EMBEDDED TECHNOLOGY™ SERIES

Hands-On ZigBee

Implementing 802.15.4 with Microcontrollers

ZigBee™ Alliance

Fred Eady

Newnes

Hands-On ZigBee:

Implementing 802.15.4 with Microcontrollers

This page intentionally left blank

Hands-On ZigBee:

Implementing 802.15.4 with Microcontrollers

By

Fred Eady

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Newnes is an imprint of Elsevier

Newnes is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

Library of Congress Cataloging-in-Publication Data

(Application submitted.)

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN-13: 978-0-12-370887-8
ISBN-10: 0-1237-0887-7

For information on all Newnes publications
visit our Web site at www.books.elsevier.com

07 08 09 10 10 9 8 7 6 5 4 3 2 1

Printed in the United States of America.

Contents

This page intentionally left blank

Preface

My friend Jim caught word that I was writing a ZigBee-related book. Knowing that I have only written about technical things in the past, Jim asked why I was writing about an obscure 1930's magician. I've never heard of the Great ZigBee but Jim must have come across him somewhere in his travels.

This book is not a collection of magic tricks and illusions. (Although sometimes I think that RF engineering is an illusion. Think about it. Why do you have to shield RF stuff? Maybe because something very, very evil is going on inside the box? Hmmm...) This book is all about teaching you about the IEEE 802.15.4 specification and how you can apply it to your own projects using IEEE 802.15.4-compliant development tools and radios. As you will find out, IEEE 802.15.4 and ZigBee are not one and the same. So, as we discuss the nuts and bolts of IEEE 802.15.4, we'll also discuss the components that comprise ZigBee.

Not too many computing gadgets are restricted by wires these days. Just look at the do-it-all wireless camera-toting, spreadsheet-running, text-messaging, internet-browsing, emailing platform we call a cell phone. The do-it-all-with-RF philosophy of today's cell phones has spread to the ISM (Industrial, Scientific and Medical) sector. Sensors, test equipment and medical instruments are cutting the wires and replacing them with small short-range networks that require little human intervention to operate. In most cases, these small networks are based on the IEEE 802.15.4 specification. There are an unlimited number of additional applications for small IEEE 802.15.4 networks and that's why I believe IEEE 802.15.4 networks and ZigBee are working solutions that engineers will adapt into our everyday lives for many years to come.

As I write these words, the ZigBee Alliance is tweaking their ZigBee specification. That's OK. Change is sometimes good. On the IEEE 802.15.4 side, those guys and gals are in the Bahamas. Things ain't gonna change too quickly over there. What that means is that the backbone of a ZigBee network, IEEE 802.15.4 networking, won't be changing significantly even though ZigBee may be going through a phase of expansion and change. Rest assured that when you finish this book you will know enough about IEEE 802.15.4 and ZigBee to make intelligent design decisions, no matter what the ZigBee protocol finally turns out to be.

While we're on the subject of protocols, many of you have asked when my 802.11g book will be available. Well, don't hold your breath. I had to pull hen's teeth to put the 802.11b book together, as no one in the industry would step forward to help me with the technical details of

the 802.11b radios. I've sent messages and placed calls to the folks that I thought would have an interest in providing you with the how-to's of embedding an 802.11g card into a microcontroller-based platform. I've received nothing in return. The same goes for SDIO. SDIO folks won't even return my calls. So, scratch both of those subjects off your wish list for now.

I can't complain about the ZigBee and IEEE 802.15.4 crowd. Out of all of the requests for assistance I generated, only a couple of them were denied or ignored. ZigBee Alliance members even referred me to other members of the ZigBee Alliance for answers and product assistance. With that, I would like to thank every IEEE 802.15.4/ZigBee product vendor and ZigBee Alliance member that returned my phone calls, answered my emails, put up with my whining and contributed to the content of this book.

You should understand that there are some things you will not get out of reading this book. This book is not a ZigBee stack doctorate-level dissertation and you won't become a ZigBee stack expert by reading this book.

Most of the IEEE 802.15.4 radio IC manufacturers offer a complete set of Gerber files that will enable you to clone their radio module if that's your goal. Building an IEEE 802.15.4-compliant radio from scratch is not something you and I will explore in this book.

If you are not familiar with microcontrollers and the communications protocols they employ, there are no in-depth tutorial discussions involving SPI and RS-232 in the pages of this book. I also pretend (we will never assume anything in this book, as assumption can turn you into a donkey) that you know enough basic C to follow along with the code examples I'll be offering to you throughout the book. If you're challenged in these areas, there are many fine Elsevier titles that you may find helpful.

On the other hand, there are many things that you *will* take away from reading these pages. The ZigBee protocol is based on the transport mechanism provided by an IEEE 802.15.4 network. You and I will begin at the lowest layers of the ZigBee stack, the IEEE layers, and work our way up. I will place a strong emphasis on helping you to understand IEEE 802.15.4 networking, as you will find out that for many of your applications ZigBee network functionality provided by the ZigBee protocol is not a prerequisite for passing meaningful data between network nodes. In fact, for many applications, ZigBee networking functionality is overkill.

All of the development kit hardware in this book is the latest and greatest. My goal is to expose you to as many of the popular IEEE 802.15.4-compliant/ZigBee-ready devices available to you. So, you'll get a good dose of IEEE 802.15.4-compliant/ZigBee-ready hardware along the way up the ZigBee stack.

Schematic diagrams of the various IEEE 802.15.4-compliant/ZigBee-ready radios and development kits will be scarce in the paper pages of this book. It is not my intent to reprint datasheet information that you can download from the manufacturers' web sites. However, if there is any supporting documentation that is important to the idea I'm trying to convey to you and it's not something you can easily download, you will find it on the Companion website that accompanies this book.

My wife says I talk too much and my Mom says that, when I do talk, nobody knows what I'm talking about. So, with that I'll shut up and let you get on with climbing through the layers of the ZigBee stack. I sincerely hope you have as much fun reading this book as I have had writing it ☺

This page intentionally left blank

What's on the Companion Website?

Following is a list of items included on the accompanying Companion website:

- UDP (User Datagram Protocol) Primer
- ARP (Address Resolution Protocol) Primer
- Frame Thrower II Source Code
- Rabbit 3000 Hardware Reference
- Cirronet Schematics
- Texas Instruments CC2420 Project with source code
- Microchip MRF24J40 Project with source code

This page intentionally left blank

CHAPTER 1

Speaking the Language

Some famous person once said, "No matter where you go, there you are." No matter where you may find yourself, it's always a good idea to know how to speak the language. For instance, when you find yourself in a foreign country, phrases like "Thank you," "Hello" and "I need to use your bathroom" can come in very handy, depending on the situation. The same philosophy holds true when it comes to learning about things technical. To that end, I'm going to take the stance that you are reading this book because you want to know more about IEEE 802.15.4 and ZigBee. In this chapter, I'm going out one step further and will work with the pretense that you know absolutely nothing about IEEE 802.15.4 or ZigBee. So, in my mind, my job is to teach you to speak the language of ZigBee and subsequently IEEE 802.15.4. Once you become familiar with acronyms like PSDU, MPDU, NWK, PAN and MAC, the rest of the ZigBee puzzle and the underlying IEEE 802.15.4 protocol will begin to come together more easily for you. You'll need to understand the nuances of ZigBee-speak and IEEE 802.15.4-speak before we move into the actual hands-on portion of this book. Otherwise, you and I will just be mindlessly assembling meaningless ZigBee radio building blocks and crawling through undecipherable C source code.

If you're new to the concept of ZigBee, I want to introduce you to the world of ZigBee the right way. So, we'll start at the beginning of ZigBee time. However, first things first. It is required that you carve the ZigBee international anthem into your memory bank. So, get up out of that recliner and repeat after me:

> ZigBee: Wireless control that simply works.
>
> *Say it again, louder:*
>
> **ZigBee: Wireless control that simply works.**
>
> *I can't hear you!*
>
> **ZigBee: Wireless control that simply works.**

A True Story about a Couple of Flying Bugs

I don't know about you, but for me the ZigBee pledge of allegiance sets the tone within which ZigBee was initially designed. However, ZigBee wasn't always ZigBee, if you know what I mean. I actually came across an old Philips presentation dated June 26, 2000 that laid out the plans for what was then called the Philips RF-Lite Program. Interestingly enough, the presentation begins with a painting called *The Tower of Babel* and in the liner notes there are

associated intellectual comments and interpretations of the Tower of Babel story. Although I found this to be pretty weird, of course, the idea was to convey that RF-Lite would cut through the clutter of remote control and existing competitive radio systems of the day.

As you progress through the Philips RF-Lite presentation, the concept of Firefly is presented—yet another protocol, but named after a flying bug. It is strongly believed that ZigBee is supposedly named for bees doing that zig-zag thing they do that always seems to find the best flowers and the hive. So, get used to references to flying bugs, particularly the bee.

By the way, ever wonder where lightning bugs (that's what us Southern kids called fireflies) went during the day?? Well, let me tell you. Those little buggers hide amongst the trees and vegetation during the day. And, if you think fireflies are docile little creatures that glow for our delight, get real. These guys come out of the gate eating meat and that glow they produce is for finding sex in the city. It has been said that if a male flashes the wrong signal, a female of another species of firefly will descend upon him and, yep, you guessed it, eat him up.)

Firefly was a spin-off of HomeRF-Lite, which was touted as a very low-cost method of low-speed data transfer that consumed very little power. (Hmmm...keep that low-power definition of HomeRF-Lite and Firefly in your long-term memory cells, as I guarantee you'll experience a little déjà vu as you continue to learn more about ZigBee and IEEE 802.15.4 networking.) A Firefly working group was formed and face-to-face quarterly meetings were planned. (Hmmmm...as I write this text, a "quarterly" ZigBee Alliance Open House is being held in Seoul, Korea and a new tactical direction for ZigBee was announced.) The Firefly working group included some big guns such as Panasonic, Texas Instruments, Honeywell, Invensys, Lego and Mattel. (Hmmm...Can you say Chipcon...Can you say Texas Instruments...Can you say Chipcon IEEE 802.15.4 radios now owned by Texas Instruments? You'll also see Panasonic play a part in IEEE 802.15.4 and ZigBee if you continue to read this little ZigBee book. Honeywell and Invensys are currently ZigBee Alliance members along with Texas Instruments. Hmmmm...)

Firefly was to be a low-speed product with a data throughput minimum of 10 Kbps and a maximum throughput of 115.2 Kbps. I can't provide any hardcopy proof that the Firefly communication link speeds were chosen to interface to and/or replace existing products with existing RS-232 serial ports, but those Firefly speeds fit nicely within practical minimum and maximum speeds of a typical RS-232 serial port.

The projected range of Firefly-based products was specified between 10 and 75 meters. Node count for a Firefly network maxed out at 254 with a maximum of four of what was termed "critical" devices. Up to 100 Firefly networks could be co-located. The real kicker was that a Firefly node would cost less than $3.00 and be able to operate up to 2 years before the Firefly's tail light would go dark.

The license-free ISM band was chosen for Firefly nodes, which would automatically insert and disassociate themselves in the network as required. Firefly was obviously aimed at indoor/outdoor use, as the marketing requirements listed RF penetration through walls and ceilings and home/garden use. To help eliminate interference with other devices operating in the same

ISM bandwidth, the Firefly nodes would use DSSS (Direct Sequence Spread Spectrum) technology and Carrier Sense Multiple Access (CSMA-CA) listen-before-transmit network access.

The Firefly protocol stack looked much like stacks look today. Data from the Firefly radio entered via a PHY (Physical) layer. The Firefly MAC (Medium Access Control) layer accepted data from the PHY layer and pushed it up to the Firefly DLC (Data Link Control) layer. The application layer resided inside the Firefly node and was accessed by an external user interface via API (Application Program Interface) calls. The configuration I just described would have resided in a Firefly slave node. A master Firefly node inserted a NWK (Network) layer between the DLC layer and the application layer.

As you've already ascertained, a master/slave relationship formed the Firefly network topology, with the master node being in direct communication contact with each slave node. This type of topology creates a virtual peer-to-peer communications link as every node can talk to every other node in the star as long as the master can pass the messages between the slave nodes that need to talk to each other.

Meanwhile, there were a number of engineers that had determined that Wi-Fi (the subject of my previous book) and Bluetooth, which is now trying to come into its own, as everyone has a Bluetooth cell phone interface in their ear, weren't going to cut it in some applications. What these guys and gals wanted was a self-healing ad hoc network of digital radios that could organize themselves into a cohesive and orderly network without external intervention. Simply put, they wanted a working Firefly. However, that was not going to be. The IEEE was already working on 802.15.4 by this time and the IEEE 802.15.4 standard came to life in 2003 and learned to fly (not glow and fly) in 2004. While all of this IEEE stuff was going on, the ZigBee Alliance sprouted from the ground in 2002 and it now looks like the ZigBee acorn is going to be a really big tree. As for the Firefly project, we all know what happens when fireflies are left in the jar too long.

Déjà vu

Although Firefly's tail light was glowing more dimly in the jar as each hour passed, many of the attributes of Firefly would find their way out of that jar and into ZigBee. Remember this? Firefly was a spin-off of HomeRF-Lite, which was touted as a very low-cost method of low-speed data transfer that consumed very little power. Well, how about this? ZigBee was designed as a low-speed means of data transportation, which consumes very little power and can operate for months or even years on a single battery. When compared with other wireless communications systems that operate in the license-free ISM band, ZigBee comes in on the lowball side as far as cost per node is concerned. As you read more and more about ZigBee and IEEE 802.15.4, think about what you've already read about Firefly. You'll experience déjà vu all over again.

The Muhammad Ali of Networks

I'm old. I still remember a young man from Louisville, Kentucky named Cassius Clay who stunned the world by knocking out a bigger and more powerful Sonny Liston. (Sonny was