HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Đỗ Viết Công

PHÂN TÍCH VÀ THIẾT KẾ TĂNG HIỆU NĂNG HỆ THỐNG MẠNG WIFI TẠI TRƯỜNG CAO ĐẲNG LÝ THÁI TỔ

Chuyên ngành: Kỹ Thuật Viễn Thông

Mã số: 8.52.02.08

TÓM TẮT LUẬN VĂN THẠC SĨ

HÀ NỘI - NĂM 2020

Luận văn được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học: TS. Lê Ngọc Thúy

Phản biện 1: TS. Nguyễn Chiến Trinh

Phản biện 2: PGS.TS. Nguyễn Hữu Trung

Luận văn được bảo vệ trước Hội đồng chấm luận văn thạc sĩ tại Học viện Công nghệ Bưu chính Viễn thông

Vào lúc: 9 giờ 00 ngày 20 tháng 06 năm 2020

Có thể tìm hiểu luận văn tại:

- Thư viện của Học viện Công nghệ Bưu chính Viễn thông.

MỞ ĐẦU

Trong bối cảnh cách mạng công nghiệp 4.0 đang diễn ra mạnh mẽ cùng với 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 mọi lĩnh vực của đời sống xã hội đã góp phần thúc đẩy sự phát triển các hệ thống mạng viễn thông di động, và mạng không dây. Trong số này phải kể đến mạng không dây WLAN với hàng loạt chuẩn mạng mới được phát triển, tiêu biểu là IEEE 802.11. WLAN với nhiều lợi thế như dễ kết nối, tính cơ động cao, chi phí để sử dụng cộng nghệ mạng không quá đắt đỏ. Và khi công nghệ mạng không dây được cải thiện, thì chi phí phần cứng cũng thấp hơn giúp cho số lượng người cài đặt mạng không dây sẽ tăng cao hơn, khả năng ứng dụng rộng rãi hơn, nên việc nghiên cứu mạng WLAN thực sự là cần thiết. Tuy nhiên, việc nghiên cứu và triển khai ứng dụng công nghệ WLAN, cần phải quan tâm tới tính bảo mật an toàn thông tin. Do môi trường truyền dẫn là truyền dẫn vô tuyến nên WLAN rất dễ bị rò rỉ thông tin và đặc biệt là các nguy cơ bị xâm nhập trái phép. Do đó, cùng với sự phát triển của WLAN cần phải quan tâm phát triển các khả năng bảo mật WLAN, cung cấp thông tin hiệu quả, tin cậy cho người sử dụng. Đồng thời trên cơ sở nghiên cứu xem xét thực trạng vấn đề bảo vệ ngăn chặn xâm nhập trái phép của mạng WLAN, đưa ra giải pháp bảo mật mạng WLAN một cách hiệu quả và phù hợp nhất nhằm tăng hiệu năng mạng.

Do đó, cùng với sự phát triển của WLAN chúng ta phải quan tâm phát triển các khả năng bảo mật WLAN an toàn, cung cấp thông tin hiệu quả, tin cậy cho người sử dụng. Đồng thời trên cơ sở nghiên cứu xem xét thực trạng vấn đề bảo vệ ngăn chặn xâm nhập trái phép của mạng WLAN, đề xuất ứng dụng giải pháp bảo mật mạng WLAN một cách hiệu quả và phù hợp nhất nhằm tăng hiệu năng. Chính vì những lý do trên, học viên quyết định chọn đề tài: "***Phân tích và thiết kế tăng hiệu năng hệ thống mạng Wifi tại Trường Cao đẳng Lý Thái Tổ***" làm luận văn thạc sỹ. Trong suốt quá trình nghiên cứu và triển khai đề tài, học viên nhận thấy vấn đề hiệu năng của một hệ thống mạng là vô cùng quan trọng vì nó cho chúng ta biết được khả năng đáp ứng cũng như hiệu quả cụ thể khi người sử dụng tham gia vào hệ thống mạng. Dựa trên thực tế hệ thống mạng của Cao đẳng Lý Thái Tổ trong nội dung chương 3 của luận văn học viên đã đi sâu và phân tích kỹ lưỡng các kỹ thuật để nhằm tăng hiệu năng cho mạng WLAN của trường một cách hiệu quả nhất.

Nội dung chính của luận văn gồm:

Chương I. Tổng quan chung về mạng không dây - WLAN

Chương II. Các vấn đề bảo mật trong mạng, yếu tố ảnh hưởng đến hiệu năng trong mạng WLAN

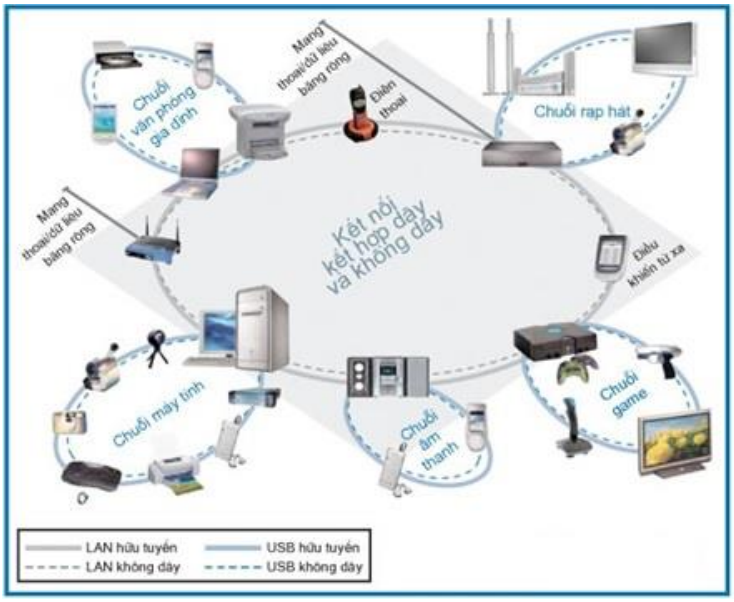
Chương III. Phân tích, mô phỏng tăng hiệu năng mạng cho hệ thống mạng WLAN Trường Cao đẳng Lý Thái Tổ

CHƯƠNG 1: TỔNG QUAN CHUNG VỀ MẠNG KHÔNG DÂY WLAN

1.1 Khái niệm và lịch sử hình thành mạng WLAN

WLAN là từ viết tắt của (Wireless Local Area Network) có nghĩa là Mạng cục bộ không dây, nó là phương thức kết nối không dây cho hai hoặc nhiều thiết bị sử dụng sóng radio tần số cao và thường bao gồm một điểm truy cập đến Internet.

Mạng không dây ngày nay bắt nguồn từ các giai đoạn phát triển của thông tin vô tuyến và những ứng dụng điện báo và radio. WLAN là công nghệ mạng do phía quân đội triển khai đầu tiên vào những năm 1990. Bởi vì họ cần một phương tiện đơn giản và dễ dàng, có thể bảo mật được sự trao đổi thông tin trong chiến tranh.



Hình 1.1: Sơ đồ mạng LAN phổ biến

1.2 Các tiêu chuẩn mạng thông dụng của WLAN

Tiêu chuẩn 802.11

Đây là chuẩn đầu tiên của hệ thống mạng không dây. Tốc độ truyền khoảng từ 1 đến 2 Mbps, hoạt động ở băng tần 2.4GHz. Chuẩn này chứa tất cả công nghệ truyền tải hiện hành bao gồm trải phổ chuỗi trực tiếp (DSS), trải phổ nhảy tần (FHSS) và hồng ngoại. Chuẩn 802.11 là một trong hai chuẩn miêu tả những thao tác của sóng truyền (FHSS) trong hệ thống mạng không dây. IEEE 802.11 bao gồm các chuẩn sau:

CÁC CHUẨN WIFI 802.11					
Chuẩn IEEE	802.11a	802.11b	802.11g	802.11n	802.11ac
Năm phát hành	1999	1999	2003	2009	2013
Tần số	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Tốc độ tối đa	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Phạm vi trong nhà	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Phạm vi ngoài trời	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

Bảng 1.1: Bảng tổng hợp các chuẩn WiFi 802.11 thông dụng

Một số tiêu chuẩn khác

Ngoài các chuẩn phổ biến trên, IEEE còn lập các nhóm làm việc độc lập để bổ sung các quy định vào các chuẩn 802.11a, 802.11b, và 802.11g nhằm nâng cao tính hiệu quả, khả năng bảo mật và phù hợp với các chuẩn cũ như:

- IEEE 802.11c: Bổ sung việc truyền thông và trao đổi thông tin giữa LAN qua cầu nối lớp MAC với nhau.

- 802.11ah - tạo ra các mạng Wifi có phạm vi mở rộng vượt ra ngoài tầm của mạng 2.4-5GHz thông thường.

- 802.11aj - được phê chuẩn năm 2017, được sử dụng chủ yếu ở Trung Quốc.

- 802.11ax - đang chờ được phê chuẩn, dự là trong năm 2018, nếu được thông qua đây chính là chuẩn Wifi 6 đang được mọi người mong chờ.

- 802.11ay - đang chờ được phê chuẩn, dự là trong năm 2019.

- 802.11F - Inter-Access Point Protocol, được đề xuất cho giao tiếp giữa các điểm truy cập để hỗ trợ roaming client (2003).

- 802.11T - dự đoán Hiệu suất Không dây.

Trong khi đó, 802.11x sẽ không được dùng như một tiêu chuẩn độc lập mà sẽ bỏ trống để trỏ đến các chuẩn kết nối IEEE 802.11 bất kì. Nói cách khác, 802.11 có ý nghĩa là "mạng cục bộ không dây", và 802.11x mang ý nghĩa "mạng cục bộ không dây theo hình thức kết nối nào đó (a/b/g/n/ac)".

1.3 Cấu trúc và mô hình mạng WLAN

Mạng sử dụng chuẩn 802.11 gồm có 4 thành phần chính:

- Hệ thống phân phối (Distribution System - DS).
- Điểm truy cập (Access Point).
- Môi trường truyền tải vô tuyến (Wireless Medium).
- Trạm (Stations).

Hình 1.2: Cấu trúc cơ bản của một mạng WLAN.

Mạng WLAN gồm 3 mô hình cơ bản như sau:

- Mô hình mạng độc lập (IBSS) hay còn gọi là mạng phi liên kết (Ad hoc).
- Mô hình mạng cơ sở (BSS).
- Mô hình mạng mở rộng (ESS).

1.4 Đánh giá ưu, nhược điểm và thực trạng mạng WLAN hiện nay

1.4.1 Ưu điểm

Độ tin cậy cao trong nối mạng của các hộ gia đình, doanh nghiệp và sự tăng trưởng mạnh mẽ của mạng Internet, các dịch vụ trực tuyến, với lợi ích của dữ liệu và tài nguyên dùng chung. Với mạng WLAN, người dùng truy cập thông tin dùng chung mà không cần phải tìm chỗ để cắm và các nhà quản lý mạng không nhất thiết phải bổ sung lắp đặt thiết lập hoặc di chuyển dây nối. Mạng WLAN cung cấp các hiệu suất sau: khả năng phục vụ, tiện nghi, và các lợi thế về chi phí thấp hơn hẳn các mạng nối dây truyền thống.

- **Khả năng lưu động cải thiện hiệu suất và dịch vụ:** Các hệ thống mạng WLAN cung cấp cho sự truy cập thông tin thời gian thực tại bất cứ đâu cho người dùng mạng trong khu vực được thiết lập. Khả năng lưu động này hỗ trợ các yêu cầu về hiệu suất và dịch vụ mà mạng nối dây không thể triển khai thực hiện được.

- **Cài đặt đơn giản:** Cài đặt hệ thống mạng WLAN nhanh và dễ dàng.
- **Linh hoạt trong cài đặt:** Công nghệ không dây cho phép kết nối mạng đến các vị trí mà mạng nối dây không thể triển khai.
- **Giảm bớt giá thành sở hữu:** Giá thành đầu tư ban đầu hệ thống phần cứng cho mạng WLAN có giá thành cao hơn các hệ thống phần cứng mạng LAN hữu tuyến, nhưng chi phí cài đặt toàn bộ và giá thành trong quá trình sử dụng bảo dưỡng, sửa chữa thấp hơn đáng kể.
- **Tính linh hoạt:** Các hệ thống mạng WLAN được định hình cấu trúc theo các kiểu liên kết mạng khác nhau tùy thuộc các nhu cầu của các ứng dụng và các cài đặt cụ thể. Cấu hình mạng dễ dàng thay đổi từ các mạng độc lập phù hợp với số lượng nhỏ người dùng đến các mạng cơ sở hạ tầng với hàng nghìn người dùng trong một vùng rộng lớn.
- **Khả năng mở rộng:** Khả năng mở rộng của mạng không dây có thể đáp ứng tức thì khi gia tăng số lượng người sử dụng.

1.4.2 Nhược điểm

Công nghệ mạng LAN không dây, ngoài những tính năng và những ưu điểm được đề cập ở trên thì cũng có các nhược điểm như:

- **Bảo mật:** Môi trường truyền dẫn không dây là không gian tự do, nên khả năng bị tấn công vào hệ thống, người dùng là rất cao.
- **Phạm vi:** Với chuẩn mạng 802.11 mới nhất hiện nay, phạm vi ứng dụng của mạng WLAN đã có sự thay đổi lớn. Tuy nhiên nó vẫn chưa thể đáp ứng được hết nhu cầu của người dùng. Để mở rộng phạm vi vùng phục vụ cần phải trang bị thêm bộ lập hay điểm truy cập, dẫn đến chi phí gia tăng. Với những mô hình mạng lớn vẫn phải kết hợp với mạng hữu tuyến có dây.
- **Độ tin cậy:** Vì sử dụng sóng vô tuyến để truyền dẫn nên việc bị nhiễu, tín hiệu bị suy giảm do tác động của vật cản và các thiết bị khác (tường bê tông, lò vi sóng, tín hiệu radio…) là không tránh khỏi. Làm giảm đáng kể hiệu quả, phạm vi đáp ứng hoạt động của mạng.
- **Tốc độ:** Tốc độ của mạng không dây với các chuẩn mới đã có cải thiện tuy nhiên vẫn còn rất chậm so với mạng sử dụng cáp (100 Mbps đến hàng Gbps).

1.4.3 Thực trạng mạng WLAN hiện nay

Trong những năm vừa qua cùng với sự phát triển mạnh mẽ của Internet và các thiết bị mạng, sự phát triển của kinh tế thị trường, nhu cầu trao đổi thông tin và dữ liệu của con người là rất lớn. Mạng WLAN hiện nay đã trở nên phổ biến và rất gần gũi trong cuộc sống. Chúng ta có thể dễ dàng kết nối sử dụng mạng không dây tại nhiều địa điểm như: cơ quan, trường học, văn phòng, quán Cafe, khu vui chơi giải trí… hoặc ngay tại nhà bằng nhiều thiết bị hiện đại như: Tivi, laptop, PDA, các thiết bị adroid. Tuy nhiên, vẫn còn một số tồn tại như:

- ✓ **Không thay đổi mật khẩu của nhà sản xuất:** Khi cầu hình các hầu hết đều không thay đổi mật khẩu truy cập của nhà sản xuất. Router rất dễ bị xâm nhập và thay đổi cấu hình.
- ✓ **Không kích hoạt các tính năng mã hóa:** khi tính năng không được kích hoạt, rất có thể dùng một số phần mềm dò mật khẩu để lấy những thông tin phục vụ cho những ý đồ xấu.
- ✓ **Kích hoạt phương pháp bảo mật cấp thấp hoặc không kích hoạt:** Hiện nay một số hệ thống mạng đang sử dụng không hề kích hoạt bất kỳ chế độ bảo mật nào. Hoặc nếu có kích hoạt thì cũng chỉ kích hoạt chế độ bảo mật ở cấp thấp như VD: WEP. Điều này hoàn toàn không nên. Người ngoài mạng có thể xâm nhập bẻ khóa và truy cập vào mạng [2] [3].

1.5 Kết luận Chương 1

Chương này giúp cho chúng ta có một cái nhìn tổng thể về sự phát triển của mạng không dây, các công nghệ ứng dụng trong mạng không dây. Chúng ta có thể hiểu một cách khái quát cơ chế hoạt động của mạng WLAN, ưu, nhược điểm cũng như các mô hình hoạt động của mạng WLAN.

Ngoài ra, chúng ta cũng tìm hiểu về chuẩn 802.11 và các thế hệ chuẩn mạng 802.11 thông dụng cho mạng WLAN, hiểu được những gì diễn ra trong quá trình thiết lập kết nối với một hệ thống WLAN đơn giản.

Trong chương tiếp theo chúng ta sẽ nghiên cứu thực trạng gây mất an ninh an toàn của mạng không dây, cách thức tấn công trong mạng không dây, các ứng dụng kỹ thuật mã hóa để bảo mật cho mạng không dây và một số giải pháp cho việc đảm bảo an ninh an toàn cho mạng không dây mà cụ thể là WLAN.

CHƯƠNG 2: CÁC VẤN ĐỀ BẢO MẬT, YẾU TỐ ẢNH HƯỞNG ĐẾN HIỆU NĂNG TRONG MẠNG WLAN

2.1 Khái quát bảo mật trong mạng cục bộ không dây WLAN

Trong mạng WLAN bảo mật là một trong những khuyết điểm lớn nhất. Do điều kiện môi trường truyền dẫn thông tin của loại mạng này, mà khả năng truy cập kết nối của các thiết bị ngoài trong phạm vi phát sóng là vô cùng lớn. Đồng thời, khả năng nhiễu sóng bởi các thiết bị điện tử cũng không thể tránh khỏi. Để an toàn trong sử dụng mạng WLAN, chúng ta cần phải bảo mật WLAN.

2.2. Nguy cơ mất an ninh mạng

2.2.1 Những nguy hiểm cho an ninh mạng

Bảo mật là sự hạn chế khả năng lạm dụng tài nguyên và tài sản. Bảo mật trở nên đặc biệt phức tạp trong quản lý, vận hành những hệ thống thông tin có sử dụng các công cụ tin học, nơi có thể xảy ra và lan tràn nhanh chóng việc lạm dụng tài nguyên (các thông tin di chuyển vô hình trên mạng hoặc lưu trữ hữu hình trong các vật liệu) và lạm dụng tài sản (các máy tính, thiết bị mạng, thiết bị ngoại vi, các phần mềm của cơ quan hoặc người sở hữu hệ thống). Hạn chế ở đây có ý rằng không thể triệt phá hết ngay việc lạm dụng, cho nên cần sẵn sàng đề phòng mọi khả năng xấu với các phương cách thích hợp và chuẩn bị xử lý các sự cố nếu có việc lạm dụng xảy ra.

Kẻ tấn công trực tiếp có thể sử dụng công cụ để tấn công hoặc dùng kỹ thuật riêng để tấn công phá hoại, lấy cắp thông tin. Đây chính là bước hacker thu thập mã số tài khoản ngân hàng, tài khoản e-mail, tài khoản thẻ tín dụng, thông tin bí mật, hay mật khẩu hệ thống…của người hay tổ chức bị tấn công. Sau đó hacker sử dụng thông tin này để trục lợi hoặc có thể bán lại thông tin. Khi nắm được mật khẩu hệ thống trang tin, kẻ mạo danh có thể đăng nhập vào trang tin này và thay đổi nội dung trang tin.

Kẻ tấn công chiếm quyền sử dụng nhiều máy tính nối mạng, có thể bao gồm cả máy chủ. Các máy tính này có thể sử dụng để tấn công từ chối dịch vụ website nào đó cùng lúc. Khi có quá nhiều yêu cầu dịch vụ gửi đến cùng một lúc, băng thông tới website bị nghẽn, hệ thống máy chủ quá tải dẫn tới ngưng hoạt động.

2.3 Kiến trúc mạng WLAN

2.4 Các phương thức bảo mật trong WLAN

2.4.1 WEP - Wired Equivalent Privacy

2.4.2 WPA

2.4.3 WPA2

2.4.4 Lọc (filtering)

Lọc là cơ chế bảo mật cơ bản có thể sử dụng cùng với WEP hoặc một số giao thức khác. Lọc hoạt động giống 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:

- Lọc SSID
- Lọc địa chỉ MAC
- Lọc giao thức

2.4.5 WLAN VPN

2.4.6 Nhận thực và tiêu chuẩn xác thực 802.1x

2.4.7 Bảo mật cấp cao (EAP)

2.4.8 Phương pháp phát hiện xâm nhập trong mạng không dây (WIDS)

2.4.9 Giải pháp ngăn ngừa và phát hiện xâm nhập IDS/IPS

Hệ thống ngăn ngừa xâm nhập mạng (NIPS – Network-based Intrusion Prevention) hát hiện tấn công, có thể khởi tạo các hành động trên thiết bị khác để ngăn chặn tấn công. Nhận ra tấn công bằng cách phân tích bản sao của lưu lượng mạng. IPS thường được triển khai trước hoặc sau firewall. Khi triển khai IPS trước firewall là có thể bảo vệ được toàn bộ hệ thống bên trong kể cả firewall, vùng DMZ. Có thể giảm thiểu nguy cơ bị tấn công từ chối dịch vụ đối với firewall. Khi triển khai IPS sau firewall có thể phòng tránh được một số kiểu tấn công thông qua khai thác điểm yếu trên các thiết bị di động sử dụng VPN để kết nối vào bên trong.

Hệ thống ngăn ngừa xâm nhập host (HIPS – Host-based Intrusion Prevention) chặn đứng trước khi tấn công đến mạng bên trong. Cung cấp khả năng bảo vệ mạng dựa vào định

danh, phân loại và ngăn chặn mối đe dọa được biết hoặc chưa biết như worm, virus, đe dọa đến ứng dụng, …thường được triển khai với mục đích phát hiện và ngăn chặn kịp thời các hoạt động thâm nhập trên các host. Để có thể ngăn chặn ngay các tấn công, HIPS sử dụng công nghệ tương tự như các giải pháp antivirus. Ngoài khả năng phát hiện ngăn ngừa các hoạt động thâm nhập, HIPS còn có khả năng phát hiện sự thay đổi các tập tin cấu hình.

2.5 Các yếu tố gây ảnh hưởng đến hiệu năng cho hệ thống mạng WLAN

2.5.1 Khái niệm hiệu năng mạng

Hiệu năng mạng là một vấn đề phức tạp do các yếu tố có thể tổng hợp đưa ra nhằm đánh giá vấn đề hiệu năng chưa thực sự rõ ràng. Tuy nhiên, trong thực tế rất cần có những khái niệm bản chất và sát thực tiễn với mục tiêu đánh giá được toàn bộ vấn đề hiệu năng bao gồm cả các yếu tố đo đạc, theo dõi, điều khiển đều được tính đến. Có thể sơ lược khái niệm hiệu năng mạng như sau: *Hiệu năng mạng là hiệu quả và năng lực hoạt động của hệ thống mạng*. Như vậy, việc đánh giá hiệu năng mạng chính là tính toán và xác định hiệu quả, năng lực thực sự của hệ thống mạng trong các điều kiện khác nhau.

2.5.2 Các tham số đánh giá hiệu năng

Để lượng hóa vấn đề hiệu năng mạng, cần thiết phải có bộ tham số tiêu biểu đặc trưng cho vấn đề này. Trong đó, các tham số sau đây được sử dụng như những khái niệm điển hình mà nhìn vào chúng có thể cho thấy kết quả của đánh giá hiệu năng mạng.

2.5.2.1 Tính sẵn sàng (Availability)

Tính sẵn sàng là thước đo đầu tiên khi xác định và đánh giá hiện trạng mạng có khả năng phục vụ, đáp ứng yêu cầu hay không. Tham số này cho phép chỉ ra luồng thông tin có đang được chuyển tiếp qua hệ thống mạng hay bị tắc nghẽn cần phải xử lý, các dịch vụ mạng đang được cung cấp có sẵn sàng cho việc trả lời các yêu cầu đưa ra. Vấn đề liên thông giữa các hệ thống trong mạng cũng được đề cập trong tính sẵn sàng.

Một trong các công cụ, phương pháp đơn giản thường được sử dụng khi kiểm

tra tính sẵn sàng của hệ thống mạng là sử dụng chương trình ping. Chương trình khi thực hiện sẽ gửi các gói tin dưới giao thức ICMP tới phía máy cần kiểm tra và đợi kết quả trả lời, nếu có kết quả trả lời chúng ta có thể xác định được tính sẵn sàng của hệ thống đích.

2.5.2.2 Thời gian đáp ứng (Response time)

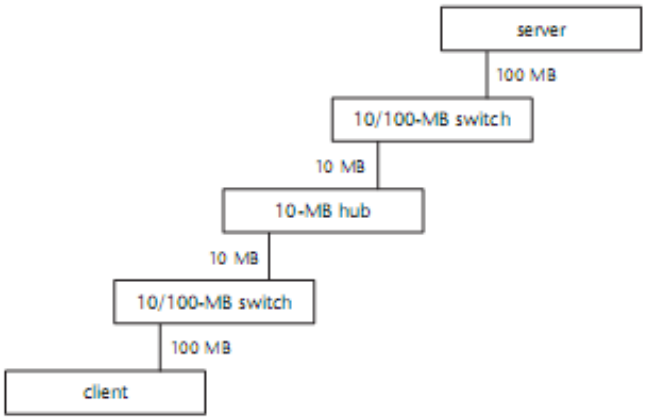
Khi yêu cầu được gửi tới, sẽ có một khoảng thời gian dành cho việc xử lý trước khi trả về kết quả, khoảng thời gian này được gọi là thời gian đáp ứng, bao gồm thời gian đi, thời gian xử lý yêu cầu và thời gian về. Đây là tham số rất quan trọng ảnh hưởng tới quá trình đánh giá khả năng giải quyết vấn đề khi có yêu cầu và hạ tầng truyền thông. Thời gian đáp ứng chậm thường do khả năng giải quyết vấn đề của ứng dụng, hạn chế trong truyền và nhận thông tin trên giao thức và hạ tầng truyền thông tin. Có thể chỉ ra một số các yếu tố ảnh hưởng trực tiếp tới thời gian đáp ứng như sau:

- Quá tải trong các phân đoạn mạng
- Các lỗi xuất hiện trên mạng
- Khiếm khuyết khi mở rộng mạng
- Xử lý các thông tin quảng bá trên mạng chưa tốt
- Thiết bị mạng kém chất lượng
- Quá tải trên các nút mạng

2.5.2.3 Khả năng sử dụng mạng (Network utilization)

Người quản trị hệ thống mạng có thể xác định thông lượng mạng bằng phương pháp tìm nút cổ chai giữa 2 điểm cần đo. Đồng thời, trong một số tình huống nhiều người sẽ khẳng định thông lượng của hai điểm sẽ được xác định bằng giá trị băng thông (Bandwidth) tại 2 điểm đó. Những điểm nêu trên là hoàn toàn không chính xác bởi 2 lý do chính sau đây:

- Giá trị băng thông không phụ thuộc vào thời gian đo và đây là khái niệm khác hoàn toàn với thông lượng.
- Thông lượng thực tế phụ thuộc rất nhiều vào tổng thể kết nối, thiết bị sử dụng, ứng dụng hoạt động, dịch vụ cung cấp của hệ thống tại thời điểm cần đo.



Hình 2.1: Độ phức tạp khi xác định thông lượng giữa client và server

2.5.2.4 Khả năng của băng thông mạng (Network bandwidth capacity)

2.6 Kết luận Chương 2

Trong chương II này chúng ta đã nghiên cứu và đánh giá về các vấn đề bảo mật cho mạng WLAN, phân tích và đánh giá được vai trò của bảo mật trong mạng không dây. Tìm hiểu nguy cơ mất an ninh mạng không dây và giới thiệu một số dạng tấn công của mạng WLAN, cộng với sự đi sâu và tìm hiểu các kiến trúc cơ bản của mạng WLAN và các phương thức bảo mật và chống xâm nhập trái phép. Các yếu tố gây ảnh hưởng đến hiệu năng cho hệ thống mạng WLAN.

Trong chương III tiếp theo chúng ta sẽ phân tích hiện trạng hệ thống mạng WLAN của trường Cao đẳng Lý Thái Tổ, đưa ra giả pháp, đi sâu vào biện pháp cụ thể để tiến hành tăng hiệu năng cho mạng WLAN.

CHƯƠNG 3: PHÂN TÍCH, MÔ PHỎNG TĂNG HIỆU NĂNG CHO HỆ THỐNG MẠNG WLAN CAO ĐẲNG LÝ THÁI TỔ

3.1 Phân tích hiện trạng hệ thống mạng WLAN của Cao đẳng Lý Thái Tổ

3.1.1 Hiện trạng hệ thống mạng WLAN

Trường đứng chân trên địa bàn Phường Đình Bảng, Thị xã Từ Sơn, Tỉnh Bắc Ninh - một thành phố trẻ đang trong quá trình công nghiệp hoá mạnh mẽ, với vị trí đắc địa là cửa ngõ thủ đô Hà Nội. Bắc Ninh được biết đến là nơi tập trung của nhiều khu công nghiệp lớn như: VSIP, Tiên Sơn, Yên Phong. Đây là các khu công nghiệp hội tụ các doanh nghiệp hàng đầu về công nghệ cao cũng như các doanh nghiệp phụ trợ cho các tập đoàn lớn như Samsung, LG, Canon, Hồng Hải - các tập đoàn hàng năm có nhu cầu tuyển dụng nhân sự rất lớn để phục vụ nghiên cứu và phát triển sản xuất.

Hình 3.1: Sơ đồ phối cảnh quan trường Cao đẳng Lý Thái Tổ

Toàn thể trường là một khu liên hợp hiện đại bao gồm các hạng mục:

- Văn phòng nhà trường
- Nhà Hiệu bộ - Học chính
- Nhà Hội trường – Giảng đường
- Thư viện
- Khu nhà xưởng thực hành
- Ký túc xá
- Vườn sinh viên, hồ cá, Quảng trường…

Các hạng mục công trình được kết nối bằng hệ thống đường giao thông thuận lợi xen lẫn các khoảng sân vườn, tiểu cảnh cây xanh, vườn hoa. Toàn bộ các khối nhà trong trường được trang bị hệ thống điều hòa trung tâm sử dụng cho tất cả phòng học, phòng làm việc với hệ thống điều khiển thông minh vận hành tự động. Hệ thống loa thông báo, camera IP giám sát… Tất cả các hệ thống vận hành tự động và toàn bộ các hạng mục trên được nối mạng với nhau, phòng server được đặt trên tầng 3 nhà Hiệu Bộ là nơi chứa toàn bộ các Server, có thể nói phòng điều khiển này là đầu não của trường Cao đẳng Lý Thái Tổ.

Toàn bộ trường được trang bị gần 840 máy tính cho phòng học, thư viện và phòng làm việc. Phòng làm việc bao gồm các phòng ban với gần 100 máy tính nằm tại nhà hiệu bộ được nối mạng với trung tâm dữ liệu, Thư viện với gần 100 máy tính được trang bị hệ thống Server riêng phục vụ cho sinh viên tra cứu sách, tài liệu và tự học trên mạng, trường còn có 10 phòng tự học nằm tại nhà hiệu bộ - học chính được trang bị Wifi Free phục vụ cho việc tự học và hệ thống phòng học khoa Tin học và các lớp tin học văn phòng với 8 phòng, mỗi phòng gồm 80 máy tính hiện đại cấu hình đủ đáp ứng tất cả các nhu cầu cho sinh viên khóa Tin học.

Nhà trường trang bị 02 đường cáp quang tốc độ cao phục vụ cho việc truy cập Internet của toàn trường, các thiết bị số như Camera IP, các Server và việc phủ sóng Wifi trong toàn bộ khuôn viên trường. 01 đường phục vụ riêng cho việc đăng ký học và trang chủ Website của trường, 01 đường phục vụ cho riêng thư viện, 01 đường dành riêng cho phòng ban và bộ môn truy cập Internet và cuối cùng 01 đường chuyên dùng cho việc học Online, 01 đường phục vụ cho việc phủ sóng Wifi toàn trường phục vụ cho sinh viên.

3.1.2 Vấn đề bảo mật mạng WLAN tại Cao đẳng Lý Thái Tổ

Hiện nay hệ thống mạng tại Cao đẳng Lý Thái Tổ đã được trang bị Firewall ASA5510, 250 máy tính và máy chủ đã trang bị phần mềm diệt virút bản quyền.

Bảng 3.1: Bảng tổng hợp hiện trạng hệ thống mạng trường Cao đẳng Lý Thái Tổ

TT	Giải pháp bảo mật của hệ thống	Khả năng đáp ứng	
		Mức đáp ứng	có/không
1	Giải pháp tường lửa (Firewall)	Layer 3 - 4	có
		Layer 4 - 7	không
2	Giải pháp dùng phần mền diệt Virut	Máy chủ	30%
		máy trạm	có
3	Giải pháp lưu trữ / phục hồi dữ liệu (Backup/restore)	Backup/restore độc lập	có
		Backup/restore tập chung, đặt lịch, lưu trữ	không
4	Giải pháp dùng các thiết bị phục vụ hỗ trợ phòng chống tấn công, xâm nhập (IDS/IPS)	Toàn mạng	không
5	Giải pháp giám sát an ninh: Phát hiện máy tính mới cắm váo mạng, các dịch vụ không được sử dụng…	Vùng Server quan trọng	không
6	Giải pháp thiết bị phục vụ hỗ trợ xác thực	Xác thực tập trung	không
7	Giải pháp thiết bị phục vụ hỗ trợ kiểm tra đánh giá định kỳ	Toàn mạng	không

Qua bảng tổng hợp trên và để từng bước tăng hiệu năng mạng cũng như khả năng bảo mật cho hệ thống mạng WLAN của Cao đẳng Lý Thái Tổ thì chúng ta cần phải đưa ra được giải pháp có khả năng phát hiện các truy cập bất hợp pháp, những cuộc tấn công vào máy chủ, dịch vụ mạng nhằm đảm bảo cho hệ thống hoạt động có tính bảo mật cao. Vì vậy giải pháp sử dụng công nghệ IDS/IPS có thể đảm đương nhiệm vụ này.

3.2 Đề xuất các phương pháp tăng hiệu năng cho hệ thống mạng WLAN tại Cao đẳng Lý Thái Tổ

Từ thực trạng hệ thống mạng WLAN đang sử dụng tại trường Cao Đẳng lý Thái Tổ đề xuất các giải pháp tăng hiệu năng cho hệ thống như:

- Đối với hệ thống phần cứng mạng sử dụng phần mềm VNPT-CAB để tối ưu.
- Đối với hệ thống phần mềm dùng các phương pháp Kiểm soát hiệu năng của mạng không dây như: Định tuyến; Chất lượng dịch vụ; Vấn đề về an ninh trong mạng không dây.

3.2.1 Sử dụng phần mềm VNPT-CAB tối ưu hệ thống mạng WLAN

3.2.1.1 Vùng phủ

Khi triển khai một mạng vô tuyến "indoor", việc xác định vùng phủ sóng là một vấn đề cơ bản. Vùng phủ sóng được xác định qua khoảng cách mà một mạng vô tuyến có thể phát và thu ở một tốc độ cho trước theo các nguyên tắc hoạt động trong băng tần của nó.

3.2.1.2 Sử dụng phần mềm VNPT-CAB tối ưu hệ thống phần cứng

Sử dụng phần mềm:

Phần mềm được viết ra mục đích sử dụng phục vụ cho công tác sản xuất dinh doanh của các đơn vị trực thuộc tập đoàn, quản lý tập trung các hoạt động sản xuất kinh doanh của các đơn vị như: Sửa chữa báo hỏng, lập hợp đồng cung cấp dịch vụ, tra cứu thông tin hạ tầng mạng, nhu cầu dịch vụ, hạ tầng đối thủ, đo kiểm chất lượng sóng di động, Wifi…

Áp dụng sử dụng phần mềm trong việc tối ưu phần cứng hệ thống mạng Wifi:

- Đăng nhập bằng User do Tập đoàn cấp.
- Kết nối điện thoại sử dụng phần mềm đến từng AP.
- Đo kiểm với khoảng cách đo thử test sóng từ Client đến AP với bán kính là 20m.
- Dựa vào kết quả đo dịch chuyển vị trí AP đến vị trí tối ưu nhất.

Hình 3.2: Chức năng đo kiểm sóng của phần mềm VNPT-CAB

Yêu cầu sau khi tối ưu hệ thống phần cứng mạng WLAN. Hệ thống WLAN phủ sóng khắp toà nhà, có chất lượng tín hiệu sóng đảm bảo cho các kết nối từ AP đến Client. Khoảng cách đo thử test sóng từ Client đến AP là 20m.

Bảng 3.2: Kết quả đo kiểm sóng của phần mềm VNPT-CAB tại trường Cao đẳng Lý Thái Tổ

STT	SSID	Tốc độ	Cường độ	Đánh giá
1	Hieubo 11	70 Mbps	-47 dBm	đạt
2	Hieubo 12	67 Mbps	-56 dBm	đạt
3	Hieubo 13	71 Mbps	-46 dBm	đạt
4	Hieubo 21	65 Mbps	-57 dBm	đạt
5	Hieubo 22	72 Mbps	-46 dBm	đạt
6	Hieubo 23	71 Mbps	-45 dBm	đạt
7	Hieubo 31	69 Mbps	-52 dBm	đạt
8	Hieubo 32	70 Mbps	-47 dBm	đạt
9	Hieubo 33	68 Mbps	-55 dBm	đạt
10	Thuvien	72 Mbps	-46 dBm	đạt
11	Quangtruong	73 Mbps	-45 dBm	đạt

3.2.2 Kiểm soát hiệu năng của mạng không dây

Thông lượng, độ trễ và tỷ lệ mất gói tin là một trong những vấn đề quan trọng quyết định mạng hoặc truyền thông có tin cậy hay không. Nó khá rõ ràng ngoài khả năng mở rộng và các vấn đề về an ninh, vì vậy trong phần này của luận văn chúng ta sẽ tập trung chủ yếu vào các yếu tố có thể trợ giúp để có được thông lượng tốt hơn và do đó sẽ cải thiện được hiệu năng của mạng. Thông lượng tốt sẽ làm cho chúng ta có thể bảo mật dữ liệu thành công từ một điểm này tới một điểm khác. Và một cách làm hiệu quả để tăng hiệu năng của mạng chính là thông qua hiệu quả của việc định tuyến. Một yếu tố khác có thể giúp tăng cường thông lượng mạng là cân bằng tải. Mất cân băng tải có thể xảy ra tại một thời điểm, một thời gian nhất định và nó sẽ làm dòng lưu lượng đi trệch hướng. Vì thế điều này sẽ dẫn đến hiện tượng tắc nghẽn mạng và giảm thông lượng mạng.

3.3 Mô phỏng tăng hiệu năng mạng WLAN tại Cao đẳng Lý Thái Tổ

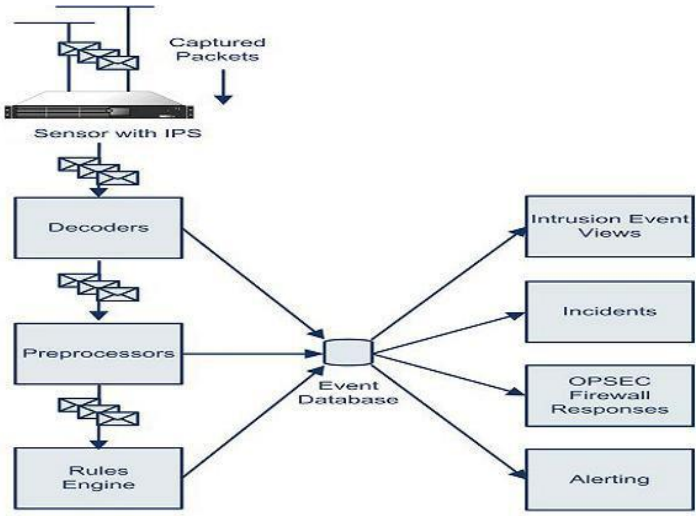
Mô phỏng được thực hiện thông qua công cụ mô phỏng Cisco SDM (Security Device Manager) là công cụ để quản lý thiết bị Router thông qua công nghệ JAVA. SDM sử dụng để cấu hình Router thông qua các interface HTTP hoặc HTTPs giúp chúng ta cấu hình LAN,

WAN và các tính năng bảo mật khác của Router (ACLs, VPN,…). SDM được thiết kế cho người quản trị mạng hay reseller SMB mà không yêu cầu người sử dụng có kinh nghiệm nhiều trong việc cấu hình Router. Việc cấu hình Router thông qua SDM giúp cho việc định tuyến và cân bằng tải trong hệ thống mạng nhằm tránh tắc nghẽn đường truyền mạng và duy trì sự ổn định của hệ thống.

3.3.1 Các công cụ cần thiết để thực hiện việc mô phỏng

- Hệ điều hành window 7
- Phần mềm giả lập GNS3
- Tool SDM của cisco
- Máy PC phải cài gói java để hỗ trợ cho SDM

Thiết lập mạng quản lý cho các thiết bị IDS/IPS: Kết nối các cổng mangement trên các thiết bị IDS/IPS với thiết bị quản lý. Từ đây, thiết bị Quản lý có thể quản lý tất cả các thiết bị IDS/IPS.



Hình 3.3: Mô hình nguyên lý hoạt động

Khi gói tin được nhận được bởi thiết bị, gói tin đó sẽ được:

- Giải mã gói tin bởi thành phần bộ giải mã của thiết bị.
- Sau đó gói tin sẽ được chuyển vào quá trình tiền xử lý.
- Gói tin sẽ được so sánh với tập Rules được sử dụng.
- Quá trình đó sẽ đưa ra được một cơ sở dữ liệu về các sự kiện.
- Các sự kiện đó có thể được lọc ra thành các dạng sự kiện khác nhau.

Mô tả các kết quả đem lại.

- Tính năng IPS: Bảo vệ mạng trước các cuộc tấn công mạng.
- Tính năng IDS/IPS kết hợp với RNA: Phát hiện và phân tích các báo cáo tình trạng bảo mật mạng sử dụng IDS hay IPS.
- Tính năng RNA phát hiện hệ thống mạng: Host active, Open Port, Protocols, Vulnerabilities.

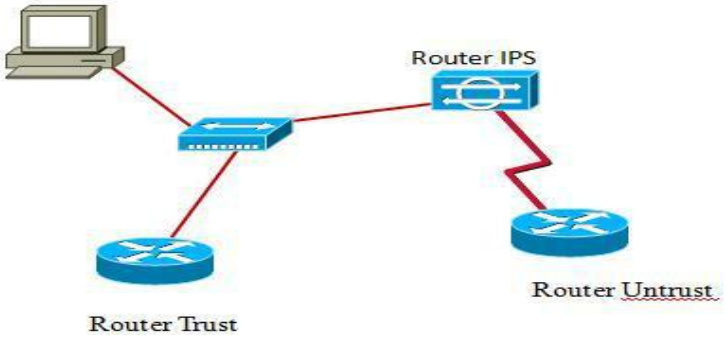
Bảng 3.3: Các kết quả đem lại qua một đợt tấn công

STT	Tình huống bị tấn công	kết quả đem lại
1	**Trước**	Tính năng RNA của thiết bị giúp phát hiện các nguy cơ an ninh mạng: Network profile (OS, Services, Open Ports, Vulnerability, Host static)
		RNA kết hợp với IPS, IDS để tự động active/disable các rules cần thiết để bảo vệ hệ thống mạng
		Tính năng Passive Scan cho phép RNA phát hiện nguy cơ an ninh hệ thống mạng mà không ảnh hưởng tới năng lực hệ thống mạng
2	**Trong**	Phát hiện và ngăn chặn các cuộc tấn công từ bên ngoài như Worms, Trojans, Buffer overflows, DoS attacks, Backdoor attacks, Spyware, Port scans, VoIP attacks, IPv6 attacks, Statistical anomalies, Protocol anomalies, P2P attacks, Blended threats, Zero-day attacks… vào các server dịch vụ.
		Có thể xác lập các qui tắc ngăn chặn các cuộc tấn công hoặc xác lập chế độ tự động tinh chỉnh tùy theo các dịch vụ.
		Đưa ra các báo cáo về các cuộc tấn công, các lỗ hổng bảo mật.
3	**Sau**	Sourcefire với hệ thống báo cáo đầy đủ, thông minh giúp người quản trị phân tích được những ảnh hưởng đối với hệ thống sau khi bị tấn công.
		RNA kết hợp với tính năng Report thiết lập độ ưu tiên cho các Events, tính năng này cho phép giảm thiểu đáng kể thời gian phân tích các Events sau khi hệ thống bị tấn công.
		RNA phân tích lỗ hổng bảo mật đưa ra các khuyến cáo về vá lỗ hổng bảo mật cho hệ thống.
		Tính năng IT Policy Compliance: Đưa ra những cảnh báo những vi phạm về chính sách bảo mật. Những vi phạm này có thể là: một cuộc tấn công nguy hiểm xảy ra, một sự cố liên quan tới một máy chủ hay một dịch vụ. Cảnh báo có thể thực hiện qua Email, SNMP hay SYSLOG.

3.3.2 Mục tiêu của mô phỏng

Mô phỏng giúp thấy được tính năng, hoạt động cũng như các bước cấu hình IDS/IPS trên router. Thực hiện tính năng gây ra cảnh báo nếu có vi phạm.

3.3.3 Mô hình mô phỏng



Hình 3.4: Mô hình mô phỏng

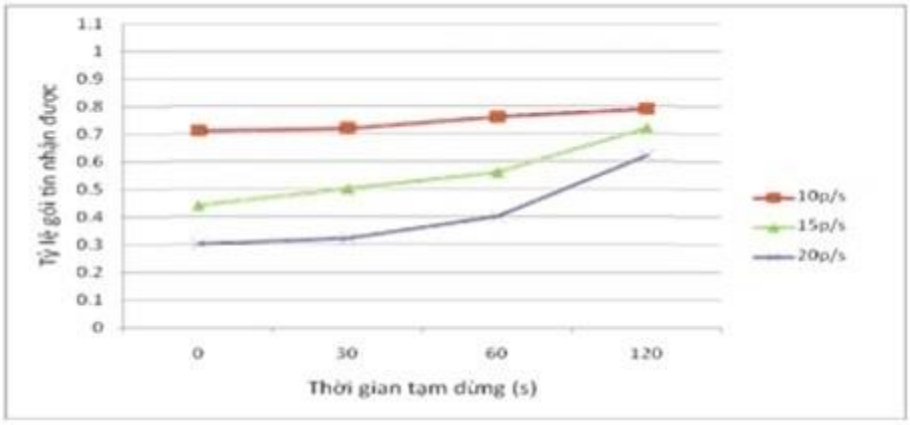
3.3.6 Kết quả thu được từ quá trình mô phỏng

Khi đánh giá ảnh hưởng của tải trong mạng, ta có thể thay đổi kích thước gói hoặc số luồng CBR, tuy nhiên thay đổi tốc độ phản ánh chính xác hơn, ta sử dụng 3 tình huống sau: 10 gói tin/giây; 15 gói tin/giây và 20 gói tin/giây

Với các thông số khác được thiết lập như bảng dưới đây:

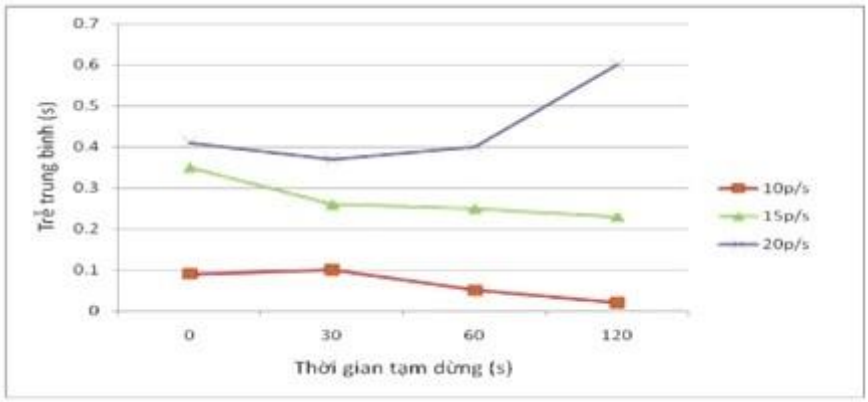
Thông số	Giá trị
Phạm vi truyền dẫn	250m
Băng thông	2Mbps
Thời gian mô phỏng	120s
Kích cỡ môi trường mô phỏng	670×670m
Loại lưu lượng	CBR
Kích thước gói tin	512 bytes
Số kết nối	20
4 giá trị của thời gian tạm dừng	0, 30, 60, 120s

3.3.6.1 Kết quả mô phỏng hiện trạng hiệu năng với hệ thống mạng Wifi trường Cao đẳng Lý Thái Tổ



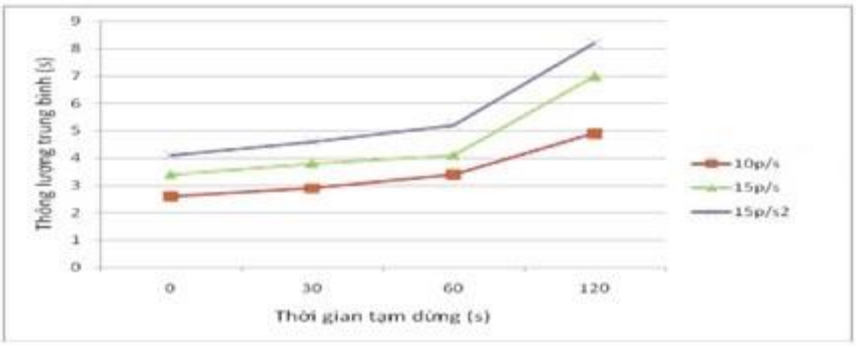
Hình 3.5: Tỷ lệ gói tin nhận được - chưa sử dụng giao định tuyến

Khi không sử dụng giao thức định tuyến với tốc độ gửi gói tin là 10 gói tin/s thì tỷ lệ gói tin nhận được giảm nhanh hơn khi thông số di chuyển cao. Tại tốc độ 15 gói tin/s, 20 gói tin/s thì gói tin hủy bỏ nhiều hơn, khi thời gian tạm dừng là 0 thì chỉ có khoảng 30-40% gói tin được nhận.



Hình 3.6: Trễ trung bình đầu cuối – chưa sử dụng giao thức định tuyến

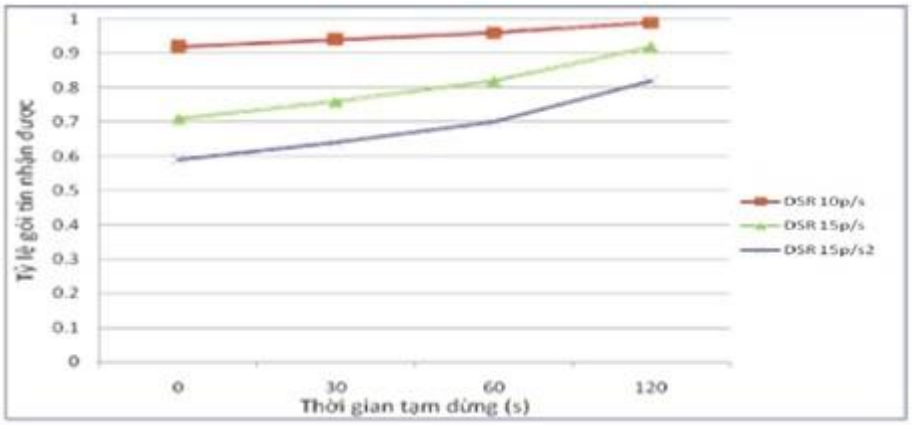
Giá trị trễ bị ảnh hưởng khi tốc độ gói CBR cao. Bộ đệm bị đầy nhanh chóng nên gói tin ở trong bộ đệm lâu hơn, ta có thể quan sát khi tốc độ 20 gói tin/giây. điểm khác biệt dễ thấy khi tốc độ gói tin là 10 gói tin/giây. Giá trị trễ cao khi thông số di chuyển cao hay thời gian tạm dừng bằng 0 và tốc độ gói tin là 20 gói tin/giây, do bộ đệm bị đầy nhanh chóng và thậm chí đường định tuyến tồn tại dài hơn.



Hình 3.7: Thông lượng từ đầu cuối – chưa sử dụng giao thức định tuyến

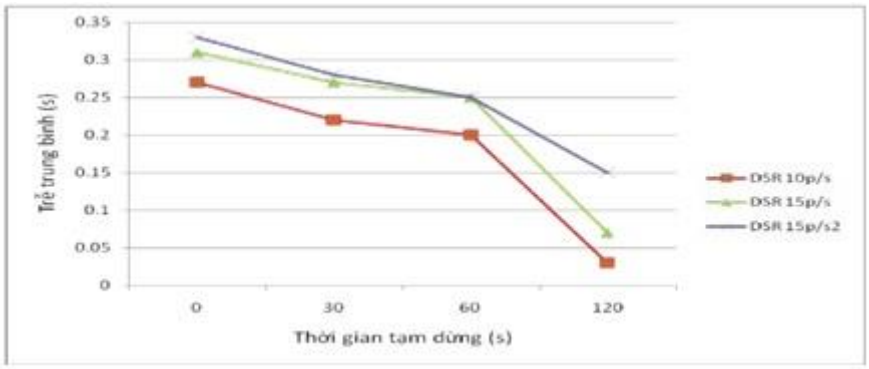
Ở tốc độ CBR thấp, thông lượng bị ảnh hưởng nhiều bởi thông số di chuyển, giá trị vào khoảng 1.5 kbps. Với tốc độ CBR cao hơn, thông lượng giảm khi thông số di chuyển tăng, thể hiện khi tốc độ CBR=10 gói tin/giây. Đây cũng là kết quả của số lượng gói tin bị rơi nhiều, thậm chí với CBR=15, 20 gói tin/giây, thì bên nhận gần như không nhận được gói tin.

3.3.6.2 Kết quả mô phỏng sử dụng phương pháp định tuyến DSR nâng cao hiệu năng



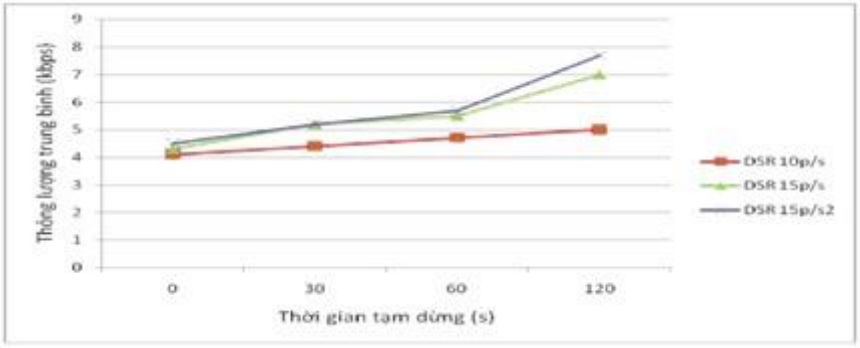
Hình 3.8: Tỷ lệ gói tin nhận được - định tuyến DSR

Khi tốc độ gửi gói tin là 10 gói tin/s thì tỷ lệ gói tin nhận được khá cao, với thời gian tạm dừng bằng 120s tỷ lệ nhận gói tin nhận được xấp xỉ 100%. Tại tốc độ 15 gói tin/s, 20 gói tin/s thì hủy bỏ nhiều gói tin hơn, khi thời gian tạm dừng là 0 thì chỉ có khoảng 60-70% gói tin được nhận.



Hình 3.9: Trễ trung bình đầu cuối – định tuyến DSR

Giá trị trễ cao khi thông số di chuyển cao hay thời gian tạm dừng bằng 0 và tốc độ gói tin là 20 gói tin/giây, do bộ đệm dần đầy lên và đường định tuyến tồn tại dài hơn. Với thời gian tạm dừng truyền càng cao thì độ trễ càng giảm.



Hình 3.10: Thông lượng từ đầu cuối – định tuyến DSR

Ở tốc độ CBR thấp, thông lượng của DSR không bị ảnh hưởng nhiều bởi thông số di chuyển, giá trị vào khoảng 2,5 kbps. Với tốc độ CBR cao hơn, thông lượng giảm khi thông số di chuyển tăng, thể hiện khi tốc độ CBR=10 gói tin/giây, tuy nhiên nó giảm nhẹ, chỉ khi tốc độ đạt 15 gói tin/giây và 20 gói tin/giây. Đây cũng là kết quả của số lượng gói tin bị rơi nhiều.

3.3.6.3 So sánh đánh giá

Từ kết quả của quá trình mô phỏng nhận thấy:

Tỷ lệ gói tin nhận được: Khi sử dụng giao thức định tuyến DSR cao hơn rất nhiều so với khi không sử dụng giao thức định tuyến. Khi thời gian tạm dừng bằng 0 thì giao thức định tuyến DSR thì tỷ nhận được gói tin nhận được toàn khoảng 60-70% so với 30-40%. Thời gian tạm dừng bằng 120s thì DSR nhận được gần như toàn bộ các gói tin gửi đến.

Trễ trung bình đầu cuối: Với DSR khi truyền các gói tin với các tốc độ 10 gói tin/giây, 15 gói tin/giây và 20 gói tin/giây độ trễ không trênh lệch nhiều, thời gian tạm dừng càng lớn độ trễ càng giảm. Còn với không sử dụng định tuyến độ trễ chỉ tốt nhất với tốc độ 10 gói tin/giây, tốc độ 15 gói tin/giây và 20 gói tin/giây độ trễ càng lớn.

Thông lượng từ đầu cuối: Giao thức định tuyến DSR ở tốc độ 15 gói tin/giây, 20 gói tin/giây tỷ lệ gói tin bị rớt nhiều. Nhưng so với không sử dụng giao thức định tuyến ở cùng tốc độ thì bên nhận gần như không nhận được gói tin.

Như vậy, với giao thức định tuyến DSR đã giải quyết được bài toán tăng hiệu năng cho hệ thống mạng WIFI cho trường Cao đẳng Lý Thái Tổ. Hiệu năng hệ thống mạng được cải thiện tốt hơn so với hiện trạng ban đầu.

3.4 Kết luận Chương 3

Chương 3 đã trình bày tóm lược mô phỏng công cụ phân tích kết quả Tracegraph. Từ đó tác giả thực hiện chương trình mô phỏng đánh giá hiệu năng khi chưa định tuyến và khi sử dụng giao thức định tuyến DSR. Mô phỏng đều thực hiện trên một đồ hình mạng giống nhau với các kịch bản được xây dựng. Giao thức DSR thực hiện chuyển tiếp các gói dữ liệu tương đối tốt khi tỷ lệ chuyển động và tốc độ di của node là thấp. Tuy nhiên khi chuyển động của các node tăng lên thì tỷ lệ gói rớt bắt đầu tăng. Hiệu suất của giao thức DSR rất tốt khi toàn bộ node dịch chuyển, mặc dù giao thức này yêu cầu số byte mào đầu định tuyến tăng. Cuối cùng hiệu suất của giao thức DSR khi tốc độ các node di chuyển và nó giảm được số

byte mào đầu định tuyến. Tuy nhiên nó vẫn yêu cầu truyền dẫn nhiều gói mào đầu định tuyến và ở tốc độ di chuyển của các node cao nó thực sự tốn hơn so với giao thức DSR.

Hệ thống phát hiện và ngăn chặn xâm nhập rất hiệu quả trong lĩnh vực bảo mật cũng như tăng hiệu năng sử dụng cho hệ thống mạng của các doanh nghiệp, tổ chức, công ty có nhu cầu bảo mật cao. Thông qua việc mô phỏng có thể thấy được cách cài đặt và sử dụng tính năng IPS trên router hệ thống sẽ gây ra cảnh báo hay ngắt kết nối nếu vi phạm chữ ký được định nghĩa chữ ký trên ips router.

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN CỦA ĐỀ TÀI

Mạng không dây hiện nay phát triển rất nhanh đó là nhờ vào sự thuận tiện của nó. Hiện nay công nghệ không dây, nhất là WLAN hiện đang được ứng dụng ngày càng mạnh mẽ trong đời sống. Nhưng đa số mọi người đều chỉ sử dụng WLAN ở các lĩnh vực liên quan đến máy tính mà không biết rằng bằng sóng WLAN, người dùng máy tính để điều khiển hệ thống đèn, quạt, máy lạnh, lò sưởi, máy tưới, hệ thống nước (internet of thing)… Nhưng vấn đề quan trọng nhất của mạng không dây hiện nay là sự bảo mật của nó chưa có một giải pháp nào ổn định.

Trong đề tài này, em đã cố gắng tổng hợp tất cả những cơ chế bảo mật và tất cả những kiến thức cơ bản về Công nghệ mạng không dây. Với khả năng nghiên cứu, thời gian còn hạn chế cũng như vấn đề về thiết bị phần cứng, phần mềm cho mạng không dây nên vẫn còn có những thiếu sót trong đề tài này. Tuy nhiên với những gì đã nghiên cứu và tìm hiểu thì: Mạng không dây là một giải pháp hay và thời đại, nó giúp cho chúng ta tiết kiệm được thời gian cũng như công sức trong việc lắp đặt cũng như sử dụng.

Trong điều kiện cho phép, công việc nghiên cứu sẽ được tiếp tục như sau:

- Tìm hiểu sâu hơn kỹ thuật bảo mật hiện nay đang được sử dụng phổ biến.
- Nghiên cứu các lỗ hổng và các cách tấn công mạng WLAN để tìm ra phương pháp bảo mật hiệu quả cho mỗi ngành giúp cho việc quản trị và trao đổi tài nguyên giữa các trạm làm việc trong mạng WLAN.
- Áp dụng giải pháp IPS/IDS vào mạng, từ đó đưa ra những mặt mạnh và những mặt còn hạn chế.

Em xin chân thành cám ơn TS Lê Ngọc Thúy đã tận tình hướng dẫn, giúp đỡ em trong thời gian thực hiện đề tài này và trong quá trình thực hiện thì luận văn vẫn còn có nhiều thiếu sót, mong thầy cô góp ý để em có thể hoàn thiện tốt hơn.

TÀI LIỆU THAM KHẢO

[1]. Hãng HP, Tài liệu giảng dạy nội bộ "Xây dựng hệ thống mạng không dây".

[2]. Nguyễn Khánh Trình "Tìm hiểu về mạng không dây và phát triển dịch vụ trên mạng không dây" – Luận văn thạc sỹ đại học Bách Khoa Hà Nội.

[3]. Phan Thành Vinh "Nguyên cứu giải pháp bảo mật mạng không dây" – Luận văn thạc sỹ Học viện Kỹ thuật Quân Sự.

[4]. Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, Network Security Bible, Copyright © 2005 by Wiley Publishing, Inc., Indianapolis, Indiana.

[5]. MIR MOHAMMAD SEYED DANESH, A Surveyon Wireless Security protocols - Faculty of Management – Multimedia University of Malaya.

[6]. Nicolas Sklavos and Xinmiao Zhang 3/2007, Wireless Securiry and Cryptography – Specifications and Implementations.

[7]. Sybex CWNA Certified Wireless Network Administrator Study Guide Exam PW0-100 Sep 2006.

Danh mục các Website tham khảo:

[8]. https: //antoanthongtin.vn

[9]. https: //www.ddth.com

[10]. https: //quantrimang.com/

[11]. https: //vnpro.vn/