

**ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
VÀ TRUYỀN THÔNG**

NGUYỄN THỊ THANH AN

**PHÂN TÍCH VÀ ĐÁNH GIÁ VẤN ĐỀ AN NINH
TRONG MẠNG KHÔNG DÂY WIMAX**

**Chuyên ngành: Khoa học máy tính
Mã số: 60 48 01**

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Người hướng dẫn khoa học: PGS.TS. NGUYỄN VĂN TAM

THÁI NGUYÊN - 2012

LỜI CAM ĐOAN

Tôi xin cam đoan luận văn này là công trình nghiên cứu, tìm hiểu và tham khảo của riêng tôi. Các số liệu trong luận văn là trung thực.

Tác giả

Nguyễn Thị Thanh An

LỜI CẢM ƠN

Luận văn này được hoàn thành tại trường Đại học Công nghệ Thông tin và Truyền thông - Đại học Thái Nguyên. Dưới sự hướng dẫn của PGS.TS. NGUYỄN VĂN TAM. Tác giả xin bày tỏ lòng kính trọng và biết ơn sâu sắc tới thầy về sự tận tình hướng dẫn trong suốt thời gian tác giả làm luận văn.

Trong quá trình học tập tại trường Đại học Công nghệ Thông tin và Truyền thông - Đại học Thái Nguyên tác giả thường xuyên nhận được sự quan tâm giúp đỡ, đóng góp ý kiến của các thầy cô trực tiếp giảng dạy và các cán bộ, giáo viên trong trường. Tác giả xin bày tỏ lòng biết ơn sâu sắc đến những thầy cô đó.

Xin chân thành cảm ơn anh chị em học viên lớp CAO HỌC K9A đã giúp đỡ, động viên, khích lệ tác giả trong quá trình học tập và nghiên cứu.

Luận văn sẽ không hoàn thành được nếu không có sự quan tâm, động viên của người thân trong gia đình tác giả. Đây là món quà tinh thần, tác giả xin gửi tặng gia đình thân yêu của mình với lòng biết ơn sâu sắc.

Tác giả

MỤC LỤC

Lời cam đoan	i
Lời cảm ơn	ii
Mục lục	iii
Danh mục chữ viết tắt	v
Danh mục các hình	viii
Danh mục các bảng	ix
MỞ ĐẦU	1
Chương 1. KIẾN TRÚC CỦA WIMAX CHUẨN IEEE802.16	2
1.1. Quá trình phát triển của WIMAX	2
1.1.1. IEEE 802.16-2001	3
1.1.2. IEEE 802.16c-2002	4
1.1.3. IEEE 802.16a-2003	4
1.1.4. Chuẩn IEEE 802.16d-2004	6
1.1.5. IEEE 802.16e và Beyond	6
1.2. Các giao thức của WIMAX	6
1.2.1. Các lớp giao thức	6
1.2.2. Lớp vật lý (PHY)	7
1.2.3. Lớp điều khiển truy nhập (MAC)	13
Kết luận	20
Chương 2. PHÂN TÍCH VẤN ĐỀ AN NINH CHUẨN IEEE802.16	21
2.1. Đánh giá về an ninh của tiêu chuẩn IEEE 802.16	21
2.1.1. Giới thiệu các lỗ hổng của mạng không dây (IEEE 802.11)	21
2.1.2. Phân tích về lỗ hổng của chuẩn IEEE 802.16	23
2.2. Các phần tử an ninh của chuẩn IEEE 802.16	35
2.2.1. Các phần tử an ninh chính của chuẩn IEEE 802.16	35
2.2.2. Thuật toán mã hóa	36

2.2.3. Chứng chỉ số X.509	38
2.2.4. Kết nối an toàn SA	39
2.2.5. Mã hóa	40
2.2.6. Giao thức trao đổi khóa PKM	41
2.2.7. Quản lý khóa cấp phép (AK)	45
2.2.8. Mã hóa dữ liệu	46
Kết luận	47
Chương 3. VẤN ĐỀ XÁC THỰC	48
3.1. Xác thực lẫn nhau	48
3.2. Đề xuất thuật toán cho BS xác thực	49
3.3. Chi tiết thông tin liên lạc với máy chủ xác thực	51
3.4. Phòng chống tấn công lặp gói tin	52
3.5. Phòng chống tấn công chen giữa và tấn công từ chối dịch vụ	53
3.6. Mô phỏng kết quả	54
Kết luận	58
Công trình trong tương lai	58
TÀI LIỆU THAM KHẢO	60
Phụ lục 1: Lập trình mã cho các BS (Base Station)	62
Phụ lục 2: Lập trình mã cho các SS (Subscriber Station)	65
Phụ lục 3: Lập trình mã cho các AS (Authentication Server)	69

DANH MỤC CHỮ VIẾT TẮT

AK	Authentication Key
AS	Authentication Server
AP	Access Point
ATM	Asynchronous Transfer Mode
AES	Advanced Encryption Standard
BS	Base Station
BSID	Base Stations ID
BWA	Broadband Wireless Access
CPE	Customer Premise Equipment
CS	Convergence Sublayer
CPS	Common Part Sublayer
CIDs	Connection Identifiers
CPE	Customer Premises Equipment
CMAC	Cipher-based Message Authentication Code
CTS	Clear to Send
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CMAC	Cipher-Based Authentication Code Wide Interoperability for
DLL	Data Link Layer Microwave Access
DL	Downlink
DES	Data Encryption Standard
DREG-CMD	Re/RE-register Command
DoS	Denial of Service
EAP	Extensible Authentication Protocol
FDD	Frequency Division Duplexing
FDMA	Frequency Division Multiple Access

HMAC	Hashed Message Authentication Code
ISO/IEC	International Organization for Standardization & the International Electrotechnical Commission
ITU	International Telecommunications Union
IP	Internet Protocol
IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LLC	Logical Link Control
LOS	Line of Sight
MAC	Media Access Control
MD5	Message-Digest algorithm 5
NLOS	Non Line of Sight
NIST	National Institute of Standards and Technology
OFDMA	Orthogonal Frequency Division Multiple Access
OSI	Open Systems Interconnection
PKM	Protocol Key Management Protocol
PTP	Point to Point
PMP	Point to Multipoint
PDU	Protocol Data Unit
PHY Layer	Physical Layer
PKM-REQ	PKM Request
PKM-RSP	PKM Response
PHS	Payload Header Suppression
PKM	Privacy Key Management
PKMv1	Key Management Protocol version 1
PKMv2	Key Management Protocol version 2

QoS	Quality of Service
RES-CMD	Reset Command
RTS	Request to Send
SS	Subscriber Station
SSID	Subscriber Stations ID
SDU	Service Data Unit
SA	Security Association
TEK	Traffic Encryption Key
TDD	Time Division Duplexing
TDMA	Time Division Multiple Access
TDM	Time Division Multiplexing
3-DES	Triple Data Encryption Standard
UL	Uplink
VoIP	Voice over Internet Protocol
WirelessMan	Wireless Metropolitan Area Network
WIMAX	World Wide Interoperability for Microwave Access

DANH MỤC CÁC HÌNH

Hình 1.1: Bảy lớp mô hình OSI cho các mạng	7
Hình 1.2: Lớp giao thức trong IEEE 802.16	10
Hình 1.3: Chi tiết phân lớp MAC trong IEEE 802.16	14
Hình 1.4: Truyền-nhận SDUs và PDUs trong quá trình gửi và nhận tín hiệu	16
Hình 2.1: Tấn công bằng thông điệp loại bỏ xác thực	25
Hình 2.2: Ngăn chặn tấn công sử dụng RES-CMD	27
Hình 2.3: Điểm truy nhập giả mạo bằng một nút giả mạo	30
Hình 2.4: SS xác thực và đăng ký	31
Hình 2.5: Thuật toán ba DES	37
Hình 2.6: Xác thực X.509	38
Hình 2.7: Nhận thực trong IEEE 802.16	39
Hình 2.8: Xác thực và cấp phát khóa cấp phép bởi BS. BS là máy chủ và SS là khách hàng	43
Hình 2.9: Quá trình trao đổi khóa	44
Hình 2.10: SS yêu cầu BS cho các khoá mã hóa TEK0 và TEK1	46
Hình 3.1: Giao thức xác thực trong chuẩn IEEE802.16	48
Hình 3.2: Quá trình xác thực lẫn nhau để tránh cuộc tấn công giả mạo BS	50
Hình 3.3: Quá trình truyền thông tổng thể	51
Hình 3.4: Phòng chống tấn công lặp gói tin bằng cách sử dụng nhãn thời gian	53
Hình 3.5: Trạm gốc (BS) đang chờ đợi kết nối	54
Hình 3.6: SS được gửi thông tin đến BS	55
Hình 3.7: BS đang gửi thông tin cho các SS	55
Hình 3.8: SS nhận được thông điệp từ BS và giải mã các thông điệp	56
Hình 3.9: SS truyền tải thông điệp đến các AS	56
Hình 3.10: AS xác minh các BS và gửi thông báo tới AS	57
Hình 3.11: SS xác minh các BS	57

DANH MỤC CÁC BẢNG

Bảng 1.1: So sánh các tiêu chuẩn IEEE 802.16 BWA [4]	5
Bảng 1.2: Năm giao diện vật lý định nghĩa trong chuẩn 802.16 [3]	9
Bảng 1.3: Ưu điểm của OFDMA so với OFDM	12
Bảng 1.4: Các tham số tỷ lệ S-OFDMA	13
Bảng 2.1: Các phép mã hóa được sử dụng trong tiêu chuẩn IEEE 802.16, IEEE 802.16-phiên bản 2004 [11]	40
Bảng 2.2: Các vấn đề cơ bản của giao thức PKMv1 trong tiêu chuẩn IEEE 802.16[11]	41