LỜI CAM ĐOAN

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi. Các kết quả nêu trong luận văn là trung thực và chưa từng được công bố trong bất cứ công trình nào của người khác.

Tác giả luận văn

Nguyễn Nhật Bình

LỜI CẢM ƠN

Tác giả xin gửi lời cảm ơn chân thành đến tiến sĩ Hà Quang Thuỵ – bộ môn Các Hệ Thống Thông Tin, khoa Công Nghệ , người trực tiếp hướng dẫn tác giả trong suốt quá trình xây dựng ý tưởng và thực hiện luận văn.

Xin chân thành cảm ơn các thầy cô trong khoa Công Nghệ đã dạy bảo, giúp đỡ em trong suốt quá trình học tập và rèn luyện tại khoa. Xin cảm ơn các bạn học, các đồng nghiệp đã đóng góp những ý kiến quý báu và tạo điều kiện cho tôi hoàn thành bản luận văn của mình đặc biệt các anh Vũ Đại Thanh, TS. Nguyễn Mạnh Hùng – công ty ISA; anh Tim Stack – nhóm tin JanOS; anh George Carlin trên diễn đàn security-forum đã ủng hộ những ý tưởng của tôi.

Cuối cùng xin gửi lời cảm ơn đến cha mẹ và gia đình, đặc biệt người vợ thân yêu đã thương yêu giúp đỡ và tạo điều kiện cho tôi hoàn thành luận văn.

PHẦN MỞ ĐẦU

Mạng tích cực [7, 8, 10] là hướng tiếp cận mới mang tính sáng tạo trong việc xây dựng các kiến trúc mạng. Trong hướng tiếp cận này, các thiết bị dẫn đường và thiết bị chuyển mạch trên mạng có thể thực hiện một số tính toán trên các thông điệp được truyền qua chúng. Hướng tiếp cận mạng tích cực có thể thực hiện được do (i) việc các ứng dụng người dùng hiện nay cho phép thực hiện các tính toán trên các nút mạng và (ii) sự phát triển công nghệ mã di chú cho phép sửa đổi động các dịch vụ mạng.

Bắt đầu luận văn, chúng tôi trình bày tổng quan một số hướng tiếp cận mạng tích cực [7, http://www.security-forum.com, http://www.cs.utah.edu/flux/janos/]. Thông qua việc khảo sát các vấn đề đang được giải quyết và các vấn đề mới đặt ra trong quá trình nghiên cứu về mạng tích cực, chúng tôi định hướng tới việc đề xuất giải pháp cho một số vấn đề đang được nhiều nhà nghiên cứu về mạng tích cực quan tâm đến. Một số nội dung đề xuất trong luận văn này đã được chúng tôi trao đổi, chia xẻ cùng với các nhà nghiên cứu khác (George Carlin, Mongrel ...) trên thế giới trong nhóm tin http://www.security-forum.com.

Phương pháp nghiên cứu chính của luận văn là (i) khảo sát các bài báo khoa học được xuất bản trong một vài năm gần đây về mạng tích cực, (ii) tham gia các nhóm tin trao đổi ý kiến với các tác giả của một số bài báo, để từ đó (iii) đề xuất một số cải tiến cho các mô hình đã và đang được xây dựng.

Nội dung của luận văn bao gồm (i) Phần mở đầu, (ii) Bốn (4) chương nội dung, (iii) Phần kết luận (iv) cuối cùng là phần tài liệu tham khảo. Nội dung chính của các chương như sau:

- Chương một "***Giới thiệu mạng tích cực***" cung cấp một cái nhìn bao quát về các hoạt động nghiên cứu mạng tích cực đang diễn ra trên thế giới, mô tả tác dụng của mạng tích cực tới việc tăng tốc quá trình đổi mới kiến trúc mạng và việc những ứng dụng mới có thể được xây dựng dựa trên đó. Phần cuối cùng của chương mô tả những tìm hiểu, khảo sát về các công việc, các hướng nghiên cứu của các nhóm nghiên cứu mạng tích cực, để từ đó lựa chọn vấn đề và định hướng việc giải quyết vấn đề đó.

- Chương hai "***Kiến trúc mạng tích cực và bộ công cụ ANTS***" trình bày về kiến trúc mạng tích cực được xây dựng ban đầu bởi bộ quốc phòng Mỹ; Các thành phần cơ bản của bộ công cụ ANTS (Active Network Transport Toolkit), việc cài đặt các phương thức trong bộ công cụ và phân tích khả năng của bộ công cụ ANTS trong việc xây dựng các ứng dụng.

- Chương ba "***An toàn thông tin trên mạng và việc xây dựng mô hình an toàn cho mạng tích cực***". Chương này tập trung vào việc phân tích vấn đề an toàn trong mạng tích cực nhằm đề xuất việc xây dựng một kiến trúc an toàn cho cách tiếp cận mạng tích cực như một mô hình tham chiếu cho việc xây dựng một mạng tích cực an toàn. Phần đầu của chương sẽ đi sâu phân tích vấn đề (giải pháp giải quyết bài toán và những vấn đề liên quan) an toàn trong liên mạng máy tính nói chung với một số ví dụ dẫn chứng trong mạng Internet. Tiếp đó, chúng tôi phân tích mạng tích cực và những cơ chế có thể gây ra những vấn đề liên quan đến an toàn thông tin. Phần cuối sẽ trình bày đề xuất của luận văn về phương thức xây dựng kiến trúc an toàn dựa trên mô hình xoắn ốc và một kiến trúc an toàn cho cách tiếp cận mạng tích cực có thể được sử dụng làm mô hình tham chiếu cho việc xây dựng mạng tích cực an toàn. Chúng tôi đã trình bày quan điểm về vấn đề về an toàn mạng (security problem or issue) trên trang www.security-forum.com và nhận được nhiều ý kiến đồng tình của những người tham gia diễn đàn như George Carlin, Mongrel ...

- Chương bốn "***Ứng dụng công nghệ mạng tích cực trong việc xây dựng hệ thống tác nghiệp quản lý việc sản xuất chương trình truyền hình***" sử dụng những công nghệ mạng tích cực và mô hình an toàn thông tin đã trình bày trong các chương trước để đưa ra một đề xuất cho việc xử lý hai vấn đề mấu chốt trong hệ thống tác nghiệp quản lý việc sản xuất chương trình truyền hình là truyền thông hình ảnh và xác thực người sử dụng. Đây là một trong những hệ thống quan trọng nhất trong các hệ thống tác nghiệp của Đài truyền hình Việt Nam đã được nêu ra trong "Kế hoạch tổng thể về phát triển công nghệ thông tin của ngành truyền hình Việt Nam giai đoạn 1996-2000" và nêu lại trong [1 - "Đề án tin học hoá cải cách hành chính Đài truyền hình Việt Nam giai đoạn 2001-2005"]. Tuy

nhiên, cho đến thời điểm hiện tại, dự án xây dựng hệ thống tác nghiệp quản lý việc sản xuất chương trình truyền hình vẫn chưa được thực hiện vì nhiều lý do trong đó có lý do công nghệ. Chúng tôi đã lựa chọn và đề xuất một số công nghệ sử dụng mạng tích cực để giải quyết vấn đề của hệ thống trên, từ đó có thể làm tiền đề cho việc xây dựng hệ thống trong tương lai. Các trao đổi của chúng tôi tại http://www.cs.utah.edu/flux/janos/ tập trung vào giải quyết các vấn đề về công nghệ trong việc cài đặt và sử dụng các công cụ để xây dựng các ứng dụng mạng tích cực đã được trình bày ở đây.

Cuối mỗi chương là phần kết luận chương tóm tắt những nội dung chính yếu được trình bày trong chương.

Phần kết luận của luận văn tổng kết những nội dung đạt được của luận văn và định hướng việc phát triển tiếp theo của các nội dung trong luận văn đặc biệt là giải quyết vấn đề công nghệ cho bài toán "X***ây dựng hệ thống tác nghiệp quản lý việc sản xuất chương trình truyền hình".*** Đây là một bài toán thực tế đang cần được giải quyết, mục tiêu chính của tác giả là phát triển những đề xuất trong luận văn thành một *dự án khả thi* và cài đặt tại Đài Truyền Hình Việt Nam.

MỤC LỤC

CÁC HÌNH VẼ

CÁC BẢNG

NHỮNG QUY ĐỊNH TRÌNH BÀY

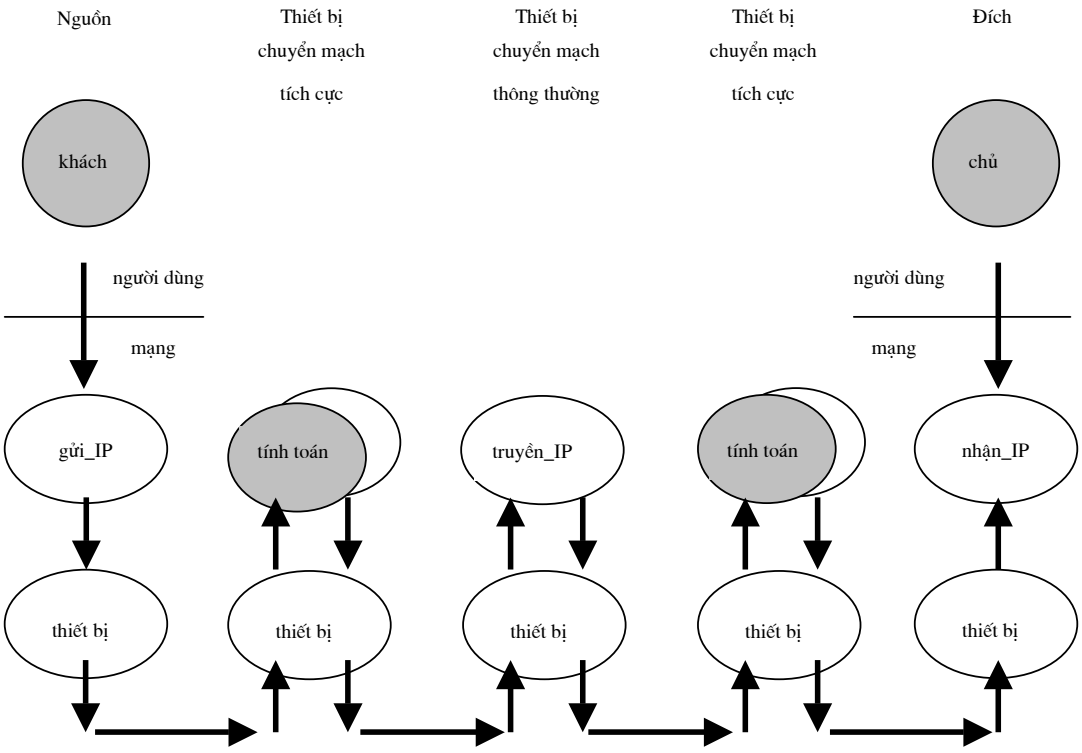
Kiểu chữ	**Quy định**
Chữ nghiêng	Thuật ngữ lần đầu tiên xuất hiện
`Chữ tròn`	Các hàm hoặc mã chương trình
(Chữ trong ngoặc)	Giải thích thuật ngữ đi trước

CÁC THUẬT NGỮ VÀ VIẾT TẮT

Viết tắt	**Thuật ngữ**	**Giải thích**
AA	Active Application	Ứng dụng tích cực hoặc mã tích cực
ANTS	Active Network Transport System	Bộ công cụ cho việc xây dựng các ứng dụng tích cực
ACL	Access Control List	Danh sách điều khiển truy cập
Capsule	Gói tin tích cực (đôi khi gọi tắt là gói tin): các gói tin thông thường sẽ được gọi kết hợp với tên giao thức như gói tin IP, gói tin TCP...	Gói tin chứa mã chương trình, là đơn vị thông tin được truyền trên mạng tích cực
EE	Excutive Environment	Môi trường thực hiện mã lệnh
MPEG	Moving Picture Experts Group	Tiểu ban tiêu chuẩn video
NodeOS	Hệ điều hành mạng tích cực	
	Quản trị viên	Người thực hiện các tác vụ quản trị mạng
	Issue	Vấn đề tranh luận
	Problem	Vấn đề cần giải quyết
	Security	An toàn
	Process	Tiến trình (quá trình)

CHƯƠNG I. GIỚI THIỆU MẠNG TÍCH CỰC

Trong mạng tích cực [7, 8, 10], các thiết bị dẫn đường và thiết bị chuyển mạch có thể thực hiện các tính toán trên các thông điệp truyền qua chúng. Ví dụ, một người sử dụng mạng tích cực có thể gửi các đoạn mã chương trình đến một số thiết bị chuyển mạch trên mạng, các đoạn chương trình này sẽ được thực hiện trong quá trình xử lý các gói tin tương ứng với chúng. Hình 1 cho thấy chúng ta có thể bổ xung các tính năng mới vào các thiết bị dẫn đường trong mạng IP để chúng có thể thực hiện các tính toán trên các gói tin được truyền qua.

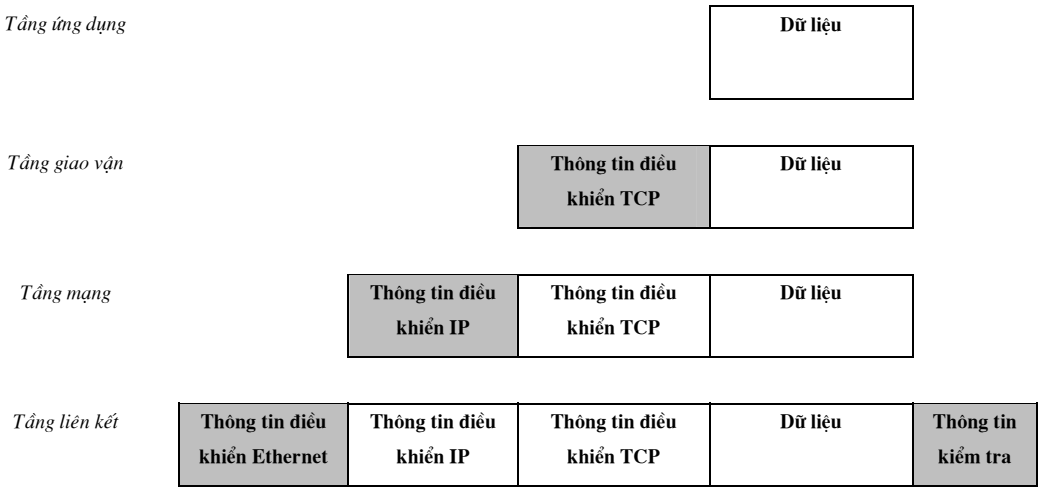


Hình 1. Thực hiện tính toán trong nút mạng tích cực

Những thiết bị dẫn đường này vẫn có khả năng làm việc được với những thiết bị thông thường khác trong mạng, tuy nhiên, những thiết bị dẫn đường thông thường chỉ đơn giản truyền những gói tin trên mạng mà không thực hiện tính toán trên các gói tin. Việc truyền các gói tin theo cách thông thường trên là *trong suốt*

(không thấy được) đối với các thiết bị chuyển mạch tích cực, do đó không làm ảnh hưởng tới việc tính toán của hệ thống.

Chúng ta sử dụng tên gọi mạng tích cực cho hướng tiếp cận này vì các thiết bị trên mạng có thể thực hiện tính toán trên các gói tin truyền qua, hơn nữa chúng còn có thể làm thay đổi nội dung của các gói tin đó hoặc sinh ra các gói tin khác... Các tính toán có thể dựa trên cơ sở từng người dùng hoặc từng ứng dụng. Nghĩa là trên các gói tin được gửi đi tương ứng với mỗi ứng dụng i và ứng dụng j ($i \neq j$) có thể có những tính toán khác nhau trên cùng một nút mạng. So sánh với các mạng chuyển mạch gói khác ví dụ mạng Internet, ta thấy việc tính toán của các mạng đó rất hạn chế. Mặc dù các thiết bị dẫn đường có thể thay đổi phần điều khiển của các gói tin, nhưng chúng không can thiệp vào phần dữ liệu của gói tin. Hình 2 cho ta thấy cách thức đóng gói tin của giao thức TCP/IP (giao thức được sử dụng rộng rãi trên mạng Internet) như thế nào.



Hình 2. Đóng gói thông tin trong giao thức TCP/IP

Từ tầng ứng dụng, dữ liệu được gửi xuống các tầng dưới, mỗi tầng có những định nghĩa riêng về dữ liệu mà nó sử dụng [1]. Tại nơi gửi, mỗi tầng coi gói tin của tầng trên gửi xuống là dữ liệu của nó và thêm vào gói tin các thông tin điều khiển của mình sau đó chuyển tiếp xuống tầng dưới. Tại nơi nhận, quá trình diễn ra ngược lại, mỗi tầng lại tách thông tin điều khiển của mình ra và chuyển dữ liệu lên tầng trên.

Khái niệm mạng tích cực được đưa ra thảo luận trong các tiểu ban nghiên cứu của Bộ Quốc phòng Mỹ (DARPA) vào những năm 1994, 1995 với mục đích tìm ra một hướng phát triển tương lai cho các hệ thống mạng. Một số vấn đề tồn tại của các mạng hiện tại đã được nêu ra như: (i) khó tích hợp những công nghệ và chuẩn mới vào kiến trúc mạng, (ii) hiệu suất thấp gây ra bởi các thành phần dư thừa trong một số lớp của các giao thức, và (iii) việc các dịch vụ mạng mới khó thích nghi được với các kiến trúc hiện tại. Các chiến lược khác nhau đã được đưa ra, trong đó, mạng tích cực có khả năng giải quyết những vấn đề trên. Trong hướng tiếp cận mạng tích cực, các *thiết bị dẫn đường và thiết bị chuyển mạch trên mạng có thể thực hiện một số tính toán trên các thông điệp được truyền qua chúng*. Điều này có thể thực hiện được do (i) việc các ứng dụng người dùng hiện nay cho phép thực hiện các tính toán trên các nút mạng và (ii) sự phát triển công nghệ mã di chú cho phép sửa đổi động các dịch vụ mạng. Ý tưởng sử dụng các thông điệp mang theo mã chương trình cùng với dữ liệu là một bước tiến tự nhiên của các mạng chuyển mạch kênh và chuyển mạch gói thông thường và có thể sử dụng để giúp mạng máy tính thích nghi một cách nhanh chóng với các yêu cầu luôn luôn thay đổi. Cách tiếp cận *dựa chương trình* (program-base) này cung cấp một môi trường thực thi dễ hiểu trên các nút mạng cũng như một nền tảng cho việc thể hiện hệ thống mạng như tổ hợp của các thành phần nhỏ hơn với những tính chất đặc biệt sau: (i) các dịch vụ có thể được phân phối và cấu hình phù hợp với yêu cầu của các ứng dụng, và (ii) có thể quan sát trạng thái của toàn bộ hệ thống mạng thông qua các tính chất của các thành phần riêng lẻ.

Chương này trình bày hai (2) cách tiếp cận trong việc thực hiện mạng tích cực (i) *thiết bị chuyển mạch lập trình được* (programable-switch), và (ii) *bao gói* (capsulation).

- Cách tiếp cận thông qua thiết bị chuyển mạch lập trình được giữ nguyên khuôn dạng của các gói tin truyền trên mạng và cung cấp một cơ chế để tải các đoạn chương trình trên mạng về chạy trên các thiết bị dẫn đường và thiết bị chuyển mạch hỗ trợ mạng tích cực. Việc xử lý gói tin được tách khỏi việc thực hiện tính toán của mạng tích cực cho phép người quản trị mạng lựa chọn

những chương trình được phép chạy trong mạng giảm thiểu được rủi ro so với việc mọi người dùng đều được phép đưa những chương trình chạy vào trong mạng.

- Ngược lại, cách tiếp cận bao gói thay thế các gói tin thụ động trong các kiến trúc mạng hiện tại bằng các chương trình nhỏ tích cực được bao gói trong các gói tin truyền thông và được thực hiện trên mỗi nút mạng mà chúng đi qua. Ngoài ra, dữ liệu của người dùng cũng có thể được gắn trong các bao gói.

Việc nghiên cứu mạng tích cực được "thúc đẩy" bởi công nghệ và được "chờ đón" bởi người dùng. Các chương trình người dùng như *tường lửa* (firewall), *dịch vụ đại diện web* (web proxy), *thông tin nhóm* (multicast router), *dịch vụ đại diện di trú* (mobile proxy), *cổng video* (video gateway)... thực hiện tính toán trên các nút trong mạng. Trong nhiều trường hợp, những dịch vụ trên được cài đặt trên các nút mạng trong khi chúng lại thực hiện những tính toán của ứng dụng, điều này phá vỡ nguyên tắc xây dựng các kiến trúc mạng thông thường [1]. Mục tiêu của việc nghiên cứu mạng tích cực là tìm cách thay thế những cách tiếp cận *phi thể thức* (do việc phá vỡ các nguyên tắc như đã nêu ở trên) bởi một môi trường tính toán mạng với khả năng cho phép người sử dụng lập trình trên mạng của họ.

Việc phát triển mạnh của công nghệ đóng vai trò thúc đẩy sự ra đời và phát triển của mạng tích cực. Cho tới gần đây, các quản trị viên vẫn thường lo ngại việc lập trình trên các thiết bị mạng có thể gây ra những vấn đề không giải quyết được liên quan đến an toàn và hiệu quả của kiến trúc. Tuy nhiên, những tiến bộ của ngôn ngữ lập trình, trình biên dịch và hệ điều hành đã có thể cung cấp chìa khoá để giải quyết vấn đề an toàn và hiệu quả của việc thực hiện mã di trú. Ngày nay, công nghệ tích cực được áp dụng trong nhiều hệ thống cuối và chạy phía trên lớp mạng ví dụ cho phép các máy chủ web và các máy khách trao đổi Java applet. Mạng tích cực thúc đẩy và mở rộng những công nghệ mới để sử dụng trong mạng.

Trong các mục tiếp theo của chương này, chúng tôi cung cấp một cái nhìn bao quát về các hoạt động nghiên cứu mạng tích cực đang diễn ra trên thế giới [7]. Chúng tôi mô tả tác dụng của mạng tích cực tới việc tăng tốc quá trình đổi mới kiến trúc mạng và việc những ứng dụng mới có thể được xây dựng dựa trên đó.

Sau đó sẽ xem xét những *vấn đề thảo luận* (issue) có thể sử dụng làm khung cho việc nghiên cứu mạng tích cực. Cuối cùng, chúng ta tìm hiểu, sẽ xem xét công việc, các hướng nghiên cứu của các nhóm nghiên cứu mạng tích cực, từ đó lựa chọn vấn đề và định hướng việc giải quyết vấn đề đó.

I.1 Kiến trúc cho phép tăng tốc việc đổi mới kiến trúc mạng

Để làm rõ việc mạng tích cực có thể hỗ trợ cho việc đổi mới kiến trúc mạng như thế nào, chúng ta cùng xem xét một số ứng dụng chạy trên các nút mạng gây ra việc phá vỡ những nguyên tắc xây dựng mạng như đã nêu trong phần giới thiệu và cách thức giải quyết những vấn đề với mạng tích cực:

- ***Bức tường lửa***: bức tường lửa là ví dụ rõ nhất của việc phá vỡ nguyên tắc xây dựng mạng. Bức tường lửa được cài đặt một cơ chế lọc gói tin để xác định các gói tin có thể truyền qua nó hoặc bị chặn. Mặc dù nó được kết nối với các thiết bị dẫn đường khác và được nhìn nhận như một thiết bị dẫn đường, nhưng bản chất, ngoài việc thực hiện dẫn đường cho các gói tin, nó được cài đặt các chương trình ứng dụng và các thủ tục người dùng. Việc nâng cấp bức tường lửa để cho phép sử dụng các giao thức mới là một trở ngại lớn. Trong mạng tích cực, việc này có thể thực hiện tự động bằng cách cho phép các ứng dụng của các nhà cung cấp đã được chấp nhận trước (thông qua một cơ chế phân quyền ví dụ username/password hoặc sử dụng chữ ký điện tử) truy cập vào bức tường lửa và cung cấp các mô đun cần thiết vào trong bức tường lửa.
- ***Dịch vụ đại diện web***: Dịch vụ đại diện cung cấp một một phương thức truy cập web và bộ nhớ đệm (cache) web. Nhóm nghiên cúu của đại học Harvest [9] đã đưa ra một kiến trúc phân cấp trong đó các nút mạng chứa bộ đệm web nằm gần miền biên của mạng. Hệ thống này có thể được mở rộng bằng cách cho phép các nút mạng trong kiến trúc nằm trong những điểm chiến lược của mạng.
- ***Thiết bị dẫn đường du cư****: Thiết bị dẫn đường "du cư"* (nomadic routers) được Kleinrock - đại học Berkeley - mô tả trong hội thảo về mạng và tính toán di chú năm 1995 được chèn vào giữa các hệ thống cuối và mạng. Module này

quản lý việc kết nối vào mạng của các đối tượng sử dụng đường link khác nhau ví dụ kết nối qua điện thoại và kết nối thông qua mạng LAN, từ đó quyết định việc sử dụng thêm bộ đệm hoặc nén đường truyền khi hệ thống kết nối vào mạng thông qua đường truyền tốc độ thấp và sử dụng chế độ an toàn như mã hoá khi người sử dụng truy cập từ xa vào hệ thống.

- ***Cổng giao vận****: Cổng giao vận* (Transport Gateways) là các nút nằm trong những điểm chiến lược của mạng, là cầu nối với các mạng lớn khác nhau về thông lượng và có độ tin cậy khác nhau ví dụ điểm nối giữa mạng hữu tuyến và mạng vô tuyến. Để hỗ trợ các thiết bị vô tuyến truy cập vào mạng hữu tuyến, người ta sử dụng cơ chế TCP snooping để ghi nhớ trạng thái của từng kết nối vô tuyến.
- ***Dịch vụ ứng dụng****:* Các cổng dịch vụ ứng dụng chuyên biệt thường được sử dụng để hỗ trợ một số ứng dụng ví dụ chuyển mã của các ảnh trong hội thảo video giữa các người dùng sử dụng truy cập mạng với tốc độ đường truyền khác nhau.

Từ việc những ứng dụng trên đều đòi hỏi việc tính toán trên mạng, ta thấy kiến trúc mạng cần phải thích nghi để giải quyết những vấn đề thực tế đó.

Hiện nay, tốc độ cải tiến mạng còn quá chậm, thời gian từ khi xây dựng các *nguyên mẫu* đến khi có thể triển khai các hệ thống lớn kéo dài khoảng mười (10) năm. Những công việc cần thực hiện để cải tiến một dịch vụ mạng bao gồm (i) tiêu chuẩn hoá, (ii) kết hợp vào trong kiến trúc nền của các nhà sản xuất phần cứng, và cuối cùng là (iii) người sử dụng mua và cài đặt. Những vấn đề còn tồn tại chưa giải quyết được của các dịch vụ Internet như chúng ta đã biết là (i) multicast, (ii) mở rộng khả năng xác thực và (iii) mở rộng khả năng di động, (iv) IP phiên bản 6.

Giao thức internet (IP) cho phép kết nối các hệ thống bằng cách cung cấp khuôn dạng gói tin chuẩn và một cơ chế đánh địa chỉ phân cấp [1]. Mặc dù các thiết bị dẫn đường được cung cấp bởi nhiều nhà sản xuất khác nhau, chúng đều phải cài đặt chung giao thức để có thể truyền thông với nhau. Như vậy, cơ chế cải tiến IP

có thể thực hiện theo các cách: thay đổi dịch vụ IP (có nghĩa là thay đổi tất cả) hoặc xây dựng một *cơ chế chồng* (overlay).

Ngược lại, mạng tích cực có thể thực hiện nhiều chương trình ví dụ chúng có thể thực hiện các tính toán rất khác nhau trên các gói tin truyền qua chúng. Thay vì việc tất cả các thiết bị dẫn đường đều áp dụng một phương thức tính toán trên tất cả các gói tin, mạng tích cực định nghĩa mọi nút hỗ trợ các mô hình tính toán tương đương, như những một *bộ lệnh ảo*. Mạng tích cực cung cấp một mô hình trừu tượng trong đó, việc kết nối là tin cậy cho phép các ứng dụng tuỳ biến việc xử lý các gói tin cho phù hợp với yêu cầu của chúng.

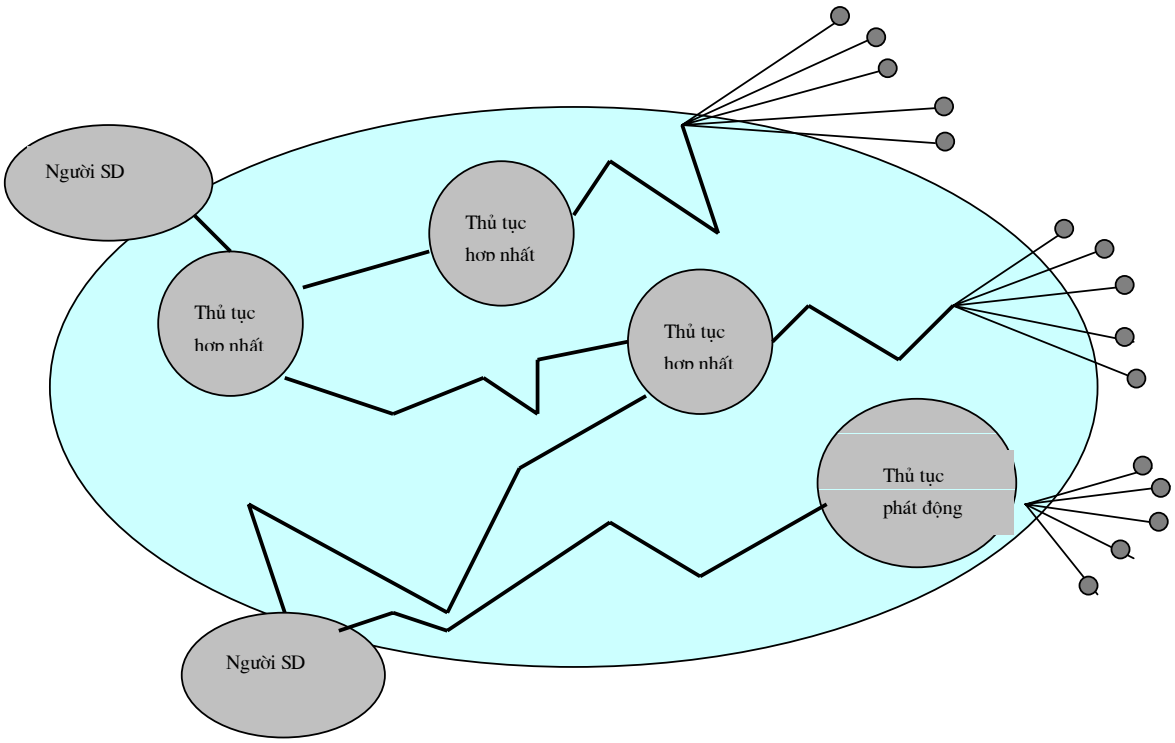
Khả năng tải các dịch vụ mới vào trong kiến trúc cho phép cải tiến các quá trình trong đó khả năng của các dịch vụ mới sẽ phụ thuộc vào việc thị trường chấp nhận chúng. Mạng tích cực cung cấp một phương thức để thay đổi kiến trúc của nền công nghiệp mạng, từ cách tiếp cận "mainframe" (trong đó phần cứng và phần mềm được đóng gói lại với nhau) đến một cách tiếp cận "ảo" trong đó phần cứng và phần mềm được cách tân một cách riêng rẽ. Quan điểm trừu tượng về mạng lập trình được cung cấp một nền tảng cho các tính toán của chương trình người dùng trong kiến trúc, cho phép các dịch vụ mới được phát triển nhanh hơn so với việc tất cả các nhà cung cấp cùng tuân theo một chuẩn và cung cấp chung dịch vụ.

I.2 Kiến trúc cho phép xây dựng các ứng dụng mới

Mạng tích cực cho phép xây dựng những ứng dụng mới trên (i) thông tin được hợp nhất, (ii) cơ chế bảo vệ, (iii) và hệ thống quản trị

I.2.1 Hợp nhất và phân bố thông tin

Số lượng ứng dụng đã được phát triển ngày nay là rất lớn, điều này đòi hỏi các dịch vụ mạng phải hỗ trợ việc hợp nhất và phân bố thông tin. Tuy nhiên, những hệ thống hiện tại đang phải dựa trên cơ sở các dịch vụ với số lượng chức năng rất hạn chế.



Hình 3. Khai thác mạng hợp nhất và phân bố thông tin

Hình 3 cho thấy việc mạng phức tạp với nhiều site ứng dụng sẽ thúc đẩy sự tính toán và việc lưu trữ trong mạng như thế nào. Trong hình này, một ứng dụng ví dụ chương trình mô phỏng hoặc vận hành từ xa có thể cho phép người sử dụng thấy một bức tranh tổng thể về mạng được xây dựng bởi thông tin nhận được từ nhiều bộ cảm biến khác nhau (như tính chất đã trình bày ở trên của mạng tích cực). Ngoài ra, mỗi bộ cảm biến có thể được theo dõi bởi một số người sử dụng với nhu cầu khác nhau về thông tin mà họ truy cập. Việc kết hợp dữ liệu vào mạng làm giảm thông lượng cần thiết đối với những người sử dụng ở những vùng biên của mạng có thông lượng không cao. Cũng giống như vậy, những dịch vụ multicast do người sử dụng định nghĩa trong mạng làm giảm tải trên các bộ cảm biến và trên mạng trục.

Dịch vụ đại diện web có thể lưu trữ đệm thông tin là một ví dụ khác của dịch vụ đa người dùng, có thể sử dụng việc tính toán và lưu trữ trên mạng. Kiến trúc lưu trữ đệm được xây dựng tại đại học Harvest có thể làm giảm độ trễ của việc nhiều

người sử dụng cùng truy cập hệ thống một lúc và chiếm nhiều thông lượng của mạng. Hiện tại, các nút mạng lưu trữ thông tin đệm thường được đặt trong vùng biên của mạng ví dụ tại nút trong mạng có người dùng cuối. Hệ thống này có thể được mở rộng bằng cách cho phép các nút trong kiến trúc có thể được đặt tại những điểm chiến lược trong mạng. Một vấn đề đáng quan tâm là xây dựng các thuật toán và công cụ tự động cân bằng kiến trúc mạng bằng cách tự sắp đặt lại những vùng lưu trữ đệm và thông tin chứa trong chúng. Một lý do nữa để sử dụng công nghệ mạng tích cực cho việc lưu thông tin đệm web là việc này yêu cầu tính toán động chứ không chỉ là việc lưu trữ thụ động (Ví dụ thống kê việc sử dụng bộ nhớ đệm hay tìm kiếm và sắp đặt bộ nhớ). Từ đó nảy sinh nhu cầu phát triển các kiến trúc hỗ trợ việc lưu trữ đệm tích cực có thể lưu trữ và thực hiện các chương trình sản sinh các trang web đó.

I.2.2 Bảo vệ hệ thống mạng

Bảo vệ thông tin có nghĩa là những thông tin đúng đắn được chuyển đến đúng người vào đúng địa điểm và thời gian. Mặc dù các kỹ thuật an toàn mạng và xác thực đang được đề xuất trên nhiều diễn đàn về mạng [http://www.security-forum.com http://www.cs.utah.edu/flux/janos/], mạng tích cực hiện tại vẫn chưa có một kỹ thuật (được thiết kế và tích hợp) quản lý tất cả các tài nguyên và thông tin truyền qua nó. Bỏ qua sự cần thiết của các hệ thống an toàn, xác thực trên mỗi tầng của giao thức, mạng tích cực cho phép chúng ta xây dựng chính sách an ninh mạng trên cơ sở từng mục tiêu hoặc từng người sử dụng khác nhau.

I.2.3 Quản lý mạng tích cực

Nhiều tác nghiệp trong quản trị mạng bao gồm việc thu thập và cung cấp dữ liệu (như bộ đếm các sự kiện). Để cung cấp thông tin quản trị mạng hữu ích nhất ví dụ xác định các ngoại lệ, các bộ phận thu thập thông tin phải lọc ra những sự kiện không mong muốn. Công nghệ tích cực có thể được sử dụng để cài đặt các phương pháp tiếp cận phức tạp của việc theo dõi và chọn lọc các sự kiện. Các thành phần trong mạng như bộ dẫn đường, có thể tự động theo dõi và tự quản lý chúng bằng cách chuyển một số chương trình quản lý và phân tích tới chạy trên một *láng giềng* gần nhất của chúng (những chương trình này sau đó có thể làm

công việc theo dõi và quản trị). Cũng với cách đó, mạng tích cực có thể cung cấp khả năng cải tiến việc xác định lỗi và cập nhật chính sách quản lý các thiết bị còn khả năng hoạt động sau những thảm hoạ như động đất hay hệ thống bị tấn công.

I.3 Khung cho việc nghiên cứu mạng tích cực

Trong phần này, chúng ta sẽ phân biệt hai cách tiếp cận mạng tích cực (i) riêng biệt và (ii) tích hợp thông qua việc chương trình và dữ liệu được truyền riêng biệt hay tích hợp cùng nhau.

I.3.1 Tiếp cận riêng biệt với các thiết bị chuyển mạch lập trình được

Trong cách tiếp cận này, đầu tiên người sử dụng phải truyền những thủ tục của mình vào các thiết bị dẫn đường, sau đó, người sử dụng có thể truyền những gói tin của mình qua những nút mạng đã được lập trình đó. Khi gói tin được truyền đến một nút mạng, phần đầu điều khiển (header) của nó được đọc và chương trình tương ứng được tách ra để thực hiện với dữ liệu chứa trong gói tin đó. Việc cho phép tải mã chương trình (code) và thực hiện trên các thiết bị dẫn đường rất có ích cho việc mở rộng khả năng của các thiết bị dẫn đường đó, ngay cả khi những chương trình được tải không thực hiện các công việc tính toán của ứng dụng hay của người dùng. Trên mạng Internet, quản trị viên có thể để một số "back door" thông qua đó, anh ta có thể tải chương trình và thực hiện trên thiết bị. Tất nhiên trong nhiều trường hợp, những backdoor này phải cung cấp những cơ chế xác thực tối thiểu và đôi khi có khả năng thực hiện một số kiểm tra trên những chương trình được tải và thực hiện.

I.3.2 Tiếp cận tích hợp thông qua đóng gói thông tin (capsule)

Một cách nhìn khác về mạng tích cực là mỗi thông điệp đều là một chương trình. Mỗi thông điệp hay gói tin chuyển qua các nút chứa một đoạn chương trình (hoặc ít nhất là một câu lệnh) nào đó và có thể chứa cả dữ liệu. Khi một gói tin được truyền đến một nút mạng tích cực, nội dung của nó được thực hiện.

Những bit thông tin nhận được ở liên kết vào được thực hiện bởi một cơ chế xác nhận gói tin, có thể sử dụng ngay việc đóng gói frame trong các giao thức tầng link cho việc này. Nội dung của gói tin sẽ được lưu vào các một môi trường thực hiện tạm thời và chạy ở đó. Các chương trình được xây dựng bởi các câu lệnh thực hiện các tính toán đơn giản trên nội dung của gói tin, đôi khi chúng có thể gọi các hàm nguyên thuỷ để truy cập vào các tài nguyên bên ngoài môi trường tạm mà chúng đang chạy. Kết quả của việc thực hiện có thể là gửi một hoặc nhiều gói tin ở đường kết nối ra hay làm thay đổi những trạng thái của nút mạng.

I.3.3 Xây dựng một mô hình lập trình chung

Các chương trình mạng phải truyền qua hạ tầng truyền thông, nạp và chạy trên các hệ thống nền khác nhau. Điều này đòi hỏi một mô hình phát triển chung cho (i) mã hoá chương trình trên mạng, (ii) các hàm nguyên thuỷ được tích hợp trong mỗi nút mạng, và (iii) quản lý tài nguyên trên nút mạng.

Mã hoá chương trình phải hỗ trợ các tính chất

- Di trú: khả năng truyền và thực hiện chương trình trên các hệ thống nền khác nhau An toàn: khả năng giới hạn những tài nguyên mà chương trình có thể truy cập
- Hiệu năng: khả năng thực hiện các điều trên mà không gây ảnh hưởng tới hiệu suất của mạng ít nhất là trong các trường hợp thông thường.

Di trú có thể thực hiện trên nhiều mức của ứng dụng: (i) thể hiện chương trình bằng một ngôn ngữ scripting mức cao ví dụ Tcl; (ii) chấp nhận một hệ thống nền độc lập, thông thường, ví dụ mã byte-code của Java; hoặc (iii) truyền chương trình dưới dạng nhị phân ví dụ Omniware. Thông thường, ba (3) cách tiếp cận trên đều có ích trong một số trường hợp: mã hoá nguồn hỗ trợ việc xây dựng nhanh các nguyên mẫu; mã độc lập phù hợp với việc cung cấp các chương trình ngắn; và các đoạn mã dùng chung phù hợp với việc thể hiện trên mức object-code.

I.4 Các nghiên cứu hiện tại

Các hướng nghiên cứu mạng tích cực đang được thực hiện một cách tương đối độc lập nhau bởi nhiều nhóm nghiên cứu khác nhau và chủ yếu tập trung vào các hướng: (i) xây dựng các kiến trúc bộ chuyển mạch lập trình được; (ii) xây dựng các công nghệ mới; (iii) định nghĩa các kỹ thuật; (iv) bàn luận về các hệ thống cuối; và (v) các ứng dụng quản trị mạng, di trú, quản lý tắc nghẽn mạng.

I.4.1 Massachusetts Institue of Technology

Nhóm nghiên cứu của MIT đang xây dựng nguyên mẫu cho một kiến trúc dựa trên cách tiếp cận bao gói và nghiên cứu trao đổi các vấn đề liên quan đến việc định nghiã các thành phần (i) lưu trữ, (ii) multicast, và (iii) bộ lọc thông tin mạng. Họ đã xây dựng các ứng dụng thử nghiệm kiến trúc bao gói trên hệ thống Linux sử dụng câc bao gói viết trên nền Java. Các công nghệ mới như mở rộng hệ điều hành, và biên dịch khi chạy cũng đang được nghiên cứu. Các thành phần tải xuống chạy và nhớ đệm đang được phát triển để hỗ trợ các chương trình nhỏ nhằm giảm thiểu các thành phần dư thừa trong việc truyền và thực hiện chúng trên mạng.

I.4.2 University of Pennsylvania

Một cách tiếp cận theo hướng xây dựng các thiết bị chuyển mạch lập trình được cho phép các đoạn mã đã được kiểm tra và xác thực được tải xuống các nút mạng đang được thực hiện trong dự án có tên là SwitchWare. Thiết bị chuyển mạch được trừu tượng hoá như một máy Turing. Cách tiếp cận này sử dụng một phương pháp luận hình thức để chứng minh các tính chất an toàn của các chương trình SwitchWare. Cách tiếp cận này đang được thử nghiệm với các nguyên mẫu dựa trên hệ thống đa bộ vi xử lý chia sẻ bộ nhớ. Các ứng dụng được xây dựng dựa trên cách tiếp cận này là: Phần mềm mở rộng giải thông dựa trên kỹ thuật chung cho việc hợp, tách kênh ví dụ phân tải mạng; và hỗ trợ mô hình gói tin tích cực ("Switchlets").

I.4.3 Bell Communication Research

Bell đang hợp tác nghiên cứu một số khía cạnh của thiết kế Penn sử dụng một kiến trúc khác (OPCV2) để mở rộng nghiên cứu. Thuật toán đa thành phần của SwitchWare và chác chức năng run-time hệ thống nhằm mục tiêu gắn kết vào các cổng điều khiển của một bộ chuyển mạch lớn đang được nghiên cứu. Định nghĩa về mặt ngữ nghĩa của một thiết bị dẫn đường tích cực đang dần dần hình thành từ kết quả nghiên cứu về ngữ nghĩa và sự cộng tác giữa các nguyên mẫu được phát triển bởi Penn. Bell còn nghiên cứu những kiến trúc mạng mới như Self-Paying Information Transport, trong đó, thông tin thanh toán điện tử được gắn kết vào các gói tin tích cực.

I.4.4 Columbia University

Dự án Netscript kết hợp một ngôn ngữ lập trình và môi trường thực thi đang được tiến hành tại đại học Columbia. Ngôn ngữ Netscript cung cấp một cách để kết hợp các xử lý của các dòng gói tin trên mạng. Các agent Netscript có thể được gửi đến các hệ thống ở xa như thiết bị dẫn đường và thiết bị chuyển mạch. Mục đích của dự án là xây dựng môi trường lập trình cho các nút mạng như đã xây dựng cho các hệ thống cuối.

I.4.5 Carnegie Mello University

Cơ chế quản lý tài nguyên hỗ trợ mạng "application-aware" đang được xây dựng bởi nhóm CMU. Ba (3) hướng của việc quản lý tài nguyên bao gồm: (i) kiến trúc vật lý, bao gồm chức năng xử lý và lưu trữ; (ii) những quyết định được thực hiện trong các khoảng thời gian khác nhau từ khi ứng dụng được khởi động đến các gói tin và việc lập lịch các tiến trình; và (iii) việc chia sẻ kiến trúc giữa các thực thể trong tổ chức đang được quan tâm. Các ứng dụng phức tạp, nhiều thành phần như hội thảo video và khai phá dữ liệu sử dụng nhiều luồng thông tin với nhiều tính chất khác nhau cũng đang được tìm hiểu.

I.4.6 Các nghiên cứu khác

Một số cơ quan khác nghiên cứu về mạng tích cực có thể kể đến là:

- Tại viện nghiên cứu công nghệ BBN Technology, các vấn đề về khả năng lập trình, từ điển dữ liệu, và cơ chế xác thực trong phạm vi giao thức IP đang được xem xét.
- Tại Viện nghiên cứu công nghệ Georgia, các khái niệm về mạng tích cực đang được áp dụng vào việc giải quyết vấn đề tắc nghẽn mạch bằng cách cho phép các ứng dụng yêu cầu các nút mạng thực hiện các giải thuật đặc biệt như nén không mất thông tin, loại bỏ có lựa chọn... khi mạng gặp sự cố nghẽn mạch.
- Tại đại học Kansas, ứng dụng của công nghệ tích cực để triển khai mạng radio đang được quan tâm.
- Tại đại học Arizona, một phần mềm "liquid" một trong những thành phần của công nghệ mã di trú đang được phát triển.
- Tại đại học Cincinatti, các công nghệ định nghĩa các chuẩn mực cho các thành phần của mạng đang được nghiên cứu.

I.5 Kết luận chương I

Mạng tích cực kéo theo sự tổng hợp và mở rộng của ngôn ngữ lập trình, hệ điều hành và tài nguyên mạng. Các ứng dụng có thể sử dụng các thành phần của giao thức trong chồng giao thức có thể được định nghĩa và xây dựng nhằm thực hiện các chức năng chuyên biệt của các ứng dụng. Điều này có thể dẫn đến khả năng tăng mức độ phức tạp của các tính toán trên mạng giúp người sử dụng (hoặc chuyên gia phát triển) thực hiện các ứng dụng của mình một cách sáng tạo, nhanh chóng, mềm dẻo.

Hiện tại các ứng dụng sử dụng công nghệ mạng tích cực chưa nhiều, thông thường là các ứng dụng cài đặt *caching* tuy nhiên với việc phát triển của các công cụ (như ANTS), trong tương lai sẽ có nhiều ứng dụng được phát triển và được sử dụng rộng rãi trong cuộc sống hiện đại.

CHƯƠNG II. KIẾN TRÚC MẠNG TÍCH CỰC VÀ BỘ CÔNG CỤ ANTS

Trong chương này, chúng tôi tập trung mô tả kiến trúc mạng tích cực được DARPA đưa ra. Sau đó tìm hiểu bộ công cụ ANTS và khả năng ứng dụng của bộ công cụ này trong việc xây dựng và triển khai các ứng dụng trên mạng tích cực.

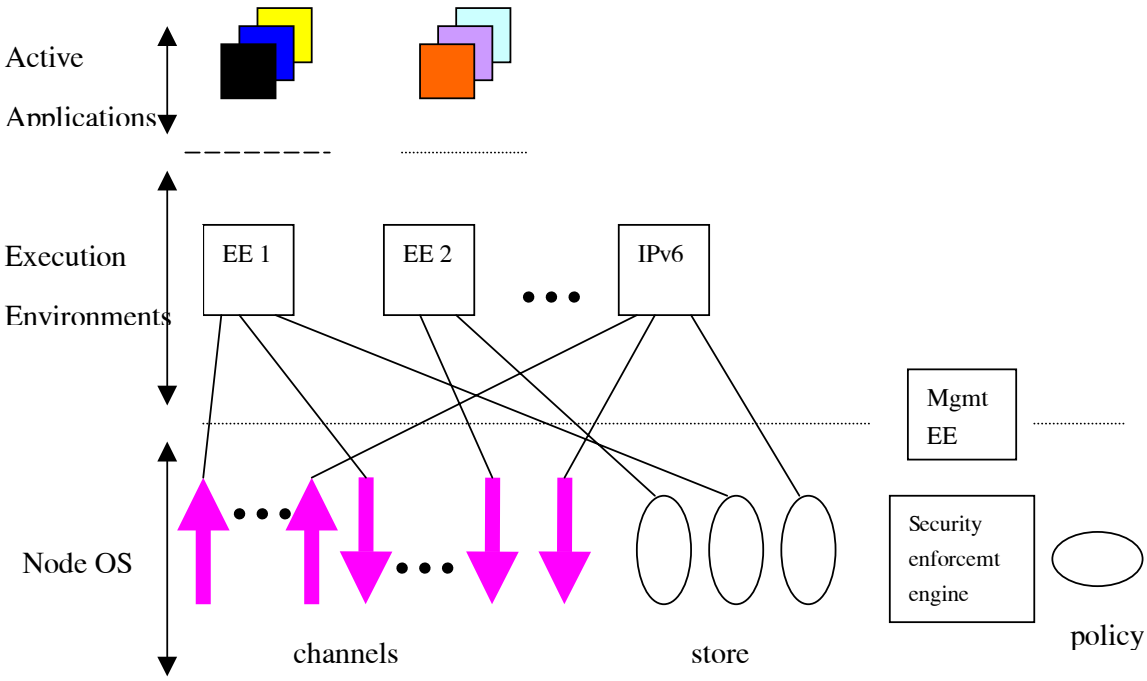
II.1 Kiến trúc mạng tích cực của DARPA

Phần này tập trung vào việc giới thiệu kiến trúc mạng tích cực được tiểu ban nghiên cứu mạng tích cực của DARPA (sau đây sẽ được gọi tắt là kiến trúc) đưa ra. Kiến trúc này đã được trình bày trong những hội thảo tại Tucson (tháng 3 năm 1998), Atlanta (tháng 7 năm 1998), New York (tháng 11 năm 1998) và được thảo luận trong nhóm tin "ActiveNets Wire" [http://www.security-forum.com]. Chúng tôi tập trung vào việc trình bày những thành phần cơ bản của kiến trúc, những giao diện chính liên kết các thành phần, và những thuận lợi cho việc xây dựng những thiết bị dẫn đường hoặc chuyển mạch có hiệu suất cao sử dụng những công nghệ mới dựa trên kiến trúc này.

II.1.1 Các thành phần cơ bản của kiến trúc

Chức năng của nút mạng tích cực được thực hiện trên các thành phần của nút bao gồm (i) hệ điều hành nút (Node Operating System - sau đây sẽ được viết tắt là NodeOS), (ii) các môi trường thực hiện (Execution Environments - sau đây sẽ được viết tắt là EEs), và những ứng dụng tích cực (Active Applications - sau đây sẽ được viết tắt là AAs).

Mỗi EE cung cấp một giao diện lập trình (hay còn gọi là máy ảo) có thể được lập trình hoặc điều khiển bằng cách gửi các gói tin đến nó. Như vậy, có thể coi EE là một chương trình vỏ (hiểu theo khái niệm shell trong hệ điều hành UNIX) cung cấp một giao diện cho phép người sử dụng truy cập đến các dịch vụ mạng. Kiến trúc cho phép nhiều EE cùng tồn tại trên một NodeOS. Tuy nhiên trong việc cài đặt và triển khai, người ta cố gắng giảm thiểu số EE khác nhau trên một nút mạng tại cùng một thời điểm.



Hình 4. Các thành phần của kiến trúc

NodeOS cung cấp các hàm cơ bản cho các EE sử dụng để xây dựng các dịch vụ của mình cung cấp cho các AA, điều này phù hợp với nguyên tắc phân lớp [1]. NodeOS quản lý tài nguyên của nút mạng tích cực bao gồm (i) truyền thông, (ii) tính toán, (iii) lưu trữ; và dàn xếp việc chia sẻ những tài nguyên đó giữa các EE. Như vậy NodeOS giúp chúng ta tách EE khỏi việc quản lý tài nguyên và tránh việc ảnh hưởng lẫn nhau giữa các EE đang cùng hoạt động trên một NodeOS.

Khi EE yêu cầu dịch vụ từ NodeOS, yêu cầu đó có thể được đính kèm một số định danh sử dụng cho việc xác định độ ưu tiên của yêu cầu đó. Độ ưu tiên này có thể là chính EE hay của một ứng dụng bên ngoài nhân danh EE yêu cầu dịch vụ để thực hiện một ứng dụng tích cực. NodeOS chuyển thông tin định danh cho bộ phận an toàn (security engine) để kiểm tra tính đúng đắn của định danh dựa vào chính sách an toàn của nút và thực thi dịch vụ khi thông tin chứa trong yêu cầu phù hợp với chính sách của nút.

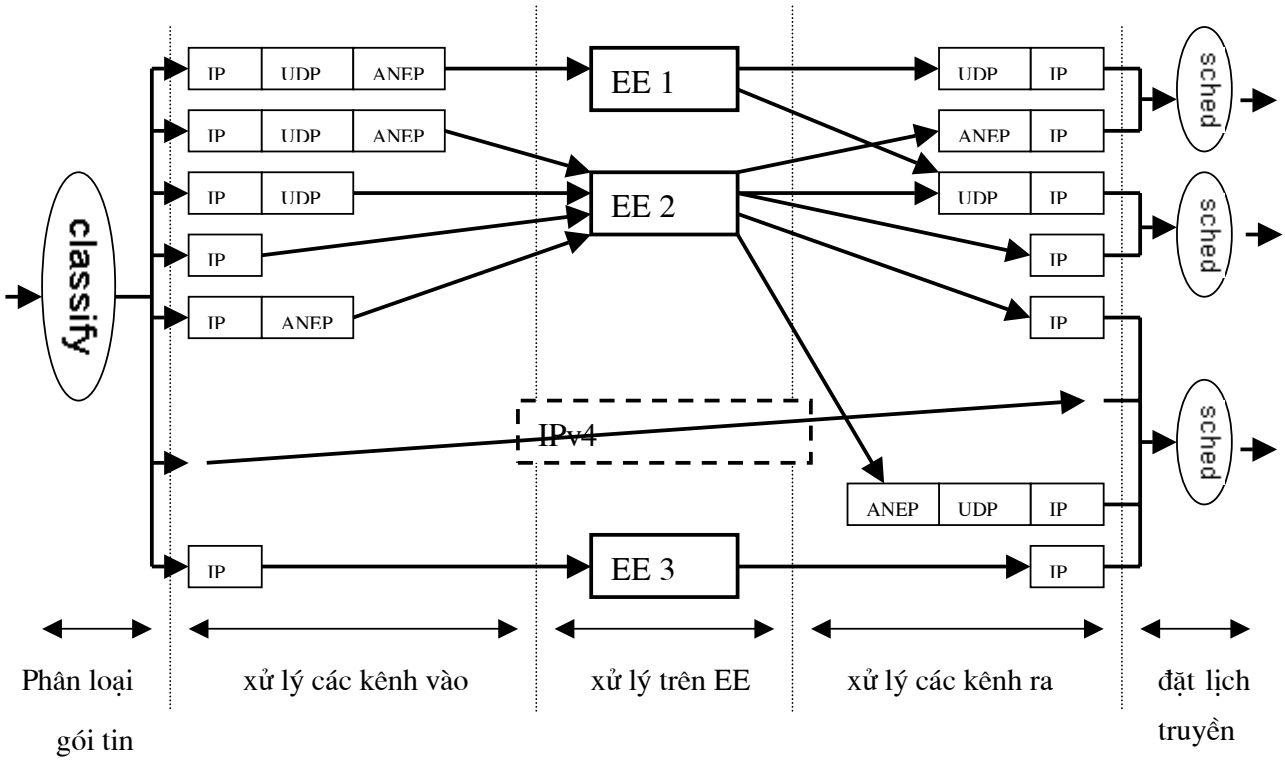
Mỗi nút có một môi trường thực hiện quản lý riêng quản lý cấu hình và chính sách của nút. Một số chức năng quản lý và điều khiển có thể được thực hiện thông qua EE quản lý bao gồm: (i) Duy trì cơ sở dữ liệu về chính sách an toàn củ

nút, (ii) tải EE mới hoặc cập nhật cấu hình của các EE đang tồn tại, (iii) hỗ trợ các dịch vụ quản trị. Những chức năng quản trị được thực thi thông qua việc gửi gói tin đến EE phải được đảm bảo an toàn thông qua việc mã hoá và tuân thủ theo chính sách an toàn của nút được lưu trong cơ sở dữ liệu chính sách.

II.1.2 Quá trình xử lý các gói tin

Các môi trường thực hiện gửi nhận các gói tin thông qua các kênh. NodeOS cài đặt các kênh này sử dụng nhiều công nghệ khác nhau từ các công nghệ lớp dưới [1] như Ethernet, ATM đến các công nghệ lớp cao như TCP, UDP hay IP.

Khi một kết nối vật lý nhận được gói tin, nó phân loại (classify) gói tin dựa trên thông tin điều khiển (có thể chứa trong header của gói tin); quá trình phân loại này xác định kênh vào và giao thức tính toán phù hợp để chuyển gói tin tới. Việc phân loại được điều khiển bởi các mẫu được định nghĩa sẵn trong EE.



Hình 5. Xử lý các gói tin qua nút mạng tích cực

Thông thường, EE yêu cầu tạo các kênh để truyền các gói tin với những thông số về công nghệ truyền tin nó sử dụng ví dụ kiểu Ethernet (802.1, Ethernet II...) hay

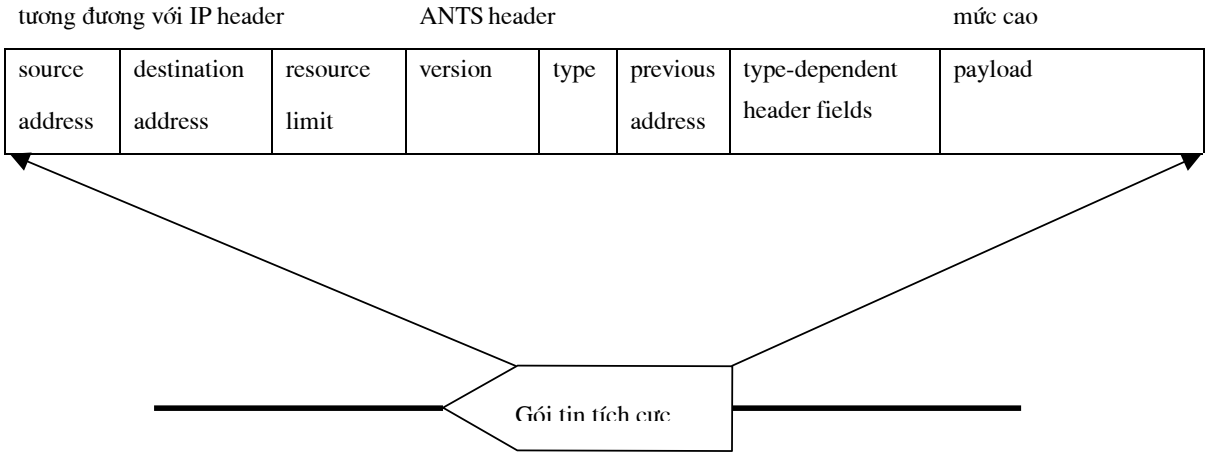
giao diện socket [1] (sự kết hợp giữa địa chỉ IP và cổng TCP); yêu cầu này có thể phục vụ cho chính EE hoặc được sử dụng cho các AA chạy trên nó. Sau khi được xử lý tại các kênh vào, gói tin được truyền cho EE (hoặc có thể lưu vào bộ đệm). Trong hình 5, EE 1 nhận được gói tin ANEP (Active Network Encapsulation Protocol - xem phần giao thức đóng gói tin mạng tích cực) được đóng gói trong gói tin UDP (UDP datagram) cùng một số hiệu cổng đích. EE 2 cũng nhận được gói tin UDP chứa ANEP (có thể có số hiệu cổng khác hoặc kiểu ANEP khác), một gói tin ANEP chứa trong gói tin IP (IP packet) và những gói tin IP phù hợp các mẫu chứa trong EE (các mẫu này có thể là số hiệu của giao thức [1] hoặc những cặp địa chỉ nguồn/đích định sẵn). Nhiệm vụ của NodeOS và security engine là số định danh chứa trong yêu cầu được phép truy cập đến các gói tin phù hợp với mẫu được gắn với kênh truyền thông được tạo ra. Những gói tin nhận được không phù hợp với các mẫu bị loại bỏ (Cơ chế này làm việc giống như cơ chế access list mô tả trong Cisco www.cisco.com).

Tại đầu ra, EE truyền các gói tin bằng cách chuyển chúng tới kênh ra, tại đây, chúng được đóng gói với giao thức tương ứng và lập lịch cuối cùng, chúng có thể được truyền qua các kết nối. Như vậy, thông thường quá trình xử lý trải qua các bước: (i) nhận gói tin từ mạng, (ii) phân loại, (iii) tách gói, (iv) xử lý trên EE/AA, (v) đóng gói, (vi) lập lịch, và cuối cùng là (vii) truyền gói tin đến nút tiếp theo. Chú ý rằng một (1) gói tin truyền một gói tin có thể không tương ứng với bất kỳ gói tin đến nào như chúng ta đã thấy ở phần trên, EE có thể sinh ra các gói tin trong quá trình thực hiện các mã lệnh.

NodeOS còn cung cấp khả năng phân cấp tài nguyên cho việc tính toán và truyền thông của nút. Bằng các cơ chế lập lịch, NodeOS phân việc truyền thông thành các lớp khác nhau, nhờ đó tránh được việc ảnh hưởng qua lại giữa việc truyền thông của các lớp. Ví dụ NodeOS có thể ngăn chặn trường hợp các EE lỗi sử dụng tất cả tài nguyên tính toán của nút. Chúng còn có thể thực hiện một số dịch vụ phức tạp khác như hạn chế thông lượng sử dụng cho việc tính toán cũng như truyền thông, hay các dịch vụ "công bằng" các kênh vào thường được lập lịch với việc lưu tâm tới tính toán, trong khi các kênh ra lại phải lập lịch với cả tính toán và truyền thông, điều này chia thông lượng không cân bằng giữa các lớp.

II.1.3 Giao thức đóng tói tin trong mạng tích cực

Trong một số trường hợp, người sử dụng phải có khả năng điều khiển việc dẫn đường các gói tin đến một (1) EE cụ thể. Giao thức đóng gói tin mạng tích cực (Active Network Encapsulation Protocol - ANEP) cung cấp khả năng này.



Hình 6. Ví dụ cài đặt ANEP trong ANTS

Trong header của ANEP chúng ta chú ý đến trường "type", trường này mang định danh của EE (hiện tại, số định danh này được cung cấp bởi Active Network Assigned Number Authority). Nếu một EE tồn tại trên một nút mạng tích cực, một gói tin chứa ANEP header (đóng gói trong các gói tin của công nghệ mạng hỗ trợ) với định danh type sẽ được dẫn đường đến kênh vào tương ứng với EE đó, kênh ngầm định được tạo ra khi EE khởi động.

Gói tin không chứa ANEP header cũng có thể được xử lý trên các EE bằng cách cung cấp các kênh riêng, EE có thể hỗ trợ việc xử lý các thông tin "kiểu cũ" trong mạng. Một ví dụ trong hình 5 là EE-giả cung cấp việc truyền tin sử dụng IPv4. Một ví dụ khác là những EE cung cấp khả năng nâng cao dịch vụ TCP.

ANEP còn cung cấp phương thức vận chuyển cho những truyền thông khác cùng với NodeOS bao gồm:

- Thông tin sửa lỗi: Khi một gói tin không đến được EE đích (trường hợp EE không được hỗ trợ bởi nút hoặc không đủ tài nguyên để thực hiện), ANEP cho

phép người sử dụng yêu cầu NodeOS thực hiện một số chức năng sửa lỗi tương ứng như: xoá gói tin, cố gắng gửi lại hoặc thông báo lỗi. Việc thông báo lỗi sử dụng đến trường địa chỉ trong ANEP header.

- Đảm bảo an toàn: trong thực tế, không phải mọi nút mạng tích cực đều lưu trữ các thông tin (như public key) để xác thực tất cả các gói tin truyền qua nó. Thường thì các gói tin chỉ được xác thực một lần tại nút mạng sinh ra nó trước khi nó được gửi lên mạng, sau đó, việc xác thực được được thực hiện sử dụng cơ chế chia sẻ key giữa các nút mạng được kết nối với nhau. ANEP header có thể chứa những thông tin uỷ nhiệm giữa các nút.

Mạng tích cực chứa các hệ thống mạng cuối phục vụ các ứng dụng của người dùng và các hệ thống trung gian thông thường làm nhiệm vụ chuyển mạch các gói tin đồng thời xử lý/biên dịch/thực hiện chúng trên đường truyền. Tính năng chính phân biệt mạng tích cực và mạng internet chính là việc tồn tại các chức năng tính toán đặc biệt (AA) trên các nút trung gian trên mạng. Như vậy cả các hệ thống cuối và các hệ thống trung gian đều bao gồm các thành phần NodeOS, EE và AA.

II.1.4 Môi trường thực hiện và các ứng dụng tích cực

Một môi trường thực hiện (EE) định nghĩa một máy ảo và một giao diện lập trình có thể được điều khiển bằng cách gửi các mã lệnh tới EE thông qua các gói tin. Chức năng của máy ảo không được định nghĩa cụ thể trong kiến trúc; NodeOS cung cấp bộ các hàm cho phép các EE cài đặt các máy ảo. Một số EE cài đặt máy ảo chung cung cấp khả năng lập trình để mô phỏng lại các máy ảo khác, trong khi một số EE khác cài đặt một số giao diện chương trình hạn chế chỉ cho phép người sử dụng thực hiện với một số tham số giới hạn trước.

Một ứng dụng tích cực (AA) là một chương trình được thực hiện trên một (1) máy ảo của một (1) EE xác định, cung cấp dịch vụ *end-to-end*. Như vậy, thông qua việc sử dụng các giao diện lập trình của EE, AA cài đặt các dịch vụ tuỳ biến cho ứng dụng của người sử dụng. Cách tải mã lệnh sử dụng cho AA được xác định bởi EE, mã lệnh có thể chứa trong gói tin (in-band), được tải trong một pha riêng (out-of-band) hoặc tải xuống khi cần (on-demand) khi gói tin được truyền tới;

việc tải mã lệnh có thể được làm tự động hoàn toàn (ví dụ khi câu lệnh trong gói tin gọi đến một hàm không chứa sẵn trong nút mạng nhưng được lưu trên một hệ thống phân phát mã - xem chương 1) hoặc được điều khiển theo một cách nào đó.

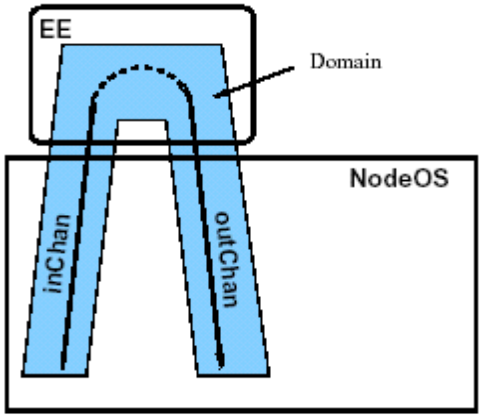
Như vậy, người sử dụng có thể lập trình mạng tích cực cũng như việc họ có thể lập trình trên máy tính cá nhân (PC) của mình. Tuy nhiên, để đảm bảo an toàn cho hệ thống mạng, các ứng dụng chạy trên các hệ thống cuối chỉ nên truy cập đến các dịch vụ mạng tích cực bằng cách gọi các AA với mã lệnh được cung cấp bởi các nhà phát triển AA.

II.1.5 Hệ điều hành mạng NodeOS

NodeOS là lớp trung gian giữa EE và kiến trúc vật lý phía dưới (bao gồm môi trường truyền thông, năng lực xử lý và thiết bị lưu trữ). Lớp này hỗ trợ cho việc các EE cùng tồn tại và cùng hoạt động đồng thời trên một nút mạng, đảm bảo an toàn mức cơ bản cho các EE, và cung cấp các dịch vụ cơ bản yêu cầu trên mọi nút mạng. Những chức năng cơ bản được cung câp bao gồm: thiết lập các kênh tryền thông phục vụ cho việc truyền các gói tin tới các mạng phía dưới, dẫn đường các gói tin giữa các kênh và các EE trong một nút mạng, quản lý việc truy cập đến các tài nguyên của nút mạng.

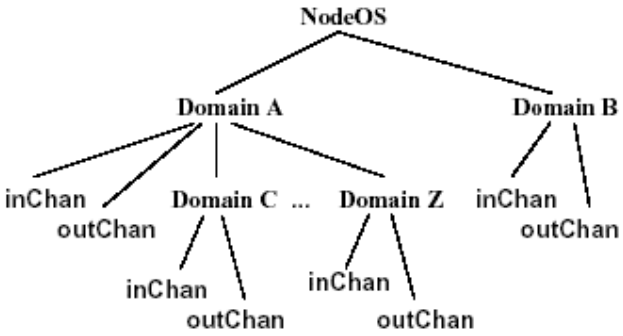
NodeOS định nghĩa năm thành phần cơ bản: (i) vùng xử lý (thread pools - thông thường là một số chu kỳ CPU) (ii) vùng nhớ (memory pool), (iii) kênh truyền thông (channel), (iv) hệ thống lưu trữ file, và thành phần cuối (v) là sự kết hợp giữa việc điểu khiển, lập lịch của bốn thành phần trên thành một cấu trúc gọi là domain (sau đây sẽ được gọi là domain).

Bốn thành phần đầu tương ứng với các thành phần trong các hệ điều hành thông thường khác. Thành phần cuối (trong một số tài liệu sử dụng khái niệm ***flow***) là một thành phần trừu tượng bao gồm việc quản trị điều khiển và lập lịch hệ thống. Trong đó, mỗi domain chứa những tài nguyên cần thiết cho việc truyền các gói tin. Thông thường những tài nguyên đó bao gồm: (i) một tập các kênh làm nhiệm vụ gửi và nhận các gói tin, (ii) một vùng bộ nhớ và (iii) một vùng xử lý. Gói tin tích cực tới một kênh vào (inChan) được xử lý bởi EE sử dụng bộ nhớ và năng lực xử lý được phân chia cho domain sau đó được truyền ra trên kênh ra (outChan).



Hình 7. Domain bao gồm các kênh, bộ nhớ, năng lực xử lý cần thiết cho EE

Chúng ta có thể thấy rằng xét về khía cạnh quản lý bộ nhớ và năng lực xử lý CPU, một domain có những nét tương đồng với một tiến trình người sử dụng trong hệ điều hành UNIX. Tuy nhiên, nếu xét trên quan điểm quản lý tài nguyên trên các kênh truyền thông, domain làm việc ở nhiều mức khác nhau với cả những công nghệ mạng lớp hai và những công nghệ mạng lớp cao.



Hình 8. Kiến trúc domain

Một điểm tương đồng nữa của domain và process là các domain có thể sinh các domain con (giống như việc các tiến trình sử dụng lời gọi `fork()` trong hệ điều hành UNIX). Các domain con cũng được NodeOS cung cấp tài nguyên dựa trên định danh của nó trong hệ thống (tương ứng với processID) tài nguyên đó không ảnh hưởng tới domain đã sinh ra nó.

II.2 Bộ công cụ ANTS

Trong phần đầu của chương 2, chúng ta đã xem xét kiến trúc của một mạng tích cực và chức năng của các thành phần chính trong mạng tích cực. Phần này tập trung giới thiệu một cách tiếp cận để xây dựng và triển khai các giao thức sử dụng bộ công cụ ANTS (Active Network Transport System). Bộ công cụ này được viết trên ngôn ngữ lập trình Java và cung cấp một khung bao gồm các lớp được cài đặt giúp người sử dụng dễ dàng phát triển các dịch vụ mới của mình. Mỗi nút mạng và các ứng dụng của nó chạy trên một máy ảo Java (Java Vitual Machine - JVM) giống như những tiến trình người sử dụng chạy trên hệ điều hành UNIX. Bộ công cụ không được xây dựng như việc mở rộng các thành phần của bộ giao thức TCP/IP mà như một lớp mạng hoàn chỉnh sử dụng các dịch vụ cung cấp bởi các thư viện chuẩn của Java.

II.2.1 Các thành phần trong kiến trúc dựa trên ANTS

Mạng xây dựng trên cơ sở ANTS chứa một nhóm các nút mạng được kết nối với nhau, trên các nút mạng này, thành phần runtime của ANTS được thực hiện; các nút có thể được kết nối thông qua mạng nội bộ (LAN), mạng diện rộng (WAN), các kết nối điểm điểm hoặc các kênh chia sẻ. Hệ thống xây dựng trên các dịch vụ lớp liên kết (về các lớp trong mô hình tham chiếu OSI [1]) để cung cấp dịch vụ lớp mạng cho các ứng dụng phân tán. Các ứng dụng khác nhau có thể đưa các giao thức mới vào trong mạng bằng cách định nghĩa các thủ tục chạy trên các nút mạng mà các gói tin truyền qua.

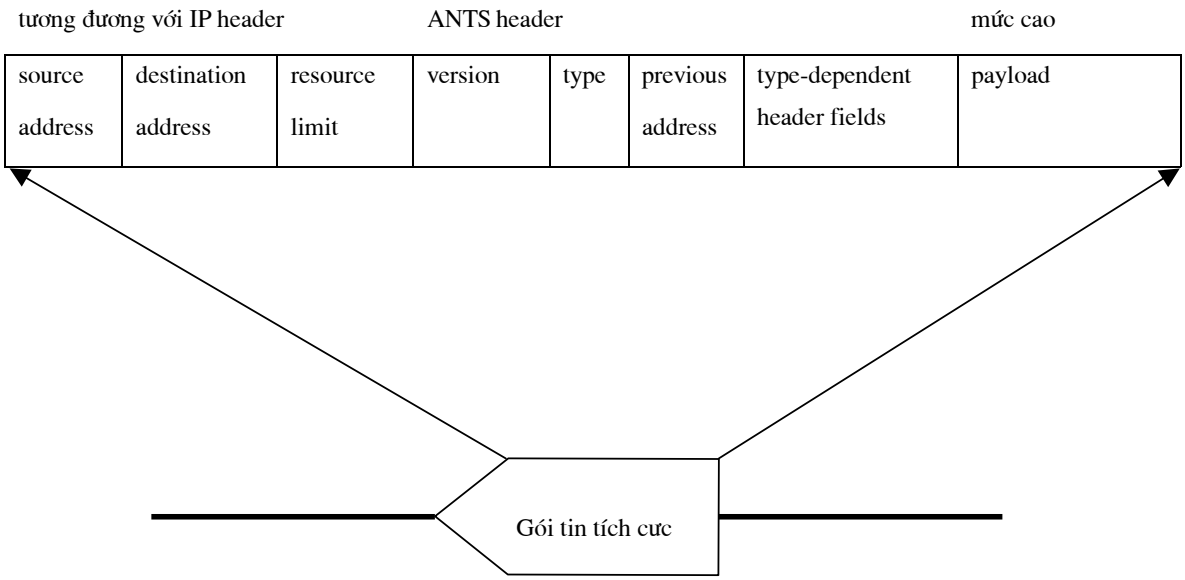
Kiến trúc xây dựng dựa trên bộ công cụ ANTSbao gồm các thành phần sau:

- Mô hình lập trình mạng tích cực trong đó định nghĩa về các gói tin trong các mạng thông thường được thay thế bởi các *capsule* (sau đây sẽ sử dụng thuật ngữ gói tin tích cực) trong đó chứa các chỉ dẫn về các chương trình sẽ được thực hiện.
- Một cơ chế phân phát mã cho phép các chương trình được phân phát tự động đến những nút mạng cần đến chúng.

- Các *nút mạng tích cực* đóng vai trò thực hiện các chương trình và duy trì trạng thái của chúng.

II.2.2 Kiến trúc gói tin

Kiến trúc gói tin được trình bày trong hình xxx bao gồm các trường



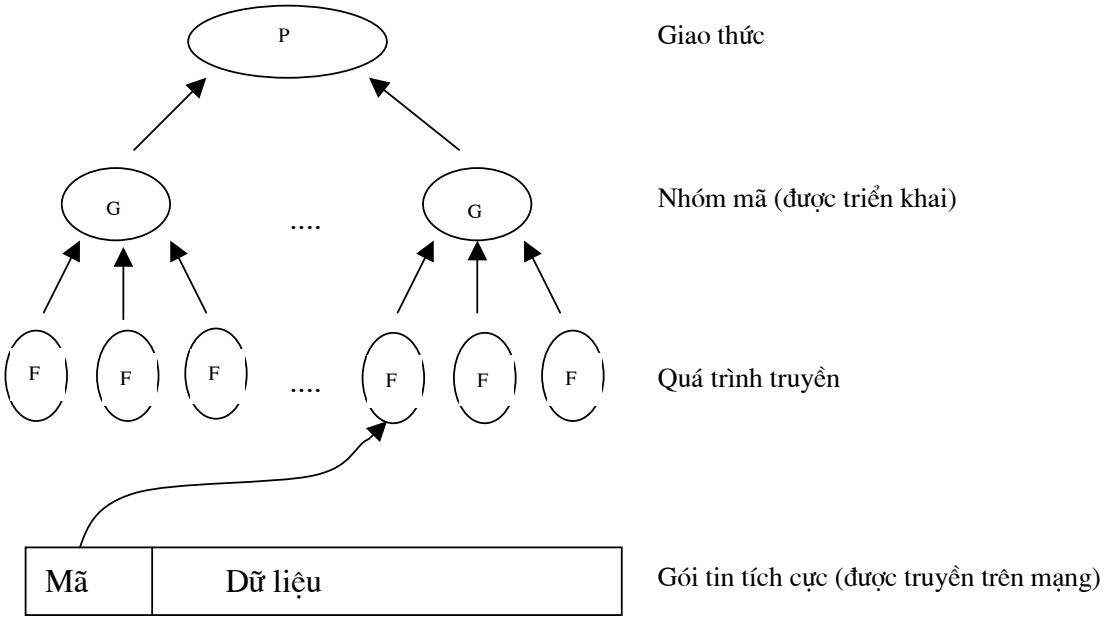
Hình 9. Kiến trúc capsule trong ANTS

- Địa chỉ nguồn và địa chỉ đích (source/destination address): tương tự như địa chỉ IP.
- Giới hạn tài nguyên (resorce limit): tương tự trường TTL (Time to Live) trong IPv4 va hop count trong IPv6.
- Phiên bản (version number): số phiên bản của ANTS.
- Kiểu (type): định danh thủ tục truyền gói tin, sử dụng cùng code group và protocol.
- Những trường khác có kiểu và độ dài tuỳ thuộc vào kiểu của gói tin.
- Dữ liệu: chứa dữ liệu của lớp trên không sử dụng cho việc tính toán trên mạng.

Việc phân chia đầu của gói tin thành hai phần (i) tương ứng với IP và (ii) phần riêng của ANTS cho phép các gói tin được truyền qua các thiết bị chuyển mạch

thông thường không hỗ trợ mạng tích cực. Tại các nút đó, việc truyền các gói tin tích cực được thực hiện như đối với các gói tin IP thông thường. Như vậy, có thể cài đặt ANTS header như một header của lớp cao hơn hoặc sử dụng phần mở rộng của IP header với cờ option trong IP header. Điều này cho phép kết hợp ANTS với IP để tránh việc phải cài đặt thêm những lớp khác và tận dụng những dịch vụ do IP cung cấp.

Trong phần đầu của gói tin ANTS, trường quan trọng nhất là type, trường này chỉ ra thủ tục sử dụng để truyền gói tin và nhóm mã, giao thức gói tin đó phụ thuộc.



Hình 10. Quan hệ giữa các thành phần

II.2.3 Hệ thống phát tán mã

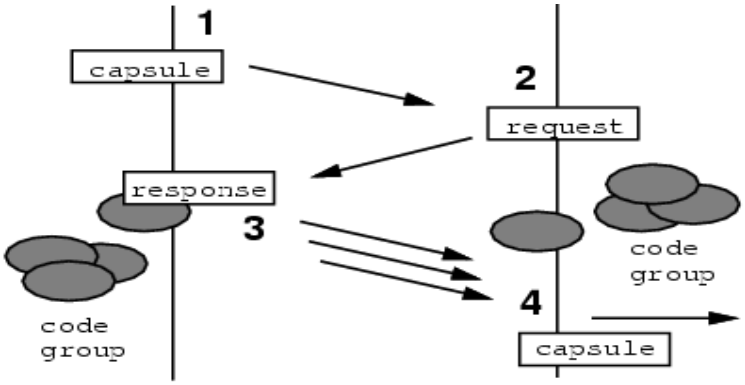
Một khi dịch vụ mới được phát triển sử dụng các gói tin tích cực, nó cần được triển khai trên toàn bộ kiến trúc mạng trước khi nó được sử dụng. ANTS cung cấp một cơ chế phát tán mã có tên gọi là *nạp khi cần* (pull demand) cho các ứng dụng sử dụng dịch vụ mới đó.

Hệ thống phát tán mã trong ANTS được thiết kế để truyền các đoạn mã sử dụng cho việc cài đặt các dịch vụ mới trên đường truyền của các gói tin. Những đoạn mã đó được lưu trữ tại các nút mạng đó để sử dụng trong tương lai. Hệ thống truyền các đoạn mã ngắn để sử dụng các dịch vụ tải nhẹ và truyền không kết nối

đảm bảo việc truyền mã sảy ra nhanh chóng và trong suốt đối với các ứng dụng. Trong trường hợp không truyền được mã tới nút yêu cầu, gói tin tích cực coi như bị mất và ứng dụng sẽ truyền lại gói tin đó theo cách thông thường. Kinh nghiệm làm việc với ANTS cho thấy các nhóm mã cho các dịch vụ nên được giữ ở mức nhỏ nhất có thể, thông thường nhỏ hơn 16KB, đôi khi người ta coi con số này là kích cỡ tối đa của một nhóm mã.

Hệ thống phân tán mã của ANTS được thiết kế để các gói tin có thể chứa mã chương trình trong nó nhưng vẫn đảm bảo hiệu suất cao và tính an toàn khi các đoạn mã đó được tải vào tất cả các nút mạng. Hệ thống được xây dựng dựa trên những mục tiêu sau:

- Thích ứng được với việc thay đổi hình trạng của mạng và lỗi tại các nút.
- Khả năng mở rộng.
- Giảm thiểu số lượng mã phải lưu trữ đệm tại các nút và khoảng cách chúng phải truyền.
- Giảm thiểu thời gian trễ từ khi gói tin nhận được ở nút tới khi các mã tương ứng được nạp. Điều này ảnh hưởng trực tiếp đến độ trễ của việc truyền gói tin.
- Chống lại được việc giả mạo mã và kiểu tấn công từ chối dịch vụ (denial-of-service). Phải đảm bảo không sử dụng được hệ thống phân tán mã để tấn công vào mạng.
- Không gây tắc nghẽn trên mạng.



Hình 11. Hệ thống phân tán mã

Hoạt động của hệ thống phân tán mã được mô tả như sau:

1. Một gói tin được truyền từ một nút mạng tích cực (nút này đã xử lý gói tin do đó, nó có lưu trữ những nhóm mã dùng để xử lý gói tin). Trước khi được gửi đi, thông tin điều khiển trong phần đầu của gói tin chỉ đến địa chỉ của nút mạng gửi gói tin đó.
2. Khi gói tin đến nút tiếp theo, và những nhóm mã dùng để xử lý gói tin đó chưa tồn tại trên nút, một gói tin yêu cầu được sinh ra và gửi lại cho nút trước đó dựa trên thông tin về địa chỉ như đã trình bày ở trên.
3. Khi nút trước đó nhận được yêu cầu, nó sinh ra các gói tin chứa những nhóm mã cần thiết và gửi cho nút tiếp theo.
4. Khi các gói tin chứa mã tới nút đang xử lý gói tin tích cực, chúng được ghép lại và kiểm tra tính đúng đắn. Cuối cùng, nút tiếp theo sử dụng những mã vừa nhận được để truyền gói tin ban đầu.

II.2.4 Nút mạng tích cực

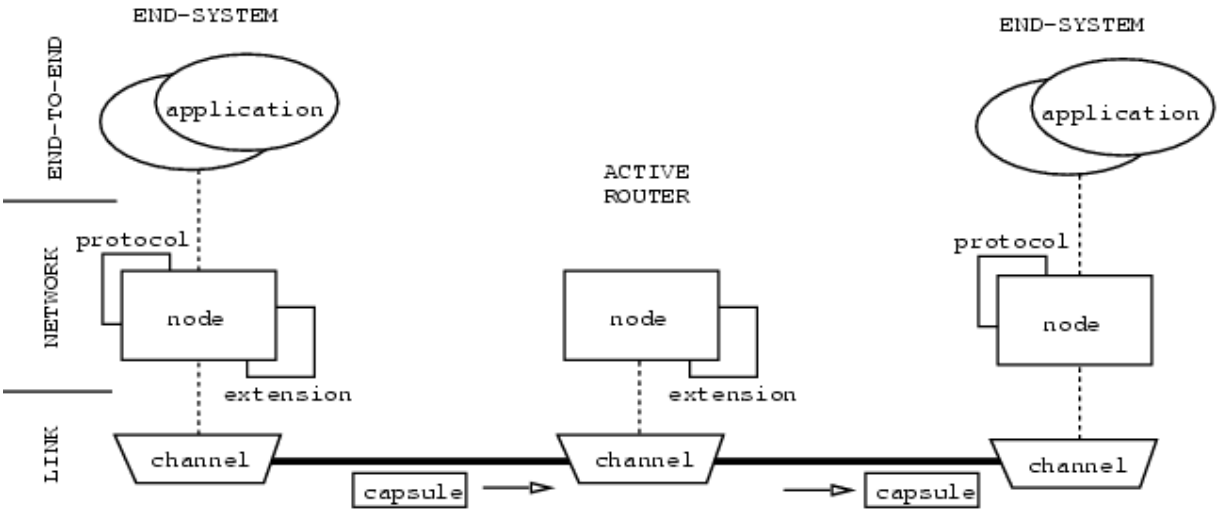
Khi các dịch vụ mới đã được triển khai, chúng sẽ sử dụng tại nguyên trên các nút mạng để hoạt động. Một khó khăn nữa trong việc xây dựng mạng tích cực là phân phối tài nguyên cho các dịch vụ để đảm bảo cho chúng hoạt động trong khi vẫn phải bảo vệ hệ thống khỏi những hành động không mong muốn. Hệ điều hành mạng tích cực đảm nhiệm điều này.

Không giống những hệ điều hành UNIX dựa trên cơ chế chia sẻ thời gian và đánh địa chỉ bộ nhớ, ANTS dựa trên một hệ điều hành đặc biệt được thiết kế để cung cấp cơ chế chia sẻ và bảo vệ để đảm bảo cho việc mở rộng các cơ chế truyền gói tin, ngoài ra nó còn hỗ trợ các ngôn ngữ lập trình bậc cao. Việc xử lý các gói tin tích cực đòi hỏi hệ thống thực hiện nhiều nhiệm vụ nhỏ chạy song song đại diện cho nhiều người dùng cùng sử dụng hệ thống. Hệ điều hành mạng tích cực cần cung cấp các cơ chế đảm bảo tốc độ cho việc truyền các gói tin để làm việc được trong môi trường đó. Như vậy, hệ điều hành cần giảm thiểu các thành phần của nó bao gồm cả những dịch vụ tải nặng và các cơ chế login.

II.3 Cài đặt các thành phần

Trong kiến trúc ANTS, các nút mạng tích cực được kết nối bởi các kênh để xây dựng nên mạng, các gói tin tích cực (capsule) được truyền vào mạng bởi các ứng dụng và được truyền thông qua các thủ tục riêng. Các khái niệm trên được mô tả trong hình 6.

- Mỗi nút mạng tích cực kể cả hệ thống cuỗi lẫn thiết bị dẫn đường được đại diện bởi một *thể hiện* (instance) của lớp `Node`. *Thành phần mởi rộng của nút* (node extention) cho phép các nút khác nhau hỗ trợ các dịch vụ khác nhau ví dụ lưu trữ đệm hoặc chuyển mã. Các thành phần mở rộng được cài đặt thông qua *lớp trừu tượng* `Extention` (abstract class trong ngôn ngữ lập trình Java là các lớp mà để sử dụng chúng cần có một lớp dẫn xuất cài đặt các phương thức của nó).



Hình 12 Các lớp chính trong bộ toolkit và quan hệ giữa chúng

Mỗi giao diện mạng được đại diện bởi một thể hiện của lớp `Channel`. Các kênh kết nối các nút mạng khác nhau thành một mạng. Các công nghệ mạng điểm-điểm hoặc chia sẻ môi trường truyền đều có thể được sử dụng như đã trình bày ở phần trước.

- Các ứng dụng mới sử dụng mạng tích cực được phát triển dựa trên lớp abstract Application. Các ứng dụng chứa những chức năng được cài đặt sử dụng các ứng dụng phân tán và hệ điều hành trên các hệ thống cuối ví dụ `vat, nv, wb`, hay sự kết hợp của HTTP và TCP.
- Các dịch vụ mới có thể được phát triển tại bất kì thời điểm nào bởi các lớp trừu tượng `Capsule` và `Protocol`. Các lớp dẫn xuất miêu tả các kiểu mới của gói tin tích cực và vị trí của nó trong giao thức, và cách truyền chúng qua ác nút mạng tích cực thông qua các *giao diện lập trình ứng dụng* (API) của lớp `Node`.

Mỗi nút quản lý máy ảo Java riêng của nó, thông thường, các máy ảo này chạy như một tiến trình Java của người sử dụng trên hệ điều hành UNIX. Các thể hiện của ứng dụng chạy trên máy ảo của nút mạng tích cực. Với cài đặt này, có thể sử dụng bộ công cụ để xây dựng các mạng nhỏ dựa trên kiến trúc vật lý bằng cách chạy mỗi nút mạng trên một thiết bị dẫn đường, cũng có giả lập các mạng ảo lớn bằng cách cài đặt nhiều nút mạng trên một máy tính (trong các thử nghiệm của

luận văn, luận văn này sử dụng cách thứ hai nhằm tiết kiệm chi phí thử nghiệm mà vẫn đảm bảo việc nghiên cứu các hiện tượng trong mạng tích cực lớn).

Trong thực tế, có thể xây dựng kiến trúc mạng tích cực dựa trên nhiều ngôn ngữ khác nhau, bộ công cụ ANTS được xây dựng dựa trên ngôn ngữ Java dựa trên những điểm sau: (i) ngôn ngữ Java thuận tiện cho việc xây dựng nhanh các nguyên mẫu, phát triển các thiết kế; (ii) Java cung cấp một kiến trúc an toàn cho việc triển khai mã di chú; (iii) có thể tăng hiệu suất của các chương trình Java dựa trên các thư viện phương thức viết trên các nền phần cứng và hệ điều hành cụ thể (sử dụng từ khoá `native`).

II.3.1 Cài đặt nút mạng tích cực

Một thể hiện của lớp `Node` đại diện cho một nút mạng, bao gồm vùng lưu trữ và hệ thống phân phát mã của nó. Nút mạng cung cấp các dịch vụ cho:

- Gói tin tích cực, cho phép chúng thực hiện các thủ tục truyền.
- Ứng dụng, đăng ký các giao thức và gửi, nhận các gói tin tích cực.
- Thành phần mở rộng, hỗ trợ chức năng cho dịch vụ của nút.

Những hoạt động này được phân chia logic và có nhu cầu được bảo vệ khác nhau. Ví dụ hoạt động của các gói tin tích cực phải được kiểm soát, trong khi các thành phần mở rộng của nút được truy cập một cách thoải mái hơn vào các tài nguyên của nút. Như vậy gói tin tích cực chỉ được truy cập đến một số API (do bộ công cụ được xây dựng trên ngôn ngữ Java, từ đây, các thuật ngữ API, hàm, thủ tục được thống nhất sử dụng là *phương thức*) nhất định, các phương thức khác hỗ trợ ứng dụng và phần mở rộng không nằm trong tầm vực của nó.

Các phương thức mà gói tin tích cực có thể truy cập và sử dụng là:

Phương thức	**Chức năng**
`int getAddress()`	Lấy địa chỉ local của nút
`ChannelObject getChannel()`	Nhận kênh vào
`Extension findExtension(String ext)`	Tìm dịch vụ mở rộng

Phương thức	**Chức năng**
`long time()`	Lấy thời gian
`Object put(Object key, Object val, int age)`	Đưa object vào vùng lưu
`Object get(Object key)`	Lấy object khỏi vùng lưu
`Object remove(Object key)`	Xoá object khỏi vùng lưu
`void routeForNode(Capsule c, int n)`	Gửi capsule đến nút mạng
`void deliverToApp(Capsule c, int a)`	Truyền capsule đến ứng dụng trên nút hiện tại
`void log(String msg)`	Ghi nhật ký thông điệp debug

Bảng 1. Các phương thức được sử dụng cho việc truyền gói tin

Các phương thức được chia làm ba (3) nhóm. Những phương thức như `getAddress()` và `time()` trả lại kết quả là các thông tin trên nút mạng tích cực. Phương thức `getChannel()` trả lại kênh mà gói tin đang được xử lý đã đi đến và trả lại giá trị `null` nếu gói tin được sinh ra trên nút mạng hiện tại. Phương thức `findExtention()` trả lại handle của tên phần mở rộng trên nút nếu nó được cài đặt.

Nhóm phương thức thứ hai quản lý bộ nhớ. Một bộ nhớ tạm chứa các object của ứng dụng được xác định và sử dụng trong thời gian ngắn. Phương thức `put()` đưa object thường là một gói tin tích cực vào vùng nhớ đệm này. Phương thức `get()` tìm lại object từ vùng nhớ. Phương thức thứ ba xoá đối tượng khỏi bộ nhớ.

Nhóm phương thức còn lại điều khiển việc xử lý các gói tin truyền qua mạng. Phương thức `routeForNode()` gửi một bản sao của gói tin tới một nút mạng dựa trên thông tin dẫn đường. Nhằm giảm việc thiếu tài nguyên cho việc xử lý gói tin. Phương thức `deliverToApp()` gọi một ứng dụng trên nút mạng để chuyển gói tin đến; ứng dụng đó có thể tạo một bản sao của gói tin nếu nó cần. Nếu không phương thức nào được gọi trong quá trình xử lý gói tin, gói tin đó bị

loại bỏ. Phương thức `log()` ghi nhận những thông tin và lỗi sảy ra trong hệ thống, thông thường phương thức này ghi các thông báo tại thiết bị đầu ra hoặc gửi các thông báo như giao thức ICMP (Giao thức thông báo lỗi trong bộ giao thức TCP/IP) thường làm.

Trong quá trình gọi các phương thức, một số lỗi có thể phát sinh dưới dạng các *ngoại lệ* (exception). Các ngoại lệ này cho phép xác định và xử lý lỗi thông qua cặp phương thức `try(), catch()` của Java hoặc thông qua việc xử lý trong phương thức `log()`.

Một số ngoại lệ được liệt kê trong bảng sau:

Ngoại lệ	**Mô tả**
`ResourceLimitException`	Không đủ tài nguyên để xử lý
`TimeLimitException`	Vượt quá khoảng tới hạn
`NoSuchRouteException`	Không có thông tin dẫn đường
`NoSuchApplicationException`	Không có ứng dụng trên nút hiện tại để truyền gói tin đến

Bảng 2. Một số ngoại lệ với việc truyền gói tin tích cực

II.3.2 Cài đặt gói tin tích cực

Các dẫn suất của lớp `Capsule` được sử dụng để điều khiển việc xử lý các gói tin tích cực trên các nút mạng. Lập trình viên phải viết các lớp dẫn suất khác nhau cho mỗi loại gói tin tích cực được sử dụng. Các đối tượng của các lớp dẫn suất đó sẽ được sử dụng để thể hiện và duy trì các loại gói tin trong khi chúng được truyền qua mỗi nút mạng tích cực.

Lớp trừu tượng `Capsule` định nghĩa một số phương thức cơ bản nhất mà mọi gói tin phải tuân thủ. Những phương thức cơ bản được định nghĩa trong lớp `Capsule` sử dụng cho việc xử lý phần đầu của gói tin bao gồm:

Phương thức	**Mô tả**
`int getSrc()`	Lấy cổng nguồn

Phương thức	**Mô tả**
`int getDst()`	Lấy cổng đích
`void setDst(int address)`	Đặt cổng đích
`int getResource()`	Lấy tài nguyên
`voide prime(Capsule parent)`	Chuẩn bị tài nguyên cho gói tin mới
`int getPrevious()`	Lấy địa chỉ nút mạng trước
`byte[] getCapsuleID()`	Lấy kiểu gói tin
`byte[] getGroupID()`	Lấy mã kiểu nhóm
`byte[] getProtocolID()`	Lấy kiểu giao thức

Bảng 3. Các phương thức xử lý phần đầu của gói tin

Địa chỉ đích và nguồn của gói tin được đánh bởi con số 32 bits, lớp `NodeAddress` cung cấp một số phương thức xử lý các địa chỉ này như các địa chỉ IP [1]. Các nút mạng chỉ cập nhật phần địa chỉ đích của gói tin. Địa chỉ nguồn lấy giá trị là địa chỉ nút gửi gói tin lên mạng và có giá trị `null` nếu như gói tin đó chưa được gửi.

Phương thức `getResource()` trả lại những tài nguyên rỗi cho gói tin. Giới hạn tài nguyên được ứng dụng đặt khi tạo ra gói tin trước khi gửi chúng vào mạng. Giới hạn tài nguyên này sẽ bị nút mạng giảm đi trước khi gói tin gửi bản sao của nó tới một nút mạng khác hoặc lưu một đối tượng trong vùng nhớ. Trong trường hợp gói tin tự tạo một bản sao của nó, phương thức `prime()` được sử dụng để đặt giới hạn tài nguyên cho gói tin mới, sử dụng tài nguyên của gói tin đó.

Các phương thức còn lại cho biết thông tin về mã của hệ phân tán mã. Phương thức `getPrevious()` trả lại địa chỉ của nút mạng tích cực trước đó đã xử lý gói tin. Các phương thức `getCaptureID()`, `getGroupID()`, `getProtocolID()` trả lại kiểu tương ứng của gói tin, nhóm và giao thức. Các kiểu được thể hiện dưới dạng mảng các byte và lớp `TypeID` cung cấp các phương thức để thao tác với chúng.

Cùng với lớp Capsule với những thao tác tối thiểu được định nghĩa cho việc xử lý gói tin, ANTS còn cung cấp một số lớp khác với các tính năng đầy đủ hơn giúp lập trình viên có thể sử dụng hoặc tạo các lớp dẫn suất từ chúng làm thuận tiện hơn cho công việc xây dựng các ứng dụng mạng tích cực của mình. Lớp DataCapture cung cấp các dịch vụ tương ứng với các dịch vụ UDP cho việc phát triển ứng dụng dựa trên giao thức không kết nối. Nó bao gồm một số phương thức sau:

Phương thức	**Mô tả**
`short getSrcPort()`	Lấy cổng nguồn
`void setSrcPort()`	Đặt cổng nguồn
`short getDstPort()`	Lấy cổng đích
`void setDstPort()`	Đặt cổng đích
`ByteArray getData()`	Lấy dữ liệu của gói tin
`void setData(ByteArray data)`	Đặt dữ liệu vào gói tin
`DataCapsule(short sp, short dp, int da, ByteArray p)`	Tạo tử

Bảng 4. Các phương thức trong lớp DataCapture

Tương tự như trong bộ giao thức TCP/IP, các ứng dụng chạy trên nút mạng được định danh bởi các số *cổng* (port). Chúng được thực hiện bởi các phương thức `getSrcPort()`, `setSrcPort()`, `getDstPort()`, `setDstPort()`. Dữ liệu trong gói tin được xử lý thông qua các phương thức `getData()` và `setData()`. Các gói tin kiểu DataCapture được tạo ra thông qua việc gọi tạo tử với tham số là địa chỉ các cổng và dữ liệu sẽ chứa trong gói tin. Trong mạng, các gói tin được truyền theo dẫn đường mặc định cho tới nút đích, tại đó, gói tin được truyền đến ứng dụng được chỉ định sẵn.

Việc truyền gói tin được thực hiện bởi phương thức `evaluate()`. Phương thức này được thực hiện tại mỗi nút mạng tích cực mà gói tin đi qua và được truyền tới nút như một tham số để truy cập tới các dịch vụ của nút. Nó có thể xử lý lỗi sử dụng việc bắt các ngoại lệ và phải kết thúc trong khoảng thời gian nút mạng cho phép. Trong khi phương thức `evaluate()` thực hiện, nút mạng phải đảm bảo

hoạt động của các gói tin khác không bị ảnh hưởng. Việc ảnh hưởng lẫn nhau có thể sảy ra trong trường hợp các gói tin cùng truy cập đến vùng nhớ hoặc cùng sử dụng một API do nút mạng cung cấp.

II.3.3 Giao thức

Để định nghĩa một dịch vụ mới, lập trình viên phải viết một lớp protocol và lớp capsule. Các lớp dẫn suất của lớp Protocol được sử dụng để tổ chức các lớp capsule và các lớp khác vào một nhóm mã và kiến trúc giao thức để chúng có thể hoạt động trên mạng.

Các phương thức trong lớp Protocol bao gồm:

Phương thức	**Mô tả**
`void startProtocolDefn()`	Bắt đầu một giao thức
`void endProtocolDefn()`	Kết thúc giao thức
`void startGroupDefn()`	Bắt đầu nhóm mã
`void endGroupDefn()`	Kết thúc nhóm mã
`void addCapsule(String name)`	Thêm gói tin vào nhóm
`void addHelperClass(String name)`	Thêm thành phần khác vào nhóm

Bảng 5. Các phưng thức trong lớp Protocol

II.3.4 Ứng dụng

ứng dụng là các thực thể độc lập sử dụng các dịch vụ mạng của ANTS. Chúng được xây dựng bằng dẫn suất của lớp Application. ứng dụng quản lý vùng chứa cho các xử lý của các hệ thống cuối, cung cấp các API cho việc kết nối với nút hiện tại, đăng ký các giao thức, gửi và nhận các gói tin trong mạng.

Lớp Application sử dụng các phương thức sau để truy cập vào mạng:

Phương thức	**Mô tả**
`void attachNode(Node n)`	Kết nối với nút hiện tại
`Node getNode()`	Lấy nút đang kết nối
`short getPort()`	Lấy cổng kết nối

`int getDefaultResource()`	Lấy giới hạn tài nguyên
`void setDefaultResouce(int l)`	Đặt giới hạn tài nguyên
`void register(Protocol p)`	Đăng ký giao thức
`void unregister(Protocol p)`	Bỏ đăng ký giao thức
`void send(Capsule c)`	Gửi gói tin sử dụng tài nguyên mặc định
`void send(Capsule c, int l)`	Gửi gói tin
`Void receive(Capsule c)`	Nhận gói tin

Bảng 6. Các phương thức trong lớp Application

Tập các phương thức đầu tiên sử dụng để kết nối với nút và truy cập đến cổng ứng dụng cũng như đặt số mặc định cho tài nguyên được sử dụng.

Để sử dụng các dịch vụ mới, mã ứng dụng tạo một thể hiện của giao thức và đăng ký nó với nút mạng sử dụng phương thức `register()`. Việc này thông báo trên mạng về giao thức mới và cho phép nút mạng nhận các mã dùng xử lý các gói tin từ hệ thống file của nút sau đó nó kích hoạt tiến trình phân tán mã. Khi mọi việc hoàn thành, ứng dụng có thể gửi nhận các gói tin của dịch vụ mới. ứng dụng có thể bỏ đăng ký giao thức sau khi công việc của nó kết thúc.

Phương thức `send()` được sử dụng để gửi các gói tin vào mạng, những gói tin này được gắn tham số tài nguyên sử dụng số mặc định của nút. Khi được gửi đi, gói tin trở thành một thành phần thuộc tính trong nút mạng, lúc này, các ứng dụng không truy cập đến nó nữa. Việc truyền các gói tin trong nút mạng tích cực được thực hiện bởi phương thức `evaluate()`. Cuối cùng, nút mạng đích gọi phương thức `receive()` để lấy gói tin ra khỏi mạng và truyền đến cho ứng dụng.

II.3.5 Thành phần mở rộng

Các thành phần mở rộng cho phép người quản trị mạng thêm các dịch vụ cho nút mạng tích cực sử dụng những đoạn mã lớn khó truyền được thông qua hệ thống phân tán mã. Trong ANTS, thành phần mở rộng cho phép xây dựng các mô hình

mạng đa dạng. Chúng được cài đặt độc lập trong quá trình triển khai các dịch vụ mới và quyết định những khả năng được phân cho mỗi nút mạng tích cực. Ví dụ người sử dụng A có thể cài đặt thành phần mở rộng `GroupsManager` để hỗ trợ công việc quản trị của mình, trong khi một số người khác lại sử dụng những thành phần hỗ trợ việc nén dữ liệu hoặc chuyển mã…

Các thành phần mở rộng được phát triển thông qua việc xây dựng các lớp dẫn suất của lớp `Extention` và cài đặt các thuộc tính và các phương thức phù hợp với yêu cầu. Sau đó, các thành phân mở rộng đó được cài đặt vào các nút mạng như một thành phần của nút đó. Do các thành phần mở rộng được cài đặt tại nút mạng và có thể truy cập được sâu hơn vào các tài nguyên của nút mạng, phải thận trọng trong việc phân chia các phương thức được sử dụng bởi các gói tin với các phương thức khác. Hơn nữa, tại nút mạng có cài đặt cơ chế bảo vệ để chế hoạt động của các gói tin, các thành phần mở rộng phải chỉ dẫn nút mạng cấp quyền cho các gói tin sử dụng các khả năng của thành phần mở rộng. Có hai (2) phương thức hỗ trợ các thành phần mở rộng thường được gọi trong quá trình khởi tạo bao gồm:

- `attachExtention(Extention e)` đăng ký thành phần mở rộng với nút mạng. Các quá trình truyền gói tin có thể thấy được các thành phần mở rộng bằng cách gọi phương thức `findExtention()` và sử dụng dịch vụ của nó.
- exportClass(Class cl) yêu cầu nút mạng cho phép các gói tin truy cập đến các lớp của thành phần mở rộng.

II.3.6 Kênh

Các kênh cho phép nút mạng giao tiếp với các giao thức lớp link (lớp 2 trong mô hình tham chiếu OSI), thông qua đó, nhiều nút có thể cùng kết nối và sử dụng mạng thông qua các kết nối điểm điểm hoặc chia sẻ môi trường truyền (Ví dụ, CSMA/CD Carrier Sense MultiAccess and Collision Detection). Các kiểu kênh khác nhau có thể được xây dựng tương ứng với các môi trường lớp link được sử dụng bằng cách tạo các lớp dẫn suất của lớp trừu tượng Channel. Lớp

UDPChannel được sử dụng cho các mô hình kết nối mạng sử dụng dịch vụ UDP. Điều này cho phép xây dựng mạng tích cực trên cơ sở sử dụng mạng Internet như môi trường truyền dẫn. Một mạng nhỏ có thể được xây dựng bằng cách chạy mỗi nút mạng trên một thiết bị dẫn đường và kết nối các nút sử dụng kênh UDP (trong trường hợp này, UDP kết nối các nút thông qua mạng máy tính). Cũng có thể mô phỏng các mạng lớn bằng việc chạy nhiều nút mạng trên một máy và kết nối chúng sử dụng các kênh UDP (trong trường hợp này, mỗi nút mạng có thể hỗ trợ nhiều điểm dịch vụ UDP).

Các phương thức chung cho mọi kiểu kênh được lớp channel cung cấp sử dụng cho việc lấy các thông số của nút mạng bao gồm:

Phương thức	**Mô tả**
`int getAddress()`	Trả lại địa chỉ giao diện
`int getBandwidth()`	Trả lại độ rộng băng thông (bps)
`int getLatency()`	Trả lại độ trễ (ms)
`int getMTU()`	Trả lại cỡ tối đa của gói (byte)
`int getBER()`	Trả lại mức lỗi bít

Bảng 7. Phương thức của channel

Nhiều thuộc tính không áp dụng cho các kênh ảo như UDP, khi đó, chúng được sử dụng cho các gói tin loại khác hoặc cho các trường hợp các nút mạng bị chia rẽ bởi các nút mạng thông thường.

II.3.7 Quản lý cấu hình

Trên thực tế, việc thử nghiệm với một mạng tích cực đòi hỏi phải xây dựng một *hình trạng* (topology) của mạng. ANTS cung cấp các công cụ tự động để làm việc này.

Công cụ `ConfigurationManager` được sử dụng để tạo và vận hành máy tính như một thành phần của mạng tích cực. Công cụ này yêu cầu một bản mô tả về mạng dưới dạng *tệp cấu hình,* tệp cấu hình này chứa một hoặc nhiều dòng mô tả từng thực thể của mạng (nút, kênh, ứng dụng và phần mở rộng) dưới dạng văn

bản đơn giản. Việc này cho phép quản trị đơn giản vì một tệp văn bản có thể sử dụng để định nghĩa toàn bộ hình trạng của mạng.

Để cho phép quản lý chung các thực thể trên mạng, câc lớp `Node`, `Channel`, `Application` và `Extention` được xây dựng là các dẫn suất từ lớp trừu tượng `Entity`. Có hai phương thức các lớp dẫn suất không thể ghi đè:

- Phương thức `setArgs(KeyArgs args)` được `ConfigurationManager` gọi để cho phép thực thể thực hiện các câu lệnh chuyển tới thông qua tệp cấu hình.
- Phương thức start() được ConfigurationManager gọi để thực hiện việc khởi tạo và cho phép các thực thể bắt đầu quá trình hoạt động. Thông thường nó sẽ tạo ra một luồng để quản lý quá trình thực hiện.

Ngoài ra lớp Entity còn cung cấp các phương thức cho các lớp dẫn suất của nó sử dụng để truyền tín hiệu, cảnh báo, và các thông điệp lỗi tới một điểm thu thập chung, lọc và thể hiện chúng.

II.4 Kết luận chương 2

Mạng tích cực là vấn đề đang được các nhà nghiên cứu quan tâm, tuy nhiên, số lượng các ứng dụng sử dụng phương pháp tiếp cận này chưa lớn do chưa có nhiều mô hình, công cụ hỗ trợ việc phát triển ứng dụng sử dụng công nghệ mạng tích cực. Sự ra đời của bộ công cụ ANTS giải quyết phần nào vấn đề trên. Với bộ công cụ này, người phát triển phần mềm (đôi khi người sử dụng) mạng có thể phát triển nhanh chóng các ứng dụng của mình. Một số ứng dụng caching đã được phát triển, nhiều ý tưởng về các phần mềm phát triển trên bộ công cụ ANTS được trao đổi rộng rãi trên nhóm tin http://www.cs.utah.edu/flux/janos/.

CHƯƠNG III. AN TOÀN THÔNG TIN TRÊN MẠNG VÀ VIỆC XÂY DỰNG MÔ HÌNH AN TOÀN CHO MẠNG TÍCH CỰC

Trong các chương trước, chúng tôi đã giới thiệu một phương pháp tiếp cận mới cho việc xây dựng và triển khai các dịch vụ mạng một cách nhanh chóng và hiệu quả. Tuy nhiên, cùng với những lợi ích mà nó mang lại, phương pháp này cũng mang lại cho chúng ta những thách thức cần vượt qua. Những thách thức lớn nhất phải kể đến là (i) việc chuẩn hoá phương pháp, (ii) xây dựng các công cụ hỗ trợ, (iii) phát triển các ứng dụng và thương mại hoá chúng, và một vấn đề quan trọng nhất là (iv) làm sao bảo vệ an toàn cho hệ thống trong khi vẫn đảm bảo cung cấp khả năng cung cấp các dịch vụ mới hiệu quả.

Chương này tập trung vào việc phân tích vấn đề an toàn trong mạng tích cực nhằm đề xuất việc xây dựng một kiến trúc an toàn cho cách tiếp cận mạng tích cực như một mô hình tham chiếu cho việc xây dựng một mạng tích cực an toàn.

Phần đầu của chương sẽ đi sâu phân tích vấn đề (Vấn đề ở đây được hiểu theo cả hai nghĩa Problem và Issue: Chúng tôi đã trình bày quan điểm về security problem or issue trên trang www.security-forum.com và được nhiều ý kiến đồng tình của những người tham gia diễn đàn) an toàn trong liên mạng (internet) máy tính nói chung với một số ví dụ dẫn chứng trong mạng Internet. Tiếp đó, chúng tôi phân tích mạng tích cực và những cơ chế có thể gây ra những vấn đề liên quan đến an toàn thông tin. Phần cuối trình bày kiến trúc an toàn cho cách tiếp cận mạng tích cực có thể được sử dụng làm mô hình tham chiếu cho việc xây dựng mạng tích cực an toàn.

III.1 Vấn đề an toàn thông tin

Để giải thích quan điểm về vấn đề an toàn thông tin được hiểu theo nghĩa *vấn đề cần giải quyết* (problem) và *vấn đề cần bàn luận* (issue), chúng ta sẽ phân tích nhu cầu bảo vệ thông tin và các phương pháp thường được sử dụng để tấn công vào hệ thống, đồng thời, xác định những đối tượng cần được quan tâm khi nói đến vấn đề an toàn thông tin.

III.1.1 Nhu cầu bảo vệ tài nguyên và uy tín

III.1.2 Bảo vệ dữ liệu

Những thông tin lưu trữ trên hệ thống máy tính cần được bảo vệ do các yêu cầu sau [5 Building Internet Firewall]:

- **Bảo mật**: Những thông tin có giá trị về kinh tế, quân sự, chính sách vv... cần được giữ kín.
- **Tính toàn vẹn**: Thông tin không bị mất mát hoặc sửa đổi, đánh tráo.
- **Tính kịp thời**: Yêu cầu truy nhập thông tin vào đúng thời điểm cần thiết.

Trong các yêu cầu này, thông thường yêu cầu về bảo mật được coi là yêu cầu số một đối với thông tin lưu trữ trên mạng. Tuy nhiên, ngay cả khi những thông tin này không được giữ bí mật, thì những yêu cầu về tính toàn vẹn cũng rất quan trọng. Không một cá nhân, một tổ chức nào lãng phí tài nguyên vật chất và thời gian để lưu trữ những thông tin mà không biết về tính đúng đắn của những thông tin đó.

III.1.3 Bảo vệ tài nguyên

Trên thực tế, trong các cuộc tấn công trên mạng, kẻ tấn công, sau khi đã làm chủ được hệ thống bên trong, có thể sử dụng các máy này để phục vụ cho mục đích của mình như chạy các chương trình dò mật khẩu người sử dụng, sử dụng các liên kết mạng sẵn có để tiếp tục tấn công các hệ thống khác vv... Những hoạt động này thông thường sử dụng rất nhiều tài nguyên của hệ thống.

III.1.4 Bảo vệ danh tiếng

Phần lớn các cuộc tấn công không được thông báo rộng rãi, và một trong những nguyên nhân là nỗi lo bị mất uy tín của cơ quan, đặc biệt là các công ty lớn và các cơ quan quan trọng trong bộ máy nhà nước. Trong trường hợp người quản trị hệ thống chỉ được biết đến sau khi chính hệ thống của mình được dùng làm bàn đạp để tấn công các hệ thống khác, thì tổn thất về uy tín lại càng rất lớn và có thể để lại hậu quả lâu dài.

III.1.5 Các kiểu tấn công

Có rất nhiều kiểu tấn công vào hệ thống, và có nhiều cách để phân loại những kiểu tấn công này. ở đây, chúng ta chia thành 3 kiểu chính như sau:

Tấn công trực tiếp

Những cuộc tấn công trực tiếp thông thường được sử dụng trong giai đoạn đầu để chiếm được quyền truy nhập bên trong. Một phương pháp tấn công cổ điển là dò cặp tên người sử dụng-mật khẩu. Đây là phương pháp đơn giản, dễ thực hiện và không đòi hỏi một điều kiện đặc biệt nào để bắt đầu. Kẻ tấn công có thể sử dụng những thông tin như tên người dùng, ngày sinh, địa chỉ, số nhà vv.. để đoán mật khẩu. Trong trường hợp có được danh sách người sử dụng và những thông tin về môi trường làm việc, có một trương trình tự động hoá về việc dò tìm mật khẩu này. một trương trình có thể dễ dàng lấy được từ Internet để giải các mật khẩu đã mã hoá của các hệ thống unix có tên là crack, có khả năng thử các tổ hợp các từ trong một từ điển lớn, theo những quy tắc do người dùng tự định nghĩa. Trong một số trường hợp, khả năng thành công của phương pháp này có thể lên tới 30%.
Phương pháp sử dụng các lỗi của chương trình ứng dụng và bản thân hệ điều hành đã được sử dụng từ những vụ tấn công đầu tiên và vẫn được tiếp tục để chiếm quyền truy nhập. Trong một số trường hợp phương pháp này cho phép kẻ tấn công có được quyền của người quản trị hệ thống (root hay administrator).
Hai ví dụ thường xuyên được đưa ra để minh hoạ cho phương pháp này là ví dụ với chương trình sendmail và chương trình rlogin của hệ điều hành UNIX.
Sendmail là một chương trình phức tạp, với mã nguồn bao gồm hàng ngàn dòng lệnh của ngôn ngữ C. Sendmail được chạy với quyền ưu tiên của người quản trị hệ thống, do chương trình phải có quyền ghi vào hộp thư của những người sử dụng máy. Và Sendmail trực tiếp nhận các yêu cầu về thư tín trên mạng bên ngoài. Đây chính là những yếu tố làm cho sendmail trở thành một nguồn cung cấp những lỗ hổng về bảo mật để truy nhập hệ thống.
Rlogin cho phép người sử dụng từ một máy trên mạng truy nhập từ xa vào một máy khác sử dụng tài nguyên của máy này. Trong quá trình nhận tên và mật khẩu của người sử dụng, rlogin không kiểm tra độ dài của dòng nhập, do đó kẻ tấn

công có thể đưa vào một xâu đã được tính toán trước để ghi đè lên mã chương trình của rlogin, qua đó chiếm được quyền truy nhập.

Nghe trộm

Việc nghe trộm thông tin trên mạng có thể đưa lại những thông tin có ích như tên-mật khẩu của người sử dụng, các thông tin mật chuyển qua mạng. Việc nghe trộm thường được tiến hành ngay sau khi kẻ tấn công đã chiếm được quyền truy nhập hệ thống, thông qua các chương trình cho phép đưa vỉ giao tiếp mạng (Network Interface Card-NIC) vào chế độ nhận toàn bộ các thông tin lưu truyền trên mạng. Những thông tin này cũng có thể dễ dàng lấy được trên Internet.

Giả mạo địa chỉ

Việc giả mạo địa chỉ IP có thể được thực hiện thông qua việc sử dụng khả năng dẫn đường trực tiếp (source-routing). Với cách tấn công này, kẻ tấn công gửi các gói tin IP tới mạng bên trong với một địa chỉ IP giả mạo (thông thường là địa chỉ của một mạng hoặc một máy được coi là an toàn đối với mạng bên trong), đồng thời chỉ rõ đường dẫn mà các gói tin IP phải gửi đi.

Vô hiệu hoá các chức năng của hệ thống (denial of service)

Đây là kểu tấn công nhằm tê liệt hệ thống, không cho nó thực hiện chức năng mà nó thiết kế. Kiểu tấn công này không thể ngăn chặn được, do những phương tiện được tổ chức tấn công cũng chính là các phương tiện để làm việc và truy nhập thông tin trên mạng. Ví dụ sử dụng lệnh ping với tốc độ cao nhất có thể, buộc một hệ thống tiêu hao toàn bộ tốc độ tính toán và khả năng của mạng để trả lời các lệnh này, không còn các tài nguyên để thực hiện những công việc có ích khác.

Lỗi của người quản trị hệ thống

Đây không phải là một kiểu tấn công của những kẻ đột nhập, tuy nhiên lỗi của người quản trị hệ thống thường tạo ra những lỗ hổng cho phép kẻ tấn công sử dụng để truy nhập vào mạng nội bộ.

Tấn công vào yếu tố con người

Kẻ tấn công có thể liên lạc với một người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi mật khẩu, thay đổi quyền truy nhập của mình đối với hệ thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các

phương pháp tấn công khác. Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn một cách hữu hiệu, và chỉ có một cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi. Nói chung yếu tố con người là một điểm yếu trong bất kỳ một hệ thống bảo vệ nào, và chỉ có sự giáo dục cộng với tinh thần hợp tác từ phía người sử dụng có thể nâng cao được độ an toàn của hệ thống bảo vệ.

III.1.6 Phân loại kẻ tấn công

Có rất nhiều kẻ tấn công trên mạng toàn cầu – Internet và chúng ta cũng không thể phân loại chúng một cách chính xác, bất cứ một bản phân loại kiểu này cũng chỉ nên được xem như là một cách nhìn nhận.

Người qua đường

Người qua đường là những kẻ buồn chán với những công việc thường ngày, họ muốn tìm những trò giải trí mới. Họ đột nhập vào máy tính của bạn vì họ nghĩ bạn có thể có những dữ liệu hay, hoặc bởi vì họ cảm thấy thích thú khi sử dụng máy tính của người khác, hoặc chỉ đơn giản là họ không tìm được một việc gì hay hơn để làm. Họ có thể là người tò mò nhưng không chủ định làm hại bạn. Tuy nhiên, họ thường gây hư hỏng hệ thống khi đột nhập hay khi xoá bỏ dấu vết của họ.

Kẻ phá hoại

Kẻ phá hoại chủ định phá hoại hệ thống của bạn, họ có thể không thích bạn, họ cũng có thể không biết bạn nhưng họ tìm thấy niềm vui khi đi phá hoại.

Thông thường, trên Internet kẻ phá hoại khá hiếm. Mọi người không thích họ. Nhiều người còn thích tìm và chặn đứng những kẻ phá hoại. Tuy ít nhưng kẻ phá hoại thường gây hỏng trầm trọng cho hệ thống của bạn như xoá toàn bộ dữ liệu, phá hỏng các thiết bị trên máy tính của bạn...

Kẻ ghi điểm

Rất nhiều kẻ qua đường bị cuốn hút vào việc đột nhập, phá hoại. Họ muốn được khẳng định mình thông qua số lượng và các kiểu hệ thống mà họ đã đột nhập qua. Đột nhập được vào những nơi nổi tiếng, những nơi phòng bị chặt chẽ, những nơi

thiết kế tinh xảo có giá trị nhiều điểm đối với họ. Tuy nhiên họ cũng sẽ tấn công tất cả những nơi họ có thể, với mục đích số lượng cũng như mục đích chất lượng. Những người này không quan tâm đến những thông tin bạn có hay những đặc tính khác về tài nguyên của bạn. Tuy nhiên để đạt được mục đích là đột nhập, vô tình hay hữu ý họ sẽ làm hư hỏng hệ thống của bạn.

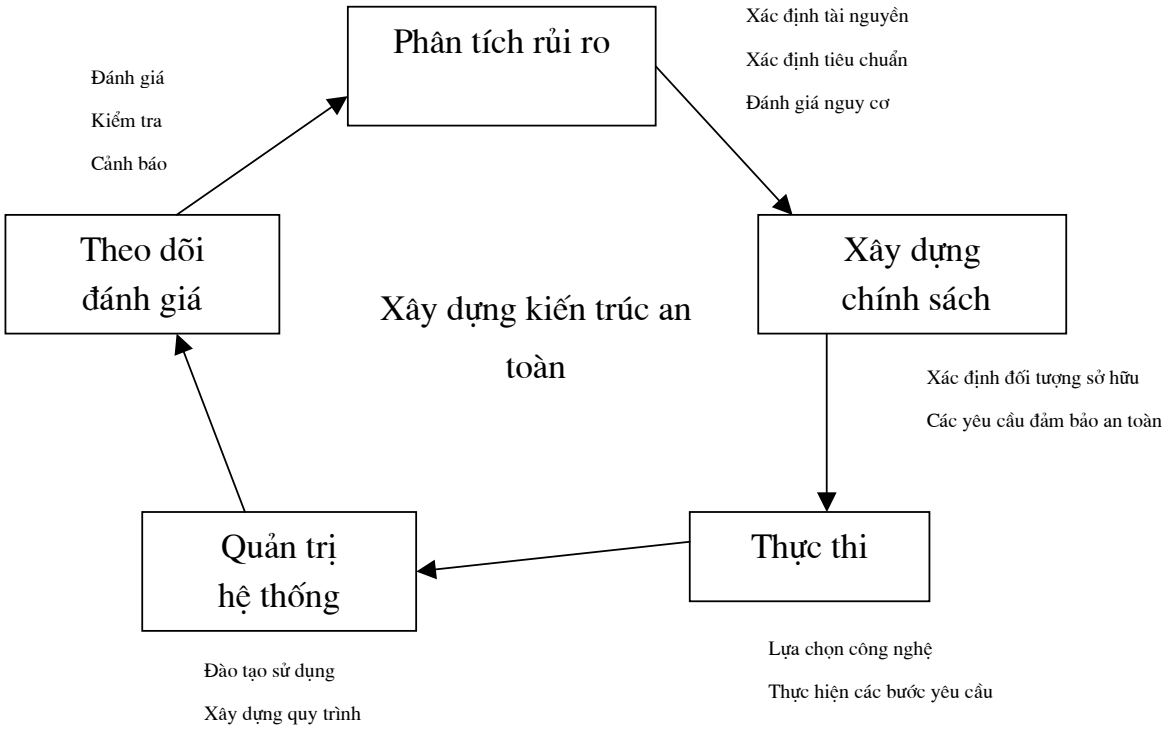
Gián điệp

Hiện nay có rất nhiều thông tin quan trọng được lưu trữ trên máy tính như các thông tin về quân sự, kinh tế... Gián điệp máy tính là một vấn đề phức tạp và khó phát hiện. Thực tế, phần lớn các tổ chức không thể phòng thủ kiểu tấn công này một cách hiệu quả và bạn có thể chắc rằng đường liên kết với Internet không phải là con đường dễ nhất để gián điệp thu lượm thông tin.

Từ những phân tích trên ta thấy, để chống lại việc tấn công vào hệ thống, người ta cần xây dựng và sử dụng những công cụ hỗ trợ để đảm bảo an toàn thông tin, chống lại những kẻ tấn công vào hệ thống đó chính là giải quyết mặt ***vấn đề cần giải quyết***. Hơn nữa, phương pháp tấn công của tin tặc luôn luôn thay đổi với nhiều thủ thuật tinh vi, tấn công cả vào yếu tố con người, cần có một chiến lược phát triển, xây dựng đội ngũ người sử dụng, người quản trị có trình độ cao, đáng tin cậy, đó chính là mặt ***vấn đề bàn luận*** trong vấn đề an toàn thông tin.

III.2 Xây dựng chiến lược đảm bảo an toàn thông tin

Việc xây dựng chiến lược đảm bảo an toàn thông tin được thực hiện như một quá trình phát triển dựa trên mô hình xoắn ốc bao gồm nhiều giai đoạn. Việc kết thúc giai đoạn này là tiền đề để thực hiện giai đoạn tiếp theo. Tuy nhiên, sau một vòng, quá trình phát triển không dừng lại mà tiếp tục chuyển sang giai đoạn đầu của một vòng tiếp theo



Hình 13. Xây dựng kiến trúc an toàn

III.2.1 Phân tích các rủi ro

Việc phân tích rủi ro là giai đoạn đầu tiên của việc xây dựng chính sách an toàn trong hệ thống. Nó là bước tối quan trọng đóng vai trò làm tiền đề để thực hiện các bước ở các giai đoạn tiếp theo. Thông thường bước này trả lời các câu hỏi "Hệ thống có gì cần bảo vệ và phải bảo vệ chống lại cái gì?"

Giai đoạn "Phân tích rủi ro" cùng với giai đoạn tiếp theo "Xây dựng chính sách" thường được trình bày trong các đề án tiền khả thi cho việc xây dựng chiến lược đảm bảo an toàn thông tin.

- **Xác định những tài nguyên cần bảo vệ:** Như phần trên đã trình bày, những tài nguyên cần được bảo vệ của một tổ chức chính là (i) dữ liệu, (ii) khả năng đáp ứng dịch vụ và cả (iii) danh tiếng của tổ chức đó. Việc xác định tài nguyên cần bảo vệ giúp cho việc xác định rủi ro được dễ dàng hơn, từ đó có

thể xây dựng các chiến lược "đúng đắn" tập trung vào việc bảo vệ các tài nguyên đó.

- **Xác định các tiêu chuẩn:** Sau khi xác định tài nguyên cần bảo vệ, phải đưa ra được các tiêu chuẩn đối với mỗi tài nguyên cần bảo vệ có thể lấy ví dụ trình bày trong phần đầu của chương, đối với dữ liệu, tiêu chuẩn an toàn là (i) tính bảo mật, (ii) tính toàn vẹn và (iii) tính kịp thời.
- **Đánh giá nguy cơ:** Các nguy cơ mất an toàn trong hệ thống cần được xác định rõ bao gồm các (i) phương pháp có thể sử dụng để tấn công hệ thống, (ii) nhận diện những kẻ tấn công vào hệ thống và (iii) lường trước những nguy cơ tiềm ẩn có thể gây nên việc mất an toàn trong hệ thống.

III.2.2 . Xây dựng chính sách

- **Xác định sở hữu:** Các (i) tài nguyên hệ thống cần bảo vệ bao gồm những gì, (ii) những thực thể nào trong hệ thống sỏ hữu và sử dụng chúng cần được xác định rõ, từ đó có thể tìm ra mối liên hệ giữa các thực thể đó đối với vấn đề an toàn của toàn hệ thống. Sau khi đã xác định được các thực thể có đóng vai trò trong việc đảm bảo an toàn, việc xây dựng chính sách có thể hướng vào giải quyết vấn đề an toàn của các thực thể đó từ đó giả quyết vấn đề an toàn của toàn hệ thống.
- **Các yêu cầu cho việc đảm bảo an toàn dữ liệu và tài sản:** Các đề án tiền khả thi về an toàn thông tin phải nêu ra được yêu cầu cho việc đảm bảo an toàn dữ liệu cũng như tài sản của tổ chức. Những thực thể trong hệ thống cần tuân thủ những quy tắc như thế nào để đảm bảo an toàn cho chúng và cho toàn hệ thống.

III.2.3 . Thực thi

Sau khi đã xây dựng chính sách cho việc đảm bảo an toàn cho hệ thống việc tiếp theo cần thực hiện là thực thi chính sách đó, giai đoạn này bao gồm hai (2) bước: (i) lựa chọn công nghệ và (ii) thực thi đề án sử dụng công nghệ đã lựa chọn.

- **Lựa chọn công nghệ:** Trong các giải pháp đảm bảo an toàn hệ thống, lựa chọn công nghệ phù hợp với nhu cầu của tổ chức và có giá cả phù hợp.
- **Các bước thực hiện:** Mỗi công nghệ có các bước thực hiện của nó, cần thực hiện nghiêm ngặt các bước này để tận dụng tối đa khả năng của công nghệ.

III.2.4 . Quản trị hệ thống

Việc quản trị hệ thống bao gồm nhiều công việc khác nhau, trong phần này, chúng tôi chú trọng vào việc trình bày những công việc liên quan trực tiếp đến đảm bảo an toàn hệ thống.

- **Đào tạo người sử dụng:** Một trong số những vấn đề về an toàn thông tin thường xuyên sảy ra nhất trong hệ thống nhiều người sử dụng với trình độ khác nhau và nhu cầu sử dụng đa dạng. Do đó, việc đào tạo nâng cao trình độ cho người sử dụng có thể làm giảm thiểu những rủi ro do việc lỗi của người sử dụng trong hệ thống. Việc người sử dụng có ý thức trong việc đảm bảo an toàn thông tin trong hệ thống cũng làm giảm khả năng tấn công vào yếu tố con người của hệ thống.
- **Xây dựng các quy trình:** Các quy trình là các bước thực hiện một số công việc đã được xây dựng và kiểm tra sau đó đưa ra để mọi người cùng thực hiện. Việc xây dựng các quy trình làm việc được kiểm tra kỹ lưỡng đóng vai trò quan trọng trong việc làm giảm lỗi trong hệ thống, đồng thời hỗ trợ người sử dụng trong hệ thống một cách tiếp cận nhanh chóng và an toàn.

III.2.5 . Theo dõi và đánh giá

Sau khi đã xây dựng hệ thống an toàn, người quản trị phải thường xuyên theo dõi hệ thống để đảm bảo nó hoạt động an toàn và không phát sinh những lỗi mới ảnh hưởng tới việc đảm bảo an toàn của hệ thống ví dụ như các lỗ hổng bảo mật của hệ điều hành mới được phát hiện, các loại virus mới hoặc người sử dụng nào đó vô tình hay hữu ý cài đặt các chương trình sử dụng *cửa sau* (backdoor – các chương trình cho phép bí mật truy cập vào hệ thống mạng).

- **Đánh giá hệ thống:** Thông thường nên thực hiện việc báo cáo định kỳ về hệ thống, từ những báo cáo đó, đánh giá hệ thống, tìm ra những nhu cầu phát sinh trong thực tế sử dụng và phát triển hệ thống. Những nhu cầu phát sinh này có thể được sử dụng cho vòng phát triển sau của hệ thống an toàn.
- **Kiểm tra bên trong và bên ngoài:** Có thể sử dụng một số phương pháp kiểm tra như ghi nhật ký việc truy cập hệ thống từ bên trong và bên ngoài nhất là những dịch vụ có tính "nhạy cảm" cao. Một phương pháp khác là sử dụng các chương trình dò tìm lỗ hổng như SATAN, SAINT để tìm ra những lỗ hổng an toàn của hệ thống. Đôi khi có thể sử dụng một số phương pháp tấn công thử tấn công vào chính hệ thống của mình. Một hệ thống có thể vượt qua những kiểm tra ngặt nghèo có thể có khả năng chống lại nhiều cuộc tấn công của các hacker trên mạng.
- **Hệ thống cảnh báo:** Hệ thống cảnh báo giúp người quản trị mạng nhận biết được lỗi khi chúng sảy ra trong hệ thống (có thể trước khi lỗi sảy ra) để kịp thời có biện pháp khắc phục. Đôi khi hệ thống này cũng giúp ích cho người sử dụng ví dụ cảnh báo người sử dụng không truy cập đến một dịch vụ có lỗi trong hệ thống.

III.3 An toàn thông tin trong mạng tích cực

Trong phần này, luận văn sử dụng quy trình được đề xuất ở phần trên xây dựng một kiến trúc an toàn cho mạng tích cực.

III.3.1 Nhu cầu đảm bảo an toàn thông tin của các thực thể

Chương II cho ta thấy mạng tích cực bao gồm nhiều thực thể liên kết với nhau, những thực thể này có nhu cầu bảo vệ những tài nguyên chúng được phân chia trong hệ thống. Người sử dụng hệ thống, nút mạng tích cực, môi trường thực hiện, và mã tích cực đều cần được bảo vệ.

III.3.2 Nút mạng tích cực

Nút mạng tích cực tập trung sự quan tâm của mình đến việc xác thực những đối tượng nào được phép sử dụng tài nguyên và dịch vụ do nút mạng cung cấp để đảm

bảo khả năng cung cấp dịch vụ của nó. Ngoài ra, nút mạng cần quan tâm đến tính toàn vẹn về dữ liệu và tài nguyên cho phép nó cung cấp dịch vụ. Nút mạng cần bảo vệ bí mật trạng thái của nó đối với những thực thể chưa được xác thực.

Nút mạng có thể bị đe doạ bởi các môi trường thực hiện (EE) vì các EE có thể sử dụng tài nguyên của nút mạng hay làm thay đổi trạng thái của chúng, ngoài ra, các EE có thể truy cập đến những dữ liệu quan trọng của nút mạng. Đôi khi người sử dụng có thể gửi quá nhiều gói tin tích cực làm cho nút mạng bị quá tải không còn khả năng xử lý, do vậy, nút mạng cũng có thể bị đe doạ bởi chính người sử dụng mạng (một kiểu tấn công thường thấy trên mạng là việc kẻ tấn công gửi nhiều gói tin đến một hệ thống làm chậm thậm chí gây sụp đổ hệ thống). Các đoạn mã gửi kèm trong gói tin tích cực có thể sử dụng tài nguyên, thay đổi trạng thái của nút mạng, truy cập đến những dữ liệu của nút mạng khi thực hiện trong EE cũng là một mối đe doạ tiềm ẩn đối với nút mạng.

Bằng việc cài đặt một cơ chế an toàn thích hợp, nút mạng có thể bảo vệ chính nó khỏi những đe doạ từ các thành phần khác của mạng tích cực.

III.3.3 . Môi trường thực hiện

Môi trường thực hiện cũng có sự quan tâm giống nút mạng tích cực đối với dịch vụ, tài nguyên và trạng thái của nó. EE có thể bị đe doạ bởi các EE khác cùng hoạt động, từ thực thể gửi các gói tin tích cực, và từ các đoạn mã tích cực chạy trên nó.

Ngoài ra, những đe doạ về việc mất an toàn có thể đến từ chính nút mạng tích cực mà EE đang chạy trên đó. EE rất khó có thể bảo vệ bản thân nó khỏi những đe doạ đến từ nút mạng, hơn nữa, các EE không thể lựa chọn nơi mà nó được thực hiện. Do đó, những dịch vụ phát tán phải đảm bảo việc EE được bảo vệ tại các nút mạng tích cực.

III.3.4 . Người sử dụng

Đối với người sử dụng quan niệm an toàn trong mạng tích cực cũng giống như quan niệm an toàn trong các mạng thông thường bao gồm việc đảm bảo (i) *xác thực* (authenticity), (ii) tính *toàn vẹn* (integrity), (iii) sự *bí mật* (confidentiality)

của các thông tin trong gói tin truyền trên mạng. Người sử dụng quan tâm đến việc dữ liệu được tạo ra trong kiến trúc như thế nào và phương pháp truy cập đến những dữ liệu đó ra sao.

Như vậy người sử dụng gửi các gói tin trên mạng tích cực có thể bị đe doạ đối với thông tin chứa trong các gói tin từ các mã tích cực khác trên mạng, từ các EE và từ chính nút mạng tích cực.

Sử dụng phương pháp mã hoá thông tin, người sử dụng có thể tránh được việc thông tin bị rò rỉ trên đường truyền, chỉ trạm gửi và trạm nhận mới có thể xem được thông tin. Tuy nhiên trong mạng tích cực, các nút phải thực hiện mã lệnh chứa trong gói tin, vì vậy, các nút phải chia sẻ thông tin về mã khoá để có thể giải mã và thực hiện chương trình. Điều này làm cho việc áp dụng phương pháp mã hoá trong việc bảo vệ thông tin trong mạng tích cực khó khăn và không hiệu quả. Có thể nói người sử dụng khó có thể bảo vệ gói tin tích cực khỏi những đe doạ từ nút mạng hay các EE mà chỉ có thể cố gắng dựa trên mã tích cực để tránh những nút mạng và những EE không tin tưởng. Nếu mối quan tâm của người sử dụng liên quan đến những thuộc tính của gói tin chứ không phải thông tin chứa trong gói tin (ví dụ độ trễ trên đường truyền – cực kỳ quan trọng trong những ứng dụng thời gian thực) thì họ có thể sử dụng những mã tích cực chứa trong gói tin để bảo vệ những thuộc tính đó.

III.3.5 . Ứng dụng tích cực

Các ứng dụng tích cực (đóng vai trò đại diện cho người sử dụng sinh ra gói tin chứa nó) quan tâm đến việc bảo vệ truy cập đến các tài nguyên nó đang sử dụng (ví dụ việc truy cập đến kênh mà nó đang sử dụng) và việc truy cập đến những tài nguyên mà nó chia sẻ cho các thực thể khác sử dụng. Tuỳ thuộc vào các tính năng của EE mà trên đó mã lệnh đang được thực hiện, nó có thể tạo ra các trạng thái có thể chia sẻ với những mã lệnh khác, sử dụng bởi các mã lệnh, hoặc có thể cung cấp dịch vụ cho các mã lệnh đó.

Mã lệnh tích cực có thể bị đe doạ bởi các gói tin tích cực, các mã lệnh khác, từ các EE và từ các nút mạng tích cực. Tuy nhiên, các mã lệnh tích cực không thể tự bảo vệ mình khỏi những đe doạ đến từ EE và nút mạng tích cực mà chúng đang

thực hiện trên đó. Chúng chỉ có thể đảm bảo rằng chúng không tự gửi chính bản thân đến những nút mạng không tin tưởng.

Thực thể	**Có thể bị đe doạ bởi**			
	Gói tin	**Mã lệnh**	**EE**	**Nút mạng**
Người gửi		Có	Có	Có
Mã lệnh	Có	Có	Có	Có
EE	Có	Có	Có	Có
Nút mạng	Có	Có	Có	

Bảng 8. Tóm tắt các mối đe doạ đối với các thực thể

Thực thể	**Có thể tự bảo vệ khỏi những đe doạ từ**			
	Gói tin	**Mã lệnh**	**EE**	**Nút mạng**
Người gửi		Có	Phải tin tưởng	Phải tin tưởng
Mã lệnh	Có	Có	Phải tin tưởng	Phải tin tưởng
EE	Có	Có	Có	Phải tin tưởng
Nút mạng	Có	Có	Có/Không	

Bảng 9. Khả năng tự bảo vệ của các thực thể

III.4 . Phương pháp phân quyền

Chúng ta sẽ xây dựng một kiến trúc an toàn cho hệ thống mạng tích cực tập trung vào việc thi hành chính sách phân quyền. Các thành phần của mạng phải tôn trọng và thực thi chính sách đặt ra. Trước tiên, cần có một ngôn ngữ mô tả chính sách được xây dựng. Sau đó, phải có một phương thức đại diện (ví dụ sử dụng số định danh) cho những thực thể cần được cấp quyền. Cuối cùng, phải có một cơ chế để đảm bảo việc xác thực.cho các định danh của những thực thể kể trên và tính toàn vẹn của các gói tin.

III.4.1 . Chính sách phân quyền

Theo cách tiếp cận xây dựng mô hình an toàn thông tin vừa trình bày trong phần trên, một chính sách cần được xây dựng và áp dụng trong hệ thống. Như vậy, một ngôn ngữ mô tả chính sách cần được xây dựng. Ngôn ngữ này phải được hiểu bởi tất cả các thực thể trên toàn mạng, nhờ đó, các đoạn mã tích cực có thể thực hiện chính sách của chúng tại mỗi nút mạng chúng truyền qua để truy cập vào dữ liệu của các gói tin, các biến trạng thái, và những dịch vụ được cung cấp bởi mã tích cực.

Một *danh sách điều khiển truy cập* (Acces Control List - ACL) đơn giản có thể phù hợp với nhiều ứng dụng. Để có thể sử dụng các ACL trong việc thể hiện các chính sách của mã tích cực, các thực thể phải được định danh duy nhất trong toàn mạng. Sau đây, chúng ta sẽ phân tích một ACL trong thiết bị dẫn đường của hãng Cisco để minh hoạ việc sử dụng chúng trong việc thể hiện các chính sách.

```
access-list 101 permit tcp host 10.1.4.98 198.1.1.0 0.0.0.255 eq www
```

Trong ACL này, router cho phép máy tính có địa chỉ 10.1.4.98 truy cập đến mạng có địa chỉ 198.1.1.0 sử dụng dịch vụ www (tương ứng với cổng 80 TCP). Lưu ý rằng đối với mạng sử dụng bộ giao thức internet TCP/IP, một cặp bao gồm (i) địa chỉ IP và (ii) cổng TCP hoặc UDP xác định duy nhất một thực thể trên mạng. Như vậy, để sử dụng ACL trên, mạng TCP/IP có một phương thức đánh địa chỉ duy nhất cho các thực thể của nó.

Chính sách của các nút mạng có thể được xây dựng và lưu trữ trên các nút mạng hoặc trên các máy chủ chứa chính sách riêng và được tải về khi cần sử dụng. Cũng có thể sử dụng các gói tin để phát tán các chính sách trên hệ thống mạng.

III.4.2 . Xác thực

Giữa các nút mạng tích cực *láng giềng* (kết nối trực tiếp với nhau) cần có một cơ chế bảo vệ điểm-điểm để đảm bảo tín hiệu truyền giữa chúng cũng như đảm bảo an toàn cho việc truyền thông. Trong trường hợp mạng bao gồm những nút mạng tích cực đan xen với những nút mạng thông thường, đôi khi các nút láng giềng không phải là nút trực tiếp kết nối với nhau mà được cấu hình để trỏ đến một nút

mạng tích cực (giữa chúng là các nút mạng thông thường). Kể cả khi các nút mạng tích cực được kết nối trực tiếp hay thông qua việc cấu hình, nút mạng tích cực phải biết các nút láng giềng của chúng và chia sẻ *mã khoá* (key) để bảo vệ việc truyền thông giữa chúng.

Một điều cần chú ý là nếu các nút mạng tích cực không kết nối trực tiếp với nhau, có thể có khả năng một nút mạng không được cấu hình là láng giềng có thể nhận được gói tin và xử lý nó. Trong trường hợp trên, nếu một nút mạng tích cực trung gian nhận được gói tin và xử lý, nó có thể phá vỡ cơ chế bảo vệ điểm-điểm. Hậu quả của việc này giống như việc một kẻ bên ngoài chặn và thay đổi gói tin (một kiểu tấn công chủ động). Trong trường hợp gói tin bị thay đổi, lựa chọn tốt nhất tại nút mạng đích là loại bỏ gói tin đó. Các nút mạng tích cực trung gian phải được thông báo về việc chúng đã thay đổi các gói tin không gửi cho chúng.

Bảo vệ điểm-điểm phù hợp với việc bảo vệ tính toàn vẹn và xác thực các kết nối giữa các nút. Trong trường hợp việc xác thực chỉ dựa trên định danh của nút láng giềng gửi gói tin, bảo vệ điểm-điểm rất có hiệu quả. Tuy nhiên, nếu việc xác thực dựa trên thông tin của nút mạng *nguồn* (nút đầu tiên nơi sinh ra gói tin), phương pháp này hoạt động không hiệu quả nữa, lý do là mỗi nút mạng có thể sinh ra các gói tin với địa chỉ nguồn giả nào đó. Việc sử dụng phương pháp bảo vệ điểm-điểm yêu cầu phải *tin tưởng* tất cả các nút mạng tích cực trên toàn bộ hệ thống mạng, như vậy, phải xây dựng một *mô hình tin tưởng* (trust model) quá rộng. Vì vậy, chúng ta có thể sử dụng một mô hình bảo vệ điểm-điểm mạnh hơn sử dụng mật mã.

Lựa chọn mã hoá điểm-điểm thực sự là một thách thức trong mạng tích cực. Các kỹ thuật mã hoá có thể được chia làm hai loại (i) *không đối xứng* (asymmetric – mã hoá sử dụng khoá công khai để mã hoá và khoá bí mật để giải mã) và (ii) *đối xứng* (symmetric – sử dụng cùng một khoá để mã hoá và giải mã). Quan hệ tin cậy được xây dựng khác nhau theo từng loại mã hoá mà ta lựa chọn.

Sử dụng kỹ thuật mã hoá không đối xứng (ví dụ chữ ký điện tử) chỉ yêu cầu nút mạng nguồn được tin cậy. Chỉ thực thể giữ khoá bí mật có thể xác nhận nút mạng nguồn đã sinh ra gói tin dựa trên mã khoá. Mã hoá không đối xứng cũng có thể sử

dụng để xây dựng những hệ thống *chống chối bỏ* (non-repudiation). Tuy nhiên, nếu gói tin bị thay đổi trên một nút mạng nào đó trong mạng tích cực (điều này có thể sảy ra trong mạng tích cực – khác với mạng thông thường nội dung gói tin không thay đổi), việc xác minh chữ ký điện tử của gói tin đó sẽ không thực hiện được. Có thể giải quyết việc các gói tin bị thay đổi bằng cách cho các nút mạng biết mã khoá bí mật để chúng có thể tính toán lại chữ ký điện tử với nội dung gói tin thay đổi, tuy nhiên điều này làm mất ý nghĩa của việc sử dụng chữ ký điện tử.

Các kỹ thuật mã hoá đối xứng (ví dụ HMAC-MD5 hoặc DES-MAC) có thể được sử dụng nếu khoá của nút mạng nguồn sinh ra gói tin được lưu tại mỗi nút mạng trên đường truyền của gói tin. Tuy nhiên, trong một mô hình tin tưởng lớn được xây dựng dựa trên việc chia sẻ mã khoá, mỗi nút mạng có thể sử dụng mã khoá đó để tạo ra các gói tin như những gói tin được sinh ra tại nút nguồn. Như vậy, sử dụng mã đối xứng chỉ có thể xây dựng hệ thống chống chối bỏ trong đó nút nguồn của gói tin phải là một trong số những nút mạng cùng chia sẻ mã khoá. Mô hình tin cậy phụ thuộc rất nhiều vào phương thức phân phát mã khoá.

Một mã khoá có thể được phân phát bởi các ứng dụng tích cực, các ứng dụng này cài đặt các mã khoá trên các nút mà gói tin tích cực đã được mã hoá có thể đi qua. Một vài kỹ thuật phân phát khoá có thể gây tốn kém về khả năng tính toán cũng như làm tăng độ trễ của hệ thống. Ngoài ra, những nút mạng làm công việc phân phát khoá cũng phải được tin tưởng vì chúng có khả năng sinh những gói tin giống như gói tin của bất cứ nút mạng nào sử dụng mã khoá mà chúng phân phát. Tóm lại, trước khi các gói tin tích cực được truyền trên mạng, có thể sử dụng những phương pháp phân phát mã để tạo ra một "*đường đi an toàn*" với các thông tin được mã hoá trong mạng. Trong trường hợp các gói tin đi lạc ra khỏi đường đi an toàn có thể làm tăng thêm số nút trong đường đi an toàn và do đó mô hình tin tưởng phải mở rộng thêm, tất nhiên điều này sẽ dẫn tới hậu quả làm tăng độ trễ của mạng cho việc thực hiện thêm việc phân phát khoá cho các nút mạng nằm bên ngoài đường đi an toàn đã định sẵn. Phân phát khoá ở mức ứng dụng cũng đòi hỏi các ứng dụng phải có cài đặt những cơ chế an toàn nhất định.

Khoá đối xứng cũng có thể được phân phát trên mức hệ điều hành mạng tích cực (NodeOS) bằng cách ký (sử dụng mã hoá không đối xứng) khoá đó tại nút mạng ban đầu và mã hoá chữ ký đó điểm-điểm trên từng nút mạng láng giềng. Mô hình tin cậy trong trường hợp này chứa tất cả những nút trong mạng có thể nhận gói tin vào một thời điểm nào đó. Tất cả các nút này đều biết khoá đối xứng và có thể tạo ra các gói tin giống như nút ban đầu. Kỹ thuật phân phát khoá này cho phép các nút mạng bảo vệ các ứng dụng không có cơ chế an toàn.

Để xây dựng mô hình tin cậy nhỏ nhất (chứa ít nhất các nút) đồng thời cung cấp dịch vụ không chối cãi được, chúng ta có thể chia phần dữ liệu của gói tin thành hai (2) phần (i) phần thứ nhất chứa mã và các dữ liệu tĩnh, (ii) phần còn lại có thể thay đổi. Chữ ký điện tử chỉ thực hiện trên phần thứ nhất, phần thứ hai có thể không cần bảo vệ. Khi sử dụng kỹ thuật mã đối xứng có thể mã hoá phần thứ nhất, thứ hai hoặc cả hai phần.

III.4.3 . Các thực thể và giấy uỷ nhiệm

Một thực thể trong một kiến trúc an toàn có thể tạo ra một yêu cầu dẫn đến việc xác thực. Nói cách khác, nó là một thực thể có thể xác thực được trong hệ thống. An toàn trong mạng tích cực không chỉ dựa vào định danh của các thành phần trong mạng mà còn dựa trên các thuộc tính sử dụng để xác thực chúng. Một định danh của thành phần và những thuộc tính xác thực của nó biểu hiện trong *giấy uỷ nhiệm* (credential) của nó, giấy uỷ nhiệm này là một thành phần quan trọng trong kiến trúc an toàn.

Kinh nghiệm trong việc thiết kế các hệ thống an toàn cho thấy việc cố gắng miêu tả các chính sách cho từng thành phần trong mạng về những thực thể chúng có quyền truy cập tới khó có thể thực hiện được. Hơn nữa, các miêu tả của chính sách có thể khó hiểu cho việc thi hành các chính sách đó. Một số cách khác đã được đề xuất để gộp các thành phần và các thực thể thành các nhóm có cùng chung một số thuộc tính và sử dụng các thuộc tính để ra các quyết định về an toàn thay cho việc quyết định trên từng thực thể. Các thuộc tính miền (domain), nhóm (group), nhãn (label)… có thể được sử dụng trong các ngôn ngữ xây dựng chính

sách để làm cho những chính sách đó dễ hiểu và dễ thực hiện hơn. Có thể làm rõ điều này qua ví dụ sau:

Có các thực thể và thuộc tính sau

Thuộc Tính / **Thực thể**	**Đến từ nút**	**Nhóm**	**Nhãn**
Thực_thể_A	Nút_X	Nhóm_A	A
Thực_thể_B	Nút_X	Nhóm_B	B
Thực_thể_C	Nút_X	Nhóm_C	C

Chính sách tại Nút_Y

Cấm thực_thể_A

Cấm thực_thể_B

Cấm thực_thể_C

Có thể được phát biểu lại: cấm mọi thực thể đến từ Nút_V

Rõ ràng phát biểu thứ hai rõ ràng hơn và dễ dàng thực hiện bằng cách kiểm tra thuộc tính "Đến từ nút" của các thực thể trong trường hợp này có thể là các gói tin. Phát biểu thứ nhất chỉ có thể thực hiện đúng nếu như Nút_A chỉ có những thực thể liên quan là thực_thể_A, thực_thể_B, thực_thể_C; trường hợp Nút_A chứa các thực thể khác, phát biểu thứ nhất trở thành không đầy đủ và không sử dụng được.

Trong quá trình một gói tin truyền trên mạng, nó phải chạm trán với nhiều miền bảo mật khác nhau. Các thuộc tính bảo đảm an toàn trên mỗi miền cũng khác nhau. Lý do là gói tin là đối tượng để xác thực tại mỗi điểm nó được thực hiện và mọi thuộc tính sử dụng trong chính sách an toàn phải được thoả mãn. Một giấy uỷ nhiệm không đủ để đáp ứng tất cả những yêu cầu vè các thuộc tính. Trong một mạng tích cực diện rộng cần có nhiều giáy uỷ nhiệm để miêu tả tất cả các thuộc tính được yêu cầu tại những điểm khác nhau trên mạng. Kiến trúc gói tin tích cực phải có khả năng truyền tải danh sách của các giấy uỷ nhiệm đó.

Không gian nhớ cần thiết để lưu các giấy uỷ nhiệm có thể khá lớn bao gồm các giấy uỷ nhiệm và danh sách của chúng. Vì lý do đó, chúng ta mong muốn những giấy uỷ nhiệm có thể được sử dụng không trực tiếp thông qua các hệ thống phân tán giấy uỷ nhiệm được hiểu trên toàn mạng và được lưu tại những vị trí dễ truy cập (ví dụ Kerberos, DNSSEC…)

III.4.4 . Kiến trúc gói tin hỗ trợ việc phân quyền

Kiến trúc gói tin phải hỗ trợ danh sách các giấy uỷ nhiệm, phần tĩnh và phần động của gói tin, thông tin xác thực sử dụng mã hoá đối xứng và không đối xứng. Kiến trúc của gói tin có thể được xây dựng dựa trên kiến trúc gói tin tích cực như sau:

Thành phần của gói tin	**ý nghĩa**
ANEP header	Phần đầu của gói tin tích cực
Static Payload	Phần cố định
Varying Payload	Phần thay đổi
Security field Credential Coverage Authenticator	Các trường sử dụng cho việc xác thực
In-Line policy	Các chính sách có thể chứa trong gói
Orginal ANEP Options	Phần đầu (nguyên thuỷ) của gói tin tích cực
Hop Integrity	Bộ đếm (tương đương với TTL trong IP)

Bảng 10. Thành phần của gói tin

III.4.5 . Các thành phần trong phương pháp phân quyền

Chúng ta giao việc xác thực các gói tin cho NodeOS vì ba lý do. Thứ nhất (i) những chức năng này thường được sử dụng cho mọi EE. Thứ hai (ii), NodeOS phải quản lý tài nguyên của chính nó. Thứ ba (iii) các kênh *chuyển nhanh* (cut-

through) thông thường khó được bảo vệ nếu việc xác thực được thực hiện tại các EE. Do các kênh chuyển nhanh được thiết kế để bỏ qua việc xử lý tại các EE, các EE không có cơ hội để xác thực những gói tin đã sử dụng tài nguyên của chúng.

- **Hệ thống mã hoá:** Hệ thống mã hoá phải cung cấp một cơ chế tính toán các thủ tục đảm bảo toàn vẹn và xác thực. Hệ thống mã hoá cũng phải cung cấp cơ chế phân phát khoá để sinh, nhận, trao đổi, thoả thuận… khoá giữa các thực thể, ngoài ra có thể quản trị cơ sở dữ liệu khoá.
- **Hệ thống giấy uỷ nhiệm:** Hệ thống giấy uỷ nhiệm bao gồm các hệ thống con hệ thống lưu trữ toàn cục, kiến trúc phân phát, và hệ thống lưu trữ địa phương. Hệ thống lưu trữ toàn cục là một hệ thống phân tán an toàn có khả năng tạo, lưu trữ, phục hồi và/hoặc phổ biến, và huỷ bỏ các giấy uỷ nhiệm. Hệ thống lưu trữ địa phương cung cấp khả năng lưu trữ, nhận và/hoặc phục hồi, công nhận và loại bỏ các giấy uỷ nhiệm được lưu trong nó. Hệ thống giấy uỷ nhiệm còn cung cấp cơ chế công nhận các giấy uỷ quyền được phục hồi từ các giấy uỷ nhiệm khác.
- **Hệ thống chính sách:** Hệ thống chính sách là một cơ sở dữ liệu quản trị chính sách và một cơ chế thực thi các chính sách. Hệ thống quản trị chính sách phải lưu trữ và bảo vệ các phát biểu trong các chính sách nó lưu trữ để cung cấp cho tiến trình thực thi. Nó phải cung cấp khả năng thêm, sửa hoặc loại bỏ các phát biểu của chính sách.
- **Thi hành:** Việc thi hành không nhất thiết phải được phân thành một phần của kiến trúc an toàn, tuy nhiên, nó là phần cần thiết cho việc thực thi các chức năng an toàn. Để đảm bảo chắc chắn an toàn trong hệ thống, việc thi hành phải đảm bảo ba tính chất sau: (i) *Không thể bỏ qua* (non-bypassable), cơ chế thi hành phải nắm bắt được mọi yêu cầu truy cập tới những tài nguyên hoặc dịch vụ được bảo vệ. (ii) *Không thể phá vỡ* (tamper proof) cơ chế thi hành phải an toàn đối với việc thay đổi có thể làm cho nó không thực hiện được chức năng

III.5 Kết luận chương 3

Trong chương 3 của luận văn, tác giả đã nêu lên một cách nhìn mới "an toàn thông tin luôn luôn là vấn đề cần giải quyết đồng thời là vấn đề để các nhà khoa học tranh luận". Phần đầu của chương trình bày những vấn đề an toàn thông tin trên mạng mà chủ yếu là định danh những kẻ tấn công và phương pháp tấn công vào hệ thống. Trong phần cuối chương, tác giả đề xuất mô hình dựng kiến trúc an toàn thông tin như một mô hình xoắn ốc gồm nhiều giai đoạn và bước đồng thời áp dụng vào việc phát triển phương pháp phần quyền trong kiến trúc an toàn của mạng tích cực.

CHƯƠNG IV. ỨNG DỤNG CÔNG NGHỆ MẠNG TÍCH CỰC TRONG VIỆC XÂY DỰNG HỆ THỐNG TÁC NGHIỆP QUẢN LÝ CHƯƠNG TRÌNH TRUYỀN HÌNH

IV.1 Đặt vấn đề

IV.1.1 Ý nghĩa của việc xây dựng hệ thống

Trong bản đề án "Tin học hoá quản lý hành chính Nhà nước Đài Truyền Hình Việt Nam", ý nghĩa của "Hệ thống tác nghiệp quản lý sản xuất chương trình truyền hình" được nêu như sau:

"Hệ thống quản lý tác nghiệp sản xuất chương trình truyền hình giúp cho lãnh đạo các đơn vị thuộc *Khối sản xuất chương trình* và *Khối quản lý* cũng như lãnh đạo Đài nắm bắt một cách thực tế kế hoạch, tiến độ sản xuất chương trình. Đồng thời hệ thống cũng cung cấp thông tin đầy đủ và chính xác nhất về mối quan hệ tác nghiệp giữa các đơn vị trong đài, hiệu suất làm việc của các bộ phận và từng cán bộ chuyên viên, phóng viên, biên tập viên để từ đó lãnh đạo các cấp đề ra những quyết định, điều chỉnh thích hợp" [5].

IV.1.2 Mô tả các bước thực hiện chương trình truyền hình

Hiện nay, việc quản lý tác nghiệp sản xuất chương trình truyền hình được thực hiện thủ công theo các bước sau:

1. Các đơn vị sản xuất chương trình căn cứ vào khả năng của mình và lịch phát sóng, đăng ký đề tài, chuyên mục để thực hiện chương trình với *Ban biên tập*.
2. Sau khi được duyệt đề tài chuyên mục hoặc đăng ký nội dung bản tin, *phóng viên* (người trực tiếp đi thu thập tin bài) kết hợp với *kỹ thuật viên* (các kỹ thuật viên sử dụng các máy móc chuyên dụng giúp đỡ phóng viên trong các công việc quay phim, dựng phim...) và các cá nhân có liên quan khác tiến hành việc quay phim.
3. Băng quay được trong bước trên được chuyển sang các phòng dựng tại Trung tâm kỹ thuật sản xuất chương trình. Tại đây, phóng viên, kỹ thuật viên kết hợp với *biên tập viên* (chịu trách nhiệm về nội dung chương trình) và hoạ sỹ thực

hiện các công việc liên quan đến kỹ thuật truyền hình như cắt dán hình, lồng tiếng, làm kỹ xảo...

4. Sau khi sản xuất xong chương trình, sản phẩm sẽ là băng hình hoàn chỉnh được trình lãnh đạo để nghiệm thu kỹ thuật và duyệt nội dung.
5. Nếu băng ghi hình đảm bảo nội dung và chất lượng, băng sẽ được chuyển qua bộ phận phát sóng.

IV.1.3 Những tồn tại trong bài toán

Trong quá trình xây dựng các chương trình thời sự, nhất là những chương trình trực tiếp như cầu truyền hình, đối thoại trực tiếp hoặc tường thuật tại chỗ một sự kiện văn hoá, thể thao, việc quản lý chỉ đạo thay đổi nội dung rất khó khăn do quy trinh làm việc thủ công.

Khi cần thay đổi nội dung chương trình, cần có công văn chỉ đạo của lãnh đạo với chữ ký và dấu; hơn nữa, việc chuyển công văn đi giữa các bộ phận đôi khi không đủ nhanh để kịp can thiệp vào quá trình sản xuất chương trình.

IV.2 Đề xuất sử dụng công nghệ mạng tích cực giải quyết vấn đề của bài toán

Trong khuôn khổ luận văn, chúng tôi không có tham vọng xây dựng hoàn chỉnh hệ thống quản lý tác nghiệp sản xuất chương trình truyền hình. Thay vào đó, chúng tôi đề xuất việc sử dụng công nghệ mạng tích cực đã được trình bày trong các phần trước của nội dung luật văn vào việc giải quyết vấn đề mấu chốt của hệ thống thông qua bài toán con "hệ thống hỗ trợ việc chỉ đạo xây dựng nội dung chương trình thời sự".

Bài toán con này có thể được miêu tả cụ thể như sau: Xây dựng mạng máy tính cho phép lãnh đạo và ban biên tập chỉ đạo trực tiếp nội dung trong khi thực hiện các chương trình thời sự hoặc phát trực tiếp.

Mạng máy tính được xây dựng phải thoả mãn những yêu cầu sau:

1. Hệ thống cho phép lãnh đạo và ban biên tập xem trực tiếp chương trình đang được xây dựng/phát sóng (có thể với chất lượng hình ảnh thấp - do chỉ có nhu cầu chỉ đạo nội dụng)
2. Hệ thống mạng cho phép xác thực người sử dụng để xác định quyền của người sử dụng đó trong hệ thống. Người sử dụng đã được xác thực có quyền tham gia vào việc chỉ đạo nội dung chương trình đang sản xuất.

Bài toán con đặt ra hai vấn đề về công nghệ cần được giải quyết: (i) vấn đề truyền thông dữ liệu hình ảnh sử dụng băng thông lớn và (ii) xác thực người sử dụng trong hệ thống.

Vấn đề thứ nhất có thể được giải quyết thông qua các công nghệ mạng tích cực là cơ chế lưu trữ đệm (caching) và khả năng tính toán trên các nút mạng. Vấn đề thứ hai có thể giải quyết thông qua các cơ chế xác thực như đã trình bày trong phần trước của luận văn.

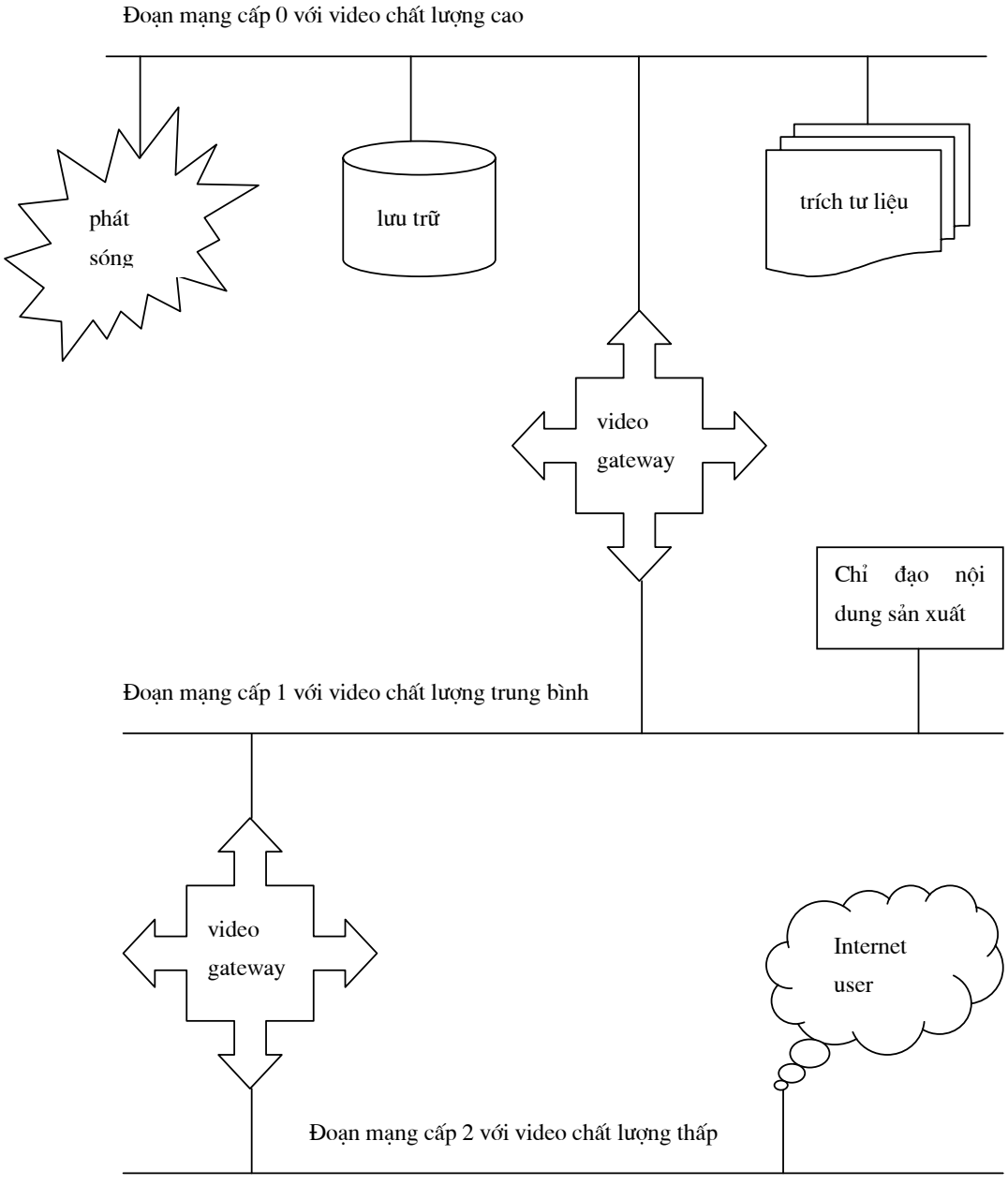
IV.2.1 Kiến trúc mạng phân cấp theo chất lượng hình ảnh

Chất lượng của hình ảnh càng cao, dung lượng của các tệp (trong truyền thông đôi khi sử dụng thuật ngữ *dòng* thay cho tệp) càng lớn. Một cách để giảm dung lượng của các tệp tin đồng nghĩa với giảm thông lượng chúng chiếm trên mạng là sử dụng những chuẩn nén khác nhau có thể cho chất lượng hình ảnh khác nhau với tỷ lệ nén khác nhau.

Tuy nhiên, phụ thuộc vào yêu cầu công việc của mình, người sử dụng hệ thống có nhu cầu sử dụng các tệp hình ảnh có chất lượng khác nhau:

- Các phóng viên, biên tập viên cần sử dụng hình ảnh tư liệu (các đoạn trích), kỹ thuật viên tại bộ phận phát sóng, bộ phận lưu trữ cần chất lượng hình ảnh cao để đảm bảo nhu cầu sử dụng và phát sóng của họ.
- Lãnh đạo Đài, các thành viên của Ban biên tập cần theo dõi và chỉ đạo nội dung các chương trình đang thực hiện chỉ có nhu cầu xem các chương trình đó với chất lượng hình ảnh trung bình, hoặc có độ phân giải thấp.
- Bộ phận quản lý trang thông tin điện tử của Đài lại quan tâm chủ yếu đến việc làm sao giảm tối thiểu dung lượng truyền thông trên mạng để phục vụ

khác hàng truy cập trang thông tin qua mạng Internet (đôi khi sử dụng modem quay số) và xem các chương trình đó. Vì vậy, họ sẽ sử dụng những công nghệ nén có tỷ lệ cao nhất mặc dù có thể làm giảm chất lượng của hình ảnh đi khá nhiều.



Hình 14. Mô hình video phân cấp

Công nghệ do chúng tôi đề xuất để giải quyết chất lượng của hình ảnh là xây dựng một kiến trúc mạng hình ảnh phân cấp với dữ liệu truyền trong cấp cao nhất bao gồm các tệp hình ảnh có chất lượng cao phục vụ nhu cầu của đối tượng thứ nhất. Tại mỗi lớp sẽ có một *video gateway* được cài đặt bởi một nút mạng tích cực xử lý việc chuyển đổi mã video cho ra những hình ảnh có chất lượng thấp hơn nhưng có dung lượng nhỏ hơn nhiều lần phục vụ cho các đối tượng sử dụng tương ứng.

Thông số	**MPEG-1**	**MPEG-1**
Độ phân giải NTSC (horizontal x vertical)	720/704 x 480 352 x 480/240	352 x 480 351 x 240
Độ phân giải PAL/SECAM (horizontal x vertical)	720/704 x 576 352 x 576/288	352 x 576 352 x 288
VBR or CBR2	VBR or CBR	CBR
PAL/SECAM frame rate	25 fps	
NTSC frame rate	24 or 29.97 fps	

Bảng 11. Các thông số video

Mô hình này, có thể tiết kiệm được băng thông của mạng sử dụng cho việc truyền thông dữ liệu hình ảnh đồng thời vẫn đảm bảo đáp ứng được nhu cầu của các đối tượng sử dụng khác nhau trong mạng.

Tính năng	**Lazer disc**	**Video CD**	**SVCD**	**DVD-VIDEO**
Định dạng mã hoá	Tương tự	MPEG-1 (CBR)	MPEG-2 (VBR)	MPEG-2 (VBR)
Kích thước hình ảnh		352 x 240/288	480 x 480/576	720 x 480/576
Video bit rate		1.15 Mb/s	2.6 Mb/s	3.5 Mb/s
Chất lượng hình ảnh	Đẹp	Không đẹp	Đẹp	Rất đẹp

Tính năng	Lazer disc	Video CD	SVCD	DVD-VIDEO
Ngôn ngữ	1	1	2 stereo 4 mono	Tối đa 8

Bảng 12. Một số chuẩn lưu trữ video

IV.2.2 Thiết bị mạng sử dụng trong hệ thống

Trong mạng mức 0, hình ảnh được sử dụng cho nhu cầu sản xuất, phát sóng, trích dẫn và lư trữ, do đó hình ảnh ở mạng mức 0 đòi hỏi có chất lượng cao. Kèm theo điều kiện trên, dung lượng đòi hỏi đối với hình ảnh ở mạng mức 0 cũng rất cao.

Chính do nhu cầu truyền thông cao trong mạng mức 0, các thiết bị sử dụng trong mạng đòi hỏi có băng thông cao để thoả mãn nhu cầu. Chúng tôi đề xuất sử dụng các thiết bị chuyển mạch tốc độ cao trong mạng mức 0.

Thiết bị chuyển mạch lựa chọn là thiết bị của hãng Extreme mang số hiệu Summit5i với 12 cổng Ethernet tốc độ 1Gbps và 8 cổng quang tốc độ 1 Gbpsc.

Mạng mức 1 phục vụ chủ yếu nhu cầu quản lý nội dung và theo dõi tiến độ thực hiện chương trình truyền hình. Hình ảnh trong mạng mức 1 không đòi hỏi yêu cầu khắt khe về chất lượng mà chủ yếu là truyền tải nội dung đến các đối tượng là lãnh đạo và ban biên tập.

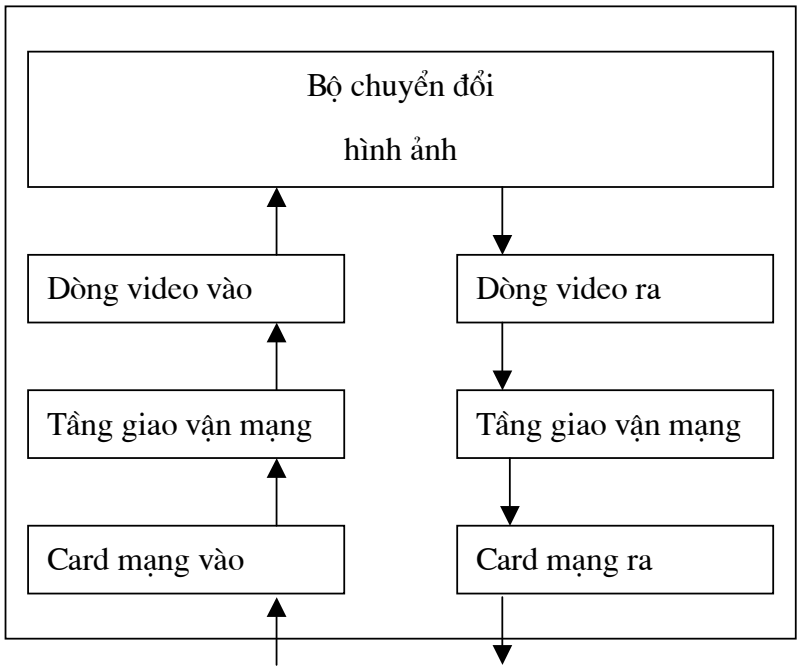
Thiết bị chuyển mạch lựa chọn là thiết bị của hãng Extreme mang số hiệu Summit24e2/ Summit24e2 với 24/48 cổng Ethernet tốc độ 100Mbps và 2 cổng Ethernet tốc độ 1 Gbpsc kết nối với mạng mức trên thông qua video gateway.

Mạng mức 2 sử dụng cho các đối tượng khác thông thường là người sử dụng quay số hoặc truy cập thông qua Internet, hình ảnh trong mạng mức 2 không yêu cầu chất lượng mà là dung lượng nhỏ để truyền trên mạng Internet.

Thiết bị mạng không cần thông lượng cao, có thể sử dụng các loại thiết bị chuyển mạch tốc độ 10/100 thông thường.

IV.2.3 Cài đặt video gateway

Video gateway có thể được cài đặt trên máy server có năng lực xử lý mạnh để đảm bảo nhu cầu tính toán trong việc chuyển đổi các khuôn dạng hình ảnh.

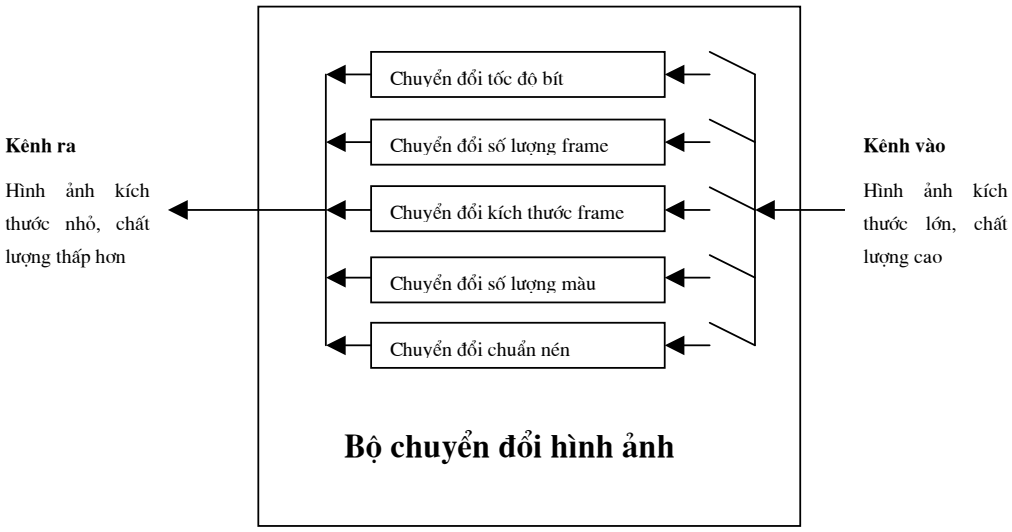


Hình 15. Sơ đồ khối video gateway

Việc cài đặt video gateway được thực hiện trên nút mạng tích cực để sử dụng khả năng tính toán trên mạng của phương pháp tiếp cận này. Trong đó, trung tâm của nút mạng chính là bộ chuyển đổi hình ảnh với khả năng chuyển đổi hình ảnh qua nhiều khuôn dạng khác nhau với tốc độ bít, số lượng frame, kích thước frame, chuẩn nén khác nhau, qua đó có thể làm giảm thông lượng cần thiết để truyền các hình ảnh giữa các đối tượng.

Chúng tôi đề xuất sử dụng máy chủ PowerEdge 6650 của hãng Dell cho việc cài đặt videogateway với các tính năng:

- 2 card mạng 10/100/1000 Mpbs
- 4 Bộ xử lý Xeon tốc độ 3.06 GHz
- Bộ nhớ RAM 8 GB (max 16 GB)



Hình 16. Cấu tạo bộ chuyển đổi hình ảnh

IV.2.4 Thử nghiệm việc chuyển đổi hình ảnh

Trong khuôn khổ luận văn, chúng tôi không đủ thiết bị và thời gian để thử nghiệm và cài đặt các mô dun đã được đề xuất. Tuy nhiên, chúng tôi thực hiện một số thử nghiệm trong việc chuyển đổi các khuôn dạng hình ảnh và đưa ra các so sánh thực tế về chất lượng và kích thước tương ứng của các khuôn dạng hình ảnh sử dụng trong thử nghiệm.

Từ đó, chúng tôi đang tiến hành chứng minh bằng thực nghiệm rằng việc cài đặt và sử dụng video gateway có thể làm giảm thông lượng mạng yêu cầu trong hệ thống tác nghiệp quản lý sản xuất chương trình truyền hình. Như vậy, một vấn đề công nghệ mấu chốt của bài toán có thể được giải quyết và bài toán tổng thể cũng có thể được giải quyết trong tương lai.

Việc thử nghiệm thực hiện trên phần mềm "Video Transcoding and Streaming Demo" được tải từ địa chỉ

http://www.discover.uottawa.ca/~leizj/Experiences/TransServer/

Ứng dụng gồm ba phần: phần server thực hiện chức năng chuyển đổi hình ảnh, phần client cho PC chạy trên các máy PC và phần client cho các máy bỏ túi.

Hình 17. Thử nghiệm với hình ảnh màu với frame rate 30

Hình 18. Thử nghiệm với hình ảnh đen trắng

IV.3 Kết luận chương 4

Trong chương này, chúng tôi áp dụng công nghệ mạng tích cực được trình bày trong các chương trước để giải quyết vấn đề công nghệ trong "Hệ thống tác nghiệp quản lý sản xuất chương trình truyền hình". Đóng góp chính trong chương này là đề xuất một mô hình mạng truyền hình ảnh được phân cấp theo nhu cầu sử dụng của các đối tượng sử dụng trong hệ thống. Chúng tôi đã đề xuất cấu hình

phần cứng và sơ đồ khối của phần mềm sử dụng trong hệ thống. Trong chương này, chúng tôi cũng thực hiện một số thử nghiệm chuyển đổi khuôn dạng hình ảnh trên một số phần mềm để chứng tỏ tính khả thi của đề xuất đã được trình bày.

Hướng phát triển tiếp theo của đề xuất là xây dựng dự án khả thi cho hệ thống tác nghiệp quản lý sản xuất chương trình truyền hình trong đó chú trọng việc hoàn thiện mô hình phần mềm đã được đề xuất và lựa chọn các công nghệ thích hợp để có thể xây dựng được hệ thống hoàn chỉnh trong tương lai.

KẾT LUẬN

1. Mạng tích cực là hướng tiếp cận mới mang tính sáng tạo trong việc xây dựng các kiến trúc mạng. Trong hướng tiếp cận này, các thiết bị dẫn đường và thiết bị chuyển mạch trên mạng có thể thực hiện một số tính toán trên các thông điệp được truyền qua chúng. Hướng tiếp cận mạng tích cực có thể thực hiện được do (i) việc các ứng dụng người dùng hiện nay cho phép thực hiện các tính toán trên các nút mạng và (ii) sự phát triển công nghệ mã di chú cho phép sửa đổi động các dịch vụ mạng. Việc phân tích tỷ mỉ từng thành phần trong các cách tiếp cận đang được nghiên cứu giúp người đọc có cái nhìn tổng quát về mạng tích cực và phương hướng phát triển của mạng tích cực trong tương lai.
2. Các ứng dụng sử dụng công nghệ mạng tích cực đang được phát triển và sử dụng tuy nhiên số lượng không nhiều do chưa có nhiều công cụ, mô hình hỗ trợ. Chính vì nguyên nhân đó, tác giả lựa chọn việc giới thiệu bộ công cụ ANTS trong luận của mình với mục đích giúp những người quan tâm đến việc phát triển ứng dụng sử dụng công nghệ này (lập trình viên, người sử dụng) có một cái nhìn tổng quan về bộ công cụ và có thể sử dụng các công cụ đó trong việc phát triển ứng dụng của mình.
3. Cùng với việc cho phép xây dựng các mô hình mạng sáng tạo bằng cách chuyển việc tính toán vào các thiết bị mạng, hướng tiếp cận mạng tích cực phải đối mặt với một vấn đề lớn đó là khả năng mất an toàn thông tin. Khi mỗi người sử dụng đều có thể lập trình cho các thiết bị mạng thông qua các gói tin gửi trên mạng của họ, nguy cơ mất an toàn là rất lớn. Tác giả đã phân tích những vấn đề an toàn thông tin trong mạng thông thường với những kẻ tấn công và phương pháp chúng sử dụng để tấn công vào các hệ thống mạng. Từ đó, tác giả phân tích các rủi ro mà các thành phần trong mạng tích cực có thể gặp phải và khả năng chống lại các rủi ro đó của từng thành phần. Một mô hình phát triển kiến trúc an toàn dạng xoắn ốc cũng được tác giả đề xuất nhằm cung cấp một định hướng cho việc xây dựng

kiến trúc an toàn thông tin nói chung và an toàn thông tin trên mạng tích cực nói riêng.

4. Việc ứng dụng công nghệ mạng tích cực có thể được sử dụng để giải quyết nhiều vấn đề về công nghệ mạng nhất là vấn đề truyền thông dữ liệu lớn. Trong luận văn, tác giả có đề xuất xây dựng mô hình mạng phân cấp được kết nối thông qua các video gateway nhằm giải quyết vấn đề công nghệ trong bài toán xây dựng hệ thống tác nghiệp quản lý sản xuất chương trình truyền hình. Tác giả đề xuất sử dụng công nghệ mạng tích cực để cài đặt các video gateway. Ý tưởng về hệ thống mạng phân cấp và công nghệ mạng tích cực đã được tác giả trao đổi với một số cán bộ kỹ thuật tham gia trực tiếp trong việc xây dựng Đề án tin học hoá cải cách hành chính tại Đài Truyền Hình Việt Nam và được nhiều ý kiến ủng hộ.

Luận văn đã trình bày tổng quan về mạng tích cực, các công cụ phát triển mạng tích cực mà tiêu biểu là bộ công cụ ANTS.

Một kết quả quan trọng là tác giả đã phân tích các vấn đề an toàn thông tin trên mạng nói chung, an toàn thông tin trong mạng tích cực nói riêng từ đó đề xuất mô hình phát triển xoắn ốc cho việc xây dựng các kiến trúc an toàn trên mạng.

Ngoài những kết quả về lý thuyết, luận văn cũng nhằm tới mục tiêu ứng dụng công nghệ mạng tích cực vào việc giải quyết bài toán thực tế tại Đài Truyền Hình Việt Nam. Những đề xuất trong luận văn có thể được phát triển thành dự án khả thi để thực hiện tại Đài Truyền Hình Việt Nam trong một tương lai gần.

TÀI LIỆU THAM KHẢO

Tiếng Việt

[1]. Nguyễn Nhật Bình (1998). *Giao thức TCP/IP và xây dựng chương trình truyền file dựa trên TCP/IP*. Luận văn tốt nghiệp đại học, Khoa Công nghệ Thông tin, Đại học Khoa học Tự nhiên, ĐHQGHN, 1998. (chương II, Chương III).

[2]. GS. TS Phan Đình Diệu (1999). *Lý thuyết mật mã và an toàn thông tin*. Tài liệu giảng dạy tại Khoa Công Nghệ (ĐHQGHN).

[3]. TS. Hà Quang Thuỵ và nhóm nghiên cứu (2002). *Hệ điều hành LINUX: Nghiên cứu và triển khai trọng hoạt động của Khoa Công Nghệ (ĐHQGHN) và ở Việt Nam*. Đề tài nghiên cứu khoa học cấp Đại học Quốc gia Hà Nội (Phần D chương I).

[4]. PGS. TS. Nguyễn Quốc Toản (1998-2002). *Nhập môn công trình học phần mềm*. Tài liệu giảng dạy tại Khoa Công Nghệ (ĐHQGHN).

[5]. *Đề án tin học hoá cải cách hành chính đài truyền hình Việt Nam giai đoạn 2001-2005* (trang 22, trang 68-70 phần phụ lục).

Tiếng Anh

[6]. AN Security Working Group (November 13, 2001). *Security Architecture for Active Nets*. (pages 2-12)

[7]. David J.Wetherall (Massachuset Institude of Technology). *A servey of Active Network Research*..

[8]. David M. Murphy (1997). *Building an Active Node on the Internet*, MIT Master's thesis, May 1997.

[9]. Edwin N. Johnson (1998). *A Protocol for Network Level Caching*, MIT Master's thesis, May 1998.

[10]. K. L Calvert (University of Kentucky). *Architectural Framework for Active Networks version 1.0*. (pages 4-10).

[11]. wssg.berkeley.edu (March 1998). *Computer Security Framwork and principle version 0.3*.

[12]. Simon Cooper, Elizabeth D. Zwicky, D. Brent Chapman. *Building Internet Firewall Second Edition*. O'Reilly Press.

Các trang web liên quan

http://wssg.berkeley.edu

http://www.security-forums.com

http://www.cs.utah.edu/flux/janos/

http://www.cs.washington.edu/research/networking/ants/

http://plateforme.ish-lyon.cnrs.fr/template/standard.php?rubrique=mpeg&langue=en