MẬT MÃ TỐC ĐỘ CAO HƯỚNG TỚI ỨNG DỤNG TRONG CÁC MẠNG TRUYỀN THÔNG KHÔNG DÂY

TỔNG QUAN

1. Ngoài nước:

Những năm gần đây trên thế giới, nhiều giao thức không dây đã được đề xuất và được đưa vào ứng dụng. Đồng thời rất nhiều trong số đó đã sẵn sàng cho việc sử dụng đối với phần lớn các khách hàng. Một số giải pháp về các giao thức an toàn, có thể được mô tả như sau:

Giao thức ứng dụng mạng không dây (Wireless Application Protocol - WAP) là chuẩn thực tế (de-facto standard) của thế giới dành cho truyền thông không dây và các dịch vụ thoại trên điện thoại di động và các dịch vụ đầu cuối không dây khác. Tầng truyền không dây bảo mật (Wireless Transport Layer Security - WTLS) là một tầng của giao thức WAP được dành riêng cho an ninh. Trong kiến trúc của WTLS, các thuật toán mã hóa mạnh đã được lựa chọn để hỗ trợ ba hoạt động mã hoá khác nhau. Mã hoá sử dụng DES, IDEA và RC5, xác thực thông điệp dựa trên RSA, Diffie-Hellman và đường cong Elliptic. MD5 và SHA sử dụng hàm băm.

Bluetooth là một hệ thống truyền thông không dây được tích hợp trên các máy tính xách tay, điện thoại di động và các thiết bị khác mà có thể được kết nối với nhau, yêu cầu sử dụng điện năng thấp và các kết nối không dây trong phạm vi ngắn. Đặc điểm kỹ thuật của Bluetooth bao gồm các tính năng an ninh. Hệ thống hỗ trợ xác thực và các quá trình mã hóa. Các tính năng này được dựa trên một khoá liên kết bảo mật nó được chia sẻ bởi một cặp thiết bị. Khóa được tạo ra khi hai thiết bị giao tiếp lần đầu tiên. Mã hóa của thông tin được thực hiện với thuật toán mã hóa dòng được gọi là Eo, nó là thuật toán tái đồng bộ cho mỗi thông tin. Thuật toán này được dựa trên một trong các phương pháp đưa ra từ kết luận phát sinh các thuật toán mật mã dòng, có thể coi là thuộc về của Massey và Rueppel. Chức năng xác thực cho Bluetooth, là một mã xác thực thường được gọi là MAC. Thuật toán mã hóa được sử dụng cho bluetooth là SAFER+. Nó là một trong những đối thủ của chuẩn mật mã nâng cao (AES) và được sự hỗ trợ của Cylink, Corp Sunnyvale, Hoa Kỳ. Thuật toán này là một phiên bản nâng cao của thuật toán 64-bit mật mã khối SAFER-SK 128.

HIPERLAN là chuẩn truy cập băng thông rộng không dây của ETSI. Các đặc tả của giao thức truyền thông này xác định cách mã hoá/giải mã từng phần cho các tùy chọn sử dụng. Tất cả các nhân HIPERLAN MAC sử dụng khóa chung cho các thuật toán mã hóa mà giao thức hỗ trợ (hình 1). Chúng được gọi là thiết lập khoá HIPERLAN. Tất cả các khóa của thiết lập này được mô tả duy nhất với đặc điểm riêng của chính nó. Trong phần bảo mật của giao thức, bản mã được tạo ra từ một thủ tục XOR trên văn bản gốc. Các hàm mã ngoại trừ các khóa, cũng đòi hỏi một chuỗi ngẫu nhiên. ETSI đòi hỏi phần bảo mật mà đã được thông qua trong HIPERLAN sử dụng các mức bảo vệ của một mạng LAN có dây. Thật không dễ để đưa ra chi tiết về mức độ bảo vệ và sức mạnh của sự bảo mật mà HIPERLAN hỗ trợ bởi các mật mã xác định vẫn chưa sẵn có.

Tổ chức IEEE đã đưa ra chuẩn 802.11 cho mạng LAN không dây (Wireless Local Area Network - WLAN) năm 1990. Mạng không dây nội bộ xác định một tùy chọn bảo mật mang tên Mã hóa bảo mật mạng không dây WEP [4]. Phần bảo vệ này hỗ trợ phòng tuyến của các giao thức chống lại sự tấn công từ bên ngoài. Về lý thuyết, một kẻ nghe trộm với bộ giải điều chế sóng vô tuyến thích hợp có thể nghe được các thông tin trao đổi của người dùng giao thức. WEP cố gắng ngăn chặn những sự can thiệp không mong muốn này trong những giao thức truyền thông đã được thiết lập. Tính năng xác thực thông điệp sử dụng khóa giống với mã hóa thông tin. Việc

sử dụng khoá chung cho cả hai tính năng bảo mật này sẽ dẫn tới sự rủi ro cao hơn cho giao thức. Tính năng xác thực chỉ hoạt động hiệu quả khi WEP được hỗ trợ bởi các mạng WLAN. Không có các phương thức mã hóa, các thủ tục xác thực cũng sẽ bị hủy bỏ.

Tuy nhiên, các kỹ thuật này cho đến nay đã bộc lộ rõ những hạn chế khi áp dụng đối với các thiết bị di động và nhiều kỹ thuật đã bị xác nhận là thám mã được trong nhiều tình huống. Kỹ thuật đang được phát triển nghiên cứu và triển khai trong các ứng dụng trên thế giới đó là vệc triển khai trên phần cứng với các sơ đồ mã hóa đơn giảm nhằm đảm bảo tốc độ mã hóa nhanh, hiệu quả trên các thiết bị di động nhưng vẫn đảm bảo độ bảo mật với tính chất điều khiển được trong mạng hoán vị - thay thế. Giải pháp đã được đề xuất bởi Moldovyan N.A., Moldovyanu P.A và phát triển bởi chính tác giả và một số nhà nghiên cứu đươc thể hiện trong các danh mục sau đây và đây cũng là các công trình nghiên cứu, các tài liệu có liên quan đến đề tài được trích dẫn khi đánh giá tổng quan:

ü Ueli Maurer (2001), "Cryptography 2000±10", Informatics - 10 Years Back, 10 Years Ahead, Lecture Notes in Computer Science, Springer-Verlag, 2000.

ü S.H. Park, A. Gaz and Z. Ganz (1998), "Security protocol for IEEE 802.11 wireless local area network", Mobile Networks and Applications .

ü Nicolas Sklavos and Odysseas Koufopavlou (2003), "Mobile Communications World Security Implementations Aspects - A State of the Art", Computer Science Journal of Moldova.

ü P. Kitsos, N. Sklavos and O. Koufopavlou (2002), "Hardware Implementation of the SAFER+ Encryption Algorithm for the Bluetooth System", proceedings of IEEE International Symposium on Circuits & Systems (ISCAS'02), 4.

ü Yeong-Kang Lai, Liang-Gee Chen, Jian-Yi Lai, and Tai-Ming Parng (2002), "VLSI Architecture Design and Implementation for Twofish Block Cipher", proceedings of IEEE International Symposium on Circuits & Systems (ISCAS'02).

ü Moldovyan N.A., Moldovyanu P.A., Summerville D.H. On Software Implementation of Fast DDP-Based Ciphers. // International Journal of Network Security. 2007. vol. 4, no. 1.

2. Trong nước:

- Phân tích, đánh giá tình hình nghiên cứu thuộc lĩnh vực của đề tài: Trong những năm qua vấn đề nghiên cứu về mật mã tại Việt Nam cũng còn nhiều hạn chế bởi nhiều lý do hoặc có những kết quả nghiên cứu chỉ mang nội dung cơ bản, đặc thù áp dụng trong những tình huống cụ thể của mỗi đơn vị sử dụng. Còn lại đa số các công nghệ, kỹ thuật mã hóa trong các ứng dụng và các thiết bị đều theo các mô hình mã hóa của thế giới như DES, AES, MD5, ... Kỹ thuật mã hóa trên phần cứng theo mô hình mạng chuyển vị thay thế điều khiển được hiện chưa có công trình công bố.
- Danh mục các công trình nghiên cứu, các tài liệu có liên quan đến đề tài được trích dẫn khi đánh giá tổng quan: Cho đến thời điểm hiện tại chưa có công trình nghiên cứu cụ thể được công bố trên thông tin đại chúng hoặc được xuất bản rộng rãi qua các hình thức sách, tài liệu.

3. Danh mục các công trình đã công bố thuộc lĩnh vực của đề tài của chủ nhiệm và những thành viên tham gia nghiên cứu (họ và tên tác giả; bài báo; ấn phẩm; các yếu tố về xuất bản)

- Đánh giá các đặc trưng thống kê của thuật toán mật mã CRYPT(D)-64". Tạp chí khoa học và kỹ thuật của Học viện kỹ thuật quân sự, 5-21, Số 126, tháng 02- 2009. Tác giả: Nguyễn Hiếu Minh, Đỗ Thị Bắc, Lưu Hồng Dũng.

MỤC TIÊU

- Nghiên cứu và xây dựng các thuật toán mật mã có khả năng thực hiện đơn giản khi tích hợp

trên thiết bị di động, trong khi đồng thời nâng cao hiệu quả tích hợp của các thuật toán để đảm bảo duy trì hiệu năng của các thiết bị khi được tích hợp các thuật toán mật mã.

- Nâng cao năng lực nghiên cứu khoa học. Từ đó phát huy để tăng cường đề xuất đưa những nội dung mới, tiên tiến trên thế giới về mật mã vào chương trình đào tạo của Khoa nhằm nâng cao chất lượng giáo dục .
- Góp phần đưa thành tựu khoa học, các kỹ thuật mới trong mật mã trên thế giới vào việc thực hiện nhiệm vụ phát triển sự nghiệp giáo dục và đào tạo.

NỘI DUNG

Nội dung nghiên cứu

- Phân tích các nguyên nhân, nguy cơ và các kiểu tấn công trên mạng di động.
- Phân tích thực trạng ứng dụng các giải pháp mật mã để đảm bảo an toàn thông tin trong các mạng di động.
- Đánh giá và lựa chọn các hàm nguyên thủy và các giải pháp xây dựng thuật toán mã tốc độ cao.
- Xây dựng các thuật toán mật mã mới hướng tới việc thực hiện tối ưu trên vi xử lý (FPGA & ASIC) có tốc độ cao.
- Phân tích và đánh giá các phương án thực hiện bằng thực nghiệm của thuật toán.
- Lựa chọn các mô hình đánh giá hiệu quả tích hợp của các thuật toán trên thiết bị.
- Phân tích các thuật toán với mục đích kiểm tra theo các tiêu chuẩn và các dạng tấn công đã biết.
- Xây dựng thử nghiệm chương trình phần mềm.

PHƯƠNG PHÁP NGHIÊN CỨU

Nghiên cứu lý thuyết kết hợp với mô phỏng và đánh giá thực nghiệm trên cơ sở các chuẩn đánh giá của các tổ chức trên thế giới. Cụ thể sử dụng kết hợp các nhóm phương pháp nghiên cứu: phân tích, so sánh, tổng hợp, đánh giá, mô phỏng bằng phần mềm thực nghiệm.

HIỆU QUẢ KTXH

- Phát huy và nâng cao năng lực nghiên cứu khoa học của giảng viên và sinh viên.
- Tăng cường việc đề xuất đưa những nội dung mới, tiên tiến trên thế giới về mật mã vào chương trình đào tạo ngành Công nghệ thông tin của Khoa nhằm nâng cao chất lượng giáo dục.
- Tiến tới đưa thành tựu khoa học, các kỹ thuật mới trong mật mã trên thế giới trong việc cải thiện vấn đề an ninh trên mạng nói chung và mạng không dây nói riêng. Từ đó góp phần phát triển nền kinh tế và xã hội của quốc gia.

ĐƠN VỊ SỬ DỤNG