

Christina Belisario
Research Coordinator
Morrison Foerster
12531 High Bluff Drive, Suite 200
San Diego, CA 92130-2040
USA

12 November 2025

Dear Christina

ZigBee Wireless Sensor and Control Network, 1st edition by Ata Elahi and Adam Gschwender – Pearson Education, 2009: Shelf mark: YK.2010.a.33481

According to our records, this item was receipted by The British Library on **19 November 2009** and would have been available for public use from that date.

Copies of the cover, title page, title page verso showing the stamp and contents pages are attached. We are also sending the text requested.

Please note that we can only provide the date that the British Library made this item available for public use; for the actual date of publication, please contact the publisher.

Yours sincerely

Tony Corsini

British Library Research Service
Tel: +44 (0) 20 7412 7903 bipc-research@bl.uk

YK.2010.a.
33481

PRENTICE
HALL

ZigBee Wireless Sensor and Control Network



Ata Elahi with Adam Gschwender

Prentice Hall Communications Engineering and Emerging Technologies Series
Theodore S. Rappaport, Series Editor

ZIGBEE WIRELESS SENSOR AND CONTROL NETWORK

Ata Elahi, Ph.D.
with Adam Gschwender



PRENTICE
HALL

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco
New York • Toronto • Montreal • London • Munich • Paris • Madrid
Cape Town • Sydney • Tokyo • Singapore • Mexico City

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The authors and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
(800) 382-3419
corpsales@pearsontechgroup.com

For sales outside the United States please contact:

International Sales
international@pearson.com

Visit us on the Web: informit.com/ph

Library of Congress Cataloging-in-Publication Data:

Elahi, Ata.

ZigBee wireless sensor and control network / Ata Elahi, with Adam Gschwender
p. cm.

ISBN 978-0-13-713485-4 (pbk. : alk. paper) 1. Personal communication service systems—Standards. 2. Sensor networks. 3. Low voltage systems—Industrial applications. 4. Radio frequency—Industrial applications. I. Gschwender, Adam, 1979- II. Title.

TK5103.485.E43 2009
004.6'2—dc22

2009032393

Copyright © 2010 Pearson Education, Inc.

All rights reserved. Printed in the United States of America. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, write to:

Pearson Education, Inc.
Rights and Contracts Department
501 Boylston Street, Suite 900
Boston, MA 02116
Fax (617) 671 3447

ISBN-13: 978-0-137-13485-4

ISBN-10: 0-137-13485-1

Text printed in the United States on recycled paper at RR Donnelley & Sons, Crawfordsville, Indiana
First printing November 2009



CONTENTS

Preface xiii

CHAPTER 1	Introduction to Wireless Networks	1
	Introduction	1
	1.1 The Open Systems Interconnection (OSI) Reference Model	3
	1.2 IEEE 802 Standard Committee	5
	1.3 Wireless Technologies	6
	1.4 Antenna	8
	1.5 Error-Detection Methods	9
	1.6 ISM and U-NII Bands	13
	1.7 Modulation	13
	1.8 Wireless Local-Area Network (WLAN)	17
	1.9 Frequency-Hopping Spread Spectrum (FHSS)	20
	1.10 Direct-Sequence Spread Spectrum (DSSS)	20
	1.11 Wireless MAN	21
	1.12 Bluetooth	25
	Summary	28
	References	30

CHAPTER 2	ZigBee Wireless Sensor and Control Network	31
	Introduction	31
	2.1 ZigBee Network Characteristics	33
	2.2 ZigBee Device Types	34
	2.3 ZigBee Topologies	35
	2.4 End Device (Node) Addressing	39
	2.5 Depth of a Network, Number of Children, and Network Address Allocation	40
	2.6 ZigBee Protocol Architecture	40

viii CONTENTS

2.7 ZigBee and ZigBee PRO Feature Sets	43
Summary	46
References	47

CHAPTER 3 IEEE 802.15.4 Physical Layer 49

Introduction	49
3.1 Frequency Band, Data Rate, and Channel Numbering	50
3.2 Physical Layer Services	52
3.3 Transmitter Power and Receiver Sensitivity	57
3.4 Physical Layer Information Base (PIB)	60
3.5 Physical Layer Transmission	61
Summary	68
References	69

CHAPTER 4 IEEE 802.15.4 Media Access Control (MAC) Layer 71

Introduction	71
4.1 MAC Layer Services	71
4.2 MAC Layer Information Base (MIB)	75
4.3 MAC Management Services	77
4.4 Scanning Channels	83
4.5 Access Method	84
4.6 Data Transfer Model	88
4.7 MAC Frame Format	90
4.8 Association Request	94
4.9 Disassociation Notification Command	96
4.10 Orphan Notification	96
4.11 Beacon Request	97
4.12 Coordinator Realignment Command	97
Summary	98
References	98

CHAPTER 5 Network Layer 99

Introduction	99
5.1 Network Layer Data Entity (NLDE) Services	100
5.2 Network Information Base (NIB)	102
5.3 Network Layer Management Entity (NLME)	105
5.4 Network Formation	108
5.5 Joining a Network	110
5.6 Network Layer Frame Format	112

5.7 Neighbor Table	114
5.8 Network Command Frame Format	114
Summary	116
References	117

CHAPTER 6 ZigBee Application Support Sublayer (APS) 119

Introduction	119
6.1 Application Support Data Entity (APSDE)	119
6.2 Application Support Sublayer Management Entity (ASME)	122
6.3 Application Support Sublayer Information Base (AIB)	123
6.4 Persistent Data	124
6.5 Application Support Sublayer Frame Format	125
6.6 APS Command Frame Format	127
Summary	128
References	128

CHAPTER 7 Application Layer 129

Introduction	129
7.1 Application Object (Endpoint)	129
7.2 Attribute, Cluster, Cluster Library, and Profile	130
7.3 Cluster	132
7.4 General Cluster Commands	134
7.5 Attribute Reporting	135
7.6 ZigBee Cluster Libraries	137
7.7 ZigBee Device Object (ZDO)	140
7.8 ZigBee Device Profile (ZDP)	140
7.9 Device Discovery	143
7.10 Binding	146
7.11 Network Management Commands	150
7.12 ZigBee Coordinator Startup	151
Summary	151
References	153

CHAPTER 8 ZigBee Security 155

Introduction	155
8.1 Elements of Network Security	155
8.2 Introduction to Cryptography	156
8.3 ZigBee Security	160

x CONTENTS

8.4 ZigBee Security Modes	161
8.5 Security Management Primitives	164
8.6 Counter (CTR) Mode Encryption	165
8.7 Cipher Block Chaining (CBC) Mode Encryption	166
8.8 Network Layer Security	166
8.9 Application Support SubLayer Security	168
Summary	174
References	175

APPEND

CHAPTER 9 Address Assignment and Routing 177

Introduction	177
9.1 Address Assignment Using Distributed Scheme	177
9.2 Stochastic Address Assignment	179
9.3 Routing	179
9.4 Dynamic Source Routing (DSR)	182
9.5 ZigBee Routing	183
9.6 ZigBee Routing Commands	187
Summary	191
References	191

APPEND

CHAPTER 10 ZigBee Home Automation and Smart Energy Network 193

10.1 Home Automation Profile	193
10.2 Smart Energy Network	197
10.3 ZigBee Stack Profile for Smart Energy (SE) Profile	200
10.4 Smart Energy Cluster	203
10.5 Smart Energy Device	203
Summary	204
References	205

APPEND

CHAPTER 11 ZigBee RF4CE 207

Introduction	207
11.1 RF4CE Nodes and Topology	208
11.2 RF4CE Protocol Architecture	209
11.3 Network Layer Data Services	210
11.4 Network Layer Management Services	211
11.5 Network Layer Information Base (NIB)	212

APPEND



11.6 Discovery Process	213
11.7 Pairing Process	214
Summary	216
References	217

APPENDIX A 6lowpan 219

Introduction	219
A.1 IPv6 Structure	220
A.2 User Datagram Protocol (UDP)	222
A.3 IEEE 802.15.4 MAC and Physical Layer Frame Format	222
A.4 64-Bit Global Identifier	223
A.5 Adaptation Layer	223
A.6 Fragmented IPv6 Payload	228

APPENDIX B Wireless HART 229

Introduction	229
B.1 Wireless HART Physical Layer	230
B.2 Wireless HART Data Link Layer	230
B.3 Wireless HART Network Layer	231
B.4 Wireless HART Network Components	231
B.5 Network Formation	232
B.6 Security	233
B.7 Wireless HART Data Transfer Mode	233

APPENDIX C Z-Wave 235

Introduction	235
C.1 Z-Wave Protocol Architecture	235
C.2 RF Media	236
C.3 MAC Layer	236

APPENDIX D Abbreviations 237

Bibliography	241
Index	245

CHAPTER 2

ZIGBEE WIRELESS SENSOR AND CONTROL NETWORK

INTRODUCTION

ZigBee is a new standard developed by the ZigBee Alliance for personal-area networks (PANs). Consisting of more than 270 companies (including Freescale, Ember, Mitsubishi, Philips, Honeywell, and Texas Instruments), the ZigBee Alliance is a consortium that promotes the ZigBee standard for a low-rate/low-power wireless sensor and control network. The ZigBee protocol stack is built on top of IEEE 802.15.4, which defines the Media Access Control (MAC) and physical layers for low-rate wireless personal-area network (LR-WPAN). The ZigBee standard offers a stack profile that defines the network, security, and application layers. Developers are responsible for creating their own application profiles or integrating with the public profiles that were developed by the ZigBee Alliance. The ZigBee specification is an open standard that allows manufacturers to develop their own specific applications that require low cost and low power.

The ZigBee specification has undergone multiple modifications. The major milestones in its revision history are listed here:

- In 2004, the ZigBee Alliance published its first specification, which supported a home control lighting profile. However, the ZigBee Alliance no longer supports the 2004 specification.
- In February 2006, the ZigBee Alliance published the ZigBee Stack 2006, which contained modifications to ZigBee 2004.
- In October 2007, the ZigBee Alliance published two feature sets called ZigBee and ZigBee PRO. The ZigBee feature set is interoperable with ZigBee PRO. If a network is based on the ZigBee PRO stack, devices

from the ZigBee feature set stack can join the network as end devices. Likewise, if a network is based on the ZigBee stack, ZigBee PRO devices can join the network as end devices.

The ZigBee feature set is backward compatible with ZigBee 2006; a ZigBee feature set device can join in a ZigBee 2006 network and vice versa.

The ZigBee Alliance developed the following application profiles:

- **Smart energy:** ZigBee can be used to quickly read electrical, gas, and water meters. The ZigBee smart energy network enables wireless communication between the advanced metering infrastructure (AMI) and the home-area network; that is, the smart energy network will connect home appliances with the utility company for improving energy efficiency and managing peak demand.
- **Commercial building automation:** In a commercial building, ZigBee can be an integral tool in building maintenance. ZigBee wireless can be used to monitor smoke-detector operation and fire-door position. Suppose that a high-rise building contains 50 floors, with each floor having 50 rooms, and each room is equipped with a smoke detector. For safety reasons, each smoke detector must be tested every month. This requires checking 2,500 rooms! Instead of requiring that someone manually test the 2,500 smoke detectors, ZigBee allows a central station to remotely monitor each smoke detector. A ZigBee device may also be used to turn on and off a light without using any wire.
- **Home automation:** ZigBee home automation profile defines devices that are used for residential and commercial applications. ZigBee can be used to remotely control lighting, heating, cooling, and door-locking mechanisms. It can also remotely monitor smoke detectors and home security systems
- **Personal, home, and hospital care (PHHC):** This profile is used for monitoring the personal health of a patient at home without limiting a patient's mobility. For example, it can remotely monitor blood pressure and heart rate.
- **Telecom applications:** Embedding a ZigBee device into a mobile phone or PDA creates a new device called a ZigBee mobile device. A ZigBee mobile device can be used to communicate with other ZigBee devices. Users of ZigBee mobile devices can send and receive messages and share ring tones, contacts and images. More important, the ZigBee mobile device can even communicate with ZigBee devices that use different application profiles. For example, a ZigBee mobile device can be used to alert emergency services when a PHHC-enabled device detects a critical problem with the patient's health.
- **Remote control for consumer electronics (ZigBee RF4CE):** Currently, most remote controllers are using infrared (IR) technology, which requires line of sight; ZigBee RF4CE is a protocol that uses radio frequency (RF) to replace IR technology for remote controllers used in consumer electronics.

• **Industrial**
sor and
processe
ment ca
This pr
machin
can rec
level, h

2.1 ZIGBEE

Several star
WiMax. Zig
lowing char

- Low l
years
- Low c
- Low
- Easy
- Supp
- ZigB
- ZigE

Table 2.1
tooth.

Table 2.1

Application
Frequency
Battery life
Nodes per
Bandwidth
Range (me
Topology
Standby c
Memory

- **Industrial process monitoring and control:** ZigBee offers solutions for wireless sensor and control. Therefore, it can be used for monitoring and controlling industrial processes without using wire. For example, in inventory tracking, each piece of equipment can be tagged with a wireless sensor and can then be located by a ZigBee node. This process is called radio frequency identification (RFID). ZigBee can monitor machine condition and the performance of operating equipment within a plant; ZigBee can record and transmit such critical information as temperature, pressure, flow, tank level, humidity, and vibration.

2.1 ZIGBEE NETWORK CHARACTERISTICS

Several standards currently exist for wireless networks, including Bluetooth, WiFi, and WiMax. ZigBee is a new standard for wireless sensor and control networks. It has the following characteristics:

- Low battery consumption. A ZigBee end device should operate for months or even years without needing its battery replaced.
- Low cost.
- Low data rate. The maximum data rate for a ZigBee device is 250Kbps.
- Easy to implement.
- Supports up to 65,000 nodes connected in a network.
- ZigBee can automatically establish its network.
- ZigBee uses small packets compared with WiFi and Bluetooth.

Table 2.1 shows a comparison of ZigBee characteristics with those of WiFi and Bluetooth.

Table 2.1 ZigBee, Bluetooth, and WiFi Characteristics

	WiFi IEEE 802.11	Bluetooth IEEE 802.15.1	ZigBee IEEE 802.15.4
Application	Wireless LAN	Cable replacement	Control and monitor
Frequency bands	2.4GHz	2.4GHz	2.4GHz, 868MHz, 915MHz
Battery life (days)	0.1–5	1–7	100–7,000
Nodes per network	30	7	65,000
Bandwidth	2–100Mbps	1Mbps	20–250Kbps
Range (meters)	1–100	1–10	1–75 and more
Topology	Tree	Tree	Star, tree, cluster tree, and mesh
Standby current	20 * 10–3 amps	200 * 10–6 amps	3 * 10–6 amps
Memory	100KB	100KB	32–60KB

Table 2.1 shows that Bluetooth, while similar in functionality to ZigBee, does not offer the range of topologies, and its standby current is nearly 70 times more than ZigBee. Of the three wireless networks under comparison, ZigBee is the only one that offers mesh topology. In addition, a ZigBee end device can be in sleep mode and still keep its association with its network. ZigBee is considered a more sophisticated network when compared to either Bluetooth or WiFi.

2.2 ZIGBEE DEVICE TYPES

A ZigBee network consists of ZigBee nodes (devices). The node architecture is shown in Figure 2.1. A node consists of a microcontroller, a transceiver, and an antenna. A ZigBee node uses stack profiles, which are developed by software. A node can be used for a wide variety of applications—for example, lighting control, smoke-detector, and home-security monitoring. Therefore, a node can support multiple subunits, and each subunit has an application object that describes the subunit function. A node can operate as either a full-function device (FFD) or reduced-function device (RFD). An FFD can perform all the tasks that are defined by the ZigBee standard, and it operates in the full set of the IEEE 802.15.4 MAC layer. An RFD performs only a limited number of tasks.

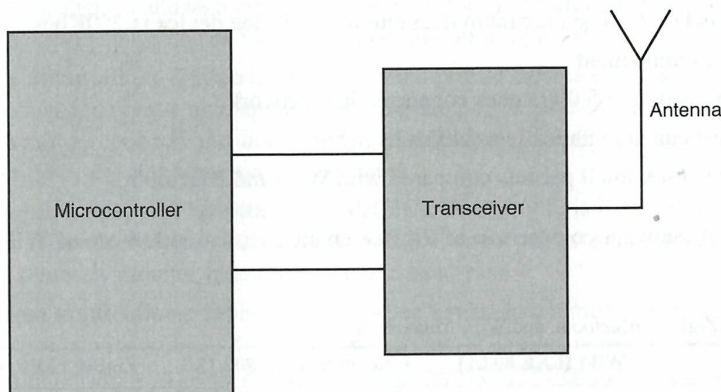


Figure 2.1 Architecture of ZigBee node

- **Coordinator:** A coordinator is an FFD and responsible for overall network management. Each network has exactly one coordinator. The coordinator performs the following functions:
Selects the channel to be used by the network
Starts the network

Assigns
Permits
Holds a
Transfer

- **End de**
the IEE
(child)
cycle p
fore, Zi
The en
Joins o
Transf
- **Route**
netwo
over v
nator
- **ZigBe**
mana
- **ZigB**
anoth

2.3 ZIG

ZigBee us
IEEE 802
only star,
It uses
end devic

- **Sta**
(no
wit
coc
on
thr
na
is

ie, does not offer
n ZigBee. Of the
ffers mesh topol-
ep its association
hen compared to

cture is shown in
ntenna. A ZigBee
e used for a wide
ad home-security
unit has an appli-
ier a full-function
the tasks that are
E 802.15.4 MAC

ntenna

network manage-
performs the fol-

Assigns how addresses are allocated to nodes or routers

Permits other devices to join or leave the network

Holds a list of neighbors and routers

Transfers application packets

- **End device:** An end device can be an RFD. An RFD operates within a limited set of the IEEE 802.15.4 MAC layer, enabling it to consume less power. The end device (child) can be connected to a router or coordinator (parent). It also operates at low duty-cycle power, meaning it consumes power only while transmitting information. Therefore, ZigBee architecture is designed so that an end device transmission time is short. The end device performs the following functions:
Joins or leaves a network
Transfers application packets
- **Router:** A router is an FFD. A router is used in tree and mesh topologies to expand network coverage. The function of a router is to find the best route to the destination over which to transfer a message. A router performs all functions similar to a coordinator except the establishing of a network.
- **ZigBee trust center (ZTC):** The ZigBee trust center is a device that provides security management, security key distribution, and device authentication.
- **ZigBee gateway:** The ZigBee gateway is used to connect the ZigBee network to another network, such as a LAN, by performing protocol conversion.

2.3 ZIGBEE TOPOLOGIES

ZigBee uses the IEEE 802.15.4 2003 specification for its physical layer and MAC layer. IEEE 802.15.4 offers star, tree, cluster tree, and mesh topologies; however, ZigBee supports only star, tree, and mesh topologies.

It uses an association hierarchy; a device joining the network can either be a router or an end device, and routers can accept more devices.

- **Star topology:** The star topology consists of a coordinator and several end devices (nodes), as shown in Figure 2.2. In this topology, the end device communicates only with the coordinator. Any packet exchange between end devices must go through the coordinator. The disadvantage of this topology is the operation of the network depends on the coordinator of the network, and because all packets between devices must go through coordinator, the coordinator may become bottlenecked. Also, there is no alternative path from the source to the destination. The advantage of star topology is that it is simple and packets go through at most two hops to reach their destination.

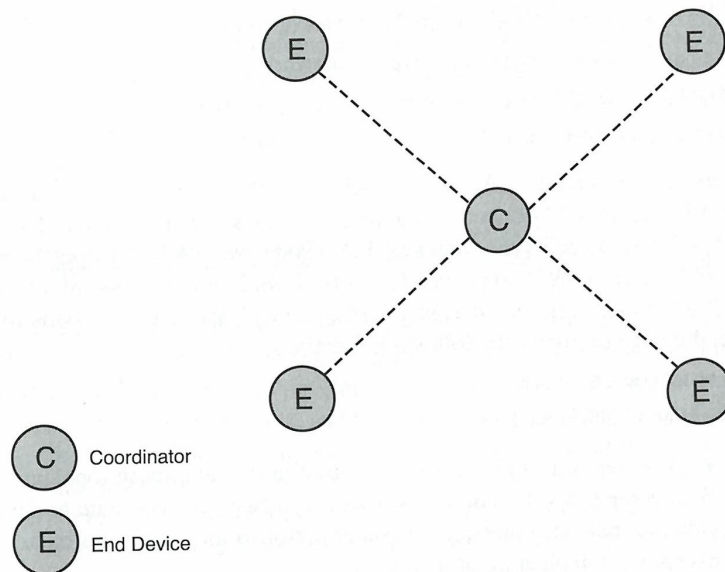


Figure 2.2 Star topology

- **Tree topology:** In this topology, the network consists of a central node (root tree), which is a coordinator, several routers, and end devices, as shown in Figure 2.3. The function of the router is to extend the network coverage. The end nodes that are connected to the coordinator or the routers are called children. Only routers and the coordinator can have children. Each end device is only able to communicate with its parent (router or coordinator). The coordinator and routers can have children and, therefore, are the only devices that can be parents. An end device cannot have children and, therefore, may not be a parent. A special case of tree topology is called a cluster tree topology.

The disadvantages of tree topology are

- If one of the parents becomes disabled, the children of the disabled parent cannot communicate with other devices in the network.
- Even if two nodes are geographically close to each other, they cannot communicate directly.

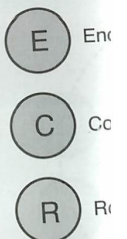


Figure 2.3

- Cl...
- wh...
- ter...
- 8C...
- M...
- or...
- ir...
- A...
- tl...
- T...
- I...

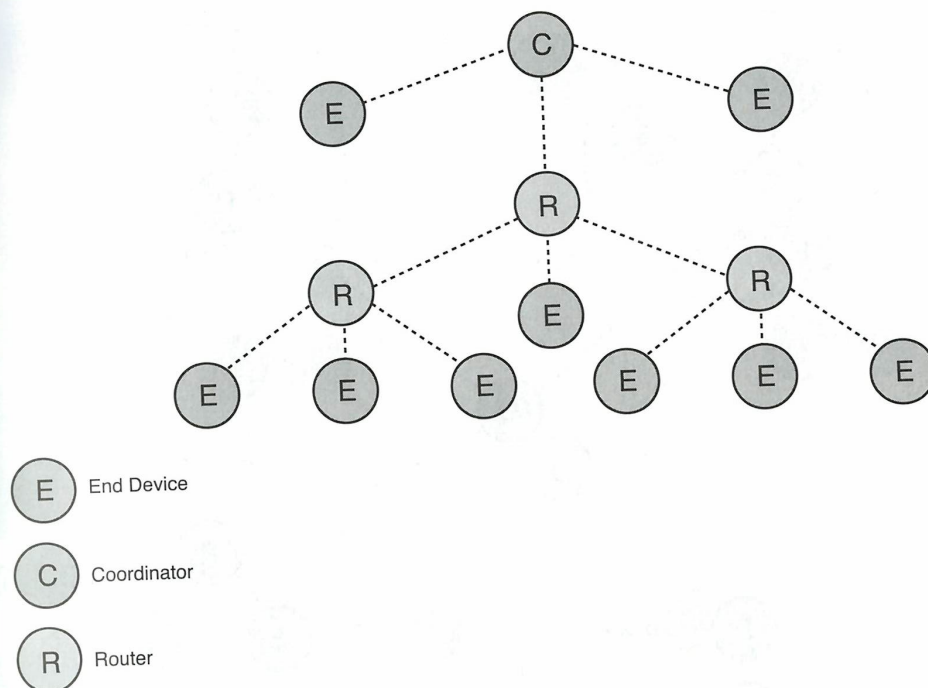


Figure 2.3 Tree topology

- **Cluster tree topology:** A cluster tree topology is a special case of tree topology in which a parent with its children is called a cluster, as shown in Figure 2.4. Each cluster is identified by a cluster ID. ZigBee does not support cluster tree topology, but IEEE 802.15.4 does support it.
- **Mesh topology:** Mesh topology, also referred to as a peer-to-peer network, consists of one coordinator, several routers, and end devices, as shown in Figure 2.5. The following are the characteristics of a mesh topology:
 - A mesh topology is a multihop network; packets pass through multiple hops to reach their destination.
 - The range of a network can be increased by adding more devices to the network.
 - It can eliminate dead zones.
 - A mesh topology is self-healing, meaning during transmission, if a path fails, the node will find an alternate path to the destination.

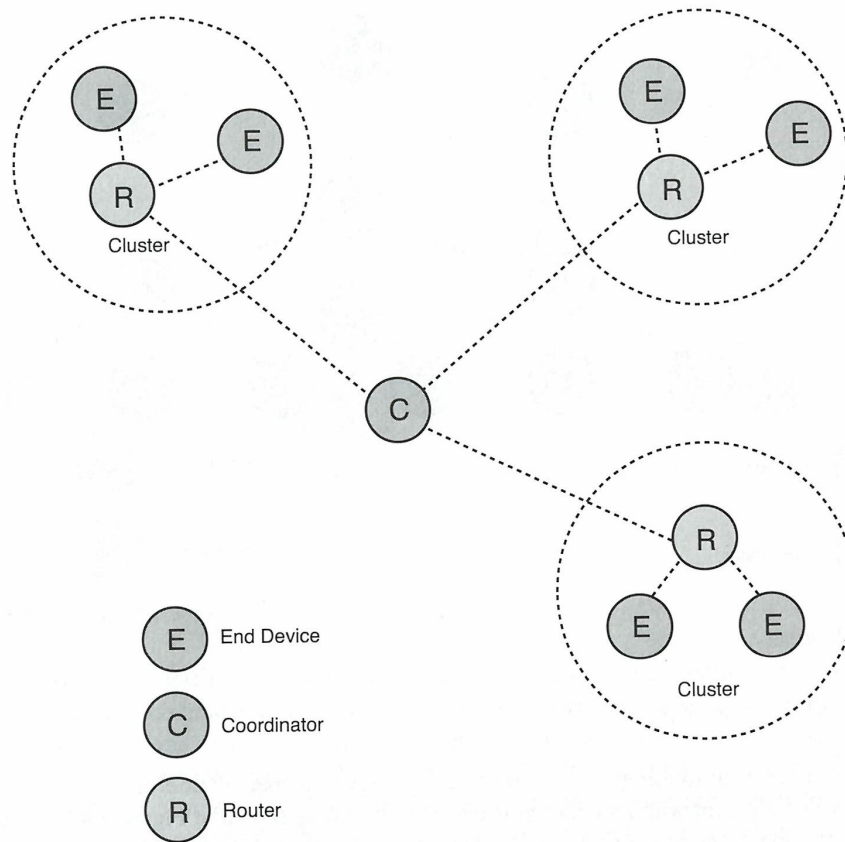


Figure 2.4 Cluster tree topology

Devices can be close to each other so that they use less power.

Adding or removing a device is easy.

Any source device can communicate with any destination device in the network.

Compared with star topology, mesh topology requires greater overhead.

Mesh routing uses a more complex routing protocol than a star topology.

Figure

2.4

When
16-b
devi
used
of th
short
tage
add

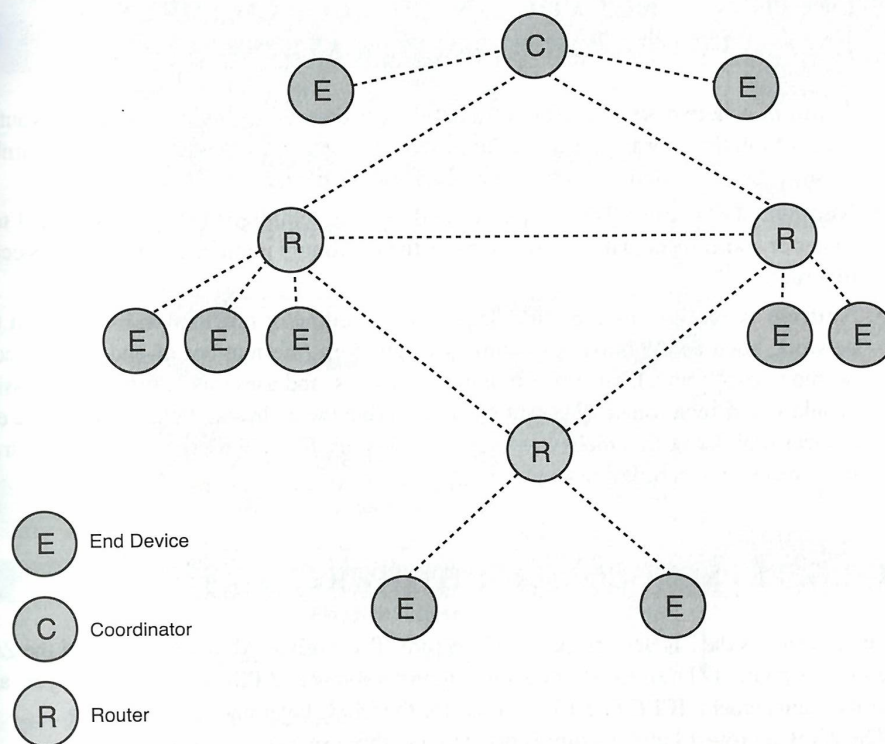


Figure 2.5 Mesh topology

2.4 END DEVICE (NODE) ADDRESSING

When a device joins a ZigBee network, the ZigBee coordinator or router assigns a logical 16-bit address to the device. Also, each device has a 64-bit IEEE address, and no two devices can have the same IEEE address in the entire world. Short addresses (16 bits) can be used by devices in a network. The advantage of using the 16-bit address is to extend the life of the battery. A 16-bit address reduces the size of the frame. A smaller frame size results in shorter transmission time. Less transmission time means greater battery life. The disadvantage of using the 16-bit address is that two nodes in different networks can have the same address.

2.5 DEPTH OF A NETWORK, NUMBER OF CHILDREN, AND NETWORK ADDRESS ALLOCATION

- **Depth of a network:** The depth of a network is determined by the number of routers (hops) from the coordinator to the farthest device, where farthest is defined by number of hops. In a star topology, the depth of a network is one.
- **Number of children:** The number of end devices (children) that are connected to a router or coordinator. The coordinator sets the maximum number of children connected to a router.
- **Address allocation:** In a tree topology, each coordinator holds information about the network, such as the maximum number of children (the number of end devices connected to each router), maximum number of routers, and uses this information to assign an address to each router. The routers, then, assign the addresses to their respective end devices (children). In a mesh topology, however, each router assigns a random address to its respective end devices.

2.6 ZIGBEE PROTOCOL ARCHITECTURE

Figure 2.6 shows the ZigBee protocol architecture. The ZigBee Alliance developed the ZigBee device object (ZDO), the application support sublayer (APS), the network layer, and security management. IEEE 802.15.4 is used for the MAC layer and physical layer.

The ZigBee protocol architecture is divided into three sections, as follows:

- IEEE 802.15.4, which consists of the MAC and physical layers.
- ZigBee layers, which consist of the network layer, the ZigBee device object (ZDO), the application sublayer, and security management.
- Manufacturer application: Manufacturers of ZigBee devices can use the ZigBee application profile or develop their own application profile.

2.6.1 Physical Layer

The physical layer performs modulation on outgoing signals and demodulation on incoming signals. It transmits information and receives information from a source. Table 2.2 shows the physical layer frequency band, data rate, and channel numbers.

Figur

Tab
Fre
868
902
2.4

2.
T
a
ti
2
T
1

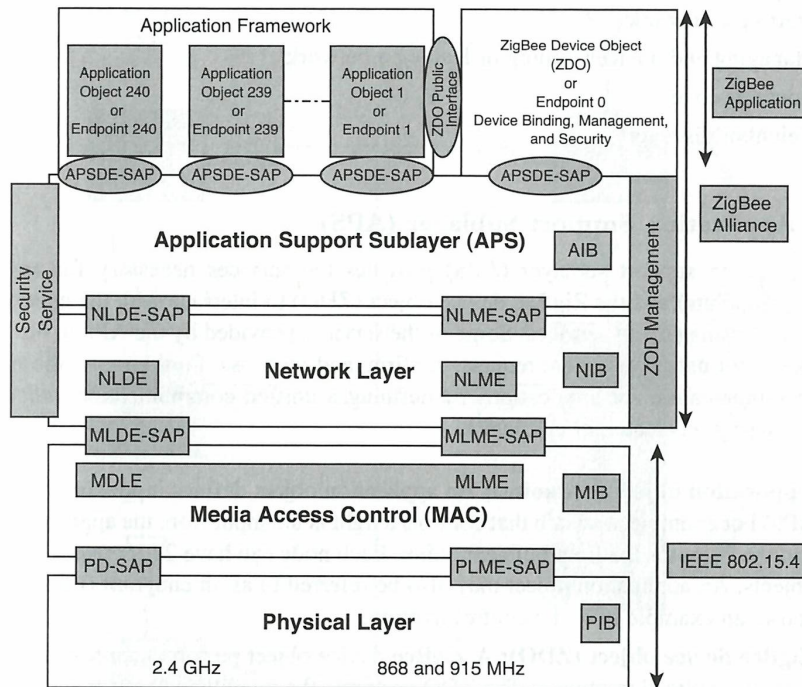


Figure 2.6 ZigBee protocol architecture

Table 2.2 Physical Layer Frequency Band

Frequency Band	Country	Data Rate	Channel Numbers
868.3MHz	European countries	20Kbps	0
902-928 MHz	United States	40Kbps	1-10
2.405GHz	Worldwide	250Kbps	11-26

2.6.2 Media Access Control (MAC) Layer

The functions of the MAC layer are to access the network by using carrier-sense multiple access with collision avoidance (CSMA/CA), to transmit beacon frames for synchronization, and to provide reliable transmission.

2.6.3 Network Layer

The network layer is located between the MAC layer and application support sublayer. It provides the following functions:

- Starting a network
- Managing end devices joining or leaving a network
- Route discovery
- Neighbor discovery

2.6.4 Application Support Sublayer (APS)

The application support sublayer (APS) provides the services necessary for application objects (endpoints) and the ZigBee device object (ZDO) to interface with the network layer for data and management services. Some of the services provided by the APS to the application objects for data transfer are request, confirm, and response. Furthermore, the APS provides communication for applications by defining a unified communication structure (for example, a profile, cluster, or endpoint).

- **Application object (endpoint):** An application object defines input and output to the APS. For example, a switch that controls a light is the input from the application object, and the output is the light bulb condition. Each node can have 240 separate application objects. An application object may also be referred to as an endpoint (EP). Figure 2.7 shows an example of home control lighting.
- **ZigBee device object (ZDO):** A ZigBee device object performs control and management of application objects. The ZDO performs the overall device management tasks:
 - Determines the type of device in a network (for example, end device, router, or coordinator)
 - Initializes the APS, network layer, and security service provider
 - Performs device and service discovery
 - Initializes coordinator for establishing a network
 - Security management
 - Network management
 - Binding management
- **End node:** Each end node or end device can have multiple EPs. Each EP contains an application profile, such as home automation, and can be used to control multiple devices or a single device. More to the point, each EP defines the communication functions within a device. As shown in Figure 2.7, the bedroom switch controls the bedroom light, and the remote control is used to control three lights: bedroom, hallway1, and hallway2.



Remote Control



Figure 2.7

- ZigBee
tran
with
of t
me
in v
all

2.7 Z

In Octo
ZigBee
specific
cant in

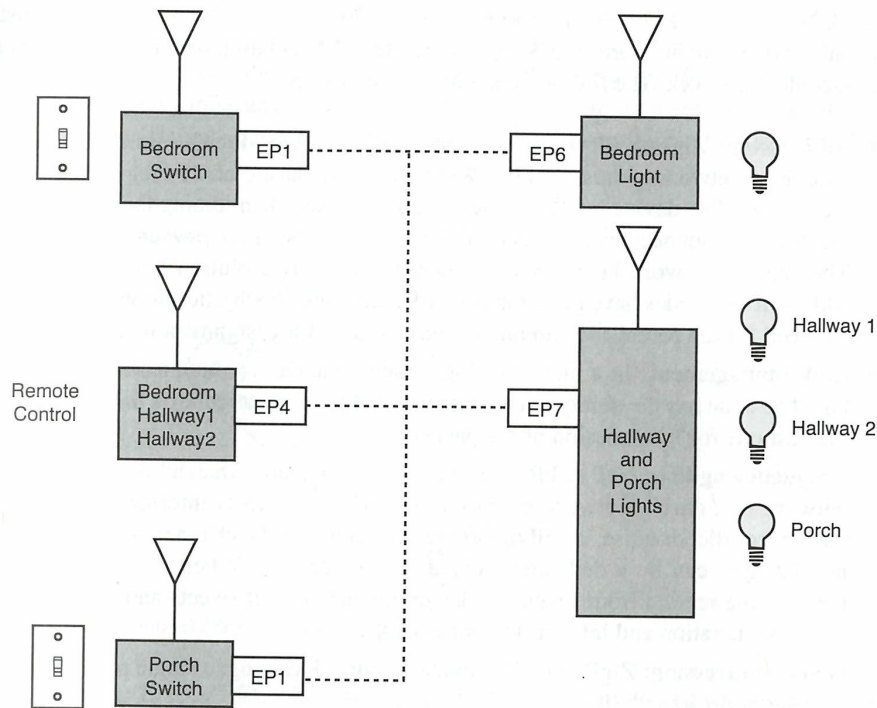


Figure 2.7 Home control lighting

- **ZigBee addressing mode:** ZigBee uses direct, group, and broadcast addressing for transmission of information. In direct addressing, two devices communicate directly with each other. This requires that the source device has both the address and endpoint of the destination device. Group addressing requires that the application assign a group membership to one or more devices. A packet is then transmitted to the group address in which the destination device lies. The broadcast address is used to send a packet to all devices in the network.

2.7 ZIGBEE AND ZIGBEE PRO FEATURE SETS

In October 2007, the ZigBee Alliance published two feature set specifications for ZigBee: ZigBee and ZigBee PRO. The ZigBee feature set is nearly the same as the ZigBee 2006 specification; however, it does offer a few new features. ZigBee PRO offers several significant improvements such as security and the capability to self-form and self-heal the

network. It is targeted for use in building automation and environmental and industrial applications that contain more than 30 nodes. ZigBee PRO is based on a mesh topology and is a beaconless network. The following are its characteristics:

- **Addressing:** ZigBee PRO uses a mesh topology. Any device joining the network requires a network address. ZigBee PRO uses a stochastic addressing method, which means a ZigBee device randomly picks up an address when joining the network. Also, the device announces its address on the network by using the `device-annnc` command. The ZigBee network layer provides address conflict resolution based on the MAC address if two nodes have the same network addresses. Stochastic addressing eliminates the need for the parent to maintain an address table for assignment to children.
- **Link management:** In a mesh topology, each node can communicate with its neighbor. The node has the ability to evaluate the quality of its neighbor's links and to select the best one for transmission of the packet.
- **Frequency agility:** ZigBee PRO selects the best available channel during startup of a network but, during network operation, if any node detects interference due to frequency conflict or noise, it will report the occurrence to the channel manager. (A channel manager can be a dedicated device or trust center.) When the channel manager receives the reports from several nodes on the network, it selects another channel for network operation and informs the nodes of the switch.
- **Group addressing:** ZigBee PRO provides group addressing; a single packet can reach a group of devices.
- **Commissioning:** It is a tool that is used by the ZigBee device installer to install ZigBee devices.
- **Compatibility:** The ZigBee PRO stack identifier is two and is advertised in its beacon frame. Any end device can join ZigBee PRO if it uses the standard security mode.
- **Asymmetric link:** The link between two nodes is usually asymmetric, meaning the quality of the link in both directions is not the same. The quality of the link is represented by the link cost. Figure 2.8 shows a ZigBee network. The link cost from node A to B is different from B to A (asymmetric link) because A and B do not have the same transmission powers and receiver sensitivities. When the nodes A and E use the same route B–D to exchange information, it is considered symmetric. In asymmetric routing, the destination node uses a different path to transmit to the source. In Figure 2.8, the source A uses the B–D path to send a packet to E, and E use the path C to send the packet to A.
- **Fragmentation:** ZigBee PRO provides fragmentation of large packets into smaller packets for transmission. The destination node will reassemble the packets.

• **Power n**
the route
sleep mo
the node
wakes u
network

Figure 2.8

- **Routi**
routin
- **Secur**
- **Sta**
and
In t
ter,
sec
- **Hi**
lin
us
de
pa
- **Trus**
coor

and industrial topology and

the network method, which network. Also, no command. on the MAC ng eliminates ldren.

with its neigh- and to select

g startup of a e due to fre- ger. (A chan- nel manger r channel for

et can reach

o install Zig-

in its beacon ty mode.

meaning the ink is repre- t from node ot have the d E use the asymmetric e. In Figure h C to send

nto smaller

- **Power management:** In ZigBee PRO, only the end devices are powered by batteries; the routers and coordinator use main power. ZigBee PRO allows end devices to go into sleep mode so that they consume less power. While the end device is in sleep mode, the node will miss any network key updates from the trust center. When the device wakes up, it uses its link key to send a message to the trust center to obtain an updated network key.

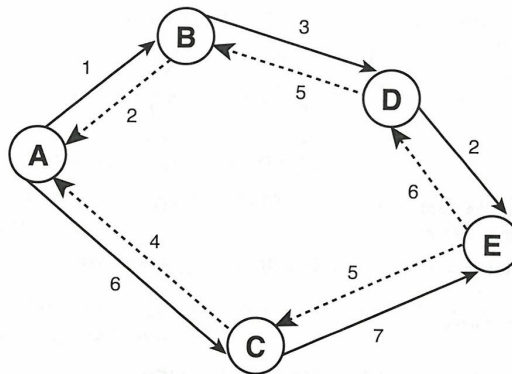


Figure 2.8 Asymmetric link

- **Routing:** ZigBee PRO offers two types of routing: many-to-one routing and multicast routing. Many-to-one routing is used for the network with a concentrator.
- **Security:** ZigBee PRO offers two security modes, as follows:
 - *Standard mode:* In standard mode, the device is permitted to use the network key and link key. The network key is a standard key and all devices share the same key. In this mode, devices do not require authentication to join a network. The trust center, master key, and SKKE are optional. The trust center for ZigBee PRO standard security mode is used for transporting the network key.
 - *High-security mode:* In this mode, three keys are permitted for use: the network, link, and master keys. The trust center and SKKE are mandatory. The trust center uses the transport key command to transport the link and network keys to the devices in the network. The device is required to perform authentication with its parent, and it is required to perform authentication between neighbors.
- **Trust center:** ZigBee PRO should have a trust center; the trust center can be a router, coordinator, concentrator, or specific device.

Table 2.3 shows a comparison of ZigBee 2006, ZigBee, and ZigBee PRO feature sets.

Table 2.3 Comparison of 2006, ZigBee, and ZigBee PRO Feature Sets

ZigBee Features	2006 Specification	ZigBee Feature Set Specification	ZigBee PRO Feature Set Specification
Network coordinator selects best channel at startup.	Yes	Yes	Yes
During operation can detect interference and change channel operation.	No	Yes	Yes
Distributed address assignment.	Yes	Yes	No
Stochastic address assignment.	No	No	Yes
Supports group addressing.	Yes	Yes	Yes
Many-to-one routing.	No	No	Yes
128-bit Advanced Encryption Standard (AES) with message integrity code (MIC).	Yes	Yes	Yes
Trust center can be any device or coordinator in the network.	Coordinator	Coordinator	Any device
Network scale up limited to address assignment scheme.	Yes	Yes	No
Message fragmentation is permitted.	No	Yes	Yes
Supports buffering for message fragmentation.	No	Yes	Yes
Supports commissioning tool.	Yes	Yes	Yes
Device keeps information about its neighbor devices.	No	No	Yes
Offers high-security mode.	No	No	Yes
Network topologies.	Tree and mesh	Tree and mesh	Mesh

SUMMARY

This chapter presented an overview of ZigBee, its applications, and its characteristics. The following are the key concepts that were described in the chapter:

- ZigBee, a wireless sensor and control network, was developed by the ZigBee Alliance.
- ZigBee applications can be used in home automation, commercial building automation, personal home health care, smart energy, and industrial process monitoring.
- The first ZigBee specification was published in 2004 and supported home control lighting; the ZigBee Alliance no longer supports the 2004 specification.
- In 2006, the ZigBee Alliance published the ZigBee 2006 specification, which was a modification of ZigBee 2004 specification.
- In 2007, ZigBee published ZigBee and ZigBee PRO feature sets.
- ZigBee defines three main types of devices: the coordinator, router, and end device. In addition, devices can act as a trust center or gateway.

REF

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.

ture sets.

PRO Feature ification

- The coordinator is a full-function device (FFD). It performs the critical function of controlling the network, starting a network, and permitting other devices to join or leave the network.
- The trust center performs authentication of devices joining the network, security management, and key distribution.
- ZigBee offers star, tree, and mesh topologies.
- It uses layer architecture for its protocol.
- It uses IEEE 802.15.4 for its physical and MAC layers.
- ZigBee protocol architecture consists of the application, application support sublayer, and network layers
- It offers direct, group, and broadcast addressing.
- A ZigBee end device can have 240 endpoints, where each endpoint may represent different application.
- ZigBee PRO uses a mesh topology, and it is a beaconless network.
- ZigBee PRO offers stochastic addressing, group addressing, asymmetric links, fragmentation, and frequency agility.
- ZigBee PRO offers many-to-one routing and multicast routing.
- ZigBee PRO offers standard and high-security modes.
- ZigBee PRO security level is set to 5.
- ZigBee PRO provides link management.
- ZigBee PRO end devices are only powered by battery.
- The ZigBee 2007 specification supports tree and mesh topologies.
- ZigBee PRO selects the best channel at startup and during operation.

REFERENCES

1. ZigBee Alliance, ZigBee Specification Document 053474r17, 2008
2. Daintree Network, "Comparing ZigBee Specification Versions," www.daintree.net/resources/spec-matrix.php
3. "How Does ZigBee Compare with Other Wireless Standards?" www.stg.com/wireless/ZigBee-comp.html
4. Craig, William C. "ZigBee: Wireless Control That Simply Works," ZigBee Alliance, 2003
5. Ember Corporation, EmberZNet Application Developer's Reference Manual, 2008
6. IEEE Std 802.15.4 2003
7. IEEE Std 802.15.4 2006