp vào một thực thể vật lý, hoặc có thể tách riêng về mặt vật lý. Theo phương án thực hiện sáng chế, khối nhận 601 và khối gửi 603 có thể được triển khai bởi bộ thu phát 402, và khối xử lý 602 có thể được triển khai bởi bộ xử lý 401. Như được thể hiện trên Fig.4, thực thể SMF 400 có thể bao gồm bộ xử lý 401, bộ thu phát 402, và bộ nhớ 403. Bộ nhớ 403 có thể được tạo cấu hình để lưu trữ mã được sử dụng khi bộ xử lý 401 thực thi giải pháp, và mã có thể được cài đặt trước bởi chương trình/mã khi thực thể SMF 400 được vận chuyển từ nhà máy.

Theo các phương án thực hiện nêu trên, tất cả hoặc một số chức năng có thể được triển khai bằng cách sử dụng phần mềm, phần cứng, firmware, hoặc tổ hợp bất kỳ của nó. Khi được triển khai bằng cách sử dụng chương trình phần mềm, tất cả hoặc một số chức năng có thể được triển khai ở dạng sản phẩm chương trình máy tính. Sản phẩm chương trình máy tính bao gồm một hoặc nhiều lệnh. Khi các lệnh chương trình máy tính được nạp và thực thi trên máy tính, các thủ tục hoặc các chức năng theo các phương án thực hiện sáng chế được tạo một phần hoặc tất cả. Máy tính có thể là máy tính đa năng, máy tính dành riêng, mạng máy tính, hoặc thiết bị lập trình được khác. Các lệnh có thể được lưu trữ trong vật lưu trữ máy tính hoặc có thể được truyền từ một vật lưu trữ máy tính sang vật lưu trữ máy tính khác. Chẳng hạn, các lệnh có thể được truyền từ website, máy tính, máy chủ, hoặc trung tâm dữ liệu sang website, máy tính, máy chủ, hoặc trung tâm dữ liệu khác theo cách hữu tuyến (chẳng hạn, cáp đồng trục, sợi quang, hoặc đường thuê bao số (digital subscriber line, DSL)) hoặc không dây (chẳng hạn, hồng ngoại, vô tuyến, hoặc vi sóng). Vật lưu trữ máy tính có thể là vật sử dụng được bất kỳ mà máy tính truy nhập được,

hoặc thiết bị lưu trữ dữ liệu, chẳng hạn máy chủ hoặc trung tâm dữ liệu, tích hợp một hoặc nhiều phương tiện sử dụng được. Phương tiện sử dụng được có thể là phương tiện từ tính (chẳng hạn, đĩa mềm, đĩa cứng, hoặc băng từ, hoặc đĩa quang từ (magneto-optical, MO)), phương tiện quang học (chẳng hạn, CD, DVD, BD, hoặc HVD), phương tiện bán dẫn (chẳng hạn, ROM, EPROM, EEPROM, bộ nhớ bất biến (NAND FLASH), hoặc SSD), hoặc tương tự.

Chuyên gia trong lĩnh vực nên hiểu rằng các phương án thực hiện sáng chế có thể được bố trí như là phương pháp, hệ thống, hoặc sản phẩm chương trình máy tính. Do vậy, các phương án thực hiện sáng chế có thể sử dụng dạng phầm cứng chỉ theo các phương án thực hiện, phần mềm chỉ theo các phương án thực hiện, hoặc các phương án thực hiện với tổ hợp của phần mềm và phần cứng. Ngoài ra, các phương án thực hiện sáng chế có thể sử dụng dạng của sản phẩm chương trình máy tính được triển khai trên một hoặc nhiều vật lưu trữ máy tính đọc được (bao gồm nhưng không bị giới hạn ở bộ nhớ đĩa, CD-ROM, bộ nhớ quang, và tương tự) bao gồm mã chương trình máy tính sử dụng được.

Các phương án thực hiện sáng chế được mô tả dựa vào các lưu đồ và/hoặc các sơ đồ khối của phương pháp, thiết bị (hệ thống), và sản phẩm chương trình máy tính theo các phương án thực hiện sáng chế. Nên hiểu rằng các lệnh có thể được sử dụng để triển khai mỗi quá trình và/hoặc mỗi khối trong các lưu đồ và/hoặc các sơ đồ khối và tổ hợp của quá trình và/hoặc khối trong các lưu đồ và/hoặc các sơ đồ khối. Các lệnh này có thể được nêu trong máy tính đa năng, máy tính dành riêng, bộ xử lý nhúng, hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác bất kỳ để chế tạo máy, sao cho các lệnh được thực thi bởi máy tính hoặc bộ xử lý của thiết bị xử lý các lệnh được thực thi bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác bất kỳ tạo thiết bị để thực hiện chức năng cụ thể trong một hoặc nhiều quá trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh này có thể được lưu trữ trong bộ nhớ máy tính đọc được có thể ra lệnh máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác bất kỳ hoạt động theo cách cụ thể, sao cho các lệnh được lưu trữ trong bộ nhớ máy tính đọc được tạo đối tượng bao gồm thiết bị ra lệnh. Thiết bị ra lệnh triển khai chức năng cụ

thể trong một hoặc nhiều quá trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh này có thể được nạp trên thiết bị xử lý dữ liệu lập trình được khác, sao cho chuỗi các hoạt động và các bước được thực hiện trên máy tính hoặc thiết bị lập trình được khác, nhờ đó tạo xử lý được triển khai bằng máy tính. Do vậy, các lệnh được thực thi trên máy tính hoặc thiết bị lập trình được khác đề xuất các bước để triển khai chức năng cụ thể trong một hoặc nhiều quá trình trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Rõ ràng là, chuyên gia trong lĩnh vực có thể thực hiện các chỉnh sửa khác nhau và các biến thể với các phương án thực hiện sáng chế mà không xa rời tinh thần và nguyên lý của sáng chế. Sáng chế sẽ bao gồm các chỉnh sửa và các biến thể này giả sử chúng nằm trong phạm vi bảo hộ được định nghĩa bởi các điểm yêu cầu bảo hộ sau và các công nghệ tương đương.

YÊU CẦU BẢO HỘ

1. Hệ thống truyền thông bao gồm thực thể thực hiện chức năng quản lý phiên (session management function, SMF) và trạm cơ sở (base station, BS);

thực thể thực hiện SMF được tạo cấu hình để: nhận thông điệp yêu cầu, trong đó thông điệp yêu cầu bao gồm tham số liên quan của chính sách bảo mật; thu được chính sách bảo mật dựa trên tham số liên quan của chính sách bảo mật; và gửi chính sách bảo mật đến BS, trong đó chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn thứ nhất, và thông tin chỉ báo bảo vệ tính toàn vẹn thứ nhất được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối;

BS được tạo cấu hình để: nhận chính sách bảo mật được gửi bởi thực thể thực hiện SMF; và kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng khi chính sách bảo mật được nhận bởi BS bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn thứ nhất và thông tin chỉ báo bảo vệ tính toàn vẹn thứ nhất chỉ báo để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng;

trong đó hệ thống truyền thông còn bao gồm thiết bị đầu cuối;

BS được tạo cấu hình để: truyền lệnh chế độ bảo mật tầng truy nhập (access stratum, (AS) (security mode command, SMC) đến thiết bị đầu cuối;

thiết bị đầu cuối được tạo cấu hình để: sau khi nhận AS SMC, tạo khóa bảo vệ mật mã hóa mặt phẳng báo hiệu, khóa bảo vệ tính toàn vẹn mặt phẳng báo hiệu, khóa bảo vệ mật mã hóa mặt phẳng người dùng, và khóa bảo vệ tính toàn vẹn mặt phẳng người dùng, và kích hoạt bảo vệ mặt phẳng báo hiệu nhờ sử dụng khóa bảo vệ mật mã hóa mặt phẳng báo hiệu và khóa bảo vệ tính toàn vẹn mặt phẳng báo hiệu;

BS được tạo cấu hình để: gửi thông điệp tái cấu hình điều khiển tài nguyên vô tuyến (Radio Resource Control, RRC) đến thiết bị đầu cuối;

thiết bị đầu cuối được tạo cấu hình để: nhận thông điệp tái cấu hình RRC từ BS; và kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng đối với phiên khối dữ liệu giao thức (protocol data unit, PDU) nhờ sử dụng khóa bảo vệ tính toàn vẹn mặt phẳng người dùng khi thông điệp tái cấu hình RRC bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn thứ hai, trong đó thông tin chỉ báo bảo vệ tính toàn

vẹn thứ hai được tạo cấu hình để ra lệnh kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

2. Hệ thống truyền thông theo điểm 1, trong đó tham số liên quan của chính sách bảo mật bao gồm tên mạng dữ liệu (data network name, DNN) của thiết bị đầu cuối và định danh của lát của thiết bị đầu cuối.

3. Hệ thống truyền thông theo điểm 1, trong đó thông tin chỉ báo bảo vệ tính toàn vẹn thứ hai được biểu diễn bằng một bit, và trong đó thông tin chỉ báo bảo vệ tính toàn vẹn thứ hai chỉ báo kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng khi giá trị của bit bằng 1.

4. Hệ thống truyền thông theo điểm 1, trong đó BS được tạo cấu hình để:

kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng khi chính sách bảo mật được nhận bởi BS bao gồm thông tin chỉ báo bảo vệ mật mã hóa thứ nhất và thông tin chỉ báo bảo vệ mật mã hóa thứ nhất chỉ báo để kích hoạt bảo vệ tính toàn vẹn mặt phẳng người dùng.

5. Hệ thống truyền thông theo điểm 1 hoặc 3, trong đó thiết bị đầu cuối còn được tạo cấu hình để: kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng cho phiên PDU nhờ sử dụng khóa bảo vệ mật mã hóa mặt phẳng người dùng khi thông điệp tái cấu hình RRC bao gồm thông tin chỉ báo bảo vệ mật mã hóa thứ hai, trong đó thông tin chỉ báo bảo vệ mật mã hóa thứ hai được tạo cấu hình để ra lệnh kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng.

6. Hệ thống truyền thông theo điểm 5, trong đó thông tin chỉ báo bảo vệ mật mã hóa thứ hai được biểu diễn bằng một bit, và trong đó thông tin chỉ báo bảo vệ mật mã hóa thứ hai chỉ báo kích hoạt bảo vệ mật mã hóa mặt phẳng người dùng khi giá trị của bit bằng 1.

7. Hệ thống truyền thông theo điểm 1, trong đó thiết bị đầu cuối còn được tạo

cấu hình để: truyền thông điệp truyền thông AS SMC hoàn chỉnh đến BS.

8. Phương pháp truyền thông bao gồm các bước:

nhận, bằng thực thể thực hiện chức năng quản lý phiên, thông điệp yêu cầu, trong đó thông điệp yêu cầu bao gồm tham số liên quan của chính sách bảo mật;

thu được, bằng thực thể thực hiện SMF, chính sách bảo mật hoặc định danh của chính sách bảo mật dựa trên tham số liên quan của chính sách bảo mật; và gửi, bằng thực thể thực hiện SMF, chính sách bảo mật hoặc định danh của chính sách bảo mật đến BS, trong đó chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối;

trong đó tham số liên quan của chính sách bảo mật bao gồm DNN của thiết bị đầu cuối và định danh của lát của thiết bị đầu cuối; và việc thu được, bằng thực thể thực hiện SMF, chính sách bảo mật hoặc định danh của chính sách bảo mật dựa trên tham số liên quan của chính sách bảo mật bao gồm bước:

thu được, bằng thực thể thực hiện SMF, chính sách bảo mật hoặc định danh của chính sách bảo mật dựa trên DNN của thiết bị đầu cuối và định danh của lát của thiết bị đầu cuối.

9. Phương pháp theo điểm 8, trong đó chính sách bảo mật còn bao gồm thông tin chỉ báo mật mã hóa, và thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS để có thể bảo vệ mật mã hóa cho thiết bị đầu cuối.

10. Phương pháp theo điểm 9, trong đó thông tin chỉ báo bảo vệ tính toàn vẹn là định danh của thuật toán bảo vệ tính toàn vẹn, và thông tin chỉ báo mật mã hóa là định danh của thuật toán mật mã hóa.

11. Phương pháp theo điểm 8 hoặc 9, trong đó thông tin chỉ báo bảo vệ tính toàn vẹn là định danh của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng, trong đó thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được

mang trong chính sách bảo mật được xác định dựa trên ít nhất một trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi mạng phục vụ, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS.

12. Thực thể thực hiện chức năng quản lý phiên bao gồm khối nhận, khối xử lý và khối gửi; trong đó khối nhận được tạo cấu hình để nhận thông điệp yêu cầu, trong đó thông điệp yêu cầu bao gồm tham số liên quan của chính sách bảo mật;

khối xử lý được tạo cấu hình để thu được chính sách bảo mật hoặc định danh của chính sách bảo mật dựa trên tham số liên quan của chính sách bảo mật; và khối gửi được tạo cấu hình để gửi chính sách bảo mật hoặc định danh của chính sách bảo mật đến BS, trong đó chính sách bảo mật bao gồm thông tin chỉ báo bảo vệ tính toàn vẹn, và thông tin chỉ báo bảo vệ tính toàn vẹn được sử dụng để chỉ báo BS liệu có kích hoạt bảo vệ tính toàn vẹn cho thiết bị đầu cuối;

trong đó tham số liên quan của chính sách bảo mật bao gồm DNN của thiết bị đầu cuối và định danh của lát của thiết bị đầu cuối; và khối xử lý được tạo cấu hình cụ thể để thu được chính sách bảo mật hoặc định danh của chính sách bảo mật dựa trên DNN của thiết bị đầu cuối và định danh của lát của thiết bị đầu cuối.

13. Thực thể thực hiện SMF theo điểm 12, trong đó chính sách bảo mật còn bao gồm thông tin chỉ báo mật mã hóa, và thông tin chỉ báo mật mã hóa được sử dụng để chỉ báo BS để có thể bảo vệ mật mã hóa cho thiết bị đầu cuối.

14. Thực thể thực hiện SMF theo điểm 12 hoặc 13, trong đó thông tin chỉ báo bảo vệ tính toàn vẹn là định danh của thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng, trong đó thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được mang trong chính sách bảo mật được xác định dựa trên ít nhất một trong thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi

mạng phục vụ, thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được hỗ trợ bởi thiết bị đầu cuối, và thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng được phép bởi BS.

15. Vật ghi máy tính đọc được, trong đó vật ghi máy tính đọc được lưu trữ lệnh phần mềm máy tính, và khi lệnh máy tính được thực thi, phương pháp theo điểm bất kỳ trong số các điểm từ 8 đến 11 được thực hiện.

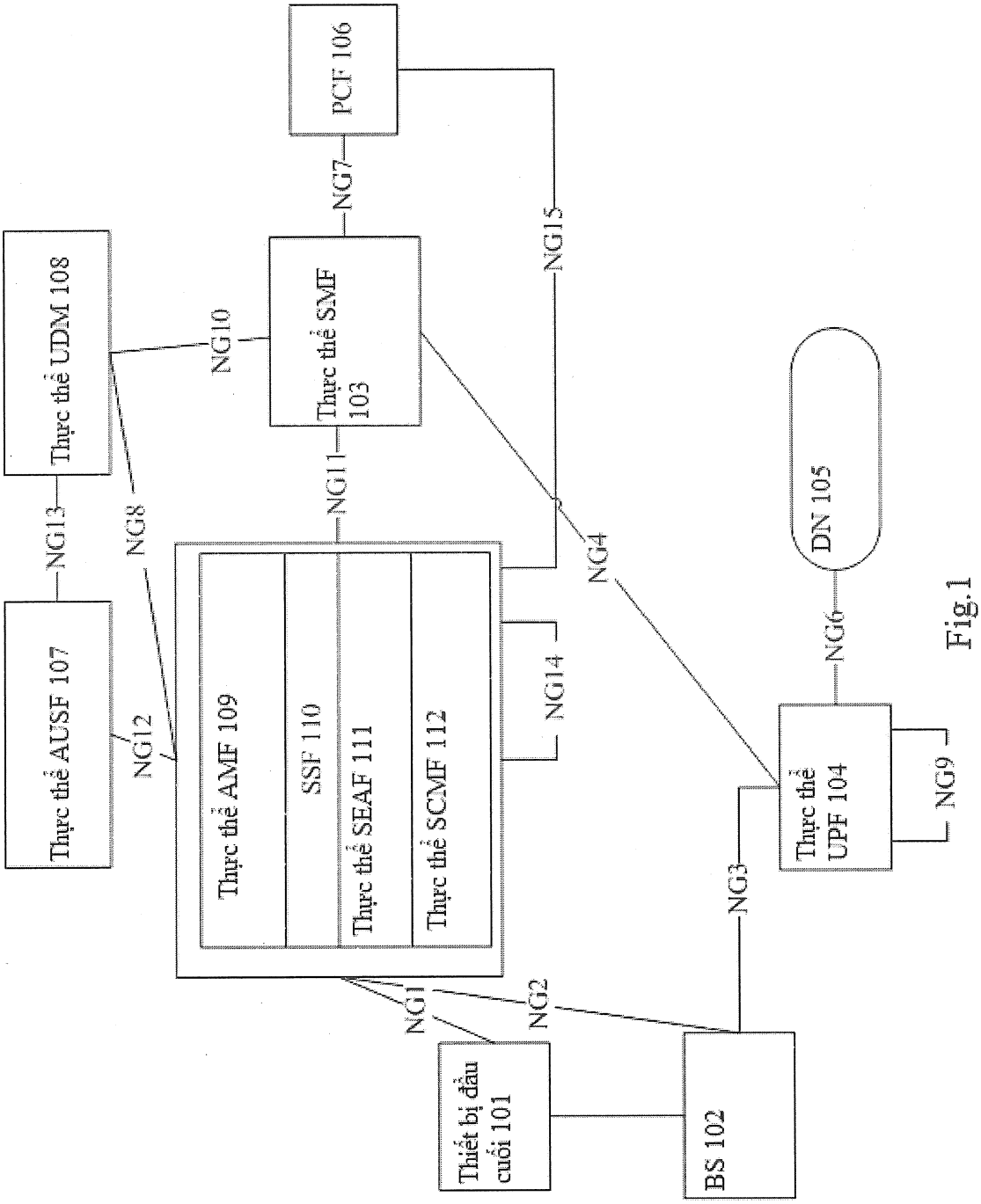

PCF 106
NG7
NG15
Thực thể UDM 108
NG10
Thực thể SMF 103
NG13
NG8
NG11
DN 105
Thực thể AUSF 107
NG12
Thực thể AMF 109
SSF 110
Thực thể SEAF 111
Thực thể SCMF 112
NG14
NG4
NG6
Thực thể UPF 104
NG9
NG3
NG1
NG2
Thiết bị đầu cuối 101
BS 102

Fig.1

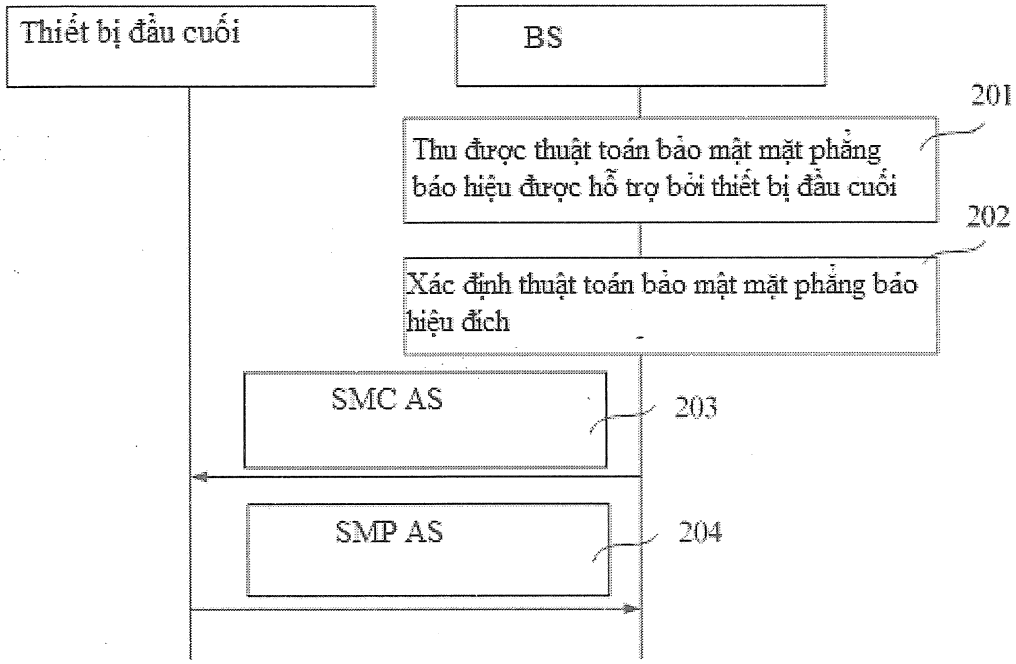

Thiết bị đầu cuối
BS
201
Thu được thuật toán bảo mật mặt phẳng báo hiệu được hỗ trợ bởi thiết bị đầu cuối
202
Xác định thuật toán bảo mật mặt phẳng báo hiệu đích
SMC AS
203
SMP AS
204

Fig.2

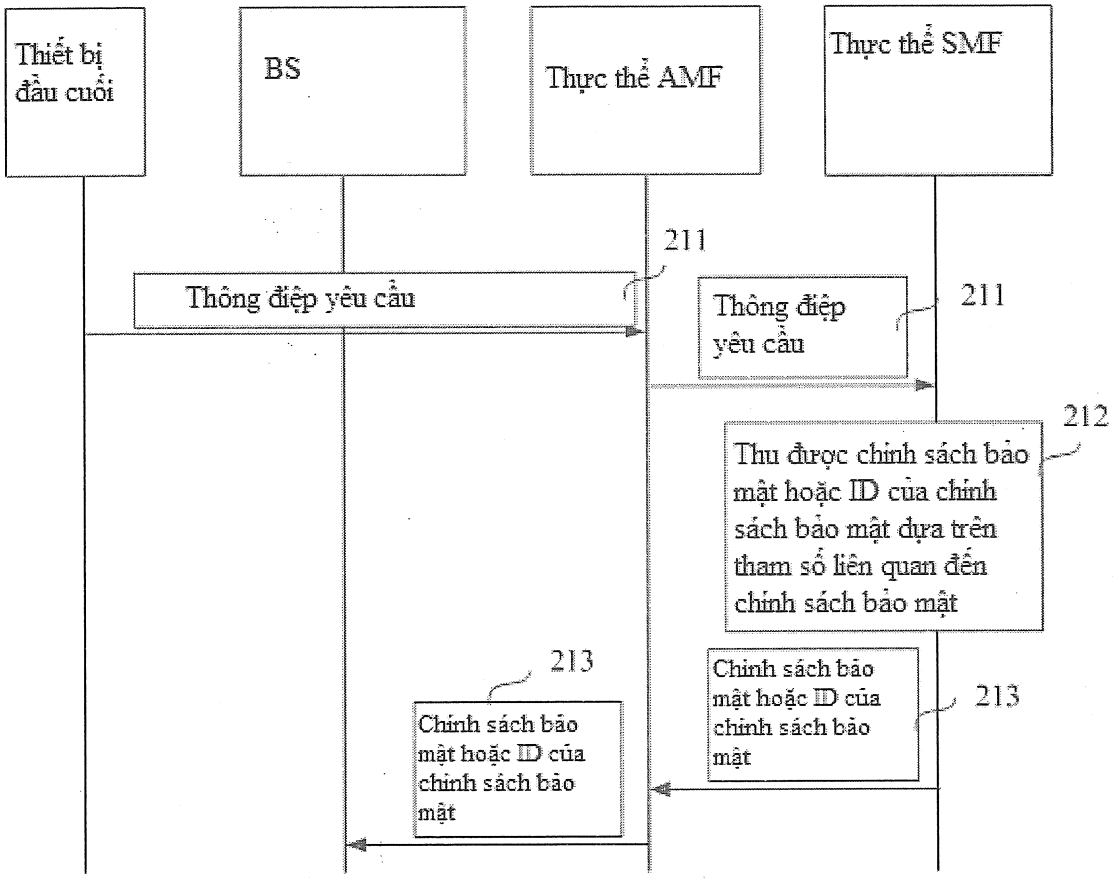

Thiết bị đầu cuối
BS
Thực thể AMF
Thực thể SMF
211
Thông điệp yêu cầu
Thông điệp yêu cầu
211
212
Thu được chính sách bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật
213
Chính sách bảo mật hoặc ID của chính sách bảo mật
213
Chính sách bảo mật hoặc ID của chính sách bảo mật

Fig.2a

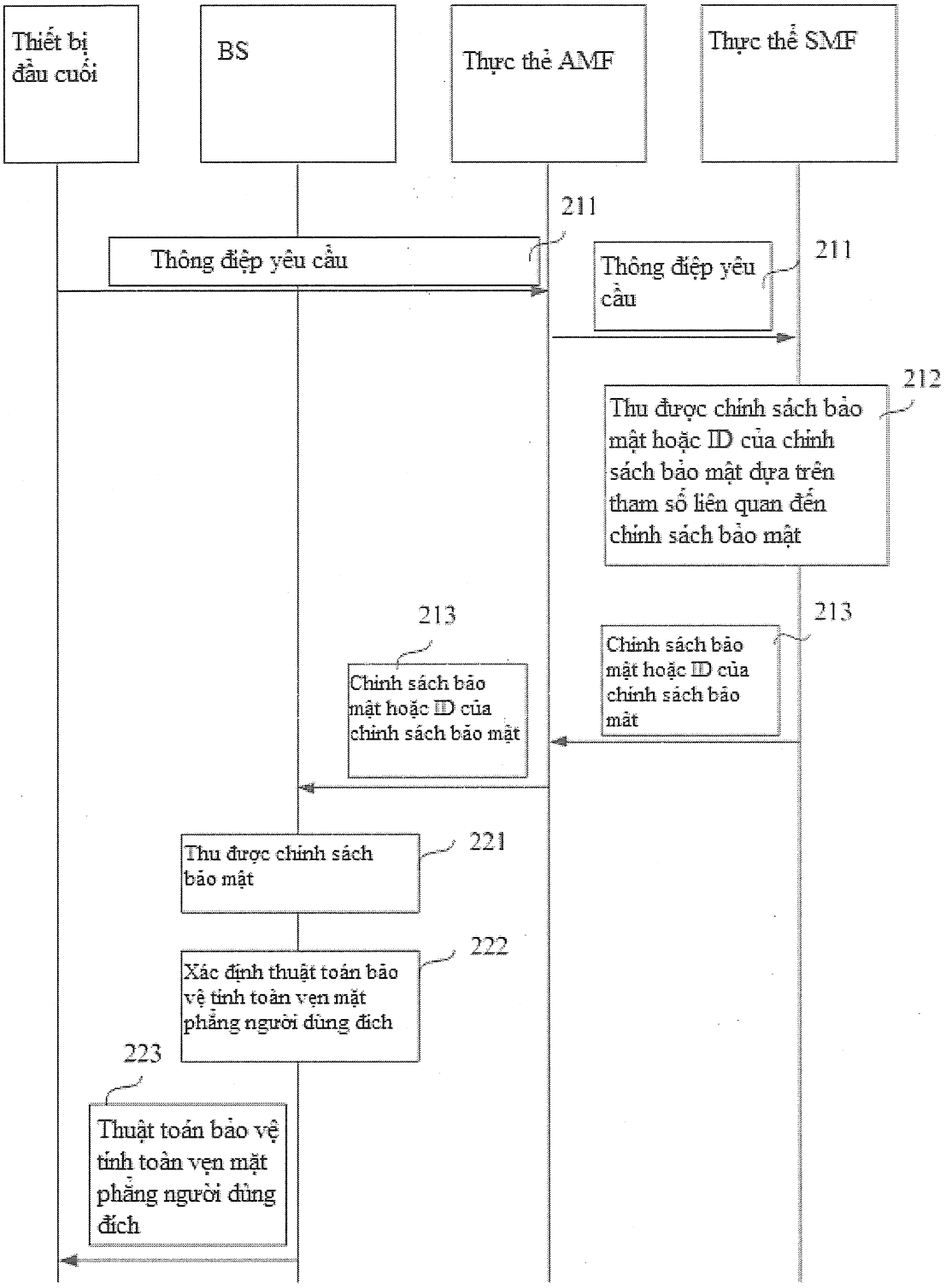

Thiết bị đầu cuối
BS
Thực thể AMF
Thực thể SMF
211
Thông điệp yêu cầu
Thông điệp yêu cầu
211
212
Thu được chính sách bảo mật hoặc ID của chính sách bảo mật dựa trên tham số liên quan đến chính sách bảo mật
213
213
Chính sách bảo mật hoặc ID của chính sách bảo mật
Chính sách bảo mật hoặc ID của chính sách bảo mật
Thu được chính sách bảo mật
221
Xác định thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích
222
223
Thuật toán bảo vệ tính toàn vẹn mặt phẳng người dùng đích

Fig.2b

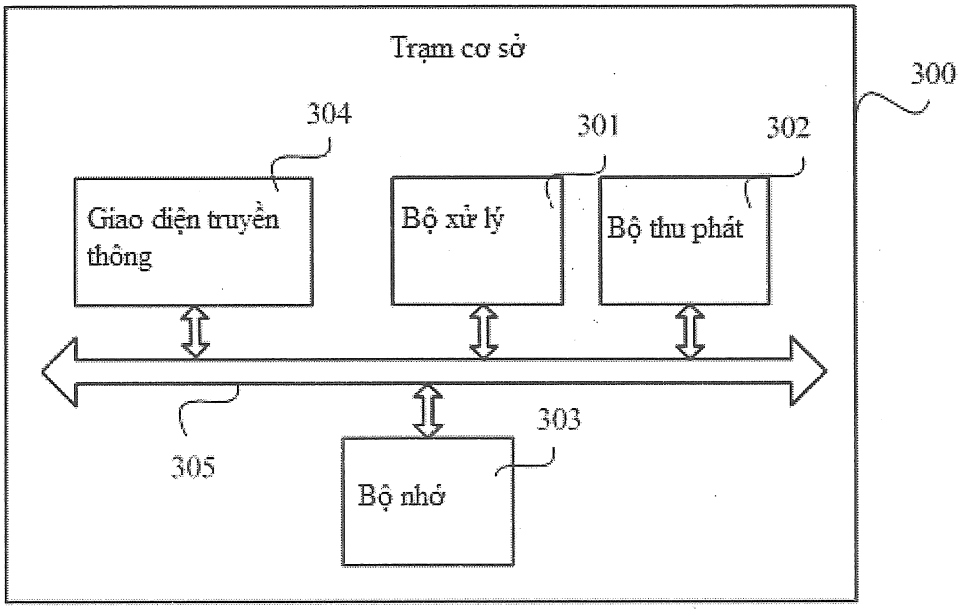

Trạm cơ sở
300
304
301
302
Giao diện truyền thông
Bộ xử lý
Bộ thu phát
305
303
Bộ nhớ

Fig.3

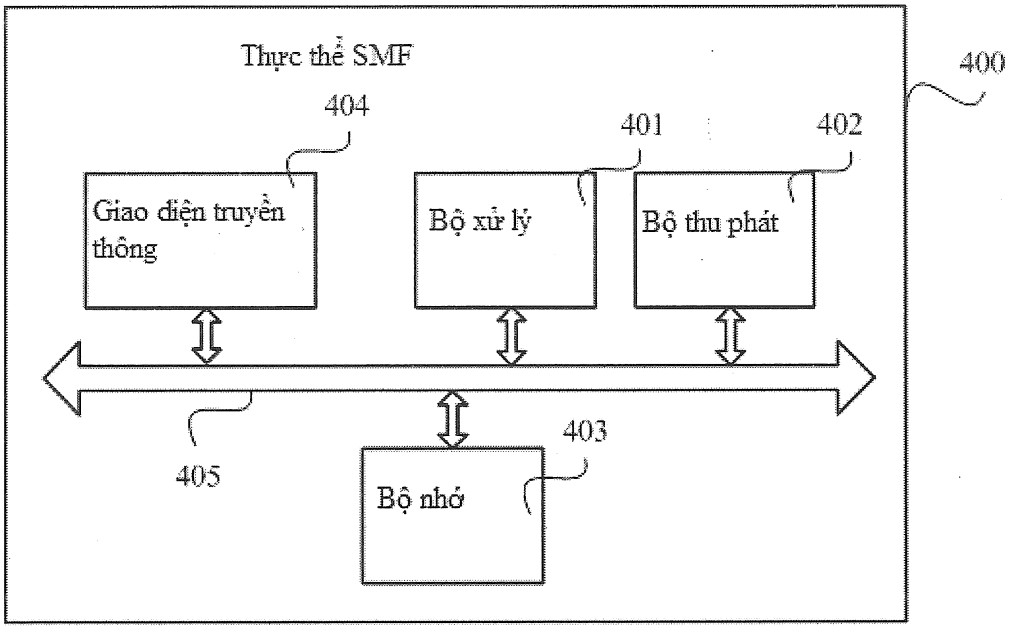

Thực thể SMF
400
404
401
402
Giao diện truyền thông
Bộ xử lý
Bộ thu phát
405
403
Bộ nhớ

Fig.4

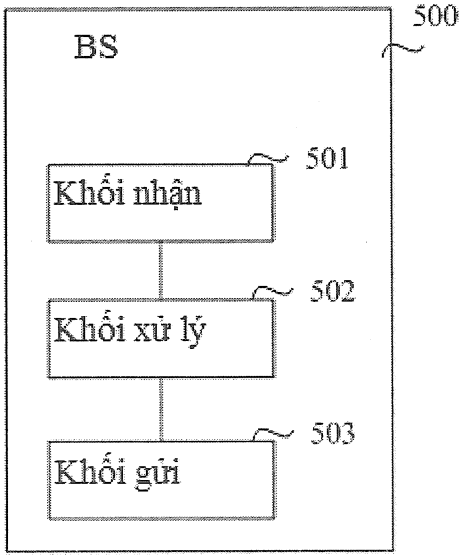

BS
500
501
Khối nhận
502
Khối xử lý
503
Khối gửi

Fig.5

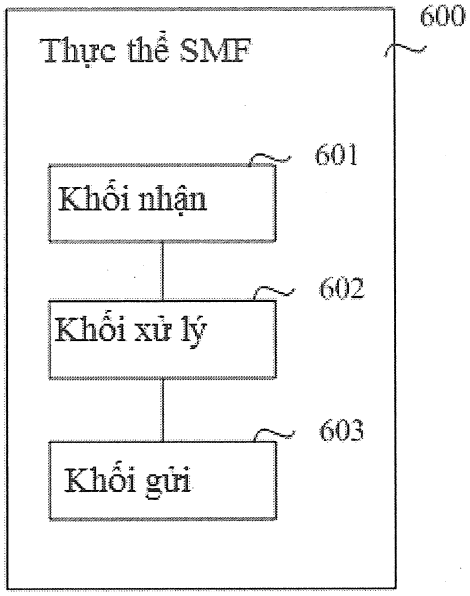

Thực thể SMF
600
601
Khối nhận
602
Khối xử lý
603
Khối gửi

Fig.6