Tampere University

Jaakko Hautamäki

INDOOR POSITIONING AND ZIGBEE

A study of ZigBee technology and it's feasibility in indoor positioning

Faculty of information and communication technology
Bachelor's thesis
May 2019

TIIVISTELMÄ

Jaakko Hautamäki: Indoor positioning and ZigBee
Kandidaatintyö
Tampereen yliopisto
Tietokonetekniikka
Toukokuu 2019

Sisätilapaikannus, kotiautomaatio ja sensoriverkot yleistyvät nykyajan yhteiskunnassa. ZigBee on lyhyen matkan langaton verkkoteknologia, jota yleisesti käytetään juuri langattomissa sensori- ja kotiautomaatioverkoissa. Tämä työ pyrkii selvittämään onko ZigBee kykenevä sisätilapaikannukseen tehokkaalla tavalla.

ZigBee tukee mesh verkkotopologiaa ja sitä pidetään yleisesti toimintavarmana turvallisena teknologiana. ZigBee toteuttaa yleisesti signaalinvoimakkuusindikaattorin (received signal strength indicator) kaikille viesteille, jota voidaan käyttää paikannukseen useammalla eri algoritmilla. ZigBee laitteet lähettävät säännöllisesti radiomajakkasignaaleja (beacons) puu- ja tähtitopologiassa, Bluetooth low energy (BLE) - radiomajakkasignaalien tapaan. Tämä toiminnallisuus auttaa erityisesti radiosormenjälkipaikannuksessa (fingerprinting). Radiomajakkasignaaleja ei lähetetä ZigBee mesh -verkoissa.

Työssä saadaan selville että ZigBee on täysin kykenevä signaalinvoimakkuusindikaattoriin perustuvaan paikannukseen, kuten kaksi työssä käsiteltyä dokumentoitua ZigBee-paikannustoteutusta todistaa. Molemmat toteutukset käyttävät radiosormenjälkimetodia. Toinen paikannustoteutus saavuttaa 0.51 m paikannustarkkuuden testiympäristössään ja toinen toteutus todistaa että paikannustarkkuutta voidaan parantaa hyödyntämällä useampaa paikannusalgoritmia samanaikaisesti. ZigBee on myös pätevä teknologia tukemaan paikannusteknologioita, jotka vaativat toimiakseen langattomia sensoriverkkoja, kuten infrapuna ja ultraääni. Työssä käsitelty ultraäänellä toimiva dokumentoitu toteutus saavuttaa jopa senttimetriluokan paikannustarkkuuden.

ZigBeen tehonkulutus on hyvin lähellä BLE:n tehonkulutusta, toisin kuin WiFi:n, joka on huomattavasti ZigBee:n ja BLE:n kulutusta korkeampi. WiFi-paikannus hyödyntää yleensä valmista WiFi-arkkitehtuuria, joka on varsin kattava kaupunkialueilla. Tämä mahdollistaa lähes ilmaisen paikannuksen. ZigBee-kotiautomaatioverkot voisivat mahdollisesti toimia samalla tavoin. Teknologioiden keskinäiset kommunikaatioteknologiat kuten FreeBee, BlueBee ja LongBee voisivat myös huomattavasti parantaa WiFi:n BLE:n ja ZigBee:n välistä yhteiseloa ja suorituskykyä niin paikannuksessa kuin kommunikaatiossa.

TABLE OF CONTENTS

TIIVISTELMÄ....I

TABLE OF CONTENTS....II

ABBREVIATIONS....IV

1. INTRODUCTION....1

2. INDOOR POSITIONING....2

    2.1 Positioning algorithms....2

    2.2 Positioning technologies....4

        2.2.1 Wi-Fi....5

        2.2.2 Bluetooth....6

        2.2.3 Other technologies....6

    2.3 Different positioning use cases....7

3. ZIGBEE TECHNOLOGY....9

    3.1 IEEE 802.15.4: low-rate wireless personal area network....10

        3.1.1 Physical layer....11

        3.1.2 Medium access control layer....12

        3.1.3 Beacons and frame structure....12

    3.2 ZigBee specification....14

        3.2.1 Network layer....14

        3.2.2 Application layer....15

        3.2.3 Security....15

4. ZIGBEE POSITIONING....17

    4.1 ZigBee specific use cases....17

    4.2 Documented solutions....18

        4.2.1 Advanced Indoor Positioning Using Zigbee Wireless Technology.18

        4.2.2 Enhanced ZigBee indoor positioning system with ensemble approach....18

        4.2.3 High-accuracy ultrasound indoor positioning system based on wireless sensor network....19

5. COMPARISON OF ZIGBEE, WIFI AND BLE....20

    5.1 Power consumption....20

        5.1.1 ZigBee and BLE....21

        5.1.2 WiFi....22

    5.2 Reliability....23

5.3 Scalability....................24
5.4 Other viewpoints....................25
5.5 Relevance to HERE Technologies....................26
6. CONCLUSIONS....................27
REFERENCES....................28

ABBREVIATIONS

BLE	Bluetooth low energy
ISM	Industrial, scientific and medical radio bands
RSS	Received signal strength
RSSI	Received signal strength indicator
LR-WPAN	Low-rate wireless personal area network
IEEE	Institute of Electrical and Electronics Engineers
GNSS	Global navigation satellite system
GPS	Global positioning system
ToA	Time of arrival
TDoA	Time difference of arrival
AoA	Angle of arrival
CSI	Channel state information
FHSS	Frequency-hopping spread spectrum
IR	Infrared
WSN	Wireless sensor network
PHY	Physical layer
MAC	Medium acces layer
NWK	Network layer
APL	Application layer
APS	Application sub-layer
FFD	Full-function device
RFD	Reduced-function device
PAN	Personal area network
P2P	Peer-to-peer
CSMA-CA	Carrier sence multiple access with collition avoidance
GTS	Guaranteed time slot
AES	Advanced encryption standard
CFP	Contention free period
CAP	Contention access period
TC	Trust center
LLS	Linear least squares
MDS	Multidimentional scaling
Tx	(Signal) Transmission
Rx	(Signal) Reception
CTC	Cross-technology communication

1. INTRODUCTION

It is getting increasingly common for homes and offices to have automated smart devices like temperature sensors, humidity sensors, remote controlled power outlets, lights and locks. Such devices need a robust network technology to support large number of nodes, low power consumption and network security. This is what ZigBee is aimed for. ZigBee is a wireless, low-power, short range network technology, and the organisation responsible for it's developement is ZigBee Alliance.

On the other hand, in the modern world, there is an increasing demand for positioning services. Tracking mobile objects, such as dementia patients or livestock, navigation in traffic or indoors and proximity sensitive solutions, like smart lighting, are just a few of the services to mention, that require positioning. The basic motivation behind positioning is to replace tedious and unnecessary work with automation and monitoring using information technology.

The purpose of this thesis is to examine ZigBee technology from a positioning perspective. ZigBee is not originally designed for positioning, but it is still an attractive technology for positioning, because of its low power consumption and possibility to utilize a ready-made network infrastructure of automation and sensor networks. The thesis aims to see if ZigBee has the necessary properties for efficient indoor positioning, and to search for documented positioning solutions that are or could be done with ZigBee.

Chapter 2 covers indoor positioning in general, describing different technologies, algorithms and different use cases. Chapter 3 describes ZigBee technology according to layer model and security. Chapter 4 describes ZigBee as a positioning technology, beginning with possible ZigBee specific positioning use cases and following with some viable documented positioning experiments that are or could be implemented with ZigBee. Chapter 5 compares WiFi, Bluetooth low energy and ZigBee roughly in terms of power consumption, reliability, scalability and some other aspects. Chapter 6 draws conclusions from the previous chapters.

The thesis is done for HERE Technologies. HERE is a company developing positioning and map solutions, including indoor positioning with various technologies. Some of HEREs positioning solutions are also covered in this thesis as a baseline for future ZigBee solutions.

2. INDOOR POSITIONING

”With the technical advances in ubiquitous computing and wireless networking, there has been an increasing need to capture the context information (such as the location) and to figure it into applications.” [1]

This quote represents the state and importance of positioning in the modern world. Positioning is everywhere these days. Global navigation satellite systems (GNSS) such as global positioning system (GPS) are providing positioning services around the globe and are common in today’s smart devices, such as mobile telephones. However GPS signals do not penetrate roofs and walls of buildings very well, so in an indoor or otherwise obstructed environment, GNSS positioning doesn’t work properly. Thus to achieve positioning in an indoor environment, the use of a different technologies is required. This is also rather relevant in the modern society, as people spend most of their time indoors [2]. [3]

Indoor positioning can be achieved with many various technologies as described in Section 2.2, but in general, the presence of computing and radio resources everywhere is the key factor in achieving a positioning system with a reasonable cost. This phenomenon of ever-present-computing is also often referred to as ubiquitous or pervasive computing.

For example, HERE offers different positioning solutions based on cellular networks, WiFi, Bluetooth and GNSS. There are also different platforms for these technologies to be utilized. HERE’s solutions excluding GPS are all based on fingerprinting method, which is descibed in more detail in the following chapter. [4]

2.1 Positioning algorithms

This section gives a brief overall view of different positioning algorithms, as shown on Figure 1. The figure and the overview is not exclusive, but gives a good basic view on the subject. Measuring parameter abbreviations in the picture represent time-of-arrival (ToA), time-difference-of-arrival (TDoA), angle-of-arrival (AoA), received signal strength (RSS) and channel state information (CSI).

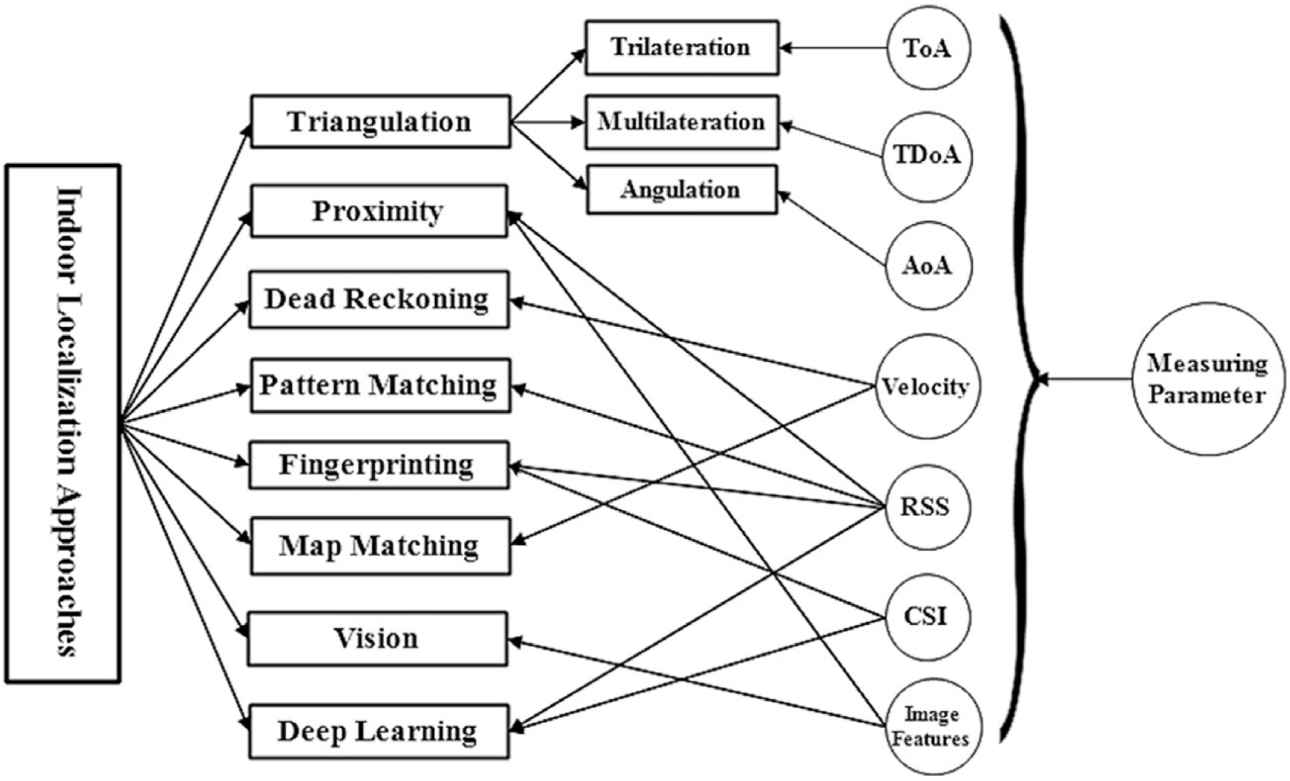

***Figure 1**: positioning algorithms and parameters [5]*

In triangulation, the geometric properties of a triangle are utilized to locate the target. It can be categorized into three techniques, as depicted in Figure 1. Trilateration and multilateration use the propagation time of the signal or the RSS as basis of measurement, while angulation uses the angle, in which the signal arrives to multiple base stations. By measuring either three lengths from a known baseline, measuring two angles from a known baseline and finding their intersection or measuring the angle and following the signal to the target, a two dimentional position can be determined. [5]

Proximity detection often measures the relative proximity from predefined known locations, which can then be used to infer the absolute position of the object. By measuring RSS values of different beacons, the proximity to these beacons can be confirmed. This can also be done with computer vision techniques. The accuracy of this technique is proportionate to the density of the beacons and the range between beacons and the tracked object. Generally this technique is cheap to implement but not very accurate. [5]

Dead reckoning estimates the target position, using the last known location of the target. Using sensors such as gyroscopes, magnetometers and accelerometers, the velocity or travelled distance can be inferred, and the position updated. Dead reconing is a relatively simple technique and efficient in estimating a position in real time, compared to other methods. However it often suffers from accumulating errors, without diverse correction methods. [5]

Fingerprinting is a technique, where the distance between a beacon and the tracked device is calculated by comparing the RSS with a pre-recorded radiomap in a database. The approach is efficient and often applied opportunistically in environments, where there is comprehensive coverage of transmitter beacons. Before fingerprint positioning can be done, the environment needs to be measured and stored in the database as radiomaps. Fingerprinting commonly offers about 1-5 m accuracy and is effective even in non-line of sight situations. The accuracy however is very much dependent on the environment and scenario. Also the signal strength at a fixed location is not always constant and the environment can change in due time, changing the radiochannel. This requires various countermeasures. Pattern matching is shown in Figure 1 as a separate approach, but is practically the same as fingerprinting in principle. [5]

Map matching usually involves estimating a target’s continuous position in a road network. In other words, deducing from the facts that the target is driving and a positioning result is near a road, that the target is probably on the road and wherein on the road. This is often used to increase the accuracy of other positioning approaches. [5]

Vision-based positioning involves camera sensors. The images are processed and the position of the mobile tracked device is estimated in reference to some landmark features of the environment in the picture. Databases are also utilized to store images and compare them with fresh images. This technique offers low complexity, but is intrusive in nature. Also the approach is unreliable when camera sensors are obstructed or the target is not in line of sight.

Deep learning is a machine-learning technique, where multiple levels of processing modules transform raw data into higher, more abstract level of representation. With enough levels, very complex functions can be achieved. In positioning, this can be utilized to identify locations with object recognition or improve radiomaps in fingerprinting method. This requires a constant stream of object position information, regardless of the distance of the object. Measurement techniques commonly used with deep learning are vision and CSI. [5, 6, 7]

2.2 Positioning technologies

In this section the focus is on other technologies than ZigBee. Positioning with ZigBee is covered in Chapter 4. The section describes positioning in general and then more specifically with a few more commonly used technologies.

Indoor positioning systems can be classified based on the signal types, signal metrics and the metric processing methods. Signal types are defined by the signal charactersitics and include for instance infrared, ultrasound, ultra-wideband, narrowband and radio frequency. Signal metrics refer to the measuring technique used to pinpoint the target and include angle of arrival, time of arrival, time difference of arrival and received signal strength. Metric processing refers to techniques and algorithms used on the received metrics to calculate the position. These include triangulation, proximity sensing and scene profiling, also often referred to as fingerprinting. There are more signal types, metrics and processing methods used in positioning in addition to the ones mentioned. [5]

There are numerous problems in indoor positioning. In radio frequencies, the signal propagation is affected by multi-path fading, temperature, humidity variations and the mobility of physical objects in the area, such as opening and closing doors and human movement [1]. Also the bandwidth of RF is limited and the signal power is regulated by national and international authorities [8]. The other signal types also have their strengths and weaknesses, which are covered in subsection 2.2.3.

In this thesis, the main focus is on ZigBee and in a lesser degree WiFi and Bluetooth as they all function on the same unlicenced industrial scientific and medical (ISM) frequency band 2.4 - 2.5 GHz, and also function similarly in positioning.

2.2.1 Wi-Fi

Wi-Fi is a wireless data transmission standard, which operates on 2.4 GHz, 5 GHz, and recently 60 GHz frequency bands. The effective coverage range is between 50 and 100 m. Wi-Fi is not originally designed for positioning, but it is often used opportunistically by collecting the advertised info of Wi-Fi-hotspots and using the RSS values for positioning. With fingerprinting method the accuracy of Wi-Fi positioning is usually around a few meters in an environment with dense Wi-Fi coverage. After radiomapping the technology is fully offline in nature, as WiFi scans do not require online connectivity. Also utilizing CSI on wireless devices, improves performance. It should be mentioned, that IEEE is preparing an addition to the current WiFi standard in amendment 802.11az, which enables absolute and relative positioning with better accuracy [9]. [5]

The upsides of Wi-Fi as a positioning technology, are the availability of networks especially in urban areas and low cost of tranceivers [5]. However the dynamic nature of Wi-Fi hotspots requires constant re-mapping and updating of fingerprint database, for the positioning system to remain accurate. Also interference from other signals on the 2.4 GHz band is problematic, as it is a non-regulated ISM band, which is used also by Bluetooth and ZigBee systems. Studies show that Wi-Fi is rather unaffected by ZigBee activity in the proximity. Bluetooth on the other hand might have a significant effect on WiFi throughput. [10, 11]

HERE has a positioning solution based on WiFi technology. It is implemented using radiomapping of existing ubiquitous WiFi infrastructure and comparing RSS measurements to stored radiomaps. HERE promises positioning accuracy up to 3 - 4 m with this approach. [12]

2.2.2 Bluetooth

Bluetooth is rather common technology, which makes it relatively cheap with many diverse devices on the market [5]. It also works on the 2.4 GHz frequency range, same as Wi-Fi and ZigBee. The usage of the 2.4 GHz ISM band causes interference from other tranceivers, but this is allegedly somewhat mitigated by frequency-hopping spread spectrum (FHSS) technology that Bluetooth uses. However [10] claims FHSS to be ineffective in countering Wi-Fi interference. [13]

As of version 4.0, Bluetooth has supported Bluetooth low energy (BLE), a technology designed for very low power operations. It advertises 50 – 99% power consumption reduction compared to regular bluetooth. BLE also supports mesh networking topology as of version 5.0 [14]. Mesh network is a non-hierarchical local network topology, which can have multi-hop routes between nodes. BLE also offers multiple data rates and transmission (Tx) power classes for different devices and use cases. [15]

Positioning with Bluetooth commonly utilizes the same principles as Wi-Fi: RSS and fingerprinting [13]. Unlike with WiFi fingerprinting, which opportunistically utilizes the ubiquity of WiFi access points, Bluetooth positioning requires BLE Beacons to be pre-installed around the premises before radiomapping. After beacon installment and radiomapping, position can be inferred comparing RSS measurements with stored radiomaps as with WiFi. Also same as with WiFi, after radiomapping the method is completely offline, as BLE scans require no online connectivity. BLE beacons broadcast a set message at regular intervals and use special advertisement channels, which are not used for regular BLE transmissions [15]. It should be mentioned that other positioning methods are also emerging, that utilize the BLE mesh networks [16]. [5]

HERE also has a positioning solution based on BLE. It is implemented as described above, by installing BLE beacons across the wanted premises and then radiomapping the environment. After this the positioning is done by comparing BLE scans RSS values with the stored radiomaps. HERE promises a position accuracy of 2 – 3 m with this approach depending on the density of the beacon infrastructure. [12]

2.2.3 Other technologies

With infrared (IR) positioning systems, there are problems such as physical obstruction and fluorescent lighting or direct sunlight [17]. IR radiation does not generally penetrate physical objects, so for positioning with, IR line of sight is required. The problem with fluorescent lighting and sunlight is that they also include infrared radiation, which interferes with the received measurements. However, IR also has a very negligible reflection capabilities, so it does not suffer from multipath effects as RF systems do. IR is also very cheap technology to implement and it can achieve positioning accuracy up to 57 cm. [5, 18]

With ultrasound there are problems such as reflection of acoustic pulses, creating reverberation, inconsistent frequency due to Doppler shift effect and changing of propagation velocity of sonic waves with change in humidity or temperature. Ultrasound beacons also have a fairly short range and need to be synchronised. Ultrasound signals do not penetrate walls effectively, but the transducers are cheap and compatible with almost any hardware. Ultrasound can achieve positioning accuracy up to ~1 cm [18]. [5]

These technologies are not very comparable to ZigBee, as they are very different in nature and implementation in positioning. However ZigBee and latest Bluetooth technologies enable large wireless sensor networks (WSN) with mesh topology. This could enable other positioning technologies, such as IR and ultrasound, as they need WSNs to implement positioning systems. This could be another feasible use for ZigBee technology.

2.3 Different positioning use cases

There are multiple different scenarios for positioning, in which the solutions usually are tradeoffs between price and precision. Also the suitability of a certain technology for a specific use case is paramount for achieving good accuracy, reliability and cost-efficiency.

In large open spaces, such as halls or auditoriums, there are usually very few objects to obstruct any signal flow, but high ceiling and large floor area can result in large signal attenuation. This is advantageous to signal types that need line-of-sight, such as infrared or ultrasound. However considering large factories and other noisy environments, simple ultrasound systems can be affected by the noise and infrared by other signals sources, such as lights. However also RF based systems can suffer in a factory setup, as electric motors and other electrical devices generate electromagnetic disturbance, which can create errors, that completely drown a signal beneath noise.

In obstructed spaces, such as office buildings, RF signals penetrate walls rather well, while ultrasound or infrared do not. This is both a positive and a negative feature, as the signal impenetrability can be used to effectively position the target to a certain walled area, such as a room, but it also increases the need for more sensors, thus increasing the cost. As WiFi penetrates walls and is abundant in office environments, it is rather effective and cheap positioning method in this kind of setup.

With apartment buildings of small flats, WiFi positioning could function similarly to offices, however with detached houses, home environment is often similar to an office environment, without the abundance of WiFi access points. In this case, home automation products, such as smart lighting and other smart devices, could be utilized opportunistically for positioning, similar to an office WiFi setup. In home automation, ZigBee has been very prominent, considering products like Philips Hue, Samsung SmartThings, Amazon Echo Plus and Ikea Smart lighting [19-22].

Use cases also differ with urban and rural environment. In urban setting, WiFi and cellular networks are commonly available and abundant, while also the environment is obstucted with buildings and is noisy considering RF and sound waves. WiFi and cellular positioning have an advantage in this kind of environment, both indoors and outdoors, as they have multiple high powered signals available. However tall buildings also obstruct GNSS and higher range cell signals, such as GSM. The noise can also effect any outdoor ultrasound systems.

With rural settings there are usually few obstructions, save for the landscape. This helps with high distance signals, such as GSM and GNSS. However in this kind of environment, any indoor positioning will most likely need a separate sensor infrastructure, such as ZigBee network or Bluetooth beacons, as no abundant WiFi or cellular networks are to be expected.

Another valuable use case from marketing perspective are the shopping malls, as one could implement personalised marketing or navigation, based on the position of the target. This would not neccessarly need much positioning accuracy, but rather a crude proximity sensing system could suffice. Knowing that the target is near a certain shop in a mall should be enough for a rather functional system. This could be implemented for example with a simple received signal strength (RSSI) limit sensing with WiFi, Bluetooth or ZigBee. For more elaborate navigation and precision, triangulation or fingerprinting method could be utilized.

3. ZIGBEE TECHNOLOGY

”The ZigBee Alliance has developed a very low-cost, very low-power-consumption, two-way, wireless communications standard. Solutions adopting the ZigBee standard will be embedded in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys, and games.” [23]

This quote describes well what ZigBee technology aims to be. This thesis concentrates on the ZigBee 2015 specification, which uses the Institute of Electrical and Electronics Engineers (IEEE) specification 802.15.4-2011 compliant radio. The newest 2017 ZigBee specification is not available without joining ZigBee Alliance. [24]

A fully functional ZigBee device is composed of 4 differentiated layers: physical (PHY), medium access control (MAC), network (NWK) and application (APL) layers. ZigBee specification defines the two upper abstraction level layers, NWK and APL, on top of the IEEE 802.15.4 specification. The aforementioned IEEE specification defines the operation of low-rate wireless personal area networks (LR-WPAN), which make up the two lowest level layers of ZigBee, PHY and MAC [25]. The ZigBee APL is further composed of application support sub-layer (APS), ZigBee device object and application framework. [23]

The full ZigBee stack architecture is depicted in Figure 2. The figure shows different interfaces, in which different layers interact with each other, and differentiates parts that are defined by IEEE 802.15.4 standard, ZigBee standard and the end manufacturer with different colors. The layers and their function is covered in the following sections. Section 3.1 describes the 802.15.4 defined properties and Section 3.2 describes the ZigBee standard defined properties and security in ZigBee.

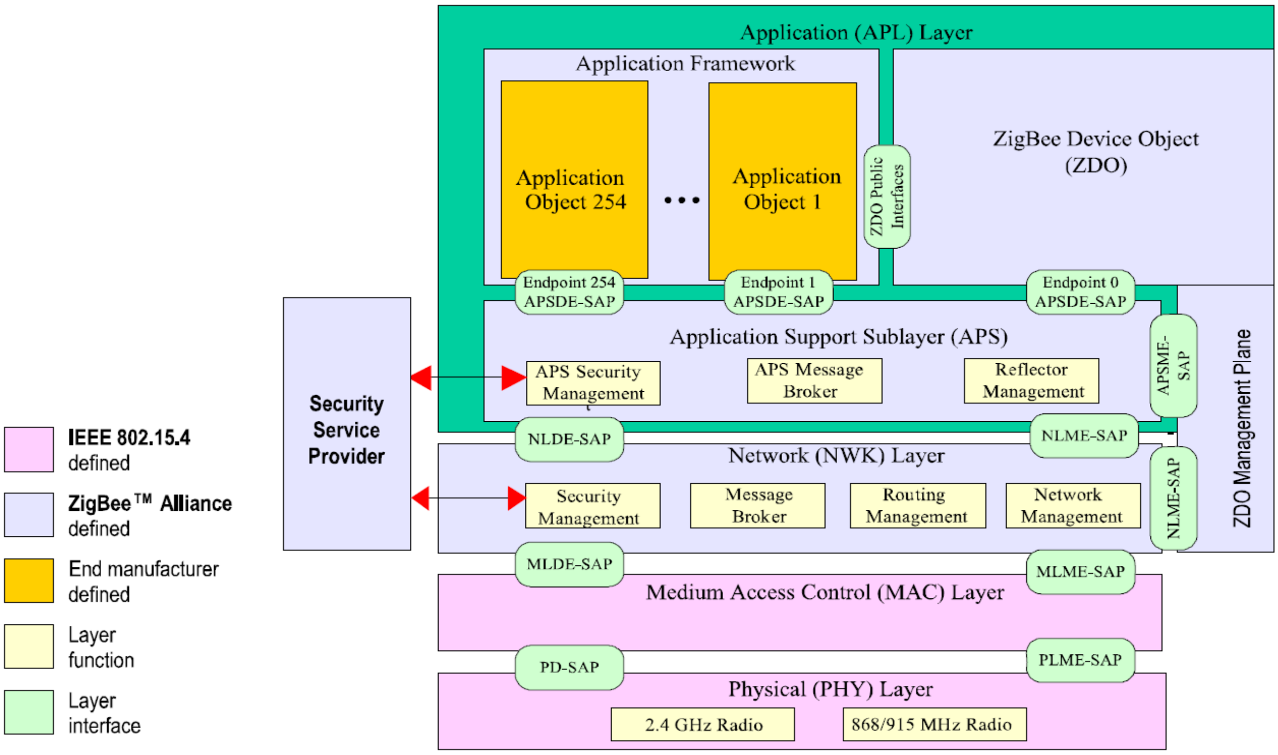

Figure 2*: ZigBee stack architecture [23]*

3.1 IEEE 802.15.4: low-rate wireless personal area network

IEEE 802.15.4 defines LR-WPANs, networks which are characterised by simplicity, extremely low cost, low power consumption, reliable data transfer and relaxed throughput requirements [25]. In other words, the data rates of LR-WPAN and ZigBee are lower than for example classic Bluetooth or WiFi, but the power consumption is also lower than classic Bluetooth and much lower than WiFi. A rough power consumption comparison is covered in Section 5.1.

802.15.4 defines two types of devices in a network: full-function devices (FFD) and reduced-function devices (RFD). It also defines three types of roles in a network: personal area network (PAN) coordinator, coordinator and device. An FFD can serve in any role, but RFD can only serve as a device. Also FFDs can talk to other FFDs or RFDs, but RFDs can only talk to FFDs. An RFD is intended for simple applications with minimal resources and memory capacity, that do not need to send large amounts of data. Sensors and ZigBee Green Power devices, which use energy harvesting technologies, are examples of typical RFD devices [26]. RFDs can only associate with a single FFD at a time. [25]

A WPAN network shall always include at least one FFD, that operates as the PAN coordinator. PAN coordinator is the primary controller of the PAN and typically mains powered, while the other devices are typically battery powered. In ZigBee PAN coordinator is generally referred to as ZigBee

Coordinator, however the more recent ZigBee specification also defines distributed security networks, which do not have a central node [23, 27]. This is covered in more detail on Subsection 3.2.1. [25]

LR-WPAN supports the star and peer-to-peer (P2P) topologies, which are depicted in Figure 3. In a star network, all other nodes communicate directly with the PAN coordinator. With P2P network, all FFD nodes may communicate with any other nodes in the range of their transceivers. A star network is reminiscent of a master-slave kind of behaviour, such as with classic Bluetooth, while a P2P network allows more complex network formations, such as mesh networks with multiple hops between sender and receivers of messages. [25]

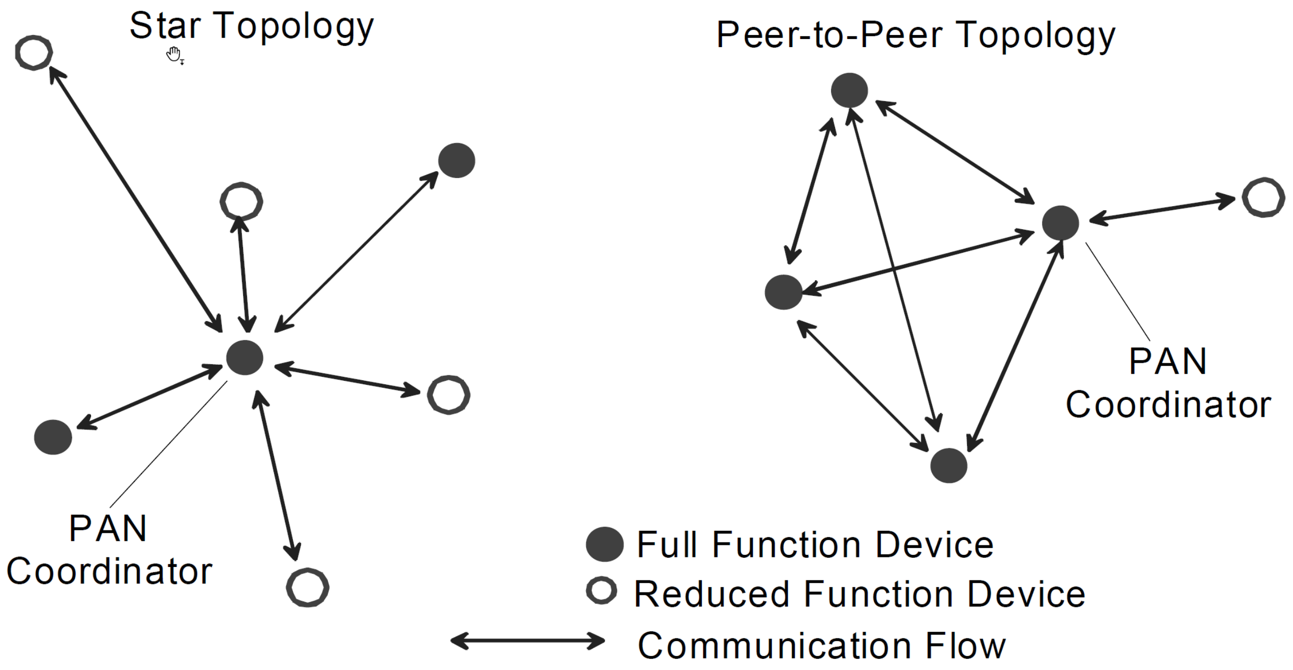

***Figure 3**: Examples of Star and peer-to-peer topologies [25]*

3.1.1 Physical layer

The physical layer is responsible for the clear channel assessment for carrier sense multiple access with collition avoidance (CSMA-CA), activation and deactivation of the radio transceiver, link quality indication for received packets, energy detection within the current channel, channel frequency selection and the physical data transmission and reception. The link quality indicator is the characterization of the quality and/or the strength of the received packet. This can mean RSS, signal-to-noise ratio estimation or a combination of the two. It is common for ZigBee and wireless devices in general to implement RSSI as a feature, and it is commonly used in positioning [2]. [25]

IEEE 802.15.4-2011 has many different PHY layers, that operate on different frequencies. ZigBee uses only two of these. The lower 868/915 MHz range has eleven different channels, one in the 868 MHz band and ten in the 915 MHz band. The 868 MHz band is used in Europe while the 915 MHz band is used in countries such as United States and Australia. The higher 2.4 GHz frequency range is virtually universal and has 16 channels. [23, 25, 13]

3.1.2 Medium access control layer

The MAC layer is responsible for synchronizing to beacons and the frame structure, generating beacons, if the device is a coordinator, supporting device security, supporting PAN association and disassociation, employing CSMA-CA mechanism for channel access, handling and maintaining the guaranteed time slot (GTS) mechanism and providing a reliable link between two peer MAC entities. GTS mechanism is covered in more detail in Subsection 3.1.3. Security services offered on MAC layer consist of symmetric encryption using advanced encryption standard (AES) algorithm. However the keys and the control of when to use security services are defined on the higher levels. [25]

3.1.3 Beacons and frame structure

LR-WPAN supports the optional use of a superframe structure depicted in Figure 4. The frame is defined by the coordinator device, bounded by beacons and divided into 16 timeslots of equal duration. The superframe can optionally have an inactive period, during which the coordinator is able to enter a low-power mode. The beacons hold information on the structure of the superframes and identify the PAN in question. They are also used to synchronize the attached devices. Although the superframe structure is optional, beacons are still required for network discovery. [25]

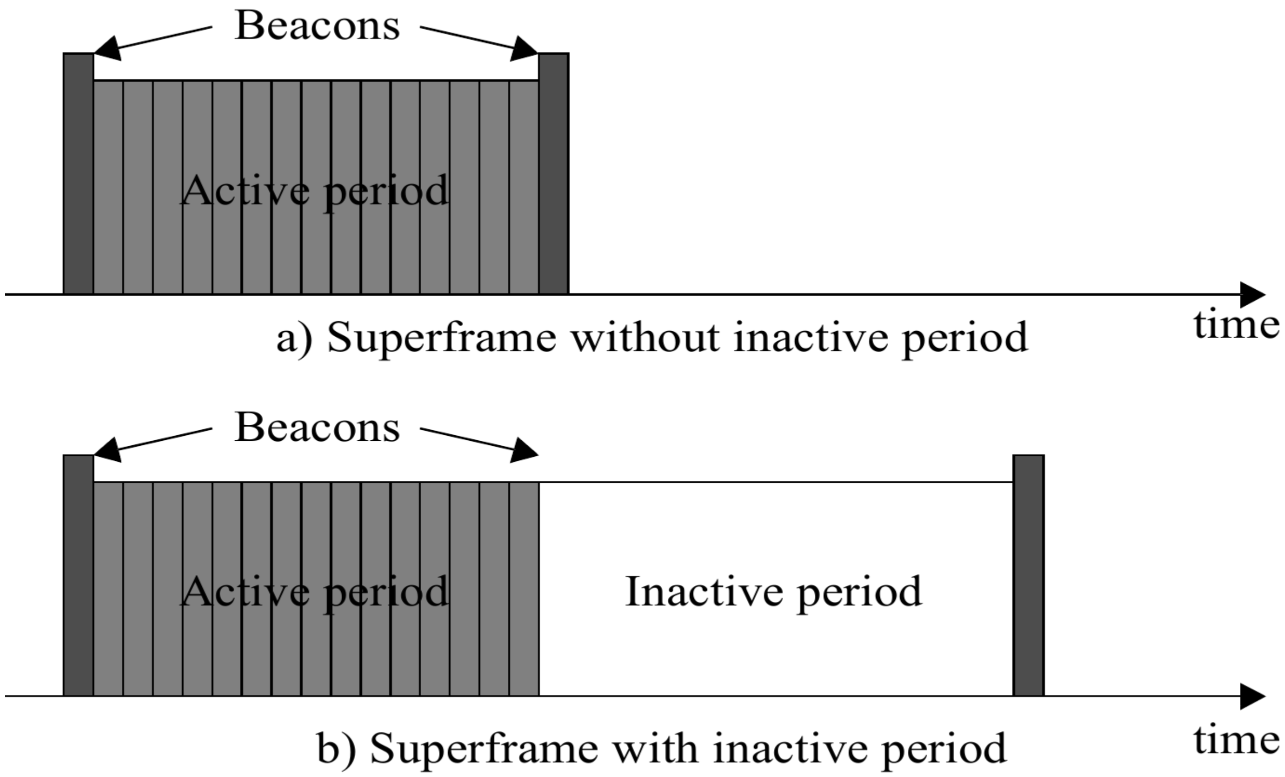
Beacons
Active period
time
a) Superframe without inactive period
Beacons
Active period
Inactive period
time
b) Superframe with inactive period

***Figure 4**: LR-WPAN superframe structure [25]*

The active period of the superframe is optionally consisted of contention free period (CFP) and contention access period (CAP), as depicted in Figure 5. The PAN coordinator may dedicate up to seven time slots to contention free period for applications, which require low latency or specific data bandwidth. These are called guaranteed time slots, and a single application may take up more than one time slot. Devices communicating in CAP need to compete with each other using CSMA-CA or ALOHA mechanism, but CFP slots are always reserved so no competition is required. [25]

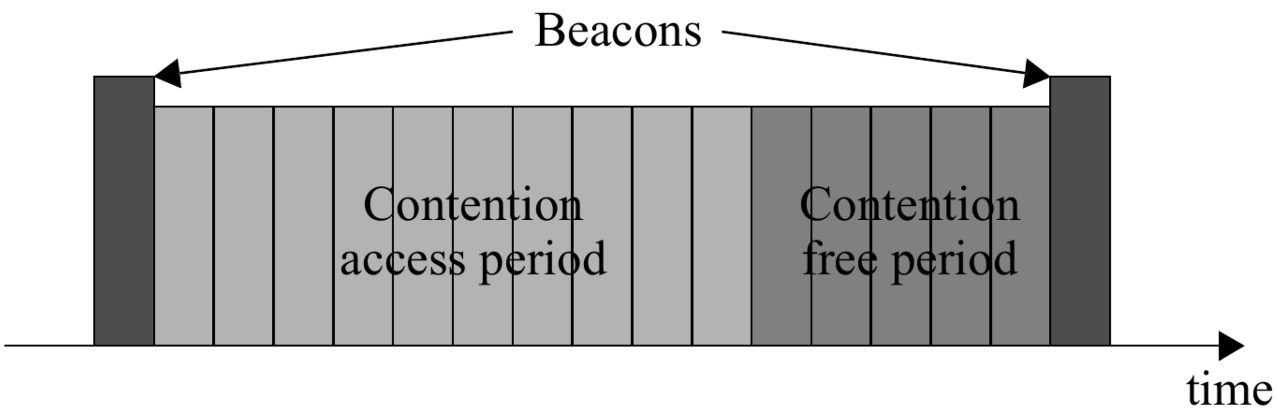

Figure 5*: structure of the active period with contention free period. [25]*

3.2 ZigBee specification

The ZigBee specification defines the NWK and APP layers. This Section gives a brief explanation on functionality of these layers and security features that they implement.

3.2.1 Network layer

The network layer is responsible for generating network packets from application data or control messages and transmitting them to the destination address or the next hop along the route to the destination address. Control messages allow applications to start, join, rejoin or leave networks, assign addresses to new devices on the network (only ZigBee coordinators and ZigBee routers), discover, record or report information on one-hop-neighbors, discover or record routes through the network to a single destination device and control the receiver activity to synchronize and control transmission times. [23]

The ZigBee network layer can use multiple routing mechanisms such as unicast, multicast, broadcast and many-to-one. ZigBee devices have two kinds of addresses: a 64-bit IEEE address, also called extended mac address, and a 16-bit network address. The 64-bit MAC address is a globally device specific address, usually set by the manufacturer or during installation and allocated and maintained by the IEEE [28]. The 16-bit network address is given to the device when it joins/creates a network, and is unique in a network. Network address 0xffff means the device is not part of a network and 0xfffe means the device is part of a network but not assigned a network address yet. When using multicast or broadcast, the network address is the broadcast address or the ID of the target multicast group, while the IEEE destination address is always omitted as the IEEE addresses are unique globally. The route to a multihop destination is also included in the network header. [23]

3.2.2 Application layer

Application layer is further composed of application sub-layer, application framework and ZigBee device object as seen in Figure 2.

Application sub-layer provides an interface between network layer through several services that are used by ZigBee device object and application objects. These services include data transmission between two or more application objects in the same network, security services, binding of devices and maintaining of database of managed objects. Application sub-layer also includes an application header for data units from application objects, applies end-to-end retries on transmissions, handles message fragmentation and reassembly, security key management and group addressing management. [23]

Application framework hosts manufacturer defined application objects. Up to 254 objects may be defined, however 14 of these are reserved by ZigBee alliance, and may not be used without approval. For example ZigBee Green Power cluster, if implemented, is one of of these ZigBee alliance defined objects. ZigBee device object presents interfaces for the application objects to control device and network functions. It handles the initialization of application sub-layer, network layer and the network security service provider. It also assembles the configuration information from application objects, to determine and implement discovery, security management, network management and binding management. [23]

3.2.3 Security

Security in ZigBee is done on “the layer that originates a frame is responsible for initially securing it” principle and open trust model. Open trust model means that all entities on a single ZigBee device trust each other, so there is no security between different application objects or between different layers on the same device. Because of this model, security keys can be reused between layers to reduce storage costs. This would mean, for example, encrypting APS broadcasts and NWK layer frames with the same key. [23, 27]

Security among the ZigBee network is based on two kinds of keys: link keys and a network key. Link keys are for securing unicast communication between two application peer entities, while the network key is for securing all network layer communications, and is shared across the network. Both keys are 128-bit long and may be periodically expired and updated. [23]

There are two kinds of security models with ZigBee: centralized security and distributed security. Distributed security model is designed for easily configurated systems, where there is no central trust center that distributes security keys. Instead every router on the network is capable of issuing security keys. All devices use the same network key to encrypt messages in distributed networks. [27]

Centralized security model is designed for higher security, where there is a central trust center (TC), which is usually also the network coordinator. In centralized model, only TC is allowed to issue security keys and periodically creates, distributes and switches to a new network key. TC allows devices to enter the network only if they have proper credentials. TC also establishes a unique link key between the TC and every device on the network called TC link key. Link keys between other devices are issued by TC on request. [27]

If protection from theft of service is required, NWK layer security is used on all frames, except between a newly joined device and a router, until the new device receives the network key. In addition to network layer security, end-to-end security can be implemented so that the messages are only accessable to the source and the destination objects. This is implemented using the link key issued to the pair by TC, and encrypting the message using AES-128 encryption. [23]

TC may also require a device to use a unique install code to be able to join a centralized security network. The code must be previously entered to the TC out-of-band, i.e. not using ZigBee. All ZigBee devices must contain a 128-bit number protected by 16-bit CRC, which is commonly printed as a number or QR code in the device packaging. The joining device and TC derive a unique 128-bit TC link key from the install key, using Matyas-Meyer-Oseas hash function. [27]

ZigBee allows secure over-the-air updates. This is done using the unique link key to send the update image, and the image can also be encrypted with another unique key. The image may be stored to an on-chip memory, that is configured with the debug read-back feature disabled. This prevents reverse engineering at least with the standard debugging tools. Devices check the validity of the active image on every boot, thus detecting image corruption quickly. In the case of a corrupted image the device returns to a previously known good image. [27]

To prevent replay attacks, in which attacker would record an RF message and replay it to cause repeated action, every ZigBee command frame includes a frame counter. The receiving device checks the frame counter on reception of a message and ignores duplicate messages. Similarly to bluetooth dynamic FHSS, which tries to avoid crowded channels in the 2.4 GHz band, ZigBee also supports frequency agility, which can relocate the network to a different channel, if current channel is impaired. [27]

4. ZIGBEE POSITIONING

This chapter covers ZigBee as a positioning technology, and envisions a few possible approaches to positioning with ZigBee. First some ZigBee specific use cases are covered. Secondly some documented solutions, which are or could be implemented with ZigBee, are addressed. The focus is to get an idea of what has already been implemented, and what could be possible to implement with ZigBee.

4.1 ZigBee specific use cases

ZigBee could be used like BLE in positioning by installing some ZigBee routers as reference beacons and taking RSSI measurements with a tracked device. This allows positioning with triangulation or fingerprinting approaches. Also the system can use ZigBee as a communication channel while using it as reference network for positioning. This allows the system to make the positioning calculations on the server side, if necessary, to save end device power, and to allow more simple end devices, without resorting to a different technology, like cellular or WiFi network on the end devices. It should be noted however, that ZigBee does not support beaconing on mesh networks, only on tree and star networks [23].

Home automation includes many modern day smart devices, such as remote-controlled lights, power outlets and other electric devices. These devices are often implemented using ZigBee technology. Such an automation system could potentially be a very functional basis for different kind of positioning systems. Examples of such devices are Philips Hue, Samsung SmartThings, Amazon Echo Plus and Ikea Smart lighting [19-22]. Assuming these devices are capable ZigBee routers and remain relatively stationary in a home environment, they could compose a ready-made architechture for positioning.

Another solution could be to use a non-RF-based technology for positioning, but to use ZigBee for communication between sensors and actuators needed for the system. Infrared and ultrasound are examples of such technologies.

4.2 Documented solutions

This Section presents some documented positioning solutions that are or could be implemented using ZigBee. The solutions are covered as a proof of consept and not in depth.

4.2.1 Advanced Indoor Positioning Using Zigbee Wireless Technology

This experiment [3] uses the fingerprint method in a ZigBee network. The emphasis of the study is on improving the accuracy of the fingerprint database, by filtering the online positioning stage results. Without going into details, the positioning accuracy achieved in the experiment was 0.51m in short distance range from sensors. The ZigBee chip used in the experiment was developed in Nanchang University, and was also tested in the experiment to achieve nearly 40m range, without decreasing positioning accuracy. [3]

This experiment shows that ZigBee is fully capable of positioning with RSSI based fingerprint method. As this method is very similar across different technologies, it would suggest that porting an existing fingerprinting method based on WiFi or Bluetooth to ZigBee, should be feasible. As HERE already has implementations on WiFi and Bluetooth positioning, it should be feasible to extend their services to ZigBee technology.

4.2.2 Enhanced ZigBee indoor positioning system with ensemble approach

This experiment [29] uses various different positioning algorithms on a ZigBee system as an ensemble, to achieve better positioning results. Different algorithms perform differently in different spatial situations, and as such weighting algorithm results and combining them achieves better results than any of the algorithms as a standalone. This is due to the complementary advantages of algorithms over each other in various different spatial situations. [29]

The ensemble system used, was a ZigBee sensor network at Yuan Ze University. The experiment compared gradient-based search, linear least squares (LLS) approximation, multidimensional scaling (MDS), the fingerprinting method and a multi-expert system to the proposed ensemble approach. The algorithms used on the ensemble system were gradient-based search, LLS approximation and MDS methods. The ensemble needs a training stage for the weights of different algorithms. This is done by recording positioning errors beforehand, similarly to fingerprinting methods online stage. [29]

This research gives examples of five different positioning methods for ZigBee systems, and proposes an additional method to combine these, to achieve more accurate position. This gives good insight on potential future ZigBee positioning systems, and might also be a feasible improvement method for already implemented HERE positioning systems with other technologies.

4.2.3 High-accuracy ultrasound indoor positioning system based on wireless sensor network

This experiment [18] describes a positioning system based on ultrasound. The emphases of this study are some improvements and implementation techniques for ultrasound positioning. The basic positioning setup uses anchor nodes with known positions and a mobile node that is tracked. All of the nodes in this setup are communicating through WiFi, and form a WSN composed of multiple subspaces. The nodes also have ultrasound transceivers, which are used for positioning. The setup achieves ~1 cm positioning accuracy, and claims to have a high and robust stability. [18]

Detailed description of the study is beyond the scope of this thesis, however the model is relevant, as ZigBee is renowned for its ability to support robust and large WSNs [13, 7]. The communication method (WiFi) in this setup, could be replaced with ZigBee, which could significantly reduce the power consumption of the system. Also ZigBee supports various kind of mesh network structures, which could make it a natural candidate for the communication in a large system of this kind. Also as this system achieves ~1cm positioning accuracy, it is a worthy candidate for use cases with the need for great accuracy.

5. COMPARISON OF ZIGBEE, WIFI AND BLE

This chapter aims to compare ZigBee, WiFi and BLE in several different aspects. Power consumption is important aspect in general, especially for battery powered devices. In this thesis this is covered only lightly in the following section. Section 5.2 covers some various techniques, that these technologies have for improving the reliability of the network, and also improve the co-existence on the same frequency range. Section 5.3 covers some technological features, that improve or limit the scalability of the technology.

5.1 Power consumption

There are several aspects to the power consumption with these technologies, including the Tx power of the transceiver, the stack overhead, the computational overhead and the opportunistic availability of ready-made infrastructure. However, even considering all these aspects, the most accurate indicator would be actual power measurements with actual hardware. Hardware on the other hand is dependant on the various components which vary between manufacturers.

In this thesis we only compare the nominal power consumption values of some devices on the market and in production. This is not very accurate, but gives some perspective on the subject. It should be emphasized, that these are different devices from different manufacturers, and only show referencial information on the performance of the actual underlying technology. These are also values from official device specifications, and can possibly deviate from real device properties.

The power consumption of ZigBee and BLE are expected to be closer to each other than WiFi. WiFi utilizes more opportunistic approaches to achieve cost efficiency, while ZigBee and BLE are commonly renowned for having low power consumption [13, 5, 7]. As such ZigBee and BLE are addressed as one subsection and WiFi in another subsection.

The compared chips are chosen from the same four manufacturers in Bluetooth/ZigBee and WiFi scenarios according to following criteria: Chip needs to be still in production, the nominal operation voltage should be around 3.3 V, the chip should be on the low end in the power consumption on the manufacturer’s stock and the chip should have comparable nominal power values. In this thesis, the power consumption of a chip is assumed to be directly proportional to the used current, i.e. the voltage is assumed to be 3.3 V in all measurements on all devices.

5.1.1 ZigBee and BLE

ZigBee or IEEE 802.15.4 specifications do not actually specify any power requirements other than Tx power conforming with local regulations [23, 25]. However ZigBee Green Power promises some power saving features, such as energy harvesting capabilities, ultra-low power RF silicon and network and application layer protocols, that support compressed messages, limited transactions and reduced packet lengths, on-network time, round-trips and connection rediscovery [26].

Bluetooth specification defines several different transmitter power classes. Class 1 devices have output power of 0 to 20 dBm, class 2 devices -6 to 4 dBm and class 3 devices < 0 dBm at maximum power settings. However this does not specify an absolute minimum value for device output power. [30]

Table 1 shows the power statistics of some BLE and ZigBee chips from four different manufacturers. XBee3 (ZigBee) seems to have the highest power consumption, followed by EFR32MG (ZigBee & BLE), CC2650 (ZigBee & BLE) and ATSAMB11XR (BLE). This would indicate that ZigBee radios generally would consume more power on average. However, considering EFR32MG consumption values on both technologies, the difference is rather subtle. Also CC2650 supports ZigBee and BLE, but it’s specification did not have separate power consumption values for these technologies. This would indicate, that these values also do not differ notably. It should be noted that CC2650 and the ATSAMB11XR, with the lowest power consumptions, are also the most recent devices on this comparison, both of them released in 2019.

Table 1: *power statistics of various BLE and ZigBee devices [31-34]*

	Digi XBee3 ZigBee 3	Microchip ATSAMB11XR (BLE)	Texas Intstuments CC2650 (ZigBee & BLE)	Silicon Labs EFR32MG (ZigBee & BLE)
Rx current	17 mA	5.26 mA	5.9 mA	10.2 mA (ZigBee) 9.5 mA (BLE)
Tx current @ 0 dBm	-	4.18 mA	6.1 mA	8.5 mA (ZigBee & BLE)
Tx current @ 5 dBm	-	-	9.1 mA	-
Tx current @ 8 dBm	40 mA	-	-	-
Standby/Sleep current	< 1 µA*	2.03 µA	1 µA	1.4 µA
Operation voltage	2.1 – 3.6 V	1.8 – 3.6V	1.8 – 3.8 V	1.8 – 3.8 V

* Assumed that the power-down current in the specification means sleep current.

Although the nominal power consumption values do not seem to differ notably between devices and technologies, it should be noted that the XBee S2C has an exceptionally high power consumption compared to the other devices, higher actually than a five year old BLE module Microchip RN4020 [34]. This indicates that there is a lot of variance on the power consumption of devices on the market. Considering this and the following subsection, it would seem that this variance could be manufacturer dependent.

5.1.2 WiFi

WiFi is considered to consume rather much power compared to ZigBee and BLE. In Table 2, there are some nominal power consumption values from some WiFi modules on the market. XBee WiFi has the highest power consumption followed by ATSAMW25, CC3235S and WFM200 as the lowest. ATSAMW25 has lower Tx consumption than CC3235S, but higher Rx consumption. This difference is somewhat mitigated considering that ATSAMW25 has a higher RX input sensitivity (-98 dBm vs -95.7 dBm) and lower Tx power compared to CC3235S [32, 34].

Table 2: *power statistic of various WiFi devices [31-34]*

	Digi XBee Wi-Fi	Microchip ATSAMW25	Texas Instruments CC3235S	Silicon Labs WFM200
Rx current	100 mA	70 mA	59 mA	41.6 mA
Tx current	up to 309 mA @ 16 dBm	172 mA @ 17 dBm	223 mA @ 18 dBm	152.6 mA @ 17 dB
Idle current	-	-	710 µA	337 µA
Operation voltage	3.14 – 3.46 V	2.7 – 3.6 V	2.1 – 3.6 V	1.8 – 3.6 V

As is seen, the power consumption is an order of magnitude higher than ZigBee or BLE regardless of the manufacturer. Also notable is that, same as with ZigBee and BLE, Microchip, Texas instruments and Silicon labs have rather low power consumption compared to Digi. Another trend can be noted, as WFM200 is the most recent of these chips, and has the lowest power consumption.

As a conclusion, it would seem that a modern transceiver correlates to low power consumption. Also some manufacturers seem to focus more on the power consumption aspect than others, which should be considered, when buying hardware. As a technology, WiFi consumes much more power compared to BLE of ZigBee as expected.

5.2 Reliability

The reliability between these technologies very much comes down to their co-existence in the 2.4 GHz frequency range. As WiFi is the most power consuming technology, it also is the most prominent of the three as a study [10] shows that Bluetooth and ZigBee do not notably affect WiFi transmissions on the 2.4 GHz range. Other studies show negligible effect of Bluetooth on ZigBee transmissions and vice-versa [13, 10, 11]. There are studies [11, 35] that show Bluetooth having adverse effect on WiFi transmissions, but considering the date of these studies, it is probable that these were done with classic Bluetooth devices, not BLE devices. However the Bluetooth core specification v5.1 does support output power of 20 dBm for BLE devices, so effects on WiFi are still plausible [30].

Bluetooth frequency hopping in general should improve the co-existence between technologies. When Bluetooth transmission clashes with another transmission, at the time the other device retransmits the message, Bluetooth device has probably already hopped to another channel. This also works the other way for Bluetooth retransmission. There are differing opinions on the effectiveness of this technique however [13, 10].

Transmission power control is a common technology between Bluetooth, WiFi and ZigBee, which aims to use only minimal power needed for transmission [24, 11]. This aims to reduce unnecessary noise and interference between these technologies. Packet fragmentation, i.e. using smaller packets, when encountering interference in a channel, is another common method used to minimise the effect of a singular packet loss. To further combat the interference of WiFi, modern Bluetooth devices implement adaptive frequency hopping. Adaptive frequency hopping is an improvement to regular FHSS approach. Instead of hopping all the channels in order as the regular FHSS does, adaptive frequency hopping avoids channels with heavy interference. [10]

ZigBee on the other hand uses receiver energy detection to assess the communication channels before forming a network. This way a ZigBee router or coordinator can choose a relatively clear channel for reliable communication. Also the current ZigBee specification supports frequency agility i.e. the changing of network channel, if the current one is interfered [23, 13]. The most reliable channels, considering WiFi interference, seem to be the channels outside the commonly used, non-overlapping WiFi channels [13]. These channels are recommended by the 802.11b standard, and consist of channels 1, 6 and 11 for North America and 1, 7 and 13 for Europe [11]. The ZigBee channels outside the recommended WiFi channels are 25 and 26 in North America and 15, 21 and maybe 16 and 22 for Europe [13, 35]. However WiFi can also use dynamic channel selection, similar to frequency agility, to move from a crowded channel to a less crowded one. This may negate the usefulness of the reliable channels especially in saturated WiFi conditions. [10]

ZigBee also advertises to have a self-forming, self-healing mesh network topology [24]. This would in theory make the network more robust, as interference or error on one node would not affect the whole network. Traffic would then just be routed around the disabled node. However ZigBee mesh networks do not currently support beaconing, which is commonly used in fingerprinting positioning [23]. However for positioning with other technology than RF, this feature would help to create a robust and reliable WSN for necessary sensors and actuators.

5.3 Scalability

ZigBee can have up to 65.000 nodes per network, with support for star, tree and mesh topologies [23, 24]. ZigBee mesh networks, being also self-forming and self-healing, adds to the scalability of the technology, as human intervention in a ~10.000 node network would be inefficient and tedious. It is also considered to be, by design, a robust technology for WSNs in general [13].

Bluetooth traditionally consists of point-to-point connections with two devices of which one assumes the role of master and the other the role of slave. With this configuration, one master device can only support up to seven slave devices, which considerably restricts the scalability of

Bluetooth as a communication method. With Bluetooth v5.0 onward, also mesh topology is supported, which makes BLE a worthy competitor to ZigBee on the matter of scaling. Bluetooth mesh has 32.767 unicast addresses, and as such supports up to that amount of devices in a network. [14]

However, positioning with Bluetooth is commonly done with broadcasting BLE beacons, which have no real restrictions on scaling aspect. With ZigBee, positioning could be done similarly with a ZigBee tree network, which can send beacons on regular intervals. Other possibilities include ultrasound or infrared sensors and actuators with a large WSN, where the mesh capabilities of a technology are of great importance.

WiFi is scalable through it’s ubiquitous availability almost everywhere in urban areas. Considering that it does not require any additional hardware or setup other than radiomapping for fingerprint method, it is a very cheap and scalable technology. However, the popularity of WiFi is also problematic for positioning, as WiFi access points are not necessarly stationary. This can make fingerprint databases obsolete and inaccurate, without proper dynamic filtering methods or remapping. ZigBee home automation networks could also potentially be used opportunistically, similarly to WiFi.

5.4 Other viewpoints

There have also been multiple experiments on cross-technology communication (CTC) between Bluetooth, WiFi and ZigBee such as BlueBee, FreeBee, WEBee and LongBee. BlueBee is a system, which emulates ZigBee frames with a BLE radio by embedding a ZigBee frame in the Bluetooth message payload. As this does not need to repack payload from one technology to another, it is an efficient approach to CTC. WEBee is a similar technology, which emulates ZigBee frames with WiFi, instead of Bluetooth. [36-39]

FreeBee is a diverse multi-feature system, which aims to enable WiFi, Bluetooth and ZigBee CTC. It requires no additional hardware, is fully transparent to legacy devices and does not introduce dedicated traffic. This is implemented using mandatory beacons, which are widely adopted in wireless technologies. With this technology a mobile device could be located, by measuring RSSI values of WiFi devices with a ZigBee receiver, which consumes less power. It has also been documented to reduce power consumption of a WiFi network in a shopping mall use case by 78.9%, and should improve the reliability of all three technologies co-existing in the same environment. LongBee concentrates on increasing the range of WiFi to ZigBee transmissions to 300m outdoors and 100m indoors. This is considered 2x compared to state-of-the-art CTC and 10x compared to standard ZigBee communication. This is achieved using WEBee with down-clocked

WiFi and more effective transition coding mechanism. The down-clocked WiFi concentrates the WiFi Tx power, by shrinking the transmission bandwidth, and the improved transition coding mechanism improves the sensitivity of the receive,r by decreasing emulation induced defects in the signal. [36-39]

5.5 Relevance to HERE Technologies

HERE has BLE positioning system that is based on beacons and fingerprinting method. The method is described in more detail in Subsection 2.2.2. This should be a possible setup to be implemented with ZigBee also. If the premises, where positioning is implemented, has a home automation system with ZigBee, it could potentially use the ready-made network opportunistically similarly to WiFi positioning. Similar filtering or remapping methods would also be necessary in non-stationary ZigBee home automation devices as with WiFi for the same reasons.

Another suggested possibility involves using other positioning technologies, such as IR or ultrasound for positioning. These technologies also require possibly large WSN:s for complete positioning systems, which could be implemented with ZigBee. For this kind of purpose ZigBee should be a very viable technology as it allows large networks with self-healing and self-forming mesh topology. This kind of setup should also be possible with modern BLE as it also supports mesh networks. [23, 13, 24, 14]

Various CTC techniques could significantly lower power consumption of various communication or positioning systems. In addition, they could improve the co-existence of WiFi, BLE and ZigBee in the same environment and thus improve communication and positioning performance. It could also be possible to implement a more generic positioning service between these technologies utilizing CTC.

6. CONCLUSIONS

The subject of this thesis was to get an overall idea of ZigBee, and find information on it's abilities and possibilities on indoor positioning. ZigBee was found out to be a robust and low powered technology well versed for WSNs, which it is generally known for. It holds features, which allow it to be used as a positioning technology similarly to Bluetooth and WiFi. In addition it could potentially be used as an effective communication technology with other positioning technologies which need sensor or actuator networks, such as IR or ultrasound. The relevant features include RSS measurement of messages and support for large robust sensor networks.

Compared to WiFi, ZigBee is much more energy efficient as a technology, but as a positioning technology WiFi usually utilizes a ready-made infrastructure, which makes the positioning a free resource. ZigBee could also possibly utilize home automation networks similarly to WiFi, which would make both technologies free in positioning sense. Compared to BLE, ZigBee is very similar in features nowadays. Both support large mesh networks and can send regular beacons, which could be used in positioning. Also in power consumption these technologies are very close to each other. Regardless of technology, the trend seems to be that the most recent devices have the lowest power consumption. However another trend seems to suggest that power consumption levels could be somewhat manufacturer specific.

With respect to positioning solutions that HERE has already implemented, it should be feasible to port HERE BLE positioning system to ZigBee. In addition, FreeBee-like implementation of co-existence between these technologies could significantly improve power consumption and performance of positioning and communication systems in various environments.

REFERENCES

[1] H. Lim, et al., Zero-configuration indoor localization over IEEE 802.11 wireless infrastructure, Wireless networks Vol. 16, Iss. 2, February 2010, p. 405-420. Available: https://link-springer-com.libproxy.tuni.fi/article/10.1007%2Fs11276-008-0140-3

[2] N. E. Klepeis, et. al., The national human activity pattern survey (NHAPS): A resource for assessing exposure to environmental pollutants. Journal of Exposure Analysis and Environmental Epidemiology, Vol 11, July 2001, p. 231-252. Available: http://dx.doi.org.libproxy.tuni.fi/10.1038/sj.jea.7500165

[3] M. Uradzinski et al., Advanced Indoor Positioning Using Zigbee Wireless Technology, Wireless Personal Communications, Vol 97, Issue 4, August 2017, p. 6509-6518. Available: https://doi-org.libproxy.tuni.fi/10.1007/s11277-017-4852-5

[4] HERE-Developer web-page. Referred: 14.3.2019. Available: https://developer.here.com

[5] G. Oguntala et al., Indoor location identification technologies for real-time IoT-based applications: An inclusive survey, Computer science review, November 2018. Available: https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S1574013718301163

[6] Y. LeCun et al., Deep learning, Nature, Vol. 521, Iss. 7553, suppl. INSIGHT: MACHINE INTELLIGENCE, May 2015, p. 436-444. Available: https://search-proquest-com.libproxy.tuni.fi/docview/1685003444?pq-origsite=summon

[7] CH. Cheng, SJ. Syu, Improving area positioning in ZigBee sensor networks using neural network algorithm, Microsystem Technologies, January 2019, Available: https://doi-org.libproxy.tuni.fi/10.1007/s00542-019-04309-2

[8] International Telecommunication Union, Radio Regulations, Vol I: Chapter II: Article 5: Frequency allocations, Edition 2016. Available: https://www.itu.int/pub/R-REG-RR-2016

[9] IEEE P802.11 – Task Group AZ - MEETINGS UPDATE -webpage. Referred: 29.4.2019. Available: http://www.ieee802.org/11/Reports/tgaz_update.htm#GOAL

[10] R. Challoo et al., An Overview and Assessment of Wireless Technologies and Co-existence of ZigBee, Bluetooth and Wi-Fi Devices, Procedia Computer Science, vol 12, November 2012, p. 386 – 391. Available: https://doi.org/10.1016/j.procs.2012.09.091

[11] NXP Laboratories, Co-existence of IEEE 802.15.4 ad 2.4 GHz, November 2013. Available: https://www.nxp.com/docs/en/application-note/JN-AN-1079.pdf#%5B%7B%22num%22%3A12%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C70%2C295%2C0%5D

[12] HERE Technologies, HERE indoor component one-pager, 2017. Referred 22.3.2019. Available: https://www.here.com/sites/g/files/odxslz166/files/2018-11/HERE_Indoor_Component_one_pager.pdf

[13] R. Gheorghiu, V. Iordache, Use of Energy Efficient Sensor Networks to Enhance Dynamic Data Gathering Systems: A Comparative Study between Bluetooth and ZigBee, Sensors, January 2018. Available: https://search-proquest-com.libproxy.tuni.fi/docview/2108718163/fulltextPDF/FF0AF71CB6C641E4PQ/1?accountid=14242

[14] Bluetooth SIG, Mesh Profile Bluetooth specification, July 2017. Available: https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=429633

[15] Bluetooth Technology Website. Referred: 22.3.2019. Available: https://www.bluetooth.com/

[16] M. Karlsson, F. Karlsson, Cooperative indoor positioning by exchange of bluetooth signals and state estimates between users, 2016 European Control Conference, July 2016. Available: https://ieeexplore-ieee-org.libproxy.tuni.fi/document/7810492

[17] J. Hightower, G. Borriello, Location systems for ubiquitous computing, Computer, August 2001. Available: https://ieeexplore-ieee-org.libproxy.tuni.fi/document/940014/authors#authors

[18] J. Qi, G. Liu, A Robust High-Accuracy Ultrasound Indoor Positioning System Based on a Wireless Sensor Network, Sensors, November 2017. Available: https://search-proquest-com.libproxy.tuni.fi/docview/1977872559?pq-origsite=summon

[19] The official website of Philips Hue. Referenced: 28.3.2019. Available: https://www2.meethue.com/

[20] The official website of Samsun SmartThings. Referenced: 28.3.2019. Available: https://www.smartthings.com/

[21] Echo plus (2nd generation) – Amazon website. Referenced 28.3.2019. Available: https://www.amazon.com/All-new-Echo-Plus-2nd-built/dp/B0794W1SKP

[22] Official website of Ikea. Referenced: 7.4.2019. Available: https://www.ikea.com

[23] ZigBee specification revision 21, ZigBee Alliance, August 2015. Available: https://www.zigbee.org/zigbee-for-developers/zigbee-3-0/

[24] The ZigBee Alliance webpage. Referred: 7.3.2019. Available: https://www.zigbee.org/zigbee-for-developers/zigbee-3-0/

[25] 802.15.4-2011 - IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE, September 2011. Available: https://ieeexplore-ieee-org.libproxy.tuni.fi/document/6012487

[26] ZigBee Alliance, ZigBee Green Power, 2016. Referred: 20.3.2019. Available: https://www.zigbee.org/zigbee-for-developers/zigbee-3-0/#

[27] ZigBee Alliance, Securing the Wireless IoT, January 2017. Referred 20.3.2019. Available: https://www.zigbee.org/zigbee-for-developers/zigbee-3-0/#

[28] Texas Instruments, Z-Stack Developer's Guide, San Diego, California 2012. Referred: 27.3.19. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwiogZWQ36HhAhUsxqYKHVhnDW4QFjAAegQIABAC&url=https%3A%2F%2Fe2echina.ti.com%2Fcfs-file%2F__key%2Fcommunity-server-discussions-components-files%2F104%2F5633.Z_2D00_Stack-Developer_2700_s-Guide.pdf&usg=AOvVaw1HXg5OshAEip5MNWYiCPR3

[29] F. Shih-Hau, et al., An Enhanced ZigBee Indoor Positioning System With an Ensemble Approach, IEEE Communications Letters, April 2012. Available: https://ieeexplore-ieee-org.libproxy.tuni.fi/document/6156509

[30] Bluetooth SIG, Bluetooth core specification v5.1, January 2019. Available: https://www.bluetooth.com/

[31] Official site of Silicon labs. Referenced: 5.4.2019. Available: https://www.silabs.com

[32] Official site of Texas instruments. Referenced: 5.4.2019. Available: http://www.ti.com/

[33] Official site of Digi international. Referenced: 5.4.2019. Available: https://www.digi.com/

[34] Official site of Microchip Technology. Referenced: 5.4.2019. Available: https://www.microchip.com/

[35] A. Sikora, V.F. Groza, Coexistence of IEEE802.15.4 with other Systems in the 2.4 GHz-ISM-Band, 2005 IEEE Instrumentation and Measurement Technology Conference Proceedings, May 2005. Available: https://ieeexplore-ieee-org.libproxy.tuni.fi/document/1604479/authors#authors

[36] Z. Li, T. He, WEBee: Physical-Layer Cross-Technology Communication via Emulation, MobiCom '17, October 2017, p. 2-14. Available: http://doi.acm.org.libproxy.tuni.fi/10.1145/3117811.3117816

[37] S.M. Kim, T. He, FreeBee: Cross-technology Communication via Free Side-channel, MobiCom '15, September 2015, p. 317–330. Available: http://doi.acm.org.libproxy.tuni.fi/10.1145/2789168.2790098

[38] Z. Li, T. He, LongBee: Enabling Long-Range Cross-Technology Communication, IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, April 2018. Available: https://ieeexplore-ieee-org.libproxy.tuni.fi/document/8485938

[39] Z. Li, et al., Demo: BlueBee: 10,000x Faster Cross-Technology Communication from Bluetooth to ZigBee, MobiCom’17, October 2017, p. 486-487. Available: http://doi.acm.org.libproxy.tuni.fi/10.1145/3117811.3119855