



NTNU – Trondheim
→ Norwegian University of
Science and Technology

Understanding Data Analysis in an End-to-End IoT System

Sindre Schei

Submission date: May 2016
Responsible professor: Frank Alexander Kraemer, ITEM
Supervisor: David Palma, ITEM

Norwegian University of Science and Technology
Department of Telematics

Abstract

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

This is the second paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

And after the second paragraph follows the third paragraph. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

After this fourth paragraph, we start a new paragraph sequence. Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of

the original language. There is no need for special content, but the length of words should match the language.

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Sammendrag

Sikkerheten til nesten all offentlig nøkkel-kryptografi er basert på et vanskelig beregnbarhetsproblem. Mest velkjent er problemene med å faktorisere heltall i sine primtallsfaktorer, og å beregne diskrete logaritmer i endelige sykliske grupper. I de to siste tiårene, har det imidlertid dukket opp en rekke andre offentlig nøkkel-systemer, som baserer sin sikkerhet på helt andre type problemer. Et lovende forslag, er å basere sikkerheten på vanskeligheten av å løse store likningssett av flervariabe polynomlikninger. En stor utfordring ved å designe slike offentlig nøkkel-systemer, er å integrere en effektiv “falluke” (trapdoor) inn i likningssettet. En ny tilnærming til dette problemet ble nylig foreslått av Gligoroski m.f., hvor de benytter konseptet om kvasigruppe-strengtransformasjoner (quasigroup string transformations). I denne masteroppgaven beskriver vi en metodikk for å identifisere sterke og svake nøkler i det nylig foreslalte multivariable offentlig nøkkel-signatursystemet MQQ-SIG, som er basert på denne idéen.

Vi har gjennomført et stort antall eksperimenter, basert på Gröbner basis angrep, for å klassifisere de ulike parametrene som bestemmer nøklen i MQQ-SIG. Våre funn viser at det er store forskjeller i viktigheten av disse parametrene. Metodikken består i en klassifisering av de forskjellige parametrene i systemet, i tillegg til en innføring av konkrete kriterier for hvilke nøkler som bør velges. Videre, har vi identifisert et unødvendig krav i den originale spesifikasjonen, som krevde at kvasigruppene måtte oppfylle et bestemt kriterie. Ved å fjerne denne betingelsen, kan nøkkelerings-algoritmen potensielt øke ytelsen med en stor faktor. Basert på alt dette, foreslår vi en ny og forbedret nøkkel-genereringsalgoritme for MQQ-SIG, som vil generere sterkere nøkler og være mer effektiv enn den originale nøkkel-genereringsalgoritmen.

Preface

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Contents

List of Figures	xi
List of Tables	xiii
List of Acronyms	xv
Glossary	xvii
1 Introduction	1
1.1 Motivation	1
1.2 Methodology	1
1.3 Scope and Objectives	1
1.3.1 Scope	1
1.3.2 Objectives	1
1.4 Structure	1
2 Background	3
2.1 Bluetooth Low Energy	3
2.2 6LoWPAN	5
2.3 Raspberry Pi	5
2.4 nRF52	6
2.5 Adafruit ADXL345 Accelerometer	9
2.6 Transport protocols	10
2.6.1 Constrained Application Protocol (CoAP)	10
2.6.2 Message Queueing Telemetry Transport (MQTT)	13
2.6.3 Router Advertisement Daemon (radvd)	14
2.7 Software tools	14
2.7.1 Other	14
2.7.2 Abbreviations used in the rest of this thesis	14
3 System Architecture	15
3.1 Connecting Raspberry Pi and nRF52	16
3.1.1 Connection challenges	18

3.2	Nordic Semiconductor example code	18
3.2.1	CoAP	18
3.2.2	Observable CoAP	21
3.3	Raspberry Pi to Network Computer or Server	21
4	Network Measurements	23
4.1	Initial limitations in the Network	23
4.1.1	Stable transfer rate	23
4.1.2	Packet fragmentation	25
4.2	Description of measurements	27
4.3	CoAP	27
4.3.1	Discussion	29
4.3.2	CoAP NON comparison	31
4.3.3	CoAP, testing with more data	33
4.3.4	Discussion	36
4.4	Comparison	36
4.4.1	Goodput per time interval	37
4.5	BLE	37
4.6	Time spent in network	37
5	Data Anaysis discussion	41
5.1	Data analysis in microcontrollers	41
5.2	Computational Power	41
5.2.1	Power consumption	41
5.3	Ease of use	41
5.3.1	Raspberry Pi	41
5.3.2	nRF52	41
References	43	
Appendices		
A Appendix A	45	
B Appendix B	47	

List of Figures

2.1	BLE protocol stack	4
2.2	BLE Data Unit Structure	4
2.3	Raspberry Pi 3	6
2.4	Nordic Semiconductor nRF52	7
2.5	Nordic Semiconductor nRF52 chip in detail	9
2.6	ADXL345 Accelerometer	10
2.7	Sequence diagram CoAP	12
2.8	CON CoAP client server sequence diagram	12
2.9	NON CoAP client server sequence diagram	13
2.10	CoAP message format	13
2.11	CoAP usage of message types	14
3.1	System architecture	15
3.2	CoAP Client-Server communication example	19
3.3	CoAP Client-Server example Wireshark capture	20
3.4	Sequence diagram CoAP Client-Server example	20
3.5	CoAP Observable Server example	21
4.1	Comparison: ping nRF52 and ping google.com	24
4.2	Ping nRF52, different time	25
4.3	Packet fragmentation - train comparison	26
4.4	CoAP CON, 0-200 bytes sent	30
4.5	CON vs NON 0-200 bytes	32
4.6	CoAP CON plot, 200 bytes to 1 kB	34
4.7	NON 0-1000 bytes	35
4.8	NON 200-1000 bytes	36
4.9	CON vs NON 0-1000 bytes	36
4.10	CON vs NON 200-1000 bytes	37

List of Tables

4.1	Wireshark CoAP CON 0 bytes	28
4.2	Wireshark CoAP CON 100 bytes	29
4.3	Wireshark CoAP NON 0 bytes	31
4.4	Wireshark CoAP NON 100 bytes	32
4.5	Wireshark CoAP CON 700 bytes	38
4.6	Wireshark CoAP NON 700 bytes	39

List of Acronyms

6LoWPAN IPv6 over Low Power Wireless Personal Area Networks.

ACK Acknowledgement.

ACL Asynchronous Connection-Less.

BLE Bluetooth Low Energy.

CoAP Constrained Application Protocol.

CON Confirmable CoAP message.

CPU Central Processing Unit.

DNS Domain Name System.

GUI Graphical User Interface.

HCI Host Controller Interface.

HTTP Hyper Text Transport Protocol.

I2C Inter-Integrated Circuit.

ICMP Internet Control Message Protocol.

ICMPv6 Internet Control Message Protocol version 6.

IDE Integrated Development Environment.

IoT Internet of Things.

IPv4 Internet Protocol version 4.

IPv6 Internet Protocol version 6.

ISM Industrial Scientific Medical.

L2CAP Logical link control and adaption protocol.

LAN Local Area Network.

M2M Machine-to-machine.

MQTT Message Queueing Telemetry Transport.

MTU Maximum transmission unit.

NDP Neighbor Discovery Protocol.

NON Non-Confirmable CoAP message.

NTNU Norwegian University of Science and Technology.

OS Operating System.

PAN Personal Area Network.

radvd Router Advertisement Daemon.

RAM Random Access Memory.

RTT Round Trip Time.

SPI Serial Peripheral Interface.

TCP Transmission Control Protocol.

TDMA Time Division Multiple Access.

TFTP Trivial File Transfer Protocol.

UDP User Datagram Protocol.

USB Universal Serial Bus.

Glossary

A_B^Q	Q dummy symbol.
Byte	Used as a synonym for <i>octet</i> , meaning 8 bits put together.
directrix	Is a mark up language specially suited for scientific documents.
Message code	Is a mark up language specially suited for scientific documents.
Message type	Is a mark up language specially suited for scientific documents.
nRF52	Nordic Semiconductor nRF52 DK , Development Kit for the nRF52 microcontroller used as end nodes in this system. From now on noted as nRF52.
parabola	Is a mark up language specially suited for scientific documents.

Chapter 1

Introduction

1.1 Motivation

This is a test in the introduction chapter.

1.2 Methodology

1.3 Scope and Objectives

1.3.1 Scope

1.3.2 Objectives

O.1: Build a star network of microcontrollers

O.2: Connect sensors to the end-nodes to collect data

O.3: Gather information of the data sent through the network

O.4: Analyse and discuss the gathered information

1.4 Structure

Chapter 2

Background

This thesis describes the setup and usage of an End-to-End Internet of Things (IoT) system. In order for this to be set up by others later to perform reproducible tests, a detailed description of components, sensors and protocols used is needed. This chapter will go through the background information of the devices, technologies and protocols used, and why these were chosen over other alternatives.

2.1 Bluetooth Low Energy

Bluetooth Low Energy (BLE), also known as *Bluetooth Smart*, is a wireless technology for short range communication developed by the Bluetooth Special Interest Group. The idea was to create a low energy single-hop network solution for Personal Area Networks (PANs). A major advantage of this solution is that Bluetooth 4.0 already is a well established technology in cell phones, laptops and several other devices. This means that few changes need to be made to these devices to be able to work with bluetooth smart. Still to this date, a device that only implements BLE is not able to communicate with a device that only implements classic Bluetooth [3]. The 6LoWPAN Working Group has recognized the importance of BLE in IoT [4].

The protocol stack of BLE has two main parts, the controller and the host, as shown in 2.1. In the system presented in this thesis this represents the Raspberry Pi as the controller (master) and Nordic nRF52 as the host (slave). The communication between these is done through the standard Host Controller Interface (HCI). All slaves are in sleep mode by default, and are woken up by the master when communication is needed. Links are being identified by a randomly generated 32-bit code, and the Industrial Scientific Medical (ISM) band used is 2,4 GHz [3]. Other protocols used include Logical link control and adaption protocol (L2CAP) used to multiplex data between higher protocol layers, and the segmentation and reassembly of packets. From here packets are being passed to the HCI, which is the interface used to communicate between the two BLE devices. This is being used in conjunction with

Denne linken
snakker om
6lowpan, fly-
tte til etter
jeg har pre-
senteret 6LoW-
PAN?

4 2. BACKGROUND

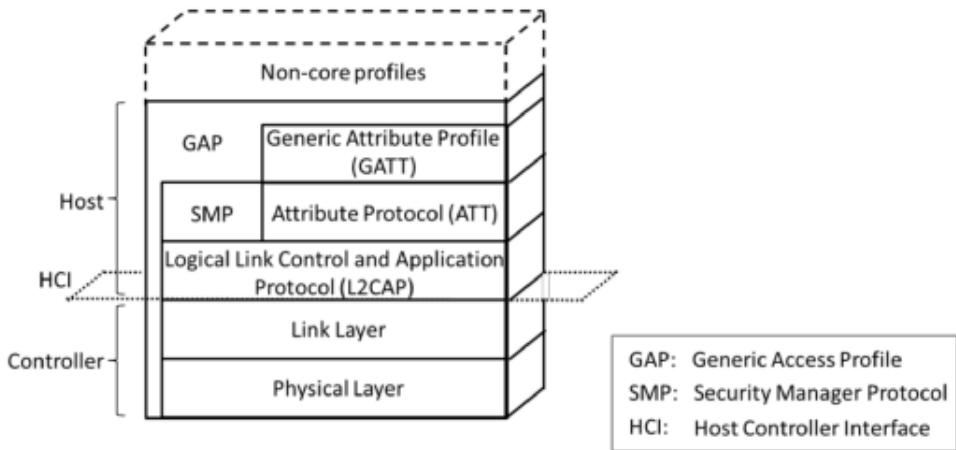


Figure 2.1: BLE protocol stack

Asynchronous Connection-Less (ACL), which is used to create the Time Division Multiple Access (TDMA) scheme used to transfer packets over the network link, as well as controlling uptime of the end nodes, as this link is set to disconnect automatically after a given time period if there is no activity on the link.

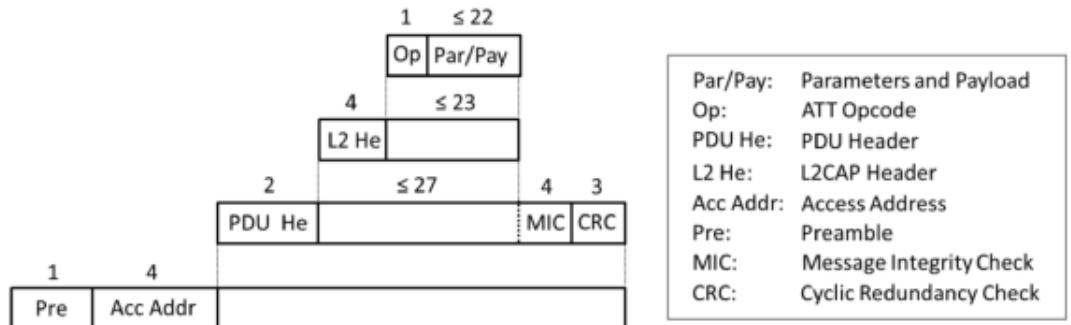


Figure 2.2: BLE Data Unit Structure

Figure 2.2 shows the data unit structure in BLE, meaning the different fields that can be used in a packet. The header fields of 4 Byte of access addresses and L2CAP will be central topics of discussion later in this thesis. The figure shows that the maximal packet size in a network like this is 31 bytes per packet. In the case of

the network presented here, when the BLE slave has been connected to a master, it stops searching for other masters, and it is not possible to connect to several masters. This means that we are only able to create a *star network*, not a *mesh network*. This could possibly be an idea for improvement later. Other than this, BLE seems like a very good alternative in this project.

2.2 6LoWPAN

IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) is a defined protocol for using Internet Protocol version 6 (IPv6) in low energy networks, to identify sensors and devices, as defined in the IEEE 802.15.4.

To use the Internet Protocol in low energy networks in addition to standard networks was proposed by Geoff Mulligan and the 6LoWPAN Working Group. In [7], the advantage of 6LoWPAN is explained as

Utilizing IP in these networks and pushing it to the very edge of the network devices flattens the naming and addressing hierarchy and thereby simplifies the connectivity model. This obviates the need for complex gateways that, in the past, were necessary to translate between proprietary protocols and standard Internet Protocols and instead can be replaced with much simpler bridges and routers, both of which are well understood, well developed and widely available technologies [7].

6LoWPAN was developed to be used in small sensor networks, and implementations can fit into 32Kb flash memory parts. The Maximum transmission unit (MTU) is given to be 1280 byte, and it also uses an impressive header comparison mechanism that allows the transmission of IPv6 packets in 4 bytes, much less than the standard IPv6 40 bytes. This is done by using stacked headers, same as in the IPv6 model, rather than defining a specific header as for Internet Protocol version 4 (IPv4). The device can send only the required part of the stack header, and does not need to include header fields for networking and fragmentation [4]. The maximum packet size of the physical layer is set to be 127 bytes, far below the limit of 1280 byte [6]. It is expected that other layers will produce packets of the desired size to fit the system. In the system presented in this thesis by the example code on the nRF52 is the side set to 270 bytes for every packet, as will be shown later in the thesis.

2.3 Raspberry Pi

Developed by Newark Element 14 [1], the Raspberry Pi has become a central tool for many people wanting to get started using small computers. The device has been known as a single-board computer the size of a credit card specially designed for small network projects and to be used as an educational tool used all the way

6 2. BACKGROUND

from elementary schools to here at Norwegian University of Science and Technology (NTNU). This was therefore a natural device to use as a starting point in this system as well.

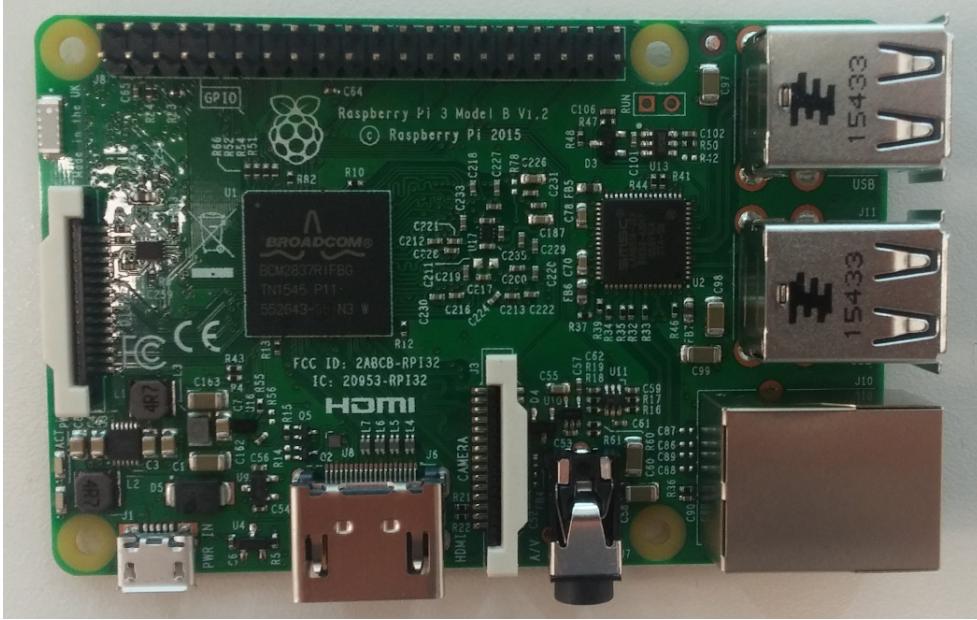


Figure 2.3: Raspberry Pi 3

The Raspberry Pi model 3 was released in February 2016, just in time to become a part of the system set up in this project. This includes a Central Processing Unit (CPU) speed of 1,2 GHz and 1 GB of Random Access Memory (RAM). This makes it approximately 12 times faster than the first Raspberry Pi. Both Bluetooth and WiFi is included, and it was quite easy to set up, given that the right Unix kernel has been used in the Operating System (OS) of the Pi. Along with the Raspberry Pi, we needed a good and stable operating system with a kernel that supported the 6LoWPAN architecture. For this, Ubuntu Mate version 15.10 with kernel version 4.15 was chosen, and used on the Raspberry Pi. As other versions of Ubuntu this is Unix based, and has a complete Graphical User Interface (GUI) of a full OS. The set up of this will be explained in chapter 3.1.

2.4 nRF52

The most central device of this network is the microcontroller used as end-nodes, the nRF52 developed by Nordic Semiconductor with the IoT development kit. This is

presented as a family of highly flexible, multi-protocol system on chip devices.

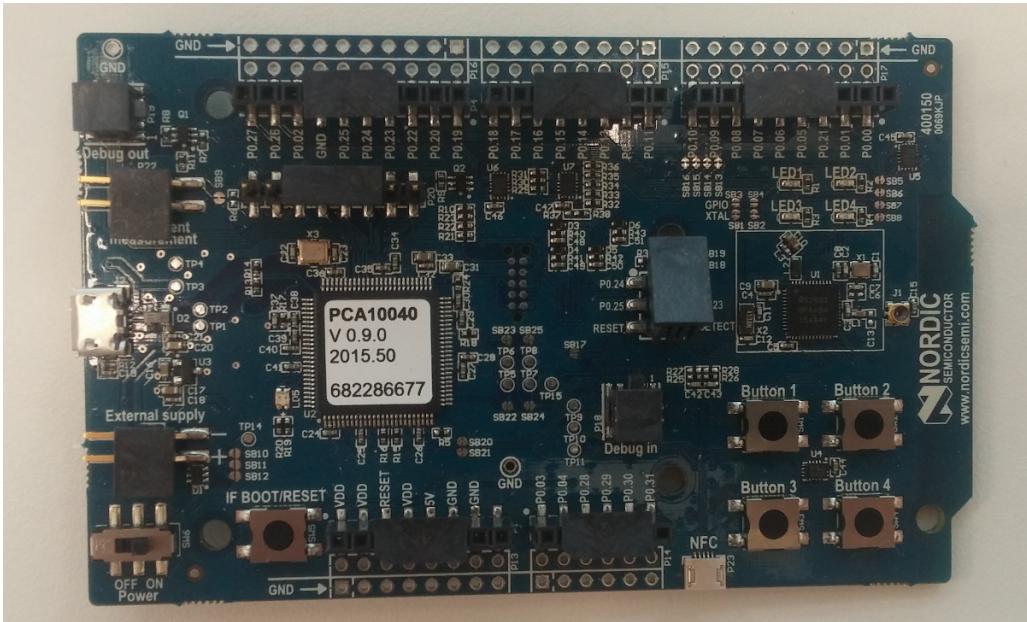


Figure 2.4: Nordic Semiconductor nRF52

[2]

This device has been advertised as a powerful multiprotocol single chip solution, with both a 32-bit ARM processor, a 512kB flash and 64kB og flash memory. The building blocks of the chip in its entirety is shown in 2.5. The key features mentioned by Nordic themselves are:

- Multi-protocol 2.4GHz radio
 - 32-bit ARM Cortex M4F processor
 - 512kB flash + 64kB RAM
 - Software stacks available as downloads
 - Application development independent from protocol stack
 - On-air compatible with nRF51, nRF24AP and nRF24L Series
 - Programmable output power from +4dBm to -20dBm

8 2. BACKGROUND

- RSSI
- RAM mapped FIFOs using EasyDMA
- Dynamic on air payload length up to 256 Bytes
- Flexible and configurable 32 pin GPIO
- Programmable Peripheral Interface – PPI
- Simple ON/OFF global power modes
- Full set of digital interfaces including: SPI/2-wire/UART/PDM/
- I2S, all with EasyDMA
- 12-bit/200KSPS ADC
- 128-bit AES ECB/CCM/AAR co-processor
- Quadrature demodulator
- Low cost external crystal 32MHz \pm 40ppm for Bluetooth, \pm 50ppm for ANT
- Low power 32MHz crystal and RC oscillators
- Ultra low-power 32kHz crystal and RC oscillators
- Wide supply voltage range (1.7 V to 3.6 V)
- On-chip DC/DC buck converter
- Individual power management for all peripherals
- Package options: 48-pin 6x6 QFN/WL-CSP

In other words much more different options than will be used in this system. The important part here is the processing power, the PPI, the Inter-Integrated Circuit (I2C) bus and the bluetooth antenna. That these things combined can run on only a 3V CR2032 battery is unbelievable.

Figure 2.5 shows how the different parts are placed on the chip.

In order to run compiled code on the nRF52, a preprogrammed *Soft device* has to be loaded onto the chip. There are several versions that can be downloaded from <http://www.nordicsemi.com>.

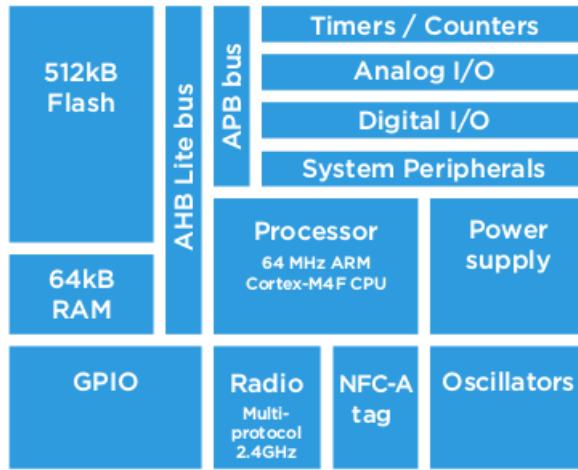


Figure 2.5: Nordic Semiconductor nRF52 chip in detail

2.5 Adafruit ADXL345 Accelerometer

In order to do collect data, a sensor needed to be connected to the Nordic Semiconductor nRF52. The main thought behind the thesis was to measure vibrations, and a good accelerometer was needed. The Adafruit ADXL345 accelerometer was chosen for several reasons.

- It is the same accelerometer built in on the Zolertia Z1 microcontroller
- It can measure acceleration in all three axes, X, Y and Z.
- It sends digital data right away. This means there is no need to use computational power to calculate digital values as needed if the data was captured by an analog accelerometer.
- It supports both I2C and Serial Peripheral Interface (SPI), which makes it easy to connect to the nRF52.

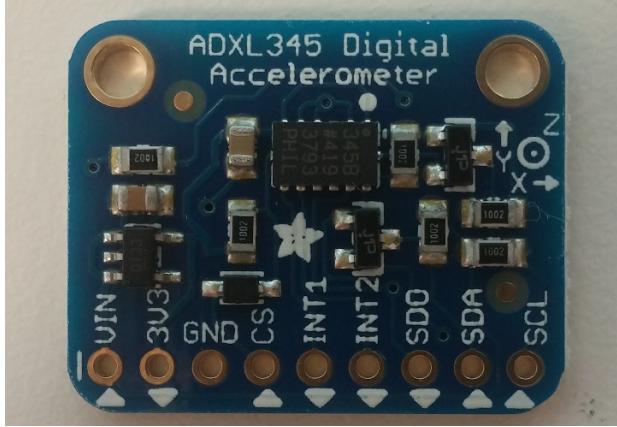


Figure 2.6: ADXL345 Accelerometer

2.6 Transport protocols

In order to transfer data from the end nodes to the central points of the network, either for analysing or already analysed data, a fast, efficient and stable transport protocol has to be used. This is a central aspect in this network, because the limitations of sending rate is thought to be one of the main limitations, either in the form of limits of data at once or number of sendings per second. The protocol needs to be stable and energy efficient and work with both BLE and 6LoWPAN. Luckily, Nordic Semiconductor provides example code and examples on how to get started with this.

2.6.1 CoAP

CoAP is a transport protocol designed to be used in constrained networks for Machine-to-machine (M2M) communication. It is User Datagram Protocol (UDP) based, and works well in low-power and lossy networks. It can be used with microcontrollers, and with IPv6 and 6LoWPAN. Both GET and PUSH functionality can be used, as well as *observable* GET. This means that a server can "subscribe" to end nodes in the network, and get updates either after a given timespan or when changes have been made. This therefore looked like a promising protocol to use, and was chosen as the main transport protocol to test in the network [8].

The main technical features described in CoAP is as follows:

- Web protocol fulfilling M2M requirements in constrained environments
- UDP binding with optional reliability supporting unicast and multicast requests.

- Asynchronous message exchanges.
- Low header overhead and parsing complexity.
- URI and Content-type support.
- Simple proxy and caching capabilities.
- A stateless HTTP mapping, allowing proxies to be built providing access to CoAP resources via HTTP in a uniform way or for HTTP simple interfaces to be realized alternatively over CoAP.
- Security binding to Datagram Transport Layer Security (DTLS).

CoAP has several similarities with working over Hyper Text Transport Protocol (HTTP), with the same client and server roles. The client sends a request, and the server sends a response back. Many of the response codes are also very similar, with *404: Not found* as the best known. When M2M communication is used, both participants sometimes needs to be both client and server, and the CoAP protocol handles this with a two-layer approach. . There are four different main messages defined in CoAP, being described as follows:

make figure of
CoAP Layer-
ing

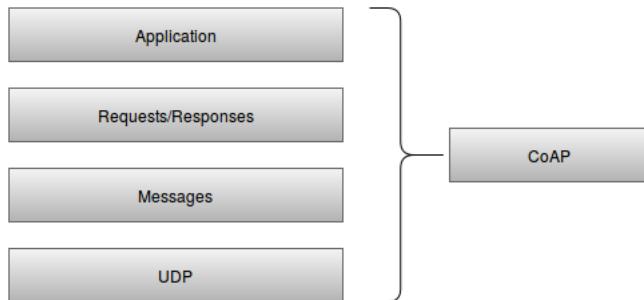
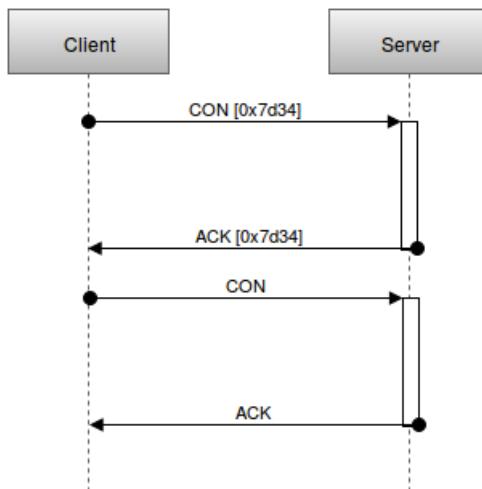
Confirmable *Some messages require an acknowledgement. These messages are called "Confirmable". When no packets are lost, each Confirmable message elicits exactly one return message of type Acknowledgement or type Reset.*

Non-confirmable Message Some other messages do not require an acknowledgement. This is particularly true for messages that are repeated regularly for application requirements, such as repeated readings from a sensor.

Acknowledgement Message An Acknowledgement message acknowledges that a specific Confirmable message arrived. By itself, an Acknowledgement message does not indicate success or failure of any request encapsulated in the Confirmable message, but the Acknowledgement message may also carry a Piggybacked Response (see below).

Other messages used is *GET, PUT, POST and DELETE*, to get or change data stored on the server.

Figure 2.9 shows the basic message sequence between the client and the server in a CoAP Confirmable CoAP message (CON) network. Every request CON message needs to be given an ack back. Figure 2.10 shows the same for Non-Confirmable CoAP message (NON), where no Acknowledgements (ACKs) are needed. The same initial set up with con and ack messages are still needed, to establish a connection

**Figure 2.7:** Sequence diagram CoAP**Figure 2.8:** CON CoAP client server sequence diagram

between the client and server before a stream of NON messages can be sent. This means a much more unreliable connection than using CON, since messages can be dropped without either the client or the server gets notified. This works in systems where every message does not need to get to its destination, for instance in a sensor based network like the network presented in this thesis. A message ID is still provided to every message to remove duplicated messages, but dropped messages are lost data. If the packages sent contained data that could not be dropped, for instance containing crucial patient information from censors on a patients body, this is not a good solution. In that case the reliable solution *must* be used.

Show examples of setting up coap NON needs acks first? Wireshark without bluetooth-sniffing?

Figure 2.11 summarizes the different message types used in CoAP. The default

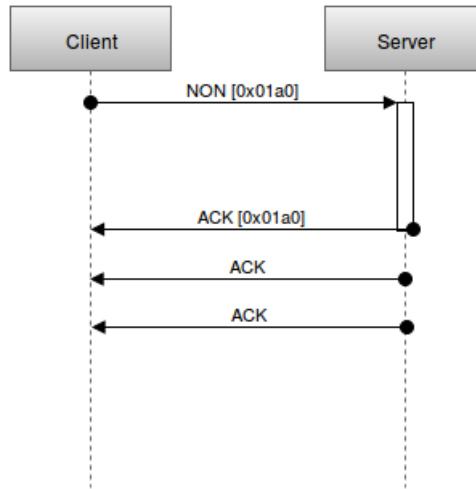


Figure 2.9: NON CoAP client server sequence diagram

Version	Type	Token Length	Code	Message ID
Token (if any, token length bytes)				
Options (in any)				
Payload (if any)				

Figure 2.10: CoAP message format

setting for an empty message is that it is a *reset* message or an ACK. The only exception is the use of *ping*, to test the Round Trip Time (RTT) in the network. In this case the empty message will work as a CON.

2.6.2 MQTT

Another transport protocol that could be used in such a network of microcontrollers is MQTT. This is known as a publish-subscribe based on Transmission Control Protocol (TCP), using a MQTT broker. NTNU does have a broker that is possible to use, or a broker can be rented from several other places. Here a

	CON	NON	ACK	RST
Request	X	X	-	-
Response	X	X	X	-
Empty	*	-	X	X

Figure 2.11: CoAP usage of message types

2.6.3 radvd

[?].

2.7 Software tools

As Integrated Development Environment (IDE), the *KEIL Vision* was used, as recommended by Nordic Semiconductor (where?), for writing C programming. For other programming languages (for instance Python 3.4, HTML, CSS, JavaScript, Flask and AJAX) *Sublime Text 2* for Windows and Linux was used, as well as *Pluma* for Ubuntu Mate on the Raspberry Pi.

2.7.1 Other

Wireshark, Firefox, GitHub

2.7.2 Abbreviations used in the rest of this thesis

Chapter 3

System Architecture

The purpose of this thesis is to build an end-to-end system, to be able to transfer data all the way from a sensor connected to a microcontroller to a server. This chapter will describe in detail how the different components of the system has been connected together, and how the different protocols has been configured to read and transfer data efficiently.

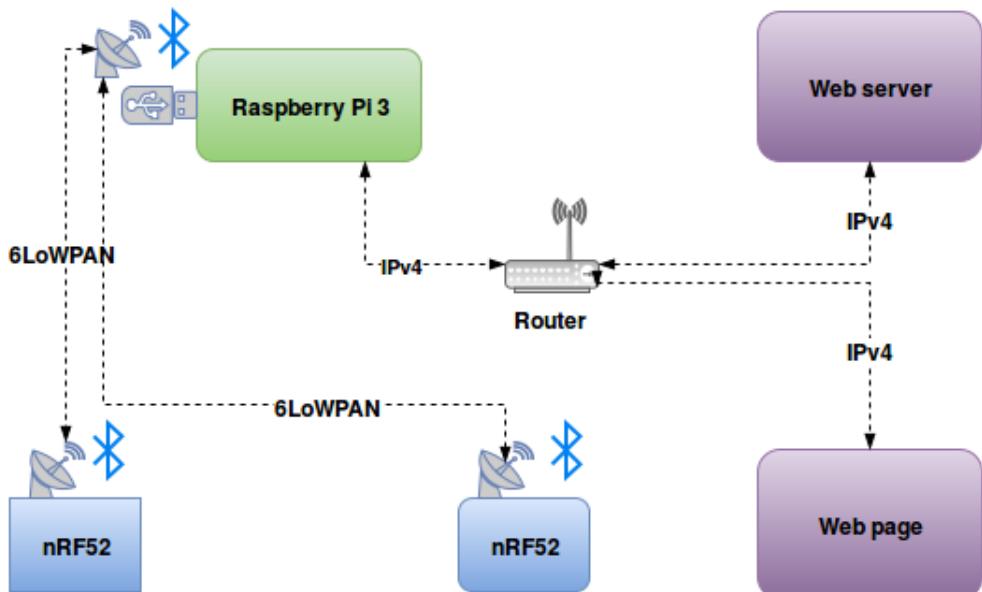


Figure 3.1: System architecture

Figure 3.1 shows how the complete end-to-end system of this thesis is set up. In short terms, the *Nordic Semiconductor nRF52* is connected to a *Raspberry Pi 3* using 6LoWPAN and BLE. This means that they are able to communicate using

IPv6 addresses, even though the nRF52 only has a bluetooth antenna built in. The limitations of BLE means that the nRF52 can only connect to *one* device at the time. Several of these put together are therefore forming a *star network* using the *Raspberry Pi* as a central point of connection. Computations can now either be done in the end nodes at the *nRF52s*, at the *Raspberry Pi*, or forwarded to a web server or another computer with more computational power. Data can also be displayed directly to a web page from the *Raspberry Pi*.

There are in general three main limitations in a network such as this:

- * Computational power in the different nodes
- * Battery capacity of the end nodes
- * Network limitations between the nodes

A central part of the testing in this thesis will be to test the different limitations, and to understand the pros and cons of doing computations in end nodes, compared to transferring information to a server with *much* more computational power. Power usage is very often closely related to computational power, and will also be a central factor. The next section will contain a walk-through of the system, from the smallest to the biggest component, to explain their computational and power capabilities, and how they can communicate efficiently.

Computational power is closely related to power usage. The nRF52 microcontroller is battery powered using a small *3V Lithium CR 2032* battery. Given this limitation the computational power will be limited as well. The optimal solutions therefore seems to handle as little data as possible here.

3.1 Connecting Raspberry Pi and nRF52

To set up the communication between a Raspberry Pi and the nRF52, the two code examples TWI and Observable server from Nordic Semiconductor was used as a starting point for coding on the nRF52. It was however quite tricky to set connect these two together the first time. The following recipe is what worked best.

Install an OS on the Raspberry Pi that has a Linux kernel version later than 3.18. On *Raspbian* version 3.18 is the only stable (Note: Jan. 2016), but *Ubuntu Mate* is stable in version 4.15. *Ubuntu Mate* was therefore chosen as the best and most stable OS. When this is done a resizing of the file system is needed to use all the capacity of the memory card.

To use BLE, install Bluez and radvd using *apt-get* in a *Unix terminal*:

```
apt-get install radvd wireshark bluez
apt-get upgrade
apt-get update
```

To activate IPv6 forwarding, uncomment the following line (remove "#") in the file *etc/sysctl.conf*

```
net.ipv6.conf.all.forwarding=1
```

Add the *bt0 interface* in *radvd.conf*:

```
touch /etc/radvd.conf
pico /etc/radvd.conf
```

Write in the *bt0 interface*

```
interface bt0
{
    AdvSendAdvert on;
    prefix 2001::/64
    {
        AdvOnLink off;
        AdvAutonomous on;
        AdvRouterAddr on;
    };
};
```

To mount the modules *bluetooth_6lowpan*, *6lowpan* and *radvd*, add the following to */etc/modules*.

```
bluetooth_6lowpan
6lowpan
radvd
```

It is now possible to use the *hcitool* command.

```
hcitool lescan
```

This command will scan for BLE devices nearby, and find the bluetooth address, for instance `0211:22FF:FE33:4455`. To connect, run the following:

```
echo 1 > /sys/kernel/debug/bluetooth/6lowpan_enable
echo "connect 0211:22FF:FE33:4455 1" > /sys/kernel/debug/bluetooth\\6lowpan_control
service radvd restart
```

The command `hcitool con` shows the connected BLE devices. If the device is connected, the connection can be tested by typing

```
ping6 2001::0211:22FF:FE33:4455
```

Using the basic example of the observable server it was easy to send CoAP messages without the need of an ACK for every message.

3.1.1 Connection challenges

```
ping6 2001:bt8::0211:22FF:FE33:4455
```

Describe
bt8-problem
and dev-
zone.nordicsemi.
com
and infocen-
ter.nordicsemi.
com

3.2 Nordic Semiconductor example code

Nordic Semiconductor has provided several examples along with the nRF52-DK documentation, that can be used as a starting point when programming applications to the device. These files are written in the programming language *C*.

3.2.1 CoAP

As a first step, the nRF52 needed to communicate with the Raspberry Pi. As explained in section 2.6, a good starting point for this is to use the CoAP trasnport protocol, and the example of the use of this on the device. The *CoAP Server* and *CoAP Observer* was loaded into two different nRF52 devices, and both of them connected to the Raspberry Pi. Now radvd had to be activated on the Pi, to be able to use this as a *forwarding server*.

Remove "Fig-
ure 1" from
image

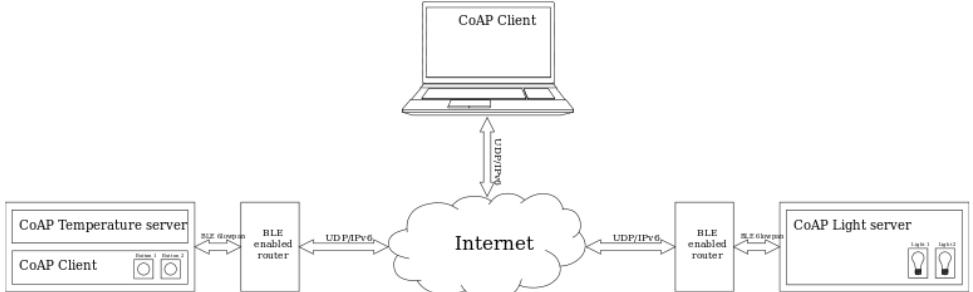


Figure 1: Setup of CoAP examples.

Figure 3.2: CoAP Client-Server communication example

Figure 3.5 shows the initial CoAP example, by using two nRF52 devices, BLE over 6LoWPAN and a BLE enabled router (Raspberry Pi) on both ends in this case. As the figure 3.5 shows, the code example for the CoAP client includes two different cases:

- * In the first case the CoAP client acts as a client requesting services from the CoAP server. Button 1 and 2 will control light 1 and 2 on the nRF52 server, which will send a confirmation back if the light was changed or if something went wrong.
- * In the second case the CoAP server is excluded, but the CoAP client works as a server that can handle requests from the router. In this case it is possible to use *Copper* in a *Firefox browser* on the Raspberry Pi to act as a client to request values from a simulated temperature sensor on the server. The server will then send the current simulated temperature back, or tell if something went wrong.

When packets are captured using *Wireshark*, we get the following capture:

This gives us the sequence diagram shown in Figure 3.4.

Create new sequence diagram

This works fine, and by writing a Python script running on the *Raspberry Pi* it is possible to request data by *GET messages* as soon as the *nRF52* is ready. However, as shown in figure 4.1 and figure 4.2, the network transfer rate can vary a lot. The

20 3. SYSTEM ARCHITECTURE

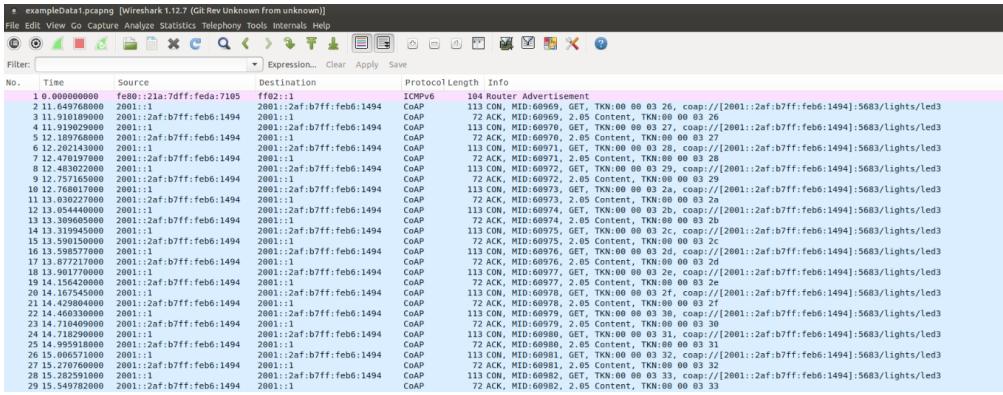


Figure 3.3: CoAP Client-Server example Wireshark capture

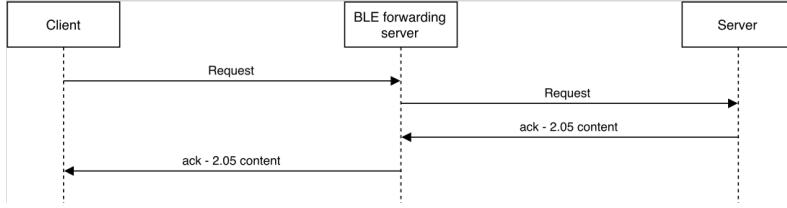


Figure 3.4: Sequence diagram CoAP Client-Server example

limitations in BLE and 6LoWPAN makes this much slower than a normal IPv6 connection, and the *ping* RTT varies from 100 ms all the way up to over 600 ms. As a comparison, to *ping google.com* from the same Raspberry Pi using IPv6 takes on average 15 ms. A comparison of this is shown in figure 4.1. This is therefore a clear limitation of sending rate in the system. Because of this, the maximum transfer rate achieved in the system using the standard CoAP server example is one message every 200 ms.

Using the standard CoAP, described as *CoAP CON* in this thesis, messages are sent with a "TCP mindset". This means that every message sent by the client must receive an ACK. This is very stable, and ensures that every message gets to its destination, but it requires a lot of unnecessary computational power in the leaf node in systems where the importance of each message is not that high. The system is meant to be used with tools for analysing, and it is not essential that data needs to get to its destination right away. In these cases there is another alternative, known in this thesis as *CoAP NON*. This is more like a "*glsudp mindset*", where each packet does *not* need an ACK. This halves the number of packages sent, saves a lot of the network as well as actions needed to be done by the nRF52 where power consumption

is a huge issue. Therefore the *CoAP Observable* function looked very interesting, and will therefore be directly compared to *standard glscoap* later in this thesis.

3.2.2 Observable CoAP

In the given Nordic example of a CoAP observable server, the problem of unnecessary packets being sent can be resolved. Using this it is easy to set up a server that can be observed by either a nRF52 client or a BLE forwarding server. The observable end point sends a *CON-ACK request* in a given time interval to assure that the observing client is still there. As long as this message is being responded the server will continue to send data without any requirements of an ACK.



Figure 2: Setup of the CoAP client with Light server application.

Figure 3.5: CoAP Observable Server example

3.3 Raspberry Pi to Network Computer or Server

When running the Unix based OS Ubuntu Mate, the raspberry Pi can be used more or less as a regular computer. This has a pre-installed version of the most basic programs needed, for instance *Mozilla Firefox Browser*, *Pluma text editor* and *Unix terminal*. This means that the user has several options on how to process data on this device:

- * No computation: All data arrives as useful data, and can be posted directly to a web page or a server for storage
- * No computation: Forward all data directly to a computer with more computational power
- * Some computation: Analyse the data to find data that is not relevant to filter out

Remove "Figure 1" from image

Create new sequence diagram for Observable as well

22 3. SYSTEM ARCHITECTURE

- * Full computation: Do a full analyse of the data. The results can then be posted directly to a server or displayed on a web page.

Which of these three that is most relevant depends on the data, and how computational power is needed.

Chapter 4

Network Measurements

This chapter will display the experiments conducted on data sending rate from the nRF52 to the Raspberry Pi in the form of graphs, tables and figures to try to determine the most efficient combination of amount of data to send, sending frequency as well as protocols to use.

4.1 Initial limitations in the Network

4.1.1 Stable transfer rate

As soon as the end nodes of the network can communicate with the Raspberry Pi, the next step is to test the transfer rate of the connection. To measure the network transfer rate, *ping6* was used. This is a software tool used to test networks using IPv6 in a network. The results is measured in ms used for every RTT.

```
ping6 2001::2e6:6aff:fe64:54dd  
ping6 google.com
```

When tested, the connection turns out to be very slow and in some cases very unstable, especially at maximum transfer rate. In the test of ping shown in figure 4.1 the connection between the Raspberry Pi and the nRF52 had 14 % packet loss, 1 out of 7 packets. Other test showed similar results, but the CoAP CON has in general got a higher stability at maximum sending rate than CoAP NON. After a test period it was therefore decided that the best solution for NON would be to gather data from sensors at a higher rate, and store them in the nRF52 temporarily. Every second all the measured values are being transferred to the Raspberry Pi, the temporarily values are deleted and the measurement continues. This has proven to be a very stable solution, with successful tests over several days. CON can handle more frequent transports than this in this system, on average 4 times per second. See the test shown in chapter 4.6. .

Make figure

```

sindre@PiMATE:~$ ping6 2001::2e6:6aff:fe64:54dd
PING 2001::2e6:6aff:fe64:54dd(2001::2e6:6aff:fe64:54dd) 56 data bytes
64 bytes from 2001::2e6:6aff:fe64:54dd: icmp_seq=1 ttl=64 time=577 ms
64 bytes from 2001::2e6:6aff:fe64:54dd: icmp_seq=2 ttl=64 time=625 ms
64 bytes from 2001::2e6:6aff:fe64:54dd: icmp_seq=3 ttl=64 time=605 ms
64 bytes from 2001::2e6:6aff:fe64:54dd: icmp_seq=4 ttl=64 time=583 ms
64 bytes from 2001::2e6:6aff:fe64:54dd: icmp_seq=5 ttl=64 time=632 ms
64 bytes from 2001::2e6:6aff:fe64:54dd: icmp_seq=6 ttl=64 time=611 ms
^C
--- 2001::2e6:6aff:fe64:54dd ping statistics ---
7 packets transmitted, 6 received, 14% packet loss, time 6007ms
rtt min/avg/max/mdev = 577.361/606.060/632.230/20.067 ms
sindre@PiMATE:~$ ping6 google.com
PING google.com(arn06s07-in-x0e.1e100.net) 56 data bytes
64 bytes from arn06s07-in-x0e.1e100.net: icmp_seq=1 ttl=56 time=15.1 ms
64 bytes from arn06s07-in-x0e.1e100.net: icmp_seq=2 ttl=56 time=15.0 ms
64 bytes from arn06s07-in-x0e.1e100.net: icmp_seq=3 ttl=56 time=15.0 ms
64 bytes from arn06s07-in-x0e.1e100.net: icmp_seq=4 ttl=56 time=15.0 ms
64 bytes from arn06s07-in-x0e.1e100.net: icmp_seq=5 ttl=56 time=15.0 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 15.007/15.065/15.162/0.144 ms
sindre@PiMATE:~$ 
```

Figure 4.1: Comparison: ping nRF52 and ping google.com

$$\bar{x}_n = \frac{\sum_{i=1}^n x_i}{n} \quad (4.1)$$

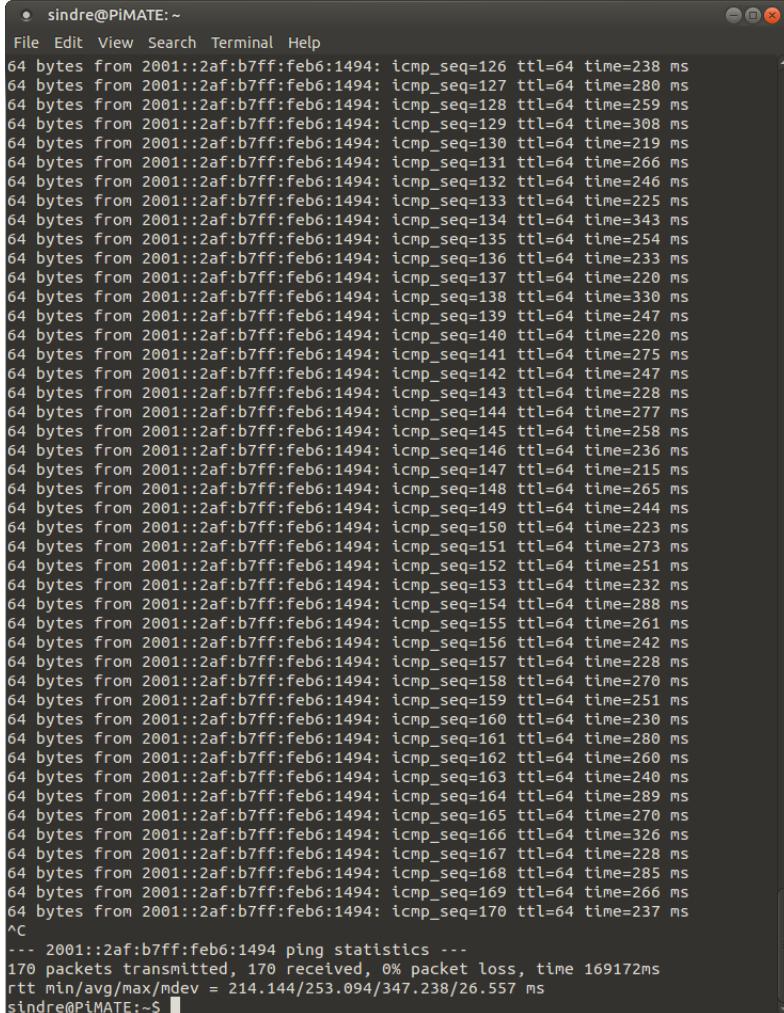
Equation 4.1 shows the standard way used to calculate an average of the measured values. Here a is any real number and n is any integer.

After a test period, the problems explained in was fixed. A more reliable test could then be performed, as shown in figure 4.2. Using equation 4.1 to calculate average gives an approximate average of 250 ms RTT. This is very slow, and way beneath the transfer limitations of both BLE, 6LoWPAN and CoAP, as explained in chapter 2. Another factor could be limited power supply and computational power, but it is not clear what is the main cause at this point. This will regardless be a huge limitation in the network.

The conclusion from these initial tests is therefore that CoAP CON is stable at lower transfer interval than CoAP NON, and can in best case cope with sending every 250th ms, which is very good compared to the high RTT. NON has been so unstable at initial tests that it was decided to only send every second. This makes

Skriv om
problemer
med bt8 i Ar-
chitecture?

Skriv spesifikt
om begren-
sninger for
disse tre i
background



```

sindre@PiMATE:~ 
File Edit View Search Terminal Help
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=126 ttl=64 time=238 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=127 ttl=64 time=280 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=128 ttl=64 time=259 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=129 ttl=64 time=308 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=130 ttl=64 time=219 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=131 ttl=64 time=266 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=132 ttl=64 time=246 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=133 ttl=64 time=225 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=134 ttl=64 time=343 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=135 ttl=64 time=254 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=136 ttl=64 time=233 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=137 ttl=64 time=220 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=138 ttl=64 time=330 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=139 ttl=64 time=247 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=140 ttl=64 time=220 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=141 ttl=64 time=275 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=142 ttl=64 time=247 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=143 ttl=64 time=228 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=144 ttl=64 time=277 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=145 ttl=64 time=258 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=146 ttl=64 time=236 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=147 ttl=64 time=215 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=148 ttl=64 time=265 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=149 ttl=64 time=244 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=150 ttl=64 time=223 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=151 ttl=64 time=273 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=152 ttl=64 time=251 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=153 ttl=64 time=232 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=154 ttl=64 time=288 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=155 ttl=64 time=261 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=156 ttl=64 time=242 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=157 ttl=64 time=228 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=158 ttl=64 time=270 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=159 ttl=64 time=251 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=160 ttl=64 time=230 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=161 ttl=64 time=280 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=162 ttl=64 time=260 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=163 ttl=64 time=240 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=164 ttl=64 time=289 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=165 ttl=64 time=270 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=166 ttl=64 time=326 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=167 ttl=64 time=228 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=168 ttl=64 time=285 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=169 ttl=64 time=266 ms
64 bytes from 2001::2af:b7ff:feb6:1494: icmp_seq=170 ttl=64 time=237 ms
^C
--- 2001::2af:b7ff:feb6:1494 ping statistics ---
170 packets transmitted, 170 received, 0% packet loss, time 169172ms
rtt min/avg/max/mdev = 214.144/253.094/347.238/26.557 ms
sindre@PiMATE:~$ 

```

Figure 4.2: Ping nRF52, different time

quite a huge difference when testing the different protocols, as *CoAP CON* can send a lot more *goodput* per second, but *CoAP NON* requires less power to send each message, and a much higher percentage of the packets sent through the network contains useful data.

4.1.2 Packet fragmentation

In Internet Routing, *fragmentation* is known as the action of splitting data into smaller packets, to satisfy the maximal limits of the different technologies or protocols

used (e.g. BLE and 6LoWPAN in the network described in this thesis). Each of these packets needs header fields of a certain size, or other requirements. In a network of microcontrollers used in this thesis fragmentation can be a factor that needs to be taken into account to optimize the goodput of the system. This will be a central part of the testing, and will therefore be explained in detail in the following section.

To better understand fragmentation, imagine a train with carriages as shown in Figure 4.3. To be able to operate at all, the train needs a locomotive with an engine driver, a conductor and a cafe carriage. As soon as these things are already there, the company owning the train gets better and better off for every passenger buying a ticket. Lets assume that every carriage can carry 4 employees and 27 passengers, to make it directly comparable to the BLE packets in the network. Eventually all the carriages will be full, and a decision has to be made if it will be profitable to fit another carriage. It will in general be most profitable to use as many carriages as the locomotive can handle, and to fill up every carriage as much as possible. It will however not be a good idea to connect another carriage if there will only be one additional passenger sitting there, since the extra weight of the carriage adds unnecessary additional weight to the train set compared to the income.

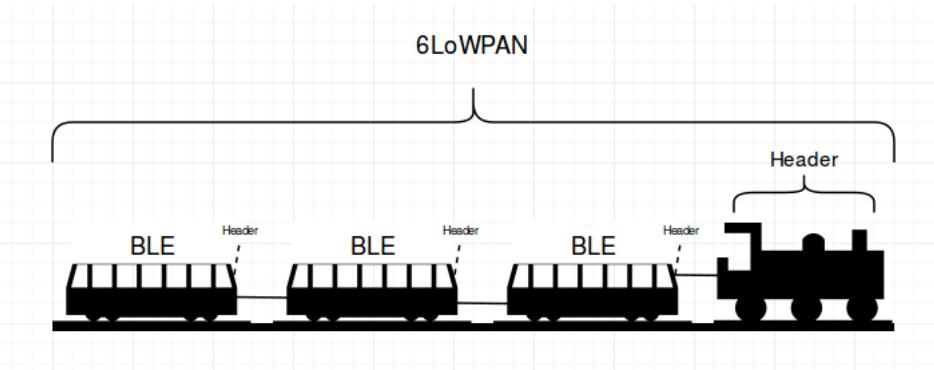


Figure 4.3: Packet fragmentation - train comparison

In this example, the locomotive and employees are the 6LoWPAN packet, that are needed no matter what to get the train working. Each additional carriage is a BLE packet. The goal is therefore to find the maximal number of passengers compared to the cost of adding additional carriages, in other words the maximal number of bytes compared to the number of packets sent. This is known as *fragmentation*, fragmenting data into smaller pieces to satisfy the maximal limitations of packet sizes in the different protocols. This can be exploited by a system developer to maximize *goodput vs throughput* in the network.

4.2 Description of measurements

The following sections will show experiments performed to test if *fragmentation* is a huge issue when sending data through low energy networks, and which of the protocols described in chapter 2 is the most efficient to use when the goal is to get as high *goodput* as possible. This will be done by sending data of constant length, capture packets using *Wireshark*, and then increasing the packet size to see the changes.

Before these experiments started, the expected results was that sending a small amount of data at a time would not be preferable, because of the needed bytes to set up the connection, header files and so on. It was not known how big the packages needed to be before it would be considered *profitable* to send.

When sending BLE packets over the network, observations from the system shows that the maximum packet size over BLE is 31 bytes. Each of these packages needs a header field of 4 bytes, meaning 27 bytes left for useful data. However, to start the connection at all, 76 byte is needed, meaning three BLE packets. The ratio between *useful* and *needed* (known as *goodput* and *throughput*) data transferred therefore start out very poorly if the payload sent is very small. The best possible percentage of useful data we can hope to achieve will also be limited by this, 27 bytes goodput and 4 bytes header field, shown in the following calculation.

$$\delta = \frac{x_2}{x_1} * 100\% \quad (4.2)$$

Equation 4.2 shows the standard way used to calculate the percentage, δ , that the natural number x_2 is of the total amount x_1 .

$$\frac{27b}{31b} * 100\% = 87,094776\% \approx 87,1\% \quad (4.3)$$

In the actual system the number will quite certainly be a lot lower than this. Both because header files in 6LoWPAN packages needs to use some of the capacity, and because of other limitations.

Like what?

4.3 CoAP

As explained in Chapter 4.1.1, CoAP can be split into two different main sections. CON messages can be sent quite frequently, but every message needs to get an ACK before the next message can be sent. This means that it is quite fast, but a lot of

packets needs to be transported through to get usable data at the other end. The other alternative is NON, where each message does *not* need an ACK.

Table 4.1: Wireshark CoAP CON 0 bytes

Number	Time	Protocol	Length	Info
36	3.7471	CoAP	72	ACK, MID:57083, 2.05 Content
37	3.7759	CoAP	113	CON, MID:57084, GET
38	3.9571	HCI_ACL	31	Rcvd [Reassembled in #40]
39	3.9584	HCI_ACL	31	Rcvd [Continuation to #38]
40	4.0274	L2CAP	5	Rcvd Connection oriented channel
41	4.0367	L2CAP	58	Sent Connection oriented channel
42	4.0368	L2CAP	50	Sent Connection oriented channel
43	4.0975	L2CAP	16	Rcvd LE Flow Control
44	4.0977	HCI_EVT	7	Rcvd Number of Completed Packets
45	4.1678	HCI_EVT	7	Rcvd Number of Completed Packets
46	4.0275	CoAP	72	ACK, MID:57084, 2.05 Content
47	4.0366	CoAP	113	CON, MID:57085, GET

Table 4.1 shows the most basic example of a capture of packets in Wireshark. The full capture can be seen in the Appendix A. In this case an empty char array was sent, meaning an goodput equal to 0 byte. All of these bytes are therefore sent to route packages through the network. The maximum of 31 bytes per BLE packet have been exceeded twice, meaning that three packets needed to be sent. The first packet is labeled *[Reassembled in #40]*, the second *[Continuation to #38]* and the last *Connection oriented channel*. After this, the ACK packages follows, two packages of 58 and 50 bytes, respectively. The last bytes received tells how many packages was completed, as a built in feature in BLE HCI and ACL. All of these packages can fit into one 6LoWPAN packet, since the total number of bytes are less than 270 bytes.

Note that packet number 46 and 47 in table 4.1 has got a timestamp that indicates that they originally was sent from the end node in the network as packet number 41 and 42, but used longer time than the other packets sent through the network at the same time. The main reason for this is of course that they are bigger than the rest of the packets, but since the network limit should be much higher than this it can maybe be seen as a weakness that this gives a clear impact even at these small values.

In table 4.2, 100 bytes of goodput is being sent through. The same basic packages needed are still there, but in addition the 100 bytes of data is added. This means adding more BLE packets, but also that the percentage of useful data sent through

Table 4.2: Wireshark CoAP CON 100 bytes

Number	Time	Protocol	Length	Info
29	2.4514	HCI_ACL	31	Rcvd [Reassembled in #36]
30	2.4516	HCI_ACL	31	Rcvd [Continuation to #29]
31	2.2425	CoAP	173	ACK, MID:16354, 2.05 Content
32	2.2538	CoAP	113	CON, MID:16355, GET
33	2.5217	HCI_ACL	31	Rcvd [Continuation to #29]
34	2.5218	HCI_ACL	31	Rcvd [Continuation to #29]
35	2.5907	HCI_ACL	31	Rcvd [Continuation to #29]
36	2.5921	L2CAP	25	Rcvd Connection oriented channel
37	2.6099	L2CAP	58	Sent Connection oriented channel
38	2.6100	L2CAP	50	Sent Connection oriented channel
39	2.6610	L2CAP	16	Rcvd LE Flow Control
40	2.6621	HCI_EVT	7	Rcvd Number of Completed Packets
41	2.5922	CoAP	173	ACK, MID:16355, 2.05 Content
42	2.3097	CoAP	113	CON, MID:16356, GET
43	2.7311	HCI_EVT	7	Rcvd Number of Completed Packets

is a lot higher, approximatley 55 % in this case. By doing several experiments like this, it was possible to create the graph in Figure 4.4. This shows the correlation between goodput and throughput compared to the number of packets sent, measured every 10th byte from 0 byte to 200 bytes large packets.

In this particular case shown in 4.4 it makes no sense to send less than 50 bytes of useful data at once, since more than 50 % of the bytes sent will be header files. This is comparable to having a locomotive and full crew at disposal, but only a few or none paying passengers. The best possible result is to have every carriage full, with 27 passengers and 4 employees. Since at least 4 bytes out of every 31 sent needs to be used to header information, the best possible result will be 87,1 %, as shown in equation 4.1. In mathematics, this is described as a *horizontal asymptote* since the distance between the graph and $y = 87,1$ will approach zero after an infinite number of bytes has been transferred. The graph will therefore converge to 87,1 %, just as the values climbing in figure 4.4, even before packet size of 200 bytes.

4.3.1 Discussion

Even though this first test was done with a very limited amount of data transferred, it is easy to see that the curve clearly flattens out and forms the shape of a *parabola* with a vertical *directrix* at $x = 0$. The next step would be to transfer a larger amount of data, to verify that the assumptions that the graph will converge to the asymptotic

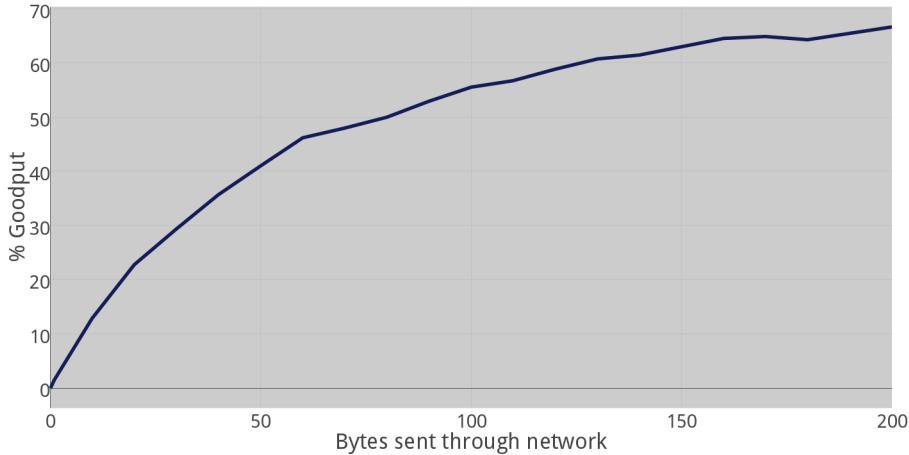


Figure 4.4: CoAP CON, 0-200 bytes sent

value $y = 87,1$ when $\lim_{x \rightarrow \infty}$. The limitations of transfer rate is not nearly yet met by either BLE or 6LoWPAN. This test will therefore be explained in the next section.

Since there is already a clear trend in the form of the graph in figure 4.4 even before the transfer rate reaches 200 bytes, it makes sense to also test the other version included in CoAP, CON. If it is possible to find a way of transportation that could give a higher mathematical maximum, and also get to this limit faster, it could be very profitable to the system. It also makes sense to test CoAP NON because it doesn't need to send an ACK for every packet, as CON does. Maybe this means that the header files can be split up in another way, and that the useful amount of data sent through therefore will be higher.

To see what happened when the limit of a 6LoWPAN packet was breached in the system, tests were being set up to send larger amounts of data than 200 bytes. This would also be a good way to test if the percentage of goodput will converge to 87,1 %, only considering BLE packets. The following test and examples will therefore send a fixed number of bytes at once from 0 to 1000 bytes (1 kB), with a 50 byte interval. As before, the messages are being sent as soon as possible, meaning approximately four messages per second on average using CoAP CON. In addition will NON be tested in detail.

4.3.2 CoAP NON comparison

A CoAP NON request does not require a response in form of an ACK. This means that the 108 bytes sent to and handled by the end node can be skipped, which means less computational power in the end node and network capacity to the node is needed. This solution makes sense to use in networks where the demand for all data is low, since packets can be lost without the use of ACKs. As explained in chapter 4.1.1, the transfer frequency is limited using NON in this system, due to unstable results in tests at the beginning of the set up. The transfer rate is therefore set to one per second for this protocol.

4 LEDs image?

Table 4.3: Wireshark CoAP NON 0 bytes

Number	Time	Protocol	Length	Info
90	23.0405	HCI_ACL	31	Rcvd [Reassembled in #92]
91	23.0411	HCI_ACL	31	Rcvd [Continuation to #90]
92	23.1107	L2CAP	9	Rcvd Connection oriented channel
93	23.1109	CoAP	76	NON, MID:14, 2.05 Content

A basic example of the CoAP NON connection is shown in table 4.3. The entire Wireshark capture can be seen in Appendix A. This is directly comparable to table 4.1, that shows a Wireshark capture of CoAP CON packages. It is easy to see that a lot fewer packages needs to be sent using BLE, without the use of ACKs. The total amount of bytes sent is $31+31+9=71$ bytes, meaning three BLE packages and one 6LoWPAN packet. This is less than half of what was needed using CoAP CON, where the 108 ACK packages was needed in addition. The packets are still recognizable the same way as before, the first packet is labeled *[Reassembled in #40]*, the second *[Continuation to #38]* and the last *Connection oriented channel*.

Fewer packages sent means less energy used, less network capacity needed and less computational power in the end node. Hopefully this will lead to a higher percentage of goodput compared to throughput as well. it would therefore be interesting to compare the rest of the measured values.

Table 4.4 shows the case where 100 bytes of data are sent using CoAP NON. This is directly comparable to the test shown in table 4.2, where the same amount of data is sent over CON. The overall structure is the same as before. Since it is only one packet noted *Reassembled in #n*, which marks the beginning of a new 6LoWPAN packet. The total amount sent must therefore be under 270 bytes, which makes sense. The NON packet size is here 177 bytes, compared to 173 bytes in CON, which represents one more header field of 4 bytes needed in NON. Overall a small difference

Table 4.4: Wireshark CoAP NON 100 bytes

Number	Time	Protocol	Length	Info
39	11.0363	CoAP	177	NON, MID:2, 2.05 Content
40	11.9452	HCI_ACL	31	Rcvd [Reassembled in #45]
41	11.9465	HCI_ACL	31	Rcvd [Continuation to #40]
42	12.0154	HCI_ACL	31	Rcvd [Continuation to #40]
43	12.0168	HCI_ACL	31	Rcvd [Continuation to #40]
44	12.0857	HCI_ACL	31	Rcvd [Continuation to #40]
45	12.0858	L2CAP	29	Rcvd Connection oriented channel
46	12.0860	CoAP	177	NON, MID:3, 2.05 Content

in the packets containing data, but as expected a lot more packets needs to be sent in total in CON.

Using these measurements the following plot could be drawn.

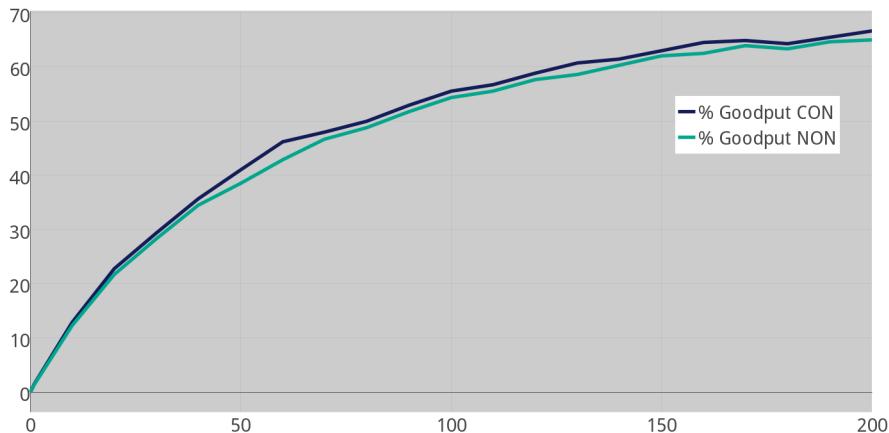
**Figure 4.5:** CON vs NON 0-200 bytes

Figure 4.5 shows the comparison between sending between 0 and 200 bytes of useful data through the network at once. Keep in mind that this does not show sending rate per time (which will be discussed in chapter), but percentage of the data sent that is useful data. CON can be sent much more often than NON in practice. It could therefore maybe be expected that this could give NON an advantage. . NON does not need to send ACKs for every package, which should be an advantage concerning to maximize throughput. Still it is the more complex and more frequently

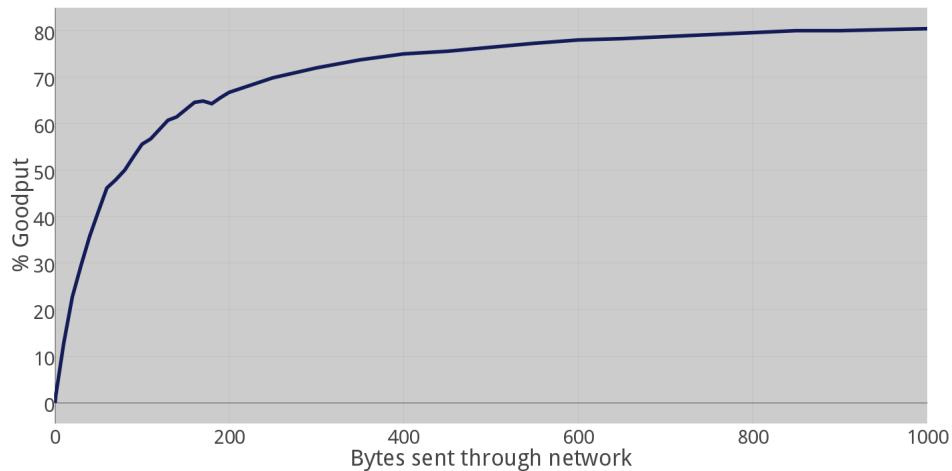
write chapter

<- Re-write

sent CON that gets the best results in this test, with a small margin.

4.3.3 CoAP, testing with more data

Table 4.5 shows a bigger and more complex case, where 700 bytes of data are being sent at once. In total 889 bytes are being sent, with a CON packet size of 774 bytes. This gives a percentage of goodput at 78.74 %. The maximum packet length of a 6LoWPAN packet in this system of 270 bytes is therefore exceeded, as we can see in the figure. After 8 BLE packages of 31 bytes each has been sent, there is only room for 22 bytes in the last packet before the 6LoWPAN packet is full. This is repeated several times, once for each 6LoWPAN packet, until the last BLE packets at the size of 17 bytes. After this the standard packages for ACK and *Number of completed packages* follows. This is in general a good example on how fragmentation of packets works in this system.

**Figure 4.6:** CoAP CON plot, 200 bytes to 1 kB

Make graph
more clear

Using these results it was possible to plot the graph in figure 4.6 . Here it is easy to see the same trends as in 4.4, but in more detail over a wider span of bytes sent. These results are as expected after the previous tests, and in compliance with the calculations done in equation 4.1.

In this example points in the graph was denoted every 50th byte sent. This gives us

set in graph
for 0-1000
before this,
to see the
flatness?

Table 4.6 shows the case where 700 bytes were sent at once through the network, using CoAP NON. The NON packet size is at 777 bytes, which is as expected from the previous tests. This means 4 bytes larger than the same test using CON, meaning an additional header field.

$$\frac{78,47}{78,74} \approx 0,9966 \rightarrow 100\% - 99,66\% = 0,34\% \quad (4.4)$$

Calculations in equation 4.4 show that the goodput here is 78,47 %, compared to 78,74 % in CON. The difference between these two is 0,34 %, which in this case is considered *very* small. This can also be seen clearly in 4.9. Because of this, it was concluded that the results for using NON and CON can be considered as negligible for transmissions larger than 1 kB. Tests with larger amounts of data than this at once was therefore not conducted in this project.

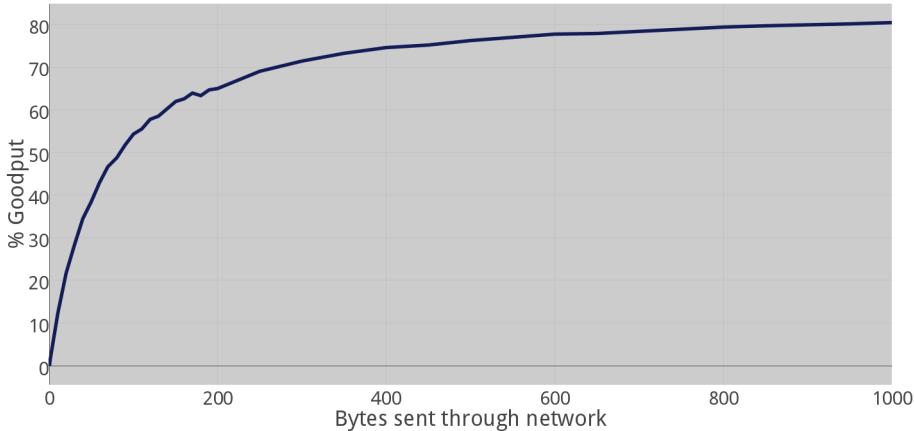


Figure 4.7: NON 0-1000 bytes

The entire scope of the tests done on CoAP NON in this system is shown in figure 4.7. Given these results, it can be concluded that to send less data than 200 bytes at the time is not preferable, since the percentage of goodput compared to the total amount sent can be very low. On the other hand, the graph stabilizes around 75-80 %. Given these measurements it looks like 400 bytes and bigger packets are preferable in this system. The system shows no signs of weakness as the packet size grows, and it will therefore be possible to send as large packets as needed until the limitations of BLE with the same amount of goodput at about 80 %.

Remove figure
4.8 200-1000?

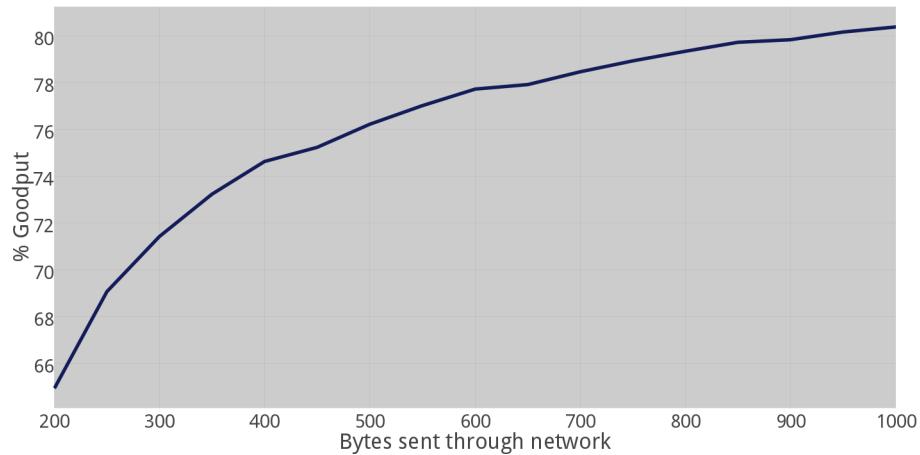


Figure 4.8: NON 200-1000 bytes

4.3.4 Discussion

4.4 Comparison

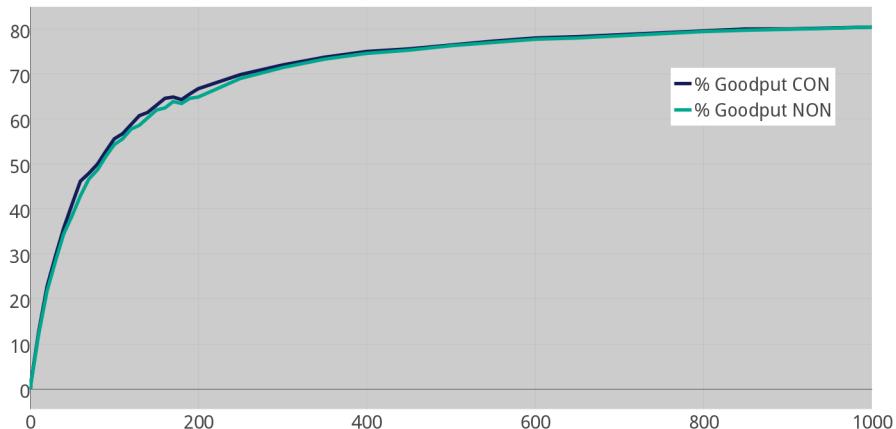


Figure 4.9: CON vs NON 0-1000 bytes

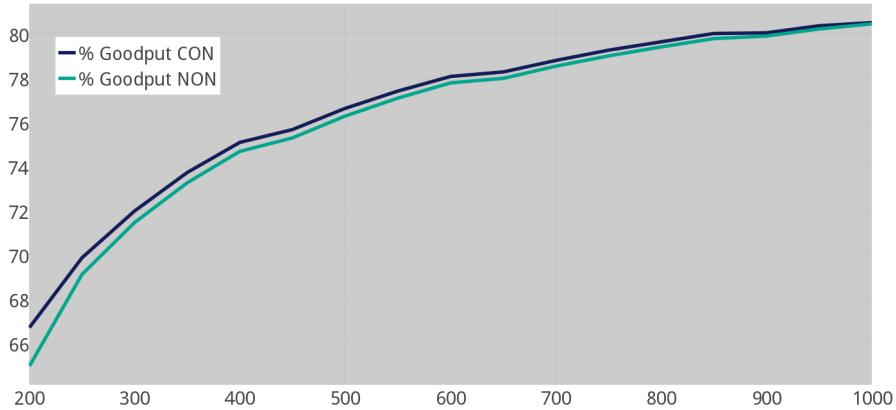


Figure 4.10: CON vs NON 200-1000 bytes

4.4.1 Goodput per time interval

4.5 BLE

4.6 Time spent in network

The previous tests shows

Calcumate time for CoAP NON, 700 bytes sent:

$$((55.9578 - 54.7750) + (57.1476 - 55.9578) + (58.3379 - 57.1476))/3 = 1.1876 \quad (4.5)$$

$$0.1876/3 = 0.0625$$

Table 4.5: Wireshark CoAP CON 700 bytes

Number	Time	Protocol	Length	Info
53	3.2570	CoAP	774	ACK, MID:35081, 2.05 Content
54	3.2727	CoAP	113	CON, MID:35082, GET
55	3.4671	HCI_ACL	31	Rcvd [Reassembled in #63]
56	3.4747	HCI_ACL	31	Rcvd [Continuation to #55]
57	3.5374	HCI_ACL	31	Rcvd [Continuation to #55]
58	3.5375	HCI_ACL	31	Rcvd [Continuation to #55]
59	3.6077	HCI_ACL	31	Rcvd [Continuation to #55]
60	3.6078	HCI_ACL	31	Rcvd [Continuation to #55]
61	3.6767	HCI_ACL	31	Rcvd [Continuation to #55]
62	3.6782	HCI_ACL	31	Rcvd [Continuation to #55]
63	3.7533	L2CAP	22	Rcvd Connection oriented channel
64	3.7534	L2CAP	16	Sent LE Flow Control
65	3.8172	HCI_EVT	7	Rcvd Number of Completed Packets
66	3.8172	HCI_ACL	31	Rcvd [Reassembled in #74]
67	3.8185	HCI_ACL	31	Rcvd [Continuation to #66]
68	3.9575	HCI_ACL	31	Rcvd [Continuation to #66]
69	3.9577	HCI_ACL	31	Rcvd [Continuation to #66]
70	4.0266	HCI_ACL	31	Rcvd [Continuation to #66]
71	4.0342	HCI_ACL	31	Rcvd [Continuation to #66]
72	4.0979	HCI_ACL	31	Rcvd [Continuation to #66]
73	4.0982	HCI_ACL	31	Rcvd [Continuation to #66]
74	4.1671	L2CAP	22	Rcvd Connection oriented channel
75	4.2372	HCI_ACL	31	Rcvd [Reassembled in #83]
76	4.2373	HCI_ACL	31	Rcvd [Continuation to #75]
77	4.3075	HCI_ACL	31	Rcvd [Continuation to #75]
78	4.3076	HCI_ACL	31	Rcvd [Continuation to #75]
79	4.3777	HCI_ACL	31	Rcvd [Continuation to #75]
80	4.4466	HCI_ACL	31	Rcvd [Continuation to #75]
81	4.4480	HCI_ACL	31	Rcvd [Continuation to #75]
82	4.4481	HCI_ACL	31	Rcvd [Continuation to #75]
83	4.5170	L2CAP	22	Rcvd Connection oriented channel
84	4.5871	HCI_ACK	31	Rcvd [Reassembled in #86]
85	4.5875	HCI_ACL	31	Rcvd [Continuation to #84]
86	4.6574	L2CAP	17	Rcvd Connection oriented channel
87	4.6731	L2CAP	58	Rcvd Connection oriented channel
88	4.6732	L2CAP	50	Rcvd Connection oriented channel
89	4.6577	CoAP	774	ACK, MID:35082, 2.05 Content
90	4.6729	CoAP	113	NON, MID:35083, GET

Table 4.6: Wireshark CoAP NON 700 bytes

Number	Time	Protocol	Length	Info
264	57.1476	CoAP	777	NON, MID:3, 2.05 Content
265	57.2177	HCI_ACL	31	Rcvd [Reassembled in #273]
266	57.2178	HCI_ACL	31	Rcvd [Continuation to #265]
267	57.2879	HCI_ACL	31	Rcvd [Continuation to #265]
268	57.2943	HCI_ACL	31	Rcvd [Continuation to #265]
269	57.3570	HCI_ACL	31	Rcvd [Continuation to #265]
270	57.3583	HCI_ACL	31	Rcvd [Continuation to #265]
271	57.4272	HCI_ACL	31	Rcvd [Continuation to #265]
272	57.4286	HCI_ACL	31	Rcvd [Continuation to #265]
273	57.4975	L2CAP	22	Rcvd Connection oriented channel
274	57.4979	L2CAP	16	Sent LE Flow Control
275	57.5676	HCI_ACL	31	Rcvd [Reassembled in #284]
276	57.5685	HCI_EVT	7	Rcvd Number of Completed Packets
277	57.5753	HCI_ACL	31	Rcvd [Continuation to #275]
278	57.6378	HCI_ACL	31	Rcvd [Continuation to #275]
279	57.6379	HCI_ACL	31	Rcvd [Continuation to #275]
279	57.7080	HCI_ACL	31	Rcvd [Continuation to #275]
280	57.7082	HCI_ACL	31	Rcvd [Continuation to #275]
281	57.7771	HCI_ACL	31	Rcvd [Continuation to #275]
282	57.7785	HCI_ACL	31	Rcvd [Continuation to #275]
283	57.7785	HCI_ACL	31	Rcvd [Continuation to #275]
284	57.8474	L2CAP	22	Rcvd Connection oriented channel
285	57.9176	HCI_ACL	31	Rcvd [Reassembled in #293]
286	57.9176	HCI_ACL	31	Rcvd [Continuation to #285]
287	57.9878	HCI_ACL	31	Rcvd [Continuation to #285]
288	57.9879	HCI_ACL	31	Rcvd [Continuation to #285]
289	58.0580	HCI_ACL	31	Rcvd [Continuation to #285]
290	58.0581	HCI_ACL	31	Rcvd [Continuation to #285]
291	58.1270	HCI_ACL	31	Rcvd [Continuation to #285]
292	58.1284	HCI_ACL	31	Rcvd [Continuation to #285]
293	58.1972	L2CAP	22	Rcvd Connection oriented channel
294	58.2673	HCI_ACK	31	Rcvd [Reassembled in #296]
295	58.2688	HCI_ACL	31	Rcvd [Continuation to #294]
296	58.3378	L2CAP	20	Rcvd Connection oriented channel
297	58.3379	CoAP	777	NON, MID:4, 2.05 Content

Chapter 5

Data Anaysis discussion

IDEA: "Collect" the strings put out in the first chapter, which told us the challenges in a system of microcontrollers. This chapter could tell what we learned from the system, and what is still a challenge. Or should all of this be in the Result chapter?

5.1 Data analysis in microcontrollers

5.2 Computational Power

5.2.1 Power consumption

Windows error message: "The device needs more data than the computer can supply".

5.3 Ease of use

5.3.1 Raspberry Pi

5.3.2 nRF52

The nRF52 is perhaps the biggest disappointment in the system, from the authors perspective.

As a comparison, take the successful hybrid car Toyota Prius. Even though the factory tells that the car is able to drive X kilometres per liter of fuel used, this is only possible for a trained driver in a fixed environment. The average driver can still use the car, but is not skilful enough to drive as careful when it comes to power usage. The average driver therefore ends up using up the batteries much faster than the test driver, and uses the petrol powered engine after this. It may still be more economical than a normal car, but it is worth discussing if this is optimal, given that a car with two engines is more heavy and expensive to make in a direct comparison with a fully petrol powered car.

Its the same story with the nRF52. A professional skilled programmer working on this specific device from Nordic Semiconductor will be able to use the low power

abilities and still use do efficient computations. When starting from the example code for the device that is not optimized for power consumption and trying to make it do more and more work, the battery consumption simply is too much for this device. An average programmer will not have specific experience enough to program this device to be power efficient.

In the case of the system built in this thesis, the small CR 2033 batteries were drained so fast that an additional power source was needed to keep a stable and reliable system, since tests have shown that the probability of an nRF52 disconnecting from the connected BLE service is higher at low battery. This meant connecting either a power bank with higher capacity or drain power from an outlet using a micro Universal Serial Bus (USB). In this case, it would have been able to use the Raspberry Pi right away, since this needs the same source of power. This means in the end, that the system only had low performance end points that still needed a power source.

References

- [1] Newark: element 14. <https://www.newark.com/>. Accessed: 13-05-2016.
- [2] Nordic Semiconductor: nrf52 series soc. <https://www.nordicsemi.com/Products/nRF52-Series-SoC>. Accessed: 25-03-2016.
- [3] Gomez, C., J. Oller, and J. Paradells (2012). Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. *Sensors* 12(9), 11734–11753.
- [4] Hui, J. W. and D. E. Culler (2008). Extending ip to low-power, wireless personal area networks. *Internet Computing, IEEE* 12(4), 37–45.
- [5] Hunkeler, U., H. L. Truong, and A. Stanford-Clark (2008). Mqtt-s—a publish/subscribe protocol for wireless sensor networks. In *Communication systems software and middleware and workshops, 2008. comsware 2008. 3rd international conference on*, pp. 791–798. IEEE.
- [6] Kushalnagar, N., G. Montenegro, D. E. Culler, and J. W. Hui (2007). Transmission of ipv6 packets over ieee 802.15. 4 networks.
- [7] Mulligan, G. (2007). The 6lowpan architecture. In *Proceedings of the 4th workshop on Embedded networked sensors*, pp. 78–82. ACM.
- [8] Shelby, Z., K. Hartke, and C. Bormann (2014). The constrained application protocol (coap).

Chapter

Appendix A

Appendix A contains samples of programming code used to gather and transfer data in the IoT system described in this thesis.

Chapter **B**

Appendix B

Appendix B contains screenshots and detailed figures from the measurements done in the network built in this thesis.

Goodput	Throughput	NON packet size	(Goodput/Throughput)*100
0	71	76	0
1	73	78	1,37
10	82	87	12,20
20	92	97	21,74
30	75	107	30,0
40	85	117	47,06
50	99	127	50,51
60	109	137	55,05
70	119	147	58,82
80	133	157	60,15
90	143	167	62,94
100	153	177	65,36
110	167	187	65,87
120	177	197	67,80
130	191	207	68,06
140	207	217	69,65
150	211	227	71,09
160	225	237	71,11
170	235	247	72,34
180	253	257	71,15
190	263	267	72,24
200	277	277	72,20