DESIGN AND EVALUATION OF A CUSTOM ZIGBEE PLATFORM

Dino Fizzotti

A dissertation submitted to the Faculty of Engineering and the Built Environment, University of the Witwatersrand, Johannesburg, in fulfilment of the requirements for the degree of Master of Science in Engineering.

Johannesburg, 2011

Declaration

I declare that this dissertation is my own, unaided work, other than where specifically acknowledged. It is being submitted for the degree of Master of Science in Engineering in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in any other university.

Signed this _____ day of _____ 2011

_____

Dino Fizzotti

Abstract

Wireless sensor networks offer significant advantages over wired solutions, including savings in installation and maintenance costs. The ZigBee stack specifies additional application and networking layers to be used with the IEEE 802.15.4 low-rate wireless personal area network standard. A custom hardware and software platform is detailed, and measurements are performed to characterise the platform. Packet Error Rate (PER) measurements for both a star network and a multi-hop network show that the PER increases as the number of devices simultaneously transmitting increases. The maximum goodput (data payload bits transmitted over time) attained is 37 kb/s. Latency measurements show an increase in microcontroller clock speed will reduce message generation and deconstruction processing time. Device lifetime estimations show the significant effect of the chosen regulator's quiescent current, reducing device lifetime when using a 9 V, 500 mAh battery from 49 days to 8 days when excluding regulator current. Valid sensor results require monitoring the device power supply, as a failing power supply influences sensor measurements whilst successful radio transmission is still possible. Devices lasted up to 71 % of the predicted lifetime.

To Nonna

Acknowledgements

I would like to thank my supervisor, Prof. George Gibbon, for allowing me the freedom to dictate my own research experience, as well as all the staff of the School of Electrical and Information Engineering for their dedication and support.

Preface

This dissertation is presented to the University of the Witwatersrand, Johannesburg for the degree of Master of Science in Engineering.

This dissertation is entitled *Design and Evaluation of a Custom ZigBee Platform.*

This document complies with the University's *paper model format.* The paper contains the main results and analysis of the research. The appendices present in detail the work conducted during the research.

As ZigBee is a fairly recent technology (the first version of the standard was published in 2003) the author feels that the reader may not be as familiar with related wireless sensor networking mechanisms as necessary for a thorough understating of the literature review. While a literature review traditionally precedes any technical chapters (or appendices, in this case) in a dissertation, the author feels that some technical background information on the ZigBee and IEEE 802.15.4 standards is required beforehand. This is why the literature review is positioned as Appendix C, with information on the IEEE 802.15.4 and ZigBee standards given in Appendix A and Appendix B respectively.

Contents

List of Figures

List of Tables

List of Acronyms

ADC	Analogue to Digital Conversion
APL	Application
APS	Application Support
APSDE	APS Data Entity
APSME	APS Management Entity
BPSK	Binary Phase Shift Keying
CCA	Clear Channel Assessment
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
DSSS	Direct-Sequence Spread Spectrum
EEPROM	Electrically Erasable Programmable Read-Only Memory
ESL	Equivalent Series Inductance
ESR	Equivalent Series Resistance
FFD	Full-function device
GTS	Guaranteed Time Slot
I^2C	Inter Integrated Circuit
IC	Integrated Circuit
ICD	In-Circuit Debugging
ICSP	In-Circuit Serial Programming
ISM	Industrial, Scientific and Medical

LDO	Low Drop-Out
LED	Light Emitting Diode
LNA	Linear Noise Amplifier
LQI	Link Quality Indicator
LR-WPAN	Low-Rate Wireless Personal Area Network
MAC	Medium Access Control
MLDE	MAC Layer Data Entity
MLME	MAC Layer Management Entity
NLDE	NWK Layer Data Entity
NLME	NWK Layer Management Entity
NWK	Network
O-QPSK	Offset-Quadrature Phase Shift Keying
OSI	Open Systems Interconnection
PA	Power Amplifier
PAN	Personal Area Network
PCB	Printed Circuit Board
PDU	Protocol Data Unit
PER	Packet Error Rate
PHY	Physical
PLME	Physical Layer Management Entity
PSK	Phase Shift Keying
RF	Radio Frequency
RFD	Reduced-function device
RSSI	Received Signal Strength Intensity
SAP	Service Access Point
SMT	Surface Mount Technology

SPI	Serial Peripheral Interface
UART	Universal Asynchronous Receiver/Transmitter
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
ZDO	ZigBee Device Objects

Design and Evaluation of a Custom ZigBee Platform

Dino Fizzotti

***Abstract*—Wireless sensor networks offer significant advantages over wired solutions, including savings in installation and maintenance costs. The ZigBee stack specifies additional application and networking layers to be used with the IEEE 802.15.4 low-rate wireless personal area network standard. A custom hardware and software platform is detailed, and measurements are performed to characterise the platform. Packet Error Rate (PER) measurements for both a star network and a multi-hop network show that the PER increases as the number of devices simultaneously transmitting increases. The maximum goodput (data payload bits transmitted over time) attained is 37 kb/s. Latency measurements show an increase in microcontroller clock speed will reduce message generation and deconstruction processing time. Device lifetime estimations show the significant effect of the chosen regulator's quiescent current, reducing device lifetime when using a 9 V, 500 mAh battery from 49 days to 8 days when excluding regulator current. Valid sensor results require monitoring the device power supply, as a failing power supply influences sensor measurements whilst successful radio transmission is still possible. Devices lasted up to 71 % of the predicted lifetime.**

I. Introduction

WIRELESS Sensor Networks (WSNs) consist of multiple devices, where each device is either a source or destination for data in a wireless network. Such devices operate autonomously, using transducers to capture data from the physical world and transfer this data to other devices in the network or to a central storage and processing device [1]. Key applications where WSNs are being employed include: plant/machine condition monitoring, structural health monitoring, asset management, healthcare, building automation/control and agriculture. There are notable advantages in using a wireless sensor network as opposed to a wired solution. Initial costs for a wired system are higher as a result of cable and terminal connection installation. The detection of faults in the transmission lines and replacement of the cables also result in greater costs [2]. Inherent characteristics of a wireless sensor system are rapid deployment and increased flexibility of sensor device placement [3].

The initial motivation behind the research presented in this document is to investigate a wireless sensor network for use on a train. Real time monitoring of transport vehicles and their goods is of crucial importance to all parties involved in the supply chain: manufacturers, logistics providers, distributors and consumers. In an effort to protect the vehicles and their cargo from damage, derailment or structural fatigue, parameters such as vibration, tilt and temperature may be measured and analysed. The IEEE 1473 standard for communications protocol aboard trains (wired solution) is the most popular solution for intra-wagon communications. It has been noted that the future of the standard lies in interoperability with wireless communications protocols. [4] [5]

With the advent of relatively cheap radio transceiver electronics and a strong focus on low power consumption and device interoperability, ZigBee has established itself as a strong contender to be the low-bandwidth wireless protocol of choice [6]. ZigBee technology has been adopted by over 350 manufacturers, with combined revenues from these companies exceeding $1 trillion (USD). Despite the current global financial slowdown, ZigBee device sales have increased an average of 62% per year since 2007. Of all the IEEE 802.15.4 devices shipped in 2009, 75% were designed specifically to work in ZigBee applications [7].

This document will focus on the the design and evaluation of a custom ZigBee platform, such that further research may apply the findings directly to railway wagon communications and related measurements.

An overview of the IEEE 802.15.4/ZigBee standards is provided in Section II, and a discussion of literature review results is given in Section III. The hardware and firmware/software design is detailed in Section IV and Section V respectively. Measurements and analysis of the custom platform is provided in Section VI, and field test results can be found in Section VII. Concluding remarks are provided in Section VIII.

II. IEEE 802.15.4 and ZigBee Overview

The IEEE 802.15 working group is tasked with developing Wireless Personal Area Network (WPAN) standards. The working group is split into task groups which handle specific areas of interest. Task Group 1, or IEEE 802.15.1 is chartered to develop the Bluetooth standard, which readers may be familiar with as technology which allows for wireless data transfer between mobile phones and personal computer peripherals. Task Group 4 was established to investigate and specify a standard for Low-Rate Wireless Personal Area Networks (LR-WPANs), focusing on low data rate, low power devices. See Appendix A for more information on IEEE 802.15.4.

ZigBee is a wireless standard developed by the ZigBee Alliance. The ZigBee alliance is a collection of global companies with interests in residential, commercial and industrial applications of Wireless Sensor Networks. Member companies have the benefits of early insight into new developments within the standard, as well as active involvement in the development of ZigBee itself. Dissemination of ZigBee specifications and documents to the public occur after access is granted to the member companies. Equipment manufacturers which feature ZigBee modules within their products must be ZigBee Alliance members, but distributors and resellers need not

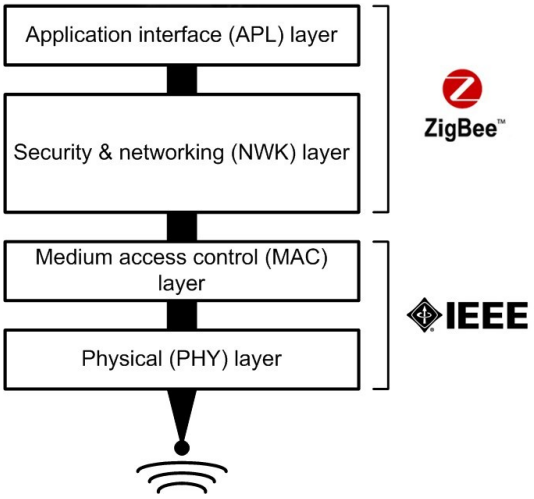


Fig. 1: The IEEE 802.15.4/ZigBee layers.

be members. Appendix B includes more information on the operation of the ZigBee stack.

A. ZigBee Architecture

The ZigBee stack is based on the Open Systems Interconnection seven-layer model, but only defines specific layers related to providing the intended functionality. The IEEE 802.15.4 standard specifies the lower Physical (PHY) and Medium Access Control (MAC) layers on which ZigBee builds upon by adding an additional Network (NWK) and Application (APL) layer, as shown in Figure 1. While encryption and secure frame transmission is supported by ZigBee, it is not mandatory. The firmware stack used in the implementation does not subscribe to these security features owing to microcontroller memory constraints. ZigBee security features are therefore omitted from the succeeding sections.

The PHY layer specifies the frequency band in which the device will operate, as well as quantifying the energy in the chosen channel and determining the link quality between two devices. The Clear Channel Assessment (CCA) mechanism is used by the PHY layer in establishing the state (busy/idle) of a channel, and precedes all transmission attempts [8].

The MAC layer allows for network synchronisation via the superframe structure, and implements the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) algorithm in an effort to avoid message transmission failure [8].

The NWK layer is responsible for message routing and route discovery, as well the storage of information about any neighbouring devices. An advantage in using the ZigBee stack as opposed to just the IEEE 802.15.4 protocol is the addition of mesh networking, which allows for dynamic route adjustment as message paths become unavailable for use [9].

The APL layer provides a framework for specifying the operation of a device with an application profile, as well as accommodating interoperability between any ZigBee devices with the same application profile. Engineers and developers interface with this layer to provide the intended functionality of a ZigBee device [9].

B. ZigBee Devices

Three general device types are specified for use in a ZigBee network: coordinator, router and end device. The coordinator is responsible for establishing the network, supporting device association and must be powered and active at all times. There is only one coordinator per ZigBee network. Routers support device association and extend the network range by relaying information to and from other routers or the coordinator. They must also be powered and active at all times, and there can be many per network. End devices cannot forward messages, and must connect to either a router or the network coordinator. End devices can be placed in “sleep” mode to conserve power and are usually the devices sourcing sensor data in a network [9].

C. ZigBee Network Topologies

ZigBee supports three distinct topologies: star, cluster tree and mesh. In a star network topology all devices are connected to a single *sink* device. The sink device in a ZigBee network is the coordinator. In a cluster tree topology ZigBee coordinators and routers can act as *parent* devices, allowing other *child* devices to associate with the network. Messages to/from a child device can only be routed via its parent. A device’s network *depth* is the minimum number of hops required for the device to receive a message from the coordinator using only parent-child hops. End devices and routers connected directly to the coordinator have a network depth of one [9].

No such hierarchical relationships exist in a mesh network. All devices are able to communicate with any other device in the network, where routing may be performed by any ZigBee router in radio range, regardless of parent-child relationships. Two important aspects of a mesh network are its self-forming and self-healing characteristics. A network which is self-forming does not need user intervention when associating new devices within the network and establishing message routing. Self-healing occurs when previously available message paths become unavailable and the network adjusts the routing mechanism to compensate such that a new attempt at message delivery is supported. Message paths will become unavailable if devices are no longer in radio range, or if the device suffers loss of power supply or hardware or firmware failure [9]. These features offer a particular advantage when placed in the context of a railway wagon based wireless sensor network. Individual wagons (and the attached wireless network devices) may be added, removed or swapped out at railway depots, requiring autonomous reconfiguration of the network.

III. Literature Review

A selection of academic research in IEEE 802.15.4 and ZigBee wireless sensor networks is provided in Appendix C. Analysis of the literature shows that there is active research in characterising ZigBee network performance. Common performance metrics include packet error rate, throughput/goodput, message latency and power consumption. Results differ from study to study, and platform to platform. Throughput results are considerably lower than the theoretically achievable 250 kb/s offered by IEEE 802.15.4/ZigBee. A number of the

studies comment on the difficulty of repeatable measurements, especially with respect to loss of network connectivity owing to multipath fading effects.

Five of the twenty one reviewed ZigBee studies use a custom platform, while the remaining sixteen studies make use of a manufacturer development kit in evaluating a wireless sensor network. Across all the studies, the Atmel ATmega128L and the Texas Instruments CC2420 are the most popular choices for a microcontroller and radio transceiver respectively. The ATmega128L microcontroller is the most popular microcontroller for manufacturer development platforms as well as custom research platforms. More than half of all reviewed platforms use the CC2420 radio transceiver, a possible reason being that it was the first IEEE 802.15.4 compliant radio transceiver.

IV. Hardware Design

The author has implemented a custom hardware configuration, the "DFZ" platform, based on the Microchip PICDEM Z development kit. Appendix D provides detailed design notes for the hardware platform. The electronic components are chosen for their low power characteristics and small form factor. With the exception of the microcontroller, all the electronic components are in surface mount packages. Using surface mount packages reduces electromagnetic interference and emissions, uses up less Printed Circuit Board (PCB) real estate, and results in a cheaper bill of materials than when using through-hole equivalents [10],[11].

A. Microcontroller

The DFZ platform uses a Microchip PIC18LF4620 microcontroller. The microcontroller may be programmed to act as any ZigBee device (coordinator, router or end device). Features of the PIC18LF4620 include [12]:

- Customisable sleep, idle and run modes of operation
- System frequency of up to 40 MHz
- Watchdog timer (4 ms to 131 s)
- 3 external interrupts
- Serial Peripheral Interface (SPI) bus, Inter Integrated Circuit (I^2C) bus and RS-232 Universal Asynchronous Receiver/Transmitter (UART) connectivity options
- 36 possible input/output pins
- 13 10-bit analogue-to-digital conversion channels
- 1 8-bit timer, 3 16-bit timers
- In-circuit programming and debugging

B. Radio Transceiver

The Microchip MRF24J40MB transceiver module enables the Radio Frequency (RF) communication of the ZigBee network. The module operates at 2.4 GHz in the Industrial, Scientific and Medical radio band. The module uses a 4-layer PCB featuring dedicated planes for RF signals, digital (microcontroller) signals as well as power and ground. A PCB trace antenna is employed for RF transmission and reception, and a metallic shield structure covers the electronic components to avoid RF interference.

The MRF24J40MB is placed on its own PCB daughterboard which then connects to the DFZ motherboard. This allows for more flexible troubleshooting, as replacement transceiver modules can be tested in the same motherboard, as well as allowing the older PICDEM Z transceiver modules to be placed in the new custom motherboards for comparison.

Specifications of the MRF24J40MB include [13]:

- Integrated Power Amplifier, Low Noise Amplifier and PCB antenna
- Up to 1.2 km possible range (outdoor open area free line of sight conditions)
- Reception mode current consumption: 25 mA
- Transmission mode current consumption: 130 mA
- Sleep mode current consumption: 5 μA
- -102 dBm receiver sensitivity
- +20 dBm transmitter output power
- IEEE 802.15.4 standard compliant
- Supports ZigBee protocol

C. Power Supply

A National Instruments LM2937 low drop-out regulator is used to supply 3.3 V to all subsystems on the node board. It operates with an input voltage in the range of 4.75 to 26 V and is able to supply up to 400 mA continuously. A combination of two capacitors in parallel are placed on the input and output of the regulator to reject noise and to provide regulator stability. A capacitor's frequency response is dominated at high frequencies by the inductance owing to its casing geometry. The DFZ devices use different capacitor casing sizes to increase the decoupling effect by extending the high frequency low impedance characteristics of the combination [11],[14].

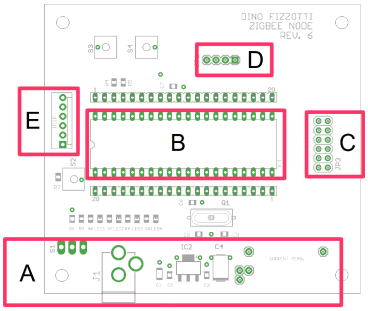
D. Serial Communication

Pin headers are provided to which a custom level-translating board may be connected in the event that serial output to a computer terminal is required. A serial communication daughterboard is tethered permanently to the DFZ coordinator device, and connected as needed for other devices (usually for debugging purposes).

E. User Input/Output

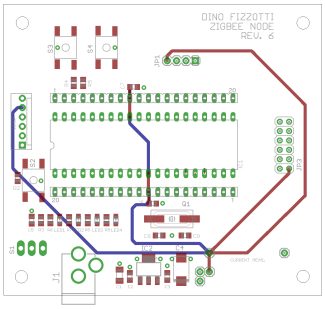
Two momentary push-buttons are available to the user, as well as a microcontroller reset button. Four Light Emitting Diodes (LEDs) are available as visual outputs. The LEDs are typically used during debugging and as indicators when taking measurements. It is not advisable to have the LEDs on for extended periods of time when used in-application as each LED draws 4 mA when on.

Female header pins are connected alongside the microcontroller's pins which allow for small daughterboards to be plugged in above the microcontroller. This allows sensors, external memory, communication modules, etc. access to all the microcontroller pins.



A: Power supply
B: Microcontroller
C: RF daughterboard connection
D: Serial comms. connection
E: In-circuit programming connection

(a) PCB Zones.



(b) Power supply track routing.

Fig. 2: PCB layout features.

F. Programming and Debugging

Pin headers are provided to which a programming device which follows Microchip's In-Circuit Serial Programming (ICSP) protocol and pin-out configuration may be connected. This allows each microcontroller to be programmed as it sits in its individual PCB. The ICSP interface also allows for In-Circuit Debugging (ICD), allowing PC software to monitor the microcontroller's registers during application operation.

G. PCB Layout

The PCB layout includes a two-layer design owing to increased costs for multi-layer PCBs and inclusion of ground fill in both layers to reduce radiated emissions. Zoning of functional areas serves to reduce noise coupling, and a wide power supply track is routed in a star network layout in an effort to decrease track impedance and noise coupling [11],[15]. Figure 2 depicts some of the PCB layout features.

V. Firmware and Software

See Appendix E for more details on the firmware and software.

A. The Microchip ZigBee Stack

The firmware consists of the Microchip ZigBee stack, as well as user application code. Microchip's ZigBee stack is free to download and use for research and prototyping purposes. Companies or manufacturers wishing to distribute a product based on the Microchip ZigBee Stack must first become a member of the ZigBee Alliance. Features of the Microchip stack include [16]:

- Certified ZigBee-2006 compliant
- Supports 2.4 GHz band of operation
- Support for all device types: coordinator, router, end device
- Uses nonvolatile storage for group, neighbour and routing tables
- Portable across many of Microchip's PIC18 and PIC24 microcontrollers
- Supports Microchip's MPLAB C Compiler for PIC18 and PIC24 microcontrollers

B. Custom Application Profile

ZigBee devices use an application profile made up of clusters and attributes as a way of structuring application specific data operations. For the purposes of this research a custom application profile is implemented across all devices. Mechanisms for device information, temperature sensor readings and network performance measurements are provided for in the custom application profile.

C. Custom Operational Modes

At compile-time the ZigBee end device application firmware can be programmed in one of two modes: *conversation* or *report*. In conversation mode the sleep period is short enough for the end device to reliably receive messages from the coordinator at any time. This allows for specific control over the operation of the end device at any time, but results in increased power consumption. The following mechanisms are supported in conversation mode:

- Single sensor reading request
- Enable/disable continuous sensor readings
- Enable/disable monitor mode sensor readings
- Set/retrieve high and low region thresholds for sensor readings
- Ping device
- Initiate Packet Error Rate and goodput measurements
- Request arbitrary single data frame (for test/measurement purposes)

In report mode the end device operates autonomously, waking up from extended periods of sleep to send messages to the coordinator. In this mode the coordinator may not reliably transmit messages to the end device as the end device may be in sleep at the time of transmission and not wake up in time to receive any retransmissions. The advantage of report mode is increased device lifetime as power consumption is decreased. The disadvantage is the lack of control from the coordinator

over the end device. In report mode the end device may either send continuous sensor readings or be in monitor mode.

D. DFZCon Software

A platform-independent Python script, entitled "DFZCon", forms the basis of the software used to monitor and control the ZigBee network used in this research. The script polls the serial port for new data and executes relevant procedures based on identification strings preceding the data from the coordinator. The script interfaces with a SQLite database to log device information and sensor readings.

VI. Measurements and Results

The succeeding sections provide a summary of the results and analysis of measurements performed using the DFZ devices. For more details of the DFZ platform measurements see Appendix F.

A. Packet Error Rate Measurements

Packet Error Rate (PER) is a measure of the number of failed packets as a percentage of the total number of transmitted packets, as seen by the receiving device. PER measurements are used to characterise the probability of a successfully received message transmitted from one device to another. The expression used in calculating the PER from the number of successfully received packets is given in Equation 1.

$$PER\ \% = \left(1 - \frac{P_r}{P_t}\right) \times 100 \tag{1}$$

P_r is the number of packets successfully received by the coordinator, and P_t is the cumulative number of packets sent by all transmitting devices.

Messages are sent at intervals which are a multiple of a 10.2 ms microcontroller timer interrupt. The exact timing of a message transmission cannot be guaranteed as the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) mechanism may introduce random delays (see Appendix A). The transmission timing for short interval, large payload messages also fluctuates as timer interrupts occur during message frame generation.

1) PER in a Star Topology: Figure 3(a) and Figure 3(b) present the PER for devices using a star topology, as a function of the number of simultaneous transmitting devices, for 10 and 99 byte payloads respectively. Increasing the number of devices simultaneously transmitting messages increases the PER. The failure rate per number of transmitting devices also increases with increased payload, for a given transmission interval. For short message intervals across all payload sizes the PER converges to between 54% and 62%, indicating throughput saturation for multiple devices transmitting at such intervals.

2) PER in a Multi-hop Network: A multi-hop network is one where a message is relayed by one or more intermediate devices en route to its destination. Network devices are "daisy-chained" together to evaluate PER performance in a multi-hop topology. Figure 3(c) shows the results obtained from the PER measurements in a multi-hop network topology. The PER increases as the number of hops increases above two, with shorter message intervals having higher failure rates. The average difference (over all intervals) between hop two and three is 6 % PER and between hop 3 and 4 it is 3.7 % PER. There is a large increase of 13.6 % in the average PER between hop 4 to hop 5. Implementing a ZigBee network on a train will most likely require multi-hop transmissions. If the coordinator (data sink) is placed in the locomotive, wagons towards the end of the train may be out of direct range and will require routers to forward messages.

B. Goodput in a Star Topology

Goodput is the number of useful bits transmitted or received per second, and excludes bits pertaining to network overhead [17]. The expression used in calculating the goodput is given in Equation 2.

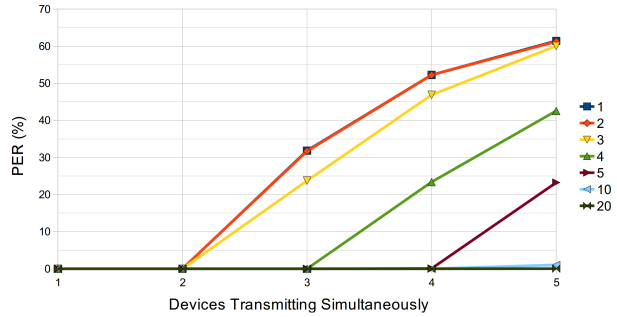
$$Goodput\ (bits/S)\ = \frac{P_r \times payload \times 8}{T_r} \tag{2}$$

P_r is the number of packets successfully received by the coordinator, *payload* is the number of bytes in the message payload, and T_r is time taken between, and including, reception of the first and last packets received.

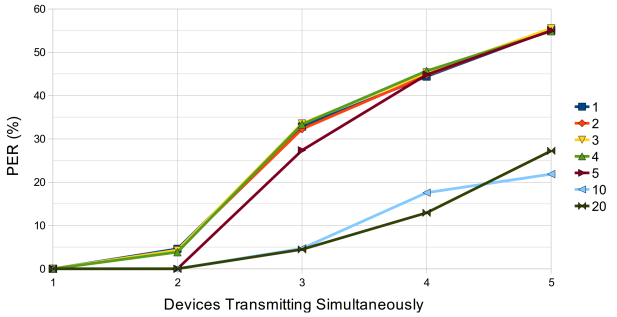
Figure 3(d) shows the results from goodput measurements in a star network featuring up to 5 devices transmitting a maximum payload of 99 bytes at the shortest possible interval. Deviation from the mean goodput value is also included. The highest goodput result recorded exists for two simultaneously transmitting devices, at 37 kb/s. This is 14.8 % of the theoretical maximum of 250 kb/s throughput stated in the IEEE 802.15.4 standard. A convergent value exists with the inclusion of additional transmitting devices: when three, four and five devices are simultaneously transmitting the goodput deviation from the mean value (31.1 kb/s) is less than 7%. The higher goodput value for two transmitting devices relative to three, four and five transmitting devices can be attributed to channel access contention, and the delays introduced by the Carrier Sense Multiple Access with Collision Avoidance mechanism.

C. Message Latency and Timing Characteristics

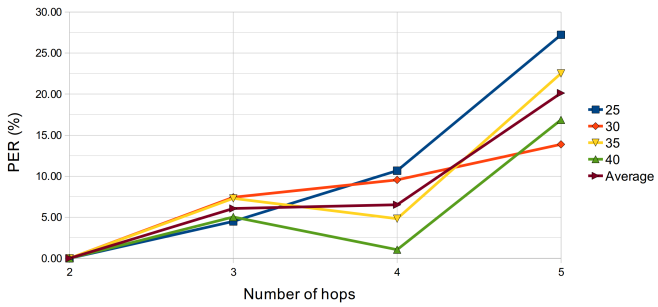
Three key time periods are defined for a ZigBee message transmission, designated A, B and C. Period A represents the time taken for the ZigBee APL layer to generate the frame before being passed on to the PHY layer for transmission. Period B represents the time taken for responsibility of the message to pass from the transmitting device to the receiving device. Period C is the time duration including the frame reception and deconstruction routines, which must occur before it may be of use in the APL layer on the receiving device. Figure 3(e) shows



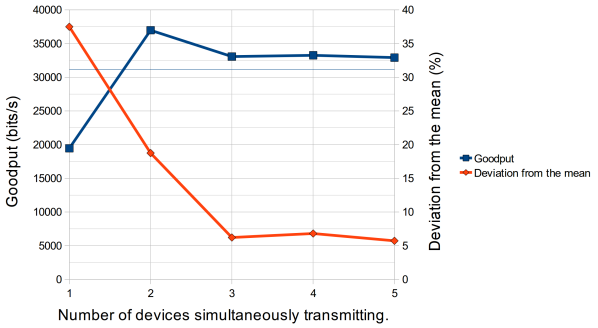
(a) PER results for star topology with a 10 byte payload. Legend indicates different transmission intervals (multiples of 10.2 ms).



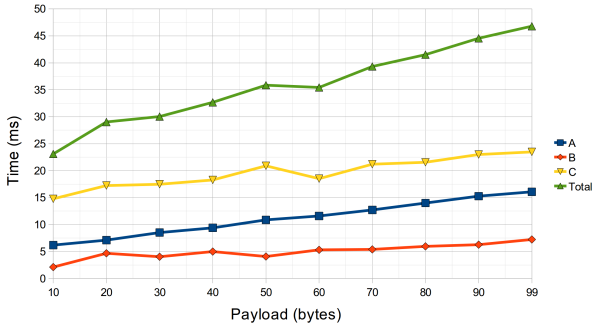
(b) PER results for star topology with a 99 byte payload. Legend indicates different transmission intervals (multiples of 10.2 ms).



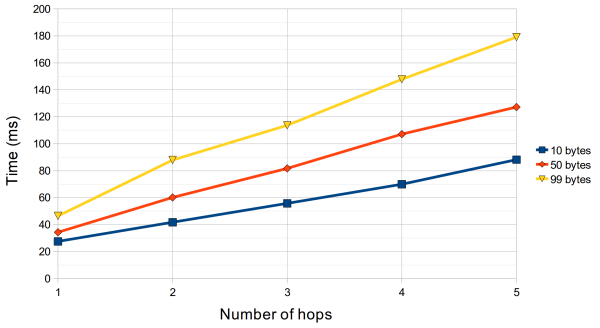
(c) PER results for a multi-hop topology with a 99 byte payload. Legend indicates different transmission intervals (multiples of 10.2 ms).



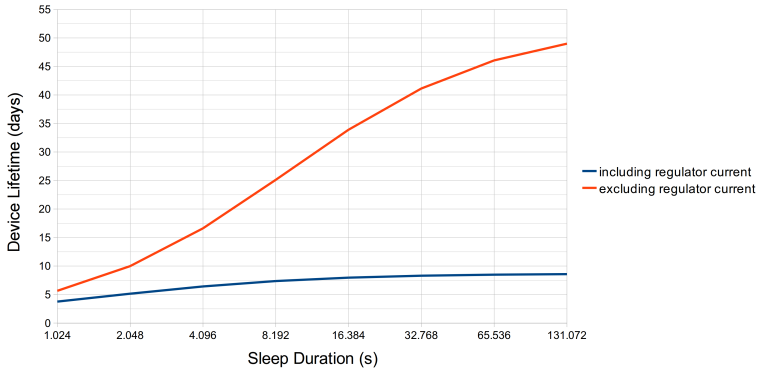
(d) Star network goodput results.



(e) Single hop message transmission results.



(f) Latency measurements for a multi-hop network.



(g) Device lifetime.

Fig. 3: DFZ platform performance results.

the timing results for different payload sizes. A linear relationship is evident from the results, with an average of 2.42 ms per 10 byte increase in payload size. The increase in payload size has a greater influence on message frame generation and deconstruction time than on the over-the-air transmission time, indicating that an increase in microcontroller clock speed may decrease latency. Figure 3(f) presents the latency results for a multi-hop network with different message payloads. Message latency is important when considering critical measurements related to railway wagon safety. Devices further from the coordinator (assumed to be situated in the locomotive) may require multiple transmission hops, thus increasing the end-to-end delay for successful message reception.

D. End Device Lifetime Estimation

A DFZ end device continuously cycles from an active state to a sleep mode in an effort to conserve power. Power conservation increases device lifetime, as end devices are typically powered from batteries or energy harvesting systems. The microcontroller sleep duration is selected by a postscale value in one of microcontroller's configuration registers. The nominal watchdog timer value is 4 ms, and the postscale value may be any power of two from 2^0 (4 ms) through 2^{15} (131072 ms or 2.18 minutes). Figure 3(g) depict device lifetime for a device operating from a 9 V battery with a capacity of 500 mAh, with and without taking the low drop-out regulator quiescent current into consideration. The influence of the regulator's quiescent current decreases the device lifetime from 49 days to 8 days when using the longest sleep duration available between message transmissions. It is recommended that an alternative linear LDO regulator is used for any further research, one with much a lower typical quiescent current but also capable of sourcing sufficient current for additional electronics. A regulator with a lower quiescent current will increase the device lifetime, thus decreasing the frequency of battery replacement.

E. Improving Results with Antenna Diversity

Multipath interference occurs when electromagnetic waves transmitted from a single device reflect off various obstacles, presenting the receiving device with multiple signals, differing in phase and amplitude. Destructive interference occurs when signals arrive out of phase, and may result in decreased throughput and increased error rates, requiring multiple re-transmissions to achieve successful message reception. A solution to multipath fading exists in the implementation of antenna diversity. This is achieved by using a single RF transceiver coupled to two multiple antennas using a high speed RF switch. Antenna selection is typically based on the RSSI value observed by each antenna during the the preamble of a packet transmission. The antenna from which the higher RSSI value is detected will be chosen to receive the remainder of the message following the preamble. [18] [19]

Implementing antenna diversity on the DFZ devices will require replacement of the MRF24J40MB transceiver module with a custom RF subsystem, consisting of a transceiver, power amplifier, low-noise amplifier, RF switch and antenna interfaces.

VII. Field Test

Where further research may implement the DFZ devices on railway wagons, the field test discussed in this section demonstrates a "proof of concept" for the custom ZigBee platform. A ZigBee network is established, end devices are associated to the network and temperature measurements are logged for later analysis.

A Microchip TC1047 temperature sensor with an analogue output was added as a sensor component to DFZ end devices. A 9 V 6LR61 battery was used as a power supply for the end devices, and an AC-DC converter was used to supply power to the coordinator from a mains outlet. The end devices were programmed at compile time to operate in "report" mode (see Section V-C), with a sleep/transmit cycle duration of 65.5 s. Some of the batteries were not new and have been used previously in an effort to observe what happens when there is insufficient power to support the devices. The coordinator node was connected to a PC running the DFZCon script (see Section V-D). The DFZCon script logged all sensor transmissions and successful network joins. The coordinator device and five end devices (labelled A to E) were scattered around three rooms occupied by postgraduate students of the School of Electrical and Information Engineering.

Figure 4 presents the results obtained by the DFZ ZigBee devices. Of special interest are device's B and E. Device B was placed in a server room, where a constant low temperature is recorded up until device failure. The thermostat action of the server room air conditioning is evident from the continuous high-low cycles. Device D was placed on a ledge on the inner side of an outside-facing window. Its proximity with the outside surface of the building, and the poor thermal insulation offered by a single glass window pane is evident in the large change in temperature experienced over a day/night cycle.

Device power supply failure is indicated by a steady increase in recorded temperatures, up to the point at which wireless communication ceases. This implies that monitoring of the power supply is required for valid temperature measurements. The longest recorded device lifetime of 5 days and 16 hours days is 71 % of the 8 days expected from the results in Appendix F. This can be attributed to a lower battery capacity used in the field test when compared to that chosen for the prediction and the effect of temperature on battery performance. It must be noted that 5 days of battery lifetime will require frequent replacement for extended use. It is recommended that a different battery technology with a greater energy density and temperature resilience (such as lithium-ion) be chosen for use in devices on railway wagons. As noted in Section VI-D, an alternative linear low drop-out regulator with a lower quiescent current will also extend device lifetime.

VIII. Conclusion

The advantages in using a wireless sensor network over a wired solution for use in railway wagon condition monitoring includes rapid, flexible device deployment, and reduced installation and maintenance costs. The benefits of a ZigBee network are its self-forming and self-healing characteristics,

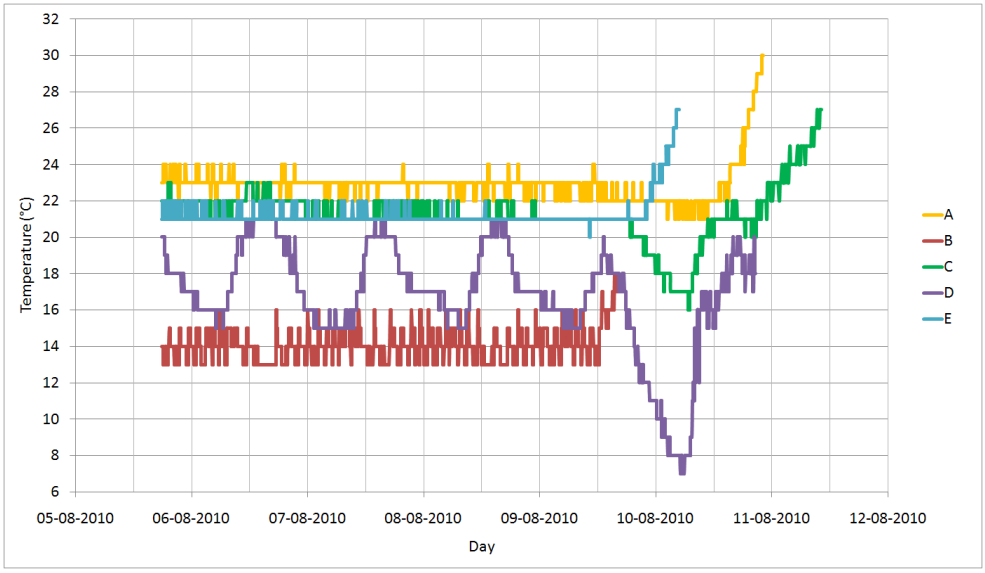


Fig. 4: Field test results.

where network hierarchy and message routing will be automatically reconfigured should railway wagons be added to or removed from the train.

The DFZ devices form part of an experimental ZigBee platform, featuring custom hardware, software and firmware considerations. Measurements of the DFZ platform show limits for network performance and device lifetime. A maximum goodput value of 37 kb/s is observed. Packet Error Rates converge to between 54 % and 62 % when multiple devices are transmitting simultaneously at short intervals, and it is recommended that for a low error rate message transmission occur at the largest intervals possible, with the smallest message payload. Lifetime predictions when using a 9 V battery yield a maximum of 8 days for the DFZ devices. Power consumption results indicate a possible lifetime of 49 days when excluding the effect of the regulator current. This indicates the great effect the regulator quiescent current has on the device.

Field test results verify the operation of the software and firmware application features, where room temperatures were successfully recorded and analysed. The results suggest monitoring of the power supply is critical in validating transmitted sensor measurements.

Measurements in multi-hop environments for PER and latency are of particular interest for ZigBee railway wagon implementations. Assuming the coordinator (data sink) to be placed in the locomotive, messages sent from wagons further down the train may require multiple retransmissions from router devices (should the source device be out of range of the coordinator). It is recommended that a lithium-ion battery technology be used and that the linear LDO regulator be replaced with an alternative regulator with lower quiescent current characteristics. These changes will help extend the device lifetime and reduce the frequency of battery replacement.

REFERENCES

[1] A. Willig, "Wireless Sensor Networks: Concepts, Challenges and Approaches," *Elektrotechnik und Informationstechnik*, vol. 123, pp. 224–231, 2006.

[2] M. Cinque, D. Cotroneo, G. D. Caro, and M. Pelella, "Reliability Requirements of Wireless Sensor Networks for Dynamic Structural Monitoring," in *DSN 2006 The International Conference on Dependable Systems and Networks*, 2006.

[3] B. Lu, L. Wu, T. G. Habetler, R. G. Harley, and J. A. Guitérrez, "On the Application of Wireless Sensor Networks in Condition Monitoring and Energy Usage Evaluation for Electric Machines," in *IECON 2005 31st Annual Conference of IEEE Industrial Electronics Soceity*, 2005.

[4] G. M. Shafiullah, A. Gyasi-Agyei, and P. Wolfs, "Survey of Wireless Communications Applications in the Railway Industry," in *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, 2007.

[5] P. A. Laplante and F. C. Woolsey, "IEEE 1473: An Open-Source Communications Protocol For Railway Vehicles," *IT Professional*, vol. 5, no. 6, pp. 12–16, 2003.

[6] "Supported by Manufacturers with Revenues Surpassing $1 Trillion, ZigBee crosses the Chasm," Smartmeters, June 2010, last accessed 02/08/2010. [Online]. Available: http://www.smartmeters.com/the-news/1012-zigbee-surpasses-1-trillion.html

[7] "ZigBee Crosses the Chasm: A Market Dynamics report on IEEE802.15.4 and ZigBee," ON World, May 2010, last accessed 02/08/2010. [Online]. Available: http://onworld.com/zigbee/

[8] *IEEE 802.15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, IEEE Computer Society, October 2003, revision designated IEEE 802.15.4-2003.

[9] *ZigBee Specification*, ZigBee Standards Organization, Document ID: 053474r13, December 2006.

[10] *PCB Design Guidelines for Reduced EMI*. Texas Instruments, 1999. [Online]. Available: http://www.ti.com/

[11] H. Ott, *Electromagnetic Compatibility Engineering*. Hoboken, New Jersey, USA: John Wiley & Sons, 2009.

[12] *PIC18F2525/2620/4525/4620 Data Sheet*, Microchip Technology Inc., Document ID: DS01146B, 2008.

[13] *MRF24J40MB Data Sheet*, Microchip Technology Inc., Document ID: DS70599B, 2009.

[14] T. Schmitz and M. Wong, *Choosing and Using Bypass Capacitors*, Intersil Americas Inc., Application Note AN1325.0, August 2007.

[15] *Power Supply and Ground Design for a WiFi Transceiver*, Maxim Integrated Products, Application Note 3630, September 2005.

[16] D. P. Lattibeaudiere, *Microchip ZigBee-2006 Residential Stack Protocol*, Microchip Technology Inc., Application Note AN1232, document ID: DS01232A, 2008.

[17] S. Farahani, *ZigBee Wireless Networks and Transceivers*. Newton, MA, USA: Newnes, 2008.

[18] *AT86RF231 Antenna Diversity*, Atmel Corporation, Application Note AVR2021, 2008.

[19] M. Burns and T. Starr, *Implementing Diversity Using Low Power Radios*, Texas Instruments, Application Note AN085, 2010.

Appendix A

IEEE 802.15.4

A.1 Introduction

The IEEE 802.15 working group is tasked with developing Wireless Personal Area Network (WPAN) standards. The working group is split into task groups which handle specific areas of interest. Task Group 1, or IEEE 802.15.1 is chartered to develop the Bluetooth standard, which readers may be familiar with as technology which allows for wireless data transfer between mobile phones and personal computer peripherals. Task Group 4 was established to investigate and specify a standard for Low-Rate Wireless Personal Area Networks (LR-WPANs), focusing on low data rate, low power devices.

Section A.2 discusses the IEEE 802.15.4 protocol architecture. The device types and network topologies implemented in IEEE 802.15.4 are detailed in Section A.3 and Section A.4 respectively. The protocol's frame structure is detailed in Section A.5. The Physical and Medium Access Control layers are presented in Section A.6 and Section A.7. This document summarises some of the structures and functions of the IEEE 802.15.4-2003 version of the standard, as this is the version to which the Radio Frequency (RF) transceiver chosen for the hardware implementation adheres to. There does exist a newer version of the standard, with a "-2006" suffix, as discussed in Section A.8. Concluding remarks can be found in Section A.9.

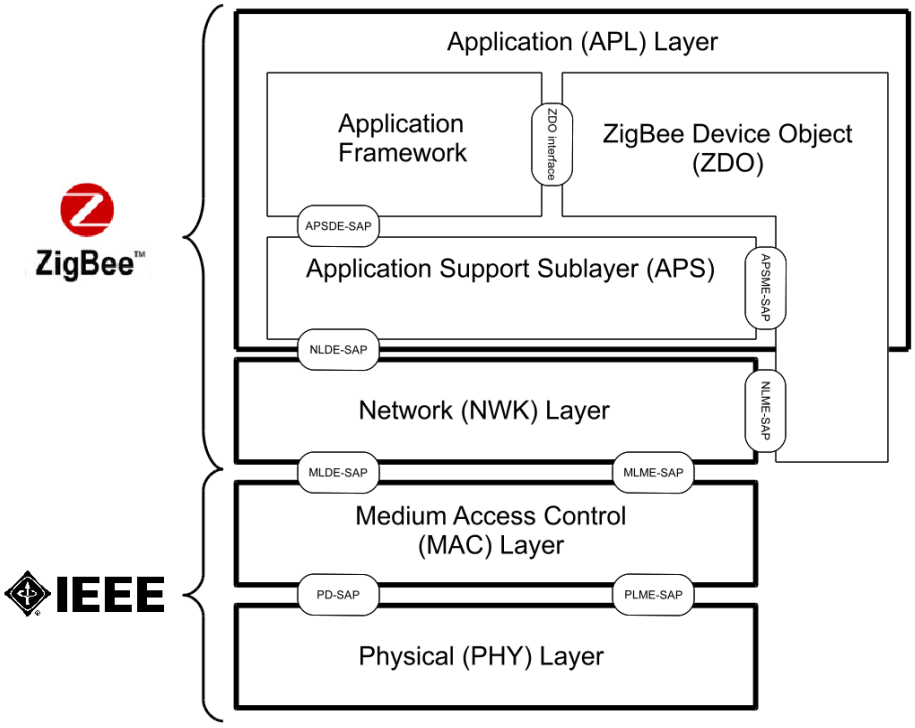


Figure A.1: The IEEE 802.15.4/ZigBee layers and interfaces.

CITATION DISCLAIMER

Unless otherwise specified, the information detailed in this appendix is a summary of that found in the IEEE 802.15.4-2003 standard [1] and Faharani's *ZigBee Wireless Networks and Transceivers* [2].

A.2 Architecture

IEEE 802.15.4 is based on an interpretation of the Open Systems Interconnection seven-layer model, but only defines the two lowest layers: the Physical (PHY) and Medium Access Control (MAC) layers. Each layer provides interfaces and services to the layer above it. Each layer includes two conceptual structures: a data entity and a service entity. The data entity enables data transmission and management, and the service entity provides the interface to the upper layer through a Service Access Point (SAP). Figure A.1 depicts the interfaces between the IEEE 802.15.4 layers (as well as the ZigBee layers discussed in Appendix B).

A.3 Devices

Two device types are specified by IEEE 802.15.4: Full-function devices (FFDs) and Reduced-function devices (RFDs). A FFD may be designated one of three roles: Personal Area Network (PAN) coordinator, coordinator or device. A RFD may only act as a device. FFDs may communicate with other FFDs or to RFDs. A RFD may only communicate with a FFD. RFDs are typically assigned simple roles with minimal message activity and where awareness of network devices other than its FFD parent is unnecessary. This allows for RFDs to be designed with limited resources with respect to those needed for FFDs, resulting in savings in both cost and power consumption. Sensor nodes are typically RFDs.

Each IEEE 802.15.4 network must consist of at least one FFD in order to establish the network. This is a PAN coordinator. Further FFDs added to the network will act as regular coordinators, supplying synchronisation services to other nodes in the network via beacon messages (discussed further in Section A.7.1).

A.4 Network Topology

IEEE 802.15.4 specifies two network topologies: star and peer-to-peer. A star topology, as shown in Figure A.2, is used when all communication within the network occurs between various devices and a single controlling device (the PAN coordinator). The role of the PAN coordinator is to manage the creation of the network and to route messages within the network to their specified destinations. Each device within the network is addressed by a unique 64-bit address, which may be exchanged by the PAN coordinator for a short address for use within the network.

A peer-to-peer network topology differs in that every device in the network may communicate directly to every other device that is in radio range. There is no need to have messages routed via the PAN coordinator, as shown in Figure A.3. This topology allows for range extension by using multiple "hops", where messages between devices out of range of each other may be routed through additional devices.

A.5 Frame Structure

The IEEE 802.15.4 defines four frame structures:

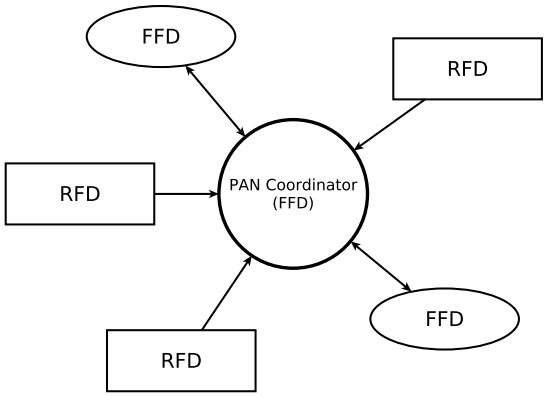


Figure A.2: IEEE 802.15.4 star network topology.

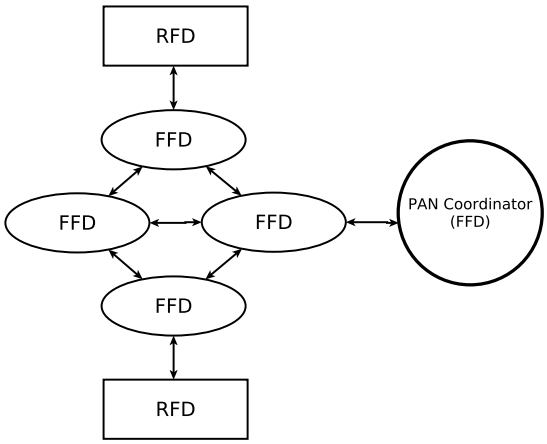


Figure A.3: IEEE 802.15.4 peer-to-peer network topology.

- Beacon frame: used by coordinators to transmit beacon messages.
- Data frame: used to transmit data from one device to another.
- Acknowledgement frame: used to confirm successful message reception.
- MAC command frame: used for transmitting MAC commands to control peer entities.

Each layer contributes its own collection of octets (8 bits) to the frame structure in the form of a Protocol Data Unit (PDU). The MAC layer will contribute a MAC

PDU (MPDU) to the PHY layer, and the PHY layer will use the MPDU as part of its own PHY PDU (PPDU).

A.6 The Physical Layer

The Physical (PHY) layer manages the device's interface with the physical medium used for communication. IEEE 802.15.4 defines the role of the PHY layer as being:

- Enabling and disabling the RF transceiver
- Detecting channel energy levels
- Indicating link quality
- Performing Clear Channel Assessment for the Carrier Sense Multiple Access with Collision Avoidance mechanism
- Selecting channel frequencies
- Transmission and reception of data

Management of the PHY layer is performed with the Physical Layer Management Entity (PLME). The PHY layer supports two services: the PHY data service and the PHY management service. Each of these services is accessible via a dedicated Service Access Point (SAP).

A.6.1 Radio Frequencies and Modulation Schemes

Table A.1 lists the characteristics of the radio frequency options available within the IEEE 802.15.4 standard. The general labels for the different frequency bands are "868 MHz", "915 MHz" and "2.4 GHz".

The modulation technique implemented by IEEE 802.15.4-2003 is Direct-Sequence Spread Spectrum (DSSS). In this method 8 bit *octets* are split into 4 bit *symbols*. A look-up table is used to pair these symbols with a unique 32 bit pseudo-random sequence. The effect of this mapping procedure is that the over-the-air bit rate is multiplied by a factor of 8. The bandwidth also increases eightfold, as the signal

Table A.1: IEEE 802.15.4-2003 Radio Frequency Characteristics.

Frequency (MHZ)	**Modulation**	**Bit rate (kb/s)**	**Symbol rate (ksymbols/s)**	**Available channels**	**Channel separation**
868-868.6	BPSK	20	20	1	-
902-928	BPSK	40	40	10	2
2400-2483.5	O-QPSK	250	62.5	16	5

bandwidth is proportional to the data rate. The required receiver bandwidth is 2 MHz for IEEE 802.15.4 devices.

Phase Shift Keying (PSK) is the specified form of modulation required by IEEE 802.15.4. PSK uses the signal phase to communicate binary information over the air. The two lower frequency bands, 868-868.6 MHz and 902-928 MHz, make use of Binary Phase Shift Keying (BPSK), while the devices operating in the 2.4 GHz band use Offset-Quadrature Phase Shift Keying (O-QPSK).

The higher data rate and its location within the Industrial, Scientific and Medical (ISM) band makes the most popular choice of frequency band for IEEE 802.15.4 transceivers being the 2.4 GHz option. WiFi-capable devices (IEEE 802.11b/g), Bluetooth devices, microwave ovens and cordless phones also make use of the 2.4 GHz ISM band. Interference from these devices and the resulting variation in IEEE 802.15.4 network performance has been recorded. Packet loss is based on channel separation and network activity [3].

A.6.2 Energy Detection and Link Quality Indication

The PHY layer also manages the energy detection (ED) for channel selection purposes. A simple estimation of the received signal power is linearly mapped (from dB values) to an 8-bit number from 0x00 to 0xFF. A value of 0x00 is specified as being a measured power of less than 10 dB above the transceiver's sensitivity. The range of measured power for all 255 possible ED values must be at least 40 dB.

Link Quality Indication (LQI) is an indication of the quality of a received packet and/or the signal strength of said packet. The LQI value is calculated for all received packets using receiver energy detection, an estimation of the receiver signal-to-noise ratio or a combination of the two. LQI values are linearly mapped to an 8-bit

number ranging from 0x00 (poor quality) to 0xFF (high quality). The standard only specifies that a minimum of 8 unique values be available within the range, leaving the specific interpretation (such as a higher LQI resolution) up to the hardware/firmware developer.

A.6.3 CCA for CSMA-CA

The MAC layer can request the PHY layer to perform a Clear Channel Assessment (CCA) routine to determine if the current channel is not occupied by another device. This forms part of the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) mechanism. If the channel is occupied ("busy") data transmission may not occur. Three modes of CCA are available in determining the state of the channel:

- Mode 1: *Energy detection* is performed to see if activity in the channel is above a manufacturer specified level. The channel is reported as busy if the measured energy is above this threshold.
- Mode 2: A *carrier sense* is performed to see if activity with the same modulation and spreading characteristics as IEEE 802.15.4 is detected in the channel. The magnitude of the activity is irrelevant.
- Mode 3: A combination of the above - the channel is reported as busy if IEEE 802.15.4 activity is detected at an energy level above the threshold.

A.7 The Medium Access Control Layer

The Medium Access Control layer manages the device's interface with the radio channel. IEEE 802.15.4 defines the role of the MAC layer as being:

- Network beacon generation
- Network synchronisation using beacons
- Enabling PAN association and disassociation
- Enabling device security
- Managing the CSMA-CA mechanism

- Maintaining the Guaranteed Time Slot (GTS) mechanism
- Providing a reliable link between two peer MAC entities

The MAC layer supports two service entities: the MAC Layer Data Entity (MLDE) and the MAC Layer Management Entity (MLME). Each of these entities have their own respective Service Access Points (SAPs): the MLDE-SAP and the MLME-SAP (see Figure A.1).

A.7.1 Beacon-enabled and nonbeacon-enabled networks

There exists two modes of network operation, decided upon by the method with which multiple devices who wish to transmit messages are given priority. In a *contention-based* channel access environment, all devices will check for channel activity and the first to find a clear channel will be allowed to transmit. In a *contention-free* channel access environment each device is given a specific time slot by the PAN coordinator in which its radio communication may take place. This is called the Guaranteed Time Slot (GTS). In order for this latter method to work all devices must be synchronised (each with their own GTS) with the PAN coordinator. To accomplish this the PAN coordinator transmits beacon signals. A network which makes use of beacon signals for synchronisation is called a *beacon-enabled* network, and a network without beacon signals is labelled a *nonbeacon-enabled* network. The advantage of a beacon-enabled network is that there is a greater chance that the current channel is clear for transmission at defined times for individual devices. The disadvantage is that devices need to check their synchronisation status at regular intervals, which obviously increases power consumption over time. This is opposed to a nonbeacon-enabled network where devices will manage their own message transmission and reception, which may occur at possibly much greater intervals.

In beacon-enabled networks there is an option to make use of a superframe structure bounded by beacon frames. Within the superframe structure exists periods of time designated for specific actions: the Contention-Access Period (CAP), the Contention-Free Period (CFP) and an optional inactive period. The CAP and CFP make up the active period. Figure A.4 depicts a superframe structure. During the CAP any device wishing to transmit data must use the CSMA-CA mechanism (see Section A.7.2). The CFP allocates specific time periods for specific devices increasing the chance of a clear radio channel. A period of inactivity may then

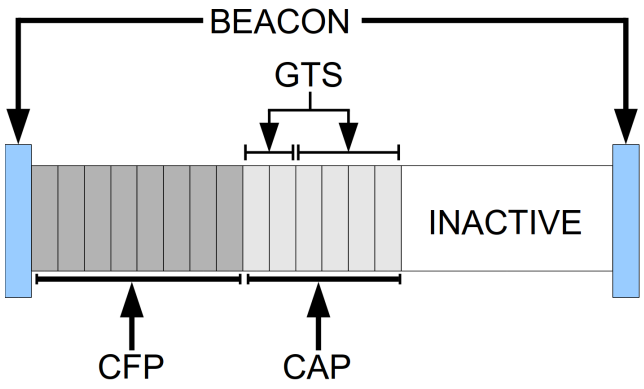


Figure A.4: Superframe structure and contents.

follow the CFP so that the device can enter a sleep mode for power conservation. This dissertation will focus on nonbeacon-enabled networks as this the only type supported by the chosen ZigBee stack firmware used in the author's research.

A.7.2 Carrier Sense Multiple Access with Collision Avoidance

Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) is a mechanism by which multiple devices on the same network may share the same radio frequency channel. Slotted CSMA-CA is used in beacon-enabled networks where the CSMA-CA algorithm must align itself with specific time slots related to the superframe structure. The remainder of the discussion on CSMA-CA will focus on nonbeacon-enabled networks, which employ unslotted CSMA-CA, as this the only type supported by the chosen ZigBee stack firmware used in the author's research. A flowchart depicting the unslotted CSMA-CA algorithm is given in Figure A.5, where *BE* is the back-off exponent and *NB* is the number of backoffs. A "backoff" is a random time delay duration in a range specified by the BE number. A backoff is employed activated when the CSMA-CA algorithm encounters a busy channel. *macMinBE*, *macMaxBE* and *macMaxCSMABackoffs* are MAC constants defined within the stack.

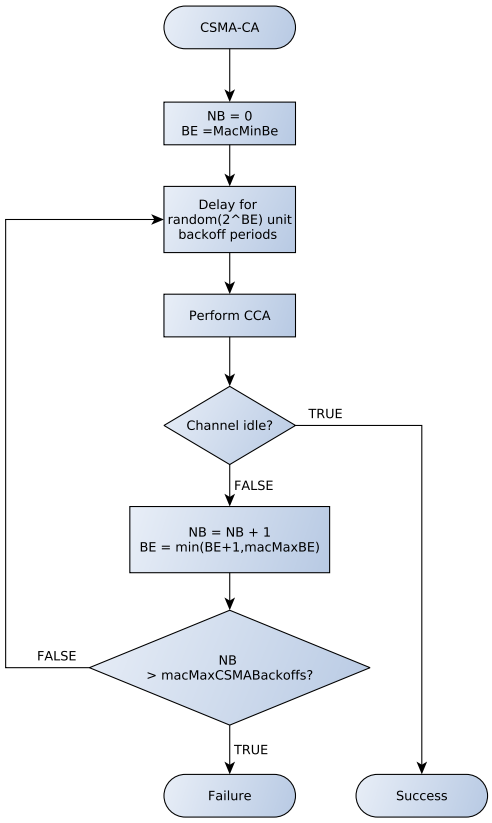


Figure A.5: Unslotted CSMA-CA algorithm.

A.8 Differences between the IEEE 802.15.4-2003 and IEEE 802.15.4-2006 versions

The IEEE 802.15.4-2003 version of the standard specifies three frequency bands for use: 868 MHz, 915 MHz and 2.4 GHz. The first two have data rates of 20 kb/s and 40 kb/s respectively using BPSK modulation (See Table A.1). The use of the 2.4 GHz band allows for a much higher data rate of 250 kb/s, and as a result is the most popular frequency employed by IEEE 802.15.4 transceivers. The BPSK modulation scheme also requires a different transceiver architecture than that of one using O-QPSK at 2.4 GHz. This means that a device wishing to support all or a combination of the three frequency options will have to include multiple radio transceivers [4].

In 2006 the IEEE 802.15 working group revised the 2003 version of the IEEE 802.15.4 standard in order to open up more frequency options for manufacturers, as well as

add some more MAC and PHY layer features. A major addition was the inclusion of using O-QPSK modulation on all three frequency bands. A potential "universal radio" may be able to accommodate two, or all three, frequency options within the same package. An advantage to manufacturers who decide to work within bands other than 2.4 GHz is that there will be no interference from technologies such as Bluetooth or WiFi (see Section A.6.1) [4].

Other additions and changes to the 2003 standard include [5]:

- Addition of data time stamping mechanism
- Addition of method for reporting the revision level frame by frame
- Supports beacon scheduling
- Broadcast messages can be synchronised in beacon-enabled networks
- Improved security features
- GTS support optional
- Removal of restrictions with respect to manually enabling the receiver
- Simplified passive and active scan procedures
- More flexible CSMA-CA algorithm
- Decreased device association time in nonbeacon networks

IEEE 802.15.4-2006 devices are backwards compatible with IEEE 802.15.4-2003 devices.

A.9 Conclusion

The IEEE 802.15.4 protocol specifies two conceptual structures, the Physical (PHY) and Medium Access Control (MAC) layers. The PHY layer details the interface between the electronic device and the physical medium, and the MAC layer details the mechanisms which help to establish a connection between peer devices.

Two device types exist, a Full-function device (FFD) and a Reduced-function device (RFD). An IEEE 802.15.4 network is established by FFDs, who are able to relay

messages to other devices. Sensor devices are typically RFDs and are designed to consume less power than FFDs, but with limited networking capabilities. Devices may connect to one another in one of two specified topologies, star or peer-to-peer.

The PHY layer specifies the frequency band in which the device will operate, as well as quantifying the energy in the chosen channel and determining the link quality between two devices. The Clear Channel Assessment (CCA) mechanism is used by the PHY layer in establishing the state (busy/idle) of a channel, and precedes all transmission attempts.

The MAC layer allows for network synchronisation via the superframe structure, and implements the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) algorithm in an effort to avoid message transmission failure.

References

[1] *IEEE 802.15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, IEEE Computer Society, October 2003, revision designated IEEE 802.15.4-2003.

[2] S. Farahani, *ZigBee Wireless Networks and Transceivers*. Newton, MA, USA: Newnes, 2008.

[3] A. Sikora, "Compatibility of IEEE802.15.4 (ZigBee) with IEEE802.11 (WLAN), Bluetooth, and Microwave Ovens in 2.4 GHz ISM-Band," Steinbeis Transfer Centre for Embedded Design and Networking, University of Cooperative Education Loerrach, Tech. Rep., September 2004. [Online]. Available: http://www.ba-loerrach.de/stzedn

[4] C. Wang, "The Differences Between 802.15.4-2003, 2006, a, c, d," Freaklabs, March 2008, last accessed 02/08/2010. [Online]. Available: http://freaklabs.org/index.php/Blog/Zigbee/802.15.4-2003-2006-c-d-explained.html

[5] *IEEE 802.15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, IEEE Computer Society, September 2006, revision designated IEEE 802.15.4-2006.

Appendix B

ZigBee

B.1 Introduction

ZigBee is a wireless standard developed by the ZigBee Alliance. The ZigBee alliance is a collection of global companies with interests in residential, commercial and industrial applications of Wireless Sensor Networks (WSNs). Member companies have the benefits of early insight into new developments within the standard, as well as active involvement in the development of ZigBee itself. Equipment manufacturers which feature ZigBee modules within their products must be ZigBee Alliance members, but distributors and resellers need not be members.

This document summarises some of the structures and functions of the "ZigBee 2006" version of the standard, as this is the version to which the firmware stack chosen for the hardware implementation adheres to. While ZigBee supports encryption and secure frame transmission, it is not mandatory. The firmware stack used in the implementation does not subscribe to these security features owing to microcontroller memory constraints. ZigBee security features are therefore omitted from the succeeding sections.

Section B.2 outlines the ZigBee stack architecture. The different ZigBee device types are detailed in Section B.3, and the ZigBee frame structure is discussed in Section B.4. The Network and Application layers specified by the ZigBee stack are presented in Section B.5 and Section B.6 respectively.

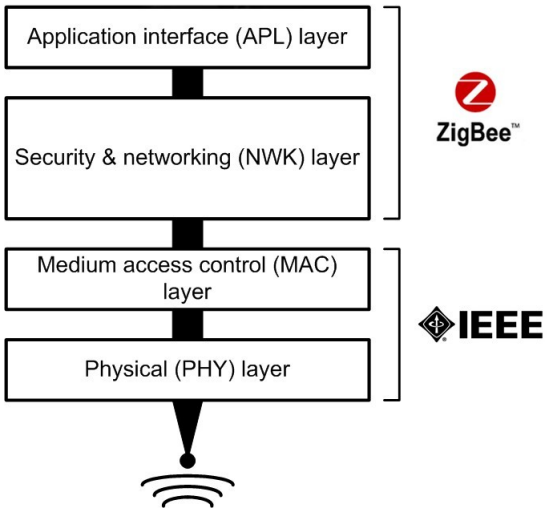


Figure B.1: The IEEE 802.15.4/ZigBee interpretation of the OSI model.

CITATION DISCLAIMER

Unless otherwise specified, the information detailed in this appendix is a summary of that found in the ZigBee-2006 standard [1] and Faharani's *ZigBee Wireless Networks and Transceivers* [2].

B.2 ZigBee Stack Architecture

The ZigBee stack is based on the Open Systems Interconnection seven-layer model, but only defines specific layers related to providing the intended functionality. The IEEE 802.15.4 standard specifies the lower Physical (PHY) and Medium Access Control (MAC) layers on which ZigBee builds upon by adding an additional Network (NWK) and Application (APL) layer, as shown in Figure B.1.

Each layer within the overall IEEE 802.15.4/ZigBee stack provides interfaces and services to the layer above it. Each layer includes two conceptual structures: a data entity and a service entity. The data entity enables data transmission and management, and the service entity provides the interface to the upper layer through a Service Access Point (SAP). Stack operation is based on service primitives supported by the SAPs. See Figure A.1 for an overview of the layers and interfaces involved in the IEEE 802.15.4/ZigBee stack architecture.

Table B.1: ZigBee Device Types.

ZB Device Type	IEEE device type	Comments
Coordinator	FFD	One per network. Responsible for establishing the network and supporting device association. Powered and active at all times.
Router	FFD	Many per network. Supports device association. Extends network range by relaying information to and from other routers or the coordinator. Powered and active at all times.
End device	RFD	Many per network. Cannot forward messages, must connect to a FFD. Can be placed in "sleep" mode. Typically acts as a sensor device on a network.

B.3 ZigBee Devices

Table B.1 describes the three general device types specified for use in a ZigBee network. The ZigBee devices are based on the devices specified by IEEE 802.15.4 (see Appendix A).

B.4 ZigBee Frame Structure

Data transmission between layers is accomplished with Protocol Data Units (PDUs). Each of the layers in the ZigBee stack contribute a PDU to the layer below it. The Application (APL) layer will generate a structure of octets in the form on an APL PDU (APDU). This is passed on to the Network (NWK) layer where additional network-relevant data octets are added to the APDU to form the NWK PDU (NPDU). The NPDU is passed to the MAC layer to form part of the MPDU, and the MPDU forms part of the PPDU, as discussed in Appendix A.

B.5 The Network Layer

The Network (NWK) layer sits on top of the IEEE 802.15.4 MAC layer and below the ZigBee APL layer. The responsibilities of the NWK layer are as follows:

- Managing the joining and leaving of networks

- Application of security to frames
- Frame routing, route discovery and route maintenance
- Neighbour discovery
- Storage of neighbour information

The NWK layer supplies the ZigBee stack with two service entities: the NWK Layer Data Entity (NLDE) and the NWK Layer Management Entity (NLME). Each of these entities have their own respective Service Access Points (SAPs): the NLDE-SAP and the NLME-SAP (see Figure A.1).

B.5.1 General NWK Layer Mechanisms

Short Addresses

ZigBee coordinators use the NWK layer to assign a 16-bit *short* address to devices joining the network. This is separate to the 64-bit MAC address (or *long* address) which is usually stored in the device firmware or external memory.

Message hopping and radius

A message frame transported from the source device to the destination device, without any forwarding from other devices, travels in a single *hop*. If forwarding by one or more devices (ZigBee routers) occurs, the message is transported within a *multi-hop* environment. The NWK layer sets a limit on the number of hops experienced by a message en route to its destination. This is the frame *radius*. The NWK layer incorporates the maximum radius number in the original message frame. The NWK layer on subsequent devices will decrease this number after every hop. The frame is no longer relayed when a device, which is not the intended destination, reads the number to be zero.

Message acknowledgement

A device transmitting a message can request that it be informed of message delivery by adding an acknowledgement request to the message frame. When the destination

device has processed the message it will generate an acknowledgement message and transmit it back to the original source address.

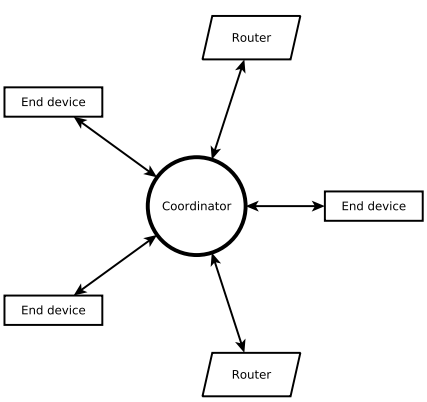
Message Communication

The NWK layer specifies three types of communication mechanisms: *broadcast*, *multicast* and *unicast*.

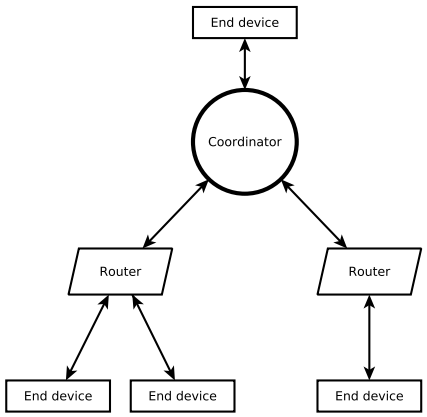
Any device in a ZigBee network may issue a message to all devices in the network with a broadcast message. A destination short address of 0xFFFF is used when generating a broadcast message. All devices will check any received frames in order to know their part in the message processing procedure. The ZigBee coordinator and ZigBee routers will both register the broadcast message for themselves and relay it to any neighbouring devices. Any end device reading a frame destination address of 0xFFFF will register the message for itself. Devices may not actively acknowledge a broadcast message because this would generate massive amounts of traffic in large networks. Instead, the coordinator and any routers which have relayed a broadcast message will wait until it receives the same frame rebroadcast by any neighbour devices. Receiving a rebroadcast is acknowledgement that it has relayed the broadcast message correctly. This is called passive acknowledgement.

A multicast message is directed towards a group of devices within the same network. Groups are identified by a 16-bit group ID value. This information is encoded into the message frame by the source device. Devices keep a list of the groups that they are part of in a table in memory. Two options for multicasting exist: member mode and non-member mode. Member mode messages are generated by a member device and transmitted to the remaining members of the group. Non-member mode messages can be generated or relayed by a device which is not a member of the intended group to any intended group member. This group member will then multicast the message to the remaining members of the group.

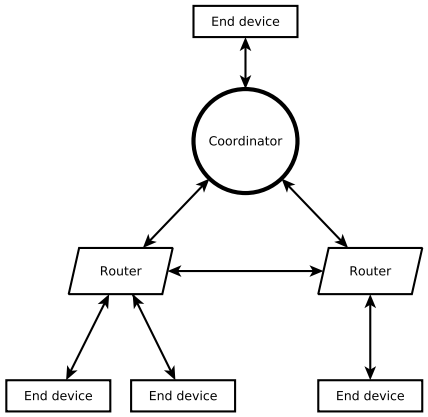
Unicast messages are intended for a single destination device, specified by a unique short address.



(a) ZigBee star network topology.



(b) ZigBee cluster tree network topology.



(c) ZigBee mesh network topology.

Figure B.2: ZigBee network topologies.

B.5.2 ZigBee Network Topologies

The IEEE 802.15.4 standard defines two network topologies: star and peer-to-peer (see Appendix A). ZigBee expands these definitions and provides an additional networking topology known as a mesh topology. ZigBee supports three distinct topologies: star, cluster tree and mesh. See Figure B.2 for a visual description of such topologies.

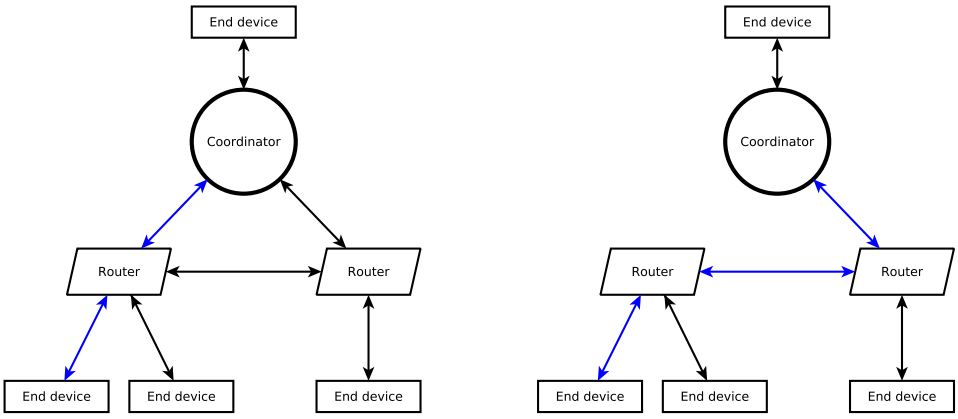
In a star network topology all devices are connected to a single *sink* device. The sink device in a ZigBee network is the coordinator. In a cluster tree topology ZigBee coordinators and routers can act as *parent* devices, allowing other *child* devices to associate with the network. Messages for a child device can only be routed via its parent. A device's network *depth* is the minimum number of hops required for the device to receive a message from the coordinator using only parent-child hops. End devices and routers connected directly to the coordinator have a network depth of one.

No such hierarchical relationships exist in a mesh network. All devices are able to communicate with any other device in the network, where routing may be performed by any ZigBee router in radio range, regardless of parent-child relationships. Two important aspects of a mesh network are its self-forming and self-healing characteristics. A network which is self-forming does not need user intervention when associating new devices within the network and establishing message routing. Self-healing occurs when previously available message paths become unavailable and the network adjusts the routing mechanism to compensate such that a message delivery featuring a different path is attempted. Message paths will become unavailable if devices are no longer in radio range, or if the device suffers loss of power supply or hardware or firmware failure. These features offer a particular advantage when placed in the context of a railway wagon based wireless sensor network. Individual wagons (and the attached wireless network devices) may be added, removed or swapped out at railway depots, requiring autonomous reconfiguration of the network. Figure B.3 depicts how the network will adjust with the loss of a message path.

B.5.3 ZigBee Routing

The selection of a path through which a message is relayed from a source device to a destination device is known as routing. Only ZigBee coordinators and routers can manage route requests and route discovery. End devices rely on routing-capable devices which are in radio range to manage route discovery on their behalf.

The presence of direct radio communication from one device to another is a *link*. A message may traverse many links before arriving at its destination. Various parameters may be considered in deciding the optimal path for routing a message. Such considerations include link quality, number of hops and power supply considerations. Comparison of various possible routes is done by choosing the route with the lowest *path cost*. The path cost is the summation of all link costs for a specific path, where



(a) Original message path.

(b) Alternate message path.

Figure B.3: Message routing before and after path loss.

a link is defined as $[D_i, D_{i+1}]$. The expression for evaluating a path P of length L is given in Equation B.1.

$$C\{P\} = \sum_{i=1}^{L-1} C\{\,[D_i, D_{i+1}]\,\} \tag{B.1}$$

where $C\{[D_i, D_{i+1}]\}$ is a link cost. The link cost $C\{l\}$ for a link l is defined in Equation B.2.

$$C\{l\} = \begin{cases} 7, \\ \min\left(7, \text{round}\left(\frac{1}{p_l^4}\right)\right) \end{cases} \tag{B.2}$$

where p_l is the probability of successful packet delivery on link l.

ZigBee coordinators and routers must maintain a *routing table* which is used to find the next hop a message must make on its way to the destination device. Devices maintaining a routing table must also maintain a *routing discovery table*. The routing discovery table consists of path costs and device addresses related to route requests.

All devices in a ZigBee network maintain a *neighbour table* which consists of information on all devices within radio range. Examples of the stored information are: device short and long (64-bit) addresses, device type and estimated Link Quality

Indicator (LQI). This information is used during network discovery or when the device is attempting to rejoin a network and is looking for candidate parents in radio range.

B.6 The Application Layer

The Application (APL) layer consists of the Application Support (APS) sublayer, the ZigBee Device Objects (ZDO) and the application framework.

B.6.1 The Application Framework

The application framework uses application objects to manage the lower protocol layers in the ZigBee stack. Application objects are developed by manufacturers and engineers and allow for device customisation. Individual application objects are assigned a unique *endpoint* address, from endpoint 1 to endpoint 240. Endpoint address 0 is used for the ZDO, and endpoint address 255 is used as a broadcast address by which a message may be sent to all application endpoints.

To further provide an application identity for a set of ZigBee devices, the ZigBee standard offers the option of using an *application profile*. An application profile is a structured set of data descriptors and objects which may be applied to a specific application. Individual devices subscribing to the same application profile are fully interoperable with each other. The ZigBee Alliance offers the following official application profiles:

- Smart Energy
- Health Care
- Radio Frequency for Consumer Electronics (RF4CE)
- Home Automation
- Telecom Services
- Building Automation (work in progress)
- Retail Services (work in progress)

Application profiles may be public or private. Public profiles are developed by ZigBee Alliance members and ensure interoperability between all subscribing devices, regardless of manufacturer. Private profiles are custom, proprietary profiles developed by manufacturers for applications where interoperability is not required.

Application profiles are distinguished from each other with a 16-bit identifier value. If a vendor wishes to use a private profile it must request a profile identifier from the ZigBee Alliance.

An application profile contains *clusters* and *device descriptions*. A cluster is a set of *attributes*, and is identified within its profile with a unique 16-bit number. Attributes are used to store data values relative to its parent cluster. For example, in an application involving ventilation control, the profile may include a fan cluster, which in turn contains attributes such as fan speed and direction. Clusters may be designated as input or output clusters.

A device description provides information on the capabilities and constraints of the device itself. Information on the device's power supply, frequency band and device type are examples of information which is accessed through the relevant device descriptor in the application profile.

B.6.2 The Application Support Sublayer

The Application Support (APS) sublayer acts as an interface between the NWK layer and the APL layer. Data and management services supported by the APS sublayer are the APS Data Entity (APSDE) and the APS Management Entity (APSME), and are accessible through their individual Service Access Points (SAPs): the APSDE-SAP and the APSME-SAP (see Figure A.1).

Responsibilities of the APS sublayer include:

- Binding table management
- Message forwarding, between bound devices
- Group address management
- Mapping of the 64-bit long address to the 16-bit short address
- Enable reliable data transportation by resending failed messages

Device binding is a process where a logical link is made between two related applications. For example, in the ventilation control application discussed in Section B.6.1, fan switches may be found on one ZigBee device, and fan motors on another. If both devices share the same clusters, but one is an input cluster (fan switch) and one an output cluster (fan motor), then the devices may be bound.

B.6.3 ZigBee Device Objects

The ZigBee Device Objects (ZDO) acts as an interface between the APS sublayer and the application framework. The ZigBee Device Profile (ZDP) is a profile which defines data structures and objects for use by the application and its interface to the other layers. Where an application profile supports a specific application, the ZDP is common to all ZigBee devices. The ZDP contains clusters and a device description (as do application profiles), but does not define any attributes. Two groups of clusters exist: mandatory and optional. The mandatory clusters exist on all ZigBee devices.

The ZDO enables the *device discovery* and *service discovery* mechanisms. Device discovery identifies other devices within the same Personal Area Network (PAN). Service discovery provides detailed information on the capabilities of devices in the network, and can be used to match and bind devices in the network.

The ZDO also defines networking related actions such as enabling a list of channels within the frequency band which may be used, managing network scan procedures, selecting a channel on which to start a PAN and network orphaning/rejoining procedures. Such actions are actually implemented in lower layers within the stack, but the ZDO acts as a supervisor in specifying which action should occur at what instance. The ZDO plays a similar role in binding management and device management.

B.7 Conclusion

The ZigBee stack specifies two layers, the Network (NWK) and Application (APL) layers, which operate above the IEEE 802.15.4 Medium Access Control (MAC) and Physical (PHY) layers.

The NWK layer is responsible for message routing and route discovery, as well the

storage of information on any neighbouring devices. An advantage in using the ZigBee stack as opposed to just the IEEE 802.15.4 protocol is the addition of mesh networking, which allows for dynamic route adjustment as message paths become unavailable for use.

The APL layer provides a framework for specifying the operation of a device with an application profile, as well as accommodating interoperability between any ZigBee devices with the same application profile. Engineers and developers interface with this layer to provide the intended functionality of a ZigBee device.

References

[1] *ZigBee Specification*, ZigBee Standards Organization, Document ID: 053474r13, December 2006.

[2] S. Farahani, *ZigBee Wireless Networks and Transceivers*. Newton, MA, USA: Newnes, 2008.

Appendix C

Literature Survey

C.1 Introduction

With the advent of cheap radio transceiver electronics and strong focus on low power consumption and device interoperability, ZigBee has established itself as a strong contender to be the low-bandwidth wireless protocol of choice [1]. Over 350 manufacturers have adopted ZigBee technology, with combined revenues from these companies exceeding $1 trillion (USD). Despite the current global financial slowdown, ZigBee device sales have increased an average of 62% per year since 2007. Of all the IEEE 802.15.4 devices shipped in 2009, 75% were designed specifically to work in ZigBee applications [2]. It has been reported that the wireless sensor network market is to reach $40 million (USD) in 2010 [3], and that the market will exceed $1 billion (USD) by 2014 [4]. These figures and the great interest in ZigBee warrant a deeper look into past and current research into the technology, which while young, is expected to grow immensely in the next few years.

This appendix investigates academic IEEE 802.15.4/ZigBee research. Journal and conference papers, as well as postgraduate dissertations have been reviewed in Section C.2. Analysis of the hardware platforms used in the reviewed research is given in Section C.3. Concluding remarks are found in Section C.4.

C.2 Literature Review

Cinque et al [5] compare the traditional wired approach to Structural Health Monitoring (SHM) against the use of wireless sensor networks, of which the latter is

proposed to be the better solution. Eliminating cables lowers the costs and time involved in device installation, fault diagnosis and fault recovery. It is noted that the primary vulnerabilities of a WSN are the characteristics of the wireless medium and the operating lifetime of the power source. Three key components for reliability are determined: reliable synchronisation of the measurements, reliable delivery of a significant amount of the measurements and minimisation of human intervention on the network.

Lynch and Loh [6] review both academic and commercial wireless sensor platforms used for SHM. A total of 24 systems are described, 17 academic platforms and 7 commercial platforms. Of all the systems reviewed only two conform to the IEEE 802.15.4 standard. One uses a Texas Instruments MSP430 microcontroller paired with a Chipcon CC2420 (2.4 GHz) transceiver, the other uses an Intel Pentium 133 MHz personal computer with a Motorola neuRFon transceiver. The authors identify the most significant limitation of WSNs being the use of finite energy power sources. Suggestions for extending WSN lifetime include low power design and component selection, duty cycle management and the employment of energy scavenging techniques.

Lu et al [7] describe a WSN used for condition monitoring of electric machines. The experimental implementation makes use of the IEEE 802.15.4 standard with a Chipcon CC2420 RF transceiver (2.4 GHz band). Sensor nodes relay information to a central supervising station which processes the measured data. The authors conclude that non-intrusive health monitoring and cable elimination allow for a low cost sensor rich environment.

A review of sensor networks used in the tracking, tracing and monitoring of refrigerated containers is presented by Ruiz-Garca et al [8]. It is noted that the transmission of data will shift from wired to wireless means in the near future. A comparison of ZigBee (802.15.4), WiFi (802.11b) and Bluetooth (802.15.1) technologies is included. The authors state that the low power consumption of a ZigBee network is the definitive reason for its suitability in WSN applications.

IBM Corporation has developed a container management product titled Secure Trade Lane [9]. The system uses multiple ZigBee-based sensing modules placed in a container for environmental data collection. These nodes may also contain actuators (i.e. for temperature adjustment). The sensing nodes communicate with an information relay node found in the container which has satellite, GSM/GPRS and ZigBee capabilities which allow it to communicate with the outside world using

internet portals and hand-held devices operated by technicians. An external GPS transceiver found on the transport vessel communicates with the relay node, providing continuous real-time location monitoring. The choice of wireless technology was made after comparison with WiFi and Bluetooth showed ZigBee offers major advantages in network depth and power consumption.

The question of an IEEE 802.15.4 system reliably operating from within a metal cargo container is investigated by Fuhr and Lau [10]. Sensor nodes are placed at different locations within the container and one routing node on the external locking bar. Another node taking the reliability measurements receives signals from 20 m outside the container. Performance of the network is evaluated by the packet transmission rate. The results show that mesh networks provide a reasonable level of packet transmission. The packet transmission rate is improved by either increasing the number of nodes per container, or increasing the transmission power of individual nodes. The former solution is more expensive in terms of increased hardware costs, while the latter decreases the power source lifetime - requiring increased recharge/replacement intervals. Optimisation of the situation is realised through strategic node placement within the container.

A system for condition and fault monitoring of commuter trains is presented by Kootkar and Al-Ars [11]. The system detects door malfunctions, monitors vibrations and brake temperatures and determines passenger numbers (via a sensor under passenger seats). The sensor nodes use the Crossbow Mica2 platform which features an Atmel ATmega128L microcontroller paired with a Chipcon CC1000 RF transceiver. “Reliability Block Diagrams” are used to assess the quality of the sensor network. An implementation focussing on reliability monitoring, alarm triggering and active quality improvement techniques is proposed.

Researchers at the Centre for Railway Engineering at Central Queensland University have developed a network of health card devices for monitoring and analysis of wheel-track interactions [12]. Two variations of the health card system exist: a wired approach, using IEEE 1473; and a wireless network. The WSN uses Analog Devices' dual-axis accelerometers connected to a Rabbit 3000 microcontroller operating at 40 MHz. The microcontroller consumes half of the 400 mW total power consumption of the health card. Power is supplied via a 10 Wp (Watts peak) solar panel connected together with a 80 Wh lithium ion battery. In this configuration, power can be supplied to the health card for at least 8 days without sunlight. Wireless communications is achieved with Bluetooth transceivers operating in a daisy-chain network.

Lönn and Olsson [13] details the design and development of a ZigBee device. An Atmel ATmega128L microcontroller is paired with a Chipcon CC2420 transceiver. A balun circuit is used for impedance matching and differential/single-ended signal conversion between the transceiver and an antenna. The author details the printed circuit board (PCB) layout, design and assembly process as well as the use of development kits and microcontroller programming tools. A test application consisting of a temperature sensing node which communicates to a data collection node is successfully implemented.

Wettergren [14] investigates the suitability of ZigBee for industry, with focus on operation in different working environments. MaxStream's XBee modules are used. The ZigBee stack consumes all of the XBee module's memory and so an Atmel ATmega162 microcontroller is paired with the module to provide a platform from which applications can be stored and executed. Details regarding the microcontroller software and Application Programming Interface (API) are provided. Reliability tests performed with results showing an average packet error rate (PER) of 0.07 %. Acceptable packet error measurements occur in an industrial plant environment, whilst the highest consecutive number of packets lost occurred when operating in the vicinity of a microwave oven. Round-trip times in all tests were equal, showing round-trip time is independent of the environment. Range tests yield a maximum of 30 m indoors and 500 m outdoors for the XBee modules.

Ramazanali [15] compares and characterises two ZigBee modules. One is the sensor node platform developed by Lönn [13], the other is part of a development kit from a transceiver manufacturer (Chipcon). Both platforms use the ATmega128L microcontroller and the Chipcon CC2420 transceiver. Characterisation of the modules is done via the measurement of various parameters: in and out of band spurious emissions, maximum power, occupied bandwidth power, adjacent channel power and transmission power spectral density. Measurements were taken in various environments: outdoor free line-of-sight (FLOS), indoor FLOS and indoor obstructed line of sight. The thesis concludes that the academic modules compare favourable with the Chipcon ones. Regulatory requirements are not met in the tests concerning spurious emissions. This problem is rectified by lowering the power output of the module. Range tests show a Packet Error Rate of ≤ 0.05 % for indoor and outdoor free-line-of-sight environments. The maximum error rate (1.12 %) occurs in transmission between building floors.

Prajzler [16] investigates ZigBee suitability for battery powered medical devices. A system using an Atmel Atmega88V microcontroller and the MaxStream XBee

(Series 2) transceiver is designed and implemented. The author states that the custom solution works reliably and devices may be used in future wireless sensor networking research, but more work will have to be done to implement the hardware in medical applications.

Pinedo-Frausto and García-Macías [17] provide an analysis of a ZigBee network and message throughput and delay measurements . They use a Freescale MC908HCS08 GT60 microcontroller paired with a Freescale MC13193 transceiver. Throughput measurements show a data rate of 8.3 kb/s for the maximum message size, much lower than the theoretical 250 kb/s offered by IEEE 802.15.4. The authors claim that the ZigBee stack overhead introduces time delays and decreases bandwidth efficiency.

A study of ZigBee and WiFi network co-existence has been undertaken by Shuaib et al. [18] using MaxStream XBee modules. The measurements show that the influence of ZigBee on WiFi is greater on transmissions from WiFi access point to client than in the opposite configuration, with a measured 11% drop in WiFi throughput. The study also shows Bluetooth has greater effect on WiFi performance than does ZigBee.

Burchfield at al. [19] present an analysis of theoretical, simulated and measured ZigBee throughput results, with and without a custom stack modification. The Ember EM2420 Developer Kit, featuring an Atmel Atmega128L microcontroller and a Ember EM2420 transceiver is used in the hardware implementation. Firmware refinements such as removal of excess functions, improving interrupt service latency and increasing available packet buffers result in doubling the ZigBee throughput relative to the original manufacturer's configuration.

A comparison of the power consumption of a ZigBee network on an Atmel RZRAVEN Development Kit and the power consumption of a SimpliciTI network using Texas Instruments' EZ430-RF2500 development kit is made by Skrzypczak et al. [20]. SimpliciTI is a Texas Instruments proprietary wireless protocol. The RZRAVEN solution has a greater operating range, but increased power consumption in sleep mode. The SimpliciTI devices have the advantage of 16-bit microcontrollers and an easy to use API interface for developing applications, but it is noted the RZRAVEN devices have more peripheral features.

Using a ZigBee network to monitor sewage water levels is explored by See et al. [21]. The Crossbow Mica2 platform is used in field trials, where an overall network reliability of 80% is achieved. Proximity of objects around the nodes affected

the performance. A proposed solution to mitigate multipath fading effects is to increase the number of repeater nodes as well as provide multiple antennas in various configurations for each device.

A distance estimation system using message round-trip time in a ZigBee network is explored by Tsai et al. [22]. The Microchip PICDEM Z development kit (old version) is used to implement the network. Message round-trip times are used in estimating distance. The authors claim a ± 1 m error for 90% of test cases. A duration of three seconds is required to transmit 100 messages for the estimation.

The question of using a WSN performance metric in determining distance is investigated by Xiao et al. [23]. Freescale MCF5208 Evaluation Boards are used to determine the message error rates. The author's findings suggest that transmission error approximations are better than signal strength measurements when attempting to measure the distance between two ZigBee devices separated by 60 feet or more.

Ferrari et al. [24] provide an analysis of the indoor performance of a ZigBee network, using a Microchip PIC18LF4620 microcontroller and Texas Instruments CC2420 transceiver (Microchip PICDEM Z development kit). Packet error, delay and throughput measurements are performed. The authors claim that ZigBee exhibits bimodal connectivity characteristics which impact all measurements; there is either connectivity between devices, and messages may be delivered or there is no connection and messages will not be delivered. The study also comments on connectivity "drops" occurring in the presence of obstacles (multipath fading effects).

Performance analysis of a non-beaconing ZigBee network is examined by Armholt et al [25]. The use of the Texas Instruments CC2420DB Platform enables the hardware implementation. The authors suggest that the addition of a waiting period before message transmission can decrease channel access failure without affecting throughput.

Tsai et al. [26] have investigated a ZigBee intra-car sensor network using the Crossbow MICAz platform. Various experiments are undertaken in locations such as vehicle garage, parking lot and on the road. Other parameters which were varied were the presence of a driver, and engine on/off status. The authors state that location of the ZigBee devices within the car affects link quality considerably. Electromagnetic noise exhibited by the engine can decreases message reception sensitivity by 4 dB. Bluetooth interference decreases goodput performance by as much as 40%.

Suarez et al. [27] have examined substituting the standard ZigBee Medium Access Control (MAC) layer (defined by IEEE 802.15.4) with an enhanced MAC layer entitled X-MAC. X-MAC implements radio transceiver power cycling. A transmitting device must first send out "strobe" packets for a long enough duration such that all devices in range will be powered on at some stage in the strobing sequence and receive at least one strobe packet. This indicates to a receiving device that a regular data frame is to follow and that its radio must be on to receive this data frame in full. Implementing the new MAC layer on the T-mote Sky platform, the authors were able to able to reduce device power consumption by 90%, increasing network lifetime tenfold. The advantage of extended network lifetime comes at the cost of increased network latency.

Kohvakka et al. [28] uses a custom hardware platform to analyse the network performance and energy consumption of a ZigBee network, with a view to large-scale device deployments. Their analysis focuses on beacon-enabled networks and the superframe timing structure relative to the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) mechanism. Their findings suggest that the beacon order and superframe order parameters which affect the timing and synchronisation of a beacon-enabled ZigBee network influence power consumption. Minimum power consumption of 73 μW is observed when data messages are 4 minutes apart. Using the shortest contention access period of 15.36 ms power consumption rises to 370 μW.

ZigBee suitability for use in electricity metering is investigated by Liu [29]. A test platform is created using Texas Instruments Z-Stack Development Kit (CC2430ZDK). Message round-trip time, error rates and power consumption measurements are performed with the conclusion being that ZigBee fulfils the basic requirements for a solution for wireless electricity monitoring. The author notes that repeatable results are a challenge to obtain, as performance varies from environment to environment. The inclusion of obstructions (humans, vehicles, etc) within radio range mitigate performance (multipath fading effects).

Watthanawisuth et al. [30] examine GPS location monitoring of farm tractors using a multi-hop ZigBee network. A custom platform including a Microchip PIC24FJ128GA010 microcontroller and a MaxStream XBee-PRO transceiver are used in field trials. Tractor data such as latitude, longitude, speed and engine status is uploaded to an internet website for observation by the farm owner. Range extension was necessary and facilitated with the addition of ZigBee router nodes at fixed positions. The implementation aided the farmer in managing farming operations.

Distance estimation using ZigBee message values is investigated by Benkic at al. [31]. A comparison in the results between two transceivers (Texas Instruments CC2420 and Microchip MRF24J40) is provided. The study shows the transceiver modules provide similar results. Suitability of results with respect to accuracy of distance estimation is application dependant.

C.3 Hardware Platform Survey

C.3.1 Tabulated Literature Survey

Table C.1 shows the hardware configurations used by a subset of the research presented in Section C.2. Only solutions which featured adequate hardware information and a fully compliant ZigBee stack were considered. In studies where an evaluation of two individual wireless platforms is presented, a number precedes the microcontroller and transceiver labels indicating to which platform they belong.

Table C.1: Table of reviewed hardware platforms

Reference	**Hardware Platform**	**Microcontroller**	**Transceiver**
Lönn [13]	Custom	Atmel ATmega128L	Texas Instruments CC2420
Wettergren [14]	Custom addition to MaxStream XBee (Series 1)	Atmel ATMega162 (application), Freescale MC9S08GT60 (ZigBee stack)	Freescale MC13193
Ramazanali [15]	(1) Texas Instruments CC2420ZDK Development Kit (2) Custom, as designed by Lönn [13]	(1) Atmel Atmega128L (2) Atmel Atmega128L	(1) Texas Instruments CC2420 (2) Texas Instruments CC2420
Prajzler [16]	Custom addition to MaxStream XBee (Series 2)	Atmel Atmega88V (application), Ember EM250 (SoC) (ZigBee stack)	Ember EM250 (SoC)
Pinedo-Frausto and García-Macías [17]	Panasonic PAN802154 Platform	Freescale MC908GT60	Freescale MC13193
Shuaib et al. [18]	MaxStream XBee (Series 1)	Freescale MC9S08GT60	Freescale MC13193
Burchfield at al. [19]	Ember EM2420 Developer Kit	Atmel Atmega128L	Ember EM2420
Skrzypczak et al. [20]	(1) Texas Instruments SimpliciTI Development Kit (2) Atmel RZRaven Development Kit	(1) Texas Instruments MSP430 (2) Atmel Atmega1284P	(1) Texas Instruments CC2500 (2) Atmel AT86RF230
See et al. [21]	Crossbow Mica2	Atmel Atmega128L	Texas Instruments CC1000
Tsai et al. [22]	Microchip PICDEM Z development kit (old)	Microchip PIC18LF4620	Texas Instruments CC2420
Xiao et al. [23]	Freescale MCF5208 Evaluation Boards	FreeScale MCF5208	FreeScale MC13192

Continued on next page

Table C.1: Table of reviewed hardware platforms (continued from previous page)

Reference	**Hardware Platform**	**Microcontroller**	**Transceiver**
Ferraro et al. [24]	Microchip PICDEM Z development kit (old)	Microchip PIC18LF4620	Texas Instruments CC2420
Armholt et al [25]	Texas Instruments CC2420DB Platform	Atmel Atmega128L	Texas Instruments CC2420
Tsai et al. [26]	Crossbow MICAz	Atmel Atmega128L	Texas Instruments CC2420
Suarez et al. [27]	Sentilla Moteiv Tmote Sky	Texas Instruments MSP430	Texas Instruments CC2420
Kohvakka et al. [28]	Custom	Microchip PIC18LF8720	Texas Instruments CC2420
Liu [29]	Texas Instruments Z-Stack Development Kit	Texas Instruments CC2430 (SoC)	Texas Instruments CC2430 (SoC)
Watthanawisuth et al. [30]	Custom addition to MaxStream XBee (Series 1)	Microchip PIC24FJ128GA010 (application), Freescale MC9S08GT60 (ZigBee stack)	Freescale MC13193
Benkic at al. [31]	(1)Microchip PICDEM Z development kit (old) (2) Microchip PICDEM Z development kit (new)	(1) Microchip PIC18LF4620 (2) Microchip PIC18LF4620	(1) Texas Instruments CC2420 (2) Microchip MRF24J40

C.3.2 Platform choice results

The survey takes into account two general cases for platform choice: custom platforms and development kits. A custom platform is one where the engineer has paired a microcontroller and radio transceiver of his/her choosing to form a ZigBee capable device or "node". The engineer will design a printed circuit board (PCB) on which to house the electronic components. Typical components of a wireless device include a power supply subsystem, a microcontroller, a transceiver and one or more transducers (see Appendix D)

A development kit platform is one purchased from a manufacturer of microcontrollers or radio transceivers. The kit will contain multiple wireless device PCBs featuring a proprietary pairing of microcontroller and radio transceiver. A development kit allows the engineer to test application firmware and wireless network performance without facing the challenge of component selection or PCB layout. Manufacturers will often provide proprietary software which interfaces with the PCBs for application development specific to wireless sensor networks, often in the form of high level Application Programming Interfaces (APIs). These APIs provide a level of abstraction from the microcontroller firmware and present a user friendly interface with which to configure and control the wireless network.

A mention must be made of the MaxStream XBee modules [32]. These ZigBee modules contain either a separate microcontroller and transceiver - XBee Series 1, or a combined System-on-Chip integrated circuit - XBee Series 2. These modules use a simple serial protocol to dictate network operation, with limited custom application capabilities. They are often used in "cable-replacement" applications. While these modules can be used as stand-alone devices, the use of the simple serial interface attracts engineers who wish to pair a microcontroller of their choice with the module. This allows for custom application firmware to be programmed into the chosen microcontroller, with networking operations controlled by the XBee module. The popularity of using an XBee module to manage the network stack is seen in its use in 3 out of 5 custom platform implementations in Table C.1.

There are 19 studies presented in Table C.1, with a total of 21 wireless networking platforms evaluated, with one unique platform featuring multiple use: the Microchip PICDEM Z development kit [33]. The study by Ramazanali [15] includes a comparison with the platform developed by Lönn [13] and is counted only once in the succeeding analysis. Figure C.1(a) shows that custom platforms comprise less than a quarter of the 21 ZigBee platforms. Texas Instruments and Microchip

development kits are the most popular of the development kit platforms, as shown in Figure C.1(b).

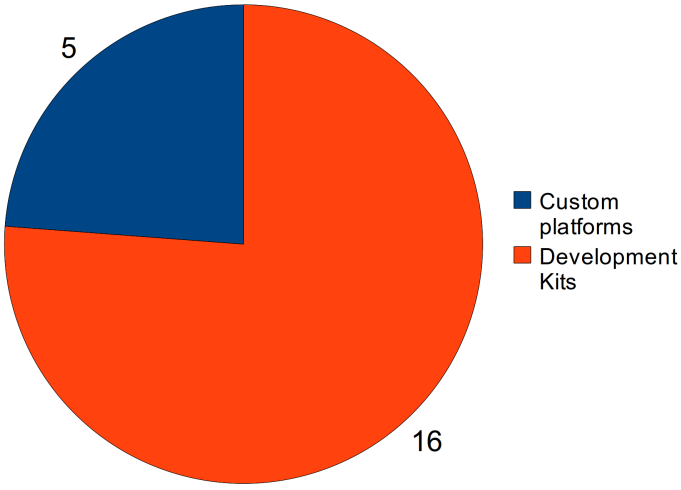
What follows in the next two sections of this document is a breakdown of the microcontroller and transceiver choices made in the studies from Table C.1. Note that a System-on-Chip (SoC) solution is counted as being both a microcontroller and a radio transceiver.

C.3.3 Microcontroller choice results

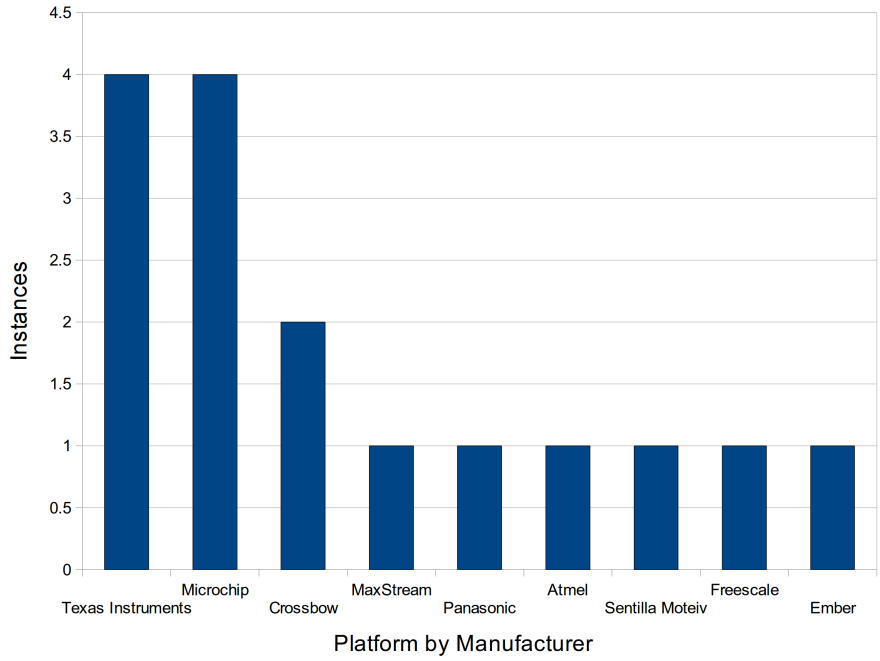
Five microcontroller manufacturers are represented in the survey presented in Table C.1. The number of microcontrollers (24) is greater than of the number of platforms (21) because some custom platforms feature a pairing of a microcontroller with an XBee module, thus using two microcontrollers in total. The most popular choice for a microcontroller manufacturer is Atmel, with 9 out of 24 microcontroller instances, as shown in Figure C.2(a). Atmel is also the most popular choice for a microcontroller across all the manufacturer development kits, featuring in 6 out of 14 unique proprietary development kits in Table C.1. Atmel microcontrollers also feature in 3 out of 5 custom platforms. Figure C.2b shows that the most popular model of microcontroller used is the Atmel ATmega128L, followed by the Microchip PIC18LF4620.

C.3.4 Transceiver choice results

Considering all the studies from Table C.1 there are five manufacturers represented in the list of transceivers used. These are the same five companies represented as microcontroller manufacturers in Section C.3.3. This implies that a company in the business of making a radio transceiver is likely to be in the business of making microcontrollers, and vice versa. By far the most popular manufacturer for a radio transceiver in Table C.1 is Texas Instruments, as shown in Figure C.3(a). More than half of all the platforms reviewed use a Texas Instruments transceiver. The CC2420 from Texas Instruments is the most popular model of choice for a radio transceiver from the given data, with the Freescale MC13193 coming second (see Figure C.3(b). The CC2420 was also the most popular choice of radio transceiver used in development kits, featuring in 7 of the 14 unique proprietary development kits. The obvious popularity of the CC2420 stems from the fact that it was the first single-chip radio transceiver compliant to the IEEE 802.15.4 standard [34].

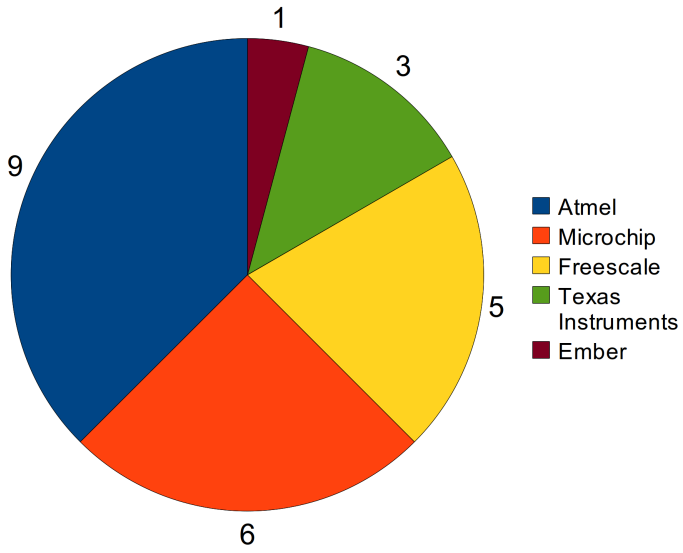


(a) Choice of platform type.

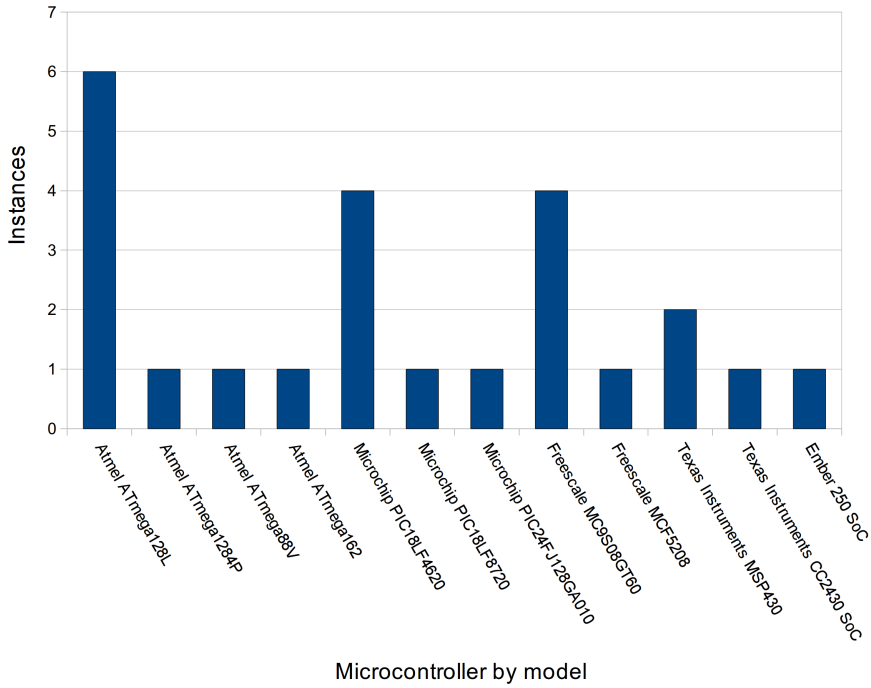


(b) Choice of development platform by manufacturer.

Figure C.1: Platform choices, by type and by manufacturer.

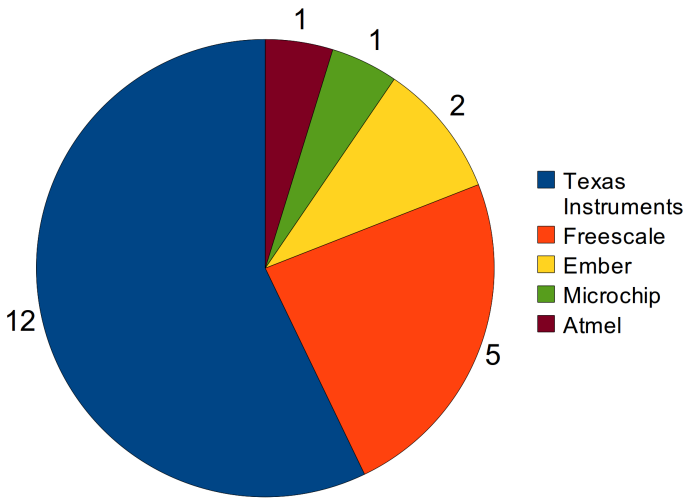


(a) Choice of microcontroller by manufacturer.

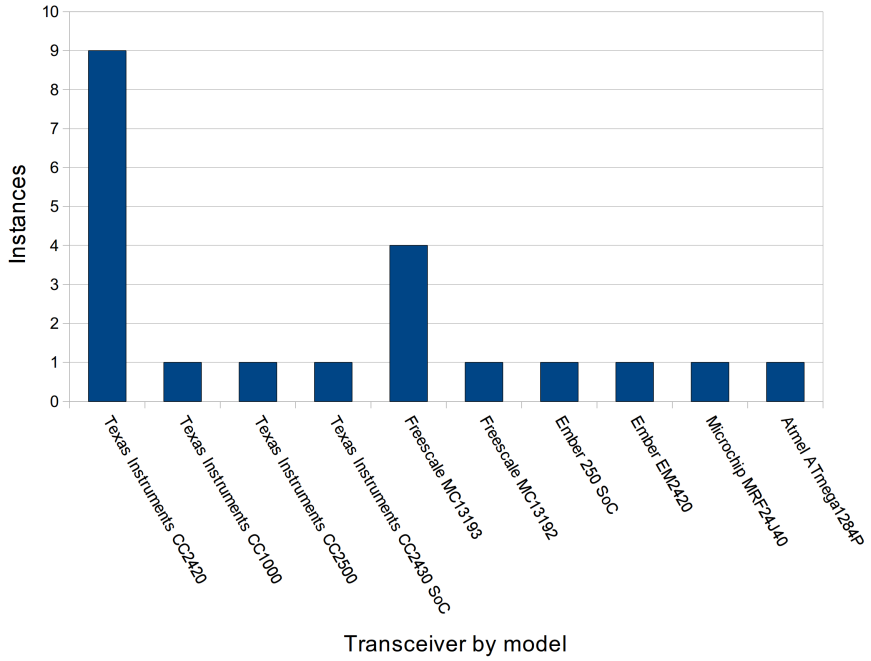


(b) Choice of microcontroller by model.

Figure C.2: Microcontroller choices, by manufacturer and model.



(a) Choice of transceiver by manufacturer.



(b) Choice of transceiver by model.

Figure C.3: Transceiver choices, by manufacturer and model.

C.4 Conclusion

Hundreds of manufacturers have adopted ZigBee technology, and the market for ZigBee devices continues to grow exponentially. ZigBee's current popularity may see it being adopted as the low rate wireless protocol of choice.

Analysis of the literature shows that there is active research in characterising ZigBee network performance. Common performance metrics include packet error rate, throughput/goodput, message latency and power consumption. Results differ from study to study, and platform to platform. Throughput results are considerably lower than the theoretically achievable 250 kb/s offered by IEEE 802.15.4/ZigBee. A number of the studies comment on the difficulty of repeatable measurements, especially with respect to loss of network connectivity owing to multipath fading effects.

When reviewing the hardware platforms used in 21 individual studies it is evident that the Atmel ATmega128L and the Texas Instruments CC2420 are the most popular choices for a microcontroller and radio transceiver respectively. The ATmega128L microcontroller is the most popular microcontroller for manufacturer development platforms as well as custom research platforms. The CC2420 radio transceiver is used in more than half of all reviewed platforms. It is also the oldest IEEE 802.15.4 compliant radio transceiver.

The results of this review may be used in deciding upon a platform on which to base a custom configuration of microcontroller and transceiver, or in choosing a suitable development kit or platform for experimentation.

References

[1] "Supported by Manufacturers with Revenues Surpassing $1 Trillion, ZigBee crosses the Chasm," Smartmeters, June 2010, last accessed 02/08/2010. [Online]. Available: http://www.smartmeters.com/the-news/1012-zigbee-surpasses-1-trillion.html

[2] "ZigBee Crosses the Chasm: A Market Dynamics report on IEEE802.15.4 and ZigBee," ON World, May 2010, last accessed 02/08/2010. [Online]. Available: http://onworld.com/zigbee/

[3] M. LaPedus, "Wireless Sensor Networks set to Take Off," EE Times, April 2010, last accessed 02/08/2010. [Online]. Available: http://www.eetimes.com/electronics-news/4088720/Wireless-sensor-networks-set-to-take-off

[4] "ZigBee for Energy Harvesting and Very Low Power," Energy Harvesting Journal, June 2010, last accessed 02/08/2010. [Online]. Available: http://www.energyharvestingjournal.com/articles/zigbee-for-energy-harvesting-and-very-low-power-00002316.asp?sessionid=1

[5] M. Cinque, D. Cotroneo, G. D. Caro, and M. Pelella, "Reliability Requirements of Wireless Sensor Networks for Dynamic Structural Monitoring," in *DSN 2006 The International Conference on Dependable Systems and Networks*, 2006.

[6] J. P. Lynch and K. J. Loh, "A Summary Review of Wireless Sensors and Sensor Networks for Structural Health Monitoring," *The Shock and Vibration Digest*, vol. 38, no. 2, pp. 91–128, March 2006.

[7] B. Lu, L. Wu, T. G. Habetler, R. G. Harley, and J. A. Guitérrez, "On the Application of Wireless Sensor Networks in Condition Monitoring and Energy Usage Evaluation for Electric Machines," in *IECON 2005 31st Annual Conference of IEEE Industrial Electronics Soceity*, 2005.

[8] L. Ruiz-Garcia, P. Barreiro, Rodriguez-Bermejo, and J. I. Robla, "Review. Monitoring the Intermodal, Refrigerated Transport of Fruit using Sensor Networks," *Spanish Journal of Agricultural Research*, vol. 5, no. 2, pp. 142–156, 2007.

[9] S. Reidy, *Secure Trade Lane*, IBM Corporation, 2007, available online: http://www.research.ibm.com, last accessed 21 May 2008.

[10] P. Fuhr and R. Lau, "Mesh Radio Network Performance in Cargo Containers," March 2005, sensors Magazine Online, site: www.sensorsmag.com, last accessed 7 May 2008.

[11] S. Kootkar and Z. Al-Ars, "Design and Implementation of Reliable Wireless Sensor Networks - A Case Study in Commuter Trains," in *ProRISC Workshop (18th ProRISC'07)*, Veldhoven, Netherlands, November 2007.

[12] P. J. Wolfs, S. Bleakley, S. T. Senini, and P. Thomas, "An Autonomous, Low Cost, Distributed Method For Observing Vehicle Track Interactions," in *Proceedings of JRC2006, Joint Rail Conference*, Atlanta, USA, April 2006, pp. 279–286.

[13] J. Lönn and J. Olsson, "ZigBee for Wireless Networking," Master's thesis, Linköping University, March 2005.

[14] A. Wettergren, "ZigBee in Industry," Bachelor Thesis Performed in Computer Engineering at Linköping Institute of Technology, August 2007.

[15] H. Ramazanali, "Characterization and Evaluation of ZigBee Modules," Master's thesis, Norrköping Department of Science and Technology (ITN), February 2006.

[16] V. Prajzler, "Use of Wireless Communications in Small Medical (Battery Powered) Electronic Equipment," Master's thesis, Czech Technical University in Prague, Faculty of Electrical Engineering, 2008.

[17] E. D. Pinedo-Frausto and J. A. García-Macías, "An experimental analysis of Zigbee networks," *LCN 2008, The 33rd IEEE Conference on Local Computer Networks, The Conference on Leading Edge and Practical Computer Networking, Hyatt Regency Montreal, Montreal, Quebec, Canada*, pp. 723–729, 2008.

[18] K. Shuaib, M. Boulmalf, F. Sallabi, and A. Lakas, "Co-existence of ZigBee and WLAN - a Performance Study," in *Wireless and Optical Communications Networks, 2006 IFIP International Conference on*, 0-0 2006, pp. 5 pp. –5.

[19] T. R. Burchfield, S. Venkatesan, and D. Weiner, "Maximizing Througput in Zigbee Wireless Networks through Analysis, Simulations and Implementations," *University of Dallas, Texas.*

[20] G. D. and S. L., "Basic Characteristics of ZigBee and Simpliciti Modules to use in Measurement Systems," in *XIX IMEKO World Congress*, Lisbon, Portugal, September 6-11 2009.

[21] C. See, K. Horoshenkov, S. Tait, R. Abd-Alhameed, Y. Hu, E. Elkhazmi, and J. Gardiner, "A ZigBee based Wireless Sensor Network for Sewerage Monitoring," in *Microwave Conference, 2009. APMC 2009. Asia Pacific*, 7-10 2009, pp. 731 –734.

[22] P. Corral, V. Almenar, and A. C. de C. Lima, "Distance Estimation System Based on ZigBee," in *Spread Spectrum Techniques and Applications, 2008. ISSSTA '08. IEEE 10th International Symposium on*, 25-28 2008, pp. 817 –820.

[23] W. Xiao, Y. Sun, Y. Liu, and Q. Yang, "TEA: Transmission Error Approximation for Distance Estimation between two ZigBee Devices," in *Networking, Architecture, and Storages, 2006. IWNAS '06. International Workshop on*, 0-0 2006, p. 8 pp.

[24] G. Ferrari, P. Medagliani, S. D. Piazza, and M. Martalo, "Wireless Sensor Networks: Performance Analysis in Indoor Scenarios," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, Article ID 81864, 2007.

[25] M. Armholt, S. Junnila, and I. Defee, "A Non-beaconing ZigBee Network Implementation and Performance Study," in *Communications, 2007. ICC '07. IEEE International Conference on*, 24-28 2007, pp. 3232 –3236.

[26] H.-M. Tsai, C. Saraydar, T. Talty, M. Ames, A. Macdonald, and O. Tonguz, "ZigBee-based Intra-car Wireless Sensor Network," in *Communications, 2007. ICC '07. IEEE International Conference on*, 24-28 2007, pp. 3965 –3971.

[27] P. Suarez, C.-G. Renmarker, A. Dunkels, and T. Voigt, "Increasing ZigBee network lifetime with X-MAC," in *REALWSN '08: Proceedings of the workshop on Real-world wireless sensor networks.* New York, NY, USA: ACM, 2008, pp. 26–30.

[28] M. Kohvakka, M. Kuorilehto, M. Hännikäinen, and T. D. Hämäläinen, "Performance analysis of IEEE 802.15.4 and ZigBee for large-scale wireless sensor network applications," in *PE-WASUN '06: Proceedings of the 3rd ACM international workshop on Performance evaluation of wireless ad hoc, sensor and ubiquitous networks.* New York, NY, USA: ACM, 2006, pp. 48–57.

[29] K. Liu, "Performance Evaluation of ZigBee Network for Embedded Electricity Meters," Master's thesis, KTH Royal Institute of Technology, School of Electrical Engineering, 2009.

[30] N. Watthanawisuth, N. Tongrod, T. Kerdcharoen, and A. Tuantranont, "Real-time Monitoring of GPS-tracking Tractor based on ZigBee Multi-hop Mesh

Network," in *Electrical Engineering/Electronics Computer Telecommunications and Information Technology (ECTI-CON), 2010 International Conference on*, 19-21 2010, pp. 580 –583.

[31] K. Benkic, M. Malajner, P. Planinsic, and Z. Cucej, "Using RSSI Value for Distance Estimation in Wireless Sensor Networks based on ZigBee," in *Systems, Signals and Image Processing, 2008. IWSSIP 2008. 15th International Conference on*, 25-28 2008, pp. 303 –306.

[32] *XBee and XBee-PRO ZB*, Digi International Inc., Document ID: 91001471 - D1/610, 2010.

[33] *PICDEM Z Demonstration Kit Users Guide*, Microchip Technology Inc., Document ID: DS51524C, 2008.

[34] "ZigBee & RF4CE," Texas Instruments, last accessed 02/08/2010. [Online]. Available: http://http://www.ti.com/

Appendix D

Electronics and PCB Design

D.1 Introduction

The details of the hardware implementation of a ZigBee wireless sensor network are presented in this appendix. The author has implemented a custom hardware configuration based on a development platform. This custom platform is designated *DFZ* (a combination of the author's name and ZigBee). The reasons for developing a custom platform include:

- The Printed Circuit Boards (PCBs) and electronic components may be bought in volume, decreasing the cost per board when compared to individual development kit devices.
- The omission of unnecessary components results in lower power consumption and cost.
- The addition of custom features increases functionality.
- A greater understanding of the electronic components making up a wireless sensor node is achieved in developing custom hardware.

Microchip products form the basis for the hardware implementation of the DFZ platform devices owing to existing hardware within the School of Electrical and Information Engineering, as well as an existing relationship between the School and the local distributor. The Microchip PICDEM Z Development Kit was used in the initial stages of research [1] and influences the custom hardware platform discussed in the succeeding sections. The same microcontroller was used, as well as the majority

of the pin configurations. Changes implemented in the DFZ platform with respect to the PICDEM Z platform are as follows:

- A new Radio Frequency (RF) module with Power Amplifier (PA) and Linear Noise Amplifier (LNA) replaces the PICDEM Z RF daughterboard.
- A Low Drop-Out (LDO) regulator with higher current sourcing capacity replaces equivalent on PICDEM Z.
- Serial communication level translation capability is moved off-board to a plug-in module.
- Two additional Light Emitting Diodes (LEDs) are available on the DFZ platform.
- Jumper-selectable current measurement capabilities are available on the DFZ platform.
- The DFZ platform features only one power input source (battery connections omitted).

Section D.2 details the electronic components used in the DFZ hardware, and Section D.3 details the PCB considerations. Concluding remarks are found in Section D.4.

D.2 Electronics

D.2.1 Overview

The hardware configuration for a basic wireless sensor network device is given in Figure D.1. The transducer is the component which converts environmental data into electrical data to be processed by the microcontroller. Signal conditioning serves to modify the transducer signal such that it can be accurately recorded by the microcontroller. The power supply ensures a stable voltage level is available to the rest of the electronic components as well as providing sufficient current sourcing capacity. The microcontroller hosts the application and ZigBee stack firmware. The radio transceiver enables transmission and reception of IEEE 802.15.4 compliant messages through the physical medium. Peripheral features such as in-circuit programming,

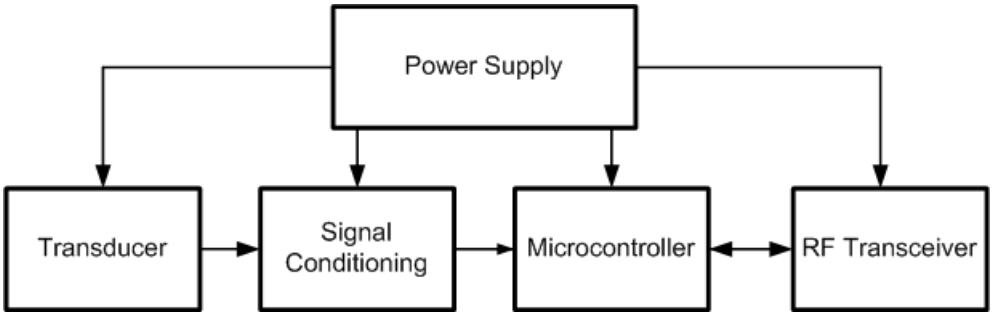


Figure D.1: Basic wireless sensor network device.

user input/output and serial (wired) communication capabilities are optional and serve to increase the functionality of the device.

The electronic components are chosen for their low power characteristics and small form factor. With the exception of the microcontroller, all the electronic components are in surface mount packages. Using surface mount packages reduces electromagnetic interference and emissions, uses up less PCB real estate, and results in a cheaper bill of materials than when using through-hole equivalents [2],[3]. The microcontroller has been specified as a through-hole component as this allows for removal of the IC for inspection and substitution without requiring any de-soldering.

A sensing element has been omitted from the DFZ boards, as the focus of this research is on general network performance. Provision is made for peripheral components through the use of the unused microcontroller pins, accessible via header pins on the PCB.

D.2.2 Microcontroller

The microcontroller into which the application and ZigBee stack firmware is programmed is a Microchip PIC18LF4620. The version used in the custom hardware platform is a 40 pin Dual In-line Package (DIP) variant. Features of the PIC18LF4620 include [4]:

- Customisable sleep, idle and run modes of operation
- System frequency of up to 40 MHz
- Watchdog timer (4 ms to 131 s)

- 3 external interrupts
- Serial Peripheral Interface (SPI) bus, Inter Integrated Circuit (I^2C) bus and RS-232 Universal Asynchronous Receiver/Transmitter (UART) connectivity options
- 36 possible input/output pins
- 13 10-bit analogue-to-digital conversion channels
- 1 8-bit timer, 3 16-bit timers
- In-circuit programming and debugging

The sleep modes are used for ZigBee end devices. End devices can be set to sleep for the duration of the watchdog timer period. After "waking up" the device will check if there are any messages pending for it, or perform a scripted operation, such as take a sensor reading and transmit it to the ZigBee coordinator (see Appendix E).

The SPI bus is used for communication with the MRF24J40MB radio transceiver, and the UART capability is used for monitoring and debugging purposes.

The timers are used within the ZigBee stack for clocking functionality as well as in the application firmware for generating intervals for periodic application data messages.

A 4 MHz crystal oscillator is used in conjunction with the microcontroller's built in phase lock loop to provide a 16 MHz system clock frequency (Note: one instruction cycle is equivalent to 4 system clock cycles). The crystal frequency is the same as that used in the PICDEM Z development kit, providing a system clock frequency sufficient to handle all stack operations whilst not so high as as to draw excessive current from the power supply.

D.2.3 Radio Transceiver

The Microchip MRF24J40MB transceiver module enables RF communication. The module operates at 2.4 GHz in the Industrial, Scientific and Medical radio band. The module uses the SPI protocol to interface with the microcontroller, in addition to signal lines for wake/sleep modes and data interrupts. The MRF24J40MB has received regulatory approval for use in the United States, Canada and Europe [5].

South Africa models its emissions standards on the European Telecommunications Standards Institute (ETSI) standards, and so this module conforms with the local regulatory body (the South African Bureau of Standards) and the related missions standard (SANS 300328) [6].

The module uses a 4-layer PCB featuring dedicated planes for RF signals, digital (microcontroller) signals as well as power and ground. A PCB trace antenna is employed for RF transmission and reception, and a metallic shield covers the electronic components to avoid RF interference.

The MRF24J40MB is placed on its own PCB daughterboard which then connects to the DFZ motherboard. This allows for more flexible troubleshooting, as replacement transceiver modules can be tested in the same motherboard, as well as allowing the older PICDEM Z transceiver modules to be placed in the new custom motherboards for comparison.

Specifications of the MRF24J40MB include [5]:

- Integrated Power Amplifier, Low Noise Amplifier and PCB antenna
- Up to 1.2 km possible range (outdoor open area free line of sight conditions)
- Reception mode current consumption: 25 mA
- Transmission mode current consumption: 130 mA
- Sleep mode current consumption: 5 μA
- -102 dBm receiver sensitivity
- +20 dBm transmitter output power
- IEEE 802.15.4 standard compliant
- Supports ZigBee protocol

D.2.4 Power Supply

A system voltage of 3.3 V is supplied to all subsystems on the device PCB by a National Instruments LM2937-3.3 linear low drop-out regulator Integrated Circuit (IC). A linear regulator is favoured over a switched-mode regulator owing to the improved efficiency at low load currents, lower cost and lower noise injection [7].

While a switched-mode regulator may be more efficient at higher loads, a battery reliant end device spends the majority of its time in sleep mode (low load current). Even routing or coordinator devices only approach maximum load current for very short intervals (when transmitting a message). The LM2937 features a quiescent current of typically 2 to 10 mA (under the expected operating conditions) and is able to supply up to 400 mA continuously. The LM2937 operates with an input voltage in the range of 4.75 to 26 V. A current measurement resistor may be switched in series with the regulator output with the use of jumper positioning.

Capacitors and the LDO regulator

Low-power RF transmissions at a short distance from an electronic component poses a much greater threat than high-power transmissions at greater distances. Voltage regulators are susceptible to radiated RF fields in the 1 to 10 V/m range [3]. Capacitors are used to mitigate the threat of RF noise from the radio transceiver and surrounding devices coupling into the power supply. Ceramic capacitors connect to the regulator's input and output pins, acting as a low impedance shunt to ground for high frequencies. The literature states this impedance should be a few ohms or less and suggests a value of 1.6 Ω relative to the capacitor impedance [3], as shown in Equation D.1.

$$X_c = \frac{1}{2\pi f C} = 1.6\Omega \tag{D.1}$$

Using f as the ZigBee centre frequency of 2.45 GHz to solve for C, a value of 40.82 pF is obtained. Consultation of radio transceiver module schematic diagram shows decoupling capacitors of 47 pF are in use around the transceiver IC. Satisfied that the calculated result is within a few picofarads of this value, a decision is made to follow the example made by the RF module schematic, and 47 pF decoupling capacitors are chosen.

In order to maintain regulator stability it is necessary to place an output capacitor which meets specific requirements for Equivalent Series Resistance (ESR) and minimum capacitance [8]. Operating at maximum current capacity (400 mA) the output capacitor must have an ESR less than 5 Ω and a minimum of capacitance of 10 μF. As increasing the capacitance will give improved transient response, a tantalum capacitor of 100 μF with an ESR value of less than 1 Ω is chosen for the

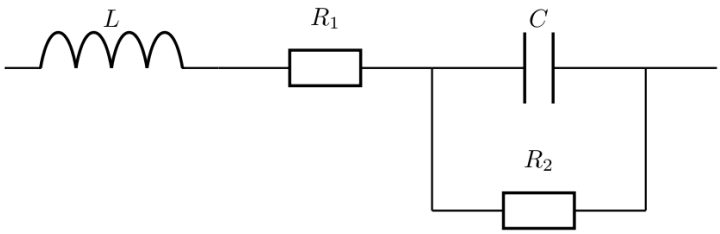


Figure D.2: Equivalent circuit for a capacitor.

output capacitor. Tantalum is preferred over aluminium electrolytic capacitors as tantalum exhibits a lower ESR and a higher capacitance-to-volume ratio [3].

The regulator datasheet also recommends using a 0.1 μF capacitor placed parallel to the unregulated input and ground [8]. In total there are four capacitors placed around the regulator: 0.1 μF and 47 pF in parallel on the input side, and 47 pF and 100 μF in parallel on the output side. In order to efficiently decouple the power supply from a wide bandwidth of frequencies it is necessary to follow certain design principles. Real capacitors include elements of resistance and inductance, as shown in the equivalent circuit in Figure D.2 and in Equation D.2.

$$X_c = 2\pi f L + R_1 + \frac{1}{2\pi f C} \| R_2 \tag{D.2}$$

L is the Equivalent Series Inductance (ESL), R_1 is the Equivalent Series Resistance (ESR), R_2 is the parallel leakage (a function of the capacitor mounting structure) and C is the capacitance. At low frequencies the capacitance dominates the overall impedance, and at higher frequencies the impedance is dominated by the inductance. The point at which the impedance of a capacitor is lowest is the frequency at which the capacitor becomes self-resonant with its own inductance [3]. Figure D.3 shows the effect of frequency on a capacitor, including the effects of its ESL.

As the ESL is primarily a function of the capacitor casing, simply placing different valued capacitors of the same size in parallel with each other will not serve to extend the effective decoupling bandwidth of such a combination. Figure D.4(a) shows this effect when using capacitors of the same casing size. It is therefore necessary to choose parallel capacitors of different values and different casing sizes, with the smaller value capacitor having the smallest casing size [9]. Figure D.4(b) shows the effect of choosing different capacitor values and casing sizes.

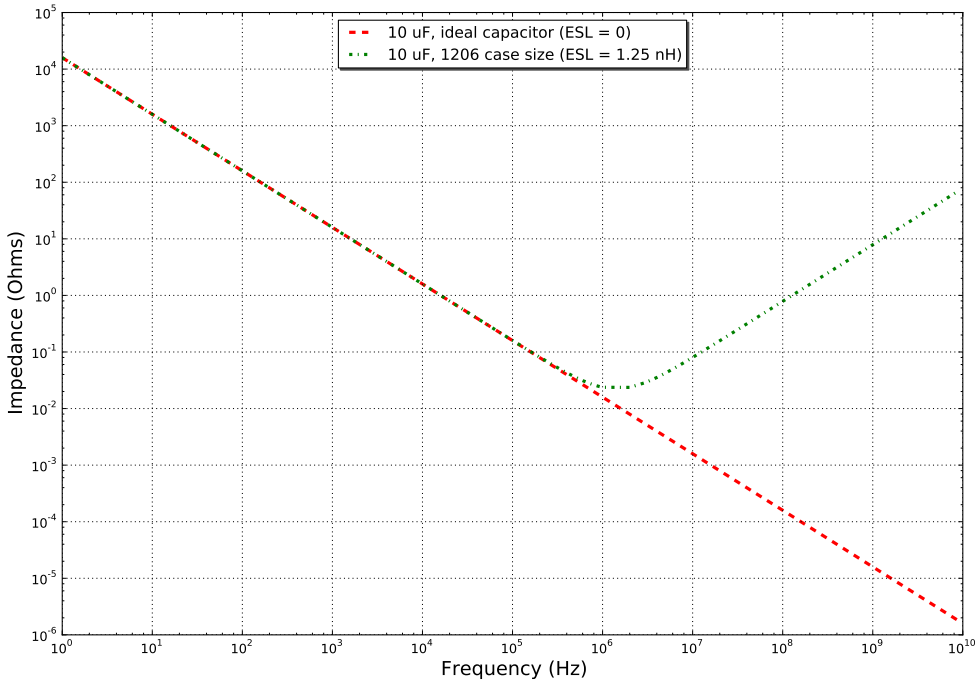


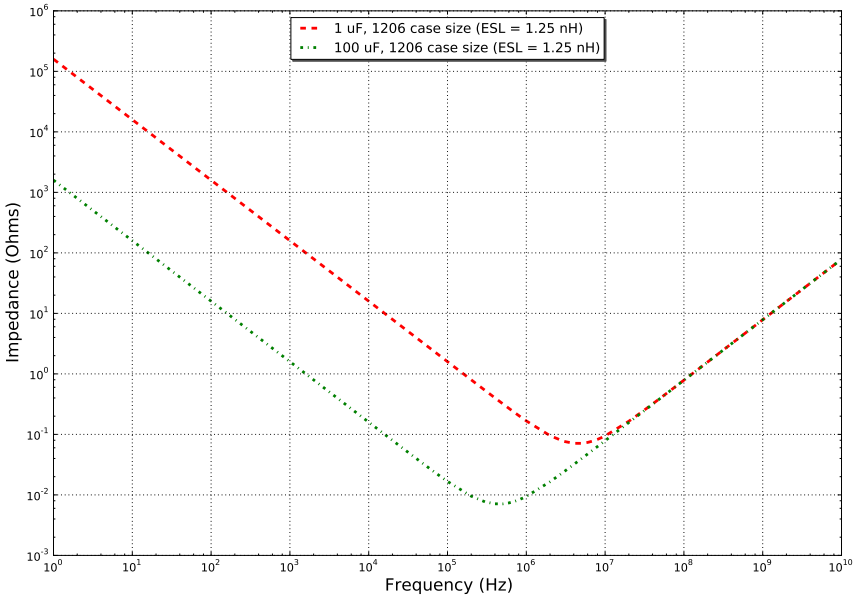
Figure D.3: Comparison of ideal capacitor frequency response with a real capacitor frequency response.

Table D.1: Capacitor case sizes

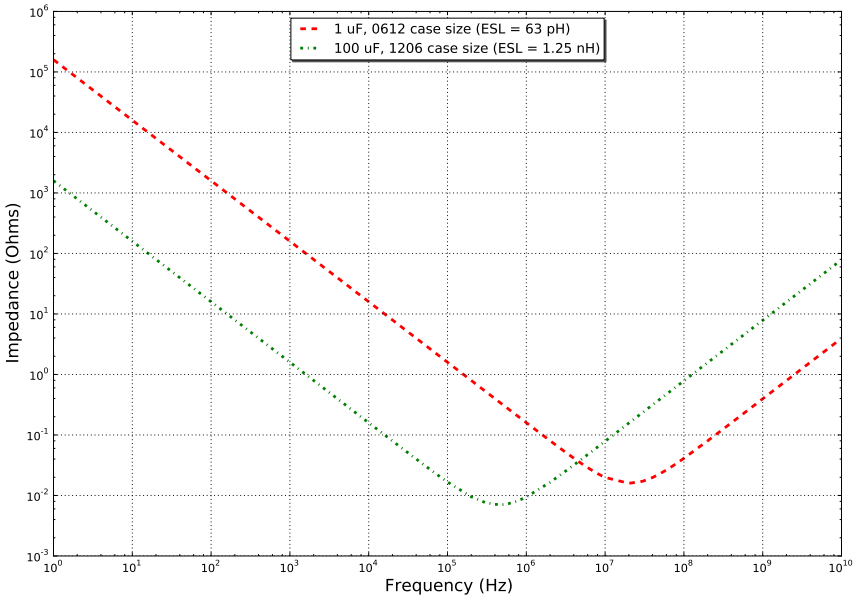
Capacitor value	**EIA case size**
47 pF	0805
0.1 μF	1206
100 μF	7343

These principles have been applied to the capacitors chosen for the LDO regulator as seen in Table D.1.

Figure D.5(a) presents the simulated frequency response of the input capacitor combination, and Figure D.5(b) presents that for the output capacitor combination. One can see that using two different case sizes results in a lower impedance path at higher frequencies, helping to decouple the RF noise from the power supply.

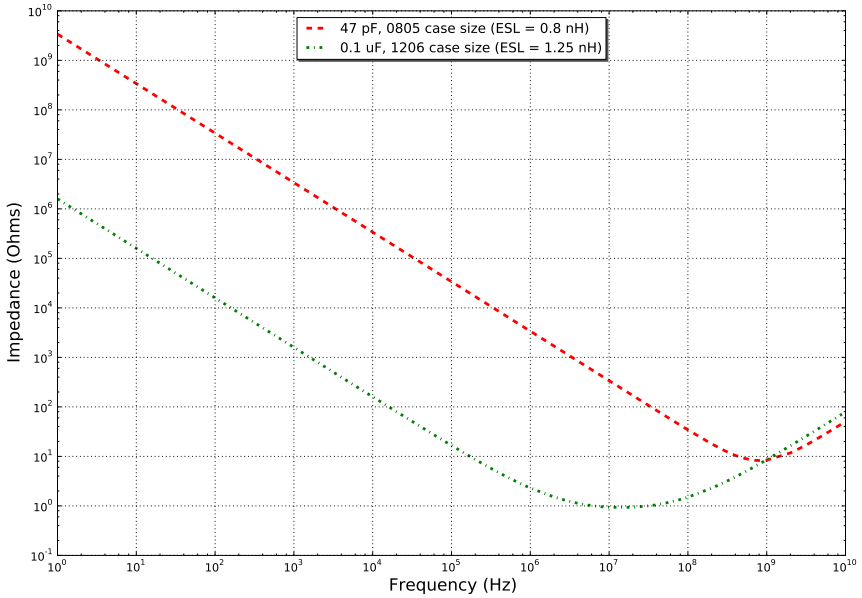


(a) Different value capacitor with same casing size.

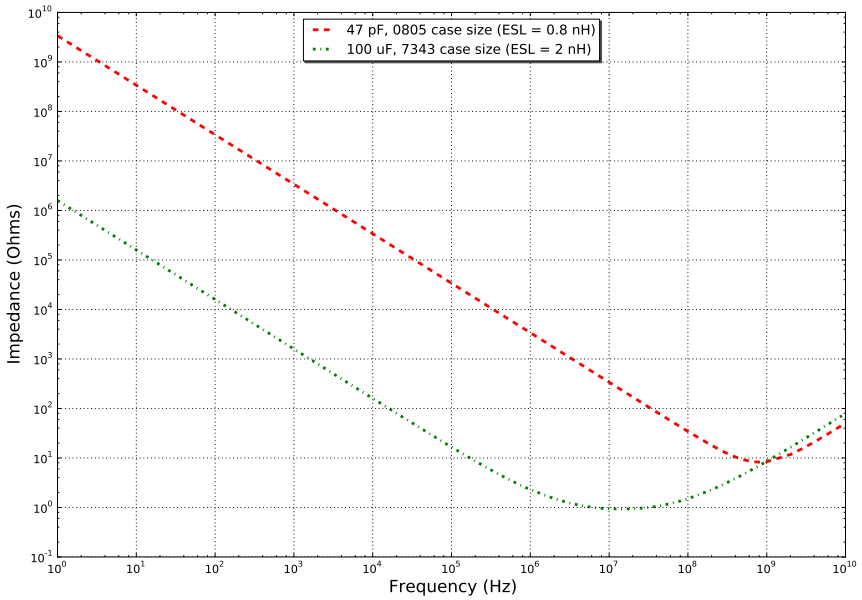


(b) Different value capacitor with different casing size.

Figure D.4: Comparison of capacitors with different values and casing sizes.



(a) Frequency response for input capacitor combination.



(b) Frequency response for output capacitor combination.

Figure D.5: Frequency response simulations for input and output capacitors.

D.2.5 Serial Communication

Pin headers are provided to which a custom level-translating board may be connected in the event that serial output to a computer terminal is required. A serial communication daughterboard is tethered permanently to the DFZ coordinator device, and connected as needed for other devices (usually for debugging purposes).

D.2.6 User Input/Output

Two momentary push-buttons are available to the user, as well as a microcontroller reset button. Four LEDs are available as visual outputs. The LEDs are typically used during debugging and as indicators when taking measurements. It is not advisable to have the LEDs on for extended periods of time when used in-application as each LED draws 4 mA when on.

Female header pins are connected alongside the microcontroller's pins which allow for small daughterboards to be plugged in above the microcontroller. This allows sensors, external memory, communications modules, etc. access to all the microcontroller pins.

D.2.7 Programming and Debugging

Pin headers are provided to which a programming device which follows Microchip's In-Circuit Serial Programming (ICSP) protocol and pin-out configuration may be connected. This allows each microcontroller to be programmed as it sits in its individual PCB. The ICSP interface also allows for In-Circuit Debugging (ICD), allowing PC software to monitor the microcontroller's registers during application operation.

D.3 Printed Circuit Board

D.3.1 Overview

The hardware components of the ZigBee device implemented in this research can be found on three separate PCBs:

- The DFZ motherboard: containing the microcontroller, power supply, user input/output features and daughterboard access.
- The MRF24J40MB RF daughterboard: containing the radio transceiver module.
- The serial communications daughterboard: containing the TTL/RS-232 level translating IC.

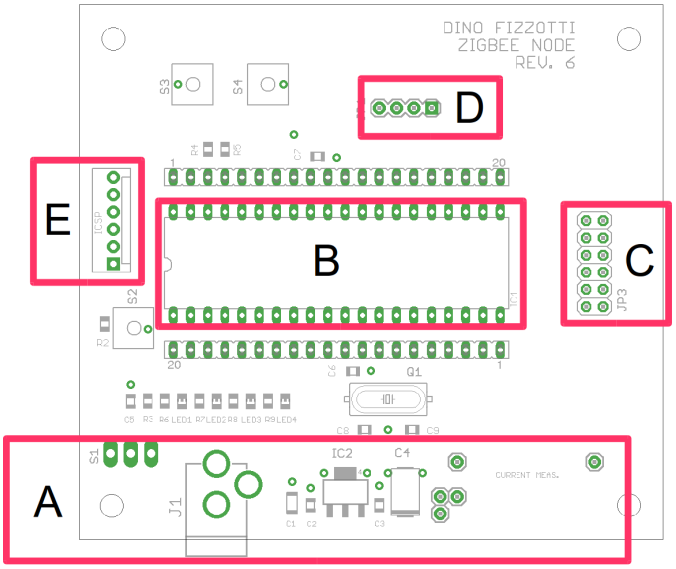
Multilayer PCBs (four or more layers) are commonly used for RF devices. Each layer is dedicated to a specific type of signal: RF and digital signal layout, RF ground, power supply layout and power supply ground. The advantages of multilayer PCBs on one- and two-layer boards are as follows [3]:

- Signals may be routed in microstrip configurations, incorporating controlled impedance transmission lines resulting in lower radiated emissions for electromagnetic compatibility.
- Reduced loop area as return current is on the adjacent plane, resulting in decreased noise sensitivity and radiated emissions.
- A dedicated ground plane decreases ground impedance and hence ground noise.

The manufacturing cost of a multilayer PCB is much higher than that of a two-layer PCB, especially when considering small volumes of PCBs. As the MRF24J40MB transceiver module is already manufactured using a multilayer PCB layout, and the clock frequencies of the digital signals on the DFZ motherboard are less than 10 MHz it is deemed acceptable to use a two-layer PCB layout for the DFZ motherboard and the MRF24J40MB daughterboard. The serial communications daughterboard contains few components and a single layer design using through-hole components is favoured as this board can be reproduced without the need for professional PCB fabrication. In following best practice principles the following design features have been incorporated into the PCB layout [3][10][11]:

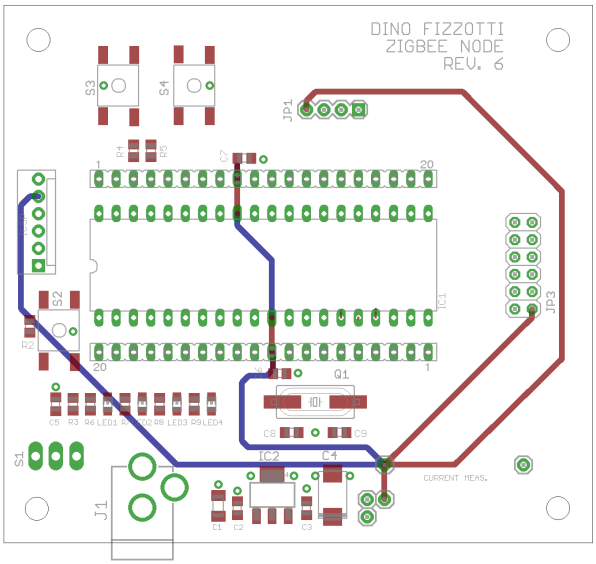
- Both the top and bottom layers make use of ground fill in an effort to reduce radiated emissions and noise sensitivity. Ground fill on both layers are coupled to each other using the through-hole component leads at multiple points on the PCB.

- PCB zoning is implemented. The power supply, ICSP programming, RF module SPI connections and UART serial connections are routed within a small locus of related ICs. The spatial isolation aims to decrease instances of coupling occurring between the components. Figure D.6(a) shows an overview of the PCB indicating the zones.
- The power supply is routed to other components in a star topology in an effort to reduce coupling between the components in the system. The 100 μF output capacitor of the LDO regulator at the central node in the star configuration helps to remove low frequency noise and create a stable DC voltage. Figure D.6(b) shows an overview of the PCB indicating power routing to the components.
- Power supply tracks are routed using wide PCB tracks in an effort to reduce the track impedance.



A: Power supply
B: Microcontroller
C: RF daughterboard connection
D: Serial comms. connection
E: In-circuit programming connection

(a) PCB zones.



(b) Power supply routing.

Figure D.6: Layout features of the DFZ PCBs.

D.3.2 Schematics

Figure D.7: DFZ motherboard schematic.

Figure D.8: MRF24J40MB daughterboard schematic.

Figure D.9: Serial communications daughterboard schematic.

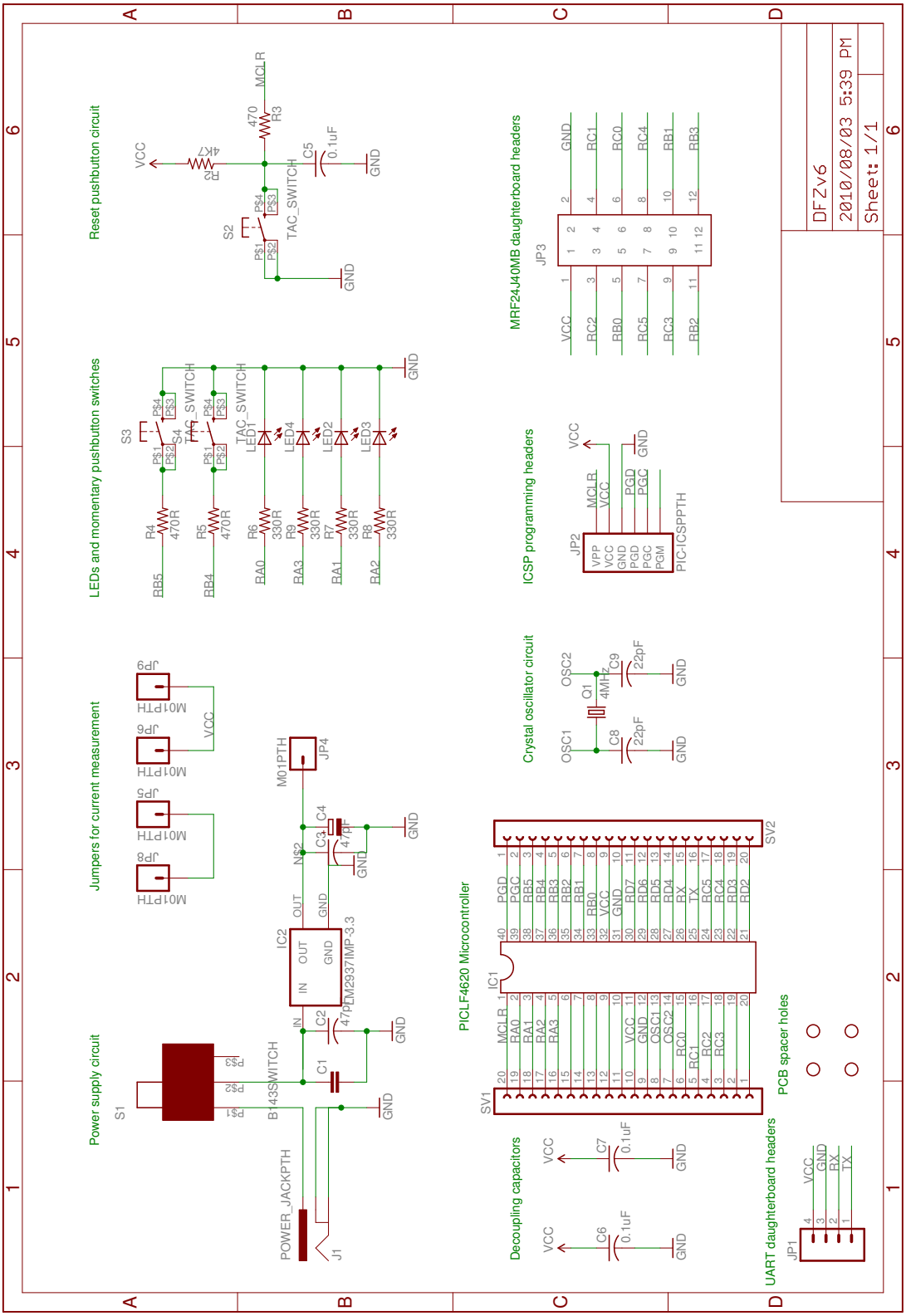


Figure D.7: DFZ motherboard schematic.

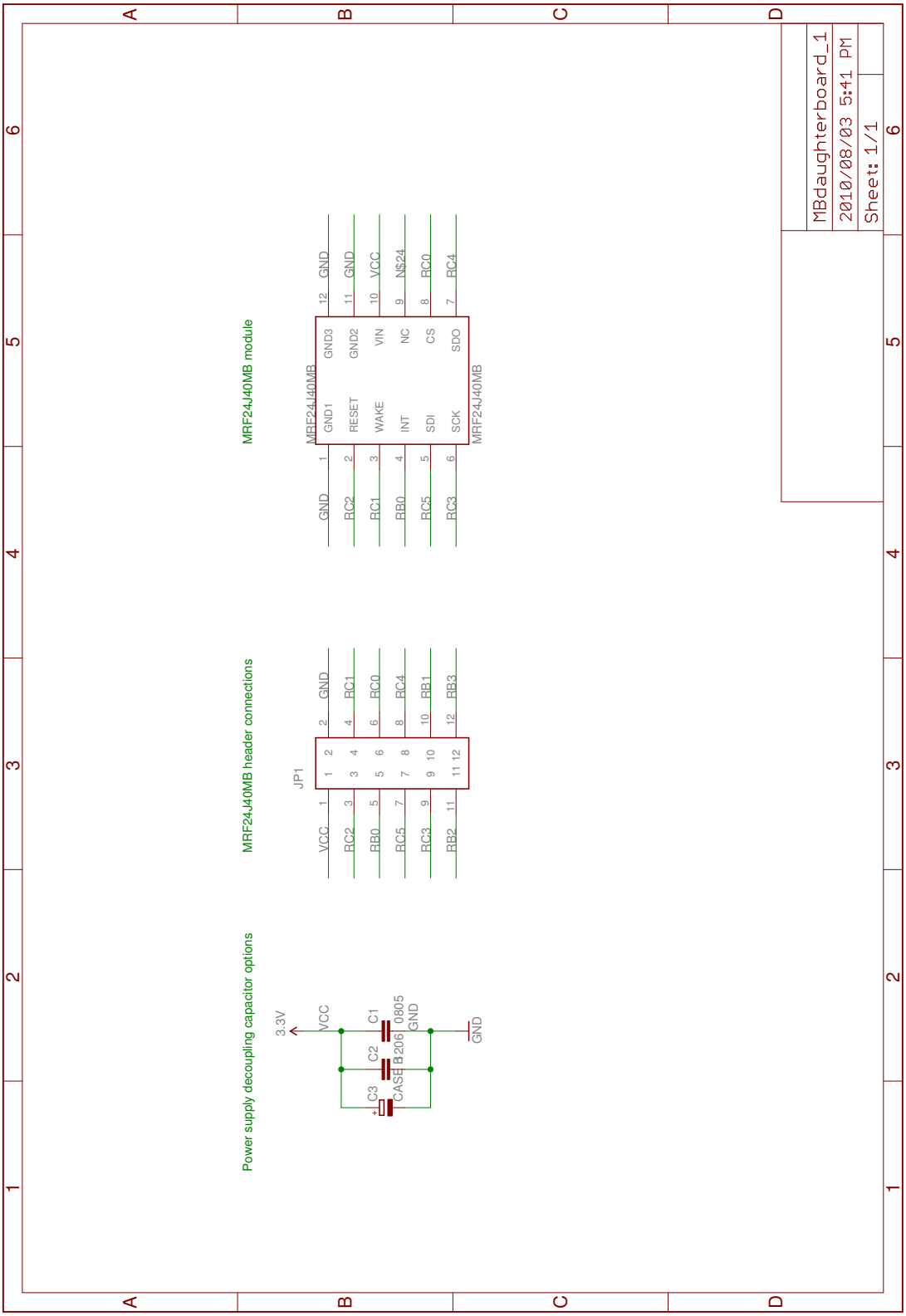


Figure D.8: MRF24J40MB daughterboard schematic.

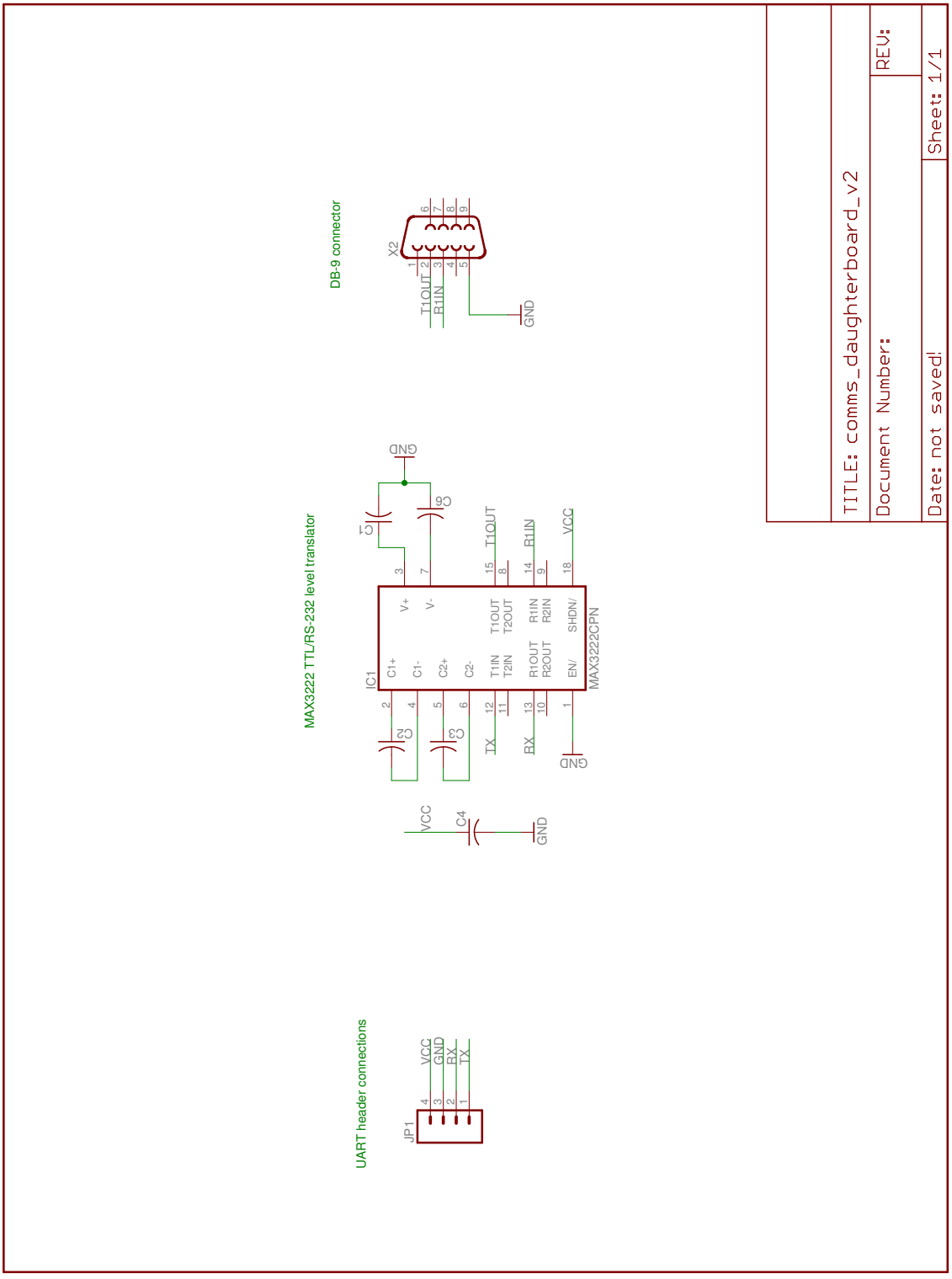


Figure D.9: Serial communications daughterboard schematic.

D.3.3 Bill of Materials

Table D.2 lists the materials used in the DFZ motherboard. The MRF24J40MB daughterboard layout provides for three different decoupling capacitor case sizes. It is recommended to place at least one 0.1 μF capacitor in one of the spaces provided, but a combination of different capacitor values and case sizes may be employed. Table D.3 lists the materials used in the MRF24J40MB daughterboard, and Table D.4 lists the materials used in the serial communications motherboard. The header pins for the microcontroller, UART daughterboard connection and current measurement facility have been omitted as these can be bought in bulk strips.

Table D.2: Bill of materials for the DFZ motherboard.

Label	Description	Value	Package	Manufacturer	Part Number
C1	Capacitor	0.1 μF	1206	Yageo	CC1206KRX7R9BB104
C2	Capacitor	47 pF	0805	Yageo	C0805JRNPO9BN470
C3	Capacitor	47 pF	0805	Yageo	C0805JRNPO9BN470
C4	Capacitor	100 μF	7343-31R	Vishay	293D107X9010D2TE3
C5	Capacitor	0.1 μF	0805	Yageo	CC0805HRX7R9BB104
C6	Capacitor	0.1 μF	0805	Yageo	CC0805HRX7R9BB104
C7	Capacitor	0.1 μF	0805	Yageo	CC0805HRX7R9BB104
C8	Capacitor	22 pF	0805	Yageo	C0805JRNPO9BN220
C9	Capacitor	22 pF	0805	Yageo	C0805JRNPO9BN220
IC1	Microcontroller		DIP40	Microchip	PIC18LF4620-I/P
IC2	Low Drop-Out Regulator		SOT223	National Semi.	LM2937IMP-3.3
LED1	Light Emitting Diode	RED	0805	Bright LED	BL-HS135A-TRB
LED2	Light Emitting Diode	RED	0805	Bright LED	BL-HS135A-TRB
LED3	Light Emitting Diode	RED	0805	Bright LED	BL-HS135A-TRB
LED4	Light Emitting Diode	RED	0805	Bright LED	BL-HS135A-TRB
Q1	Crystal	4 MHz	HC-49SMD	MEC	SMD49S-4M2030F
R2	Resistor	4.7 kΩ	0805	Yageo	RC0805JR-074K7
R3	Resistor	470 Ω	0805	Yageo	RC0805JR-07470R
R4	Resistor	470 Ω	0805	Yageo	RC0805JR-07470R
R5	Resistor	470 Ω	0805	Yageo	RC0805JR-07470R
R6	Resistor	330 Ω	0805	Yageo	RC0805JR-07330R
R7	Resistor	330 Ω	0805	Yageo	RC0805JR-07330R
R8	Resistor	330 Ω	0805	Yageo	RC0805JR-07330R

Continued on next page

Table D.2: Bill of materials for the DFZ motherboard (continued from previous page).

Label	Description	Value	Package	Manufacturer	Part Number
R9	Resistor	330 Ω	0805	Yageo	RC0805JR-07330R
S1	Slide Switch			EIE	B143
S2	Momentary Pushbutton			MEC	MTS-1132 4.3MM
S3	Momentary Pushbutton			MEC	MTS-1132 4.3MM
S4	Momentary Pushbutton			MEC	MTS-1132 4.3MM
J1	DC Power Plug			EIE	K375B
JP3	RF Daughterboard connector			Samtec	LST-106-07-F-D

Table D.3: Bill of materials for the MRF24J40MB daughterboard.

Label	Description	Value	Package	Manufacturer	Part Number
C1	Capacitor		0805		
C2	Capacitor		1206		
C3	Capacitor		3528-21W		
IC1	Radio Transceiver			Microchip	MRF24J40MB-I/RM
JP1	RF Daughterboard connector			Samtec	LST-106-07-F-D

Table D.4: Bill of materials for the serial communications daughterboard.

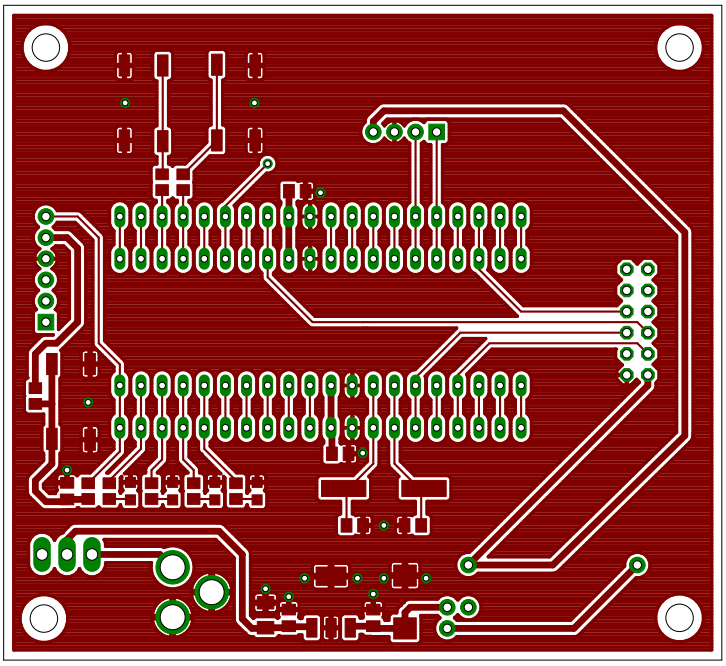
Label	**Description**	**Value**	**Package**	**Manufacturer**	**Part Number**
C1	Capacitor	0.1 μF	Through-hole	Fenghua	CT4-0805Y104M630-F1
C2	Capacitor	0.1 μF	Through-hole	Fenghua	CT4-0805Y104M630-F1
C2	Capacitor	0.1 μF	Through-hole	Fenghua	CT4-0805Y104M630-F1
C2	Capacitor	0.1 μF	Through-hole	Fenghua	CT4-0805Y104M630-F1
C2	Capacitor	0.1 μF	Through-hole	Fenghua	CT4-0805Y104M630-F1
IC1	Logic Level Translator		DIP18	Maxim	MAX3222CPN

D.3.4 Copper Layout

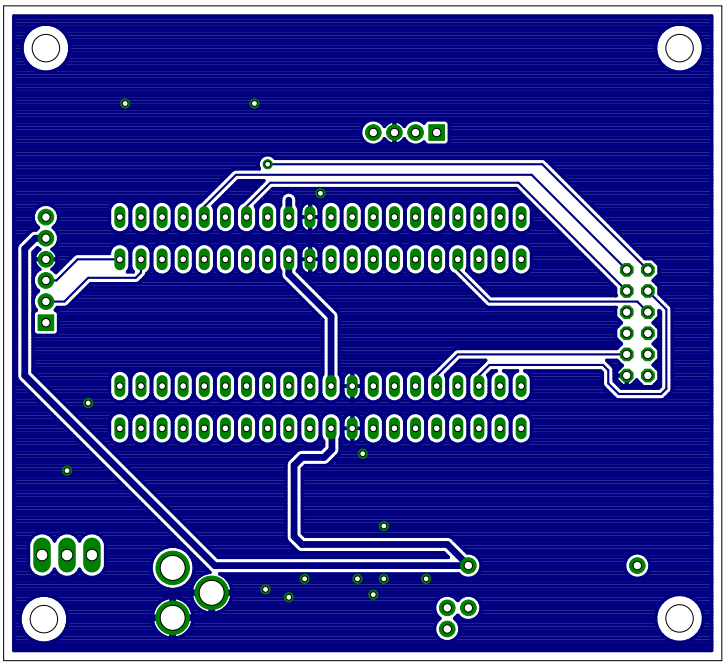
Figure D.10: Copper layout for the DFZ motherboard.

Figure D.11: Copper layout for the MRF24J40MB daughterboard.

Figure D.12: Copper layout for the serial communications daughterboard.

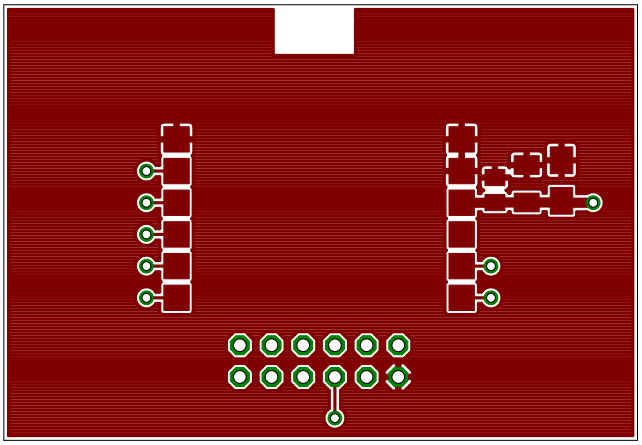


(a) Top copper for the DFZ motherboard.

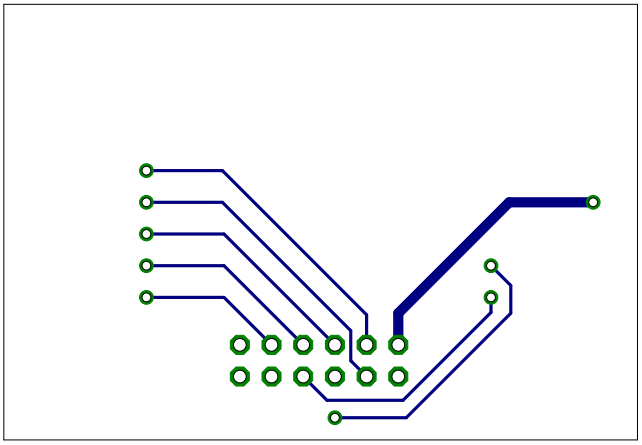


(b) Bottom copper for the DFZ motherboard.

Figure D.10: Copper layout for the DFZ motherboard.

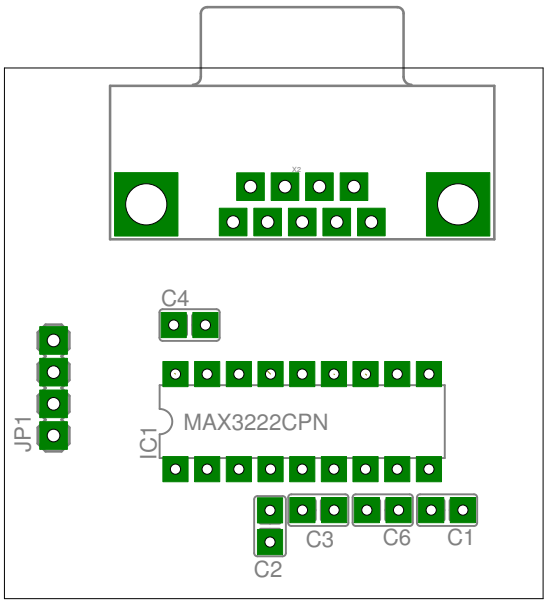


(a) Top copper for the MRF24J40MB daughterboard.

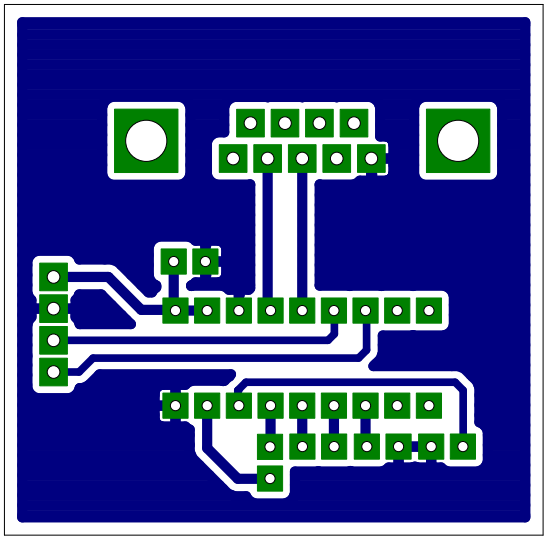


(b) Bottom copper for the MRF24J40MB daughterboard.

Figure D.11: Copper layout for the MRF24J40MB daughterboard.



(a) Top copper for the serial communications daughterboard.



(b) Bottom copper for the serial communications daughterboard.

Figure D.12: Copper layout for the serial communications daughterboard.

D.4 Conclusion

The Microchip PICDEM Z development kit provides the basis for the custom DFZ hardware platform, with similar microcontroller pin configurations for input/output and serial communication signals. The omission of on-board UART and a dedicated battery connection serve to conserve power and save PCB space. Additional output LEDs aid firmware debugging, and a connection for a new RF daughterboard that is backwards compatible with the PICDEM Z RF daughterboards is provided.

The LM2937 Low Drop-Out (LDO) regulator can supply up to 400 mA at 3.3 V for the microcontroller, transceiver and all other peripherals. The increase in current capacity over the PICDEM Z boards allow for additional components to be added to the DFZ motherboard via the microcontroller header pins. A MRF24J40MB radio transceiver module, with PA/LNA features is implemented on a daughterboard.

Special consideration is taken in the LDO decoupling capacitors in an effort to decrease RF noise susceptibility and radiated emissions on the power supply. Using different capacitor values with different casing sizes results in a decrease of the combined capacitor impedance at higher frequencies, increasing the decoupling effect.

The PCB layout includes a two-layer design owing to increased costs for multi-layer PCBs and inclusion of ground fill in both layers to reduce radiated emissions. Zoning of functional areas serves to reduce noise coupling, and a wide power supply track is routed in a star network layout in an effort to decrease track impedance and noise coupling.

References

[1] *PICDEM Z Demonstration Kit Users Guide*, Microchip Technology Inc., Document ID: DS51524C, 2008.

[2] *PCB Design Guidelines for Reduced EMI.* Texas Instruments, 1999. [Online]. Available: http://www.ti.com/

[3] H. Ott, *Electromagnetic Compatibility Engineering.* Hoboken, New Jersey, USA: John Wiley & Sons, 2009.

[4] *PIC18F2525/2620/4525/4620 Data Sheet*, Microchip Technology Inc., Document ID: DS01146B, 2008.

[5] *MRF24J40MB Data Sheet*, Microchip Technology Inc., Document ID: DS70599B, 2009.

[6] *SANS 300328:2007/ETSI EN 300328:2006*, South African Bureau of Standards, 2007.

[7] *Linear Regulators in Portable Applications*, Maxim Integrated Products, Application Note 751, May 2001.

[8] *LM2937-2.5, LM2937-3.3 Data Sheet*, National Semiconductor Corporation, Document ID: DS100113, 2005.

[9] T. Schmitz and M. Wong, *Choosing and Using Bypass Capacitors*, Intersil Americas Inc., Application Note AN1325.0, August 2007.

[10] *Power Supply and Ground Design for a WiFi Transceiver*, Maxim Integrated Products, Application Note 3630, September 2005.

[11] C. Rostamzadeh and B. Archambeault, "Numerical and experimental investigation of PCB ground-fill on radiated EMI," in *Electromagnetic Compatibility, 2006. EMC 2006. 2006 IEEE International Symposium on*, vol. 1, 14-18 2006, pp. 79 –83.

Appendix E

Firmware and Software

E.1 Introduction

This appendix details the firmware used in implementing the ZigBee network on the DFZ devices. The firmware consists of the Microchip ZigBee stack, as well as user application code. While modifications to the ZigBee stack are prohibited by the ZigBee Alliance and Microchip, the author has contributed a custom application ZigBee profile, custom firmware for interfacing application events to the ZigBee stack, as well as a software script running on a personal computer for data logging and network control.

Section E.2 lists the features and limitations of the Microchip ZigBee stack. Section E.3 discusses the custom application profile used in the implementation of the ZigBee network. Section E.4 details the operation of the custom application firmware developed by the author. Software implemented on a personal computer for network monitoring and control is discussed in Section E.5. Section E.6 provides concluding remarks for this appendix.

The microcontroller firmware and PC software program code is included in a CD, found in an envelope on the back cover of this dissertation.

E.2 The Microchip ZigBee Stack

Microchip's ZigBee stack is free to download and use for research and prototyping purposes. Companies or manufacturers wishing to distribute a product based on

the Microchip ZigBee Stack must first become a member of the ZigBee Alliance. Features of the Microchip stack include [1]:

- Certified ZigBee-2006 compliant
- Supports 2.4 GHz band of operation
- Support for all device types: coordinator, router, end device
- Uses nonvolatile storage for group, neighbour and routing tables
- Portable across many of Microchip's PIC18 and PIC24 microcontrollers
- Supports Microchip's MPLAB C Compiler for PIC18 and PIC24 microcontrollers

There are limitations to the Microchip stack where explicit support has been neglected at the stack level in favour of developer preferences:

- Beacon-enabled networks are not supported
- Network addresses of devices which have left the network are not reassigned
- Fragmentation is not supported
- Frequency agility is not supported

The Microchip ZigBee stack operates as a *state machine*. The stack uses *switch-case* statements to check what state, or *primitive* the machine is in. Specific ZigBee networking operations such as network association requests and indications and data message requests and indications are assigned their own primitives. Such events, identified by their specific primitives, may generate subsequent primitives in the process of completing a task. The basic code structure of an application interfacing with the ZigBee stack is given in Listing E.1.

A "watchdog" timer prevents the microcontroller from stalling in the event that a process does not return the stack to regular operation in a timely manner.

Listing E.1: Basic ZigBee application code structure [1].

```
while (1)
{
    /* Clear the watch dog timer */
    CLRWDT();

    /* Process the current ZigBee Primitive */
    ZigBeeTasks( &currentPrimitive );

    /* Determine the next ZigBee Primitive to process */
    ProcessZigBeePrimitives();

    /* do any non ZigBee related tasks here */
    ProcessNONZigBeeTasks();
}
```

E.3 The Custom Application Profile

As discussed in Appendix B, ZigBee devices use an application profile made up of clusters and attributes as a way of structuring application specific data operations. For the purposes of this research a custom application profile is implemented in each device. Mechanisms for device information, temperature sensor readings and measurement readings are provided for in the custom application profile. Support for additional sensing elements may be added at the developers discretion. The following clusters and attributes are found in the custom application profile:

- Temperature sensor message cluster: containing attributes such as the reading type (single, continuous, monitor mode) and the temperature region of the current reading (high, low , normal).
- Temperature thresholds cluster: indicates to application code which threshold should be modified (high or low).
- Information cluster: activated on device association to relay device information to the coordinator.
- Test cluster: used for research purposes to manage Packet Error Rate (PER), goodput and delay measurements.

E.4 DFZ Application Operation

E.4.1 Device Functionality

The different ZigBee devices perform the following functions from an application perspective:

- Coordinator: creates and maintains the network. Logs all device association activity and sensor readings as well as test packets used in performance measurements.
- Routers: relay messages originating from other devices and also used to transmit test packets in performance testing.
- End devices: Sensing nodes, generating application specific data; also used to transmit test packets.

Power saving compile-time options enable/disable the use of serial communications and Light Emitting Diode (LED) output for each device.

E.4.2 Device Constants and Variables in Non-volatile Memory

Each device is hard-coded with a 16-bit Device Identification number to distinguish it from other devices (irrespective of the ZigBee address assigned to it during network association).

Device information such as device type and number of sensors are stored in non-volatile flash memory and can only be changed at compile-time. The sensor thresholds are stored in Electrically Erasable Programmable Read-Only Memory (EEPROM) and can be modified by sending a relevant message from the coordinator.

E.4.3 Coordinator Application Firmware

The application firmware on the DFZ coordinator device serves to relay messages from a personal computer (PC) to end devices, and vice versa. The PC is connected via a serial cable using the serial communications daughterboard. A simple message format is used to transfer data between the PC and the coordinator device. Data to

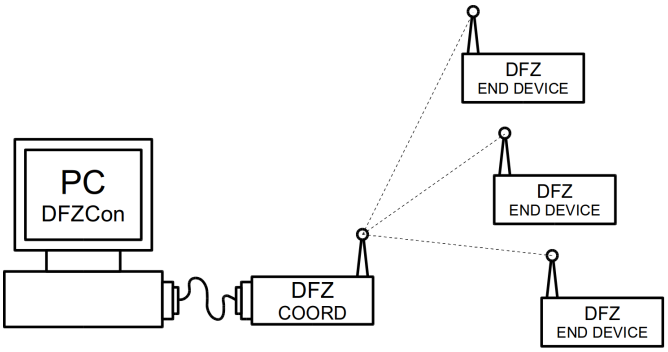


Figure E.1: Example of coordinator and end device layout, showing coordinator-PC connection.

Table E.1: Information message contents.

Data label	**Octets**	**Comment**	**Example**
Device ID	2	Unique device identification number	ABCD
Short ID	2	ZigBee short network address	796F
Device Type	1	Router or end device	02*
Num. Sensors	1	Number of sensors attached to the device	01
Parent Address	2	ZigBee short network address of parent device	0001
Parent Device Type	1	Coordinator or Router	01*

* Numeric representation, decoded in PC software; 00 = coordinator, 01 = router, 02 = end device.

be sent to the PC is preceded with an indicative text string, e.g. “SENS” for sensor readings and “INFO” for device association announcements. Data received by the coordinator is preceded with a single character value, which is decoded by a switch-case statement resulting in a call to the relevant function in the microcontroller firmware.

E.4.4 Device Information Announce

When any device (router or end device) is associated with the network it immediately sends an information message to the coordinator. The coordinator interfaces with a script running on a PC, connected via RS-232, and stores the information in a database. The data included in the information message is given in Table E.1:

E.4.5 End Device Mode of Operation

At compile-time the ZigBee end device application firmware can be programmed in one of two modes: *conversation* or *report*. In conversation mode the sleep period is short enough for the end device to reliably receive messages from the coordinator at any time. This allows for specific control over the operation of the end device at any time, but results in increased power consumption. Conversation mode support the following mechanisms:

- Single sensor reading request
- Enable/disable continuous sensor readings
- Enable/disable monitor mode sensor readings
- Set/retrieve high and low region thresholds for sensor readings
- Ping device
- Initiate Packet Error Rate and goodput measurements
- Request arbitrary single data frame (for test/measurement purposes)

In report mode the end device operates autonomously, waking up from extended periods of sleep to send messages to the coordinator. In this mode the coordinator may not reliably transmit messages to the end device as the end device may be in sleep at the time of transmission and not wake up in time to receive any retransmissions. The advantage of report mode is increased device lifetime as power consumption is decreased. The disadvantage is the lack of control from the coordinator over the end device. In report mode the end device may either send continuous sensor readings or be in monitor mode.

E.4.6 Sensor Reading Data Messages

There are three types of sensor reading:

- Single: when a single temperature sensor reading is requested by the coordinator from the end device.

Table E.2: Sensor reading message contents.

Data label	**Octets**	**Comment**	**Example**
Device ID	2	Unique device identification number	ABCD
Sensor ID	1	Unique sensor identification number	08*
Sensor Type	1	e.g. temperature, humidity, etc	02*
Reading Type	1	Single, Continuous or Monitor	01*
Sensor Reading	2	16-bit sensor reading	0001
Reading Region	1	High, low, normal	01*

* Numeric representation, decoded in PC software.

- Continuous: when temperature sensor readings are transmitted periodically by the end device.
- Monitor Mode: when temperature sensor data acquisition is performed periodically by the end device, but only transmitted if the reading falls into a "high" or "low" region, specified by threshold values.

Figure E.2 and Figure E.3 depict the continuous and monitor modes of operation respectively. Note that interval value x is either specified at compile-time for report mode, or provided in a message from the coordinator in conversation mode.

The data transmitted whenever a sensor reading is sent from an end device to the coordinator is listed in Table E.2.

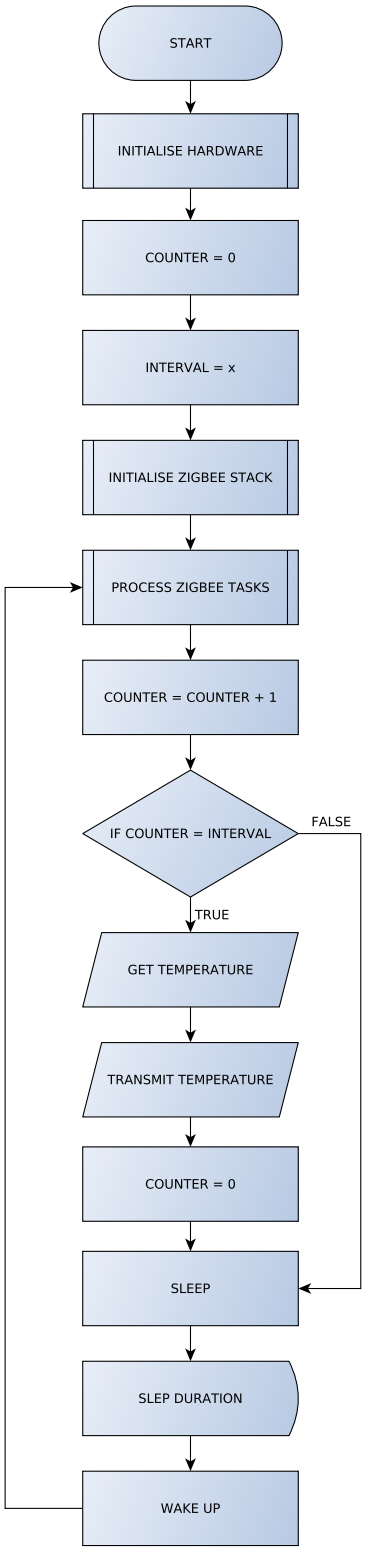


Figure E.2: Continuous transmission mode of operation.

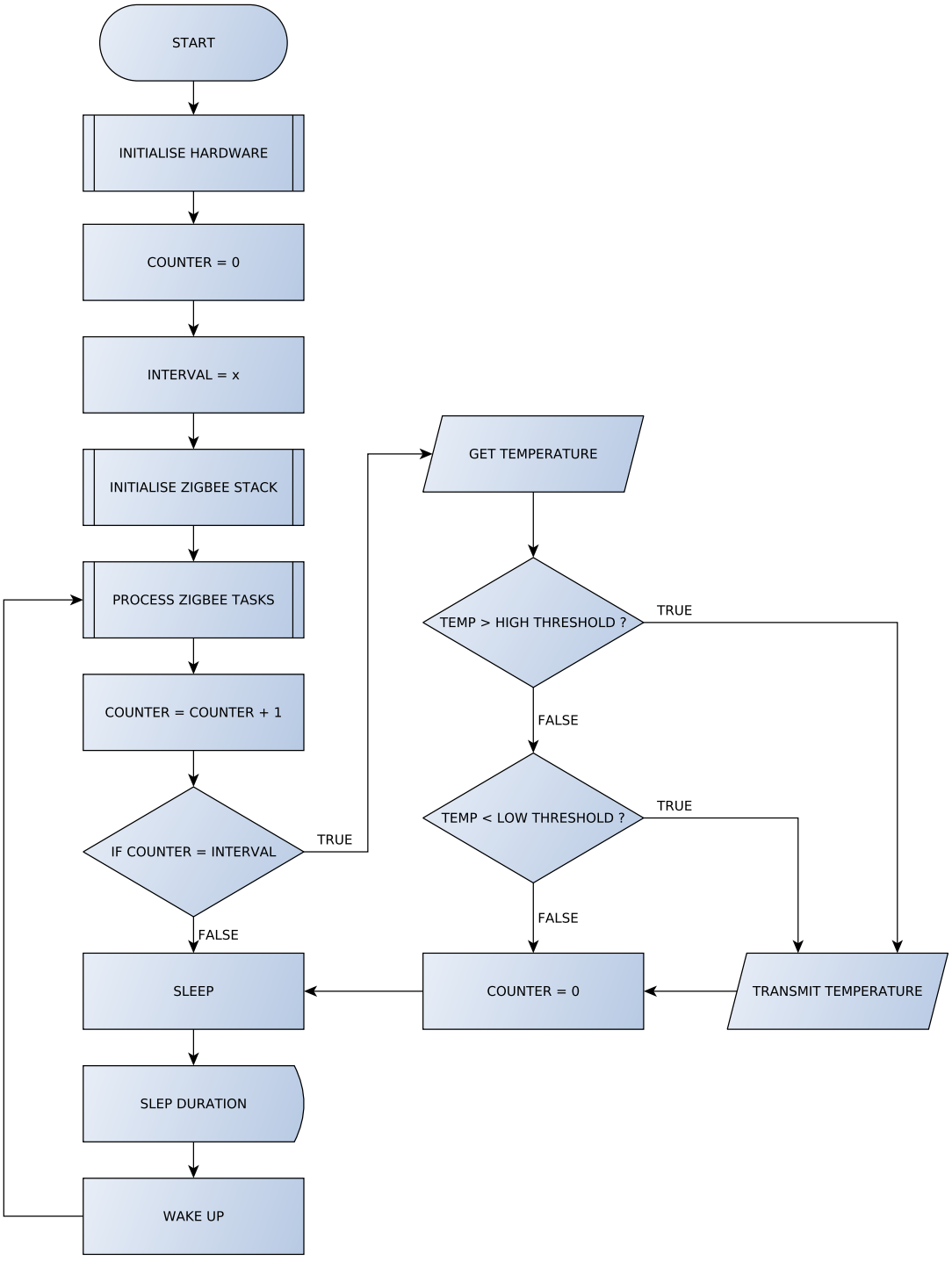


Figure E.3: Monitor mode of operation.

E.5 ZigBee Network Monitoring and Control Software

A platform-independent Python script, entitled "DFZCon", forms the basis of the software used to monitor and control the ZigBee network used in this research. The Python script is based on Chris Liechti's *miniterm.py*, an open source example application for his Python Serial Port Extension software [2]. The script polls the serial port for new data and executes relevant procedures based on identification strings preceding the data from the coordinator (see Section E.4.3). The script interfaces with a SQLite database to log device information and sensor readings. Listing E.2 depicts the events occurring after the script is initiated, featuring network creation, device announce and sensor reading request and reply actions.

The SQLite database contains the following tables:

- Device Information Table: Stores information on all devices announcing their association with the network. If a device ID has already been associated with the current network then it is not necessary to update existing details.
- Device Log Table: Stores the instances of network association regardless of prior association. This log is useful in checking for devices repeatedly re-connecting with the network.
- Sensor Reading Table: Logs all sensor readings transmitted to the coordinator.

Listing E.2: DFZCon script activity.

```
--- DFZCon on /dev/ttyUSB0: 19200,8,N,1 ---
--- Quit: Ctrl+]  |  Menu: Ctrl+T | Help: Ctrl+T followed by Ctrl+H ---
Trying to start network...

PAN 1AAA started successfully.
Joining permitted.

Node:796F With MAC Address 0000000000000001 just joined.

        INFO!  INFO:0101:796F:02:01:00:00:00:0000:00


NODE ID:          0101
NODE ADDR:        796F
NODE DEV TYPE:    RFD
NUM SENSORS:      1
PARENT ADDR:      0000
PARENT TYPE:      COORD
TIME:             2010-08-15 13:29:34


----------------------MENU----------------------
        1: List Devices
        2: Request Single Reading
        3: Request Continuous Readings
        4: Cancel Continous Readings
        5: Ping Node
        6: Get Thresholds
        7: Set High Threshold
        8: Set Low Threshold
        9: PER Test
        m: RFD Monitor mode
        n: Cancel RFD Monitor mode
        g: Goodput test
        p: PER RECVD
        c: CLEAR PER RECVD
        s: Single Packet Request
        t: Test Suite

------------------------------------------------


        2: Request Single Reading

Enter node id:
0101

Message sent successfully!

        SENS!  SENS:0101:01:01:01:36C0:02


NODE ID:          0101
SENSOR ID:        1
SENSOR TYPE:      TEMP
READING TYPE:     SINGLE
VALUE:            20 deg. C
REGION:           NORMAL
TIMESTAMP:        2010-08-15 13:46:58
```

E.6 Conclusion

The ZigBee network implemented in this research uses the Microchip ZigBee stack, which conforms to the ZigBee-2006 specification. It operates as a state machine, with unique primitives representing network operations. In addition to the stack, application specific code has been added by the author, implementing a sensor network using the ZigBee protocol. A custom application profile is used to structure the application operation and defines application specific constants for use in the firmware.

The application framework implements a device announce mechanism, reporting device information to the coordinator after network association. Three types of sensor readings are implemented: single, continuous and monitor. A compile-time option enables one of two modes of operation for an end device: conversation or report. Conversation mode allows for real-time control over end devices but features increased power consumption. Devices in report mode are typically in low power sleep mode for extended periods, waking up periodically to transmit sensor readings to the coordinator.

A Python script is implemented on a personal computer which provides network control and data logging facilities.

References

[1] D. P. Lattibeaudiere, *Microchip ZigBee-2006 Residential Stack Protocol*, Microchip Technology Inc., Application Note AN1232, document ID: DS01232A, 2008.

[2] C. Liechti, "pySerial v2.5 Documentation," last accessed 02/08/2010. [Online]. Available: http://pyserial.sourceforge.net/

Appendix F

Measurements and Results

F.1 Introduction

In this appendix the details the network performance and power consumption measurements performed on DFZ devices operating a ZigBee network are presented. Network performance is evaluated using Packet Error Rate (PER), goodput and latency measurements, and power consumption results are obtained by measuring the current drawn by the devices in different states of operation. The results of these measurements are used in characterising the DFZ devices and suggest limits for message transmission activity and device lifetime.

Many of the measurements and experiments are performed in the School of Electrical and Information Engineering's anechoic chamber in the Electromagnetics Laboratory. This limits the effects of the environment by reducing the influence of external Radio Frequency (RF) energy, as well as avoiding multipath fading effects owing to obstacles and room surfaces. Using the anechoic chamber results in limited device positioning and device-device distances, thus all distances are kept constant.

ZigBee frames may be up to 126 bytes in length, with up to 99 available to the user as the application payload. The remaining 37 bytes are used by the ZigBee Physical (PHY), Medium Access Control (MAC) and Network (NWK) layers in network overhead functions.

Section F.2 presents and discusses the PER measurements. Goodput results are discussed in Section F.3. Latency measurements are presented in Section F.4. Section F.5 details the power consumption measurements. Concluding remarks can be found in Section F.7.

F.2 Packet Error Rate Measurements

F.2.1 Overview

Packet Error Rate (PER), derived from the definition of bit error rate, is a measure of the number of failed packets as a percentage of the total number of transmitted packets, as seen by the receiving device [1]. In this context packet is synonymous with the word "message" and "frame". Changing parameters such as distance, time interval between packets and packet size will have an effect on the PER. PER measurements are used to characterise the probability of a successfully received message transmitted from one device to another. A low PER is better than a high PER.

The following assumptions and constraints apply to the PER measurements presented in this Appendix:

- All measurements are taken in the anechoic chamber.
- Distances between the devices are kept constant.
- Application payloads of 10, 50 and 99 bytes are used.
- Three sets of 1000 message transmissions are used to provide an average value for each result relative to a change in one of the parameters.
- Successful message reception is acknowledged at the Application (APL) Layer in the ZigBee stack, at the point where information within the data frame is available for application use. Success is determined by identification of the message with the correct cluster (see Appendix B).
- The devices transmitting the PER packets are ZigBee routers as they do not need to periodically check for messages from the PAN coordinator as end devices do.
- A microcontroller timer peripheral is used to generate the message transmission intervals.
- The transmitting device operates at full power (20 dBm).

Table F.1: Timer Multiples and Nominal Transmission Periods.

Timer Multiple	**Nominal Period***
1	34.6 ms
2	35.0 ms
3	37.6 ms
4	41.0 ms
5	51.0 ms
10	102.0 ms
20	204.0 ms

* Accurate to +/- 0.1 ms

- The expression used in calculating the PER from the number of successfully received packets is given in Equation F.1.

$$PER\ \% = \left(1 - \frac{P_r}{P_t}\right) \times 100 \tag{F.1}$$

P_r is the number of packets successfully received by the coordinator, and P_t is the cumulative number of packets sent by all transmitting devices.

F.2.2 Timer Interrupts and Intervals

Messages are sent at intervals which are a multiple of a 10.2 ms microcontroller timer interrupt. The exact timing of a message transmission cannot be guaranteed as the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) mechanism may introduce random delays (see Appendix A). The transmission timing for short interval, large payload messages also fluctuates as timer interrupts occur during message frame generation. Table F.1 lists the nominal transmission intervals for some timer multiples. Increasing the timer multiple will increases the chances that the transmission interval is a direct multiple of the timer interrupt, as there is less conflict between frame generation and timer interrupts. For intervals higher than four the transmission interval is a multiple of 10.2 ms. These intervals serve to expose ZigBee network performance at high data rates. A wireless sensor network implementation with focus on low power consumption should transmit messages at the maximum allowable interval based on the application.

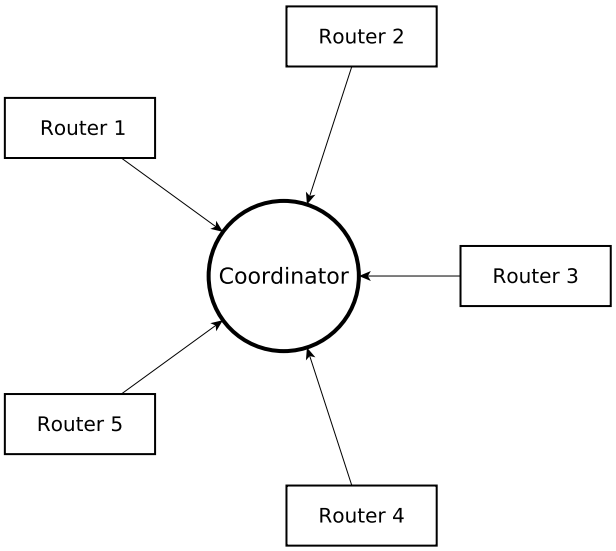


Figure F.1: Star topology for PER measurements featuring five router devices.

F.2.3 Star Network Topology

For the results presented in this section a ZigBee network is formed with all devices connecting directly to the coordinator, from one to five devices simultaneously transmitting PER test packets. Figure F.1 shows how all five router devices are connected to the coordinator in this topology. Figure F.2, Figure F.3 and Figure F.4 present the PER as a function of the number of simultaneous transmitting devices, for 10, 50 and 99 byte payloads respectively.

Increasing the number of devices simultaneously transmitting messages increases the PER. For two or less devices there is no recorded packet failures for 10 and 50 byte payloads. At maximum payload (99 bytes) failure is recorded at all instances with more than one device. The failure rate per number of transmitting devices also increases with increased payload, for a given transmission interval. The PER converges to approximately 60% for the 10 byte and 50 byte payloads, and approximately 55% for the 99 byte payload, for short transmission intervals, as the number of devices increases. This indicates that at data rates approaching maximum throughput there exists a convergent PER value as the number of transmitting devices increase.

The effect of message frame formation and channel access mechanisms at short message intervals is also apparent. At short message intervals timer interrupts are occurring while the firmware is still constructing the message frames, resulting in an

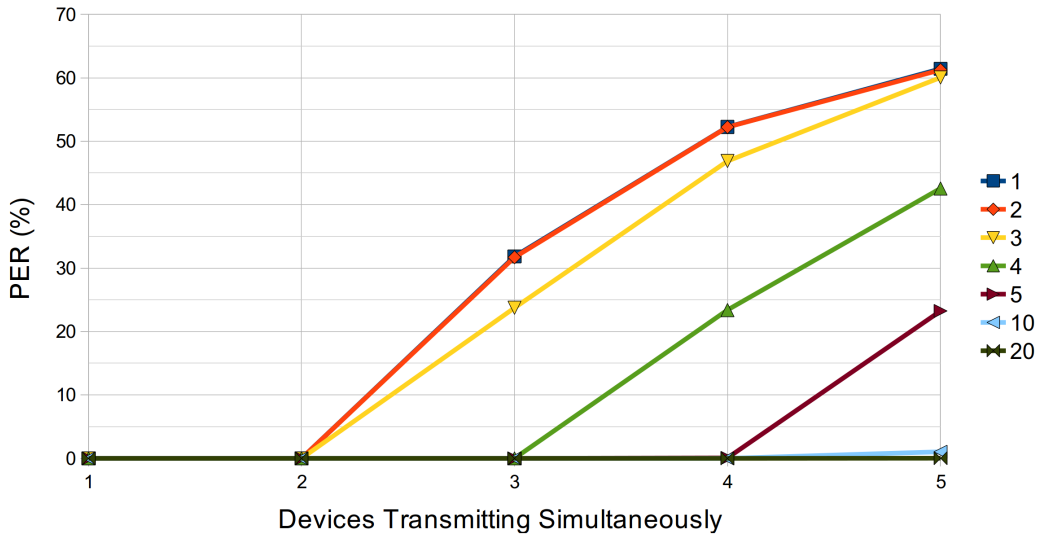


Figure F.2: PER results for star topology for a 10 byte payload. Legend indicates timer multiple value (see Table F.1).

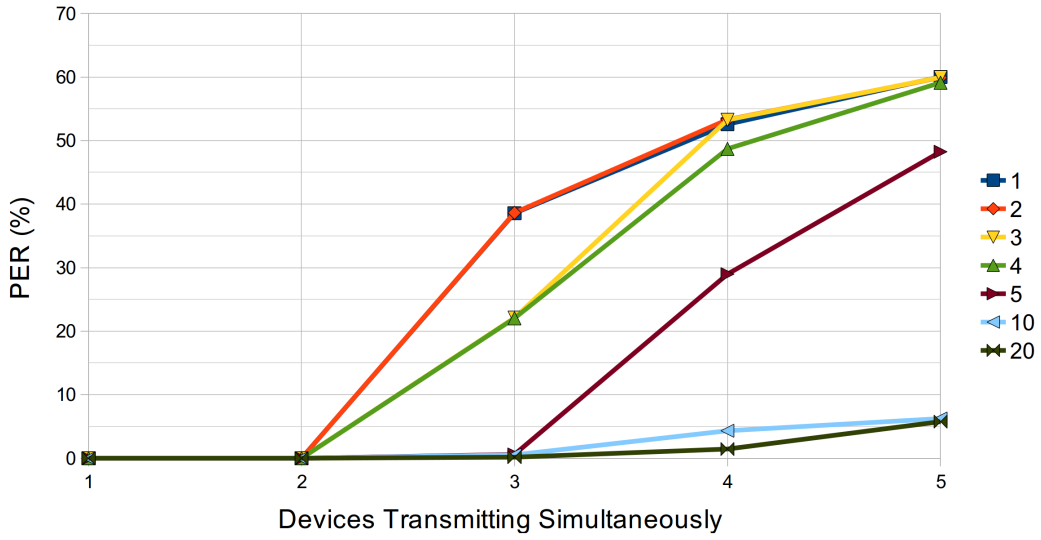


Figure F.3: PER results for star topology for a 50 byte payload. Legend indicates timer multiple value (see Table F.1).

increase in the overall interval between transmissions. This is shown in the nominal interval times associated with specific timer multiples in Table F.1, as well as how the PER rates for the two lowest intervals are similar under the same payload and device count parameters.

F.2.4 Multi-hop Network Topology

A multi-hop network is one where a message is relayed by one or more intermediate devices en route to its destination. Network devices are "daisy-chained" together to evaluate PER performance in a multi-hop topology, as shown in Figure F.5.

The timing intervals used in the PER measurements for a multi-hop network are set to much higher values than those used for the star network topology measurements, owing to the extra delay incurred each time a message frame is relayed by an intermediate device. Using shorter intervals results in frequent device disconnects, erratic device behaviour and network failure. Only one large payload of 99 bytes (the maximum permitted) is implemented in these measurements.

Figure F.6 shows the results obtained from the PER measurements in a multi-hop network topology. The PER increases as the number of hops increases above two, with shorter message intervals having higher failure rates. The average difference (over all intervals) between hop two and three is 6.1 % PER and between hop 3 and 4 it is 3.7 % PER. There is a large increase of 13.6 % in the average PER between hop 4 to hop 5. Implementing a ZigBee network on a train will most likely require multi-hop transmissions. If the coordinator (data sink) is placed in the locomotive, wagons towards the end of the train may be out of direct range and will require routers to forward messages.

F.3 Goodput Measurements and Analysis

F.3.1 Overview

Where throughput is the total number of bits transmitted or received per second, goodput is the number of *useful* bits transmitted or received per second, and excludes bits pertaining to network overhead [2]. A goodput measurement is an indication

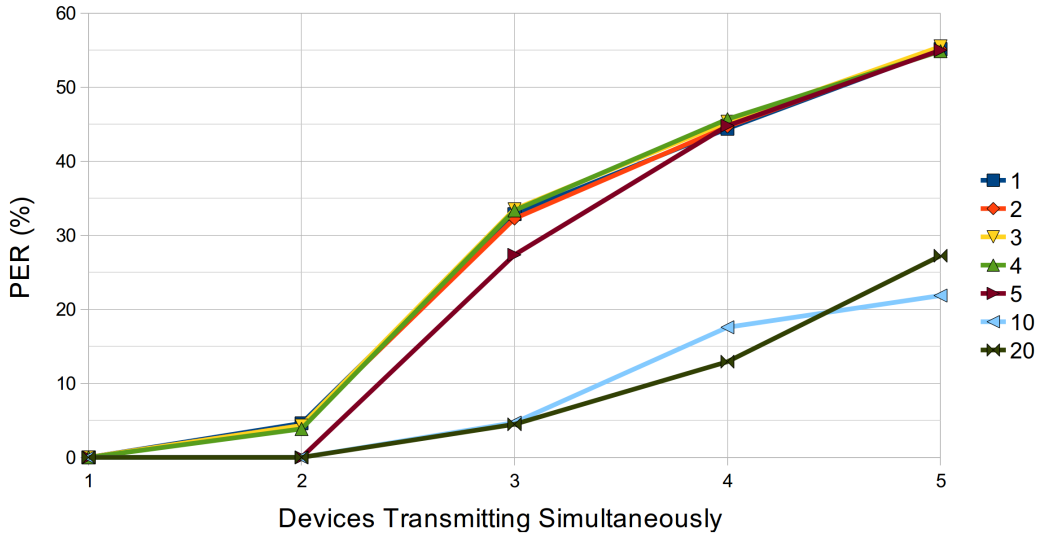


Figure F.4: PER results for star topology for a 99 byte payload. Legend indicates timer multiple value (see Table F.1).

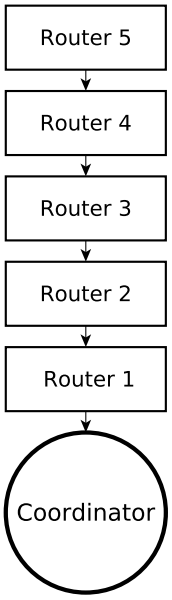


Figure F.5: Multi-hop topology for PER measurements.

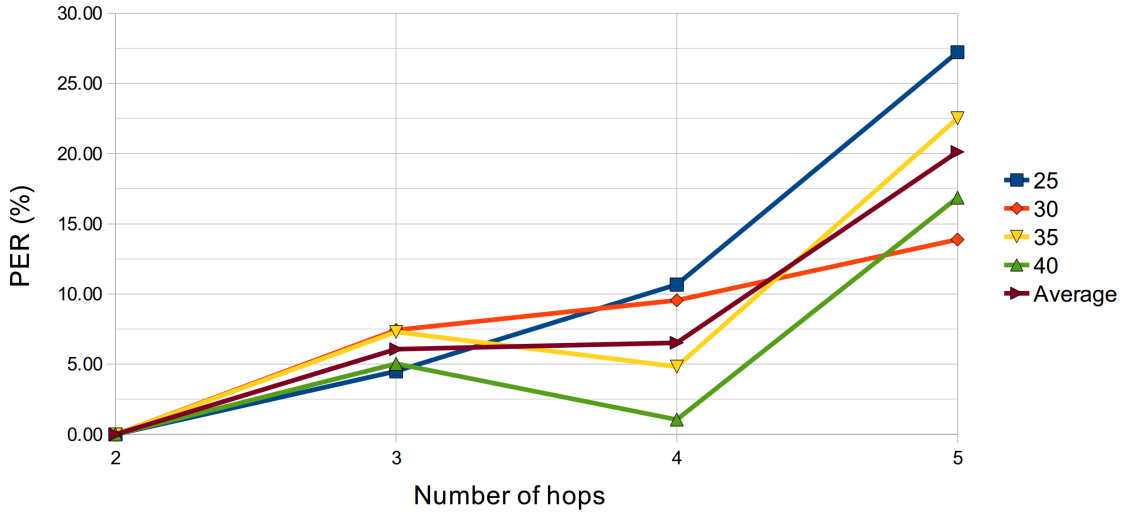


Figure F.6: PER results for a multi-hop topology for a 99 byte payload. Legend indicates timer interval value (see Table F.1).

of the useful data rate which may be achieved by the network under test. The measurements in this section conform to the following assumptions and constraints:

- All measurements are taken in the anechoic chamber.
- Distances between the devices are kept constant.
- Messages of maximum application payload (99 bytes) are used for goodput transmission frames.
- Three sets of 1000 message transmissions are used to provide an average value for each result relative to a change in one of the parameters.
- Only a star network topology is considered.
- The devices transmitting the PER packets are ZigBee routers as they do not need to periodically check for messages from the coordinator as end devices do.
- A microcontroller timer peripheral is used to generate the message transmission intervals.
- An timer interval multiplier of 1 is used to provide minimal delay between messages.

- The transmitting device operates at full power (20 dBm).
- The expression used in calculating the goodput is given in Equation F.2.

$$Goodput\ (bits/S)\ = \frac{P_r \times payload \times 8}{T_r} \tag{F.2}$$

P_r is the number of packets successfully received by the coordinator, *payload* is the number of bytes in the message payload, and T_r is time taken between, and including, reception of the first and last packets received.

F.3.2 Results and Analysis

Figure F.7 shows the results from goodput measurements in a star network featuring up to 5 devices transmitting a maximum payload of 99 bytes at the shortest possible interval. Deviation from the mean goodput value is also included. The goodput for a single device transmitting is 37.5 % lower than the mean value of 31143 bits/s ($\approx$ 31 kb/s), indicating that there is room for a higher data rate for a single transmitting device. The highest goodput data rate is 36983 bits/s ($\approx$ 37 kb/s) and is achieved with two devices transmitting simultaneously. This is 14.8 % of the maximum 250 kb/s *throughput* specified in the IEEE 802.15.4 standard for 2.4 GHz (the frequency band in which the DFZ devices operate). For three, four and five simultaneously transmitting devices the deviation from the mean is less than 7 %, suggesting an upper limit for goodput is achieved when more than two devices are transmitting simultaneously. This convergent value for goodput is lower than the highest value, indicating that some other factor decreases the rate at which the coordinator receives data from multiple devices. As multiple devices are transmitting simultaneously, contention for channel access will be more problematic, incurring delays in successful message transmission. This may account for the lower data rate experienced when more than 2 devices are simultaneously transmitting.

F.4 Message Latency Measurements

F.4.1 Overview

Message latency measurements help to characterise the time durations involved in message generation, transmission and reception within a ZigBee network. Latency

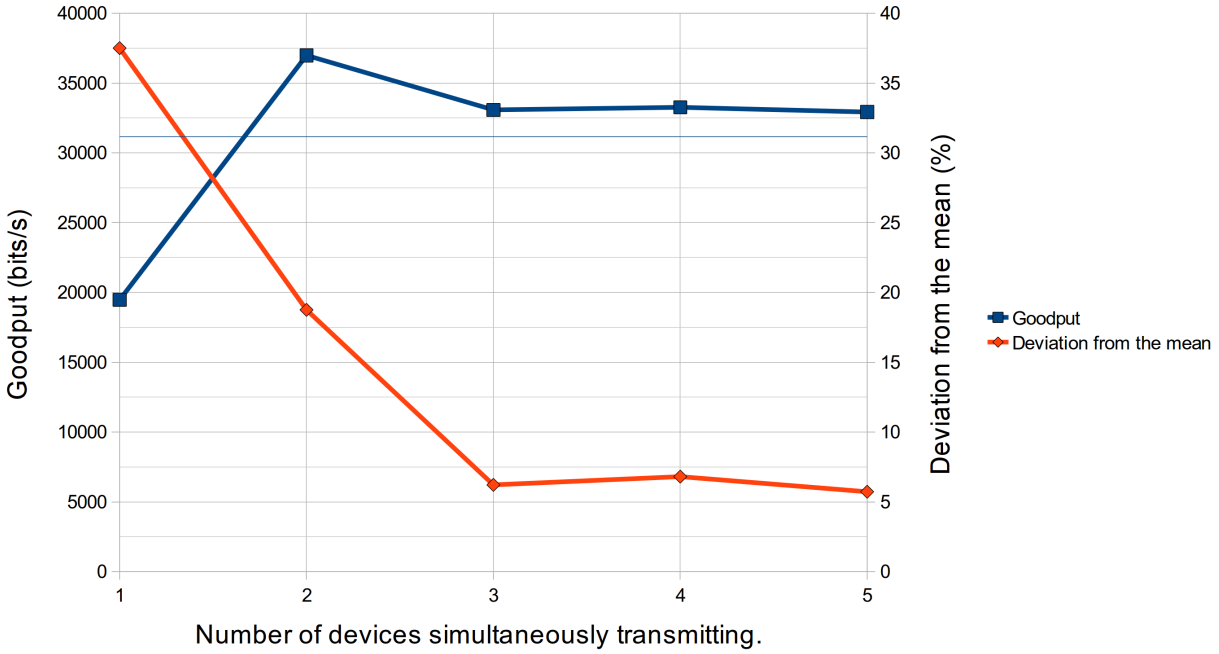


Figure F.7: Star network goodput results for a 99 payload message transmitted at timer multiple 1.

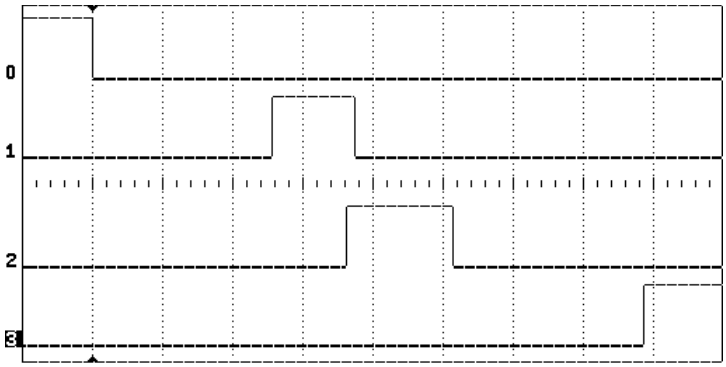
aspects of both a simple single-hop network as well as multi-hop scenarios are evaluated.

Observation of events with respect to time are performed by setting and clearing "flags" on both the transmitting and receiving device. Flags are implemented on unused microcontroller pins. Accuracy of 0.01 ms is applicable to all measurements. The logic-level measurement capabilities of an HP54645D Mixed Signal Oscilloscope are used to record the changes in the flag states.

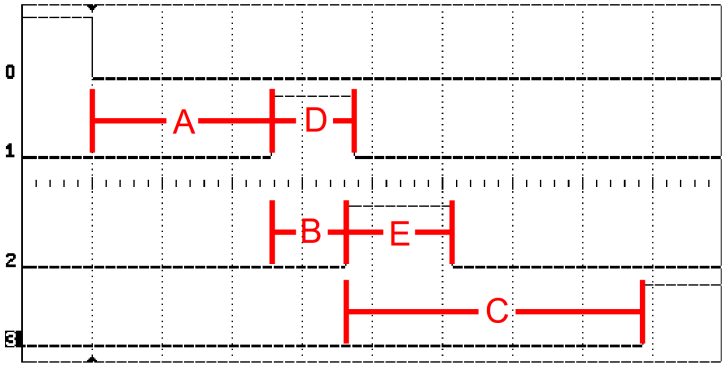
F.4.2 Single-hop Network Latency

In this scenario timing parameters of different message payloads are recorded. A single message event transmitted by Device X and received by Device Y is presented as changes in flag statuses in Figure F.8(a). Figure F.8(b) shows the same image but overlaid with information allocating certain time durations to specific events.

- A: time between event initiating message inception and generation in ZigBee



(a) Single message event.



(b) Single message event overlaid with time "zone" information.

Figure F.8: Timing zones for a single message event.

Application (APL) layer and start of message transmission from ZigBee Physical (PHY) layer, on Device X.

- B: time between start of message transmission (PHY) on Device X and generation of receive interrupt on Device Y (PHY).
- C: time between receive interrupt (PHY) and message availability in ZigBee APL Layer on Device Y.
- D: time between transmission start and transmission finished interrupt on Device X.
- E: time between receive interrupt and end of reception routine processing on Device Y.

Of most importance are periods A, B and C. Period A represents the time taken for the ZigBee APL layer to recognise an event requiring message transmission has occurred, the creation of the message frame in the APL layer and additional network

overhead data additions to the frame from the NWK and MAC layers, before finally being passed on to the PHY layer for transmission. Period B represents the time taken for responsibility of the message to pass from the transmitting device to the receiving device. Period C is the time duration including the frame reception and deconstruction routines, which must occur before it may be of use in the APL layer.

The measurements in this section conform to the following assumptions and constraints:

- All measurements are taken in the anechoic chamber.
- Distances between the devices are kept constant.
- 20 message transmissions are used to provide an average value for each result relative to a change in one of the parameters.
- Only a two device, single-hop network is implemented.

Figure F.9 shows the timing results for different payload lengths for periods A, B and C, as well as the total time taken from the beginning of period A to the end of period C. A linear relationship is evident from the results, with an average of 2.42 ms per 10 byte increase in payload size. Periods A and B experience the biggest increases in time from the smallest to the largest payload of 9.88 ms and 8.70 ms respectively, with period B experiencing a 5.12 ms increase. This indicates that the increase in payload size has a greater influence on message frame generation and deconstruction time than on the over-the-air transmission time.

Figure F.10 depicts the average times across all payload lengths for periods A, B and C as a percentage of the total time from period A to C. The majority of the time (55 %) is spent on frame processing after message reception. Message frame generation and transmission account for 31 % and 14 % respectively. This indicates that the most time-consuming tasks in a ZigBee transmission are related directly to the microcontroller's processing capabilities and not the transceivers' interaction with the physical medium: it takes longer to create and decode a packet than it does to transport it from device to device. While modifying the Microchip ZigBee stack to make it more efficient is prohibited, using a higher system clock speed may result in processing the message frame faster, resulting in less time spent on periods A and C. This would undoubtedly come at the expense of increased power consumption, as clock speed is directly proportional to supply current [3].

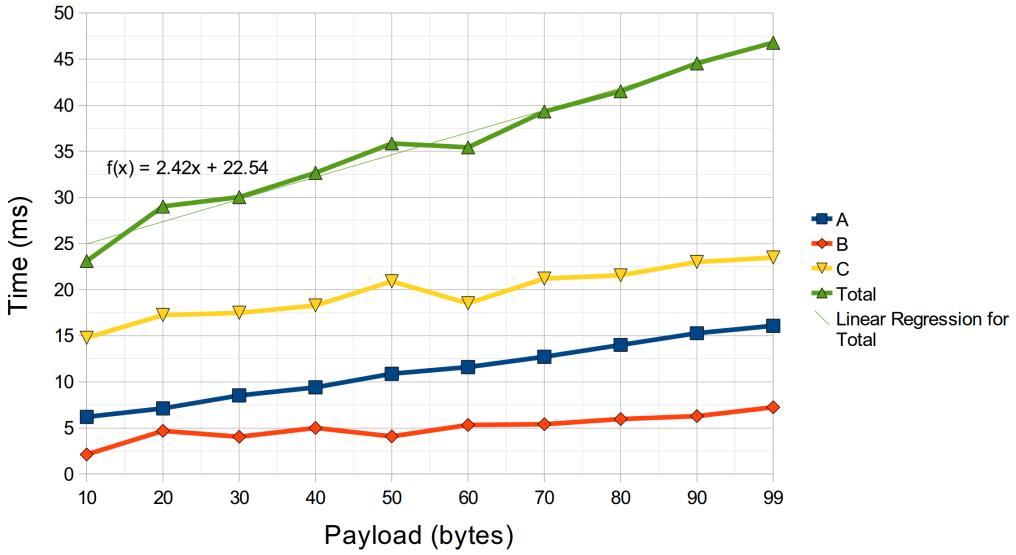


Figure F.9: Timing results for a single-hop network transmitting various payloads.

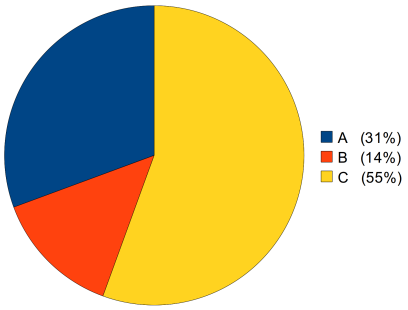


Figure F.10: Average times for periods A, B and C as a percentage of the total average time taken for a message transmission.

F.4.3 Multi-hop Network Latency

This subsection details the results and analysis made on a multi-hop network, with respect to timing delays between message inception on a transmitting device and reception on the receiving device. The following assumptions and constraints apply to these measurements:

- All measurements are taken in the anechoic chamber.
- Distances between the devices are kept constant.

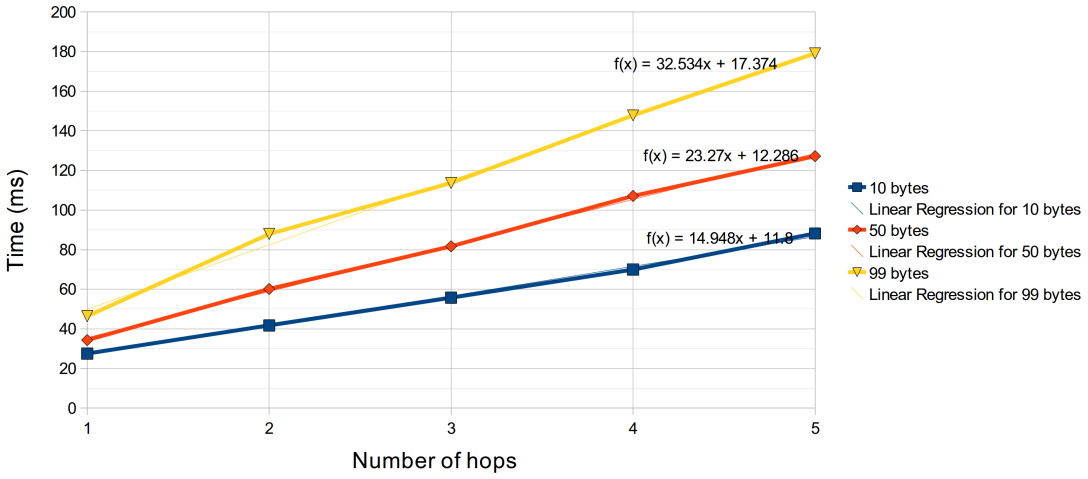


Figure F.11: Latency measurements from message inception to reception across a multi-hop network, with varying payloads. Equations refer to linear trend lines.

- 20 message transmissions are used to provide an average value for each result relative to a change in one of the parameters.
- The number of message hops varies from one to five.

Figure F.11 presents the latency results for a multi-hop network with different message payloads. For each payload size a linear trend is observed such that, in addition to the fixed time period representing message fame inception, generation and deconstruction, the delivery time for a 10 byte payload increases by 15 ms/hop, a 50 byte payload increases by 23 ms/hop and a 99 byte payload increases by 33 ms/hop. These results can be used to predict the delivery times for messages in large scale multi-hop networks with great network depth. Message latency is important when considering critical measurements related to railway wagon safety. Devices further from the coordinator (assumed to be situated in the locomotive) may require multiple transmission hops, thus increasing the end-to-end delay for successful message reception.

F.5 Power Consumption Measurements and Analysis

F.5.1 Overview

Power consumption results are important in determining the device lifetime of a wireless device, as well as the load characteristics the device presents to an energy harvesting system or power supply in general. Power consumption is evaluated in terms of the current drawn by the device under different conditions. This is done by placing a resistor in series with the voltage supply, and using an oscilloscope to measure the voltage drop across the resistor. The resistor is placed on the output of the Low Drop-Out (LDO) regulator so that the quiescent current of the regulator does not influence the results. This section details the current measurements performed on the custom ZigBee hardware implemented in this research - the DFZ devices. The measurements in this section conform to the following assumptions and constraints:

- All measurements are taken in the anechoic chamber.
- Distances between the devices are kept constant.
- An average value is calculated from multiple measurements for all values presented in this section.
- Only a two device, single-hop network is implemented.
- DFZ coordinator devices under test operate with full Light Emitting Diode (LED) and serial communications capabilities active, as would be in a real-world implementation.
- DFZ router and end devices under test operate with LED and serial communications capabilities disabled.
- For all measurements except the DFZ end device sleep current measurement, a 1% 1 Ω resistor is used to measure the current.
- For the DFZ end device sleep current measurement, a 1% 10 Ω resistor is used to measure the current.
- An HP54645D Mixed Signal Oscilloscope is used to record the voltages representing the current measurements, with an accuracy of 1.5% of full scale.

- The combination of the 1% resistor and the oscilloscope accuracy results in a maximum possible error of ±0.406 mA for all measurements except radio transmission current measurements.
- The combination of the 1% resistor and the oscilloscope accuracy results in a maximum possible error of ±1.624 mA for all radio transmission current measurements.

F.5.2 Device Current Measurements

ZigBee router and coordinator devices must be active at all times and are not intended to use a battery as a power supply. ZigBee end devices, which are intended to be wireless sensing devices, cycle from a low power sleep state to an active state. Sleep mode is disengaged by interrupt events, such as a change of state of specific microcontroller pins (external interrupts), or an internal watchdog timer interrupt. The period of the watchdog timer is the period of sleep duration provided no other "wake up" events occur. The average DFZ end device sleep current is measured to be 0.389 mA. Figure F.12 presents the current measurements for devices in one of three states: *micro only* is the current drawn by the microcontroller with the RF transceiver disabled, *RX* is the current drawn by the device when the transceiver's receiver is functioning, and *TX* is the current drawn during message transmission at maximum power. The noticeably lower current value for the coordinator in TX mode can be attributed to the relationship between the system voltage and the transmission power of the transceiver. As current is being drawn by the LEDs during transmission the coordinator device experiences a greater voltage drop across the current measurement resistor relative to the other DFZ devices. This decreases the system voltage available to the coordinator device's transceiver, to which the transmission power is proportional.

F.5.3 End Device Lifetime Estimation

End devices operating with a focus on low power consumption spend the majority of their activity in a sleep mode. They wake up as a result of the watchdog timer interrupt and transmit a message to the coordinator, checking for any pending messages. Following this activity the end device will wait for a reply. If unsuccessful, the end device will attempt to rejoin the network, or connect to any other willing ZigBee networks. If the wake up message is successful the end device will either go

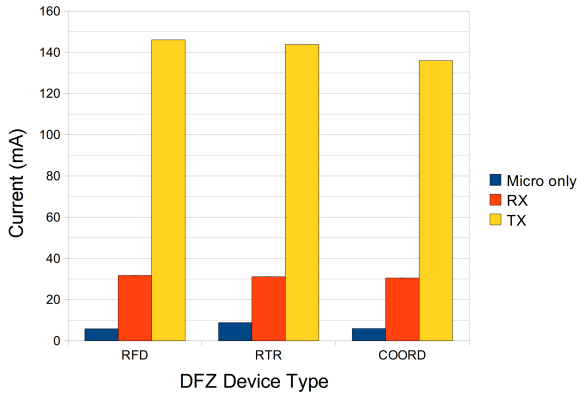


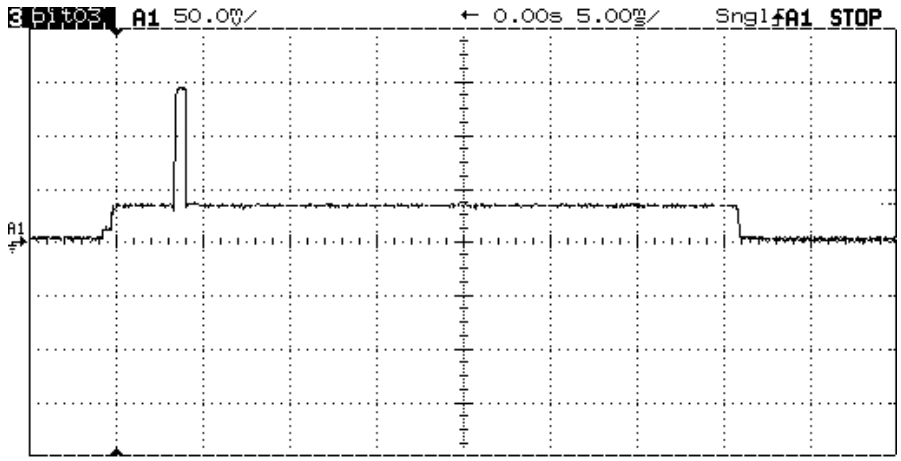
Figure F.12: Current consumption for the three DFZ devices.

back to sleep mode, or transmit any application related messages. Figure F.13(a) shows the current drawn by a device which has woken up, checked for messages with the coordinator, and gone back to sleep mode. Figure F.13(b) depicts the same operation but for two sleep/wake cycles.

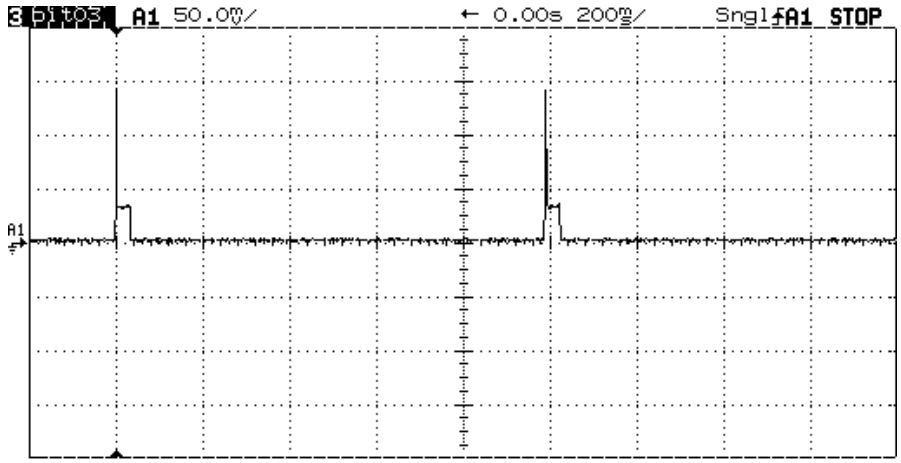
Figure F.14(a) shows the states relevant to a device just waking up to check for any pending messages ("network check"), and then returning to sleep. Figure F.14(b) shows the same states but with the addition of an application message transmission (i.e. sensor reading). The first TX current spike is associated with the network check, and the second with an application message featuring a 99 byte payload. The difference in message frame lengths between the two different message types is evident from their duration.

A power budget may be constructed from the time duration and current measurement data. Sleep duration is omitted as this is the variable which will influence power consumption the most, and is used to predict device lifetime later in this section. The influence of the LDO regulator is ignored so that the power drawn in each of the individual operational states is more distinct to the reader. Two budgets are provided: Table F.2 represents an end device waking up, performing a network check and going back to sleep (see Figure F.14(a)), and Table F.3 represents an end device waking, performing a network check, transmitting an application data message with a 99 byte payload and going back to sleep (see Figure F.14(b)). Note the different durations for TX and RX modes.

The microcontroller sleep duration is selected by a postscale value in one of microcontroller's configuration registers. The nominal watchdog timer value is 4 ms,



(a) Single sleep/wake cycle for a DFZ end device.

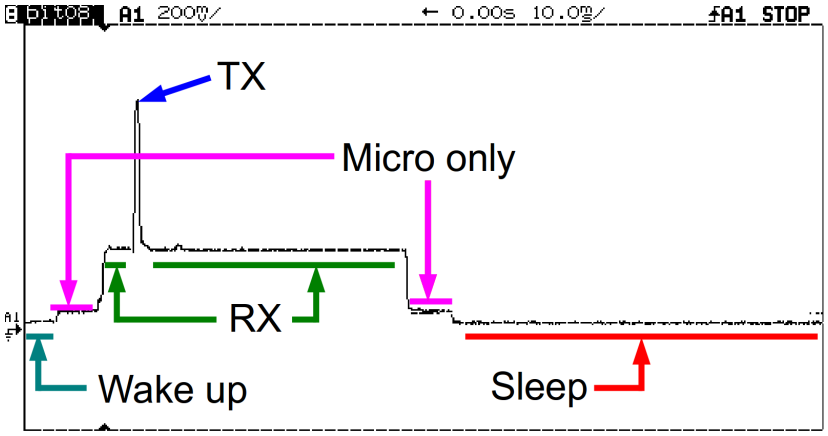


(b) Two sleep/wake cycles for a DFZ end device.

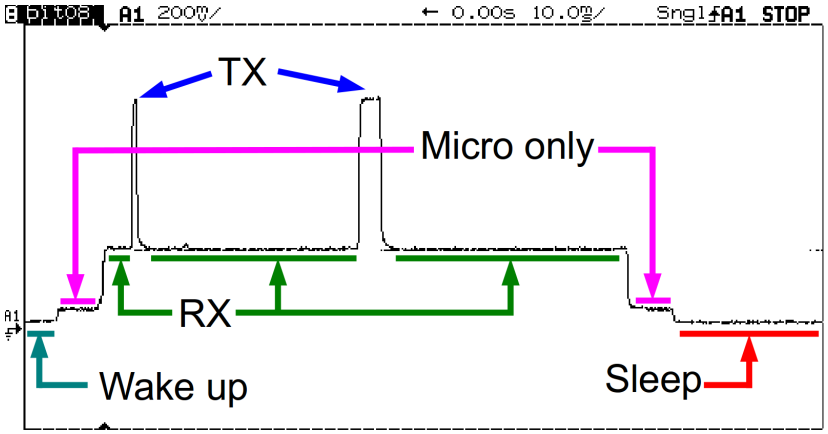
Figure F.13: Sleep/wake cycles for an end device. Note the change in the time scale for each.

Table F.2: Power budget for an end device, featuring network check only.

Mode	**Duration (ms)**	**Current (mA)**	**Charge (mAh)**
Sleep	?	0.398	?
Wake up	3.40	0.965	9.11E-07
Micro only	16.13	5.83	2.61E-05
RX	41.02	31.76	3.62E-04
TX	0.64	146.00	2.60E-05



(a) End device activity featuring wake, network check and sleep.



(b) End device activity featuring wake, network check, data message transmission and sleep.

Figure F.14: End device activity showing operational activity.

Table F.3: Power budget for an end device, featuring network check and application message transmission.

Mode	Duration (ms)	Current (mA)	Charge (mAh)
Sleep	?	0.398	?
Wake up	3.40	0.965	9.11E-07
Micro only	16.13	5.83	2.61E-05
RX	86.86	31.76	7.66E-04
TX	4.98	146.00	2.02E-04

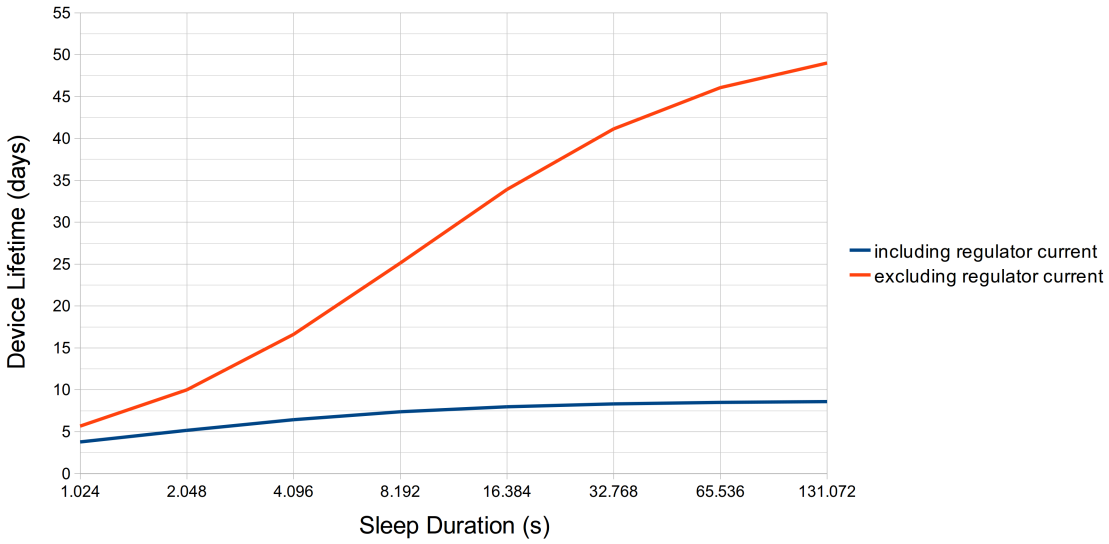


Figure F.15: Device lifetime for various sleep durations, performing a network check and message transmission.

and the postscale value may be any power of two from 2^0 (4 ms) through 2^{15} (131072 ms or 2.18 minutes). Figure F.15 depicts device lifetime for sleep durations from 1024 ms (4 ms $\times$ 2^8) to 2.18 minutes, in increments of powers of two. The following assumptions are made:

- A nine-volt PP3/6LR61 battery with a capacity of 500 mAh is used.
- The battery's self discharge rate is excluded.
- The effect of temperature on battery performance is excluded.
- A worst case scenario where the device checks the network *and* transmits a message with the maximum (99 byte) payload every wake up cycle is assumed.
- The quiescent current drawn by the LDO regulator is omitted.

Figure F.15 also presents the device lifetime for a device where the effect of the LDO regulator quiescent current is included. An additional resistor is placed in series with the input to the regulator. The average difference between current present on the input side and the current present on the output side is 2.1 mA. It is evident that the effect of the LDO regulator quiescent current is considerable, with a decrease in device lifetime from 49 days to 8 days for the greatest sleep duration. It is recommended that an alternative linear low drop-out regulator is chosen, with

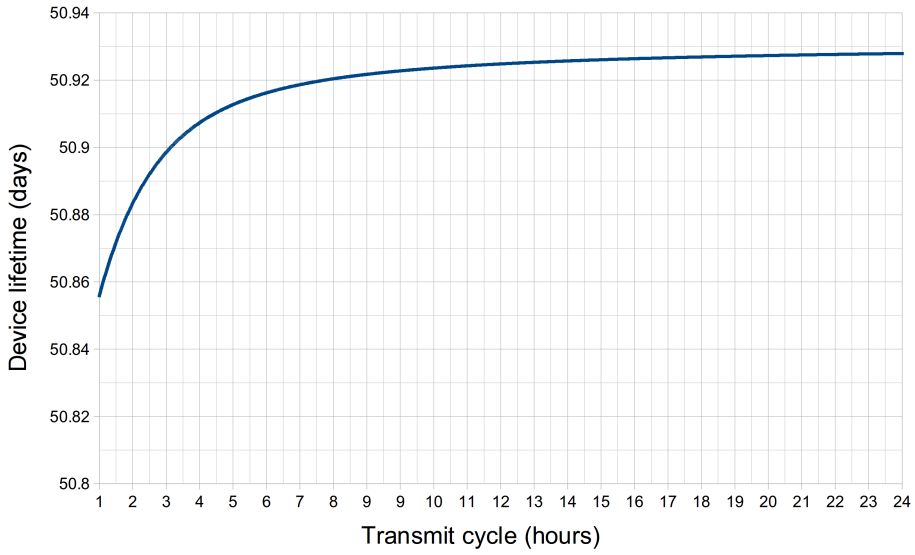


Figure F.16: Device lifetime for various transmit cycles, performing many network checks and one message transmission for the cycle duration specified.

sufficient load current capacity for additional electronics. Substituting the National Semiconductor LM2937 regulator with a Maxim MAX882 will reduce the maximum quiescent current from 10 mA to 15 μA for the same operating conditions [4]. Using Table F.2 it can be seen that the maximum measured current is 146 mA (during message transmission). The MAX882 is able to supply 200 mA of current, thus able to supply additional current for added electronics whilst still allowing for maximum transmission power. Implementing a lower quiescent current will increase device lifetime, and thus decrease the frequency with which batteries need be replaced - an important consideration when considering massive device deployment (i.e. a wireless network operating on railway wagons).

Figure F.16 predicts the device lifetime for extended transmit cycles. The effect of LDO regulator quiescent current is omitted. As the maximum sleep duration is 2.18 minutes, the prediction is calculated by fitting as many network check cycles plus one check-and-transmit cycle in the duration specified with all cycles observing a maximum sleep period of 2.18 minutes. For example, 26 network check cycles and one check-and-transmit cycle amount to a total duration of 59 minutes or approximately one hour. The effect of the current drawn by the transmit cycle is minimal compared to the effect of the sleep duration. The device lifetime is extended by only 0.072 days (4.32 hours) when changing the transmission of an application message every hour to a transmission every 24 hours.

It is recommended that a different battery technology is chosen for use in a railway wagon network implementation. Lithium-ion batteries offer better cold temperature performance and energy density when compared with the alkaline PP3 battery used in these measurements [5]. Battery performance at colder temperatures is important in railway wagon network implementations. A train spends the majority of its lifetime idle, in depots or stations. While a moving train generates heat, a stationary train does not. The effect of temperature during the winter months will also be of concern. The higher energy density offered by a lithium-ion battery means that higher battery capacity is available for the same cell size. Increased capacity results in increased lifetime. Lithium-ion technology also allows for rechargeable batteries. Energy harvesting technology can then be used to charge the batteries, extending the lifetime of the device. Various methods of energy harvesting exist, such as thermal, solar, piezo-electric and electromagnetic methods [6].

F.6 Improving Results with Antenna Diversity

Multipath interference occurs when electromagnetic waves transmitted from a single device reflect off various obstacles, presenting the receiving device with multiple signals, differing in phase and amplitude. Destructive interference occurs when signals arrive out of phase, and may result in decreased throughput and increased error rates, requiring multiple re-transmissions to achieve successful message reception. A solution to multipath fading exists in the implementation of antenna diversity. This is achieved by using a single RF transceiver coupled to two multiple antennas. In the simplest case, two antennas are physically separated by a distance based on the carrier wavelength. This results in one antenna being exposed to constructive interference whilst the other is experiencing destructive interference. Switching between the antennas is done using a high speed RF switch. Antenna selection is typically based on the RSSI value observed by each antenna during the the preamble of a packet transmission. The antenna which detects the higher RSSI value is then chosen to receive the remainder of the message. [7] [8]

Implementing antenna diversity on the DFZ devices will require replacement of the MRF24J40MB transceiver module with a custom RF subsystem, consisting of a transceiver, power amplifier, low-noise amplifier, RF switch and multiple antenna interfaces.

In the context of a ZigBee wireless network on a train, various reflective surfaces

exist in the metal surfaces of the wagons, in addition to the surfaces present in the landscape through which the train is moving. This is certainly a more "reflective" environment than that provided by the anechoic chamber in which the performance measurements were taken.

F.7 Conclusion

Packet Error Rate, goodput, latency and power consumption measurements help to characterise the performance of a ZigBee wireless sensor network based on the DFZ devices implemented in this research.

Packet Error Rate (PER) results for a ZigBee network featuring a star topology show that the PER increases as the number of devices simultaneously transmitting increases. For short message intervals across all payload sizes the PER converges to between 54% and 62%, indicating throughput saturation for multiple devices transmitting at such intervals. In a multi-hop network the PER increases as the number of hops increase above two, with shorter message intervals exhibiting higher failure rates.

The highest goodput result recorded exists for two simultaneously transmitting devices, at 37 kbps. This is 14.8 % of the theoretical maximum of 250 kb/s stated in the IEEE 802.15.4 standard. A convergent value exists with the inclusion of additional transmitting devices in a star topology: when three, four and five devices are simultaneously transmitting the goodput deviation from the mean value is less than 8%. The higher goodput value for two transmitting devices relative to three, four and five transmitting devices can be attributed to channel access contention, and the delays introduced by the Carrier Sense Multiple Access with Collision Avoidance mechanism.

Message latency results show that for a two-device single-hop network there exists a linear relationship between the payload size and the time between message inception and reception in the Application layers of the ZigBee stack on the two devices. The observed trend indicates a 2.42 ms increase in latency for every 10 byte increase in the payload. The increase in payload size influences the message frame generation, construction and deconstruction times more than it influences the actual over-the-air transmission time. The most time-consuming tasks in a ZigBee data message transmission are those related to packet generation and deconstruction, indicating

that an increase in microcontroller clock speed may decrease latency. Latency results for a multi-hop network show a linear relationship between the end-to-end delay and the number of hops, with an increase of 15 ms per hop for a 10 byte payload, 23 ms for a 50 byte payload and 33 ms for a 99 byte payload.

Power consumption measurements have resulted in device lifetime predictions for a 9 V, 500 mAh capacity, battery. A device transmitting a maximum payload at maximum sleep duration intervals is expected to last 49 days, disregarding the effect of the Low Drop-Out (LDO) regulator quiescent current. Including the effect of the LDO regulator current the battery lifetime decreases considerably, from 49 days to 8 days at the maximum sleep interval. Sleep duration has a greater effect on power conservation than does the current drawn during message transmission. It is recommended that an alternative LDO regulator with a lower quiescent current is chosen, and that a lithium-ion battery technology is adopted for use in a railway wagon wireless network implementation. These changes will increase device lifetime, thus decreasing the frequency of battery replacement.

It is recommended that antenna diversity be implemented to mitigate multipath interference from reflective surfaces, which will help decrease error rates and increase throughput.

References

[1] H. Newton, *Telecom Dictionary: Telecommunications, Networking, Information Technologies, the Internet, Wired, Wireless, Satellites and Fiber.* New York, New York, USA: Flatiron Books, 2009.

[2] S. Farahani, *ZigBee Wireless Networks and Transceivers.* Newton, MA, USA: Newnes, 2008.

[3] *Compiled Tips N Tricks Guide*, Microchip Technology Inc., Document ID: DS39626E, 2009.

[4] *MAX882/MAX883/MAX884 Data Sheet*, Maxim Integrated Products, Document ID: 19-0275, July 2009.

[5] T. R. Crompton, *Battery Reference Book*, 3rd ed. Oxford, United Kingdom: Newnes, 2000.

[6] C. Mathna, T. ODonnella, R. V. Martinez-Catalaa, J. Rohana, and B. OFlynn, "Energy Scavenging for Long-term Deployable Wireless Sensor Networks," *Talanta*, vol. 75, no. 3, pp. 613–623, 2008.

[7] *AT86RF231 Antenna Diversity*, Atmel Corporation, Application Note AVR2021, 2008.

[8] M. Burns and T. Starr, *Implementing Diversity Using Low Power Radios*, Texas Instruments, Application Note AN085, 2010.

Appendix G

Wireless Sensor Network Field Test

G.1 Introduction

Where further research may implement the DFZ devices on railway wagons, the field test discussed in this Appendix demonstrates a "proof of concept" for the custom ZigBee platform. A ZigBee network is established, end devices are associated to the network and temperature measurements are logged for later analysis. This simple test serves to prove the functionality of the DFZ platform, incorporating the hardware and software features developed by the author. Section G.2 provides an overview of how the test was conducted. Results and analysis of the data is found in Section G.3. Concluding remarks are found in Section G.4.

G.2 Overview

A Microchip TC1047 temperature sensor with an analogue output is used as the sensor component. It operates at 3.3 V and is able to measure temperatures from $-40°C$ to $+125°C$ with an accuracy of $\pm 2°C$ and a low supply current of 35 μA [1]. A 9 V 6LR61 battery is used as a power supply for the end devices, and an AC-DC converter is used to supply power to the coordinator from a mains outlet.

The end devices are programmed at compile time to operate in "report" mode (see Appendix E), with a sleep/transmit cycle duration of 65.5 s. Some of the batteries are not new and have been used previously in an effort to observe what happens when there is insufficient power to support the devices.

The coordinator node is connected to a PC running the DFZCon script (see Appendix E). The DFZCon script logs all sensor transmissions and successful network joins.

The coordinator device and five end devices are scattered around three rooms occupied by postgraduate students of the School of Electrical and Information Engineering. Figure G.1 shows the layout of the rooms, and the placement of the end devices.

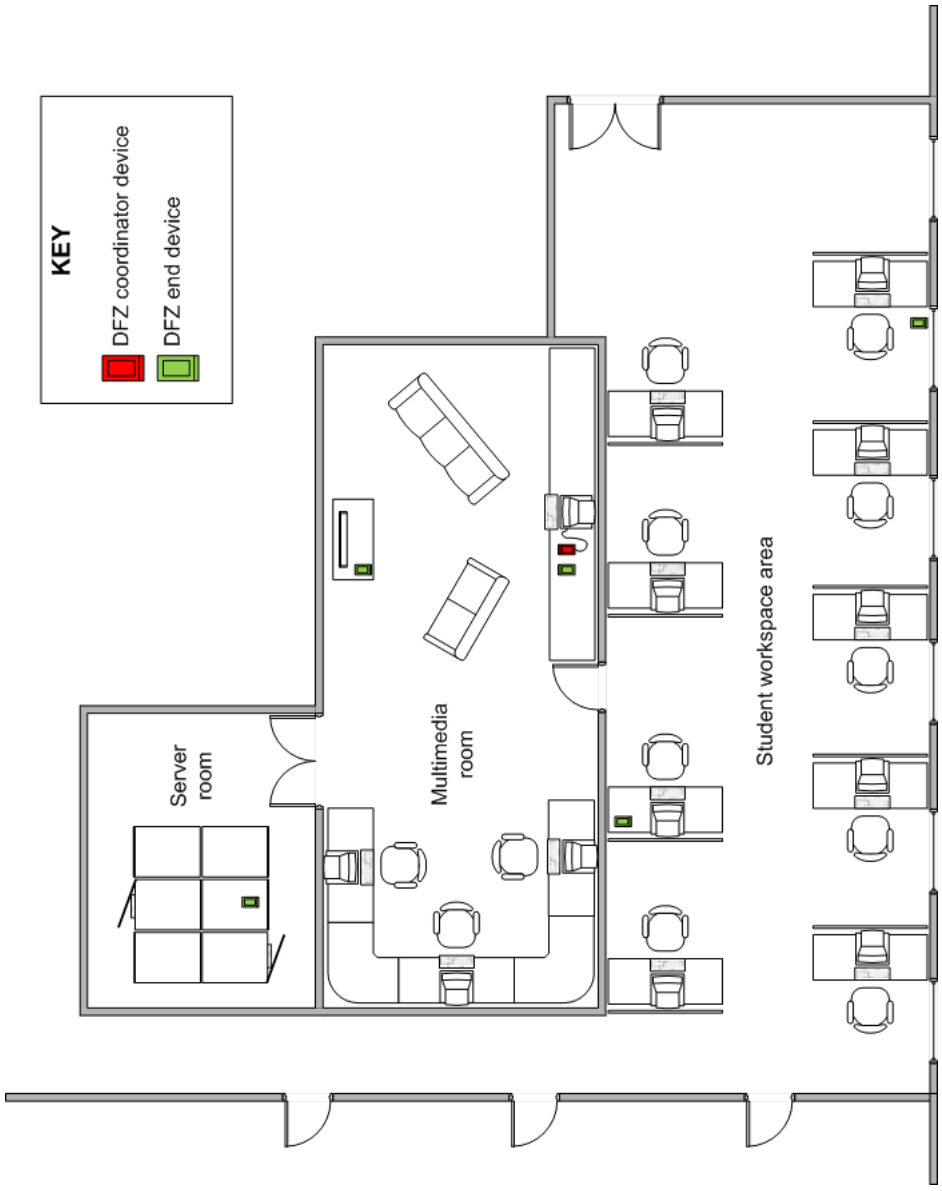


Figure G.1: Field test device layout.

Table G.1: Device network association log.

Device ID	Timestamp
A	2010-08-05 17:49:01
B	2010-08-05 17:49:11
C	2010-08-05 17:49:45
D	2010-08-05 17:50:25
E	2010-08-05 17:50:57
A	2010-08-10 21:19:50
A	2010-08-10 22:07:15

G.3 Results and Analysis

Figure G.2 presents the results obtained by the DFZ ZigBee devices. The device association log is given in Table G.1. Devices B, C, D and E remained associated with the coordinator for the duration of their lifetime. Device A connected to the network on three occasions, implying it twice experienced a loss in connection upon wakeup from sleep. The last two connections occur toward the end of the device's lifetime, where a failing power supply may have contributed to the network disconnection events.

Power supply failure on all devices is indicated by an increase in recorded temperature, continuing until loss of data transmission. This is evident in device E where a steady increase in temperature on 9 August contrasts that recorded by devices C and D. This behaviour suggests that the status of the power supply is an important parameter in determining the validity of sensor results. The device with the longest lifetime was device C, which transmitted for messages 5 days and 16 hours. Device C's lifetime is 71 % of the expected 8 days suggested in Figure F.15, for a sleep duration of 65.5 s. It is assumed that the batteries used in the field test exhibit a lower capacity than that of 500 mAh, the value used in the device lifetime prediction given in Figure F.15. The capacity of the batteries used in the field test are not published. The effect of temperature on battery performance is also excluded in the predictions given in Figure F.15 and may contribute to the lower lifetime result.

Devices A and E were in the same room, and exhibit similar results. Each device recorded a 3°C difference in maximum and minimum recorded values, before ex-

hibiting erratic behaviour associated with insufficient power supply. Device A was placed on a cabinet which encloses a television satellite decoder, various gaming consoles and other multimedia equipment. The heat generated by these devices is evident in the slightly higher average temperature.

Device B was placed in the laboratory server room and recorded the lowest average temperature. The thermostat action of the server room air conditioning is evident from the continuous high-low cycles.

Device D is placed on a ledge on the inner side of an outside-facing window. Its proximity with the outside surface of the building, and the poor thermal insulation offered by a single glass windowpane is evident in the large change in temperature experienced over a day/night cycle. The first three days exhibit a maximum change of 10°C. The fourth and fifth days (9 and 10 August) are marked by a drop in temperature down to 7°C, and then a steady increase until power supply failure.

Device C is just 30 cm closer to the building's outer wall than device E, however device E has an additional wall between itself and the building exterior. The loss of the extended insulation offered by an additional wall (as experienced by device E), is evident in device C's drop in recorded temperature on the night of 9 August relative to the temperatures recorded by device E. Device C's drop in recorded temperature on 9 August is supported by the drop in recorded temperature experience by device D at the same time.

These results show that the current configuration of the power supply is impractical for use in devices on railway wagons. As indicated in Appendix F, it is recommended that a lithium-ion battery technology and an alternative linear low drop-out regulator be used. The higher energy density and improved low temperature performance of a lithium-ion battery will extend the battery's useful lifetime. An alternative linear regulator with a lower quiescent current will result in lower power consumption over time, extending the device lifetime.

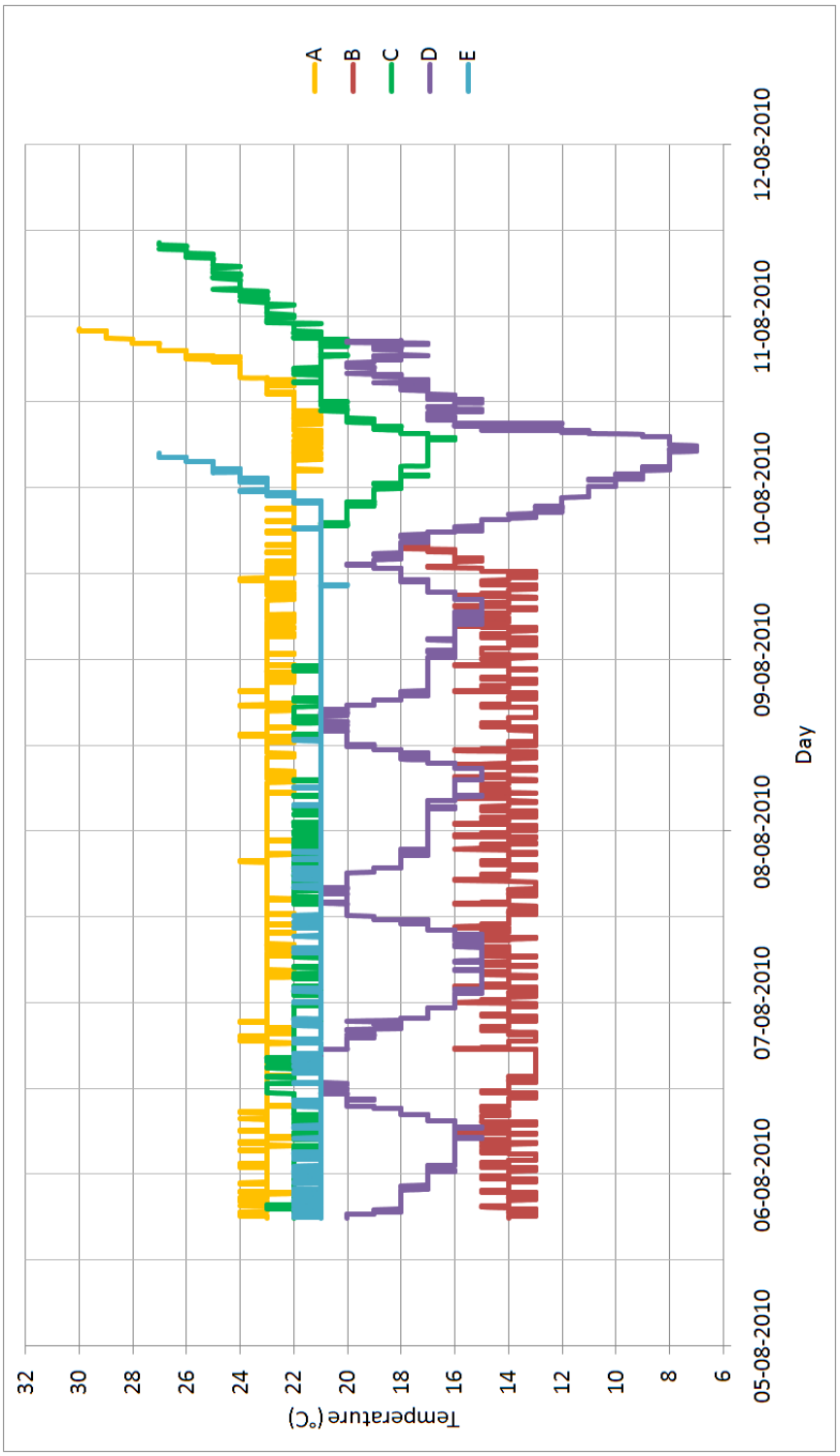


Figure G.2: Field test results.

G.4 Conclusion

A simple field test is demonstrated by the temperatures recorded from five DFZ ZigBee devices in three distinct rooms, a server room, a multimedia room and an office workspace. The results exhibit the usefulness and functionality of the DFZ platform in its data logging capabilities.

With respect to the actual temperature results, close proximity to a building's exterior surface and the poor insulation offered by a single glass windowpane makes for lower localised temperatures than devices in positions further away from the exterior surface. Susceptibility to lower temperatures is also decreased as the number of insulating surfaces (walls) increase between recording device and the exterior wall.

Validating temperature measurements requires monitoring of the power supply, as a failing power supply influences sensor measurements whilst successful radio transmission is still possible. The longest recorded device lifetime of 5 days and 16 hours is 71 % of the expected 8 days from the device lifetime expected from results in Section F.5.3. This can be attributed to a lower battery capacity used in the field test when compared to that chosen for the prediction, as well as the effect of temperature on battery performance. It is recommended that further implementations of the DFZ devices make use of a lithium-ion battery technology, as well as the use of an alternative linear regulator with a lower quiescent current.

References

[1] *TC1047/TC1047A Data Sheet*, Microchip Technology Inc., Document ID: DS21498C, 2005.