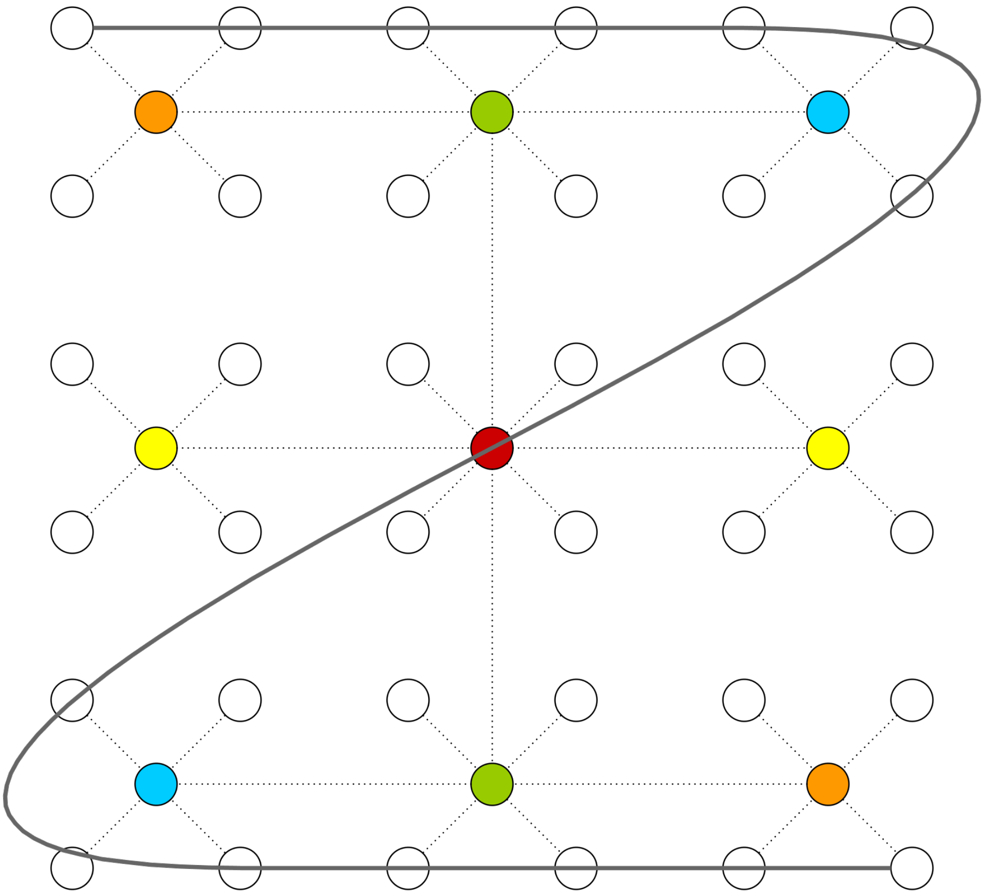
CHALMERS



Implementation of an instrument for analyzing IEEE 802.15.4 signals

Bachelor's thesis in Electrical and Electronic Engineering

TARIQ AL-TAHA

Department of Signals and Systems
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden 2016

BACHELOR'S THESIS

Implementation of an instrument for analyzing IEEE 802.15.4 signals

TARIQ AL-TAHA

Department of Signals and Systems
Division of Signal Processing and Biomedical Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY

Göteborg, Sweden 2016

Implementation of an instrument for analyzing IEEE 802.15.4 signals
TARIQ AL-TAHA

Examiner: Manne Stenberg - Chalmers University of Technology, department of Signals and Systems

Bachelor's thesis 201606
ISSN 1654-4676

Department of Signals and Systems
Division of Signal Processing and Biomedical Engineering
Chalmers University of Technology
SE-412 96 Göteborg
Sweden
Telephone: +46 (0)31-772 1000

Cover:
ZigBee Conceptual Nodes Network

Implementation of an instrument for analyzing IEEE 802.15.4 signals

TARIQ AL-TAHA
Department of Signals and Systems , Chalmers University of Technology

Bachelor's thesis

Abstract

Electrical energy meters have been undergoing technological development. One such development is in a field of digital communication where meters communicate wirelessly in order to forward their metering data to databases, an outstanding communication technology used for this purpose is known as ZigBee. This technology which is based on the IEEE 802.15.4 standard has been implemented widely due to its low-power, low-cost and effective mesh topology. However, this technology can experience communication loss between meters due to a number of factors such as: change in surroundings and radio-frequency interference. The purpose of this thesis is to design and implement an instrument that can detect signals transmitted by nodes in the network and then display decoded parameters of the signals in terms of source address, destination PAN-ID address, signal strength and respective operation channel. For this purpose, theoretical reading using a number of books and papers was done. In addition, theoretical background and technical skills acquired from Electrical and Electronic engineering were utilized. Existing electronics such as a Micro-Controller Unit (MCU), display and transceiver were used in the main design of the instrument. Simulation methods were used in order to evaluated the instrument's reliability in real-world communication scenarios. As a result an instrument that fulfills the requirements was constructed and evaluated.

Keywords: IEEE 802.15.4, ZigBee, MCU, Mesh topology, transceiver, PAN-ID

Sammanfattning

En teknisk utveckling för elmätare har gjorts i området digital kommunikation. Ett växande teknik känd som ZigBee möjliggör trådlös kommunikation mellan mätaren för att vidarebefordra mätningsdata till databaser. Denna teknik är baserat på IEEE 802.15.4 standaren som är känd för låg strömförbrukning, låg kostnad och effektiv meshtopologi. Dock kan denna teknik medföra förluster i kommunikationen mellan mätare på grund av ett antal faktorer såsom: radio interferens och förändringar i omgivningen. Syftet med detta kandidatarbete är att designa och implementera ett instrument som detekterar ZigBee signaler som sänds av mätare och sedan visa avkodad version av signalerna i form av källadress, destination PAN-ID adress, signalstyrka och respektive radiokanal. För denna anledning, läsning av teoretiska böcker har gjorts för att få djupare kunskaper om tekniken och standaren. Befintlig elektronik såsom Micro-Controller-Unit (MCU), skärm och transceiver användes i utformningen av instrumentet. Simulationsmetoder användes för att utvärdera instrumentets funktionalitet vid fältdrift. Som ett resultat av detta, ett instrument som fyller kraven konstruerades och prövades.

Nyckelord: IEEE 802.15.4, ZigBee, MCU, Mesh topology, transceiver, PAN-ID

Preface

This thesis report is written documenting a design of an instrument and aims to appeal to Electrical and Electronic engineers. This report is a part of my bachelor thesis that documents my work and illustrates to the reader the intuition I have obtained from my thesis. The report covers an introduction to ZigBee networking and digital communication fundamentals of the IEEE 802.15.4 standard in chapter 2. The report then explains the practical approach of implementing the instrument in terms of main electronic components as well as evaluation methods of the instrument in chapter 3. Results of the evaluation and implementation of the instrument are repsented in chapter 4.

Acknowledgements

I thank my supervisor at Göteborg Energi Sven Palmersjö for his continuous support throughout my work and introducing me to Göteborg Energi's ZigBee infrastructure. I thank Peter Berggren for handling formal arrangements in Göteborg Energi and aiding in project initiation. I would like to thank my supervisor at Chalmers University of Technology Göran Hult för helping in technical planning, choice of electronic components and academic documents. I thank Ali Salehson, Arto Heikkilä and Erik Ström at Chalmers University of Technology for their intuitive lectures in the field of digital communication. Finally I thank my examiner Manne Stenberg at Chalmers University of Technology for accepting my thesis and willingly examine my work.

List of Abbreviations

Abbreviation	Explanation
ACK	Acknowledgment
ADC	Analog-to-Digital Converter
APL	ZigBee's Application Layer
BPSK	Binary-PSK
CCA	Clear Channel Assessment
CSMA	Carrier Sense Multiple Access
CSMA-CA	CSMA-Collision Avoidance
CSMA-CD	CSMA-Collision Detection
CTS	Clear to Send
DSSS	Direct Sequence Spread Spectrum
ED	Energy Detection
EDA	Electronic Design Automation
FDMA	Frequency Division Multiple Access
GPIO	General-Purpose Input/Output
IC	Integrated Circuit
ISM	Industrial, Scientific and Medical
LQI	Link Quality Indication
MAC	Medium Access Control
MCU	Micro-Controller Unit
MHR	MAC header (MHR)
MIPS	Million Instructions Per Second
MLME	MAC Layer Management Entity
MPDU	MAC PDU
NWK	ZigBee's Network Layer
O-QPSK	Offset Quadrature Phase Shift Keying
OSI	Open Systems Interconnection
PAN	Personal Area Network
PAN-ID	Personal Area Network ID
PDU	Protocol Data Unit
PER	Packet Error Rate
PIB	PAN Information Base
PLME	PHY Layer Management Entity
PSK	Phase Shift Key
QPSK	Quadrature PSK
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
RTS	Request to Send
SDU	Service Data Unit
SPI	Serial Peripheral Interface
SRAM	Static Random-Access Memory
UI	User Interface
USB	Universal Serial Bus
WPAN	Wireless Personal Area Network
ZC	Zigbee Coordinator
ZD	Zigbee Device

Contents

1 Introduction

This chapter gives a short description, purpose and organization of the project.

1.1 Background

As the dependency on electricity is increasing, there is a need for measuring electricity consumption. As an electricity distribution company, it is essential to know how much electricity a subscriber consumes, therefore electricity meters are installed at subscribers' sites. Those meters have to send measurement data to the company's headquarters in order for the data to be associated to a subscriber and a bill to be issued.

Göteborg Energi is a company based in Gothenburg, Sweden that does distribute and sell electricity to Gothenburg's population. GE uses electronic meters at the subscribers' sites in order to collect sensor data. The meters communicate collaboratively and wirelessly using a low power communication technology known as Zigbee.

ZigBee technology is a result of a collaboration between global brands to create a united wireless communication technology that mainly target sensors and industrial automation. As a result a simple, low-cost, environment-friendly and easily expandable technology known as ZigBee was invented. ZigBee technology targets small devices, such as electricity meters and complex sensors which normally are found in commercial building and recently growing in households. Therefore ZigBee has become an essential technology for companies to be utilized on a large scale.

The problem that faces Göteborg Energi today is meters halt after a period of time following installations due to signal loss. According to Göteborg Energi the most common causes for signal loss are fences and buildings built around households that have ZigBee meters installed.

Due to Göteborg Energi wishes, the schematics and the program code of this project are kept confidential while providing sufficient explanation of the implementation.

1.2 Purpose

Since Zigbee devices collaborate wirelessly in order to forward data, they are dependent on radio frequency which is generally sensitive to noise. Zigbee is normally affected by interference with other wireless technologies which potentially degrades its performance. Occasionally, changes in the surroundings after installations of meters at consumers' sites cause wireless communication between meters to malfunction. GE normally detects malfunctioning meters by using significant amount of resources which the company believes unnecessary.

The purpose of this project is to design and construct a portable instrument that detects Zigbee signals that may exist in its radio range. The instrument should analyze each Zigbee signal and then respectively displays a few of many relative parameters (mentioned in section 1.3) to the user.

1.3 Aim

The aim of the instrument design is to provide a set of functions and an interface that helps a user to utilize those functions. The instrument's main functions should be aimed at providing the user with the following Zigbee's traffic parameters:

- A hexadecimal value of the Source address
- Destination Personal Area Network ID (PAN-ID) address
- Signal strength
- Respective radio channel of the traffic

Furthermore, auxiliary characteristics can be implemented in presence of time, those are as follows:

- Sleep mode
- Data logging
- Single handheld design
- Scrollable interface

The instrument is to be constructed using individual electronic existing components which together form a unit.

1.4 Methodology

In order to achieve the aim of this project, it had to be done in a method that consists of the following stages:

1.4.1 Problem clarification

Field visits in collaboration with Göteborg Energi (GE) were conducted in order to provide practical perspective of the problem, limitations and feasible solutions. The visits help also in highlighting the foundation of GE's Zigbee network infrastructure. Additionally, the company introduced their database software which aided in further understanding of their network infrastructure.

1.4.2 Literature

In order to broaden theoretical knowledge about this field of communication, different literature was studied through Chalmers library.

1.4.3 Software

In order to study real-time Zigbee traffic and confirm whether the designed instrument displays reliable results, a software known as "SmartRF Packet Sniffer" and a USB dongle transceiver from Texas Instruments (TI) were used. The software provides substantial amount of parameters including the main required communication traffic information mentioned in section 1.3. A CAD software known as QCAD was used to digitally draw and average the instrument before the practical construction. An Electronic Design Automation (EDA) tool known as EAGLE from Cadsoft, was used to help in drawing schematic of the instrument digitally. A serial communication software known as Putty was used to communicate with an electricity meter from Göteborg Energi.

1.4.4 Components

The designed of the instrument is based on electronic components which are required to form it. Therefore they were chosen with the aims of this project in mind. All components were ordered using the Internet by Göteborg Energi.

The rest of this thesis report is organized as follows. Chapter 2 will give in-depth theoretical knowledge that is needed in order to analyze and understand ZigBee networking. The fundamental communication standard IEEE 802.15.4 that define ZigBee's characteristics is also explained. Chapter 3 will explain how an instrument was designed and constructed using both engineering and gained theoretical skills. In addition, simulations methods which evaluate the instrument are also clarified. Chapter 4 views simulations results that were done on the implemented instrument.

2 Theoretical Background

2.1 ZigBee Technology

ZigBee technology operates in the radio frequency (RF) 2.4 GHz which is widely used by other technologies such as WiFi, Bluetooth, Microwave ovens and cordless phones. ZigBee can also operate in 915 MHz mainly in N.America and Australia or in 868 MHz in EU countries. ZigBee technology has 16 allocated radio channels in the Industrial, Scientific and Medical (ISM) band with center carrier frequency separated by 5 MHz [2]. Channels are numbered from 11 to 26. The center carrier frequency for a channel is calculated using:

$$f_c(MHz) = 2405 + 5(n - 11) \tag{2.1}$$

Where f_c is the centre frequency and n is the channel number.

Using equation 2.1 the first and last channel frequencies can be calculated by putting 11 and 26 respectively as n into the equation which results in center frequencies 2405 MHz and 2480 MHz respectively. Therefore the 16 channel frequencies are in the interval 2405 MHz -2480 MHz as shown in figure 2.1

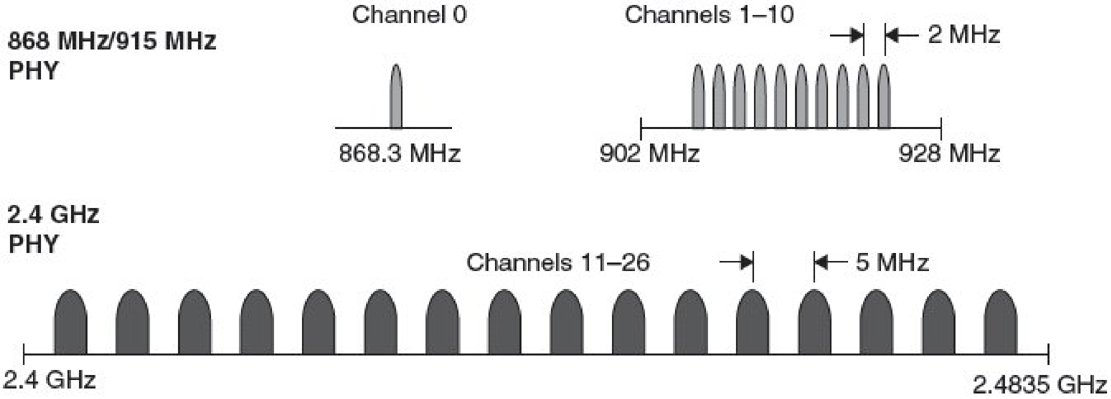


Figure 2.1: *ZigBee RF Channels in the different bands. reprinted from "Zigbee and Wifi RF Channels" by Fosiao LLC, 2014, Retrieved from "http://fosiao.com/content/zigbee-and-wifi-rf-channels". Copyright© 2009-2016 Fosiao LLC. All Rights Reserved. Reprinted with permission.*

Transmission of sensor data require very low data rate, in fact a data rate as low as 9.6 Kbps can be sufficient, however, a standard data rate of 250 Kbps is used for ZigBee in 2.4 GHz band which makes it a preferable band [2]. A higher data rate allows faster transmission of bits across a channel and thereby occupying less time in a channel, more details explained in section 2.5.

Nodes in a ZigBee network that participate in communication can either be a ZigBee Device (ZD) or a ZigBee Coordinator (ZC) and the latter normally initiates and maintains an area network known as Wireless Personal Area Network (WPAN). Normally a WPAN require only one ZC and can support up to thousands of devices [20]. Every Personal Area Network (PAN) is created by a ZC and given a unique address known as Personal Area Network ID (PAN-ID) which is used as a label for ZigBee networks. ZD nodes mostly act as sensors that collect local information such as metering data and then attempt to transmit that data to its PAN's ZC, this type of network is known as Wireless Sensor Network (WSN). Therefore a ZC is the bottleneck of its PAN where collected information is forwarded to external destinations such as the Internet to be utilized and stored.

Although ZigBee is classified as a short-range communication technology, ZigBee networks can stretch in radius by utilizing one of its characteristics which is mesh topology that is based on providing a route to ZC even if it is not within range of the sender. Therefore it is not required to increase the number of ZCs in order broaden a WPAN. Instead ZigBee sensors send data to neighboring sensors that have a route to PAN's ZC. To illustrate mesh topology further, figure 2.2 shows sensor A attempting to communicate with its PAN coordinator ZC which is not within range. Therefore A forwards its sensor data to neighboring sensor ZD (next to A) and it in turn will forward the data to either sensor B or any other arbitrary sensor (ZD) that has a path to ZC. By default the sensor that is forwarding data to a ZC is known as next hop. In reality, there may exist hundreds hops between source ZD and its PAN's ZC, that mainly depends on the infrastructure. In [20], it was noted that many environments have ZD devices that are close in distance (dense) and can route each other's messages.

Taking figure 2.2 into account, suppose that nodes have largely increased in numbers and they could directly reach the ZC in one single hop, then all ZDs can communicate directly with ZC which alters the topology to star topology, as shown in figure 2.3. More transmit power will be required in order to reach ZC resulting in high power consumption. Star topology can potentially create substantial amount of traffic collisions at the ZC due to the hidden terminal problem [14]. More on hidden terminal problem is covered in section 2.5.

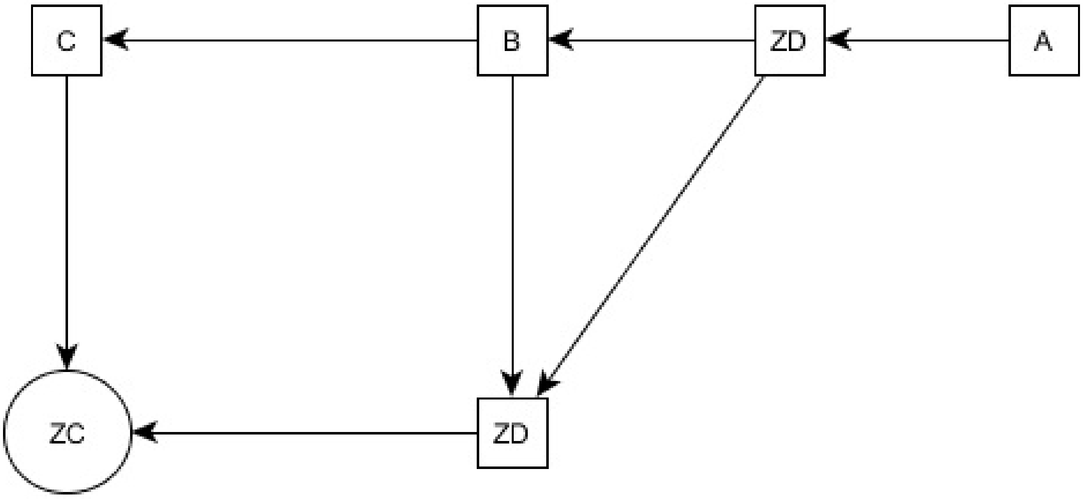


Figure 2.2: *Mesh Topology in ZigBee networks*

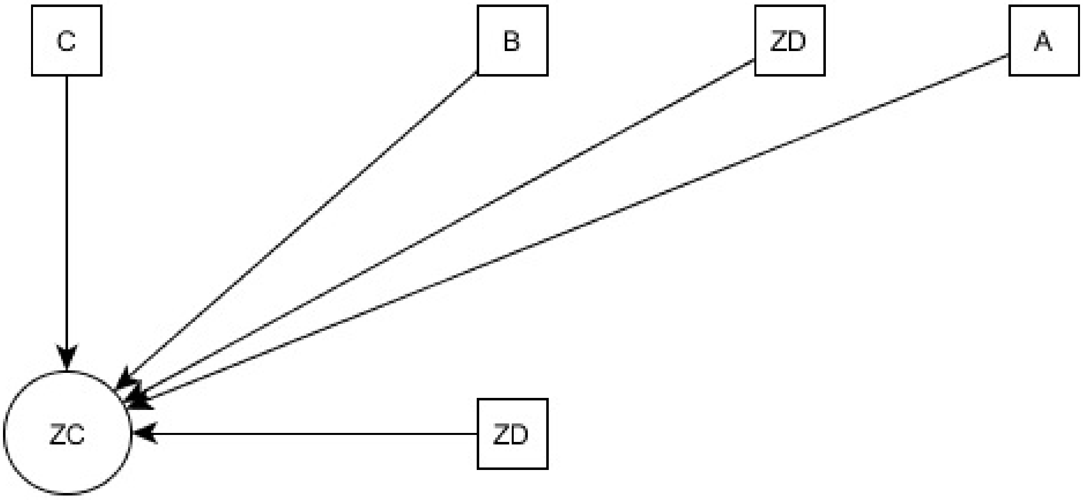


Figure 2.3: *Star Topology in ZigBee networks*

Traffic in ZigBee operate in two modes: beacon mode and non-beacon mode. The beacon mode lowers energy consumption and it does that by allowing all nodes and ZC to go into sleep-mode saving energy. The ZC periodically wakes up and polls (ask) nodes for any available messages. In the non-beacon mode nodes can go into sleep-mode when transmission is done, however, to prevent messages from being missed the ZC never switches to sleep-mode. The difference in energy consumption can be significant, according to [15] where 100 devices per home in a city that consists of 50000 homes that use ZigBee devices were studied. In the non-beacon mode where the Rx power is 30 mW, the total power consumption is 150 kW, whereas a much lower power consumption of 150 W was achieved in beacon mode due to a 1% duty cycle.

2.2 Radio Frequency

Radio signals tend to be affected by degrading factors, such as path loss, penetration and scattering in real-world scenarios. In addition the signal power tend to decrease by distance, the signal power P_d at distance d in free space can be calculated [3] using equation 2.2.

$$P_d(dBm) = P_0 - 10 \cdot 2 \cdot log_{10}(f) - 10 \cdot 2 \cdot log_{10}(d) + 27.56 \tag{2.2}$$

Where P_0 is the signal power in dBm at zero distance from the antenna, f is the signal frequency in MHz and d is the distance in meters from the antenna. Using equation 2.2 a signal power at a distance of 15 m from antenna and a frequency f of 2410 MHz can be calculated and results in approximately -60 dBm. In comparison to a different frequency f of 900 MHz and using the same parameters, a result of -51 dBm is acquired. The two previous examples show the relationship between frequency, distance and signal power.

The signal wavelength (λ) which is the distance in meters that a wave travels in one signal period (T) can be calculated [3] using equation 2.3.

$$\lambda = c \cdot T \iff \frac{c}{f} \tag{2.3}$$

where c is equal is $3 \cdot 10^8$ m/s (speed of light).

Signals can also be subjected to scattering upon hitting rough surfaces. According to [10], with variations more than $\frac{\lambda}{8}$ the roughness will cause the signals to scatter. Typically that happens upon signals coming in contact with trees.

As presented in [3] and from equation 2.2, we can assume transmitter A and receiver B and then calculate estimated range (R) in meters related with two wireless nodes. In order to calculate the range R, equation 2.4 is used.

$$R = 10^{\frac{P_0 - F_m - P_r - 10 \cdot n \cdot log_{10}(f) + 30 \cdot n - 32.44}{10 \cdot n}} \tag{2.4}$$

Where P_r is receiver's sensitivity in dBm, n is path-loss exponent (1.6 to 1.8 for a line of sight environment), F_m is the fade margin (found experimentally, 8 dB for a P_r of -95 dBm is recommended) in dB [3].

2.3 Communication Layers

In order to understand digital transmission from application data to radio waves, transmission of bits from user application to radio signals go through conceptual layers. The most common model is known as The Open Systems Interconnection (OSI) reference model and is divided into seven layers starting from Application layer in the top, down to the Physical layer in the bottom (see figure 2.4). Normally communication layers together are also called stack, such as ZigBee Protocol stack (covered in section 2.4).

Every layer has a specific task and it provides services to the layer above it, together all layers provide transmission of data such as sensor data. Normally the information is passed from above in a top-down manner. In general, every layer adds its overhead (specific information to respective layer) to the passed information from above also known as Service Data Unit (SDU). The combination of the overhead and the SDU results

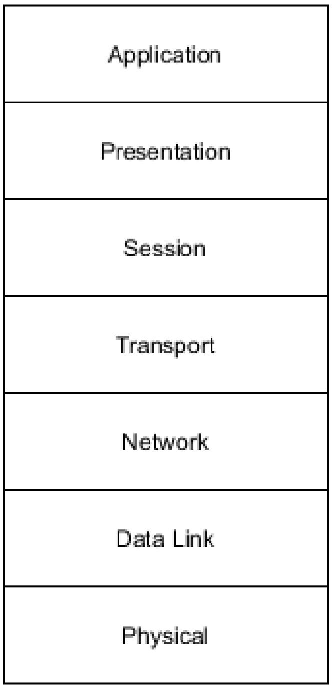


Figure 2.4: *OSI model's seven layers starting from the top with Application layer to Physical layer in the bottom*

in a Protocol Data Unit (PDU) for respective layer, for example at the MAC layer level a combination of a SDU and MAC's overhead results in MAC-PDU (MPDU). The physical layer handles transferring of bits over a communication channel, such as transferring information bits over radio or copper cables. The Data Link layer adds control and addressing information into its SDUs to form frames. The Data Link layer provides the use of broadcast messages, which are the type of messages that are sent to all nodes in a channel at once. An important sublayer of the Data Link layer is Medium Access Control (MAC) that handles the procedure of accessing a channel [11]. Very often the first three layers (Application, Presentation and Session) of the OSI model are summed up into one layer known as Application layer. More on MAC in ZigBee technology is covered in 2.5.

Each communication layer has a specific role, however, as a whole system those layers perform similarly. For example all layers have request, indication, response and confirmation functions [5]. Those layers are made to ease communication between stations, nonetheless, they communicate between each other in order to do so. Since the information is passed in top-down approach, any delay that occurs during the process is added to the transmission time. The effective rate R^0_{eff} for a layer can be calculated as shown in equation 2.5 with the assumption of an error-free transmission, in other words, no collisions or loss of data hence 0 in R^0_{eff} [16].

$$R^0_{eff} = \frac{n_f - n_o}{t_0} \tag{2.5}$$

Where n_f is the total frame length (bits), n_o is overhead length (bits) and t_0 is the total transmission time (seconds). In addition to effective rate of a layer, efficiency η^0 of a layer can also be calculated using equation 2.6 and often expressed in percent [16].

$$\eta^0 = \frac{R^0_{eff}}{R} \tag{2.6}$$

Where R is the protocol rate which is always determined by the lowest layer and is 250 kbps for ZigBee technology as mentioned in 2.1. For example, suppose a 120 bytes frame consisting of 20 bytes overhead is transmitted by MAC layer in approximately 3.4 ms using IEEE 802.15.4's standard 2.4 GHz operation R of

250 kbps. Using equation 2.5 and 2.6, an $R^0_{eff-MAC}$ of approximately 235 kbps and an efficiency η^0_{MAC} of 94% are obtained. In practical scenarios, it is rare to obtain an efficiency higher than 99%.

2.4 ZigBee Protocol Stack

ZigBee technology layers are partly based on the OSI model and consist of 4 layers. Two first top layers are ZigBee specific layers which are used for achieving functionality. Those layers add specific technology features, such as security and low-power. Those layers are known as ZigBee Application (APL) layer and ZigBee Network (NWK) layer and are shown in figure 2.5

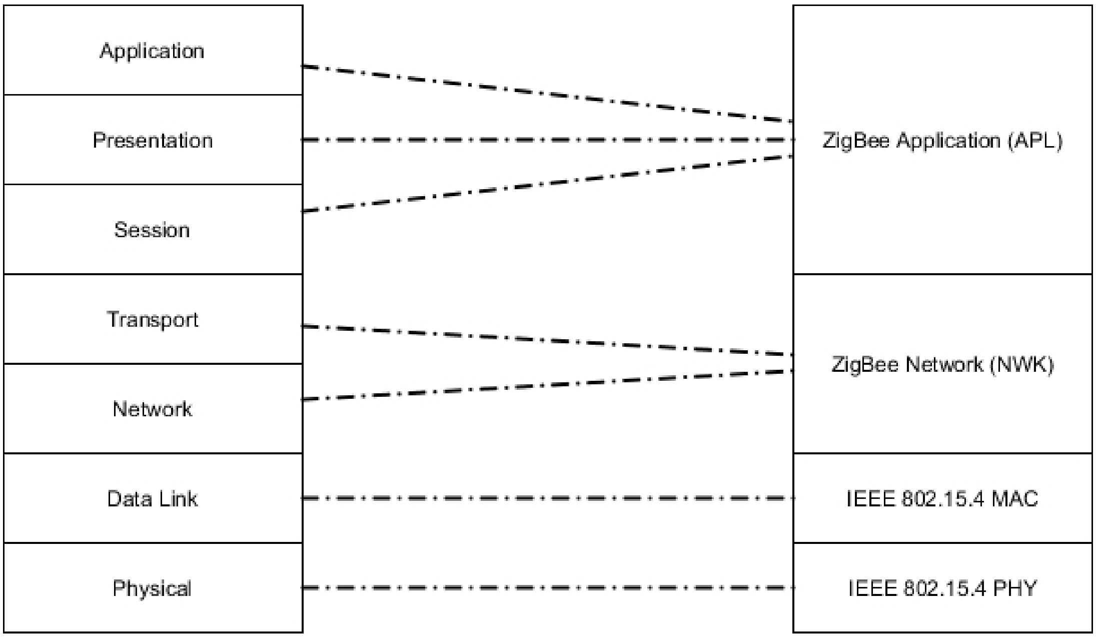


Figure 2.5: *OSI model (Left) in comparison with ZigBee protocol stack starting from APL to the IEEE 802.15.4 PHY in the bottom*

ZigBee's APL layer consists of Application Support Sub-layer (APS), ZigBee (ZDO) and eventually the manufacturer-defined application objects. The NWK layer adds support for network topologies, such as star and mesh topologies. The NWK layer provides crucial services such as forming networks, routing information and leasing logical addresses to nodes in a PAN, however, it always receives commands from the layer above (APL) [9]. Since ZC initiates PANs, it utilizes the mentioned services provided by NWK.

The last two bottom layers in the ZigBee protocol stack are defined by IEEE and standardized as IEEE 802.15.4. This IEEE standard is covered with more details in section 2.5.

2.5 IEEE 802.15.4

The IEEE 802.15.4 standard consists of two layers: MAC layer and PHY layer as shown in figure 2.5. This standard provides ZigBee technology with its prominent properties that make ZigBee technology preferable such as modulation, Carrier Sense Multiple Access (CSMA), PHY and MAC layers, coexistence and interference mitigation.

2.5.1 Modulation

IEEE 802.15.4 in the 2.4 GHz requires Offset Quadrature Phase Shift Keying (O-QPSK) [2]. Phase Shift Key (PSK) is based on embedding information in the phase of the signal such that every phase represents a discrete value. For instance, the simplest form of PSK is Binary-PSK (BPSK) which is based on modulating 0 and 1 for two discrete phases. Consider equation 2.7 where signal $s(t)$ and carrier frequency f_c, amplitude A and phase $\phi(t)$ are taken into account.

$$s(t) = A \cdot sin(2\pi f_c t + \phi(t)) \tag{2.7}$$

In PSK, A does not carry information and therefore makes PSK less susceptible to noise. In BPSK the value of $\phi(t)$ can be either 0° or 180° and represents a binary value of 0 or 1 respectively. The Quadrature PSK (QPSK) uses four phases: 45°, 135°, -45° and -135°. QPSK represent the four phases with two binary values: 00, 01, 10 and 11 respectively.

Since bits in QPSK are modulated in pairs, consecutive pairs of 00 and 11 could occur in the modulator. These two pairs require $\phi(t)$ to shift 180° (see table 2.1) which causes large amplitude variations that require complex modulator designs. O-QPSK on the other hand uses a time offset which limits $\phi(t)$ shift to a maximum of 90° [6]. Before modulation, groups of bits are converted to form symbols which are normally used to determine rates at a communication layer (often PHY layer) [18]. IEEE 802.15.4 groups each 4 bits into 1 symbol [6], for example in order to transmit 0101 a symbol S is transmitted. Since the data rate of IEEE 802.15.4 is 250 kbps which determines the rate of this technology as mentioned in 2.1, the symbol rate of IEEE 802.15.4 is 62500 symbol/s.

Angle (degrees)	Binary Value
45°	00
135°	01
-45°	10
-135°	11

Table 2.1: QPSK phases and their corresponding binary values

2.5.2 Carrier Sense Multiple Access

CSMA is a random multiple access method that is used to access a radio channel with the purpose of avoiding radio collisions. CSMA is based on Listen-before-talk methodology, stations sense the channel and then transmit if it is idle. However, if the channel is busy or a collision is detected then stations back off for a period of time. There are 3 different approaches that CSMA uses to access a channel [17]:

- Persistent: Sensing the channel and transmitting as soon as the channel is free
- non-persistent: Sensing the channel and then starting a random back-off timer until next sense
- p-persistent: A combination of persistent and non-persistent. The probability to transmit after sense is p.

One of the issues with wireless communication that is mentioned before in 2.1 is hidden terminal problem. This type of problems cause collisions at the receiving station when two transmitters use the channel simultaneously despite using CSMA. Suppose that station A and C are about to attempt to transmit to station B. A and C are not in range of each other, however, they are both in range of B. They both sense their respective medium using CSMA and find it to be free. Therefore they both start transmitting which results in a collision at station B [19]. Figure 2.6 illustrates the explained scenario.

CSMA handles collisions differently depending on type used: CSMA-Collision Avoidance (CSMA-CA) or CSMA-Collision Detection. CSMA-CD is based on sensing the channel and detecting if a collision is present, this type is mainly used in IEEE 802.2 (Ethernet, also known as CSMA-CD). However, in radio implementations it is extremely difficult to implement CSMA-CD and therefore only CSMA-CA is used. In CSMA-CA a coordinator helps in arranging time slots for stations for transmission. CSMA-CA uses short messages known as Request to Send (RTS) and Clear to Send (CTS) messages in order to arrange transmission. For instance, if a station A

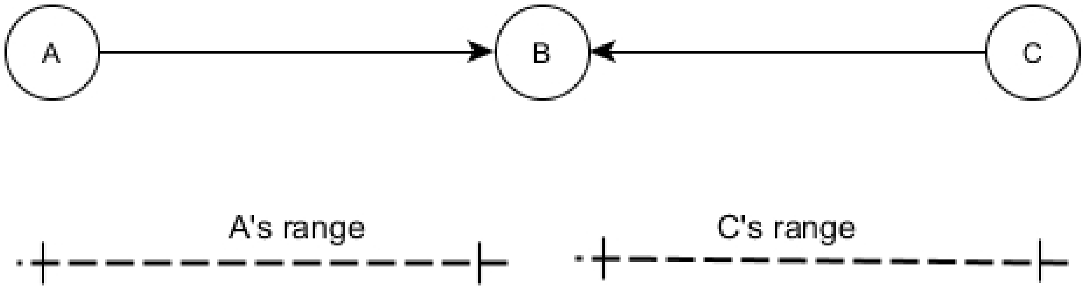


Figure 2.6: *Hidden terminal problem. A collision at station B due to A and C are not in range*

is willing to transmit, it sends a short RTS message to the coordinator and wait for a confirmation message (CTS). The coordinator then sends a CTS message informing all stations in listening range that station A is about to transmit and hence avoiding potential collisions at the coordinator and this in turn prevents the hidden terminal problem [19].

2.5.3 PHY and MAC layers

When data is about to be transmitted, it is sent through layers in top-down approach. When it arrives at the MAC layer, the MAC header (MHR) which contains transmission relevant information such as addressing fields is added to the SDU to form MAC-PDU (MPDU). Then a transmission request to PHY layer is made. Upon receiving data from radio, the PHY layer notifies the MAC layer about an available MPDU to be delivered. In addition, Link Quality Indication (LQI) information is delivered to MLME layer and accessible by higher layers (APL and NWK) determining the signal quality of last received MPDU [4].

The MAC layer has an entity that is responsible for managing MAC services and known as MAC Layer Management Entity (MLME). The PHY layer is located in the bottom of IEEE 802.15.4 standard, where information is prepared to transmitted as bits through a channel. The PHY Layer Management Entity (PLME) controls whether a transceiver is enabled or disabled. In addition channel management services are provided by PLME to the layer above (MAC layer) such as Clear Channel Assessment (CCA), Energy Detection (ED), data transmission and reception and selection of operational channel. The CCA service performed by PLME helps in providing access to the channel using CSMA-CA. The status (idle or busy) of the channel is then returned to the MLME and an action is taken by MAC layer depending on the status [5]. The PLME issues an ED process in order to estimate signal energy over eight symbol periods and a returned 8-bit integer value is returned to MLME and accessible by higher layers. The PLME has a database known as PHY-PAN Information Base (PIB) that stores operation parameters such as frequency channel of operation and transmit power in dBm [4]. However, PHY-PIB's parameters are only accessible by PLME and only given upon request by MLME [5]. IEEE 802.15.4 supports a mode known as Promiscuous that allows a node to capture all received frames that go through MAC and send them up to the higher layers even if they are not destined to that node. In addition, Promiscuous mode does not send ACKs back to the sender [8]. According to [4] the IEEE 802.15.4 requires receiver's sensitivity to be 10 dB above ED's detectable value. For example a receiver with sensitivity of -90 dBm must be able to perform ED and detect -80 dBm signals. Another requirement in the IEEE 802.15.4 standard is an ED value with the accuracy of ±6 dB or higher.

In radio communication, signal power attenuates the farther away a receiver is from a transmitter. According to [13], measurements were done to verify IEEE 802.15.4 parameters in outdoor environments. The measurements provided Received Signal Strength Indicator (RSSI) values (in dBm) in environments up to 70 m in distance between transmitter and receiver. The study focused on sending as little data as possible and low-power consumption to simulate real outdoor implementations of IEEE 802.15.4. Figure 2.7 depicts the results of the study, where the distance from the transmitter and RSSI values are shown.

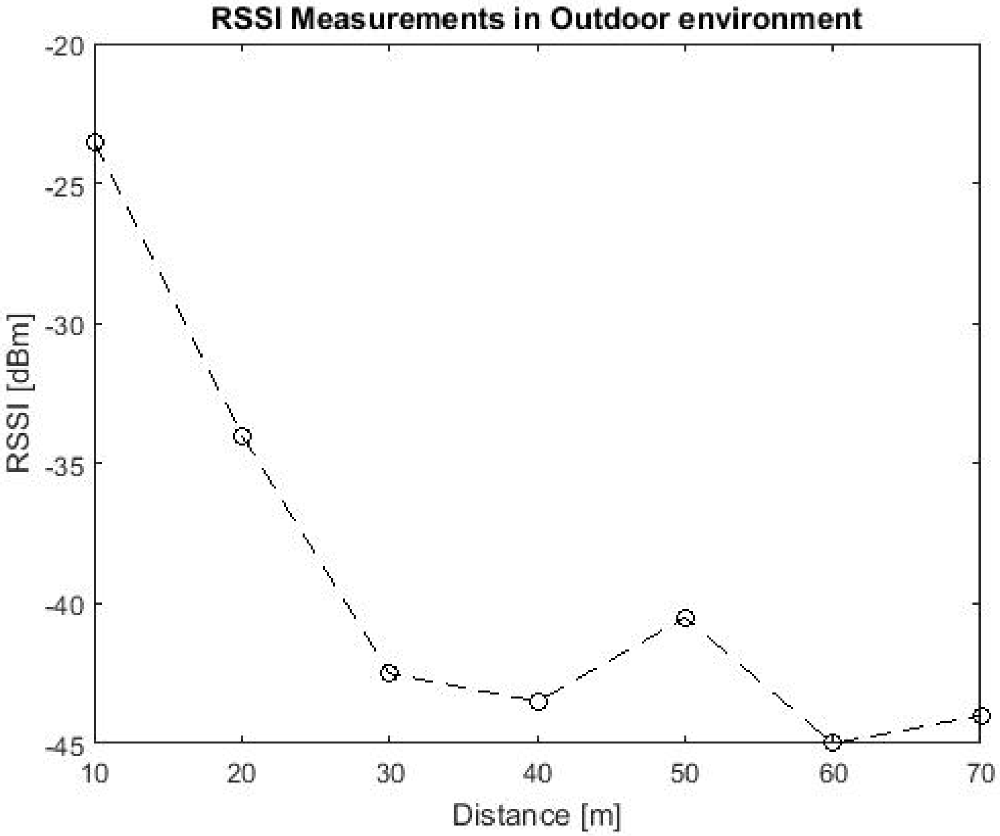


Figure 2.7: *RSSI measurements of a receiver along with the distance from the transmitter*

2.5.4 Coexistence and Interference

The IEEE 802.15.4 standard provides 16 non-overlapping channels as mentioned in section 2.1 by using Frequency Division Multiple Access (FDMA) to insure coexistence with other technologies. One of the provided methods by IEEE 802.15.4 to reduce collisions between two narrow-band signals in ISM spectrum is to use Direct Sequence Spread Spectrum (DSSS). This method is based on using a bandwidth that is greater in magnitude than the neighboring signals. By spreading the signal over a much larger bandwidth, the signal can then coexist together with narrow-band signals [20]. As mentioned in 2.5.3, CSMA is another characteristic of IEEE 802.15.4 that promotes fairness and thereby coexistence.

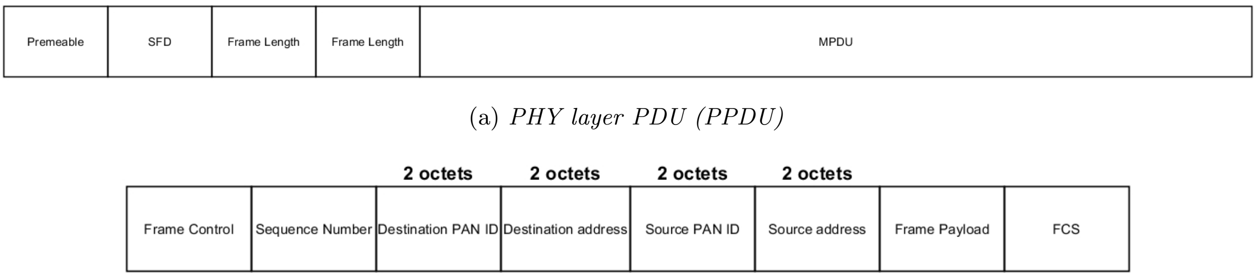
The IEEE 802.15.4 provided acknowledging communication, meaning that each device has a time window to send an acknowledgment (ACK) to the sender after it has received information. If the sender does not receive an ACK from the receiver within the time window, the sender assumes that the sent information was lost and it then attempts to send it again [20].

According to a test done by [20] on interference and everyday RF use of IEEE 802.15.4 along with ZigBee stack performed substantially well for none lost message when thousands were sent. However, the latency was affected in RF activity but in conclusion ZigBee devices proved effective even in presence of interference. On the other hand, according to a study [13] based on interference between IEEE 802.11 (Wi-Fi) and IEEE 802.15.4 in both indoor and outdoor environments. The study concluded that IEEE 802.15.4 has no negative impacts on IEEE 802.11, however, IEEE 802.15.4's transmission performance is negatively affected by IEEE 802.11 if operation channels are poorly chosen.

2.5.5 Protocol Data Unit

Both PHY and MAC layers create specific frame formats that contain relevant overhead respectively. Any PDU at layer n contains layer n's overhead and above layer's $(n+1)$ payload in other words information also known as layer n's SDU. PHY layer's PDU consists of MAC layer's payload (PSDU) and PHY layer's overhead that contains mainly medium relevant parameters such as Preamble, SFD, Frame length and reserved. The Preamble and SFD fields are used for synchronization, the Frame length parameter field contains the length in octets of the PSDU [7]. The structure of the PHY PDU is shown in figure 2.8a. The MAC layer PDU (MPDU) contains addressing fields that help in labeling traffic and identifying control parameters of the sender in a network. The MPDU consists of the following fields: Frame control, Sequence number, Destination PAN identifier, Destination address, Source PAN identifier, Source address, MAC layer's payload (MSDU) and FCS. The general frame format for MAC is also shown in figure 2.8b.

The Frame control and Sequence number fields are mainly used identify a frame's parameters such as: security mode, ACK state, addressing mode and frame type. Source and Destination addresses in IEEE 802.15.4 can be either in 16-bit or 64-bit. There are 3 main frame types: control, data and acknowledgement [8]. Data frames as the name implies have data as payload and ACK frames are sent back to sender to confirm reception of frames (often data frames). Control frames provide management of the network, such as beacon frames which are initiated by ZC and contain information that arrange transmission times among nodes in a PAN to achieve fairness in accessing a channel. The addressing fields indicate relevant parameters such as Destination PAN ID, Source address. The Destination PAN ID is a field of two octets that contains a unique PAN-ID. The Source address contains the address of which the frame had transmitted from and it is either 16-bits or 64-bits in length depending on the addressing mode [8]. The Destination address field contains either a 16-bit (2 octets) or a 64-bit address depending on the addressing mode, this address indicates to which station the frame is sent. Often a hexadecimal value of 0xFFFF is used in Destination Address field indicating a broadcast frame, on other words, a frame that is sent to all stations.



Premeable	SFD	Frame Length	Frame Length	MPDU

(a) *PHY layer PDU (PPDU)*

		2 octets	2 octets	2 octets	2 octets		
Frame Control	Sequence Number	Destination PAN ID	Destination address	Source PAN ID	Source address	Frame Payload	FCS

(b) *MAC layer PDU (MPDU)*

Figure 2.8: *PHY and MAC layers' PDUs*

3 Implementation

In order to fulfill the main requirements mentioned in section 1.3, an instrument had to be designed, a program had to be written and simulations had to be done. ZigBee technology faces a number of obstacles such as the ones mentioned in 2.5.4 that need to be overcome with the aid of this implementation. This implementation should detect all existing traffic signals in all 16 channels and then view the captured frames in terms of 16-bit source address, 16-bit destination PAN-ID, Signal strength of that frame and respective channel. In addition, the implementation aims to provide a low-power instrument that can last on battery power. This chapter explains the design and implementation of an instrument in details in section 3.1, a program along with algorithms in section 3.2 and real-world communication traffic simulation in section 3.3.

3.1 Instrument Design

The instrument was designed to consist of specific Integrated Circuits (IC) and existing components that together fulfill the requirements mentioned in 1.3. The instrument design was chosen to consist mainly of a transceiver, User Interface (UI) and Micro-Controller Unit (MCU). Additionally, a 5 Volts switching regulator, user-input buttons, a 3.7 V battery with a capacity of 4400 mAh and Universal Serial Bus (USB) battery-charging IC were used, however, those are not discussed in depth due to their little relevance in achieving implementation's aims.

The transceiver IC which consists of a transmitter and a receiver (hence the name) maintains radio communication such as: accessing a channel and setting frequency of operation, more details are covered in section 3.1.1. The UI consists of input-buttons and a display that collectively provide commands and response to and from the instrument, more details are covered in section 3.1.2. The MCU is the main core of the instrument design, it handles transceiver operation, user input, display, program execution and last but not least power management. More details on the operation of the MCU are covered in 3.1.3. Figure 3.1 shows a block diagram of the most relevant components included in the instrument design.

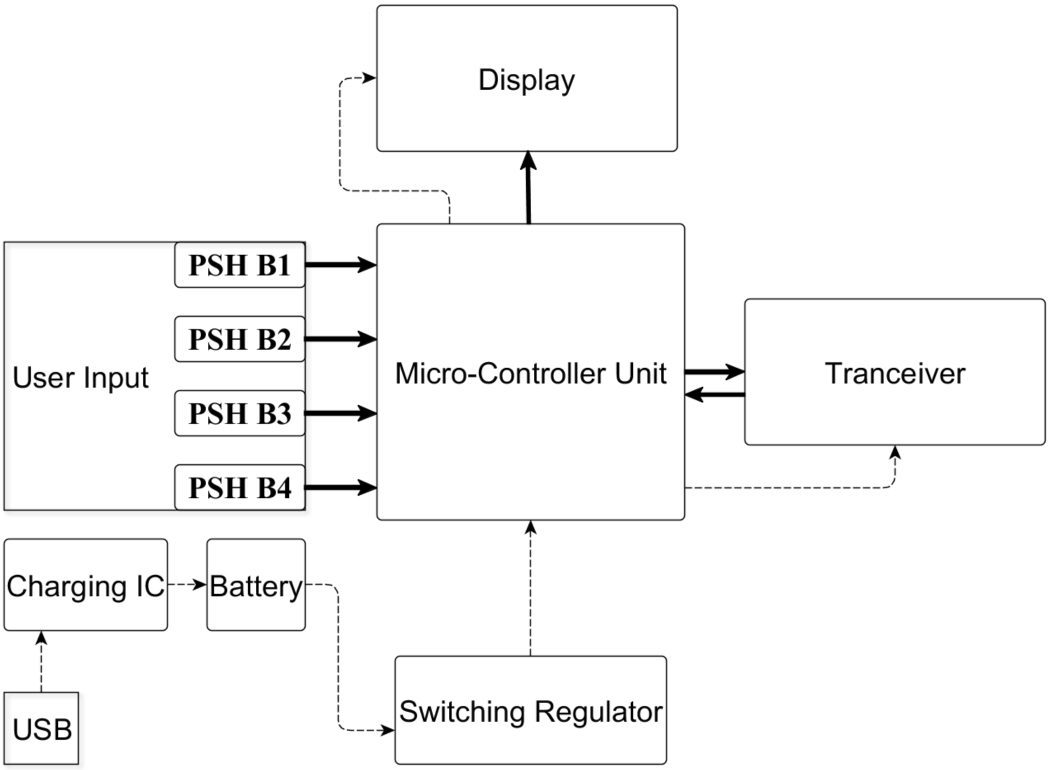


Figure 3.1: *Block diagram of ICs designed for the instrument. The dashed arrows represent analog power supply connections and the solid arrows represent digital connections.*

3.1.1 Transceiver

In order to design an instrument that is capable of operating in the IEEE 802.15.4's spectrum (2.4 GHz) and complies to the standard, an IEEE 802.15.4-compliant transceiver should be used. In addition, the transceiver should have a supply voltage within 3.3-5.0 Volts, communication interface and external antenna connection. An IEEE 802.15.4-compliant transceiver that fulfills the requirements known as AT86RF231 was chosen.

The AT86RF231 promotes low-power consumption, this IC draws 12.3 mA while listening to channel, in other words, in receiving mode (RX). The IC also provides a sleep mode that can be triggered using a General-Purpose Input/Output (GPIO) pin and draws as little as 0.02 μA. The supply voltage is in the interval 1.8-3.6 Volts. The transceiver supports a communication interface known as Serial Peripheral Interface (SPI) that communicates serially using 4 pins. The transceiver also has output pins for connecting an external RF front-end if operated in Extended mode, which can help in signal reception [12].

As seen in figure 3.1 the MCU was chosen to supply the transceiver with 3.3 volts which is within the operational voltage. The AT86RF231 transceiver has a receiver sensitivity of -101 dBm, in other words, the transceiver should be able to perform ED and detect a minimum of -91 dBm (see section 2.5.3). The transceiver supports IEEE 802.15.4 Promiscuous mode which allows capture of all in-going traffic regardless of destination (covered in 2.5.3). The transceiver consists of blocks, each with a specific purpose such as receiver's block, see figure 3.2 for a simplified block diagram of the receiver's circuit.

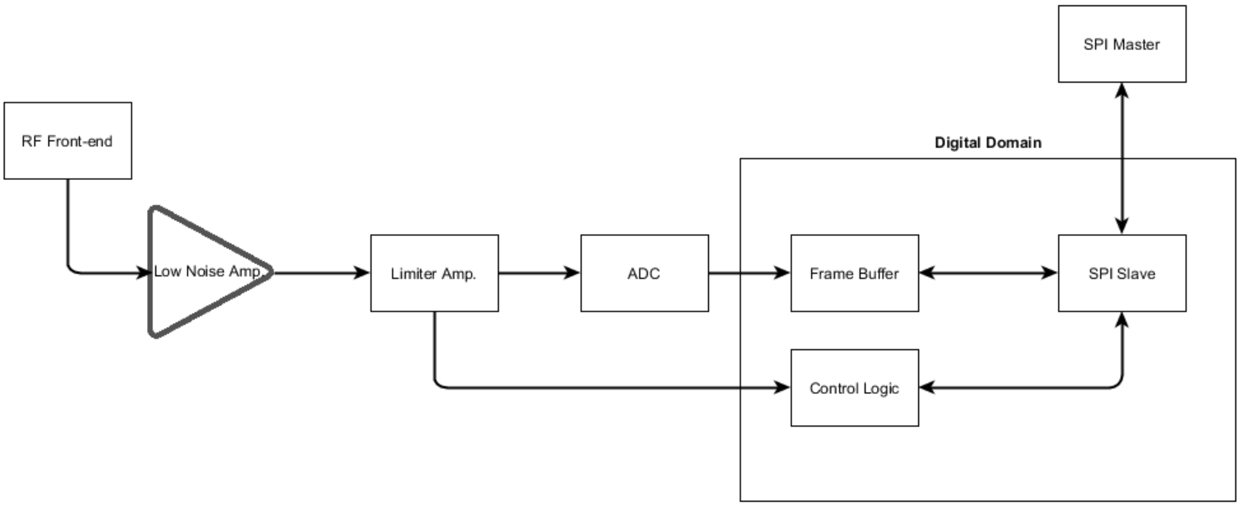


Figure 3.2: *Simplified block diagram of AT86RF231 (receiver's circuit)*

The received signal is amplified in the Low Noise Amplifier and then sent through the Limiter Amplifier to Analog-to-Digital Converter (ADC) as an analog value and a digital RSSI value of the received signal is sent to the control logic. The ADC's output is then sampled into data that is stored into a 128-byte RAM Frame Buffer. In SPI communication, the transceiver acts as a Slave in SPI communication and receives commands from the SPI master in this case the MCU. The SPI master is able to obtain the status of the transceiver's by reading transceiver's register values through Control Logic through which crucial register values can be read or altered such as operation channel, data rate, modulation and sleep mode. In RX mode the PHY listens for available frames, if frames are received they are demodulated and stored in Frame Buffer. Then the SPI master is notified about an available frame, the SPI master can then request the transceiver for the received frame stored in Frame Buffer including the overhead. The SPI communication is synchronous and a clock output provided by the SPI master. The SPI master can also request Control Logic for an ED value of the last received frame which helps determining the signal strength of that frame [12].

Since the transceiver operates in Extended Mode, reading RSSI values is not recommended, therefore ED measurement was chosen instead. The ED value is an averaged value of the RSSI over eight symbols or 32-bits (covered in section 2.5.1) and therefore more accurate value. The ED value is automatically updated upon frame reception and is in the interval 0 - 84 where 0 is lowest and 84 is the highest. The receiver input Power

P_{RF} can be calculated for ED values 0 - 84 using equation 3.1 and expressed in unit of dBm [12].

$$P_{RF}(dBm) = -91 + ED \tag{3.1}$$

For example an ED value of 50 corresponds to received signal power of -41 dBm (using 3.1). This relation is linear in the interval and can be depicted in figure 3.3.

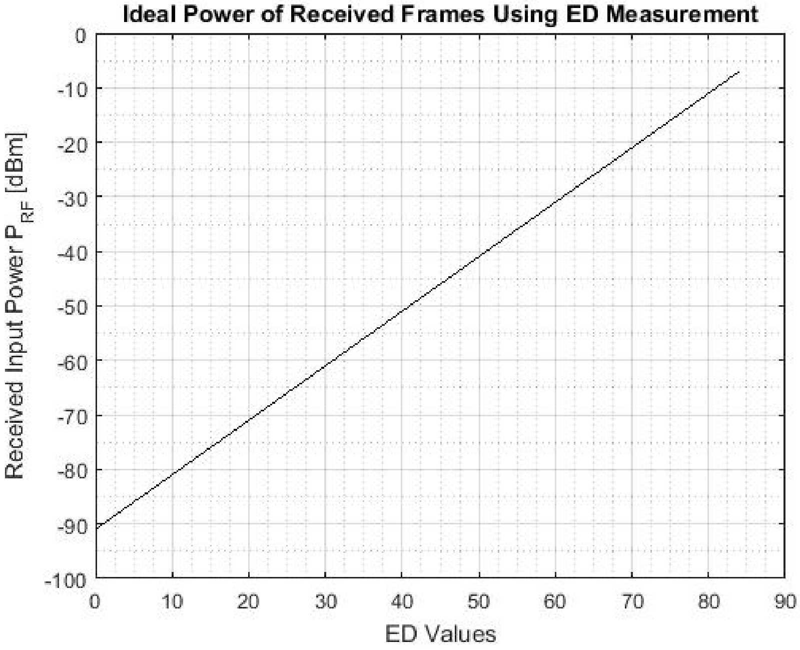


Figure 3.3: *Ideal Power of Received Frames Using ED Measurement (AT86RF231)*

The transceiver performs tasks at cost of time, for instance settling between channels requires 24 μs and ED measurement requires 140 μs. An approximate and confident time between channel switch was chosen to be 1 ms. For example a continuous channel switch between all 16 IEEE 802.15.4 will require 16 ms.

3.1.2 User Interface

In order to provide a communicative user interface, a display along with buttons were used. One commonly used display is Liquid Crystal Display (LCD) due to its simplicity and availability. LCDs are based on layers of molecules which together form blocks of pixels, each block represents a character. The size of the LCDs is expressed as $R \times C$, where R is the number of rows and C is the number of columns. The display should be able to be powered in relative voltages (3.3 - 5.0) Volts. Data is sent in parallel and controlled externally, for instance by a MCU.

The display that was chosen for this project is an LCD of the series JHD204A. The size of the display is 4×20, in other words 80 characters in total which is adequate for this implementation. The display uses a HD44780 controller which supports 4-bit or 8-bit parallel connections and connected using 4 or 8 pins respectively. The latter transfer more data simultaneously thus faster, however, the LCD display was chosen to operate in 4-bit operation to spare connection pins (more covered in section 3.1.3). In addition to data connections, two more control connections known as Enable (E) and Reset (RS) that control communication with the driver which results in a total of 6 connections. The display and its back-light both operate with a supply voltage of 5 Volts which is compatible with the implementation, the LCD back-light was controlled by the MCU. The response time of the display is not discussed nor has a substantial impact in this implementation.

Four buttons of type push-button were used to provide user input. The four buttons are shown in figure 3.1 and are designated as ”Back”, ”Up”, ”Down” and ”Select” respectively. The buttons are normally pulled up and are active low (more covered in section 3.1.3).

The User Interface was simply designed to ease navigation between menus. Using push buttons to provide scrolling with a pointer by using up and down buttons, selecting between sub-menus. The main menu consists of 2 sub-menus: Scan and Settings. Selecting Scan sub-menu performs a radio scan for a specified duration of time which is set in settings' sub-menu. After a full scan is performed, results are shown in terms of number of frames found and their corresponding channel as depicted in figure 3.4. Using this figure as an illustration, there were n_J frames found in channel J, a real-world example could be 30 frames (n_J) found in channel 11 (J). Since the display has 4 rows as mentioned above, each page displays 4 results at a time.

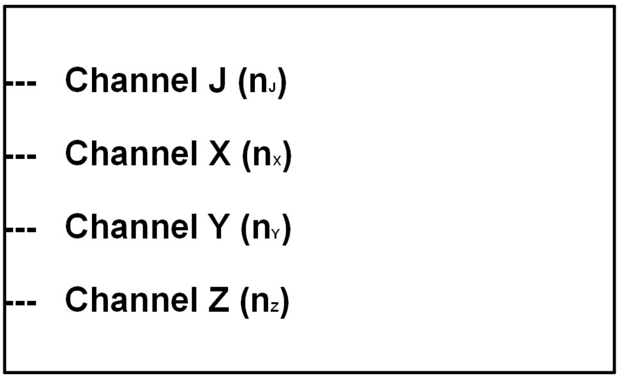


Figure 3.4: *Illustration of scan results after a performed scan shown on display*

Selecting a channel from the scan results displays numbered rows containing frames along with their specific parameters. Those parameters include: Source Address, Destination PAN-ID and ED's value. Due to limited characters per display row, the parameters were indicated using "S", "D" and "E" respectively. Figure 3.5 illustrate the concept of the design of this sub-menu with an example of a source address of 0xF298, a destination PAN-ID of 12345 and an ED value of 25. In addition the illustration shows the pointer in the first row to the left, line number, dots and spaces.

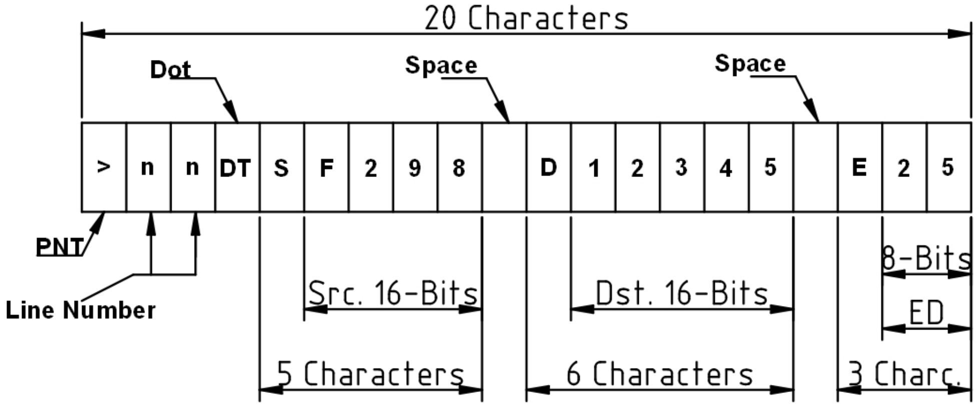


Figure 3.5: *Conceptual sub-menu of a channel's detected frames with Source Address ("S"), Destination PAN-ID ("D") and ED value ("E")*

Pressing Back button always returns the user output to previous sub-menu, such as returning to scan results from frames' sub-menu. The settings sub-menu has multiple status and configuration parameters that can be set by users depending on demands and situations. For example the battery voltage of the instrument is shown and the total (all channels) scanning duration can be set in the settings sub-menu as mentioned above.

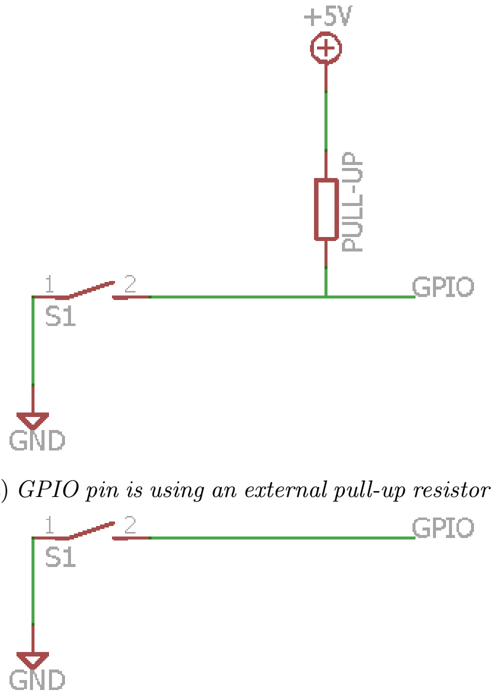
3.1.3 Micro-Controller Unit

The MCU provides essential operations of the transceiver, processing of user-input and power management. Therefore the MCU should provide SPI communication, has a sufficient number of GPIOs to accommodate 11

UI connections, 6 transceiver connections and an additional 2 connections for serial communication. Therefore at least 19 pins are required to be used as digital connections to the MCU. An 8-bit MCU with a 32 kBytes of flash program memory was chosen known as Atmega328P-PU. Finally the MCU should be programmed in C environment due to availability of code libraries and ease of implementation.

The Atmega328P-PU is a package with 28 pins, where GPIO 23 pins are reprogrammable and the rest handle power, external crystal oscillators and hard reset. The GPIO pins can acquire internal pull-up resistors if running as input pins with an extremely low sink current. The MCU has a 2 kBytes internal Static Random-Access Memory (SRAM) that helps in storing program variables and retrieve them quickly when needed, however, this type of memories only retains data while power is present. The MCU has two essential communication peripherals, SPI and Universal Asynchronous Receiver/Transmitter (UART). The SPI communication requires 4 pin connections and provides synchronous communication using a generated clock by the master (MCU). The MCU runs at a supply voltage range 1.8 - 5 Volts and draws approximately 8 mA in normal operation and supports up to 40 mA current through each GPIO pin. The MCU has an internal oscillator of 8 MHz which executes up to 8 Million Instructions Per Second (MIPS), in addition an external oscillator can be used to override the internal oscillator and achieve frequencies up to 20 MHz [1]. This MCU also supports program code written in C environment and using a boot-loader (program installed on the MCU), Arduino code libraries can be compiled and uploaded to the MCU using Arduino IDE.

The MCU was chosen to operate with the internal oscillator 8 MHz and resulted in an adequate speed for this application. During implementation, 22 pins were occupied including two UART pins used for debugging resulting in 1 unused pin for future development. The SPI bus was connected to the transceiver to provide communication and operation of transceiver (covered in section 3.1.1). The LCD back-light was powered and controlled by a GPIO pin. For debugging purposes, The UART interface was connected to a computer station in order to send real-time data from the MCU to detect program errors and understand program behavior such as changes in variable values. The MCU detects whether a UI button is pressed or not by studying respective GPIO's pin state which is one of two, High for 5 V and Low for 0 V. Using the internal pull-up resistors (mentioned above) made the circuit design more efficient by occupying internal resistors to save space on the circuit board. Figure 3.6b and figure 3.6a illustrates the difference between internal and external pull-up resistors respectively.



(a) *GPIO pin is using an external pull-up resistor*

(b) *GPIO pin utilizing internal pull-up resistor*

Figure 3.6: *Internal and External Pull-Up resistors*

3.2 Program

The MCU was programmed in C using open source libraries in order to interface with the transceiver and the LCD. The code was complied using Arduino IDE as mentioned above. The program was implemented with the following aims taken into account:

- Operating transceiver using SPI communication.
- Detect, analyze, extract relevant parameters (mentioned in section 1.3) through radio scanning.
- Receive user-input by reading user-buttons' state.
- Operating LCD driver in order to provide results and response to user.

The program used an open source library which is compatible with the transceiver. The library provided the essential functions such as: retrieval of received frame from Frame Buffer, set channel frequency and perform ED measurement. Although the library does provide the received frame from the Frame Buffer, it does not directly provide the parameters mentioned in section 1.3. Therefore the library was modified in order to analyze the frame and extract source address and destination PAN-ID address parameters. In order to initialize the transceiver, the data rate is set to 250 kbps and the MLME is requested to operate in Promiscuous mode. Since the instrument will only be listening to traffic and not transmit anything, no address was assigned to it. Setting the channel frequency is done by sending a request to the PHY layer through MLME which is done using a function included in the library that can take in values 11-26 (IEEE 802.15.4 channels).

In the scanning phase, the MCU starts by requesting PHY layer to set frequency to first channel (channel 11) and starts listening to channel for approximately 10 ms. If any frame is detected, the following procedure takes places orderly for each unique frame:

- Its source address and destination PAN-ID are extracted.
- PHY layer is requested to perform an ED measurement, a value in interval 0 - 84 is returned.
- The values above are stored in an array to respective channel.

If 10 ms passes, the MCU requests the PHY layer to set channel frequency to next (channel 12) through MLME. If all channels are scanned for 10 ms, the program starts over from the first channel, however, if the total scanning time has passed then the instrument views the results as illustrated in section 3.1.2. The program implements sleep-mode by turning off the LCD's back-light and transceiver's radio in order to reduce current consumption, however, not during scanning. In addition, the program constantly reads user-input button in order to navigate program accordingly. To illustrate further, figure 3.7 shows a flowchart of the scanning program.

The program also operates the LCD driver using a simple library that can write characters on the display. The characters are seen as text that help in formulating menus, provide operation feedback to the user and last but not least view scanning results. The program views a main-menu when the instrument is first powered on where the user can select to scan or view settings.

3.3 PAN Simulation

In order to evaluate the instrument, real-world ZigBee communication needed to be simulated. In order to do so, two different techniques were used:

- Using a transceiver to periodically transmit random data.
- Using a typical electricity meter of the company.

The above techniques are explained in more details in section 3.3.1 and 3.3.2 respectively.

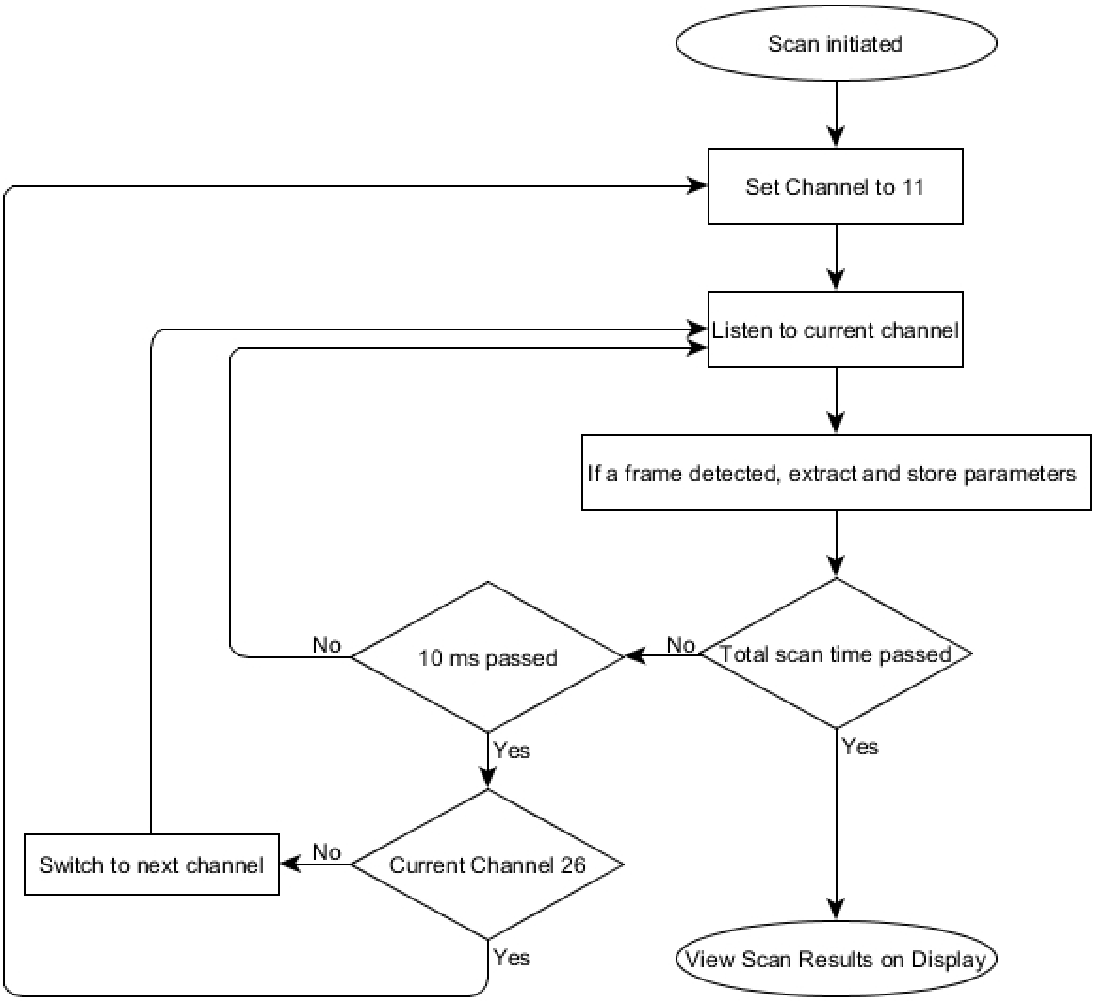


Figure 3.7: *Flowchart of the scanning program. The flowchart shows when the scan is initiated until the results are shown on the display*

3.3.1 Transceiver as a Periodic transmitter

A transceiver as the one mentioned in section 3.1.1 was used to periodically transmit data across all channels. The transceiver partially acts as a ZC by transmitting to 16 different meters each has an arbitrary defined short (16-bit) destination address and transmits on a different channel. The source address was chosen to be the same to ease implementation and debugging. For instance the transceiver sets operation channel to 11 and source address to 0xABCD by sending a request to PHY layer through MLME. Then the transceiver repeatedly sends a short message to 0x1111 for a short period of time before it switches to next channel (channel 12) in order to repeat the whole procedure. Table 3.1 shows the destination addresses that were used in respective channel.

3.3.2 A Typical Electricity Meter

Another simulation technique was used which involved connecting meters to a computer station in order to establish serial communication using a computer software known as Putty. This communication allowed a set of commands to be sent to the meter, in order to perform operations such as: reset, join and leave ZigBee network. The serial communication also provided meter operational parameters such as: meter address (16-bit) and operation channel. The meter joins a ZigBee network by searching for a ZC in order to associate with the company's ZigBee network. If a ZC is found, an address is leased to the meter and can be viewed using the

Channel	Destination Address (hexadecimal)	Source Address (hexadecimal)
11	1111	ABCD
12	2222	ABCD
13	3333	ABCD
14	4444	ABCD
15	5555	ABCD
16	6666	ABCD
17	7777	ABCD
18	8888	ABCD
19	9999	ABCD
20	AAAA	ABCD
21	BBBB	ABCD
22	CCCC	ABCD
23	DDDD	ABCD
24	EEEE	ABCD
25	FFFF	ABCD
26	A1B1	ABCD

Table 3.1: Transmitting scheme used in a transceiver to simulate real-world ZigBee PAN network

serial communication interface (Putty).

Evaluating the instrument was done using both techniques explained above. The scanning program in the instrument was then initiated to scan channels and view results. The results could then be compared to the ones of the two explained techniques above to confirm whether the instrument is reliable or not.

4 Results

Evaluating the instrument using the simulation techniques explained in section 3.3 was done. The results (shown in table 4.1) shows the captured serial data of the instrument using the technique explained in section 3.3.1. In addition the signal strength in terms of an ED value was stored in an array for respective frame.

Channel	Destination Address (hexadecimal)	Source Address (hexadecimal)
21	BBBB	ABCD
26	A1B1	ABCD
13	3333	ABCD
24	EEEE	ABCD
15	5555	ABCD
22	CCCC	ABCD
12	2222	ABCD
25	FFFF	ABCD
14	4444	ABCD
16	6666	ABCD
17	7777	ABCD
18	8888	ABCD
19	9999	ABCD
20	AAAA	ABCD
11	1111	ABCD
23	DDDD	ABCD
11	1110	ABCD

Table 4.1: Results of the captured frames' source and destination address with respective channel after a performed scan by the instrument. Results were obtained using a simulation technique that is explained in section 3.3.1

A low-power consumption sleep-mode was implemented (see section 3.1. In order to evaluate the efficiency of this mode, the current consumption of the instrument was measured. The results are shown in figure 4.1.

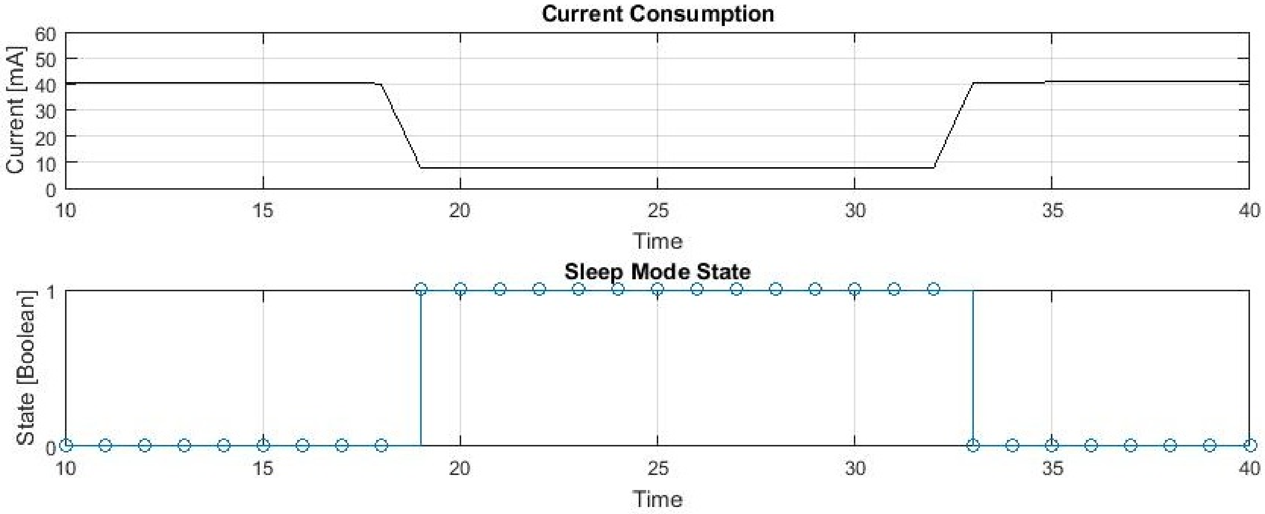


Figure 4.1: *Lowered current consumption at 5 V of the instrument by implementing sleep mode. Sleep-mode's state is shown in 1 or 0 indicating active or inactive respectively*

For instance, considering the current consumption of sleep-mode shown in figure 4.1 which can be approximated to 8 mA at 5 V. Using the battery capacity mentioned in section 3.1, the instrument can ideally run on sleep mode for approximately 360 hours or 15 days.

5 Conclusion

The aim of this thesis is to implement an instrument that fulfills the aims mentioned in 1.3. Through theoretical background and research, implementation and simulation an instrument was designed and constructed. It was evaluated both by simulations and in real-world communication scenarios and proved to be reliable. However, unreliable data were acquired from time to time during simulation (as shown in table 4.1) where 0x1110 was acquired instead of 0x1111. This type of errors was eliminated by increasing the scanning time period per channel to approximately 10 ms. In addition, The instrument have achieved extra functionalists such as sleep-mode that helped in saving substantial amount of battery energy which in turn provided an adequate standby time. In conclusion, the instrument can now aid in troubleshooting and tracing weak communication links between nodes in ZigBee networks while lasting for an adequate time of operation.

6 Discussion

Although the instrument achieved the aims, there are improvement that can be made. In a scenario where a substantial amount of traffic to be captured and viewed, it becomes rather difficult to scroll up or down to find a specific frame. For that reason, a logging feature can be added in order to log data on an external memory that can be used later to view data on a computer station. The instrument does not provide manual selection for channels to be scanned which is often is the case, instead, the instrument scans all ZigBee channels.

References

[1] *Atmel 8-Bit Microcontroller With 4/8/16/32KBytes In-System Programmable Flash.* Atmega328P-PU. Rev. 8271J. Atmel Corporation. Nov. 2015.

[2] S. Farahani. “ZigBee Wireless Networks and Transceivers”. Elsevier, 2008. Chap. 1.

[3] S. Farahani. “ZigBee Wireless Networks and Transceivers”. Elsevier, 2008, pp. 171–184.

[4] S. Farahani. “ZigBee Wireless Networks and Transceivers”. Elsevier, 2008, pp. 36–37.

[5] S. Farahani. “ZigBee Wireless Networks and Transceivers”. Elsevier, 2008, pp. 40–56.

[6] S. Farahani. “ZigBee Wireless Networks and Transceivers”. Elsevier, 2008, pp. 142–158.

[7] IEEE. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). *IEEE Std 802.15.4-2003* (2003), 43–44.

[8] IEEE. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). *IEEE Std 802.15.4-2003* (2003), 111–179.

[9] N. L. L. Pengfei L. Jiakun and W. Bo. “Research and Application of ZigBee Protocol Stack”. *Proc. IEEE International Conference on Measuring Technology and Mechatronics Automation.* Changsha City, Mar. 2010, pp. 1031–1032.

[10] W. C. Y. Lee. *Mobile Communications Engineering: Theory and Applications, Second Edition.* NY: McGraw-Hill, 1998.

[11] A. Leon-Garcia and I. Widjaja. “Communication Networks”. McGraw Hill, 2004, pp. 44–52.

[12] *Low Power 2.4 GHz Transceiver for ZigBee, IEEE 802.15.4, 6LoWPAN, RF4CE, SP100, WirelessHART, and ISM Applications.* AT86RF231. Rev. C. Atmel Corporation. Sept. 2009.

[13] P. M. M. Petrova J. Riihijarvi and S. Labella; “Performance Study of IEEE 802.15.4 Using Measurements and Simulations”. *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006.* Las Vegas, NV, Apr. 2006, pp. 487–492.

[14] A. Salehson. “The Link Layer and LANs, Lecture in Data Communication LEU061”. Chalmers University of Technology. Unpublished. 2015.

[15] *Setting Standards for Energy-Efficient Control Networks.* White Paper. Schneider Electric, June 2011.

[16] E. Ström. “Flow control; Framing; Multiple Access, Lectures in Communication Systems SSY305”. Dept. of Signals and Systems, Chalmers University of Technology. Unpublished. Feb. 2016.

[17] E. Ström. “Random access and Scheduled access, Lectures in Communication Systems SSY305”. Dept. of Signals and Systems, Chalmers University of Technology. Unpublished. Feb. 2016.

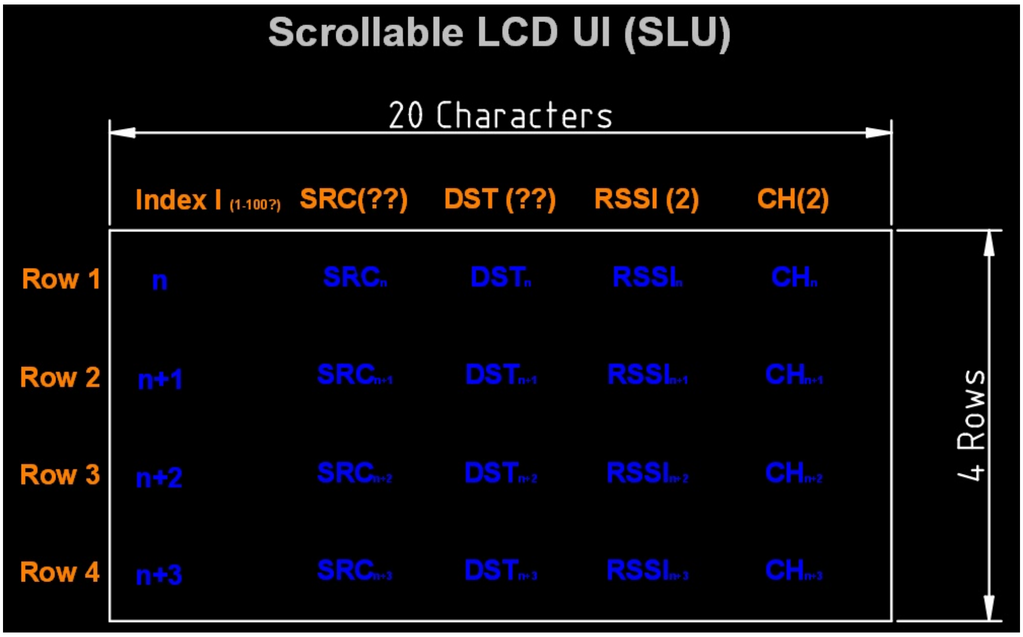
[18] E. Ström. “Shannon’s Model for Digital Communication and Modulation, Lectures in Communication Systems SSY305”. Dept. of Signals and Systems, Chalmers University of Technology. Unpublished. Feb. 2016.

[19] E. Ström. “WiFi, LAN bridges, Lectures in Communication Systems SSY305”. Dept. of Signals and Systems, Chalmers University of Technology. Unpublished. Mar. 2016.

[20] *ZigBee and Wireless Frequency Coexistence.* White Paper. ZigBee Alliance, June 2007.

Appendices

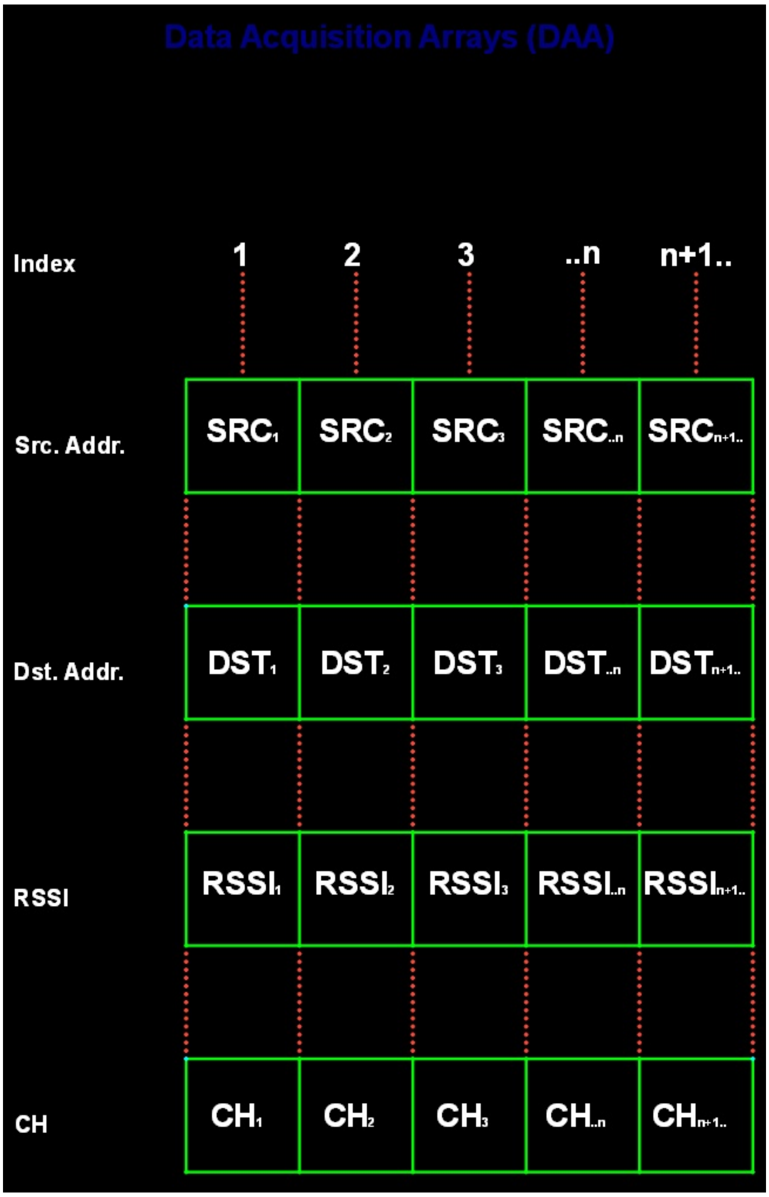
Conceptual Design of User Interface



	Index I (1-100?)	SRC(??)	DST (??)	RSSI (2)	CH(2)
Row 1	n	SRC_n	DST_n	$RSSI_n$	CH_n
Row 2	n+1	SRC_{n+1}	DST_{n+1}	$RSSI_{n+1}$	CH_{n+1}
Row 3	n+2	SRC_{n+2}	DST_{n+2}	$RSSI_{n+2}$	CH_{n+2}
Row 4	n+3	SRC_{n+3}	DST_{n+3}	$RSSI_{n+3}$	CH_{n+3}

Figure A.1: *Scrollable display pages - conceptual design*

Arrays that store captured frames' specific parameters

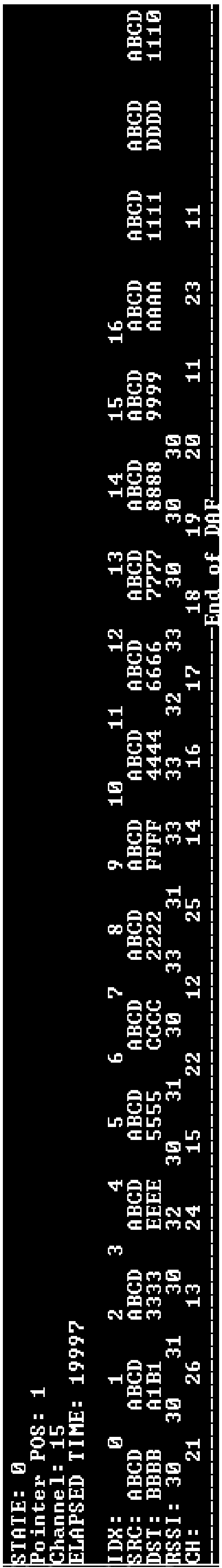


Data Acquisition Arrays (DAA)

Index	1	2	3	..n	n+1..
Src. Addr.	SRC_1	SRC_2	SRC_3	$\text{SRC}_{..n}$	$\text{SRC}_{n+1..}$
Dst. Addr.	DST_1	DST_2	DST_3	$\text{DST}_{..n}$	$\text{DST}_{n+1..}$
RSSI	RSSI_1	RSSI_2	RSSI_3	$\text{RSSI}_{..n}$	$\text{RSSI}_{n+1..}$
CH	CH_1	CH_2	CH_3	$\text{CH}_{..n}$	$\text{CH}_{n+1..}$

Figure B.2: *Arrays to store the required frame parameters*

Results acquired Using PAN Simulation Techniques

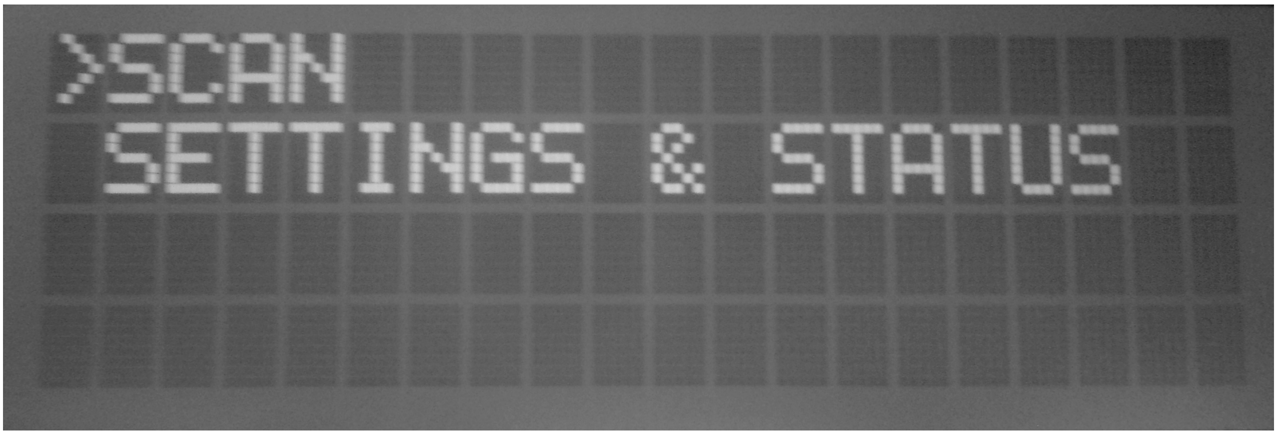


```
STATE: 0
Pointer POS: 1
Channel: 15
ELAPSED TIME: 19997

IDX:     0    1    2    3    4    5    6    7    8    9    10    11    12    13    14    15    16
SRC: ABCD   ABCD   ABCD   ABCD   ABCD   ABCD   ABCD   ABCD   ABCD   ABCD   ABCD   ABCD   ABCD   ABCD   ABCD   ABCD   ABCD
DST: BBBB   A1B1   3333   EEEE   5555   CCCC   2222   FFFF   4444   6666   7777   8888   9999   AAAA   1111   DDDD   1110
RSSI: 30   30   31   30   32   30   31   30   33   31   33   33   32   33   30   30   30
CH:     21    26    13    24    15    22    12    25    14    16    17    18    19    20    11    23    11
-------------------------------------------------------------------------End of DAF--------------------------------------
```

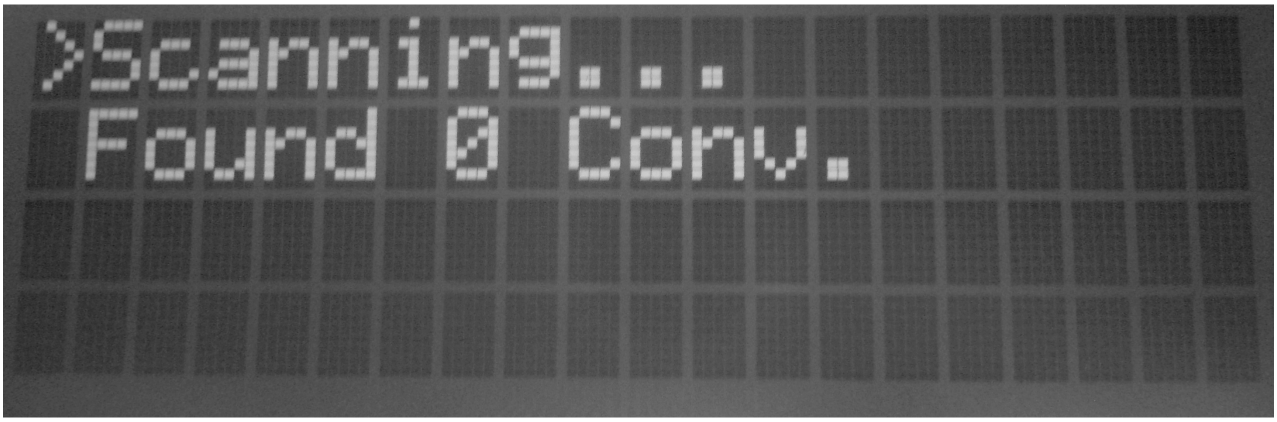
Figure C.3: *Results using transceiver as transmitter technique*

Physical screen showing the instrument in different states



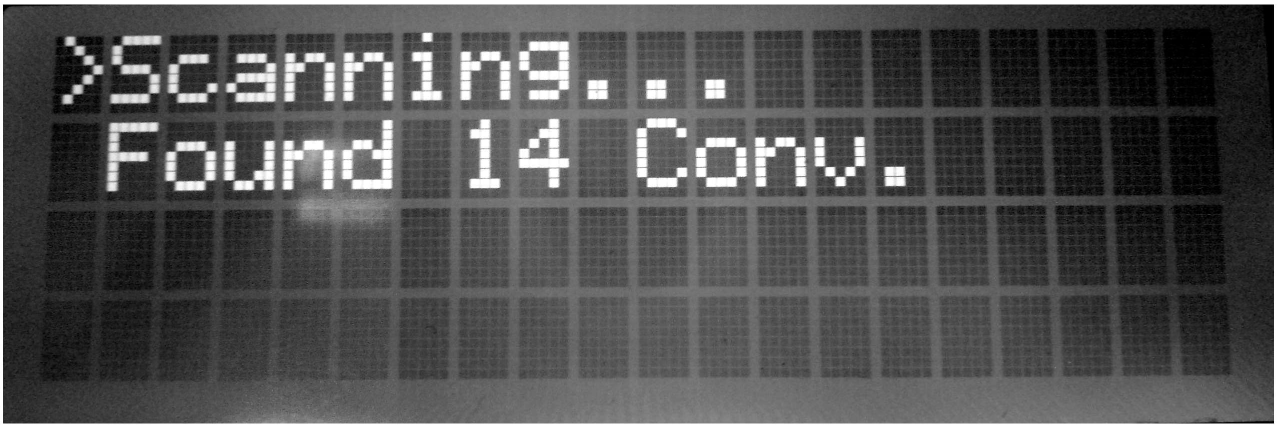
```
>SCAN
 SETTINGS & STATUS
```

Figure D.4: *Instrument's main-menu*



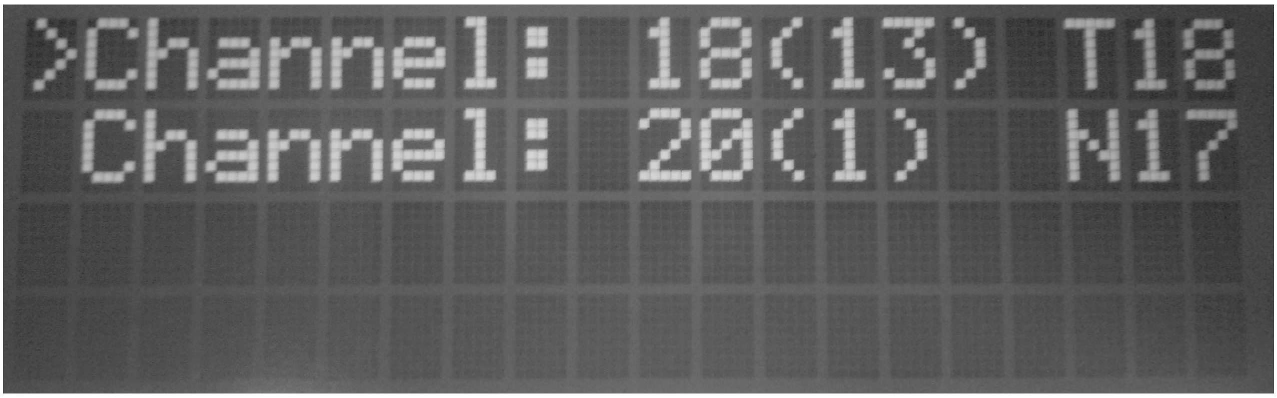
```
>Scanning...
 Found 0 Conv.
```

Figure D.5: *Instrument is scanning (no frames are found so far)*



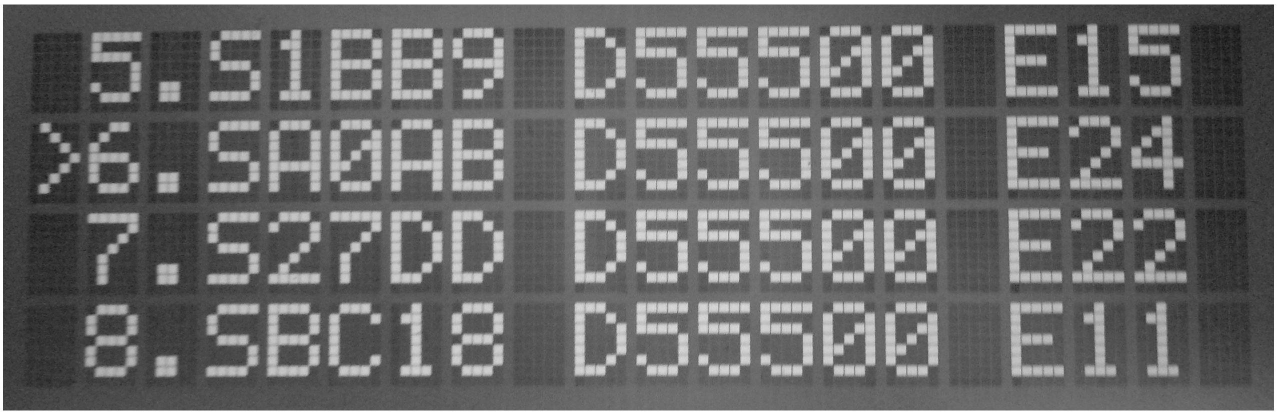
```
>Scanning...
 Found 14 Conv.
```

Figure D.6: *Instrument is scanning (14 frames are found so far)*



```
>Channel: 18(13) T18
 Channel: 20(1)  N17
```

Figure D.7: *Results of the scan in terms of channels*



```
 5.S1BB9 D55500 E15
>6.SA0AB D55500 E24
 7.S27DD D55500 E22
 8.SBC18 D55500 E11
```

Figure D.8: *Content of a channel in terms of frames. For instance conversation 5 seen in the figure has the source address 0x1BB9, destination PAN-ID 55500 and ED value of 15*