IEEE Std 802.15.4™-2003

IEEE Standards

802.15.4™

IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements

Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE

Published by
The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

1 October 2003

Print: SH95127
PDF: SS95127

IEEE Standard for
Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks Specific requirements—

Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 12 May 2003

IEEE-SA Standards Board

Abstract: This standard defines the protocol and compatible interconnection for data communication devices using low data rate, low power and low complexity, short-range radio frequency (RF) transmissions in a wireless personal area network (WPAN).

Keywords: ad hoc network, low data rate, low power, LR-WPAN, mobility, personal area network (PAN), radio frequency (RF), short range, wireless, wireless personal area network (WPAN)

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2003 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1 October 2003. Printed in the United States of America.

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

Print: ISBN 0-7381-3686-7 SH95127
PDF: ISBN 0-7381-3677-5 SS95127

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

(This introduction is not part of IEEE Std 802.15.4-2003, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.4: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANS).)

IEEE Std 802.15.4-2003

This standard defines the protocol and interconnection of devices via radio communication in a personal area network (PAN). The standard uses carrier sense multiple access with a collision avoidance medium access mechanism and supports star as well as peer-to-peer topologies. The media access is contention based; however, using the optional superframe structure, time slots can be allocated by the PAN coordinator to devices with time critical data. Connectivity to higher performance networks is provided through a PAN coordinator.

This standard specifies two PHYs: an 868/915 MHz direct sequence spread spectrum (DSSS) PHY and a 2450 MHz DSSS PHY. The 2450 MHz PHY supports an over-the-air data rate of 250 kb/s, and the 868/915 MHz PHY supports over-the-air data rates of 20 kb/s and 40 kb/s. The PHY chosen depends on local regulations and user preference.

This standard contains state-of-the-art material. The area covered by this standard is undergoing evolution. Revisions are anticipated to this standard within the next few years to clarify existing material, to correct possible errors, and to incorporate new related material. Details on the contents of this standard are provided on the following pages. Information on the current revision state of this and other IEEE 802® standards may be obtained from:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O.Box 1331
Piscataway, NJ 08855-1331
USA

Participants

At the time the draft of this standard was sent to sponsor ballot, the IEEE P802.15™ Working Group had the following voting members:

Robert F. Heile, *Chair*
James D. Allen, *Vice Chair*
Patrick W. Kinney, *Secretary*
Michael D. McInnis, *Assistant Secretary and Editor*

Ian C. Gifford, *Task Group 1 Chair*
Stephen J. Shellhammer, *Task Group 2 Chair*
John R. Barr, *Task Group 3 Chair*

Patrick W. Kinney, *Task Group 4 Chair*
Phil Jamieson, *Task Group 4 Vice Chair*
José A. Gutierrez, *Task Group 4 Editor-in-Chief*
Marco Naeve, *Task Group 4 Secretary*

Monique Bourgeois, *MAC Technical Editor*
Said Moridi, *PHY Technical Editor*
Phil Jamieson, *Layer Management Technical Editor*

Copyright © 2003 IEEE. All rights reserved.

Greg Breen, *Low-Band PHY Technical Editing*
Ed Callaway, *Networking Technical Editing*
Paul Gorday, *High-Band PHY Technical Editing*
Marco Naeve, *General Description Technical Editing*
David Cypher, *PICs/SDLs Technical Editing*
Robert Poor, *Coexistence Technical Editing*
Farron Dacus, *Regulatory Technical Editing*

Roberto Aiello
Masaaki Akahane
Richard Alfvin
James D. Allen
Arun Arunachalam
Naiel Askar
Venkat I. Bahl
Daniel Bailey
Jay Bain
James Baker
Jaiganesh Balakrishnan
John R. Barr
Anuj Batra
Timothy Blaney
Kenneth Boehike
Stan Bottoms
Monique Bourgeois
Mark V. Bowles
Chuck Brabenac
Ed Callaway
Soo-Young Chang
Francois Po_Shin Chin
Aik Chindapol
Craig Conkling
David Cypher
Anand Dabak
Kai Dombrowski
Mary DuVal
Michael Dydyk
Jason L. Ellis
Mark W. Fidler
Jeff R. Foerster
David S. Furuno
Pierre Gandolfo
Atul Garg
Ian C.Gifford
James Gilb
Nada Golmie
Paul Gorday
José A. Gutierrez
Yasuo Harada
Allen Heberling
Robert F. Heile
Barry Herold
Robert Y. Huang
Eran Igler
Katsumi Ishii
Phil Jamieson
Jeyhan Karaoguz
Masami Katagiri
Joy H. Kelly
Stuart J. Kerry
Yongsuk Kim
Young Hwan Kim
Patrick W. Kinney
Günter Kleindl
Bruce P. Kraemer
DoHoon Kwon
Jim Lansford
David Leeper
Liang Li
Yeong-Chang Maa
Steven March
Ralph Mason
Michael D. McInnis
Jim Meyer
Leonard E. Miller
Akira Miura
Andreas Molisch
Antonio Mondragon
Tony Morelli
Said Moridi
Marco Naeve
Chiu Ngo
Kei Obara
Knut Odman
John B. Pardee
Jongun Park
Dave Patton
Marcus Pendergrass
Robert D. Poor
Gregg Rasor
Ivan Reede
Jim Richards
Glyn Roberts
Richard Roberts
William Roberts
Chris Rogers
Philippe Rouzet
Chandos Rypinski
John H. Santhoff
Mark Schrader
Tom Schuster
Erik Schylander
Michael Seals
Stephen J. Shellhammer
Nick Shepherd
Gadi Shor
William Shvodian
Thomas Siep
Kazimierz Siwiak
Carl Stevenson
Rene Struik
Shigeru Sugaya
Kazuhisa Takamura
Katsumi Takaoka
Teik-Kheong Tan
Larry Taylor
Stephen E. Taylor
Hans vanLeeuwen
Ritesh Vishwakarma
Thierry Walrant
Jing Wang
Fijio Watanabe
Mathew Welborn
Richard Wilson
Stephen Wood
Edward G. Woodrow
Hirohisa Yamaguchi
Amos Young
Song-Lin Young
Nakache Yves-paul
Jim Zyren

Copyright © 2003 IEEE. All rights reserved.

Major contributions were received from the following individuals:

Tony Adamson
David Archer
David Avery
Venkat Bahl
Daniel Bailey
Edul Batliwala
Pratik Bose
Boaz Carmeli
Farron Dacus
Martin Digon
Ian C. Gifford

Ed Hogervorst
Stephen Korfhage
Charles Luebke
Masahiro Maeda
Ian Marsden
Chris Marshall
Paul Marshall
Fred Martin
Ralph Mason
Rod Miller
Phil Rudland

Niels Schutten
Nick Shepherd
Ari Singer
Ralph D'Souza
Carl Stevenson
Mark Tilinghast
Hans Van Leeuwen
Jacco van Muiswinkel
Luis Pereira
Richard Wilson
Wim Zwart

The following members of the balloting committee voted on this standard:

Morris Balamut
John R. Barr
Shlomo Berliner
Pratik Bose
Monique Bourgeois
Daniel Brueske
Ed Callaway
Yawgeng Chau
Todor Cooklev
Guru Dutt Dhingra
Thomas Dineen
Dominic Espejo
Avraham Freedman
Ian C. Gifford
James Gilb
Paul Gorday
Rajugopal Gubbi
José A. Gutierrez

Simon Harrison
Robert F. Heile
Phil Jamieson
Tony Jeffree
Niket Jindal
James Kemerling
Stuart Kerry
Brian Kiernan
Yongsuk Kim
Patrick W. Kinney
Cees Klik
Gregory Luri
Roger Marks
Peter Martini
Ralph Mason
Lance McBride
Michael D. McInnis
George Miao

Hiroshi Miyano
Said Moridi
Marco Naeve
Paul Nikolich
Erwin Noble
Timothy O'Farrell
Bob O'Hara
Jack Pardee
Subbu Ponnuswamy
Robert Poor
Vikram Punj
Jon Rosdahl
Mark Schrader
Stephen J. Shellhammer
Jerry Thrasher
Johannes Van Leeuwen
Edward Woodrow
Jung Yee
Oren Yuen

When the IEEE-SA Standards Board approved this standard on 12 May 2003, it had the following membership:

Don Wright, *Chair*
Howard M. Frazier, *Vice Chair*
Judith Gorman, *Secretary*

H. Stephen Berger
Joe Bruder
Bob Davis
Richard DeBlasio
Julian Forster*
Toshio Fukuda
Arnold M. Greenspan
Raymond Hapeman
Donald M. Heirman
Laura Hitchcock
Richard H. Hulett
Anant Jain
Lowell G. Johnson
Joseph L. Koepfinger*
Tom McGean
Steve Mills
Daleep C. Mohla
William J. Moylan
Paul Nikolich
Gary Robinson
Malcolm V. Thaden
Geoffrey O. Thompson
Doug Topping
Howard L. Wolfman

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Alan Cookson, *NIST Representative*
Satish K. Aggarwal, *NRC Representative*

Michelle Turner
IEEE Standards Project Editor

CONTENTS

Copyright © 2003 IEEE. All rights reserved.

Copyright © 2003 IEEE. All rights reserved.

IEEE Standard for
Information technology—
Telecommunications and information
exchange between systems—
Local and metropolitan area networks—
Specific requirements

Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)

1. Overview

Wireless personal area networks (WPANs) are used to convey information over relatively short distances. Unlike wireless local area networks (WLANs), connections effected via WPANs involve little or no infrastructure. This feature allows small, power-efficient, inexpensive solutions to be implemented for a wide range of devices.

This document defines a standard for a low-rate WPAN (LR-WPAN).

1.1 Scope

The scope of this project is to define the physical layer (PHY) and medium access control (MAC) sublayer specifications for low data rate wireless connectivity with fixed, portable, and moving devices with no battery or very limited battery consumption requirements typically operating in the personal operating space (POS) of 10 m. It is foreseen that, depending on the application, a longer range at a lower data rate may be an acceptable trade-off.

It is the intent of this project to work toward a level of coexistence with other wireless devices in conjunction with Coexistence Task Groups, such as 802.15.2™ and 802.11™/ETSI-BRAN/MMAC 5GSG.

1.2 Purpose

The purpose of this document is to provide a standard for ultra-low complexity, ultra-low cost, ultra-low power consumption, and low data rate wireless connectivity among inexpensive devices. The raw data rate will be high enough (maximum of 250 kb/s) to satisfy a set of simple needs such as interactive toys, but scalable down to the needs of sensor and automation needs (20 kb/s or below) for wireless communications.

Copyright © 2003 IEEE. All rights reserved.

Copyright © 2003 IEEE. All rights reserved.

2. References

The following standards and specifications contain provisions which, through references in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the references listed below.

2.1 IEEE documents[1]

IEEE Std 802®-1990, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.

2.2 ISO documents[2]

ISO/IEC 7498-1:1994, Information technology—Open systems interconnection—Basic reference model: The basic model.

ISO/IEC 8802-2:1998 (IEEE Std 802.2™, 1998 Edition), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.

ISO/IEC 9646-1:1994, Information technology—Open systems interconnection—Conformance testing methodology and framework— Part 1: General concepts.

ISO/IEC 9646-7:1995 (ITU-T Rec. X.296 (1994)), Information technology—Open systems interconnection—Conformance testing methodology and framework—Part 7: Implementation conformance statements.

ISO/IEC 10039:1991, Information technology—Open systems interconnection—Local area networks—Medium Access Control (MAC) service definition.

ISO/IEC 15802-1:1995, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 1: Medium Access Control (MAC) service definition.

2.3 ITU-T documents[3]

ITU-T Recommendation X.210, Service Definitions—Open Systems Interconnection—Layer Service Definition Conventions.

ITU-T Recommendation Z.100, CCITT Specification and Description Language (SDL).

2.4 Other documents

NIST FIPS Pub 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, U.S. Department of Commerce/N.I.S.T., November 2001.[4]

[1] IEEE Publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA http://standards.ieee.org/catalog/.

[2] ISO and ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse http://www.iso.ch/. They are also available in the Unites States from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA http://www.ansi.org.

[3] ITU-T publications are available from the International Telecommunications Union, Place des Nations, CH-1211, Geneva 20, Switzerland/Suisse (http://www.itu.int/).

[4] FIPS publications are available from the National Technical Information Service (NTIS), U. S. Dept. of Commerce, 5285 Port Royal Rd., Springfield, VA 22161 (http://www.ntis.org/).

Copyright © 2003 IEEE. All rights reserved.

Copyright © 2003 IEEE. All rights reserved.

3. Definitions

For the purposes of this standard, the following terms and definitions apply. Terms not defined in this clause can be found in the *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition [B1].

3.1 access control list (ACL): A table used by a device to determine which devices are authorized to perform a specific function.

3.2 ad hoc network: An ad hoc network is typically created in a spontaneous manner. The principal characteristic of an ad hoc network is its limited temporal and spatial extent.

3.3 alternate personal area network (PAN) coordinator: A coordinator that is capable of replacing the personal area network (PAN) coordinator, should it leave the network for any reason. A PAN can have zero or more alternate PAN coordinators.

3.4 association: The service used to establish a device's membership in a wireless personal area network (WPAN).

3.5 authentic data: Data whose source is verifiable through cryptographic protection.

3.6 authentication: The service used to establish the identity of one device as a member of the set of devices authorized to communicate securely to other devices in the set.

3.7 confidentiality: Assurance that communicated data remain private to the parties for whom the data are intended.

3.8 coordinator: An full-function device (FFD) that is configured to provide synchronization services through the transmission of beacons. If a coordinator is the principal controller of a personal area network (PAN), it is called the PAN coordinator.

3.9 coverage area: The area where two or more IEEE 802.15.4 ™ units can exchange messages with acceptable quality and performance.

3.10 data integrity: Assurance that the data have not been modified from their original form.

3.11 device: Any entity [reduced-function device (RFD) or full-function device (FFD)] containing an implementation of the IEEE 802.15.4 medium access control (MAC) and physical interface to the wireless medium.

3.12 disassociation: The service that removes an existing association.

3.13 frame: The format of aggregated bits from a medium access control (MAC) sublayer entity that are transmitted together in time.

3.14 full-function device (FFD): A device capable of operating as a coordinator or device and implementing the complete protocol set.

3.15 integrity code: A data string generated using a symmetric key that is typically appended to data in order to provide data integrity and source authentication (also called a *message integrity code*).

3.16 key establishment: A public-key process by which two entities securely establish a symmetric key that is known only by the participating entities.

Copyright © 2003 IEEE. All rights reserved.

3.17 key management: Methods for controlling keying material throughout the life cycle of the low-rate wireless personal area network (LR-WPAN) including creation, distribution, and destruction.

3.18 key transport: A process by which an entity sends a key to another entity.

3.19 logical channel: One of a variety of channels on a physical link.

3.20 message integrity code: *See:* **integrity code**.

3.21 mobile device: A device that uses network communications while in motion.

3.22 m-sequence: Maximal length linear feedback shift register sequence.

3.23 nonce: A time stamp, a counter, or a special marker intended to prevent unauthorized replay.

3.24 orphaned device: A device that has lost contact with its associated personal area network (PAN) coordinator.

3.25 personal area network (PAN) coordinator: A coordinator that is the principal controller of a personal area network (PAN). An IEEE 802.15.4 network has exactly one PAN coordinator.

3.26 payload data: The contents of a data message that is being transmitted.

3.27 payload protection: The generic term for providing security services on payload data, including confidentiality, data integrity, and authentication.

3.28 protocol data unit (PDU): The unit of data exchanged between two peer entities.

3.29 packet: The format of aggregated bits that are transmitted together in time across the physical medium.

3.30 personal operating space (POS): The space about a person or object that is typically about 10 m in all directions and envelops the person or object whether stationary or in motion.

3.31 portable device: A device that may be moved from location to location, but uses network communications only while at a fixed location.

3.32 pseudo-random number generation: The process of generating a deterministic sequence of bits from a given seed that has the statistical properties of a random sequence of bits when the seed is not known.

3.33 random number generator: A device that provides a sequence of bits that is unpredictable.

3.34 reduced-function device (RFD): A device operating with a minimal implementation of the IEEE 802.15.4 protocol.

3.35 security suite: A group of security operations designed to provide security services on medium access control (MAC) frames.

3.36 self-organizing: The ability of network nodes to detect the presence of other nodes and to organize into a structured, functioning network without human intervention.

3.37 self-healing: The ability of the network to detect, and recover from, faults appearing in either network nodes or communication links, without human intervention.

3.38 service data unit (SDU): Information that is delivered as a unit through a service access point (SAP).

Copyright © 2003 IEEE. All rights reserved.

3.39 symmetric key: A secret key that is shared between two or more parties that may be used for encryption/decryption or integrity protection/integrity verification depending on its intended use.

3.40 transaction: The exchange of related, consecutive frames between two peer medium access control (MAC) entities, required for a successful transmission of a MAC command or data frame**.**

3.41 wireless medium (WM): The medium used to implement the transfer of protocol data units (PDUs) between peer physical layer (PHY) entities of a low-rate wireless personal area network (LR-WPAN).

Copyright © 2003 IEEE. All rights reserved.

Copyright © 2003 IEEE. All rights reserved.

4. Acronyms and abbreviations

ACL	access control list
AES	advanced encryption standard
ASN.1	Abstract Syntax Notation Number 1
AWGN	additive white Gaussian noise
BE	backoff exponent
BER	bit error rate
BI	beacon interval
BO	beacon order
BPSK	binary phase-shift keying
BSN	beacon sequence number
CAP	contention access period
CBC-MAC	cipher block chaining message authentication code
CCA	clear channel assessment
CCM	CTR + CBC-MAC
CFP	contention-free period
CID	cluster identifier
CLH	cluster head
CRC	cyclic redundancy check
CSMA-CA	carrier sense multiple access with collision avoidance
CTR	counter mode
CW	contention window (length)
DSN	data sequence number
DSSS	direct sequence spread spectrum
ED	energy detection
EIRP	effective isotropic radiated power
EMC	electromagnetic compatibility
ERP	effective radiated power
EVM	error-vector magnitude
FCS	frame check sequence
FFD	full-function device
FH	frequency hopping
FHSS	frequency hopping spread spectrum
GTS	guaranteed time slot
IFS	interframe space or spacing
IR	infrared
ISM	industrial, scientific, and medical
IUT	implementation under test
LAN	local area network
LIFS	long interframe spacing
LLC	logical link control
LQ	link quality
LQI	link quality indication
LPDU	LLC protocol data unit
LR-WPAN	low-rate wireless personal area network

Copyright © 2003 IEEE. All rights reserved.

LSB	least significant bit
MAC	medium access control
MCPS	MAC common part sublayer
MCPS-SAP	MAC common part sublayer-service access point
MFR	MAC footer
MHR	MAC header
MIC	message integrity code
MLME	MAC sublayer management entity
MLME-SAP	MAC sublayer management entity-service access point
MSB	most significant bit
MSC	message sequence chart
MPDU	MAC protocol data unit
MSDU	MAC service data unit
NB	number of backoff (periods)
O-QPSK	offset quadrature phase-shift keying
OSI	open systems interconnection
PAN	personal area network
PANPC	personal area networkcomputer
PD-SAP	PHY data service access point
PDU	protocol data unit
PER	packet error rate
PHR	PHY header
PHY	physical layer
PIB	PAN information base
PICS	protocol implementation conformance statement
PLME	physical layer management entity
PLME-SAP	physical layer management entity-service access point
PN	pseudo-random noise
POS	personal operating space
PPDU	PHY protocol data unit
PRF	pulse repetition frequency
PSD	power spectral density
PSDU	PHY service data unit
ppm	parts per million
RF	radio frequency
RFD	reduced-function device
RSSI	received signal strength indication
RX	receive or receiver
SAP	service access point
SD	superframe duration
SDL	specification and description language
SPDU	SSCS protocol data units
SDU	service data unit
SFD	start-of-frame delimiter
SHR	synchronization header
SIFS	short interframe spacing

SO	superframe order
SRD	short-range device
SSCS	service specific convergence sublayer
SUT	system under test
TRX	transceiver
TX	transmit or transmitter
UML	unified modeling language
WLAN	wireless local area network
WPAN	wireless personal area network

Copyright © 2003 IEEE. All rights reserved.

Copyright © 2003 IEEE. All rights reserved.

5. General description

A LR-WPAN is a simple, low-cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. The main objectives of an LR-WPAN are ease of installation, reliable data transfer, short-range operation, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol.

Some of the characteristics of an LR-WPAN are

- Over-the-air data rates of 250 kb/s, 40 kb/s, and 20 kb/s
- Star or peer-to-peer operation
- Allocated 16 bit short or 64 bit extended addresses
- Allocation of guaranteed time slots (GTSs)
- Carrier sense multiple access with collision avoidance (CSMA-CA) channel access
- Fully acknowledged protocol for transfer reliability
- Low power consumption
- Energy detection (ED)
- Link quality indication (LQI)
- 16 channels in the 2450 MHz band, 10 channels in the 915 MHz band, and 1 channel in the 868 MHz band

Two different device types can participate in an LR-WPAN network; a full-function device (FFD) and a reduced-function device (RFD). The FFD can operate in three modes serving as a personal area network (PAN) coordinator, a coordinator, or a device. An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD. An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor; they do not have the need to send large amounts of data and may only associate with a single FFD at a time. Consequently, the RFD can be implemented using minimal resources and memory capacity.

5.1 Components of the IEEE 802.15.4 WPAN

A system conforming to IEEE 802.15.4 consists of several components. The most basic is the device. A device can be an RFD or an FFD. Two or more devices within a POS communicating on the same physical channel constitute a WPAN. However, a network shall include at least one FFD, operating as the PAN coordinator.

An IEEE 802.15.4 network is part of the WPAN family of standards although the coverage of an LR-WPAN may extend beyond the POS, which typically defines the WPAN.

A well-defined coverage area does not exist for wireless media because propagation characteristics are dynamic and uncertain. Small changes in position or direction may result in drastic differences in the signal strength or quality of the communication link. These effects occur whether a device is stationary or mobile as moving objects may impact station-to-station propagation.

5.2 Network topologies

Depending on the application requirements, the LR-WPAN may operate in either of two topologies: the star topology or the peer-to-peer topology. Both are shown in Figure 1. In the star topology the communication is established between devices and a single central controller, called the PAN coordinator. A device typically has some associated application and is either the initiation point or the termination point for network communications. A PAN coordinator may also have a specific application, but it can be used to initiate, terminate, or route communication around the network. The PAN coordinator is the primary controller of the

Copyright © 2003 IEEE. All rights reserved.

PAN. All devices operating on a network of either topology shall have unique 64 bit extended addresses. This address can be used for direct communication within the PAN, or it can be exchanged for a short address allocated by the PAN coordinator when the device associates. The PAN coordinator may be mains powered, while the devices will most likely be battery powered. Applications that benefit from a star topology include home automation, personal computer (PC) peripherals, toys and games, and personal health care.

The peer-to-peer topology also has a PAN coordinator; however, it differs from the star topology in that any device can communicate with any other device as long as they are in range of one another. Peer-to-peer topology allows more complex network formations to be implemented, such as mesh networking topology. Applications such as industrial control and monitoring, wireless sensor networks, asset and inventory tracking, intelligent agriculture, and security would benefit from such a network topology. A peer-to-peer network can be ad hoc, self-organizing and self-healing. It may also allow multiple hops to route messages from any device to any other device on the network. Such functions can be added at the network layer, but are not part of this standard.

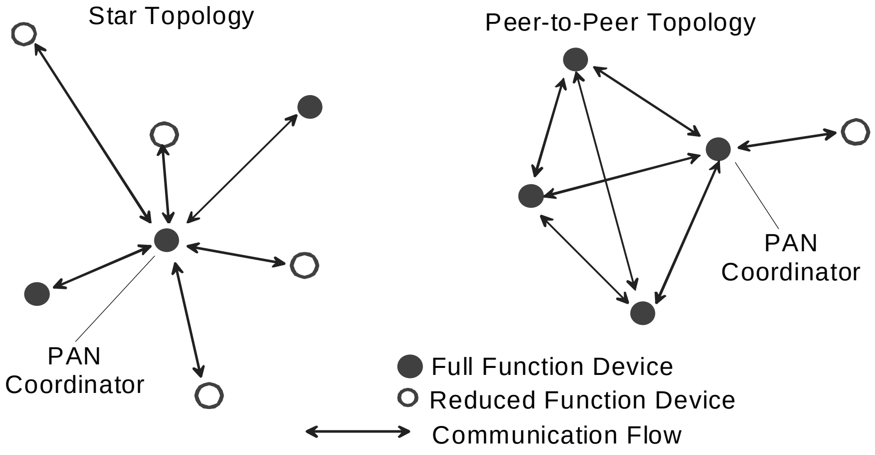

Figure 1—Star and peer-to-peer topology examples

Each independent PAN will select a unique identifier. This PAN identifier allows communication between devices within a network using short addresses and enables transmissions between devices across independent networks.

5.2.1 Network formation

The network formation is performed by the network layer, which is not part of this standard. However, this subclause provides a brief overview on how each supported topology may be formed.

5.2.1.1 Star network formation

The basic structure of a star network can be seen in Figure 1. After an FFD is activated for the first time, it may establish its own network and become the PAN coordinator. All star networks operate independently from all other star networks currently in operation. This is achieved by choosing a PAN identifier, which is not currently used by any other network within the radio sphere of influence. Once the PAN identifier is chosen, the PAN coordinator can allow other devices to join its network; both FFDs and RFDs may join the network. The detailed procedure can be found in 7.5.2 and 7.5.3.

Copyright © 2003 IEEE. All rights reserved.

5.2.1.2 Peer-to-peer network formation

In a peer-to-peer topology, each device is capable of communicating with any other device within its radio sphere of influence. One device will be nominated as the PAN coordinator, for instance, by virtue of being the first device to communicate on the channel. Further network structures can be constructed out of the peer-to-peer topology and may impose topological restrictions on the formation of the network.

An example of the use of the peer-to-peer communications topology is the cluster-tree. The cluster-tree network is a special case of a peer-to-peer network in which most devices are FFDs. An RFD may connect to a cluster tree network as a leave node at the end of a branch, because it may only associate with one FFD at a time. Any of the FFDs may act as a coordinator and provide synchronization services to other devices or other coordinators. Only one of these coordinators can be the overall PAN coordinator, which may have greater computational resources than any other device in the PAN. The PAN coordinator forms the first cluster by establishing itself as the cluster head (CLH) with a cluster identifier (CID) of zero, choosing an unused PAN identifier, and broadcasting beacon frames to neighboring devices. A candidate device receiving a beacon frame may request to join the network at the CLH. If the PAN coordinator permits the device to join, it will add the new device as a child device in its neighbor list. Then the newly joined device will add the CLH as its parent in its neighbor list and begin transmitting periodic beacons; other candidate devices may then join the network at that device. If the original candidate device is not able to join the network at the CLH, it will search for another parent device. The detailed procedures describing how a PAN is started and how devices join a PAN can be found in 7.5.2 and 7.5.3. The simplest form of a cluster tree network is a single cluster network, but larger networks are possible by forming a mesh of multiple neighboring clusters. Once predetermined application or network requirements are met, the PAN coordinator may instruct a device to become the CLH of a new cluster adjacent to the first one. Other devices gradually connect and form a multicluster network structure, such as the one seen in Figure 2. The lines in Figure 2 represent the parent-child relationships of the devices and not the communication flow. The advantage of a multicluster structure is increased coverage area, while the disadvantage is an increase in message latency.

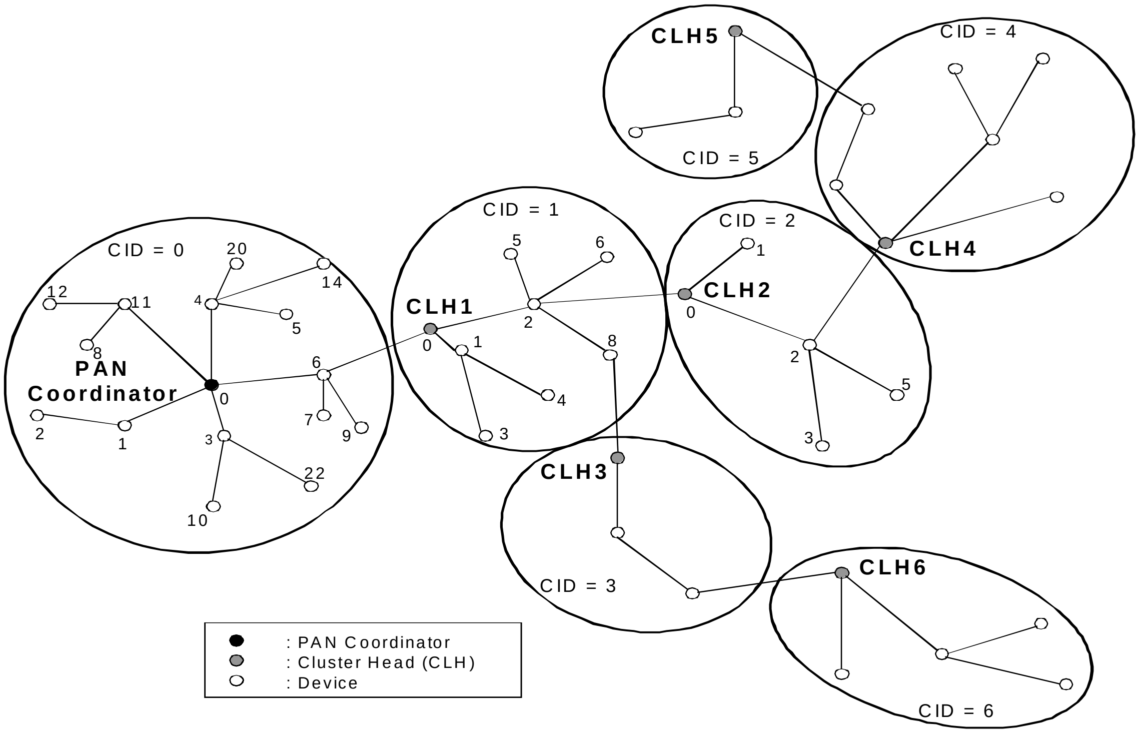

Figure 2—Cluster tree network

5.3 Architecture

The LR-WPAN architecture is defined in terms of a number of blocks in order to simplify the standard. These blocks are called layers. Each layer is responsible for one part of the standard and offers services to the higher layers. The layout of the blocks is based on the open systems interconnection (OSI) seven-layer model (see 2.2).

The interfaces between the layers serve to define the logical links that are described in this standard.

An LR-WPAN device comprises a PHY, which contains the radio frequency (RF) transceiver along with its low-level control mechanism, and a MAC sublayer that provides access to the physical channel for all types of transfer. Figure 3 shows these blocks in a graphical representation, which are described in more detail in 5.3.1 and 5.3.2.

The upper layers, shown in Figure 3, consist of a network layer, which provides network configuration, manipulation, and message routing, and an application layer, which provides the intended function of the device. The definition of these upper layers is outside the scope of this standard. An IEEE 802.2™ Type 1 logical link control (LLC) (see 2.1) can access the MAC sublayer through the service specific convergence sublayer (SSCS), defined in Annex A. The LR-WPAN architecture can be implemented either as embedded devices or as devices requiring the support of an external device such as a PC.

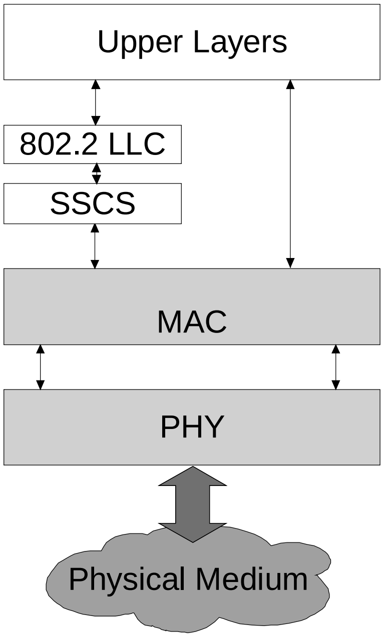

Figure 3—LR-WPAN device architecture

5.3.1 PHY

The PHY provides two services: the PHY data service and the PHY management service interfacing to the physical layer management entity (PLME). The PHY data service enables the transmission and reception of PHY protocol data units (PPDUs) across the physical radio channel.

Clause 6 contains the specifications for the PHY.

Copyright © 2003 IEEE. All rights reserved.

The features of the PHY are activation and deactivation of the radio transceiver, ED, LQI, channel selection, clear channel assessment (CCA), and transmitting as well as receiving packets across the physical medium. The radio shall operate at one of the following license-free bands:

- 868–868.6 MHz (e.g., Europe),
- 902–928 MHz (e.g., North America) or
- 2400–2483.5 MHz (worldwide).

Refer to Annex F for an informative summary of regulatory requirements.

5.3.2 MAC sublayer

The MAC sublayer provides two services: the MAC data service and the MAC management service interfacing to the MAC sublayer management entity (MLME) service access point (SAP) (known as MLME-SAP). The MAC data service enables the transmission and reception of MAC protocol data units (MPDUs) across the PHY data service.

The features of the MAC sublayer are beacon management, channel access, GTS management, frame validation, acknowledged frame delivery, association, and disassociation. In addition, the MAC sublayer provides hooks for implementing application appropriate security mechanisms.

Clause 7 contains the specifications for the MAC sublayer.

5.4 Functional overview

A brief overview of the general functions of a LR-WPAN is given in 5.4.1 through 5.4.6 and includes information on the superfame structure, the data transfer model, the frame structure, robustness, power consumption considerations, and security.

5.4.1 Superframe structure

The LR-WPAN standard allows the optional use of a superframe structure. The format of the superframe is defined by the coordinator. The superframe is bounded by network beacons, is sent by the coordinator (see Figure 4), and is divided into 16 equally sized slots. The beacon frame is transmitted in the first slot of each superframe. If a coordinator does not wish to use a superframe structure, it may turn off the beacon transmissions. The beacons are used to synchronize the attached devices, to identify the PAN, and to describe the structure of the superframes. Any device wishing to communicate during the contention access period (CAP) between two beacons shall compete with other devices using a slotted CSMA-CA mechanism. All transactions shall be completed by the time of the next network beacon.

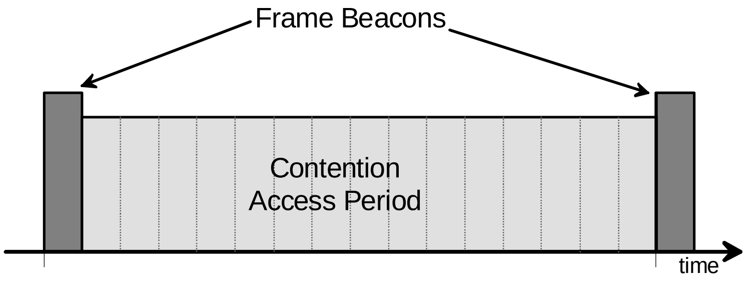

Figure 4—Superframe structure without GTSs

The superframe can have an active and an inactive portion. During the inactive portion, the coordinator shall not interact with its PAN and may enter a low-power mode.

Copyright © 2003 IEEE. All rights reserved.

For low-latency applications or applications requiring specific data bandwidth, the PAN coordinator may dedicate portions of the active superframe to that application. These portions are called guaranteed time slots (GTSs). The GTSs form the contention-free period (CFP), which always appears at the end of the active superframe starting at a slot boundary immediately following the CAP, as shown in Figure 5. The PAN coordinator may allocate up to seven of these GTSs, and a GTS may occupy more than one slot period. However, a sufficient portion of the CAP shall remain for contention-based access of other networked devices or new devices wishing to join the network. All contention-based transactions shall be complete before the CFP begins. Also each device transmitting in a GTS shall ensure that its transaction is complete before the time of the next GTS or the end of the CFP. More information on the superframe structure can be found in 7.5.1.1.

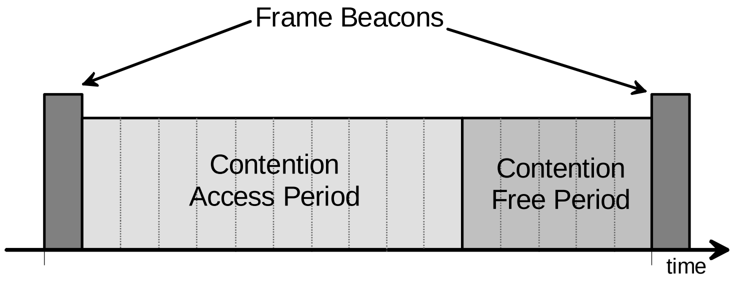

Figure 5—Superframe structure with GTSs

5.4.2 Data transfer model

Three types of data transfer transactions exist. The first one is the data transfer to a coordinator in which a device transmits the data. The second transaction is the data transfer from a coordinator in which the device receives the data. The third transaction is the data transfer between two peer devices. In star topology only two of these transactions are used, because data may be exchanged only between the coordinator and a device. In a peer-to-peer topology data may be exchanged between any two devices on the network; consequently all three transactions may be used in this topology.

The mechanisms for each transfer type depend on whether the network supports the transmission of beacons. A beacon-enabled network is used for supporting low-latency devices, such as PC peripherals. If the network does not need to support such devices, it can elect not to use the beacon for normal transfers. However, the beacon is still required for network association. The structure of the frames used for the data transfer is described in 5.4.3.

5.4.2.1 Data transfer to a coordinator

This data transfer transaction is the mechanism to transfer data from a device to a coordinator.

When a device wishes to transfer data to a coordinator in a beacon-enabled network, it first listens for the network beacon. When the beacon is found, the device synchronizes to the superframe structure. At the appropriate point, the device transmits its data frame, using slotted CSMA-CA, to the coordinator. The coordinator acknowledges the successful reception of the data by transmitting an optional acknowledgment frame. The transaction is now complete. This sequence is summarized in Figure 6.

Copyright © 2003 IEEE. All rights reserved.

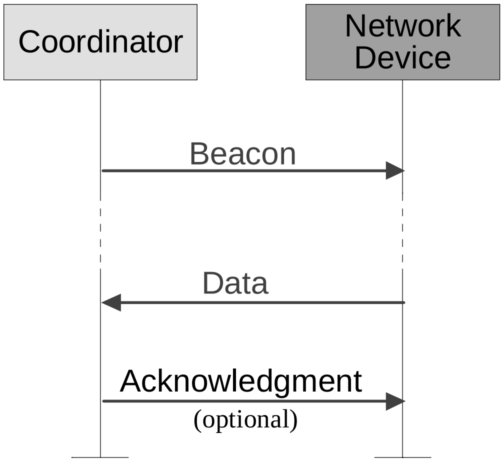

Figure 6—Communication to a coordinator in a beacon-enabled network

When a device wishes to transfer data in a nonbeacon-enabled network, it simply transmits its data frame, using unslotted CSMA-CA, to the coordinator. The coordinator acknowledges the successful reception of the data by transmitting an optional acknowledgment frame. The transaction is now complete. This sequence is summarized in Figure 7.

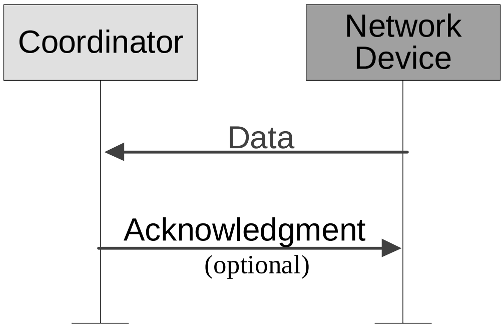

Figure 7—Communication to a coordinator in a nonbeacon-enabled network

5.4.2.2 Data transfer from a coordinator

This data transfer transaction is the mechanism for transferring data from a coordinator to a device.

When the coordinator wishes to transfer data to a device in a beacon-enabled network, it indicates in the network beacon that the data message is pending. The device periodically listens to the network beacon and, if a message is pending, transmits a MAC command requesting the data, using slotted CSMA-CA. The coordinator acknowledges the successful reception of the data request by transmitting an optional acknowledgment frame. The pending data frame is then sent using slotted CSMA-CA. The device acknowledges the successful reception of the data by transmitting an acknowledgment frame. The transaction is now complete. Upon receiving the acknowledgement, the message is removed from the list of pending messages in the beacon. This sequence is summarized in Figure 8.

Copyright © 2003 IEEE. All rights reserved.

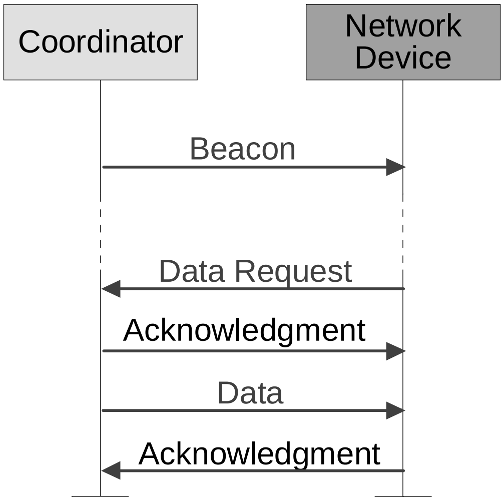

Figure 8—Communication from a coordinator a beacon-enabled network

When a coordinator wishes to transfer data to a device in a nonbeacon-enabled network, it stores the data for the appropriate device to make contact and request the data. A device may make contact by transmitting a MAC command requesting the data, using unslotted CSMA-CA, to its coordinator at an application-defined rate. The coordinator acknowledges the successful reception of the data request by transmitting an acknowledgment frame. If data are pending, the coordinator transmits the data frame, using unslotted CSMA-CA, to the device. If data are not pending, the coordinator transmits a data frame with a zero-length payload to indicate that no data were pending. The device acknowledges the successful reception of the data by transmitting an acknowledgment frame. The transaction is complete. This sequence is summarized in Figure 9.

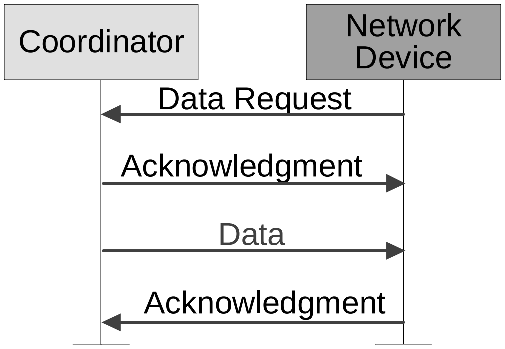

Figure 9—Communication from a coordinator in a nonbeacon-enabled network

5.4.2.3 Peer-to-peer data transfers

In a peer-to-peer PAN, every device may communicate with every other device in its radio sphere of influence. In order to do this effectively, the devices wishing to communicate will need to either receive constantly or synchronize with each other. In the former case, the device can simply transmit its data using unslotted CSMA-CA. In the latter case, other measures need to be taken in order to achieve synchronization. Such measures are beyond the scope of this standard.

Copyright © 2003 IEEE. All rights reserved.

5.4.3 Frame structure

The frame structures have been designed to keep the complexity to a minimum while at the same time making them sufficiently robust for transmission on a noisy channel. Each successive protocol layer adds to the structure with layer-specific headers and footers. The LR-WPAN defines four frame structures:

— A beacon frame, used by a coordinator to transmit beacons
— A data frame, used for all transfers of data
— An acknowledgment frame, used for confirming successful frame reception
— A MAC command frame, used for handling all MAC peer entity control transfers

The structure of each of the four frame types is described in 5.4.3.1 through 5.4.3.4. The diagrams in these subclauses illustrate the fields that are added by each layer of the protocol. The packet structure illustrated below the PHY represents the bits that are actually transmitted on the physical medium.

5.4.3.1 Beacon frame

Figure 10 shows the structure of the beacon frame, which originates from the MAC sublayer. A coordinator can transmit network beacons in a beacon-enabled network. The MAC service data unit (MSDU) contains the superframe specification, pending address specification, address list, and beacon payload fields (see 7.2.2.1). The MSDU is prefixed with a MAC header (MHR) and appended with a MAC footer (MFR). The MHR contains the MAC frame control fields, beacon sequence number (BSN), and addressing information fields. The MFR contains a 16 bit frame check sequence (FCS). The MHR, MSDU, and MFR together form the MAC beacon frame (i.e., MPDU).

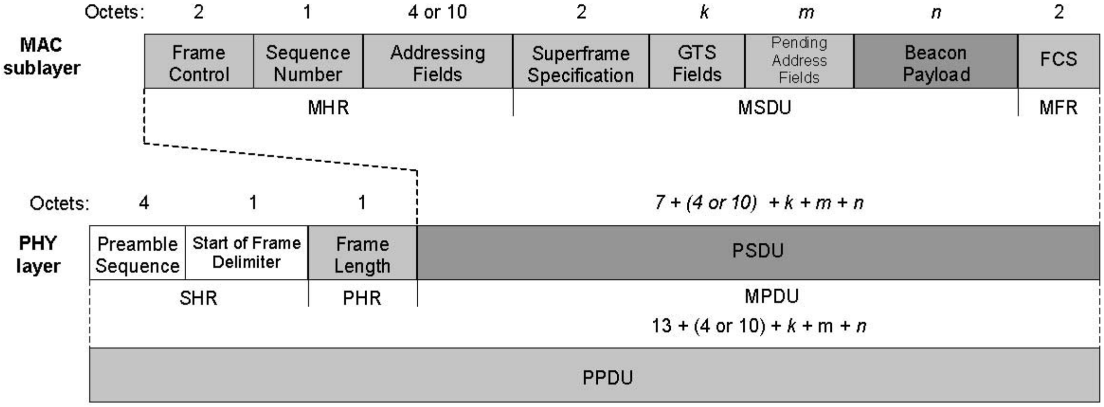

Figure 10—Schematic view of the beacon frame

The MPDU is then passed to the PHY as the PHY beacon packet payload (PHY service data unit, PSDU). The PSDU is prefixed with a synchronization header (SHR), containing the preamble sequence and start-of-frame delimiter (SFD) fields, and a PHY header (PHR) containing the length of the PSDU in octets. The preamble sequence enables the receiver to achieve symbol synchronization. The SHR, PHR, and PSDU together form the PHY beacon packet, (i.e., PPDU).

5.4.3.2 Data frame

Figure 11 shows the structure of the data frame, which originates from the upper layers.

Copyright © 2003 IEEE. All rights reserved.

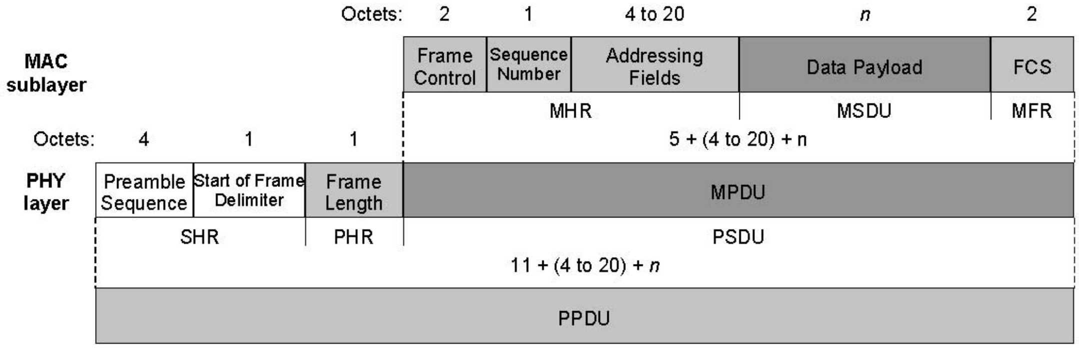

Figure 11—Schematic view of the data frame

The data payload is passed to the MAC sublayer and is referred to as the MSDU. The MSDU is prefixed with an MHR and appended with an MFR. The MHR contains the frame control, sequence number, and addressing information fields. The MFR is composed of a 16 bit FCS. The MHR, MSDU, and MFR together form the MAC data frame, (i.e., MPDU).

The MPDU is passed to the PHY as the PHY data frame payload, (i.e., PSDU). The PSDU is prefixed with an SHR, containing the preamble sequence and SFD fields, and a PHR containing the length of the PSDU in octets. The preamble sequence and the data SFD enable the receiver to achieve symbol synchronization. The SHR, PHR, and PSDU together form the PHY data packet, (i.e., PPDU).

5.4.3.3 Acknowledgment frame

Figure 12 shows the structure of the acknowledgment frame, which originates from the MAC sublayer. The MAC acknowledgment frame is constructed from an MHR and an MFR. The MHR contains the MAC frame control and data sequence number fields. The MFR is composed of a 16 bit FCS. The MHR and MFR together form the MAC acknowledgment frame (i.e., MPDU).

The MPDU is passed to the PHY as the PHY acknowledgment frame payload, (i.e., PSDU). The PSDU is prefixed with the SHR, containing the preamble sequence and SFD fields, and the PHR containing the length of the PSDU in octets. The SHR, PHR, and PSDU together form the PHY acknowledgment packet, (i.e., PPDU).

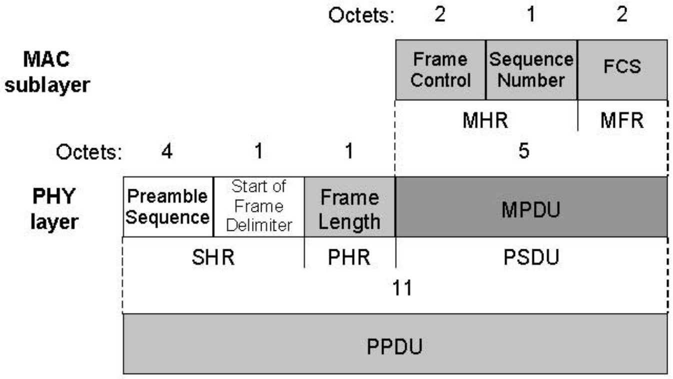

Figure 12—Schematic view of the acknowledgment frame

Copyright © 2003 IEEE. All rights reserved.

5.4.3.4 MAC command frame

Figure 13 shows the structure of the MAC command frame, which originates from the MAC sublayer. The MSDU contains the command type field and command specific data, called the command payload (see 7.2.2.4). The MSDU is prefixed with an MHR and appended with an MFR. The MHR contains the MAC frame control, data sequence number, and addressing information fields. The MFR contains a 16 bit FCS. The MHR, MSDU, and MFR together form the MAC command frame, (i.e., MPDU).

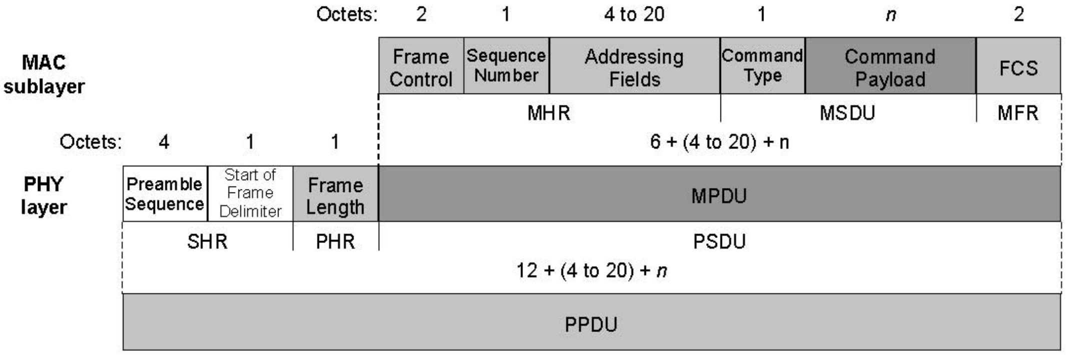

Figure 13—Schematic view of the MAC command frame

The MPDU is then passed to the PHY as the PHY command frame payload, (i.e., PSDU). The PSDU is prefixed with an SHR, containing the preamble sequence and SFD fields, and a PHR containing the length of the PSDU in octets. The preamble sequence enables the receiver to achieve symbol synchronization. The SHR, PHR, and PSDU together form the PHY command packet, (i.e., PPDU).

5.4.4 Robustness

The LR-WPAN employs various mechanisms to ensure robustness in the data transmission. These mechanisms are the CSMA-CA mechanism, frame acknowledgment, and data verification and are briefly discussed in 5.4.4.1 through 5.4.4.3.

5.4.4.1 CSMA-CA mechanism

The LR-WPAN uses two types of channel access mechanism, depending on the network configuration. Nonbeacon-enabled networks use an unslotted CSMA-CA channel access mechanism. Each time a device wishes to transmit data frames or MAC commands, it shall wait for a random period. If the channel is found to be idle, following the random backoff, the device shall transmit its data. If the channel is found to be busy, following the random backoff, the device shall wait for another random period before trying to access the channel again. Acknowledgment frames shall be sent without using a CSMA-CA mechanism.

Beacon-enabled networks use a slotted CSMA-CA channel access mechanism, where the backoff slots are aligned with the start of the beacon transmission. Each time a device wishes to transmit data frames during the CAP, it shall locate the boundary of the next backoff slot and then wait for a random number of backoff slots. If the channel is busy, following this random backoff, the device shall wait for another random number of backoff slots before trying to access the channel again. If the channel is idle, the device can begin transmitting on the next available backoff slot boundary. Acknowledgment and beacon frames shall be sent without using a CSMA-CA mechanism.

The CSMA-CA mechanism is discussed in 7.5.1.

Copyright © 2003 IEEE. All rights reserved.

5.4.4.2 Frame acknowledgment

A successful reception and validation of a data or MAC command frame can be optionally confirmed with an acknowledgment. If the receiving device is unable to handle the received data frame for any reason, the message is not acknowledged.

If the originator does not receive an acknowledgment after some period, it assumes that the transmission was unsuccessful and retries the frame transmission. If an acknowledgment is still not received after several retries, the originator can choose either to terminate the transaction or to try again. When the acknowledgment is not required, the originator assumes the transmission was successful.

The use of acknowledgment is discussed in detail in 7.5.6.4.

5.4.4.3 Data verification

In order to detect bit errors, an FCS mechanism, employing a 16 bit International Telecommunication Union—Telecommunication Standardization Sector (ITU-T) cyclic redundancy check (CRC), is used to protect every frame.

The FCS mechanism is discussed in 7.2.1.8.

5.4.5 Power consumption considerations

In many applications that use this standard, the devices will be battery powered where their replacement or recharging in relatively short intervals is impractical; therefore the power consumption is of significant concern. This standard was developed with the limited power supply availability in mind. However, the physical implementation of this standard will require additional power management considerations that are beyond the scope of this standard.

The protocol has been developed to favor battery-powered devices. However, in certain applications some of these devices could potentially be mains powered. Battery-powered devices will require duty-cycling to reduce power consumption. These devices will spend most of their operational life in a sleep state; however, each device shall periodically listen to the RF channel in order to determine whether a message is pending. This mechanism allows the application designer to decide on the balance between battery consumption and message latency. Mains-powered devices have the option of listening to the RF channel continuously.

5.4.6 Security

Although the diverse range of applications to which this standard is targeted imposes significant constraints on requiring a baseline security implementation in the MAC sublayer, some required security functionality is needed in order to provide basic security services and interoperability among all devices implementing this standard. This baseline includes the ability to maintain an access control list (ACL) and use symmetric cryptography to protect transmitted frames. The ability to perform this security functionality does not imply, however, that security shall be used at any given time by any given device. The higher layers determine when security is to be used at the MAC sublayer and provide all keying material necessary to provide the security services. Key management, device authentication, and freshness protection may be provided by the higher layers, but are out of scope of this standard. A brief introduction of some security terms is provided in 5.4.6.1 and 5.4.6.2; for more detailed information refer to Clause 7.

5.4.6.1 Security services

The security mechanisms in this standard are symmetric-key based using keys provided by higher layer processes. The management and establishment of these keys is the responsibility of the implementer. The

Copyright © 2003 IEEE. All rights reserved.

security provided by these mechanisms assume the keys are generated, transmitted, and stored in a secure manner.

5.4.6.1.1 Access control

Access control is a security service that provides the ability for a device to select the other devices with which it is willing to communicate. In this standard, if the access control service is provided, a device shall maintain a list of devices in its ACL from which it expects to receive frames.

5.4.6.1.2 Data encryption

In this standard data encryption is a security service that uses a symmetric cipher to protect data from being read by parties without the cryptographic key. Data may be encrypted using a key shared by a group of devices (typically stored as the default key) or using a key shared between two peers (typically stored in an individual ACL entry). In this standard, data encryption may be provided on beacon payloads, command payloads, and data payloads.

5.4.6.1.3 Frame integrity

In this standard frame integrity is a security service that uses a message integrity code (MIC) to protect data from being modified by parties without the cryptographic key. It further provides assurance that data came from a party with the cryptographic key. In this standard, integrity may be provided on data frames, beacon frames, and command frames. The key used to provide frame integrity may be shared by a group of devices (typically stored as the default key) or by two peers (typically stored in an individual ACL entry).

5.4.6.1.4 Sequential freshness

Sequential freshness is a security service that uses an ordered sequence of inputs to reject frames that have been replayed. When a frame is received, the freshness value is compared with the last known freshness value. If the freshness value is newer than the last known value, the check has passed, and the freshness value is updated to the new value. If the freshness value is not newer than the last known freshness value, the check has failed. This service provides evidence that the received data are newer than the last data received by that device, but it does not provide a strict sense of time.

5.4.6.2 Security modes

Depending on the mode in which the device is operating and the security suite selected, the MAC sublayer may provide different security services.

5.4.6.2.1 Unsecured mode

Because security is not used for unsecured mode, no security services are provided by devices operating in unsecured mode.

5.4.6.2.2 ACL mode

Devices operating in ACL mode provide limited security services for communications with other devices. While in ACL mode, the higher layer may chose to reject frames based on whether the MAC sublayer indicates that a frame is purported to originate from a specific device. Because cryptographic protection is not provided in the MAC sublayer in this mode, the higher layer should implement other mechanisms to ensure the identity of the sending device. The service that is provided while in ACL mode is access control (see 5.4.6.1.1).

Copyright © 2003 IEEE. All rights reserved.