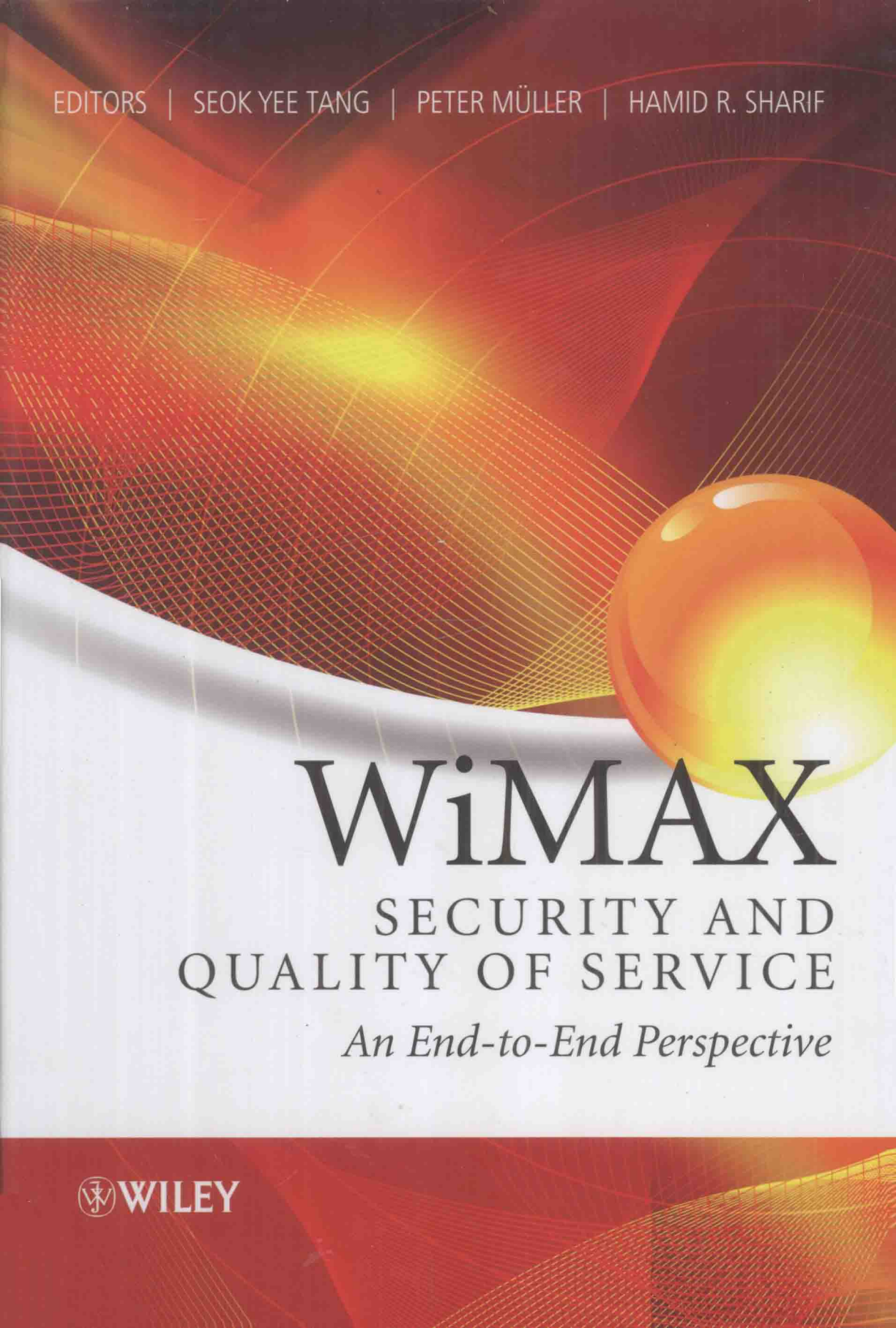


EDITORS | SEOK YEE TANG | PETER MÜLLER | HAMID R. SHARIF



WiMAX

SECURITY AND
QUALITY OF SERVICE

An End-to-End Perspective

 WILEY

WiMAX SECURITY AND QUALITY OF SERVICE

AN END-TO-END PERSPECTIVE

Edited by

Seok-Yee Tang

Think Wireless Tech Pte. Ltd., Singapore

Peter Müller

IBM Zurich Research Laboratory, Switzerland

Hamid R. Sharif

University of Nebraska-Lincoln, USA



A John Wiley and Sons, Ltd., Publication

This edition first published 2010

© 2010 John Wiley & Sons Ltd.,

Registered office

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

The right of the author to be identified as the author of this work has been asserted in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior permission of the publisher.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Designations used by companies to distinguish their products are often claimed as trademarks. All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners. The publisher is not associated with any product or vendor mentioned in this book. This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Library of Congress Cataloging-in-Publication Data

WiMAX security and quality of service : an end-to-end perspective / edited by Seok-Yee Tang, Peter Müller, and Hamid Sharif.

p. cm.

Includes bibliographical references and index.

ISBN 978-0-470-72197-1 (cloth)

1. Wireless metropolitan area networks—Security measures. 2. IEEE 802.16 (Standard)

I. Tang, Seok-Yee, 1968- II. Müller, Peter, 1961 July 8- III. Sharif, Hamid R. (Hamid Reza), 1958-
TK5105.85.W55 2010

621.382'1 – dc22

2010003319

A catalogue record for this book is available from the British Library.

ISBN 978-0-470-72197-1 (H/B)

Typeset in 10/12 Times by Laserwords Private Limited, Chennai, India
Printed and Bound in Singapore by Markono Print Media Pte Ltd

WiMAX SECURITY AND QUALITY OF SERVICE

Preface

The rapid increase in demand for high-speed broadband wireless networks has spurred the development of new technologies in recent years. Worldwide Interoperability for Microwave Access, known as WiMAX, is one of these technologies. WiMAX is based on the IEEE 802.16 family of standards and offers flexible fixed and mobile wireless solutions along with high-bandwidth services for extended distance coverage and a variety of applications including support of an array of multimedia functions.

IEEE 802.16e is the most popular implementation of this standard; it defines a path of evolution to support high throughput wireless technology for mobile systems. The WiMAX mobile wireless standard, which was defined originally by the IEEE 802.16e-2005 amendment, is now being deployed in more than 140 countries by more than 475 operators.

The 802.16 Medium Access Control (MAC) is designed to support high data transfer for uplink and downlink communications between a base station and a large number of clients for continuous and bursty traffic. WiMAX also supports significant flexible operations across a wide range of spectrum allocation including both licensed and license-exempt frequencies of 2 to 11 GHz. It provides an access system which is based on a request-grant mechanism designed to support service requirements, scalability and efficiency. Along with the bandwidth allocation task, the IEEE 802.16 access mechanism provides a sublayer designed to support privacy and authentication for network access and establishment of connection.

Quality of Service (QoS) is an important factor in WiMAX technologies. WiMAX can provide QoS for wireless broadband communications over an extended coverage area for real-time delay-sensitive applications such as Voice over IP and real-time streaming in stationary or mobile environments. It offers different access methods for different classes of traffic. The 802.16e protocol is a connection-oriented medium access control with service flows as well as a grant-based system which allows centralized control and eliminates overheads and delay of acknowledgements. This in turn provides an effective QoS handling which is fundamentally different from connectionless wireless protocols such as IEEE 802.11. The IEEE 802.16 grant-based MAC can react to QoS requests in real time which reduces the workload of the base stations and produces lower overheads since connections are aggregated.

Additionally, in order to guarantee the QoS of competing services, the fragmentation of the 802.16 Protocol Data Units allows for very large Service Data Units to be sent across frame boundaries. OFDM and OFDMA also provide error correction and interleaving in order to improve QoS. Furthermore, the adaptive modulation techniques used in WiMAX technology result in extended wireless distance coverage areas.

Security is also an important feature of WiMAX and was included in the 802.16 protocol after the failures that restricted the early IEEE 802.11 networks. Security is handled by a privacy sublayer within the WiMAX MAC. WiMAX provides a flexible means for authenticating subscriber stations and users in order to prevent unauthorized use. The 802.16 protocol provides several mechanism designed to protect the service provider and the customer from unauthorized information disclosure.

‘WiMAX Security and Quality of Service: An End-to-End Perspective’ is a collection of carefully selected articles by researchers with extensive experience with WiMAX. Determining how to provide QoS and security for different applications is a significant issue and the aim of this book is to provide readers with an in-depth discussion of security and QoS considerations in WiMAX based communications. Many books and articles have addressed WiMAX and the IEEE 802.16e protocol, but an end-to-end prospective on security and QoS has been missing. This book is split into four parts. Part A introduces an overview of the end-to-end WiMAX architecture, its protocols and system requirements. Three chapters in Part B discuss security issues in WiMAX, while in Part C five chapters examine QoS in detail. Advanced topics on WiMAX architecture, resource allocation, mobility management and interfacing WiFi and WiMAX are discussed in Part D.

Part A: Introduction

Chapter 1 provides an overview of end-to-end WiMAX network architecture. The objective of this chapter is to discuss the detail of different wireless communications technologies, mobile WiMAX, radio interface specifications for WiMAX, different interface specifications and various interoperability issues of WiMAX networks, as well as interoperability among the different WiMAX network vendors.

Part B: Security

Chapter 2 analyzes WiMAX security as defined in the different released versions of the IEEE 802.16 standards. It provides an overview of the WiMAX 802.16 networks and discusses the main security requirements to be met by a standard for broadband access. It then describes the security mechanisms that are to be guaranteed by the security sublayer and describes the weaknesses revealed in the initial versions, namely those related to fixed WiMAX. In this chapter, the security amendments made in the recent versions of mobile WiMAX are described and analyzed.

Key management in 802.16e is an important security issue and is discussed in Chapter 3. This chapter focuses specifically on the key management scheme of 802.16. Key derivation procedures and the key hierarchy of PKM version 2 are examined and discussed thoroughly. The weaknesses and countermeasures are identified and analyzed. Some comparisons with IEEE 802.11i and Third Generation (3G) mobile networks standards are also provided.

In Chapter 4, WiMAX network security is examined. The analysis is based on WiMAX Forum specification 1.2 and focuses on the standards, technical challenges the solutions for the issues of; 1) integration of authentication techniques and management of AAA (Authorization, Authentication, Accounting); 2) IP addressing and networking issues; and

3) distribution of the QoS parameters. These topics are analyzed from the perspective of the network manager and the interaction between the access network and the back-end.

Part C: Quality of Service

Chapter 5 focuses on cross-layer QoS architecture, highlighting both PMP and mesh topology aspects and the differences between them. Each type of topology presents a different means of obtaining QoS; however other important elements such as bandwidth allocation scheduling and call admission control algorithms are left to vendor implementation. This deficiency with reference to the MAC and PHY layers as well as other important issues are discussed in this chapter. The challenges for WiMAX QoS are also discussed, focusing the future of QoS in the IP world for multimedia applications.

QoS in Mobile WiMAX is addressed in Chapter 6. Here, QoS management in WiMAX networks is discussed. The analysis focuses on demonstrating how mobile WiMAX technology offers continuity of services while providing enhanced QoS guarantees in order to meet subscribers' demands. The architectural QoS requirements that have to be fulfilled during subscribers' mobility and the mechanisms constructed by the Mobile WiMAX network to provide QoS are discussed in this chapter. Service flow, the 'connection-oriented' nature of the MAC layer, the bandwidth request, and allocation procedures and the scheduling service are also examined.

Mobility Management in WiMAX Networks is addressed in Chapter 7. The authors discuss the amendment of the IEEE 802.16d-2004 standard which provides improvements related mainly to mobility management. This chapter also examines the logical architecture of a mobile WiMAX network defined by the Network Working Group1 (NWG) of the WiMAX Forum. Other topics discussed in this chapter include horizontal and vertical handover mechanisms and means for their improvement, as well as analysis of co-existence with other access technologies in networks in the future.

Chapter 8 discusses the challenges facing QoS in the handover process. This chapter describes the challenges that the handover process represents for the QoS performance indicators in full mobility scenarios. It also describes the application of QoS requirements for full mobility and the requirements relating to end-to-end performance. Timing and performance considerations in the handover process and the Media Independent Handover Initiative (MIH or IEEE802.21) are also discussed. The efficient scheduling of the handover process and its influence on handover performance, end-to-end quality of service and a handover performance analysis are the other topics presented in this chapter.

Resource Allocation in Mobile Networks is discussed in Chapter 9. Here, a technical overview is presented of the emerging Mobile WiMAX solution for broadband wireless and important issues related to QoS in Mobile WiMAX are discussed. Additionally, resource allocation in Mobile WiMAX is examined in this chapter. Issues related to scheduling and method of channel access for different Service Flows in MAC layer and burst profiles based on the AMC slot structure in OFDMA frame are examined. Multiuser resource allocation, which involves OFDMA, AMC and multiuser diversity, is presented for downlink mobile WiMAX networks. Furthermore, the Channel Aware Class Based Queue (CACBQ), which is an adaptive cross-layer for scheduling and slot allocation, is introduced.

Part D: Advanced Topics

Chapter 10 provides a discussion of QoS issues and challenges in WiMAX and WiMAX MMR networks. MAC-level QoS scheduling algorithms in WiMAX networks for multimedia traffic are also provided. This includes scheduling algorithms designed for a WiMAX mobile multi-hop relay (MMR) network. This chapter also discusses the characteristics of real-time traffic and the different codecs used for voice and video. A description of a few algorithms on uplink scheduling for real-time traffic in WiMAX networks is also provided. Additionally, MMR based WiMAX networks and downlink scheduling schemes for MMR based WiMAX networks are examined.

The Integration of WiFi and WiMAX Networks is an important issue and is discussed in Chapter 11. The deployment of an architecture that allows users to switch seamlessly between WiFi and WiMAX networks would afford several advantages to both users and service providers. However, WiMAX and WiFi networks have different protocol architectures and QoS support mechanisms; therefore an adaptation of protocol is required for their internetworking. This chapter outlines the design tenets for an interworking architecture between both WiFi and WiMAX technologies. The authors also define the various functional entities and their interconnections as well as end-to-end protocol layering in the interworking architecture, network selection and discovery and IP address allocation. Additionally, details are provided for the functional architecture and processes associated with security, QoS and mobility management.

QoS simulation and an enhanced solution for cell selection for WiMAX networks is discussed in Chapter 12. In this chapter, the authors examine the major WiMAX network simulation tools. A detailed system model for a cell selection algorithm is presented in this chapter. The authors have also performed simulation for QoS in a WiMAX network for several scenarios. An analysis of their simulation results are also provided.

The editors believe that this book is unique and significant in that it provides a complete end-to-end perspective on QoS and security issues in WiMAX and that it can be of great assistance to a large group of scientists, engineers and the wireless community with regard to the fast growing era of multimedia applications over wireless networks.

Seok-Yee Tang
Hamid R. Sharif
Peter Müller

Acknowledgement

To Ursula, Samira, Francis and Alena.

Peter Müller

To my three boys and the love of my life for her encouragement,
inspiration and support.

Hamid space

In memory of my mother.

To my husband Chong Ming, my best friend Bibi, and my sister Seok Hun.

Seok-Yee Tang

The editors would like to thank and acknowledge all authors for their contribution to the book content and their cooperation during this book's preparation process.

We would also like to thank the John Wiley & Sons Ltd team for their assistance and encouragement in making of this book.

List of Contributors

Editors

Peter Müller

IBM Zurich Research Laboratory, Switzerland;
Formerly with Siemens R&D, Switzerland

Hamid R. Sharif

University of Nebraska-Lincoln, USA

Seok Yee Tang

Think Wireless Tech Pte. Ltd., Singapore

Authors

Luca Adamo

Department of Electronics and Telecommunications
University of Florence, Italy

Marina Aguado

ETSI, Departamento de Electrónica y Telecomunicaciones
University of the Basque Country, Spain

Marion Berbineau

INRETS (Institut National de recherche sur les Transports et leur Sécurité),
Université Lille Nord de France,
Villeneuve d'Ascq, France

Debika Bhattacharyya

Head, Department of CSE
Institute of Engineering & Management, Salt Lake,
Kolkata, India

Noureddine Boudriga

Communication Networks and Security Research Laboratory (CNAS),
University of the 7th November at Carthage, Tunisia

Daniel Câmara

EURECOM
Mobile Communications Department
Sophia-Antipolis Cedex, France

Mohuya Chakraborty

Head, Department of Information Technology
Institute of Engineering & Management, Salt Lake,
Kolkata, India

Hakima Chaouchi

Telecom and Management Sud Paris
Evry cedex, France

Floriano De Rango

DEIS Department
University of Calabria, Italy

Romano Fantacci

Head of LaRT Laboratory
Department of Electronics and Telecommunications
University of Florence, Italy

Fethi Filali

QU Wireless Innovations Center
Doha, Qatar

Stefanos Gritzalis

Laboratory of Information and Communication Systems Security
Department of Information and Communication Systems Engineering
University of the Aegean, Karlovassi, Greece

Shen Gu

Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, China

Eduardo Jacob

ETSI, Departamento de Electrónica y Telecomunicaciones
University of the Basque Country, Spain

Georgios Kambourakis

Laboratory of Information and Communication Systems Security
Department of Information and Communication Systems Engineering
University of the Aegean, Karlovassi, Greece

Neila Krichene

Communication Networks and Security Research Laboratory (CNAS),
University of the 7th November at Carthage, Tunisia

Kiran Kumari

Indian Institute of Technology Madras
Chennai, India

Leonardo Maccari

Department of Electronics and Telecommunications
University of Florence, Italy

Andrea Malfitano

DEIS Department
University of Calabria, Italy

Salvatore Marano

DEIS Department
University of Calabria, Italy

Ikbal Chammakhi Msadaa

EURECOM
Mobile Communications Department
Sophia-Antipolis Cedex, France

Srinath Narasimha

Indian Institute of Technology Madras
Chennai, India

Slim Rekhis

Communication Networks and Security Research Laboratory (CNAS),
University of the 7th November at Carthage, Tunisia

Ivan Lledo Samper

Bournemouth University, UK

Krishna M. Sivalingam

Indian Institute of Technology Madras, Chennai, India;
Formerly with University of Maryland Baltimore County,
Baltimore, USA

Jiajing Wang

Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, China

Xinbing Wang

Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, China

Yuan Wu

Department of Electronic Engineering
Shanghai Jiaotong University
Shanghai, China

Tara Ali Yahiya

Computer Science Laboratory, Paris-Sud 11 University, France

List of Acronyms

2G	Second Generation mobile networks
3G	Third Generation mobile networks
3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
4G	Fourth Generation mobile networks
AAA	Authorization, Authentication and Accounting
AAS	Adaptive Antenna System
AAT	Advanced Antenna Technology
AC	Access Category
ACK	Acknowledge
ACM	Adaptive Coding and Modulation
ACs	Access Categories
AES	Advanced Encryption Standard
AIFS	Arbitration Interframe Space
AK	Authorization Key
AKA	Authentication and Key Agreement
AKID	Authentication Key Identifier
AMC	Adaptive Modulation and Coding
AMR	Adaptive Multi Rate
AP	Access Point
AR	Access Router
ARQ	Automatic Repeat Request
AS	Authentication Server
ASN	Access Service Network
ASN	Abstract Syntax Notation
ASN-GW	Access Service Network Gateway
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
AUTN	Authentication Token
AV	Authentication Vector
AWGN	Additive White Gaussian Noise
BCID	Basic Connection Identity
BE	Best Effort

BER	Bit Error Rate
BLER	Block Error Rate
BPSK	Binary Phase Shift Keying
BR	Bandwidth Request
BRAS	Broadband Access Server
BS	Base Station
BSID	Base Station Identity
BW	Bandwidth
BWA	Broadband Wireless Access
CA	Certification Authority
CAC	Call Admission Control
CACBQ	Channel Aware Class Based Queue
CAPF	Cost Adjusted Proportional Fair
CBC	Cipher Block Chaining
CBR	Constant Bit Rate
CCM	Counter with CBC-MAC
CDMA	Code Division Multiple Access
CELP	Code Excited Linear Prediction
CID	Connection Identifier
CINR	Carrier to Interference plus Noise Ratio
CK	Cipher key
CMAC	Cipher Message Authentication Code
CMIP	Client-MIP
COA	Care-of-Address
COTS	Commercial Off-The-Shelf
CPE	Consumer Premises Equipment
CPS	Common Part Sublayer
CQI	Channel Quality Indicator
CQICH	Channel Quality Indicator Channel
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CS	Convergence Sublayer
CSC	Connectivity Service Controllers
CSCI	Convergence Sublayer Classifiers
CSMA CA	Carrier Sense Multiple Access with Collision Avoidance
CSN	Connectivity Service Network
CSP	Common Part Sub-layer
CSs	Service Classes
CW	Contention Window
DAD	Duplicate Address Detection
DCD	Downlink Channel Descriptor
DCF	Distributed Coordination Function
DER	Distinguished Encoding Rule
DES	Data Encryption Standard
DFR	Decode and Forward Relay
DFS	Dynamic Frequency Selection

DHCP	Dynamic Host Configuration Protocol
DHMM	Dynamical Hierarchical Mobility Management
DIAMETER	Protocol extending RADIUS
DiffServ	Differentiated Service
DL	Downlink
DOCSIS	Data Over Cable Service Interface Specification
DoD	Department of Defence
DoS	Denial of Service
DSA-REQ	Dynamic Service Addition request
DSA-RSP	Dynamic Service Addition response
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAP-AKA	EAP-Authentication and Key Agreement
EAPOL	EAP over LAN
EAP-TTLS	EAP-Tunneled Transport Layer Security
EC	Encryption Control
EDCA	Enhanced Distributed Channel Access
EDCF	Enhanced Distributed Coordination Function
EDF	Earliest Deadline First
EFR	Enhanced Full Rate
EIK	EAP Integrity Key
EKS	Encryption Key Sequence
ertPS	Extended Real Time Polling Service
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
FA	Foreign Agent
FBack	Fast Binding Acknowledgment
FBSS	Fast Base Station Switching handover
FBU	Fast Binding Update
FCH	Frame Control Header
FDD	Frequency Division Duplex
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
FIFO	First In First Out
FPC	Fast Power Control
FTP	File Transfer Protocol
FUSC	Full Usage of Subchannels
GKDA	Group-based Key Distribution Algorithm
GKEK	Group Key Encryption Key
GKMP	Group Key Management Protocol
GMH	Generic MAC Frame Header
GPC	Grant Per Connection
GPRS	General Packet Radio Service

GSA	Group Security Association
GSAID	Group SAID
GSM FR	GSM Full rate
GSM	Global System for Mobile Communications
GTEK	Group Traffic Encryption Key
GTK	Group Transient Key
HA	Home Agent
HAck	Handover Acknowledgment
HAP	High Altitude Platform
HARQ	Hybrid Automatic Repeat Request
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
HCS	Header Check Sequence
HDR	High Data Rate
HDTV	High-definition TV
HHO	Hard Handover
HI	Handover Initiation
HIPERMAN	High Performance Radio Metropolitan Area Network
HMAC	Hash Message Authentication Code
HNSP	Home Network Service Provider
HO	Handover
HOA	Home-of-Address
HOKEY	Handover Keying (Group)
HoL	Head of Line
HSPA	High-Speed Packet Access
HSPA+	Evolved HSPA
HT	Header Type
HUF	Highest Urgency First
ICV	Integrity Checking Value
ID	Identifier
IE	Information Element
IEEE	Institute of Electrical & Electronics Engineers, Inc.
IETF	Internet Engineering Task Force
IK	Integrity Key
IKE	Internet Key Exchange (protocol)
ILBC	Internet Low Bit rate Codec
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISI	Intersymbol Interference
ISO	International Standard Organization
ISP	Internet Service Provider
ITU	International Telecommunication Union
IV	Initialization Vector
KDF	Key Derivation Function
KEK	Key Encryption Key
L2	Layer 2