



NTNU – Trondheim
Norwegian University of
Science and Technology

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

Sindre Schei

Submission date: April 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 Algorithms	xv
List of Symbols	xvii
List of Acronyms	xix
1 Introduction	1
1.1 Motivation	1
1.2 Methodology	1
1.3 Structure	1
2 Background	3
2.1 Bluetooth Low Energy	3
2.2 6LoWPAN	4
2.3 Raspberry Pi	4
2.3.1 Ubuntu Mate	5
2.4 nRF52	5
2.5 Adafruit ADXL345 Accelerometer	6
2.6 Transport protocols	7
2.6.1 Constrained Application Protocol (CoAP)	7
2.6.2 Message Queueing Telemetry Transport (MQTT)	7
2.6.3 Router Advertisement Daemon (radvd)	7
2.7 Software tools	7
3 Architecture	9
3.1 Connecting nRF52 and ADXL345	10
3.2 IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) and Bluetooth Low Energy (BLE)	10
3.3 Connecting Raspberry Pi and nRF52	10

3.3.1	Serial Peripheral Interface (SPI)	14
3.3.2	Inter-Integrated Circuit (I2C)	14
3.3.3	Problems	14
4	Coding and Limitations	15
4.1	Nordic Semiconductor example code	15
4.1.1	CoAP	15
4.1.2	Observable CoAP	17
4.1.3	Stable transfer rate	17
4.2	Getting acceleration values	18
4.3	Limitations	19
4.4	Measurements	19
5	Measurements	21
5.1	temp/notes	21
5.2	Goodput vs throughput	21
5.3	Packet fragmentation	21
5.3.1	Train example	21
References		23
Appendices		

List of Figures

2.1	ADXL345 Accelerometer	6
3.1	System architecture	9
3.2	Connected nRF52 – ADXL345	11
3.3	Nordic Semiconductor NRF52	12
3.4	Raspberry Pi 3	13
4.1	CoAP Client-Server communication example	16
4.2	CoAP Client-Server example Wireshark capture	16
4.3	Sequence diagram CoAP Client-Server example	17
4.4	CoAP Observable Server example	17
4.5	Comparison: ping nRF52 and ping google.com	18

List of Tables

List of Algorithms

List of Symbols

A_B^C A dummy symbol.

List of Acronyms

6LoWPAN IPv6 over Low Power Wireless Personal Area Networks.

ACK Acknowledgement.

BLE Bluetooth Low Energy.

CoAP Constrained Application Protocol.

DNS Domain Name System.

GUI Graphical User Interface.

HCI Host Controller Interface.

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.

LAN Local Area Network.

M2M Machine-to-machine.

MQTT Message Queueing Telemetry Transport.

NDP Neighbor Discovery Protocol.

NTNU Norwegian University of Science and Technology.

OS Operating System.

PAN Personal Area Network.

radvd Router Advertisement Daemon.

RTT Round Trip Time.

SPI Serial Peripheral Interface.

TCP Transmission Control Protocol.

TFTP Trivial File Transfer Protocol.

UDP User Datagram Protocol.

Chapter 1

Introduction

1.1 Motivation

This is a test in the introduction chapter.

1.2 Methodology

1.3 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 and technologies used, and why these were chosen over other alternatives.

2.1 Bluetooth Low Energy

Read this: <http://chapters.comsoc.org/vancouver/BTLER3.pdf>

BLE is a wireless technology for short range communication developed by the Bluetooth Special Interest Group [4]. The idea was to create a low energy single-hop network solution for Personal Area Networks (PANs). A major advantage of this is that Bluetooth 4.0 is already a well established technology in cell phones, laptops and several other devices, and BLE can use several similarities with this. The 6LoWPAN Working Group has recognized the importance of BLE in IoT [5].

The protocol stack of BLE has two main parts, the controller and the host. In the system used 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.

In the case of the network used in this thesis, 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

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 was proposed by Geoff Mulligan and the 6LoWPAN Working Group in [7]. In this paper the advantage of 6LoWPAN is explained as the easiest way to use standard protocols such as User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), glsdns and Trivial File Transfer Protocol (TFTP), since they can be used directly without the requirement of a translation mechanism. They are already adapted to run over IPv6.

In addition to this, the paper argues that 6LoWPAN was developed to be used in small sensor networks. Implementations can fit into 32Kb flash memory parts, which is smaller than Zigbee and Zensys (which are the two main comparisons made in the paper). It also uses an impressive header compression mechanism that allows the transmission of IPv6 packets in 4 bytes, much less than the standard 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). This means that a device can send only the required part of the stack header, and does not need to include header fields for networking and fragmentation [5].

6LoWPAN was therefore a natural tool to use in this project, in the IPv6 and BLE based network.

2.3 Raspberry Pi

Developed by Element 14, the Raspberry Pi has become a central tool for many people wanting to get started using microcomputers. This was therefore a natural starting point for us as well.

The Raspberry Pi 2 model B+ is the second generation of its kind, and its *ARMv7 processor* has approximately six times the performance of the predecessor [3]. With a USB Bluetooth dongle connected, it is quite simple to enable both 6LoWPAN and BLE, given that the right Unix kernel has been used in the Operating System (OS) of the Pi.

Later in this thesis, the processing power of the Pi compared to performing calculations in the end-points will be a central topic for discussion.

2.3.1 Ubuntu Mate

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.

2.4 nRF52

The nRF52 is developed by Nordic Semiconductor, and is being described as a family of highly flexible, multi-protocol system on chip.

[2]

Running at 64MHz it racks up impressive stats: EEMBC Coremark® score of 215 and 58 Coremark®/mA. Built in a cutting edge 55nm process technology the nRF52 Series is architected for todays need for speed, speed to carry out increasingly complex tasks in the shortest possible time and return to sleep, conserving precious battery power. Introducing a Cortex-M4F processor at its heart, it is the most capable Bluetooth Smart SoC on the market today. With a brand new multiprotocol radio architecture limits are pushed even further for Bluetooth Smart: A total link budget of 100dBm, -96dBm sensitivity, +4dBm output power and -42dBm selectivity, it is built to exist reliably and effectively in a busy 2.4GHz band. Couple this RF resilience with outstanding power consumption: 5.3mA at 0dBm TX output power and 5.4mA RX it is miserly with power when getting things done on-air.

Designed with wealth of digital and analog interfaces and peripherals, there's something to cover every design requirement. The demands of today's Bluetooth smart single chip designs are increasingly varied and complex, they can range from digital audio processing, to FFT/FIR and security algorithms, to driving device displays and UIs. Whatever the task, nRF52 series has it covered.

We've truly made low power easy. We haven't just just great datasheet numbers, but an automatic and adaptive power management system which combined with extensive EasyDMA and PPI makes the nRF52 Series positively frugal with power.

nRF52 Series brings NFC for the first time to a Bluetooth Smart SoC. The on-chip NFC-A tag allows developers to take advantage of NFC 'touch-to-pair' functionality in their designs.

Maintaining the total flexibility philosophy of the nRF51 Series, it is a flash device. With 512kB flash + 64kB RAM on chip, developers keep all the software

6 2. BACKGROUND

stack flexibility and Over-The-Air Device Firmware Upgrade (OTA-DFU) features they enjoyed with the nRF51 Series.

We understand that in the world of wearables, size really is everything, so we built a device that is the smallest Bluetooth Smart SoC to date measuring as small as 3.0 x 3.2mm (CSP). With an on-chip balun and a minimum of external components it has the smallest design footprint out there.

Tomorrow's Bluetooth Smart Solutions are going to ask a lot. The nRF52 Series delivers.

2.4.1 Softdevice

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 SPI, which makes it easy to connect to the nRF52.

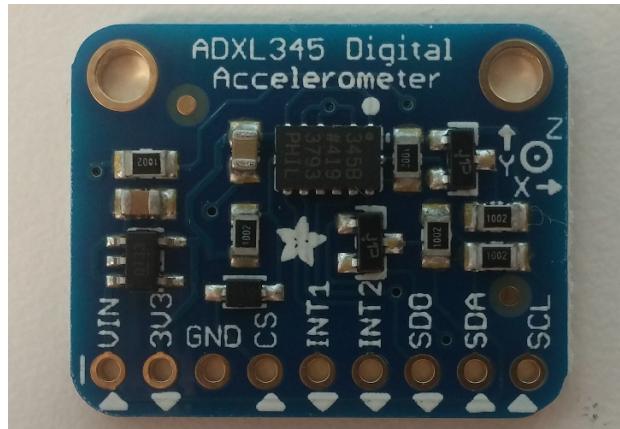


Figure 2.1: ADXL345 Accelerometer

2.6 Transport protocols

2.6.1 CoAP

CoAP is a transport protocol designed to be used in constrained networks for Machine-to-machine (M2M) communication. It is UDP based, and works good 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 notes 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 first transport protocol to test the network [8].

2.6.2 MQTT

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

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.

Chapter 3

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.

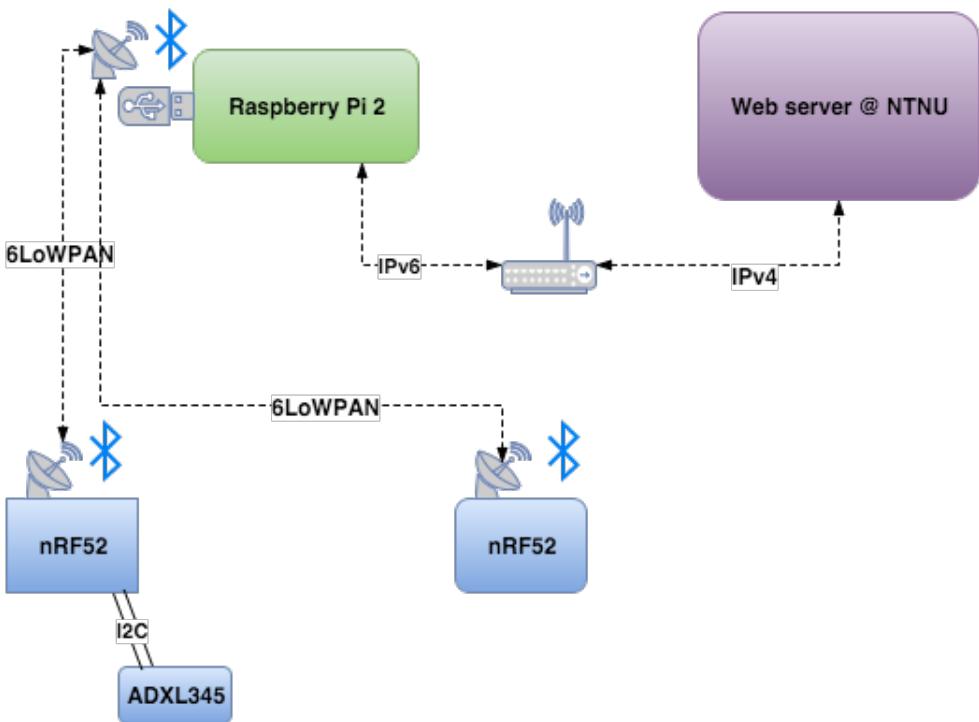


Figure 3.1: System architecture

There are two main limitations in a network such as this:

- Computational power in the different 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.

3.1 Connecting nRF52 and ADXL345

The ADXL345 Accelerometer used was connected using I2C, which is quite straight forward using the nRF52. Connection scheme is as follows (nRF52 -> ADXL345):

- 5V – VIN *Power source, green cable in Figure 3.2*
- GND – GND *Ground, red cable in Figure 3.2*
- P0.27 – SDA *I2C Serial Data Line, orange cable in Figure 3.2*
- P0.26 – SCL *I2C Serial Clock Line, brown cable in Figure 3.2*

After this is done it is possible to write to and read from the registers of the accelerometer over the two SDA and SCL cables.

The communication between the nRF52 in Figure 3.3 and the Raspberry Pi in Figure 3.4, is done using 6LoWPAN over BLE.

3.2 6LoWPAN and BLE

3.3 Connecting Raspberry Pi and nRF52

As a microcontroller the nRF52 works great, both as a low-power and powerful device.

To set up the communication between these two, the two code examples TWI and Observable server from Nordic Semiconductor was used as a starting point. It was

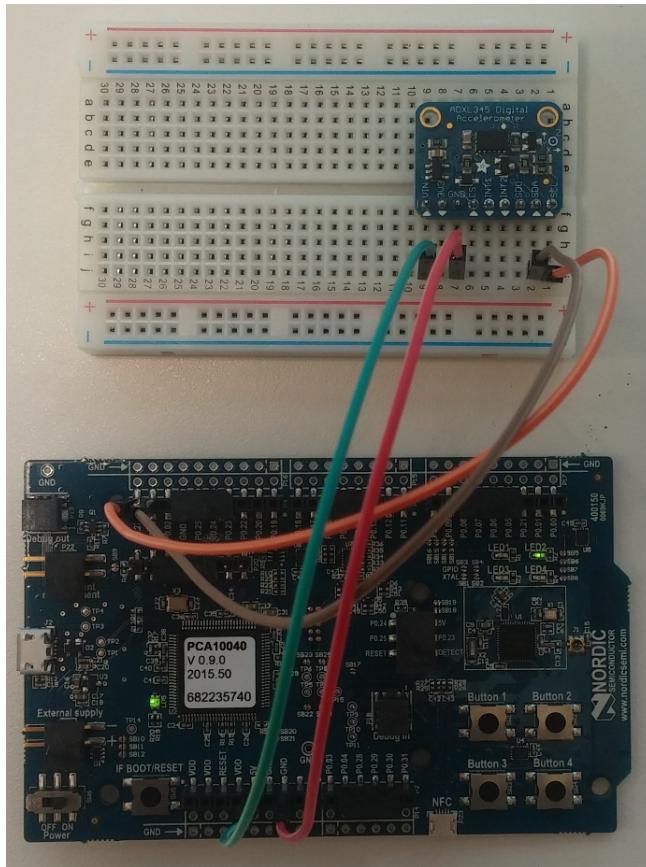


Figure 3.2: Connected nRF52 – ADXL345

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: Feb. 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*:

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

12 3. ARCHITECTURE

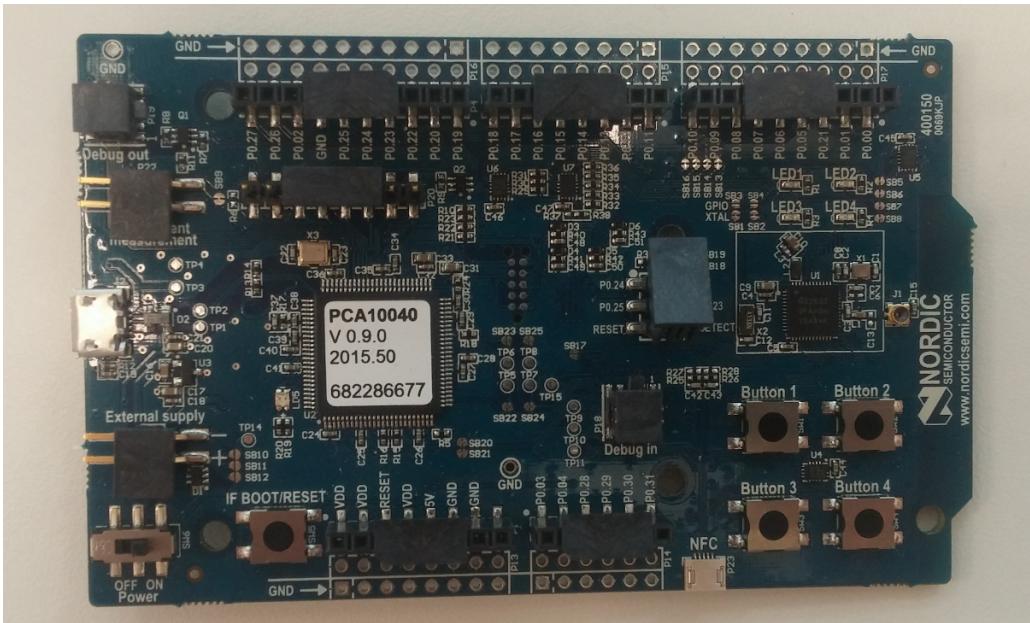


Figure 3.3: Nordic Semiconductor NRF52

To activate IPv6 forwarding, uncomment the following line in *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
```

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

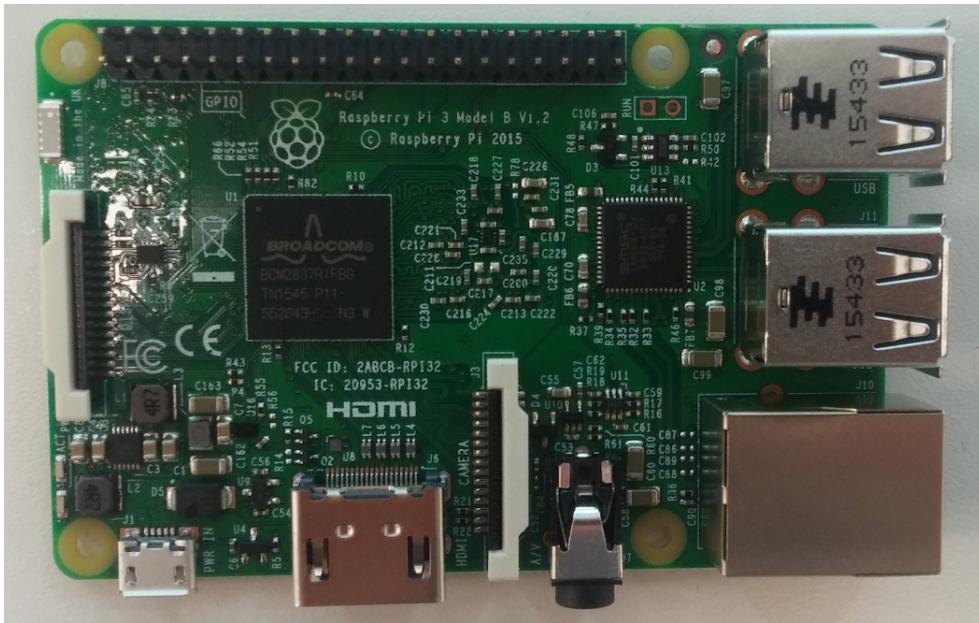


Figure 3.4: Raspberry Pi 3

```
        AdvRouterAddr on;  
    };  
};
```

To mount the modules *bluetooth_glowpan*, *glowpan* 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
```

As mentioned before, using the basic example of the observable server it was easy to send CoAP messages without the need of an Acknowledgement (ACK) for every message.

3.3.1 SPI

3.3.2 I2C

3.3.3 Problems

Chapter 4

Coding and Limitations

The general idea of the sensor network is to collect data from the accelerometer,

4.1 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.

4.1.1 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*.

Figure 4.4 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 4.4 shows, the code example for the CoAP client includes two different cases:

- In the fist 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 conformation 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

16 4. CODING AND LIMITATIONS

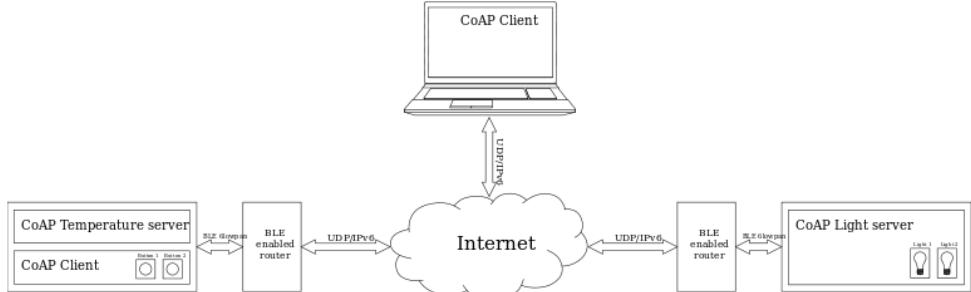


Figure 1: Setup of CoAP examples.

Figure 4.1: CoAP Client-Server communication example

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:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::21a:7dff:fed:7105	ff02::1	ICMPv6	104	Router Advertisement
2	11.649768800	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60969, GET, TKN:00 00 03 26, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
3	11.650000000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60970, GET, TKN:00 00 03 27, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
4	11.919029000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60970, GET, TKN:00 00 03 27, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
5	12.189768000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60970, GET, TKN:00 00 03 27, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
6	12.202143000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60970, GET, TKN:00 00 03 27, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
7	12.202143000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60970, GET, TKN:00 00 03 27, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
8	12.483022000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60972, GET, TKN:00 00 03 29, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
9	12.751765000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60972, GET, TKN:00 00 03 29, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
10	12.768017600	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60973, GET, TKN:00 00 03 29, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
11	13.054449000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60973, GET, TKN:00 00 03 29, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
12	13.054449000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60974, GET, TKN:00 00 03 29, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
13	13.309665000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60974, GET, TKN:00 00 03 29, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
14	13.319945000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60975, GET, TKN:00 00 03 29, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
15	13.319945000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60975, GET, TKN:00 00 03 29, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
16	13.598577000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60976, GET, TKN:00 00 03 2d, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
17	13.877217000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	72	ACK, MID:60976, 2.05 Content, TKN:00 00 03 2d
18	13.901700000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60977, GET, TKN:00 00 03 2e, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
19	14.042220000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	72	ACK, MID:60977, 2.05 Content, TKN:00 00 03 2e
20	14.167545000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60978, GET, TKN:00 00 03 2f, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
21	14.429804000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	72	ACK, MID:60978, 2.05 Content, TKN:00 00 03 2f
22	14.460300000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60979, GET, TKN:00 00 03 30, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
23	14.504460000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	72	ACK, MID:60979, 2.05 Content, TKN:00 00 03 30
24	14.718290000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60980, GET, TKN:00 00 03 31, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
25	14.718290000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	72	ACK, MID:60980, 2.05 Content, TKN:00 00 03 31
26	15.086011000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60981, GET, TKN:00 00 03 32, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
27	15.086011000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	72	ACK, MID:60981, 2.05 Content, TKN:00 00 03 32
28	15.282591000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	113	CON, MID:60982, GET, TKN:00 00 03 33, coap://[2001::2af:b7ff:feb6:1494]:5683/lights/led3
29	15.549782000	2001::1	2001::2af:b7ff:feb6:1494	CoAP	72	ACK, MID:60982, 2.05 Content, TKN:00 00 03 33

Figure 4.2: CoAP Client-Server example Wireshark capture

This gives us the sequence diagram shown in Figure 4.3.

This works fine, but in the case of the system built in this thesis there is no need to receive a confirmation for every single message. The system is meant to be used with tools for analysing, and it is not essential that data needs to get to its

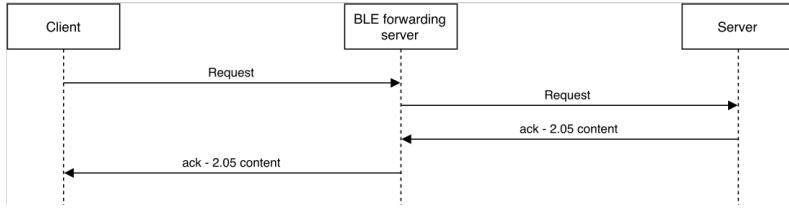


Figure 4.3: Sequence diagram CoAP Client-Server example

destination right away. It therefore makes sense to send messages in an *UDP fashion*, where packages are being sent right away without acknowledgement. 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 like an even better solution.

4.1.2 Observable CoAP

In the given Nordic example of a CoAP observable server, this problem can be resolved. It is here 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.



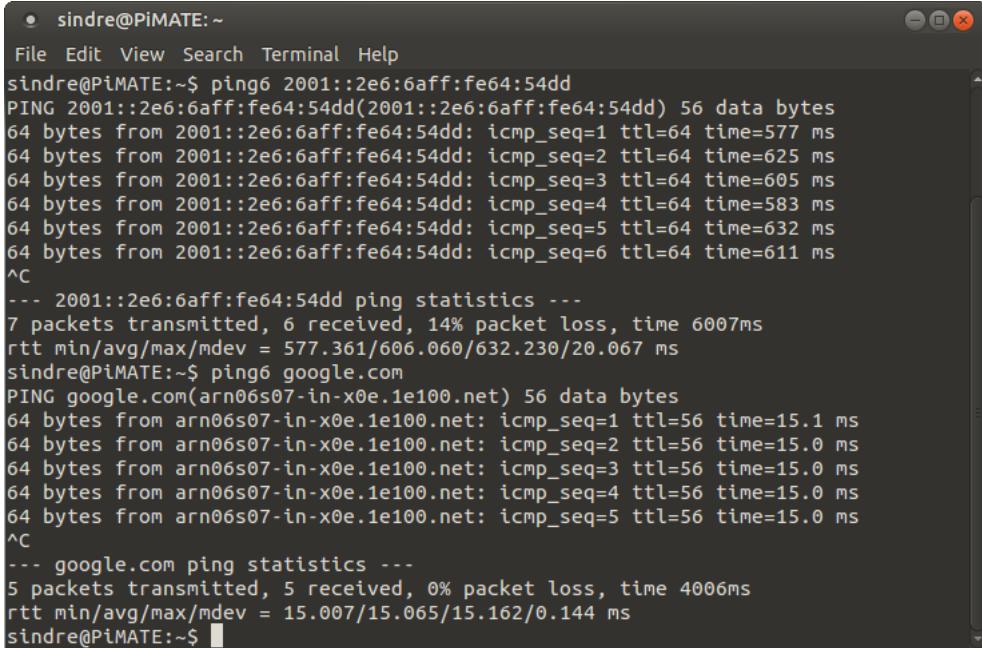
Figure 2: Setup of the CoAP client with Light server application.

Figure 4.4: CoAP Observable Server example

4.1.3 Stable transfer rate

When the observable CoAP is working fine, the next step is to determine the optimal transfer rate of the connection. Since the number of messages sent has been halved, it should be possible use this as an advantage. However, the link in itself is quite slow. The limitations in BLE and 6LoWPAN makes this much slower than a normal IPv6 connection, and the *ping* Round Trip Time (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 4.5. This is therefore a clear limitation of sending rate in the system.



```

• sindre@PiMATE: ~
File Edit View Search Terminal Help
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 4.5: Comparison: ping nRF52 and ping google.com

In addition, at tests, the connection turns out to be quite unstable at maximal transfer rate. Even in the test of ping shown in figure 4.5 the connection between the Raspberry Pi and the nRF52 had 14 % packet loss, 1 out of 7 packets. Other tests showed similar results, and that any sending rate much faster than once per second was more or less unstable when sending data. After a test period it was therefore decided that the best solution 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.

4.2 Getting acceleration values

As soon as the sending of values is being handled in a good way, the next step is to read acceleration values from the ADXL345 accelerometer, which is connected to the NRF52 using the I2C interface.

Acceleration values can only be read from the ADXL345 if this has been correctly initialized at compile time. In order to do this, code to write to and read from the registers had to be added. The initializing process is described in the accelerometer data sheet [1]. In short, registers for *data format control*, *initial power saving*, *interrupt enable control* and *the offset of each axis* has to be written to in that order before the acceleration value from the different axes can be read.

In the solution proposed in this thesis the acceleration values are being read as often as possible, limited by the processing power of the nRF52, and then stores in a simple dynamical char array before being sent and reset after one second.

4.3 Limitations

4.4 Measurements

Chapter 5 Measurements

This chapter will display the measured data from the accelerometer, and graphs, tables and figures to try to determine the most efficient solution.

5.1 temp/notes

Trying to understand the details of a capture in Wireshark.

Can fragmentation give us an advantage, if you can send more data per header.

An empty char array sent over CoAP is 76 bytes. 19 bytes char array, 96 bytes
21 bytes char array, 98 bytes. Adds only as much as needed.

5.2 Goodput vs throughput

5.3 Packet fragmentation

5.3.1 Train example

References

- [1] ADXL345:digital accelerometer data sheet. <http://www.analog.com/media/en/technical-documentation/data-sheets/ADXL345.pdf>. Accessed: 20-04-2016.
- [2] Nordic Semiconductor: nrf52 series soc. <https://www.nordicsemi.com/Products/nRF52-Series-SoC>. Accessed: 25-03-2016.
- [3] Raspberry Pi: raspberry pi 2 model b. <https://www.raspberrypi.org/products/raspberry-pi-2-model-b/>. Accessed: 27-03-2016.
- [4] 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.
- [5] Hui, J. W. and D. E. Culler (2008). Extending ip to low-power, wireless personal area networks. *Internet Computing, IEEE* 12(4), 37–45.
- [6] 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.
- [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).