ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

LÊ ĐỨC HUY

KỸ THUẬT XÁC THỰC VÀ MÃ HÓA DỮ LIỆU TRONG CÔNG NGHỆ WIMAX

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Thái Nguyên – 2015

ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

LÊ ĐỨC HUY

KỸ THUẬT XÁC THỰC VÀ MÃ HÓA DỮ LIỆU TRONG CÔNG NGHỆ WIMAX

LUẬN VĂN THẠC SĨ CÔNG NGHỆ THÔNG TIN

Chuyên ngành: Khoa học máy tính

Mã số: 60480101

NGƯỜI HƯỚNG DẪN KHOA HỌC

PGS – TS. NGUYỄN VĂN TAM

Thái Nguyên - 2015

LỜI CẢM ƠN

Trên thực tế không có thành công nào mà không gắn liền với những sự hỗ trợ, giúp đỡ. Trong suốt thời gian từ khi bắt đầu học tập tại trường đến nay, em đã nhận được rất nhiều sự quan tâm, giúp đỡ của quý Thầy Cô trường Đại học Công nghệ Thông tin và Truyền thông – Đại học Thái Nguyên đã cùng với tri thức và tâm huyết của mình để truyền đạt vốn kiến thức quý báu cho chúng em trong suốt thời gian học tập tại trường, và luôn luôn tạo mọi điều kiện tốt nhất cho chúng em trong suốt quá trình theo học tại trường. Em xin chân thành cảm ơn quý Thầy Cô và Ban lãnh đạo nhà trường!

Với lòng biết ơn sâu sắc nhất em xin gửi lời cảm ơn tới PGS.TS Nguyễn Văn Tam, viện Hàn Lâm Khoa Học Việt Nam, là cán bộ trực tiếp hướng dẫn khoa học cho em. Thầy đã dành nhiều thời gian cho việc hướng dẫn em cách nghiên cứu, đọc tài liệu, cài đặt các thuật toán và giúp đỡ em trong việc xây dựng chương trình, em xin chân thành cảm ơn Thầy!

Mặc dù tôi đã có nhiều cố gắng hoàn thiện luận văn bằng tất cả sự nhiệt tình và năng lực của mình, tuy nhiên không thể tránh khỏi những thiếu sót, rất mong nhận được những đóng góp quí báu của quí thầy cô và các bạn.

Hà nội , ngày 25 tháng 08 năm 2015

Học viên

LÊ ĐỨC HUY

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn là kết quả nghiên cứu của tôi, không sao chép của ai. Nội dung luận văn có tham khảo và sử dụng các tài liệu liên quan, các thông tin trong tài liệu được đăng tải trên các tạp chí và các trang website theo danh mục tài liệu của luận văn.

Tác giả luận văn

Lê Đức Huy

MỤC LỤC

LỜI CẢM ƠN 2
LỜI CAM ĐOAN 4
MỤC LỤC 5
DANH MỤC CÁC TỪ VIẾT TẮT 7
DANH MỤC CÁC HÌNH 8
LỜI NÓI ĐẦU 9
CHƯƠNG 1: TỔNG QUAN VỀ WIMAX VÀ VẤN ĐỀ AN NINH TRONG WIMAX. 11
1.1 Giới thiệu WIMAX 11
1.1.1 Kiên trúc phân lớp WIMAX 11
1.1.2 Khái quát phân lớp trong giao thức IEEE 802.16 11
1.1.2.1 Lớp vật lý 11
1.1.2.2 Lớp MAC 12
1.1.3 Ưu điểm của WIMAX 17
1.2 Một số các cách tấn công trong WIMAX 19
1.3 Vấn đề an toàn bảo mật trong WIMAX 20
1.3.1 Nhận thực 20
1.3.2 Bảo mật 21
1.3.3 Toàn Vẹn 21
1.3.4 Một số giải pháp an ninh trong Wimax 22
CHƯƠNG II: KỸ THUẬT XÁC THỰC VÀ MÃ HÓA DỮ LIỆU TRONG CÔNG NGHỆ WIMAX 23
2.1 Thuật toán xác thực 23
2.1.1 Thuật toán mã hóa khóa công khai (RSA) 23
2.1.1.1 Giới thiệu thuật toán 23
2.1.1.2 Thuật toán 24
2.1.1.3 Ưu nhược điểm. 27
2.1.1.3.1 Nhược điểm 27
2.1.1.3.2 Ưu điểm. 27
2.1.1.4 Đặc trưng của hệ mật RSA 28
2.1.1.5 Độ an toàn của hệ mật RSA 30
2.1.1.6 Quản lý khoá của hệ mật mã RSA 31
2.1.1.7 Các ứng dụng của RSA 37
2.1.2 Thuật toán mã hóa dựa trên định danh (IBE) 41
2.1.2.1 Giới thiệu 41

2.1.2.2 Các khả năng ứng dụng IBE 41
2.1.2.3 Lược đồ mã hóa dựa trên định danh 43
2.2 Thuật toán mã hóa dữ liệu 45
2.2.1 Thuật toán mã hóa DES 45
2.2.1.1 Giới thiệu: 45
2.2.1.2 Thuật toán : 46
2.2.2 Thuật toán mã hóa 48
2.2.2.1 Giới thiệu: 48
2.2.2.2 Thuật toán 49
CHƯƠNG III: XÂY DỰNG CHƯƠNG TRÌNH MÔ PHỎNG DỰA TRÊN THUẬT TOÁN XÁC THỰC CẢI TIẾN RSA 56
3.1 Xác thực lẫn nhau dựa trên RSA 56
3.1.1. Đặt vấn đề bài toán 56
3.1.2. Mô tả thuật toán 56
3.2 Xây dựng chương trình mô phỏng 60
3.2.1 Lựa chọn công cụ và ngôn ngữ 60
3.2.2 Hoạt động và giao diện của chương trình 63
3.3 Đánh giá hiệu quả của giải pháp cải tiến 69
3.3.1 Phòng chống tấn công Replay 70
3.3.2 Phòng chống tấn công Man in Middle Attack và Denial of Service . 70
KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 72
PHỤ LỤC MÃ NGUỒN CỦA CHƯƠNG TRÌNH 74

Từ Viết Tắt	Từ Viết Đầy Đủ	Nghĩa
AES	Advanced Encryption Standard	Chuẩn mã hóa dữ liệu cao cấp
ARQ	Automatic Repeat Request	Tự động lặp lại yêu cầu
ADSL	Asymmetric Digital Subcriber Line	Đường dây thuê bao số bất đối xứng
BPSK	Binary Phase Shift Keying	Khóa dịch pha nhị phân
BER	Bit Error Rate	Tỷ số lỗi bít
BPSK	Binary Phase Shift Keying	Điều chế pha nhị phân
BS	Base Station	Trạm gốc
CID	Connection Identify	Nhận dạng kết nối
CSMA	Carrier Sense Multiple Access	Đa truy nhập cảm ứng sóng mang
CS	Channel Switched	Chuyển mạch kênh
DHCP	Dynamic host Configuration Protocol	Giao thức cấu hình Host động
DSL	Digital Subcriber Line	Đường dây thuê bao số
DES	Data Encryption Standard	Tiêu chuẩn mã hóa dữ liệu
IEEE	Institute of Electrical and Electronics Engineers	Viện kỹ nghệ Điện và Điện tử
WMAN	Wireless Metropolitan Area Network	Mạng vô tuyến khu vực đô thị
OFDM	Orthogonal Frequency Division Multiplexing	Ghép phân chia tần số trực giao
NLOS	Non light of Sight	Không tầm nhìn thẳng
SOFDMA	Scalable Orthogonal Frequency Division Multiple Access	Khả năng mở rộng đa truy cập phân chia theo tần số trực giao
TDD	Time Division Duplex	Song công phân chia theo thời gian
FDD	Frequence Division Duplex	Song công phân chia theo tần số
TDMA	Time Division Multiple Access	Đa truy nhập phân chia theo thời gian
MAC	Medium Access Control	Điều khiển truy nhập môi trường
PMP	Point to Multipoint	Điểm-đa điểm
SA	Security Association	Liên kết bảo mật
TEK	Traffic Encryption Key	Khóa bảo mật dữ liệu
UMTS	Universal Mobile Telecommunication seytem	Hệ thống viễn thông di động toàn cầu
IBE	Indetity Base Encryption	Mã hóa dựa trên định danh
QPSK	Quadrature phase-shift keying	Điều chế pha cầu phương
SS	Subcriber Station	Trạm thuê bao
PDA	Personal Digital Assistance	Thiết bị hỗ trợ cá nhân kĩ thuật số

DANH MỤC CÁC TỪ VIẾT TẮT

DANH MỤC CÁC HÌNH

Hình 1: Lớp giao thức trong IEEE 802.16 12
Hình 2: Chi tiết phân lớp MAC trong IEEE 802.16 13
Hình 3: Khuôn dạng bản tin MAC 14
Hình 4: Nhận thực trong IEEE 802.16 16
Hình 5: Quá trình trao đổi khóa 17
Hình 6: Quá trình mã hóa khóa công khai RSA 29
Hình 7: Ứng dụng RSA trong chữ kí điện tử 38
Hình 8: Ứng dụng của RSA trong thẻ ATM của ngân hàng. 39
Hình 9: Mã hoá bằng hệ thống IBE 43
Hình 10: Giải mã bằng hệ thống IBE 44
Hình 11: Hàm F (F-function) dùng trong DES 47
Hình 12: Quá trình tạo khóa con trong DES 48
Hình 13: Bước SubBytes 50
Hình 14: Bước ShiftRows 51
Hình 15: Bước MixColumns 52
Hình 16: Bước AddRoundKey 52
Hình 17: Quá trình xác thực lẫn nhau để tránh BS giả mạo tấn công 57
Hình 18: Lưu đồ thuật toán SS 58
Hình 19: Lưu đồ thuật toán BS 59
Hình 20: Quy trình truyền thông tổng thể. 60
Hình 21: Phòng chống tấn công phát lại bằng cách sử dụng Timestamp 70

LỜI NÓI ĐẦU

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 theo mô hình 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.

Ngành công nghệ viễn thông đã chứng kiến những phát triển ngoạn mục trong những năm gần đây, đặc biệt là truyền thông không dây băng thông rộng. Khi mà công nghệ mạng thông tin di động thế hệ thứ ba 3G chưa có đủ thời gian để khẳng định vị thế của mình trên toàn cầu, người ta đã bắt đầu nói về công nghệ Wimax từ những năm gần đây.

Tiềm năng cung cấp kết nối mềm dẻo, mọi lúc mọi nơi 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 cũng xuất 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 thiết bị truyền thông di động được và do đó 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.

Do đặc điểm trao đổi thông tin trong không gian truyền sóng nên khả năng thông tin bị rò rỉ ra ngoài là hoàn toàn dễ hiểu. Hơn nữa, ngày nay với sự

phát triển cao của công nghệ thông tin, các hacker có thể dễ dàng xâm nhập vào mạng hơn bằng nhiều con đường khác nhau. Vì vậy có thể nói điểm yếu cơ bản nhất của mạng di động Wimax đó là khả năng bảo mật, an toàn thông tin. Thông tin là một tài sản quý giá, đảm bảo được an toàn dữ liệu cho người sử dụng là một trong những yêu cầu được đặt ra hàng đầu.

Xuất phát từ những lý do trên, tôi đã chọn đề tài "Kỹ thuật xác thực và mã hóa dữ liệu trong công nghệ WIMAX". Chủ đề quan tâm ở đây là lĩnh vực an ninh thông tin trong mạng không dây băng thông rộng, mà điểm mấu chốt là tìm hiểu các kỹ thuật, công nghệ để đảm bảo sự an ninh đó. Đó thực sự là lĩnh vực rất rộng lớn và phức tạp.

Luận văn gồm có các nội dung như sau:

Chương 1 : Tổng quan về Wimax và vấn đề an ninh trong Wimax.

Chương 2 : Kỹ thuật xác thực và mã hóa dữ liệu trong công nghệ Wimax.

Chương 3 : Xây dựng chương trình mô phỏng dựa trên thuật toán xác thực cải tiến RSA.