Bluetooth Low Energy Industrial Sensor

Haithem Elhesseawy and Lamiaa Riad

Supervisors:

Stefan Höst (EIT) , Jens Jakobsen (HMS) and Jörgen Pålson (HMS)

Examiner: Maria Kihl (EIT)

LUND UNIVERSITY

Master Thesis

Lund, August 2018

Haithem Elhesseawy and Lamiaa Riad

Printed in Sweden by Tryckeriet i E-huset, Lund University, Lund.

Abstract

Industrial Internet of Things (IIoT) market is rapidly growing and expected to further expand in the incoming years. To keep up with such a fast pace, new wireless technologies need to be developed to accommodate the huge number of devices expected to connect to the internet. IIoT devices are designed to be low cost devices which operate in low power mode to provide long battery life time. In order to achieve so, low complexity and low power consumption algorithms are a must to be implemented that leads to new fields of research. Moreover, a robust, reliable, and secure network technology is required to support the IIoT devices connectivity and operation. Bluetooth Low Energy (BLE) mesh protocol has been developed to enable BLE devices to be a part of this enormous IIoT market. Other competing technologies are there as well in the market such as ZigBee and Low Power Wide Area Network (LPWAN).

This thesis studies the performance of the physical links among several BLE mesh nodes. Real world measurements in an industrial environment have been carried out (factory), then they are used to build an indoor path loss model, where Received Signal Strength Indicator (RSSI) values are measured. Furthermore, a comparison between theoretical and practical (based on measurements) path loss has been studied. Moreover, the probability of receiving packets successfully has been measured. As a result, we can briefly state that BLE mesh network can be a possible technology which supports the creation of a very reliable, secure, robust, and low power consumption if it is configured wisely.

Popular Science Summary

The current progress of industrial modernization leads to the need of monitoring and controlling large number of sensors to enhance productivity and quality. These sensors are used to measure temperature, pressures, air humidity, light, location, level of fluids, etc. Data is gathered either automatically over wired data acquisition systems or wireless in modern factories using Wireless Sensor Network (WSN). WSN is ideally suited for modern factories where enormous number of sensors need to reliably and securely communicate over the netwrok. Consequently, Industrial Internet of Things (IIoT) concept has been established.

IIoT is a part of Internet of Things (IoT) technology which aims to enable the controlling and monitoring of smart devices in the industrial environment using the internet. The development of industrial WSNs opens the door to considerable challenges for the wireless market, such as the necessity of low power consumption, low cost and simple reliable secure technology. One of these wireless technologies is Bluetooth.

Bluetooth originally released in 2000 to act as a cable replacement technology by enabling two devices to communicate wireless and form a 1-to-1 network topology. Due to the rapid growth in the IIoT market and the need to have more devices connected together via a wireless technology, Bluetooth Low Energy (BLE) emerged in 2010.

BLE is optimized to consume as low energy as possible. It has different means of communication, either 1-to-1 topology or a 1-to-many (star), where one device can communicate with several devices. The main disadvantage of such connections setup is that all communications have to pass through one main unit and in case of its failure, the whole network connections will be dropped.

Lately, in 2017 a new Bluetooth mesh protocol has been developed to overcome the disadvantages of the existing star networks. This is accomplished by allowing BLE devices to work in mesh topology that provides multi-paths to the target device instead of the former peer-to-peer communications. Bluetooth mesh protocol enables many-to-many communication and it is optimized in a way to create a large-scale device network with an unlimited coverage area.

Bluetooth mesh protocol is ideally suited for building automation, sensors networks, and for any solution that requires tens, hundreds, or thousands of devices to reliably and securely communicate with one another. Within this thesis, analysis of Bluetooth mesh protocol has been executed, and some of its features have been highlighted and a practical model of received signal power for mesh network devices has been constructed.

Acknowledgments

We would like to thank HMS in Halmstad, Sweden for giving us the opportunity to write our thesis within its premises. Moreover, special thanks to our supervisors, Stefan Höst, Jörgen Pålson and Jens Jakobsen for their continuous supervision, feedback, comments and advice through the whole thesis. Without their support, the finding of this thesis would have been impossible. Finally, we are grateful to all of our family and friends that have shown support along the way.

Haithem Elhesseawy
Lamiaa Riad

Contents

List of Figures

List of Tables

Acronyms and Mathematical Notations

ACK	Acknowledged
AD	Advertising Data
ATT	Attribute Protocol
AWGN	Additive White Gaussian Noise
BLE	Bluetooth Low Energy
BR	Basic Rate
CRC	Cyclic Redundancy Check
EDR	Enhanced Data Rate
EIT	Electrical and Information Technology
FDMA	Frequency Division Multiple Access
GAP	Generic Access Profile
GATT	Generic Attribute Profile
GFSK	Gaussian Frequency Shift Keying
GUI	Graphical User Interface
HCI	Host Controller Interface
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISM	Industrial, Scientific and Medical
L2CAP	Logical Link Control and Adaptation Protocol

LCI Lower Confidence Interval
LL Link Layer
LOS Line Of Sight
LPN Low Power Node
LSB Least Significant Bit

MPCs Multi Path Components

NACK Unacknowledged
NLOS Non Line Of Sight

PDU Protocol Data Unit
PHY Physical Layer

RSSI Received Signal Strength Indicator
Rx Receiver

SIG Special Interest Group
SMP Security Manager Protocol

TDMA Time Division Multiple Access
TTL Time To Live
Tx Transmitter

UCI Upper Confidence Interval
UUID Universally Unique Identifier

1 Introduction

Within this thesis, the new Bluetooth mesh protocol which has been released in 2017 is analyzed. This new Bluetooth mesh profile can be applied to any Bluetooth Low Energy (BLE) device with a simple firmware update.

This chapter gives a brief background and presents the overall structure of this thesis. Furthermore, it is intended to give a clear illustration of the purpose, problem definition and methodology for the work that has been performed during this thesis.

1.1 BACKGROUND

Nowadays, a fast-growing Internet of Things (IoT), promises to establish smart environments. These include a variety of applications such as home automation, traffic congestion, smart roads, etc., as shown in Figure 1.1. One of the most important applications of the IoT are the ones related to industrial environment aiming to improve manufacturing and industrial operations. In IoT industrial applications, a broad number of machines are connected together to allow a machine-to-machine communication, in order to gather and transfer data. One of the most available and popular wireless technologies for short-range machine-to-machine communications is Bluetooth.

Bluetooth is a wireless communication technology for exchanging data over a short distance. Bluetooth technology was developed in 1994 at Ericsson to replace the wired communication between devices. Moreover, Bluetooth communication is characterized by robustness, low power consumption, reliability, and low cost. However, due to the rapid growth in the Industrial Internet of Things (IIoT) market and the need for more connected devices that enables devices to minimize power usage, Bluetooth Special Interest Group (SIG) in 2010 made a noticeable change in its protocol stack and introduced another version

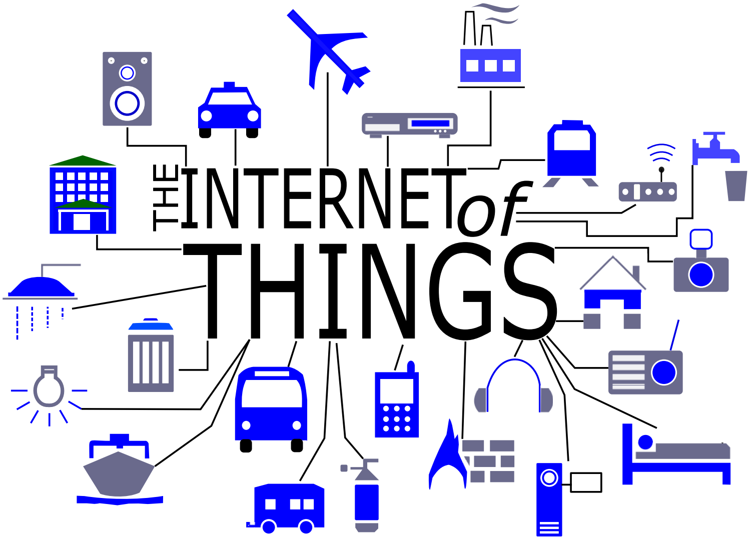


Figure 1.1 IoT applications.

of Bluetooth which is BLE.

BLE is a new and smart wireless technology which aims to comply with IIoT fundamental requirements. BLE supports a mesh networking, enabling many-to-many devices communications as a replacement of the former peer-to-peer communication to extend the network range. BLE mesh creates IIoT solutions where tens, hundreds, or thousands of devices need to reliably and securely communicate with one another.

In mesh network, the connected devices have the capability to relay the messages not destined to themselves. Consequently, the network range is extended. Another advantage of the mesh topology is that any two devices belong to the network can communicate directly with each other without any need to communicate with a master device first. The BLE mesh protocol is considered as a software update, this means that there is no need to add any extra hardware. This protocol is used to upgrade the modern Bluetooth devices in order to have the ability to establish mesh networks.

1.2 PROBLEM DEFINITION

In recent years, there has been an increasing interest in designing and implementing BLE mesh networks in factories, but in order to do that the quality of the communications link between different BLE devices needs to be studied, in order to specify the position of each BLE device for high performance mesh networks and do network performance simulations for BLE networks. Industrial environments have particular signal propagation characteristics that not exist in typical office or residential environments. There are different factors that can degrade the performance of wireless communication systems in industrial environments, which they are often characterized by metallic objects and large dimension machines. Moreover, the signal propagation also depends on the movements of tools, rotating machines and persons.

All of the previous factors affect on signal propagation and increase multi-path propagation. That is why it is highly important to study the link performance between any two BLE devices. Also, with the link knowledge of attenuation, and especially packet error probability, it is possible to set up a computer simulation model. Consequently, the main aim of this Master thesis work is to analyze the link performance properties between two BLE devices and create a complete model that describes that link and how the signals affected by the surrounding environment to enable BLE users to create a BLE mesh network. Therefore, in order to effectively study the link performance, industrial measurements were taken. There are three types of measurements were carried out in HMS factory to analyze the link performance characteristics:

- Received Signal Strength Indicator (RSSI) to build path loss models that explain the industrial environment effects on the received signal power.
- Object signal loss to see the radio signal performance if BLE devices are put inside the machine to detect temperature and how this machine affects this signal.
- Probability of receiving packets successfully to study the probability of packets being successfully received between two BLE devices at different distances and areas.

1.3 METHODOLOGY

This thesis is written as collaboration between the department of Electrical and Information Technology (EIT) of Lund University and HMS Industrial Networks company in Halmstad. In order to achieve the thesis goals, the following steps are carried out:

- Be familiar with Bluetooth technology especially with the new Bluetooth mesh specifications.
- Study the behavior of radio signals propagation in an industrial environment.

- Analyze the empirical path loss models for indoor propagation focusing on BLE mesh characteristics.
- Measure the RSSI in HMS factory (real industrial environment).
- Estimate and build an appropriate path loss model based on the measured values and fit it with the empirical models.
- Take object signal loss measurements to give a guide of the type of loss due to blocked objects
- Calculate the probability of successfully receiving packets transmitted between any two nodes in Bluetooth mesh network.

1.4 THESIS OVERVIEW

The rest of this thesis is organized as follows:

- **Chapter 2:** Introduces the theory of the BLE and the BLE mesh network.
- **Chapter 3:** Presents an overview of the radio wave propagation characteristics in the industrial environment.
- **Chapter 4:** Describes the Received Signal Strength Indicator (RSSI) measurement setup, hardware characteristics, object signal loss measurement and probability of successfully receiving packets measurements.
- **Chapter 5:** Presents and discusses the results of the measurements.
- **Chapter 6:** Concludes with a summary of the thesis results and future work.

2

Bluetooth Therotical

This chapter describes briefly the Bluetooth and BLE, then it provides an overview of the Bluetooth mesh features, concepts, and fundamentals. During this chapter, Bluetooth core specification version 5.0 [13], and Bluetooth mesh specification version 1 [14] are used as references.

2.1 BLUETOOTH

Bluetooth is a short-range wireless communication technology which aims to achieve a low cost and low power consumption. Bluetooth contains two main systems, Basic Rate (BR), and low energy. The BR also includes Enhanced Data Rate (EDR) as an option. the BR/EDR systems are known as classic Bluetooth, while the low energy system is called BLE which will be further explained in Section 2.2. Any Bluetooth device can operate using either one or both systems. In order to utilize all system features, both communicating devices must operate using the same system.

The Bluetooth operates in the unlicensed Industrial, Scientific and Medical (ISM) band at 2.4 GHz. It uses a frequency hopping transceiver to combat multi-path interference and fading. The BR supports a maximum bit rate of 1 Mbps, while the EDR supports a higher bit rate of 2 or 3 Mbps, furthermore, the BLE has similar bit rate to BR of 1 Mbps.

Communication between different Blutooth devices mainly depends on its supported Bluetooth profile. The Bluetooth profile defines which features of the core specifications to be used based on the needed application. For example, in audio/video remote control, the profile provides a standardization to control Tv, Hi-Fi, and any other types of Bluetooth equipment that can be controlled by a remote. For a successful operation, both devices, namely TV and remote control, must support the same protocol. As well as, in Bluetooth technology, there exists another profile called Generic Access Profile (GAP), which has to be supported by all Bluetooth devices.

In Bluetooth technology, any transmitted packet contains a transmitter (Tx) field which defines the device transmitting power value. Besides that, most of the industrial Bluetooth devices have the ability to measure RSSI values which can be used to specify the location of the transmitter.

2.2 BLUETOOTH LOW ENERGY

BLE has been developed in 2010 and introduced for the first time in core specifications version 4.0. It has been built over the classic Bluetooth to enable the integration of products that require lower power consumption, lower cost, and lower complexity than the classic Bluetooth could offer.

2.2.1 BLE PROTOCOL OVERVIEW

The BLE protocol stack composed of three blocks (Application, Host, and Controller), each block contains other layers as shown in Figure 2.1 [1] [2].

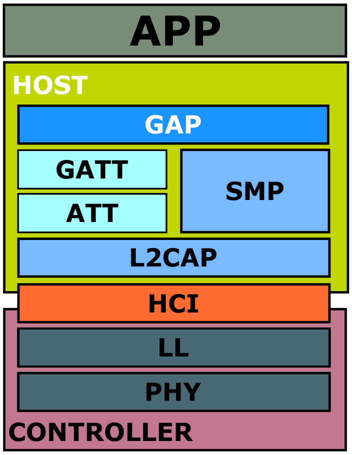


Figure 2.1 BLE protocol stack [1] [2].

- The Application block: it represents the direct interface with the user.
- The Host block contains the following layers:
  - GAP
  - Generic Attribute Profile (GATT)
  - Logical Link Control and Adaptation Protocol (L2CAP)

  - Attribute Protocol (ATT)
  - Security Manager Protocol (SMP)
  - Host Controller Interface (HCI), Host side

- The Controller block includes the following layers:
  - HCI, Controller side
  - Link Layer (LL)
  - Physical Layer (PHY)

For the purpose of this thesis, only GAP, GATT,the physical layer and link layer are described briefly. Interested readers may refer to the Bluetooth core specification version 5.0 [15] to understand the functionality of each layer in details.

2.2.1.1 GAP PROFILE

This layer is used to define the common base functionality between all Bluetooth devices such as device roles, modes, and procedures, moreover, it manages connection establishment and security. For BLE, GAP defines four roles which listed as follows [16] [1]:

- **Broadcaster (Advertiser):** It is a device that periodically transmits advertising data over the advertising channels to any device(s) within its radio range. This device works either as a transceiver or operates as a transmitter.

- **Observer (Scanner):** It is a device that continuously scans the advertising channels at periodic intervals, looking for any advertising data from any broadcaster. This device works either as a transceiver or operates as a receiver.

- **Central (Master):** It is a device that scans for connectible advertising data and establishes the connection. When the connection is active, the central defines all the setting required for data exchange. Here, it must have both transmitter and receiver.

- **Peripheral (Slave):** It is a device periodically transmits connectible advertising data and accepts connections established by the master. Upon connection establishment, it follows the settings introduced by the central and exchanges data with it. This device is similar to the Master one and it consists of both transmitter and receiver.

The broadcaster and observer roles are used in the connectionless (broadcasting) communication between two devices to exchange data. While the master and slave roles are used in the connected communication to establish the connection between devices and exchange data.

2.2.1.2 GATT PROFILE

Its main function is to define how different profiles information and data could be exchanged between BLE devices. There are two roles defined for any device implementing GATT, which are [1]:

- **Client:** It is the device that sends commands and requests to the server and can receive responses, indications and notifications sent by the server.
- **Server:** It is the device that accepts incoming commands and requests from the client and can send responses, indications and notifications to the client.

Any device can act in both roles at the same time.

2.2.1.3 PHYSICAL LAYER

BLE uses Frequency Division Multiple Access (FDMA), and Time Division Multiple Access (TDMA) techniques. In FDMA, the BLE ISM band is split into 40 channels with 2 MHz separation between them as shown in Figure 2.2. Three of these channels are used in data broadcasting (advertising) for connectionless communication between devices, while the others are used in data exchanging after establishing the connection between devices. The advertising channels (37,38,39) have been selected to be between the Wi-Fi technology channels to reduce the interference [16] [1] [13].

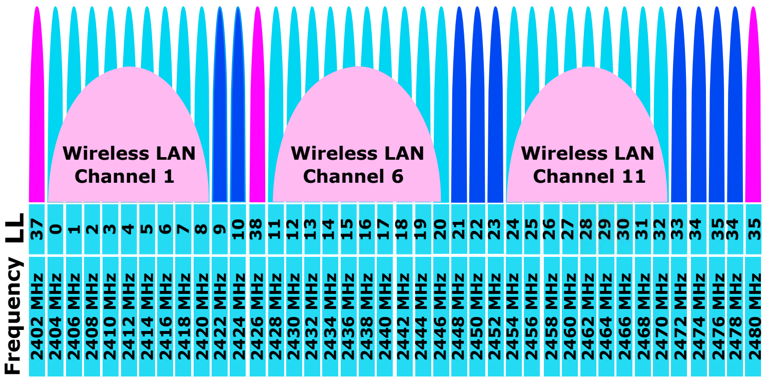


Figure 2.2 BLE channels.

In TDMA, each channel is subdivided into time slots called events. There exists four types of events: Advertising, Extended Advertising, Periodic Advertising, and Connection events. BLE packets are sent within these events. Moreover, when one device wants to transmit a packet, it sends that packet at a predetermined time and the receiving device should wait for a certain defined interval before it replies back. The modulation used in BLE is Gaussian Frequency Shift Keying (GFSK) where 0 and 1 are represented by a negative and positive frequency deviation of 185 kHz, respectively, as illustrated in Equation 2.1 [13].

$$\begin{aligned} f_1 &= f_c + \Delta \\ f_0 &= f_c - \Delta \end{aligned} \tag{2.1}$$

where f_c is the Carrier frequency and Δ is the frequency deviation.

Bluetooth core specification version 5.0 [15] defines the transmitting power to be in the range of -20 to 20 dBm. In addition, minimum receiver sensitivity needs to be -70 dBm. Moreover, the maximum bit error rate should be 0.1 percent.

2.2.1.4 LINK LAYER

The Link Layer is responsible for advertising, scanning, creating and establishing connections. It is also responsible for packets structure. Data that is transmitted between two link layer requires a special packet format that consists of 80 to 2120 bits. The BLE packet format structure is as shown in Figure 2.3, which is used for both advertising channel packets and data channel packets. Each packet consists of four components which are Preamble, Access Address, Protocol Data Unit (PDU), and Cyclic Redundancy Check (CRC). The Preamble is transmitted first, followed by the Access Address, followed by the PDU followed by the CRC [13].

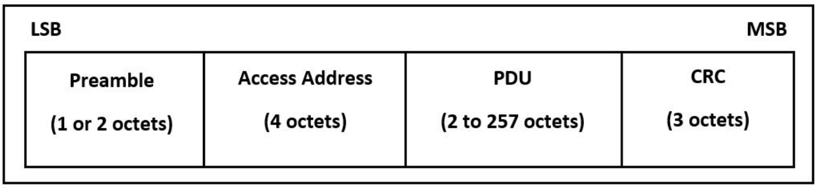


Figure 2.3 Link Layer packet format.

The packet components are described as the following:

- Preamble: It is used in the receiver to perform frequency synchronization to enable the receiver to decode the transmitted signal correctly and mark the start of the packet. The preamble consists of 1 octet and is either 01010101 or 10101010 depending on the access address. If the Least Significant Bit (LSB)of the access address is 1 then 01010101 is used, otherwise 10101010 is used.

- Access Address: It consists of 4 octets and identifies the communication on a physical link. It is used to prevent packets directed to different receivers. The Access Address in data channel packets shall be different for each Link Layer connection between any two devices, while it is the same for all advertising channel packets.

- PDU: It ranges from two to 257 octets, and the PDU length depends on the type of communication used. When a packet transmitted on either the primary or secondary advertising channel, the PDU shall be the Advertising Channel PDU. When a packet transmitted on the data physical channel, the PDU shall be the Data Channel PDU.

- CRC: It consists of 3 octets , checks the bit errors in the packet and analyses the PDU only, which could have generated during packet transmission. The CRC shall be calculated on the PDU field in all Link Layer packets. If the PDU is encrypted, then the CRC shall be calculated after encryption of the PDU has been performed.

2.2.2 ADVERTISING

Advertising is broadcasting a packet on one or more of the three advertising channels. Any scanning devices within the radio range of the broadcaster are able to receive the advertised packet. Advertising is used mainly for two purposes: to enable devices that are not connected together to exchange data in form of advertising packets, and to establish a connection between two devices [16] [2].

Advertisement data is sent over the GAP profile with a packet size of 31 bytes only, it can be controlled using the following timing parameters as shown in Figure 2.4:

- **Advertising Interval (advInterval):** It defines the rate at which the advertising packets are sent. During each advertising interval, the same advertising packet will be sent over the three advertising channels.

- **Scan Interval (scanInterval):** It defines the rate at which the radio of the scanner device will be on. In each scan interval the scanner changes the scanning channel.

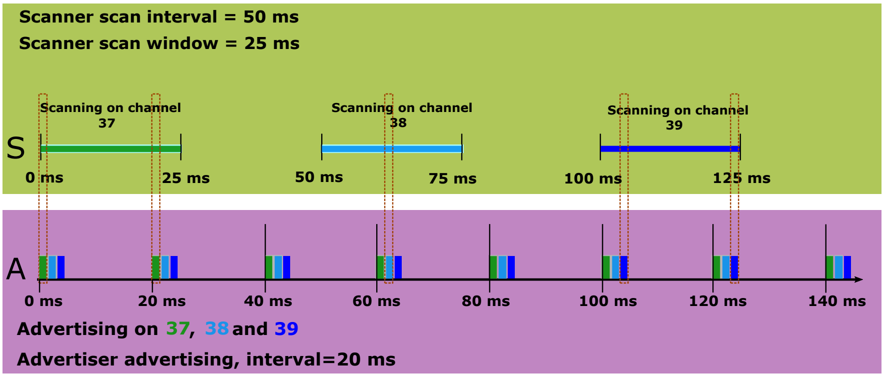


Figure 2.4 Timing parameters.

- **Scan Window:** It defines the time that the receiver radio keeps on scanning per each scan interval.

2.2.3 NETWORK TOPOLOGY

The BLE supports two types of network topologies, star, and scatternet. Star topology is composed of a master and multiple slaves, where there must be a connection between the master device and each slave. Scatternet consists of several star topologies, at each star topology, one of the slave's has to act as a master and a slave at the same time to connect several star topologies together as shown in Figure 2.5 [17].

Those topologies suffer from many limitations such as short coverage distance between two nodes, as well as, they enable only one-to-one and one-to-many communication, besides that, they have a single point of failure.

2.3 BLUETOOTH MESH

Bluetooth mesh is a network technology not a wireless communication technology, at which many-to-many devices communicate at the same time with efficient power consumption, that is done by introducing new nodes roles and messages. Bluetooth mesh stack is built over the BLE stack version 4.0 or higher. In other words, Bluetooth mesh profile is built on broadcasting the data over the BLE advertising channels, which means that Bluetooth mesh uses the physical layer of BLE to exchange data with different devices [14].

Bluetooth mesh is a connectionless communication that has certain types of messages that can be sent and received by nodes. Blutooth mesh is not meant for standard communication like classic Bluetooth which in turns means, audio, video and other personal data can't be shared over a Bluetotth mesh net-

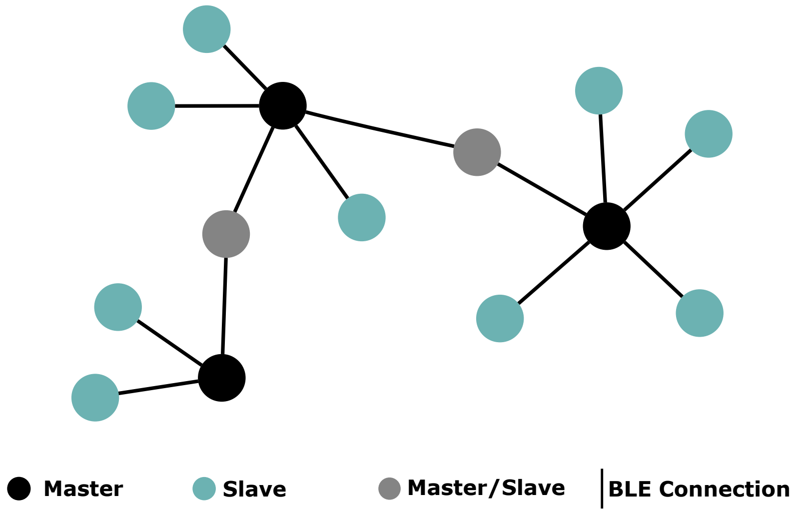


Figure 2.5 Scatternet topology

work. It is a technology that can be applied to any BLE device via a software update. This update allows that device to work in a mesh topology.

2.3.1 BLUETOOTH MESH BASICS

This Section provides a brief overview of Bluetooth mesh basic concepts in order to clarify its mode of operation.

2.3.1.1 PROVISIONING

Provisioning is the process at which new device is added to the mesh network. The device that is not part of the mesh network is called unprovisioned device, once it is added to the network, it is called provisioned node. The provisioner is the device that manage the provisioning process it could be mobile, pc, or tablet. Provisioning process passes through 5 steps [14], as follows:

- **Step 1**: The unprovisioned device broadcasts advertising packets (Mesh Beacons) through all three advertising channels.The mesh beacon payload is included within a Bluetooth GAP Advertising Data (AD) Types called the mesh beacon AD. This is done in several ways based on the device, for example, holding down a button for a certain time.

- **Step 2**: Once the provisioner receives the advertising packets from the unprovisioned device, it sends a provisioning invite PDU, then the unprovisioned device replies with its specific information, like, manufacturer, operating temperature, and its MAC address.

- **Step 3**: Public keys are exchanged between the provisioner and the unprovisioned devices.

- **Step 4**: During this step, the user will notice that the unprovisioned device generates a random single or multiple digit numbers in a a way that depends on its capabilities. For example, the unprovisioned device may flash a LED or produce a beep sound several times. These random digits must be entered to the provisioner by the user. To complete the authentication process between the two devices, cryptographic are exchanged using the random digits takes place.

- **Step 5**: The session key is derived by the provisioner and the unprovisioned nodes from the exchanged public keys in step 3, and their private keys. The session key is used to secure sending the required data needed to complete the provisioning process. These data include network Netkey, IV index which is a mesh security parameter, and a unicast address allocated only for this device. Now the device is provisioned and it is called a node.

2.3.1.2 ELEMENT

The element is referred to a part of the node that awaits to be controlled. Each node has one primary element, and can hold up to many other secondary ones. Each element holds a unique identification address. For example, if there is a measuring device that contains two sensors, then it has two elements, one of them will be identified as the primary, while the other is the secondary. The primary element is specified as the first sensor that get its address during the provisioning process [14].

2.3.1.3 STATE

The state is a value used to describe element condition. For example, if there is a lamp, its state will be either on or off.

2.3.1.4 MESSAGES

In Bluetooth mesh, nodes communicate with each other's using only three broad types of messages (get, set, and status) which used to either specify or modify the element state and will be explained shortly. Messages are defined using the opcode. They can be either Acknowledged (ACK) messages where a reply from the target destination is required, or Unacknowledged (NACK) message where a reply is unneeded [14].

During ACK process, acknowledged message timeout needs to be specified by the application which is defined as the total message transmission interval including original message interval with its retransmissions if it has been configured. Upon the expiry of acknowledged message timeout with no successful acknowledgment, message transmission failure is considered. Hence, if retransmission is configured by the application, then a retransmission timer needs to be defined which is smaller than acknowledged message timeout. The exact value of the acknowledged message timeout varies between different applications and it should be selected to be greater than or equal to 30 seconds.

- **Get message**: This message request the value of a given state from single or multiple nodes. A Status message is the response to this get message and it contains the state value information.
- **Set message**: This message is used to change the value of a given state in a particular element. An ACK Set message results in a status message which is returned in response to the Set message.
- **Status message**: It is a replay message for the Get message request, ACK Set message request or NACK Set message request.

2.3.1.5 MODELS

Models are used to define the functionality and behavior of any node inside the mesh network. This is done by defining the element state, types of used messages, and how these messages will change nodes states. Three model categories are used in Bluetooth mesh models which can be shortlisted as Server, Client, and Control. For example, if there is a LED that is controlled by an on/off switch, then the LED is a server, while the switch is a client [14].

The Bluetooth mesh communication is a client-server architecture, in other words when a client communicates, it must communicate with a server, and vice versa. Models can be adopted and defined by either Bluetooth SIG or any other vendors. The models defined by vendors are called vendor models which are 32 bits in length, while the others are called SIG adopted models which are 16 bits in length [14] [3].

- **Server model**: It consists of a single or several states cover either one or more elements. It also defines a set of messages, element behavior while sending or receiving such messages, and any behavior that might happen afterwards.
- **Client model**: It does not have any definitive state, but it determines the messages that can be sent by the client to get, change, or use the states of the corresponding server.
- **Control model**: It may contains client model and server model functionalities, which is used to provide communication between server and

client models. It may also contain control logic, which is defined by specific rules that help to coordinate between other models connected to control one. Control model can be shown in Figure 2.6.

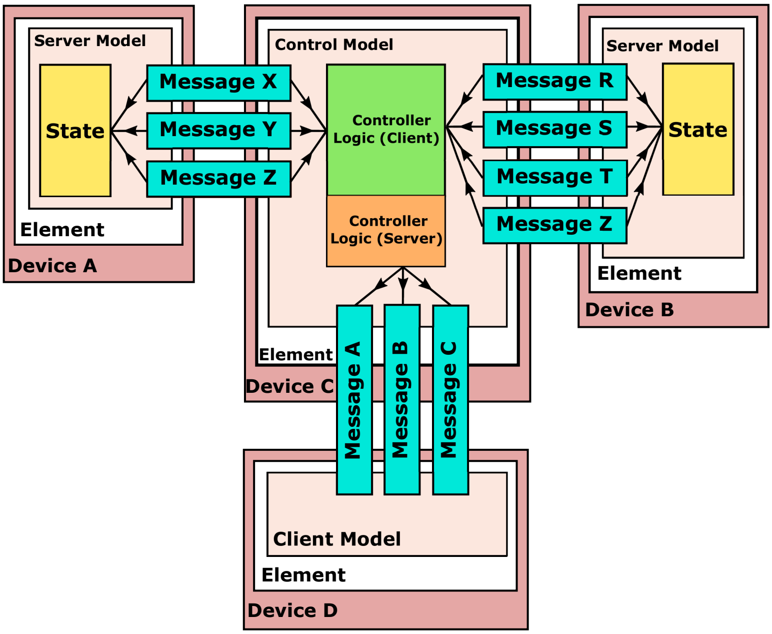


Figure 2.6 control-model communication [3].

2.3.1.6 ADDRESS

In Bluetooth mesh, any message has to be sent and received using specified address. Bluetooth mesh defines three types of address which are, unicast, virtual, and group [14] .

- **Unicast Address:** It is a unique address that is assigned to a single element in a node during the provisioning process to identify it. There are 32767 unicast addresses available for each mesh network.
- **Group address:** It is a multicast address which represents one or more elements in one or multiple nodes. When a message is sent from a node to a group address, all the elements subscribed in that group will receive this message. Group addresses are divided into two sets, one set is defined by SIG which is called SIG fixed group addresses, while the other is called dynamically assigned group addresses. Fixed group addresses contain four subgroups (All-Proxies, All-Nodes, All-Relays,

All-Friends), which are used to address multiple nodes based on their functionalities. Dynamically assigned group addresses have to be set up by the user using the configuration application, which is used to assign any user-defined elements in one group. There are 256 fixed group addresses and 16128 dynamically assigned group addresses for each mesh network.

- **Virtual address:** It is a multicast address which represents one or more elements in one or multiple nodes. Virtual addresses take the form of a 128-bit Universally Unique Identifier (UUID) value, which is more like a label. There are about seventy trillion virtual addresses for each mesh network. It can be used to assign all products of a given manufacturer in one group for easier addressing. For example, assigning all the sensors made by HMS company in one group named HMS.

2.3.2 BLUETOOTH MESH LAYER ARCHITECTURE

The Bluetooth mesh stack contains seven layers implemented over the BLE stack as shown in Figure 2.7. Each layer will be explained later in this section [3].

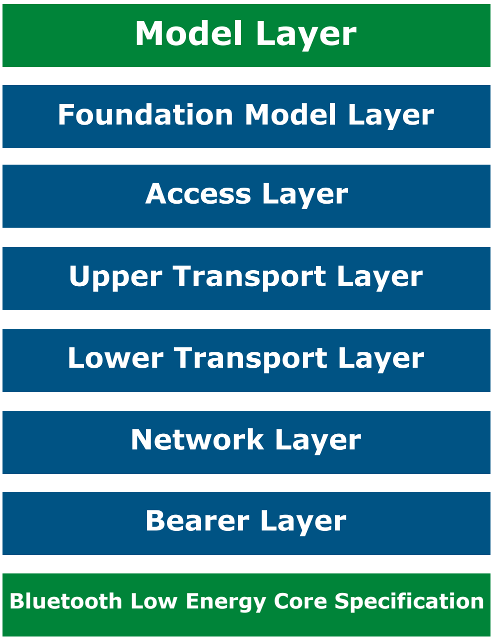


Figure 2.7 Bluetooth mesh Layers [3].

2.3.2.1 MODEL LAYER

The Model Layer defines models mentioned in Section 2.3.1.5 that are used to standardize the users operations for different scenarios.

2.3.2.2 FOUNDATION MODEL LAYER

The Foundation Model Layer defines the states, models, and messages needed to configure and manage a mesh network.

2.3.2.3 ACCESS LAYER

The Access Layer is responsible for defining how applications can make use of the upper transport layer, this done through:

- Application data format definition.
- Encryption and decryption process definition and control which is performed in the upper transport layer.
- Verifying that the received data from upper transport layer belongs to the right application and network before forwarding it.

2.3.2.4 UPPER TRANSPORT LAYER

The Upper Transport Layer handles transport control messages between different transport layers of different peer nodes, also, it is responsible for encryption, decryption, and authentication of application data passing through access layer processed here.

2.3.2.5 LOWER TRANSPORT LAYER

The Lower Transport Layer sends the PDU from the upper transport layer to the lower transport layer of the other device. If the PDU from the upper transport layer is longer than 31 bytes, the lower transport layer will perform segmentation to split that PDU into smaller PDUs. This process enables long messages to be sent over the advertising bearer. When the other device lower transport layer receives the segmented PDUs, it will reassemble it again into a single upper transport layer PDU, then forward it to the upper layers.

2.3.2.6 NETWORK LAYER

The Network Layer defines the network message format to support the PDUs to be transported by bearer layer. At this layer, the implementation of the proxy and relay features, which will be discussed later (see Section 2.3.3), take place. Moreover, various message address types are defined which has been introduced earlier in Section 2.3.1.6.

Within this layer, input and output filters are applied to the data. Initially, input filter processes the messages and decides either to drop them or to further process them by network layer. On the other hand, the output filter is used to control the processed messages (either dropped or could be delivered to the bearer layer).

2.3.2.7 BEARER LAYER

The Bearer Layer defines how network messages are exchanged between different nodes. Two bearers are defined by the bearer layer, the advertising bearer and the GATT bearer.

The advertising bearer is the main bearer. It uses the BLE GAP advertising and scanning features, to transmit and receive mesh PDUs. Any node depends only on the advertising bearer must support both GAP observer and broadcaster roles. Additionally, passive scanning is done with 100 percent duty cycle, to avoid missing any mesh or provisioning PDUs.

The GATT bearer enables nodes, that do not support the advertising bearer to communicate indirectly with any node which is part of the mesh network, through the proxy node using the proxy protocol.

2.3.2.8 BLUETOOTH LOW ENERGY CORE SPECIFICATION

Within this layer, BLE full stack is contained which has been defined in Bluetooth core specifications version 4.0 or higher, to clarify how BLE is supposed to communicate at the lower layers [13].

2.3.3 NODES FEATURES

All nodes in any Bluetooth mesh network could send and receive messages at any time. As well as, these nodes have four features (proxy, relay, low power, and friend) which give the node susceptibility to hold more responsibilities, rather than sending and receiving. A node may support zero or more of these features, any supported feature can be enabled or disabled on the node.

- **Relay node:** A node that supports and enables the relay feature. Relay node has the ability to relay/retransmit the received mesh messages to all neighbors, over the advertising bearer. It plays the main role in extending the communication range of the Bluetooth mesh network, by allowing devices that are not in radio range to communicate.

  The relay node should scan with 100 percent duty cycle to avoid missing any mesh messages that should be relayed, which means, it should not be operated by a battery. In addition, when a relay node receives a mesh message, it should wait for a short random time before relaying that message to avoid collisions between relay nodes that received the message at the same time. Any message can be relayed up to a maximum of 126 times.

- **Proxy node:** A node that supports and enables the proxy feature. Any proxy node has the ability to exchange messages between the advertising bearer and the GATT bearer using the proxy protocol. This node enables BLE devices that do not have mesh stack to communicate with devices which is a part of a Bluetooth mesh network.

- **Low Power Node (LPN):** A node that supports and enables the low power feature. The low power feature helps nodes which are powered by batteries and transmits a few messages such as sensors to minimize their power consumption as much as possible. This process is done by forcing the device to be in sleep mode all the time and only wakes up upon messages transmission.

  A node cannot have the low power feature enabled unless it is supported by another node that has the friend feature enabled. The process of supporting LPN by a friend node is known as friendship. Furthermore, each LPN can have friendship relation with only a single friend node.

- **Friend node:** A node that supports and enables friend feature. The friend node role is to support LPN during sleeping mode, by storing any messages that is sent to the LPN. Once the LPN moves into a wake up state, it automatically requests a message update from the friend node. Friend node replies with all the stored messages received during LPN sleeping time one by one. A friend node can have friendship relation with a maximum of seven LPNs based on device hardware capabilities.

2.3.4 MESSAGES REPETITION

Within Bluetooth mesh, there exists some types of NACK messages. If one of those messages has been transmitted, it is impossible to decide whether the message is received correctly or not. This can be considered as an issue, especially for critical data.

To increase network reliability and the probability of successfully receiving transmitted messages for both NACK and ACK messages, Bluetooth mesh allows messages retransmission at the message source, and every relay node. Bluetooth mesh enables the user to control the retransmission of messages by defining the transmit count and the interval. Initially the transmit count represents the number of required message repetitions, while the transmit interval stands for the time between two successive retransmissions, which should be in steps of 10 ms.

2.3.5 MESSAGES DELIVERY

Bluetooth mesh uses a technique called "Managed Flooding" which is based on the flooding technique to transmit and relay messages.

Flooding means that message is not going to be routed to a specific destination through a certain path. Instead, the message is broadcasted such that all neighbor nodes within the radio range will be able to receive it. Then, only relay nodes will be able to further broadcast the message.

Flooding technique strength lies on its ability to remove the need of a central network node, which leads to complete network unavailability upon its failure. In addition, the message will be delivered to the target node via multiple paths so if one path is interrupted, others exist to deliver the message to its destination. This highly increases network reliability. Regardless the benefits provided by flooding technique, it still leads to increase network payload. It has infinite loops and it causes network inefficiency since messages will be propagated beyond its target node(s).

Managed flooding is designed to optimize the performance of flooding technique without losing its strengths. This is achieved by using three measures (Time To Live (TTL), Heartbeat, and message cache) to restrict the flooding process.

- **Heartbeat:** It is a message that is transmitted periodically by all nodes, with exception of low power ones. Heartbeat message is used to indicate to the other nodes in the network that the heartbeat transmitter still alive. The receiving nodes make use of the data contained in the heartbeat message in order to define how far the sender is in terms of the number of hops which is used by TTL field.

- **TTL:** It is a field that can be found in all mesh messages. The TTL is used to prevent the messages from being relayed further than their destinations, by limiting the number of hops a message can be relayed over it. Each time a relay node receives a message that needs to be relayed, it decrements the value of the TTL by one, before the message is being relayed. The maximum value of the TTL field is 126 hops.

- **Message cache:** It is a cache list that all nodes have, which contains all recently received messages. The number of messages that can be stored in the cache list is limited by its implementation, to prevent it from becoming too long.

  When any node receives a message, it will be compared with all the messages stored in the cache list. If it already exists, it will be discarded, if not, then the message will be processed and the cache list will be updated. The cache list is used to prevent the relay nodes from relaying already relayed messages, which will decrease the network payload and make it more power efficient.

2.3.6 FRIENDSHIP

Friendship is a special relation between the LPN and the friend node, this relation goal is to help the LPN to conserve power and at the same time not to miss the messages sent for it. These messages may include the network security messages, at which if the LPN fails to keep up-to-date with it, it will be dropped off from the whole network.

Friendship defines three main parameters that do not change during all the relationship duration (ReceiveDelay, ReceiveWindow, PollTimeout). The friendship procedure is divided into two processes, the friendship establishment, and the friendship messaging as shown in Figure 2.8. The friendship procedure can be summarized in the following steps:

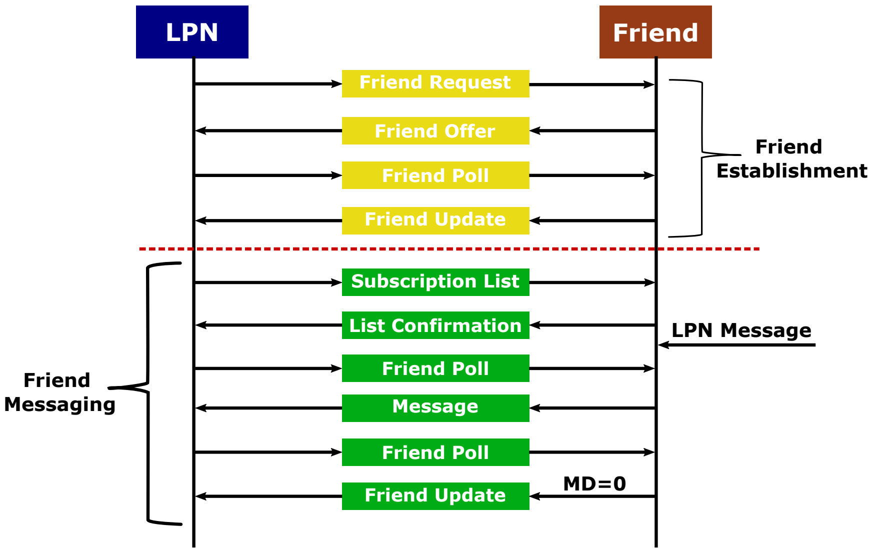


Figure 2.8 Friendship procedure.

1. At first, the LPN broadcast a friend request message with TTL field set to zero, so only the friend nodes within direct radio range will receive it. The friend request message includes the LPN friendship required parameters that must be supported by the friend node.

2. All friend nodes that receive the friend request and can support the requirement, reply to the LPN with friend offer message. The friend offer

message contains the parameters that can be offered to the LPN (RSSI value, receiver window size, messages queue size, and subscription list size).

3. The LPN selects the friend node that suites it more using a product developer defined algorithm that works on the friend node offered parameters.

4. The LPN sends a friend poll message to the selected friend node, then the friend node replies with a friend update message. Now the friendship has been established between the two nodes.

5. After the friendship has been established, the friend messaging process starts. The LPN sends a friend subscription list message to the friend node, which contains all the LPN subscribed addresses. This list enables the friend node to define which messages will be sent to the LPN.

6. The friend node will store the friend subscription list, then it will reply to the LPN with subscription list confirmation message.

7. When the friend node receives a message with a destination address of the LPN friend, it will be stored in the friend queue, this queue is allocated only for that LPN.

8. Upon the waking of the LPN, it will send a friend poll message to the friend node, asking for the stored messages. The friend node will reply back by sending only one message from the stored messages per time, then the LPN will send again a friend poll message. This step will be repeated until the friend node sends a friend update message with LPN field set to zero to inform the LPN, that there is no more stored messages for it.

2.3.7 NETWORK AND SUBNET

A network is a group of nodes that have the same four parameters. These parameters have been assigned to each node during the provisioning process :

- **Network addresses:** They are used to identify different messages source and destination addresses, which have been described in Section 2.3.1.6.

- **Network keys:** They are used for authentication and security of different messages at the network layer.

- **Application keys:** They are used for authentication and security of different messages at the access layer.

- **IV Index:** It is used to define how long the network should be alive.

A subnet is a group of nodes that have the same network key. Bluetooth mesh network can have an unlimited number of subnets, a node could be in one or more subnets by knowing their network keys. A subnet could be used to isolate an area, for example, isolating an office in a factory from the main factory network. a message that belongs to a certain subnet, will be exchanged within the nodes of that subnet only, moreover, this could be a way of reducing the network payload, and increasing the security at the same time.

2.3.8 SECURITY

Security is one of the main priorities in the Bluetooth mesh, which could be summarized as follow:

- All messages types are encrypted and authenticated at different layers.

- Using three different types of security keys (network key, application key, and device key) to authenticate and encrypt mesh messages. Network key used to identify each network or subnet. As well as, it is used by any node to be a member of specific network or subnet. The application key is used by certain nodes to decrypt application data for a specific application only, for example, the doors will have the access application key only, while the lights will have the lighting application key only, which mean that the lights could relay the messages sent to the doors without being able to decrypt it. The device key is used to secure the provisioning process, each node has a unique device key which is known to the provisioner device.

- When a node needs to be removed from the network, that node will be added to the blacklist by the provisioner then the key refresh procedure will take place. During the key refresh procedure, all the nodes within a mesh network will get new security keys, except the nodes in the blacklist.

- A privacy key which is derived from the network key is used to obfuscate the message network header. This makes tracking nodes and messages very difficult.

- To prevent the messages from being captured and used again which is called replay attacks, Bluetooth mesh uses two network PDU fields, the sequence number, and the IV index. Each time a node sends a new message, it increments the value of the sequence number.

When a node receives a message with a sequence number value less than or equal to the value found in the last message sent from the same node, it will be discarded. If a node receives a message with an IV index value less than the value found in the last message sent from the same node, it will be discarded.

3

Industrial Radio Wave Propagation

It is known that the propagation of the electromagnetic waves depends on the characteristics of the transmission medium which they travel through it. The propagation path connecting the Tx and receiver (Rx) is well known as the communication channel. Awareness of radio channel propagation is very important in order to understand the wireless communication system. Consequently, this chapter gives an overview of the radio wave propagation characteristics in industrial environment [18] [6] [19] [20] [5] [21] [22] [4] [23].

3.1 INDUSTRIAL ENVIRONMENT

Industrial environments have particular propagation characteristics that not exist in typical office or residential environments. They are often characterized by metallic objects and large dimension machines. Moreover, it also depends on the movements of tools, rotating machines and persons. All of the previous things affect on radio wave propagation and increase multi-path propagation.

3.2 PROPAGATION MECHANISM

In wireless communications system, when the radio signal travels through the communication channel, it interacts with objects in the surrounding environment (industrial environment). There are three basic mechanisms that impact radio signal propagation in a wireless communication system. They are reflection, diffraction, and scattering.

3.2.1 REFLECTION

Reflection happens when the incident radio wave collides into a smooth surface of an object that has a very large dimensions compared to the wavelength of the radio propagation wave. As illustrated in Figure 3.1, the angle of the incident wave is the same as the angle of the reflected wave. The radio waves may be reflected partly or entirely, which depends on the object material properties, the incidence angle and the carrier frequency. Reflection may exist in walls, ceilings and objects [22] [4].

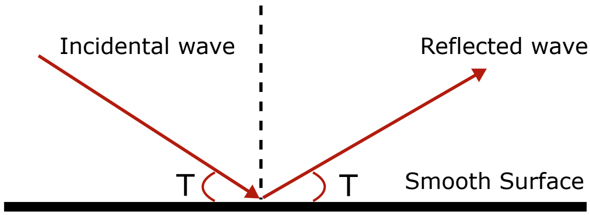


Figure 3.1 Reflection example.

3.2.2 DIFFRACTION

Diffraction happens when the radio wave is obstructed by an object surface that has sharp edges. These edges cause two different characteristics for the incident waves: reflection and diffraction. The diffracted wave appears behind the obstructed object in the shadow area. Diffraction is also known as shadowing, because the diffracted wave can reach the Rx even when shadowed by an invincible obstruction. The received signal strength measured at the shadowed area is usually weak. Figure 3.2 clarifies the diffraction phenomenon [22] [4].

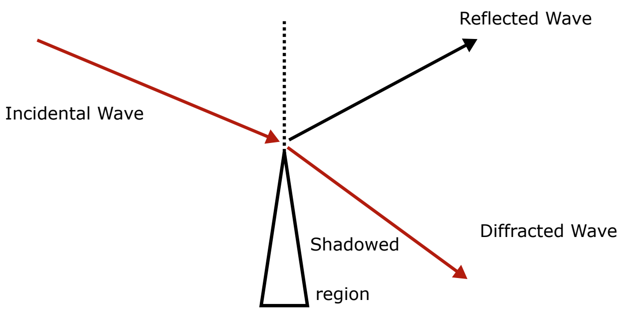


Figure 3.2 Diffraction phenomenon.

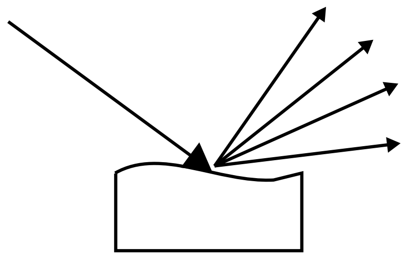


Figure 3.3 Scattering phenomenon example.

3.2.3 SCATTERING

Scattering is a process where radio waves are forced to deviate from a straight path by one or more objects that have a small size compared to the wavelength of the radio propagation waves. Also, scattering can occur when the radio wave impinge with a surface which is not completely smooth (rough surface). Figure 3.3 illustrates the situation when incident wave hits a rough surface results in random reflected waves in different directions caused by scattering phenomenon [20].

3.3 MULTI-PATH PROPAGATION MECHANISM

Multi-path is defined as the effect that happens when the radio signal arrives at the receiving antenna through more than one path. Multi-path propagation means that the transmitted radio signal is reflected, diffracted and scattered by interacting objects exist in the path between Tx and Rx. Multi-path propagation is a combination between Non Line Of Sight (NLOS) connections which occurs when there is no direct connection path between Tx and Rx with obstacles existing in that path, and a Line Of Sight (LOS) connection which occurs if there is a direct connection path between Tx and Rx [4].

As shown in Figure 3.4 the multiple copies of the transmitted radio signal reach to the Rx from different paths, after that the receiver adds them together. Each copy of the radio signal has a different amplitude, phase shift, delay (runtime of the signal), direction of departure from the Tx, and direction of arrival at the Rx, which is termed as multi-path fading. All of these components are known as a Multi Path Components (MPCs) [4]. Thus, an industrial environment with metallic objects and large machines introduces high levels of multi-path fading compared to other indoor environments such as office and residential environment.

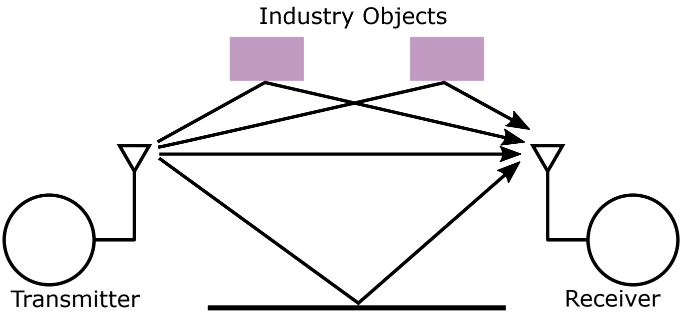


Figure 3.4 Multi-path propagation [4].

3.4 FADING DEFINITION

Due to the received signal is a composition of various amplitude and phase shifted versions of the transmitted radio signal executed by the radio channel, the Rx can not distinguish between the different MPCs; it only adds them up, consequently they overlap with each other. The overlapping between them can be constructive or destructive depending on the phase of the MPCs [4], as illustrated in Figure 3.5 .

Industrial high rise objects can cause shadowing in the propagated signal. This occurs when the signal going through or around the shadowing object, as a result the received signal is greatly attenuated. This impairment is known as fading. In wireless communication systems fading may either be due to small

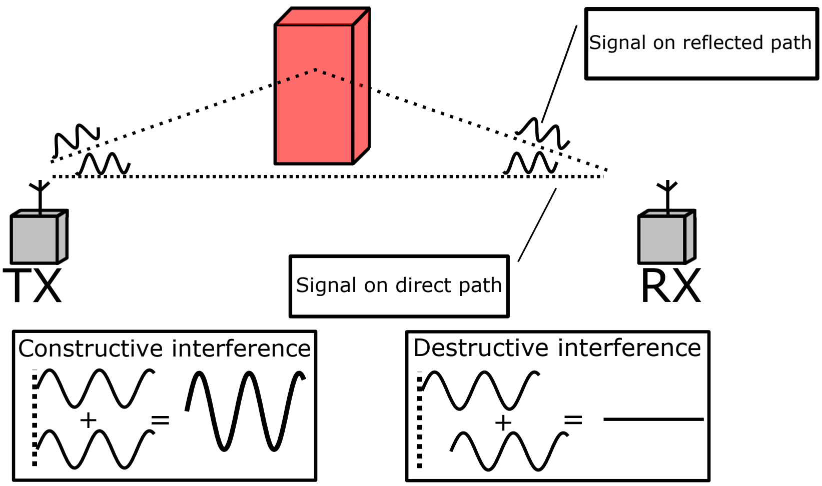


Figure 3.5 Constructive and destructive interference [4].

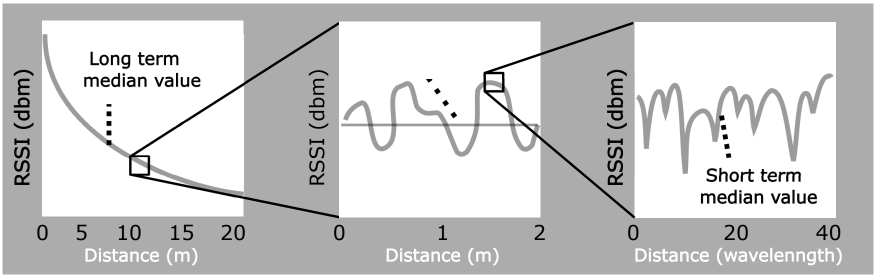


Figure 3.6 large scale fading and small scale fading phenomenon [5].

scale or large scale.

3.4.1 SMALL SCALE FADING

Multi-path propagation creates small scale fading effects, which describes the fast fluctuation of RSSI over a short period of time of travel distances, where RSSI is a power indicator of the received radio signal. The small scale fading is used to describe the self-interference of the received radio signals from various paths with various amplitudes, delays and phases over a short period. In addition, it relies on the properties of the radio channel and the characteristics of the transmitted radio signal for example bandwidth B_s, bit time T_b and symbol time T_s. There are many factors that influence the small scale fading such as: transmission bandwidth of the channel and time variation of the channel.

3.4.2 LARGE SCALE FADING

Large scale fading is the power fluctuations of the radio signal around its mean value due to large distance between Tx and Rx. This phenomenon happens due to large objects exist between the Tx and Rx. Figure 3.6 illustrates, the decay of the RSSI with distance, the large scale fading and the small scale fading.

3.5 CHANNEL MODELING

Most wireless communication systems use large bandwidth for high data rates. Thus the variations of the channel over a large bandwidth will be clarified in this part. In order to fully understand the radio channel properties, a channel model is needed. The channel model is defined as a mathematical representation of the effects of a radio communication channel. The channel model is the impulse response of the channel medium in the time domain or its Fourier transform in the frequency domain. Generally, the channel impulse response of a wireless communication system changes rapidly over time as the following equation [24].

$$y(t) = h(t,\tau) * x(t) + n(t) \tag{3.1}$$

Where $h(t,\tau)$ is the radio channel impulse response as a function of time t and delay τ, $y(t)$ and $x(t)$ are the received and transmitted signals,respectively, and $n(t)$ is Additive White Gaussian Noise (AWGN). The following equation can be represented as a tapped delay line model of the channel (channel impulse response).

$$h(t,\tau) = \sum_{i=1}^{N} a_i(t)\,\delta(\tau - \tau_i) \tag{3.2}$$

Where a_i are the time dependent complex coefficients (attenuation), τ is the time delay and N is the total number of MPCs (taps) [4].

Figure 3.7 illustrates the tapped delay line of the radio communication channel due to the multi-path, caused by the surrounding environment.

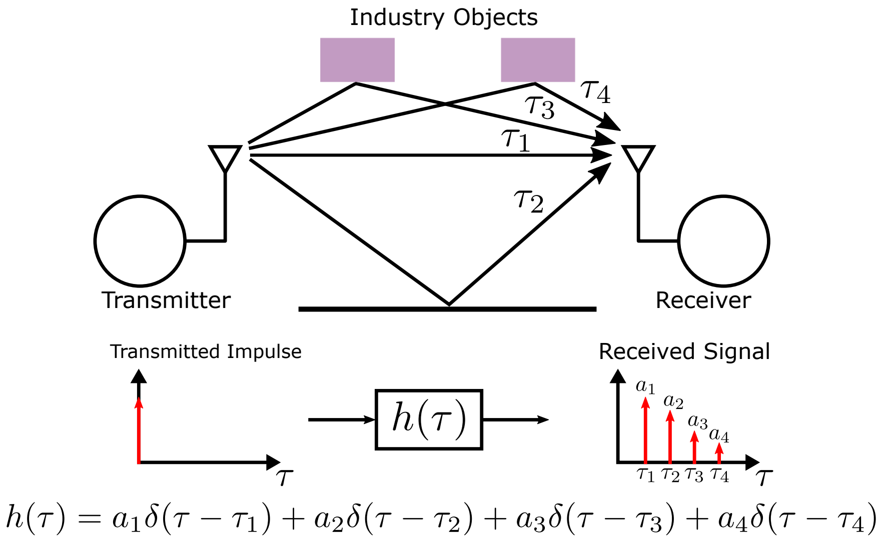


Figure 3.7 Multi-path due to surrounding environment and channel impulse response.

3.5.1 PATH LOSS

Path loss is the attenuation that a radio signal suffers when it travels through the surrounding environment. This attenuation is a function of the distance between the Tx and Rx [4]. This path loss changes depending on some factors such as distributed industrial objects, human body interference and location of the walls.

Different path loss models have been developed over the last years. There are two types of path loss models:

- Theoretical models: they are based on physical propagation principles of the radio signal. These models are not accurate enough, and in some situations, they are more complicated to be implemented, because they need huge databases of all characteristics of the surrounding environment.

- Empirical models: they are based on measurements information about the surrounding environment. They are environmental and hardware characteristics dependent. These models are more accurate.

Indoor path loss is more difficult to estimate in contrast to outdoor, where attenuation is very unexpected due to the large number of industrial objects in the environment, in addition to walls and ceilings that obstruct the path.

In this thesis, empirical path loss model has been chosen. The aim is to build a path loss model which characterizes the signal attenuation happened by both distance and obstructions exist in the path [25] [26], as it will be seen in more details in section 3.5.4.

3.5.2 FREE SPACE PROPAGATION MODEL

The free space propagation model is one kind of the theoretical models. It is used to calculate the RSSI when the path between the Tx and Rx is free from obstacles (LOS). Also, it is the most basic model that relates the RSSI as a function of distance [4].

The received power collected by the Rx antenna which is at distance d from the Tx antenna is given by the following Equation

$$P_{Rx}(d) = P_{Tx} G_{Tx} \frac{1}{4\pi d^2} A_{Rx} \tag{3.3}$$

where P_{Tx} is the transmitted power, G_{Tx} is the transmitter antenna gain and A_{Rx} is the effective antenna area. Equation 3.4 shows the simple relationship between the antenna effective area A_{Rx} and the antenna gain G_{Rx} [4].

$$G_{Rx} = \frac{4\pi}{\lambda^2} A_{Rx} \tag{3.4}$$

In Equation 3.4, λ is the wavelength of the carrier. It can be generated from Equation 3.5

$$\lambda = \frac{c}{f_c} \tag{3.5}$$

where f_c is the carrier frequency and c is the speed of light. Substituting Equation 3.4 into Equation 3.3 gives the received signal power as a function of the distance d in free space as clear in Equation 3.6, where it is also known as Friis law [4].

$$P_{Rx}(d) = P_{Tx} G_{Tx} G_{Rx} \left(\frac{\lambda}{4\pi d} \right)^2 \tag{3.6}$$

The previous equation shows that RSSI decreases as the square of separation distance increases. The factor$(\lambda/4\pi d)^2$ is known as the free space loss factor.

In order to set up link budgets as shown in Figure 3.8, it is important to write Friis law equation on a logarithmic scale where antenna gains are included as in Equation 3.7

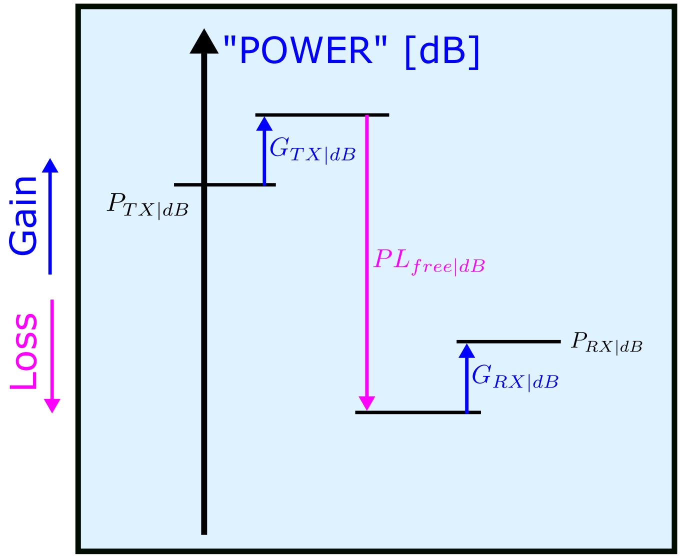


Figure 3.8 Link budget for free space for non isotropic antenna.

$$\begin{aligned} P_{Rx|dB}(d) &= P_{Tx|dB} + G_{Tx|dB} - 20\log_{10}\left(\frac{4\pi d}{\lambda}\right) + G_{Rx|dB} \\ &= P_{Tx|dB} + G_{Tx|dB} - PL_{free|dB} + G_{Rx|dB} \end{aligned} \tag{3.7}$$

where $PL_{free|dB} = 20\log_{10}\left(\frac{4\pi d}{\lambda}\right)$ and it is called free space path loss in dB.

When the transmitter and receiver antennas are isotropic (isotropic antenna is an ideal antenna that radiates its power uniformly in all directions), their gains G_{Tx} and G_{Rx} will be equal to unity which means it is equal to 0 dB, as illustrated in the next equation.

$$P_{Rx|dB}(d) = P_{Tx|dB} - PL_{free|dB} \tag{3.8}$$

$$PL_{free|dB} = P_{Tx|dB} - P_{Rx|dB}(d) \tag{3.9}$$

Equation 3.9 illustrates the free space path loss $PL_{free|dB}$, which represents signal attenuation measured in dB, and it is defined as the difference between the effective transmitted power and the received power.

The received power in free space at a distance d is given by

$$P_{Rx}(d) = P_{Rx}(d_0)\left(\frac{d_0}{d}\right)^2 d \geq d_0 \tag{3.10}$$

where $P_{Rx}(d_0)$ is the reference power measured at distance d_0. The distance d_0 has to be greater than 0 and it is equal to 1 m in this thesis.

3.5.3 LOG-DISTANCE PATH LOSS MODEL

In reality radio channel seldom follows the simple model described above. Actually the radio signal suffers from large and small scale fading. The log-distance path loss model takes into account the small small fading effect. This model calculates the attenuation for the radio signal power for any separation distance d between the Tx and Rx. The log-distance path loss is calculated as [4]

$$PL_{dB}(d) = PL_{dB}(d_0) + 10n\log_{10}\left(\frac{d}{d_0}\right) \tag{3.11}$$

where $PL_{dB}(d)$ is the path loss approximation at distance d from the transmitter, and $PL_{dB}(d_0)$ is the path loss at the reference distance d_0 due to free space propagation from the transmitter to a 1 m distance. n is the path loss exponent and the value of n depends on the surrounding environment. The following table 3.1 shows some of these values.

This table is for reference only (example). The value of n may be within the range mentioned in the table or may not fit the desired environment we are trying to model, as it changes from environment to another environment.

3.5.4 INDOOR EMPIRICAL PATH LOSS MODELS AT FREQUENCY 2.4 GHZ

Indoor radio signal propagation is affected by the same fading mechanisms as outdoor propagation, but indoor radio channels differ from the common outdoor radio channels. Various measurements have been executed to deter-

Environment	Path loss exponent n
Free space	2
Urban area cellular radio	2.7 to 3.5
Shadowed urban cellular radio	3 to 5
In building LOS	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in Factories	2 to 3

Table 3.1 The path loss exponent n for different environments [6] [5] [7].

mine the propagation characteristics of the radio signal in the industrial environment at frequency 2.4 GHz. Empirical path loss models are experimental mathematical formulations which estimate radio signal losses based on fixed but primary parameters like frequency f, path loss exponent n, distance d and others [27] [25] [26].There are different types of indoor empirical path loss models. Consequently, in this study the log-normal shadowing and ITU model used a lot for indoor environments as they are simple and common.

3.5.4.1 LOG-NORMAL SHADOWING MODEL

The log-Normal Shadowing Model is one type of indoor empirical path loss models and it is an extension of the log normal model.Most parts of the empirical models are build on this model. Shadowing is generated from the presence of large objects in the surrounding environment and causes variation in the received power. The average path loss between Tx and Rx is [27]

$$PL_{dB}(d) = PL_{dB}(d_0) + 10n\log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \tag{3.12}$$

Where X_σ is a zero-mean Gaussian distributed random variable with shadow fading standard deviation σ. Shadowing may be expressed as a random process, determined by the normally distributed random variable X_σ, as shown in the Figures 3.9 and 3.10.

As clear from Figure 3.9, the measured received path loss levels at specific separation distances have a normal distribution. The values of n and σ can be estimated from measured signal power, using linear regression (curve fitting) [5] [28]. Log linear regression is a curve or mathematical function which best fits the series of measured data. Figure 3.11 defines the basis of a linear regression analysis, where the points in blue are the measured data and the points in red are the predicted values from the regression equation. The difference between the blue points and red ones is the residual error r. The total

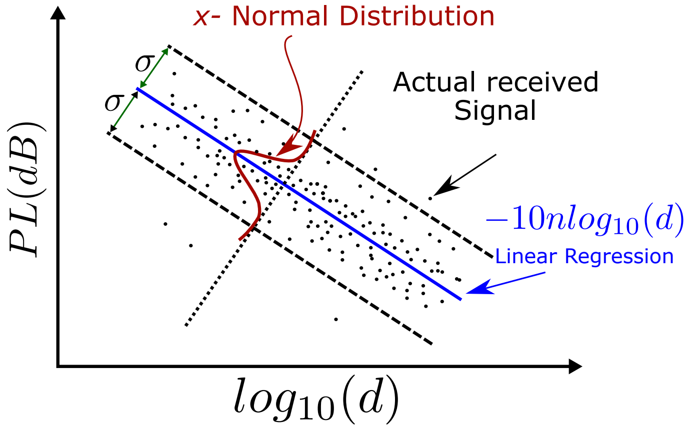


Figure 3.9 Measured received power with log- normal shadowing [6] [5] [7].

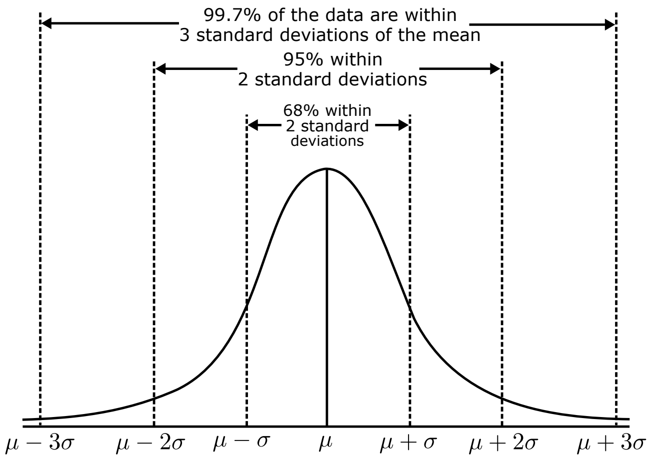


Figure 3.10 Normal distribution with standard deviation σ and mean μ [8].

residual error R is the sum of the square of the individual residual errors. The smaller the value of R, the better the fit of the straight line to the measured data [28].

In order to explore shadowing characteristics of the industrial environment, X_σ is calculated as the difference between the estimated parameters and the average measured path loss as follows [10]

$$X_\sigma = PL_{est|dB} - PL_{mes|dB} \tag{3.13}$$

In Equation 3.13, $PL_{mes|dB}$ is the average measured path loss in dB and $PL_{est|dB}$

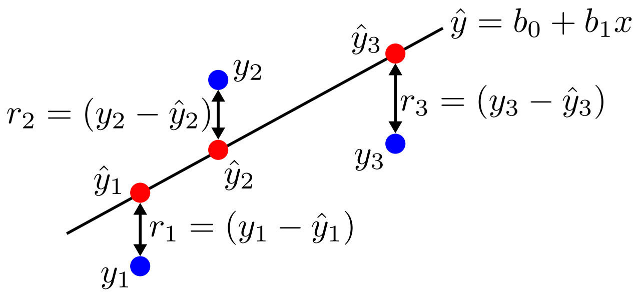


Figure 3.11 Linear regression concept.

is the estimated path loss according to curve fitting in dB. It is shown that shadow fading X_σ follows closely a normal distribution with mean equal to 0 dB and standard deviation σ. n may be derived as the slope of the log-linear regression line.

This model estimates path loss as a function of distance. The model parameters n and σ are determined as functions of the surrounding environment. The following table shows some of these values for two wood processing and two metal processing factories at 2.4 GHz [10].

Propagation Topographies	$PL_{dB}(d_0)$	n	σ_{dB}
LOS	67.43	1.72	4.73
Obstructed with light clutter	72.71	1.52	4.61
Obstructed with heavy clutter	80.48	1.69	6.62

Table 3.2 n and σ_{dB} for different propagation topographies [10].

As illustrated in previous table the industrial environment is classified into several propagation topographies to describe large scale fading. Characteristics of this environment specify these topographies. The propagation topographies are based on if LOS exists or not between the Tx and the Rx, in addition, it also depends on the height of industrial objects and the elevation position of the Tx and the Rx. The classification of propagation topographies are assigned as follows [29]

- Line of sight with light surrounding clutter: this topography is described by the existence of a LOS path. In this topography, the transmitting and receiving antennas are surrounded by little industrial objects. These objects heights are lower than the hight of the Tx and Rx antennas.

- Line of sight with heavy surrounding clutter: this topography is also described by the existence of a LOS path, but the transmitting and receiving antennas are surrounded by heavy industrial objects, where their heights are greater than the hight of the Tx and Rx antennas.

- Obstructed with light surrounding clutter: this topography is described by the existence of obstacles in the LOS path between the transmitting and receiving antennas. Furthermore, these objects heights are slightly greater than the hight of the receiving antenna, but below the transmitting antenna.
- Obstructed with heavy surrounding clutter: this topography is described by the existence of obstacles in the LOS path between the transmitting and receiving antennas. These objects heights are greater than the hight of transmitting and the receiving antennas.

In this thesis our industrial environment is classified into LOS with heavy surrounding clutter and Obstructed with heavy surrounding clutter propagation topographies.

3.5.4.2 ITU MODEL

ITU model is another type of indoor empirical path loss models. The path loss of this model is given by the following equation [10] [11]

$$PL_{dB}(d) = 20\log_{10}(f) + N\log_{10}(d) + L_f(n) - 28 \qquad (3.14)$$

Where N is the distance power loss coefficient, this value depends on the type of the environment, f is the frequency in MHz, d is the distance in meters between Tx and Rx, L_f is the floor loss penetration factor in dB and n is number of floors penetrated, -28 is constant and there is no explanation in the standard

Frequency(GHz)	Residential	Office	Commercial	Factory
0.8	-	22.5	-	-
0.9	-	33	20	-
1.25	-	32	22	-
1.9	28	30	22	-
2.1	-	25.5	20	21.1
2.2	-	20.7	-	-
2.4	28	30	-	-
2.625	-	44	-	33

Table 3.3 Different values of distance power loss coefficient N [11] .

why it is -28. As this thesis focuses only on single floor, the parameter related to floor loss penetration in equation 3.14 is substituted with zero. To increase the accuracy of this model, parameter N would also be adjusted based on site measurement. There are limits for this model which are

- 900 MHz $\leq f \leq$ 5200 MHz
- 20$\leq N \leq$ 40
- $d > 1m$

The value of distance power loss coefficient depends on the frequency and the type of the surrounding environment. Some values recommended by the ITU are given in table 5.2.

4 Factory Measurements Campaign

In recent years, there has been an increasing interest in designing and implementing wireless communication networks in factories for the unlicensed 2.4 GHz band. There are different factors that can degrade the performance of wireless communication systems in industrial environment, such as objects material and dimensions. This chapter describes the hardware used in the measurements.

The thesis has three targets. The first one is to measure RSSI in order to build path loss model for the suggested deployment location. The second target is to take object signal loss measures to give a guide of the type of loss due to blocked objects. The final target is to calculate the probability of receiving packets successfully between two BLE devices in the deployment area. The measurement campaign was executed on HMS Industrial Networks AB factory located in Halmstad, Sweden.

4.1 HARDWARE CHARACTERISTICS

In the measurements the Anybus wireless Bridge II was used. This device can communicate via both Bluetooth, BLE and WLAN and is ideal for communication through dangerous areas or hard to reach locations where cables are not desirable. Also, this device creates industrial wireless connection between two points in an industrial Ethernet network. The Anybus wireless Bridge is not only point to point communication but also an access point for up to seven BLE/WLAN clients. There are several applications for these devices such as

- Adding wireless cloud connectivity to industrial devices.
- Accessing devices from laptop or smart phones.

- Ethernet cable replacement between devices.

Figure 4.1 Point to point connection BLE [9].

Figure 4.1 illustrates a point to point connection of EtherNet/IP IO device and EtherNet/IP PLC device over BLE using two wireless bridge. Whereas, Figure 4.2 shows an access point connection of wireless bridge (central) to three different slaves (peripheral). Table 4.1 clarifies wireless standards for BLE [9].

Figure 4.2 Access point connection BLE [9].

4.1.1 CONFIGURATION

Anybus Wireless Bridge II can be controlled via the Graphical User Interface (GUI) by accessing the web browser to the IP address of the product. The IP address of the used device is 192.168.0.99. The computer accessing the web interface must be in the same IP subnet as the unit. After that the AT commands were used for setting advanced parameters that are not accessible

Wireless standards (profiles)	GATT
Operation modes	central or peripheral
RF output power	4 dBm
Max number of slaves for central	7
Bluetooth version support	v4.0
Maximum transmission rate	1 Mbps

Table 4.1 Wireless standards for BLE [9].

in the web interface and to read out parameters in text format. Moreover, the commands were entered into the text box, then click on Send, as explained in Figure 4.3. The AT result will be displayed below the text box [9].

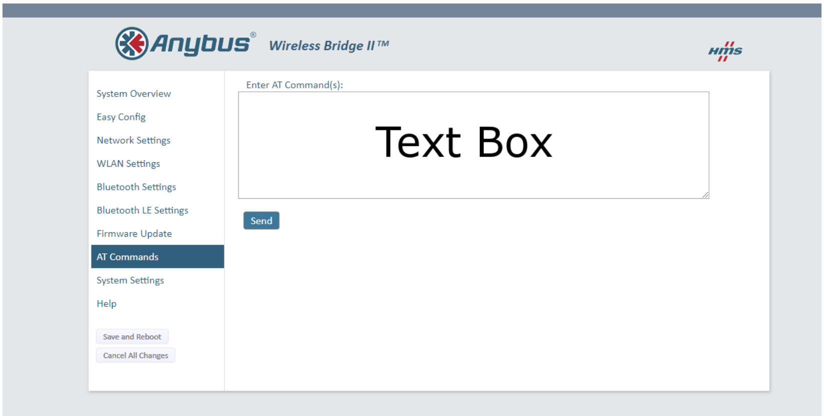


Figure 4.3 Anybus GUI.

4.1.1.1 MANUAL BLEDD COMMAND

The bledd command (at*bledd) is used to search for BLE devices and it is available when the device is in the central operating mode. The syntax of the bledd command is at*bledd=<type>,<length>,<scan>. Type, length and scan are the input parameters of the bledd command. The description of these input parameters are as in the following Table 4.2 and the characterizations of the output parameters after finding out BLE devices are in Table 4.3. Figure 4.4 illustrates the input and output parameters.

In Figure 4.4, the command at*bledd=0,5000,0 was entered in the central device, in order to scan for surrounding BLE devices. The input ’0’ is for discovering all devices, but display each device once, 5000 msec is the discovery interval and '0' means active scan. The extract parameters after scanning are RSSI of the peripheral devices, showing their addresses, their local names and Advertising/Scan-response data.

4.2 RSSI MEASUREMENT SETUP

A picture of the measurement setup is shown in Figure 4.5. To carry out measurements, the Anybus Wireless Bridge peripheral device was used as the Tx. This device was connected to power source to generate and send advertising packets through three advertisement channels (37, 38 and 39). In addition, the Anybus Wireless Bridge central device was used as Rx which is connected to the laptop through Ethernet cable M12/RJ45. The BLE 'At' command was

Name	Type	Description
type	Integer	Type of discovery. 0:.Discover all devices, but only display each device once. 1: Discover devices in general or limited discoverability mode. 2: Discover devices in limited discoverability mode. 3: Discover all devices, each device may be displayed multiple times.
length	Integer	Length of discovery in milliseconds. Max 65535 ms.
scan	Integer	Type of scan. 0: Active scan. 1: Passive scan.

Table 4.2 Input parameters for bledd command [9].

Name	Type	Description
bd-addr	String	Bluetooth address of the BLE device.
Rssi	Integer	RSSI
Name	String	Complete local name of BLE device, if included in data.
Data	String	Advertise/Scan response data as a HEX string.

Table 4.3 Output parameters for bledd command [9].

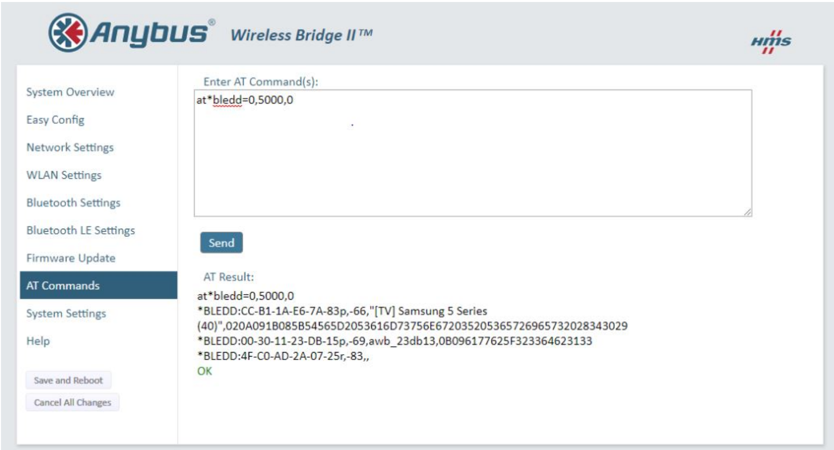


Figure 4.4 The result of the AT command.

entered into the text box of the laptop web browser (web interface) in order to measure RSSI of the Tx. For all measurements, the transmitter output power was 4 dBm and the receiver sensitivity was -95 dBm. The height of the Tx and Rx antennas was fixed at 74 cm above the floor. Both the Tx and Rx use external monopole antennas which have a gain of maximum 3 dBi each.

Figure 4.5 Measurement setup.

4.2.1 MEASUREMENT PROCEDURES

Using the hardware mentioned above, measurements were performed at three different areas in HMS Industrial Networks AB factory and taken place during working days. There are three measurement scenarios resulted from these measurement areas which are LOS, NLOS-area1 and NLOS-area2. The difference between the NLOS-area1 and NLOS-area2 scenarios is that in the NLOS-area1 scenario there are three machines with free space between them that obstruct the propagation of the signal, while in the NLOS-area2 scenario five machines with no free space between them, which in this case blocked the transmitted signal.

The description of the environment of the three measurement scenarios is explained in details in Section 4.2.2. The Tx was always located in a fixed position and the Rx was moved to capture the measurements. Knowledge of the physical distance between Tx and Rx allowed the measured data to be related with distance. Measurements were made while the two devices (Tx/Rx) were within LOS of each other or while they were within NLOS of each other. LOS is used to describe a direct and unobstructed path between two devices, whereas NLOS is an obstructed path between the location of the source and the location of the destination. Obstacles that can cause an obstruction are walls, floors, machines and people moving inside the factory. The procedure to get the results for the three measurement scenarios was as the following:

- Place the Anybus wireless Bridge II (Tx) at the desired position inside the factory to send advertising packets.
- Place the Rx at several distances in a range between 1 meter (reference distance d_0) to 20 meters. The receiver scan for surrounding BLE devices.
- Measure the RSSI level at each distance .
- Take a set of RSSI measurements at each distance .
- Store the average of the multiple measurements ($RSSI_{average}$).
- Analyze data with MATLAB: average RSSI distribution, path loss model estimations, etc.

4.2.2 MEASUREMENT LOCATIONS

The measurements were carried out in three different areas in the factory. This factory is an electronic manufacturing place which consists of different automation machines. These machines are used in order to manufacture printed circuit boards which are stacked in big racks. In addition, the factory environment also includes tables, electronic instruments components, PCs..etc. The walls and celling are made from concentrate and the windows are made from glass. Figures 4.6, 4.7 and 4.8 show the HMS factory environment and layout.

The three measurement areas in the factory are described as the following:

- LOS area: In this area there are no machines in the path between Tx and Rx. Figure 4.9 clarifies this area.
- NLOS-area1: In this area there are three machines with free space between them. Figure 4.10 shows this area.

Figure 4.6 HMS factory environment.

Figure 4.7 HMS factory environment.

- NLOS-area2: In this area there are five machines with no free space between them. Figure 4.11 illustrates this area.

4.3 OBJECT SIGNAL LOSS MEASUREMENT

The main target of this section is to measure the signal loss of objects founded in the factory. These objects are the machines inside the factory. These measurements give a guide of the type of signal loss due to blocked objects. High signal losses will cause the BLE not working probably even when the distance between Tx and Rx is short. Therefore, the goal is to find if it is possible to put the BLE devices inside the machines and what will be the signal loss in that case.

4.3.1 MEASUREMENT PROCEDURES

The measurement of object signal loss was performed for two cases. The first case is when the Tx and Rx are adherent to the purposed machine, and the second case is when there is a space between Tx and the machine, and also between Rx and the machine. Figures 4.12 and 4.13 illustrate those two cases. The measurement procedures for the first case are as follow:

- Transmit advertising packets from the Tx.
- Put the Tx and Rx at distance of 1.85 m (reference distance) to measure

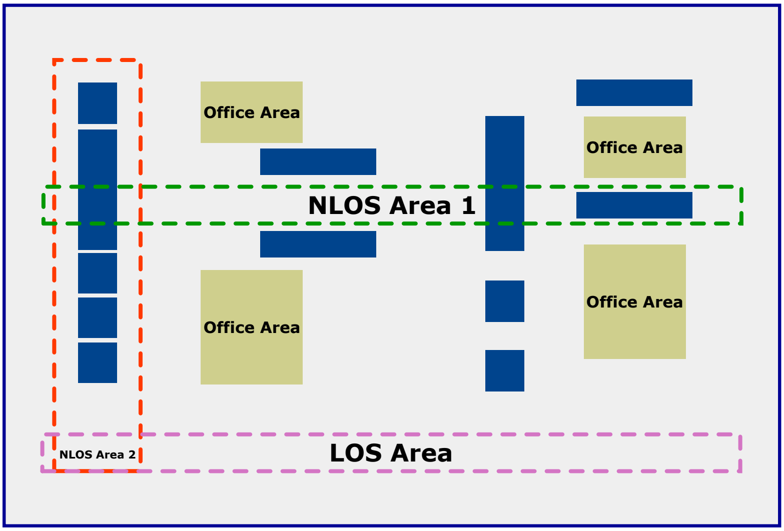


Figure 4.8 HMS factory layout.

the RSSI.

- Place the intended machine in between the Tx and Rx.
- Measure RSSI.
- Record the measured RSSI.
- Calculate the object signal loss as: object signal loss= $RSSI_{ref}$- $RSSI_{machine}$.
- Repeat the previous steps for different objects in the factory.

The measurement procedures for the second case are as follow:

- Transmit advertising packets from the Tx.
- Put the Tx and Rx at distance of 4 m (reference distance) to measure the RSSI.

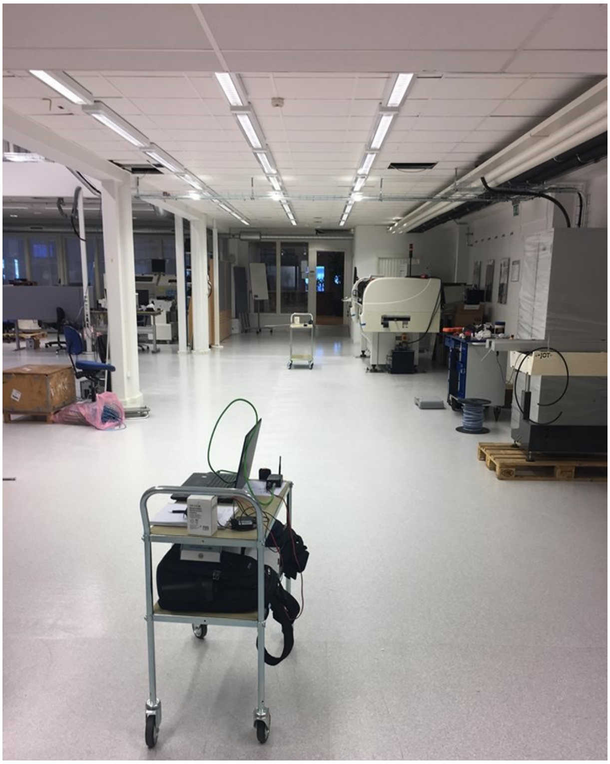


Figure 4.9 The LOS area.

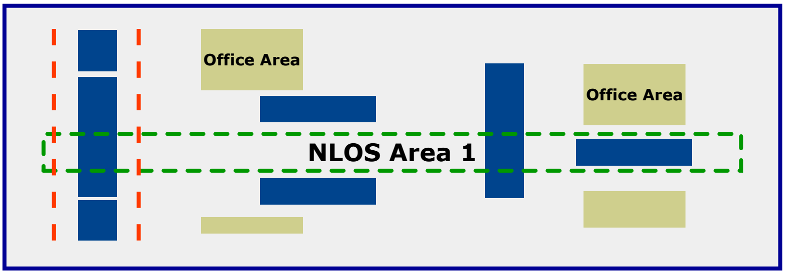


Figure 4.10 The NLOS-area1.

Figure 4.11 The NLOS-area2.

- Place the intended machine in between the Tx and Rx with free space equal to 1.20 m between them and the machine.
- Measure RSSI.
- Record the measured RSSI.
- Object signal loss = $RSSI_{ref}$-$RSSI_{machine}$.
- Repeat the previous steps for different objects in the factory.

4.4 PROBABILITY OF SUCCESSFULLY RECEIVING PACKETS MEASUREMENTS

The main object of this experiment is to study the probability of packets being successfully received between two BLE devices at different distances for two different areas (LOS area and NLOS-area1). The peripheral device sends one advertising packet each advertising interval T_{adv} on the three advertisement channels (37, 38 and 39). Whereas, the central device discovers BLE devices and their discovery packets within time T_{dis}. In this device there are two types of scan; passive and active. If the passive scan is performed, the devices advertisement data will be included, while If the active scan is performed, the devices scan response data will be included. In this experiment the central device was in the passive scan mode to read the advertising packets and the command at*bledd=3,10400,1 was used as shown in Figure 4.14. The description of these parameters in the 'At' command is described in Section 4.1.1.1. This experiment was performed to find the optimal location that the BLE devices can be placed to create a BLE mesh network in the required factory.

Figure 4.12 First case.

Figure 4.13 Second case.

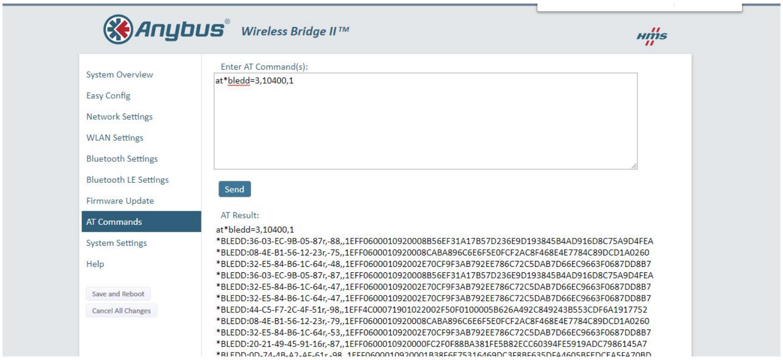


Figure 4.14 The 'at' command used in measuring the probability of success.

4.4.1 MEASUREMENT PROCEDURES

Measurement procedures for LOS area and NLOS-area1 are as follow:

- Transmit advertising packet each advertising interval *Tadv* (T_{adv} =835 msec) from the Tx, consequently the number of transmitted packets equal to 20 packets.
- Put the transmitter and receiver at distance of 1 m from each other.

- Enter the 'at' command (at*bledd=3,10400,1) in the central device in order to read the received packets.
- Read the received packets which are sent from the transmitter.
- Take a set of readings of the received packets (the number of readings in this experiment was 6) at each distance.
- Calculate the probability of success.
- Change the distance between the transmitter and receiver.
- Read again the received advertising packets.
- Record readings.
- Repeat the procedure for different distances in the factory.

5

Measurement Results

The target in this chapter is to develop and estimate the path loss model which represents the signal decay caused by distance and obstructions along the path between Tx and Rx. The models used in this study are Log-distance Model,Log-normal shadowing model and ITU model. This Chapter presents and discusses the results of the experiments carried out in HMS factory in three different areas (LOS area, NLOS-area1 and NLOS-area2). Also, this chapter shows the results of the measured signal loss of objects and the measured probability of receiving packets successfully. The description of these measurements is described in Section 4.3.

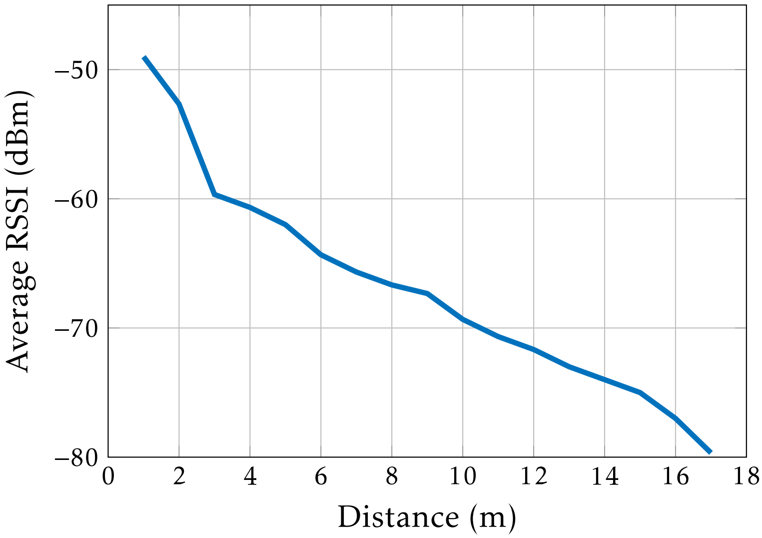
5.1 RSSI MEASURED RESULTS

There are three measurement scenarios resulted from the measurement area which are LOS area, NLOS-area1 and NLOS-area2. Consequently this section presents the RSSI measurement results for these different areas.

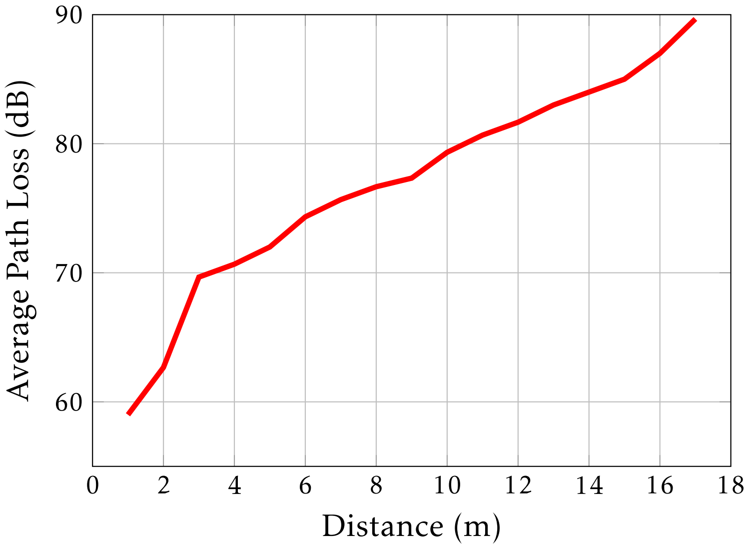
5.1.1 LOS AREA

The LOS area is clear from any machines in the path between Tx and Rx (see Section 4.2.2). A set of RSSI readings were done by the central device (Rx) at different distances from the peripheral (Tx). These readings were collected and the average value was calculated. The measurements range in the LOS area was between 1 m to 17 m. The average RSSI readings are shown in Table 5.1. The measured results of this area can be observed in Figure 5.1(a). This figure illustrates that the average RSSI decreases over the distance. The average RSSI at 1 m is taken as a reference and it is equal to -49 dBm. Equation 5.1 is used to determine the average measured path loss, as follows:

$$PL_{|dB} = P_{Tx|dBm} + G_{Tx|dB} + G_{Rx|dB} - P_{Rx|dBm} \tag{5.1}$$



(a) Average measured RSSI.



(b) Average measured path loss.

Figure 5.1 Measured RSSI and path loss for LOS area.

Where $P_{Tx|dBm}$ is the transmitted power, $P_{Rx|dBm}$ is the received power, G_{Tx} and G_{Rx} are the transmitting and receiving antennas gains respectively. Figure 5.1(b) illustrates that the average measured path loss increases with distance d. The measured data is shown in Table 5.1 .

5.1.1.1 LOG-DISTANCE MODEL

The log-distance path loss model parameter is determined from the average measured path loss data. These parameter is the path loss exponent n (see Section 3.5.3). The path loss exponent n is the slope of the linear regression line (curve fitting) of the average measured path loss as outlined previously in Section 3.5.4.1. MATLAB curve fitting tool is used in order to fit the measured data. Figure 5.2 shows the linear curve fitting for average measured path loss. The slope of the graph is 23.6505. This indicates that the path loss exponent n for the LOS area is 2.36505, as n equals to the slope divided by 10.

Table 5.2 illustrates the parameters of the log-distance path loss model in LOS area. Substituting the values of PL(d_0) and n into Equation 3.12 in Section

Distance (m)	Average measured RSSI (dBm)	Average measured path loss (dB)
1	-49	59
2	-52.666	62.666
3	-59.666	69.666
4	-60.666	70.666
5	-62	72
6	-64.33	74
7	-65.666	75
8	-66.666	76
9	-67.333	77
10	-69.333	79
11	-70.666	80.666
12	-71.666	81.666
13	-73	83
14	-74	84
15	-75	85
16	-77	87
17	-97.666	89.6666

Table 5.1 Average measured RSSI and path loss at different distances for LOS area.

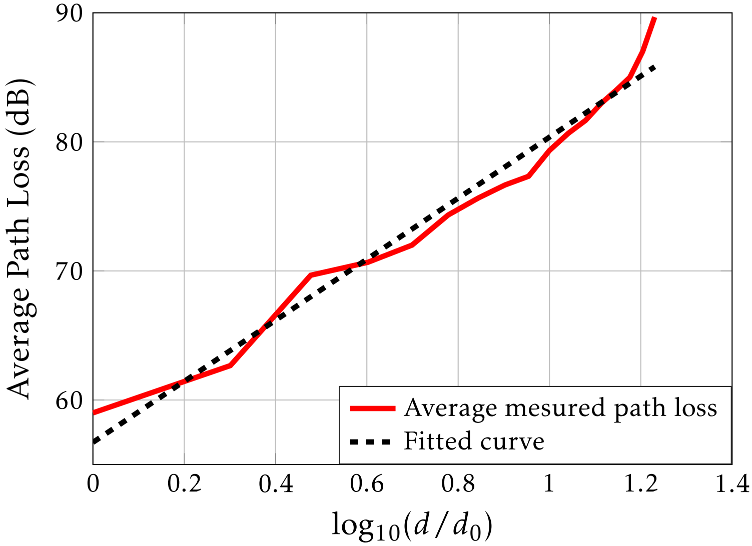


Figure 5.2 Average measured and linear curve fitting against distance for LOS area.

Average path loss at 1 m PL(d_0) (dB)	56.7547
Path loss exponent n	2.36505

Table 5.2 Parameters of the log-distance path loss model for LOS area.

3.5.3, gives the model for LOS area in HMS factory as shown in equation 5.2

$$PL_{dB} = 56.7547 + 10(2.36505)\log_{10}\left(\frac{d}{d_0}\right) \tag{5.2}$$

This equation gives the mathematical model for any random distance d from the Tx for LOS area. The obtained model is simulated using MATLAB as illustrated in Figure 5.3.

5.1.1.2 ITU MODEL

The ITU path loss model parameters are also extracted from the measured path loss data. These parameters are the distance power loss coefficient N and constant C, as discussed previously in Section 3.5.4.2. The value of N is also equal to the slope of the fitted curve of the average measured path loss as the log-normal shadowing model. This value is 23.6505. The value of C is equal to 11, where it is calculated to fix the error exists between the produced fitted

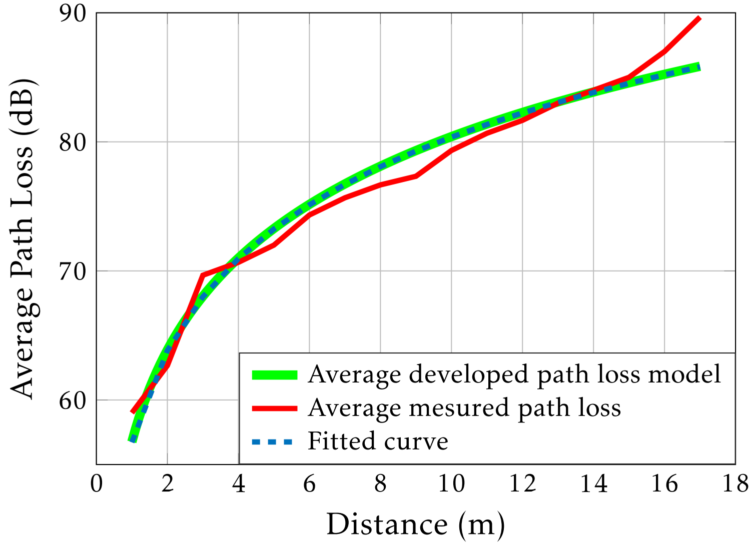


Figure 5.3 The average developed log-distance model for LOS area.

curve and the developed model.

Table 5.3 illustrates the parameters of ITU path loss model in LOS area. .

Constant C (dB)	11
Distance power loss coefficient N	23.6505

Table 5.3 Parameters of ITU path loss model for LOS area.

Substituting the values of C and N into equation 3.14 in Section 3.5.4.2, gives the ITU model for the LOS area in HMS factory as shown in equation 5.3

$$PL_{dB} = 20\log_{10} 2400 + 23.6505\log_{10}(d) - 11 \tag{5.3}$$

This equation gives the mathematical model for any random distance d from the Tx for the LOS area. The obtained model is simulated using MATLAB as illustrated in Figure 5.4.

5.1.2 NLOS-AREA1

In this area there are three machines with free space between them. A set of RSSI measurements were done also as the LOS case by the central device (Rx) at different distances from the peripheral (Tx). The measurement results were

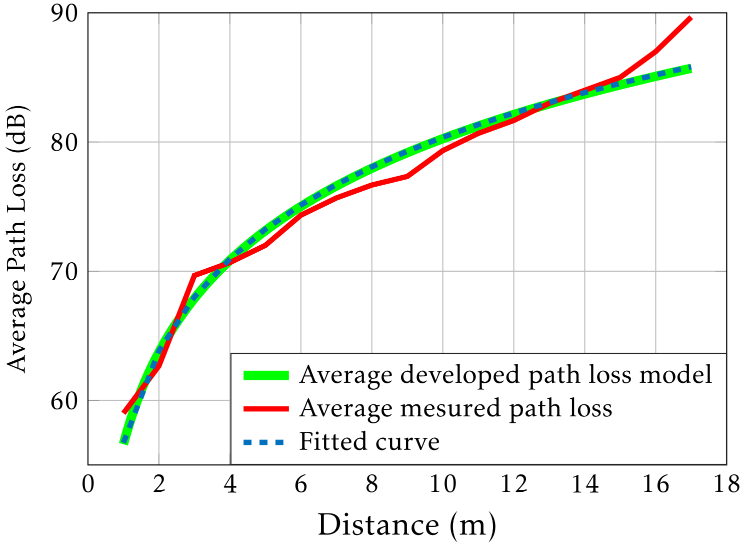


Figure 5.4 The average developed ITU model for LOS area.

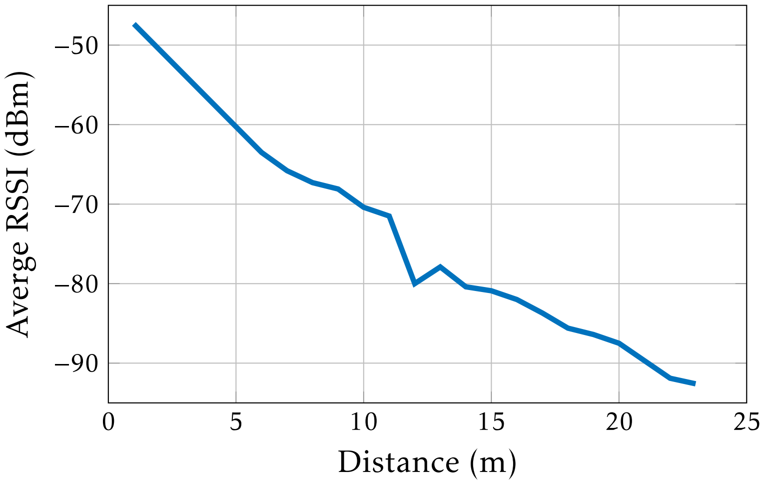
collected and an average value was calculated. The measurements distance range is from 1 m to 23 m. These informations are listed in table 5.4. As shown from the results, there is a long jump from 1 m to 6 m, as the first machine length is 5 m and the Rx can not be put inside that machine.

The measured results of this area can be shown in Figure 5.5(a). At distances 6 m and 12 m there are degradation in the average RSSI, because the Rx was adherent to the first and second machine in the NLOS-area1 path. Equation 5.1 is used to determine the average measured path loss as in LOS area. Consequently, the average measured path loss for this area is illustrated in Figure 5.6. Table 5.4 shows these values.

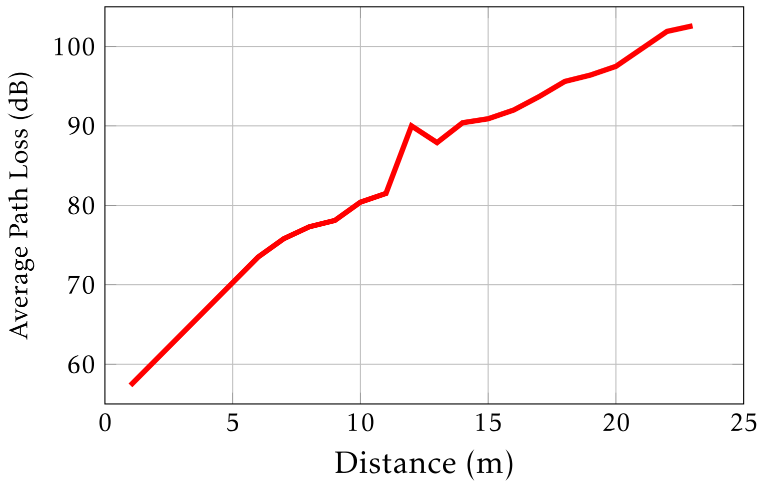
5.1.2.1 LOG-NORMAL SHADOWING MODEL

Following the same steps as LOS area, in order to calculate the path loss exponent n for NLOS-area1 are calculated. The slope of the curve in Figure 5.6 is 35.3937 and n is equal to 3.53937.In addition, the shadowing standard deviation σ is statistically computed from equation 3.13 outlined in Section 3.5.4.1. The value of σ is calculated to be 3.729 dB.

Table 5.5 shows the parameters of the log-normal shadowing path loss model in NLOS-area1. Substituting the values of PL(d_0), n and σ into Equation 3.12 in Section 3.5.4.1, gives the NLOS-area1 model in HMS factory as shown in



(a) Average measured RSSI.



(b) Average measured path loss.

Figure 5.5 Measured RSSI and path loss for NLOS-area1.

Equation 5.4.

$$PL_{dB} = 45.8953 + 10(3.53937)\log_{10}\left(\frac{d}{d_0}\right) + 3.7290 \tag{5.4}$$

Equation 5.4 gives the mathematical model for any distance d from the Tx

Distance (m)	Average measured RSSI	Average measured path loss (dB)
1	-47.330	57.3330
6	-63.500	73.5000
7	-65.800	75.8000
8	-67.300	77.3000
9	-68.100	78.1000
10	-70.400	80.4000
11	-71.500	81.5000
12	-80.000	90.000
13	-77.900	87.9000
14	-80.400	90.4000
15	-80.900	90.9000
16	-82.000	92.000
17	-83.700	93.7000
18	-85.600	95.6000
19	-86.400	96.4000
20	-87.500	97.5000
21	-89.700	99.7000
22	-91.900	101.9000
23	-92.600	102.6000

Table 5.4 Average measured RSSI and average measured path loss at different distances for NLOS-area1.

for NLOS-area1. The obtained model is simulated using MATLAB as illustrated in Figure 5.7.

5.1.2.2 ITU MODEL

The same study as LOS case was done in order to find the distance power loss coefficient N and the constant C. Table 5.6 shows the parameters of ITU path

Average path loss at 1 m PL(d_0) (dB)	45.953
Path loss exponent n	3.53937
Standard deviation σ (dB)	3.729

Table 5.5 Parameters of the log-normal shadowing path loss model for NLOS-area1.

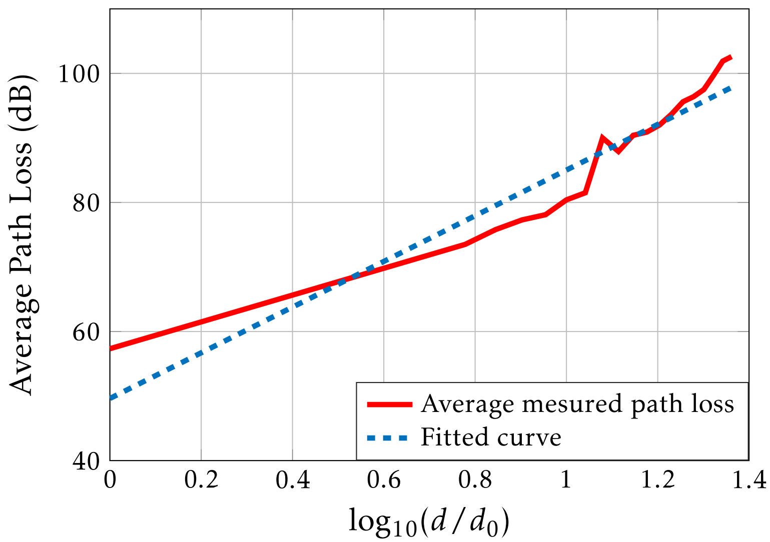


Figure 5.6 Average measured and linear curve fitting against distance NLOS-area1.

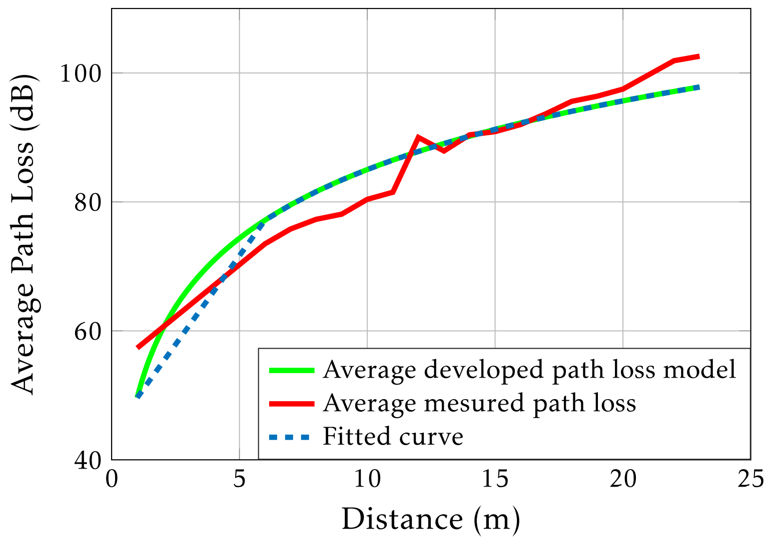


Figure 5.7 The average developed log-normal model for NLOS-area1.

loss model in NLOS-area1. Substituting the values of C and N into equation 3.14 in Section 3.5.4.2, gives the ITU model for NLOS-area1 as indicated in

Equation 5.5.

$$PL_{dB} = 20 \log_{10} 2400 + 35.393 \log_{10}(d) - 18 \tag{5.5}$$

Constant C (dB)	18
Distance power loss coefficient N	35.393

Table 5.6 Parameters of ITU path loss model for NLOS-area1.

This equation gives the mathematical model for any random distance d from the Tx for NLOS-area1. The obtained model is simulated using MATLAB as illustrated in Figure 5.8.

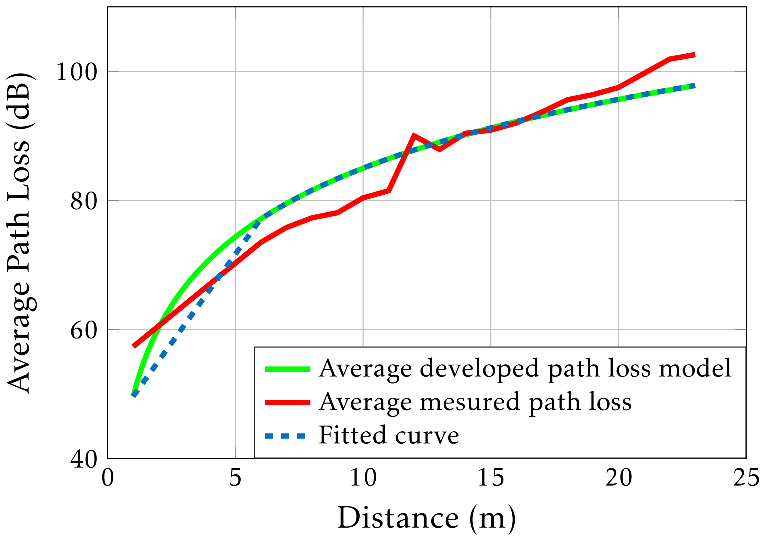


Figure 5.8 The average developed ITU model for NLOS-area1.

5.1.3 NLOS-AREA2

In this area there are five machines with no free space between them. The measurements were taken from distance 1 m to 27 m. The set of RSSI measurements were done as in NLOS-area1 and LOS area. These informations are listed in Table 5.7. As in the NLOS-area1, there is a hop in distance from 6 m to 8.6 m as the first machine length is 2.6 m and Rx can not be put inside it.

Distance (m)	Average measured RSSI	Average measured path loss(dB)
1	-47.333	57.333
2	-54.000	64.000
3	-54.8330	64.8330
4	-58.0800	68.0800
5	-60.5000	70.5000
6	-61.8000	71.8000
8.6	-71.2000	81.2000
12.85	80.000	90.000
16	-85.7000	95.7000
23.80	-86.8000	96.8000
27	-93.5000	103.5000

Table 5.7 Average measured RSSI and path loss at different distances for NLOS-area2.

The same situations happen also with the rest.

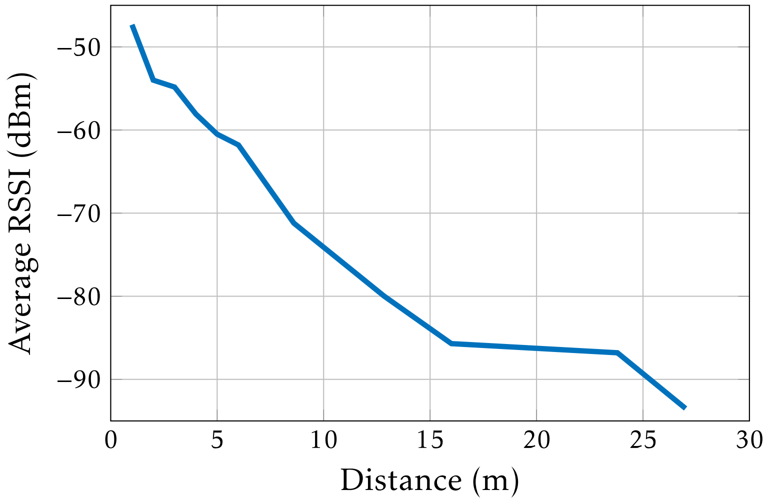
The measured results in this area are shown in Figure 5.9(a). At distances 8.6, 12.85, 16,23.80 and 27 there are degradation in the average RSSI because the Rx was adherent to the first and second machines and so on until the fifth machine in the NLOS-area2 path. Equation 5.1 is used to determine the average measured path loss, as in LOS area, so the average measured path loss for this area is illustrated in Figure 5.10. Also, these values are shown in Table 5.7.

5.1.3.1 LOG-NORMAL SHADOWING MODEL

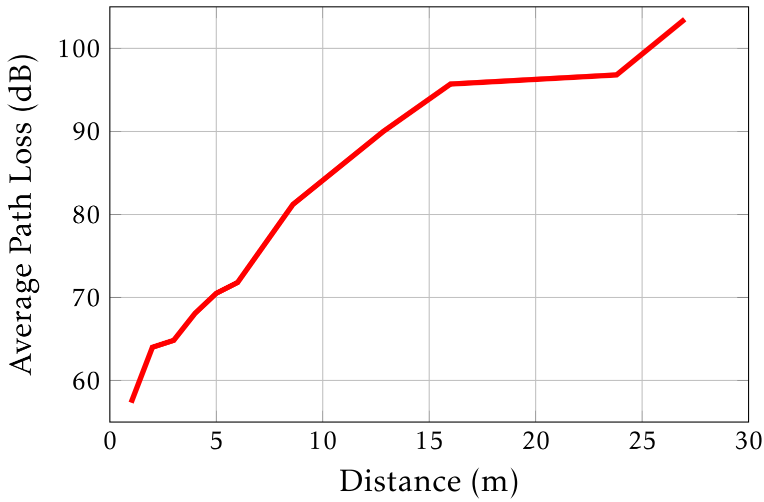
Following the same procedures as NLOS-area1, the path loss exponent n and standard deviation σ for NLOS-area2 are calculated, as illustrated in Table 5.8. Substituting the values of PL(d_0), n and σ in to equation 3.12 in Section

Average path loss at 1 m PL(d_0) (dB)	47.3266
Path loss exponent n	3.35642
Standard deviation σ (dB)	3.8563

Table 5.8 Parameters of log-normal shadowing path loss model for NLOS-area2.



(a) Average measured RSSI.



(b) Average measured Path loss.

Figure 5.9 Measured RSSI and path loss for NLOS-area2.

3.5.4.1, gives the model for NLOS-area2 as shown in Equation 5.6.

$$PL_{dB} = 47.3266 + 10(3.35642)\log_{10}\left(\frac{d}{d_0}\right) + 3.8563 \tag{5.6}$$

This equation gives the mathematical model for any random distance d from the Tx for NLOS-area2. The obtained model is simulated using MATLAB as

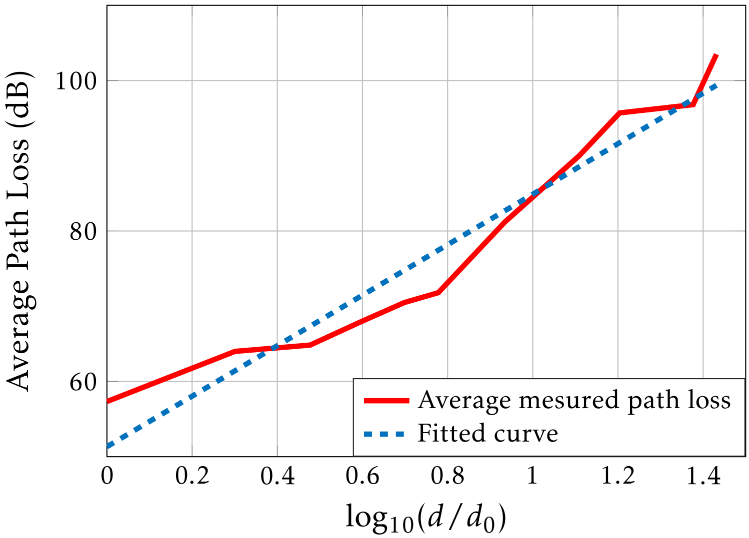


Figure 5.10 Average measured path loss and linear curve fit against distance for NLOS-area2.

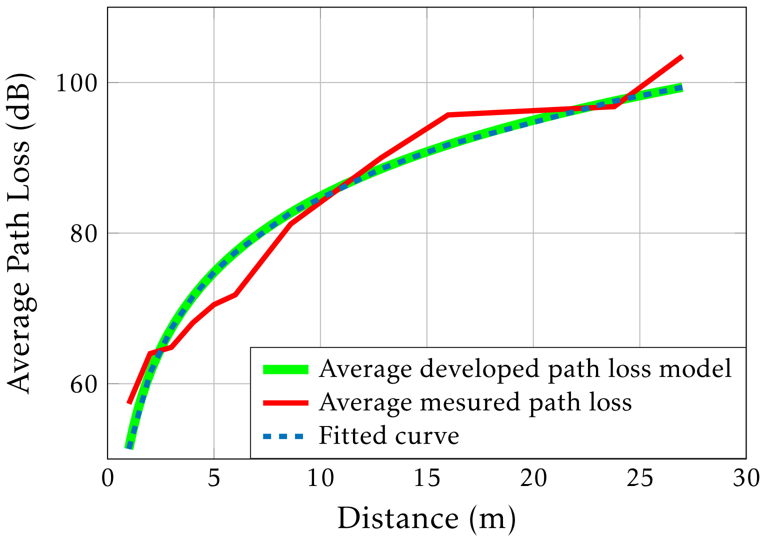


Figure 5.11 The average developed log-normal model of NLOS-area2.

illustrated in Figure 5.11.

5.1.3.2 ITU MODEL

The same study as LOS case was done in order to find the distance power loss coefficient N and the constant C, as indicated in Table 5.9. Substituting the

Constant C (dB)	16.278
Distance power loss coefficient N	33.5642

Table 5.9 Parameters of ITU path loss model. for NLOS-area2.

values of C and N into Equation 3.14 in Section 3.5.4.2, gives the model for NLOS-area2 as given in Equation 5.7.

$$PL_{dB} = 20\log_{10} 2400 + 33.5642\log_{10}(d) - 16.278 \quad (5.7)$$

This equation gives the mathematical model for any random distance d from the Tx for NLOS-area2. The obtained model is simulated using MATLAB as illustrated in Figure 5.12.

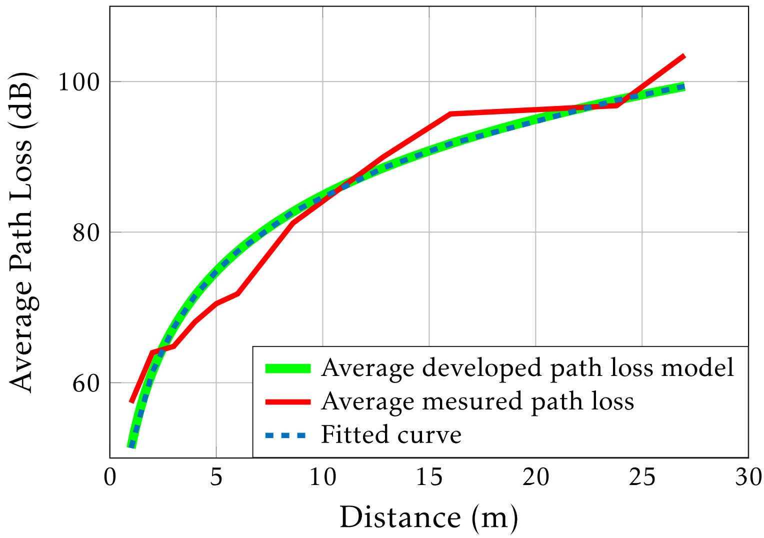


Figure 5.12 The average developed ITU model of NLOS-area2.

From the previous results, some conclusions can be drawn. Indoor propagation models based on measurements were developed for LOS area, NLOS-area1 and NLOS-area2. The Log-normal path loss model, the log-normal shadowing model and the ITU model were used to determine path loss equations for these different areas in the HMS factory. Each model has different parameters and these parameters were exacted from the measurement data. The values of these parameters were determined by fitting these models to measurement data. The results for these different areas are summarized below:

- For LOS area, the extracted parameters of log-distance path loss model show that path loss exponent n and average path loss at 1 m are 2.36505 and 56.7547 respectively. In addition, the parameters of ITU model reveal that the constant C and distance power loss coefficient are 11 and 23,6505 respectively. The values in these two models are acceptable and reasonable [10] [11].

- For NLOS-area1, the extracted parameters of log-normal shadowing path loss model show that path loss exponent n, average path loss at 1 m and standard deviation σ are 3.53937, 45.953 and 3.729 respectively. The parameters of ITU model reveal that the constant C and distance power loss coefficient are 18 and 35.393 respectively. The values in these two models are acceptable and reasonable [10] [11].

- For NLOS-area2, the extracted parameters of log-normal shadowing path loss model show that path loss exponent n, average path loss at 1 m and standard deviation σ are 3.35642, 47.3266 and 3.8563 respectively. In addition, the parameters of ITU model reveal that the constant C and distance power loss coefficient are 16.278 and 33.5642 respectively. The values in these two models are acceptable and reasonable [10] [11].

5.2 OBJECT SIGNAL LOSS RESULTS

The measurement of the signal loss due to the factory machines were collected to give a sign of the type of signal loss due to these machines. The material of these machines are metal and plastic. Table 5.10 shows the results of the object signal loss for two cases (see Section 4.3). From that table, the conclusion is that

Machine Name	**Signal loss (case1)**	**Signal loss (case2)**
Big device	17.25 dBm	9.82 dBm
Iinneo +	12.25 dBm	7.42 dBm
DEK	17.58 dBm	8.82 dBm

Table 5.10 wireless standards for BLE.

if the BLE devices are put inside the machines to detect temperature, they will cause high loss to the signal.

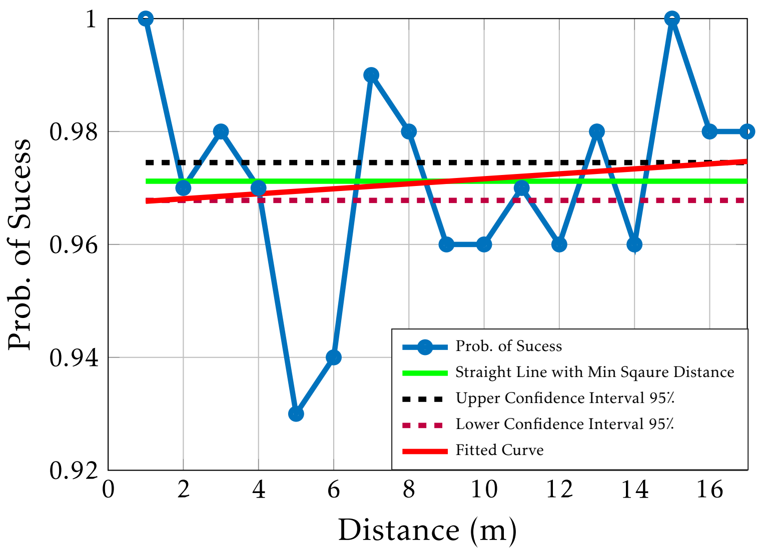


Figure 5.13 Probability of success at different distances for LOS area with 95% confidence intervals.

5.3 MEASURING PROBABILITY OF RECEIVING PACKETS SUCCESSFULLY RESULTS

Following the measurement procedures mentioned in Section 4.4.1 for LOS area and NLOS-area1, Figures 5.13 and 5.15 are drawn. Matlab regression fitting method is used to fit the measurement results as shown in Figure 5.13 which shows that the probability of success almost constant with distance, which is normal in this case where the distance range was not large enough to see high packets loss especially with no obstructing objects between the Tx and Rx for LOS area. In addition, a small number of readings was taken at each distance. Consequently, a line without slope (average of the measurements) needs to be drown in order to achieve minimum square distance between measured results and fitted results, as clarified by the green line in Figure 5.13. Also this figure shows the calculated 95% confidence intervals (upper confidence interval and lower confidence interval) of the fitted curve which are plotted in black and purple.

The confidence intervals are calculated to make sure that the measured results are within an acceptable interval of confidence which means that it is a range of values we are fairly sure our true value lies in. These two confidence intervals are divided into two limits, the first limit is the Upper Confidence Interval (UCI) and the second limit is the Lower Confidence Interval (LCI). The confidence intervals can be expressed as

$$UCI = \bar{X} + Z \times \frac{S}{\sqrt{n}}$$
$$LCI = \bar{X} - Z \times \frac{S}{\sqrt{n}} \tag{5.8}$$

Where $\bar{X}$ is the mean of the measured data, S is the standard deviation of the measured data, n is the number of measurements and Z can be found form the next table 5.11 [12].

Confidence level(%)	Z
80	1.282
85	1.440
90	1.645
95	1.960
99	2.576

Table 5.11 The Z values for Confidence Interval [12].

Figure 5.14 shows the probability of receiving packets successfully for LOS-area and the calculated 85% confidence intervals (upper confidence interval and lower confidence interval) of the fitted curve.

The probability of receiving packets results for NLOS-area1 can be observed in Figure 5.15. Also, Figure 5.15 shows the probability of success of the measurement results after regression fitting method decrease with distance.

It is also possible to get the probability of packet loss by the following Equation

$$P_{loss} = 1 - P_{success} \tag{5.9}$$

where $P_{success}$ is the probability of receiving packet successfully.

This section analyzed the measurement results of the probability of receiving packets successfully between two BLE devices for two different areas (LOS and NLOS-area1). The results for these different areas are summarized below:

- For LOS area, the results were expected, as the path between the Tx and Rx in LOS area is clear from any obstructing objects which will not cause high loss for the transmitted packets and also the distance between them was not enough to see a high packets loss. Further more,a small number of readings was taken at each distance.

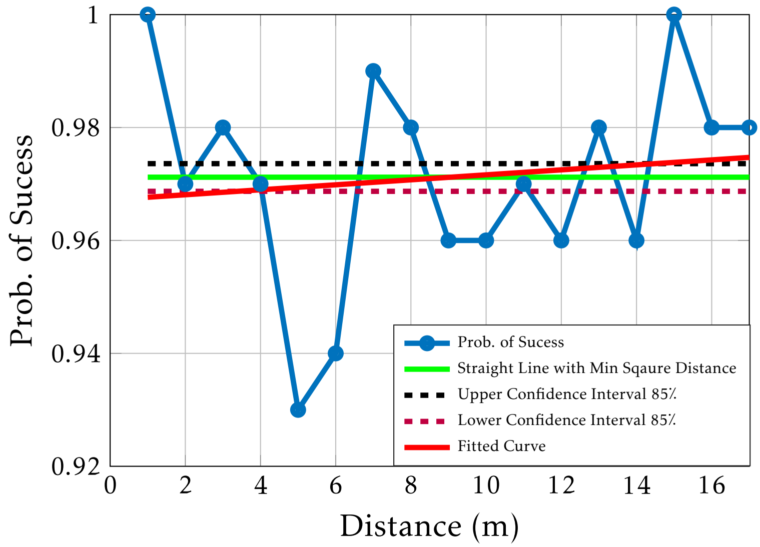


Figure 5.14 Probability of success at different distances for LOS area with 85% confidence intervals.

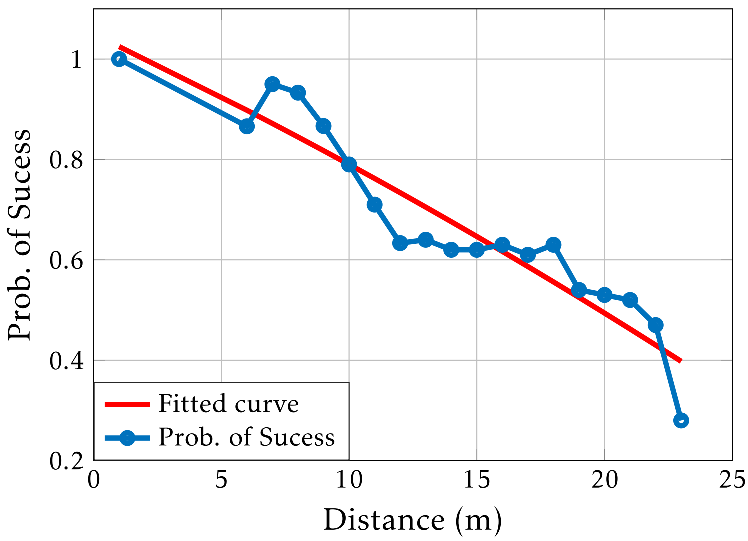


Figure 5.15 Probability of success at different distances for NLOS-area1.

- For NLOS-area1, the results were reasonable and expected as the probability of success decreases as the distances increases. The distance range was almost as the same range for LOS area, but in this case there were obstructing objects between the Tx and Rx that cause high packets loss.

5.4 RESULT SUMMERY

At the end of this chapter we can conclude that, the RSSI and probability of receiving packets successfully measured results were performed in order to analyze the link performance properties between two BLE devices and create a complete model that describes that link and how the signals are affected by the surrounding environment in order to create BLE mesh network.

Also, these extensive measurements taken at different distances in different areas, allow the BLE users to know at which distance the BLE devices should be put to establish a BLE mesh network. It is the users responsibility to decide which distance should the BLE devices should be put, taking into account the environment, the area if its LOS or NLOS-area1 or NLOS-area2 and if there obstructing objects or not.

6 Conclusion

This chapter contains conclusions about the project and what is the future work related to the studies which introduced in this project

6.1 CONCLUSION

The main objectives of this project are to gain knowledge of the Bluetooth technology features, especially with the new specification of BLE mesh and to study and understand radio wave propagation and indoor empirical path loss models in industrial environment focusing on Bluetooth mesh networking characteristics, as can be seen from the study done in Chapters 2 and 3. The indoor path loss models used in this project are the log-distance path loss model, the log-normal shadowing model and the ITU model (Chapter 3). Each model has different parameters and these parameters were exacted from the measurement data. There are three types of measurements were carried out in HMS factory to analyze the quality of the communication link between any two BLE devices. These measurements are RSSI, object signal loss and probability of receiving packet successfully, as can be seen from the measured results introduced in Chapters 5.

The RSSI extensive measurements were recorded at three different areas in HMS factory (LOS, NLOS-area1 and NLOS-area2), at 2.4 GHz band using Anybus wireless Bridge II. These RSSI readings were measured in order to build path loss models and determine path loss equations for that areas in this factory. A detailed description of the measurement setup, the experimental procedures, measurement locations and the hardware used for measurements were presented (Chapter 5). The measurement results for these different areas illustrated that the extracted parameters of the two models used in LOSarea (log-distance path loss and ITU) are reasonable. Also, the extracted parameters of the two models used in NLOS area1 and area2 (log-normal shadowing path loss and ITU) are also reasonable.

Object signal loss measurement results showed that when the BLE device put inside the factory machines will cause high attenuation to the signal. Hence, Table 5.10 can be used as a guide for BLE users.

The measurement results for the probability of receiving packet successfully showed that for LOS area there is no high loss for the transmitted packets because, the small number of readings taken at each distance, the separation distance between the Tx and Rx was not long enough to see high packet loss and this area is clear from obstructing objects. For NLOS-area1 the measurement results are reasonable and expected as, in this area there are obstructing objects between the Tx and Rx which cause high loss for the packets.

At the end of this work we can conclude that, These different measurement results enable the BLE users to know at which distance the BLE devices should be put in order to establish a BLE mesh network in side the factory environment. It is the users responsibility to decide which distance should the BLE devices should be put, taking into account the environment, the area if its LOS or NLOS-area1 or NLOS-area2 and if there obstructing objects or not.

6.2 FUTURE WORK

There are several steps that could be taken in order to further this project. BLE mesh sensors network simulation needs to be carried out in order to find, the latency and the buffer size required. The latency also depends on other factors, such as the processing time for different types of incoming packets, the random delay in the relay node introduced by the latest mesh protocol to decrease the collision between the transmitted data, and the buffer size in the node. The buffer size which effects on the latency as the size increase as the waiting time for packets before being processed by the node will increase. Furthermore, the buffer size depends on the traffic load in the network, it should be calculated in order to make sure no packets will be dropped as there is not enough buffer for it.

Bibliography

[1] R. Rondón, K. Landernäs, and M. Gidlund, "An Analytical Model of the Effective Delay Performance for Bluetooth Low Energy," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 1–6, Sept 2016.

[2] J. Tosi, F. Taffoni, M. Santacatterina, R. Sannino, and D. Formica, "Performance Evaluation of Bluetooth Low Energy: A Systematic Review," *Sensors*, vol. 17, no. 12, 2017.

[3] B. S. I. Group, "Bluetooth Mesh Profile Specifications." `https://www.bluetooth.com/specifications/mesh-specification`. Accessed: 2017-09-11.

[4] F. Andreas, *Wireless Communications Second Edition*. 2011.

[5] L. Zhang, "Channel Measurement and Modeling in Complex Environment ," Master's thesis, Technical University of Madrid School of Telecommunication Systems and Engineering, September 2016.

[6] C. Jeffrey H. Reed, "3.5 GHz Indoor Propagation Modeling and Channel Characterization ," Master's thesis, Virginia Polytechnic Institute and State University, April 2015.

[7] G. S. P. Simplified, "Log Distance Path Loss or Log Normal Shadowing Model." `https://www.gaussianwaves.com/2013/09/log-distance-path-loss-or-log-normal-shadowing-model/,[Online;accessed20-maj-2018]`. Accessed: 2018-05-20.

[8] S.Loyka, "Lecture Notes in Wireless Communication Fundamentals," September 2016.

[9] "Anybus Wireless Bridge." https://www.anybus.com/support/file-doc-downloads/wireless-bridge?ordercode=awb3000. Accessed: 2017-09-11.

[10] E. Tanghe, W. Joseph, L. Verloock, L. Martens, H. Capoen, K. V. Herwegen, and W. Vantomme, "The Industrial Indoor Channel: Large-scale and Temporal Fading at 900, 2400, and 5200 MHz," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 2740–2751, July 2008.

[11] I.-R. P.1238, "Propagation Data and Prediction Methods for The Planning of Indoor Radio Communication Systems and Radio Local Area Networks in The Frequency Range 300 MHz to 100 GHz." https://www.itu.int/rec/R-REC-P.1238/en. Accessed: 2017-06-18.

[12] L. Fang-mei, L. Shu-ru, Z. Su-zhi, C. Zeng-yu, and L. Na-Na, "The simulation and assessment of network performance based on confidence interval," in *2011 IEEE 3rd International Conference on Communication Software and Networks*, pp. 394–397, May 2011.

[13] B. S. I. Group, "Bluetooth Core Specifications v5." https://www.bluetooth.com/specifications/bluetooth-core-specification. Accessed: 2017-09-11.

[14] B. S. I. Group, "Bluetooth Mesh Model Specification ." https://www.bluetooth.com/specifications/adopted-specification. Accessed: 2017-09-11.

[15] B. S. I. Group, "Our History." https://www.bluetooth.com/about-us/our-history. Accessed: 2017-09-11.

[16] S. Brauer, A. Zubow, S. Zehl, M. Roshandel, and S. Mashhadi-Sohi, "On Practical Selective Jamming of Bluetooth Low Energy Advertising, year=2016," in *2016 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 1–6, Oct.

[17] O. Hinrichsen, *An Evaluation of Network Protocols for Bluetooth Low Energy Mesh Networks*. PhD thesis, Examensarbete utfört i Datorsystem vid Tekniska högskolan vid Linköpings universitet, 2015.

[18] R. S. MARIN, "Wireless Indoor Localization Using Path Loss-based Techniques ," Master's thesis, Tampere University of Technology, October 2015.

[19] J. Cherukuri, "Competitive Study of Stochastic Indoor Propagation Models ," Master's thesis, The University of North Carolina at Charlotte, May 2004.

[20] S. Šain, "Modeling and Characterization of Wireless Channels in Harsh Environments ," Master's thesis, Mälardalen University School of Innovation Design and Engineering, June 2011.

[21] A. STEFANSKI, "Characterization of Radio Wave Propagation in Indoor Industrial Environments ," Master's thesis, The University of British Columbia, August 2010.

[22] K. H. C. Khoo, "Indoor Radio Channel of Bluetooth Technology ," Master's thesis, Edith Cowan University Western Australia, February 2001.

[23] L. Couch, II, *Mobile Communications Handbook*. 1999.

[24] T. S. Rappaport, S. Y. Seidel, and K. Takamizawa, "Statistical Channel Impulse Response Models for Factory and Open Plan Building Radio Communicate System Design," *IEEE Transactions on Communications*, vol. 39, pp. 794–807, May 1991.

[25] R. Mardeni and Y. Solahuddin, "Path Loss Model Development for Indoor Signal Loss Prediction at 2.4 GHz 802.11n network," in *2012 International Conference on Microwave and Millimeter Wave Technology (ICMMT)*, vol. 2, pp. 1–4, May 2012.

[26] B. Sujak, D. K. Ghodgaonkar, B. M. Ali, and S. Khatun, "Indoor Propagation Channel Models for WLAN 802.11b at 2.4 GHz ISM Band," in *2005 Asia-Pacific Conference on Applied Electromagnetics*, pp. 5 pp.–, Dec 2005.

[27] Y. F. Solahuddin and R. Mardeni, "Indoor Empirical Path Loss Prediction Model for 2.4 GHz 802.11n network," in *2011 IEEE International Conference on Control System, Computing and Engineering*, pp. 12–17, Nov 2011.

[28] A. Alwarafy, A. I. Sulyman, A. Alsanie, S. Alshebeili, and H. Behairy, "Receiver Spatial Diversity Propagation Path-loss Model for an Indoor Environment at 2.4 GHz," in *2015 6th International Conference on the Network of the Future (NOF)*, pp. 1–4, Sept 2015.

[29] T. S. Rappaport and C. D. McGillem, "UHF Fading in Factories," *IEEE Journal on Selected Areas in Communications*, vol. 7, pp. 40–48, Jan 1989.