(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) **1-0050322**

(51)[2021.01] **H04W 12/121**; H04W 12/61

(13) **B**

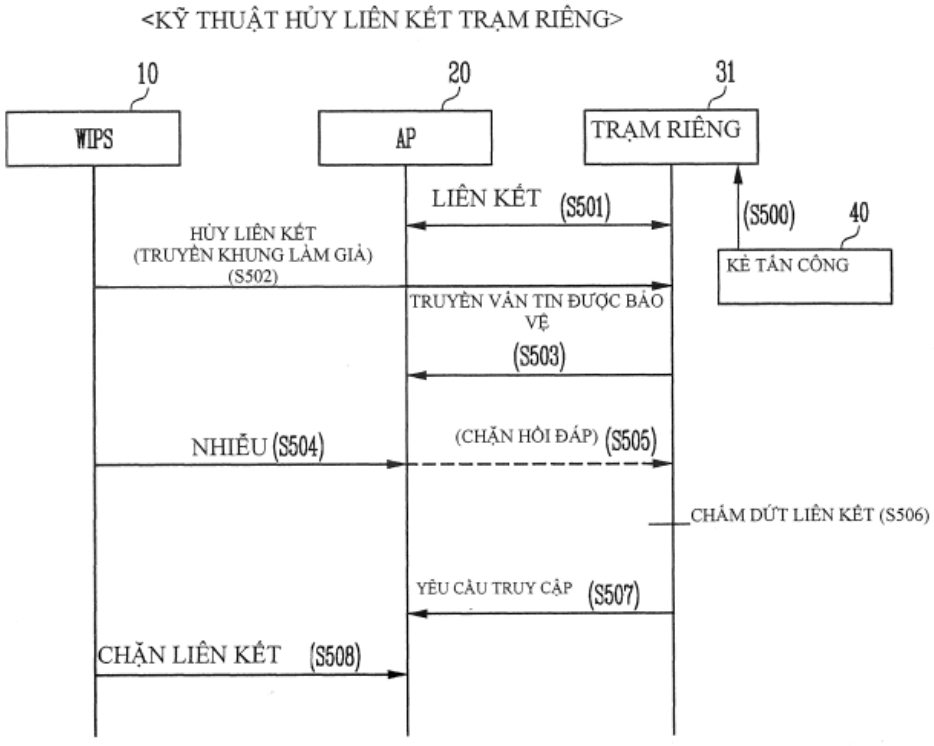
(21) 1-2022-05951
(22) 03/04/2020
(86) PCT/KR2020/004571 03/04/2020
(87) WO 2021/182667 16/09/2021
(30) 10-2020-0030422 11/03/2020 KR
(45) 25/08/2025 449
(43) 25/11/2022 416A
(73) SECUI CORPORATION (KR)
3rd, 5th, 6th Floors 51, Jong-ro, Jongno-gu, Seoul 03161, Republic of Korea
(72) HAM, Seong Yun (KR).
(74) Công ty TNHH Quốc tế D &N (D&N INTERNATIONAL CO.,LTD.)

(54) HỆ THỐNG MẠNG KHÔNG DÂY, PHƯƠNG PHÁP VẬN HÀNH HỆ THỐNG MẠNG KHÔNG DÂY VÀ HỆ THỐNG NGĂN CHẶN XÂM NHẬP KHÔNG DÂY

(21) 1-2022-05951

(57) Sáng chế đề cập đến hệ thống ngăn chặn xâm nhập không dây, hệ thống mạng không dây bao gồm hệ thống ngăn chặn xâm nhập không dây, và phương pháp vận hành hệ thống mạng không dây. Trong số này, hệ thống ngăn chặn xâm nhập không dây bao gồm điểm truy cập, nhiều trạm được tạo cấu hình để truyền/nhận khung không dây đến/từ điểm truy cập qua mạng không dây, và hệ thống ngăn chặn xâm nhập không dây được tạo cấu hình để giám sát khung không dây, trong đó hệ thống ngăn chặn xâm nhập không dây truyền yêu cầu hủy liên kết đến trạm riêng, trong số nhiều trạm, và ngăn không cho điểm truy cập đáp lại trạm riêng.

Fig.10



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống ngăn chặn xâm nhập không dây (wireless intrusion prevention system - WIPS), hệ thống mạng không dây bao gồm hệ thống ngăn chặn xâm nhập không dây, và phương pháp vận hành hệ thống mạng không dây.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển và phổ biến nhanh chóng của Internet, các môi trường mạng được mở rộng, và hình thức của Internet trở nên phức tạp hơn do việc truy cập Internet dễ dàng và thuận tiện và các loại hình dịch vụ khác nhau được cung cấp qua Internet. Tuy nhiên, do nhiều kiểu tấn công mạng, như virut, bẻ khóa (hack), xâm nhập hệ thống, chiếm quyền quản trị viên hệ thống, che giấu xâm nhập, và tấn công từ chối dịch vụ được thực hiện qua Internet, Internet luôn tiềm ẩn nguy cơ về bẻ khóa, do đó tăng thêm các vụ xâm phạm Internet, tăng dần quy mô thiệt hại đối với các tổ chức công cộng, cơ sở hạ tầng xã hội, và các tổ chức tài chính, và cũng tăng ảnh hưởng của chúng. Để giải quyết các vấn đề bảo mật Internet như vậy, nhu cầu về công nghệ an ninh mạng, như chương trình chống virut, tường lửa, quản lý bảo mật tích hợp, và hệ thống phát hiện xâm nhập, đã được đặt lên hàng đầu.

Hệ thống mạng không dây để truyền thông Internet không dây bao gồm Điểm truy cập (Access Point - AP) Mạng cục bộ (Local Area Network - LAN) không dây và trạm LAN không dây. AP được dùng bằng cách lắp đặt một phần thiết bị được gọi là thiết bị điểm truy cập.

Gần đây, hệ thống mạng tích hợp sử dụng mạng có dây và không dây đã được phát triển và ứng dụng rộng rãi. Thật khó để chặn một cách tin cậy lưu lượng truy cập có hại đến

theo cách có dây, nhưng càng khó hơn để chặn một cách tin cậy lưu lượng có hại đến theo cách không dây. Để giải quyết vấn đề này, Hệ thống ngăn chặn Xâm nhập Không dây (WIPS) đang được phát triển liên tục. WIPS là hệ thống phát hiện và chặn sự xâm nhập không dây, như AP (giả mạo - rouge) trái phép hoặc cuộc tấn công Từ chối Dịch vụ (Denial of Service - DoS), thông qua giám sát khu vực không dây.

Bản chất kỹ thuật của sáng chế

Vấn đề kỹ thuật

Các phương án khác nhau của sáng chế hướng đến WIPS, hệ thống này chặn quyền truy cập bởi trạm riêng khi trạm riêng truy cập vào AP qua khung hủy xác thực được bảo vệ, như trong trường hợp của, ví dụ, công nghệ IEEE 802.11w, và hệ thống mạng không dây bao gồm WIPS.

Các mục đích của sáng chế không giới hạn ở mục đích được mô tả ở trên, và các mục đích khác, không được mô tả ở đây, có thể được người có hiểu biết trung bình trong lĩnh vực kỹ thuật này hiểu rõ từ phần mô tả sau.

Giải pháp kỹ thuật

Hệ thống mạng không dây theo một phương án của sáng chế để đạt được mục đích ở trên có thể bao gồm điểm truy cập, nhiều trạm được tạo cấu hình để truyền/nhận khung không dây đến/từ điểm truy cập qua mạng không dây, và hệ thống ngăn chặn xâm nhập không dây được tạo cấu hình để giám sát khung không dây, trong đó hệ thống ngăn chặn xâm nhập không dây truyền yêu cầu hủy liên kết cho trạm riêng, trong số nhiều trạm, và ngăn điểm truy cập đáp lại trạm riêng.

Hệ thống ngăn chặn xâm nhập không dây có thể truyền tín hiệu nhiễu đến điểm truy cập để ngăn điểm truy cập đáp lại trạm riêng.

Tín hiệu nhiễu có thể bao gồm khung Sẵn sàng để Gửi (Clear to Send - CTS) hoặc

khung Yêu cầu để Gửi (Request to Send - RTS).

Tín hiệu nhiễu có thể bao gồm tín hiệu để làm tăng mức tắc nghẽn của điểm truy cập.

Tín hiệu nhiễu có thể bao gồm gói giả mạo.

Gói giả mạo có thể bao gồm khung yêu cầu liên kết mới (khung liên kết - Association frame), khung yêu cầu tái liên kết (khung tái liên kết - Re-Association frame), hoặc khung yêu cầu hủy liên kết cho trạng thái liên kết hiện tại (khung hủy liên kết - Dis-Association frame).

Trạm riêng có thể truyền vấn tin được bảo vệ đến điểm truy cập để đáp lại yêu cầu hủy liên kết.

Trạm riêng có thể lệnh cho điểm truy cập đáp lại vấn tin được bảo vệ trong thời gian thứ nhất định trước, và trạm riêng có thể bị chấm dứt mối liên kết với điểm truy cập khi không nhận được hồi đáp trong thời gian thứ nhất.

Trạm riêng có thể gửi khung yêu cầu xác thực đến điểm truy cập sau khi chấm dứt mối liên kết với điểm truy cập.

Hệ thống ngăn chặn xâm nhập không dây có thể gửi khung hủy xác thực đến điểm truy cập hoặc trạm riêng sau khi khung yêu cầu xác thực được gửi đi.

Trạm riêng có thể là trạm kết nối với trạm trái phép hoặc kẻ tấn công trái phép qua mạng.

Mạng không dây có thể bao gồm công nghệ IEEE 802.11w.

Phương pháp vận hành hệ thống mạng không dây theo một phương án khác của sáng chế để thực hiện mục đích ở trên có thể bao gồm bước duy trì, bởi điểm truy cập, mối liên kết với trạm riêng, trong số nhiều trạm được tạo cấu hình để truyền/nhận khung không dây đến/từ điểm truy cập qua mạng không dây, và truyền, bởi hệ thống ngăn chặn xâm nhập không dây được tạo cấu hình để giám sát khung không dây, tín hiệu nhiễu để ngăn điểm truy

cập đáp lại trạm riêng hoặc ngăn điểm truy cập truyền vấn tin được bảo vệ cho trạm riêng.

Phương pháp vận hành hệ thống mạng không dây có thể bao gồm bước truyền, bởi hệ thống ngăn chặn xâm nhập không dây được tạo cấu hình để giám sát khung không dây, yêu cầu hủy liên kết với trạm riêng, truyền, bởi trạm riêng, vấn tin được bảo vệ đến điểm truy cập, lệnh cho, bởi trạm riêng, điểm truy cập đáp lại vấn tin được bảo vệ trong thời gian thứ nhất định trước, và khi không nhận được hồi đáp trong thời gian thứ nhất, chấm dứt, bởi trạm riêng, liên kết với điểm truy cập.

Phương pháp vận hành hệ thống mạng không dây có thể bao gồm thêm bước, sau khi chấm dứt liên kết với điểm truy cập, gửi, bởi trạm riêng, khung yêu cầu xác thực đến điểm truy cập và sau khi khung yêu cầu xác thực được gửi đi, gửi, bởi hệ thống ngăn chặn xâm nhập không dây, khung hủy xác thực đến điểm truy cập hoặc trạm riêng.

Phương pháp vận hành hệ thống mạng không dây có thể bao gồm bước truyền, bởi trạm riêng, yêu cầu truy cập đến điểm truy cập, trong đó tín hiệu nhiễu bao gồm tín hiệu để ngăn điểm truy cập truyền yêu cầu từ chối truy cập đến trạm riêng hoặc ngăn điểm truy cập truyền vấn tin được bảo vệ đến trạm riêng.

Phương pháp vận hành hệ thống mạng không dây có thể bao gồm thêm bước truyền, bởi hệ thống ngăn chặn xâm nhập không dây, yêu cầu truy cập đến điểm truy cập, trong đó tín hiệu nhiễu bao gồm tín hiệu để ngăn điểm truy cập truyền vấn tin được bảo vệ đến trạm riêng.

Hệ thống ngăn chặn xâm nhập không dây theo một phương án của sáng chế để đạt được mục đích ở trên có thể bao gồm thiết bị cảm biến được tạo cấu hình để giám sát khung không dây mà được truyền/nhận giữa điểm truy cập và nhiều trạm qua mạng không dây và xử lý thông tin dựa trên khung không dây, và máy chủ được tạo cấu hình để xác định xem liệu điểm truy cập và nhiều trạm có trái phép và đang hoạt động bất thường hay không, dựa trên thông tin đã xử lý, trong đó hệ thống ngăn chặn xâm nhập không dây bao gồm chức

năng cung cấp tín hiệu nhiễu để chấm dứt liên kết của trạm riêng, trong số nhiều trạm, với điểm truy cập.

Hệ thống ngăn chặn xâm nhập không dây có thể bao gồm thêm chức năng gửi khung hủy xác thực đến điểm truy cập hoặc trạm riêng khi trạm riêng gửi khung yêu cầu xác thực đến điểm truy cập để yêu cầu quyền truy cập vào điểm truy cập.

Tín hiệu nhiễu có thể bao gồm tín hiệu để ngăn điểm truy cập đáp lại trạm riêng hoặc không cho truyền vấn tin được bảo vệ đến trạm riêng.

Các vấn đề chi tiết khác của các phương án được bao gồm trong phần mô tả chi tiết và các hình vẽ.

Hiệu quả có lợi của sáng chế

Theo các phương án của sáng chế, khi nhiều trạm được liên kết với AP qua khung hủy xác thực được bảo vệ, như trong trường hợp, ví dụ, công nghệ IEEE 802.11w, mối liên kết với trạm riêng, trong số nhiều trạm, có thể được giải phóng, và việc truy cập vào trạm riêng có thể bị chặn.

Hiệu quả theo các phương án không bị giới hạn ở phần mô tả ở trên, và các hiệu quả khác nhau không được mô tả ở đây nằm trong phạm vi của sáng chế.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ khối minh họa cấu hình sơ đồ của WIPS.

Fig.2 là lưu đồ minh họa phương pháp ngăn chặn truy cập bằng WIPS.

Fig.3 là sơ đồ khái niệm giải thích kỹ thuật liên kết trong hệ thống ngăn chặn xâm nhập không dây theo một phương án của sáng chế.

Fig.4 là sơ đồ khái niệm giải thích kỹ thuật bảo vệ liên kết trong hệ thống ngăn chặn xâm nhập không dây theo một phương án của sáng chế.

Fig.5 là sơ đồ khái niệm giải thích kỹ thuật liên kết trong hệ thống ngăn chặn xâm

nhập không dây theo một phương án của sáng chế.

Fig.6 là sơ đồ khái niệm giải thích kỹ thuật bảo vệ hủy liên kết trong hệ thống ngăn chặn xâm nhập không dây theo một phương án của sáng chế.

Fig.7 là sơ đồ khái niệm giải thích kỹ thuật hủy liên kết trạm riêng trong hệ thống ngăn chặn xâm nhập không dây theo một phương án của sáng chế.

Fig.8 và Fig.9 minh họa các biến thể trên Fig.7, và là các sơ đồ khái niệm giải thích kỹ thuật hủy liên kết trạm riêng.

Fig.10 là sơ đồ khái niệm giải thích kỹ thuật hủy liên kết trạm riêng trong hệ thống ngăn chặn xâm nhập không dây theo một phương án khác của sáng chế.

Fig.11 và Fig.12 minh họa các biến thể trên Fig.10, và là các sơ đồ khái niệm minh họa trường hợp trong đó phương án trên Fig.8 hoặc Fig.9 được áp dụng thêm cho hệ thống ngăn chặn xâm nhập không dây.

Fig.13 đến Fig.15 là các sơ đồ khái niệm giải thích kỹ thuật hủy liên kết trạm riêng trong hệ thống ngăn chặn xâm nhập không dây theo một phương án khác của sáng chế.

Fig.16 là sơ đồ khái niệm giải thích kỹ thuật hủy liên kết trạm riêng trong hệ thống ngăn chặn xâm nhập không dây theo một phương án khác của sáng chế.

Mô tả chi tiết sáng chế

Các lợi thế và đặc điểm của sáng chế và các phương pháp để đạt được các lợi thế và đặc điểm này sẽ được làm rõ khi dựa vào các phương án được mô tả chi tiết sau cùng với các hình vẽ kèm theo. Tuy nhiên, sáng chế có thể được triển khai dưới nhiều hình thức khác nhau mà không bị giới hạn ở các phương án sẽ được mô tả sau đây, và các phương án của sáng chế được dự định sẽ làm cho việc mô tả khái niệm sáng chế trở nên hoàn chỉnh và được cung cấp để giúp những người có hiểu biết trung bình trong lĩnh vực kỹ thuật này hiểu rõ hơn về phạm vi của sáng chế. Phạm vi kỹ thuật của sáng chế phải được xác định theo phạm

vi kỹ thuật của phần yêu cầu bảo hộ.

Mặc dù các thuật ngữ "thứ nhất" và "thứ hai" được dùng để mô tả các thành phần khác nhau, nhưng rõ ràng là các thành phần này không bị giới hạn bởi các thuật ngữ. Các thuật ngữ này chỉ được dùng để phân biệt thành phần này với thành phần kia. Do đó, rõ ràng là thành phần thứ nhất, sẽ được mô tả dưới đây, cũng có thể là thành phần thứ hai mà không vượt ra ngoài phạm vi của sáng chế. Các dạng số ít được dự định để bao gồm cả dạng số nhiều, trừ khi ngữ cảnh biểu thị một cách rõ ràng theo cách khác.

Hệ thống ngăn chặn xâm nhập không dây (sau đây gọi là WIPS), sẽ được mô tả dưới đây, là hệ thống phát hiện và ngăn chặn sự xâm nhập không dây, như Điểm truy cập (giả mạo - rouge) trái phép hoặc tấn công Từ chối dịch vụ (DoS), thông qua giám sát khu vực không dây.

Các mạng không dây chung như được mô tả trong sáng chế này có thể định rõ mạng không dây mà công nghệ IEEE 802.11 được áp dụng, và, trong số các mạng không dây chung, mạng không dây mà công nghệ bảo mật xác định trước được áp dụng có thể định rõ mạng không dây mà công nghệ IEEE 802.11w được áp dụng. IEEE 802.11w là công nghệ IEEE 802.11 sửa đổi để cải thiện tính bảo mật của các khung quản lý. Tuy nhiên, sáng chế không bị giới hạn ở đó và rõ ràng là các phương án của sáng chế có thể được áp dụng cho mạng không dây áp dụng các công nghệ bảo mật khác nhau.

Hệ thống mạng không dây bao gồm một hoặc nhiều Tập Dịch vụ Cơ bản (Basic Service Set - BSS), mỗi trong số các tập đề cập đến tập hợp thiết bị mà được đồng bộ hóa thành công với nhau để có khả năng truyền thông với nhau.

Nói chung, BSS có thể được chia thành BSS hạ tầng và BSS độc lập (Independent BSS - IBSS).

Điểm truy cập (sau đây gọi là AP) là thực thể cung cấp quyền truy cập vào hệ thống phân phối thông qua môi trường không dây cho các trạm liên kết với AP đó. AP được dùng

như một khái niệm bao gồm Điểm phối hợp BSS Cá nhân (Personal BSS Coordination Point - PCP) và có thể bao gồm, theo nghĩa rộng, tất cả các khái niệm về bộ điều khiển tập trung, trạm gốc (base station - BS), nút-B, hệ thống thu phát gốc (Base Transceiver System - BTS), hoặc bộ điều khiển vị trí. Theo sáng chế này, AP có thể được định rõ là trạm truyền thông không dây gốc, và trạm truyền thông không dây gốc có thể được dùng, theo nghĩa rộng, vì thuật ngữ này bao gồm tất cả AP, trạm gốc, eNodeB (eNB), và điểm truyền (transmission point - TP). Ngoài ra, trạm truyền thông không dây gốc có thể bao gồm nhiều loại trạm truyền thông không dây khác nhau, các trạm này phân bổ tài nguyên môi trường truyền thông và thực hiện lập lịch khi truyền thông với nhiều trạm truyền thông không dây.

Trạm có thể là thiết bị bất kỳ bao gồm điều khiển truy cập môi trường (media access control - MAC) tuân theo với đặc tả kỹ thuật của IEEE 802.11 và giao diện lớp vật lý cho môi trường không dây, và có thể bao gồm, theo nghĩa rộng, AP cũng như trạm (không phải AP) điểm không truy cập. Trong bản mô tả sáng chế, 'trạm' đề cập đến trạm không phải AP, nhưng có thể được dùng làm thuật ngữ đề cập đến cả trạm không phải AP và AP theo một phương án. Trạm truyền thông không dây có thể còn bao gồm bộ xử lý và đơn vị truyền/nhận, và có thể bao gồm thêm đơn vị giao diện người dùng, đơn vị hiển thị, v.v. theo một phương án. Bộ xử lý có thể tạo ra khung để truyền qua mạng không dây hoặc xử lý khung nhận được qua mạng không dây, và có thể thực hiện thêm một số kiểu xử lý khác nhau để điều khiển trạm. Ngoài ra, đơn vị truyền/nhận có thể được ghép nối về mặt chức năng với bộ xử lý, và có thể truyền/nhận, cho trạm, các khung qua mạng không dây. Trạm có thể truyền/nhận khung đến/từ AP qua mạng không dây.

Sau đây, các phương án của sáng chế sẽ được mô tả dựa vào các hình vẽ kèm theo. Các số tham chiếu giống nhau hoặc tương tự được dùng để định rõ các thành phần giống nhau trong toàn bộ các hình vẽ.

Fig.1 là sơ đồ khối minh họa cấu hình sơ đồ của WIPS.

Như thể hiện trên Fig.1, WIPS 10 có thể bao gồm thiết bị cảm biến 100 và máy chủ 130. Trong khi đó, mạng doanh nghiệp mà dịch vụ mạng không dây và thiết bị cảm biến có thể được tạo cấu hình đồng thời có thể bao gồm thêm bộ điều khiển AP nếu cần thiết.

Hoạt động trong đó WIPS 10 xác định chính sách chặn có thể như sau.

Ví dụ, thiết bị cảm biến 100 có thể giám sát khung không dây, và có thể xử lý thông tin, như địa chỉ MAC, nội dung cấu hình bảo mật, tần số xuất hiện khung, tốc độ truyền, lượng dữ liệu, SSID, IEEE 802.11 a/b/g/n, kênh, và RSSI của trạm hoặc AP đã truyền khung không dây, dựa trên khung không dây được giám sát. Hơn nữa, thiết bị cảm biến 100 có thể truyền thông tin đã xử lý đến máy chủ 130.

Máy chủ 130 có thể xác định xem liệu trạm hoặc AP tương ứng có trái phép hay không và liệu trạm hoặc AP tương ứng có đang hoạt động bất thường hay không bằng cách so sánh thông tin đã xử lý với thông tin chữ ký lưu trong cơ sở dữ liệu (database - DB). Trong trường hợp này, chữ ký có thể bao gồm thông tin phần đầu của khung không dây hoặc thông tin về tần số xuất hiện khung.

Máy chủ 130 có thể xác định xem liệu AP dò được có là trái phép hay không trong hai trường hợp. Máy chủ 130 có thể xác định xem liệu AP dò được có phải là trái phép hay không dựa trên SSID, địa chỉ MAC, hoặc thông tin bổ sung lưu trong DB, hoặc có thể xác định AP dò được là AP trái phép nếu AP tương ứng không được kết nối với mạng có dây nội bộ. Trong trường hợp này, liệu AP tương ứng có được kết nối với mạng có dây nội bộ hay không có thể được xác định theo nhiều cách khác nhau. Trạm trái phép có thể được xác định theo cách tương tự.

Khi xác định rằng AP tương ứng là trái phép hoặc xác định rằng AP tương ứng là một trạm hoặc AP hoạt động bất thường, máy chủ 130 có thể thực hiện chặn tự động dựa trên chính sách chặn, hoặc có thể đưa ra cảnh báo để quản trị viên thực hiện chặn thủ công. Máy chủ 130 có thể truyền danh sách đích chặn hoặc thông tin chính sách chặn cho thiết bị

cảm biến 100 dựa trên việc xác định chặn.

Thiết bị cảm biến 100 có thể chọn AP và trạm sẽ bị chặn tùy thuộc vào việc xác định dựa trên danh sách đích chặn và chính sách chặn, và có thể thực hiện chặn.

Ví dụ, bước chặn bằng thiết bị cảm biến 100 dựa trên danh sách đích chặn và chính sách chặn có thể có các kiểu sau.

Theo một số ví dụ, bước chặn bằng thiết bị cảm biến 100 có thể bao gồm bước chặn AP. Tại đây, khi BSSID của AP đích chặn được phát hiện, thiết bị cảm biến 100 có thể chặn tất cả các trạm truy cập vào AP, thay vì chặn trạm riêng.

Theo một số ví dụ khác, bước chặn bằng thiết bị cảm biến 100 có thể bao gồm bước chặn trạm. Ở đây, khi một trạm tương ứng được xác định là trạm trái phép hoặc nó được phát hiện rằng trạm tương ứng đang giả mạo là trạm được phép, thiết bị cảm biến 100 có thể chặn trạm tương ứng. Khi MAC của trạm tương ứng xuất hiện, thiết bị cảm biến 100 có thể chặn quyền truy cập vào tất cả các AP của trạm tương ứng.

Theo một ví dụ khác, bước chặn bằng thiết bị cảm biến 100 có thể bao gồm bước chặn trạm-AP riêng. Ở đây, khi trạm được phép được liên kết với AP trái phép hoặc khi trạm trái phép được kết hợp với AP được phép, thiết bị cảm biến 100 có thể chặn sự liên kết này. Khi MAC của trạm tương ứng xuất hiện, thiết bị cảm biến 100 chỉ có thể chặn quyền truy cập vào AP được định rõ, nhưng có thể không liên quan đến việc truy cập vào các AP khác.

Ví dụ, thiết bị cảm biến 100 có thể bao gồm bộ điều khiển 105 và mođun truyền thông 125.

Mođun truyền thông 125 có thể giám sát khung không dây, và có thể gửi bản tin chặn cho trạm và AP khi tạo ra bản tin chặn.

Bộ điều khiển 105 có thể tạo ra bản tin chặn liên quan đến khung không dây nhận được là kết quả giám sát dựa trên thông tin chính sách và danh sách chặn liên quan đến việc

ngăn chặn xâm nhập không dây. Hơn nữa, bộ điều khiển 105 có thể điều khiển bản tin chặn đã tạo ra để gửi cho AP và trạm được định rõ để truyền/nhận khung không dây.

Ví dụ, bộ điều khiển 105 có thể bao gồm bộ thu cảm biến 110, bộ phân tích cảm biến 115, và bộ chặn cảm biến 120.

Bộ thu cảm biến 110 có thể giám sát khung không dây trong nhiều kênh bằng cách điều khiển mođun truyền thông 125.

Bộ phân tích cảm biến 115 có thể phân tích khung không dây nhận được là kết quả giám sát, và có thể thêm/cập nhật thông tin của AP hoặc trạm mà đã truyền khung không dây. Bộ phân tích cảm biến 115 có thể xác định liệu AP hoặc trạm có vi phạm chính sách chặn hay không dựa trên danh sách đích chặn và chính sách chặn, sau đó có thể tạo ra sự kiện chặn. Bộ phân tích cảm biến 115 có thể truyền sự kiện chặn đã tạo cho máy chủ 130.

Bộ chặn cảm biến 120 có thể thực thi sự kiện chặn đã tạo. Bộ chặn cảm biến 120 có thể tạo ra bản tin chặn và gửi bản tin chặn cho AP và trạm được định rõ để truyền/nhận khung không dây.

Ví dụ, khi AP và trạm được liên kết với nhau, bộ chặn cảm biến 120 có thể thực hiện bước chặn bằng cách tạo ra khung hủy xác thực và truyền khung này đến AP và trạm. Bộ chặn cảm biến 120 có thể thiết lập địa chỉ mà khung hủy xác thực được truyền từ đó dưới dạng BSSID của AP, có thể thiết lập địa chỉ mà khung hủy xác thực được nhận dưới dạng địa chỉ MAC của trạm tại đó, có thể tạo ra khung hủy xác thực, và có thể truyền khung hủy xác thực cho trạm. Hơn nữa, bộ chặn cảm biến 120 có thể thiết lập địa chỉ mà khung hủy xác thực được truyền từ đó dưới dạng địa chỉ MAC của trạm, có thể thiết lập địa chỉ mà khung hủy xác thực được nhận dưới dạng BSSID của AP tại đó, có thể tạo ra khung hủy xác thực, và có thể truyền khung hủy xác thực đến AP. Mỗi AP và trạm mà nhận được khung hủy xác thực từ thiết bị cảm biến 100 có thể xác định rằng bản sao đã truyền khung hủy xác thực cung cấp thông báo về việc chấm dứt mối liên kết, và có thể dừng kết nối giữa chúng.

Fig.2 là lưu đồ minh họa phương pháp chặn truy cập bằng WIPS.

Ở bước 205, máy chủ 130 có thể truyền thông tin chính sách và danh sách chặn liên quan đến việc ngăn chặn xâm nhập không dây cho thiết bị cảm biến 100.

Ở bước 210, bộ thu cảm biến 110 có thể giám sát khung không dây trong nhiều kênh. Khi khung không dây được nhận dưới dạng kết quả của quá trình giám sát, bộ thu cảm biến 110 có thể gọi bộ phân tích cảm biến 115 để phân tích khung không dây tương ứng ở bước 215.

Bộ phân tích cảm biến 115 có thể phân tích khung không dây tương ứng ở bước 220, và có thể thêm hoặc cập nhật thông tin về AP hoặc trạm đã truyền khung không dây tương ứng ở bước 225. Hơn nữa, ở bước 230, có thể xác định xem liệu AP hoặc trạm tương ứng có vi phạm chính sách hay không. Khi xác định rằng chính sách đã bị vi phạm, bộ phân tích cảm biến 115 có thể tạo ra sự kiện chặn ở bước 235. Bộ phân tích cảm biến 115 có thể truyền thông tin sự kiện chặn đã tạo đến máy chủ 130 ở bước 240.

Tại bước 245, khi việc tạo ra sự kiện chặn được truyền cho bộ chặn cảm biến 120, bộ chặn cảm biến 120 có thể thực thi sự kiện chặn ở bước 250. Ví dụ, như mô tả ở trên, bộ chặn cảm biến 120 có thể tạo ra khung hủy xác thực và truyền khung hủy xác thực cho AP và trạm được định rõ để truyền/nhận khung không dây.

Fig.3 là sơ đồ khái niệm giải thích kỹ thuật liên kết trong hệ thống ngăn chặn xâm nhập không dây theo một phương án của sáng chế.

Trong các hình vẽ sau, các bước riêng di chuyển xuống dưới theo thời gian được minh họa trong mỗi hình vẽ.

Ví dụ, kỹ thuật liên kết có thể được thực hiện khi trạm 30 mất khóa mã hóa.

Như thể hiện trên Fig.3, trong khi AP 20 và trạm 30 được liên kết với nhau, trạm 30 có thể mất khóa mã hóa vì lý do riêng (S101). Ví dụ, lý do riêng của trạm 30 có thể bao gồm

thiết lập lại, khởi động lại, hoặc tương tự. Ở đây, trạm 30 có thể ở trong trạng thái trong đó khóa mã hóa bị mất (S101).

Trong trạng thái mất khóa mã hóa, trạm 30 có thể yêu cầu truy cập vào AP 20 (S102). Trong trường hợp này, vì trạm 30 đã mất tất cả các khóa mã hóa, nên nó có thể truyền khung yêu cầu truy cập không được bảo vệ cho AP 20.

Vì AP 20 xác định rằng trạm 30 vẫn duy trì liên kết hợp lệ bằng cách sử dụng khóa mã hóa, AP 20 từ chối yêu cầu truy cập từ trạm 30, và có thể lệnh cho trạm 30 thử truy cập lại sau thời gian thứ nhất định trước (S103).

Sau đó, AP 20 có thể thực hiện kiểm tra để xác định xem liệu yêu cầu truy cập như vậy (S102) có phải là cuộc tấn công (S104) hay không. Theo một phương án, cơ chế cho bước kiểm tra (S104) có thể bao gồm bước truy vấn liên kết bảo mật (Security Association - SA). Ví dụ, bước truy vấn SA có thể bao gồm thêm bước truyền, bằng AP 20, ít nhất một vấn tin liên kết bảo mật được bảo vệ đến trạm 30.

Trong trường hợp trạm 30 không đáp lại trước thời gian đáp ứng (thời gian thứ hai) của trạm 30 định trước ở bước truy vấn SA, trôi qua, AP 20 có thể truyền yêu cầu hủy liên kết cho trạm 30 hiện thời (S105), và có thể loại bỏ khóa mã hóa mà không còn hợp lệ nữa.

Sau khi thời gian thứ nhất trôi qua, trạm 30 có thể truyền khung yêu cầu (tái) truy cập cho AP 20 (S106). Sau đó, AP 20 có thể cho phép trạm 30 truy cập (S107), và AP 20 và trạm 30 có thể được liên kết với nhau (S108).

Fig.4 là sơ đồ khái niệm giải thích kỹ thuật bảo vệ liên kết trong hệ thống ngăn chặn xâm nhập không dây theo một phương án của sáng chế.

Ví dụ, kỹ thuật bảo vệ liên kết có thể được thực hiện khi kẻ tấn công cố gắng truy cập vào AP 20.

Như thể hiện trên Fig.4, AP 20 và trạm 30 có thể được liên kết với nhau (S200). Kẻ

tấn công 40 có thể yêu cầu quyền truy cập vào AP 20 (S201). Ở đây, kẻ tấn công 40 có thể là trạm trái phép và trạm 30 được điều khiển từ bên ngoài, và có thể bao gồm trạm 30 hoặc tương tự về cơ bản được coi là trạm trái phép.

Vì AP 20 xác định rằng trạm 30 vẫn duy trì sự liên kết hợp lệ bằng cách sử dụng khóa mã hóa, AP 20 có thể từ chối yêu cầu truy cập từ kẻ tấn công 40, và có thể lệnh cho kẻ tấn công 40 thử truy cập lại sau thời gian thứ ba định trước (S202).

Sau đó, AP 20 có thể thực hiện kiểm tra để xác định xem liệu yêu cầu truy cập như vậy có phải là một cuộc tấn công hay không. AP 20 có thể truyền riêng vấn tin được bảo vệ cho kẻ tấn công 40 và trạm 30 (S203a và S203b). Theo một phương án, AP 20 có thể truyền đồng thời vấn tin được bảo vệ cho kẻ tấn công 40 và trạm 30, nhưng thời gian mà (trình tự trong đó) để truyền vấn tin được bảo vệ không bị giới hạn ở đó.

Trạm 30 có thể đáp lại AP 20 qua câu trả lời được bảo vệ để đáp lại vấn tin được bảo vệ (S204).

AP 20 có thể xác định rằng yêu cầu từ kẻ tấn công 40 là yêu cầu liên kết giả mạo, và có thể bỏ qua yêu cầu truy cập từ kẻ tấn công 40 (S205).

Fig.5 là sơ đồ khái niệm giải thích kỹ thuật liên kết trong hệ thống ngăn chặn xâm nhập không dây theo một phương án của sáng chế.

Ví dụ, kỹ thuật liên kết có thể được thực hiện khi AP 20 mất khóa mã hóa.

Như thể hiện trên Fig.5, trong khi AP 20 và trạm 30 được liên kết với nhau, AP 20 có thể mất khóa mã hóa vì lý do riêng (S301). Ví dụ, lý do riêng có thể bao gồm thiết lập lại, khởi động lại, hoặc tương tự của AP 20. Ở đây, trạm 20 có thể ở trong trạng thái trong đó khóa mã hóa bị mất (S301).

Khi trạm 30 được liên kết trước đó truyền khung dữ liệu được mã hóa cho AP (S302), AP 20 có thể thử lại mối liên kết bằng cách truyền khung không được bảo vệ cho trạm 30

(S303). Vì trạm 30 vẫn bao gồm khóa mã hóa và xác định rằng mối liên kết hợp lệ với AP 20 được duy trì, nên trạm 30 có thể thực hiện kiểm tra để xác định xem liệu nỗ lực liên kết của AP 20 có phải là một cuộc tấn công hay không. Theo một phương án, cơ chế cho quy trình kiểm tra có thể bao gồm bước truy vấn SA. Ví dụ, bước truy vấn SA có thể bao gồm thêm bước truyền, bằng trạm 30, ít nhất một vấn tin được bảo vệ (vấn tin SA) cho AP 20 (S304).

Khi AP 20 không thể đáp lại vấn tin được bảo vệ ngay cả khi thời gian thứ tư định trước trôi qua, trạm 30 có thể xác định rằng mối liên kết với AP 20 đã được giải phóng, và có thể loại bỏ khóa mã hóa không hợp lệ với AP 20.

Sau đó, khi trạm 30 truyền vấn tin không được bảo vệ cho AP 20 (S305) và AP 20 đáp lại trạm 30 qua câu trả lời không được bảo vệ để đáp lại vấn tin không được bảo vệ (S306), AP 20 và trạm 30 có thể liên kết với nhau.

Fig.6 là sơ đồ khái niệm giải thích kỹ thuật bảo vệ hủy liên kết trong hệ thống ngăn chặn xâm nhập không dây theo một phương án của sáng chế.

Ví dụ, kỹ thuật bảo vệ hủy liên kết có thể được thực hiện để cung cấp quy trình bảo vệ trong trường hợp kẻ tấn công 40 giải phóng mối liên kết với trạm 30 truy cập vào AP 20.

Như thể hiện trên Fig.6, AP 20 và trạm 30 có thể vẫn liên kết với nhau (S401).

Liên quan đến vấn đề này, kẻ tấn công 40 có thể yêu cầu hủy liên kết với trạm 30 để hủy liên kết trạm 30 với AP 20 (S402). Theo một phương án, kẻ tấn công 40 có thể truyền yêu cầu hủy liên kết mô tả ở trên cho nhiều trạm 30 được liên kết với AP 20 để hủy liên kết nhiều trạm 30 với AP 20 (S402).

Mỗi trạm 30 có thể thực hiện kiểm tra để xác định xem liệu yêu cầu hủy liên kết từ kẻ tấn công 40 có phải là cuộc tấn công hay không để đáp lại yêu cầu hủy liên kết (S402). Trạm 30 có thể truyền ít nhất một vấn tin được bảo vệ cho AP 20 (S403). Vì mối liên kết giữa AP 20 và trạm 30 vẫn còn hiệu lực, nên AP 20 có thể đáp lại trạm 30 qua câu trả lời

được bảo vệ (S404).

Bằng cách này, trạm 30 có thể xác định rằng yêu cầu hủy liên kết từ kẻ tấn công 40 là cuộc tấn công, có thể bỏ qua yêu cầu hủy liên kết từ kẻ tấn công 40, và có thể duy trì liên kết với AP 20.

Fig.7 là sơ đồ khái niệm giải thích kỹ thuật hủy liên kết trạm riêng trong hệ thống ngăn chặn xâm nhập không dây theo một phương án của sáng chế.

Ví dụ, kỹ thuật hủy liên kết với trạm 31 riêng có thể được thực hiện trong trường hợp trong đó nó muốn hủy liên kết với trạm trái phép riêng 31, hoặc hủy liên kết trạm riêng 31, trạm này được điều khiển bởi kẻ tấn công 40 và về cơ bản có thể được coi là trạm trái phép, trong số nhiều trạm liên kết với AP 20, như được minh họa trong hình vẽ. Trong bản mô tả của sáng chế, thuật ngữ 'trạm riêng 31' đề cập đến ít nhất một số trạm 30 được nhắm đích để hủy liên kết, trong số nhiều trạm 30 được liên kết với AP 20. Theo một phương án, trạm riêng 31 có thể được liên kết với kẻ tấn công 40 qua mạng.

Như thể hiện trên Fig.7, hệ thống mạng không dây có thể bao gồm AP 20, các trạm 30 bao gồm trạm riêng 31, và WIPS 10.

AP 20 có thể được kết hợp với nhiều trạm 30, và mối liên kết giữa AP 20 và trạm riêng 31 có thể được duy trì (S501). Theo một phương án, trạm riêng 31 có thể là trạm trái phép, hoặc có thể bao gồm trạm 30 được kẻ tấn công 40 điều khiển (S500) và về cơ bản có thể được coi là trạm trái phép.

Theo một phương án, WIPS 10 có thể truyền yêu cầu hủy liên kết cho nhiều trạm 30 liên quan cho AP 20. Trong trường hợp này, yêu cầu hủy liên kết cũng có thể được truyền cho trạm riêng 31 (S502). Yêu cầu hủy liên kết (S502) có thể bao gồm khung làm giả. Ví dụ, khung làm giả có thể bao gồm khung giả mạo như khung yêu cầu liên kết mới (khung liên kết), khung yêu cầu tái liên kết (khung tái liên kết), hoặc khung yêu cầu hủy liên kết cho trạng thái liên kết hiện tại (Khung hủy liên kết).

Do đó, trạm riêng 31 có thể thực hiện kiểm tra để xác định xem liệu yêu cầu hủy liên kết nhận được từ AP 20 (S502) có phải là cuộc tấn công hay không. Tức là, trạm riêng 31 có thể thử xác thực lại lẫn nhau với AP 20. Trạm riêng 31 có thể truyền vấn tin được bảo vệ cho AP 20 (S503). Theo một phương án, trạm riêng 31 có thể thực hiện truyền nhiều lần vấn tin được bảo vệ cho AP 20 (S503).

Trong trường hợp này, WIPS 10 có thể gây nhiễu cho việc hồi đáp của AP 20 với trạm riêng 31. Đối với việc gây nhiễu như vậy (S504), WIPS 10 có thể truyền tín hiệu nhiễu cho AP 20 và/hoặc trạm riêng 31 Mặc dù AP 20 cần đáp lại vấn tin được bảo vệ truyền từ trạm riêng 31, nhưng AP 20 có thể bị ngăn (S505) không cho đáp lại trạm riêng 31 do việc gây nhiễu (S504).

Do đó, trạm riêng 31 có thể bị hủy liên kết với AP 20 sau thời gian thứ năm định trước vì nó không nhận được hồi đáp từ AP 20 trong thời gian thứ năm định trước. Do đó, trạm riêng 31 có thể bị chấm dứt mối liên kết với AP 20 (S506).

Sau đây, tín hiệu nhiễu được truyền ở bước gây nhiễu (S504) sẽ được mô tả chi tiết có dựa vào các hình vẽ trên Fig.8 và Fig.9. Sau đây, trong phần mô tả trên Fig.8 và Fig.9, việc mô tả lặp lại các thành phần giống nhau như các thành phần trên Fig.7 được bỏ qua, và các số tham chiếu giống hoặc tương tự được sử dụng.

Các hình vẽ trên Fig.8 và Fig.9 minh họa các biến thể trên Fig.7, và là các sơ đồ khái niệm giải thích kỹ thuật hủy liên kết trạm riêng.

Như thể hiện trên Fig.8, WIPS 10 có thể gây nhiễu kênh bằng cách truyền khung CST và/hoặc khung RTS để ngăn không cho AP 20 đáp lại trạm riêng 31 (S504a).

Trạm mà thực hiện truyền thông LAN không dây, kiểm tra xem liệu kênh có ở trạng thái bận hay không bằng cách thực hiện nhận biết sóng mang trước khi truyền dữ liệu. Khi tín hiệu không dây có cường độ nhất định hoặc hơn được nhận biết, nó xác định rằng kênh tương ứng đang ở trạng thái bận, và trạm làm trễ việc truy cập vào kênh tương ứng. Quy

trình này được gọi là Đánh giá kênh rỗi (Clear Channel Assessment - CCA), và mức mà nó xác định xem liệu tín hiệu tương ứng có được nhận biết tại đó hay không được gọi là ngưỡng CCA. Khi tín hiệu không dây bằng hoặc lớn hơn ngưỡng CCA, được trạm nhận, có trạm tương ứng làm bộ thu, trạm sẽ xử lý tín hiệu không dây nhận được. Mặt khác, khi tín hiệu không dây không được nhận biết trong kênh tương ứng, hoặc khi tín hiệu không dây có cường độ nhỏ hơn ngưỡng CCA được nhận biết, thì nó có thể xác định rằng kênh đang ở trạng thái rỗi.

Khi xác định rằng kênh đang ở trạng thái rỗi, mỗi trạm có dữ liệu cần truyền thực hiện thủ tục chờ truyền sau một khoảng thời gian, như không gian giữa các khung (InterFrame Space - IFS) phù hợp với tình hình của trạm, ví dụ, IFS phân xử (Arbitration IFS - AIFS) hoặc IFS chức năng Điều phối điểm (Point Coordination function - PCF) IFS ((Point Coordination function - PCF) IFS - PIFS)).

Theo một phương án, AIFS có thể được dùng như một thành phần để thay thế DCF IFS (DCF IFS - DIFS) hiện có. Mỗi trạm đang chờ trong khi giảm một số thời gian khe đồng nhất với số ngẫu nhiên, được gán cho trạm tương ứng, trong khoảng thời gian tương ứng với trạng thái rỗi của kênh, và trạm đã hết tất cả thời gian khe sẽ cố gắng truy cập kênh tương ứng. Khoảng thời gian mà các trạm tương ứng thực hiện các thủ tục chờ truyền theo cách này được gọi là khoảng thời gian cửa sổ tranh chấp.

Nếu trạm truy cập thành công kênh, thì trạm tương ứng có thể truyền dữ liệu qua kênh. Tuy nhiên, khi trạm cố gắng truy cập gây xung đột với trạm khác, thì các trạm gây xung đột lần lượt được gán các số ngẫu nhiên mới để thực hiện lại các thủ tục chờ truyền. Theo một phương án, số ngẫu nhiên được gán mới cho mỗi trạm có thể được xác định trong phạm vi rộng gấp đôi phạm vi các số ngẫu nhiên đã được gán trước đó cho trạm tương ứng. Trong khi đó, mỗi trạm cố gắng truy cập bằng cách thực hiện lại thủ tục chờ truyền trong khoảng thời gian cửa sổ tranh chấp tiếp theo, trong đó mỗi trạm thực hiện thủ tục chờ truyền từ một thời gian khe còn lại trong khoảng thời gian cửa sổ tranh chấp trước đó. Các trạm

thực hiện truyền thông LAN không dây bằng cách sử dụng phương pháp này có thể tránh xung đột với nhau cho kênh riêng.

Các trạm tranh chấp quyền truyền dữ liệu với nhau. Khi quá trình truyền dữ liệu ở bước trước được hoàn thành, mỗi trạm có dữ liệu cần truyền thực hiện thủ tục chờ truyền đồng thời giảm bộ đếm chờ truyền (hoặc bộ định thời chờ truyền) cho số ngẫu nhiên được gán cho nó sau thời gian tương ứng với AIFS trôi qua. Trạm mà bộ đếm chờ truyền đã hết hạn cung cấp thông báo rằng trạm tương ứng có dữ liệu cần truyền bằng cách gửi khung Yêu cầu gửi (Request to Send - RTS). Khung RTS bao gồm thông tin về địa chỉ bộ thu, địa chỉ bộ phát, và thời khoảng. Sau khi AP 20 nhận được khung RTS đợi trong khoảng thời gian tương ứng với IFS Ngắn (Short IFS - SIFS), nó có thể thông báo cho trạm riêng 31 rằng có thể truyền dữ liệu bằng cách gửi khung Sẵn sàng để Gửi (Clear to Send - CTS). Khung CTS bao gồm thông tin như địa chỉ bộ thu và thời khoảng. Ở đây, địa chỉ bộ thu của khung CTS có thể được thiết lập giống với địa chỉ bộ phát của khung RTS tương ứng với nó, tức là, địa chỉ của trạm riêng 31.

AP 20 mà nhận được khung CTS sẽ truyền dữ liệu sau thời gian tương ứng với SIFS đã trôi qua. Khi bước truyền dữ liệu được hoàn thành, AP 20 cung cấp thông báo rằng bước truyền dữ liệu đã hoàn thành bằng cách nhận biết khung hồi đáp (ACK) sau khi thời gian tương ứng với SIFS đã trôi qua. Khi khung hồi đáp được nhận trong thời gian thiết lập trước, trạm phát cho rằng việc truyền dữ liệu đã thành công. Khi không nhận được khung hồi đáp trong thời gian thiết lập trước, trạm phát cho rằng việc truyền dữ liệu đã thất bại. Trong khi đó, các trạm lân cận 30 đã nhận được ít nhất một trong số khung RTS và khung CTS trong quy trình truyền thiết lập Vectơ phân bổ Mạng (Network Allocation Vector - NAV), và không thực hiện truyền dữ liệu đến khi NAV thiết lập hết hạn. Ở đây, NAV của mỗi trạm có thể được thiết lập dựa trên trường thời khoảng của khung RTS hoặc khung CTS nhận được.

Theo một phương án, trạm riêng 31 có thể truyền vấn tin được bảo vệ cho AP 20 (S503), và có thể lệnh cho AP 20 đáp lại trong thời gian thứ sáu định trước.

Theo một phương án, WIPS 10 có thể thu thập các vấn tin được bảo vệ được truyền từ trạm riêng 31 cho AP 20 (S503). Theo các vấn tin thu thập được, WIPS 10 có thể gửi khung CST và/hoặc khung RTS cho AP 20 và/hoặc trạm riêng 31 (S504a).

Mặc dù AP 20 phải đáp lại vấn tin được bảo vệ nhận được từ trạm riêng 31 trong thời gian thứ sáu, nó nhận khung CST và/hoặc khung RTS từ WIPS 10, và do đó AP 20 có thể không thực hiện truyền dữ liệu cho đến khi NAV thiết lập hết hạn. Tức là, AP 20 có thể bị ngăn đáp lại trạm riêng 31 trong thời gian thứ sáu (S505). Do đó, trạm riêng 31 có thể xác định rằng yêu cầu hủy liên kết truyền từ WIPS 10 (S502) là đúng, và có thể bị chấm dứt mối liên kết với AP 20 (S506).

Như thể hiện trên Fig.9, WIPS 10 có thể gây nhiễu kênh bằng cách tăng mức tắc nghẽn của AP 20 và/hoặc trạm riêng 31 (S504b) để ngăn AP 20 đáp lại trạm riêng 31.

Theo một phương án, WIPS 10 có thể thu thập các vấn tin được bảo vệ truyền từ trạm riêng 31 cho AP 20 (S503), và có thể tăng mức tắc nghẽn của AP 20 và/hoặc trạm riêng 31 theo các vấn tin thu thập được(S504b). Ví dụ, WIPS 10 có thể tạo ra một lượng lớn các gói giả mạo bao gồm khung yêu cầu liên kết mới (khung liên kết), khung yêu cầu tái liên kết (khung tái liên kết), hoặc khung yêu cầu hủy liên kết với trạng thái liên kết hiện tại (Khung hủy liên kết), do đó, mức tắc nghẽn tăng lên khi các vấn tin được bảo vệ được truyền (S503), do đó gây ra lỗi xác thực lẫn nhau giữa AP 20 và trạm riêng 31. Ngoài ra, ví dụ, WIPS 10 có thể tăng mức tắc nghẽn bằng cách sử dụng phương pháp kiểm soát tốc độ bit của tín hiệu được truyền từ AP 20 hoặc kiểm soát thời gian trễ truyền, do đó gây ra lỗi xác thực lẫn nhau giữa AP 20 và trạm riêng 31. Tức là, WIPS 10 có thể tăng mức tắc nghẽn của AP 20 và/hoặc trạm riêng 31 (S504), do đó khiến mối liên kết giữa AP 20 và trạm riêng 31 được thiết lập thông qua IEEE 802.11w sẽ bị chấm dứt (S506).

Fig.10 là sơ đồ khái niệm giải thích kỹ thuật hủy liên kết trạm riêng trong hệ thống ngăn chặn xâm nhập không dây theo một phương án khác của sáng chế.

Như thể hiện trên Fig.10, có sự khác biệt so với phương án trên Fig.7, trong đó bao gồm thêm bước WIPS 10 gửi lệnh chặn liên kết cho AP 20 và/hoặc trạm riêng 31 (S508).

Theo một phương án, sau khi mối liên kết giữa trạm riêng 31 và AP 20 bị chấm dứt (S506), trạm riêng 31 có thể lại yêu cầu quyền truy cập vào AP 20 (S507). Ví dụ, trạm riêng 31 có thể gửi khung yêu cầu xác thực cho AP 20.

Theo một phương án, WIPS 10 có thể gửi khung quản lý như khung hủy xác thực cho AP 20 và/hoặc trạm riêng 31 theo khung yêu cầu xác thực gửi từ trạm riêng 31 cho AP 20. Do đó, mối liên kết giữa trạm riêng 31 và AP 20 có thể thất bại.

Các hình vẽ trên Fig.11 và Fig.12 minh họa các biến thể trên Fig.10, và là các sơ đồ khái niệm minh họa trường hợp trong đó phương án trên Fig.8 hoặc Fig.9 được áp dụng thêm cho hệ thống ngăn chặn xâm nhập không dây.

Như được thể hiện trên Fig.11 và Fig.12, WIPS 10 có thể gây nhiễu kênh bằng cách nhận biết khung CST và/hoặc khung RTS (S504a) hoặc bằng cách tăng mức tắc nghẽn của AP 20 và/hoặc trạm riêng 31 (S504b) để ngăn AP 20 đáp lại trạm riêng 31.

Ngay cả khi trạm riêng 31 gửi khung yêu cầu xác thực cho AP 20 sau khi mối liên kết giữa trạm riêng 31 và AP 20 bị chấm dứt (S506), WIPS 10 có thể gửi lệnh chặn liên kết, như khung hủy xác thực, cho AP 20 và/hoặc trạm riêng 31 (S508), do đó khiến cho liên kết giữa trạm riêng 31 và AP 20 thất bại.

Các hình vẽ từ Fig.13 đến Fig.15 là các sơ đồ khái niệm giải thích kỹ thuật hủy liên kết trạm riêng trong hệ thống ngăn chặn xâm nhập không dây theo một phương án khác của sáng chế.

Trước tiên, như thể hiện trên Fig.13, trong khi AP 20 và trạm riêng 31 được liên kết với nhau (S601), thì trạm riêng 31 có thể mất khóa mã hóa vì lý do riêng (S101).

Ở trạng thái khóa mã hóa bị mất, trạm riêng 31 có thể yêu cầu quyền truy cập vào AP

20 (S603). Trong trường hợp này, vì trạm riêng 31 đã mất tất cả các khóa mã hóa, nó có thể truyền khung yêu cầu truy cập không được bảo vệ đến AP 20.

Vì AP 20 xác định rằng trạm riêng 31 vẫn duy trì liên kết hợp lệ bằng cách sử dụng khóa mã hóa, nên AP 20 có thể từ chối yêu cầu truy cập từ trạm riêng 31, và có thể lệnh cho trạm riêng 31 thử truy cập lại sau khi thời gian thứ bảy xác định trước trôi qua (S604a). Theo một phương án, vấn tin được bảo vệ có thể được truyền cùng với lệnh (S604b).

Sau thời gian thứ bảy, trạm riêng 31 có thể gửi khung yêu cầu truy cập lại cho AP 20 (S605).

Trong khi đó, theo một phương án, WIPS 10 có thể gây nhiễu cuộc truyền, bằng AP 20, vấn tin được bảo vệ với trạm riêng 31 theo khung yêu cầu truy cập lại (S606a). Đối với nhiễu (S606a), WIPS 10 có thể truyền tín hiệu nhiễu cho AP 20 và/hoặc trạm riêng 31 theo một phương án. Mặc dù AP 20 phải truyền vấn tin được bảo vệ cho trạm riêng 31 để đáp lại khung yêu cầu truy cập lại, nhưng nó có thể bị ngăn truyền vấn tin được bảo vệ cho trạm riêng 31 (S607a) do nhiễu (S606a).

Do đó, liên kết giữa AP 20 và trạm riêng 31 có thể bị chấm dứt (S608).

Như thể hiện trên Fig.14, theo một phương án, WIPS 10 có thể gây nhiễu cuộc truyền, bằng AP 20, vấn tin được bảo vệ cho trạm riêng 31 (S606b) để đáp lại khung yêu cầu truy cập (S603). Đối với nhiễu (S606b), WIPS 10 có thể truyền tín hiệu nhiễu cho AP 20 và/hoặc trạm riêng 31. AP 20 phải truyền vấn tin được bảo vệ cho trạm riêng 31 để đáp lại khung yêu cầu truy cập, nhưng có thể bị ngăn truyền vấn tin được bảo vệ cho trạm riêng 31 (S604c) do nhiễu (S606b). Theo một phương án, AP 20 có thể từ chối yêu cầu truy cập từ trạm riêng 31, và cũng có thể bị ngăn truyền lệnh để cho phép trạm riêng thử truy cập lại sau thời gian thứ bảy định trước.

Do đó, liên kết giữa AP 20 và trạm riêng 31 có thể bị chấm dứt (S608).

Như thể hiện trên Fig.15, theo một phương án, WIPS 10 có thể gây nhiễu cuộc truyền,

bằng AP 20, vấn tin được bảo vệ cho trạm riêng 31 (S606b) để đáp lại khung yêu cầu truy cập (S603). Đối với nhiễu (S606b), WIPS 10 có thể truyền tín hiệu nhiễu cho AP 20 và/hoặc trạm riêng 31. Mặc dù AP 20 phải truyền vấn tin được bảo vệ cho trạm riêng 31 để đáp lại khung yêu cầu truy cập, nó có thể bị ngăn truyền vấn tin được bảo vệ cho trạm riêng 31 (S604c) do nhiễu (S606b). Theo một phương án, AP 20 có thể từ chối yêu cầu truy cập từ trạm riêng 31, và cũng có thể bị ngăn truyền lệnh để cho phép trạm riêng thử truy cập lại sau thời gian thứ bảy định trước.

Sau đó, liên kết giữa AP 20 và trạm riêng 31 không bị chấm dứt, và trạm riêng 31 có thể gửi khung yêu cầu truy cập lại cho AP 20 (S605).

Trong trường hợp này, WIPS 10 có thể lại gây nhiễu cho cuộc truyền, bằng AP 20, vấn tin được bảo vệ cho trạm riêng 31 để đáp lại khung yêu cầu truy cập lại (S606a). Đối với nhiễu (S606a), WIPS 10 có thể truyền tín hiệu nhiễu cho AP 20 và/hoặc trạm riêng 31 theo một phương án. Mặc dù AP 20 phải truyền vấn tin được bảo vệ cho trạm riêng 31 để đáp lại khung yêu cầu truy cập lại, nó có thể bị ngăn truyền vấn tin được bảo vệ cho trạm riêng 31 (S607a) do nhiễu (S606a).

Do đó, liên kết giữa AP 20 và trạm riêng 31 có thể bị chấm dứt (S608).

Theo tín hiệu nhiễu được mô tả ở trên liên quan đến các Fig.13 đến Fig.15, ít nhất một trong số các tín hiệu nhiễu, được mô tả ở trên có dựa vào Fig.9 và Fig.10 có thể được áp dụng.

Fig.16 là sơ đồ khái niệm giải thích kỹ thuật hủy liên kết trạm riêng trong hệ thống ngăn chặn xâm nhập không dây theo một phương án khác của sáng chế.

Như thể hiện trên Fig.16, AP 20 và trạm riêng 31 có thể được liên kết với nhau (S701). WIPS 10 có thể yêu cầu truy cập vào AP 20 (S702).

Vì AP 20 xác định rằng trạm riêng 31 vẫn duy trì liên kết hợp lệ bằng cách sử dụng khóa mã hóa, nên AP 20 có thể từ chối yêu cầu truy cập từ WIPS 10 và có thể lệnh cho

WIPS 10 thử truy cập lại sau khi thời gian thứ tám định trước trôi qua (S703).

Sau đó, để AP 20 thực hiện kiểm tra để xác định xem liệu yêu cầu truy cập như vậy có phải là cuộc tấn công hay không, AP 20 phải truyền riêng vấn tin được bảo vệ cho WIPS 10 và trạm riêng 31, nhưng vấn tin được bảo vệ có thể bị WIPS 10 chặn. Theo một phương án, WIPS 10 có thể truyền tín hiệu nhiễu cho AP 20 và/hoặc trạm riêng 31 (S703a). AP 20 có thể bị ngăn truyền vấn tin được bảo vệ cho WIPS 10 và/hoặc trạm riêng 31 do tín hiệu nhiễu (S704a).

Do đó, mối liên kết giữa AP 20 và trạm riêng 31 có thể bị chấm dứt (S705).

Vì tín hiệu nhiễu được mô tả ở trên dựa vào Fig.16, ít nhất một trong số các tín hiệu nhiễu được mô tả ở trên dựa vào Fig.9 và Fig.10 theo ví dụ có thể được áp dụng.

Bằng phương pháp được mô tả ở trên dựa vào các hình vẽ từ Fig.7 đến Fig.16, WIPS 10 có thể giải phóng mối liên kết với trạm riêng 31, trạm này được liên kết với AP 20 và có thể về cơ bản được coi là trạm trái phép. Cụ thể, WIPS 10 có thể giải phóng liên kết với trạm riêng bằng cách nhắm đích đến trạm riêng, trong số tất cả các trạm được liên kết với AP 20, qua mạng không dây mà công nghệ IEEE 802.11w được áp dụng.

Mặc dù các phương án của sáng chế đã được bộc lộ, nhưng những người có hiểu biết trung bình trong lĩnh vực kỹ thuật này sẽ hiểu rằng sáng chế có thể được thực hiện ở các dạng cụ thể khác mà không vượt ra ngoài bản chất kỹ thuật hoặc đặc tính then chốt của sáng chế như được nêu trong các điểm yêu cầu bảo hộ kèm theo. Do đó, cần phải hiểu rằng các phương án được mô tả ở trên chỉ là ví dụ về mọi khía cạnh chứ không phải là bị giới hạn.

YÊU CẦU BẢO HỘ

1. Hệ thống mạng không dây bao gồm:

điểm truy cập;

nhiều trạm được tạo cấu hình để truyền/nhận khung không dây đến/từ điểm truy cập qua mạng không dây; và

hệ thống ngăn chặn xâm nhập không dây được tạo cấu hình để giám sát khung không dây,

trong đó hệ thống ngăn chặn xâm nhập không dây truyền yêu cầu hủy liên kết đến trạm riêng, trong số nhiều trạm, và truyền tín hiệu nhiễu đến điểm truy cập, để ngăn điểm truy cập đáp lại trạm riêng.

trong đó tín hiệu nhiễu bao gồm gói giả mạo, và

trong đó gói giả mạo bao gồm khung yêu cầu liên kết mới (khung liên kết), hoặc khung yêu cầu tái liên kết (khung tái liên kết).

2. Hệ thống mạng không dây theo điểm 1, trong đó tín hiệu nhiễu bao gồm khung Sẵn sàng để gửi (Clear to Send - CTS) hoặc khung Yêu cầu để Gửi (Request to Send - RTS).

3. Hệ thống mạng không dây theo điểm 1, trong đó tín hiệu nhiễu bao gồm tín hiệu để làm tăng mức tắc nghẽn của điểm truy cập.

4. Hệ thống mạng không dây theo điểm 1, trong đó trạm riêng truyền vấn tin được bảo vệ đến điểm truy cập để đáp lại yêu cầu hủy liên kết.

5. Hệ thống mạng không dây theo điểm 4, trong đó:

trạm riêng lệnh cho điểm truy cập đáp lại vấn tin được bảo vệ trong thời gian thứ nhất định trước, và

trạm riêng chấm dứt mối liên kết với điểm truy cập khi không nhận được hồi đáp

trong thời gian thứ nhất.

6. Hệ thống mạng không dây theo điểm 5, trong đó trạm riêng gửi khung yêu cầu xác thực đến điểm truy cập sau khi mối liên kết với điểm truy cập bị chấm dứt.

7. Hệ thống mạng không dây theo điểm 6, trong đó hệ thống ngăn chặn xâm nhập không dây gửi khung hủy xác thực đến điểm truy cập hoặc trạm riêng sau khi khung yêu cầu xác thực được gửi đi.

8. Hệ thống mạng không dây theo điểm 1, trong đó trạm riêng là trạm được kết nối với trạm trái phép hoặc kẻ tấn công trái phép qua mạng.

9. Hệ thống mạng không dây theo điểm 1, trong đó mạng không dây bao gồm công nghệ IEEE 802.11w.

10. Phương pháp vận hành hệ thống mạng không dây bao gồm các bước:

duy trì, bởi điểm truy cập, mối liên kết với trạm riêng, trong số nhiều trạm được tạo cấu hình để truyền/nhận khung không dây đến/từ điểm truy cập qua mạng không dây; và

truyền, bởi hệ thống ngăn chặn xâm nhập không dây được tạo cấu hình để giám sát khung không dây, tín hiệu nhiễu để ngăn điểm truy cập đáp lại trạm riêng hoặc ngăn điểm truy cập truyền vấn tin được bảo vệ đến trạm riêng,

trong đó tín hiệu nhiễu bao gồm gói giả mạo, và

trong đó gói giả mạo bao gồm khung yêu cầu liên kết mới (khung liên kết), hoặc khung yêu cầu tái liên kết (khung tái liên kết).

11. Phương pháp theo điểm 10 còn bao gồm các bước:

truyền, bởi hệ thống ngăn chặn xâm nhập không dây được tạo cấu hình để giám sát khung không dây, yêu cầu hủy liên kết đến trạm riêng;

truyền, bởi trạm riêng, vấn tin được bảo vệ đến điểm truy cập;

lệnh cho, bởi trạm riêng, điểm truy cập đáp lại vấn tin được bảo vệ trong thời gian thứ nhất định trước; và

khi không nhận được hồi đáp trong thời gian thứ nhất, chấm dứt, bởi trạm riêng, mối liên kết với điểm truy cập.

12. Phương pháp theo điểm 11 còn bao gồm các bước:

sau khi mối liên kết với điểm truy cập bị chấm dứt, gửi, bởi trạm riêng, khung yêu cầu xác thực đến điểm truy cập; và

sau khi khung yêu cầu xác thực được gửi đi, gửi, bởi hệ thống ngăn chặn xâm nhập không dây, khung hủy xác thực đến điểm truy cập hoặc trạm riêng.

13. Phương pháp theo điểm 10 còn bao gồm bước:

truyền, bởi trạm riêng, yêu cầu truy cập đến điểm truy cập,

trong đó tín hiệu nhiễu bao gồm tín hiệu để ngăn điểm truy cập truyền từ chối yêu cầu truy cập đến trạm riêng hoặc ngăn điểm truy cập truyền vấn tin được bảo vệ đến trạm riêng.

14. Phương pháp theo điểm 10, phương pháp này còn bao gồm bước:

truyền, bởi hệ thống ngăn chặn xâm nhập không dây, yêu cầu truy cập đến điểm truy cập,

trong đó tín hiệu nhiễu bao gồm tín hiệu để ngăn điểm truy cập truyền vấn tin được bảo vệ đến trạm riêng.

15. Hệ thống ngăn chặn xâm nhập không dây bao gồm:

thiết bị cảm biến được tạo cấu hình để giám sát khung không dây được truyền/nhận giữa một điểm truy cập và nhiều trạm qua mạng không dây và để xử lý thông tin dựa trên khung không dây; và

máy chủ được tạo cấu hình để xác định xem liệu điểm truy cập và nhiều trạm có trái phép và đang hoạt động bất thường hay không, dựa trên thông tin đã xử lý,

trong đó hệ thống ngăn chặn xâm nhập không dây bao gồm chức năng cung cấp tín hiệu nhiễu để chấm dứt mối liên kết của trạm riêng, trong số nhiều trạm, với điểm truy cập.

trong đó tín hiệu nhiễu bao gồm gói giả mạo, và

trong đó gói giả mạo bao gồm khung yêu cầu liên kết mới (khung liên kết), hoặc khung yêu cầu tái liên kết (khung tái liên kết).

16. Hệ thống ngăn chặn xâm nhập không dây theo điểm 15 còn bao gồm:

chức năng gửi khung hủy xác thực đến điểm truy cập hoặc trạm riêng khi trạm riêng gửi khung yêu cầu xác thực đến điểm truy cập để yêu cầu truy cập vào điểm truy cập.

17. Hệ thống ngăn chặn xâm nhập không dây theo điểm 15, trong đó tín hiệu nhiễu bao gồm tín hiệu để ngăn điểm truy cập đáp lại trạm riêng hoặc truyền vấn tin được bảo vệ đến trạm riêng.

Fig.1

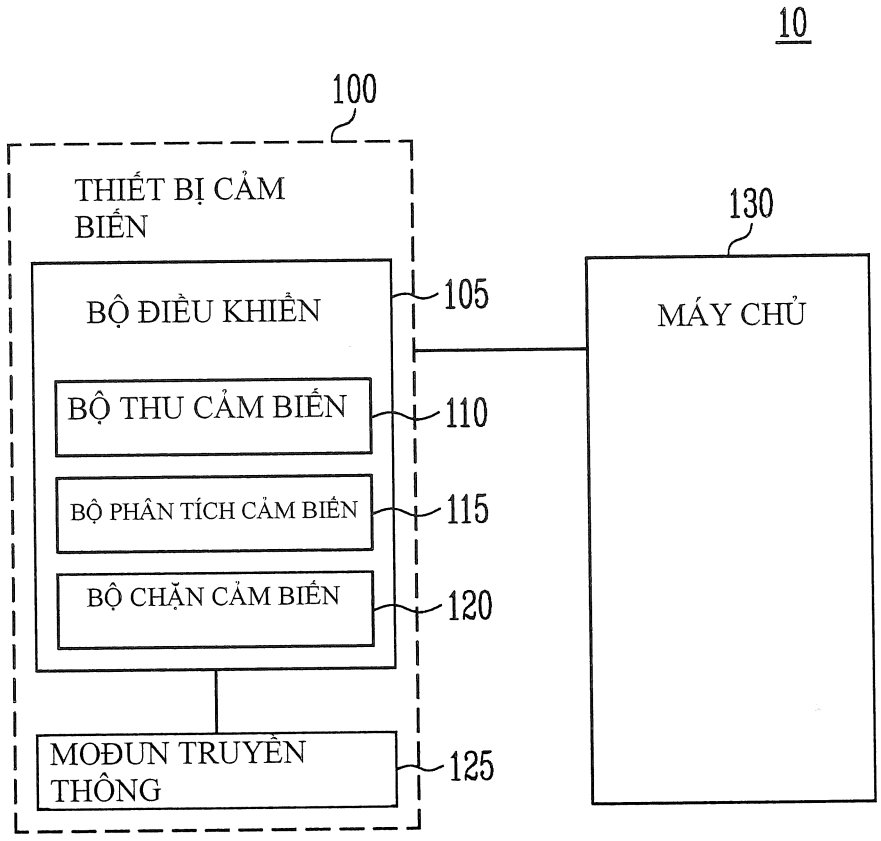

10
100
THIẾT BỊ CẢM BIẾN
BỘ ĐIỀU KHIỂN
105
BỘ THU CẢM BIẾN
110
BỘ PHÂN TÍCH CẢM BIẾN
115
BỘ CHẶN CẢM BIẾN
120
MOĐUN TRUYỀN THÔNG
125
130
MÁY CHỦ

Fig.2

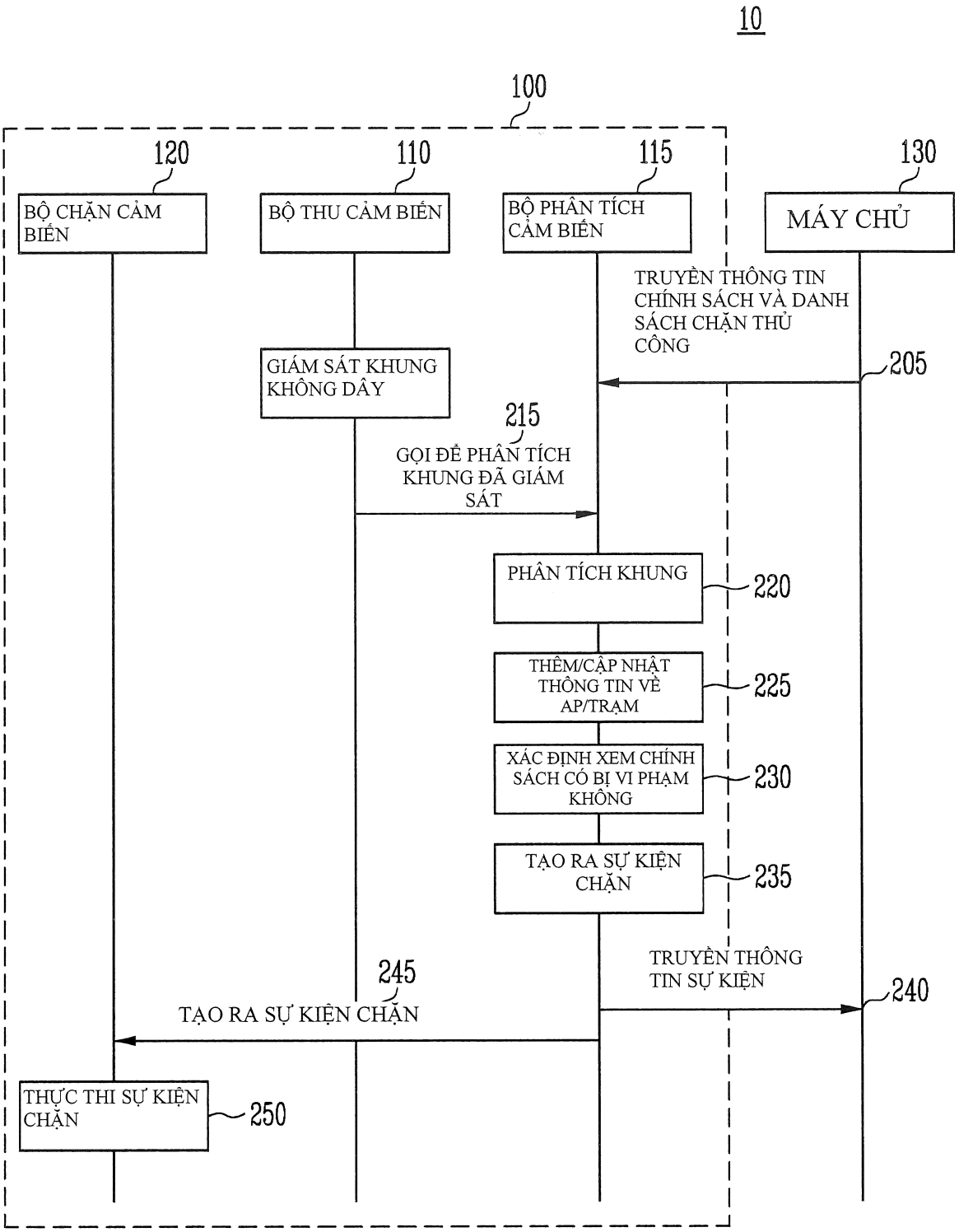

10
100
120
110
115
130
BỘ CHẶN CẢM BIẾN
BỘ THU CẢM BIẾN
BỘ PHÂN TÍCH CẢM BIẾN
MÁY CHỦ
TRUYỀN THÔNG TIN CHÍNH SÁCH VÀ DANH SÁCH CHẶN THỦ CÔNG
205
GIÁM SÁT KHUNG KHÔNG DÂY
215
GỌI ĐỂ PHÂN TÍCH KHUNG ĐÃ GIÁM SÁT
PHÂN TÍCH KHUNG
220
THÊM/CẬP NHẬT THÔNG TIN VỀ AP/TRẠM
225
XÁC ĐỊNH XEM CHÍNH SÁCH CÓ BỊ VI PHẠM KHÔNG
230
TẠO RA SỰ KIỆN CHẶN
235
TRUYỀN THÔNG TIN SỰ KIỆN
240
245
TẠO RA SỰ KIỆN CHẶN
THỰC THI SỰ KIỆN CHẶN
250

Fig.3

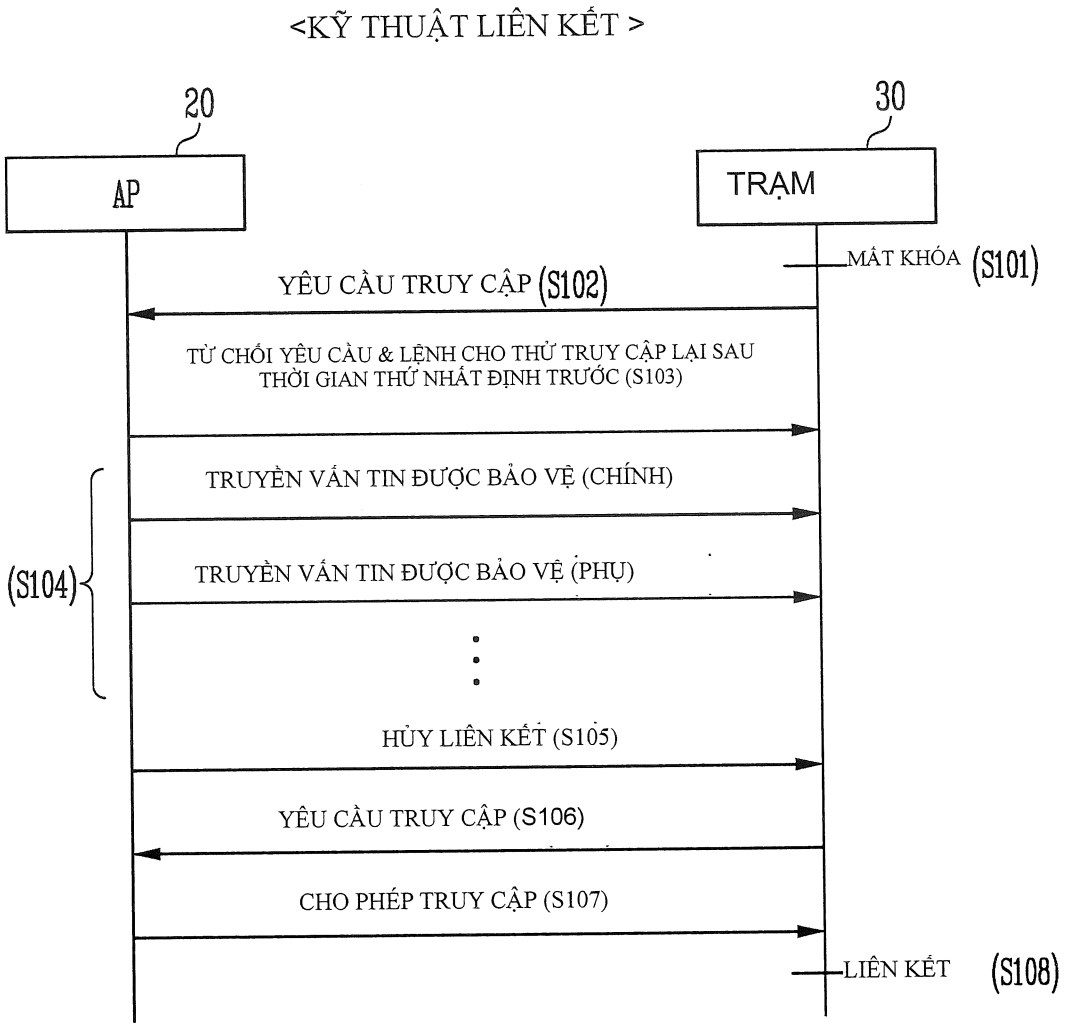

<KỸ THUẬT LIÊN KẾT >
20
AP
30
TRẠM
MẤT KHÓA (S101)
YÊU CẦU TRUY CẬP (S102)
TỪ CHỐI YÊU CẦU & LỆNH CHO THỬ TRUY CẬP LẠI SAU THỜI GIAN THỨ NHẤT ĐỊNH TRƯỚC (S103)
TRUYỀN VẤN TIN ĐƯỢC BẢO VỆ (CHÍNH)
(S104)
TRUYỀN VẤN TIN ĐƯỢC BẢO VỆ (PHỤ)
HỦY LIÊN KẾT (S105)
YÊU CẦU TRUY CẬP (S106)
CHO PHÉP TRUY CẬP (S107)
LIÊN KẾT (S108)

Fig.4

<KỸ THUẬT BẢO VỆ LIÊN KẾT>

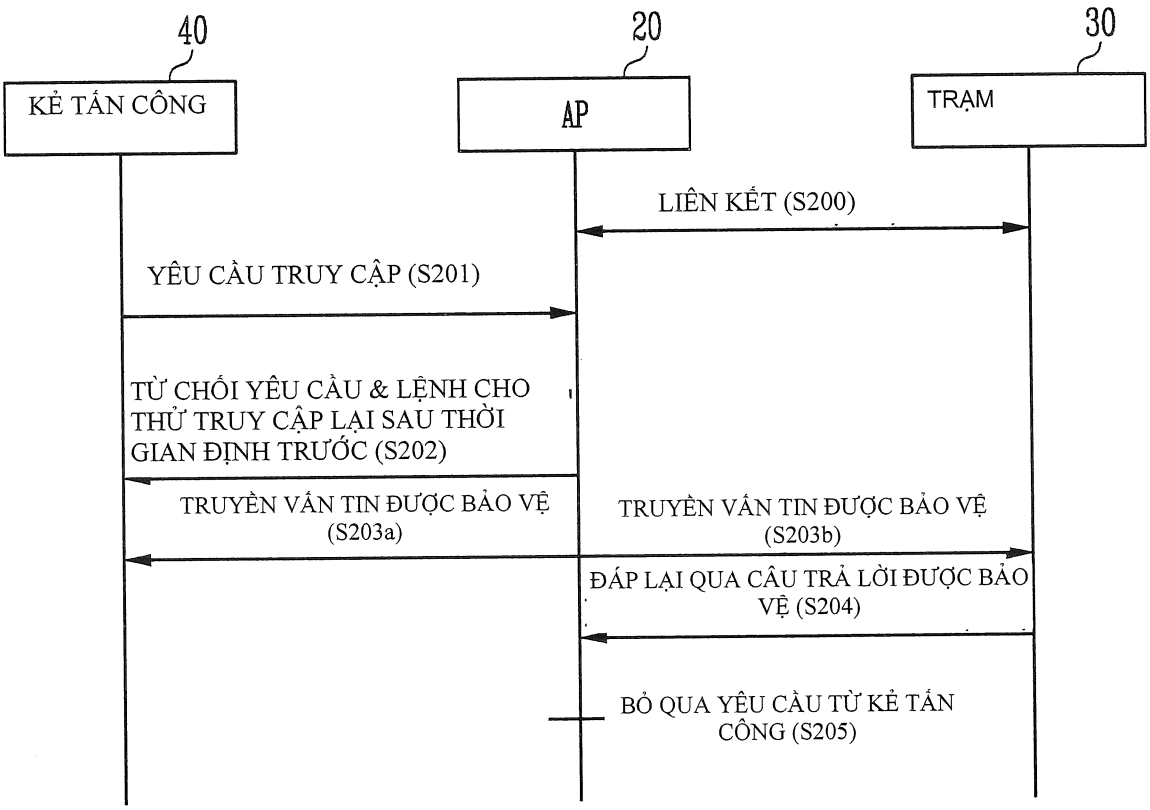


Fig.5

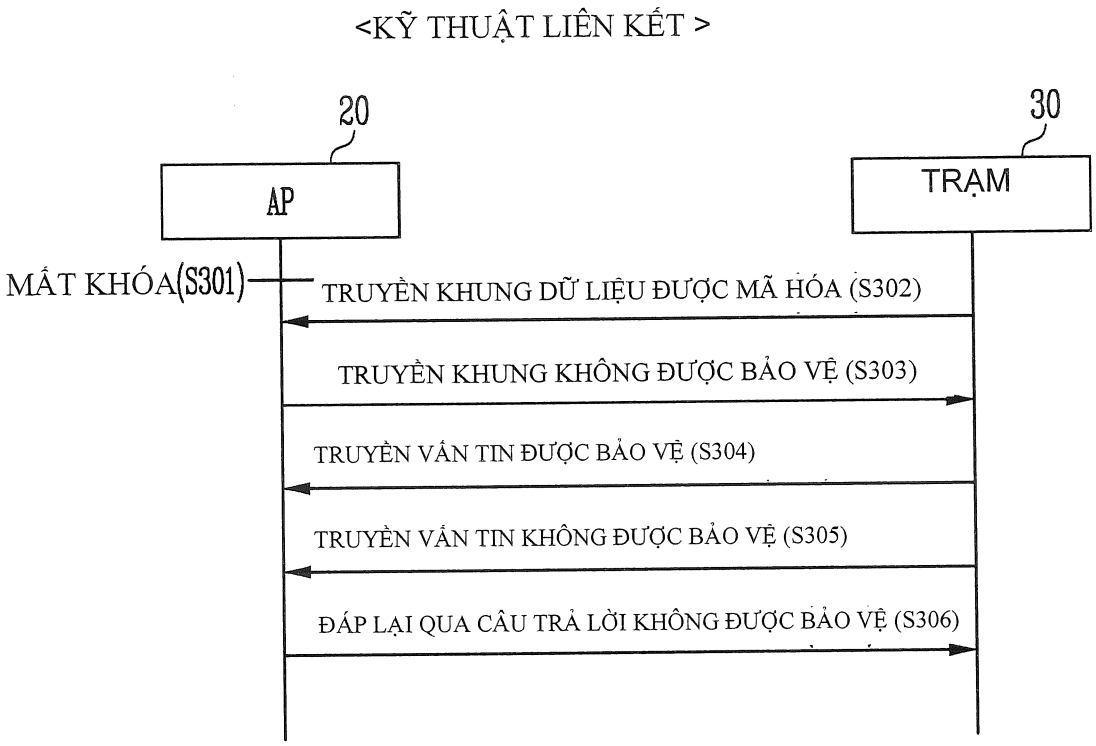

<KỸ THUẬT LIÊN KẾT >
20
AP
30
TRẠM
MẤT KHÓA(S301)
TRUYỀN KHUNG DỮ LIỆU ĐƯỢC MÃ HÓA (S302)
TRUYỀN KHUNG KHÔNG ĐƯỢC BẢO VỆ (S303)
TRUYỀN VẤN TIN ĐƯỢC BẢO VỆ (S304)
TRUYỀN VẤN TIN KHÔNG ĐƯỢC BẢO VỆ (S305)
ĐÁP LẠI QUA CÂU TRẢ LỜI KHÔNG ĐƯỢC BẢO VỆ (S306)

Fig.6

<KỸ THUẬT BẢO VỆ HỦY LIÊN KẾT >

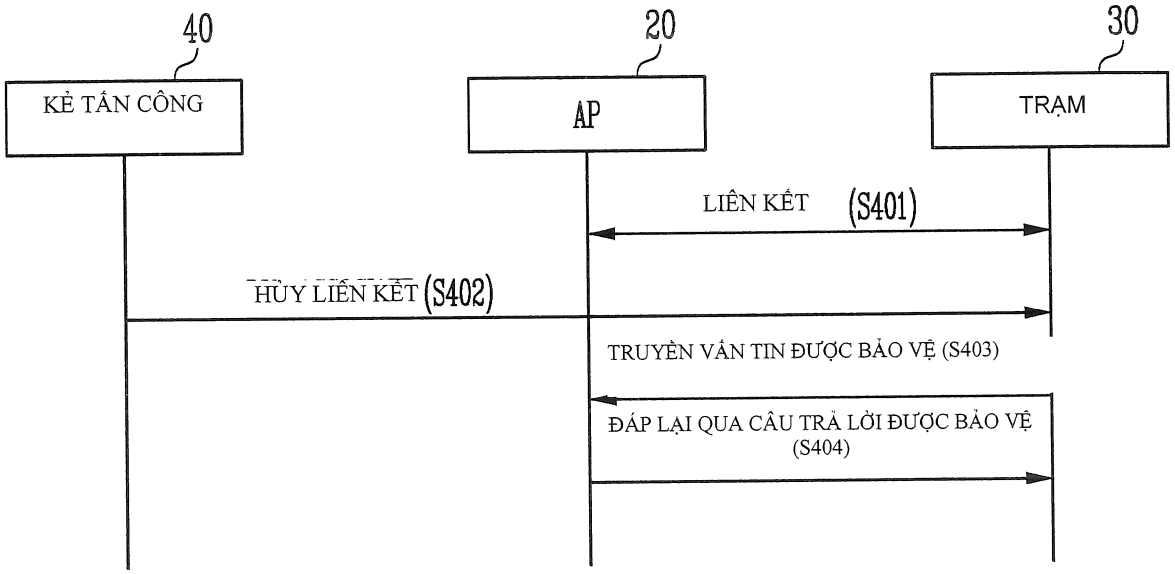


Fig.7

<KỸ THUẬT HỦY LIÊN KẾT TRẠM RIÊNG>

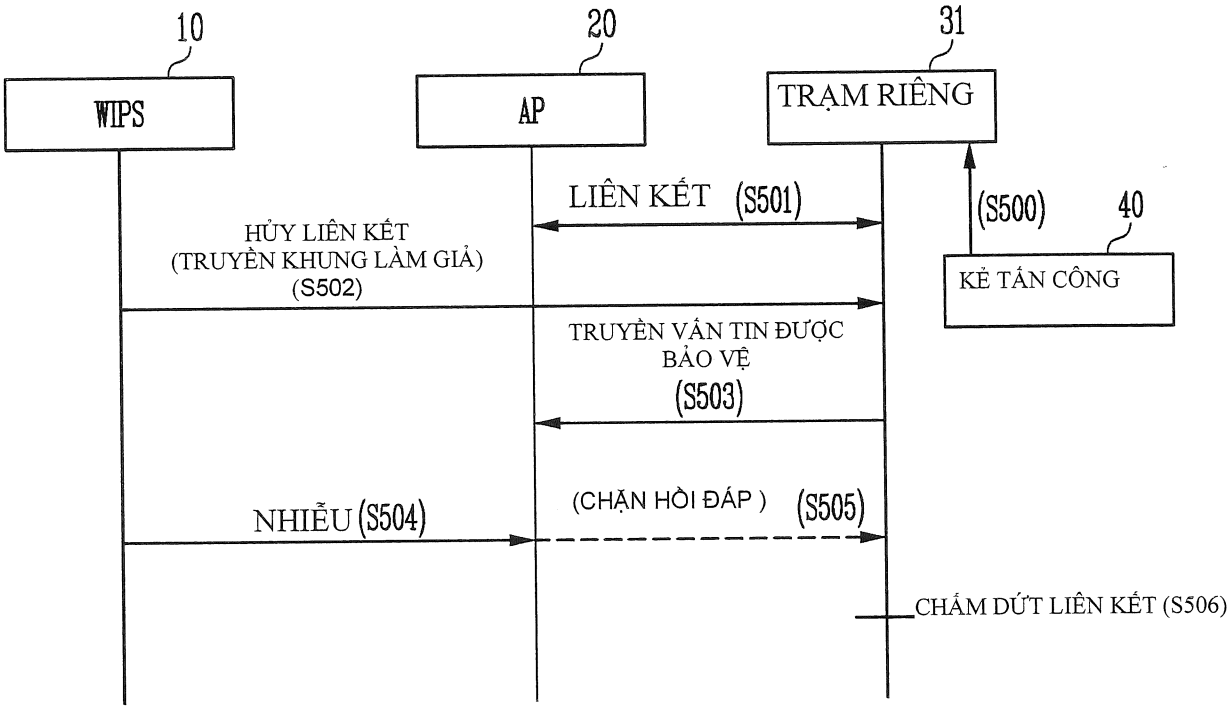


Fig.8

<KỸ THUẬT HỦY LIÊN KẾT TRẠM RIÊNG>

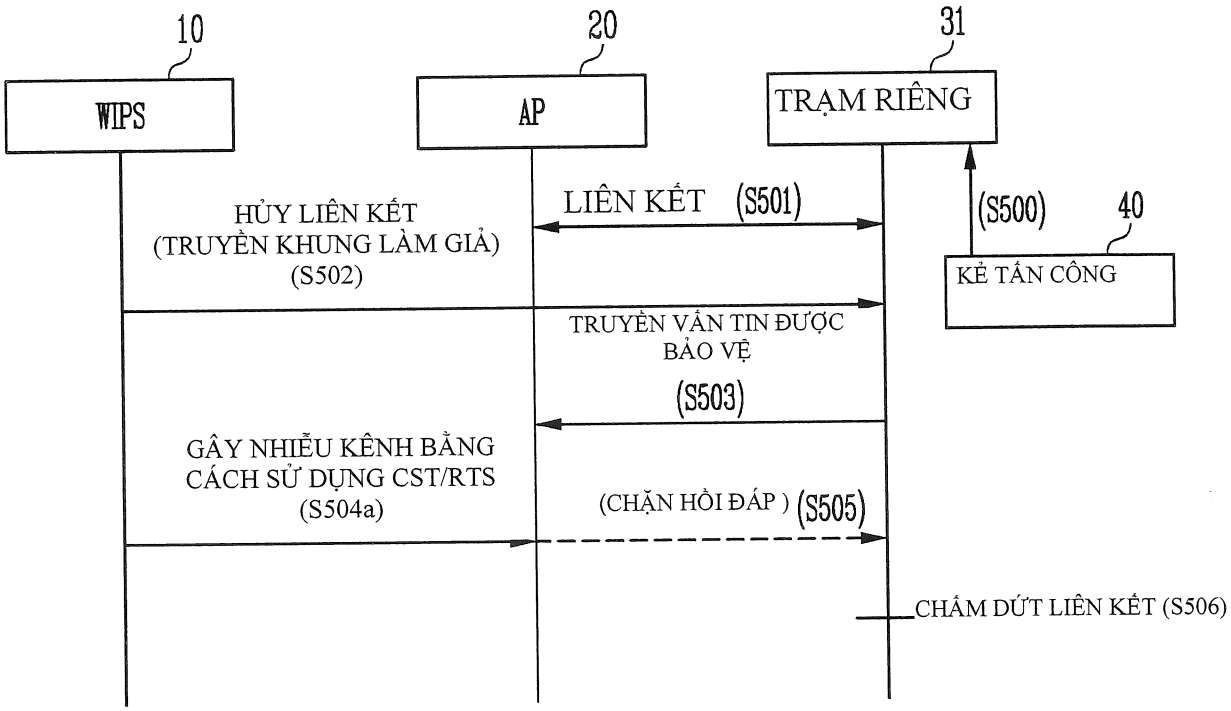


Fig.9

<KỸ THUẬT HỦY LIÊN KẾT TRẠM RIÊNG>

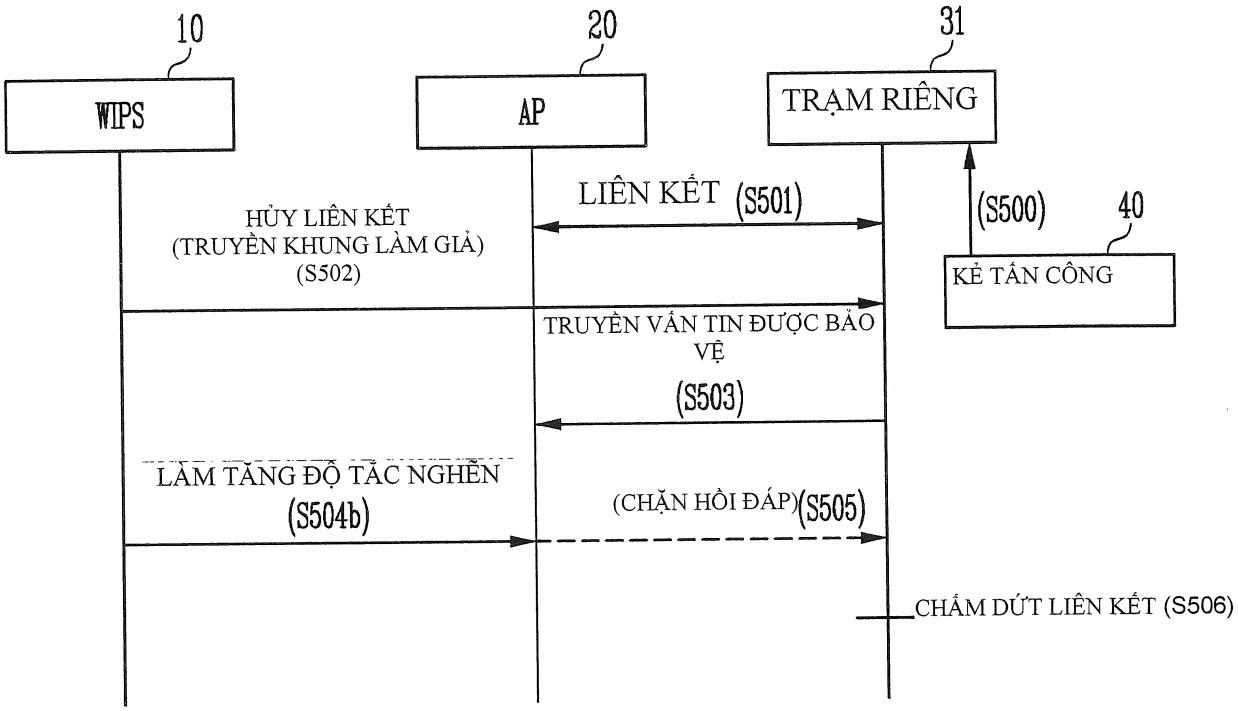


Fig.10

<KỸ THUẬT HỦY LIÊN KẾT TRẠM RIÊNG>

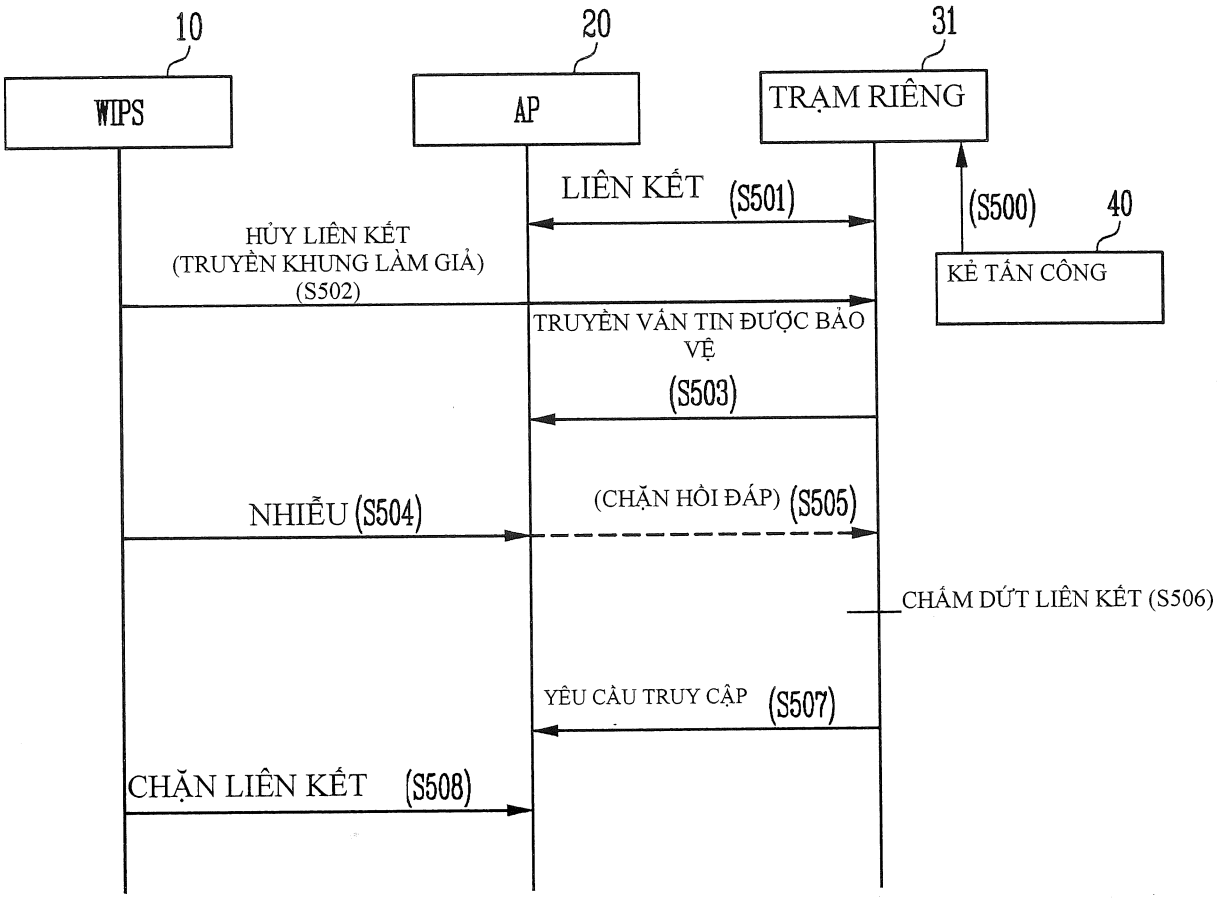


Fig.11

<KỸ THUẬT HỦY LIÊN KẾT CỦA TRẠM RIÊNG>

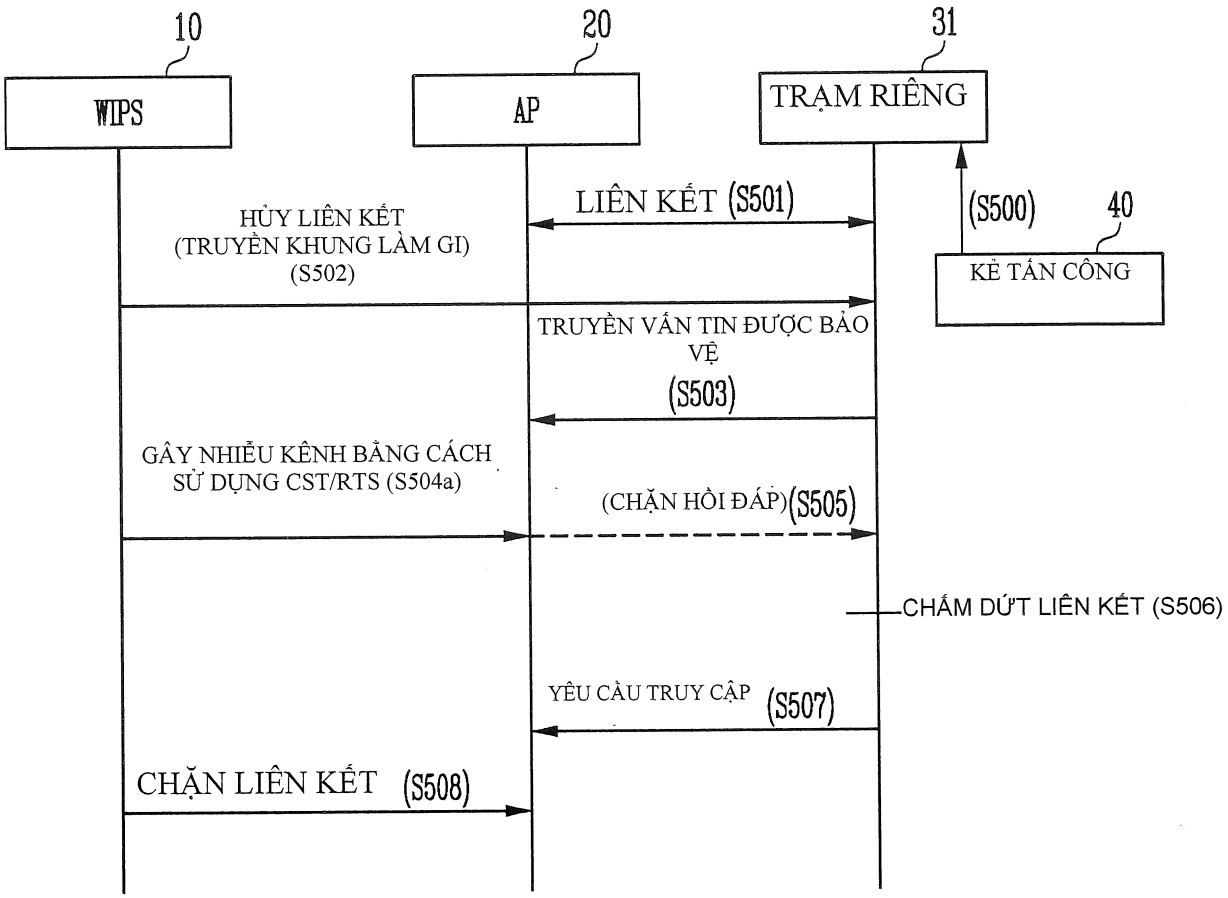


Fig.12

<KỸ THUẬT HỦY LIÊN KẾT TRẠM RIÊNG>

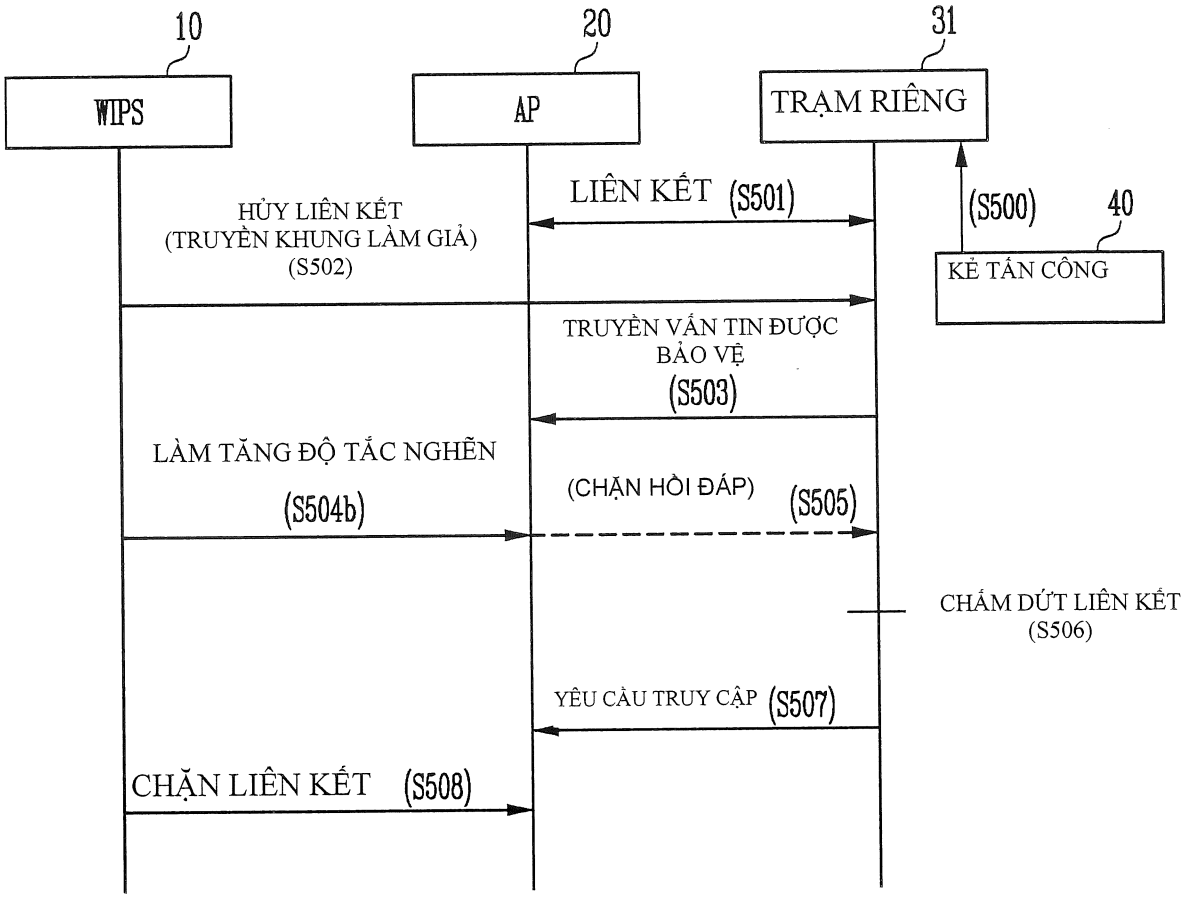


Fig.13

<KỸ THUẬT HỦY LIÊN KẾT TRẠM RIÊNG>

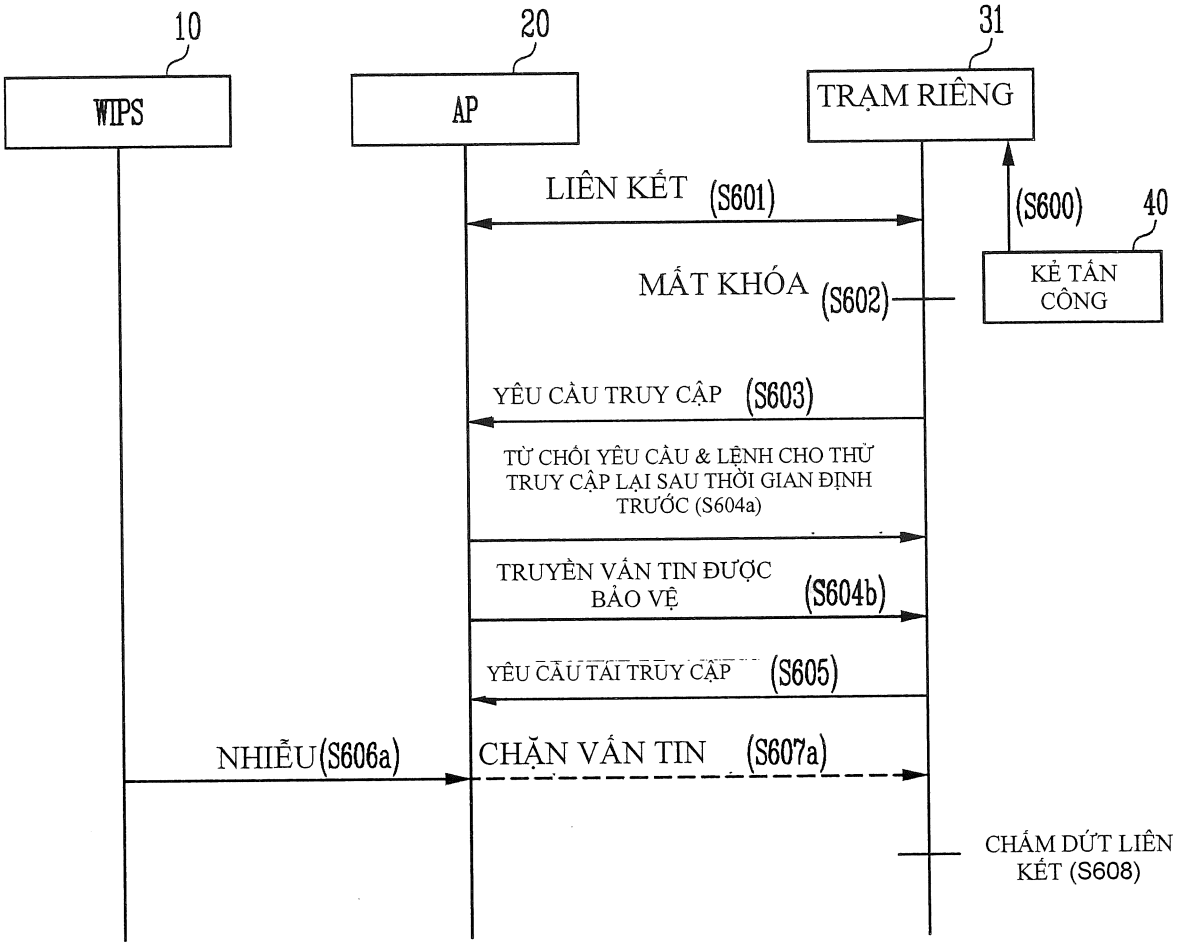


Fig.14

<KỸ THUẬT HỦY LIÊN KẾT TRẠM RIÊNG>

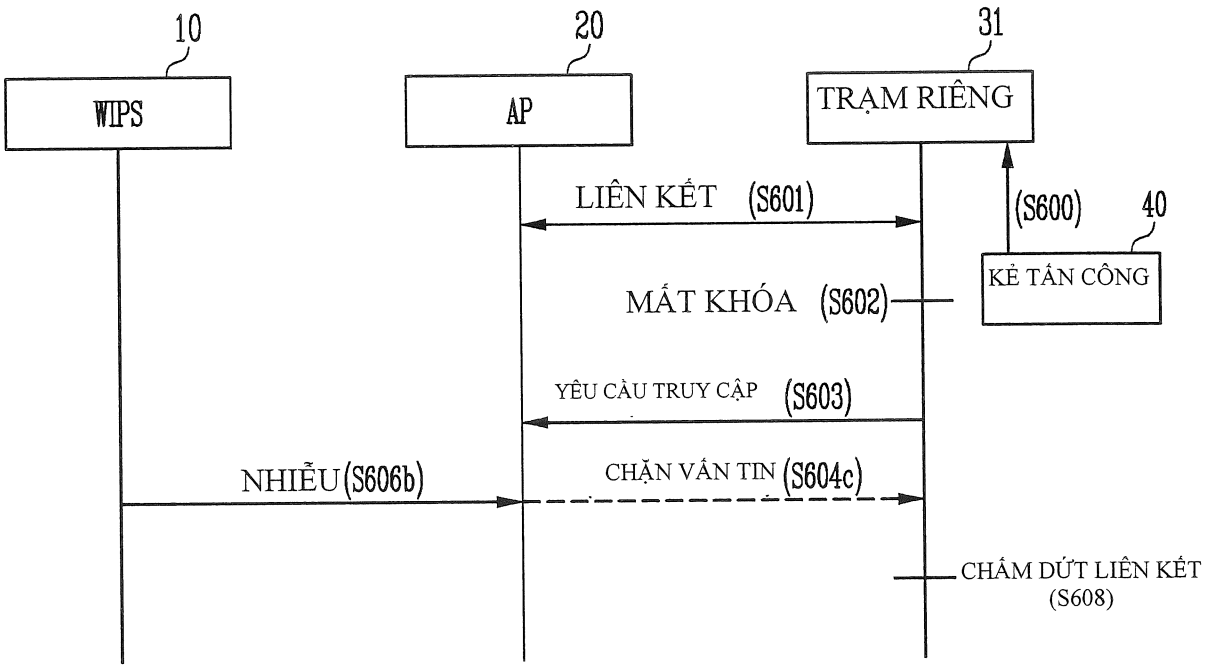


Fig.15

<KỸ THUẬT HỦY LIÊN KẾT TRẠM RIÊNG>

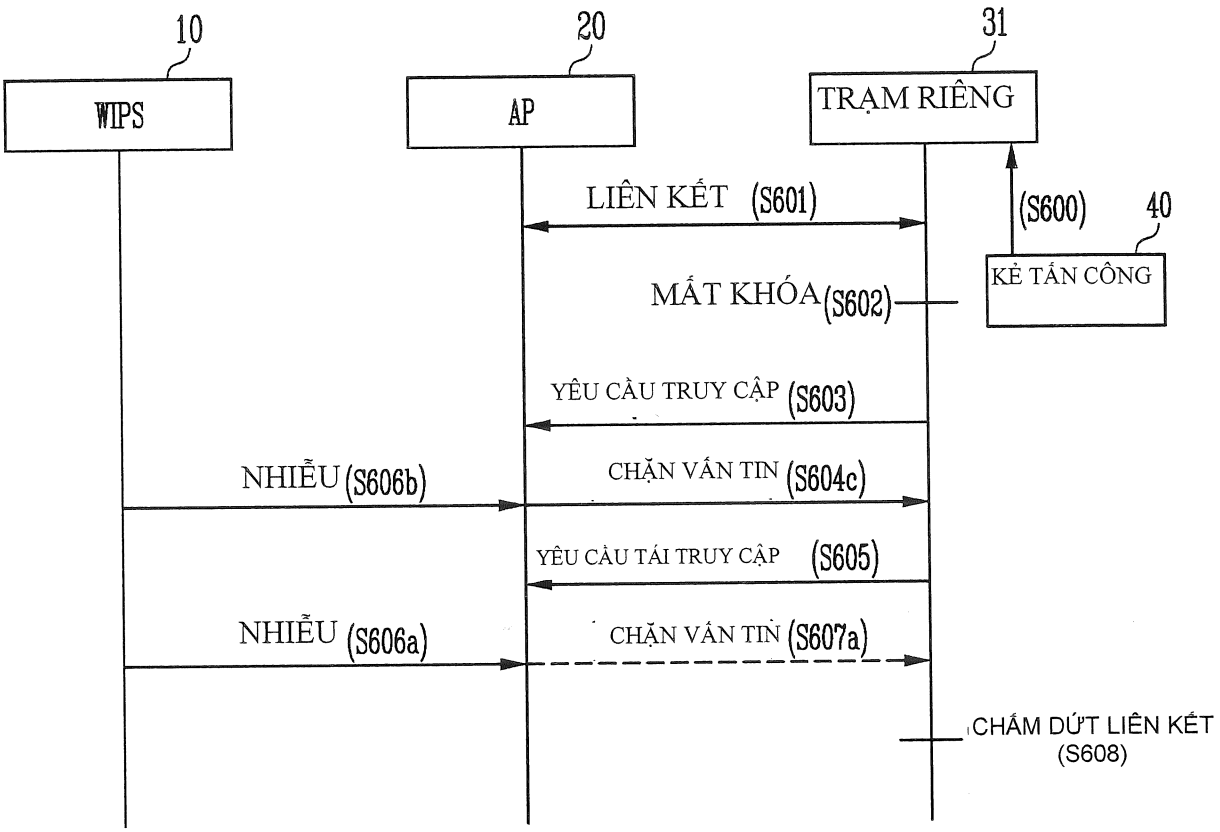
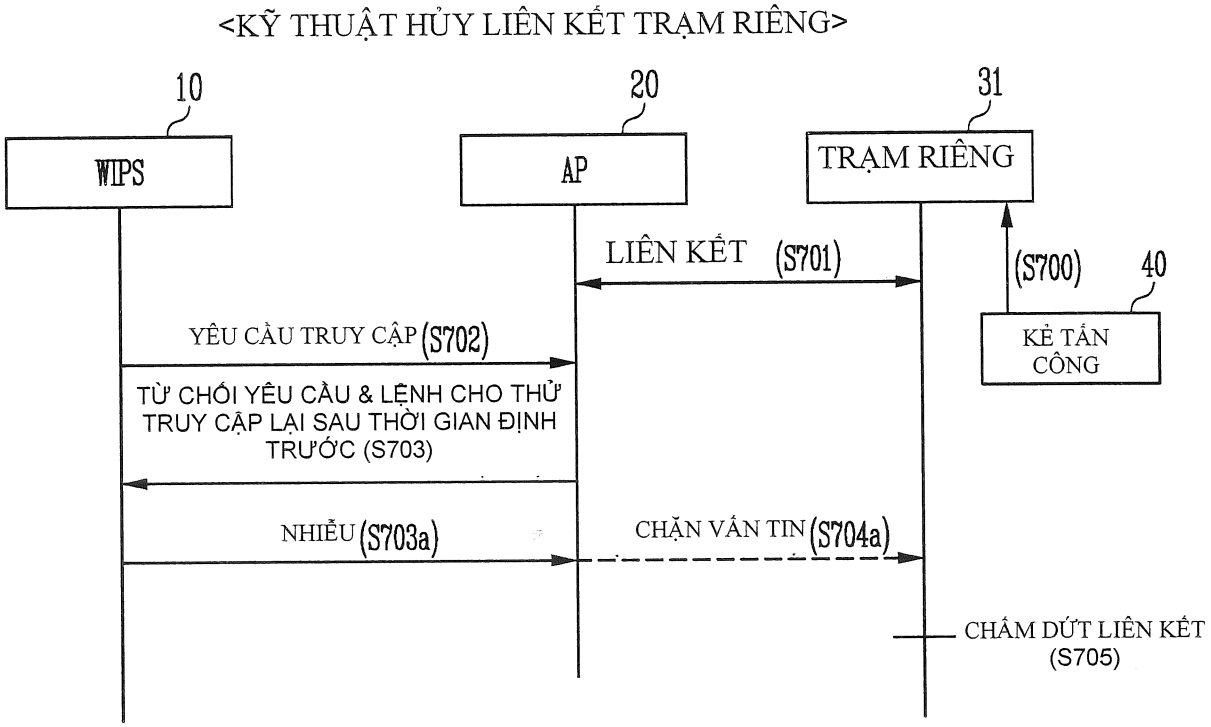


Fig.16


<KỸ THUẬT HỦY LIÊN KẾT TRẠM RIÊNG>
10
WIPS
20
AP
31
TRẠM RIÊNG
LIÊN KẾT (S701)
(S700)
40
KẺ TẤN CÔNG
YÊU CẦU TRUY CẬP (S702)
TỪ CHỐI YÊU CẦU & LỆNH CHO THỬ TRUY CẬP LẠI SAU THỜI GIAN ĐỊNH TRƯỚC (S703)
NHIỄU (S703a)
CHẶN VÁN TIN (S704a)
CHẤM DỨT LIÊN KẾT (S705)