LUẬN VĂN

AN NINH TRONG THONG TIN DI ĐỘNG

Công nghệ thông tin vô tuyến tạo ra sự thay đổi sâu sắc theo cách mà mọi người tương tác với nhau và trao đổi thông tin trong xã hội chúng ta. Một thập kỷ qua, các mô hình đang thịnh hành cho cả các hệ thống điện thoại và các mạng máy tính là các mô hình mà người sử dụng tiếp cận mạng – tổ hợp điện thoại hoặc trạm máy tính được nối bằng dây tới cơ sở hạ tầng liên mạng rộng hơn. Ngày nay, các mô hình đó đã dịch chuyển đến một mô hình nơi mà mạng tiếp cận người sử dụng bất kì khi nào họ xuất hiện và sử dụng chúng. Khả năng liên lạc thông qua các máy điện thoại tổ ong trong khi đang di chuyển là thực hiện được và các hệ thống cho truy nhập Internet không dây ngày càng phổ biến.

Tiềm năng cung cấp độ mềm dẻo và các khả năng mới của thông tin vô tuyến cho người sử dụng và các tổ chức là rõ ràng. Cùng thời điểm đó, việc cung cấp các cơ sở hạ tầng rộng khắp cho thông tin vô tuyến và tính toán di động giới thiệu những nguy cơ mới, đặc biệt là trong lĩnh vực an ninh. Thông tin vô tuyến liên quan đến việc truyền thông tin qua môi trường không khí, điển hình là bằng các sóng vô tuyến hơn là thông qua môi trường dây dẫn khiến cho việc chặn hoặc nghe lén các cuộc gọi khi người sử dụng thông tin với nhau trở nên dễ dàng hơn. Ngoài ra, khi thông tin là vô tuyến thì không thể sử dụng vị trí kết nối mạng của người sử dụng như là một phần tử để đánh giá nhận dạng chúng. Để khai thác tiềm năng của công nghệ này mọi người phải có thể chuyển vùng tự do với các sản phẩm thông tin di động được và từ quan điểm cơ sở hạ tầng mạng ít nhất mọi người có thể xuất hiện tự do trong những vị trí mới. Trong khi các đặc tính này cung cấp cho người sử dụng các tiện ích mới thì nhà cung cấp dịch vụ và nhà quản trị hệ thống phải đối mặt với những thách thức về an ninh chưa có tiền lệ.

Luận văn này sẽ tìm hiểu đề tài về nhận thực thuê bao vì nó liên quan đến môi trường mạng vô tuyến. Theo ngữ cảnh này một "thuê bao" là người sử dụng: chẳng hạn một khách hàng của một dịch vụ điện thoại tổ ong hoặc một người sử dụng một dịch vụ truy nhập Internet không dây. Nhận thực thuê bao là một thành phần then chốt của an ninh thông tin trong bất kỳ môi trường mạng nào, nhưng khi người sử dụng là di động thì nhận thực đảm nhận các thành phần mới.

Những nghiên cứu ở đây tìm hiểu cơ chế để nhận thực thuê bao trong hai môi trường liên mạng. Đầu tiên là mạng tổ ong số hỗ trợ truyền thông bằng các máy điện thoại tổ ong. Mạng này đang trải qua một cuộc phát triển từ công nghệ thế hệ thứ hai sang thế hệ thứ 3 và các phương pháp trong đó nhận thực thuê bao kèm theo cũng đang thay đổi. Môi trường mạng thứ hai là Giao thức Internet di động (Mobile IP), một giao thức được phát triển trong những năm 90 của thế kỷ 20 cho phép Internet hỗ trợ tính toán di động. Điều quan trọng là nhận ra rằng hai môi trường này có nguồn gốc khác nhau. Môi trường tổ ong số được trình bày trong nghiên cứu này chẳng hạn như UMTS bắt nguồn từ các mạng điện thoại. Về mặt lịch sử nhiệm vụ chính của mạng này là hỗ trợ các cuộc hội thoại và phương pháp thiết lập các "mạch" cung cấp một kết nối liên tục giữa các điểm đầu cuối. Giao thức Internet di động là một sự mở rộng của kiến trúc liên mạng Internet hiện có trong đó tập trung vào việc hỗ trợ cho truyền thông giữa các máy tính và kiểu lưu lượng là số liệu hơn là thoại. Trong thế giới Internet, nhiệm vụ quan trọng nhất là định tuyến và phân phối các gói dữ liệu hơn là thiết lập các kênh tạm thời điểm-điểm.

Ngoài những sự khác nhau này theo nguồn gốc mạng tổ ong số và môi trường Internet trong đó Mobile IP hoạt động chúng ta còn gặp phải sự khác nhau trong các phương pháp được thực hiện đối với nhận thực và an ninh. Tuy nhiên quan trọng là hiểu rằng tất cả các công nghệ truyền thông cả công nghệ hỗ trợ hội thoại lẫn công nghệ hỗ trợ truyền số liệu ngày nay đều sử dụng công nghệ số. Vì vậy, tại các tầng dưới của ngăn xếp giao thức truyền thông, chúng sử dụng các cơ chế tương tự để truyền và nhận thông tin. Hơn nữa, khi truy nhập Internet không dây phát triển quan trọng không chỉ đối với máy tính mà còn đối với máy điện thoại tế bào thì thách thức mà hai môi trường liên mạng này phải đối mặt trong lĩnh vực an ninh có khuynh hướng hợp nhất. Trong tương lai, nếu điện thoại tế bào của ai đó trở thành một loại đầu cuối truy nhập Internet chính thì một kết quả có tính khả thi lâu dài là sự khác biệt giữa công nghệ truyền thông tổ ong và công nghệ của Internet sẽ không còn rõ ràng.

Chủ đề quan tâm thực sự ở đây là lĩnh vực máy tính, truyền thông và an ninh thông tin vì nó bị ảnh hưởng bởi liên mạng vô tuyến và tính toán di động. Tuy nhiên đó là lĩnh

vực khổng lồ và phức tạp. Nhận thực thuê bao là một chủ đề hẹp hơn và vì vậy thích hợp hơn cho phạm vi của luận văn này. Tuy nhiên, dự định của luận văn này là sử dụng những khám phá về nhận thực thuê bao trong các mạng tổ ong số theo giao thức Mobile IP như một ống kính cho phép chúng ta nhận thức rõ ràng hơn khuynh hướng rộng hơn trong an ninh cho các môi trường liên mạng vô tuyến.

Chương 1 giới thiệu nhận thực vì nó liên quan đến lĩnh vực lớn hơn của máy tính, truyền thông và bảo mật thông tin trong mạng vô tuyến và cung cấp một số đặc tính cụ thể của môi trường mạng vô tuyến gây trở ngại cho người thiết kế hệ thống an ninh.

Chương 2, trọng tâm chuyển đến việc nghiên cứu từ những năm 1990 khẳng định rằng tồn tại phương pháp cho hệ thống mật mã khoá công cộng với tiềm năng lớn cho môi trường thông tin vô tuyến.

Chương 3, trọng tâm chuyển đến sự xem xét các giao thức cho các mạng truyền thông tổ ong băng tần cao thế hệ thứ 3 được gọi là UMTS (Universal Mobile Telecommunications System).

Chương 4 khảo sát nhận thực vì nó được đề xuất cho ứng dụng trong miền truy nhập Internet không dây được gọi là Mobile IP (Mobile Internet Protocol).

Cuối cùng em xin gửi lời cảm ơn chân thành sâu sắc đến thầy TS. Nguyễn Phạm Anh Dũng, thầy Nguyễn Viết Đảm và cô Phạm Thị Thuý Hiền đã nhiệt tình giúp đỡ em hoàn thành đề tài này.

Hà Nội – 2005

Nguyễn Lê Trường

CHƯƠNG 1: NHẬN THỰC TRONG MÔI TRƯỜNG LIÊN MẠNG VÔ TUYẾN

Từ điển New International của Webster, phiên bản năm 1925 định nghĩa "nhận thực" nghĩa là: "Hành động về nhận thực hoặc trạng thái được nhận thực; trao cho quyền hoặc thẻ tín nhiệm bằng các thủ tục, xác nhận cần thiết". Động từ "authenticate" được định nghĩa chặt chẽ hơn: "(1) là để đưa ra tính xác thực, để trao quyền bằng các bằng chứng, chứng nhận hoặc các thủ tục được yêu cầu bằng luật hoặc cần thiết để dán tên cho thẻ tín nhiệm giống như văn bản được xác nhận bằng các con dấu. (2) là để chứng minh tính xác thực; để xác định rõ tính chân chính, có thực hoặc tính chính thống như xác nhận một bức chân dung". 75 năm qua theo ngữ cảnh của truyền thông và máy tính số, những định nghĩa này vẫn còn có giá trị.

1.1 Vai trò của nhận thực trong kiến trúc an ninh

Trong thế giới an ninh thông tin, nhận thực nghĩa là hành động hoặc quá trình chứng minh rằng một cá thể hoặc một thực thể là ai hoặc chúng là cái gì. Theo Burrows, Abadi và Needham: "Mục đích của nhận thực có thể được phát biểu khá đơn giản nhưng không hình thức và không chính xác. Sau khi nhận thực, hai thành phần chính (con người, máy tính, dịch vụ) phải được trao quyền để được tin rằng chúng đang liên lạc với nhau mà không phải là liên lạc với những kẻ xâm nhập". Vì vậy, một cơ sở hạ tầng IT hợp nhất muốn nhận thực rằng thực tế người sử dụng hệ thống cơ sở dữ liệu của công ty là giám đốc nguồn nhân lực trước khi cho phép quyền truy nhập vào dữ liệu nhân công nhạy cảm (có lẽ bằng các phương tiện mật khẩu và thẻ thông minh của người dùng). Hoặc nhà cung cấp hệ thống thông tin tổ ong muốn nhận thực máy điện thoại tổ ong đang truy nhập vào hệ thống vô tuyến của họ để thiết lập rằng các máy cầm tay thuộc về những người sử dụng có tài khoản là mới nhất và là các máy điện thoại không được thông báo là bị đánh cắp.

1.2 Vị trí của nhận thực trong các dịch vụ an ninh

Nhận thực là một trong các thành phần thuộc về một tập hợp các dịch vụ cấu thành nên một phân hệ an ninh trong cơ sở hạ tầng thông tin hoặc tính toán hiện đại. Các dịch vụ cụ thể cấu thành nên tập hợp đầy đủ có thể hơi khác phụ thuộc vào mục đích, nội dung thông tin và mức độ quan trọng của hệ thống cha. William Stallings, trong quyển sách của ông ***Cryptography and Network Security*** (Mật mã và an ninh mạng) cung cấp các dịch vụ bảo mật lõi có giá trị tham khảo lâu dài để đặt nhận thực trong ngữ cảnh hệ thống chính xác:

Tính tin cậy (Confidentiality): Đảm bảo rằng thông tin trong hệ thống máy tính và thông tin được truyền đi chỉ có thể truy nhập được để đọc bởi các bên có thẩm quyền.[….]

Nhận thực (Authentication): Đảm bảo rằng khởi nguồn của một bản tin hoặc văn bản điện tử được nhận dạng chính xác và đảm bảo rằng việc nhận dạng là không bị lỗi.

Tính toàn vẹn (Integrity): Đảm bảo rằng chỉ những bên có thẩm quyền mới có thể sửa đổi tài nguyên hệ thống máy tính và các thông tin được truyền. [….]

Không thoái thác (Non-repudiation): Yêu cầu rằng cả bên nhận lẫn bên gửi không được từ chối truyền dẫn.

Điều khiển truy nhập (Access Control): Yêu cầu rằng truy nhập tới tài nguyên thông tin có thể được điều khiển bởi hoặc cho hệ thống quan trọng.

Tính sẵn sàng (Availability): Yêu cầu rằng tài nguyên hệ thống máy tính khả dụng đối với các bên có thẩm quyền khi cần thiết.

Mô tả của Stallings đề xuất rằng những chức năng bảo mật hệ thống này cho những người sử dụng hệ thống. Như được chỉ ra bởi chú thích Burrows, Abadi và Needham, quan trọng để hiểu rằng khi điều này là chân thực thì các chức năng này cũng có thể áp dụng cho các thiết bị vật lý (nhận thực một máy điện thoại tổ ong) hoặc áp dụng với hệ thống máy tính (nhận thực một server mạng không dây).

Nhận thực trong các mạng hữu tuyến thông thường đã thu hút các công trình nghiên cứu và nỗ lực thực hiện trong suốt hai thập kỷ qua. Trở lại những năm 1980, trong số các giao thức nhận thực nổi tiếng cho các hệ thống máy tính phân tán là Kerberos (đầu tiên được phát triển tại MIT như là một phần của dự án Athena), giao thức cái bắt tay RPC (Remote Procedure Call) của Andrew, giao thức khoá công cộng của Needham-Schroeder và giao thức X.509 của CCITT. Thảo luận chi tiết về các giao thức nhận thực cho môi trường liên mạng vô tuyến là phạm vi của đề tài này. Đối với việc thảo luận sâu sắc về các giao thức Kerberos, CCITT X.509 và các khía cạnh nhận thực tổng quát người đọc xem tài liệu của Stallings. Đối với việc phân tích hình thức các thủ tục tương ứng, sự đảm bảo và sự yếu kém của của bốn giao thức vừa được đề cập ở trên thì các tài liệu của Burrows, Abai, Needham là hữu dụng.

1.3. Các khái niệm nền tảng trong nhận thực

Trong khi luận văn này tránh những tìm hiểu chi tiết về nhận thực trong các mạng không phải di động thông thường và các hệ thống phân tán thì một vài khái niệm trong nhận thực là quan trọng đối với việc thảo luận trong các chương tiếp theo. Đó là:

1.3.1 Trung tâm nhận thực (Authentication Center)

Trong các giao thức liên quan đến việc sử dụng các khoá bí mật dành cho nhận thực, các khoá bí mật này phải được lưu trữ bởi nhà cung cấp dịch vụ cùng với thông tin về cá nhân người sử dụng hoặc thuê bao trong một môi trường bảo mật cao. Nói riêng trong thế giới điện thoại tổ ong một hệ thống như thế thường được gọi là một Trung tâm nhận thực.

1.3.2 Nhận thực thuê bao (Subscriber Authentication)

Nhiều cuộc thảo luận liên quan đến nhận thực trong các mạng tổ ong số bao gồm nhận thực thuê bao. Điều này nói tới nhận thực người sử dụng dịch vụ điện thoại tổ ong và sẽ xảy ra một cách điển hình khi một người sử dụng thử thiết lập một cuộc gọi, vì vậy sẽ đăng ký một yêu cầu với trạm gốc mạng cho việc cung cấp dịch vụ. Nên chú ý rằng "Nhận thực thuê bao" thường nói tới nhận thực tổ hợp điện thoại tổ ong và các thông tin

trên thẻ thông minh của tổ hợp đó hơn là đối với việc nhận thực người sử dụng thực sự là con người (mặc dù việc nhận thực này dĩ nhiên là mục tiêu cuối cùng).

1.3.3 Nhận thực tương hỗ (Mutual Authentication)

Hầu hết các giao thức nhận thực liên quan đến hai "thành phần chính (principals)" và có thể có các bên thứ ba tin cậy ví dụ như Certification Authority phụ thuộc vào giao thức. Trong nhận thực tương hỗ, cả hai principal được nhận thực lẫn nhau. Một chú ý quan trọng là nhận thực không cần phải tương hỗ, có thể chỉ là một chiều. Chẳng hạn khi thảo luận nhận thực trong các mạng điện thoại tổ ong thế hệ thứ ba, chúng ta sẽ gặp phải các trường hợp trong đó mạng nhận thực máy điện thoại tổ ong đang tìm sử dụng các dịch vụ của nó nhưng trạm gốc của mạng không được nhận thực tới máy điện thoại này.

1.3.4 Giao thức yêu cầu/đáp ứng (Challenge/Response Protocol)

Một số các giao thức được tìm hiểu trong luận văn này sử dụng cơ chế Challenge/Response như là cơ sở cho nhận thực. Trong kịch bản Challenge/Response, bên thứ nhất (first principal) đang muốn để thực hiện nhận thực trên principal thứ hai tạo ra một số ngẫu nhiên và gửi nó đến principal thứ hai. Trong nhiều giao thức, số ngẫu nhiên này được truyền ngay lập tức tới Trung tâm nhận thực. Principal thứ hai tổ hợp số nhẫu nhiên này với khoá bí mật của nó theo một thuật toán được thoả thuận chung. Chuỗi bit kết quả cuối cùng được xác định bởi tổ hợp Challenge ngẫu nhiên với khoá bí mật của principal thứ hai rồi truyền trở lại principal thứ nhất. Trong khi đó, Trung tâm nhận thực - hoặc các phía thứ ba tin cậy tương tự - mà có quyền truy nhập tới khoá bí mật của các principal, thực hiện cùng các tính toán và chuyển kết quả trở lại principal thứ nhất. Principal thứ nhất so sánh hai giá trị và nếu chúng bằng nhau thì nhận thực principal thứ hai. Chú ý rằng cơ chế Challenge/Response không yêu cầu principal thứ nhất biết khoá bí mật của principal thứ hai hoặc ngược lại.

1.3.5 Tạo khoá phiên (Session Key Generation)

Mặc dù việc tạo một khoá phiên không cần thiết là một phần của nhận thực thuê bao theo nghĩa hẹp nhất, thường nó xảy ra trong cùng quá trình và vì vậy sẽ được thảo

luận trong các chương sau. Một khoá phiên là một khoá số được sử dụng trong quá trình mật mã các bản tin được trao đổi trong một phiên thông tin đơn giữa hai principal. Vì vậy khoá phiên được phân biệt với khoá công cộng hoặc khoá riêng của người sử dụng hệ thống, những khoá điển hình có thời gian tồn tại dài hơn. Các hệ thống thông tin thường tạo ra khoá phiên với các thuật toán chạy song song với thuật toán thực hiện giao thức Challenge/Response (xem ở trên) và với những thuật toán có cùng đầu vào.

Khi những thuật ngữ này xuất hiện trong các chương tiếp theo của luận văn này, chúng mang ý nghĩa được định nghĩa ở trên.

1.4 Mật mã khoá riêng (Private-key) so với khoá công cộng (Public-key)

Khái niệm nền tảng khác được thảo luận trong các chương tiếp theo là sự phân biệt giữa mật mã khoá công cộng và mật mã khoá riêng. Nói chung, với mật mã khoá riêng (cũng được gọi là mật mã khoá đối xứng) hai bên đang muốn trao đổi các bản tin mật dùng chung khoá bí mật "secret key" (thường là một chuỗi bit ngẫu nhiên có độ dài được thoả thuận trước). Những khoá này là đối xứng về chức năng theo nghĩa là principal A có thể sử dụng khoá bí mật và một thuật toán mật mã để tạo ra văn bản mật mã (một bản tin được mã hoá) từ văn bản thuần tuý (bản tin ban đầu). Dựa trên việc nhận bản tin được mật mã này, principal B tháo gỡ quá trình này bằng cách sử dụng cùng khoá bí mật cho đầu vào của thuật toán nhưng lần này thực hiện ngược lại – theo mode giải mật mã. Kết quả của phép toán này là bản tin văn bản thuần tuý ban đầu ("bản tin" ở đây nên được hiểu theo nghĩa rộng – nó có thể không phải là văn bản đọc được mà là các chuỗi bit trong một cuộc hội thoại được mã hoá số hoặc các byte của một file hình ảnh số). Những ví dụ phổ biến của hệ thống mật mã khoá riêng đối xứng gồm DES (Data Encryption Standard: Chuẩn mật mã số liệu). IDEA (International Data Encryption Algorithm: Thuật toán mật mã số liệu quốc tế) và RC5.

Với công nghệ mật mã khoá công cộng, không có khoá bí mật được dùng chung. Mỗi principal muốn có thể trao đổi các bản tin mật với các principal kia sở hữu khoá bí mật riêng của chúng. Khoá này không được chia sẻ với các principal khác. Ngoài ra, mỗi

principal làm cho "public key" trở nên công cộng (không cần phải che giấu khoá này - thực tế, hoạt động của hệ thống mật mã khoá công cộng yêu cầu những principal khác có thể dễ dàng truy nhập thông tin này). Mật mã khoá công cộng sử dụng thuật toán mật mã bất đối xứng. Nghĩa là khi principal A tìm cách để gửi một bản tin an toàn tới principal B, A mật mã bản tin văn bản thuần tuý bằng cách sử dụng khoá công cộng và bản tin ban đầu của B là đầu vào cho thuật toán. Điều này không yêu cầu B có những hành động đặc biệt trong đó khoá công cộng của B luôn khả dụng cho A. Principal A sau đó truyền bản tin tới principal B. Thuật toán mật mã khoá công cộng hoạt động theo cách thức là bản tin được mật mã với khoá công cộng của B chỉ có thể được giải mật mã với khoá riêng của B. Khi B không chia sẻ khoá riêng này với ai thì chỉ có B có thể giải mật mã bản tin này. RSA (được đặt tên theo Ron Rivest, Adi Shamir và Len Adleman) có lẽ là ví dụ nổi tiếng nhất của hệ thống mật mã khoá công cộng.

Thêm nữa, việc tìm hiểu chi tiết công nghệ mật mã khoá riêng và mật mã khoá công cộng là phạm vi của luận văn này. Người đọc xem tài liệu của Stallings để thảo luận rộng và sâu hơn. Một tài liệu năm 1992 của Beller, Chang và Yacobi cung cấp sự thảo luận chi tiết về việc phân biệt giữa hệ thống khoá riêng và khoá công cộng trong trường hợp cụ thể mạng di động.

Trong mạng tổ ong thế hệ thứ hai như GSM (Global Systems Mobile), việc sử dụng công nghệ mật mã khoá riêng đã trở nên toàn cầu. Một sự giả định chung liên quan đến các công nghệ khoá công cộng là chúng đòi hỏi nhiều tính toán đến mức không thể đưa vào thực tế trong môi trường liên mạng vô tuyến. Như chúng ta sẽ thấy trong chương 3, việc nghiên cứu được tiến hành trong đầu và giữa những năm 1990 về các thuật toán mật mã khoá công cộng "processor-light" đã được tối ưu cho các mạng vô tuyến đã đặt ra nghi vấn cho sự thông minh này. Cuộc tranh luận đang diễn ra về giá trị của các phương pháp khoá công cộng và khoá riêng đối với nhận thực và an ninh là sơ đồ khoá cho việc nghiên cứu liên quan đến hoạt động của mạng vô tuyến và sẽ chính nó sẽ đóng vai trò quyết định trong việc thiết kế phát triển các hệ thống trong thập kỷ tới.

1.5. Những thách thức của môi trường liên mạng vô tuyến

Các mạng vô tuyến mở rộng phạm vi và độ mềm dẻo trong thông tin và tính toán một cách mạnh mẽ. Tuy nhiên, môi trường liên mạng vô tuyến vốn dĩ là môi trường động, kém mạnh mẽ hơn và bỏ ngỏ hơn cho sự xâm nhập và gian lận so với cơ sở hạ tầng mặt đất cố định. Những nhân tố này đặt ra những vấn đề cho nhận thực và an ninh trong môi trường liên mạng vô tuyến. Chúng đặt ra những thách thức mà những người thiết kế hệ thống và kiến trúc an ninh phải vượt qua.

Trong một tài liệu xuất sắc năm 1994 mang tựa đề "Những thách thức của tính toán di động" tổng kết sự khác nhau giữa môi trường liên mạng không dây và có dây và những vấn đề mạng vô tuyến đặt ra cho kĩ sư phần mềm, George Forman và John Zahorjan đã phân biệt những nhân tố xuất phát từ "ba yêu cầu thiết yếu: việc sử dụng liên mạng vô tuyến, khả năng thay đổi vị trí và nhu cầu về tính di động không bị gây trở ngại". Trong khi phân tích Forman và Zahorjan là rộng – Họ đang khảo sát ảnh hưởng của môi trường liên mạng vô tuyến lên toàn bộ phạm vi của kỹ thuật phần mềm thì vẫn cơ cấu đó có thể được sử dụng cho những ưu điểm lớn trong việc xác định tình huống khi nó gắn cụ thể với an ninh và nhận thực. Kết luận của tác giả vẫn rất có ích và có thể ứng dụng được cho đến ngày nay:

Thông tin vô tuyến mang đến điều kiện trở ngại mạng, truy nhập đến các nguồn tài nguyên xa thường không ổn định và đôi khi hiện thời không có sẵn. Tính di động gây ra tính động hơn của thông tin. Tính di động đòi hỏi các nguồn tài nguyên hữu hạn phải sẵn có để xử lý môi trường tính toán di động. Trở ngại cho những người thiết kế tính toán di động là cách để tương thích với những thiết kế hệ thống đã hoạt động tốt cho hệ thống tính toán truyền thống.

Nên chú ý rằng trong lĩnh vực an ninh, "việc thiết kế đã hoạt động tốt cho tính toán truyền thống" chính chúng đang trong trạng thái thay đổi liên tục cộng thêm với độ bất định bổ sung tới sự cân bằng này.

Trong phần còn lại, ta sẽ xác định khái quát những trở ngại chính của môi trường liên mạng vô tuyến cho các giao thức nhận thực và an ninh bằng cách sử dụng ba phần được đề xuất bởi Forman và Zahojan.

1.5.1 Vùng trở ngại 1: Các đoạn nối mạng vô tuyến

Theo định nghĩa, các mạng vô tuyến phụ thuộc vào các đoạn nối thông tin vô tuyến, điển hình là sử dụng các tín hiệu sóng vô tuyến (radio) để thực hiện truyền dẫn thông tin ít nhất là qua một phần đáng kể cơ sở hạ tầng của chúng. Dĩ nhiên, sức mạnh to lớn của công nghệ thông tin vô tuyến là nó có thể hỗ trợ việc truyền thông đang diễn ra với một thiết bị di động chẳng hạn như một máy điện thoại tổ ong hoặc một máy hỗ trợ số cá nhân (PDA: Personal Digital Assistant), nghĩa là thiết bị di động. Tuy nhiên về nhiều phương diện, việc sử dụng các đoạn nối vô tuyến trong một mạng đặt ra nhiều vấn đề so với mạng chỉ sử dụng dây đồng, cáp sợi quang hoặc tổ hợp các cơ sở hạ tầng cố định như thế.

Băng tần thấp: Tốc độ tại đó mạng vô tuyến hoạt động đang tăng khi công nghệ được cải thiện. Tuy nhiên, nói chung các đoạn nối vô tuyến hỗ trợ truyền số liệu thấp hơn vài lần về độ lớn so với mạng cố định. Ví dụ, mạng điện thoại tổ ong thế hệ thứ hai được thảo luận trong luận văn này truyền dữ liệu trên kênh tại tốc độ xấp xỉ 10Kbits/s. Tốc độ này sẽ tăng lên hơn 350Kbits/s một chút khi đề cập đến các mạng tổ ong thế hệ thứ ba. Hiện thời, các hệ thống LAN không dây sử dụng chuẩn 802.11b có thể đạt tốc độ lên tới 11Mbits/s. Tuy nhiên nên chú ý rằng tốc độ này là cho toàn bộ mạng, không phải cho kênh thông tin đối với một máy đơn lẻ, và chỉ hoạt động trong một vùng nhỏ, ví dụ như một tầng của một toà nhà. Trong mạng hữu tuyến, Fast Ethernet, hoạt động ở tốc độ 100Mbits/s đang trở thành một chuẩn trong các mạng ở các toà nhà, trong khi các kênh đường trục Internet cự ly dài hoạt động tại tốc độ nhiều Gigabits/s.

Suy hao số liệu thường xuyên: So với mạng hữu tuyến, dữ liệu số thường xuyên bị suy hao hoặc sai hỏng khi truyền qua đoạn nối vô tuyến. Các giao thức liên mạng sử dụng các cơ chế để kiểm tra tính toàn vẹn số liệu có thể nhận dạng những tình huống này và yêu cầu thông tin được truyền, mà tác động sẽ là tổ hợp hiệu ứng của băng tân thấp.

Ngoài việc làm chậm tốc độ tại đó thông tin được truyền chính xác, suy hao dữ liệu có thể tăng tính thay đổi của thời gian được yêu cầu để truyền một cấu trúc dữ liệu cho trước hoặc để kết thúc chuyển giao.

"Tính mở" của sóng không gian: Các mạng hữu tuyến dù được tạo thành từ dây đồng hay cáp sợi quang đều có thể bị rẽ nhánh. Tuy nhiên, điều này có khuynh hướng là một thủ tục gây trở ngại về mặt kỹ thuật và việc xâm nhập có thể thường xuyên được phát hiện bằng các thiết bị giám sát mạng. Ngược lại, khi mạng vô tuyến gửi số liệu qua khí quyển bằng cách sử dụng các tín hiệu sóng vô tuyến (radio) thì bất kỳ ai có thể nghe được thậm chí chỉ bằng cách sử dụng thiết bị không đắt tiền. Những sự xâm nhập như thế là tiêu cực và khó phát hiện. Trường hợp này đặt ra một sự đe doạ cơ bản về an ninh cho mạng vô tuyến. Như chúng ta sẽ thấy trong những chương sau, những người thiết kế hệ thống tổ ong thế hệ thứ hai đã giải quyết những nguy cơ rõ ràng nhất được đặt ra khi con người đơn giản truyền dữ liệu thoại hoặc dữ liệu nhạy cảm qua đoạn nối vô tuyến bằng cách sử dụng kỹ thuật mật mã. Tuy nhiên, sự phơi bày phát sinh là rộng khắp, và không được giải quyết một cách triệt để.

1.5.2 Vùng trở ngại 2: Tính di động của người sử dụng

Như đã đề cập, tiến bộ vượt bậc của công nghệ liên mạng vô tuyến là người sử dụng có thể di chuyển trong khi vẫn duy trì được liên lạc với mạng. Tuy nhiên, những đặc điểm này của liên mạng vô tuyến làm yếu đi và loại bỏ một vài phỏng đoán cơ bản mà giúp đảm bảo an ninh trong mạng hữu tuyến. Ví dụ, các mạng hữu tuyến điển hình trong văn phòng, một máy tính để bàn của người sử dụng sẽ luôn được kết nối đến cùng cổng trên cùng Hub mạng (hoặc một phần tương đương của thiết bị kết nối mạng). Hơn nữa, tập hợp các máy tính, máy in, và các thiết bị mạng khác được kết nối với mạng tại bất kì điểm nào theo thời gian được nhà quản trị hệ thống biết và dưới sự điều khiển của nhà quản trị này.

Trong môi trường liên mạng vô tuyến, những phỏng đoán cơ bản này không còn được áp dụng. Người sử dụng không phải là nhà quản trị hệ thống xác định "cổng (port)" mạng nào và thậm chí mạng nào họ kết nối tới với thiết bị di động của họ. Tương tự, một

tập các thiết bị kết nối với mạng vô tuyến tại bất kì điểm nào theo thời gian sẽ phụ thuộc vào sự di chuyển và hành động của cá nhân người sử dụng, và ngoài sự điều khiển của người vận hành mạng.

Ngắt kết nối và tái kết nối: người sử dụng mạng thông tin vô tuyến thường xuyên có nguy cơ bị ngắt kết nối đột ngột từ mạng. Điều này có thể xảy ra vì nhiều lý do: do người sử dụng di chuyển thiết bị di động ngoài vùng phủ sóng của trạm gốc mà chúng đang liên lạc với nó; do sự di chuyển của người sử dụng gây ra chướng ngại vật lý - ví dụ như một toà nhà hoặc một đường hầm giao thông giữa thiết bị di động và trạm gốc; hoặc chỉ bởi vì độ tin cậy thấp của đoạn nối vô tuyến. Cũng vậy, trong khi vận hành mạng thông tin tổ ong, vì người sử dụng di chuyển từ vùng phủ sóng của trạm gốc này đến vùng khác nên mạng phải truyền sự điều khiển của phiên truyền thông với một "hand-off" (chuyển giao), gây trễ và có thể bị ngắt kết nối.

Kết nối mạng hỗn tạp: Trong mạng hữu tuyến điển hình, một máy tính được kết nối cố định với cùng mạng nhà. Đặc tính của mạng này là số lượng biết trước trong khi sự thay đổi - tức là một hệ thống nâng cấp cho file server hoặc firewall có thể được hoạch định và giám sát một cách cẩn thận. Tuy nhiên, trong mạng vô tuyến, một trạm di động ví dụ như một máy điện thoại tổ ong hoặc PDA là được chuyển vùng thường xuyên giữa các mạng host khác nhau. Đặc tính của các mạng này và cách mà chúng tương tác với mạng nhà của người sử dụng có thể thay đổi đáng kể.

Cư trú địa chỉ: Trong mạng hữu tuyến thông thường, máy tính và các thiết bị khác được kết nối với cùng một mạng và gắn cùng địa chỉ mạng (địa chỉ IP trong thế giới Internet) trong một thời gian dài. Nếu thiết bị được di chuyển giữa các mạng, nhà quản trị mạng co thể cập nhật địa chỉ mạng. Trong môi trường liên mạng vô tuyến, các địa chỉ mạng - hoặc ít nhất mạng mà chúng liên quan - phải được quản lý trong những nguy cơ về an ninh và độ phức tạp nhiều hơn nhiều.

Thông tin phụ thuộc vị trí: Tình huống nói đến thông tin vị trí là song song với tình huống trong trường hợp cư trú địa chỉ. Trong mạng hữu tuyến, vị trí của các thiết bị tính toán tương đối tĩnh và được người quản trị biết trước. Trong môi trường vô tuyến, vị

trí của các thiết bị truyền thông và tính toán thay đổi thường xuyên. Cơ sở hạ tầng liên mạng vô tuyến không chỉ phải bám và trả lời những sự thay đổi vị trí này để cung cấp dịch vụ cho người sử dụng mà nó còn phải cung cấp sự phân phối an toàn để bảo vệ thông tin vị trí. Trong môi trường vô tuyến, bảo vệ tính bảo mật của người sử dụng dĩ nhiên gồm: bảo vệ nội dung bản tin và cuộc hội thoại chống lại sự xâm nhập, ngoài ra yêu cầu hệ thống giữ tính riêng tư vị trí người sử dụng hệ thống.

1.5.3 Vùng trở ngại 3: Tính di động của thiết bị

Để khai thác tiềm năng của mạng vô tuyến, người sử dụng yêu cầu các thiết bị truyền thông và tính toán có thể mang được dễ dàng. Một cơ sở hạ tầng truyền thông và tính toán di động sẽ không được sử dụng rộng rãi nếu con người phải mang máy tính để bàn để khai thác. Vì vậy, các sản phẩm điện tử thông dụng ngày nay ví dụ như điện thoại tổ ong, PDA, máy tính xách tay, camera số có nối mạng và những thiết bị giống như vậy được thiết kế để mang theo người khi di chuyển. Như Forman và Zahorjan nói: "Các máy tính để bàn ngày nay không được dự định để mang theo bên người, vì thế việc thiết kế chúng là tự do về mặt sử dụng không gian, nguồn nối cáp và nhiệt. Ngược lại, việc thiết kế, máy tính di động cầm tay nên cố gắng có được những tính chất của một chiếc đồng hồ đeo tay: nhỏ gọn, nhẹ, bền, chống thấm và tuổi thọ nguồn dài."

Một sự bao hàm hiển nhiên liên quan đến an ninh của tính di động của thiết bị là: bất kì sản phẩm nào được thiết kế để mang theo và sử dụng khi di chuyển đều dễ dàng bị đánh cắp. Không chỉ là một máy điện thoại tổ ong - một mục tiêu đơn giản của bọn trộm mà từ quam điểm của hệ thống, rằng không còn nghi ngờ gì nữa thiết bị đang di chuyển từ thị trấn này đến thị trấn khác mặc dù bây giờ nó có thể đang thuộc quyền sở hữu của một ai đó không phải người sở hữu.

Nhân tố di động cũng áp đặt những giới hạn khác lên người thiết kế các sản phẩm tính toán và truyền thông di động về mặt nhận thực và an ninh. Những điều này bao gồm:

Tốc độ bộ xử lý: Năng lực xử lý được cho bởi các mạch tích hợp IC được sử dụng trong các thiết bị như điện thoại tổ ong và PDA đang tăng theo thời gian nhưng chưa đạt đến tốc độ bộ xử lý của máy tính để bàn hoặc các server mạng. Thuật toán mật mã và

nhận thực yêu cầu sự tính toán thậm chí là rất lớn. trong một vài ứng dụng về an ninh trong môi trường vô tuyến ví dụ như mật mã và giải mật mã một cuộc thoại được tiến hành thông qua máy điện thoại tổ ong thì các thủ tục an ninh phải thực thi gần như thời gian thực. Vì vậy, năng lực xử lý khả dụng trên thiết bị di động giới hạn sự lựa chọn của người thiết kế hệ thống an ninh cho môi trường vô tuyến.

Dung lượng lưu trữ giới hạn: Vì các lý do tương tự, một lượng dữ liệu được lưu trữ trong thiết bị tính toán và truyền thông di động nhỏ hơn dung lượng lưu trữ dữ liệu của máy tính để bàn hoặc server. Mặc dù ít quan trọng hơn tốc độ bộ xử lý nhưng nhân tố này cũng ảnh hưởng đến sự lựa chọn được thực hiện trong khi thiết kế hệ thống an ninh cho mạng vô tuyến.

Sự vận hành công suất nhỏ: Các sản phẩm điện tử di động hoạt động dựa vào pin. Bất kỳ công việc nào được thực hiện bởi bộ xử lý trong máy điện thoại tổ ong hoặc PDA tiêu hao năng lượng và vì vậy làm giảm tuổi thọ của nguồn. Theo quan điểm của người sử dụng sản phẩm, khi an ninh là đặc điểm quan trọng thì việc thực hiện nó được đặt lên hàng đầu. Vì vậy, thậm chí có thể thực thi thuật toán nhận thực hoặc an ninh tốn nhiều công việc xử lý theo quan điểm kỹ thuật, thì sự tiêu tốn năng lượng nguồn nuôi có lẽ không thể chấp nhận được.

Như có thể thấy từ danh sách này, những trở ngại mà người thiết kế kiến trúc và hệ thống bảo mật cho mạng vô tuyến phải đối mặt là rất lớn lao, và chúng khác nhau theo cả loại hình lẫn mức độ so với trường hợp trong mạng hữu tuyến thông thường. Thực tế, những nhân tố này giải thích tại sao sự quan tâm về an ninh trong môi trường vô tuyến khác với sự xem xét tương ứng về mạng hữu tuyến. Một khuynh hướng đáng quan tâm là truy nhập Internet không dây đang phát triển ngày càng rộng khắp, và nhiều mạng nhà và mạng liên kết đang kết hợp chặt chẽ với các thành phần vô tuyến. Vì lí do này, các nhân tố được phác thảo trong phần này sẽ được đề cập sau để tăng ảnh hưởng lên việc thiết kế hệ thống an ninh mà không dự định cho môi trường vô tuyến thuần tuý.

CHƯƠNG 2: NHỮNG ỨNG DỤNG TIỀM NĂNG CỦA CÁC PHƯƠNG PHÁP KHOÁ CÔNG CỘNG TRONG MÔI TRƯỜNG LIÊN MẠNG VÔ TUYẾN

Trong những năm 1980, khi các giao thức bảo mật cho GSM đang được phát triển, sự phê bình được nói đến nhiều nhất về mật mã khóa công cộng cũng như mạng vô tuyến liên quan là các giao thức yêu cầu việc xử lý quá nhiều. Chẳng hạn, RSA được ước tính là yêu cầu tính toán gấp 1000 lần so với công nghệ mật mã khóa riêng. Cho trước giới hạn của các máy điện thoại tổ ong dưới dạng cả tốc độ xử lý lẫn tuổi thọ nguồn, người thiết kế mạng tổ ong đã nhận thấy điều này phải trả một giá quá cao.

2.1. Thuật toán khóa công cộng "Light-Weight" cho mạng vô tuyến

Bắt đầu vào đầu những năm 1990, các nhà nghiên cứu đã tìm ra các thuật toán luân phiên yêu cầu phải thực hiện ít xử lý hơn. Các thuật toán này có thể được áp dụng cho nhận thực và an ninh trong môi trường liên mạng vô tuyến. Trong số này có kỹ thuật MSR (Module Square Root) và một vài biến thể của ECC (Elliptic Curve Cryptography: Mật mã đường cong). Những thuật toán này sẽ được mô tả khái quát trong các phần nhỏ dưới đây.

2.1.1 Thuật toán MSR

Thuật toán MSR được giới thiệu bởi M.O.Rabin năm 1979, và sau đó được nghiên cứu cho tiềm năng trong các hệ thống thông tin cá nhân bởi Beller, Chang và Yacobi đầu những năm 1990. Giống như hầu hết các thuật toán mật mã, phương pháp ở đây là dựa trên số học modul và phụ thuộc vào sự phức tạp của việc phân tích ra thừa số những số lớn.

Nói chung, MSR hoạt động như sau. Khóa công cộng là một modul, N, là tích của hai số nguyên tố lớn, p và q (trong đó, khi thực hiện trong thực tế, p và q điển hình là những số nhị phân có độ dài từ 75 đến 100 bít). Tổ hợp p và q tạo thành thành phần khóa riêng của thuật toán. Nếu Principal A muốn chuyển bản tin tin cậy M tới Principal B, đầu tiên A tính $C \equiv M^2 \bmod N$, trong đó C là đoạn văn bản mật mã phát sinh và M^2 là giá trị nhị

phân của bản tin M đã được bình phương. Chú ý rằng đây là phép toán modul vì thế lấy giá trị phần dư modul N. Khi nhận được đoạn văn bản mã hóa C, principal B, người biết p và q có thể đảo ngược quá trình này bằng cách lấy ra modul căn bậc 2 của C để lấp ra M (nghĩa là M≡SQRT(C) mod N). Đối với phía không có quyền truy nhập đến các giá trị của p và q, thực hiện giải pháp bị cản trở do sự khó khăn của thừa số N – không có thuật toán độ phức tạp đa thức.

Ngoài sự thật rằng nó trợ giúp mật mã khóa riêng/khóa công cộng và chế độ truyền bản tin, MSR có một ưu điểm lớn thứ hai khi nó được sử dụng cho môi trường vô tuyến. Việc tải thuật toán có sử dụng máy điện toán là bất đối xứng. Tính modul bình phương cần cho mật mã yêu cầu ít tính toán hơn nhiều (chỉ một phép nhân modul) so với lấy modul căn bậc 2 để trở lại văn bản thường (điều này yêu cầu phép tính số mũ). Vì vậy, nếu chức năng mã hóa có thể được đặt trên trạm di động, và chức năng giải mật mã trên trạm gốc, một cách lý tưởng MSR đáp ứng những hạn chế được đặt ra bởi máy điện thoại có bộ xử lý chậm và dự trữ nguồn giới hạn.

2.1.2 Mật mã đường cong elíp (ECC: Elliptic Curve Cryptography)

Trong những năm gần đây, ECC cũng đã nổi lên như một kỹ thuật mật mã tiềm năng cho các ứng dụng trong các mạng vô tuyến. Trọng tâm đặt vào việc tối thiểu các yêu cầu cho tài nguyên bộ xử lý dành cho mật mã trong trạm di động, "sức mạnh của mật mã cho mỗi bít khóa" trở thành một phẩm chất quan trọng. Nói chung người ta chấp nhận rằng mật mã với ECC sử dụng các khóa 160 bít đưa ra xấp xỉ cùng mức bảo mật như RSA có khóa 1024 bít và ít nhất một nghiên cứu đã chỉ ra rằng ECC thậm chí có khóa 139 bít cũng cung cấp được mức bảo mật này.

Koduri, Mahajan, Montague, và Moseley đã đề xuất một phương pháp nhận thực tổ hợp các mật khẩu cá nhân ngắn với mật mã dựa trên ECC. Các tác giả sử dụng hai biến thể của phương pháp ECC cơ bản, EC-EKE (Elliptic Curve Encrypted Key Exchange: Trao đổi khóa mật mã đường cong elíp) và SPECKE (Simple Password Elliptic Curve Key Exchange: Trao đổi khóa đường cong mật khẩu đơn giản). Cả hai biến thể đều yêu cầu các Principal đang liên lạc thảo thuận một password, định nghĩa toán học của một

đường cong elip cụ thể, và một điểm trên đường cong này, trước khi thiết lập một phiên truyền thông (mặc dù không được nghiên cứu trong tài liệu này, một trung tâm nhận thực có thể cung cấp các thông tin cần thiết cho các Principal như một sự trao đổi nhận thực).

Khi thực hiện thử một thủ tục nhận thực cho các môi trường vô tuyến sử dụng ECDSA (Elliptic Curve Digital Signature Algorithm: Thuật toán chữ ký số đường cong elíp), Aydos, Yanik và Koc đã sử dụng các máy RISC 80MHz ARM7TDMI như là bộ xử lý mục tiêu (ARM7TDMI được sử dụng trong các ứng dụng số trong các sản phẩm di động được thiết kế để liên lạc thông qua mạng vô tuyến). Bằng cách sử dụng khóa ECC độ dài 160 bit, việc tạo chữ ký ECDSA yêu cầu 46,4 ms, đối với 92,4 ms cho sự xác minh chữ ký. Với một độ dài khóa 256 bít phải mất tới 153,5 ms cho việc tạo chữ ký và 313,4 ms cho việc xác minh. Các tác giả kết luận rằng cách tiếp cận ECDSA dựa trên ECC tới việc xác minh thuê bao là một sự lựa chọn thực tế cho môi trường vô tuyến.

2.2. Beller, Chang và Yacobi: Mật mã khóa công cộng gặp phải vấn đề khó khăn

Trong một bài viết năm 1993 của *IEEE Journal on Selected Areas in Communications*, Beller, Chang và Yacobi định nghĩa các cách tiếp cận cho nhận thực và mật mã dữ liệu trong các ứng dụng mạng vô tuyến dựa trên mật mã khóa công cộng. Phương pháp đầu tiên được gọi là Giải pháp khóa công cộng MSR tối thiểu sử dụng phương pháp MSR và chính quyền trung ương tin cậy lưu giữ một modulus N và các thừa số cấu thành p và q. Khi các thuê bao bắt đầu các hợp đồng dịch vụ của chúng, một chứng nhận bí mật được đưa vào trong tổ hợp điện thoại mà tổ hợp này cũng sử dụng modul N. Giải pháp khóa công cộng MSN tối thiểu có sự yếu kém rằng người mạo nhận cổng trạm gốc nếu thành công sau đó có thể mạo nhận người sử dụng. Giao thức thứ hai trong ba giao thức này, giao thức MSR cải tiến (IMSR) giải quyết điểm yếu kém này bằng cách thêm việc nhận thực mạng tới trạm di động. Cuối cùng, giao thức thứ 3 – Giao thức MSR+DH bổ sung sự trao đổi khóa Diffie-Hellman vào phương pháp Modul căn bậc 2 cơ sở.

Các mục nhỏ dưới đây khám phá giao thức MSR cải tiến chi tiết hơn. Một số chú ý sau đó được cung cấp về cách mà giao thức MSR+DH bổ sung vào khả năng của IMSR, cùng với một lời chú thích về sự quan trọng của giao thức của Beller, Chang, và Yacobi.

2.2.1 Các phần tử dữ liệu trong giao thức MSN cải tiến

Trong giao thức IMSR, cả Trạm gốc mạng phục vụ (SNBS: Serving Network Base Station) lẫn Chính quyền chứng nhận (CA: Certification Authority) giữ các khóa công cộng được mô tả khi thảo luận về MSR, biểu diễn tích của hai số nguyên tố lớn p và q, cái mà tạo thành các khóa riêng. Mỗi trạm gốc mạng giữ một chứng chỉ, nhận được từ Chính quyền chứng nhận, áp dụng hàm băm h cho ID mạng của trạm gốc mạng và cho khóa công cộng của nó. Beller, Chang và Yacobi sử dụng thuật ngữ "Thiết bị điều khiển vô tuyến (RCE: Radio Control Equipment)" để xác định thực thể chức năng điều khiển các cổng truyền thông trên mạng vô tuyến. Vì chúng ta đã sử dụng "trạm gốc" để xác định chức năng này trong các chương khác của luận văn nên để nhất quán vẫn thuật ngữ này sẽ được sử dụng ở đây. (Thuật ngữ của Beller, Chang và Yacobi cũng đã được sửa đổi trong một vài chi tiết để giữ nhất quán).

Các phần tử và chức năng dữ liệu then chốt trong giao thức IMSR bao gồm:

1. **ID_{BS} (Base Station Identifier):** Bộ nhận dạng duy nhất của trạm gốc mạng vô tuyến (trong ngữ cảnh này là một trạm gốc trong mạng phục vụ hoặc mạng khách).
2. **ID_{MS} (Mobile Station Identifier):** Bộ nhận dạng duy nhất trạm di động. Điều này tương ứng với IMSI (International Mobile Subscriber Identity : Nhận dạng thuê bao di động quốc tế) trong giao thức nhận thực GSM.
3. **N_{BS} (Public Key of Base Station):** N_{BS}, khóa công cộng của trạm gốc là tích của 2 số nguyên tố lớn, p_{BS} và q_{BS}, chỉ trạm gốc của mạng và Chính quyền chứng nhận (CA) biết.
4. **N_{CA} (Public Key of CA):** N_{CA}, khóa công cộng của CA tương tự là tích của 2 số nguyên tố lớn, p_{CA} và q_{CA}, chỉ CA được biết.

5. **Ks (Session Key):** Một khóa phiên cho mật mã dữ liệu đến sau trong phiên truyền thông, được đàm phán trong giao thức nhận thực.

6. **RANDX (Random Number):** Một số ngẫu nhiên được chọn bởi trạm di động trong khi xác định Ks.

7. **h (Hash Function):** h là hàm băm một chiều, tất cả các Principal đều biết, hàm này giảm các đối số đầu vào tới cỡ của các modulus (nghĩa là cùng độ dài như N_{BS} và N_{CA}).

8. Trạm gốc kiểm tra tính hợp lệ của chứng nhận bằng cách bình phương giá trị chứng nhận modul N_{CA}, và so sánh nó với giá trị của h (ID_{BS}, N_{BS}) (được tính toán một cách độc lập). Nếu các giá trị trùng khớp với nhau thì trạm di động thông qua, nếu khác nó hủy bỏ phiên truyền thông.

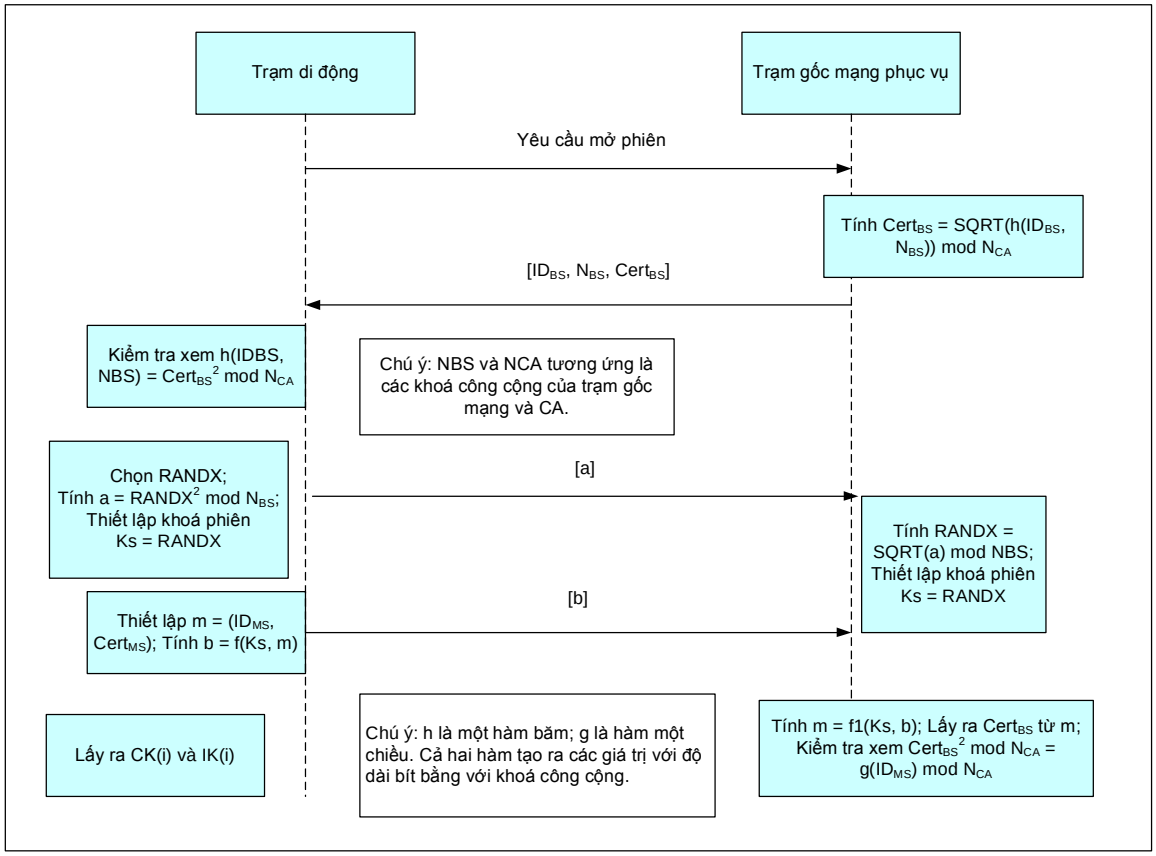
9. Trạm di động chọn một số ngẫu nhiên được gọi là RANDX có chức năng như khóa phiên Ks. Trạm di động sau đó tính một giá trị gọi là a, trong đó $a \equiv RANDX^2 \bmod N_{BS}$. Trạm di động sau đó sẽ gửi a đến trạm gốc.

10. Server mạng tính giá trị RANDX (trong thực tế đây là khóa phiên Ks) bằng cách tính $RANDX \equiv sqrt(a) \bmod N_{BS}$. Chú ý rằng kẻ nghe trộm không thể thực hiện được tính toán này bởi vì kẻ nghe trộm không truy cập được các thừa số p và q của trạm gốc. Cả trạm gốc lẫn trạm di động bây giờ dùng chung khóa phiên Ks.

11. Bây giờ trạm di động sử dụng khóa phiên Ks, hàm f, và một chuỗi m để tính ra một giá trị gọi là b, trong đó $b \equiv f(Ks, m)$. Chuỗi m ở trên móc nối ID_{MS} và $Cert_{MS}$ với nhau. Trạm di động truyền b tới trạm gốc mạng.

12. Trạm di động sử dụng sự hiểu biết của nó về khóa phiên Ks để giải mật mã b và lấy ra m. Từ chuỗi m, trạm gốc lấy ra chứng nhận cho trạm di động $Cert_{MS}$, và tính $Cert_{MS}^2 \bmod N_{CA}$. Giá trị này được so sánh với $g(ID_{MS}) \bmod N_{CA}$. Nếu kết quả trùng nhau, thì trạm di động trong thực tế là đúng và khoá phiên được xác nhận.

Hoạt động của giao thức IMSR được mô tả theo sơ đồ trong **hình 2.1**. Chú ý rằng, trong khi hình vẽ chỉ mô tả giao tiếp giữa trạm di động và trạm gốc mạng, thì quyền xác nhận cũng là một phần quan trọng của cơ sở hạ tầng. Tuy nhiên với giao thức IMSR cho trước, thì CA được yêu cầu khi trạm gốc được thiết lập và khi thuê bao đăng ký dịch vụ trừ thời điểm phiên riêng. Điều này có ưu điểm giảm yêu cầu cho truyền thông khoảng cách xa từ các mạng phục vụ đến mạng nhà trong khi thiết lập một phiên truyền thông.



Hình 2.1: Biểu đồ minh hoạ hoạt động của thuật toán IMSR

2.2.2 Giao MSR+DH

Beller, Chang và Yacobi thông báo một sự yếu kém quan trọng trong giao thức IMSR. Trạm gốc mạng được cung cấp với các thông tin đủ bí mật về trạm di động mà trạm gốc chứng minh là không tin cậy, vì vậy trong tương lai nó có thể đóng vai trò trạm gốc và nhận các dịch vụ một cách gian lận. Giải pháp mà các nhà nghiên cứu đặt ra cho vấn đề này là bổ xung khoá chuyển đổi Diffie-Hellman vào giao thức IMSR. Với sự tăng

cường này, sự tiếp xúc bị hạn chế đối với những thành viên nội bộ mà biết được các giá trị p và q cho CA.

2.2.3 Beller, Chang và Yacobi: Phân tích hiệu năng

Một phần quan trọng được đề xuất bởi Beller, Chang và Yacobi về khả năng phát triển của giao thức khoá công cộng ví dụ như những giao thức họ đề xuất trong tài liệu năm 1993 là phân tích hiệu năng. Như đã chú ý trước đây, tất cả ba giao thức là bất đối xứng theo yêu cầu tính toán. Về phía server, các giao thức này yêu cầu lấy ra modul căn bậc 2 - một quá trình đòi hỏi nhiều tính toán thậm chí ngay cả khi các thừa số nguyên tố p và q có sẵn. Tuy nhiên với các server mật mã chuyên dụng trong trạm gốc mạng, tác giả biện luận rằng điều này là khả dụng thậm chí bằng cách sử dụng phần cứng năm 1993. Ngược lại, gánh nặng tính toán bị áp đặt bởi IMSR trên máy cầm tay là nhỏ. Chỉ cần đến hai phép nhân modul. Mức tính toán này có thể quản lý một cách dễ dàng ngay cả với bộ vi xử lý 8 bít. Khi bổ xung khoá chuyển đổi Diffie-Hellman vào thì với giao thức MSR+DH, khối lượng tính toán tăng lên tới 212 phép nhân modul trong giao thức nhận thực, thực hiện các modul 512 bít. Điều này là không thực tế đối với các máy cầm tay chỉ được trang bị một bộ vi điều khiển. Tuy nhiên tác giả biện luận rằng, với các chuẩn phần cứng năm 1993 thì có thể triển khai được cho máy cầm tay có trang bị một DSP (Digital Subscriber Processor: Bộ xử lý tín hiệu số) và sẵn sàng có thể thực hiện trong năm 2001.

2.3 Carlsen: Public-light – Thuật toán Beller, Chang và Yacobi được duyệt lại

Trong một tài liệu năm 1999 xuất hiện trong *Operating System Review,* Ulf Carlsen đánh giá và phê bình phương pháp khoá công cộng được đề xuất bởi Beller, Chang và Yacobi (BCY) được mô tả trong phần trước. Carlsen đồng ý với BCY rằng giao thức MSR đơn giản dễ bị tấn công nơi bọn trộm giả mạo là trạm gốc hợp pháp tạo ra 2 số nguyên tố p và q riêng của nó, và chuyển tích N tới trạm di động như thể nó là khoá công cộng thực. Theo Carlsen, những chứng nhận giao thức IMSR cũng có sự yếu kém trong đó chúng không chứa các dữ liệu liên quan đến thời gian ví dụ như dữ liệu hết hạn. Điều này nghĩa là IMSR dễ bị tấn công phát lại trong đó chứng nhận cũ được sử dụng lại bởi

bọn tấn công sau khi khoá phiên tương ứng được tiết lộ. Giải pháp tiềm năng để giải quyết vấn đề này là gồm việc thêm tem thời gian vào chứng nhận IMSR, làm cho CA hoạt động "online" như một thành phần tham gia tích cực trong giao thức, hoặc tạo và phân phối "quyền thu hồi giấy phép".

Carlsen đề xuất hai giao thức để tăng cường cho các giao thức được đưa ra bởi BCY nhằm tăng cường việc đảm bảo an ninh trong khi vẫn giữ được một vài ưu điểm của phương pháp khoá công cộng.

- **Giao thức trả lời khoá bí mật (Secret – Key Responder Protocol):** Giao thức này giới thiệu lại một khoá bí mật được xử lý bởi trạm di động cũng như server tin cậy ("trusted server") mà riêng biệt với trạm di động và trạm gốc mạng. Trusted server biết khoá riêng của trạm di động và vì vậy có thể giải mật mã một nonce được mật mã bởi trạm di động với khoá riêng của trạm di động. Nonce được sử dụng để đảm bảo đúng thời hạn trao đổi bản tin nhận thực; trong khi sự có mặt của trusted server trong hình ảnh cho phép trạm di động khởi tạo phiên truyền thông mà không phải quảng bá nhận dạng riêng của nó một cách rõ ràng.
- **Giao thức an ninh Đầu cuối-đến-Đầu cuối (End –to – End Security Protocol):** Carlsen chỉ ra rằng nhiều sơ đồ bảo mật cho mạng vô tuyến đảm nhận an ninh của mạng vô tuyến. Tuy nhiên, điều này là giả thuyết tối ưu thái quá: " Người sử dụng nghĩ rằng dưới dạng an ninh di động và ít tin tưởng vào hiệu quả của việc đo đạc độ an toàn được điều khiển bởi người vận hành. Vì vậy yêu cầu của người sử dụng là các dịch vụ bảo mật end -to- end (các thành phần mạng được điều khiển bởi người vận hành không thể can thiệp đến) nên được cung cấp." Một khía cạnh thú vị của Giao thức bảo mật đầu cuối đến đầu cuối là, trước khi khoá phiên được tạo ra và được trao đổi thì giao thức yêu cầu hai người nghe nhận thực ID của nhau bằng cách nhận ra giọng nói của nhau và xác nhận nó (Giao thức vì vậy không hữu dụng khi tương tác với những người nghe mà người sử dụng không quen biết).

Nói chung, Carlsen ít lạc quan hơn Beller, Chang và Yacobi rằng phương pháp khoá công cộng có thể thực hiện một mức hiệu năng cho phép chúng có thể linh động sử dụng trong các hệ thống mạng vô tuyến thực.

Do hiệu năng về thời gian hạn chế, công nghệ khoá công cộng hiện thời không thích hợp cho việc cung cấp độ tin cậy nhận dạng đích trong giao thức responder. Ngoài ra chúng ta đã thấy rằng ưu điểm của công nghệ khoá công cộng giảm khi server online và có thể là trusted server được yêu cầu. Điều này ít tối ưu hơn cho việc sử dụng công nghệ khoá công cộng như một giải pháp chung cho nhận thực và tính riêng tư trong các giao thức PCS (Personal Communications Services: Các dịch vụ thông tin cá nhân) khi độ tin cậy nhận dạng đích được yêu cầu.

Vấn đề này hiện ra rõ ràng đặc biệt trong các vùng đô thị, nơi mà số các máy di động được đặt đồng thời tại một cổng vô tuyến cụ thể có thể lên đến hàng trăm.

2.4. Aziz và Diffie: Một phương pháp khoá công cộng hỗ trợ nhiều thuật toán mật mã

Trong một bài viết năm 1994 trong *IEEE Personal Communications*, Ashar Aziz và Witfield Diffie cũng đề xuất một giao thức cho các mạng vô tuyến sử dụng giao thức khoá công cộng cho nhận thực và tạo khoá phiên, và một phương pháp khoá riêng cho mật mã dữ liệu trong một phiên truyền thông. Giống như đề xuất của Beller, Chang và Yacobi được mô tả ở trên, phương pháp của Aziz và Diffie sử dụng chứng nhận số và CA. Một đặc tính riêng biệt của phương pháp Aziz-Diffie là nó cung cấp sự hỗ trợ rõ ràng cho trạm di động và trạm gốc mạng để đàm phán thuật toán mật mã khoá riêng nào sẽ được sử dụng để thực hiện tính tin cậy dữ liệu.

2.4.1 Các phần tử dữ liệu trong giao thức Aziz-Diffie

Các phần tử dữ liệu quan trọng trong giao thức nhận thực được đề xuất bởi Aziz và Diffie gồm:

1. **RCH1 (Random Chanllenge):** RCH1 là một giá trị yêu cầu ngẫu nhiên được tạo bởi trạm di động trong pha khởi tạo của giao thức nhận thực. Aziz và Diffie đề xuất độ dài 128 bít.
2. **$Cert_{MS}$ (Certificate of the Mobile Station):** Certificate của trạm gốc chứa các phần tử dữ liệu dưới đây: Số Sêri (Serial number), thời gian hiệu lực, tên máy, khoá công cộng của máy và tên CA. Nội dung và định dạng Cert tuân theo CCITT X.509. Cert được kí với bản tin digest được tạo với khoá riêng của CA. Nhận dạng chứa trong CA này trong Cert cho phép Principal khác đảm bảo an toàn khoá công cộng CA.
3. **$Cert_{BS}$ (Certificate of Base Station):** $Cert_{BS}$ có cùng các phần tử và cấu trúc như của trạm di động.
4. **KU_{MS} (Public Key):** Khoá công cộng của trạm di động.
5. **KU_{BS} (Public Key):** Khoá công cộng của trạm gốc.
6. **RAND1; RAND2 (Random Numbers):** RAND1, được tạo bởi trạm gốc và RAND2, mà trạm di động tạo ra được sử dụng trong việc tạo khoá phiên.
7. **Ks (Session Key):** Khoá phiên được tạo thông qua việc sử dụng cả RAND1 lẫn RAND2.
8. **SKCS (List of Encription Protocols):** SKCS cung cấp một danh sách các giao thức mật mã dữ liệu khoá riêng mà trạm di động có thể sử dụng cho việc mật mã dữ liệu được truyền dẫn trong một phiên truyền thông.
9. **Sig (Digital Signatures):** Những chữ ký số dưới giao thức Aziz-Diffie, được tạo ra bằng cách sử dụng khoá riêng của đăng ký principal, và được áp dụng bằng cách áp dụng khoá công cộng của người ký.

2.4.2 Hoạt động của giao thức Aziz-Diffie

Chuỗi trao đổi bản tin giữa trạm di động và trạm gốc mạng trong giao thức Aziz-Diffie bao gồm:

1. Trạm di động gửi bản tin "request-to-join" (yêu cầu tham gia) tới một trạm gốc mạng trong vùng lân cận của nó. Bản tin request to join chứa ba phần tử chính: số được tạo ngẫu nhiên đóng vai trò như một yêu cầu (challenge), RCH1; chứng nhận trạm di động, $Cert_{MS}$; và một danh sách các thuật toán mật mã dữ liệu khoá riêng mà trạm di động có thể hỗ trợ, SKCS.
2. Trạm di động xác nhận giá trị của chữ ký trên chứng nhận của trạm di động. Chú ý rằng điều này chứng nhận rằng chính chứng nhận cũng là điều xác nhận có giá trị mà không phải là chứng nhận nhận được từ trạm di động cùng trạm di động mà chứng nhận phát hành tới. Nếu chứng nhận không có giá trị thì trạm gốc kết thúc phiên; nếu khác nó tiếp tục.
3. Trạm gốc trả lời trạm di động bằng cách gửi chứng nhận của nó, $Cert_{BS}$; một số ngẫu nhiên, RAND1, mật mã bằng cách sử dụng khoá công cộng của trạm di động; và lựa chọn thuật toán mật mã khoá riêng từ các thuật toán được giới thiệu bởi trạm di động. Trạm gốc chọn từ sự giao nhau của tập các thuật toán được giới thiệu bởi trạm di động và tập các thuật toán mà trạm gốc hỗ trợ thuật toán đó mà nó xem là đưa ra độ bảo mật cao. Độ dài khoá được đàm phán đến độ dài tối thiểu mà trạm di động có khả năng xử lý và trạm gốc hỗ trợ. Trạm gốc tính toán một chữ ký bản tin bằng cách sử dụng khoá riêng trên một tập các giá trị mà chứa giá trị đã mật mã RAND1, thuật toán mật mã dữ liệu được chọn, challenge RCH1 ban đầu nhận được từ trạm di động và danh sách ban đầu các thuật toán mật mã ứng cử.
4. Trạm di động xác nhận tính chất hợp lệ của chứng nhận nó đã nhận được từ trạm gốc. Trạm di động cũng xác nhận chữ ký trạm gốc bằng cách giải mật mã tập các giá trị nó đã nhận được trong bản tin đã kí, bằng cách sử dụng khoá công cộng của trạm gốc. Nếu giá trị RCH1 và giá trị các thuật toán mật mã ứng cử nhận được từ trạm gốc phù hợp với những giá trị này được truyền ban đầu bởi trạm di động thì nhận dạng trạm gốc được xác nhận. Nếu khác trạm di động kết thúc phiên truyền thông.
5. Trạm di động lấy ra giá trị RAND1 bằng giải mật mã sử dụng khoá riêng của nó.

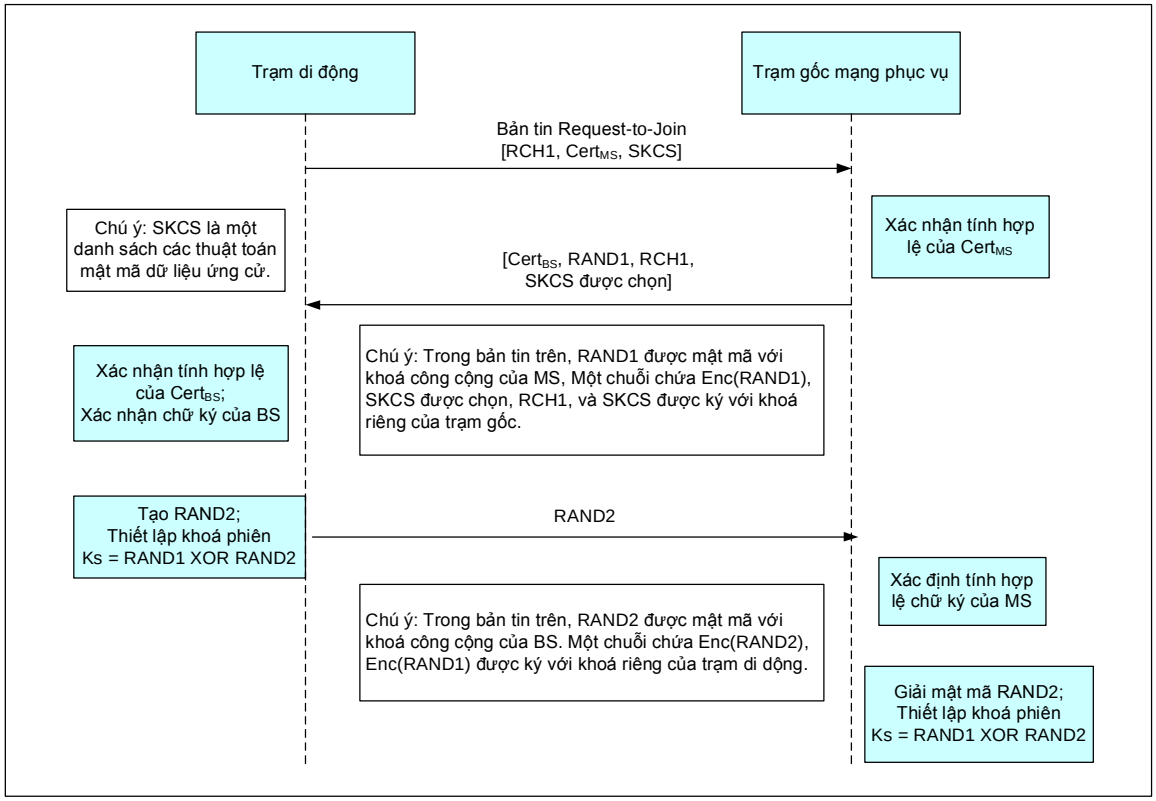
6. Trạm di động bây giờ tạo ra một giá trị ngẫu nhiên thứ hai, RAND2 có cùng độ dài bít như RAND1 và làm phép toán logic XOR hai chuỗi. Chuỗi tạo ra bởi RAND1⊗RAND2 sẽ cấu thành một khoá phiên cho phiên truyền thông này. Trạm di động mật mã giá trị RAND2 theo khoá công cộng của trạm gốc.
7. Trạm di động gửi giá trị đã mật mã RAND2 tới trạm gốc. Nó cũng tính toán chữ ký của nó trên một tập các giá trị chứa giá trị mật mã RAND2, và giá trị đã mật mã RAND1 mà nó đã nhận được trước đây từ trạm gốc. (Bởi vì giá trị mật mã RAND1 này bây giờ được ký với khoá riêng của trạm di động nên trạm gốc có một cơ chế để xác nhận việc nhận thực trạm di động). Trạm di động gửi các phần tử dữ liệu này tới trạm gốc.
8. Trạm gốc xác nhận chữ ký trên bản tin vừa nhận được từ trạm di động bằng cách sử dụng khoá công cộng trạm di động. Nếu chữ ký được xác nhận, trạm gốc chấp nhận trạm di động như một thuê bao hợp lệ.
9. Trạm gốc giải mật mã giá trị RAND2 bằng cách sử dụng khoá riêng của nó. Trạm gốc bây giờ có thể tạo ra RAND1⊗RAND2, để nó cũng nắm giữ khoá phiên. (Chú ý rằng để đảm bảo an toàn khoá phiên RAND1⊗RAND2, một kẻ xâm nhập cần truy nhập vào khoá riêng của cả trạm gốc lẫn trạm di động ít có khả năng hơn là một trong hai bị xâm nhập).

Đáng chú ý rằng chữ ký số được thêm vào bản tin được gửi bởi trạm gốc trong bước 3 ở trên có ba vai trò khác nhau sau đây: (1) để nhận thực bản tin, (2) để cung cấp sự trả lời yêu cầu (Challenge) tới bản tin đầu tiên của trạm di động, và (3) để nhận thực bản tin đầu tiên nhận được thông qua việc chứa danh sách ban đầu các thuật toán ứng cử. Cũng chú ý rằng, trong khi CA không liên quan trực tiếp đến chuỗi giao thức nhận thực thì CA đã ký các xác nhận cả trạm gốc lẫn trạm di động trong một bước ưu tiên.

Để vạch ra sự trao đổi bản tin trong giao thức Aziz-Diffie, hãy xem **hình 2.2**.

Aziz và Diffie nhấn mạnh tình huống nơi mà không chỉ có một CA mà có nhiều CA được yêu cầu trong một mạng hoạt động rộng tuân theo đặc tả CCITT X.509. Trong

trường hợp này, bản tin thứ 2, được gửi trạm gốc tới trạm di động, sẽ bao gồm không chỉ chứng nhận trạm gốc mà còn chứa đường dẫn chứng nhận mà sẽ cho phép chứng nhận được công nhận hợp lệ trong một phân cấp các CA.



Hình 2.2: Sơ đồ minh hoạ chuỗi trao đổi bản tin trong giao thức Aziz-Diffie.

2.5 Bình luận và đánh giá giao thức Aziz-Diffie

Ngược với kiến trúc các giao thức thế hệ hai, Aziz và Diffie nhấn mạnh giao thức hỗ trợ nhận thực tương hỗ. Các chứng nhận số và một CA đóng một vai trò quan trọng trong phương pháp lai khoá riêng và khoá công cộng. Giao thức này chỉ bảo vệ đoạn nối vô tuyến chính xác nhưng Aziz và Diffie muốn cho phép có chế bảo mật end-to-end hoạt động ở mức ứng dụng và mức truyền tải trong khi giao thức của họ hoạt động ở tầng mạng. Một khía cạnh quan trọng phân biệt giao thức này với các giao thức khác được mô tả trong chương này là Aziz-Diffie tạo ra một cơ chế rõ ràng cho phép trạm di động và trạm gốc mạng đàm phán và chọn trong số các giao thức mật mã dữ liệu ứng cử.

2.6 Tổng kết mật mã khoá công cộng trong mạng vô tuyến

Từ quan điểm của những người thiết kế và vận hành mạng thông tin tổ ong, các công trình được mô tả trong chương này rõ ràng là vượt thời đại. Các phương pháp khoá công cộng được tán thành bởi BCY, Carlsen và Aziz và Diffie gần đây đã nổi lên, trong khi kinh nghiệm nhận được từ chúng trong lĩnh vực Internet thì chúng chưa được chứng minh trong môi trường mạng tổ ong thương mại diện rộng. Bằng cách tập trung vào các phương pháp tính toán vừa phải như MSR và mật mã đường cong elíp, việc nghiên cứu ở đây tìm kiếm mối quan tâm liên quan tới hiệu năng và khả năng mở rộng. Từ đầu đến giữa những năm 1990, sự trải rộng vẫn là quá lớn cho các nhà vận hành mạng. Tuy nhiên khi thế giới mạng, thậm chí đối với các lưu lượng thoại hướng tới cơ chế dựa trên IP và khi Internet trở thành một mô hình nổi bật cho tất cả các loại truyền thông dữ liệu thì sự việc này sẽ thay đổi.

CHƯƠNG 3: NHẬN THỰC VÀ AN NINH TRONG UMTS

3.1 Giới thiệu UMTS

Hệ thống viễn thông di động toàn cầu (UMTS) là một cơ cấu tổ chức được phối hợp bởi Liên minh viễn thông quốc tế (ITU) để hỗ trợ các dịch vụ thông tin vô tuyến thế hệ ba. UMTS là một phần của một cơ cấu tổ chức lớn hơn là IMT-2000. Vai trò chính của cả UMTS và IMT-2000 là tạo ra một nền tảng cho thông tin di động khuyến khích việc giới thiệu phân phối nội dung số và các dịch vụ truy nhập thông tin mà bổ xung cho thông tin thoại thông thường trong môi trường vô tuyến. Thực hiện mục tiêu này rõ ràng đòi hỏi băng tần rộng hơn 10Kbit/s sẵn có trong hầu hết hệ thống thế hệ thứ hai, vì thế UMTS sẽ hỗ trợ tốc độ truyền số liệu lên tới 2 Mbits/s. Phổ cho lưu lượng UMTS, cũng như việc thực hiện IMT-2000 trên thế giới rơi vào khoảng giữa 1870GHz và 2030GHz.

Giấy phép đầu tiên cho hệ thống UMTS đã được thực hiện ở Châu Âu. Tại Nhật Bản, các kế hoạch yêu cầu việc triển khai sớm IMT-2000 băng tần cao tương thích với các dịch vụ tổ ong bắt đầu từ tháng 5-2001. Trên toàn thế giới, việc triển khai cơ sở hạ tầng UMTS sẽ tiếp tục giữa năm 2001 đến 2005 với nhiệt tình ban đầu có thể bị kiềm chế bởi thực tế thị trường - những hệ thống này đắt đối với các nhà cung cấp dịch vụ, và đòi hỏi một số lượng lớn các thuê bao để tạo ra lợi nhuận. Một báo cáo gần đây được phát hành bởi UMTS Forum đưa ra một vài ưu điểm về thế hệ ba: "…Thế hệ 3 mang đến nhiều tính di động hơn tới Internet, xây dựng trên đặc tính di động duy nhất nhằm cung cấp nhắn tin nhóm, các dịch vụ dựa trên vị trí, các thông tin cá nhân hoá và giải trí. Nhiều dịch vụ thế hệ ba mới sẽ không dựa trên Internet, chúng thực sự là các dịch vụ di động thuần tuý. Vào năm 2005, nhiều dữ liệu hơn thoại sẽ chảy qua mạng di động."

Theo quan điển này về tiềm năng của các dịch vụ thông tin vô tuyến thế hệ thứ ba, các thuê bao sẽ không chỉ thông tin với nhau qua mạng. Họ sẽ tải các nội dung giàu tính đồ hoạ và tận hưởng các trò chơi trong khi đang di chuyển. Họ sẽ trao đổi các văn bản qua đầu cuối vô tuyến của họ. Và họ sẽ tiến hành một phạm vi rộng các giao dịch thương mại điện tử từ bất kỳ nơi nào họ xuất hiện. Mặc dù chi tiết về cách các nhà cung cấp dịch vụ

sẽ bổ xung vào tầm nhìn này thông qua việc thực hiện hệ thống thực chưa được xác định, một điều rõ ràng là - một mức độ bảo mật thông tin và nhận thực thuê bao cao sẽ là cấp bách và bắt buộc.

Nhiều công trình gần đây trong việc định nghĩa kiến trúc an ninh cho UMTS đã được tiến hành trong một số các dự án nghiên cứu được tài trợ bởi Liên minh Châu Âu và các chương trình quốc gia Châu Âu. Những dự án này bao gồm ASPeCT ("Advanced Security for Personal Communications Technology"—ACTS program), MONET (part of RACE Program) và '3GS3 – (Third Generation Mobile Telecommunications System Security Studies: Nghiên cứu an ninh hệ thống viễn thông di động thế hệ ba) (theo chương trình UK LINK). Một dự án gần đây hơn, USECA (UMTS Security Architecture: Kiến trúc an ninh UMTS) được chỉ đạo bởi các nhà nghiên cứu tại Vodafone đang định nghĩa một tập đầy đủ các giao thức an ninh và các thủ tục cho môi trường UMTS. Phạm vi của dự án là rộng, bao gồm các nghiên cứu sáu miềm con: các đặc điểm và yêu cầu bảo mật, các cơ chế bảo mật, kiến trúc bảo mật, cơ sở hạ tầng khoá công cộng, modul thông tin thuê bao (USIM), và bảo mật đầu cuối (handset).

Các kiến trúc quan trọng khác trong sự phát triển của các giao thức an ninh và nhận thực UMTS được gọi là 3GPP (Third-Generation Partnership Project: Dự án hợp tác thế hệ ba), một dự án quốc tế bao gồm những thành viên từ Bắc Mĩ và Châu Á.

3.2. Nguyên lý của an ninh UMTS

Các mạng tổ ong thế hệ hai được dự định mở ra một kỉ nguyên mới thông tin vô tuyến băng rộng, thúc đẩy phổ các dịch vụ thông tin và giải trí không khả thi với công nghệ thế hệ hai hiện thời. Tuy nhiên từ sự khởi đầu người thiết kế kiến trúc an ninh cho UMTS đã cố gắng xây dựng trên kiến trúc sẵn có và hoạt động một cách hiệu quả, đặc biệt là trong cơ sở hạ tầng GSM. Một phần điều này là bởi vì nó có ý nghĩa để xây dựng trên công nghệ đã được chứng minh; một phần nó phát sinh từ thực tế không thể chối cãi rằng trong nhiều năm UMTS sẽ phải cùng tồn tại và cùng hoạt động với mạng tổ ong thế hệ hai.

3.2.1 Nguyên lý cơ bản của an ninh UMTS thế hệ 3

Rất sớm các nhóm làm việc chịu trách nhiệm về việc phát triển kiến trúc an ninh và các giao thức cho môi trường UMTS đã thông qua ba nguyên lý cơ bản:

(1) Kiến trúc an ninh UMTS sẽ xây dựng trên các đặc điểm an ninh của các hệ thống thế hệ thứ hai. Các đặc điểm mạnh mẽ của các hệ thống 2G sẽ được duy trì.

(2) An ninh UMTS sẽ cải thiện trên an ninh của các hệ thống thế hệ hai. Một vài lỗ hổng an ninh và nhược điểm của các hệ thống 2G sẽ được giải quyết.

(3) An ninh UMTS cũng sẽ đưa ra nhiều đặc điểm mới và các dịch vụ bảo mật mới không có mặt trong các hệ thống 2G.

Khái niệm này tạo ra một điều gì đó tốt hơn GSM nhưng không phải là một điều gì đó hoàn toàn khác. Sự đổi mới trong UMTS nên được điều khiển không chỉ bởi tiềm năng kĩ thuật thuần tuý mà còn bởi những yêu cầu về môi trường quan trọng và tập các dịch vụ tham gia cho các mạng vô tuyến thế hệ ba.

Theo ngữ cảnh này, vào giữa năm 1999 3GPP đã định nghĩa một tập các đặc điểm an ninh mới hữu dụng cho UMTS, và cho các hệ thống thế hệ ba nói chung. Các đặc điểm an ninh mới cấu thành việc mô tả về các đặc tính then chốt của môi trường thế hệ ba. Những điểm then chốt như sau:

(1) Sẽ có những nhà cung cấp dịch vụ mới và khác nhau ngoài các nhà cung cấp các dịch vụ viễn thông vô tuyến. Sẽ bao gồm các nhà cung cấp nội dung và các nhà cung cấp dịch vụ số liệu;

(2) Các hệ thống di động sẽ được định vị như một phương tiện truyền thông yêu thích cho người dùng – ưa chuộng hơn các hệ thống đường dây cố định;

(3) Sẽ có nhiều dịch vụ trả trước và *pay-as-you-go*. Việc thuê bao dài hạn giữa người sử dụng và người vận hành mạng có thể không phải là một mô hình quen thuộc;

(4) Người sử dụng sẽ có quyền điều khiển nhiều hơn đối với các profile dịch vụ của họ và đối với các khả năng đầu cuối của họ.

(5) Sẽ có các cuộc tấn công chủ động vào người sử dụng;

(6) Các dịch vụ phi thoại sẽ quan trọng như các dịch vụ thoại hoặc quan trọng hơn;

(7) Các máy cầm tay di động sẽ được sử dụng như một nền tảng cho thương mại điện tử. Nhiều thẻ thông minh đa ứng dụng sẽ được sử dụng để trợ giúp nền tảng này.

Khi quan tâm đến các đặc điểm của môi trường thế hệ ba, nhóm cộng tác 3GPP đã phác thảo những đặc điểm nào của các hệ thống an ninh thế hệ hai được giữ lại, những sự yếu kém nào của thế hệ hai phải được giải quyết trong UMTS, và nơi mà kiến trúc an ninh UMTS sẽ giới thiệu những khả năng mới.

3.2.2 Ưu điểm và nhược điểm của GSM từ quan điểm UMTS

Các khả năng thế hệ hai được đưa tới xác định các phần tử hệ thống dưới đây (các đoạn văn bản giải thích được lấy ra từ tài liệu hợp tác 3GPP):

(1) Nhận thực thuê bao: "Các vấn đề với các thuật toán không phù hợp sẽ được giải quyết. Những điều kiện chú ý đến sự lựa chọn nhận thực và mối quan hệ của nó với mật mã sẽ được thắt chặt và làm rõ ràng."

(2) Mật mã giao diện vô tuyến: "Sức mạnh của mật mã sẽ lớn hơn so với mật mã được sử dụng trong các hệ thống thế hệ hai… Điều này để đáp ứng nguy cơ được đặt ra bởi năng lực tính toán ngày càng tăng sẵn có đối với việc phân tích mật mã của mật mã giao diện vô tuyến."

(3) Độ tin cậy nhận dạng thuê bao sẽ được thực hiện trên giao diện vô tuyến.

(4) SIM (Subscriber Identity Module: Modul nhận dạng thuê bao) sẽ là modul an ninh phần cứng có thể lấy ra được riêng rẽ với máy cầm tay theo tính năng an ninh của nó (nghĩa là SIM là một thẻ thông minh).

(5) Các đặc điểm an ninh toolkit phần ứng dụng SIM cung cấp kênh tầng ứng dụng an toàn giữa SIM và server mạng nhà sẽ được tính đến.

(6) Hoạt động của các đặc điểm an ninh hệ thống sẽ độc lập với người sử dụng (nghĩa là người sử dụng không phải làm bất cứ điều gì để kích hoạt các đặc tính an ninh).

(7) Yêu cầu cho mạng nhà tin cậy các mạng phục vụ để thực hiện một mức tính năng an ninh sẽ được tối thiểu hóa.

Trong lĩnh vực nhận thực thuê bao, phân tích này thông báo các vấn đề đã phát sinh xung quanh các thuật toán GSM độc quyền và yếu kém. Tuy nhiên một sự thoả mãn cơ bản với phương pháp của các hệ thống thế hệ hai đối với nhận thực cũng là hiển nhiên mà như chúng ta sẽ thấy đã ảnh hưởng lên việc ra quyết định cho nhận thực thuê bao trong UMTS:

Một danh sách những khiếm khuyết trong các giao thức an ninh thế hệ thứ hai mà UMTS phải quan tâm cũng là hữu dụng. Những vấn đề đó như sau:

(1) Các cuộc tấn công chủ động trong đó trạm gốc bị giả mạo là có khả năng xảy ra (thiếu nhận thực mạng đối với máy cầm tay di động).

(2) Khoá phiên và dữ liệu nhận thực trong khi được che đậy trong các tuyến vô tuyến lại được truyền một cách rõ ràng giữa các mạng.

(3) Mật mã không mở rộng đủ phức tạp đối với lõi mạng, dẫn đến việc truyền các văn bản rõ ràng của người sử dụng và các thông tin báo hiệu qua các tuyến vi ba.

(4) Thiếu chính sách mật mã và nhận thực đồng nhất qua các mạng nhà cung cấp dịch vụ tạo cơ hội cho việc xâm nhập.

(5) Cơ chế toàn vẹn dữ liệu cũng đang thiếu. Các cơ chế như thế ngoài việc tăng độ tin cập còn cung cấp việc bảo vệ chống lại sự mạo nhận trạm gốc.

(6) IMEI (International Mobile Equipment Identifier: Bộ nhận dạng thiết bị di động quốc tế) là một sự nhận dạng không an toàn.

(7) Sự gian lận và "sự can thiệp hợp pháp" (bị nghe trộm bởi các chính quyền thực thi luật) được xử lý như là một sự giải quyết đến sau hơn là trong pha thiết kế GSM ban đầu.

(8) Có một thiết sót về kiến thức mạng nhà và điều khiển cách mà mạng phục vụ sử dụng các tham số nhận thực cho các thuê bao mạng nhà chuyển vùng trong vùng phục vụ của mạng phục vụ.

(9) Độ mềm dẻo nhằm cập nhật và bổ xung các tính năng bảo mật theo thời gian để duy trì tính phổ biến các giao thức an ninh hệ thống là không cần thiết.

Yêu cầu sau đó đối với người thiết kế UMTS nhằm định nghĩa nhiều sự tăng cường cho các thủ tục và giao thức an ninh thế hệ hai mà giữ lại các đặc điểm của an ninh thế hệ hai mà giải quyết những thiếu sót trên của thế hệ hai và điều đó sẽ cho phép tính liên thông giữa hai miền trong những năm tới.

3.2.3 Các lĩnh vực tăng cường an ninh cho UMTS

Trong một tài liệu tháng 3-2000 được giới thiệu tại *Hội thảo IAB về liên mạng vô tuyến,* N.Asokan của trung tâm nghiên cứu Nokia đã cung cấp tổng kết dưới đây và các lĩnh vực then chốt trong đó UMTS sẽ giới thiệu những tăng cường cho các chế độ an ninh GSM.

- Nhận thực tương hỗ: Mạng phục vụ được nhận thực tới các thuê bao di động cũng như thuê bao di động được nhận thực tới mạng.
- Tăng sự hỗ trợ cho anh ninh và mật mã dữ liệu trong mạng lõi.
- Tăng độ dài khoá để chống lại các cuộc tấn công mạnh: Như được biết, các thuật toán mật mã số liệu GSM thế hệ hai có độ dài khoá hiệu quả chỉ 40 bít và người ta nghĩ có thể bị phá vỡ gần như trong thời gian thực. Các khoá cho mật mã số liệu trong UMTS sẽ là 128 bít.
- Tính an toàn nhận dạng người sử dụng sẽ được tăng cường thông qua việc sử dụng khoá nhóm.
- Các thuật toán mật mã UMTS cơ bản sẽ được thực hiện công khai có quan tâm đến các phê bình thường xuyên về GSM.
- Sự hỗ trợ cho tính toàn vẹn cũng như tính an toàn sẽ được cung cấp.

Một khái niệm quan trọng trong lĩnh nhận thực thuê bao cho UMTS là mạng khách quan tâm được trả phí hơn là về việc nhận dạng người sử dụng. Vì vậy một sự nhấn mạnh về mối quan tâm của mạng khách là việc trao quyền để cung cấp các dịch vụ hơn là việc nhận thực. Các hệ thống thực hiện việc nhận thuê bao nhấn mạnh sự tương tác giữa thuê bao di động và mạng nhà, với các thông tin trao quyền được truyền tới mạng mà sẽ cung cấp các dịch vụ tới thuê bao di động (mạng khách). Theo cách này, nhận thực có thể được thực hiện mà không phải đàm phán về tính tin cậy nhận dạng thuê bao.

3.3. Các lĩnh vực an ninh của UMTS

Một mục tiêu mức cao cho việc thiết kế kiến trúc an ninh cho UMTS là để tạo một cơ cấu tổ chức có thể phát triển theo thời gian. Như trong trường hợp thiết kế mạng Internet, một phương pháp quan trọng đã modul hoá kiến trúc an ninh bằng cách tạo ra một tập các tầng và sau đó liên kết một tập các phần tử cùng với các mục tiêu thực hiện và thiết kế hệ thống tới những tầng này. Những modul này được người thiết kế gọi là các "domain" (miền) và hiện thời sẽ có năm domain:

3.3.1 An ninh truy nhập mạng (Network Access Security)

Một số các đặc điểm an ninh cung cấp cho người sử dụng sự truy nhập an toàn tới cấu trúc cơ sở hạ tầng UMTS và các đặc điểm bảo vệ người sử dụng chống lại các cuộc tấn công trên các tuyến vô tuyến không dây cho các mạng mặt đất. Các phần tử then chốt bao gồm:

- *Tính tin cậy nhận dạng người sử dụng:* IMUI và các thông tin nhận dạng cố định khác liên quan đến người sử dụng không được phơi bày cho những kẻ nghe lén.
- *Nhận thực tương hỗ:* Cả đầu cuối di động và trạm gốc của mạng phục vụ được nhận thực đối với nhau, ngăn ngừa các cuốc tấn công mạo nhận trên cả hai phía của phiên truyền thông.
- *Tính tin cậy của số liệu báo hiệu và số liệu người sử dụng:* Thông qua mật mã mạnh mẽ, cả nội dung của phiên truyền thông thuê bao lẫn thông tin báo hiệu liên quan được bảo vệ trong khi truyền dẫn qua đoạn nối vô tuyến.

- *Toàn vẹn số liệu và nhận thực khởi đầu:* Thực thể nhận trong một phiên truyền thông có thể xác nhận rằng các bản tin nhận được không bị thay đổi khi truyền và rằng nó thực sự được khởi đầu từ phía được yêu cầu.

3.3.2 An ninh miền mạng (Network Domain Security)

Tập các đặc điểm an ninh cho phép các node trong cơ sở hạ tầng mạng của nhà cung cấp trao đổi các dữ liệu với sự đảm bảo an ninh và bảo vệ chống lại sự xâm nhập trái phép cơ sở hạ tầng mạng hữu tuyến.

- *Nhận thực phần tử mạng:* Khả năng của các thành phần cơ sở hạ tầng mạng bao gồm những khả năng thuộc về các nhà cung cấp dịch vụ khác nhau nhận thực nhau và dữ liệu nhạy cảm được trao đổi.
- *Tính tin cậy của dữ liệu được trao đổi:* Việc bảo vệ dữ liệu được trao đổi giữa các phần tử mạng khỏi các cuộc nghe lén. Điều này điển hình sẽ được thực hiện thông qua mật mã.
- *Toàn vẹn dữ liệu và nhận thực ban đầu:* Điều này là song song với các khía cạnh toàn vẹn dữ liệu và nhận thực ban đầu của An ninh truy nhập mạng nhưng áp dụng đối với mối quan hệ giữa các phần tử mạng. Khi một phần tử mạng truyền dữ liệu đến phần tử khác, node nhận có thể xác nhận rằng dữ liệu không bị thay đổi khi truyền, và nó thực sự khởi đầu với phần tử mạng được thông báo như nguồn gốc khởi đầu. Thêm nữa, những tính chất này phải áp dụng qua các mạng của các nhà cung cấp dịch vụ khác nhau.

3.3.3 An ninh miền người sử dụng (User Domain Security)

Tập các đặc điểm an ninh gắn vào sự tương tác giữa một người sử dụng và máy cầm tay UMTS của họ. Một mục tiêu quan trọng trong miền này là tối thiểu thiệt hại và gian lận có thể xảy ra khi một máy cầm tay bị đánh cắp.

- *Nhận thực User-to-USIM:* Nhận thực trong miền con này gắn vào mối quan hệ giữa một thuê bao riêng và thẻ thông minh SIM trong máy cầm tay UMTS của họ. Để giới hạn sự hoạt động đối với chủ sở hữu hoặc một nhóm cá nhân có

quyền, người sử dụng có thể cần cung cấp PIN để khởi tạo một phiên truyền thông.

- *Đoạn nối USIM-Terminal:* Vì thẻ thông minh trợ giúp USIM (được gắn trong thẻ thông minh) có thể di chuyển được, nên cũng cần thiết để bảo vệ an toàn mối quan hệ giữa USIM và máy cầm tay UMTS. Điển hình điều này sẽ được thực hiện thông qua một sự nhúng bí mật dùng chung trong cả USIM lẫn đầu cuối bởi các nhà cung cấp dịch vụ khi dịch vụ được khởi tạo. Đoạn nối USIM-Terminal ngăn ngừa thẻ USIM của người sử dụng không bị chèn vào trong máy cầm tay khác và bị sử dụng khi không có quyền.

3.3.4 An ninh miền ứng dụng (Application Domain Security)

Các đặc điểm an ninh cho phép sự trao đổi an toàn các bản tin ở mức ứng dụng giữa máy cầm tay và hệ thống của nhà cung cấp dịch vụ thứ ba. Trong kiến trúc UMTS, việc cung cấp cần được thực hiện cho các nhà vận hành mạng hoặc các nhà cung cấp dịch vụ khác tạo ra các ứng dụng nằm trong USIM hoặc trong tổ hợp.

- *Nhắn tin an toàn:* Nhắn tin an toàn sẽ cung cấp một kênh an toàn cho việc truyền các bản tin giữa USIM và server mạng.

- *Tính tin cậy lưu lượng người sử dụng trên toàn mạng:* Việc bảo vệ các bản tin khỏi các cuộc nghe lén - điển hình là thông qua mật mã – trên các đoạn mạng hữu tuyến cũng như vô tuyến của toàn bộ kiến trúc hạ tầng mạng.

3.4.5 Tính cấu hình và tính rõ ràng của an ninh (Visibility and Configurability)

Tập các tính năng qua đó người sử dụng hệ thống có thể biết các đặc điểm an ninh nào đang hoạt động và điều khiển các dịch vụ nào đang được sử dụng đưa ra một tập nhất định các dịch vụ an ninh.

- *Tính rõ ràng:* Người sử dụng hệ thống thông qua các cơ chế được cung cấp bởi cơ sở hạ tầng UMTS có thể xác định được đặc điểm an ninh nào đang hoạt động tại bất kỳ điểm nào theo thời gian và mức độ an ninh là gì.

- *Tính định hình:* Người sử dụng thông qua cơ chế được cung cấp bởi cơ sở hạ tầng UMTS có thể yêu cầu tập các dịch vụ an ninh nào phải đang hoạt động trước khi người sử dụng một dịch vụ nhất định. Chẳng hạn, logic này có thể áp dụng cho *enable* và *disable* việc sử dụng mã PIN cá nhân với USIM trong máy cầm tay của ai đó hoặc áp dụng cho việc quyết định như việc chấp nhận các cuộc gọi đến mà không được mật mã.

Chia toàn bộ lĩnh vực an ninh thành các miền theo kiểu này có một vài ưu điểm. Thứ nhất, nó xử lý bằng cách chia nhỏ toàn bộ không gian vấn đề thành các miền con rời rạc (hơn nữa, quan tâm nhiều đến độ phức tạp được xử lý như thế nào trong môi quan hệ với các giao thức liên mạng Internet). Ngoài ra, bằng việc tạo ra các modul an ninh với các giao diện được biết rõ để có thể cập nhật hoặc thay thế các thành phần của kiến trúc an ninh mà không phải làm lại toàn bộ việc kinh doanh.

Chú ý: Các từ dưới đây được sử dụng cho các miền anh ninh UMTS trong **hình 3.1**.

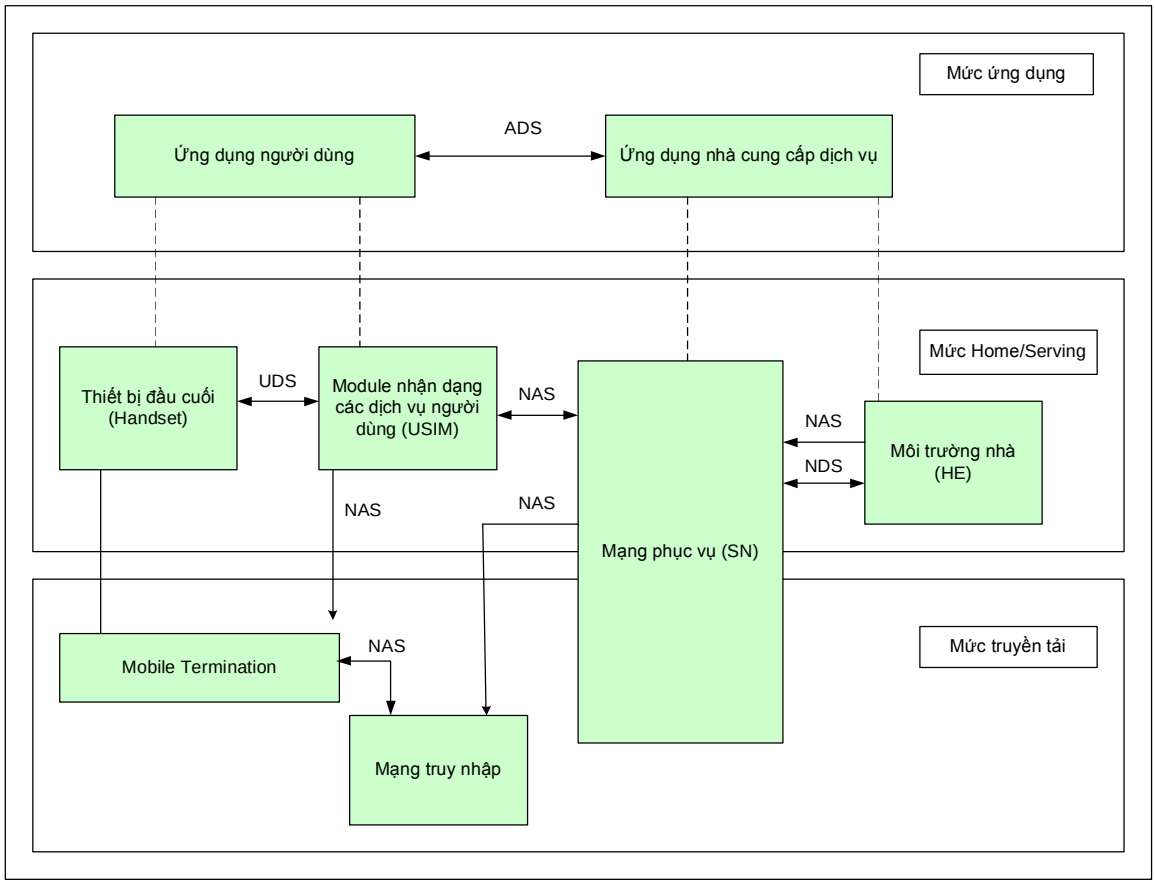
NAS: Network Access Security

NDS: Network Domain Security

UDS: User Domain Security

ADS: Application Domain Security

Hình 3.1 cung cấp sự minh hoạ về toàn bộ môi trường UMTS với chỉ thị về nơi mà năm miền an ninh định trú trong sự tương tác giữa các phần tử khác nhau của môi trường.



Hình 3.1: Sơ đồ minh hoạ nơi năm miền an ninh UMTS định trú trong các mối quan hệ giữa các thành phần của toàn bộ môi trường mạng UMTS. [Nguồn: S. Putz]

3.4. Nhận thực thuê bao UMTS trong pha nghiên cứu

Như đã chú ý trên đây trong chương này, kiến trúc an ninh UMTS đã xuất phát chủ yếu từ các dự án được tài trợ bởi Cộng đồng Châu âu và vài quốc gia thành viên của nó. Phần này quan tâm đến các giao thức nhận thực thuê bao được phát triển khá sớm trong quá trình phát triển UMTS thông qua dự án ASPeCT (Advanced Security for Personal Communications) theo chương trình ACT.

Dự án ASPeCT đã nghiên cứu nhiều phương pháp nhận thực thuê bao trong UMTS, với các báo cáo ban đầu được đệ trình vào 2-1996. Các báo cáo này có thể được xem như mang tính chất khám phá; nó nhấn mạnh vào việc tiếp nhận các giao thức nhận thực thuê bao đã được đề xuất từ các tổ chức quan tâm và sau đó phân tích các giao thức này áp dụng vào các yêu cầu UMTS. Tháng 2-1996 báo cáo ASPeCT đã mô tả các đề

xuất cho nhận thực thuê bao và tạo khoá phiên trong UMTS được đệ trình bởi Royal Holloway, Siemens và KPN.

Đề xuất của Royal Holloway dựa trên cơ chế yêu cầu-đáp ứng (Challenge-Response) tương tự với cơ chế trong GSM. Giao thức này đưa ra nhận thực tương hỗ giữa trạm di động và trạm gốc mạng và tăng cường an ninh định vị người sử dụng (an ninh định vị người sử dụng được thực hiện bằng cách chỉ sử dụng bộ nhận dạng người sử dụng hiện thời và tránh sự truyền dẫn của bộ nhận dạng vĩnh cửu của thuê bao di động trong clear-text qua đoạn nối vô tuyến). Hai giao thức được đề xuất khác của Siemens và KPN là rất khác nhau trong đó chúng bắt nguồn từ các kỹ thuật khoá công cộng. Các phần dưới đây mô tả phương pháp được đề xuất bởi Siemens.

3.4.1 Mô tả giao thức khoá công cộng của Siemens cho UMTS

Giao thức dựa trên khoá công cộng cho nhận thực và tạo khoá phiên được đề xuất bởi Siemens sử dụng nhiều nhóm trường hữu hạn hoặc các phân nhóm đường cong elíp như phương pháp khoá công cộng cơ sở. Trong cả hai trường hợp, an ninh mật mã phụ thuộc vào việc vấn đề thuật toán rời rạc khó khăn hay không. Giao thức do Siemens đề xuất yêu cầu CA tin cậy và một Certification Server (CA) an toàn mà có thể tạo các chứng nhận chứa các khoá công cộng khả dụng đối với cả thuê bao và nhà vận hành mạng và phù hợp với các phương pháp cơ sở hạ tầng khoá công cộng cổ điển. Một phần khác của cơ sở hạ tầng là một danh sách thu hồi ("revocation list") ghi lại các bộ nhận dạng thuê bao, người không còn đủ tư cách nhận dịch vụ.

Đề xuất của Siemens thực sự có ba phần, đó là các giao thức con được định rõ A, B và C. Ba giao thức này đề cập các trường hợp hơi khác nhau:

- *Sub-protocol A:* xử lý trường hợp nơi mà các bản copy được nhận thực của khoá công cộng trạm di động và mạng phục vụ đã khả dụng trong server mạng phục vụ và máy di động tương ứng và vì vậy không cần thiết phải trao đổi trong phiên truyền thông.

- *Sub-protocol B:* xử lý các trường hợp nơi mà chứng chỉ có giá trị của khoá xác nhận công cộng trạm di động là khả dụng trong máy cầm tay di động nhưng không phải trên server mạng phục vụ, và một chứng nhận có giá trị khoá thoả thuận công cộng của người vận hành mạng nhưng không phải trong máy cầm tay di động.
- *Sub-protocol C:* xử lý trường hợp nơi không có bản copy được nhận thực khoá công cộng của thuê bao di động khả dụng trên server mạng phục vụ và không có bản copy được nhận thực khoá công cộng của nhà vận hành mạng trong máy cầm tay di động.

Trong thảo luận này, chúng ta sẽ quan tâm đến Sub-protocol C, vì điều này đưa ra cái nhìn tốt nhất tới các khía cạnh giao thức khoá công cộng và cơ sở hạ tầng liên quan đến đề xuất của Siemens.

3.4.2 Các điều kiện tiên quyết để thực hiện giao thức Siemens

Để Sub-protocol C do Siemens đề xuất cho nhận thực thuê bao làm việc hiệu quả, một số các điều kiện tiên quyết phải được thực hiện. Đáng chú ý trong số này là:

- Việc nhận dạng người vận hành mạng trên mạng phục vụ được biết trước đối với trạm di động.
- Người vận hành mạng phục vụ giữ các khoá thoả thuận công cộng s và g^s.
- Trạm di động sở hữu hệ thống chữ ký bất đối xứng với khả năng chuyển đổi chữ ký bí mật Sig_u.
- CS giữ danh sách thu hồi (revocation list) mới nhất đối với các khoá công cộng của người vận hành mạng và các thuê bao di động.
- Cả CS và server của người vận hành mạng phục vụ có thể tạo và xác nhận tem thời gian (time-stamp).
- Cả server của người vận hành mạng phục vụ và trạm di động giữ khoá công cộng của CS. Khoá này cần thiết để xác nhận tính hợp lệ của các vé được phát hành bởi CS.

- CS khống chế cặp khoá private-public gồm khoá riêng u và khoá công cộng g^s.
- Trạm di động giữ một bản copy có giá trị khoá công cộng g của CS.
- CS sở hữu khoá xác nhận công cộng PK_NO cần để xác nhận các chữ ký được tạo bởi server của người vận hành mạng phục vụ bằng cách sử dụng khoá chữ ký riêng SK_NO.

3.4.3 Hoạt động của Sub-protocol C của Siemens

Sub-protocol C bao gồm sự trao đổi năm pha các bản tin giữa trạm di động (máy cầm tay của thuê bao), server của người vận hành mạng phục vụ và CS. CS truy nhập tới khoá công cộng được cấp phép cho trạm di động. Một khía cạnh cốt yếu của giao thức này là trong khi người vận hành mạng đệ trình một chứng nhận chứa khoá công cộng của nó tới trạm di động, trạm di động không cần thiết phải đệ trình một chứng nhận tương đương tới server của mạng phục vụ. Người vận hành mạng có thể tìm các thông tin cần thiết thông qua CS.

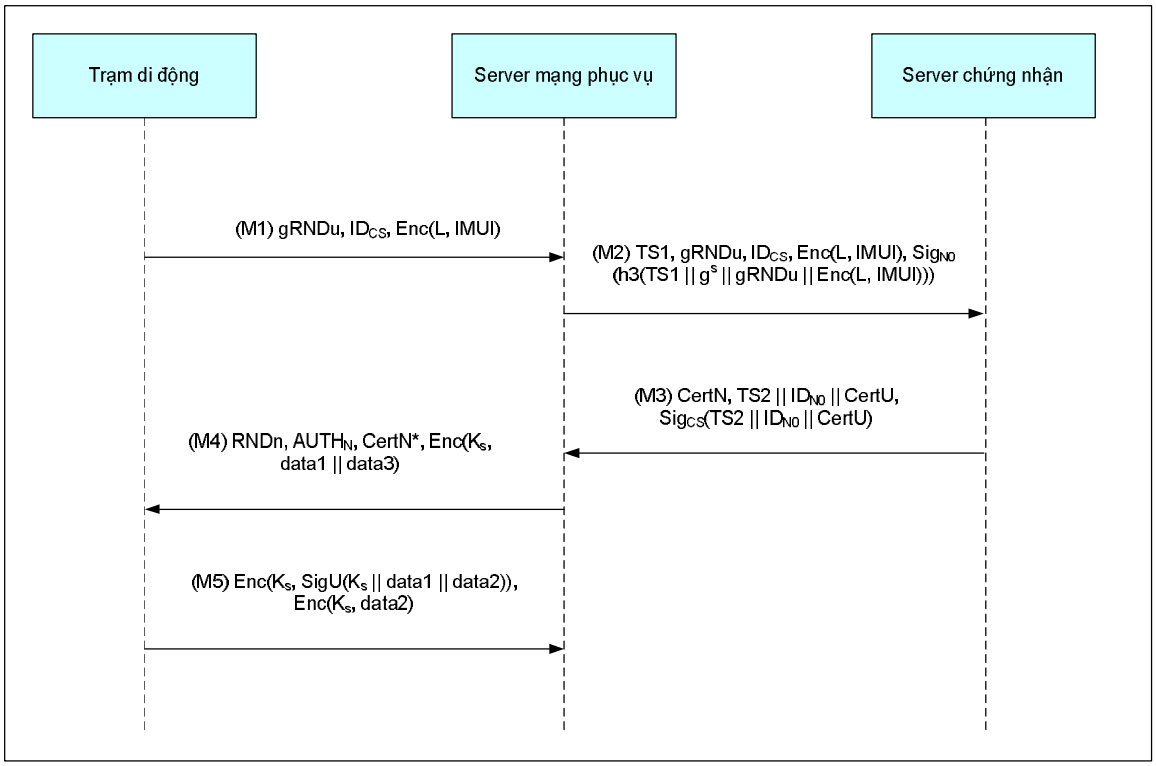
Sub-protocol của Siemens được trình bày như **hình 3.2**. Đây là tổng quan về các bước:

- Trạm di động khởi tạo phiên truyền thông. Đầu tiên nó tạo một số ngẫu nhiên g(RNDU). Sau đó trạm di động tính toán, (1) L=gu(RNDU), bằng cách sử dụng khoá công cộng gu của CS, và (2) chuỗi mật mã Enc(L, IMUI) trong đó IMUI là bộ nhận dạng duy nhất (Bộ nhận dạng người sử dụng di động quốc tế: International Mobile User Identifier) của trạm di động.
- Trạm di động gửi g(RNDU), ID_{CS} và Enc(L, IMUI) tới server của nhà vận hành mạng. Chú ý rằng ID_{CS} là bộ nhận dạng của CS trong đó khoá công cộng của trạm di động có thể được bảo vệ (nó có thể thuộc về nhà cung cấp dịch vụ nhà của thuê bao di động). Điều này cấu thành Bản tin 1 (Message 1).
- Server của nhà vận hành mạng lấy lại khoá công cộng của nó g_s và tạo một nhãn thời gian TS1. Server sau đó sử dụng hàm băm (hash function) h3 cùng với thuật

toán chữ ký SigNO và khoá riêng của nó SK_NO để ký chuỗi (TS1||gs|| |g(RNDU) || Enc(L,IMUI)|).

- Server của nhà vận hành mạng gửi chuỗi dưới đây qua mạng vô tuyến tới CS: TS1, gs, g(RNDU), Enc(L, IMUI), SigNO(h3(TS1 || gs || g(RNDU) || Enc(L, IMUI))). Điều này cấu thành Bản tin 2 (Message 2).
- CS: (1) sử dụng thuật toán xác nhận VerNO và khoá công cộng của nhà vận hành mạng PK_NO để xác nhận bản tin; (2) kiểm tra tem thời gian T1; (3) tính L bằng cách sử dụng khoá công cộng của thuê bao di động, L = (g(RNDU)u); (4) giải mật mã Enc(L, IMUI) bằng cách sử dụng thuật toán giải mật mã Dec và khoá L; (5) lấy lại CertU, chứng nhận cho thuê bao di động từ cơ sở dữ liệu thuê bao của nó; (6) kiểm tra khoá công cộng gs của nhà vận hành mạng và chứng nhận của thuê bao CertU dựa vào revocation lists; (7) tạo một chứng nhận CertN bằng cách sử dụng khoá công cộng của nhà vận hành mạng và ký chứng nhận này; (8) tạo tem thời gian TS1; và (9) tính toán một chữ ký trên chuỗi TS||IDNO||CertU. CertN bao gồm SigCS(H3(credentials)), trong đó credentials là g(RNDU), gs, ID_{NO} và data3. Data3 là một tuỳ chọn.
- CS gửi một bản tin gồm CertN, TS2 || ID_{NO} || CertU, SigCS(TS2 || ID_{NO} || CertU) tới server của nhà vận hành mạng. Điều này cấu thành Bản tin 3.
- Server của nhà vận hành mạng sử dụng thuật toán xác nhận VerCS và khoá công cộng của CS PK_CS để xác nhận Bản tin 3. Sau đó Server của nhà vận hành mạng: (1) tính toán một CertN được rút gọn được gọi là $CertN^*$, $CertN^*$ bao gồm gs || SigCS(h3 (credentials)); (2) tính chuỗi ngẫu nhiên (g(RNDU)s) bằng cách sử dụng khoá riêng của nó; (3) tạo khoá phiên Ks, trong đó Ks = h1(g(RNDU)s || RNDN); (4) tạo khoá nhận thực AUTHN = h2(Ks), trong đó h2 là một hàm băm thứ 2; và (5) tạo chuỗi mật mã Enc(Ks, data1 || data3), trong đó data1 là một nonce được tạo bởi server của nhà vận hành mạng.

- Server của nhà vận hành mạng gửi tới trạm di động qua đoạn nối vô tuyến RNDN, AUTHN, CertN* và Enc(Ks, data1, data3). Điều này cấu thành Bản tin 4 (Message 4).
- Trạm di động bây giờ làm công việc xác nhận việc truyền dẫn và tạo các phần tử dữ liệu mà nó cần để tiếp tục phiên truyền thông. Đầu tiên trạm di động sử dụng thuật toán xác nhận VerCS và khoá công cộng của CS để xác nhận chữ ký trên CertN và xây dựng lại credentials. Trạm di động sau đó tính: (1) gs(RNDU) bằng cách sử dụng khoá công cộng của nhà vận hành mạng; (2) khoá phiên Ks trong đó Ks bây giờ bằng h1(gs(RNDU) || RNDN); (3) khoá nhận thực AUTHN, trong đó AUTHN = h2(Ks); và (4) chuỗi data1 || data3 bằng cách sử dụng thuật toán giải mật mã Dec và khóa phiên Ks. Bằng cách sử dụng thuật toán mật mã Enc với khoá phiên đóng vai trò input, trạm di động sau đó tạo: (1) Enc(Ks, SigU(h3(Ks || data1 || data2))), và (2) Enc(Ks, data2).
- Trạm di động gửi Enc(Ks, SigU(h3(Ks || data1|| data2))) và Enc(Ks, data2) trở lại server của nhà vận hành mạng qua đoạn nối vô tuyến. Việc truyền dẫn này cấu thành Bản tin 5 (Message 5) là bản tin cuối cùng trong quá trình trao đổi giao thức Siemens.
- Server của nhà vận hành mạng sau đó thực hiện một vài tính toán và so sánh cuối cùng để hoàn thành quá trình nhận thực và khởi tạo phiên truyền thông. Đầu tiên, server của nhà vận hành mạng sử dụng khoá phiên Ks để giải mật mã tất cả các phần của bản tin nhận được từ trạm di động. Khi server biết Ks, data1 và data2 nó tiếp tục tính toán h3(Ks || data1 || data2) theo quyền hạn riêng của nó. Sau đó nó sử dụng thuật toán xác nhận VerU và khoá công cộng của trạm di động PK_U để lấy ra h3(Ks || data1 || data2) từ SigU(h3(Ks, data1, data2)). Server so sánh giá trị tính toán được với giá trị vừa lấy ra. Nếu hai giá trị giống nhau thì trạm di động được nhận thực.



Hình 3.2: Sơ đồ minh hoạ sự trao đổi các bản tin trong giao thức nhận thực của Siemens cho UMTS, Sub-protocol C.

Một trong số các tiện lợi của Sub-protocol C được xác nhận bởi các nhà nghiên cứu ASPeCT Project là duy trì tính tin cậy nhận dạng người sử dụng: IMUI chỉ được gửi dưới dạng mật mã từ khi bắt đầu giao thức. Cũng quan trọng không kém là việc sử dụng các tem thời gian để đảm bảo tính hiện thời của các chứng nhận, và để cản trở các tấn công. Cũng đáng chú ý các trường như data1, data2 và data3 - được nhận dạng trong mô tả ở trên như là các nonce – có thể được tạo ra để đóng vai trò kép và thực sự truyền thông tin giữa CS, server mạng và trạm di động.

3.4.4 Đánh giá giao thức nhận thực Siemens

Chúng ta đã rõ ràng từ mô tả Sub-protocol C trong phương pháp Siemens cho nhận thực thuê bao và tạo khoá phiên, điều này là rất khác so với những gì chúng ta thấy trong mạng thế hệ hai. Đề xuất của Siemens dựa trên kiến trúc an ninh khoá công cộng đang phát triển mạnh, bao gồm một CS được quản lý bởi CA tin cậy. Phương pháp này bao gồm các chứng nhận số cho cả các thuê bao di động lẫn nhà vận hành mạng cùng với việc

sử dụng chữ ký số và các thuật toán băm. Các giao thức được đề xuất này là phức tạp nhưng sẽ cung cấp mức an ninh cao và tính mở rộng nếu được triển khai cụ thể một cách đầy đủ.

Như chúng ta sẽ thấy, đây không phải là phương pháp nhận thực thuê bao mà các nhà thiết kế chọn như là nền tảng thực sự cho việc thực hiện hệ thống. Mặc dù các lý do không hoàn toàn rõ ràng, một khả năng là đề xuất của Siemens khởi đầu hoàn toàn từ sự kế thừa cơ sở hạ tầng GSM làm cho sự hoạt động liên đới với thế hệ hai một cách khó khăn. Cũng là sự thật rằng các báo cáo của ASPeCT Project là không nhiều khi mô tả về mật mã thực sự, các giao thức chữ ký số, các thuật toán xác nhận và băm được sử dụng làm cho việc mô phỏng hiệu năng hệ thống khó khăn hơn.

3.5 Nhận thực thuê bao trong việc thực hiện UMTS

Vì thời điểm để thực hiện các hệ thống truyền thông vô tuyến sử dụng công nghệ UMTS đã đến, các nhóm làm việc 3GPP đã chuyển sự tập trung ra khỏi nghiên cứu lí thuyết đã được mô tả trong phần trước. Trong việc ra quyết định cụ thể liên quan đến nhận thực thuê bao trong UMTS, các nhà hoạch định 3GPP đã chọn sử dụng sơ đồ giống với nhận thực GSM nhất với các tăng cường có lựa chọn. Giao thức UMTS này sử dụng một phương pháp dựa trên khoá công cộng đối xứng trong đó Trung tâm nhận thực của mạng nhà thuê bao và thẻ thông minh USIM trong máy cầm tay của người sử dụng dùng chung một khoá bí mật.

Ngoài ra vì nhận thực bây giờ được hoạch định cho việc thực hiện trong UMTS nên nó khác với nhận thực trong thế hệ hai một vài điểm quan trọng sau:

(1) Modul nhận dạng thuê bao (SIM hoặc trong mạng UMTS là USIM) trong máy cầm tay và Trung tâm nhận thực (AuC) dùng chung một số chuỗi cũng như khoá bí mật. Số chuỗi không phải là một giá trị cố định mà thay đổi theo thời gian.

(2) Ngoài nhận thực thuê bao chuẩn, trạm gốc của mạng khách được nhận thực đối với trạm di động như là một phần của giao thức nhận thực.

(3) Trong pha nhận thực, UMTS thiết lập một khoá phiên cho mật mã dữ liệu trong phiên truyền thông và một khoá thứ 2 để thực hiện đảm bảo toàn vẹn dữ liệu.

(4) Các thuật toán mật mã của UMTS sẽ được đặt tại domain công cộng để phê bình và phân tích.

Những bước chính trong giao thức UMTS để nhận thực tương hỗ và thiết lập khoá phiên như sau. Sự song song với giao thức challenge-response của GSM nên biết rõ ràng. (Thuật ngữ đang được sử dụng để mô tả các phần tử then chốt của cơ sở hạ tầng và các giao thức nhận thực UMTS khác về một vài khía cạnh so với những gì chúng ta đã thấy trong GSM – Chúng ta sẽ dành sự phân biệt này trong mô tả dưới đây).

(1) Node phục vụ (SN: Serving Node) giữ Bộ ghi định vị tạm trú VLR (Visitor Location Register) yêu cầu dữ liệu nhận thực từ Môi trường nhà (HE) mà hỗ trợ Bộ ghi định vị thường trú (HLR) và Trung tâm nhận thực (AuC).

(2) Môi trường nhà gửi một mảng các véctơ nhận thực (AV) tới SN. Mỗi véctơ như thế có thể được sử dụng để thực hiện thoả thuận khoá phiên và nhận thực giữa SN và USIM trong trạm di động. Mỗi AV (tương ứng với bộ ba của GSM) bao gồm: (1) một số ngẫu nhiên challenge RAND; (2) một response mong muốn cho challenge, XRES; (3) một khoá phiên mật mã CK; (4) một khoá toàn vẹn dữ liệu IK; và (5) một thẻ nhận thực AUTN.

(3) Mạng phục vụ gửi challenge ngẫu nhiên RAND và thẻ nhận thực AUTN tới trạm di động qua đoạn nối vô tuyến.

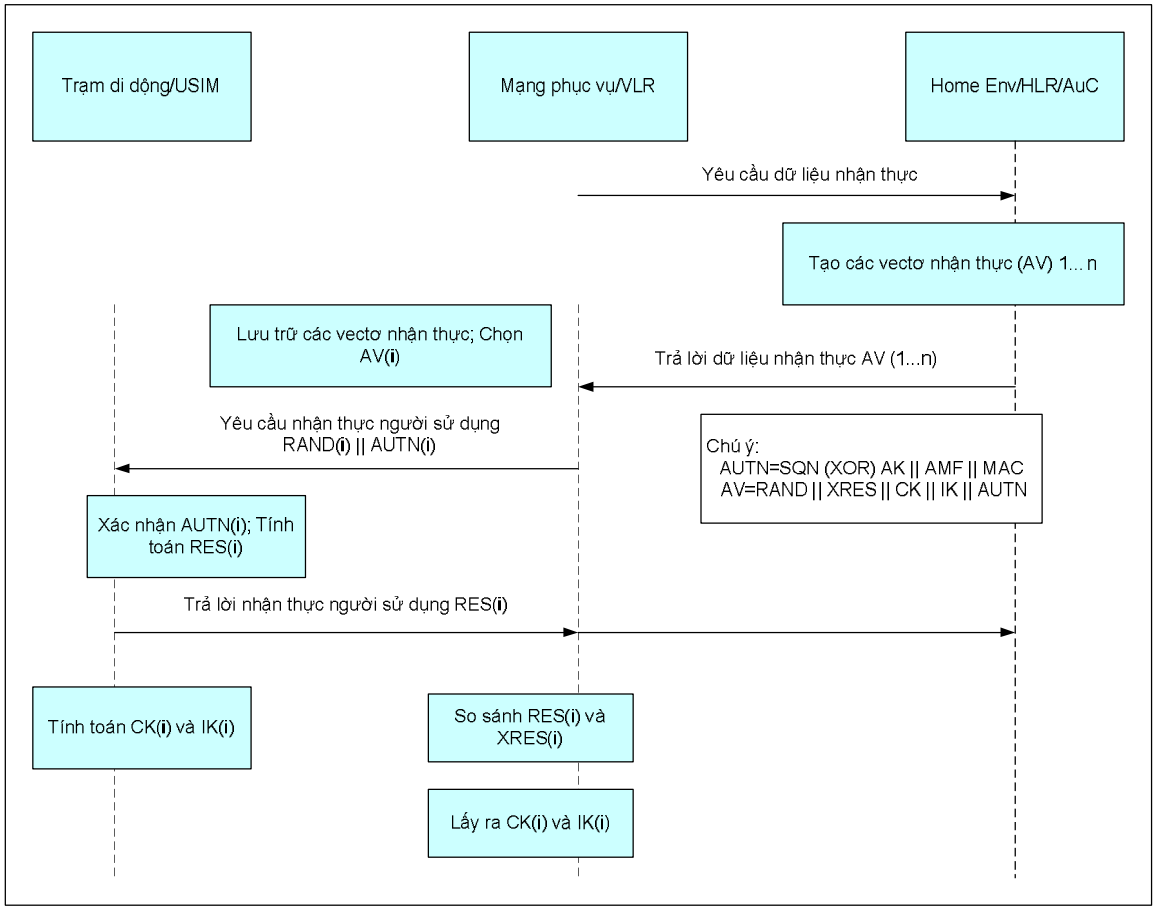
(4) USIM trong trạm di động xác nhận rằng AUTN là có thể chấp nhận được (vì vậy thực hiện nhận thực đối với trạm di động). Khi đó trạm di động tạo một response, RES tới challenge ngẫu nhiên và truyền trở lại SN.

(5) USIM tính toán phiên bản CK và IK riêng của nó bằng cách sử dụng RAND, số chuỗi (được nhúng trong AUTN) và khoá bí mật của nó.

(6) Mạng phục vụ so sánh RES mà nó đã nhận được từ trạm di động với XRES. Nếu hai giá trị trùng nhau thì trạm di động được nhận thực.

(7) USIM và SN truyền CK tới các thành phần của hệ thống chịu trách nhiệm về mật mã dữ liệu được truyền, và IK tới các thành phần của hệ thống chịu trách nhiệm về kiểm tra tính toàn vẹn dữ liệu.

Sơ đồ của giao thức nhận thực UMTS cơ sở xem **hình 3.3.**

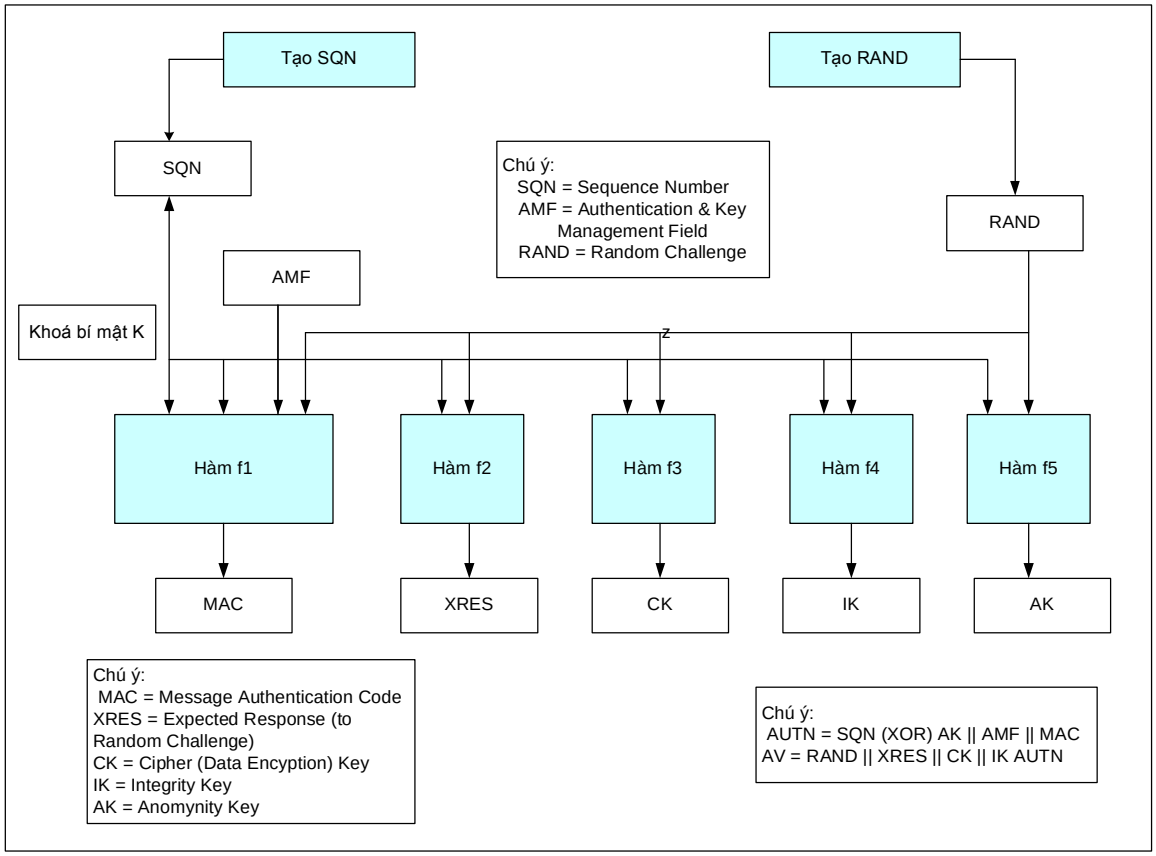


Hình 3.3: Luồng các bản tin trong giao thức tạo khoá phiên và nhận thực UMTS cơ sở. [Lấy từ J.Salva]

Trong giao thức nhận thực như được mô tả ở trên, các thẻ nhận thực AUTN là một phần tử dữ liệu then chốt. AUTN bao gồm: (1) Số chuỗi (Sequence Number), SQN, thực hiện phép hoặc loại trừ (XORed) với một khoá "nặc danh" AK, (2) Trường quản lý khoá và nhận thực, AMF (Authentication and Key Management Field), và (3) một Mã nhận thực bản tin, MAC (Message Authentication Code). Mục đích của khoá nặc danh là để che đậy Sequence Number mà nếu bị tiết lộ có thể cung cấp các thông tin về nhận dạng và

vị trí của thuê bao. AMF có thể mang những thông tin từ Trung tâm nhận thực tới trạm di động về các vấn đề như sử dụng các thuật toán tạo khoá và nhận thực. Nó cũng hướng dẫn trạm di động sử dụng một khoá trong số các khóa bí mật.

Giao thức nhận thực UMTS sử dụng năm hàm một chiều (one-way) được ký hiệu từ f1 đến f5 để tạo các giá trị thành phần của chuỗi AUTN và AV. Các đầu vào cho các hàm này là khoá bí mật của thuê bao, challenge số ngẫu nhiên RAND và Sequence Number. **Hình 3.4** cung cấp một sơ đồ về cách giao thức này hoạt động trong Trung tâm nhận thực.



Hình 3.4: Tạo chuỗi Véctơ nhận thực UMTS và Thẻ nhận thực (AUTN) trong Trung tâm nhận thực. [lấy từ J.Salva]

3.6 Tổng kết về nhận thực trong UMTS

Quá trình thiết lập pha đầu tiên của việc nhận thực UMTS trên các giao thức nhận thực thuê bao là một quá trình lâu dài và phải thực hiện nhiều lần. Như chúng ta đã thấy, một vài công trình nghiên cứu ban đầu đã đảm nhận như là một công trình tiền thân cho UMTS trong các chương trình Châu âu như ACTS đã tập trung vào một giải pháp với một phần tử mạnh các phương pháp mã hoá. Tuy nhiên trong pha thực hiện cuối cùng việc bắt buộc phải xây dựng trên các thành tựu GSM hiện có và duy trì tính liên thông với GSM được chứng minh là áp đảo. Một lần nữa các phương pháp khoá công cộng đối xứng lại chiến thắng. Tuy nhiên kiến trúc khoá công cộng cuả UMTS quan tâm đến nhiều thiếu sót của hệ thống tổ ong thế hệ hai, bao gồm việc nhận thực của mạng đối với trạm di động, nhận dạng người sử dụng và tính tin cậy định vị, tính toàn vẹn dữ liệu và sử dụng các thuật toán mật mã thích hợp.

CHƯƠNG 4: NHẬN THỰC VÀ AN NINH TRONG IP DI ĐỘNG (Mobile IP)

Những người thiết kế mạng điện thoại tổ ong số thế hệ hai và ba đã thảo luận trong các chương đầu tiên của luận văn này đã bắt đầu hỗ trợ truyền thông di động – nghĩa là sau hết là toàn bộ quan điểm về điện thoại tổ ong. Mặt khác Internet ban đầu khởi đầu như là một mạng nhằm kết nối các máy tính tại những vị trí cố định. Theo một số phương diện khác các môi trường cũng khác nhau một cách đáng kể. Chẳng hạn các mạng tổ ong thế hệ hai được thiết kế để truyền chủ yếu là lưu lượng thoại và hỗ trợ các kênh truyền thông giữa các bên trong cuộc thoại thì mạng tổ ong thế hệ ba sẽ quan tâm nhiều hơn đến truyền thông số liệu ngoài lưu lượng thoại. Mặt khác, những người thiết kế Internet đã tìm cách tạo ra một mạng cho việc truyền dẫn số liệu giữa các máy tính ("voice over IP" đã xuất hiện sau) và đã sử dụng chuyển mạch gói hơn là thiết lập các kênh như một mô hình truyền dẫn chính.

Trong những năm 1980, thế giới nơi mà các máy tính đặt trong các phòng máy hoặc trên các bàn của người sử dụng tại những vị trí cố định với địa chỉ mạng cố định đã bắt đầu bị phá vỡ. Trong tương lai các máy tính – bao gồm không chỉ các máy tính xách tay mà còn bao gồm các thiết bị như các PDA (Personal Digital Assistant), "Web pad", và máy điện thoại tổ ong thông minh - sẽ đến với người sử dụng, những người muốn kết nối tới Internet từ bất cứ nơi nào họ xuất hiện tại bất cứ thời điểm nào. Mô hình về cách mà các địa chỉ mạng được chỉnh sửa trong thế giới Internet có dây – thông qua việc can thiệp của các nhà quản trị hệ thống, gán các địa chỉ IP mới và việc cấu hình lại các máy (machine) và cơ sở hạ tầng mạng – không còn được chấp nhận. Một điều gì đó phải được đưa ra để cung cấp sự hỗ trợ cho tính toán di động trong môi trường Internet. Giao thức được phát triển thông qua IETF (Internet Engineering Task Force: Nhóm đặc trách ký thuật Internet) là giao thức Internet di động hay ngắn gọn là Mobile IP. Mục tiêu của Mobile IP là để trợ giúp truy nhập Internet cho các thiết bị tính toán di chuyển từ nơi này

đến nơi khác mà không yêu cầu thay đổi toàn bộ cơ sở hạ tầng Internet ngay lập tức để bao hàm tính di động.

4.1. Tổng quan về Mobile IP

Trong kiến trúc Internet hiện thời, giao thức Internet Version 4 hoặc IPv4, Mobile IP là một tuỳ chọn. Các mạng cố gắng hỗ trợ tính toán di động có thể bổ xung Mobile IP, trong khi đó các mạng chỉ cung cấp các dịch vụ cho các máy tính có dây không cần thay đổi. Trong tương lai, IP Version 6 sẽ hỗ trợ tính di động như một phần của các giao thức Internet chung với sự thừa nhận truy nhập Internet có dây cũng trở nên rất quan trọng.

4.1.1 Các thành phần logic của Mobile IP

Như đã đề cập ở trên, khởi nguồn của IPv4 và các mạng tổ ong số chúng ta đã nghiên cứu trong luận văn này là rất khó khăn. Tuy nhiên ở mức logic các phần tử của kiến trúc Mobile IP rất gần với các khái niệm quen thuộc hiện nay trong mạng tổ ong số. Ví dụ, dưới mobile IP, mỗi thiết bị tính toán di động có một mạng nhà tuy rằng mỗi máy cầm tay tổ ong trong môi trường GSM cũng có một mạng nhà. Trên mạng nhà này, trong thế giới Mobile IP là một hệ thống phần mềm được gọi là "Home Agent" (Tác nhân nhà) chạy trên một node mạng. Chức năng chính của Home Agent là để duy trì các thông tin, bao gồm các khoá mật mã, thuộc về các máy tính di động - được gọi là "Mobile Host" (MH) – Nó coi mạng đó như là mạng nhà của nó. Home Agent cũng bám các vị trí hiện thời của Mobile Host mà nó chịu trách nhiệm và vì vậy tại mức khái niệm nó phù hợp với tổ hợp Bộ ghi định vị thường trú/Trung tâm nhận thực (HLR/AuC) trong GSM. Hơn nữa, mỗi Mobile Host dưới Mobile IP có một địa chỉ logic cố định - địa chỉ giao thức Internet (hay địa chỉ IP) của nó trên mạng nhà – tuy rằng mỗi máy cầm tay GSM có một bộ nhận dạng duy nhất được nhúng trong thẻ thông minh SIM của nó.

Dưới giao thức Mobile IP, khi Mobile Host chuyển vùng ra ngoài miền điều khiển của mạng nhà (dĩ nhiên nó có thể tương tác với mạng nhà của nó nhưng trường hợp này không quan tâm), nó có thể thiết lập một kết nối Internet thông qua mạng con Internet khác có cung cấp hỗ trợ IP. Một mạng con host như thế sẽ có các cổng vô tuyến (các khối

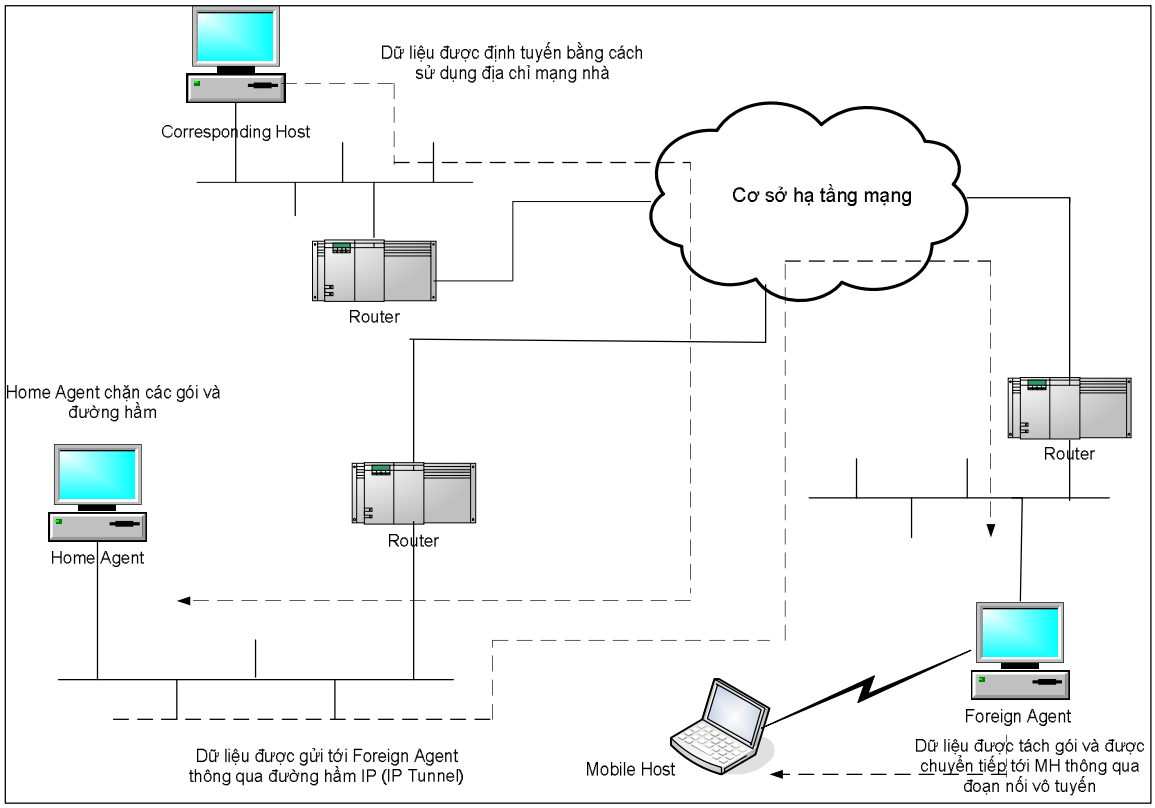
thu/phát vô tuyến) có thể trao đổi các tín hiệu với Mobile Host. Cũng phải có mặt trên mạng host một hệ thống được gọi là một tác nhân khách (FA: Foreign Agent). FA tương tác với Mobile Host trong khi nó được kết nối với mạng host cung cấp các dịch vụ tới nó và thông tin thay mặt nó với HA.

Tóm lại, khi Mobile Host cố gắng thiết lập truyền thông từ mạng host khi nó đang chuyển vùng, đầu tiên nó sẽ khởi tạo truyền thông với FA trên mạng đó. Sau đó nó sẽ truyền một bản tin với cả địa chỉ IP riêng của nó lẫn "Chăm sóc địa chỉ mới của nó" (địa chỉ IP của FA) mà FA chuyển tiếp tới HA. Nhận và xác nhận bản tin này, HA thực hiện "ràng buộc cập nhật" (Binding Update) bằng cách tạo một bảng đầu vào ghi lại các chăm sóc địa chỉ mới cùng với các Mobile Host cụ thể này.

Một thành phần khác trong sơ đồ của Mobile IP là máy đối tác (CA: Corresponding Host). CA có thể là bất kì máy tính nào trên Internet mà cố gắng giao tiếp với Mobile Host. Dưới Mobile IP, CA không cần biết rằng Mobile Host đang chuyển vùng ra khỏi mạng nhà (đây là giả thiết đơn giản hoá quan trọng của Mobile IP) và đơn giản truyền các gói khi truyền thông với MH theo cách thông thường tới mạng nhà. Ở đây HA, biết rằng Mobile Host đang chuyển vùng và Chăm sóc địa chỉ hiện thời của nó, nhận các gói đi về hướng Mobile Host và chuyển tiếp chúng tới FA tại Chăm sóc địa chỉ hiện thời này trong một quá trình được gọi là *"triangular routing"* (định tuyến tay ba). FA sau đó chuyển tiếp các gói tới Mobile Host qua đoạn nối vô tuyến mà chúng đã thiết lập.

Kiến trúc chung của Mobile IP được minh hoạ trong **hình 4.1**.

Chú ý rằng các mạng bao gồm HA và FA cần thiết phải thực hiện Mobile IP và có khả năng hỗ trợ di động. Tuy nhiên, một khía cạnh then chốt của Mobile IP là CA và các thành phần khác của nền tảng Internet được giới thiệu bởi đám mây Internet trong sơ đồ mạng không cần biết gì về giao thức này.



Hình 4.1: Sơ đồ minh hoạ các thành phần then chốt của kiến trúc Mobile IP.

4.1.2 Mobile IP – Nguy cơ về an ninh

Như một sự mở rộng đối với giao thức Internet thông thường (IPv4), Mobile IP, nhằm cung cấp sự hỗ trợ di động cho chuyển vùng host, phát sinh các nguy cơ về an ninh. Trong thực tế hầu hết các nhà phân tích đồng ý rằng những nguy cơ lớn nhất mà Mobile IP gặp phải nằm trong miền an ninh. Như trong trường hợp mạng tổ ong số, các đoạn nối vô tuyến giữa Mobile Host và FA dễ tiếp xúc với việc nghe trộm và tiềm năng tiếp xúc với các cuộc tấn công mạo nhận. Tuy nhiên, không giống như mạng tổ ong truyền thông trong mạng Internet có dây không chạy trên mạng độc quyền của một hay một vài nhà cung cấp dịch vụ thông tin vô tuyến mà trên mạng Internet mở. Vì vậy nguy cơ an ninh trong phần mạng hữu tuyến có lẽ lớn hơn trong mạng tổ ong số.

John Zao và Matt Condell của BBN xác định hai lĩnh vực an ninh cụ thể trong Mobile IP:

– Khả năng một node có hại bắt chước việc nhận dạng node di động và định hướng lại các gói tin đi đến node di động tới các vị trí mạng khác;

– Nguy cơ về các node thù địch tiềm ẩn (đến từ các miền quản trị mạng khác nhau) nhằm tiến hành các cuộc tấn công chủ động/thụ động tới các node khác khi chúng sử dụng chung các tài nguyên mạng và các dịch vụ được đưa ra bởi các mạng con hỗ trợ di động.

Các giao thức nhận thực người sử dụng được thảo luận trong chương này đều quan tâm đến hai nguy cơ an ninh này nhưng thực hiện theo các phương pháp khác nhau.

4.2. Các phần tử nền tảng môi trường nhận thực và an ninh của Mobile IP

Giao thức Mobile IP xác định việc sử dụng Các mã nhận thực bản tin (MAC) - được gọi là "authenticator" (bộ nhận thực) theo cách nói đặc tả nhận thực Mobile IP - để nhận thực và cung cấp tính toàn vẹn dữ liệu cho các bản tin điều khiển được trao đổi giữa Home Agent và Mobile Node. Trong khi MAC không được uỷ nhiệm trong đặc tả Mobile IP thì phương pháp MAC có thể cũng được áp dụng cho các bản tin được trao đổi với các đầu vào khác chẳng hạn như FA. Thuật toán MAC lấy các bản tin được truyền và một khoá bí mật là các input và tạo ra một chuỗi bít có độ dài cố định như là đầu ra. Nếu bộ phát và bộ thu sử dụng chung khoá bí mật này thì bộ thu có thể tạo ra MAC riêng của nó từ bản tin mà nó đã nhận được. Bộ thu sau đó so sánh chuỗi được tạo ra với MAC nhận được với bản tin. Nếu trùng nhau, điều này xác nhận rằng (1) không có ai thay đổi nội dung bản tin khi truyền, và (2) nguồn bản tin phải là các bên mong đợi (trong đó nguồn các bản tin phải biết khoá bí mật để tạo ra một MAC thích hợp). Giao thức Mobile IP xác định MD5, theo mode tiền tố thêm hậu tố (nghĩa là mã MAC được gắn vào cả trước và sau nội dung bản tin) như là thuật toán tạo MAC mặc định. Các thuật toán khác có thể được triển khai theo thoả thuận hai bên của các bên tương ứng.

4.2.1 An ninh IPSec

Một khái niệm nền tảng then chốt trong nhận thực và an ninh cho Mobile IP và khái niệm về liên kết an ninh (SA: Security Association). SA là một mối quan hệ một chiều, được định nghĩa trước giữa người gửi và người nhận định nghĩa phương pháp an ninh nào đối với an ninh Internet được thực hiện trong thông tin từ người gửi đến người nhận, và áp dụng các tham số nào. Trong trường hợp truyền thông song hướng có thể tồn tại hai liên kết an ninh như thế với mỗi liên kết định nghĩa một hướng truyền thông. Các SA định nghĩa tập các dịch vụ IPSec nào (An ninh giao thức Internet) được đưa vào tầng IP hay tầng mạng (Layer 3) trong ngăn xếp giao thức Internet. Trong một gói tin IP, ba tham số được lấy cùng với nhận dạng duy nhất một liên kết an ninh: Đó là địa chỉ đích IP; Bộ nhận dạng giao thức an ninh, nó xác định liên kết an ninh áp dụng cho Authentication Header (AD) hay đối với Encapsulating Security Payload (ESP); và một chuỗi bít được gọi là Chỉ số các tham số an ninh (SPI: Security Parameters Index), nó được liên kết duy nhất với một liên kết an ninh cho trước. Trong một router hoặc các phần tử thích hợp của cơ sở hạ tầng mạng trên một mạng, tại đó có một file được gọi là Cơ sở dữ liệu chính sách an ninh (SPD: Security Policy Database) định nghĩa các qui tắc dựa trên các nội dung các trường này trong gói tin IP. Phụ thuộc vào thiết lập trong trường SPI và vị trí của host đích, các kiểu và mức an ninh khác nhau có thể bị áp đặt vào các gói tin đi ra ngoài. Điều này cho phép các thành phần – Mobile Host, Home Agent, Foreign Agent và trong một số trường hợp cả Corresponding Host – trong một phiên truyền thông Mobile IP chọn chế độ an ninh thích hợp.

4.2.2 Sự cung cấp các khoá đăng ký dưới Mobile IP

Vì một cơ sở hạ tầng như Mobile IP phát triển rất nhanh nên không thể giả sử rằng một Mobile Host (MH) đang chuyển vùng sẽ có bất kỳ liên kết trước nào với FA trên các mạng mà nó tạm trú. Một vấn đề chính là cách cung cấp cho MH và FA các khoá đăng ký chung một cách an toàn khi bắt đầu phiên truyền thông. Toàn bộ các hướng đi trong sự phát triển Mobile IP là để hoàn thành bước này thông qua cơ sở hạ tầng khoá công cộng có thể truy nhập toàn cầu (PKI: Public-Key Infrastructure), nhưng vì kiến trúc này chưa

có tính khả dụng rộng rãi nên vài bước trung gian phải được thực hiện như là một giải pháp chuyển tiếp. Chẳng hạn, Charles Perlins đã đề xuất áp dụng năm kĩ thuật thực hành hiện thời. Các kí thuật này được xem xét theo trật tự ưu tiên bởi MH và FA với kỹ thuật đầu tiên được lựa chọn (có thể được thực hiện bằng nhân công). Năm sự lựa chọn này là:

- Nếu FA và MH đã dùng chung một liên kết an ninh, hoặc có thể thiết lập một liên kết thông qua ISAKMP hoặc SKIP, thì FA tiếp tục chọn khoá đăng ký này.
- Nếu FA và HA của MH dùng chung một liên kết an ninh thì HA có thể tạo một khoá đăng ký và truyền nó tới FA được mật mã với khoá công cộng này.
- Nếu FA có khoá công cộng riêng của nó thì FA có thể yêu cầu HA của MH tạo ra một khoá đăng ký và thông tin nó tới FA được mật mã với khoá công cộng này.
- Nếu MH giữ một khoá công cộng, nó có thể chứa khoá này trong yêu cầu đăng ký của nó, với FA thì tạo một khoá đăng ký và truyền nó tới MH được mật mã với khoá công cộng này.
- FA và MH có thể sử dụng một giao thực trao đổi khoá Diffie-Helman để thiết lập một khoá đăng ký chung.

Lựa chọn Diffie-Helman giả thiết một mức ưu tiên thấp bởi vì độ phức tạp tính toán của nó có thể áp đặt một gánh nặng trên host di động và do đó tạo ra trễ.

Trong hầu hết các kịch bản mà Perkins đề xuất, MH và HA sử dụng chung một liên kết an ninh theo cách suy diễn. Vì vậy, nếu HA và FA sử dụng chung đủ các thông tin mà HA có thể truyền một khoá bí mật tới FA thì HA có thể hoạt động như là một Trung tâm phân phối khoá (KDC: Key Distribution Center). Chẳng hạn nếu HA và FA sử dụng chung một khoá bí mật thông qua một liên kết an ninh giữa chúng thì kỹ thuật dưới đây, sử dụng thuật toán MD5, có thể được sử dụng để truyền một khoá phiên hoặc khoá đăng ký từ HA đến FA.

HA gửi chuỗi dưới đây tới FA:

String1 = MD5(secret||regrep||seret) ⊗ Kr

Trong đó secret là khoá riêng được sử dụng chung giữa HA và FA, Kr là khoá đăng ký đang được truyền thông, và regrep là một reply cho bản tin yêu cầu đăng ký được gửi bởi FA tới HA. Nhận được bản tin này (String1), FA bây giờ có thể tính toán:

String2 = MD5(secret||regrep||secret)

FA sau đó có thể lấy ra khoá đăng ký đơn giản bằng cách thực hiện một toán tử XOR như sau:

Kr = String1 ⊗ String2

Khi vắng mặt một liên kết an ninh được thiết lập giữa HA và FA, một phương pháp tương tự có thể được thực hiện nếu FA có thể tạo ra một khoá công cộng khả dụng.

Trong trường hợp mà FA và Mobile Node sử dụng chung một liên kết an ninh (điều này ít xảy ra hơn trường hợp MN sử dụng chung một khoá bí mật với HA) thì FA và MN có thể đàm phán trực tiếp một khoá đăng ký, mà không cần sử dụng HA như một Trung tâm phân phối khoá. Điều tương tự có thể được hoàn thành nếu MN tạo ra khoá công cộng khả dụng cho FA.

4.3. Giao thức đăng ký Mobile IP cơ sở

Dưới Mobile IP, Khi MH thấy chính nó trong một miền mạng mới, nó phải thiết lập liên lạc với FA cho mạng đó và khởi tạo chuỗi giao thức đăng ký để thông tin cho HA của nó về vị trí hiện thời của nó. Giao thức đăng ký này cấu thành một thành phần nhận thực quan trọng trong thế giới Mobile IP. Nếu MS đang hoạt động trong phạm vi địa lí điều khiển mạng nhà của nó thì dĩ nhiên FA sẽ không hoạt động và truyền thông và nhận

thực sẽ xảy ra trực tiếp giữa MS và HA. Trong mô tả này chúng ta sẽ xem xét các trường hợp chung nhất trong đó MH đang chuyển vùng và FA được yêu cầu trong chuyển giao.

Giao thức đăng ký Mobile IP cung cấp hai cơ chế để chống lại các cuộc tấn công lặp lại (replay): cả các tem thời gian và các nonce đều được hỗ trơ, và các principal trong phiên truyền thông có thể chọn giữa hai biến thể của giao thức này phụ thuộc vào cái nào chúng muốn sử dụng. Trong mô tả ở các phần nhỏ dưới đây, chúng ta sẽ phác thảo giao thức đăng ký Mobile IP với các tem thời gian.

4.3.1 Các phần tử dữ liệu và thuật toán trong giao thức đăng ký Mobile IP

Các phần tử dữ liệu then chốt và các thuật toán trong giao thức đăng ký được định nghĩa bởi đặc tả Mobile IP như sau:

1. **MH_{HM} (Home Address of the Mobile Node):** Địa chỉ IP của MH trên mạng nhà của nó (chú ý rằng điều này sẽ khác với Care of Address trên mạng của FA).
2. **MH_{COA} (Care of Address of the Mobile Node):** Địa chỉ IP của MH trên mạng mà nó đang tạm trú. Trong hầu hết các trường hợp, điều này sẽ tương ứng với địa chỉ IP của FA.
3. **HA_{ID} (Address of Home Agent):** Địa chỉ IP của HA trên mạng nhà của MH.
4. **FA_{ID} (Addresss of Foreign Agent):** địa chỉ IP của FA trên mạng mà MH đang tạm trú.
5. **T_{MH}, T_{HA} (Time Stamps):** T_{MH} và T_{HA} là các tem thời gian được phát hành bởi MH và HA tương ứng.
6. **Enc(K, M):** Mật mã bản tin M theo khoá K.
7. **MAC(K, M):** Tạo một MAC (Message Authentication Code) từ bản tin M theo khoá K.
8. **KS_{MH-HA} (Shared Secret Key):** KS_{MH-HA} là một khoá bí mật được dùng chung

giữa MH và HA. Nó không được dùng chung với FA hoặc các phần tử khác của cơ sở hạ tầng mạng.

9. **Request:** Một mẫu bít chỉ thị rằng các bản tin dưới đây là một bản tin yêu cầu.
10. **Reply:** Một mẫu bít chỉ thị rằng bản tin dưới đây là một bản tin trả lời.
11. **Result:** Một giá trị chỉ thị kết quả của một request được gửi tới HA (tiếp nhận, loại bỏ, giải thích cho sự loại bỏ, v.v…).

Chú ý rằng Khoá bí mật dùng chung là một phần tử của mật mã khoá riêng đã được giữ lại trong thế hệ trợ giúp di động đầu tiên cho Internet. Nó có thể sẽ không cần thiết trong tương lai, nếu cơ sở hạ tầng khoá công cộng trở thành khả dụng.

4.3.2 Hoạt động của Giao thức đăng ký Mobile IP

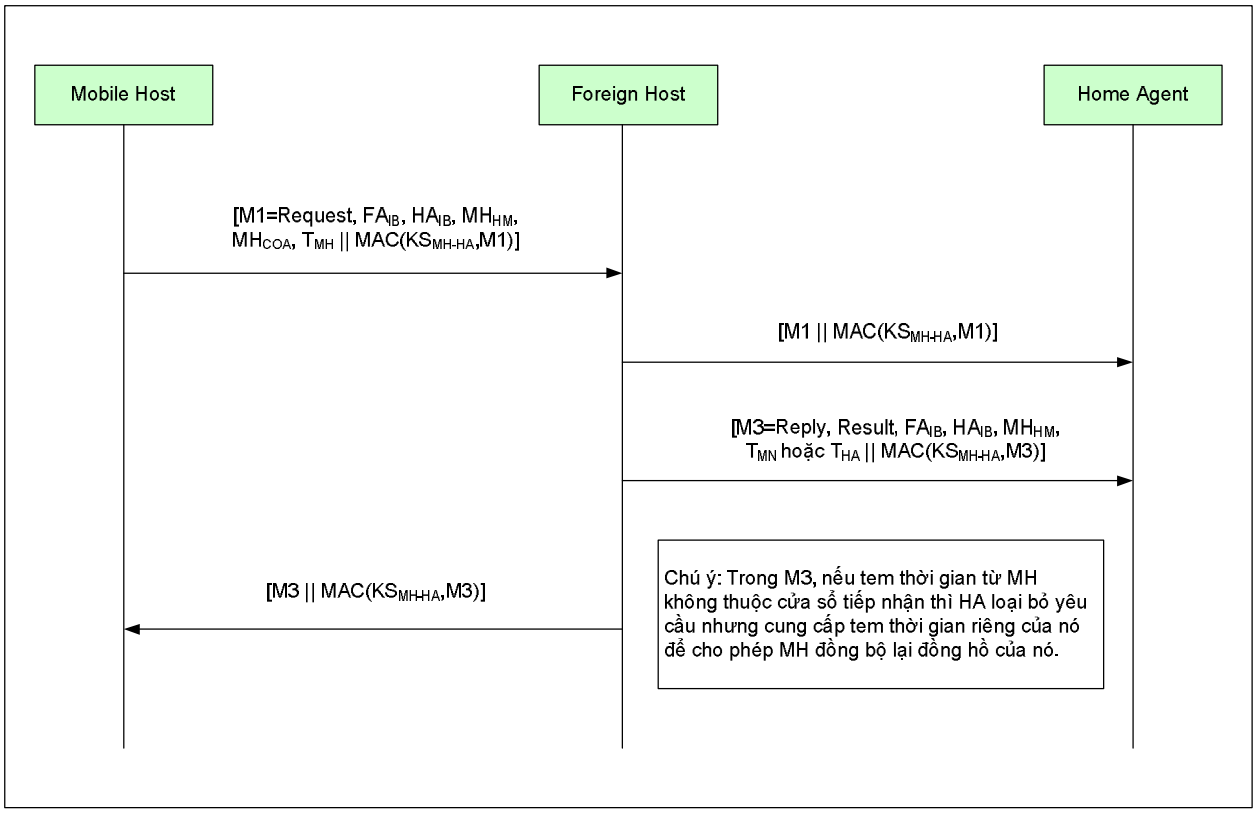
Các bước chính khi thực thi giao thức đăng ký Mobile IP tiến hành như sau:

1. MH sẽ sở hữu một tem thời gian nhận được trước từ HA trên mạng nhà của nó. Điều này trợ giúp trong việc đồng bộ các tem thời gian riêng của nó với các tem thời gian của HA.
2. MH truyền một bản tin yêu cầu tới FA. Bản tin yêu cầu này chứa các phần tử dưới đây: Request Designator, ID của FA (địa chỉ IP của nó), ID của HA, địa chỉ nhà của MH, Care-of-Address của MH, và một tem thời gian được phát hành bởi MH. Chuỗi này được theo sau bởi mã MAC mà MH tạo ra bằng cách áp dụng thuật toán MD5 cho các phần tử trong bản tin yêu cầu cùng với khoá bí mật $KS_{MH\text{-}HA}$ mà nó sử dụng chung với HA.
3. FA chuyển tiếp cả bản tin yêu cầu lẫn MAC tương ứng tới HA. Chú ý rằng các phần tử dữ liệu trong bản tin yêu cầu – không chứa khoá bí mật – đã được truyền đi một cách rõ ràng, vì thế FA có thể đọc địa chỉ của FA.
4. Khi nhận được việc truyền dẫn từ FA, HA tính MAC riêng của nó trên

bản tin yêu cầu của MH. Nếu giá trị tính được phù hợp với MAC nhận được trong truyền dẫn thì MH được nhận thực và nội dung bản tin yêu cầu được xác nhận là không bị thay đổi.

5. HA bây giờ tạo ra một bản tin trả lời chứa các phần tử dữ liệu dưới đây: Reply Designator, Result Code, ID của FA (địa chỉ IP của FA), ID của HA, địa chỉ nhà của MH, và một tem thời gian TS. Tem thời gian này sẽ bằng với tem thời gian được phát hành bởi MH nếu giá trị này nằm trong cửa sổ hiện thời có thể chấp nhận được đối với HA. Mặt khác tem thời gian này sẽ là tem thời gian được thiết lập bởi HA, nhằm cho phép việc tái đồng bộ xảy ra. HA cũng tính toán một MAC trên các phần tử dữ liệu này bằng cách sử dụng khoá bí mật mà nó sử dụng chung với MH và gửi kết quả cùng với bản tin. (Chú ý rằng với các biến thể prefix plus suffix của thuật toán MD5 thì hai phiên bản của MAC được gửi đi thực sự nhưng trong sơ đồ dưới đây điều này bị bỏ qua vì tính đơn giản). HA truyền bản tin trả lời và MAC này đến FA.
6. FA chấp nhận việc truyền dẫn được mô tả trong bước 5 từ HA, và chuyển nó tới MH qua đoạn nối vô tuyến.
7. MH tính toán MAC riêng của nó trên bản tin trả lời và so sánh kết quả với MAC mà nó đã nhận được cùng với bản tin trả lời từ FA. Nếu hai giá trị MAC trùng nhau thì HA được nhận thực tới MH và nội dung bản tin trả lời được xác định hợp lệ.

Tại thời điểm này, MH, FA, HA có thể sử dụng một trong các phương pháp được khuyến nghị bởi Perkins để thiết lập một khoá đăng ký, hoặc khoá phiên mà sẽ được sử dụng để mật mã dữ liệu trong phiên truyền thông này. **Hình 4.2** minh hoạ sự trao đổi các bản tin trong Giao thức đăng ký Mobile IP.



Hình 4.2: Sơ đồ phác thảo sự trao đổi các bản tin trong Giao thức đăng ký Mobile IP. [Lấy từ Sufatrio và Lam]

Chú ý rằng việc thiết lập một khoá đăng ký phải không tiết lộ khoá bí mật dùng chung tới FA, vì điều này sẽ tạo thành một kẽ hở nghiêm trọng về an ninh.. Cũng chú ý rằng, trong khi khoá đăng kí có thể được thiết lập thông qua ứng dụng khoá công cộng, nếu cơ sở hạ tầng khoá công cộng đang trong trạng thái hoạt động thì nó cũng có thể được thiết lập bằng các lựa chọn nghĩa là không yêu cầu PKI.

4.4 Mối quan tâm về an ninh trong Mobile Host - Truyền thông Mobile Host

Hầu hết mọi sự thảo luận về giao thức Mobile IP tập trung vào truyền thông giữa Corresponding Host (CS) và Mobile Host với một giả định ngầm rằng CH nằm ở một vị trí cố định trong Internet. Dĩ nhiên, truy nhập Internet không dây phát triển, kịch bản mà trong đó hai MH, cả hai chuyển vùng tự do, cố gắng truyền thông đang trở nên ngày một quan trọng. Trong một bài viết năm 1998 được trình bày tại hội nghị Glocom năm 1998,

Alessandra Giovanardi và Gianluca Mazzini đã đề xuất các giao thức nhằm tối ưu hiệu năng truyền thông trong MH - Kịch bản MH.

Vấn đề trong truyền thông giữa hai MH theo giao thức Mobile IP là vấn đề "định tuyến tay ba" (triangular routing) phát triển nhanh. Trong trường hợp mà CH cố định cố gắng thông tin với một MH đang chuyển vùng, đầu tiên nó sẽ gửi các gói tin của nó tới tới mạng nhà của MH, nơi mà chúng bị chặn bởi HA. HA sau đó chuyển tiếp các gói tin này tới vị trí hiện thời MH (sự gián tiếp này được gọi là định tuyến tay ba). Các gói tin đã được truyền theo hướng khác, mặc dù đầu tiên chúng phải được gửi qua đoạn nối vô tuyến từ MH tới FA, có thể di chuyển trực tiếp tới CH (CH có địa chỉ IP cố định). Tuy nhiên với hai MH các gói di chuyển theo hai hướng đầu tiên được gửi tới các mạng nhà của các MH tương ứng để định tuyến tay ba trở thành định tuyến hai hướng.

Để giải quyết vấn đề định tuyến tay ba này, Giovanardi và Mazzini đã đề xuất việc sử dụng tác nhân ngoài (EA: External Agent). EA phát triển sự hiểu biết về vị trí hiện thời của hai MH và các FA tương ứng của chúng. Một đường hầm an toàn sau đó có thể được thiết lập nên các tuyến giữa hai FA này, vì vậy loại bỏ được định tuyến tay ba hai hướng.

Theo sơ đồ truyền thông MH-to-MH này, Giovanardi và Mazzini đã chỉ ra rằng cần thiết các cơ chế an ninh bảo vệ chống lại cả các MH gian lận lẫn các thực thể mà nặc danh cơ sở hạ tầng mạng nhằm sắp xếp các đường hầm an toàn giữa các FA. Các tác giả đã đề xuất một chế độ an ninh bao gồm năm phần tử hay các mức độ như sau:

1. **Tích hợp địa chỉ IP và địa chỉ MAC:** Khi tiến hành nhận thực các MH thông qua HA, một địa chỉ được tạo ra là sự tích hợp của địa chỉ IP và địa chỉ MAC (Media Access Control) của MH được sử dụng hơn là chỉ sử dụng chỉ địa IP. Vì địa chỉ MAC là một chuỗi bít duy nhất được nhúng trong phần cứng hoặc phần sụn nên nó khó sửa đổi và bắt chước hơn địa chỉ IP dựa trên phần mềm. Vì vậy HA duy trì một bộ nhớ cache chứa cặp địa chỉ IP/MAC được sử dụng trong nhận thực các MH.
2. **Hashing các địa chỉ MAC:** Để đảm bảo hơn nữa việc chống lại việc chặn các thông tin địa chỉ, FA áp dụng các hàm băm một chiều tới địa chỉ MAC của MH và gửi đi

giá trị này hơn là chính địa chỉ MAC tới HA cùng với địa chỉ IP của MH. HA sau đó có thể sử dụng địa chỉ IP mà nó nhận được để tham chiếu bảng các cặp địa chỉ IP/MAC của nó, lấy ra địa chỉ MAC mong muốn, và áp dụng thuật toán băm đối với MAC này. Nếu giá trị kết quả trùng với giá trị băm nhận được từ FA thì MH được nhận thực.

3. **Sở hữu khoá công cộng dùng chung:** Khái niệm ở đây là tất cả các hệ thống tác nhân trong cộng đồng xác định dùng chung một khoá bí mật. Khi truyền dẫn các bản tin giữa các agent, một hàm băm được áp dụng tới tổ hợp bản tin này, hoặc một phần của bản tin và một khoá bí mật. Agent nhận sau đó có thể tạo giá trị băm riêng của nó và xác nhận rằng bản tin khởi đầu từ một node sở hữu khoá bí mật này.
4. **Sử dụng các tem thời gian:** Để ngăn chặn các cuộc tấn công, các nhãn thời gian được chứa trong bản tin điều khiển dù bản tin được nhận thực hay không. Hệ thống nhận đánh giá nhãn thời gian trong bản tin và tiếp nhận các bản tin này nếu tem này rơi vào cửa sổ xác định. Giao thức này yêu cầu vài mức đồng bộ thời gian giữa các agent, được thực hiện thông qua việc sử dụng RFC 1305 NTP.
5. **Sử dụng mã khoá thông điệp:** Theo giao thức con này, khoá bí mật dùng chung có thể được sử dụng để mật mã các bản tin điều khiển trong trạng thái toàn vẹn và một mã khoá thông điệp sau đó được tạo ra được gắn vào bản tin. Điều này giúp đảm bảo cả tính tin cậy và toàn vẹn các bản tin được trao đổi giữa các hệ thống agent.

Nên chú ý rằng những đề xuất của Giovanardi và Mazzini trong phần này quan tâm chủ yếu đến an ninh và nhận thực vì nó áp dụng cho sự tương tác giữa các HA, FA và External Agent trong tương tác Mobile IP. Cũng quan trọng để thực hiện các bước bảo vệ đoạn nối thông tin vô tuyến giữa MH và FA.

4.5. Phương pháp lai cho nhận thực theo giao thức Mobile IP

Nhận thực theo giao thức đăng ký cơ sở trong Mobile IP được trình bày ở trên cần thiết phải giữ lại một phương pháp dựa trên khoá công cộng. Nó đã bị phê bình là không có tính mở rộng đối với những môi trường trong đó nhiều tổ chức quản lý muốn tương tác

và muốn các MH của họ tận dụng các dịch vụ thông qua các mạng được quản lý bởi các tổ chức khác. Trong một tài liệu năm 1999, Sufatrio và Kwok Yan Lam đã đề xuất một khoá riêng lai, một phương pháp khoá công cộng cho nhận thực theo Mobile IP được thiết kế để giải quyết vấn đề tính mở rộng mà không phải thay đổi căn bản sự trao đổi bản tin trong giao thức đăng ký Mobile IP. Điều này được thực hiện bằng cách cho phép HA đóng vai trò cả agent nhận thực khoá công cộng và Trung tâm phân phối khoá (KDC) cho các khoá phiên. Sufatrio và Lam chứng minh rằng đây là sự lựa chọn có ý nghĩa cho cơ sở hạ tầng khoá công cộng (PKI) đang phát triển mạnh, trong đó MH và HA điển hình thuộc về cùng một tổ chức.

4.5.1 Các phần tử dữ liệu trong Giao thức nhận thực Sufatrio/Lam

Các phần tử dữ liệu chính được sử dụng trong Giao thức nhận Sufatrio/Lam như sau:

- **CA (Certification Authority: Chính quyền chứng nhận):** CA chịu trách nhiệm về việc phát hành các chứng nhận (certificate) trong cơ sở hạ tầng khoá công cộng được đề xuất (PKI).
- **HA_{ID}, FA_{ID} (Các bộ nhận dạng của HA và FA):** HA và FA được nhận dạng bởi các địa chỉ IP tương ứng của chúng.
- **MH_{HM} (Địa chỉ nhà của MH):** Địa chỉ nhà của MH bao gồm địa chỉ IP trên mạng nhà của nó.
- **MH_{COA} (Care-of-Address của MH):** Chăm sóc địa chỉ hiện thời của MH được tạo thành bởi địa chỉ mạng của FA.
- **N_{MH}, N_{HA}, N_{FA} (Nonces):** Các Nonce được phát hành bởi MH, HA, và FA tương ứng.
- **T_{MH}, T_{HA} (Time Stamps):** Các tem thời gian được tạo bởi MH và HA tương ứng.

- **KS_{HA-MH} (Symmetric Private Key: Khoá riêng đối xứng):** Một khoá đối xứng được dùng chung giữa HA và MH.
- **KR_{HA}, KR_{FA}, KR_{CA} (Private Keys: Các khoá riêng):** Các khoá riêng trong các cặp khoá riêng/khoá công cộng thuộc các cặp khoá không đối xứng của HA, FA và CA tương ứng.
- **KU_{HA}, KU_{FA}, KU_{CA} (Public Keys: Các khoá công cộng):** Các khoá công cộng trong các cặp khoá riêng/khoá công cộng thuộc các cặp khoá bất đối xứng của HA, FA và CA tương ứng.
- **$Cert_{HA}$, $Cert_{FA}$ (Certificates: Các chứng nhận):** Các chứng nhận số của HA và FA tương ứng.
- **Request, Reply, Advert (Message-Type Codes: Mã kiểu bản tin):** Chuỗi bít chỉ thị các kiểu bản tin yêu cầu, trả lời và quảng cáo tương ứng.
- **Sig (K, Mx) (Digital Signature: Chữ ký số):** Một chữ ký số được tạo bằng cách áp dụng khoá K đối với bản tin Mx.
- **MAC(K, Mx) (Message Authentication Code: Mã nhận thực bản tin):** Một MAC được tạo bằng cách áp dụng khoá K tới bản tin Mx.

4.5.2 Hoạt động của giao thức nhận thực Sufatrio/Lam

Giao thức nhận thực dựa trên khoá công cộng tối thiểu được đề xuất bởi Sufatrio và Lam năm 1999 liên quan đến sự trao đổi bản tin dưới đây giữa MH, FA và HA.

- FA làm cho MH biết được sự khả dụng của nó thông qua việc truyền dẫn bản tin "quảng cáo agen." Quảng cáo agent bao gồm chứng nhận của FA và một chuỗi bản tin M1 bao gồm một mã chỉ thị rằng đây là một bản tin quảng cáo agent, địa chỉ IP của FA, và Care-of-Address mà sẽ được gán cho MH. FA cũng gắn một chữ ký số được tạo ra bằng cách áp dụng khoá riêng KR_{FA} của cặp khoá riêng/khoá công

cộng của nó vào bản tin M1.

- MH trả lời bằng cách gửi trở lại FA chuỗi bản tin M2. M2 bao gồm một mã chỉ thị một yêu cầu dịch vụ, địa chỉ IP của FA, địa chỉ IP của HA của MH, địa chỉ nhà của MH, COD của HM (vừa nhận được từ FA), một nonce được tạo bởi HA, một nonce được tạo bởi MH, và một phiên bản của bản tin M1 nhận được trong bước trước. MH ký bản tin này với khoá bí mật KS_{MH-HM}, khoá này được sử dụng chung với HA của nó.
- FA nhận bản tin M2 và chuyển tiếp nó tới HA của MH, gắn một nonce của riêng nó.
- HA đầu tiên đánh giá tính hợp lệ của chữ ký trên bản tin M2, bằng cách sử dụng phiên bản của khoá bí mật dùng chung của nó KS_{MH-HA}. HA xác nhận rằng các địa chỉ IP cho các FA được xác định trong sự trùng khớp bản tin M1 và bản tin M2 và sau đó đánh giá tính hợp lệ của chứng nhận của FA thông qua khả năng của nó như một trung tâm nhận thực khoá công cộng. HA sau đó cũng có thể đánh giá tính hợp lệ của chữ ký số của FA trên bản tin M1, đã lấy ra khoá công cộng KU_{FA} từ chứng nhận của FA.
- HA gửi trở lại FA chứng nhận của nó, $Cert_{HA}$ cùng với một chuỗi bản tin M4. M4 chứa một mã chỉ thị rằng đây là một reply đăng ký, một mã chỉ chị kết quả yêu cầu đăng ký, địa chỉ IP của FA, địa chỉ IP của HA, địa chỉ nhà của MH, một nonce được tạo bởi HA, và một nonce được tạo trước bởi MH. Một chữ ký số được tạo với khoá bí mật được dùng chung bởi HA và MH được gắn vào chuỗi M4, và nonce được gửi bởi FA sau đó được gắn vào chuỗi này, cấu thành bản tin M3. Đến lượt HA ký M3 bằng cách sử dụng khoá riêng từ cặp khoá riêng/khoá công cộng của nó.
- Khi nhận được bản tin này từ HA, FA đảm nhận các bước dưới đây: (1) đánh giá tính hợp lệ phiên bản nonce của nó N_{FA} nhận được từ HA; (2) đánh giá tính hợp lệ của chữ ký số trên bản tin M3, bằng cách sử dụng khoá công cộng của HA; và (3)

tạo một đầu vào bản ghi với bản tin này mà sau đó đóng vai trò như một bằng chứng rằng nó đã cung cấp dịch vụ tới MH. FA cũng lấy ra bản tin M4, như được mô tả trong bước 5 ở trên từ toàn bộ quá trình truyền dẫn nó đã nhận được từ HA.

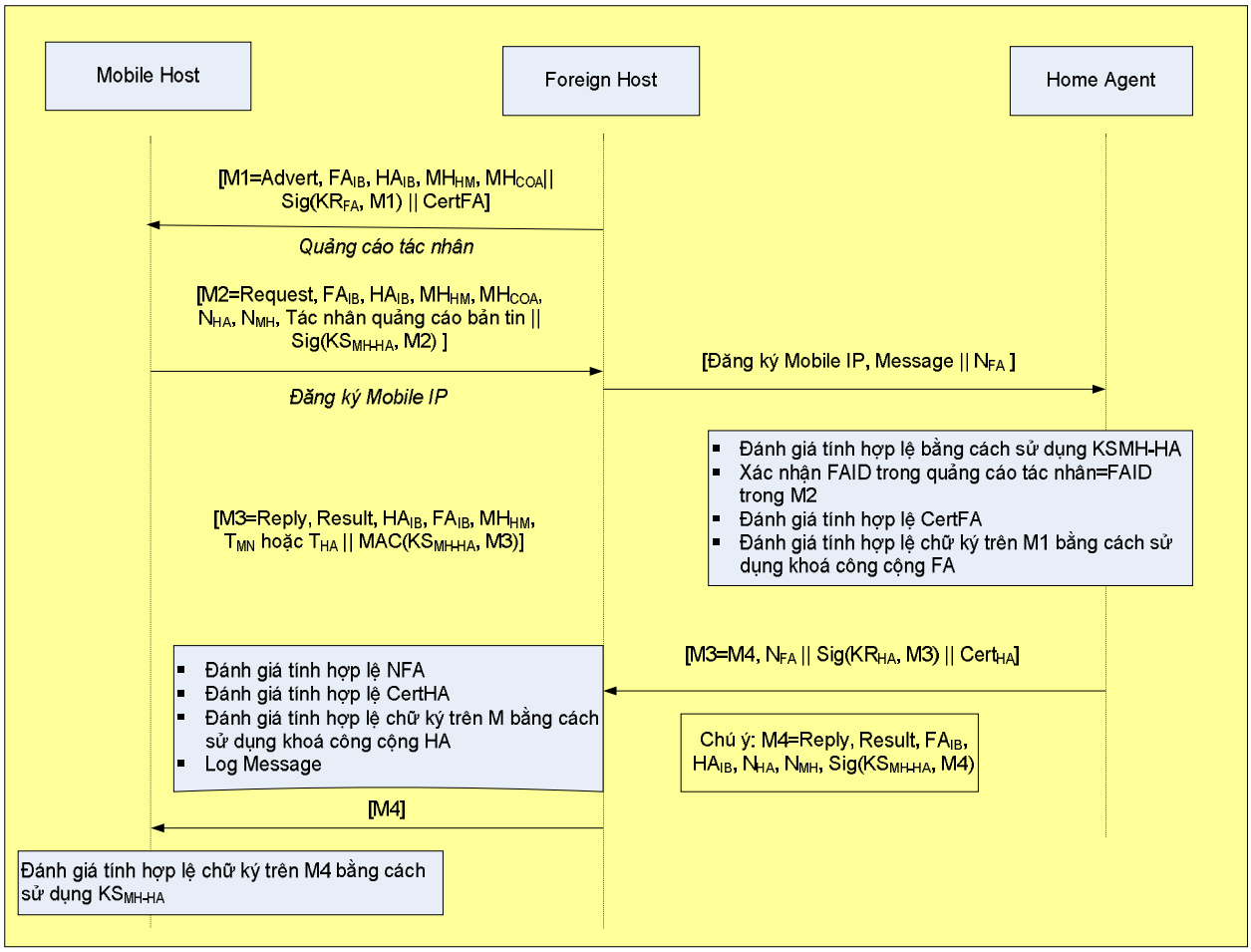
- FA sau đó chuyển bản tin M4 tới MH qua đoạn nối vô tuyến.
- MH sử dụng khoá bí mật KS_{MH-HA} để đánh giá tính hợp lệ chữ ký trên bản tin M4 (Điều này làm cho giao thức Sufatrio/Lam trở thành một thiết kế lai khoá riêng và khoá công cộng).

Ba thực thể HA, FA và MH bây giờ được nhận thực tới nhau và có thể tiếp tục phiên truyền thông của chúng. Sơ đồ hoạt động của giao thức Sufatrio/Lam xem hình 4.3.

Thực tế, MH không nhận thực FA một cách trực tiếp nhưng có thể đảm bảo rằng HA đã làm như vậy khi nó nhận được bản tin M4 và đánh giá tính hợp lệ của chữ ký trên bản tin này. Chữ ký này lấy từ một bí mật mà chỉ này MH dùng chung với HA. Theo giao thức Sufatrio/Lam, MH không phải thực hiện đánh giá chứng nhận hoặc kiểm tra các revocation list, vì vậy giảm gánh nặng xử lý và truyền thông trên khối di động.

4.6. Hệ thống MoIPS: Mobile IP với một cơ sở hạ tầng khoá công cộng đầy đủ

Khi truy nhập Internet phát triển ngày càng mạnh và khi có thêm nhiều tổ chức vận hành mạng mà chứa các MH hoặc muốn cung cấp các dịch vụ thông tin qua cơ sở hạ tầng Mobile IP thì cơ sở hạ tầng khoá công cộng (PKI) trở nên hấp dẫn hơn. Việc tạo ra một cơ sở hạ tầng PKI như thế cho tính toán di động là một trở ngại khó vượt qua. Tuy nhiên nghiên cứu được tiến hành bởi John Zao và các đồng nghiệp tại BBN Technology và các tổ chức cộng tác trong thiết kế và thực hiện hệ thống MoIPS (Mobile IP Security) đã cung cấp một kiến trúc mẫu cho một cơ sở hạ tầng như thế và hé mở về an ninh Mobile IP có thể thực hiện như thế nào trong tương lai.



Hình 4.3: Sơ đồ minh hoạ hoạt động của giao thức Sufatrio/Lam cho nhận thực trong môi trường Mobile IP. [Lấy từ Sufatrio và Lam]

4.6.1 Tổng quan về hệ thống MoIPS

Như được thiết kế bởi Zao và những người khác, như mục tiêu của nó, hệ thống MoIPS có các dịch vụ an ninh phân phối sau: (1) nhận thực các bản tin điều khiển Mobile IP trong cập nhật vị trí, (2) áp dụng điều khiển truy nhập qua các MH muốn sử dụng các tài nguyên trong mạng khách, và (3) cung cấp các đường hầm an ninh cho các gói tin IP được định hướng lại.

- **Nhận thực trong quá trình cập nhật vị trí:** MoIPS hỗ trợ cả giao thức Mobile IP cơ bản lẫn cái được gọi là Mobile IP định tuyến tối ưu hoá. Theo Mobile IP định tuyến tối ưu hoá, CS mà cung cấp hỗ trợ di động có thể được thông báo về vị trí hiện thời của MH mà chúng muốn truyền thông, vì vậy loại bỏ sự quanh co của định

tuyến tay bao thông qua mạng nhà. Nguy cơ an ninh là các cuộc tấn công định hướng lại lưu lượng xa, trong đó một kẻ mạo danh chỉ dẫn CH chuyển tiếp các gói tin tới một vị trí khác vị trí mà MH đang cư trú hiện thời. Theo MoIPS, mỗi đăng ký Mobile IP và cập nhật ràng buộc (là sự thay đổi của bản tin vị trí được chuyển đến CH) bao gồm một đuôi nhận dạng 64-bit (identification tag) để ngăn chặn các cuộc tấn công và một hoặc nhiều phần mở rộng nhận thực (authentication extension) cung cấp tính toàn vẹn dữ liệu và nhận thực ban đầu thông qua việc sử dụng MAC được tạo bởi hàm băm. MoIPS cũng cung cấp các cặp khoá mật mã cho việc sử dụng giữa MH và FA, giữa FA và HA, và giữa MH và Corresponding Agent.

- **Điều khiển truy nhập cho các Mobile Host:** Theo kiến trúc MoIPS, cả các node đầu cuối (như MH và CH) và các tác nhân hỗ trợ di động (HA và FA) giữ các chứng nhận X.509 chứa các tham số khoá công cộng cũng như các thông tin về nhận dạng và sự sáp nhập các thực thể. Các chứng nhận được phát hành thông qua các phân cấp CA theo cách bị ràng buộc bởi chuẩn X.509. Một FA có thể sử dụng chứng nhận của một MH để nhận thực MH, và thành công của quá trình nhận thực được bao hàm khi FA chuyển tiếp một yêu cầu đăng ký từ MH đến HA. Tuy nhiên quyền sử dụng tài nguyên mạng liên quan đến việc kiểm tra các trạng thái của MH mà xảy ra trong quá trình nhận thực (chẳng hạn, kiểm tra liệu người sở hữu MH có phải đang trả hoá đơn không). Chỉ có HA tiến hành kiểm tra trạng thái này. Một sự kiểm tra thành công và vì vậy quyền sử dụng các tài nguyên mạng được yêu cầu là được phép nếu HA gửi lại trả lời tới FA.

- **Đường hầm an ninh các gói tin IP (Secure Tunneling of IP Packets):** Trong thế giới Mobile IP, các gói dữ liệu di chuyển giữa các Mobile Node, FA, HA và CS (mà như chúng ta thấy có thể là MH) đi qua Internet rộng lớn và không được bảo vệ, và ít nhất một phần truyền dẫn của chúng đi qua một đoạn nối vô tuyến. Các bước phải được thực hiện để bảo vệ các gói tin chống lại các cuộc nghe trộm và sự sửa đổi các gói tin. Kiến trúc hệ thống MoIPS xác định rằng HA và FA chịu trách nhiệm về việc đảm bảo rằng tất cả việc truyền thông với MH sử dụng các đường hầm an ninh cho

tính toàn vẹn dữ liệu, nhận thực khởi đầu và khi cần có cả tính tin cậy dữ liệu. MoIPS xác định việc sử dụng kiểu xuyên đường hầm giao thức an ninh đóng gói (ESP: Encapsulation Security Protocol) của IPSec như là phương pháp để thực hiện các mục tiêu an ninh này. Các bên truyền thông đàm phán các cơ chế bảo mật và mật mã được sử dụng trong cơ cấu tổ chức ESP, nhưng tất cả các gói sẽ được đóng gói trong một header IPSec và một header IP mở rộng mà nhận dạng các điểm đầu cuối của đường hầm. Để thực hiện điều này, MoIPS chứa một module hệ thống hỗ trợ IPSec và ISAKMP (Internet Security Association and Key Management Protocol).

So với các giao thức nhận thực chúng ta đã nghiên cứu trong các chương trước cho các mạng tổ ong số thì MoIPS có sự khởi đầu rõ ràng hơn trong thế giới giao thức Internet ngược với các giao thức độc quyền của các mạng truyền thông tổ ong. Cũng rõ ràng hơn là sự phụ thuộc vào mật mã khoá công cộng và các phần tử của PKA, bao gồm các chứng nhận số và một tập các CA liên quan với nhau.

4.6.2 Các đặc tính chính của kiến trúc an ninh MoIPS

MoIPS cung cấp một ví dụ tốt nhất về phương pháp khoá công cộng chúng ta gặp phải đối với an ninh và nhận thực trong môi trường Mobile IP. Vì vậy cần xác định một vài thành phần then chốt của kiến trúc an ninh này.

1. Như chúng ta đã thấy, tại mức giao thức Internet, MoIPS áp dụng biến thể ESP của IPSec và ISAKMP cùng với Mobile IP. Các mở rộng định tuyến tối ưu tới Mobile IP được trợ giúp.

2. Đối với các chứng nhận số khoá công cộng, MoIPS sử dụng đặc tả X.509 Version 3 với danh sách chứng nhận revocation Version 2 (CRL: Certificate Revocation List). Đối với kho chứa chứng nhận, những người thiết kế của MoIPS sử dụng hệ thống tên miền (DNS: Domain Name System) Internet chuẩn. Theo các tác giả, phương pháp này có vài ưu điểm: (1) sử dụng hệ thống DNS được biết rõ và được sử dụng rộng rãi giúp giải quyết vấn đề phát hiện server; (2) các chứng nhận công cộng loại bỏ yêu cầu về truyền dẫn thời gian thực các khoá, vì sẽ cần thiết với một cơ sở hạ tầng của trung tâm phân phối khoá (KDC: Key Distribution Center), vì có

thể thực hiện với Kerberos; và (3) yêu cầu về phương pháp có tính mở rộng cao: "chúng ta phải có một công nghệ có thể thiết lập các bí mật được chia sẻ giữa một số lớn các node trải rộng nhiều miền Internet"

3. Phân cấp CA theo MoIPS giả định một kiến trúc nhiều cây. Mỗi cây trong cấu trúc có một CA đỉnh (TLCA: Top-Level CA), các CA ở các mức giữa (MLCA: Middle-Level CA) hoặc mức 0, và một tầng các CA mức thấp hơn. Các CA mức thấp hơn chịu trách nhiệm về một khối các địa chỉ kề nhau và phát hành các chứng nhận MoIPS tới các thực thể Mobile IP mà có các địa chỉ IP rơi vào phạm vi đó (chẳng hạn, tất cả các node trên một mạng cho trước sẽ có khả năng được phục vụ bởi cùng một CA). Việc xác nhận chéo được cho phép giữa các TLCA và các MLCA.

4. Việc tham gia vào MoIPS yêu cầu việc sở hữu một chứng nhận. Mỗi thực thể muốn tham gia vào trong các phiên truyền thông trong môi trường MoIPS – dù là MH, FA, HA hay CH có khả năng nhận biết tính di động - phải đảm bảo an toàn một chứng nhận X.509 V3 với một profile cụ thể được xác định cho MoIPS. Các chứng nhận cho các CH chỉ là một yêu cầu khi MoIPS trợ giúp Mobile IP định tuyến tối ưu hoá an toàn.

5. Trong các chứng nhận MoIPS, địa chỉ IP của thực thể được sử dụng như trường tên chủ đề chứng nhận cho các MH, FA, HA và các CH. Khi điều này có nghĩa là chứng nhận phải được phát hành lại khi có sự thay đổi địa chỉ IP bởi một thực thể thì nó cho phép một hệ thống máy tính hoạt động, chẳng hạn như cả HA và FA nằm trên các giao diện khác nhau. Ngược lại trong trường hợp CA, tên miền theo qui tắc tiêu chuẩn được sử dụng như là tên chủ đề trên chứng nhận, loại bỏ yêu cầu về tra tên miền trong trường hợp này.

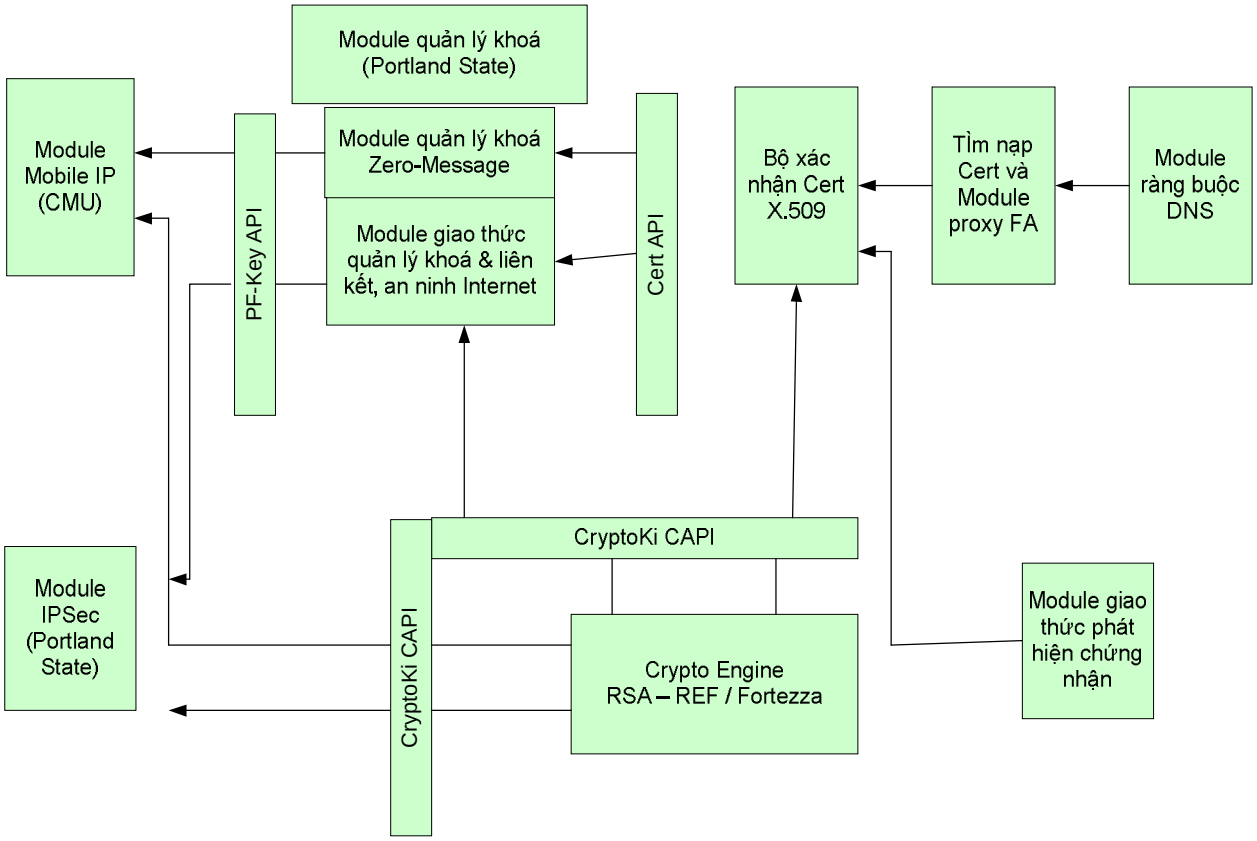
6. MoIPS sử dụng thuật toán băm SHA-1 để tạo các chữ ký số trên các chứng nhận X.509. MoIPS sử dụng một kĩ thuật giống Diffie-Helman (DH) để tạo các khoá mật mã, như các khoá phiên. Mỗi chứng nhận MoIPS chứa các giá trị công cộng DH cần thiết để hỗ trợ trao đổi tạo khoá Diffie-Helman. Bí mật Diffie-Helman và

sự lặp lại số nhận dạng bảo vệ chống tấn công được đưa vào hàm HMAC (MoIPS sử dụng hàm HMAC-MD5) như các thành phần "khoá" và "bản tin" tương ứng. Đầu ra sau đó được sử dụng trong quá trình nhận thực các bản tin điều khiển Mobile IP bằng cách trả lại chuỗi đầu ra và bản tin điều khiển thông qua hàm HMAC.

7. MoIPS sử dụng RSA CryptoKi CAPI (Cryptographic Application Program Interface: Giao diện lập trình ứng dụng mật mã) như một cơ chế qua đó truy nhập các engine mật mã. Cũng được trợ giúp là PF Key CAPI dành cho quản lý các khoá ngắn hạn (như các khoá phiên) và các liên kết an ninh. Những người thiết kế MoIPS đã tạo ra một API thứ ba, được gọi là Cert_API, nhằm cung cấp một tuyến giữa các module quản lý khoá và các bộ xác nhận chứng nhận của hệ thống.
8. MoIPS sử dụng các trường mở rộng chính sách khoá trong các chứng nhận để truyền thông tin cần cho điều khiển truy nhập theo Mobile IP.
9. Theo Mobile IP, đường hầm IPSec an toàn có thể được thiết lập từ MH đến FA, từ MH tới HA, và từ FA tới HA. Ngoài ra, ngoài tầm ảnh hưởng của MoIPS/Mobile IP có thể thiết lập một đường hầm an ninh giữa MH và CH nhằm cung cấp mật mã đầu cuối đến đầu cuối và an toàn thông tin. Các thực thể Mobile IP hoạt động trong môi trường MoIPS có thể yêu cầu thiết lập các đường hầm IPSec bằng cách thêm một trường mở rộng chọn đường hầm IPSec vào các bản tin Khẩn nài tác nhân Mobile IP (Mobile IP Agent Solicitation), Quảng cáo tác nhân, và yêu cầu đăng kí chuẩn. Chi tiết về đường hầm được thiết lập sau đó được đàm phán giữa các thực thể thông qua ISAKMP.

Một nguyên mẫu ban đầu của môi trường MoIPS, được phát triển bởi các nhà nghiên cứu BBC và việc tái sử dụng các module hệ thống sớm được phát triển tại CMU và đại học State Porland được hoàn thành vào năm 1997. Những điểm then chốt là: (1) khả năng nhận được các chứng nhận X.509 và các danh sách thu hồi từ các server DNS như là các bản ghi tài nguyên X509CCRRL; (2) khả năng xác nhận các chứng nhận X.509 và CRL bằng cách đi theo phân cấp CA nhiều cây; (3) khả năng nhận thực các bản tin

đăng kí Mobile IP được cấu tạo theo đặc tả IETF thông qua các khoá phiên được tạo ra bởi thuật toán khoá công cộng đã được mô tả ở trên; và (4) việc tích hợp MH tới các đường hầm CH IPSec với việc định hướng lại các gói tin Mobile IP. Sơ đồ khối minh hoạ các module hệ thống của nguyên mẫu MoIPS xem **hình 4.4**.



Hình 4.4: Sơ đồ khối của nguyên mẫu môi trường MoIPS. (Lấy từ Zao và et al)

Các ứng dụng mục tiêu cho các phiên bản tăng cường của MoIPS gồm việc thực hiện mở rộng các hỗ trợ IPSec và Mobile IP định tuyến tối ưu hoá cho các mạng riêng ảo chứa các MH. Các tác giả xác định một yêu cầu cho việc điều tra về việc quản lí vị trí nhanh và quản lí tinh vi hơn các liên kết an ninh.

4.7 Tổng kết an ninh và nhận thực cho Mobile IP

Chương này đã nghiên cứu một phạm vi rộng các phương pháp cho an ninh và nhận thực người sử dụng trong môi trường Mobile IP. Như được thiết lập với Giao thức đăng kí Mobile IP, các phương pháp khoá công cộng đối xứng có thể được sử dụng theo

Mobile IP. Tuy nhiên, chúng là hiệu quả nhất khi một tổ chức quản lí khoá điều khiển môi trường tính toán di động, hoặc khi một tập những người tham gia chính đã đàm phán trước các mối quan hệ qua lại, như trong tình huống các thoả thuận chuyển vùng giữa các nhà cung cấp dịch vụ tổ ong. Những ví dụ về các trường hợp như thế chứa một tập đoàn với nhiều địa điểm cung cấp hỗ trợ tính toán di động tới các nhân viên của nó, hoặc một nhà cung cấp các dịch vụ truyền thông vô tuyến tạo ra các dịch vụ truy nhập Internet không dây khả dụng thông qua cơ sở hạ tầng xác định nhưng không phải toàn cầu. Đây là những ví dụ quan trọng nhưng mục tiêu cuối cùng của Mobile IP có thể cho rằng là một kịch bản trong đó các hệ thống của hàng nghìn các nhà cung cấp dịch vụ thông tin qua mạng của hàng trăm nhà cung cấp các dịch vụ truy nhập Internet không dây. Giao thức đăng kí Mobile IP cơ sở không thể mở rộng đối với mức này.

Cũng được nghiên cứu trong chương này là Giao thức Sufatrio/Lam đưa ra một phương pháp "light-weight" cho nhận thực người sử dụng bằng cách sử dụng việc lai ghép hai kỹ thuật mật mã đối xứng và không đối xứng và bằng cách khiến HA thực hiện nhiệm vụ gấp đôi như một Trung tâm phân phối khoá. Cuối cùng, chúng ta đã khám phá hệ thống MoIPS của John Zao và các đồng nghiệp của anh ấy đã thông qua một chiến lược khoá công cộng đối xứng đang phát triển mạnh dựa trên các chứng nhận X.509 và một cơ sở hạ tầng khoá công cộng hoàn chỉnh. Nhiều phần tử của kiến trúc này đã tiến tới trạng thái mà chúng có thể được sử dụng như một nền tảng cho thực hiện thương mại trái với nguyên mẫu nghiên cứu. MoIPS vì vậy không thể thấy sự phát triển của nó trong các hệ thống dựa trên Mobile IP thế hệ thứ nhất. Tuy nhiên, sự liên kết chặt chẽ mật mã khoá công cộng và một PKI hoàn chỉnh với Mobile IP sẽ đưa ra một hướng trong tương lai giải quyết các vấn đề lớn về tính mở rộng.

KẾT LUẬN

Luận văn này chủ yếu là xem lại các tài liệu và các khảo sát có khuynh hướng hiện đại và then chốt đang nghiên cứu trong nhận thực thuê bao cho các mạng tổ ong số và Internet không dây. Điều này xác định việc thực hiện then chốt và một vài nghiên cứu chủ đạo trong lĩnh nực này cung cấp một phác thảo cho công việc hiện thời, cố gắng để làm nổi bật những vấn đề, khuynh hướng quan trọng nhất và đưa ra dự án cho việc đầu tư trong tương lai. Tuy nhiên quan trọng để nhận thấy toàn bộ lĩnh vực nhận thực và an ninh cho môi trường liên mạng vô tuyến là một công việc đang phát triển. Nhiều vấn đề như sự cạnh tranh đang diễn ra giữa công nghệ khoá mật mã khoá công cộng (public key) và khoá riêng (private key) vẫn còn chưa được giải quyết, đồng thời những nền tảng tính toán và truyền thông cơ sở đang phát triển không ngừng. Công nghệ an ninh cho thông tin vô tuyến sẽ tiếp tục thay đổi nhanh chóng trong thập kỷ tới vì tiềm năng thực hiện được công nghệ và tính chất đe doạ tới an ninh phát triển theo thời gian. Từ một nghiên cứu như luận văn này có thể dự đoán một số thành phần của lộ trình phát triển. Các phần tử còn lại chắc chắn vẫn còn bí ẩn. Điều không mong muốn đã thúc đẩy chính nó hướng tới lịch sử của Internet một cách thường xuyên và có lẽ sẽ tiếp tục như vậy với tần số ngày càng tăng vì lịch sử Internet không dây đang mở ra.

TÀI LIỆU THAM KHẢO

1. ***Giáo trình thông tin di động GSM*. Biên soạn: TS. Nguyễn Phạm Anh Dũng**
2. ***Giáo trình thông tin di động thế hệ ba*. Biên soạn: TS: Nguyễn Phạm Anh Dũng**
3. ***3G Wireless Networks*: Clint Smith and Daniel Collins and others. McGraw-Hill, 2002.**
4. ***Subscriber Authentication and Security in Digital Cellular* Network. Howard Wolfe Curtis, PDF File.**