(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) **1-0035616**

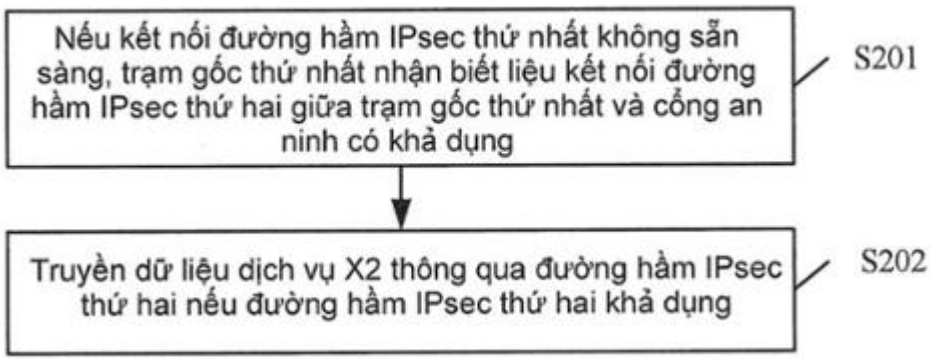
(51)[19] **H04W 24/00**

(13) **B**

(21) 1-2019-03359
(22) 29/11/2016
(86) PCT/CN2016/107711 29/11/2016
(87) WO 2018/098630 07/06/2018
(45) 25/05/2023 422
(43) 25/09/2019 378A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, China
(72) XUE, Wan (CN); DONG, Changcong (CN); CHEN, Jianfeng (CN).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) THIẾT BỊ MẠNG VÀ PHƯƠNG TIỆN BẤT BIẾN ĐỌC ĐƯỢC BỞI MÁY TÍNH

(57) Sáng chế đề cập đến thiết bị mạng và phương tiện bất biến đọc được bởi máy tính bao gồm các lệnh mà làm cho bộ xử lý thực hiện các hoạt động truyền. Các hoạt động truyền này có thể bao gồm: nếu kết nối đường hầm bảo mật giao thức Internet (IPsec- Internet Protocol Security) thứ nhất không khả dụng, nhận biết, bởi trạm gốc thứ nhất, liệu kết nối đường hầm IPsec thứ hai giữa trạm gốc thứ nhất và cổng bảo mật có khả dụng, trong đó kết nối đường hầm IPsec thứ nhất là kết nối đường hầm IPsec được thiết lập giữa trạm gốc thứ nhất và trạm gốc thứ hai, và trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc thứ hai thông qua kết nối đường hầm IPsec thứ hai; và truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ hai nếu kết nối đường hầm IPsec thứ hai khả dụng. Việc này giải quyết vấn đề kỹ thuật là sự dư thừa tự động không thể đạt được khi dịch vụ X2 được truyền giữa các trạm gốc thông qua kết nối đường hầm IPsec trực tiếp.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực các kỹ thuật truyền thông và cụ thể là đề cập đến phương pháp truyền dịch vụ X2 và thiết bị mạng.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển nhanh của các công nghệ truyền thông di động, hệ thống truyền thông di động thế hệ thứ ba đã vào pha phát triển dài hạn (Long Term Evolution, LTE). Ngoài ra, do các đặc điểm như lượng dữ liệu dịch vụ viễn thông lớn, cấu trúc mạng phức tạp, và LTE dựa trên toàn bộ giao thức Internet (Internet Protocol), dự án đối tác thế hệ thứ ba (3GPP) đề xuất sử dụng công nghệ bảo mật giao thức Internet (Internet Protocol Security, IPsec) để tăng cường việc bảo vệ các dịch vụ dữ liệu. IPsec là giao thức khung bảo mật lớp IP mở được đề xuất bởi lực lượng chuyên trách về kỹ thuật Internet (The Internet Engineering Task Force, IETF), và là giao thức đường hầm lớp 3. IPsec hoạt động ở lớp mạng, và có thể cung cấp sự bảo vệ bảo mật cho việc truyền dữ liệu nhạy cảm, và bảo vệ và xác thực gói dữ liệu IP được truyền giữa các thiết bị mà tham gia trong IPsec. IPsec ngăn ngừa dữ liệu không bị kiểm soát, bị can thiệp, và bị làm giả bởi kẻ tấn công trong suốt quá trình truyền qua mạng công cộng.

Trong kỹ thuật đã biết, đối với mạng đường trục không dây LTE, cơ chế văn bản thuần túy được sử dụng để truyền dữ liệu truyền thông của trạm gốc. Cụ thể, dòng dữ liệu giao diện X2 giữa các trạm gốc có nhiều khả năng bị giải mã, nghe trộm, mạo nhận, can thiệp, và tương tự, và đối mặt với rủi ro bảo mật lớn. Để làm giảm rủi ro bảo mật, bảo mật truyền của dòng dữ liệu giao diện X2 đã được bảo vệ trong kỹ thuật đã biết bằng cách hỗ trợ đường hầm bảo mật giao diện X2 được thiết lập tự động giữa các trạm gốc. Tuy nhiên, khi dịch vụ X2 cần được truyền giữa các trạm gốc, đường hầm IPsec trực tiếp được thiết lập tự động là không khả dụng. Do đó, gói dữ liệu tương ứng với dịch vụ X2 chỉ có thể được loại bỏ, và do đó việc truyền của dịch vụ X2 không thể được hoàn thành. Theo

cách khác, ngay cả nếu có thể có đường hầm IPsec trực tiếp chờ sẵn được thiết lập trước khác được sử dụng với đường hầm IPsec trực tiếp cho các mục đích dư thừa, có thể là không có sự dư thừa hiệu quả có thể đạt được ngay cả nếu có nhiều đường hầm IPsec trực tiếp chờ sẵn do liên kết vật lý giữa các trạm gốc không khả dụng hoặc bị lỗi. Kết quả là, hiệu quả truyền thông thấp, gây ảnh hưởng đến trải nghiệm người dùng.

Bản chất kỹ thuật của sáng chế

Vấn đề kỹ thuật cần được giải quyết trong các phương án của sáng chế là đề xuất phương pháp truyền dịch vụ X2 và thiết bị mạng, để giải quyết vấn đề kỹ thuật là sự dư thừa tự động không thể đạt được khi dịch vụ X2 được truyền giữa các trạm gốc thông qua kết nối đường hầm IPsec trực tiếp.

Theo khía cạnh thứ nhất, phương án của sáng chế đề xuất phương pháp truyền dịch vụ X2. Phương pháp này có thể bao gồm:

nếu kết nối đường hầm IPsec thứ nhất không khả dụng, nhận biết, bởi trạm gốc thứ nhất, liệu kết nối đường hầm IPsec thứ hai giữa trạm gốc thứ nhất và cổng bảo mật có khả dụng, trong đó kết nối đường hầm IPsec thứ nhất là kết nối đường hầm IPsec được thiết lập giữa trạm gốc thứ nhất và trạm gốc thứ hai, và trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc thứ hai thông qua kết nối đường hầm IPsec thứ hai; và truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ hai nếu kết nối đường hầm IPsec thứ hai khả dụng. Nếu kết nối đường hầm Ipsec được thiết lập tự động giữa các trạm gốc không khả dụng, còn được xác định liệu kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật khả dụng. Nếu kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật khả dụng, dữ liệu dịch vụ X2 được truyền thông qua kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật. Điều này giải quyết vấn đề là sự dư thừa bảo mật không thể tự động đạt được khi dữ liệu dịch vụ X2 được truyền giữa các trạm gốc thông qua kết nối đường hầm IPsec, nhờ đó cải thiện độ tin cậy của việc truyền dữ liệu dịch vụ X2.

Viện dẫn tới khía cạnh thứ nhất, theo cách thức thực hiện có thể thứ nhất,

trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc khác bất kỳ thông qua kết nối đường hầm IPsec thứ hai. Đường hầm IPsec thứ hai được tạo cấu hình để ở dạng hỗ trợ việc truyền dịch vụ X2 giữa trạm gốc thứ nhất và trạm gốc khác bất kỳ, sao cho đường hầm IPsec thứ hai có thể hỗ trợ sự dư thừa của các đường hầm IPsec giữa nhiều trạm gốc hơn, nhờ đó cải thiện độ tin cậy của việc truyền dữ liệu dịch vụ X2 trong toàn bộ hệ thống.

Viện dẫn tới khía cạnh thứ nhất hoặc cách thức thực hiện có thể thứ nhất của khía cạnh thứ nhất, theo cách thức thực hiện có thể thứ hai, sau khi việc truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ hai, phương pháp còn bao gồm: xác định liệu kết nối đường hầm IPsec thứ nhất có khả dụng; và chuyển đổi dữ liệu dịch vụ X2 được truyền thông qua kết nối đường hầm IPsec thứ hai sang đường hầm IPsec thứ nhất để truyền dẫn nếu kết nối đường hầm IPsec thứ nhất khả dụng. Liệu hiệu quả truyền dẫn có thể còn được cải thiện còn được kiểm soát trong khi đảm bảo là dịch vụ X2 có thể được truyền, và nếu kết nối đường hầm IPsec trực tiếp (đường hầm IPsec thứ nhất) khả dụng, dịch vụ X2 vẫn được chuyển sang đường hầm IPsec trực tiếp để truyền dẫn, để làm giảm độ trễ dịch vụ và cải thiện hiệu quả truyền dẫn.

Viện dẫn tới cách thức thực hiện có thể thứ hai của khía cạnh thứ nhất, theo cách thức thực hiện có thể thứ ba, bước xác định liệu kết nối đường hầm IPsec thứ nhất có khả dụng bao gồm: khởi tạo gói tin yêu cầu thiết lập đường hầm IPsec cho trạm gốc thứ hai; và nếu thu gói tin phản hồi thiết lập đường hầm IPsec được phản hồi bởi trạm gốc thứ hai, xác định rằng đường hầm IPsec thứ nhất khả dụng.

Viện dẫn tới bất kỳ một trong số khía cạnh thứ nhất hoặc các cách thức thực hiện khả thi nêu trên của khía cạnh thứ nhất, theo cách thức thực hiện có thể thứ tư, phương pháp còn bao gồm: loại bỏ, bởi trạm gốc thứ nhất, dữ liệu dịch vụ X2 nếu không có kết nối đường hầm IPsec thứ nhất cũng không có kết nối đường hầm IPsec thứ hai khả dụng. Nếu không có kết nối đường hầm IPsec thứ nhất cũng không có kết nối đường hầm IPsec thứ hai khả dụng, gói dữ liệu tương ứng với dịch vụ X2 được loại bỏ, để tránh rủi ro bảo mật dữ liệu.

Viện dẫn tới bất kỳ một trong số khía cạnh thứ nhất hoặc các cách thức thực hiện khả thi nêu trên của khía cạnh thứ nhất, theo cách thức thực hiện có thể thứ năm, phương pháp còn bao gồm: truyền, bởi trạm gốc thứ nhất, dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ nhất nếu kết nối đường hầm IPsec thứ nhất khả dụng. Nếu kết nối đường hầm IPsec thứ nhất khả dụng, dịch vụ X2 được xem xét theo cách ưu tiên để được truyền thông qua kết nối đường hầm IPsec thứ nhất, để làm giảm độ trễ dịch vụ và cải thiện hiệu quả truyền dẫn.

Theo khía cạnh thứ hai, phương án của sáng chế đề xuất thiết bị mạng. Thiết bị mạng là trạm gốc thứ nhất, và có thể bao gồm bộ xử lý và bộ thu phát, trong đó bộ xử lý được tạo cấu hình để: nếu kết nối đường hầm IPsec thứ nhất không khả dụng, nhận biết liệu kết nối đường hầm IPsec thứ hai giữa trạm gốc thứ nhất và cổng bảo mật khả dụng, trong đó kết nối đường hầm IPsec thứ nhất là kết nối đường hầm IPsec được thiết lập giữa trạm gốc thứ nhất và trạm gốc thứ hai, và trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc thứ hai thông qua kết nối đường hầm IPsec thứ hai; và bộ thu phát được tạo cấu hình để gửi và/hoặc thu dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ hai nếu kết nối đường hầm IPsec thứ hai khả dụng.

Viện dẫn tới khía cạnh thứ hai, theo cách thức thực hiện có thể thứ nhất, trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc khác bất kỳ thông qua kết nối đường hầm IPsec thứ hai.

Viện dẫn tới khía cạnh thứ hai hoặc cách thức thực hiện có thể thứ nhất của khía cạnh thứ hai, theo cách thức thực hiện có thể thứ hai, bộ xử lý còn được tạo cấu hình để: sau khi dữ liệu dịch vụ X2 được truyền thông qua kết nối đường hầm IPsec thứ hai, xác định liệu kết nối đường hầm IPsec thứ nhất có khả dụng; và bộ thu phát còn được tạo cấu hình để chuyển dữ liệu dịch vụ X2 được truyền thông qua kết nối đường hầm IPsec thứ hai sang đường hầm IPsec thứ nhất để truyền dẫn nếu kết nối đường hầm IPsec thứ nhất khả dụng.

Viện dẫn tới cách thức thực hiện có thể thứ hai của khía cạnh thứ hai, theo cách thức thực hiện có thể thứ ba, bộ xử lý được tạo cấu hình để xác định liệu kết nối đường hầm IPsec thứ nhất có khả dụng cụ thể là: khởi tạo gói tin yêu cầu

thiết lập đường hầm IPsec cho trạm gốc thứ hai bằng cách sử dụng bộ thu phát; và nếu thu, bằng cách sử dụng bộ thu phát, gói tin phản hồi thiết lập đường hầm IPsec được phản hồi bởi trạm gốc thứ hai, xác định rằng đường hầm IPsec thứ nhất khả dụng.

Viện dẫn tới bất kỳ một trong số khía cạnh thứ hai hoặc các cách thức thực hiện khả thi nêu trên của khía cạnh thứ hai, theo cách thức thực hiện có thể thứ tư, bộ xử lý còn được tạo cấu hình để loại bỏ dữ liệu dịch vụ X2 nếu không có kết nối đường hầm IPsec thứ nhất cũng không có kết nối đường hầm IPsec thứ hai khả dụng.

Viện dẫn tới bất kỳ một trong số khía cạnh thứ hai hoặc các cách thức thực hiện khả thi nêu trên của khía cạnh thứ hai, theo cách thức thực hiện có thể thứ năm, bộ thu phát còn được tạo cấu hình để: nếu kết nối đường hầm IPsec thứ nhất khả dụng, xác định để truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ nhất.

Viện dẫn tới bất kỳ một trong số khía cạnh thứ hai hoặc các cách thức thực hiện khả thi nêu trên của khía cạnh thứ hai, thiết bị mạng còn bao gồm bộ nhớ, được tạo cấu hình để lưu trữ lệnh chương trình và dữ liệu mà cần thiết cho thiết bị mạng.

Viện dẫn tới bất kỳ một trong số khía cạnh thứ hai hoặc các cách thức thực hiện khả thi nêu trên của khía cạnh thứ hai, bộ xử lý còn được tạo cấu hình để hỗ trợ thiết bị mạng trong việc thực hiện chức năng tương ứng trong phương pháp theo bất kỳ một trong số khía cạnh thứ nhất hoặc các cách thức thực hiện khả thi của khía cạnh thứ nhất, ví dụ, điều khiển bộ thu phát để truyền dữ liệu dịch vụ trên đường hầm IPsec thứ nhất hoặc đường hầm IPsec thứ hai.

Theo khía cạnh thứ ba, phương án của sáng chế đề xuất phương tiện lưu trữ đọc được bởi máy tính, được tạo cấu hình để lưu trữ lệnh phần mềm máy tính được sử dụng bởi thiết bị mạng được đề xuất trong khía cạnh thứ hai nêu trên. Lệnh phần mềm máy tính bao gồm chương trình được thiết kế để thực hiện khía cạnh nêu trên.

Theo khía cạnh thứ tư, sáng chế đề xuất thiết bị mạng. Thiết bị mạng có chức năng thực hiện trạng thái của thiết bị mạng trong phương án phương pháp nêu trên. Chức năng này có thể được thực hiện bởi phần cứng, hoặc bởi phần cứng nhờ thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều môđun tương ứng với chức năng nêu trên. Một cách tùy chọn, thiết bị mạng có thể là thiết bị mạng truy nhập vô tuyến, ví dụ, trạm gốc.

Theo khía cạnh thứ năm, sáng chế đề xuất hệ thống chip. Hệ thống chip bao gồm bộ xử lý, được tạo cấu hình để hỗ trợ thiết bị mạng trong việc thực hiện chức năng trong khía cạnh nêu trên, ví dụ, tạo ra hoặc xử lý dữ liệu và/hoặc thông tin trong phương pháp nêu trên. Theo thiết kế có thể, hệ thống chip còn bao gồm bộ nhớ. Bộ nhớ được tạo cấu hình để lưu trữ lệnh chương trình và dữ liệu mà cần thiết cho thiết bị mạng. Hệ thống chip có thể bao gồm chip, hoặc có thể bao gồm chip và thiết bị riêng biệt khác.

Theo phương pháp truyền dữ liệu dịch vụ X2 và thiết bị mà được đề xuất trong các phương án của sáng chế, nếu kết nối đường hầm IPsec được thiết lập tự động giữa các trạm gốc không khả dụng, còn được xác định liệu kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật có khả dụng để truyền dẫn. Nếu kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật khả dụng, dữ liệu dịch vụ X2 được truyền thông qua kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật. Điều này giải quyết vấn đề là sự dư thừa bảo mật không thể tự động đạt được khi dữ liệu dịch vụ X2 được truyền giữa các trạm gốc thông qua kết nối đường hầm IPsec, nhờ đó cải thiện độ tin cậy của việc truyền dữ liệu dịch vụ X2.

Mô tả vắn tắt các hình vẽ

Phần sau đây mô tả vắn tắt các hình vẽ kèm theo được yêu cầu để mô tả các phương án hoặc kỹ thuật đã biết.

FIG.1 là sơ đồ của kiến trúc mạng truyền thông theo phương án của sáng chế;

FIG.2 là lưu đồ giản lược của phương pháp truyền dịch vụ X2 theo phương

án của sáng chế;

FIG.3 là sơ đồ giản lược của kịch bản ứng dụng cụ thể của phương pháp truyền dịch vụ X2 theo phương án của sáng chế;

FIG.4 là lưu đồ giản lược của phương pháp truyền dịch vụ X2 khác theo phương án của sáng chế;

FIG.5 là sơ đồ cấu trúc giản lược của thiết bị truyền dịch vụ X2 theo phương án của sáng chế; và

FIG.6 là sơ đồ cấu trúc giản lược của thiết bị mạng theo phương án của sáng chế.

Mô tả chi tiết sáng chế

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

Trong bản mô tả, yêu cầu bảo hộ, và các hình vẽ kèm theo của sáng chế, các thuật ngữ "thứ nhất", "thứ hai", "thứ ba", "thứ tư", và tương tự nhằm mục đích phân biệt giữa các đối tượng khác nhau nhưng không nhằm mô tả thứ tự cụ thể. Ngoài ra, các thuật ngữ "bao gồm", "có", và bất kỳ cải biến khác của nó đều nhằm mục đích là sự bao gồm không loại trừ. Ví dụ, quy trình, phương pháp, hệ thống, sản phẩm, hoặc thiết bị mà bao gồm một loạt các bước hoặc các bộ phận không bị giới hạn ở các bước hoặc các bộ phận được liệt kê, mà một cách tùy chọn còn bao gồm bước hoặc bộ phận không được liệt kê, hoặc một cách tùy chọn còn bao gồm bước hoặc bộ phận riêng khác của quy trình, phương pháp, sản phẩm, hoặc thiết bị.

"Phương án" được đề cập trong bản mô tả này có nghĩa là đặc tính cụ thể, cấu trúc, hoặc dấu hiệu được mô tả dựa vào phương án có thể được chứa trong ít nhất một phương án của sáng chế. Thuật ngữ mà xuất hiện ở các vị trí khác nhau trong bản mô tả này không nhất thiết có nghĩa là cùng phương án, và không là phương án độc lập hoặc luân phiên ngoại trừ phương án khác. Được hiểu một cách rõ ràng và đầy đủ bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật là các phương án được mô tả trong bản mô tả này có thể được kết hợp với

phương án khác.

Phần sau đây giải thích một số thuật ngữ trong sáng chế, để giúp người có hiểu biết trung bình trong lĩnh vực kỹ thuật hiểu rõ hơn.

(1) Thiết bị mạng có thể là các loại khác nhau của các trạm hoặc các trạm gốc, và có thể là nút B cải tiến (Evolved NodeB, eNB hoặc eNodeB) trong LTE, thiết bị mạng trong mạng 5G tương lai, hoặc tương tự. Thiết bị mạng trong sáng chế bao gồm trạm gốc thứ nhất và trạm gốc thứ hai. Tuy nhiên, điều này không bị giới hạn.

(2) Quy tắc lập danh mục điều khiển truy nhập (Access Control List RULE, ACLRULE) được sử dụng để xác định các gói tin dữ liệu mà được nhập vào/xuất ra thông qua cổng, và có thể áp dụng được với tất cả các giao thức định tuyến như giao thức IPsec và tường lửa. ACLRULE có thể được sử dụng trong giao thức IPsec để xác định dòng dữ liệu mà cần được bảo vệ. Dựa trên ACLRULE, IPsec xác định các gói tin mà cần sự bảo vệ bảo mật và các gói tin mà không cần sự bảo vệ bảo mật. Ở đầu khởi tạo đường hầm, dòng dữ liệu mà phù hợp với ACLRULE là cần được bảo vệ, cụ thể, dòng dữ liệu được gửi sau khi xử lý mã hóa mật IPsec; và dòng dữ liệu mà không thể phù hợp với ACLRULE lập tức được chuyển tiếp. Ở đầu thu đường hầm, dòng dữ liệu được mã hóa mật, nó được kiểm tra xem liệu dòng dữ liệu được mã hóa mật có phù hợp với ACLRULE, và gói tin mà không phù hợp với ACLRULE được loại bỏ.

(3) Trao đổi khóa Internet (Internet Key Exchange, IKE): IKE là giao thức lai, là một trong số chuỗi các trao đổi khóa, và được gọi là "chế độ". IKE có thể được sử dụng để thương lượng về mạng riêng ảo (Virtual Private Network, VPN), và có thể cũng được sử dụng bởi người dùng từ xa (địa chỉ IP của người dùng từ xa không cần được biết trước) để truy nhập máy chủ bảo mật hoặc mạng, và IKE hỗ trợ việc thương lượng của máy khách. Chế độ máy khách là bộ thương lượng không là điểm cuối mà khởi tạo kết nối bảo mật. Khi chế độ máy khách được sử dụng, ký hiệu nhận dạng của điểm cuối bị ẩn.

(4) Chính sách bảo mật (IPsec Policy) được sử dụng để xác định các gói tin

mà cần được mã hóa mật, các thuật toán tương ứng như mã hóa mật IPsec và xác thực, và các tham số liên quan đến IPsec khác, để xác định liệu đầu truyền và đầu thu có thể truyền thông với nhau, và để xác định thuật toán xử lý dữ liệu cần được sử dụng để truyền thông nếu đầu truyền và đầu thu được cho phép truyền thông với nhau.

(5) "Nhiều" nghĩa là "hai hoặc nhiều hơn". "Và/hoặc" mô tả quan hệ kết hợp giữa các đối tượng được kết hợp và thể hiện rằng ba quan hệ có thể tồn tại. Ví dụ, A và/hoặc B có thể biểu diễn ba trường hợp sau đây: Chỉ A tồn tại, cả A và B cùng tồn tại, và chỉ B tồn tại. Ký tự "/" chỉ báo quan hệ "hoặc" giữa các đối tượng được kết hợp.

"Dữ liệu" được mô tả trong sáng chế có thể là dữ liệu dịch vụ, hoặc có thể bao gồm nội dung như báo hiệu hoặc bản tin mà cần được truyền bởi hệ thống. "Truyền dẫn" được mô tả trong sáng chế bao gồm gửi và/hoặc thu.

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

Để dễ hiểu các phương án của sáng chế, trước tiên phần sau đây mô tả kiến trúc mạng truyền thông mà các phương án của sáng chế được dựa trên. FIG.1 là sơ đồ của kiến trúc mạng truyền thông theo phương án của sáng chế. Kiến trúc mạng bao gồm mạng lõi, trạm gốc thứ nhất, trạm gốc thứ hai, và cổng bảo mật mà hỗ trợ giao thức IPsec. Giao diện X2 giữa trạm gốc thứ nhất và trạm gốc thứ hai hỗ trợ truyền dẫn trực tiếp của thông tin mặt phẳng điều khiển giữa các trạm gốc và thông tin mặt phẳng người dùng (dữ liệu và báo hiệu) giữa các trạm gốc, để tránh độ trễ truyền và hiệu quả truyền thông thấp mà bị gây ra nếu thông tin đi qua cổng bảo mật. Ví dụ, dịch vụ phối hợp mà dựa trên mạng truy nhập vô tuyến IP (IP Radio Access Network, IPRAN) có yêu cầu rất cao về độ trễ truyền. Do đó, sự đối thoại trực tiếp thông qua giao diện X2 có thể làm giảm hiệu quả các đường truyền, nhờ đó làm giảm độ trễ. Giao diện S1 là giao diện truyền thông giữa trạm gốc (ví dụ, eNodeB của LTE) và mạng lõi (ví dụ, mạng lõi gói tin EPC), và được tạo cấu hình để: truyền thông tin quản lý phiên (Session Management, SM) và quản lý tính di động (Mobility Management, MM), và

truyền dịch vụ dữ liệu người dùng, cụ thể, được tạo cấu hình để truyền thông tin mặt phẳng điều khiển và mặt phẳng báo hiệu hoặc dữ liệu mặt phẳng người dùng giữa trạm gốc và mạng lõi. Đường hầm IPsec được thiết lập giữa trạm gốc thứ nhất và trạm gốc thứ hai là kết nối đường hầm IPsec trực tiếp, có thể được gọi là kết nối đường hầm IPsec trực tiếp (Direct IPsec), và được tạo cấu hình để truyền chỉ dịch vụ X2, ví dụ, là kết nối đường hầm IPsec thứ nhất trong sáng chế. Dịch vụ X2 có thể được thực hiện trực tiếp giữa trạm gốc thứ nhất và trạm gốc thứ hai thông qua kết nối đường hầm IPsec trực tiếp. Đường hầm IPsec giữa trạm gốc thứ nhất và cổng bảo mật là kết nối đường hầm IPsec cổng bảo mật, và có thể được tạo cấu hình để truyền dịch vụ X2 hoặc dịch vụ S1, ví dụ, đường hầm IPsec thứ hai trong sáng chế. Thông qua kết nối đường hầm IPsec cổng bảo mật, dịch vụ X2 có thể được thực hiện không trực tiếp giữa trạm gốc thứ nhất và trạm gốc thứ hai bằng cách sử dụng cổng bảo mật nếu kết nối đường hầm IPsec trực tiếp không khả dụng. Nói cách khác, dịch vụ X2 giữa các trạm gốc có thể được truyền thông qua cả đường hầm IPsec trực tiếp và đường hầm IPsec cổng bảo mật của cổng bảo mật. Ngoài ra, đường hầm IPsec trực tiếp được tạo ra tự động giữa các trạm gốc, trong khi đường hầm IPsec cổng bảo mật cần được cấu hình thủ công. Một cách tùy chọn, đường hầm IPsec trực tiếp trong kiến trúc hệ thống tương ứng với FIG.1 có thể còn bao gồm thiết bị mạng như bộ định tuyến hoặc bộ chuyển mạch. Lưu ý rằng kiến trúc mạng trên FIG.1 chỉ là cách thức thực hiện ví dụ trong các phương án của sáng chế. Kiến trúc mạng trong các phương án của sáng chế bao gồm nhưng không giới hạn ở kiến trúc mạng nêu trên.

FIG.2 là lưu đồ giản lược của phương pháp truyền dịch vụ X2 theo phương án của sáng chế. Phương pháp có thể được áp dụng với kiến trúc mạng trên FIG.1. Trạm gốc thứ nhất và trạm gốc thứ hai có thể là các trạm gốc liền kề, hoặc có thể là các trạm gốc không liền kề. Như được thể hiện trên FIG.2, phương pháp có thể bao gồm bước S201 và bước S202 sau đây.

Bước S201: Nếu kết nối đường hầm IPsec thứ nhất không khả dụng, trạm gốc thứ nhất nhận biết liệu kết nối đường hầm IPsec thứ hai giữa trạm gốc thứ

nhất và cổng bảo mật có khả dụng.

Cụ thể, đường hầm IPsec thứ nhất là kết nối đường hầm IPsec được thiết lập giữa trạm gốc thứ nhất và trạm gốc thứ hai, và trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc thứ hai thông qua kết nối đường hầm IPsec thứ hai.

Trong ví dụ cụ thể, trước khi trạm gốc thứ nhất xác định rằng đường hầm IPsec không khả dụng, phương pháp còn bao gồm: thu, bởi trạm gốc thứ nhất, thông tin thiết lập đường hầm IPsec bảo mật giao thức Internet, trong đó thông tin thiết lập đường hầm IPsec bao gồm địa chỉ bảo mật của trạm gốc thứ hai; và thiết lập, bởi trạm gốc thứ nhất, đường hầm IPsec thứ nhất với trạm gốc thứ hai dựa trên địa chỉ bảo mật. Cụ thể, sau khi thu địa chỉ bảo mật của trạm gốc thứ hai mà trạm gốc thứ nhất cần thực hiện truyền thông bảo mật với và được mang trong báo hiệu được gửi bởi mạng lõi, trạm gốc thứ nhất thiết lập đường hầm IPsec trực tiếp cho giao diện X2 với trạm gốc thứ hai dựa trên địa chỉ bảo mật, để thực hiện truyền thông bảo mật trực tiếp, và đảm bảo độ trễ thấp và bảo mật truyền thông. Ví dụ, trong giao thức 3GPP, bản tin báo hiệu của "MME CONFIGURATION TRANSFER" mang địa chỉ ngang hàng bảo mật, và trạm gốc (trạm gốc thứ nhất, ví dụ, eNodeB) thiết lập tự động đường hầm IPsec bằng cách sử dụng địa chỉ ngang hàng bảo mật (ví dụ, trạm gốc thứ hai) và địa chỉ cục bộ. Đường hầm IPsec là IPsec trực tiếp.

Đường hầm IPsec thứ nhất là được thiết lập tự động. Quy trình thiết lập tự động là linh hoạt và hiệu quả, trong khi cấu hình thủ công là phức tạp và bất tiện. Cụ thể, quy trình thiết lập tự động của đường hầm IPsec thứ nhất trong phương án này của sáng chế chủ yếu bao gồm quy trình thương lượng của hiệp hội bảo mật giao thức trao đổi khóa Internet (Internet Key Exchange Protocol Security Association, IKE SA) và hiệp hội bảo mật giao thức Internet (Internet Protocol Security, IPsec SA). IKE SA chịu trách nhiệm thiết lập và duy trì IPsec SA, và đóng vai trò điều khiển. IPsec SA chịu trách nhiệm mã hóa mật dòng dữ liệu cụ thể. IKE SA có thể phân phối theo cách an toàn khóa, xác thực ký hiệu nhận dạng, và thiết lập IPsec SA trên mạng không an toàn, có thể cung cấp dịch

vụ thương lượng thuật toán và dịch vụ thương lượng khóa cho hai bên truyền thông mà cần mã hóa mật và xác thực, và có thể được sử dụng bởi eNodeB để thiết lập động IPsec SA. IKE SA được thiết lập thông qua ba sự trao đổi: thương lượng chính sách, trao đổi khóa DH (Diffie-Hellman key exchange), và xác thực nhận dạng đầu ngang hàng.

Trong ví dụ cụ thể, phương pháp xác thực IKE SA bao gồm xác thực khóa được chia sẻ trước và xác thực chứng nhận số. Các chi tiết là như sau.

(1) Trong xác thực khóa được chia sẻ trước, hai bên truyền thông sử dụng cùng khóa để xác thực các ký hiệu nhận dạng của nhau. Phía trạm gốc eNodeB thực hiện truy nhập mạng hợp pháp bằng cách sử dụng khóa được chia sẻ trước được thiết lập trước.

(2) Thông qua xác thực chứng nhận số của cơ quan chứng nhận (Certificate Authority, CA), hệ thống hạ tầng khóa công cộng (Public Key Infrastructure, PKI) cần được triển khai trong mạng.

Thủ tục IPsec SA có thể bảo vệ giao diện X2, giao diện S1-MME, giao diện S1-U, giao diện quản lý mạng OM, và tương tự của eNodeB. Một bộ giao thức bao gồm IKE, tải tin bảo mật đóng gói (Encapsulating Security Payload, ESP), đoạn đầu xác thực (AH), và tương tự. Thủ tục cụ thể của công nghệ IPsec là như sau:

Trong pha thứ nhất, hai bên truyền thông thiết lập kênh mà trên đó xác thực bảo mật thành công, nghĩa là, IKE SA.

Trong pha thứ hai, IPsec SA cụ thể được thiết lập thông qua thương lượng bằng cách sử dụng IKE SA được thiết lập.

Trong pha thứ ba, trong quá trình truyền thông dữ liệu, đầu truyền IPsec mã hóa mật dữ liệu, và đầu thu giải mã mật dữ liệu.

Trong kỹ thuật đã biết, khi đường hầm IPsec thứ nhất không khả dụng, gói dữ liệu tương ứng với dịch vụ X2 có thể chỉ được loại bỏ, và do đó việc truyền của dịch vụ X2 không thể được hoàn thành. Ngay cả nếu có đường hầm IPsec trực tiếp chờ sẵn được thiết lập trước khác được sử dụng với đường hầm IPsec

trực tiếp thứ nhất cho các mục đích dư thừa, rất có thể là không có sự dư thừa hiệu quả có thể đạt được ngay cả nếu có đường hầm IPsec trực tiếp chờ sẵn do liên kết vật lý giữa các trạm gốc không khả dụng hoặc bị lỗi. Kết quả là, độ tin cậy của dịch vụ X2 là thấp. Tuy nhiên, trong kỹ thuật đã biết, có đường hầm IPsec cổng bảo mật giữa trạm gốc và cổng bảo mật, và đường hầm IPsec cổng bảo mật có thể truyền dữ liệu của giao diện S1, và có thể cũng chuyển tiếp dữ liệu của giao diện X2. Nói cách khác, dịch vụ X2 có thể đi trực tiếp qua kết nối đường hầm IPsec trực tiếp, và có thể cũng đi qua kết nối đường hầm IPsec cổng bảo mật bằng cách sử dụng cổng bảo mật, và sự khác nhau chỉ nằm ở chỗ việc truyền thông qua kết nối đường hầm IPsec trực tiếp là nhanh hơn, trong khi việc truyền thông qua kết nối đường hầm IPsec cổng bảo mật hơi chậm hơn. Do đó, theo sáng chế, nếu kết nối đường hầm IPsec thứ nhất không khả dụng, có thể còn được kiểm tra liệu có đường hầm IPsec cổng bảo mật, và nếu có đường hầm IPsec cổng bảo mật, dữ liệu dịch vụ X2 có thể được truyền thông qua kết nối đường hầm IPsec cổng bảo mật. Nói cách khác, nếu kết nối đường hầm IPsec trực tiếp không thể đảm bảo việc truyền thông thường, đường hầm IPsec cổng bảo mật với tỷ lệ truyền thấp hơn được sử dụng làm đường hầm tốt nhất thứ hai để truyền dịch vụ X2, để đảm bảo sự dư thừa của dịch vụ X2. Trong ví dụ cụ thể, đường hầm IPsec cổng bảo mật được cấu hình trước thủ công.

Cụ thể, việc xác định liệu kết nối đường hầm IPsec thứ nhất có khả dụng chủ yếu là xác định liệu gói tin thương lượng dịch vụ X2 mà được khởi tạo bởi trạm gốc thứ nhất cho trạm gốc thứ hai có phù hợp với bộ lựa chọn lưu lượng (Traffic Selector, TS) của gói tin thương lượng của đường hầm IPsec thứ nhất được thiết lập tự động. Theo cách khác, một cách tùy chọn, có thể được xác định liệu quy tắc ACL rule (ACLRULE) của gói tin thương lượng mà được sử dụng trong chính sách IPsec (IPsec Policy) được tham chiếu bởi dịch vụ X2 phù hợp với ACLRULE được sử dụng bởi đường hầm IPsec thứ nhất. Nếu gói tin thương lượng dịch vụ X2 mà được khởi tạo bởi trạm gốc thứ nhất cho trạm gốc thứ hai phù hợp với bộ lựa chọn lưu lượng của gói tin thỏa thuận của đường hầm IPsec thứ nhất được thiết lập tự động hoặc quy tắc ACL của gói tin thương lượng mà

được sử dụng trong chính sách IPsec được tham chiếu bởi dịch vụ X2 phù hợp với ACLRULE được sử dụng bởi đường hầm IPsec thứ nhất, và IPsec SA của đường hầm IPsec thứ nhất tồn tại, chỉ báo rằng đường hầm IPsec thứ nhất khả dụng; hoặc nếu gói tin thương lượng dịch vụ X2 mà được khởi tạo bởi trạm gốc thứ nhất cho trạm gốc thứ hai không phù hợp với bộ lựa chọn lưu lượng của gói tin thương lượng của đường hầm IPsec thứ nhất được thiết lập tự động hoặc quy tắc ACL của gói tin thương lượng mà được sử dụng trong chính sách IPsec được tham chiếu bởi dịch vụ X2 không phù hợp với ACLRULE được sử dụng bởi đường hầm IPsec thứ nhất, hoặc IPsec SA của đường hầm IPsec thứ nhất không tồn tại, chỉ báo rằng đường hầm IPsec thứ nhất không khả dụng. Nội dung cụ thể mà phù hợp với TS hoặc ACLRULE bao gồm loại giao thức, địa chỉ IP nguồn, địa chỉ IP đích, số cổng nguồn, số cổng đích, và tương tự. Tương tự, nguyên tắc xác định liệu kết nối đường hầm IPsec thứ hai có khả dụng là giống như nguyên tắc xác định liệu kết nối đường hầm IPsec thứ nhất có khả dụng. Các chi tiết không được mô tả ở đây.

Trong phương án này của sáng chế, để cho phép quan hệ dư thừa được tạo ra tự động giữa đường hầm IPsec cổng bảo mật (đường hầm IPsec thứ hai) và đường hầm IPsec trực tiếp (đường hầm IPsec thứ nhất), chế độ của địa chỉ nguồn và địa chỉ đích trong TS của cổng bảo mật cần được cấu hình. Chế độ của địa chỉ nguồn và địa chỉ đích trong TS của đường hầm IPsec trực tiếp là IP đến IP, cụ thể là, địa chỉ nguồn cố định đến địa chỉ đích cố định. Điều này tương đương với vùng địa chỉ cục bộ TS (vùng địa chỉ IP cục bộ TS) đến vùng địa chỉ đích (vùng địa chỉ IP từ xa TS). Do đó, địa chỉ nguồn và địa chỉ đích trong TS của đường hầm IPsec cổng bảo mật có thể được cấu hình như IP đến IP, IP đến ANY (cụ thể, địa chỉ nguồn cố định đến địa chỉ đích bất kỳ), hoặc ANY đến ANY (cụ thể, địa chỉ nguồn bất kỳ đến địa chỉ đích bất kỳ). Tuy nhiên, nếu chế độ của đường hầm IPsec cổng bảo mật được thiết lập ở IP đến IP, đường hầm IPsec cổng bảo mật bị giới hạn nghiêm ngặt chỉ ở chế độ đầu đến đầu cố định. Cụ thể, chỉ đường hầm IPsec giữa trạm gốc cố định và trạm gốc cố định có thể được cấu hình thủ công mỗi lần. Hiển nhiên là, trong quy tắc này, không có sự

dư thừa có thể tự động đạt được cho đường hầm IPsec trực tiếp nếu trạm gốc thứ nhất cần truyền dịch vụ X2 với nhiều trạm gốc. Ngoài ra, các quy trình cấu hình thủ công quá mức gây ra nhiều vấn đề như các cấu hình phức tạp và tỷ lệ lỗi cao của đường hầm IPsec cổng bảo mật. Do đó, trong phương án này của sáng chế, đường hầm IPsec cổng bảo mật được tạo cấu hình để ở chế độ IP đến ANY hoặc ANY đến ANY, cụ thể là, địa chỉ IP của đầu ngang hàng thu (đầu đích) không được xác định, hoặc địa chỉ của đầu truyền cũng không được xác định. Do đó, gói dữ liệu tương ứng với dịch vụ X2 được truyền có thể được gửi đến địa chỉ bảo mật của trạm gốc bất kỳ. Tóm lại, TS của đường hầm IPsec cổng bảo mật có vẻ không đồng nhất với TS của đường hầm IPsec trực tiếp, nhưng về cơ bản là TS của đường hầm IPsec cổng bảo mật bao gồm TS của đường hầm IPsec trực tiếp. Do đó, quan hệ dư thừa có thể được tạo ra giữa đường hầm IPsec cổng bảo mật trong phương án này của sáng chế và đường hầm IPsec trực tiếp IP đến IP bất kỳ. Chắc chắn là, có thể được hiểu là, vùng địa chỉ đến ANY có thể được cấu hình linh hoạt như được yêu cầu bởi dịch vụ X2 của trạm gốc thứ nhất.

Cần lưu ý cụ thể là, việc cấu hình đường hầm IPsec cổng bảo mật để ở chế độ IP đến ANY hoặc ANY đến ANY chủ yếu là cấu hình vùng địa chỉ IP nguồn và vùng địa chỉ IP đích mà có thể cho phép trong cổng bảo mật. Ví dụ, trong chế độ IP đến IP, cả địa chỉ IP nguồn và địa chỉ IP đích được tạo cấu hình để được cố định. Trong chế độ IP đến ANY, địa chỉ IP nguồn được cố định, và địa chỉ IP đích được tạo cấu hình để là 0.0.0.0. Trong chế độ ANY đến ANY, địa chỉ IP nguồn được tạo cấu hình để là 0.0.0.0, và địa chỉ IP đích được tạo cấu hình để là 0.0.0.0. Ccó thể hiểu là, vùng địa chỉ IP đích trong cổng bảo mật có thể được thiết lập linh hoạt dựa trên vùng mà trong đó trạm gốc thứ nhất cần truyền dịch vụ X2. Vùng địa chỉ IP đích được cấu hình rộng hơn có thể cho phép dịch vụ X2 được truyền giữa nhiều trạm gốc hơn thông qua kết nối đường hầm IPsec cổng bảo mật bằng cách sử dụng cổng bảo mật.

Tóm lại, đường hầm IPsec thứ hai trong phương án này của sáng chế được tạo cấu hình để ở chế độ mà trạm gốc thứ nhất có thể truyền dịch vụ X2 với trạm gốc khác bất kỳ thông qua kết nối đường hầm IPsec thứ hai, nghĩa là, chế độ IP

đến ANY hoặc ANY đến ANY. Do đó, sau khi chế độ của đường hầm IPsec thứ hai được cấu hình thủ công trước, khi trạm gốc cần truyền dịch vụ trên giao diện X2, trạm gốc đầu tiên xác định liệu kết nối đường hầm IPsec thứ nhất được thiết lập ở bước S202 có khả dụng. Do hiệu quả truyền dẫn của đường hầm IPsec trực tiếp cao hơn hiệu quả truyền dẫn của đường hầm IPsec cổng bảo mật, nên đường hầm IPsec trực tiếp, nghĩa là, đường hầm IPsec thứ nhất, được lựa chọn theo cách ưu tiên để truyền dịch vụ X2. Nếu kết nối đường hầm IPsec thứ nhất không khả dụng, được xem xét xem liệu kết nối đường hầm IPsec thứ hai có khả dụng. Điều này tạo thuận lợi cho sự dư thừa.

Bước S204: Truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ hai nếu kết nối đường hầm IPsec thứ hai khả dụng.

Cụ thể, nếu kết nối đường hầm IPsec thứ nhất không khả dụng và đường hầm IPsec thứ hai khả dụng, dịch vụ X2 của trạm gốc thứ nhất có thể được truyền thông qua kết nối đường hầm IPsec thứ hai. Cho đến nay, quy trình mà trong đó kết nối đường hầm IPsec thứ hai tự động trở thành đường hầm tự do cấu hình của đường hầm IPsec thứ nhất đã được hoàn thành. Bất kể là trạm gốc (cụ thể, địa chỉ của đầu đích) cần thực hiện truyền thông dịch vụ X2 thông qua kết nối đường hầm IPsec thứ nhất, việc truyền có thể được thực hiện thông qua kết nối đường hầm IPsec thứ hai mà chứa nhiều hơn và có phân đoạn mạng rộng hơn. Do đó, chỉ một cấu hình tổng thể được yêu cầu, mà không cần thực hiện các cấu hình lần lượt, sao cho thuận tiện hơn và dễ dàng hơn cho người dùng thực hiện việc cấu hình.

Trong kịch bản ứng dụng cụ thể, FIG.3 là sơ đồ giản lược của kịch bản ứng dụng cụ thể của việc truyền dịch vụ X2 theo phương án của sáng chế. Trên FIG.3, trạm gốc thứ nhất thương lượng với trạm gốc thứ hai về IKE SA 1 của pha thứ nhất và IPsec SA 1 của pha thứ hai, để tạo ra đường hầm IPsec thứ nhất để truyền dịch vụ X2. Khi đường hầm IPsec thứ nhất không khả dụng, trạm gốc thứ nhất khởi tạo việc thương lượng về IKE SA 2 của pha thứ nhất và IPsec SA 2 của pha thứ hai cho cổng bảo mật, và tiếp tục truyền dịch vụ X2 thông qua kết nối đường hầm IPsec thứ hai sau khi thương lượng thành công. Liệu việc thương

lượng về IKE SA của pha thứ nhất có thành công chủ yếu phản ánh liệu kênh vật lý giữa các trạm gốc hoặc giữa trạm gốc và cổng bảo mật có được kết nối và khả dụng để truyền thông. Liệu việc thương lượng về IPsec SA của pha thứ hai có thành công chủ yếu phản ánh liệu ACLRULE giữa các trạm gốc hoặc giữa trạm gốc và cổng bảo mật có phù hợp. Trên FIG.3, ACLRULE 2 mà được sử dụng khi trạm gốc thương lượng với cổng bảo mật về IPsec SA 2 bao gồm ACLRULE 1 mà được sử dụng khi các trạm gốc thương lượng về IPsec SA 1, do khoảng truyền địa chỉ IP đến ANY hoặc ANY đến ANY bao gồm khoảng truyền địa chỉ IP đến IP như được mô tả ở trên. Do đó, quan hệ dư thừa tự động có thể được tạo ra giữa đường hầm IPsec thứ hai và đường hầm IPsec thứ nhất, nhờ đó cải thiện độ tin cậy của dịch vụ X2. Có thể được hiểu là, trên FIG.3, ACLRULE chỉ được sử dụng làm ví dụ. Một cách tùy chọn, ACLRULE có thể được thay thế bởi TS. Điều này không bị giới hạn cụ thể trong sáng chế này.

Lưu ý rằng, khi dữ liệu dịch vụ X2 đạt tới cổng bảo mật, cổng bảo mật cũng cần thiết lập đường hầm IPsec thứ hai với trạm gốc thứ hai, để cuối cùng gửi dữ liệu được chuyển tiếp đến trạm gốc thứ hai. Đối với thủ tục cụ thể, tham khảo thủ tục truyền thông giữa trạm gốc thứ nhất và cổng bảo mật. Các chi tiết không được mô tả ở đây.

Theo phương pháp truyền dữ liệu dịch vụ X2 được đề xuất trong phương án này của sáng chế, nếu kết nối đường hầm IPsec được thiết lập tự động giữa các trạm gốc không khả dụng, còn được xác định liệu kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật khả dụng. Nếu kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật khả dụng, dữ liệu dịch vụ X2 được truyền thông qua kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật. Điều này giải quyết vấn đề là sự dư thừa bảo mật không thể tự động đạt được khi dữ liệu dịch vụ X2 được truyền giữa các trạm gốc thông qua kết nối đường hầm IPsec, nhờ đó cải thiện độ tin cậy của việc truyền dữ liệu dịch vụ X2.

FIG.4 là lưu đồ giản lược của phương pháp truyền dịch vụ X2 khác theo phương án của sáng chế. Phương pháp có thể được áp dụng với kiến trúc mạng trên FIG.1. Trạm gốc thứ nhất và trạm gốc thứ hai có thể là các trạm gốc liền kề,

hoặc có thể là các trạm gốc không liền kề. Như được thể hiện trên FIG.4, phương pháp có thể bao gồm bước S401 đến bước S404 sau đây.

Bước S401: Nếu kết nối đường hầm IPsec thứ nhất không khả dụng, trạm gốc thứ nhất nhận biết liệu kết nối đường hầm IPsec thứ hai giữa trạm gốc thứ nhất và cổng bảo mật có khả dụng.

Bước S402: Truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ hai nếu kết nối đường hầm IPsec thứ hai khả dụng.

Cụ thể, đối với bước S401 và bước S402, tham khảo bước S201 và bước S202 trong phương án trên FIG.2.

Bước S403: Xác định liệu kết nối đường hầm IPsec thứ nhất có khả dụng.

Cụ thể, mặc dù dịch vụ X2 giữa trạm gốc thứ nhất và trạm gốc thứ hai hiện tại được truyền thông qua kết nối đường hầm IPsec thứ hai giữa trạm gốc thứ nhất và cổng bảo mật, do hiệu quả truyền dẫn của đường hầm IPsec thứ nhất trực tiếp hiển nhiên cao hơn của đường hầm IPsec thứ hai, trong phương án này của sáng chế, việc khởi tạo thủ tục thương lượng đường hầm IPsec cho trạm gốc thứ hai vẫn được duy trì trong quy trình truyền dữ liệu dịch vụ X2 giữa trạm gốc thứ nhất và cổng bảo mật. Trong ví dụ cụ thể, trạm gốc thứ nhất khởi tạo gói tin yêu cầu thiết lập đường hầm IPsec cho trạm gốc thứ hai; và giám sát liệu gói tin phản hồi thiết lập IPsec được phản hồi bởi trạm gốc thứ hai được thu. Nếu gói tin phản hồi thiết lập đường hầm IPsec được phản hồi bởi trạm gốc thứ hai được thu, đường hầm IPsec thứ nhất khả dụng. Ngoài ra, trạm gốc thứ nhất có thể khởi tạo gói tin yêu cầu thiết lập đường hầm IPsec định kỳ hoặc theo quy tắc thời gian cụ thể. Có thể được hiểu là, gói tin phản hồi thiết lập IPsec bao gồm gói tin phản hồi thương lượng IKE SA của pha thiết lập đường hầm IPsec thứ nhất và gói tin phản hồi thương lượng IPsec SA của pha thiết lập đường hầm IPsec thứ hai.

Bước S404: Chuyển dữ liệu dịch vụ X2 được truyền thông qua kết nối đường hầm IPsec thứ hai sang đường hầm IPsec thứ nhất để truyền dẫn nếu kết nối đường hầm IPsec thứ nhất khả dụng.

Cụ thể, nếu gói tin phản hồi thiết lập IPsec được phản hồi bởi trạm gốc thứ hai được thu, đường hầm IPsec thứ nhất khả dụng. Nếu gói tin phản hồi thiết lập IPsec được phản hồi bởi trạm gốc thứ hai không được thu, đường hầm IPsec thứ nhất không khả dụng. Theo sáng chế, nếu kết nối đường hầm IPsec trực tiếp không khả dụng, được xem xét theo cách ưu tiên để đảm bảo rằng dịch vụ X2 của trạm gốc thứ nhất có thể được thực hiện thông thường. Tuy nhiên, nếu IPsec trực tiếp khả dụng, hiệu quả truyền dẫn được xem xét theo cách ưu tiên. Cụ thể, mỗi lần so khớp gói tin được thực hiện cho dữ liệu dịch vụ X2, được nhận biết xem liệu kết nối đường hầm IPsec thứ nhất có khả dụng. Nếu kết nối đường hầm IPsec thứ nhất khả dụng, nó được dự định, ở thời điểm bất kỳ, chuyển dữ liệu dịch vụ X2 được truyền trên đường hầm IPsec cổng bảo mật ngược trở lại IPsec trực tiếp để truyền dẫn. Có thể được hiểu là, gói dữ liệu được truyền tương ứng với dịch vụ X2 có thể không được gửi lại, và chỉ gói dữ liệu mà chưa được truyền được chuyển đến đường hầm IPsec thứ nhất tương ứng với trạm gốc thứ nhất và trạm gốc thứ hai để gửi lại. Theo cách này, hiệu quả truyền dẫn cao của dịch vụ X2 được đảm bảo nhiều nhất có thể trong khi đảm bảo là dịch vụ X2 có thể được truyền.

Một cách tùy chọn, trạm gốc thứ nhất loại bỏ dữ liệu dịch vụ X2 nếu không có kết nối đường hầm IPsec thứ nhất cũng không có kết nối đường hầm IPsec thứ hai khả dụng. Khi không có kết nối đường hầm IPsec trực tiếp cũng không có kết nối đường hầm IPsec cổng bảo mật không khả dụng, gói dữ liệu tương ứng với dịch vụ X2 cần được loại bỏ, do nếu không có cả hai đường hầm truyền dẫn không khả dụng, rủi ro bảo mật bị gây ra nếu gói dữ liệu không được loại bỏ. Điều này ngăn gói dữ liệu không bị chặn bởi thiết bị không an toàn khác.

Một cách tùy chọn, trạm gốc thứ nhất truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ nhất nếu kết nối đường hầm IPsec thứ nhất khả dụng. Ví dụ, trạm gốc thứ nhất truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ nhất nếu cả đường hầm IPsec thứ nhất và đường hầm IPsec thứ hai khả dụng. Nếu cả hai loại đường hầm IPsec khả dụng để truyền dẫn, đường hầm IPsec thứ nhất với tốc độ truyền cao hơn và hiệu quả cao hơn

được ưu tiên sử dụng.

Lưu ý rằng, khi dữ liệu dịch vụ X2 đạt tới cổng bảo mật, cổng bảo mật cũng cần thiết lập đường hầm IPsec thứ hai với trạm gốc thứ hai, để cuối cùng gửi dữ liệu được chuyển tiếp đến trạm gốc thứ hai. Đối với thủ tục cụ thể, tham khảo thủ tục truyền thông giữa trạm gốc thứ nhất và cổng bảo mật. Các chi tiết không được mô tả ở đây.

Theo phương pháp truyền dữ liệu dịch vụ X2 và thiết bị mà được đề xuất trong phương án này của sáng chế, nếu kết nối đường hầm IPsec được thiết lập tự động giữa các trạm gốc không khả dụng, còn được xác định liệu kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật có khả dụng. Nếu kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật khả dụng, dữ liệu dịch vụ X2 được truyền thông qua kết nối đường hầm IPsec giữa trạm gốc và cổng bảo mật. Điều này giải quyết vấn đề là sự dư thừa bảo mật không thể tự động đạt được khi dữ liệu dịch vụ X2 được truyền giữa các trạm gốc thông qua kết nối đường hầm IPsec, nhờ đó cải thiện độ tin cậy của việc truyền dữ liệu dịch vụ X2.

FIG.5 là sơ đồ cấu trúc giản lược của thiết bị truyền dịch vụ X2 theo phương án của sáng chế. Như được thể hiện trên FIG.5, trạm gốc thứ nhất 10 bao gồm môđun nhận biết 101 và môđun truyền thứ nhất 102.

Môđun nhận biết 101 được tạo cấu hình để: nếu kết nối đường hầm IPsec thứ nhất không khả dụng, nhận biết liệu kết nối đường hầm IPsec thứ hai giữa trạm gốc thứ nhất và cổng bảo mật có khả dụng, trong đó kết nối đường hầm IPsec thứ nhất là kết nối đường hầm IPsec được thiết lập giữa trạm gốc thứ nhất và trạm gốc thứ hai, và trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc thứ hai thông qua kết nối đường hầm IPsec thứ hai. Môđun truyền thứ nhất 102 được tạo cấu hình để truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ hai nếu kết nối đường hầm IPsec thứ hai khả dụng.

Cụ thể, trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc khác bất kỳ thông qua kết nối đường hầm IPsec thứ hai.

Cụ thể, như được thể hiện trên FIG.5, thiết bị 10 còn bao gồm:

môđun xác định 103, được tạo cấu hình để xác định liệu kết nối đường hầm IPsec thứ nhất có khả dụng; và môđun chuyển đổi 104, được tạo cấu hình để chuyển dữ liệu dịch vụ X2 được truyền thông qua kết nối đường hầm IPsec thứ hai sang đường hầm IPsec thứ nhất để truyền dẫn nếu kết nối đường hầm IPsec thứ nhất khả dụng.

Ngoài ra, môđun xác định 103 bao gồm: bộ yêu cầu, được tạo cấu hình để khởi tạo gói tin yêu cầu thiết lập đường hầm IPsec cho trạm gốc thứ hai; và bộ xác định, được tạo cấu hình để: nếu gói tin phản hồi thiết lập đường hầm IPsec được phản hồi bởi trạm gốc thứ hai được thu, xác định rằng đường hầm IPsec thứ nhất khả dụng.

Hơn nữa, như được thể hiện trên FIG.5, thiết bị 10 còn bao gồm môđun loại bỏ 105, được tạo cấu hình để loại bỏ dữ liệu dịch vụ X2 nếu không có kết nối đường hầm IPsec thứ nhất cũng không có kết nối đường hầm IPsec thứ hai khả dụng.

Hơn nữa, như được thể hiện trên FIG.5, thiết bị 10 còn bao gồm môđun truyền thứ hai 106, được tạo cấu hình để truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ nhất nếu kết nối đường hầm IPsec thứ nhất khả dụng.

Lưu ý rằng, đối với các chức năng của các môđun chức năng trong thiết bị mạng 10 được mô tả trông phương án này của sáng chế, có thể tham chiếu tới các phần mô tả liên quan của trạm gốc thứ nhất tương ứng trong các phương án được thể hiện trên FIG.1 đến FIG.4. Các chi tiết không được mô tả ở đây.

FIG.6 là sơ đồ cấu trúc giản lược của thiết bị mạng theo phương án của sáng chế. Thiết bị mạng có thể là trạm gốc thứ nhất. Như được thể hiện trên FIG.6, thiết bị mạng 20 bao gồm bộ xử lý 201, bộ nhớ 202, và bộ thu phát 203. Bộ xử lý 201, bộ nhớ 202, và bộ thu phát 203 có thể được kết nối bằng cách sử dụng kênh truyền hoặc theo cách thức khác.

Một cách tùy chọn, thiết bị mạng 20 có thể còn bao gồm giao diện mạng 204 và môđun cấp nguồn 205.

Bộ xử lý 201 có thể là bộ xử lý trung tâm (CPU), bộ xử lý mục đích chung, bộ xử lý tín hiệu số (DSP), mạch tích hợp ứng dụng riêng (ASIC), mảng cổng có thể lập trình dạng trường (FPGA) hoặc thiết bị logic có thể lập trình khác, thiết bị logic bán dẫn, thành phần phần cứng, hoặc kết hợp bất kỳ của chúng. Bộ xử lý 201 có thể thực hiện hoặc thực thi các khối logic, các môđun, và các mạch ví dụ khác nhau được mô tả viện dẫn tới nội dung được bộc lộ trong sáng chế. Theo cách khác, bộ xử lý có thể là kết hợp mà thực hiện chức năng điện toán, ví dụ, kết hợp bao gồm một hoặc nhiều bộ vi xử lý, hoặc kết hợp của DSP và bộ vi xử lý.

Bộ nhớ 202 được tạo cấu hình để lưu trữ chỉ dẫn. Trong quá trình thực hiện cụ thể, bộ nhớ 202 có thể là bộ nhớ chỉ đọc (Read-Only Memory, ROM) hoặc bộ nhớ truy nhập ngẫu nhiên (Random Access Memory, RAM). Trong phương án này của sáng chế, bộ nhớ 202 được tạo cấu hình để lưu trữ mã chương trình thiết lập kết nối phiên.

Bộ thu phát 203 được tạo cấu hình để thu/gửi tín hiệu, và được tạo cấu hình để truyền thông với thiết bị mạng khác, ví dụ, thu hoặc gửi dữ liệu từ hoặc đến trạm gốc khác, cổng bảo mật, hoặc tương tự.

Giao diện mạng 204 được sử dụng bởi thiết bị mạng 20 để thực hiện truyền thông dữ liệu với thiết bị khác. Giao diện mạng 204 có thể là giao diện có dây hoặc giao diện không dây, và thực hiện kết nối truyền thông giữa thiết bị mạng cục bộ và thiết bị mạng khác, ví dụ thiết bị đầu cuối, trạm gốc, máy chủ, hoặc cổng bảo mật, qua mạng có dây hoặc không dây.

Môđun cấp nguồn 205 được tạo cấu hình để cấp nguồn đến mỗi môđun trong thiết bị mạng 20.

Bộ xử lý 201 được tạo cấu hình để gọi ra lệnh được lưu trữ trong bộ nhớ 202 để thực hiện các thao tác sau đây:

Bộ xử lý 201 được tạo cấu hình để: nếu kết nối đường hầm IPsec thứ nhất không khả dụng, nhận biết liệu kết nối đường hầm IPsec thứ hai giữa trạm gốc thứ nhất và cổng bảo mật có khả dụng, trong đó kết nối đường hầm IPsec thứ

nhất là kết nối đường hầm IPsec được thiết lập giữa trạm gốc thứ nhất và trạm gốc thứ hai, và trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc thứ hai thông qua kết nối đường hầm IPsec thứ hai. Bộ thu phát 203 được tạo cấu hình để gửi và/hoặc thu dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ hai nếu kết nối đường hầm IPsec thứ hai khả dụng.

Cụ thể, trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc khác bất kỳ thông qua kết nối đường hầm IPsec thứ hai.

Ngoài ra, bộ xử lý 201 còn được tạo cấu hình để: sau khi dữ liệu dịch vụ X2 được truyền thông qua kết nối đường hầm IPsec thứ hai, xác định liệu kết nối đường hầm IPsec thứ nhất khả dụng. Bộ thu phát còn được tạo cấu hình để chuyển dữ liệu dịch vụ X2 được truyền thông qua kết nối đường hầm IPsec thứ hai sang đường hầm IPsec thứ nhất để truyền dẫn nếu kết nối đường hầm IPsec thứ nhất khả dụng.

Hơn nữa, bộ xử lý 201 được tạo cấu hình để xác định liệu kết nối đường hầm IPsec thứ nhất có khả dụng cụ thể là: khởi tạo gói tin yêu cầu thiết lập đường hầm IPsec cho trạm gốc thứ hai bằng cách sử dụng bộ thu phát 203; và nếu thu, bằng cách sử dụng bộ thu phát 203, gói tin phản hồi thiết lập đường hầm IPsec được phản hồi bởi trạm gốc thứ hai, xác định rằng đường hầm IPsec thứ nhất khả dụng.

Hơn nữa, bộ xử lý 201 còn được tạo cấu hình để loại bỏ dữ liệu dịch vụ X2 nếu không có kết nối đường hầm IPsec thứ nhất cũng không có kết nối đường hầm IPsec thứ hai khả dụng.

Hơn nữa, bộ xử lý 201 còn được tạo cấu hình để: nếu kết nối đường hầm IPsec thứ nhất khả dụng, xác định để truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ nhất. Bộ thu phát 203 còn được tạo cấu hình để truyền dữ liệu dịch vụ X2 thông qua kết nối đường hầm IPsec thứ nhất.

Lưu ý rằng, đối với các chức năng của các môđun chức năng trong thiết bị mạng 20 được mô tả trông phương án này của sáng chế, tham khảo các phần mô tả liên quan của trạm gốc thứ nhất tương ứng trong các phương án được thể hiện

trên FIG.1 đến FIG.4. Các chi tiết không được mô tả ở đây.

Phương án của sáng chế còn đề xuất phương tiện lưu trữ đọc được bởi máy tính. Phương tiện lưu trữ đọc được bằng máy tính có thể lưu trữ chương trình. Khi chương trình được thực thi, một số hoặc tất cả các bước của phương pháp truyền dịch vụ X2 bất kỳ được ghi trong các phương án phương pháp nêu trên được thực hiện.

Mặc dù sáng chế được mô tả ở đây viện dẫn tới các phương án, nhưng trong quy trình thực hiện sáng chế mà yêu cầu bảo hộ, người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể hiểu và thực hiện cải biến khác của các phương án được bộc lộ bằng cách xem các hình vẽ kèm theo, nội dung được bộc lộ, và các yêu cầu bảo hộ kèm theo. Trong các yêu cầu bảo hộ, thuật ngữ "bao gồm" không loại trừ thành phần khác hoặc bước khác, và mạo từ tiếng Anh "a/an" khi được dịch sang tiếng Việt hoặc "một" không loại trừ trường hợp "nhiều". Bộ xử lý đơn hoặc bộ phận khác có thể thực hiện các chức năng được liệt kê trong các yêu cầu bảo hộ. Một số biện pháp được ghi trong các điểm yêu cầu bảo hộ kèm theo là khác nhau, nhưng việc này không có nghĩa là các biện pháp này không thể được kết hợp để tạo ra hiệu quả tốt hơn.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật cần hiểu rằng các phương án của sáng chế có thể được đề xuất như là phương pháp, thiết bị, hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể sử dụng dạng của các phương án chỉ phần cứng, các phương án chỉ phần mềm, hoặc các phương án với kết hợp của phần cứng và phần mềm. Ngoài ra, sáng chế có thể sử dụng dạng của sản phẩm chương trình máy mà được thực hiện trên một hoặc nhiều phương tiện lưu trữ có thể sử dụng bởi máy tính (bao gồm nhưng không bị giới hạn ở bộ nhớ đĩa từ, CD-ROM, bộ nhớ quang, và loại tương tự) mà chứa mã chương trình có thể sử dụng bởi máy tính. Chương trình máy tính được lưu trữ/được phân phối trong phương tiện thích hợp và được cung cấp cùng với phần cứng khác hoặc được sử dụng như một phần của phần cứng, hoặc có thể được phân phối ở dạng khác, ví dụ, bằng cách sử dụng Internet hoặc hệ thống viễn thông không dây hoặc có dây khác.

Sáng chế được mô tả dựa vào các lưu đồ và/hoặc các sơ đồ khối của phương pháp, thiết bị, và sản phẩm chương trình máy tính theo các phương án của sáng chế. Lưu ý rằng các lệnh chương trình máy tính có thể được sử dụng để thực hiện mỗi xử lý và/hoặc mỗi khối trong các lưu đồ và/hoặc các sơ đồ khối và kết hợp của xử lý 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 mục đích chung, máy tính dành riêng, bộ xử lý gắn kèm, hoặc bộ xử lý của thiết bị xử lý dữ liệu có thể lập trình khác để tạo ra máy tính, sao cho các lệnh này được thực hiện bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu có thể lập trình khác để tạo ra thiết bị thực hiện chức năng cụ thể trong một hoặc nhiều xử lý trong các lưu đồ và/hoặc một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể còn được lưu trữ trong bộ nhớ đọc được bởi máy tính mà có thể chỉ dẫn máy tính hoặc thiết bị xử lý dữ liệu có thể lập trình khác hoạt động theo cách thức cụ thể, sao cho các lệnh được lưu trữ trong bộ nhớ đọc được bởi máy tính tạo ra mẫu giả mà bao gồm thiết bị chỉ dẫn. Thiết bị chỉ dẫn thực hiện chức năng cụ thể trong một hoặc nhiều xử lý trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể còn được tải trên máy tính hoặc thiết bị xử lý dữ liệu có thể lập trình khác, sao cho các thao tác và các bước được thực hiện trên máy tính hoặc thiết bị có thể lập trình khác, nhờ đó tạo ra xử lý được thực hiện bởi máy tính. Do đó, các lệnh được thực hiện trên máy tính hoặc thiết bị khả trình khác cung cấp các bước để thực hiện chức năng cụ thể trong một hoặc nhiều xử lý trong các lưu đồ và/hoặc trong một hoặc nhiều khối trong các sơ đồ khối.

Mặc dù sáng chế được mô tả viện dẫn tới các dấu hiệu cụ thể và các phương án của chúng, nhưng hiển nhiên là, các cải biến khác và các kết hợp khác có thể được tạo ra với sáng chế mà không đi chệch khỏi tinh thần và phạm vi của sáng chế. Một cách tương ứng, bản mô tả và các hình vẽ kèm theo chỉ là các phần mô tả ví dụ của sáng chế được xác định bởi các yêu cầu bảo hộ kèm theo, và được xem xét bao gồm bất kỳ hoặc tất cả trong số các cải biến, các biến

thể, các kết hợp, hoặc tương đương trong phạm vi của sáng chế. Rõ ràng là, người có hiểu biết trung bình trong lĩnh vực kỹ thuật có thể thực hiện các cải biến và biến thể khác nhau đối với sáng chế mà không đi chệch khỏi bản chất và phạm vi của sáng chế. Theo cách này, sáng chế được dự định bao gồm các cải biến và các biến thể này của sáng chế miễn là chúng nằm trong phạm vi của các yêu cầu bảo hộ của sáng chế và các kỹ thuật tương đương của chúng.

YÊU CẦU BẢO HỘ

1. Thiết bị mạng, bao gồm: bộ xử lý và bộ thu phát, trong đó thiết bị mạng là trạm gốc thứ nhất; trong đó bộ xử lý có cấu trúc để dò tìm rằng kết nối đường ngầm bảo mật giao thức Internet (IPsec-Internet Protocol Security) thứ hai giữa trạm gốc thứ nhất và cổng bảo mật có khả dụng hay không nếu kết nối đường ngầm IPsec thứ nhất là không khả dụng, trong đó kết nối đường ngầm IPsec thứ nhất là kết nối đường ngầm IPsec được thiết lập giữa trạm gốc thứ nhất và trạm gốc thứ hai, và trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc thứ hai thông qua kết nối đường ngầm IPsec thứ hai và bộ thu phát có cấu trúc để gửi và/hoặc thu dữ liệu dịch vụ X2 thông qua kết nối đường ngầm IPsec thứ hai nếu kết nối đường ngầm IPsec thứ hai là khả dụng; và trong đó bộ xử lý còn có cấu trúc để xác định rằng kết nối đường ngầm IPsec thứ nhất có khả dụng hay không sau khi dữ liệu dịch vụ X2 được truyền thông qua kết nối đường ngầm IPsec thứ hai và bộ thu phát còn có cấu trúc để chuyển đổi dữ liệu dịch vụ X2 được truyền thông qua kết nối đường ngầm IPsec thứ hai tới kết nối đường ngầm IPsec thứ nhất để truyền nếu kết nối đường ngầm IPsec thứ nhất là khả dụng.

2. Thiết bị mạng theo điểm 1, trong đó trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với bất kỳ trạm gốc khác thông qua kết nối đường ngầm IPsec thứ hai.

3. Thiết bị mạng theo điểm 1, trong đó bộ xử lý còn có cấu trúc để khởi tạo gói tin yêu cầu thiết lập kết nối đường ngầm IPsec tới trạm gốc thứ hai bằng cách sử dụng bộ thu phát và xác định rằng kết nối đường ngầm IPsec thứ nhất là khả dụng nếu thu, bằng cách sử dụng bộ thu phát, gói tin phản hồi thiết lập kết nối đường ngầm IPsec được phản hồi bởi trạm gốc thứ hai.

4. Thiết bị mạng theo điểm 1, trong đó bộ xử lý còn có cấu trúc để loại bỏ dữ liệu dịch vụ X2 nếu kết nối đường ngầm IPsec thứ nhất và kết nối đường ngầm IPsec thứ hai là không khả dụng.

5. Thiết bị mạng theo điểm 1, trong đó bộ thu phát còn có cấu trúc để truyền dữ

liệu dịch vụ X2 thông qua kết nối đường ngầm IPsec thứ nhất nếu kết nối đường ngầm IPsec thứ nhất là khả dụng.

6. Phương tiện bất biến đọc được bởi máy tính bao gồm các lệnh mà, khi được thực thi bởi bộ xử lý, làm cho bộ xử lý thực hiện các hoạt động truyền, các hoạt động truyền này bao gồm: dò tìm, bởi trạm gốc thứ nhất, rằng kết nối đường ngầm bảo mật giao thức Internet (IPsec-Internet Protocol Security) thứ hai giữa trạm gốc thứ nhất và cổng bảo mật có khả dụng hay không nếu kết nối đường ngầm IPsec thứ nhất là không khả dụng, trong đó kết nối đường ngầm IPsec thứ nhất là kết nối đường ngầm IPsec được thiết lập giữa trạm gốc thứ nhất và trạm gốc thứ hai, và trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với trạm gốc thứ hai thông qua kết nối đường ngầm IPsec thứ hai; truyền dữ liệu dịch vụ X2 thông qua kết nối đường ngầm IPsec thứ hai nếu kết nối đường ngầm IPsec thứ hai là khả dụng; xác định rằng kết nối đường ngầm IPsec thứ nhất có khả dụng hay không sau khi dữ liệu dịch vụ X2 được truyền thông qua kết nối đường ngầm IPsec thứ hai; và chuyển đổi dữ liệu dịch vụ X2 được truyền thông qua kết nối đường ngầm IPsec thứ hai tới kết nối đường ngầm IPsec thứ nhất để truyền nếu kết nối đường ngầm IPsec thứ nhất là khả dụng.

7. Phương tiện bất biến đọc được bởi máy tính theo điểm 6, trong đó trạm gốc thứ nhất có thể truyền dữ liệu dịch vụ X2 với bất kỳ trạm gốc khác thông qua kết nối đường ngầm IPsec thứ hai.

8. Phương tiện bất biến đọc được bởi máy tính theo điểm 6, trong đó bước xác định rằng kết nối đường ngầm IPsec thứ nhất có khả dụng hay không bao gồm: khởi tạo gói tin yêu cầu thiết lập kết nối đường ngầm IPsec tới trạm gốc thứ hai; và xác định rằng kết nối đường ngầm IPsec thứ nhất là khả dụng nếu thu gói tin phản hồi thiết lập kết nối đường ngầm IPsec được phản hồi bởi trạm gốc thứ hai.

9. Phương tiện bất biến đọc được bởi máy tính theo điểm 6, các hoạt động truyền còn bao gồm: loại bỏ, bởi trạm gốc thứ nhất, dữ liệu dịch vụ X2 nếu kết nối đường ngầm IPsec thứ nhất hoặc kết nối đường ngầm IPsec thứ hai không khả dụng.

10. Phương tiện bất biến đọc được bởi máy tính theo điểm 6, các hoạt động

truyền còn bao gồm: truyền, bởi trạm gốc thứ nhất, dữ liệu dịch vụ X2 thông qua kết nối đường ngầm IPsec thứ nhất nếu kết nối đường ngầm IPsec thứ nhất là khả dụng.

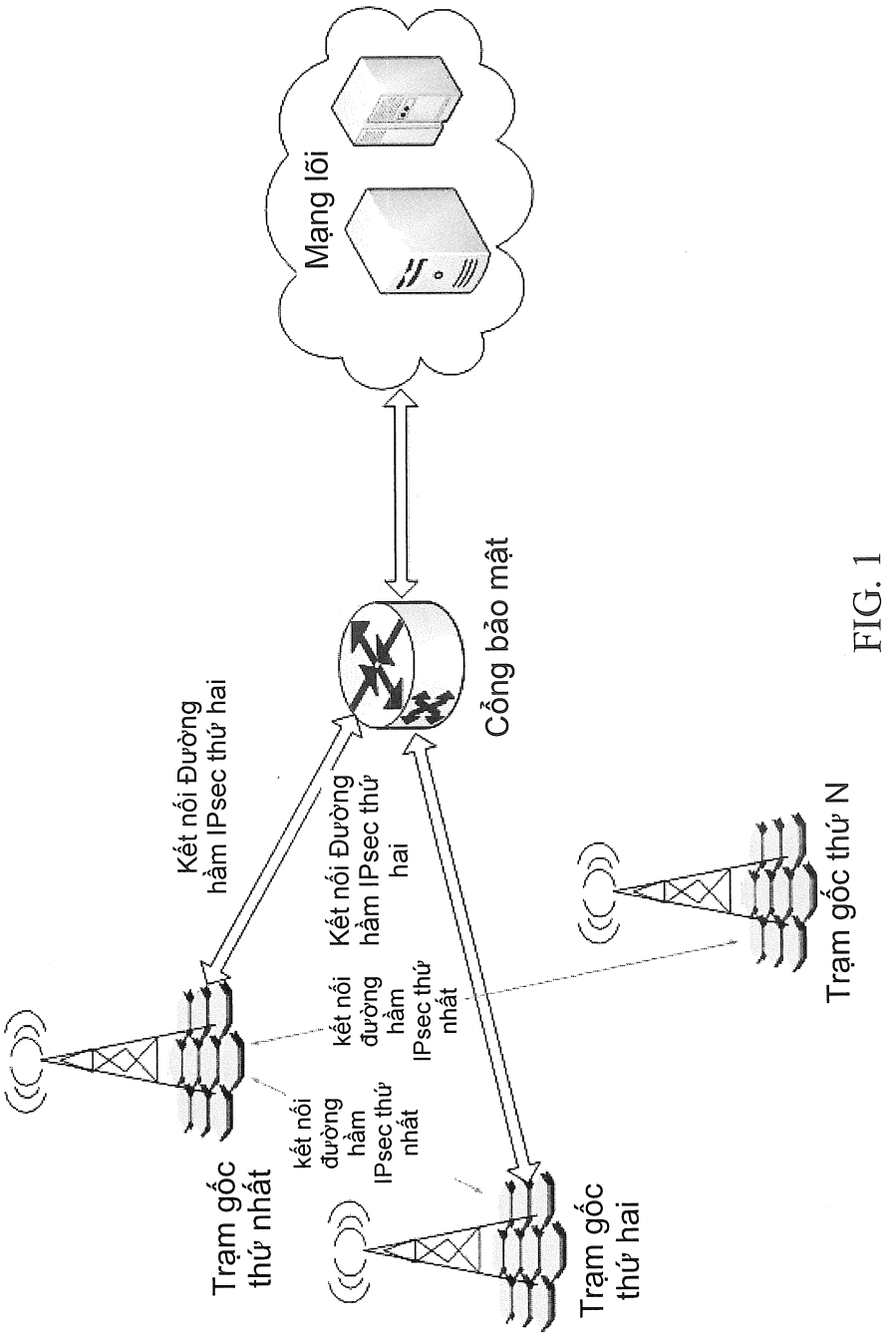

Mạng lõi
Cổng bảo mật
Kết nối Đường hầm IPsec thứ hai
Kết nối Đường hầm IPsec thứ hai
kết nối đường hầm IPsec thứ nhất
kết nối đường hầm IPsec thứ nhất
Trạm gốc thứ nhất
Trạm gốc thứ hai
Trạm gốc thứ N

FIG. 1

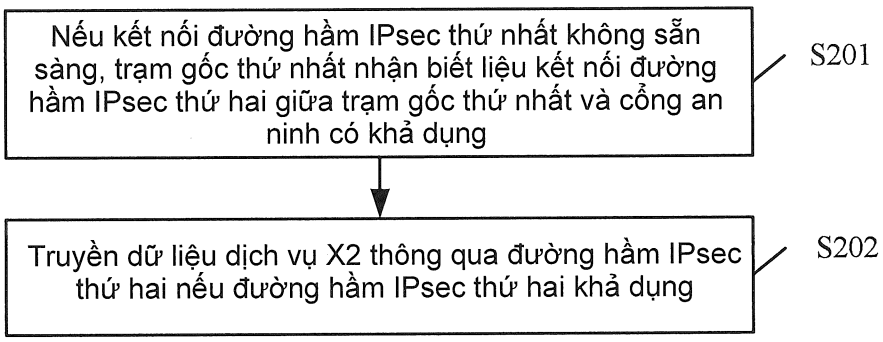

Nếu kết nối đường hầm IPsec thứ nhất không sẵn sàng, trạm gốc thứ nhất nhận biết liệu kết nối đường hầm IPsec thứ hai giữa trạm gốc thứ nhất và cổng an ninh có khả dụng
S201
Truyền dữ liệu dịch vụ X2 thông qua đường hầm IPsec thứ hai nếu đường hầm IPsec thứ hai khả dụng
S202

FIG. 2

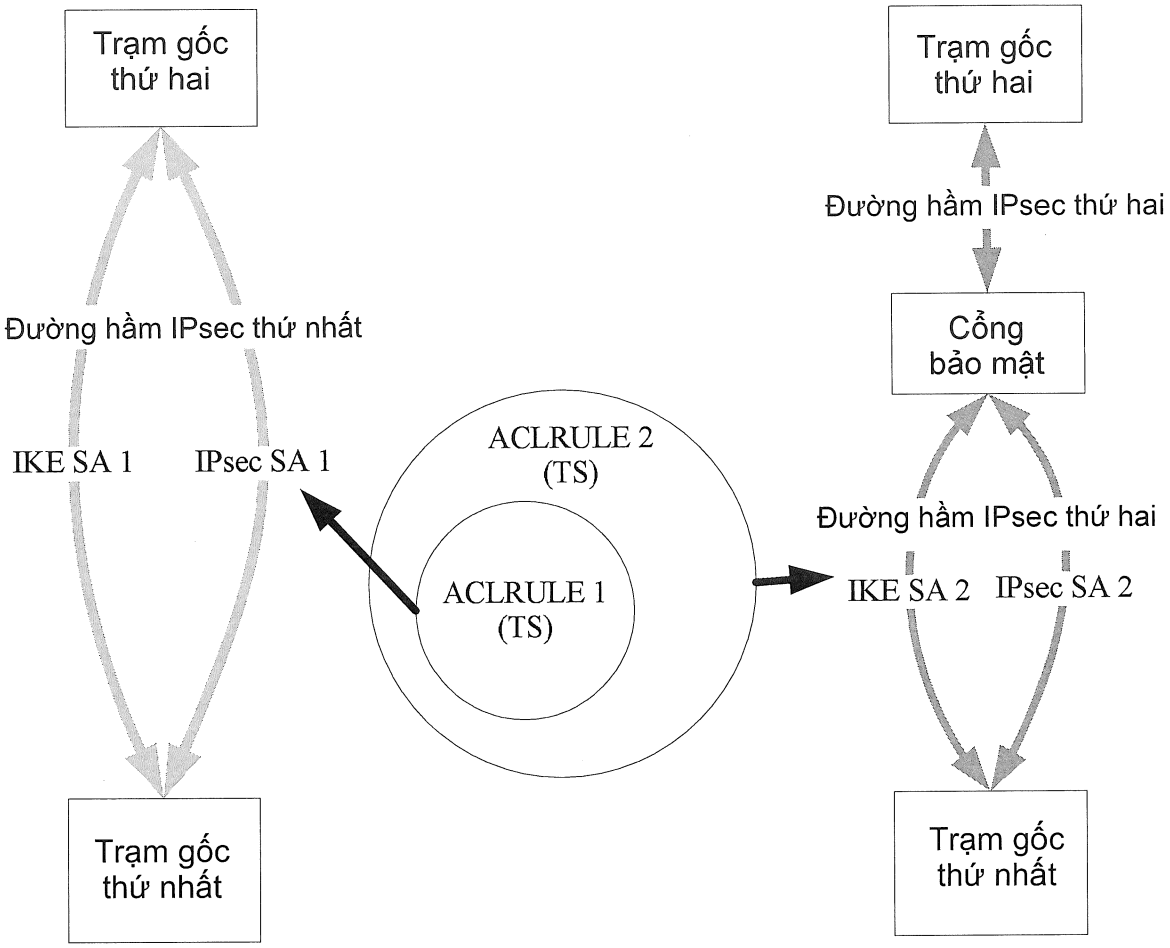

Trạm gốc thứ hai
Đường hầm IPsec thứ nhất
IKE SA 1
IPsec SA 1
Trạm gốc thứ nhất
ACLRULE 2 (TS)
ACLRULE 1 (TS)
Trạm gốc thứ hai
Đường hầm IPsec thứ hai
Cổng bảo mật
Đường hầm IPsec thứ hai
IKE SA 2
IPsec SA 2
Trạm gốc thứ nhất

FIG. 3

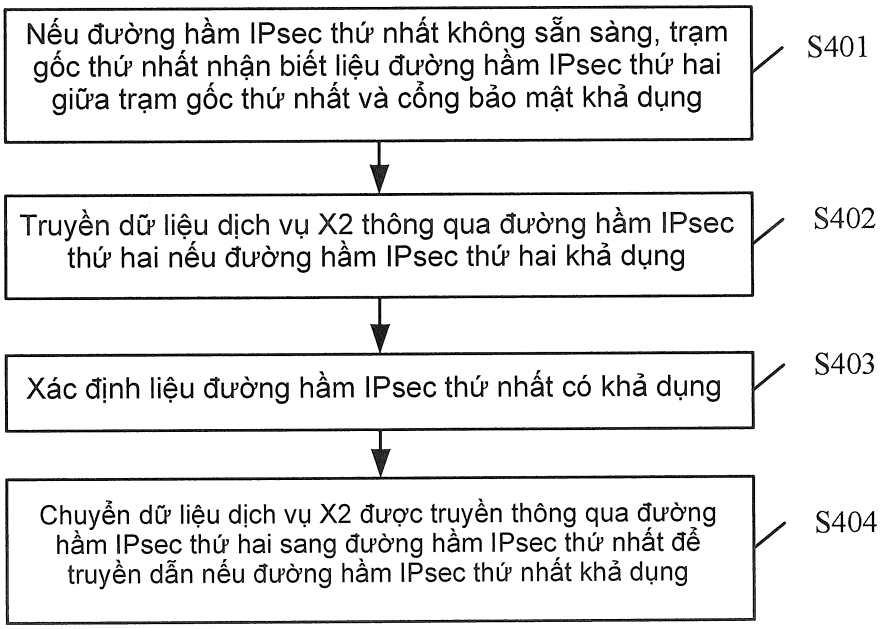

Nếu đường hầm IPsec thứ nhất không sẵn sàng, trạm gốc thứ nhất nhận biết liệu đường hầm IPsec thứ hai giữa trạm gốc thứ nhất và cổng bảo mật khả dụng
S401
Truyền dữ liệu dịch vụ X2 thông qua đường hầm IPsec thứ hai nếu đường hầm IPsec thứ hai khả dụng
S402
Xác định liệu đường hầm IPsec thứ nhất có khả dụng
S403
Chuyển dữ liệu dịch vụ X2 được truyền thông qua đường hầm IPsec thứ hai sang đường hầm IPsec thứ nhất để truyền dẫn nếu đường hầm IPsec thứ nhất khả dụng
S404

FIG. 4

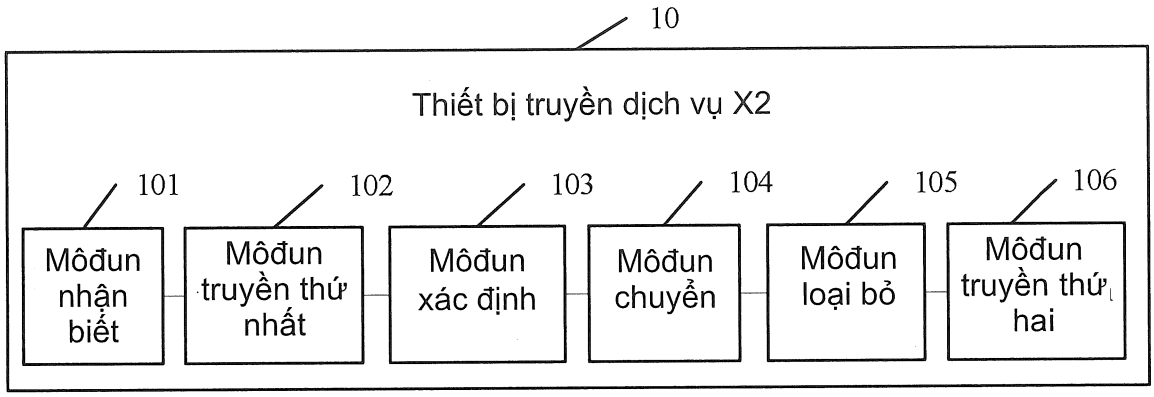

10
Thiết bị truyền dịch vụ X2
101
Môđun nhận biết
102
Môđun truyền thứ nhất
103
Môđun xác định
104
Môđun chuyển
105
Môđun loại bỏ
106
Môđun truyền thứ hai

FIG. 5

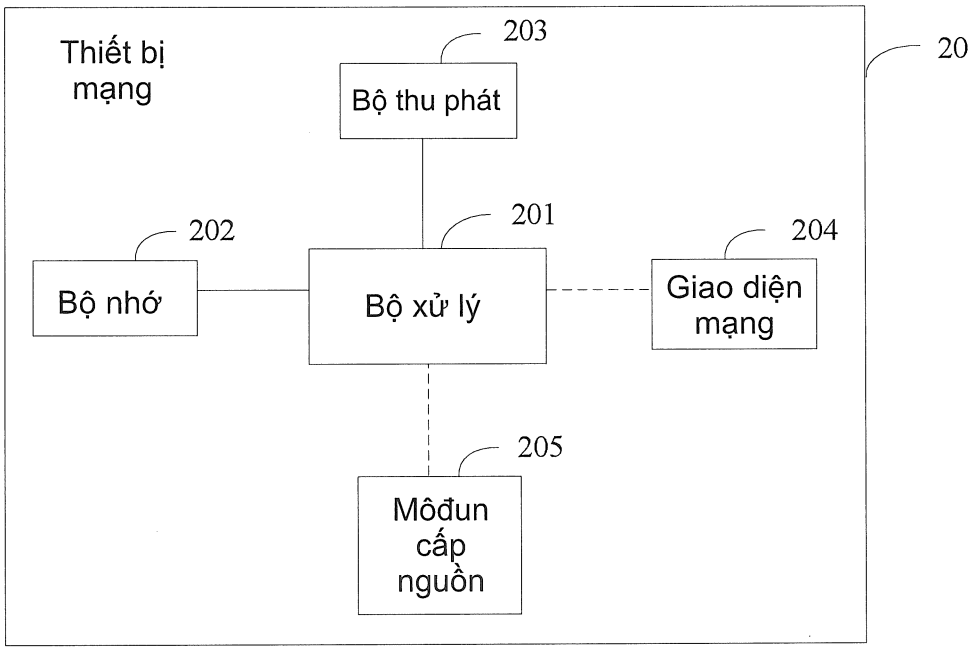

Thiết bị mạng
203
Bộ thu phát
20
202
Bộ nhớ
201
Bộ xử lý
204
Giao diện mạng
205
Môđun cấp nguồn

FIG. 6