Km-scale Industrial Networking

Jonathan Mauricio Muñoz Soto

Thesis

of the

École Doctorale Informatique, Télécommunications
et Électronique (Paris)

km-scale Industrial Networking

presented by

Jonathan Mauricio MUÑOZ SOTO

A dissertation submitted in partial satisfaction of the
requirements for the degree of

Doctor of Philosophy

in

Computer Science

at the

Université Pierre et Marie Curie

Presented on 29 March 2019.

Jury:

André-Luc Beylot	ENSEEIHT, Toulouse, France	Reviewer
Nadjib Achir	Paris 13 (L2Ti), Paris, France	Reviewer
Aline Carneiro Viana	Inria, Saclay, France	Examiner
Ken Chen	Paris 13 (L2Ti), Paris, France	Examiner
Paul Muhlethaler	Inria, Paris, France	PhD Adviser
Thomas Watteyne	Inria, Paris, France	PhD co-Adviser

Contents

Acronyms

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
6P	6top Protocol
6top	6TiSCH Operation Sublayer
6TiSCH	IPv6 over TSCH
ACK	Acknowledgement (frame)
ASN	Absolute Slot Number
CoAP	Constrained Application Protocol
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA)
DODAG	Destination-Oriented Directed Acyclic Graph
ETSI	European Telecommunications Standards Institute
FDMA	Frequency-Division Multiple Access
FSK	Frequeny shift-keying
FSPL	Free Space Path Loss
HART	Highway Addressable Remote Transducer
HVAC	Heating, Ventilation and Air Conditioning
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IoT	Internet of Things
IPv6	Internet Protocol version 6
JSON	JavaScript Object Notation
KPI	Key Performance Indicators
LLN	Low-power and Lossy Network
LoS	Line Of Sight

MAC	Medium Access Control
MCS	Modulation and Coding Scheme
MTU	Maximum Transmission Unit
M2M	Machine-to-Machine
O-QPSK	Offset quadrature phase-shift keying
OFDM	Orthogonal frequency division multiplexing
OSI	Open Systems Interconnection
PDR	Packet Delivery Ratio
PHY	Physical layer
ppm	parts per million
QoS	Quality of Service
RFC	Request For Comments
RPL	Routing Protocol for Low-Power and Lossy Networks
SCADA	Supervisor Control And Data Acquisition
SF	Scheduling Function
TDMA	Time Division Multiple Access
TSCH	Time Slotted Channel Hopping
TSMP	Time Synchronized Mesh Protocol
UDP	User Datagram Protocol
WSN	Wireless Sensor Networks

Acknowledgements

This thesis work was made possible thanks to the National Institute of Research in Computing and Automation (Inria), the Doctoral School of the University Pierre et Marie Curie (UPMC) in Paris and start-up company Gridbee Communications.

I thank Prof. Andre-Luc Beylot from the ENSEEIHT and Dr. Nadjib Achir, Assistant Professor at University of Paris 13 for having accepted to review my thesis.

I thank Dr. Aline Carneiro Viana, Researcher at Inria and Prof. Ken Chen from the University of Paris 13 for serving as examiners of my thesis.

I am profoundly thankful to my advisor Thomas Watteyne for his indefatigable support, encouragement and expert eye throughout the past three years we have worked together.

I thank my advisor Paul Muhlethaler for his advice and suggestions through this work.

I thank Dr. Xavier Vilajosana, Professor at the Open University of Catalunya (UOC), for the inspiring discussions and advice.

I thank Dr. Tengfei Chang, Dr. Keoma Brun-Laguna, Mr. Yasuyuki Tanaka, Dr. Remy Leone and Dr. Malisa Vucinic for their support and inspiring ideas.

I thank the team at Gridbee Communications for the great working environment.

Chapter 1

Introduction

1.1 The Internet of Things

The Internet of Things (IoT) provides connectivity to otherwise unconnected devices. The IoT is a vast domain, encompassing a myriad of protocols and applications that run over a plethora of different devices.

The authorship of the term *Internet of Things* is given to Kevin Ashton who used it, while working for Procter & Gamble, to explain the idea of connecting the company's supply chain to the Internet [1]. Eventually, the definition was made wider to include connecting sensors with computer so those could gather information without human intervention.

Today, there are numerous IoT applications, from connected tennis rackets to the Industry 4.0.

1.2 Wireless Sensor Networks

Typical wireless low-power mesh networks are composed of tiny, inexpensive, low-power devices featuring a micro-controller, a radio and physical sensors bundled onto a single printed circuit board. These devices, called "motes" or "nodes", self-configure to establish a network without requiring any dedicated infrastructure. The characteristics of these nodes are: limited computational capacities and memory, low power consumption, lossy communication and low data rate radio interface.

The reduced size of these computers, sensors/actuators and radio chips at an affordable price[1] open the possibility to new applications. Due to their low cost, sensor nodes can be deployed in large number and offer a finer-grained visibility over the process they are observing. Nodes can be deployed outside of the wireless communication range of the data collecting node, often called "sink", "gateway", "access point", or "root". In this case,

[1] It is commonplace to find micro-controllers with radio chips embedded for less that 5 USD.

nodes organize as a multi-hop mesh network: a message sent by node far from the root, "hops" from mote to mote, each mote potentially playing the role of relay.

Due to the unreliable nature of wireless, links regularly appear and disappear, even without movement of nodes. Therefore, the network must be self-healing, adapting the multi-hop routing paths to the changing connectivity.

Even if this wireless environment is lossy, wire-like reliability can be achieved. Techniques, such as channel hopping, introduce determinism into the network, achieving wire-like end-to-end reliability in a network made up of unreliable links. Chapter 2 surveys these techniques. Tens of thousands of such mesh networks operate today, including in the most critical applications.

In the last 5 years, we have seen a trend to use longer range technologies, in which motes can be separated by multiple km. Popular technology in the "Low Power Wide-Area Networking" (LPWAN) space are LoRa and Sigfox (see Chapter 2). Today's LPWAN technology uses simple "star" topologies: the nodes in the network send their frames directly to the gateway of the network. This has the advantage of being very simple: motes can be off most of the time, and turn on their radio just to transmit their data to a gateway that is always listening. The disadvantage is that, when starting to roll these networks out, there are always a number of nodes that are out of range of the gateway. The very resource-intensive solution that is used today is to conduct a site survey and install additional gateways. Yet, this is not satisfactory as it is labor-intensive, costly as new gateways need to be mains powered and connected to the Internet, not permanent as the connectivity will change again, and sometimes simply not possible. The resuls is that such LPWAN network "mostly work", but every deployment has nodes that cannot report data or exhibit very low end-to-end reliability.

1.3 IoT Impact and Business Opportunities

The amount of connected devices is growing rapidly. During the years 2008-2009 some estimations say that the number of connected devices overtook the world's population and that by the year 2020 this number will increase to 50 billion [1]. This solely suppose that connected devices are being widely adopted in almost every human activity. And the economic impacts are significant. Some predictions for 2025 say that the IoT ecosystem will have an economic impact of USD 4 trillion to USD 11 trillion pera year [2].

IoT applications using low-power wireless networks can be used in many application domains.

Smart Cities. Local governments are interested in having public resources and infrastructure managed better. Applications such as smart parking, public lighting, monitoring air pollution levels and waste management

are some of the examples we can find in this space.

Smart Buildings. Security, comfort and energy-efficiency are some of the goals for applications in this environment. Example applications include intrusion and fire detection, elevator monitoring, HVAC, lighting and room occupancy among others. **Smart Utilities**. Applications in this field are based on monitoring the consumption of water, electricity and gas among others, allowing automated billing.

Environmental Monitoring. The objective in these applications is to monitor environmental phenomena such as humidity, snow, temperature, seismic or volcanic activity. Typically, these networks are deployed in remote places at the mercy of elements, wild animals, failing trees and fires. Usually the devices are deployed over vast areas and are required to last for many years with the same batteries.

Smart Agriculture. In these scenarios we find applications such as livestock monitoring and soil humidity, frost events and pH readings in plantations.

Industrial Monitoring & Automation: In the industry, monitoring and automation present all along the industrial process. Wireless solutions are easy to deploy and the cost of deployment does not linearly increase with the number of devices. IoT applications target the *missing measurements*. For instance the temperature, pressure and vibration are measurements that can improve the safety of the working sites and reduce maintenance costs as preventive maintenance is preferred to corrective maintenance. However, it is important to highlight that computer-monitoring systems such as SDA and SCADA have existed for many years and will continue to exist. Low-power mesh networks are replacing and otherwise wired process control application.

1.4 Grand Challenge & Contributions

The Grand Challenge of this thesis is to combine mesh networking and long-range radio technology in a "best-of-both-worlds" approach. That is, we contribute to answering the following questions: *Can we build a mesh network with long range radios? What radio technology and settings should we be using, in different applications? Is there an advantage in allowing motes to dynamically change their radio settings on a frame-by-frame basis?*

Towards addressing this Grand Challenge, the contributions of this thesis are:

- We benchmark the 31 different configurations of IEEE802.15.4g compliant hardware operating at sub-GHz frequencies (combining different modulation, different data rates, and other settings) through extensive in-situ experimental measurements. This allows us to make clear recommendations on what configuration to use in 4 application domains: Line-of-Sight, Agriculture, Urban Canyon and Urban.

- For smart building applications, we focus on particular on sub-GHz IEEE802.15.4g OFDM technology. We conduct a series of experiments comparing this technology against 2.4 GHz IEEE802.15.4 - OQPSK, the most commonly used in smart buildings. We show that OFDM brings higher reliability, longer range and lower power consumption that 2.4 GHz IEEE802.15.4 - OQPSK, making it a game changer for smart building applications.

- We extend this analysis of OFDM into the 2.4 GHz frequency band. We show that, despite the robustness OFDM signals present at the physical layer, somewhat conter-intuitively, OFDM greatly benefits from being combined with a channel hopping medium access technique when coping with multi-path fading and external interference.

- We introduce the concept of "Agile Networking", in which a mote can dynamically change the radio setting it is using on a frame-by-frame basis. We discuss the impact Agile Networking has on a standardized protocols stack such as 6TiSCH. In the process, we have developed an Agile Networking ready mote, and deployed an 80-mote testbed.

1.5 Organization of this Thesis

This thesis is organized as follows.

Chapter 2 presents the state of the art, starting by giving an overview of the most used wireless standards and protocols in low-power wireless networks. We present a more detailed description of the IEEE802.15.4 standard, including its "e" and "g" amendments, before introducing the 6TiSCH protocol stack for the Industrial Internet of Things. We give some examples of low power wireless networks and we finalize by presenting the state of the art on testbeds.

Chapter 3 presents the path we follow during this thesis and the tools we use for the experiments and for the construction of our testbed.

Chapter 4 presents a performance evaluation of the IEEE802.15.4g standard (using all 31 possible configurations) in sub-GHz bands. We set one transmitter node and 3 receiver nodes in different outdoors scenarios and analyze the PDR of the radio links at different distances. We draw recommendations on which PHYs to use for four different application spaces.

Chapter 5 presents, by experimentation, a comparative study between the most prevalent technology in Smart Building applications – IEEE802.15.4 - OQPSK (2.4 GHz band) – and the sub-GHz IEEE802.15.4g OFDM. We

determine the applicability of the IEEE802.15.4g for Smart Building applications.

Chapter 6 focuses on determining whether IEEE802.15.4g OFDM PHYs need to be used with the same MAC approach as IEEE802.15.4 - OQPSK. We benchmark the technology through experimentation and propose a MAC approach for the IEEE802.15.4g OFDM.

Chapter 7 describes the considerations to be taken into account when adopting Agile Networking on a low-power mesh network. Here we list how Agile Networking impacts the different layers of the 6TiSCH protocol stack. Finally, **Chapter 8** concludes this thesis, outlying its contributions and presenting directions for future work.

Two appendices complement these chapters.

Appendix A summarizes the current regulation in Europe, in the US and in Japan for sub-GHz frequency bands.

Appendix B presents a dynamic, wireless testbed architecture that is scalable, easily replicable and inexpensive in comparison to larger institutional testbeds. We deploy our own testbed, featuring 80 mote with both IEEE802.15.4 and IEEE802.15.4g compliant radios.

Chapter 2

State of the Art

This chapter gives an overview over the state of the art in wireless IoT standards and protocols. We start by providing the characteristics the most used IoT technologies. We then introduce the IIoT and its requirements for deterministic networks. We present the 6TiSCH protocol stack and explain each item in this stack. Then, we provide an overview of the low power wireless networks using sub-GHz frequencies and we finalize by giving an overview of the most important testbeds.

2.1 IoT Standards & Products

The starting point for IoT networks are the *things*. The distance from these *things* to the collecting data point go from a handful of centimeters to several kilometers. Here we present a list of the standards which define physical connectivity using wireless technologies. This list is not exhaustive and only shows the most used by the market.

2.1.1 Bluetooth

This standard was created as a joined effort between several companies: Ericsson, Intel, 3Com, Lucent, Microsoft, Motorola Toshiba and Nokia [3]. It provides short-range communications typically around 10 m with 1 mW output power, but it can reach 100 m with 100 mW output power. It operates in the 2.4 GHz ISM band, and can therefore be used worldwide without license. There are two types of specifications: Bluetooth (Basic Rate and Enhanced Data Rate) and Bluetooth Low Power (BLE). Channel spacing is 1 MHz (BR/EDR) or 2 MHz (BLE), resulting in 79 and 40 channels, respectively. Channel access uses Frequency Hopping Spread Spectrum. As modulation technology, it uses GFSK, $\pi/4$DQPSK and 8DPSK. Data rates are 125 kbps, 500 kbps, 1 Mbps, 2 Mbps and 3 Mbps.

Bluetooth transceivers are small enough to be embedded into, *inter alia*,

computers, cell phones, wireless headsets, printers and Smart Building devices. It supports point-to-point communication, broadcast transmissions and mesh networks [4]. The maximum payload size for the Bluetooth BR/EDR specification is 1,021 B whereas, only 29 B BLE in the mesh topology configuration. This standard is adopted by over 1,300 manufacturers.

2.1.2 IEEE802.11ah - WiFi

Considering only unconstrained devices (unlimited energy budget), the family of IEEE802.11 WiFi standards is the most deployed wireless technology [1]. Due to its ubiquity, this standard is of utmost importance for providing wireless access to high data rate sensors, audio and/or video devices, and to work as a backhaul technology for smart cities and in oil and mining industry applications. It works in the ISM bands at 2.4 GHz and 5 GHz.

However, its high energy consumption and limited range do not fit for IoT applications with constrained devices. To overcome this, the IEEE802.11 working group has develop the IEEE802.11ah [5] standard that targets, *inter alia*, support for unlicensed sub-GHz bands that helps to increase the range of the signal, to have better signal penetration and to enable power-efficient devices in sensors and meters in wearable devices, building automation, outdoor monitoring for agriculture, environmental and smart industry applications. It uses OFDM modulation, with channels of 1, 2, 4, 8, or 16 MHz. It is expected to offer radio links of 1 km at 100 kbps. It it meant to be deployed in a star topology but includes a simplify hops relay capability to extend it range. However, the IEEE802.11 makes the assumption of two hops. This technology is in the early stages of adaptation by the market and few manufacturers have come up with IEEE802.11ah transceivers, including Newracom [1] and Palma Ceia [2].

2.1.3 LoRaWAN

LoRaWAN is a communication protocol and system architecture for constrained devices [6]. The protocol stack consists of an application layer on top of the LoRa MAC and LoRa PHY. It is part of a new set of technologies known as **Low-Power Wide-Area Networks** (LPWAN). LoRaWAN networks only support a star topology, where end-devices have direct radio links with one or several gateways. Gateways are always listening or transmitting and therefore mains powered. Gateways' backhaul link can be any technology (e.g., 3G, Ethernet) [6] and every packet it receives is sent over IP to the Network Server and then to the Application Servers.

LoRaWAN started being only a PHY called LoRa. It uses chirp spread

[1] http://www.newracom.com/products/NRC7292.php
[2] https://www.pcsemi.com/devices/halow-transceiver/

spectrum [7] modulation technique developed by Cycleo [1] [3]. Due to its success, many manufacturers and telecommunication companies came together to form open and non-profit industrial alliance called *LoRa Alliance* to develop the protocol stack. Today, more than 500 members are part of the LoRa Alliance [4]. It is important to mention that the LoRa PHY is proprietary technology, the rest of the protocol stack is open.

The details of the LoRa PHY are the following. LoRa PHY uses a spreading technique where each symbol is encoded in a long sequence of bits. Its length is determine by 2^{SF}, where SF is a adjustable parameter known as *Spreading Factor* ($7 \leq SF \leq 12$). The SF determines the data rate of the transmission: low SF values result in high data rates; high SF values in low data rates. In the same sense, low SF values increase the link budget (by lowering the sensitivity of the receiver) and high SF values decrease the link budget [8]. Each of the sequences of bits from different SF are orthogonal between them. Depending on the region, the channel width can vary. In Europe, channels can be of 125 kHz and 250 kHz wide whereas in the US can be 125 kHz and 500 kHz.The link budget of LoRaWAN devices is around 155 dB (the sensitivity of the receiver is around -140 dBm). The price to pay for those high link budgets is the reduced data rate these links can support. The minimum data date is 250 bps and it can reach 21.9 kbps [1]. The maximum payload size is between 51 B and 222 B, depending on the SF chosen. LoRaWAN networks use unlicensed sub-GHz frequencies, increasing the coverage of the transceivers. Typical lengths of the radio links are 3-5 km for urban scenarios and 10-15 km in rural scenarios [9].

There are 3 classes of end devices in the LoRAWAN ecosystem: *Class A* - All, *Class B* - Beacon and *Class C* - Continuously listening [10]. These classes are associated with a mode of operation. Class A states that transmissions are always started by the end-nodes (uplink) at a random time (i.e. following "Aloha" behavior). Right after, the end device opens at least two reception windows, where commands or data can be sent from the gateway from the Network Server. This mode of operation yields the lowest energy consumption. Typically, Class A behaviour is adopted by any monitoring application [9]. All LoRaWAN nodes must at least implement Class A behaviour [10]. Class B devices synchronize with the Network Server through beacon packets that are synchronously sent by all gateways and provide a time reference to end devices. These devices can open receive windows using this reference and it is the network infrastructure through the Network Server that initiates downlink communication [10]. Downlink and uplink transmissions are independent. Class C devices are mains-powered and therefore can have their receive window always open except when transmitting.

Inside the LoRa MAC payload is the application data. LoRaWAN uses

[3] French company later acquired by Semtech.

[4] https://lora-alliance.org/about-lora-alliance

the IEEE 64-bit EUI of the end devices to map these to IPv6 addresses. IPv6/6LoWPAN protocols can be deployed within LoRaWAN networks.

LoRaWAN networks can serve applications where not-so-frequent events of measurements need to be reported per day [11]. This includes smart parking, smart waste collection, smart lighting, environmental control, leak detection, and agriculture applications. These applications are latency-tolerant.

LoRaWAN networks do not fit applications where deterministic data delivery and low latency are needed. Examples are industrial automation, where control loops need predicable response times, typically under 100 ms. Similarly, due to the low data rate of network, image and video applications do not fit. The price of this solution is variable, depending on the service provider chosen.

2.1.4 Sigfox

Founded in 2009, it is another LPWAN technology serving IoT applications. The protocol stack used by Sigfox is similar to LoRaWAN. From top to down, first comes the *Frame* layer that gets the application data and creates the radio frame and adds a sequence number. Then it comes the *MAC* layer, which adds a device ID and CRC code to the frame. Devices access the physical resource in a pseudo random fashion [12].Finally, the PHY layer uses D-BPSK modulation for uplink and GFSK modulation for downlink. Sigfox uses ultra narrowband (UNB) modulation [9], with each transmission occupying only 100 Hz and data rates of 100 bps or 600 bps. Data payloads are of limited size: 12 B for uplink; 8 B for downlink. The maximum packet size – payload and overhead – is 26 B. Similar to LoRaWAN, Sigfox uses only sub-GHz frequencies. Typical coverage is 3-10 km in the urban scenarios, and 30-50 km in rural scenarios [9].

End device communicates with the gateway(s), forming a star topology. Sigfox is an IoT operator, providing the infrastructure (gateways) to provide coverage to the end devices. Users can select the amount of packets their end devices will be sending (uplink) per day. At the time of writing, a subscription for a device to send 2 messages per day for one year is 6 €. To send 140 messages per day for one year, the subscription is 14 € [13].

Sigfox networks can serve IoT applications with little information to transmit and no so frequently. It suits for values of physical measurements (e.g. smart cities, utilities, agriculture), where 12 B of payload is enough.

2.1.5 Wireless M-BUS

Wireless M-Bus is a standard for automatic meter reading using sub-GHz frequency bands (169 MHz, 433 MHz, 868 MHz) [14]. It is defined in the *EN 13757-4* standard. It is the wireless version of the M-Bus (meter bus) standard. Wireless M-Bus networks have a star topology, with the sensors

communicating directly with the Data Collector. Six modes of operation are possible and these define the communication: S (Stationary), T (Frequent Transmit), R (Frequent Receive), N (Narrowband), C (Compact), F (Frequent Tx and Rx) [15]. It defines whether the communication is unidirectional (uplink) or bi-directional, whether few or frequent messages are sent, and what data rate to use.

The protocol stack is simplified to three entities: PHY, Data Link, Application layer. Optionally, there is another layer between the Application and Data Link for advanced security and routing for extended networks [15]. This standard does not have a certification body and manufacturers/developers follow an *honor system* to trust that other vendors correctly implement the standard. Differences in the implementation are solved by field trials.

2.1.6 NB-IoT and LTE-M

Mobile vendors and network operators want to take advantage of their infrastructure for IoT applications. However, existing cellular technologies such as GPRS, 3G and 4G/LTE is not suitable for constrained devices in the IoT. The 3GPP (3rd Generation Partnership Project) [5] is working to provide other cellular-based technologies that are customized for IoT applications. The advantage telecommunication operators have over other LPWAN technologies is that they use licensed radio spectrum. Each provider has its own set of frequencies. A second advantage is that telecommunication infrastructure is found almost everywhere. Base Stations (BS) are gateways for end devices. This simplifies the network architecture of any IoT solution provided by the 3GPP, as end devices can communicate directly with the BS as LoRaWAN and Sigfox do.

One of the first 3GPP attempts to address LPWAN applications is the **LTE-M** standard. The characteristics of this technology are: 1.4 MHz bandwidth (normal LTE devices use 20 MHz), data rate of 200 kbps, enhanced discontinuous reception (end devices can sleep for minutes and thereby save power), and half-duplex operation mode (lowering the complexity and cost of end devices). This technology requires additional software development and new hardware for end devices. On the other hand, only software updates are required on the BS, avoiding further investments [1].

LTE-M still provides a high data rates and consumes high bandwidth when compare with the other LPWAN technologies. For that reason, 3GPP has developped the Narrowband IoT (NB-IoT) specification. NB-IoT introduces several new techniques making it appealing for a LPWAN solution. These include: an enhanced link budget of 164 dB, better coverage in difficult environments such as basements, and a reduced channel width of 200 kHz, allowing operators to optimize their frequency band spectrum.

[5] 3GPP is a joint standardization partnership in charge of standardizing mobile protocols such as UMTS, HSPA and LTE, see `www.3gpp.org`.

NB-IoT has three operation modes: standalone, in-band and guard band.

Standalone: an NB-IoT carrier frequency uses a GSM carrier frequency, so the 900 MHz or 1800 MHz bands can be reused.

In-band: an NB-IoT carrier frequency gets allocated within a section of LTE carrier frequency band. The network operator is responsible for making such allocation and must configure the end device accordingly. This represents a risk for inter-operability within different operators if the devices are to be deployed across multiple countries, because the section of the LTE carrier needs to be the same.

Guard band: A NB-IoT carrier is placed between LTE bands. This approach requires coexistence of NB-IoT an LTE.

NB-IoT uses half-duplex frequency-division duplexing (FDD). The maximum data rates are 30 kbps for downlink, 60 kbps for uplink. Once NB-IoT is completely available, it is expected to be adopted as an LPWAN technology within the licensed bands. The remaining challenge for acceptability is the opportunity for other competitors outside the network operator ecosystem to offer IoT services without incurring expensive frequency spectrum licenses.

2.1.7 Discussion

Most of the IoT technologies presented in this section only support a star topology. The simplicity of this approach is certainly appealing for constrained devices. One key disadvantage, however, is that installing the infrastructure for these technologies is a considerable investment. That is, when a device needs to be installed beyond its communication range with the gateway, another gateway must be deployed. This requirements is lifted by using a multi-hop "mesh" topology, as is typically used by IEEE802.15.4-complaint devices.

2.2 IEEE802.15.4

IEEE802.15.4 is designed for Low Power Low-Rate Wireless Personal Area Networks. It covers the PHY and MAC layers. Its first version of 2003 [16] defines the use of two modulations for the PHY: BPSK for 868/915 MHz bands and O-QPSK DSSS for the 2.40-2.48 GHz band. Regarding the latter, the standard cuts it into 16 orthogonal frequencies (numbered 11 to 26), 2 MHz wide and separated by 5 MHz. The data rate is 250 kbps and the maximum frame size is 127 B. Throughout this manuscript, whenever we refer to IEEE802.15.4–PHY we refer to these characteristics.

The access to the physical radio channel is control by the MAC layer and it is done by employing CSMA-CA method. The standard supports star (1-hop) and peer-to-peer (allowing multi-hop) networks topologies.

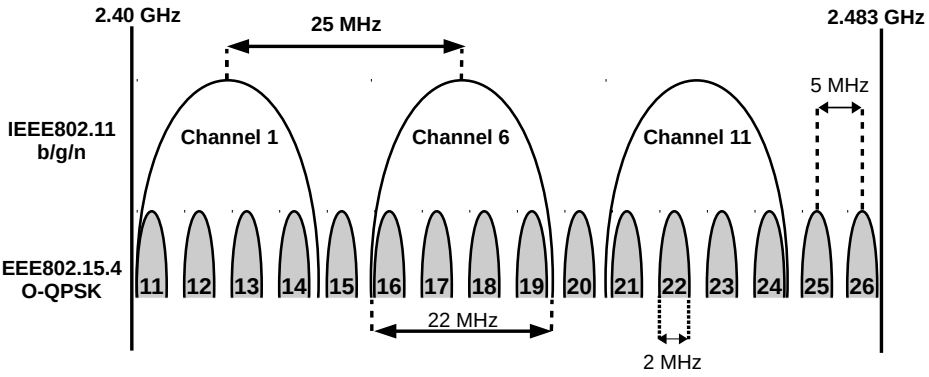


Figure 2.1: IEEE802.15.4 and WiFi channels.

Low power low rate wireless networks are found in industrial [17], home [18], urban [19], smart building [20] and other applications. IEEE802.15.4-PHY provides a trade-off between energy consumption, communication range, and reliability which is absolutely suited to those applications. All major chip vendors have adopted the standard and have cheap [6] IEEE802.15.4-compliant radios in their catalogs, making it a very accessible technology.

In the decade after its first version, several fully standards-compliant protocol stacks were built on top of IEEE802.15.4. Industrial alliances have formed, which typically put together several standards to form a complete protocol stack, and serve as labeling/certification bodies. The most prevalent examples are the Zigbee Alliance [21], the Thread Group [22], WirelessHART [23] and ISA100.11a. Tens of thousands of networks based on IEEE802.15.4 are operating today, and achieve over 99.999% end-to-end reliability and over a decade of battery lifetime.

2.2.1 Challenges of IEEE802.15.4

There are two main challenges for making a network composed of IEEE802.15.4 devices, operating at 2.4 GHz, reliable.

The first challenge is **external interference**. At 2.4 GHz, external interference mainly comes from IEEE802.11 (WiFi) and Bluetooth.

Fig. 2.1 shows how a 22 MHz WiFi channel overlaps 4 IEEE802.15.4 channels. IEEE802.15.4 networks are in disadvantage against WiFi in case of collisions. WiFi access points usually transmit at +20 dBm, IEEE802.15.4 nodes typically between 0 dBm and +8 dBm.

Khaleel et al. [24] investigate the cross-interference between IEEE802.15.4 and IEEE802.11b (WiFi). They use a Crossbow Telos device equipped with

[6] Sub-5 USD IEEE802.15.4 radio chips are commonplace.

an IEEE802.15.4-compliant CC2420 radio to sense the frequency spectrum by using RSSI, under different WiFi data rate conditions. They show that when there is a WiFi connection of 3 Mbit/s, the probability of failure to access the medium for a IEEE802.15.4 device reaches 90%, when operating on the same frequency as the WiFi connection.

Watteyne et al. [25] conduct an experiment to record the connectivity between 350 nodes in a typical office environment, using the IoT-lab large-scale testbed [26]. These nodes communicate on each of the 16 available frequencies at 2.4 GHz. They show the impact of WiFi interference on the reliability of the IEEE802.15.4 wireless links: even when the WiFi network sits idle, IEEE802.11 beaconing causes a significant number of links to drop from 90% to 70-80% Packet Delivery Ratio (PDR).

Guo *et al.* [27] analyze how different Interference Sources (IS) impact the Packet Error Rate for IEEE802.15.4 radio links. With combinations of Interference Sources (none, WiFi, Bluetooth and microwave), distance between TX and RX, distance between IS and RX, position of IS in relation to TX-RX and IEEE802.15.4 channel;. The authors observe that WiFi and microwave ovens can degrade the quality of the radio links, causing a 25% PER depending of the distances between TX, RX, IS and as well as the chosen channel.

The second challenge is **multi-path fading**. In any indoor environment, objects in the surroundings of a wireless link cause a reflection of the radio signal. These different "echoes" of the same signal reach the receiver's antenna at slightly different times. All these reflections can interfere constructively, increasing the signal strength. Yet, they can also interfere destructively, making the communication between transmitter and receiver impossible. Wireless propagation properties can vary at the slightest change: opening/closing doors, people walking by, movement of furniture can affect the reflections on the signal and thus enhance or deteriorate the radio link.

Watteyne et al. [28] visualize the effect of multi-path fading. They install a transmitting node on a robotic arm which moves inside a 20 cm by 35 cm plane, with a 1 cm step, yielding 735 positions. At each position, the transmitting node sends 1000 frames of 29 bytes long to the receiver node located 1 m away. The experiment is repeated over each of the 16 available frequencies. Results show that the PDR of the wireless link between transmitter and receiver can swing from 100% to 0% by moving the transmitter by just 3 cm. This is entirely due to multi-path fading.

There have been continuous developments in the PHY and MAC layers of the IEEE802.15.4 standard. Its 2015 revision includes, *inter alia*, amendments IEEE802.15.4g [29] and IEEE802.15.4e [30], defining new physical layers and MAC approaches, respectively. We provide an overview of these amendment in the following sections.

2.2.2 IEEE802.15.4e - TSCH

This amendment introduces Time Slotted Channel Hopping (TSCH), a MAC approach in which tightly synchronized nodes heavy duty cycle their radios to conserve energy and use frequency hopping to combat external interference and multi-path fading. This approach provides high reliability while minimizing energy consumption.

The predecessor of this amendment is the Time Synchronized Mesh Protocol (TSMP) [31], a proprietary protocol for self-organizing low-power wireless mesh nodes, developped by *Dust Networks* in 2006. Devices in the TSMP network (called *motes*) are synchronized; the communication between them occurs following a schedule. Time is divided into slots (timeslot) that are long enough to allow one frame transmission and its correspondent acknowledgement (ACK). The schedule tells the mote what to do on each timeslot: transmit, receive or sleep. In addition to the schedule, motes implement the Channel Hopping technique. Each Tx/Rx occurs on a different channel with respect to the previous, increasing the reliability of the communication on noisy scenarios.

Two industrial low-power wireless standards, WirelessHART and ISA100.11a, adopted the TSMP concept. Many industrial process monitoring and factory automation applications use these standards. The IEEE802.15 Task Group 4e was launched in order to provide a MAC amendment that meets the needs of industrial applications. This MAC amendment also implements the TSMP concept, which it calls Time Slotted Channel Hopping.

TSCH has become a default MAC approach in IEEE802.15.4 since its 2015 version [32]. Further standardization at the IETF 6TiSCH working group defines how to combine TSCH with IPv6. Watteyne *et al.* [33] present the performance of SmartMesh IP, a commercial TSCH solution, which yields over 99.999% end-to-end reliability, and over a decade of battery lifetime. TSCH (and 6TiSCH) networks are widely regarded as the future for low-power wireless networks, and are the base for all major open source implementations [34] as well as several commercial ongoing implementations.

Time Slotted

In TSCH networks, time is divided into timeslot. Timeslots are grouped into slotframes that are repeated over time. Timeslots are identified by two values: *Absolute Slot Number* (ASN) and *timeslot offset*. The *ASN* is a unique 5 B global counter value [7] that increases with every timeslot that passes. The *timeslot offset* is a value between 0 and the amount of timeslots in the slotframe. This determines the relative position of the timeslot in the slotframe. Fig. 2.2 shows an slotframe of n timeslots. The duration of a

[7] Considering a timeslot of 10 ms, the ASN value overlaps every 127,258 days, more than 348 years!

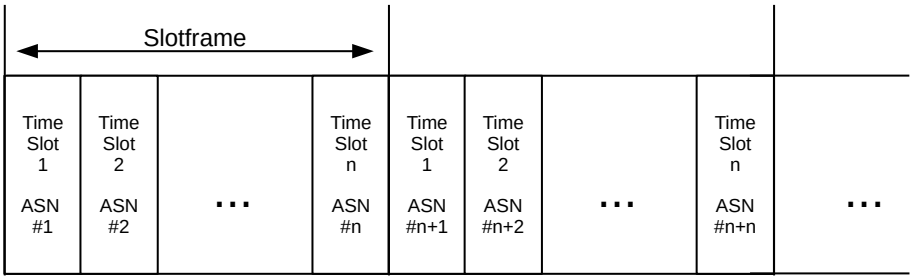


Figure 2.2: Timeslots and slotframes.

timeslot should be large enough to allow the transmission of a frame and its correspondent acknowledgment (ACK) if the frame needs it (see fig. 2.4).

A communication schedule orchestrates all communication in the network. Each node has its own schedule that determines which task must perform during each timeslot: transmit, receive or sleep. If the task is transmit, the node switches on its radio and sends a frame that has in its TX buffer (and listens for an ACK if required). If the task is receive, the node switches on the radio and listens for any frame (and transmits an ACK if required). If the task is sleep, the node goes to sleep mode until the end of that timeslot. In battery-powered nodes, having the radio switched on for transmissions/receptions is an energy-expensive task. Therefore, it is of utmost importance for nodes to switch *on* their radios only if needed. When sleeping, nodes draw as little as few μA. When communicating, they draw 10-25 mA [35] [36].

With several non-overlapping frequencies (different channels), parallel communications can happen at the same timeslot without interfering with one another. Fig. 2.3 shows a simplified example of a TSCH schedule. Here we see how each slotframe is exactly repeated. Communications from C to A and from D to B happen at the same timeslot (*timeslot offset* 1), but on different channels (*channel offsets* 1 and 3) and therefore, not interfering with each other. The combination of *timeslot offset* and *channel offset* defines a *cell*. There are two types of cells in TSCH networks: *shared* cells and *dedicated* cells.

- Shared cell. A contention-based cell. Any node can try to use this cell and therefore, collisions may occur. Mechanisms such as *Random Exponential Back-off* may be implemented to cope with several nodes competing for the same cell.
- Dedicated cell. A contention-free cell. The cell is allocated for a pair of nodes in a specific direction. Each node knows whether it is the emitter or the receiver of a frame. No other pair of nodes within the network should be using the same cell.

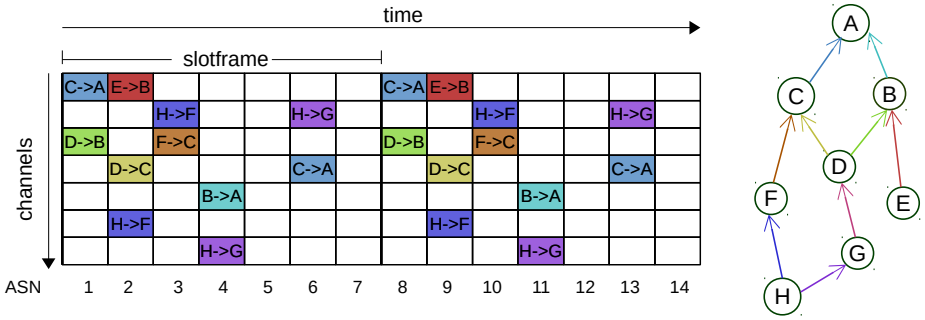


Figure 2.3: Example of a TSCH schedule.

Channel Hopping

In the unlicensed frequency bands, it is expected that different devices use the physical medium and thus causing interfering with one another. Some frequencies might be more used than others. For example, if one IEEE802.15.4 device uses only channel 18 (see Fig. 2.1) and it happens to be near to a WiFi access point using the IEEE802.11 channel 6, the IEEE802.15.4 device would see its communications severely affected.

Multi-path fading also affects the frequencies in a non-uniformly fashion. Therefore, changing the frequency (*channel*) on which transmissions take place on a regular basis is beneficial for the reliability of the communication as it helps to cope with the external interference and multi-path fading [37].

This is done with **channel hopping**. It is a technique where the communication frequency changes on a timeslot basis. That is, nodes tune their radio to a different frequency every time the schedule tells them to either transmit or receive. This frequency is determined by (2.1).

$$frequency = (ASN + channel\_offset) \ \% \ number\ of\ channels \quad (2.1)$$

The *ASN* value always increases, so the *frequency* changes for the same cell in consecutive slotframes. The objective is that transmissions take place over all frequencies available in a uniform fashion. This way, TSCH, through **channel hopping**, exploits all the frequencies available in the frequency band and the radio links gain reliability [28]. TSCH is a perfect candidate for a MAC layer for IoT applications requiring high reliability and low power consumption.

Time Synchronization

We have seen that in TSCH, every communication is scheduled. In order to follow this schedule, nodes need to be tightly synchronized. Nodes keep the same notion of global time (ASN) by typically using crystal oscillators

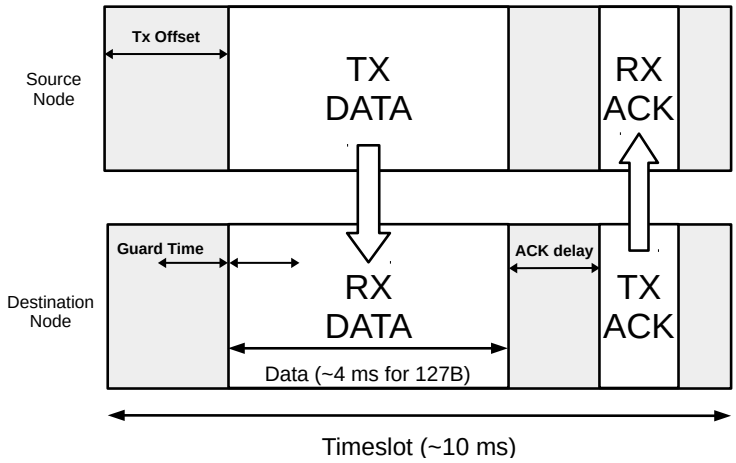


Figure 2.4: An example timeslot for networks using IEEE802.15.4– PHY. Its maximum PSDU is 127 B. At 250 kbps, the radio needs just over 4 ms to send 127 B. Timeslots are long enough to allow the transmission of a maximum length frame and its acknowledgement.

as internal clocks. However, these are not perfect, and tend to drift with respect to one another[8]. Nodes therefore need to regularly re-synchronize in order to align their clocks.

The drift of crystal oscillators is typically measured in *parts per million* (ppm). Manufacturers provide this value in their data sheets. Typical values for drifts in low-cost crystals are 10-50 ppm. This means that, over 1 s, the clock drift is up to $\pm$ 50 μs, or 180 ms per hour with respect to a perfect clock. This is a large value, given that timeslots are typically 10 ms long. This can be even more severe when neighbor nodes have their clocks drifting in opposite directions: one clock being 50 ppm fast and the other 50 ppm slow, for a total of 100 ppm relative drift.

The drift two nodes can bear is related to the inner structure of a timeslot. Fig. 2.4 shows the main tasks within a timeslot when a transmission take place. On the source node, the transmission takes place not at the beginning of the timeslot, but after a precise delay (`Tx Offset`). However, on the destination part, the node start listening at `Guard Time` before the `Tx Offset`, and keeps listening as long as twice the `Guard Time`, or until it receives a frame. this way, the receiver ensures it is listening when the source node starts transmitting with a margin of safety (in the case the transmission occurs early or late). Therefore, the maximum drift tolerance is `Guard Time`. Bigger relative clock drift makes the transmission to fail.

Nodes need to re-synchronize continuously. In TSCH, nodes re-synchronize their clocks every time frames are exchanged. Nodes calculate the time difference between the moment the frame should be received (`Tx Offset`) and the

[8] Temperature also impact in the drift of crystal oscillators.

actual time it is received. This allows nodes to re-align their clocks, correcting the drift. The time between re-synchronizations must be short enough to avoid the relative drift between nodes to become larger than the `Guard Time`. For instance, having a relative drift of 50 ppm and `Guard Time` of 1 ms, a pair of nodes needs to re-synchronize (exchange a frame) at least every $1\ ms/50\ ppm = 20\ s$ before being de-synchronized. Nodes can send dummy frames (*keep-alive*) if no data frame is exchanged during this time. The cost of keeping synchronization is low: for a transmission that takes roughly 4 ms being sent every 20 s results in a duty cycle of $4\ ms/20\ s = 0.02$ %.

2.2.3 IEEE802.15.4g - SUN

The IEEE802.15.4g amendment [29] was created for Smart Utility Network (SUN) applications. One strong requirement to be able to build neighborhood-wide (mesh) networks, is a multi-km range. To do so, this standard is mostly used in sub-GHz bands. However, the regulation in these frequencies impose heavy duty cycle restrictions (see all details in Appendix A). The IEEE802.15.4g amendment, first published in 2012, was rolled into the main IEEE802.15.4 specification in its 2015 revision [38].

IEEE802.15.4g introduces three alternative PHYs: SUN FSK (Frequency Shift Keying), SUN O-QPSK (Offset-Quadrature Phase Shift Keying) and SUN OFDM (Orthogonal Frequency Division Multiplexing). Each physical layer was designed for a specific market segment, and is marketed as having distinct advantages. FSK increases the transmit power efficiency by the constant envelope of the signal. O-QPSK shares the characteristics of IEEE802.15.4 DSSS O-QPSK. OFDM provides high data rates, and is designed to operate in environments with frequency selective fading, such as indoors [39]. In all cases, compliant radio chips can exchange frames of up to 2047 B.

FSK and O-QPSK are well known PHYs widely implemented in low power devices. This is not the case for OFDM, which has been extensively used in high-end wireless systems, and which is now entering the low-power wireless space. In the following section we give an overview of the SUN OFDM PHY, and provide the main characteristics of SUN FSK and O-QPSK PHYs.

SUN OFDM PHY

OFDM was created to combat multi-path fading. Like TSCH, it exploits frequency diversity. But while TSCH does so at the MAC layer, OFDM does so directly at the physical layer. In OFDM, a frequency band (called "channel") is divided into numerous frequencies ("sub-carriers"). The sub-carriers are far enough apart in frequency to be orthogonal: they do not interfere with one another. An OFDM symbol is the combination of the

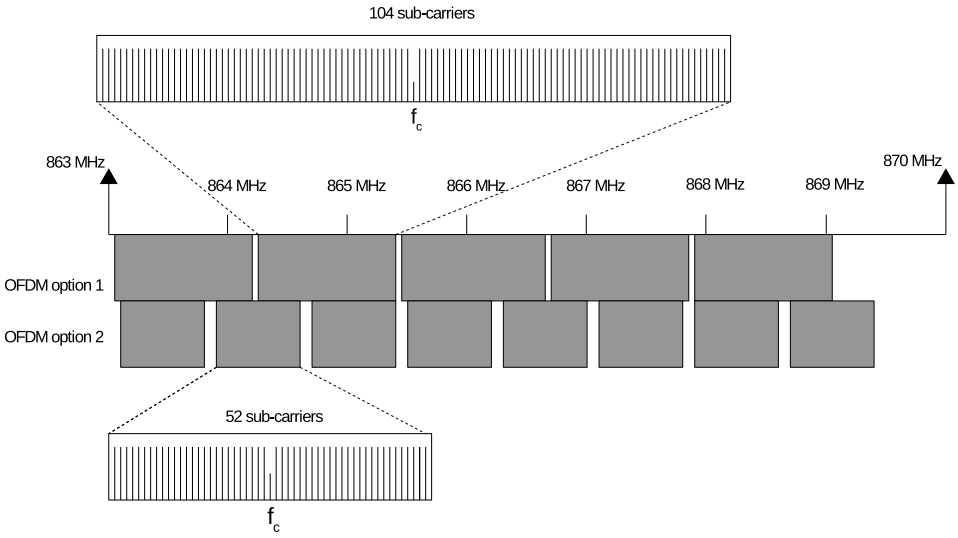


Figure 2.5: In OFDM, data is transmitted on multiple sub-carriers. Multiple sub-carriers are grouped into channels; the OFDM option determines how this grouping is done.

sub-carriers, each carrying a portion of the information to be transmitted. Each sub-carrier is modulated with a low-order modulation (BPSK, O-QPSK or 16-QAM). Combining the sub-carriers is equivalent to having a high order signal modulation (e.g. 16,777,216-PSK for 24 bits per symbol), making it possible to achieve high data rates. Fig. 2.5 shows the OFDM channels in IEEE802.15.4g where communication uses multiple sub-carriers, separated by a constant equal frequency distance Δf. In the center frequency f_c, no information is sent (null tone).

In SUN OFDM, the effective duration of a symbol (t_s) is 96 μs. To ensure orthogonality between sub-carriers, they are separated by $1/t_s$, or 10,416.667 Hz. The standard describes 4 ways of grouping sub-carriers to form an OFDM symbol; these are called "options", and are numbered from 1 to 4. Table 2.1 shows the number of sub-carriers for each option, as well as the bandwidth it occupies.

The sub-carrier modulation is specified by the Modulation and Coding Scheme (MCS). There are 7, numbered from 0 to 6. The data rate of the signal is given by the combination of the OFDM option and MCS. Table 2.2 shows the details of the MCS and the data rates for each OFDM option/MCS combination.

Frequency repetition is an OFDM technique in which more than one sub-carrier transports the same information. While it reduces the effective data rate of the transmission, it makes the signal much more robust against multi-path fading. That is, even if one sub-carrier is not successfully demodulated, there is another sub-carrier (at a different frequency) that carries the same

	option 1	option 2	option 3	option 4
# sub-carriers	104	52	26	14
(data/pilot)	96/8	48/4	24/2	12/2
Channel width (kHz)	1094	552	281	156
Space between channels (kHz)	1200	800	400	200
# Channels	5	8	17	34

Table 2.1: The OFDM option specifies how many sub-carriers are used in one channel.

	option 1	option 2	option 3	option 4
MCS0 BPSK rate 1/2 – 4× freq. rep.	100 kbps	50 kbps	-	-
MCS1 BPSK rate 1/2 – 2× freq. rep.	200 kbps	100 kbps	50 kbps	-
MCS2 QPSK rate 1/2 – 2× freq. rep.	400 kbps	200 kbps	100 kbps	50 kbps
MCS3 QPSK rate 1/2 – no freq. rep.	800 kbps	400 kbps	200 kbps	100 kbps
MCS4 QPSK rate 3/4 – no freq. rep.	-	600 kbps	300 kbps	150 kbps
MCS5 16-QAM rate 1/2 – no freq. rep.	-	800 kbps	400 kbps	200 kbps
MCS6 16-QAM rate 3/4 – no freq. rep.	-	-	600 kbps	300 kbps

Table 2.2: The MCS setting specifies the modulation used on each sub-carrier, its symbol rate, and whether frequency repetition is used. Combined with an OFDM option, this yields a data rate. A dash ('-') indicates a combination that does not exist. Colored cells are settings explored in Section 4.2.

Parameter	Operating mode #1	Operating mode #2	Operating mode #3
Data rate(kbps)	50 kbps	100 kbps	200 kbps
Modulation	2-FSK	2-FSK	4-FSK
Modulation index	1.0	1.0	0.33
Channel spacing	200 kHz	400 kHz	400 kHz

Table 2.3: Characteristics of SUN FSK for the European 863–870 MHz band.

data.

SUN FSK PHY

This is currently the most used PHY for SUN applications. The standard suggest that any SUN device must implement this FSK. Industrial alliances such as Wi-SUN [40] use this PHY for their user profiles[9]. Table 2.3 shows the main characteristics of this PHY for the European 863-870 MHz band.

Multiple SUN networks can be operating within the same location and sharing the same frequency band. In order to mitigate interference, the standard defines a Multi-PHY Management (MPM) procedure that facilitate the coexistence between networks using different PHYs. Nodes acting as coordinators with a duty cycle greater than 1% should implement a Common Signalling Mode (CSM). The CSM is the operating mode #1 and serves as a common PHY between all networks to manage the coexistence through the MPM procedure [41].

The use of Forward Error Correction (FEC) is optional. The standard proposes two types: a recursive and systematic code (RSC), and a non-recursive and non-systematic code (NRNSC). Both are 1/2 rate (one bit of information encoded into two bits transmitted). Data whitening can be used and it is also optional. SUN FSK devices are simple and do not require complex circuitry consuming high processing power, resulting in a less power-hungry technology. This PHY targets low data rates and high energy efficiency applications, e.g. smart metering. Most electric meters in the US use this PHY.

SUN O-QPSK PHY

The SUN O-QPSK PHY shares some characteristics with IEEE802.15.4 - PHY, making multi-mode systems easier to design and more cost-effective [42]. This PHY uses Direct Sequence Spread Spectrum (DSSS) and Multiplexed Direct Sequence Spread Spectrum (MDSSS)[10], both with multiple spreading

[9] Wi-SUN is the industrial alliance for the *Smart Ubiquitous Networks.*

[10] Not in all frequency bands, e.g. MDSSS is not supported within the 868 870 MHz band.

factors that results in several data rates. These vary depending on the frequency band used. The standard supports the 868-870 MHz band (European regulation does not allow this PHY to be used in the whole 863-870 MHz band) with data rates of 6.25, 12.5, 25 and 50 kbps. Only 3 channels are available in this 2 MHz band: centered at 868.3 MHz, 868.950 MHz and 869.525 MHz.

In the following section, we introduce the requirements for the IoT in industrial application and already proposed solutions and standardization efforts.

2.3 Industrial IoT Protocol Stacks

Industrial applications served with lower-power wireless have specific requirements: devices within the low-power wireless network need to have low power consumption profiles, the communication provided by the network needs to be reliable (infinitesimal tolerance to data losses), and the network needs to be easy to deploy and maintain [17].

We have seen how IEEE802.15.4 - TSCH can provide determinism, reduce power consumption and increase reliability. Commercial products already exist using TSCH (or similar approaches), fulfilling the requirements for industrial applications. This is the case of WirelessHART [23] and SmartMesh IP [43]. These are proven technologies, with manufacturers such as Dust Networks [11] who has sold more than 76,000 networks in 120 countries [44]. These are proprietary solutions.

In the following section, we review protocol stack we believe are the best suited for industrial IoT applications. These protocols sit over the IEEE802.15.4 - TSCH and go up to the application layer. All these protocols are specifically designed to work in Low-power and Lossy Networks (LLNs).

2.3.1 6TiSCH Protocol Stack

The IETF 6TiSCH Working Group (WG) has been created to standardize a solution to combine IPv6 with the TSCH MAC mode of the IEEE802.15.4 standard[12]. This WG proposes a protocol stack to meet the requirements of industrial applications (low-power and high reliability) combined with the capacity to enable IPv6 connectivity within the low-power wireless network.

The 6TiSCH protocol stack is defined from the TSCH MAC layer up to the application layer [45]. Fig. 2.6 shows a simplified protocol stack proposed by 6TiSCH. The 6TiSCH protocol stack is not bound to a particular PHY.

[11] Dust Networks was bought by Linear Technologies who subsequently got bought by Analog Devices.

[12] `https://datatracker.ietf.org/wg/6tisch/about/`

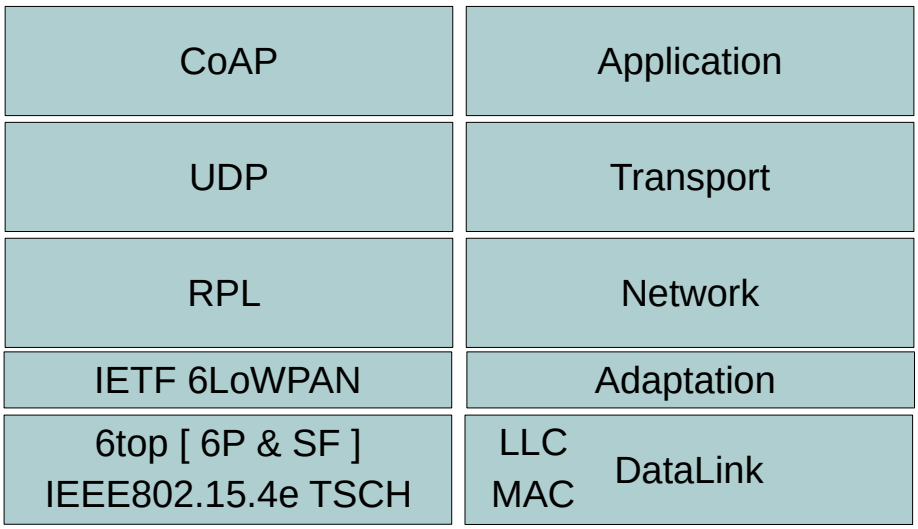


Figure 2.6: A simplified version of the 6TiSCH protocol stack.

In theory, any wireless technology can be used here. However, the *de-facto* PHY is the IEEE802.15.4 - PHY [46].

Open source implementations such as OpenWSN [47] and Contiki [48] come with the 6TiSCH protocol stack already implemented. In this section, we provide a brief descriptions of the protocols that make up that stack.

Data Link layer: Scheduling Functions and 6top Protocol

Until now, we have seen that TSCH is capable of executing a schedule. However, TSCH does not define how this schedule is built, nor managed. The *intelligence* that builds and manages the schedule comes from one upper layer: the Scheduling Function (SF). The SF is in charge of allocating networks resources (*cells*) to the nodes. This has a direct impact on the Key Performance Indicators (KPIs) of network, and is important for operators to comply with the Service Level Agreements. For instance, it determines the amount of bandwidth each node has: more cells allocated to a given node means more opportunities to communicate (TX/RX) and less to allocate to other nodes.

There are several ways how to classify and build SFs. The most simple schedule is a **static** schedule. Here, the schedule is fixed and does change dynamically. This type of scheduling is useful when bootstrapping the network or a backup mode. Teles Hermeto *et al.* [49] provide a classification of SFs (algorithms) that can build schedules in an either centralized, hierarchical or distributed manner. **Centralized** schedules are based on an external entity (e.g. computer in the network coordinator node) which builds the schedule based on the information recollected from all the nodes within the network.

Hierarchical schedules are built once the topology of the network is established. The paths to the sink are first set up, then the SF allocates resources from node to node. **Distributed** schedules are built locally, between pairs of nodes where they negotiate the resources according to their application requirements (e.g. bandwidth, latency).

Duquennoy *et al.* [50] introduce a way to build schedules based on the ID of the nodes. Nodes choose which cells to allocate depending of an unique identifier (e.g., EUI-64). Nodes are aware of their RPL neighbor IDs, and using some predetermined function they translate those IDs into coordinates of cells (timeslot offset and channel offset) to be allocated. This predetermined function should map one ID to one cell[13]. Since it cannot be assured that there will be more cells than IDs, it may be the case that two or more IDs generate the same cell coordinates. Therefore, cells allocated by this mechanism should be treated as shared cells although contention is reduced. The efficiency of this mechanism lays in the fact that no negotiation is needed. This approach has been adopted by the 6TiSCH WG and merged into the 6TiSCH Minimal Scheduling Function (MSF) [51].

SFs have attracted the attention of the research and industrial community. SFs are being developed constantly to target specific requirements. This is the case for Chang *et al.* [52], who present the Low Latency Scheduling Function (LLSF). This daisy-chains timeslots in order to reduce latency.

While SFs are "policy" to determine which cells to allocate, the **6top** Protocol (6P) [53] is the "mechanism" used by nodes to negotiate those resources. 6P defines the structure of the messages (*commands*) nodes exchange in order to, *inter alia*, add and delete cells to their neighbours.

Each decision taken by the SF is executed through a **6P Transaction**. This consists of a sequence of 6P commands exchanged between a pair of nodes to negotiate modifications in their schedule. They can be a 2-step or 3-step transaction. Fig. 2.7 and fig 2.8 show an example of these 6P Transactions. Each 6P Transaction is identified by a sequence number. This mechanism ensures that every modification to the schedule is kept consistent between any pair of nodes. Inconsistencies create mismanagement of the network resources, e.g., waste of energy, increase of packet loss, etc.

TSCH, 6P and SF correspond to the Data Link layer in the equivalent OSI model.

Adaptation Layer: 6LoWPAN

The *IPv6 over Low-Power Wireless Personal Area Networks* standard [54] of the IETF provides an adaptation layer for IPv6 traffic to be sent over over constrained devices typically implementing IEEE802.15.4 - PHY and IEEE802.15.4- MAC.

The benefits of bringing IPv6 connectivity to WSNs are many:

[13] This predetermined function might be a *non-injective non-surjective function.*

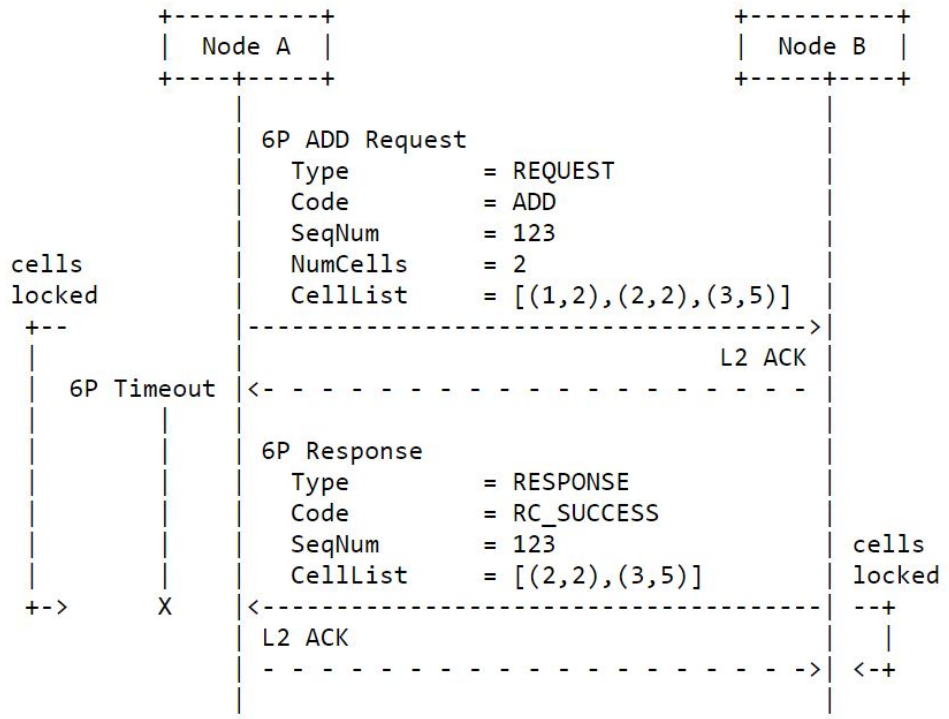


Figure 2.7: A 2-step 6P Transaction. Node A wants (message type `REQUEST`) to add 2 cells (code ADD) from node B and proposes a list of cell candidates. If node B agrees, it responds (message type `RESPONSE`) with the code RC_SUCCESS and the chosen cells. Figure taken from [53].

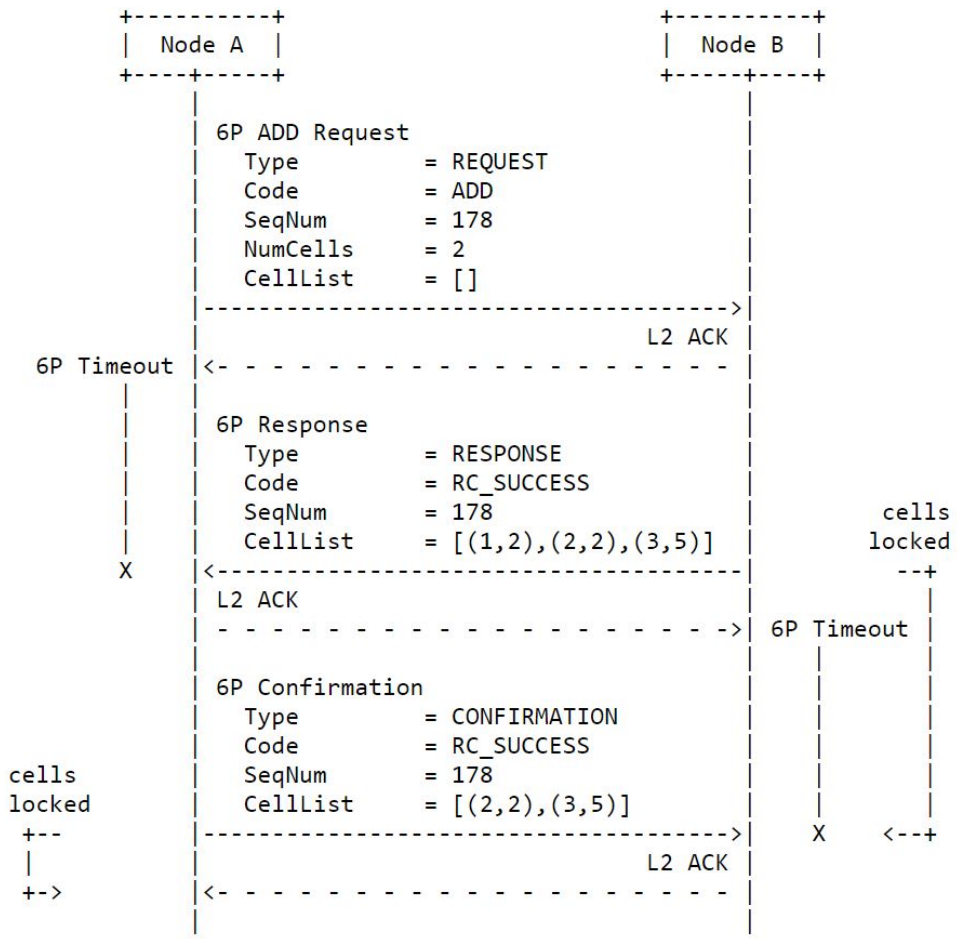


Figure 2.8: A 3-step 6P Transaction. Node A wants (message type `REQUEST`) to add 2 cells (code ADD) from node B without providing any candidate cell. If node B agrees, it responds (message type `RESPONSE`) with the code RC_SUCCESS and proposes a list of candidate cells. A confirms the success of the transaction (message type `CONFIRMATION`) and adds a list of the chosen cells. Figure taken from [53].

- IP devices can be connected seamlessly to other IP networks.
- Networks using IP can use already existing network infrastructure.
- IP is a proven technology that can scale very well and we have decades of experience on it.
- IP technology is open and free. Innovation is always going on.
- Many tools are available for managing and diagnosing IP networks.

However, the transition from the IP world towards constrained devices is not trivial. IPv6 requires at least 1280 B of Maximum Transmission Unit, while the IEEE802.15.4 PHY can transport 127 B frames at most. 6LoWPAN is the standard that provides the mechanisms to compress and fragment IPv6 datagrams into transportable fragments over the IEEE802.15.4 -PHY.

6LoWPAN compresses the IPv6 and UDP header. This compression is stateless and relies on information known by every node on the network. IPv6 addresses can be omitted most of the time [55].

Network Layer: RPL

In low-power wireless networks implementing the 6TiSCH protocol stack, each node has an IPv6 address. As in any other IP-based networks, IP packets destined to remote devices need to be routed over multiple routers until they reach the destination. In wireless networks these nodes (routers) are interconnected by unstable radio links, low data rates and with traffic patterns including point-to-multipoint and multipoint-to-point in addition to simply point-to-point within thousands of nodes. Conventional routing protocols (OSPF, ISIS) rely on static link metrics, and therefore are not designed to work under these conditions. The IETF ROLL WG produced a set of routing requirements documents which cover building automation [20], home automation [18], industrial [17] and urban [19] applications. This WG has tailored a routing protocol to meet these application requirements (but applicable for any network application with similar conditions) for constrained devices[14]: **RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks** [56].

RPL builds routes following a Destination-Oriented Directed Acyclic Graph (DODAG). A DAG is formed by a set of nodes interconnected by links in such a way that it is not possible to start at a given node X and follow a path that cycles back to this node X. That is, the structre is acyclic, which prevents loops within the network. A Destination Oriented DAG has a single DAG root (sink node). It is common for this DAG root node to be less constrained that the rest of the nodes (usually mains powered) and connected to a IPv6 backbone network. Fig. 2.9 depicts a DODAG network.

[14] RPL is agnostic of the underlying technologies.

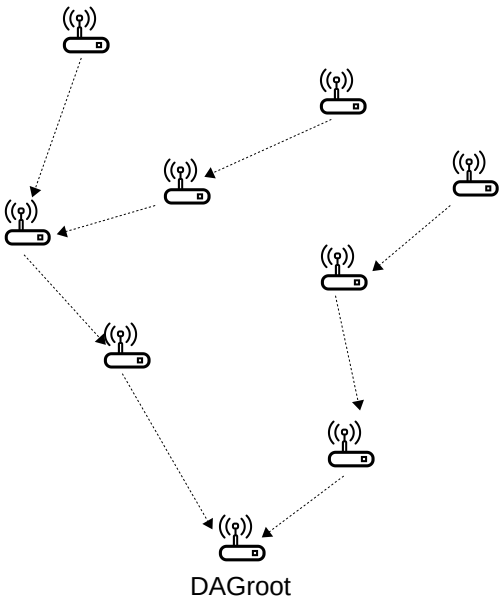


Figure 2.9: A simplified DODAG network example.

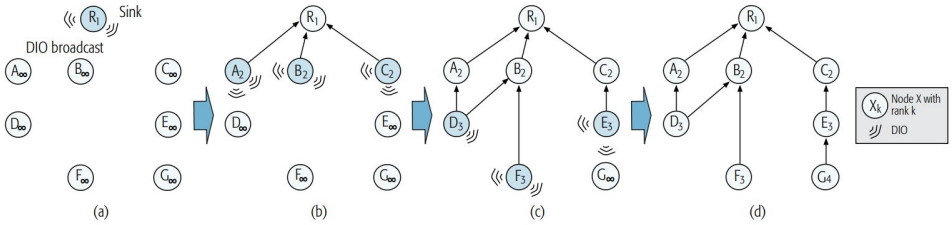


Figure 2.10: Steps on the network formation with RPL. Figure borrowed from [58].

Nodes choose to connect to other nodes using a gradient approach upon a metric that can be a combination of number of hops to the DAG root, link quality or any other parameter. How this metric is obtained is defined by an *Objective Function* (OF). This defines which parameters are considered and the formula each node will apply to obtain its own metric (known as *Rank*). An example is the OF0 (Objective Function Zero) [57]. Each hop has a given weight into the metric which is multiply by the link quality between the nodes (typically its Expected Transmissions Count – ETX –, the number of attempts to successfully send a frame from one node to its neighbor). As the number of hops increase between the node and the sink, its own rank increases too. Nodes elect as routing parents neighbors which have a lower rank (and are therefore closer to the root of the DODAG). This is an additive metric: nodes joining the network connect through the best candidate. A node's rank is that of its parent, plus the link cost to that parent.

A RPL network forms as follows. The network starts with only one node

in it, the DAG root, which typically has connectivity to the Internet (or to some backbone network). The DAG root then starts advertising itself as a path to the Internet through DODAG Information Oriented (DIO) messages (sent broadcast). Nodes within its range hear these messages and connect to it. The nodes which are now connected to the DAGroot calculate their own rank and start broadcasting their own DIOs messages. This allows nodes out of the range of the DAG root to connect to the network and send messages through intermediate nodes. Nodes can receive many DIOs messages from different nodes and they have to choose the most convenient node to connect through (*preferred parent* with lowest rank). Fig 2.10 depicts the process of DODAG formation. Once a node has joined the network, it regularly sends DIO messages. If one node looses connectivity to its preferred parent (because of battery depletion, because it is removed from the network, etc), by getting DIOs from other nodes, it can change its preferred parent, calculate its new rank and advertising it through the DIOs that it regularly sends. This allows the network to adapt to the changing conditions of LLNs.

The traffic that comes from the nodes to the DAG root is called *upwards*. In the opposite direction – traffic from the DAG root to the nodes within the network – is called *downwards*. In most applications, the vast majority of the traffic is upwards. Once a node has a route to the DAG root of network (RPL) and resources allocated (bandwidth), the embedded application on it can start generating application data.

Transport and Application Layer: UDP - CoAP

In 6TiSCH, UDP and CoAP are the default choices for transport and application layers UDP is an connection-less protocol, where data is sent quickly, but without any guarantees of successful reception. UDP allows point-to-multipoint traffic. This is very important for low-power wireless application where devices may get firmware updates over the air (OTA).

In the context of low-power wireless, verbose web-based and data model protocols are too heavy for IoT applications running on constrained devices. The industry has come up with new lightweight protocols such has CoAP. CoAP stands for Constrained Application Protocol, and as RPL and 6LoWPAN, is a IETF protocol produced by the CoRE (Constrained RESTful Environment) WG. The CoAP protocol [59] defines a simple and flexible message format which facilitates the interaction between web services, embedded sensors and embedded actuators. It provides low overhead and its format is simple to parse. These characteristics facilitate the processing tasks of constrained devices.

2.4 State of the Art in Low-Power Wireless Deployments

This section reviews previously published studies on the performance of sub-GHz and low data rate low-power wireless solutions. We pay particular attention to communication range.

Low-power wireless is a wide subject with around two decades of intensively research and experience. We don't attempt to create an exhaustive list of deployments and benchmarking efforts, but rather present the subset which, to the best of our knowledge, is the most informative and revealing.

Thelen et al. [60] present an early extensive set of measurements taken in a potato field of 154 m × 105 m in order to study how the environmental conditions affects the performance of the radio communications. For their experiment they used 13 Mica2Dot nodes with a Chipcon CC1000 radio chip in the 433 MHz band, working with a FSK modulation, 19.2 kbps and +10 dBm TX power. Nodes are placed on the ground and the antennae are at a height of 11 cm. While one node transmits, all other nodes listen and store the number of received packets and their Received Strength Signal Indicator (RSSI) value. The authors show that radio waves propagate better in high humidity, e.g. during rain and at night. They concluded that for reliable communication (RSSI $\geq$ -90 dBm), nodes need to be separated for at most 10 m during blooming (potato plants grow to be approx. 1 m high), and 23 m when the crop is on its return.

Hartung et al. [61] described FireWxNet, an hybrid wireless system to monitor weather conditions. This system allows fire fighters to measure fire and weather conditions in order to predict fire behavior and reduce the damage caused by these events. Two sensor networks are deployed in the Bitterroot National Forest. The nodes are Mica2, featuring a Chipcon CC1000 radio operating at 900 MHz, with a maximum TX power of +10 dBm. Nodes are mounted on a tripod 1.5 m from the ground, and are located on the surface of the Hell's Half Acre and Kit Carson mountains, at different heights. Stable radio links up to 400 m are formed.

Lazarescu [62] describe the design considerations of a low cost low-power wireless solution for wildfire monitoring. A 50-node network is deployed, using the 433 MHz frequency band. Nodes connect to a gateway embedded inside a wooden birdhouse with solar panels on the top. The antenna of the gateway is left inside the box. This choice drastically reduces the quality of the radio links between gateway and sensor nodes, allowing communication ranges only up to 70 m.

Cerpa et al. [63] presented SCALE, a measurement visualization tool that allows the collection of packet delivery statistics, and can help engineers to determine the data capacity and latency of the system. They use the same micro-controller with two types of radios, a RFM TR1000 and a Chipcon

CC1000. The former operates at 916 MHz, at 13.3 kbps, and with a Amplitude Shift Keying (ASK) modulation. The latter operates at 433 MHz, at 19.2 kbps, and with FSK modulation. The authors show that radio links of 50 m with PDR over 60% are achieved in outdoor environments, with a 0 dBm TX power with the TR1000 radio. Due to the lack of more hardware, they could not test over longer distances. They conclude that there is no evident correlation between PDR and distance for more than 50% of the communication range.

There are a handful of studies focusing specifically on IEEE802.15.4g, and therefore perfectly in line with the work presented in this manuscript.

Sum et al. [64] evaluate the performance of a WPAN when using IEEE802.15.4, IEEE802.15.4e and IEEE802.15.4g for smart utility networks through simulations.

Dias et al. [65] deploy a low-power wireless network in office, canteen and warehouse buildings in a smart grid application, and evaluate the performance of a single radio setting (O-QPSK, 250 kbps, 2 MHz channel bandwidth).

Mochizuki et al. [66] propose an enhancement to a conventional Wi-SUN system by increasing the transmission power of the downlink communication, and using a 2-FSK 100 kbps setting for their system tested in the city of Kyoto.

Sum et al. [67] study the communication and interference range for deployments for IEEE802.15.4g Smart Utility Network (SUN) devices in low and high dense environments (from 10 to 2500 devices per square kilometer). Based on realistic channel models, and assuming FSK modulation with -90 dBm sensitivity, the authors conclude that the communication range in urban environments (PER $\leq$ 1%) for SUN devices is 33 m, 65 m and 104 m when using 2.4 GHz, 915 MHz and 460 MHz frequency bands, respectively.

Bragg et al. [68] deploy six sensor nodes and two dedicated routing nodes in the Cairngorm Mountains, in Scotland. The Zolertia Z1 sensor mote with a CC1120 radiochip is used. Motes are separated into two clusters covering one kilometer square area. The border router is located 3.5 km away of the closest router. The data rate is 50 kbps. The deployment shows that the radios can provide a single hop communication over that distance. By using a Line-of-Sight propagation model for a CC2420 radio (implementing O-QPSK PHY, 250 kbps at 2.4 GHz), the authors determine at least 25 routing nodes would be necessary to cover the same area using a 2.4 GHz solution.

Through simulations and outdoor experimentation, Kojima et al. [69] investigate the feasibility of employing the Gaussian FSK PHY under multipath conditions in a suburban area. With transmitter and receiver operating at 413 MHz, with a BPSK modulation and a TX power of +10 dBm, the radio signal is received with a power level of -60 dBm. Results show that for a frame length of 1500 B, PER $\leq$ 10 % and considering a receiver sensitivity

of -100 dBm, the coverage area of the radio link is few hundred meters.

Discussion

All these IEEE802.15.4g studies and experiments have something in common: they only consider a single radio setting. What is missing from the state-of-the-art is a comparative performance evaluation of *all* possible radio settings of IEEE802.15.4g, with a particular focus on communication range, performance and limits for different scenarios. Chapter 4 answers just that. In it, we test all IEEE802.15.4g PHYs in different scenarios where a wide range of applications can take place.

2.5 State of the Art in Testbeds

Several institutional testbeds have been built over the last decade, and are available to the research community to run experiments. We are in particular interested in low-power wireless testbeds, which are composed of 10's to 100's of low-power wireless devices and used to develop IoT applications. Here we detail the three testbeds we believe are the most advanced in terms or infrastructure and real indoor-outdoor use-case scenarios. For a more exhaustive survey of testbeds, we recommend the work done by Tonneau *et al.* [70].

One of the most advanced testbeds is the SmartSantander project [71], a 20,000 node, city-scale testbed which is installed in indoor and outdoor areas in the cities of Santander (Spain), Guildford (UK), Lubeck (Germany) and Belgrade (Serbia). The nodes include IEEE802.15.4 devices and GPRS modules. Only nodes which are mains powered are available to be (re-)programmed over-the-air through a second IEEE802.15.4 transceiver. The strength of the SmartSantander testbed is that it is deployed in an actual smart city environment, increasing the confidence one can have in the result it yields.

FIT IoT-lab [26] is a federation of open-source testbeds located across 6 cities in France, and composed of 2728 low-power wireless devices. A user can request an account, then reserve an arbitrary number of nodes for an arbitrary amount of time to conduct an experiment. Using that account, a user can log into a central Linux machine, in which she can recompile her binary. When an experiment is running, the user has bare-metal access to the low-power wireless devices, and she can load any arbitrary on any node. In the back-end, each low-power wireless device is connected to a single-board computer, which itself is wired into the testbed network over a dedicated Ethernet network with Power-over-Ethernet capabilities. The back-end consist of a series of servers, some local to each deployment site, and interconnected to a central set of servers in Paris. The filesystem of the single-board computers is mapped over NFS to the user's Linux account,

resulting in very powerful logging capabilities. The user also has the option of doing in-circuit debugging on each low-power wireless device, over JTAG. Moreover, each device is equipped with dedicated hardware to monitor instantaneous power consumption. At the heart of that system is an Analog-to-Digital Converter chip connected to a series resistor.

FIT IoT-lab is arguably the most full-featured IoT testbed available today. But that comes at a price. First, because of the dedicated wiring, Power-over-Ethernet and NFS mapping, each of the 6 testbeds requires a dedicated Ethernet network to be put up across the deployment site. Because of the NFS mapping, the amount of data transitioning over that network is high, and piggy-backing the testbed traffic over the already existing Ethernet or WiFi network in the building was not an option. A side-effect of that is that, in most deployments, all devices are deployment in a single room, with the unfortunate side-effect that the wireless environment is very stable and not generally representative of a deployment done across an entire building. Finally, because of the feature-rich hardware needs (e.g. JTAG to all boards, power consumption measurement), FIT IoT-lab nodes are custom-made hardware. The unfortunate side-effect is that the low-power devices are not off-the-shelf, so a researcher outside of the FIT IoT-lab consortium cannot buy a handful of the same boards for local development.

The EWSN conference has featured a competition on each edition from 2016, organized by Boano *et al.* [72]. This competition has been the catalyst for creating and maintaining a testbed, which is evolving at each edition. The testbed consists of 51 TelosB low-power wireless devices deployed across a building at TU Graz, in Austria. Each TelosB is connected to a Raspberry Pi which runs the management software. The team has developed an open-hardware interface board between the Raspberry Pi and the TelosB to monitor energy consumption. The back-end solution consists of a very complete set of services custom made for the competition. Competitors submit a binary image they have developed outside of the testbed. That image is then loaded into the boards and an experiment runs for a pre-set duration. After the experiment, the testbed outputs the key performance indicators (latency, reliability, power consumption) that are used to rank the competitors.

A drawback that is often raised about testbeds is that the connectivity between the nodes does not represent that of a real-world deployment. That is because the deployment is done in a single room, and/or far from any source of interference. This means the wireless links exhibit a very good quality and very little variation over time. Brun *et al.* [73] have recorded the quality of the links between nodes both in testbeds and real-world deployment. From the analysis of the latter, they identify the three phenomena that often appear: external interference, multi-path fading and dynamism in the connectivity between nodes. They then develop a tool that verifies whether those as present in a testbed, and thereby quantify the "realism" of

different testbed deployments.

2.6 Summary

More than 20 years of experience in constrained low-power wireless has resulted in a myriad of IoT solutions. New technologies such as LoRaWAN, Sigfox and NB-IoT are being considered for LPWAN applications, as they support simple star topology deployments that can cover entire cities. However, these technologies cannot provide any sort of determinism nor reliability to the applications they serve. Other not-so-new technologies based on IEEE802.15.4 - TSCH can provide reliability and determinism while supporting more complex mesh topologies. With the emergence of IEEE802.15.4g, targeting to increase the length or radio links, and the combination with TSCH, we believe that **city-scale mesh deployments** are feasible.

This is the overall goal that we present in this manuscript. Chapter 3 starts by exposing the methodology we have been following to carry out this research. Chapter 4 presents the results on a experimental campaign where we look at the performance of IEEE802.15.4g outdoors. Chapter 5 focus on indoor applications, and whether OFDM is useful in that context. Chapter 6 goes one step further, and shows that, in that context, coupling OFDM with channel hopping makes perfect sense. Chapter B presents the 80-mote testbed we have deployed at Inria-Paris, composed of the technology-agile OpenMote B boards. Chapter 7 discusses the opportunities of frequency agility, and discusses the impact this has on the protocol stack. Finally, Chapter 8 concludes this manuscript and presents avenues for future work.

Chapter 3

Methodology

IEEE802.15.4g does not introduce new modulations or physical-layer capabilities. That being said, it brings exciting new capabilities to a protocol stack that runs above it, especially when compared to more traditional 2.4 GHz IEEE802.15.4.

First, IEEE802.15.4g operates at sub-GHz frequencies, and therefore features a longer range, perfectly appropriate for smart utility applications. IEEE802.15.4g is therefore the core technology for the Wi-SUN alliance. This is also why it is considered by the IETF IPv6 over Low Power Wide-Area Networks (lpwan) WG as a long-range technology, together to Sigfox, NB-IoT and LoRaWAN [1].

Second, the diversity on the 31 PHYs supported by IEEE802.15.4g brings some interesting trade offs: FSK and O-QPSK modulations offer long radio links with very low data rates, or shorter radio links with high data rates offered by OFDM.

Third, the incorporation of the OFDM PHYs into constrained devices is a novelty. The properties of this technology makes it, in theory, very appealing for networks deployed in challenging environments where high interference and multi-path fading are present.

These capabilities open new horizons for research that was until now outside of the realm of low-power wireless networking. Surprisingly, there is little work which involves with real deployments with real use-case scenarios using the entire set of capabilities of IEEE802.15.4g.

This is why we consider that a first step for understanding the capabilities and uses of the technology is to conduct field experiments with off-the-shelf hardware. In Chapter 4, we conduct experiments to evaluate the performance of the IEEE802.15.4g in sub-GHz bands, using IEEE802.15.4g compliant hardware in outdoor use cases. The results allow us to provide recommendations on which radio setting to use, given a target distance, reliability and throughput. This allows us to have a clear view over the trade-offs

[1] https://datatracker.ietf.org/wg/lpwan/about/

between data rate and range.

In Chapter 5, we analyse the use of IEEE802.15.4g OFDM in sub-GHz bands for indoor applications. We use as a reference the ruling technology for indoor applications, the IEEE802.15.4 O-QPSK at 2.4 GHz. The results determine whether IEEE802.15.4g OFDM is a valid candidate for these applications

From Section 2.2 we learn that frequency diversity brings reliability. OFDM technology offers this but, unlike TSCH, it does it at the physical layer. Therefore another question rises: *should we still use a TSCH MAC approach when using a OFDM PHY?* In Chapter 6, we compare IEEE802.15.4 O-QPSK against the IEEE802.15.4g -OFDM in the 2.4 GHz band. We want to determine whether both technologies are affected by the same challenges by looking the evolution of the PDR during the experiment. The experiment also shows a direct comparison of both technologies under the conditions. From these experiments, we learn how to use IEEE802.15.4g OFDM (MAC approach) and where it stands against IEEE802.15.4 O-QPSK. All these "lessons learnt" are rooted in in-site real-world experimentation and measurements.

The remainder of this chapter describes the tools we use for conducting these studies, and details the work we carried on.

3.1 Tools Used in Range Measurements

Chapters 4, 5 and 6 represent the technical contributions of this work, derived from experiments in realistic use-case scenarios. This section describe the tools we use in these experiments.

3.1.1 Experimental Apparatus

System-on-Chip (SoC) solutions with radio interface being *fully* IEEE802.15.4g compliant were not available at the beginning of this thesis[2]. Therefore, we assembled our own **nodes** with different pieces of commercial off-the-shelf hardware to carry on experiments and evaluate the technology.

A node consists of an ATREB215-XPRO-A radio board evaluation kit, a Raspberry Pi 3 (rPi) model B, two 2 dBi omni-directional antennae, a GPS module[3] and a push button; all housed in a plastic box. Fig. 3.1 depicts a node. The rPi controls the radio board through am SPI bus. The rPi can be either mains powered or powered by a battery bank. For outdoors experiments, we use a 22,000 mAh battery bank. In all conducted experiments, nodes are mounted on a 1.8 m tripod. Fig. 3.2 depicts a node during an experiment.

[2] Some solutions such as the CC1200 are available but they do not implement the entire IEEE802.15.4g standard

[3] For outdoors measurement campaigns.

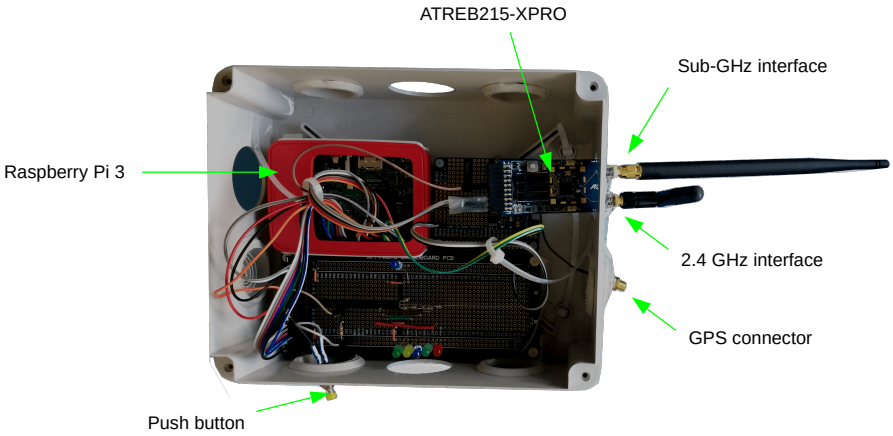


Figure 3.1: A node used throughout the field experiments.

ATREB215-XPRO-A: This radio board features an AT86RF215 radio chip implementing both the IEEE802.15.4 - PHY and the IEEE802.15.4g PHYs. It contains two transceivers, one for sub-1GHz frequencies and the other for the 2.45 GHz frequency band. It has two SMA connectors, one for each transceiver, where we connect two 2 dBi 1/2 wavelength whip antennae. It is driven through an SPI bus. It is powered by +3 V from the rPi. Table 3.1 shows the sensitivity for each radio setting in the sub-GHz transceiver.

Raspberry Pi: Each rPi runs a Linux Debian distribution. Through an SPI bus, it drives the radio board and configures it on each PHY to be tested. For every experiment conducted, it stores the results into a system file in a JSON format. The scripts the rPi uses to execute the experiments and to drive the radio board are written in Python.

GPS module: We use the Ultimate GPS module from Adafruit, with an external u.FL connector to an active GPS antenna. This module is built around the MTK3339 GPS chipset. It provides the rPi with the GMT Time and the position. Each rPi has the same System time, making tightly synchronization possible.

3.1.2 Radio Driver

We develop the radio driver to drive the ATREB215 XPRO radio board through the field experiments. The radio driver is written in Python, and it is in charge of taking the AT86RF215 radio chip over the different states (see fig 3.3) through SPI commands. Within the node, the rPi plays the role of the master and the AT86RF215 radio chip plays the role of slave. Following the data sheet guidance, we configured the front-end of the radios to implement each of the PHY specified in IEEE802.15.4g. This is done by modifying the registers of the AT86RF215 radio chip. The result is 31 different PHY

Table 3.1: Radio characteristics of the ATREB215 XPRO Extension board featuring the AT86RF215 radio chip. For each item in the PHY column, the table specifies the maximum TX power allowed by the hardware, its current consumption when transmitting at maximum power, the receiver sensitivity with the condition in which this value is obtained and the link budget for each PHY (considering the 2 dBi antennae connected to the radios). PSDU stands for Packet Service Data Unit and is the PHY payload. PER stands for Packet Error Rate. TX power was set to the maximum allowed by the hardware.

PHY	**Max TX power**	**Current Comsumption @max TX power**	**Receiver Sensitivity**	**Sensitivity Condition**	**Link Budget**
2FSK-50	+14 dBm	84.1 mA	-109 dBm	PSDU length	127 dB
2FSK-100	+14 dBm	83.9 mA	-106 dBm	250 B	124 dB
4FSK-200	+14 dBm	83.6 mA	-96 dBm	PER $< 10\%$	114 dB
2FSK-FEC-50	+14 dBm	83.7 mA	-114 dBm		132 dB
2FSK-FEC-100	+14 dBm	83.6 mA	-111 dBm		129 dB
4FSK-FEC-200	+14 dBm	83.7 mA	-104 dBm		122 dB
OFDM1-100	+10 dBm	75.6 mA	-109 dBm	PSDU length	123 dB
OFDM1-200	+10 dBm	75.6 mA	-109 dBm	250 B	123 dB
OFDM1-400	+10 dBm	75.6 mA	-107 dBm	PER $< 10\%$	121 dB
OFDM1-800	+10 dBm	76 mA	-104 dBm		118 dB
OFDM2-50	+10 dBm	76.5 mA	-111 dBm		125 dB
OFDM2-100	+10 dBm	76.5 mA	-111 dBm		125 dB
OFDM2-200	+10 dBm	76.7 mA	-108 dBm		122 dB
OFDM2-400	+10 dBm	76.7 mA	-106 dBm		120 dB
OFDM2-600	+10 dBm	76.8 mA	-104 dBm		125 dB
OFDM2-800	+10 dBm	77.1 mA	-101 dBm		115 dB
OFDM3-50	+10 dBm	76 mA	-113 dBm		127 dB
OFDM3-100	+10 dBm	76.1 mA	-109 dBm		123 dB
OFDM3-200	+10 dBm	76.1 mA	-107 dBm		121 dB
OFDM3-300	+10 dBm	75.3 mA	-106 dBm		120 dB
OFDM3-400	+10 dBm	75.8 mA	-102 dBm		116 dB
OFDM3-600	+10 dBm	76 mA	-97 dBm		111 dB
OFDM4-50	+11 dBm	75.8 mA	-111 dBm		126 dB
OFDM4-100	+11 dBm	75.8 mA	-109 dBm		124 dB
OFDM4-150	+11 dBm	75.8 mA	-108 dBm		123 dB
OFDM4-200	+11 dBm	75.8 mA	-105 dBm		120 dB
OFDM4-300	+11 dBm	75.8 mA	-101 dBm		116 dB
OQPSK-6.25	+14 dBm	84.1 mA	-123 dBm	PSDU length 20 B	141 dB
OQPSK-12.5	+14 dBm	84.1 mA	-121 dBm	PER $< 10\%$	139 dB
OQPSK-25	+14 dBm	84.1 mA	-119 dBm		137 dB
OQPSK-50	+14 dBm	84.1 mA	-117 dBm	PSDU length 250 B PER $< 10\%$	135 dB

Figure 3.2: A node in a field experiment. Nodes are mounted on a 1.8 m tripod.

configurations.

3.1.3 Experiment Scripts

The experiment scripts are written in Python. These have a series of tasks that need to be performed in precise moments (tenths of seconds accuracy) as the different nodes in the network need to be synchronize. For example, when the TX node starts sending packets with a given PHY configuration, the RX nodes MUST be already listening with the radios front-end configured in the very same PHY as the TX. Synchronization within the nodes comes from an external source, either GPS for outdoor experiments or NTP in indoor experiments. Schedules in the experiments have few seconds guard times to guarantee that RX nodes are listening and continue listening for the entire time the TX node is transmitting. After each PHY tested, the results are store into a file system as a JSON object.

3.1.4 Experimental Evaluation

We evaluate each radio link by looking at the Packet Delivery Ratio (PDR) of each PHY. This allows us to compare the performance of the PHYs tested against one another. By direct comparison, we can determine which PHY

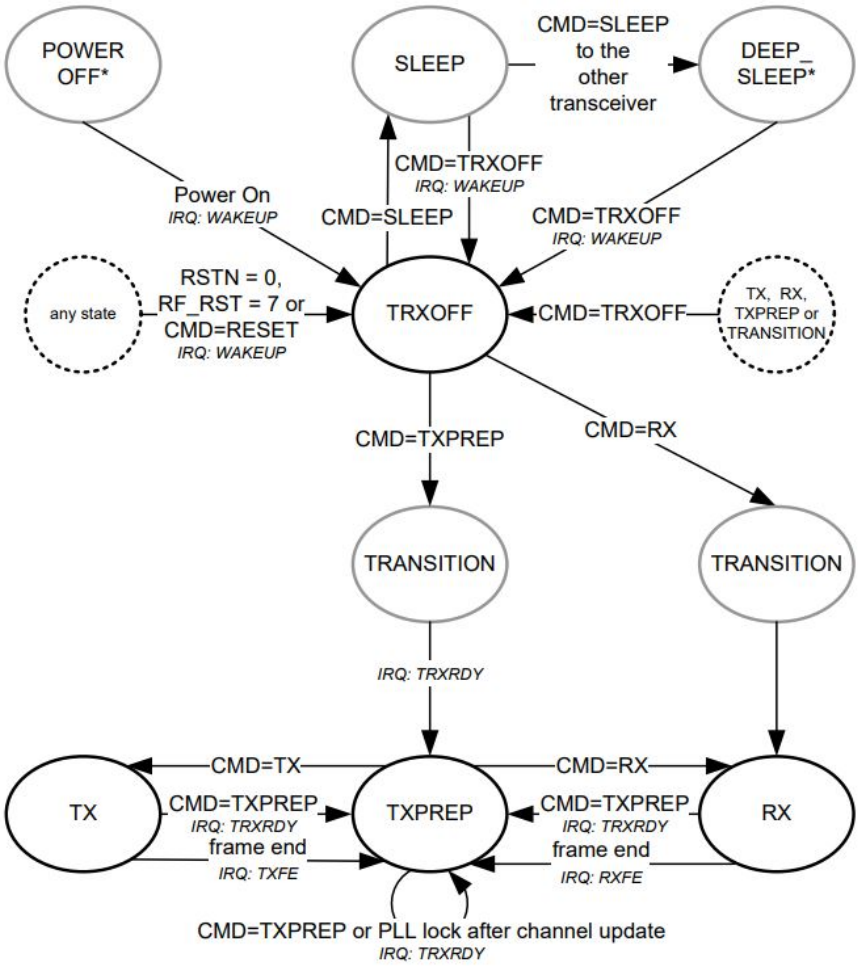


Figure 3.3: State machine of the radio chip AT86RF215. Image taken from the AT86RF215 datasheet [74].

makes the most sense for some use case. We take into account the sensitivity of each PHY in order to detect any inconsistency in the results. As the experiments take place in real use-case scenarios, we do **not** control the environment and therefore interference is expected.

Always considering the PDR, we also evaluate the evolution of this indicator over time. We can do this only indoors, where we can leave the experiments runnig continuously for several days.

3.2 Tools used in the OpenTestBed Platform

Chapter B describes the development of a wireless testbed. Here we describe the tools we use for that development.

3.2.1 Raspberry Pi

We use the rPi 3 model B+ for providing out of band control to the DUT. This model provides WiFi connectivity on 2.4 GHz and 5 GHz bands. This option is very handy for our testbed deployment because most of the devices uses the 2.4 GHz and we do not want that control/monitoring out-of-band messages to the Device Under Test (DUT) cause interference with the experiments been conducted, as WiFi communications can deteriorate the quality of radio links using IEEE802.15.4 [24]. This rPi provides 4 USB ports, where we can attached up to 4 DUT.

3.2.2 Message Queuing Telemetry Transport (MQTT)

MQTT is a lightweight and cost-effective protocol based on a client/server and publish/subscribe framework. It runs over TCP/IP. This protocol, developed by IBM and Arcom [4], is designed to work with reduced bandwidth and variable latency.

MQTT clients can act as publisher or subscribers. Acting as publishers, they send data to a MQTT broker. Acting as subscribers, they receive data from the MQTT broker. The subscribers tell the broker which information they want to receive. They *subscribe* to a topic and every time the broker receives a message with that topic, it will send the information to all devices who shown their interest in the topic. On the publisher side, every *published* message has a topic. Topics are related to an application and are useful to identify the data that is contained in the message. This is useful in the case the same device publishes data of different nature (e.g. temperature, humidity, brightness) and subscribers are interested in some of them.

MQTT provides three levels of quality of service (QoS):

QoS 0: this level is known as *"at most once"* delivery. It does not provide any guarantee of successful delivery since messages are not acknowledged.

[4]Later acquired by Eurotech.

Messages are sent to the broker only one time and this to the subscribers just once as well.

QoS 1: knows as *"at least once"* delivery. This level guarantees that messages are delivered at least once between publisher and broker, and then between broker and subscribers.

QoS 2: This is the highest level of quality of service, known as *"exactly once"* delivery. This level is used when no message loss/duplication is acceptable. It guarantees that messages are delivered just one time regardless the number of retries.

The MQTT flow of information is such that publishers and subscribers need not be aware of each other's existence. MQTT clients are responsible for setting the QoS level in their side of the communication. It can be the case that both sides of the MQTT flow have different QoS.

We use MQTT for out-of-band communication between the DUT and the user conducting the experiments. In our deployment, the MQTT clients are the rPis where the all DUT are connected and the user PC from which the experiments are set up. The MQTT server is a machine inside the Inria data server infrastructure.

3.3 Approach Taken and Thesis Structure

This thesis work is develop following an empirical approach. Our contributions derived from experiments conducted in real use-case scenarios and with off-the-shelf hardware, in conditions where IoT applications using low-power networks can take place.

The chapters 4, 5 and 6 represent the technical contributions of this work. These are extracted from analyzing the experiments results.

Chapter 7 presents an description of the impact Agile Networking has in the 6TiSCH protocol stack.

Chapter 8 summarizes the contributions of this thesis and presents the future work.

Chapter 4

Evaluation of IEEE802.15.4g and Recommendations for Outdoor Applications

Chapter 2 surveys studies of IEEE802.15.4g exploring its capabilities in sub-GHz bands on different scenarios. However, all these studies have something in common: they only consider one PHY at a time on their simulations/experiments.

This chapter focuses on providing a comparative performance evaluation, through experimentation, of all PHYs defined in IEEE802.15.4g, in the European 863-870 MHz band. We focus on communication range, performance and throughout, for scenarios where a wide range of outdoor applications can take place. Due to the extend amount of PHYs defined in this standard, we highlight the best performing PHYs according to high data rate and range.

4.1 Goals of this Study

Low-power wireless networks drastically decrease the cost of implementing monitoring/control systems. Wireless mesh networks are used over a wide spectrum of environmental observation applications such as smart agriculture, fire monitoring, seismic activity, snow-pack monitoring and more. The standard IEEE802.15.4 O-QPSK in 2.4 GHz is often used to provide connectivity between sensor nodes.

When sensors need to cover extended areas, repeater nodes are required to ensure enough density in the deployment. Example of this is seen in Malek *et al.* [75], where they need to install three times more repeaters than sensor nodes, incurring in an increase of cost and time of deployment.

In this type of networks, longer communication links between sensors are desired in order to reduce the amount of repeaters needed. Our hint is that the IEEE802.15.4g use in sub-GHz can be suitable for these networks, due to

its extended range in comparison with IEEE802.15.4 O-QPSK at 2.4 GHz [1]. But this longer range frequencies cannot be indiscriminately used: regional regulation bodies strongly limit the amount of time devices can transmit per unit of time [2].

In this chapter, we experiment with the complete IEEE802.15.4g standard in the 863-870 MHz band on different scenarios where outdoor monitoring applications are likely to take place. We thus make a comparison and analysis between all the PHYs considering their PDR, maximum range, energy consumed and amount of packets that can be transmitted under the European regulation.

4.2 Range Test Setup

The networking terms "PHY" and "radio setting" are interchangeably used. The purpose of these experiments is to measure the PDR between the TX node and the RX nodes at different distances for all the radio settings defined in IEEE802.15.4g. RX nodes are located at an increasing distance from the TX node, therefore we see the variation of the quality of the link versus the distance.

For carrying out these experiments, we use 4 nodes (all information about the node is in section 3.1.1), one configured as a TX and three RX. The characteristics of the ATREB215-XPRO-A are detailed in table 3.1.

For synchronization purposes, we use the Ultimate GPS module from Adafruit, with an external uFL connector to a active GPS antenna. This module is built around the MTK3339 GPS chip-set. It provides the rPi in the node with the GMT Time and the position. Each rPi has the same System time, making them tightly synchronized. We add a push button to each node to signal the start of each experiment. The nodes are powered by a 22,000 mAh battery bank.

Section 4.2.1 describe the software used in these range test experiments. Section 4.2.2 details the scenarios where the nodes were deployed.

4.2.1 Software

The experiment scripts are written in Python. When powering the nodes, the GPS modules are switched on and start listening for satellite signals. Once the GPS gets a locked signal, they feed the rPis with GMT time and position, enabling the experiment scripts to start. Then the tests script wait for the signal from the push button to start the experiment. When the signal is received, the scripts wait for the next change of minute to start the

[1] At the same TX power, the use of sub-GHz (863-860 MHZ) offer 2-3× longer range compared to its 2.4 GHz counterpart.

[2] See regulations in the annex.

experiment. They drive the radio board through an experiment, making the TX node loop over the 31 radio settings and sending burst of 100 frames with 127 B and 2047 B. On the RX nodes, the scripts configure the radio board with the same PHY and frequency as the TX node at the same time. Since the System time in the nodes is the same, GMT, fed by the GPS module, the nodes are tightly synchronized. Appropriate guard times are taken into account, in order to guarantee that the RX nodes are listening before the TX nodes start the frame transmission.

An **experiment** consists of the node sending 100 frames of 127 B and 100 frames of 2047 B, using the 31 radio settings shown in Table 3.1. 127 B is the maximum size of the previous version of the standard, defined in 2006, that uses O-QPSK with 250 kbps, and that can be used just as a comparison for the interested reader willing to perform the same experiments with that technology. 2047 B is the maximum size of the **g** amendment, and now appended to the standard as SUN-PHYs. The inter-frame spacing time is 20 ms.

RX nodes log, for each frame received, the radio setting and frequency it listens on, the RSSI value and the correctness of the FCS. This information is stored as a JSON object in a file system, in addition to the GPS information (position and time). Because 100 frames are sent on each radio setting and length, the PDR can be computed. [3]

4.2.2 Scenarios

The range test experiments are carried out in the city of Paris, France, in 4 scenarios, each being a likely IoT application environment. These are:

- Line of sight: nodes are deployed in the *Bois de Vincennes*, on a pedestrian 12 m wide route (*Rue Dauphine*). Dense vegetation area with several meters tall trees is placed at both sides of the route. The soil is covered with asphalt. No important obstruction between the TX and RX nodes during the length of the experiment with people occasionally crossing this path. Numerous IoT applications are foreseen in this scenario: monitoring natural resources on a prairie-like environment, smart metering in the country side, smart grid in rural areas, livestock monitoring, mining and more. Fig. 4.2 depicts the where the nodes were deployed and the distances between the nodes.

- Smart Agriculture: nodes are deployed in the *Parc de Vincennes*, next to the *Lac Daumesnil*. There are trees between the TX and RXs nodes, obstructing the direct path between the nodes. This scenario mimics IoT application environments such as: Smart agriculture, monitoring

[3] All the details of the test scripts can be found at https://github.com/openwsn-berkeley/range_test.

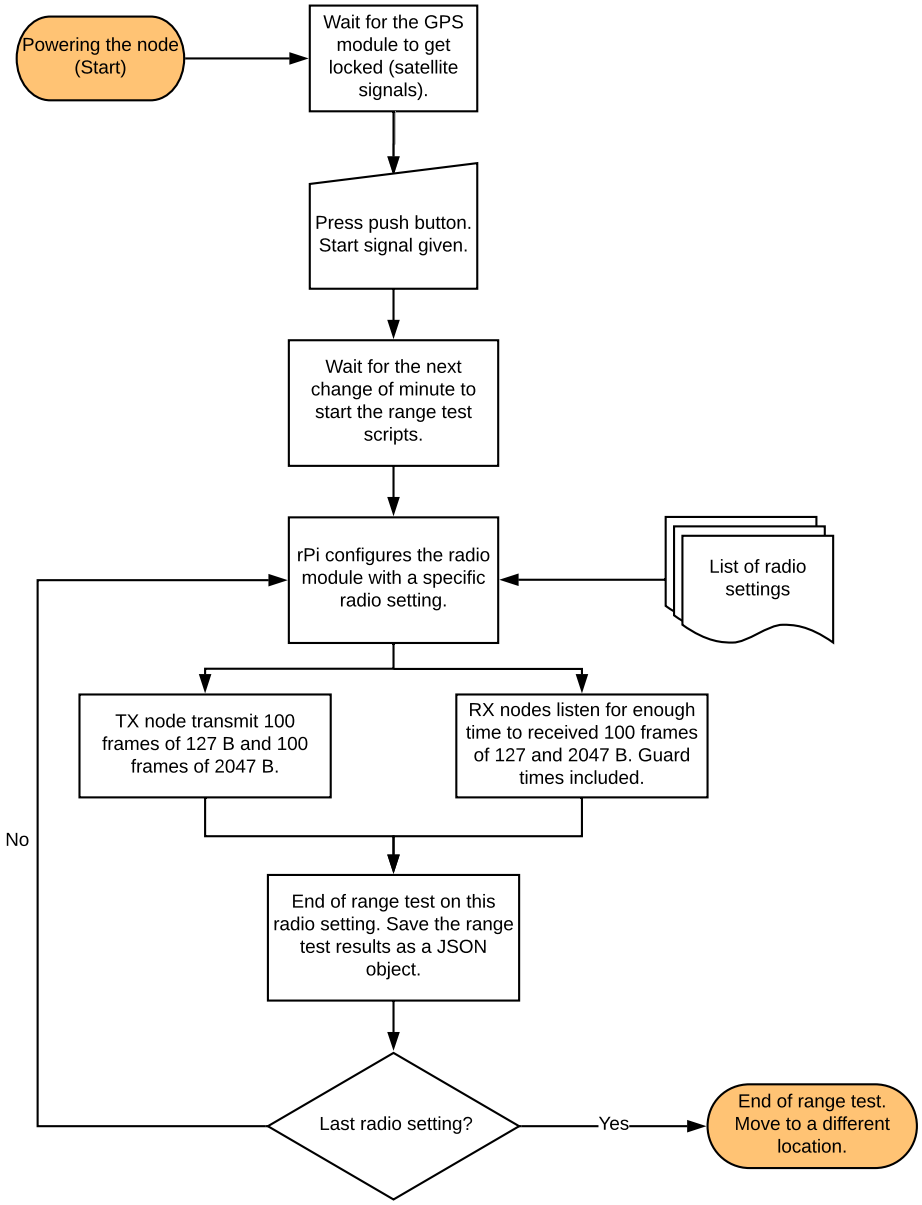


Figure 4.1: Diagram of the steps followed by each node during an experiment.

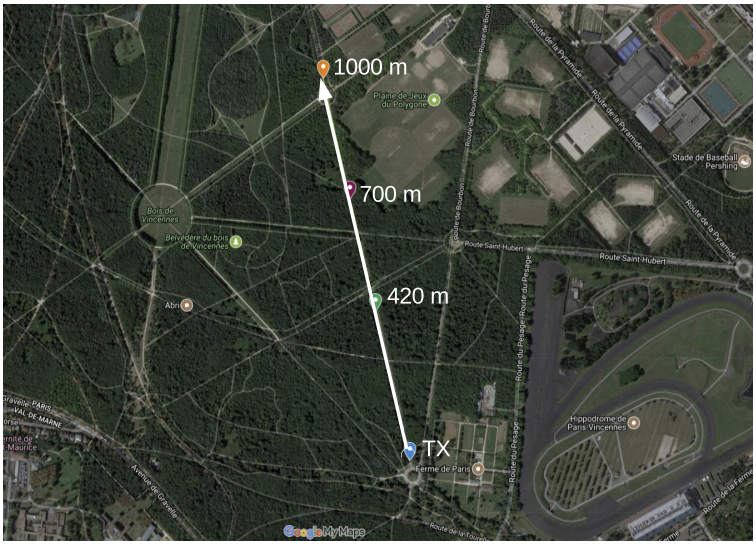


Figure 4.2: Line of Sight scenario.

natural resources on a forest-like environment, livestock monitoring on a vegetation-abundant terrain and more. Fig. 4.3 shows the deployment setup and the distances between the nodes.

- Urban canyon: we chose the *Avenue Daumesnil*, which is in the middle of a 35 m wide urban canyon. This is a hectic place, with people walking and automobiles transiting across and along the path between the nodes. Up to 10 storey buildings are found at both sides, and trees along the avenue. In this scenario is likely to find IoT applications related to smart cities: parking, metering, lighting, traffic control, pollution monitoring, etc. Fig. 4.4 depicts the node location and the distance between them.

- Advanced Metering Infrastructure: nodes are located along the street *Jorge Semprun*, next to the Inria buildings in Paris. The TX node is located at one extreme of the street and the RX nodes along the same street but "hidden" between buildings, so there is no LOS with the TX node. Urban Advanced Metering applications are deployed in this type of scenario. Fig. 4.5 details the position of the nodes and the distance between them.

Figure 4.3: Smart agriculture scenario.

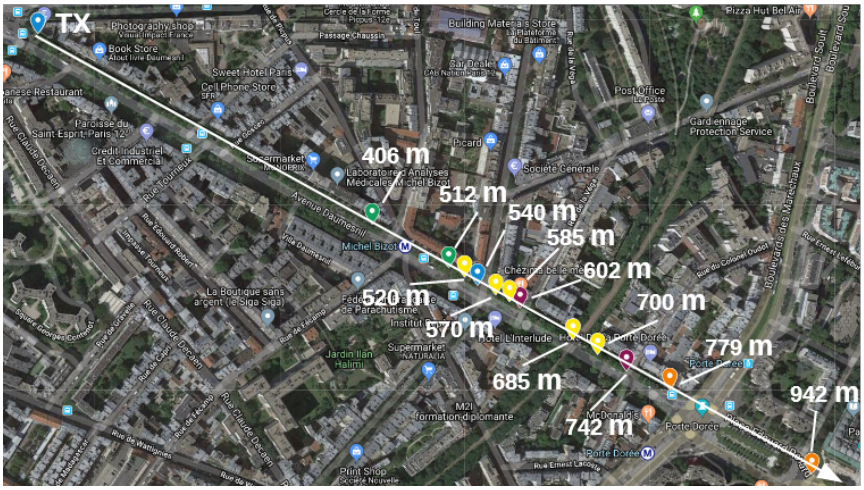


Figure 4.4: Urban canyon scenario.

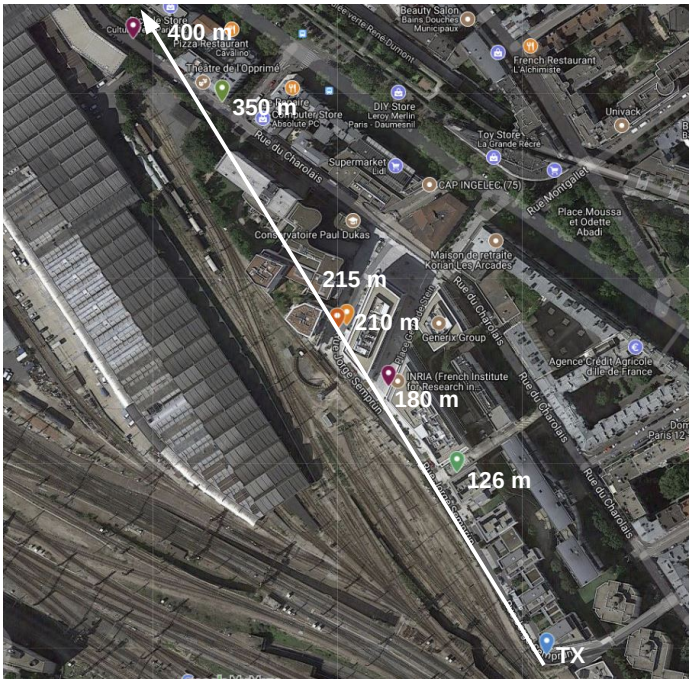


Figure 4.5: Urban environment scenario.

4.3 Results

This section provides the results as follows. We show the PDR value for every radio setting of every node on every scenario previously described. We use the terms useful PDR and high PDR for values of at least 50% and 75% respectively.

4.3.1 Line of Sight (LoS)

RX nodes are located at 420 m, 700 m and at 1000 m from the TX node. Table 4.1 shows the PDR value for the three RX nodes considering packets of 127 B and 2047 B. At 420 m, radio settings with high data rate have a PDR around 100%. At 700 m, the PDR stays between 70% and 100% for radio settings using FSK and O-QPSK. Radio settings using OFDM have a poor PDR, in most cases incapable of getting any frame across. The exception is OFDM2-100, with PDR of 92% for short frames and 47% for long frames.

The poor performance of OFDM at 700 m, in comparison to FSK and O-QPSK PHYs is due to that the TX power is not the same for all radio settings. According to Table 3.1, the maximum TX power for OFDM radio settings is +11 dBm whereas for the rest is +14 dBm. The robustness of OFDM can be shown in strong multi-path environments (e.g., dense cities),

Table 4.1: Line of Sight. PDR considering packets of 127 B and 2047 B for each RX node. High data rates with high PDR are achieved at least up to 420 m from the TX node. Maximum length of the radio link is close to 700 m.

PHY Alias	**RX at 420 m PDR 127 B–2047 B**	**RX at 700 m PDR 127 B–2047 B**	**RX at 1000 m PDR 127 B–2047 B**
2FSK-50	100%–100%	83%–58%	0%–0%
2FSK-100	100%–100%	76%–0%	0%–0%
4FSK-200	100%–99%	0%–0%	0%–0%
2FSK-FEC-50	100%–100%	95%–94%	0%–0%
2FSK-FEC-100	100%–100%	100%–79%	0%–0%
4FSK-FEC-200	100%–100%	73%–38%	0%–0%
OFDM1-100	100%–100%	31%–5%	0%–0%
OFDM1-200	100%–100%	0%–18%	0%–0%
OFDM1-400	100%–100%	0%–0%	0%–0%
OFDM1-800	100%–100%	0%–0%	0%–0%
OFDM2-50	99%–98%	23%–59%	0%–0%
OFDM2-100	100%–98%	92%–47%	0%–0%
OFDM2-200	100%–100%	0%–0%	0%–0%
OFDM2-400	100%–99%	0%–0%	0%–0%
OFDM2-600	100%–100%	0%–0%	0%–0%
OFDM2-800	98%–51%	0%–0%	0%–0%
OFDM3-50	100%–100%	34%–26%	0%–0%
OFDM3-100	100%–100%	0%–0%	0%–0%
OFDM3-200	100%–100%	0%–0%	0%–0%
OFDM3-300	100%–100%	0%–0%	0%–0%
OFDM3-400	100%–97%	0%–0%	0%–0%
OFDM3-600	26%–0%	0%–0%	0%–0%
OFDM4-50	100%–98%	35%–11%	0%–0%
OFDM4-100	98%–99%	1%–1%	0%–0%
OFDM4-150	100%–99%	8%–0%	0%–0%
OFDM4-200	99%–100%	0%–0%	0%–0%
OFDM4-300	97%–63%	0%–0%	0%–0%
OQPSK-6.25	100%–99%	100%–98%	27%–1%
OQPSK-12.5	100%–100%	94%–94%	2%–1%
OQPSK-25	100%–100%	100%–83%	0%–0%
OQPSK-50	100%–99%	100%–100%	0%–0%

where singled-carrier radio signals would suffer from self-Interference caused by multiple rays of the same symbol arriving at different time and interfering with subsequent symbols. Here it is not the case. We see how singled-carrier signals have a good PDR and OFDM PHYs do not. Therefore, the low performance of OFDM is due to the attenuation the radio signal suffers through the path towards the RX node.

At 1000 m, the radio link is almost nonexistent, not useful for data exchange.

4.3.2 Smart Agriculture Scenario

In this scenario, the experiment is run twice during the same day and with equal weather conditions. RX nodes are located at 213 m, 439 m and 615 m from the TX node on the first run and at 337 m, 538 m and 715 m on the second run. Table 4.2 shows the PDR for all the RX nodes, for packets of 127 B and 2047 B. High data rates radio setting with high PDR are achievable at least up to 337 m. At 615 m, the radio link allows communication of at least 50 kbps with high PDR value. At 715 m, only OQPSK-12.5 present a high PDR for short packets.

4.3.3 Urban Canyon

In this scenario we collect measurements from 12 locations, between 406 m and 942 m and within 3 non-consecutive days with similar conditions (sunny days, at noon). Tables 4.3 and 4.4 show the PDR for packets of 127 B and 2047 B on each RX node location.

In this scenario, interference and multi-path fading are expected since this is a high populated area with many buildings along the street, with smart metering devices already implemented and other applications accessing the same frequency band. As shown in Table 4.3, the PDR for OFDM2 is lower at 406 m than at 512 m. An explanation for this is external interference. These two measurements were not taken at the same moment, and we can also see that the interference was present during the transmission of packets with OFDM2-50, OFDM2-100, OFDM2-200 and OFDM2-400. Before and after that time, PDR rose to values close to 100%. In addition, for the following node locations, these high values are maintained.

After 540 m, there is a negative slope in the street level and after 685 m there is a viaduct which is perpendicular to the avenue Daumesnil. High data rates with high PDR are achieved at least up to 540 m, and the maximum coverage of the radio link is around 780 m.

4.3.4 Advanced Metering Infrastructure

In this scenario, we run the experiment twice during non-consecutive days having similar weather conditions. In the first run, RX nodes are located at

Table 4.2: Smart Agriculture. PDR for packets of 127 B and 2047 B for each RX node. Maximum coverage with high data rate happens at 337 m and maximum length of the radio link with useful PDR and data rate of at least 50 kbps is at 615 m.

PHY Alias	RX at 213 m PDR 127 B–2047 B	RX at 337 m PDR 127 B–2047 B	RX at 439 m PDR 127 B–2047 B	RX at 538 m PDR 127 B–2047 B	RX at 615 m PDR 127 B–2047 B	RX at 715 m PDR 127 B–2047 B
2FSK-50	100%–96%	100%–100%	31%–33%	0%–0%	5%– 11%	0%–0%
2FSK-100	100%–100%	100%–100%	0%–2%	0%–0%	0%–0%	0%–0%
4FSK-200	99%–100%	100%–100%	0%–0%	0%–0%	0%–0%	0%–0%
2FSK-FEC-50	100%–98%	100%–100%	100%–100%	0%–33%	98%–64%	0%–0%
2FSK-FEC-100	100%–100%	100%–91%	85%–32%	23%–6%	0%–0%	0%–0%
4FSK-FEC-200	100%–100%	100%–60%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM1-100	100%–99%	100%–100%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM1-200	100%–99%	100%–100%	0%–0%	0%–0%	52%–1%	0%–0%
OFDM1-400	100%–100%	100%–100%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM1-800	100%–100%	100%–100%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM2-50	100%–100%	100%–100%	5%–5%	0%–0%	17%–14%	0%–0%
OFDM2-100	100%–99%	98%–100%	0%–0%	0%–0%	81%–1%	0%–0%
OFDM2-200	73%–98%	100%–99%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM2-400	99%–100%	100%–100%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM2-600	99%–99%	99%–100%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM2-800	99%–100%	97%–40%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM3-50	100%–100%	100%–100%	49%–0%	0%–0%	4%–3%	0%–0%
OFDM3-100	100%–100%	100%–92%	4%–0%	0%–0%	0%–0%	0%–0%
OFDM3-200	100%–100%	100%–100%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM3-300	100%–100%	100%–86%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM3-400	100%–99%	99%–97%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM3-600	100%–100%	84%–36%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM4-50	99%–98%	100%–100%	3%–3%	0%–0%	0%–0%	0%–0%
OFDM4-100	100%–100%	100%–100%	14%–0%	0%–0%	0%–0%	0%–0%
OFDM4-150	100%–99%	100%–100%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM4-200	100%–99%	99%–95%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM4-300	89%–99%	44%–75%	0%–0%	0%–0%	0%–0%	0%–0%
OQPSK-6.25	100%–100%	100%–100%	100%–96%	44%–37%	100%–87%	22%–64%
OQPSK-12.5	100%–100%	100%–100%	94%–97%	91%–31%	90%–90%	91%–35%
OQPSK-25	100%–100%	100%–100%	100%–100%	47%–34%	92%–100%	4%–14%
OQPSK-50	100%–100%	100%–100%	100%–100%	56%–13%	100%–99%	0%–34%

Table 4.3: Urban Canyon. PDR for packets of 127 B and 2047 B for each RX node, for node locations from 406 m to 585 m. Up to 520 m, all radio settings present a PDR over 50%. PDR of high data rates decay at 540 m.

PHY Alias	RX at 406 m PDR 127 B–2047 B	RX at 512 m PDR 127 B–2047 B	RX at 520 m PDR 127 B–2047 B	RX at 540 m PDR 127 B–2047 B	RX at 570 m PDR 127 B–2047 B	RX at 585 m PDR 127 B–2047 B
2FSK-50	100%–68%	100%–100%	100%–98%	95%–84%	7%–0%	92%–30%
2FSK-100	100%–100%	100%–98%	100%–93%	99%–95%	41%–0%	89%–21%
4FSK-200	94%–100%	100%–99%	93%–99%	98%–87%	0%–0%	0%–0%
2FSK-FEC-50	88%–100%	98%–97%	100%–100%	100%–93%	92%–84%	91%–86%
2FSK-FEC-100	100%–100%	100%–100%	100%–99%	100%–96%	91%–69%	98%–78%
4FSK-FEC-200	100%–100%	100%–99%	100%–100%	100%–95%	42%–26%	78%–39%
OFDM1-100	96%–99%	83%–89%	97%–85%	96%–80%	0%–0%	7%–0%
OFDM1-200	96%–99%	98%–92%	100%–84%	99%–83%	0%–0%	0%–0%
OFDM1-400	90%–90%	36%–61%	99%–94%	97%–91%	0%–0%	0%–0%
OFDM1-800	43%–87%	68%–68%	98%–98%	97%–79%	0%–0%	0%–0%
OFDM2-50	72%–58%	97%–76%	97%–86%	97%–86%	1%–1%	6%–6%
OFDM2-100	17%–59%	97%–88%	99%–93%	97%–86%	0%–0%	58%–4%
OFDM2-200	72%–61%	84%–93%	98%–93%	95%–76%	0%–0%	0%–0%
OFDM2-400	41%–57%	40%–42%	99%–95%	91%–92%	0%–0%	0%–0%
OFDM2-600	98%–98%	29%–0%	98%–97%	97%–88%	0%–0%	0%–0%
OFDM2-800	88%–96%	99%–94%	97%–90%	84%–11%	0%–0%	0%–0%
OFDM3-50	97%–92%	97%–85%	100%–84%	97%–75%	23%–1%	56%–8%
OFDM3-100	95%–90%	82%–90%	98%–93%	99%–93%	2%–0%	10%–0%
OFDM3-200	100%–99%	99%–84%	99%–96%	99%–92%	0%–0%	1%–0%
OFDM3-300	100%–89%	98%–86%	100%–93%	98%–84%	0%–0%	0%–0%
OFDM3-400	99%–89%	99%–88%	89%–64%	86%–42%	0%–0%	0%–0%
OFDM3-600	100%–82%	98%–89%	90%–58%	21%–0%	0%–0%	0%–0%
OFDM4-50	100%–100%	99%–100%	100%–99%	99%–91%	9%–0%	33%–8%
OFDM4-100	100%–100%	98%–98%	99%–100%	97%–96%	0%–0%	33%–0%
OFDM4-150	99%–80%	98%–100%	94%–98%	95%–91%	0%–0%	31%–0%
OFDM4-200	100%–88%	99%–86%	100%–88%	93%–22%	0%–0%	0%–0%
OFDM4-300	99%–99%	100%–92%	88%–72%	60%–31%	0%–0%	0%–0%
OQPSK-6.25	94%–85%	91%–49%	97%–55%	97%–81%	60%–12%	89%–7%
OQPSK-12.5	93%–86%	86%–59%	96%–56%	97%–56%	73%–4%	82%–12%
OQPSK-25	95%–63%	91%–61%	96%–75%	95%–61%	23%–6%	57%–14%
OQPSK-50	91%–74%	90%–76%	99%–86%	98%–84%	41%–19%	67%–48%

Table 4.4: Urban Canyon. PDR for packets of 127 B and 2047 B for each RX node for node locations from 602 m to 942 m The limit of the radio link is at 779 m.

PHY Alias	RX at 602 m PDR 127 B–2047 B	RX at 685 m PDR 127 B–2047 B	RX at 700 m PDR 127 B–2047 B	RX at 742 m PDR 127 B–2047 B	RX at 779 m PDR 127 B–2047 B	RX at 942 m PDR 127 B–2047 B
2FSK-50	0%–0%	99%–94%	2%–0%	0%–0%	42%–0%	0%–0%
2FSK-100	0%–0%	40%–0%	0%–0%	0%–0%	0%–0%	0%–0%
4FSK-200	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%
2FSK-FEC-50	15%–3%	100%–80%	100%–88%	0%–0%	66%–55%	0%–0%
2FSK-FEC-100	8%–0%	100%–46%	38%–4%	0%–0%	17%–0%	0%–0%
4FSK-FEC-200	0%–0%	73%–24%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM1-100	0%–0%	79%–53%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM1-200	0%–0%	55%–1%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM1-400	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM1-800	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM2-50	0%–0%	90%–54%	51%–2%	0%–0%	2%–0%	0%–0%
OFDM2-100	0%–0%	89%–69%	37%–0%	0%–0%	0%–0%	0%–0%
OFDM2-200	0%–0%	44%–15%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM2-400	0%–0%	11%–0%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM2-600	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM2-800	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM3-50	0%–0%	97%–94%	0%–0%	0%–0%	12%–1%	0%–0%
OFDM3-100	0%–0%	85%–51%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM3-200	0%–0%	96%–14%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM3-300	0%–0%	16%–0%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM3-400	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM3-600	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM4-50	0%–0%	93%–9%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM4-100	0%–0%	6%–1%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM4-150	0%–0%	11%–0%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM4-200	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%
OFDM4-300	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%	0%–0%
OQPSK-6.25	36%–0%	88%–53%	99%–79%	15%–0%	86%–16%	29%–1%
OQPSK-12.5	27%–0%	100%–79%	97%–87%	0%–0%	72%–38%	32%–0%
OQPSK-25	8%–1%	98%–66%	92%–64%	0%–0%	73%–18%	0%–0%
OQPSK-50	0%–1%	98%–73%	94%–76%	0%–0%	89%–48%	0%–0%

126 m, 180 m and 215 m. In the second run, RX nodes are located at 210 m, 350 m and 400 m. All nodes located within 215 m, even without line of sight, have a PDR close to 100% for almost all radio settings considering packets of 127 B and 2047 B. There are some buildings between the TX node and the RX nodes located at 350 m and 400 m. This severely affects the quality of the radio link. In these two node locations only the O-QPSK radio settings and in less proportion the 2FSK-FEC-50 are able to get connectivity. These PHYs happen to be the most sensitive of the radio. Table 4.5 shows these PDR values for all the RX nodes.

4.4 Analysis

In this section, we provide an analysis per scenario based on three parameters: PDR, throughput and electric charge consumption [4]

The first parameter, PDR, tackles latency. Making the assumption that retransmissions do not take place right after the failure of a packet exchange, this time between retries increases latency. Also, a radio link with high PDR is of utmost interest in order to reduce retransmissions and thus, electric charge consumption.

The second parameter, throughput, takes into account the nominal data rate of each radio setting times its PDR. The result is the "goodput", and with this value we can calculate the maximum amount of packets that can be exchanged during a given time.

European regulation requires the use of this frequency band with a duty cycle $< 0.1\%$ (see Appendix A for a more detailed explanation about the duty cycle regulations).

Accordingly, we calculated the maximum amount of correct packets we could send during one hour, which corresponds to 3.6 s combined transmission time. Equation (4.1) shows how we calculated this number.

$$\text{Max\_Packets} \leq \frac{3.6\text{ s} \times \text{DR(B/s)} \times \text{PDR}}{\text{Packet size(B)} + \text{Packet overhead(B)}} \tag{4.1}$$

where 3.6 s is the maximum time a node can transmit per hour and *DR* is the nominal data rate of the radio setting. Packet size is the length of the data in the PHY (PSDU), and Packet overhead includes the PHY header and the Synchronization Header (in the case of FSK and O-QPSK) (the Synchronization Header is composed of a Preamble and a Start of Frame Delimiter (SFD). We consider the shortest preamble defined in the standard [38] for our calculation.) or the Short Training Field (STF) and Long Training Field

[4] the reason we provide the electric charge (C) consumption is that low-power devices are usually battery-powered and the voltage supply is considered fixed. We acknowledge the fact that electric circuitry consumes electric energy (J) and not only electric charge (C).

Table 4.5: AMI. PDR for packets of 127 B and 2047 B long. Even without LoS, high data rates can be achieved up to 215 m with the maximum packet length. At 350 m and 400 m, the PDR decays due to the multiple buildings between TX and RX nodes.

PHY Alias	RX at 126 m PDR 127 B–2047 B	RX at 180 m PDR 127 B–2047 B	RX at 210 m PDR 127 B–2047 B	RX at 215 m PDR 127 B–2047 B	RX at 350 m PDR 127 B–2047 B	RX at 400 m PDR 127 B–2047 B
2FSK-50	100%–100%	100%–100%	100%–100%	100%–100%	0%–0%	0%–0%
2FSK-100	100%–100%	0%–0%	100%–100%	100%–100%	0%–0%	0%–0%
4FSK-200	94%–98%	0%–1%	97%–100%	97%–100%	0%–0%	0%–0%
2FSK-FEC-50	83%–92%	100%–100%	100%–100%	100%–100%	3%–5%	79%–17%
2FSK-FEC-100	100%–100%	100%–73%	100%–100%	100%–100%	0%–0%	0%–0%
4FSK-FEC-200	100%–100%	43%–0%	100%–100%	100%–100%	0%–0%	0%–0%
OFDM1-100	100%–100%	100%–100%	100%–99%	100%–100%	0%–0%	0%–0%
OFDM1-200	100%–99%	100%–100%	93%–100%	100%–98%	0%–0%	0%–0%
OFDM1-400	100%–94%	100%–100%	100%–100%	100%–100%	0%–0%	0%–0%
OFDM1-800	31%–5%	100%–100%	100%–100%	100%–100%	0%–0%	0%–0%
OFDM2-50	84%–100%	100%–100%	99%–99%	99%–83%	0%–0%	0%–0%
OFDM2-100	100%–99%	100%–100%	100%–100%	100%–100%	0%–0%	0%–0%
OFDM2-200	99%–99%	100%–99%	100%–100%	100%–100%	0%–0%	0%–0%
OFDM2-400	100%–99%	100%–100%	100%–100%	100%–100%	0%–0%	0%–0%
OFDM2-600	97%–95%	99%–100%	100%–100%	99%–100%	0%–0%	0%–0%
OFDM2-800	100%–100%	99%–100%	100%–100%	100%–100%	0%–0%	0%–0%
OFDM3-50	100%–100%	100%–100%	100%–98%	100%–100%	0%–0%	0%–0%
OFDM3-100	100%–91%	100%–100%	100%–100%	100%–100%	0%–0%	0%–0%
OFDM3-200	100%–100%	29%–84%	100%–100%	100%–95%	0%–0%	0%–0%
OFDM3-300	100%–72%	100%–99%	100%–100%	100%–87%	0%–0%	0%–0%
OFDM3-400	100%–99%	100%–100%	100%–100%	100%–100%	0%–0%	0%–0%
OFDM3-600	99%–91%	99%–93%	87%–76%	97%–94%	0%–0%	0%–0%
OFDM4-50	100%–100%	99%–100%	100%–100%	100%–98%	0%–0%	0%–0%
OFDM4-100	100%–100%	99%–99%	99%–100%	99%–99%	0%–0%	0%–0%
OFDM4-150	100%–99%	100%–97%	100%–100%	100%–98%	0%–0%	0%–0%
OFDM4-200	99%–100%	100%–98%	100%–100%	100%–99%	0%–0%	0%–0%
OFDM4-300	100%–99%	99%–99%	100%–100%	97%–99%	0%–0%	0%–0%
OQPSK-6.25	100%–96%	100%–100%	100%–100%	100%–100%	97%–10%	76%–24%
OQPSK-12.5	100%–100%	100%–100%	100%–100%	100%–100%	0%–0%	98%–31%
OQPSK-25	100%–100%	100%–100%	100%–100%	100%–100%	3%–0%	98%–68%
OQPSK-50	100%–100%	100%–100%	100%–100%	100%–100%	0%–0%	98%–78%

(LTF) (in the case of OFDM). The addition of Packet size and Packet overhead result in the total amount of bytes the radio needs to transmit in order to send a frame.

The third parameter, electric charge consumption, is obtained by calculating how much electric charge is needed to transmit a single packet. We take into account all radio activity, including the packet overhead and packet size (PSDU). Equation (4.2) shows how we get the electric charge per packet. The I_{TX} value is the current drawn by the radio module when it is in transmission mode (see Table 3.1).

$$\text{Electric charge (Coulombs)} \geq \frac{\text{Packet size(B)} + \text{Packet overhead(B)}}{\text{DR(B/s)} \times \text{PDR}} \times I_{TX} \text{ (A)} \tag{4.2}$$

The radios used in the experiment are powered with 3 V. The electric energy (J) the radios consume can be derived from Equation (4.2) $\times$ 3 V (Energy (J) = C $\times$ V).

We see that the PDR value is present in both (4.1) and (4.2). This takes into account the potential number of retransmissions needed in order to get one correct packet at the receiver side.

For each scenario, two node locations are considered: the longer coverage where high data rates can be achieved and the maximum coverage of the radio link, despite of the data rate. For these node locations, we differentiate short (127 B) and long (2047 B) packets.

We take the value of 2FSK–50 as a reference because this is the most used configuration in the industry for smart metering applications worldwide. In addition, this PHY is the one designated to be used as the Common Signaling Mode (CSM) during the Multi-PHY Management procedure defined in the standard [38]. Moreover, the 2FSK-50 radio setting is the mandatory mode for the Wi-SUN alliance in the US and in Europe.

In the following graphs, we highlight the highest values of each parameter with dotted bars and the reference 2FSK–50 with a striped bar. A dotted line is added as a reference on every figure to easily compare the 2FSK–50 kbps radio setting with the rest of the PHYs. Although in most cases 2FSK–50 delivers a good PDR in comparison with most of the other PHYs, this study shows that there may be more interesting PHYs depending on the constraints of range, throughput, duty cycle and electric charge consumption.

4.4.1 Line of Sight Scenario

High data rates can be achieved up to 420 m, and the maximum length of the radio link with low data rates can reach 700 m with a high PDR. There is not useful radio link at 1000 m.

RX at 420 m

As shown in Figure 4.6a for a packet size of 127 B, most of the radio settings have a PDR close to 100%, including the reference 2FSK-50. OFDM3-600 is the only exception, with a 26% PDR. The majority of the radio settings has a high reliability at 420 m with LoS.

Increasing the packets size to 2047 B, Figure 4.6b shows that the performance of the radio settings is not much affected, with high data rates still having a PDR close to 100%, including the reference 2FSK-50. The exception in this case are OFDM2-800, OFDM3-600 and OFDM4-300, the highest data rates of OFDM options 2, 3 and 4. One of the reasons is that these PHYs present the lowest sensitivity (the lower the sensitivity value is, the higher sensitivity is. e.g., a device A with sensitivity of -110 dBm and another device B with sensitivity of -120 dBm, device B has a higher sensitivity than device A.) (-101 dBm, -97 dBm and -101 dBm respectively) of the different OFDM radio settings. The poor performance of OFDM3-600 (with a 26% PDR) could be linked to its low sensitivity, being at least 4 dB lower than any other OFDM radio setting. The sensitivity for 4FSK-200 is 1 dB lower but the TX power is 4 dBm higher. Therefore, the signal at the receiver is 4 dB higher for the 4FSK-200 PHY, enough to present a PDR of 100%.

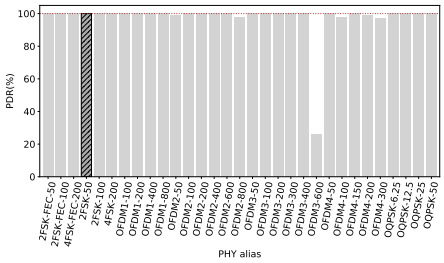
On the other hand, the rest of the PHYs present high reliability. Thus, we do not highlight any particular PHY in Figure 4.6a,b since most of them have 100% PDR.

Considering throughput, with 127 B packets, Figure 4.6c clearly shows that OFDM1-800 is the PHY than can have the maximum amount of correct packets transmitted within an hour (duty cycle of 0.1%), with 1531 packets. The reference value, 2FSK–50, can transmit during the same time just 166 packets.

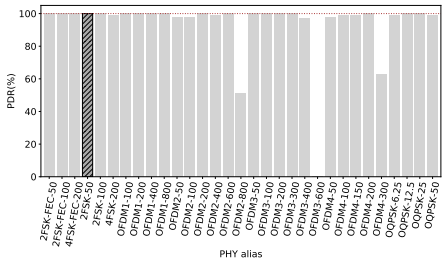
This proportion is maintained with packets of 2047 B, as shown in Figure 4.6d. OFDM1-800 stands alone with the possibility of transmitting 167 packets against roughly 11 of 2FSK-50 whilst having 0.1% duty cycle. Therefore, OFDM1-800 has the capability of transmitting more short and long packets than any other PHY within the standard, under the 0.1% duty cycle regulation and at 420 m from the TX. If it is the interest of the user to maximize the amount of packets that can be sent, OFDM1-800 or any other OFDM option with high data rate can be used, as Figure 4.6c,d show.

Figure 4.6e shows the average electric charge consumption per packet transmitted for all radio settings. We can see that high data rates PHYs, mostly OFDM, consume several times less electric charge that the reference 2FSK-50. The most electric charge-efficient is, again, OFDM1-800. It consumes 178.6 μC to get a 127 B packet across while 2FSK-50 consumes 1807 μC.

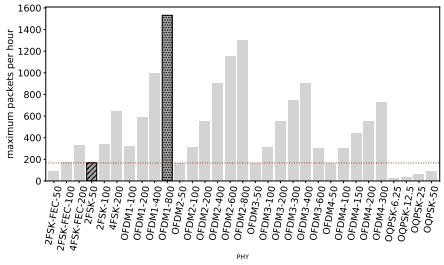
For long packets, average electric charge consumption is depicted in Fig-



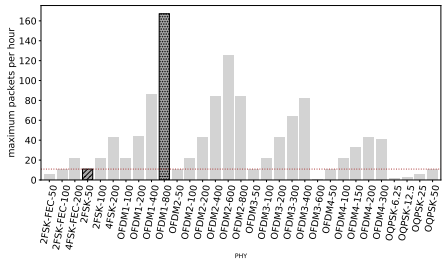
(a) PDR of all radio settings at 420 m from TX with packets of 127 B. Except for OFDM3-600, all radio settings have a PDR close to 100%



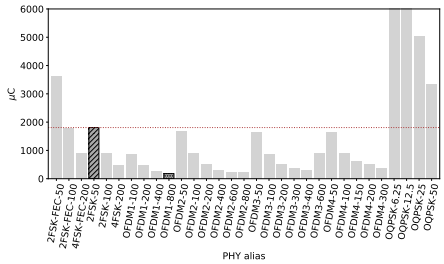
(b) PDR of all radio settings at 420 m from TX with packets of 2047 B. OFDM2-800 and OFDM4-300 do not have PDR values close to 100%. OFDM2-800 and OFDM4-300 do not have PDR values close to 100%. OFDM3-600 has 0% PDR



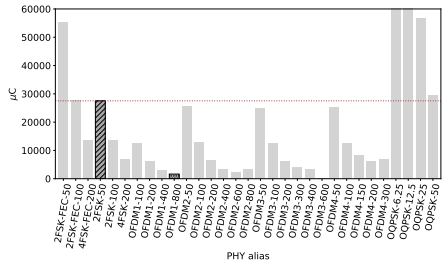
(c) Maximum amount of 127 B packets that can be correctly sent per PHY under 0.1% duty cycle regulation. OFDM1-800 can send 1531 packets while 2FSK-50 only 166.



(d) Maximum amount of 2047 B packets that can be correctly sent per PHY under 0.1% duty cycle regulation. OFDM1-800 can send 167 packets while 2FSK-50 roughly 11.



(e) Average electric charge consumption per packet of 127 B correctly sent. OFDM1-800 is the most electric charge-efficient, consumes 178.6 μC whereas the reference 2FSK-50 consumes 1807 μC



(f) Average electric charge consumption per packet of 2047 B correctly sent. OFDM1-800 consumes the lowest amount of electric charge per packet, with 1637 μC whereas the reference 2FSK-50 consumes 27.5 mC

Figure 4.6: Line of Sight, 420 m. The radio link allows the transmission of packets with 2047 B even with the highest data rates available with a PDR very close to 100%. Within this distance, high data rates radio settings maintain high reliability while consuming less electric charge and allowing more data exchange than low data rates radio settings.

ure 4.6f. The tendency is maintained, high data rates consumed less electric charge than the rest. 2FSK-50 consumes on average 27.5 mC while OFDM1-800 only 1.637 mC.

RX at 700 m

Considering the RX node at 700 m, we approach to the limit of the radio link. Figure 4.7 shows that high data rates are not capable of delivering any packet, making them unusable for similar distances.

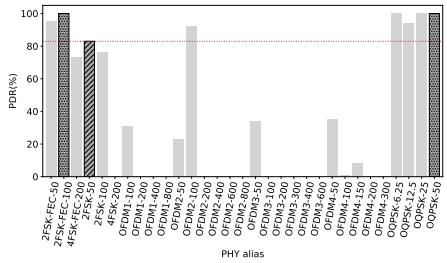
From Figure 4.7a, with short packets, we see that most OFDM radio settings have a poor or nonexistent PDR. The reference 2FSK-50 has a PDR of 83%. Only OFDM2-100 presents a PDR of 92%. O-QPSK radio settings have a high reliability, with 3 out of 4 PDR values of 100% and the remaining (OQPSK-12.5) of 94%. 2FSK-FEC-100 has 100% PDR. Therefore, we highlight 2FSK-FEC-100 and O-QPSK since they have the highest PDR and highest data rate in their technology.

Increasing the packet size to 2047 B, we see from Figure 4.7b that the PDR slightly drops in comparison to small packets. Nonetheless, it is still around 80% for some radio settings. The reference is at 58% PDR, being matched by OFDM2-50 and outperformed by all O-QPSK PHYs and 2FSK-FEC-50 and 2FSK-FEC-100. We highlight the highest PDR of each technology, therefore 2FSK-FEC-50 and OQPSK-50.

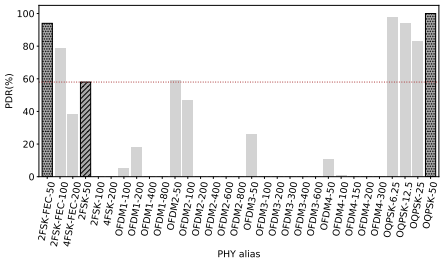
It is notable that for OFDM2-50, the PDR concerning long packets is 59% whereas for short packets is only 23%. This is counterintuitive since short packets should have a higher PDR than long packets due to is lower probability of getting a wrong symbol throughout the complete received frame. Therefore, this effect can be attributed to interference that occurred only in that precise moment. For the following radio setting tested, OFDM2-100, we see how the PDR for short packets increased to 92%, using the same frequency as OFDM2-50, which shows that the interference is no longer present.

Ref. [68] shows that a link of 3.5 km can be obtained with this technology. They were in the Highlands of Scotland and the router node with that link was located at the top of a hill (`https://mountainsensing.org/deployment/router-nodes/`). In our case, our link did not arrive to one kilometer, mainly due to the obstacle the ground poses at that distance (the Fresnel radius to that distance is 9.29 m and the nodes are at 1.8 m above the ground).

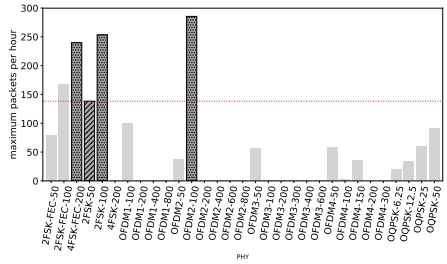
Now, considering the maximum amount of packets that can be transmitted under the duty cycle regulation with short packets. Figure 4.7c shows that OFDM2-100 is the radio setting that can send up to 285 short packets within an hour. Not far behind we have 4FSK-FEC-200 and 2FSK-100 capable of transmitting 239 and 253 short packets per hour. 2FSK-50 can transmit only 138 short packets in the same period.



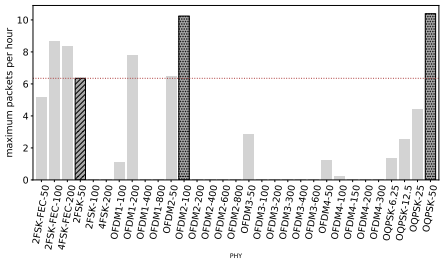
(a) PDR at 700 m from TX with packets of 127 B. Highest reliability achieved with 2FSK-FEC-100, OQPSK-6.25, OQPSK-12.5 and OQPSK-50. The reference has 83% PDR. OFDM2-100 has also higher reliability than the reference.



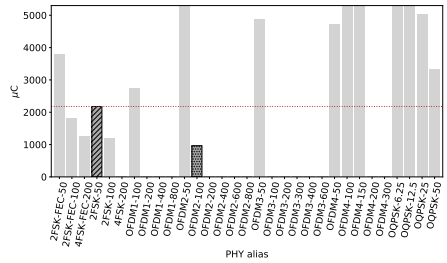
(b) PDR at 700 m from the TX with packets of 2047 B. The reference has 58% PDR, while 2FSK-FEC-50 94% PDR and OQPSK-50 100% PDR.



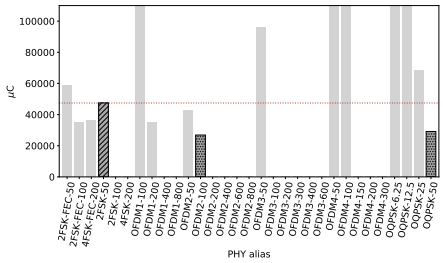
(c) Maximum amount of 127 B packets correctly sent within an hour. 4FSK-FEC-200 and 2FSK-100 can send 239 and 253 short packets. OFDM2-100 can send up to 285 packets, while the reference only 138 packets.



(d) Maximum amount of 2047 B packets that can be correctly sent within an hour. OFDM2-100 and OQPSK-50 can send up to 10 packets, while the reference 2FSK-50 just 6 packets.



(e) Average electric charge consumption per packet of 127 B. OFDM2-100 consumes the less electric charge, 964 μC while 2FSK-50 consumes 2178 μC



(f) Average charge per 2047 B frame. OFDM2-100 and OQPSK-50 exhibit the lowest charge, at 26.8 mC and 29.1 mC. 2FSK-50 draws almost double, 47.5 mC.

Figure 4.7: Line of Sight, 700 m. Only O-QPSK and FSK radio settings are able to provide the highest reliability. This node is close to the limits of the coverage. OFDM radio settings have a poor performance at this distance, but the difference is that OFDM transmissions are at least 3 dBm weaker that the rest of the PHYs.

At this distance from TX, a few long packets can be transmitted per hour. The reference 2FSK-50 can transmit roughly 6 packets per hour while OFDM2-100 and OQPSK-50 just 10. We highlight those two PHYs. Therefore, if the user is interested in maximizing the throughput, 4FSK-FEC-200, 2FSK-100 and OFDM2-100 are the most performing PHYs to do so with short packet. With long packets, OFDM2-100 and OQPSK-50.

Figure 4.7e shows the average electric charge consumption per packet of 127 B transmitted. For short packets, the reference consumes 2178 μC whereas the less power-hungry in this case, OFDM2-100, consumes 964 μC.

For long packets, average power consumption is depicted in Figure 4.7f. 2FSK-50 consumes in average 47.5 mC. The less electric charge-consuming PHYs in this scenario are OFDM2-100 and OQPSK-50, with 26.8 mC and 29.1 mC respectively. Should the potential user be focused on reducing electric charge consumption, dotted-pattern highlighted bars in Figure 4.7e,f depict the less electric charge-hungry PHYs in this case.

4.4.2 Smart Agriculture Scenario

In this scenario, high data rates with high PDR are achieved up to 337 m, and maximum length of the radio link is reached around 615 m away from the TX node.

RX at 337 m

With a packet size of 127 B, Figure 4.8a shows the PDR of almost all radio settings are very close to 100%, including those with the highest data rate possible (800 kbps). Increasing the packet size to 2047 B, Figure 4.8b shows that the PDR remains 100% for the majority of the radio settings, including OFDM1-800. 2FSK-50 is 100% in both, with short and long packets, as well as its variations with higher data rates. Therefore we do not highlight any other PHY, since the potential user has many options to choose a radio setting with 100% PDR.

We can see that the PDR values for some radio settings are higher for long packets than short packets. This is the case for OFDM2-200 and OFDM4-300 at 213 m, and for OFDM4-300 at 337 m. This can be linked to interference. Since we are transmitting packets with only 20 ms separation between them, short packets series are more likely to be affected than longer packets by a single transmission of a different radio technology device using the same frequency and with a lower data rate (a LoRa packet using Spreading Factor 12 with a 13 B payload has a ToA of 925 ms (LoRa Modem Calculator Tool)).

Figure 4.8c shows the maximum amount of packets that can be transmitted per hour, and we can see that OFDM1-800 can transmit up to 1531 packets while the reference 2FSK-50 only 166. We highlight OFDM1-800 since it can transmit at least 25% more packets than any other radio setting,

and more that 9 times the amount of the reference. Considering long packets, OFDM1-800 has the capability of sending the maximum amount of packets per hour, up to 167 packets, while the reference roughly 11. Figure 4.8d shows the maximum amount of 2047 B packets that can be delivered at 337 m. In consequence, if the potential user wants to maximize the throughput of the nodes separated by a similar distance, OFDM1-800 offers the highest throughput.

Figure 4.8e depicts the average electric charge consumption per packet the radio needs in order to send a 127 B packet. The reference 2FSK-50 needs on average 1800 μC. The lowest amount of electric charge needed corresponds to OFDM1-800, with just 178 μC, around ten times less electric charge. Other radio settings are also "low energy" such as OFDM2-800 with 215 μC, and OFDM2-600 with 243 μC.

In Figure 4.8f, we can see the average electric charge consumed by the TX radio in order to transmit a long packet. The radio setting with the smallest electric charge requirement is OFDM1-800, with 1630 μC on average per a 2047 B transmitted packet. The reference 2FSK-50 consumes 27.5 mA, 16 times more than OFDM1-800. OFDM2-600 consumes 2200 μC, more than 12 times less than the reference. If the potential user wants to increase the lifetime of a battery power node, OFDM1-800 is the less electric charge demanding PHY in these conditions.

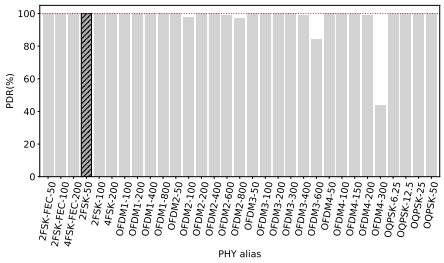
RX at 615 m

At this distance, the overall performance of the radio settings is poor.

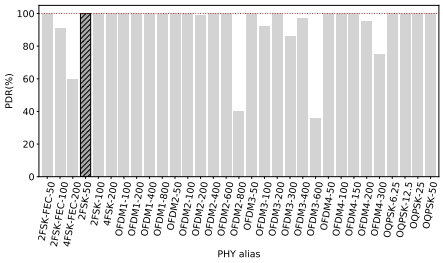
Figure 4.9a shows the PDR of all radio settings for short frames, where the majority of OFDM and FSK radio settings are not able to get any frames across. Only O-QSPK PHYs, 2-FSK-FEC-50 and OFDM2-100 have a PDR over 80%. The reference 2FSK-50 has a negligible PDR, only 5%.

PDR values for long packets are shown in Figure 4.9b. Only OQPSK PHYs maintain a high PDR. 2FSK-FEC-50 drops to 64% and the reference is only 11%. Therefore, if the potential user wants to have radio links with similar length, 2FSK-FEC-50, OFDM2-100 and any O-QPSK radio setting are useful for such requirement with short packets. For long packets, any O-QPSK radio setting is useful.

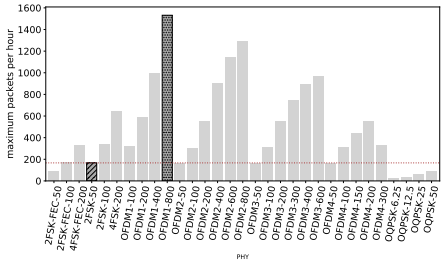
It can be seen in Table 4.2 that the PDR values at 538 m are lower than at 615 m. This seems counterintuitive since at further distance, lower should be the power of the received signal and thus, the PDR. This assumption is correct in environments where the attenuation of the radio signals are only due to distance, without obstacles located between the transmitter and receiver. But this is not our case. The obstacles surrounding the RX node located at 538 m and its relative position to the TX node cause this shadowing effect, affecting its PDR. At 615 m, the surroundings of the RX node did not have this effect and therefore, the PDR values are higher.



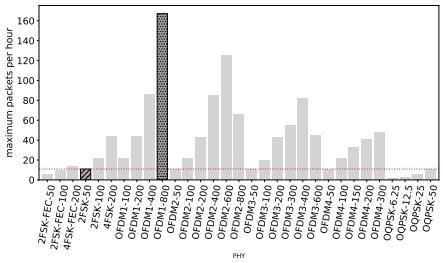
(a) Packets of 127 B. Almost all radio settings with a PDR close to 100%, including those with the higher data rates.



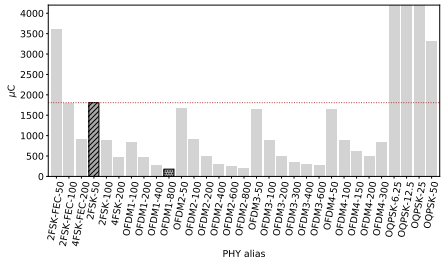
(b) Packets of 2047 B. PDR of some radio settings drops, such as OFDM2-800, 2FSK-100 and 4FSK-200. The whole OFMD option 1 PHYs stay at 100%, as well as the reference 2FSK-50 and all the O-QPSK radio settings.



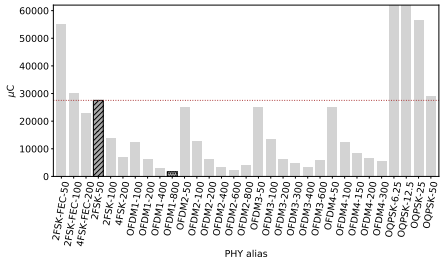
(c) Maximum amount of short packets that can be transmitted per hour. OFDM1-800 can transmit up to 1531 packets while the reference just 166.



(d) Maximum amount of long packets that can be transmitted per hour. OFDM1-800 can transmit up to 167 packets, more than 10 times the reference with just 11 packets.



(e) Average electric charge per 127 B frame. OFDM1-800 exhibts the lowest charge (178 μC); 2SFK-50 the most (1800 μC). Other high data rate OFDM PHYs consume significantly less than the reference.



(f) Average electric charge consumed to send a long packet. Still OFDM1-800 is the less electric charge-consuming, with 1637 μC per packet, whereas the reference consumes 27.5 mC.

Figure 4.8: Smart Agriculture, 337 m. The PDR for all radio setting considering short and long packets is high. Using high data rates does not impact in the reliability while reducing electric charge consumption and increasing the number of packets exchange within the 0.1% duty cycle regulation.

The maximum amount of short packets that can be sent under the 0.1% duty cycle regulation are shown in Figure 4.9c. Even though OFDM1-200 has only 52% PDR, its high data rate allows it to send just over 300 packets per hour. Not far behind, OFDM2-100 has the possibility of sending up to 251 packets per hour. 2FSK-50 only 8 packets, and OQPSK-50 below 100 packets of 127 B.

Now considering long packets, Figure 4.9d shows the maximum amount each PHY can correctly send within an hour. 2FSK-50 can send one long packet per hour, whereas OQPSK-50 just 10. For a potential user, if it is wanted to maximize the amount of transmitted packets, OFDM1-200 is the best option for short packets. For long packets, OQPSK-50 is the best option but just a few packets possible.

Figure 4.9e shows the electric charge consumed on average per short packet transmitted to this node. 2FSK-50 has a poor PDR, thus the eventual need for retransmissions makes energetically expensive to get a packet across. It consumes 36 mC, whereas OFDM1-200 and OFDM2-100 consume 895 μC and 1095 μC respectively. Therefore, we highlight these last two as the more efficient in electric charge consumption. For long packets, Figure 4.9f shows the average consumption. The reference 2FSK-50 consumes 250 mC per packet of 2047 B. We can observe that the less consuming PHY is OQPSK-50, with 29.5 mC. In both cases, for short and long packets, 2FSK-50 is at least one magnitude higher than the most electric charge-efficient PHYs.

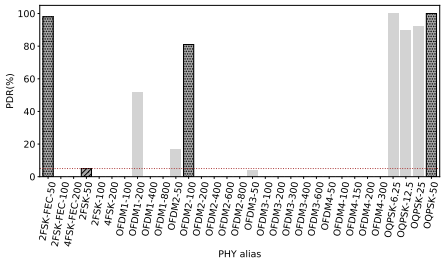
4.4.3 Urban Canyon Scenario

High data rates with high PDR values are reached up to 540 m away from the TX node. The maximum length of the radio link is at 779 m, with important losses at 602 m and 742 m due to obstacles and the topography of the scenario.

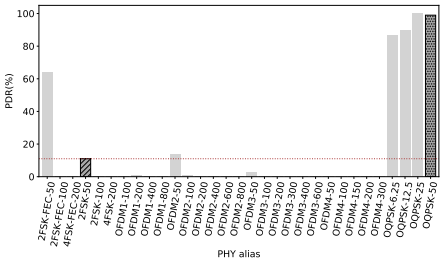
RX at 540 m

PDR values of all radio settings are depicted in Figure 4.10a for short packets. Overall, all PHYs have a high reliability, with values between 84% and 100% PDR. The exceptions are OFDM3-600 and OFDM4-300, with values of 21% and 60% PDR respectively. The reference 2FSK-50 has 95% PDR. We do not highlight any since there are many PHYs with their PDR greater that the reference.

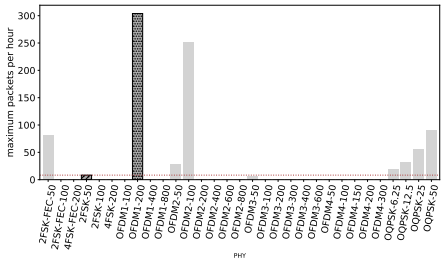
For long packets, the PDR values are shown in Figure 4.10b. We can see the PDR values decay a few points, but still several PHYs with higher PDR that the reference (with 84% PDR). The two PHY with highest reliability with long packets are 2FSK-FEC-100 and OFDM4-100 with 95% and 96% PDR respectively. Noticeably, O-QPSK radio settings have a lower PDR, even though their sensitivity is higher. Their low data rate makes



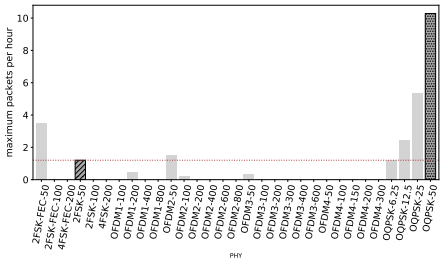
(a) PDR values for all radio settings with short packets. Only 2FSK-FEC-50, OFDM2-100 and all the O-QPSK radio settings have a PDR over 80%. The reference has a poor PDR, only 5%.



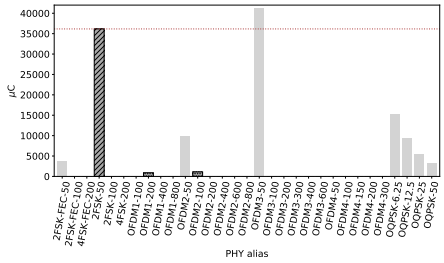
(b) PDR values considering long packets. Only O-QPSK PHYs have PDR values over 85%, against the reference with 11%.



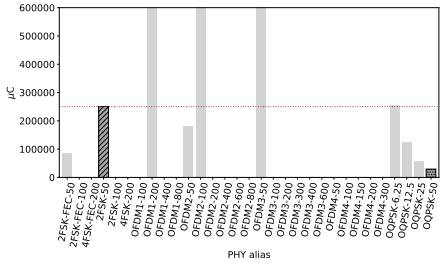
(c) Maximum amount of TXs with short packets under 0.1% duty cycle. Despite its PDR of 52%, OFDM1-200 is able to transmit up to 300 short packets. The reference can send just 8 packets.



(d) Maximum amount of TXs with long packets within one hour. OQPSK-50 can send up to 10 long packets while the reference roughly 1 packet per hour.



(e) Energy consumed per 127 B packet transmitted. OFDM1-200 and OFDM2-100 are the most electric charge-efficient, consuming 895 μC and 1095 μC respectively. The reference consumes 36 mC. This is due to its poor PDR.



(f) Energy consumed per 127 B packet transmitted. O-QPSK is the less electric charge-consuming radio setting, with 29.5 mC while the reference consumes 250 mC.

Figure 4.9: Smart Agriculture, 615 m. The radio link is very close to the maximum distance where it can deliver connectivity. High data rates OFDM radio settings are unable to get any packet across. Maximum data rate that can provide connectivity is 200 kbps, but with PDR of 52% with short packets.

the time needed to send each frame longer, increasing the probabilities of collision with other networks/technologies during transmissions.

Figure 4.10c shows the maximum number of packets that can be sent under the 0.1% duty cycle regulation. OFDM1-800 stands alone with the possibility of sending 1485 packets. Some hundreds of packets behind, OFDM2-600 and OFDM2-800 with roughly 1115 packets. The reference 2FSK-50 can send up to 158 packets per hour.

Figure 4.10d shows the maximum number of long packets that can be sent per hour. Still, OFDM1-800 is the PHY that allows the maximum number of transmissions per hour, under the duty cycle regulation, with roughly 132 packets. OFDM2-600 allows 110 full packet length transmissions, while the reference only 9. Consequently, if the potential user wants to maximize the amount of packets until the duty cycle regulation limit, OFDM1-800 is shown to be the best for short and long packets.

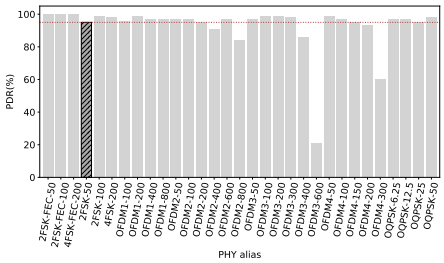
The average amount of electric charge used to transmit a 127 B packet for all the radio settings can be seen in Figure 4.10e. The lower electric charge consumption to get one packet across is achieved with OFDM1-800, spending 184 μC. The reference 2FSK-50 spends 1900 μC, one magnitude higher.

Concerning the electric charge consumption for long packets, Figure 4.10f shows these values. The tendency is maintained, OFDM1-800 is the most efficient radio setting to send a packet of 2047 B, with an average consumption of 2070 μC. OFDM2-600 is close to this value, with 2507 μC per 2047 B sent. 2FSK-50 consumes, for the same transmission, around 32,760 μC.

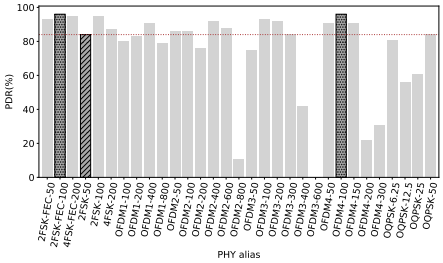
RX at 779 m

At this distance we approach to the limit of the radio link. As shown in Figure 4.11a, only radio settings with data rates $\leq$ 50 kbps present PDR values over 60% for frames of 127 B. The PDR of the reference 2FSK-50 is only 42%. 2FSK-FEC-50 is the only non O-QPSK PHY with its PDR $>$ 50%. This RX node is located at the limits of the coverage proportionated by the TX node. We can observe the PDR values in Figure 4.11b for packets of 2047 B. Only 2FSK-FEC-50 has a PDR over 50%. Even OQPSK PHYs, with their higher sensitivity, do not have a PDR over 50%. At this distance and in these conditions, only short packets can deliver a good reliability of 80% with OQPSK-50.

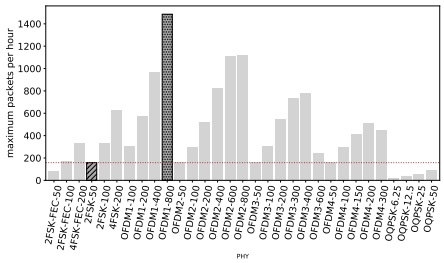
Figure 4.11c shows the maximum amount of 1287 B packets that can be sent within an hour under the 0.1% duty cycle regulation. Only OQPSK-50 outperforms the reference, with the possibility of sending up to 81 packets per hour against 70 packets of 2FSK-50. For long packets, the maximum amount of packets per hour can be seen in Figure 4.11d. With a maximum of roughly 5 packets per hour, OQPSK-50 is the most convenient PHY. 2FSK-FEC-50 can send up to just 3 full packets and 2FSK-50 is incapable



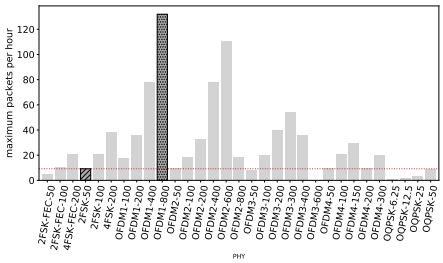
(a) PDR values with packets of 127 B. Overall, high reliability except for OFDM3-600 and OFDM4-300. Reference value, 98% PDR.



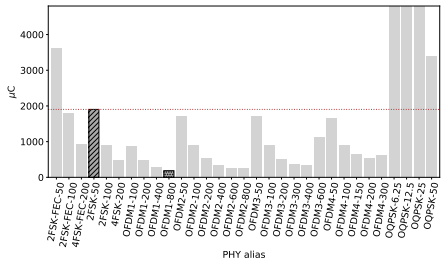
(b) PDR values with 2047 B packets. Overall values are over 50%, with a few OFDM radio settings. Highest values with 2FSK-FEC-100 and OFDM4-100, 95% PDR and 96% PDR. Reference value, 84% PDR.



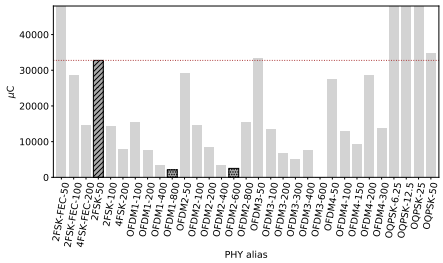
(c) Maximum amount of TX packets of 127 B under the 0.1% duty cycle regulation. OFDM1-800 can transmit up to 1485 packets, while the reference 158 packets. OFDM2-600 and OFDM2-800 can also transmit more than 1000 short packets.



(d) Maximum amount of TX packets of 2047 B under the 0.1% duty cycle regulation. OFDM1-800 can send up to 132 packets, OFDM2-600 110 packets and the reference just 9 packets.



(e) Average electric charge consumed per packet of 127 B sent. OFDM1-800 is the less consuming radio setting, with 184 μC per packet whilst 2FSK-50 consumes 1900 μC.



(f) Average electric charge per 2047 B frame. OFDM1-800 and OFDM2-600 exhibit the lowest charge (2.1 mC and 2.5 mC, resp.). 2FSK-50 consumes around 33 mC

Figure 4.10: Urban Canyon, 540 m. Some high data rate radio settings have a good PDR, close to 100%, and some others suffer from interferences. This is expected in this type of scenarios so an agile MAC layer would be useful in order to overcome those interferences by either changing frequency or waiting for the availability of the medium.

of get any packet across.

Figure 4.11e shows the average electric charge consumed by the TX node in order to get a 127 B packet across with the different PHYs. 2FSK-50 consumes 4.3 mC and OQPSK-50 consumes 3.7 mC. Any other PHY does not consume less electric charge than those two.

Similarly but with long packets, we see the electric charge consumption in Figure 4.11f. The TX node needs 105 mC to get a packet across when using 2FSK-FEC-50 and 60.7 mC with OQPSK-50. In this scenario and at this distance, low data rates and poor PDR make energetically expensive to get packets correctly transmitted. If compared with the values at 540 m, at 779 m it is consumed twice the electric charge (2FSK-50 at 540 m consumes 32 mC vs. OQPSK-50 at 779 m with 60.7 mC).

In this scenario, we can see results that are counterintuitive:

For OFDM1-800 and OFDM2 PHYs at 406 m, the PDR is lower for low data rates (50 to 400 kbps) than for high data rates (600 and 800 kbps). In interference-and-obstacle-free scenarios, it should be the opposite since lower data rates PHYs have a higher sensitivity. This can be attributed to interference occurred at the moment of the experiment. This affirmation is backed by the fact that for the rest of the radio settings at this distance, the PDR values are above 90%, even for those PHYs with lower sensitivity. Same reasoning goes with OFDM2-400 and OFDM2-600 at 512 m.

Short frames have worst PDR than long frames. The reason is also interference, since a burst of short packets can be more affected by a single transmission of different technology/network using a lower data rated communication than a long packet burst. We see this more notably in OFDM2-100 at 406 m and OFDM1-400 at 512 m.

Nodes located at further distance presenting higher PDR values than nodes located closer to the TX node. We are in a scenario where the radio signals interact with trees, people, cars, buses, shops, buildings and big metal infrastructure and for some RX locations, these objects are in the way between the TX and RX nodes. These objects can cause the shadowing effect of the node, affecting the quality of the link between TX and RX and thus, drastically reducing the PDR for that link.

4.4.4 Advanced Metering Infrastructure Scenario

For the nodes located within 215 m, the PDR values of almost all radio settings are close to 100%. Taking one of those 4 locations would have similar results to those exposed in Section 4.4.3. For the RX nodes at 350 m and 400 m, PDR values decay and we approach to the limits of the radio link. Therefore we present the analysis for those 2 RX locations. Several buildings are between TX and those 2 RX nodes, making it a challenging environment to the radio link.

RX at 350 m

Figure 4.12a shows the PDR values for all radio settings with a packet length of 127 B. The radio link is almost nonexistent. Only OQPSK-6.25, the PHY with the slowest data rate available in the standard, has a high PDR value, 97%. The rest of the radio settings have a negligible PDR. Figure 4.12b depicts the poor PDR values with long packets. It is not possible to establish a radio communication with these PDR values, which is as high as 10% for OQPSK-6.25.

Figure 4.12c shows the maximum number of packets that can be sent within an hour. OQPSK-6.25 is capable of delivering roughly 19 short packets. This is enough for some applications where few sensor readings are performed per hour. Considering long packets, it is not possible to get even one packet across for any PHY, as it is shown in Figure 4.12d.

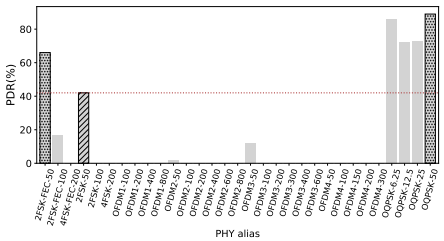
The average electric charge consumed to transmit a packet is shown in Figure 4.12e. With OQPSK-6.25, the TX node consumes 15.7 mC per packet of 127 B to get correctly sent. For long frames, it would take more than 2 C to get a packet across. Therefore, long frames in this scenario are not achievable.

RX at 400 m

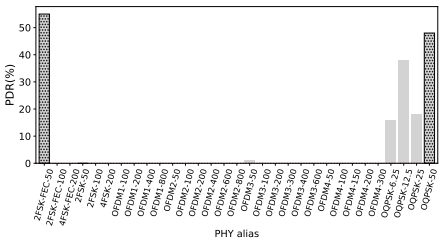
Figure 4.13a depicts the PDR values for short packets. 2FSK-FEC-50 and O-QPSK PHYs present PDR values above 75%. The rest of the PHYs do not have any reliability, PDR values are zero. OQPSK-12.5, OQPSK-25 and OQPSK-50 have 98% PDR. In Figure 4.13b is shown the PDR for 2047 B packets. The PDR of 2FSK-FEC-50 decays below 20% while the PDR of OQPSK-50 is still high, at 78%. Therefore, the radio setting with the highest reliability for short and long packets is OQPSK-50 and we highlight it.

Figure 4.13c shows the maximum number of short packets that can be transmitted. The radio setting that can transmit more packet within one hour is OQPSK-50 with roughly 90 packets. Now considering long packets, see Figure 4.13d, OQPSK-50 is still the PHY with a maximum of 8 possible packets per hour. Ergo, in order to maximize the throughput of the nodes and being compliant with the duty cycle regulation, OQPSK-50 is the most convenient.

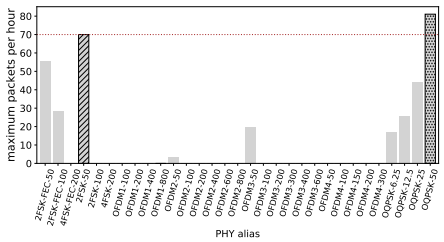
It is depicted in Figure 4.13e the average electric charge consumed per short packet transmitted. The less power-hungry is the OQPSK-50 PHY, with 3.4 mC. Similarly, Figure 4.13f shows the electric charge consumption for long packets. The tendency is maintained, OQPSK-50 consumes the less amount of electric charge per 2047 B packet, with 37 mC. Thus, OQPSK-50 is the more electric charge-efficient PHY for this scenario, despite of the length of the packet.



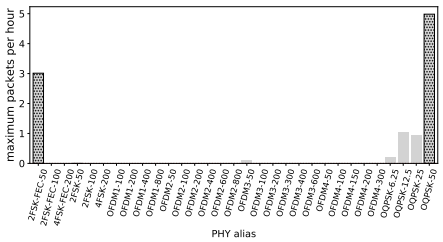
(a) PDR with packets of 127 B. Only data rates up to 50 kbps provide some connectivity, with the exception of O-QPSK-50 whose PDR is above 80%. We are very close to the maximum length of the radio link. PDR of 2FSK-50 is 42%.



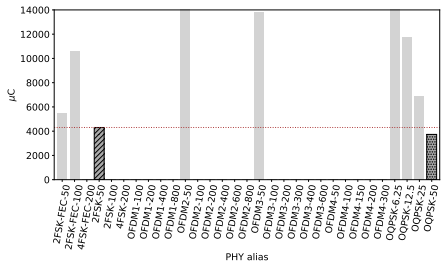
(b) PDR with packets of 2047 B. Only 2FSK-FEC-50 has a PDR over 50%. The rest of the radio settings does not provide any connectivity, with the exception of the O-QPSK radio settings.



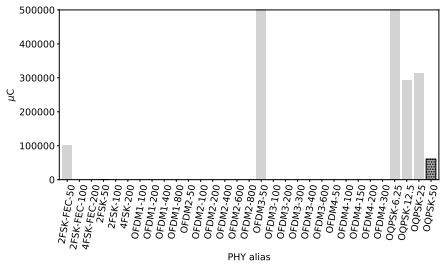
(c) Maximum amount of short packets transmitted per hour. The reference 2FSK-50 can send up to 70 packets and OQPSK-50 81 packets.



(d) Maximum amount of long packets transmitted per hour. OQPSK-50 can send up to 5 2047 B packets per hour under the 0.1% duty cycle regulation.

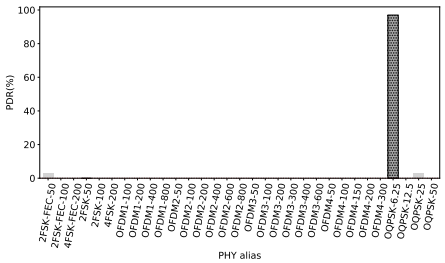


(e) Average electric charge consumption per 127 B packet sent. 2FSK-50 needs 4.3 mC to transmit one short packet whilst OQPSK-50 consumes 3.7 mC per packet.

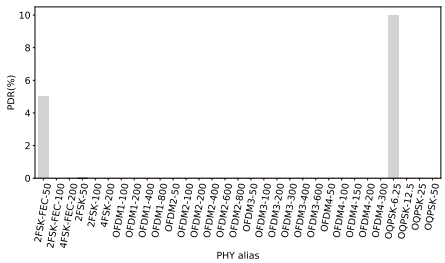


(f) Average electric charge consumption per packet of 2047 B sent. O-QSPK consumes 60.7 mC, less than any other radio setting.

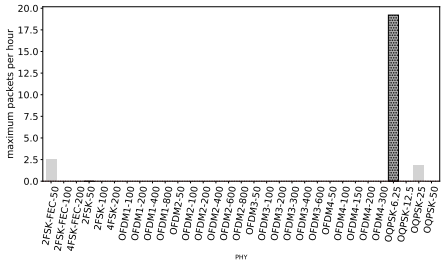
Figure 4.11: Urban Canyon, 779 m. The limit of the radio link is very close to this distance of 779 m from the TX node. The PDR for short and long packets is poor, so is the maximum amount of packets per hour. Applications with short packets and low throughput can stand radio links with similar characteristics.



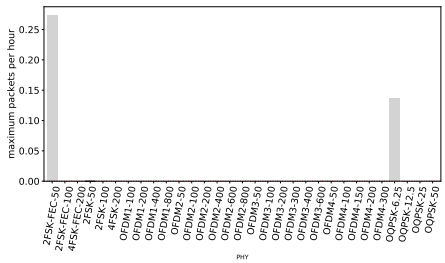
(a) PDR values considering packets of 127 B. Only OQPSK-6.25 can provide good connectivity with 97% PDR. The rest of the radio links offers no connectivity at all, PDR values of 0%.



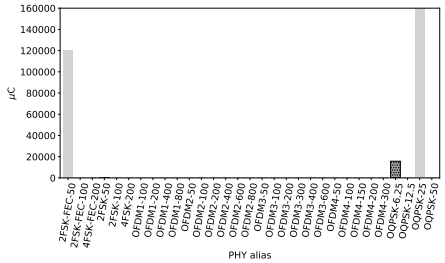
(b) PDR values with long packets of 2047 B. The quality of the radio link is overall poor. With PDR values below 10%, no communication link is possible.



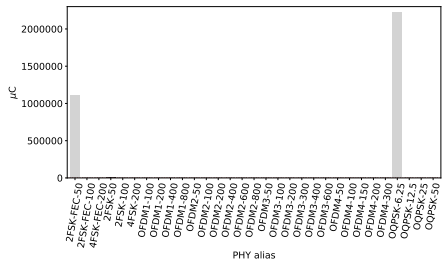
(c) Maximum amount of TX packets per hour. OQPSK-50 can roughly send 19 packets per hour. 2FSK-FEC-50 only 2 and OQPSK-25 only 1. The rest of the PHYs cannot get even one packet across.



(d) Maximum amount of TX packets per hour. Any radio setting is able to send one packet.

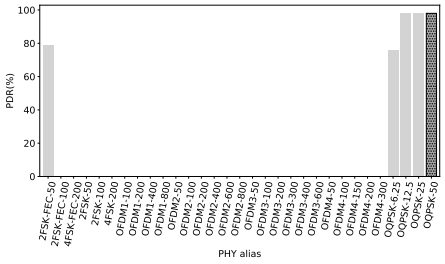


(e) Average electric charge consumed per packet of 127 B transmitted. OQPSK-6.25 needs 15.7 mC per short packet.

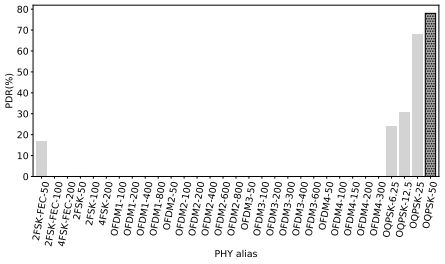


(f) Average electric charge consumed per packet of 2047 B transmitted. On average, it takes more than 1 C per packet using 2FSK-FEC-50 and more than 2 C if OQPSK-6.25 is used.

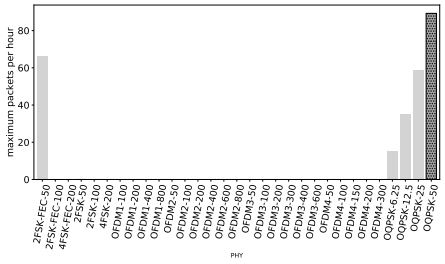
Figure 4.12: AMI, 350 m. Only the radio setting OQPSK-6.25 with short packets is useful for this type of challenging conditions, with several buildings between nodes.



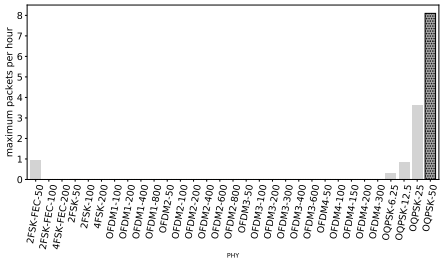
(a) PDR values with packets of 127 B. OQPSK-12.5, OQPSK-25 and OQPSK-50 have 98% PDR. We see that the most advantageous of that group is OQPSK-50, offering same reliability with higher data rate.



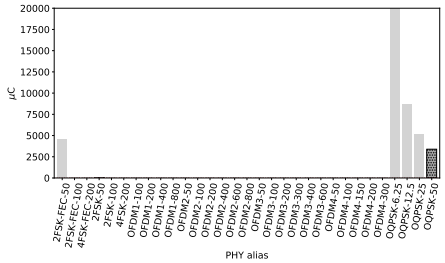
(b) PDR values with packets of 2047 B. OQPSK-50 offers the highest reliability, 78%, between the 5 radio settings with non-zero PDR.



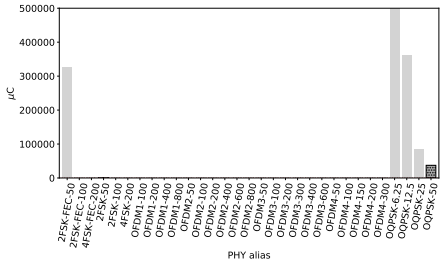
(c) Maximum amount of TX short packets under 0.1% duty cycle regulation. OQPSK-50 can send up to 90 short packets, more than any other radio setting.



(d) Maximum amount of TX long packets under 0.1% duty cycle regulation. OQPSK-50 is able to send up to 8 long packets within one hour.



(e) Average electric charge consumed per packet of 127 B transmitted. OQPSK-50 consumes on average, 3.4 mC per packet transmitted.



(f) Average electric charge consumed per packet of 2047 B transmitted. OQPSK-50 is the less electric charge-hungry radio setting, consuming 37 mC per packet transmitted.

Figure 4.13: AMI, 400 m. It is normal to have several buildings and any other kind of obstacles between nodes. Having these conditions, the most useful radio setting is OQPSK-50.

4.5 Discussion

The lower the frequency, the higher the maximum coverage of the signal with the same TX power (considering devices with similar sensitivity). Consequently, the use of a frequency band below 2.4 GHz increases the range of the radio signals. In comparison with a 2.4 GHz solution, sub-GHz enables networks with fewer hops, allowing simpler deployments but with the performance and flexibility that mesh networks provide.

The adoption of the PHYs described in the IEEE802.15.4g can be beneficial to any type of WSN due to the following reasons:

- They can be used in sub-GHz bands, increasing the range of the radio links.
- Higher data rates, up to 800 kbps, reduce the transmission/reception time for a packet; this lowers the electric charge consumption per byte exchanged and increases the maximum amount of packets that can be exchanged considering duty cycle regulations.
- They provide long range as a Low-Power Wide Area Network (LPWAN) combined with the flexibility of a mesh network. This enables networks to be built with simple architectures (few-hop deep networks) bringing good trade-off between performance and simplicity.
- The diverse characteristics of each modulation enable further optimization to the low-power networks solutions. Networks are now able to trade-off data rate, robustness, electric charge consumption, range and duty cycle. Choices on the PHY to be used can be made according to the current conditions.

Regulations on sub-GHz bands are in constant revision, which poses an additional challenge to keep up with all the evolution.

This work is meant to provide the reader a first reference of what can be achieved by the IEEE802.15.4g standard in terms of PDR and range on different scenarios where WSN are likely to be deployed. We acknowledge that the ideal approach would be to run the experiments several times, well separated in time in order to provide results richer in statistical relevance. By doing this, we can reduce the impact that transient effects may have in the results. In addition, experiments should be repeated with the RX nodes located half wavelength away in several directions from the selected measurement point. This would be useful in order to discard positions where multi-path fading can heavily attenuate the radio signal.

Nonetheless, these empirical results are taken in real-world scenarios. This provides a snapshot of the performance of IEEE802.15.4g at the precise moment of the experiment, including few inconsistencies in some measurements due to external factors, as a real deployment would encounter. To the

best of our knowledge, these are the first experiments exploring the entire IEEE802.15.4g standard.

4.5.1 On the Longer Range of FSK-FEC and O-QPSK

Throughout the experiments, we can observe that the longest radio links were obtained when using the FSK-FEC and O-QPSK PHYs. This is expected as both set of PHYs have the highest sensitivity of all PHYs, delivering up to 141 dB of link budget (see Table 3.1, OQPSK-6.25).

OFDM radio signals are more robust against interference and multi-path effects. OFDM1-100 uses 104 sub-carriers (96 data and 8 pilot tones) with 4x frequency repetition (there are 4 sub-carriers with the same information), providing a high level of robustness. OFDM2-50 has the same characteristics but half of the sub-carriers and thus, half of the data rate.

Each OFDM option 1 channel occupies 1.2 MHz and the 4 equal sub-carriers are separated by the same distance (in frequency). Even if 3 sub-carriers get compromised during one symbol transmission on the path towards the receiver, this can still recover the information. Even though that robustness is provided, in Table 4.1 the PDR for this PHY is just 31% and 5% for short and long packets at 700 m. For OFDM2-100, the PDR increased to 92% and 47%. This PHY is 2 dB more sensitive than OFDM1-100. We see in Table 3.1 that the maximum power for OFDM is +11 dBm whereas for the rest is +14 dBm.

Our believe is that the longer range of the O-QPSK and FSK-FEC PHYs can be attributed to their higher sensitivity in comparison to the rest of the PHYs tested. FSK-FEC holds 5 dB, 5 dB and 8 dB higher sensitivity than its non-FEC counterpart (2FSK-50, 2FSK-100, 4FSK-200). When compared 2FSK-50 with OQPSK-50, the difference is 8 dB.

The reason why OFDM PHYs do not reach as far as these PHYs is that they present a lower sensitivity and a lower maximum TX power.

These values of sensitivity and maximum TX power are directly dependent of the hardware and can vary depending on the manufacturer.

4.6 Summary

This chapter presents a performance evaluation, through experimentation, of the entire IEEE802.15.4g on the European 863-870 MHz band in scenarios where low-power networks are likely to be deployed. Today, most deployments use IEEE802.15.4 - OQPSK at 2.4 GHz and typically required relay nodes. With radio links of more of 700 m in the LoS and Urban Canyon scenarios, we believe this technology can be beneficial on low power networks because can reduce the need of these relay nodes, while providing an acceptable connectivity.

Chapter 5

Is IEEE802.15.4g OFDM useful for Smart Building Applications?

This chapter focuses on the applicability of the IEEE802.15.4g OFDM in the Smart Building context. Section 2.2.3 explains in detail this technology and how it is implemented in the IEEE802.15.4 standard. In most of the Smart Building applications, the ruling PHY technology used is the IEEE802.15.4 - PHY used at 2.4 GHz, with 16 channels and 250 kbps data rate.

We compare this well-known and widely implemented PHY against the IEEE802.15.4g SUN OFDM options 1 and 2 with high data rates (400 kbps and 800 kbps) in the sub-GHz band, strictly from the user's point of view and inside a office building where smart building applications are likely to be deployed.

We understand the impact changing frequencies (sub-GHz and 2.4 GHz) has on many different metrics, including range. Some might even qualify comparing 2.4 GHz O-QPSK with sub-GHz OFDM as "unfair". Yet, this comparison is purely from an end-user point of view: *given the choice between technologies, and given that all operate in unlicensed bands, does it make sense to use Sub-GHz OFDM for a Smart Building application?*

Experimental results shown in Section 5.2 show that the PDR of IEEE802.15.4g-OFDM is higher than for IEEE802.15.4 O-QPSK, for all node locations where experiments take place. This holds even when sending 2047 B frames over IEEE802.15.4g-OFDM and 127 B over IEEE802.15.4 O-QPSK.

Section 5.1 details how experiments are conducted. Section 5.3 concludes that IEEE802.15.4g can be applied for Smart Building applications.

Radio Setting	Frequency	Data rate	Tx Current[1]	Rx Current
"O-QPSK"	2.4-2.484 GHz	250 kbps	64.5 mA	32.4 mA
"OFDM1@400"	863-870 MHz	400 kbps	70.0 mA	30.5 mA
"OFDM1@800"	863-870 MHz	800 kbps	70.3 mA	30.5 mA
"OFDM2@800"	863-870 MHz	800 kbps	70.8 mA	31.0 mA

Table 5.1: The PHY characteristics evaluated in this chapter.

5.1 Experimental Setup

We conduct this study through a number of experiments. We use 4 nodes to run an experiment: one is a transmitter (TX), the other 3 are receivers (RX). During an experiment, the nodes loop through all combinations of PHY, frequency and frame length, and, for each, measure the PDR of the link and RSSI value of each frame received.

We compare the performance of 2.4 GHz IEEE802.15.4 O-QPSK and sub-GHz IEEE802.15.4g OFDM. The former is almost synonymous with smart building applications, and therefore represents a baseline. The latter is newer, and promises exceptional performance in environment in which multi-path fading is very present.

Each test considers all 31 radio settings, covering all IEEE802.15.4 and IEEE802.15.4g modulations. For reasons of space, and to provide the reader with the most insightful information, we only present results for the following 4 PHYs: 2.4 GHz O-QPSK at 250 kbps, sub-GHz OFDM option 1 at 400 kbps, sub-GHz OFDM option 1 at 800 kbps and sub-GHz OFDM option 2 at 800 kbps. Table 5.1 provides an "alias" and assigns a color for each PHY. These are used throughout the remainder of this chapter.

The rPi of each node runs a Linux Debian distribution, and is connected to the Internet over WiFi. We connect over SSH to each node to remotely launch the test scripts. The test scripts are written in Python, and drive the radio throughout an experiment[2]. The scripts are responsible for having the TX node loop through all combinations of modulation, frequency and frame length, and, for each, send 100 frames. On the RX side, the scripts are responsible for (re-)configuring the radio so it is listening on the same frequency using the same modulation as the TX node at the same time. TX and RX nodes are synchronized over NTP. Appropriate guard times are introduced to ensure that the RX node is listening when the TX node transmits a frame.

The frame lengths considered depend on the PHY. For OFDM, the TX node sends frames of lengths 127 B and 2047 B. For IEEE802.15.4 O-QPSK, the TX node sends frames of length 127 B. Similarly, the frequencies consid-

[1] +8 dBm power transmission

[2] As an online addition to this paper, all the software is published under an open-source license at `https://github.com/openwsn-berkeley/range_test`.

ered depend on the physical layer. For OFDM, there are 5 and 8 available frequencies for option 1 and 2, respectively. For the 2.4 GHz frequency band, there are 16 frequencies. In all cases, the inter-frame spacing is 20 ms and the TX power is +8 dBm.

An experiment – looping through all modulations, frequencies and frame lengths – takes roughly 30 min. During an experiment, an RX node logs, for each frame received, the modulation and frequency it listens on, the counter contained in the frame, whether its FCS is correct and the RSSI value. Because 100 frames are sent for each modulation/frequency/length, the PDR for that setting can be computed.

5.1.1 Radio Characteristics

Table 5.1 gives the current draw of the AT86RF215 radio chip, at 3.3 V, for each radio setting. Because the chip's datasheet does not provide the current draw for each setting, we measured it. For each radio setting, we configure the TX node to transmit in continuous transmission mode, and measure the current draw using an ammeter.

Table 5.1 also details the sensitivity of the AT86RF215 radio chip, for each radio setting, as read from the datasheet[3].

5.1.2 Deployments

Fig. 5.1 shows a floorplan of the deployment area, the Inria office building in Paris, France. The ceiling is metallic, the floor is covered with carpet, external concrete walls have glass windows. Two concrete staircases and two elevator shafts are at the center of each floor.

A total of 3 experiments are conducted, during business hours (people are moving around and WiFi being actively used). All nodes are mounted on 1.8 m PVC poles. Between experiments, only the RX nodes are relocated, the TX node stays in the same position. Over the course of the 3 experiments, the RX nodes are placed at 8 locations on the same floor as the TX node, and at 3 locations on the floor above.

5.2 Experimental Results

In total, we collected 57,200 atomic measurements, one for each frame, RX location, frequency, frame length, and index. This dataset contains a wealth of information. The goal of this section is to explore this dataset and extract the lessons they contain.

[3] The sensitivity for IEEE802.15.4g is defined as the RSSI which yields 10% PER with 250 B frames. The sensitivity for IEEE802.15.4 is defined as the RSSI which yields 1% PER with 20 B frames.

Figure 5.1: Floorplan of the deployment area.

RX node	O-QPSK *(250 kbps)*	OFDM1@400 *(400 kbps)*		OFDM1@800 *(800 kbps)*		OFDM2@800 *(800 kbps)*	
	127 bytes	127 bytes	2047 bytes	127 bytes	2047 bytes	127 bytes	2047 bytes
1A	96 %	100 %	100 %	100 %	100 %	100 %	92 %
1B	78 %	100 %	100 %	100 %	100 %	97 %	92 %
1C	91 %	100 %	100 %	100 %	100 %	100 %	100 %
1D	88 %	100 %	100 %	100 %	100 %	100 %	100 %
1E	81 %	100 %	100 %	100 %	100 %	100 %	100 %
1F	62 %	94 %	92 %	89 %	89 %	85 %	75 %
1G	81 %	100 %	100 %	100 %	98 %	99 %	96 %
1H	71 %	100 %	100 %	99 %	99 %	99 %	94 %
2A	0 %	100 %	100 %	100 %	100 %	100 %	98 %
2B	0 %	88 %	80 %	74 %	44 %	4 %	0 %
2C	0 %	0 %	0 %	0 %	0 %	0 %	0 %

Table 5.2: The Packet Delivery Ratio (PDR) of the wireless link for multiple positions of the RX node, for each radio setting and frame length.

5.2.1 The Longer Range of OFDM

Table 5.2 gives the average PDR value over all frequencies available per PHY and per RX node location. It shows three tiers of RX positions. In the first tier (positions 1A through 1E), the receiver and transmitter nodes are close. PDR is over 80% in all cases, for both OFDM and O-QPSK. In the second tier (1F–1H), the PDR of O-QPSK starts decreasing (down to 62%), whereas the PDR of OFDM stays above 75%. In the third tier (2A–2C), OFDM still offers some connectivity while O-QPSK is not able to get any frame across.

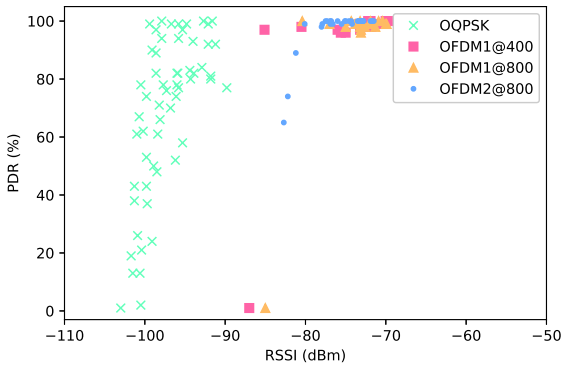
Fig. 5.2 depicts the PDR/RSSI relationship for nodes 1F, 1G and 1H. Each dot corresponds to the PDR/average RSSI relationship for 100 frames of 127 B sent on one frequency[4]. All the OFDM samples exhibit a higher RSSI than O-QPSK. OFDM is well inside the sensitivity of its radio, O-QPSK presents samples closer to the sensitivity. This is expected given the difference in frequency [76].

Yet, there is more involved than simply the difference in frequency. Because it operates at 2.4 GHz, O-QPSK should suffer from external interference from WiFi. By transmitting on multiple frequencies at the same time, OFDM should also be more robust against multi-path fading. We witness both phenomena in Sections 5.2.2 and 5.2.3, respectively.

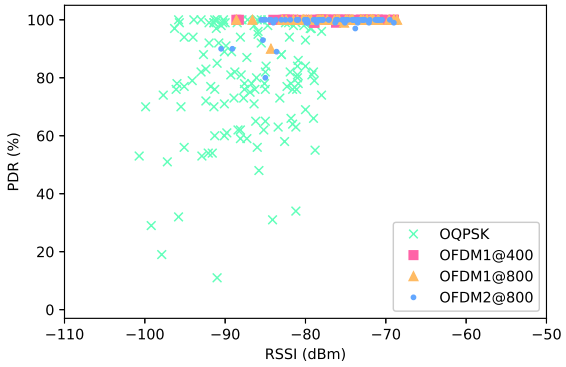
5.2.2 The (Limited) Impact of WiFi Interference over O-QPSK

Fig. 5.3 shows the average PDR for each IEEE802.15.4 frequency at 2.4 GHz, for positions 1F, 1G and 1H. At the same time as the experiment was

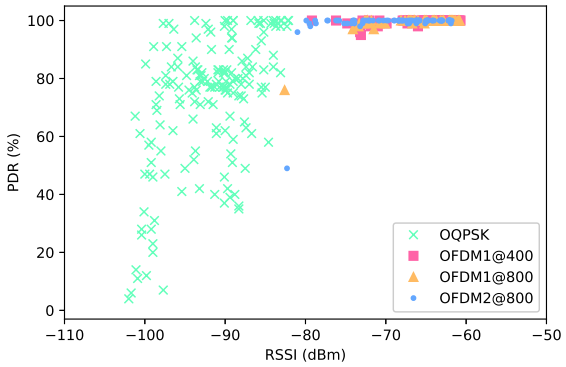
[4] Some experiments were run multiple times, which is why there are more dots than there are frequencies available.



(a) node 1F



(b) node 1G



(c) node 1H

Figure 5.2: PDR vs RSSI (127 B frames).

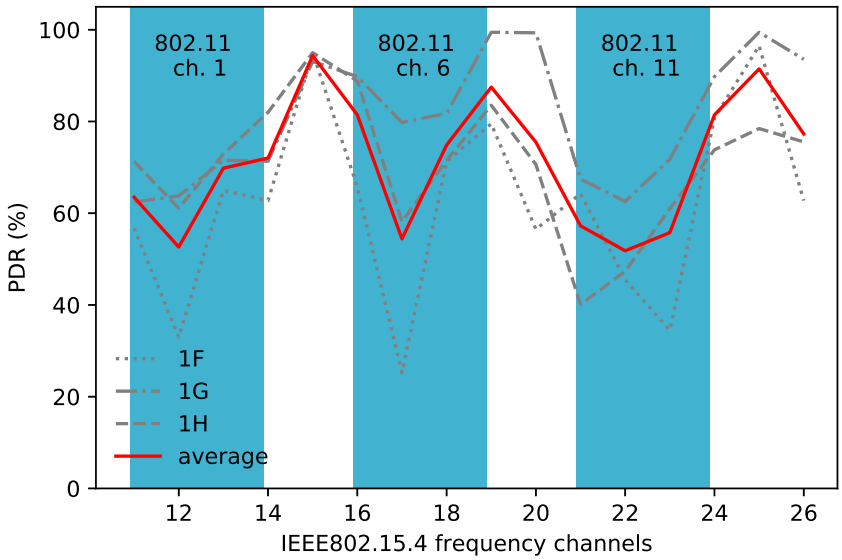


Figure 5.3: Average PDR per channel on locations 1F, 1G and 1H.

conducted, WiFi was operating in the building on IEEE802.11 channels 1 (2.412 GHz), 6 (2.437 GHz) and 11 (2.462 GHz). WiFi channels are 22 MHz wide, each covering roughly 4 IEEE802.15.4 frequencies. Fig. 5.3 clearly shows a degradation in the PDR for IEEE802.15.4 frequencies in the WiFi channels, from 80-90% down to 50-60%. Yet, this impact is small, and will just require an IEEE802.15.4 radio to retransmit more often when operating in a WiFi channel. That effect alone does not explain the better PDR of OFDM presented in Table 5.2.

5.2.3 The Power of Frequency Repetition

Table 5.2 shows that, at 127 B, OFDM1@400 and OFDM1@800 perform the same. The difference between OFDM1@400 and OFDM1@800 is that only the former uses a 2× frequency repetition, meaning that each portion of data is repeated on two different frequencies. This means that if multi-path fading prevents the receiver from correctly decoding the frame on one frequency, it should be able to on the second copy. Of course, enabling 2× frequency repetition reduces the data rate by half.

When increasing the frame length, however, things change. With 2047 B frames, it takes the radio longer to transmit the frame. At a constant bit error rate, it is normal to have a higher frame error rate. Table 5.2 clearly shows the benefit of frequency repetition: from RX location for example enabling frequency repetition for a 2047 B frame raises the PDR from 44%

to 80%.

The resulting recommendation is hence to use frequency repetition when the PDR of the link is marginal.

5.2.4 The Importance of Using a Wide OFDM Band

In order to achieve a high data rate, the radio can be configured to use a lower OFDM option (more sub-carriers in the channel) and/or a higher MCS value (higher data rate per sub-carrier). We want to explore which approach is better, from a PDR point of view. In particular, we compare OFDM1@800 and OFDM2@800: they both result in the same data rate (800 kbps), OFDM1@800 by using more sub-carriers, OFDM2@800 by increasing the data rate of each subcarrier (16-QAM has a constellation size of 16, QPSK a constellation of 4).

Location 2B in Table 5.2 satisfies our trade-off. From a PDR perspective, using a wide band yields good connectivity (74% PDR with 127 B), while using a higher MCS number as in OFDM2@800 causes the communication to be almost impossible (4% PDR with 127 B).

The resulting recommendation is hence to use the lowest possible OFDM option (wider channels), even if this means fewer channels.

5.2.5 Resulting Battery Lifetime Comparison

Table 5.1 indicates the current draw of the radio in each mode[5]. We assume a state-of-the-art MAC protocol, such as TSCH, which ensures that a node's radio is only on when needed (no idle listening).

We want to compute the charge the TX node needs to successfully send a 127 B to an RX node, for several locations. The term "successfully" implies retransmissions: if the PDR of the link is 50%, the TX node will have to transmit on average twice. Eq. (5.1) expresses that charge. C is the charge in Coulomb, d is the duration a radio needs to send the 127 B frame, I is the current the radio draws when transmitting, and PDR is the Packet Delivery Ratio (a number between 0.0 and 1.0) of the link between the transmitter and receiver nodes.

$$C = \frac{d \times I}{PDR} \tag{5.1}$$

Fig. 5.4 plots (5.1) for nodes 1F–2B, for all 4 radio settings. OFDM is more efficient than O-QPSK, in all cases. This is because the PDR of O-QPSK is lower than OFDM, and because OFDM has a higher data rate.

[5] There are radios on the market which draw significantly less current for O-QPSK (9.7/4.5 mA TX/RX current for Analog Devices' LTC5800). While exact numbers presented in this section will be different with different hardware, the conclusions hold.

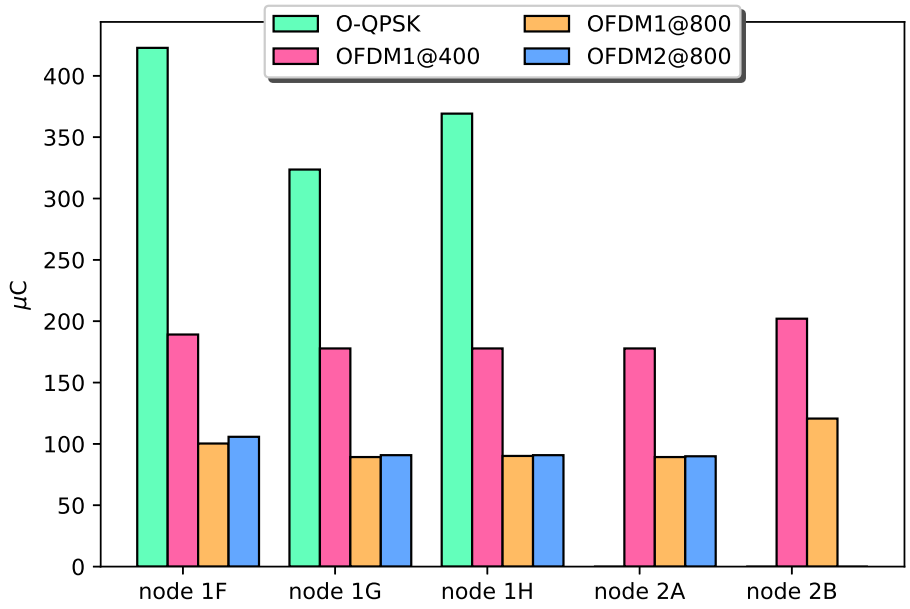


Figure 5.4: Charge needed by the TX node to successfully transmit a 127-byte frame to a particular RX node, including retransmissions. For positions 2A and 2B, the computation cannot be done for O-QPSK and OFDM2@800, as the PDR is zero.

While a more complete benchmarking/analysis (possibly using different radios, and taking radio wake-up times and acknowledgment overhead into account), the superiority of OFDM Fig. 5.4 shows is so clear that the trend will still hold.

5.3 Discussion

The overall lesson learnt from this chapter is that OFDM should not (no longer) be overlooked for low-power wireless networks, in particular in Smart Building applications. Not only are OFDM-capable radios readily available on the market, their performance meets the expectations. Their range is better than traditional 2.4 GHz O-QPSK, with techniques such as frequency repetition very efficiently handling multi-path fading and external interference directly at the physical layer. Current OFDM radios still consume in the order of 6× more than the best-in-class 2.4 GHz O-QPSK counterparts, but that is bound to change as inter-vendor competition kicks in.

For Smart Building applications, this paper makes the recommendation of using OFDM option 1, with MCS2 with short (<128 B) frames, MCS3 otherwise.

It is clear that a MAC-layer scheme will need to be introduced (for exam-

ple through the 6TiSCH standardization action) which exploits the agility of these radios: for each frame, agree with your neighbor on the most appropriate radio setting.

5.4 Summary

IEEE802.15.4g is designed for Smart Utility Network applications. We want to determine whether this standard is useful outside of these applications. One example of an IoT application outside the SUN is found in the Smart Building context. So we compare IEEE802.15.4g OFDM in sub-GHz bands against what is used today on Smart Building, IEEE802.15.4 - O-QPSK. We conclude that IEEE802.15.4g OFDM outperforms its counterpart IEEE802.15.4 - OQPSK, and therefore is a valid option for these applications.

Chapter 6

Does Channel Hopping Makes Sense with IEEE802.15.4g OFDM at 2.4 GHz?

Previous chapters show that IEEE802.15.4g can be used in sub-GHz for more applications other than in the Smart Utility Networks context. In this chapter, we analyze the use of IEEE802.15.4g OFDM at 2.4 GHz, and determine whether it is relevant for low-power wireless applications and if so, how it should be used.

We compare the performance of the IEEE802.15.4g OFDM option 1 (both MCS0 and MCS3) against IEEE802.15.4 O-QPSK throughout the complete 2.4 GHz band. We use the O-QPSK as a base of performance due to its wide acceptability by the industry. This allows us to determine whether OFDM is a valid alternative for low-power wireless. We base our analysis on a comprehensive connectivity dataset, 141,587,000 points, collected continuously over 21 days.

6.1 Using OFDM PHY at 2.4 GHz

We do not know what is the MAC layer that would make the most of the IEEE802.15.4g OFDM PHY. One hint is not to use the same channel hopping approach, since OFDM per se exploits the frequency diversity as TSCH but at the physical layer[1].

The OFDM options and MCS values are independent of the frequency band used. The only change occurs in the amount of channels available on each frequency band. In the 2.4 GHz band, only 16 channels are available for O-QPSK; 64 channels are available with OFDM option 1 (up to 416 for option 4). The reason is that OFDM does not need a frequency space guard

[1] More on the OFDM PHY in section 2.2.3.

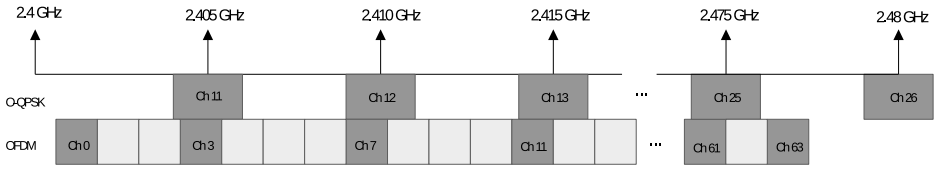


Figure 6.1: The O-QPSK PHY of IEEE802.15.4-2015 divides the 2.4 GHz band into 16 channels, each 2 MHz wide, separated by 5 MHz. The OFDM option 1 PHY divides the band into 64 channels, 1.094 MHz wide, separated by 1.2 MHz. Greyed-out channels are the ones used in our experiments.

as O-QPSK does, since all sub-carriers are orthogonal to one another of any channel across the complete band. Fig. 6.1 shows how O-QPSK and OFDM channelize the same 2.4 GHz frequency band.

6.2 Experimental Setup

This study is carried out by successive experiments using 4 nodes: one transmitter (TX) and three receivers (RX). In an experiment, the four nodes configure their radios with the three PHYs: IEEE802.15.4 - OQPSK, IEEE802.15.4g OFDM opt. 1 MCS0 (100 kbps) and IEEE802.15.4g OFDM opt. 1 MCS3 (800 kbps). More details in table 2.2.

We choose the OFDM option 1 due to the benefits of a wide OFDM band (section 5.2.4) with the lowest and highest MCS value (MCS0 and MCS3) for that option. MCSO provides the highest level of robustness with 4× frequency repetition whereas MCS3 the lowest with no frequency repetition.

In IEEE802.15.4 O-QPSK, the nodes tune their radios to the 16 channels available in the 2.4 GHz frequency band. In IEEE802.15.4g OFDM, we switch between 17 channels, a subset of the 64 available (see rationale in Section 6.2.1).

6.2.1 Software

A Linux Debian distribution is running on the rPi of each node. Nodes are synchronized over NTP. A number of scripts drive the experiment[2]. These scripts configure the radios with a specific PHY, frequency, and for enough time to allow the TX node to send 1,000 127 B frames. TX power is +8 dBm; the spacing between frames is 20 ms. The experiment runs continuously: the nodes loop through all PHY settings, each time sending 1,000 frames.

[2] The software used for these experiments is available under an open-source license at `https://github.com/openwsn-berkeley/range_test/releases/tag/REL-3.0.0`.

center frequency	O-QPSK channel
2.400 GHz	
2.405 GHz	11
2.410 GHz	12
2.415 GHz	13
2.420 GHz	14
2.425 GHz	15
2.430 GHz	16
2.435 GHz	17
2.440 GHz	18
2.445 GHz	19
2.450 GHz	20
2.455 GHz	21
2.460 GHz	22
2.465 GHz	23
2.470 GHz	24
2.475 GHz	25
2.480 GHz	26

OFDM channel	center frequency
0	2.4012 GHz
3	2.4048 GHz
7	2.4096 GHz
11	2.4144 GHz
16	2.4204 GHz
20	2.4252 GHz
24	2.4300 GHz
28	2.4348 GHz
32	2.4396 GHz
36	2.4444 GHz
41	2.4504 GHz
45	2.4552 GHz
49	2.4600 GHz
53	2.4648 GHz
57	2.4696 GHz
61	2.4744 GHz
63	2.4768 GHz

Table 6.1: Center frequencies of the channels used for IEEE802.15.4 O-QPSK and OFDM

Because looping over 64 channels for OFDM would be too time consuming, they loop over the subset of 17 channels listed in Table 6.1, which are chosen to almost match the frequencies used in O-QPSK. In total, 50 channels are tested: 16 in O-QPSK, 17 in both OFDM option 1 MCS0 and MCS3.

For each frame it receives, the RX node logs the PHY and channel used, the sequence number in the received frame, the RSSI value and whether the FCS is correct. Since 1,000 frames are sent, we can compute the PDR for each PHY/channel combination, and see its evolution over time.

We conduct the experiments within the Inria-Paris building in France. Fig. 6.2 shows the location of the nodes. The floor is covered with carpet, the ceiling is metallic, with two concrete staircases and two elevator shafts in the center of the floor. Divisions between offices are made of glass and prefabricated walls. External walls are made of concrete with glass windows.

The nodes are installed on 1.8 m PVC poles. Experiments were conducted for 21 continuous days, with people around and WiFi being actively used during business hours.

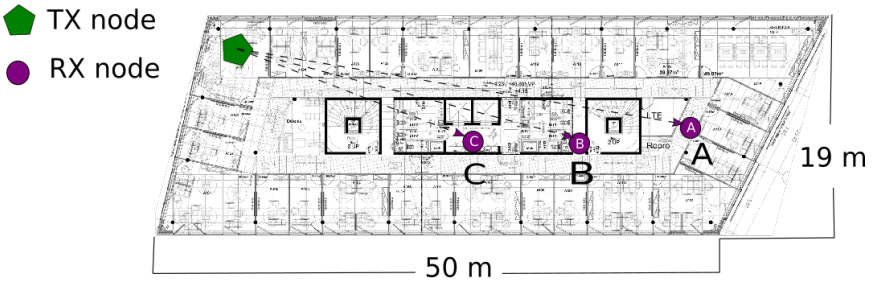


Figure 6.2: The location of the nodes in the Inria-Paris building during the 21-day experiment.

PHY	Node A	Node B	Node C
O-QPSK *(250 kbps)*	82%	61%	83%
OFDM Option 1 MCS0 *(100 kbps)*	85%	76%	92%
OFDM Option 1 MCS3 *(800 kbps)*	92%	77%	93%

Table 6.2: PDR for each node, averaged over time and over all channels.

6.3 Experimental Results

We collected a dataset of 141,587,000 atomic measurements. This section lists the lessons learnt from analyzing this dataset.

6.3.1 On the PDR over the 2.4 GHz frequency band

Table 6.2 shows the PDR of the three links for each PHY layer, averaged over time and over all channels. While it is impossible to draw any general conclusion about data gathered over just 3 links, we can make two interesting observations. First, OFDM consistently yields a better PDR than O-QPSK. Second, MCS3 yields a better PDR than MCS0, even when it offers a much higher data rate and uses no frequency repetition. This will be explained in Section 6.3.5.

The average PDR does not give us nearly as many insights as Fig. 6.3, which plots the PDR of each link evolving during the 21 days of the experiment, *for each channel*. Fig. 6.3 is for node B, equivalent lessons learnt appear for the other nodes. Drawing a subplot for each channel allows us to

"see" the effect of external interference and multi-path fading on a channel-by-channel basis. For easier readability, each subplot is highlighted in green when PDR>50%. This section makes a number of qualitative observations which are analyzed in greater detail in subsequent sections.

Fig. 6.3 shows that there is no single frequency that is "good" all the time. The PDR on each frequency is dynamic, as a result of changes in the environment. One can clearly see week-end/weekday and day/night transitions.

These dynamics in PDR are caused by multi-path fading and external interference. It is entirely expected – and well documented – in the IEEE802.15.4 O-QPSK case. In an entirely counter-intuitive manner, they are also equally present in OFDM. OFDM was designed to combat multi-path fading and external interference at the PHY layer, by encoding data on dozens of frequencies. One would expect the resulting frequency diversity at the PHY layer to cause the per-channel PDR to be very stable. The reason we *do* see PDR dynamics in OFDM is that the channels are only 1.094 MHz wide: multi-path fading and external interference affect *all* sub-carriers at the same time. As a result, **OFDM alone does not provide a sufficient mechanism in IEEE802.15.4 at 2.4 GHz to combat external interference and multi-path fading.**

6.3.2 Impact of Nearby WiFi

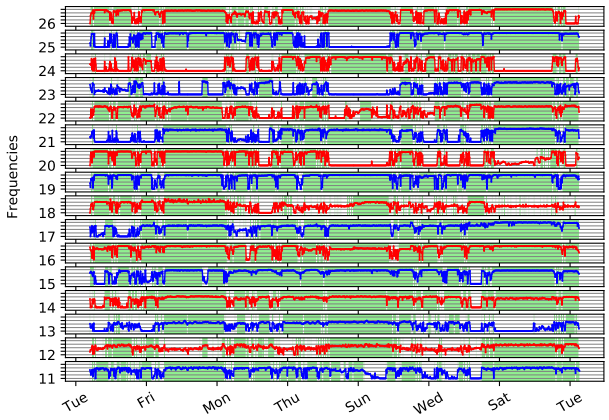
Fig. 6.3b shows a constantly bad link for channels 3, 7, 11. This can be attributed to external interference. To verify this, we use the `iwlist` Linux utility to list the RSSI and frequency of the WiFi signals received by node B, see Fig. 6.4. WiFi activity is centered on WiFi channels 1 (2.412 GHz), 6 (2.437 GHz) and 11 (2.462 GHz). Node B receives 21 WiFi signals; the highest noise level is in the 2.404–2.414 GHz band, the same as channels 3, 7, 11 in Fig. 6.3b.

Section 6.3.5 further details why the same does not happen to MCS3.

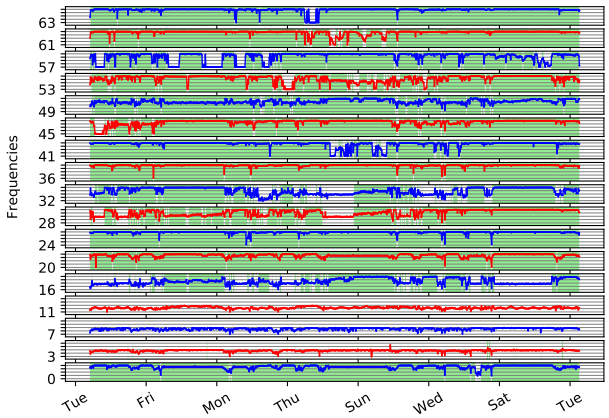
6.3.3 Quantifying Multi-path Fading in OFDM

Multi-path fading causes some frequencies to exhibit a PDR above 50%, others below. The experiment is conducted in cycles of approximately 30 min, during which the TX node sends 1,000 frames on each PHY and channel. This means that, every 30 min, we can compute the PDR of each link, on each channel, for each PHY.

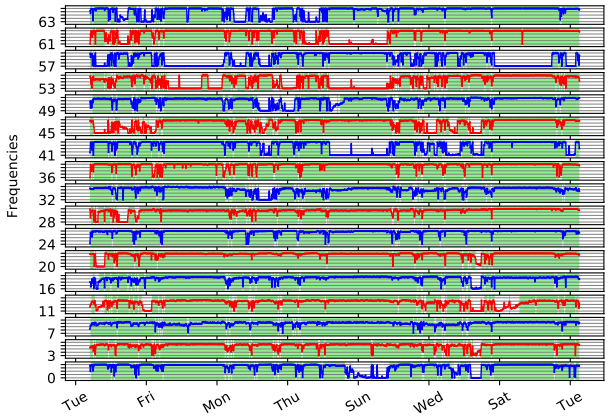
Fig. 6.5 plots the number of channels which exhibit a PDR above 50%. In the absence of external interference and multi-path fading, either all channels would be good, or bad. That is, there would be a single bar at the maximum number of channels.



(a) O-QPSK *(250 kbps)*



(b) OFDM option 1 mcs 0 *(100 kbps)*



(c) OFDM option 1 mcs 3 *(800 kbps)*

Figure 6.3: PDR per PHY channel for node B during 21 days. Areas in green indicate PDR greater than 50%.

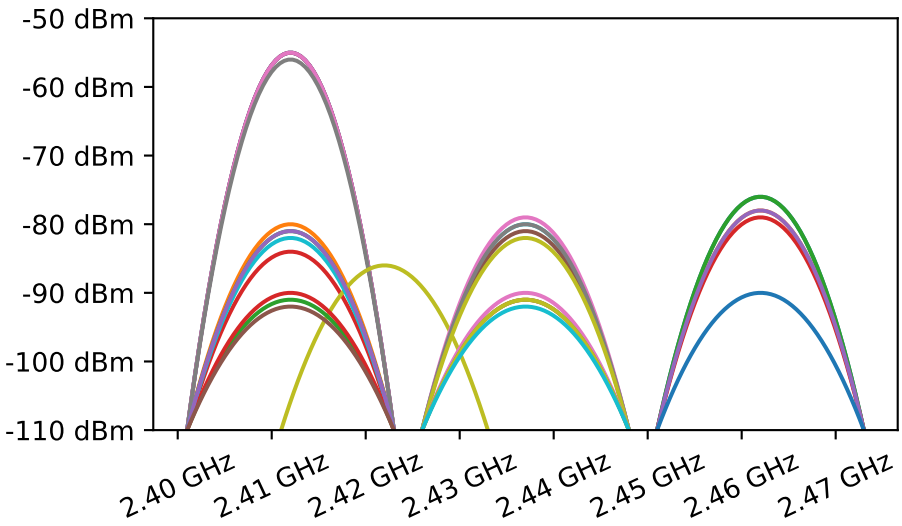
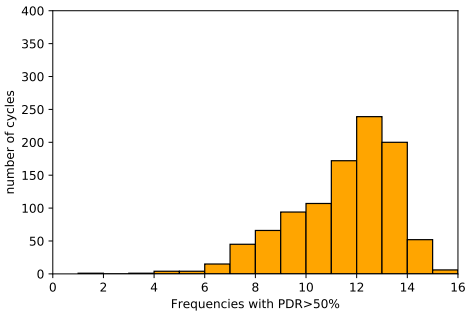
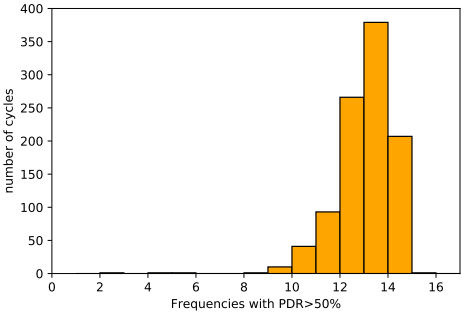


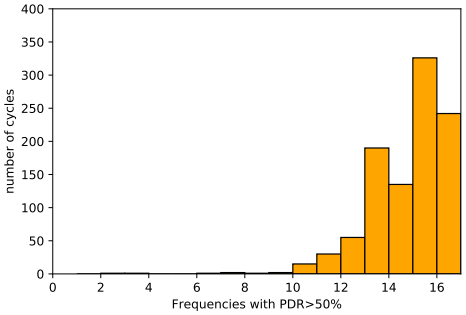
Figure 6.4: Strengths of the WiFi signals received at node B.



(a) O-QPSK *(250 kbps)*

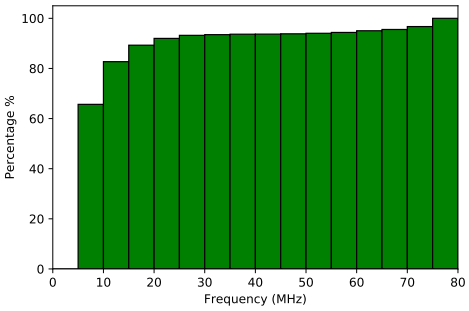


(b) OFDM option 1 MCS0 *(100 kbps)*

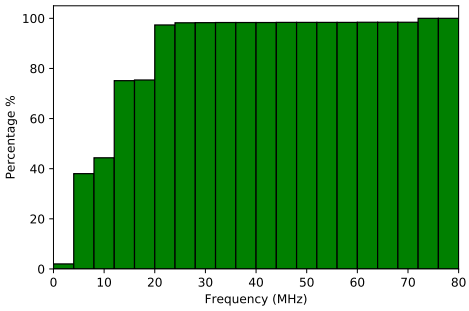


(c) OFDM option 1 MCS3 *(800 kbps)*

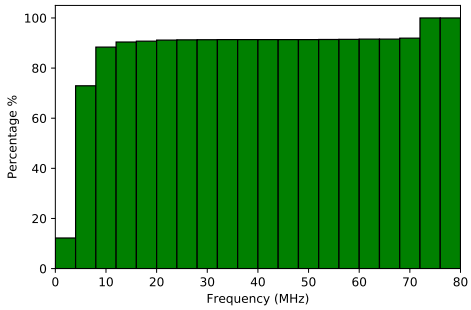
Figure 6.5: Number of frequencies with PDR>50%, for node B.



(a) O-QPSK *(250 kbps)*



(b) OFDM option 1 MCS0 *(100 kbps)*



(c) OFDM option 1 MCS3 *(800 kbps)*

Figure 6.6: Coherence bandwidth.

Rather, we see that, for O-QPSK, in most of the cases 13 channels are "good", the remaining 3 being affected by multi-path fading or interference. This is a simple way of "seeing" those effects, and is entirely expected for O-QPSK. What is counter-intuitive is that **OFDM is affected by multi-path fading and external interference in a way similar to O-QPSK.**

6.3.4 Coherence Bandwidth

When node A sends a frame to node B on frequency f_1, and that transmission fails because of multi-path fading, a valid approach is to re-transmit on a different frequency f_2. We are interested in understanding how far f_2 should be from f_1 to offer enough frequency diversity. We call "coherence bandwidth" the difference $|f_2 - f_1|$ which is sufficient for a link to transition from "bad" (PDR<50%) to "good" (PDR>50%).

We explore this experimentally in our dataset: we find a frequency with PDR<50%, and see how big a frequency shift is needed to result in PDR>50%. Fig. 6.6 shows the result. When using O-QPSK (fig. 6.6a) and OFDM option 1 MCS3 (fig. 6.6c), a frequency shift of 10 MHz is sufficient 60% of the time. For OFDM option 1 MCS0, a frequency shift of 10 MHz is

sufficient 40% of the time, 80% of the time with a shift of 20 MHz.

6.3.5 Pros and Cons of Frequency Repetition

Section 5.2.3 shows how frequency repetition improves the PDR of links at sub-GHz frequencies. Higher levels of frequency repetition should result in a higher PDR. This is not what we see when comparing MCS3 (no repetition) to MCS0 (4 × repetition).

The reason is that frequency repetition increases the time on air of a frame, making it more prone to collisions with other radio signals. As seen in Fig. 6.4, there are WiFi networks in the proximity of node B, each of which emits beacons at least every 100 ms, even when the WiFi network sits idle. A 127 B frame takes with OFDM option 1 MCS0 (100 kbps) roughly 10 ms to be transmitted, only 1.27 ms with MCS3 (800 kbps). **Frequency Repetition is useful only if there is no strong external interference**.

6.4 Discussion

This chapter investigates the usefulness of IEEE802.15.4 OFDM at 2.4 GHz, how it compares to O-QPSK, and how it should be used. Our analysis is based on a 141,587,000-point connectivity dataset gathered indoors over 21 days. We show that OFDM alone does not yield immunity to multi-path fading and external interference. We recommend combining OFDM *with* channel hopping at the MAC layer, with subsequent channels in the hopping sequence separated by at least 20 MHz. In the presence of nearby WiFi access points, we further recommend using OFDM option 1 MCS3 (i.e. without frequency repetition), with frames shorter than 127 B.

6.5 Summary

In this chapter, we acknowledge the capabilities of IEEE802.15.4g OFDM, such as its robustness against multi-path fading environments and inter-symbolic interference. Since this PHY can be used in sub-GHz bands as well as at 2.4 GHz, we want to determine what should be the policy when using this PHY at 2.4 GHz. We know from previous work that channel hopping is an useful technique to mitigate the effects of multi-path fading and external interference. Since the OFDM version has more properties already embedded at the physical level, i.e. frequency repetition and FEC over each sub-carrier, we want to know whether the Channel Hopping technique is useful, or whether OFDM alone is enough to manage the challenges impacting O-QPSK. Though experimentation, we determine that channel hopping is still interesting when using IEEE802.15.4g OFDM, but that frequency repetition may be harmful where heavy external interference is present. We

recommend the use of the fastest OFDM PHY in order to be less prone to external interference.

Chapter 7

Towards Agile Networking

7.1 Agile Networking Concept

Low-power mesh network devices had, traditionally, only one radio interface. Today, a new wave a low power devices has appeared and is changing this: devices with a single radio chip capable of change their radio configuration in order to comply with several norms/standards.

This opens the door to a new possibility of networks: Agile Networking. Low-power devices capable of (re-)configuring their radio interfaces dynamically on a frame to frame basis. This is an uncharted situation on low-power mesh networks. Motes creating radio links with other motes with different radio configurations. This new approach will impact in the protocol stack. The first part of this chapter describes how Agile Networking affect the 6TiSCH stack Then, it details the environment where these network can be experimented with and evaluated.

7.2 Impact on the 6TiSCH Protocol Stack

The protocol stack in a IPv6 over the TSCH mode of IEEE802.15.4e (6TiSCH) network is defined by multiple protocols covering multiple layers starting from the data link layer, up to the application layer (depicted in Fig. 2.6). The *de facto* PHY of this protocol stack is the IEEE802.15.4 standard.

However, since the introduction of IEEE802.15.4g, it is now possible to choose another PHY, and to change its settings. Apart from the difference in the technology used by IEEE802.15.4g, the frame size (up to 2047 B), frequency band and variable data rate (6.25 kbps up to 800 kbps) diverge from IEEE802.15.4.

Radio chips supporting all these new PHY configurations are now available, giving the opportunity to implementers to exploit the benefits of this diversity in terms of throughput, range and reliability that each PHY brings with it.

But it is not sufficient to just change one PHY for another. The adoption of a PHY different from IEEE802.15.4 poses new design considerations across the 6TiSCH protocol stack. Even though layer separation exists between protocols, from the link layer upwards, 6TiSCH protocols have been designed considering one PHY only. The approach of having radio links over multiple PHYs in the same 6TiSCH network is new, and poses hitherto unknown considerations for network designers.

This chapter describes how the behavior of each item of the 6TiSCH protocol stack may be impacted by the inclusion of multiple PHYs with such different properties.

7.2.1 Impact on Neighbor Table

In a low-power wireless network with nodes using a single PHY, nodes are neighbors if they are within their interference domain. Now, if nodes are able to use multiple PHYs, a pair of nodes using a given PHY may be neighbors and when using another PHY, they may not be neighbors.

Therefore, the definition of a neighbor node changes to any device within the same interference domain for a given PHY configuration. This modifies how nodes can manage their neighbors' information. This information is accessed from the MAC sub-layer up to the Network layer. In case of handling by the Data Link layer, a new entity is required between MAC and Routing layers to choose which PHY layer is going to be used. This entity could be part of a Scheduling Function (Section 7.2.3). In case of handling by the Routing layer, each PHY layer could be considered as a neighbor. For RPL, if only one DODAG exist through the network, a dedicated Objective Function for multiPHY features is required. If each PHY layer has a dedicated DODAG, the OF0 for 6TiSCH could be used with little modification. However, this increases the complexity of the network.

7.2.2 Impact on MAC layer

The considerations that arise according to the used PHY include network formation, node discovery, and TSCH configuration.

- **Network Formation**

  Getting nodes to join the network as fast as possible is a major interest to minimize energy consumption. Radio activity is the most power consuming task for nodes, therefore the more time nodes spend listening to get an Enhanced Beacon (EB) the more energy they consume, reducing their lifespan. Considering a current 6TiSCH network, with just one PHY and one frequency band (16 frequencies), nodes have to tune their radios in one frequency wait for an EB. Nodes which are already part of the network transmit EBs in a round-robin fashion on

these 16 frequencies. If the node did not receive any EB after some time, it may tune its radio on a different frequency and listen again for an EB. This means a node listen for a long time before hearing an EB.

In the case of multiple PHYs, nodes attempting to join the network need to over even more PHYs, until hearing an EB. A mechanism might be needed to reduce join time, for example use a particular PHY for joining.

- **Discovering Node PHY Capabilities**

  For 6TiSCH networks using one PHY configuration, discovering the PHY neighbor node's capabilities is not necessary. But in a new multi-PHY network context, knowing the capabilities of neighbor nodes is important. Once a node is part of the network, it may have not have joined using the most convenient PHY configuration for this pair of nodes. Any of these nodes might then *(a)* unicast a request its neighbors to get the information about their PHY capabilities, or *(b)* discover the PHY capabilities of the neighbors by listening for EBs at specific times over other PHYs.

  If using *(a)*, further choices need to be taken to decide whether nodes would use shared slots or negotiate dedicated timeslots to test the connectivity over other PHYs. Agreeing on which PHY to test and when has to be done under the already tested PHY configuration, and the energy consumption footprint of this process may be too heavy. If using *(b)*, it may take long time until the most efficient PHY configuration is discovered between two nodes.

A multi-PHY approach has an impact on timeslot duration and channel hopping sequence.

- **Timeslot Duration**

  The diversity of data rates of the PHYs in the IEEE802.15.4-2015 standard makes it challenging to find a timeslot duration that is both efficient and fits all PHYs options. In current 6TiSCH networks, a common practice is to have a timeslot of 10 ms. This is time enough for transmitting a 127 B frame using IEEE802.15.4 - PHY, taking roughly 4 ms, to wait for the acknowledgment, leaving a handful of milliseconds for data processing with proper guard times.

  But for multiple PHYs with data rates going from 6.25 kbps up to 800 kbps and with maximum frame size of 2047 B, the time of transmission for a full size packet varies from 0.020 s (800 kbps) to 2.62 s (6.25 kbps). With such disparity, considering a timeslot long enough ($>$ 2.62 s) to allow the transmission (and its acknowledge frame) of the maximum frame size with the slowest data rate results in a waste of time (network

resources) if faster PHY can be used, by leaving the most part of the timeslot unused. Such a long timeslot would cause slotframes to have a duration in the order of minutes (considering for example a slotframe of 101 timeslots), and as tight synchronization is mandatory, multiple KA frames would have to be sent within the same slotframe, considerably reducing the network resources and efficiency.

On the other hand, choosing a shorter timeslot poses a rigid limitation in the size of the frames when slow data rates PHYs are used. By having timeslots in the order of 10's of ms, the frame size for slow data rate is heavily reduced: with a 100 ms timeslot, only 78 B can be transmitted using 6.25 kbps, without considering time for acknowledgment and guard times.

Multi-PHY designs should therefore tune these parameters to find the right trade-off between shorter or longer timeslots (limiting sizes of frames with some PHYs), as well as the size of the slotframe.

- **Channel Hopping Sequence**

  Current 6TiSCH implementations use the 2.4 GHz band, with 16 frequencies separated by 5 MHz and 2 MHz wide. Channel hopping sequences use only the frequency number identification. By introducing multiple PHYs, these do not have the same characteristics of channel spacing, bandwidth nor channel numbering. Moreover, channels from different PHYs may overlap.

  As a result, by only referring to a channel by some index doesn't carry over to multiple PHYs. Multi-PHY designs need to solve how to identify channels.

7.2.3 Impact on 6top sub-layer

The 6top sub-layer (Wang *et al.* [53]) is responsible for resource allocation (cells) between pairs of neighbor nodes. In a multi-PHY environment, cells have different capabilities depending on the PHY used. Moreover, in some frequency bands, duty cycle regulation must be met.

- **Resource Allocation**

  Current 6TiSCH networks account the network resources allocation in the amount of cells per slotframe a pair of nodes needs. In a multi-PHY design, allocating cells does not provide enough information, since depending on the PHY used, more or less data can fit in a timeslot. Multi-PHY designs have to define how to network resource needs are measured.

- **Duty Cycle Regulations**

Duty cycle regulations apply to most frequency bands. These regulations vary from country to country, so multi-PHY designs need to comply with local regulations. Therefore, the 6top sub-layer must control that each node does not exceed in the bandwidth occupation.

7.2.4 Impact on 6LoWPAN sub-layer

6LoWPAN has been initially designed with IEEE802.15.4 O-QPSK in mind. Header compression, fragmentation and reassembly are the main tasks of this adaptive layer. However, in this new context, other PHYs allow to send more than 127 bytes in one frame. 6LoWPAN functionalities should be adapted to efficiently fit in the layer below. This includes the sizes of the fragments that should be calculated depending on the PHY to be used and the maximum amount of data that can transport, given the length of the timeslot.

7.2.5 Impact on RPL Layer

In multi-PHY context, RPL is impacted in several ways: Objective Functions must now consider more than one PHY, and each node's rank must be calculated accordingly. A multi-PHY design may consider new Objective Functions that take into account the difference in throughput, resource occupancy and energy consumption of each PHY. For example, in Objective Funcion 0 (Thubert *et al.* [57]) , the rank factor can have a different value for each PHY, depending on its characteristics.

7.2.6 Summary

This section describes the needs that arise when considering to use more than one PHY in a IPv6 over the TSCH mode of IEEE802.15.4e (6TiSCH) network. These considerations are present in: the choice of the PHY, the configuration of the MAC layer, the 6top protocol, 6LoWPAN and RPL.

7.3 Thoughts on Evaluating Agile Networking

Agile Networking comes with great promises, and is a paradigm shift in low-power mesh networks. We consider that the starting point to understand the potential of Agile Networking is to have access to the right infrastructure in order to run experiments and be able to evaluate the properties of the resulting networks.

One question that rises is: *What are the benefits of Agile Networking when compared to a low-power mesh network featuring a single static radio configuration?* That is, *if we use a platform capable of changing radio configurations dynamically from one frame to another, will Agile Networking tend to converge to a single radio configuration?*

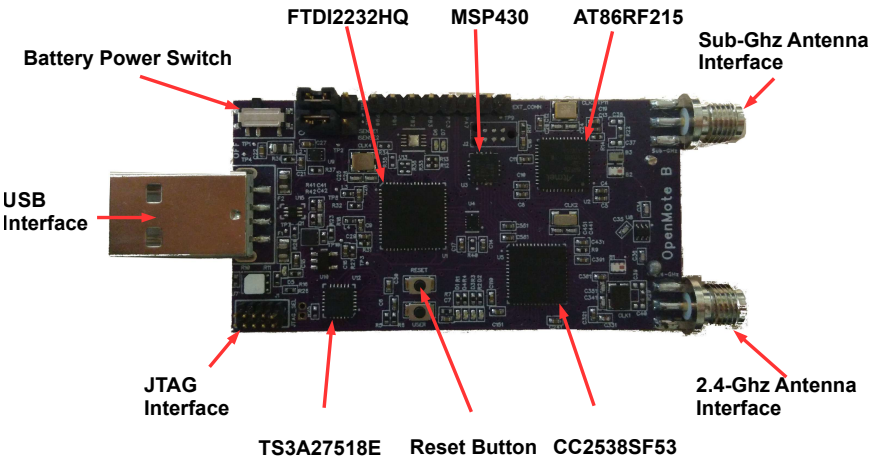


Figure 7.1: The Openmote B sensor node.

We believe that the right way to answer this question starts by implementing the 6TiSCH protocol stack, taking into account the considerations and recommendations detailed in section 7.2. Then, run experiments on a testbed and extract the Key Performance Indicators of the network.

From Chapter 4, we know that two of the most complementary radio configurations from the 31 available in IEEE802.15.4g standard are OFDM option 1 MCS3 (800 kbps) and 2-FSK FEC (50 kbps). With these radio configurations at sub-GHz and IEEE802.15.4 - OQPSK in 2.4 GHz, we can start designing an "Agile 6TiSCH" implementation in which motes dynamically change between those three radio configurations.

The remainder of this section details the different steps to being able to answer the questions above.

7.3.1 OpenMote B: an Agile Networking Platform

Together with the OpenMote company[1], we designed the OpenMote B specifically to be used for Agile Networking. The OpenMote B features two radios: the CC2538[2] IEEE802.15.4 compliant radio communicating at 2.4 GHz and

[1] `http://www.openmote.com/`
[2] `http://www.ti.com/lit/ds/symlink/cc2538.pdf`

the AT86RF215[3] IEEE802.15.4g compliant radio communicating in the sub-GHz bands. The latter implements all IEEE802.15.4g modes (FSK, OQPSK, OFDM). The CC2538 also contains an ARM Cortex-M3 micro-controller, and is connected to the AT86RF215 over SPI.

7.3.2 OpenTestbed: an Agile Networking Testbed

Like any networking technology, IoT solutions must to be extensively tested and validated before being applied to real-world problems. Running a high-level simulation of the general behavior of a solution is generally the first step. The second step is usually to run the firmware that fully implements the solution on a testbed, a collection of low-power wireless devices deployed in a controlled environment.

The key service a testbed offers is to be able to load new firmware onto the devices, and observe their behavior when that firmware runs. More advanced services include user and testbed reservation management, toolchains to compile the firmware, energy measurement, and storing logs. Testbeds are usually built as part of a large research project, and represent a significant effort. This can go as far as building dedicated hardware, installing dedicated wiring for powering and networking the testbed, and running a large number of management servers. The danger is that the resulting testbeds take a long time to build, are quickly outdated, and are deployed in dedicated rooms, which does not represent the wireless environment of most real-world deployments. That being said, these large institutional testbeds have made an enormous contribution in pushing the IoT research to making deployment-ready solutions.

For creating an Agile Networking testbed, we use a minimalistic approach very complementary to larger institutional testbeds. We ask ourselves the following questions. *What are the minimal services a low-power wireless testbed must offer? Can this be built using only off-the-shelf components? How can we make sure a testbed as easy to install and operate as possible?*

We designed the OpenTestbed and deployed it at Inria-Paris (see Fig. 7.2). This testbed features 80 OpenMote B boards. Appendix B details how this testbed is built, and gives 3 examples of institutions using it.

7.3.3 Generalizing the OpenWSN Implementation

OpenWSN is the reference 6TiSCH protocol stack implementation. For the OpenWSN stack to work, it needs to interact with the micro-controller and device peripherals of the board on which the stack is running. To accomplish this, OpenWSN provides a set of functions that need to be filled by the developer so the stack can interact with the hardware (including timers and

[3] `http://ww1.microchip.com/downloads/en/devicedoc/atmel-42415-wireless-at86rf215_datasheet.pdf`

Figure 7.2: The Inria-Paris OpenTestBed before deployment. 20 OtBox contain a total of 80 OpenMote B boards.

digital interfaces during execution. For devices with a single radio interface, this process is straightforward: when the stack needs to interact with the radio, it calls the functions and these execute the tasks required.

The Openmote-B has two radio interfaces, one for sub-GHz bands and the other for 2.4 GHz band. The micro-controller has to be able to communicate with both interfaces while using the same functions as for single-radio boards.

To solve this issue, the OpenWSN project creates one radio driver structure that gets as many instances there are PHYs supported. OpenWSN creates a helper structure interface[4], namely *"openradios"*, which interacts with each of the radio driver instances. When the OpenWSN stack needs to access one of the radio interfaces, it does so through the *"openradios"* structure that points to the right radio interface that needs to be accessed.

7.3.4 Next Steps

Agile Networking nodes open new horizons in the low-power mesh networking context. For instance, we have observed the interesting trade-offs between data rate, coverage, frequency band, allowed throughput (duty cycle regulations) and energy consumption found in IEEE802.15.4g. We think it would be interesting to define new 6TiSCH Scheduling Functions that take these trade-offs into account. Then, studies can be conducted about which SF correspond best to a particular application requirement.

In addition, it would be interesting to observe how Agile Networking affects the KPIs of the networks and how to use it to improve these values. Similarly, Agile Networking brings the necessity of defining new KPIs for these networks.

[4] More information at `https://github.com/openwsn-berkeley/openwsn-fw/blob/develop_FW-708/bsp/boards/common/openradios.h`

Chapter 8

Conclusions and Future Work

8.1 Contributions of this Thesis

The main contributions of this thesis is four-fold.

First, this thesis work focuses on evaluating the performance and applicability of IEEE802.15.4g in low-power wireless networking. Today, most low-power wireless solutions use IEEE802.15.4 - OQPSK operating at 2.4 GHz. Before of the range of that technology, relay nodes are sometime needed. By conducting experiments in real use case scenarios with off-the-shelf hardware, we show that, in LoS scenarios, radio links can be longer than 700 m with data rates of 50 kbps and more than 400 m with data rate of 800 kbps. We determine that, for environmental monitoring applications, using IEEE802.15.4g at sub-GHz frequencies allows one to reduce the number of nodes needed to cover wide areas.

Second, IEEE802.15.4 - OPQSK is the most prevalent technology in the smart building and home automation applications. The characteristics of OFDM PHYs make them, in theory, a good candidate for these applications in indoor scenarios. We want to determine whether the OFDM PHYs are useful for these indoor applications. We show that IEEE802.15.4g OFDM PHYs in sub-GHz bands outperform the ruling technology IEEE802.15.4 - OQPSK. Devices implementing OFDM should be considered to serve these types of applications. The only drawback is the increased current draw.

Third, we further compare the IEEE802.15.4g OFDM against IEEE802.15.4 - OQPSK, both operating at 2.4 GHz. Through experimentation, we show how, despite the frequency diversity OFDM brings at the physical layer, it is still interesting to employ channel hopping at the MAC layer. Combining both PHY and MAC frequency diversity allows this TSCH/OFDM solution to very efficiently combat multi-path fading and external interference. Both OFDM PHY tested (OFDM option 1 MCS0 and OFDM option 1 MCS3) outperform IEEE802.15.4 - OPSK in this scenario. They yield a PDR value which is at least 10 point higher than IEEE802.15.4 - OPSK in the three

node locations.

Fourth, we introduce the concept of "Agile Networking", which generalizes a mote as having multiple radios (or radio configurations). The promise of Agile Networking is that a network designer need to make a hard decision on which radio to pick for her application. The 6TiSCH protocol stack can efficiently orchestrate the use of these radios, but Agile Networking brings a number of changes to the different layers in the protocol stack. And while we only start scratching the surface on the potential of Agile Networking, we detail the design on an Agile Network platform and testbed.

8.2 Future Work

Having low-power mesh networks featuring diverse PHY technologies opens a new area of study. In this section, we present what we consider are the next steps to achieving full "Agile Networking", i.e. heterogeneous low-power mesh networks.

In Chapter 4 we have seen how the different PHYs of IEEE802.15.4g have different capabilities in terms of goodput and range We have also shown how duty cycle regulations impact on the throughput of each PHY in the 863-870 MHz band. We consider important to extend this study to the 2.4 GHz band and to include the IEEE802.15.4 - OQPSK PHY.

Devices are appearing which feature multiple radio technologies and settings. One example is the OpenMote B. This study can be extended to other technologies outside the IEEE802.15.4 ecosystem. Logical candidates are LoRa and Sigfox, two LPWAN technologies. An important question to answer is what advantage technology agility brings. That is, *if a mote is capable of changing its radio (configuration) on the fly, will it do so for each frame, or is the system going to converge to one setting only?*

Sub-GHz bands impose heavy duty cycle restrictions. Nodes changing PHYs and frequency band need to be aware of their duty cycle regulation. Since resources are demanded by the directive of the Scheduling Functions, these need to keep an eye in the duty cycle regulations. New SFs need to be designed to take into account the characteristics of Agile Networking devices.

An challenge in that work is that different PHYs have different channelization characteristics. Channel hopping techniques make the assumption that it is only a PHY which is being used on the network. In different PHYs, different logical channels can select the same frequency and therefore interfere with one another. More extended mechanisms have to be designed to better orchestrate and maintain the determinism TSCH provides on single PHY networks.

A final issue we want to raise is backwards compatibility. Ideally, new devices with multiple PHY would be able to interact with nodes that are capable of only one PHY, IEEE802.15.4 - OPQSK. We consider this an im-

portant issue because if these technologies become one day a commercial product, the adoption of these devices should be seamless into already deployed networks.

Chapter 9

Publications

Journal Articles:

1. *Evaluation of IEEE802.15.4g for Environmental Observations.* Jonathan Muñoz, Tengfei Chang, Xavier Vilajosana, Thomas Watteyne. **MPDI Sensors, special issue on Environmental Observations.**

Conference Papers:

1. *OpenTestBed: Poor Man's IoT Testbed.* Jonathan Muñoz, Fabian Rincon, Tengfei Chang, Xavier Vilajosana, Brecht Vermeulen, Thijs Walcarius, Wim Van de Meerssche, Thomas Watteyne. **IEEE INFOCOM, CNERT workshop**, Paris, France, 29 April 2019 *(under review)*

2. *Why Channel Hopping Makes Sense, even with IEEE802.15.4 OFDM at 2.4 GHz.* Jonathan Muñoz, Paul Muhlethaler, Xavier Vilajosana, Thomas Watteyne. **Global IoT Summit (GIoTS)**, Bilbao, Spain, 4–7 June 2018. **Best Paper Finalist**.

3. *Overview of IEEE802.15.4g OFDM and its Applicability to Smart Building Applications.* Jonathan Muñoz, Emmanuel Riou, Xavier Vilajosana, Paul Muhlethaler, Thomas Watteyne. **IEEE Wireless Days (WD)**, 3–5 April 2018.

4. *OpenWSN & OpenMote: Demo'ing A Complete Ecosystem for the Industrial Internet of Things.* Tengfei Chang, Pere Tuset-Peiro, Jonathan Muñoz, Xavier Vilajosana, Thomas Watteyne. **IEEE International Conference on Sensing, Communication and Networking (SECON)**, poster and demo session, London, UK, 27-30 June 2016.

Standardization:

1. *Example Packets for 6TiSCH Configuration.* Jonathan Muñoz, Emmanuel Riou, Dominique Barthel. draft-munoz-6tisch-minimal-examples. IETF99, Prague, July 2017.

2. *Problem Statement for Generalizing 6TiSCH to Multiple PHYs.* Jonathan Muñoz. draft-munoz-6tisch-considerations-multiplePHYs. IETF102, Montreal, July 2018.

3. *Global Time Distribution in 6TiSCH Networks.* Xavier Vilajosana, Pere Tuset, Borja Martinez, Jonathan Muñoz. draft-vilajosana-6tisch-globaltime. IETF102, Montreal, July 2018.

Research Report:

1. *SmartMesh Range Measurements.* Marcelo Ferreira, Jonathan Muñoz, Thomas Watteyne. **Inria Research Report RR-9205.** 2018.

Open-source contributions:

1. OpenWSN project (`http://www.openwsn.org`). Generalization of the radio interface to multiple technologies.

2. Wireshark project (`https://www.wireshark.org/`). Enhancement of the Wireshark IEEE802.15.4 protocol dissector and 6LoWPAN protocol dissector.

References

[1] D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, and J. Henry, *IoT Fundamentals*. Cisco Press, 2017.

[2] M. G. Institute, https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-ofdigitizing-the-physical-world, accessed: February 2019.

[3] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[4] "Topology Options for Bluetooth," https://www.bluetooth.com/bluetooth-technology/topology-options, accessed: 2019-01-28.

[5] IEEE, "IEEE Standard for Information technology–Telecommunications and information exchange between systems - Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHz License Exempt Operation," *IEEE Std 802.11ah-2016 (Amendment to IEEE Std 802.11-2016, as amended by IEEE Std 802.11ai-2016)*, pp. 1–594, May 2017.

[6] "What is LoRaWAN," https://lora-alliance.org/sites/default/files/2018-04/what-is-lorawan.pdf, accessed: 2019-01-28.

[7] A. Berni and W. Gregg, "On the utility of chirp modulation for digital signaling," *IEEE Transactions on Communications*, vol. 21, no. 6, pp. 748–751, June 1973.

[8] "LoRa Modulation Basics," https://www.semtech.com/uploads/documents/an1200.22.pdf, accessed:2019-01-29.

[9] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 60–67, October 2016.

[10] "LoRaWAN specification V1.1," https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf, accessed: 2019-01-28.

[11] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the Limits of LoRaWAN," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 34–40, September 2017.

[12] "Sigfox Technology Overview," https://www.sigfox.com/en/sigfox-iot-technology-overview, accessed: 2019-01-29.

[13] "Buy Sigfox," https://buy.sigfox.com/buy/offers/FR, accessed: 2019-01-29.

[14] K. Zeman, P. Masek, J. Krejci, A. Ometov, J. Hosek, S. Andreev, and F. Kroepfl, "Wireless M-BUS in Industrial IoT: Technology Overview and Prototype Implementation," in *European Wireless 2017; 23th European Wireless Conference*, May 2017, pp. 1–6.

[15] V. Mohan, "An Introduction to Wireless M-Bus," http://pages.silabs.com/rs/634-SLU-379/images/introduction-to-wireless-mbus.pdf, accessed: 2019-01-30.

[16] *IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Std., 2003.

[17] K. Pister, P. Thubert, S. Dwars, and T. Phinney, *Industrial Routing Requirements in Low-Power and Lossy Networks*, IETF Std. RFC5673, October 2009.

[18] A. Brandt, J. Buron, and G. Porcu, *Home Automation Routing Requirements in Low-Power and Lossy Networks*, IETF Std. RFC5826, April 2010.

[19] M. Dohler, T. Watteyne, T. Winter, and D. Barthel, *Routing Requirements for Urban Low-Power and Lossy Networks*, IETF Std. RFC5548, May 2009.

[20] J. Martocci, P. De Mil, N. Riou, and W. Vermeylen, "Building Automation Routing Requirements in Low-Power and Lossy Networks," June 2010.

[21] "Zigbee Alliance," https://www.zigbee.org/, accessed: 2019-01-30.

[22] "Thread Group," https://www.threadgroup.org, accessed: 2019-01-30.

[23] D. Chen, M. Nixon, and A. Mok, *WirelessHART: Real-Time Mesh Network for Industrial Automation*, 1st ed. Springer, 2010.

[24] H. Khaleel, C. Pastrone, F. Penna, M. A. Spirito, and R. Garello, "Impact of Wi-Fi Traffic on the IEEE 802.15.4 Channels Occupation in Indoor Environments," in *Conference on Electromagnetics in Advanced Applications*, September 2009, pp. 1042–1045.

[25] T. Watteyne, C. Adjih, and X. Vilajosana, "Lessons Learned from Large-scale Dense IEEE802.15.4 Connectivity Traces," in *Conference on Automation Science and Engineering*, August 2015, pp. 145–150.

[26] C. Adjih, E. Baccelli, E. Fleury, G. Harter, N. Mitton, T. Noel, R. Pissard-Gibollet, F. Saint-Marcel, G. Schreiner, J. Vandaele, and T. Watteyne, "FIT IoT-LAB: A Large Scale Open Experimental IoT Testbed," in *World Forum on Internet of Things (WF-IoT)*, December 2015, pp. 459–464.

[27] W. Guo, W. Healy, and M. Zhou, "Impacts of 2.4-GHz ISM Band Interference on IEEE 802.15.4 Wireless Sensor Network Reliability in Buildings," *IEEE Transactions on Instrumentation and Measurement, vol. 61, no. 9, pp. 2533-2544*, 2012.

[28] T. Watteyne, S. Lanzisera, A. Mehta, and K. S. J. Pister, "Mitigating Multipath Fading through Channel Hopping in Wireless Sensor Networks," in *IEEE International Conference on Communications (ICC)*, May 2010, pp. 1–5.

[29] IEEE, *IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks. IIEEE Std 802.15.4g-2012 (Amendment to IEEE Std 802.15.4-2011)*, 2012.

[30] *IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer*, April 2012.

[31] K. S. Pister and L. Doherty, "TSMP: Time Synchronized Mesh Protocol," in *IASTED International Symposium on Distributed Sensor Networks (DSN)*, 2008.

[32] IEEE, *IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks Specific Requirements Part 15.4: Wireless Medium*

Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) IEEE Std 802.15.4-2015, 2015.

[33] T. Watteyne, J. Weiss, L. Doherty, and J. Simon, "Industrial IEEE802.15.4e Networks: Performance and Trade-offs," in *Conference on Communications (ICC)*. IEEE, June 2015, pp. 604–609.

[34] T. Watteyne, V. Handziski, X. Vilajosana, S. Duquennoy, O. Hahm, E. Baccelli, and A. Wolisz, "Industrial Wireless IP-Based Cyber - Physical Systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1025–1038, May 2016.

[35] *LTC5800-IPM: SmartMesh IP Node 2.4GHz 802.15.4e Wireless Mote-on-Chip*, https://www.analog.com/media/en/technical-documentation/data-sheets/5800ipmfa.pdf, Analog Devices, 2013, rev. A.

[36] X. Vilajosana, Q. Wang, F. Chraim, T. Watteyne, T. Chang, and K. Pister, "A realistic energy consumption model for tsch networks," *Sensors Journal, IEEE*, vol. 14, pp. 482–489, 02 2014.

[37] T. Watteyne, A. Mehta, and K. Pister, "Reliability Through Frequency Diversity: Why Channel Hopping Makes Sense," in *International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN)*. Tenerife, Canary Islands, Spain: ACM, October 2009.

[38] *802.15.4-2015 - IEEE Standard for Low-Rate Wireless Networks*, IEEE Std., April 2016.

[39] E. McCune, "This Emperor Has No Clothes?" *IEEE Microwave Magazine*, 2013.

[40] "Wi SUN Alliance," https://www.wi-sun.org/, accessed: 2019-04-02.

[41] C.-S. Sum, F. Kojima, and H. Harada, "Performance Analysis of a Multi-PHY Coexistence Mechanism for IEEE 802.15.4g FSK Network," *IEEE Wireless Communications and Networking Conference (WCNC): MAC*, 2013.

[42] K.-H. Chang and B. Mason, "The IEEE 802.15.4g Standard for Smart Metering Utility Networks," *IEEE SmartGridComm 2012 Symposium - Smart Grid Standards, Testbeds and Field Trials Symposium*, 2012.

[43] T. Watteyne, L. Doherty, J. Simon, and K. Pister, "Technical Overview of SmartMesh IP," in *International Workshop on Extending Seamlessly to the Internet of Things (esIoT)*, Taiwan, July 2013.

[44] J. Yoshida. (2014, May) Do Linear's Dust Networks Matter in IoT? EETimes.

[45] P. Thubert, *An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4*, https://datatracker.ietf.org/doc/draft-ietf-6tisch-architecture/, IETF, 2018.

[46] X. Vilajosana, K. Pister, and T. Watteyne, *TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration*, IETF, 05 2017.

[47] T. Watteyne, X. Vilajosana, B. Kerkez, F. Chraim, K. Weekly, Q. Wang, S. Glaser, and K. S. Pister, "OpenWSN: a standards-based low-power wireless development environment," *Transactions on Emerging Telecommunications Technologies (ETT)*, vol. 23, no. 5, pp. 480–493, 2012.

[48] S. Duquennoy, A. Elsts, B. A. Nahas, and G. Oikonomo, "TSCH and 6TiSCH for Contiki: Challenges, Design and Evaluation," in *Distributed Computing in Sensor Systems (DCOSS)*, June 2017, pp. 11–18.

[49] R. Teles Hermeto, A. Gallais, and F. Theoleyre, "Scheduling for IEEE802.15.4-TSCH and slow channel hopping MAC in low power industrial wireless networks: A survey," *Computer Communications*, vol. 114, pp. 84 – 105, 2017.

[50] S. Duquennoy, B. Al Nahas, O. Landsiedel, and T. Watteyne, "Orchestra: Robust Mesh Networks Through Autonomously Scheduled TSCH," in *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*. New York, NY, USA: ACM, 2015, pp. 337–350. [Online]. Available: http://doi.acm.org/10.1145/2809695.2809714

[51] T. Chang, M. Vicinic, X. Vilajosana, S. Duquennoy, and D. Dujovne, *6TiSCH Minimal Scheduling Function (MSF)*, IETF, 07 2018.

[52] T. Chang, T. Watteyne, Q. Wang, and X. Vilajosana, "LLSF: Low Latency Scheduling Function for 6TiSCH Networks," in *2016 International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, May 2016, pp. 93–95.

[53] Q. Wang, X. Vilajosana, and T. Watteyne, *RFC 8480 - 6TiSCH Operation Sublayer (6top) Protocol 6P*, https://datatracker.ietf.org/doc/rfc8480/, IETF, 11 2018.

[54] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over the IEEE802.15.4 Networks." IETF, 2007.

[55] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*. Wiley Publishing, 2010.

[56] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*, IETF Std. RFC6550, March 2012.

[57] P. Thubert, *Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)*, IETF, 03 2012.

[58] O. Iova, F. Theoleyre, T. Watteyne, and T. Noel, "The Love-Hate Relationship between IEEE 802.15.4 and RPL," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 188–194, January 2017.

[59] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," IETF, 2014.

[60] J. Thelen, D. Goense, and K. Langendoen, "Radio Wave Propagation in Potato Fields," in *First workshop on Wireless Network Measurements (co-located with WiOpt 2005)*, 04 2005.

[61] C. Hartung, R. Han, C. Seislstad, and S. Holbrook, "FireWxNet: A Multi-Tiered Portable Wireless System for Monitoring Weather Conditions in Wildland Fire Environments," in *Proceedings of the 4th International Conference on Mobile Systems, Applications and Services*, no. 14. ACM, 2006, pp. 28–41.

[62] M. Lazarescu, "Desing and field test of a WSN platform prototype for long-term enviromental monitoring." *Sensors*, no. 4, pp. 9481–9518, 2015.

[63] A. Cerpa, N. Busek, and D. Estrin, "SCALE: A tool for Simple Connectivity Assessment in Lossy Environments," UCLA Center for Embedded Network Sensing, Tech. Rep. 21, 5 September 2003.

[64] C. S. Sum, L. Lu, M. T. Zhou, F. Kojima, and H. Harada, "System Evaluation of a Practical IEEE 802.15.4/4e/4g Multi-Physical and Multi-Hop Smart Utility Network," *IET Communications*, vol. 9, no. 5, pp. 665–673, 2015.

[65] J. Dias, F. Ribeiro, M. Campos, R.and Ricardo, L. Martins, F. Gomes, and A. Carrapatoso, "Evaluation of an RPL/6LoWPAN/IEEE 802.15.4g Solution for Smart Metering in an Industrial Environment," in *Conference on Wireless On-demand Network Systems and Services (WONS)*, January 2016, pp. 1–4.

[66] K. Mochizuki, K. Obata, K. Mizutani, and H. Harada, "Development and Field Experiment of Wide Area Wi-SUN System Based on IEEE 802.15.4g," in *World Forum on Internet of Things (WF-IoT)*, December 2016, pp. 76–81.

[67] C.-S. Sum, M. A. Rahman, L. Lu, F. Kojima, and H. Harada, "On Communication and Interference Range of IEEE 802.15.4g Smart Utility Networks," *IEEE Wireless Communications and Networking Conference*, 2012.

[68] G. M. Bragg, K. Martinez, P. J. Basford, and J. K. Hart, "868MHz 6LoWPAN with ContikiMAC for an Internet of Things Environmental Sensor Network," *SAI Computing Conference*, pp. 1273–1277, Jul. 2016.

[69] F. Kojima and H. Harada, "Study on Multipath Characteristics for IEEE 802.15.4g SUN Applications in the Frequency Band Used in Japan," in *IEEE Conference on Communications Workshops*, May 2010, pp. 1–5.

[70] A.-S. Tonneau, N. Mitton, and J. Vandaele, "How to Choose an Experimentation Platform for Wireless Sensor Networks?" *Elsevier Adhoc Networks*, 2015.

[71] L. Sanchez, J. A. Galache, G. V., J. M. Hernandez, J. Bernat, A. Gluhak, and T. Garcia, "SmartSantander: The meeting point between Future Internet research and experimentation and the smart cities," in *2011 Future Network Mobile Summit*, June 2011, pp. 1–8.

[72] C. A. Boano, M. Schuß, and K. U. Römer, "EWSN Dependability Competition: Experiences and Lessons Learned," *IEEE Internet of Things eNewsletter*, Mar 2017.

[73] K. Brun-Laguna, P. Henrique Gomes, P. Minet, and T. Watteyne, "Moving Beyond Testbeds? Lessons (We) Learned about Connectivity," *IEEE Pervasive Computing, Special Issue on Beyond Testbeds: Real-World IoT Deployments*, 2018, to appear in 2019.

[74] "Atmel AT86RF215 DATASHEET," http://ww1.microchip.com/downloads/en/devicedoc/atmel-42415-wireless-at86rf215_datasheet.pdf, accessed: 2019-02-08.

[75] S. Malek, F. Avanzi, K. Brun-Laguna, T. Maurer, C. Oroza, P. Hartsough, T. Watteyne, and S. Glaser, "Real-Time Alpine Measurement System Using Wireless Sensor Networks," *Sensors*, 2017.

[76] ITU-R, "Recommendation ITU-R P.1238-9. Propagation Data and Prediction Methods for the Planning of Indoor Radiocommunication Systems and Radio Local Area Networks in the Frequency Range 300 MHz to 100 GHz," International Telecommunication Union, Tech. Rep., 06-2017.

[77] *Short Range Devices (SRD) operating in the frequency range 25 MHz to 1 000 MHz; Part 2: Harmonised Standard covering the essential requirements of article 3.2 of Directive 2014/53/EU for non specific radio equipment*, European Telecommunications Standards Institute, February 2017.

[78] CEPT-ECC, "Relating to the use of Short Range Devices (SRD)," CEPT-ECC, Tech. Rep. ERC Recommendation 70-03, 2017.

[79] FCC, *15.247 Operation within the bands 902–928 MHz, 2400–2483.5 MHz, and 5725–5850 MHz*, 13.

[80] *920MHz-Band Telemeter, Telecontrol and Data Transmission Radio Equipment. STD-T108*, Association of Radio Industries and Businesses (ARIB), 02 2012.

Appendices

Appendix A

ISM Frequency Bands and Regulations

Duty cycle, maximum bandwidth per communication channel, maximum dwell time and maximum transmission power are some of the parameters each region/country regulates. This section summarizes the regulations in Europe, the United States and Japan.

A.1 Europe

The European Telecommunication Standards Institute (ETSI) and the Electronic Communications Committee (part of the European Conference of Postal and Telecommunications Administrations, CEPT) define the set of recommendations and standards [77, 78] for Short Range Devices operating in the 25–1000 MHz frequency band.

Considering that the CEPT includes 48 European countries (national level) and ETSI has more than 800 members (regulatory bodies, governments, companies, universities, research bodies) from 66 countries and five continents, their normative and regulations are complex, as consensus within the parties have to be made. In addition, some countries may differ on the designated bands or impose certain conditions on uses of specific bands.

The normative for EU wide harmonized National Radio Interfaces cuts the 863–870 MHz band into sub-bands, as detailed in Table A.1. Table A.2 shows conformance to any National Radio Interface, in the case of using the entire 7 MHz band.

The duty cycle restriction of 0.1% in some of the sub-bands could be eased and taken up to 2.8% if polite spectrum access is applied to the transmitters. Polite spectrum access refers to Listen Before Talk (LBT) and Adaptability Frequency Agility (AFA). Prior to transmission, a "polite" device performs Clear Channel Assessment (CCA) to check its availability. If the channel is free, the device continues its transmission. If it is not, the device should

Table A.1: EU Harmonized NRI for the 863–870 MHz band. A device following these rules can be used across Europe. This band is divided into sub-bands, each with a specific regulation. Channel access and occupation rules refers to the duty cycle that devices must respect. Each sub-band also defines the maximum bandwidth a channel can have. The other usage restrictions column indicates the applications that can take place and the transmission techniques than can be used. DSSS is short for Direct Sequence Spread Spectrum, FHSS is short Frequency Hopping Spread Spectrum.

Frequency Band	Maximum effective radiated power (e.r.p.)	Channel access and occupation rules	Maximum occupied bandwidth	Other usage restrictions
863–865 MHz	25 mW e.r.p.	$\leq$ 0.1 % duty cycle or polite spectrum access	the entire band except audio/video apps. limited to 300 kHz	
865–868 MHz	25 mW e.r.p. +6.2 dBm/100 kHz	$\leq$ 1 % duty cycle or polite spectrum access	the entire band except audio/video apps. limited to 300 kHz	DHSS and any techniques other than FHSS
868.0–868.6 MHz	25 mW e.r.p.	$\leq$ 1 % duty cycle or polite spectrum access	the entire band except audio/video apps. limited to 300 kHz	
868.7–869.2 MHz	25 mW e.r.p.	$\leq$ 0.1 % duty cycle or polite spectrum access	the entire band except audio/video apps. limited to 300 kHz	
869.40–869.65 MHz	25 mW e.r.p.	$\leq$ 0.1 % duty cycle or polite spectrum access	the entire band	Analogue audio apps. other than voice excluded. Analogue video apps excluded.
869.40–869.65 MHz	500 mW e.r.p.	$\leq$ 0.1 % duty cycle or polite spectrum access	the entire band	Analogue video apps. are excluded.
869.7–870 MHz	5 mW e.r.p.	No requirement	the entire band	Audio and video apps. are excluded.
869.7–870 MHz	25 mW e.r.p.	$\leq$ 1 % duty cycle or polite spectrum access	the entire band	Analogue audio apps. are excluded. Analogue video apps. are excluded.

Table A.2: Non EU wide harmonized National Radio Interfaces. Some European countries accept the use of the 863–870 MHz band with these characteristics. Channel access and occupation rules refers to the duty cycle that devices must respect. The other usage restrictions column indicates the applications that can take place and the transmission techniques than can be used.

Frequency Band	Maximum effective radiated power (e.r.p)	Channel access and occupation rules	Maximum occupied bandwidth	Other usage restrictions
863–870 MHz	25 mW e.r.p	$\leq$ 0.1 % duty cycle or polite spectrum access	the entire band except audio/video limited to 300 kHz and voice to 25 kHz	sub-bands 868.6–868.7 MHz, 869.25–869.4 MHz and 869.65–869.7 MHz can only be used for alarm systems

not retry its transmission until a random time has passed. Optionally, the device can change the intended transmitting frequency and listens again before starts the transmission.

The timing parameters of polite spectrum access are:

- Minimum CCA time: 160 μs
- Maximum single TX duration: 1 s
- Maximum cumulative TX time in one hour: 100 s (duty cycle of 2.8 %) per 200 kHz spectrum

A.2 United States

The Federal Communications Commission is the body in charge of the regulation of the radio electric space in the US [79]. For the 902–928 MHz ISM band, its use is limited to frequency hopping and digitally modulated radiators. US duty cycle regulation is more permissive, as well as the maximum TX power, than the European regulation. In the case of frequency hopping systems, devices have to be compliant with:

- Channel hopping carrier frequencies should be separated by the greater between 25 kHz or the 20 dB bandwidth channel.
- If the 20 dB bandwidth of the hopping channel is $<$ 250 kHz, at least 50 hopping frequencies should be used and each up to 0.4 s per 20 s period.
- If the 20 dB bandwidth of the hopping channel is $\geq$ 250 kHz up to 500 kHz, at least 25 hopping frequencies should be used and each up to 0.4 s per 10 s period.

For the case of systems using digital modulation techniques, the minimum 6 dB bandwidth should be at least 500 kHz. The maximum peak output power is:

- If using channel hopping: 30 dBm if at least 50 hopping channels are used, 21 dBm if less than 50 hopping channels are used (minimum 25 hopping channels).
- If using digital modulation: 30 dBm. A duty cycle of 0.4 s each 20 s gives us a channel occupancy of 2 % and in the best case, 0.4 s each 10 s, 4 %.

A.3 Japan

The Association of Radio Industries and Businesses defines the use of the 922.4–928 MHz band [80], using carrier sense under these premises:

- Minimum listening time during CCA of 128 μs; maximum: 5 ms.
- Maximum single TX time: 400 ms.
- Duty cycle $\leq$ 10 %.
- If the previous TX time is $>$ 200 ms, the device shall wait for at least 10 times the TX time before the next TX.
- If the previous TX time is $\leq$ 200 ms and more than 6 ms, it shall wait for 2 ms before consecutive TX.
- Using two radio channels at the same time (i.e. signal is 400 kHz wide), the maximum single TX time has to be less than 200 ms.
- Using up to 5 radio channels at the same time, maximum single TX time has to be less than 100 ms.
- Maximum TX power is 20 mW.

If no carrier sense is used:

- Maximum TX power is 1 mW.
- Maximum single TX time: 100 ms.
- Duty cycle $\leq$ 0.1 %.

Appendix B

OpenTestBed

This sections details the OpenTestBed. We start by reviewing the requirements for the OpenTestBed, and the approach we have taken, for example to ensure the testbed is accepted by the occupants of the building in which it is deployed (Section B.1). From that, we detail the hardware (Section B.2) and software (Section B.3) used.

B.1 Requirements and Approach

As detailed in Section 2.5, a testbed such as FIT IoT-lab offers countless features. In our experience of implementing protocol stacks for low-power wireless IoT network, some of these features are not strictly necessary. Our approach when developing this type of firmware has been to first develop it on a handful of boards on our desk. Having the hardware in front of us allows the use of in-circuit debuggers, logic analyzer and oscilloscopes, do the bulk of the development while verifying all works as expect on a network of 2-5 boards. The result of this work is a firmware image, which we now want to test at scale. Only then we do need a testbed, and the only thing we need from that testbed is to be able to load the firmware on all the devices, let an experiment run, and verify the performance of the network. Because each firmware is different and each developer wants to log different information, the most generic approach is to send and receive serial bytes to each of the nodes in the testbed.

This translates into the following (minimalistic) set of user stories for a firmware developer using the testbed:

- As a developer, I want the testbed to be composed of devices which are well-known, commercially available and state-of-the-art.
- As a developer, I want the testbed to be deployed in an environment which is representative of the environment of my final deployment.

- As a developer, I want to be able to load arbitrary binary images on any device at any time during an experiment.
- As a developer, I want to be able to reset/disable any device at any time during an experiment.
- As a developer, I want to be able to send and receive serial bytes with any device at any time during an experiment.

The operator is the person who builds and maintains the testbed. Since the testbed needs to be deployed in a building, the operator wants a solution that it easy to install, and which is accepted by the occupants of the building. Furthermore, she doesn't want to have to maintain a complex back-end system.

B.2 Hardware

We chose the OpenMote B (Section 7.3.1) as the low-power wireless device for the OpenTestBed.

The OpenTestBed consists of a number of "OtBoxes", shown in Fig. B.1. Each OtBox contains:

- A **Raspberry Pi**. This single-board computer runs the OpenTestBed software connects to the back-end over WiFi. We use a 5 GHz WiFi (available on the Raspberry Pi 3B+) in order not to interfere with the OpenMote B board communicating at 2.4 GHz.
- 4 **OpenMote B** motes.
- A **screen**.
- A **QR code** pointing to an explanation of the OpenTestBed.

The overall aesthetics of the OtBox ("barbershop" looking glass dome and laser engraves dark wood) are designed increase acceptability of the devices.

Table B.1 details the cost of an OtBox.

B.3 Software

Each OtBox runs the `otbox.py` single-file Python program[1]. This program connects to each OpenMote B over its serial port, and offers the following services to a user, over a simple API:

[1] As an online addition to this chapter, the OtBox software is available under a BSD open-source license at `https://github.com/openwsn-berkeley/opentestbed/`.

Figure B.1: At OtBox: a Raspberry Pi, 4 OpenMote B boards, a screen and a QR code in a glass dome.

Component	Cost
4× OpenMote B	90 €
1× Raspberry Pi 3B +	50 €
1× IKEA glass dome	15 €
1× LED screen	30 €
1× USB extensions	14 €
1× engraved wood	5 €
Total	**474 €**

Table B.1: Cost breakdown of an OtBox.

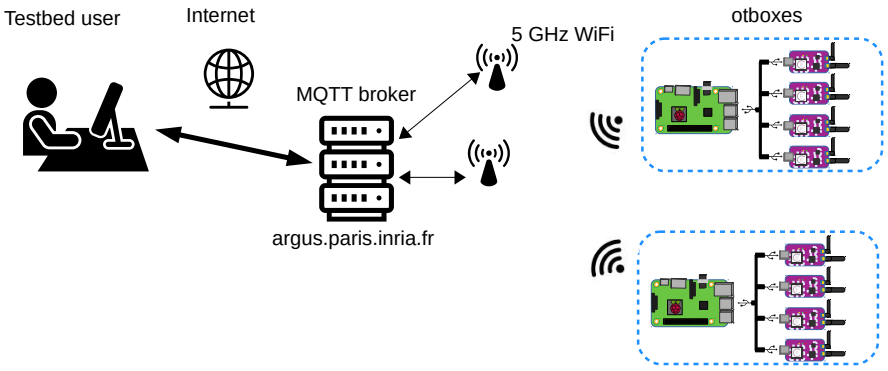


Figure B.2: OpenTestBed Infrastructure.

- Mote management: reprogramming any mote with any firmware, reset any mote, disable any mote.
- OtBox management: retrieve the status of the OtBox, discover the MAC address of the motes connected, upgrade the software, disply an image on the screen.
- Serial port forwarding: publish the bytes sent by any mote, send bytes to a motes.

This API is transported over MQTT. That is, each OtBox connects to a central MQTT broker, a popular publish-subscribe solution. To run an experiment, a user connects to the same broker and thereby can receive any notification sent by any OtBox, and issue commands. As such there is *no* "testbed server". Fig. B.2 shows the overall architecture.

Purely for ease of use, we developed the OpenTestBed dashboard. This dashboard connects to the MQTT broker and allows a user to interact with the API by clicking on a web interface. The dashboard is *not* a "testbed server", and is not required for the OpenTestBed to run. The dashboard is developed as a Node-RED flow (which is part of the available source code).

The dashboard participates in the acceptability of the tesbed. Every 10 s, the dashboard will issue a command to send an image onto the screens of all OtBoxes. The result is the screens displaying different pictures in a round robin fashion.

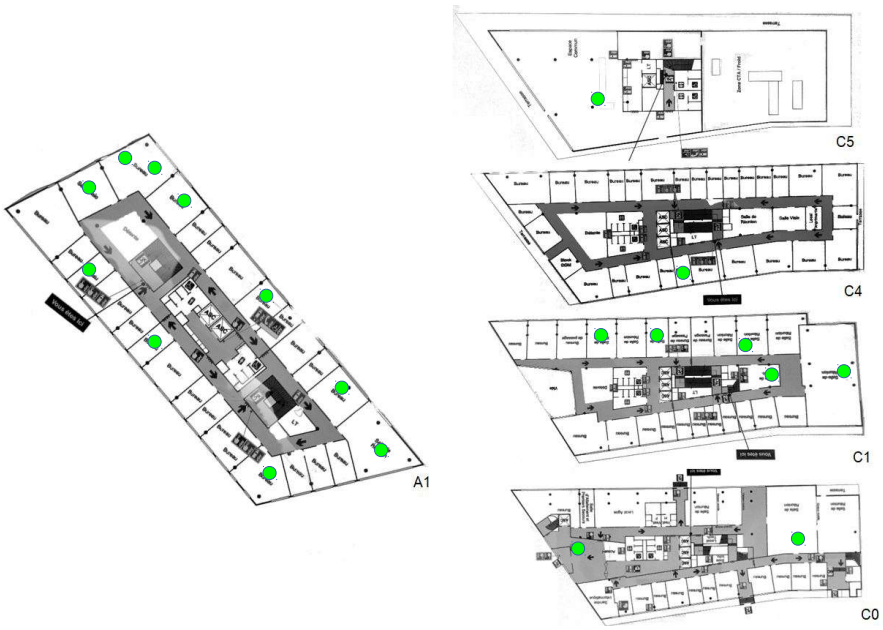


Figure B.3: The OtBoxes deployment across the Inria buildings A and C throughout different floors. Each green dot is an OtBox.

B.4 Examples Use Cases

B.4.1 Inria-Paris testbed

Fig. 7.2 is a picture of the Inria-Paris OpenTestBed right before deployment. It consist of 80 motes deployed in 20 OtBoxes. Fig. B.3 shows the locations of the OtBoxes once deployed across two multi-story buildings. The OtBoxes are located throughout offices, meeting rooms and the main lobby. Since each OtBox just needs an electrical outlet, it can be installated anywhere. The full installation of the OpenTestBed takes less than an hour.

The total hardware cost of the Inria-Paris OpenTestBed is 9,480 €, an order of magnitude lower than some institutional testbeds of the same size. The OpenTestBed was developed and deployed by an engineering intern in 1 month.

To ensure acceptability of the testbed, the communications department of the institute manages the images that appear on the OtBoxes, turning the OtBoxes into information radiators (annoucements, events, etc.). The dashboard[2] runs as a service on IBM Cloud. The OtBoxes connect to a vanilla Mosquito MQTT broker running in the Inria datacenter.

The OpenTestBed has been very well received by the Inria community. People like its design, and the OpenTestBed often serves as a ice-breaker

[2] For the Inria-Paris OpenTestBed, the dashboard runs at `http://testbed.openwsn.org/`.

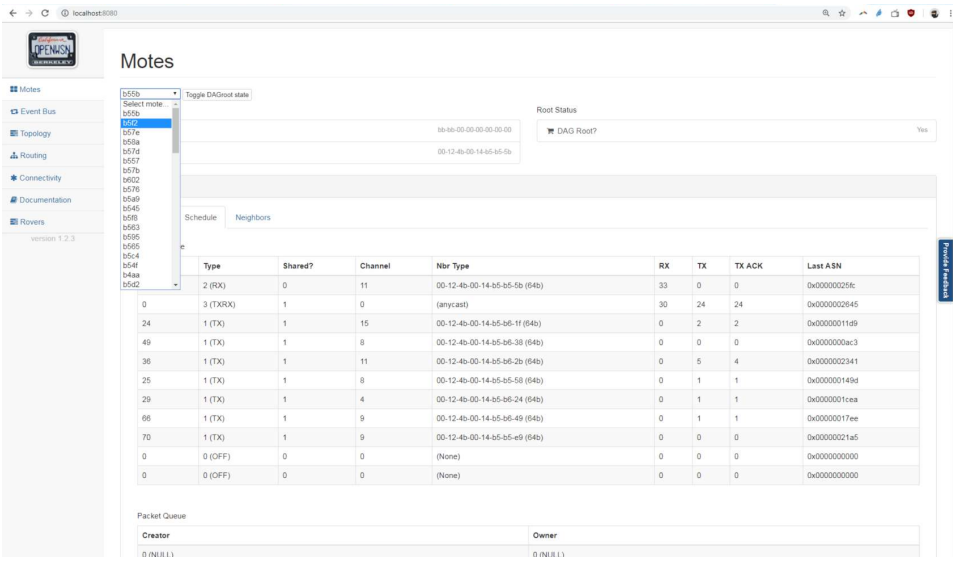


Figure B.4: The OpenVisualizer, the debugging/visualization tool of OpenWSN. The drop-down menu lists the motes in the Inria-Paris OpenTestBed.

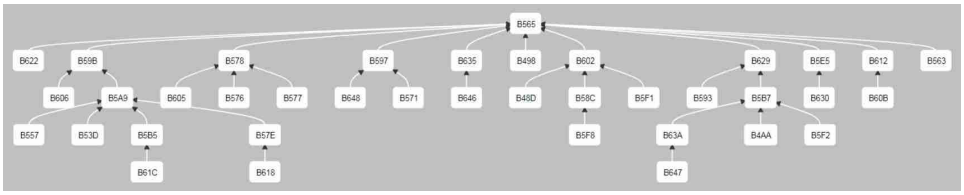


Figure B.5: Routing topology formed by an OpenWSN network running on the Inria-Paris OpenTestBed.

during meetings as many meeting rooms feature an OtBox.

B.4.2 Integration of the OpenTestBed into OpenWSN

OpenWSN [47][3] is the reference implementation of 6TiSCH, a protocol stack for the Industrial IoT standardized by the IETF. The OpenVisualizer is a tool to monitor and debug OpenWSN deployments. It shows the internal state (message queue, neighbour tables, scheduling table) of any node in the OpenWSN network on a web interface. It does so by parsing debug information each note periodically publishes on its serial port.

We added support for OpenTestBed into OpenWSN; this consists of two elements. First, we added `bootload=opentestbed` into OpenWSN's build environment. This allows a developer to automatically load the OpenWSN binary onto an OpenTestBed testbed as the last step of the build process. Second, we added the `-opentestbed` flag to the OpenVisualizer. This allows

[3] `https://github.com/openwsn-berkeley/`

Figure B.6: Hardware employed in the testbed and the scenario where it is deployed.

a developer to have the OpenVisualizer connect to all motes in an OpenTestBed instance, and visualize the state of all the nodes. Fig. B.4 shows the resulting OpenVisualizer web interface. Fig. B.5 shows the routing topology formed by those nodes.

B.4.3 w-iLab.t Testbed

The imec iLab.t testbed w-iLab.t is a diverse wireless testbed in Ghent, Belgium. It offers technologies such as 802.11a/b/g/n/ac, 802.15.1 (Bluetooth), 802.15.4, LTE and devices such as linux PCs, embedded IoT devices, software defined radios, mobile robots, environment emulators, and shielded boxes. Fig. B.6 shows the environment of this testbed, and the different hardware used.

Zolertia re-motes (1 to 2 per node) are connected via USB to Linux boxes that can be reserved by experimenters. By default, the Linux box gets a fresh operating system automatically augmented with the ssh-keys of the team that has reserved the node. This testbed is compatible and federated with the Fed4FIRE and GENI API standards. The jFed tool is used to provision the Linux nodes.

The default Linux OS image loaded on the box has the necessary tools to configure the Zolertia re-motes, but there is no automation foreseen from the testbed side to flash all Zolertia re-motes at once. So each experimenter has his own toolset for doing this. By leveraging the OpenTestBed framework, the imec now offers this functionality to the testbed users.

jFed has the functionality to do advanced automated software deployment at the initial provisioning stage with the Experiment Specification functionality. The imec team used this to create an ESpec that deploys the OpenTestBed framework automatically. In the process, the tools to in-

tegrate natively with the w-iLab.t testbed were added to the OpenTestBed (including supporting different numbers of Zolertia devices per box, and automatic registration of unique addresses).

The simplicity of using the OpenTestBed framework with a simple command line interface is beneficial to our testbed users who are looking for a simple way to quickly manage an experiment with multiple motes.

B.5 Summary

This chapter presents the OpenTestBed platform: a simple, cheap, versatile, scalable, easily deployable and replicable open-source testbed. Because of its simplicity, the OpenTestBed can easily be extended to support other low-power wireless devices. An 80-mote 20-OtBox OpenTestBed is deployed in an open-access fashion at Inria-Paris. The w-iLab.t testbed run by imec in Belgium now automatically starts an OpenTestBed instane for each low-power wireless experiment run. We hope the community can benefit from this platform and architecture, and that it can contribute to accelerating the development and evaluation of real-world IoT solutions.