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

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

DANH MỤC CÁC BẢNG