Tạp chí Tin học và Điều khiển học, T.21, S.4 (2005), 312–322

HỆ THỐNG THOẠI INTERNET AN TOÀN

NGUYỄN VĂN TAM, ĐÀO VĂN THÀNH, PHẠM THANH GIANG

Viện Công nghệ thông tin

Abstract. In this article we present our research into the security problems in Internet phone and our solution for them. In the security problems, the security for information in voice data packet is most important. Our solution is developing the Security Internet phone. In our system, this problem has been solved by encrypting audio data packets before they are transferred in RTP protocol.

Tóm tắt. Bài báo nghiên cứu vấn đề an ninh cho hệ thống thoại Internet. Trong hệ thống điện thoại Internet an toàn, mã mật gói dữ liệu âm thanh là quan trọng nhất. Bài báo trình bày giải pháp mã hóa gói tin trước khi truyền tải qua giao thức thời gian thực RTP.

1. ĐẶT VẤN ĐỀ

Điện thoại Internet đang trở nên rất phổ biến như một hình thức đàm thoại quốc tế với mức cước phí rất rẻ. Tuy nhiên, điện thoại Internet sẽ là mục tiêu dễ dàng của nạn nghe lén. Không như các loại hình nghe lén trên đường điện thoại truyền thống, việc xâm nhập vào các cuộc gọi thoại Internet có thể thực hiện dễ dàng do không yêu cầu có một thiết bị đặc biệt nào.

Để đảm bảo tính riêng tư cho hệ thống thoại Internet ta cần xây dựng các tính năng an toàn như mã hóa hoặc cơ chế bảo mật riêng được tích hợp bên trong mỗi dịch vụ khi lựa chọn một giải pháp thoại Internet.

2. VẤN ĐỀ VỀ AN NINH CỦA THOẠI INTERNET

2.1. Yêu cầu về an ninh

Thoại Internet là một dạng khác của kỹ thuật điện thoại, các gói tiếng nói dưới dạng số hóa được truyền dựa trên việc sử dụng Internet toàn cầu. Địa chỉ của các gói tin dựa vào các giao thức Internet (IP).

Một hệ thống thoại Internet phổ biến gồm có những phần tử chính sau:

+ Người tham gia vào cuộc gọi: người gọi và người nhận cuộc gọi

+ Các thiết bị đầu cuối: được sử dụng để thực hiện gọi và nhận các cuộc gọi.

+ Hệ thống máy chủ quản lý: các cổng nối và các máy chủ tham chiếu tới tất cả các thiết bị trung gian cần trong thời gian cuộc gọi.

+ Phương tiện truyền thông: cổng kết nối liên kết dữ liệu và các thiết bị đầu cuối khác nhau, hình thành đường truyền thông End to End cho những gói thoại Internet đi qua.

Trong thoại Internet các gói tin chưa được mã hoá, tin tặc có thể bắt các gói tin sau đó phân tích. Thông tin trong gói tin bao gồm dữ liệu audio, thông tin điều khiển và các thông

tin liên quan đến hệ thống. Như vậy để đảm bảo an ninh cho thông tin thoại Internet, thông tin trao đổi giữa những người tham gia một cuộc gọi cần phải được giữ bí mật. Những thông tin thoại phải đảm không thể tới bất kì thành viên thứ ba nào kể cả nhà cung cấp dịch vụ.

2.2. Tính nhạy cảm đối với trễ

Vấn đề quan trọng trong truyền tiếng nói qua IP là vấn đề chất lượng của dịch vụ. Trễ trong cuộc nói chuyện khi sử dụng thoại Internet ảnh hưởng lớn đến chất lượng dịch vụ và gây ra sự khó chịu cho người dùng.

+ Để có một cuộc đàm thoại bình thường trên mạng, độ trễ đầu cuối nhất thiết phải là một hằng số và nằm trong giới hạn cho phép:

+ Độ trễ nhỏ từ 10 đến 15ms; người sử dụng sẽ không cảm nhận được vì thế các bộ điều chỉnh tiếng vang, vọng điện tử và âm thanh là không cần thiết.

+ Độ trễ lên tới 150ms thì yêu cầu có điều khiển tiếng vang nhưng không làm giảm tác động lẫn nhau về hiệu quả giữa những người sử dụng hệ thống.

+ Nếu độ trễ từ 200 đến 400ms, hiệu quả của tác động qua lại sẽ thấp hơn nhưng vẫn có thể cảm nhận được.

Nếu độ trễ lớn hơn 400 ms, thông tin thoại tác động lẫn nhau sẽ rất khó và sẽ yêu cầu có các qui luật đàm thoại.

Như vậy để hệ thống thoại Internet đạt được chất lượng chấp nhận được ở người dùng thì độ trễ của hệ thống phải tối thiểu nhỏ hơn 150ms.

Một trong những cách tốt nhất để xử lý giải quyết trễ trong truyền gói VoIP thông thường là sử dụng bộ đệm jitter. Bộ đệm jitter có nhiệm vụ đảm bảo thông tin thoại luôn luôn truyền tới người nghe.

Khi gói thoại đến chúng được gửi vào một bộ đệm mà có thể điều tiết 10 gói (giả sử ta thiết lập một bộ đệm jitter là 100ms), mỗi 10 ms có một gói được truyền xuống bộ đệm. Sự ùn tắc mạng là nguyên nhân một gói không đến được bộ đệm jitter, bộ đệm sẽ vẫn được truyền gói tiếp theo. Điều này tiếp tục cho đến khi nào bộ đệm rỗng. Bộ đệm sẽ đầy lên nhanh chóng sau sự ùn tắc mạng các gói thoại nằm trong hàng đợi sẽ được gửi đi đúng sau khi một gói khác truyền xuống. Ta cần chắc chắn rằng những gói thoại trong hàng đợi có quyền ưu tiên cao hơn các dịch vụ thông thường.

Để thực sự đảm bảo an ninh cho kết nối End to End thì dữ liệu trên đường truyền phải được bảo vệ. Có hai phương pháp mã hóa thường được sử dụng chống lại các cuộc tấn công trên đường truyền là: Mã hóa khóa đối xứng và mã hóa khóa bất đối xứng.

Mã hóa bất đối xứng thích hợp cho việc chứng thực đối với qui mô mạng lớn. Tuy nhiên sử dụng giải pháp dựa trên mã khóa công khai có một số khó khăn. Thứ nhất, hiện nay chưa có tổ chức chứng thực khóa công khai tại Việt Nam. Thứ hai, mã khóa công khai yêu cầu sử dụng sức mạnh tính toán lớn. Nếu mã hóa thực hiện trên hai End Point (EP), thì không có ảnh hưởng lớn nếu thiết bị đủ mạnh để tính toán. Nhưng nếu việc mã hóa được thực hiện trên các thiết bị trung gian có thể dẫn đến hiện tượng thắt cổ chai tại các thiết bị trung gian. Vấn đề đó làm tăng thời gian trễ, gây chậm việc truyền các gói tin thoại.

Mã hóa khóa đối xứng có điểm yếu là cần phải chia sẻ khóa bí mật giữa hai bên truyền thông, do vậy khả năng bị lộ khóa cao hơn so với khóa bất đối xứng. Điểm mạnh của mã hóa khóa đối xứng là có thể thực hiện nhanh hơn so với mã hóa khóa bất đối xứng, do các thuật toán mã hóa khóa đối xứng có độ phức tạp thấp hơn.

Giải pháp được đề xuất là giải pháp End to End sử dụng mật mã khóa đối xứng cho hệ thống an ninh thoại Internet. Các gói thoại Internet được mã hóa và xác nhận trên đường truyền từ người gửi đến người nhận. Việc sử dụng mã hóa khóa bí mật sẽ giảm được các nguy cơ trễ và thắt cổ chai trên đường truyền.

Để có thể xây dựng được hệ thống thoại Internet an toàn, chúng ta sẽ tìm hiểu các giao thức liên quan và các công cụ xây dựng hệ thống.

3. GIAO THỨC KHỞI ĐỘNG CUỘC GỌI SIP

SIP là giao thức báo hiệu, được sử dụng để tạo ra, sửa đổi hoặc kết thúc các cuộc gọi đa phương tiện. Các cuộc gọi có thể được thiết lập với một hoặc nhiều người tham gia. Lớp vận chuyển sử dụng cho giao thức SIP có thể là cả hai UDP hoặc TCP.

Mục đích thiết kế của SIP là có tính chất động, các thành phần có thể sử dụng lại và có tính vận hành với nhau. Trước hết, tính biến đổi được số lượng cuộc gọi. Một người có thể có quyền thực hiện nhiều cuộc gọi khác nhau cùng lúc. SIP được thiết kế để hỗ trợ phạm vi rộng. Người dùng có thể được định vị trên mạng.

3.1. Các phương thức trong SIP

Thông điệp INVITE

Thông điệp Invite là thông điệp đầu tiên được người gọi gửi đi để báo hiệu cuộc gọi. Thông điệp chứa thông tin cuộc gọi trong SIP, qua đó định danh cuộc gọi, người gọi, người nhận cuộc gọi, chỉ số tuần tự của cuộc gọi và các thông tin về giao thức tầng dưới.

Thông điệp ACK

Một phiên SIP đơn giản thành công được bắt đầu bằng thông điệp INVITE. Sau đó sẽ là đáp ứng OK từ đối tác được mời và được xác nhận bằng thông điệp ACK.

Thông điệp OPTION

Thông điệp Option được gửi để truy vấn các khả năng của một đại diện gọi, cũng như để cho đối tác kia biết các khả năng của nơi truyền.

Thông điệp BYE

Khi một đối tác muốn giải phóng cuộc gọi sẽ gửi thông điệp BYE đến đối tác tham gia phiên thoại.

Thông điệp CANCEL

Thông điệp Cancel được sử dụng để huỷ bỏ một yêu cầu trong tiến trình nhưng không ảnh hưởng đến việc thiết lập gọi khi không có yêu cầu nào đang xúc tiến.

3.2. Các bước đăng ký và thực hiện cuộc gọi SIP

Cần có 6 bước để thiết lập và thực hiện một cuộc gọi sử dụng giao thức SIP:

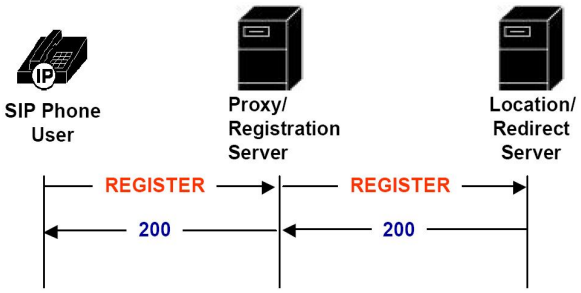
1. Đăng ký, khởi tạo, xác định vị trí của người dùng.

2. Xác định phương tiện truyền thông được sử dụng rồi chuyển các thông tin liên quan tới người nhận cuộc gọi.

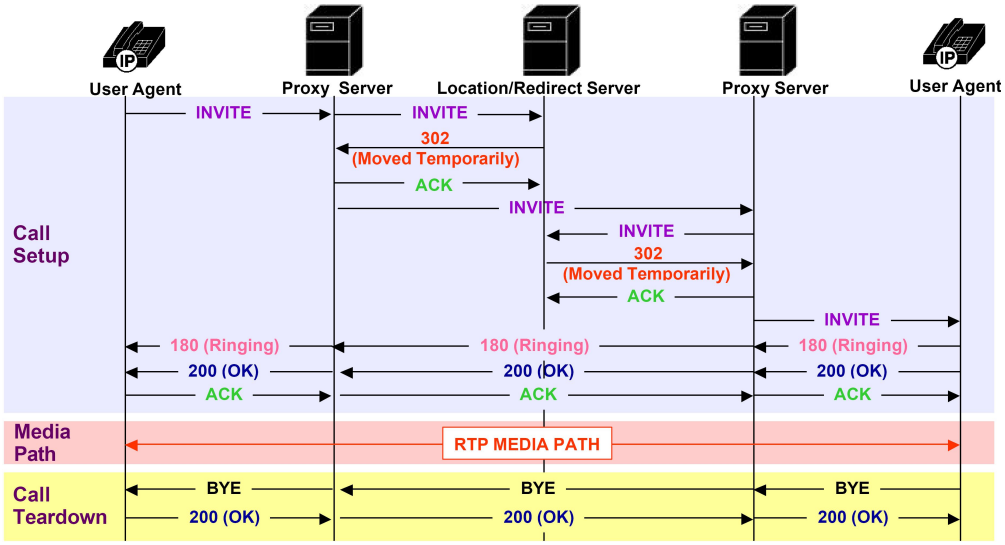
3. Xác nhận sự chấp nhận truyền thông của bên được gọi, bên được gọi phải gửi gói tin trả lời để xác nhận việc chấp nhận hay từ chối cuộc gọi.

4. Thiết lập cuộc gọi.

5. Thay đổi cuộc gọi; ví dụ: Giữ máy, chuyển cuộc gọi.
6. Kết thúc cuộc gọi.



Hình 1. Đăng ký



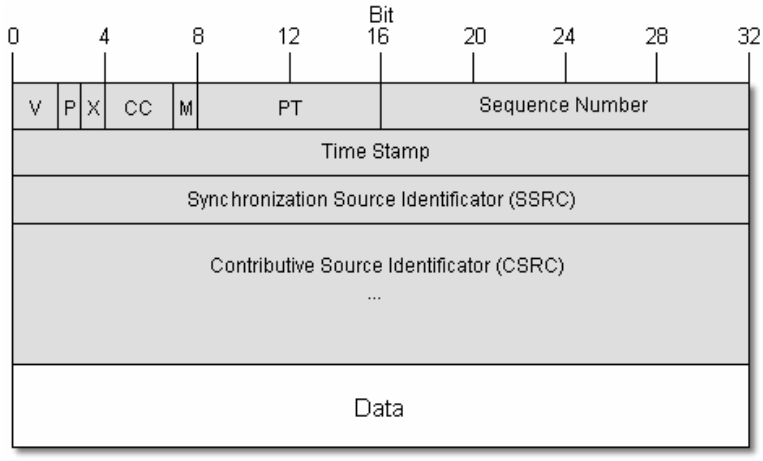
Hình 2. Thực hiện cuộc gọi

4. GIAO THỨC RTP

Giao thức RTP sử dụng cho việc định nghĩa định dạng các gói tin audio, video khi truyền trên Internet. Giao thức RTP không đảm bảo được việc truyền dữ liệu theo thời gian thực, tuy vậy giao thức cung cấp các cơ chế điều khiển thời gian thực trong nội dung gói tin, như nhãn thời gian (timestamp), cơ chế điều khiển các luồng đồng bộ theo thời gian.

Giao thức RTP là một dịch vụ ở tầng ứng dụng, được xây dựng dựa trên cơ sở tầng UDP/IP. Giao thức UDP là giao thức không hướng kết nối (connectionless), không đảm bảo việc truyền tin cậy, tuy nhiên các gói tin RTP được đánh số theo thứ tự, cho phép phát hiện gói tin bị mất trên đường truyền.

Giao thức RTP bao gồm định dạng loại payload, đánh số trình tự, điều khiển truyền dữ liệu. Giao thức RTP cung cấp các chức năng thời gian thực cho ứng dụng, với chức năng tổ chức lại thời gian, phát hiện mất gói tin, xác định kiểu mã dữ liệu.



Hình 3. Định dạng của gói tin RTP

5. LỰA CHỌN THUẬT TOÁN MÃ HÓA

Thuật toán được lựa chọn để mã hóa trong hệ thống phải được đảm bảo về độ an toàn và không ảnh hưởng lớn đến tốc độ và độ trễ của hệ thống. Chúng tôi chọn thuật toán DES, thuật toán DES đã và đang được sử dụng rộng rãi và đã được chứng minh về độ an toàn bảo mật. Hình vẽ mô tả sơ đồ khối cấu trúc của thuật toán mã DES, trong đó bao gồm cả phần mã hóa và phần giải mã được tiến hành đồng thời. Hình mô tả mã khối với độ dài đoạn tin là 64 bit, khóa là 56 bit.

Ta cần phải chứng minh chất lượng cuộc thoại không bị ảnh hưởng về tốc độ và độ trễ khi sử dụng thuật toán DES. Giả sử, trên một mạng truyền voice với tốc độ 128Kbps có sử dụng chương trình nén theo chuẩn G.711. Tín hiệu sau khi đã được nén sẽ được mã hóa với khóa bí mật DES mà cả bên gửi và bên nhận cùng biết.

+ Độ trễ của hệ thống bao gồm:

+ Độ trễ do thời gian lấy mẫu, nén, giải nén theo chuẩn G.711.

+ Độ trễ do thời gian mã, giải mã theo thuật toán DES.

+ Độ trễ do thời gian truyền thông trên mạng.

+ Độ trễ do chia sẻ băng thông cho các dịch vụ khác.

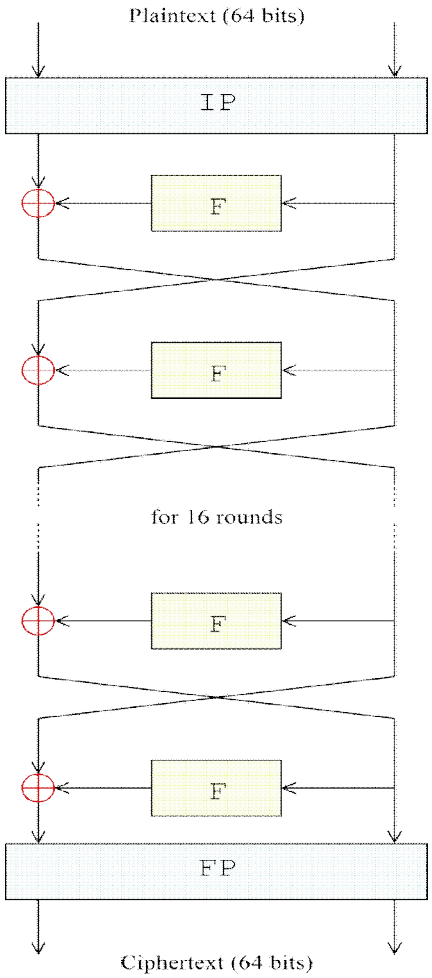
+ Bỏ qua thời gian thao tác của máy tính và thiết bị.

Tốc độ bit của G.711 là 64Kbps, ta đợi cứ 10ms để có được 80 byte voice. Thời gian nén của G.711 là 1 ms [9]. Thời gian lấy mẫu, nén, giải nén theo chuẩn G.711 là:

Thời gian lấy mẫu + Thời gian nén + Thời gian giải nén = 2*10 + 1 + 1 = 22ms

Trong trường hợp xấu nhất là độ nén của G.711 là 0%, ta coi dung lượng là không đổi, sau khi nén bằng G.711 thì tín hiệu voice số hóa vẫn là 80 byte và đưa vào mã DES. Mã DES mã hóa theo block có chiều dài 8 byte, vậy 80 byte ta nén 10 lần để vừa khung tin của mã hóa DES. Thời gian mã của một block theo thuật toán DES là 0.27 ms [8,9] . Thời gian mã, giải mã theo thuật toán DES là:

2(nén và giải nén)*10(block)*thời gian nén 1 bock = 2 * 10 * 0.27 = 5.4ms



Hình 4. Sơ đồ khối cấu trúc của thuật toán mã DES

Sau đó, mã luồng thông tin được chuyển xuống tầng dưới để tạo các gói tin RTP/UDP/IP. Kích thước gói tin sẽ được thêm 20 byte cho một IP header, 8 byte cho một UDP header và 12 byte cho một RTP header. Như vậy kích thước của một gói thoại sẽ là:

$$80 + 20 + 8 + 12 = 120 \text{ (byte)}.$$

Thời gian truyền thông trên mạng là:

$$\text{Kích thước gói tin/băng thông} = 120 * 8/(128 * 10^3) = 7.5\text{ms}$$

Nếu người sử dụng yêu cầu một trang web trong khi một cuộc thoại đang tiến hành tại đó nảy sinh yêu cầu cho dữ liệu. Theo tiêu chuẩn MTU (Maximum Transmittial Unit: Đơn vị chuyển giao cực đại) gói tin có kích thước tối đa là 1500 byte. Độ trễ do chia sẻ băng thông cho các dịch vụ khác là:

$$\text{Kích thước gói tin/băng thông} = 1500 * 8/(128 * 10^3) = 93.75\text{ms}$$

Vậy tổng thời gian trễ trước khi gói tin thoại đến được người nhận là:

$$22 + 5.4 + 7.5 + 93.75 = 128.65\text{ms} < 150\text{ms}$$

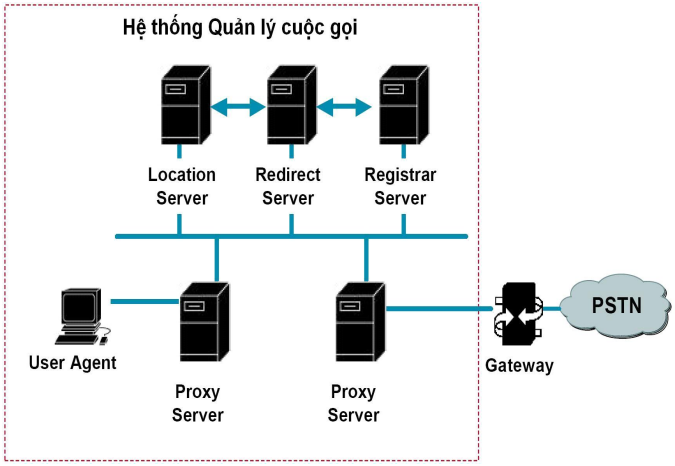
Như theo như phân tích thì độ trễ do áp dụng giải pháp an ninh cho VoIP trong mô hình thực nghiệm hoàn toàn đáp ứng được yêu cầu chất lượng của một cuộc đàm thoại trên mạng.

6. XÂY DỰNG HỆ THỐNG QUẢN LÝ CUỘC GỌI

Hệ thống Quản lý cuộc gọi hoạt động trên hệ điều hành mã nguồn mở Linux. Hệ thống Quản lý cuộc gọi được phát triển dựa theo hệ thống mã nguồn mở. Phát triển hệ thống để có thể hiểu và cho phép các cuộc gọi sử dụng mã hoá.

6.1. Chức năng của hệ thống

Hệ thống quản lý cuộc gọi là một hệ thống các server phân tán có khả năng cung cấp nhiều dịch vụ Voice Over Internet Protocol nói chung. Hệ thống quản lý cuộc gọi có khả năng hỗ trợ các thiết bị truyền thông theo các giao thức SIP, Media Gateway Control Protocol (MGCP) và H.323. Hệ thống cũng có khả năng hỗ trợ các loại điện thoại truyền thống thông qua các gateway phù hợp.



Hình 5. Hệ thống quản lý cuộc gọi

6.2. Các thành phần của hệ thống

Máy chủ định vị (Location Server)

Máy chủ định vị được máy chủ SIP chuyển tiếp và máy chủ SIP uỷ quyền sử dụng để lấy các thông tin về vị trí các bên tham gia truyền thông. Máy chủ định vị còn có thể được sử dụng với các giao thức khác giao thức SIP, có thể chuyển đổi từ các giao thức khác; ví dụ chuyển từ giao thức Telephony Routing over IP (TRIP), để có thể trao đổi với máy chủ chuyển tiếp.

Máy chủ uỷ quyền (Proxy Server)

Đây là một chương trình trung gian, có thể hoạt động vừa là máy chủ khi nhận yêu cầu từ máy trạm, vừa là máy trạm khi đại diện cho một máy trạm đưa ra các yêu cầu. Không giống các User Agent, máy chủ uỷ quyền không tạo ra yêu cầu mới, mà chỉ làm công việc phiên dịch hoặc nếu cần thiết thì có thể viết lại yêu cầu trước khi chuyển đi. Các yêu cầu có thể được xử lý tại đây, hoặc có thể được chuyển tới một máy chủ khác để xử lý

Máy chủ chuyển tiếp (Redirect Server)

Máy chủ chuyển tiếp làm nhiệm vụ nhận yêu cầu, sau đó sẽ ánh xạ địa chỉ được yêu cầu thành không hay một số địa chỉ mới và trả về các địa chỉ này cho client.

Máy chủ đăng ký (Registrar Server)

Máy chủ đăng ký có nhiệm vụ nhận các yêu cầu đăng ký của client. Máy chủ đăng ký thường được cài đặt cùng với các máy chủ uỷ quyền, máy chủ chuyển tiếp cung cấp các thông tin về vị trí cho máy chủ định vị.

7. XÂY DỰNG CHƯƠNG TRÌNH VNPHONE

Chương trình VNPhone được xây dựng nhằm thực hiện các cuộc gọi trên mạng IP. Cơ chế điều khiển cuộc gọi của VNPhone hoạt động theo giao thức SIP, dữ liệu audio được truyền theo giao thức RTP, hỗ trợ các cuộc gọi an toàn với nội dung thông tin thoại được mã hoá.

Chương trình VNPhone được phát triển dựa trên phần mềm mã nguồn mở cho phép thực hiện các cuộc gọi theo giao thức SIP. Với mục đích thừa kế nền tảng của chương trình, chúng tôi phát triển thêm các module hỗ trợ việc an toàn bảo mật trong các cuộc gọi SIP.

7.1. Xây dựng chức năng mã hóa dữ liệu audio

Do bản thân giao thức RTP chưa hỗ trợ chức năng mã hóa dữ liệu. Cần phải có cơ chế để chức năng mã hóa không làm ảnh hưởng đến các cuộc gọi thông thường. Module mã hóa khi được thêm vào hệ thống phải không làm thay đổi cấu trúc gói tin SIP và cấu trúc gói tin RTP. Chương trình Internet phone được xây dựng phải đảm bảo có thể thực hiện các cuộc gọi an toàn, đồng thời vẫn phải tương thích và có thể thực hiện các cuộc gọi với các hệ thống sử dụng giao thức SIP và RTP khác.

Bên nhận cuộc gọi khi nhận được gói dữ liệu audio do bên gọi gửi theo giao thức RTP, thì bên nhận phải xác định được đó có phải gói tin mã hóa hay không để có cách xử lý thích hợp. Do vậy gói tin có mã hóa phải được đánh dấu trong header gói tin RTP.

Trường chọn để đánh dấu gói tin mã hóa trong header gói tin RTP là trường mở rộng (X eXtention). Việc sử dụng trường mở rộng (X) để đánh dấu gói tin mã hóa sẽ đảm bảo không ảnh hưởng khuôn dạng và đặc điểm của gói tin RTP. Do vậy hệ thống vẫn có thể tương thích và có thể thực hiện cuộc gọi tới các hệ thống SIP phone khác.

Trong việc truyền tín hiệu audio theo thời gian thực kích thước gói tin có thể được lựa chọn theo độ dài ngắn của thời gian lấy mẫu tín hiệu audio hoặc video. Thuật toán mã hóa được xây dựng có chức năng mã hóa theo khối đảm bảo thời gian mã hóa tỷ lệ thuận với kích thước của gói tin.

7.2. Xây dựng cơ chế xử lý khoá

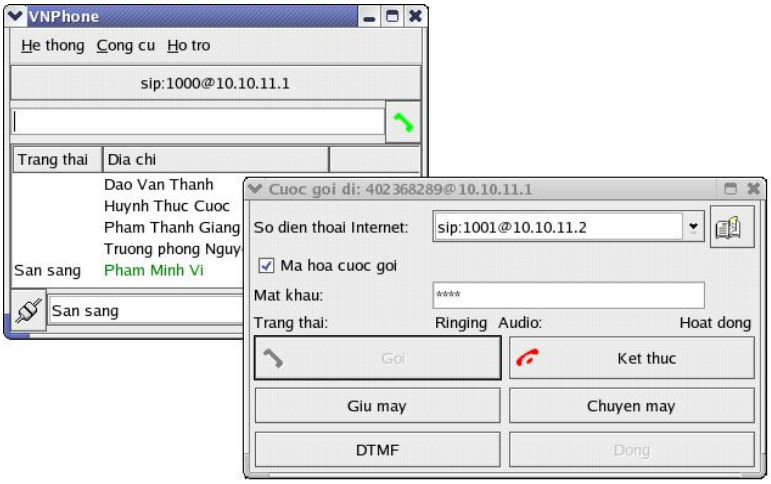
Để hệ thống có thể thực hiện được các cuộc gọi sử dụng mã hoá, hệ thống cần phải có cơ chế hoạt động của khóa trong phiên thoại và cơ chế mã và giải mã trong phiên đó.

Cơ chế hoạt động của khoá

Mỗi người dùng sử dụng hệ thống Internet phone an toàn sử dụng một khóa chính (Master Key). Khóa chính là khóa sẽ được sử dụng để mã hóa và giải mã dữ liệu audio trong các cuộc gọi mà người dùng đóng vai trò là người nhận cuộc gọi. Như vậy khi đóng vai trò là

người nhận cuộc gọi, khóa chính luôn được sử dụng để mã hóa dữ liệu đi từ người nhận và giải mã dữ liệu tới người nhận.

Khi một người dùng muốn thực hiện cuộc gọi sử dụng mã hóa tới người dùng khác. Người dùng sẽ nhập khóa phiên (Section key), khóa phiên này sẽ được sử dụng để mã hóa và giải mã dữ liệu audio trong các cuộc gọi mà người dùng đóng vai trò là người thực hiện cuộc gọi. Như vậy khi đóng vai trò là người gọi, khóa phiên được sử dụng để mã hóa dữ liệu đi từ người gọi và giải mã dữ liệu tới người gọi. Đối với người gọi, với từng cuộc gọi tới mỗi người khác nhau thì người dùng sẽ phải chọn một khóa phiên tương ứng với khóa chính của người nhận để thực hiện việc mã hóa và giải mã thành công.



Hình 6. Thực hiện cuộc gọi mã hoá

Như vậy trong cuộc gọi, khi người dùng đóng vai trò là người nhận cuộc gọi, khóa được sử dụng để giải mã là khóa chính, khi người dùng đóng vai trò là người gọi, khóa được sử dụng để mã hóa là khóa phiên. Do khóa được sử dụng là khóa bí mật nên người thực hiện cuộc gọi muốn thực hiện cuộc gọi có mã hóa đến người nhận thì anh ta phải biết khóa chính của người nhận và sử dụng khóa chính đó làm khóa phiên để thực hiện cuộc gọi. Cơ chế mã và giải mã

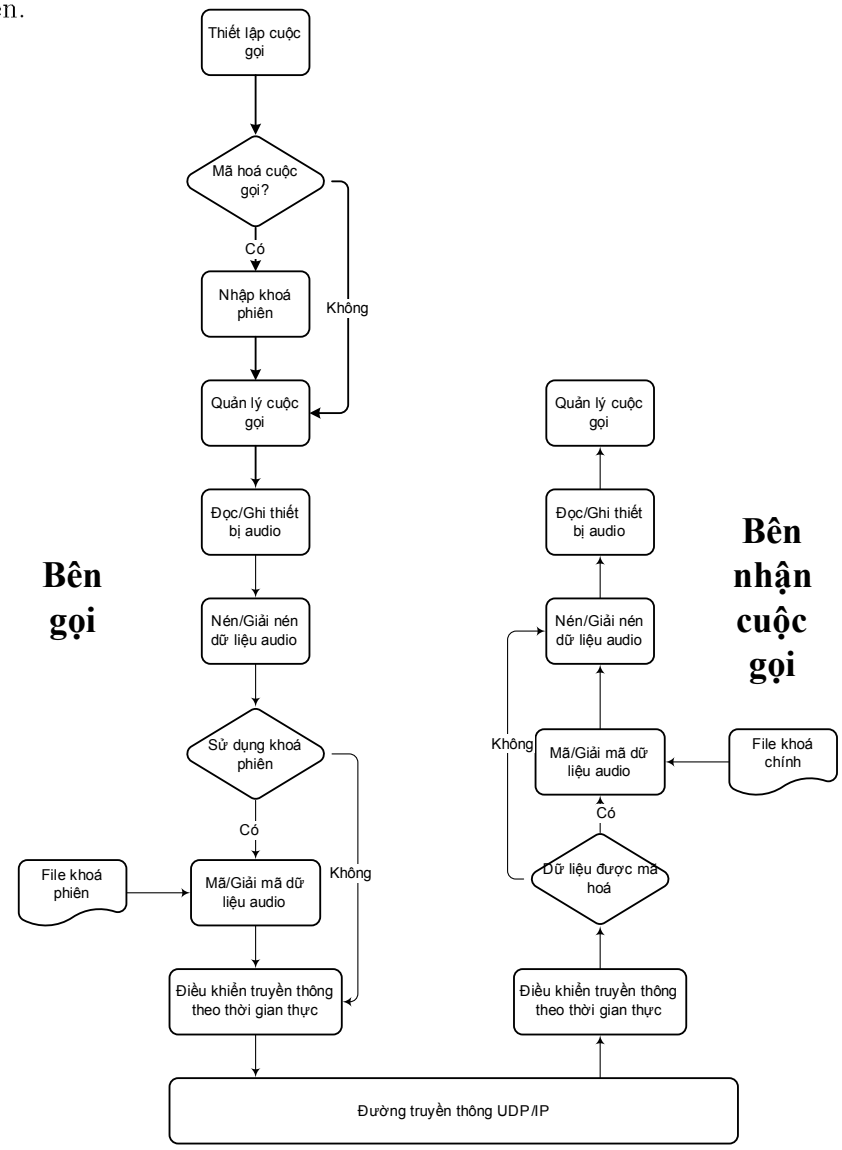
Hệ thống Internet Phone an toàn đảm bảo có thể có thể thực hiện cả các cuộc gọi có mã hóa hoặc không mã hóa với các hệ thống khác sử dụng giao thức SIP và RTP. Việc mã hóa và giải mã được thực hiện ngay trước khi dữ liệu được truyền trên mạng theo thời gian thực và ngay sau khi dữ liệu audio được nén theo các chuẩn truyền thông media.

8. KẾT LUẬN

Hiện nay vấn đề bảo đảm an toàn cho cuộc gọi thoại Internet đang được xem xét một cách tích cực, đặc biệt khi cuộc gọi thoại Internet càng ngày càng trở nên phổ biến.

Hệ thống thoại Internet an toàn hiện đang được chạy thử nghiệm tại viện Công nghệ thông tin, viện Khoa học và Công nghệ Việt Nam. Hệ thống đã đáp ứng được một số chức năng về an ninh; xác thực người dùng, mã hóa dữ liệu audio. Các chức năng an ninh của hệ thống đảm bảo chống được người dùng nặc danh sử dụng hệ thống, dữ liệu bị nghe lén trên

đường truyền.



Hình 7. Cơ chế mã và giải mã

Trong hệ thống của chúng tôi, đã giải quyết được vấn đề an toàn cho gói dữ liệu âm thanh. Hiện tại hệ thống chưa bảo vệ được các thông tin điều khiển trong cuộc gọi, hoặc bảo vệ trước một số kiểu tấn công đặc thù của mạng như: từ chối dịch vụ, quét cổng,... Hệ thống sẽ được tăng cường an ninh, chống được các kiểu tấn công đặc thù, nếu hệ thống được cài cùng với các chương trình bảo vệ khác như firewall, hoặc sử dụng hạ tầng mã hóa của IPSec, VPN.

TÀI LIỆU THAM KHẢO

[1] Douglas E. Comber, Internetworking with TCP/IP, *Principles, Protocol and Architecture*, Vol.1, Prentice-Hall International, ISBN 0-13-474321-0, 1991

[2] Nguyễn Phương Lan, Hoàng Đức Hải, *Lập trình Linux*, Nhà xuất bản Giáo dục, 1998.

[3] Richard Stevens, *UNIX Network Programming,* PTR Prentice-Hall, Englewood Cliffs, New Jersey 07632, 1990.

[4] RFC 2543 SIP: Session Initiation Protocol. M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg. March 1999.

[5] RFC 3261 SIP: Session Initiation Protocol. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. June 2002.

[6] RFC 3267 - Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs. J. Sjoberg, M. Westerlund, A. Lakaniemi, Q. Xie. June 2002.

[7] RFC 0791 - Internet Protocol. J. Postel. Sep-01-1981.

[8] The Data Encryption Standard vs. Exhaustive Search. R. R. Jueneman, Practicalities and Politics. 5 Feb 1981.

[9] "Báo cáo đề tài hệ thống thoại Internet an toàn", Phòng tin học viễn thông - Viện Công nghệ Thông tin, VAST 12/2004.

Nhận bài ngày 23 - 2 - 2005
Nhận lại sau sửa ngày 23 - 8 - 2005