(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) **1-0049132**

(51)[2022.01] **H04W 12/00**

(13) **B**

(21) 1-2022-07685
(22) 14/05/2021
(86) PCT/CN2021/093828 14/05/2021
(87) WO2021/228227 18/11/2021
(30) 202010415321.3 15/05/2020 CN
(45) 25/07/2025 448
(43) 27/02/2023 419A
(73) VIVO MOBILE COMMUNICATION CO., LTD. (CN)
No.1, Vivo Road, Chang'an, Dongguan, Guangdong 523863, China
(72) ZHENG, Qian (CN).
(74) Công ty TNHH Đại Tín và Liên Danh (DAITIN AND ASSOCIATES CO.,LTD)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ XỬ LÝ LỖI BẢO VỆ TÍNH TOÀN VẸN, VÀ PHƯƠNG TIỆN LƯU TRỮ CÓ THỂ ĐỌC ĐƯỢC

(21) 1-2022-07685

(57) Sáng chế đề xuất phương pháp và thiết bị xử lý lỗi bảo vệ tính toàn vẹn, và phương tiện lưu trữ có thể đọc được. Phương pháp này bao gồm: thực hiện, bằng thiết bị người dùng thứ nhất, hành động kiểm soát bảo vệ ít nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho một kênh mang tín hiệu đường bên.

Fig.1

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực kỹ thuật truyền tin, và cụ thể là đề cập đến phương pháp và thiết bị xử lý lỗi bảo vệ tính toàn vẹn, và phương tiện lưu trữ có thể đọc được.

Tình trạng kỹ thuật của sáng chế

Truyền đường bên (Sidelink, SL) vô tuyến mới (New Radio, NR) chủ yếu được chia thành các chế độ là truyền rộng, truyền nhóm và truyền đơn điểm. Hiện tại, tín hiệu điều khiển tài nguyên vô tuyến (Radio Resource Control, RRC) đường bên đã được đưa vào truyền tin đơn điểm đường bên NR và một kênh mang vô tuyến để truyền tín hiệu RRC đường bên được gọi là kênh mang tín hiệu đường bên (Sidelink Signaling Bearer, SL-SRB). Để đảm bảo an toàn cho việc truyền tín hiệu, việc kiểm tra tính toàn vẹn cần được thực hiện đối với truyền trên kênh mang tín hiệu đường bên. Trong kỹ thuật trước đây, không có phương pháp xử lý nào cho các kênh mang tín hiệu đường bên trong trường hợp lỗi kiểm tra tính toàn vẹn, dẫn đến tính bảo vệ thấp của truyền tin đường bên.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp và thiết bị xử lý lỗi bảo vệ tính toàn vẹn và thiết bị người dùng, để giải quyết vấn đề là chưa có phương pháp xử lý tiếp theo trong trường hợp lỗi kiểm tra tính toàn vẹn cho các kênh mang tín hiệu đường bên của kỹ thuật liên quan, từ đó cải thiện hơn nữa tính bảo vệ của truyền tin đường bên.

Theo khía cạnh thứ nhất, một phương án thực hiện của sáng chế đề xuất phương pháp xử lý lỗi bảo vệ tính toàn vẹn, được áp dụng cho thiết bị người dùng thứ nhất, trong đó thiết bị người dùng thứ nhất thực hiện truyền tin đường bên dựa trên địa chỉ đích và phương pháp xử lý lỗi bảo vệ tính toàn vẹn bao gồm:

thực hiện hành động kiểm soát bảo vệ ít nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên.

Theo khía cạnh thứ hai, một phương án thực hiện của sáng chế đề xuất thiết bị xử lý lỗi bảo vệ tính toàn vẹn, được áp dụng cho thiết bị người dùng thứ nhất, trong đó thiết bị người dùng thứ nhất thực hiện truyền tin đường bên dựa trên địa chỉ đích và thiết bị bao gồm:

một mô-đun thực hiện thứ nhất, được cấu hình để thực hiện hành động kiểm soát bảo vệ trong ít nhất một trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên.

Theo khía cạnh thứ ba, một phương án thực hiện của sáng chế đề xuất thiết bị cho người dùng, bao gồm bộ xử lý, bộ nhớ và chương trình hoặc lệnh được lưu trữ trong bộ nhớ và có khả năng chạy trên bộ xử lý, khi chương trình hoặc lệnh được thực thi bởi bộ xử lý, thực hiện các bước của phương pháp xử lý lỗi bảo vệ tính toàn vẹn theo khía cạnh thứ nhất.

Theo khía cạnh thứ tư, một phương án thực hiện của sáng chế đề xuất một phương tiện lưu trữ có thể đọc được, trong đó một chương trình hoặc một lệnh được lưu trữ trong phương tiện lưu trữ có thể đọc được; và khi chương trình hoặc lệnh được thực thi bởi bộ xử lý, thực hiện các bước của phương pháp xử lý lỗi bảo vệ tính toàn vẹn theo khía cạnh thứ nhất.

Trong các phương án thực hiện của sáng chế, thiết bị người dùng thứ nhất thực hiện hành động kiểm soát bảo vệ trong ít nhất một trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên. Có nghĩa là, thực hiện hành động kiểm soát bảo vệ bởi thiết bị người dùng thứ nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên, từ đó có thể cải thiện tính bảo vệ của truyền tin đường bên.

Mô tả vắn tắt các hình vẽ

Fig.1 là lưu đồ minh họa phương pháp xử lý lỗi bảo vệ tính toàn vẹn theo một phương án thực hiện của sáng chế;

Fig.2 là sơ đồ cấu trúc minh họa chồng giao thức mặt phẳng điều khiển ở phía thiết bị người dùng;

Fig.3 là lưu đồ khác minh họa phương pháp xử lý lỗi bảo vệ tính toàn vẹn theo một phương án thực hiện của sáng chế;

Fig.4 là sơ đồ cấu trúc minh họa thiết bị xử lý lỗi bảo vệ tính toàn vẹn theo một phương án thực hiện của sáng chế; và

Fig.5 là sơ đồ cấu trúc minh họa thiết bị người dùng theo một phương án thực hiện của sáng chế.

Mô tả chi tiết sáng chế

Sau đây, các phương pháp thực hiện của sáng chế sẽ được mô tả rõ ràng hơn thông qua các phương án thực hiện cùng với các hình vẽ kèm theo. Rõ ràng, các phương án thực hiện được mô tả chỉ nhằm mục đích minh họa mà không giới hạn phạm vi của sáng chế. Dựa trên các phương án thực hiện, tất cả các phương án khác được đưa ra bởi người có trình độ trung bình trong cùng lĩnh vực kỹ thuật mà không có cải tiến vẫn thuộc phạm vi bảo hộ của sáng chế.

Trong đơn yêu cầu bảo hộ này, thuật ngữ "bao gồm" và bất kỳ sửa đổi nào trong đó nhằm mục đích bao hàm sự bao gồm không độc quyền, ví dụ, quy trình, phương pháp, hệ thống, sản phẩm hoặc thiết bị chứa một loạt các bước hoặc đơn vị không nhất thiết bị giới hạn các bước hoặc đơn vị được liệt kê rõ ràng, nhưng có thể bao gồm các bước hoặc đơn vị khác không được liệt kê rõ ràng hoặc vốn có của các quy trình, phương pháp, sản phẩm hoặc thiết bị này. Ngoài ra, "và/hoặc" được sử dụng trong đơn yêu cầu bảo hộ này có nghĩa là ít nhất một trong các đối tượng được kết nối. Ví dụ, A và/hoặc B đại diện cho ba trường hợp sau: chỉ A, chỉ B, hoặc cả A và B.

Theo các phương án của sáng chế, các từ như "ví dụ" hoặc "lấy ví dụ" được sử dụng để thể hiện việc đưa ra ví dụ, minh họa hoặc mô tả. Bất kỳ phương án hoặc sơ đồ thiết kế nào được mô tả là "ví dụ" hoặc "lấy ví dụ" theo các phương án của sáng chế không được giải thích là được ưu tiên hơn hoặc có nhiều ưu điểm hơn so với phương án hoặc sơ đồ thiết kế khác. Nói một cách chính xác, việc sử dụng thuật ngữ như "ví dụ" hoặc "lấy ví dụ" nhằm trình bày một khái niệm liên quan theo cách cụ thể.

Thuật ngữ "thứ nhất" và "thứ hai" trong đơn yêu cầu bảo hộ này này được sử dụng để phân biệt giữa các đối tượng tương tự và không cần được sử dụng để mô tả một thứ tự

hoặc trình tự cụ thể. Cần hiểu rằng các số được sử dụng theo cách này có thể hoán đổi cho nhau trong các trường hợp thích hợp để các phương án thực hiện của sáng chế được mô tả ở đây có thể được triển khai theo các thứ tự khác với thứ tự được minh họa hoặc mô tả.

Trước tiên, cần hiểu rõ rằng quy trình xử lý lỗi phát hiện tính toàn vẹn trên giao diện NR Uu của kỹ thuật trước đây không áp dụng cho các lỗi kiểm tra tính toàn vẹn của kênh mang tín hiệu đường bên. Đối với các lỗi phát hiện tính toàn vẹn trên giao diện Uu, việc thiết lập lại bảo vệ có thể được thực hiện thông qua việc chọn lại một tế bào thích hợp. Tuy nhiên, một đường bên được thiết lập giữa một cặp thiết bị người dùng đặc trưng (hoặc một cặp địa chỉ đích đặc trưng) và việc thiết lập lại bảo vệ không thể được thực hiện bằng các UE khác (hoặc các địa chỉ đích).

Cơ chế trong kỹ thuật trước đây không thể được áp dụng để xử lý lỗi kiểm tra tính toàn vẹn đối với các kênh mang tín hiệu đường bên, điều này cũng gây ra một số khó khăn cho việc triển khai các phương án thực hiện của sáng chế.

Fig.1 là lưu đồ minh họa phương pháp xử lý lỗi bảo vệ tính toàn vẹn theo một phương án thực hiện của sáng chế. Như được minh họa trên Fig.1, phương án thực hiện này của sáng chế đề xuất phương pháp xử lý lỗi bảo vệ tính toàn vẹn, được áp dụng cho thiết bị người dùng thứ nhất. Thiết bị người dùng thứ nhất thực hiện truyền tin đường bên dựa trên địa chỉ đích và phương pháp xử lý lỗi bảo vệ tính toàn vẹn bao gồm bước sau.

Bước 101: Thực hiện hành động kiểm soát bảo vệ ít nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên.

Như được minh họa trên Fig.2, Fig.2 là sơ đồ cấu trúc minh họa chồng giao thức mặt phẳng điều khiển ở phía thiết bị người dùng. Chồng giao thức mặt phẳng điều khiển bao gồm lớp vật lý (Physical Layer, PHY), lớp điều khiển truy cập môi trường (Medium Access Control, MAC), lớp điều khiển liên kết vô tuyến (Radio Link Control, RLC), giao thức hội tụ dữ liệu gói (Packet Data Convergence Protocol, PDCP), lớp điều khiển tài nguyên vô tuyến (Radio Resource Control, RRC) và tầng không truy cập (Non-Access Stratum, NAS). Lớp giao thức PDCP chủ yếu nhằm mục đích gửi hoặc nhận dữ liệu gói đến hoặc từ một thực thể PDCP ngang hàng, chủ yếu hoàn thành các chức năng sau: nén và giải nén tiêu đề gói IP, mã hóa dữ liệu và tín hiệu cũng như bảo vệ tính toàn vẹn của tín hiệu.

Chức năng bảo vệ tính toàn vẹn bao gồm hai quy trình bảo vệ tính toàn vẹn và kiểm tra tính toàn vẹn. Một thuật toán và một khóa cho chức năng bảo vệ tính toàn vẹn của thực thể PDCP được cấu hình bởi một lớp cao hơn. Khi một chức năng bảo vệ được kích hoạt, chức năng bảo vệ tính toàn vẹn sẽ được kích hoạt và chức năng này được áp dụng cho tất cả các đơn vị dữ liệu giao thức (Protocol Data Unit, PDU) PDCP được chỉ báo bởi lớp cao hơn.

Có thể thấy từ mô tả ở trên rằng trong một phương án thực hiện đặc trưng của sáng chế, chỉ báo lỗi kiểm tra tính toàn vẹn (Integrity Check Failure Indication) có thể được gửi bởi thực thể PDCP và phương pháp xử lý lỗi bảo vệ tính toàn vẹn được thực hiện bởi một thực thể điều khiển tài nguyên vô tuyến (Radio Resource Control, RRC).

Cần hiểu rằng, trong phương án thực hiện này của sáng chế, chỉ báo lỗi kiểm tra tính toàn vẹn không chỉ giới hạn ở việc thu được bằng cách gửi bởi thực thể PDCP, hoặc có thể nhận được bằng các phương tiện khác, điều này không bị giới hạn ở đây. Thiết bị người dùng thứ nhất có thể thực hiện hành động kiểm soát bảo vệ khi có thể xác định được lỗi kiểm tra tính toàn vẹn đối với kênh mang tín hiệu đường bên, điều này có thể cải thiện tính bảo vệ của truyền tin đường bên.

Nói cách khác, phương pháp xử lý lỗi bảo vệ tính toàn vẹn theo các phương án thực hiện đặc trưng của sáng chế được áp dụng cho thiết bị người dùng thứ nhất, trong đó thiết bị người dùng thứ nhất thực hiện truyền tin đường bên dựa trên địa chỉ đích. Phương pháp xử lý lỗi bảo vệ tính toàn vẹn bao gồm:

thực hiện hành động kiểm soát bảo vệ trong trường hợp phát hiện sự kiện lỗi kiểm tra tính toàn vẹn đối với kênh mang tín hiệu đường bên.

Tuy nhiên, trường hợp nhận chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên từ thực thể PDCP có thể được coi là phát hiện sự kiện lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên.

Theo một phương án thực hiện đặc trưng của sáng chế, thiết bị người dùng thứ nhất có thể là điện thoại di động, máy tính, thiết bị người dùng trong xe, hoặc tương tự. Địa chỉ đích là địa chỉ để truyền đơn điểm với thiết bị người dùng thứ nhất và địa chỉ đích có thể tương ứng với thiết bị người dùng thứ hai. Tuy nhiên, cần hiểu rằng thiết bị người dùng

thứ nhất có thể thiết lập nhiều truyền tin đường bên, nghĩa là thiết bị người dùng thứ nhất có thể có nhiều địa chỉ đích. Nhiều địa chỉ đích có thể tương ứng với một thiết bị người dùng đích hoặc có thể tương ứng với nhiều thiết bị người dùng đích. Nghĩa là, nhiều địa chỉ đích đều tương ứng với thiết bị người dùng thứ hai hoặc có thể tương ứng lần lượt với thiết bị người dùng thứ hai, thiết bị người dùng thứ ba, v.v.

Trong phương án thực hiện này, thiết bị người dùng thứ nhất thực hiện hành động kiểm soát bảo vệ ít nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên. Nghĩa là, việc thực hiện hành động kiểm soát bảo vệ bởi thiết bị người dùng thứ nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên sẽ cải thiện tính bảo vệ của truyền tin đường bên.

Trong một phương án thực hiện đặc trưng của sáng chế, tiêu chí đánh giá đối với các lỗi kiểm tra tính toàn vẹn khác nhau có thể được cấu hình bởi lớp cao hơn hoặc được xác định trước bởi một giao thức. Ví dụ, sau đây cung cấp các tiêu chí đánh giá cho các lỗi kiểm tra tính toàn vẹn khác nhau:

bất kỳ một PDCP PDU nào của kênh mang tín hiệu đường bên gặp lỗi kiểm tra tính toàn vẹn;

một số lượng được xác định trước của các PDU PDCP trùng lặp gặp phải lỗi kiểm tra tính toàn vẹn; và

một số lượng định trước của các PDU PDCP liên tiếp gặp phải lỗi kiểm tra tính toàn vẹn.

Như được minh họa trên Fig.3, theo một phương án thực hiện của sáng chế, phương pháp xử lý lỗi bảo vệ tính toàn vẹn còn bao gồm bước sau.

Bước 102: Thực hiện hành động kiểm soát bảo vệ trong trường hợp phát hiện lỗi liên kết vô tuyến đường bên.

Trình tự giữa bước 101 và bước 102 không bị giới hạn. Thiết bị người dùng thứ nhất có thể thực hiện hành động kiểm soát bảo vệ trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên và cũng có thể thực hiện hành động kiểm soát bảo vệ trong trường hợp phát hiện lỗi liên kết vô tuyến đường bên.

Phương pháp theo phương án thực hiện đặc trưng của sáng chế có thể được áp dụng cho truyền tin đường bên của các tiêu chuẩn truyền thông khác nhau. Trong trường hợp được áp dụng cho truyền tin đường bên của 5G NR, theo một phương án thực hiện của sáng chế, kênh mang tín hiệu đường bên là ít nhất một trong kênh mang tín hiệu đường bên 1 (nghĩa là SL-SRB1), kênh mang tín hiệu đường bên 2 (nghĩa là, SL-SRB2) và kênh mang tín hiệu đường bên 3 (nghĩa là SL-SRB3). Nghĩa là, trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn trên ít nhất một kênh mang tín hiệu đường bên là SL-SRB1, SL-SRB2 và SL-SRB3, thì hành động kiểm soát bảo vệ sẽ được thực hiện. SL-SRB1 được sử dụng để truyền tín hiệu PC5 (PC5 Signaling, PC5-S) mà kích hoạt bảo vệ, SL-SRB2 được sử dụng để truyền tín hiệu PC5-S mà yêu cầu bảo vệ và SL-SRB3 được sử dụng để truyền tín hiệu PC5 RRC mà yêu cầu bảo vệ. Bảo vệ ở đây đề cập đến các yêu cầu về mã hóa và bảo vệ tính toàn vẹn.

Nói cách khác, phương án thực hiện đặc trưng của sáng chế có thể được áp dụng cho một phần của kênh mang tín hiệu đường bên, hoặc có thể được áp dụng cho tất cả kênh mang tín hiệu đường bên.

Việc cấu hình chức năng bảo vệ tính toàn vẹn nhằm cải thiện tính bảo vệ của truyền tin, chẳng hạn như ngăn dữ liệu bị can thiệp. Khi một lỗi kiểm tra tính toàn vẹn xảy ra, nó chỉ báo rằng truyền tin đường bên không còn đáp ứng các yêu cầu bảo vệ và khi đó hành động kiểm soát bảo vệ có thể được thực hiện trong trường hợp này.

Theo phương án thực hiện đặc trưng của sáng chế, hành động kiểm soát bảo vệ có thể sử dụng một trong ba loại hoạt động sau.

Loại thứ nhất là ngắt một kênh mang hoặc kết nối liên quan cho truyền tin đường bên, do đó một đường hầm truyền cho truyền tin đường bên không còn tồn tại, do đó tránh tái tạo truyền tin đường bên.

Ví dụ, ngắt một đường truyền liên quan hoặc kết nối cho truyền tin đường bên có thể là ít nhất một trong các thao tác sau:

ngắt một kênh mang dữ liệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

ngắt một kênh mang tín hiệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích; và

ngắt kết nối RRC của giao diện PC5 tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích, trong đó giao diện đường bên còn được gọi là giao diện PC5.

Loại thứ hai là loại bỏ thông tin cấu hình liên quan của kênh mang tín hiệu đường bên, do đó không thể bắt đầu truyền tin đường bên.

Ví dụ, loại bỏ thông tin cấu hình liên quan của kênh mang tín hiệu đường bên có thể là ít nhất một trong các hoạt động sau:

loại bỏ thông tin cấu hình tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích; trong đó thông tin cấu hình có thể là thông tin cấu hình từ tín hiệu RRC, tín hiệu PC5 RRC, hoặc tín hiệu cấu hình trước (pre-configuration); và

loại bỏ khóa bảo vệ tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích; trong đó

khóa bảo vệ bao gồm KNRP, KNRP-sess, NRPEK, NRPIK và tương tự; K_{NRP} là khóa gốc được chia sẻ giữa hai thiết bị người dùng trong truyền tin đường bên và cần được trao đổi thông qua giao diện PC5; khóa gốc K_{NRP}-sess được sử dụng trong ngữ cảnh bảo vệ thực tế có thể được trích xuất từ K_{NRP}, và sau đó khóa mã hóa NRPEK được sử dụng bởi một thuật toán mã hóa và khóa tính toàn vẹn NRPIK được sử dụng bởi một thuật toán toàn vẹn còn được trích xuất từ K_{NRP}-sess. Loại thứ ba là dừng truyền tin đường bên bằng cách dừng bộ đếm thời gian, ví dụ:

dừng bộ hẹn giờ tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích hoặc dừng tất cả bộ hẹn giờ đối với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất.

Bộ hẹn giờ có thể được bao gồm trong thông tin cấu hình.

Tức là hành động kiểm soát bảo vệ cụ thể bao gồm ít nhất một trong các hoạt động sau:

ngắt một kênh mang dữ liệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

ngắt một kênh mang tín hiệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

ngắt kết nối điều khiển tài nguyên vô tuyến giao diện đường bên PC5 RRC tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

loại bỏ thông tin cấu hình tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

loại bỏ khóa bảo vệ tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích; và

dừng bộ hẹn giờ tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích hoặc dừng tất cả bộ hẹn giờ đối với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất.

Ví dụ, tất cả các bộ hẹn giờ liên quan đến truyền tin đường bên bị dừng hoặc bộ hẹn giờ liên quan đến truyền tin đường bên với địa chỉ đích bị dừng. Ngoài ra, bộ hẹn giờ bao gồm ít nhất T400 và T400 được sử dụng cho quy trình cấu hình lại RRC đường bên và được bắt đầu tại thời điểm khi UE đường bên gửi tin nhắn cấu hình lại RRC đường bên.

Theo một phương án thực hiện của sáng chế, ở bước 101, trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên, sau khi thực hiện hành động kiểm soát bảo vệ, phương pháp này còn bao gồm:

gửi một tin nhắn RRC tới một thiết bị phía mạng, trong đó tin nhắn RRC được sử dụng để báo cáo rằng truyền tin đường bên với địa chỉ đích bởi thiết bị người dùng thứ nhất không thành công.

Tin nhắn RRC được gửi đến thiết bị phía mạng có thể sử dụng tin nhắn thông tin thiết bị người dùng đường bên SidelinkUEInformation hiện có. Thiết bị người dùng thứ nhất gửi tin nhắn RRC đến thiết bị phía mạng để báo cáo rằng truyền tin đường bên với địa chỉ đích bởi thiết bị người dùng thứ nhất không thành công.

Sau khi nhận được tin nhắn, thiết bị phía mạng có thể ngắt các tài nguyên liên quan được phân bổ cho thiết bị người dùng thứ nhất để truyền tin với đường bên dựa trên địa chỉ đích, do đó giảm lãng phí tài nguyên.

Hơn nữa, tin nhắn RRC cũng được sử dụng để chỉ báo rằng nguyên nhân gây ra lỗi truyền tin đường bên là lỗi kiểm tra tính toàn vẹn, để thông báo cho thiết bị phía mạng về nguyên nhân gây ra lỗi truyền tin đường bên. Bằng cách này, thiết bị phía mạng có thể thực hiện xử lý tập trung dựa trên nguyên nhân gây ra lỗi truyền tin đường bên, cải thiện độ chính xác của việc xử lý.

Theo một phương án thực hiện của sáng chế, trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên, sau khi thực hiện hành động kiểm soát bảo vệ, phương pháp này còn bao gồm:

gửi thông tin chỉ báo đến một thực thể lớp trên của thiết bị người dùng thứ nhất, trong đó thông tin chỉ báo được sử dụng để thông báo rằng kết nối PC5 RRC đã được ngắt.

Theo một phương án thực hiện đặc trưng của sáng chế, thực thể lớp trên có thể là một thực thể nằm trên một tầng truy cập (Access Stratum, AS), ví dụ, một lớp V2X và một lớp ứng dụng.

Sau khi thiết bị người dùng thứ nhất thực hiện hành động kiểm soát bảo vệ, thông tin chỉ báo được gửi đến thực thể lớp trên của thiết bị người dùng thứ nhất, để thực thể lớp trên dừng truyền tin đường bên dựa trên địa chỉ đích, ngăn chặn thực thể lớp trên khỏi việc tiếp tục xử lý và / hoặc gửi dữ liệu cần được truyền thông qua đường bên.

Hơn nữa, thông tin chỉ báo còn được sử dụng để thông báo rằng nguyên nhân khiến kết nối PC5 RRC bị ngắt là lỗi kiểm tra tính toàn vẹn hoặc lỗi kết nối PC5 RRC.

Theo một phương án thực hiện của sáng chế, phương pháp xử lý lỗi bảo vệ tính toàn vẹn còn bao gồm:

gửi một tin nhắn PC5 RRC tới thiết bị người dùng thứ hai tương ứng với địa chỉ đích, trong đó tin nhắn PC5 RRC được sử dụng để chỉ báo thiết bị người dùng thứ hai dừng truyền tin đường bên được thực hiện dựa trên địa chỉ đích.

Bước trong phương án thực hiện này có thể được thực hiện trước khi thiết bị người dùng thứ nhất thực hiện hành động kiểm soát bảo vệ hoặc có thể được thực hiện sau khi thiết bị người dùng thứ nhất thực hiện hành động kiểm soát bảo vệ và trình tự thực hiện của bước này phụ thuộc vào nội dung cụ thể của hành động kiểm soát bảo vệ. Khi hành động gửi tin nhắn PC5 RRC được thực hiện trước hành động kiểm soát bảo vệ, nó không bị ảnh hưởng bởi nội dung cụ thể của hành động kiểm soát bảo vệ. Tuy nhiên, khi hành động gửi tin nhắn PC5 RRC được thực hiện sau khi thiết bị người dùng thứ nhất thực hiện hành động kiểm soát bảo vệ, thì hành động kiểm soát bảo vệ được thực hiện bởi thiết bị người dùng thứ nhất không bao gồm việc ngắt kênh mang tín hiệu, tức là ít nhất thực hiện một hành động kiểm soát bảo vệ của thiết bị người dùng thứ nhất không bao gồm việc ngắt kênh mang tín hiệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích. Tin nhắn PC5 RRC có thể được truyền bằng cách sử dụng kênh mang tín hiệu được dự phòng trong trường hợp này vì kênh mang tín hiệu chưa được ngắt.

Hoạt động dừng truyền tin đường bên dựa trên địa chỉ đích bởi thiết bị người dùng thứ hai có thể bao gồm: ngắt kênh mang dữ liệu tương ứng (ngắt kênh mang liên quan hoặc kết nối cho truyền tin đường bên như được mô tả ở trên), ngắt thông tin cấu hình tương ứng (loại bỏ thông tin cấu hình liên quan cho kênh mang tín hiệu đường bên như được mô tả ở trên), và những thứ tương tự.

Thiết bị người dùng thứ nhất sẽ gửi tin nhắn PC5 RRC đến thiết bị người dùng thứ hai, do đó thiết bị người dùng thứ hai không cần giám sát và nhận dữ liệu dựa trên địa chỉ đích nữa.

Ngoài ra, tin nhắn PC5 RRC mang chỉ báo thiết lập lại cấu hình đường bên. Tin nhắn PC5 RRC có thể là tin nhắn chuyên dụng cho PC5 RRC, ví dụ, là tin nhắn sl-ResetConfig-r16 (tin nhắn đặt lại cấu hình đường bên R16). Tin nhắn sl-ResetConfig-r16 được sử dụng để thông báo cho thiết bị người dùng thứ hai rằng cả kênh mang dữ liệu và cấu hình tương ứng với truyền tin đường bên được thực hiện dựa trên địa chỉ đích đều được

ngắt, do đó thiết bị người dùng thứ hai không cần giám sát và nhận dữ liệu dựa trên trên địa chỉ đích nữa, điều này có thể giảm mức tiêu thụ năng lượng của thiết bị người dùng và tài nguyên của bộ xử lý.

Tham khảo Fig.4, Fig.4 là sơ đồ cấu trúc minh họa thiết bị xử lý lỗi bảo vệ tính toàn vẹn theo một phương án thực hiện của sáng chế. Thiết bị được áp dụng cho thiết bị người dùng thứ nhất và thiết bị người dùng thứ nhất thực hiện truyền tin đường bên dựa trên địa chỉ đích. Như được minh họa trên Fig.4, thiết bị xử lý lỗi bảo vệ tính toàn vẹn 300 bao gồm:

mô-đun thực hiện thứ nhất 301, được cấu hình để thực hiện hành động kiểm soát bảo vệ ít nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn đối với kênh mang tín hiệu đường bên.

Trong một phương án thực hiện của sáng chế, chỉ báo lỗi kiểm tra tính toàn vẹn được gửi bởi một thực thể giao thức hội tụ dữ liệu gói (Packet Data Convergence Protocol, PDCP).

Trong một phương án thực hiện của sáng chế, thiết bị xử lý lỗi bảo vệ tính toàn vẹn 300 còn bao gồm:

mô-đun thực hiện thứ hai, được cấu hình để thực hiện hành động kiểm soát bảo vệ trong trường hợp phát hiện thấy lỗi liên kết vô tuyến đường bên.

Theo một phương án thực hiện của sáng chế, kênh mang tín hiệu đường bên là ít nhất một trong kênh mang tín hiệu đường bên 1, kênh mang tín hiệu đường bên 2 và kênh mang tín hiệu đường bên 3.

Trong một phương án thực hiện của sáng chế, hành động kiểm soát bảo vệ cụ thể bao gồm ít nhất một trong các hoạt động sau:

ngắt một kênh mang dữ liệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

ngắt một kênh mang tín hiệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

ngắt kết nối điều khiển tài nguyên vô tuyến giao diện đường bên PC5 RRC tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

loại bỏ thông tin cấu hình tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

loại bỏ khóa bảo vệ tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích; và

dừng bộ hẹn giờ tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích hoặc dừng tất cả bộ hẹn giờ đối với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất.

Trong một phương án thực hiện của sáng chế, thiết bị xử lý lỗi bảo vệ tính toàn vẹn 300 còn bao gồm:

mô-đun gửi thứ nhất, được cấu hình để gửi tin nhắn RRC đến thiết bị phía mạng, trong đó tin nhắn RRC được sử dụng để báo cáo rằng truyền tin đường bên với địa chỉ đích bởi thiết bị người dùng thứ nhất không thành công.

Trong một phương án thực hiện của sáng chế, tin nhắn RRC còn được sử dụng để chỉ báo rằng nguyên nhân gây ra lỗi truyền tin đường bên là lỗi kiểm tra tính toàn vẹn.

Theo một phương án thực hiện của sáng chế, thiết bị còn bao gồm:

mô-đun gửi thứ hai, được cấu hình để gửi thông tin chỉ báo đến thực thể lớp trên của thiết bị người dùng thứ nhất, trong đó thông tin chỉ báo được sử dụng để thông báo rằng kết nối PC5 RRC đã được ngắt.

Trong một phương án thực hiện của sáng chế, thông tin chỉ báo còn được sử dụng để thông báo rằng nguyên nhân khiến kết nối PC5 RRC bị ngắt là do lỗi kiểm tra tính toàn vẹn hoặc lỗi của kết nối PC5 RRC.

Trong một phương án thực hiện của sáng chế, thiết bị xử lý lỗi bảo vệ tính toàn vẹn 300 còn bao gồm:

mô-đun gửi thứ ba, được cấu hình để gửi tin nhắn PC5 RRC đến thiết bị người dùng thứ hai tương ứng với địa chỉ đích, trong đó tin nhắn PC5 RRC được sử dụng để chỉ báo thiết bị người dùng thứ hai dừng truyền tin đường bên được thực hiện dựa trên địa chỉ đích.

Trong một phương án thực hiện của sáng chế, tin nhắn PC5 RRC mang chỉ báo thiết lập lại cấu hình đường bên.

Thiết bị xử lý lỗi bảo vệ tính toàn vẹn 300 theo phương án thực hiện này của sáng chế có khả năng thực hiện các quy trình của phương án được minh họa trên Fig.1 và Fig.3. Để tránh lặp lại, không mô tả lại ở đây. Trong phương án thực hiện này, thiết bị người dùng thứ nhất thực hiện hành động kiểm soát bảo vệ ít nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên. Nghĩa là, việc thực hiện hành động kiểm soát bảo vệ bởi thiết bị người dùng thứ nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên sẽ cải thiện tính bảo vệ của truyền tin đường bên.

Cần lưu ý rằng thiết bị xử lý lỗi bảo vệ tính toàn vẹn trong phương án thực hiện của sáng chế có thể là một thiết bị, hoặc có thể là một bộ phận, mạch tích hợp hoặc chip trong thiết bị người dùng.

Fig.5 là sơ đồ minh họa cấu trúc phần cứng của thiết bị người dùng để triển khai các phương án thực hiện của sáng chế.

Thiết bị người dùng 400 bao gồm nhưng không giới hạn ở các thành phần như đơn vị tần số vô tuyến 401, mô-đun mạng 402, đơn vị đầu ra âm thanh 403, đơn vị đầu vào 404, cảm biến 405, đơn vị hiển thị 406, đơn vị đầu vào của người dùng 407, đơn vị giao diện 408, bộ nhớ 409 và bộ xử lý 410.

Người có trình độ trong cùng lĩnh vực kỹ thuật có thể hiểu rằng thiết bị người dùng 400 còn có thể bao gồm nguồn điện (ví dụ, pin) cung cấp năng lượng cho các bộ phận và nguồn điện có thể được kết nối hợp lý với bộ xử lý 410 thông qua hệ thống quản lý nguồn. Theo cách này, các chức năng như quản lý xạc, xả và quản lý tiêu thụ điện năng được thực hiện bằng cách sử dụng hệ thống quản lý nguồn. Cấu trúc của thiết bị người dùng được minh họa trên Fig.5 không tạo thành bất kỳ giới hạn nào đối với thiết bị người dùng. Thiết bị người dùng có thể bao gồm nhiều hơn hoặc ít thành phần hơn những thành phần được

minh họa trên Fig.5, hoặc tổ hợp của một số thành phần, hoặc các thành phần được bố trí khác nhau. Chi tiết không được mô tả lại ở đây.

Bộ xử lý 410 được cấu hình để thực hiện hành động kiểm soát bảo vệ trong ít nhất một trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên.

Hơn nữa, chỉ báo lỗi kiểm tra tính toàn vẹn được gửi bởi một thực thể giao thức hội tụ dữ liệu gói PDCP.

Ngoài ra, bộ xử lý 410 còn được cấu hình để thực hiện hành động kiểm soát bảo vệ trong trường hợp phát hiện thấy lỗi liên kết vô tuyến đường bên.

Hơn nữa, kênh mang tín hiệu đường bên là ít nhất một trong kênh mang tín hiệu đường bên 1, kênh mang tín hiệu đường bên 2 và kênh mang tín hiệu đường bên 3.

Hơn nữa, hành động kiểm soát bảo vệ cụ thể bao gồm ít nhất một trong các hoạt động sau:

ngắt một kênh mang dữ liệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

ngắt một kênh mang tín hiệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

ngắt một kết nối điều khiển tài nguyên vô tuyến giao diện đường bên PC5 RRC tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

loại bỏ thông tin cấu hình tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

loại bỏ khóa bảo vệ tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích; và

dừng một bộ đếm thời gian tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích hoặc dừng tất cả các bộ hẹn giờ cho truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất.

Hơn nữa, đơn vị tần số vô tuyến 401 được cấu hình để gửi tin nhắn RRC đến thiết bị phía mạng, trong đó tin nhắn RRC được sử dụng để báo cáo rằng truyền tin đường bên với địa chỉ đích bởi thiết bị người dùng thứ nhất không thành công.

Hơn nữa, tin nhắn RRC còn được sử dụng để chỉ báo rằng nguyên nhân của lỗi truyền tin đường bên là lỗi kiểm tra tính toàn vẹn.

Hơn nữa, đơn vị tần số vô tuyến 401 được cấu hình để gửi thông tin chỉ báo đến thực thể lớp trên của thiết bị người dùng thứ nhất, trong đó thông tin chỉ báo được sử dụng để thông báo rằng kết nối PC5 RRC đã được ngắt.

Hơn nữa, thông tin chỉ báo còn được sử dụng để thông báo rằng nguyên nhân khiến kết nối PC5 RRC bị ngắt là lỗi kiểm tra tính toàn vẹn hoặc lỗi kết nối PC5 RRC.

Hơn nữa, đơn vị tần số vô tuyến 401 được cấu hình để gửi một tin nhắn PC5 RRC tới thiết bị người dùng thứ hai tương ứng với địa chỉ đích, trong đó tin nhắn PC5 RRC được sử dụng để chỉ báo thiết bị người dùng thứ hai dừng truyền tin đường bên được thực hiện dựa trên địa chỉ đích.

Hơn nữa, tin nhắn PC5 RRC mang chỉ báo đặt lại cấu hình đường bên.

Theo tùy chọn, một phương án thực hiện của sáng chế còn đề xuất thiết bị người dùng, bao gồm bộ xử lý 410, bộ nhớ 409 và chương trình hoặc lệnh được lưu trữ trong bộ nhớ 409 và có khả năng chạy trên bộ xử lý 410. Khi chương trình hoặc lệnh được thực thi bởi bộ xử lý 410, thực hiện các quy trình của phương pháp xử lý lỗi bảo vệ tính toàn vẹn nêu trên, với cùng hiệu quả kỹ thuật. Để tránh lặp lại, chi tiết không được mô tả lại ở đây.

Một phương án thực hiện của sáng chế còn đề xuất một chip, trong đó chip bao gồm một bộ xử lý và một giao diện truyền tin. Giao diện truyền tin được kết hợp với bộ xử lý và bộ xử lý được cấu hình để chạy một chương trình hoặc một lệnh để triển khai các quy trình của phương pháp xử lý lỗi bảo vệ tính toàn vẹn nêu trên, với cùng hiệu quả kỹ thuật. Để tránh lặp lại, chi tiết không được mô tả lại ở đây.

Cần hiểu rằng chip được đề cập trong phương án thực hiện này của sáng chế cũng có thể được gọi là chip cấp hệ thống, chip hệ thống, hệ thống chip, hệ thống trên chip hoặc tương tự.

Cần lưu ý rằng trong đơn yêu cầu bảo hộ này, thuật ngữ "gồm có", "bao gồm", hoặc bất kỳ biến thể nào khác của chúng nhằm bao hàm sự bao gồm không loại trừ, để một tiến trình, một phương pháp, một mục hoặc một thiết bị bao gồm danh sách các yếu tố không chỉ bao gồm các yếu tố đó mà còn bao gồm các yếu tố khác không được liệt kê rõ ràng, hoặc còn bao gồm các yếu tố vốn có trong tiến trình, phương pháp, mục hoặc thiết bị đó. Trong trường hợp không có nhiều ràng buộc hơn, một phần tử đứng trước "bao gồm một..." không loại trừ sự tồn tại của các phần tử giống hệt nhau khác trong tiến trình, phương pháp, mục hoặc thiết bị bao gồm phần tử đó. Ngoài ra, cần lưu ý rằng phạm vi của phương pháp và thiết bị trong các phương án thực hiện của sáng chế không giới hạn ở việc thực hiện các chức năng theo thứ tự được trình bày hoặc thảo luận, mà còn có thể bao gồm việc thực hiện các chức năng theo cách cơ bản đồng thời hoặc theo một thứ tự ngược lại, tùy thuộc vào các chức năng liên quan. Ví dụ, các phương pháp được mô tả có thể được thực hiện theo thứ tự khác với thứ tự được mô tả và các bước có thể được thêm vào, bỏ qua hoặc kết hợp với nhau. Ngoài ra, các tính năng được mô tả có tham chiếu đến một số ví dụ có thể được kết hợp trong các ví dụ khác.

Theo mô tả các phương án thực hiện sáng chế ở trên, người có trình độ trung bình trong cùng lĩnh vực kỹ thuật có thể hiểu rõ ràng rằng phương pháp trong các phương án thực hiện nêu trên có thể được triển khai bằng phần mềm ngoài nền tảng phần cứng phổ thông cần thiết hoặc chỉ bằng phần cứng. Trong hầu hết các trường hợp, cách triển khai trước đây được ưu tiên hơn. Dựa trên sự hiểu biết như vậy, các phương pháp thực hiện của sáng chế về cơ bản, hoặc phần đóng góp vào kỹ thuật trước đây có thể được triển khai dưới dạng một sản phẩm phần mềm. Sản phẩm phần mềm máy tính được lưu trữ trong một phương tiện lưu trữ (ví dụ: ROM/RAM, đĩa từ hoặc đĩa quang) và bao gồm một số lệnh để chỉ dẫn thiết bị đầu cuối (có thể là điện thoại di động, máy tính, máy chủ, máy điều hòa không khí, thiết bị mạng, hoặc loại tương tự) để thực hiện phương pháp được mô tả trong các phương án thực hiện của sáng chế.

Các phương án thực hiện của sáng chế được mô tả ở trên có tham chiếu đến các hình vẽ kèm theo, nhưng sáng chế không giới hạn ở các phương án thực hiện đã nêu. Các

phương án thực hiện chỉ mang tính minh họa mà không giới hạn phạm vi của sáng chế. Dựa vào phần mô tả, người có trình độ trung bình trong cùng lĩnh vực kỹ thuật có thể thực hiện nhiều biến thể khác mà vẫn thuộc phạm vi bảo hộ của sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp xử lý lỗi bảo vệ tính toàn vẹn, được áp dụng cho thiết bị người dùng thứ nhất, trong đó thiết bị người dùng thứ nhất thực hiện truyền tin đường bên dựa trên địa chỉ đích và phương pháp xử lý lỗi bảo vệ tính toàn vẹn bao gồm:

thực hiện hành động kiểm soát bảo vệ ít nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên.

2. Phương pháp xử lý lỗi bảo vệ tính toàn vẹn theo điểm 1, trong đó chỉ báo lỗi kiểm tra tính toàn vẹn được gửi bởi một thực thể giao thức hội tụ dữ liệu gói (Packet Data Convergence Protocol, PDCP).

3. Phương pháp xử lý lỗi bảo vệ tính toàn vẹn theo điểm 1, còn bao gồm:

thực hiện hành động kiểm soát bảo vệ trong trường hợp phát hiện thấy lỗi liên kết vô tuyến đường bên.

4. Phương pháp xử lý lỗi bảo vệ tính toàn vẹn theo điểm 1, trong đó kênh mang tín hiệu đường bên là ít nhất một trong kênh mang tín hiệu đường bên 1, kênh mang tín hiệu đường bên 2 và kênh mang tín hiệu đường bên 3.

5. Phương thức xử lý theo điểm 1, trong đó hành động kiểm soát bảo vệ cụ thể bao gồm ít nhất một trong các hoạt động sau:

ngắt một kênh mang dữ liệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

ngắt một kênh mang tín hiệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

ngắt kết nối điều khiển tài nguyên vô tuyến giao diện đường bên (Sidelink Interface Radio Resource Control, PC5 RRC) tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

loại bỏ thông tin cấu hình tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

loại bỏ khóa bảo vệ tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích; và

dừng bộ hẹn giờ tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích hoặc dừng tất cả bộ hẹn giờ đối với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất.

6. Phương pháp xử lý theo điểm bất kỳ trong các điểm 1-5, trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên, sau khi thực hiện hành động kiểm soát bảo vệ, còn bao gồm:

gửi tin nhắn RRC đến thiết bị phía mạng, trong đó tin nhắn RRC được sử dụng để báo cáo rằng truyền tin đường bên với địa chỉ đích bởi thiết bị người dùng thứ nhất không thành công.

7. Phương pháp xử lý theo điểm 6, trong đó tin nhắn RRC còn được sử dụng để chỉ báo rằng nguyên nhân của lỗi truyền tin đường bên là lỗi kiểm tra tính toàn vẹn.

8. Phương pháp xử lý theo điểm bất kỳ trong các điểm 1-5, trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên, sau khi thực hiện hành động kiểm soát bảo vệ, bao gồm:

gửi thông tin chỉ báo đến một thực thể lớp trên của thiết bị người dùng thứ nhất, trong đó thông tin chỉ báo được sử dụng để thông báo rằng kết nối PC5 RRC đã được ngắt.

9. Phương pháp xử lý theo điểm 8, trong đó thông tin chỉ báo còn được sử dụng để thông báo rằng nguyên nhân khiến kết nối PC5 RRC bị ngắt là lỗi kiểm tra tính toàn vẹn hoặc lỗi kết nối PC5 RRC.

10. Phương pháp xử lý theo điểm bất kỳ trong các điểm 1-5, còn bao gồm:

gửi một tin nhắn PC5 RRC đến thiết bị người dùng thứ hai tương ứng với địa chỉ đích, trong đó tin nhắn PC5 RRC được sử dụng để chỉ báo thiết bị người dùng thứ hai dừng truyền tin đường bên được thực hiện dựa trên địa chỉ đích.

11. Phương pháp xử lý theo điểm 10, trong đó tin nhắn PC5 RRC mang chỉ báo đặt lại cấu hình đường bên.

12. Thiết bị xử lý lỗi bảo vệ tính toàn vẹn, được áp dụng cho thiết bị người dùng thứ nhất, trong đó thiết bị người dùng thứ nhất thực hiện truyền tin đường bên dựa trên địa chỉ đích và thiết bị bao gồm:

mô-đun thực hiện thứ nhất, được cấu hình để thực hiện hành động kiểm soát bảo vệ ít nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn đối với kênh mang tín hiệu đường bên.

13. Thiết bị xử lý lỗi bảo vệ tính toàn vẹn theo điểm 12, trong đó chỉ báo lỗi kiểm tra tính toàn vẹn được gửi bởi một thực thể giao thức hội tụ dữ liệu gói (Packet Data Convergence Protocol, PDCP).

14. Thiết bị xử lý lỗi bảo vệ tính toàn vẹn theo điểm 12, còn bao gồm:

mô-đun thực hiện thứ hai, được cấu hình để thực hiện hành động kiểm soát bảo vệ trong trường hợp phát hiện thấy lỗi liên kết vô tuyến đường bên.

15. Thiết bị xử lý lỗi bảo vệ tính toàn vẹn theo điểm 12, trong đó kênh mang tín hiệu đường bên là ít nhất một trong kênh mang tín hiệu đường bên 1, kênh mang tín hiệu đường bên 2 và kênh mang tín hiệu đường bên 3.

16. Thiết bị xử lý theo điểm 12, trong đó hành động kiểm soát bảo vệ cụ thể bao gồm ít nhất một trong các hoạt động sau:

ngắt kênh mang dữ liệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

ngắt một kênh mang tín hiệu tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

ngắt một kết nối điều khiển tài nguyên vô tuyến giao diện đường bên PC5 RRC tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

loại bỏ thông tin cấu hình tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích;

loại bỏ khóa bảo vệ tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích; và

dừng bộ hẹn giờ tương ứng với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất dựa trên địa chỉ đích hoặc dừng tất cả bộ hẹn giờ đối với truyền tin đường bên được thực hiện bởi thiết bị người dùng thứ nhất.

17. Thiết bị xử lý theo điểm bất kỳ trong các điểm 12-16, còn bao gồm:

mô-đun gửi thứ nhất, được cấu hình để gửi tin nhắn RRC đến thiết bị phía mạng, trong đó tin nhắn RRC được sử dụng để báo cáo rằng truyền tin đường bên với địa chỉ đích bởi thiết bị người dùng thứ nhất không thành công.

18. Thiết bị xử lý theo điểm 17, trong đó tin nhắn RRC còn được sử dụng để chỉ báo rằng nguyên nhân gây ra lỗi truyền tin đường bên là lỗi kiểm tra tính toàn vẹn.

19. Thiết bị xử lý theo điểm bất kỳ trong các điểm 12-16, còn bao gồm:

một mô-đun gửi thứ hai, được cấu hình để gửi thông tin chỉ báo đến một thực thể lớp trên của thiết bị người dùng thứ nhất, trong đó thông tin chỉ báo được sử dụng để thông báo rằng kết nối PC5 RRC đã được ngắt.

20. Thiết bị xử lý theo điểm 19, trong đó thông tin chỉ báo còn được sử dụng để thông báo rằng nguyên nhân khiến kết nối PC5 RRC bị ngắt là lỗi kiểm tra tính toàn vẹn hoặc lỗi kết nối PC5 RRC.

21. Thiết bị xử lý theo điểm bất kỳ trong các điểm 12-16, còn bao gồm:

một mô-đun gửi thứ ba, được cấu hình để gửi một tin nhắn PC5 RRC tới thiết bị người dùng thứ hai tương ứng với địa chỉ đích, trong đó tin nhắn PC5 RRC được sử dụng để chỉ báo thiết bị người dùng thứ hai dừng truyền tin đường bên được thực hiện dựa trên địa chỉ đích.

22. Thiết bị xử lý theo điểm 21, trong đó tin nhắn PC5 RRC mang chỉ báo đặt lại cấu hình đường bên.

23. Phương tiện lưu trữ có thể đọc được, trong đó chương trình hoặc lệnh được lưu trữ trong phương tiện lưu trữ có thể đọc được và khi chương trình hoặc lệnh được thực thi bởi bộ xử lý, thực hiện các bước của phương pháp xử lý lỗi bảo vệ tính toàn vẹn theo điểm bất kỳ trong các điểm 1-11.

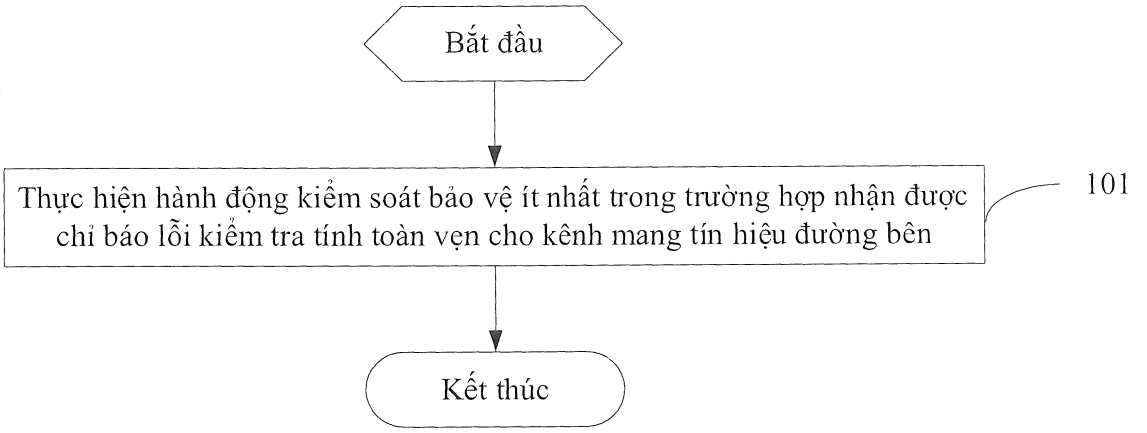
Bắt đầu
Thực hiện hành động kiểm soát bảo vệ ít nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên
101
Kết thúc

Fig.1

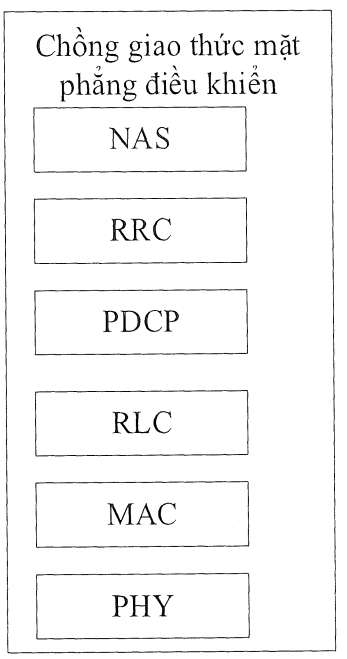
Chồng giao thức mặt phẳng điều khiển
NAS
RRC
PDCP
RLC
MAC
PHY

Fig.2

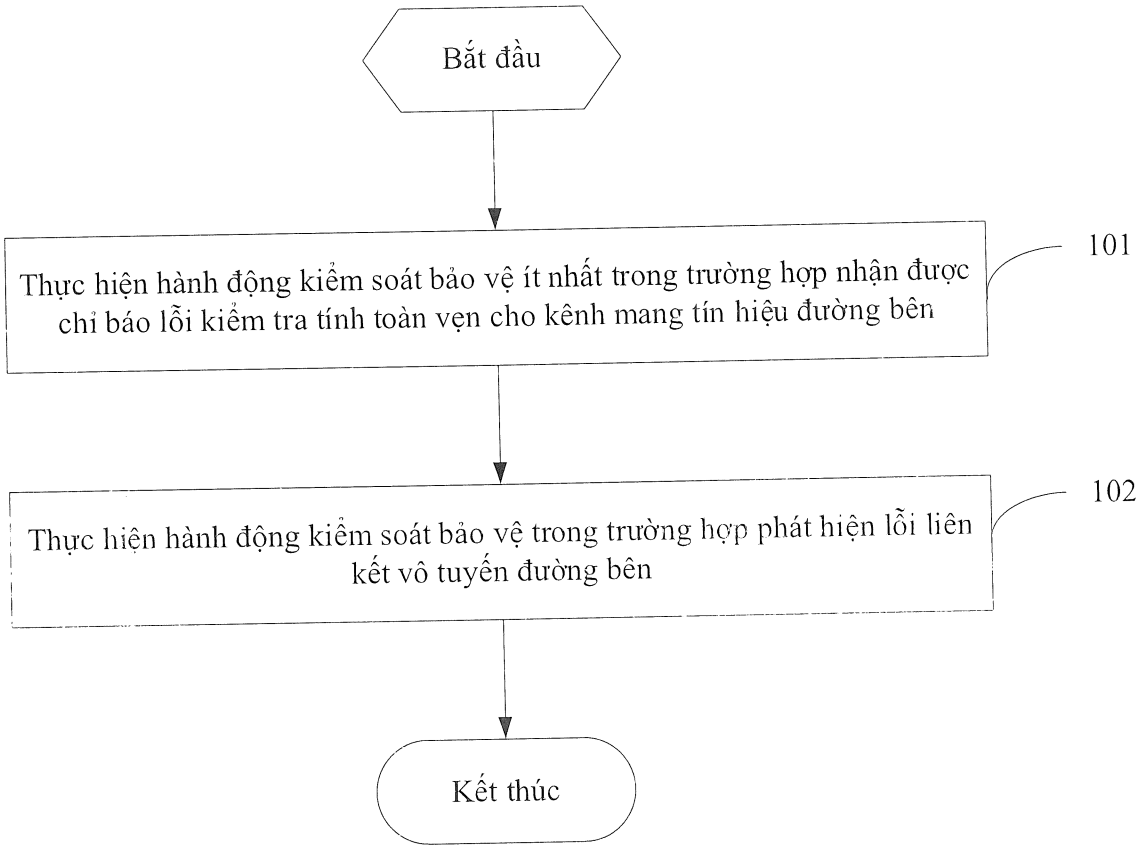
Bắt đầu
Thực hiện hành động kiểm soát bảo vệ ít nhất trong trường hợp nhận được chỉ báo lỗi kiểm tra tính toàn vẹn cho kênh mang tín hiệu đường bên
101
Thực hiện hành động kiểm soát bảo vệ trong trường hợp phát hiện lỗi liên kết vô tuyến đường bên
102
Kết thúc

Fig.3

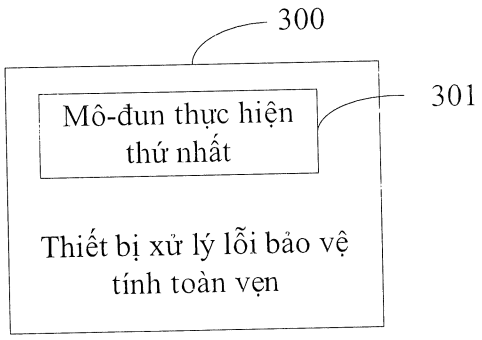
300
Mô-đun thực hiện thứ nhất
301
Thiết bị xử lý lỗi bảo vệ tính toàn vẹn

Fig.4

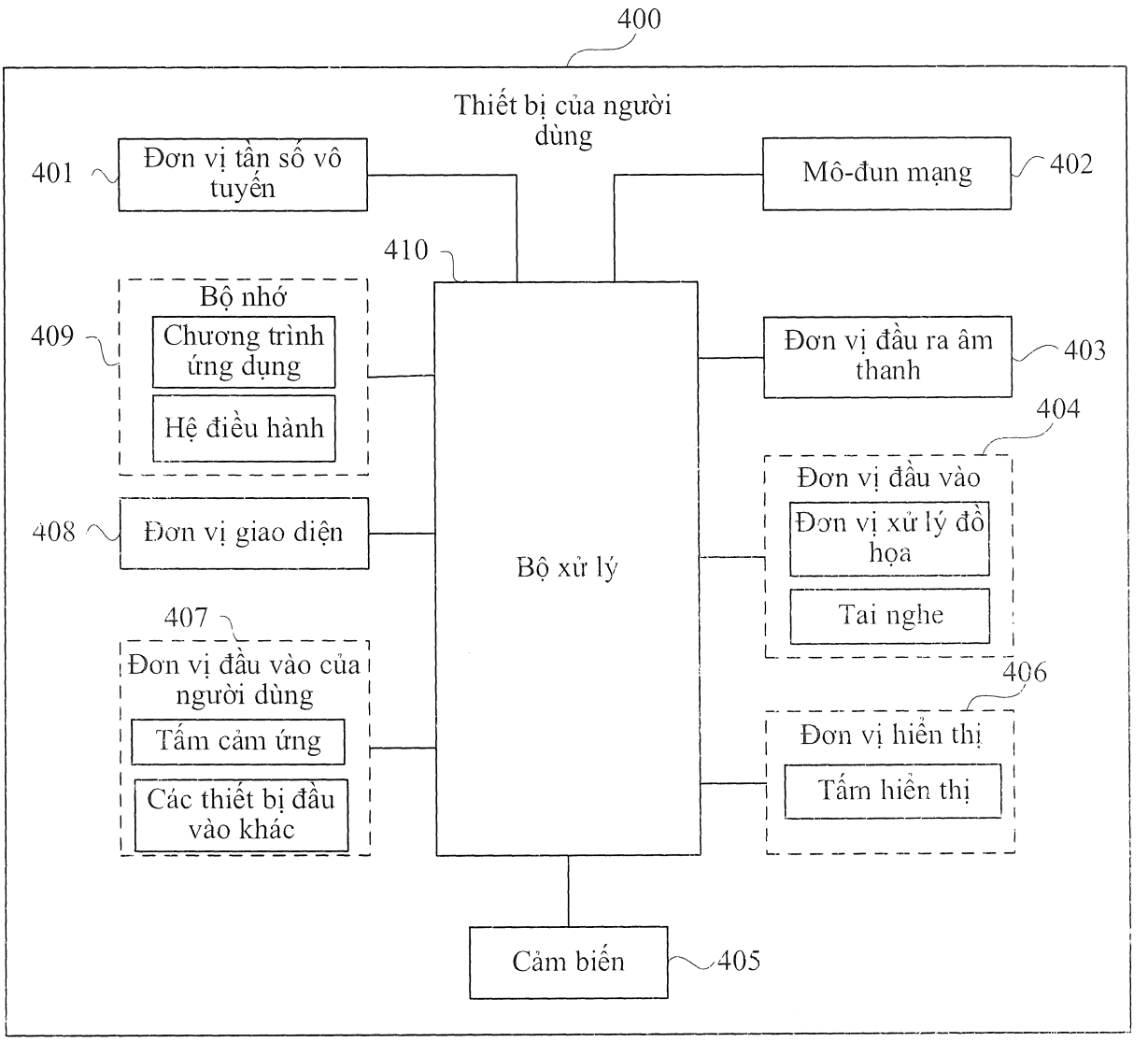
400
Thiết bị của người dùng
401
Đơn vị tần số vô tuyến
402
Mô-đun mạng
410
Bộ nhớ
409
Chương trình ứng dụng
Hệ điều hành
403
Đơn vị đầu ra âm thanh
404
Đơn vị đầu vào
Đơn vị xử lý đồ họa
Tai nghe
408
Đơn vị giao diện
Bộ xử lý
407
Đơn vị đầu vào của người dùng
Tấm cảm ứng
Các thiết bị đầu vào khác
406
Đơn vị hiển thị
Tấm hiển thị
Cảm biến
405

Fig.5