(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) **1-0047581**

(51)[2020.01] **H04W 12/08**; H04W 12/04

(13) **B**

(21) 1-2022-01877

(22) 13/07/2020

(86) PCT/CN2020/101714 13/07/2020

(87) WO 2021/051974 25/03/2021

(30) 201910870247.1 16/09/2019 CN; 201910974006.1 14/10/2019 CN

(45) 25/06/2025 447

(43) 25/07/2022 412A

(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, P. R. China

(72) LI, Fei (CN); DENG, Juan (CN).

(74) Công ty Luật TNHH WINCO (WINCO LAW FIRM)

(54) PHƯƠNG PHÁP, THIẾT BỊ BẢO VỆ AN TOÀN THÔNG TIN GIAO DIỆN KHÔNG GIAN, HỆ THỐNG TRUYỀN THÔNG VÀ VẬT GHI CÓ THỂ ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(21) 1-2022-01877

(57) Sáng chế đề cập đến phương pháp, thiết bị bảo vệ an toàn thông tin giao diện không gian, hệ thống truyền thông và vật ghi có thể đọc được bằng máy tính để bảo vệ hiệu năng an toàn của thông tin giao diện không gian được gửi bởi thiết bị đầu cuối tới trạm gốc. Phương pháp này bao gồm các bước: Thiết bị đầu cuối xác định giá trị mã nhận thực bản tin (message authentication code, MAC) thứ nhất dựa trên khóa an toàn và thông tin giao diện không gian, trong đó khóa an toàn là khóa an toàn tầng không truy nhập (non-access stratum, NAS) giữa thiết bị đầu cuối và thiết bị mạng lõi; và thiết bị đầu cuối gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc; hoặc gửi, bởi thiết bị đầu cuối, thông tin giao diện không gian và giá trị MAC thứ nhất tới thiết bị mạng lõi.

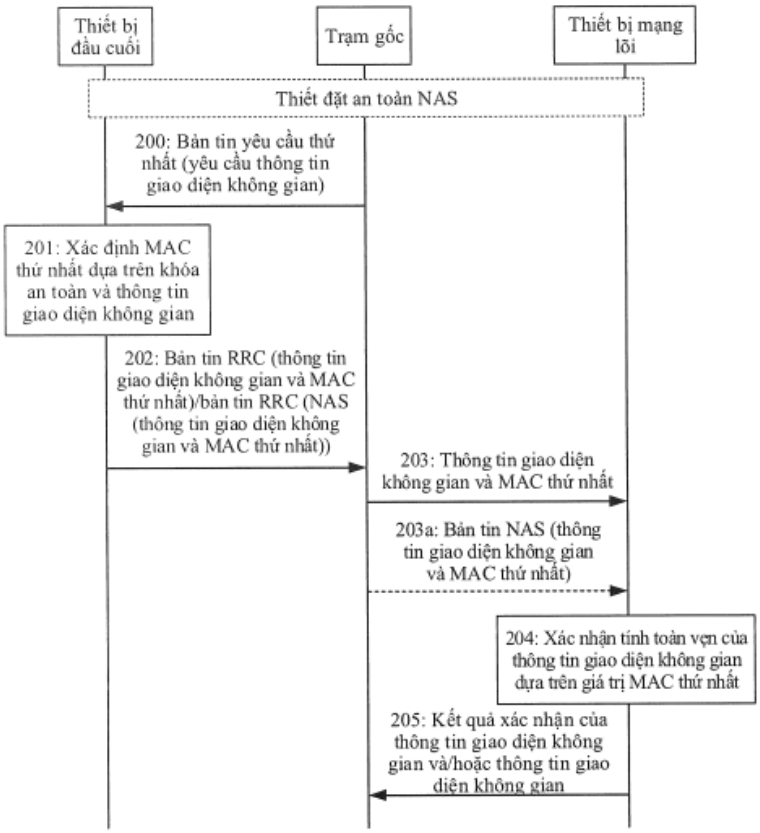

Fig.2

Lĩnh vực kỹ thuật được đề cập

Các phương án của sáng chế đề cập đến lĩnh vực kỹ thuật truyền thông, và cụ thể là đề cập đến phương pháp, thiết bị bảo vệ an toàn thông tin giao diện không gian, hệ thống truyền thông và vật ghi có thể đọc được bằng máy tính.

Tình trạng kỹ thuật của sáng chế

Trạm gốc yêu cầu hoặc truy vấn một số thông tin giao diện không gian từ thiết bị đầu cuối, và thiết bị đầu cuối gửi thông tin giao diện không gian tới trạm gốc. Ví dụ, dự án đối tác thế hệ thứ ba (3rd generation partnership project, 3GPP) định nghĩa khả năng vô tuyến của thiết bị người dùng (user equipment, terminal) (khả năng vô tuyến của thiết bị đầu cuối). Thông tin giao diện không gian có thể là khả năng vô tuyến. Khả năng vô tuyến của thiết bị đầu cuối bao gồm các thông số chẳng hạn như mức công suất và băng tần số của thiết bị đầu cuối. Trạm gốc truy vấn khả năng vô tuyến của thiết bị đầu cuối từ thiết bị đầu cuối, và thiết bị đầu cuối gửi khả năng vô tuyến của thiết bị đầu cuối tới trạm gốc. Tuy nhiên, khi thiết bị đầu cuối gửi khả năng vô tuyến của thiết bị đầu cuối tới trạm gốc, thì khả năng vô tuyến dễ bị tấn công giả mạo bởi kẻ tấn công. Kết quả là, khả năng vô tuyến của thiết bị đầu cuối được thu bởi trạm gốc không chính xác. Dựa trên việc này, việc bảo vệ tính toàn vẹn cần phải được thực hiện trên khả năng vô tuyến được gửi bởi thiết bị đầu cuối tới trạm gốc, để đảm bảo rằng khả năng vô tuyến được gửi bởi thiết bị đầu cuối không bị giả mạo bởi kẻ tấn công.

Trong kỹ thuật thông thường, để đảm bảo rằng khả năng vô tuyến được gửi bởi thiết bị đầu cuối tới trạm gốc không bị giả mạo, thì thiết bị đầu cuối cần phải thiết đặt an toàn tầng truy nhập (access stratum, AS) với trạm gốc. Trạm gốc truy vấn khả năng vô tuyến của thiết bị đầu cuối chỉ sau khi thiết bị đầu cuối thiết đặt an toàn AS với trạm gốc. Thiết bị đầu cuối sử dụng ngữ cảnh của an toàn AS được thiết đặt với trạm gốc để bảo vệ khả năng vô tuyến, để ngăn không cho khả năng vô tuyến của thiết bị đầu cuối bị giả mạo bởi kẻ tấn công.

Tuy nhiên, một số kiểu thiết bị đầu cuối không thể thiết đặt an toàn AS với trạm gốc. Do đó, các thiết bị đầu cuối này không thể sử dụng ngữ cảnh của an toàn AS để bảo vệ

khả năng vô tuyến, và khả năng vô tuyến có thể bị tấn công bởi kẻ tấn công.

Bản chất kỹ thuật của sáng chế

Các phương án của sáng chế đề xuất phương pháp và thiết bị bảo vệ an toàn thông tin giao diện không gian, để bảo vệ hiệu năng an toàn của thông tin giao diện không gian được gửi bởi thiết bị đầu cuối tới trạm gốc.

Các giải pháp kỹ thuật cụ thể được đề xuất theo các phương án của sáng chế như sau:

Theo khía cạnh thứ nhất, phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất. Phương pháp này có thể được thực hiện bằng cách sử dụng các bước sau đây: Thiết bị đầu cuối xác định giá trị mã nhận thực bản tin MAC thứ nhất dựa trên khóa an toàn tầng không truy nhập NAS giữa thiết bị đầu cuối và thiết bị mạng lõi, và thiết bị đầu cuối gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc; hoặc thiết bị đầu cuối gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới thiết bị mạng lõi. Khi thiết bị đầu cuối gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới thiết bị mạng lõi, thì thiết bị đầu cuối trước hết gửi bản tin NAS tới trạm gốc, và trạm gốc chuyển tiếp bản tin NAS tới thiết bị mạng lõi, trong đó bản tin NAS mang thông tin giao diện không gian và giá trị MAC thứ nhất. Giá trị MAC thứ nhất được sử dụng để bảo vệ an toàn của thông tin giao diện không gian. Đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thì an toàn của thông tin giao diện không gian có thể được đảm bảo.

Theo một phương án có thể, thiết bị đầu cuối xác định giá trị mã nhận thực bản tin MAC thứ nhất dựa trên ít nhất hai thông số trong số khóa an toàn, thông tin giao diện không gian, hoặc thông số nhập, trong đó khóa an toàn là khóa an toàn tầng không truy nhập NAS giữa thiết bị đầu cuối và thiết bị mạng lõi; và thiết bị đầu cuối gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc. Phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất theo phương án này của sáng chế có thể áp dụng được cho kiểu thiết bị đầu cuối bất kỳ, và giúp đảm bảo an toàn của thông tin giao diện không gian khi thiết bị đầu cuối trao đổi thông tin giao diện không gian với trạm gốc.

Theo một phương án có thể, thiết bị mạng lõi bao gồm thực thể quản lý di động MME trong 4G hoặc chức năng quản lý truy nhập và di động AMF trong 5G; và khóa an

toàn là một khóa bất kỳ trong số các khóa sau đây hoặc là khóa nhận được thông qua việc suy diễn dựa trên một khóa bất kỳ trong số các khóa sau đây: khóa Kasme giữa thiết bị đầu cuối và MME, khóa Kamf giữa thiết bị đầu cuối và AMF, khóa bảo vệ tính toàn vẹn NAS giữa thiết bị đầu cuối và thiết bị mạng lõi, hoặc khóa bảo vệ tính bí mật NAS giữa thiết bị đầu cuối và thiết bị mạng lõi.

Theo một phương án có thể, thông số nhập bao gồm thông số tươi và/hoặc bộ nhận dạng tế bào, và thông số tươi bao gồm một hoặc nhiều thông số bất kỳ trong số các thông số sau đây: một phần hoặc tất cả các bit để đếm NAS count đường lên, một phần hoặc tất cả các bit để đếm NAS count đường xuống, hoặc số ngẫu nhiên. Thông số nhập còn có thể bao gồm thông số khác.

Theo một phương án có thể, việc thiết bị đầu cuối gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc được thực hiện theo cách thức sau đây: Thiết bị đầu cuối gửi bản tin điều khiển tài nguyên vô tuyến RRC thứ nhất tới trạm gốc, trong đó bản tin RRC thứ nhất mang thông tin giao diện không gian và giá trị MAC thứ nhất.

Ngoài ra, việc thiết bị đầu cuối gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc được thực hiện theo cách thức sau đây: Thiết bị đầu cuối gửi bản tin RRC thứ hai tới trạm gốc, trong đó bản tin RRC thứ hai mang bản tin NAS, và bản tin NAS bao gồm thông tin giao diện không gian và giá trị MAC thứ nhất.

Theo một phương án có thể, thiết bị đầu cuối thu bản tin yêu cầu từ trạm gốc, trong đó bản tin yêu cầu mang giá trị MAC thứ hai, và bản tin yêu cầu được sử dụng để yêu cầu thông tin giao diện không gian; và thiết bị đầu cuối xác nhận giá trị MAC thứ hai. Bằng cách này, thiết bị đầu cuối có thể xác nhận việc trạm gốc có hợp lệ hay không dựa trên giá trị MAC thứ hai, sao cho khi không có an toàn AS được thiết lập giữa thiết bị đầu cuối và trạm gốc, thì an toàn truyền dẫn thông tin được đảm bảo, và việc xác nhận hai chiều được thực hiện.

Theo một phương án có thể, thông tin giao diện không gian là khả năng vô tuyến hoặc bộ nhận dạng khả năng vô tuyến.

Theo khía cạnh thứ hai, phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất. Phương pháp này có thể được thực hiện bằng cách sử dụng các bước sau đây: Trạm gốc thu bản tin điều khiển tài nguyên vô tuyến RRC từ thiết bị đầu cuối, trong đó bản tin RRC mang bản tin NAS, và bản tin NAS bao gồm thông tin giao diện không gian và giá trị MAC thứ nhất; trạm gốc gửi bản tin NAS tới thiết bị mạng lõi; và trạm gốc

thu kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian từ thiết bị mạng lõi. Đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thì an toàn của thông tin giao diện không gian có thể được đảm bảo.

Theo khía cạnh thứ ba, phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất. Phương pháp này có thể được thực hiện bằng cách sử dụng các bước sau đây: Trạm gốc thu thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất từ thiết bị đầu cuối; trạm gốc gửi thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất tới thiết bị mạng lõi; và trạm gốc thu kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian từ thiết bị mạng lõi. Đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thì an toàn của thông tin giao diện không gian có thể được đảm bảo.

Dựa trên khía cạnh thứ hai và khía cạnh thứ ba, các phương án có thể sau đây có thể được cung cấp thêm.

Theo một phương án có thể, phương pháp này còn bao gồm bước: Trạm gốc gửi bản tin yêu cầu thứ nhất tới thiết bị mạng lõi; trạm gốc thu bản tin hồi đáp thứ hai của bản tin yêu cầu thứ nhất từ thiết bị mạng lõi, trong đó bản tin hồi đáp thứ hai mang giá trị MAC thứ hai; và trạm gốc gửi bản tin yêu cầu thứ hai tới thiết bị đầu cuối, trong đó bản tin yêu cầu thứ hai được sử dụng để yêu cầu thông tin giao diện không gian, và bản tin yêu cầu thứ hai mang giá trị MAC thứ hai. Bằng cách này, thiết bị đầu cuối có thể xác nhận việc trạm gốc có hợp lệ hay không dựa trên giá trị MAC thứ hai, sao cho khi không có an toàn AS được thiết lập giữa thiết bị đầu cuối và trạm gốc, thì an toàn truyền dẫn thông tin được đảm bảo, và việc xác nhận hai chiều được thực hiện.

Theo một phương án có thể, trước việc trạm gốc gửi bản tin yêu cầu thứ nhất tới thiết bị mạng lõi, thì trạm gốc xác định rằng thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển.

Theo một phương án có thể, thông tin giao diện không gian là khả năng vô tuyến hoặc bộ nhận dạng khả năng vô tuyến.

Theo khía cạnh thứ tư, phương pháp bảo vệ an toàn thông tin giao diện không gian

được đề xuất. Phương pháp này có thể được thực hiện bằng cách sử dụng các bước sau đây: Thiết bị mạng lõi thu bản tin yêu cầu thứ nhất từ trạm gốc, trong đó bản tin yêu cầu thứ nhất mang thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất; thiết bị mạng lõi xác nhận tính toàn vẹn của thông tin giao diện không gian dựa trên giá trị MAC thứ nhất; và thiết bị mạng lõi gửi bản tin hồi đáp thứ nhất của yêu cầu thứ nhất tới trạm gốc, trong đó bản tin hồi đáp thứ nhất bao gồm kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian. Đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thì an toàn của thông tin giao diện không gian có thể được đảm bảo.

Theo một phương án có thể, thiết bị mạng lõi thu bản tin yêu cầu thứ hai từ trạm gốc; thiết bị mạng lõi xác định giá trị MAC thứ hai dựa trên khóa an toàn; và thiết bị mạng lõi gửi bản tin hồi đáp thứ hai của bản tin yêu cầu thứ hai tới trạm gốc, trong đó bản tin hồi đáp thứ hai mang giá trị MAC thứ hai. Bằng cách này, trạm gốc có thể mang giá trị MAC thứ hai khi gửi bản tin RRC tới thiết bị đầu cuối, và thiết bị đầu cuối có thể xác nhận việc trạm gốc có hợp lệ hay không dựa trên giá trị MAC thứ hai, sao cho khi không có an toàn AS được thiết lập giữa thiết bị đầu cuối và trạm gốc, thì an toàn truyền dẫn thông tin được đảm bảo, và việc xác nhận hai chiều được thực hiện.

Theo một phương án có thể, khóa an toàn bao gồm một khóa bất kỳ trong số các khóa sau đây hoặc là khóa nhận được thông qua việc suy diễn dựa trên một khóa bất kỳ trong số các khóa sau đây: khóa được chia sẻ giữa thiết bị đầu cuối và thiết bị mạng lõi, khóa bảo vệ tính toàn vẹn giữa thiết bị đầu cuối và thiết bị mạng lõi, hoặc khóa bảo vệ tính bí mật giữa thiết bị đầu cuối và thiết bị mạng lõi.

Theo một phương án có thể, việc thiết bị mạng lõi xác định giá trị MAC thứ hai dựa trên khóa an toàn được thực hiện theo cách thức sau đây: Thiết bị mạng lõi xác định giá trị MAC thứ hai dựa trên khóa an toàn, thông số nhập, và thông tin giao diện không gian, trong đó thông số nhập bao gồm thông số tươi và/hoặc bộ nhận dạng tế bào, và thông số tươi bao gồm một hoặc nhiều thông số bất kỳ trong số các thông số sau đây: một phần hoặc tất cả các bit để đếm NAS count đường lên, một phần hoặc tất cả các bit để đếm NAS count đường xuống, hoặc số ngẫu nhiên.

Theo một phương án có thể, thông tin giao diện không gian là khả năng vô tuyến

hoặc bộ nhận dạng khả năng vô tuyến.

Theo khía cạnh thứ năm, phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất. Phương pháp này có thể được thực hiện bằng cách sử dụng các bước sau đây: Thiết bị đầu cuối thu bản tin yêu cầu từ thiết bị mạng lõi, trong đó bản tin yêu cầu được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối; và thiết bị đầu cuối gửi bản tin hồi đáp tới mạng lõi, trong đó bản tin hồi đáp mang thông tin giao diện không gian của thiết bị đầu cuối. Đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thông tin giao diện không gian có thể nhận được từ thiết bị đầu cuối thông qua mạng lõi, và an toàn của thông tin giao diện không gian có thể được đảm bảo.

Tùy chọn là, thông tin giao diện không gian là khả năng vô tuyến hoặc bộ nhận dạng khả năng vô tuyến.

Tùy chọn là, thiết bị đầu cuối thiết đặt an toàn tầng không truy nhập NAS với thiết bị mạng lõi. Bằng cách này, thông tin giao diện không gian được gửi bởi thiết bị đầu cuối tới thiết bị mạng lõi có thể được bảo vệ bằng cách sử dụng ngữ cảnh của an toàn NAS.

Theo khía cạnh thứ sáu, phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất. Phương pháp này có thể được thực hiện bằng cách sử dụng các bước sau đây: Thiết bị mạng lõi gửi bản tin yêu cầu thứ nhất tới thiết bị đầu cuối, trong đó bản tin yêu cầu thứ nhất được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối; và thiết bị mạng lõi thu bản tin hồi đáp thứ nhất của bản tin yêu cầu thứ nhất từ thiết bị đầu cuối, trong đó bản tin hồi đáp thứ nhất mang thông tin giao diện không gian của thiết bị đầu cuối. Đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thông tin giao diện không gian có thể nhận được từ thiết bị đầu cuối thông qua mạng lõi, và an toàn của thông tin giao diện không gian có thể được đảm bảo.

Theo một phương án có thể, trước việc thiết bị mạng lõi gửi bản tin yêu cầu tới thiết bị đầu cuối, thì thiết bị mạng lõi xác định rằng thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển.

Theo một phương án có thể, trước việc thiết bị mạng lõi gửi bản tin yêu cầu tới thiết bị đầu cuối, thì thiết bị mạng lõi thu bản tin yêu cầu thứ hai từ trạm gốc, trong đó bản tin

yêu cầu thứ hai được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối.

Theo một phương án có thể, bản tin yêu cầu thứ hai được sử dụng để chỉ báo rằng thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển.

Theo một phương án có thể, thiết bị mạng lõi trả về bản tin hồi đáp thứ hai của bản tin yêu cầu thứ hai cho trạm gốc, trong đó bản tin hồi đáp thứ hai mang thông tin giao diện không gian của thiết bị đầu cuối.

Theo một phương án có thể, thông tin giao diện không gian là khả năng vô tuyến hoặc bộ nhận dạng khả năng vô tuyến.

Tùy chọn là, thiết bị mạng lõi thiết đặt trước an toàn tầng không truy nhập NAS với thiết bị đầu cuối. Bằng cách này, thông tin giao diện không gian được gửi bởi thiết bị đầu cuối tới thiết bị mạng lõi có thể được bảo vệ bằng cách sử dụng ngữ cảnh của an toàn NAS.

Theo khía cạnh thứ bảy, phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất. Phương pháp này có thể được thực hiện bằng cách sử dụng các bước sau đây: Trạm gốc gửi bản tin yêu cầu tới thiết bị mạng lõi, trong đó bản tin yêu cầu được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối; và trạm gốc thu bản tin hồi đáp của bản tin yêu cầu từ thiết bị mạng lõi, trong đó bản tin hồi đáp mang thông tin giao diện không gian của thiết bị đầu cuối. Đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thông tin giao diện không gian có thể nhận được thông qua mạng lõi, và an toàn của thông tin giao diện không gian có thể được đảm bảo.

Theo một phương án có thể, trước việc trạm gốc gửi bản tin yêu cầu tới thiết bị mạng lõi, thì trạm gốc xác định rằng thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển.

Theo khía cạnh thứ tám, thiết bị được đề xuất. Thiết bị này có thể là thiết bị đầu cuối, thiết bị trong thiết bị đầu cuối, hoặc thiết bị mà có thể được sử dụng cùng với thiết bị đầu cuối. Theo một phương án, thiết bị này có thể bao gồm các môđun mà ở dạng tương ứng một-một với các phương pháp/hoạt động/bước/nhiệm vụ được thực hiện bởi thiết bị đầu cuối theo khía cạnh thứ nhất, hoặc thiết bị này có thể bao gồm các môđun mà ở dạng

tương ứng một-một với các phương pháp/hoạt động/bước/nhiệm vụ được thực hiện bởi thiết bị đầu cuối theo khía cạnh thứ năm. Môđun này có thể là mạch phần cứng, có thể là phần mềm, hoặc có thể được thực hiện bằng cách kết hợp mạch phần cứng và phần mềm. Theo một phương án, thiết bị có thể bao gồm môđun xử lý và môđun truyền thông.

Ví dụ, khi thiết bị này được tạo cấu hình để thực hiện các hoạt động được thực hiện bởi thiết bị đầu cuối theo khía cạnh thứ nhất:

môđun xử lý được tạo cấu hình để xác định giá trị mã nhận thực bản tin MAC thứ nhất dựa trên khóa an toàn và thông tin giao diện không gian, trong đó khóa an toàn là khóa an toàn tầng không truy nhập NAS giữa thiết bị đầu cuối và thiết bị mạng lõi; và môđun truyền thông được tạo cấu hình để gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc.

Theo một phương án có thể, thiết bị mạng lõi bao gồm thực thể quản lý di động MME hoặc chức năng quản lý truy nhập và di động AMF; và khóa an toàn là một khóa bất kỳ trong số các khóa sau đây hoặc là khóa nhận được thông qua việc suy diễn dựa trên một khóa bất kỳ trong số các khóa sau đây: khóa Kasme giữa thiết bị đầu cuối và MME, khóa Kamf giữa thiết bị đầu cuối và AMF, khóa bảo vệ tính toàn vẹn NAS giữa thiết bị đầu cuối và thiết bị mạng lõi, hoặc khóa bảo vệ tính bí mật NAS giữa thiết bị đầu cuối và thiết bị mạng lõi.

Theo một phương án có thể, môđun xử lý được tạo cấu hình để: xác định giá trị MAC thứ nhất dựa trên khóa an toàn, thông tin giao diện không gian, và thông số nhập, trong đó thông số nhập bao gồm thông số tươi và/hoặc bộ nhận dạng tế bào, và thông số tươi bao gồm một hoặc nhiều thông số bất kỳ trong số các thông số sau đây: một phần hoặc tất cả các bit để đếm NAS count đường lên, một phần hoặc tất cả các bit để đếm NAS count đường xuống, hoặc số ngẫu nhiên.

Theo một phương án có thể, môđun truyền thông được tạo cấu hình để: gửi bản tin điều khiển tài nguyên vô tuyến RRC thứ nhất tới trạm gốc, trong đó bản tin RRC thứ nhất mang thông tin giao diện không gian và giá trị MAC thứ nhất; hoặc gửi bản tin RRC thứ hai tới trạm gốc, trong đó bản tin RRC thứ hai mang bản tin NAS, và bản tin NAS bao gồm thông tin giao diện không gian và giá trị MAC thứ nhất.

Theo một phương án có thể, môđun truyền thông còn được tạo cấu hình để: thu bản tin yêu cầu từ trạm gốc, trong đó bản tin yêu cầu mang giá trị MAC thứ hai, và bản tin yêu cầu được sử dụng để yêu cầu thông tin giao diện không gian; và môđun xử lý còn

được tạo cấu hình để xác nhận giá trị MAC thứ hai.

Theo một phương án có thể, thông tin giao diện không gian là khả năng vô tuyến hoặc bộ nhận dạng khả năng vô tuyến.

Ví dụ, khi thiết bị này được tạo cấu hình để thực hiện các hoạt động được thực hiện bởi thiết bị đầu cuối theo khía cạnh thứ năm, môđun truyền thông được tạo cấu hình để: thu bản tin yêu cầu từ thiết bị mạng lõi, trong đó bản tin yêu cầu được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối; và gửi bản tin hồi đáp tới mạng lõi, trong đó bản tin hồi đáp mang thông tin giao diện không gian của thiết bị đầu cuối. Bằng cách này, đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thì thông tin giao diện không gian có thể nhận được từ thiết bị đầu cuối thông qua mạng lõi, và an toàn của thông tin giao diện không gian có thể được đảm bảo.

Tùy chọn là, thông tin giao diện không gian là khả năng vô tuyến hoặc bộ nhận dạng khả năng vô tuyến.

Tùy chọn là, môđun xử lý được tạo cấu hình để thiết đặt an toàn tầng không truy nhập NAS với thiết bị mạng lõi. Bằng cách này, thông tin giao diện không gian được gửi bởi thiết bị đầu cuối tới thiết bị mạng lõi có thể được bảo vệ bằng cách sử dụng ngữ cảnh của an toàn NAS.

Theo khía cạnh thứ chín, thiết bị được đề xuất. Thiết bị này có thể là trạm gốc, thiết bị trong trạm gốc, hoặc thiết bị mà có thể được sử dụng cùng với trạm gốc. Theo một phương án, thiết bị này có thể bao gồm các môđun mà ở dạng tương ứng một-một với các phương pháp/hoạt động/bước/nhiệm vụ được thực hiện bởi trạm gốc theo khía cạnh thứ hai, khía cạnh thứ ba, hoặc khía cạnh thứ bảy. Theo một phương án, thiết bị có thể bao gồm môđun xử lý và môđun truyền thông.

Ví dụ, khi thiết bị này được tạo cấu hình để thực hiện các hoạt động được thực hiện bởi trạm gốc theo khía cạnh thứ hai:

môđun truyền thông được tạo cấu hình để: thu bản tin điều khiển tài nguyên vô tuyến RRC từ thiết bị đầu cuối, trong đó bản tin RRC mang bản tin NAS, và bản tin NAS bao gồm thông tin giao diện không gian và giá trị MAC thứ nhất; và gửi bản tin NAS tới thiết bị mạng lõi; và môđun truyền thông còn được tạo cấu hình để thu kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian

từ thiết bị mạng lõi.

Ví dụ, khi thiết bị này được tạo cấu hình để thực hiện các hoạt động được thực hiện bởi trạm gốc theo khía cạnh thứ ba:

môđun truyền thông được tạo cấu hình để: thu thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất từ thiết bị đầu cuối; và gửi thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất tới thiết bị mạng lõi; và

môđun truyền thông còn được tạo cấu hình để thu kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian từ thiết bị mạng lõi.

Khi thiết bị này được tạo cấu hình để thực hiện các hoạt động được thực hiện bởi trạm gốc theo khía cạnh thứ hai hoặc khía cạnh thứ ba, tùy chọn là, môđun truyền thông và môđun xử lý còn có thể thực hiện các hoạt động sau đây.

Theo một phương án có thể, môđun truyền thông còn được tạo cấu hình để: gửi bản tin yêu cầu thứ nhất tới thiết bị mạng lõi; thu bản tin hồi đáp thứ hai của bản tin yêu cầu thứ nhất từ thiết bị mạng lõi, trong đó bản tin hồi đáp thứ hai mang giá trị MAC thứ hai; và gửi bản tin yêu cầu thứ hai tới thiết bị đầu cuối, trong đó bản tin yêu cầu thứ hai được sử dụng để yêu cầu thông tin giao diện không gian, và bản tin yêu cầu thứ hai mang giá trị MAC thứ hai.

Theo một phương án có thể, môđun xử lý được tạo cấu hình để: trước khi trạm gốc gửi bản tin yêu cầu thứ nhất tới thiết bị mạng lõi, thì xác định rằng thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển.

Ví dụ, khi thiết bị này được tạo cấu hình để thực hiện các hoạt động được thực hiện bởi trạm gốc theo khía cạnh thứ bảy:

môđun truyền thông được tạo cấu hình để: gửi bản tin yêu cầu tới thiết bị mạng lõi, trong đó bản tin yêu cầu được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối; và thu bản tin hồi đáp của bản tin yêu cầu từ thiết bị mạng lõi, trong đó bản tin hồi đáp mang thông tin giao diện không gian của thiết bị đầu cuối. Đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thông tin giao diện không gian có thể nhận được thông qua mạng lõi, và an toàn của thông tin giao diện không gian có thể được đảm bảo.

Theo một phương án có thể, môđun xử lý được tạo cấu hình để: trước khi trạm gốc gửi bản tin yêu cầu tới thiết bị mạng lõi, thì xác định rằng thiết bị đầu cuối là thiết bị đầu

cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển.

Theo khía cạnh thứ mười, thiết bị được đề xuất. Thiết bị này có thể là thiết bị mạng lõi, thiết bị trong thiết bị mạng lõi, hoặc thiết bị mà có thể được sử dụng cùng với thiết bị mạng lõi. Theo một phương án, thiết bị này có thể bao gồm các môđun mà ở dạng tương ứng một-một với các phương pháp/hoạt động/bước/nhiệm vụ được thực hiện bởi thiết bị mạng lõi theo khía cạnh thứ tư hoặc khía cạnh thứ sáu. Theo một phương án, thiết bị có thể bao gồm môđun xử lý và môđun truyền thông.

Ví dụ, khi thiết bị này được tạo cấu hình để thực hiện các hoạt động được thực hiện bởi thiết bị mạng lõi theo khía cạnh thứ tư:

môđun truyền thông được tạo cấu hình để thu bản tin yêu cầu thứ nhất từ trạm gốc, trong đó bản tin yêu cầu thứ nhất mang thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất; môđun xử lý được tạo cấu hình để xác nhận tính toàn vẹn của thông tin giao diện không gian dựa trên giá trị MAC thứ nhất; và môđun truyền thông còn được tạo cấu hình để gửi bản tin hồi đáp thứ nhất của yêu cầu thứ nhất tới trạm gốc, trong đó bản tin hồi đáp thứ nhất bao gồm kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian. Đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thì an toàn của thông tin giao diện không gian có thể được đảm bảo.

Theo một phương án có thể, môđun truyền thông được tạo cấu hình để thu bản tin yêu cầu thứ hai từ trạm gốc; môđun xử lý được tạo cấu hình để xác định giá trị MAC thứ hai dựa trên khóa an toàn; và môđun truyền thông được tạo cấu hình để gửi bản tin hồi đáp thứ hai của bản tin yêu cầu thứ hai tới trạm gốc, trong đó bản tin hồi đáp thứ hai mang giá trị MAC thứ hai. Bằng cách này, trạm gốc có thể mang giá trị MAC thứ hai khi gửi bản tin RRC tới thiết bị đầu cuối, và thiết bị đầu cuối có thể xác nhận việc trạm gốc có hợp lệ hay không dựa trên giá trị MAC thứ hai, sao cho khi không có an toàn AS được thiết lập giữa thiết bị đầu cuối và trạm gốc, thì an toàn truyền dẫn thông tin được đảm bảo, và việc xác nhận hai chiều được thực hiện.

Theo một phương án có thể, khóa an toàn bao gồm một khóa bất kỳ trong số các khóa sau đây hoặc là khóa nhận được thông qua việc suy diễn dựa trên một khóa bất kỳ trong số các khóa sau đây: khóa được chia sẻ giữa thiết bị đầu cuối và thiết bị mạng lõi, khóa bảo vệ tính toàn vẹn giữa thiết bị đầu cuối và thiết bị mạng lõi, hoặc khóa bảo vệ

tính bí mật giữa thiết bị đầu cuối và thiết bị mạng lõi.

Theo một phương án có thể, môđun xử lý được tạo cấu hình để xác định giá trị MAC thứ hai dựa trên khóa an toàn, thông số nhập, và thông tin giao diện không gian, trong đó thông số nhập bao gồm thông số tươi và/hoặc bộ nhận dạng tế bào, và thông số tươi bao gồm một hoặc nhiều thông số bất kỳ trong số các thông số sau đây: một phần hoặc tất cả các bit để đếm NAS count đường lên, một phần hoặc tất cả các bit để đếm NAS count đường xuống, hoặc số ngẫu nhiên.

Ví dụ, khi thiết bị này được tạo cấu hình để thực hiện các hoạt động được thực hiện bởi thiết bị mạng lõi theo khía cạnh thứ sáu:

môđun truyền thông được tạo cấu hình để: gửi bản tin yêu cầu thứ nhất tới thiết bị đầu cuối, trong đó bản tin yêu cầu thứ nhất được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối; và thu bản tin hồi đáp thứ nhất của bản tin yêu cầu thứ nhất từ thiết bị đầu cuối, trong đó bản tin hồi đáp thứ nhất mang thông tin giao diện không gian của thiết bị đầu cuối. Đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thông tin giao diện không gian có thể nhận được từ thiết bị đầu cuối thông qua mạng lõi, và an toàn của thông tin giao diện không gian có thể được đảm bảo.

Theo một phương án có thể, môđun xử lý được tạo cấu hình để: trước khi thiết bị mạng lõi gửi bản tin yêu cầu tới thiết bị đầu cuối, thì xác định rằng thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển.

Theo một phương án có thể, môđun truyền thông còn được tạo cấu hình để: trước khi thiết bị mạng lõi gửi bản tin yêu cầu tới thiết bị đầu cuối, thì thu bản tin yêu cầu thứ hai từ trạm gốc, trong đó bản tin yêu cầu thứ hai được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối.

Theo một phương án có thể, bản tin yêu cầu thứ hai được sử dụng để chỉ báo rằng thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển.

Theo một phương án có thể, môđun truyền thông còn được tạo cấu hình để trả về bản tin hồi đáp thứ hai của bản tin yêu cầu thứ hai cho trạm gốc, trong đó bản tin hồi đáp thứ hai mang thông tin giao diện không gian của thiết bị đầu cuối.

Theo một phương án có thể, thông tin giao diện không gian là khả năng vô tuyến

hoặc bộ nhận dạng khả năng vô tuyến.

Tùy chọn là, môđun xử lý còn được tạo cấu hình để thiết đặt trước an toàn tầng không truy nhập NAS với thiết bị đầu cuối. Bằng cách này, thông tin giao diện không gian được gửi bởi thiết bị đầu cuối tới thiết bị mạng lõi có thể được bảo vệ bằng cách sử dụng ngữ cảnh của an toàn NAS.

Theo khía cạnh thứ mười một, một phương án của sáng chế đề xuất thiết bị. Thiết bị này bao gồm giao diện truyền thông và bộ xử lý, và giao diện truyền thông được sử dụng bởi thiết bị này để truyền thông với thiết bị khác, ví dụ, để thu và gửi dữ liệu hoặc tín hiệu. Ví dụ, giao diện truyền thông có thể là bộ thu phát, mạch, bus, môđun, hoặc kiểu giao diện truyền thông khác, và thiết bị khác có thể là trạm gốc khác hoặc thiết bị mạng lõi khác. Bộ xử lý được tạo cấu hình để thực hiện phương pháp được thực hiện bởi thiết bị đầu cuối được mô tả theo khía cạnh thứ nhất hoặc khía cạnh thứ năm. Thiết bị này còn có thể bao gồm bộ nhớ, được tạo cấu hình để lưu các lệnh được gọi ra bởi bộ xử lý. Bộ nhớ được ghép nối với bộ xử lý. Khi thực hiện các lệnh được lưu trong bộ nhớ, bộ xử lý có thể thực hiện phương pháp được thực hiện bởi thiết bị đầu cuối được mô tả theo khía cạnh thứ nhất hoặc khía cạnh thứ hai.

Theo khía cạnh thứ mười hai, một phương án của sáng chế đề xuất thiết bị. Thiết bị này bao gồm giao diện truyền thông và bộ xử lý, và giao diện truyền thông được sử dụng bởi thiết bị này để truyền thông với thiết bị khác, ví dụ, để thu và gửi dữ liệu hoặc tín hiệu. Ví dụ, giao diện truyền thông có thể là bộ thu phát, mạch, bus, môđun, hoặc kiểu giao diện truyền thông khác, và thiết bị khác có thể là thiết bị đầu cuối khác hoặc thiết bị mạng lõi khác. Bộ xử lý được tạo cấu hình để thực hiện phương pháp được thực hiện bởi trạm gốc được mô tả theo khía cạnh thứ hai, khía cạnh thứ ba, hoặc khía cạnh thứ bảy. Thiết bị này còn có thể bao gồm bộ nhớ, được tạo cấu hình để lưu các lệnh được gọi ra bởi bộ xử lý. Bộ nhớ được ghép nối với bộ xử lý. Khi thực hiện các lệnh được lưu trong bộ nhớ, thì bộ xử lý có thể thực hiện phương pháp được thực hiện bởi trạm gốc được mô tả theo khía cạnh thứ hai, khía cạnh thứ ba, hoặc khía cạnh thứ bảy.

Theo khía cạnh thứ mười ba, một phương án của sáng chế đề xuất thiết bị. Thiết bị này bao gồm giao diện truyền thông và bộ xử lý, và giao diện truyền thông được sử dụng bởi thiết bị này để truyền thông với thiết bị khác, ví dụ, để thu và gửi dữ liệu hoặc tín hiệu. Ví dụ, giao diện truyền thông có thể là bộ thu phát, mạch, bus, môđun, hoặc kiểu giao diện truyền thông khác, và thiết bị khác có thể là trạm gốc khác hoặc thiết bị đầu cuối

khác. Bộ xử lý được tạo cấu hình để thực hiện phương pháp được thực hiện bởi thiết bị mạng lõi được mô tả theo khía cạnh thứ tư hoặc khía cạnh thứ sáu. Thiết bị này còn có thể bao gồm bộ nhớ, được tạo cấu hình để lưu các lệnh được gọi ra bởi bộ xử lý. Bộ nhớ được ghép nối với bộ xử lý. Khi thực hiện các lệnh được lưu trong bộ nhớ, thì bộ xử lý có thể thực hiện phương pháp được thực hiện bởi thiết bị mạng lõi được mô tả theo khía cạnh thứ tư hoặc khía cạnh thứ sáu.

Theo khía cạnh thứ mười bốn, một phương án của sáng chế còn đề xuất vật ghi có thể đọc được bằng máy tính. Vật ghi có thể đọc được bằng máy tính lưu các lệnh có thể đọc được bằng máy tính. Khi các lệnh có thể đọc được bằng máy tính được chạy trên máy tính, thì máy tính được cho phép để thực hiện các phương pháp theo các khía cạnh.

Theo khía cạnh thứ mười lăm, một phương án của sáng chế còn đề xuất sản phẩm chương trình máy tính, bao gồm các lệnh. Khi các lệnh này được chạy trên máy tính, thì máy tính được cho phép để thực hiện các phương pháp theo các khía cạnh.

Theo khía cạnh thứ mười sáu, một phương án của sáng chế đề xuất hệ thống chip. Hệ thống chip bao gồm bộ xử lý, và còn có thể bao gồm bộ nhớ, được tạo cấu hình để thực hiện phương pháp theo một khía cạnh bất kỳ trong số các khía cạnh được đề cập ở trên. Hệ thống chip có thể bao gồm chip, hoặc có thể bao gồm chip và bộ phận rời rạc khác.

Theo khía cạnh thứ mười bảy, một phương án của sáng chế đề xuất hệ thống truyền thông. Hệ thống truyền thông bao gồm thiết bị theo khía cạnh thứ tám, thiết bị theo khía cạnh thứ chín, và thiết bị theo khía cạnh thứ mười.

Mô tả vắn tắt các hình vẽ

Fig.1 là hình vẽ sơ đồ cấu trúc của hệ thống truyền thông theo một phương án của sáng chế;

Fig.2 là hình vẽ lưu đồ thứ nhất của phương pháp bảo vệ an toàn thông tin giao diện không gian theo một phương án của sáng chế;

Fig.3 là hình vẽ lưu đồ thứ nhất của phương pháp bảo vệ an toàn đường xuống theo một phương án của sáng chế;

Fig.4 là hình vẽ lưu đồ thứ hai của phương pháp bảo vệ an toàn đường xuống theo một phương án của sáng chế;

Fig.5 là hình vẽ lưu đồ thứ hai của phương pháp bảo vệ an toàn thông tin giao diện

không gian theo một phương án của sáng chế;

Fig.6 là hình vẽ lưu đồ thứ ba của phương pháp bảo vệ an toàn thông tin giao diện không gian theo một phương án của sáng chế;

Fig.6a là hình vẽ lưu đồ thứ tư của phương pháp bảo vệ an toàn thông tin giao diện không gian theo một phương án của sáng chế;

Fig.7 là hình vẽ lưu đồ thứ năm của phương pháp bảo vệ an toàn thông tin giao diện không gian theo một phương án của sáng chế;

Fig.8 là hình vẽ sơ đồ thứ nhất của kết cấu của thiết bị theo một phương án của sáng chế;

Fig.9 là hình vẽ sơ đồ thứ hai của kết cấu của thiết bị theo một phương án của sáng chế; và

Fig.10 là hình vẽ lưu đồ thứ sáu của phương pháp bảo vệ an toàn thông tin giao diện không gian theo một phương án của sáng chế.

Mô tả chi tiết sáng chế

Phần sau đây mô tả chi tiết các phương án của sáng chế có dựa vào các hình vẽ kèm theo.

Các phương án của sáng chế đề xuất phương pháp và thiết bị bảo vệ an toàn thông tin giao diện không gian, để bảo vệ hiệu năng an toàn của thông tin giao diện không gian được gửi bởi thiết bị đầu cuối tới trạm gốc. Phương pháp và thiết bị dựa trên khái niệm sáng chế giống nhau. Vì nguyên lý giải quyết vấn đề của phương pháp tương tự với thiết bị, nên phần tham khảo lẫn nhau có thể được thực hiện với các dạng thực hiện của thiết bị và phương pháp. Các phần lặp lại không được mô tả chi tiết. Trong các phần mô tả của sáng chế, thuật ngữ "và/hoặc" mô tả mối quan hệ liên kết giữa các đối tượng được liên kết và thể hiện rằng có ba mối quan hệ có thể tồn tại. Ví dụ, A và/hoặc B có thể thể hiện ba trường hợp sau: Chỉ A tồn tại, cả A và B tồn tại, và chỉ B tồn tại. Ký tự "/" thường thể hiện mối quan hệ "hoặc" giữa các đối tượng có liên quan. Theo sáng chế, "ít nhất một" có nghĩa là một hoặc nhiều, và "nhiều" có nghĩa là từ hai trở lên. Ngoài ra, phải hiểu rằng, trong các phần mô tả của sáng chế, các thuật ngữ chẳng hạn như "thứ nhất", "thứ hai", và "thứ ba" chỉ đơn thuần được sử dụng để phân biệt và mô tả, nhưng không được hiểu là thể hiện hoặc ngụ ý mức ưu tiên tương đối hoặc thể hiện hoặc ngụ ý thứ tự.

Phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất theo các

phương án của sáng chế có thể được áp dụng cho hệ thống truyền thông thế hệ thứ tư (4th generation, 4G), ví dụ, hệ thống phát triển dài hạn (long term evolution, LTE); hệ thống truyền thông thế hệ thứ năm (5th generation, 5G), ví dụ, hệ thống vô tuyến mới (new radio, NR); hoặc các hệ thống truyền thông tương lai khác nhau, ví dụ, hệ thống truyền thông thế hệ thứ sáu (6th generation, 6G).

Fig.1 thể hiện cấu trúc của hệ thống truyền thông có thể mà phương pháp bảo vệ an toàn thông tin giao diện không gian theo một phương án của sáng chế có thể áp dụng được. Như được thể hiện trên Fig.1, hệ thống truyền thông 100 bao gồm thiết bị đầu cuối, thiết bị mạng truy nhập, và thiết bị mạng lõi. Thiết bị mạng truy nhập có thể cung cấp dịch vụ dành cho thiết bị đầu cuối trong vùng phủ. Các thiết bị mạng truy nhập được kết nối để truyền thông thông qua giao diện X2. Thiết bị mạng truy nhập được kết nối với thiết bị mạng lõi thông qua giao diện S1. Ví dụ, như được thể hiện trên Fig.1, hệ thống truyền thông 100 bao gồm trạm gốc 101 và trạm gốc 101'. Thiết bị đầu cuối trong vùng phủ của trạm gốc 101 được thể hiện bởi thiết bị đầu cuối 102, và thiết bị đầu cuối trong vùng phủ của trạm gốc 101' được thể hiện bởi thiết bị đầu cuối 102'. Hệ thống truyền thông 100 còn bao gồm thiết bị mạng lõi 103 và thiết bị mạng lõi 103'. Các dạng thiết bị mạng truy nhập, thiết bị đầu cuối, và thiết bị mạng lõi được chứa trong hệ thống truyền thông được mô tả bên dưới bằng cách sử dụng các ví dụ. Trạm gốc 101, thiết bị đầu cuối 102, và thiết bị mạng lõi 103 được sử dụng để mô tả.

Trạm gốc 101 là nút trong mạng truy nhập vô tuyến (radio access network, RAN), và cũng có thể được gọi là thiết bị mạng truy nhập, hoặc cũng có thể được gọi là nút (hoặc thiết bị) RAN. Hiện nay, ví dụ, trạm gốc 101 là gNB/NR-NB, điểm thu truyền (transmission reception point, TRP), NodeB tiến hóa (evolved Node B, eNB), bộ điều khiển mạng vô tuyến (radio network controller, RNC), NodeB (Node B, NB), bộ điều khiển trạm gốc (base station controller, BSC), trạm thu phát gốc (base transceiver station, BTS), trạm gốc thường trú (ví dụ, home evolved NodeB hoặc home Node B, HNB), đơn vị băng gốc (base band unit, BBU), Wi-Fi (wireless fidelity, Wifi), điểm truy nhập (access point, AP), thiết bị phía mạng trong hệ thống truyền thông 5G hoặc hệ thống truyền thông có thể có trong tương lai. Theo phương án này của sáng chế, thiết bị được tạo cấu hình để thực hiện chức năng trạm gốc có thể là trạm gốc, hoặc có thể là thiết bị mà có thể hỗ trợ trạm gốc để thực hiện chức năng này, ví dụ, hệ thống chip. Thiết bị này có thể được lắp đặt trong trạm gốc. Theo giải pháp kỹ thuật được đề xuất theo các phương án của sáng chế,

một ví dụ mà trong đó thiết bị được tạo cấu hình để thực hiện chức năng trạm gốc là trạm gốc được sử dụng để mô tả giải pháp kỹ thuật được đề xuất theo phương án này của sáng chế.

Thiết bị đầu cuối 102 còn được gọi là thiết bị người dùng (user equipment, UE), trạm di động (mobile station, MS), đầu cuối di động (mobile terminal, MT), hoặc thiết bị tương tự, và là thiết bị mà cung cấp khả năng kết nối giọng nói hoặc dữ liệu dành cho người dùng, hoặc có thể là thiết bị hệ thống vạn vật kết nối internet. Ví dụ, thiết bị đầu cuối 102 bao gồm thiết bị cầm tay hoặc thiết bị được lắp trên phương tiện vận chuyển mà có chức năng kết nối không dây. Hiện nay, thiết bị đầu cuối 102 có thể là điện thoại di động (mobile phone), máy tính bảng, máy tính dạng notebook, máy tính cầm tay, thiết bị internet di động (mobile internet device, MID), thiết bị đeo được (chẳng hạn như đồng hồ thông minh, băng đeo thông mình, hoặc thiết bị đếm bước chân), thiết bị được lắp trên phương tiện vận chuyển (chẳng hạn như xe ôtô, xe đạp, thiết bị vận chuyển chạy bằng điện, máy bay, tàu thủy, tàu hỏa, hoặc tàu tốc độ cao), thiết bị thực tế ảo (virtual reality, VR), thiết bị tăng cường thực tế (augmented reality, AR), thiết bị đầu cuối không dây trong dùng trong việc kiểm soát công nghiệp (industrial control), thiết bị gia dụng thông minh (chẳng hạn như tủ lạnh, máy thu hình, điều hòa không khí, hoặc đồng hồ đo điện), rôbôt thông minh, thiết bị dùng trong nhà xưởng, thiết bị đầu cuối không dây dùng trong việc tự lái xe (self driving), thiết bị đầu cuối không dây dùng trong phẫu thuật y tế từ xa (remote medical surgery), thiết bị đầu cuối không dây trong mạng lưới thông minh (smart grid), thiết bị đầu cuối không dây dùng trong an toàn vận tải (transportation safety), thiết bị đầu cuối không dây dùng trong thành phố thông minh (smart city), thiết bị đầu cuối không dây dùng trong nhà thông minh (smart home), thiết bị bay (chẳng hạn như rôbôt thông minh, khinh khí cầu, phương tiện vận chuyển bay không người lái, hoặc máy bay), hoặc thiết bị tương tự. Theo phương án này của sáng chế, thiết bị được tạo cấu hình để thực hiện chức năng thiết bị đầu cuối có thể là thiết bị đầu cuối, hoặc có thể là thiết bị mà có thể hỗ trợ thiết bị đầu cuối để thực hiện chức năng này, ví dụ, hệ thống chip. Thiết bị này có thể được lắp đặt trong thiết bị đầu cuối. Theo phương án này của sáng chế, hệ thống chip có thể bao gồm chip, hoặc có thể bao gồm chip và bộ phận rời rạc khác. Theo giải pháp kỹ thuật được đề xuất theo các phương án của sáng chế, một ví dụ mà trong đó thiết bị được tạo cấu hình để thực hiện chức năng thiết bị đầu cuối là thiết bị đầu cuối hoặc UE được sử dụng để mô tả giải pháp kỹ thuật được đề xuất theo phương án này của

sáng chế.

Thiết bị mạng lõi 103 được sử dụng để truyền thông giữa trạm gốc 101 và mạng IP. Mạng IP có thể là mạng (internet), mạng IP riêng, hoặc mạng dữ liệu khác. Ví dụ, trong hệ thống truyền thông phát triển dài hạn (long term evolution, LTE), thiết bị mạng lõi 103 bao gồm thực thể quản lý di động (mobile management entity, MME)/cổng dịch vụ (service-network gateway, S-GW). Hệ thống 5G được sử dụng như một ví dụ. Thiết bị mạng lõi 103 là chức năng quản lý truy nhập và di động (access and mobility management function, AMF).

Có thể được hiểu rằng hệ thống truyền thông 100 còn có thể bao gồm số lượng lớn các thiết bị đầu cuối 101, các trạm gốc 102, hoặc các thiết bị mạng lõi 103.

Theo phương án này của sáng chế, thông tin giao diện không gian là thông tin nhận được bởi trạm gốc từ thiết bị đầu cuối thông qua giao diện không gian.

Ví dụ, thông tin giao diện không gian có thể là khả năng vô tuyến của thiết bị đầu cuối hoặc bộ nhận dạng khả năng vô tuyến. Bộ nhận dạng khả năng vô tuyến được sử dụng để nhận dạng khả năng vô tuyến cụ thể. Phần sau đây sử dụng một ví dụ mà trong đó thông tin giao diện không gian là khả năng vô tuyến để mô tả. Có thể hiểu rằng giải pháp mà liên quan đến thông tin giao diện không gian và được mô tả theo phương án này của sáng chế có thể được thay thế bằng giải pháp liên quan đến khả năng vô tuyến hoặc bộ nhận dạng khả năng vô tuyến. Khả năng vô tuyến của thiết bị đầu cuối bao gồm các thông số chẳng hạn như mức công suất và băng tần số của thiết bị đầu cuối. Theo một dạng thực hiện có thể, trong thời gian đăng ký khởi tạo của thiết bị đầu cuối, thì thiết bị đầu cuối không mang khả năng vô tuyến tới thiết bị mạng lõi. Do đó, trạm gốc không thể nhận khả năng vô tuyến của thiết bị đầu cuối từ bản tin N2 (ví dụ, bản tin thiết đặt ngữ cảnh khởi tạo (initial context setup)) của mạng lõi. Trong trường hợp này, trạm gốc có thể chỉ khởi tạo bản tin truy vấn khả năng vô tuyến tới thiết bị đầu cuối, và thiết bị đầu cuối thu bản tin truy vấn khả năng vô tuyến từ trạm gốc, và trả về khả năng vô tuyến cho trạm gốc. Vì lượng dữ liệu của khả năng vô tuyến của thiết bị đầu cuối tương đối lớn, nên để ngăn thiết bị đầu cuối không thường xuyên gửi khả năng này tới trạm gốc, thì trạm gốc gửi khả năng vô tuyến nhận được bởi truy vấn tới thiết bị mạng lõi để lưu trữ. Khả năng vô tuyến được lưu trong thiết bị mạng lõi trong một thời gian dài cho đến khi thiết bị đầu cuối hủy đăng ký. Khả năng vô tuyến của thiết bị đầu cuối được lưu trong thiết bị mạng lõi. Khi chuyển vùng trạm gốc xảy ra khi thiết bị đầu cuối di chuyển, hoặc thiết bị đầu

cuối đi vào trạng thái được kết nối từ trạng thái nghỉ, thì trạm gốc có thể trực tiếp nhận khả năng vô tuyến của thiết bị đầu cuối từ thiết bị mạng lõi, và không cần phải truy vấn thiết bị đầu cuối lần nữa.

Để đảm bảo an toàn khi thiết bị đầu cuối gửi thông tin giao diện không gian tới trạm gốc, 3GPP quy định rằng sau khi thiết bị đầu cuối thiết đặt an toàn AS với trạm gốc, thì thiết bị đầu cuối sử dụng ngữ cảnh của an toàn AS để bảo vệ thông tin giao diện không gian. Vì các kiểu thiết bị đầu cuối trong hệ thống truyền thông tiến hóa, nên một số kiểu thiết bị đầu cuối không hỗ trợ hoặc không cần thiết đặt an toàn AS với trạm gốc. Ví dụ, một số thiết bị hệ thống vạn vật kết nối internet (internet of things, IoT), ví dụ, thiết bị đầu cuối tối ưu (optimization) hệ thống vạn vật kết nối internet tế bào mặt (cellular IoT, CIoT) phẳng điều khiển (control plane), không thể thiết đặt an toàn AS với trạm gốc. Thiết bị đầu cuối tối ưu CIoT mặt phẳng điều khiển bao gồm thiết bị đầu cuối tối ưu CIoT 4G mặt phẳng điều khiển (control plane CIoT EPS optimization) hoặc thiết bị đầu cuối tối ưu CIoT 5G mặt phẳng điều khiển (control plane CIoT 5GS optimization). EPS là hệ thống gói tiến hóa (evolved packet system). Đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, khi thiết bị đầu cuối gửi thông tin giao diện không gian tới trạm gốc, thì thiết bị đầu cuối không thể sử dụng ngữ cảnh của AS để mã mật và bảo vệ thông tin giao diện không gian. Kết quả là, thông tin giao diện không gian có thể bị tấn công bởi kẻ tấn công.

Phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất theo phương án này của sáng chế có thể áp dụng được cho kiểu thiết bị đầu cuối bất kỳ, và giúp đảm bảo an toàn của thông tin giao diện không gian khi thiết bị đầu cuối trao đổi thông tin giao diện không gian với trạm gốc. Tùy chọn là, đối với thiết bị đầu cuối mà không hỗ trợ hoặc không thể thiết đặt an toàn AS với trạm gốc, theo phương pháp được đề xuất theo phương án này của sáng chế, khi thiết bị đầu cuối không thiết đặt an toàn AS với trạm gốc, thì an toàn của thông tin giao diện không gian có thể được đảm bảo.

Như được thể hiện trên Fig.2, quy trình của phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất theo phương án này của sáng chế được mô tả như sau.

S201: Thiết bị đầu cuối xác định giá trị mã nhận thực bản tin (message authentication code, MAC) thứ nhất dựa trên khóa an toàn và thông tin giao diện không gian.

Khóa an toàn là khóa an toàn tầng không truy nhập (non-access stratum, NAS) giữa

thiết bị đầu cuối và thiết bị mạng lõi.

An toàn NAS có thể được thiết đặt trước giữa thiết bị đầu cuối và thiết bị mạng lõi. Để biết tất cả các bước để thiết đặt an toàn NAS giữa thiết bị đầu cuối và thiết bị mạng lõi theo các phương án của sáng chế, thì có thể tham khảo các phần mô tả theo phương án trên Fig.2.

Nếu thiết bị mạng lõi là MME trong mạng 4G, khi an toàn NAS được thiết đặt giữa thiết bị đầu cuối và MME, thì thiết bị đầu cuối và MME chia sẻ khóa an toàn NAS, và khía an toàn NAS có thể là khóa Kasme giữa thiết bị đầu cuối và MME. Nếu thiết bị mạng lõi là AMF trong mạng 5G, khi an toàn NAS được thiết đặt giữa thiết bị đầu cuối và AMF, thì thiết bị đầu cuối và AMF chia sẻ khóa an toàn, và khóa an toàn NAS có thể là khóa Kamf giữa thiết bị đầu cuối và AMF. Khóa an toàn NAS giữa thiết bị đầu cuối và thiết bị mạng lõi còn có thể là khóa bảo vệ tính toàn vẹn Kansint hoặc khóa bảo vệ tính bí mật Knasenc.

Khóa an toàn NAS giữ thiết bị đầu cuối và thiết bị mạng lõi có thể là một hoặc nhiều khóa bất kỳ trong số Kasme, Kamf, Kansint, hoặc Knasenc. Ngoài ra, khóa an toàn NAS giữa thiết bị đầu cuối và thiết bị mạng lõi có thể là khóa nhận được thông qua suy diễn dựa trên một hoặc nhiều khóa trong số Kasme, Kamf, Kansint, hoặc Knasenc.

Tùy chọn là, S200 được thực hiện trước bước S201.

S200: Trạm gốc gửi bản tin yêu cầu tới thiết bị đầu cuối, trong đó bản tin yêu cầu được ký hiệu là bản tin yêu cầu thứ nhất, và thiết bị đầu cuối thu bản tin yêu cầu thứ nhất từ trạm gốc.

Bản tin yêu cầu thứ nhất được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối. Sau khi thu bản tin yêu cầu được gửi bởi trạm gốc, thì thiết bị đầu cuối thực hiện bảo vệ tính toàn vẹn trên thông tin giao diện không gian.

Cụ thể là, thiết bị đầu cuối xác định giá trị MAC dựa trên khóa an toàn NAS giữa thiết bị đầu cuối và thiết bị mạng lõi và thông tin giao diện không gian, trong đó giá trị MAC được ký hiệu là giá trị MAC thứ nhất. Việc xác định giá trị MAC cũng có thể được hiểu như việc tính giá trị MAC.

Tùy chọn là, khi xác định giá trị MAC thứ nhất dựa trên khóa an toàn và thông tin giao diện không gian, thì thiết bị đầu cuối còn có thể xác định giá trị MAC thứ nhất dựa vào thông số nhập. Ví dụ, thiết bị đầu cuối có thể thực hiện tính hàm băm (hash) dựa trên khóa an toàn, thông số nhập, và thông tin giao diện không gian, để nhận giá trị MAC thứ

nhất. Khóa an toàn và/hoặc thông số nhập có thể được xác định dựa trên ngữ cảnh của an toàn NAS giữa thiết bị đầu cuối và thiết bị mạng lõi. Thông số nhập có thể bao gồm bộ nhận dạng tế bào và/hoặc thông số tươi. Thông số tươi có thể là một hoặc nhiều thông số bất kỳ trong số các thông số sau đây: một phần hoặc tất cả các bit để đếm NAS count đường lên (uplink NAS count), một phần hoặc tất cả các bit để đếm NAS count đường xuống (downlink NAS count), hoặc số ngẫu nhiên. Thông số nhập để tính giá trị MAC thứ nhất không bị hạn chế theo sáng chế.

S202: Thiết bị đầu cuối gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc.

Thiết bị đầu cuối có thể gửi bản tin điều khiển tài nguyên vô tuyến (radio resource control, RRC) tới trạm gốc, trong đó bản tin RRC mang thông tin giao diện không gian và giá trị MAC thứ nhất. Trong trường hợp này, sau khi thu bản tin RRC từ thiết bị đầu cuối, thì trạm gốc có thể nhận thông tin giao diện không gian và giá trị MAC thứ nhất từ bản tin RRC.

Ngoài ra, thiết bị đầu cuối có thể bao gồm bản tin NAS trong bản tin RRC được gửi tới trạm gốc. Ví dụ, bản tin RRC mang bản tin NAS, và bản tin NAS mang thông tin giao diện không gian và giá trị MAC thứ nhất. Trạm gốc chuyển tiếp bản tin NAS tới thiết bị mạng lõi.

Dựa trên hai trường hợp được đề cập ở trên, các hoạt động được thực hiện bởi phía trạm gốc được mô tả bằng cách sử dụng S203 và S203a.

S203: Sau khi thu thông tin giao diện không gian và giá trị MAC thứ nhất từ thiết bị đầu cuối, thì trạm gốc gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới thiết bị mạng lõi, và thiết bị mạng lõi thu thông tin giao diện không gian và giá trị MAC thứ nhất từ trạm gốc.

Thông tin giao diện không gian và giá trị MAC thứ nhất có thể được mang trong bản tin RRC. Trạm gốc thu bản tin RRC từ thiết bị đầu cuối, và nhận thông tin giao diện không gian và giá trị MAC thứ nhất từ bản tin RRC.

Tùy chọn là, trạm gốc có thể gửi bản tin yêu cầu tới thiết bị mạng lõi, trong đó bản tin yêu cầu được ký hiệu là bản tin yêu cầu thứ hai, và bản tin yêu cầu thứ hai mang thông tin giao diện không gian và giá trị MAC thứ nhất.

Bản tin yêu cầu thứ hai được sử dụng để yêu cầu thiết bị mạng lõi để xác nhận tính toàn vẹn của thông tin giao diện không gian.

S203a: Trạm gốc thu bản tin RRC từ thiết bị đầu cuối, trong đó bản tin RRC mang bản tin NAS, và bản tin NAS mang thông tin giao diện không gian và giá trị MAC thứ nhất. Trạm gốc gửi bản tin NAS tới thiết bị mạng lõi, và thiết bị mạng lõi thu bản tin NAS từ trạm gốc.

Bản tin RRC có thể được hiểu là bản tin hồi đáp, và bản tin hồi đáp được sử dụng để hồi đáp bản tin yêu cầu mà được gửi bởi trạm gốc tới thiết bị đầu cuối và được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối. Trạm gốc có thể trực tiếp chuyển tiếp bản tin NAS được thu từ thiết bị đầu cuối tới thiết bị mạng lõi.

Tùy chọn là, bản tin NAS được gửi bởi trạm gốc tới mạng lõi là bản tin yêu cầu thứ hai; hoặc trạm gốc gửi bản tin yêu cầu thứ hai tới thiết bị mạng lõi, và bản tin yêu cầu thứ hai mang bản tin NAS. Bản tin yêu cầu thứ hai được sử dụng để yêu cầu thiết bị mạng lõi để xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc trả về thông tin giao diện không gian.

Trước khi gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới thiết bị mạng lõi, thì trạm gốc còn có thể xác định kiểu của thiết bị đầu cuối. Cụ thể là, trạm gốc xác định việc thiết bị đầu cuối có phải là thiết bị đầu cuối mà không thể thiết đặt an toàn AS hay không, hoặc trạm gốc xác định việc thiết bị đầu cuối có phải là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển hay không.

S204: Sau khi thu bản tin yêu cầu thứ hai từ trạm gốc, thì thiết bị mạng lõi xác nhận tính toàn vẹn của thông tin giao diện không gian dựa trên giá trị MAC thứ nhất.

Cụ thể là, thiết bị mạng lõi thiết đặt trước an toàn NAS với thiết bị đầu cuối, và thiết bị mạng lõi xác nhận tính toàn vẹn của thông tin giao diện không gian bằng cách sử dụng ngữ cảnh của an toàn NAS và giá trị MAC thứ nhất.

S205: Thiết bị mạng lõi gửi kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian tới trạm gốc.

Ví dụ, nếu thiết bị mạng lõi thu bản tin yêu cầu thứ hai từ trạm gốc, trong đó bản tin yêu cầu thứ hai mang thông tin giao diện không gian và giá trị MAC thứ nhất, thì thiết bị mạng lõi gửi bản tin hồi đáp của bản tin yêu cầu thứ hai tới trạm gốc, trong đó bản tin hồi đáp được ký hiệu là bản tin hồi đáp thứ hai. Bản tin hồi đáp thứ hai mang kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian.

Nếu thiết bị mạng lõi thu bản tin yêu cầu thứ hai từ trạm gốc, trong đó bản tin yêu cầu thứ hai mang bản tin NAS, và bản tin NAS mang thông tin giao diện không gian và

giá trị MAC thứ nhất, thì thiết bị mạng lõi trả về bản tin hồi đáp thứ hai của bản tin yêu cầu thứ hai cho trạm gốc, và bản tin hồi đáp thứ hai mang kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian. Bằng cách này, trạm gốc có thể nhận thông tin giao diện không gian của thiết bị đầu cuối và kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian. Tùy chọn là, nếu việc xác nhận trên thông tin giao diện không gian không thành công, thì thiết bị mạng lõi cũng có thể chỉ phản hồi kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và không phản hồi thông tin giao diện không gian.

Tóm lại, thiết bị đầu cuối thực hiện bảo vệ an toàn dành cho thông tin giao diện không gian bằng cách sử dụng khóa an toàn NAS của thiết bị mạng lõi. Hiệu năng an toàn của thông tin giao diện không gian được gửi bởi thiết bị đầu cuối có thể được đảm bảo khi thiết bị đầu cuối không thể thiết đặt an toàn AS với trạm gốc.

Dựa trên cùng một khái niệm kỹ thuật, thiết bị đầu cuối còn có thể xác nhận việc trạm gốc có hợp lệ hay không. Như được thể hiện trên Fig.3, phương pháp cụ thể được mô tả như sau.

S301: Trạm gốc gửi bản tin yêu cầu tới thiết bị mạng lõi. Để phân biệt, bản tin yêu cầu ở đây được ký hiệu là bản tin yêu cầu thứ ba. Thiết bị mạng lõi thu bản tin yêu cầu thứ ba từ trạm gốc.

Tùy chọn là, trước khi gửi bản tin yêu cầu thứ ba tới thiết bị mạng lõi, thì trạm gốc xác định kiểu của thiết bị đầu cuối. Cụ thể là, trạm gốc xác định việc thiết bị đầu cuối có phải là thiết bị đầu cuối mà không thể thiết đặt an toàn AS hay không, hoặc trạm gốc xác định việc thiết bị đầu cuối có phải là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển hay không.

S302: Sau khi thu bản tin yêu cầu thứ ba từ trạm gốc, thì thiết bị mạng lõi xác định giá trị MAC thứ hai.

An toàn NAS có thể được thiết đặt trước giữa thiết bị mạng lõi và thiết bị đầu cuối. Thiết bị mạng lõi xác định giá trị MAC thứ hai dựa trên ngữ cảnh của an toàn NAS.

S303: Thiết bị mạng lõi gửi bản tin hồi đáp thứ ba của bản tin yêu cầu thứ ba tới trạm gốc, trong đó bản tin hồi đáp thứ ba mang giá trị MAC thứ hai. Trạm gốc thu bản tin hồi đáp thứ ba từ thiết bị mạng lõi.

Trạm gốc nhận giá trị MAC thứ hai từ bản tin hồi đáp thứ ba.

S304: Trạm gốc gửi bản tin yêu cầu thứ nhất tới thiết bị đầu cuối, và thiết bị đầu

cuối thu bản tin yêu cầu thứ nhất từ trạm gốc.

Bản tin yêu cầu thứ nhất mang giá trị MAC thứ hai. Giá trị MAC thứ hai được sử dụng bởi thiết bị đầu cuối để xác nhận trạm gốc. Bản tin yêu cầu thứ nhất được sử dụng để yêu cầu thông tin giao diện không gian. Bản tin yêu cầu thứ nhất có thể là bản tin RRC.

S305: Sau khi thu bản tin yêu cầu thứ nhất từ trạm gốc, thì thiết bị đầu cuối xác nhận độ chính xác của giá trị MAC thứ hai. Nếu việc xác nhận thành công, thì giá trị MAC thứ nhất được xác định, và các bước tiếp theo được tiếp tục.

Bằng cách này, thiết bị đầu cuối có thể xác nhận việc trạm gốc có hợp lệ hay không dựa trên giá trị MAC thứ hai, sao cho khi không có an toàn AS được thiết lập giữa thiết bị đầu cuối và trạm gốc, thì an toàn truyền dẫn thông tin được đảm bảo, và việc xác nhận hai chiều được thực hiện.

Dựa trên cũng một khái niệm kỹ thuật, phương pháp khác dành cho thiết bị đầu cuối để xác nhận việc trạm gốc có hợp lệ hay không được thể hiện trên Fig.4.

S401: Trạm gốc gửi bản tin yêu cầu thứ ba tới thiết bị mạng lõi, và thiết bị mạng lõi thu bản tin yêu cầu thứ ba từ trạm gốc, trong đó bản tin yêu cầu thứ ba mang bản tin yêu cầu thứ nhất.

Ví dụ, bản tin yêu cầu thứ nhất là bản tin RRC mà sẽ được gửi bởi trạm gốc tới thiết bị đầu cuối và được sử dụng để yêu cầu thông tin giao diện không gian.

Tùy chọn là, trước khi gửi bản tin yêu cầu thứ ba tới thiết bị mạng lõi, thì trạm gốc xác định kiểu của thiết bị đầu cuối. Cụ thể là, trạm gốc xác định việc thiết bị đầu cuối có phải là thiết bị đầu cuối mà không thể thiết đặt an toàn AS hay không, hoặc trạm gốc xác định việc thiết bị đầu cuối có phải là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển hay không.

S402: Mạng lõi xác định giá trị MAC thứ hai.

Giá trị MAC thứ hai được sử dụng để thực hiện bảo vệ NAS trên bản tin yêu cầu thứ nhất được mang trong bản tin yêu cầu thứ ba. An toàn NAS có thể được thiết đặt trước giữa thiết bị mạng lõi và thiết bị đầu cuối. Thiết bị mạng lõi xác định giá trị MAC thứ hai dựa trên ngữ cảnh của an toàn NAS.

S403: Thiết bị mạng lõi gửi bản tin yêu cầu thứ nhất mà trên đó bảo vệ NAS được áp dụng cho trạm gốc, và trạm gốc thu bản tin yêu cầu thứ nhất mà trên đó bảo vệ NAS được áp dụng từ thiết bị mạng lõi.

Bản tin yêu cầu thứ nhất mà trên đó bảo vệ NAS được áp dụng có nghĩa là bản tin yêu cầu thứ nhất mang giá trị MAC thứ hai.

S404: Trạm gốc gửi bản tin yêu cầu thứ nhất mà trên đó bảo vệ NAS được áp dụng cho thiết bị đầu cuối, và thiết bị đầu cuối thu bản tin yêu cầu thứ nhất mà trên đó bảo vệ NAS được áp dụng từ trạm gốc.

Bằng cách này, mạng lõi thực hiện bảo vệ NAS trên bản tin yêu cầu thứ nhất, sao cho khi không có an toàn AS được thiết lập giữa thiết bị đầu cuối và trạm gốc, thì an toàn truyền dẫn thông tin có thể được đảm bảo, và việc xác nhận hai chiều có thể được thực hiện.

Như được thể hiện trên Fig.5, một ví dụ mà trong đó thông tin giao diện không gian của thiết bị đầu cuối là khả năng vô tuyến được sử dụng bên dưới để mô tả thêm phương pháp bảo vệ an toàn thông tin giao diện không gian. Nhiều bước liên tiếp hoặc không liên tiếp bất kỳ trong các phần mô tả sau đây có thể tạo thành các giải pháp kỹ thuật sẽ được bảo hộ theo sáng chế, và các bước còn lại là các bước tùy chọn.

S501: An toàn NAS được thiết đặt giữa thiết bị đầu cuối và thiết bị mạng lõi.

S502: Trạm gốc gửi bản tin yêu cầu 1 tới thiết bị mạng lõi, và thiết bị mạng lõi thu bản tin yêu cầu 1 từ trạm gốc.

S503: Thiết bị mạng lõi xác định giá trị MAC 1.

Thiết bị mạng lõi tính giá trị MAC 1 dựa trên ngữ cảnh của an toàn NAS giữa thiết bị mạng lõi và thiết bị đầu cuối.

S504: Thiết bị mạng lõi gửi bản tin hồi đáp 1 tới trạm gốc, và trạm gốc thu bản tin hồi đáp 1 từ thiết bị mạng lõi.

Bản tin hồi đáp 1 được sử dụng để hồi đáp bản tin yêu cầu 1, và bản tin hồi đáp 1 mang giá trị MAC 1.

S505: Trạm gốc gửi bản tin yêu cầu 2 tới thiết bị đầu cuối, và thiết bị đầu cuối thu bản tin yêu cầu 2 từ trạm gốc.

Bản tin yêu cầu 2 được sử dụng để yêu cầu khả năng vô tuyến của thiết bị đầu cuối. Tùy chọn là, bản tin yêu cầu 2 mang MAC 1.

S506: Thiết bị đầu cuối xác định giá trị MAC 2.

Thiết bị đầu cuối có thể xác định giá trị MAC 2 dựa trên ngữ cảnh của an toàn NAS được thiết đặt giữa thiết bị đầu cuối và thiết bị mạng lõi.

Tùy chọn là, thiết bị đầu cuối trước hết xác nhận độ chính xác của MAC 1, và xác

định giá trị MAC 2 nếu việc xác nhận thành công.

S507: Thiết bị đầu cuối gửi thông tin về khả năng vô tuyến tới trạm gốc, trong đó thông tin về khả năng vô tuyến có thể mang MAC 2. Trạm gốc thu thông tin về khả năng vô tuyến từ thiết bị đầu cuối.

S508: Trạm gốc gửi bản tin yêu cầu 2 tới thiết bị mạng lõi, và thiết bị mạng lõi thu bản tin yêu cầu 2 từ trạm gốc.

Bản tin yêu cầu 2 mang khả năng vô tuyến và MAC 2, và được sử dụng để yêu cầu để xác nhận tính toàn vẹn của khả năng vô tuyến.

S509: Thiết bị mạng lõi xác nhận tính toàn vẹn của khả năng vô tuyến dựa trên MAC 2 và ngữ cảnh của an toàn NAS.

S510: Thiết bị mạng lõi trả về kết quả xác nhận cho trạm gốc, và trạm gốc thu kết quả xác nhận của khả năng vô tuyến từ thiết bị mạng lõi.

Theo một dạng thực hiện có thể, bản tin yêu cầu 1 được gửi bởi trạm gốc tới thiết bị mạng lõi ở bước S502 mang bản tin yêu cầu 2. Ở bước S503, thiết bị mạng lõi thực hiện bảo vệ an toàn NAS trên bản tin yêu cầu 2, và ở bước S504, thiết bị mạng lõi trả về bản tin yêu cầu 2 mà trên đó bảo vệ an toàn NAS được thực hiện cho trạm gốc. Ở bước S505, trạm gốc gửi bản tin yêu cầu 2 mà trên đó bảo vệ an toàn NAS được thực hiện tới thiết bị đầu cuối.

Tương tự, theo một dạng thực hiện có thể, khả năng vô tuyến được gửi bởi thiết bị đầu cuối tới trạm gốc ở bước S507 có thể được đóng gói trong bản tin NAS, và trạm gốc chuyển tiếp bản tin NAS tới thiết bị mạng lõi ở bước S508. Ở bước S509, mạng lõi phân tích cú pháp khả năng vô tuyến và MAC 2 trong bản tin NAS, và trả về kết quả xác nhận và/hoặc khả năng vô tuyến của thiết bị đầu cuối cho trạm gốc.

Dựa trên cùng một khái niệm kỹ thuật, như được thể hiện trên Fig.6, một phương án của sáng chế còn đề xuất phương pháp bảo vệ an toàn thông tin giao diện không gian khác.

S601: Thiết bị mạng lõi gửi bản tin yêu cầu tới thiết bị đầu cuối, và thiết bị đầu cuối thu bản tin yêu cầu từ thiết bị mạng lõi.

Bản tin yêu cầu được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối.

S602: Thiết bị đầu cuối trả về bản tin hồi đáp của bản tin yêu cầu cho thiết bị mạng lõi, và thiết bị mạng lõi thu bản tin hồi đáp từ thiết bị đầu cuối.

Bản tin hồi đáp mang thông tin giao diện không gian của thiết bị đầu cuối. Bản tin hồi đáp là bản tin NAS và là bản tin mà trên đó bảo vệ an toàn NAS được thực hiện.

Trước bước S601, phương pháp này còn có thể bao gồm bước sau đây: An toàn NAS được thiết đặt giữa thiết bị đầu cuối và mạng lõi. Trước khi gửi bản tin yêu cầu tới thiết bị đầu cuối, thiết bị mạng lõi xác định rằng kiểu của thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển. Nói cách khác, thiết bị mạng lõi xác định rằng an toàn AS không thể được thiết đặt giữa thiết bị đầu cuối và trạm gốc. Do đó, thông tin giao diện không gian có thể bị tấn công khi thiết bị đầu cuối trực tiếp gửi thông tin giao diện không gian tới trạm gốc, và an toàn không thể được đảm bảo. Trong trường hợp này, thiết bị mạng lõi trực tiếp yêu cầu thông tin giao diện không gian từ thiết bị đầu cuối bằng cách sử dụng ngữ cảnh của an toàn NAS, và thiết bị đầu cuối trả về thông tin giao diện không gian cho thiết bị mạng lõi dựa trên ngữ cảnh của an toàn NAS. Bằng cách này, khi trạm gốc cần phải nhận thông tin giao diện không gian của thiết bị đầu cuối, thì trạm gốc có thể yêu cầu thông tin giao diện không gian của thiết bị đầu cuối từ mạng lõi.

Thiết bị mạng lõi có thể thực hiện bước S601 sau khi thiết bị đầu cuối đăng ký với thiết bị mạng lõi.

Theo một dạng thực hiện có thể, bước S600 còn được thực hiện trước bước S601.

S600: Trạm gốc gửi bản tin yêu cầu tới thiết bị mạng lõi. Mạng lõi thu bản tin yêu cầu từ trạm gốc.

Bản tin yêu cầu được sử dụng để yêu cầu để truy vấn thông tin giao diện không gian của thiết bị đầu cuối. Tùy chọn là, trạm gốc xác định kiểu của thiết bị đầu cuối; và khi xác định rằng kiểu của thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển, thì trạm gốc gửi bản tin yêu cầu tới thiết bị mạng lõi. Trạm gốc xác định rằng thiết bị đầu cuối không thể báo cáo thông tin giao diện không gian bằng cách sử dụng an toàn AS, và yêu cầu thông tin giao diện không gian của thiết bị đầu cuối từ mạng lõi.

Bước S604 còn được thực hiện sau bước S602.

S604: Thiết bị mạng lõi gửi thông tin giao diện không gian của thiết bị đầu cuối tới trạm gốc, và trạm gốc thu thông tin giao diện không gian của thiết bị đầu cuối từ thiết bị mạng lõi.

Tùy chọn là, dựa trên bước S601 và S602, mạng lõi nhận thông tin giao diện không

gian của thiết bị đầu cuối từ thiết bị đầu cuối, và thiết bị mạng lõi có thể lưu thông tin giao diện không gian của thiết bị đầu cuối. Khi thu bản tin yêu cầu mà được gửi bởi trạm gốc và được sử dụng để yêu cầu thông tin giao diện không gian của thiết bị đầu cuối, thì thiết bị mạng lõi gửi thông tin giao diện không gian đã được lưu sẵn của thiết bị đầu cuối tới trạm gốc.

Tóm lại, thông tin giao diện không gian của thiết bị đầu cuối được nhận từ thiết bị đầu cuối thông qua mạng lõi, thông tin giao diện không gian của thiết bị đầu cuối có thể được bảo vệ bằng cách sử dụng ngữ cảnh của an toàn NAS, và hiệu năng an toàn của thông tin giao diện không gian của thiết bị đầu cuối được bảo vệ khi thiết bị đầu cuối và trạm gốc không thể thiết đặt an toàn AS.

Dựa trên cùng một khái niệm kỹ thuật, như được thể hiện trên Fig.6a, một phương án của sáng chế còn đề xuất phương pháp bảo vệ an toàn thông tin giao diện không gian khác.

S601a: Thiết bị đầu cuối xác định kiểu của thiết bị đầu cuối.

Thiết bị đầu cuối xác định rằng kiểu của thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển, hoặc thiết bị đầu cuối mà không thể thiết đặt an toàn AS.

S602a: Thiết bị đầu cuối gửi thông tin giao diện không gian tới thiết bị mạng lõi, và thiết bị mạng lõi thu thông tin giao diện không gian từ thiết bị đầu cuối.

Trước bước S601a, phương pháp này còn có thể bao gồm bước sau đây: An toàn NAS được thiết đặt giữa thiết bị đầu cuối và mạng lõi. Sau khi xác định kiểu của thiết bị đầu cuối, thì thiết bị đầu cuối biết rằng an toàn AS không thể được thiết đặt giữa thiết bị đầu cuối và trạm gốc. Do đó, thông tin giao diện không gian có thể bị tấn công khi thiết bị đầu cuối trực tiếp gửi thông tin giao diện không gian tới trạm gốc, và an toàn không thể được đảm bảo. Trong trường hợp này, thiết bị đầu cuối gửi thông tin giao diện không gian tới thiết bị mạng lõi bằng cách sử dụng bản tin NAS. Bằng cách này, khi trạm gốc cần phải nhận thông tin giao diện không gian của thiết bị đầu cuối, thì trạm gốc có thể yêu cầu thông tin giao diện không gian của thiết bị đầu cuối từ mạng lõi.

Dựa trên cùng một khái niệm kỹ thuật, như được thể hiện trên Fig.7, phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất theo phương án này của sáng chế còn có thể được thực hiện bằng cách sử dụng các bước sau đây. Nhiều bước liên tiếp hoặc không liên tiếp bất kỳ trong các phần mô tả sau đây có thể tạo thành các giải pháp kỹ

thuật sẽ được bảo hộ theo sáng chế, và các bước còn lại là các bước tùy chọn.

S701: Thiết bị đầu cuối thiết đặt an toàn NAS với thiết bị mạng lõi.

S702: Trạm gốc gửi bản tin yêu cầu tới thiết bị mạng lõi, và thiết bị mạng lõi thu bản tin yêu cầu từ trạm gốc.

Bản tin yêu cầu được sử dụng để yêu cầu thông số an toàn, ví dụ, giá trị MAC hoặc khóa an toàn được sử dụng để yêu cầu để truy vấn thông tin giao diện không gian.

Tùy chọn là, trước khi gửi bản tin yêu cầu, thì trạm gốc xác định kiểu của thiết bị đầu cuối. Cụ thể là, trạm gốc xác định việc thiết bị đầu cuối có phải là thiết bị đầu cuối mà không thể thiết đặt an toàn AS hay không, hoặc trạm gốc xác định việc thiết bị đầu cuối có phải là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển hay không. Nếu trạm gốc xác định rằng thiết bị đầu cuối là thiết bị đầu cuối mà không thể thiết đặt an toàn AS hoặc là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển, thì trạm gốc gửi bản tin yêu cầu tới thiết bị mạng lõi.

S703: Thiết bị mạng lõi thu khía trạm gốc Key*, trong đó khóa này có thể nhận được thông qua việc suy diễn bằng cách sử dụng Kamf hoặc Kasme. Điều này không bị hạn chế.

S704: Thiết bị mạng lõi trả về Key* cho trạm gốc, và trạm gốc thu Key* từ thiết bị mạng lõi.

Tùy chọn là, thông số tươi còn có thể được trả về cho trạm gốc, và có thể được trả về bằng cách sử dụng bản tin N2.

S705: Trạm gốc bảo vệ bản tin RRC của UE bằng cách sử dụng Key*.

S706: Trạm gốc gửi bản tin yêu cầu tới thiết bị đầu cuối, trong đó bản tin yêu cầu được sử dụng để yêu cầu để truy vấn thông tin giao diện không gian của thiết bị đầu cuối.

Bản tin yêu cầu được bảo vệ bằng cách sử dụng Key*, và bản tin yêu cầu có thể mang giá trị MAC 3, thông số tươi, và/hoặc thông tin tương tự.

S707: Sau khi thu bản tin yêu cầu từ trạm gốc, thì thiết bị đầu cuối tính Key* theo cách thức giống như của thiết bị mạng lõi.

Giá trị MAC 3 được mang trong bản tin yêu cầu ở bước S706 được xác nhận. Nếu việc xác nhận thành công, thì bước S708 được thực hiện.

S708: Thiết bị đầu cuối gửi thông tin giao diện không gian của thiết bị đầu cuối mà được bảo vệ bằng cách sử dụng Key* tới trạm gốc, và trạm gốc thu thông tin giao diện

không gian từ thiết bị đầu cuối.

Thông tin giao diện không gian được gửi bởi thiết bị đầu cuối có thể mang MAC 4 và/hoặc thông số tươi.

S709: Sau khi thu thông tin giao diện không gian từ thiết bị đầu cuối, thì trạm gốc xác nhận MAC 4 bằng cách sử dụng Key*.

Sau khi việc xác nhận thành công, thì nhận được thông tin giao diện không gian của thiết bị đầu cuối.

Phải lưu ý rằng các tên gọi của một số bản tin hoặc báo hiệu theo các phương án của sáng chế chỉ đơn thuần là các tên gọi làm ví dụ, và cũng có thể được gọi bằng các tên gọi khác. Việc này không bị hạn chế theo sáng chế. Ví dụ, bản tin yêu cầu 1, bản tin yêu cầu 2, yêu cầu khóa key, bản tin hồi đáp 1, bản tin hồi đáp 2, hoặc hồi đáp khóa đều có thể được gọi bằng tên gọi khác. Ngoài ra, các phần mô tả được đề cập ở trên được cung cấp dựa trên trường hợp thỏa thuận khóa trong hệ thống các phương tiện vận chuyển kết nối internet, và cũng có thể được cung cấp dựa trên trường hợp thỏa thuận khóa cụ thể. Điều này không bị hạn chế.

Theo các phương án được đề cập ở trên được đề xuất theo sáng chế, các phương pháp được đề xuất theo các phương án của sáng chế được mô tả riêng biệt từ quan điểm sự tương tác giữa thiết bị đầu cuối, trạm gốc, và thiết bị mạng lõi. Để thực hiện các chức năng theo các phương pháp được đề xuất theo các phương án của sáng chế, thiết bị đầu cuối, trạm gốc, và thiết bị mạng lõi có thể bao gồm kết cấu phần cứng và/hoặc môđun phần mềm, và thực hiện các chức năng được đề cập ở trên dưới dạng kết cấu phần cứng, môđun phần mềm, hoặc dạng kết hợp của kết cấu phần cứng và môđun phần mềm. Việc chức năng trong số các chức năng được đề cập ở trên có được thực hiện bằng cách sử dụng kết cấu phần cứng, môđun phần mềm, hoặc dạng kết hợp của kết cấu phần cứng và môđun phần mềm hay không tùy thuộc vào các ứng dụng cụ thể và các điều kiện ràng buộc thiết kế của các giải pháp kỹ thuật.

Như được thể hiện trên Fig.8, dựa trên cùng một khái niệm kỹ thuật, một phương án của sáng chế còn đề xuất thiết bị 800. Thiết bị 800 có thể là thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi, có thể là thiết bị trong thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi, hoặc có thể là thiết bị mà có thể được sử dụng cùng với thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi. Theo một phương án, thiết bị 800 có thể bao gồm các môđun mà ở dạng tương ứng một-một với các phương pháp/hoạt động/bước/nhiệm vụ được thực

hiện bởi thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi theo các phương án phương pháp được đề cập ở trên. Các môđun này có thể được thực hiện bằng cách sử dụng mạch phần cứng, phần mềm, hoặc dạng kết hợp của mạch phần cứng và phần mềm. Theo một phương án, thiết bị này có thể bao gồm môđun xử lý 801 và môđun truyền thông 802.

Khi thiết bị này được tạo cấu hình để thực hiện phương pháp được thực hiện bởi thiết bị đầu cuối:

môđun xử lý 801 được tạo cấu hình để xác định giá trị mã nhận thực bản tin MAC thứ nhất dựa trên khóa an toàn và thông tin giao diện không gian, trong đó khóa an toàn là khóa an toàn tầng không truy nhập NAS giữa thiết bị đầu cuối và thiết bị mạng lõi; và

môđun truyền thông 802 được tạo cấu hình để gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc.

Khi thiết bị này được tạo cấu hình để thực hiện phương pháp được thực hiện bởi trạm gốc:

môđun truyền thông 802 được tạo cấu hình để: thu bản tin điều khiển tài nguyên vô tuyến RRC từ thiết bị đầu cuối, trong đó bản tin RRC mang bản tin NAS, và bản tin NAS bao gồm thông tin giao diện không gian và giá trị MAC thứ nhất; và gửi bản tin NAS tới thiết bị mạng lõi; và

môđun truyền thông 802 còn được tạo cấu hình để thu kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian từ thiết bị mạng lõi.

Ngoài ra, khi thiết bị này được tạo cấu hình để thực hiện phương pháp được thực hiện bởi trạm gốc:

môđun truyền thông 802 được tạo cấu hình để: thu thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất từ thiết bị đầu cuối; và gửi thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất tới thiết bị mạng lõi; và

môđun truyền thông 802 còn được tạo cấu hình để thu kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian từ thiết bị mạng lõi.

Tùy chọn là, môđun xử lý 801 được tạo cấu hình để: trước khi trạm gốc gửi bản tin yêu cầu thứ nhất tới thiết bị mạng lõi, thì xác định rằng thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển.

Khi thiết bị này được tạo cấu hình để thực hiện phương pháp được thực hiện bởi thiết bị mạng lõi:

môđun truyền thông 802 được tạo cấu hình để thu bản tin yêu cầu thứ nhất từ trạm gốc, trong đó bản tin yêu cầu thứ nhất mang thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất;

môđun xử lý 801 được tạo cấu hình để xác nhận tính toàn vẹn của thông tin giao diện không gian dựa trên giá trị MAC thứ nhất; và

môđun truyền thông 802 còn được tạo cấu hình để gửi bản tin hồi đáp thứ nhất của yêu cầu thứ nhất tới trạm gốc, trong đó bản tin hồi đáp thứ nhất bao gồm kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian.

Môđun xử lý 801 và môđun truyền thông 802 còn có thể được tạo cấu hình để thực hiện các bước hoặc các hoạt động tương ứng khác được thực hiện bởi thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi theo các phương án phương pháp được đề cập ở trên. Các chi tiết sẽ không được mô tả lại trong phần mô tả này.

Việc phân chia thành các môđun theo các phương án của sáng chế là một ví dụ, chỉ đơn thuần là dạng phân chia chức năng lôgic, và có thể có dạng phân chia khác trong khi thực hiện thực tế. Ngoài ra, các môđun chức năng theo các phương án của sáng chế có thể được tích hợp vào trong một bộ xử lý, hoặc mỗi môđun có thể tồn tại độc lập về mặt vật lý, hoặc hai hoặc nhiều môđun có thể được tích hợp vào trong một môđun. Môđun tích hợp có thể được thực hiện dưới dạng phần cứng, hoặc có thể được thực hiện dưới dạng môđun chức năng phần mềm.

Fig.9 thể hiện thiết bị 900 theo một phương án của sáng chế. Thiết bị 900 được tạo cấu hình để thực hiện các chức năng của thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi theo các phương pháp được đề cập ở trên. Thiết bị 900 có thể là thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi, có thể là thiết bị trong thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi, hoặc có thể là thiết bị mà có thể được sử dụng cùng với thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi.

Thiết bị này có thể là hệ thống chip. Theo phương án này của sáng chế, hệ thống chip có thể bao gồm chip, hoặc có thể bao gồm chip và bộ phận rời rạc khác. Thiết bị 900 bao gồm ít nhất một bộ xử lý 920, được tạo cấu hình để thực hiện các chức năng của thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi theo các phương pháp được đề xuất theo các phương án của sáng chế. Thiết bị 900 còn có thể bao gồm giao diện truyền thông 910.

Theo phương án này của sáng chế, giao diện truyền thông có thể là bộ thu phát, mạch, bus, môđun, hoặc giao diện truyền thông có kiểu khác, và được tạo cấu hình để

truyền thông với thiết bị khác thông qua môi trường truyền dẫn. Ví dụ, giao diện truyền thông 910 được sử dụng bởi thiết bị trong thiết bị 900 để truyền thông với thiết bị khác.

Ví dụ, khi thiết bị 900 là thiết bị đầu cuối, thì thiết bị khác có thể là trạm gốc hoặc thiết bị mạng lõi. Khi thiết bị 900 là trạm gốc, thì thiết bị khác có thể là thiết bị đầu cuối hoặc thiết bị mạng lõi. Khi thiết bị 900 là thiết bị mạng lõi, thì thiết bị khác có thể là thiết bị đầu cuối hoặc trạm gốc. Bộ xử lý 920 thu và gửi dữ liệu thông qua giao diện truyền thông 910, và được tạo cấu hình để thực hiện các phương pháp theo các phương án phương pháp được đề cập ở trên.

Ví dụ, khi các chức năng của thiết bị đầu cuối được thực hiện, thì bộ xử lý 920 được tạo cấu hình để xác định giá trị mã nhận thực bản tin MAC thứ nhất dựa trên khóa an toàn và thông tin giao diện không gian, trong đó khóa an toàn là khóa an toàn tầng không truy nhập NAS giữa thiết bị đầu cuối và thiết bị mạng lõi; và giao diện truyền thông 910 được tạo cấu hình để gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc.

Khi các chức năng của trạm gốc được thực hiện, thì giao diện truyền thông 910 được tạo cấu hình để thu bản tin điều khiển tài nguyên vô tuyến RRC từ thiết bị đầu cuối, trong đó bản tin RRC mang bản tin NAS, và bản tin NAS bao gồm thông tin giao diện không gian và giá trị MAC thứ nhất; được tạo cấu hình để gửi bản tin NAS tới thiết bị mạng lõi; và còn được tạo cấu hình để thu kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian từ thiết bị mạng lõi.

Ngoài ra, khi các chức năng của trạm gốc được thực hiện, thì giao diện truyền thông 910 được tạo cấu hình để thu thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất từ thiết bị đầu cuối; và được tạo cấu hình để gửi thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất tới thiết bị mạng lõi; hoặc còn được tạo cấu hình để thu kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian từ thiết bị mạng lõi.

Khi các chức năng của thiết bị mạng lõi được thực hiện, thì giao diện truyền thông 910 được tạo cấu hình để thu bản tin yêu cầu thứ nhất từ trạm gốc, trong đó bản tin yêu cầu thứ nhất mang thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất; bộ xử lý 920 được tạo cấu hình để xác nhận tính toàn vẹn của thông tin giao diện không gian dựa trên giá trị MAC thứ nhất; và giao diện truyền thông 910 còn được tạo cấu hình để gửi bản tin hồi đáp thứ nhất của yêu cầu thứ nhất tới trạm gốc, trong đó bản tin hồi đáp thứ nhất bao gồm kết quả xác nhận tính toàn vẹn của thông tin giao diện

không gian và/hoặc thông tin giao diện không gian.

Bộ xử lý 920 và giao diện truyền thông 910 còn có thể được tạo cấu hình để thực hiện các bước hoặc các hoạt động tương ứng khác được thực hiện bởi thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi theo các phương án phương pháp được đề cập ở trên. Các chi tiết sẽ không được mô tả lại trong phần mô tả này.

Thiết bị 900 còn có thể bao gồm ít nhất một bộ nhớ 930, được tạo cấu hình để lưu các lệnh chương trình và/hoặc dữ liệu. Bộ nhớ 930 được ghép nối với bộ xử lý 920. Việc ghép nối theo phương án này của sáng chế có thể là ghép nối gián tiếp hoặc kết nối truyền thông giữa các thiết bị, đơn vị, hoặc môđun dưới dạng điện, cơ khí, hoặc dạng khác, và được sử dụng để trao đổi thông tin giữa các thiết bị, đơn vị, và môđun này. Bộ xử lý 920 có thể cùng hoạt động với bộ nhớ 930. Bộ xử lý 920 có thể thực hiện các lệnh chương trình được lưu trong bộ nhớ 930. Ít nhất một trong số ít nhất một bộ nhớ có thể được chứa trong bộ xử lý.

Phương tiện kết nối cụ thể giữa giao diện truyền thông 910, bộ xử lý 920, và bộ nhớ 930 không bị hạn chế theo phương án này của sáng chế. Theo phương án này của sáng chế, bộ nhớ 930, giao diện truyền thông 920, và bộ thu phát 910 được kết nối thông qua bus 940 trên Fig.9. Bus được thể hiện bởi đường in đậm trên Fig.9. Cách thức kết nối của các bộ phận khác chỉ đơn thuần là một ví dụ để mô tả,và không bị hạn chế ở đó. Bus có thể được phân loại thành bus địa chỉ, bus dữ liệu, bus điều khiển, và bus tương tự. Để dễ dàng thể hiện, thì chỉ một đường đậm được sử dụng để thể hiện bus trên Fig.9, nhưng không có nghĩa rằng chỉ có một bus hoặc chỉ một kiểu bus.

Theo các phương án của sáng chế, bộ xử lý có thể là bộ xử lý đa năng, bộ xử lý tín hiệu số, mạch tích hợp chuyên dụng, mảng cổng khả lập trình bằng trường hoặc thiết bị lôgic khả lập trình, cổng rời rạc hoặc thiết bị lôgic tranzito, hoặc thành phần phần cứng rời rạc khác, và có thể thực thi hoặc thực hiện các phương pháp, bước, và các sơ đồ lôgic được bộc lộ theo các phương án của sáng chế. Bộ xử lý đa năng có thể là bộ vi xử lý, bộ xử lý thông thường bất kỳ hoặc bộ xử lý tương tự. Các bước của các phương pháp được bộc lộ có dựa vào các phương án của sáng chế có thể được thực hiện trực tiếp bởi bộ xử lý phần cứng, hoặc có thể được thực hiện bằng cách sử dụng dạng kết hợp của phần cứng trong bộ xử lý và môđun phần mềm.

Theo các phương án của sáng chế, bộ nhớ có thể là bộ nhớ bất khả biến, chẳng hạn như ổ đĩa cứng (hard disk drive, HDD) hoặc bộ nhớ ở trạng thái rắn (solid-state drive,

SSD), hoặc có thể là bộ nhớ khả biến (volatile memory), chẳng hạn như bộ nhớ truy nhập ngẫu nhiên (random-access memory, RAM). Bộ nhớ là vật khác bất kỳ mà có thể mang hoặc lưu mã chương trình mong muốn dưới dạng lệnh hoặc cấu trúc dữ liệu và có thể được truy nhập bởi máy tính, nhưng không bị hạn chế ở đó. Bộ nhớ theo các phương án của sáng chế còn có thể là mạch hoặc thiết bị bất kỳ khác mà có thể thực hiện chức năng lưu trữ, và được tạo cấu hình để lưu các lệnh chương trình và/hoặc dữ liệu.

Dựa trên cùng một khái niệm kỹ thuật, như được thể hiện trên Fig.10, phương pháp bảo vệ an toàn thông tin giao diện không gian được đề xuất theo phương án này của sáng chế còn có thể được thực hiện bằng cách sử dụng các bước sau đây. Nhiều bước liên tiếp hoặc không liên tiếp bất kỳ trong các phần mô tả sau đây có thể tạo thành các giải pháp kỹ thuật sẽ được bảo hộ theo sáng chế, và các bước còn lại là các bước tùy chọn.

S1001: Thiết bị đầu cuối gửi thông tin giao diện không gian của thiết bị đầu cuối tới trạm gốc, và trạm gốc thu thông tin giao diện không gian của thiết bị đầu cuối từ thiết bị đầu cuối.

Để biết các phần giải thích của thông tin giao diện không gian, thì có thể tham khảo các phần mô tả được đề cập ở trên. Tùy chọn là, thiết bị đầu cuối còn có thể gửi giá trị băm của thông tin giao diện không gian của thiết bị đầu cuối tới trạm gốc hoặc thiết bị mạng lõi. Để phân biệt, giá trị băm được ký hiệu là giá trị băm thứ nhất ở đây. Ngoài ra, thiết bị đầu cuối còn có thể gửi giá trị xác nhận của thông tin giao diện không gian của thiết bị đầu cuối tới trạm gốc hoặc thiết bị mạng lõi. Để phân biệt, giá trị xác nhận được ký hiệu là giá trị xác nhận thứ nhất ở đây.

S1002: Trạm gốc gửi bản tin yêu cầu tới thiết bị mạng lõi, và thiết bị mạng lõi thu bản tin yêu cầu từ trạm gốc.

Bản tin yêu cầu được ký hiệu là bản tin yêu cầu thứ nhất, và bản tin yêu cầu thứ nhất có thể được sử dụng để yêu cầu để xác nhận thông tin giao diện không gian của thiết bị đầu cuối, hoặc bản tin yêu cầu thứ nhất có thể được sử dụng để yêu cầu thông số liên quan để xác nhận thông tin giao diện không gian của thiết bị đầu cuối.

Nếu trạm gốc thu giá trị băm thứ nhất hoặc giá trị xác nhận thứ nhất của thông tin giao diện không gian của thiết bị đầu cuối từ thiết bị đầu cuối ở bước S1001, thì trạm gốc còn có thể gửi giá trị băm thứ nhất hoặc giá trị xác nhận thứ nhất của thông tin giao diện không gian của thiết bị đầu cuối tới thiết bị mạng lõi. Thiết bị mạng lõi thu giá trị băm thứ nhất hoặc giá trị xác nhận thứ nhất từ trạm gốc.

Theo phương án này của sáng chế, an toàn NAS được thiết đặt trước giữa thiết bị đầu cuối và mạng lõi.

Sau khi thu bản tin yêu cầu từ trạm gốc, thì thiết bị mạng lõi có thể xác nhận thông tin giao diện không gian của thiết bị đầu cuối theo một số cách thức hoạt động tùy chọn. Các chi tiết như sau.

Nếu thiết bị mạng lõi không nhận giá trị băm thứ nhất hoặc giá trị xác nhận thứ nhất của thông tin giao diện không gian của thiết bị đầu cuối, thì bước S1003 và S1004 được thực hiện.

Nếu thiết bị mạng lõi đã nhận giá trị băm thứ nhất hoặc giá trị xác nhận thứ nhất của thông tin giao diện không gian của thiết bị đầu cuối, thì bước S1003 và S1004 được bỏ qua, và các bước tiếp theo được thực hiện.

S1003: Thiết bị mạng lõi gửi bản tin yêu cầu tới thiết bị đầu cuối, trong đó bản tin yêu cầu được ký hiệu là bản tin yêu cầu thứ hai ở đây để phân biệt với bản tin yêu cầu ở bước S1002. Thiết bị đầu cuối thu bản tin yêu cầu thứ hai từ thiết bị mạng lõi.

Bản tin yêu cầu thứ hai được sử dụng để yêu cầu giá trị băm thứ nhất hoặc giá trị xác nhận thứ nhất của thông tin giao diện không gian của thiết bị đầu cuối.

S1004: Thiết bị đầu cuối trả về giá trị băm thứ nhất hoặc giá trị xác nhận thứ nhất của thông tin giao diện không gian của thiết bị đầu cuối cho thiết bị mạng lõi, và thiết bị mạng lõi thu giá trị băm thứ nhất hoặc giá trị xác nhận thứ nhất của thông tin giao diện không gian của thiết bị đầu cuối từ thiết bị đầu cuối.

S1005: Thiết bị mạng lõi xác nhận thông tin giao diện không gian của thiết bị đầu cuối để nhận kết quả xác nhận.

Cụ thể là, thiết bị mạng lõi có thể tính giá trị băm thứ hai dựa trên thông tin giao diện không gian của thiết bị đầu cuối, và so sánh giá trị băm thứ hai với giá trị băm thứ nhất. Nếu giá trị băm thứ hai giống với giá trị băm thứ nhất, thì chỉ báo rằng thông tin giao diện không gian của thiết bị đầu cuối không bị giả mạo; ngược lại, thì chỉ báo rằng thông tin giao diện không gian của thiết bị đầu cuối có thể bị giả mạo.

Ngoài ra, thiết bị mạng lõi có thể tính giá trị xác nhận thứ hai dựa trên thông tin giao diện không gian của thiết bị đầu cuối, và so sánh giá trị xác nhận thứ hai với giá trị xác nhận thứ nhất. Nếu giá trị xác nhận thứ hai giống với giá trị xác nhận thứ nhất, thì chỉ báo rằng thông tin giao diện không gian của thiết bị đầu cuối không bị giả mạo; ngược lại, thì chỉ báo rằng thông tin giao diện không gian của thiết bị đầu cuối có thể bị giả mạo.

S1006: Thiết bị mạng lõi gửi kết quả xác nhận tới trạm gốc, và trạm gốc thu kết quả xác nhận từ thiết bị mạng lõi.

S1007: Trạm gốc xác định, dựa trên kết quả xác nhận, việc thông tin giao diện không gian của thiết bị đầu cuối có tin cậy hay không.

Nếu kết quả xác nhận là việc xác nhận thành công (ví dụ, giá trị băm thứ nhất giống với giá trị băm thứ hai, hoặc giá trị xác nhận thứ nhất giống với giá trị xác nhận thứ hai), thì trạm gốc xác định rằng thông tin giao diện không gian của thiết bị đầu cuối không bị giả mạo. Nếu kết quả xác nhận là việc xác nhận không thành công (ví dụ, giá trị băm thứ nhất không giống với giá trị băm thứ hai, hoặc giá trị xác nhận thứ nhất không giống với giá trị xác nhận thứ hai), thì trạm gốc xác định rằng thông tin giao diện không gian của thiết bị đầu cuối có thể bị giả mạo, rằng thông tin giao diện không gian có nguy cơ, và không sử dụng thông tin giao diện không gian.

Tùy chọn là, theo một dạng thực hiện có thể, nếu bản tin yêu cầu thứ nhất ở bước S1002 được sử dụng để yêu cầu thông số liên quan để xác nhận thông tin giao diện không gian của thiết bị đầu cuối, thì các bước sau đây được thực hiện.

S1003*: Thiết bị mạng lõi gửi, tới trạm gốc, thông số liên quan để xác nhận thông tin giao diện không gian của thiết bị đầu cuối, và trạm gốc thu thông số này từ thiết bị mạng lõi.

S1004*: Trạm gốc xác định việc thông tin giao diện không gian của thiết bị đầu cuối có tin cậy hay không.

Thông số liên quan để xác nhận thông tin giao diện không gian của thiết bị đầu cuối có thể là giá trị băm thứ nhất của thông tin giao diện không gian của thiết bị đầu cuối. Trạm gốc có thể tính giá trị băm thứ hai dựa trên thông tin giao diện không gian của thiết bị đầu cuối, và so sánh giá trị băm thứ hai với giá trị băm thứ nhất. Nếu giá trị băm thứ hai giống với giá trị băm thứ nhất, thì chỉ báo rằng thông tin giao diện không gian của thiết bị đầu cuối không bị giả mạo; ngược lại, thì chỉ báo rằng thông tin giao diện không gian của thiết bị đầu cuối có thể bị giả mạo.

Ngoài ra, thông số liên quan để xác nhận thông tin giao diện không gian của thiết bị đầu cuối có thể là giá trị xác nhận thứ nhất của thông tin giao diện không gian của thiết bị đầu cuối. Trạm gốc có thể tính giá trị xác nhận thứ hai dựa trên thông tin giao diện không gian của thiết bị đầu cuối, và so sánh giá trị xác nhận thứ hai với giá trị xác nhận thứ nhất. Nếu giá trị xác nhận thứ hai giống với giá trị xác nhận thứ nhất, thì chỉ báo rằng thông tin

giao diện không gian của thiết bị đầu cuối không bị giả mạo; ngược lại, thì chỉ báo rằng thông tin giao diện không gian của thiết bị đầu cuối có thể bị giả mạo.

Vì không có an toàn AS được thiết đặt giữa thiết bị đầu cuối và trạm gốc, nên an toàn của thông tin giao diện không gian của thiết bị đầu cuối có thể được đảm bảo bằng cách yêu cầu thiết bị mạng lõi xác nhận thông tin giao diện không gian của thiết bị đầu cuối.

Phương án được thể hiện trên Fig.10 có thể được thực hiện thông qua thiết bị được thể hiện trên Fig.8 hoặc Fig.9.

Theo các phương pháp được đề xuất theo các phương án được đề cập ở trên của sáng chế, một số hoặc tất cả các hoạt động và các chức năng được mô tả được thực hiện bởi thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi có thể được thực hiện bằng cách sử dụng chip hoặc mạch tích hợp.

Để thực hiện các chức năng của thiết bị trên Fig.8 hoặc Fig.9, một phương án của sáng chế còn đề xuất chip. Chip này bao gồm bộ xử lý, được tạo cấu hình để hỗ trợ thiết bị thực hiện các chức năng liên quan đến thiết bị đầu cuối, trạm gốc, hoặc thiết bị mạng lõi theo các phương án phương pháp được đề cập ở trên. Theo một phương án có thể, chip này được kết nối với bộ nhớ hoặc chip này bao gồm bộ nhớ, và bộ nhớ được tạo cấu hình để lưu các lệnh chương trình và dữ liệu cần thiết đối với thiết bị.

Một phương án của sáng chế đề xuất vật ghi có thể đọc được bằng máy tính. Vật ghi có thể đọc được bằng máy tính lưu chương trình máy tính, và chương trình máy tính bao gồm các lệnh được sử dụng để thực hiện các phương án phương pháp được đề xuất theo các phương án được đề cập ở trên.

Một phương án của sáng chế còn đề xuất sản phẩm chương trình máy tính bao gồm các lệnh. Khi sản phẩm chương trình máy tính chạy trên máy tính, thì máy tính này được cho phép thực hiện các phương án phương pháp được đề xuất theo các phương án được đề cập ở trên.

Người có hiểu biết trung bình về lĩnh vực kỹ thuật này phải hiểu rằng các phương án của sáng chế có thể được thực hiện như phương pháp, hệ thống, hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể sử dụng dưới dạng các phương án chỉ gồm phần cứng, các phương án chỉ gồm phần mềm, hoặc các phương án với dạng kết hợp phần mềm và phần cứng. Ngoài ra, sáng chế có thể sử dụng dưới dạng sản phẩm chương trình máy tính mà được thực hiện trên một hoặc nhiều vật ghi có thể sử dụng được trên máy

tính (bao gồm nhưng không hạn chế đĩa nhớ, đĩa CDROM, và bộ nhớ quang, và bộ nhớ tương tự) mà bao gồm mã chương trình có thể sử dụng được trên máy tính.

Sáng chế được mô tả có dựa vào các lưu đồ và/hoặc các sơ đồ khối của phương pháp, thiết bị (hệ thống), và sản phẩm chương trình máy tính theo các phương án của sáng chế. Phải hiểu rằng các lệnh chương trình máy tính có thể được sử dụng để thực hiện mỗi quy trình và/hoặc mỗi khối trong các lưu đồ và/hoặc các sơ đồ khối và dạng kết hợp của quy trình và/hoặc khối trong các lưu đồ và/hoặc các sơ đồ khối. Các lệnh chương trình máy tính này có thể được cung cấp cho máy tính đa năng, máy tính chuyên dụng, bộ xử lý nhúng, hoặc bộ xử lý của thiết bị xử lý dữ liệu khả lập trình khác để tạo ra máy, sao cho các lệnh này được thực hiện bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu khả lập trình khác tạo ra máy để thực hiện chức năng cụ thể theo một hoặc nhiều quy trình theo các lưu đồ và/hoặc theo một hoặc nhiều các khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể được lưu trong bộ nhớ có thể đọc được bằng máy tính mà có thể chỉ thị máy tính hoặc thiết bị xử lý dữ liệu khả lập trình khác làm việc theo cách thức cụ thể, sao cho các lệnh này được lưu trong bộ nhớ có thể đọc được bằng máy tính tạo ra vật nhân tạo mà bao gồm thiết bị chỉ huy. Thiết bị chỉ huy thực hiện chức năng cụ thể theo một hoặc nhiều quy trình theo các lưu đồ và/hoặc theo một hoặc nhiều các khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể được nạp vào trong máy tính hoặc thiết bị xử lý dữ liệu khả lập trình khác, sao cho một loạt các hoạt động và bước được thực hiện trên máy tính hoặc thiết bị khả lập trình khác này để tạo ra hoạt động xử lý được thực hiện bởi máy tính. Do đó, các lệnh được thực hiện trên máy tính hoặc thiết bị khả lập trình khác thực hiện các bước để thực hiện chức năng cụ thể trong một hoặc nhiều quy trình theo các lưu đồ và/hoặc theo một hoặc nhiều các khối trong các sơ đồ khối.

Mặc dù một số phương án của sáng chế đã được mô tả, nhưng người có hiểu biết trung bình về lĩnh vực kỹ thuật này có thể thực hiện phương án thay đổi và cải biến với các phương án được mô tả này khi người có hiểu biết trung bình về lĩnh vực kỹ thuật này hiểu khái niệm sáng chế cơ sở. Do đó, các điểm yêu cầu bảo hộ sau đây được hiểu là bao gồm các phương án được bộc lộ và tất cả các phương án thay đổi và cải biến thuộc phạm vi của sáng chế.

Rõ ràng là, người có hiểu biết trung bình về lĩnh vực kỹ thuật này có thể thực hiện các phương án cải biến và phương án thay đổi với các phương án của sáng chế mà vẫn

không nằm ngoài phạm vi của các phương án của sáng chế. Trong trường hợp này, sáng chế được hiểu là bao gồm các phương án cải biến và thay đổi này miễn là các phương án như vậy đều nằm trong phạm vi bảo hộ được xác định bởi các điểm yêu cầu bảo hộ sau đây và các phương án tương đương của chúng.

Yêu cầu bảo hộ

1. Phương pháp bảo vệ an toàn thông tin giao diện không gian bao gồm các bước:

xác định, bởi thiết bị đầu cuối, giá trị mã nhận thực bản tin (message authentication code, MAC) thứ nhất dựa trên khóa an toàn và thông tin giao diện không gian, trong đó khóa an toàn là khóa an toàn tầng không truy nhập (non-access stratum, NAS) giữa thiết bị đầu cuối và thiết bị mạng lõi; và

gửi, bởi thiết bị đầu cuối, thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc; hoặc gửi, bởi thiết bị đầu cuối, thông tin giao diện không gian và giá trị MAC thứ nhất tới thiết bị mạng lõi.

2. Phương pháp theo điểm 1, trong đó thiết bị mạng lõi bao gồm thực thể quản lý di động (mobility management entity, MME) hoặc chức năng quản lý truy nhập và di động (access and mobility management function, AMF); và

khóa an toàn là một khóa bất kỳ trong số các khóa sau đây hoặc là khóa nhận được thông qua việc suy diễn dựa trên một khóa bất kỳ trong số các khóa sau đây: khóa Kasme giữa thiết bị đầu cuối và MME, khóa Kamf giữa thiết bị đầu cuối và AMF, khóa bảo vệ tính toàn vẹn NAS giữa thiết bị đầu cuối và thiết bị mạng lõi, hoặc khóa bảo vệ tính bí mật NAS giữa thiết bị đầu cuối và thiết bị mạng lõi.

3. Phương pháp theo điểm 1 hoặc điểm 2, trong đó bước xác định, bởi thiết bị đầu cuối, giá trị mã nhận thực bản tin MAC thứ nhất dựa trên khóa an toàn và thông tin giao diện không gian bao gồm bước:

xác định, bởi thiết bị đầu cuối, giá trị MAC thứ nhất dựa trên khóa an toàn, thông tin giao diện không gian, và thông số nhập, trong đó

thông số nhập bao gồm thông số tươi và/hoặc bộ nhận dạng tế bào, và thông số tươi bao gồm một hoặc nhiều thông số bất kỳ trong số các thông số sau đây: một phần hoặc tất cả các bit để đếm NAS count đường lên, một phần hoặc tất cả các bit để đếm NAS count đường xuống, hoặc số ngẫu nhiên.

4. Phương pháp theo điểm bất kỳ trong số các điểm từ điểm 1 đến 3, trong đó bước gửi, bởi thiết bị đầu cuối, thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc bao gồm các bước:

gửi, bởi thiết bị đầu cuối, bản tin điều khiển tài nguyên vô tuyến (radio resource control, RRC) thứ nhất tới trạm gốc, trong đó bản tin RRC thứ nhất mang thông tin giao

diện không gian và giá trị MAC thứ nhất; hoặc

gửi, bởi thiết bị đầu cuối, bản tin RRC thứ hai tới trạm gốc, trong đó bản tin RRC thứ hai mang bản tin NAS, và bản tin NAS bao gồm thông tin giao diện không gian và giá trị MAC thứ nhất.

5. Phương pháp theo điểm bất kỳ trong số các điểm từ điểm 1 đến 4, trong đó phương pháp này còn bao gồm các bước:

thu, bởi thiết bị đầu cuối, bản tin yêu cầu từ trạm gốc, trong đó bản tin yêu cầu mang giá trị MAC thứ hai, và bản tin yêu cầu được sử dụng để yêu cầu thông tin giao diện không gian; và

xác nhận, bởi thiết bị đầu cuối, giá trị MAC thứ hai.

6. Phương pháp theo điểm bất kỳ trong số các điểm từ điểm 1 đến 5, trong đó thông tin giao diện không gian là khả năng vô tuyến hoặc bộ nhận dạng khả năng vô tuyến.

7. Phương pháp bảo vệ an toàn thông tin giao diện không gian bao gồm các bước:

thu, bởi trạm gốc, bản tin điều khiển tài nguyên vô tuyến RRC từ thiết bị đầu cuối, trong đó bản tin RRC mang bản tin NAS, và bản tin NAS bao gồm thông tin giao diện không gian và giá trị MAC thứ nhất;

gửi, bởi trạm gốc, bản tin NAS tới thiết bị mạng lõi; và

thu, bởi trạm gốc, kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian từ thiết bị mạng lõi.

8. Phương pháp bảo vệ an toàn thông tin giao diện không gian bao gồm các bước:

thu, bởi trạm gốc, thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất từ thiết bị đầu cuối;

gửi, bởi trạm gốc, thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất tới thiết bị mạng lõi; và

thu, bởi trạm gốc, kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian từ thiết bị mạng lõi.

9. Phương pháp theo điểm 7 hoặc điểm 8, trong đó phương pháp này còn bao gồm các bước:

gửi, bởi trạm gốc, bản tin yêu cầu thứ nhất tới thiết bị mạng lõi;

thu, bởi trạm gốc, bản tin hồi đáp thứ hai của bản tin yêu cầu thứ nhất từ thiết bị mạng lõi, trong đó bản tin hồi đáp thứ hai mang giá trị MAC thứ hai; và

gửi, bởi trạm gốc, bản tin yêu cầu thứ hai tới thiết bị đầu cuối, trong đó bản tin yêu

cầu thứ hai được sử dụng để yêu cầu thông tin giao diện không gian, và bản tin yêu cầu thứ hai mang giá trị MAC thứ hai.

10. Phương pháp theo điểm 9, trong đó trước bước gửi, bởi trạm gốc, bản tin yêu cầu thứ nhất tới thiết bị mạng lõi, thì phương pháp này còn bao gồm bước:

xác định, bởi trạm gốc, rằng thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển.

11. Phương pháp bảo vệ an toàn thông tin giao diện không gian bao gồm các bước:

thu, bởi thiết bị mạng lõi, bản tin yêu cầu thứ nhất từ trạm gốc, trong đó bản tin yêu cầu thứ nhất mang thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất;

xác nhận, bởi thiết bị mạng lõi, tính toàn vẹn của thông tin giao diện không gian dựa trên giá trị MAC thứ nhất; và

gửi, bởi thiết bị mạng lõi, bản tin hồi đáp thứ nhất của yêu cầu thứ nhất tới trạm gốc, trong đó bản tin hồi đáp thứ nhất bao gồm kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian.

12. Phương pháp theo điểm 11, trong đó phương pháp này còn bao gồm các bước:

thu, bởi thiết bị mạng lõi, bản tin yêu cầu thứ hai từ trạm gốc;

xác định, bởi thiết bị mạng lõi, giá trị MAC thứ hai dựa trên khóa an toàn; và

gửi, bởi thiết bị mạng lõi, bản tin hồi đáp thứ hai của bản tin yêu cầu thứ hai tới trạm gốc, trong đó bản tin hồi đáp thứ hai mang giá trị MAC thứ hai.

13. Phương pháp theo điểm 12, trong đó khóa an toàn bao gồm một khóa bất kỳ trong số các khóa sau đây hoặc là khóa nhận được thông qua việc suy diễn dựa trên một khóa bất kỳ trong số các khóa sau đây: khóa được chia sẻ giữa thiết bị đầu cuối và thiết bị mạng lõi, khóa bảo vệ tính toàn vẹn giữa thiết bị đầu cuối và thiết bị mạng lõi, hoặc khóa bảo vệ tính bí mật giữa thiết bị đầu cuối và thiết bị mạng lõi.

14. Phương pháp theo điểm 12 hoặc điểm 13, trong đó bước xác định, bởi thiết bị mạng lõi, giá trị MAC thứ hai dựa trên khóa an toàn bao gồm bước:

xác định, bởi thiết bị mạng lõi, giá trị MAC thứ hai dựa trên khóa an toàn, thông số nhập, và thông tin giao diện không gian, trong đó

thông số nhập bao gồm thông số tươi và/hoặc bộ nhận dạng tế bào, và thông số tươi bao gồm một hoặc nhiều thông số bất kỳ trong số các thông số sau đây: một phần hoặc tất cả các bit để đếm NAS count đường lên, một phần hoặc tất cả các bit để đếm NAS count

đường xuống, hoặc số ngẫu nhiên.

15. Thiết bị bảo vệ an toàn thông tin giao diện không gian, trong đó thiết bị này là thiết bị đầu cuối hoặc được sử dụng trong thiết bị đầu cuối, và bao gồm:

môđun xử lý, được tạo cấu hình để xác định giá trị mã nhận thực bản tin MAC thứ nhất dựa trên khóa an toàn và thông tin giao diện không gian, trong đó khóa an toàn là khóa an toàn tầng không truy nhập NAS giữa thiết bị đầu cuối và thiết bị mạng lõi; và

môđun truyền thông, được tạo cấu hình để gửi thông tin giao diện không gian và giá trị MAC thứ nhất tới trạm gốc.

16. Thiết bị theo điểm 15, trong đó thiết bị mạng lõi bao gồm thực thể quản lý di động MME hoặc chức năng quản lý truy nhập và di động AMF; và

khóa an toàn là một khóa bất kỳ trong số các khóa sau đây hoặc là khóa nhận được thông qua việc suy diễn dựa trên một khóa bất kỳ trong số các khóa sau đây: khóa Kasme giữa thiết bị đầu cuối và MME, khóa Kamf giữa thiết bị đầu cuối và AMF, khóa bảo vệ tính toàn vẹn NAS giữa thiết bị đầu cuối và thiết bị mạng lõi, hoặc khóa bảo vệ tính bí mật NAS giữa thiết bị đầu cuối và thiết bị mạng lõi.

17. Thiết bị theo điểm 15 hoặc điểm 16, trong đó môđun xử lý được tạo cấu hình để:

xác định giá trị MAC thứ nhất dựa trên khóa an toàn, thông tin giao diện không gian, và thông số nhập, trong đó

thông số nhập bao gồm thông số tươi và/hoặc bộ nhận dạng tế bào, và thông số tươi bao gồm một hoặc nhiều thông số bất kỳ trong số các thông số sau đây: một phần hoặc tất cả các bit để đếm NAS count đường lên, một phần hoặc tất cả các bit để đếm NAS count đường xuống, hoặc số ngẫu nhiên.

18. Thiết bị theo điểm bất kỳ trong số các điểm từ điểm 15 đến 17, trong đó môđun truyền thông được tạo cấu hình để:

gửi bản tin điều khiển tài nguyên vô tuyến RRC thứ nhất tới trạm gốc, trong đó bản tin RRC thứ nhất mang thông tin giao diện không gian và giá trị MAC thứ nhất; hoặc

gửi bản tin RRC thứ hai tới trạm gốc, trong đó bản tin RRC thứ hai mang bản tin NAS, và bản tin NAS bao gồm thông tin giao diện không gian và giá trị MAC thứ nhất.

19. Thiết bị theo điểm bất kỳ trong số các điểm từ điểm 15 đến 18, trong đó môđun truyền thông còn được tạo cấu hình để:

thu bản tin yêu cầu từ trạm gốc, trong đó bản tin yêu cầu mang giá trị MAC thứ hai, và bản tin yêu cầu được sử dụng để yêu cầu thông tin giao diện không gian; và

môđun xử lý còn được tạo cấu hình để xác nhận giá trị MAC thứ hai.

20. Thiết bị theo điểm bất kỳ trong số các điểm từ điểm 15 đến 19, trong đó thông tin giao diện không gian là khả năng vô tuyến hoặc bộ nhận dạng khả năng vô tuyến.

21. Thiết bị bảo vệ an toàn thông tin giao diện không gian bao gồm:

môđun truyền thông, được tạo cấu hình để: thu bản tin điều khiển tài nguyên vô tuyến RRC từ thiết bị đầu cuối, trong đó bản tin RRC mang bản tin NAS, và bản tin NAS bao gồm thông tin giao diện không gian và giá trị MAC thứ nhất; và gửi bản tin NAS tới thiết bị mạng lõi, trong đó

môđun truyền thông còn được tạo cấu hình để thu kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian từ thiết bị mạng lõi.

22. Thiết bị bảo vệ an toàn thông tin giao diện không gian bao gồm:

môđun truyền thông, được tạo cấu hình để: thu thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất từ thiết bị đầu cuối; và gửi thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất tới thiết bị mạng lõi, trong đó

môđun truyền thông còn được tạo cấu hình để thu kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian từ thiết bị mạng lõi.

23. Thiết bị theo điểm 21 hoặc điểm 22, trong đó môđun truyền thông còn được tạo cấu hình để:

gửi bản tin yêu cầu thứ nhất tới thiết bị mạng lõi;

thu bản tin hồi đáp thứ hai của bản tin yêu cầu thứ nhất từ thiết bị mạng lõi, trong đó bản tin hồi đáp thứ hai mang giá trị MAC thứ hai; và

gửi bản tin yêu cầu thứ hai tới thiết bị đầu cuối, trong đó bản tin yêu cầu thứ hai được sử dụng để yêu cầu thông tin giao diện không gian, và bản tin yêu cầu thứ hai mang giá trị MAC thứ hai.

24. Thiết bị theo điểm 23, trong đó thiết bị này còn bao gồm môđun xử lý, được tạo cấu hình để: trước khi môđun truyền thông gửi bản tin yêu cầu thứ nhất tới thiết bị mạng lõi, thì xác định rằng thiết bị đầu cuối là thiết bị đầu cuối tối ưu hệ thống vạn vật kết nối internet tế bào mặt phẳng điều khiển.

25. Thiết bị bảo vệ an toàn thông tin giao diện không gian, trong đó thiết bị này là thiết bị mạng lõi hoặc được sử dụng trong thiết bị mạng lõi, và bao gồm:

môđun truyền thông, được tạo cấu hình để thu bản tin yêu cầu thứ nhất từ trạm gốc,

trong đó bản tin yêu cầu thứ nhất mang thông tin giao diện không gian và giá trị mã nhận thực bản tin MAC thứ nhất; và

môđun xử lý, được tạo cấu hình để xác nhận tính toàn vẹn của thông tin giao diện không gian dựa trên giá trị MAC thứ nhất, trong đó

môđun truyền thông còn được tạo cấu hình để gửi bản tin hồi đáp thứ nhất của yêu cầu thứ nhất tới trạm gốc, trong đó bản tin hồi đáp thứ nhất bao gồm kết quả xác nhận tính toàn vẹn của thông tin giao diện không gian và/hoặc thông tin giao diện không gian.

26. Thiết bị theo điểm 25, trong đó môđun truyền thông còn được tạo cấu hình để thu bản tin yêu cầu thứ hai từ trạm gốc;

môđun xử lý còn được tạo cấu hình để xác định giá trị MAC thứ hai dựa trên khóa an toàn; và

môđun truyền thông còn được tạo cấu hình để gửi bản tin hồi đáp thứ hai của bản tin yêu cầu thứ hai tới trạm gốc, trong đó bản tin hồi đáp thứ hai mang giá trị MAC thứ hai.

27. Thiết bị theo điểm 26, trong đó khóa an toàn bao gồm một khóa bất kỳ trong số các khóa sau đây hoặc là khóa nhận được thông qua việc suy diễn dựa trên một khóa bất kỳ trong số các khóa sau đây: khóa được chia sẻ giữa thiết bị đầu cuối và thiết bị mạng lõi, khóa bảo vệ tính toàn vẹn giữa thiết bị đầu cuối và thiết bị mạng lõi, hoặc khóa bảo vệ tính bí mật giữa thiết bị đầu cuối và thiết bị mạng lõi.

28. Thiết bị theo điểm 26 hoặc điểm 27, trong đó môđun xử lý được tạo cấu hình để:

xác định giá trị MAC thứ hai dựa trên khóa an toàn, thông số nhập, và thông tin giao diện không gian, trong đó

thông số nhập bao gồm thông số tươi và/hoặc bộ nhận dạng tế bào, và thông số tươi bao gồm một hoặc nhiều thông số bất kỳ trong số các thông số sau đây: một phần hoặc tất cả các bit để đếm NAS count đường lên, một phần hoặc tất cả các bit để đếm NAS count đường xuống, hoặc số ngẫu nhiên.

29. Hệ thống truyền thông, bao gồm ít nhất hai thiết bị trong số thiết bị đầu cuối, trạm gốc, và thiết bị mạng lõi, trong đó

thiết bị đầu cuối được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ điểm 1 đến 6;

trạm gốc được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ điểm 7 đến 10; và

thiết bị mạng lõi được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong

số các điểm từ điểm 11 đến 14.

30. Vật ghi có thể đọc được bằng máy tính, trong đó vật ghi có thể đọc được bằng máy tính này lưu các lệnh có thể đọc được bằng máy tính; và khi các lệnh có thể đọc được bằng máy tính này được chạy trên máy tính, thì máy tính được cho phép thực hiện phương pháp thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ điểm 1 đến 14.

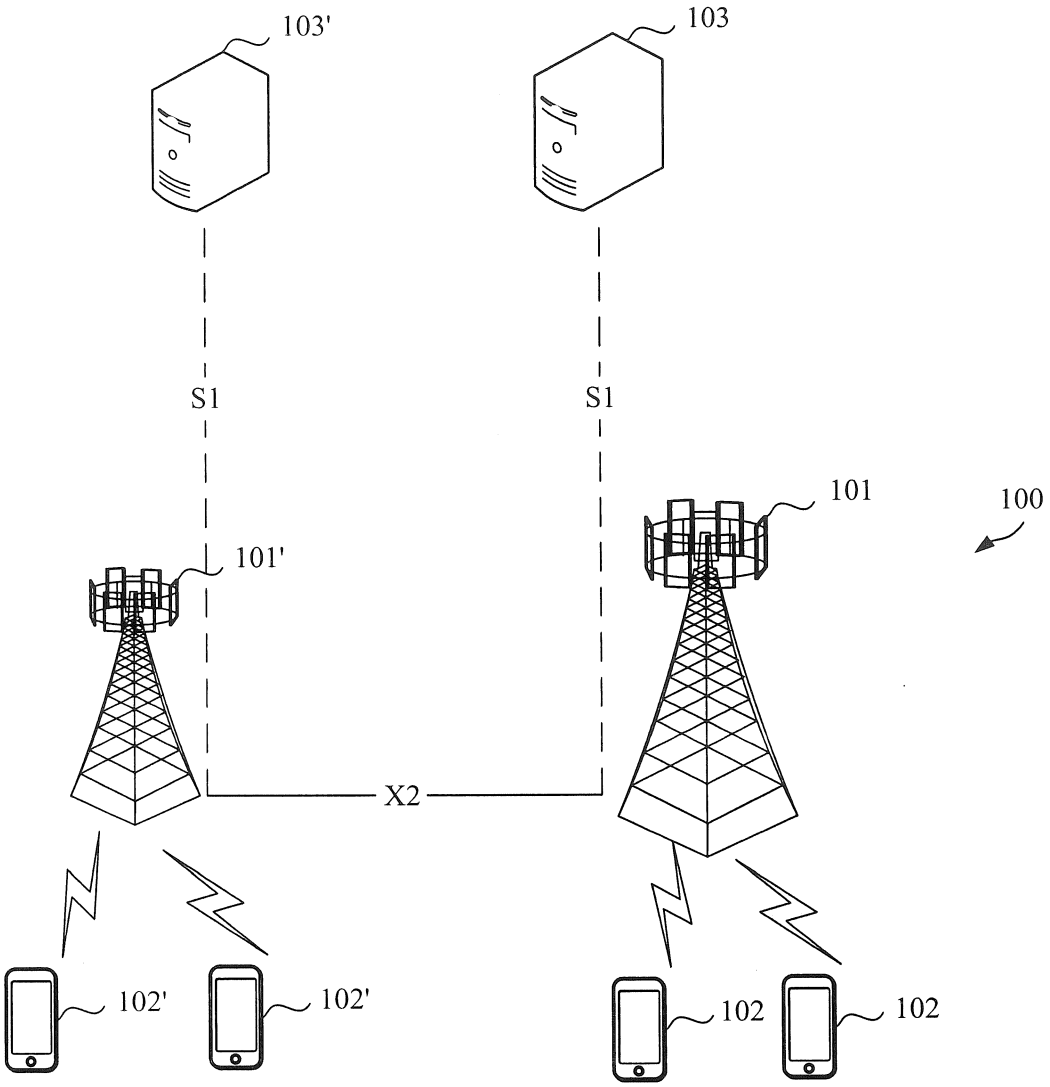

Fig.1

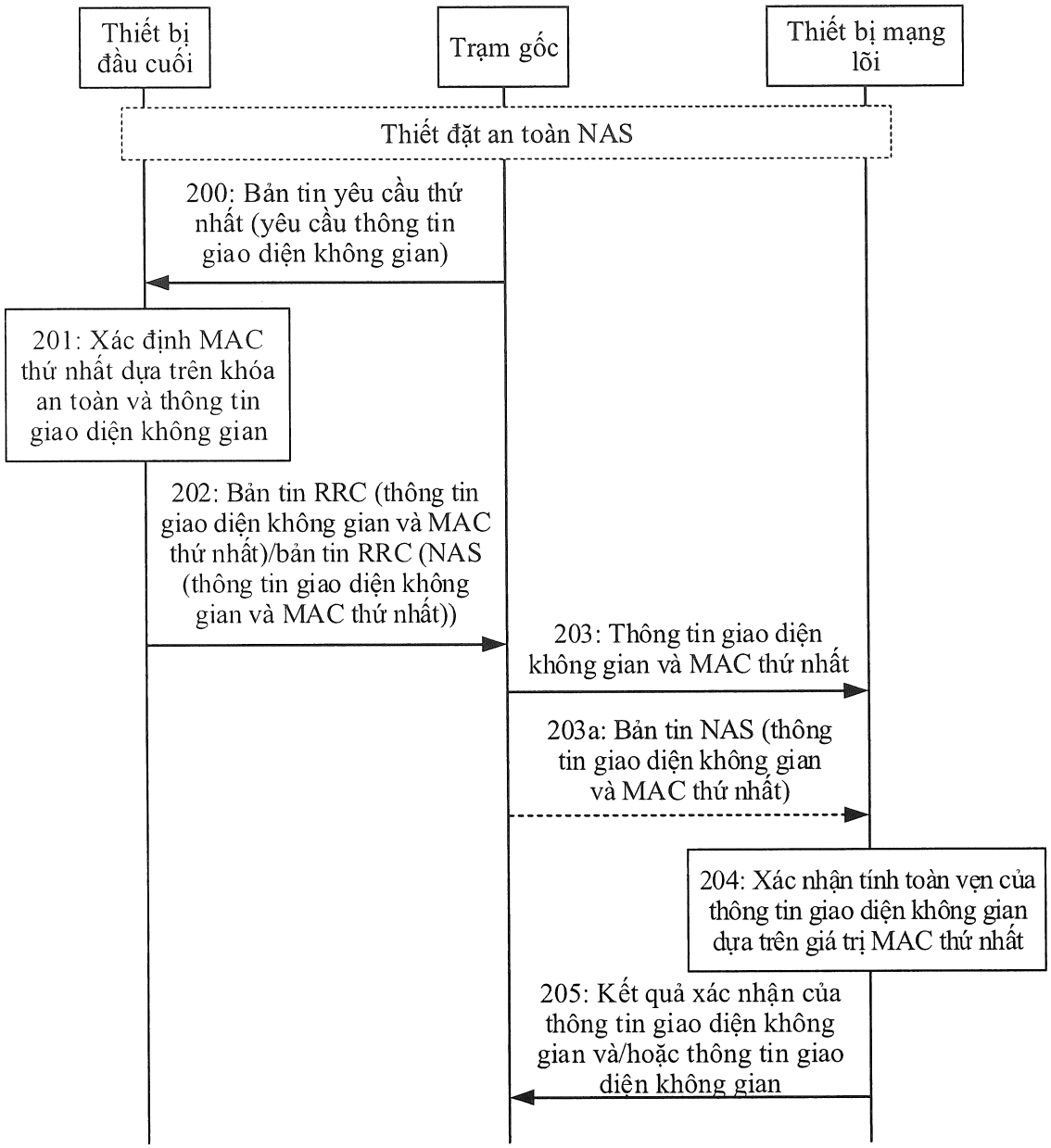
Thiết bị đầu cuối
Trạm gốc
Thiết bị mạng lõi
Thiết đặt an toàn NAS
200: Bản tin yêu cầu thứ nhất (yêu cầu thông tin giao diện không gian)
201: Xác định MAC thứ nhất dựa trên khóa an toàn và thông tin giao diện không gian
202: Bản tin RRC (thông tin giao diện không gian và MAC thứ nhất)/bản tin RRC (NAS (thông tin giao diện không gian và MAC thứ nhất))
203: Thông tin giao diện không gian và MAC thứ nhất
203a: Bản tin NAS (thông tin giao diện không gian và MAC thứ nhất)
204: Xác nhận tính toàn vẹn của thông tin giao diện không gian dựa trên giá trị MAC thứ nhất
205: Kết quả xác nhận của thông tin giao diện không gian và/hoặc thông tin giao diện không gian

Fig.2

3/8

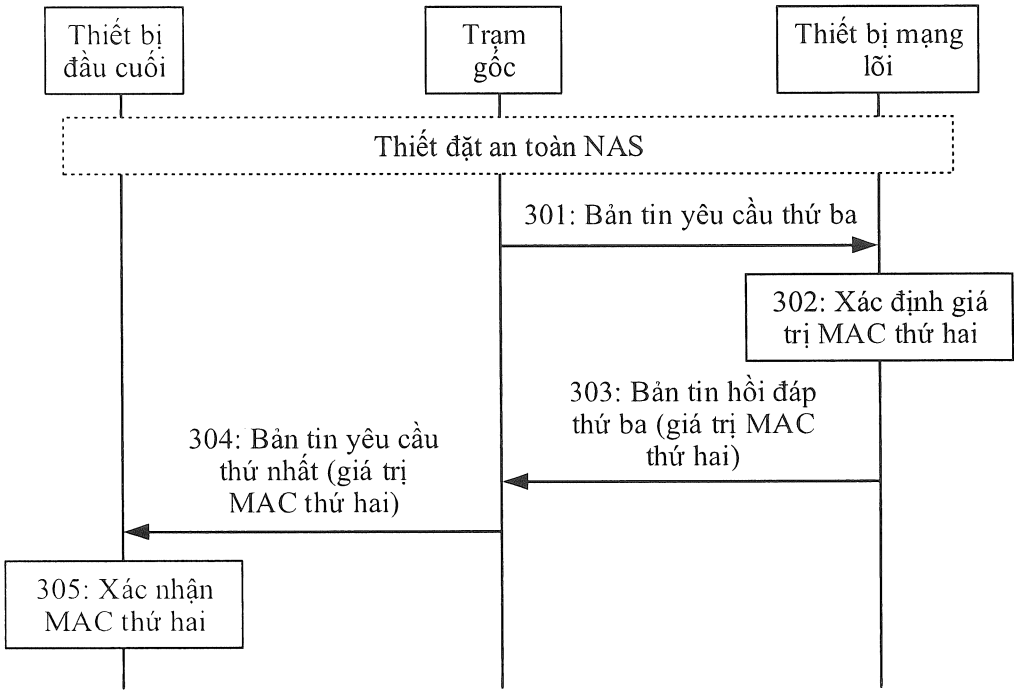
Thiết bị đầu cuối
Trạm gốc
Thiết bị mạng lõi
Thiết đặt an toàn NAS
301: Bản tin yêu cầu thứ ba
302: Xác định giá trị MAC thứ hai
303: Bản tin hồi đáp thứ ba (giá trị MAC thứ hai)
304: Bản tin yêu cầu thứ nhất (giá trị MAC thứ hai)
305: Xác nhận MAC thứ hai

Fig.3

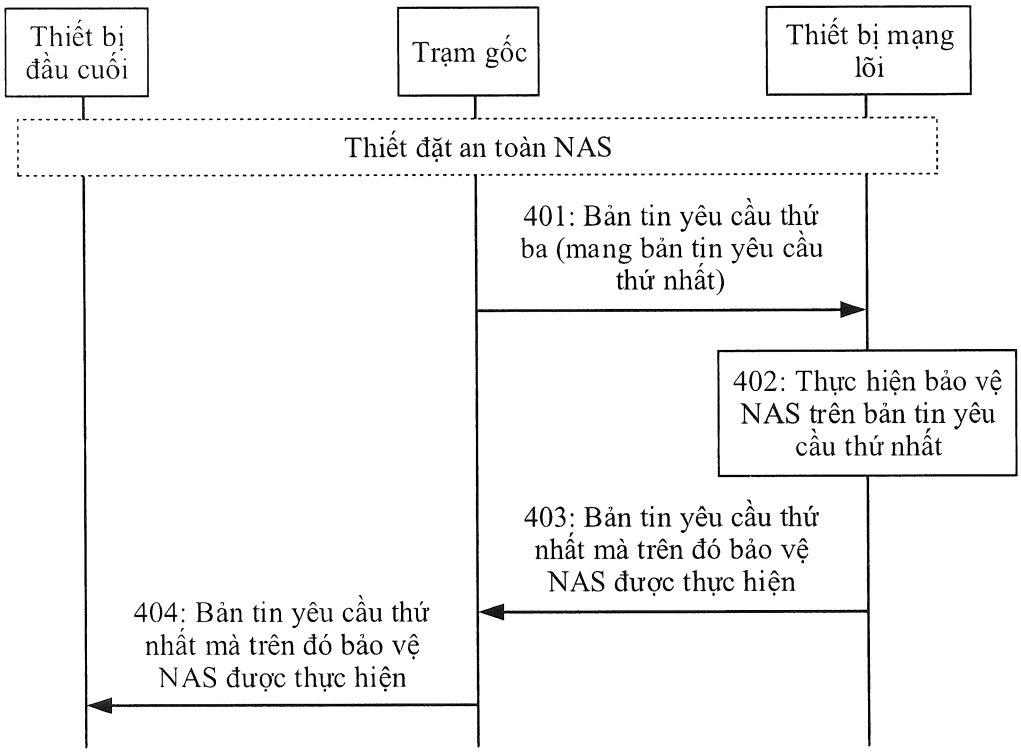
Thiết bị đầu cuối
Trạm gốc
Thiết bị mạng lõi
Thiết đặt an toàn NAS
401: Bản tin yêu cầu thứ ba (mang bản tin yêu cầu thứ nhất)
402: Thực hiện bảo vệ NAS trên bản tin yêu cầu thứ nhất
403: Bản tin yêu cầu thứ nhất mà trên đó bảo vệ NAS được thực hiện
404: Bản tin yêu cầu thứ nhất mà trên đó bảo vệ NAS được thực hiện

Fig.4

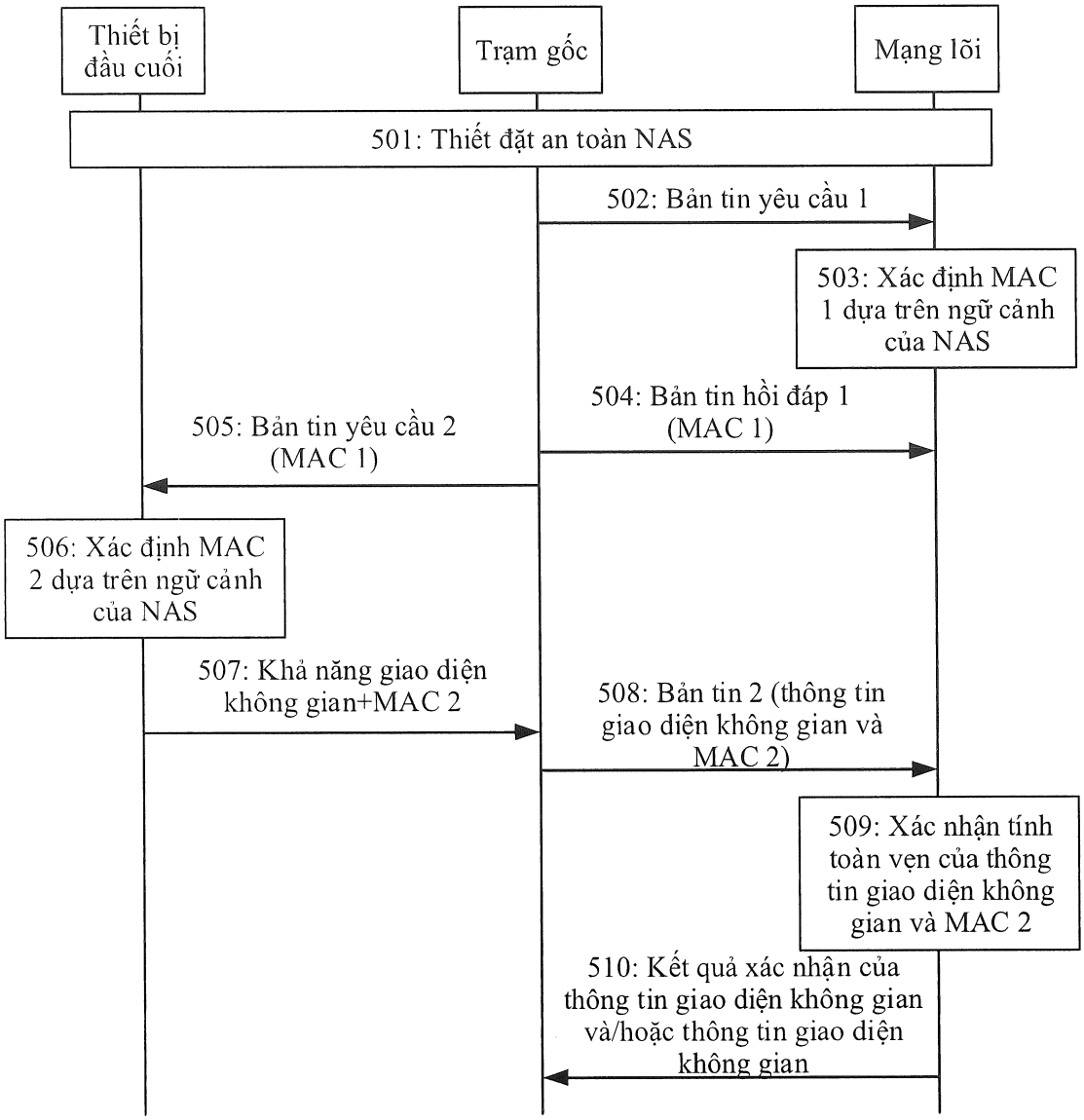
Thiết bị đầu cuối
Trạm gốc
Mạng lõi
501: Thiết đặt an toàn NAS
502: Bản tin yêu cầu 1
503: Xác định MAC 1 dựa trên ngữ cảnh của NAS
504: Bản tin hồi đáp 1 (MAC 1)
505: Bản tin yêu cầu 2 (MAC 1)
506: Xác định MAC 2 dựa trên ngữ cảnh của NAS
507: Khả năng giao diện không gian+MAC 2
508: Bản tin 2 (thông tin giao diện không gian và MAC 2)
509: Xác nhận tính toàn vẹn của thông tin giao diện không gian và MAC 2
510: Kết quả xác nhận của thông tin giao diện không gian và/hoặc thông tin giao diện không gian

Fig.5

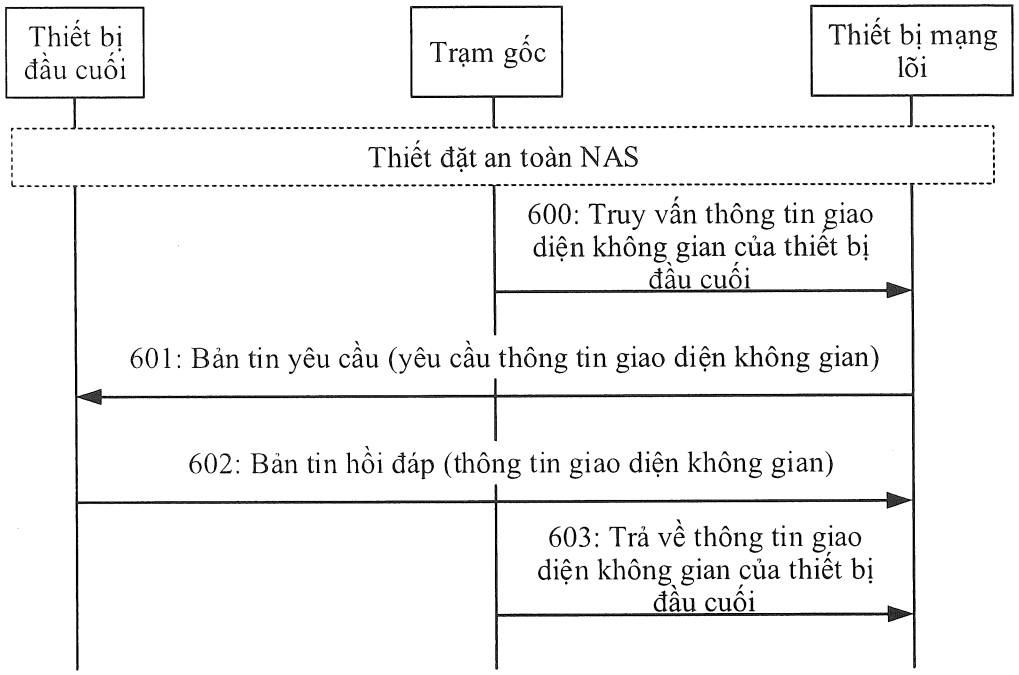
Thiết bị đầu cuối
Trạm gốc
Thiết bị mạng lõi
Thiết đặt an toàn NAS
600: Truy vấn thông tin giao diện không gian của thiết bị đầu cuối
601: Bản tin yêu cầu (yêu cầu thông tin giao diện không gian)
602: Bản tin hồi đáp (thông tin giao diện không gian)
603: Trả về thông tin giao diện không gian của thiết bị đầu cuối

Fig.6

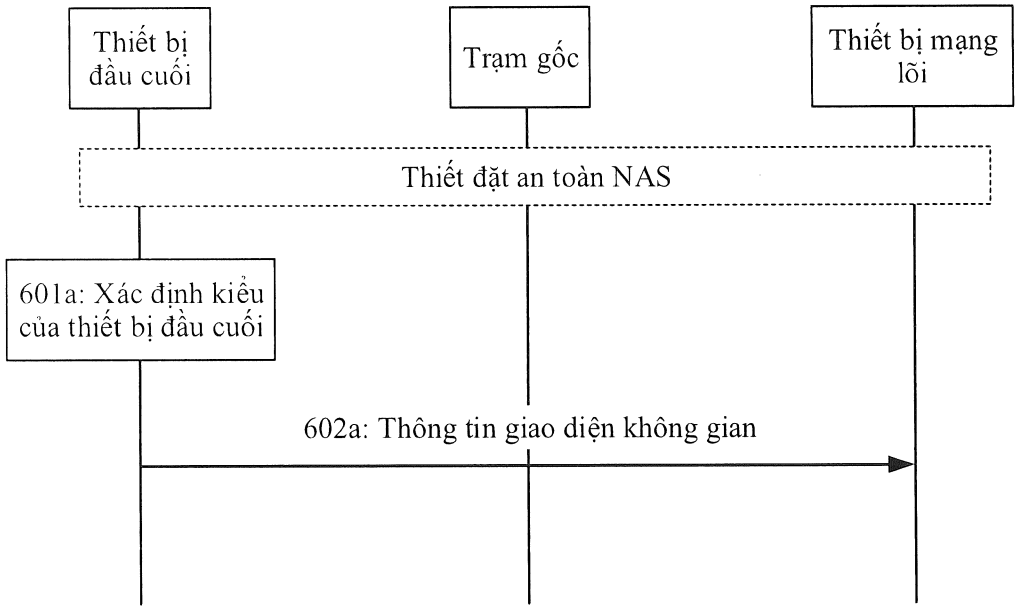
Thiết bị đầu cuối
Trạm gốc
Thiết bị mạng lõi
Thiết đặt an toàn NAS
601a: Xác định kiểu của thiết bị đầu cuối
602a: Thông tin giao diện không gian

Fig.6a

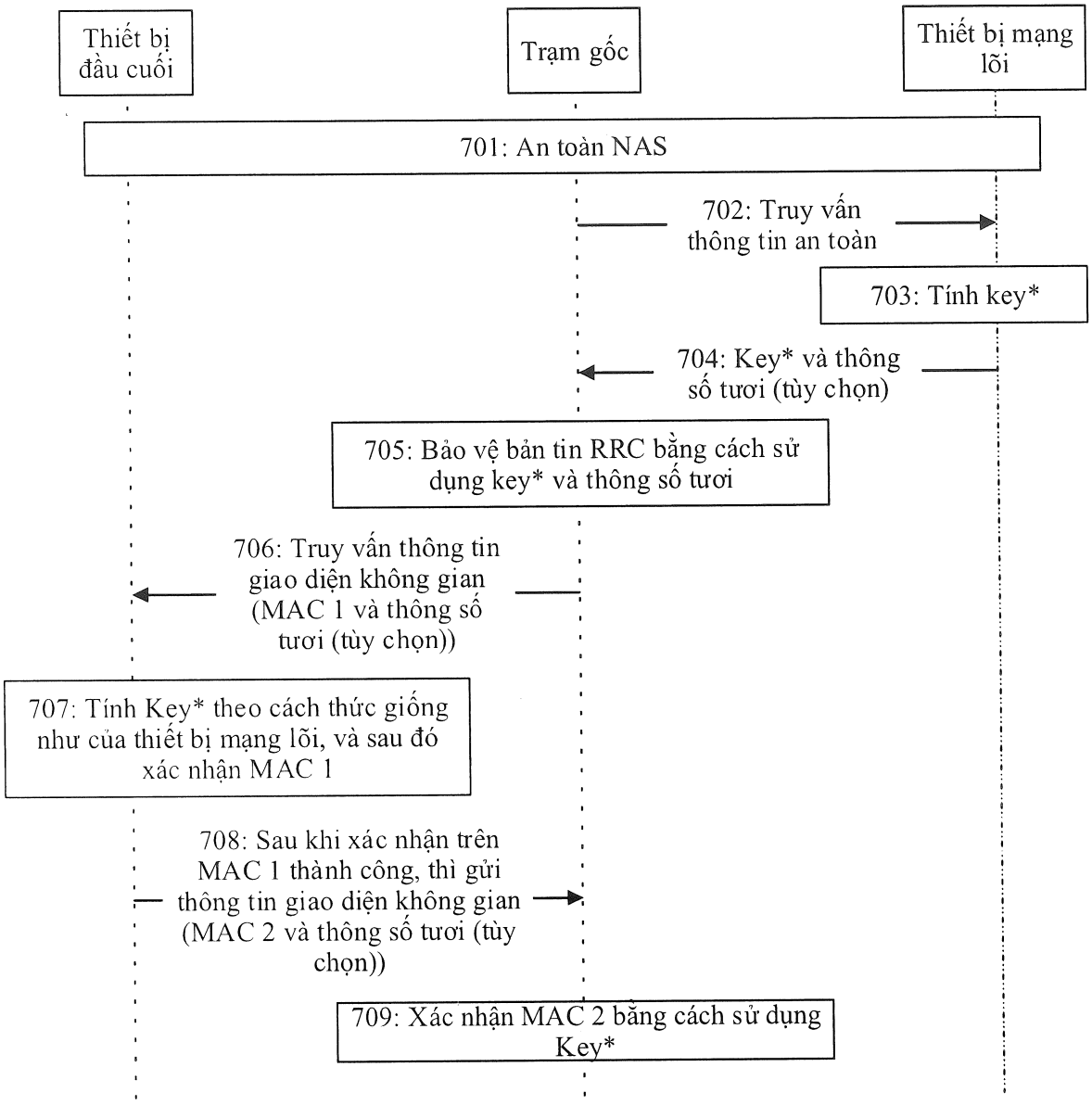
Thiết bị đầu cuối
Trạm gốc
Thiết bị mạng lõi
701: An toàn NAS
702: Truy vấn thông tin an toàn
703: Tính key*
704: Key* và thông số tươi (tùy chọn)
705: Bảo vệ bản tin RRC bằng cách sử dụng key* và thông số tươi
706: Truy vấn thông tin giao diện không gian (MAC 1 và thông số tươi (tùy chọn))
707: Tính Key* theo cách thức giống như của thiết bị mạng lõi, và sau đó xác nhận MAC 1
708: Sau khi xác nhận trên MAC 1 thành công, thì gửi thông tin giao diện không gian (MAC 2 và thông số tươi (tùy chọn))
709: Xác nhận MAC 2 bằng cách sử dụng Key*

Fig.7

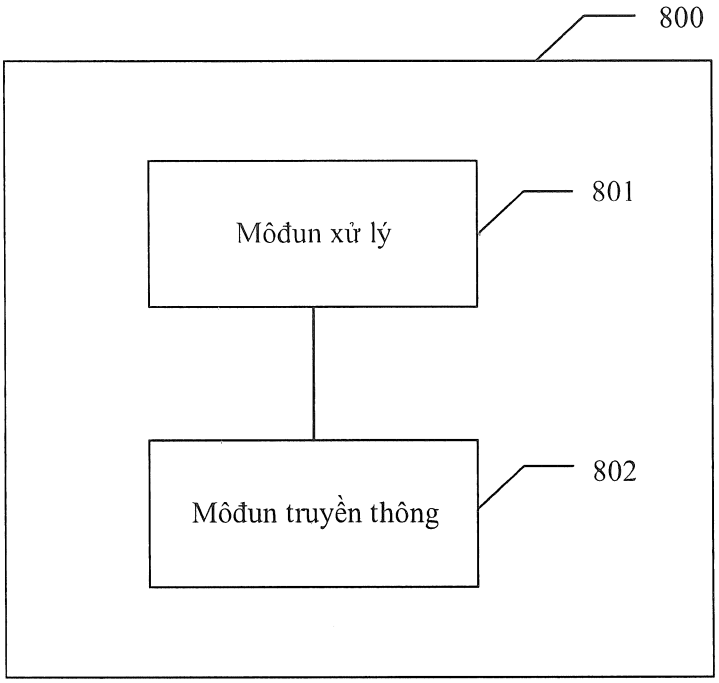
800
801
Môđun xử lý
802
Môđun truyền thông

Fig.8

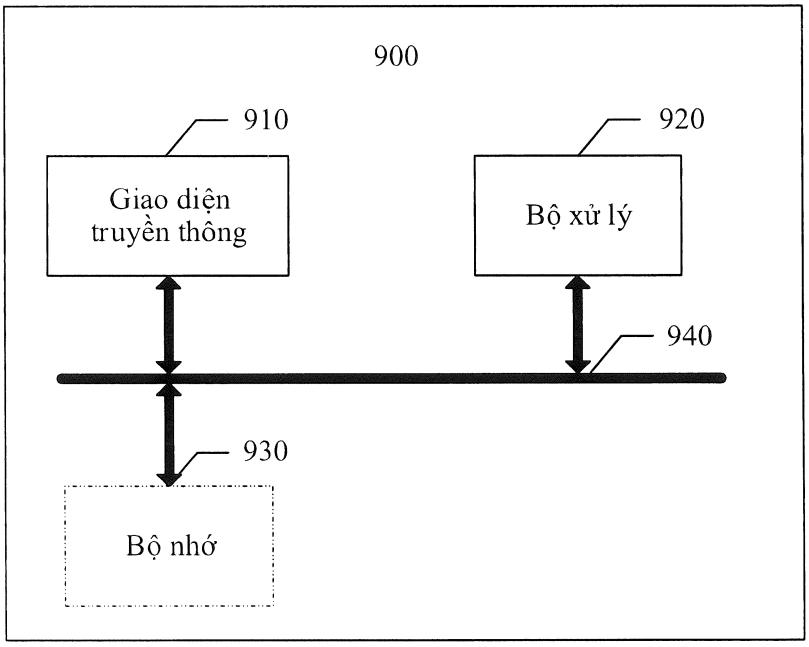
900
910
Giao diện truyền thông
920
Bộ xử lý
940
930
Bộ nhớ

Fig.9

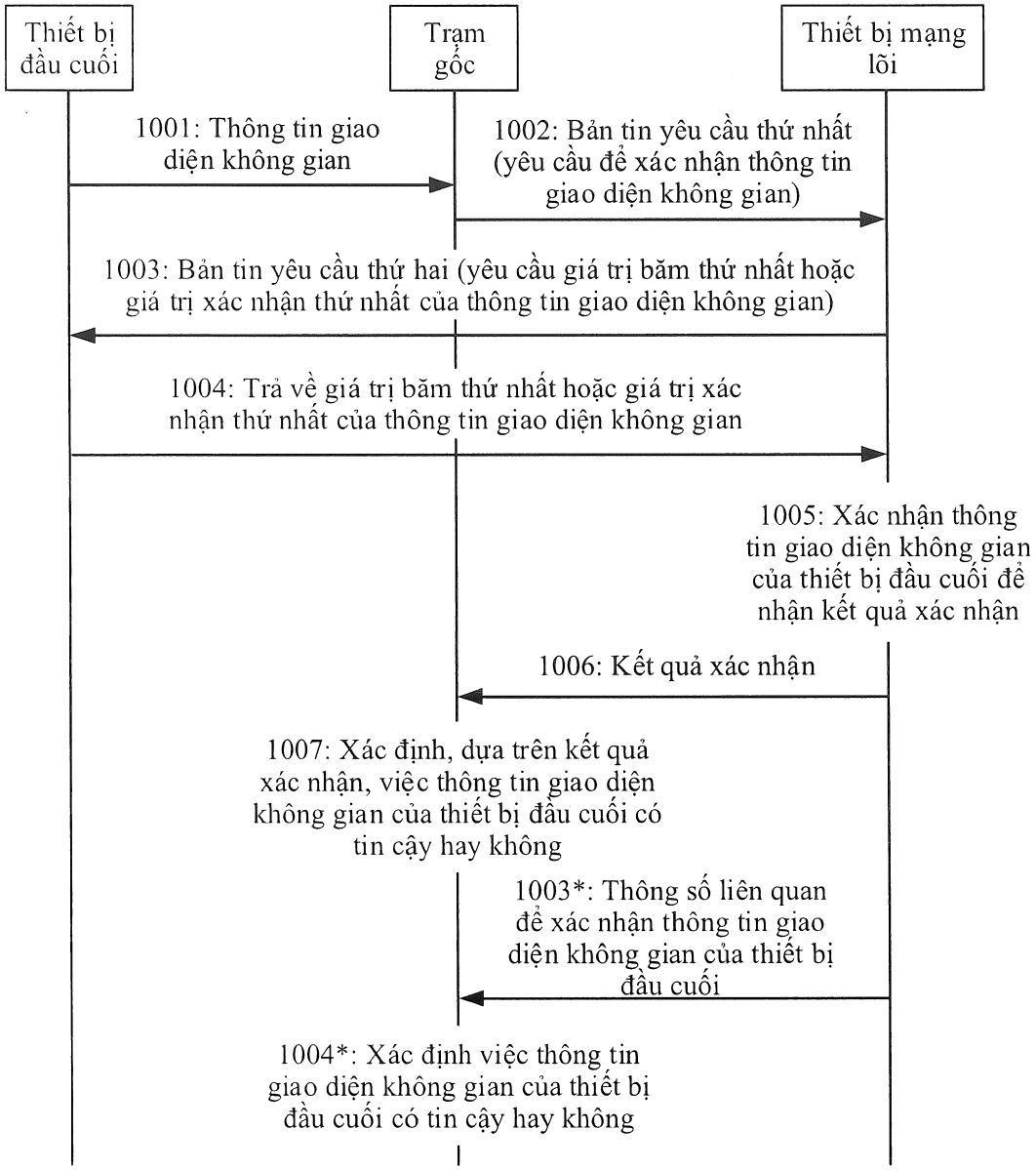
Thiết bị đầu cuối
Trạm gốc
Thiết bị mạng lõi
1001: Thông tin giao diện không gian
1002: Bản tin yêu cầu thứ nhất (yêu cầu để xác nhận thông tin giao diện không gian)
1003: Bản tin yêu cầu thứ hai (yêu cầu giá trị băm thứ nhất hoặc giá trị xác nhận thứ nhất của thông tin giao diện không gian)
1004: Trả về giá trị băm thứ nhất hoặc giá trị xác nhận thứ nhất của thông tin giao diện không gian
1005: Xác nhận thông tin giao diện không gian của thiết bị đầu cuối để nhận kết quả xác nhận
1006: Kết quả xác nhận
1007: Xác định, dựa trên kết quả xác nhận, việc thông tin giao diện không gian của thiết bị đầu cuối có tin cậy hay không
1003*: Thông số liên quan để xác nhận thông tin giao diện không gian của thiết bị đầu cuối
1004*: Xác định việc thông tin giao diện không gian của thiết bị đầu cuối có tin cậy hay không

Fig.10