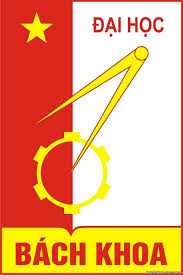
**ĐẠI HỌC BÁCH KHOA HÀ NỘI**

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

-------------------\*\*\*--------------------



**BÁO CÁO BÀI TẬP LỚN**

AN NINH MẠNG

**Đề tài**: Bảo mật cho mạng không dây. Phân tích các đặc trưng thống kê của các dạng tấn công từ chối dịch vụ. Xác thực và bảo mật trong mạng không dây. Phát hiện bất thường trong mạng không dây.

Giảng viên hướng dẫn: **PGS.TS. Nguyễn Linh Giang**

Sinh viên thực hiện: Nhóm 17

|  |  |
| --- | --- |
| **Nguyễn Gia Tuyến** | **20122726** |
| **Bùi Tuấn Ánh** | **20121247** |
| **Nguyễn Thị Nga** | **20122136** |
| **Thái Thị Lộc** | **20122020** |

**HÀ NỘI 12/2015**

**MỤC LỤC**

[**I. Giới Thiệu** 4](#_Toc436906614)

[**1. Khái niệm** 4](#_Toc436906615)

[**2. Các dạng chuẩn** 6](#_Toc436906616)

[**3. Mô hình** 10](#_Toc436906617)

[3.1 Mô hình mạng Ad-hoc 10](#_Toc436906618)

[3.2 Mô hình mạng cơ sở Basic Service Set (BSS) 11](#_Toc436906619)

[3.3 Mô hình mạng mở rộng Extended Service Set (ESS) 12](#_Toc436906620)

[**4. Các thành phần trong mạng không dây** 13](#_Toc436906621)

[**5. Hoạt động của mạng không dây** 14](#_Toc436906622)

[**III. Các dạng tấn công từ chối dịch vụ mạng không dây** 16](#_Toc436906623)

[**1. Định nghĩa** 16](#_Toc436906624)

[**2. Nguyên nhân** 16](#_Toc436906625)

[**3. Các dạng tấn công từ chối dịch vụ mạng không dây** 16](#_Toc436906626)

[3.1. Tấn công Access Point overloading 16](#_Toc436906627)

[3.3. Tấn công dựa trên cảm nhận sóng mang lớp vật lý – Gây nhiễu 20](#_Toc436906628)

[3.4. Tấn công ngắt kết nối – Disassociation flood attack 21](#_Toc436906629)

[**IV. Xác thực và bảo mật trong mạng không dây** 22](#_Toc436906630)

[**1. WEP** 22](#_Toc436906631)

[**2. WLAN VPN** 24](#_Toc436906632)

[**3. TKIP (Temporal Key Integrity Protocol)** 24](#_Toc436906633)

[**4. AES (Advanced Encryption Standard)** 24](#_Toc436906634)

[**5. 802.1x và EAP** 25](#_Toc436906635)

[**6. WPA** 26](#_Toc436906636)

[**7. WPA2** 28](#_Toc436906637)

[**8. Lọc** 29](#_Toc436906638)

[**V. Phát hiện bất thường trong mạng không dây** 30](#_Toc436906639)

[**1. WIDS (Wireless Instrusion Detection System)** 31](#_Toc436906640)

[**2.** **IPS (Instruction Prevention System)** 34](#_Toc436906641)

[**VI. Tài liệu tham khảo** 36](#_Toc436906642)

**LỜI MỞ ĐẦU**

Ngày nay, cùng với sự bùng nổ thông tin thì sự phát triển của các phương tiện truyền tải thông tin liên lạc và nhu cầu cập nhật, trao đổi thông tin ở mọi lúc mọi nơi đang trở nên thiết yếu trong các hoạt động xã hội. Tuy nhiên, để có thể kết nối trao đổi thông tin người sử dụng phải truy nhập Internet từ một vị trí cố định. Điều này gây hạn chế khi người dùng không cố định hoặc ở những nơi không có điều kiện kết nối vào mạng. Do đó, để giải quyết vấn đề này, hệ thống mạng không dây đã được hình thành. Cùng với sự phát triển của mạng di động, mạng không dây thực sự là một bước đột phá trong lĩnh vực truyền thông.

Với nhiều lợi thế như dễ kết nối, tính cơ động cao, chi phí giá thành rẻ, có khả năng ứng dụng rộng rãi nên việc nghiên cứu mạng không dây là thực sự cần thiết. Vì vậy khi nghiên cứu và triển khai hệ thông mạng không dây, cần phải quan tâm đến các vấn đề bảo mật an toàn thông tin, bởi môi trường truyền dẫn của mạng không dây dễ bị rò rỉ dữ liệu, đặc biệt là nguy cơ tấn công của các hacker.

Trong quá trình tìm hiểu về đề tài mạng không dây, tuy chúng em đã rất cố gắng để hoàn thành báo cáo, nhưng không thể tránh những thiếu sót và hạn chế. Vì vậy, chúng em rất mong nhận được sự góp ý của thầy để bản báo cáo được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn.

Hà Nội, tháng 12 năm 2015.

**I. Giới Thiệu**

**1. Khái niệm**

Mạng không dây là một hệ thống mà ở đó các máy tính có thể nói chuyện, giao tiếp với nhau và cùng chia sẻ các nguồn tài nguyên như máy in hay các file dữ liệu mà không cần dùng dây cáp mạng. Hệ thống mạng không dây sử dụng môi trường truyền dẫn tần số radio-radio frequencies (RF). Tần số radio thường được sử dụng rất phổ biến vì băng thông rộng nên truyền tín hiệu đi rất xa, phủ sóng rộng hơn.

Công nghệ mạng không dây do tổ chức IEEE xây dựng và được tổ chức WiFi Alliance chính thức đưa vào sử dụng. Mạng không dây có tính năng, đặc trưng hoàn toàn giống như mạng cổ điển Ethernet, Token Ring, … Điểm nổi bật của hệ thống mạng không dây là không sử dụng cáp để kết nói hoặc ứng dụng tại nơi không thể thi công cáp. Hệ thống này sử dụng tần số Radio 2.4MHz để chuyển tải dữ liệu, do đó bạn dễ dàng nâng cấp, thay đổi tốc độ truyền thông không giống như hệ thống cổ điển như chôn cáp xuống đất, âm trong tường..

* *Phân loại*

Hệ thống mạng không dây chia thành 2 loại:

+ Mạng không dây trong nhà

+ Mạng không dây ngoài trời

* + *Ưu điểm*

Mạng không dây không dùng cáp cho các kết nối, chúng sử dụng sóng radio. Ưu thế của mạng không dây là khả năng di động và sự tự do, người dùng không bị hạn chế về không gian và vị trí kết nối. Các mạng máy tính không dây có ưu điểm về hiệu suất, sự thuận lợi, cụ thể như sau:

+ Tính di dộng

Người sử dụng laptop và người dùng di động có thể thay đổi vị trí mà vẫn luôn duy trì được kết nối mạng. Điều này cho phép họ có thể di chuyển từ địa điểm này sang địa điểm khác mà vẫn có thể truy cập vào dữ liệu mạng. Nếu không có mạng không dây, người dùng phải mạng theo cáp và bị hạn chế vì phải làm việc gần với các giác cắm cáp.

+ Tính đơn giản

Để kết nối mạng trong hai tòa nhà cao tầng được tách biệt bởi trở ngại về vật lý, bạn có thể tạo một liên kết không dây point-to-point bằng việc sử dụng công nghệ LAN không dây, có thể tiết kiệm một cách đáng kể chi phí cho tổ chức. Sử dụng mạng không dây linh hoạt hơn việc triển khai bằng các đường truyền cáp với kiểu nối mạng chạy dây Ethernet truyền thống, khi phải đục lỗ, kéo dây cáp qua các bức tường và trần nhà.

+ Tiết kiệm chi phí lâu dài

Trong khi vốn đầu tư cần thiết ban đầu đối với phần cứng của một mạng máy tính không dây (chi phí của các card mạng) có thể cao hơn chi phí phần cứng của một mạng hữu tuyến nhưng toàn bộ phí tổn lắp đặt và các chi phí về thời gian tồn tại có thể thấp hơn đáng kể. Mở rộng mạng lưới là rẻ hơn. Vì với mạng không dây, không cần chi phí cho vật liệu, lắp đặt và bảo trì. Chi phí dài hạn có lợi nhất trong các môi trường động cần phải di chuyển và thay đổi thường xuyên.

+ Khả năng vô hướng

Các mạng máy tính không dây có thể được cấu hình theo các topo khác nhau để đáp ứng các nhu cầu ứng dụng và lắp đặt có thể. Các cấu hình dễ dàng thay đổi từ các mạng ngang hàng thích hợp cho một số lượng nhỏ người sử dụng đến các mạng có cơ sở hạ tầng đầy đủ dành cho hàng nghìn người sử dụng mà có khả năng di chuyển trên một vùng rộng.

+ Dễ dàng truy cập tại các địa điểm Internet công cộng.

Các địa điểm công cộng như sân bay, khách sạn, nhà hàng,... Có thể cung cấp các loại hình dịch vụ không dây cho khách hàng, người dùng. Hay truy cập vào các trang của công ty có thể được thực hiện thông qua các mạng hot-spot không dây công cộng.

* + *Nhược điểm*

Do mạng không dây sử dụng truyền dẫn sóng radio nên chúng có thể bị gây nhiễu bởi các thiết bị như lò vi sóng, các mạng không dây khác khi có cũng tần số sóng. Mặt khác, khi truyền dữ liệu qua mạng không dây thì tính an toàn rất thấp, có thể bị nghe trộm, đánh cắp thông tin.

* + *Hoạt động*

Các mạng máy tính không dây sử dụng các sóng điện từ (vô tuyến hoặc ánh sáng) để truyền thông tin từ một điểm tới điểm khác. Các sóng vô tuyến thường được xem như các sóng mang vô tuyến do chúng chỉ thực hiện chức năng cung cấp năng lượng cho một máy thu ở xa. Dữ liệu đang được phát được điều chế trên sóng mang vô tuyến sao cho có thể được khôi phục chính xác tại máy thu.Các sóng vô tuyến được phát trên các tần số vô tuyến khác nhau. Để nhận lại dữ liêu, máy thu vô tuyến sẽ thu trên tần số vô tuyến của máy phát tương ứng.

Trong một cấu hình mạng máy tính không dây tiêu chuẩn, một thiết bị thu phát được gọi là một điểm truy cập, nối với mạng hữu tuyến từ một vị trí cố định sử dụng cáp tiêu chuẩn. Chức năng tối thiểu của điểm truy cập là thu, làm đệm, và phát dữ liệu giữa mạng máy tính không dây và cơ sở hạ tầng mạng hữu tuyến. Một điểm truy cập đơn có thể hỗ trợ một nhóm nhỏ người sử dụng và có thể thực hiện chức năng trong một phạm vi từ một trăm đến vài trăm mét.

Những người sử dụng truy cập vào mạng máy tính không dây thông qua các bộ thích ứng máy tính không dây như các Card mạng không dây trong vi máy tính, các máy Palm, PDA. Các bộ thích ứng máy tính không dây cung cấp một giao diện giữa hệ thông điều hành mạng (NOS-Network Operation System) của máy khách và các sóng không gian qua một anten. Bản chất của kết nối không dây là trong suốt đổi với hệ điều hành mạng.

## **2. Các dạng chuẩn**

Hiện nay, có 3 dạng chuẩn của mạng không dây : các chuẩn IEEE 802.11, HiperLAN và Bluetooth.

* 1. Các chuẩn IEEE 802.11
* *Giới thiệu về chuẩn IEEE 802.11*

Hiện nay, mạng không dây, cụ thể hơn là wireless LAN/MAN dùng các chuẩn dạng 802.11, ra đời 1997. Đây là chuẩn sơ khai của mạng không dây, nó mô tả cách truyền thông trong mạng không dây sử dụng các phương thức như DSSS (Direct Sequence Spread Spectrum), FHSS (Frequency Hopping Spread Specture) và Infrared (hồng ngoại). Tốc độ hoạt động từ 1-2 Mbps, hoạt động trong băng tần 2.4 GHz ISM.

Sau này chuẩn này còn được bổ sung thêm nhiều chuẩn dạng 802.11x. Tất cả những mạng trong chuẩn 802.x đều bao gồm các thành phần MAC và PHY:   
 - MAC: tập các quy tắc xác định giao thức truy cập môi trường và truyền nhận dữ liệu.

- PHY: chi tiết thông tin về giao thức truyền và nhận dữ liệu.

* *Nhóm lớp vật lý PHY*
  1. Chuẩn 802.11b

IEEE đã mở rộng trên chuẩn 802.11 gốc vào 7/1999, đó chính là chuẩn 802.11b. Chuẩn này tăng băng thông lên 11 Mbs, tương quan với Ethernet truyền thống. 802.11b sử dụng tần số vô tuyến (2.4 GHz) giống như chuẩn ban đầu. Các hãng thích sử dụng các tần số này để giảm chi phí trong sản xuất. Các thiết bị 802.11b có thể bị xuyên nhiễu từ các thiết bị điện thoại không dây, lò vi sóng hoặc các thiết bị khác dử dụng cùng dải tần.

* *Ưu điểm*: giá thành thấp nhất, phạm vi tín hiệu tốt và không dễ bị cản trở.
* *Nhược điểm*: tốc độ tối da thấp, các ứng dụng gia đình có thể bị xuyên nhiễu.
  1. Chuẩn 802.11a

Trong khi 802.11b vẫn đang được phát triển, IEEE đã tạo mở rộng thứ cấp cho chuẩn 802.11 có tên gọi 802.11a. 802.11a và 802.11b được tạo một cách đồng thời. Do giá thành cao hơn nên 802.11a chỉ được sử dụng trong các mạng doanh nghiệp còn 802.11b thích hợp với thị trường mạng gia đình.

802.11a hỗ trợ băng thông lên đến 54 Mbps và sử dụng tần số vô tuyến 5GHz nên nó sẽ không giao tiếp được với chuẩn 802.11 và 802.11b. Tần số của 802.11a cao hơn so với 802.11b chính vì vậy đã làm cho phạm vi của hệ thống này hẹp hơn so với các mạng 802.11b. Với tần số này, các tín hiệu 802.11a cũng khó xuyên qua các vách tường và các vật cản khác hơn. Do 802.11a và 802.11b sử dụng các tần số khác nhau, nên hai công nghệ này không thể tương thích với nhau.

* *Ưu điểm*: tốc độ cao, tần số 5GHz tránh được sự xuyên nhiễu từ các thiết bị khác.
* *Nhược điểm*: giá thành đắt, phạm vi hẹp và dễ bị che khuất.
  1. Chuẩn 802.11g

Vào năm 2002 và 2003, các sản phẩm WLAN hỗ trợ một chuẩn mới hơn đó là 802.11g, được đánh giá cao trên thị trường. 802.11g thực hiện sự kết hợp tốt nhất giữa 802.11a và 802.11b. Nó hỗ trợ băng thông lên đến 54Mbps và sử dụng tần số 2.4 GHz để có phạm vi rộng. 802.11g có khả năng thương thích với các chuẩn 802.11b.

* *Ưu điểm*: tốc độ cao, phạm vi tín hiệu tốt và ít bị che khuất.
* *Nhựơc điểm*: giá thành đắt hơn 802.11b, các thiết bị có thể bị xuyên nhiễu từ nhiều thiết bị khác sử dụng cùng băng tần.
  1. Chuẩn 802.11n

802.11n là chuẩn được thiết kế để cải thiện cho 802.11g.Khi chuẩn này được đưa ra, các kết nối 802.11n sẽ hỗ trợ tốc độ dữ liệu lên đến 100 Mbps. 802.11n cũng cung cấp phạm vi bao phủ tốt hơn nhờ cường độ tín hiệu mạnh của nó. Thiết bị 802.11n sẽ tương thích với các thiết bị 802.11g.

* *Ưu điểm*: Tốc độ vừa phải và vấn đề về khả năng tương thích là những đặc điểm được tìm thấy trong các sản phẩm dự thảo 802.11n. 802.11n ứng dụng công nghệ “channel bonding”, bằng cách kết hợp hai kênh 20MHz liền nhau thành một kênh 40MHz. Tuy nhiên, “channel bonding” có thể gây nhiễu cho hai “láng giềng” chuẩn 802.11b và 802.11g, bởi nó sẽ lấy toàn bộ dải phổ 2.4GHz mà các sản phẩm chuẩn này đang sử dụng. Mặt khác, để tránh tình trạng “quá tải”, 802.11n hỗ trợ cả hai tần số 2.4GHz và 5GHz.
* *Nhược điểm*: chuẩn 802.11n chưa an toàn cho người dùng. Trước hết là lỗ hổng trong hệ thống phát hiện xâm nhập trên mạng không dây (WIDS). Nếu dùng cách truyền dữ liệu qua các kênh 40 MHz, hệ thống WIDS sẽ mất gấp đôi thời gian quét tần số để phát hiện ra các dấu hiệu nguy hiểm, so với kênh 20MHz trước đây. Điều này sẽ khiến hacker mất gấp đôi thời gian để tham nhập vào một tần số cho trước đến khi máy quét dò đến tần số đó lần nữa (4-8s). Nhưng giữa khoảng thời gian đó, hacker sẽ lặp lại các đợt tấn công chứ không chỉ thử một lần rồi thôi. Như vậy, thời gian quét dài nghĩa là nguy hiểm lớn hơn. Kẻ tấn công cũng có thể khai thác trình điều khiển (driver) để chiếm quyền truy cập hệ thống quản lý. Hiện nay chuẩn 802.11n cũng chưa có lá chắn nào để chặn đồng ý truy cập (ACK). Nó có cơ chế chấp nhận một bó gói tin thay vì các gói tin riêng lẻ được xác định bởi một nhận dạng đầu và cuối. Dù vậy, cơ chế này không được bảo vệ và bất kì kẻ tấn công nào cũng có thể chèn vào đó một gói tin lừa và tạo ra một cửa sổ lớn gồm những cấu trúc được gửi đi mà không cần ACK. Như vậy 802.11b có thể bị tấn công từ chối dịch vụ DDOS.
* *Nhóm lớp liên kết dữ liệu MAC*

1. Chuẩn 802.11d

Chuẩn này chỉnh sửa lớp MAC của 802.11 cho phép máy trạm sử dụng FHSS có thể tối ưu các tham số vật lý để tuân tho các quy tắc của các nước khác nhau mà nơi đó được sử dụng.

1. Chuẩn 802.11r

Mở rộng của IEEE 802.11d, cho phép nâng cấp khả năng chuyển vùng.

1. Chuẩn 802.11e

Đây là chuẩn bổ sung cho chuẩn 802.11 cũ, nó định nghĩa thêm các mở rộng về chất lượng dịch vụ (QoS) nên rất thích hợp cho các ứng dụng đa phương tiện như voice, video. Chuẩn 802.11e cho phép phân các mức độ ưu tiên lưu thông để các dữ liệu cần thời gian thực (như các luồng tín hiệu hình hay cuộc gọi VoIP) sẽ được truyền trước các dữ liệu kém quan trọng hơn (như e-mail hoặc trang web).

1. Chuẩn 802.11f

Được phê duyệt năm 2003, đây là chuẩn định nghĩa các AP giao tiếp với nhau khi một client roaming từ vùng này sang vùng khác. Chuẩn này còn được gọi là Inter-AP Protocol (IAPP). Chuẩn này cho phép một AP có thể phát hiện được sự hiện diện của các AP khác cũng như cho phép AP “chuyển giao” client sang AP mới, điều này giúp cho quá trình roaming được thực hiện một cách thông suốt.

1. Chuẩn 802.11h

Hiện đang được sử dụng tại châu Âu, đây là khu vực mà quy định tần số radio đòi hỏi các sản phẩm phải có hệ thống TPC (Transmission Power Protocol) và DFS (Dynamic Frequency Selection). TCP giới hạn anwng lượng được truyền tải tới mức tối thiểu cần thiết để vươn tới người dùng xa nhất. DFS lựa chọn kênh dẫn radio tại điểm truy nhập nhằm hạn chế tối thiểu nhiễu với các hệ thống khác, đặc biệt là ra-đa. Tại một số khu vực trên thế giới, đa phần tần số 5GHz được dành cho chính phủ và quân đội sử dụng.

1. Chuẩn 802.11i

Là một chuẩn về bảo mật, nó bổ sung cho các yếu điểm của WEP trong chuẩn 802.11. Chuẩn này sử dụng giao thức như giao thức xác thực dựa trên cổng 802.1X, và một thuật toán mã hóa được xem như là không thể crack được đó lad thuật toán AES (Advance Encryption Standard), thuật toán này sẽ thay thế cho thuật toán RC4 được sử dụng WEP.

* 1. HiperLAN

HiperLAN (High Performance Radio LAN) là dạng chuẩn của ETSI (European Telecommunications Standard Institute) và là đối thủ cạnh tranh của IEEE 802.11. Nó chia hai loại:

* HiperLAN 1: sử dụng băng tần 5GHz và cung cấp tốc độ dữ liệu từ 10-20 Mbps.
* HiperLAN 2: sử dụng băng tần 5 GHz và cung cấp tốc độ dữ liệu lên đến 54 Mbps.
  1. Bluetooth

Bluetooth là 1 dạng chuẩn được thiết kế bởi nhiều công ty như Agere, Ericson. IBM, Intel, Microsoft, Motorola, Nokia, Toshiba. Bluetooth hoạt động với băng tần 2.4 GHz, sử dụng FHSS và có khoảng hoạt động với bán kính 10m. Đối với đặc điểm này và sử dụng chi phí thấp, bluetooth là thích hợp với các mạng cá nhân không dây (WPANs) và cũng được sử dụng để kết nối các thiết bị ngoại vi như bàn phím, máy in, tai nghe điện thoại. Công nghệ sóng vô tuyến bluetooth hoạt động theo mô hình master-slaver. Mỗi thiết bị có thể hoạt động như một master hoặc một slaver.

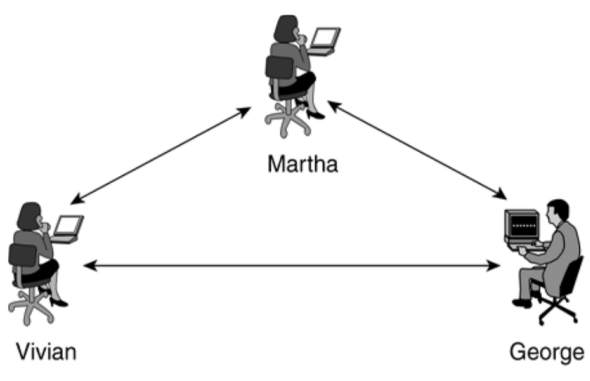
## **3. Mô hình**

Mạng không dây có thiết kế rất linh hoạt, gồm 3 mô hình mạng sau:

* Mô hình mạng độc lập AD-HOC (hoặc Independent Basic Service Sets-IBSS).
* Mô hình mạng cơ sở BSSs.
* Mô hình mạng mở rộng ESSs.

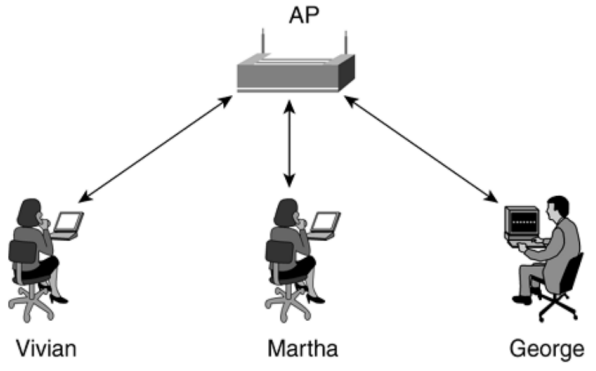
### 3.1 Mô hình mạng Ad-hoc

Các nút di động (máy tính có hỗ trợ card mạng không dây) tập trung lại trong một không gian nhỏ để hình thành nên kết nối ngang cấp (peer to peer) giữa chúng. Các nút di động có card mạng wireless là chúng có thể trao đổi thông tin trực tiếp với nhau, không cần phải quản trị mạng. Vì các mạng Ad-hoc này có thể thực hiện nhanh và dễ dàng nên chúng thường được thiết lập mà không cần một công cụ hay kĩ năng đặc biệt nào. Vì vậy nó rất thích hợp để sử dụng trong các hội nghị thương mại hoặc trong các nhóm làm việc tạm thời. Tuy nhiên chúng có thể có những nhược điểm về vùng phủ sóng bị giới hạn, mọi người sử dụng đều phải nghe được lẫn nhau.

  
Hình 1.1: Mô hình mạng Ad-hoc

### 3.2 Mô hình mạng cơ sở Basic Service Set (BSS)

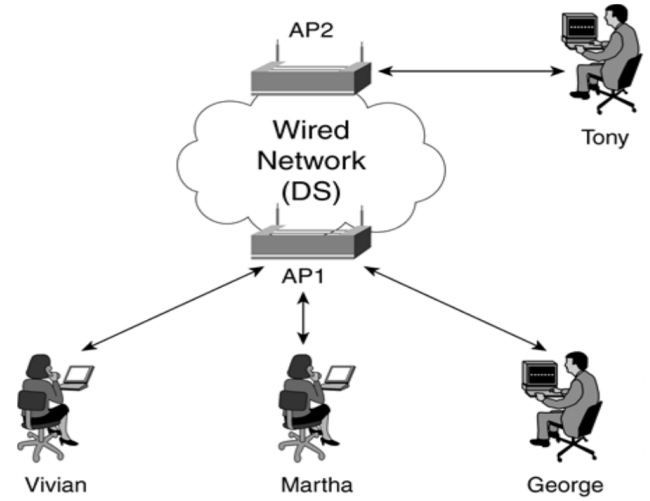
Bao gồm các điểm truy nhập AP (Access Point) gắn với mạng đường trục hữu tuyến và giao tiếp với các thiết bị di động trong vùng phủ sóng của một cell. AP đóng vai trò điều khiển cell và điều khiển lưu lượng tới mạng. Các thiết bị di động không giao tiếp trực tiếp với nhau mà giao tiếp với các AP. Các cell có thể chồng lấn lên nhau khoảng 10-15% cho phép các trạm di động có thể di chuyển mà không bị mất kết nối vô tuyến và cung cấp vùng phủ sóng với chi phí thấp nhất. Các trạm di động sẽ chọn AP tốt nhất để kết nối. Một điểm truy nhập nằm ở trung tâm có thể điều khiển và phân phối truy cập cho các nút tranh chấp, cung cấp truy nhập phù hợp với mạng đường trục, ấn định các địa chỉ và các mức ưu tiên, giám sát lưu lượng mạng, quản lý chuyển đi các gói và duy trì theo dõi cấu hình mạng. Tuy nhiên giao thức đa truy nhập tập trung không cho phép các nút di động truyền trực tiếp tới các nút khác nằm trong cùng vùng với điểm truy nhập. Trong trường hợp này, mỗi gói sẽ phải được phát đi 2 lần (từ nút gốc và sau đó là điểm truy nhập) trước khi nó tới đích, quá trình này sẽ làm giảm hiệu quả truyền dẫn và tăng trễ truyền dẫn.



Hình 1.2: Mô hình mạng BSS

### 3.3 Mô hình mạng mở rộng Extended Service Set (ESS)

Mạng 802.11 mở rộng phạm vi di động tới một phạm vi bất kì thông qua ESS. Một ESS là một tập hợp các BSS nơi mà các AP giao tiếp với nhau để chuyển lưu lượng từ một BSS này đến BSS khác để làm cho việc di chuyển dễ dàng của các trạm giữa các BSS, AP thực hiện việc giao tiếp thông qua hệ thống phân phối. Hệ thống phân phối là một lớp mỏng trong mỗi AP mà nó xác định đích đến cho một lưu lượng nhận được từ một BSS. Hệ thống phân phối được tiếp sóng trở lại một đích trong cùng một BSS, chuyển tiếp trên hệ thống phân phối tới một AP khác, hoặc gửi tới một mạng có dây tới đích không nằm trong ESS. Các thông tin nhận bởi AP từ một hệ thống phân phối được truyền tới BSS sẽ được nhận bởi trạm đích.



Hinh 3: Mo hinh mang ESS

## **4. Các thành phần trong mạng không dây**

* *Stations* (các máy trạm)

Các mạng được xây dựng để truyền dữ liệu giữa các trạm, station là các thiết bị tính toán có giao tiếp mạng không dây. Điển hình như các máy tính để bàn hay máy tính cá nhân sử dụng pin. Trong một số môi trường, mạng không dây được sử dụng nhằm tránh phải kéo cáp mới và các máy bàn được kết nối với mạng LAN không dây. Những khu vực lớn hơn cũng có lợi khi sử dụng mạng không dây như xưởng sản xuất sử dụng mạng cục bộ không dây để kết nối các bộ phận 802.11 nhanh chóng trở thành chuẩn thực tế để liên kết những người sử dụng thiết bị điện tử với nhau.

* *Access Point* (các điểm truy cập)

Các khung dữ liệu trên mạng 802.11 phải được chuyển thành dạng khung dữ liệu khác để phân phối trong các mạng khác. Thiết bị được gọi là điểm truy cập thể hiện các chức năng chuyển đổi từ không dây sang có dây (AP bao gồm nhiều chức năng khác nhau, nhưng thực hiện chuyển đổi là chức năng quan trọng nhất). Các chức năng điểm truy cập được đặt tại những thiết bị độc lập. Tuy nhiên, nhiều sản phẩm mới hơn tích hợp các giao thức 802.11 vào hai loại AP cấp thấp và bộ điều khiển AP.

* *Wireless Medium* (Môi trường không dây)

Để chuyển các khung dữ liệu từ trạm này sang trạm khác trong môi trường không dây, người ta xây dựng nhiều chuẩn vật lý khác nhau. Nhiều lớp vật lý được phát triển để hỗ trợ 802.11 MAC, lớp vật lý vô tuyến và lớp vật lý hồng ngoại được chuẩn hóa.

* *Distribution System* (Hệ thống phân tán)

Khi các điểm truy cập được kết nối với nhau trong một khu vực, chúng phải liên lạc với nhau để kiểm soát quá trình di chuyển của các thiết bị di động. Hệ thống phân tán là một thành phần logic của 802.11 được dùng để chuyển các khung dữ liệu đến đích, bao gồm các phần tử chuyển đổi và môi trường hoạt động phân tán, chính là mạng đường trục được dùng để chuyển tiếp khung dữ liệu giữa các điểm truy cập.

## **5. Hoạt động của mạng không dây**

* *Nguyên tắc hoạt động của Wireless Access Point*

Chức năng cơ bản của một AP là làm cầu nối (bridge) cho những dữ liệu mạng không dây từ không khí (môi trường sóng vô tuyến) vào mạng có dây bình thường. Một AP có thể chấp nhận những kết nối từ một số các máy trạm không dây sao cho nó có thể trở thành các thành viên bình thường của một mạng LAN dùng dây.

Một AP cũng có thể hoạt động như một cầu nối để hình thành kết nối không dây giữa một mạng LAN này và một mạng LAN khác trên khoảng cách xa. Trong tình huống đó, ở mỗi đầu của kết nối không dây cần một AP. Kiểu kết nối này gọi là AP-to-AP hoặc kết nối line-of-sight, thường được dùng để kết nối giữa các tòa nhà.

Cisco cũng đã phát triển một loại AP có thể làm cầu nối cho các loại lưu lượng trong mạng không dây từ AP này sang AP khác theo kiểu một chuỗi các cầu nối. Kiểu kết nối này cho phép một vùng không gian rộng lớn có thể được bao phủ bởi mạng không dây. Các AP lúc này sẽ hình thành nên sơ đồ mess, rất giống với mô hình ESS, trong đó các AP kết nối liên hoàn với nhau thông qua các kết nối không dây khác.

AP hoạt động như một điểm truy cập trung tâm, kiểm soát các truy cập từ các máy trạm. Bất kì máy trạm nào khi cố gắng dùng WLAN thì trước hết phải thiết lập một kết nối với một AP. AP có thể cho phép kết nối theo dạng mở sao cho bất kì máy trạm nào cũng có thể kết hợp, hoặc có thể kiểm soát chặt chẽ hơn bằng cách yêu cầu xác thực, hoặc có thể dùng các tiêu chuẩn khác trước khi cho phép kết hợp.

Hoạt động của WLAN thì liên quan chặt chẽ đến quá trình phản hồi từ đầu bên kia của kết nối không dây. Ví dụ, các máy trạm phải bắt tay với AP trước khi nó có thể kết nối và sử dụng mạng không dây. Ở mức độ cơ bản nhất, yêu cầu này đảm bảo một kết nối hai chiều bởi vì cả máy trạm và AP đều có khả năng truyền và nhận frame thành công. Tiến trình này sẽ loại bỏ khả năng truyền thông một chiều, khi máy trạm có thể nghe AP nhưng AP thì không thể nghe máy trạm. Ngoài ra, AP có thể kiểm soát nhiều khía cạnh của phạm vi không dây của nó bằng cách yêu cầu một số điều kiện phải được đáp ứng điều kiện trước khi máy trạm có thể kết nối vào.

* *Các frame trong mạng không dây*

Các frame wireless có thể thay đổi kích thước. Khi một frame được truyền, làm thế nào để các máy khác biết là frame đã được truyền hoàn tất và đường truyền là rảnh cho các máy khác sử dụng? Chuẩn 802.11 yêu cầu tất cả các máy trạm phải chờ một khoảng thời gian. Khoảng thời gian này được gọi là khoảng thời gian giữa các frame DCF (DCF interframe space). Sau khoảng thời gian này, các máy trạm mới có thể truyền.

Bên máy truyền có thể chỉ ra một khoảng thời gian dự kiến để gửi đi hết một frame bằng cách chỉ ra trong một trường của frame 802.11. Khoảng thời gian này chứa số timeslot cần thiết để truyền frame. Các máy trạm khác phải xem giá trị chứa trong header này và phải chờ khoảng thời gian đó trước khi truyền cho chính nó.Bởi vì tất cả các máy trạm phải chờ cùng một khoảng thời gian chỉ ra trong một frame, tất cả các máy đó có thể sẽ quyết định cùng truyền khi khoảng thời gian đó trôi qua. Điều này có thể dẫn đến hiện tượng xung đột, chính là một hiện tượng cần tránh.

Bên cạnh thông số thời gian nêu trên, các trạm không dây cũng phải triển khai một bộ định thời ngẫu nhiên. Trước khi truyền một frame, máy tính đó phải chọn một số ngẫu nhiên timeslot phải chờ. Con số này sẽ nằm trong khoảng từ 0 đến kích thước tối đa của sổ cạnh tranh. Ý tưởng cơ bản của cách làm này là khi một máy truyền, mỗi máy sẽ chờ một khoảng thời gian ngẫu nhiên, giảm số trạm cố gắng truyền đồng thời cùng lúc.

Toàn bộ tiến trình này được gọi là chức năng phối hợp phân phối. Chức năng này được mô tả như dưới đây. Ba người dùng mạng không dây có cùng một frame phải truyền ở các khoảng thời gian khác nhau. Một chuỗi các sự kiện sau sẽ xảy ra:

* Người dùng A lắng nghe và xác định rằng không có người dùng nào khác đang truyền. người dùng A truyền frame của nó, đồng thời quảng bá khoảng thời gian để truyền frame
* Người dùng B cũng có frame để truyền. Nó phải chờ cho đến khi nào frame của người dùng A là hoàn tất, sau đó phải chờ hết khoảng thời gian DIFS (thời gian phối hợp phân phối) hoàn tất.
* Người dùng B phải chờ một khoảng thời gian ngẫu nhiên trước khi cố gắng truyền.
* Khi người dùng B đang chờ, người dùng C có frame phải truyền. Anh ta lắng nghe và phát hiện rằng không có ai đang truyền. Người dùng C phải chờ một khoảng thời gian ngẫu nhiên. Khoảng thời gian này là ngắn hơn khoảng thời gian ngẫu nhiên của người dùng B.
* Người dùng C truyền frame và quảng bá thời gian để truyền.
* Người dùng B phải chờ khoảng thời gian truyền frame của người dùng C cộng với thời gian giữa các frame DIFS trước khi cố gắng truyền lại một lần nữa.

# **III. Các dạng tấn công từ chối dịch vụ mạng không dây**

## **1. Định nghĩa**

Một cuộc tấn công từ chối dịch vụ (Denial of Service) hay tấn công từ chối dịch vụ phân tán (Distributed Denial of Service) là một nỗ lực làm cho những người dùng không thể sử dụng tài nguyên của một máy tính. Mặc dù phương tiện để tiến hành, động cơ, mục tiêu của tấn công từ chối dịch vụ có thể khác nhau, nhưng nói chung nó gồm có sự phối hợp, sự cố gắng ác ý của một người hay nhiều người để một trang, hay hệ thống mạng không thể sử dụng, làm gián đoạn, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống. Thủ phạm tấn công từ chối dịch vụ thường nhắm vào các trang mạng hay server tiêu biểu như ngân hàng, cổng thanh toán thẻ tín dụng và thậm chí DNS roots server

**2. Nguyên nhân**

Hai lý do chính khiến mạng Wireless dễ bị tấn công từ chối dịch vụ đó là:

* Không có các ranh giớ vật lý như các mạng không dây: sóng radio dùng để truyền dữ liệu có thể có mặt ở khắp mọi nơi và đến từ mọi nơi. Điều này làm cho các tin tặc có thể dễ dàng bắt tín hiệu, nắm bắt thông tin để chiếm quyền điều khiển hệ thống. Ngoài ra tin tặc có thể sử dụng các thiết bị gây nhiễu làm ảnh hưởng đến khả năng truyền tải của mạng không dây.
* Thiếu cơ chế chững thực các gói tin quản lý: giao thức 802.11 quản lý truy cập bằng các gói tin quản lý, trong khi đó lại thiếu cơ chế chứng thực các gói tin này. Như vậy tin tặc có thể mạo danh các Access Point hay các máy chạm để can thiệp vào quá trình quản lý truy cập, hủy các kết nối hiện hành hoặc ngăn các kết nối mới vào hệ thống.

**3. Các dạng tấn công từ chối dịch vụ mạng không dây**

3.1. Tấn công Access Point overloading

Đây là loại tấn công vào khả năng của các thiết bị, cụ thể là các Access Point. Các Access Point của mạng không dây chuẩn 802.11 chỉ có thể xử lý thông tin truyền trước khi bộ nhớ của chúng bị đầy hoặc CPU quá tải. Các tin tặc có thể khai thác điểm yếu trong các Access Point xếp vào hàng đợi các yêu cầu từ máy trạm trong bảng client association identifier (AID) – phần bộ nhớ lưu trữ thông tin kết nối của máy trạm. Bảng ADI có kích thước bộ nhớ hữu hạn và một khi nó đây thì Access Point sẽ không chấp nhận các yêu cầu kết nối từ các máy trạm nữa, hoặc Access Point sẽ bị treo.

Hiện nay vẫn chưa có giải pháp nào chống lại được các dạng tấn công này. Chúng ta chỉ có thể hạn chế phần nào bằng cách sử dụng hạn chế độ chứng thực chia sẻ khóa (WPA, WPA2) thay thế cho chế độ chứng thực mở (Open)

a. Access Point được cấu hình không hoàn chỉnh

Một Access Point có thể bât ngờ trở thành một thiết bị giả mạo do sai sót trong việc cấu hình. Sự thay đổi trong SSID, thiết lập xác thực, thiết lập mã hóa… điều nghiêm trọng nhất là sẽ không thể chứng thực các kết nối nếu bị cấu hình sai.

Ví dụ: trong trạng thái xác thực mở các ngời dùng không dây ở trạng thái 1 (chưa xác thực và chưa kết nối) có thể gửi các yêu cầu xác thực đến một Access Point và được xác thực thành công sẽ chuyển sang trạng thái 2 (được xác thực nhưng chưa kết nối). Nếu 1 Access point không xác nhận sự hợp lệ của một máy khách do lỗi trong cấu hình, kẻ tấn công có thể gửi đến một số lượng lớn yêu cầu xác thực, làm tràn bảng yêu cầu kết nối của các máy tính khách ở Access point, làm cho Access point từ chối truy cập của người dùng khác bao gồm cả người dùng được phép truy cập.

b. Access Point giả mạo từ các mạng Wireless lân cận

Các thiết bị chuẩn 802.11 tự dộng chọn Access point có sóng mạnh nhất mà nó phát hiện được để kết nối.

Ví dụ: Windows XP tự động kết nối đến kết nối tốt nhất có thể xung quanh nó. Vì vậy những người dùng được xác thực của 1 tổ chức có thể kết nối đến các Access point của các tổ chức khác lân cận. Mặc dù các Access point lân cận không cố ý thu hút các kết nối từ các người dùng, những kết nối đó có thể vô tình để lộ thông tin.

c. Access Point giả mạo do kẻ tấn công tạo ra

Giả mạo Access point là kiểu tấn công “man in the middle” cổ điển. Đây là kiểu tấn công mà tin tặc đứng ở giữa và trộm lưu lượng truyền giữa hai nút. Kiểu tấn công này rất mạnh vì tin tặc có thể trộm vả lưu lượng đi qua mạng.

Trông mạng dây, rất khó khăn tạo một cuộc tấn công “man in the middle nhưng trong mạng không dây thì lại rất dễ dàng. Tin tặc tạo ra một Access point thu hút nhiều lựa chọn hơn Access point chính thống, Access point giả này có thể thiết lập bằng cách sao chép tất cả cấu hình của Access point chính thống: SSID, địa chỉ MAC... bước tiếp là làm cho đối tượng nạn nhân thực hiện kết nối tới Access point giả.

* Cách thứ nhất là đợi cho người dùng tự kết nối
* Cách thứ hai là gây ra một cuộc tấn công từ chối dịch vụ DoS trong Access point chính thống do vậy người dùng sẽ phả kết nối lại với Access point giả

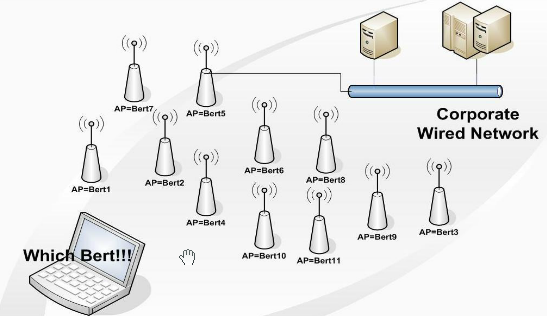
Trong mạng 802.11 sự lựa chọn được thực hiện bởi cường độ tín hiệu nhận. Điều duy nhất tin tặc phải thực hiện là chắc chắn rằng Access point giả có cường độ tín hiệu mạnh hơn cả bằng cách đặt Access point giả gần người sử dụng hơn là Access chính thống hoặc sử dụng kỹ thuật anten định hướng. Vì vậy sau khi kết nối với Access point giả, nạn nhân vẫn hoạt động như bình thường nhưng kho kết nối với Access chính thống, mọi dữ liệu sẽ đi qua Access point giả mạo.

d. Access Point giả mạo được thiết lập bởi chính nhân viên của tổ chức

Vì sự tiện lợi của mạng không dây, một số nhân viên trong tổ chức đã tự trang bị Access point và kết nối chúng vào mạng có dây của tổ chức. Do không hiểu rõ về bảo mật trong mạng không dây nên họ vô tình tạo ra một lỗ hổng lớn về bảo mật. Những người ngoài tổ chức hoặc hacker có thể kết nối đến Access point không xác thực để đánh cắ băng thông, thông tin mật của tổ chức, sử dụng mạng của tổ chức để tấn công người khác…

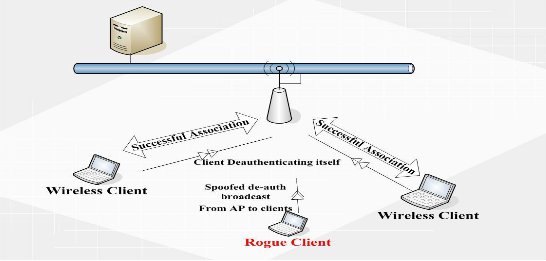
e. Fake Access point

Kẻ tấn công sử dụng công cụ có khả năng gửi các gói beacon với các địa chỉ vật lý MAC giả mạo và SSID giả để tạo ra vô số Access point gả lập. Điều này làm xáo trộn tất cả các phần mềm điều khiển card mạng không dây của người dùng.



Hình 3.1: Fake Access Point

3.2. Tấn công yêu cầu xác thực lại – De-authentication Flood Attack



Hình 3.2: Mô hình tấn công yêu cầu xác thực lại

* Kẻ tấn công xác định mục tiêu tấn công là các người dùng trong wireless và các kết nối của họ (Access point đến các các kết nối của nó)
* Chèn các frame yêu cầu xác thực tại vào mạng Wireless bằng cách giả mạo địa chỉ MAC nguồn và đích lần lượt của Access Point và các người dùng
* Người dùng wireless khi nhận được frame yêu cầu xác thực lại thì nghĩ rằng chúng do Access Point gửi đến
* Sau khi ngắt được một ngwoiwif dùng ra khỏi dịch vụ không dây, kẻ tấn công tiếp tục thực hiện tương tự đối với các người dùng còn lại
* Thông thường người dùng sẽ kết nối lại để phục hồi dịch vụ, kẻ tấn công đã nhanh chóng tiếp tục gửi lại các gói yêu cầu xác thực lại cho người 3

3.3. Tấn công dựa trên cảm nhận sóng mang lớp vật lý – Gây nhiễu

Kẻ tấn công lợi dụng giao thức chống đụng độ CSMA/CA, tức là nó sẽ làm cho tất cả người dùng nghĩ rằng lúc nào trong mạng cũng có một máy tính đang truyền thông. Điều này làm cho các máy tính khác luôn luôn ở trạng thái chờ đợi kẻ tấn công ấy truyền dữ liệu xong, dẫn đến tình trạng nghẽn trong mạng.

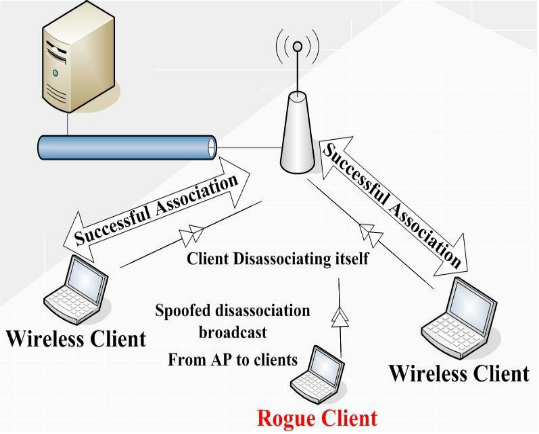
Tần số là một nhược điểm bảo mật trong mạng không dây. Mức độ nguy hiểm thay đổi phụ thuộc vào giao diện của lớp vật lý. Có một vài tham số quyết định sự chịu đựngcủa mạng là năng lượng máy phát, độ nhạy của máy thu, tần số RF, băng thông và sự định hướng của anten. Trong mạng 802.11 sử dụng thuật toán đa truy nhập cảm nhận sóng mang (CSMA) để tránh va chạm. CSMA là một thành phần của lớp MAC. CSMA được sử dụng để chắc chắn rằng sẽ không có va chạm dữ liệu trên đường truyền. Kiểu tấn công này không sử dụng tạp âm để tạo ra lỗi cho mạn nhưng sẽ lợi dụng chính chuẩn đó.

Có nhiều cách khai thác giao thức cảm nhận sóng mang vật lý. Cách đơn giản là làm cho các nút trong mạng đều tin tưởng rằng có một nút đang truyền dữ liệu tại thời điểm hiện tại. Cách dễ nhất đạt được điều này là tạo ra một nút giả mạo để truyền tin một cách liên tục. Một chác khác là sử dụng bộ tạo tín hiệu RF. Một cách tấn công tinh vi hơn là làm cho card mạng chuyển vào chế độ liểm tra mà ở đó nó truyền đi liên tiếp một mấu kiểm tra. Tất cả các nút trong phạm vi của một nút giả là rất nhạy với sóng mạng và trong khi đó có một nút đang truyền thì sẽ không có nút nào được truyền.

Hiện nay chống lại việc gây nhiễu là điều còn hạn chế. Chúng ta chỉ có thể kiểm tra hệ thống có bị nhiễu hay không bằng các công cụ, ví dụ như NetSumber.

3.4. Tấn công ngắt kết nối – Disassociation flood attack

Đối với chuẩn IEEE 802.11 hiện hành, khi một máy trạm muốn rời khỏ mạng Wireless, nó gửi một gói de-authentication hoặc disassociation đến Access Point. Tuy nhiên hai gói tin này không được mã hóa và không được Access Point chứng thực. Do đó kẻ tấn công có thể làm giả hai gói tin này xuất phát từ máy trạm hoặc Access Point (bằng cách giả mạo địa chỉ MAC, BSSID) trong hệ thống để đứt các kết nối. Đây là loại hình tấn công nhằm vào điểm yếu của giao thức 802.11. Dạng tấn công này đặc biệt nguy hiểm vì nó có thể dễ dàng ngắt toàn bộ kết nối trong mạng Wireless.



Hình 3.3: Mô hình tấn công ngắt kết nối

* Kẻ tấn công xác định mục tiêu (wireless clients) và mối liên kết giữa các Access Point với các clients
* Kẻ tấn công gửi disassociation frame bằng cách giả mạo Source và Destination MAC đến Access Point và các client tương ứng
* Client sẽ nhận các frame này và nghĩ rằng frame hủy kết nối đến từ Access Point. Đồng thời kẻ tấn công cũng gởi disassoication frame đến Access Point.
* Sau khi đã ngắt kết nối của một client, kẻ tấn công tiếp tục thực hienj tương tự các client còn lại làm cho các client tự động ngắt kết nối với Access Point
* Khi các client bị ngắt kết nối sẽ thực hiện lại kết nối lại với Access Point ngay lập tức. Kẻ tấn công tiếp tục gửi disassociation frame đến Access Point và client

So sánh Disassociation flood attack và De-authentication Flood Attack

* Giống nhau: Về hình thức tấn công: cùng vừa tấn công Access Point vừa tấn công Client và đặc biệt là tấn công liên tục
* Khác nhau:
  + De-authentication Flood Attack: yêu cầu cả Access Point và client gửi lại frame xác thực
  + Disassociation flood attack: gửi disassociation frame làm cho Access và client tin tưởng rằng kết nối giữa chúng đã bị ngắt.

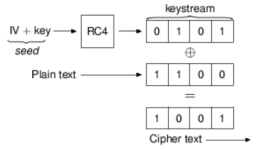
Giải pháp: với tiêu chí hiệu quả và ít tốn chi phí để triển khai trên các thiết bị 802.11 hiện có, giải pháp được đưa ra mang tên Letter Envelop Protocol. Giải pháp này đã được kiểm chứng thực nghiệm và trình bày tại hội nghị quốc tế về mạng máy tính và truyền thông ICCCN 2008. Vì là 1 phần mở rộng trên chuẩn 802.11 nên nó dễ dàng triển khai trên các thiết bị mạng không dây, giúp giảm bớt chi phí. Tuy nhiên giải pháp này chỉ giải quyết vấn đề tấn công từ chối dịch mà chưa đặt trong mối tương quan với các loại hình tấ công khác.

**IV. Xác thực và bảo mật trong mạng không dây**

**1. WEP**

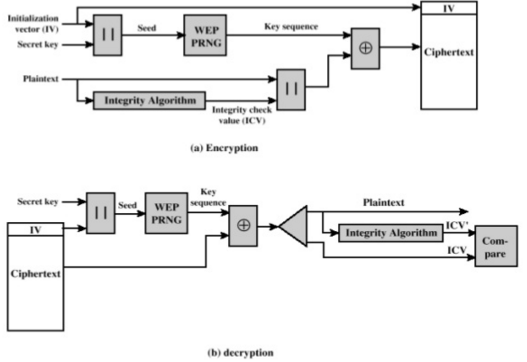
Là thuật toán bảo nhằm bảo vệ sự trao đổi thông tin chống lại sự nghe trộm và những kết nối mạng không được phép.

WEP sử dụng stream cipher RC4 cùng với mã 40bit và một số ngẫu nhiên 24 bit để mã hóa thông tin. Thông tin mã hóa được tạo ra bằng các XOR keystream và plain text. Thông tin mã hóa và IV sẽ dược gửi đến người nhận. Người nhận sẽ giải mã thông tin dựa vào IV và khóa WEP.



Chuẩn 802.11 yêu cầu WEP phải được cấu hình trên cả client và Access Point khớp với nhau thì chúng mới có thể truyền và giao tiếp được.

WEP mã hóa những phần trong phần dữ liệu và trường kiểm tra tính toàn vẹn của dữ liệu (Integrity Check value). Giá trị IV được truyền mà không cần mã hóa để cho trạm nhận sử dụng được nó để giải mã phần dữ liệu



Điểm yếu của WEP:

* Sử dụng khóa cố định để chia sẻ giữa một AP và nhiều người dùng với một IV ngẫu nhiên 24 bit.
* Dễ dàng bị tấn công nếu kẻ tấn công biết được khóa cố định.
* Cho phép user xác thực AP nhưng không cho AP xác thực user

**2. WLAN VPN**

Mạng riêng ảo VPN bảo vệ mạng WLAN bằng cách tạo ra một kênh che chắn dữ liệu khỏi các truy cập trái phép. VPN tạo ra một tin cậy cao thông qua việc sử dụng một cơ chế bảo mật như IPSec (Internet Protocol Security). IPSec dùng các thuật toán mạnh như Data Encryption Standard (DES) và Triple DES (3DES) để mã hóa dữ liệu, và dùng các thuật toán khác để xác thực gói dữ liệu. IPSec cũng sử dụng thẻ xác nhận số để xác nhận khóa mã (public key). Khi được sử dụng trên mạng WLAN, cổng kết nối VPN đảm nhạn việc xác thực, đóng gói và mã hóa.

**3. TKIP (Temporal Key Integrity Protocol)**

Là giải pháp của IEEE được phát triển năm 2004. Là một nâng cấp cho WEP nằm vá những vấn đề bảo mật trong cài đặt mã dòng RC4 trong WEP. TKIP dùng hàm băm(hashing) IV để chống lại việc giả mạo gói tin, nó cũng cung cấp phương thức để kiểm tra tính toàn vẹn của thông điệp MIC (message integrity check) để đảm bảo tính chính xác của gói tin. TKIP sử dụng khóa đọng bằng cách đặt cho mỗi frame một chuỗi số riêng chống lại dạng tấn công giả mạo.

**4. AES (Advanced Encryption Standard)**

Là một chức năng mã hóa được phê chuẩn bởi NIST (Nation Instutute of Standard and Technology). IEEE đã thiết kế một chế độ ASE để đáp ứng nhu cầu của mạng WLAN. Chế độ này được gọi là CBC-CTR (Cipher Block Chaning Counter Mode) với CBC-MAC (Cipher Block Chaning Message Authenticity Check). Tổ hợp của chúng được gọi là AES-CCM. Chế độ CCM là sự kết hợp của mã hóa CBC-CTR và thuật toán xác thực thông điệp CBC-MAC. Sự kết hợp này cung cấp cả việc mã hóa cũng như kiểm tra tính toàn vẹn của dữ liệu gửi.

a. Mã hóa CBC-CTR sử dụng một biến đếm để bổ sung cho chuỗi khóa. Biến đếm sẽ tăng lên 1 sau khi mã hóa cho mỗi khối. Tiến trình này đảm bảo chỉ có duy nhất một khóa cho mỗi khối. Chuỗi ký tự chưa được mã hóa sẽ được phân mảnh thành các khối 16 byte.

b. Mã hóa CBC-MAC hoạt động bằng cách sử dụng kết quả của mã hóa CBC cùng với chiều dài frame, địa chỉ nguồn, địa chỉ đích và dữ liệu. Kết quả sẽ cho ra giá trị 128bit và được cắt thành 64bit để sử dụng truyền thông.

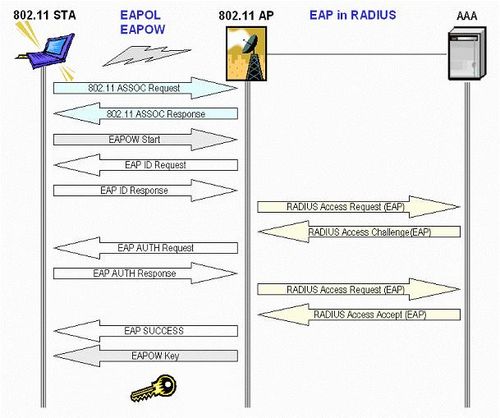
**5. 802.1x và EAP**

5.1. 802.1x

802.1x là chuẩn đặc ta cho việc truy cập dựa trên cổng (port-based) được định nghĩa IEEE. Hoạt động trên cả môi trường có dây truyền thống và không dây. Việc điều khiển truy cập được thực hiện bằng cách: Khi một người dùng cố gắng kết nối vào hệ thống mạng, kết nối của người dùng sẽ được đặt ở trạng thái bị chặn (blocking) và chờ cho việc kiểm tra định dạnh người dùng hoàn tất.

5.2. EAP

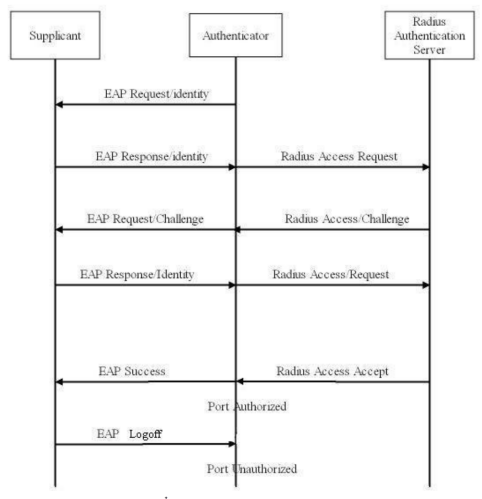
EAP là phương thức xác thực bao gồm yêu cầu định danh người dùng, giao thức được sử dụng và hỗ trợ tự động sinh khóa xác thực lần nhau.

Mô hình xác thực 802.1X-EAP cho Client diễn ra như sau 

**6. WPA**

WEP được xây dựng để bảo vệ một mạng không dây tránh bị nghe trộm. Nhưng nhanh chóng sau đó người ta phát hiện ra nhiều lỗ hổng ở công nghệ này. Do đó công nghệ mới có tên là WPA (Wifi Protected Access) ra đời, khắc phục được nhiều nhược điểm của WEP.

a. Các cải tiến của WPA

* WPA mã hóa thông tin bằng RC4 nhưng chiều dài của khóa là 128bit và IV có chiều dài là 48bit. Một cải tiến của WPA đối với WEP là WPA sử dụng giao thức TKIP nhằm thay đổi khóa dùng AP và user một cách tự động trong quá trình truyền tin. Cụ thể là TKIP dùng một khóa nhất thời 128bit kết hợp với địa chỉ MAC của user host và IV để tạo ra mã khóa. Mã khóa này sẽ được thay đổi sau khi 10000 gói thông tin được trao đổi.
* WPA sử dụng 802.1x/EAP để đảm bảo xác thực lẫn nhau nhằm chống lại tấn công giả mạo. Quá trình xác thực của WPA dựa trên một authentication server, còn được biết đến với tên gọi RADIUS/DIAMETER. Server RADIUS cho phép xác thực user trong mạng cũng như định nghĩa những quyền kết nối user. Tuy nhiên trong một mạng WiFi nhỏ, đôi khi không cần thiết phải đặt một server mà có thể dùng một phiên bản WPA-PSK. Ý tưởng của WPA-PSK là sẽ dùng một password chung cho AP và client devices. Thông tin xác thực giữa user và server sẽ được trao đổi thông qua giao thức EAP. EAP session sẽ được tạo ra giữa user và server để chuyển đổi thông tin liên quan đến identity của user cũng như của mạng. Trong quá trình này AP đóng vai trò là một EAP proxy, làm nhiệm vụ chuyển giao thông tin giữa server và user. Những thông điệp xác thực chuyển đổi được miêu tả như trong hình vẽ 

Ảnh 1 Thông điệp trao đổi trong quá trình xác thực

* WPA sử dụng MIC (Michael Message Integrity Check) để tăng cường integrity của thông tin truyền. MIC là một thông điệp 64 bit được dựa trên thuật toán Michael. MIC sẽ được gửi trong gói TKIP và giúp người nhan kiểm tra xem thông tin nhận được có bị lỗi trên đường truyền hoặc bị thay đổi bởi kẻ phá hoại hay không.

b. Điểm yếu của WPA

* Nó vẫn chưa giải quyết được kiểu tấn công từ chối dịch vụ. Kẻ phá hoại có thể làm nhiễu mạng WPA Wifi bằng cách gửi ít nhất 2 gói thông tin với một khóa sai mỗi giây. Trong trường hợp đó, AP sẽ cho rằng một kẻ phá hoại đang tấn công mạng và AP sẽ cắt tất cả các kết nối trong vòng một phút để tránh hao tổn tài nguyên mạng. Do đó, sự tiếp diễn của thông tin không được phép làm xáo trộn hoạt động của mạng và ngăn cản sự nối kết của những người dùng được phép.
* Do sử dụng thuật toán RC4 mà có thể bị bẻ vỡ bởi FMS attack để nghị bởi những nhà nghiên cứu ở trường đại học Berkeley. Hệ thống mã hóa RC4 chứa đựng những khóa yếu. Những khóa yếu này cho phép truy ra khóa encrytion. Để có thể tìm ra khóa yếu của RC4, chỉ cần thu thập một số lượng đủ thông tin trên kênh truyền không dây.
* WPA-PSK là một phiên bản yếu của WPA mà ở đó nó gặp vấn đề về quản lý password hoặc shared secret giữa nhiều người dùng. Khi một người trong nhóm rời nhóm, một password/secret mới cần phải được thiết lập

**7. WPA2**

Một giải pháp về lâu dài là sử dụng 802.11i tương đương WPA2, được chứng nhận bởi Wi-Fi Alliance. Chuẩn này sử dụng thuật toán mã hóa mạnh mẽ và được gọi là Chuẩn mã hóa nâng cao AES. AES sử dụng thuật toán mã hóa đổi xứng theo khối Rijndael, sử dụng khối mã khóa 128bit, và 192bit hoặc 256bit. Để đánh giá chuẩn mã hóa này, Viện nghiên cứu quốc qua về Chuẩn và Công nghệ của Mỹ NIST đã thông qua thuật toán mã đối xứng này.

Trong khi AES được xem như là bảo mật tốt hơn rất nhiều so với WEP 128bit hoặc 168bit DES. Để bảo đảm về mặt hiệu năng, quá trình mã hóa cần được thực hiện trong các thiết bị phần cứng như tích hợp vào chip. Tuy nhiên, hầu hết các thiết bị cầm tay Wifi và máy quét mã vạch đều không tương thích với chuẩn 802.11i

WPA2 cung cập cho các quản trị viên mạng lưới dựa trên một mức độ dảm bảo rằng chỉ cho phép người dùng có thể truy cập vào mạng. Dựa trên phé chuẩn IEEE 802.11i, WPA2 cung cấp lớp bảo mật của chính phú triển khai thực hiện các quốc qua Viện Tiêu chuẩn và Công nghệ (NIST) FIPS 140-2 tuân thủ thuật toán mã hóa ASE. WPA2 có thể được kích hoạt một trong hai phiên bản là WPA2-person và WPA2-Business. WPA2-person không được phép truy cập vào mạng lưới của sử dụng một thiết lập mật khẩu. WPA2-Business xác minh thông qua một mạng lưới người sử dụng máy chủ. WPA2 quay trở lại tương thích với WPA

**8. Lọc**

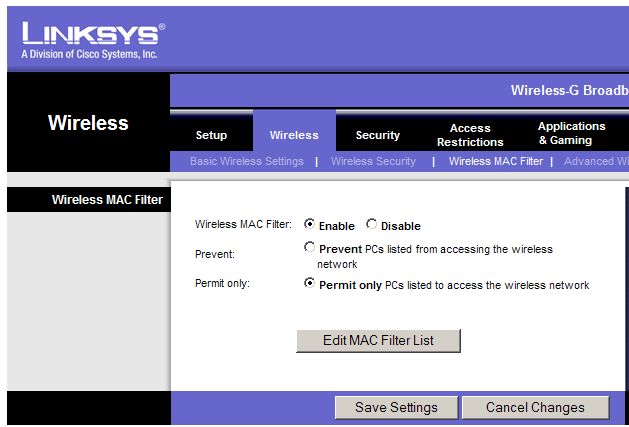
Lọc là cơ chế bảo mật cơ bản có thể sử dụng cùng với WEP. Lọc hoạt động như Access list trên router, cấm những cái không mong muốn và cho phép những cái mong muốn. Có 3 kiểu lọc cơ bản có thể được sử dụng trong wireless lan.

8.1. Lọc SSID

Là phương thức cơ bản của lọc và chỉ sử dụng cho việc điều khiển truy cập cơ bản.

SSID của client phải khớp với SSID của AP để có thể xác thực và kết nối với dịch vụ. Hạn chế của phép lọc SSID là SSID được quảng bá mà không được mã hóa trong các Beacon nên rất dễ bị phát hiện bằng cách sửa dụng các phần mềm dò tìm SSID.

8.2. Lọc địa chỉ MAC

Các Access Point đều có khả năng lọc địa chỉ MAC của máy kết nối đến nên người quản trị mạng có thể cho phép hoặc từ chối những máy đã biết hoặc chưa biết.

Hạn chế của phép lọc địa chỉ MAC là vẫn bị đánh lừa bởi những phần mềm giả địa chỉ MAC.

8.3 Lọc giao thức

Ngoài hai phương pháp lọc kể trên thì chúng ta có thể sử dụng phương pháp lọc giao thức. Trong mạng không dây thì các Access Point có thể cho phép hoặc hạn chế các giao thức được sử dụng HTTP, SMTP, HTTPS, FTP, ... Nên các kết nối được cài đặt với mục đích nào thì cho phép các giao thức phù hợp với mục đích cài đặt đó và hạn chế các giao thức không liên quan và làm giảm thiểu nguy cơ tấn công của kẻ tấn công.

# **V. Phát hiện bất thường trong mạng không dây**

Nhu cầu truy cập Internet qua mạng không dây không ngừng gia tăng, đặc biệt ở các nước đang phát triển, ví dụ hiện nay tại Việt Nam có chương trình phủ sóng mạng không dây cho các thành phố trực thuộc trung ương và các thành phố du lịch như Hội An, Đà Nẵng, Quảng Ninh… Mạng không dây mang đến những lợi ích to lớn cho người dùng thông qua việc cung cấp khả năng kết nối mọi nơi mọi lúc một cách dễ dàng. Bên cạnh những thuận lợi, mạng không dây cũng chứa đựng nhiều rủi ro tiềm ẩn về bảo mật cho người sử dụng, như hacker hoàn toàn có thể nghe lén (sniffing) các thông tin quan trọng của người dùng nếu mạng không dây không sử dụng mã hóa, người dùng dễ bị lừa để truy cập vào các điểm truy cập giả mạo để lấy cấp thông tin… Đồng thời, nhà cung cấp dịch vụ mạng không dây hay doanh nghiệp cũng có thể phải hứng chịu các rủi ro như các cuộc tấn công từ chối dịch vụ (De-authentication) để làm tê liệt hoàn toàn khả năng cung cấp kết nối của các điểm truy cập, tấn công gây nhiễu sóng,..

Hiện nay, các hãng cung cấp thiết bị mạng nổi tiếng như Cisco, AirDefense, AirTight… đều cung cấp những giải pháp phát hiện bất thường và xâm nhập mạng không dây của riêng họ nhằm tăng cường an ninh cho mạng không dây. Mục tiêu của việc phát hiện bất thường và xâm nhập là xác định các hoạt động trái phép dùng sai, lạm dụng đới với hệ thống máy tính gây ra bởi cả người dùng trong hệ thống lẫn người xâm nhập ngoài hệ thống. Nó dựa trên phân tích các sự kiện để phát hiện các bất thường và tấn công: phát hiện dựa trên các dấu hiệu và phát hiện dựa trên sự bất thường. Trong đó, phát hiện dựa trên dấu hiệu là nhạn dạng các sự kiện hoặc tập hợp các sự kiện phù hợp với một mẫu các sự kiện đã được định nghĩa là tấn công; phát hiện sự bất thường nghĩa là thiết lập một hiện trạng các hoạt động bình thường và sau đó duy trì một hiện trạng hiện hành cho hệ thống, khi hai yếu tố có sự khác biệt nghĩa là đã có sự xâm nhập. Sau đây chúng ta tìm hiểu về 1 số hệ thống giúp phát hiện bất thường trong mạng không dây.

## **1. WIDS (Wireless Instrusion Detection System)**

Cách làm việc của IDS trong mạng không dây có nhiều khác biệt so với môi trường mạng LAN truyền thống. Trong môi trường mạng có dây ta có toàn quyền quản lý đối với các loại lưu lượng được truyền trên dây dẫn. Trong mạng không dây, tất cả mọi người trong phạm vi phủ sóng của tần số theo chuẩn 802.11 đều có thể truy cập vào mạng. Do đó cần phải có sự giám sát cả bên trong và bên ngoài mạng. Một khác biệt nữa là WIDS cần cho mạng máy tính đã triển khai và chưa triển khai mạng không dây. Lý do là dù khả năng bị tấn công từ mạng không dây vào mạng LAN chưa rõ ràng nhưng đó là một mối đe dọa thực sự. Một điều luôn phải để tâm đến là các AP giả mạo bất kể bạn đang dùng mạng không dây hay mạng LAN truyền thống. Đôi khi bạn không thể biết chắc ai đó đã triển khai mạng không dây trong khi bạn cho rằng công nghệ không dây chưa được thực hiện trong mạng của mình.

Một hệ thống WIDS thường là một hệ thống máy tính có phần cứng và phần mềm đặc biệt để phát hiện các hoạt động bất thường. Phần cứng wireless có nhiều tính năng so với card mạng wireless thông thường, nó bao gồm việc giám sát tần số sóng (RF\_Radio frequency), phát hiện nhiễu,... Một WIDS bao gồm một hay nhiều thiết bị lắng nghe để thu thập địa chỉ MAC (Media Access Control), SSID, các đặc tính được thiết lập ở các trạm, tốc độ truyền, kênh hiện tại, trạng thái mã hóa,..

*Nhiệm vụ của WIDS :*

* Giám sát và phân tích các hoạt động của người dùng và hệ thống
* Nhận diện cấc loại tấn công đã biết
* Xác định các loại bất thường của hệ thống mạng
* Xác định các chính sách bảo mật cho WLAN
* Thu thập tất cả truyền thông cho mạng không dây và đưa ra các cảnh những dấu hiệu đã biết hay sự bất thường của truyền thông.

*Mô hình hoạt động của WIDS:*

*+ WIDS tập trung*: gồm một bộ tập trung sẽ thu thập tất cả các dữ liệu tần số 802.11 của các cảm biến mạng riêng lẻ và chuyển chúng tới thiết bị quản lý trung tâm, nơi dữ liệu IDS được lưu trữ và xử lý để phát hiện xâm nhập.

Hầu hết các IDS tập trung đều có nhiều cảm biến để có thể phát hiện xâm nhập trong phạm vi toàn mạng. Để thuận tiện, log file và các tín hiệu báo động đều được đưa về thiết bị quản lý trung tâm, thiết bị này có thể dùng quản lý cũng như cập nhật cho tất cả các cảm biến. WIDS tập trung phù hợp với mạng WLAN phạm vi rộng vì dễ quản lý và hiệu quả trong việc xử lý dữ liệu.



Hình 5.1: Mô hình WIDS tập trung

+ *WIDS phân tán*:  bao gồm một hoặc nhiều thiết bị thực hiện cả chức năng cảm biến và quản lý. Mô hình này phù hợp với mạng WLAN nhỏ và có ít hơn 3 AP, WIDS phân tán tất nhiên sẽ tiết kiệm chi phí hơn.



Hình 5.2: Mô hình WIDS phân tán

*Hoạt động của hệ thống WIDS*: WIDS -> thu thập lưu lượng mạng -> phân tích -> phát hiện bất thường -> cảnh báo.

Cụ thể: hệ thống WIDS giám sát toàn bộ mạng không dây,chuyển tiếp lưu lượng đã được tổng hợp và thu thập từ các cảm biến. Sau đó phân tích lưu lượng đã được thu thập. Nếu phát hiện có sự bất thường thì cảnh báo sẽ được hiển thị.

Hệ thống WIDS có thể gửi cảnh báo trong một số trường hợp sau:

* AP bị quá tải khi có quá nhiều trạm kết nối vào
* Kênh truyền quá tải khi có quá nhiều AP hoặc lưu lượng sử dụng cùng kênh.
* AP có cấu hình không thích hợp hoặc không đồng nhất với các AP khác trong hệ thống mạng.
* Số các gói fragment quá nhiều
* WIDS dò ra được các trạm ẩn
* Số lần kết nối vào mạng quá nhiều

Mạng không dây được thiết kế để có thể bao phủ một phạm vi vật lý rộng lớn đảm bảo cho người dùng có thể truy cập thuận tiện từ nhiều nơi khác nhau. Chính vì lý do đó, nhiều điểm truy cập không dây phải được thiết lập ở các vị trí khác nhau trong mạng để đảm bảo độ đồng đều tín hiệu cho toàn mạng. Một quy tắc chung khi triển khai giải pháp WIDS là các cảm biến phải đặt ngay ở nơi AP được cài đặt. Lợi thế rõ nhất của việc làm này là có thể bảo vệ cho mạng không dây một cách toàn diện và triệt để. Ngoài ra tuân theo quy tắc này kẻ tấn công sẽ bị định vị chính xác dễ dàng hơn sau khi người quản trị xác định được cảm biến nào đặt gần kẻ tấn công nhất. Hầu hết các chính sách bảo mật cho mạng không dây đều đề xuất rằng mọi truyền thông trong mạng không dây đều cần mã hóa. Do đó WIDS có thể kiểm soát tất cả các lưu lượng và dữ liệu từ AP tới các thiết bị không dây khác và cảnh báo bất cứ khi nào phát hiện thấy dữ liệu chưa được mã hóa. Một thuộc tính khác có thể thực hiện cho WIDS là tạo một danh sách các AP hợp lệ, do đó bất cứ khi nào không nhận diện được hay phát hiện ra một AP giả mạo, WIDS có thể nhanh chóng phát hiện và cảnh báo.

*Kết luận:* Rõ ràng thấy rằng thông tin thu thập được bởi WIDS tạo ra cơ sở dữ liệu được sử dụng để lập báo cáo về tình trạng hoạt động của mạng và lập ra kế hoạch cho hệ thống mạng. So sánh cảnh báo của các AP qua nhiều vị trí có thể giúp ta xác định được vấn đề gây ra bởi sự khác nhau về các dòng sản phẩm, phiên bản, cấu hình, phiên bản về phần mềm hệ thống (firmware) và về cấu hình.

## **2.** **IPS (Instruction Prevention System)**

Hệ thống IPS là 1 kỹ thuật an ninh mới, kết hợp các ưu điểm của kĩ thuật firewall với hệ thống phát hiện xâm nhập IDS, có khả năng phát hiện sự xâm nhập, các cuộc tấn công và tự động ngăn chăn các cuộc tấn công đó.

*Chức năng*: Các giải pháp IPS nhằm mục đích bảo vệ tài nguyên, dữ liệu và mạng. Chúng sẽ làm giảm bớt những mối đe dọa tấn công bằng việc loại bỏ những lưu lượng mạng có hại hay có ác ý trong khi vẫn cho phép các hoạt động hợp pháp tiếp tục.

*Kiến trúc chung*: Hệ thống IPS gồm 3 modul chính:

* *Modul phân tích luồng dữ liệu*: có nhiệm vụ lấy tất cả các gói tin đi đến mạng để phân tích.
* *Modul phát hiện tấn công*: có nhiệm vụ phát hiện các cuộc tấn công. Có hai phương pháp để phát hiện các cuộc tấn công, xâm nhập là do sự lạm dụng và dò sự không bình thường.
* Phương pháp dò sự lạm dụng: phân tích các hoạt động của hệ thống, tìm kiếm các sự kiện giống với các mẫu tấn công đã biết trước.
* Phương pháp dò sự không bình thường: nhận ra các hành động không bình thường của mạng.
* *Modul phản ứng*: khi modul phát hiện tấn công gửi tín hiệu báo cáo sự cố tấn công hoặc thâm nhập đến modul phản ứng. Lúc đó modul phản ứng sẽ kích hoạt tường lửa thực hiện chức năng ngăn chặn cuộc tấn công hay cảnh báo tới người quản trị.

*Phân loại hệ thống IPS:*

* *IPS ngoài luồng*: luồng dữ liệu vào hệ thống mạng sẽ cùng đi qua tường lửa và IPS. IPS có thể kiểm soát các luồng dữ liệu vào phân tích và phát hiện các dấu hiện của sự xâm nhập, tấn công. Với vị trí này, IPS có thể quản lý tường lửa, chỉ dẫn nó chặn lại các hành động nghi ngờ mà không làm ảnh hưởng đến tốc độ lưu thông của mạng.
* *IPS trong luồng*: vị trí IPS nằm trước tường lửa, luồng dữ liệu phải đi qua IPS trước khi tới bức tường lửa. Điểm khác chính so với IPS ngoài luồng là có thêm chức năng chặn lưu thông. Điều đó làm cho IPS có thể ngăn chặn luồng lưu thông nguy hiểm nhanh hơn so với IPS ngoài luồng. Tuy nhiên, vị trí này sẽ làm cho tốc độ luồng thông tin ra vào mạng chậm hơn.

**VI. Tài liệu tham khảo**

* <https://www.wikipedia.org/>
* <http://www.infosec.gov.hk/english/technical/files/wireless.pdf>
* <http://www.iwar.org.uk/comsec/resources/wireless/NIST_SP_800-48.pdf>