DESIGN CONSIDERATIONS FOR WIRELESS SENSOR NETWORK FOR INDUSTRIAL AUTOMATION

BY

YOUSUF DAWOOD AL-MOALLEM

A Thesis Presented to the
DEANSHIP OF GRADUATE STUDIES

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

In

ELECTRICAL ENGINEERING

June 1, 2010

KING FAHAD UNIVERSITY OF PETROLEUM & MINERALS
DHAHRAN 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

This thesis, written by **YOUSUF DAWOOD AL-MOALLEM** under the direction of his thesis advisor and approved by his thesis committee, has been presented to and accepted by the Dean of the Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN ELECTRICAL ENGINEERING**.

THESIS COMMITTEE

Prof. Asrar Ul-Haq Sheikh (Advisor)

Prof. Slim Alouini (Member)

Dr. Tareq Y. Al-Naffouri (Member)

Dr. Samir Al-Ghadban (Member)

Dr. Ali Hussein Muqaibel (Member)

Dr. Samir H. Abdul-Jauwad
Department Chairman

Dr. Salam A. Zummo
Dean of Graduate Studies

21/6/10
Date

In the name of Allah, Most Gracious, Most Merciful

DEDICATION

All praises are due to Allah, who created me from null, and gifted to me all of the favors that I am holding, including health and prosperity. This accomplishment will not be forgotten as a gift out of those uncountable favors that Allah has given me.

This work is dedicated to my beloved parents. My father, who has been a source of encouragement and inspiration to me throughout my life, was the source of my vision in this achievement. It is also dedicated to my mother, who continues to teach and develop me and for her resilience in insisting I make a contribution to our world.

This thesis would be incomplete without a mention of the support given to me by my wife, to whom this work is also dedicated. She kept my spirits up when the muses failed me. Without her never-failing encouragement when this thesis seemed interminable, and her unlimited support and immolation in my total years of Master study, I doubt it should ever have been completed.

May God bless you.

ACKNOWLEDGEMENT

Acknowledgment is due to the King Fahad University of Petroleum & Minerals for supporting this research with all research facilities in the central library, and for the sounder device used in the measurements within this work.

I wish to express my honest appreciation to my Advisor, Professor Asrar Sheikh, who was not only supporting as usual in his thesis supervision, but also treated the study as if the work belongs to him. I gained much from him, and could feel very clearly the sharp improvement in my thinking as well as in my research experience after spending more than two years working with him, and seeing the countless hours of attention he devoted throughout the course of the work. The days we spent for the measurements in the plant cannot be forgotten.

I also wish to thank the other members of my thesis committee. Thanks to Dr. Slim Alouini from KAUST, who contributed a lot in the work remotely though e-mails and videoconference meetings. Thanks to Dr. Tareq Al-Naffouri, who was very helpful and always followed up with me throughout the whole work. Thanks to Dr. Samir Al-Ghadban, who taught med that patience and insistence are essential for success in research. Thanks to Dr. Ali Hussein Muqaibel for his constant concern and continuous advice; from the comments I received from him significantly improved the

research and he gave me critical pushes during my work. I also further want to thank Mr. Umar Johar, who always concerned himself with the thesis' progress, supporting me with many favors, and Mr. Abdul Hameed Farazi, the lab technician, for assistance in all measurement sessions and for his time spent working in the lab. I can't forget to also thank our department chairman, who did not miss any chance to help.

I wish to express my appreciation to SABIC Cooperation, represented by HADEED management, who provide all required support and time required to complete the study. I wish to thank Mr. Abdullah Al- Jaedi (SABIC General Manger), who did not miss any chance to help; Mr. Alaa Fadak (SABIC Manger), who served to complete measurements needed inside Hot Strip Mill plant, offered beneficial discussions in different topics, and continuously advising me; Mr. Mubarak Al-Mutairi (HADEED Superintendent), who was very helpful and always concerned about the work progress; and Mr. Abdulaziz Al-Ruwaily (HADEED Superintendent), who give me the most support and facilitated all allowable opportunity throughout the entire work.

TABLE OF CONTENTS

LIST OF TABLES

Table# Description Page

LIST OF FIGURES

Figure No. **Description** **Page**

ABSTRACT

NAME: YOUSUF DAWOOD SULAIMAN AL-MOALLEM

TITLE: DESIGN CONSIDERATION FOR WIRELESS SENSOR NETWORK FOR INDUSTRIAL AUTOMATION

MAJOR FILED: ELECTRICAL ENGINEERING

DATE OF DEGREE: June 1, 2010

This thesis studies three major issues that affect deployment of wireless network in Industrial Plants for monitoring and control. Many benefits are acquired by using wireless communication systems in industries such as financial saving, safer for maintenance, and easier diagnosing. The **First** issue is to assess suitability of wireless technologies for industrial networks. This thesis evaluates WPAN (IEEE802.15) and WLAN (IEEE802.11) as Bluetooth, ZigBee, Wi-Fi and SP100 are candidate networks. The **Second** hurdle is to characterize the industrial environment from radio wave propagation aspects. Extensive measurements are done in Hot Strip Mill and resulting Impulse responses are analyzed. The **Third** issue is of performance of candidate data transmission formats to determine data rates and ensuring bit error rates.

ABSTRACT (ARABIC)

ملخص الرسالة

الاسم: يوسف بن داود بن سليمان المعلم

عنوان الرسالة: تصميم شبكات الأجهزة اللاسلكية في المصانع الأوتوماتيكية

التخصص: الهندسة الكهربائية

تاريخ منح الدرجة: 1 يونيو 2010

يتم في هذه الأطروحة دراسة ثلاث مباحث رئيسية تسببت في تأخير استخدام شبكات الأجهزة اللاسلكية في بيئة المصانع. المبحث الأول: يختص بتعريف النموذج المثالي لتصميم شبكات المصانع اللاسلكية، من خلال تعيين مؤشرات الأداء الفاعلة لشبكات المصانع، ثم استخدامها لتقييم التكنولوجيات اللاسلكية المنتشرة على نطاق واسع في العالم اليوم؛ وهذه التكنولوجيات تنتمي إما إلى الشبكات اللاسلكية المحلية أو إلى الشبكات اللاسلكية الشخصية المبنية على قواعد المقاييس العالمية (IEEE802.15) أو (IEEE802.11) والتكنولوجيات المختارة هي البلوتوث ، والزيجبي ، والواي فاي. المبحث الثاني: يعرض نتائج تجارب قياس ميدانية تم أخذها في أحد مصانع الحديد لاختبار القنوات اللاسلكية عن طريق أجهزة السبر (channel sounder)، ثم تحليل الردود والقياسات لمعرفة المقدرة الواقعية للقنوات اللاسلكية في المصانع؛ كالاعتمادية والأمان و سرعة نقل البيانات المحتملة . المبحث الثالث: يتم تصميم الشبكات اللاسلكية من خلال ربط جميع نتائج مباحث الرسالة، مع التركيز على دراسة تأثير تشتت الإشارات داخل ممرات القنوات اللاسلكية على مستوى جودة الاتصال، ثم تمثيل نظم شبكات الأجهزة اللاسلكية في المصانع على برامج الكمبيوتر لقياس معدل الأداء والخطأ.

INTRODUCTION

Most industry analysts are forecasting a rapid growth in the use of wireless data network technologies in monitoring and control of industrial operations over the next few years. At present, only a few industries have deployed wireless technology in their existing plants, but the trend of replacing wired network by wireless network is growing. Examples of these are basic product industries like chemicals or metals plants, oil, gas, or petroleum refineries, power generation and desalination, and high-tech plants like, pharmaceuticals industries [1]. Several automation and control companies, e.g. Honeywell[1], Siemens[2], Emerson[3], Rockwell[4] and ABB[5], offer wireless solutions to industry.

The used of wireless networks in Industrial Plants offers many advantages including operating saving, as well it results in massive reduction in time and effort compared with wired systems in both installation and maintenance. The commissioning period is shortened since all wire laying and connection work is eliminated. In harsh environments potential damage to cabling is avoided. Wireless systems are scalable as provision of additional capacity, system setup and reconfiguration becomes easier.

[1] http://hpsweb.honeywell.com
[2] http://w1.siemens.com
[3] http://www.emersonprocess.com/Rosemount
[4] http://www.rockwellautomation.com
[5] http://www.abb.com

The saving in time is one of most important performance indicator of operational and maintenance health in industrial business. It directly affects the plant production rate and equipment availability. Replacing cables is expansive not only because of cable cost but also difficulties arising in routing the cable to inaccessible places which is a time consuming process. Furthermore non-operational or defective link in a wireless network can be rectified quickly by replacing either the transmitter or the receiver. In harsh environment, which is the case in many industries, maintaining cables in heat, motion, humidity, etc. is much more difficult as compared to troubleshooting of conveniently located boxes in wireless systems. This assures higher equipment availability and more time becomes available for production. Furthermore, the task of temporarily accessing any machinery in the plant for diagnostic or programming purposes can be greatly simplified by the use of wireless technologies.

From safety aspect, wireless networks are ideal for deployment in hazardous environments. Human exposure to field and hazardous equipment is reduced since cabling is avoided. Risk increases during replacement of damaged cables which may need a major labor-effort. The extend of the cabling task can be seen in Figure 1.1.

Figure 1.1: Cable marshaling panel

Even with all these advantages of using wireless sensor network technology in plants, wireless networks were not deployed to date in most industries. This is because of lack in-depth evaluation of the suitability of wireless technologies.

This research reported in this thesis provides a clear understanding to the issues. The thesis describes the design procedure of deploying wireless technology in industry by considering three major issues: wired industrial network characteristics; assessment of wireless technologies; and industrial wireless channel sounding. Figure 1.2 presents a clearer global view for the problem.

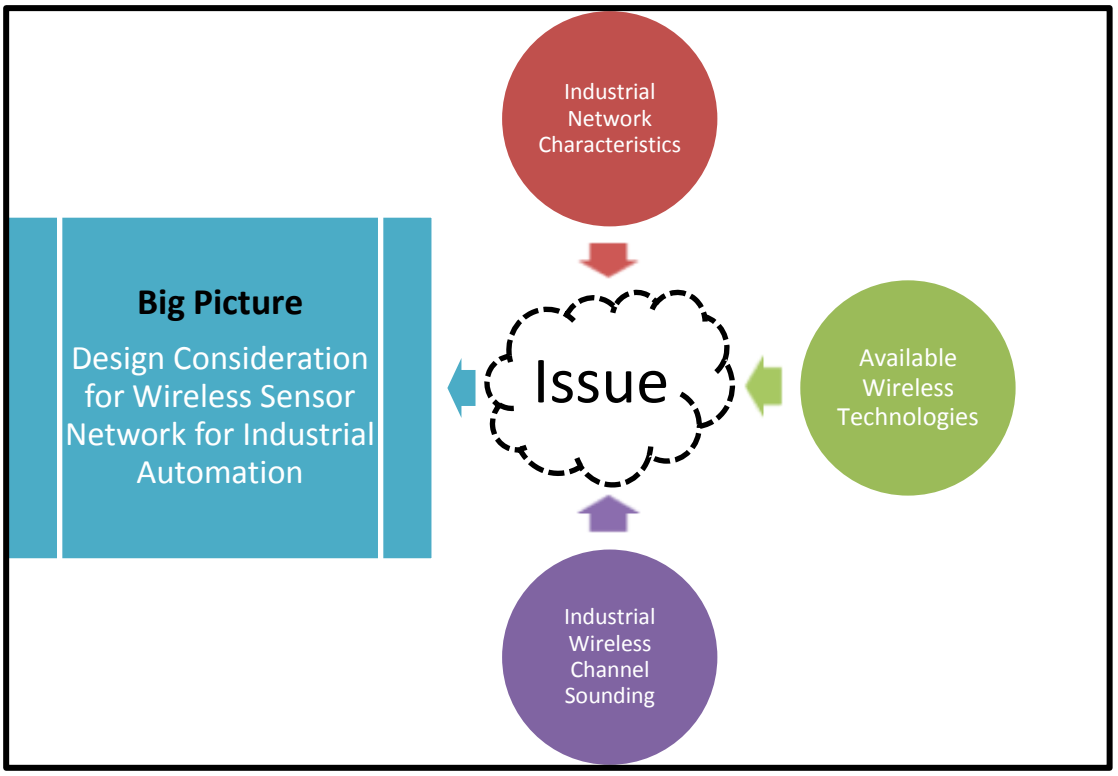


Figure 1.2: Thesis objective

Research methodology in this thesis is to study the three issues and to present the results of studies in a unified way. In **Chapter 2**, an answer to the previously raised question is given by presenting an understanding of wired network used in industries. The research highlights opportunities for improvements that need to be considered in designing wireless systems. Plant owners usually do not have much faith in wireless network reliability, its availability and security. Wireless system availability and its security aspect are discussed in **Chapter 3** for several wireless systems with their standards. The suitability to industrial plants of the most widely used wireless technologies that belonging to IEEE standards either IEEE802.15 (WPAN) or IEEE802.11 (WLAN) are discussed. Third important issue is that of to characterization of radio environment which is addressed in **Chapter 4**.

Channel sounding systems have been used to measure wireless channel impulse response which is essential for radio link designs. Hot strip steel mill is selected as a target to characterize wireless channel. Finally, **Chapter *5*** ties together the collected information, in recommending a certain System Configuration. The performance of digital transmission System is studied by running simulation experiments to find several modulations formats over the measured channels.

This thesis presents guidelines to design wireless network but it does not go into detailed network design. In the appendices of this thesis report, there are; (1) figures of all measurements power delay profiles, (2) generated channel models foe selected measurements, (3) simulation results of bit error rate for selected measurements, and (4) list of all acronyms used in the report.

2

CHARACTERISTICS OF INDUSTRIAL NETWORK

With unprecedented growth in application of wireless systems in public and private sectors, this technology is now making inroads in industrial application. The researchers are developing new wireless systems using mature technologies to break barriers in the use of wireless system in industries. But the industrial environment has its own special characteristics and requirements. The major challenge of a wireless system in achieving industrial standards is to be robust enough to manage running plant processes for both monitoring and control. Control of plant processes requires assortment data transmission speeds depending on the application on hand. In some situations requiring a very high speed process, digital networking may not be able to meet required needs and a use of direct analog connections between controller and devices may become necessary.

Before starting the design, the key characteristics of industrial sensor networks need to be pointed out. Since Fieldbus is the most commonly wired technology used in industries, studying Fieldbus properties can provide excellent reference that forms the desired key characteristics of industrial sensor networks.

Fieldbus is a mature system specifically designed to perform automation tasks. It is a wired technology that assures reliable communication and relies on the interconnection of digital controllers, sensors and actuators located at various places in the plant. Its break down record proves its ability to provide sustained high Quality of Service (QoS) in industrial wired networking. Fieldbus properties are used for benchmarking new industrial wireless network technologies.

In industrial environment, only some of the existing wireless technologies can be used. Applications of wireless technologies in industrial automation and process control have many advantages over the wired system. There exist some additional concerns like security, susceptible radio environment etc. However these can be overcome with inclusion of certain safeguards like encryption, modulation and encoding techniques. This chapter studies requirements of wireless industrial network, starting with a brief history of Fieldbus with technical description. Then, the desirable characteristics for industrial networking in the light of wireless challenges are presented.

2.1 FIELDBUS OVERVIEW

Wired Fieldbus systems like: PROFIBUS[1], CAN[2], HART[3] or ABB-AF100[4] are wired systems currently used in many industries. In 1994, Inter Operable Systems Project (ISP) and WorldFIP[5], two supplier consortia, merged to form the Fieldbus Foundation. Fieldbus Foundation[6] is a non-profit trade consortium representing the major process automation industry suppliers and end-users worldwide. It has taken a leadership role in the development of Fieldbus digital communications and integrated system architecture based on regional and international standards. The technology began in 1970 with the first attempts to distribute control functionality to the field level. With the introduction of the Distributed Control System (DCS), processing plants were able to distribute intelligent control throughout process facilities. Fieldbus is a single bus, i.e. twisted pair, coaxial, or fiber-optic, carrying digital signals and sometimes DC power that connect several field devices [2].

Fieldbus protocol architecture usually covers physical layer, data-link layer including Medium Access Control (MAC) sub layer, and the application layer. The key purpose of the network is to grant real-time communication services that are both reliable and predictable, i.e. error-free packets delivery without much delay.

[1] http://www.profibus.com see also PROFINET: http://www.profibus.com/pn/profinet
[2] http://www.can-cia.org
[3] http://www.hartcomm2.org
[4] http://www.abb.com
[5] http://www.worldfip.org
[6] http://www.fieldbus.org

Fieldbus system supports two kinds of communication: (1) process data and (2) message transfer. **Process data** are dynamic data used to monitor and control a process, while message transfer is used for parameters, program loading and diagnostic purposes. Process Data is managed through Cyclic Data Packets (CDP). Each CDP is configured on the communication interface for a certain signal identity, cycle time, size and direction. Each signal identity uniquely represents transmitter-receiver pair. The cycle time determines how often the data packet is transferred on the bus. Because the interval between consecutive transfers is fixed, process data transfer is deterministic, regardless of the current communication tasks. Packet size is usually fixed also. Unless both the size and the signal address of corresponding packet are correct no transmission takes place. Some features of Fieldbus traffic, i.e. data type and data rate transmitted through the Fieldbus, are; presence of periodic traffic and presence of important acyclic traffic packets like alarms; and short packets.

Second type of communication in Fieldbus is **Message transfer.** It is not performed cyclically like process data. Message transfer does not influence process data since a certain amount of the bandwidth is reserved for message transfer, regardless of the bus load due to process data transfer. A bus-master node is usually required in Fieldbus to control all transmissions on network. Communication is based on the Master-Slave concepts where the master node initiate communication request and the slave node responds. Thus, without a communication request from the master node no communication is possible. If a slave frame is missed, the master frame simply asks to recover with another frame.

Real-time communication between controllers and sensors/actuators is a fundamental requirement in the industrial environment which puts many constraints in the digital network design. In [3], depending on process nature, controller reaction time is classified into three classes:

1. **Class I**: with 100 ms cycle time is meant for human machine interface. This requirement can be fulfilled by TCP/IP communication protocol without any problem.

2. **Class II**: with 10 ms cycle time is used for tooling machine control. This needs special care in Real-Time Ethernet (RTE) equipment.

3. **Class III**: has the most demanding rate of 1 ms cycle time. It is used for motion control. To meet this requirement, many modifications are required on MAC layer. At present, this class is controlled through a direct analog interface connection between controller and the field device because digital networks cannot support this class.

2.2 WIRELESS FIELDBUS CHARACTERISTICS

Because of Industrial environment has its own specific characteristics and requirements, many wireless technologies are not suited to industrial application if these do not meet certain key requirements. In this section, a scientific method of technologies comparison is used to assess a number of selected wireless technologies in industrial environment. Methodology first defines the performance criteria called Key Performance Indicators (KPI) and then assigns sensible weight for each criterion. According to the selected KPI, each selected wireless technology is assessed and ranked. These are carefully selected based on both *literature survey* as well as *work experience* point of view. The following 12 KPI from the basis of this study for selecting the suitable technology: *Data Rate*, *Device Range*, *Reliability*, *Availability Resilience*, *Network Latency*, *Throughput*, *Security*, *Power Consumption*, *Network Topology*, *Number of Devices*, *Medium Accessing*, *Operating Frequency*, *Complexity*, *Scalability*, *and Flexibility*. KPI's are ordered according to their priorities starting from highest to lowest.

1. *Data Rate*: Data rate indicates the speed at which data is transferred from one device to another. In industries, Fieldbus data rate is a function of cable length, see Table 2.1 [4]. The table shows the data rate as a function of segment length for two selected wired technologies: ProfiBus & DeviceNet. In industrial environment, data rate varies from several tens of kbps up to few Mbps depending on the nature of the process [4]. For wireless system, the time

dispersion in industrial wireless channel is large. Waveforms of different symbols may overlap at the receiver which causes inter-symbol interference (ISI) and hence either data rate should be reduced or additional effort is necessary to reconstruct the correct symbol [5]. Industrial networks require both low duty cycle communication as regular-packet, and fast communication for delivering emergency-packets. Data rate for wireless systems is related to available bandwidth and modulation format. The modulation technology, encryption techniques, packet length, and radio frequency also influence the data transmission rate. [3]

Table 2.1: Some Wire Fieldbus data rate [4]

Wired Technology	ProfiBus (number of nodes=32)		DeviceNet (number of nodes=64)	
	Segment Length (m)	Data Rate (kbps)	Segment Length (m)	Data Rate (kbps)
Range 1	1200	93.75	500	125
Range 2	600	182.5	250	250
Range 3	200	500	100	500

2. *Device Range*: Device range defines the maximum allowable distance between transmitter and receiver. In Fieldbus there is a limit for bus cable length; see Table 2.1. In wireless systems, a device must be within the range of second device in order to exchange data. The data range is influenced by interference, the radio transceiver (transmitted power and receiver sensitivity), and the operating frequency. Path-loss is the attenuation experienced by radio wave while in transit from a transmitter to a receiver. It is affected by, large scale effects, free space loss, refraction, diffraction, reflection and shadow. In addition, path-loss is affected by terrain undulations, distance between transmitter and

receiver, antenna height and antenna location. There are several propagation loss models, e.g. Okumura, and Hata Model, which calculate path-loss for outdoor systems. However, those models cannot be applied to industrial environment because of their unique nature. In most industries, 50m is the maximum range required for communication between the devices [6]. The presence of metallic bodies and structures increases the amount of radio interference.

3. *Number of Devices*: All communication systems define the maximum number of nodes that network can handle. This property depends on more than one parameter like network data rate, process updating speed requirement, and network topology. In most real industrial applications many hundreds and possibly thousands of devices are installed. Hence the more nodes that a network can handle the better it is.

4. *Reliability, Availability and Resilience*: (4.a) Reliability is the probability that a device will perform its intended function during a specified period of time under stated conditions. Reliability can be expressed as:

$$R\{T\} = Pr\{t > T\} \qquad (2.1)$$

where; $R\{T\}$ is the reliability of the system defined as the probability that the system perform intended function reliably exceeding time period T without failure. A similar function maybe defined in communication system as the probability delivering error-free packets. However, received signal often can be represented as:

$$r(t) = \alpha(t) \times x(t) + \mathcal{N}(t) \qquad (2.2)$$

where; $x(t)$ is the transmitted signal, $\mathcal{N}(t)$ is the additive noise and $\alpha(t)$ is the attenuation factor function. From this equation, there are two sources of impairment affecting reliability; additive noise (i.e. AWGN), and attenuation effects, i.e. large- and small-scale. In industrial environment, a transmitted signal is subjected to many reflections and diffraction which distort the signal waveform. Due to multipath propagation, multiple copies of the same waveform reach the receiver with delays causing time dispersion of the signal known as ISI. The Inter-Symbol Interference (ISI) is an important consequence of time dispersion of the signal caused by the channel vagaries [7].

(4.b) *Availability* is defined as ratio of time period for which the system is performs as intended to the total given time period. It is usually measured based on Mean Time Between Failures (*MTBF*), and Mean Time To Repair (*MTTR*):

$$A = \frac{MTBF}{MTBF + MTTR} \qquad (2.3)$$

In Fieldbus network, availability can be improved by sharing the bus-master responsibility between all bus-administrative nodes and optimizing it. This can be achieved if network is designed to handle a dummy bus-master node, where responsibilities are cyclically passed over from node to node. Therefore, network operation can be recovered once the bus-master node crashes, and then another bus-administrator node detect timeout due to bus-master silence and becomes

the new bus-master. In wireless systems, network availability is affected if the signal is significantly attenuated during a deep fade, for instance.

(4.c) *Resilience* is system's ability to adopt automatically to changes or at least is able to detect irresolvable situations. It is preferable that technology manages the network configuration without human interference. A new node is automatically recognized and participates in communication as configured without any manual intervention. Starting, stopping, and restarting stations can also be done without disturbing the traffic flow on the network.

5. *Network Latency and Throughput*: (5.a) *Network latency* is a performance indicator for the network that measures the time that data gets transferred from source to destination. It is application dependant. Industry designers define the maximum acceptable delay between data transmission and reception to avoid production loss due to uncontrollable process. The industrial networks works on half-duplex system which allows communication in both directions, but only one direction at a time and not simultaneously which is normally achieved through either Time Division Duplexer (TDD) with Frequency Division Multiple-Access (FDMA) for Process Transfer or Carrier Sense Multiple-Access (CSMA) for Message Transfer. In Fieldbus, real-time characteristic is very important which depends on the temporal property of the MAC protocol. Some Fieldbus manufacturers are adopting a Schedule Table (ST) to control the real-time communication, as explained in [8]. End of transmission indication is required for half-duplex system which adds a drawback of time loss, or capacity loss, for receives-transmit turnovers [4]. Time synchronization messages are sent over the network

periodically to synchronize all node's clocks. Performing this task assures real-time communication validity. Some Fieldbus systems are using token-passing protocols to reduce packet collision where token authority is passed around between authorized nodes. But this may increase the time delay when network load is small [9]. Another latency consideration is how long a new device takes to join the network.

(5.b) *Throughput* is the amount of data transferred per unit of time. Latency and throughput are generally inversely proportional.

6. *Security:* Communication security is the system ability to avoid unauthorized access to the network. Fieldbus uses few security-encoding techniques like cyclic redundancy check (CRC) to maintain security. In general, wired communication systems authenticity is much easier than in wireless systems. Wireless system is easier to hack than a wired system. In unprotected networks, both authorized and unauthorized entities have equal access level. It is very critical for industries to avoid data hacking which directly affects network reliability and timely transmission. Four types of threats are possible; eavesdropping, inserting malicious packets to damage the message, viruses attacking to damage the system, or simply jamming the medium. On the other hand, ensuring security goals like confidentiality or accountability was not the main focus in the design of many Fieldbus systems. The recent trend to connect industrial network to the Internet by means of gateways has led to research towards securing the gateway but it is also required to protect a Fieldbus against attacks from the inside, for example by employing proper encryption and authentication schemes.

7. *Power Consumption*: Power consumption of a device is an important consideration as frequent replacement of power sources (i.e. batteries) are to be avoided. A good indicator for the power profile of a given system can be defined as the period of time for which a device can sustain without a need to attend for repair as battery replacement for instance. In Fieldbus network, this is not considered since power cabling is available. In contrast, wireless devices are preferably to be battery-operated to avoid cabling. This decreases power wiring costs and increases device flexibility. The huge reduction in size and power consumption of CMOS circuit has led researchers and field-devices manufacturers to work on industrial wireless field. Sleep mode is needed as a power saver option. The power required for a device to join a network and access the channel for normal cyclic data packet influences the efficiency of power profile. Multi-access technology also influences the time at which device should not be in sleep mode. Several mechanisms to conserve energy in protocols and applications have been developed in the context of wireless sensor networks. In absence of power cabling, which is the often case of wireless systems, few options are available such as; batteries, energy-scavenging methods or wireless energy transmission.

   a. *Batteries*: It is the most important method indicating importance of ability to conserve power is a key consideration. Frequent batteries replacement may not be feasible in industries as it leads to increase machine downtimes or increase preventive maintenance which increases manpower cost.

   b. *Energy Scavenging*: Many researchers work to explore methods of scavenging ambient power to be used on low power wireless electronic devices as self-sustaining. Studies are concentrating on the development of vibration based

generators which converts energy from low-level vibrations to electricity. Current results have verified power density of about 200mW/cm^3 from input vibrations of 2.25m/s^2 at 120Hz. [10]

In the design of wired Fieldbus protocols, the main concern is the real-time communications feature but not energy-efficient feature. However, there are efforts to combine both targets [11]. In [12], power consumption is given as a function of device range, see Table 2.2

Table 2.2: Power consumption for different wireless ranges

	Power	Range
Class I:	20 dBm (100 mW)	100 m
Class II:	4 dBm (2.5 mW)	10 m
Class III:	0 dBm (1 mW)	1 m

Another consideration is the duty cycle time which is defined as transmission period over total cycle period,

$$\text{Duty Cycle} = \frac{T_{tx}}{T_{cyc}} \qquad (2.4)$$

where, T_{tx} is the transmission period, and T_{cyc} is the total cycle period, see Figure 2.1. Power consumption is optimized by using extremely low duty cycles, so that the device is active for a very small fraction of the time. If device is not transmitting or receiving, power consumption is minimal and it is said to be in *sleep mode*. Also modulation can affect power consumption by optimizing peak-to-average power ratio.

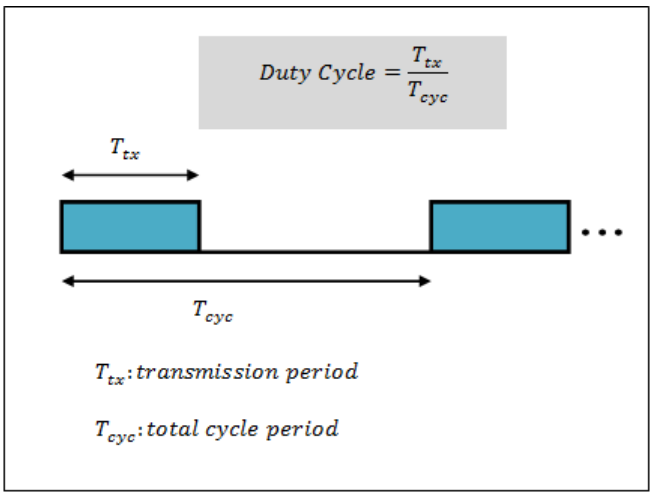


Figure 2.1: Power consumption for deferent wireless ranges

8. *Network Topology:* Network topology refers to the manner in which network nodes and links are arranged or mapped physically and logically. Most Fieldbus manufacturer build their product based on a bus topology where packets are broadcast on the bus, i.e. while a node sends a data packet, all other nodes are listening but only the node with correct address identity receives the data. Fieldbus also supports network redundancy and in case one bus failed, the redundant one takes over. Available network topology options influence which applications a network model is most suitable. It can increase the channel diversity and improve signal quality. Usually, mesh topology gives the highest number of independent paths. In wireless system the most common network topologies are: (see Figure 2.2)

   a. **Star Topology:** Star topology has a central node, which is linked to all other nodes in the network. All messages travel via the central node.

b. **Tree Topology:** Tree topology has a top node with a branch/leaf structure below. To reach its destination, a message travels up the tree (as far as necessary) and then down the tree.

c. **Mesh Topology:** Mesh topology has a tree-like structure in which some leaves are directly linked. Messages can travel across the tree, when a suitable route is available. Some systems with mesh topology have built-in intelligence called route discovery that ensures messages reception at their destinations and if a default route to destination node is down, the network can discover an alternative route to deliver the message.

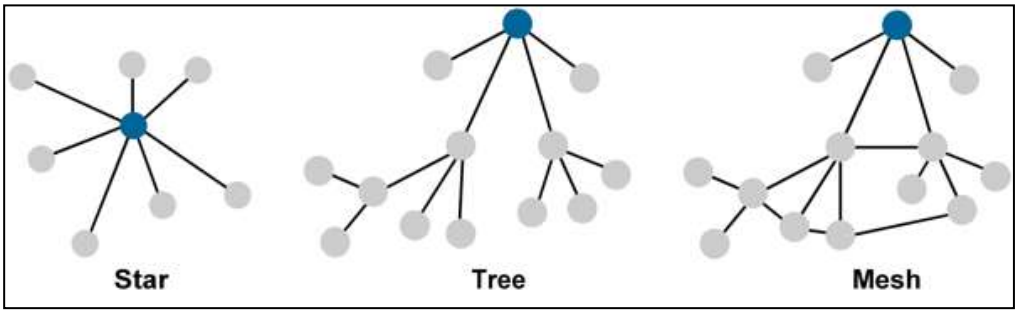


Figure 2.2: Wireless network topologies types

Medium Accessing and Operating Frequency: (9.a) *Medium access* aspect can be defined as the methodology by which channel is shared among the devices. Since number of devices in an industrial set-up is quite large, selection of a medium accessing technique is a key factor. In Fieldbus, few multi-access technologies are used by different manufacturer like; Time Division Multiple Access (TDMA), CSMA, and Token-Passing. Another aspect in the band selection is to strike a balance between minimizing the cost (by using unlicensed band and avoiding the cost of purchasing license rights from the local regulation body) and reducing the

interference from other users. In order to ensure communications reaching their destinations uncorrupted and following techniques might be used:

a. *Channel Selection:* When a network is initialized, channels of the chosen Radio Frequency (RF) band are assessed for activity.
b. *Listen Before Sending*: To avoid conflicting transmissions (more than one device transmitting in the same frequency channel at the same time), before beginning a transmission, a node listens on the relevant channel to check whether it is clear.
c. *Data Coding*: even if there are conflicting transmissions, there is a higher probability that a message will get through to its destination intact.
d. *Acknowledgements:* To confirm that messages reached their destinations. If the sending device does not receive an acknowledgement within a certain time interval, it resends the original message again.

(9.b) *Operating frequency* put another feature where some bands are busier than others and also more susceptible to noise. The choice of frequency band is an important factor in system design. The frequency selection affects the data transmission speeds, the likelihood of interference with other devices, the complexity of radio transceivers.

9. *Complexity*: Profile design is considered to reach optimal targets through most possible simplified way. This reduces time delay for profile processing time and required packet overhead tags [13]. Fieldbus has a very simplified profile. This simplification is done in favor of commissioning team as well as end-user. The technology should be relatively simple to implement and support.

10. *Scalability*: Scalability determines how system can grow once required. For example network load should not be used at the limit and provision is made for future expansion. Industrial keep changing in size and the number of network nodes. The wireless network must be capable of accommodating these changes without significant increase in the cost to the enterprise.

11. *Flexibility*: Flexibility ensures interoperability between devices regardless of their developers or manufacturers. The system profile: suggests user-interface formats, defines dependencies on other profiles for external systems, identifies protocol stack configurations, and describes device-to-device behavior. Flexible profile ensures that a device may communicate with the third party devices. It should be able to handle different types of node devices without needing a lot of device-specific requirements.

After these twelve characteristics are identified, a **proper weight** is assigned for each Key Performance Indicator (KPI) depending on the application field in which wireless technology to be used. In Table 2.3, all twelve KPI's are listed with their proper weights for wireless sensor network application at steel rolling mill. Higher the weight indicates more importance to the KPI.

The selection of appropriate weights for each KPI depends mainly on its classification. The three categories of KPI: system existence category, link availability category, and additional competency category. The KPI is classified under system existence category, if absence of the indicator affects directly system existence and the indicator shall hold high weight. For link availability category, if

absence of the indicator affects directly link availability and the indicator shall hold average weight. Finally, if absence of the indicator affects only additional competency of communication system then the indicator shall be classified under additional competency category and shall hold low weight.

Table 2.3: Sensible weights for performance indicators in Steel Mills

Item No.	Characteristics	Wight out of 10
1	Data Rate	10
2	Device Range	10
3	Number of Devices	9
4	Reliability, Availability and Resilience	8
5	Network Latency and Throughput	8
6	Security	8
7	Power Consumption	6
8	Network Topology	6
9	Medium Accessing and Operating Frequency	6
10	Complexity	4
11	Scalability	3
12	Flexibility	2

Few wireless technologies are available that can be used in the industrial networking. They might replace the wired network or work together to improve performance and implementation. In the following section some selected technologies are assessed on the biases of defined 12 KPI's. This scientific methodology is applicable for any other wireless technologies for future work.

3

EVALUATION OF WIRELESS TECHNOLOGIES IN INDUSTRIAL ENVIRONMENT

The *Institute of Electrical and Electronics Engineers* (IEEE) established in 1884 is the widely known and influential organization for computer networking and wireless communications. In the early 1980s, IEEE began work on development computer network architecture standards. IEEE802 standard defines a family of IEEE standards dealing with local area networks and metropolitan area networks. This 802 project quickly expanded to several different categories of network technologies. The specified standards protocols define the lower two layers of the seven-layer Open System Interconnection (OSI) networking reference model: Physical Layer (PHL) and Data Link Layer (DLL). In fact, IEEE802 splits the DDL into two sub-layers named Logical Link Control (LLC) and MAC. The study on IEEE802 is divided among many working groups each responsible for a specific scientific branch. Each working group consists of one or more task groups and that deals with a certain aspect of technology. In this study, widely-used technologies that fall under either

IEEE802.15 Wireless Personal Area Networks (WPAN) or IEEE802.11 Wireless Local Area Network (WLAN) are presented. For WPAN, both IEEE802.15.1 and IEEE802.15.4 are conferred. IEEE802.11 family (a, b, g) are studied for WLAN. SP100 as a potential technology is discussed. Figure 3.1 shows overview of wireless landscape for few important technologies.

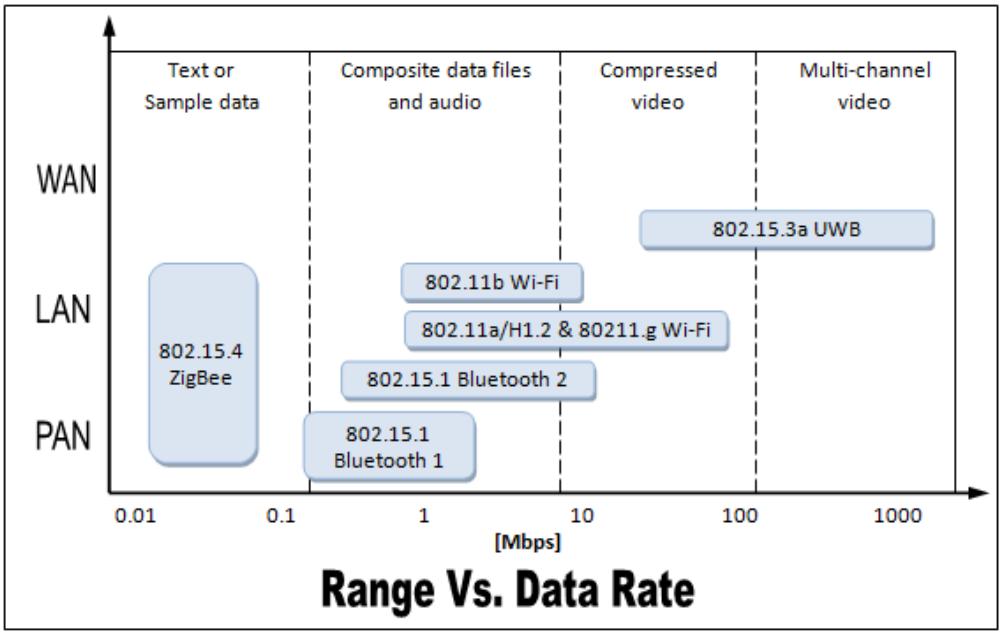


Figure 3.1: Overview of wireless landscape for few important technologies (modified from [6])

Table 3.1 shows wireless working groups in IEEE. The widely used technologies under selected standard like Bluetooth (IEEE802.15.1), ZigBee (IEEE802.15.4), and Wi-Fi (IEEE802.11) are presented in the following. For both ZigBee and Bluetooth separate alliances of companies worked to develop specifications covering the network/link, security and application profile layers so that the commercial potential of the standards could be realized. SP100 standard can also be studied as a great opportunity in the near future. In [14], author supports

using more than one technology at the same site. In [15] and [4] a hybrid wired/wireless Fieldbus system is presented. The remainder of this section presents a comparison between the four selected technologies on the basis of mentioned characteristics across industrial Fieldbus network.

Table 3.1: Wireless Working Groups in IEEE

SN	Standard	Description
1	IEEE802.11	WLAN Working Group (selected for the study)
2	IEEE802.15	WPAN Working Group (selected for the study)
3	IEEE802.16	WMAN Working Group (wimax)
4	IEEE802.18	Radio Regulatory TAG
5	IEEE802.19	Coexistence TAG
6	IEEE802.20	Mobile BWA Working Group
7	IEEE1451.5	Working Group for Wireless Sensors

In this section, WPAN standards of IEEE802.15.1 and IEEE802.15.4 are discussed and followed by WLAN standard with IEEE802.11-family. Then, upcoming SP100 standard is touched as a future opportunity and finally few wireless system common concerns are presented. Under each discussed standard, one example is given that is assessed based on industrial characteristics. The intent is to highlight the pros and cons of each standard and summary of comparison is given in next section.

3.1 IEEE802.15 WORKING GROUP (WPAN)

IEEE802.15 is the 15th working group of IEEE802 standard which is dedicated for WPAN. This working group has many sub Task Groups see Table 3.2. IEEE802.15.1 and IEEE802.15.4 are the most widely used task groups. This working group serves networks interconnecting devices located around individual persons, typically within few tens meters. A key concept of this standard is called *plugging-in*, i.e. when two devices come into close proximity, a communication channel is established. In industries field-devices network (Fieldbus) hold similar features that is short range and in sometimes mobility. Following sections discuss both IEEE802.15.1 and IEEE802.15.4 task groups with related selected technologies of Bluetooth and ZigBee respectively.

Table 3.2: IEEE802.15 Task Groups

g	Standard	Description
1	IEEE802.15.1	Task Group 1 WPAN/Bluetooth™ (selected)
2	IEEE802.15.2	Task Group 2 Coexistence
3	IEEE802.15.3	Task Group 3 WPAN High Rate
4	IEEE802.15.3a	Task Group 3a WPAN Alt. Higher Rate
5	IEEE802.15.4	Task Group 4 WPAN Low Rate (selected)

3.1.1 IEEE802.15.1 STANDARD (SHORT & MOBILE)

In 2002, IEEE802.15.1-2002 published a WPAN based on the Bluetooth v1.1 specifications. Later, an updated version of this standard, with certain additions as Bluetooth v1.2, was published as IEEE802.15.1-2005. Following the publication of IEEE802.15.1-2005, the IEEE Study Group 1b voted to discontinue their relationship with the Bluetooth Special Interest Group (SIG), effectively meaning that the later versions of Bluetooth will not become in the future IEEE standards.

3.1.1.1 BLUETOOTH[1]

Bluetooth originated when Ericsson joined IBM, Nokia, Intel, and Toshiba to form the Bluetooth SIG and standard was published in 2002 [6]. Bluetooth SIG mission statement defines Bluetooth objective targeting: *short range and mobile*. It is concentrating on *creating the preferred wireless technology for diverse-to-devices connection*. It is utilizing short-range communications technology and facilitating data transmission between fixed and mobile devices. It was originally conceived as a wireless alternative to RS232 data cables as a cable replacement. It can connect multiple devices and overcome problems arising from synchronization of these devices. On Mar-2006, the Bluetooth SIG announced its selection of the WiMedia Alliance Multi-Band Orthogonal Frequency Division Multiplexing (MB-OFDM) version of Ultra Wide Band (UWB) system for integration with Bluetooth for achieving higher data rate. On Jun-2007, Bluetooth SIG announced that Wibree will be a part of the Bluetooth specification, as an ultra-low-power Bluetooth. By Nov-2006, The Bluetooth SIG claims that 12 millions Bluetooth devices are shipped per week and are in the hands of one billion consumers [16]. Following are the Bluetooth versions:

1. *Bluetooth 1.0 and 1.0B*: They had many problems and manufacturers had difficulty making their products interoperable.

[1] For more information see http://www.bluetooth.com/Bluetooth/SIG

2. *Bluetooth 1.1*: It was ratified as IEEE Standard IEEE802.15.1-2002 and both support to non-encrypted channels and received Signal Strength Indicator were incorporated.
3. Bluetooth 1.2: It was ratified as IEEE Standard IEEE802.15.1-2005 and it added the Adaptive Frequency Hopping (AFH) spread spectrum, which improves resistance to RF interference by avoiding the use of crowded frequencies in the hopping sequence.
4. Bluetooth 2.0: It was released in Nov-2004. It enhanced data rate (3 Mb/s) using combination of Gaussian Frequency Shift Keying (GFSK) and Phase Shift Keying (PSK) modulation with two variants π/4-DQPSK (Differential Quadrature Phase Shift Keying) and 8-DPSK (Differential Phase Shift Keying).
5. Bluetooth 2.1: was adopted in July-2007 with added features of extended battery life resulting with sniff low-power mode; and stronger encryption that uses Encryption Pause Resume technology with a facility to refresh the key.

Bluetooth Technology is operated within the unlicensed band at 2.4 GHz for voice and data transfer (up to 1Mbps) using GFSK modulation. Practical experiments show that it is more suitable for voice application [17]. AFH allows Bluetooth to detect and exclude interference from others [18]. This ensures minimal frequency interference, transmission security, and a high Quality of Service (QoS) at the expensive of processing and battery power. It is made of master and slave nodes. All slave nodes can communicate only through its master node. Each slave can have up to four masters. One master coordinates communication between its slaves (up to 8 active devices at a time) which form one piconet. Different piconets are interlinked in scatternet manner. Piconet traffic is TDMA/Duplex scheme [19]. [20], [21]

Bluetooth supports three different protocols:

1. *Link Manager Protocol (LMP):* establishes the link setup between Bluetooth devices and manages ongoing links, including: security aspects (e.g. authentication and encryption), controling and negotiation of baseband packet size.
2. *Logical Link Control and Adaptation Protocol (L2CAP):* adapts the upper-layer protocols to the baseband layer, providing both connectionless and connection-oriented services.
3. *Cable Replacement Protocol:* RF communications is the cable replacement protocol used to create a virtual serial port used to make replacement of cable technologies transparent through minimal modification of existing devices. RF communication provides for binary data transport and emulates Electronic Industry Association EIA-232 (formerly RS-232) control signals over the Bluetooth baseband layer.

In industrial environment, Bluetooth can fit in machine-to-machine communication and for ad-hoc connectivity between mobile computing devices and fixed equipment [6]. The following points result from evaluation of suitability of Bluetooth technology for industrial application:

1. *Data Rate*: Bluetooth clearly has ability to support almost all industrial application with ordinary average value of 1Mbps [6]. This is achieved using GFSK modulation. It can support up to 3 Mb/s with latest version 2.0 and above. [22]

2. *Device Range*: As designed and without special equipment it is clear that Bluetooth has limited range. Distance coverage is multiple of tens of meters, e.g. Indoors of 10m and outdoors of 100m, which is very small for normal factory size [18]. The upper range limit has been possible only with proprietary mesh networking protocols [6].

3. *Number of Devices*: Bluetooth can support up to 8 active devices simultaneously in a single piconet and up to 255 further devices can be inactive, or parked, which the master device can bring into active status at any time. These 255 parked slave devices occupy the same physical channel [18]. Slave devices may only communicate with the master device and never directly with another slave; however a slave device may participate in one or more piconets (a scenario known as a scatternet). A single device may never be master of more than one piconet. Unfortunately, the Bluetooth standard does not define any networking between the piconets within a scatternet, but applications may be designed to facilitate such communication. This increases network complexity while connecting different piconets to get the large number of devices in the plant.

4. *Reliability, Availability and Resilience*: Bluetooth reliability can be rated in the medium range compared to other technologies. Three types of error correction are implemented in Bluetooth systems: 1/3 & 2/3 rate Forward Error Correction (FEC), and Automatic Repeat Request (ARQ). Within its constraints Bluetooth is resilient; it works very well for certain applications. Another consideration is that Bluetooth technology is commonly used in most hand held devices. This fact makes it more difficult for designers to protect their network from other handset

interferences. Even with proper encryption, noise floor level increases and overall signal quality decays.

5. *Network Latency and Throughput*: Bluetooth is designed for single hop device-to-device where the nodes do not sleep for much of the time and as a result network access is fast. On the other hand, it does not support the mesh topology that gives more alternative paths to be used in case one becomes dysfunctional; it increases the time to deliver data because of waiting for that particular path. Also, the time to join the network as a new node is around 10 sec and 3 sec to wake up from sleep mode which are very long. However it takes 2 ms for active slave to access the channel. [18]

6. *Security*: Bluetooth protocol has a built in security system that specifies the use of 128 bit Advanced Encryption Standard. Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher. In Bluetooth, key generation is generally based on a Bluetooth PIN, which must be entered into both devices. It embodies fast Frequency Hopping Spread Spectrum (FHSS) over 79 1MHz widely pseudo-randomly ordered channels. The frequency hopping rate of 1600 hops/sec is used with Time Division Duplex (TDD). Transmissions performed in 625 microsecond slots with a single packet transmitted over a single slot. For long data transmission users may occupy multiple slots using the same transmission frequency thus reducing the hopping rate. In August 2004, range of Class 2 Bluetooth was extended with directional antennas to 1.08 mile (1.78km) [23]. This poses a potential security threat since attackers can hack from a distance beyond expectation. In [24], the

author shows both passive and active methods for obtaining the PIN for a Bluetooth link by which hacker can easily spy the devices. In passive method, PIN can be found during the Bluetooth pairing process. On the other hand, active method is done in Re-Pairing process that requires injecting a specific message at a precise point in the protocol.

7. *Power Consumption*: Bluetooth keeps all nodes on active mode always which increases the power consumption [25]. It does not have the sleep mode which conserves the battery life. However, there are few studies to improve Bluetooth power consumption. Many of those studies are based on over–simplified power models and do not consider number and role (master vs. slave) of links [26], [27]. AFH in Bluetooth ensures minimal frequency interference, transmission security, and a high QoS at the expensive of processing and battery power. In [28] a full power model of Bluetooth is presented in a complex scatternet scenario where each link can be inactive or low–power sniff mode. The model Root Mean Square (RMS) error is validated to be below 4%. A standard Bluetooth device usually can keep batteries for some days only.

8. *Network Topology*: Bluetooth supports only the star ad-hoc piconets network. It allows connecting two or more piconets together to form a scatternet, with some devices acting as a bridge by playing simultaneously the master role in one piconet and the slave role in another. Although it does not support the mesh networking which is preferable for industrial network as it provides better diversity. However, the role of scatternets is still relatively limited. Problems specific to scatternets are discussed in [19].

9. *Medium Accessing and Operating Frequency*: Bluetooth operates on the unlicensed 2.45 GHz using FHSS signal of 79 channels each 1MHz node ordered pseudo-random channels. AFH allows Bluetooth to detect and exclude frequencies in use by other devices and select channels to minimize interference. A piconet master communicates with each active slave during each multiplexed time slot in a round-robin-like fashion. [18]

10. *Complexity*: Bluetooth embodies device profiles for equipment interoperability. Bluetooth complexity is limited by the small number of devices allowed in each network. In addition, Bluetooth protocol stack is relatively complex.

11. *Scalability*: Bluetooth network has very low ability to extend. It is quite difficult to include new nodes in the existing network.

12. *Flexibility*: Devices can switch roles, i.e. the slave can become the master at any time. The master switches rapidly from one device to another in a round-robin fashion. Simultaneous transmission from the master to multiple devices is also possible. In general Bluetooth protocol has the flexibility feature whereas its profile carries some inflexibility.

3.1.2 IEEE802.15.4 STANDARD (LOW RATE WPAN)

IEEE802.15.4 is Low Rate Wireless Personal Area Network. This IEEE task group optimizes low duty cycle to get longer battery life (ranging from months to years) at the cost of low data rate but very low complexity. In May 2003, the first edition of IEEE802.15.4-2003 was released. Following are the sub-technologies:

1. *IEEE802.15.4a* (WPAN low rate alternative PHY): It is adding scalability to data rates, longer range, with lower power consumption and cost.
2. *IEEE802.15.4b* (revisions and enhancements): It is chartered to enhance the standard by resolving ambiguities, reducing complexity, increasing flexibility with security key usage.

In Jul-2008, an enhancement to IEEE802.15.4-2006 standard was published for hybrid contention access and scheduled access. It provides better support to the industrial markets improving MAC Layer reliability. Another advantage is to realize a balance between fast communication for emergency information and the very low duty cycle communication for regular information [29]. IEEE802.15.4 works in unlicensed RF bands: 868 MHz, 915MHz, or 2.4 GHz with total of 27 channels, see Table 3.3[6]. Nearly 20 Million IEEE802.15.4 units were shipped up to end of 2008.

Table 3.3: IEEE802.15.4 RF Bands [6]

Freq. Band	Area	Data Rate	Channel Numbers
868.3 MHz	Europe	20kbps	0(*)
902-928 MHz	Americas	40kbos	1-10
2.405-2.480 GHz	Worldwide	250kbps	11-26

(*) In Europe only one channel is assigned in 868.3 MHz band

All network protocols that are built for IEEE802.15.4 use a basic packet format with simple address-header. When data is communicated over multi hops, time or frequencies, the network header specifies where it starts, where it ends, and how to get from one node to another. Unfortunately, many current industrial protocols perform this operation differently and none of them address how packets are transferred between existing controllers or devices and IEEE802.15.4 network. Many wireless technologies are built on IEEE802.15.4 standard like ZigBee, SP100.11a, and Wireless HART. In the following section ZigBee is assessed in the light of industrial characteristics.

3.1.2.1 ZIGBEE [1] [2] [3]

The ZigBee set of high level communication protocols is based upon the specification produced by the IEEE802.15.4 task group. It started when Motorola worked on low power mesh networking. Phillips, Motorola, Invensys, Honeywell, and Mitsubishi joined together and formed the ZigBee Alliance in mid-2002. There is a focus on *remote sensing and control*, reflecting the original ZigBee mission statement. It is intent for interfacing thousands of small, cheep, and ultra-low power devices in a flexible network topology. These advantages save in industrial environment significant cost by increasing plant productivity. Today, ZigBee Alliance consists of Nearly 30 members. Some of those members are ZigBee Alliance **Promoters** including: Motorola, Ember, Samsung, Schneider, Philips, Eaton, Honeywell, Huawei, ST-Microelectronics, Freescale-Semiconductor, Texas-Instruments, Mitsubishi, and Siemens. As of Jul-2006, ZigBee reports that Alliance members have shipped over 10,000 Developer Kits and processed 29,000+ free downloads of the ZigBee specification [30]. This shows observable growth for ZigBee market.

IEEE802.15.4 has simple frame structure that ensures reliable data delivery using Carrier Sense Multiple Access Collision Avoidance (CSMA-CA) with message acknowledgement. It conserves power at the expense of QoS. There are three types of devices: Coordinator, Router, and End devices. ZigBee has few additional coexistence features which decrease ISI or/and increase QoS like: network formation

[1] http://www.zigbee.org
[2] http://zigbee.iii.org.tw
[3] http://www.jennic.com/elearning/zigbee/files/content_frame.htm

procedures, mesh networking and path diversity, network-layer frequency agility, and end-to-end acknowledgement and retransmission. Protocol Stack for ZigBee is shown in Figure 3.2.

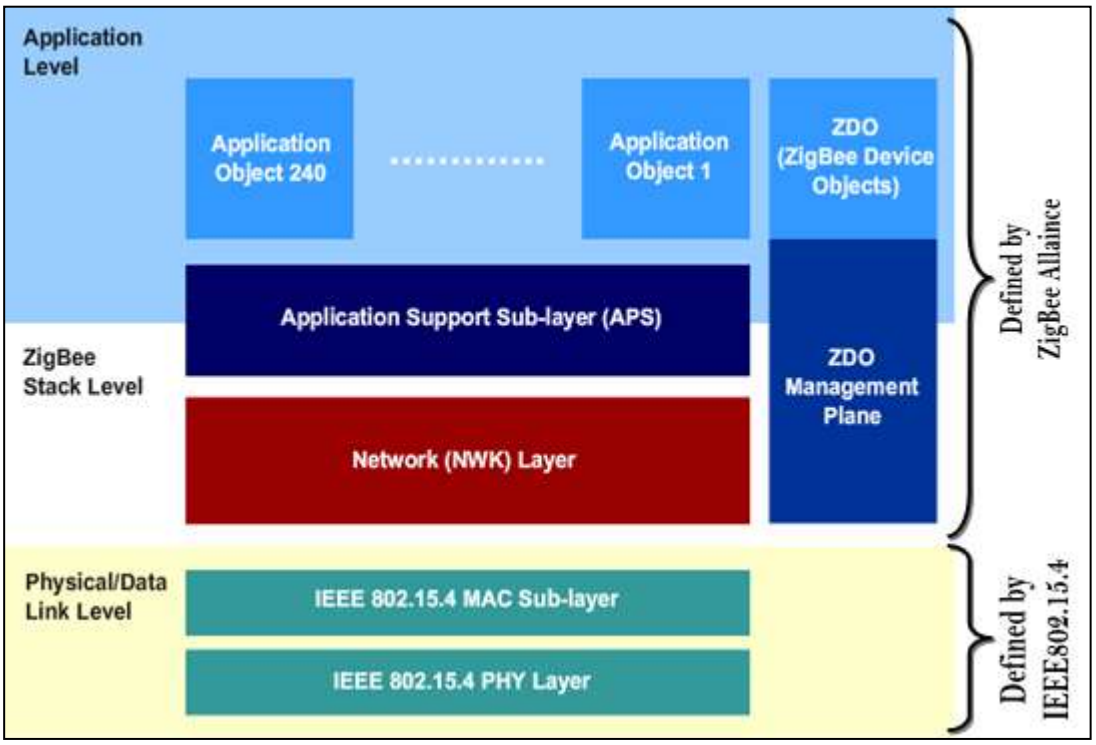


Figure 3.2: ZigBee protocol stack configuration (modified from [30])

In industrial environment, ZigBee has the ability to make inroads into existing industries replacing wired-systems through 'off-the-shelf' product elements of mesh networking and can be linked to wide range of existing sensor and actuators. ZigBee can fit in low rate field devices communication and their mesh topology increases their network range coverage. The following points result from evaluation of ZigBee technology in industrial application:

1. *Data Rate*: This is one of the most challenging properties for low rate WPAN task group, IEEE802.15.4, technologies which reduce duty cycle time in favor of

extending battery life-time. ZigBee technology has low data rate in range of few hundreds of kbps, see Table 3.3. [6]

2. *Device Range*: ZigBee has the potential to operate over a large range because of its mesh networking topology. Practical experiment show that it can cover up to 10-100m for Indoors application and 400m for outdoors [31].

3. *Number of Devices:* ZigBee can support very high number of devices in the network which is normally required in industrial wireless networking. It can handle 65,000 nodes in the same network. [4]

4. *Reliability, Availability and Resilience:* ZigBee has many features that increase network reliability like: data packet acknowledgement, CSMA-CA approach, encryption, mesh multi-path transmission redundancy, and ability to physically work around the built environment due to the hybrid network configuration options. Multipath feature enhances system diversity and reliability by routing around obstacles, detecting losses, and retransmitting packets. ZigBee reduces packet collisions using CSMA-CA offering random delay between packet transmissions. ZigBee resilience can be rated on very high range. [18]

5. *Network Latency and Throughput:* ZigBee has a great ability to conserve power with sleep mode that has limited effect on network latency. Although it could achieve acceptable delay because of very short wake up period (15 ms), the multi-hop nature of mesh networks also increases latency. For new slave enumeration, it takes 30 ms and active node takes 15 ms to access the channel. [4], [18]

6. *Security:* ZigBee uses Direct-Sequence Spread Spectrum (DSSS) technique with Orthogonal Quadrature Phase Shift Keying (O-QPSK) Modulation (in 2.4GHz band only). DSSS coding scheme increase system robustness in harsh environment around heavy machinery. It employs the 128 bit Advanced Encryption Standard (AES-128) that assures basic security tool for the standard [18]. Beyond encryption each ZigBee node receives a unique short address from the network coordinator and each ZigBee network has a unique ID and networks can be open or locked to new devices [6]. Standard co-existence feature is satisfied using following techniques: complementary channel mapping, built-in scanning and reporting, DSSS, FDMA, and CSMA. Another security tool is available in ZigBee called Message Freshness Timers (MFT) at which timed-out messages are rejected, preventing message replay attacks on the network. An example of a replay attack would be a malicious individual recording the open command for a garage door opener, and then replaying it to gain entry.

7. *Power Consumption:* ZigBee has been developed specifically to permit low power consumption and years of battery life. It optimizes slave power requirements by forcing to sleep mode most of the time. It operates on a very low duty cycle of <1% [18]. In addition, time of wake up is minimized to reduce communication latency as well as to increase battery life. ZigBee power profile is an application dependant that on average can sustain for years. [6]

8. *Network Topology:* ZigBee Supports both ad-hoc star and mesh network topology. Also it can combine more than one type in the same network as hybrid system [18]. ZigBee defines three device types: ZigBee Coordinator (ZC), ZigBee

Router (ZR), and ZigBee End Device (ZED). A network must contain at least one coordinating device as the coordinator initiates the networking formation and participates in the routing of messages. The router device actively routes messages between devices. The end device does not route messages to other devices. [32]

9. *Medium Accessing and Operating Frequency:* Many current wireless hardware technologies use CC2420 radio which provides multiple channels [33]. It uses DSSS to reduce interfaces at those unlicensed bands. Given the limited radio available bandwidth of 250Kbps, designing MAC protocols which can exploit the available frequencies to improve parallel transmission and increase the network throughput seems to be an imperative task. Reference [34] shows strengths of combining both TDMA and FDMA schemes in MAC layer (HyMAC). This provides high throughput with small delay, i.e. real-time communication. For operation, ZigBee supports most the widely used unlicensed ISM bands in Europe, North America, and around the world. It works on IEEE802.15.4 bands: 868 MHz, 915MHz, or 2.4 GHz with total of 27 channels, see Table 3.3. Although the 2.4 GHz band is becoming a global standard, many companies support other bands, e.g. 915MHz, for industry networking [6]. In 868- and 915-MHz frequency bands, there are fewer users which reduce interference, absorption and reflection. Whereas in 2400-MHz band, it is far more widely used, available with higher data rate and has more channels that reduce power consumption, shorter transmission time because higher data rate.

10. *Complexity:* ZigBee uses short packets that include the header with source and destination address fields. ZigBee is intended to be an open global standard where a ZigBee compliant device from any manufacturer could be interoperated with any other. IEEE802.15.4-based technology is a mesh networking technology that makes it easier to implement and support networks of several hundred nodes. [6]

11. *Scalability:* ZigBee has a significant advantage in terms of allowing network growth to quite large scale and having ability to use the flexible topologies to accommodate real-world situations. [4]

12. *Flexibility:* IEEE802.15.4 has some difficulties in implementation in industries of defining IP-based communication over this wireless standard. IP provides a set of widely used, long-standing, open standards that manage diverse and evolving suites of devices and networks with well-established mechanisms for protecting critical network resources. With the advent of 6LoWPAN, these protocols have been scale down sufficiently to be useful in wireless embedded networks. The 6LoWPAN breakthrough is to leverage the shared context typical of use cases for this technology to obtain a very compact and efficient IP implementation, removing the factors that have given rise to a plethora of ad-hoc standards and proprietary protocols. In general, ZigBee has high flexible approach for industrial applications except where there is a need for higher data rates. [31]

3.2 IEEE802.11 WORKING GROUP (WLAN)

IEEE802.11 is the 11th working group of IEEE802 standard that looks after standardization of WLAN. One of the most well-known standards is IEEE802.3, which sets specifications for Ethernet LAN technology. It links two or more computers or devices using spread-spectrum or Orthogonal Frequency Division Multiplexing (OFDM) modulation technology in a local area. This working group has developed many IEEE Standards but the most popular amendments are displayed on Table 3.4 [35].

Table 3.4: Most Popular Amendments of IEEE802.11 Standards

SN	Standard	Data Rate	Band	Released	Comments
1	IEEE802.11a	54 Mbps	5.0 GHz	Oct-1999	Wi-Fi Certified
2	IEEE802.11b	11 Mbps	2.4 GHz	Oct-1999	Wi-Fi Certified
3	IEEE802.11d	International roaming extensions - specification for operation in additional regulatory domains (2001)			
4	IEEE802.11g	54 Mbps	2.4 GHz	Jun-2003	Compatible with b, Wi-Fi Certified
5	IEEE802.11h	Dynamic Freq. selection	5.0 GHz	2004	European – to solve satellites/radar interference
6	IEEE802.11i	Addresses Encryption & Authentication		Jun-2004	Security solution WPA2: PSK & AES-CCMP
7	IEEE802.11n	200 Mbps	5.0/2.4 GHz	Jan-2010 (Est.)	MIMO System, Wi-Fi Certified

Following section discusses IEEE802.11 family standard with Wi-Fi technology. In 1990, the IEEE formed a committee to develop a standard for WLANs that operates at a speed of 1 and 2 million bits per second (Mbps). Several different protocols were recommended before a draft was developed, and this draft

went through seven different revisions that took almost seven years to complete. In 1997, the IEEE approved the IEEE802.11 WLAN standards.

In 1999, a new IEEE802.11b amendment was created raising speed to 5.5 & 11Mbps covering range of 115 meter at 2.4GHz. At the same time IEEE also issued another standard named IEEE802.11a with even higher speed of 54 Mbps but working at 5 GHz. The IEEE 802.11g standard, formally ratified in 2003, can support devices transmitting at 54 Mbps. Since 2004, the IEEE has been working on new standard, called IEEE802.11n, to significantly increase the bandwidth with MIMO technology.

3.2.1 IEEE802.11 FAMILY OF STANDARDS (HIGH DATA RATE)

IEEE802.11 family of standards is designed to provide users with high data rates (tens of Mbps) over ranges of tens to hundreds of meters, WLAN standard, that basically supports Ethernet access [7]. This family employs different over-the-air modulation techniques that use the same basic protocol. The original version of the standard was released in 1997 and certified in 1999. IEEE802.11b is the first wireless networking amendment widely accepted followed by IEEE802.11g and IEEE802.11n.

The IEEE802.11 working group divides allocated frequency bands into channels. For example the 2.4000–2.4835 GHz band is divided into 13 overlaying channels each of width 22 MHz but spaced only 5 MHz apart, with channel 1 centered on 2.412 GHz and 13 on 2.472 GHz. Japan adds a 14th channel 12 MHz at 2.484 GHz, see Figure 3.3.

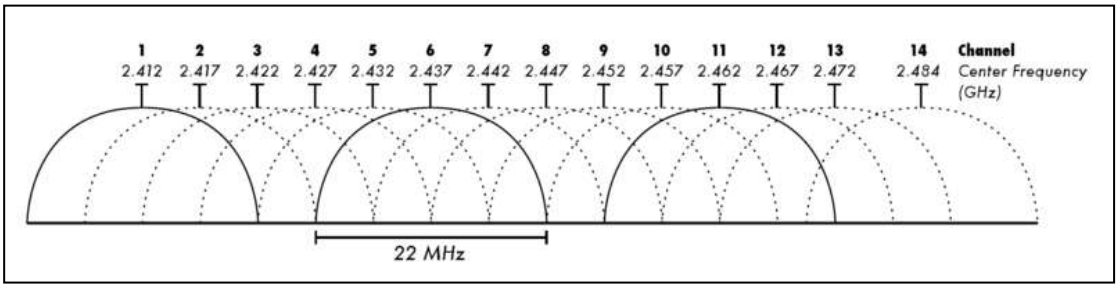


Figure 3.3: IEEE802.11 channels at 2.4000–2.4835 GHz band

The most popular are those defined by the IEEE802.11b and IEEE802.11g protocols, the amendments to the original standard. Security provision was originally weak due to export requirements of some governments [36], and was later enhanced via the IEEE802.11i amendment after legislative changes done by governments. Other standards in the family (c–f, h, j) pertain to service amendments and extensions or corrections to previous specifications.

3.2.1.1 WI-FI[1]

In 1999, several industry leaders came together to form a global, non-profit organization to adopt a single worldwide-accepted high-speed wireless LAN standard. This organization was named as the Wi-Fi Alliance. Wi-Fi is a trademark of certified products based on the IEEE802.11 standards that guarantees interoperability between different wireless devices. Unlicensed spread spectrum was first made available in the US by the Federal Communications Commission (FCC) in 1985 and these FCC regulations were later adopted with some amendments in many other countries enabling use of this technology in all major countries [6]. The FCC action was part of a broader proposal to allow civil use of spread spectrum technology and was opposed at the time by main stream equipment manufacturers and many radio system operators. [19]

The first wireless product was brought on the market under the name WaveLAN with speeds of 1 Mbps to 2 Mbps. In fact Australian Commonwealth Scientific and Research Organization (CSIRO), which is the national government body for scientific research in Australia, has consistently maintained that it owns the rights to a key part of IEEE802.11 Patent. In 2009 the CSIRO reached a settlement with 14 companies, including Hewlett-Packard, Intel, Dell, Toshiba, ASUS, Microsoft and Nintendo, on the condition that the CSIRO did not broadcast the resolution.

Today, more than 300 members and growing from more than 20 countries, still bind them together for common goals. As Wi-Fi networks continue to expand in

[1] http://www.wi-fi.org

businesses, homes, and now public hotspots that provide wireless access locations for people on the go, compatibility between devices is critical. The Wi-Fi Alliance develops rigorous tests and conducts Wi-Fi certification of wireless devices that implement the universal IEEE802.11 specifications. The Wi-Fi Alliance has completed more than 5,000 product certifications to date.

In industrial environment, Wi-Fi technology can fit in master network communication for monitoring, open loop control or slow-speed closed loop control. The following points result from evaluation of Wi-Fi technology in industrial application:

1. *Data Rate:* Wi-Fi is rated for high data rate technologies for all its families (amendments) especially for IEEE802.11n. Data rate depends on the modulation scheme used. BPSK modulation with ½-FEC gives a 6 Mbps data rate, whereas 64-QAM (Quadrature Amplitude Modulation) with ¾-FEC gives 54 Mbps. The maximum throughput rate per user is a function of packet size. The theoretical maximum throughput value depends on the packet size. For example, for highest modulation rate of 54 Mbps, throughput of 1500 bytes packets long is 30 Mbps. While packets of just 60 bytes long result in a throughput of 2.7 Mbps. IEEE802.11n can support data rate more than 200 Mbps, while using MIMO technology (see Table 3.4). [37]

2. *Device Range:* Since Wi-Fi is a WLAN technology, it provides higher device ranges than PAN technologies. A typical Wi-Fi router using IEEE802.11b or IEEE802.11g with a stock antenna may result in a range of 32 m indoors and 95 m outdoors. Moreover, the new IEEE802.11n can exceed that range by more

than double. Range or coverage also varies with frequency band where the 2.4 GHz frequency block has slightly better range than the 5 GHz bands.

3. *Number of Devices:* 253 is the maximum-number of clients accepted per single Access Point (AP). However, only 15-20 clients are recommended to be used per each AP.

4. *Reliability, Availability and Resilience:* Wi-Fi uses both single carrier DSSS radio technology and multi-carrier OFDM radio technology [7]. For example, IEEE802.11a physical layer (PHY) is based on the multicarrier system OFDM [38]. OFDM modulation scheme used in the Wi-Fi plays a major role in increasing system QoS. In OFDM, the sub-carrier frequencies are chosen so that the sub-carriers are orthogonal to each other. Hence, cross-talks between the sub-channels are avoided and inter-carrier guard bands are not necessary. This greatly simplifies the design of both the transmitter and the receiver; unlike conventional FDM. While OFDM usually does not require equalizers; it is robust against narrow-band co-channel interference, Inter-symbol interference (ISI), and fading caused by multipath propagation. OFDM has high spectral efficiency, efficient implementation using FFT and exhibit low sensitivity to time synchronization errors.

5. *Network Latency and Throughput:* IEEE802.11n has improved MAC layer efficiency through reducing the protocol overhead of headers and inter-frame gaps. Because of frame overhead, the shorter the frames, the lower the efficiency or throughput. For example, voice traffic composed of short frames is inefficient.

Combining multiple frames into one longer frame increases throughput. On other words, IEEE802.11n maximizes the MAC layer transport efficiency through the frame aggregation (i.e. combination) protocol. Because of the existence of metallic obstacles and the comparably large transmit power of 20 dBm, the delay spread of a factory floor must be examined if intention is to use IEEE802.11. While the delay spread in homes and offices is known to be less than 50 ns and 100 ns respectively, it may take values of 200-300 ns in a factory floor setting. On other hand, Bluetooth may be able to tolerate higher delay spread because of lower transmit power and data rate. This introduces a restriction on the maximum data rate since the design of a conventional RAKE receiver considers the delay spread. In the case of IEEE802.11b, RAKE receiver supports 60 ns delay spread in 11 Mbps mode and 200 ns in 5.5 Mbps mode. Yet, more receiver algorithms with suitable robustness have recently come into existence. In the case of IEEE802.11a or g, the situation is better, because of the guard interval between channel symbols inherent in the OFDM technology, delay spreads of several hundred nanoseconds can be supported easily without paying attention to the receiver algorithm implementations. [39], [40], [41]

6. *Security:* The most common wireless encryption standard, Wired Equivalent Privacy (WEP), has been shown to be easily breakable even with a correct configuration. Wi-Fi Protected Access (WPA) and WPA2 are used. WPA2 is a new form of AES offering a high level of security with pre-authentication. Both WPA and WPA2 began shipping in 2003, aiming to resolve security concerns and it is now available on most products. Wi-Fi Access Points typically default to an open "encryption-free" mode. Some users benefit from a zero-configuration

device that works out of the box, but this default is without any wireless security enabled, providing open wireless access to their LAN. Wi-Fi networks that are open (unencrypted) can be monitored and used to read and copy data (including personal information) transmitted over the network, unless another security method such as a VPN or a secure web page is used to secure the data. IEEE802.11i with WPA2 addresses two security issues: Encryption & Authentication.

1. Pre-Shared Keys (PSK) Authentication: PSK Authentication is intended for personal and small office or home users without advanced server capabilities. PSK Authentication keys are automatically changed (called rekeying) and authentication between devices after a specified period of time known as rekeying interval.
2. Advanced Encryption Standard for Counter Mode CBC-MAC Protocol (AES-CCMP): Encryption under the WPA2 personal security model is accomplished by AES-CCMP. CBC-MAC is the Cipher Block Chining Message Authentication Code of the AES encryption algorithm. CCM is the algorithm providing data privacy, while the CBC-MAC component of CCMP provides data integrity and authentication.

7. *Power Consumption:* Due to high requirements for WLAN applications, power consumption is fairly high compared to WPAN standards. Technologies such as Bluetooth provide a much shorter propagation range and so in general have lower power consumption. Other low-power technologies such as ZigBee have

fairly long range, but much lower data rate. The high power consumption of Wi-Fi makes battery life a concern for mobile devices.

8. *Network Topology:* In *ad-hoc network mode*, Wi-Fi has Peer-to-peer setup where clients or mobile stations connect to each other directly. Generally, this ad-hoc mode is not used for business networks. *Infrastructure network mode* has an AP, which becomes the hub of a "star topology" though which all communication flow through. If a Mobile Station (MS) wants to communicate with another MS, it needs to send the information to AP first, then AP sends it to the destination MS. Multiple APs can be connected together and handle a large number of clients. Only one user is allowed to communicate with a receiver at a time and is not allowed to use another frequency channel to connect to a second or third user which is done through CSMA-CA random access method. There are two ways to deal with access collision:

    a. Two-way handshake: Node with packet to send monitors channel. If channel remains idle for a specified time interval called DIFS (DCF Inter Frame Space), then the node transmits and if channel is found busy, then node continues to monitor until channel becomes idle for DIFS. At this point, terminal backs-off for random time (repeated collision avoidance) and attempts transmission after waiting a random amount of time. First way is for the transmitter to send the packet and the second way is for destination to send the acknowledgement.

b. Four-way handshake: Sender listens to activities on the channel before talk and if medium is busy; node backs-off for a random length of time. Then transmitter sends a short message called Ready to Send (RTS) to inform others that it has a manage to send. RTS contains destination address and duration of message telling everyone else to back-off for the next available packet (slot) duration. If RTS reaches the destination it sends a Clear to Send (CTS) message. Then transmitter sends the information packet to its destination. In this system, the transmitter is capable to detect collisions. A collision is indicated if the information packet is not acknowledged, then the source tries again to retransmit same packet.

9. *Medium Accessing and Operating Frequency:* IEEE802.11b/g works in unlicensed 2.4 GHz band. Wi-Fi uses DSSS and FHSS. IEEE802.11b Channels for both DSSS and FHSS WLAN Standards for different countries is shown in Table 3.5. In [42], the experiments and measurements were evaluated to qualify interference effect of Bluetooth device on the throughput performance of the IEEE802.llg and IEEE802.1lb. The results show the degree to which IEEE802.llg is immune to interferences than IEEE802.11b when the signal strength of the WLAN is strong.

Table 3.5: Most Popular Amendments of IEEE802.11 Standard [42]

Country	Frequency Range Available	DSSS Channels Available	FHSS Channels Available
US	2.4 to 2.4835 GHz	1 Through 11	2 Through 80
Canada	2.4 to 2.4835 GHz	1 Through 11	2 Through 80
Japan	2.4 to 2.497 GHz	1 Through 14	2 Through 95
France	2.4465 to 2.4835 GHz	10 Through 13	48 Through 82
Spain	2.445 to 2.4835 GHz	10 Through 11	47 Through 73
Remainder of Europe	2.4 to 2.4835 GHz	1 Through 13	2 Through 80

10. *Complexity:* Wi-Fi Technology has many features like high speed and wide coverage. This introduces additional functions to coordinate the network making the technology more complicated than that of Bluetooth or ZigBee [43].

11. *Scalability:* Wi-Fi nodes are limited and it is preferable not to use many nodes in each network. There are many restrictions on network scalability.

12. *Flexibility:* It has much lower flexibility compared to other technologies.

Wi-Fi technology suits more the Industrial Master Network, where communicate between controllers and/or Humane Machine Interface (HMI) in desirable for monitoring or open loop control, than for Wireless Sensor Networks.

3.3 SP100 TECHNOLOGY

SP100 defines a wireless system that uses wireless technology in industrial environment. The International Society for Automation (ISA) is an international nonprofit association of more than 30 thousands automation professionals. ISA proposed SP100 after considering issues in design, development, production, control, measurement, systems, and devices in industrial processes and manufacturing operations. SP100.11a is the first amendment of SP100 family of standards for multiple industrial applications.

Devices are classified function-wise into 4 types: *Field Device Function*, *Routing Function*, *Gateway Function*, and *Handheld Function*. A brief description of these functions is following:

1. *Field Device Function*: (sensing/data with limited range) Its function is for sensing/data and actuation via I/O connectivity User Application Processes (UAP). Nodes are typically optimized for low energy wireless operation. Nodes can optionally be powered by normal electronic supplies for increased performance and where domination of wired communication is beneficial. The nodes can be stationary or mobile with a limited range of operation.

2. *Routing Function*: (forward traffic) Its function is to forward network traffic on behalf of neighboring nodes by utilizing network layer protocols. Routers move infrequently if at all.

3. *Gateway Function*: (connectivity to anther network) Its function is to provide connectivity between one or more field devices on the wireless network and one or more industrial automation applications via a protocol translation UAP. There can be a number of interposing routing nodes between the gateway and the field device nodes.

4. *Handheld Function*: (interact with display system) Its function is to enable wireless workers to interact with the wireless network via a display oriented UAP. Nodes are nomadic: moving to a location, establishing a local connection to the network, communicating with one or more network nodes, and when finished disconnecting from the network.

There is no minimal or the maximal configurations limits. The architecture supports 3 types of mobility: fixed position, relative motion with fixed reference frames, and relative motion with low speed reference. The architecture supports all power levels as mains, limited battery and moderate power. There is rechargeable battery as well as scavenging power. It also supports the following time related functions: *Sleep timers*, *Network time synchronization*, *Network time*, *Secure network time synchronization*, *Application services to utilize network time*, *Application services to convert network time*, *and Application sampling time*. From security point of view there are: transport confidentiality, per message integrity, and digital-signature service.

A SP100.11a network is comprised of nodes that host the network and device functions. It is possible to construct a system using range of topologies from the nodes and functions. A star topology connects field devices directly to gateways whereas a mesh topology connects field devices to gateways through intermediate

routers. This architecture supports both the mesh and star topologies. This covers a broad range of application scenarios. It can be accomplish by configuration options, because a star topology may be considered to be a subset of a mesh topology.

The architecture supports two time related functions; (1) *Sleep timers function* which saves energy consumption via periodic wakeup, and (2) *Network time synchronization* which minimizes messaging wait time. Network time includes periodic transport, timeslot calculation, and message delivery expiration. Secure network time synchronization used for security algorithms. Application services utilize network time creating high resolution timestamps for sequence of event determination. Application services normally are used to convert network time that includes wall clock time for low resolution event logging. There is a provision for Rechargeable battery as well as scavenging power, see Table 3.6.

Table 3.6: Typical Power Source Characteristics

Function Type	Power Source
Field Node	Limited, Moderate or Mains
Routing Device	Limited, Moderate or Mains
Combined Routing Device / Field Node	Limited, Moderate or Mains
Gateway Device	Moderate or Mains
Handheld Device	Rechargeable
Network Manager host	Moderate or Mains
Security Manager host	Moderate or Mains

SP100.11a supports the following three optional security assurances. Transport confidentiality: per-message integrity combined with per message source authentication, and an application-level digital-signature service. Secured operation supports three security methods: (1) secured subnet communication assurances based on DLL enforcement, (2) secured application communication assurances on a per application basis based on transport layer, and (3) a combination of secured subnet and secured application communications.

3.4 SUMMARY OF COMPARISON

Three widely-used technologies are studied: two of WPAN standard which are Bluetooth and ZigBee, and one of WLAN standard which is Wi-Fi. This section summarizes the comparison between the three technologies based on usage in industrial networking. All twelve KPI's comparisons across the three technologies are summarized in Table 3.7.

Table 3.7: Summary of comparison between selected technologies

Item No.	Characteristics	Bluetooth	ZigBee	Wi-Fi
1	Data Rate	3 Mbps	250 Kbps	200 Mbps
2	Device Range	10m Indoor 100m Outdoor	100m Indoor 400m Outdoor	32m Indoor 95m Outdoor
3	Number of Devices	8/piconet	56,000	15-20
4	Reliability, Availability and Resilience	Medium 2/3-FEC	High CSMA-CA	Very High 3/4-FEC
5	Network Latency and Throughput	Access 3 s Sleep 2 ms	Access 15 ms Sleep 15 ms	No sleep mode
6	Security	128-AES	128-AES	WEP-2
7	Power Consumption	Days	Years	Very High
8	Network Topology	Star	Mesh	Peer-to-Peer, Star
9	Medium Accessing and Operating Frequency	79-FHSS 2.45 GHz	DSSS 868/915/2400MHz	DSSS/FHSS 2.4xGHz
10	Complexity	High	Low	Very High
11	Scalability	Below average	High	Low
12	Flexibility	Medium	Above average	Low

Bluetooth (IEEE802.15.1): Bluetooth can support almost all industrial applications with up to 3 Mb/s data rate in latest version 2.0. It has a limited range in multiple of few meters up to tens of meters. Reliability is rated in the medium range with error correction assistance but interference is more since used commonly by individuals in most of hand set devices increasing noise floor level. Because it is single hop device-to-device design, it must wait for that particular path to become available after it had gone down. However, network access for active slave is fast, though takes sufficient time to wake up from the sleep mode. Security model uses the 128 bit Advanced Encryption Standard. Bluetooth PIN must be entered into both communicating devices. In August 2004, range of Class 2 Bluetooth is extended to 1.78km with directional antennas. This extension in the range poses a potential security threat since attackers can hack the system from a distance beyond plants perimeter. Since all nodes are active most of the time, power consumption is high. A standard Bluetooth device battery lasts for few days only. Bluetooth supports only the star ad-hoc piconets network in which two or more piconets are connected together, with some bridging devices. It does not support the mesh networking. It can support up to 8 active devices simultaneously in a single piconet and up to 255 devices can be inactive, or parked. All parked devices occupy the same physical channel. Slave devices may only communicate with the master device. Bluetooth operates in the unlicensed 2.45 GHz band using FHSS signal of 79 1 MHz node pseudo-randomly ordered channels. AFH allows Bluetooth to detect and exclude frequencies in use by other devices and select channels in order to minimize interference. While Bluetooth complexity is limited by the small number of devices per network, its protocol stack is relatively quite complex. The degree of scalability is

low since it is quite difficult to add new nodes in the existing network. Devices can switch roles from slave to master at any time. The master switches rapidly from one device to another in a round-robin fashion. Simultaneous transmission from the master to multiple other devices is also possible.

ZigBee (IEEE802.15.4): Data rate is one of the most challenging properties for Low Rate WPAN task group technologies, IEEE802.15.4, in which duty cycle time is reduced in favor of extending battery life-time. ZigBee technology has low data rate in range of few hundreds of kbps. Moreover ZigBee has the potential to operate over a greater range because of its mesh networking topology. Experiment show that for Indoors application it can cover up to 100m and 400m for outdoors [31]. ZigBee has many features that help to increase network reliability: data packet acknowledgement, CSMA-CA, encryption and mesh topology. Multipath feature enhances system diversity and reliability by routing around obstacles and detecting losses. Resilience is very high. ZigBee has a great ability to conserve power with sleep mode that has limited effect on network latency. For new slave enumeration, it takes 30 ms and active node takes 15 ms to access the channel. ZigBee uses DSSS technique with Orthogonal O-QPSK Modulation. It employs the 128 bit Advanced Encryption Standard (AES-128) that assures basic security tool for the technology. Beyond encryption each node receives a unique short address from the network coordinator and each network has a unique ID. ZigBee has been developed specifically to permit low power consumption and years of battery life. It optimizes slave power requirements by forcing sleep mode most of the time. It operates on a very low duty cycle of <1%. It Support both ad-hoc star and mesh network topology. Device types are: Coordinator, Router, and End Device. ZigBee can support up to

65,000 nodes in the network, which are sufficient for industrial wireless networking. It has limited radio bandwidth of 250Kbps. Working bands are: 868 MHz, 915MHz, or 2.4 GHz with total of 27 channels. ZigBee packets include header with source and destination address. Network can grow easily to quite large scale implementations. In general, ZigBee has a very flexible approach for industrial applications except for cases where higher data rates are needed.

Wi-Fi (IEEE802.11): Wi-Fi is classified as high data rate technology especially for IEEE802.11n which gives more than 200 Mbps. Since Wi-Fi is a WLAN technology, it provides higher device ranges than WPAN. A typical Wi-Fi router using a stock antenna reaches 32 m indoors and 95 m outdoors. Wi-Fi uses both single carrier DSSS and multi-carrier OFDM. OFDM modulation scheme plays a major role increasing system QoS. It is robust against narrow-band co-channel interference, Inter-symbol interference (ISI) and fading caused by multipath propagation. IEEE802.11n has improved MAC layer efficiency through reducing the protocol overhead due to frame headers and inter-frame gaps. Delay spread evaluation of a factory floor is needed when IEEE802.11 is to be deployed. It takes on values of 200-300 ns in a factory floor setting. Wi-Fi networks that are open (unencrypted) can be monitored and used to read and copy data transmitted over the network, unless another security method is used to secure the data. Due to reach requirements for wireless WLAN applications, power consumption is fairly high. Network has the star topology. If an MS wants to communicate with another MS, it needs to send the information through AP. Channel sharing depends on the CSMA-CA. The maximum number of devices is 253 clients per AP, but 15-20 is recommended. IEEE802.11b/g works on unlicensed band at 2.4 GHz. It is a DSSS. It

is quit complex and has much lower scalability compared to other technologies, and even lower than Bluetooth. It is not very flexible also.

From previous discussion, IEEE802.15.4 based technologies (e.g. ZigBee) is recommended and can be selected as the best suitable technology up to date for industrial sensor networks. It satisfies the industrial requirements as data rate, reliability and security with minimum power consumption and reasonable complexity, scalability and flexibility sustained by the mesh topology turn out acceptable network latency. Bluetooth does not support mesh networking which limits the number of devices and system reliability. Whereas the Wi-Fi (WLAN technology) is delivering network speed much more than industrial requirements but number of devices, power consumption and security restrict the technology usage in sensor networking.

ZigBee works better than others in power consumption feature. The availability of other technology devices are affected drastically by battery because of large time of replacement. It is also the best choice for applications requiring small packets and infrequent communication throughout a distributed mesh network which fits the industrial application. It simultaneously supports hundreds of devices in the same network. In addition, it makes use of diversity by routing messages to a device out of the direct transmission range of the sending device. Bluetooth does not support mesh networking, which limits the number of devices and system reliability. Whereas the Wi-Fi (WLAN technology) is delivering network speed much more than industrial requirements but number of devices, power consumption and security restrict the technology usage in sensor networking.

To complete the defined scientific methodology of assessment, each technology is evaluated against industrial environment requirement which is given in chapter two, in Table 2.3. In view of that, technologies are ranked for all KPI's.

The result of the evaluation of the three selected technologies is given in Table 3.8. Each technology is assessed among the twelve items and each item is ranked out of 100%. High percentage ranking is given if technology completely satisfies industrial requirements of that item, medium is given for partial satisfaction, and minimum if it fails to achieve the minimum requirement. This ranking is multiplied by the weighting factor given in Table 2.3. Finally, for each selected wireless technology resultant rankings are summed to get final mark out of maximum 80 points. This scientific methodology of assessment ensures fair comparison between the selected technologies. In the coming section the measurement done in Hot Strip Mill plant at HADEED is presented.

Table 3.8: Sensible weights for performance indicators in Steel Mills

Item No.	Characteristics	Wight out of 10	Bluetooth	ZigBee	Wi-Fi
1	Data Rate	10	100%	80%	100%
2	Device Range	10	20%	100%	100%
3	Number of Devices	9	20%	100%	50%
4	Reliability, Availability and Resilience	8	50%	80%	100%
5	Network Latency and Throughput	8	50%	100%	50%
6	Security	8	80%	80%	100%
7	Power Consumption	6	20%	100%	0%
8	Network Topology	6	50%	100%	50%
9	Medium Accessing and Operating Frequency	6	100%	100%	100%
10	Complexity	4	50%	80%	20%
11	Scalability	3	40%	100%	20%
12	Flexibility	2	50%	80%	20%
	Total	**80**	**43**	**74**	**55**

4

INDOORS WIRELESS CHANNEL CHARACTERIZATION

Studies on wideband transmissions started in 1950; since then a substantial amount of literature is now available in the public domain. Most of the published works are concentrated mainly on providing basic understanding of radio channels and evaluation of their disruptive effects on the performance of wideband transmissions. Wideband transmissions are now a reality and to evaluate their performance, availability of channel characterization is essential. It is fundamental to understand the channel behavior in order to design a reliable wideband wireless system. Thus, analytical and practical approaches are generally combined. Impulse response of a channel provides complete information on the channel behavior. Time dispersion is a channel parameter that is related to sustainable data rate over the channel. The process of channel sounding is essentially of the Channel Impulse Response (CIR) measurement. [44]

A channel impulse response can be modeled as a tapped delay line with measured delays and amplitudes associated of each tap. The channel sounding system

used in this thesis is built on standard form that comprises: a Wideband Channel Sounder (WCS), an integrated data acquisition system, and software FCL_WCS.

The channel sounder system is basically a device that transmits a repetitive impulse or emulation of it with interval of T_b seconds and uses a receiver with a wide band filter, as shown in Figure 4.1. The received signal is amplified, detected with an envelope detector, sampled and stored. The pulse repetition rate must be fast enough to allow observation of the time-varying response of individual propagation paths, while the time interval between pulses must be long enough to ensure that all multipath signals have decayed between successive pulses. The wideband channel sounder consists of an independent transmitter and receiver. The equipment can provide the time delay resolution of 33 ns that allows obtaining a very accurate representation of the characteristics of the channel. The impulse responses generated by the sounder receiver are sampled, digitized and subsequently stored in a laptop computer for each experimental run. In this thesis, channel sounder machine works at 1.8 GHz with 60 MHz bandwidth. Receiver antenna gets sequence of impulses separated by 17.1 μs. [44]

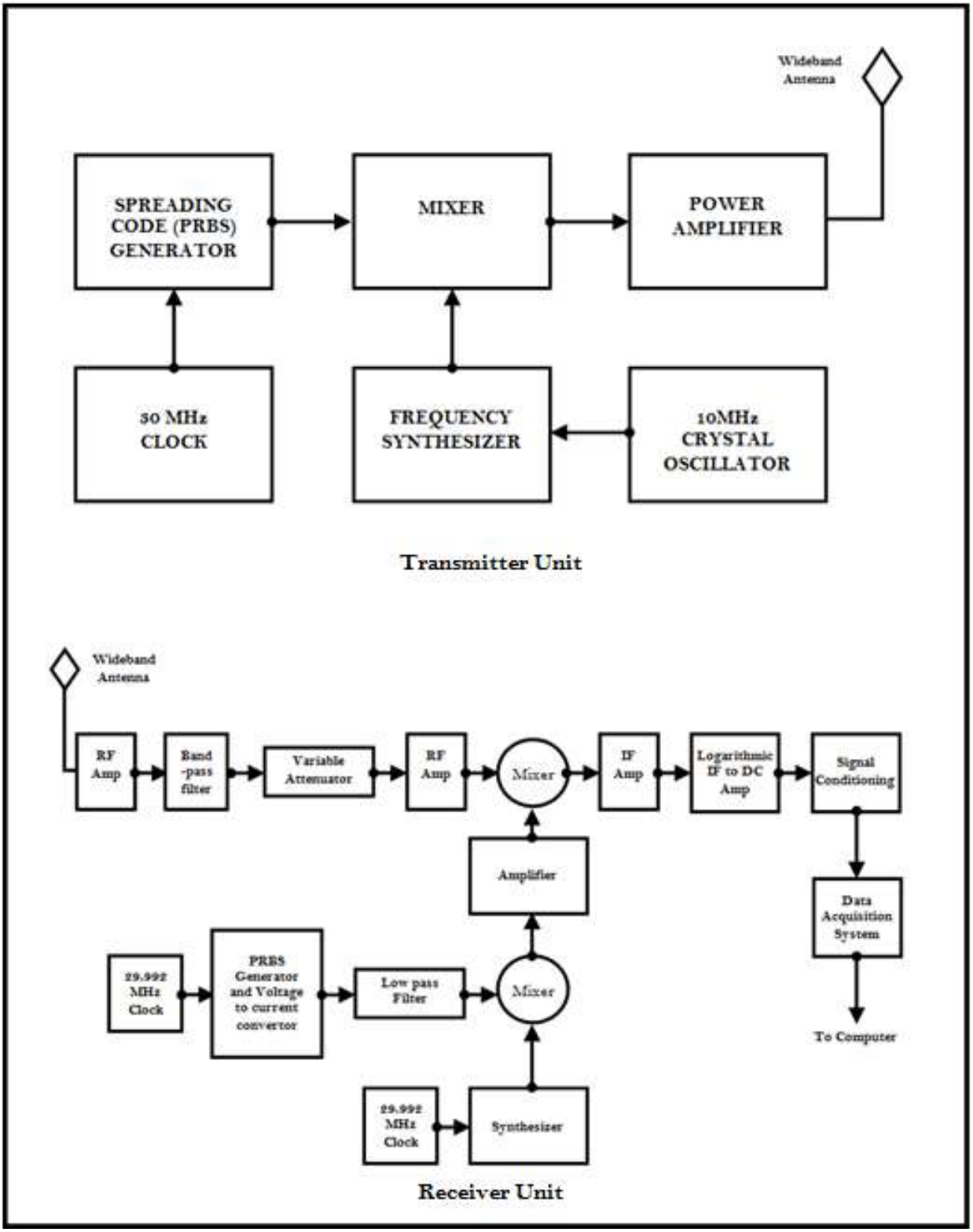


Figure 4.1: Block diagram for the channel sounder system [44]

4.1 CHANNEL CHARACTERIZATION

A first step in the design of any wideband digital mobile radio system is to acquire adequate knowledge of the radio channel. The data being transmitted signal interacts with obstructions and surface irregularities creating a continuum of scattered partial waves. Therefore, the received signal is superposition of many copies of the original transmitted signal with random time delays, amplitudes and phases. In addition, a Doppler shift ν caused by motion contributes random frequency contributing to the received signal. [45]

A multipath radio channel can be modeled as a time-varying linear filter, and thus it is formally described by its impulse response. CIR provides complete information on the channel. Measurement of CIR is analyzed to get the small-scale descriptors like: delay spread, average delay, delay intervals and delay RMS windows. Auto-correlation and cross-correlation between different measures also provide additional information on the channel. The received signal $y(t)$ is given by the convolution of the transmitted signal $x(t)$ with the time-varying channel impulse response $h(t,\tau)$:

$$y(t) = \int_{-\infty}^{t} x(t)h(t,\tau)d\tau \qquad (4.1)$$

The time variation of $h(t,\tau)$ depends on the relative motion between transmitter and receiver, the wavelength of the carrier and the nature of the scattering process. The time-varying impulse response $h(t,\tau)$ provides a general model for the channel, synthesizing the relation between a specific propagation environment, and its

influence on the received signal. However, several simplifications of this general model are possible. If the maximum Doppler shift ν_{max} is much less than the inverse of the maximum delay τ_{max} of the channel (which is normally the case), then the channel is said to be separable [46], and $h(t,\tau) \approx h_t(\tau)$. If we further assume that signals in different paths are uncorrelated, we can express the channel impulse response as: $h(t,\tau) \approx \sum_j h_j(t)\,\delta(t-\tau_j)$ where $\delta(\cdot)$ is the unit impulse function. For most purposes channel response outside a certain signal bandwidth is irrelevant, and thus channel can be sampled leading to:

$$h_b(t,\tau) = \sum_{j=0}^{P-1} a_j(t) \exp\left\{j\left[2\pi f_c \tau_j(t) + \phi\left(t,\tau_j(t)\right)\right]\right\} \delta\left(\tau - \tau_j(t)\right) \qquad (4.2)$$

This particular model $h_b(t,\tau)$ represents the equivalent baseband impulse response of the channel, where $a_j(t)$ represents the real amplitudes associated with each multipath component, and $\tau_j(t)$ represents the relative delay or excess delay of each component as compared to that of the first arriving one. The phase term $2\pi f_c \tau_j(t) + \phi\left(t,\tau_j(t)\right)$ represents phase shift due to the propagation component, plus any additional phase shifts that may be encountered in the channel. P is the total number of multipath components. Note that the amplitude, phase and delay of each multipath component can experience temporal variations due to the motion of the receiver, and that there are only P possible values of the excess delay $\tau_j(t)$. This particular model implies discrete scatterers and a geometrical optics approximation.

In order to have a satisfactory channel characterization, the amplitudes, phase shifts, and delays associated with each multipath component in the channel model represented by (4.2) must be determined. In view of the multitude of possible propagation environments, a deterministic modeling of these parameters is not feasible. The observed characteristics of mobile radio channels lead to the conclusion that their behavior is non-stationary [47], and in practice characterization proves extremely difficult unless stationarity is assumed over short distances of travel or short intervals of time. Assuming stationary over a small time or distance interval, the channel impulse response described by (4.2) can be simplified to yield:

$$h_b(\tau) = \sum_{j=0}^{P-1} a_j \exp\{j\theta_j\}\delta(\tau - \tau_j) \qquad (4.3)$$

where θ_j represents $2\pi f_c \tau_j + \phi(t, \tau_j)$. If there are no mobile obstructions within the path, or channel's pdf is Wide Sense Stationary (WSS) over a small-scale time or distance interval, system may be considered time-invariant. Equation (4.3) describes Linear Time-Invariant (LTI) system. The objective is to estimate the amplitudes, phases and delays in this simplified model; several snapshots of these estimates can be averaged to derive a statistical description of the radio channel in parameterized form [48]. This information allows evaluation of modulation schemes for different data rates, diversity techniques, coding strategies and equalization techniques; whereas from the standpoint of radio propagation modeling such information allows to relate multipath phenomena to local conditions, making possible a classification in terms of several propagation environments [45].

4.1.1 CIR PARAMETERS

Channel Impulse Responses can be compared on the base of several different parameters such as: Path-Loss (L_p), Power Delay Profile (PDP), Auto-Correlation, coherence bandwidth (B_c), etc. Several papers are available that study CIR performance. Some literatures confer CIR parameters in general like in [49], [50], and [51]. In [52], [53] and [54], CIR models with their parameter are manipulated and used for Code Division Multiple-Access (CDMA) or OFDM systems simulation.

Path loss or attenuation per unit distance is a major parameter needed in the analysis and design of the link budget of a telecommunication system. Received power is given by following equation: $P_r = P_t G_t G_r L_p$ where all are expressed in absolute values, P_r is the received power, P_t is the transmitted power, G_t is the transmitter antenna gain, G_r is the receiver antenna gain, and L_p is the path loss. In CIR measurement, gains and transmitted power are given as fixed values but received power is a variable value that can be measured during experiment. In case of multipath channel, P_r is the total received power. However, it can be approximated by the first arrival path which is usually defined as, P_{max}. Using previous equation, path loss (L_p) can be found as:

$$L_p = \frac{P_r}{P_t G_t G_r} \tag{4.4}$$

In a study of wireless communications, system path loss takes into account the frequency of operation and the link distance, i.e. $L_p = \left[\frac{\lambda}{4\pi R}\right]^{-n}$, where R is the link distance and λ is the wavelength ($\lambda = S_l/f_c$), where S_l is speed of light and f_c is

carrier frequency, n is the path loss exponent. Value of n is normally in the range of 2 to 4 and higher n means more rapid signal distance. Path loss is usually measured in dB. In its simplest form, the path loss can be calculated using following formula:

$$L_p = 10\, n\, log_{10}(R) + C \qquad [dB] \tag{4.5}$$

where R is the distance and C is a constant accounts for system losses. In next chapter, path loss exponent is estimated in the selected plant using collected measurements.

Power Delay Profile (PDP) shows the channel response for a single impulse. It gives the intensity of received signal showing multipath as a function of time delay. Each path k, also called tap, is expressed by the path time delay τ_k and the path amplitude A_k. All taps are identified by being above certain threshold level to filter out all noise.

Delay spread is an effect of this channel multipath behavior which can be defined as a type of distortion that is caused when a signal arrives at different times at its destination. This is due to reflection and diffraction of the signal in the channel where each path takes different distances and time to arrive. Estimating the stochastic measures of delay spread is an important parameter to characterize the channel. In Figure 4.2, both mean and variance for delay spread, or PDP, is shown.

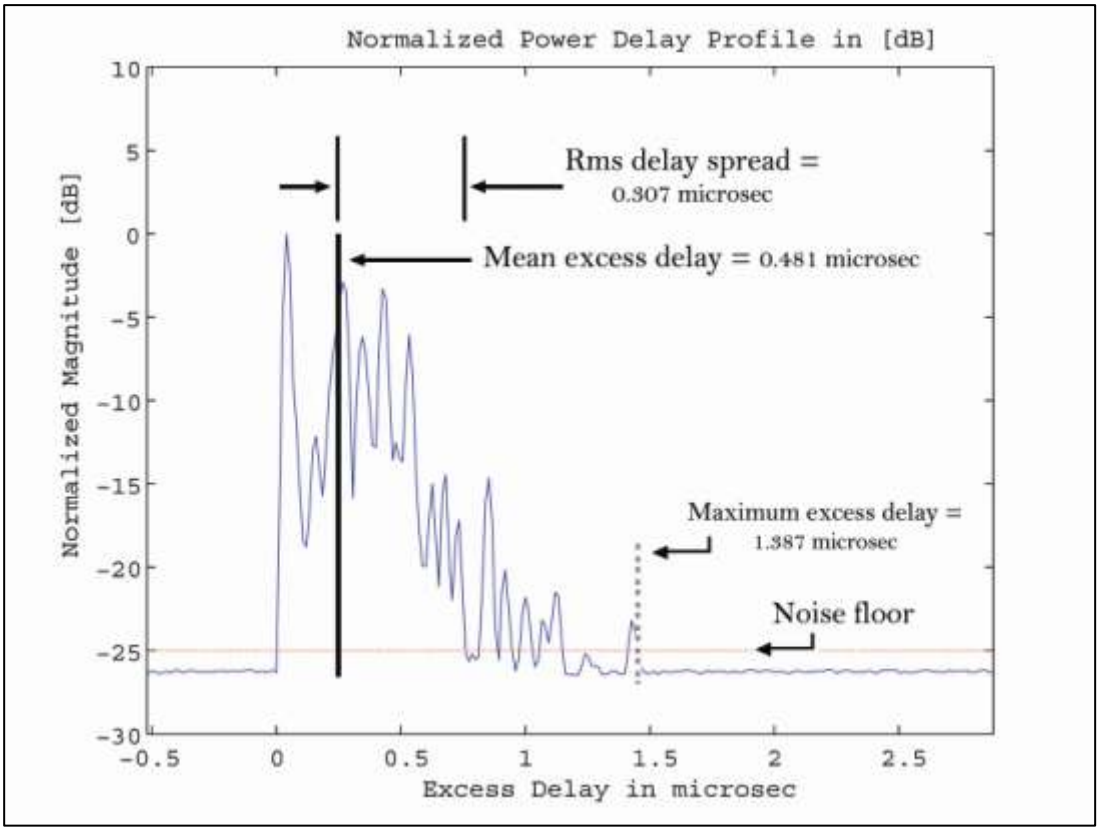


Figure 4.2: A typical CIR power delay profile

Average excess delay, or the mean, ($\bar{\tau}$) is a channel parameter that defines the average as:

$$\bar{\tau} = \frac{\sum_k \tau_k P(\tau_k)}{\sum_k P(\tau_k)} \tag{4.6}$$

where τ_j is the delay of the j^{th} path, and $P(\tau_j)$ is the power of that path. **RMS delay spread** (σ_τ) is a measure of the amount of signal dispersion in the channel which is defined as:

$$\sigma_\tau = \sqrt{\overline{\tau^2} - \bar{\tau}^2} \tag{4.7}$$

where second moment can be found form: $\overline{\tau^2} = \frac{\sum_j \tau_j{}^2 P(\tau_j)}{\sum_j P(\tau_j)}$. The RMS delay spread ($\sigma_\tau$) gives a rough estimate of the maximum symbol rate ($R_{s_{max}}$) for the channel. If σ_τ is

comparable to or larger than symbol period (T_s), time dispersion results in significant overlap among neighboring received symbol, i.e. channel-induced Inter-Symbol Interference, which requires equalization to mitigate ISI. But if $\sigma_\tau \ll T_s$, ISI is negligible. By this, the minimum symbol period for given channel can be defined as: $T_{s_{min}} = \sigma_\tau/\alpha$ where α is a constant factor. Therefore, maximum symbol rate can be approximated by: [12]

$$R_{s_{max}} = \alpha \frac{1}{\sigma_\tau} \tag{4.8}$$

Coherence bandwidth (B_c) defines the frequency range over which the components experience more-or-less the same loss while propagating through the channel. In this range, channel does not distort the signal. Coherence bandwidth, with 50% correlation factor, is given below: [12]

$$B_c = {}^{1}/_{(5\,\sigma_\tau)} \tag{4.9}$$

Reference [55] shows detailed experiments that relate coherence bandwidth with delay spread. According to channel bandwidth W, channel can be classified either to be frequency selective ($W > B_c$), or flat fading ($W \ll B_c$).

Cross-correlation is known as a sliding dot product or inner-product between two different functions or random processes which is called covariance function. For channel impulse response, cross-correlation can be calculated between different profiles spaced by selected time shifts for the same measurement location. This shows how much channel is changing with respect of temporal axis.

Autocorrelation function is defined as the cross-correlation between the function and itself with zero time difference as per following equation:

$$\Re_X(t_1, t_2) = \mathcal{E}[X_{t_1}, X_{t_2}] = cor(X_{t_1}, X_{t_2}) \quad (4.10)$$

where $\mathcal{E}[X_{t_1}, X_{t_2}]$ is the mean of the same random process with a time shift difference.

Power Spectral Density (PSD) is defined as a positive real function of a frequency variable associated with a stationary stochastic process which has dimensions of power per Hz. It shows the power distribution across the frequency axis. It is computed by taking Fourier Transform for autocorrelation function of CIR.

Number of received paths affects channel delay modeling and can be used in channel simulation to estimate bit-error-rate. Availability of what is known as Line-Of-Sight (**LOS**) path affects channel behavior. LOS is not always available because obstacles which causes Non-Line-Of-Sight (**NLOS**) condition. Multipath effect becomes apparent while analyzing channel impulse response. The received response of a single impulse might appear as a train of pulses as shown in Figure 4.3.

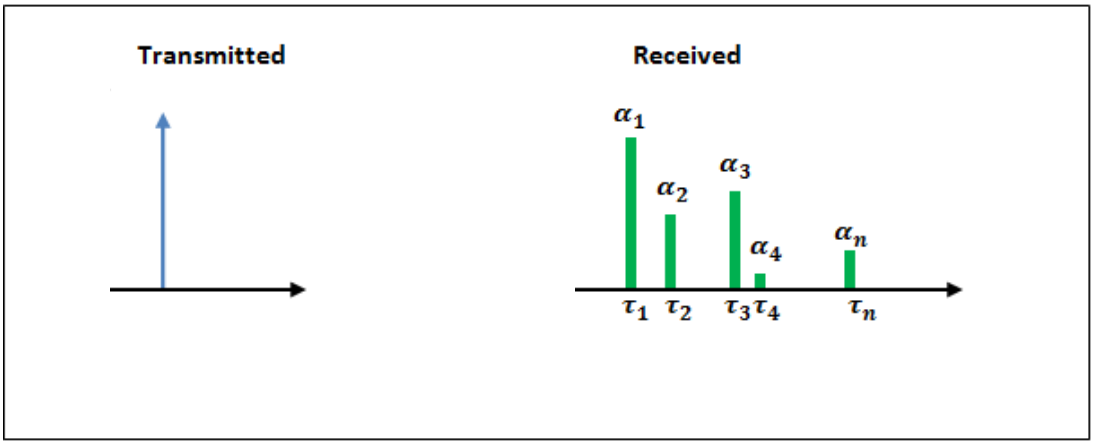


Figure 4.3: Effect of multipath channel on transmitted impulse

If experiment is repeated, changes occurring in individual received responses, in terms of strength and delay, determine channel mobility. Using equation (4.3) and considering time invariant channel condition, received signal for transmitted impulse can be expressed as follow:

$$r = \sum_j \alpha_j e^{-j2\pi f_c \tau_j} \qquad (4.11)$$

where received signal is time independent and α_j path amplitude and τ_j is the path delay. Thus, the received signal consists of the sum of number of time invariant vectors having amplitude α_j and phase τ_j. These two parameters are calculated from the CIR experimental results.

Bit Error Rate (BER) is one way to characterize the performance quality of the entire system. Several modulation schemes are used in modern digital communication systems where each scheme offers different BER behavior. Theoretical BER is given for commonly used versions of PSK and QAM modulations operating in a zero mean AWGN channel. The performance of the selected modulations schemes in ISI channel is simulated in the next chapter.

PSK scheme conveys data by the carrier phase. Binary-PSK (BPSK or 2-PSK) is the simplest form of PSK using two phases separated by 180°. Figure 4.4 shows diagrams of 2, 4 & 8-PSK constellations with gray coding. BPSK points located at 0° and 180°. This modulation is the most robust PSK modulation since distance between constellations points are the maximum for the same signal power. However, its data rate is the lowest since it carries only 1 bit/Hz. BER of BPSK in AWGN can be calculated as:

$$P_b = Q\left(\sqrt{\frac{2\,E_b}{N_0}}\right) \tag{4.12}$$

where $Q(.)$ is the Gaussian Q-function and $\frac{E_b}{N_0}$ is the bit to noise ratio. Since there is only one bit per symbol, the same equation is also valid the symbol error rate.

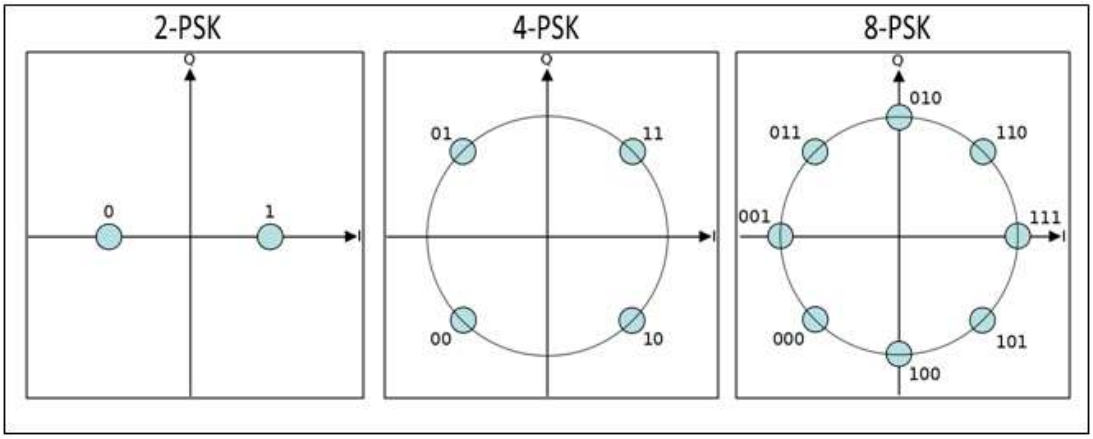


Figure 4.4: PSK constellations with gray coding

Quadrature-PSK (QPSK, 4-PSK, or 4-QAM) uses 4 constellation points equispaced around a circle. Each constellation point represents a symbol consisting of two bits. Both In-phase and Quadrature channels are utilized in QPSK and each can be treated as a single BPSK receiver. Multi-PSK points located at unity cycle with 90° difference for QPSK and with 45° difference for 8-PSK as shown in Figure 4.4. With Gray coding, Symbol Error Rate (SER) is minimized to be closer to BPSK but has twice bit rate of BPSK. Since both carriers can be independently demodulated BER of QPSK is the same as BPSK given in equation (4.12). However, QPSK consumes twice BPSK power using simultaneously 2-bits. If Signal to Noise Ratio (SNR) is high, SER of QPSK may be approximated as:

$$P_s \approx 2\,Q\left(\sqrt{\frac{E_s}{N_0}}\right) \tag{4.13}$$

where $\frac{E_s}{N_0}$ is the symbol energy to noise ratio. For multilevel signaling M-PSK, a closed form equation for the probability of bit error cannot be obtained. Instead bounds on the symbol error probability have been derived such as: [56]

$$P_s \approx 2\,Q\left(\sqrt{2\,\gamma_s}\sin\frac{\pi}{M}\right) \tag{4.14}$$

where $\gamma_s = k\gamma_b = k\frac{E_b}{N_0}$ and $M = 2^k$ with k the number of bits per symbol. Bit error probability can be approximated by $P_b \approx \frac{1}{k}P_s$. [56]

QAM conveys two digital bit streams changing amplitudes of two carrier waves. These two waves, usually sinusoids, are out of phase. Rectangular QAM constellations are, in general, sub-optimal in sense of energy. **16-QAM** is the first rectangular QAM which is shown in Figure 4.5 with gray coding, given that 4-QAM can be treated as QPSK. BER for multilevel QAM signaling is bounded through following equation:

$$P_s \approx 4\,Q\left(\sqrt{2\,\gamma_b\eta_M}\right) \tag{4.15}$$

where $\gamma_b = \frac{E_b}{N_0}$ and η_M is -4dB for 16-QAM, -6dB for 32-QAM, -8.5dB for 64-QAM, -10.2dB for 128-QAM, and -13dB for 256-QAM. [57]

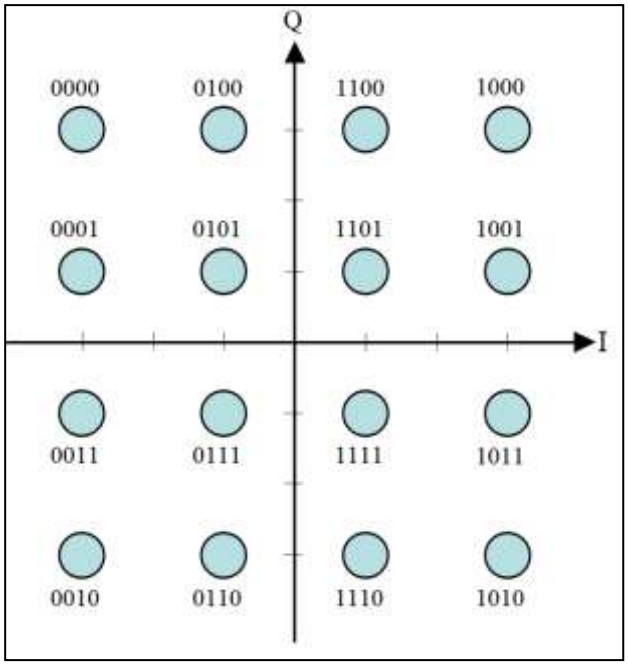


Figure 4.5: 16-QAM constellations with gray coding

Until now, BER was presented only for AWGN channel; however evaluation in multipath channel is more challenging. AWGN channel performance can be improved by increasing SNR, but on the other hand, an irreducible *floor* of BER is approached in presence of **ISI** which increases in proportion to the desired signal level. Thus, signal to noise plus interferences ratio remains constant as the signal level is increased. This effect can be mitigated by designing signal pulse shape. The amount of interference is normally determined by CIR and is used in channel modeling to predict receiver response. BER is studied and simulated using the channel impulse response.

To summarize, channel fading effect can be classified into either; time dispersion due to multipath effect, or frequency dispersion due to motion. This study

concentrates more on the former type because later type can be neglected since all sensors are located at fixed positions and the channel mobility is negligible.

In view of the preceding discussion, it is apparent that field surveys are essential in determining the parameters that describe the wireless channel impulse response in industrial environment. The studies of this kind can convince the industries owners about the high level of reliability that wireless system can achieve. This can be assured only after studying practical channel characteristics using a channel sounder. The CIR parameters of steel rolling mill plant (SABIC-HADEED) are measured, such as mean delay spread, average delay and significant number of paths. The collected data are also analyzed for autocorrelation and power spectral density in order to estimate channel bandwidth.

4.2 STEEL ROLLING MILL MEASUREMENT

In order to evaluate the performance of a practical communication system, before it is constructed, a channel model is required. Such a model is desirable as it reduces both the cost and time of system evaluation as well as highlighting the important characteristics of the channel. To develop a suitable channel model, the characteristics of the environment have to be determined through experimental measurements. Once these have been performed, measured results are analyzed to evaluate the wireless technology performance in the selected environment. Although there are many literatures covering channel measurements, very few papers are related to wireless channels harsh industrial environments which are clearly differ in their channel impulse responses.

Steel rolling mill is a typical plant model that has a unique finger print with slight structure differences. Its environment is very dense with many metallic barriers and existence of thousands of devices. The main purpose of experiments is to character the wireless channel at 1.8 GHz inside one of HADEED plants. Both transmitter and receiver are located inside the plant, i.e. indoor environment. The characteristics of wideband wireless channel are presented in terms of Tx-Rx distance separation, antenna polarization, and availability of line of sight.

4.3 PLANT OVERVIEW

Experiments were conducted in Hot Strip Mill (HSM) producing flat steel product. It is located in Jubail Industrial City in Kingdom of Saudi Arabia. This plant is part of HADEED Company belonging to SABIC Cooperation. Figure 4.6 shows few camera shots inside the plant. They show the amount of metal barriers and reflectors that can characterize wireless channel unique signature. All these obstacles increase scattering on signal transmitted over-the-air causing multipath.

Figure 4.6: Camera shots inside Hot Strip Mill

First picture, on top-right, shows roughing mill stand with exit roller table. It is a stand with four high rolls where major reduction in thickness is performed from 220mm to 30mm. Second picture, on top-left, shows the red-hot coil in coil box area before feeding to finishing mill stands. Third picture, on bottom-left, shows the red-hot bar while inter-passes in roughing mill stand. Last picture shows strip rolling process in finishing mill area.

This type of plants has a very harsh environment combining many tough conditions like: heat, water, vibration, noise, grease, etc. Some of these factors affect the wireless channel performance and some show additional importance to wireless system against wired system. In the selected HSM, there are several thousands of devices for monitoring or controlling the process.

Plant produce hot rolled coils of commercial, drawing, structural, pressure vessel, API line pipe and high strength micro-alloyed steel grades. Plant capacity is 2 million tons per year. The thickness of these products ranges between 1.5 and 16 mm while the width ranges between 850 and 1650 mm. The product meets the dimensional and shape tolerances as per American, Japanese, European standards and other specifications.

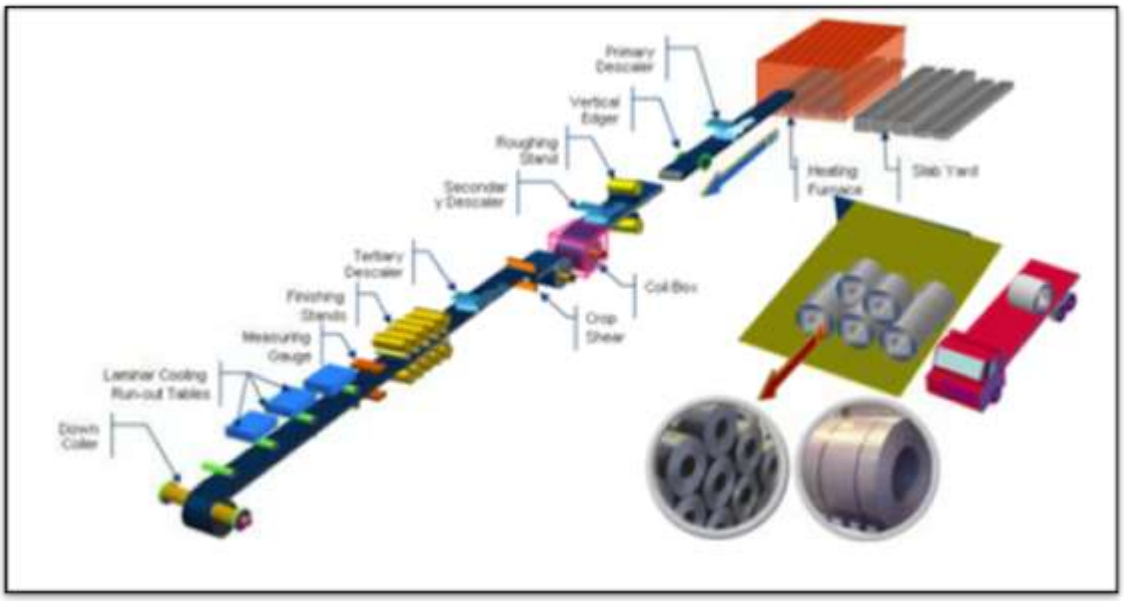


Figure 4.7: Hot Strip Mill layout

Plant layout is shown in Figure 4.7. Production process starts with heating steel slab of 220 mm thickness in a reheat furnace up to 1250°C. After red-hot slab is discharged from the furnace, it gets descaled to remove the scale by pressured water of 200 bar. Then, it is rolled for several passes through edger and roughing stands to reduce the thickness with controlled width. Red hot material at this stage, called as transfer bar, is coiled in coil box to conserves heat and interchanged head with tail. Afterward, transfer bar is fed to finishing stands train to get final required thickness, profiled, and flatness. Finally, strip is coiled in the coiler after it is cooled in laminar cooling area to control metal grains structure.

4.4 NETWORK LAYOUT

HADEED HSM plant network is divided into several layers of communication and automation functions. There are three different levels: level-3 handling customer orders with their specifications, level-2 calculating set-point references for equipments and predicted output parameters through few mathematical models, level-1 handling actual equipment control and monitoring to achieve desired set-points. Data flow up and down through these three layers starting from level-3 till level-1.

For illustration, customer places an order that is planned and scheduled on level-3 system. Then, these order specifications, for instance finished thickness, are sent to level-2 system in schedule. Level-2 runs its mathematical models to calculate expected forces, called references, required to achieve desired thickness and send it to Level-1. Level-1 system activate actuators, like motors, valves, heaters, etc., to work in closed loop control system using sensors, like load cells and thickness gauges, to achieved these force and thickness references. Throughout this process, data is exchanged up and down between different system layers through different network types of dissimilar topologies separated by gateways. This study is considering level-1 network only where process control is really performed.

There are two types of network that carryout communication in Level-1 system: (1) *master networks* and (2) *field-devices networks. Master network* is responsible for communication between different Programmable Logic Controllers (PLC) and

HMI operator stations. Traffic in this type of network carries either monitoring or open loop control packets. Both types require slow response actions where range of few seconds reaction-time is sufficient. *Field-devices network*, known as sensor network, is responsible for communication between PLC and actuators or sensors. This type of network is used for closed loop control which requires fast response actions with maximum of one second reaction-time. Controller cycle time in sensor networks varies from very fast controller of 1 ms to slower controller of one second. Level-1 network layout is shown in Figure 4.8.

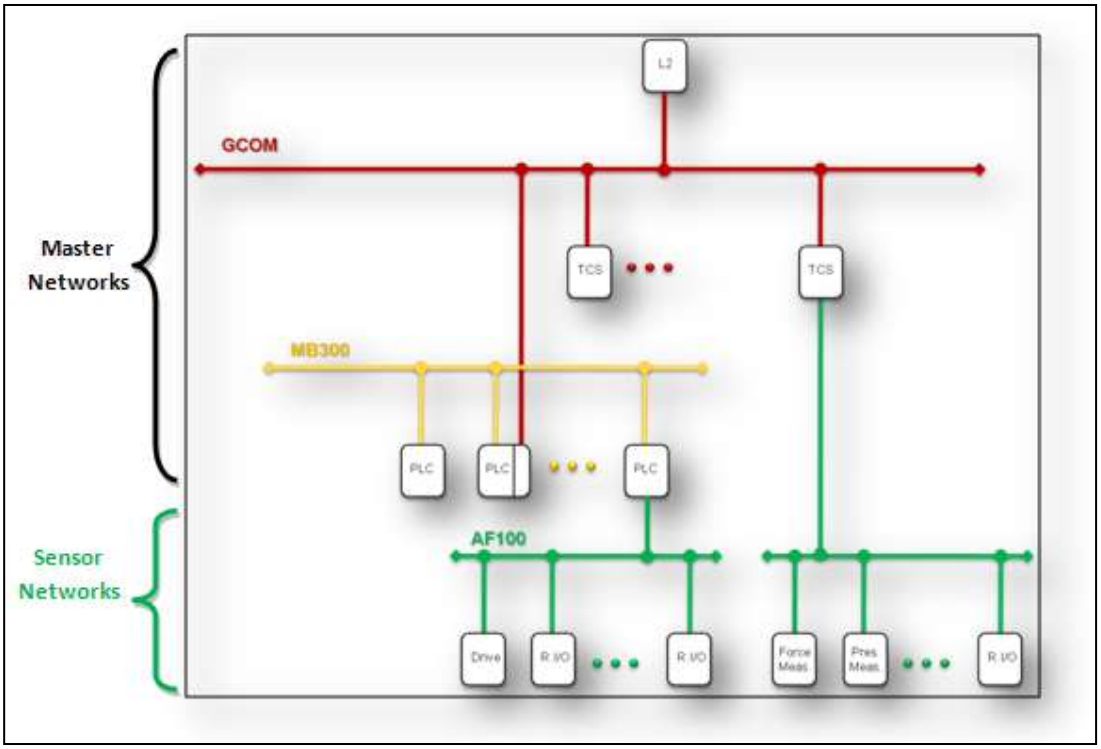


Figure 4.8: Level-1 network layout

Master networks require higher data rate than sensor network because they handle traffic between all controllers and HMI's. Network latency is not very rigid because emergency command travels through sensor network, where latency is

important. In contrast, sensor network features differ from those of master network, as it carries process control packets that require fast response, i.e. real-time communication feature. Sensor network transmits cyclic packets for both normal process control updating, and for process events and emergency alarms.

4.5 DATA COLLECTION

There were two phases of measurement experiment inside Hot Strip Mill in HADEED and each phase consisted of two sessions. First phase was conducted on 14-Apr-2009 and second phase was on 6-Jun-2009, see Figure 4.9. Wideband Omni-directional antennas were used in the experiment. The sounder system works at 1.8 GHz band. Transmitter sends a phase reversed modulated pseudo random sequence, which emulates impulses.

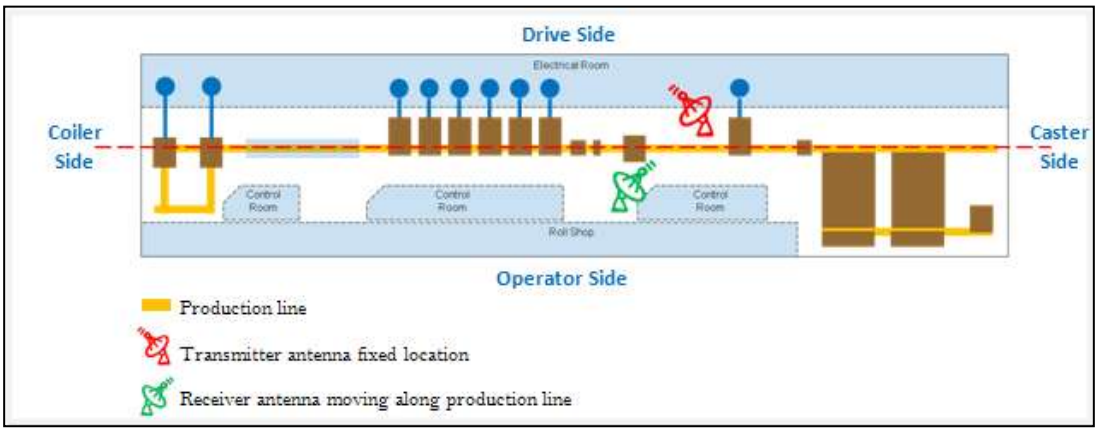


Figure 4.9: Measurements overview at Hot Strip Mill

Impulses are broadcasted with output power of 10 mW (-20 dB). Automatic Gain Control (AGC) attenuation at receiver was switched off in phase-I but switched on in phase-II. The AGC functions as a programmable attenuator with feedback from detector output used in receiver to keep the receiver within its linear region over a wide range of input signal levels. This is essentially to avoid losing data due to high level responses, i.e. AGC controls y-axis scale that moved up or down throughout measurement experiment to avoid received signal clipping. Antenna Polarization (POL) was also tested in this environment and there was a clear difference due to

antenna polarization. Summary of experimental antennas setup details per session are provided in the Table 4.1.

Table 4.1: Measurement Parameters per session

	Session-1 P01-M1 to P05-M1	**Session-2:** P06-M1 to P09-M1	**Session 3:** P11-M1 to P15-M2	**Session 4:** P16-M1 to P19-M1
Date	14-Apr-09	14-Apr-09	6-Jun-09	6-Jun-09
Tx location	RM-DS-Exit Side	RM-DS-Exit Side	FM-MCC-Room, Exit-Door	RM-DS-Exit Side
Tx Antenna height	200 cm	200 cm	140 cm	200 cm
Tx Antenna direction	Coiler Side	Operator Side	N/A	N/A
AGC switch	OFF	OFF	ON	ON
Rx location	Drive Side	Operator Side	FM-MCC-ROOM	Drive Side
Rx Antenna height	140 cm	140 cm	140 cm	140 cm
Rx Antenna direction	as per table	as per table	N/A	N/A
Antenna POL	Horizontal	Horizontal	Vertical (except P15-M2 was XPOL)	Vertical

Phase-I: The channel sounding experiment was conducted using antenna with Horizontal Polarization (HPOL). There were 13 measurements with HPOL antenna and AGC was off. To measure the CIR, transmitter antenna was placed 2.00 m high behind Roughing Mill (RM) Stand at drive side of production line. The receiver was placed at 1.4 m height. Figure 4.10 shows Tx and Rx antenna locations and distances during the first phase. In the *first session*, Tx antenna was oriented towards coiler side. Three measurements were taken when Rx was at drive side and four when it was inside the electrical rooms. In the *second session*, Rx was shifted to the operator side to measure CIR across production line. With the Rx antenna at 1.4 m height a six measurements were collected and Tx antenna was oriented towards

the operator side during these measurements. In both sessions, Rx was moved along production line and CIR was measured with different Tx-Rx distance separation.

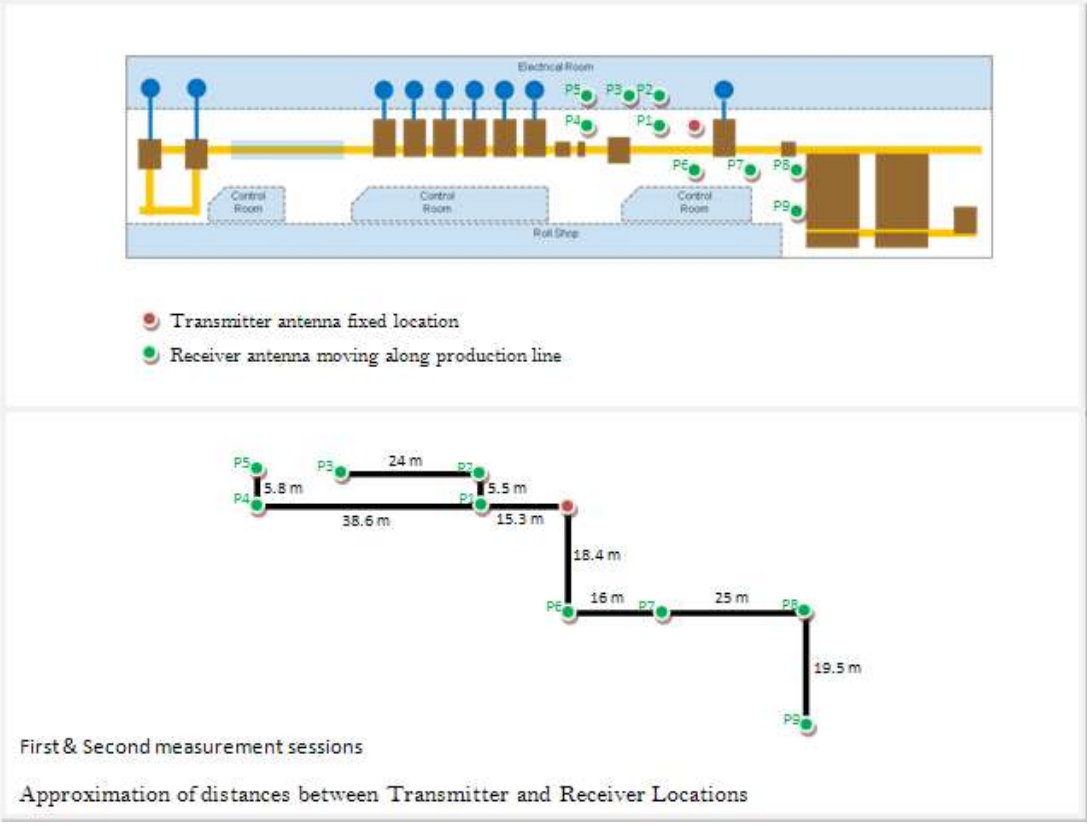


Figure 4.10: Phase-I measurement antenna locations

Phase-II: The channel sounding experiment was conducted again using antenna with Vertical Polarization (VPOL) to test antenna POL effect on CIR. There were 10 measurements with VPOL antenna and AGC was on. Similarly, there were two sessions as shown in Figure 4.11. In the *third session*, both Tx and Rx were located inside electrical room next to medium voltage AC drives; Variable Voltage Variable Frequency (VVVF) drives. The purpose behind this session was to evaluate AC drive effect. LOS path was available in three out of six measurements. In measurement P15-M2, cross-POL (XPOL) measurements were made, where Tx

antenna was HPOL while Rx antenna was VPOL. In the *fourth session*, Tx was again placed at same location of first phase, behind Roughing Mill Stand, and Tx antenna was oriented towards coiler side. Four measurements were conducted while Rx is placed at 1.40m height drive side.

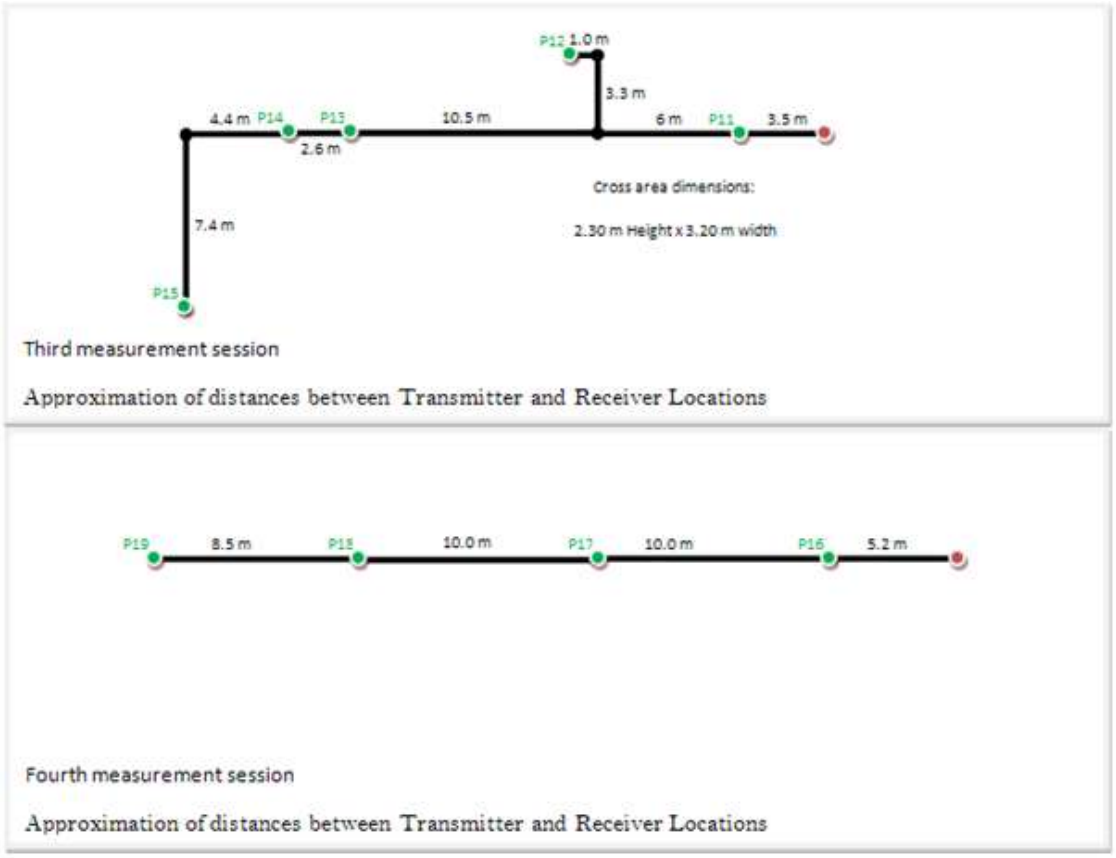


Figure 4.11: Phase-II measurement antenna locations

Table 4.2 shows the details of all 23 measurements including: locations, distances, AGC status, and orientation of Rx antenna relative to Tx antenna.

Table 4.2: Measurements details in HSM

Data File Name	Location of Rx	AGC gain [dB]	Tx-Rx Distance (m)	Tx Antenna toward	Rx Antenna toward	Tx-Rx Antenna angle diff (deg)	Comments
P01-M1	RM DS at HV Room door caster side (outside)	OFF	15.3	Coiler side	Caster side	0	LOS
P01-M2	RM DS at HV Room door caster side (outside)	OFF	15.3	Coiler side	Coiler side	180	LOS
P02-M1	HV Room door caster side (inside)	OFF	20.8	Coiler side	Operator side	90	NLOS, Door opened
P02-M2	HV Room door caster side (inside)	OFF	20.8	Coiler side	Operator side	90	NLOS, Door closed, partially opened during exper.
P03-M1	HV Room door coiler side (inside)	OFF	44.8	Coiler side	Coiler side	180	NLOS, Door closed, people walking initially
P04-M1	CB DS near to FM-PLC Room door (outside)	OFF	53.9	Coiler side	Caster side	0	NLOS, strong air blast rattling the antenna
P05-M1	FM-PLC Room door (inside)	OFF	59.7	Coiler side	Coiler side	180	LOS, Door partially opened
P06-M1	RM OS below Pulpit	OFF	18.4	Operator side	Drive Side	0	LOS
P06-M2	RM OS below Pulpit	OFF	18.4	Operator side	Caster side	90	LOS
P06-M3	RM OS below Pulpit	OFF	18.4	Operator side	Coiler side	90	LOS
P07-M1	RM OS Entry side	OFF	34.3	Operator side	Coiler side	90	NLOS
P08-M1	Furnace#1 Mill side	OFF	59.4	Operator side	Coiler side	90	NLOS
P09-M1	Furnace#1 Charging Side Mill side corner	OFF	78.9	Operator side	Drive Side	0	NLOS
P11-M1	In front of PR Drive	ON	3.5	Up side	Up side	N/A	LOS, movement in the link
P12-M1	Between Load Centers	ON	13.8	Up side	Up side	N/A	NLOS, people moved during exp
P13-M1	At edge of ROT Drives	ON	21.0	Up side	Up side	N/A	LOS, obstruction table with rack
P14-M1	After edge of ROT Drives	ON	23.6	Up side	Up side	N/A	LOS, edges and obstructive table
P15-M1	Next to Lighting panel	ON	35.4	Up side	Up side	N/A	NLOS
P15-M2	Next to Lighting panel	ON	35.4	Up side	Caster side	N/A	NLOS; Rx: HPOL
P16-M1	FM-PLC Room door (outside)	ON	33.7	Up side	Up side	N/A	LOS, Mill running
P17-M1	HV Room door coiler side (outside)	ON	25.2	Up side	Up side	N/A	LOS, signal attenuation
P18-M1	Behind RM Slab Pusher	ON	15.2	Up side	Up side	N/A	LOS
P19-M1	Near to Tx	ON	5.2	Up side	Up side	N/A	LOS

In the next chapter, CIR measurements results are analyzed for delay spread and number of paths. Then, BER performances are simulated for the measured CIR using several digital modulation schemes in order to compare performances. Transmission data rate is estimated by running simulations that used measured wireless channel impulse response.

5

DATA ANALYSIS AND RESULTS

The WCS 1800 channel sounder system transfers collected measurements to a data acquisition system, i.e. computer unit (PC), where data is stored. Data are stored in a file with extension of [*.PDP] which can be used by MATLAB program. Each measurement consisted of several hundreds of profiles which are averaged to get average delay profile per measurement. After processing average profile, all stochastic results are generated by MATLAB code. Each multipath Power Delay Profile (PDP) is analyzed to estimate PDP parameters like; number of paths, average delay, delay spread, delay interval, and delay window.

Measurements show that the channel Infrared Radiation (IR) does not vary appreciably with time and is therefore considered as static. This result is valid since almost all devices in plant are fixed and temporal variation in channel can be neglected. Hence, channel maybe considered as a LTI system and CIR can be simplified as given in equation (4.3).

In this chapter, the collected data is analyzed and used for understanding the channel behavior. Actually, **design part** arrives now to tie all these valuable results together. This design is done through several analysis stages as follow, see

Figure 5.1. In the **First Stage**, channel link budget is estimated using received power level. The expected outcome of this stage is to estimate the propagation loss exponent n as per equation (4.5). In the **Second Stage,** Power Delay Profile (PDP) is viewed by identifying power and delay associated to each tap, i.e. received path. Measurements recorded are analyzed for all stated CIR parameters namely; number of paths, maximum excess delay τ_{max}, mean excess delay $\bar{\tau}$, RMS delay σ_τ, maximum symbol rate R_s, coherence bandwidth B_C, and autocorrelation with power spread spectrum plots. In addition, overall plant PDP parameters are estimated. In the **Third Stage,** multipath CIR model is estimated for the same measurements. This stage uses the output of previous stage as an input. This channel modeling stage is done through optimization process for the highest significant taps. In the **Fourth Stage**, using these realistic channel models, ISI caused by channel time dispersion is tested to get best detection position. Finally in the **Fifth Stage,** BER is simulated for channel models using results of ISI test for best detection position. BER is simulated for several modulation schemes, and the results are compared with theoretical in the presence of AWGN.

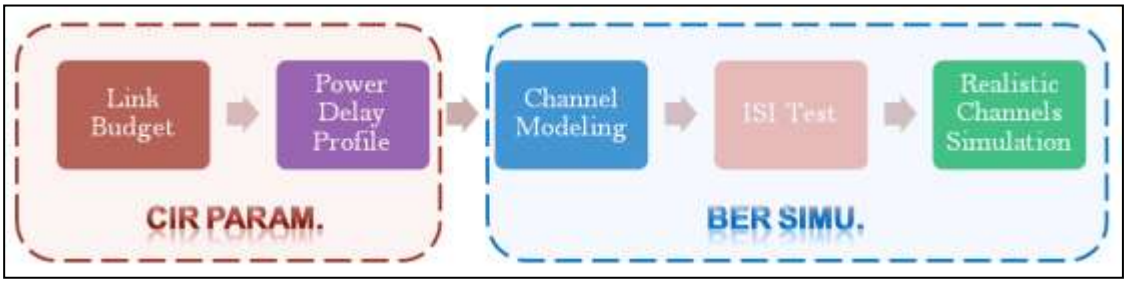


Figure 5.1: Flow chart for design stages

Analysis starts with locating the starting point of profile. Then, minimum power threshold level is defined and all responses above the selected threshold are considered. After that, the CIR paths are separated with their amplitudes and inter-pulse delays which are noted. Received power is noted to be used in link budgeting analysis. Averaged profiles are used to analyze data for channel parameters. Finally, the CIR paths and their strengths are used for simulating data transmission through channel model using several modulation schemes.

Experiment setups for all 23 measurements are given in Table 4.2. Two measurements were not valid, i.e. P05-M1 and P16-M1, because these did not meet the minimum requirement for valid CIR. One measurement was having almost only noise starting with a very minor peak, i.e. P06-M1. In link budgeting stage, the all 21 valid measurements are used considering carefully measurements affected by concrete wall (NLOS), as in Table 5.1. Similarly, in the channel PDP parameters analysis stage, all 20 valid measurements, excluding P06-M1, are considered as in Table 5.2. Out of these, 7 measurements are selected in channel modeling stage, as this set can represent others, as shown in Table 5.4. Those were also used in bit error rate simulation.

5.1 LINK BUDGET

A **link budget** is an estimation of received power level at receiver. To get an accurate estimation, all gains and losses in the telecommunication system from the transmitter to the receiver shall be accounted. This includes attenuation of a transmitted signal due to; (1) channel propagation, (2) antenna gains, and (3) system losses. However, this thesis estimates losses due to channel propagation only since antenna gains and system losses are communication system dependant unlike channel losses which is fixed for the selected environment. In this section, path loss explained in Section 4.1.1, is estimated for 21 valid CIR measurements.

This is the **First Stage** of deign, where channel **link budget** is calculated through interpolating path loss differences between measurement points verses antennas' locations, i.e. the distance separation between transmitter and receiver. To have an accurate estimation of the attenuation exponent *n*, measurements which have only NLOS paths is treated in a way considering having additional loss due to signal propagation though concrete walls. To estimate a channel link budget, received power must be provided using PDP figure. The stored values in files are expressed in terms of actual received voltage unit. This stored voltage values are converted using the scalar factor, as per manual, to get the channel attenuation power in logarithmic scale (dB). In fact, the path loss attenuation (in dB) of any CIR is derived from stored voltage values using the linear relation shown in Figure 5.2.

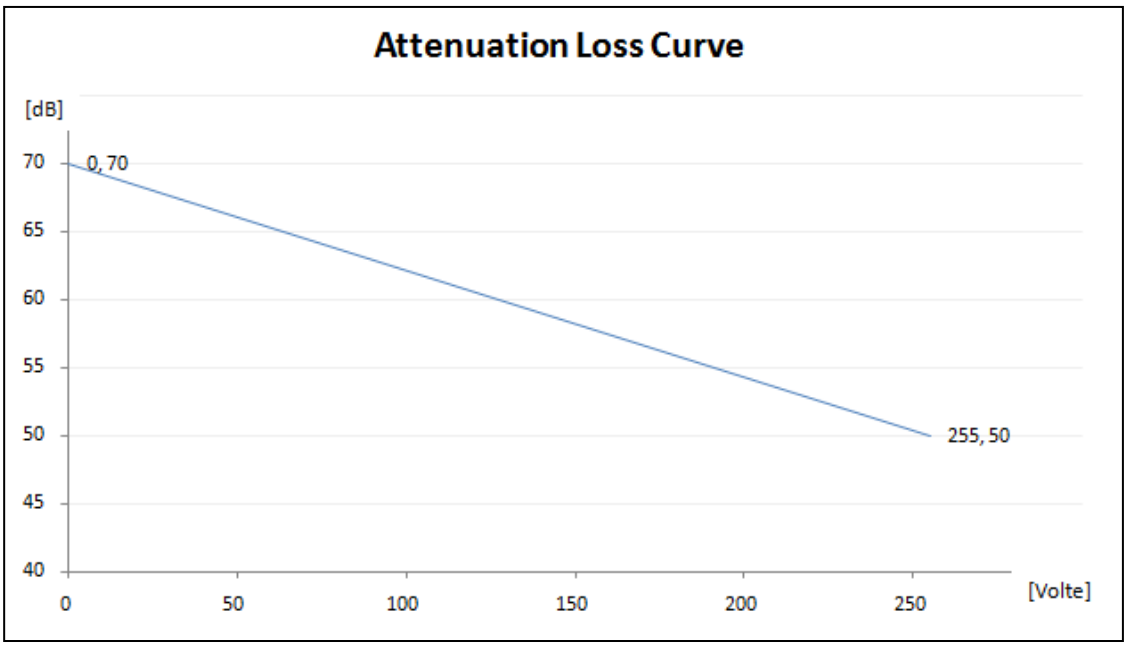


Figure 5.2: Conversion curve between stored voltage and attenuation loss [44]

This linear relation figure converts the stored values to a prim attenuation loss in dB ($\hat{L}_p$). This dB value is added to AGC gain, given in Table 5.1, to get path loss (L_p), for each CIR measurement. To estimate the path loss exponent (n), equation (4.5) is used, by means of following approximation: ($C = 0$). Because transmitted power (P_t) is fixed at 10 dBm, received power (P_r) can be found from above calculated path loss by following straight forward equation of: ($P_r = P_t - L_p$). However, there are two methods to estimate the received power:

- **Method-1:** To consider the power for the first received path only
- **Method-2:** To consider the power for all received paths

All those calculations (P_t, L_p, and n) are summarized and shown in Table 5.1, for both methods.

Table 5.1: Path Loss data of Measurements

Data File Name	Comments on Results	Distance R [m]	AGC gain [dB]	Method-1: Consider 1st path only			Method-2: Consider all paths		
				P_r [dB]	L_p [dB]	n expon.	P_r [dB]	L_p [dB]	n expon.
P01-M1	LOS	15.3	0.0	-72	52	4.41	-66	46	3.92
P01-M2	LOS	15.3	0.0	-74	54	4.53	-64	44	3.73
P02-M1	NLOS, wall between Rx-Tx	20.8	0.0	-84	64	4.85	-76	56	4.28
P02-M2	NLOS, wall between Rx-Tx	20.8	0.0	-87	67	5.05	-81	61	4.60
P03-M1	NLOS, wall between Rx-Tx	44.8	0.0	-87	67	4.08	-83	63	3.80
P04-M1	LOS	53.9	0.0	-83	63	3.61	-74	54	3.14
P05-M1	Not Valid	59.7	0.0	N/A	N/A	N/A	N/A	N/A	N/A
P06-M1	LOS, only noise	18.4	0.0	-89	69	5.48	-73	53	4.17
P06-M2	LOS	18.4	0.0	-70	50	3.96	-64	44	3.46
P06-M3	LOS	18.4	0.0	-70	50	3.96	-64	44	3.51
P07-M1	NLOS	34.3	0.0	-77	57	3.74	-68	48	3.15
P08-M1	NLOS	59.4	0.0	-86	66	3.69	-69	49	2.75
P09-M1	NLOS	78.9	0.0	-87	67	3.51	-77	57	3.00
P11-M1	LOS	3.5	28	-48	28	5.15	-47	27	4.96
P12-M1	NLOS	13.8	25	-49	29	2.57	-49	29	2.57
P13-M1	LOS	21.0	24	-52	32	2.38	-51	31	2.31
P14-M1	LOS	23.6	20	-55	35	2.52	-54	34	2.48
P15-M1	NLOS	35.4	4	-69	49	3.18	-68	48	3.11
P15-M2	NLOS	35.4	8	-68	48	3.10	-67	47	3.06
P16-M1	Not Valid	33.7	20	N/A	N/A	N/A	N/A	N/A	N/A
P17-M1	LOS	25.2	19.5	-56	36	2.55	-55	35	2.52
P18-M1	LOS	15.2	24	-50	30	2.50	-49	29	2.48
P19-M1	LOS	5.2	28	-48	28	3.87	-48	28	3.87

Table 5.1 shows the received power, average AGC gain and Tx-Rx antenna distances for all measurements. During the experiment, there were two different situations where we can approximate a single value of path loss exponent (n) for each situation. These situations are defined as following:

- **Case1:** consists of some measurements done during Phase-I which was inside plant or inside electrical room with HPOL antenna: [P01-M1 till P09-M1]
- **Case2:** consists of some measurements done during Phase-II which was inside plant with VPOL antenna: [P11-M1 till P19-M1]

To estimate the path loss exponent (n), each measurement is represented by a dot or x mark in the scattered plot in Figure 5.3. After all measurements are presented on same figure, exponential trendLine is plotted on the top of same figure for each situation. There are two cases into two methods, which result in total of four curves as following: HPOL all paths, HPOL 1st path, VPOL all paths, VPOL 1st path.

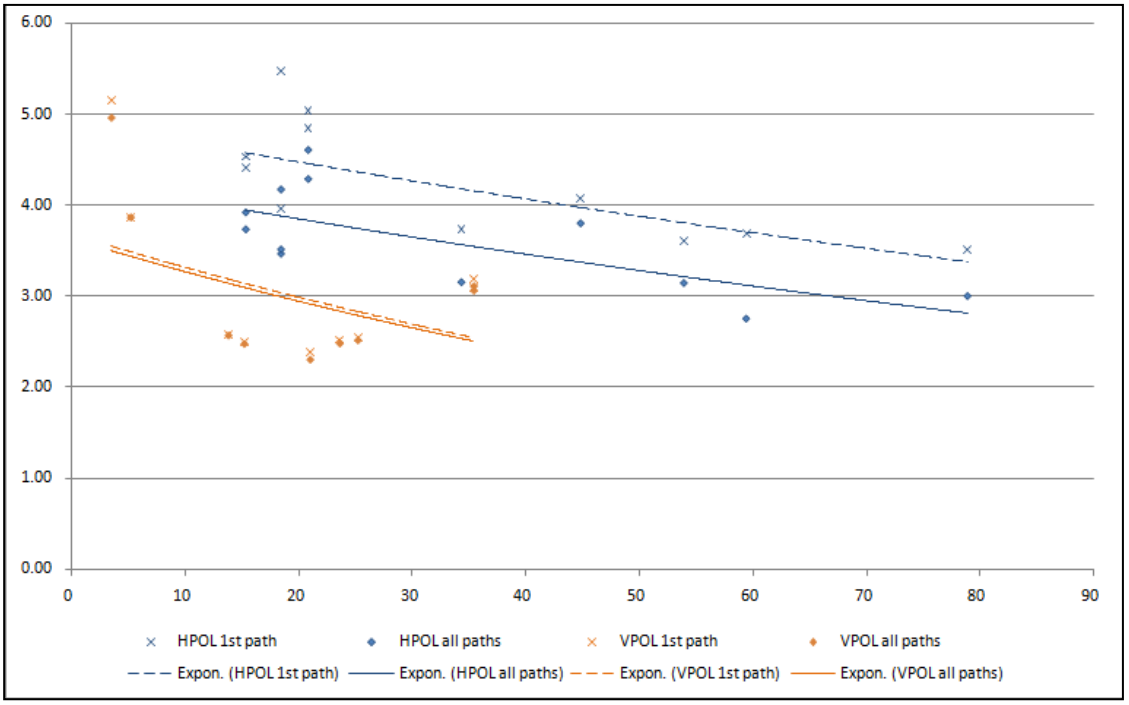


Figure 5.3: TrendLine for estimating path loss exponent n

After taking the average of each curve individually, following approximation of path loss exponent (n) can be estimated:

- **Case1, method-1**: $n \approx 4.0$
- **Case1, method-2**: $n \approx 3.5$
- **Case2, method-1**: $n \approx 3.0$
- **Case2, method-2:** $n \approx 3.0$

These values are very reasonable as other measurements repeated in literatures prove that n is between 2 and 4 [12]. In electrical room where n is equal to ideal case, the exponent is in the range of 2. However, inside the plant the value of n is higher as expected due to effect of the harsh environment. One very important point that needs to be highlighted here is that VPOL situation gives better n factor than that result for HPOL. Nevertheless, these approximations of n factor are to deploy in wireless system design. For the **case2**, both methods give almost same trendline since there is less number of paths, and most of the received power is concentrated within the first path. This is not the **case1** where the power is more distributed through other paths due to high time dispersion effect in HPOL.

Comparing with results shown in [58], n estimation in this thesis is in higher side for HPOL cases which reaches more than 4 (around 4.5). On the other hand in [58], for obstructed paths in heavy clutter, however, attenuation increases with distance to the 3rd or 4th power. Average factory path loss was found to be a function of distance to the 2.2 power [58], [59]

A **concrete wall effect** is clear since the received power levels are very low, i.e. for points: P02-M1, P02-M2, P03-M1, and P05-M1 with power of 12.6, 5.4, 3.6, and 0 dBm respectively. In these points, Rx is located inside electrical room whereas Tx is on the mill floor and doors of electrical room are kept closed, see Figure 4.10. This is because of absence of LOS path in those measurements. Comparing with other measurements that fall in same distance Tx-Rx separation but having LOS paths, additional attenuations in received power can be easily observed. This extra attenuation is due to that the signal penetrates through the concrete wall before reaching destinations causing another loss as per all known large-scale models. Result of calculation shows that wall add additional attenuation loss of almost 18 dB because there is no LOS path. This is an important observation for network design stage since all control computers are located in those almost isolated air-conditions rooms.

Many medium voltage AC motor **Variable Voltage Variable Frequency** (VVVF) drive-converters are available to control the rolling speed. Although, those voltage and frequency converters drives have a strong electromagnetic field affecting many small electronic devices performance, there is no impact at all of those drives on the wireless channel. It shows almost same behavior inside plant.

5.2 CHANNEL MODELING

As explained in Chapter 4, the industrial wireless channel is considered as a LTI channel. Therefore, this study concentrates only on multipath effect. In **second stage** of deign, the measured CIR profile is analyzed to get channel parameters. This analysis can explain and configure the plant shape that causes irregularity in the height of equipment and surfaces are disjoint. These surfaces are likely to produce large number of multipath due to irregularity in current distribution. This information facilitates the design for better channel model and error prediction.

As explained in Section 4.5, 23 measurements were collected for different locations. In this section, all channel parameters, explained in Section 4.1.1, are estimated using equations (4.6), (4.7), (4.8), and (4.9). PDP parameters are calculated from measured average profiles and results for 20 measurements are shown in Table 5.2, i.e. number of paths, maximum excess delay τ_{max}, mean excess delay $\bar{\tau}$, RMS delay σ_τ, maximum symbol rate R_s, and coherence bandwidth B_C. Using MATLAB, average PDP response for those measurements are plotted in Appendix-A.

Number of paths is found by locating the peaks with strengths above a selected threshold. Noise level is determined by referring to receive noise figure at tail. Then, threshold level is identified as 10 percentile out of maximum peak starting from noise level. It is more accurate to identify peaks/taps on dB scale. As shown in Figure 4.2, noise floor level is identified around 27dB below normalized maximum peak ($0dB$) in PDP. Then, threshold level is identified at 25dB below normalized maximum peak which is the 10 percentile.

A separated path is identified wherever its peak crosses the defined threshold level. The peak of the path identifies the time at which it occurs. By indicating path location, both time delays τ_j and power amplitudes $P(\tau_j)$ in equation (4.6) are found. Maximum excess delay is found by the time difference between first and last identified peaks before falling below the threshold level. From the discussion, it is very clear that changing the threshold level affects all PDP parameters.

Table 5.2: Measurement channel PDP parameters

Data File Name	Number of paths	Max Excess Delay [µs]	Mean Excess Delay [µs]	RMS Delay [µs]	$R_{s_{max}}$ [Ksps]	Bc [KHz]
P01-M1	16	1.387	0.480	0.307	815	650
P01-M2	23	1.187	0.436	0.310	806	640
P02-M1	8	0.640	0.252	0.182	1,372	1,100
P02-M2	6	0.333	0.163	0.125	1,993	1,590
P03-M1	4	0.267	0.097	0.111	2,248	1,800
P04-M1	9	0.880	0.365	0.254	983	790
P06-M2	19	1.027	0.378	0.269	928	740
P06-M3	17	1.187	0.401	0.291	858	690
P07-M1	20	1.253	0.478	0.304	821	660
P08-M1	18	1.267	0.387	0.315	794	640
P09-M1	11	0.760	0.397	0.224	1,119	890
P11-M1	3	0.200	0.070	0.056	4,449	3,560
P12-M1	1	0.000	0.000	0.001	250,000	200,000
P13-M1	3	0.107	0.061	0.031	8,035	6,430
P14-M1	3	0.227	0.108	0.076	3,289	2,630
P15-M1	3	0.093	0.075	0.038	6,542	5,230
P15-M2	2	0.067	0.057	0.029	8,592	6,870
P17-M1	2	0.093	0.064	0.041	6,126	4,900
P18-M1	2	0.067	0.051	0.025	10,003	8,000
P19-M1	1	0.000	0.000	0.001	250,000	200,000

Finding PDP parameters for the plant is extremely useful; mean and standard deviation or variance. This provides better understanding of this industrial

channel. This can be done after isolating similar measurement points together in a group. Situations are classified into three sets as following:

- **Situation1:** It consists of some measurements done during Phase-I which was inside plant with HPOL antenna: [P01-M1, P04-M1, P06-M2, P06-M3]
- **Situation2:** It consists of some measurements done during Phase-II which was inside electrical room with VPOL antenna: [P11-M1, P13-M1, P14-M3]
- **Situation3:** It consists of some measurements done during Phase-II which was inside plant with VPOL antenna: [P17-M1, P18-M1, P19-M1]

Results are summarized in Table 5.3.

Table 5.3: Plant PDP parameters

Situation	Averaged Number of paths	Averaged Max Excess Delay [ns]	Averaged Mean Excess Delay [ns]	S. d. of Mean Excess Delay [ns]
Situation1	14	926	348	125
Situation2	3	139	74	20
Situation3	2	80	58	9

Browsing the results, it becomes clear that the presence of large number of paths in CIR is indicative of metallic barriers or sharp edges inside the plant. This smooth surface contour of equipment increases the reflections, diffractions due to sharp metallic edges, and scattering due to irregular surfaces. In addition, VPOL in case2 and case3 provides lesser number of paths and shorter delay spread. HPOL in case1 results in more than four to five fold increases in the number of paths. Thus, transmission with VPOL shows better performance than transmission with HPOL. This influences directly the channel delay spread, available channel bandwidth and

hence, data transmission rate. However, the primary data rates can be improved with the use of diversity, error control coding and equalization.

An electromagnetic wave POL is defined by electrical vector. As general rule, HPOL is quieter than VPOL and particularly, there are many devices using VPOL at 2.4GHz. Likewise, a similar behavior is expected at 1.8GHz; the measurement frequency of our set up. The results provide explanation to what is observed in HADEED HSM. Since, selected plant environment are full of sharp edges and metallic equipments with very limited space this has more effect on HPOL because of higher sensitivity to environmental clutter. On the other hand VPOL is more rugged against these conditions. HPOL normally works better for limited power devices since there is lower noise floor.

Looking at results of other lectures, the number of significant multipath components P was determined in the selected factory in [60]. After filtering out all samples corresponding to noise, the number of multipath components was found to be $P = 60$, which is much more than the situation found here, with maximum access delay of 250 ns, which is less than the situation found here. The calculated statistical results show that of excess delay modeling fit to lognormal PDF and that amplitude modeling fit to Nakagami PDF. [60], [61]

In reference [58] there are five factories that make up a diverse collection of industries and building structures. Results show that the range of RMS delay spreads is from 100 to 250 ns with the excess delay, in a heavy clutter area, of about 800 ns. None of the five selected factories has the same results as what is shown here in this

thesis for HPOL case were RMS reaches to 315 ns with maximum excess delay of 1,387 ns.

Before channel modeling stage, PDP parameters calculated earlier are used as the input for this stage. Total summation of peaks/taps amplitudes of average profile is normalized to unity to have total power equals one. This normalization is done while channel model stage, because received power level is important as relative to noise ratio (**SNR**) but not as absolute value. First received path is considered as the starting point of the impulse response.

In the **third stage** of deign, using previous identified indices of peaks/ taps, number of peaks that are included in the analysis is determined. Only peaks/taps that hold together 80-95% of total received power (absolute values) form the **channel model**. This procedure is used to reduce the computing time and it does not seem to affect the channel behavior significantly. Once again, these selected peaks/taps are scaled to produce unity summation. This normalization procedure is followed to have fair comparison between different measurements while total absolute signal power is normalized to unity. Finally, power amplitudes with respective time delays of channel model peaks/taps are stored in a vector which is used to define channel model.

Channel modeling is done only for 7 selected measurements stated in Table 5.4. They are selected to compare all possible combination of situations. This can show the effect of: channel model parameters (including delay spread and number of paths), antenna POL selection, and LOS path availability. Appendix-B presents channel models for these selected measurements. This channel model is used in the

next section describing simulations to evaluate the bit error rate performance for selected digital modulation schemes.

Table 5.4: Channel model PDP parameters

Data File Name	POL and LOS	Noise floor [dB]	Model Number of paths	Model max excess delay [ns]	Model mean excess delay [ns]	Model RMS delay [ns]	$R_{s_{max}}$ [Msps]
P01-M1	HPOL LOS	-25	5	493	33	98	1.03
P04-M1	HPOL LOS	-11	7	613	174	129	0.78
P07-M1	HPOL NLOS	-24	9	680	253	12	8.61
P09-M1	HPOL NLOS	-7	10	760	452	111	0.91
P19-M1	VPOL LOS	-20	1	0	0	0	-
P15-M1	VPOL NLOS	-23	2	53	0.001	0.27	365
P15-M2	XPOL NLOS	-20	1	0	0	0	-

The results in the Table 5.4 show that the number of paths has reduced drastically when a 80-95% of total received power is used. This assures less data processing time with reasonable accurate approximation. Results of channel sounding may be analyzed in different ways. Taking Fourier Transform for CIR gives Spaced-Frequency Correlation Function (SFCF) which provides an idea about frequency response of this model and coherence bandwidth B_C can be defined at $-3dB$ as shown in Figure 5.4.

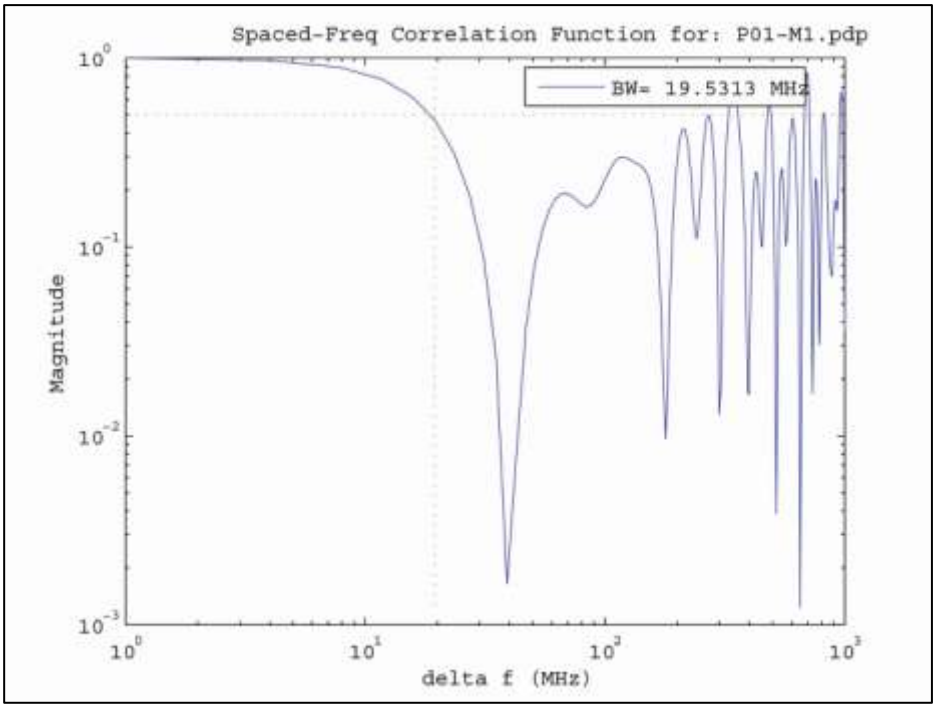


Figure 5.4: Spaced-frequency correlation function

For channel model P01-M1, coherence bandwidth B_C *is* $19.5MHz$ as shown in Figure 5.4. Whereas with 50% correlation factor and using equation (4.9) $B_C = 2.0MHz$ since $\sigma_\tau = 98ns$ in Table 5.4. Whenever used signal BW is more than this value *frequency-selectivity* kicks in and signal faces strong distortion. For bandwidth, channel is narrower than be the coherence bandwidth defined *frequency-nonselective* (or *time-selective*) where signal faces flat fading effect only.

Auto-correlation function is calculated using MATLAB function and plotted for measurement P01-M1 for individual profiles in Figure 5.5. It shows that the channel does not change much across time axis. Cross-correlation function is calculated using MATLAB function between different profiles for the same measurement. It is plotted for P01-M1 measurement in Figure 5.6, and its Power Spectral Density plot is shown in Figure 5.7.

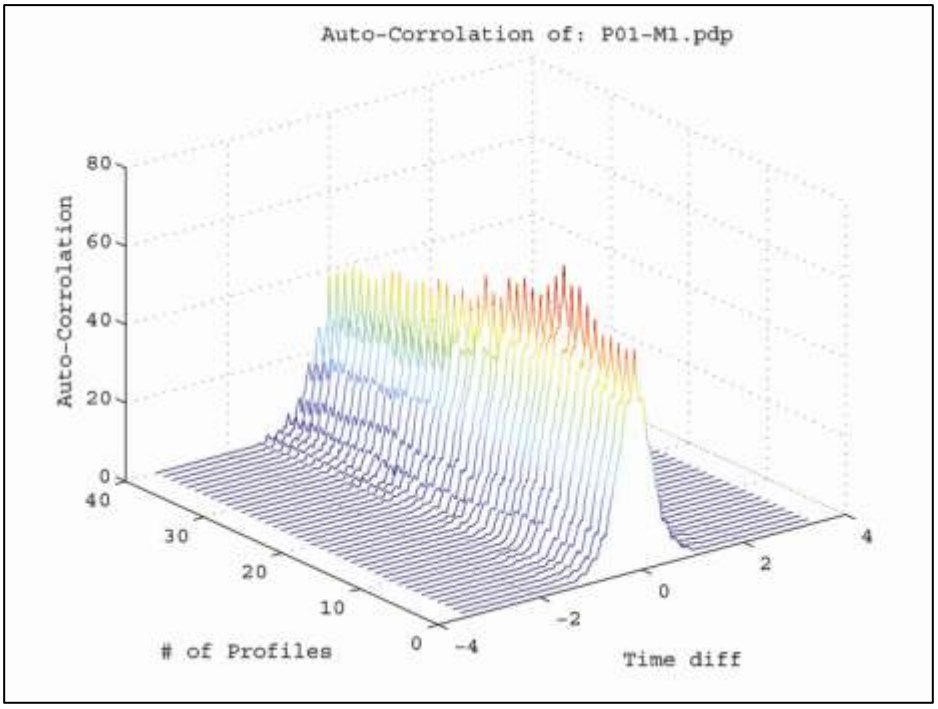


Figure 5.5: Auto-correlation function

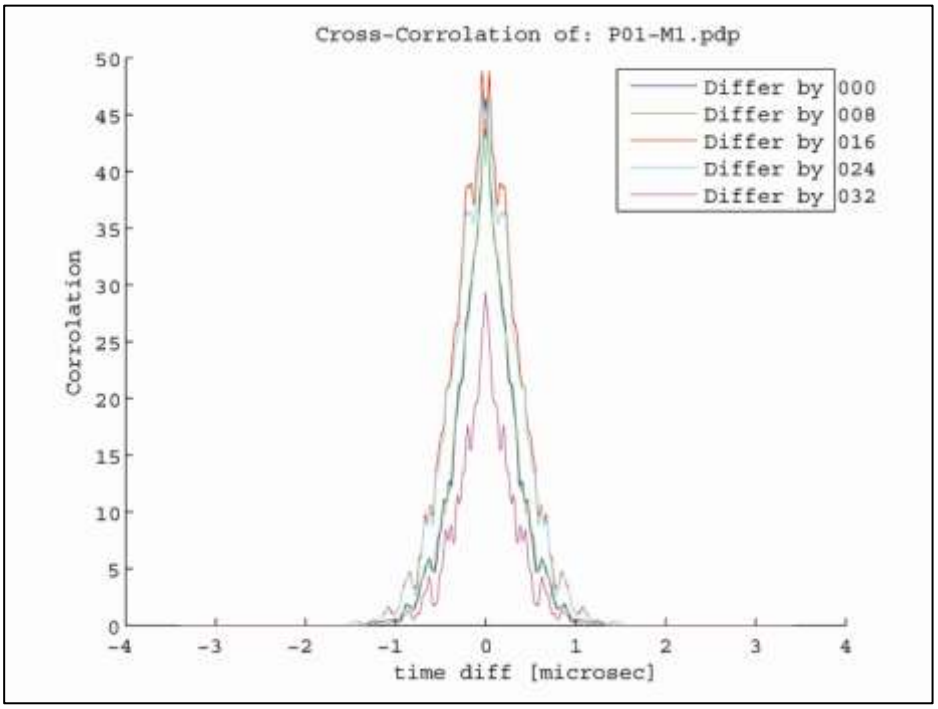


Figure 5.6: Cross-correlation function

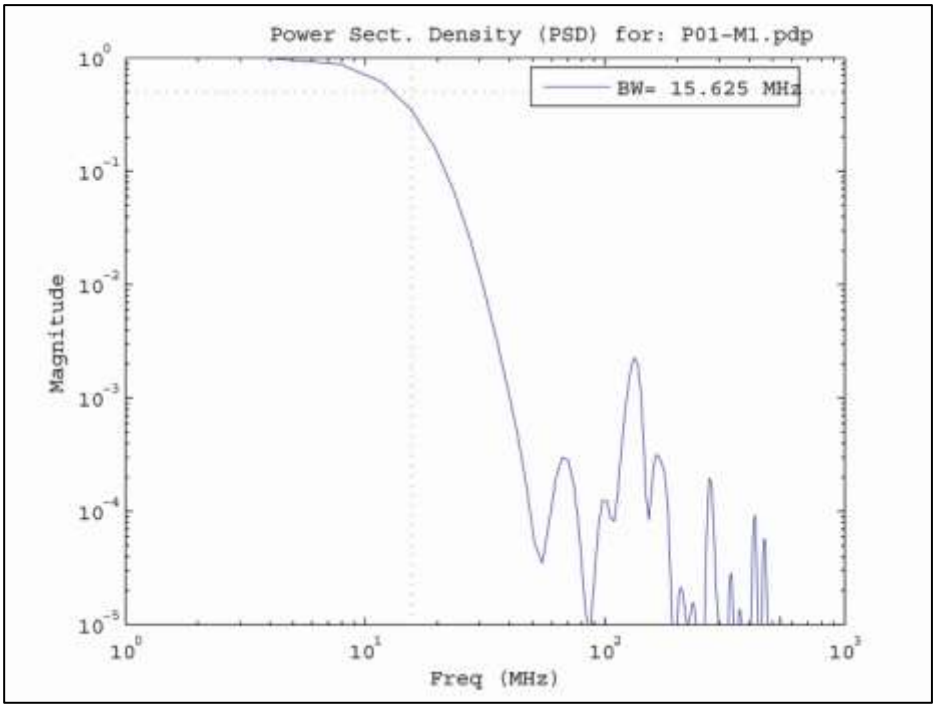


Figure 5.7: Power spectral density

5.3 BIT ERROR RATE

The channel models produced in previous section are used in simulation codes using MATLAB to evaluate bit error rate of the wireless links that used different signal formats. Existence of ISI caused by multipath effect restricts achievable BER. This phenomenon introduces what is generally known as BER floor level where pumping more signal power into channel does not improve the performance. This situation is also valid for HADEED measurements. There are two steps in simulating performance using measured channel models. The first step estimates (symbol error rate) SER caused by ISI for noise-free channel with different data rate. The second step is to add AWGN to received signal and compute BER for different PSK, and QAM modulations.

Defining **data rate** at the beginning is important in comparing performance of modulation schemes in the presence ISI. Starting with same bit rate gives fair comparison between different modulation schemes. Bit rates used are: 100Kbps, 500Kbps, 1Mbps, and 3Mbps. These values are close to the data rate speeds usually used in most of the applications in industrial wired networks. Flow chart for the MATLAB code is sown in Figure 5.8 and results for the seven selected channels are displayed in Appendix-C.

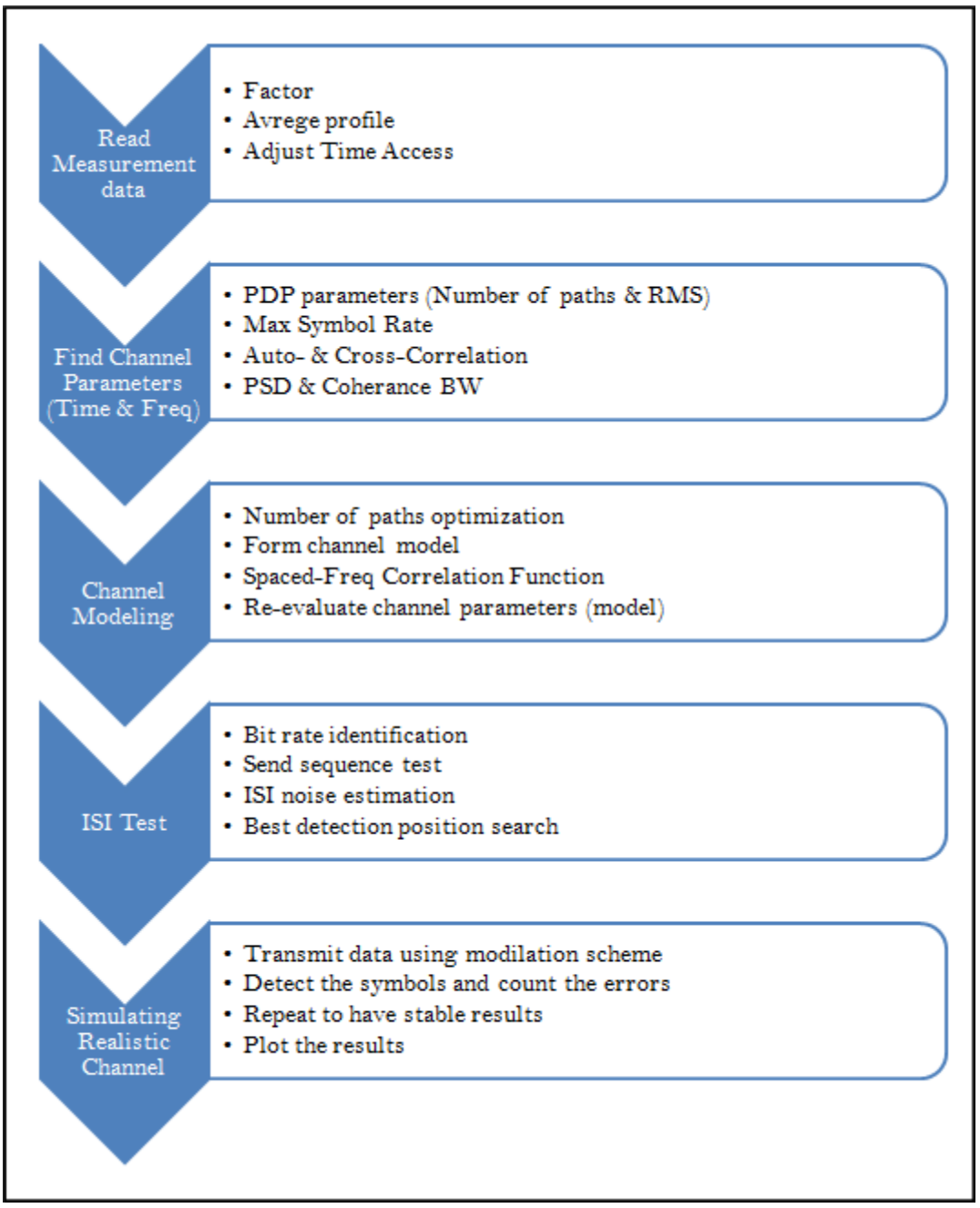


Figure 5.8: Flow chart for MATLAB program

5.3.1 STEP 1: ISI TEST

In **fourth stage** of deign, symbols are transmitted through measured channel CIR without adding AWGN noise. Purpose of this step is to identify optimum detection time instance that achieves lowest number of errors in presence of ISI. The MATLAB code algorithm is given in Figure 5.9.

To do that, detection position search begins at zero delay and ends at the end of first symbol of last path in CIR. In other words, iterative steps in program are defined to start at zero step and end at last step which is the sum of maximum excess delay step pulse symbol duration. This is done using the channel model as steps of sampling time, see Figure 5.10 and Figure 5.11. Detection position array is selected in order to cover all possible combination of paths with respective delays. Then, for individual path, required delay shift is calculated in terms of number of symbols. Afterward, all weighted paths are added corresponding to path delays. Sum of amplitudes for paths that hold targeted symbol represents the signal portion in SNR. On the other hand, sum of amplitudes for paths that hold other symbols represents ISI noise portion in SNR which provide a way to estimate the SNR in presence of ISI.

This process is repeated with changing detection position to next sampling slot until the end of detection position array. Optimum detection position is identified which has minimum ISI noise. If more than one minimum is found, selection is done for the position that is located in the middle of longest detection positions stream of those minimums. This optimum detection position is used in BER estimation with AWGN channel verses SNR.

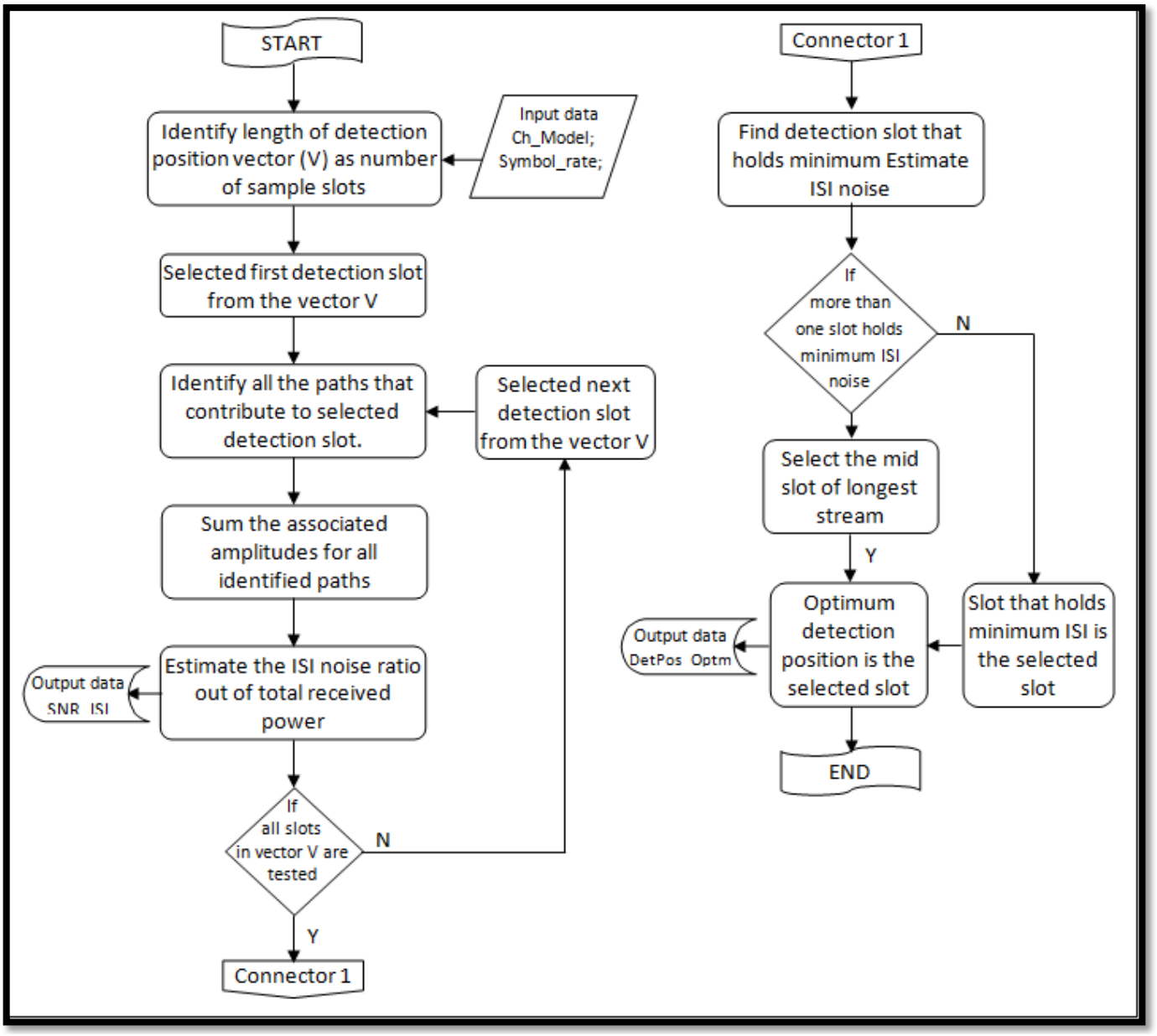


Figure 5.9: Algorithm of MATLAB program for ISI test step

To explain the algorithm again, two examples of different situations are shown below. First example is shown in Figure 5.10, when $\boldsymbol{T_s > \tau_{max}}$. Second example is shown in Figure 5.11 when $\boldsymbol{T_s \leq \tau_{max}}$. Both figures use the same symbol rate, i.e. number of samples per symbol. Channel model used has four paths with amplitudes as shown in first column. Similar channel model is used in both cases with

only one difference which is that last path is delayed in second example by 5 samples instead of 4 samples. If the decision is made on samples that lay during the symbol overlap period; errors cannot be avoided because of severe ISI. If symbol rate is slow enough, ISI problem can be mitigated by selecting the optimum detection time where there is no overlap or minimum of overlap between symbols.

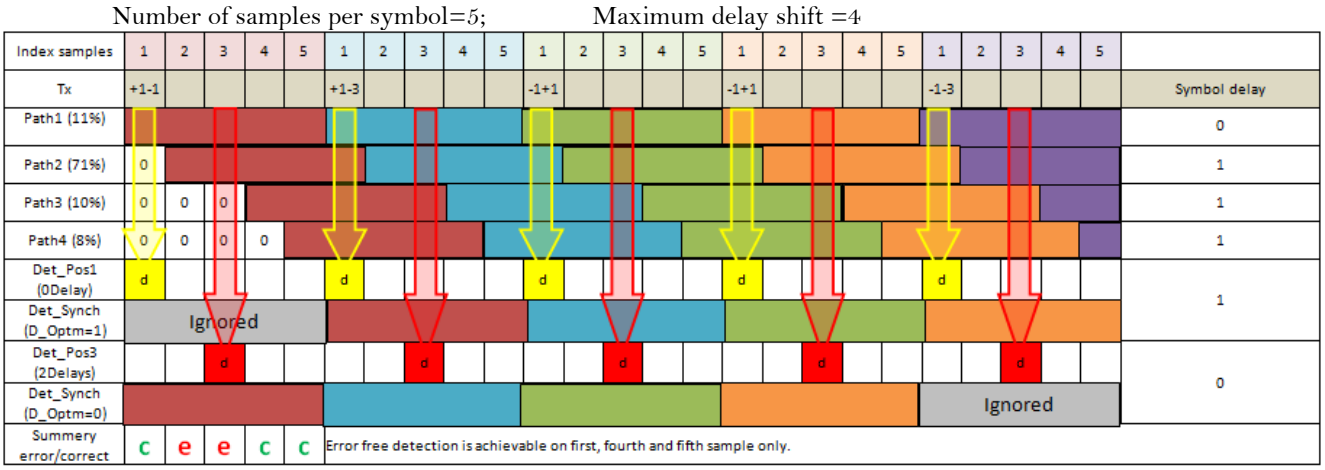


Figure 5.10: ISI test example table for $T_s > \tau_{max}$ (max excess delay)

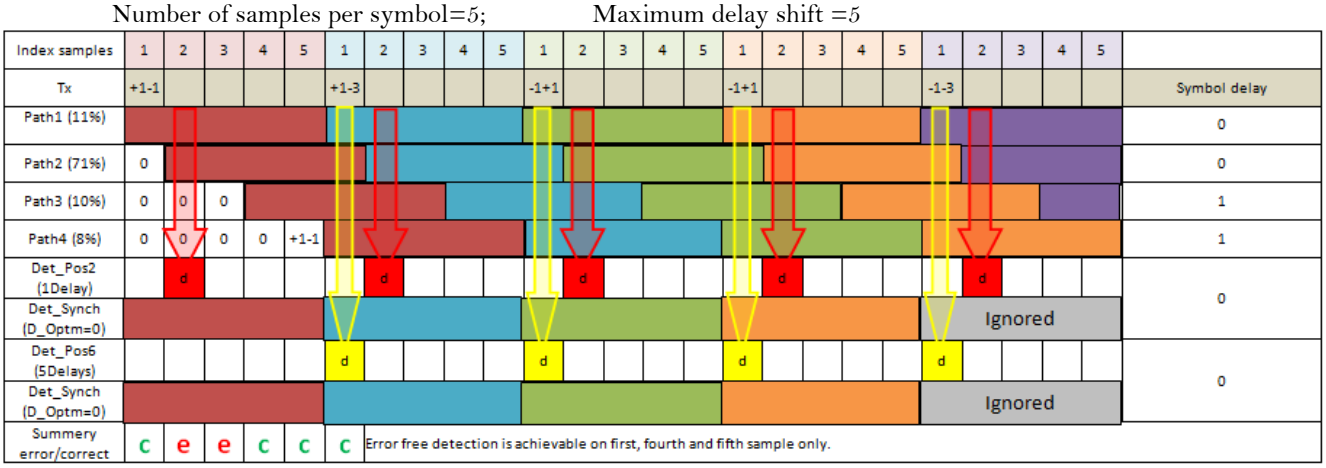


Figure 5.11: ISI test example table for $T_s < \tau_{max}$ (max excess delay)

5.3.2 STEP 2: SNR TEST

QoS of digital system wireless is defined by the BER, and the BER for different modulation schemes depends on SNR. In the **fifth stage**, the performances of the following modulation schemes are evaluated: BPSK, QPSK, 8-PSK, 16-PSK and 16-QAM. Using equations given in Section 4.1.1, theoretical BER can be calculated for those modulations, i.e. equations (4.10), (4.12), (4.13), and (4.14). Building on previous acquired CIR results, simulation experiments of these modulation methods on the measured channels can be completed. AWGN effect is also included. Channel models from Section 5.2, and optimum detection position from Section 5.3.1 are used as input for this communication system simulation. The MATLAB code algorithm for simulating the channel performance in this stage is given in Figure 5.12.

The simulation structure is build based on Monte Carlo simulation method. In MATLAB, data bit rate is initially defined which is converted to symbol rate after selecting the applicable modulation scheme. Then, program derives a channel model from the measured CIRs that covers 80-95% of total signal power. After that, ISI test is performed and delay detection position is optimized at receiver. At this point, all required parameters are available to start realistic channel simulation.

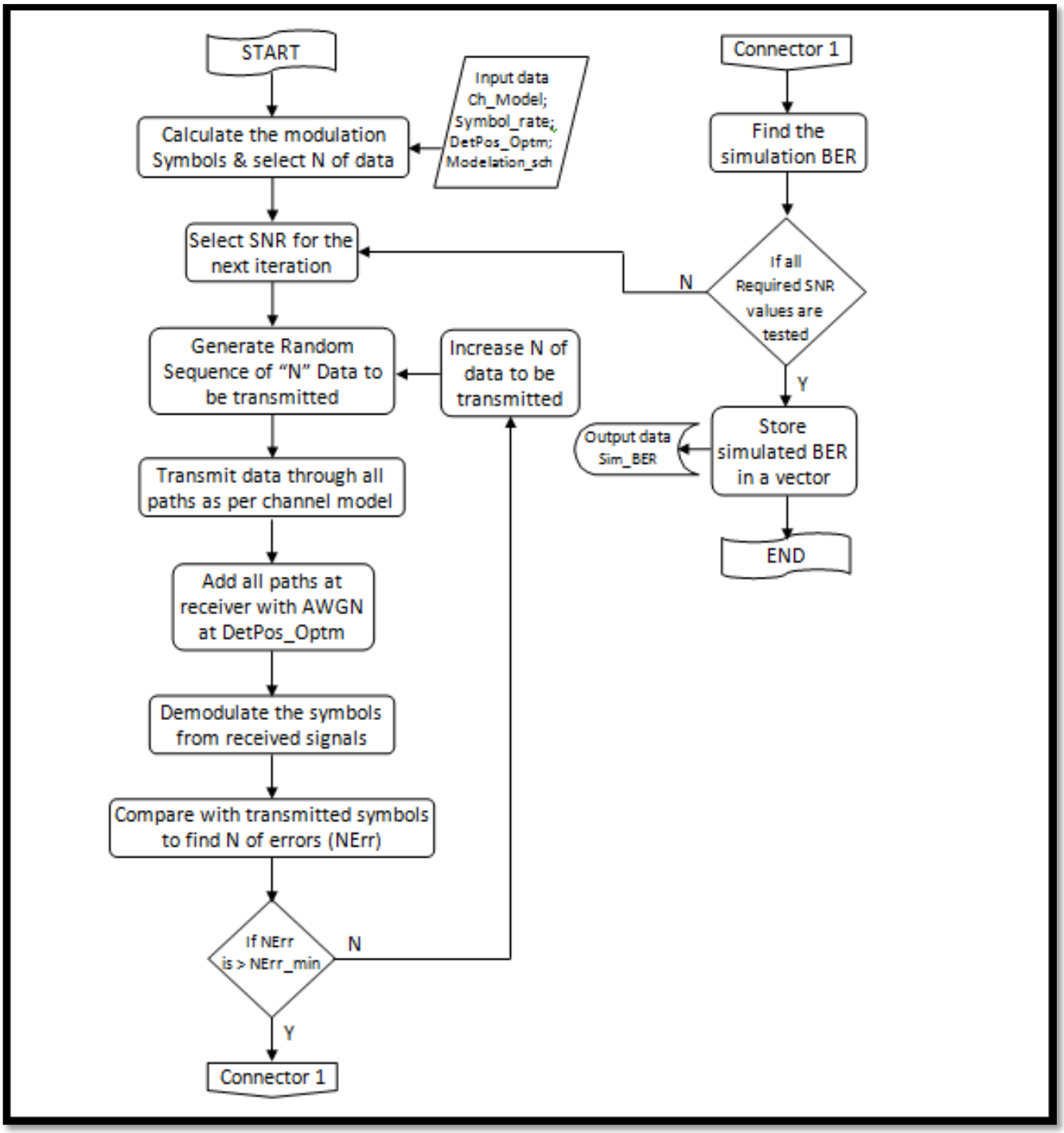


Figure 5.12: Algorithm of MATLAB program for SNR test step

For each simulation a minimum of 100,000 symbol sequence is generated with normalized power of unity. The sequence of generated symbols is transmitted through each path with associated delay and power scaled according to channel CIR model. AWGN sequence is generated and added to the received signal after all paths are summed. Now, at optimum detection position found in ISI test; decisions are taken at identified optimal detection position. Finally, number of errors is counted to find BER. Loop iterations are repeated till achieving defined minimum number of error $\mathcal{E}_{min}$ to ensure statistical reliability of the results.

Same operation is repeated for different SNR's in range of 0dB up to 50dB, depending on modulation scheme used. By doing this, BER verses SNR plots for one modulation scheme for initially defined bit rate becomes available. Similarly plot for all other modulation schemes are obtained. The figure shows BER from 0 to 10^{-5} for all modulation schemes. This is repeated for other bit rates and finally 4 figures are generated for each channel model that explains modulation scheme performance against data rate. BER results for all seven selected channel models are shown in Appendix-C.

Theoretical BER for all modulations without ISI are shown in Figure 5.13 which is used as reference to compare simulation results. Simulated BER results for different modulation formats are plotted on same figure to be able to compare between them. It represents P19-M1 channel model at 3Mbps. Since there is only one path in selected channel model (P19-M1) with zero delay spread, simulation results are very close to theoretical figures. Only at very low SNR, values are not matching because theoretical formulas used are valid for high SNR values only, ($SNR \gg 1$) [56].

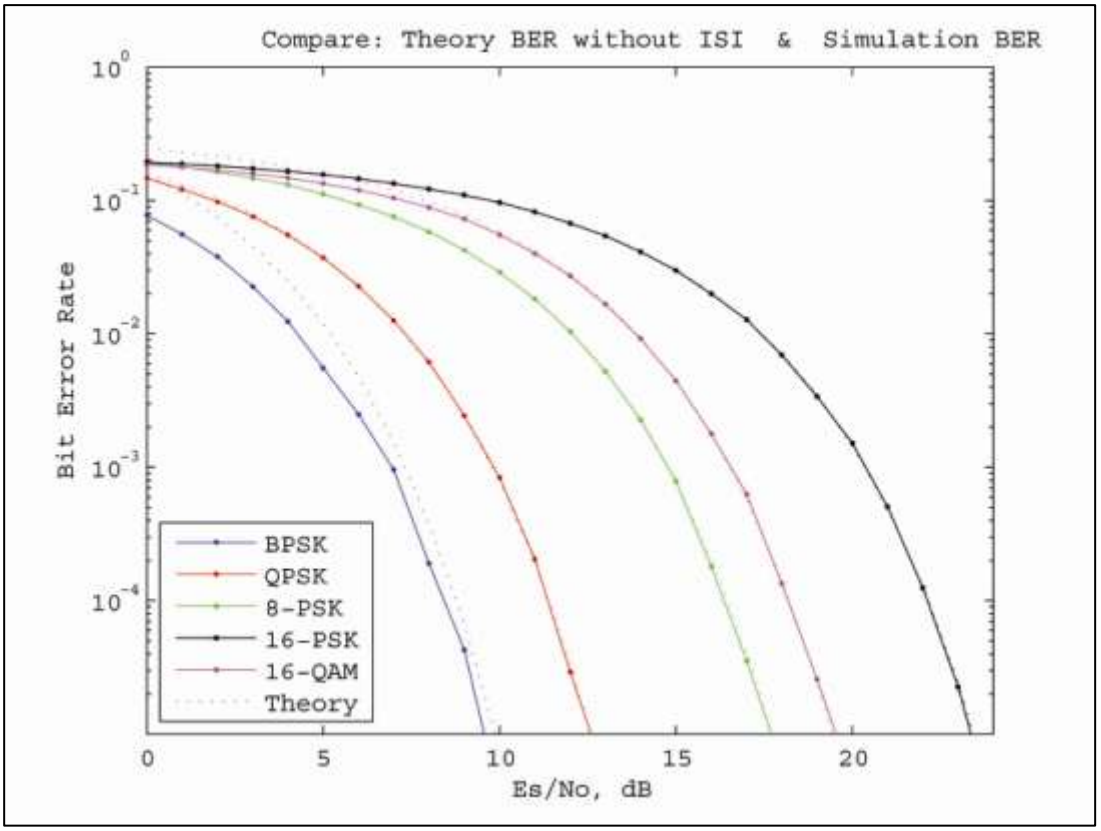


Figure 5.13: Compare simulation results with theoretical BER

The simulation is done to achieve statically meaningful results with minimum number of errors ($\mathcal{E}_{min}$) equals to 20. However, when the channel behavior is good, the simulation time was observed to be too long as error rate was low particularly at higher signal to noise ratio. In this situation number of errors was adjusted to run the simulation with reasonable simulation time. CIR was simulated for all modulation schemes up to BER of 10^{-5} to have better plots for comparison. Summary of those results, for only 3Mbps speed, are in Table 5.5 where deviations from theoretical BER at 10^{-5} are presented.

Table 5.5: Summary of simulation BER deviation at 3Mbps rate

Data File Name	SNR for Theoretical BER	Deviation from Theoretical SNR [dB]						
		P01-M1	P04-M1	P07-M1	P09-M1	P19-M1	P15-M1	P15-M2
BPSK	10	8	5	2	12	0	0	0
QPSK	13	0	0	0	1	0	0	0
8-PSK	18	0	0	0	0	0	0	0
16-PSK	19	0	0	0	0	0	0	0
16-QAM	24	0	0	0	0	0	0	0

Some learning observations are highlighted here. ISI noise effect appears with higher data rate relatively compared with available channel bandwidth. For 0.1 Mbps bit rate, all channels were showing ideal BER behavior, i.e. locked with theoretical figures without ISI. Once date rate increases, ISI effect becomes clearer by reducing BER performance, like in P01-M1 for 3Mbps. In Table 5.4, the calculated maximum symbol rate is matching with BER devotion results @ 3Mbps speeds. $R_{s_{max}}$ for P01-M1, P04-M1, and P09-M1 are less than 1Mbps which cause bad behavior for 3Mbps simulations.

Higher levels of modulation schemes, e.g. 8-PSK, 16-PSK and 16-QAM, are less sensitive to ISI noise as per the results up to 3 Mbps speed. This is reasonable since their symbol rates are slower than lower levels of schemes which provide larger spaces in time axis between successive transmitted symbols.

BPSK works worst than QPSK in P01-M1, P04-M1, P07-M1, and P09-M1. P01-01 results, for instance, show that BPSK requires the minimum SNR performance for bit rates ranging between 0.1-1Mbps. However, QPSK achieved better performance for 3Mbps. This result is expected since theoretically calculated $R_{s_{max}} = 1.03\ Msps$ for this channel model as calculated before, see Table 5.4. Thus,

symbol rate $R_{s_{BPSK}} = R_b = 3.0\,Msps$ is more than maximum allowed symbol rate for this channel model. Physically, the reason is that 3 Mbps rate causes high ISI errors in BPSK since number of samples per symbols becomes selectively low (25 slots) compared to maximum delay caused by channel (62 slots). This causes greater interference between the two successive received symbols.

Similarly, ISI harsh effect appears on measurement P09-M1 with $R_b = 3.0\,Msps$ plot, because its $R_{s_{max}} = 0.91\,Msps$ which is less than used bit rate. ISI harsh effect disappears or decreases with measurement P07-M1 where $R_{s_{max}} = 8.61\,Msps$ with QPSK modulation. QPSK is not affected because its $R_{s_{QPSK}} = \frac{1}{2} R_b = 1.5\,Msps$ which is within channel maximum data rate.

To show the effect of ISI test stage, where best detection position is identified, simulation results are plotted for same system, channel model P01-M1, with and without this test as shown in Figure 5.14. It is very clear that very large amount of energy can be conserved to achieve similar BER.

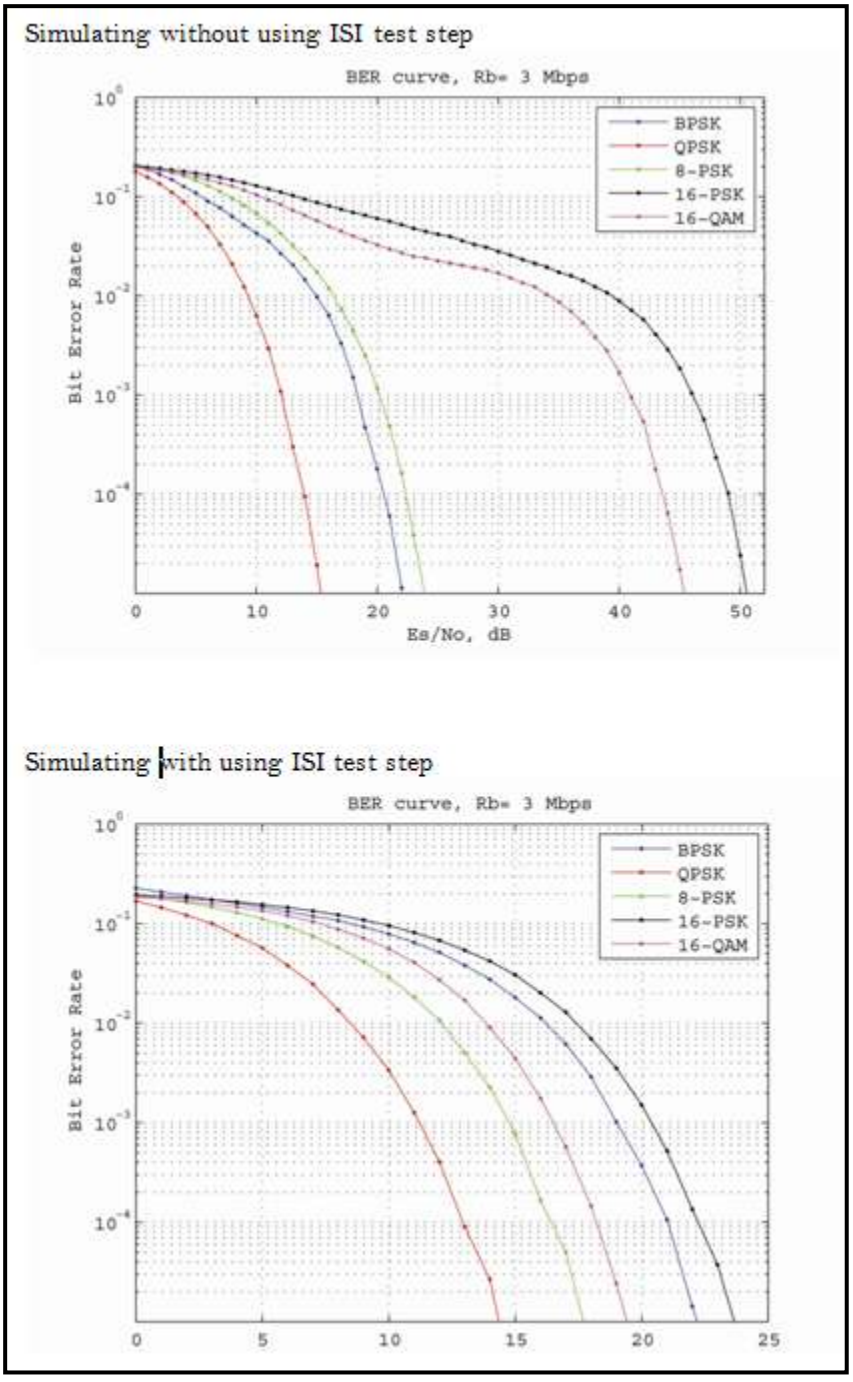


Figure 5.14: Comparing Simulation results with/without ISI test

Measurement P09-M1 provides worst SNR performance to achieve same BER. This is because its channel model has maximum RMS delay and largest number of paths. This channel model is simulated again but using higher bit rates till 16Mbps where all modulation schemes face flat fading. This step provides understanding of difference between modulation schemes performance in presence if ISI noise. This channel (P09-M1) is simulated using 6, 8 12 and 16Mbps speeds, see Figure 5.15.

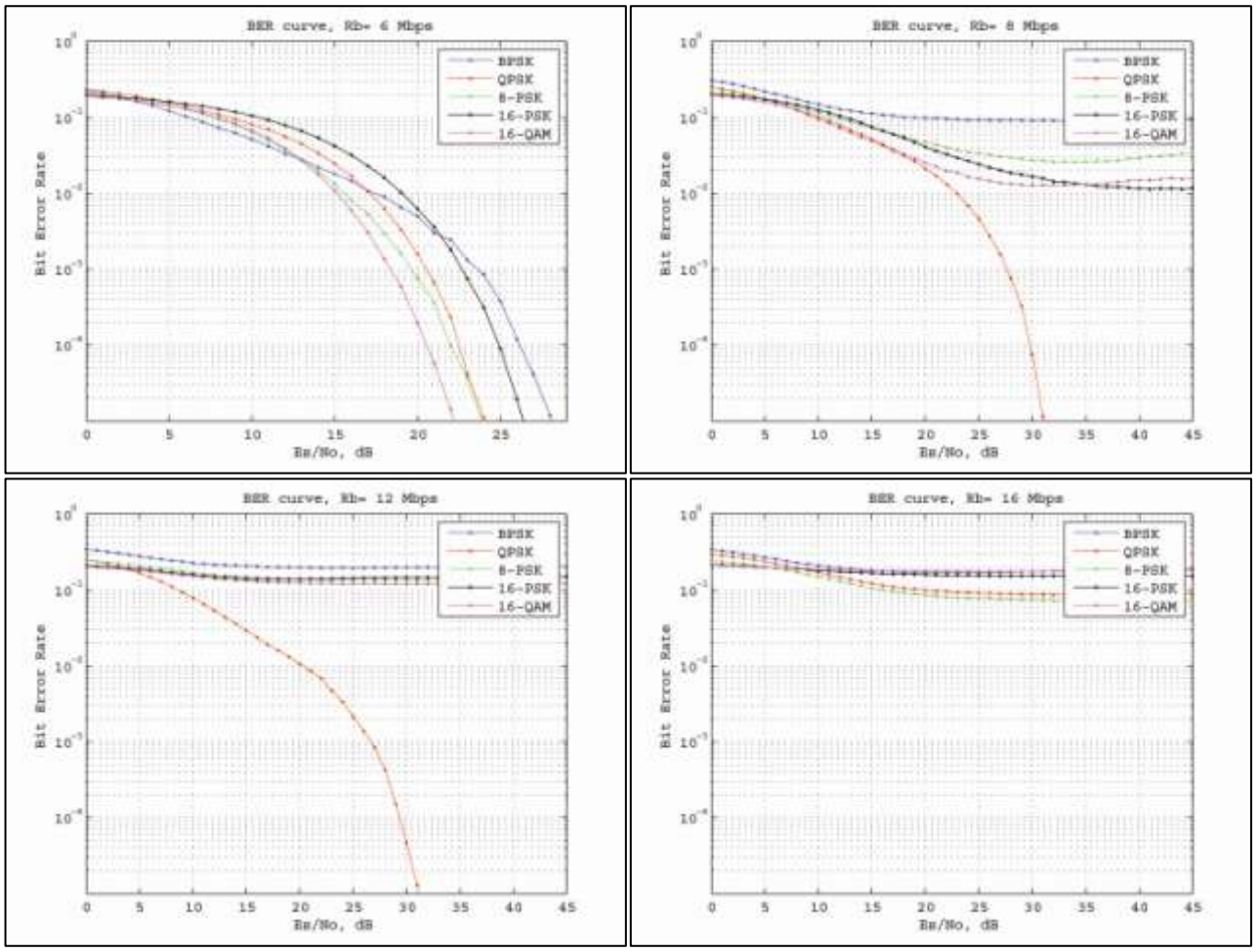


Figure 5.15: Simulation results for higher bit rate for measurement P09-M1

6

CONCLUSION AND DISCUSSION

This research combines three major phases: wired industrial network characteristics; assessment of wireless technologies; and industrial wireless channel sounding. Jointly all three give a deeper understanding on the design of wireless networks for industry.

In **first phase**, understanding of the characteristics of wired network used in industries are achieved by identifying the key performance indicators for highlighting opportunities for improvements in design of wireless systems. The most important twelve attributes (KPI) for future industrial wireless network are: *Data Rate*, *Device Range*, *Reliability*, *Availability Resilience*, *Network Latency*, *Throughput*, *Security*, *Power Consumption*, *Network Topology*, *Number of Devices*, *Medium Accessing*, *Operating Frequency*, *Complexity*, *Scalability*, *and Flexibility*.

In **second phase**, the most widely spread wireless technologies, Bluetooth, ZigBee, Wi-Fi and SP100, based on IEEE standard (WPAN & WLAN), are assessed to provide state of knowledge that currently exists. IEEE802.15.4 based technology (e.g. ZigBee) is recommended and can be selected as the best suitable technology

available up to date for industrial sensor networks. Mesh topology increase the system reliability because of alternative paths become available. Short duty cycle minimizes power consumption drastically and the need to attend frequently for battery replacement is reduced. ZigBee satisfies the industrial requirements of data rate, reliability and security with minimum power consumption, reasonable complexity, scalability and flexibility provided by the mesh topology that result in acceptable network latency. Bluetooth does not support mesh networking that limits the number of devices and system reliability. Whereas the Wi-Fi (WLAN technology) is delivering network speed much more than industrial sensor network requirements but number of devices, power consumption and security restrict the technology usage in sensor networking.

In the **third phase**, characterizing heavy industrial wireless channel, Hot Strip Mill as an example, with channel sounding systems can give a good picture of wireless channel in an industrial environment which is essential for design stage. In Master Network type, it is recommended to use IEEE802.11 base technology because of high data rate requirement. Whereas in Sensor Network type, IEEE802.15.4 base technology fits better because of higher reliability due to mesh topology; good low power profile; and controlled network latency requirements.

With two phases of experiment inside Hot Strip Mill in HADEED including total of 4 sessions, 23 measurements were completed. The use of modern wideband sounding system with Omni-directional antenna at 1.8 GHz leads to test many experiment setup parameters like: AGC, vertical/horizontal POL, presence/absence of LOS path, etc.

Measurements show that channel variation with time is very small and can be neglected. This result is valid since almost all devices in plant are fixed and temporal variation in channel can be neglected.

Design part is divided into stages. In **first stage**: channel link budget is calculated for path loss differences between gathered location data. Approximate estimation is done for channel path loss exponent that is in range of 3.0 for VPOL and 4.0 for HPOL. Also, configuration of plant contour effect on channel performance is shown clearly in results.

In **second stage**: power delay profile parameters are calculated for each measurement. They are: number of paths, maximum excess delay, the mean excess delay, RMS delay, maximum symbol rate, and coherence bandwidth. Maximum excess delay for selected plant is high, i.e. in range of 900 ns for HPOL and 140 for VPOL, compared with results shown in literature which is in range of 200-300 ns. Plant overall estimation for those parameters assures that 3Msps speed can be reached without need of equalizers. VOPL antenna provides less number of paths and delay spread than HPOL antenna.

In **third stage**: model of measured CIR is design for selected points through optimization process for the highest significant taps. The realistic channel models are designed using MATLAB program with optimized number of paths.

In **fourth stage**: using the realistic channel models, ISI due to time dispersion is tested to get best detection position. For ISI test, there are two different situations $\boldsymbol{T_s > \tau_{max}}$, and $\boldsymbol{T_s \leq \tau_{max}}$. If detection done on samples taken during the period overlapping symbols; errors are not be avoided due to ISI. If symbol rate is

slow enough, ISI problem can be avoided by selecting the optimum detection time where there is no overlap between symbols. Optimum detection position is found to be at center of longest stream of zero error indices. Simulation results show a huge performance improvement for the same channel over the results done without ISI test to locate optimum detection position.

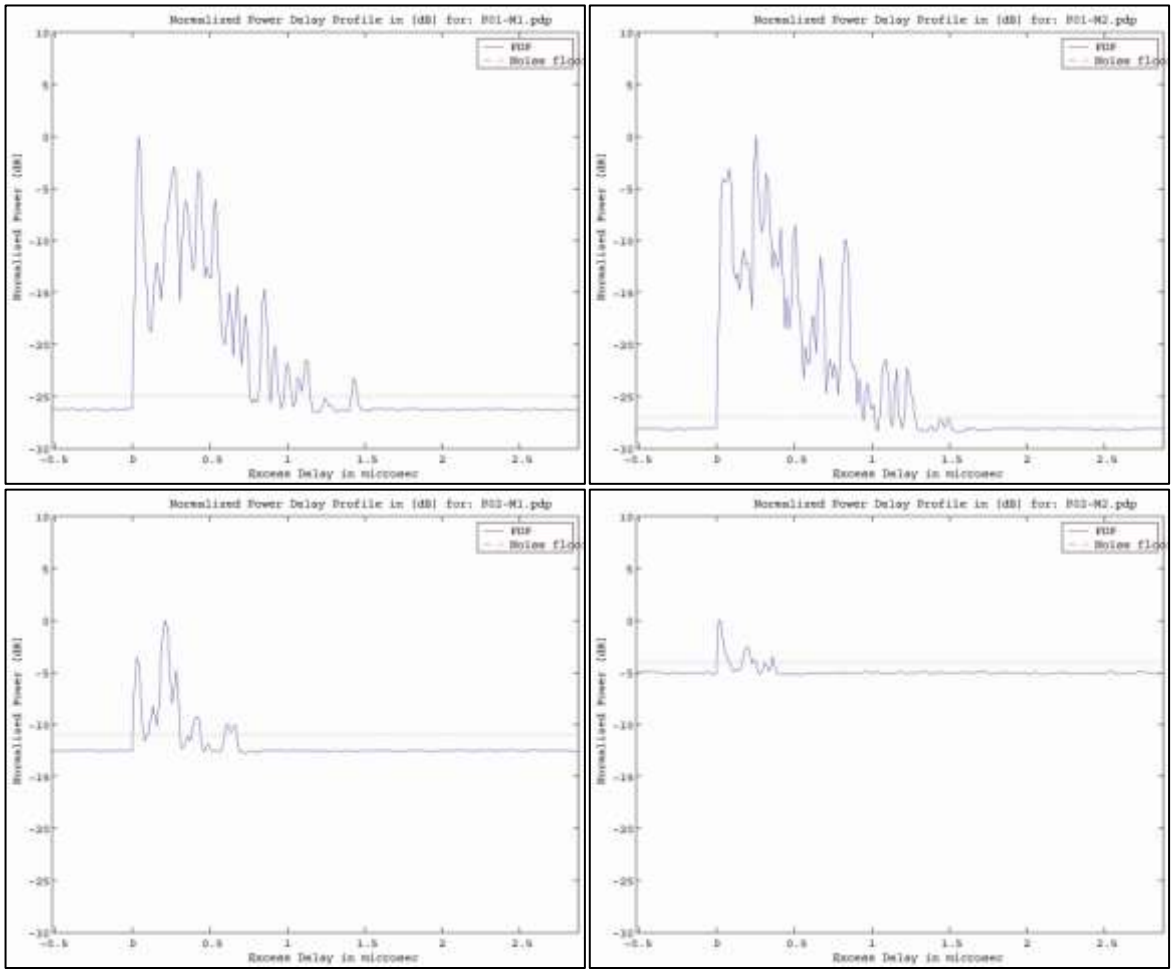
In **fifth stage**: bit error rate is simulated for the measured channel models using: BPSK, QPSK, 8-PSK, 16-PSK and 16-QAM modulation schemes. Results for simulated BER which include ISI effect of realistic channels are compared with theoretical AWGN BER. QPSK result is better for 3Mbps in some experiments because symbol rate is slower than max channel rate which is for BPSK. Another important point to note is that multilevel modulation schemes are more sensitive to ISI because of reduced distance between constellation points.

Yet, these primary data rates can be increased with deployment of diversity techniques, coding strategies or equalization techniques. Also, applying rake receivers can improve QoS of the channel significantly. Still, industry analysts are forecasting an accelerated growth in the use of wireless network technologies in industrial environment over the next few years!

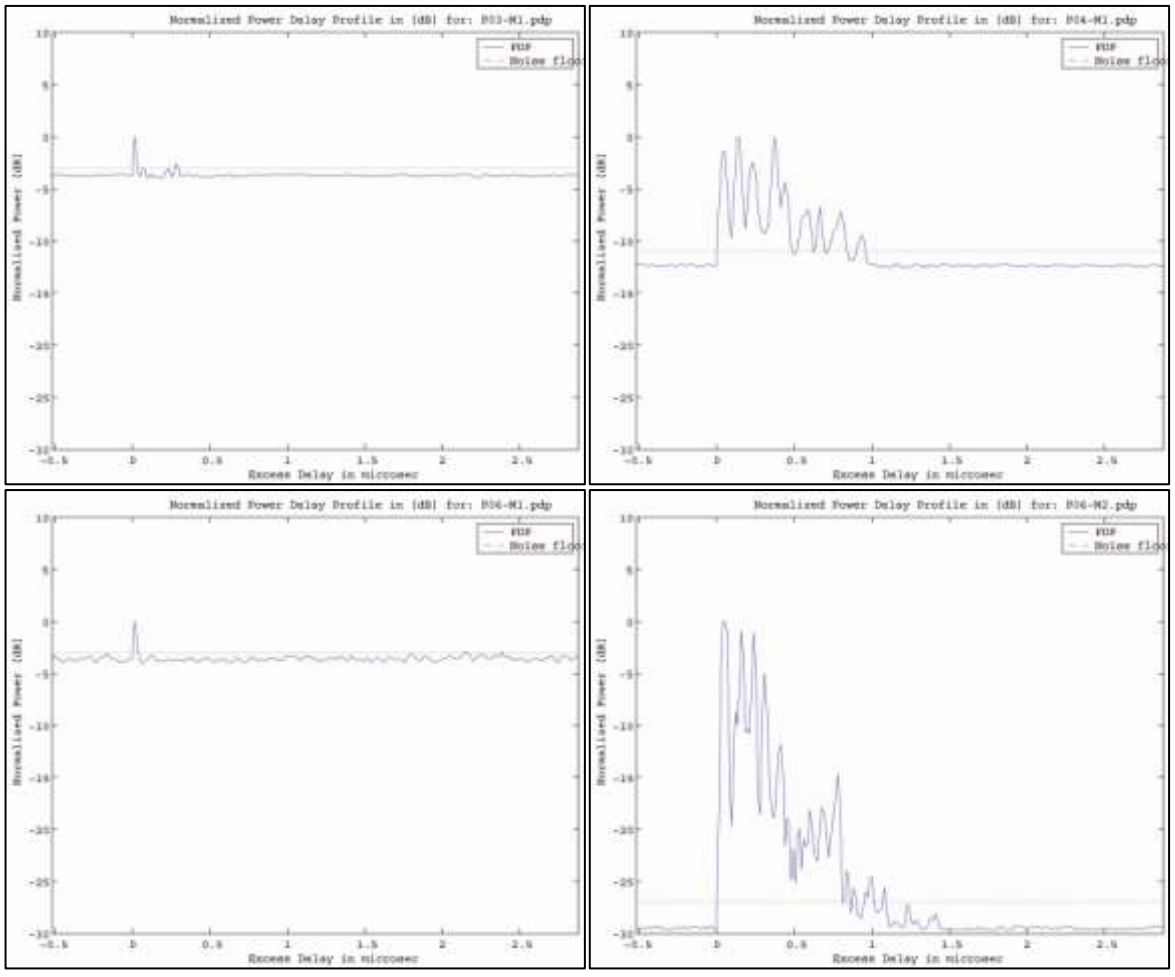
APPENDIX-A

POWER DELAY PROFILES

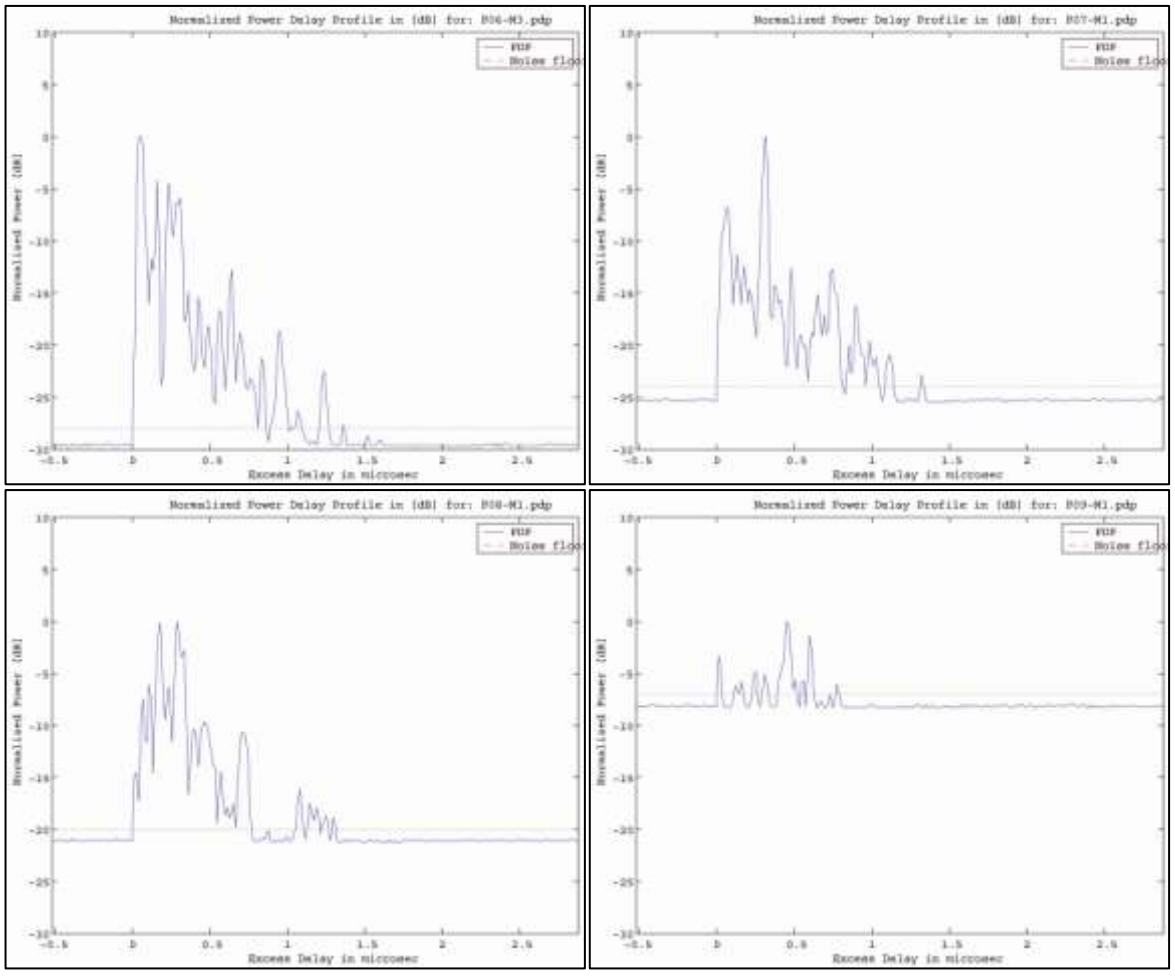
For Measurements P01-M1 to P02-M2



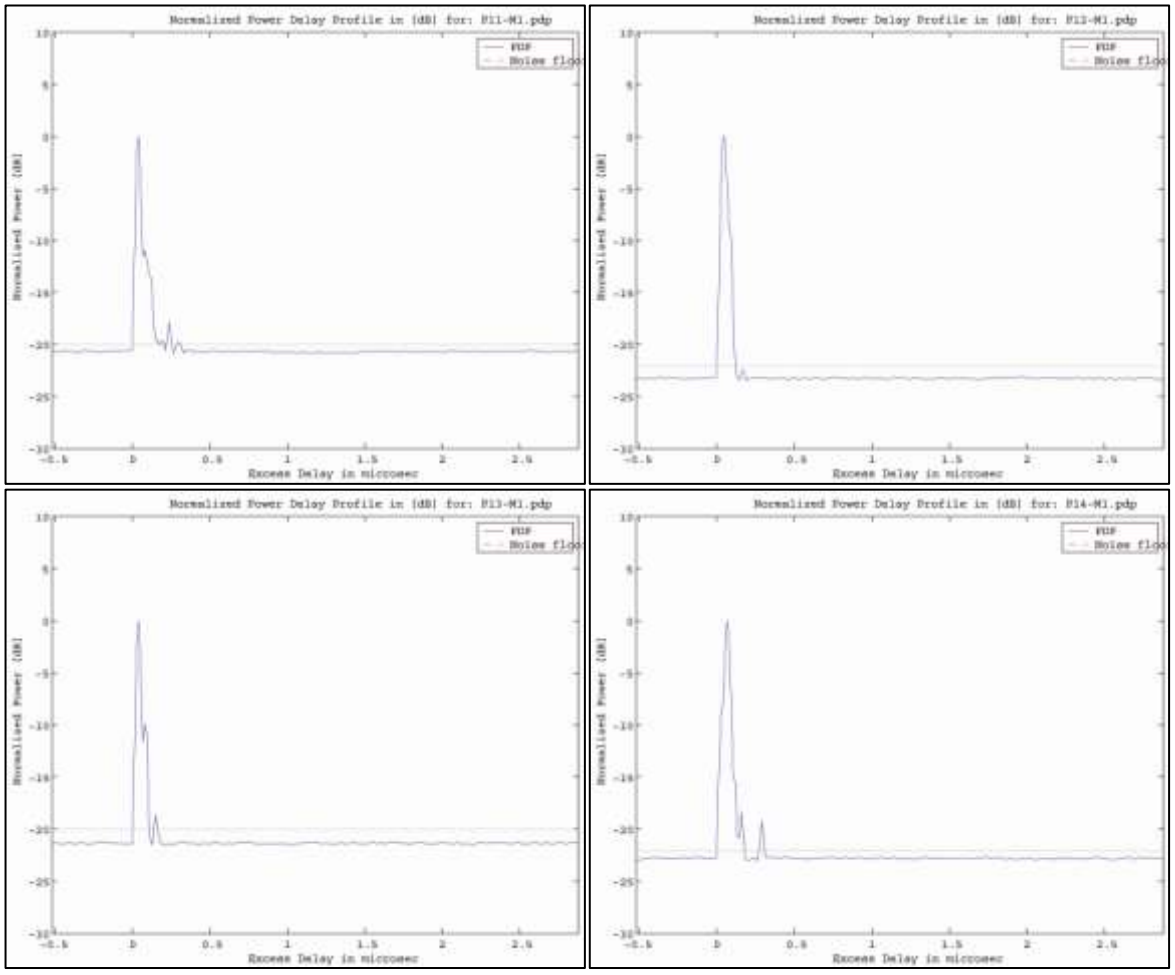
For Measurements P03-M1 to P06-M2



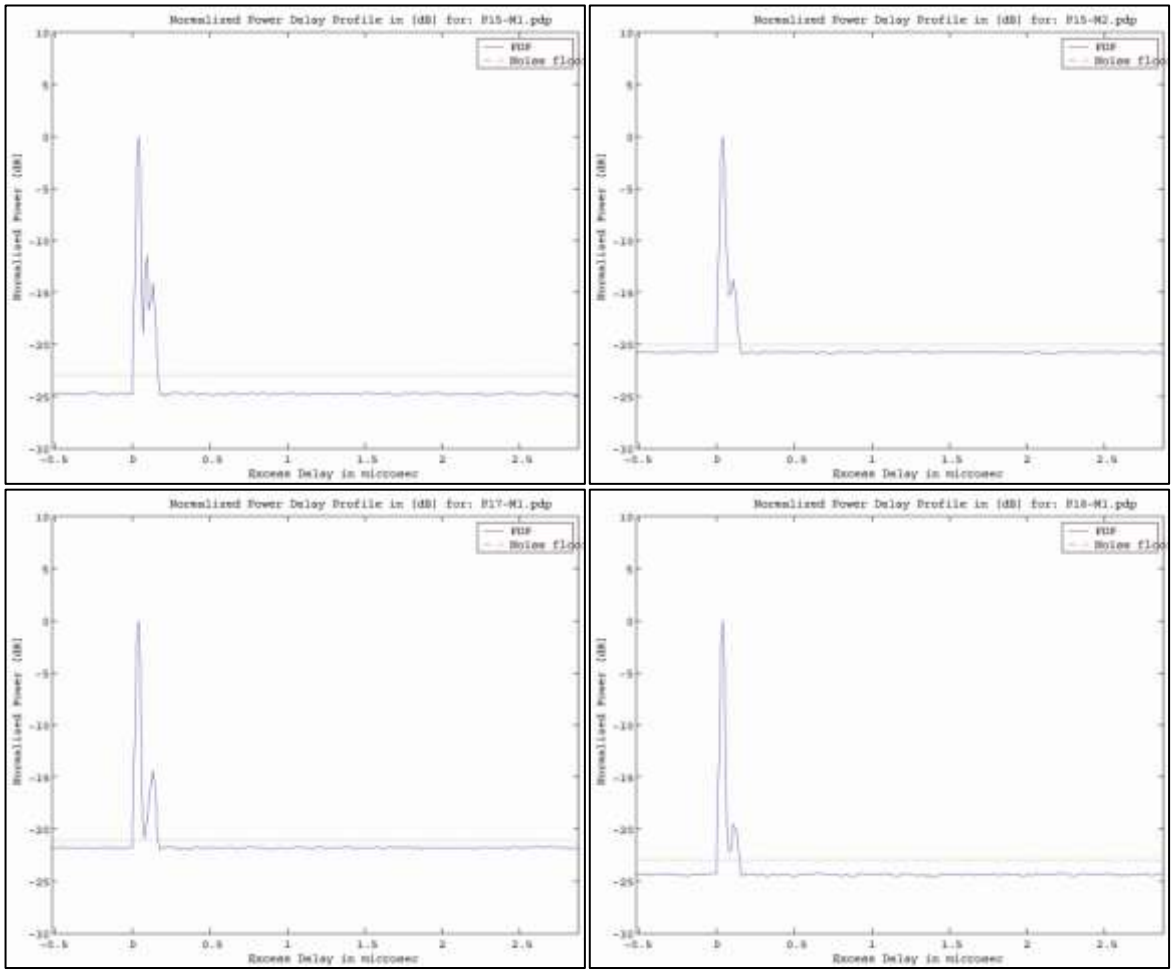
For Measurements P06-M3 to P09-M1



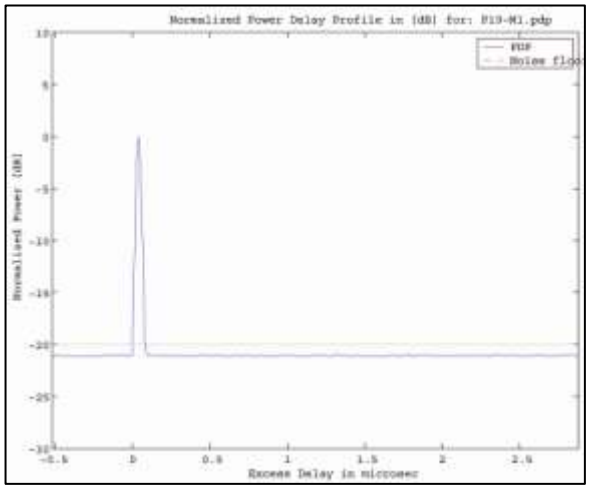
For Measurements P11-M1 to P14-M01



For Measurements P15-M1 to P18-M01



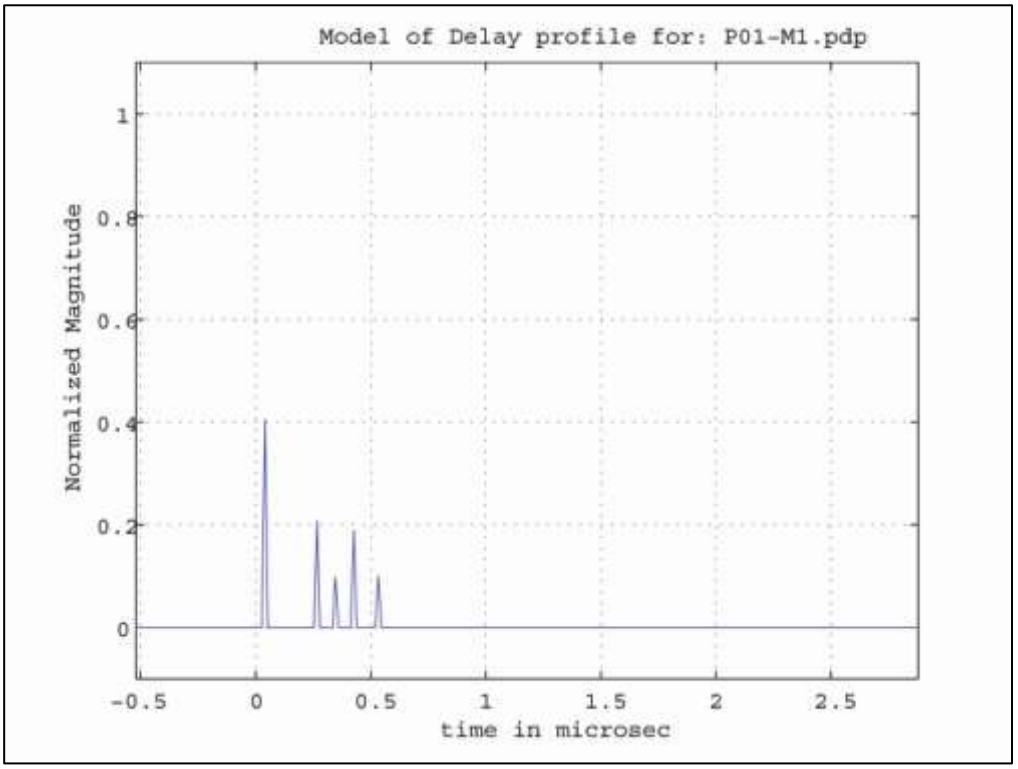
For Measurement P19-M1



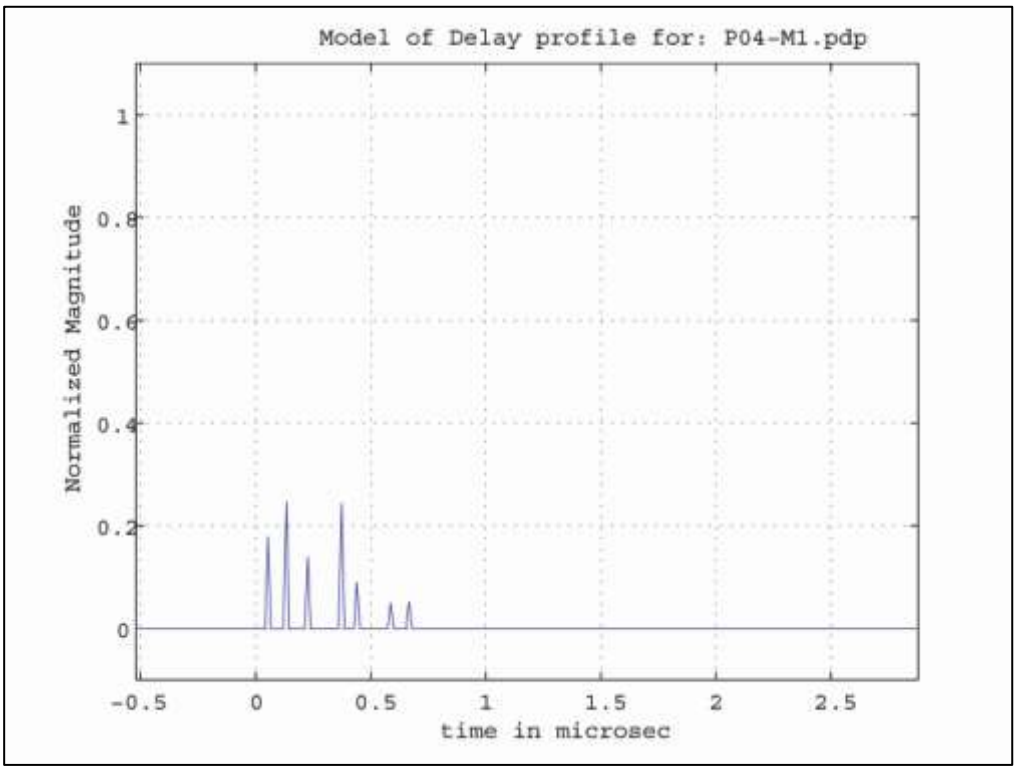
APPENDIX-B

CHANNEL MODELS

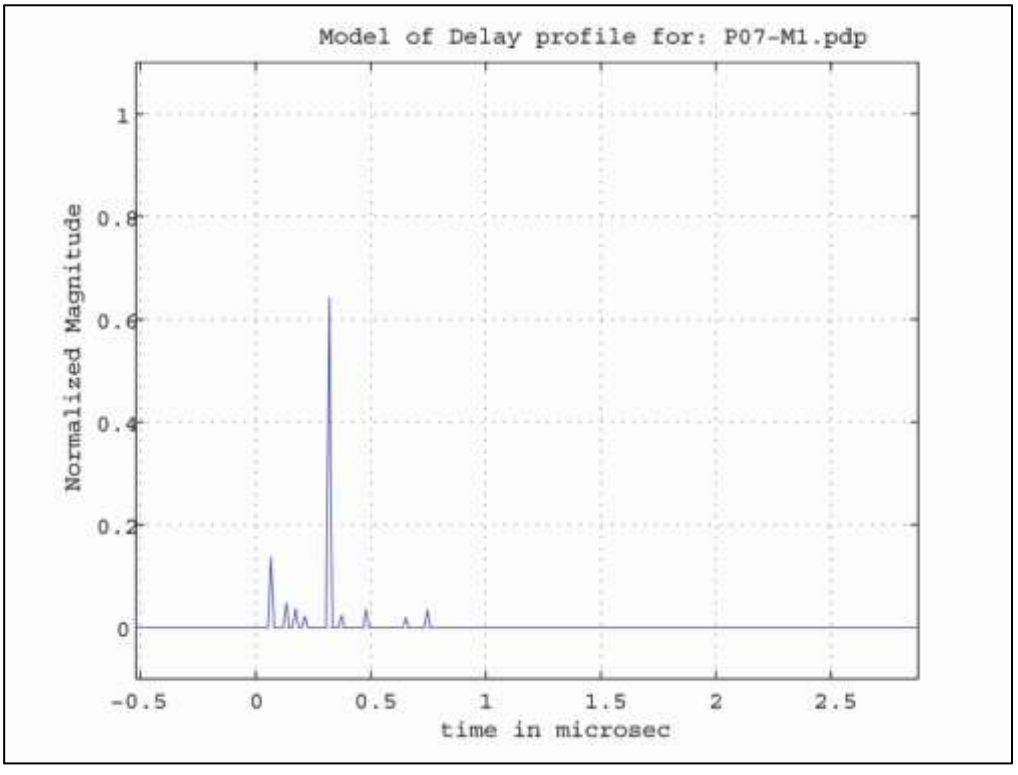
For Measurement P01-M1



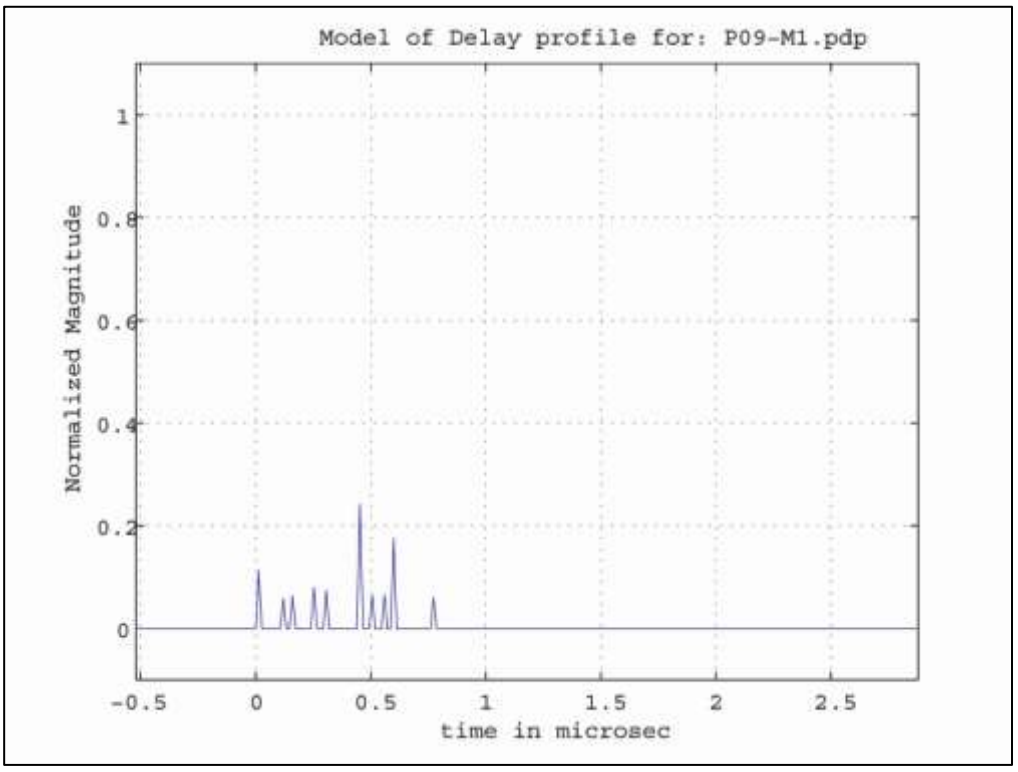
For Measurement P04-M1



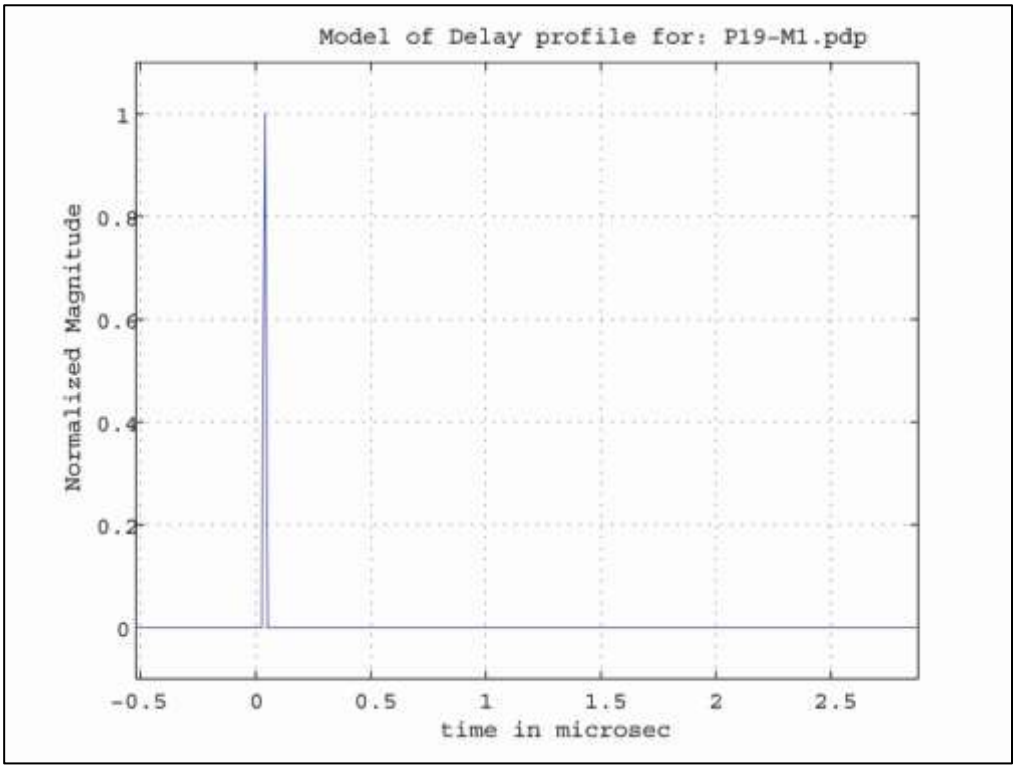
For Measurement P07-M1



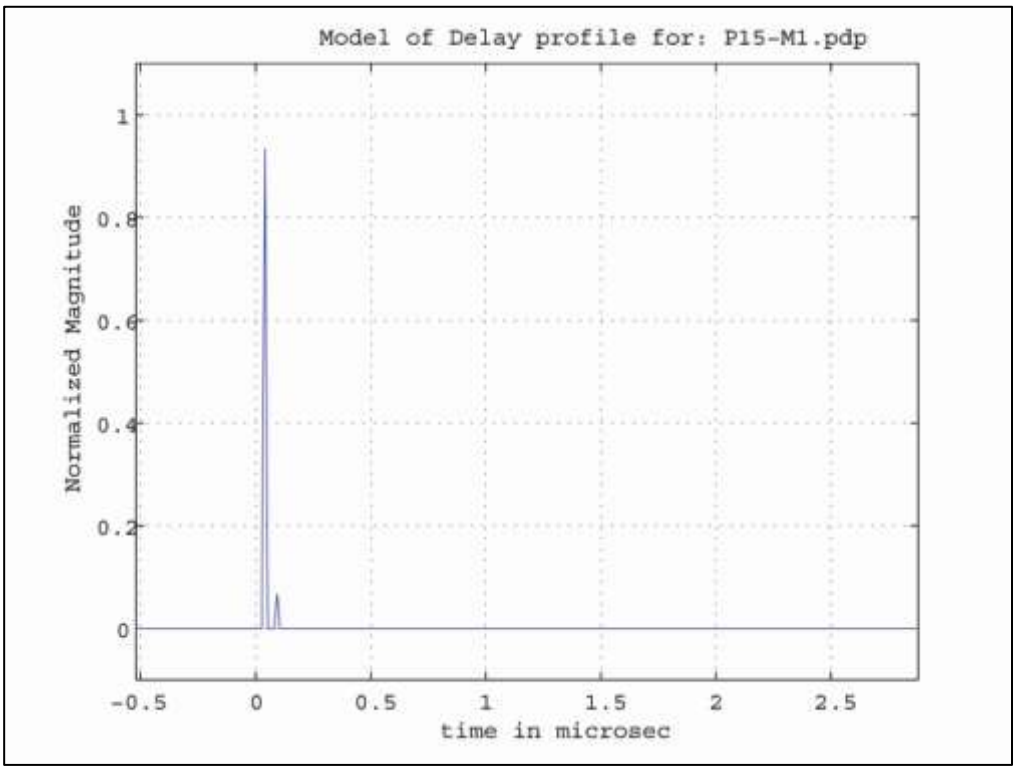
For Measurement P09-M1



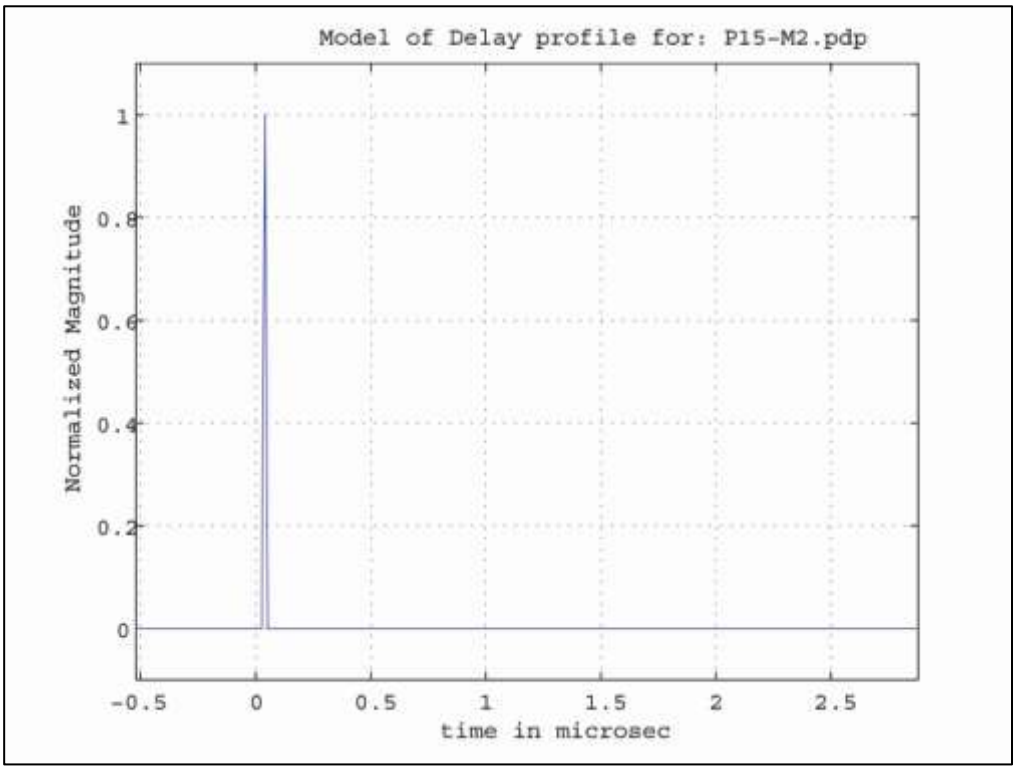
For Measurement P19-M1



For Measurement P15-M1



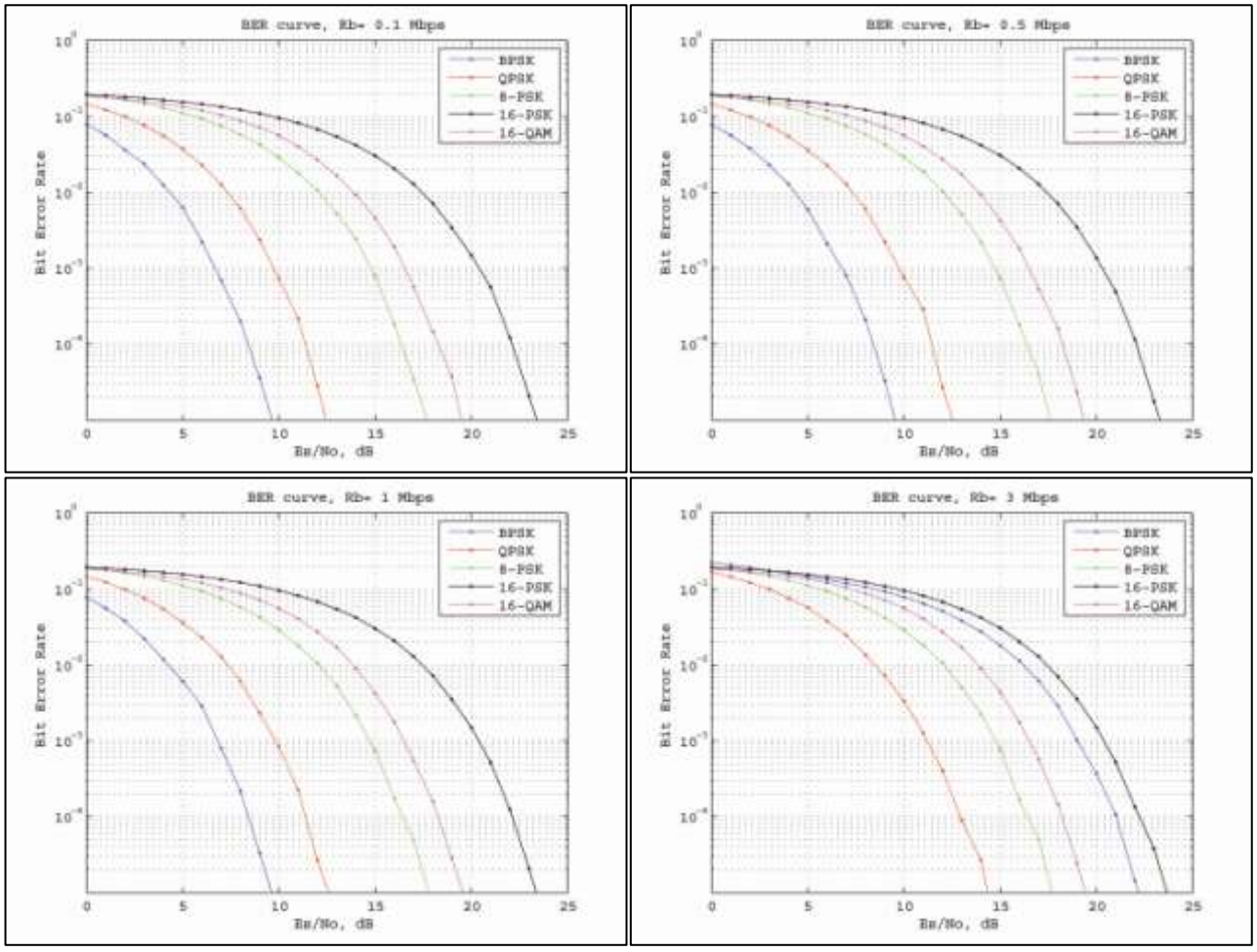
For Measurement P15-M2



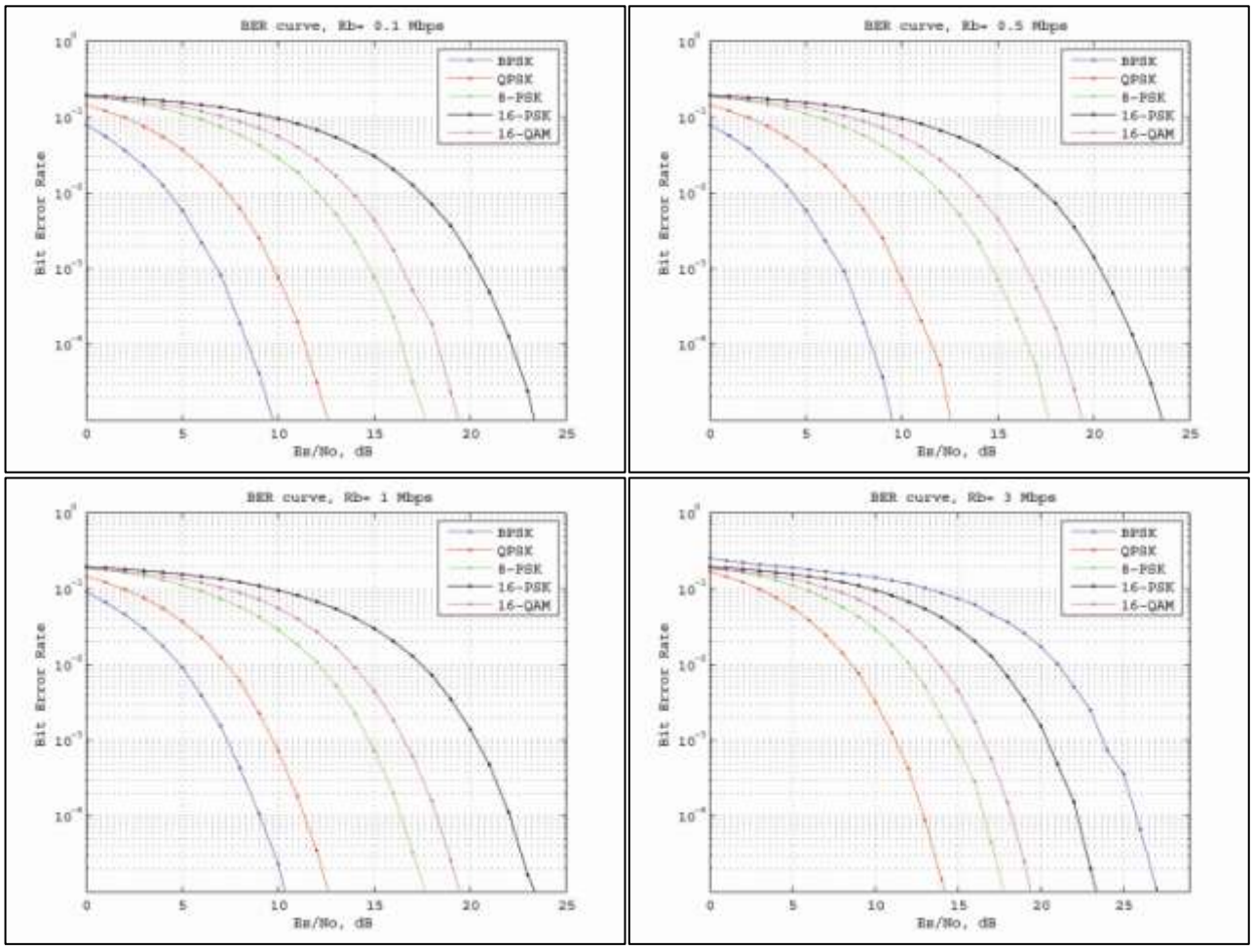
APPENDIX-C

BIT ERROR RATE FIGURES

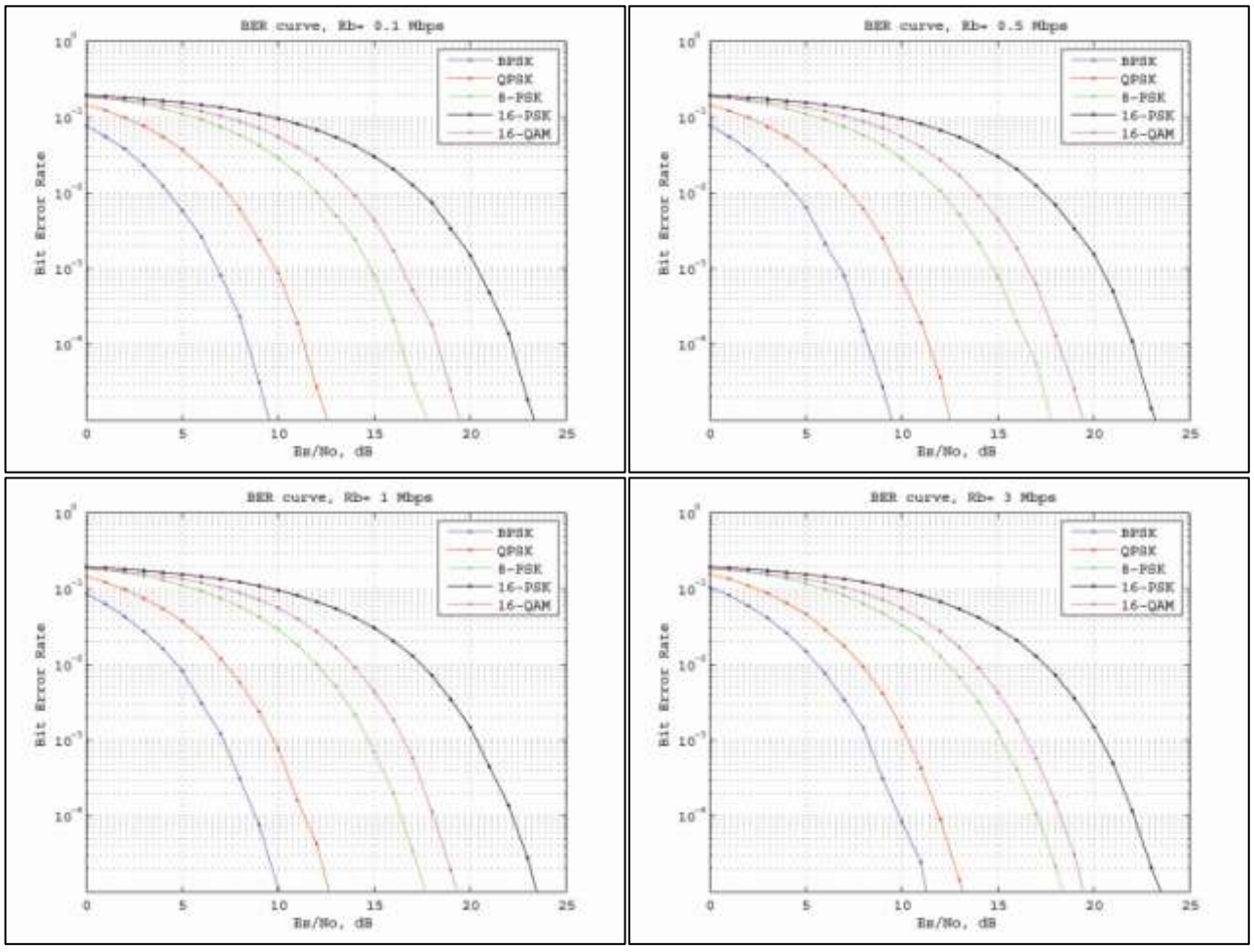
For Measurement P01-M1



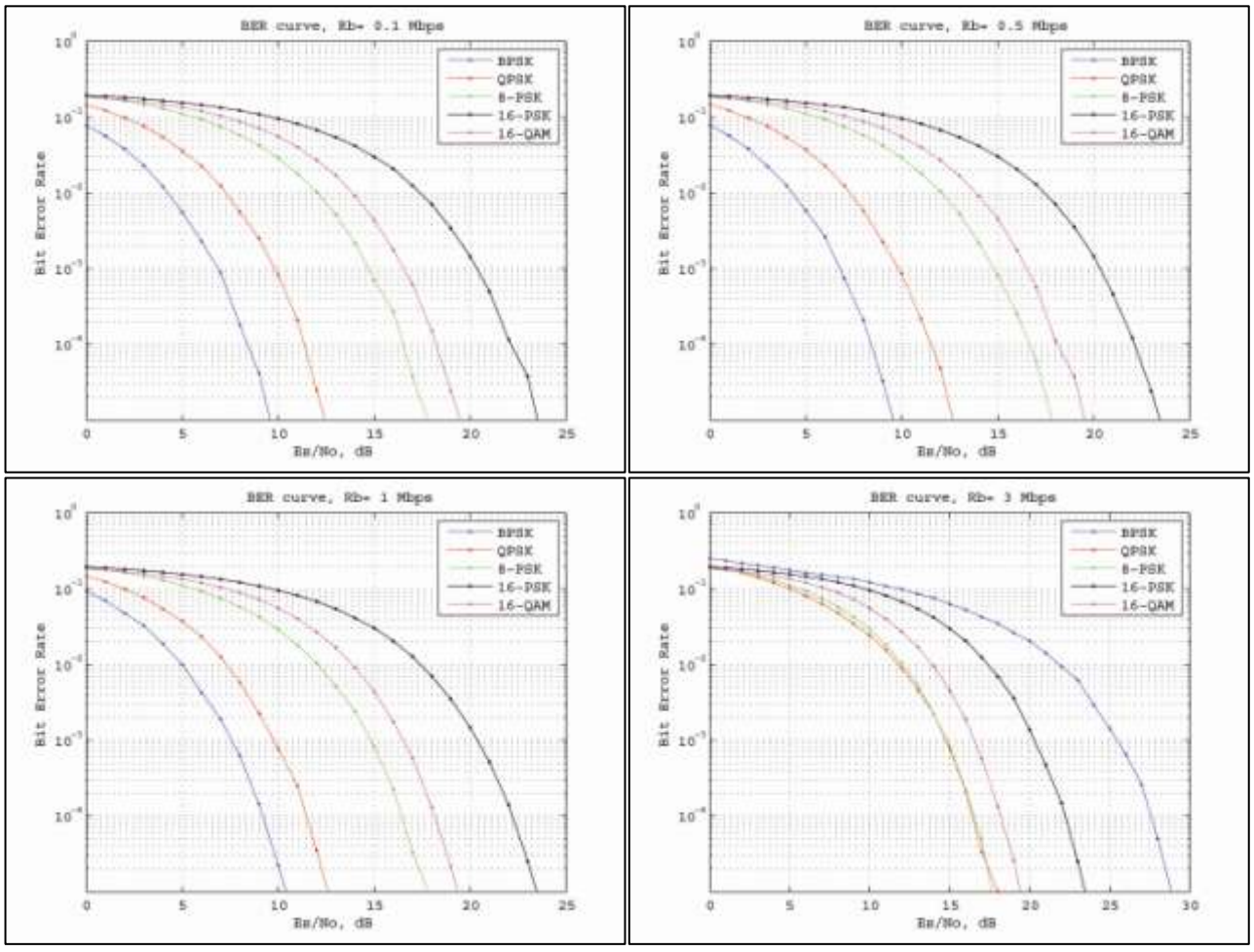
For Measurement P04-M1



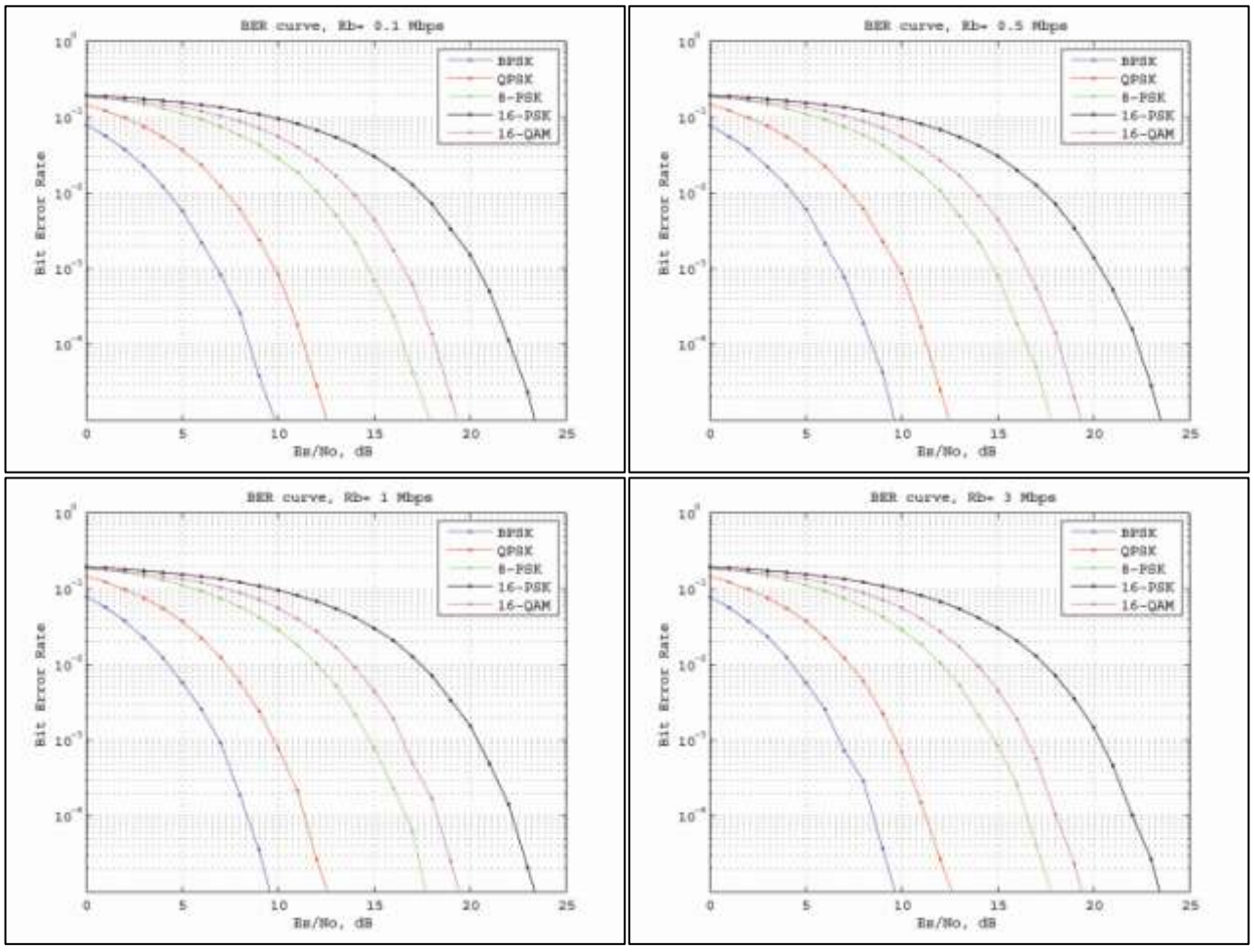
For Measurement P07-M1



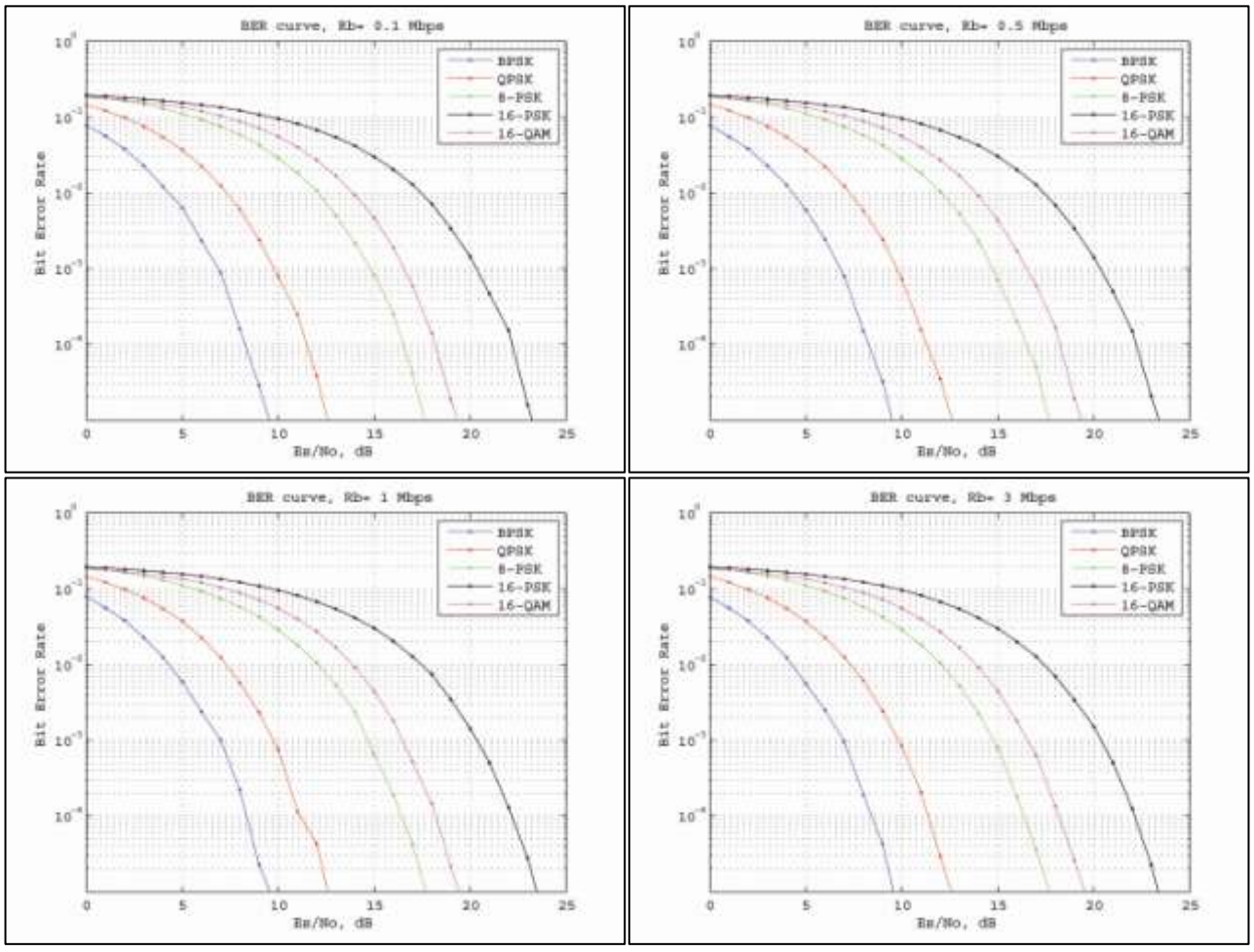
For Measurement P09-M1



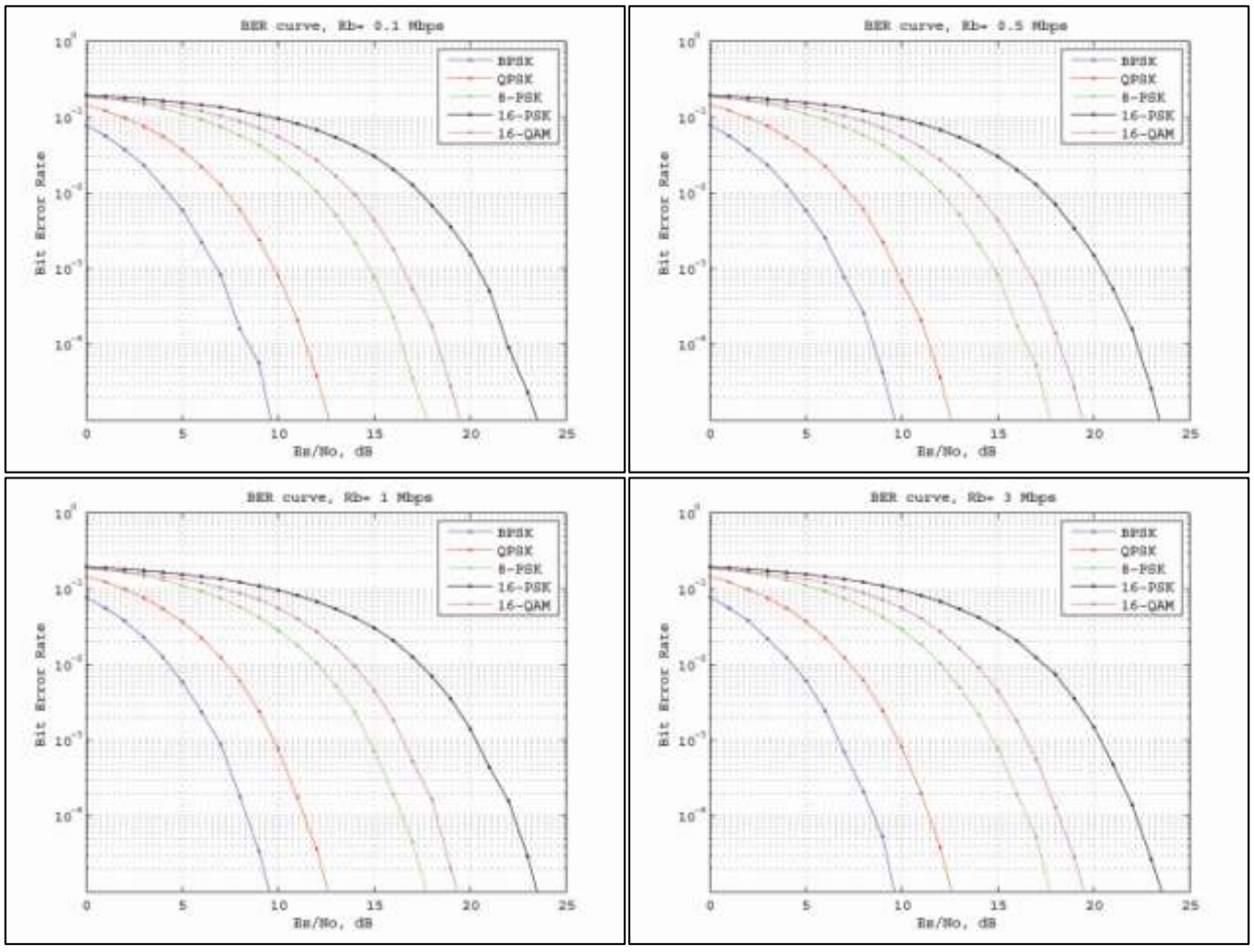
For Measurement P19-M1



For Measurement P15-M1



For Measurement P15-M2



APPENDIX-D

ABBREVIATIONS & ACRONYMS

A-B

AES Advanced Encryption Standard
AFH Adaptive Frequency Hopping
AGC Automatic Gain Control
AP Access Point
ARQ Automatic Repeat Request
AWGN Additive White Gaussian Noise
BER Bit Error Rate
BPSK Binary Phase Shift Keying modulation

C

CBC-MAC Cipher Block Chining Message Authentication Code
CDMA Code Division Multiple-Access
CDP Cyclic Data Packets
CIR Channel Impulse Response
CSIRO Australian Commonwealth Scientific and Research Organization
CSMA Carrier Sense Multiple-Access
CSMA-CA Carrier Sense Multiple Access Collision Avoidance
CTS Clear to Send

D-E

DIFS DCF Inter Frame Space
DLL Data Link Layer
DPSK Differential Phase Shift Keying
DQPSK Differential Quadrature Phase Shift Keying
DSSS Direct-Sequence Spread Spectrum
AES-CCMP Advanced Encryption Standard - Counter Mode CBC-MAC Protocol
EIA Electronic Industry Association

F-G

FCC Federal Communications Commission
FDM Frequency Division Multiplexing
FDMA Frequency Division Multiple-Access
FEC Forward Error Correction
FHSS Frequency Hopping Spread Spectrum
GFSK Gaussian Frequency Shift Keying

H-K

HMI Humane Machine Interface
HPOL Horizontal Polarization
HSM Hot Strip Mill
IEEE Institute of Electrical and Electronics Engineers
IR Infrared Radiation
ISA International Society for Automation
ISI Inter-Symbol Interference
KPI Key Performance Indicators

L-N

L2CAP Logical Link Control and Adaptation Protocol
LLC Logical Link Control
LMP Link Manager Protocol
LOS Line-Of-Sight
LTI Linear Time-Invariant
MAC Medium Access Control
MB-OFDM Multi-Band Orthogonal Frequency Division Multiplexing
MFT Message Freshness Timers
MS Mobile Station
NLOS Non-Line-Of-Sight

O-P

OFDM Orthogonal Frequency Division Multiplexing
OSI Open System Interconnection
O-QPSK Orthogonal Quadrature Phase Shift Keying
PDP Power Delay Profile
PH Physical Layer
PLC Programmable Logic Controllers
POL POLarization
PSD Power Spectral Density
PSK Phase Shift Keying
PSK Auth Pre-Shared Keys Authentication

Q-R

QAM Quadrature Amplitude Modulation
QoS Quality-of Service
QPSK Quadrature Phase Shift Keying
RF Radio Frequency
RM Roughing Mill
RMS Root Mean Square
RTE Real-Time Ethernet
RTS Ready To Send

S-T

SER Symbol Error Rate
SFCF Spaced-Frequency Correlation Function
SIG Special Interest Group
SNR Signal to Noise Ratio
TDD Time Division Duplex
TDMA Time Division Multiple Access

U-V

UAP User Application Processes
UWB Ultra Wide Band
VPOL Vertical Polarization
VVVF Variable Voltage Variable Frequency

W-Z

WEP Wired Equivalent Privacy
WLAN Wireless Local Area Network
WPA Wi-Fi Protected Access
WPAN Wireless Personal Area Networks
WSS Wide Sense Stationary
ZC ZigBee Coordinator
ZED ZigBee End Device
ZR ZigBee Router

REFERENCES

[1] Wireless Industrial Networking Alliance, 67 Alexander Drive, Research Triangle Park, NC 27709 USA. http://www.wina.org

[2] "Introduction to Fieldbus", http://www.automation.com/pdf_articles/fieldbus.pdf 2006 Moore Industries-International, Inc.

[3] Richard Zurawski, The Industrial Communication Technology Handbook, CRC Press, 2005.

[4] Pulat Matkurbanov, SeungKi Lee, and Dong-Sung Kim. "A Survey and Analysis of Wireless Fieldbus for Industrial Environments" SICE-ICASE 2006 International Joint Conferencein, Busan-Korea, IEEE Oct 2006, pp5555-5561

[5] A. Willig, M. Kubisch, C. Hoene, and A. Wolisz, "Measurements of a Wireless Link In an Industrial Environment Using an IEEE8022.11 Compliant Physical Layer", Transactions on Industrial Electronics, IEEE Dec 2002, vol-49, iss-6, pp1265-1282.

[6] Baker, N., "ZigBee & Bluetooth Strengths and Weaknesses for Industrial applications". Computing & Control Engineering Journal , IEEE Apr-May 2005, vol-16, iss-2, pp20-25.

[7] Andeas Willig, Kirsten Matheus, & Adam Wolisz "Wireless Technology in Industrial Networks". Proceeding of IEEE Jun 2005, vol-93, iss-6, pp1130-1151.

[8] Jiming Chen; Zhi Wang; Youxian Sun, "A Basic Study on Algorithm of Real-Time Schedule Table for Fieldbus", Intelligent Control and Automation, IEEE Nov 2002, vol-3, pp1760-1763.

[9] A. Willig, A. Woliesz, "Ring Stability of the Profibus Token-Passing Protocol Over Error-Prone Links", Transactions on Industrial Electronics, IEEE Oct 2001, vol-48, iss-5, pp1025-1033.

[10] Roundy, Shad, "Energy Scavenging for Wireless Sensor Nodes with a Focus on Vibration-to-Electricity Conversion", Phd. Dissertation, University of California, Berkeley, 19 Feb 2003.

[11] Goldsmith, A.J. and Wicker, S.B., "Design challenges for energy-constrained ad hoc wireless networks", Wireless Communications, IEEE Aug 2002, vol-9 iss-4, pp8–27.

[12] Theodore S. Rappaport, Wireless Communications: Principles and Practice, pp. 181-215, 2nd Edition, Prentice-Hall publisher 2002.

[13] Timothy Van Zandt, "Communication Complexity and Mechanism Design", INSEAD CEPR. 19 October 2006.

[14] Mats Andersson, "IEEE 802.11b and Bluetooth Industrial Environment", CTO connectBlue AB, Version 1.0 - May 2001.

[15] Zhong Tang, Haibin Yu and Hong Wang, "Implementation of Hybrid Wired and Wireless Foundation in Fieldbus", World Congress on Intelligent Control and Automation WCICA, IEEE Jun 2003, pp25-27.

[16] Bluetooth SIG (Nov 13, 2006). Bluetooth Wireless Technology Surpasses One Billion Devices. Press release. Retrieved January 17, 2007 from http://www.bluetooth.com/Bluetooth/Press/SIG/BLUETOOTH_WIRELESS_TECHNOLOGY_SURPASSES_ONE_BILLION_DEVICES.htm

[17] U. Bilstrup, Per-Arne Wiberg, "Bluetooth in Industrial Environment", International Workshop on Factory Communication Systems, Porto-Portugal, IEEE Sep 2000, pp239-246.

[18] Janell Armstrong, and C. Richard Helps, "Comparative Evaluation Of Zigbee And Bluetooth: Embedded Wireless Network Technologies for Students and Designers", Brigham Young University, American Society for Engineering Education, 2007.

[19] G. Miklos, A. Racz, Z. Turanyi, A. Valko, and P. Johansson, "Performance Aspects of Bluetooth Scatternet Formation", Mobile and Ad Hoc Networking and Computing MobiHOC, IEEE Aug 2000, pp147-148.

[20] Mats Andersson, "Using Bluetooth in an Industrial Environment, Reliability and Robustness"; connectBlue White Paper.

[21] Mats Andersson, connectBlue; "Intelligent Industrial Automation Devices using Bluetooth and Internet Technologies"; connectBlue White Paper

[22] Bluetooth SIG (2007), "Bluetooth Basics", Learn Retrieved January 17, 2007 from http://www.bluetooth.com/Bluetooth/Learn/Basics

[23] Carettoni, L., Merloni, C., and Zanero, S. "Studying Bluetooth Malware Propagation: The BlueBag Project", Security & Privacy IEEE Mar-Apr 2007, vol-5 iss-2, pp17-25.

[24] Shaked, Yaniv, and Wool, Avishai, "Cracking the Bluetooth PIN". School of Electrical Engineering Systems, and Tel Aviv University. 2007-02-01. http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/

[25] Nick Baker. "ZigBee & Bluetooth". Computing and Control Engineering. April 2005, volume 16, Issue 2. Pp 20-25.

[26] I. Chakraborty, A. Kashyap, A. Rastogi, H. Saran, R. Shorey, and A. Kumar. "Policies for Increasing Throughput and Decreasing Power Consumption in Bluetooth MAC". Personal Wireless Communications, IEEE Dec 2000, pp90–94.

[27] H. Zhu, G. Cao, G. Kesidis, and C. Das. "An Adaptive Powerconserving Service Discipline for Bluetooth". ICC 2002 International Conference on Communications. IEEE Apr 2002, vol-1, pp303–307.

[28] Luca Negri, Jan Beutel, and Matthias Dyer. "The Power Consumption of Bluetooth Scatternets" Consumer Communications and Networking Conference CCNC 2006. IEEE Jan 2006, vlo-1, pp519-523.

[29] Peng Zeng, Qin Wang, "Enhancement to IEEE802.15.4-2006 for hybrid contention access and scheduled access" Jul 2008, https://mentor.ieee.org/802.15/file/08/15-08-0619-01-004e-enhancement-to-802-15-4-2006-for-hybrid-contention-access-and-scheduled-access.pdf, Project: IEEE P802.15 Working Group for WPANs.

[30] ZigBee Alliance. About the ZigBee Alliance. Retrieved January 17, 2007 from http://www.zigbee.org/LearnMore/AnalystReports/tabid/259/Default.aspx

[31] David Culler, "Secure, Low-Power, IP-Based Connectivity with IEEE802.15.4 Wireless Networks", Industrial Embedded Systems, 2007.

[32] Pandey, J. N.; Kudva, S. S.; & Amrutur, B " A Low Power Frequency Multiplication Technique for ZigBee Transciever", Embedded Systems VLSI Design, IEEE Jan 2007, pp150-155.

[33] "CC2420 2.4 GHz IEEE802.15.4 / ZigBee - Ready RF Transceiver", http://www.datasheetarchive.com/CC2420-datasheet.html

[34] Mastooreh Salajegheh, Hamed Soroush, and Antonis Kalis, "HyMAC: Hybrid TDMA/FDMA Medium Access Control Protocol for Wireless Sensor Networks", Personal, Indoor and Mobile Radio Communications PIMRC, IEEE Sep 2007, pp1-5.

[35] Institute of Electrical and Electronic Engineering, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 5: Spectrum and Transmit Power Management Extensions in the 5GHz Band in Europe", IEEE Standard Oct 2003.

[36] "802.11g Wireless Internet Access Information and Technology Descriptions", http://www.bbwexchange.com/wireless_internet_access/802.11g_wireless_internet_access.asp

[37] K. Matheus, Wireless Local and Wireless Personal Area Network Technologies for Industrial Deployment, in The Industrial Communication Technology Handbook (R. Zurawski, ed.), CRC Press, 2004, chapter-19.

[38] R. van Nee and R. Prasad, "OFDM for Wireless Multimedia Communications". Artech House Publisher, 2000, pp240-255.

[39] R. van Nee, G. Awater, M. Morikura, H. Takanashi, M. Webster, and K. W. Halford, "New High-Rate Wireless LAN Standards", IEEE Communications Magazine, Dec 1999, vol-37, pp82–88.

[40] M. V. Clark, K. K. Leung, B. McNair, and Z. Kostic, "Outdoor IEEE802.11 Cellular Networks: Radio Link Performance", International Conference on Communications ICC, IEEE May 2002, pp512-516.

[41] K. K. Leung, B. McNair, L. J. Cimini, and J. H. Winters, "Outdoor IEEE802.11 Cellular Networks: MAC Protocol Design and Performance", International Conference on Communications ICC, IEEE May 2002, pp595-599.

[42] K. Shuaib, M. Boulmalf, F. Sallabi and A. Lakas "Performance Analysis: Co-existence of IEEE802. 1Ig with Bluetooth" Wireless and Optical Communications Networks WOCN, IEEE Mar 2005, pp40-44.

[43] Patrick McCurdy and Ira Sharo. "Wi-Fi, Why Now? Exploring New Wireless Technologies for Industrial Application", ISA Expo 2006, pp 1-11.

[44] User Guide Manual, "Wideband Channel Sounder System Model WCS3500", *Freshfield Communications Limited, Croydon, Surrey U.K. June 2005.* support@fclcom.demon.co.uk

[45] Jose Manuel Albornoz, "Wideband Channel Sounder", Master Thesis, *The Ohio State University, 2001.*

[46] Macario R.C, Modern Personal Radio Systems, pp47, chapter-3, *IEE Press, London 1996.*

[47] Parsons J, and Demery D., Turkmani A, "Sounding Techniques for Wideband Mobile Radio Channels ", Communications, Speech and Vision IEE Proceedings, IEEE Oct 1991, pp437–446, vol-138, iss-5.

[48] Braun W, and Dersch U, "A Physical Mobile Radio Channel Model". Transactions on Vehicular Technology, IEEE May 1991, pp172-182, vol-40, iss-2.

[49] Muqaibel, A., Safaai-Jazi, A., Woerner, B., and Riad, S.;. "UWB Channel Impulse Response Characterization Using Deconvolution Techniques". IEEE Aug 2002, pp605-8 vol-3.

[50] Rappaport, T.S., Seidel, S.Y., and Takamizawa, K. "Statistical Channel Impulse Response Models for Factory and Open Plan Building Radio Communication System Design". IEEE May 1991, vol-39, iss-5, pp794-807.

[51] Chiu, S., Chuang, J., and Michelson, D. G. "Characterization of UWB Channel Impulse Responses within the Passenger Cabin of a Boeing 737-200 Aircraft". IEEE Dec 2009, iss-99 pp1-1.

[52] Celik, N., Zhengqing Yun, Iskander, M.F. "Employing Realistic Propagation Models in Wireless System Simulations". Hawaii Center for Advanced Communications, College of Engineering, University of Hawaii, Manoa, IEEE Jun 2007, pp3772-3775.

[53] Cheng Li, Tianqi Wang, and Hsiao-Hwa Chen. "On Iterative EM-Based Frequency Domain Joint Estimation of Synchronization Parameter and Channel Impulse Response". PIMRC, IEEE Nov 2007, pp4160-4164.

[54] Hideaki Tanaka, Naoto Sasaoka, Takaharu Nakanishi and Yoshio Itoh. "A Study of Adaptive Guard Interval with Estimation of Channel Impulse Response for OFDM system". Graduate School of Engineering, Tottori University, IEEE Feb 2009, pp1-4.

[55] Mauel Dinis, jose Garcia, Valdemar Monteiro, and Nelson Oliveira. "Millimetre-Wave Channel Impulse Response Experimental Evaluation and Relation Between Delay Spread and Channel Coherence Bandwidth". PIMRC, IEEE Sep 2002, pp2292-2296 vol-5.

[56] Proakis, John G., "Digital Communication". *Fourth Edition, p254-282 , 2001.*

[57] Leon W. Couch, II. "Digital and Analog Communication Systems". New Jersey:Prentice Hall, 2001.

[58] T. S. Rappaport and C. D. McGillem, "Characterising the UHF Factory radio Channel". IEEE Engineering Research Centre for Intelligent Manufacturing Systems Purdue University West Lafayette, USA. Electronics Letters Vol. 23 No. 19 pp 1015-1017, 10 Sep 1987.

[59] T. S. Rappaport, "Characterization of UHF Multipath Radio Channels in Factory Buildings". IEEE Transactions on Antennas and Propagation, Vol. 37. no. 8, pp 1058-1069, Aug 1989.

[60] Sebastian Kozłowski, Rafał Szumny, Krzysztof Kurek, Jozef Modelski, "Statistical Modelling of a Wideband Propagation Channel in the Factory Environment". IEEE European Conference on Wireless Technology, EuWiT. Vol. 37. no. 8, pp 190-193, Oct 2008, Amsterdam, The Netherlands.

[61] R. Szumny, K. Kurek, S. Kozłowski, and J. Modelski, "Measurements and analysis of the propagation channel for various indoor environments," in EUROCON 2007 International Conference on Compuer as a Tool, Warsaw, Poland, Sep 2007.

VITA

Nationality:	**SAUDI**
April 5, 1981	Born - Abha, Kingdom of Saudi Arabia (KSA)
1998-2004	B.S. Electrical Engineering King Fahad University of Petroleum and Minerals, Dhahran, KSA
2006-2010	M.S. Electrical Engineering, King Fahad University of Petroleum and Minerals, Dhahran, KSA
2004-present	Engineer, Process Control Specialist, Saudi Iron & Steel Co. (HADEED), Jubail, KSA

Fields of Study

Major Field: Telecommunication Engineering

Sub-Field: Industrial Wireless Communications

Addresses

Present Address: Saudi Arabia, Jubail Industry City, 31961 (PO Box: 10053)

Permanent Address: Saudi Arabia, Mekkah, Al-Senaeya (PO Box: 20710)

E-mail Address: yousufdm@hadeed.com.sa; ymoallem@gmail.com; y_moallem@hotmail.com