(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) **1-0051121**

(51)[2020.01] **H04W 8/14**

(13) **B**

(21) 1-2020-01309
(22) 10/08/2018
(86) PCT/CN2018/099916 10/08/2018
(87) WO2019/029691 14/02/2019
(30) 201710686855.8 11/08/2017 CN
(45) 25/09/2025 450
(43) 27/07/2020 388A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, China
(72) LOU, Chong (CN); HUANG, Qufang (CN); LIU, Xing (CN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) PHƯƠNG PHÁP BẢO VỆ TÍNH TOÀN VẸN DỮ LIỆU, THIẾT BỊ TRUYỀN THÔNG VÀ PHƯƠNG TIỆN ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(21) 1-2020-01309

(57) Sáng chế đề xuất phương pháp bảo vệ tính toàn vẹn dữ liệu, thiết bị truyền thông, thiết bị đầu cuối, thiết bị mạng truy cập, thiết bị mạng lõi, phương tiện đọc được bằng máy tính, và hệ thống truyền thông. Thiết bị đầu cuối thu được thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và DRB tương ứng với phiên, và thực hiện, bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB tương ứng với phiên; hoặc thiết bị đầu cuối thu được thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng, và thực hiện, bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB tương ứng đối với luồng, trong đó một phiên bao gồm nhiều luồng, các thuật toán và khóa bảo vệ tính toàn vẹn khác nhau có thể được sử dụng cho các phiên khác nhau, và các thuật toán và khóa bảo vệ tính toàn vẹn khác nhau cũng có thể được sử dụng cho các luồng khác nhau. Theo cách này, sự bảo vệ tính toàn vẹn linh hoạt hơn và đáp ứng các yêu cầu bảo mật của cùng một người dùng cho các dịch vụ khác nhau.

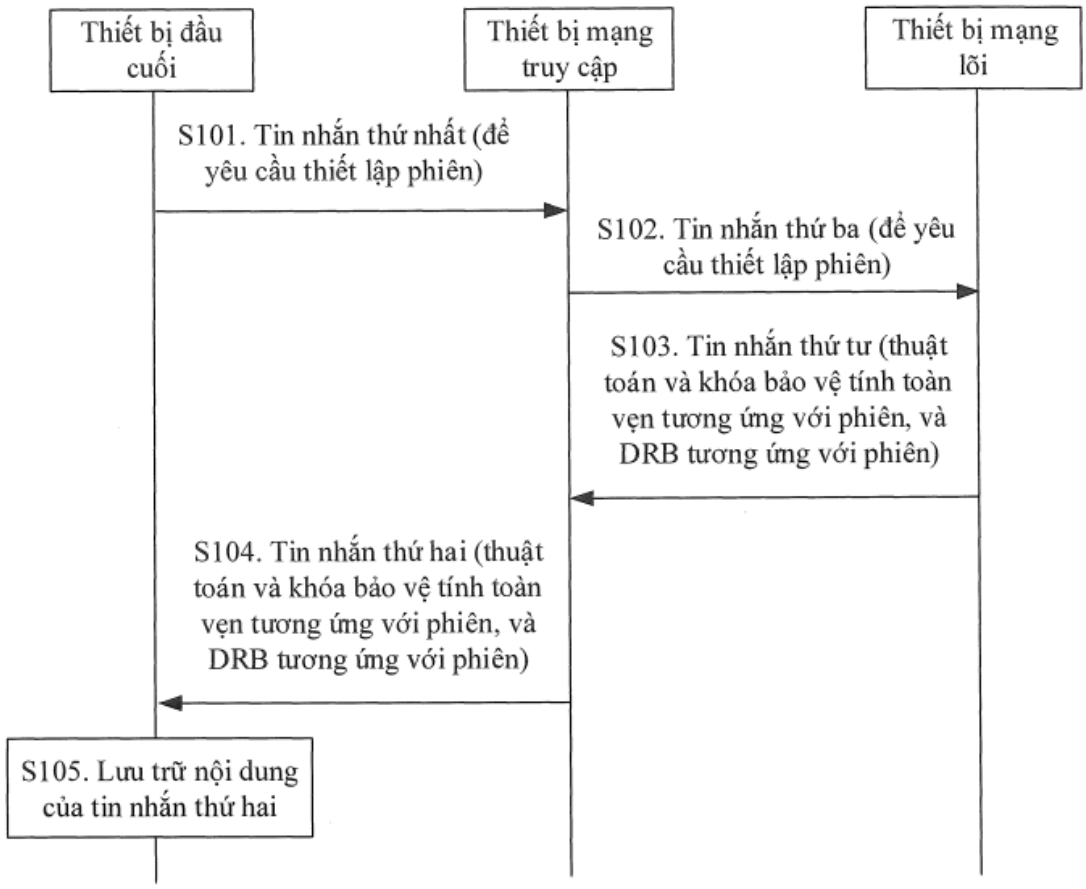

FIG.2

Lĩnh vực kỹ thuật được đề cập

Sáng chế này đề cập đến công nghệ truyền thông, và cụ thể, đến phương pháp và thiết bị bảo vệ tính toàn vẹn dữ liệu.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển nhanh chóng của các công nghệ truyền thông, vấn đề bảo mật thông tin của hệ thống truyền thông di động thu hút sự chú ý ngày càng tăng. Hệ thống Tiến hóa dài hạn (Long Term Evolution, LTE) được sử dụng làm ví dụ. Mục đích của chức năng bảo vệ tính toàn vẹn (Integrity Protection) trong hệ thống LTE là ngăn chặn dữ liệu người dùng bị giả mạo. Khi đầu nhận phát hiện ra lỗi kiểm tra tính toàn vẹn, thủ tục cập nhật khóa (Key) mã hóa/giải mã có thể được kích hoạt, để bảo vệ dữ liệu người dùng bằng cách sử dụng khóa mới.

Chức năng bảo vệ tính toàn vẹn bao gồm sự bảo vệ tính toàn vẹn và sự kiểm tra tính toàn vẹn. Chức năng bảo vệ tính toàn vẹn của LTE được triển khai tại lớp Giao thức hội tụ dữ liệu gói (Packet Data Convergence Protocol, PDCP). Trước khi mã hóa, đầu truyền thực hiện sự bảo vệ tính toàn vẹn trên cả tiêu đề (header) và phần dữ liệu của đơn vị dữ liệu giao thức PDCP (Protocol Data Unit, PDU). Cụ thể, tính toán đầu truyền, theo thuật toán bảo vệ tính toàn vẹn được tạo cấu hình bởi lớp giao thức trên, mã xác thực tin nhắn 32 bit (Mã xác thực tin nhắn cho tính toàn vẹn, Message Authentication Code for Integrity, MAC-I) bằng cách sử dụng ít nhất một trong các tham số chẳng hạn như khóa, giá trị đếm (COUNT), bộ nhận dạng sóng mang rađio, chiều (DIRECTION), bản thân tin nhắn, và độ dài của tin nhắn làm tham số đầu vào, và đặt mã xác thực tin nhắn 32 bit vào trường MAC-I của PDCP PDU. Sau khi nhận tin nhắn, đầu nhận tính toán, bằng cách sử dụng cùng phương pháp, mã xác thực dự kiến XMAC-I cho tin nhắn và thực hiện kiểm tra tính toàn vẹn bằng cách so sánh XMAC-I với MAC-I. Nếu MAC-I bằng với XMAC-I, đầu nhận xác định rằng sự kiểm tra

tính toàn vẹn thành công; hoặc nếu MAC-I không bằng XMAC-I, đầu nhận xác định rằng sự kiểm tra tính toàn vẹn không thành công.

Tuy nhiên, chức năng bảo vệ tính toàn vẹn trong hệ thống LTE nằm ở mức độ chi tiết của thiết bị đầu cuối. Nói cách khác, thiết bị đầu cuối sử dụng cùng một tham số bảo vệ tính toàn vẹn cho tất cả dữ liệu, gây ra sự bảo vệ tính toàn vẹn không linh hoạt.

Bản chất kỹ thuật của sáng chế

Sáng chế này đề xuất phương pháp và thiết bị bảo vệ tính toàn vẹn dữ liệu, để thực hiện sự bảo vệ tính toàn vẹn ở mức độ chi tiết của phiên hoặc ở mức độ chi tiết của luồng, sao cho sự bảo vệ tính toàn vẹn linh hoạt hơn và đáp ứng các yêu cầu bảo mật của cùng một người dùng cho các dịch vụ khác nhau.

Khía cạnh thứ nhất của sáng chế này đề xuất phương pháp bảo vệ tính toàn vẹn dữ liệu, bao gồm các bước: thu được, bởi thiết bị đầu cuối, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và DRB tương ứng với phiên; và thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn. Các thuật toán và các khóa bảo vệ tính toàn vẹn khác nhau có thể được sử dụng cho các phiên khác nhau, sao cho sự bảo vệ tính toàn vẹn linh hoạt hơn và đáp ứng các yêu cầu bảo mật của cùng một người dùng cho các dịch vụ khác nhau.

Tùy chọn, bước thu được, bởi thiết bị đầu cuối, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và DRB tương ứng với phiên cụ thể là: gửi, bởi thiết bị đầu cuối, tin nhắn thứ nhất, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên; và nhận, bởi thiết bị đầu cuối, tin nhắn thứ hai, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên; hoặc

tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Khía cạnh thứ hai của sáng chế này đề xuất phương pháp bảo vệ tính toàn vẹn dữ

liệu, bao gồm các bước: thu được, bởi thiết bị đầu cuối, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng; và thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn. Các thuật toán và các khóa bảo vệ tính toàn vẹn khác nhau cũng có thể được sử dụng cho các luồng khác nhau, sao cho sự bảo vệ tính toàn vẹn linh hoạt hơn và đáp ứng các yêu cầu bảo mật của cùng một người dùng cho các dịch vụ khác nhau.

Tùy chọn, bước thu được, bởi thiết bị đầu cuối, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với luồng cụ thể là: gửi, bởi thiết bị đầu cuối, tin nhắn thứ nhất, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên, và phiên tương ứng với luồng; và nhận, bởi thiết bị đầu cuối, tin nhắn thứ hai, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng; hoặc

tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Tùy chọn, trong khía cạnh thứ nhất và khía cạnh thứ hai của sáng chế này, phương pháp còn bao gồm bước: thu được, bởi thiết bị đầu cuối, ít nhất một trong các thông tin sau:

chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn, trong đó

chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo vệ tính toàn vẹn được thực hiện;

chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà thực hiện sự bảo vệ tính toàn vẹn;

chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không; và

chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng, hoặc dữ liệu mặt phẳng người

dùng và sự báo hiệu mặt phẳng điều khiển.

Tùy chọn, trong khía cạnh thứ nhất và khía cạnh thứ hai của sáng chế này, dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP của DRB.

Khi dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, phương pháp này còn bao gồm: đánh dấu, bởi thiết bị đầu cuối, bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP của DRB.

Khía cạnh thứ ba của sáng chế này đề xuất phương pháp bảo vệ tính toàn vẹn dữ liệu, bao gồm các bước: nhận, bởi thiết bị mạng truy cập, tin nhắn thứ nhất được gửi bởi thiết bị đầu cuối, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên; gửi, bởi thiết bị mạng truy cập, tin nhắn thứ ba đến thiết bị mạng lõi, trong đó tin nhắn thứ ba bao gồm tin nhắn thứ nhất; nhận, bởi thiết bị mạng truy cập, tin nhắn thứ tư được gửi bởi thiết bị mạng lõi, trong đó tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và DRB tương ứng với phiên; lưu trữ, bởi thiết bị mạng truy cập, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và DRB tương ứng với phiên; và gửi, bởi thiết bị mạng truy cập, tin nhắn thứ hai đến thiết bị đầu cuối, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên; hoặc tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Khía cạnh thứ tư của sáng chế này đề xuất phương pháp bảo vệ tính toàn vẹn dữ liệu, bao gồm các bước: nhận, bởi thiết bị mạng truy cập, tin nhắn thứ nhất được gửi bởi thiết bị đầu cuối, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên; gửi, bởi thiết bị mạng truy cập, tin nhắn thứ ba đến thiết bị mạng lõi, trong đó tin nhắn thứ ba bao gồm tin nhắn thứ nhất; nhận, bởi thiết bị mạng truy cập, tin nhắn thứ tư được gửi bởi thiết bị mạng lõi, trong đó tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với luồng, và phiên tương ứng với luồng; lưu trữ, bởi thiết bị mạng truy cập, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng; và gửi, bởi thiết bị mạng truy cập, tin nhắn thứ hai đến thiết bị đầu cuối, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của

phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng; hoặc tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Tùy chọn, trong khía cạnh thứ ba và khía cạnh thứ tư của sáng chế này, tin nhắn thứ ba hoặc tin nhắn thứ hai còn bao gồm ít nhất một trong các thông tin sau:

chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn, trong đó

chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo vệ tính toàn vẹn được thực hiện;

chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà thực hiện sự bảo vệ tính toàn vẹn;

chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không; và

chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng, hoặc dữ liệu mặt phẳng người dùng và sự báo hiệu mặt phẳng điều khiển.

Tùy chọn, trong khía cạnh thứ ba và khía cạnh thứ tư của sáng chế này, phương pháp còn bao gồm bước: thực hiện, bởi thiết bị mạng truy cập, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn.

Tùy chọn, trong khía cạnh thứ ba và khía cạnh thứ tư của sáng chế này, dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP của DRB.

Khi dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, phương pháp còn bao gồm: đánh dấu, bởi thiết bị mạng truy cập, bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP của DRB.

Khía cạnh thứ năm của sáng chế này đề xuất phương pháp bảo vệ tính toàn vẹn dữ liệu, bao gồm các bước: nhận, bởi thiết bị mạng lõi, tin nhắn thứ ba được gửi bởi thiết bị

mạng truy cập, trong đó tin nhắn thứ ba bao gồm tin nhắn thứ nhất, và tin nhắn thứ nhất được sử dụng để yêu cầu để thiết lập phiên; và gửi, bởi thiết bị mạng lõi, tin nhắn thứ tư đến thiết bị mạng truy cập, trong đó tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với phiên; hoặc bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng, trong đó phiên tương ứng với luồng.

Tùy chọn, tin nhắn thứ tư còn bao gồm ít nhất một trong các thông tin sau:

chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn, trong đó

chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo vệ tính toàn vẹn được thực hiện;

chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà thực hiện sự bảo vệ tính toàn vẹn;

chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không; và

chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng, hoặc dữ liệu mặt phẳng người dùng và sự báo hiệu mặt phẳng điều khiển.

Tùy chọn, phương pháp còn bao gồm bước: thực hiện, bởi thiết bị mạng lõi, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn.

Tùy chọn, dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP của DRB.

Khi dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, phương pháp còn bao gồm: đánh dấu, bởi thiết bị mạng lõi, bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP của DRB.

Khía cạnh thứ sáu của sáng chế này cung cấp thiết bị đầu cuối, bao gồm: môđun thu được, được tạo cấu hình để thu được thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với phiên; và môđun bảo vệ tính toàn vẹn, được tạo cấu hình để thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn.

Tùy chọn, môđun thu được được tạo cấu hình cụ thể để: gửi tin nhắn thứ nhất, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên; và nhận tin nhắn thứ hai, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên; hoặc tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Khía cạnh thứ bảy của sáng chế này cung cấp thiết bị đầu cuối, bao gồm: môđun thu được, được tạo cấu hình để cthu ó được thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với luồng; và môđun bảo vệ tính toàn vẹn, được tạo cấu hình để thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn.

Tùy chọn, môđun thu được được tạo cấu hình cụ thể để: gửi tin nhắn thứ nhất, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên, và phiên tương ứng với luồng; và nhận tin nhắn thứ hai, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng; hoặc tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Tùy chọn, trong khía cạnh thứ sáu và khía cạnh thứ bảy của sáng chế này, môđun thu được còn được tạo cấu hình để: thu được ít nhất một trong các thông tin sau:

chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn, trong đó

chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo vệ tính toàn vẹn được thực hiện;

chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà thực hiện sự bảo vệ tính toàn vẹn;

chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không; và

chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng, hoặc dữ liệu mặt phẳng người dùng và sự báo hiệu mặt phẳng điều khiển.

Tùy chọn, trong khía cạnh thứ sáu và khía cạnh thứ bảy của sáng chế này, dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP của DRB.

Khi dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, thiết bị đầu cuối còn bao gồm: môđun đánh dấu, được tạo cấu hình để đánh dấu bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP của DRB.

Khía cạnh thứ tám của sáng chế này cung cấp thiết bị mạng truy cập, bao gồm:

môđun nhận, được tạo cấu hình để nhận tin nhắn thứ nhất được gửi bởi thiết bị đầu cuối, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên;

môđun gửi, được tạo cấu hình để gửi tin nhắn thứ ba đến thiết bị mạng lõi, trong đó tin nhắn thứ ba bao gồm tin nhắn thứ nhất, trong đó

môđun nhận còn được tạo cấu hình để nhận tin nhắn thứ tư được gửi bởi thiết bị mạng lõi, trong đó tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với phiên; và

môđun lưu trữ, được tạo cấu hình để lưu trữ thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và DRB tương ứng với phiên, trong đó

môđun gửi còn được tạo cấu hình để gửi tin nhắn thứ hai đến thiết bị đầu cuối, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên; hoặc tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Khía cạnh thứ chín của sáng chế này cung cấp thiết bị mạng truy cập, bao gồm:

môđun nhận, được tạo cấu hình để nhận tin nhắn thứ nhất được gửi bởi thiết bị đầu

cuối, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên;

môđun gửi, được tạo cấu hình để gửi tin nhắn thứ ba đến thiết bị mạng lõi, trong đó tin nhắn thứ ba bao gồm tin nhắn thứ nhất, trong đó

môđun nhận còn được tạo cấu hình để nhận tin nhắn thứ tư được gửi bởi thiết bị mạng lõi, trong đó tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với luồng, và phiên tương ứng với luồng; và

môđun lưu trữ, được tạo cấu hình để lưu trữ thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng, trong đó

môđun gửi còn được tạo cấu hình để gửi tin nhắn thứ hai đến thiết bị đầu cuối, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng; hoặc

tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Trong khía cạnh thứ tám và khía cạnh thứ chín của sáng chế này, tin nhắn thứ ba hoặc tin nhắn thứ hai còn bao gồm ít nhất một trong các thông tin sau:

chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn, trong đó

chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo vệ tính toàn vẹn được thực hiện;

chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà thực hiện sự bảo vệ tính toàn vẹn;

chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không; và

chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng, hoặc dữ liệu mặt phẳng người

dùng và sự báo hiệu mặt phẳng điều khiển.

Tùy chọn, thiết bị mạng truy cập còn bao gồm: môđun bảo vệ tính toàn vẹn, được tạo cấu hình để thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn.

Tùy chọn, dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP của DRB.

Khi dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, thiết bị mạng truy cập còn bao gồm: môđun đánh dấu, được tạo cấu hình để đánh dấu bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP của DRB.

Khía cạnh thứ mười của sáng chế này cung cấp thiết bị mạng lõi, bao gồm:

môđun nhận, được tạo cấu hình để nhận tin nhắn thứ ba được gửi bởi thiết bị mạng truy cập, trong đó tin nhắn thứ ba bao gồm tin nhắn thứ nhất, và tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên; và

môđun gửi, được tạo cấu hình để gửi tin nhắn thứ tư đến thiết bị mạng truy cập, trong đó tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với phiên; hoặc bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng, trong đó phiên tương ứng với luồng.

Tùy chọn, tin nhắn thứ tư còn bao gồm ít nhất một trong các thông tin sau:

chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn, trong đó

chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo vệ tính toàn vẹn được thực hiện;

chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà thực hiện sự bảo vệ tính toàn vẹn;

chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không; và

chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng, hoặc dữ liệu mặt phẳng người dùng và sự báo hiệu mặt phẳng điều khiển.

Tùy chọn, thiết bị mạng lõi còn bao gồm: môđun bảo vệ tính toàn vẹn, được tạo cấu

hình để thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn.

Tùy chọn, dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP của DRB.

Khi dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, thiết bị mạng lõi còn bao gồm: môđun đánh dấu, được tạo cấu hình để đánh dấu bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP của DRB.

Khía cạnh thứ mười một của sáng chế này cung cấp thiết bị đầu cuối, bao gồm: bộ xử lý, bộ nhớ, bộ nhận, và bộ truyền, trong đó bộ nhớ, bộ nhận, và bộ truyền được kết nối và truyền thông với bộ xử lý bằng cách sử dụng bus, bộ nhớ được tạo cấu hình để lưu trữ lệnh có thể thực thi trên máy tính, và bộ xử lý được tạo cấu hình để thực thi lệnh có thể thực thi trên máy tính, sao cho thiết bị đầu cuối thực hiện các phương pháp được cung cấp theo khía cạnh thứ nhất và khía cạnh thứ hai.

Khía cạnh thứ mười hai của sáng chế này cung cấp thiết bị mạng truy cập, bao gồm: bộ xử lý, bộ nhớ, bộ nhận, và bộ truyền, trong đó bộ nhớ, bộ nhận, và bộ truyền được kết nối và truyền thông với bộ xử lý bằng cách sử dụng bus, bộ nhớ được tạo cấu hình để lưu trữ có thể thực thi trên máy tính, và bộ xử lý được tạo cấu hình để thực thi có thể thực thi trên máy tính, sao cho thiết bị mạng truy cập thực hiện các phương pháp được cung cấp theo khía cạnh thứ ba và khía cạnh thứ tư.

Khía cạnh thứ mười ba của sáng chế này cung cấp thiết bị mạng lõi, bao gồm: bộ xử lý, bộ nhớ, bộ nhận, và bộ truyền, trong đó bộ nhớ, bộ nhận,và bộ truyền được kết nối và truyền thông với bộ xử lý bằng cách sử dụng bus, bộ nhớ được tạo cấu hình để lưu trữ lệnh có thể thực thi trên máy tính, và bộ xử lý được tạo cấu hình để thực có thể thực thi trên máy tính, để thiết bị mạng lõi thực hiện phương pháp được cung cấp theo khía cạnh thứ năm.

Khía cạnh thứ mười bốn của sáng chế này cung cấp phương tiện đọc được bằng máy tính, trong đó phương tiện đọc được bằng máy tính bao gồm lệnh có thể thực thi trên máy tính, và lệnh có thể thực thi trên máy tính được sử dụng để cho phép thiết bị đầu cuối thực hiện các phương pháp được cung cấp theo khía cạnh thứ nhất và khía cạnh thứ hai của sáng chế này.

Khía cạnh thứ mười lăm của sáng chế này cung cấp phương tiện đọc được bằng máy tính, trong đó phương tiện đọc được bằng máy tính bao gồm lệnh có thể thực thi trên máy tính, và lệnh có thể thực thi trên máy tính được sử dụng để cho phép thiết bị mạng truy cập

thực hiện các phương pháp được cung cấp theo khía cạnh thứ ba và khía cạnh thứ tư của sáng chế này.

Khía cạnh thứ mười sáu của sáng chế này cung cấp phương tiện đọc được bằng máy tính, trong đó phương tiện đọc được bằng máy tính bao gồm lệnh có thể thực thi trên máy tính, và lệnh có thể thực thi trên máy tính được sử dụng để cho phép thiết bị mạng lõi thực hiện phương pháp được cung cấp theo khía cạnh thứ năm của sáng chế này.

Khía cạnh thứ mười bảy của sáng chế này cung cấp hệ thống trên chip. Hệ thống có thể được áp dụng cho thiết bị đầu cuối, và hệ thống trên chip bao gồm: ít nhất một giao diện truyền thông, ít nhất một bộ xử lý, và ít nhất một bộ nhớ, trong đó giao diện truyền thông, bộ nhớ, và bộ xử lý được kết nối với nhau bằng cách sử dụng bus, và bộ xử lý dẫn ra lệnh được lưu trữ trong bộ nhớ, để thực hiện các phương pháp được cung cấp theo khía cạnh thứ nhất và khía cạnh thứ hai của sáng chế này.

Khía cạnh thứ mười tám của sáng chế này cung cấp hệ thống trên chip. Hệ thống có thể được áp dụng cho thiết bị mạng truy cập, và hệ thống trên chip bao gồm: ít nhất một giao diện truyền thông, ít nhất một bộ xử lý, và ít nhất một bộ nhớ, trong đó giao diện truyền thông, bộ nhớ, và bộ xử lý được kết nối với nhau bằng cách sử dụng bus, và bộ xử lý dẫn ra lệnh được lưu trữ trong bộ nhớ, để thực hiện các phương pháp được cung cấp theo khía cạnh thứ ba và khía cạnh thứ tư của sáng chế này.

Khía cạnh thứ mười chín của sáng chế này cung cấp hệ thống trên chip. Hệ thống có thể được áp dụng cho thiết bị mạng lõi, và hệ thống trên chip bao gồm: ít nhất một giao diện truyền thông, ít nhất một bộ xử lý, và ít nhất một bộ nhớ, trong đó giao diện truyền thông, bộ nhớ, và bộ xử lý được kết nối với nhau bằng cách sử dụng bus, và bộ xử lý dẫn ra lệnh được lưu trữ trong bộ nhớ, để thực hiện phương pháp được cung cấp theo khía cạnh thứ năm của sáng chế này.

Khía cạnh thứ hai mươi của sáng chế này cung cấp sản phẩm chương trình, trong đó sản phẩm chương trình bao gồm chương trình máy tính, chương trình máy tính được lưu trữ trong phương tiện lưu trữ có thể đọc được, và ít nhất một bộ xử lý của thiết bị đầu cuối thực thi chương trình máy tính, sao cho thiết bị đầu cuối thực hiện các phương pháp được cung cấp theo khía cạnh thứ nhất và khía cạnh thứ hai của sáng chế này.

Khía cạnh thứ hai mươi mốt của sáng chế này cung cấp sản phẩm chương trình, trong đó sản phẩm chương trình bao gồm chương trình máy tính, chương trình máy tính được lưu trữ trong phương tiện lưu trữ có thể đọc được, và ít nhất một bộ xử lý của thiết bị mạng truy

cập thực thi chương trình máy tính, sao cho thiết bị mạng truy cập thực hiện các phương pháp được cung cấp theo khía cạnh thứ ba và khía cạnh thứ tư của sáng chế này.

Khía cạnh thứ hai mươi hai của sáng chế này cung cấp sản phẩm chương trình, trong đó sản phẩm chương trình bao gồm chương trình máy tính, chương trình máy tính được lưu trữ trong phương tiện lưu trữ có thể đọc được, và ít nhất một bộ xử lý của thiết bị mạng lõi thực thi chương trình máy tính, sao cho thiết bị mạng lõi thực hiện phương pháp được cung cấp theo khía cạnh thứ năm của sáng chế này.

Sáng chế này đề xuất phương pháp và thiết bị bảo vệ tính toàn vẹn dữ liệu. Thiết bị đầu cuối thu được thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và DRB tương ứng với phiên, và thực hiện, bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB tương ứng đến phiên; hoặc thiết bị đầu cuối thu được thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng, và thực hiện, bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB tương ứng với luồng. Một phiên bao gồm nhiều luồng, các thuật toán và khóa bảo vệ tính toàn vẹn khác nhau có thể được sử dụng cho các phiên khác nhau, và các thuật toán và khóa bảo vệ tính toàn vẹn khác nhau cũng có thể được sử dụng cho các luồng khác nhau, sao cho sự bảo vệ tính toàn vẹn linh hoạt hơn và đáp ứng các yêu cầu bảo mật của cùng một người dùng cho các dịch vụ khác nhau.

MÔ TẢ VẮN TẮT CÁC HÌNH VẼ

Fig. 1 là sơ đồ kiến trúc phác họa của kịch bản ứng dụng theo sáng chế này;

Fig. 2 là biểu đồ tiến trình sự báo hiệu của phương pháp bảo vệ tính toàn vẹn dữ liệu theo phương án 1 của sáng chế này;

Fig. 3 là sơ đồ phác họa các lớp giao thức của hệ thống 5G;

Fig. 4 là biểu đồ tiến trình sự báo hiệu của phương pháp bảo vệ tính toàn vẹn dữ liệu theo phương án 2 của sáng chế này;

Fig. 5 là sơ đồ phác họa của MAC-I khi sự bảo vệ tính toàn vẹn được thực hiện ở lớp PDCP;

Fig. 6 là sơ đồ cấu trúc phác họa của thiết bị đầu cuối theo phương án 3 của sáng chế này;

Fig. 7 là sơ đồ cấu trúc phác họa của thiết bị mạng truy cập theo phương án 5 của sáng chế này;

Fig. 8 là sơ đồ cấu trúc phác họa của thiết bị mạng lõi theo phương án 7 của sáng chế này;

Fig. 9 là sơ đồ cấu trúc phác họa của thiết bị đầu cuối theo phương án 8 của sáng chế này;

Fig. 10 là sơ đồ cấu trúc phác họa của thiết bị mạng truy cập theo phương án 9 của sáng chế này; và

Fig. 11 là sơ đồ cấu trúc phác họa của thiết bị mạng lõi theo phương án 10 của sáng chế này.

MÔ TẢ CHI TIẾT SÁNG CHẾ

Sáng chế này đề xuất phương pháp bảo vệ tính toàn vẹn dữ liệu, có thể được áp dụng cho nhiều loại hệ thống truyền thông. Hệ thống truyền thông có thể là hệ thống viễn thông di động toàn cầu (Universal Mobile Telecommunications System, UMTS), hệ thống đa truy cập phân chia mã (Code Division Multiple Access, CDMA), hệ thống đa truy cập phân chia mã băng rộng (Wideband Code Division Multiple Access, WCDMA), mạng cục bộ không dây (Wireless Local Area Network, WLAN), hệ thống tiến hóa dài hạn (Long Term Evolution, LTE), hoặc hệ thống truyền thông di động thế hệ thứ năm (5th-Generation, 5G).

Fig. 1 là sơ đồ kiến trúc phác họa của kịch bản ứng dụng theo sáng chế này. Như được thể hiện trên Fig.1, hệ thống 5G có thể bao gồm: mạng truy cập (vô tuyến) ((Radio) Access Network, (R)AN), mạng lõi (Core Network, CN), và thiết bị đầu cuối. RAN chịu trách nhiệm cho sự truy cập của thiết bị đầu cuối. Nhiều thiết bị đầu cuối được bao gồm trong vùng phủ sóng của RAN. Giao diện giữa RAN và CN là giao diện NG. Giao diện giữa các phần tử mạng RAN là giao diện Xn. Giao diện giữa phần tử mạng RAN và thiết bị đầu cuối là giao diện không khí. Phần tử mạng RAN có thể là trạm cơ sở trong hệ thống UMTS, trạm cơ sở (Trạm truyền nhận cơ sở, Base Transceiver Station, BTS) trong hệ thống CDMA, trạm cơ sở (NodeB, NB) trong hệ thống WCDMA, trạm cơ sở đã phát triển (evolved NodeB, eNB) hoặc trạm chuyển tiếp trong hệ thống LTE, điểm truy cập (access point, AP) trong mạng WLAN, trạm cơ sở (ví dụ, gNB hoặc điểm truyền (Transmission Point, TRP)) trong hệ thống 5G, hoặc tương tự. Hệ thống 5G cũng được gọi là hệ thống truyền thông vô

tuyến mới, công nghệ vô tuyến mới (New Radio), hoặc hệ thống truyền thông di động thế hệ tiếp theo. Trong hệ thống truyền thông di động thế hệ tiếp theo, kiến trúc chất lượng dịch vụ (Quality of Service, QoS) dựa trên luồng được đưa ra. Luồng là, ví dụ, luồng QoS. QoS được phân loại thành QoS lớp tầng không truy cập (Non-access stratum, NAS) QoS lớp tầng truy cập (access stratum, AS) QoS. QoS lớp NAS ở mức luồng QoS. Luồng QoS là mức độ chi tiết tối thiểu cho sự phân biệt QoS trong phiên (session) đơn vị dữ liệu giao thức (Protocol Data Unit, PDU), và là tập hợp các gói dữ liệu. Việc xử lý tương tự được thực hiện trên các gói dữ liệu mà được bao gồm trong một luồng QoS duy nhất.

Các phần tử mạng CN bao gồm thực thể chức năng quản lý truy cập và di động (Access and Mobility Management Function, AMF) và thực thể chức năng mặt phẳng người dùng (User Plane Function, UPF). Thực thể AMF chịu trách nhiệm chính cho các dịch vụ chẳng hạn như quản lý di động và quản lý truy cập, và tương đương với các chức năng của thực thể quản lý di động (Mobility Management Entity, MME) trong hệ thống LTE ngoại trừ chức năng quản lý phiên. UPF tương đương với cổng mạng dữ liệu gói (Packet Data Network Gateway, P-GW) trong hệ thống LTE, và chịu trách nhiệm cho các chức năng chẳng hạn như quản lý phiên và bộ mang và phân bổ địa chỉ giao thức Internet (Internet Protocol, IP). UPF tạo ra luồng QoS đường xuống, và UE tạo luồng QoS đường lên.

Tùy chọn, các phần tử mạng CN có thể còn bao gồm thực thể chức năng quản lý phiên (Session Management Function, SMF), thực thể chức năng máy chủ xác thực (Authentication Server Function, AUSF)/thực thể chức năng xử lý và kho lưu trữ chứng nhận xác (Authentication Credential Repository and Processing Function, ARPF), thực thể chức năng kiểm soát chính sách (Policy Control Function, PCF), và máy chủ xác thực, ủy quyền và tính toán (Authentication, Authorization and Accounting, AAA).

Thực thể SMF chịu trách nhiệm chính cho việc thiết lập phiên, sửa đổi phiên, hoặc phát hành phiên. Thực thể PCF chịu trách nhiệm chính cho việc cung cấp chính sách cho mạng. Máy chủ AAA chịu trách nhiệm chính cho việc xác thực thẻ môđun nhận dạng thuê bao (Subscriber Identification Module, SIM), ủy quyền các dịch vụ mà có thể được sử dụng bởi thẻ SIM, và ghi lại tài nguyên mạng được sử dụng bởi thẻ SIM. Máy chủ AAA có thể được cung cấp bởi nhà điều hành, hoặc có thể được cung cấp bởi bên thứ ba. AUSF là điểm kết thúc của tin nhắn yêu cầu xác thực, và tương tác với thực thể ARPF để thu được thông tin bảo mật dài hạn (long-term security credential) của thiết bị đầu cuối. Thực thể ARPF chịu trách nhiệm chính cho việc lưu trữ thông tin bảo mật dài hạn (long-term security

credential) của thiết bị đầu cuối.

Khi phương pháp trong sáng chế này được áp dụng cho hệ thống LTE, thực thể AMF và thực thể SMF có thể được thay thế với MME, thực thể UPF có thể được thay thế với thực thể P-GW và thực thể cổng phục vụ (Serving Gateway, S-GW) trong hệ thống LTE, và thực thể AUSF và thực thể ARPF có thể được thay thế với máy chủ thuê bao gia đình (Home Subscriber Server, HSS). Các HSS được tạo cấu hình để lưu trữ thông tin thuê bao. Thông tin thuê bao có thể là thông tin thuê bao của thẻ SIM. MME là phần tử mạng quản lý sự báo hiệu, và chịu trách nhiệm cho việc mã hóa sự báo hiệu NAS, phân bổ mã nhận dạng tạm thời cho thiết bị đầu cuối, lựa chọn các phần tử mạng CN chẳng hạn như SGW và PGW, và cung cấp các chức năng chẳng hạn như chuyển vùng, theo dõi, và bảo mật. SGW là mẩu neo di động cho sự chuyển giao giữa các eNB, và cung cấp các chức năng liên quan đến đánh chặn hợp pháp. PGW chịu trách nhiệm cho các chức năng chẳng hạn như phân bổ địa chỉ IP, kiểm soát giải pháp, nạp cưỡng bức quy tắc, và đánh chặn hợp pháp.

Thiết bị đầu cuối trong sáng chế này có thể là thiết bị đầu cuối không dây. Thiết bị đầu cuối không dây có thể là thiết bị mà cung cấp cho người dùng kết nối giọng nói và/hoặc dữ liệu, thiết bị cầm tay có chức năng kết nối không dây, hoặc thiết bị xử lý khác được kết nối với modem không dây. Thiết bị đầu cuối không dây có thể truyền thông với ít nhất một mạng lõi thông qua (R)AN. Thiết bị đầu cuối không dây có thể là thiết bị đầu cuối di động, chẳng hạn như điện thoại di động (mobile phone) (hoặc cũng được gọi là điện thoại "di động"("cellular")) hoặc máy tính mà có thiết bị đầu cuối di động. Ví dụ, thiết bị đầu cuối không dây có thể là thiết bị di động, bỏ túi, cầm tay, máy tính tích hợp, hoặc thiết bị di động trên xe, mà trao đổi giọng nói và/hoặc dữ liệu với mạng truy cập vô tuyến. Thiết bị đầu cuối không dây cũng có thể được gọi là đơn vị thuê bao (Subscriber Unit), trạm thuê bao (Subscriber Station), trạm di động (Mobile Station), trạm di động (Mobile Station), trạm từ xa (Remote Station), điểm truy cập (Access Point), thiết bị đầu cuối từ xa (Remote Terminal), thiết bị đầu cuối truy cập (Access Terminal), thiết bị đầu cuối người dùng (User Terminal), thiết bị người dùng (User Equipment, UE), hoặc tác nhân người dùng (User Agent). Điều này không bị giới hạn ở đây.

Dựa trên hệ thống truyền thông được thể hiện trên Fig.1, phương pháp bảo vệ tính toàn vẹn dữ liệu được cung cấp trong sáng chế này là để giải quyết vấn đề bảo vệ tính toàn vẹn không linh hoạt trong tình trạng kỹ thuật.

Dưới đây sử dụng các phương án cụ thể để chi tiết các giải pháp kỹ thuật của sáng

chế này và cách các giải pháp kỹ thuật của sáng chế này được sử dụng để giải quyết vấn đề kỹ thuật đã nói ở trên. Một vài phương án cụ thể sau đây có thể được kết hợp, và một khái niệm hoặc quy trình giống nhau hoặc tương tự có thể không được mô tả lặp đi lặp lại trong một số phương án. Dưới đây mô tả các phương án của sáng chế này với sự tham chiếu đến các bản vẽ đi kèm.

Fig. 2 là biểu đồ tiến trình sự báo hiệu của phương pháp bảo vệ tính toàn vẹn dữ liệu theo phương án 1 của sáng chế này. Phương pháp trong phương án này có thể chủ yếu bao gồm các bước sau.

Bước S101: Thiết bị đầu cuối gửi tin nhắn thứ nhất đến thiết bị mạng truy cập.

Tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên. Phiên này cũng được gọi là phiên PDU. Tin nhắn thứ nhất có thể mang tin nhắn NAS. Tin nhắn NAS mang tin nhắn yêu cầu thiết lập phiên. Tin nhắn yêu cầu thiết lập phiên bao gồm bộ nhận dạng của phiên được thiết lập. Tin nhắn yêu cầu thiết lập phiên có thể còn bao gồm bộ phân biệt giao thức (Protocol discriminator), được sử dụng để chỉ báo ngăn xếp giao thức L3 tương ứng với tin nhắn thứ nhất. Nếu tin nhắn yêu cầu thiết lập phiên được thực hiện bằng cách sử dụng tin nhắn NAS, mạng truy cập sẽ bổ sung tin nhắn NAS vào tin nhắn thứ ba và gửi tin nhắn thứ ba đến thiết bị mạng lõi.

Ví dụ, tin nhắn thứ nhất có thể là tin nhắn điều khiển tài nguyên vô tuyến (Radio Resource Control, RRC), tin nhắn Điều khiển truy cập phương tiện (Media Access Control, MAC), tin nhắn lớp vật lý, hoặc tương tự. Tin nhắn RRC, ví dụ, yêu cầu thiết lập kết nối RRC, yêu cầu thiết lập lại kết nối RRC, tin nhắn hoàn thành thiết lập kết nối RRC, hoặc tương tự. Tin nhắn MAC là, ví dụ, phần tử điều khiển (Control Element, CE) MAC. Tin nhắn lớp vật lý là, ví dụ, sự báo hiệu lớp vật lý.

Bước S102: Thiết bị mạng truy cập gửi tin nhắn thứ ba đến thiết bị mạng lõi, trong đó tin nhắn thứ ba bao gồm tin nhắn thứ nhất.

Tin nhắn thứ ba được sử dụng để yêu cầu thiết lập phiên. Cụ thể, sau khi nhận tin nhắn thứ nhất, thiết bị mạng truy cập sẽ bổ sung tin nhắn NAS trong tin nhắn thứ nhất vào tin nhắn thứ ba và gửi tin nhắn thứ ba đến thiết bị mạng lõi. Tin nhắn thứ ba là tin nhắn giao diện giữa RAN và CN.

Bước S103: Thiết bị mạng lõi gửi tin nhắn thứ tư đến thiết bị mạng truy cập, trong đó tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và sóng mang rađio dữ liệu (Data Radio Bearer, DRB) tương ứng với phiên.

Tin nhắn thứ tư được sử dụng để yêu cầu thiết bị mạng truy cập chuẩn bị tài nguyên cho phiên được thiết lập. Tin nhắn thứ tư có thể là tin nhắn yêu cầu thiết lập bối cảnh ban đầu của UE, được sử dụng để thiết lập cấu hình bối cảnh cho UE; hoặc tin nhắn thứ tư là tin nhắn yêu cầu thiết lập tài nguyên phiên PDU, được sử dụng để tạo cấu hình tài nguyên cho phiên. Tin nhắn thứ tư mang thông tin phiên và cấu hình bảo vệ tính toàn vẹn tương ứng với phiên. Thông tin phiên bao gồm bộ nhận dạng của phiên và DRB tương ứng với phiên. Tùy chọn, tin nhắn thứ tư mang tin nhắn NAS, và cấu hình bảo vệ tính toàn vẹn tương ứng với phiên được mang trong tin nhắn NAS. Chắc chắn, cấu hình bảo vệ tính toàn vẹn tương ứng với phiên có thể không được thực hiện trong tin nhắn NAS.

Tin nhắn thứ tư bao gồm tham số cấu hình của ít nhất một lớp giao thức, được sử dụng để thiết lập một hoặc nhiều DRB cho phiên, để thực hiện một dịch vụ được khởi tạo bởi thiết bị đầu cuối. Fig.3 là sơ đồ phác họa các lớp giao thức của hệ thống 5G. Như được thể hiện trên Fig.3, từ trên xuống dưới, các lớp giao thức của thiết bị đầu cuối và thiết bị truy cập tuần tự là lớp giao thức tổng hợp dữ liệu dịch vụ (Service Data Aggregation Protocol, SDAP), lớp PDCP, lớp điều khiển liên kết vô tuyến (Radio Link Control, RLC), lớp MAC, và lớp vật lý (Physical, PHY). Lớp SDAP là lớp giao thức mới được bổ sung vào hệ thống LTE. Lớp SDAP được sử dụng để xử lý ánh xạ từ luồng (flow) sang DRB. Trong phương án này, một thiết bị đầu cuối có thể thiết lập nhiều phiên, mỗi phiên bao gồm một hoặc nhiều luồng, mỗi luồng có thể được ánh xạ tới một hoặc nhiều DRB, và luồng là, ví dụ, luồng QoS.

Ví dụ, tham số cấu hình của ít nhất một lớp giao thức bao gồm tham số của ngăn xếp giao thức của mỗi lớp, chế độ truyền, cấu hình kênh logic, và tham số liên quan đến lập lịch. Chế độ truyền có thể là chế độ truyền trong suốt RLC, chế độ được xác nhận, hoặc chế độ chưa được xác nhận. Cấu hình kênh logic là, ví dụ, quyền ưu tiên kênh logic. Đối với nội dung cụ thể, tham khảo các giao thức LTE hoặc 5G. Các chi tiết không được mô tả ở đây.

Trong phương án này, cấu hình bảo vệ tính toàn vẹn tương ứng với phiên được mang trong tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên. Tùy chọn, tin nhắn thứ tư có thể không mang thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên được thực hiện bằng cách sử dụng một tin nhắn khác, hoặc thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên được tạo cấu hình trước. Tin nhắn thứ tư có thể còn bao gồm ít nhất một trong các thông tin sau: chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp

giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn. Tương tự, một hoặc nhiều chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn có thể được tạo cấu hình trước, thay vì được chỉ ra động bằng cách sử dụng tin nhắn thứ tư.

Chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo vệ tính toàn vẹn được thực hiện. Sự bảo vệ tính toàn vẹn có thể được thực hiện trên phía RAN, hoặc được thực hiện trên phía CN, hoặc được thực hiện trên cả phía RAN và phía CN, hoặc tương tự. Do đó, phần tử mạng cho sự bảo vệ tính toàn vẹn có thể là thiết bị mạng truy cập hoặc thiết bị mạng lõi, hoặc sự bảo vệ tính toàn vẹn có thể được thực hiện ở cả thiết bị mạng truy cập và thiết bị mạng lõi. Khi vị trí bảo vệ tính toàn vẹn là phía RAN, chức năng bảo vệ tính toàn vẹn được thực hiện bởi ngăn xếp giao thức ở phía RAN, và phía thiết bị đầu cuối tương ứng thực hiện chức năng bảo vệ tính toàn vẹn ở tầng truy cập. Khi vị trí bảo vệ tính toàn vẹn là phía CN, chức năng bảo vệ tính toàn vẹn cần được thực hiện bởi ngăn xếp giao thức ở phía CN, và phía thiết bị đầu cuối tương ứng thực hiện chức năng bảo vệ tính toàn vẹn ở tầng không truy cập. Khi vị trí bảo vệ tính toàn vẹn là cả phía RAN và phía CN, chức năng bảo vệ tính toàn vẹn cần được thực hiện ở cả phía RAN và phía CN, và sự bảo vệ tính toàn vẹn của mặt phẳng điều khiển hoặc mặt phẳng dữ liệu của người dùng cần được thực hiện hai lần.

Chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà sự bảo vệ tính toàn vẹn được thực hiện. Lớp giao thức để bảo vệ tính toàn vẹn có thể là lớp SDAP, lớp PDCP, hoặc lớp RLC.

Chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không. Chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được liên kết với chỉ báo của vị trí bảo vệ tính toàn vẹn. Ví dụ, nếu vị trí bảo vệ tính toàn vẹn được chỉ ra bởi chỉ báo của vị trí bảo vệ tính toàn vẹn là phía RAN, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng chức năng bảo vệ tính toàn vẹn được cho phép hoặc không được cho phép ở phía RAN. Nếu vị trí bảo vệ tính toàn vẹn chỉ ra bởi chỉ báo của vị trí bảo vệ tính toàn vẹn là cả bên RAN và bên CN, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng chức năng bảo vệ tính toàn vẹn cho phép hoặc không được cho phép ở phía RAN và phía CN.

Chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng

cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng (User plane, UP), hoặc dữ liệu mặt phẳng người dùng và mặt phẳng điều khiển (Control Plane, CP).

Các thuật toán và các khóa bảo vệ tính toàn vẹn giống nhau hoặc khác nhau có thể được sử dụng cho các phiên khác nhau. Thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với vị trí bảo vệ tính toàn vẹn. Ví dụ, nếu thiết bị mạng lõi chỉ chỉ ra một vị trí bảo vệ tính toàn vẹn (phía RAN hoặc phía CN), thuật toán và khóa bảo vệ tính toàn vẹn tương ứng chỉ được tạo cấu hình ở vị trí bảo vệ tính toàn vẹn. Nếu thiết bị mạng lõi chỉ ra hai vị trí bảo vệ tính toàn vẹn (cả phía RAN và phía CN), thuật toán và khóa bảo vệ tính toàn vẹn tương ứng cần được tạo cấu hình cho hai vị trí bảo vệ tính toàn vẹn, và các thuật toán và khóa bảo vệ tương ứng với hai tính toàn vẹn vị trí bảo vệ có thể giống hoặc khác nhau.

Theo một cách thức, các khóa được sử dụng cho các phiên khác nhau có thể được thu được thông qua sự tính toán dựa trên khóa gốc (root key). Các khóa được thu được cho các phiên khác nhau có thể khác nhau hoặc giống nhau. Khóa gốc có thể là khóa gốc được thu được từ thiết bị mạng truy cập trong thủ tục SMC.

Theo một cách thức khác, các khóa được sử dụng cho các phiên khác nhau có thể được thu được thông qua sự tính toán dựa trên các khóa gốc khác nhau. Ví dụ, tin nhắn thứ tư chỉ ra khóa gốc được sử dụng cho phiên, hoặc chuyển giao tham số liên quan, sao cho thiết bị mạng truy cập tính toán, dựa trên khóa gốc, khóa được sử dụng cho phiên.

Trong phương án này, cấu hình bảo vệ tính toàn vẹn tương ứng với phiên có thể được đặt trong danh sách thông tin phiên PDU (danh sách thiết lập tài nguyên phiên PDU, PDU Session Resource Setup List) trong tin nhắn thứ tư, để chỉ ra cấu hình bảo vệ tính toàn vẹn tương ứng với phiên, hoặc có thể được đặt riêng trong tin nhắn thứ tư, với bộ nhận dạng phiên tương ứng với cấu hình bảo vệ tính toàn vẹn được bổ sung. Thiết bị mạng truy cập tìm hiểu về cấu hình bảo vệ tính toàn vẹn tương ứng với phiên từ tin nhắn thứ tư, và tìm hiểu thêm về cấu hình bảo vệ tính toàn vẹn của DRB tương ứng với phiên. Bảng 1 là sơ đồ cấu trúc phác họa của tin nhắn thứ tư, bảng 2 là sơ đồ nguyên lý của danh sách thông tin phiên PDU và bảng 3 là sơ đồ nguyên lý của sự chuyển giao yêu cầu thiết lập phiên PDU (PDU Session Setup Request Transfer). Tin nhắn thứ tư trong bảng 1 là, ví dụ, tin nhắn yêu cầu thiết lập tài nguyên phiên PDU trong phần 9.2.1.1 của giao thức ứng dụng RAN NG (NG Application Protocol, NGAP) thế hệ tiếp theo (Next Generation, NG) dự án hợp tác thế hệ thứ 3 (rd Generation Partnership Project, 3GPP mà số phiên bản giao thức là 0.1.0. Danh sách thông tin phiên PDU trong bảng 2 là, ví dụ, tin nhắn danh sách thiết lập tài nguyên

phiên PDU trong phần 9.3.1.5 của 3GPP NG RAN NGAP mà số phiên bản giao thức là 0.1.0.

Bảng 1

IE/Tên nhóm (Information element/Group name)	Có mặt (Presence)	Phạm vi (Range)	Loại IE và tham chiếu (Information element type and reference)	Mô tả ngữ nghĩa (Semantics description)	Mức độ rủi ro (Criticality)	Mức độ rủi ro đã chuyển nhượng (Assigned criticality)
Loại tin nhắn (Message Type)	M (Mandatory) (Bắt buộc)		<ref>		CÓ	loại bỏ
AMF UE NGAP ID	M (Bắt buộc, Mandatory)		<ref>		CÓ	loại bỏ
gNB UE NGAP ID	M (Bắt buộc, Mandatory)		<ref>		CÓ	loại bỏ
NAS PDU	FFS (để nghiên cứu tiếp, for further study)		<ref>		CÓ	loại bỏ
Danh sách thiết lập tài nguyên phiên PDU (PDU Session Resource Setup List)	M (Bắt buộc, Mandatory)		<ref>		CÓ	loại bỏ

Bảng 2

IE/Tên nhóm (Information element/Group name)	Có mặt (Presence)	Phạm vi (Range)	Loại IE và tham chiếu (Thông tin loại phần tử và tham chiếu)	Mô tả ngữ nghĩa (Semantics description)	Mức độ rủi ro (Criticality)	Mức độ rủi ro đã chuyển nhượng (Assigned criticality)
Danh sách thiết lập tài nguyên phiên PDU (PDU Session Resource Setup List)		1			CÓ	loại bỏ
> Các IE phần tử thiết lập tài nguyên phiên PDU (PDU Session Resource Setup Item Information Elements)		1.. <maxnoof PDUSessionResources> 1…<Số tối đa của tài nguyên phiên PDU>			MỖI	loại bỏ
>> ID phiên PDU [FFS] (PDU Session ID)	M (Bắt buộc, Mandatory)		<ref>		-	

IE/Tên nhóm (Information element/Group name)	Có mặt (Presence)	Phạm vi (Range)	Loại IE và tham chiếu (Thông tin loại phần tử và tham chiếu)	Mô tả ngữ nghĩa (Semantics description)	Mức độ rủi ro (Criticality)	Mức độ rủi ro đã chuyển nhượng (Assigned criticality)
>> S-NSSAI (Thông tin hỗ trợ lựa chọn phiến mạng đơn, Single Network Slice Selection Assistance Information)	O		<ref>		-	
>> Truyền yêu cầu thiết lập phiên PDU (PDU Session Setup Request Transfer)	O (tùy chọn, Optional)		<ref>		-	
>> Cấu hình bảo vệ tính toàn vẹn (Vị trí tùy chọn 1)						

Bảng 3

IE/Tên nhóm (Phần tử thông tin/Tên nhóm)	Có mặt (Presence)	Phạm vi (Range)	Loại IE và tham chiếu (Information element type and reference)	Mô tả ngữ nghĩa (Semantics description)	Mức độ rủi ro (Criticality)	Mức độ rủi ro đã chuyển nhượng (Assigned criticality)
Truyền yêu cầu thiết lập phiên PDU (PDU Session Setup Request Transfer)		1			CÓ	loại bỏ
> Cấu hình bảo vệ tính toàn vẹn (Vị trí tùy chọn 2)						
Tài nguyên phiên PDU kết hợp tốc độ bit lớn nhất PDU Session Resource Aggregated Maximum Bitrate)	M (Bắt buộc, Mandatory)		<ref>		-	
>Thông tin lớp vận chuyển (Transport Layer Information)	M (Bắt buộc, Mandatory)		<ref>		-	
> Loại phiên PDU (PDU Session Type)	M (Bắt buộc, Mandatory)		<ref>		-	
> Danh sách		1			-	

IE/Tên nhóm (Phần tử thông tin/Tên nhóm)	Có mặt (Presence)	Phạm vi (Range)	Loại IE và tham chiếu (Information element type and reference)	Mô tả ngữ nghĩa (Semantics description)	Mức độ rủi ro (Criticality)	Mức độ rủi ro đã chuyển nhượng (Assigned criticality)
thiết lập các dòng chảy QoS (QoS Flows Setup List)						
>> Các IE phần tử thiết lập các dòng chảy QoS (QoS Flows Setup Item Information Elements)		1..<maxnoofQoSFlows>			-	
>>> Chỉ báo dòng chảy QoS (QoS Flow Indicator)	M (Bắt buộc, Mandatory)		<ref>		MỖI	loại bỏ
>>> Các tham số QoS mức độ dòng chảy QoS (QoS Flow Level QoS Parameters)	FFS		<ref>		MỖI	loại bỏ
>>> Kích hoạt QoS phản chiếu (Reflective QoS Activation)	O (tùy chọn, Optional)		<ref>		MỖI	loại bỏ

Bảng 2 và bảng 3 thể hiện hai vị trí có thể có của cấu hình bảo vệ tính toàn vẹn tương ứng với phiên trong tin nhắn thứ tư. Trong bảng 2, cấu hình bảo vệ tính toàn vẹn tương ứng với

phiên được mang trong danh sách thiết lập tài nguyên phiên PDU, và danh sách thiết lập tài nguyên phiên PDU bao gồm một hoặc nhiều phần tử thông tin (information element, IE) thiết lập tài nguyên phiên. Mỗi phần tử thông tin bảo vệ ít nhất một trong các thông tin sau: mã nhận dạng phiên, và thông tin hỗ trợ lựa chọn phiến mạng đơn. Thông tin hỗ trợ lựa chọn phiến mạng được sử dụng để chỉ báo mã nhận dạng phiến mạng tương ứng với phiên. Trong Bảng 3, cấu hình bảo vệ tính toàn vẹn tương ứng với phiên được thực hiện trong chuyển giao yêu cầu thiết lập phiên PDU, và chuyển giao yêu cầu thiết lập phiên PDU bao gồm ít nhất một trong các thông tin sau: tốc độ bit tổng hợp tối đa tương ứng với một hoặc nhiều phiên, thông tin vận chuyển lớp, loại phiên, danh sách thông tin tài nguyên luồng QoS, và tương tự. Danh sách thông tin tài nguyên luồng QoS bao gồm bộ nhận dạng tương ứng với một hoặc nhiều luồng, tham số QoS của mức luồng QoS, và tương tự.

Bước S104: Thiết bị mạng truy cập gửi tin nhắn thứ hai đến thiết bị đầu cuối, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng DRB tương ứng với phiên.

Sau khi nhận tin nhắn thứ tư, thiết bị mạng truy cập lưu trữ cấu hình bảo vệ tính toàn vẹn được mang trong tin nhắn thứ tư, chẳng hạn như thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, thiết lập DRB cho thiết bị đầu cuối dựa trên tham số cấu hình của ít nhất một lớp giao thức mà được mang trong tin nhắn thứ tư, để thực hiện dịch vụ được khởi tạo bởi thiết bị đầu cuối, sau đó tạo tin nhắn thứ hai, và gửi tin nhắn thứ hai đến thiết bị đầu cuối. Tin nhắn thứ hai có thể là tin nhắn NAS, tin nhắn RRC, tin nhắn lớp MAC, hoặc tin nhắn lớp vật lý. Khi tin nhắn thứ hai là tin nhắn RRC: nếu tin nhắn RRC không bao gồm tin nhắn NAS, bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên tất cả được mang trong tin nhắn RRC; hoặc nếu tin nhắn RRC bao gồm tin nhắn NAS, tất cả hoặc một số tham số đã nói ở trên được mang trong tin nhắn NAS mà được bao gồm trong tin nhắn RRC.

Trong phương án này, tin nhắn thứ hai bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên. Tùy chọn, tin nhắn thứ hai có thể không mang theo thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên được thực hiện bằng cách sử dụng một tin nhắn khác, hoặc thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên được tạo cấu hình trước. Theo một phương án khác, tin nhắn thứ hai bao gồm ít nhất một trong các thông tin sau: thuật toán và khóa bảo vệ tính toàn vẹn, chỉ báo vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ

tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn. Tương tự, một hoặc nhiều chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn có thể được tạo cấu hình trước, thay vì được chỉ ra động bằng cách sử dụng tin nhắn thứ hai.

Cấu hình bảo vệ tính toàn vẹn được mang trong tin nhắn thứ hai có thể giống hoặc khác với cấu hình bảo vệ tính toàn vẹn được mang trong tin nhắn thứ tư. Ví dụ, nếu tin nhắn thứ tư chỉ ra khóa gốc được sử dụng cho phiên, sau khi nhận tin nhắn thứ tư, thiết bị mạng truy cập sẽ tính toán, dựa trên khóa gốc được chỉ ra, khóa được sử dụng cho phiên, và sau đó bổ sung khóa được sử dụng cho phiên vào tin nhắn thứ hai.

Tùy chọn, cấu hình bảo vệ tính toàn vẹn tương ứng với phiên có thể được mang trong tham số cấu hình lớp SDAP trong tin nhắn thứ hai, nghĩa là, cấu hình bảo vệ tính toàn vẹn được sử dụng làm tham số cấu hình của lớp SDAP. Ngoài ra, cấu hình bảo vệ tính toàn vẹn tương ứng với phiên có thể được mang trong tham số cấu hình lớp PDCP, nghĩa là, cấu hình bảo vệ tính toàn vẹn được sử dụng làm tham số cấu hình lớp PDCP. Tin nhắn thứ hai bao gồm tham số cấu hình của ít nhất một lớp giao thức. Cả tham số cấu hình lớp SDAP và tham số cấu hình lớp PDCP có thể được mang trong tin nhắn thứ hai; hoặc một trong các tham số cấu hình được mang trong tin nhắn thứ hai, và tin nhắn cấu hình khác được mang trong một tin nhắn khác khác với tin nhắn thứ hai. Phần sau đây mô tả một số vị trí có thể có của cấu hình bảo vệ tính toàn vẹn trong tin nhắn thứ hai. Ví dụ, tin nhắn thứ hai là tin nhắn cấu hình lại sự kết nối RRC (RRC Connection Reconfiguration message). Thông báo cấu hình lại sự kết nối RRC, ví dụ, thông báo cấu hình lại sự kết nối RRC sau đây trong phần 6.2.2 của giao thức RRC truy cập vô tuyến mặt đất phổ dụng phát triển 3GPP (Evolved Universal Terrestrial Radio Access, E-UTRA) có số phiên bản giao thức là 13.0.0.

RRC connection reconfiguration message (Thông báo cấu hình lại sự kết nối RRC)

RRCConnectionReconfiguration-r8-IEs ::= SEQUENCE {

measConfigMeasConfigOPTIONAL, -- Need ON

mobilityControlInfoMobilityControlInfoOPTIONAL, -- Cond HO

dedicatedInfoNASListSEQUENCE (SIZE(1..maxDRB)) OF

DedicatedInfoNASOPTIONAL,-- Cond nonHO

radioResourceConfigDedicatedRadioResourceConfigDedicatedOPTIONAL, -- Cond HO-toEUTRA

RadioResourceConfigDedicated information element (Phần tử thông tin RadioResourceConfigDedicated)

RadioResourceConfigDedicated ::=SEQUENCE {

srb-ToAddModListSRB-ToAddModList(SRB-To add/modify a list (SRB-để bổ sung/sửa đổi danh sách))sdap-ToAddModListSDAP-ToAddModList (SDAP-To add/modify a list (SDAP-để bổ sung/sửa đổi danh sách))

SDAP-ToAddMod ::=SEQUENCE{

Sdap-Identity(SDAP identifier (bộ nhận dạng SDAP))

(Possible position 1 (Vị trí 1 có thể có)) Integrity protection configuration (cấu hình bảo vệ tính toàn vẹn)}

drb-ToAddModListDRB-ToAddModList (DRB-To add/modify a list (DRB- để bổ sung/sửa đổi danh sách))

DRB-ToAddMod ::=SEQUENCE {

eps-BearerIdentity(Evolved packet core, evolved packet system bearer identifier (lõi gói đã phát triển, bộ nhận dạng bộ mang hệ thống gói đã phát triển))

drb-Identity(DRB identifier (Bộ nhận dạng DRB))

PDCP-Config(PDCP configuration) {Possible position 2 of the integrity protection configuration (vị trí 2 có thể có của cấu hình bảo vệ tính toàn vẹn)}

rlc-Config(RLC configuration (Cấu hình RLC)

logicalChannelIdentity(Logical channel identifier (Bộ nhận dạng kênh logic))

LogicalChannelConfig(Logical channel configuration (Cấu hình kênh logic))

...,

}

}

Trong ví dụ trên, vị trí 1 có thể có của cấu hình bảo vệ tính toàn vẹn tương ứng với phiên là tham số cấu hình lớp SDAP và vị trí 2 có thể có của cấu hình bảo vệ tính toàn vẹn tương ứng với phiên là tham số cấu hình lớp PDCP.

Tùy chọn, sau bước S104, thiết bị mạng truy cập gửi tin nhắn thứ năm đến thiết bị mạng lõi. Tin nhắn thứ năm được sử dụng để phản hồi kết quả xử lý tin nhắn thứ tư được gửi bởi thiết bị mạng lõi. Nếu thiết bị mạng truy cập tạo cấu hình bối cảnh của thiết bị đầu cuối thất bại, tin nhắn thứ năm được sử dụng để phản hồi lỗi cấu hình và bao gồm chỉ báo nguyên nhân lỗi, cụ thể là, giá trị nguyên nhân. Tin nhắn thứ năm được còn được sử dụng để mang tài

nguyên giao diện không khí được phân bổ bởi thiết bị mạng truy cập cho một hoặc nhiều phiên, và bao gồm, ví dụ, danh sách thông tin phiên được thiết lập của thiết bị mạng truy cập, và danh sách các luồng QoS mà không thể được thiết lập.

Bước S105: Thiết bị đầu cuối lưu trữ nội dung của tin nhắn thứ hai.

Thiết bị đầu cuối lưu trữ cấu hình bảo vệ tính toàn vẹn tương ứng với phiên được mang trong tin nhắn thứ hai, để thực hiện sau đó, dựa trên cấu hình bảo vệ tính toàn vẹn được lưu trữ tương ứng với phiên, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB tương ứng với phiên. Phiên có thể tương ứng với một hoặc nhiều DRB. Nếu phiên tương ứng với nhiều DRB, cấu hình bảo vệ tính toàn vẹn được sử dụng cho nhiêu DRB tương ứng với phiên là như nhau.

Cụ thể, thiết bị đầu cuối thực hiện, bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB tương ứng với phiên. Dữ liệu của DRB là gói dữ liệu lớp SDAP hoặc gói dữ liệu lớp PDCP của DRB. Nói cách khác, thiết bị đầu cuối có thể thực hiện, ở lớp SDAP và lớp PDCP, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB. Các gói dữ liệu của lớp SDAP bao gồm PDU và đơn vị dữ liệu dịch vụ (service Data Unit, SDU), và các gói dữ liệu của lớp PDCP cũng bao gồm PDU và SDU.

Thiết bị đầu cuối đó là đầu truyền và dữ liệu của DRB là gói dữ liệu lớp PDCP được sử dụng làm ví dụ. Thiết bị đầu cuối tính toán, theo thuật toán bảo vệ tính toàn vẹn, MAC-I 32 bit bằng cách sử dụng ít nhất một trong các tham số chẳng hạn như khóa, giá trị đếm (COUNT), mã nhận dạng mang vô tuyến, chiều (DIRECTION), bản thân gói dữ liệu của lớp PDCP, và độ dài của gói dữ liệu lớp PDCP làm tham số đầu vào, và đặt MAC-I 32 bit vào trường MAC-I của PDU PDCP. Sau khi nhận gói dữ liệu lớp PDCP, đầu nhận (thiết bị mạng truy cập hoặc thiết bị mạng lõi) tính toán, bằng cách sử dụng cùng một phương pháp, mã xác thực được dự kiến XMAC-I cho gói dữ liệu lớp PDCP, và thực hiện sự kiểm tra tính toàn vẹn bằng cách so sánh XMAC-I với MAC-I. Nếu MAC-I bằng với XMAC-I, đầu nhận xác định rằng sự kiểm tra tính toàn vẹn thành công; hoặc nếu MAC-I không bằng XMAC-I, đầu nhận xác định rằng sự kiểm tra tính toàn vẹn thất bại. Chắc chắn, thiết bị đầu cuối cũng có thể phục vụ như đầu nhận.

Trong phương án này, thiết bị đầu cuối thu được, bằng cách sử dụng tin nhắn thứ hai, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên từ thiết bị mạng truy cập. Cần lưu ý rằng thiết bị đầu cuối mặt khác có thể thu được, theo một cách khác, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên. Ví dụ, thuật toán và khóa bảo vệ tính toàn vẹn tương

ứng với phiên được tạo cấu hình trước trên thiết bị đầu cuối, tin nhắn thứ hai chỉ cần mang bộ nhận dạng phiên, và thiết bị đầu cuối tìm kiếm, dựa trên bộ nhận dạng phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên. Tương tự, các cấu hình bảo vệ tính toàn vẹn khác của phiên, ví dụ, một hoặc nhiều chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn có thể được chỉ ra động bằng cách sử dụng tin nhắn thứ hai, hoặc được thông báo theo cách tạo cấu hình trước cho thiết bị đầu cuối.

Trong phương án này, thiết bị đầu cuối thu được thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và DRB tương ứng với phiên, và thực hiện, bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB, sao cho có thể sử dụng các thuật toán và các khóa bảo vệ tính toàn vẹn khác nhau cho các phiên khác nhau, và sự bảo vệ tính toàn vẹn linh hoạt hơn và đáp ứng các yêu cầu bảo mật của cùng một người dùng cho các dịch vụ khác nhau.

Fig. 4 là biểu đồ tiến trình sự báo hiệu của phương pháp bảo vệ tính toàn vẹn dữ liệu theo phương án 2 của sáng chế này. Khác với phương án 1, sự bảo vệ tính toàn vẹn trong phương án này là ở mức độ chi tiết của dòng chảy luồng. Như được thể hiện trên Fig.4, phương pháp trong phương án này chủ yếu bao gồm các bước sau.

Bước S201: Thiết bị đầu cuối gửi tin nhắn thứ nhất đến thiết bị mạng truy cập.

Bước S202: Thiết bị mạng truy cập gửi tin nhắn thứ ba đến thiết bị mạng lõi, trong đó tin nhắn thứ ba bao gồm tin nhắn thứ nhất.

Đối với cách triển khai cụ thể của bước S201 và bước S202, tham khảo các mô tả liên quan trong phương án 1.

Bước S203: Thiết bị mạng lõi gửi tin nhắn thứ tư đến thiết bị mạng truy cập, trong đó tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng.

Khác với phương án 1, trong phương án này, tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng. Luồng tương ứng với phiên mà tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập. Phiên bao gồm nhiều luồng, và mỗi luồng có thể được ánh xạ tới nhiều DRB. Trong phương án này, các thuật toán và khóa bảo vệ tính toàn vẹn giống hoặc khác nhau có thể được sử dụng cho nhiều luồng được bao gồm trong phiên.

Tùy chọn, tin nhắn thứ tư có thể không mang thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng được thực hiện bằng cách sử dụng một tin nhắn khác, hoặc thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng được tạo cấu hình trước. Tùy chọn, tin nhắn thứ tư có thể còn bao gồm ít nhất một trong các thông tin sau: chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn. Tương tự, một hoặc nhiều chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn có thể được tạo cấu hình trước, thay vì được chỉ ra động bằng cách sử dụng tin nhắn thứ tư.

Trong phương án này, cấu hình bảo vệ tính toàn vẹn của luồng có thể được đặt trong danh sách thông tin tài nguyên luồng QoS trong tin nhắn thứ tư, để chỉ ra cấu hình bảo vệ tính toàn vẹn tương ứng với luồng, hoặc có thể được đặt riêng trong tin nhắn thứ tư, với bộ nhận dạng luồng tương ứng với cấu hình bảo vệ tính toàn vẹn được bổ sung, ví dụ, được đặt trong danh sách thông tin tài nguyên phiên PDU, sao cho thiết bị mạng truy cập biết sự tạo cấu hình bảo vệ tính toàn vẹn của luồng từ tin nhắn thứ tư. Đối với cấu trúc của tin nhắn thứ tư, tham khảo bảng 1 đã nói ở trên. Đối với danh sách thông tin phiên PDU, tham khảo bảng 2 đã nói ở trên. Bảng 4 là sơ đồ nguyên lý của danh sách thông tin tài nguyên luồng QoS.

Bảng 4

IE/Tên nhóm (Information element/Group name)	Có mặt (Presence)	Phạm vi (Range)	Loại IE và tham chiếu (Information element type and reference)	Mô tả ngữ nghĩa (Semantics description)	Mức độ rủi ro (Mức độ rủi ro)	Mức độ rủi ro đã chuyển nhượng (Assigned criticality)
Truyền yêu cầu thiết lập phiên PDU (PDU Session Setup Request Transfer)		1			CÓ	loại bỏ

IE/Tên nhóm (Information element/Group name)	Có mặt (Presence)	Phạm vi (Range)	Loại IE và tham chiếu (Information element type and reference)	Mô tả ngữ nghĩa (Semantics description)	Mức độ rủi ro (Mức độ rủi ro)	Mức độ rủi ro đã chuyển nhượng (Assigned criticality)
Tài nguyên phiên PDU kết hợp tốc độ bit lớn nhất PDU Session Resource Aggregated Maximum Bitrate)	M (Bắt buộc, Mandatory)		<ref>		-	
>Thông tin lớp vận chuyển (Transport Layer Information)	M (Bắt buộc, Mandatory)		<ref>		-	
> Loại phiên PDU [FFS] (PDU Session Type)	M (Bắt buộc, Mandatory)		<ref>	eNote: IP, không có cấu trúc hoặc Ethernet	-	
> Danh sách thiết lập các dòng chảy QoS (QoS Flows Setup List)		1			-	
>> Các IE phần tử thiết lập các dòng chảy QoS (QoS Flows Setup Item Information Elements)		1..<maxnoof QoSFlows>			-	

IE/Tên nhóm (Information element/Group name)	Có mặt (Presence)	Phạm vi (Range)	Loại IE và tham chiếu (Information element type and reference)	Mô tả ngữ nghĩa (Semantics description)	Mức độ rủi ro (Mức độ rủi ro)	Mức độ rủi ro đã chuyển nhượng (Assigned criticality)
>>> Chỉ báo dòng chảy QoS (QoS Flow Indicator)	M (Bắt buộc, Mandatory)		<ref>		MỖI	loại bỏ
>>> Các tham số QoS mức độ dòng chảy QoS (QoS Flow Level QoS Parameters)	FFS		<ref>		MỖI	loại bỏ
>>> Vị trí tùy chọn: cấu hình bảo vệ tính toàn vẹn						
>>> Kích hoạt QoS phản chiếu [FFS] (Reflective QoS Activation)	O (tùy chọn, Optional)		<ref>		MỖI	loại bỏ

Trong ví dụ được thể hiện trong bảng 4, cấu hình bảo vệ tính toàn vẹn tương ứng với luồng được mang trong danh sách thông tin tài nguyên luồng QoS. Danh sách thông tin tài nguyên luồng QoS còn bao gồm bộ nhận dạng tương ứng với một hoặc nhiều luồng, tham số QoS của mức luồng QoS, và tương tự.

Bước S204: Thiết bị mạng truy cập gửi tin nhắn thứ hai đến thiết bị đầu cuối, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, bộ nhận dạng của luồng, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và mã nhận dạng của DRB tương ứng với luồng.

Sau khi nhận tin nhắn thứ tư, thiết bị mạng truy cập lưu trữ bộ nhận dạng của phiên, bộ nhận dạng của luồng, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và bộ nhận dạng của DRB tương ứng với luồng mà được mang trong tin nhắn thứ tư, thiết lập DRB cho thiết bị đầu cuối dựa trên tham số cấu hình của ít nhất một lớp giao thức mà được mang trong tin nhắn thứ tư, để thực hiện dịch vụ được khởi tạo bởi thiết bị đầu cuối, xác định DRB tương ứng với mỗi luồng, sau đó tạo ra tin nhắn thứ hai, và gửi tin nhắn thứ hai đến thiết bị đầu cuối. Tin nhắn thứ hai có thể là tin nhắn NAS, tin nhắn RRC, tin nhắn lớp MAC, hoặc tin nhắn lớp vật lý. Khi tin nhắn thứ hai là tin nhắn RRC: nếu tin nhắn RRC không bao gồm tin nhắn NAS, bộ nhận dạng của phiên, bộ nhận dạng của luồng, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và bộ nhận dạng của DRB tương ứng với luồng tất cả được thực hiện trong tin nhắn RRC; hoặc nếu tin nhắn RRC bao gồm tin nhắn NAS, tất cả hoặc một số tham số đã nói ở trên được mang trong tin nhắn NAS mà được bao gồm trong tin nhắn RRC.

Trong phương án này, tin nhắn thứ hai bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng. Tùy chọn, tin nhắn thứ hai có thể không mang thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng được thực hiện bằng cách sử dụng một tin nhắn khác, hoặc thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng được tạo cấu hình trước. Theo một phương án khác, tin nhắn thứ hai bao gồm ít nhất một trong các thông tin sau: thuật toán và khóa bảo vệ tính toàn vẹn, chỉ báo vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn. Tương tự, một hoặc nhiều chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn có thể được tạo cấu hình trước, thay vì được chỉ ra động bằng cách sử dụng tin nhắn thứ hai.

Cấu hình bảo vệ tính toàn vẹn tương ứng với luồng được mang trong tin nhắn thứ hai có thể giống hoặc khác với cấu hình bảo vệ tính toàn vẹn tương ứng với luồng được mang trong tin nhắn thứ tư. Ví dụ, nếu tin nhắn thứ tư chỉ ra khóa gốc được sử dụng cho luồng, sau khi nhận tin nhắn thứ tư, thiết bị mạng truy cập tính toán, dựa trên khóa gốc được chỉ ra, khóa được sử dụng cho luồng, và sau đó bổ sung khóa được sử dụng cho luồng vào tin nhắn thứ hai.

Tùy chọn, cấu hình bảo vệ tính toàn vẹn tương ứng với luồng có thể được mang trong tham

số cấu hình lớp SDAP trong tin nhắn thứ hai, nghĩa là, cấu hình bảo vệ tính toàn vẹn tương ứng với luồng được sử dụng làm tham số cấu hình lớp SDAP. Ngoài ra, cấu hình bảo vệ tính toàn vẹn tương ứng với luồng có thể được mang trong tham số cấu hình lớp PDCP, nghĩa là, cấu hình bảo vệ tính toàn vẹn tương ứng với luồng được sử dụng làm tham số cấu hình lớp PDCP. Tin nhắn thứ hai bao gồm tham số cấu hình của ít nhất một lớp giao thức. Cả tham số cấu hình lớp SDAP và tham số cấu hình lớp PDCP có thể được mang trong tin nhắn thứ hai; hoặc một trong các tham số cấu hình được mang trong tin nhắn thứ hai, và tin nhắn cấu hình khác được mang trong một tin nhắn khác khác với tin nhắn thứ hai.

Tùy chọn, sau bước S204, thiết bị mạng truy cập gửi tin nhắn thứ năm đến thiết bị mạng lõi. Tin nhắn thứ năm được sử dụng để phản hồi kết quả xử lý tin nhắn thứ tư được gửi bởi thiết bị mạng lõi. Nếu thiết bị mạng truy cập tạo cấu hình bối cảnh của thiết bị đầu cuối thất bại, tin nhắn thứ năm được sử dụng để phản hồi lỗi cấu hình và bao gồm chỉ báo nguyên nhân lỗi, cụ thể là, giá trị nguyên nhân. Tin nhắn thứ năm được còn được sử dụng để mang tài nguyên giao diện không khí được phân bổ bởi thiết bị mạng truy cập cho một hoặc nhiều phiên, và bao gồm, ví dụ, danh sách thông tin phiên được thiết lập của thiết bị mạng truy cập, và danh sách các luồng QoS mà không thể được thiết lập.

Bước S205: Thiết bị đầu cuối lưu trữ nội dung của tin nhắn thứ hai.

Thiết bị đầu cuối lưu trữ cấu hình bảo vệ tính toàn vẹn tương ứng với luồng được truyền trong tin nhắn thứ hai, để thực hiện sau đó, dựa trên cấu hình bảo vệ tính toàn vẹn được lưu trữ tương ứng với luồng, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB tương ứng với luồng. Luồng có thể tương ứng với một hoặc nhiều DRB, và các thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với các luồng khác nhau có thể khác nhau.

Cụ thể, thiết bị đầu cuối thực hiện, bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB tương ứng với luồng. Dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP của DRB. Nói cách khác, thiết bị đầu cuối có thể thực hiện, ở lớp SDAP và lớp PDCP, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB. Các gói dữ liệu của lớp SDAP bao gồm PDU và SDU, và các gói dữ liệu của lớp PDCP cũng bao gồm PDU và SDU.

Nếu sự bảo vệ tính toàn vẹn được thực hiện ở lớp PDCP, vì lớp PDCP không thể phân biệt các luồng và chỉ lớp SDAP có thể xác định luồng được bao gồm trong phiên, lớp SDAP cần đánh dấu bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP, sao cho lớp PDCP xác định các luồng khác nhau dựa trên các bộ nhận dạng luồng, và thực hiện thêm, dựa trên thuật

toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, sự bảo vệ tính toàn vẹn trên các gói dữ liệu tương ứng với luồng. Bộ nhận dạng của luồng có thể được đặt trong tiêu đề của gói dữ liệu lớp SDAP, hoặc có thể được đặt trong nội dung dữ liệu cụ thể của gói dữ liệu lớp SDAP. Định dạng cụ thể không bị giới hạn trong sáng chế này.

Trong phương án này, thiết bị đầu cuối thu được, bằng cách sử dụng tin nhắn thứ hai, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng từ thiết bị mạng truy cập. Cần lưu ý rằng thiết bị đầu cuối mặt khác có thể thu được, theo một cách khác, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng. Ví dụ, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng được tạo cấu hình trước trên thiết bị đầu cuối, tin nhắn thứ hai chỉ cần mang bộ nhận dạng phiên và bộ nhận dạng luồng, và thiết bị đầu cuối tìm kiếm, dựa trên bộ nhận dạng phiên và định danh luồng, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng. Tương tự, các cấu hình bảo vệ tính toàn vẹn khác của luồng, ví dụ, một hoặc nhiều chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn có thể được chỉ ra động bằng cách sử dụng tin nhắn thứ hai, hoặc được thông báo theo cách tạo cấu hình trước cho thiết bị đầu cuối.

Trong phương án này, thiết bị đầu cuối thu được thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng, và thực hiện bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB tương ứng với luồng, sao cho có thể sử dụng các thuật toán và khóa bảo vệ tính toàn vẹn khác nhau cho các luồng khác nhau, và sự bảo vệ tính toàn vẹn linh hoạt hơn và đáp ứng các yêu cầu bảo mật của cùng một người dùng cho các dịch vụ khác nhau.

Trong các phương án đã nói ở trên, đầu truyền có thể thực hiện sự bảo vệ tính toàn vẹn dữ liệu theo bất kỳ một trong các quy trình, chẳng hạn như đánh số thứ tự, nén tiêu đề, và mã hóa. Tương ứng, điều này là giống nhau đối với đầu nhận. Ngoài ra, vị trí và kích thước của MAC-I có thể được thiết lập linh hoạt. Fig.5 là sơ đồ phác họa của MAC-I khi sự bảo vệ tính toàn vẹn được thực hiện ở lớp PDCP. Như được thể hiện trên Fig.5, MAC-I có thể được mang trong một vài byte cuối của tin nhắn.

Trong các phương án đã nói ở trên, đầu nhận thực hiện sự kiểm tra tính toàn vẹn, và nếu sự kiểm tra tính toàn vẹn của tin nhắn thất bại, bất kỳ một trong các hoạt động xử lý sau có thể được thực hiện: (1) hướng dẫn RRC thiết lập lại sự kết nối RRC; (2) loại bỏ tin nhắn; (3) loại bỏ tin nhắn và thiết lập lại sự kết nối RRC; và (4) thiết lập lại sự kết nối RRC khi số

lượng các lỗi kiểm tra tính toàn vẹn đạt đến giá trị đặt trước.

Các phương pháp trong các phương án đã nói ở trên có thể được áp dụng trong kịch bản kết nối kép (Dual Connection, DC) hoặc kịch bản chuyển giao ô. Trong kịch bản chuyển giao ô, nếu thiết bị đầu cuối được bàn giao từ trạm cơ sở nguồn đến trạm cơ sở đích, thiết bị đầu cuối cần gửi cấu hình bảo vệ tính toàn vẹn tương ứng với phiên hoặc cấu hình bảo vệ tính toàn vẹn tương ứng với luồng đến trạm cơ sở đích, sao cho trạm cơ sở đích thực hiện sự bảo vệ tính toàn vẹn dựa trên cấu hình bảo vệ tính toàn vẹn tương ứng với phiên hoặc cấu hình bảo vệ tính toàn vẹn tương ứng với luồng. Trong kịch bản DC, sự bảo vệ tính toàn vẹn chỉ có thể được thực hiện tại một nút, hoặc sự bảo vệ tính toàn vẹn có thể được thực hiện ở cả hai nút. Nút chủ (Master node, MN) cần gửi cấu hình bảo vệ tính toàn vẹn tương ứng với phiên hoặc cấu hình bảo vệ tính toàn vẹn tương ứng với luồng đến nút thứ cấp (Secondary node, SN), sao cho nút thứ cấp có thể thực hiện sự bảo vệ tính toàn vẹn dựa trên trên cấu hình bảo vệ tính toàn vẹn tương ứng với phiên hoặc cấu hình bảo vệ tính toàn vẹn tương ứng với luồng.

Fig. 6 là sơ đồ cấu trúc phác họa của thiết bị đầu cuối theo phương án 3 của sáng chế này. Như được thể hiện trên Fig.6, thiết bị đầu cuối được cung cấp trong phương án này bao gồm:

môđun thu được 11, được tạo cấu hình để thu được thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với phiên; và

môđun bảo vệ tính toàn vẹn 12, được tạo cấu hình để thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn.

Tùy chọn, môđun thu được 11 được tạo cấu hình cụ thể để: gửi tin nhắn thứ nhất, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên; và nhận tin nhắn thứ hai, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên; hoặc tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Tùy chọn, môđun thu được 11 còn được tạo cấu hình để thu được ít nhất một trong các

thông tin sau:

chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn, trong đó

chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo vệ tính toàn vẹn được thực hiện;

chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà thực hiện sự bảo vệ tính toàn vẹn;

chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không; và

chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng, hoặc dữ liệu mặt phẳng người dùng và sự báo hiệu mặt phẳng điều khiển.

Tùy chọn, dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP của DRB. Khi dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, thiết bị đầu cuối còn bao gồm: môđun đánh dấu, được tạo cấu hình để đánh dấu bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP của DRB.

Thiết bị đầu cuối được cung cấp trong phương án này có thể được tạo cấu hình để thực hiện các bước được thực hiện bởi thiết bị đầu cuối trong phương án 1, và sự triển khai cụ thể và hiệu ứng kỹ thuật cũng tương tự. Các chi tiết không được mô tả lại ở đây.

Phương án 4 của sáng chế này cung cấp thiết bị đầu cuối. đối với cấu trúc của thiết bị đầu cuối, tham khảo Fig.6. Trong phương án này, môđun thu được 11 được tạo cấu hình để thu được thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với luồng; và môđun bảo vệ tính toàn vẹn 12 được tạo cấu hình để thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn.

Tùy chọn, môđun thu được 11 được tạo cấu hình cụ thể để: gửi tin nhắn thứ nhất, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên, và phiên tương ứng với luồng; và nhận tin nhắn thứ hai, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ

nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng; hoặc tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Tùy chọn, môđun thu được 11 còn được tạo cấu hình để thu được ít nhất một trong các thông tin sau:

chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn, trong đó

chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo vệ tính toàn vẹn được thực hiện;

chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà thực hiện sự bảo vệ tính toàn vẹn;

chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không; và

chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng, hoặc dữ liệu mặt phẳng người dùng và sự báo hiệu mặt phẳng điều khiển.

Tùy chọn, dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP của DRB. Khi dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, thiết bị đầu cuối còn bao gồm: môđun đánh dấu, được tạo cấu hình để đánh dấu bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP của DRB.

Thiết bị đầu cuối được cung cấp trong phương án này có thể được tạo cấu hình để thực hiện các bước được thực hiện bởi thiết bị đầu cuối trong phương án 2, và sự triển khai cụ thể và hiệu ứng kỹ thuật cũng tương tự. Các chi tiết không được mô tả lại ở đây.

Fig. 7 là sơ đồ cấu trúc phác họa của thiết bị mạng truy cập theo phương án 5 của sáng chế này. Như được thể hiện trên Fig.7, thiết bị mạng truy cập được cung cấp trong phương án này bao gồm:

môđun nhận 21, được tạo cấu hình để nhận tin nhắn thứ nhất được gửi bởi thiết bị đầu cuối, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên;

môđun gửi 22, được tạo cấu hình để gửi tin nhắn thứ ba đến thiết bị mạng lõi, trong đó

tin nhắn thứ ba bao gồm tin nhắn thứ nhất, trong đó

môđun nhận 21 còn được tạo cấu hình để nhận tin nhắn thứ tư được gửi bởi thiết bị mạng lõi, trong đó tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với phiên; và

môđun lưu trữ 23, được tạo cấu hình để lưu trữ thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và DRB tương ứng với phiên, trong đó

môđun gửi 22 còn được tạo cấu hình để gửi tin nhắn thứ hai đến thiết bị đầu cuối, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên; hoặc tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và bộ nhận dạng của DRB tương ứng với phiên.

Tùy chọn, tin nhắn thứ ba hoặc tin nhắn thứ hai còn bao gồm ít nhất một trong các thông tin sau:

chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn, trong đó

chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo vệ tính toàn vẹn được thực hiện;

chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà thực hiện sự bảo vệ tính toàn vẹn;

chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không; và

chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng, hoặc dữ liệu mặt phẳng người dùng và sự báo hiệu mặt phẳng điều khiển.

Tùy chọn, thiết bị mạng truy cập còn bao gồm: môđun bảo vệ tính toàn vẹn 24, được tạo cấu hình để thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn.

Tùy chọn, dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP

của DRB.

Khi dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, thiết bị mạng truy cập còn bao gồm: môđun đánh dấu, được tạo cấu hình để đánh dấu bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP của DRB.

Phương án 6 của sáng chế này cung cấp thiết bị mạng truy cập. Đối với cấu trúc của thiết bị mạng truy cập, tham khảo Fig.7. Trong phương án này:

Môđun nhận 21 được tạo cấu hình để nhận tin nhắn thứ nhất được gửi bởi thiết bị đầu cuối, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên.

Một môđun gửi 22 được tạo cấu hình để gửi tin nhắn thứ ba đến thiết bị mạng lõi, trong đó tin nhắn thứ ba bao gồm tin nhắn thứ nhất.

Môđun nhận 21 còn được tạo cấu hình để nhận tin nhắn thứ tư được gửi bởi thiết bị mạng lõi, trong đó tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với luồng, và phiên tương ứng với luồng.

Môđun lưu trữ 23 được tạo cấu hình để lưu trữ thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng.

Môđun gửi 22 còn được tạo cấu hình để gửi tin nhắn thứ hai đến thiết bị đầu cuối, trong đó tin nhắn thứ hai bao gồm: bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Tùy chọn, tin nhắn thứ hai bao gồm cấu hình lớp SDAP, và cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng; hoặc tin nhắn thứ hai bao gồm cấu hình lớp PDCP, và cấu hình lớp PDCP bao gồm bộ nhận dạng của phiên, bộ nhận dạng của luồng, bộ nhận dạng của DRB tương ứng với luồng, và thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng.

Tùy chọn, tin nhắn thứ ba hoặc tin nhắn thứ hai còn bao gồm ít nhất một trong các thông tin sau:

chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn, trong đó

chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo

vệ tính toàn vẹn được thực hiện;

chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà thực hiện sự bảo vệ tính toàn vẹn;

chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không; và

chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng, hoặc dữ liệu mặt phẳng người dùng và sự báo hiệu mặt phẳng điều khiển.

Tùy chọn, môđun bảo vệ tính toàn vẹn 24 được tạo cấu hình để thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn.

Tùy chọn, dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP của DRB.

Khi dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, thiết bị mạng truy cập còn bao gồm: môđun đánh dấu, được tạo cấu hình để đánh dấu bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP của DRB.

Fig. 8 là sơ đồ cấu trúc phác họa của thiết bị mạng lõi theo phương án 7 của sáng chế này.

Như được thể hiện trên Fig.8, thiết bị mạng lõi được cung cấp trong phương án này bao gồm:

môđun nhận 31, được tạo cấu hình để nhận tin nhắn thứ ba được gửi bởi thiết bị mạng truy cập, trong đó tin nhắn thứ ba bao gồm tin nhắn thứ nhất, và tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên; và

môđun gửi 32, được tạo cấu hình để gửi tin nhắn thứ tư đến thiết bị mạng truy cập, trong đó tin nhắn thứ tư bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và sóng mang rađio dữ liệu (data radio bearer, DRB) tương ứng với phiên; hoặc bao gồm thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với luồng, và DRB tương ứng với luồng, trong đó phiên tương ứng với luồng.

Tùy chọn, tin nhắn thứ tư còn bao gồm ít nhất một trong các thông tin sau:

chỉ báo của vị trí bảo vệ tính toàn vẹn, chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn, chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn, và chỉ báo của đối tượng bảo vệ tính toàn vẹn, trong đó

chỉ báo của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo phần tử mạng mà sự bảo vệ tính toàn vẹn được thực hiện;

chỉ báo vị trí của lớp giao thức bảo vệ tính toàn vẹn được sử dụng để chỉ báo lớp giao thức mà thực hiện sự bảo vệ tính toàn vẹn;

chỉ báo việc kích hoạt của vị trí bảo vệ tính toàn vẹn được sử dụng để chỉ báo xem có cho phép chức năng bảo vệ tính toàn vẹn hay không; và

chỉ báo của đối tượng bảo vệ tính toàn vẹn được sử dụng để chỉ báo rằng đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng, hoặc dữ liệu mặt phẳng người dùng và sự báo hiệu mặt phẳng điều khiển.

Tùy chọn, thiết bị mạng lõi còn bao gồm: môđun bảo vệ tính toàn vẹn 33, được tạo cấu hình để thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán và khóa bảo vệ tính toàn vẹn.

Tùy chọn, dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, hoặc gói dữ liệu lớp PDCP của DRB.

Khi dữ liệu của DRB là gói dữ liệu lớp SDAP của DRB, thiết bị mạng lõi còn bao gồm: môđun đánh dấu, được tạo cấu hình để đánh dấu bộ nhận dạng của luồng trong gói dữ liệu lớp SDAP của DRB.

Cần lưu ý rằng trong các phương án của thiết bị đã nói ở trên, môđun nhận và môđun gửi có thể được thực hiện bằng cách sử dụng bộ truyền nhận, hoặc môđun thu được triển khai bởi bộ nhận độc lập và môđun gửi được thực hiện bởi bộ truyền độc lập. Môđun thu được, môđun bảo vệ tính toàn vẹn, và môđun đánh dấu trong các phương án đã nói ở trên có thể được triển khai bởi bộ xử lý có chức năng xử lý dữ liệu.

Fig. 9 là sơ đồ cấu trúc phác họa của thiết bị đầu cuối theo phương án 8 của sáng chế này. Như được thể hiện trên Fig.9, thiết bị đầu cuối 400 trong phương án này bao gồm: bộ xử lý 41, bộ nhớ 42, bộ nhận 43, và bộ truyền 44, trong đó bộ nhớ 42, bộ nhận 43, và bộ truyền 44 được kết nối và truyền thông với bộ xử lý 41 bằng cách sử dụng bus, bộ nhớ 42 được tạo cấu hình để lưu trữ lệnh có thể thực thi trên máy tính, và bộ xử lý 41 được tạo cấu hình để thực thi lệnh có thể thực thi trên máy tính, sao cho thiết bị đầu cuối 400 thực hiện các bước được thực hiện bởi thiết bị đầu cuối trong các phương pháp được cung cấp trong phương án 1 và phương án 2. Triển khai cụ thể và hiệu ứng kỹ thuật cũng tương tự. Các chi tiết không được mô tả lại ở đây.

Fig. 10 là sơ đồ cấu trúc phác họa của thiết bị mạng truy cập theo phương án 9 của sáng chế này. Như được thể hiện trên Fig.10, thiết bị mạng truy cập 500 trong phương án này bao gồm: bộ xử lý 51, bộ nhớ 52, bộ nhận 53, và bộ truyền 54, trong đó bộ nhớ 52, bộ nhận 53,

và bộ truyền 54 được kết nối và truyền thông với bộ xử lý 51 bằng cách sử dụng bus, bộ nhớ 52 được tạo cấu hình để lưu trữ lệnh có thể thực thi trên máy tính, và bộ xử lý 51 được tạo cấu hình để thực thi lệnh có thể thực thi trên máy tính, sao cho thiết bị mạng truy cập 500 thực hiện các bước được thực hiện bởi thiết bị mạng truy cập trong các phương pháp được cung cấp trong phương án 1 và phương án 2. Triển khai cụ thể và hiệu ứng kỹ thuật cũng tương tự. Các chi tiết không được mô tả lại ở đây.

Fig. 11 là sơ đồ cấu trúc phác họa của thiết bị mạng lõi theo phương án 10 của sáng chế này. Như được thể hiện trên Fig.11, thiết bị mạng lõi 600 trong phương án này bao gồm: bộ xử lý 61, bộ nhớ 62, bộ nhận 63, và bộ truyền 64, trong đó bộ nhớ 62, bộ nhận 63, và bộ truyền 64 được kết nối và truyền thông với bộ xử lý 61 bằng cách sử dụng bus, bộ nhớ 62 được tạo cấu hình để lưu trữ lệnh có thể thực thi trên máy tính, và bộ xử lý 61 được tạo cấu hình để thực thi lệnh có thể thực thi trên máy tính, sao cho thiết bị mạng lõi 600 thực hiện các bước được thực hiện bởi thiết bị mạng lõi trong các phương pháp được cung cấp trong phương án 1 và phương án 2. Triển khai cụ thể và hiệu ứng kỹ thuật cũng tương tự. Các chi tiết không được mô tả lại ở đây.

Phương án 11 của sáng chế này cung cấp phương tiện đọc được bằng máy tính, trong đó phương tiện đọc được bằng máy tính bao gồm lệnh có thể thực thi trên máy tính, và lệnh có thể thực thi trên máy tính được sử dụng để cho phép một thiết bị đầu cuối thực hiện các bước của các phương pháp được thực hiện bởi thiết bị đầu cuối trong phương án 1 và phương án 2 của sáng chế này.

Phương án 12 của sáng chế này cung cấp phương tiện đọc được bằng máy tính, trong đó phương tiện đọc được bằng máy tính bao gồm lệnh có thể thực thi trên máy tính, và lệnh có thể thực thi trên máy tính được sử dụng để cho phép thiết bị mạng truy cập thực hiện các bước của các phương pháp được thực hiện bởi thiết bị mạng truy cập trong phương án 1 và phương án 2 của sáng chế này.

Phương án 13 của sáng chế này cung cấp phương tiện đọc được bằng máy tính, trong đó phương tiện đọc được bằng máy tính bao gồm lệnh có thể thực thi trên máy tính, và lệnh có thể thực thi trên máy tính được sử dụng để cho phép thiết bị mạng lõi thực hiện các bước của các phương pháp được thực hiện bởi thiết bị mạng lõi trong phương án 1 và phương án 2 của sáng chế này.

Phương án 14 của sáng chế này cung cấp hệ thống trên chip. Hệ thống có thể được áp dụng cho thiết bị đầu cuối, và hệ thống trên chip bao gồm: ít nhất một giao diện truyền thông, ít

nhất một bộ xử lý, và ít nhất một bộ nhớ, trong đó giao diện truyền thông, bộ nhớ, và bộ xử lý được kết nối với nhau bằng cách sử dụng bus, và bộ xử lý dẫn ra lệnh được lưu trữ trong bộ nhớ, để thực hiện các bước của các phương pháp được thực hiện bởi thiết bị đầu cuối trong phương án 1 và phương án 2 của sáng chế này.

Phương án 15 của sáng chế này cung cấp hệ thống trên chip. Hệ thống có thể được áp dụng cho thiết bị mạng truy cập, và hệ thống trên chip bao gồm: ít nhất một giao diện truyền thông, ít nhất một bộ xử lý, và ít nhất một bộ nhớ, trong đó giao diện truyền thông, bộ nhớ, và bộ xử lý được kết nối với nhau bằng cách sử dụng bus, và bộ xử lý dẫn ra lệnh được lưu trữ trong bộ nhớ, để thực hiện các bước của các phương pháp được thực hiện bởi thiết bị mạng truy cập trong phương án 1 và phương án 2 của sáng chế này.

Phương án 16 của sáng chế này cung cấp hệ thống trên chip. Hệ thống có thể được áp dụng cho thiết bị mạng lõi, và hệ thống trên chip bao gồm: ít nhất một giao diện truyền thông, ít nhất một bộ xử lý, và ít nhất một bộ nhớ, trong đó giao diện truyền thông, bộ nhớ, và bộ xử lý được kết nối với nhau bằng cách sử dụng bus, và bộ xử lý dẫn ra lệnh được lưu trữ trong bộ nhớ, để thực hiện các phương pháp được thực hiện bởi thiết bị mạng lõi trong phương án 1 và phương án 2 của sáng chế này.

Phương án 17 của sáng chế này cung cấp sản phẩm chương trình, trong đó sản phẩm chương trình bao gồm chương trình máy tính, chương trình máy tính được lưu trữ trong phương tiện lưu trữ có thể đọc được, và ít nhất một bộ xử lý của thiết bị đầu cuối thực hiện chương trình máy tính, sao cho thiết bị đầu cuối thực hiện các bước của các phương pháp được thực hiện bởi thiết bị đầu cuối trong phương án 1 và phương án 2 của sáng chế này.

Phương án 18 của sáng chế này cung cấp sản phẩm chương trình, trong đó sản phẩm chương trình bao gồm chương trình máy tính, chương trình máy tính được lưu trữ trong phương tiện lưu trữ có thể đọc được, và ít nhất một bộ xử lý của thiết bị mạng truy cập thực hiện chương trình máy tính, sao cho thiết bị mạng truy cập thực hiện các bước của các phương pháp được thực hiện bởi thiết bị mạng truy cập trong phương án 1 và phương án 2 của sáng chế này.

Phương án 19 của sáng chế này cung cấp sản phẩm chương trình, trong đó sản phẩm chương trình bao gồm chương trình máy tính, chương trình máy tính được lưu trữ trong phương tiện lưu trữ có thể đọc được, và ít nhất một bộ xử lý của thiết bị mạng lõi thực hiện chương trình máy tính, sao cho thiết bị mạng lõi thực hiện các bước của các phương pháp được thực hiện bởi thiết bị mạng lõi trong phương án 1 và phương án 2 của sáng chế này.

Có thể hiểu rằng bộ xử lý trong sáng chế này có thể là bộ xử lý trung tâm (central processing unit, CPU), bộ xử lý đa năng, bộ xử lý tín hiệu số (digital signal processor, DSP), mạch tích hợp dành riêng cho ứng dụng (application-specific integrated circuit, ASIC), mảng cổng khả lập trình trường (field programmable gate array, FPGA), hoặc một thiết bị logic khả lập trình khác, thiết bị logic bóng bán dẫn, thành phần phần cứng, hoặc sự kết hợp bất kỳ của chúng. Bộ xử lý có thể triển khai hoặc thực thi các khối, các môđun, và các mạch logic minh họa được mô tả trong sáng chế này. Ngoài ra, bộ xử lý có thể là sự kết hợp của các bộ xử lý triển khai chức năng tính toán, ví dụ, sự kết hợp của một hoặc nhiều bộ vi xử lý hoặc kết hợp DSP và bộ vi xử lý.

Bus trong sáng chế này có thể là bus kiến trúc tiêu chuẩn công nghiệp (Industry Standard Architecture, ISA), bus kết nối thành phần ngoại vi (Peripheral Component Interconnect, PCI), bus kiến trúc tiêu chuẩn mở rộng (Extended Industry Standard Architecture, EISA), hoặc tương tự. Bus có thể được phân loại thành bus địa chỉ, bus dữ liệu, bus điều khiển, và loại tương tự. Để dễ thể hiện, bus trong các bản vẽ đi kèm của sáng chế này không giới hạn với chỉ một bus hoặc một loại bus.

Trong một vài phương án được cung cấp trong sáng chế này, các phương án của thiết bị được mô tả chỉ là các ví dụ. Ví dụ, sự phân chia môđun chỉ là sự phân chia chức năng logic và có thể là sự phân chia khác trong triển khai thực tế. Ví dụ, nhiều môđun hoặc thành phần có thể được kết hợp hoặc được tích hợp vào một hệ thống khác, hoặc một số tính năng có thể bị bỏ qua hoặc không được thực hiện. Ngoài ra, các khớp nối được hiển thị hoặc thảo luận hoặc khớp nối trực tiếp hoặc các kết nối truyền thông có thể được triển khai thông qua một số giao diện. Các khớp nối gián tiếp hoặc các kết nối truyền thông giữa các thiết bị hoặc các môđun có thể được triển khai bằng điện, cơ khí, hoặc các hình thức khác.

Các đơn vị được mô tả là các phần riêng biệt có thể hoặc không thể tách rời về mặt vật lý, nghĩa là, có thể được đặt trong một vị trí, hoặc có thể được phân phối trên nhiều đơn vị mạng. Một số hoặc tất cả các đơn vị có thể được lựa chọn dựa trên các yêu cầu thực tế để đạt được các mục đích của các giải pháp của các phương án.

YÊU CẦU BẢO HỘ

1. Phương pháp bảo vệ tính toàn vẹn dữ liệu, phương pháp này bao gồm các bước:

gửi (S101), bởi thiết bị đầu cuối, tin nhắn thứ nhất tới thiết bị mạng truy cập, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên đơn vị dữ liệu giao thức (Protocol Data Unit, PDU);

nhận (S104), bởi thiết bị đầu cuối, tin nhắn thứ hai từ thiết bị mạng truy cập, trong đó tin nhắn thứ hai bao gồm bộ nhận dạng của phiên PDU, và bộ nhận dạng của sóng mang rađio dữ liệu (Data Radio Bearer, DRB) tương ứng với phiên PDU; và

thực hiện, bởi thiết bị đầu cuối, sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán bảo vệ tính toàn vẹn và khóa tương ứng với phiên PDU, trong đó tin nhắn thứ hai bao gồm thuật toán bảo vệ tính toàn vẹn và thông tin cho khóa, hoặc thuật toán bảo vệ tính toàn vẹn và khóa được tạo cấu hình trước, trong đó đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng.

2. Phương pháp theo điểm 1, trong đó tin nhắn thứ hai còn bao gồm:

chỉ báo thứ nhất, trong đó chỉ báo thứ nhất được sử dụng để chỉ báo xem có kích hoạt chức năng bảo vệ tính toàn vẹn hay không.

3. Phương pháp theo điểm 2, trong đó tin nhắn thứ hai bao gồm cấu hình lớp giao thức hội tụ dữ liệu dữ liệu gói (PDCP: Packet Data Convergence Protocol), và cấu hình lớp PDCP bao gồm chỉ báo thứ nhất.

4. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó tin nhắn thứ hai còn bao gồm:

chỉ báo thứ hai, trong đó chỉ báo thứ hai được sử dụng để chỉ báo lớp giao thức nơi mà sự bảo vệ tính toàn vẹn được thực hiện.

5. Phương pháp theo điểm bất kỳ trong các điểm từ 1 đến 4, trong đó tin nhắn thứ hai bao gồm cấu hình lớp giao thức kết tập dữ liệu dịch vụ (Service Data Aggregation Protocol, SDAP), cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên PDU, và lớp SDAP được sử dụng để xử lý sự ánh xạ từ luồng sang DRB.

6. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 5, trong đó phiên PDU tương ứng với một hoặc nhiều DRB, và khi phiên PDU tương ứng với nhiều DRB, các cấu hình bảo vệ tính toàn vẹn được sử dụng cho nhiều DRB là như nhau, trong đó mỗi một trong số các cấu hình bảo vệ tính toàn vẹn bao gồm thuật toán bảo vệ tính toàn vẹn và khóa.

7. Phương pháp theo điểm bất kỳ trong các điểm từ 1 đến 6, trong đó dữ liệu của DRB là gói dữ liệu lớp PDCP.

8. Thiết bị truyền thông dùng trong thiết bị đầu cuối, thiết bị truyền thông này bao gồm:

phương tiện để gửi tin nhắn thứ nhất tới thiết bị mạng truy cập, trong đó tin nhắn thứ nhất được sử dụng để yêu cầu thiết lập phiên đơn vị dữ liệu giao thức (Protocol Data Unit, PDU);

phương tiện để nhận tin nhắn thứ hai từ thiết bị mạng truy cập, trong đó tin nhắn thứ hai bao gồm bộ nhận dạng của phiên PDU, và bộ nhận dạng của sóng mang rađio dữ liệu (Data Radio Bearer, DRB) tương ứng với phiên PDU; và

phương tiện để thực hiện sự bảo vệ tính toàn vẹn trên dữ liệu của DRB bằng cách sử dụng thuật toán bảo vệ tính toàn vẹn và khóa tương ứng với phiên PDU, trong đó tin nhắn thứ hai bao gồm thuật toán bảo vệ tính toàn vẹn và thông tin cho khóa, hoặc thuật toán bảo vệ tính toàn vẹn và khóa được tạo cấu hình trước, trong đó đối tượng cho sự bảo vệ tính toàn vẹn là dữ liệu mặt phẳng người dùng.

9. Thiết bị theo điểm 8, trong đó tin nhắn thứ hai bao gồm:

chỉ báo thứ nhất, trong đó chỉ báo thứ nhất được sử dụng để chỉ báo xem có kích hoạt chức năng bảo vệ tính toàn vẹn hay không.

10. Thiết bị theo điểm 9, trong đó tin nhắn thứ hai bao gồm cấu hình lớp giao thức hội tụ dữ liệu gói (Packet Data Convergence Protocol, PDCP), và cấu hình lớp PDCP bao gồm chỉ báo thứ nhất.

11. Thiết bị theo điểm bất kỳ trong số các điểm từ 8 đến 10, trong đó tin nhắn thứ hai còn bao gồm:

chỉ báo thứ hai, trong đó chỉ báo thứ hai được sử dụng để chỉ báo lớp giao thức nơi mà sự bảo vệ tính toàn vẹn được thực hiện.

12. Thiết bị theo điểm bất kỳ trong các điểm từ 8 đến 11, trong đó tin nhắn thứ hai bao gồm cấu hình lớp giao thức kết tập dữ liệu dịch vụ (Service Data Aggregation Protocol, SDAP), cấu hình lớp SDAP bao gồm bộ nhận dạng của phiên PDU, và lớp SDAP được sử dụng để xử lý sự ánh xạ từ luồng sang DRB.

13. Thiết bị theo điểm bất kỳ trong số các điểm từ 8 đến 12, trong đó phiên PDU tương ứng với một hoặc nhiều DRB, và khi phiên PDU tương ứng với nhiều DRB, các cấu hình bảo vệ tính toàn vẹn được sử dụng cho nhiều DRB là như nhau, trong đó mỗi một trong số các cấu hình bảo vệ tính toàn vẹn bao gồm thuật toán bảo vệ tính toàn vẹn và khóa.

14. Thiết bị theo điểm bất kỳ trong số các điểm từ 8 đến 13, trong đó dữ liệu của DRB là gói dữ liệu lớp PDCP.

15. Phương tiện đọc được bằng máy tính, bao gồm chương trình mà, khi được gọi và được thực thi bởi bộ xử lý của thiết bị đầu cuối, khiến cho thiết bị đầu cuối thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 7.

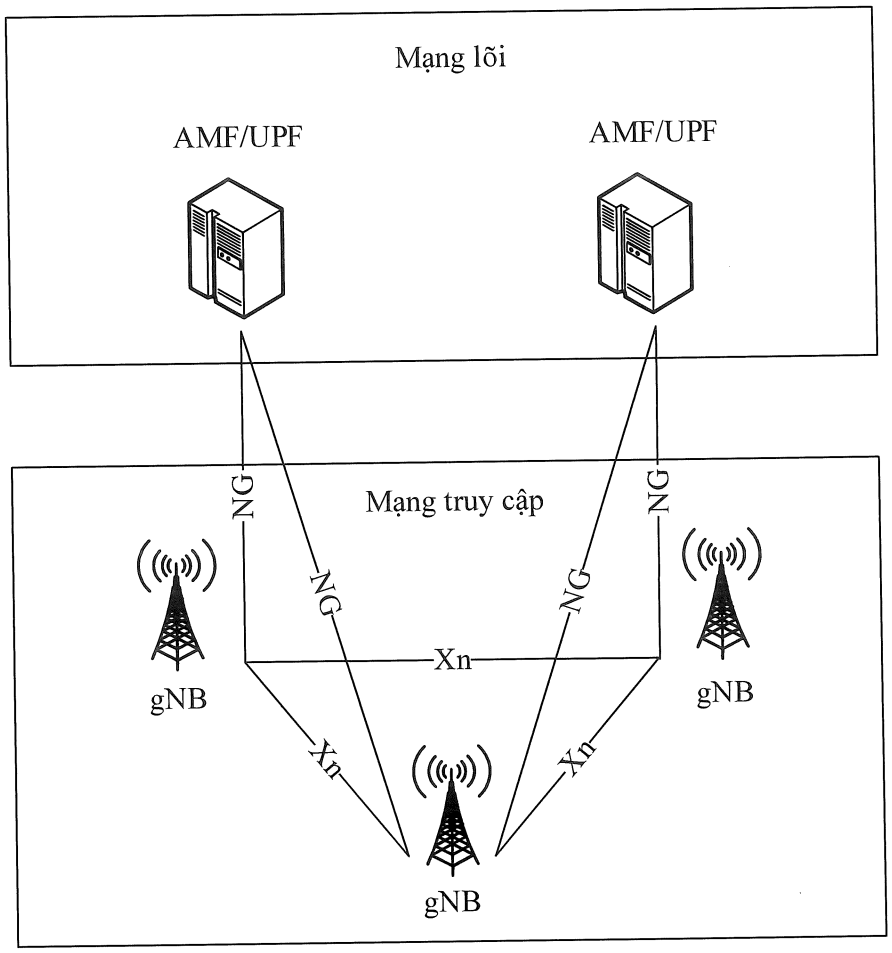
Mạng lõi
AMF/UPF
AMF/UPF
NG
NG
NG
NG
Mạng truy cập
Xn
gNB
gNB
Xn
Xn
gNB

FIG.1

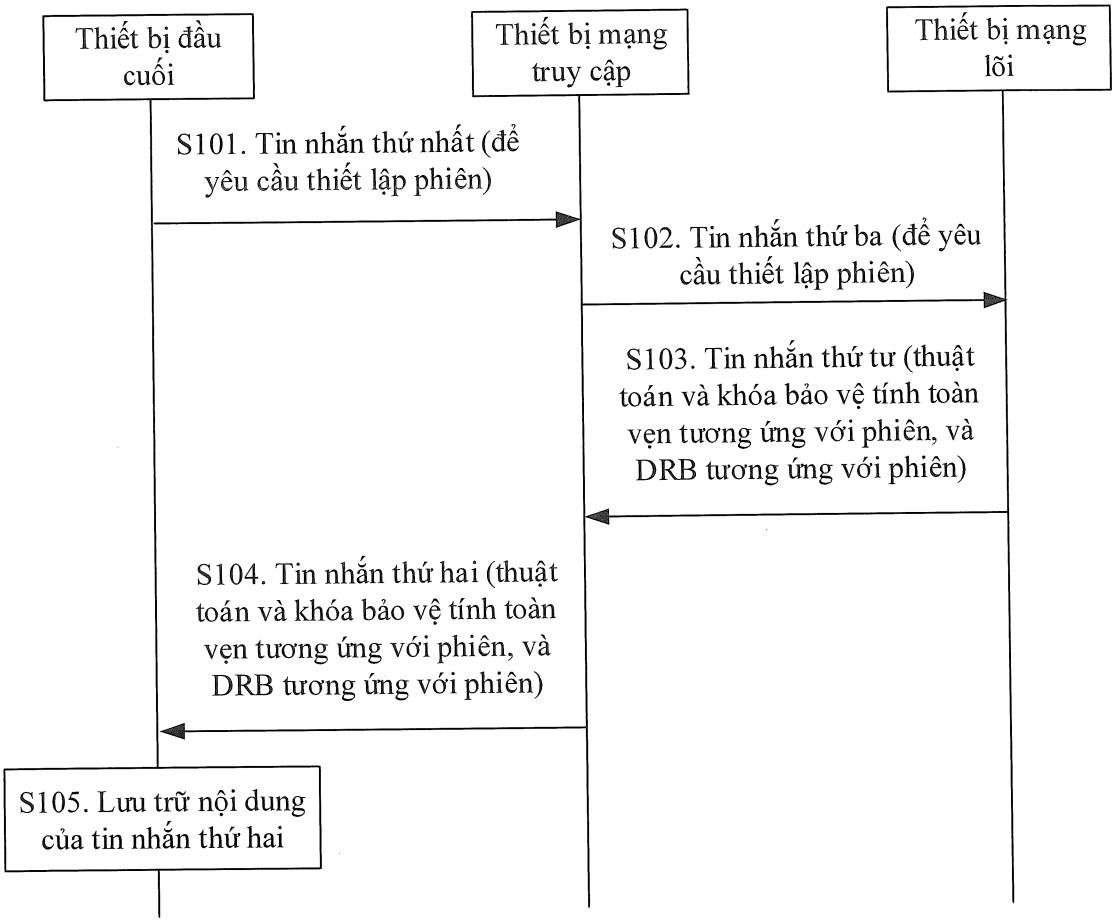
Thiết bị đầu cuối
Thiết bị mạng truy cập
Thiết bị mạng lõi
S101. Tin nhắn thứ nhất (để yêu cầu thiết lập phiên)
S102. Tin nhắn thứ ba (để yêu cầu thiết lập phiên)
S103. Tin nhắn thứ tư (thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và DRB tương ứng với phiên)
S104. Tin nhắn thứ hai (thuật toán và khóa bảo vệ tính toàn vẹn tương ứng với phiên, và DRB tương ứng với phiên)
S105. Lưu trữ nội dung của tin nhắn thứ hai

FIG.2

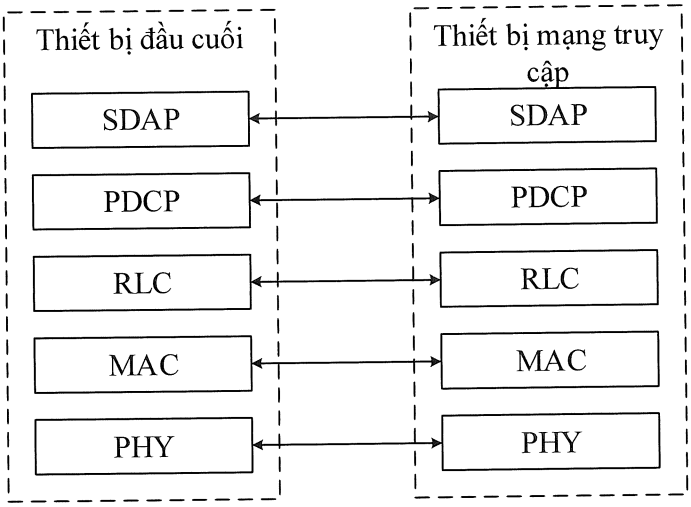
Thiết bị đầu cuối
Thiết bị mạng truy cập
SDAP
PDCP
RLC
MAC
PHY
SDAP
PDCP
RLC
MAC
PHY

FIG.3

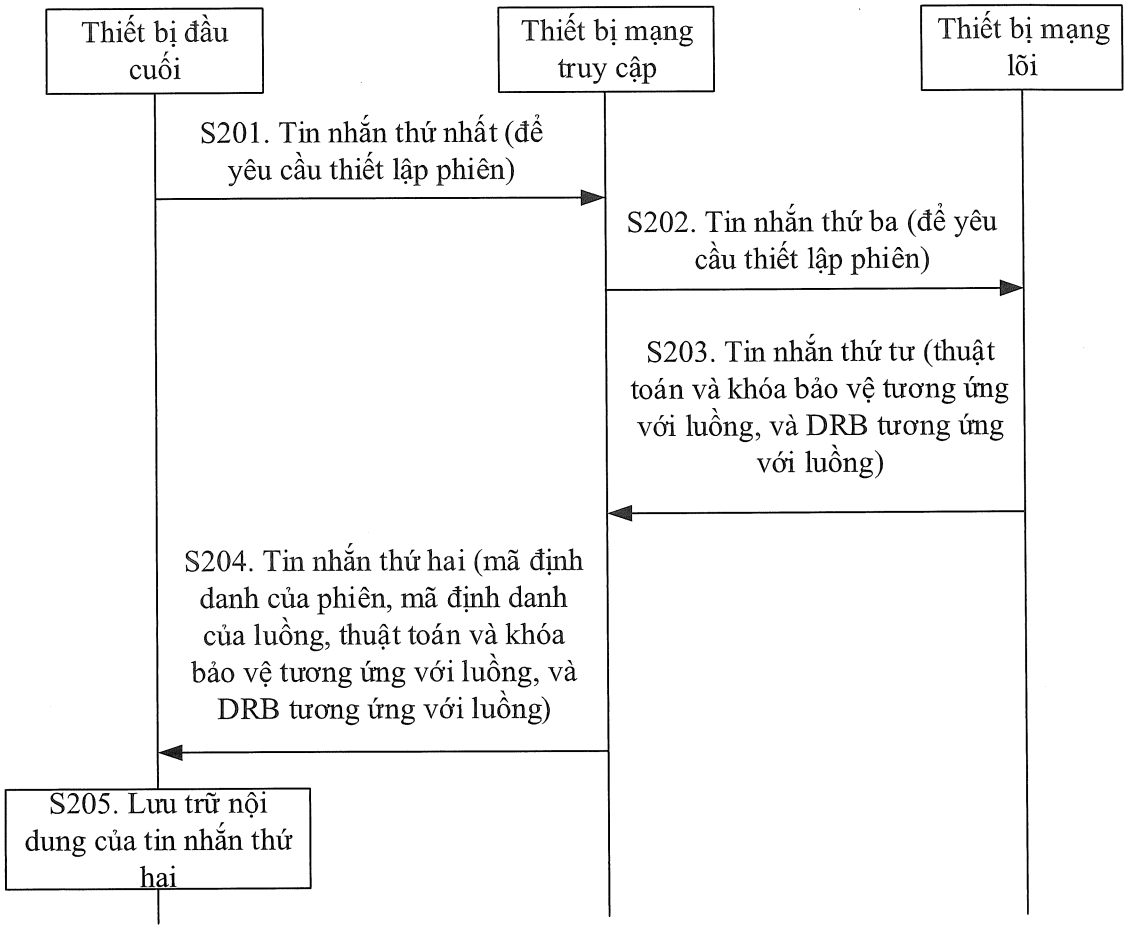
Thiết bị đầu cuối
Thiết bị mạng truy cập
Thiết bị mạng lõi
S201. Tin nhắn thứ nhất (để yêu cầu thiết lập phiên)
S202. Tin nhắn thứ ba (để yêu cầu thiết lập phiên)
S203. Tin nhắn thứ tư (thuật toán và khóa bảo vệ tương ứng với luồng, và DRB tương ứng với luồng)
S204. Tin nhắn thứ hai (mã định danh của phiên, mã định danh của luồng, thuật toán và khóa bảo vệ tương ứng với luồng, và DRB tương ứng với luồng)
S205. Lưu trữ nội dung của tin nhắn thứ hai

FIG.4

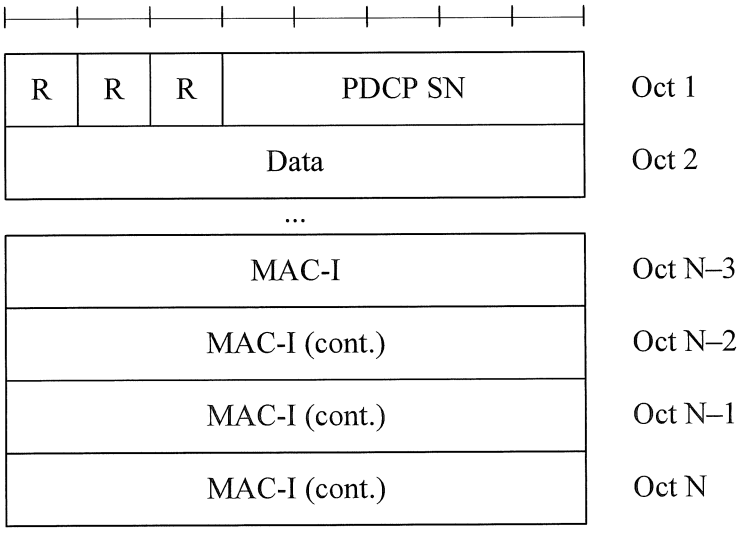
R
R
R
PDCP SN
Oct 1
Data
Oct 2
...
MAC-I
Oct N–3
MAC-I (cont.)
Oct N–2
MAC-I (cont.)
Oct N–1
MAC-I (cont.)
Oct N

FIG.5

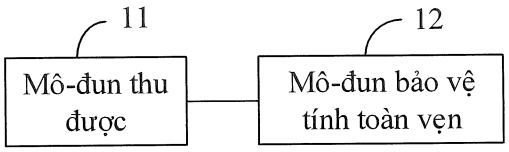

FIG.6

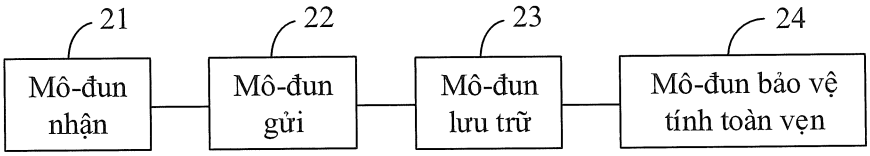

FIG.7

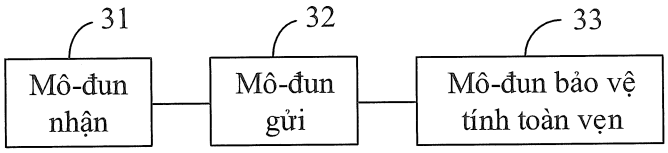

FIG.8

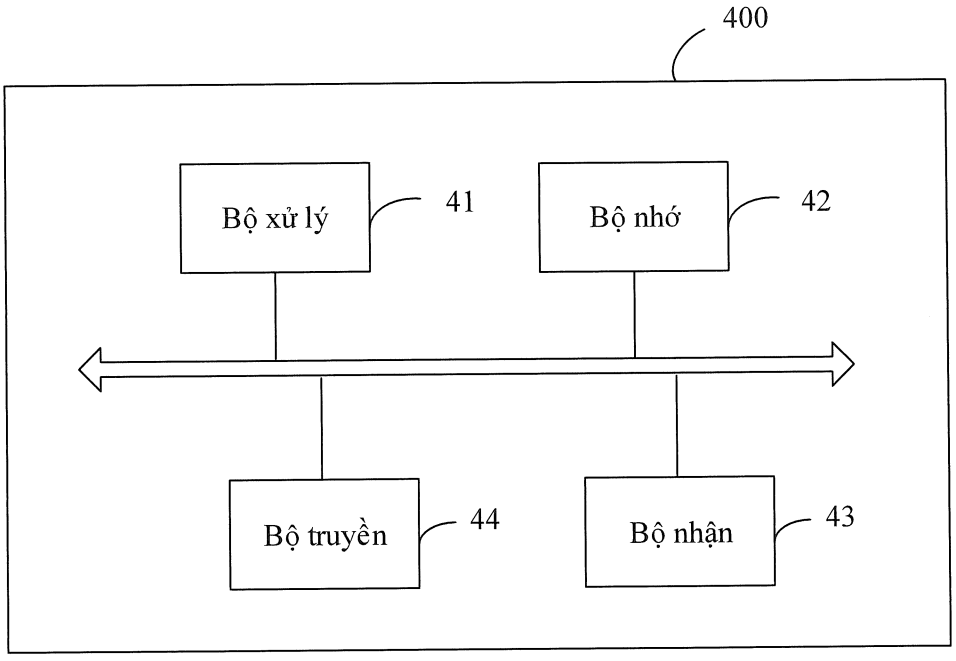

FIG.9

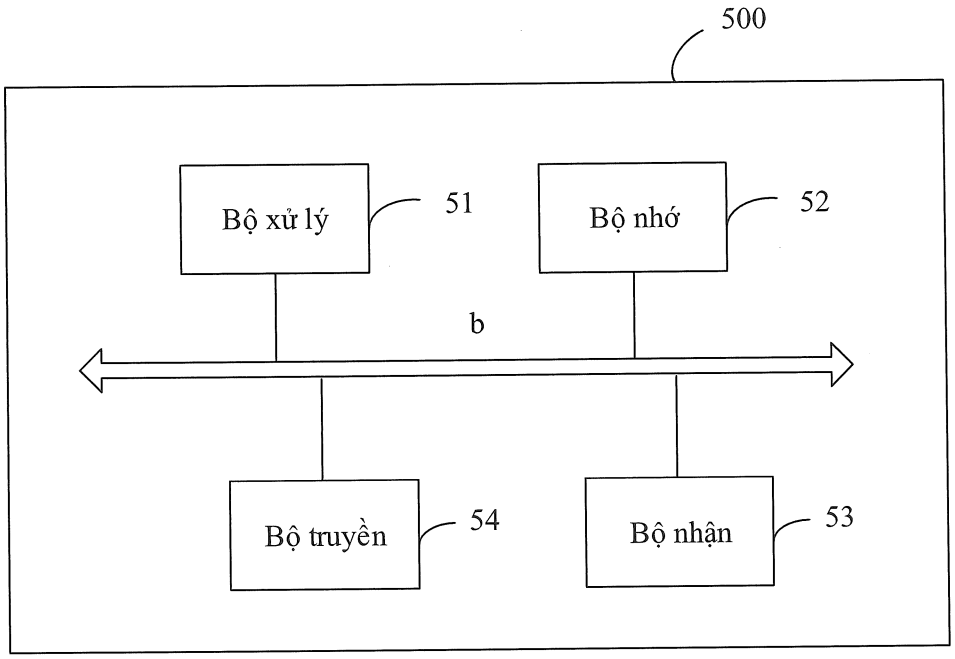
500
Bộ xử lý
51
Bộ nhớ
52
b
Bộ truyền
54
Bộ nhận
53

FIG.10

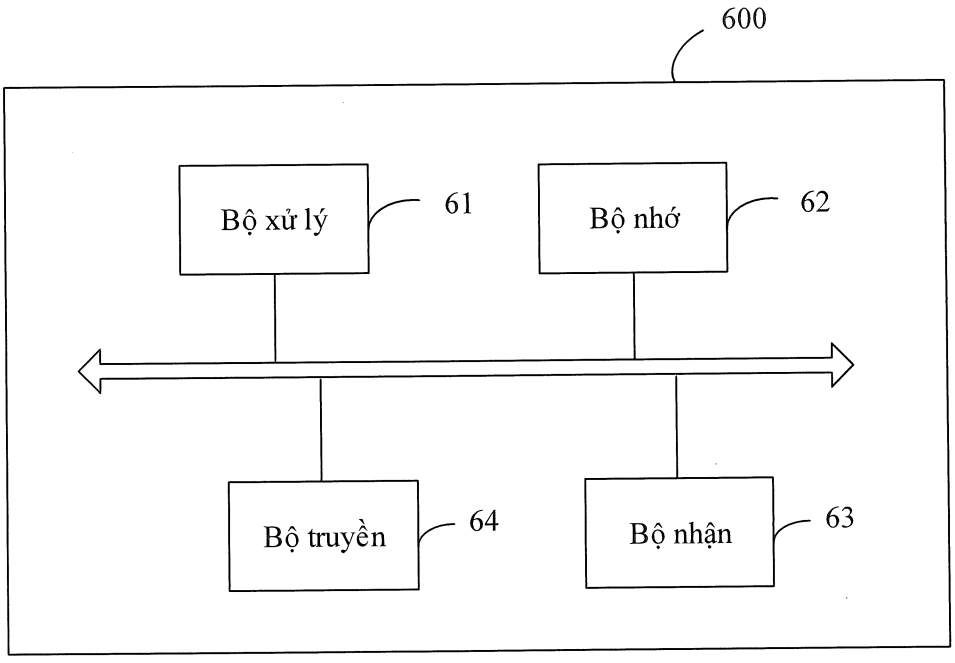
600
Bộ xử lý
61
Bộ nhớ
62
Bộ truyền
64
Bộ nhận
63

FIG.11