



(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)



1-0026406

(51)⁷ H04W 48/14; H04W 76/02

(13) B

(21) 1-2015-01494

(22) 15/10/2013

(86) PCT/KR2013/009187 15/10/2013

(87) WO 2014/061957 A1 24/04/2014

(30) 61/713,633 15/10/2012 US; 61/721,028 01/11/2012 US; 61/730,472 27/11/2012 US

(45) 25/11/2020 392

(43) 27/07/2015 328A

(73) LG ELECTRONICS INC. (KR)

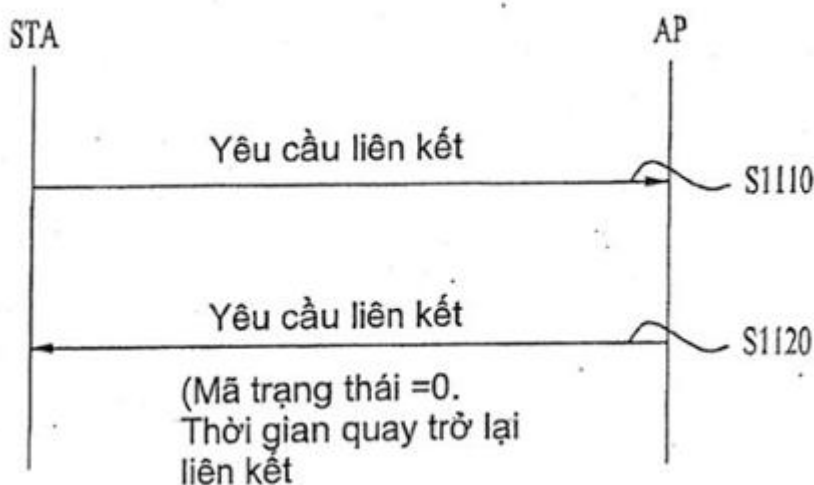
20 Yeouido-dong, Yeongdeungpo-gu Seoul 150-721, Republic of Korea

(72) SEOK, Yongho (KR).

(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) PHƯƠNG PHÁP THỰC HIỆN LIÊN KẾT BỞI TRẠM TRONG HỆ THỐNG MẠNG VÙNG CỤC BỘ (LAN) KHÔNG DÂY, PHƯƠNG PHÁP HỖ TRỢ LIÊN KẾT CỦA TRẠM BỞI ĐIỂM TRUY CẬP TRONG HỆ THỐNG LAN KHÔNG DÂY, TRẠM VÀ ĐIỂM TRUY CẬP

(57) Sáng chế đề cập đến phương pháp và thiết bị duy trì liên kết trong hệ thống WLAN. Phương pháp thực hiện liên kết bởi trạm (STA) trong hệ thống LAN không dây (WLAN) bao gồm: truyền khung yêu cầu liên kết từ trạm (STA) đến điểm truy cập (AP); và thu khung phản hồi liên kết từ điểm truy cập (AP) phản hồi lại khung yêu cầu liên kết. Nếu yêu cầu liên kết được chấp nhận bởi điểm truy cập (AP), khung phản hồi liên kết bao gồm thông tin liên quan đến với thời gian quay trở lại liên kết.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hệ thống truyền thông không dây, và cụ thể hơn là sáng chế đề cập đến phương pháp và thiết bị duy trì liên kết trong hệ thống LAN không dây (WLAN).

Tình trạng kỹ thuật của sáng chế

Các hệ thống công nghệ truyền thông không dây khác nhau đã được phát triển với sự phát triển nhanh chóng của các công nghệ truyền thông thông tin. Công nghệ WLAN trong số các công nghệ truyền thông không dây cho phép truy cập internet không dây tại nhà hoặc trong các doanh nghiệp hoặc ở khu vực cung cấp dịch vụ cụ thể bằng cách sử dụng các thiết bị đầu cuối di động, chẳng hạn thiết bị kỹ thuật số hỗ trợ cá nhân (Personal Digital Assistant - PDA), máy tính xách tay, máy nghe nhạc cầm tay đa chức năng (Portable Multimedia Player - PMP), v.v., dựa trên công nghệ tần số radio (Radio Frequency - RF).

Để tránh tốc độ truyền thông bị giới hạn, một trong số những ưu điểm của WLAN, tiêu chuẩn kỹ thuật gần đây đã đề xuất hệ thống cải tiến có khả năng tăng tốc độ và độ ổn định của mạng khi đồng thời mở rộng vùng phủ sóng của mạng không dây. Ví dụ, viện kỹ thuật điện và điện tử (Institute of Electrical and Electronics Engineers - IEEE) 802.11n cho phép tốc độ xử lý dữ liệu để hỗ trợ thông lượng cao (high throughput HT) lớn nhất là 540Mbps. Ngoài ra, công nghệ đa đầu vào và đa đầu ra (Multiple Input and Multiple Output - MIMO) gần đây được ứng dụng cho cả bộ truyền và bộ thu để tối thiểu hóa các lỗi truyền cũng như lớn nhất hóa tốc độ chuyển dữ liệu.

Vấn đề kỹ thuật cần giải quyết

Công nghệ truyền thông máy tới máy (Machine to Machine - M2M) đã được thảo luận như là công nghệ truyền thông thế hệ kế tiếp. Tiêu chuẩn kỹ thuật

để hỗ trợ truyền thông M2M trong WLAN IEEE 802.11 được phát triển là IEEE 802.11ah. Truyền thông M2M có thể xem xét trường hợp có khả năng truyền thông một lượng nhỏ dữ liệu một cách không thường xuyên ở tốc độ thấp trong môi trường bao gồm một lượng lớn các thiết bị.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất phương pháp cho phép trạm (STA) duy trì liên kết chính xác với điểm truy cập (AP).

Được hiểu rằng các mục đích kỹ thuật đạt được bởi sáng chế là không bị giới hạn ở các mục đích kỹ thuật được đề cập ở trên và các mục đích kỹ thuật khác mà không được đề cập ở đây sẽ là rõ ràng từ phần mô tả dưới đây đối với người có hiểu biết trung bình trong lĩnh vực mà sáng chế đề cập tới.

Giải pháp kỹ thuật

Mục đích của sáng chế có thể đạt được bằng cách đề xuất phương pháp thực hiện liên kết bởi trạm (STA) trong hệ thống LAN không dây (WLAN) bao gồm: truyền khung yêu cầu liên kết từ trạm (STA) đến điểm truy cập (AP); và thu khung phản hồi liên kết từ điểm truy cập (AP) này phản hồi lại khung yêu cầu liên kết, trong đó, nếu yêu cầu liên kết này được chấp nhận bởi điểm truy cập (AP), khung phản hồi liên kết bao gồm thông tin liên quan đến thời gian quay trở lại liên kết

Theo khía cạnh khác của sáng chế, phương pháp hỗ trợ liên kết của trạm (STA) bởi điểm truy cập (AP) trong hệ thống LAN không dây (WLAN) bao gồm: thu khung yêu cầu liên kết từ trạm (STA); và truyền khung phản hồi liên kết đến trạm (STA) này phản hồi lại khung yêu cầu liên kết này, trong đó, nếu yêu cầu liên kết này được chấp nhận bởi điểm truy cập (AP), khung phản hồi liên kết bao gồm thông tin liên quan đến thời gian quay trở lại liên kết.

Theo khía cạnh khác của sáng chế, thiết bị trạm (STA) thực hiện liên kết trong hệ thống LAN không dây (WLAN) bao gồm: bộ thu truyền; và bộ xử lý, trong đó bộ xử lý này truyền khung yêu cầu liên kết đến điểm truy cập (AP) bằng cách sử dụng bộ thu truyền, và thu khung phản hồi liên kết từ điểm truy cập (AP) này phản hồi lại khung yêu cầu liên kết, trong đó, nếu yêu cầu liên kết được chấp nhận bởi điểm truy cập (AP), khung phản hồi liên kết bao gồm thông tin đối với thời gian quay trở lại liên kết.

Theo khía cạnh khác của sáng chế, thiết bị điểm truy cập (AP) hỗ trợ liên kết của trạm (STA) trong hệ thống LAN không dây (WLAN) bao gồm: bộ thu truyền; và bộ xử lý, trong đó bộ xử lý này thu khung yêu cầu liên kết từ trạm (STA) bằng cách sử dụng bộ thu truyền, và truyền khung phản hồi liên kết đến trạm (STA) phản hồi lại khung yêu cầu liên kết bằng cách sử dụng bộ thu truyền, trong đó, nếu yêu cầu liên kết được chấp nhận bởi điểm truy cập (AP), khung phản hồi liên kết bao gồm thông tin liên quan đến thời gian quay trở lại liên kết

Phần mô tả sau đây nói chung có thể được áp dụng cho các phương án của sáng chế.

STA có thể hoạt động trên cơ sở thời gian quay trở lại liên kết, và cố gắng thu khung yêu cầu truy vấn liên kết bảo mật (SA) từ AP.

STA có thể hoạt động ở các khoảng thời gian giống nhau hoặc khoảng thời gian ngắn hơn thời gian định trước được chỉ báo bởi thời gian quay trở lại liên kết, và cố gắng thu khung yêu cầu truy vấn SA.

Dựa trên thu khung yêu cầu truy vấn SA từ AP, STA có thể truyền khung yêu cầu truy vấn SA đến AP.

Thông qua việc thu khung yêu cầu truy vấn SA hoặc truyền khung yêu cầu truy vấn SA, trạng thái SA hợp lệ của STA có thể được duy trì.

Giá trị thời gian chờ của quy trình truy vấn SA có thể được thiết lập trên cơ sở thời gian quay trở lại liên kết.

Giá trị thời gian chờ của quy trình truy vấn SA có thể được đặt giá trị là `dot11AssociationSAQueryMaximumTimeout`.

Nếu yêu cầu liên kết được chấp nhận bởi AP, mã trạng thái của khung phản hồi liên kết có thể được thiết đặt ở số không (0), trong đó mã trạng thái '0' chỉ báo "thành công".

Nếu yêu cầu liên kết bị từ chối bởi AP, khung phản hồi liên kết có thể bao gồm thông tin liên quan đến thời gian quay trở lại liên kết.

Nếu yêu cầu liên kết bị từ chối bởi AP, mã trạng thái của khung phản hồi liên kết có thể được thiết đặt ở 30, trong đó mã trạng thái '30' chỉ báo "Yêu cầu liên kết tạm thời bị từ chối; thử lại sau".

STA có thể hoạt động trong chế độ tiết kiệm điện (PS).

Trạm (STA) có thể có trạng thái liên kết bảo mật (SA) với điểm truy cập (AP) trước khi truyền khung yêu cầu liên kết.

Được hiểu rằng cả phần mô tả chung trước đó và phần mô tả chi tiết sau đây của sáng chế là để làm ví dụ và có tính giải thích và nhằm mục đích đề xuất sự giải thích thêm về sáng chế như được bảo hộ.

Hiệu quả của sáng chế

Như rõ ràng từ phần mô tả ở trên, các phương án được lấy làm ví dụ của sáng chế đề xuất phương pháp cho phép trạm (STA) duy trì liên kết chính xác với điểm truy cập (AP).

Người có hiểu biết trung bình trong lĩnh vực sẽ hiểu rằng những hiệu quả mà có thể đạt được bởi sáng chế không bị giới hạn ở những phần được mô tả cụ thể ở trên và những ưu điểm khác của sáng chế sẽ được hiểu rõ hơn từ phần mô tả chi tiết dưới đây được mô tả dựa vào các hình vẽ đi kèm.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo, mà được bao gồm để hiểu thêm về sáng chế, minh họa các phương án của sáng chế và cùng với phần mô tả giải thích nguyên lý của sáng chế.

Fig.1 thể hiện dưới dạng ví dụ hệ thống IEEE 802.11 theo một phương án của sáng chế.

Fig.2 thể hiện dưới dạng ví dụ hệ thống IEEE 802.11 theo phương án khác của sáng chế.

Fig.3 thể hiện dưới dạng ví dụ hệ thống IEEE 802.11 theo phương án khác nữa của sáng chế.

Fig.4 là sơ đồ khái niệm minh họa hệ thống WLAN.

Fig.5 là lưu đồ minh họa quy trình cài đặt kết nối để sử dụng trong hệ thống WLAN.

Fig.6 là sơ đồ khái niệm minh họa hoạt động quản lý công suất.

Fig.7 là sơ đồ khái niệm minh họa định dạng được lấy làm ví dụ của khung yêu cầu truy vấn liên kết bảo mật (SA) và khung phản hồi truy vấn liên kết bảo mật (SA).

Fig.8 là sơ đồ khái niệm minh họa ví dụ về quy trình truy vấn SA.

Fig.9 là sơ đồ khái niệm minh họa ví dụ khác về quy trình truy vấn SA.

Fig.10 là sơ đồ khái niệm minh họa ví dụ khác về quy trình truy vấn SA.

Fig.11 là các sơ đồ khái niệm minh họa các phương án khác nhau của quy trình hỏi vòng PS bảo mật.

Fig.12 là sơ đồ khối minh họa phương pháp duy trì liên kết theo ví dụ của sáng chế.

Fig.13 là sơ đồ khối minh họa thiết bị tần số radio (RF) theo một phương án của sáng chế.

Mô tả chi tiết sáng chế

Dựa vào các phương án được ưu tiên của sáng chế, các ví dụ của sáng chế được minh họa trên các hình vẽ kèm theo. Phần mô tả chi tiết, được trình bày dưới đây dựa vào các hình vẽ kèm theo, nhằm để giải thích các phương án được lấy làm ví dụ của sáng chế, chứ không phải là chỉ thể hiện các phương án mà có thể được thực hiện của sáng chế. Phần mô tả chi tiết dưới đây gồm có các chi tiết cụ thể để cung cấp hiểu biết toàn bộ về sáng chế. Tuy nhiên, điều rõ ràng đối với người có hiểu biết trung bình trong lĩnh vực kỹ thuật này là sáng chế có thể được áp dụng thực tế mà không cần có những chi tiết cụ thể như vậy.

Các phương án sau đây được đề xuất bằng cách kết hợp các thành phần và các dấu hiệu đặc trưng cấu thành của sáng chế theo định dạng được định trước. Các thành phần hoặc các dấu hiệu đặc trưng riêng rẽ cấu thành được coi là các yếu tố tùy chọn với điều kiện là không có lưu ý nào thêm. Nếu cần, các thành phần hoặc các dấu hiệu đặc trưng riêng rẽ cấu thành có thể không được kết hợp với các thành phần hoặc các dấu hiệu đặc trưng khác. Ngoài ra, một số các thành phần và/hoặc các dấu hiệu đặc trưng cấu thành có thể được kết hợp để thực hiện các phương án của sáng chế. Thứ tự các hoạt động được bộc lộ trong các phương án của sáng chế có thể được thay đổi. Một số các thành phần hoặc các dấu hiệu đặc trưng của phương án bất kỳ có thể cũng có thể được bao gồm trong các phương án khác, hoặc có thể được thay thế bằng các thành phần hoặc các dấu hiệu đặc trưng của các phương án khác nếu cần.

Cần lưu ý rằng các thuật ngữ cụ thể được bộc lộ trong sáng chế được đề xuất để thuận tiện cho phần mô tả và hiểu rõ hơn về sáng chế, và việc sử dụng các thuật ngữ cụ thể này có thể được thay đổi sang các định dạng trong phạm vi kỹ thuật của sáng chế.

Trong một số trường hợp, các cấu trúc và các thiết bị đã biết được bỏ qua để tránh làm khó hiểu những khái niệm của sáng chế và các chức năng quan trọng của các cấu trúc và các thiết bị được thể hiện dưới dạng sơ đồ khối. Các số chỉ dẫn giống nhau sẽ được sử dụng trong toàn bộ các hình vẽ để đề cập đến các phần giống nhau hoặc các phần tương tự.

Các phương án được lấy làm ví dụ của sáng chế được hỗ trợ bởi các tài liệu tiêu chuẩn được bộc lộ đối với ít nhất một trong số các hệ thống truy cập không dây bao gồm hệ thống viện kỹ thuật điện và điện tử (IEEE) 802, hệ thống dự án đối tác thế hệ thứ ba (3GPP), hệ thống phát triển dài hạn (LTE) 3GPP, hệ thống LTE-cải tiến (LTE-A), và hệ thống 3GPP2. Cụ thể, các bước hoặc các phần, mà không được mô tả để bộc lộ rõ ý tưởng công nghệ của sáng chế, trong các phương án của sáng chế có thể được hỗ trợ bằng các tài liệu ở trên. Tất cả thuật ngữ được sử dụng ở đây có thể được hỗ trợ bởi ít nhất một trong số các tài liệu được đề cập ở trên.

Các phương án sau đây của sáng chế có thể được áp dụng cho các kỹ thuật truy cập không dây khác nhau, ví dụ, CDMA (Code division multiple access - Đa truy cập phân chia theo mã), FDMA (Frequency division multiple access - Đa truy cập phân chia theo tần số), TDMA (Time division multiple access - Đa truy cập phân chia theo thời gian), OFDMA (Orthogonal frequency division multiple access - Đa truy cập phân chia theo tần số trực giao), SC-FDMA (Single carrier frequency division multiple access - Đa truy cập phân chia theo tần số sóng đơn), và tương tự. CDMA có thể được thể hiện qua công nghệ không dây (hoặc radio) chẳng hạn UTRA (Universal terrestrial radio access - Truy cập vô tuyến mặt đất toàn cầu) hoặc CDMA2000. TDMA có thể được thể hiện qua công nghệ không dây (hoặc radio) chẳng hạn GSM (Global system for Mobile communication - Mạng thông tin di động toàn cầu)/GPRS (General

packet radio service - Dịch vụ vô tuyến gói dữ liệu chung)/EDGE (Enhanced data rates for GSM Evolution - Tốc độ chuyển dữ liệu nâng cao cho GSM cải tiến). OFDMA có thể được bao gồm công nghệ không dây (hoặc radio) chẳng hạn viện kỹ thuật điện và điện tử (IEEE) 802.11 (Wi-Fi), IEEE 802.16 (WiMAX), IEEE 802.20, và E-UTRA (UTRA cải tiến). Để làm rõ, phần mô tả sau đây tập trung vào các hệ thống IEEE 802.11. Tuy nhiên, các dấu hiệu kỹ thuật của sáng chế không bị giới hạn ở đó.

Cấu trúc hệ thống WLAN

Fig.1 thể hiện dưới dạng ví dụ hệ thống IEEE 802.11 theo một phương án của sáng chế.

Cấu trúc của hệ thống IEEE 802.11 có thể bao gồm nhiều thành phần. WLAN mà hỗ trợ tính di động STA trong suốt cho lớp cao hơn có thể được đề xuất bởi các hoạt động tương hỗ của các thành phần. Tập dịch vụ cơ bản (Basic service set - BSS) có thể tương ứng với khối cấu thành cơ bản trong LAN IEEE 802.11. Trên Fig.1, hai BSS (BSS1 và BSS2) được thể hiện và hai STA được bao gồm trong mỗi BSS (tức là STA1 và STA2 được bao gồm trong BSS1 và STA3 và STA4 được bao gồm trong BSS2). Hình elíp chỉ báo BSS trên Fig.1 có thể được hiểu là vùng phủ sóng trong đó các STA được bao gồm trong BSS tương ứng duy trì truyền thông. Vùng này có thể được gọi là vùng dịch vụ cơ bản (BSA). Nếu STA di chuyển khỏi BSA, STA không thể trực tiếp truyền thông với các STA trong BSA tương ứng.

Trong LAN IEEE 802.11, dạng cơ bản nhất của BSS là BSS độc lập (IBSS). Ví dụ, IBSS có thể có dạng nhỏ nhất bao gồm chỉ hai STA. BSS (BSS1 hoặc BSS2) của Fig.1, là dạng đơn giản nhất và trong đó các thành phần khác được bỏ qua, có thể tương ứng với ví dụ điển hình về IBSS. Cấu hình như vậy là có thể khi các STA mà có thể trực tiếp truyền thông với những cái khác. Dạng

LAN như thế không được lập lịch trước và có thể được cấu hình khi LAN là cần thiết. Điều này có thể được gọi là mạng ad-hoc.

Các thành viên của STA trong BSS có thể được thay đổi động khi STA được bật hoặc tắt hoặc STA đi vào hoặc ra khỏi vùng BSS. STA có thể sử dụng quy trình đồng bộ hóa để tham gia BSS. Để truy cập tất cả các dịch vụ của hạ tầng cơ sở BSS, STA nên được liên kết với BSS. Liên kết như vậy có thể được cấu hình động và có thể bao gồm việc sử dụng dịch vụ hệ thống phân phối (DSS).

Fig.2 là sơ đồ thể hiện cấu trúc khác được lấy làm ví dụ của hệ thống IEEE 802.11 mà sáng chế có thể ứng dụng. Trên Fig.2, các thành phần chẳng hạn hệ thống phân phối (DS), môi trường hệ thống phân phối (DSM), và điểm truy cập (AP) được bổ sung vào cấu trúc của Fig.1.

Khoảng cách STA-đến-STA trực tiếp trong LAN có thể bị hạn chế bởi hiệu suất PHY. Trong một số trường hợp, sự hạn chế khoảng cách như vậy có thể là đủ để truyền thông. Tuy nhiên, trong các trường hợp khác, sự truyền thông giữa các STA ở khoảng cách dài có thể là cần thiết. DS có thể được cấu hình để hỗ trợ phủ sóng mở rộng.

DS đề cập đến cấu trúc trong đó các BSS được kết nối với những cái khác. Cụ thể, BSS có thể được cấu hình là thành phần dạng mở rộng của mạng bao gồm nhiều BSS, thay vì cấu hình độc lập như được thể hiện trên Fig.1.

DS là khái niệm logic và có thể được cụ thể hóa bởi dấu hiệu đặc trưng của DSM. Liên quan tới điều này, môi trường không dây (WM) và DSM về mặt logic được phân biệt trong IEEE 802.11. Các môi trường logic tương ứng được sử dụng cho các mục đích khác nhau và được sử dụng bởi các thành phần khác nhau. Trong định nghĩa về IEEE 802.11, các môi trường như vậy không bị giới hạn đối với các môi trường giống hoặc khác nhau. Tính linh động của kiến trúc LAN IEEE 802.11 (kiến trúc DS hoặc các kiến trúc mạng khác) có thể được giải

thích trong đó nhiều môi trường khác nhau về mặt logic. Tức là, kiến trúc LAN IEEE 802.11 có thể được thực hiện một cách khác nhau và có thể được cụ thể hóa một cách độc lập bởi dấu hiệu đặc trưng vật lý của mỗi cách thực hiện.

DS có thể hỗ trợ các thiết bị di động bằng cách đề xuất sự tích hợp liên mạch của nhiều BSS và đề xuất các dịch vụ logic mà cần thiết để điều khiển địa chỉ đối với điểm đích.

AP đề cập đến thực thể mà cho phép các STA được liên kết để truy cập DS qua WM và có chức năng STA. Dữ liệu có thể di chuyển giữa BSS và DS qua AP. Ví dụ, STA2 và STA3 được thể hiện trên Fig.2 có chức năng STA và có chức năng tạo ra các STA được liên kết (STA1 và STA4) để truy cập DS. Ngoài ra, bởi vì tất cả các AP về cơ bản tương ứng với các STA, tất cả các AP là các thực thể có địa chỉ. Địa chỉ được sử dụng bởi AP để truyền thông trên WM không cần luôn luôn giống với địa chỉ được sử dụng bởi AP để truyền thông trên DSM.

Dữ liệu được truyền từ một trong số các STA được liên kết với AP đến địa chỉ STA của AP này có thể luôn được thu bởi cổng chưa được điều khiển và có thể được xử lý bởi thực thể truy cập cổng IEEE 802.1X. Nếu cổng được điều khiển được xác thực, dữ liệu (hoặc khung) truyền có thể được truyền đến DS.

Fig.3 là sơ đồ thể hiện cấu trúc được lấy làm ví dụ khác của hệ thống IEEE 802.11 mà sáng chế ứng dụng vào. Ngoài cấu trúc của Fig.2, Fig.3 thể hiện về mặt khái niệm tập dịch vụ mở rộng (ESS) để cung cấp sự phủ sóng rộng.

Mạng không dây có kích cỡ và tính phức tạp tùy ý có thể bao gồm DS và các BSS. Trong hệ thống IEEE 802.11, kiểu mạng như vậy được đề cập là mạng ESS. ESS này có thể tương ứng với tập hợp các BSS được kết nối với một DS. Tuy nhiên, ESS này không bao gồm DS. Mạng ESS khác biệt ở chỗ mạng ESS xuất hiện như mạng IBSS trong lớp điều khiển kết nối logic (LLC). Các STA

được bao gồm trong ESS có thể truyền thông với nhau và các STA di động có thể di chuyển trong suốt trong LLC từ một BSS đến BSS khác (trong cùng ESS).

Trong IEEE 802.11, các vị trí vật lý tương đối của các BSS trên Fig.3 không được giả định và tất cả các dạng sau đây là có thể. Các BSS có thể chồng lên một phần và dạng này thông thường được sử dụng để cung cấp sự phủ sóng liên tục. Các BSS có thể không được kết nối về mặt vật lý và các khoảng cách logic giữa các BSS không bị giới hạn. Các BSS có thể được đặt ở cùng vị trí vật lý và dạng này có thể được sử dụng để tạo ra sự dư thừa. Một hoặc nhiều các IBSS hoặc các mạng ESS có thể về mặt vật lý được đặt trong cùng một khoảng không như là một hoặc nhiều các mạng ESS. Điều này có thể tương ứng với mạng dạng mạng ESS trong trường hợp trong đó mạng ad-hoc hoạt động trong khu vực trong đó mạng ESS có mặt, trường hợp trong đó các mạng IEEE 802.11 của các tổ chức khác nhau chồng lên nhau về mặt vật lý, hoặc trường hợp trong đó hai hoặc nhiều chính sách bảo mật và truy cập khác nhau là cần thiết trong cùng một khu vực.

Fig.4 là sơ đồ thể hiện cấu trúc được lấy làm ví dụ của hệ thống WLAN. Trên Fig.4, ví dụ về hạ tầng cơ sở BSS bao gồm DS được thể hiện.

Trong ví dụ của Fig.4, BSS1 và BSS2 cấu thành ESS. Trong hệ thống WLAN, STA là thiết bị hoạt động theo quy định MAC/PHY của IEEE 802.11. Các STA bao gồm các STA AP và các STA không phải AP. Các STA không phải AP tương ứng với các thiết bị, chẳng hạn các máy tính xách tay hoặc các điện thoại di động, được điều khiển trực tiếp bởi những người sử dụng. Trên Fig.4, STA1, STA3, và STA4 tương ứng với các STA không phải AP và STA2 và STA5 tương ứng với các STA AP.

Trong phần mô tả sau đây, STA không phải AP có thể được gọi là thiết bị đầu cuối, bộ truyền/thu Không dây (WTRU), Thiết bị người sử dụng (UE), trạm

di động (MS), thiết bị đầu cuối di động, hoặc trạm thuê bao di động (MSS). AP là khái niệm tương ứng với trạm gốc (BS), nút B (Node-B), nút B cải tiến (e-NB), hệ thống thu truyền gốc (BTS), hoặc BS cỡ siêu nhỏ trong các trường truyền thông không dây khác.

Cấu trúc lớp

Các hoạt động của AP và/hoặc STA để sử dụng trong hệ thống WLAN sẽ được mô tả dưới đây xét theo cấu trúc lớp. Cấu trúc lớp này có thể được thực hiện bởi bộ xử lý xét theo cấu trúc thiết bị. AP hoặc STA có thể bao gồm nhiều cấu trúc lớp. Ví dụ, cấu trúc lớp được mô tả trong các tài liệu 802.11 chủ yếu bao gồm lớp con MAC và lớp PHY trên lớp kết nối dữ liệu (Data link layer - DLL). Lớp PHY này có thể bao gồm thực thể thủ tục hội tụ lớp vật lý (Physical layer convergence procedure - PLDP), thực thể phụ thuộc môi trường vật lý (Physical medium dependent - PMD), v.v... Lớp con MAC và lớp PHY về mặt khái niệm có thể bao gồm một thực thể quản lý được gọi là thực thể quản lý lớp con MAC (MLME) và thực thể quản lý khác được gọi là thực thể quản lý lớp vật lý (PLME). Các thực thể trên có thể cung cấp bề mặt hỗ trợ quản lý lớp để thực hiện chức năng quản lý lớp.

Để cung cấp hoạt động MAC chính xác, thực thể quản lý trạm (SME) có mặt trong mỗi AP hoặc mỗi STA. SME này có thể là thực thể độc lập lớp mà có thể được quan sát là lưu trữ trong mặt phẳng quản lý riêng rẽ hoặc là lưu trữ “qua một bên”. Để tạo ra hoạt động MAC chính xác, SME (Station management entity - Thực thể quản lý trạm; 1430) có mặt trong mỗi STA. SME (1430) này là thực thể độc lập lớp mà có thể được quan sát là lưu trữ trong mặt phẳng quản lý riêng rẽ hoặc là lưu trữ “qua một bên.” Các chức năng chính xác của SME này không được cụ thể hóa trong tài liệu này, nhưng nói chung thực thể này có thể được quan sát là chịu trách nhiệm về các chức năng như tập hợp trạng thái phụ thuộc

lớp từ nhiều thực thể quản lý lớp khác nhau (LME), và thiết lập một cách tương tự giá trị của các tham số cụ thể lớp. SME sẽ thực hiện một cách điển hình các chức năng như vậy thay mặt các thực thể quản lý hệ thống chung và sẽ thực hiện các giao thức quản lý tiêu chuẩn.

Các thực thể được đề cập ở trên tương tác với nhau theo nhiều cách khác nhau. Ví dụ, các từ gốc GET/SET được trao đổi giữa các thực thể này, sao cho các thực thể này tương tác với nhau. Từ gốc XX-GET.request được sử dụng để yêu cầu giá trị MIBattribute đã cho (thuộc tính cơ sở thông tin quản lý). Từ gốc XX-GET.confirm được sử dụng để quay lại giá trị thuộc tính MIB phù hợp nếu trạng thái = “thành công,” nếu không quay lại chỉ báo lỗi trong trường trạng thái. Từ gốc XX-SET.request được sử dụng để yêu cầu rằng thuộc tính MIB được chỉ báo được thiết lập đến giá trị cho trước. Nếu thuộc tính MIB này ngụ ý thao tác riêng, sau đó nó yêu cầu rằng thao tác này được thực hiện. Và, từ gốc XX-SET.confirm được sử dụng sao cho, nếu trạng thái = “thành công,” nó khẳng định rằng thuộc tính MIB được chỉ báo được thiết lập đến giá trị được yêu cầu, nếu không thì nó quay lại điều kiện lỗi trong trường trạng thái. Nếu thuộc tính MIB này ngụ ý thao tác riêng, sau đó nó khẳng định rằng thao tác này được thực hiện.

Ngoài ra, các từ gốc MLME_GET/SET khác nhau có thể được trao đổi giữa MLME và SME qua MLME_SAP (Điểm truy cập dịch vụ). Các từ gốc PLME_GET/SET khác nhau có thể được trao đổi giữa PLME và SME qua PLME_SAP, và có thể được trao đổi giữa MLME và PLME qua MLME-PLME_SAP.

Quy trình cài đặt kết nối

Fig.5 là giản đồ giải thích quy trình cài đặt kết nối chung theo phương án được lấy làm ví dụ của sáng chế.

Để cho phép STA thiết lập cài đặt kết nối trên mạng cũng như truyền/thu dữ liệu qua mạng, STA này phải thực hiện cài đặt kết nối như thế qua các quy trình phát hiện mạng, xác thực, và liên kết, và phải thiết lập liên kết và thực hiện xác thực bảo mật. Quy trình cài đặt kết nối này cũng có thể được gọi là quy trình bắt đầu truy cập hoặc quy trình cài đặt truy cập. Ngoài ra, bước liên kết là thuật ngữ chung để phát hiện, xác thực, liên kết, và các bước cài đặt bảo mật của quy trình cài đặt kết nối.

Quy trình cài đặt kết nối được mô tả dựa vào Fig. 5.

Trong bước S510, STA có thể thực hiện thao tác phát hiện mạng. Thao tác phát hiện mạng này có thể bao gồm thao tác quét STA. Tức là, STA phải tìm kiếm mạng hiện có để truy cập mạng. STA phải nhận dạng mạng tương thích trước khi tham gia mạng không dây. Ở đây, quy trình để nhận dạng mạng được chứa trong vùng riêng được gọi là quy trình quét.

Phương án quét được chia thành quét chủ động và quét thụ động.

Fig.5 là giản đồ minh họa thao tác phát hiện mạng bao gồm quy trình quét chủ động. Trong trường hợp quét chủ động, STA được cấu hình để thực hiện quét sẽ truyền khung yêu cầu thăm dò và đợi phản hồi lại khung yêu cầu thăm dò, sao cho STA có thể di chuyển giữa các kênh và có thể xác định cùng lúc AP (điểm truy cập) nào có mặt trong vùng ngoại vi. Bộ phản hồi truyền khung phản hồi thăm dò, đóng vai trò là thông tin phản hồi lại khung yêu cầu thăm dò, đến STA đã truyền khung yêu cầu thăm dò. Trong trường hợp này, bộ phản hồi có thể là STA mà cuối cùng đã truyền khung báo hiệu trong BSS của kênh được quét. Trong BSS, bởi vì AP truyền khung báo hiệu, AP này hoạt động như bộ phản hồi. Trong IBSS, bởi vì các STA của IBSS liên tiếp truyền khung báo hiệu, bộ phản hồi là không cố định. Ví dụ, STA này, mà truyền khung yêu cầu thăm dò ở kênh #1 và thu khung phản hồi thăm dò ở kênh #1, lưu trữ thông tin liên kết BSS được

chứa trong khung phản hồi thăm dò đã được thu, và di chuyển đến kênh kế tiếp (ví dụ, kênh #2), sao cho STA này có thể thực hiện quét bằng cách sử dụng cùng phương pháp (tức là, truyền/thu yêu cầu/phản hồi thăm dò ở kênh #2).

Mặc dù không được thể hiện trên Fig.5, thao tác quét cũng có thể được thực hiện nhờ sử dụng quét thụ động. STA được cấu hình để thực hiện quét trong chế độ quét thụ động đợi khung báo hiệu khi đồng thời di chuyển từ một kênh đến kênh khác. Khung báo hiệu là một trong những khung quản lý trong IEEE 802.11, chỉ báo sự có mặt của mạng không dây, cho phép STA thực hiện quét để tìm kiếm mạng không dây, và được truyền một cách định kì theo cách mà STA có thể tham gia vào mạng không dây. Trong BSS, AP được cấu hình để truyền một cách định kì khung báo hiệu. Trong IBSS, các STA của IBSS được cấu hình để truyền liên tiếp khung báo hiệu. Nếu mỗi STA để quét thu khung báo hiệu, STA này lưu trữ thông tin BSS được chứa trong khung báo hiệu này, và di chuyển đến kênh khác và ghi thông tin khung báo hiệu ở mỗi kênh. STA thu khung báo hiệu lưu trữ thông tin liên kết BSS được chứa trong khung báo hiệu được thu, di chuyển đến kênh kế tiếp, và do đó thực hiện quét bằng cách sử dụng cùng phương pháp.

So sánh giữa quét chủ động và quét thụ động, quét chủ động có nhiều ưu điểm hơn quét thụ động xét về độ trễ và điện năng tiêu thụ.

Sau khi STA phát hiện mạng, STA này có thể thực hiện quy trình xác thực trong bước S520. Quy trình xác thực này có thể được gọi là quy trình xác thực thứ nhất theo cách mà quy trình xác thực có thể được phân biệt rõ ràng với quy trình cài đặt bảo mật ở bước S540.

Quy trình xác thực có thể bao gồm truyền khung yêu cầu xác thực đến AP bởi STA, và truyền khung phản hồi xác thực đến STA bởi AP phản hồi lại khung

yêu cầu xác thực. Khung xác thực được sử dụng cho yêu cầu/phản hồi xác thực có thể tương ứng với khung quản lý.

Khung xác thực có thể bao gồm số thuật toán xác thực, số trình tự giao dịch xác thực, mã trạng thái, chuỗi kí tự mời kết nối, mạng bảo mật mạnh (RSN), nhóm tuần hoàn hữu hạn (FCG), v.v... Thông tin được đề cập ở trên được chứa trong khung xác thực có thể tương ứng với một số phần thông tin có khả năng được chứa trong khung yêu cầu/phản hồi xác thực, có thể được thay thế bằng thông tin khác, hoặc có thể bao gồm thông tin bổ sung.

STA có thể truyền khung yêu cầu xác thực tới AP. AP này có thể quyết định có xác thực STA tương ứng hay không trên cơ sở thông tin được chứa trong khung yêu cầu xác thực được thu. AP này có thể đưa ra kết quả xác thực đối với STA qua khung phản hồi xác thực.

Sau khi STA này được xác thực thành công, quy trình liên kết này có thể được thực hiện trong bước S530. Quy trình liên kết này có thể bao gồm truyền khung yêu cầu liên kết đến AP bởi STA, và truyền khung phản hồi liên kết đến STA bởi AP phản hồi lại khung yêu cầu liên kết.

Ví dụ, khung yêu cầu liên kết có thể bao gồm thông tin được liên kết với các dung lượng khác nhau, khoảng nghe báo hiệu, bộ nhận dạng tập dịch vụ (SSID), các tốc độ chuyển dữ liệu được hỗ trợ, các kênh được hỗ trợ, RSN, miền di động, các loại hoạt động được hỗ trợ, yêu cầu phát rộng TIM (Traffic indication map - bản đồ chỉ báo lưu lượng), dung lượng dịch vụ liên kết mạng, v.v...

Ví dụ, khung phản hồi liên kết có thể bao gồm thông tin được liên kết với các dung lượng khác nhau, mã trạng thái, ID liên kết (AID), các tốc độ chuyển dữ liệu được hỗ trợ, tập tham số truy cập kênh được phân bổ tăng cường (Enhanced distributed channel access - EDCA), bộ chỉ báo nguồn điện kênh được

thu (Receive channel power indicator - RCPI), bộ chỉ báo tín hiệu trên nhiễu được thu (Receive signal to noise indicator - RSNI), miền di động, khoảng thời gian chờ (thời gian quay trở lại liên kết), tham số quét BSS chồng, phản hồi phát rộng TIM, bản đồ QoS, v.v...

Thông tin được đề cập ở trên có thể tương ứng với một số các phần của thông tin có khả năng được chứa trong khung yêu cầu/phản hồi liên kết, có thể được thay thế bằng thông tin khác, hoặc có thể bao gồm thông tin bổ sung.

Sau khi STA được liên kết thành công với mạng, quy trình cài đặt bảo mật có thể được thực hiện trong bước S540. Quy trình cài đặt bảo mật của bước S540 này có thể được gọi là quy trình xác thực dựa trên yêu cầu/phản hồi liên kết mạng bảo mật mạnh (RSNA). Quy trình xác thực của bước S520 này có thể được gọi là quy trình xác thực thứ nhất, và quy trình cài đặt bảo mật của bước S540 cũng có thể được gọi đơn giản là quy trình xác thực.

Ví dụ, quy trình cài đặt bảo mật của bước S540 có thể bao gồm quy trình cài đặt khóa riêng tư qua bắt tay 4 đường dựa trên khung giao thức xác thực mở rộng qua LAN (Extensible authentication protocol over LAN - EAPOL). Ngoài ra, quy trình cài đặt bảo mật này cũng có thể được thực hiện theo các lược đồ bảo mật khác mà không được xác định trong các tiêu chuẩn IEEE 802.11.

Phát triển WLAN

Để tránh những giới hạn trong tốc độ truyền thông WLAN, IEEE 802.11n gần đây đã được thiết lập như là tiêu chuẩn truyền thông. IEEE 802.11n nhằm mục đích tăng tốc độ mạng và độ ổn định cũng như mở rộng vùng phủ sóng của mạng không dây. Cụ thể hơn, IEEE 802.11n hỗ trợ thông lượng cao (HT) tối đa là 540Mbps, và được dựa trên công nghệ MIMO trong đó nhiều nhiều anten được lắp vào mỗi bộ truyền và bộ thu.

Để tránh giới những giới hạn trong tốc độ truyền thông WLAN, IEEE 802.11n gần đây đã được thiết lập như là tiêu chuẩn truyền thông. IEEE 802.11n nhằm mục đích tăng tốc độ mạng và độ ổn định cũng như mở rộng vùng phủ sóng của mạng không dây. Chi tiết hơn, IEEE 802.11n hỗ trợ thông lượng cao (HT) tối đa ở 540Mbps, và được dựa trên công nghệ MIMO trong đó nhiều anten được lắp vào mỗi bộ truyền và bộ thu.

Để sử dụng một cách hiệu quả kênh tần số radio (RF), hệ thống WLAN thể hệ tiếp theo hỗ trợ sự truyền MU-MIMO (Multi user multi input multi output - đa người sử dụng đa đầu ra đa đầu vào) trong đó nhiều STA có thể đồng thời truy cập kênh. Theo lược đồ truyền MU-MIMO, AP có thể đồng thời truyền các gói đến ít nhất một STA được ghép cặp MIMO.

Ngoài ra, công nghệ để hỗ trợ các hoạt động hệ thống WLAN trong khoảng trắng đã được bàn luận gần đây. Ví dụ, công nghệ để đưa hệ thống WLAN trong khoảng trắng (TV WS) chẳng hạn dải tần số không tác dụng (ví dụ, dải 54~698MHz) còn lại do chuyển tiếp đến TV kỹ thuật số đã được bàn luận theo tiêu chuẩn IEEE 802.11af. Tuy nhiên, thông tin được đề cập ở trên được bộc lộ chỉ nhằm các mục đích minh họa, và khoảng trắng có thể là dải được cấp phép có khả năng chỉ được sử dụng chủ yếu bởi người sử dụng được cấp phép. Người sử dụng được cấp phép có thể là người sử dụng mà có quyền sử dụng dải được cấp phép này, và cũng có thể được gọi là thiết bị được cấp phép, người sử dụng chính, người sử dụng truyền thống, hoặc tương tự.

Ví dụ, AP và/hoặc STA hoạt động trong khoảng trắng (WS) phải cung cấp chức năng để bảo vệ người sử dụng được cấp phép. Ví dụ, giả định rằng người sử dụng được cấp phép chẳng hạn như máy vi âm đã sử dụng kênh WS cụ thể đóng vai trò là dải tần số được phân chia theo quy định theo cách mà băng thông cụ thể được chiếm giữ từ dải WS, AP và/hoặc STA không thể sử dụng dải tần số

này tương ứng với kênh WS tương ứng để bảo vệ người sử dụng được cấp phép. Ngoài ra, AP và/hoặc STA phải ngừng sử dụng dải tần số tương ứng trong điều kiện là người sử dụng được cấp phép sử dụng dải tần số được sử dụng để truyền và/hoặc thu khung hiện thời.

Vì vậy, AP và/hoặc STA phải xác định có sử dụng dải tần số cụ thể của dải WS hay không. Nói cách khác, AP và/hoặc STA phải xác định sự có hay không có của người sử dụng truyền thông hoặc người sử dụng được cấp phép trong dải tần số. Lược đồ để xác định sự có hay không có người sử dụng truyền thông trong dải tần số cụ thể được gọi là lược đồ cảm biến phổ. Lược đồ phát hiện năng lượng, lược đồ phát hiện kí hiệu và tương tự có thể được sử dụng làm cơ chế cảm biến phổ. AP và/hoặc STA có thể xác định rằng dải tần số đang được sử dụng bởi người sử dụng truyền thông nếu cường độ của tín hiệu được thu vượt quá giá trị định trước, hoặc khi phân đầu DTV được phát hiện.

Công nghệ truyền thông M2M (Máy tới máy) được thảo luận như là công nghệ truyền thông thế hệ tiếp theo. Tiêu chuẩn kỹ thuật để hỗ trợ truyền thông M2M được phát triển là IEEE 802.11ah trong hệ thống WLAN IEEE 802.11. Truyền thông M2M đề cập đến lược đồ truyền thông bao gồm một hoặc nhiều máy, hoặc cũng có thể được gọi là truyền thông dạng máy (MTC) hoặc truyền thông máy tới máy (M2M). Trong trường hợp này, máy có thể là thực thể mà không yêu cầu điều khiển và can thiệp trực tiếp của người sử dụng. Ví dụ, không chỉ máy đo hoặc máy bán hàng tự động bao gồm môđun RF, mà còn thiết bị người sử dụng (UE) (chẳng hạn điện thoại thông minh) có khả năng thực hiện truyền thông bằng cách truy cập mạng tự động mà không cần người sử dụng can thiệp/điều khiển có thể là ví dụ về các máy như vậy. Truyền thông M2M có thể bao gồm truyền thông thiết bị-đến-thiết bị (D2D) và truyền thông giữa thiết bị và máy chủ ứng dụng, v.v... Truyền thông giữa máy bán hàng tự động và máy chủ

ứng dụng, truyền thông giữa thiết bị chấp nhận thẻ thanh toán (POS) và máy chủ ứng dụng, và truyền thông giữa đồng hồ điện, đồng hồ ga hoặc đồng hồ nước và máy chủ ứng dụng là ví dụ truyền thông giữa thiết bị và máy chủ ứng dụng được lấy làm ví dụ. Các ứng dụng truyền thông dựa trên M2M có thể bao gồm bảo mật, vận tải, chăm sóc sức khỏe, v.v... Trong trường hợp xem xét các ví dụ ứng dụng được đề cập ở trên, truyền thông M2M phải hỗ trợ phương pháp để đôi lúc truyền/thu lượng nhỏ dữ liệu ở tốc độ thấp trong môi trường bao gồm số lượng lớn các thiết bị.

Cụ thể hơn, truyền thông M2M phải hỗ trợ lượng lớn các STA. Mặc dù hệ thống WLAN hiện thời giả định rằng một AP được liên kết với tối đa 2007 STA, các phương pháp khác để hỗ trợ các trường hợp khác trong đó nhiều hơn các STA (chẳng hạn, khoảng 6000 STA) được liên kết với một AP được thảo luận gần đây trong truyền thông M2M. Ngoài ra, mong muốn rằng nhiều ứng dụng để hỗ trợ/yêu cầu tốc độ truyền thấp có mặt trong truyền thông M2M. Để dễ dàng hỗ trợ nhiều STA, hệ thống WLAN có thể nhận biết có hay không dữ liệu được truyền đến STA trên cơ sở TIM (bản đồ chỉ báo lưu lượng), và các phương pháp khác để giảm kích cỡ sơ đồ bit của TIM được thảo luận gần đây. Ngoài ra, mong muốn rằng lưu lượng lớn dữ liệu có khoảng truyền/thu rất dài có mặt trong truyền thông M2M. Ví dụ, trong truyền thông M2M, lượng rất nhỏ dữ liệu (chẳng hạn, đo điện/ga/nước) cần được truyền trong các khoảng thời gian dài (ví dụ, từng tháng). Do đó, mặc dù số lượng STA liên kết với một AP tăng lên trong hệ thống WLAN, nhiều nhà phát triển và các công ty đang thực hiện nghiên cứu kỹ lưỡng hệ thống WLAN mà có thể hỗ trợ một cách hiệu quả trường hợp trong đó có số lượng rất nhỏ các STA, mỗi STA có khung dữ liệu được thu từ AP trong một chu kỳ báo hiệu.

Như được mô tả ở trên, công nghệ WLAN đang phát triển nhanh chóng, và không những các công nghệ được lấy làm ví dụ được đề cập ở trên mà còn các công nghệ khác chẳng hạn cài đặt kết nối trực tiếp, cải thiện thông lượng tạo luồng phương tiện, tốc độ cao và/hoặc hỗ trợ cài đặt phiên bản đầu quy mô lớn, và hỗ trợ băng thông mở rộng và tần số hoạt động, được phát triển mạnh mẽ.

Quản lý nguồn điện

Như được mô tả ở trên, hệ thống WLAN cần thực hiện cảm biến kênh trước khi STA thực hiện truyền/thu dữ liệu. Hoạt động luôn cảm biến kênh này gây ra sự tiêu thụ điện ổn định của STA. Không có quá nhiều khác biệt trong việc tiêu thụ điện giữa trạng thái thu (Rx) và trạng thái truyền (Tx). Việc duy trì liên tục trạng thái Rx có thể gây ra tải lớn cho STA bị giới hạn nguồn điện (tức là, STA được hoạt động bởi pin). Do đó, nếu STA duy trì chế độ chờ Rx để cảm biến kênh một cách ổn định, nguồn điện được tiêu thụ không hiệu quả, mà không có những ưu điểm vượt trội về thông lượng WLAN. Để giải quyết vấn đề nêu trên, hệ thống WLAN hỗ trợ chế độ quản lý nguồn điện (PM) của STA.

Chế độ PM của STA được chia thành chế độ hoạt động và chế độ tiết kiệm điện (PS). STA về cơ bản được hoạt động trong chế độ hoạt động. STA hoạt động trong chế độ hoạt động duy trì trạng thái hoạt động. Nếu STA ở trong trạng thái hoạt động, STA có thể hoạt động bình thường sao cho nó có thể thực hiện truyền/thu khung, quét kênh, hoặc tương tự. Mặt khác, STA hoạt động trong chế độ PS được cấu hình để chuyển từ trạng thái chờ có hẹn giờ sang trạng thái hoạt động hoặc ngược lại. STA hoạt động trong trạng thái chờ được hoạt động với nguồn điện tối thiểu, và STA không thực hiện truyền/thu khung và quét kênh.

Lượng tiêu thụ điện được giảm theo tỷ lệ với thời gian cụ thể trong đó STA ở trong trạng thái chờ, sao cho thời gian hoạt động STA được tăng lên tương ứng với việc tiêu thụ điện bị giảm đi. Tuy nhiên, không thể truyền hoặc thu

khung trong trạng thái chờ, sao cho STA không thể hoạt động bắt buộc trong khoảng thời gian dài. Nếu có khung được truyền đến AP, STA hoạt động trong trạng thái chờ được chuyển sang trạng thái hoạt động, sao cho nó có thể truyền/thu khung trong trạng thái hoạt động. Mặt khác, nếu AP có khung được truyền đến STA, STA ở trạng thái chờ không thể thu khung và không thể nhận biết sự có mặt của khung được thu. Do đó, STA có thể cần chuyển sang trạng thái hoạt động theo chu kỳ riêng để nhận biết có hay không khung được truyền đến STA (hoặc để thu tín hiệu chỉ báo sự có mặt của khung dựa trên giả định rằng sự có mặt của khung được truyền đến STA được quyết định).

Fig.6 là sơ đồ khái niệm minh họa hoạt động quản lý nguồn điện (PM).

Liên quan đến Fig.6, AP 210 truyền khung báo hiệu đến các STA có mặt trong BSS ở các khoảng của chu kỳ thời gian định trước trong các bước (S211, S212, S213, S214, S215 và S216). Khung báo hiệu này bao gồm phần tử thông tin TIM. Phần tử thông tin TIM này bao gồm lưu lượng được đếm liên quan đến với các STA được liên kết với AP 210, và bao gồm thông tin riêng chỉ báo rằng khung phải được truyền. Phần tử thông tin TIM này bao gồm TIM để chỉ báo khung đơn hướng và bản đồ chỉ báo lưu lượng vận chuyển (DTIM) để chỉ báo khung đa hướng hoặc khung phát rộng.

AP 210 có thể truyền DTIM một lần bất cứ khi nào khung báo hiệu được truyền ba lần. Mỗi STA1 220 và STA2 222 được hoạt động trong chế độ PS. Mỗi STA1 220 và STA2 222 được chuyển từ trạng thái chờ sang trạng thái hoạt động mỗi khoảng thời gian hoạt động, sao cho STA1 220 và STA2 222 có thể được cấu hình để thu phần tử thông tin TIM được truyền bởi AP 210. Mỗi STA có thể tính toán thời gian bắt đầu chuyển tại đó mỗi STA có thể bắt đầu chuyển sang trạng thái hoạt động trên cơ sở đồng hồ cục bộ của nó. Trên Fig.6, được giả định rằng đồng hồ của STA là giống với đồng hồ của AP.

Ví dụ, khoảng thời gian hoạt động được định trước có thể được cấu hình theo cách mà STA1 220 có thể chuyển sang trạng thái hoạt động để thu phần tử TIM mỗi khoảng báo hiệu. Do đó, STA1 220 có thể chuyển sang trạng thái hoạt động trong bước S221 khi AP 210 truyền lần đầu khung báo hiệu trong bước S211. STA1 220 thu khung báo hiệu, và thu được phần tử thông tin TIM. Nếu phần tử TIM đã thu được này chỉ báo sự có mặt của khung được truyền đến STA1 220, STA1 220 có thể truyền khung thăm dò tiết kiệm điện (hỏi vòng PS), mà yêu cầu AP 210 truyền khung, đến AP 210 trong bước S221a. AP 210 này có thể truyền khung đến STA 1 220 phản hồi lại khung hỏi vòng PS trong bước S231. STA1 220 đã thu khung được chuyển lại sang trạng thái chờ, và hoạt động trong trạng thái chờ.

Khi AP 210 truyền khung báo hiệu lần thứ hai, trạng thái môi trường bận trong đó môi trường này được truy cập bởi thiết bị khác thu được, AP 210 có thể không truyền khung báo hiệu ở khoảng báo hiệu chính xác và có thể truyền khung báo hiệu ở thời gian trễ trong bước S212. Trong trường hợp này, mặc dù STA1 220 được chuyển sang trạng thái hoạt động phản hồi lại khoảng báo hiệu, nó không thu được khung báo hiệu được truyền trễ sao cho nó vào lại trạng thái chờ trong bước S222.

Khi AP 210 truyền khung báo hiệu lần thứ ba, khung báo hiệu tương ứng có thể bao gồm phần tử TIM được biểu thị bởi DTIM. Tuy nhiên, bởi vì trạng thái môi trường bận được đưa ra, AP 210 truyền khung báo hiệu ở thời gian trễ trong bước S213. STA1 220 được chuyển sang trạng thái hoạt động phản hồi lại khoảng báo hiệu, và có thể thu DTIM qua khung báo hiệu được truyền bởi AP 210. Giả định rằng DTIM được thu bởi STA1 220 không có khung được truyền đến STA1 220 và có khung cho STA khác. Trong trường hợp này, STA1 220 xác nhận sự vắng mặt của khung để được thu trong STA1 220, và vào lại trạng thái

chờ, sao cho STA1 220 này có thể hoạt động trong trạng thái chờ. Sau đó AP 210 truyền khung báo hiệu, AP 210 truyền khung đến STA tương ứng trong bước S232.

AP 210 truyền khung báo hiệu lần thứ tư trong bước S214. Tuy nhiên, STA1 220 không thể thu được thông tin liên quan đến sự có mặt của lưu lượng được đệm được liên kết với STA1 220 qua việc thu hai lần phần tử TIM, sao cho STA1 220 này có thể điều chỉnh khoảng thời gian hoạt động để thu phần tử TIM này. Theo cách khác, với điều kiện là thông tin báo hiệu để phối hợp với giá trị khoảng thời gian hoạt động của STA1 220 được chứa trong khung báo hiệu được truyền bởi AP 210, giá trị khoảng thời gian hoạt động của STA1 220 này có thể được điều chỉnh. Trong ví dụ này, STA1 220, mà được chuyển để thu phần tử TIM mỗi khoảng báo hiệu, có thể được chuyển sang trạng thái hoạt động khác trong đó STA1 220 có thể hoạt động từ trạng thái chờ một lần với mỗi ba khoảng thời gian báo hiệu. Do đó, khi AP 210 truyền khung báo hiệu lần thứ tư trong bước S214 và truyền khung báo hiệu lần thứ năm trong bước S215, STA1 220 duy trì trạng thái chờ sao cho nó không thể thu phần tử TIM tương ứng.

Khi AP 210 truyền lần thứ sáu khung báo hiệu trong bước S216, STA1 220 được chuyển sang trạng thái hoạt động và hoạt động trong trạng thái hoạt động, sao cho STA1 220 không thể thu được phần tử TIM được chứa trong khung báo hiệu trong bước S224. Phần tử TIM này là DTIM chỉ báo sự có mặt của khung phát rộng, sao cho STA1 220 không truyền khung hỏi vòng PS đến AP 210 và có thể thu khung phát rộng được truyền bởi AP 210 trong bước S234. Trong khi đó, khoảng thời gian hoạt động của STA2 230 có thể dài hơn khoảng thời gian hoạt động của STA1 220. Do đó, STA2 230 vào trạng thái hoạt động ở thời gian riêng S215 nơi AP 210 truyền khung báo hiệu lần thứ năm, sao cho STA2 230 có thể thu phần tử TIM trong bước S241. STA2 230 nhận biết sự có

mặt của khung được truyền đến STA2 230 qua phần tử TIM, và truyền khung hỏi vòng PS đến AP 210 để yêu cầu truyền khung trong bước S241a. AP 210 có thể truyền khung đến STA2 230 phản hồi lại khung hỏi vòng PS trong bước S233.

Để hoạt động/quản lý chế độ tiết kiệm điện (PS) được thể hiện trên Fig.6, phần tử TIM hoặc có thể bao gồm TIM chỉ báo sự có hay không có khung được truyền đến STA, hoặc bao gồm DTIM chỉ báo sự có hay không có khung phát rộng/đa hướng. DTIM có thể được thực hiện qua trường thiết lập phần tử TIM.

Quy trình truy vấn liên kết bảo mật (SA)

Như có thể thấy từ Fig.5, STA có thể truyền khung yêu cầu liên kết đến AP, và AP này có thể truyền khung phản hồi liên kết đến STA phản hồi lại khung yêu cầu liên kết. Khung yêu cầu liên kết và khung phản hồi liên kết này có thể thuộc về khung quản lý. Khung yêu cầu liên kết này có thể bao gồm dung lượng STA, SSID, v.v... Khung phản hồi liên kết này có thể bao gồm dung lượng AP, v.v... Cụ thể, khung phản hồi liên kết này có thể bao gồm thêm ID liên kết (AID) được cấp đến liên kết yêu cầu STA.

Bảng 1 thể hiện định dạng được lấy làm ví dụ của thân khung yêu cầu liên kết.

Bảng 1

Thứ tự	Thông tin (độ dài trong 8 bit)	Các ghi chú
1	Dung lượng (2)	
2	Khoảng nghe (2)	
3	SSID (2)	
4	Các tốc độ chuyển dữ liệu được hỗ trợ (3-10)	
5	Các tốc độ hỗ	Phần tử các tốc độ hỗ được hỗ trợ mở rộng là có mặt

	được hỗ trợ mở rộng (3-257)	nếu có hơn tám tốc độ chuyển dữ liệu được hỗ trợ, và nói cách khác là tùy chọn.
6	Dung lượng công suất (4-257)	Phần tử dung lượng công suất là có mặt nếu dot11SpectrumManagementRequired là đúng hoặc dot11RadioMeasurementActivated là đúng.
7	Các kênh được hỗ trợ (4-256)	Phần tử các kênh được hỗ trợ là có mặt nếu dot11SpectrumManagementRequired và dot11ExtendedChannelSwitchActivated là sai.
8	RSN (36-256)	Phần tử RSN là có mặt nếu dot11RSNAActivated thiết lập là đúng.
9	Dung lượng QoS (3)	Phần tử dung lượng QoS là có mặt nếu dot11QosOption-Implemented là đúng.
10	Các dung lượng cho phép RM (7)	Phần tử các dung lượng cho phép RM là có mặt nếu dot11RadioMeasurementActivated là đúng.
11	Miền di động (5)	MDE có mặt trong khung yêu cầu liên kết nếu dot11FastBSSTransitionActivated là đúng và nếu khung này được chuyển đến AP mà được quảng cáo dung lượng FT của nó trong MDE trong khung báo hiệu của nó hoặc khung phản hồi thăm dò của nó (tức là, AP cũng có dot11FastBSSTransitionActivated thiết lập là đúng).
12	Các hạng hoạt động được hỗ trợ (4-255)	Phần tử các hạng hoạt động được hỗ trợ là có mặt nếu dot11ExtendedChannelSwitchActivated là đúng.
13	Các dung lượng HT (28)	Phần tử các dung lượng HT là có mặt khi thuộc tính dot11HighThroughputOptionImplemented là đúng.
14	20/40 cùng tồn tại BSS (3)	Phần tử 20/40 cùng tồn tại BSS là có mặt một cách tùy chọn khi thuộc tính dot112040BSSCoexistenceManagementSupport tính là đúng.
15	Các dung lượng được mở rộng	Phần tử các dung lượng được mở rộng là có mặt một cách tùy chọn nếu bất kỳ trường nào trong phần tử này là khác không.
Cuối cùng	Đặc trưng của nhà cung cấp (3-257)	Một hoặc nhiều các phần tử đặc trưng của nhà cung cấp là có mặt một cách tùy chọn. Các phần tử này theo sau tất cả các phần tử khác.

Bảng 2 thể hiện định dạng được lấy làm ví dụ của thân khung phản hồi liên kết.

Bảng 2

Thứ tự	Thông tin	Các ghi chú
1	Dung lượng	
2	Mã trạng thái	
3	AID	
4	Các tốc độ chuyển dữ liệu được hỗ trợ	
5	Các tốc độ chuyển dữ liệu được hỗ trợ mở rộng	Phần tử các tốc độ chuyển dữ liệu được hỗ trợ mở rộng là có mặt nếu có hơn tám các tốc độ chuyển dữ liệu được hỗ trợ, và mặt khác là tùy chọn.
6	Tập tham số EDCA	
7	RCPI	Phần tử RCPI là có mặt nếu dot11RMRCPIMeasurementActivated là đúng.
8	RSNI	Phần tử RSNI là có mặt nếu dot11RMRSNIMeasurementActivated là đúng.
9	Các dung lượng được cho phép RM	Các dung lượng được cho phép RM là có mặt nếu dot11RadioMeasurementActivated là đúng.
10	Miền di động	MDE có mặt trong khung phản hồi liên kết khi dot11FastBSSTransitionActivated là đúng và khung này là phản hồi lại khung yêu cầu liên kết mà đã chứa MDE (tức là, trao đổi liên kết miền di động ban đầu FT).
11	Chuyển tiếp BSS nhanh	Phần tử chuyển tiếp BSS nhanh (FTE) có mặt trong khung phản hồi liên kết khi dot11FastBSSTransitionActivated là đúng, dot11RSNAActivated là đúng và khung này là phản hồi lại khung yêu cầu liên kết mà chứa MDE (tức là, miền di động liên kết ban đầu FT trao đổi trong RSN).
12	Vị trí được đăng ký DSE	Phần tử vị trí được đăng ký DSE là có mặt nếu dot11LCIDSERequired là đúng
13	Khoảng thời gian chờ (Thời gian quay trở lại liên kết)	Phần tử khoảng thời gian chờ chứa thời gian quay trở lại liên kết là có mặt khi dot11RSNAActivated là đúng, dot11RSNAProtectedManagementFramesActivated là đúng và yêu cầu liên kết bị từ chối với mã trạng thái 30.
14	Các dung lượng HT	Phần tử các dung lượng HT là có mặt khi thuộc tính dot11HighThroughputOptionImplemented là đúng.
15	Hoạt động HT	Phần tử hoạt động HT được bao gồm bởi AP khi thuộc tính dot11HighThroughputOptionImplemented là

		đúng.
16	20/40 Cùng tồn tại BSS	Phần tử 20/40 cùng tồn tại BSS là có mặt một cách tùy chọn khi dot112040BSSCoexistenceManagementSupport là đúng.
17	Chồng các tham số quét BSS	Phần tử chồng các tham số quét BSS là có mặt một cách tùy chọn nếu thuộc tính dot11FortyMHzOptionImplemented là đúng.
18	Các dung lượng mở rộng	Phần tử các dung lượng mở rộng là có mặt một cách tùy chọn nếu bất kỳ các trường nào trong phần tử này là khác không.
Cuối cùng	Đặc trưng của nhà cung cấp	Một hoặc nhiều các phần tử đặc trưng của nhà cung cấp là có mặt một cách tùy chọn. Các phần tử này theo sau tất cả các phần tử khác.

Phương pháp duy trì liên kết được đề xuất bởi sáng chế bao gồm phương pháp để ngăn ngừa liên kết giữa STA và AP không bị phá vỡ. Ngoài ra, khi STA không liên kết được với AP cũ và cố gắng liên kết lại với AP tương ứng, phương pháp để giảm thời gian được dùng cho quy trình liên kết này cũng được bao gồm trong phương pháp duy trì liên kết ở trên. Trong trường hợp này, chúng tôi giả định rằng trường hợp liên kết thất bại giữa STA và AP bao gồm, ví dụ, một trường hợp trong đó STA bị tắt nguồn tức thời, và trường hợp khác trong đó STA di chuyển và thoát ra khoảng dịch vụ của của AP được kết nối cũ.

STA khôi phục lại từ thất bại này có thể thực hiện lại quy trình quét, và có thể truyền khung yêu cầu liên kết đến AP được lựa chọn qua quét. Trong trường hợp này, giả định rằng AP được lựa chọn qua quét đã được liên kết với STA, là cần thiết cho AP để xác nhận STA tương ứng có đúng là người sử dụng xác thực hay không. Do đó, giả định rằng STA truyền khung yêu cầu liên kết đến AP duy trì trạng thái liên kết bảo mật (SA) liên quan đến AP tương ứng, AP này có thể thực hiện thủ tục truy vấn SA trước trước khi đưa ra tín hiệu phản hồi chỉ báo yêu cầu liên kết thành công đối với khung yêu cầu liên kết được thu mới.

Dựa trên sự thu khung yêu cầu liên kết từ STA mà ở trong trạng thái SA liên quan tới AP, thủ tục truy vấn SA có thể là quy trình cụ thể trong đó STA tương ứng ở trong trạng thái SA liên quan tới AP này.

Cụ thể hơn, dựa trên sự thu khung yêu cầu liên kết từ STA, AP truyền khung phản hồi liên kết phản hồi lại khung yêu cầu liên kết. Mã trạng thái của khung phản hồi liên kết có thể được đặt ở 30. Trường mã trạng thái '30' có thể chỉ báo rằng yêu cầu liên kết tạm thời bị từ chối và thử lại sau. Thời gian quay trở lại liên kết được phân bổ đến STA bởi trường khoảng thời gian chờ của khung phản hồi liên kết. Nếu giá trị thời gian quay trở lại liên kết được gán cho STA, STA có thể truyền lại khung yêu cầu liên kết đến AP sau khi thời gian quay trở lại liên kết trôi qua. Thời gian quay trở lại liên kết này là giá trị mặc định chẳng hạn, ví dụ, 1 giây.

Sau khi AP từ chối khung yêu cầu liên kết của STA, AP có thể trao đổi các khung yêu cầu/phản hồi truy vấn SA với STA được cấu hình để duy trì trạng thái liên kết bảo mật (SA) trong suốt thời gian quay trở lại liên kết. Việc trao đổi của các khung yêu cầu/phản hồi truy vấn SA có thể được thực hiện để xác định xem trạng thái SA được lưu trong AP là thông thường hay không hợp lệ.

AP có thể truyền khung yêu cầu truy vấn SA đến STA. Khi thu khung yêu cầu truy vấn SA này, STA có thể truyền khung yêu cầu truy vấn SA chỉ báo rằng trạng thái SA là thông thường đối với AP. Khung yêu cầu truy vấn SA và khung phản hồi truy vấn SA có thể tương ứng với các khung quảng lý được bảo vệ.

Fig.7 là sơ đồ khái niệm minh họa định dạng được lấy làm ví dụ của khung yêu cầu truy vấn liên kết bảo mật (SA) và khung phản hồi truy vấn liên kết bảo mật (SA).

Fig.7(a) thể hiện định dạng được lấy làm ví dụ của khung yêu cầu truy vấn SA.

Liên quan đến Fig.7(a), trường phân loại có thể được đặt giá trị riêng (chẳng hạn, 8) chỉ báo phân loại truy vấn SA.

Trường thao tác truy vấn SA có thể được đặt giá trị riêng (chẳng hạn, 0) chỉ báo khung yêu cầu truy vấn SA.

Trường bộ nhận dạng giao dịch có thể được sử dụng như giá trị riêng để nhận dạng giao dịch yêu cầu/phản hồi truy vấn SA. Giá trị của bộ nhận dạng giao dịch này có thể được thiết lập bởi bên truyền (chẳng hạn, AP) được cấu hình để truyền khung yêu cầu truy vấn SA, và có thể được thiết lập ở giá trị bộ đếm trình tự không âm 16 bit.

Fig.7(b) thể hiện định dạng được lấy làm ví dụ của khung yêu cầu truy vấn SA.

Liên quan đến Fig.7(b), trường phân loại có thể được đặt giá trị riêng (chẳng hạn, 8) chỉ báo phân loại truy vấn SA.

Trường thao tác truy vấn SA có thể được đặt giá trị riêng (chẳng hạn, 1) chỉ báo khung yêu cầu truy vấn SA.

Trường bộ nhận dạng giao dịch có thể có cùng giá trị với giá trị của trường bộ nhận dạng giao dịch được bao gồm trong khung yêu cầu truy vấn SA.

Nếu AP không thu khung yêu cầu truy vấn SA hợp lệ từ STA trong thời gian định trước (chẳng hạn, khoảng thời gian được thiết lập phản hồi lại giá trị tham số 'dot11AssociationSAQueryMaximumTimeout') sau khi truyền khung yêu cầu truy vấn SA, AP không thực hiện quy trình truy vấn SA đối với khung yêu cầu liên kết để được thu sau đó.

Các hoạt động SME và MLME của AP và STA được liên kết với quy trình SA sau đây sẽ được mô tả một cách chi tiết.

Nếu AP có liên kết bảo mật (SA) hợp lệ đối với STA, AP này có thể được hoạt động như sau. SME của từ gốc AP tạo ra MLME-ASSOCIATE.response chỉ

báo “yêu cầu liên kết tạm thời bị từ chối; thử lại sau” và do đó từ chối yêu cầu liên kết. SME của AP có thể bao gồm phần tử khoảng thời gian chờ trong từ gốc MLME-ASSOCIATE.response. Trong trường hợp này, phần tử khoảng thời gian chờ có thể có ba dạng khoảng thời gian chờ (tức là, thời gian quay trở lại liên kết), và giá trị khoảng thời gian chờ có thể chỉ rõ thời gian quay trở lại trong đó AP có thể chấp nhận liên kết với STA tương ứng. Tiếp theo, SME của AP có thể truyền từ gốc MLME-SAQuery.request hướng đến STA ở các khoảng thời gian của thời gian định trước tương ứng với số lượng các đơn vị thời gian (TU) ‘dot11AssociationSAQueryRetryTimeout’. Trong trường hợp này, việc truyền từ gốc MLME-SAQuery.request có thể được thực hiện trước khi từ gốc ‘MLME-SAQuery.confirm’ tương ứng với từ gốc MLME-SAQuery.request được thu, hoặc có thể được thực hiện cho đến khi thời gian định trước tương ứng với số lượng các TU ‘dot11AssociationSAQueryMaximumTimeout’ trôi qua sau khi quy trình truy vấn SA bắt đầu.

Fig.8 là sơ đồ khái niệm minh họa ví dụ về quy trình truy vấn SA.

Trong điều kiện mà trạng thái SA hợp lệ giữa AP và STA được duy trì như được thể hiện trên Fig.8, AP có thể thu khung yêu cầu liên kết mới từ STA khác (sau đây được gọi là bên tấn công) có cùng địa chỉ MAC với địa chỉ của STA tương ứng. Trong trường hợp này, AP nhận biết khung yêu cầu liên kết được truyền từ bên tấn công làm khung yêu cầu liên kết được truyền từ STA có trạng thái SA hợp lệ, truyền khung yêu cầu liên kết từ chối khung yêu cầu liên kết tương ứng đến bên tấn công, và thông báo bên tấn công về thời gian quay trở lại liên kết qua khung phản hồi liên kết. Bên tấn công có thể lại cố gắng để đạt được liên kết sau khi thời gian quay trở lại liên kết trôi qua.

Mặt khác, sau khi AP từ chối yêu cầu liên kết từ bên tấn công, AP này có thể truyền khung yêu cầu truy vấn SA đến STA tương ứng để xác định STA

tương ứng có duy trì trạng thái SA hợp lệ hay không. STA duy trì trạng thái SA, sao cho nó có thể trả lời khung yêu cầu truy vấn SA được thu từ AP. Nếu AP thu thành công khung phản hồi truy vấn SA, AP này xem xét rằng STA tương ứng duy trì trạng thái SA hợp lệ, và sau đó từ chối khung yêu cầu liên kết được thu từ bên tấn công.

Ngoài ra, khung yêu cầu liên kết được truyền từ bên tấn công bị từ chối trước khi thời gian quay trở lại liên kết hết hạn.

Trên Fig.8, giá trị 'dot11AssociationSAQueryMaximumTimeout' được thiết lập là số lượng các đơn vị thời gian (TU) dựa trên yêu cầu truy vấn SA thứ nhất mà quy trình liên kết bắt đầu hoạt động. Cụ thể hơn, sau khi lập lịch yêu cầu truy vấn SA thứ nhất bắt đầu quy trình liên kết, nếu quy trình truy vấn SA không được thu, AP ở trong chế độ chờ mà không phải bắt đầu quy trình truy vấn SA bổ sung nào trong mỗi TU.

Nói chung, giá trị dot11AssociationSAQueryMaximumTimeout và thời gian quay trở lại liên kết có cùng giá trị. Nếu cần, thời gian quay trở lại liên kết có thể cao hơn giá trị dot11AssociationSAQueryMaximumTimeout xem xét đến độ trễ thời gian được xử lý bởi MAC. Độ trễ thời gian không thể tránh khỏi xảy ra trong MAC khi khung yêu cầu liên kết bị từ chối và quy trình truy vấn SA bắt đầu hoạt động sau đó.

Fig.9 là sơ đồ khái niệm minh họa ví dụ khác về quy trình truy vấn SA.

Fig.9 thể hiện rằng STA duy trì trạng thái SA hợp lệ liên quan tới AP khôi phục liên kết thất bại. Nếu thất bại xảy ra trong STA, thông tin trạng thái SA liên quan đến AP biến mất khỏi STA. Do đó, STA được phục hồi thực hiện nhắc lại quy trình liên kết AP, và có thể truyền lại khung yêu cầu liên kết đến AP.

Mặt khác, AP có thể duy trì trạng thái SA liên quan tới STA tương ứng. Do đó, giả định rằng AP nhận biết thu yêu cầu liên kết từ STA có trạng thái SA

hợp lệ, AP có thể truyền khung phản hồi liên kết của mã trạng thái từ chối yêu cầu liên kết được tạo ra từ STA. Trong trường hợp này, AP có thể thiết lập thời gian quay trở lại liên kết là giá trị định trước (chẳng hạn, 1 giây hoặc 1 phút) qua khung yêu cầu liên kết, và có thể truyền thời gian quay trở lại liên kết của giá trị định trước đến STA.

Trong khi đó, sau khi AP từ chối yêu cầu liên kết từ STA, AP này có thể truyền khung yêu cầu truy vấn SA đến STA tương ứng. Mặc dù STA khôi phục trạng thái thất bại, tất cả thông tin trạng thái SA trước đã bị mất, sao cho STA không thể trả lời khung truy vấn SA được thu từ AP. Nếu AP không thu khung yêu cầu truy vấn SA hợp lệ từ STA trong thời gian `dot11AssociationSAQueryMaximumTimeout`, AP xem xét rằng STA tương ứng có trạng thái SA không hợp lệ. Do đó, khung yêu cầu liên kết được truyền từ STA sau khi thời gian quay trở lại liên kết được chấp nhận bởi AP trôi qua.

Như được mô tả ở trên, khung yêu cầu liên kết được thu từ STA có trạng thái SA bị từ chối lần thứ nhất, và AP thực hiện hoạt động truy vấn SA đối với STA trong suốt thời gian quay trở lại liên kết. Nếu STA không trả lời yêu cầu truy vấn SA, AP có thể chấp nhận yêu cầu liên kết tiếp theo được tạo ra sau khi thời gian quay trở lại liên kết trôi qua. Tức là, nếu STA trả lời truy vấn SA, được xác định là khung yêu cầu liên kết thứ nhất thuộc về bên tấn công, sao cho yêu cầu liên kết được tạo ra sau khi thời gian quay trở lại liên kết bị từ chối trôi qua. Nếu STA không trả lời truy vấn SA, được xác định rằng STA hiện tại nhưng không bên tấn công truyền yêu cầu liên kết, sao cho yêu cầu liên kết được tạo ra sau khi thời gian quay trở lại liên kết được chấp nhận trôi qua.

Fig.10 là sơ đồ khái niệm minh họa ví dụ khác về quy trình truy vấn SA.

Theo cùng một cách như trên Fig.8, ví dụ của Fig.10 giả định rằng STA duy trì trạng thái SA hợp lệ đối với AP, và bên tấn công truyền yêu cầu liên kết

đến AP bằng cách sử dụng địa chỉ MAC của STA. AP truyền khung yêu cầu liên kết từ chối yêu cầu liên kết bên tấn công, và cùng lúc thông báo cho STA về thời gian quay trở lại liên kết

AP có thể cố gắng trao đổi yêu cầu truy vấn/phản hồi SA với STA trong thời gian quay trở lại liên kết hoặc trong thời gian `dot11AssociationSAQueryMaximumTimeout`.

Ví dụ, để hỗ trợ các ứng dụng (chẳng hạn bộ cảm biến, lưới thông minh, truyền thông M2M, v.v...) trong dải 1 GHz hoặc thấp hơn bởi STA (chẳng hạn, STA loại chờ dài dạng hoặc STA S1G (1GHz con)) có khả năng duy trì trạng thái nguồn điện thấp trong thời gian dài, STA có thể tiếp tục ở trong trạng thái chờ có hạn giờ trong suốt thời gian `dot11AssociationSAQueryMaximumTimeout`. Trong trường hợp này, STA có thể không trả lời khung yêu cầu truy vấn SA được thu từ AP. Do đó, AP có thể chấp nhận yêu cầu liên kết của bên tấn công sau khi thời gian quay trở lại liên kết trôi qua, sao cho không thể bảo vệ STA hợp lệ đúng cách thức.

Như được mô tả ở trên, theo hoạt động truy vấn SA cũ, không thể tạo ra sự phân biệt giữa một yêu cầu liên kết của STA và yêu cầu liên kết khác của bên tấn công.

Bổ sung vấn đề bảo mật

Theo quy trình truy vấn SA được đề cập ở trên, khung được truyền đến STA hợp lệ có thể được chuyển đến STA độc. Cụ thể, STA nguồn điện thấp có thể bị tổn hại do tấn công của STA độc.

Để cải thiện vấn đề được đề cập ở trên, giả định rằng STA được kết nối SA không trả lời truy vấn SA, và AP chấp nhận yêu cầu liên kết được tạo ra từ STA đã biết sau khi thời gian quay trở lại liên kết trôi qua, nếu khung được truyền đến STA được kết nối SA được đệm bởi AP, AP phải xóa bỏ các khung

tương ứng khỏi bộ đệm, bởi vì không thể xác định xem STA cố gắng thử liên kết mới là STA hợp lệ hay là STA độc.

Ngoài ra, giả định rằng SA được kết nối SA không trả lời truy vấn SA và AP chấp nhận yêu cầu liên kết được thu từ STA đã biết sau khi thời gian quay trở lại liên kết trôi qua, STA tương ứng được liên kết với AP có thể truyền khung hỏi vòng PS đến AP để thu khung được đệm từ AP. Trong trường hợp này, AP có khung hỏi vòng PS được thu không truyền ngay khung được đệm đến STA tương ứng, truyền khung yêu cầu truy vấn SA đến STA tương ứng, xác nhận thông tin trạng thái SA một lần nữa, và truyền kết quả được xác nhận. Thủ tục được đề cập ở trên có thể xác định có hay không STA truyền khung hỏi vòng PS có thông tin trạng thái SA thông thường, để chuẩn bị cho trường hợp trong đó STA độc xóa thông tin trạng thái SA của STA hợp lệ khỏi AP. Do đó, giả định rằng AP thu khung quản lý được bảo vệ tùy ý được cấu hình để xác nhận thông tin trạng thái SA từ STA tương ứng, AP có thể không luôn luôn truyền khung yêu cầu truy vấn SA sau khi khung hỏi vòng PS trôi qua.

Fig.11 là sơ đồ các khái niệm minh họa các phương án khác nhau của quy trình hỏi vòng PS bảo mật.

Liên quan đến Fig.11(a), AP có khung hỏi vòng PS được thu từ STA truyền khung yêu cầu truy vấn SA, và do đó tạo ra yêu cầu xác nhận về thông tin trạng thái SA của STA tương ứng. STA đã thu khung yêu cầu truy vấn SA xác nhận xem khung yêu cầu truy vấn SA tương ứng với khung quản lý được bảo vệ có được mã hóa bình thường hay không, và sau đó truyền khung yêu cầu truy vấn SA đến AP. Tức là, nếu thông tin trạng thái SA của AP là giống với những thông tin trạng thái SA của STA tương ứng, STA có thể truyền khung yêu cầu truy vấn SA và truyền bản tin xác nhận việc chuyển khung dữ liệu đến AP. Mặt khác, nếu thông tin trạng thái SA của AP là khác so với những thông tin trạng

thái SA của STA tương ứng, STA thực hiện thất bại việc kiểm tra tính toàn vẹn của yêu cầu truy vấn SA, sao cho STA có thể không tạo ra phản hồi nào. Nếu phản hồi truy vấn SA không được tạo ra phản hồi lại yêu cầu truy vấn SA, AP có thể không thực hiện chuyển khung dữ liệu đến STA tương ứng.

Ngoài ra, sau khi STA truyền khung ACK phản hồi lại yêu cầu truy vấn SA như được thể hiện trong Fig.11(a), STA này thực hiện sự chờ để truyền sau khi thời gian định trước trôi qua và truyền khung yêu cầu truy vấn SA sau đó. AP đã thu khung yêu cầu truy vấn SA truyền khung ACK, thực hiện sự chờ để truyền sau khi thời gian định trước trôi qua, và truyền khung dữ liệu sau đó. Kết quả là, STA có thể truyền khung ACK.

Mặc dù AP đã thu khung hỏi vòng PS từ STA có thể truyền ngay khung yêu cầu truy vấn SA như được thể hiện trên Fig.11(b), AP này có thể truyền khung ACK lần thứ nhất và sau đó truyền khung yêu cầu truy vấn SA.

Lược đồ hỏi vòng PS được thể hiện trên Fig.11(a) được gọi là lược đồ hỏi vòng PS bảo mật trung bình trong đó khung yêu cầu truy vấn SA được truyền phản hồi lại khung hỏi vòng PS này mà không sử dụng khung ACK. Lược đồ hỏi vòng PS được thể hiện trên Fig.11(b) được gọi là lược đồ hỏi vòng PS bảo mật trì hoãn trong đó khung ACK được truyền phản hồi lại khung hỏi vòng PS và khung yêu cầu truy vấn SA được truyền sau đó.

Ngoài ra, lược đồ hỏi vòng PS được thể hiện trong Fig.11(c) được gọi là ‘không cần nguyên tắc hỏi vòng PS bảo mật trì hoãn ACK’ trong đó khung yêu cầu truy vấn SA được truyền ngay như là phản hồi lại khung yêu cầu truy vấn SA.

Nếu sự truyền nhiều khung được cho phép sau khi khung hỏi vòng PS trôi qua, khung yêu cầu truy vấn SA có thể được truyền sau khoảng không liên khung

ngắn hơn (SIFS), sau khi khung ACK của khung hỏi vòng PS trôi qua như được thể hiện trên Fig.11(d).

Khi thu khung phản hồi cầu truy vấn SA từ STA phản hồi lại khung yêu cầu truy vấn SA, AP có thể xác định giao thức để truyền khung được đếm đến STA. Do đó, khung dữ liệu được đếm cho STA hợp lệ được ngăn chặn không bị cấp tới STA độc.

Tối ưu hóa hoạt động liên kết

Sáng chế đề xuất phương pháp để chỉ báo có hay không liên kết của STA tương ứng được chấp nhận trước khi thời gian quay trở lại liên kết hết hạn để ngăn ngừa sự cố gắng liên kết không cần thiết của các STA.

Sau khi AP từ chối yêu cầu liên kết mới, giả định rằng phản hồi truy vấn SA đối với yêu cầu truy vấn SA được thu thành công trước khi thời gian quay trở lại liên kết hết hạn. Trong trường hợp này, AP có thể chỉ báo rằng liên kết của địa chỉ MAC của STA tương ứng bị từ chối qua khung báo hiệu, khung phản hồi thăm dò, v.v...

Ví dụ, phần tử thông tin điều khiển liên kết có thể được chứa trong khung báo hiệu, khung phản hồi thăm dò, v.v... Phần tử thông tin điều khiển liên kết này có thể bao gồm địa chỉ MAC của STA, yêu cầu liên kết của nó sẽ bị từ chối.

Ngoài ra, nếu AP nhằm mục đích chấp nhận yêu cầu liên kết của STA đã biết bởi lý do đặc biệt, phần tử thông tin điều khiển liên kết có thể bao gồm thêm thông tin liên quan đến địa chỉ MAC của STA mà mong muốn chấp nhận yêu cầu liên kết này. Trong trường hợp này, không những dạng trường chỉ báo liên kết của STA tương ứng hoặc được chấp nhận hoặc bị từ chối, mà còn thông tin địa chỉ MAC của STA có thể được chứa trong phần tử thông tin điều khiển liên kết.

Phương pháp duy trì liên kết

Sáng chế có thể ngăn khung được cấp đến STA hợp lệ không bị cấp nhầm đến STA độc theo phương pháp được đề cập ở trên. Tuy nhiên, về cơ bản, sáng chế không thể giải quyết vấn đề trong đó STA độc được liên kết với AP và STA hợp lệ không được liên kết với AP này.

Để tránh vấn đề được đề cập ở trên, cần thiết thay đổi thiết lập thời gian quay trở lại liên kết cũ. Ví dụ, giả định rằng STA ở trong trạng thái nguồn điện thấp (chẳng hạn, trạng thái chờ hoặc trạng thái chờ có hẹn giờ) trong 10 phút, là cần thiết để phân bổ thời gian khoảng 10 phút hoặc nhiều hơn đối với thời gian quay trở lại liên kết được liên kết với quy trình truy vấn SA hoặc tham số `dot11AssociationSAQueryMaximumTimeout`. Sau khi AP từ chối khung yêu cầu liên kết ban đầu, AP phải cố gắng trao đổi khung yêu cầu/phản hồi truy vấn SA trong 10 phút, sao cho STA có chế độ chờ ở khoảng 10 phút có thể có cơ hội truyền phản hồi truy vấn SA. Tức là, thời gian quay trở lại liên kết hoặc thời gian `dot11AssociationSAQueryMaximumTimeout` có thể được thiết lập trong thời gian dài xem xét đến thời gian duy trì chế độ chờ STA, sao cho được xác định liệu STA không trả lời khung yêu cầu truy vấn SA hay không bởi vì STA ở trong trạng thái nguồn điện thấp, hoặc được xác định liệu STA có không trả lời khung yêu cầu truy vấn SA hay không bởi vì trạng thái SA của STA tương ứng không hợp lệ.

Sáng chế đề xuất phương pháp để cho phép AP cung cấp các thời gian quay trở lại liên kết khác nhau theo các dạng STA. Ví dụ, dạng STA (chẳng hạn, STA S1G(Sub 1 GHz)) hỗ trợ các ứng dụng chẳng hạn bộ cảm biến, lưới thông minh, M2M, v.v... có chu trình hoạt động thấp, sao cho giá trị tương đối cao có thể được gán cho thời gian quay trở lại liên kết. Ngược lại, STA chung khác (chẳng hạn, STA định hướng lưu lượng) có chu trình hoạt động cao, sao cho giá trị tương đối thấp có thể được gán cho thời gian quay trở lại liên kết.

Ngoài ra, nếu một số lượng lớn STA đồng thời được phục hồi lại từ trạng thái thất bại, các STA này đồng thời cố gắng thực hiện liên kết, dẫn đến các sự xung đột tần số tăng. Để giải quyết vấn đề trên, thời gian quay trở lại liên kết được ngẫu nhiên hóa ngay cả khi các dạng STA là giống nhau, kết quả được ngẫu nhiên hóa có thể được áp dụng cho STA. Nếu các STA có các thời gian quay trở lại khác nhau được phân bổ đến các STA có cùng thời gian cố gắng liên kết ban đầu, các STA riêng rẽ có các thời gian đợi khác nhau cho đến khi cố gắng thực hiện lại liên kết, dẫn đến giảm khả năng thực hiện kênh truy cập cùng lúc.

Đối với mục đích này, khi STA truyền khung yêu cầu liên kết, thông tin dạng STA có thể được chứa trong khung yêu cầu liên kết. Nếu AP thu thông tin dạng STA được chứa trong khung yêu cầu liên kết, AP này có thể quyết định thời gian quay trở lại liên kết của STA tương ứng trên cơ sở thông tin được thu.

AP có thể thông báo STA về thời gian quay trở lại liên kết qua khung phản hồi liên kết. Theo sáng chế, ngay cả khi STA cố gắng thực hiện liên kết ban đầu với AP, AP này có thể bao gồm thông tin liên quan đến thời gian quay trở lại liên kết trong khung phản hồi liên kết. Ngoài ra, Theo sáng chế, khi STA yêu cầu liên kết, và mã trạng thái (0) chỉ báo thành công được gán cho khung phản hồi liên kết bởi AP, thông tin liên quan đến thời gian quay trở lại liên kết có thể được chứa trong khung phản hồi liên kết tương ứng.

Tức là, theo đề xuất của sáng chế, khi AP từ chối yêu cầu liên kết, AP này thông báo cho STA về thời gian quay trở lại liên kết, sao cho STA tương ứng không cố gắng thực hiện lại liên kết trong suốt thời gian quay trở lại liên kết. Ngoài ra, ngay cả khi AP chấp nhận yêu cầu liên kết STA, thời gian quay trở lại liên kết có thể được chứa trong khung phản hồi liên kết. Do đó, nếu STA mong muốn duy trì liên tục trạng thái SA, AP có thể cung cấp thông tin cần thiết (chẳng hạn, thông tin cụ thể chỉ báo rằng thời gian quay trở lại liên kết hoặc

dot11AssociationSAQueryMaximumTimeout được gán cho khoảng thời gian hoạt động của STA) đến STA ở các khoảng thời gian của thời gian quay trở lại liên kết sao cho STA có thể hoạt động ở các khoảng thời gian của thời gian quay trở lại liên kết. Do đó, STA hoạt động trên cơ sở thời gian quay trở lại liên kết hoặc khoảng thời gian dot11AssociationSAQueryMaximumTimeout (chẳng hạn, thời gian ngắn hơn dot11AssociationSAQueryMaximumTimeout), sao cho STA có thể cố gắng thu khung yêu cầu truy vấn SA và có thể duy trì trạng thái SA hợp lệ.

Ngoài ra, nếu AP mong muốn thay đổi thời gian quay trở lại liên kết được áp dụng cho STA, AP này có thể thông báo STA về giá trị thời gian quay trở lại liên kết được thay đổi qua khung báo hiệu, khung phản hồi thăm dò, v.v...

Ngoài ra, nếu AP gán các giá trị thời gian quay trở lại liên kết khác nhau cho các dạng STA, các giá trị dot11AssociatioSAQueryMaximumTimeout khác nhau có thể được gán cho các dạng STA. Theo cách khác, mặc dù các dạng STA giống nhau được sử dụng, các giá trị dot11AssociatioSAQueryMaximumTimeout khác nhau có thể được gán cho các STA riêng rẽ.

Thời gian quay trở lại liên kết được chuyển từ AP đến STA qua khung phản hồi liên kết hoặc khung phản hồi liên kết lại có thể được gán cùng giá trị là dot11AssociatioSAQueryMaximumTimeout, hoặc có thể được gán giá trị cao hơn giá trị dot11AssociatioSAQueryMaximumTimeout.

Nếu STA mà đã hoàn tất thành công quy trình liên kết thu thời gian quay trở lại liên kết (hoặc dot11AssociatioSAQueryMaximumTimeout) từ AP, STA hoạt động ở các khoảng thời gian của thời gian ngắn hơn khoảng thời gian quay trở lại liên kết (hoặc dot11AssociatioSAQueryMaximumTimeout), sao cho STA phải nhận biết có hay không khung yêu cầu truy vấn SA được thu từ AP.

Tức là, STA hoạt động thường xuyên hơn khoảng thời gian quay trở lại liên kết (hoặc `dot11AssociatioSAQueryMaximumTimeout`) và truyền khung hỏi vòng PS; hoặc STA xác nhận khung được đếm có mặt trong AP qua phần tử TIM của khung báo hiệu và thu khung được đếm hay không.

Fig.12 là giản đồ minh họa phương pháp duy trì liên kết theo ví dụ của sáng chế.

Trong bước S1110, STA có thể truyền khung yêu cầu liên kết đến AP. Trong trường hợp này, STA có trạng thái SA hợp lệ đối với AP. Ngoài ra, STA này có thể hoạt động trong chế độ PS (power save - tiết kiệm điện).

Trong bước S1120, ngay cả khi AP chấp nhận yêu cầu liên kết của STA, thông tin thời gian quay trở lại liên kết có thể được chứa trong khung phản hồi liên kết. Ví dụ, mã trạng thái của khung phản hồi liên kết được thiết lập là số không (0) (tức là, thành công), và khung phản hồi liên kết có thể bao gồm thông tin thời gian quay trở lại liên kết.

Do đó, khi thu thời gian quay trở lại liên kết từ AP, STA hoạt động ở các khoảng thời gian của thời gian tương tự hoặc ngắn hơn thời gian quay trở lại liên kết được thu từ AP, và cố gắng thu khung yêu cầu truy vấn SA từ AP. Khi thu yêu cầu truy vấn SA, STA có thể truyền phản hồi truy vấn SA đến AP. Do đó, trạng thái SA hợp lệ giữa STA và AP có thể được duy trì.

Phương pháp duy trì liên kết theo phương án được thể hiện trên Fig.12 có thể được thực hiện sao cho các phương án khác được mô tả ở trên của sáng chế có thể được áp dụng một cách độc lập hoặc hai hoặc nhiều các phương án của nó có thể được áp dụng đồng thời.

Fig.13 là sơ đồ khối minh họa thiết bị tần số radio (RF) theo một phương án của sáng chế.

Liên quan đến Fig.13, AP 10 có thể bao gồm bộ xử lý 11, bộ nhớ 12, và bộ thu truyền 13. STA 20 có thể bao gồm bộ xử lý 21, bộ nhớ 22, và bộ thu truyền 23. Các bộ thu truyền 13 và 23 có thể truyền/thu các tín hiệu tần số radio (RF) và có thể thực hiện lớp vật lý theo hệ thống IEEE 802. Các bộ xử lý 11 và 21 được kết nối một cách tương ứng tới các bộ thu truyền 13 và 21, và có thể thực hiện lớp vật lý và/hoặc lớp MAC theo hệ thống IEEE 802. Các bộ xử lý 11 và 21 có thể được cấu hình để hoạt động theo các phương án khác được mô tả ở trên của sáng chế. Các môđun để thực hiện hoạt động của AP và STA theo các phương án khác được mô tả ở trên của sáng chế được lưu giữ trong các bộ nhớ 12 và 22 và có thể được thực hiện bởi các bộ xử lý 11 và 21. Các bộ nhớ 12 và 22 có thể được bao gồm trong các bộ xử lý 11 và 21 hoặc có thể được cài đặt ở bên ngoài của các bộ xử lý 11 và 21 và được kết nối đến các bộ xử lý 11 và 21 bởi cách phương pháp đã biết.

Bộ xử lý 11 của AP 10 được thể hiện trên Fig.12 có thể thu khung yêu cầu liên kết từ STA 20 bằng cách sử dụng bộ thu truyền 13. Ngoài ra, bộ xử lý 11 có thể truyền khung phản hồi liên kết đến STA 20 bằng cách sử dụng bộ thu truyền 13. Trong trường hợp này, ngay cả khi yêu cầu liên kết được chấp nhận, thông tin liên quan đến thời gian quay trở lại liên kết có thể được chứa trong khung phản hồi liên kết.

Bộ xử lý 21 của STA 20 được thể hiện trên Fig.12 có thể truyền khung yêu cầu liên kết đến AP 10 bằng cách sử dụng bộ thu truyền 23. Ngoài ra, bộ xử lý 21 có thể thu khung phản hồi liên kết từ AP 10 bằng cách sử dụng bộ thu truyền 23. Trong trường hợp này, ngay cả khi AP 10 chấp nhận yêu cầu liên kết, thông tin thời gian quay trở lại liên kết có thể được chứa trong khung phản hồi liên kết. Do đó, bộ xử lý 21 của STA 20 có thể hoạt động ở các khoảng thời gian của thời gian tương tự hoặc ngắn hơn thời gian quay trở lại liên kết, và có thể có

gắng thu khung yêu cầu truy vấn SA từ AP 10. Dựa trên thu yêu cầu truy vấn SA, phản hồi truy vấn SA có thể được truyền đến AP 10.

Toàn bộ cấu hình của AP 10 và STA 20 được thể hiện trên Fig.13 có thể được thực hiện sao cho các phương án khác được mô tả ở trên của sáng chế có thể được áp dụng một cách độc lập hoặc hai hoặc nhiều phương án của nó có thể áp dụng đồng thời và phần mô tả lặp lại của nó được bỏ qua để làm sáng tỏ.

Các phương án được mô tả ở trên có thể được thực hiện bằng nhiều cách khác nhau, chẳng hạn, bằng phần cứng, vi chương trình, phần mềm, hoặc sự kết hợp của nó.

Cấu hình phần cứng, phương pháp theo các phương án của sáng chế có thể được thực hiện bởi một hoặc nhiều các mạch tích hợp ứng dụng cụ thể (ASIC), các bộ xử lý tín hiệu số (DSP), các thiết bị xử lý tín hiệu số (DSPD), các thiết bị logic lập trình (PLD), các mảng cổng khả lập trình dạng trường (FPGA), các bộ xử lý, các bộ điều khiển, các vi điều khiển, hoặc các bộ vi xử lý.

Trong cấu hình phần cứng và phần mềm, phương pháp theo các phương án của sáng chế có thể được thực hiện ở dạng các môđun, các thủ tục, các chức năng, v.v... thực hiện các chức năng hoặc các hoạt động được mô tả ở trên. Mã phần mềm có thể có thể được lưu trữ trong đơn vị bộ nhớ và được thực hiện bởi bộ xử lý. Bộ nhớ có thể được đặt ở bên trong hoặc bên ngoài bộ xử lý và có thể truyền và thu dữ liệu đến và từ bộ xử lý qua nhiều cách đã biết khác.

Phần mô tả chi tiết các phương án ưu tiên của sáng chế đã được trình bày cho phép người có hiểu biết trung bình trong lĩnh vực thực hiện và áp dụng sáng chế. Mặc dù sáng chế được mô tả cùng với các phương án ưu tiên, những người có hiểu biết trung bình trong lĩnh vực sẽ hiểu được rằng các sửa đổi và thay đổi khác có thể được thực hiện theo sáng chế mà không nằm ngoài phạm vi của sáng chế được mô tả trong bộ yêu cầu bảo hộ kèm theo. Do đó, sáng chế không bị giới

hạn đối với các phương án cụ thể được mô tả ở đây, nhưng được thống nhất với phạm vi rộng nhất phù hợp với các nguyên lý và các dấu hiệu mới được bộc lộ ở đây.

Khả năng ứng dụng trong công nghiệp

Mặc dù các phương án khác ở trên của sáng chế có được mô tả dựa trên hệ thống IEEE 802.11, các phương án có thể được áp dụng theo cùng một cách cho các hệ thống truyền thông di động khác.

YÊU CẦU BẢO HỘ

1. Phương pháp thực hiện liên kết bởi trạm (Station - STA) trong hệ thống LAN không dây (WLAN), phương pháp bao gồm:

truyền khung yêu cầu liên kết từ trạm (STA) đến điểm truy cập (Access point - AP); và

thu khung phản hồi liên kết từ điểm truy cập (AP) phản hồi lại khung yêu cầu liên kết,

trong đó, nếu yêu cầu liên kết được chấp nhận bởi điểm truy cập (AP), khung phản hồi liên kết bao gồm thông tin liên quan đến thời gian quay trở lại liên kết, và

trong đó thời gian quay trở lại liên kết là khoảng thời gian để thu khung yêu cầu truy vấn liên kết bảo mật (Security Association - SA).

2. Phương pháp theo điểm 1, trong đó trạm (STA) hoạt động trên cơ sở thời gian quay trở lại liên kết, và cố gắng thu khung yêu cầu truy vấn liên kết bảo mật (SA) từ AP.

3. Phương pháp theo điểm 2, trong đó STA hoạt động ở các khoảng thời gian của thời gian tương tự hoặc ngắn hơn thời gian định trước được chỉ báo bởi thời gian quay trở lại liên kết, và cố gắng thu khung yêu cầu truy vấn SA.

4. Phương pháp theo điểm 3, trong đó:

khi thu khung yêu cầu truy vấn SA từ AP, STA truyền khung phản hồi truy vấn SA đến AP.

5. Phương pháp theo điểm 4, trong đó:

thông qua việc thu khung yêu cầu truy vấn SA hoặc sự truyền khung phản hồi truy vấn SA, trạng thái SA hợp lệ của STA được duy trì.

6. Phương pháp theo điểm 1, trong đó:

giá trị thời gian chờ của quy trình truy vấn SA được thiết lập trên cơ sở thời gian quay trở lại liên kết.

7. Phương pháp theo điểm 6, trong đó giá trị thời gian chờ của quy trình truy vấn SA được thiết lập ở giá trị tham số dot11AssociationSAQueryMaximumTimeout.

8. Phương pháp theo điểm 1, trong đó:

nếu yêu cầu liên kết được chấp nhận bởi AP, mã trạng thái của khung phản hồi liên kết được thiết lập ở không (0),

trong đó mã trạng thái '0' chỉ báo "thành công".

9. Phương pháp theo điểm 1, trong đó:

nếu yêu cầu liên kết bị từ chối bởi AP, khung phản hồi liên kết bao gồm thông tin liên quan đến thời gian quay trở lại liên kết.

10. Phương pháp theo điểm 9, trong đó:

nếu yêu cầu liên kết bị từ chối bởi AP, mã trạng thái của khung phản hồi liên kết được thiết lập ở 30,

trong đó mã trạng thái '30' chỉ báo "Yêu cầu liên kết tạm thời bị từ chối; thử lại sau".

11. Phương pháp theo điểm 1, trong đó STA hoạt động ở chế độ tiết kiệm điện (power save - PS).

12. Phương pháp theo điểm 1, trong đó trạm (STA) có trạng thái liên kết bảo mật (SA) với điểm truy cập (AP) trước khi truyền khung yêu cầu liên kết.

13. Phương pháp hỗ trợ liên kết của trạm (STA) bởi điểm truy cập (AP) trong hệ thống LAN không dây (WLAN), phương pháp bao gồm các bước:

thu khung yêu cầu liên kết từ trạm (STA); và

truyền khung phản hồi liên kết đến trạm (STA) phản hồi lại khung yêu cầu liên kết,

trong đó, nếu yêu cầu liên kết được chấp nhận bởi điểm truy cập (AP), khung phản hồi liên kết bao gồm thông tin liên quan đến thời gian quay trở lại liên kết, và

trong đó thời gian quay trở lại liên kết là khoảng thời gian để truyền khung yêu cầu truy vấn liên kết bảo mật (Security Association - SA).

14. Thiết bị trạm (STA) để thực hiện liên kết trong hệ thống LAN không dây (WLAN), thiết bị bao gồm:

bộ thu truyền; và

bộ xử lý,

trong đó bộ xử lý truyền khung yêu cầu liên kết đến điểm truy cập (AP) bằng cách sử dụng bộ thu truyền, và thu khung phản hồi liên kết từ điểm truy cập (AP) phản hồi lại khung yêu cầu liên kết,

trong đó, nếu yêu cầu liên kết được chấp nhận bởi điểm truy cập (AP), khung phản hồi liên kết bao gồm thông tin liên quan đến thời gian quay trở lại liên kết, và

trong đó thời gian quay trở lại liên kết là khoảng thời gian để thu khung yêu cầu truy vấn liên kết bảo mật (Security Association - SA).

15. Thiết bị điểm truy cập (AP) để hỗ trợ liên kết của trạm (STA) trong hệ thống LAN không dây (WLAN), thiết bị này bao gồm:

bộ thu truyền; và

bộ xử lý,

trong đó bộ xử lý thu khung yêu cầu liên kết từ trạm (STA) bằng cách sử dụng bộ thu truyền, và truyền khung phản hồi liên kết đến trạm (STA) phản hồi lại khung yêu cầu liên kết bằng cách sử dụng bộ thu truyền này,

trong đó, nếu yêu cầu liên kết được chấp nhận bởi điểm truy cập (AP), khung phản hồi liên kết bao gồm thông tin liên quan đến thời gian quay trở lại liên kết, và

trong đó thời gian quay trở lại liên kết là khoảng thời gian để truyền khung yêu cầu truy vấn liên kết bảo mật (Security Association - SA).

FIG. 1

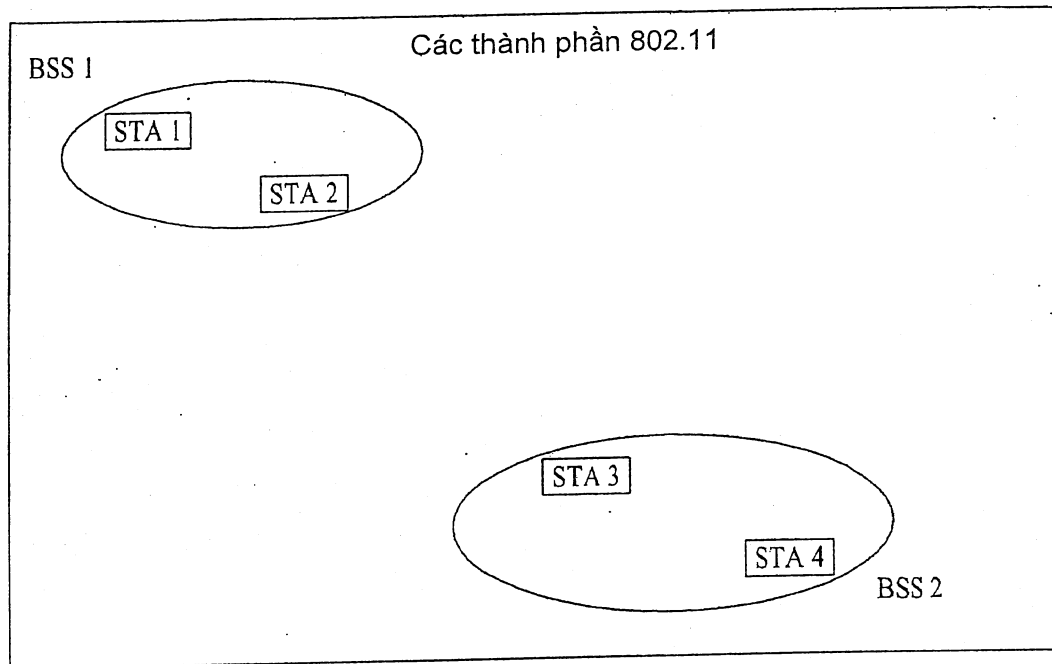
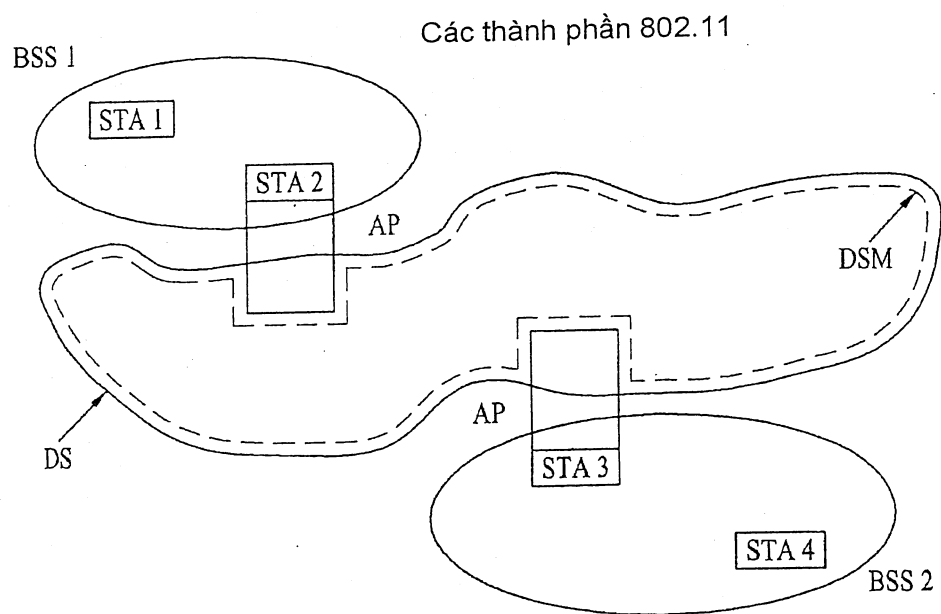


FIG. 2



Các thành phần 802.11

FIG. 3

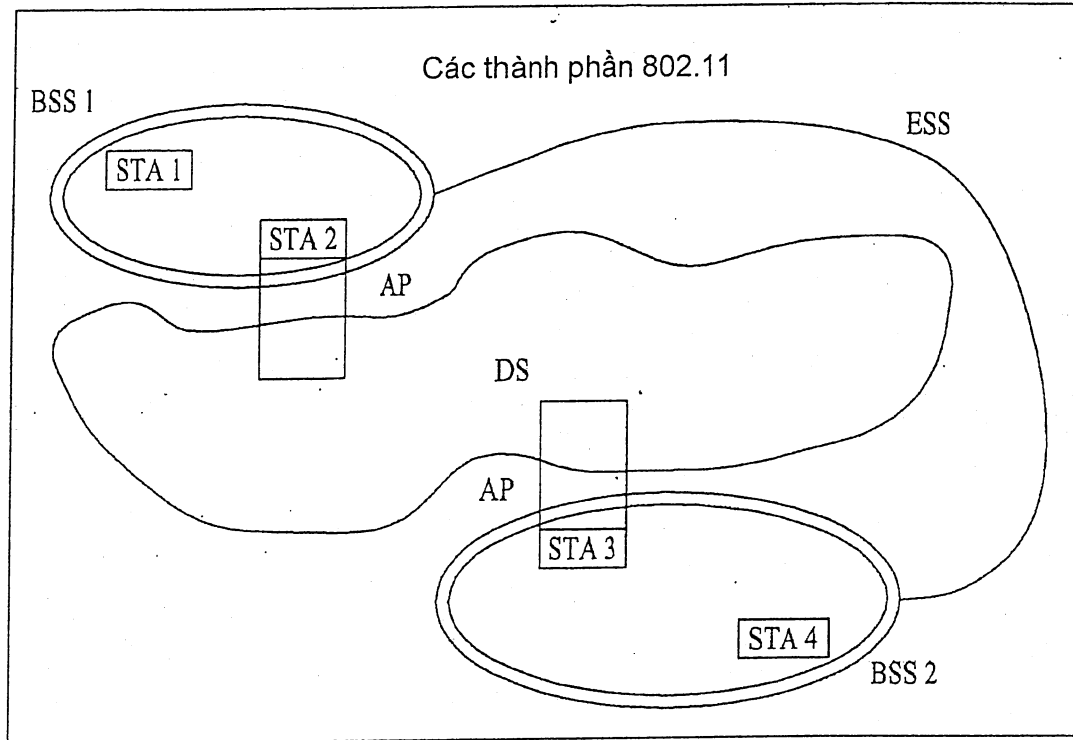


FIG. 4

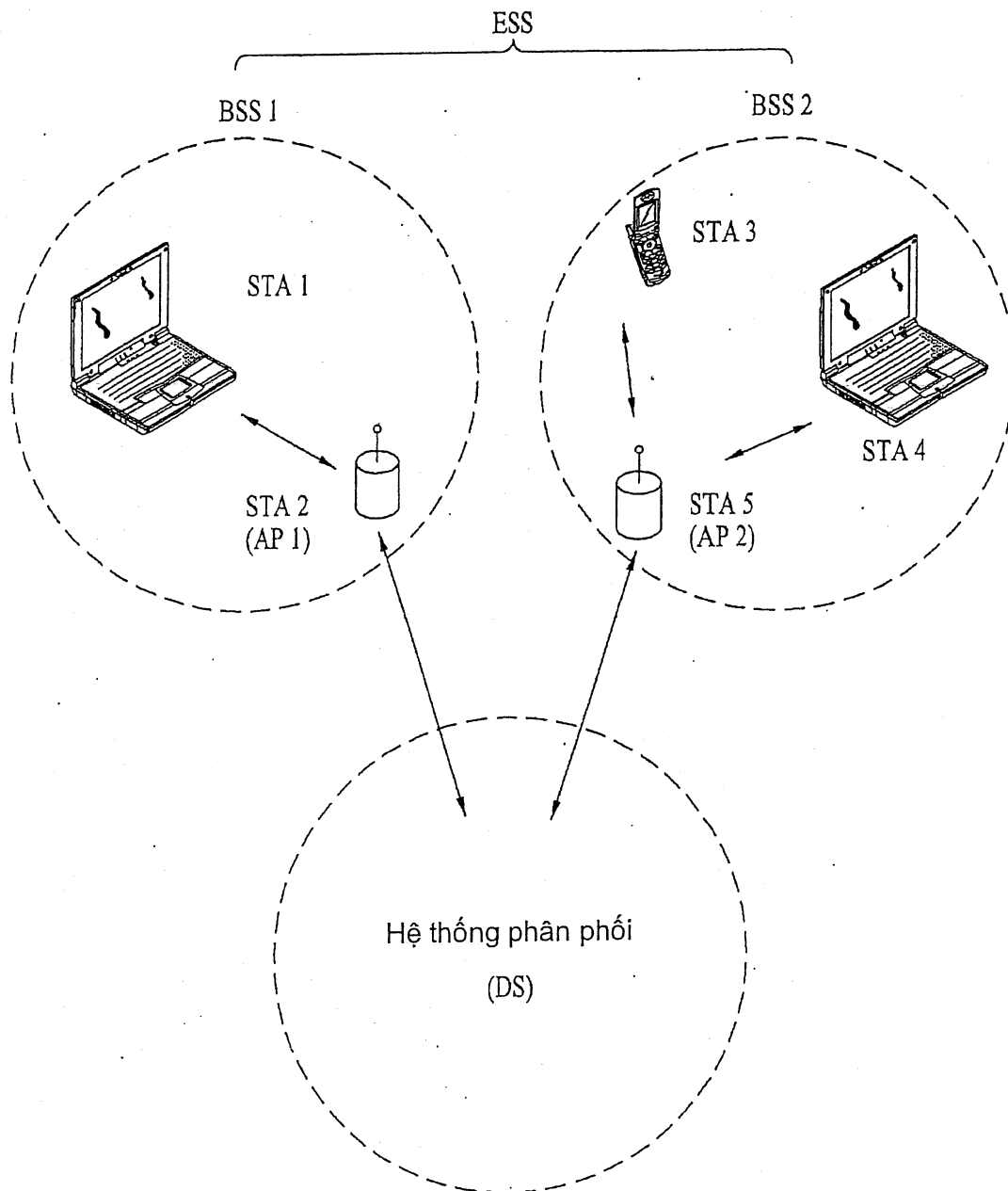


FIG. 5

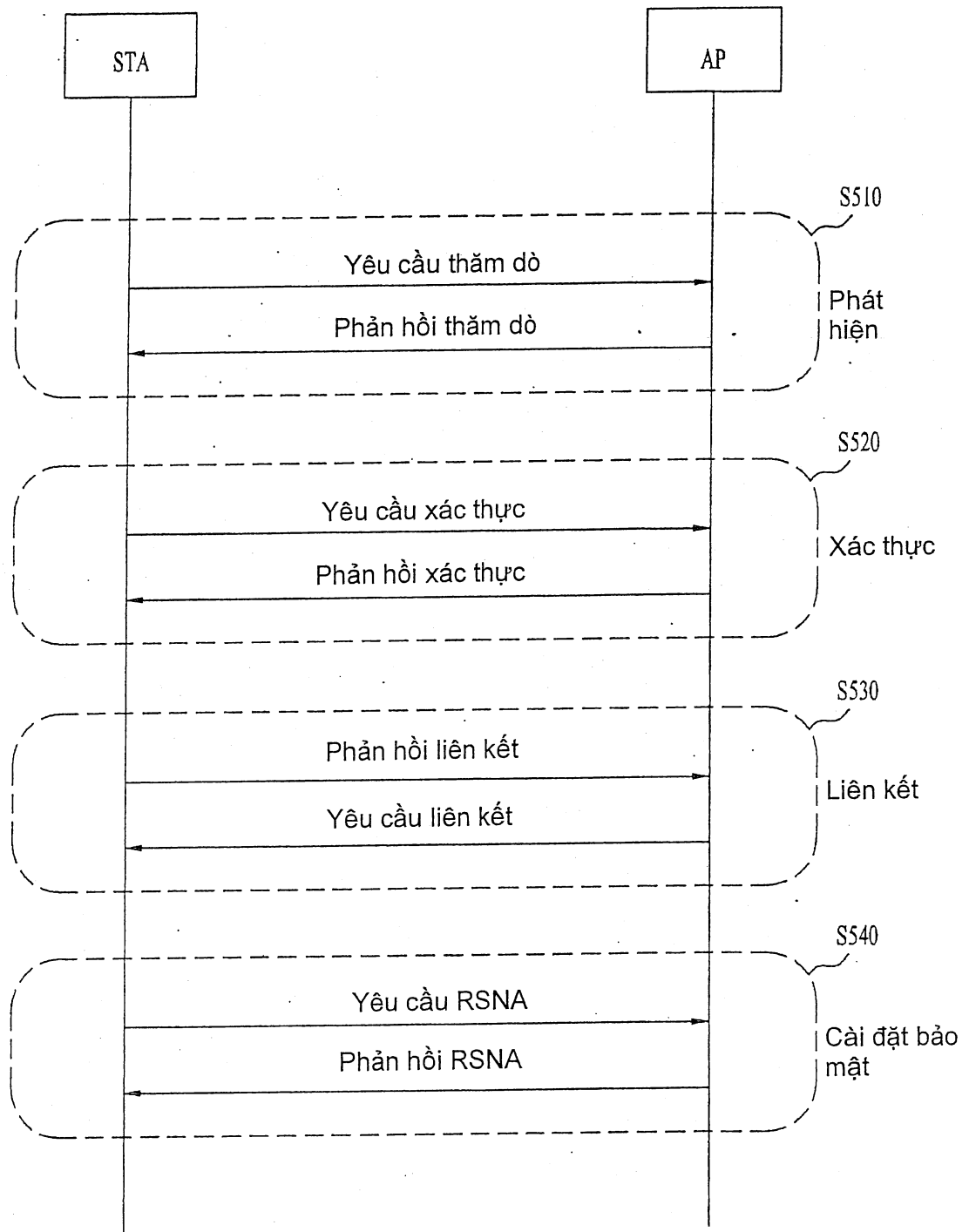


FIG. 6

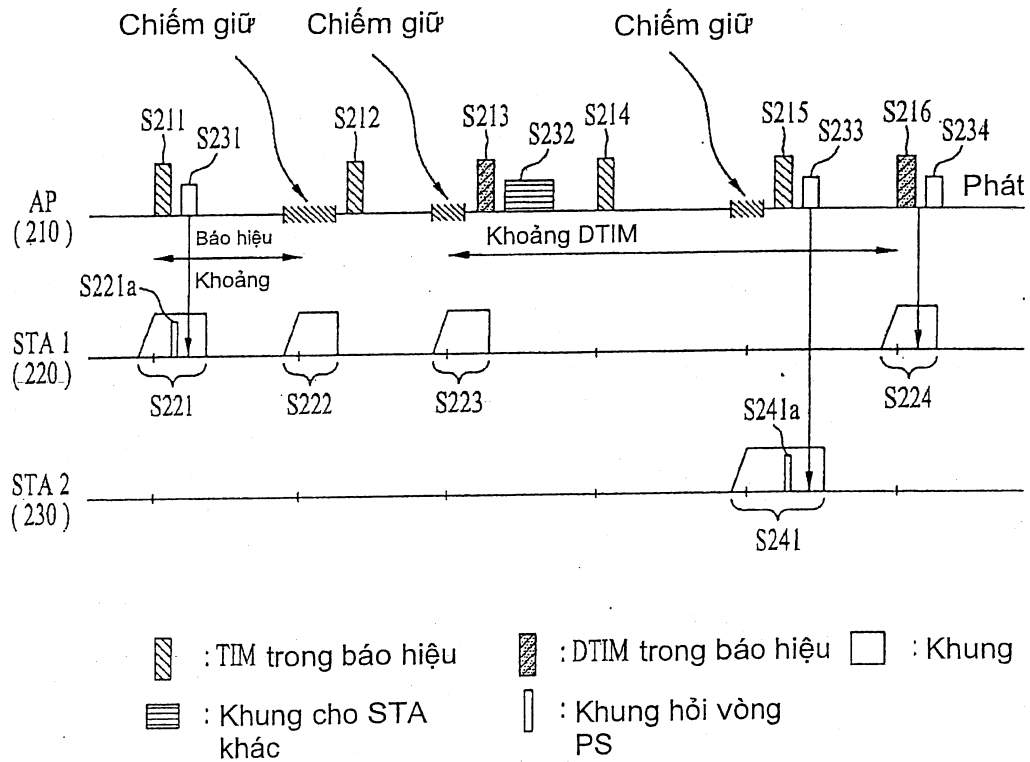


FIG. 7

Phân loại	Thao tác truy vấn SA (thiết đặt ở giá trị chỉ báo khung yêu cầu truy vấn SA)	Bộ nhận dạng giao dịch
1	1	2

Bộ tám bit : (a)

Phân loại	Thao tác truy vấn SA (thiết đặt ở giá trị chỉ báo khung phản hồi truy vấn SA)	Bộ nhận dạng giao dịch
1	1	2

Bộ tám bit : (b)

FIG. 8

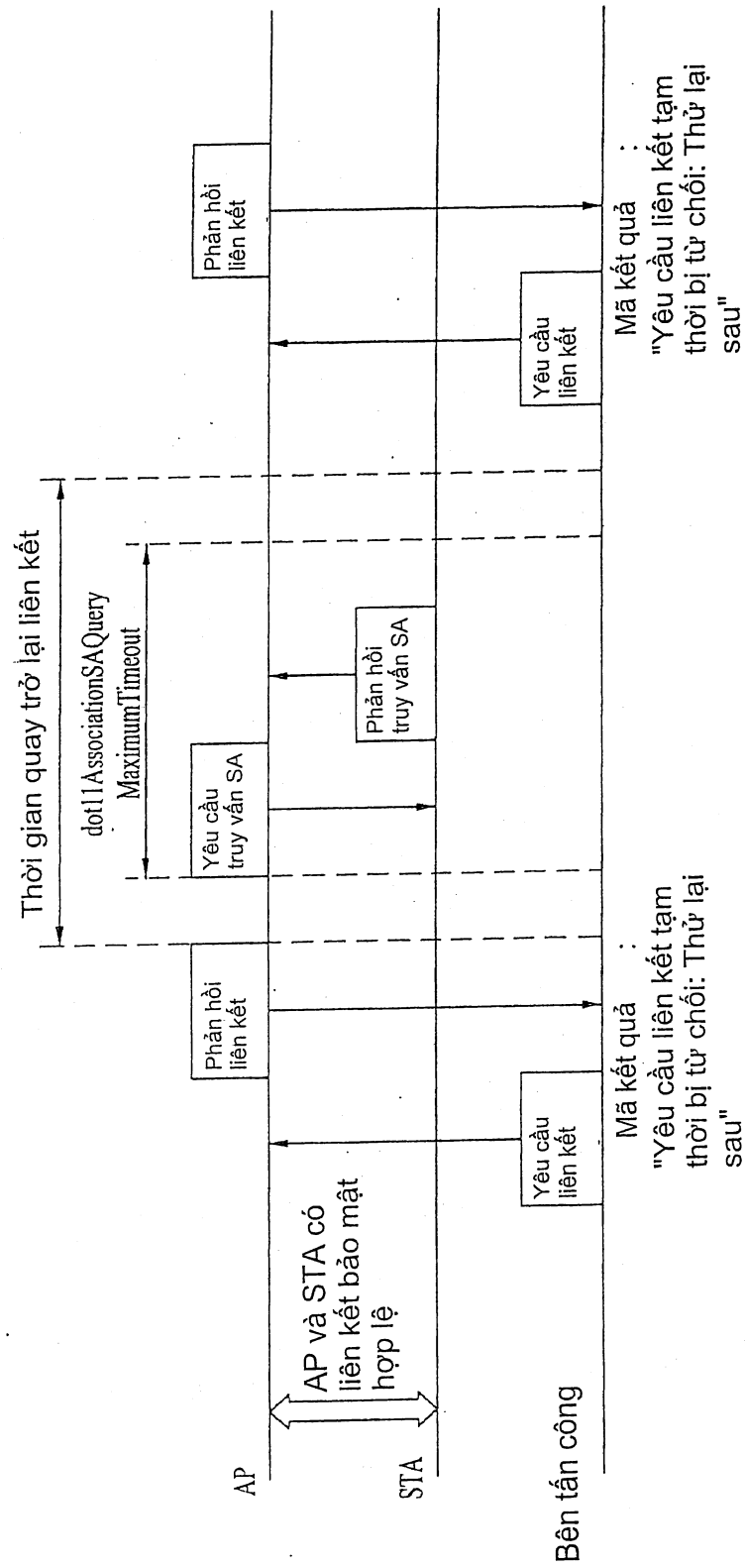


FIG. 10

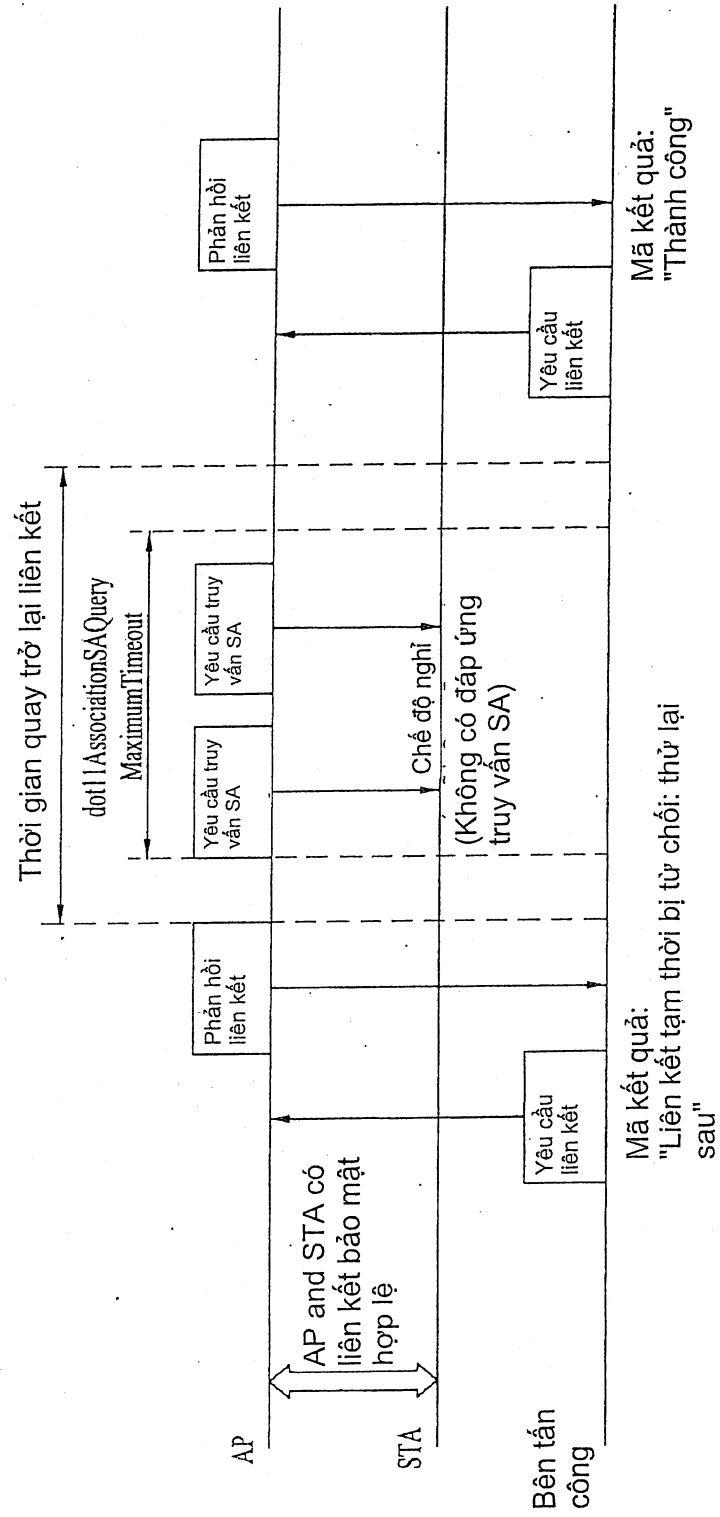
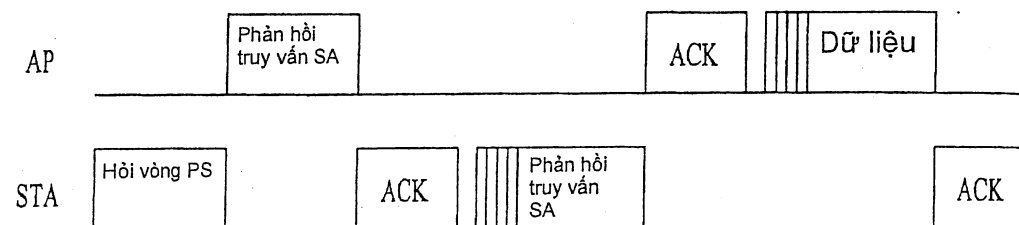
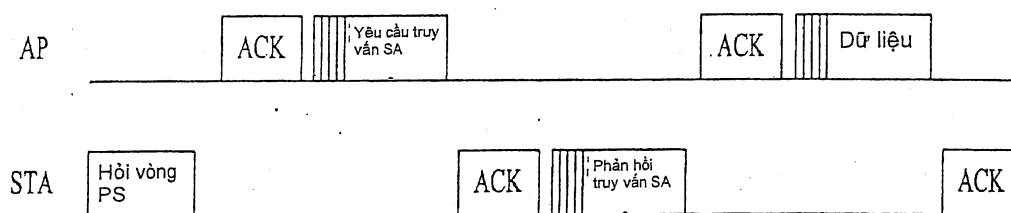


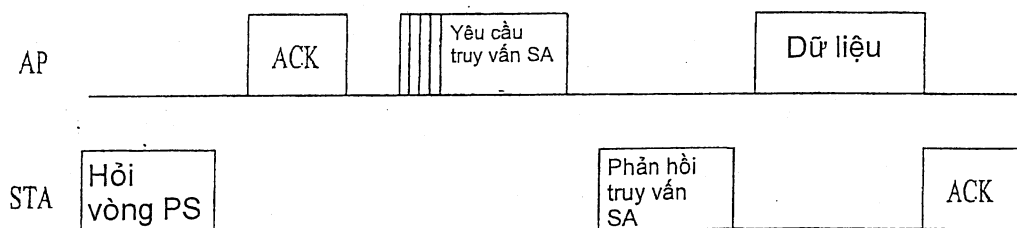
FIG. 11



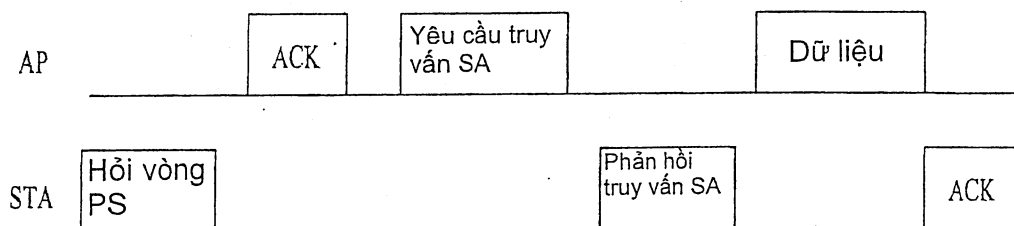
(a) Hỏi vòng PS bảo mật trung bình



(b) Hỏi vòng PS bảo mật tạm hoãn



(c) Hỏi vòng PS bảo mật tạm hoãn không có nguyên tắc ACK



(d) Hỏi vòng PS bảo mật tạm hoãn không có nguyên tắc ACK

FIG. 12

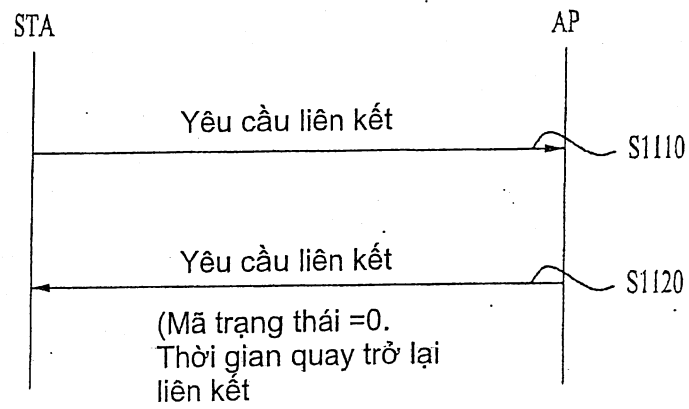


FIG. 13

