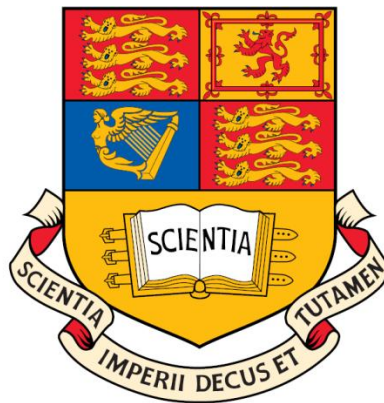


Wireless Communication in Process Monitoring and Control

by

Waqas Ikram



A thesis submitted for the degree of Doctor of Philosophy (PhD)
and for Diploma of Imperial College (DIC)

October 2012

Centre for Process Systems Engineering (CPSE),
Department of Chemical Engineering,
Imperial College London
London SW7 2AZ

Abstract

Recent developments in wireless communication technology offer new opportunities for wireless connectivity of field devices in industries such as oil and gas, chemical processing and water distribution. Wireless communications can assist these industries to improve plant knowledge by acquiring additional measurements from processes and equipment when wired communication would be infeasible.

Requirements for a field communication network in the process industry include real-time support for mixed traffic, robustness, availability, security, reliability and scalability in a harsh industrial environment. Furthermore, to build such a network on license-exempt band raises concerns relating to its safety, security, performance and governance.

Three specific issues have been addressed in this thesis. The first issue investigated is time synchronization which is necessary to ensure data integrity and determinism in network operations. The second investigation is the study of the performance of a closed-loop control application running over a resource-constrained wireless network. The need to ensure co-existence with the other wireless networks operating over the same radio band while offering predictability and reliability has added a new concern to the use of wireless technology in networked control systems. The third issue is to ensure longevity of wireless field nodes operated on standalone batteries which requires a mechanism to minimize energy consumption. This topic was addressed in an investigation into methods for transmission power control. The research presented in this thesis has discovered new ways to solve these problems. It has characterized their performance and implemented them in several practical demonstrations, including one field deployment.

The thesis also provides an insight into the opportunities which wireless technology offers, the challenges which it encompasses, and gives a review of key emerging wireless networking technologies relevant to process automation. Finally, it offers an opinion about the future directions of wireless communications in the process industries.

Acknowledgments

First and foremost, I would like to express my deepest gratitude to God Almighty Who provided me with His blessing and the opportunity to successfully conclude this project.

I would like to express my appreciation to my supervisor, Prof. Nina Thornhill, for her constant and unending support in making this project possible. I thank her for having given me the opportunity to undertake such a wonderful research project, and for having taken a personal interest in bringing me to this moment of time towards the completion of my studies. I also have Dr. Ivan Stoianov, Dr. Julie McCann and Prof. Geoffrey Maitland to thank for their invaluable advice regarding matters of my research.

In addition, I would like to thank ABB for their commitment, support, time and expertise in making this research industrially relevant. In this regard, I would like to acknowledge the contributions by Dr. John Pretlove, Dr. Paula Doyle, Dr. Charlotte Skourup and Trygve Harvei of ABB for their constant support for making the project a success. Additionally, I would also like to thank them for providing me an opportunity to experience firsthand the challenges my research was addressing through an industrial placement which I undertook at an R&D facility of ABB in Norway in 2010. The expertise and the outlook I was exposed to, and the resources made available to facilitate my research at the R&D facility of ABB was appreciable. Furthermore, the discussion I had with Stig Petersen of SINTEF and Simon Carlsen of Statoil during my placement was very valuable and much appreciated.

Moreover, I would also like to acknowledge the DTA scholarship from Imperial College London and funding from the ABB/RAEng Chair of Process Automation for financing my research.

I would also like to thank my friends, both in Imperial College London and elsewhere, who continued to support me throughout my years of study and for their excellent co-operation and inspiration, and making my time as a PhD student more enjoyable. My special thanks goes to my colleagues, both past and present – Ali, Colin, Dionysios, Erlend, Haroon, Ines, Jerry, Mahdi, May, Nick, Sarah, Tope and Yang. Furthermore, many

thanks to my friends outside the office world: Abd el-ilah, Ali, Asher, Azeem, Erkan, Esa, Hassan, Nasir, Shahzad and Yasir.

Finally and most importantly, I acknowledge my sincere indebtedness and gratitude to my grandparents, parents and not forgetting my dearest siblings for their love, support and sacrifice throughout my life. I cannot find appropriate words to express my appreciation for everything my family has done for me. Many thanks to my brothers: Imran, Shahid, Shahzad and Umair, and my sisters: Azmat, Sitara, Sana and Komal, who have put up with me, especially through the busy days of my life. I would like to acknowledge their comments and suggestions which were valuable and crucial for successful completion of my degree.

Declaration of Originality

The author declares that the present thesis reports the results of his own research and that all else is appropriately referenced. In addition, the presented materials are not submitted elsewhere for another degree.

Dedicated to almighty God, family and friends...

Table of Contents

List of Figures	v
List of Tables	viii
List of Panels	ix
List of Abbreviations.....	x
CHAPTER 1. Introduction	1
1.1. Introduction to the Research Problems.....	1
1.1.1. Automation and Oil and Gas Industry – An Overview.....	2
1.1.2. Time Synchronization in Distributed Wireless Systems	6
1.1.3. Process Control over a Wireless Network.....	8
1.1.4. Transmission Power Control	11
1.2. Motivation for the Research.....	15
1.2.1. Wireless Technology in Process Automation	15
1.2.2. The Need for Time Synchronization.....	18
1.2.3. Towards Wireless Networked Control Systems	20
1.2.4. The Incentive for Transmission Power Control.....	22
1.2.5. Summary.....	23
1.3. Aims and Objectives, Requirements and Challenges	24
1.3.1. Aims and Objectives.....	24
1.3.2. Requirements Analysis.....	27
1.4. Layout of the Thesis	30
1.5. Contribution of the Thesis	32
1.6. Chapter Summary.....	34
CHAPTER 2. Background and Context: Wireless Technologies and Process Automation.....	36
2.1. Opportunities for Wireless Communication in Process Automation	36
2.2. Automation Pyramid and Usage Classes	38
2.3. Comparison of Commercial Wireless Communication Technologies	44
2.4. Advent of Industrial Strength Wireless Networks	50
2.4.1. ZigBee PRO	50
2.4.2. WirelessHART.....	52
2.4.3. ISA100.11a.....	53
2.4.4. WIA-PA	55
2.4.5 Comparison of Industrial Standards.....	58
2.5. Chapter Summary.....	63
CHAPTER 3. Background and Context: Review of Literature	65

3.1	Time Synchronization in Distributed Systems.....	65
3.1.1.	Overview: Historical Perspective.....	66
3.1.2.	Time Synchronization Protocols.....	70
3.1.3.	Hardware Assisted Time Synchronization.....	72
3.1.4.	Challenges	75
3.1.5.	Related Work in Context.....	76
3.1.6.	Summary.....	78
3.2.	Wireless Communication in Networked Control Systems.....	78
3.2.1.	Control over Wireless Network: Overview and Approach.....	79
3.2.2.	Current Practices and System Architecture	81
3.2.3.	Concerns and Challenges.....	83
3.2.4.	Related Work in Context.....	89
3.2.5.	Summary.....	91
3.3.	Transmission Power Control in IEEE 802.15.4 Networks	92
3.3.1.	Overview.....	93
3.3.2.	TPC Strategies, Applicability and Wider Considerations	95
3.3.3.	Classification of Strategies for Transmission Power Control.....	100
3.3.4.	Industrial Requirements, Challenges and Assumptions.....	104
3.3.5.	Related Work in Context.....	104
3.3.6.	Summary.....	107
CHAPTER 4.	Time Synchronization in Distributed Wireless Systems	108
4.1.	Overview of Proposed Solution.....	108
4.2.	MSF Signal and Radio Controlled Clock Receiver	110
4.3.	Radio Controlled Clock Performance	115
4.3.1	Theoretical Analysis	115
4.3.2.	Empirical Results	122
4.3.3.	Radio Controlled Time Synchronized Wireless Sensor Network	131
4.4.	Minimization of Time Synchronization Error.....	135
4.5.	Procedure for Time Synchronization of a Field Node	148
4.6.	Radio Clocks in Challenging Environments	152
4.6.1	Illustrative Example: Practical Deployment.....	153
4.6.	Chapter Summary.....	157
CHAPTER 5.	Studies on Performance of a Control Application Operating over a Wireless Network.....	159
5.1.	Overview	159
5.1.1.	Networked Control Systems.....	160
5.1.2.	Requirements and Challenges.....	162
5.1.3.	IEEE 802.15.4 MAC and PHY limits.....	165

5.1.4.	Sink and Hopping in a Wireless Sensor and Actuator Network.....	167
5.1.5.	Distinction between WSN and WSNAN.....	169
5.2.	Network Setup for Process Control Loop Performance Analysis: A Case Study.....	171
5.2.1.	Control Architecture and Non-Standardized Regions.....	171
5.2.2.	Process Model	174
5.2.3.	Control Strategy	175
5.2.4.	Simulation of a Control Loop Performance Setup	175
5.2.5.	Hardware-in-loop Setup	177
5.3.	Proposed Mechanism to Improve Performance	178
5.3.1.	Control Loop Performance	178
5.3.1.	Data Recovery to Improve Integral and Derivative parts of PID Algorithm.....	183
5.3.2.	Improving Data Delivery Success within a Time Frame	185
5.3.3.	Fast Lane Selection based on Minimization of Spectrum Occupancy subject to time delay and throughput constraints	189
5.3.4.	Overall Framework	196
5.4.	Chapter Summary.....	197
CHAPTER 6.	Transmission Power Control	199
6.1.	Overview	199
6.1.1.	Industrial Requirements	200
6.1.2.	Constraints.....	201
6.2.	System Model.....	202
6.2.1.	Terminology	203
6.2.2.	Problem Specification	204
6.2.3.	SINR and SNR Estimation.....	205
6.3.	Empirical Studies on Link Quality Assessment.....	206
6.3.1.	Hardware Implementation and Experimental Setup	206
6.3.2.	Results and Performance Analysis.....	207
6.3.3.	Characterizing RSSIs.....	215
6.4.	Design of Transmission Power Control Algorithm	216
6.4.1.	Overview of the Algorithm	216
6.4.2.	Building the TPC Table	217
6.4.3.	Estimation of Golden Receive Power Range	219
6.4.4.	Setting the Transmission Power Level.....	220
6.4.5.	Procedure of Transmission Power Control	221
6.4.6.	Implementation of Transmission Power Control.....	224
6.4.7.	Implementation Results.....	227
6.4.8.	Energy Consumption Analysis.....	228

6.5.	Chapter Summary	232
CHAPTER 7. Conclusions, Evaluation and Future Directions		233
7.1.	Overview	233
7.1.1.	Topics of Research	233
7.1.2.	Motivation, Aims and Objectives	234
7.2.	Summary of Main Findings and Conclusions	237
7.2.1.	Time Synchronization in Distributed Networks	237
7.2.2.	Wireless Networked Control Systems	240
7.2.3.	Transmission Power Control	242
7.3.	Critical Evaluation	243
7.4.	Recommendations for Future Work	245
7.5.	Chapter Summary	247
Appendix A1. Energy Savings		249
Appendix A2. Improved Receiver Sensitivity		250
Appendix B1. WLAN and WPAN Technologies		251
B1.1.	IEEE 802.11 Family of Standards (Wi-Fi)	252
B1.2.	Bluetooth	254
B1.3.	ZigBee	256
B1.4.	UWB	257
Appendix B2. IEEE 802.15.4-2006		260
Appendix C1. EM2 MSF Datasheet		262
Appendix C2. Simulink Model for Hardware in Loop Setup		263
Appendix C3. Time Slot Calculation		264
References		265

List of Figures

Figure 1.1.	Operations in oil and gas industry.....	4
Figure 1.2.	Hierarchical view of research categories within industrial automation and the problems addressed in this thesis.....	5
Figure 1.3.	Feedback control loop operating over a wireless network.....	10
Figure 1.4.	Transmission power control loop.....	13
Figure 1.5.	Tables for communication in a network.....	14
Figure 1.6.	Comparison between conventional 4-20 mA current loop, fieldbus and wireless communication architectures.....	17
Figure 1.7.	Open-loop control system demonstrating remote monitoring.....	19
Figure 1.8.	Timeline of network evolution in measurement and control technology.....	21
Figure 1.9.	Evolution in network architecture.....	22
Figure 2.1.	Overview of sensor network applications in industry.....	37
Figure 2.2.	Hierarchical view of automation classes.....	40
Figure 2.3.	The automation pyramid.....	41
Figure 2.4.	Application requirement per usage class.....	44
Figure 2.5.	The relationship of the IEEE 802 standards to the protocol structure of WPAN and WLAN technologies.....	46
Figure 2.6.	Examples of typical (a) WirelessHART (b) ISA100.11a (c) two-layered star-mesh WIA-PA networks.....	57
Figure 2.7.	Illustrating the relationship of WirelessHART, ISA100.11a and WIA-PA to the reference OSI seven-layer model.....	62
Figure 3.1.	Advancements and milestones in timekeeping.....	68
Figure 3.2.	Typical timing accuracy over a period of 24 hours of various timing standards....	69
Figure 3.3.	Hierarchical tree showing available methods for achieving time synchronization in distributed systems.....	73
Figure 3.4.	Depiction of (a) Direct Structure and (b) Hierarchical Structure.....	82
Figure 3.5.	Wireless Networked Control System Architecture.....	84
Figure 4.1.	A minute time frame of MSF time and date code signal, 00-59 seconds.....	111
Figure 4.2.	MSF signal bit stream.....	111
Figure 4.3.	A flow chart of the MSF signal receiver and its extensions.....	113
Figure 4.4.	Snapshot of the experimental setup for time and date code validation.....	113
Figure 4.5.	Snapshot of the experimental setup for signal quality assessment.....	114
Figure 4.6.	Snapshot of two versions of the radio clock.....	114
Figure 4.7.	Demodulated MSF signals captured from the developed module. Panels (a) to (d) are explained in the text.....	118
Figure 4.8.	Latency calculations based on timing pulses of GPS and MSF modules.....	123
Figure 4.9.	Test sites for the experiments.....	123
Figure 4.10.	Cumulative probability distribution of latency value corresponding to RCCv1. recorded at a site in (a) London, and in (b) Whitehaven.....	124
Figure 4.11.	Latency distribution of RCCv1 for experiment conducted at two locations.....	124
Figure 4.12.	Latency value of RCCv2 for experiment conducted in Whitehaven.....	126
Figure 4.13.	Latency distribution of RCCv1 and RCCv2 as recorded in Whitehaven.....	126
Figure 4.14.	(a) SoF as captured from two receivers, and (b) is magnified version of (a).....	127
Figure 4.15.	Cumulative probability of RCCv1 and RCCv2 for experiments conducted in Whitehaven.....	128
Figure 4.16.	Snapshot of the GUI developed for displaying, archiving, and validating the time and date information extracted from the MSF signal.....	129
Figure 4.17.	Summary of the received MSF data frames.....	130

Figure 4.18.	Time offset between two motes which are synchronized by the MSF signal.....	132
Figure 4.19.	Allan deviation of RCCv1 and RCCv2 clocks which are based on EM2S.....	134
Figure 4.20.	Long term trend in Allan deviation values for RCCv1.	135
Figure 4.21.	KLD with respect to reference distribution versus time (a) for RCCv1 and (b) for RCCv2 for experiments conducted in Whitehaven.....	136
Figure 4.22.	Latency versus time trend recorded over a period of 4 hours at UTC 00 seconds. Panels (a) to (d) explained in text.	137
Figure 4.23.	Flow chart of time synchronization (a) off-line stage, (b) on-line stage.....	139
Figure 4.24.	Transmission and reception of the on-time markers.....	143
Figure 4.25.	Kalman filter output of latency value for RCCv1 for (a) experiment conducted in London, (b) for experiment conducted in Whitehaven.....	143
Figure 4.26.	Latency versus time plot (a) for +30 PPM and (b) for +2 PPM oscillator.	147
Figure 4.27.	Time synchronization accuracy as a result of the proposed algorithm.	147
Figure 4.28.	Block diagram for time synchronization procedure.	149
Figure 4.29.	(a) An outside view of a fire hydrant with a metal cover, (b)-(d) inside view of typical fire hydrants with monitoring equipments. (e-f) deployment sites for conducting field-trials, referred to as FH1 and FH2 respectively.....	156
Figure 4.30.	Latency versus time plot for deployment in (a) FH1 and (b) FH2.....	156
Figure 4.31.	Time synchronization error relative to GPS for RCCv1 deployment in (a) FH1, and (b) in FH2. Time synchronization accuracy as a result of the proposed algorithm, (c) in case of FH1 and (d) for FH2. <i>Before</i> represents the time accuracy using MSF receivers only without any processing, and <i>after</i> represents time accuracy post processing of receiver output using the proposed methodology	157
Figure 5.1.	Closed loop control over a wireless mesh network.....	161
Figure 5.2.	Process response of a first order plus time delay system from HCF (2009).	163
Figure 5.3.	Example of an IEEE 802.15.4 superframe structure (a) with inactive and (b) without inactive period, modified from IEEE 802.15.4 (2006).	167
Figure 5.4.	Hierarchy of control systems and network architecture, modified from individual standards.....	172
Figure 5.5.	Timeline of feedback control execution.	173
Figure 5.6.	Schematic of a furnace process.	175
Figure 5.7.	Schematic of a process flow diagram.....	176
Figure 5.8.	A hardware-in-loop setup to quantify the issues in a WNCS.....	177
Figure 5.9.	Industrial furnace response to changes in set points. Network delays are ignored in this simulation.....	178
Figure 5.10.	Oxygen concentration response to a step change in reference with varying sensor and controller execution period and controller gain. The upper panel corresponds to a controller gain of 340, and the lower panel corresponds to 240.....	179
Figure 5.11.	Upper panel corresponds to a network delay of one second and the lower path corresponds to a network delay of two seconds.	180
Figure 5.12.	Random distribution of sensor packet delays within a range of one to two seconds.	180
Figure 5.13.	A hardware-in-loop experiment demonstrating random distribution of sensor packet delays and packet losses as a result of co-channel interference from Wi-Fi.	181
Figure 5.14.	Control system response to a network outage of a 30 second duration..	182
Figure 5.15.	The switched state mode operation of the controller depending on the network status. Reference point is not shown explicitly and is considered to be known to each state.....	184
Figure 5.16.	Comparison of the control system performance with recovered ID method.....	185
Figure 5.17.	A superframe structure highlighting a time slot within the time frame.....	186

Figure 5.18.	(a) shows an example of allocated time slots in time and frequency, whereas (b) highlights an enhancement with the dedicated channel for time bounded critical data.	186
Figure 5.19.	The control system performance subjected to data packet losses. The control loop was scheduled to be updated every second.	188
Figure 5.20.	Aggregated spectrum occupancy versus aggregated network throughput in the fast lane.	195
Figure 5.21.	The layered model of interaction between different layers with information sharing via a common repository.	197
Figure 6.1.	(a) Experimental setup and (b) spatial distribution of transmitter and receiver, not drawn to scale. The grey region represents the office cubicles, whereas blue regions are planes above those cubical with Line of Sight (LoS).	209
Figure 6.2.	(a) RSSI distribution versus transmission power between T1 and R1, and (b) linear approximation of data presented in (a).	209
Figure 6.3.	RSSI distribution versus transmission power of Channel 15 over varying distance.	210
Figure 6.4.	Heatmap and the spectrogram of activity recorded in IEEE 802.11 channels at location R1.	210
Figure 6.5.	IEEE 802.15.4 channels and the recommended selection of IEEE 802.11 extension networks.	211
Figure 6.6.	RSSI distributions for channel 15 are shown in (a) and (b), whereas for channel 24 are shown in (c) and (d). Power levels are indicated in plots.	211
Figure 6.7.	Heatmap and the spectrogram of activity recorded in IEEE 802.11 channels at location R2.	213
Figure 6.8.	Kullback-Leibler Divergence with respect to final distribution versus number of packets.	216
Figure 6.9.	Illustration of transmission power control loops.	219
Figure 6.10.	(a) Initialization phase, and (b) operational phase of the proposed TPC algorithm.	226
Figure 6.11.	Upper: Transmission power. Lower: RSSI at receiver.	228
Figure 6.12.	Run-time TPC operation. Left: transmission power responses to fading. Right: transmission power responses to changes in position of the receiver.	229
Figure A1.1	Ratio of energy consumption as a function of communication interval and transmitter current drain. Based on CC2430 module and 127 bytes packet size.	249
Figure A2.1.	Receive signal as a function of distance and transmission power.	250
Figure B1.1.	Illustration of wireless network technologies based on range, transmission power and data rate.	252

List of Tables

Table 1.1.	Basic requirements for communications in process automation.....	28
Table 1.2.	Wireless associated requirements for process automation.....	29
Table 2.1.	Example applications of wireless communications in the process industry.....	39
Table 2.2.	Classification of the process automation applications.....	43
Table 2.3.	Terminologies used in application requirements per usage class illustration... ..	44
Table 2.4.	Comparison of short-range wireless communication technologies.....	47
Table 2.5.	Qualitative comparison of short-range wireless communication technologies for use in process automation.....	49
Table 2.6.	Comparison of ZigBeePRO, WirelessHART, ISA100.11a and WIA-PA networks.....	63
Table 3.1.	Terrestrial time broadcasting radio stations.....	74
Table 4.1.	Comparison of energy consumption in Joules between MSF and GPS based time synchronization solutions.....	120
Table 4.2.	Latency distribution values in milliseconds for RCCv1.....	125
Table 4.3.	Jitter in milliseconds as recorded in experiments.....	126
Table 4.4.	Latencies distribution in milliseconds as experienced in Whitehaven.....	127
Table 4.5.	Comparison of required time synchronization intervals.....	132
Table 5.1.	Closed loop control performance evaluated in terms of Sum of Square Errors (SSE).. ..	182
Table 6.1.	Summary of RSSI distributions for various channels under LOS conditions and with T1 and R2 installations.....	214
Table 6.2.	Summary of RSSI distributions for NLOS conditions with transmitter at T2 operating at 0 dBm.....	214
Table B1.1.	IEEE 802.11 standard and its extensions.....	125

List of Panels

Panel 4.1. Summary of nomenclature.....	138
Panel 6.1. Details of the hardware used.	207
Panel 6.2. Energy cost estimation based on CC2420 transceiver specification.	231

List of Abbreviations

AD	Allan Deviation
ATPC	Adaptive Transmission Power Control
CCA	Clear Channel Assessment
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CRC	Cyclic Redundancy Check
CPU	Central Processing Unit
DS-UWB	Direct Sequence – Ultra Wideband
DSSS	Direct Sequence Spread Spectrum
DCS	Distributed Control System
ED	Energy Detection
ERP	Enterprise Resource Planning
FHSS	Frequency Hopping Spread Spectrum
FFD	Full Function Device
FTSP	Flooding Time Synchronization Protocol
GSM	Global System for Mobile communications
GPS	Global Positioning System
GUI	Graphical User Interface
HART	Highway Addressable Remote Transducer Protocol
HCF	HART Communication Foundation
ISM	Industrial, Scientific and Medical
ITU	International Telecommunication Union
KF	Kalman Filter
KLD	Kullback-Leibler Divergence
LOS	Line of Sight
LR-WPAN	Low Rate – Wireless Personal Area Network
LQI	Link Quality Indicator
MEMS	Micro-Electro-Mechanical Systems
MAC	Medium Access Control
NTP	Network Time Protocol
NCS	Networked Control System
NLOS	No Line of Sight
NPL	National Physics Laboratory
OCXO	Oven Controlled Crystal Oscillator
OTM	On-Time Marker
OFDM	Orthogonal Frequency Division Multiplexing
PAN	Personal Area Network
PCB	Printed Circuit Board
PER	Packet Error Rate
PID	Proportional Integral Derivative
QoS	Quality of Service
RFD	Reduced Function Device
RBS	Reference Broadcast System
RCC	Radio Controlled Clock
RSSI	Received Signal Strength Indicator
SCADA	Supervisory Control and Data Acquisition

SIR	Signal to Interference Ratio
SINR	Signal to Interference plus Noise Ratio
SO	Spectrum Occupancy
TCXO	Temperature Compensated Crystal Oscillator
TDMA	Time Division Multiple Access
TPC	Transmission Power Control
TPSN	Timing-sync Protocol for Sensor Networks
UTC	Coordinated Universal Time
UWB	Ultra-Wideband
WSN	Wireless Sensor Network
WSAN	Wireless Sensor and Actuator Network
WISA	Wireless Interface for Sensors and Actuators
Wi-Fi	Wireless Fidelity (Certificated IEEE 802.11 compliant devices)
WPAN	Wireless Personal Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WWAN	Wireless Wide Area Network
WNCS	Wireless Networked Control Systems
XO	Crystal Oscillator

CHAPTER 1

Introduction

This chapter presents an overview of the research problems addressed in this thesis, the motivation behind this research and the corresponding aims and objectives. It begins with an examination of the existing relevant research problems within the context of wireless process automation. Moreover, it provides information about the motivation for the research and the drive from both academic and industrial community which steered the research goals. It is followed by the description of the overall aims and challenges of this research, and the requirements which are to be adhered to while addressing these problems. The contributions made by the thesis and the novelty in the proposed solutions have been elaborated too. Finally, it reveals the outline of the rest of the thesis in detail. In short, the aim of this chapter is to define the research problems and communicate those specifications which will govern the development of the algorithms and systems.

1.1. Introduction to the Research Problems

This section places the research problems in the context of wireless process automation. It begins by providing an overview of process automation within the context of process industries, especially the oil and gas industry which is one of the sectors of interest in this project. It further examines the different components of operation within this industry and highlights the importance of process automation to the industry. Communication networks, an area of research in this thesis occupy an essential place in process automation. Within the communication domain various solutions are currently available based on wired and wireless networks. Their use is application and deployment specific; however, this research focuses on wireless networks. The wireless communication solutions are based on radio, cellular and

satellite technologies. These solutions vary in range, cost, availability and the services they offer. The work presented in this thesis is confined to the use of short-range, low-power and license-exempt standardized wireless communication technologies and their applicability in process automation for monitoring and control related applications. Their use is relatively new to the industry and has created new research opportunities.

The prerequisites of a field communication network in process industry include real-time support for mixed traffic, robustness, availability, security, reliability and scalability in a harsh industrial environment. Furthermore, to build such a network on license-exempt band raises concerns relating to its safety, security, performance and overall Quality of Service (QoS). QoS is about managing network resources and offering services which are required by application by means of controlling delay, jitter, packet loss rate and bandwidth. To develop an industrial strength wireless network which can address these stringent process automation requirements imposes restrictions on the network design which incorporates the hardware and software components used. To achieve the required QoS, a wider view of systems has to be considered as the overall performance of network based applications will rely on operation of individual components, their interaction and cooperation.

To achieve the envisioned network, various problems are to be dealt with. As part of this research, three specific issues have been addressed; namely, time synchronization issue in distributed systems, closed-loop control over a resource-constraint wireless network, and Transmission Power Control (TPC) in wireless field nodes. They address the issue linked to limited resources available in distributed field nodes with the aim of maximizing the use of available resources. They will be explained in detail later.

The next section provides an overview of the automation technology and the oil and gas industry before identifying the need to address the aforementioned issues.

1.1.1. Automation and Oil and Gas Industry – An Overview

Automation

Automation technology generally refers to the integration of machines into a self-governing system, whereby the task of process operations is achieved without human intervention (Groover, 2009). To substitute for human effort and intelligence,

automation technologies depend on information technology and control systems [Jämsä-Jounela (2007), Samad *et al.* (2007)]. The term automation has its roots in manufacturing. Within this thesis, however, its use is confined to process automation.

Oil and gas operations

The operations of Oil and Gas Industry (OGI) can be divided into: *Upstream*, *Midstream* and *Downstream*. Upstream refers to the processes involved in OGI operations ranging from exploration, drilling, extraction and post production treatment of wells in both onshore and off-shore platforms. Midstream operations involve storage and transportation. Some processing also takes place at this stage as the oil wells produce oil, natural gas and water which need to be separated before routing to destination storage locations (Nicholls *et al.*, 2008). Oil and gas are two products which need storage. The extracted oil and gas can either enter a flow line or be stored in containers for transportation to destination. At the destination, downstream, the separation and refining of hydrocarbons take place in refineries. Once the products are separated they are distributed to the consumers via a distribution network which may be a gas distribution network, cargo docking station or other outlets.

Figure 1.1 depicts these operations. The use of communication technology is vital for information sharing within each component of operations and with the monitoring and control centre, which can be on-site or remotely located. The communications technology varies because of the hostile environment and widely distributed nature of these operations. The use of Supervisory Control and Data Acquisition Systems (SCADA) to monitor and control these activities utilize various wired and wireless communication technologies. In some deployments, wireless communication technology may be the only available technology for remote monitoring such as in infrastructure monitoring of gas pipelines. Many activities carried within each of these components, however, require local communication within a field for the purpose of data sharing between sensors, actuators and local controllers. These applications include well-head pressure monitoring in upstream, tank farm level monitoring and control in midstream, and temperature control at tanks to avoid cold spots in downstream. There are numerous such applications found in the industry.

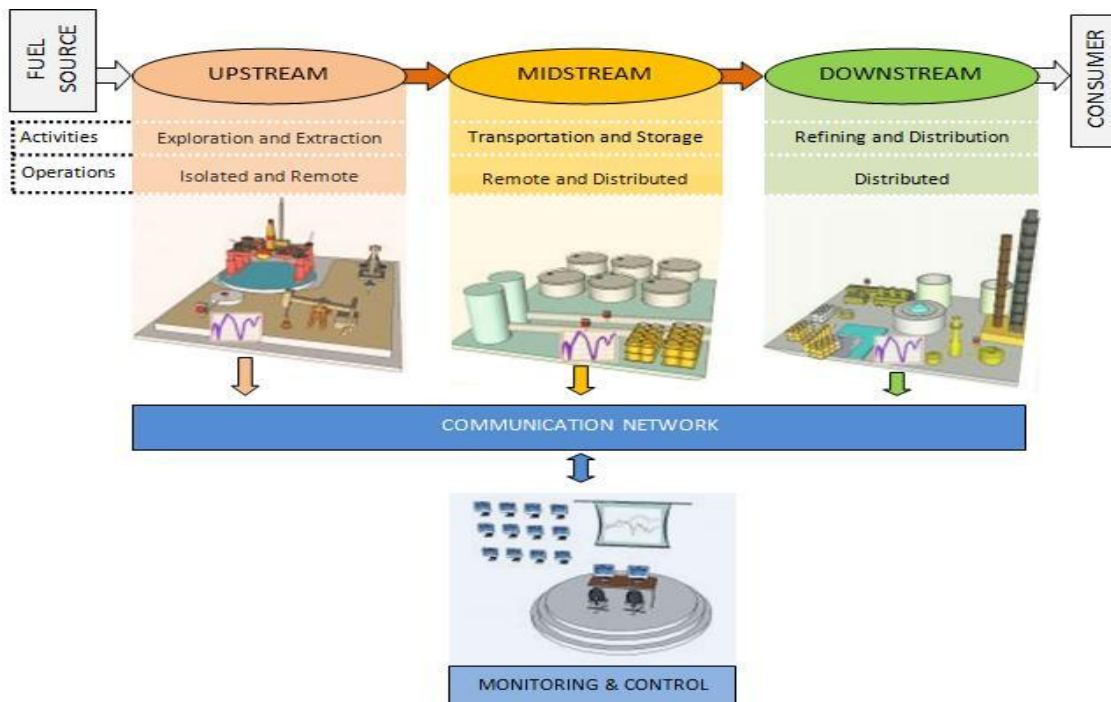


Figure 1.1. Operations in oil and gas industry.

Hierarchical structure of the research domains

The three key research issues investigated as part of this study are highlighted in Figure 1.2. It demonstrates the hierarchical structure of the various technologies and engineering fields which are involved in process automation, and the research categories of interest within this research. Industrial automation can be divided into two streams: process automation and factory automation. The factory automation involves the execution of tasks within a production cell, and is beyond the scope of this thesis. Process automation is the use of information technologies and control systems to help process industries to operate efficiently and safely (ABB, 2006). Within the communication domain, wireless communication technology is of interest to this research. Various short-range and long-range solutions exist. This research, however, primarily focuses on short-range communication technologies. Establishment of a secure and reliable network with longevity for standalone battery operated telemetry units is a research category within this area. Two problems linked to this research category addressed in this thesis are about time synchronization and transmission

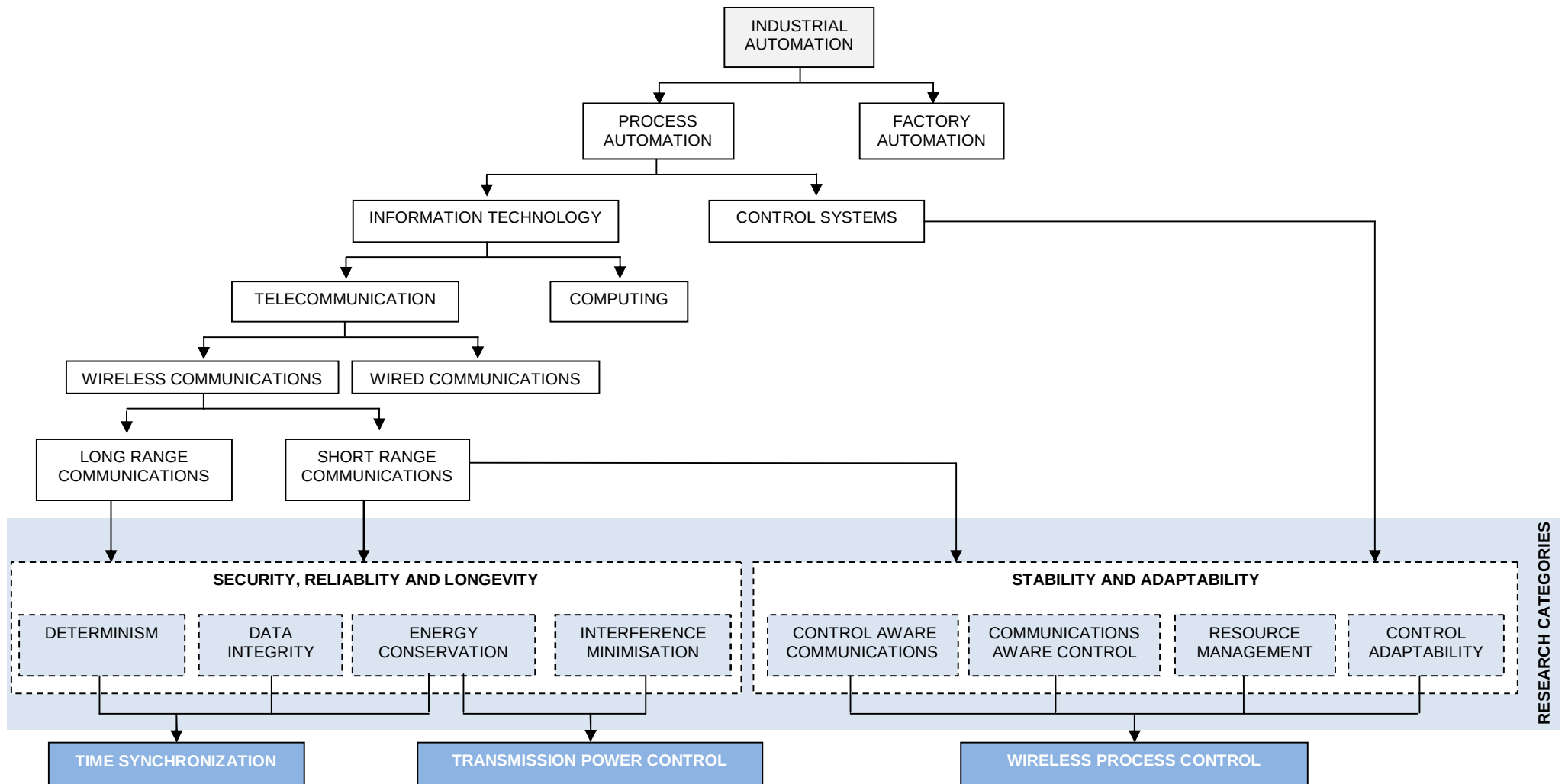


Figure 1.2. Hierarchical view of research categories within industrial automation and the problems addressed in this thesis.

power control. They deal with the issues linked to both application requirement and networking requirement, and are vital for successful network operations. Another dimension of this research is about running a closed-loop control over a resource-constrained wireless network which requires stability of control-loop and adaptability to changing environment. Initially, this requires translating the application requirement into networking requirement to ensure adequate control performance. Afterwards, during run time operations the wireless channel can be subjected to noise which affects the QoS and requires the application to seamlessly adapt to these changes. These problems and the subdivisions within each category highlighted in Figure 1.2 will be described in detail in the following sections.

1.1.2. Time Synchronization in Distributed Wireless Systems

Wireless telemetry instruments are deployed to monitor real-world phenomena, and are experiencing a growing demand in the industry. The range of operation of these devices varies from short range WirelessHART instruments, medium range UHF/VHF instruments, wider range GSM/GPRS instruments and range independent Satellite based telemetry instruments. A typical wireless sensing unit comprises sensor(s), processing unit(s), radio-transceiver(s), memory and a battery (Karl *et al.*, 2007). In addition to the resources available on-board to achieve this task, other requirements include precise time information at the node, which is a middleware service, often provided at the expense of increased protocol complexity and the burden on the network resources (Yick, 2008). Time synchronization is important from application, networking, security and coordination perspectives. It can ensure safe operations and efficient utilization of limited resources.

1.1.2.1. Clocks in Distributed Systems

Problem with a quartz clock

The quartz clock as normally found in electronic equipment is essentially a timer that counts oscillations in an accurately-machined quartz crystal (Sundararaman *et al.*, 2005). Most of these hardware clocks have low accuracy and large drift because of inaccuracies in the crystal frequency due to factors like temperature, magnetic field, humidity and acceleration. As the accuracy depends on operational environment it may

lead to a higher offset in an industrial deployment [Sundararaman *et al.* (2005), Elson *et al.*, (2003)]. In a distributed wireless network, timers run at slightly different frequencies leading to divergence from one another known as *clock skew* (Sundararaman *et al.*, 2005). Clock performance is measured in Parts per Million (PPM). Commonly used oscillators found in computers have nominal frequency accuracy in the range of 1PPM to 100PPM, which may result in a drift between 0.1 and 10 seconds per day (Uchimura *et al.*, 2007). As the standalone telemetry instruments are required to operate in the field for longer period of times ranging from months to years, this random drift in frequency and also its dependence on aging becomes a key concern and needs addressing.

Challenges of time synchronization in wireless instruments

The issue of time synchronization has been widely studied in distributed systems. However, the solutions developed for wired solutions are not directly applicable to a Wireless Sensor Network (WSN) because of the uncertainty linked to the wireless channels and the available resources. The problem with time synchronization is not only limited to process industry but it is encountered in power industry as well, where to ensure power transmission security it is vital to monitor oscillations. Wide Area Monitoring Systems (WAMS) are used to monitor oscillations in the grid and make the data available to host application for analysis (Zhang *et al.*, 2010). The need for common reference is a must in these systems, and is achieved using Global Positioning Systems (GPS). This solution is not applicable to wireless instruments which do not have clear line-of-sight to the sky, such as the flow meters and pressure sensors used in pipeline condition monitoring. These standalone modules are also restrictive in terms of onboard energy available for operation, and GPS modules require considerable energy and time to operate.

Furthermore, the comments from Sundararaman *et al.* (2005) identify that limited bandwidth, hardware limitations, protocol complexity, network topology and unstable network connections are time synchronization challenges.

1.1.2.2. Summary

To ensure data integrity, reliability, security and real-time operations of these wireless networks time synchronization becomes mandatory. Time synchronized operation of

these networks is a prerequisite and requires a low-cost and low-power solution. To achieve and maintain time synchronization in a resource-constrained distributed wireless network is a challenge. Existing approaches based on time synchronization protocols have been able to address application specific solutions, but they have shortcomings [Ranganathan *et al.* (2010), Sundararaman *et al.* (2005)]. There is a need for a new solution for time synchronization which is scalable, energy-efficient, topology independent, fast convergent and less application dependent, a view shared by many researchers such as Ranganathan *et al.* (2010), Chen *et al.* (2011) and Sundararaman *et al.* (2005). Furthermore, the solution has to ensure operability without the restriction of line-of-sight. It is an important requirement for utility companies because infrastructure monitoring of underground pipeline networks uses field instruments that are housed indoors or deployed underground.

1.1.3. Process Control over a Wireless Network

Wireless communication is already used in process automation for process monitoring. The next stage of implementation of wireless technology in industrial applications is for process control. Many researchers like Han *et al.* (2010), Jafari *et al.* (2011) and Park *et al.* (2011) are exploring this area and some preliminary results have also emerged. However, many issues are yet to be addressed. Earlier, the need for modular and flexible system design for control systems at reduced cost paved the way for distributed control systems, where the information is exchanged over a communication network (Yepez *et al.* 2003). These networks have evolved over years, initially from a pair of twisted wires required for each device to a single bus based fieldbus technology where multiple devices share a common communication medium (Han *et al.* 2010). A *fieldbus* refers to a family of communication protocols especially designed for real-time distributed control applications. The advantages of these fieldbus based Networked Controlled Systems (NCSs) compared to traditional point-to-point links include [Wang *et al.* (2010), Calandrini (2002)]:

- Lower installation cost due to reduced cabling
- Ease of installation and expansion
- Reduction in complexity, and
- Increased reliability and efficiency.

Now, the need for Wireless Networked Control Systems (WNCS) has evolved because of the necessity for extensibility, mobility, modularity, flexible installation, fast deployment, and reduced installation and maintenance cost [Han *et al.* (2010), Mazumder (2011)]. They will be further explained in Section 1.2.1. These benefits are only applicable given that the wireless network of choice can meet the strict requirements of process control applications, which are the key barriers for moving from monitoring only to closed-loop feedback control.

1.1.3.1. Wireless Networked Control Systems

Problems with wireless networks in process control

There are three subdivisions in control category, namely: open loop control, supervisory control and regulatory control, in the order of increased reliability requirement from the network (ISA, 2009). Within this thesis, one application of interest is regulatory control, where the feedback control is used to govern the output of a process. In a Networked Control System (NCS) the field devices which include sensors, actuators and controllers are interconnected by a communications network. In a feedback control loop as depicted in Figure 1.3, a distributed sensor measures the process and conveys the information to the controller. Based on this measured value and the desired reference value, the controller computes the required operating value for the actuator, and conveys the data to the actuator to adjust the process accordingly.

The network required to operate at this level must have reliable and deterministic operation. The book by Hristu-Varsakelis *et al.* (2005) explains that the data between these field devices needs to be delivered periodically and at pre-determined times. The delays introduced by the network from the point of data generation to the delivery are referred to as network induced delays. These delays have to be deterministic, and lower in magnitude compared to the application sampling interval. Randomly varying network induced delays can degrade a system performance and can even lead to system instability [Hristu-Varsakelis *et al.* (2005), Yezpez *et al.* (2002)]. Moreover, in a shared medium, data loss may also result due to packet collision, interference and higher channel noise. This can be considered as a special case of network induced delay where time approaches infinity (Yang, 2006). A wireless network in general is more susceptible than a wired network to delays especially if operated in the ISM band where

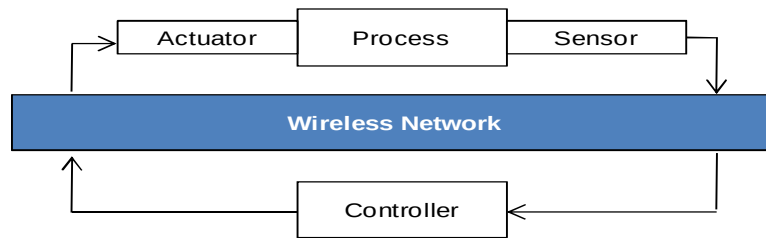


Figure 1.3. Feedback control loop operating over a wireless network.

multiple networks and applications share the same radio spectrum. Timeliness of data delivery, reliability, security, and QoS is a must for the use of wireless in process control. It is difficult to achieve these objectives, because of the properties of the radio channels, limited network resources and the need to ensure co-existence with other networks utilizing the same unlicensed frequency band.

Challenges

An accurate and timely delivery of feedback data without significant data loss is a challenge for incorporating wireless communication in process control. A faster communication speed is not enough to meet the real-time constraint because the process data involves frequent generation of small data packets. The network must be able to support the required sampling interval, which is not possible to be achieved without a certain network capacity and bandwidth. The sampling period and loop execution depends on the process response time which may vary from milliseconds to minutes (Chen *et al.* 2008).

The use of wireless communication in NCS raises the following concerns, and addressing them is a challenge [Mazumder (2011), Hristu-Varasakeli (2005), Chen *et al.* (2010)].

- How to handle and minimize packet delays induced by a wireless network?
- How to avoid packet dropout which may result during network operations?
- How to ensure longevity of battery operated wireless field devices?
- How to ensure co-existence with other devices operating in same radio band?
- How to avoid network congestion?
- How to avoid connection outages, and
- How to adapt control strategy under varying channel conditions while ensuring performance and stability?

Some of these issues will be examined in this thesis in order to achieve required application performance. In short, the interactions between systems, interlinks, network scheduling, topology and controller implementation and its scheduling are vital part of successful control operation.

1.1.3.2. Summary

Fieldbus networks are deployed as a default for use in wired based NCSs. They are designed for process control applications and serve short-distances with high reliability. Replacing them with wireless technology requires a careful design of the network infrastructure and protocol to ensure adequate control performance. It has to operate in a harsh industrial environment, needs to be robust, have low power requirement and must provide adequate coverage. Security becomes critical as the radio wave signals are easy to receive. The additional requirements of control applications are data accuracy, timeliness of message delivery and its availability.

1.1.4. Transmission Power Control

Efficient utilization of radio resources is up to the Radio Resource Management (RRM) strategy. One such radio resource unit is transmission power level (Gbor *et al.*, 2009). This involves the adjustment of transmission power level at the transmitting node to a minimum level which can ensure successful communication without affecting the performance. The algorithms used to achieve this are referred to as TPC algorithms. TPC mechanisms are used to achieve various objectives, such as (Callaghan *et al.* 2006):

- To *reduce energy consumption* of mobile terminal and to prolong its battery life
- To *reduce co-channel interference* in a shared medium to enable coexistence and overall improve spectrum efficiency in both fixed and mobile applications, and
- To *address the fading issue* during adverse channel conditions while maintaining the Bit Error Rate.

1.1.4.1. Power Control

Problem formulation

TPC algorithms rely on the availability of selection of transmission power levels at the transmitter. For fine-grain TPC algorithms this is often a limiting constraint because the commercially available transmitters often have few available power selection levels. Additionally, the regulatory requirement also imposes limits on the maximum power level allowed for transmission. The lower limit to the available power levels is often specified by the wireless communication standards. Generally, lowering the transmission power will affect the received power, which will influence the performance. However, the transmission power can be adjusted to a minimum level while still obtaining the performance of a given QoS class. To estimate the minimum power required for successful communication it is vital to account for the gains and losses from the transmitter through the medium to the receiver. This calculation is called a *link budget*. If the received power is near receiver sensitivity, then packet error rate will rise. The amount by which the received signal power exceeds the receiver sensitivity is referred to as *link margin*, and has to be selected taking into consideration the fluctuations in the received signal value.

Figure 1.4 depicts a generic control structure for TPC. To the left in the figure is a transmitter operating at a transmission power level of P and the received signal represented by S . The wireless block here represents the signal attenuation as it propagates through the wireless channel.

Equation 1.1 which is adapted from Ares *et al.* (2007) represents the relationship between the transmission power and the receive signal given in dBm. dBm is the power ratio given in decibels of the measured power referenced to one milliwatt. Here, the first term P on the right corresponds to transmission power. The second term L_p corresponds to path loss in dB, which entails free-space path loss and other losses dependent on the time and physical environment. The third term ζ is the shadowing component. The last two terms G_{Tx} and G_{Rx} refer to antenna gains at transmitter and receiver.

$$S = P - L_p + \zeta + G_{Tx} + G_{Rx} \quad (\text{dBm}) \quad \text{Equation 1.1}$$

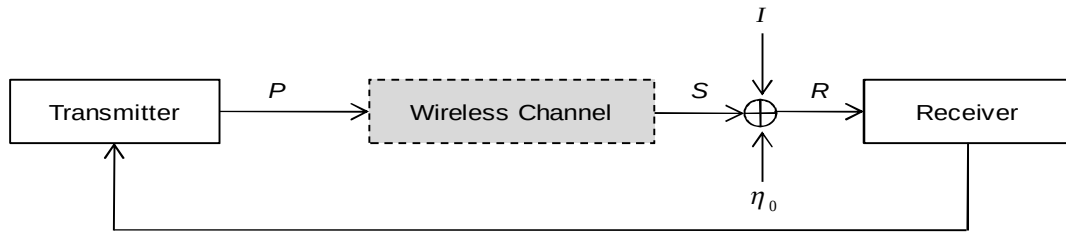


Figure 1.4. Transmission power control loop. After Ares *et al.* (2007) and Alavi *et al.* (2009).

The receive signal then gets subjected to interference I and noise η_0 at the receiver, and the final value reported as Received Signal Strength Indicator (RSSI) by the receiver. The term I takes into account interference-powers from co-channel interferers. The implementation details mapping RF receiver register value to RSSI are omitted here as they are hardware specific.

In order to adjust the transmission power to a minimum level, it is vital to assess the link quality. Wireless *link quality* refers to the communication performance of a radio channel which changes significantly with time and environment (Lin *et al.* 2009). Changing link quality will affect link margin and has to be monitored and adjusted.

To summarize, in a fast changing environment and with limited resources, a TPC algorithm is required which can quickly adapt to network changes, is independent of hardware module used, supports multi-channel operations and can prevent network outage under channel fading conditions.

Challenges

The topology in an industrial wireless network may vary from simple star topology to multi-hop mesh network based on the application demand. Therefore a decentralized TPC approach is preferred. Moreover, the TPC algorithm needs to operate over all the available channels, a maximum of 16 in 2.4 GHz band, and needs to adapt to the changing environment. As shown in Figure 1.5, each node will have its neighbor's information such as its unique identification number, allocated time slot and channel number stored in communication tables. For each neighbor and for all available communication channels, a set of minimum power levels has to be estimated to ensure successful communications. This list linked to transmission power level needs to be dynamically adjusted to compensate for environmental changes.

The requirement for TPC is to estimate minimum transmission power level while ensuring (i) minimum overhead linked to TPC (ii) adaptable to all channels and changing conditions (iii) prevents outage and is reactive (iv) independent of hardware platform, and (v) adaptable to asymmetric links, varying transmission power levels and sensitivity threshold of the receiver.

1.1.4.2. Summary

TPC is important from networking perspective and can address interference and fading issues while ensuring longevity. The transmission power if feasible can be lowered to reduce the energy consumed during transmission. However, it can have an adverse effect on the application performance if the transmission power is insufficient to yield a receive signal strength above the receiver sensitivity. It is, therefore, important to calculate the link budget. Furthermore, interference affects the receiver ability to successfully receive the transmitted signal. It is, hence, important to keep track of link quality and make necessary adjustments in transmission power level to ensure adequate performance of a given QoS class. In an industrial environment, the fast changing link quality from one channel to the other and the effect of interference on some channels compared to others for TPC has to be considered. Therefore, a TPC algorithm is required which can adapt to changing radio environment, is quick to respond, is lightweight in terms of communication and computational needs, works on pair-wise basis, and is practical.

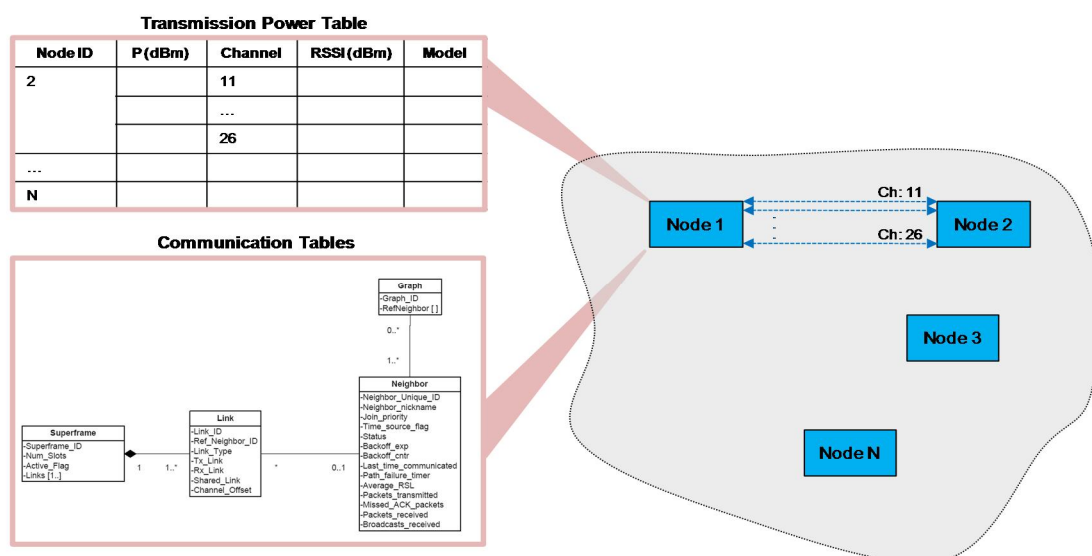


Figure 1.5. Tables for communication in a network. Adapted from Chen *et al.* (2010).

1.2. Motivation for the Research

This section presents an overall motivation for the research. It begins by providing an overview of the development of communication technology in process automation. The text then examines the industrial perspective on wireless technology alongside with its key drivers for adoption in process automation. Afterwards, the motivations for three distinct research problems which are addressed in this thesis are outlined. An overview of these drivers and the difference in theory and practice provides a motivating case for the research.

1.2.1. Wireless Technology in Process Automation

Overview

Global competition is driving the industry to continuously improve process operations, product quality, productivity, reliability and compliance with regulations [DoE (2002), William (2010)]. A key driver for the adoption of wireless communication technology in the process industries is access to enhanced process information to help in meeting these targets. Plant knowledge can be increased by acquiring additional measurements from the underlying processes and equipments, and wireless communication networks can assist the process industry to gather more data by providing low-cost connectivity when wired communications would be infeasible [Johnston and Munns (2008), Emerson (2009)].

Present communication technologies found in process automation are mainly based on wired networks and have their limitations. Problems with wired communications technology include the following [Ferris (2010), Hartebrodt *et al.* (2004), Akerberg *et al.* (2011)]:

- Higher planning, installation and maintenance cost of the network.
- Inflexible infrastructure due to fixed connections.
- Difficulty in troubleshooting connectors.
- Higher connector failure rates.
- Wired networks have to be designed with spare capacity on cards, marshalling cabinets and junction boxes to cater for future expansion.

- Inaccessible locations such as on or inside rotating equipment.

By contrast, some advantages of wireless communications technology are [Ferris (2010), Flammini *et al.* (2008), Forgue (2010)]:

- Wear-and tear free data transfer.
- Lower installation and maintenance costs. Up to 90% reduction in deployment cost compared to wired counterpart according to Emerson (2009a).
- Deployment in mobile and rotating equipment or in hostile and remote locations.
- Temporary deployments as the network nodes do not require physical infrastructure.
- Deployment of MEMS (Micro-Electromechanical Systems) technology, advantages of which includes: cost efficiency, low power, high performance sensing and integration.

The aforementioned points suggest that wireless technology can assist the process industries to overcome the limitations of wired networks and to benefit from the flexibility in infrastructure it offers at a reduced maintenance cost. Wireless communication is one of the fastest growing technologies in process automation (Humphrey *et al.*, 2008).

The observed trend in communication architecture

The trend in the communication technologies used in process automation has seen a drive towards reduction in the amount of cabling required for communication and the supported infrastructure. Figure 1.6 depicts the trend as seen in communication architecture found in process automation. The dotted line represents an optional wireless link, whereas, the solid lines represent wired communication links. As can be seen from the Figure 1.6, the move from 4-20 mA current loop (i.e. commonly used analog sensor signaling standard) to the fieldbus technology offered considerable reduction in required cabling, and this next phase of transition using wireless technology further eliminated most of the cables.

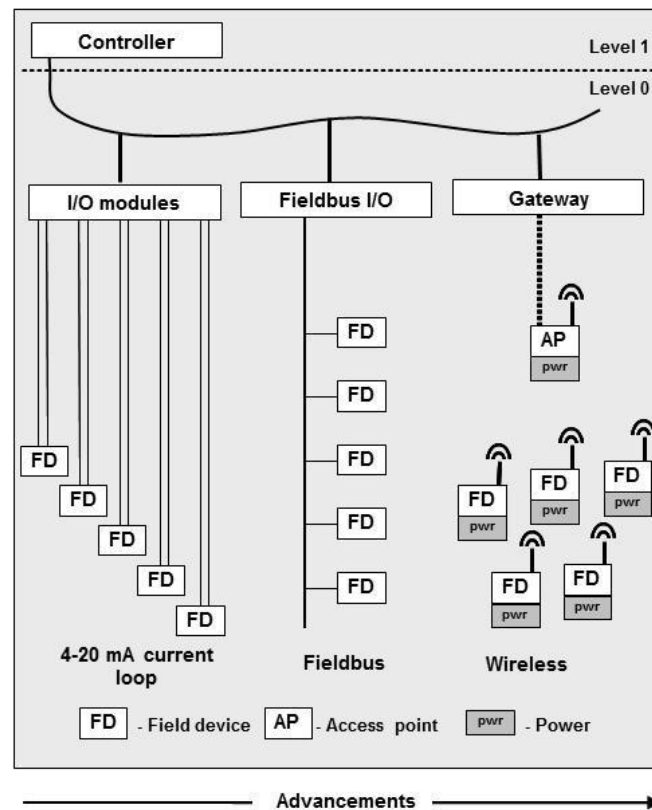


Figure 1.6. Comparison between conventional 4-20 mA current loop, fieldbus and wireless communication architectures. After Ferris (2010) and, Kennedy and Mistry (2003).

Industrial concern and current adoption

In industrial applications, any problem with the equipment or plant translates into economical loss. Hence, if the equipment is operated wirelessly, the reliability and availability of the network is of importance [Carlsen and Petersen (2010) Doyle *et al.* (2007), NAMUR (2011)]. Equipment and systems used must provide reliable services, and the operational and support cost must be kept to the minimum [EH (2010), Siemens (2010)].

The commonly found communication technologies used in commerce are not well positioned to offer such services to industrial applications, such as timely message delivery, security and data integrity. To design a network which can offer such services has stimulated research in industry and academia. As a result, various standards have emerged to address these needs such as WirelessHART, ISA100.11a and WIA-PA [IEC (2010), ISA (2009), IEC (2009)]. More information about these standards is available in Section 2.4.

The current focus on wireless technology for process automation has concentrated primarily on non-critical monitoring applications. The next phase of this extension is avenue of control over a wireless network and overall integration of these distributed systems. For a typical oil and gas installation around 55% of field instruments data are linked to closed-loop control according to Petersen *et al.* (2011). Therefore, running a closed-loop control over a wireless network is the natural extension and is subjected to new challenges and concerns linked to wireless network reliability and availability. These issues have to be dealt with in order to use wireless technology beyond non-critical monitoring applications. This thesis is a work towards addressing some of these unique challenges, and to identify the difference between theory and in-situ practice. In addition, a review is also provided comparing the standing of existing standardized state-of-the-art wireless communication technologies and their suitability for process automation based on outlined requirements analysis.

The motivation behind each specific research problem is identified in the following sections.

1.2.2. The Need for Time Synchronization

The motivation for time synchronization is two-way: firstly, due to the distributed nature of wireless telemetry there is a need for a solution which is energy-efficient, topology-independent, scalable, fast convergent and less application dependent. Secondly, the increasing sophistication in field equipment and their wider coverage and heterogeneous nature calls for a global time synchronization solution. Within this context, the use of time synchronization is not limited to short range communications but also encompasses long-range networking technologies.

Importance of time synchronization and growing demand

Time synchronization is very important in a distributed wireless network for the following reasons:

- APPLICATION REQUIREMENT:

The application in context could be a wider area network application covering entire city such as infrastructure monitoring of a pipeline network for a utility

company or confined but spatially distributed instrumentation network in a refinery or water-treatment plant, and even limited to a building or office workspace. An application requirement to integrate the data collected from distributed field instruments requires accurate time stamps. It can be seen from Figure 1.7 that the data is first collected from a process, such as oil and gas pipeline flow measurement using wireless telemetry units and then communicated to the remote monitoring center wirelessly. At the control center, the aggregated view of the underlying process is visualized and any discrepancy in the process measurements is highlighted. To ensure data integrity it mandates the need for time synchronization across the network. *Data integrity* within this context covers both the actual data and the associated time stamps.

- NETWORKING REQUIREMENT:

Time synchronization is also important to offer contention free, deterministic and correlated operation of the field devices (Doyle *et al.*, 2007). In case of wireless networks some resources are time-varying, some are fixed, while others are limited. Time-varying shared resources include channels. They are shared amongst the participating nodes and have to ensure co-existence. Similarly, onboard buffer and memory are also fixed in wireless field nodes. In addition, for battery operated wireless instruments, it is vital to maximize the lifetime of field devices by minimizing the consumption of limited onboard battery power. Therefore, it becomes a challenge to actively and effectively manage both radio resources and on-board finite and limited resources. Time synchronized communication can ensure determinism and efficient channel utilization (Wang *et al.*, 2008).

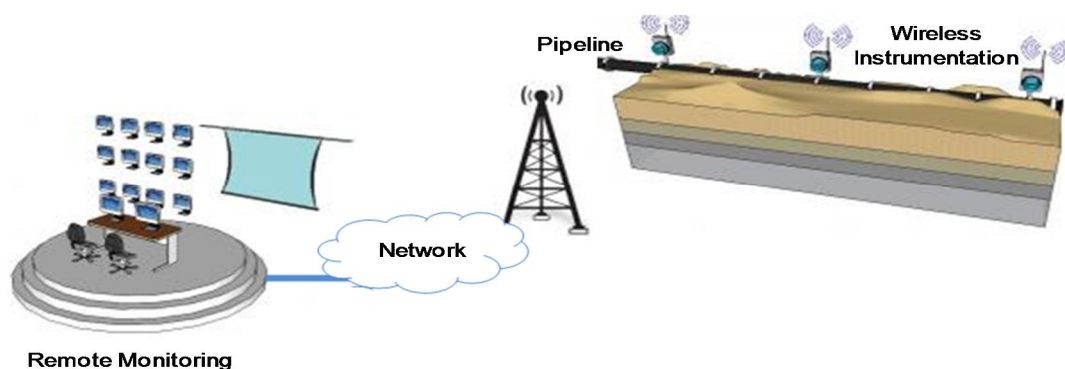


Figure 1.7. Open-loop control system demonstrating remote monitoring.

- SECURITY AND COORDINATED OPERATIONS REQUIREMENT:

Time synchronization is crucial in cryptographic devices for various aspects such as planning, security and managing network. The authentication schemes rely on time synchronization to prevent against replay and delay attacks, and other forms of circumvention from adversaries (Tilborg and Jajodia, 2011). In addition, for network devices to coordinate amongst themselves and to assign tasks to each other time synchronization is needed. Authors like Vedantham *et al.* (2006) have highlighted the importance of synchronization and coordination mechanisms followed by the hazards which may result due to out-of-order execution of commands and lack of coordination amongst the field devices, emphasizing its importance in closed-loop control systems.

Briefly, wireless telemetry instrumentations are deployed to monitor real-world phenomena, and are seeing growing demand in industry. Time synchronized operation of these networks is a prerequisite and calls for low-cost and low-power solutions.

1.2.3. Towards Wireless NCSs

The benefits of wireless technology paved the way for its use in process monitoring applications and are now seeing industrial interest towards its use for control applications. Traditional control systems operate at fixed rate and assume that the communication networks offer instant communication service without data-loss [Yang (2006), Bai *et al.* (2011), Arzen *et al.* (2006)]. This assumption in control implementation is valid given that the dedicated point-to-point communication links are used. However, the use of shared communication networks in control loops violates these arguments [Bemporad *et al.* (2010), Hristu-Varsakelis (2005)]. It is because in a shared network the data packets are subject to network induced delays, processing delays, and may even experience data-loss [Yepez *et al.* (2003), Pennington *et al.* (2009)]. These delays can degrade a system performance and can lead to instability [Kim *et al.* (2007), Zhang (2001)]. Therefore, they have to be carefully taken into consideration in NCSs design. To move from monitoring only to closed-loop control is a leap forward and imposes certain constraints on the network.

Advancements in control technology

Figure 1.8 depicts the advancements as seen over last few decades in automation technology. The move from pneumatic control was superseded by 4-20 mA analog loops and later complemented by 4-20 mA smart networks. The drive for reducing the cabling required and minimizing maintenance cost led to the arrival of fieldbuses. All of these succeeding technologies were based on industrial drive and advancements as were observed in communication technology of time. The current phase to this evolution is adoption of wireless technology which brings alongside unique research challenges. It can be seen from Figure 1.9 that the use of networked and embedded control systems has evolved over time. The control which initially resided in a central computer as in Direct Digital Control (DDC) systems was later distributed in the case of Distributed Control Systems (DCS). Additionally, the use of fieldbuses in Field Control Systems (FCS) provided a provision to move the control in a field device like in the case of Foundation Fieldbus (FF, 1999). The questions which the research community is trying to address are: how this block of WNCS will appear in time to come: which wireless technology would be applied, what would the configuration be, where the control will reside, the performance limits of control operation over a wireless network, and the suitability of both periodic and event-triggered control strategies [(Park *et al.* (2011), WiCon (2010), Jafari *et al.* (2011), Xia *et al.* (2008), SGER (2008), Gupta *et al.* (2010), Georgiev (2003), Johansson (2009))].

In order to restrict network induced time delay, ensure reliability and availability, certain boundaries are required in scheduling and topology control. Moreover, to determine which of the various available standards is best suited to address the need for industrial control is amongst the key motivation for this avenue of research.

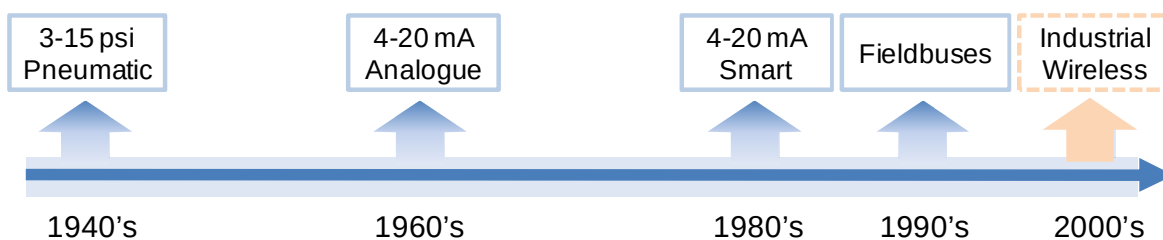


Figure 1.8. Timeline of network evolution in measurement and control technology, after Sai (2009) and, Kennedy and Mistry (2003).

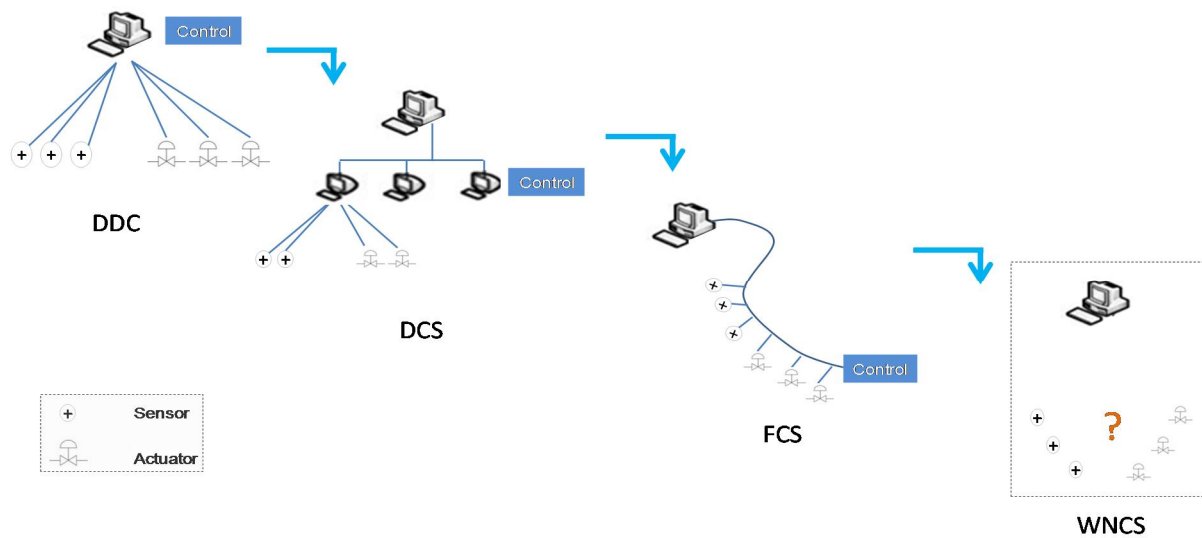


Figure 1.9. Evolution in network architecture, after Georgiev (2003) and Sai (2009).

The academic papers which have dealt with this research issue are either mostly theoretical papers like Nair *et al.* (2007), Hespanha *et al.* (2007) and Schenato *et al.* (2007), while others have considered moderate requirements for control application as in HCF (2009), Han *et al.* (2010) and Chen *et al.* (2010)]. An effort towards bridging this gap is a drive behind this research.

1.2.4. The Incentive for TPC

The motivation for TPC in short-range, low-power industrial wireless networks can be summarized as follows:

- ENERGY SAVINGS:

TPC can offer significant energy savings as opposed to transmitting at a fixed power level given that there is a window of opportunity. It depends on communication distance, available transmission powers, interference and receiver sensitivity. The contribution of the energy saving becomes apparent for devices which require fast update rate. It is demonstrated through a graph in Appendix A1.1.

- IMPROVED RECEIVER SENSITIVITY:

The minimum sensitivity of the receiver as defined by IEEE 802.15.4 standard is -85 dBm and the best case theoretical sensitivity can be -113.2 dBm (Lanzisera *et*

al. 2007). Devices which support up to -104 dBm sensitivity are available (Meshnetics, 2007). This improved sensitivity offers an opportunity for TPC and is shown and discussed in Appendix A2.1.

- DIFFERENTIAL TRAFFIC MANAGEMENT:

In a process automation application where sporadic and periodic traffic coexist during normal operations, a mechanism is required to prioritize the safety-critical data. The use of higher transmission power for safety-critical data and lower power for the rest can result in higher probability of success (Douros *et al.* 2011). Therefore, signal to interference ratio can be adjusted accordingly for each node.

- INDUSTRIAL PROTOCOLS:

The industrial wireless standards incorporate the provision for TPC but do not specify the details [ISA 100.11a (2009), IEC (2010), IEC (2009)]. It is an avenue of research and can result in considerable energy savings given that the demand for fast sampling applications is on increase, due to the move towards control applications.

1.2.5. Summary

This section has provided an outline of the key motivations behind the adoption of wireless technology in process automation. It begins by providing a brief overview of the current state of the communication technology and highlights the new avenues of research. The motivations behind three distinct research problems which are addressed within this thesis are summarized. Advances in wireless communication technology coupled with the need for enhanced process monitoring is driving the research in wireless process automation systems. On one hand, the use of wireless technology has widened the application horizon of process automation applications by minimizing the economical and physical barriers linked with traditional wired systems. On the other hand, their use in conventional closed-loop control application has raised new concerns and challenges due to the limited available shared resources onboard.

Based on the driving motivation covered here, the next section will outline the aims and objectives of this research.

1.3. Aims and Objectives, Requirements and Challenges

This section starts by elaborating on the aims and objectives of this research, which are based on the issues mentioned earlier, and the drive to address these problems mentioned in the motivation section. Next, it provides information about the requirements for using wireless technology in process automation. It has two-fold objectives. Firstly, it will identify the requirements which are to be adhered to during the formulation of the algorithms. Secondly, it will provide a benchmark to evaluate the relative standing of the existing wireless communication technologies and identifying their shortcomings, which will be discussed in the next chapter.

1.3.1. Aims and Objectives

Aims

Plant knowledge can be enhanced by acquiring additional measurements from the underlying processes and equipment, and the advancements in standardized wireless communication technology have enabled the process industry to do so. However, its adoption is still in early stages, and many issues and challenges remain, as were discussed in the previous sections. The research in the thesis concerns the performance of a network-based application arising from limited network resources. The thesis addresses the following:

- Time synchronization issue in distributed wireless networks. The aim is:
 “To design a solution for time synchronization of nodes in a distributed system, while ensuring that it is *energy-efficient*, *scalable*, *topology-independent*, *available* and *fast-converging* time synchronization solution”.

The key words in this aim are *energy-efficient*, *scalable*, *topology-independent*, *available* and *fast-converging*. *Energy-efficient* implies the need for a mechanism for time synchronization of network nodes which is light in terms of energy required for communication, computation and operating supporting circuitry. *Scalable* highlights the requirement of extensibility, so that the number of network nodes is not restrictive. Further, *topology-independent* operation requires the decoupling of the time synchronization mechanisms from underlying network topology. For evolving networks it is an important criterion. It also needs to be *available* which emphasizes on its

coverage and continuity of operations. Finally, *fast-converging* solution highlights the need for a mechanism to swiftly converge the entire network to the same notion of time.

- Resources constraint on wireless closed-loop control performance. The aim is:
 “To identify the *suitability* of standardized wireless networks for use in process automation, and to formulate a mechanism for running a *closed-loop control* application over a *resource constraint* wireless network”.

The key words mentioned above are *suitability*, *closed-loop control*, and *resource constraint*. Within this context, *suitability* refers to the examination of existing short-range licensed-exempt standardized wireless technology against the requirements of using wireless in process automation. It will identify the technologies which are considered eligible for use in process automation. *Closed-loop control* highlights the specific class of interest belonging to process automation. *Resource constraint* highlights the limited resources available to network nodes, both on-board and shared network resources which affect the application performance.

- Varying channel condition and its impact on TPC. The aim is:
 “To develop an algorithm for transmission power control in wireless instruments which can adapt to changing radio environment, is quick to respond, works on pair-wise basis, is vendor-independent, and practical”.

The key words in this aim are *adapt*, *quick*, *pair-wise*, *vendor-independent* and *practical*. *Adapt* signifies the need to adjust to varying radio link quality. *Quick* highlights the importance of timely adjustments of transmission power and also refers to proactive measures needed to avoid network outages. Furthermore, *pair-wise* operation is a requirement for independent operation of nodes without the need for a coordinator to manage the operation. It is important for decentralized operations. *Vendor-independent* solution here implies the need for an algorithm which works on standardized transceiver hardware compliant with IEEE 802.15.4 physical layer. Finally, *practical* here summarizes the need for light communication and computational demand.

Objectives

The aims mentioned above are further broken into number of objectives:

- TIME SYNCHRONIZATION:
 - Identification of different approaches available for time synchronization.
 - Identification of solutions which offer topology-independency.
 - Identification of solutions which are scalable and fast converging.
 - Identification of solutions which are available.
 - Identification of the sources of error in time synchronization.
 - Theoretical analysis of time synchronization accuracy.
 - Theoretical analysis of convergent time.
 - Theoretical analysis of energy-consumption.
 - Experimental results for the proposed solution.
 - Overall theoretical analysis and validation through empirical results.
- WIRELESS PROCESS CONTROL:
 - Requirements analysis for using wireless in process automation.
 - Identification of closed-loop control requirements.
 - Identification of the control-loop structure used in NCS and industry practices.
 - Identification of standardized short-range license-exempt wireless technologies.
 - Analysis of the suitability of standardized wireless technologies for process control.
 - Analyze the limits of operation of IEEE 802.15.4 compliant network.
 - Formulate a mechanism suitable for process control over resource limited network.
 - Performance evaluation of the proposed approach.
- TRANSMISSION POWER CONTROL:
 - Identification of measures available for wireless link quality assessment.
 - Determine a measure suitable for estimating link quality in IEEE 802.15.4 networks.
 - Feasibility study of the selected measure through empirical results.
 - Determine an approach suitable for TPC.
 - Formulate an algorithm for TPC which is adaptable and practical.

- Implementation of the proposed algorithm and performance evaluation.
- Evaluation of associated energy consumption.

The research aims to address these objectives by formulating algorithms and identify structures which can effectively address the requirements.

1.3.2. Requirements Analysis

Protocols for field network communications in process automation are designed for real-time operation, and must address network requirements for process automation. These requirements can be classified into two categories: *basic requirements* which a network protocol has to satisfy regardless of the underlying media used, and the *wireless-associated* requirements which are linked specifically with the use of wireless technology. These requirements are summarized in Table 1.1 and 1.2.

These below mentioned requirements are for process automation. The key performance indicators such as reliability, latency, stability and availability are of most high concern to the control applications. The other requirements mostly concern compliance with regulations, the network capacity and operations.

Table 1.1. Basic requirements for communications in process automation.

Availability:

Availability as defined by (NAMUR, 2010) is the number of packets arriving at the destination in a predefined time. The availability of network is very critical because information flow is vital to control a physical process or plant. For closed-loop applications belonging to Class1 of ISA-100.11a process automation applications, linked outages of greater than 500ms are intolerable. Availability on demand has to be 99.99% or more according to ISA100.11a.

Data length and bandwidth:

In process automation, typical data length is short and the bandwidth required per node is generally low (Sikora, 2007). These aspects are not usually constraints.

Latency and jitter:

Latency is the time from the packet generation to the reception of packet at the receiver. It is influenced by propagation delay, queuing, and processing delays. Latency has to be less than the sampling time. Jitter refers to variation in the latency. Latency has to be bounded in order to achieve real-time operation, and it will become apparent later that it becomes a design challenge for wireless mesh networks.

Ordering of events:

The orders in which events occur have to be identified for sporadic traffic, and this information is vital for applications that make decisions.

Range and Network Size:

The range is the distance between two communicating nodes (e.g. field devices, controller). It may be tens of meters in process automation applications.

Reliability:

A reliable network protocol guarantees that messages are delivered to the intended recipient. It is a measure of the percentage of data (e.g. sensor data) that reaches its destination (e.g. gateway) (Doyle *et al.*, 2007).

Stability:

It is the percentage of successfully transmitted data packets in a network and takes into consideration packet re-transmissions (Doyle *et al.*, 2007).

Scalability:

The network has to accommodate multiple nodes, hundreds to even thousands in number (Sikora, 2007). Therefore, scalability is a key requirement of a process automation network.

Timeliness:

The network should have the capability to handle and cater for traffic associated with periodic data, sporadic data and configuration messages data (Choi *et al.*, 2008]. Periodic data is sampled data needed for the input and output of control algorithms. This information has to be transported within a given time before a new sample is taken. Sporadic traffic, for example alarm data, when generated has a given bounded deadline for reporting. Configuration messages are non-real-time and are related to network maintenance.

Table 1.2. Wireless associated requirements for process automation.

Coexistence:

International standards have to be taken into consideration when designing a network to operate in a license-free ISM (industrial/scientific/medical) band. Many wireless technologies belonging to wireless local area network and wireless personal area network have emerged globally using the license-free radio spectrum in the 2.45GHz and 5.8GHz bands. Therefore, it is vital to ensure co-existence with these other applications.

Duty Cycle:

Duty cycle refers to percentage of time a node is active in a given period. In process automation it is typically low meaning the nodes are mainly inactive. If all devices are operated as routers, as in a mesh network, then duty cycle will increase when the radio traffic accumulates (Sikora, 2007). The duty cycle has an impact on power consumption and battery life.

Data recovery in case of data loss:

Wireless networks can be affected by noise and interference which can degrade performance of the communication channels, or by data congestion. A wireless network must provide data retransmission or some other method to compensate for packet loss. This may require path diversity, i.e. more than one route to the destination node.

Energy consumption and battery life:

Energy consumption should be kept low if wireless nodes are battery operated. In the process industries a battery life of greater than 5 years is preferred (Kang *et al.* 2008], otherwise, battery replacement will create a maintenance problem. Batteries suitable for industrial environments are commercially available. Battery life can be prolonged by minimizing the amount of transmission.

Interference and temporal adaptability:

Wireless is an open access medium and, therefore, operation in a license-free band network will need to be immune to interference. Adaptability to both short-term and long-term interference is a requirement (NAMUR, 2010].

License free ISM Band:

Wireless radio communication systems within same band and operational vicinity share the medium for data transfer; therefore regulations

exist for deploying wireless systems. Use of certain frequency bands is subject to licensing requirements, whereas other are exempted. More information can be found from the local regulatory body, such as OFCOM in the UK. A widely used license-free band is ISM (Industrial, Scientific and Medical) band. Many industrial standards use the 2.4GHz ISM band which is generally available globally. However, it is important to understand that the availability of channels and transmission power may vary between countries. For instance, in France there is a restriction in channels 10-13, and similarly in Spain for use of channel 10-11 for IEEE 802.11b [Buda (2010), Cisco (2004)]. The transmission power also has different limits in different countries, such as 100mW in Europe and 1 W in United States (Clark, 2004).

Mobility:

The network should offer connectivity to both static (e.g. fixed equipment) and mobile (e.g. user terminal) nodes in the field. In process automation applications, the majority of nodes are static (Sikora, 2007].

Packet error rate:

Packet error rate is the number of erroneous packets received at the recipient within a predefined time (NAMUR, 2010). It depends on the network traffic. The requirement is that it should be minimized.

Reliability:

A wireless network is inherently more susceptible to noise and interference which affects reliability. High reliability is attained by having packets following different transmission paths in parallel. However, such a solution compromises other requirements such as, timeliness. Reliability demands diversity in time, space and frequency (Chen *et al.*, 2010].

Safety:

Radio waves can cause ignition in a flammable environment under certain conditions if the radio wave transmission levels are high (Schultz, 2007). Therefore, signal power must be kept under certain levels as specified in the British Standard BS6656 (2002).

Security:

Information should be encrypted and protected against eavesdropping. Additionally, malicious packets should be identified and discarded.

1.4. Layout of the Thesis

This section gives an outline of the thesis. The focus of this thesis is on improving the overall performance of the automation applications running over a wireless network. In a wireless network all participating network nodes can be considered as systems. Overall interaction and co-operation of these systems affect the application performance. In order to meet the aforementioned requirements, it is essential that each system manages its resources efficiently and independently, at the same time it needs to collate information about the shared-network resources available at its disposal. This mandates the need to manage and allocate network-resources available on demand to individual systems. This collective effort is important to ensure efficient utilization of the limited available resources. Contributing towards this effort, three issues have been addressed and presented in this thesis. The outline of the thesis is as follows:

Chapter 2

This chapter presents an overview of the use of wireless communication technology in process automation and the corresponding usage classes. Furthermore, the commercially available wireless communication technologies are compared and their suitability for use in process automation is evaluated based on the requirements analysis presented earlier. The new protocols designed for industrial applications are reviewed and a comparison amongst these different standardized protocols is presented and discussed. The chapter goes on to identify the strategies adopted by the standardized protocols to make them industrial strength and the commonalities between these standards. In short, this chapter will present the wireless technologies relevant to this research and introduce the concepts and terminologies relevant for the discussion to follow later in Chapter 5 and 6.

Chapter 3

Based on the foundation laid earlier in Chapter 1 and 2, the corresponding related works are presented in this review chapter. The chapter provides a detailed overview of the background and context to the three issues addressed in this thesis. An overview of relevant methods and approaches reported in the literature to address each specific

issue is presented. In short, this chapter collates the information collected from literature reviews to identify the relevant methods, structures and approaches which are promising to meet the research aims set out in this thesis.

Chapter 4

Chapter 4 presents an approach to time synchronize the distributed field nodes (e.g. wireless telemetry units). The proposed approach which is a hardware-assisted time synchronization solution, based on radio clock is explained in detail. A detailed overview of the applicability of the proposed solution and its availability around the globe are discussed. As part of this research, theoretical analysis of the proposed solution is conducted and the results are validated through empirical results. The results show that the proposed solution is energy-efficient, available, topology-independent, fast-convergent and an economical solution compared to the other similar approaches.

Chapter 5

This chapter presents the outcome of the study conducted to evaluate the performance of operating a closed-loop control over a network compliant with IEEE 802.15.4 standard, which defines the physical and medium access control layers of the communication stack and are employed by the industrial wireless standards. An analysis of the limit of this standard in terms of the throughput constraint is highlighted which is important for control application. It further goes on to explain the outcome of a case study conducted to quantitatively analyze the performance of a control loop running over a wireless network both through simulations and also through hardware in the loop tests. It further highlights the importance of a co-design approach and how it can address the issue of unpredictable network behavior.

Chapter 6

This chapter proposes a new algorithm for TPC in wireless instruments. Within this context, the wireless instruments in question are those which are compliant with IEEE 802.15.4 standard. First, an investigation into the industrial requirement concerning TPC is presented along with the limitations of the hardware on which the algorithm is meant to operate. Next, the basis of the formulation of TPC algorithm is elaborated. Furthermore, the proposed algorithm is implemented on wireless sensor nodes. The

performance of the proposed algorithm is analyzed and is shown to be effective in order to cope with both short and long term variations to the link quality.

Chapter 7

Finally, Chapter 7 concludes the thesis with the summary and critical evaluation of the work presented and a discussion on the possible future extensions.

1.5. Contribution of the Thesis

The output of this research is a contribution to both the academic and industrial community. Throughout the work an effort was made to highlight the difference between theory and in-situ practice. The benefits to the research community and the main contributions of the thesis are as follows:

Wireless communication in process automation

The benefit to the research community is substantiated by the following two review papers highlighting the opportunities, requirements, concerns, challenges and future outlook regarding the use of wireless communication technology in process automation.

- Waqas Ikram and Nina F. Thornhill, “Wireless Communication in Process Automation: A Survey of Opportunities, Requirements, Concerns and Challenges”. Presented at Control 2010 Conference, Coventry, UK, 7-10 September 2010.
- Waqas Ikram and Nina F. Thornhill, “Wireless Communication in Process Control: A Survey of Opportunities, Challenges, Key Technologies, and Future Outlook”, (in the process of submission).

Furthermore, an overview regarding the use of wireless for monitoring and control was presented at the 9th ICheme conference on Advances in Process Control.

- Waqas Ikram and Nina F. Thornhill, “Wireless monitoring and control”, ICheme: Advances in Process Control 9, York, UK, 19-20 September 2011 (Presentation).

Time synchronization of distributed wireless field devices

To address the problem of time synchronization, a novel hardware-assisted solution is developed based on MSF radio-clock. The problems linked to hardware variations and

volatility in recorded latency has been addressed by the use of Kalman filter, high-precision local oscillator and signal processing. The approach has been shown to be effective in order to increase the time synchronization accuracy. The following two publications are an outcome of this work:

- Waqas Ikram, Ivan Stoianov, Nina F. Thornhill, “Towards a Radio-Controlled Time Synchronized Wireless Sensor Network: A Work in-Progress Paper”. Presented at IEEE EFTA Conference, Bilbao, Spain, 13-16 September 2010.
- Waqas Ikram, Ivan Stoianov, Asher Hoskins, Nina F. Thornhill, “Radio Controlled Time Synchronization for Distributed Monitoring of Civil Infrastructure Systems” (in the process of submission).

Process control using wireless networks

The output of this work is the investigation into the performance limits of IEEE 802.15.4 network. Further studies have been conducted regarding the closed-loop control performance of an industrial furnace operating over an IEEE 802.15.4 compliant wireless network. In this case study, two versions of wireless network were examined: a simulated version based on TRUE TIME simulator, and another version used a hardware in-loop for wireless sensing. Actual wireless sensor nodes were used in the last scenario to incorporate the characteristics of a physical radio channel and its effect on the controller performance. Further details are presented in Chapter 5.

TPC of wireless instruments

The use of TPC can help address industrial issues concerning energy consumption, interference, fading and critical-data priority. As part of this research an algorithm has been designed for industrial instruments based on theoretical and empirical studies. It is shown that the proposed algorithm is adaptive to both short and long term variations to link quality and is lightweight, hardware-independent and practical. The performance evaluation result of this algorithm is presented in the following publication.

- Waqas Ikram, Nina F. Thornhill, Stig Petersen, “Adaptive Multi-Channel Transmission Power Control for Industrial Wireless Instrumentation”, (under review).

1.6. Chapter Summary

This chapter has presented an overall description of the project and has introduced the aims and objectives. The use of WSNs has enabled the process industry to collect the vast amount of hitherto unknown data from the physical monitoring of the underlying processes. The chapter has shown that wireless communication has led to new applications in the field of wireless process automation which in the past were subjected to economical, physical and technological barriers.

The use of wireless sensors and actuators in process automation provides the ability to monitor and interact remotely and cost-efficiently with the physical world. Moreover, the factors which are driving the research within this area are presented, such as the access to enhanced process information, which enables the industry to improve on-site safety, process operations, product quality, productivity, reliability and compliance with regulations. The current use of the standardized short-range wireless communication technologies in process automation for process monitoring has enabled the industry to address industrial concerns regarding security, reliability and safety. However, to further expand the horizon of these applications and to move towards the wireless control and safety applications, new concerns have emerged which have introduced new constraints. To address these new problems a more transparent and controlled flow of information in a network is required, where the system and network manager are dependent on the analysis tools and resource management strategies to provide them with clear and concise information about the state of the wireless network. It is an important requirement to ensure the adequate performance of the application class.

The chapter further provides an overview of process automation and highlights its reliance on communication networks. The use of wireless communication is the area of research in this thesis, and one of the sectors of interest in this research is the oil and gas industry which is further discussed. The chapter went on to explain the three key issues addressed as part of this research. The first issue being linked to time synchronization has been elaborated and its root cause has been identified alongside of its necessity to be addressed which is linked to data integrity, determinism and energy conservation in network operations. These are important to meet the application and networking requirements. The second issue under investigation in this research is the

study of the performance of a closed-loop control application running over an IEEE 802.15.4 compliant wireless network. The need to comply with local regulations and to ensure co-existence with the other wireless networks operating over the same radio band has added a new concern to the use of wireless in NCSs. It is further made complicated with the requirement of efficient resource utilization while complying with the industrial practices regarding the networked control structure and the time-triggered control-loop execution mechanism. To ensure longevity of wireless field nodes operated on standalone batteries a mechanism is required to optimize the energy consumption. This is the third issue investigated in this research and is addressed by means of TPC.

Finally, the outline of the rest of the thesis was presented along with the contributions of the thesis, which includes the publications.

CHAPTER 2

Background and Context: Wireless Technologies and Process Automation

This chapter reviews the existing wireless networking technologies and analyses their suitability for use in process automation. The main discussion presented here brings forth the shortcomings of commercial wireless technologies from industrial perspective. In order to address some of these shortcomings standardized wireless technologies aimed for industry have emerged. Amongst them, the standards for wireless process automation industry are predominantly based on the range, power and license-exempt communication band requirements mentioned in the previous chapter. This chapter explains what these standards are and why they are suitable. The features and methods adopted by these standards which make them industrial strength are outlined. The second line of discussion presented in this chapter is the comparison between standardized industrial wireless networks and identifies the applications for which these standards are suitable. All in all, this chapter will briefly introduce the short-range wireless networking technologies and will examine their suitability for process automation.

2.1. Opportunities for Wireless Communication in Process Automation

Figure 2.1 presents an overview of sensor network applications as found in process industries. The applications are divided into two divisions: monitoring and tracking, based on application requirements. The *monitoring* domain refers to applications which rely on industrial measurements for the purpose of regulatory compliance, equipment and infrastructure condition monitoring, process control and on-site safety. These activities may require wider collaboration between distributed sensors. The other

division is *tracking* and refers to locating of individuals or equipments. In this case the proximity of these objects in a space is of concern and the data from individual nodes is sufficient to draw conclusions. Tracking is important for the purpose of supply chain optimization and emergency response management.

Table 2.1 presents a non-exhaustive list of applications found in process automation based on the overview of sensor networks outlined in Figure 2.1. Table 2.1 shows that wireless communication enables better utilization of assets, enhances workforce productivity, assists compliance with regulations, improves on-site safety, and allows connections to locations which were either unfeasible or uneconomical to reach in the past. According to Drathen (2009) the use of wireless technology and the internet will become significant for process automation in future to provide up-to-date knowledge of on-going activities and effective knowledge management. Other commentators suggest that wireless communications will improve the monitoring and visibility of processes and equipment and achieve higher yields and better quality at lower costs [Flammini *et al.* (2008), Ferris (2010), Hartebrodt *et al.* (2004), Akerberg *et al.* (2011)].

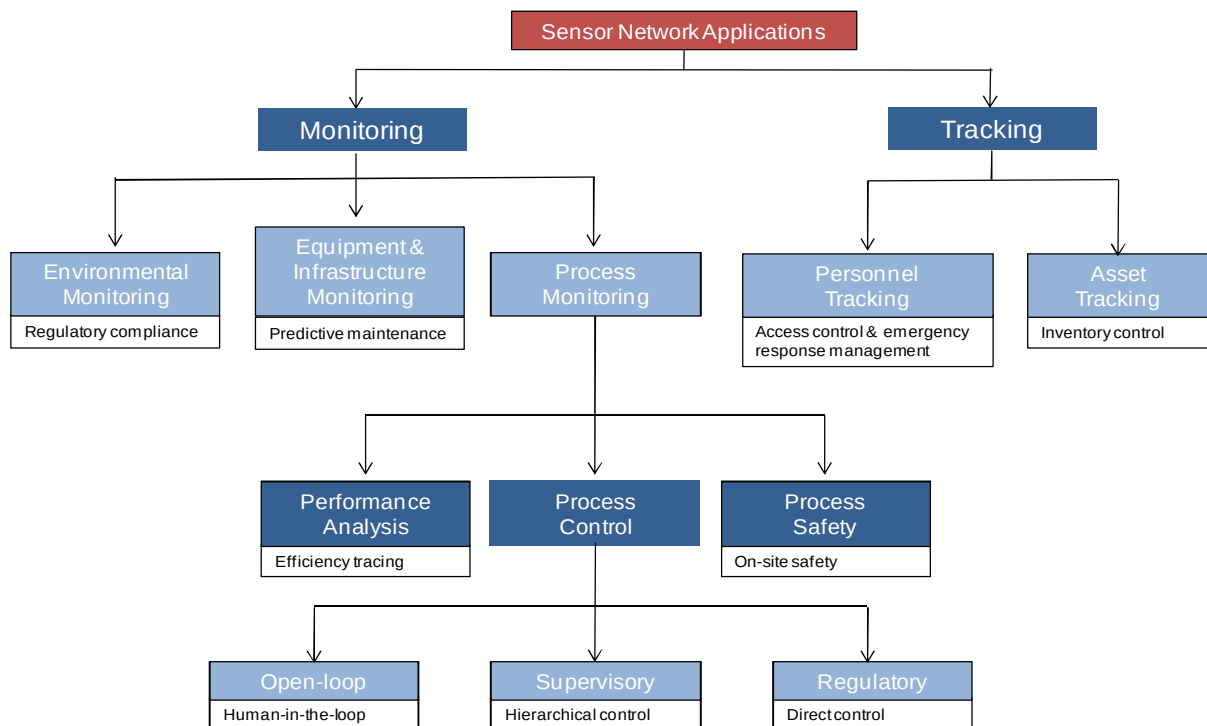


Figure 2.1. Overview of sensor network applications in industry.

Process industry automation activities are classified by ISA and NAMUR as related to safety, control or monitoring applications. Due to the criticality associated with the safety data, and data linked to critical-control applications, wired solutions are currently considered the best available methods within these domains (Han, 2010) (Chen, 2010). However, as shown in Table 2.1 wireless communications are being used in process automation, especially when the update-rate is moderate and the application is non-critical. The current focus is on monitoring applications. Use of wireless communications in a feedback control loop is developing considerably more slowly for reasons that will be explored in a later section.

2.2. Automation Pyramid and Usage Classes

This section introduces the automation pyramid and the classification of applications found in process automation as specified by the ISA 100 working group. The need for automation is necessary for many applications belonging to both industrial and non-industrial domains. Figure 2.2 shows the hierarchical view of these automation domains. However, the requirements differ between each domain. Industrial automation has more stringent requirement due to the criticality of the operations involved. Two forms of automation used in the industry are factory automation and process automation. Factory automation is related to manufacturing and its operations are confined within a production cell, such as the operation of a robot arm. Process automation on the other hand involves automation of a process like that of a distillation column, as found in an oil refinery.

There are different sets of requirements for both and the requirements differ in many ways like availability and coverage requirements. This section will limit the discussion to process automation only, which is the area of research in this thesis. As mentioned earlier, process automation refers to the set of technologies working together to attain superior operational performance of processes, machines and systems without significant human intervention (Groover, 2009). Therefore, it involves synchronization of devices, technologies and the overall integration of machines into a self-governing system. It requires bringing technologies together and makes them operate autonomously.

Table 2.1. Example applications of wireless communications in the process industry.

Collection of diagnostic data from 4-20 mA process instruments:

Traditional 4-20mA current loop instruments are increasingly becoming equipped with HART protocol which provides diagnostics data for condition monitoring and maintenance (HCF, 2011). However, according to Johnston (2009), there are 30 million HART devices installed worldwide, and amongst those only 10% have a pathway back to the host for the instrument diagnostics. A significant application of wireless communications in process plant is for wireless transmission of HART data by means of adaptors using the WirelessHART standard fitted to the wired instruments. WirelessHART provides access to such data at much lower installation and planning costs and can bypass legacy DCS systems [Siemens (2010) Johnston (2008)]. Figure 1.6 shows an example of a wireless field device which can be a WirelessHART transmitter.

Tracking and tracing:

Radio frequency identification tagging (RFID) provides an electronic bar code which can be read remotely. RFIDs are in routine use in supply chain operations for inventory tracking and also enable tracking and tracing of personnel and equipment, with advantages for safety (Motorola, 2009). They are mainly used in enclosed spaces. For wider coverage other tracking methods like GPS are available.

Difficult measurement locations:

Wireless communication enables access to measurements from remote or inaccessible locations where wired connectivity is infeasible, too expensive or too bulky or heavy, for example on refinery tank farms or offshore platforms. Wireless communication eliminates cables, and occupies less space (Emerson, 2010a). Wireless communication also gives access to data originating from rotating equipment such as rotary kilns, replacing the slip-ring contacts, connectors and festoon cables that are needed for wired sensors (Forge, 2010).

Equipment condition monitoring and predictive maintenance:

Mechanical failures of equipment like motors and drives are amongst the most common

causes of production stoppage according to Ralston (2007). Wireless communication allows continuous acquisition of vibration and other equipment condition monitoring data and thus enables predictive maintenance.

Field rounds:

Measurements in a process plant are often documented manually by engineers in the field. Examples include corrosion monitoring on critical areas of vessels or pipelines (BP, 2011), ball valve position, temperature and level monitoring in tank farms. WSNs can collect this data automatically and eliminate or speed up manual cyclic patrol checks. For instance, they enable collection of data while an operator drives past the equipment.

Safety and environmental monitoring: Applications related to safety include fire and gas detection and elimination of spills to avoid safety violations. A novel application is the monitoring of eye wash and safety showers to mobilize an emergency response (Apprion, 2012). Environmental monitoring using wireless can be used for emission monitoring. Vacuum columns and flare stacks are examples of applications linked to environmental regulations.

Short-term deployments and new sites: Short-term measurements can use wireless communications, e.g. in equipment monitoring where one expensive sensor is installed at different locations in a site over a period of time. The alternative is to save the data within the instrument and download it at the end of the monitoring period. On new sites, or extensions of existing sites, the cost effectiveness of wireless installation and the reduction of cable runs may make wireless communication attractive (William, 2010). Issues of power supply remain,

Distributed and remote facilities:

Wireless communications enable remote operation of facilities. These include: tank farms, pipelines, loading piers, production platforms and wellheads (Yokogawa, 2011).

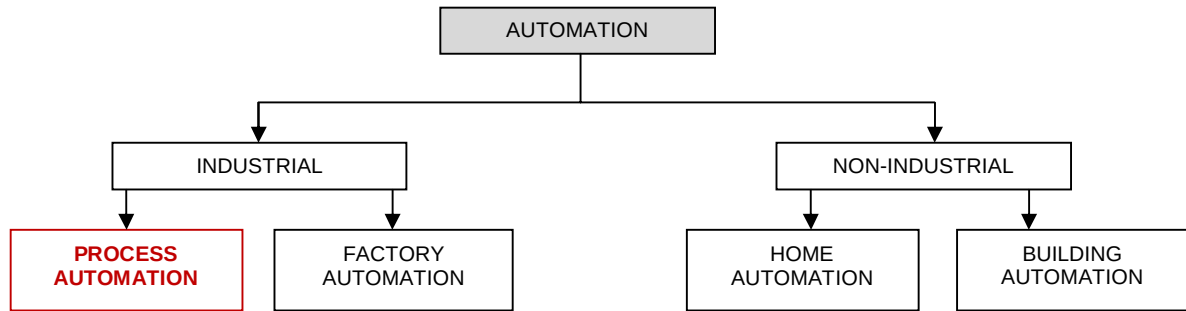


Figure 2.2. Hierarchical view of automation classes.

Automation pyramid

The industrial automation systems comprise various systems and devices responsible for a variety of functions related to instrumentation, control, supervision and operational management (Groover, 2009). Figure 2.3 shows the hierarchical structure of an industrial automation system based on ISA-95 functional hierarchy from ISA-95 Part 3 (ANSI/ISA-95, 2000). The different layers in the automation pyramid represent different sets of application requirements linked to their corresponding activities. There are five distinct layers of functional hierarchy in the automation pyramid.

At the bottom of the pyramid is Layer 0, which can also be referred to as sensor and actuator layer. This layer is closest to the physical process. It is at this layer that the data is collected from field devices like sensors, and sent to the higher layers for analysis and decision making. Similarly, actuators also implement the commands issued by controllers at this level. Level 0 provides services to Level 1 which is responsible for regulatory control. It is at this layer where Programmable Logic Controllers (PLCs) reside. The PLCs interact with field devices and perform real-time control.

The next layer is Level 2 which is the supervisory control and operations layer. This layer is responsible for operations of the automatic control layer. This layer sets out the control parameters for the controllers. The regulatory layer looks after the control loops and also the equipment. SCADA systems are used for monitoring and controlling of devices like PLCs. Level 3 on the other hand deals with operational and management related activities such as detailed production scheduling, managing resources, scheduling maintenance and dispatching production. Manufacturing Execution Systems (MES) are found at this layer. Level 4 is the top layer in the hierarchy. This layer is

related to enterprise management and deals with the commercial aspects of the business. The tasks involved are linked to production targets, plant production scheduling and overall management. High level planning systems such as Enterprise Resource Planning (ERP) systems are used at this level which relies on the services of MESS.

The focus of this research is on Levels 0 and 1 that use sensors to collect process data which is further used for various tasks such as calculation of control actions. The arrow heads on the left side of Figure 2.3 show that, for wired connections, the amount of cabling increases lower in the hierarchy and the requirements for safety, reliability, transmission frequency and real-time communications also increase. The trend is that at the bottom of the pyramid, the timeliness of information becomes vital as it is directly linked to the operation of equipment or the performance of a process. Reliability of a communication network used at this level is also very critical and is further linked to safety. Moreover, as the numbers of components in the bottom layer is high they require more connections. Wireless connections have the benefit of reducing the amount of cabling. Furthermore, the operating conditions in a process industry are also often harsh compared to the ones present at the higher layers. On the other hand, the volume of data at the bottom of the pyramid is less as it is related to process values whereas the volume of data found at higher layers is high.

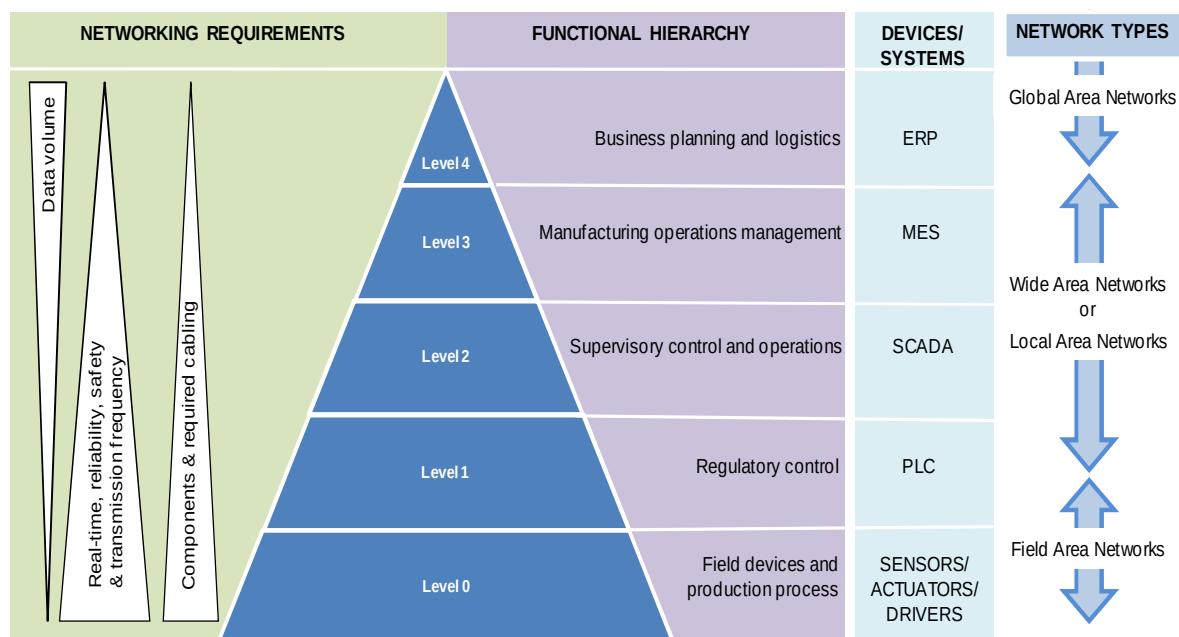


Figure 2.3. The automation pyramid. After ANSI/ISA-95 (2000), Sauter (2010) and Züge et al. (2010).

It is due to these requirements that various network types are used concurrently in industrial automation. The 4-20 mA control loop, HART protocol and fieldbus are examples of technologies designed to connect sensors, actuators and controllers. At the higher levels the wide area network or local area network technologies can be used which can be IP-based networks, such as Ethernet or wireless LAN (Wi-Fi). The bottom two layers are of interest to this research and this is where wireless technology can have significant impact on the process automation according to Chen *et al.* (2010), Song *et al.* (2005), and (Johnston, 2009). It is based on the requirements of this level that the currently available wireless solutions will be evaluated. All of the higher layers have less stringent application requirement, and the commercially available solutions are already addressing their needs, refer to Caro (2004) for further details.

Usage classes

In process automation various applications exist and they have different requirements and levels of tolerance towards timelines of message delivery. The ISA100 working group has identified six different classes within the process automation domain which are classified based on timing restrictions and the criticality of the information. They are shown in Table 2.2.

At the field network level, the applications belonging to monitoring domain and open-loop control have less stringent requirements and wireless networks are currently being used in such deployments. However, the higher two classes have more complexity involved. The guarantees on the network availability and its stability are important. In case of the safety application, wired networks are currently considered as the most reliable options. In the case of Class 1 which involves closed-loop regulatory control, the requirements are further linked to the process which needs to be controlled. The parameters which are linked to the dynamics of the physical process such as, its response time and deadtime, specify the sampling rates for the sensors and controller.

Based on the discussion above and the requirements mentioned earlier, the ISA usage classes can be represented on a 3-dimensional axis as shown in Figure 2.4. The three axes here represent update rate, availability and reliability in general. The mapping represents a general overview of relative standing of each application. The terminologies used in Figure 2.4 are highlighted in Table 2.3. Within this graph, closed

loop regulatory control as defined by the ISA group can further be subdivided into fast and slow loop control. It is to signify that it is linked to process dynamics and the update rate (i.e. sampling rate) required will vary from process to process. It also highlights that some processes which may have slow process dynamics may be eligible for control over a wireless network. For the other loops which require fast update rate, they mandate the need for certain bandwidth capacity, network topology, and channel access mechanism. If a network cannot provide these features then running a control application over a wireless network may not be an option. From here onwards fast loop control will refer to control which requires sampling period of 1s or below. Additionally, safety applications are further split into process safety and machine safety based on the requirement of update rate. This detailed layout of applications presented in Figure 2.4 signifies that with relaxed update rate requirement, advance methods can be deployed to achieve the requirement of availability and reliability.

Figure 2.3 also highlights that there may not be one solution for all applications. In some cases, the design of a communication network to address a particular requirement like update rate, availability and reliability may dominate the entire network design. These governing design principles will impose restrictions on networking architecture, routing and redundancy. As a result, the network may not be optimal for use for other classes of applications, other than the intended one.

Table 2.2. Classification of the process automation applications based on ISA100 working group and NAMUR specifications.

Category	Classification	Description	↑ Importance of message timeliness, availability and operational consequences
Safety	ISA Class0: Emergency action	Always critical	
	NAMUR Class A: Functional Safety	Examples: - Emergency shutdown - Automatic fire control	
Control	ISA Class1: Closed loop regulatory control	Often critical	
	NAMUR Class B: Process/ Management Control	Example: - Direct control of primary actuators	
	ISA Class2: Closed loop supervisory control	Usually non-critical	
Monitoring	NAMUR Class B: Process/ Management Control	Example: - Multivariable controls	
	ISA Class3: Open loop control	Human in the loop	
	NAMUR Class B: Process/ Management Control	Example: - Operator performs manual adjustments	
Monitoring	ISA Class4: Alerting	Short-term operational consequence	
	NAMUR Class C: Display/ Monitoring	Example: - Event-based maintenance	
Monitoring	ISA Class5: Logging and down-loading/ uploading	No immediate operational consequence	
	NAMUR Class C: Display/ Monitoring	Examples: - History collection - Preventive maintenance	

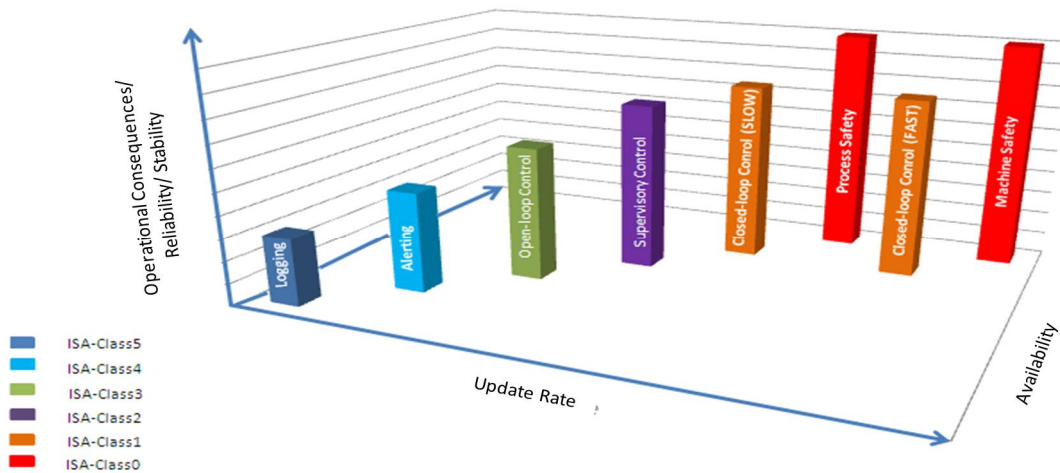


Figure 2.4. Application requirement per usage class.

Table 2.3. Terminologies used in application requirements per usage class illustration.

Reliability:	A measure of the percentage of sensor data that reaches its destination, usually the gateway.
Stability:	A measure of the percentage of successfully transmitted data. It takes into consideration the retransmissions.
Availability:	The number of packets that arrive within a predefined period of time.
Update Rate:	The number of transmissions per unit time.

Next, a selected set of available wireless communication technologies are presented, analyzed and their suitability for use in the field network is evaluated based on the requirements criteria presented in the previous chapter.

2.3. Comparison of Commercial Wireless Communication Technologies

This section presents a comparison between the competing wireless communication technologies, namely, ZigBee, WiMedia (i.e. based on UWB scheme), Bluetooth and Wi-Fi. An overview of these technologies is provided in Appendix B1. Figure 2.5 presents the seven-layer OSI model and maps the scope of IEEE 802 standards to the model. It highlights that the lower two-layers, the PHY and MAC layers are within the scope of the IEEE 802 suite of standards. MAC is a sub layer of data link layer. PHY is the lowest layer of the OSI model, also known as Layer 1, and deals with transmission of raw bits over a medium. MAC layer on the other hand is responsible for managing and

coordinating access to shared medium. Furthermore, the protocol stack of each of the aforementioned technologies is shown in the Figure 2.5 for comparison. From the figure it can be seen that the lowest two layers of ZigBee, Bluetooth and WLAN stack have associated IEEE 802.xx standard. The ZigBee protocol stack builds upon the IEEE 802.15.4 standard, and the upper layers are specified by ZigBee Alliance. In case of Bluetooth stack they are specified by Bluetooth SIG. The WiMedia UWB specification is formulated by WiMedia Alliance. The Common Radio Platform (CRP), which includes PHY and MAC, is part of the specification and the Protocol Adaption Layer (PAL), and provides mean to bridge the MAC sublayer to the protocols at upper layers (Heidari, 2008). In the case of WLAN stack, the lower layers are certified by Wi-Fi Alliance. Above these layers protocols such as TCP/IP can operate.

Table 2.4 shows typical applications and technical specifications for the commercially available communication protocols in Wireless Personal Area Network (WPAN) and Wireless Local Area Network (WLAN). The frequency bands, bandwidth, modulation, spreading and transmission power in the physical layer are specified by the relevant IEEE 802 family of standards. Distance and data rates are dependent on these parameters. UWB has the fastest supported data rate within a confined radius of less than 10 meters, whereas, Wi-Fi in general supports fast data rate over longer distance.

The term *spreading* refers to spread spectrum, where the signal occupies a bandwidth in excess of the minimum necessary to transmit the information. It is accomplished by means of a code which is independent of source data. Its ability to resist jamming and interference are amongst the main reasons for the use of spread spectrum techniques. The widely used techniques for spread spectrum include Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). In case of FHSS, the available bandwidth can be divided into a number of channels, each with a slightly different carrier frequency so that messages can be sent in different channels as needed to avoid interference. Therefore, instead of transmitting at one frequency the spread spectrum system switches rapidly from one frequency to the other. The selection of the next frequency in the sequence is random and makes it robust against narrow band jamming. The idea of spread spectrum originated with actress Hedy Lamarr and collaborator George Antheil who patented the idea and a method for implementation in 1942 to avoid jamming of radio-guided torpedoes.

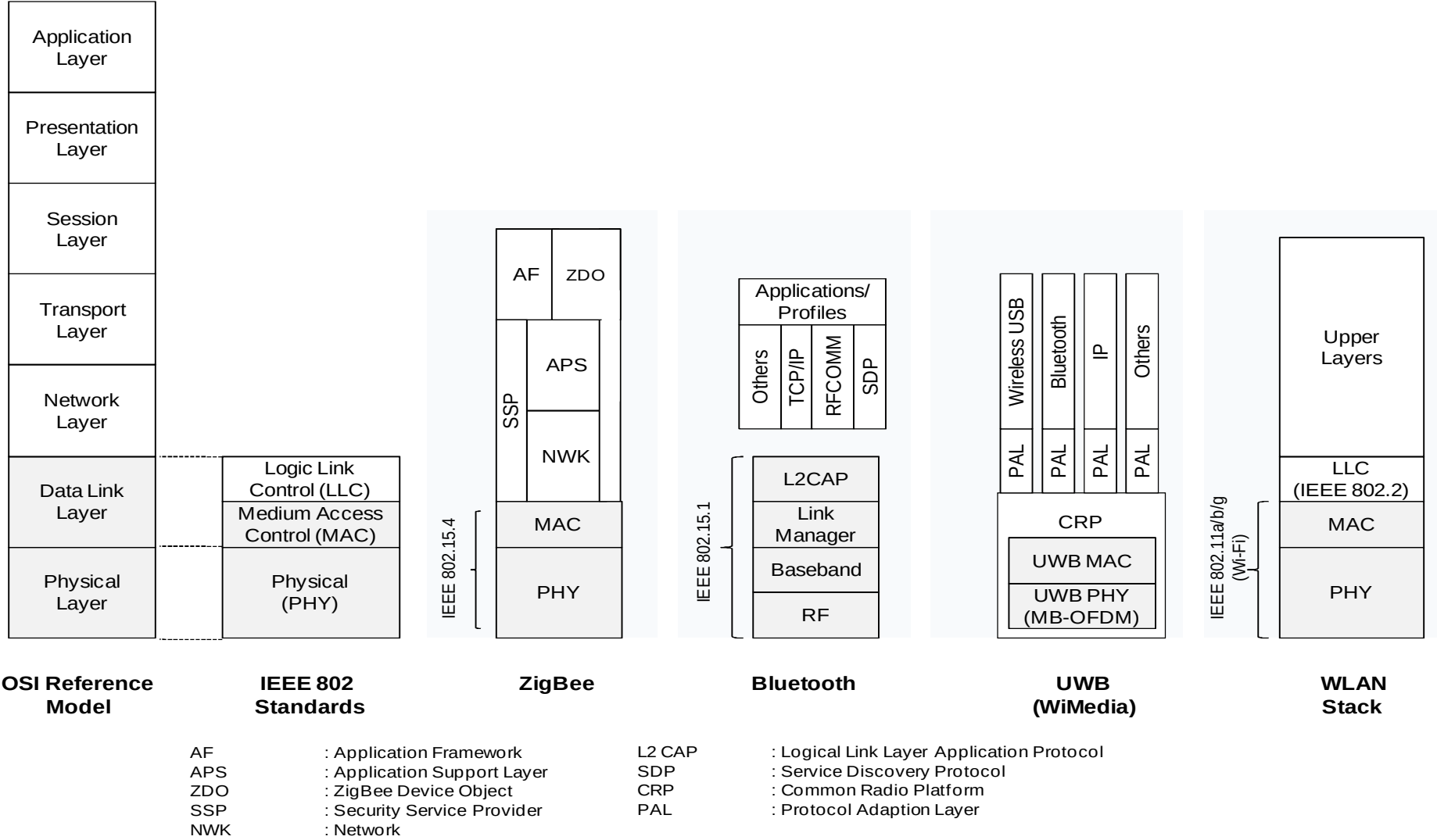


Figure 2.5. The relationship of the IEEE 802 standards to the protocol structure of WPAN and WLAN technologies. After Agbinya (2009).

Table 2.4. Comparison of short-range wireless communication technologies. After Lee *et al.* (2007), Akyildiz (2009), Stieglitz *et al.* (2011), and Yang (2006).

	ZigBee	UWB	Bluetooth	Wi-Fi
Frequency band(s)	868 MHz ¹ , 915 MHz ² , 2.4 GHz [*]	3.1-10.6 GHz ³ , 4.8-6 GHz ⁴	2.4 GHz	a: 5 GHz, b,g: 2.4
Bandwidth	600 kHz, 1.2 MHz, 2.0 MHz	528 MHz ⁵	1 MHz	a: 16.25 MHz, b: 22 MHz g: 16.25-22 MHz
Nominal transmission power	(-25) – 0 (dBm)	-41.3 dBm/MHz ⁷ (39.1 μ W per band) ⁵	0 – 10 dBm	15 – 20 dBm
Raw data rate (max)	250 Kbps ⁸	480 Mbps ⁵	3 Mbps ⁶	a,g < 54 Mbps b < 11 Mbps
Spreading	DSSS	DS-UWB, MB-OFDM	FHSS	DSSS, OFDM
Medium access	CSMA/CA	CSMA/CA (TDMA optional)	TDD (master slave polling)	CSMA/CA (TDMA optional)
Basic cell [Extensions]	Star, [Tree, mesh]	Peer-to-peer ⁵ , piconet ⁹ [Child piconet]	Piconet [Scatternet]	BSS [ESS]
Node enumeration time	30 ms (typical)	Protocol dependent	< 10 s	< 3 s
Supported number of nodes	65,535	Protocol dependent	8 (7 active slaves)	2007 (Structured BSS)
Data protection	16-bit CRC	32-bit CRC	16-bit CRC	32-bit CRC
Encryption	AES block cipher	AES block cipher	Stream cipher	AES block cipher ¹⁰
Power consumption	Very low	Low	Low	High
Nominal range (m)	10-30	1-10	1-100	100
Associated IEEE standard	IEEE 802.15.4	-	IEEE 802.15.1	IEEE 802.11a/b/g
Organization(s)	ZigBee Alliance	UWB Forum and WiMedia Alliance	Bluetooth SIG	Wi-Fi Alliance
Typical applications	Monitoring and control	High bandwidth cable replacement	Cable replacement	Computer networking

^{*} Global ^{1,4} Europe ^{2,3} America ⁵ MB-OFDM (WiMedia) ⁶ v2.1 ⁷ FCC defined spectral density ⁸ 2.4GHz (IEEE 802.15.4-2003) ⁹ DS-UWB (UWB Forum) ¹⁰ WPA2

The use of a spread spectrum requires a synchronized decoder in the receiver as well as an encoder in the sending device. Bluetooth adopts this method of spreading. In case of DSSS, the frequency of the carrier is constant. The information signal in this case is multiplied with pseudo random spreading code. Each bit in the spreading code is called a chip. This spreading code has a higher chip rate and results in a wideband signal. ZigBee and Wi-Fi uses DSSS which offers resistant against interference and gives the ability to share a single channel among multiple users.

The MAC protocol enables multiple devices to transmit and share the capacity of the same physical space. ZigBee and Wi-Fi MAC are based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) which means that each node monitors the

transmissions of other nodes to determine whether the channel is busy or idle. A consequence of this contention-based channel access is that the transmission waiting times are random, in contrast to Time Division Multiple Access (TDMA). In TDMA systems the time axis is divided into time slots and the nodes are assigned times to transmit. TDMA provides deterministic communication as the channel access is contention-free. In terms of network topology, ZigBee offers the most flexibility compared to others. Bluetooth and UWB (DS-UWB) is restrictive as the basic unit of operation is a piconet.

The data protection method employed by the technologies presented in Table 2.4 is Cyclic Redundancy Check (CRC) and is part of data link layer. In this method of verifying the integrity of data during transfers, a CRC word (also called checksum) is appended at the end of each data packet. It is an extension of the parity bit method. CRC is generated by dividing the message bits by a fixed binary string referred to as *generator polynomial* and the remainder is the checksum (Barr, 2007). By carefully selecting amongst the available standardized polynomials, most of the errors can be detected which occurred during transmission (Barr, 2007). The use of 16-bits CRC means that the checksum size is 16 bits and the algorithm is able to detect error burst lengths of up to 16 bits. *Error burst length* refers to number of bits between and including erroneous bits (Sinha et al. 1998). ZigBee and Bluetooth use 16 bit CRC, whereas, UWB and Wi-Fi uses 32 bit CRC. In terms of message encryption, ZigBee, UWB and Wi-Fi support AES block ciphers, whereas, Bluetooth uses a stream cipher called E0. Block ciphers divide the input stream of bits into discrete sections called blocks and encrypts them.

Shortcomings

Table 2.5 presents a qualitative comparison of the WLAN and WPAN technologies presented above. It can be seen from the table that the lack of support for real-time traffic and differential QoS are the key shortcomings of these technologies for the purpose of process automation. Additionally, the contention-based channel access mechanism adds random delay to the data which is a serious concern for process control and safety applications. It is because the network traffic will cause the contention-based MAC devices to backoff. Therefore, the transmitter waits for a random backoff period before sensing the medium and initiating transmission, and this will affect message latency. Furthermore, ZigBee offers flexibility in network topology

which includes the use of spatial diversity as in the case of mesh networks and leads to high reliability. However, it is achieved at an expense of having redundant nodes and can result in an increase in latency time. The latter case is again a concern for process control. Higher data rate can be an added benefit but not a main requirement for process automation, especially when dealing with process data. In addition, the battery lifetime of field nodes equipped with UWB and Wi-Fi transceivers consume higher power compared to the other two. ZigBee is optimized for energy-consumption, and has the best performance compared to the others. Finally, the main concern is about reliability and stability which is linked to coexistence mechanisms and their adaptability to the varying channel conditions. This is where they all fall short, especially ZigBee and Wi-Fi. ZigBee uses one static channel for communication in a network, which makes it susceptible to interference and jamming. Bluetooth does offer adaptive frequency hopping but can still be affected by the channels which are subjected to interference and are part of the channel hopping sequence. UWB is inherently robust to these interferences but within a very limited region of operation due to limited transmission power. Regulatory issues linked to UWB are a main concern in addition to these requirements.

Table 2.5. Qualitative comparison of short-range wireless communication technologies for use in process automation.

	ZigBee	UWB	Bluetooth	Wi-Fi
Scalability	Very high	Limited (specification dependent)	Low	Medium
Real-time support/QoS	No	Limited (MAC dependent)	No	No
Channel Access	Contention-based	Supports both	Contention-free	Contention-based (Contention-free is optional)
Topology flexibility	Yes	Limited (specification dependent)	No	No
Data Rate	Enough	Best	Good	Better
Coexistence strategy	Dynamic channel selection	Multi-band operation, Limited transmit power	Frequency hopping (adaptive)	Dynamic channel selection, Transmission power control
Adaptability to varying channel conditions	No	Inherent advantage (wideband)	Limited	No
Battery Life *	Long	Very short	Short	Very short
Reliability	High (mesh networks)	Low (peer-to-peer)	Low	Low

* Based on the power consumption of commercially available transceivers reported by Lee et al., (2007).

In short, the aforementioned communication technologies in their original format based on the parameters mentioned above are not well positioned to address the demands of process automation applications. The need to address the shortcomings of these wireless technologies and the necessity for a standardized solution has resulted in the emergence of three standards referred to as WirelessHART, ISA100.11a and WIA-PA. They will be discussed next.

2.4. Advent of Industrial Strength Wireless Networks

Based on the discussion presented above, it was concluded that the commercially available wireless communication technologies are not well positioned to meet the demands of process automation. Amongst them was ZigBee technology, which itself is not suitable for process automation, but the MAC and PHY on which it operates is specified by IEEE 802.15.4 standard. The industrial strength wireless networks are based on this standard. A brief overview of this standard is provided in Appendix B2.

2.4.1. ZigBee PRO

ZigBee PRO feature set is an extension of ZigBee released in 2007 aiming at the industrial markets and employs enhanced security and network resilience features in order to compensate for the shortcomings of the ZigBee network [Hunn (2010), Rashvand *et al.* (2012)]. The background to ZigBee technology is provided in Appendix B1.3. In this subsection, few key features which are part of ZigBee PRO are highlighted.

- FREQUENCY AGILITY:

This standard supports frequency agility, which consists of scanning available channels to determine the channel with least interference, noise and traffic. It is then selected and used by all ZigBee devices. For a network which experiences changing RF environment, frequency agility concept allows the host application to scan for a better channel, and move the whole network to the new channel (Suhonen *et al.*, 2012). This feature of dynamic channel switching helps to avoid interference. When a network node experiences interference, the likelihood of packet dropout increases and hence misses an acknowledgment. Above a certain threshold of transmit failures, the channel is assumed to be experiencing interference and then frequency agility appears. However, the utilization of

information collected from distributed nodes such as scanned channels energy levels, the corrective action taken and policy adopted, is up to the network coordinator (Elahi *et al.*, 2010). Frequency agility is a corrective action which is taken once the network experiences such changes and hence the data loss during the process and time to switch the whole network to a new channel will consume time, which is a concern for time-critical control applications.

- **STOCHASTIC ADDRESSING:**

In order to simplify network formation, the stochastic addressing feature allows each device to be randomly assigned a unique network address. In earlier release of ZigBee, the network addresses were predetermined and distributed during network formation (Suhonen *et al.*, 2012). The new approach simplifies network address calculation, allows devices to retain their addresses and decouples the link between network address of devices and their relative position in network.

- **SECURITY:**

Network wide security is achieved via security keys, network encryption and device security. The protection of network and implementation of optional advance security features along with effective key management and distribution are up to the implementation (Elahi *et al.*, 2010). The network and application link keys can be either pre-configured or non-preconfigured. In the earlier mentioned case the keys are defined earlier as part of the stack, whereas, in the latter case the keys are transmitted by the Trust Centre, as the devices join the network. For devices which were in sleep mode during the change of key, a mechanism is in place for devices to use a special link to encrypt a message to validate itself and get the new key.

ZigBee PRO also supports many-to-one routing discovery which allows the ZigBee coordinator to build routes to the devices in the network. The building up of routing table is helpful to route messages at a later stage as opposed to having first issue routing request (Hunn, 2010). Many-to-one route aggregation and source routing allows using common routes, and the use of source routing back to end devices help reduce route table discovery broadcasts (Elahi *et al.*, 2010). However, for a network which experiences bottlenecks or link outages due to the blocked paths the re-routing or route re-discovery is required. It will consume time if the MAC utilizes a contention based

channel access mechanism which is again a concern. In general, ZigBee PRO is an improvement over the earlier version of ZigBee.

2.4.2. WirelessHART

WirelessHART is based on wireless mesh network protocol designed by the HART Communication Foundation (HCF) for wireless transmission of the HART messages. HART is a communication protocol used in the industry. WirelessHART is based on the 2006 release of IEEE 802.15.4 standard. It utilizes a time synchronized, self-organized, self-healing and redundant path mesh architectural network which operates in 2.4GHz ISM band.

Key features

WirelessHART is designed for process automation and has focused on robustness and security (WirelessHART, 2009). At the data-link layer WirelessHART utilizes 10ms time slots for communications. These time slots can be dedicated to individual devices or shared amongst a group. At the network level, WirelessHART supports graph routing, source routing and superframe routing (Chen *et al.*, 2010). In case of graph routing, paths are stored by each device and are used for forwarding packets. In case of source routing, the packet contains the information about the nodes from source to destination. In the latter case, a specialized form of graph routing a device forwards a packet according to superframe ID embedded in the message (Chen *et al.*, 2010). It also supports broadcast, unicast and multicast transmissions. In order to ensure reliable transfer of information, WirelessHART supports connection-oriented communication. It supports out-of-order packet delivery.

The key features of WirelessHART include: channel hopping, multi-hop mesh network and TDMA for radio channel access. Channel hopping (also known as frequency hopping) allows devices to choose different channels for communication to avoid jamming and prevent using poor link-quality. WirelessHART uses packet-by-packet frequency hopping which helps to avoid multi-path fading and interference (Chen *et al.* 2010). In order to increase reliability, redundant communication paths provide path diversity (Suhonen *et al.*, 2012). In order to provide contest-free utilization of the radio channel, TDMA is used to arbitrate and coordinate communications between the

devices in the field. The devices can be allocated fixed time slots for accessing the radio channel. The communication link between devices is made secure by using join keys, session keys and data-link network keys. The security in the data transfer is achieved through encryption, authentication and integrity check.

Network architecture

Figure 2.6 (a) depicts the typical layout of a WirelessHART network. It comprises field devices such as sensors and actuators connected to rest of the plant automation network via a gateway. A gateway is a bridge between field devices and host application, and allows buffering of sensor data, diagnostics data and event notification (Chen *et al.* 2010). The field devices can be configured in a star or mesh format. However, star network is not recommended according to Lennvall *et al.*, (2008). The field devices in a WirelessHART mesh network have the capability to operate as routers. The use of this functionality is linked to the use of routing strategy. The wireless field network is managed by the Network Manager (NM), which is responsible for setting up a network and supervising the network operations. Only one NM has to be active at any time. The NM manages time slots, routing tables, schedules communications, monitors network health and queries field devices for information. The Security Manager (SM) fortifies the wireless field network. In commercially available products, these three functionalities are often housed in one system. The access to the plant network is provided via service access points, and helps translate the messages from one domain to the other. WirelessHART protocol is the first industrial strength wireless protocol aimed at process automation.

2.4.3. ISA100.11a

ISA100.11a is a wireless networking standard developed by ISA for process control and related applications. The ISA100 working group has addressed factors like industrial environment, technology and lifecycle, and applications of wireless technology for fixed, mobile and portable devices (ISA100.11a, 2009). ISA100.11a is based on IEEE802.15.4-2006. The specification includes features like security and management of usage classes referred in Section 2.2.

Key features

This standard uses channel 11-26 of 2.4GHz ISM band specified in IEEE 802.15.4-2006 standard. It addresses the needs of periodic monitoring and control applications where latencies of order 100 ms or above are tolerated (ISA100.11a, 2009). The use of automatic repeat request is employed to achieve reliable data communication. The ISA100.11a network utilizes TDMA for channel access and frequency hopping. Within frequency hopping there are two types, slotted channel hopping and slow hopping (ISA100.11a, 2009). They are used either to minimize the energy consumption or to smooth the time synchronization requirement. On the other hand, the timeslots in the case of ISA100.11a are configurable. This standard also supports channel blacklisting which helps to identify and block channels which can interfere with the normal wireless network operation (ISA100.11a, 2009). The network supports graph and source routing. In order to support future compatibility ISA100.11a network headers are compatible with Internet Engineering Task Forces 6LoWPAN standard, which allows IPv6 packets to be sent and received from IEEE 802.15.4 based networks (Liptak *et al.*, 2012). The transport layer supports end-to-end data delivery, flow control, segmentation and reassembly.

Amongst the special features of this standard are adaptive hopping and mesh routing, which can mitigate coexistence issues. The staccato transmissions as expected from the network enable the co-located IEEE802.11 networks to quickly recover if experiencing interference from this network (ISA100.11a, 2009). In order to avoid busy channels and to ensure coexistence, this standard supports three methods: Clear Channel Assessment (CCA), Spectrum Management, and Adaptive Channel Hopping. In CCA, a device performs a CCA before transmission. If the outcome shows that the channel is busy then the device will not transmit in that channel. In *Spectrum Management*, limiting the availability of channels for hopping either due to regulatory issues or poor-link quality being experienced in certain channels is achieved via appropriate resource allocation. Therefore, certain channels can be blacklisted temporarily, locally or network-wide (ISA100.11a, 2009). Adaptive channel hopping is a mechanism to avoid problematic channels on link-by-link basis, in this method a device may autonomously treat problematic channels (ISA100.11a, 2009). This will help reduce unnecessary interference and energy waste.

The above mentioned features will ensure co-existence amongst the competing devices in a co-located space. The reliability of the network is increased using frequency hopping, mesh networking and short time slots. ISA100.11a is a relatively new standard and is aimed for multi-protocol capability.

Network architecture

Figure 2.6 (b) shows a typical architecture of ISA100.11a network which comprises of field devices, gateways and handhelds. The devices can be arranged in different topologies based on application demand such as star, tree and mesh formats. In case of ISA100.11a some of the field devices like sensors, valves or actuators may provide additional routing functionalities to forward messages from other devices. Therefore, in case of ISA100.11a network some devices can be Full Function Device (FFD) and others can be Reduced Function Device (RFD). Moreover, a backbone router provides an interface to the field network and a backbone network. A gateway on the other hand has at least an interface to field network and to the plant network. The infrastructure devices in the network communicate to other devices via an interface to backbone network. A backbone network is not defined in the standard, and preferably should be a high data rate network. In an ISA100.11a network as shown in Figure 2.6 (b) the wireless field network nodes connect to the control system via backbone routers and gateway. This standard allows devices to encapsulate foreign PHY data units and transmit them through the network, also referred to as tunneling (ISA100.11a, 2009). The gateway supports interoperability with different standards by translating and tunneling information. Appropriate levels of authentication, encryption and data protection levels are in place. Device-to-device communication is protected via symmetric keys.

2.4.4. WIA-PA

Wireless Network for Industrial Automation – Process Automation (WIA-PA) is an IEC approved Chinese Industrial Wireless Standard for Process Automation. It is based on IEEE802.15.4 radio, and is aimed at industrial monitoring, measurement and control applications. WIA-PA defines the data link, network and application layer of the protocol suite.

Key features

The packets transmitted in a WIA-PA network have an associated packet lifecycle and are discarded at the end of packet lifetime (WIA-PA, 2009). In WIA-PA, timeslot duration is configurable. To ensure coexistence and avoid fading, WIA-PA, in addition to collision avoidance, adopts frequency diversity. It helps to change transmission channel based on actual channel conditions. The frequency hopping mechanism in WIA-PA supports Adaptive Frequency Diversity (AFD) and Timeslot Hopping (TH) (WIA-PA, 2009). In first approach, a channel which is experiencing channel errors, measures the performance via packet drop rate or resend time and can change transmission channel. Retransmissions are also supported in AFD. TH is performed during inter-cluster and intra-cluster communication.

Integrity and confidentiality is achieved via message integrity check and encryption. The network uses various cryptographic keys such as Provision Key, Join Key, Encryption Key and Session Keys to protect the data. Data transfer services provide three modes of communication: Client-Server (CS), Publisher-Subscriber (PS), and Report-Sink (RS) Modes. CS modes are used for information acquisition and setting, PS is used for periodic data, and RS is used for alert data.

Network architecture

Figure 2.6 (c) shows a typical WIA-PA network with a gateway, routing devices, and field devices. It can further be connected to other networks such as plant network. The five device types defined in WIA-PA network are: host computer, gateway, routing device, field device, and handheld device. The latter mentioned three devices are to be found in the field. The routing device forwards the packets from field devices, whereas the field devices are devices which can either monitor or control the process. The cluster head acts as the agent of NM and is responsible for constructing the star network of field devices and monitoring its performance. The field devices should act as a cluster member only and have to send data to the cluster head. Therefore, in a WIA-PA hierarchical network structure, the first step involves connecting the routing devices and gateway in a mesh topology format, whereas, in the second step the field devices are connected to the routing devices in a star based topology.

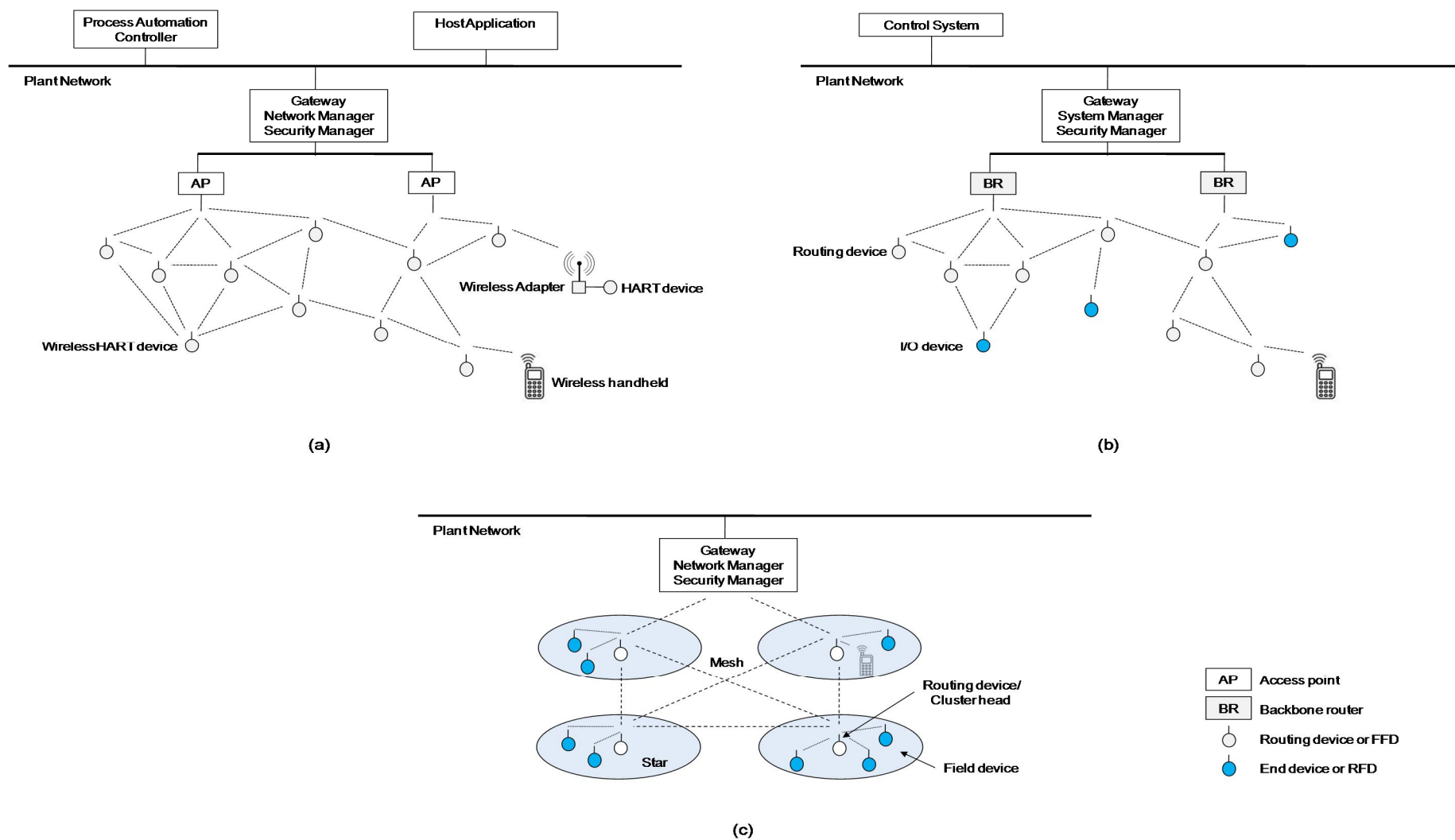


Figure 2.6. Examples of typical (a) WirelessHART (b) ISA100.11a (c) two-layered star-mesh WIA-PA networks. Adapted from WirelessHART (2009), ISA-100.11a (2009), WIA-PA (2009).

2.4.5 Comparison of Industrial Standards

This section will provide a comparison of the four main standardized wireless networking technologies presented above, namely ZigBee PRO, WirelessHART, ISA100.11a and WIA-PA. The reason for exploring these specifications in detail is that research into wireless process control needs a good understanding of the technologies on which the results of research will be implemented.

Figure 2.7 represents the seven-layer OSI model and maps it to WirelessHART, ISA100.11a and WIA-PA stack architecture. A standard WSN stack implementations consist of five-layers as opposed to seven-layer reference OSI model (Kuorilehto *et al.*, 2007). The physical layer of all of them is based on IEEE 802.15.4 radio. WirelessHART and ISA100.11a further define the four higher layers. In the case of WIA-PA the above three layers are defined by the standard. Table 2.7 presents a comparison of these technologies. A discussion on each row is provided underneath.

Origins

ZigBee PRO is a variant of ZigBee with enhancements for high security and message routing. One of its main uses is for building automation. WirelessHART extended the existing HART protocol, for getting HART information from existing field devices. HART is a bi-directional communication protocol which transmits digital information in addition to process data, for instance remote diagnostics for a field device. It is widely used in the process industries. ISA100.11a and WIA-PA are new protocols created specifically for wireless process automation.

Physical layer

The physical layer is the same in each case when operated in 2.4GHz ISM band using DSSS and O-QPSK as specified in the IEEE802.15.4 standard. DSSS provides resistance to interference from other sources and efficient use of the available channels. IEEE 802.15.4 standard defines three bands of operation. In case of WirelessHART and ISA100.11a the wireless activity is confined to 2.4 GHz ISM band. Furthermore, a restriction on the use of Channel 26 is found in WirelessHART (WirelessHART, 2009).

Data link layer

ZigBee PRO has adopted the CSMA/CA access method of IEEE802.15.4, and for this reason does not guarantee deterministic communication. On the other hand, WirelessHART and ISA100.11a standards deviate from the CSMA/CA approach in the IEEE802.15.4 standard [Wagner, 2010]. They implement TDMA which provides deterministic time slots for the multiple transmitters in the network. The time slots in WirelessHART are fixed at 10 ms, whereas, they can be configured in ISA100.11 and WIA-PA. WirelessHART and ISA100.11a media access and network layers are based on Time Synchronized Mesh Protocol (TSMP) protocol originally designed by Dust Networks. According to Pister *et al.* (2008), TSMP is a reliable and scalable wireless networking protocol. In the case of WIA-PA the data link layer is based on IEEE 802.15.4 MAC. The paper by Zhong *et al.* (2010) considered some shortcomings the data link layer of WIA-PA in process control related to concurrent handling of real-time and non-real-time messages.

Channel hopping gives industrial protocols a high level of communication reliability. ZigBee PRO supports frequency agility, which consists of scanning available channels to determine the channel with least interference, noise and traffic which is then selected and used by all ZigBee devices. Other protocols allow individual devices to choose different channels or different time slots for communication of individual packets. Poor quality channels may be blacklisted and taken out of use, and channels that have been found to provide good transmission can be whitelisted for preferential use. Channel hopping also enhances network security because devices outside the network do not have information about the hopping sequence.

The use of TDMA based MAC enables the design of a wireless network which is predictable. It is an important requirement for process automation and is achieved via TDMA because it allows accurate determination of latency. The operation of a TDMA based network requires time synchronization and a central NM. However, the use of a TDMA based centralized network approach limits a network size and its tolerance to varying network conditions as highlighted by Suhonen *et al.* (2012).

Network layer

The nodes in a wireless network are either Full Function Devices (FFDs) which can communicate with any other node, or Reduced Function Devices (FRDs) which can communicate only with an FFD. In general, FFDs do more communication and processing and hence consume more power. FFDs are needed to create a mesh network. The terminology is adopted from the ZigBee standard and is applied to the rest of the standards for a comparison. The network topologies supported by the various standards are illustrated in Table 2.6. The top left panel shows a WirelessHART mesh network. The gateway provides buffering of sensor data, diagnostics data and event notification. The field devices must be HART devices, either sensors or actuators configured in a mesh network. Mesh topology gives the network the capability of self-repair and self-optimization. All nodes are FFDs in the Wireless HART network. WirelessHART supports three modes of data routing, namely, graph routing, source routing and superframe routing as mentioned before.

Figure 2.6 (b) depicts a typical ISA100.11a network which comprises of field devices (sensors and actuators) and mobile handheld devices. The devices can be arranged in different topologies such as star or multi-hop mesh network. Some of the field devices are FFDs and may forward messages from other devices. The standard also allows the use of a high-speed network backbone (wired or wireless) for wide-area installation. ISA100.11a supports graph and source routing. ISA100.11a also supports IPv6 addressing.

A WIA-PA network, shown in Figure 2.6 (c) comprises a hybrid topology with mobile handheld and field devices arranged in a star configuration around FFD nodes (cluster head) which are connected in a mesh. The network layer adopts static routing method for forwarding data packets (Zhong *et al.*, 2010).

Gateway and NM

The wireless networks are linked to the rest of the plant automation network via a gateway, which was discussed in Section 2.4.2. The gateway acts as a single entry point to the WirelessHART network. Wireless access points before the gateway detect and decode the wireless RF signal.

The wireless field network is managed by a NM which is responsible for setting up a network and supervising the network operations. It manages time slots, routing tables, schedules communications, monitors network health and queries field devices for information. In commercially available products, the gateway, NM and security manager are often housed in one system.

Security

The security methods used by the protocols are listed in Table 2.6 They include: authentication which specifies which devices are allowed to join the network, encryption of data, and integrity checking which establishes that messages have not been tampered with.

The security managers shown in Figure 2.6 are software components that manage secure operation of the network by controlling access and deploying security keys, data encryption and integrity checking and device security. Variation in security policies are found in these standards and are summarized in Table 2.6.

Conclusion

This sub-section has compared the standards and protocols suitable for use in wireless process automation. The aim has been to demonstrate why networks based on IEEE 802.15.4 are preferred and to support the discussions on research directions that follow in the rest of the thesis. Additionally, a detailed investigation into the standards based on the IEEE 802.15.4 defined PHY are analyzed and it has been found that WirelessHART and ISA100.11a are well positioned to address the demands of process automation.

In addition, due to the similarities between WirelessHART and ISA100.11a and to avoid repeating the history which resulted in multiple fieldbus standards, industry is working towards the convergence of these two standards (ISA100.12, 2011).

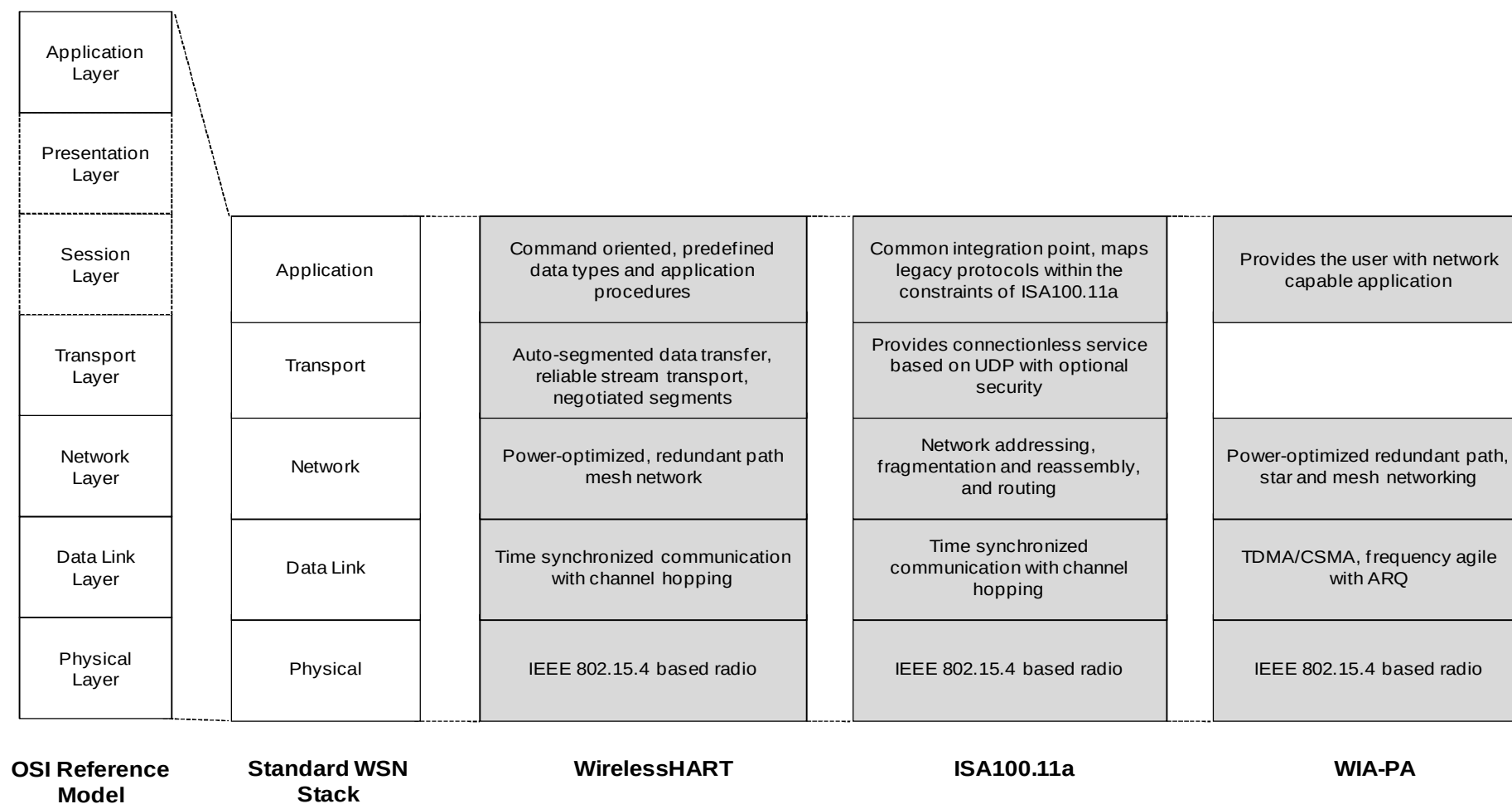


Figure 2.7. Illustrating the relationship of WirelessHART, ISA100.11a and WIA-PA to the reference OSI seven-layer model.

Table 2.6. Comparison of ZigBeePRO, WirelessHART, ISA100.11a and WIA-PA networks.

	STANDARDS			
	ZigBee PRO	WirelessHART	ISA100.11a	WIA-PA
Origins	Extension of ZigBee	Extension of HART protocol	New protocol	New protocol
Physical layer				
Transceiver standard	IEEE802.15.4-2003	IEEE802.15.4-2006	IEEE802.15.4-2006	IEEE802.15.4-2006
Frequency band	868/915 MHz, 2.4GHz	2.4 GHz	2.4 GHz	868/915 MHz, 2.4GHz
Data link layer				
Media access control	CSMA/CA	TDMA	TDMA (CSMA/CA optional) ¹	TDMA and CSMA hybrid
Time slot size	N/A	10ms	Configurable	Configurable
Coexistence mechanism (Interference avoidance)	Frequency agility	Frequency hopping (Timeslot hopping)	Frequency hopping (Timeslot hopping and slow channel hopping)	Frequency hopping (Timeslot hopping and adaptive frequency hopping)
Channel Management Features	Preferred Channel	Blacklist	Whitelist & Blacklist	Adaptive
Determinism	No	Yes	Yes	Yes ²
Network layer				
Topology	Star, tree, mesh	Mesh, star	Star, tree, mesh	Hybrid of star and mesh
Device type	FFD, RFD	FFD	FFD, RFD	FFD, RFD
Reliability (Spatial diversity support)	Yes	Yes	Yes	Limited ³
Other comments				
Security	Authentication, integrity check and encryption at network layer and application layer	Authentication, integrity check and encryption	Authentication and encryption available at data link and transport layers	Data Integrity, data confidentiality , device & data authentication
(Policy)	(Standard Security & High Security Modes)	(Not specified)	(Exists at five levels)	(Based on business, service type and objects)

¹ Refer to Akyol et al. (2010) for further details.² IEEE 802.15.4 MAC supports GTS. For real-time issues linked to WIA-PADLL refer to Zhong et al. (2010).³ Cluster heads form mesh network but not the cluster members.

2.5. Chapter Summary

This chapter has presented a review of wireless communication technologies. The first section gave an overview of the wireless sensor network applications relevant to the process industry. This section was accompanied with examples of actual implementations reported in literature.

The second section introduced the automation pyramid and highlighted the functional hierarchy. It also mapped the scope of the research presented in this thesis to the automation pyramid. Furthermore, it was identified that the networking requirements at the bottom of the pyramid are the stringent. In addition, it was explained that the operation of wireless network at this level is subjected to constraints imposed by the application. It was also highlighted that applications especially those linked to process

safety and control mandate the need for predictability and robustness in network operations. Moreover, the application classes defined by the ISA 100 working group were introduced and expanded to identify the difference in networking requirements of each application.

The following section then compared the commercially available wireless technologies, namely Wi-Fi, Bluetooth, UWB and ZigBee. The reason for reviewing these technologies was to analyze their suitability for use in process automation. It was concluded that these commercially available wireless communication technologies in their original format are not able to provide services which are vital to process automation.

Afterwards, ZigBee PRO, WirelessHART, ISA100.11a and WIA-PA were reviewed. The reason for selection of these four technologies is that they are based on IEEE 802.15.4 standard, which offers a good performance physical layer. Also, they are aimed at industrial applications and are claimed to be industrial strength. Reliability in the harsh industrial environment and associated security has been widely considered in the formulation of these standards and the underlying protocols. It was found that the use of spatial, frequency and time diversity techniques in particular have resulted in a creation of a reliable network.

In short, the reason for including the overview presented in this chapter was twofold. Firstly, it was needed to ascertain that only few amongst the wide range of available wireless technologies are able to address the demand of process industry. The second was to identify the methods and techniques adopted by the technologies which are considered suitable for process automation. These technologies have, so far, demonstrated to be capable to carry out monitoring and open-loop control related tasks. However, the latency control mechanism needs to be designed in order to transit from open-loop application domain to closed-loop control domain.

The outcome of the review presented in this section, especially the details of the IEEE 802.15.4 compliant physical layer and the diversity techniques highlighted here will be used in the later chapters.

CHAPTER 3

Background and Context: Review of Literature

This chapter will present the review of related literature and will examine the relevance in addressing the research problems specified in Chapter 1. As part of the research work presented in this thesis, three key issues have been addressed. They are linked to time synchronization in distributed systems, process control over a wireless network, and TPC in industrial wireless networks. Therefore, the three key sub-sections of this chapter comprise of an overview of background and context, available methods and approaches to solve similar problems, and the associated challenges and constraints. The chapter further documents the methodologies and approaches which are adopted or built-upon as part of the PhD research to address the given issues.

3.1 Time Synchronization in Distributed Systems

The methods used for keeping record of time, the instruments used for measuring time, the accuracy in timekeeping, and even the definition of second, has gone through transformations over ages. A clock is a device used for keeping track of time, which essentially comprises of an oscillator and a counter. The oscillator is used for determining the length of a time interval and is meant to produce periodic event that repeats at a constant rate. The counter keeps a track of the oscillations. Collectively they are used for timekeeping. It is the accuracy of the resonator which has in recent history seen significant improvements. The crystal in the oscillator is the resonator.

3.1.1. Overview: Historical Perspective

Figure 3.1 shows a timeline identifying the key milestones related to time and timekeeping. From the figure it can be seen that the earlier devised methods for timekeeping involved the use of sundials where the apparent motion of the sun was used as the resonator. Later on, the use of candle clock, water clock, sandglass and pendulum clock prevailed. It was up to 19th century that the use of mechanical clocks was common (Bregni, 2011). It was in the late 19th century and in the 20th century when significant advancements were made in timekeeping technology. Those advancements which are relevant today and those which are directly or indirectly related to the domain of time synchronization in distributed systems are highlighted (in red) in Figure 3.1. These important and relevant milestones are as follows:

- 1880: Piezoelectric effect discovered by Curie brothers (Taylor, 1985). Commonly used quartz resonators in clocks used today consist of a piece of piezoelectric material.
- 1898: Sir Howard Grubbs proposed the idea of a radio controlled clock. In those days, time signals were distributed by telegraph (Simcock, 1992).
- 1903: The first radio time signal was broadcast in September 1903 by the US Navy (Hellweg, 1940).
- 1918: The first use of piezoelectric crystal in an oscillator (Vig, 2000).
- 1923: WWV (HF transmitter) started broadcasting standard frequencies on a weekly schedule.
- 1949: First atomic clock, based on ammonia was introduced by Harold Lyons (Bregni, 2011). Its stability was limited.
- 1955: Essen and Perry start keeping time with a cesium atomic clock (HP, 1997). They demonstrated the potential for an accurate atomic frequency standard.
- 1966: MSF (LF transmitter) started continuous operations. It is the principal dissemination method for standard frequency and time in the UK.
- 1967: The definition of unit of time, the second, was replaced. Earlier, it was defined as the fraction 1/86400 of the mean solar day (Lerner, 1996). The new definition of time as in use today was provisionally defined at the 13th General Conference on Weights and Measures, and is as follows (Rao, 2004):

“The second is the duration of 9,192,631,770 periods of radiation corresponding to the transition between the two hyperfine levels of the ground state of the Cesium-133 atom”

It is this definition of a second which is adopted in the SI unit of time.

1986: In 1884, at the International Meridian Conference, prime meridian was placed at Greenwich (PoP, 1884). Originally, Greenwich Mean Time (GMT) was set up to aid navigators and was used as a time standard against which other time zones were referenced. GMT is the time linked to the rotation of Earth, and is the mean time Earth takes to rotate from noon to the following noon (ASCE, 1994). In 1986, GMT was replaced by Coordinated Universal Time (UTC). It is the International time standard kept by laboratories around the world, and is a high precision atomic time standard. The International Bureau of Weights and Measures makes use of the time data collected from these geographically distributed time laboratories around the world to provide the standard UTC, which is accurate to about a nanosecond per day (Harmegnies et al., 2009). UTC time scale is kept close to the mean solar time at Greenwich (Doody, 2009).

1995: In 1978, first GPS satellite was launched and in 1995 GPS was announced operational (HP, 1997). GPS is mostly known for providing location services. However, amongst many different methods of time dissemination, GPS is the most accurate method. The time broadcast from GPS satellites are in the UTC format.

Further details about these advancements and milestones are given in the following books and papers: Jespersen and Fitz-Randolph (1999), Bregni (2011), HP (1997) and Koscielniak (2004).

The ability of a clock to maintain its time accurately depends on the frequency accuracy and stability of its reference oscillator. Figure 3.2 shows the typical timing uncertainty expected after a day (24 hours) of operation in the typical mechanical, quartz and atomic clocks. The graph highlights that atomic clocks have superior performance compared to both the mechanical and quartz clocks. However, the quartz oscillators which are widely used in quartz clocks and in embedded systems, by far, are the most common time and frequency standard. Amongst the different types of oscillators which are based on quartz crystal, TCXO strikes a balance between performance and cost.

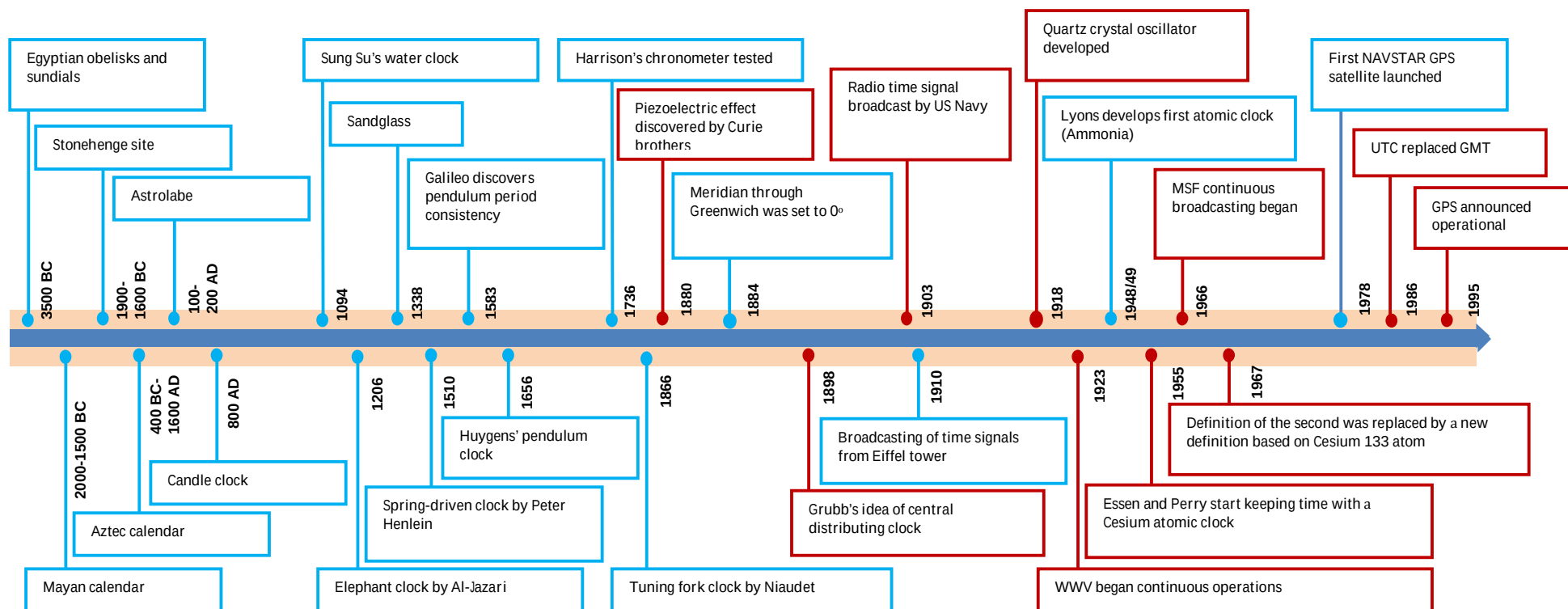
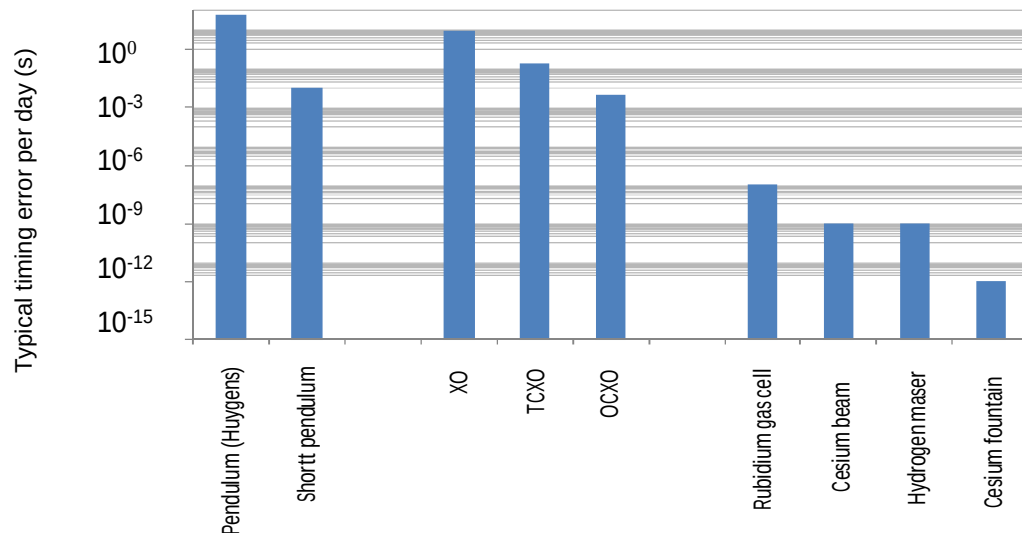


Figure 3.1. Advancements and milestones in timekeeping. The data presented in this figure is predominantly based on the information collected from the references presented in Section 3.1.1.



Type	Mechanical clock	Quartz clock	Atomic clock
Time Period	1656-1920's	1918-onwards	1952-onwards

Figure 3.2. Typical timing accuracy over a period of 24 hours of various standards. Information sources, Bishop (2005), Bishop (2008), Bregni (2011) and Simonis (2008).

Time synchronization

In order to achieve and maintain accurate time synchronization two different approaches exist:

- Distributed clocks are synchronized to an actual time standard like Universal Coordinated Time (UTC), referred to as *physical clocks* (Hofmann and Hilgers 1998). Such time and frequency methods and services include: internet and dial-up computer time services, HF and LF operated time and frequency standard stations and Global Positioning System (GPS).
- Distributed clocks can be relatively synchronized to one another, referred to as *logical clocks* (Rowe, et al. 2008).

Furthermore, in order to achieve time synchronization, either a time synchronization protocol can be employed or a specialized hardware can be used in conjunction with the clock. Time synchronization relative to UTC is within the scope of the research presented in this thesis.

3.1.2. Time Synchronization Protocols

The protocols which offer time synchronization services are referred to as time synchronization protocols. In general, the exchanges of messages which occur during time synchronization are subject to various delays. The four components which contribute towards synchronization error are [Sundararaman *et al.* (2005), Sivrikaya *et al.* (2004)]:

- *Send time*: It is the time spent at the sender node to construct the message and access the network.
- *Access time*: It takes into consideration the time taken to access the communication channel.
- *Propagation time*: Time for the message to travel from source to destination.
- *Receive time*: This is the time taken by the receiver to receive the message and notify the host.

Time synchronization protocols address these components. In order to achieve higher accuracy, uncertainties in these components are to be minimized. Furthermore, time synchronization challenges include limited energy, bandwidth, hardware limitations, protocol complexity, network topology and unstable network connections.

The time accuracy and stability limits for the operation of a distributed sensing and control system are defined by the application requirements. These were discussed in Chapter 1 and 2. The system level requirements of industrial monitoring and control systems, spatially distributed nature of wireless telemetry units, and the limited onboard resources limits the relevant time synchronization protocols, and are briefly discussed next.

NTP for WSNs

Amongst the existing protocols used for time synchronizing, a wired distributed network includes Network Time Protocol (NTP). It is used for synchronizing computers over a network. NTP has been proven effective in the internet. According to Elson *et al.* (2003), the use of NTP is not suited for WSNs. The reasons outlined for non-suitability were based on the following; absence of highly accurate master nodes and the assumption that the pair of nodes on a network are constantly connected and

experience consistent communication delays in packet exchanges. In a WSN, communication delays are inconsistent and unpredictable (Song *et al.*, 2006).

NTP for telecommunication network

Furthermore, the work from Motorola (2009) shows that the level of accuracy achievable at client using NTP over GPRS network is up to 100 ms on wide area networks. Moreover, the paper published by Miškinis *et al.* (2011) last year has highlighted the issues linked to timing and synchronization in telecommunication networks. They have highlighted that the issues are linked to asymmetrical uplink and downlink.

Time synchronization protocols used in WSNs

Time synchronization protocols have been widely studied by the research community working in the area of WSNs [Ranganathan (2010), Sundararaman *et al.* (2005), Sivrikaya *et al.* (2004)]. Based on the application requirements such as topology-independency, scalability and fast convergence, the use of in-band time synchronization protocols is a limiting constraint.

Some well-studied protocols include Reference Broadcast Synchronization (RBS) (Roche, 2006), Time-sync Protocol for Sensor Networks (TPSN) (Heuber and Haritha, 2007) and Flooding Time Synchronization Protocol (FTSP) (Maroti *et al.*, 2004). RBS protocol uses broadcast method to disseminate its time information which is received by nodes in its coverage region then the receiving nodes can record the local time and synchronize (Roche, 2006). Sequence of messages is exchanged to estimate offset. RBS achieves high level of energy conservation by using synchronization only when required (Maroti *et al.*, 2004). In a multi-hop communication often found in sensor networks, RBS protocol would lose accuracy because of high degree of variability in message transmission. The disadvantages of RBS protocol include high number of message exchanges and high network traffic overhead (Ping, 2003). The use of TPSN attains better performance compared to RBS but does not calculate clock drifts and limits accuracy (Akl *et al.*, 2007). The same document explains that both RBS and TPSN suffers from uncertainty of medium access control (MAC) time stamping, whereas, FTSP reduces all such occurrences with the exception of propagation time and utilizes less resources. FTSP can provide synchronization in multi-hop topology and the algorithms

can adapt to node failure, it uses linear regression for calculating clock skew and requires initiation period due to LR (Maroti *et al.*, 2004). Therefore, it is apparent that the different time synchronization protocols have their own merits of selection.

Predominantly, due to the need for topology-independent, fast-convergent and scalable time synchronization solution which can be applied on heterogeneous network (i.e. networks supporting different communication technologies), time synchronization protocols will be restrictive and will impose a constant burden on available data communication networks. Hardware assisted time synchronization which utilizes a long range time broadcast signal can concurrently address multiple of these issues. Next, these available options are discussed.

3.1.3. Hardware Assisted Time Synchronization

There are two available options for hardware assisted time synchronization. Based on their availability (i.e. coverage), they are referred to as global availability and regional availability in Figure 3.3. They include the following:

Global availability

- GLOBAL POSITIONING SYSTEM (GPS):

It can be used to achieve time accuracy within few microseconds of UTC [Kim *et al.*, (2012), Lacatus *et al.* (2012), Meyer *et al.* (2012)]. GPS receivers successfully achieve sub-microsecond time accuracy under specific installation conditions. The main limitation is the requirement for a clear sky view to operate. This is difficult to achieve when the monitoring and control is done underground (e.g. manholes for the water/gas utilities), indoors (e.g. treatment, pumping and process plants) or in urban environment. Indoor GPS reception requires sensitivities 20 dB below that of outdoor receivers, making it susceptible to jamming from low-power sources (Bickerstaff *et al.*, 2005). Other constraints include the relatively high power consumption (Dedes and Dempster, 2005). They are also relatively expensive compared to some other means (such as a radio clock) for getting access to the UTC.

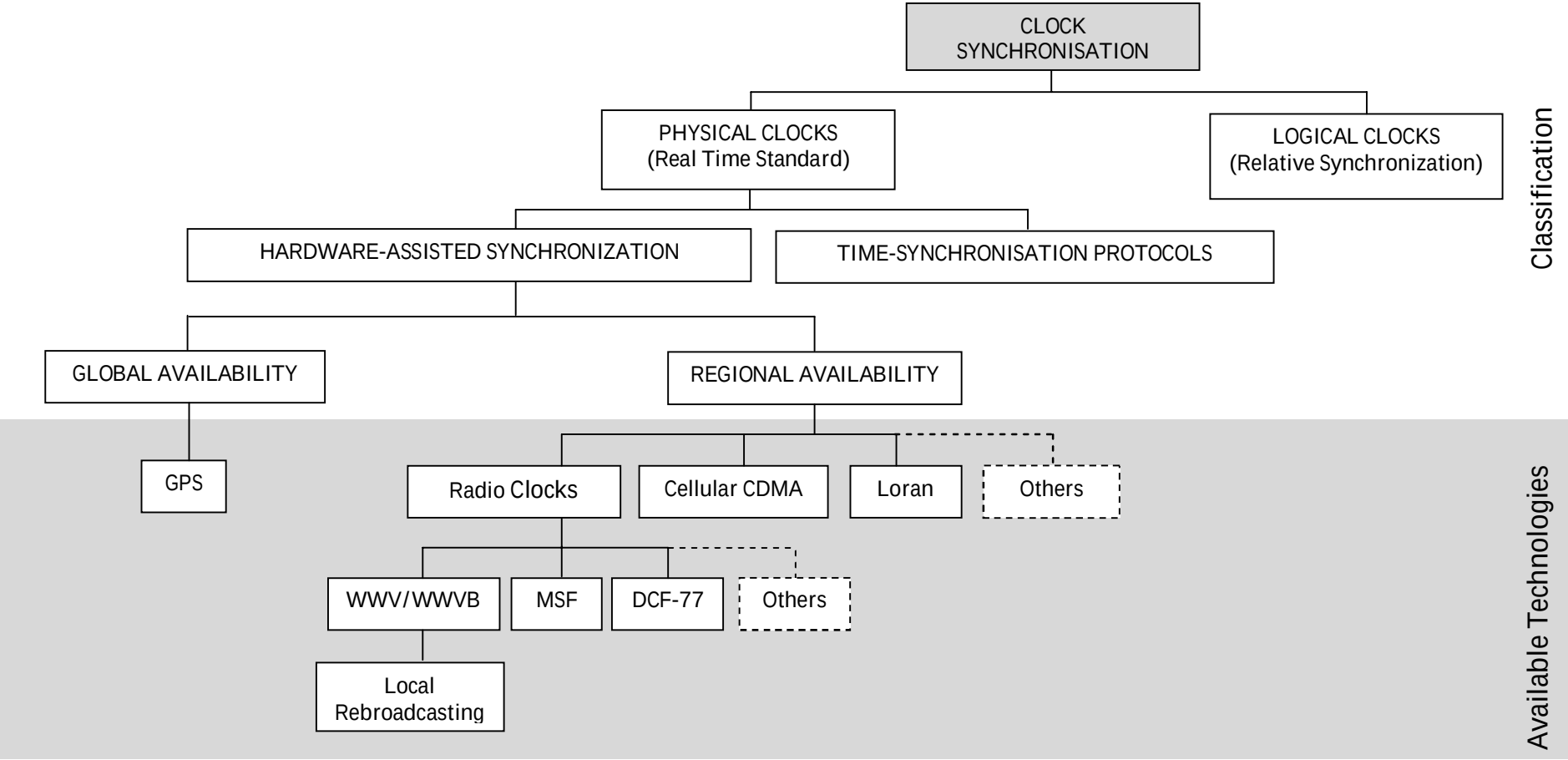


Figure 3.3. Hierarchical tree showing available methods for achieving time synchronization in distributed systems.

Regional availability

▪ TERRESTRIAL TIME BROADCASTING RADIO STATIONS:

There are various dedicated radio signals available around various regions of the world which are disseminating accurate and reliable civil time (Lombardi, 2002). Table 3.1. provides a summary of terrestrial time broadcasting stations and their operational frequencies. The majority of these transmitters operate at the Low Frequency (LF) spectrum. The LF time signal broadcast covers a wide geographic area, it penetrates buildings and underground utility services close to the surface and no LOS is necessary between the transmitter and receiver (Lombardi, 2010). The receivers are cheaper and consume less power than GPS modules.

▪ CODE DIVISION MULTIPLE ACCESS (CDMA):

CDMA is a digital radio technology used in mobile telephone networks. CDMA requires time synchronization within a few microseconds among all fixed and

Table 3.1. Terrestrial time broadcasting radio stations. Sources include [BIPM (2010), NIST (2010), NPL (2007), DCF77 (2011), NICT (2005), HBG (2008), NRCC (2010) and Kuhn (2006)].

Country	Call Sign	Frequency (kHz)
UK	MSF	60
Canada	CHU	3330, 7850, 14670
China	BPC	68.5
	BPM	2500, 5000, 10000, 15000
France	TDF	162
Germany	DCF77	77.5
Japan	JJY	40, 60
South Korea	HLA	5000
Russia	RBU	66.66
	RWM	4996, 9996, 14996
Spain	EBC	4998, 15006
USA	WWVB	60
	WWV	2500, 5000, 10000, 15000, 2000
	WWVH	2500, 5000, 10000, 15000

mobile stations so that cellular signals originating from synchronous stations operate in compliance with IS-95 (Dooley and Nandi, 1998). The CDMA fixed stations have GPS receivers and consequently they act as a GPS repeater, which ensures a reliable timing reference. However, compared to GPS time synchronization, CDMA has significantly higher power consumption. This option is expensive and is available in areas where cellular systems offer such services.

- LONG RANGE NAVIGATION (Loran):

Terrestrial based radio navigation systems utilize various ground stations to determine the location of the receiver. This broadcast does not contain time information. However, receivers can produce on-time UTC pulse (Wechsler, 1990). Loran systems are being phased out (NC, 2010), hence they are not a viable option.

To summarize, GPS signals are available worldwide, however, they require a line-of-sight to operate. On the other hand, the selection of available hardware modules which can provide access to the physical time and have region based availability limits the options to either radio-controlled clocks or CDMA based time synchronization solutions. Moreover, their selection depends on the application requirements. They are discussed and analyzed in the following section.

3.1.4. Challenges

The main challenges which need to be addressed in designing a robust time synchronization solution are:

- The operational environment which includes: variable spatial distribution ranging from meters (e.g. a pumping station/building) to tens of kilometers (e.g. monitoring utilities networks), with no or limited LOS. Elimination of the need for in-band time synchronization protocols.
- The time to achieve and maintain network-wide synchronization is independent of network size, number and distance between distributed nodes and the sequence of their deployment.
- Independence between various processes such as data acquisition, in-band communication, control and time synchronization.

Elimination and minimization of sources of time synchronization error

It was explained earlier that the time synchronization uncertainty relates to the estimation and elimination of delays incurred from inception to the reception of the time synchronization messages. They are provided by the time synchronization protocols. In the case of hardware assisted time synchronization, similar uncertainties also exist. Therefore, a mechanism is required to eliminate those errors which constitute to increasing time synchronization error relative to the UTC. The model relevant in the case of hardware-assisted time synchronization is sender-receiver paradigm. The sender, in the case of a radio clock, is the transmitter and the receiver is the radio-clock. The errors which are linked to the transmitter (the time broadcasting source) cannot be controlled, whereas, those which occur after the time dissemination can be catered for. They are described next.

Sender-receiver synchronization paradigm

In sender-receiver synchronization, the sources of synchronization error are affected by random events. As mentioned earlier, there are four sources of errors which contribute to time synchronization error. The use of radio-controlled clocks will help eliminate send time and access time linked to on-time markers in a time frame because all nodes will experience same effect of these two sources of error. Regarding the propagation time, the further the devices are relative to the transmitter; this error will increase relative to UTC. However, if the nodes in a WSN under investigation are within close proximity of one other, say meters to a few kilometers then this error relative to one other is still within few microseconds. Therefore, the relative time synchronization error amongst the radio clocks within this approach comes down dominantly to receive time error. However, relative to UTC it will encompass all those errors. For a given receiver and location, these errors can be estimated and compensated.

3.1.5. Related Work in Context

The use of radio clocks and in some cases their derived systems have been proposed in literature for time synchronizing distributed systems. However, very limited performance results have been published. A brief review of some of the relevant work is as follows:

Allison *et al.* (2003) proposed the use of WWVB receivers for time synchronizing geographically distributed data acquisition systems. They have presented a method for time synchronization. Based on theoretical analysis, they have highlighted that the only limitation using WWVB is the 100 ms variance of the WWVB time code. WWVB transmitter serves North America. The results of the implemented system were not reported. Maloco *et al.* (2006) on the other hand proposed to use MSF clocks for time division multiplexing synchronization in a housing community sensor network. It was identified that the falling edge of the start of a new minute can be used for time synchronization if within a 3 ms tolerance limit. This tolerance is linked to interference, and influences the hardware output. Since their work was published, in 2007 the MSF transmitter was relocated from Rugby to Anthorn in Cumbria, England. An enhancement to the approach of directly using radio clocks was the work by Rowe *et al.* (2008). They used AM transmitters to locally rebroadcast the atomic time signals from WWVB transmitter. The system developed by them does not decode the entire time frame, and only detects the rising edges associated with the WWVB signal. They used power grid of the building as the antenna for broadcasting time synchronization pulse. The carrier current signal radiation was limited to within 50 meters of the building. This approach was primarily for indoor applications. They have also proposed using WWVB receivers for time synchronization in outdoor applications but the performance data was not reported. Niemann *et al.* (2009) have proposed using the German based DCF77 radio transmitter for global time synchronization of sensor networks. They have identified the requirements of the proposed system and have identified means to achieve high accuracy for decoding distorted signals. However, no results were presented by them.

The research, which is presented in this thesis, is an extension of the earlier work published in Ikram *et al.*, (2010). After that publication, a paper from Chen *et al.* (2011) was published which has highlighted the same issues for two different transmitters. They have investigated into two time broadcasting radio stations, DCF77 and WWVB. They have reported the outcome of experimental finding regarding the radio time signal availability, quality of synchronization across motes and power consumption. They have also compared their results to an alternative GPS solution and to a message passing protocol (which was FTSP) to compare its energy-efficiency. An important observation

regarding their reported time synchronization accuracy is that they considered it as the difference in reported time by a mote at a particular instance in time to the mean for that particular instance. In the case of WWVB, it was reported that 90% of synchronization error percentile in the indoor experiment was 3.9 ms, and for outdoor experiment was 4.3 ms. These readings are based on perceived UTC time derived from WWVB signal. These readings are not marked against an independent and actual UTC time source. Finally, the work from Maloco *et al.* (2010) has examined the use of MSF receivers for time synchronization. They have also compared the output of three receivers to see how close they align. Synchronization accuracy reported by them was within 5 ms for 99.65% of time for data samples collected over a period of one month.

3.1.6. Summary

Time synchronization is of utmost importance to distributed systems, from both application and networking point of view. It plays a pivotal role to establish a deterministic, efficient and secure data-link. It is due to this central importance that it has received extensive attention from the research community. In order to automatically time synchronize a distributed unit to the ongoing UTC either a time synchronization protocol or dedicated hardware can be used. This section has focused on hardware-assisted time synchronization solution and has justified the reasons for its selection. The use of radio-controlled clock is considered to be feasible within the context of time synchronization of distributed systems, especially because of the need for topology-independency, fast-convergence and energy-efficiency. Furthermore, the different components which affect the time synchronization accuracy are discussed alongside with ways to estimate and minimize them. Finally, the relevant literature about the use of radio clocks is analyzed and avenues where the research falls short have been identified.

3.2. Wireless Communication in NCSs

This section of the chapter focuses on NCS and especially on its new extension, the WNCS. In particular, wireless feedback loops will be examined and those networking and architecture related issues which can influence the performance of a control application will be identified and analyzed. As a result, this section will provide the basis

of the study regarding the performance of closed loop control operating over an IEEE 802.15.4 compliant network presented later in Chapter 5.

3.2.1. Control over Wireless Network: Overview and Approach

In a traditional control system, it is assumed that the communication networks offer instant communication service without data loss (Zhang, 2001). This assumption in control implementation is valid given that the dedicated point-to-point communication links are used, as is the case in 4-20 mA systems. However, the use of shared communication networks in control loops violates these arguments. It is because in a shared network the data packets are subjected to network induced delays, processing delays, and may even experience data-loss. These delays can degrade a system performance and can lead to instability (Zhang, 2001)). Therefore, they have to be carefully taken into consideration in NCS design. The approach to address this issue was initially dominated in the research community by two means [Mazumder (2011), Wang and Liu (2008), Hristu-Varsakelis and Levine (2005), Tipsuwan and Chow (2003)]:

- **CONTROL AWARE NETWORK:**

In this strategy, the approach is to design or select a communication protocol and the network infrastructure which will support minimum delays (i.e. bounded latency) and ideally no packet losses. It has resulted in the design of specialized field communication protocols such as Profibus, Foundation Fieldbus (FF) and DeviceNet. In this approach, wider issues need to be examined, such as, network topology, real-time scheduling, control structure and architecture. Mohammadi and Akl (2005) have provided a survey on scheduling algorithms for real-time systems. Saifullah *et al.* (2010) has further examined the real time scheduling issue in WirelessHART networks. A survey on real-time Medium Access Control (MAC) protocols is provided by Teng and Kim (2010). They have classified real-time MAC protocols into hard real-time and soft real-time protocols and have compared them in terms of energy efficiency, timeliness, synchrony and adaptability. An obvious trade-off between energy conservation and latency was emphasized.

- **NETWORK AWARE CONTROL:**

In this approach, the design of control application has to compensate for the channel imperfections. Hence, communication imperfections are modelled with

time delays and packet loss probability [Naghshtabrizi and Hesphana (2007), Park, (2011), Yang (2006)]. The process measurement sampling, control algorithm execution and the resulting actuation are closely linked to scheduling. Hong (1995) presents a sampling time scheduling methodology to appropriately select the sampling period for NCSs. Moreover, Tipsuwan and Chow (2001) proposed a control adaption methodology where the controller adapts its parameters (for instance, its gain) based on network traffic conditions. Hence, the parameters are selected based on traffic conditions and are optimal for a given state of the network. Furthermore, Tipsuwan and Chow (2004) propose and examine a methodology to enhance the performance of Proportional-Integral (PI) controller by using gain scheduling so that it can be used over traditional IP networks.

These approaches have worked well in scenarios where either the control-over-channel can be strictly regulated or in the latter case where these parameters can be accurately modelled. However, in the case of licence-exempt wireless networks these approaches are not feasible on their own. The reasons are linked to the limited onboard power, time-varying channels, limited spectrum, and interference. Generally, in a wireless communication network as opposed to wired network, delays, packet-error and losses are to be expected (Mazumder, 2011). Therefore, in recent years a different approach has surfaced to address control-over-wireless issue, which is the co-design approach [Johansson (2008), Colandairaj *et al.* (2005), Liu and Goldsmith (2004)]:

- CO-DESIGN APPROACH:

This approach involves the joint-design of network and the controller. The integrated design of application and communication layer will address the shortcomings of earlier mentioned approaches. This is achieved via designing a controller which is tolerant to network failures, and the network is optimized for end-to-end control performance (Saifullah *et al.*, 2012) Therefore, a co-design approach will help leverage the burden on communication network by providing an adaptive control layer.

Most of the work related to this approach is in simulated models, and will need to be implemented in hardware to test its performance in real scenarios. In terms of cross-layer design involving PHY layer, it is technology dependent as to what parameters can

be adapted. In this adaptive technique, initial work is done on IEEE 802.11 based technologies such as in Colandairaj *et al.* (2005), which is different compared to IEEE 802.15.4. The latter mentioned technology is what is currently being used in industrial wireless standards. A step closer towards IEEE 802.15.4 standard based industrial communication in NCSs is the work from Saifullah *et al.* (2012). They have examined the scheduling-control co-design problem of determining the optimal sampling rates of feedback control loops for WirelessHART networks with the objective of keeping control cost low while ensuring end to end bounded data delivery.

On the other hand, some research work is also dedicated to finding the control algorithms which are suitable for distributed wireless control, such as open or closed-loop control, Proportional-Integral-Derivative (PID) or Model Predictive Control (MPC) [Vilanova (2011), Liu *et al.* (2011), Tipsuwan and Chow (2003)]. The work presented by Park (2011) examines the performance of LQC in a wireless network.

In short, the new mentioned approach based on co-design principle is what is believed to be a solution which can help achieve closed-loop control over a wireless network.

3.2.2. Current Practices and System Architecture

In this section, a brief overview of the current practices as are employed in the wired NCS is introduced. It will provide a platform to introduce the limitations which are imposed on WNCS, if they mimic the conventional control practices. The identification of such limitations has led to the development of new features to circumvent the WNCS limitations without jeopardizing the control-loop performance. Some of the key ones will be discussed in this section.

Closed-loop control comprises of sensors (plant measurements), controllers (computing control action) and actuators which take action based on the controller output. The loops are executed periodically. In a NCS, the control loops are coordinated and closed over a shared real-time communication network such as a fieldbus, as shown in Figure 1.4. The measurement and controller outputs are transmitted in the form of digital information packets. If wireless communication is employed in a NCS, it is termed a Wireless Networked Controlled System (WNCS). A WNCS comprises nodes that communicate by means of wireless links.

Two patterns of communication commonly found in the NCS literature are the direct structure and hierarchical structure (Wang and Liu, 2010). The structures with their data flows are shown in Figure 3.4. The network resources used for data transfer are shared amongst sensors, controllers and actuators in the case of direct structure, as shown in Figure 3.4(a). The hierarchical structure uses a main controller which coordinates the operation of local closed-loop controllers over a network as illustrated in Figure 3.4(b). The appropriate choice between direct or hierarchical structure, or a hybrid of the two, is an important research question in wireless process control.

Network architecture

The network architecture is equally important in the performance of closed-loop system and its integration with the legacy systems. Figure 3.5 provides an overview of different formats of network architecture, and the vicinity where the controller resides. In a conventional NCS, the control is often implemented in a dedicated controller. However, in the case of WNCS it may not be the only option. Based on control systems evolution shown in Figure 1.10 and the comparison of industrial wireless networks shown in Figure 2.7, the following options exist.

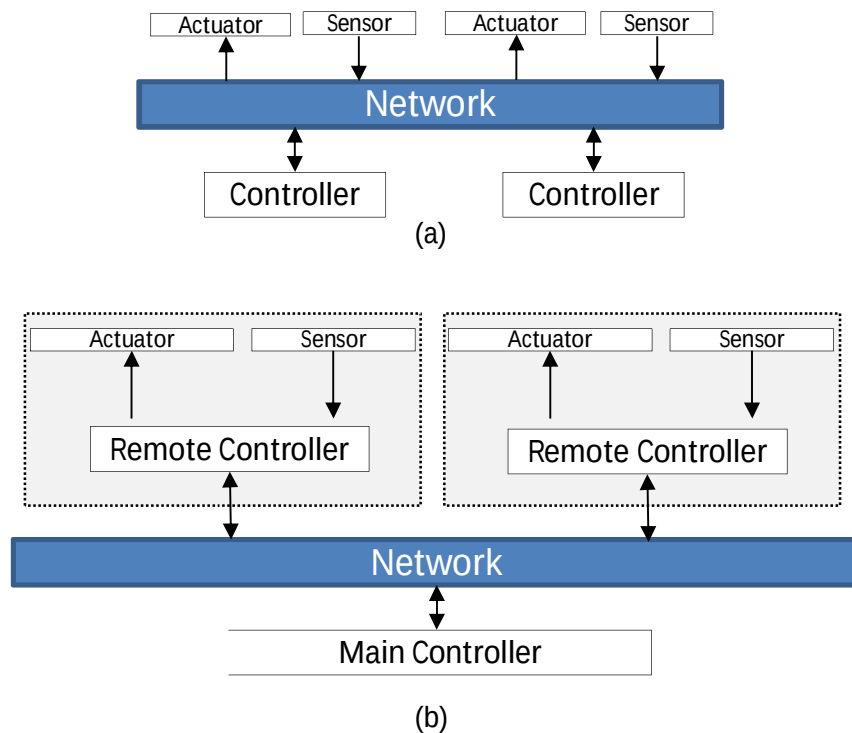


Figure 3.4. Depiction of (a) Direct Structure and (b) Hierarchical Structure after Wang and Liu (2010).

- Control algorithm can reside inside the gateway. The rest of the network architecture can follow the direct structure and is depicted in Figure 3.5 (a).
- Figure 3.5 (b) depicts the conventional model of NCS. In this method, wireless sensing and actuation is conducted via an intermediate cache memory in the gateway where the Input-Output (IO) information is updated periodically. The cache memory is updated in the gateway.
- This option involves running the control algorithm in the field device like in an actuator (Figure 3.5(c)) or at the sensor (Figure 3.5(d)). This option is also available in some wired based networks, such as Foundation Fieldbus.

These options are not an exhaustive list of available scenarios, none the less, vital options are being considered for having wireless sensors and actuators in loop. The latter mentioned option involving the field-control is considered to be a good option for wireless control. This architecture is also referred to as Automated WSAN in literature, which can further be used for event-triggered control.

To summarize, the use of wireless in process automation and especially for control is an active area of research. The use of wireless for non-critical monitoring is already underway. However, the use of wireless in relation to closed-loop control is challenging and requires revising the current approaches and the practices as well. These architectures will be referred to later in Chapter 5 during the study of hardware-in-control loop setup. For now, it is worth to highlight that control in the field looks promising from WNCS perspective. However, in the past it did not have much success in process automation, and some of those reasons, which are linked to current practices, will be explained in the next section.

3.2.3. Concerns and Challenges

This section discusses concerns and challenges for implementation of wireless process control. *Concerns* are challenges of the past which have been addressed, while *challenges* remain open and still to be resolved by further research. Many technical challenges remain with all three of the physical hardware, the wireless communication, and the performance of the wireless system in which wireless process control will have

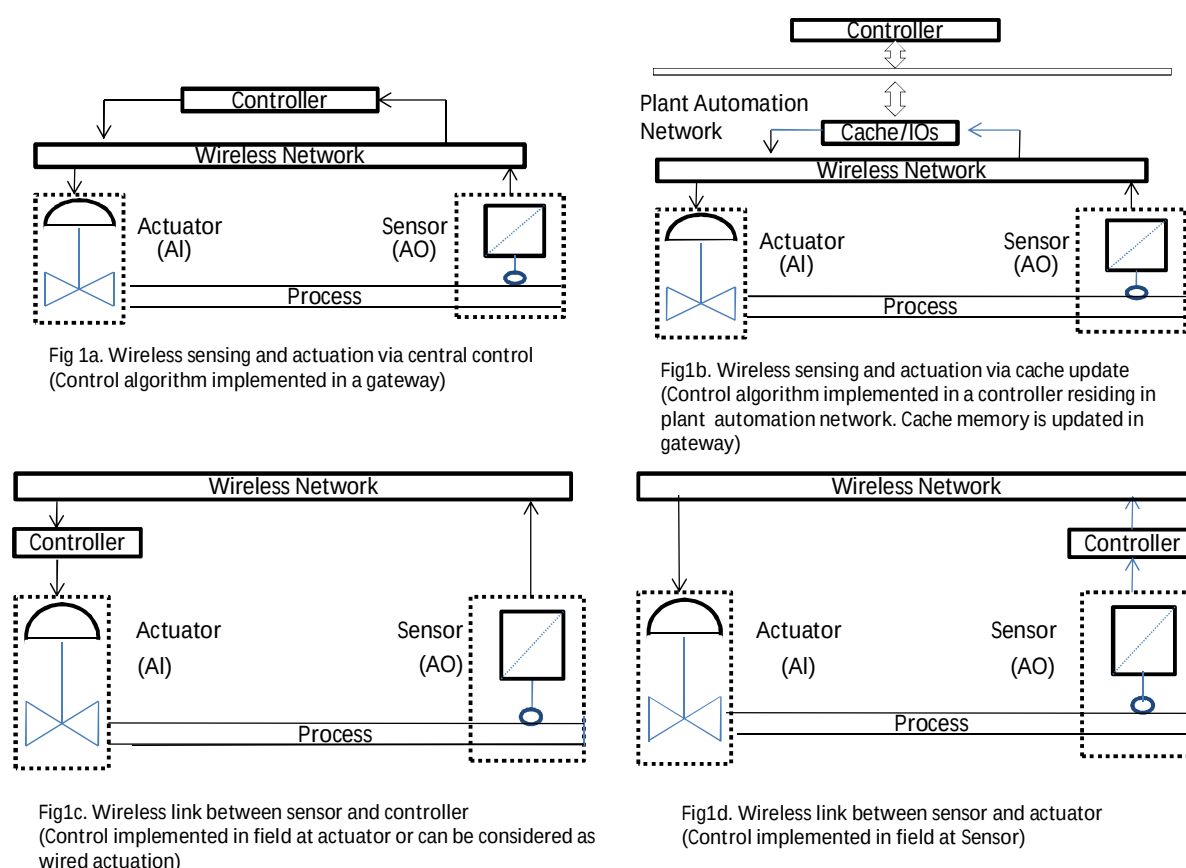


Figure 3.5. Wireless Network Control System Architecture after Johansson (2005) and HCF (2009).

to be implemented. Section 1.3.2 provides the necessary background which discusses research directions in wireless closed loop control for process systems. There it was highlighted that reliability, availability, data integrity, security and determinism are critical from process automation perspectives. Here, an overall systems level approach is taken to identify the challenges for safe operation of process control over wireless network and its integration to control systems. A researcher working on process control using wireless communications will encounter the challenges and constraints described here.

▪ RADIO-WAVES IN HAZARDOUS ENVIRONMENTS:

Electromagnetic waves can cause currents to flow in metallic structures and if that flow is interrupted momentarily, sparks can occur resulting in ignitions in flammable atmosphere (BS6656, 2002). Wireless technology for process automation involves power levels which are well below the threshold of ignition of all gas groups [Ikram and Thornhill (2010), Schultz (2007)]. There are no new

challenges here because field devices are available for all ATEX levels including Zone 0, highest risk of explosion (WiMon, 2010), while access points and gateways are available for Zone 2.

- ENERGY USAGE:

Minimization of energy usage requires energy-efficient network operation. The power requirement increases with high throughputs, high reliability, low packet latency, and when devices operate as routers e.g. in a mesh network. A research priority in closed loop control over a wireless network will be for energy-efficient control algorithms that minimise communications across the wireless control network while maintaining closed loop control performance.

Another mode of powering field devices is through energy scavenging where devices harvest energy from external sources. The survey by Mitcheson *et. al*/ (2008) gives an overview of advancements in motion-driven energy harvesters, comparison of effectiveness of work published on motion harvesters, and their suitable applications.

- BIT ERROR RATE:

Radio transmission suffers from bit error rates which are higher by orders of magnitude compared to cables, where bit error rates range from 10^{-7} to 10^{-9} (Camacho et al., 2003). Wireless communications, therefore, use error correction techniques and time-shared communication to reduce the bit error rate. In the case of missed inputs and outputs, the host applications are designed to be robust to these network effects. These concerns have been addressed in the wireless process automation standards.

- FREQUENCY SPECTRUM JAMMING:

The use of one static channel can be subject to jamming and interference leading to communication degradation as highlighted in Table 2.5. This concern has been addressed in the industrial protocols for wireless process automation using the spread spectrum techniques together with frequency or time-slot hopping. Table 2.6 summarized the detailed mechanisms adopted by each protocol.

- INTERFERENCE AND COEXISTENCE:

The use of a license-free radio band for communication is susceptible to interference from other nearby sources operating in the same band. Constant interference may persist, for instance, if a domestic or office Wi-Fi router is installed in the vicinity of wireless field nodes.

In addition to spread spectrum, the concept of channel blacklisting is used for wireless communications in process automation. If a permanent source of interference is known then that channel is not utilised in frequency hopping. However, over time, multiple channels could be unnecessarily blocked leaving fewer channels available for frequency hopping. Also, in a wireless mesh network only a few distributed nodes in one part of the plant may require channel blacklisting, not the entire network. Therefore, there is scope for research and commercial development in automated channel blacklisting.

- TRADE-OFF BETWEEN RELIABILITY AND TIMELINESS:

Process values being transmitted to or from field devices must be received with a high probability of success. Lost sensor readings or controller commands for actuators would have an impact on the performance of a control loop. Packets received after the deadline will by definition improve reliability but they may not be useful for control purposes (Park, 2011). The FeedNetBack project is an effort towards co-design framework to integrate communication, control, computation and energy management in NCSs with the aim to develop efficient, robust, adaptable and affordable NCS (FeedNetBack, 2010). A good understanding of the trade-off between reliability and timeliness in wireless communication protocols is essential for wireless process control.

- LATENCY, JITTER AND REAL-TIME COMMUNICATION:

Latency depends on network topology, routing, scheduling mechanism, network traffic and retransmission schemes. In general, a mesh network will experience random variations in latency, which is referred to as jitter, and latency may increase as the network increases in scale.

Real-time communications are characterized by consistency in their performance regarding latency and jitter. They are classified as either hard real-time or soft real-

time. The sampling interval of the application dictates the deadline, and delays have to be kept to a fraction of these values.

Hard real-time systems are found in factory automation. The communication is fully deterministic; hence, variability in the latency must be bounded. Process automation applications, by contrast, use soft real-time communication where lateness of some information packets is accepted and probabilistic guarantees are sufficient (Lemmon and Hu, 2011). Closed-loop control applications require bounds on latency and jitter, however. In short, networks which have delays that are random and potentially longer than the sampling interval may not be suitable for wireless process control.

Research into wireless process control has to take into account of the soft real-time nature of a wireless network. The latency control mechanism needs to be designed in order to transit from open-loop monitoring applications to closed-loop control. To ensure latency, limits have to be defined which link the network topology, number of hops, devices types, sinks, application mode (synchronization or asynchronized control execution), and sampling time. Some schemes have emerged to achieve real-time communications using confined hops and topology-aware mesh networks [Li *et al.* (2009), Teng and Kim (2010)].

Current network size is often considered to be limited only by the size of the device address, but this is not true when latency must be bounded. A more realistic detailed mathematical formulation is required to encapsulate the aforementioned parameters, and to put a theoretical limit on such networks.

- DATA AND NETWORK SECURITY:

The use of wireless instead of wired communication makes security more difficult. Concerns about security measures were addressed early in the development of wireless communications systems for process automation by means of encryption, verification and authentication.

The analysis and comparison by Raza *et al.* (2009) illustrates that security measures are well developed. Therefore, security and encryption for wireless process automation networks does not seem to be a high priority for new research.

- ADAPTATION TO NETWORK BEHAVIOR:

An example of adaptive communication is found in Wi-Fi, where network data rate changes automatically in responses to the quality of the wireless signal. Adaptive communication is an active research area which includes technologies like adaptive radio, cognitive radio, and intelligent radio. However, most of these technologies are enabled by software defined radio, typically running in a desktop PC. There is a paper from Kar *et al.* (2006) defining the opportunities for using UWB in process industry. In order to benefit from such adaptive techniques, it is important to have an analytical model describing the relationship between protocol parameters and the performance indicators. To summarise, network resources which change over time have to be adapted by the network devices to cater for varying network size, topology and application demand.

- SYSTEM INTEGRATION:

Seamless integration into Levels 2 to 4 of the ISA-95 function hierarchy shown in Figure 2.3 is a requirement for wireless process automation applications. The interface at the wireless gateway between Layer 0 and Layer 1 must use real-time protocols to link the real-time sensor network to the plant automation network. Levels 2 to 4 typically use wired Ethernet based connections which are non-deterministic, and can add significant delays if used in a control loop. This gives a fundamental limitation on the use of feedback control involving direct linking of the business planning and logistics layer, or the manufacturing operations management layer to the production process, whether or not wireless communications are in use for field devices. Integration effort is required from industry and from network vendors.

- SCALABILITY:

Scalability is the ability of a network to accommodate growth. One of the key requirements from a wireless communications network is to accommodate size variations due to obstacles, mobile nodes and addition of new nodes. Scalability of a WSN depends on various factors like the number of access points and routing of information via other nodes in the network.

Summary

The bullet points below summarize the research directions that have been identified in this section related to the design and implementation of wireless process automation networks.

Those which relate to the use of a wireless network to support closed loop control areas are as follows.

- Energy-efficient control algorithms to minimize communications across the network
- Design of a latency control mechanism
- Mathematical formulation of the theoretical limit on the size of a network to meet a latency specification
- Closed-loop control algorithms when delays are uncertain and unbounded

3.2.4. Related Work in Context

Periodic versus event-triggered control

In a conventional wired communication network found in process automation, the control commands are executed periodically. The sensors provide data to the controllers in a periodic manner. The controllers then compute the controller output based on the information received from the sensors. The general rule for executing control command is that it should be executed 4-10 times faster than the process response time (HCF, 2009). Therefore, as the controller output works on the process variable value, the values should also be updated often to meet the application demand. This model of periodic execution can be adapted in an alternative wireless communication network, but may not be a feasible option because of limited bandwidth and onboard power. An alternative solution to periodic sampling and control is event-triggered strategy. Event-based control is a good option for better resource utilization. Amongst the many listed benefits of event-driven control as opposed to periodic control include better use of Central Processing Unit (CPU) time at controller by omitting the use of CPU during time of non-significant activity and also better use of available bandwidth. Similar approaches earlier used for effective utilization of computational resources are now being examined for wireless control [Johansson (2009),

FeedNetBack (2010)]. The use of event-triggered control is not new in some industry sectors, for instance it is used in the power industry. However, it has not been widely used in the process industries. The work from the researchers in this arena is focusing on achieving similar levels of performance as in the case of periodic control.

However, the fundamental challenges involve the event-definition. To define an event is often challenging, for instance: a level crossing or relative change are often used [HCF (2009), Rabi and Johansson (2008)]. The event-triggered control if used for wireless control can help avoid the unnecessary periodic communication. It will result in reduction in power consumption and network traffic. A project concerning event-triggered control over wireless sensor and actuator network is cited in SGER (2011).

Enhanced PID

The most widely used control algorithm in industry is a PID control (Song *et al.*, 2006). A step towards getting the best performance from a PID algorithm if used in conjunction with an unreliable communication can be found in Song *et al.* (2006). Their proposed algorithm, referred to as an Enhanced PID, compensates for communication imperfections. The algorithm takes into consideration the times when the packets are lost and the corresponding controller output computed. The undesired features such as anti-windup and derivative kicks are addressed in the formulation of this algorithm. It modifies the output of the conventional PID controller when packets are missed. Therefore, it helps to achieve a better performance.

Data rate scaling techniques for control

Amongst the different techniques used in IEEE 802.11 networks for avoiding network congestion involves the use of data rate scaling. Transmitting data at a higher rate is a possibility using technologies like IEEE802.11 a/b/g which support data rate scaling to avoid queues. Colandairaj *et al.* (2005) have presented a new co-design method for wireless feedback control in which, when the channel performance deteriorates, the data rate decreases. The proposed approach of data rate scaling and sample rate adaptation compensates the reduction in bandwidth through reduction in traffic. This is a good method for ensuring performance but is only a viable option in technologies supporting data rate scaling.

Smart publishing

This feature which is part of the WirelessHART standard is designed to increase the battery lifetime of field nodes and to reduce the unnecessary communications. This feature controls the transmissions of process variable values. In a WirelessHART network, devices can transmit process variable information based on time, relative-change or crossing of user-defined signal threshold. The latter mentioned features of reporting on exception are what are encapsulated in smart publishing. However, the handling of multiple exceptions simultaneously, data prioritization, and controller execution rate adaption are important for reliable operations. These features which are linked to systems and network are to be well considered in the design of NCS, and especially in scheduling. Moreover, Jafari and Lang (2011) proposes an approach to find the optimal sample rate for each network structure and have shown that when the network size becomes larger the automated WSN architecture is more favourable to compensate for increase in communication.

Others

The discussion presented in this section has been limited to what is within the scope of this thesis. Based on the discussion presented in Chapter 2, it was identified that TDMA based MAC protocols have been favoured by research community for process automation. The standardised industrial wireless networks are based on this MAC. Even the earlier work presented by Willig (2003) investigated the polling based MAC protocols for improving performance in a Wireless PROFIBUS because of its deterministic behaviour. However, some researchers, such as Park (2011), have presented a protocol referred to as BREATH for real-time systems and is based on CSMA. Moreover, SPEED on the other hand is an example of real-time communication protocol which combines feedback control and non-deterministic QoS aware geographic packet forwarding (He *et al.*, 2003). This is aimed at soft-real time applications and improves the end-to-end delay while maintaining the desired delivery speed.

3.2.5. Summary

This section has presented an overview of existing strategies for designing a NCS and has highlighted that the co-design approach appears to be the most prominent, as it can address the inherent issues and challenges linked to the wireless networks. WNCS is a

multidisciplinary research area and involves engineering and information technology disciplines. The success of NCS lies at the intersection of control and communication theories, and a reliable and energy-efficient implementation of WNCS.

Furthermore, the control network architecture was introduced alongside the current structure in use in the process industry. In addition to the existing challenges linked to WNCS, the current practices of process industry further put a strain to the design of WNCS. Finally, the section concluded by highlighting some new innovative research underway within this field towards deriving and applying a co-design framework for achieving a practical WNCS.

3.3. TPC in IEEE 802.15.4 Networks

The resources in a wireless network which include the foremost important, radio spectrum, is limited and is subjected to heavy regulations which mandate the need for efficient spectrum management. These inherent issues in wireless networks fall under the category of Radio Resource Management (RRM). It is an active area of research and demands advance schemes [Gungor and Hancke, (2009), Willing, (2008)].

Efficient utilization of radio resources is up to the RRM strategy, one such radio resource unit is the transmission power level (Willing, 2008). Most often, the MAC protocols use the TPC in order to manipulate the transmission power at the transmitter to achieve reliable, energy-efficient and balanced network operations. This involves the adjustment of transmission power level at the transmitting node to a minimum level which can ensure successful communication without affecting the performance (Sheth and Han, 2003). Over the last two decades, TPC in cellular networks has been extensively studied and many review papers have been published which includes the recent publication by Douros and Polyzos (2011). Cellular networks have seen an increase in demand for data transmissions as opposed to traditional voice transmissions. It is evident from the trend observed in evolution in cellular networks technology from 1G network to LTE. Consequently, power control algorithms have evolved over time to cater to the shift in paradigm. TPC is an integral part of the serving generations of cellular networks like 3G networks. It is considered by many such as Chiang *et al.* (2008), Douros and Polyzos (2011) and Qiang *et al.* (2002) that it will

remain a key configurable component in future generations of mobile networks to ensure quality of service.

Despite the availability of literature regarding TPC in cellular networks, they cannot be directly applied to other networks, such as WSNs due to reasons which will be explained later in this section. This section will provide an overview of the existing strategies for TPC, their classification, requirements for industrial wireless networks, and a summary of related research which can be of practical use to industrial WSNs.

3.3.1. Overview

TPC is also referred to as *power diversity*. It can be used to improve the performance of a wireless network in many aspects. Examples are as follows:

- TPC can help mitigate the effect of fading, such as rain fading. When the data-link experiences degradation due to fading and the Bit Error Rate (BER) falls below the required threshold, the transmission power is increased gradually to achieve the required BER. However, it is limited by the maximum allowed transmission power level available at the transmitter (Shrivastava *et al.*, 2007). It is a common method adopted in fixed microwave links (Callaghan *et al.*, 2006).
- TPC can be used to solve the near-far problem. It arises when the transmitters broadcast at a constant power level. For example, if two transmitters broadcast at same power level and communicate with the same receiving node then the transmitter which is at a far distance from the receiver compared to that which is near the receiver will have low probability of getting its message across to the receiver. It is because the received signal from the transmitter which is at a far distance will have a weaker signal at reception compared to the one transmitted by a transmitter located near the receiver (Chiang *et al.*, 2008). Therefore, TPC can help minimize interference and increases probability of successful data transmission.
- TPC can reduce energy consumption of a mobile terminal and consequently prolong its battery life. It is of significant importance to networks such as WSNs, where the nodes have limited on-board battery. Furthermore, as the battery technology is improving it is still slower than advancement seen in

communications technology. Therefore, it is a constraint in development of wireless applications. A brief review into advancements in battery technology is presented in Chapter 7.

- TPC helps to minimize interference resulting in increased network capacity. It is because TPC reduces the number of packets lost due to interference and minimizes retransmissions. As a result, spatial reuse increases leading to enhanced network utilization from both network capacity and data throughput perspectives (Luo *et al.*, 2011). Power control in ad-hoc networks from theoretical and architecture point of view has been presented by Narayanaswamy *et al.* (2002) They have presented a solution which aims to provide high capacity, extend battery life and reduce contention.
- TPC can be combined with other interference mitigation mechanisms, such as directional antennas to improve network performance.
- TPC can further be used with data rate adaption schemes in order to enhance network throughput (Gjendemsjø *et al.*, 2006). Therefore, increasing or decreasing the available bandwidth accordingly. In addition, it can also be used to differentiate between critical and non-critical data generated in a wireless network, and to provide adequate QoS to each respectively.

Applications

TPC is used in Wideband Code Division Multiple Access (W-CDMA), a channel access technique used in the third generation of cellular technology, UMTS (Callaghan *et al.*, 2006). Various TPC algorithms are also suggested for WSNs (Gjendemsjø *et al.*, 2006). The use of TPC is also compulsory for Bluetooth class 1 devices but optional for others (Holma and Toskala, 2010). The use of TPC is also an option for Wi-Fi networks but its use has been restrictive due to reasons explained in Shrivastava *et al.*, (2007). Within the context of industrial wireless standards, support for TPC is included as part of the framework but the details of its implementation are not specified in the standards like in IEC (2010), ISA (2011), IEC (2009). Although TPC is widely used in different communication technologies, its use in short-range, low-power industrial strength wireless networks is new and is subjected to unique challenges.

3.3.2. TPC Strategies, Applicability and Wider Considerations

TPC has been proposed for wireless networks which include cellular, fixed point-to-point microwave links, Mobile Ad hoc NETWORKS (MANETs), VANETS, WLAN and WPAN networks. For some networks it has been in use for many years, such as cellular networks. In contrast, for non-traditional networks such as MANETs, WSNs and cognitive radio networks, the traditional strategy is restrictive and requires new approach for TPC. For example, a Wi-Fi based WLAN which is widely deployed in commerce and industry supports both infrastructure mode (similar to cellular approach) and ad-hoc mode (which is not cellular). Therefore, even within same network, different TPC strategy may be required which is optimal. Hence, the TPC strategies and methods which have predominantly been designed for cellular networks cannot simply be replicated for industrial WSNs. This section will briefly review some of these strategies and highlight their applicability.

Ultimate TPC scheme

The ultimate TPC scheme should satisfy the following criteria: simplicity, flexibility, scalability, ensures availability (no outage), quick adaption to link quality variations (implies dynamic adjustments) and overall balanced network operations from capacity, throughput and QoS perspectives (Douros and Polyzos, 2011).

Typical process

A typical process which a TPC algorithm needs to model is shown in Figure 1.3. The transmitter sends a signal at a particular power level. The receiver measures the incoming signal strength and after successful decoding it sends back an acknowledgment to the transmitter. If the data packet was not successfully decoded then a negative acknowledgment is sent to the transmitter. As a result, the data packet is retransmitted. This is an example of communication between a pair of nodes. How a transmitter adjusts its transmission power depends on TPC strategy.

The link quality changes over time and varies from link to link. Hence, a requirement which is common amongst various TPC schemes both in traditional and non-traditional networks is the need to dynamically adjust the transmission power. It is so, in order to ensure good link quality at all times with least amount of energy expenditure at the distributed node. A *good link quality* is referred to as a direct link between pair of

communicating nodes which supports successful data delivery. To maintain a good link quality the following factors play a vital role: distance between the pair of communicating nodes, the physical barriers between link, climatic conditions and receiver's sensitivity and its measurement uncertainty of link quality metric (e.g. RSSI). Therefore, to transit from a particular link quality to a good link quality the transmission power has to be adjusted accordingly. Reijers *et al.* (2004) presents a study regarding the effect of obstacles and environmental changes on link quality. In addition, Zhou *et al.* (2004) proposed a propagation model that closely resembles the experimentally obtained results.

TPC strategies

In the simplest of form, a transmitter can adopt an iterative approach where it adjusts its output power based on the signal strength of the acknowledgment packet. Here it is assumed that the same link is used in transmission and reception. The transmitter then adjusts its output iteratively such that the received power at the receiver is above a minimum required threshold (which is often the sensitivity). Furthermore, the transmitter can store this information in a table which can be consulted every time before the next transmission. As can be expected this method is slow and assumes reciprocal channels where the link gain coincides. This was the example of strength-based TPC. On the other hand, the received power at the receiver can be used in combination with other parameters, such as noise at the receiver to yield SNR. Moreover a statistical measurement like Packet Reception Rate (PRR) can be used in combination with Received Signal Strength Indicator (RSSI) to identify required threshold at the receiver. For example, in the case of research published by Lin *et al.*, (2007), an average RSSI of -80 dBm yielded a PRR of 99%. It signifies that this calculated RSSI can be used as the required threshold instead of receiver sensitivity. Therefore, multiple link quality assessment measures can be employed in TPC formulation.

Within the research community there are different opinions as to which parameter should be used as a metric for link quality. In cellular networks this split is often based on network services and in the case of WSNs it is based on the empirical studies on the performance of different metrics supported by commercially available hardware nodes [Douros and Polyzos (2011), Srinivasan and Philip Levis (2007)]. The parameters which

are supported by the IEEE 802.15.4 compliant wireless transceivers are RSSI and LQI and will be presented in detail in Chapter 6. It is important to note that these metrics cannot be used interchangeably.

The aforementioned simple form of TPC can be enhanced by employing a feedback loop. The transmitter knows its transmission power, and can communicate this information to the receiver. The receiver can use this information and make estimate of link gains and losses which can be linked to SINR and will assist to compute the required minimum transmission power which can ensure good link quality. This information can be communicated to the transmitter which adjusts its power accordingly. In this case, the receiver conducts the main TPC computation. On the other hand, corresponding to each received packet, the receiver can incorporate its strength value in the acknowledgment packet. The strength of the transmitted packet at the receiver and the strength of the received acknowledgement packet can be used to identify the validating of reciprocity and link gains and losses. The transmitter can then compute required transmission power based on the above mentioned information. Within this approach, the main computation is conducted at the transmitter. There are other ways too, as discussed in Chapter 6. Within the adjustment of transmission power phenomenon such as fading needs to be considered and its parameter needs to be defined. For SINR based TPC strategies such phenomena defines the required threshold. Goyal *et al.* (2010) shows that the required threshold is different in the case of AWGN channel from that of Rayleigh fading channel.

The above mentioned examples were for ad-hoc networks, whereas in the case of infrastructure based networks the centralized controller can make use of the network topology and individual links information to compute the minimum required output power which each node can achieve and will ensure network-wide QoS. In this approach, a network-wide QoS is considered whereas in the earlier case each node competed to get its best performance. The work by Zander *et al.* (1992) examines this approach which delivers an overall QoS of network as opposed to that of an individual link basis. They show that there is an optimal solution which leads to the convergence of all links to the same SIR.

Examples of TPC

An approach called the Hybrid (Correia *et al.*, 2007), is an example of TPC for MAC protocols in WSNs which uses closed loop control and iterates over available transmission power levels in order to achieve and maintain the target link quality. The same authors have also presented another TPC approach referred to as AEWMA which utilizes the reception power, noise power and transmission power in order to determine the ideal transmission power. These strategies were shown to be able to deliver 98% of delivery rate. LMA (Kubisch *et al.*, 2003) is proposed for WSNs where the transmitter counts the number of reachable neighbors at a particular power level, this value is adjusted if the received acknowledgments are less than what was expected. A modification to LMA is LMN where the receiver adds the number of its neighbor's number to the acknowledgment packet (Khemapech *et al.*, 2007). Using this enhanced information of its neighbor's neighbor information the transmitter makes adjustments. This way the connectivity of its neighbors becomes visible. This strategy does not require storing of neighbors table. It requires fewer resources and is based on number of reachable neighbors.

Considerations

The increase in transmission power of one node will increase its Signal to Interference plus Noise Ratio (SINR). However, a neighbour node may also increase its transmission power if its performance deteriorates. Consequently, the SINR will decrease due to increased interference. The effect of concurrent transmissions on SINR and on link reliability is studied by Son *et al.* (2006).

It is also argued whether the TPC should be implemented in MAC layer alone, which is responsible for link selection and configuration. Correia *et al.*, (2007) have investigated whether TPC is to be implemented in the MAC or routing layer. It is done so to take into consideration the energy-efficient routes which incorporate links in a multi-hop network. In the power-aware routing protocol referred to as RPAR presented in Chipara *et al.*, (2005) the dynamic power adjustment and routing decisions are made in order to minimize the packet loss rate. It is specifically defined for real-time applications and overall end-to-end delay is considered. It was emphasized that transmitting a packet at

a higher transmission power improved link quality and reduced the number of transmissions required to deliver a packet to destination.

Furthermore, some analytical models do not consider the effect of collisions. Collisions are often assumed to be negligible due to traffic pattern of data networks which is often modeled as short bursts in contention based networks. This assumption is often not the case in contention-free networks and is a critical issue which can lead to increase in transmission power.

Moreover, in some cases the TPC schemes are designed for platforms which support cross-layer design as is the case of cognitive radio networks. These networks can adapt their transmission rate by changing modulation schemes which changes their SINR reference.

TPC can further be used to blacklist channels with unreliable link quality. An example of such study is presented by Son et al., (2004). In their work a testbed was deployed and experimentally obtained results were used in the analysis. Two metrics were used in evaluation and several factors were studied which includes communication distance, hardware difference and location of nodes. It was highlighted that each link required different transmission power to achieve good link quality and that both link-based and packet-based blacklisting can be considered.

To summarize, a common procedure amongst the main TPC strategies is to discover their neighbors (predefined or reachable). A feedback loop can be used to convey the information regarding the packet reception to the transmitter. Whether to store or not to store the neighbor and connectivity solution is up to the TPC strategy. It is further linked to whether it is MAC based on routing based. Due to the limited onboard resources in a WSN, the TPC table if used should have small footprint (i.e. memory requirement) and its storing and maintain cost should be kept to minimum. Furthermore, the TPC strategy adopted should be practical and adaptive. In addition, the link quality metric should be selected based on network type, metric used, topology and its dynamic adjustment behavior. As the link quality changes over time it should be assessed frequently. However, this frequency has to be balanced with energy required to frequently monitor link quality which requires communication and computational resources. A common notion is that collectively adapting power, modulation and

channel assignment can enhance throughput, energy and fairness in network operations (Douros and Polyzos, 2011). However, these schemes are often not directly employable in WSNs due their predefined and fixed parameters (such as modulation).

3.3.3. Classification of Strategies for TPC

The methods and techniques adopted to calculate and adjust the transmission power at the transmitter which can deliver the required received power or any other link quality metric at the receiver can be used to differentiate amongst various TPC strategies. Furthermore, they can even be categorized based on the information the network is designed to support as different network types have varying QoS requirements. In general, the TPC strategies can be classified as follows.

Centralized versus decentralized TPC schemes

In the case of centralized schemes, a central controller is responsible for keeping track of link qualities of nodes in a network and generating control commands. The control commands are based on the information gathered from the distributed nodes (such as SINRs). Therefore, the central controller makes the transmission power adjustments. Due to its pivotal role, its design becomes complicated and at times not practical due to fast changing environments (Chiang *et al.*, 2008). In contrast, in the decentralized scheme a node adjusts its transmission power for all available links. This requires only coordination between pair of communicating nodes. This strategy is quick in adapting to network changes. However, it may not be the optimal solution for the entire network as can be in the case of centralized approach. It is because in the decentralized approach every link is considered independent to other nodes in a network. Satisfying SINR of one link may affect that of the other. Whereas, in the case of centralized schemes a unique solution can be found which leads to convergence of all links in a network (Douros and Polyzos, 2011). Within the context of WSNs the decentralized schemes are considered more feasible, Yook *et al.* (2002).

Metric employed in TPC formulation

The transmission power is adjusted at the transmitter based on a metric which is employed at the receiver to estimate the link quality. These metrics vary between network types. They can be based on measures such as: signal strength at the receiver,

SIR (in noiseless channel), SINR (in case of noisy channel), SNR (in the absence of noise), Bite Error Rate (BER), Link Quality Indicator (LQI) or Packet Reception Rare (PRR).

Therefore, these schemes are signal-strength based, signal-to-interference and noise based or statistical measure based techniques. SIR based schemes are used in cellular systems due to their superior performance in terms of network capacity and overall QoS (Douros and Polyzos, 2011). SIR based schemes can further be subdivided based on fixed or variable SIR. Furthermore, BER based schemes are linked to the SIR and the type of modulation. Collectively power control and modulation adoption improves QoS (Gjendemsjø *et al.*, 2006). The selection of the metric depends on the PHY involved, application requirement and the overall TPC scheme.

Information-driven network type

A wireless network may be designed to support voice, data or a hybrid of both. Different TPC methodologies are needed to cater these application demands as they have different QoS requirements. The difference between voice and data network from transmission control point of view can be identified as the objective of running TPC in each case. According to Douros and Polyzos (2011), in the case of voice networks the objective is to maximize the number of links in a network while satisfying the SINR requirement. In contrast, in the case of data networks the objective is to minimise the transmission errors for each link, therefore BER is preferred. In recent years, due to the demand for Voice over IP (VoIP) service, the hybrid nature of traditional data networks like Wi-Fi is prevailing. Therefore, the TPC mechanism has to be designed taking into consideration the type of network on which the TPC strategy is to be implemented. Hence, it is a way to categorize the TPC strategy.

Loop specific TPC

In this way of classification, a TPC approach can be defined as:

- OPEN-LOOP POWER CONTROL:

In this method, a wireless node measures its received signal level and adjusts its transmission power accordingly. Reciprocity is considered in the case of uplink and downlink. This is a relatively fast approach for TPC. However, its

performance is limited because of limited correlation between the uplink and downlink between transmitter and receiver. Open loop control is adequate when round-trip time is significant as is in the case of Satellite communications (Monk *et al.*, 2006).

- CLOSED-LOOP POWER CONTROL:

In this paradigm, the pair of communicating nodes coordinates amongst themselves in order to make adjustment to the transmission power. The receiver sends information to the transmitter regarding the adjustments based on the channel gains and losses. This process introduces delays and has to be kept to minimum in order to avoid outages. The loop execution rate depends on application. In case of UMTS, the inner loop power control frequency is 1500 Hz. The loop execution frequency depends on the environment which is to ensure connectivity and required QoS. A combination of open loop and closed loop control is used in cellular systems.

Event-triggered versus periodic TPC control

The power control loop can be executed on a periodic basis in order to ensure that the selected transmitted power is adequate to ensure required QoS at the receiver. This approach adapts to any short and long term variations in the link but introduces overheads. In the case of event-triggered control the receiver initiates the process of transmission power adjustment when an event is signalled. This approach is sensitive to the definition of event used in this approach. TPC used in Bluetooth can be classified as event-triggered TPC mechanism.

Packet versus circuit switch modes

In packet switched mode of operation, which is linked to network type, the data is moved as packets based on destination address. In contrast, a dedicated point-to-point connection is used in the case of circuit switched mode. The selection of mode of operation is linked to sensitivity of information which needs to be routed. Circuit switched networks are used for delay-sensitive applications. Packet switched mode is favourable when the application is not sensitive to network induced delays. The selection of TPC strategy needs to consider this as it is linked to intervals between communications, and the traffic behaviour within each network type. The network

traffic can be busy and can lead to delays or data losses which increase the probability for network outage. Therefore, operation modes are to be considered during TPC formulation and the TPC algorithms can be categorised accordingly.

Models for link estimation in TPC

To model the relationship between the transmission power and the received power, analytical, statistical or empirical based models are used. Further, these channel models which encompass path gains and losses can be linked to the SINR. Therefore, the model which is employed to relate the transmission power and required link quality metric at the receiver can be used as a method to classify TPC algorithms.

Topology specific TPC algorithm

If the topology of a network is known then the TPC algorithms which are specifically designed for such networks can be used. Star-based networks such as cellular networks or mesh-based WSNs can use TPC algorithms tailored to individual topology. The use of link-state topology with neighbour information is used in TPC proposed in Ramanathan *et al.* (2000).

There are other ways of also categorizing the TPC schemes such as: opportunistic power control, game theoretic approach, joint power control and beam forming techniques, schemes for handover and base-station assignment (Yates and Huang, 1995), spectral-temporal scheduling methodology, and those with and without cost functions (Saraydar, *et al.*, 2002).

In the technique presented in Jeong *et al.* (2005), the transmitter power is adjusted if the observed number of neighbors is less than the predefined value. It keeps the degree of adjustments to minimum and is designed for convergence.

The objective of presenting this classification was to identify the different key factors which are of concern when designing a TPC approach and to identify the subtle difference between them. They will be referred to later in this chapter and in Chapter 6.

3.3.4. Industrial Requirements, Challenges and Assumptions

The topology in an industrial wireless network may vary from simple star topology to multi-hop mesh network and is application dependent. WirelessHART supports frequency hopping on per packet basis, whereas, ISA100.11a supports both slow and fast hopping. Generally, TPC algorithm needs to operate over all the available channels, a maximum of 16 in 2.4 GHz band, and needs to adapt to the changing environment. Each node has information about its neighbors stored in communication tables. For each neighbor and for all available communication channels, a set of minimum power levels are required to be estimated to ensure SINR.

The assumptions regarding the industrial WSNs are as follows.

- There is no centralized controller (adjustments based on link basis).
- There is no common goal for the entire network (such as capacity).
- The SINR reference may be different for each pair (depends on application category).
- The deployed nodes are expected to be predominantly static or subjected to slow-fading (shadowing).
- The TPC needs to ensure link quality when subjected to co-channel interference.
- The output power of wireless transceiver will vary from vendor to vendor even if they still comply with the same IEEE 802.15.4 standard. These discrete values with upper and lower bounds are hardware specific and the proposed TPC algorithm should adapt to it.
- The TPC should not depend on specific routing protocols.
- And finally, measuring the link quality metric, processing it, and generating control signal (which is linked to network schedule) requires time and so cannot be assumed instantaneous in practice.

3.3.5. Related Work in Context

Based on the requirements mentioned above and the discussion presented earlier the relevant work can be classified into three categories: (i) performance limitations of IEEE 802.15.4 standard (ii) link quality assessment and (iii) TPC algorithms for WSNs.

Performance limitations of IEEE 802.15.4

Industrial wireless standards are based on IEEE 802.15.4 physical layer (PHY). Link budget is important for TPC and depends on sensitivity, and the work in Specification of the standard highlights the theoretical and practical limits of the IEEE 802.15.4 compliant receivers. These results were included in illustrating the opportunity for TPC in industrial wireless networks shown in Figure 1.3. The opportunity arose due to improved sensitivity. Further, (Lanzisera and Pister, 2007) highlights the effect of IEEE 802.11b networks on the Packet Error Rate (PER) of IEEE 802.15.4 networks. Even though the work was limited to IEEE 802.11b networks and the new installation includes IEEE 802.11g/n networks, the work offers insights to the effect of interference. The investigation by Douros and Polyzos (2011) has summarized the impact of Signal to Noise Ratio (SNR) on packet loss rate under Additive White Gaussian Noise (AWGN) and Rayleigh fading models; and further coexistence is studied through simulations in Khangura *et al.* (2010). Empirical evaluation of the IEEE 802.15.4 network is carried in Goyal *et al.* (2010), and has indicated the operational limitations.

In short, their work emphasizes on theoretical and practical limits of the underlying PHY used in industrial wireless standards and the gap in theory and in-situ practice.

Link quality assessment

Wireless link quality refers to the communication performance of a radio channel, and changes significantly with time and environment (Shuaib *et al.*, 2007). Received Signal Strength Indicator (RSSI) and Link Quality Indicator (LQI) can be used as a binary link quality metrics [Shuaib *et al.* (2007), Srinivasan *et al.* (2010)]. There are two different opinions as to which one is a better indicator (Srinivasan *et al.*, 2010). The work in (Shin *et al.*, 2007) highlights that the RSSI of a single packet is a good estimator of average RSSI over many packets. On the other hand, averaging LQI over a window of packets may better predict link quality than RSSI, however, it is slow to adapt. In (Lin *et al.*, 2009), the authors conducted experiments to evaluate the performance of wireless link quality based on the aforementioned metrics by varying distance and transmission power levels. The experiments presented in Alavi *et al.* (2009) further investigate the effect of interference on IEEE 802.15.4 transceivers by varying transmit power, distance, orientation, packet size, and relative distance from interfering nodes.

To summarize, in a fast changing environment and with limited resources, RSSI is a better indicator of link quality, and is also better defined in the standard compared to LQI (Srinivasan and Levis, 2006).

TPC algorithms

TPC algorithms rely on the availability of selection of transmission levels at the transmitter and this is often a limiting constraint. The selection criterion for useful power levels within indoor environments is highlighted by Lee *et al.* (2010) for IEEE 802.11 networks. In Myers *et al.*, (2007) an algorithm referred to as Adaptive Transmission Power Control (ATPC) is proposed where each communicating node builds a model for each of its neighbors, describing the relationship between transmission power and the link quality indicator. The linear approximation is assumed between transmission power and RSSI. The authors in IEEE (2006) have proposed two algorithms for TPC based on the analytical model of RSSI. An investigation of the performance of TPC algorithms in terms of Packet Error Rate (PER), power gain, and energy efficiency in AWGN and Rayleigh channels is presented in Shrivastava (2007). The TPC approach in Srinivasan (2010) is based on tracking RSSI where the effect of radio channel uncertainty and interference were considered as disturbance. Quantifiable improvements were shown in terms of outage probability and power consumption.

The SINR approximation by Ares *et al.*, (2007) assumes that interference is negligible, whereas, TPC used in Bluetooth only uses RSSI (Holma and Toskala. 2010). For an industrial strength TPC, the algorithm has to be robust and such assumptions can have an adverse impact on the performance of wireless instruments.

Much research within this context has considered soft application requirements, whereas, the industrial wireless have strict requirements, such as reliability and is addressed by using time slotted frequency hopping (Lin *et al.* 2006). The power control algorithms studied in WSNs and their performances are often reported for static channel deployments. In addition, these static channels are often out-of-band channels to a co-habited IEEE 802.11 network, in order to avoid degradation due to interference. In an industrial environment the fast changing link quality from one channel to the other and the effect of IEEE 802.11 on few channels compared to others for TPC has to

be comprehended. Therefore, a TPC algorithm is required which can adapt to changing radio environment, is quick to respond, works on pair-wise basis, and is practical.

3.3.6. Summary

The use of TPC is a common practice in some applications in order to increase reliability and efficiency of network operations. In recent years, this approach has gained attention from research community addressing the limited power constraint in WSNs in order to prolong network lifetime. This section has highlighted the difference between the traditional and non-traditional network types. Due to this split and also due to varying infrastructure it is, therefore, challenging to develop a generic TPC scheme. They have to tailor to individual needs. The limitations of wireless sensor nodes further impose restrictions in the selection of TPC. This section has further highlighted the challenges, constraints and the split which is within the research community regarding the TPC quality metric and the hardware support. Moreover, the decision as to incorporate TPC at the MAC layer only or at routing layer is also an area which is briefly discussed and is an active area of research.

Lastly, it was discussed that in some cases it is possible to reduce transmission power without degrading link quality. However, there is a possibility that an increase in transmission power may not lead to improved SINR if the interference from neighboring nodes also increases comparably.

CHAPTER 4

Time Synchronization in Distributed Wireless Systems

This chapter presents research into time synchronization of distributed wireless systems. A common way to achieve time synchronization is by the use of GPS. However GPS is expensive and can only be used when there is direct line of sight to the GPS satellite. An alternative approach is to use time synchronization based on the MSF time broadcast signal. This chapter provides a comparison between MSF and GPS based time synchronization. It describes development of circuits and algorithm to achieve MSF time synchronization and presents a detailed characterization of the system. It also presents empirical results obtained from field trials which demonstrate the suitability of the MSF time synchronization approach.

The developed time-synchronization system was able to work well in a variety of locations. Also, the results show that the proposed filtering mechanism which takes account of latency and jitter is able to improve the time synchronization accuracy by a factor of 80 (90th percentile) compared with the use of basic received MSF signal alone.

4.1. Overview of Proposed Solution

The requirements for time synchronization in distributed wireless systems were outlined in Chapter 1, and various techniques which can be adopted to fully or partially meet these requirements were reviewed in Chapter 3. The approach proposed in this thesis for time synchronization of wireless systems such as telemetry units (PLCs, RTUs, PACs, wireless sensor nodes) is by means of on-board radio-controlled clocks. The approach requires equipping the distributed wireless systems with radio clocks. This will result in isolating the time synchronization process from the in-band

communication in the wireless network. In addition to the global time synchronization this approach will result in the following key benefits:

- Elimination of the need to run an in-band time synchronization protocol.
- Reduction in network traffic due to elimination of the in-band time synchronization service.
- Topology-independent time synchronization method due to the segregation of the in-band networking protocol and its effect on time synchronization process.

Some additional observations about the system are:

- It will be fast-converging and scalable because the same MSF signal is used for time synchronization of the entire network.
- It will have high coverage and signal availability because the MSF signal is continuously broadcast.
- It will be independent of in-band communication and its wider coverage makes it a strong candidate for installations in remote locations with wide area systems or even on individual telemetry units.
- It is further noted that this out-of-band solution is suitable for time synchronizing networks and systems which even utilize different communication technologies.

On the other hand, dedicated hardware for time synchronization raises the following concerns:

- The cost and complexity associated with a radio clock.
- The operational requirement of a radio clock.
- The energy consumption of the proposed solution.
- The quality of the time code signal.
- The synchronization accuracy which can be achieved with this approach.

This chapter will further explore these issues in detail. The radio time broadcast has been around for many decades but the availability of economical radio clocks have surfaced over the last two decades. Their use has been primarily confined to non-critical and less strict time-dependent applications. Within the context of this thesis, the

application horizon needs to be extended and the quality of the MSF time signal along with the performance of the radio clock needs to be evaluated.

4.2. MSF Signal and Radio Controlled Clock Receiver

The dedicated RF signal for disseminating time and date code information in the UK is known as MSF signal, which is broadcast from Anthorn, Cumbria (54° 55' N, 3° 15' W) in England. This signal is available round the clock, all over the UK (NPL, 2007). The radiated power of the transmitter is 15 kW and is operated on a frequency of 60 kHz (NPL, 2010). It is this signal which will be detected and used by the proposed time synchronization system.

MSF signal

The MSF signal carries information related to difference between astronomical time and atomic time, current time and date (NPL, 2007). This information is coded into bits which are transmitted every second. A minute frame format of the MSF signal is shown in Figure 4.1. It highlights in detail the sequence in which the information is transmitted. It is a pictorial representation of a minute frame which comprises of 60 seconds. Difference between the astronomical time and atomic time is excluded in the pictorial representation which is transmitted during the first seventeen seconds.

Two bits are transmitted every second in a minute frame. Figure 4.2 further elaborates the bit stream in a minute frame which includes xxA and xxB bits, where xx represents the second. The information is coded in BCD format. For further details about the data structure, the bits which are permanently set and the leap year information refer to NPL (2007).

Due to the simplicity of the modulation used in radio time signals, the cost of the MSF receiver much lower than that of an alternative GPS solution.

Distinct and repetitive pattern in MSF code

In order to synchronize a node, a distinctive and repetitive pattern in time has to be identified from Figure 4.1. The key distinct markers in MSF signals are as follows (NPL 2007b):

- Start of Frame (SoF): The first second of every minute begins with a period of 500ms of carrier off. It is demonstrated in Figure 4.1.
- Second Marker: The start of every other second is marked with at least 100ms of carrier off and ends with at least 700ms of carrier on.
- Minute Identifier: Bits 53A to bit 58A are permanently set to '1', with prior and post bits set to '0'. This sequence 01111110 only appears once.

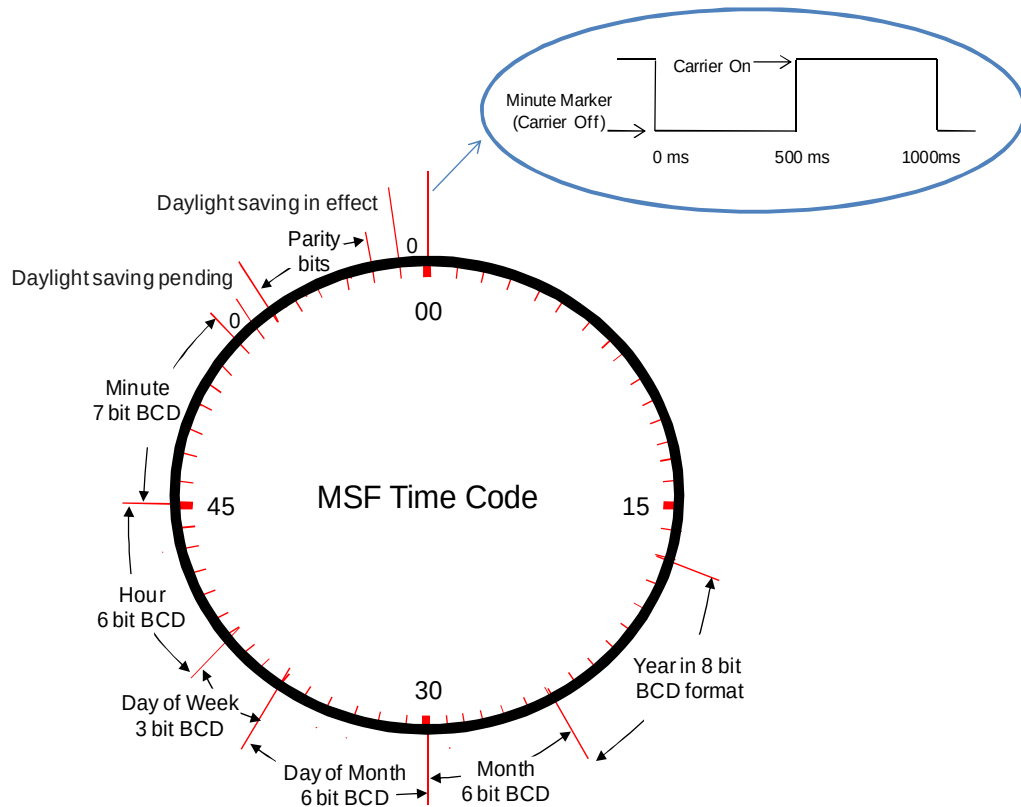


Figure 4.1. A minute time frame of MSF time and date code signal, 00-59 seconds. Information source NPL (2007b).

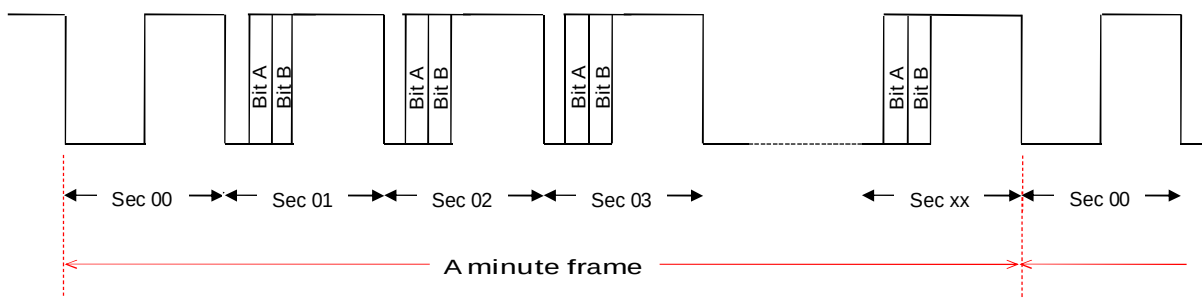


Figure 4.2. MSF signal bit stream.

MSF radio clock receiver

To evaluate the effectiveness of the proposed methodology, radio clocks were built to be used with the field nodes. The built version of the prototype MSF clocks are based on the EM2S receiver module from Galleon systems. The current drain of the module is 0.2 mA at 3V according to the datasheet given in Appendix C1. The schematic and the PCB diagrams of the designed time synchronization system will be submitted separately on a compact disk.

The flowchart of the MSF compliant radio clock and its extension circuits are shown in Figure 4.3. The design focused on receiving, decoding and evaluating the received MSF signal performance. Radio clock itself comprises of antenna, receiver and a decoder. The modules which are used are shown in the figure. The decoding was done inside the PIC18F13K50 microcontroller using decoding routines written during the PhD. PIC18F13K50 was also used to switch the EM2S receiver on and off.

Three extensions of this MSF radio clock were implemented.

- TIME AND DATE CODE VALIDATION:

In order to validate the received MSF time and date code information against another independent time and date code source, an extension was made to connect the radio clock to a computer. It was achieved by using the serial port. MAX232 was used to convert the TTL levels to the RS232 levels which enable communication with a standard computer. The data, therefore, terminates at the computer where it is evaluated and archived. The snapshot of this setup is shown in Figure 4.4 which shows the radio clock and laptop computer outdoors on a bench.

- SIGNAL QUALITY ASSESSMENT:

Another strand of the extension was to conduct the MSF signal quality assessment. This hardware extension was carried out to enable the time synchronization accuracy calculation. Radio clock was programmed to generate 1PPS and 1PPM aligned with UTC seconds in order to compare the on-time markers with those generated by GPS. Here, GPS is used as a reference signal which has accuracy better than a microsecond. Figure 4.5 represents the snapshot of this setup.

These two extensions helped to quantify the performance of the radio clocks.

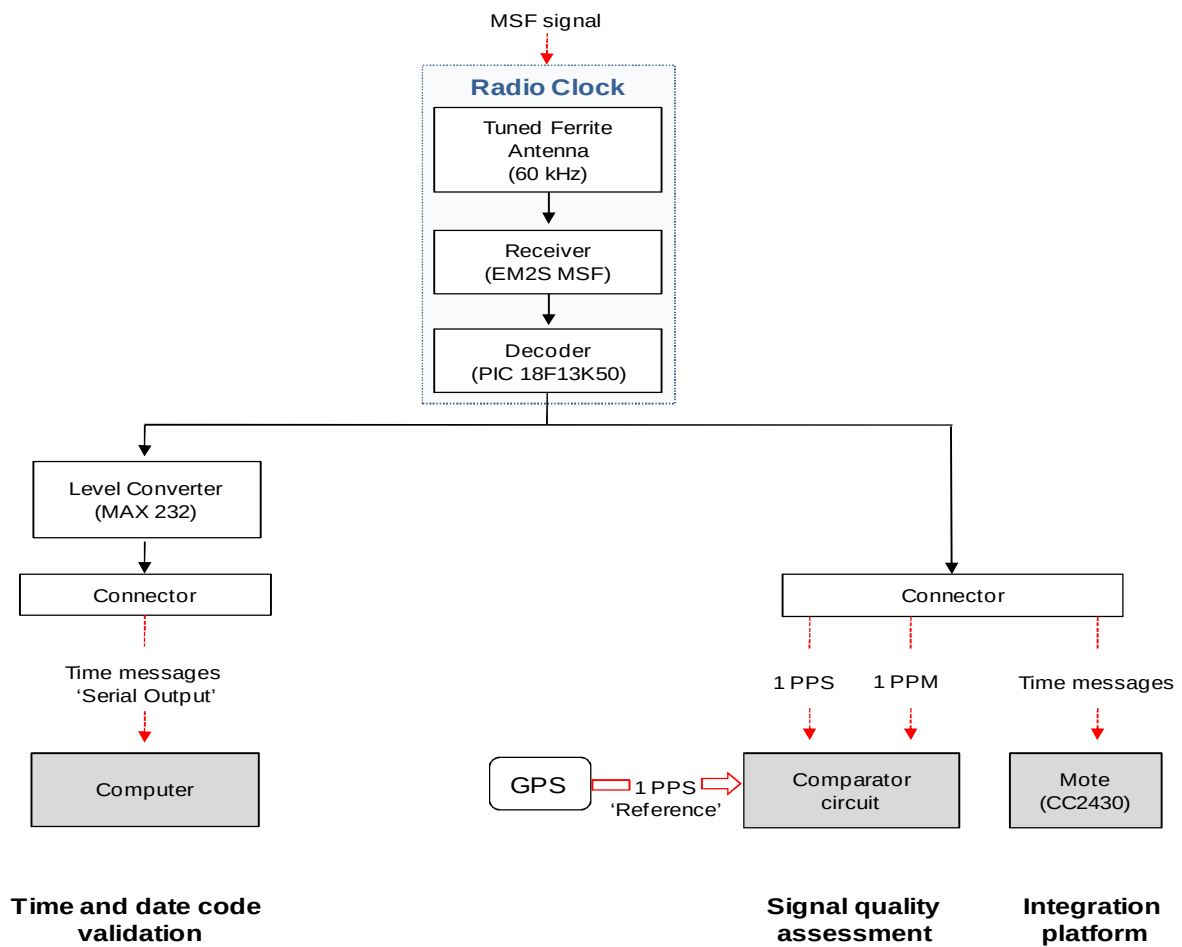


Figure 4.3. A flow chart of the MSF signal receiver and its extensions.

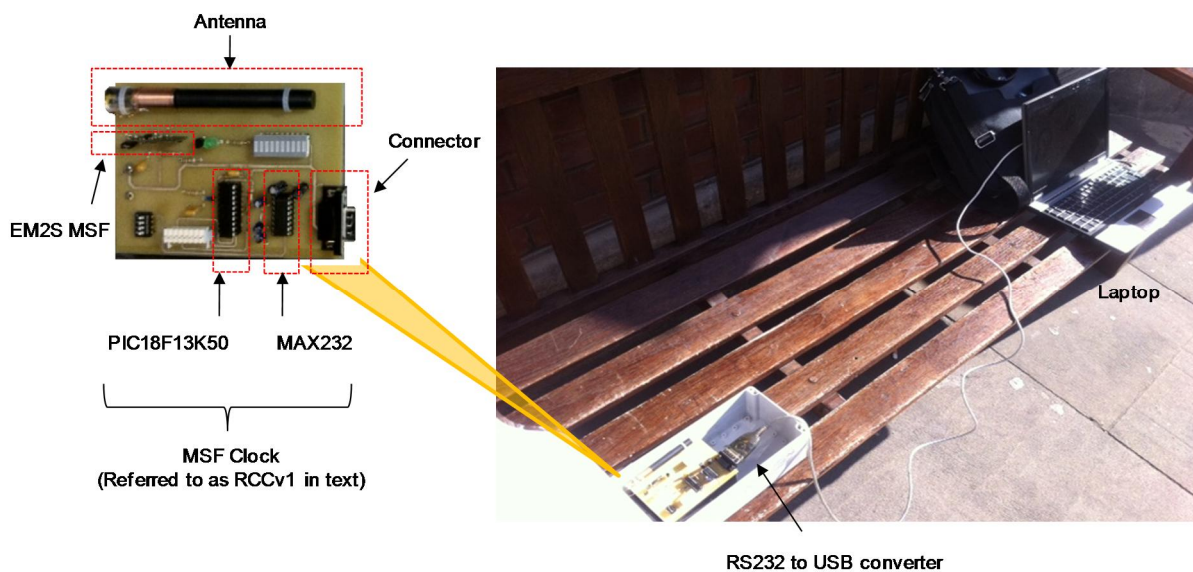


Figure 4.4. Snapshot of the experimental setup for time and date code validation.

- INTEGRATION PLATFORM:

The radio clock was connected directly to the mote, which is the CC2430EM module from Chipcon. This was done to establish a wireless sensor network which can be time synchronized by the MSF signal. A snapshot of this setup is shown in Figure 4.6. The compact version was built to show that the size of the MSF clock can be reduced if there is a size constraint. The compact design was achieved by using an antenna with a small footprint. The MSF clock was stacked underneath the CC2430EM module.

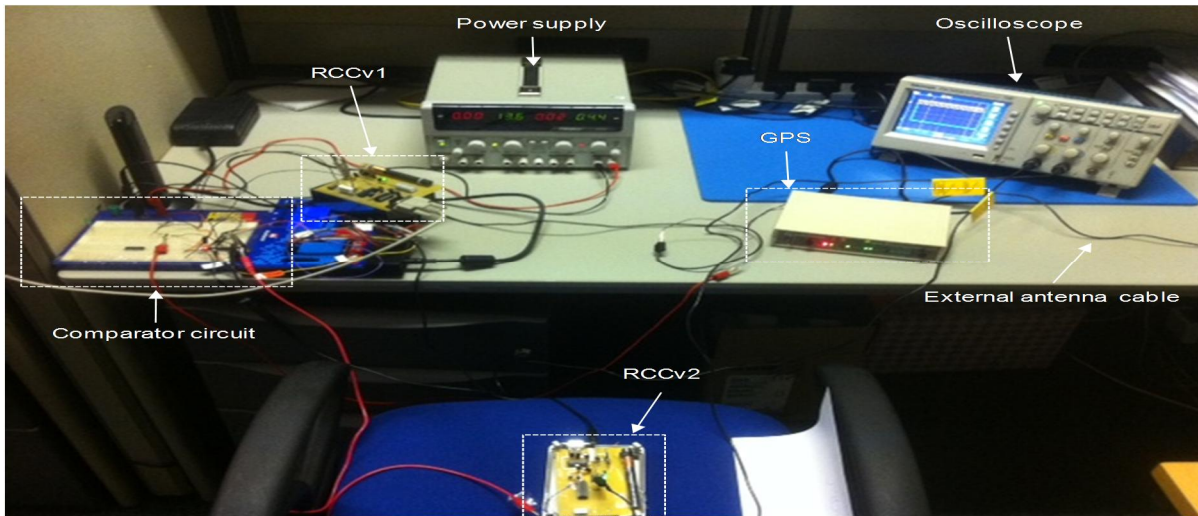


Figure 4.5. Snapshot of the experimental setup for signal quality assessment.

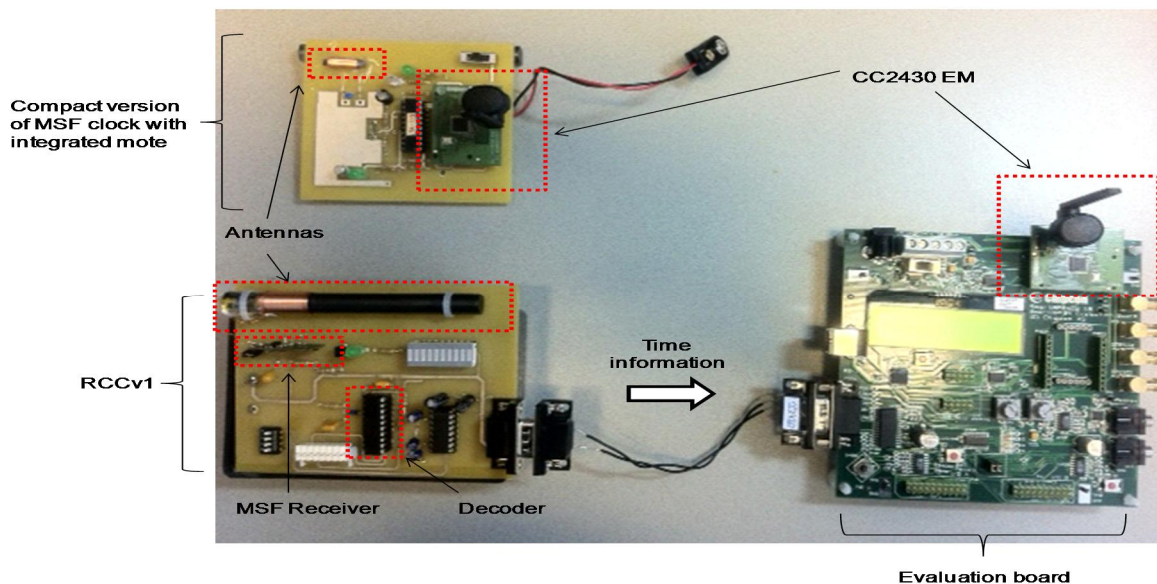


Figure 4.6. Snapshot of two versions of the radio clock. The upper version includes a radio clock and a mote. The two independent modules are shown underneath. In this case, CC2430EM module is connected via the evaluation board to the radio clock.

4.3. Radio Controlled Clock Performance

This section provides an in-depth overview of the performance of the MSF clock designed to work with the wireless nodes. The experimentally obtained results agree with the analytical results.

4.3.1 Theoretical Analysis

An analysis on the performance of MSF clock is presented in relation to its time required to achieve synchronization, coverage, energy-consumption and accuracy.

Time to synchronize:

To synchronize a node with the incoming MSF signal, a node needs to perform the following tasks:

- Detect the Start of Frame (SoF).
- Acquire the required bits from the data stream.
- Decode the acquired bits.

The time taken, τ_{sync} , to synchronize a mote with an incoming MSF time broadcast signal can be represented by Equation 4.1.

$$\tau_{sync} = \tau_{SoF} + \tau_{acq} + \tau_{dec} \quad \text{Equation 4.1}$$

where,

τ_{SoF} is the time duration to detect the SoF. It depends on the UTC time at the start of the synchronization process.

τ_{acq} is the time duration to acquire data bits. It depends on the information required from the data stream, and also whether the parity bit is included or not.

τ_{dec} is the time duration to decode the data bits. It is related to the processor speed and also on its availability.

The different factors which contribute towards adding time delay to synchronization process are elaborated below.

τ_{SoF} is equal to the seconds left in the start of next minute plus the time required to detect the unique pattern illustrating the start of a new minute. It is represented by Equation 4.2. Most minutes have 60 seconds, numbered 00-59 seconds. A positive or

negative leap second therefore lengthens or shortens a minute frame to 61 or 59 second minute (NPL, 2007).

$$\tau_{SoF} = T\{S_{MF}\} - t_{UTC} + 0.5 \quad \text{Equation 4.2}$$

$$S_{MF} = \{t_{UTC} \in \mathbb{N} | t_{UTC} \leq 59 + \ell_a\}$$

Where, ℓ_a represents the adjustment to a minute frame due to leap second.

$\ell_a = (-1)$, for negative leap second

$\ell_a = (0)$, for no adjustments, and

$\ell_a = (+1)$, for positive leap second.

Here, $T\{S_{MF}\}$ represents the last UTC second in the ongoing minute frame before new minute. t_{UTC} refers to the ongoing UTC second. S_{MF} defines the data set which incorporates the values of UTC seconds in the ongoing minute frame and $\mathbb{N}$ represents a natural number.

The time required to acquire the data bits depends on the information which is required from the bit stream. Figure 4.1 illustrates in detail the information contained within the broadcast MSF time signal. Here, two options can be exercised: one with and the other without the use of the parity bits.

$$\tau_{acq}[Incl. \text{ parity}] = 51 + 0.3 - 0.5 = 50.8$$

$$\tau_{acq}[Excl. \text{ parity}] = 57 + 0.3 - 0.5 = 56.8$$

τ_{dec} , the time required by the processor to decode the bit stream is negligible in relation to the above figures, especially, if the processor is running at MHz speed. It is also considered that the delay induced by processor to service the request is also negligible. As a result, Equation 4.1 becomes:

$$\tau_{sync} \approx \tau_{SoF} + \tau_{acq}$$

τ_{sync} without parity is given by Equation 4.3, and with parity bit is given by Equation 4.4.

$$\tau_{sync} = T\{S_{MF}\} - t_{UTC} + 0.5 + 50.8 \quad \text{Equation 4.3}$$

$$\tau_{sync} = T\{S_{MF}\} - t_{UTC} + 0.5 + 56.8 \quad \text{Equation 4.4}$$

Taking into consideration the leap second and substituting in the above mentioned approximation, results in the following:

$$\tau_{sync}(el, ep) = 110.3 - t_{UTC}$$

$$\tau_{sync}(il_+, ep) = 111.3 - t_{UTC}$$

$$\tau_{sync}(el, ip) = 116.3 - t_{UTC}$$

$$\tau_{sync}(il_+, ip) = 117.3 - t_{UTC}$$

where,

el: excluding leap second

il₊: including a positive leap second. Only positive leap second is considered here as it adds a delay to time synchronization process, whereas, a negative leap second will shorten this period.

ep: excluding parity bit

ip: including parity bit

The analysis shows that the time to synchronize a node depends on the UTC time at the start of synchronization process, and it can take up to 118 seconds. The time required by the receiver to stabilize after start-up is not considered in the calculations, and is vendor dependent.

In addition, if the objective of synchronization is to control a local oscillator, for instance with the UTC second and minute marker, and not to decode the entire bit-stream then the time required to synchronize will be reduced due to elimination of the data acquisition stage.

Signal coverage and received signal

The horizontal radiation of the MSF antenna is substantially omni-directional [NPL, 2007b]. According to NPL (2007b), the signal provides field strength which exceeds 100 $\mu\text{V/m}$ at a distance of about 1000 km from the transmitter. This covers the whole of the UK. The signal can also be satisfactorily received in much of northern and western Europe (NPL, 2007).

Furthermore, the carrier frequency of the MSF signal is maintained at 60 kHz to within 2 parts in 10^{12} (NPL, 2007). The signal can also be used as a frequency reference. The National Physical Laboratory (NPL) monitors the carrier frequency of the MSF signal and measures its phase difference against a reference signal derived from the UK national time scale. The values are expressed in terms of time intervals recorded at

midday each day and reported in the monthly bulletins. They can be used to calculate the frequency offset of the MSF carrier. For further details, refer to NPL (2011). The research presented here only focuses on the MSF time and date code signal and its quality and not on its use as a standard-frequency reference.

The results which will be shown in this chapter are based on the measurements made on the developed radio controlled clock systems which were operated independently. They will be referred to as RCCv1 and RCCv2 and are shown in Figure 4.5. The designs of the clocks are same and are built using the same components. Next, Figure 4.7 illustrates the traces obtained using oscilloscope and highlights the distinct markers.

The output from the MSF receiver at the start of a new minute is shown in Figure 4.7(a) with a distinct pattern of 500ms of carrier off, followed by 500ms of carrier on. BitA in the time code is transmitted after 100ms of start of every new second as shown in Figure 4.7(b). Figure 4.7(c) shows the traces of two MSF receivers operating independently. This illustrates the signal stability over time. Figure 4.7(d) illustrates the SoF as detected at two different receivers. These values are in accordance with the expected values explained in Section 4.2.

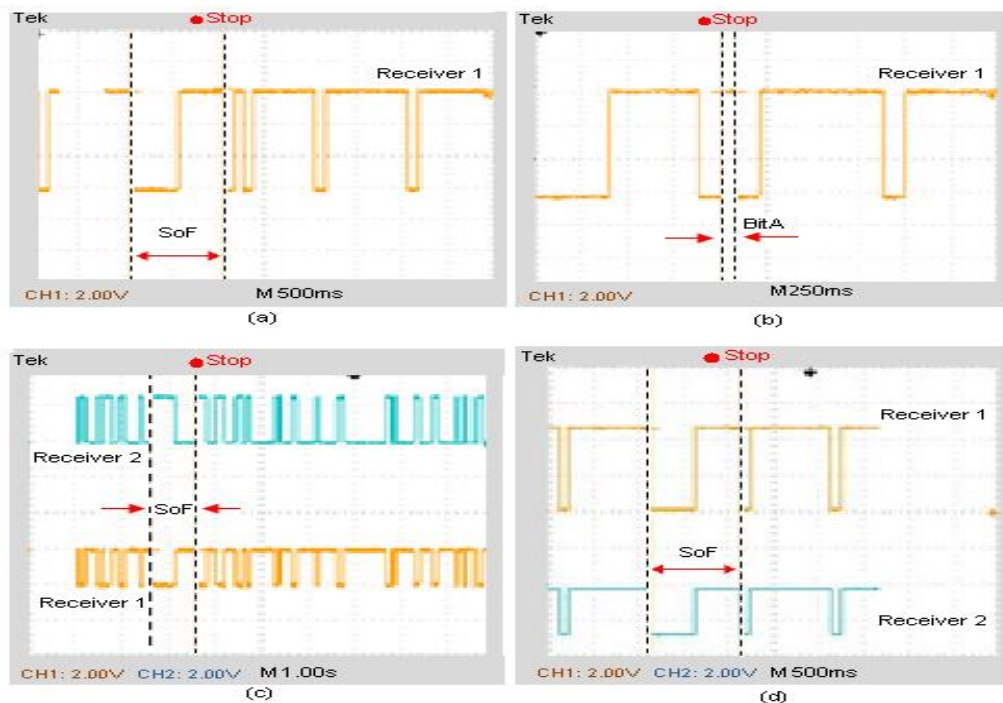


Figure 4.7. Demodulated MSF signals captured from the developed module. Panels (a) to (d) are explained in the text.

Energy consideration regarding hardware-assisted time synchronization

In this section, the energy consumed by an MSF receiver to operate is evaluated and compared to that of a GPS clock. For one time synchronization, the maximum energy consumed is:

$$E_{MSF} = I_{max} V \tau_{sync}$$

$$E_{MSF} = (0.0002)(3)(118) = 0.0708 \text{ J}$$

This value is based on maximum τ_{sync} calculated earlier. This calculation only considers the energy cost of operating an MSF receiver module, and not the supporting circuitry. It is because the supporting circuitry depends on the rest of the system architecture (i.e. the interfaces) and will vary from node to node. The receiver is used in conjunction with a passive LC-tuned ferrite antenna.

To compare these results with those linked to the GPS clock, time to first fix, t_{TTFF} , has to be identified. It is the time which a GPS receiver takes to calculate its initial location. The time required for fixing depends on several factors such as sensitivity, cold start, warm start and so forth. The required time to first fix is used in the calculation of energy cost. The GPS developmental kit used for evaluation purposes is based on Jupiter 32X series, and its t_{TTFF} are as follows (Navman, 2006):

$$t_{TTFF} \text{ at } -125\text{dBm} = 42 \text{ s}$$

$$t_{TTFF} \text{ at } -140\text{dBm} = 66 \text{ s}$$

These values are based on *cold start*, where either position or time data is unknown. If no information about the satellites is stored or if the information is outdated, then the time required to receive the complete signal is 12.5 minutes, and is referred to as *blank start* (Kowoma, 2007).

The initial power required for acquisition at 3.3V is 189mW, and average sustained afterwards is 136mW. The energy required in case of GPS development kit (Jupiter XLP series) is as follows:

$$E_{(GPS|-125dBm)} = (189/1000)(42) = 7.94 \text{ J}$$

$$E_{(GPS|-140dBm)} = (189/1000)(66) = 12.5 \text{ J}$$

$$E_{(complete \text{ reception})} = (189/1000)(750) = 142 \text{ J}$$

Table 4.1. Comparison of energy consumption in Joules between MSF and GPS based time synchronization solutions.

	MSF		GPS	
	Energy	Ratio	Energy	Ratio
Cold start at -125dBm	0.0708	1	7.938	112
Cold start at -140dBm	0.0708	1	12.474	176
Blank start for GPS	0.0708	1	141.75	2002

A comparison of energy required as discussed above is summarized in Table 4.1 which demonstrates that the energy consumption of the MSF clock is significantly less compared to a GPS clock. These calculations have not taken into consideration warm start, as it is only applicable after a recent location fix (Navman, 2006).

The calculations presented here are based on the operational parameters of EM2S receiver. Other more energy-efficient off-the-shelf RF receiver such as CME6005 from C-MAX can be used to further reduce the radio clock energy consumption. Similarly, more efficient GPS receiver can also be found such as JN3 receiver (Telit, 2012). Using the energy calculation of EM2S and JN3 receiver still gives a ratio of (1:59). The objective of presenting this information and a comparison in Table 4.1 is to provide an estimate of the ratio of energy consumption between these two available time synchronization options.

Accuracy of a radio clock

A radio clock regulates itself by employing an electronic circuitry to decode the incoming time broadcast signal. As a result, the radio clock functions as a time-keeping device which is steered by the time broadcast signal. A radio clock has accuracy within given bounds. Its accuracy depends on the signal it utilizes, its location and the update frequency. A radio clock periodically synchronizes its time to the time broadcast signal.

Radio clock time synchronization errors

The factors which contribute towards time synchronization error in a radio clock are as follows.

- **ACCURACY OF TIME BROADCAST SIGNAL:**
This error is similar to send time and access time as confronted by time synchronization protocols and were introduced in Chapter 3. In the case of MSF

transmitter, there are three atomic clocks at the radio station; one main and two backups (NPL 2007a). Clocks at the radio station are steered to confine with the UTC. The timing of the rise and fall of the edges of the MSF signal is governed by seconds of the UTC. Every UTC second is marked by switching the carrier off, this second marker is transmitted with accuracy better than ± 1 ms [NPL, 2007b].

- PROPAGATION TIME:

If the signal travels the shortest distance from station to radio clock then this time is kept short. The signal reflected from ionosphere will take long time to receive and will also be attenuated. The coverage of MSF signal is up to 1000 km from Anthorn. The distance of 100km will delay the time signal by 0.33ms, whereas a path distance of 1000km will induce a delay of approximately 3.33ms. The value can be estimated given that the distance between the transmitter and the radio clock is known.

- RECEIVE TIME:

The start of every UTC second is marked by a carrier off and this On-Time-Marker (OTM) is the first of the 60 kHz cycle that is switched-off. According to Lombardi (2010), a radio clock should be able to detect OTM within ± 0.000008 s. OTM detection accuracy is related to antenna bandwidth, and is difficult to identify when the power drop occurred exactly in the time signal and when was it detected at receiver (Lombardi 2010). Hence, the receive time depends on received signal, receiver design and associated digital processing delay. In addition, the processing delays include: time to retrieve data, time to process and produce output, and response time of the display circuitry. Such sources of delay can be estimated.

The accuracy of the radio clock at the time of synchronization can be estimated as follows.

<u>Sources of Inaccuracy</u>	<u>Seconds (s)</u>
Accuracy of MSF broadcast signal	± 0.0010
Propagation delay (1000 km from Anthorn)	$+ 0.0033$
OTM selection	± 0.000008
Quartz Crystal (32.768 kHz)	± 0.000015

The processing delays are ignored in this calculation. It can be seen that the inherent sources of inaccuracy can lead to a synchronization error of up to 4.323ms between the radio clock time and the actual UTC time.

4.3.2. Empirical Results

This section presents experimental results and compares them to those expected based on theoretical analysis presented in the previous section. The setup of the experiment comprises of two MSF clocks, a reference GPS module, interface circuitry for comparison and a laptop running a custom-built program to log the data. The snapshot of the setup is shown in Figure 4.5.

Latency

In order to identify the accuracy of the radio clock, the output of the radio clock is compared to that of the GPS receiver in order to calculate the latency, which essentially is the time synchronization error. The GPS module used in the experiment outputs a pulse per second aligned to the UTC, and has accuracy better than a microsecond (Navman, 2006).

A timer was programmed to calculate the difference between the start of a new minute according to GPS clock and that of a MSF clock. This delay in reporting is being referred to as *latency* and is linked to accuracy of the radio clock. The value is measured in microseconds and is graphically shown in Figure 4.8. The GPS clock will be leading compared to the MSF clock. This value of latency measured will encompass all the sources of inaccuracy discussed in the previous section. Therefore, the outcomes of these experiments will be used to: (i) report the trend observed in latency values (ii) to identify the difference in theory and in practice, and (iii) highlight the sources of inaccuracy dominant in practical deployments.

The experiment was carried out for longer intervals of time to characterize the trend in latency with time. It was conducted at different locations to identify the effect of distance on latency distribution. One location was selected to be away from transmitter which is London and the other was chosen to be near transmitter which was Whitehaven. The test sites are shown in Figure 4.9.

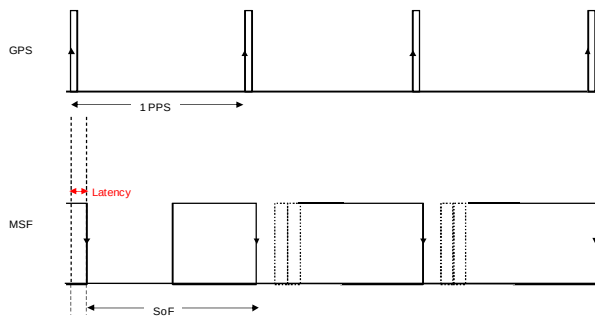


Figure 4.8. Latency calculations based on timing pulses of GPS and MSF modules.

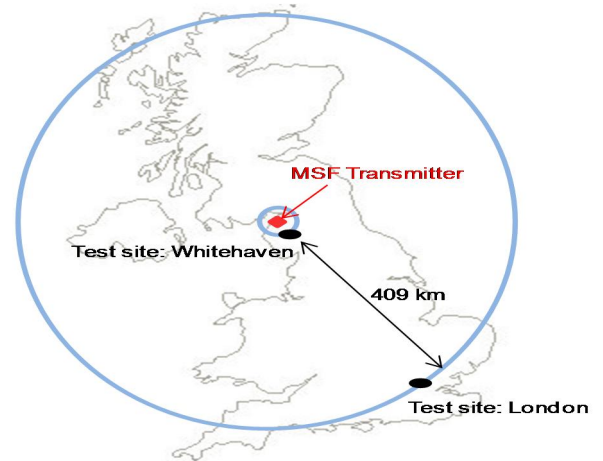


Figure 4.9. Test sites for the experiments.

To quantify the quality of the MSF signal, the latency value of each MSF receiver was recorded. Figure 4.10(a) shows a cumulative distribution plot of latency values associated with the RCCv1. The experiment was conducted in a site in London and it can be seen that the 90% of the recorded latency value is within 20 ms of the UTC time.

The same experiment was then conducted in a site in Whitehaven and the cumulative distribution plot of latency is shown in Figure 4.10(b). In this case, it was noted that the 90th percentile was found at 16.75 ms. From these plots it is apparent that in both cases the recorded value of latency, even minimum recorded latency, was higher than what was expected based on the analysis presented in Section 4.3.1. The minimum recorded latency is referred to as minimum time synchronization error relative to the UTC in the plot because it causes an offset during clock synchronization leading to synchronization error. The higher value of radio clock uncertainty is due to the receiver module. The internal processing of the radio receiver such as antenna bandwidth, components tolerances and automatic gain control are the cause of higher than expected clock synchronization error relative to the UTC.

To further analyze the results, Figure 4.11 shows the latency distributions of these results as normalized histograms. Table 4.2 summarizes the outcome. The obtained results show that the mean of the distribution is approximately 17.59 ms for

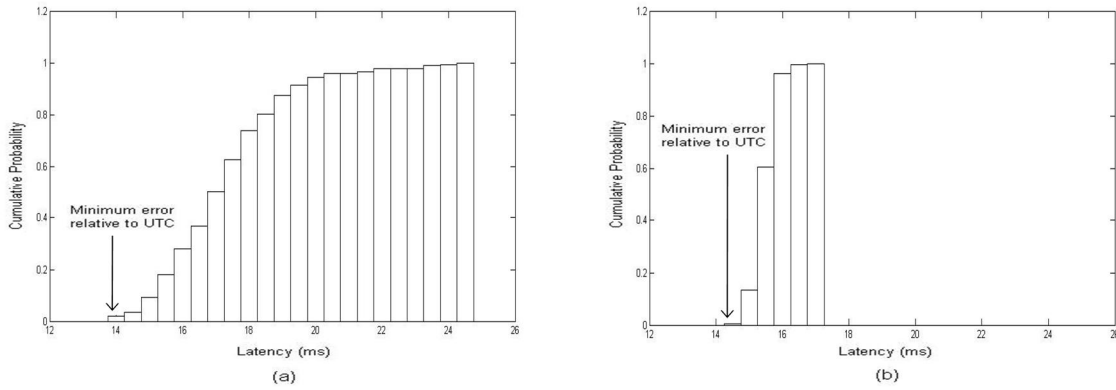


Figure 4.10. Cumulative probability distribution of latency value corresponding to RCCv1. recorded at a site in (a) London, and in (b) Whitehaven.

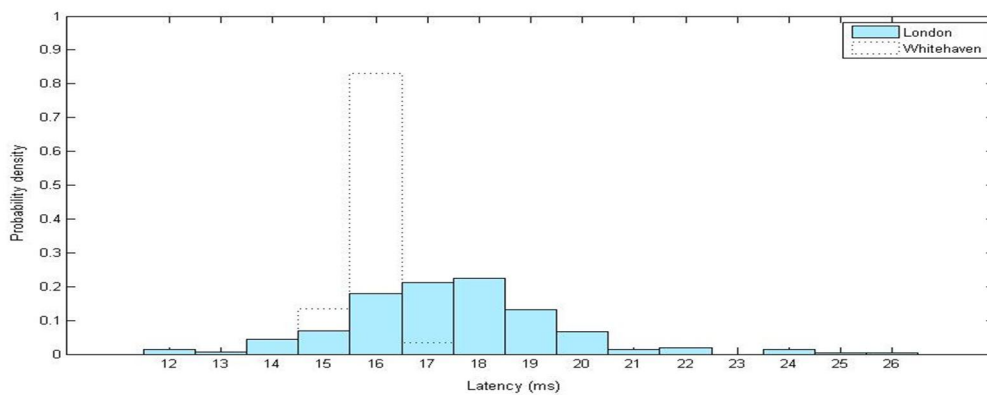


Figure 4.11. Latency distribution of RCCv1 for experiment conducted at two locations.

experiment conducted in London, whereas the mean of the distribution for experiment conducted in Whitehaven was 16.02 ms. The standard deviations were 2.19 ms and 0.39 ms respectively.

The cause of this shift in the latency is due to the propagation time. The path which MSF signal can take are two: the portion which follows the ground is groundwave, and the other bouncing from ionosphere is referred to as skywave (Winder et al. 2002). The path followed by skywave is guided between the earth and the D layer of the ionosphere, and at night this ionized layer becomes less dense, allowing radio signals to travel further (Lombardi 2002). According to Allison (2003), within 1000 km of transmitter the received signal is mostly groundwave. Hence, it is assumed that the signal travels the distance equal to the distance between the two sites. This distance of 409 km would cause a propagation delay of approximately 1.36 ms, and the shift experienced is approximately 1.57 ms. The difference is due to the variation in distance travel and also due to the counter used. The counter used in the experiment increments

at discrete value of 512 μ s. It is concluded that the propagation time is responsible for this shift. Furthermore, the cause of reduction in the standard deviation is due to the strong signal strength near the source because it is predominantly groundwave for the experiment conducted in Whitehaven.

The results shown and discussed up to now were related to the RCCv1. Figure 4.12 shows a cumulative distribution plot of latency values corresponding to RCCv2. It is for the experiment conducted in Whitehaven and it can be seen that the 90% latency percentile is at 23.5 ms. The difference in the two reported results based on same radio clock design have different reported uncertainty and it is due to the receiver design and its hardware implementation.

The outcome of these experiments has shown that the latency values corresponding to both RCCv1 and RCCv2 are higher than what was expected, and it holds true for experiments conducted in geographically different locations. It signifies that this latency is linked to the receivers hardware variation (e.g. individual components tolerance within each receiver, EM2S), its internal operation (e.g. automatic gain controller – the radio controlled clock receivers use the LF signals field strength to generate an output to control the amplifiers, and their time constant are further influenced by the capacitors as in the case of Temic (1996)), and further on the LC-tuned antenna bandwidth. Moreover, based on the experimental results it is noted that the recorded latency is fixed for each receiver, therefore it can be estimated and compensated for.

Jitter

The variation in latency is referred to as *jitter*. A summary of the jitter values recorded in milliseconds are shown in Table 4.3. The values reported are of RCCv1 and RCCv2.

Table 4.2. Latency distribution values in milliseconds for RCCv1.

	Experiment Site: Whitehaven	Experiment Site: London
Minimum	14.85	9.216
Maximum	17.41	28.16
Mean	16.02	17.59
Mode	15.87	17.41
Medium	15.87	17.41
Standard Deviation	0.39	2.19

They are based on the same receiver module. However, they have different performance due to hardware variations due to factors mentioned above. The columns labeled *s.d.* and *max* here refer to standard deviation and maximum value of jitter recorded respectively. It can be seen that the two clocks have similar but varying values of jitter recorded. Near the broadcast source, the value of jitter is significantly less compared to that experienced at a far distance. The jitter experienced in the latency of the MSF signal increases the time synchronization error.

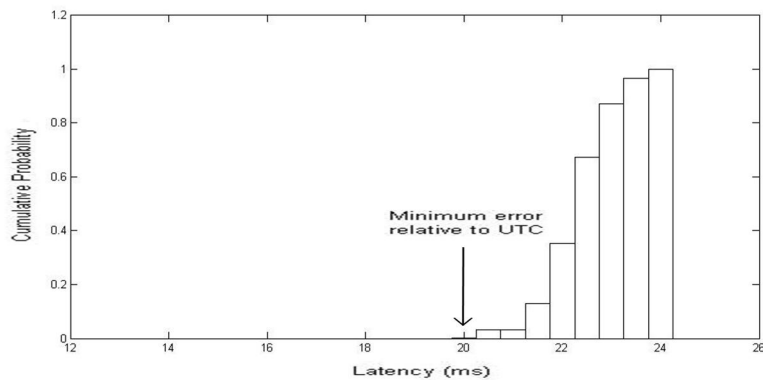


Figure 4.12. Latency value of RCCv2 for experiment conducted in Whitehaven.

Table 4.3. Jitter in milliseconds as recorded in experiments.

Experiment site	RCCv1		RCCv2	
	s.d.	max	s.d.	max
London	2.19	10.57	2.78	11.78
Whitehaven	0.39	1.39	0.68	2.05

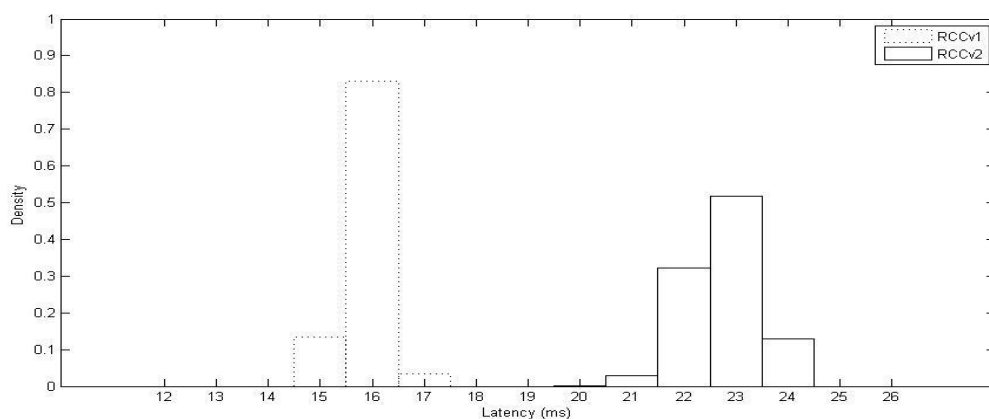


Figure 4.13. Latency distribution of RCCv1 and RCCv2 as recorded in Whitehaven.

Time synchronization error

The latency values presented earlier are in relation to the actual UTC time. In order to identify the time synchronization error experienced between RCCv1 and RCCv2, the normalized histograms are presented in Figure 4.13, and the summary is given in Table 4.4. The figure highlights that the two data sets are non-overlapping. Therefore, they will introduce a minimum time synchronization error.

It can be seen that the time synchronization error between RCCv1 and RCCv2 based on mean latency values reported in Table 4.4 is approximately 6.5 ms. The deviation is seen originating from the difference in SoF reported by RCCv1 and RCCv2, and is shown in Figure 4.14. Therefore, in order to reduce time synchronization error, receive time has to be addressed. For further information relating to this source of error, refer to Galleon (2009).

Table 4.4. Latencies distribution in milliseconds as experienced in Whitehaven.

	RCCv1	RCCv2
Minimum	14.85	20.48
Maximum	17.41	24.06
Mean	16.02	22.51
Mode	15.87	22.53
Medium	15.87	22.53
Standard Deviation	0.39	0.68

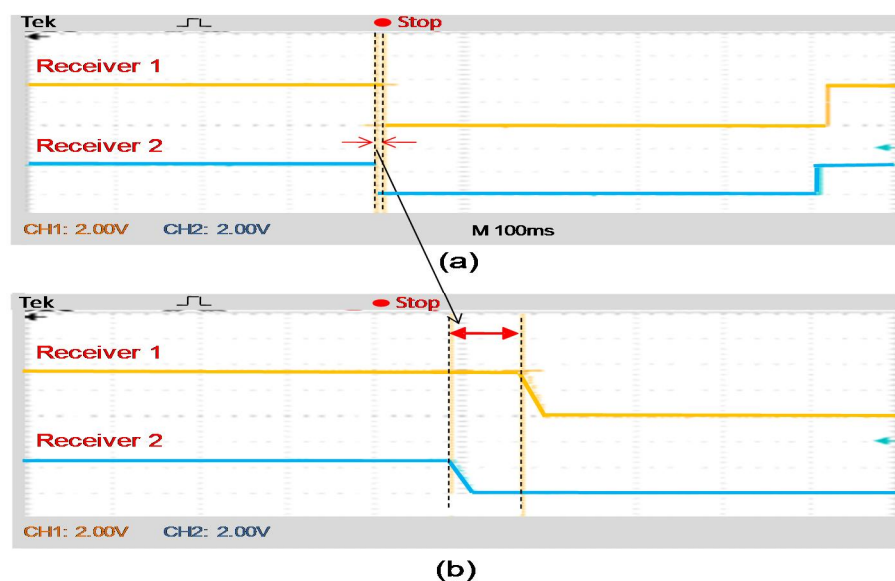


Figure 4.14. (a) SoF as captured from two receivers, and (b) is magnified version of (a).

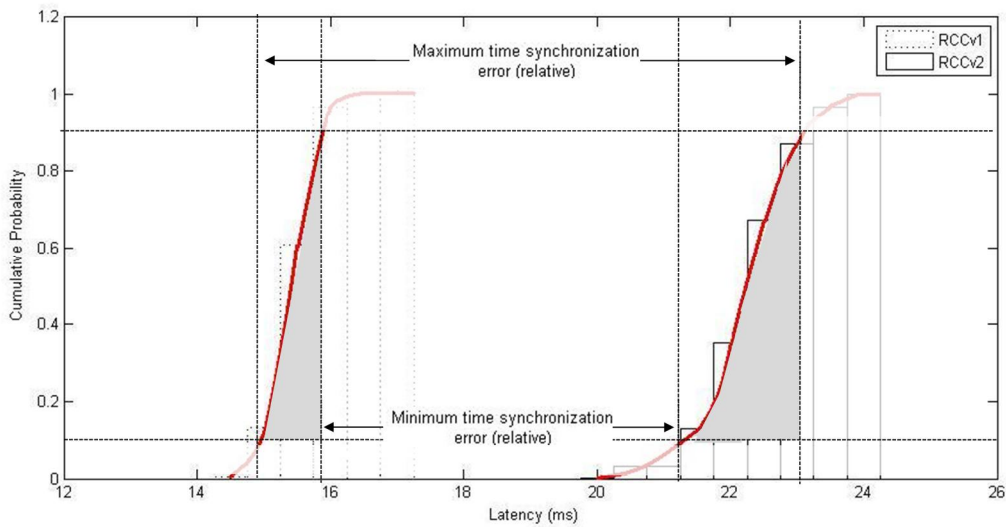


Figure 4.15. Cumulative probability of RCCv1 and RCCv2 for experiments conducted in Whitehaven.

Figure 4.15 presents a cumulative probability plot of the data presented in Figure 4.13. The plot highlights the region where 10-90% of the latency values reside for both radio clocks. Based on this data, the minimum time synchronization error amongst RCCv1 and RCCv2 is approximately 5.4 ms and maximum time synchronization error is 8.2 ms.

The two independent radio clocks have time synchronization error relative to the UTC given by latency. Practical experience has shown that latency varies from device to device and also depends on the geographic location of the receiver. Moreover, the latency values reported are higher than those which were expected based on theoretical analysis presented earlier. The receive time which incorporates hardware variations in this case is found to be the main cause of this discrepancy. In the theoretical analysis the only factors considered in receive time were OTM detection and quartz crystal uncertainty. The results highlight that the detailed operation of the receiver and its implementation cannot be ignored in building a time synchronization system using an off-the shelf radio clock receiver.

Reliability of MSF signal

So far, the experiments conducted were to identify the accuracy of the SoF marker which were detected by the radio clocks and can be used as a reference for time synchronization. In order to validate the integrity of the received time and date code information contained within the bit stream of the MSF signal, the entire frame was

received and decoded. This value was recorded and compared to that of the actual ongoing time from another source. A snapshot of the GUI which was developed for this purpose is shown in Figure 4.16. The GUI allows the selection of computer port to which the radio clock is connected and configures the communication baud rate. Once the connection is set up, radio clock sends the received bit stream for each frame every one minute. The software then compares the value of the time and date information conveyed by the MSF clock to that of the computers own clock. This comparison does not include the second information. It is because the information regarding the ongoing second's integrity is governed by the OTM. To quantify its reliability, an accurate reference is required. The hardware setup shown in Figure 4.3 using GPS was used for this purpose. Previous discussion has in detail elaborated the obtained results with latency reported in milliseconds in relation to the UTC time.

To quantify the quality of the received bits from the MSF minute frame the RCCv1 was left to run continuously for three days in an indoor site in London. Figure 4.17 summarizes the outcome of this experiment. Each individual received frame was analyzed separately. Within each frame, bits were further analyzed based on the group.

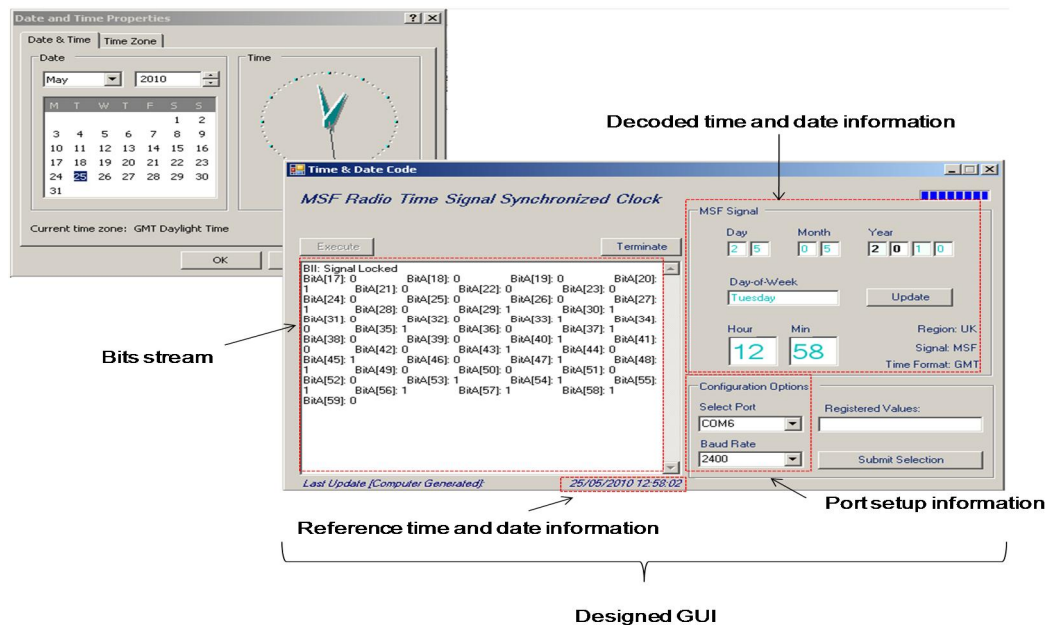


Figure 4.16. Snapshot of the GUI developed for displaying, archiving, and validating the time and date information extracted from the MSF signal.

As can be seen from Figure 4.17 that at least 99.5% of the received MSF frames were able to successfully decode the year, month and day related information. The least successful decoding was linked to minute related bits. Even in that case, successful decoding was achieved in excess of 95%. At the receiver end, there is groundwave and also a residual sky wave which is reflected off the ionosphere. The sky wave component of MSF signal varies from time to time and depends on seasons, for instance it is stronger in winter than summer and is different during dark path hours compared to those during daylight hours and is linked to the sub-layers in ionosphere like D-layer and its state throughout the radio clock operation (NPL, 2011). Therefore the drop in signal strength due to destructive interference can result in BER. Here, it is assumed that there is no nearby sources of interference at the receiver which compromised the received MSF time and date code information.

The high success rates show that the data retrieved from the incoming MSF signal is reliable. However, there were instances where SoF was not detected, and neither was the bit stream which follows. The signal recovers itself and a maximum outage of 5 minutes has been experienced. In addition, the quality of the signal has been seen to be better during the night time.

In the reported results, parity bits were not utilized and can be used to identify if the bit stream has altered. A similar test carried out near the transmitter recorded a higher reliability than that presented in Figure 4.17.

It can be concluded that the experimental observations match the analytically expected results. However, the time synchronization accuracy is dependent on the hardware used and its geographic location.

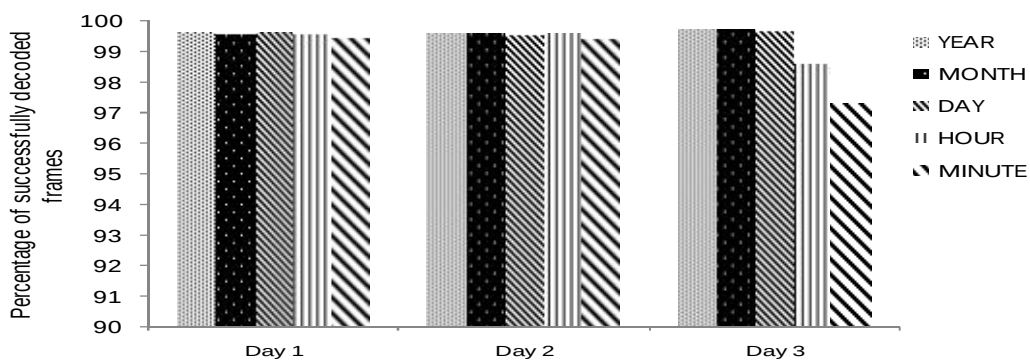


Figure 4.17. Summary of the received MSF data frames.

4.3.3. Radio Controlled Time Synchronized Wireless Sensor Network

One of the applications of the proposed system is for time synchronization of WSNs. Previous sections have presented the performance analysis of the built versions of the MSF clocks. This section will demonstrate the performance of a wireless sensor network synchronized using these radio clocks. RCCv1 and RCCv2 were connected to the CC2430EM modules. A WSN was established based on the time synchronization achieved via the radio clocks and the data generated was accordingly time stamped. The use of this out-of-band broadcast signal helped to achieve time synchronization relatively faster and also in a topology independent manner.

Time synchronization at regular intervals

An experiment was setup in which two motes were programmed to synchronize at regular intervals, every 3 hours in this case with the MSF signal. The radio clocks were programmed to independently receive and decode the time information. In order to conserve the battery life, the motes were programmed to switch off the radio clocks after time synchronization, till the time for next synchronization. The outcome of the experiment is shown in Figure 4.18. The experiment highlights the clock offset between two motes over a given period of time. In Figure 1.3 it was demonstrated that the clocks go out of synchronization in time. Therefore, they are resynchronized at regular intervals. As a result, the motes always remain synchronized within a given bound during their operation. Also, the time synchronization error is within milliseconds at the time of synchronization, as was expected based on the results shown in Section 4.3.2.

How frequently the synchronization should be done depends on the maximum offset which an application can tolerate. To remain synchronized within a bound of, for instance, 100 ms, the time synchronization is required at intervals, $\tau_{interval}$, specified in Table 4.5. The calculations are based on Equation 4.5, modified from Dargie *et al.* (2010).

$$\tau_{interval} \leq \frac{|\varepsilon_{offset}| - |\varepsilon_{sync}|}{\rho_{max}} \quad \text{Equation 4.5}$$

Here ε_{offset} is maximum allowed clock offset, ε_{sync} is time synchronization error, and ρ_{max} is maximum skew (i.e. frequency offset) of the oscillator. The table shows a comparison between two hardware assisted time synchronization schemes, and also for

oscillators with varying accuracy. In between time synchronization, the local oscillators are used for timing purposes. In addition to frequency inaccuracy, oscillators are also affected due to aging and operating temperature. In the calculations presented in Table 4.5 it is assumed that the oscillator is stable but not accurate. In the table, the MSF-theory calculations are based on synchronization error of 1 ms. MSF practice (without the proposed algorithm and only using off-the shelf receivers) calculations are based on synchronization error of 6.5 ms. This value is based on mean error reported in Table 4.4. Further, GPS related calculations are based on time synchronization error of a microsecond.

It can be seen that even with a synchronization accuracy of a microsecond, achieved via a GPS receiver, the periodic synchronization intervals needed do not differ a lot compared to that with MSF clock. This is because of the inaccuracy of the local oscillator. On the other hand, a high precision local oscillator such as Temperature Compensated Crystal Oscillator (TCXO) compensates for deviation due to temperature, and results in longer duration of operation without the need for time synchronization. To summarize, the benefits of high time synchronization accuracy are outweighed by the crystal oscillator inaccuracy.

Table 4.5. Comparison of required time synchronization intervals.

Required Synchronization Intervals (minutes)				
Allowed offset	10 ms		100 ms	
	4 PPM (TCXO)	40PPM (XO)	4 PPM (TCXO)	40PPM (XO)
MSF - theory	37.5	3.75	412.5	41.25
MSF - practice	14.6	1.5	389.6	39.0
GPS	41.7	4.2	416.7	41.7

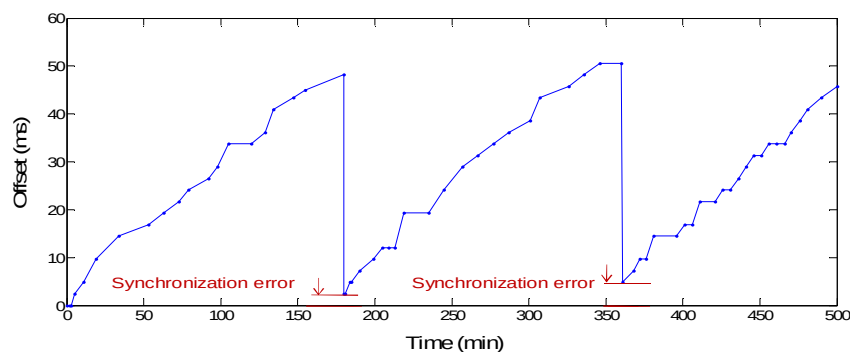


Figure 4.18. Time offset between two motes which are synchronized by the MSF signal.

Stability

Stability is an estimate of the frequency or time fluctuations of a signal over a given time interval with respect to a mean frequency or time offset (Bishop, 2005). The Allan variance is a commonly used statistical measure of stability. The stability values of oscillators are often reported as the square root of Allan variance known as *Allan deviation* (Lombardi, 2008). It quantifies the rate of change of clock parameters correlated with observation intervals (Riley, 2007). Therefore, it depends on length of time used to make measurements and its rate (Bishop, 2005). The Allan deviation formula requires estimation of the fractional frequency. It is expressed as a dimensionless value and can be calculated using Equation 4.6 (Jeffay et al., 2002).

$$y_k = \frac{x_k - x_{k-1}}{\tau} \quad \text{Equation 4.6}$$

Here, x_k represents the k -th measurement of time offset between the clock under test and the reference standard. The Allan deviation formula is expressed in Equation 4.7 (Drentea, 2010).

$$\sigma_y(\tau) = \sqrt{\frac{1}{2(M-1)} \sum_{i=1}^{M-1} (\bar{y}_{i+1} - \bar{y}_i)^2} \quad \text{Equation 4.7}$$

Here, the $\bar{y}_i$ series contain the estimates of the average fractional difference and M is the total number of values in the series. The data samples are equally spaced in segments τ seconds long.

In the case of computer clock the deviation is expected to happen in measure of hours according to Bletsas (2005). To measure the stability of the built version of the radio clocks the following experiment was conducted.

Two independent radio clocks were left to operate continuously for several hours. At the start of every minute the time of the radio clock was noted and its offset compared to the time reported by GPS was recorded. The resolution of the data recorded was 0.5 ms. From those time offset values the dimensionless frequency offset values were calculated. The frequency offset values were then used to compute Allan deviation for various values of averaging times, τ , and the results are shown in Figure 4.19.

From the figure it is noted that the two clocks have similar trend. Starting from left, the plot tends to a straight line with a logarithmic slope of -1, which is attributed to phase

noise (Bishop, 2008). Thermal noise is one of the types of noises found in an oscillator and appears as phase noise. It is usually considered as additive noise with high cutoff frequency (Dyer, 2001). Furthermore, as the averaging time increases the offset between the two narrows, and both clocks tend to have the Allan deviation value below 10^{-7} at an averaging time of 10000 seconds. It highlights the two clocks are likely not to deviate more than 1 ms in 2.77 hours.

To further highlight the long term trend in the stability of RCCv1, the same experiment was conducted for several days. This time, the time offset values were recorded every hour. The Allan deviation values of this experiment are plotted in Figure 4.20. Here, it is noted that as the averaging time is increased, the long term stability increases. The graph highlights that based on past experiences recorded in the operation of RCCv1, the clock is likely not to exceed 1 ms of time error in a week.

To summarize, it can be concluded that the RCCv1 exhibit a long term stability as the Allan deviation value decreases with the increase in averaging time. It is also noted that the uncertainty value is around 1 ms for longer intervals of time. It is because the RCCv1 was operated continuously, and it outputs a pulse stream. This consistent demodulated output is governed by the MSF signal which is transmitted within an accuracy of about 1 ms. Therefore, the uncertainty is directly linked to the MSF transmitter and the receiver circuit. The hardware variation in the receiver circuit and its effect on the stability of the Allan deviation are illustrated in Figure 4.19.

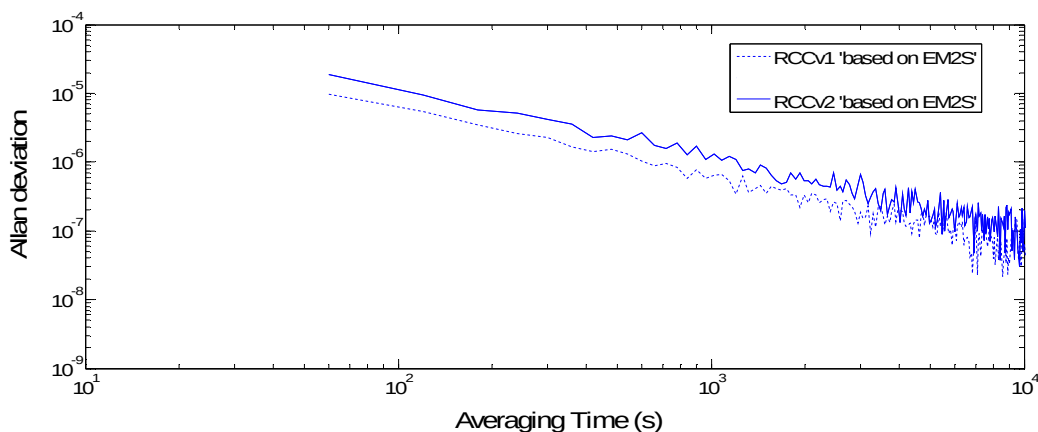


Figure 4.19. Allan deviation of RCCv1 and RCCv2 clocks which are based on EM2S.

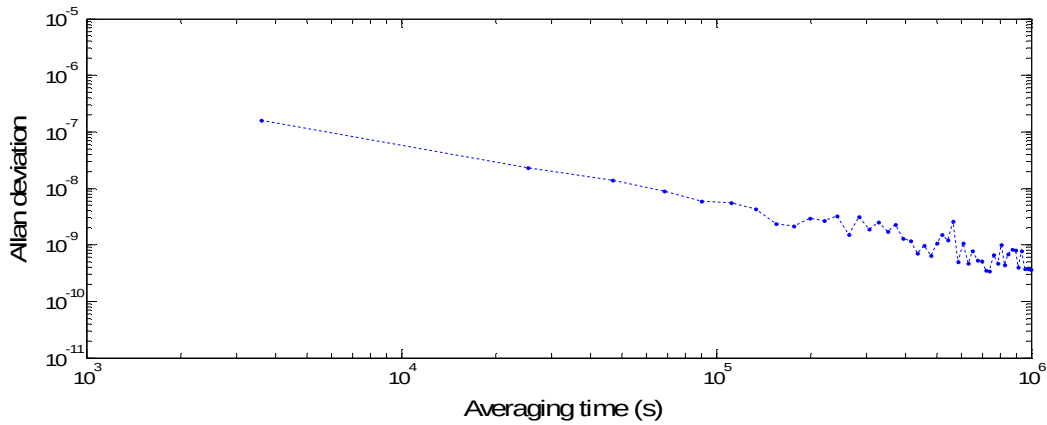


Figure 4.20. Long term trend in Allan deviation values for RCCv1.

4.4. Minimization of Time Synchronization Error

In this section, an algorithm has been proposed to increase the time synchronization accuracy. It was found through experiments that each field device experiences different offset and the latency changes with distance. If only one OTM marker is used to time synchronize a field node then its accuracy will be limited as was shown in Figure 4.15 and Figure 4.18. Therefore, the effect of jitter on time synchronization accuracy needs to be minimized.

Characterizing the latency distribution

In order to estimate as to for how long the radio clock needs to be operated for recording the latency readings and also to approximate the latency distribution, a statistical measure referred to as Kullback-Leibler Divergence (KLD) is used. It quantifies the difference of latency between two distributions. As KLD is not symmetric, an average is taken between two relative KLDs, an approach similar to Shrivastava *et al.* (2007). The value of KLD is zero when two distributions are identical. KLD for two probability mass function $p(x)$ and $q(x)$ is defined in Equation 4.8 (Thomas, 1991).

$$D(p||q) = \sum_{x \in X} p(x) \log \frac{p(x)}{q(x)} \quad \text{Equation 4.8}$$

The method requires a reference distribution to represent the true distribution of latency values. The best empirical approximation to the reference distribution is when a large amount of continuous latency data has been collected. Here, it is assumed that the distribution formulated using continuous one hour of latency data as a reference final

distribution. The estimated latency distribution for comparison was computed using latency readings collected over a period of time, up to one hour. Then, the average KLD was found using distribution formulated using latency data collected over a given period of time. The aim is to find the minimum time required to collect the latency data which gives a good estimate of the reference distribution. The average KLD found is shown in Figure 4.21.

It can be seen from Figure 4.21 that in case of both radio clocks the average KLD stabilizes after 10 minutes. It implies that a data recorded over a period of 10 minutes is a fair approximation of the latency trend. The KLD values shown in Figure 4.2.1 (b) do not converge to zero but have stabilized and the difference with KLD value of zero (i.e. in case of identical distributions) is marginal. These results are used for identify the duration for which the MSF receiver needs to be operated in order to characterize the latency distribution.

Latency time trend

Figure 4.22 plots the time series value of the recorded latency. Figure 4.22(a) and (c) are for RCCv1 readings at two different sites, and (b) and (d) are for RCCv2 also at two different locations. As discussed earlier, latency is characterized by its mean value and its standard deviation, where the deviation is termed jitter.

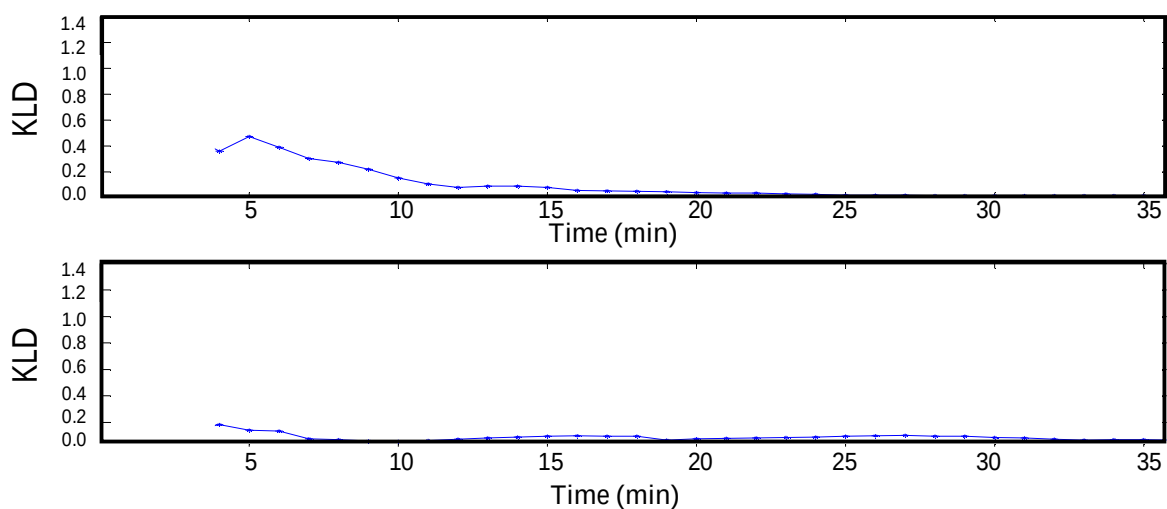


Figure 4.21. KLD with respect to reference distribution versus time (a) for RCCv1 and (b) for RCCv2 for experiments conducted in Whitehaven.

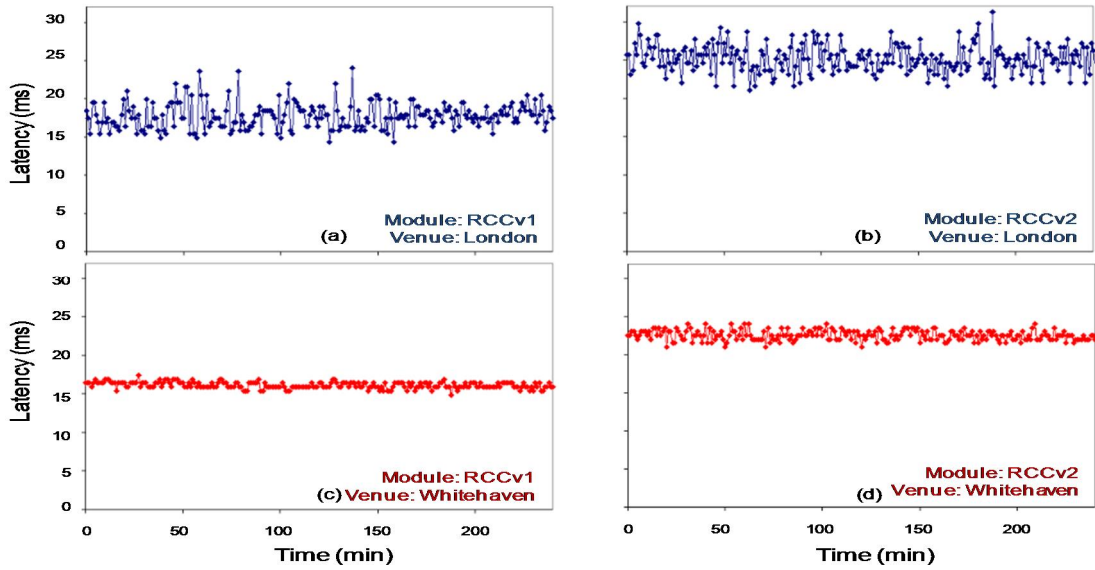


Figure 4.22. Latency versus time trend recorded over a period of 4 hours at UTC 00 seconds. Panels (a) to (d) explained in text.

Overview of proposed algorithm to improve accuracy

The latency values reported above were recorded using GPS as a reference signal. During the actual deployment, however, GPS will not be available. Therefore, a local reference was needed to measure the variation in latency. As a result, a high precision Temperature Compensated Crystal Oscillator (TCXO), which is DS3232 module, was included in the design of the radio clock. The signal from DS3232, has an accuracy of ± 2 PPM, and can be used for reference in order to identify the jitter.

The procedure to improve the time synchronization accuracy of the radio clock is shown in Figure 4.23. The process is divided into two stages. In first-stage, which is referred to as an *off-line stage*, a device gathers the latency data for a period of time in order to characterize the trend in latency for each individual radio clock. The outcome of this process is an estimation of a clock offset value. A flow chart of the procedure is given in Figure 4.23(a). This process requires a reference GPS clock and the radio clock which needs to be characterized. Initially, both of these clocks are allowed to stabilize before taking the time offset readings, referred to as latency. The outcome of the KLD estimation presented earlier is used to estimate how many readings are to be taken. Furthermore, the Kalman filter can be operated on the latency data to estimate the clock offset.

The second-stage is an *on-line stage* in which the moving average of consecutive markers is used to minimize the effect of jitter. The flow chart of this process is given in Figure 4.23(b). Here, the objective is to align the local clock offset value such that it is near the value estimated earlier. In this case, the local reference, DS3232, is used to minimize the effect of jitter. The process involves the time synchronization of the local oscillator with the i -th marker of the Start of Frame (SoF). Afterwards, the variation in the following x samples of SoF are recorded. A simple moving average is taken of those values, and the local oscillator output which was initially aligned with the i -th marker is adjusted based on the experience of later recorded jitter values. As a result, the output from the radio clock can then be approximated to be offset by a value equivalent to earlier estimated C_{o-p} value. The radio clock can then compensate for this offset.

If the same procedure is repeated for all concerned radio clocks then the time synchronization accuracy will be improved and the minimum time synchronization error as shown in Figure 4.15 can be eliminated. This procedure was implemented partly on hardware and rest through simulations. Based on obtained results, it is found that it offers a better accuracy than a one-off synchronization because of moving average. The detailed working of the algorithm is described below.

Clock time: Let $C_n(t)$ represent the clock time on node n at time t .

Frequency: The rate at which the clock progresses, and is denoted by $C_n'(t)$.

Offset: The clock offset $C_n(t)$ is the difference in time reported by a clock relative to any other clock. This can even be in relation to UTC time.

Skew: It is the difference in frequencies of the two clocks. Therefore skew of $C_n(t)$ relative to $C_m(t)$ at time t is $C_n'(t) - C_m'(t)$.

Drift: It is the second derivative of $C_n(t)$.

Panel 4.1. Summary of nomenclature.

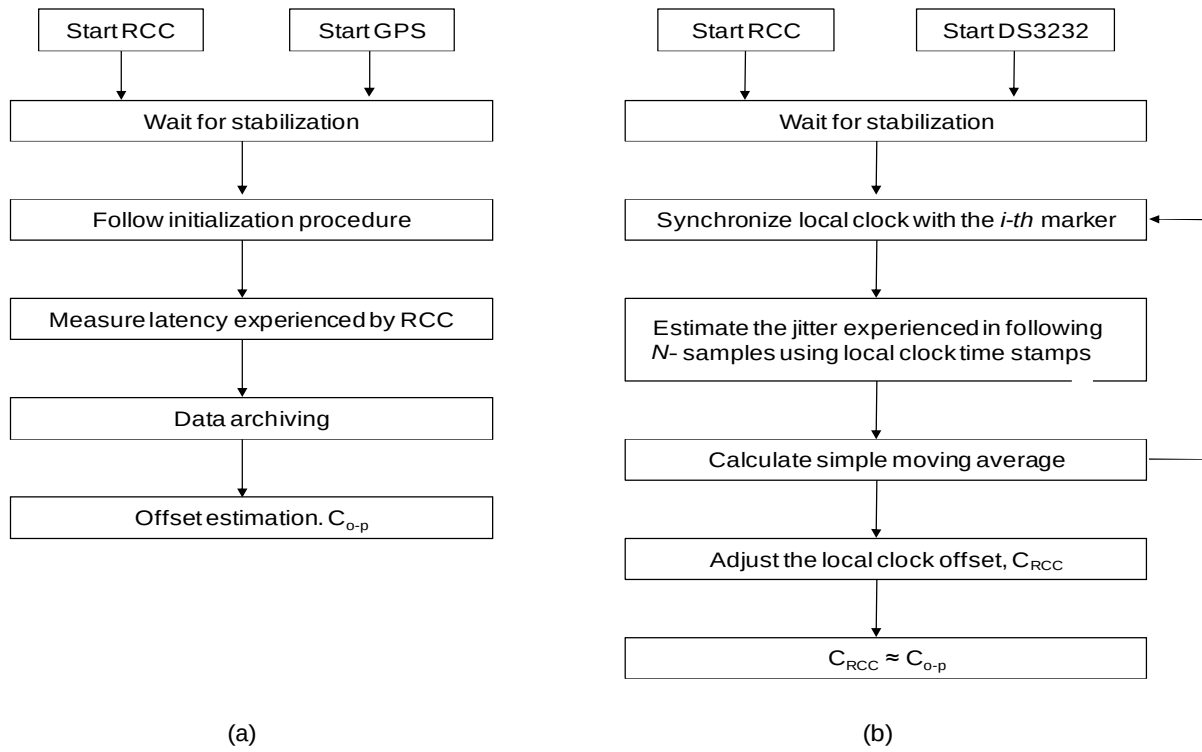


Figure 4.23. Flow chart of time synchronization (a) off-line stage, (b) on-line stage.

To define the clock characteristics the following nomenclature is used, which is in line with those used by Sundararaman et al. (2005) and Bletsas (2005), and are summarized in Panel 4.1. A clock can be represented as a function $C_n(t)$ of the real-time t . Here, real-time represents the ongoing standard time. Therefore, it is a continuous function twice differentiable except on finite set of points where clock parameters suddenly change, it is represented by set P (Bletsas, 2001):

$$C_n(t): R \rightarrow R$$

$$t \in P \subseteq R$$

here, $\|P\|$ is finite.

For a clock whose time is equal to the real time, it is referred to as a perfect clock given in Equation 4.9 (Sundararaman et al., 2005). It specifies that an ideal clock is theoretically a linear function of time where $\|P\| = 0$ (Blestas, 2001).

$$C_n(t) = t \quad \text{Equation 4.9}$$

Physical clocks however exhibit a deviation from this ideal behavior, and each clock can be represented by piecewise continuous function of time which gets incremented based

on crystal oscillations (Sundararaman *et al.*, 2005). Thermodynamic fluctuations, supply voltage, and aging are amongst the causes of the deviation in crystal oscillator frequency (Blestas, 2001). Therefore the clock function can be represented by Equation 4.10. The function shows that the clock output depends on the frequency of crystal oscillator which changes over time and depends on other factors like environment, and so can be represented as a summation of integral of frequency of clock oscillator (Wu, 2011).

$$C_n(t_s) = t_{0s} + \int_{s_0}^{s_1} C_n' dt + \int_{s_1}^{s_2} C_n' dt + \dots + \int_{s_n}^{t_s} C_n' dt \quad \text{Equation 4.10}$$

$$\text{where } s_0 < s_1 < s_2 < \dots < t_s.$$

Here, t_{0s} is the initial time of the clock when true time is s_0 . It emphasizes that the time which has passed according to the local clock depends on the frequency of the clock.

The time in hardware clocks is usually the value of counter which counts intervals of ideally fixed length duration. Therefore, a time duration measured by a clock, $C_n(t)$, in relation to true time is given by Equation 4.11 (Moon *et al.*, 1999).

$$C_n(t_2) - C_n(t_1) \equiv \int_{t_1}^{t_2} C_n' dt$$

$$C_n(t_2) - C_n(t_1) = \int_{t_1}^{p_1} C_n' dt + \int_{p_1}^{p_2} C_n' dt + \dots + \int_{p_n}^{t_2} C_n' dt \quad \text{Equation 4.11}$$

where, $P_a \cap (t_1, t_2) = \{p_1, p_2, \dots, p_n\}$ and $t_1 < p_1 < p_2 < \dots < p_n < t_2$.

In short, the time reported by a clock, and also the time interval recorded by a clock varies from clock to clock. The frequency accuracy of the reference oscillator and its stability governs the performance of a clock. The piecewise nature of the clock function captures these changes. Various behaviors are associated with the clocks, such as bounded-drift model, which states that the drift in frequency is bounded. When it comes to measuring the time duration, the behavior of the timing clock must be understood. Later on during the on-line stage assumptions will be made regarding the behavior of the reference local clock which is used to measure time intervals between the OTM.

An ideal radio clock earlier can be represented as a clock with a constant offset, as in Equation 4.12. The reason for constant offset $C_{0-t}(t_{tt}, x_t, t_r)$ is due to the factors such as use of broadcast medium and others discussed in Section 4.3.1.

$$C_{RCC-t}(t) \approx t - C_{0-t}(t_{tt}, x_t, t_r) \quad \text{Equation 4.12}$$

Here,

t_{tt} : Time from data generation to transmission. It includes send time and access time.

x_t : The propagation distance travelled by the signal.

t_r : Receive time at the receiver and includes the length of period starting from the instance when the MSF signal is received till the time of processing the signal. It depends on the receiver module, and is, therefore, hardware dependent.

The experimental results reported above can be used to model the actual behavior of the radio clock, which can be approximated by Equation 4.13.

$$C_{RCC-p}(t) \approx t - C_{0-p}(t_{tt}, x_t, t_r) + R(x_t, t_r) \quad \text{Equation 4.13}$$

Collectively, $C_{0-p}(t_{tt}, x_t, t_r)$ and $R(x_t, t_r)$ contribute towards the latency. The experimental results show that the clock offset is higher than what was expected based on the calculations presented in Section 4.2. It is evident from the recorded latency values presented in Figure 4.22. The cause for high offset was due to the receiver response time. Each radio clock has a different offset which can be estimated.

In addition, the clock experiences jitter, which is dependent on time and distance, and can be represented as measurement noise $R(x_t, t_r)$. Based on the observations, it has been found that the distance has an effect on the jitter, and a distance of more than 400 km caused a change in jitter value by 1.8 ms. The received signal strength, temperature, SNR and receiver sensitivity are not considered in the formulation above because they effect signal coverage and reliability, and have less impact on latency distribution within the coverage region.

Off-line stage

In order to increase the time synchronization accuracy of the radio clocks relative to the MSF signal, and also amongst the different radio clocks, it is necessary to estimate the values of $C_{0-p}(t_{tt}, x_t, t_r)$ for different radio clocks and also to minimize the jitter.

Figure 4.24 depicts the operation of a radio clock. The data is broadcast continuously by the source $C_{MSF}(t)$, with distinct pattern at the start of every new second, being referred to as on-time markers. The edges of these on time markers are controlled by the source,

and kept within a limit as specified in NPL (2007). These markers which occur at discrete instances are denoted by t_k , and are observed by the radio clock at a later time. On the arrival of these markers, time stamps are generated using the local clock $C_n(t)$. The local clock may have a clock offset while time stamping markers.

The difference between on-time markers being generated is known, and can be represented as:

$$t_{k-2} - t_{k-1} = t_{k-1} - t_k = \Delta T$$

$$k \in [1 \dots M]$$

Ideally, at the receiver side,

$$C_n(t_k) + l_k - C_n(t_{k-1}) - l_{k-1} = \Delta T$$

$$C_n(t_{k-1}) + l_{k-1} - C_n(t_{k-2}) - l_{k-2} = \Delta T$$

The experimentally obtained results highlight that the signal experiences jitter, and therefore l_k (i.e. the latency corresponding to on-time marker sent at time instance, k) varies. With this formulation a Kalman filter can be applied to estimate the expected latency and the variation can be modeled as a measurement noise.

As the latency is not meant to change from step to step, and there is no control input so the state model can be simplified to:

$$x_k = x_{k-1} + w_k \quad \text{Equation 4.14}$$

Similarly, as the noisy measurements are of the state directly measured using GPS as a reference, therefore $H=1$. The measurement model is simplified to:

$$z_k = x_k + v_k \quad \text{Equation 4.15}$$

The standard time and measurement update equations are omitted here, which can be found in Kay (1993). The measurement noise depends on the location and was reported earlier. Applying this Kalman filter to the data presented in Section 4.3.2 results in Figure 4.25. Panel (a) represents the Kalman filter output for experimental data collected in London and (b) for experimental data collected in Whitehaven.

The latency value at which the Kalman filter estimation settles is approximately 17.603 ms in case of Figure 4.25(a), and it is 16.077 ms in case of Figure 4.25(b). These results are in line with the analysis presented before, where the difference was identified to be linked to propagation time. Therefore, by applying the filtering for each

device a value can be estimated which is its expected offset at the time of arrival of on-time marker to that of the real time. It will vary from device to device due to hardware variations and also depends on location, but is expected to remain constant for the same device within same location. Therefore, for each radio clock an estimation of the expected clock offset can be computed and stored on a device, which can be represented by Equation 4.16.

$$C_{0-p}(t_{tt}, x_t, t_r) = \theta_{0-p} + \left(\frac{d}{c}\right) \quad \text{Equation 4.16}$$

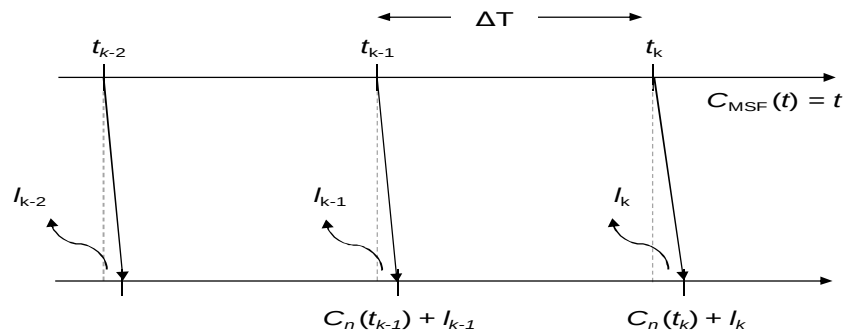


Figure 4.24. Transmission and reception of the on-time markers.

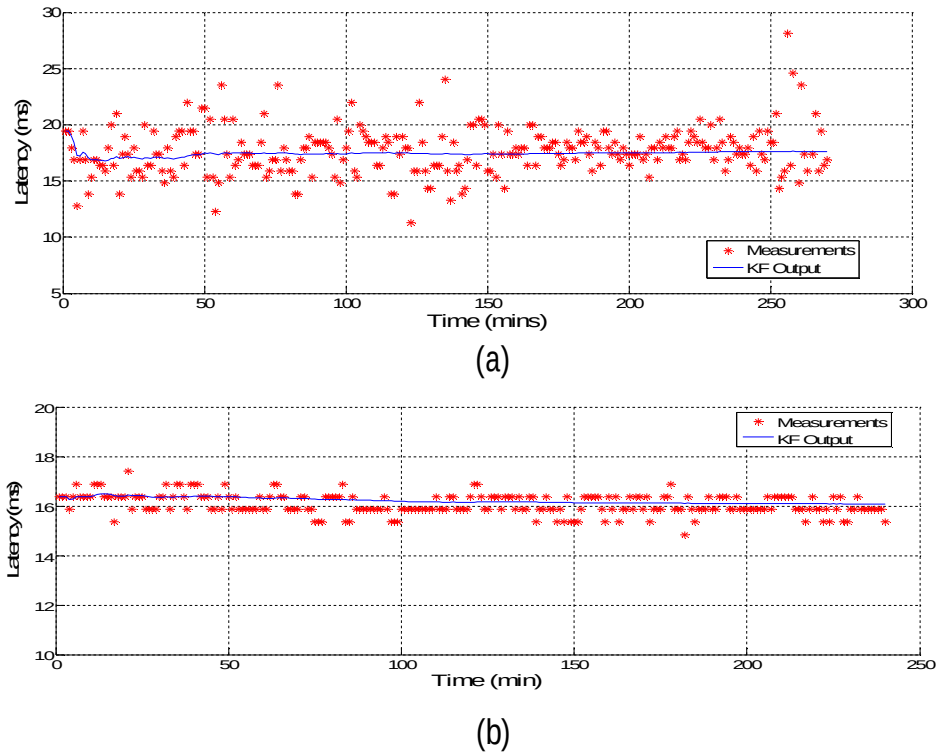


Figure 4.25. Kalman filter output of latency value for RCCv1 for (a) experiment conducted in London, (b) for experiment conducted in Whitehaven.

where $(\frac{d}{c})$ represents the variation in offset due to displacement, d , of the node from its original place of offset estimation, and c is the speed of light. This value can be computed and compensated for. If the system is operated in the same location where the calibration was done then because the displacement is zero the $(\frac{d}{c})$ will remain zero, therefore it will result in $C_{0-p}(t_{tt}, x_t, t_r) = \theta_{0-p}$.

On-line stage

The problem of an offset which is constant for one clock but varying between clocks has been addressed. However, to increase the time synchronization accuracy the jitter has to be addressed as well. It is proposed to use a sequence of SoF markers rather than one SoF marker. Jitter can be addressed by taking a Simple Moving Average (SMA) of the consecutive time markers such as of SoF.

In order to use SMA, it is critical to estimate the variation in latency experience by the radio clock. The data reported above was recorded using GPS as a reference signal which has accuracy better than a microsecond. However, in real deployment the GPS reference is not present and is therefore difficult to accurately record jitter. Using a local inbuilt oscillator as a scale to calculate the variation in latency will itself introduce errors. However, this value can be kept within a limit. To utilize this as a primary timing reference in a wireless field device, and assuming that the clock has a constant skew δ , then it is represented by Equation 4.17 (Ridoux *et al.*, 2010).

$$C_n(t) = C_o + (1 + \delta)t \quad \text{Equation 4.17}$$

The value of skew is bounded and the clock is allowed to diverge in the range specified by the manufacturer. With reference to the ideal clock it can be represented by Equation 4.18 (Sundararaman *et al.*, 2005), where ρ is the maximum skew.

$$1 - \rho \leq C_n'(t) \leq 1 + \rho \quad \text{Equation 4.18}$$

The SMA is calculated using Equation 4.19. Here, the selection of N depends on the duration of radio clock operation $t_{\text{operation}}$ in minutes, skew δ , and energy budget. Only the first two parameters are taken into consideration in the following calculations. The calculations are based on 60 second minute frame and also on SoF markers.

$$SMA_k = \sum_{i=0}^{N-1} \frac{l_{k-i}}{N} \quad \text{Equation 4.19}$$

Therefore, over a period of time the skew of the local reference clock would itself cause an error in the estimated value of the jitter, based on Equation 4.11. The error which it is allowed to induce is linked to the selection of the number of samples used in the SMA calculation. The error in the time scale induced by the local oscillator is given by Equation 4.20 (Eidson, 2006).

$$x(t) = x_0 + y_0 t + \frac{D}{2} t^2 + \frac{\phi(t)}{2\pi f_{nom}} \quad \text{Equation 4.20}$$

Here,

x_0 : Represents the offset at the origin of the time scale.

y_0 : Fractional frequency offset.

D : Represents linear fractional frequency drift. It represents environmental and inherent effects.

$\phi(t)$: The random phase deviation of the measured oscillator.

f_{nom} : The nominal frequency of the oscillator.

A high precision oscillator such as a TCXO compensates for environmental and aging influences. Therefore, it is assumed that the local reference oscillator behaves as a clock with constant offset and the last two terms in the above equation are ignored. For such a reference scale, the time error, $x(t_{operation})$, which it can accumulate over a given period of time is given by Equation 4.21.

$$x(t_{operation}) = 60000(\delta/10^6)t_{operation} \quad \text{Equation 4.21}$$

To take into consideration the skew and the operational time, N can be calculated using Equation 4.22, given that: $\frac{x(t_{operation})}{\delta} \geq 0.06$.

$$N = \lfloor t_{operation} \rfloor \quad \text{Equation 4.22}$$

where,

$$t_{operation} = \left\lceil \left(\frac{\varepsilon}{60000} \right) \left(\frac{10^6}{\delta} \right) \right\rceil$$

In order to demonstrate the effect of skew, the use of the in built oscillator on a mote oscillator can be used. The oscillator found in motes often has an accuracy of 30 PPM (Sommer et al. 2009).

The plot shown in Figure 4.26(a) represents three distinct results. One of them shows the outcome of moving average using GPS as a reference after synchronization and the others use a local oscillator with ± 30 PPM accuracy for reference. It can be seen from Figure 4.26(a) that even by eliminating the offset at the start, the error introduced by the local oscillator is high and is not a good option for recording jitter.

Using a TCXO like DS3232 on the other hand offers a better solution as demonstrated in Figure 4.26(b). It can be seen that even by utilizing a reference signal from a constant skew clock, the difference between the actual reading and the ones recorded by utilizing ± 2 PPM oscillator can be approximated to be same for a longer interval. The maximum error induced by a constant skew clock is less than a millisecond for intervals of up to 8 minutes.

This method addresses the volatility in the value of jitter, and the value estimated will be within the given bounds of actual SMA, which is governed by the maximum allowable reference error. The output achieved via SMA can then be approximated to be equivalent to $C_{0-p}(t_{tt}, x_t, t_r)$. Hence, as a result each device will have an estimate of its own expected offset and will compensate for it resulting in better time synchronization accuracy.

Applying this proposed algorithm to the latency data collected from the operation of the radio clocks, RCCv1 and RCCv2, in Whitehaven results in improved time synchronization accuracy as shown in Figure 4.27. The figure shows a cumulative distribution plot of the time synchronization error as calculated between these two clocks. The results highlight that time synchronization accuracy between these clocks, based on 90th percentile is better than a millisecond, as calculated from the latency data collected for over four hours of continuous operation. Compared to earlier presented data shown in Figure 4.15, the minimum time synchronization error was 5.4 ms. In the case of this proposed algorithm, the maximum time synchronization error is itself a fractional of that value. A significant contribution towards this accuracy improvement is due to the elimination of constant offset, which is linked to each individual radio clock.

To summarize, the proposed two stage algorithm described earlier enables the radio clocks to minimize the discrepancy as found between theory and practice. Also, it addresses the issue of hardware mismatch between different radio clocks. It is achieved by formulating the time synchronization error accuracy issue as a calibration issue. The volatility in the recorded latency, which is the other part which contributes to time synchronization error, is minimized by taking an average of the jitter experienced over a defined period of time. In the latter mentioned case, it exploits the short term accuracy of the crystal oscillators.

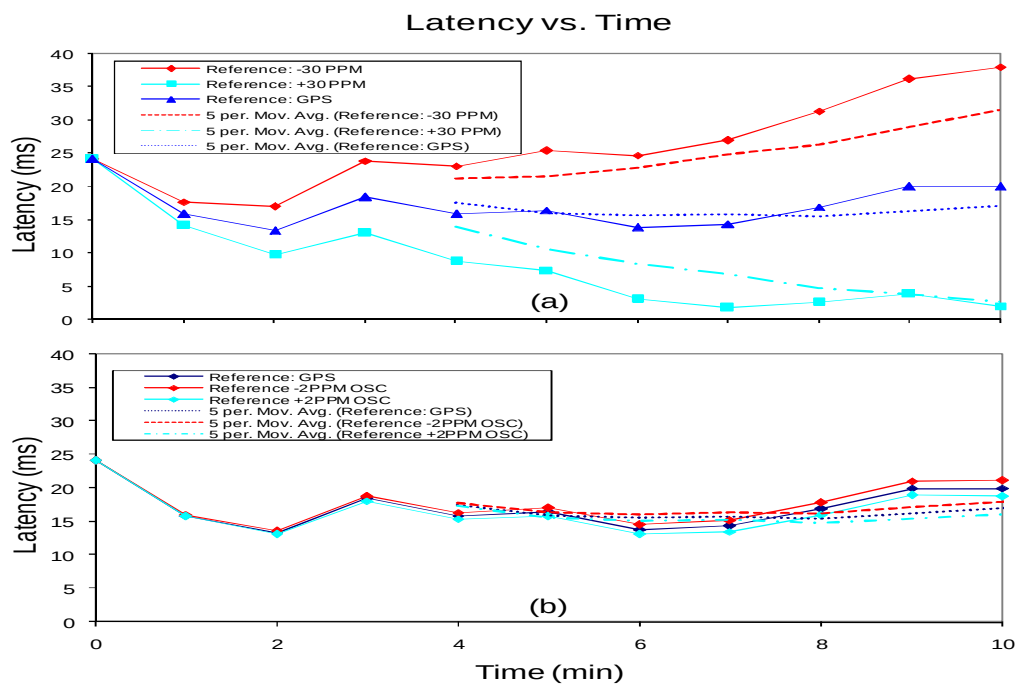


Figure 4.26. Latency versus time plot (a) for ± 30 PPM and (b) for ± 2 PPM oscillator.

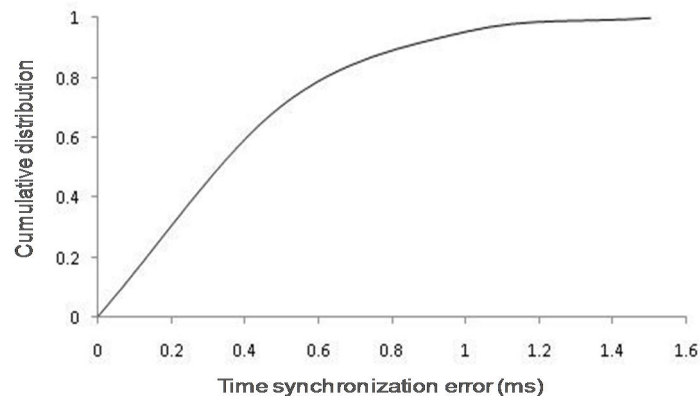


Figure 4.27. Time synchronization accuracy as a result of the proposed algorithm.

4.5. Procedure for Time Synchronization of a Field Node

The procedure for time synchronization of a field node to an incoming MSF signal is summarized in Figure 4.28. The figure highlights the two stages which are involved in time synchronization process and the various inputs which are required from the user during this process. The description of each stage is as follows:

Calibration

- LATENCY DISTRIBUTION:

The process starts by recording the latency as experienced in the detection of the OTM. The use of GPS clock which outputs a pulse per second aligned to the UTC is used as a reference to record the latency in OTM reported by the MSF receiver. Either SoF or a second marker can be used to record the latency. Therefore, the latency samples are taken once every T_s seconds, and is within the range:

$$1 \leq T_s \leq T_{max}$$

where, T_{max} depends on the minute frame. If the second marker is used to record the latency then $T_s=1s$, whereas, if SoF is used then $T_s = 60s$. It is assumed that the MSF minute frame comprises of 60 seconds. The number of samples, X_i , required depends on the sampling rate and the time window used to characterize latency distribution. The minimum samples required are based on the normalized KLD value reported earlier.

- KALMAN FILTER:

The latency distribution as recorded is used as part of the Kalman filter model. The output of the Kalman filter is used to estimate the clock offset, θ o-p. This is the value at which the Kalman filter output stabilizes, and is specific to the geographic location where the calibration is conducted.

- USER INPUT:

In order to time synchronize any field node to an incoming MSF signal various user inputs are required. These inputs are required once at the beginning and are used by the algorithm to adapt to the application requirement. They are as follows:

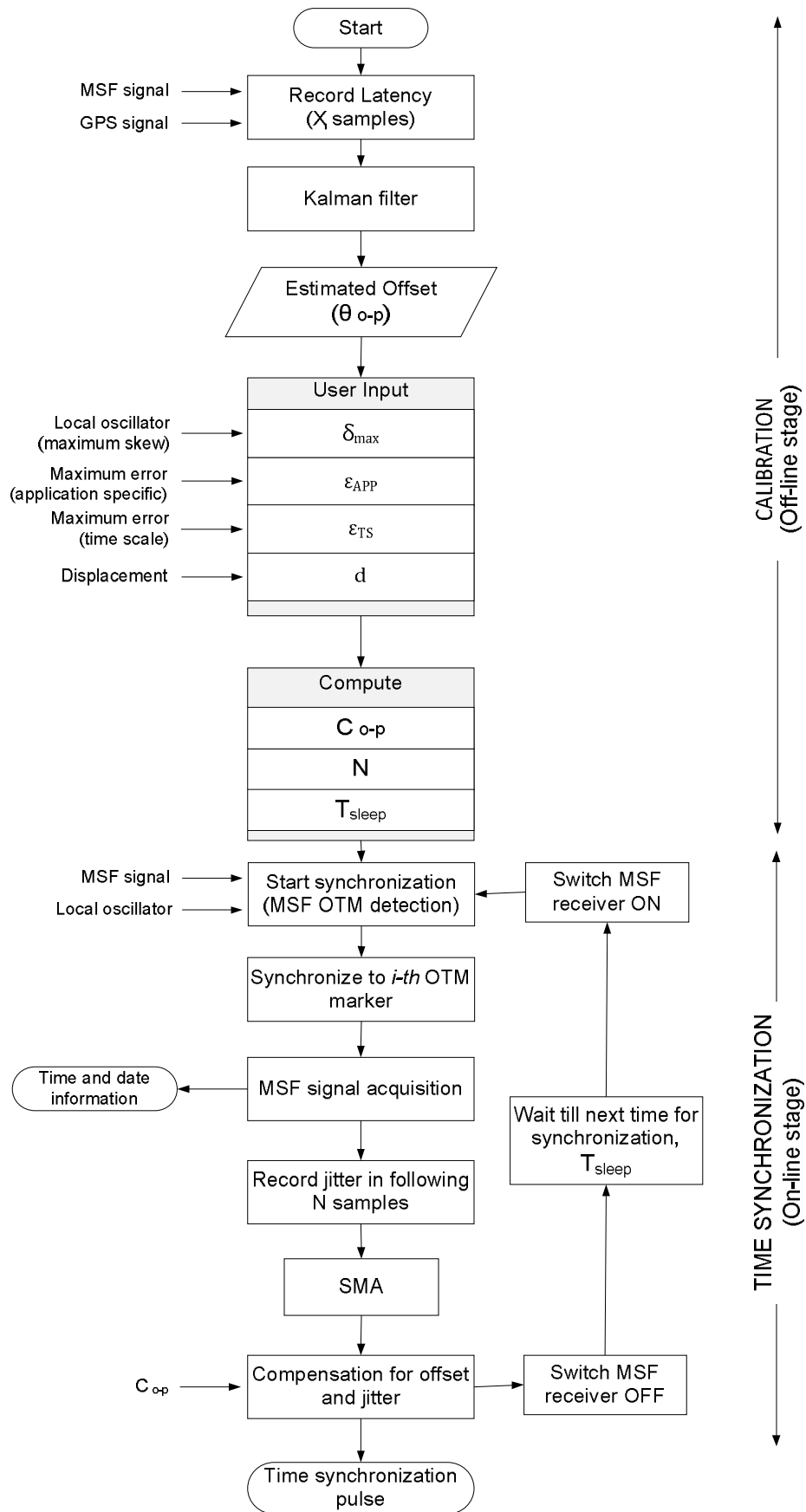


Figure 4.28. Block diagram for time synchronization procedure.

$\delta_{\max}$: Maximum allowed skew of the local reference oscillator. The local oscillator is used as a timing source in between time synchronization, and its skew will result in an offset which is accumulated over a period of time. Local oscillator will also be used to calculate the jitter during on-line stage.

ϵ_{APP} : Maximum allowed time error between synchronization intervals.

ϵ_{TS} : Maximum allowed time scale error introduced by the reference oscillator during jitter estimation.

d : Displacement of the MSF clock from its initial location of calibration.

▪ **COMPUTE:**

Based on the inputs provided by the user the following values are computed.

C_{o-p} : The estimated clock offset at its venue of deployment. It introduces a bias to the initial estimated value of the clock offset, θ_{o-p} , by taking into consideration the displacement of the clock from its initial point of calibration.

N : It calculates the number of jitter samples which can be used in SMA calculation before the time scale error exceeds the specified maximum value.

T_{sleep} : The time span for which the MSF receiver can be switched off. In between synchronization intervals, MSF receiver can be switched off to conserve the onboard battery.

Up to this point, all the above mentioned user inputs and the computed values will be stored in the field node. The information will be used by the proposed on-line algorithm to improve time synchronization accuracy of the radio clock with the incoming MSF signal. This calibration is required once at the beginning or every time when the user overwrites the input values provided earlier. It is so because the later stage, on-line stage uses those values to orchestrate the procedure.

Time synchronization during operation:

- **START SYNCHRONIZATION PROCESS:**
During operation in the field, the procedures followed by the field nodes to time synchronize themselves involve the use of the MSF receiver and the local oscillator. OTM in the MSF signal is identified and the local oscillator is aligned to the OTM which is specified by the user. The local oscillator is aligned to one of the selected OTM.
- **MSF SIGNAL TIME AND DATE INFORMATION:**
The entire minute frame of the MSF signal is then acquired, decoded and the time and date code information conveyed to the host application.
- **JITTER RECORDING AND SMA:**
After the synchronization of the local oscillator with the i -th OTM marker, the jitter is recorded in the value of following N samples of OTM. This information is used along with SMA to estimate average and RMS jitter. The maximum numbers of samples which can be used in this calculation are linked to the maximum allowed time scale error, ϵ_{TS} .
- **COMPENSATION AND SYNCHRONIZATION PULSE:**
After the accumulation of N samples of jitter. This information along with the earlier defined estimated clock offset, Co_p , can be used to compensate for the sources of time synchronization errors at the time of calculation of N^{th} sample of jitter. At this instance, a pulse can be generated which has better accuracy relative to UTC. It is because of the elimination of constant clock offset, and minimization of effect of jitter.
- **TIME TO SLEEP:**
Once the synchronization pulse is generated, the MSF receiver can be switched off. This is done so in order to conserve the on board battery. The time, T_{sleep} , for which the device can be switched off depends on δ_{max} , ϵ_{APP} and recorded RMS of jitter. After the elapse of T_{sleep} the MSF receiver is switched on and the same procedure is repeated. This periodic time synchronization process will help keep the time accuracy at the field node bounded within a range specified by the ϵ_{APP} .

4.6. Radio Clocks in Challenging Environments

This section will highlight the practical issues associated with the use of radio clock receivers and also on identifying means to address those issues.

Practical insights

Based on the experience of operating radio clocks in various environments, it was found that there were difficulties receiving the MSF signal in some locations. The signal experiences higher attenuation due to location of the radio clocks inside a building, close to power lines, or other large metal structures. The other issues which have been reported by NPL (2010a) are related to the background interference from sources such as an electric motor, fluorescent tube, computer or TV which can degrade the time signal quality if operated within close proximity. An approximate distance of more than a meter is required to counteract the effect of these interferences. The use of an active antenna can enhance this range.

The reliability test carried on the radio clocks reveals a general trend that the signal has a good reception at the night time. The SoF marker is a unique pattern and is detected very reliably. The bit durations do vary, and is not exactly 100 ms, and it is due to the receiver design. The problem in reception within coverage area is often linked to nearby noise source. The signal, if it experiences erroneous bits, recovers itself within few minutes.

Rebroadcasting

For applications where the MSF clock has to be located well inside an enclosed environment or it has to be co-habitated with an external interference source then the MSF signal can be rebroadcasted. Multiple such options exist, and they include:

- IN-BAND REBROADCASTING

The products such as TSG100 from C-MAX can be used to rebroadcast the MSF signal. It offers a coverage region of up to 50 m radius. For further information refer to (C-MAX, 2012).

- OUT-OF-BAND REBROADCASTING

Another option is to rebroadcast the time signal out-of-band to the LF signal. One

such example is the work from Rowe *et al.* (2008). These researchers used AM transmitter to locally rebroadcast the atomic time signals from WWVB transmitter in the US. The system developed by them does not decode the entire time frame, and only detects the rising edges associated with the WWVB signal. They used building's power grid as the antenna for broadcasting time synchronization pulse. The carrier current signal radiation was limited to within 50 meters of the building's structure.

Another example would be of rebroadcasting the time signal within 2.4 GHz ISM band. It is a band of choice for WSNs. The time signal can be rebroadcast at regular intervals, and a maximum PHY packet size supported by the IEEE 802.15.4 standard is 127 octets (IEEE802.15.4, 2006). The rebroadcast signal will have a constant offset with the UTC seconds for restricted hops. These retransmission packets will allow the devices to synchronize within milliseconds, as the devices do not have to listen for the entire minute frame. A 127 byte packet would take 4.064 ms to transmit. Furthermore, as the latency of such transmission will be constant, it can be compensated. In this case, due to the restrictions on the emission levels in 2.4GHz ISM band, a maximum transmission power available for transmission is often 10 dBm. Based on this transmission and a sensitivity of -104 dBm available in modules like Atmel (2009), it offers a link budget of 114 dB. As a result, it will help to considerably enhance the performance of MSF clock in indoors and challenging environments. The use of channels 15, 16, 21 and 22 are often a good choice for IEEE802.15.4 networks. Moreover, spread spectrum techniques like FHSS can be incorporated to avoid jamming and to ensure coexistence.

Various issues can limit the operation of a radio clock when located within an enclosed space or close to an interference source. For such installations, a time signal rebroadcasting would be advantageous to boost the signal quality. Such rebroadcasting equipments are commercially available.

4.6.1 Illustrative Example: Practical Deployment

In this section, a use case is presented where the system designed earlier has been deployed and tested. The monitoring capabilities with accurate time stamps when

integrated with novel computing techniques such as time and frequency domain methods, system identification, filtering, prediction, optimization and control creates complex cyber-physical systems. Such cyber-physical systems encompass the management of both large scale sparse networks. The water industry is one such field where the above designed time synchronization solution is of significant importance.

As part of the research presented in this chapter, the hardware developed was deployed as part of water pipeline infrastructure monitoring system. The idea is to use MSF driven radio clocks to time synchronize data loggers and WSNs used for pressure level monitoring. Currently, the use of pressure sensors is employed to monitor the pressure levels in range of 3-7 bars. Any deviation in the expected value will help to identify the abnormality. However, the existing deployments suffer from time synchronization problem because of the challenges associated with regularly time synchronizing distributed data loggers. The operating environment in a fire hydrant is very difficult, in addition to design, and fixed locations challenges, which further impose limitations.

Figure 4.29 shows the snapshot of various fire hydrants as found in England, and also the two locations where the RCCv1 was deployed. The RCCv1 was operated independently and it was seen that the radio clock was able to time synchronize without any extra effort. The coverage of the system was good enough to synchronize to the MSF signal, despite being enclosed inside a reinforced concrete chamber with a metal cover. This deployment was conducted within the premises of South Kensington campus of Imperial College London.

The result of the experiment conducted over a period of half an hour is summarized in Figure 4.30. It can be seen that the offset and jitter experience is within the same bounds as was previously presented in Figure 4.25(a). The cumulative probability plot of the time synchronization error is shown in Figure 4.31. These results are based on the readings recorded from the RCCv1. GPS was used here as a reference signal. Therefore, this recorded latency can be regarded as time synchronization error relative to the UTC. Time synchronization error has been found to be in order of tens of milliseconds. To reduce this time synchronization error the proposed algorithm with both the on-line and off-line stages was used. The results obtained are shown on the

same figure and shows a significant improvement in time synchronization accuracy. The minimum error reported without the use of proposed algorithm in both FH1 and FH2 deployments was above 10 ms, whereas, after processing the data based on the proposed algorithm the maximum synchronization error in case of FH1 was 4.5 ms and in the case of FH2 was 3.5 ms. Moreover, the 90th percentile reveals that without the use of the proposed algorithm the time synchronization error was 20 ms, whereas, after utilizing the proposed algorithm it was below 4 ms. The results shown here are based on moving average of five consecutive data samples.

The conclusions which can be drawn from these deployments are as follows:

- The MSF clock can operate in an underground environment as demonstrated through successful deployments in fire hydrants. This implies that MSF signal penetrates buildings and underground utility services close to the surface and no line-of-sight is necessary between the transmitter and receiver for the radio clock to work.
- The deployment was conducted for more than half an hour and in between all the SoF markers were successfully received.
- The latency recorded in field trials is in line with what was reported earlier in lab experiments.
- The proposed two-stage algorithm proved to be effective in increasing time accuracy relative to GPS, which in effect is time synchronization relative to UTC.
- It is an energy-efficient, low-cost and practical time synchronization solution for wireless telemetry units.

To summarize, the use of radio clocks with data loggers offers a considerable improvement in monitoring the water infrastructure compared to existing systems. The aggregated data collected from spatially distributed pipeline infrastructure with global time synchronization will assist in fault diagnostics and in maintenance. The deployment has been demonstrated to be energy-efficient (Section 4.3.1). It is also low-cost because it uses an MSF clock receiver rather than GPS, and the field deployment has shown it practically.



Figure 4.29. (a) An outside view of a fire hydrant with a metal cover, (b)-(d) inside view of typical fire hydrants with monitoring equipments. (e-f) deployment sites for conducting field-trials, referred to as FH1 and FH2 respectively. Photographs are courtesy of Dr. Ivan Stoianov and Asher Hoskins from Civil Engineering Department at Imperial College London.

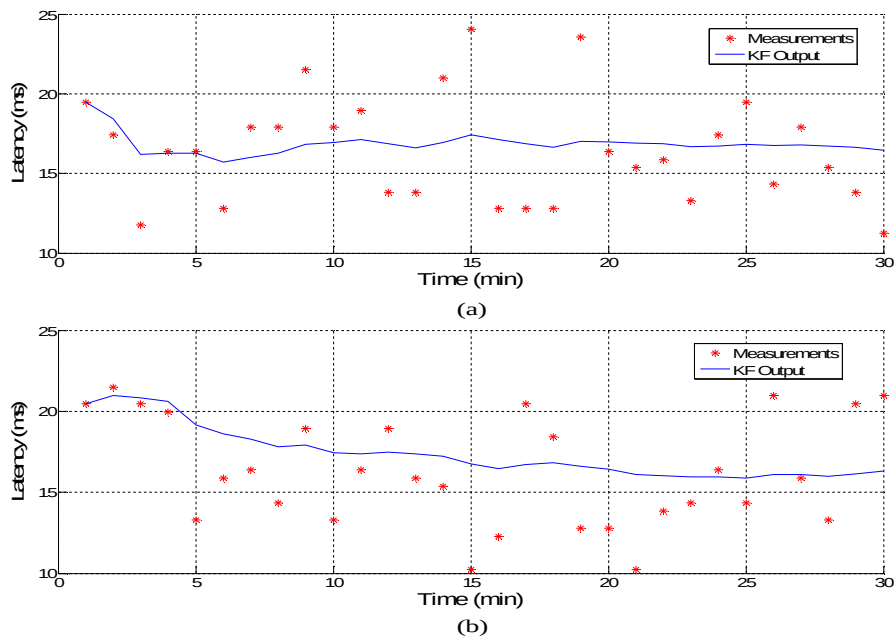


Figure 4.30. Latency versus time plot for deployment in (a) FH1 and (b) FH2.

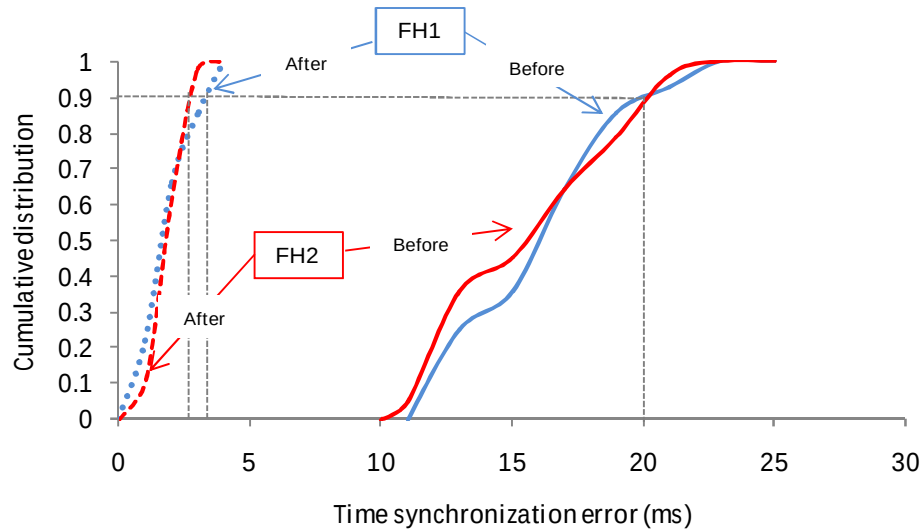


Figure 4.31. Time synchronization error relative to GPS for RCCv1 deployment in (a) FH1, and (b) in FH2. Time synchronization accuracy as a result of the proposed algorithm, (c) in case of FH1 and (d) for FH2. *Before* represents the time accuracy using MSF receivers only without any processing, and *after* represents time accuracy post processing of receiver output using the proposed methodology (including on-line and off-line stages).

4.6. Chapter Summary

This chapter has presented an approach to time synchronize distributed wireless systems. It is needed as it is essential for network applications as well as for the formulation of wireless network itself. The proposed approach of network-wide time synchronization is based on the use of radio controlled clocks. This approach helps to eliminate and minimize three sources of time synchronization error introduced in normal sender-receiver synchronization systems, namely the send time, access time and propagation time. These errors remain between the sender and receiver, but amongst the receivers themselves, they are cancelled out. The network, hence, becomes susceptible merely to receiver related error.

This hardware-assisted time synchronization approach has been analyzed theoretically and also practically, with results shown to be in agreement. The results have highlighted that it offers a better solution for time synchronization especially in terms of energy consumption, cost, compactness and coverage. The long term independent and continuous operation of the built version of the radio clocks highlight that the MSF time signal is reliable and stable. The use of radio clocks has been wide spread in commerce for decades. However, the commercial applications can tolerate poorer accuracy than

process applications. Therefore, this chapter has focused on the achievable levels of time synchronization accuracy by using MSF clock in particular. The approach has been to use the existing commercially available receivers and enhance their capability using either physical modification or software based processing on the received signal. The experimental results have revealed that the system is subjected to jitter, which varies with distance from transmitter and affects the time synchronization accuracy. A novel approach to address the problems linked to hardware variations and volatility in recorded latency has been proposed. It involves the use of Kalman filter, high-precision local oscillator and signal processing. The algorithm is based on the findings of both the theoretical and empirical studies. A Kalman filter is employed to address the measurement and process noise issues. It formulates this time synchronization accuracy issue partly as a calibration issue, which deals with the hardware mismatch. This process was referred to as off-line stage. The other issue was linked to jitter and is addressed by using simple moving average and by relying on the short-term precision of the quartz crystal oscillator. This process is referred to as an on-line stage. Therefore, collectively these two stages can improve the time synchronization accuracy of radio clocks. Laboratory experiments and field trials have shown that this method is effective in order to increase the time synchronization accuracy.

To conclude, the hardware-assisted time synchronization approach is independent of network-size, and, hence, is scalable. It is also topology-independent synchronization solution, as it does not matter whether the network is single-hop based star connection or multi-hop mesh network, as all devices can be synchronized concurrently.

CHAPTER 5

Studies on Performance of a Control Application Operating over a Wireless Network

Information gathering from the field devices either for the purpose of closed loop control or even for event logging has an associated timing requirement. In some cases, the timeliness of information is highly important (such as in control applications) and the late delivery of data may compromise the process system operation. This chapter will examine the efficient use of wireless technology for addressing the requirements of control applications. No particular industrial standard or industrial controller will be used in this chapter and the proposed mechanisms to improve the control system performance will be applicable to any IEEE 802.15.4 network. Hence, this chapter focuses on the requirements of process control applications which have an impact on wireless network design and configuration. These requirements can help to govern the design of a wireless network for ensuring the required quality of service. Wireless technology and its adoption in process industries at the field level for control is the theme of this chapter and relatively a new trend which requires an understanding of the trade-off between control and wireless communication fields.

5.1. Overview

This section will first introduce the NCSs and later their wireless counterpart the WNCSSs. This section will further highlight the absolute theoretical limits of the selected IEEE 802.15.4 network and how they affect the control loop system. Furthermore, the current practices in the process industry are highlighted and the practical issues linked to Wireless Sensors and Actuator Networks (WSANs) have been presented. These are

vital to be understood in order to run a control loop application over a wireless network.

5.1.1. NCSs

In a NCS, the control loops are closed over a shared real-time communication network. If the network is to be wireless, then feedback control mandates the need for a reliable, secure and deterministic network operation. Deployment of a wireless network for running multiple closed loop control requires examination of both the application demand and the services which are expected from the wireless network and its capacity. Further requirements from a network for process control application include availability of accurate information in real time, wider network coverage, secure network, scalable solution and sufficient bandwidth. In a traditional wired communication network, sensors provide data to controllers in a periodic manner. The controllers then compute the controller output based on the information received from sensors. The sensor must measure, and the controller must update the controller output at least as fast as the process response time. Therefore, as the controller output works on the process variable value the control loop execution depends on process type which specifies as to how often the loop should be updated. Figure 5.1 shows an illustration of a closed loop control operating over a wireless mesh network.

The performance of the control loop will depend on the operation of individual components, their interaction and cooperation. The Figure 5.1 depicts two distinct communication links, one from the sensor to the controller and the other from the controller to the actuator. The paths shown with arrows highlight the possible data flow trace while closing the loop. Here, it is assumed that both the sensing and actuation is done over a wireless network. These wireless networks can be associated to the same or different access points (sink nodes). Furthermore, the figure also provides a detailed description of various network induced delays which include communication delays (T_{SC} , T_{CA}) and processing delays (T_S , T_C , T_A).

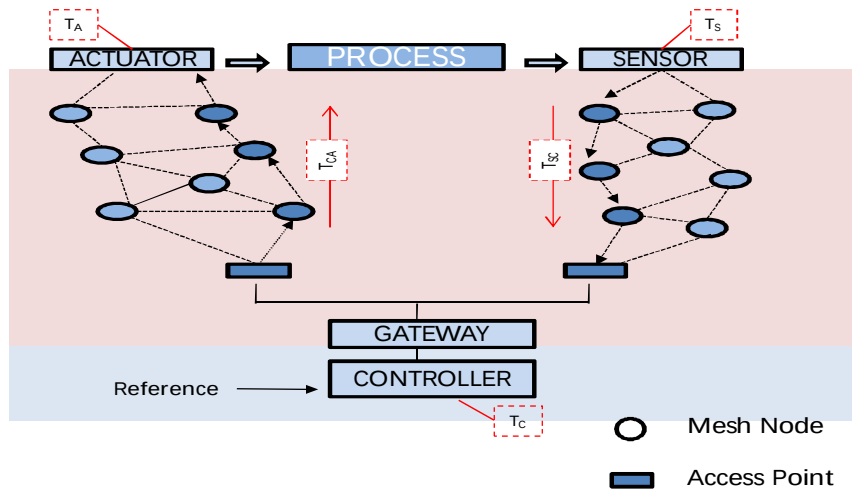


Figure 5.1. Closed loop control over a wireless mesh network.

Communication delays are delays related to getting the data transferred from the source to the destination node and processing delays are internal delays introduced by network nodes. Here, T_{SC} represents the delay associated with getting the data transferred from sensor to controller (where the control algorithm resides) and T_{CA} represents the delay incurred from control data generation at controller to its reception at the actuation. Within this process, the intermediate nodes and their associated time delays from reception to forwarding are all aggregated within the process of delay estimation. The greater the number of hops the more susceptible the communication path will be to communication delays. Hence, network topology, message scheduling, buffer size, MAC mechanism and error correction mechanism becomes critical. The processing delays (i.e. T_S – sensor processing delay, T_C – controller processing delay, and T_A – actuator processing delay) in relation to the communication delay are less constraining and can be dealt with. They are outside the scope of this research.

Network induced time delays can degrade system performance and can lead to process instability (Wang and Liu, 2008). Therefore, these network delays are to be minimized. In a short-range, low-power and license-exempt wireless network packet delays and packet losses are expected. A data retransmission or use of Forward Error Correction (FEC) can help address the issue but the process will itself incur delays. In short, the maximum allowed delay in data transport from source to destination is controlled by the physical process being governed and the controller execution rate. Despite the presence of such shortcomings the wireless network needs to be optimised in order to

deliver the required QoS. These challenges will be discussed in the following sub-sections and the study presented in this chapter will address some of the concerned issues.

5.1.2. Requirements and Challenges

A detailed requirements analysis was provided in Chapter 1 for the use of wireless in process automation. There, the focus was to cater for three types of data: periodic (i.e. control data), sporadic (i.e. alarm data) and non-real time data (i.e. network maintenance data). Here, the emphasis has been only on control data which is scheduled as a cyclic data.

Feedback control loops requirements, practices and considerations

- A general rule of thumb is that the feedback control loop should be executed four to ten times faster than the process response time. The process response time includes process time constant plus process deadtime and is shown in Figure 5.2, therefore communication delays are to be kept low (HCF, 2009).
- The process of data acquisition, execution of control algorithm, and dissemination and reception of actuation command has to be performed in half of the process time constant (HCF, 2009). It is because the measurement systems and control system are often unsynchronized. An important point to highlight is that if multiple loops with varying process response times operate over the same wireless network than the process with fastest dynamics will dominate the network design.
- In addition, ISA 100.11a has specified that the network reliability and availability are to be ensured for each application class and have defined six such classes. For instance, in Class 1 (which is a closed loop regulatory control class presented in Table 2.2) a network outage of more than 500 ms is unacceptable.
- In general, the scheduling of the algorithm in the controller becomes vital for control loop execution. For the industrial controllers such as AC800M from 800xA family of controllers from ABB the execution cycle begins by reading values of all sensors, and then computing the control signal values and writing

them to the output registers. Therefore, all the sensing values are to be made available before the control algorithm can be executed. It is a general practice as often cascaded control loops are used.

- The control systems are heavily regulated and one such requirement for certification is that the inter-node signals should reach the destination within a pre-defined time. This time is specified by the manufacturers.

To conclude, it can be stated that the wireless network must be able to support the required update rate which is not possible to be achieved without a certain capacity and supervision. In addition, the interaction between systems, interlinks, scheduling, network topology, control algorithm, control architecture and its implementation (including its scheduling) are important for successful control operation.

The current practices highlight the following challenges.

- THE SAMPLING RATE SELECTION FOR SENSORS:

The challenge is to find the longest sampling time that can achieve stability, and can consequently lower the network usage and increase lifetime of battery operated field devices. On one hand, the performance of a digital control system

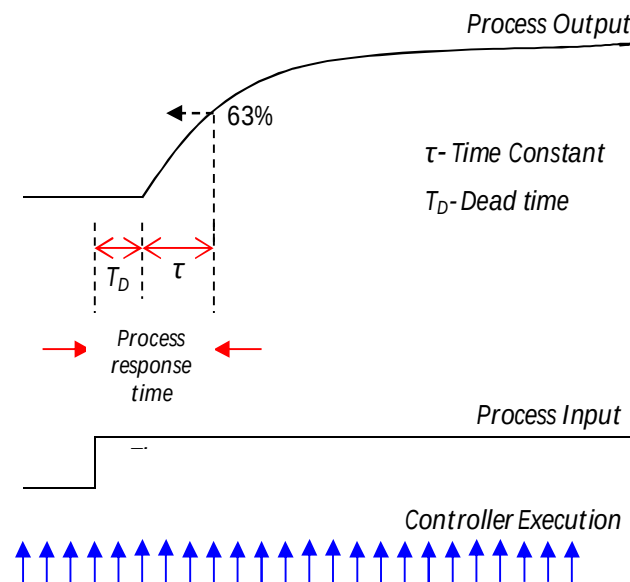


Figure 5.2. Process response of a first order plus time delay system from HCF (2009).

improves if operated at higher sampling rate, and decreases with low sampling rate (Jafari *et al.*, 2011). On the other hand, the higher sampling rate means an increase in traffic and shorter lifetime of battery operated devices. Therefore, choosing an optimal sampling rate is important.

- DEALING WITH DATA LOSS AND FAIL-SAFE OPERATION:

After a certain amount of continuous packet losses or denial of service, the loop is declared fail-safe and the operational values are set according to fail-safe configurations. Constant occurring of such events will keep bringing the control to manual mode. In addition to the cost of unnecessary shutdown, it causes the unnecessary wear-and-tear of equipment. It is therefore important to design a mechanism which can ensure smooth operation during connection outage and keeps it to the minimum level below to that which causes the intervention from integrated safety system.

- POWER CONSUMPTION (BATTERY OPERATED FIELD DEVICES):

The challenge here is to keep the battery consumption to minimum in order to increase network lifetime. It is quite similar to sampling rate selection discussed above but has some other factors to be considered as well. For instance, in industrial applications the sensing and communication are both high power consumers. Industrial sensors tend to have higher power consumption as compared to non-industrial sensors. Furthermore, power consumption is linked to sensors and their utilization, the device type (i.e. RFD or FFD) and the communication protocol it utilises. These issues need to be addressed or at least be considered during WNCS design and operation. Energy scavenging is an area of research which has seen acceleration in research activity during recent years to address this limitation.

- REAL-TIME COMMUNICATION:

This challenge is to ensure the safe delivery of data with a bounded delay. A network which supports various data types (e.g. periodic, sporadic and network message data) needs to prioritize data based on its criticality. Therefore, the scheduling of network channel access becomes vital. Moreover, dynamic scheduling polices can be utilized to enhance the performance as opposed to the

use of static scheduling policies. Within this arena, network-outages and co-existence need to be addressed.

Therefore, in order to design a wireless network which is deterministic and has limited latency, a time divided scheduling mechanism is often used by the devices to access the radio channel. In addition to this network sharing mechanism the communication delays are also kept to minimum by synchronizing the sampling time and on-air time. Furthermore, the process values can only be transmitted when it is necessary in order to conserve battery and reduce traffic.

5.1.3. IEEE 802.15.4 MAC and PHY limits

The IEEE 802.15.4 MAC supports two modes of operation, referred to as beacon-enabled and nonbeacon-enabled mode (IEEE 802.15.4, 2006). In the former case, the standard specifies the use of a superframe structure. The coordinator of a Personal Area Network (PAN) bounds the channel time using a superframe structure which is bounded by the transmission of beacon frames and is shown in Figure 5.3(a). It is the mode of choice for applications which require low latency. In the latter case, the PAN coordinator does not transmit any beacons. In this scenario, the communication is based on unslotted CSMA/CA. Beacon-enabled mode will be the focus of attention to the work presented in this chapter because nonbeacon-enabled network cannot meet the process automation requirements specified in Chapter 1.

An example of an IEEE 802.15.4 superframe structure is shown in Figure 5.3 (a). Here, it can be seen that in between beacon intervals the time is divided into two main segments: an active portion and an inactive portion. During the active portion, referred to as *Superframe Duration* (SD) in the standard, there are 16 equal sized time slots. The first segment of these slots which follow the beacon transmission is the Contention Access Period (CAP). In CAP the devices use slotted CSMA/CA to access the channel. On the other hand, during the Contention Free Period (CFP) the nodes which are assigned Guaranteed Time Slots (GTSs) by the PAN coordinator can access the channel without contention. A maximum of seven nodes can be allocated GTS according to the standard (IEEE 802.15.4, 2006). Haque (2012) proposes an algorithm for efficient utilisation of GTS by utilising the traffic arrival information of devices to allow sharing of GTS slots

between more than seven devices. Further, after the end of the CFP all devices are allowed to enter into sleep mode in order to conserve battery till the start of next superframe. During the assignment of GTs a condition has to be met which is linked to the minimum length of the CAP which has to be at least 440 symbols. Exceptions to this role exist and further information can be found in the IEEE 802.15.4 (2006) standard.

Update period supported per superframe

The superframe structure of an IEEE 802.15.4 standard is defined by two MAC parameters: the Beacon Order (BO) and Superframe Order (SO). The BO specifies the intervals at which the coordinator shall transmit its beacon frames. The Beacon Interval (BI) is specified in symbols and is computed using Equation 5.1. *aBaseSuperframeDuration* represents the number of symbols forming a superframe when SO is equal to zero. Therefore, it is a product of MAC layer constants: *aBaseSlotDuration* which is 60 symbols and *aNumSuperframeSlot* which is 16.

$$BI = aBaseSuperframeDuration \cdot 2^{BO} \quad \text{Equation 5.1}$$

The Superframe Duration (SD) as specified in Figure 5.1(a,b) can be calculated using Equation 5.2. It depends on SO which describes the length of active period of the superframe.

$$SD = aBaseSuperframeDuration \cdot 2^{SO} \quad \text{Equation 5.2}$$

The relationship between BO and SO is specified by the following: $0 \leq SO \leq BO \leq 14$. If $BO=15$ then the coordinator should not transmit beacon frames and if $SO=15$ then the superframe shall not exist.

In order to calculate the shortest duration of a superframe, BO and SO are to be equated to zero. As a result, BI becomes equal to SD and the outcome is a superframe structure of 15.36 ms duration. Assuming that one device can be allocated one GTS in a superframe by the PAN coordinator, and that the duration is sufficient for it to communicate without acknowledgment then the fastest update period supported by the standard using one repetitive superframe is 15.36 ms. The underlying calculations also assume the use of a 2.45 GHz PHY which operates at 250 kbps and uses single-hop star network topology.

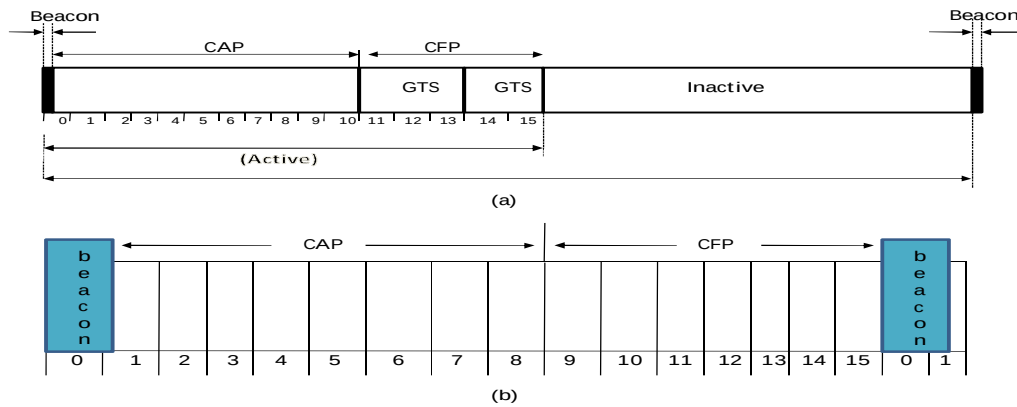


Figure 5.3. Example of an IEEE 802.15.4 superframe structure (a) with inactive and (b) without inactive period, modified from IEEE 802.15.4 (2006).

Update period supported in a multi-channel and multi-superframe setup

If multiple superframes can be used simultaneously with frequency diversity then the limitation described above can also be avoided. It is so because a device can subscribe to multiple superframes and each of them can have a GTS allocated to the device which needs frequent data update. In the case of WirelessHART network, at a given time a device can be participating in more than one superframe.

To summarize, for process automation applications the update time should not be an issue for a majority of applications, however network availability, latency control and fail-safe operation are different yet relevant challenges.

5.1.4. Sink and Hopping in a Wireless Sensor and Actuator Network

Automation architecture

According to Verdone *et al.* (2008), two communication formats are often found in WSN, known as automated architecture and semi-automated architecture. In the former case sensors detect the phenomena and pass on the information to actuator nodes without an involvement of a sink node (where data is collected and commands are issued). In the latter case, sensors route their information to the sink node which further issues command to actuators. The use of semi-automated architecture is a common practice in process industry.

Scalability (ability of a network to accommodate growth) is an important aspect of selection of wireless technology for monitoring applications. Traditional single-sink

WSN networks have limited scalability whereas; multi-sink WSN networks can reach high levels of scalability (Verdone *et al.*, 2008). The information which is collected from these processes under supervision can even be routed on the internet through gateway. This can facilitate the process of information distribution subject to latency requirements and security concerns.

Scalability of a WSN depends on various factors like the number of sinks and hopping of information via other routers in the network. The two cases below will provide some insights.

Single-sink single-hop wireless sensor network

It is a star topology, all of the network devices communicate directly to the sink node. In the following example, the sensed data size is D bytes and the samples are taken every T_R seconds. Communication protocols introduce overhead and hence the maximum data throughput at the application layer is given by $S_A = R_b \alpha_A$, where R_b is channel bit rate and α_A accounts for protocol overhead. The maximum number of homogenous devices N_{HD} which can be connected to a wireless network is given by the following equation (Verdone *et al.*, 2008).

$$N_{HD} \leq \frac{R_b \alpha_A T_R}{8D} \quad \text{Equation 5.3}$$

The expression shows that protocol overhead, transmission rate and sample size impose N_{HD} limit, as to how many devices can join a network. The channel bit rate for IEEE 802.15.4 radio modules is 250 kbps in 2.4 GHz band. The increase in sample size decreases the network capacity as can be seen from the Equation 5.3.

Multi-sink multi-hop wireless sensor network

Nodes which function as Full Functional Devices (FFD) not only communicate their own sensed information but also relay information pass on by other devices. This helps to extend the range to which the network can operate and the number of nodes which can join such networks given by Equation 5.4. Here, h_m accounts for average number of hops per data sample. Furthermore the Equation 5.4 taken from Verdone *et al.* (2008) shows that multi-sink networks become scalable with the introduction of multiple sinks in a network, N_s .

$$N_{HD} \leq \frac{N_s R_b \alpha_A T_R}{8Dh_m} \quad \text{Equation 5.4}$$

The control architectures which are relevant to control were previously presented in Section 3.2. Here, the discussion signifies the limits related to the use of sink nodes and hops. In addition to the theoretical analysis presented here the IEEE 802.15.4 standard imposes restriction in the assignment of GTs in a superframe, therefore it is an additional constraint.

5.1.5. Distinction between WSN and WSN

A network involving both wireless sensor and actuators is not a simple extension of wireless sensor network. The list below provides a description of various differences and explains how WSN brings complexity and considerations which are not present in WSN applications.

- **ARCHITECTURE:**
In a WSN, the end devices which monitor the phenomena of interest are often low-cost, low-power devices with sensing, computation and wireless communication capability (Aky *et al.*, 2004). Actuators, by contrast, are resource rich nodes equipped with better processing capability and higher energy storage, allowing longer wireless transmission distance (Hu *et al.*, 2005). They may even be mains powered in static deployment.
- **REAL-TIME:**
In a control application, real-time data delivery is of critical importance as the late delivery of process data will be of no use for controller to compute control action as the process value may have changed. Therefore, WSN has strict deadline requirements for network devices whereas, devices in WSN which are providing data only for monitoring non-critical application generally have less tighter delivery requirements.
- **DATA FLOW:**
In a typical WSN, data from sensor nodes flows towards single or multi-sink nodes where the collated information is analyzed and a wider picture of the ongoing activities is formed and decisions are made. The presence of actuators may require devices to make decision in the field and provide direct

communication between sensors and actuators for control applications (Xia *et al.*, 2007). Hence, the concept of single data collection unit may be unnecessary in WSN.

- COORDINATION:

There is a wider need for coordination amongst the sensors and actuators to perform designated tasks effectively. Coordination mechanisms can help in ordering of events and by taking appropriate action. Coordination amongst the sensor-sensor, sensor-actuator and actuator-actuator can help to form a smart, intelligent and robust wireless network (Hu *et al.*, 2005).

- EVENTS ORDERING AND REPORTING:

Ordering of events in a WSN is very critical. In case of event detection and reporting, appropriate action or series of actions must be taken. In an automated system where devices make decision based on the collected information requires not only integrity of data but also highly synchronized clocks amongst the field devices.

- ACTUATOR DYNAMICS:

Some applications, like industrial automation involve both static and mobile sensors and actuators. Therefore, there is a requirement for reliable coverage and real-time data delivery for devices in the field. The number of actuators in a WSN can be generally fewer than the number of sensor nodes, for many-to-single sensor to actuator reporting of data.

- HYBRID NETWORK:

In the presence of both wireless sensors (passive) and actuators (active) nodes, there will be a hybrid environment and these computationally different devices require different network performance. Protocols which are to be used in such network require reliability and real-time delivery of accurate data between the two parties either through centralized or non-centralized mechanism.

- NETWORK LIFETIME:

Energy consumption is an important feature of WSN. Similarly, in a WSN it is highly important and the network lifetime is a function of not only sensor node lifetime but also actuators.

The reason for an overview of the distinction between these two networks is to assist the design of a communication network to provide communication to both sensors and actuators. Designing a communication network to serve control application over a wireless network requires analysis of trade-off amongst computation versus communication, continuous versus event-driven control, and understanding of communication model for the field devices.

5.2. Network Setup for Process Control Loop Performance Analysis: A Case Study

In this section, a background is being provided for the case study used to evaluate the performance of a control loop operating over a wireless network. Therefore, this section outlines the boundaries within which the wireless control is restricted in this study and also justifies the assumptions.

5.2.1. Control Architecture and Non-Standardized Regions

Figure 5.4 depicts a typical control hierarchy with highlighted communication flows. It is a detailed version of the centralized control architecture shown in Figure 3.5(a). This enhanced version of the figure serves the following purposes:

- It shows the regions where the wireless field network resides in the automation hierarchy. The right hand side of the figure depicts a typical ISA 100.11a network topology and the left hand side highlights the WirelessHART network. They were described in detail in Chapter 2.
- It also identifies the regions which are not standardized. For instance, the link between the access points and gateway, and between the gateway and plant automation network are not specified.
- It is important to understand that these regions which are not standardized are part of the control loop and will affect the control loop performance. For instance, getting the data from sensor S1 to controller needs to pass through the non-standardized region. Furthermore, the controller output needs to be communicated to actuator A1. Again the non-standardized region lies in the path.

Therefore, from a control over a wireless network perspective all forms of delays or deadtimes which are encountered in path from sensing to actuation need to be understood, restricted and compensated if necessary.

Time delay involved from sensing to actuation

The network induced time delay can be divided into two halves: uplink and downlink. Here, *uplink* refers to the communication path from sensor to controller, and *downlink* refers to the communication path from controller to the actuator.

The delays incurred in uplinking are as follows:

- T_S – the time from sensing to the scheduling of network access.
- T_{S-AP} – the time taken to get the data transferred from sensor to the AP. This depends on MAC, network topology and on routing protocol.
- $T_{Transition}$ – the time taken to get the data from AP to controller via gateway. This will encompass the non-standardized region mentioned above.

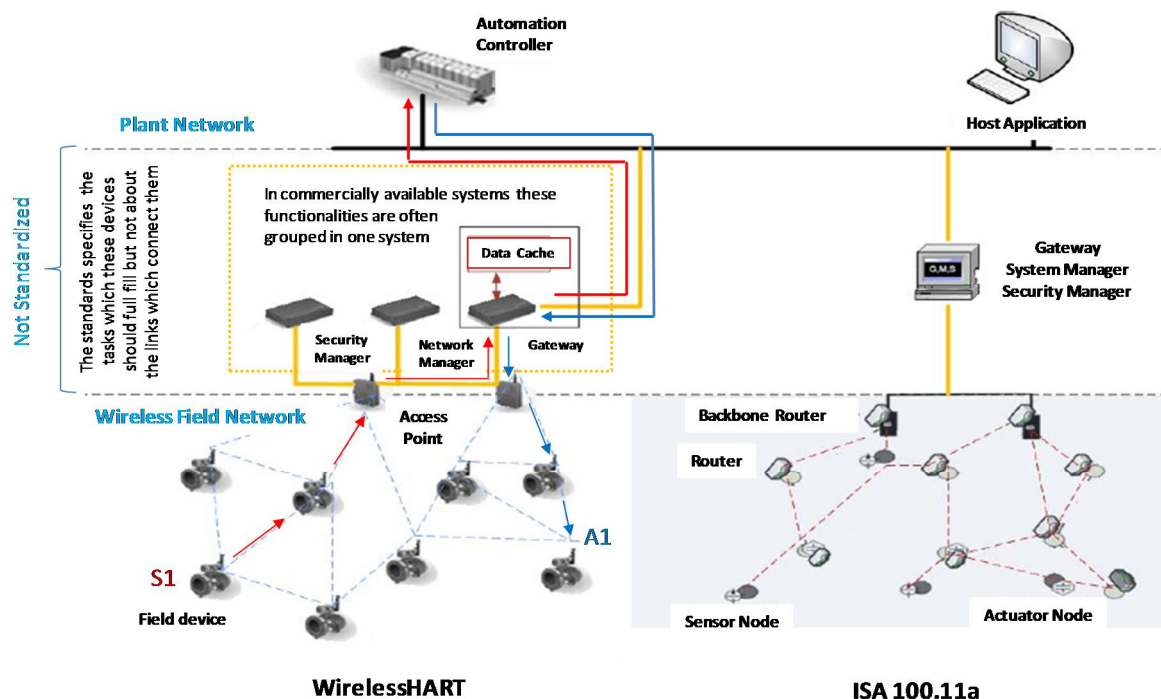


Figure 5.4. Hierarchy of control systems and network architecture, modified from individual standards.

- T_C – the time the controller takes to compute output and also the start of its execution time.

Similarly, the delays in downlinking are as follows:

- $T_{C'}$ – the time from control command generation to the network access.
- $T_{Transition'}$ – the time taken to get the data from controller to AP via gateway.
- T_{AP-A} – the time consumed in getting the data transferred from AP to the actuator.
- T_A – the time taken to serve the incoming command at the actuator.

All these delays incurred from sensing to actuation can be represented on a time line and an example is shown in Figure 5.5.

Assumptions

In the control architecture used in the performance analysis of process control over a wireless network which will be presented later the following assumptions are taken:

- The sensing time and network access time can be synchronized. Therefore, T_S can be assumed to be zero. Similarly T_A can also be assumed to be negligible.
- The time consumed from getting the data routed between the AP and gateway can also be ignored for now. It is assumed on the basis that existing real-time wired industrial protocols can be used at this level and they can be scheduled to keep this delay to minimum.

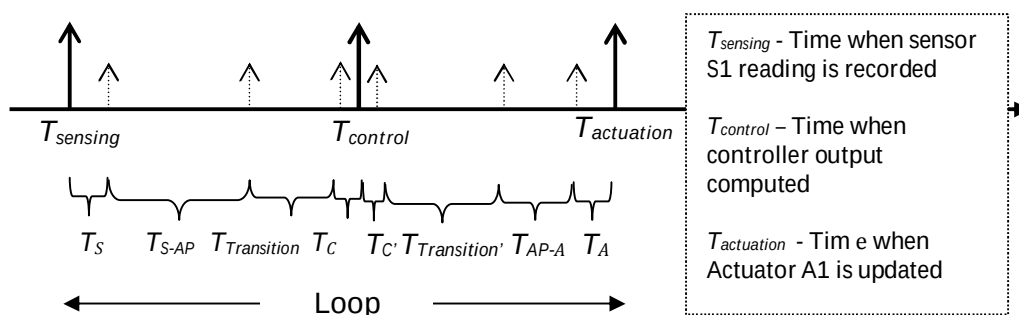


Figure 5.5. Timeline of feedback control execution.

- The time consumed at the controller, T_C and T_C can also be ignored. If a high speed controller is used and the scheduling is done accordingly then this is a fair assumption.

In addition, the last two assumptions can be complemented by having two asynchronous loops running in the system. One of them gets the information from the sensors and updates that information in the cache memory which is kept at the gateway and also updates the actuators data accordingly. The other loop is between the Input Output (IO) data kept at the cache memory and the controller. The controller periodically reads the input data from the cache memory of gateway and computes the control signal and conveys it to the gateway. This loop can be updated at a higher rate and is not restricted by the limited resources of a wireless network. Doing so will help keep the delays associated with the non-standardized region to the minimum.

As a result, the entire feedback control loop performance is linked to these two sub-operational communication loops. The network induced delays from standardized wireless region will therefore play a vital role in the control loop performance, and the following discussion will be restricted to the wireless field network only from delay perspective.

5.2.2. Process Model

The process which needs to be controlled and is under investigation in this wireless process control study is an industrial furnace and its schematic is shown in Figure 5.6. It is used to heat up a crude process stream by burning either fuel oil, gas or their mixture in air. The temperature and flow of the process stream entering the furnace are not controllable and are a part of an upstream process.

The objective of the control is to maintain a steady outlet temperature of the feed out and to control the concentration of oxygen in the flue gas. They are to be achieved by manipulating the flow rates of fuel oil, gas and air. For the purpose of this case study this process is simulated in Simulink.

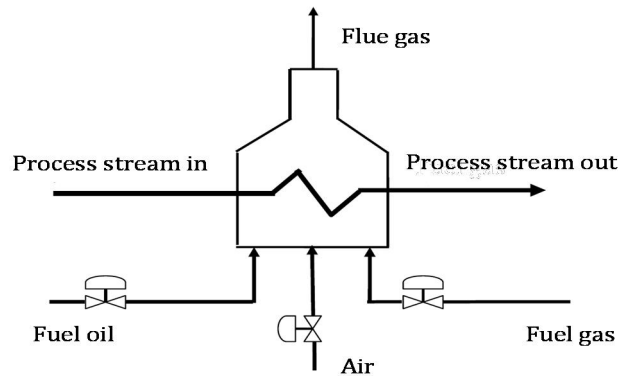


Figure 5.6. Schematic of a furnace process.

5.2.3. Control Strategy

The control algorithm used in the control strategy is Proportional-Integral-Derivative (PID). The loop pairing used is as follows:

- The output feed temperature is controlled by manipulating the fuel gas flow rate.
- The oxygen concentration in flue gas is controlled by manipulating the air flow rate.

In this setup, the flow rate of oil is set manually and is not part of the automatic control loop. The process flow diagram of the furnace and the information flow lines under the given flow scheme are shown in Figure 5.7. Furthermore, in order to decouple the interaction between the two control loops shown in the figure a decoupler is used. Moreover, in order to compensate for disturbances, such as flow and temperature of input process stream, feedforward controls are used. A detailed description of the process and the control strategy can be found in the process control project lecture notes given in Che203.1 (2008). A snapshot of the implemented Simulink model is provided in Appendix D1.

5.2.4. Simulation of a Control Loop Performance Setup

The simulation platform used for this case study is TrueTime. It is a Matlab/Simulink based freeware toolbox for simulation of Real-Time Control Systems. It has been developed at Lund University. TrueTime Simulator consists of Simulink Block Library. It facilitates the co-simulation of (Ohlin, 2007): controller task execution, network transmissions, and continuous plant dynamics.

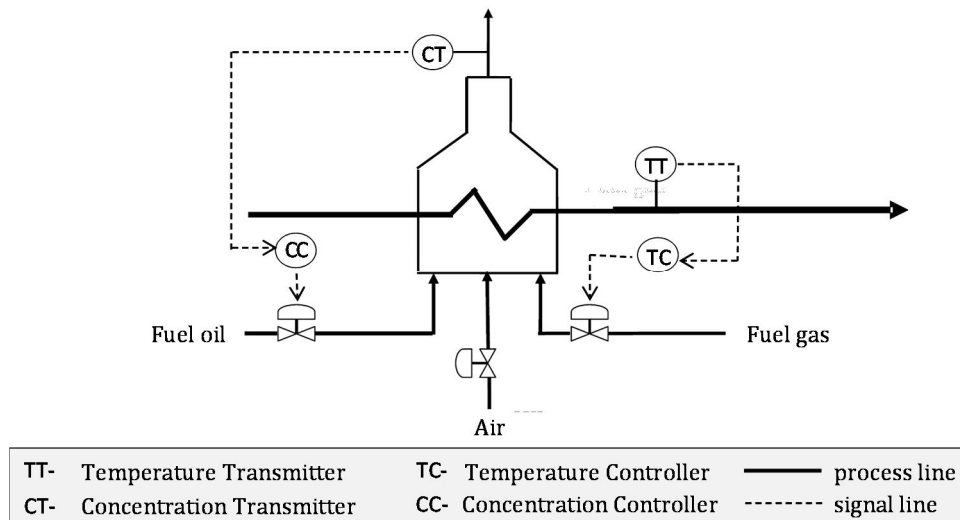


Figure 5.7. Schematic of a process flow diagram.

Therefore, this integrated environment can be used to study the interaction between different cross-disciplinary research areas such as control and communication as in WNCSSs. TrueTime has useful built-in models such as of real-time kernels, networks (wireless and wired), battery powered devices and embedded systems clock. The radio model used in wireless network simulation contains support for (Henriksson et al. 2007):

- Ad-hoc wireless networks
- Isotropic antenna
- Path loss of radio signal in 2D space which has been extended to 3D by Biasi et al. (2009)
- User-define path loss function which is important to reflect real deployments
- Interference from other terminals such as Wi-Fi
- Half-duplex communication which signifies its inability to send and receive packet at the same time
- Calculation of error probabilities based on additive white noise which gives probability density function for the received symbol.

Furthermore, TrueTime also supports IEEE 802.15.4 MAC. Biasi *et al.* (2009) have further extended this work and have included some features of WirelessHART to the TrueTime simulator. Therefore, based on the above TrueTime is selected for the simulation of WNCS in this study.

5.2.5 Hardware-in-loop Setup

The success of simulation results for wireless process control depends on the model used to represent the network. In order to enhance the experience of closed loop control over an actual wireless network a hardware-in-loop setup was constructed as shown in Figure 5.8. In this setup, the use of Real Time Windows Target toolbox was used to connect the output of the sensor reading to a wireless transmitter (in this case a CC2430 module) which transmits it to the controller. The output of the sensor is routed through an actual wireless network which is subjected to co-channel interference and other environmental features like multipath. After the reception of data packet at the receiver it is communicated to the computer which acts as a controller and generates the control commands. The controller is implemented in Simulink as well as the process. In addition, the control commands sent to the actuator from controller are internal communications within Simulink.

The outcomes of these experiments are presented and analyzed in the following section.

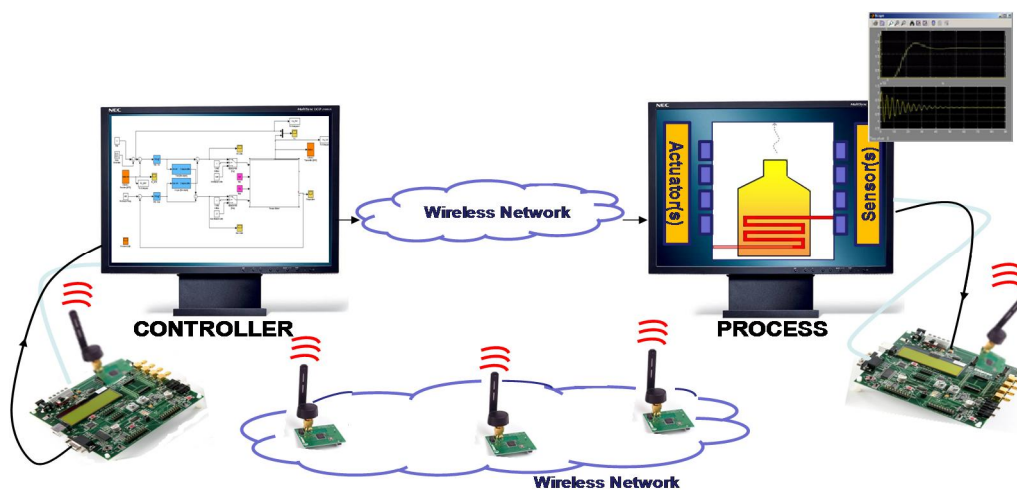


Figure 5.8. A hardware-in-loop setup to quantify the issues in a WNCS.

5.3. Proposed Mechanism to Improve Performance

In this section, the performance of the designed controls system will be examined while subjecting it to varying network delays and data losses. Additionally, based on the acquired knowledge, mechanisms will be proposed to improve the control system performance.

5.3.1. Control Loop Performance

Control performance without network induced delay and data loss

Figure 5.9 shows the performance of a closed loop control system with one second update rate without data loss. Here it is assumed that all sensors, controller and actuators execution rates are same and synchronized. In the figure, the upper panel corresponds to the response of oxygen concentration (i.e. O_2) with a changing reference point. Similarly, the lower panel shows the temperature response of the same industrial furnace. These both processes are assumed to be First Order Plus Time Delay (FOPTD) processes. The process response time of oxygen concentration loop has fast dynamics as compared to temperature control loop. Therefore, the impact of data delay or loss will be visible early and more prominently in the oxygen control loop. The discussion from now onwards will focus only on the oxygen concentration control loop.

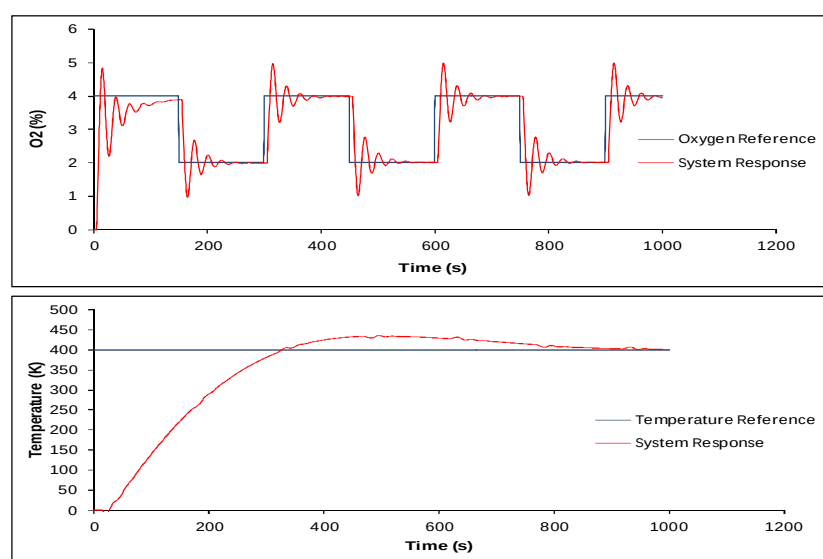


Figure 5.9. Industrial furnace response to changes in set points. Network delays are ignored in this simulation.

Controller gain, sensor sampling and controller scheduling

The response of the oxygen control loop shown in Figure 5.9 is of an underdamped system. The controller gain can be altered in order to change its behaviour. Figure 5.10 presents the outcome of the control system performance with altering sampling and controller execution period. The controller gain in the upper panel of Figure 5.10 is 340 and in the lower panel is 240. Therefore, it can be seen that the scheduling of sensing and control task and also the controller gain affects the system response time. The higher the controller gain above the underdamped region, the more it increases settling time. Similarly, the higher sampling period of sensing and control both increases settling time.

Network delay

The effect of network induced delay on control system performance is shown in Figure 5.11. Two outcomes are shown in this case, one for a constant network delay of one second, and the other of two seconds. The time-triggered sampling and controller execution is scheduled every second. Therefore, it can be seen that the controller is less effective to control the process response if the network induced delays are higher than the overall system sampling time.

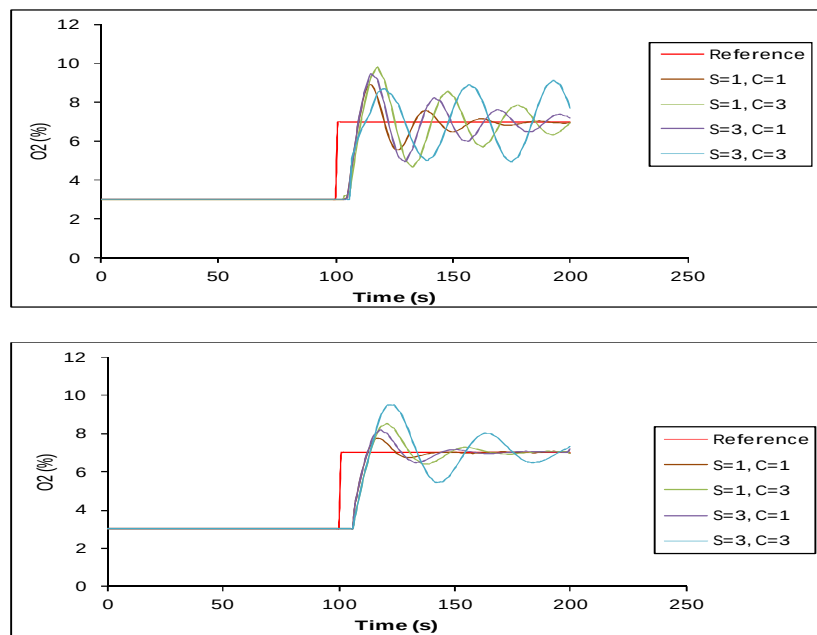


Figure 5.10. Oxygen concentration response to a step change in reference with varying sensor and controller execution period and controller gain. The upper panel corresponds to a controller gain of 340, and the lower panel corresponds to 240.

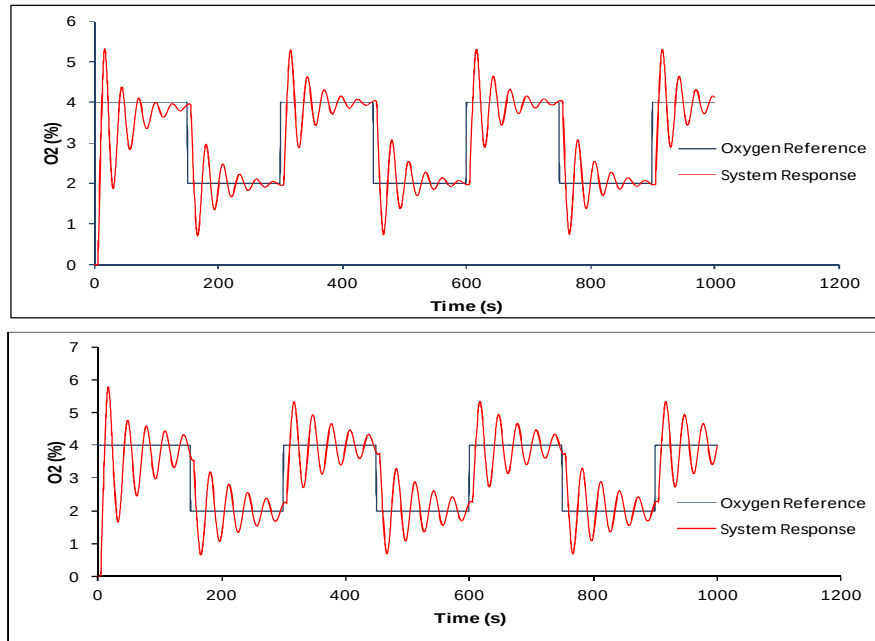


Figure 5.11. Upper panel corresponds to a network delay of one second and the lower path corresponds to a network delay of two seconds.

Bounded but random network delay

Depending on the network topology and communication protocol, the delays incurred in a network may be varying but bounded in time. The simulation of a control loop system under such a scenario where the network delays are randomly distributed is shown in Figure 5.12. Here, it can be seen that the performance of control loop depends on the packet delay incurred and also at the time when it occurred. If the delay is during a transitional period then it will affect the control loop performance. However, if it is outside the transitional period then it will not affect the controller performance as the controller output remains same.

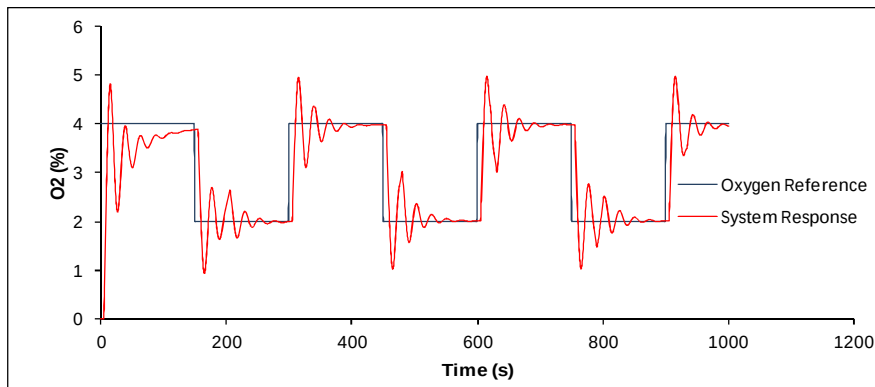


Figure 5.12. Random distribution of sensor packet delays within a range of one to two seconds.

Random packet delay and data loss

Figure 5.13 illustrates the effect of combination of random packet delays and data losses as a result of co-channel interference. It can be seen from the figure that the control performance is significantly varying in time. Therefore, it highlights the necessity to address network induced delays and packet losses. In this case, only few consecutive packet losses have been observed. The maximum window size of consecutive packet losses was a quarter in lengths to the process response time.

Network outage

Network outage is undesirable in a WNCS. It introduces a dead time and violates the availability requirement of process control systems if it is above a certain period. The maximum allowed outage is specified by standards such as ISA 100.11a. For now, they are ignored. The focus here is to identify and minimize the effects of packet losses on control system performance. Figure 5.14 shows the effect of a network outage of duration 30 seconds on a control loop performance. The network outage started at 300 second past the start of experiment.

Table 5.1 summarizes the control loop performance with different combinations of setups and network outage duration. These combinations include the controller gain, sampling times and of network with and without outage. The Sum of Square Error (SSE) highlights that due to network outage if the PID algorithm keeps computing the control output based on last received process value then it can drive an actuator to saturation.

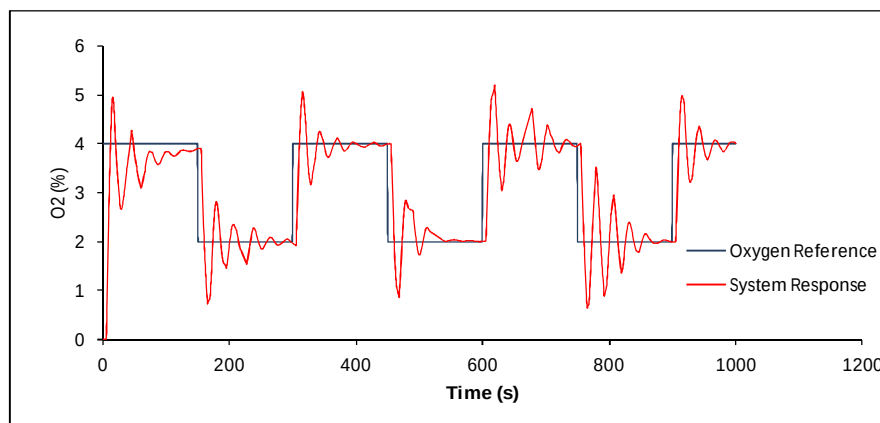


Figure 5.13. A hardware-in-loop experiment demonstrating random distribution of sensor packet delays and packet losses as a result of co-channel interference from Wi-Fi.

It is because the error from the integral part of the PID algorithm will keep accumulating and when the network re-establishes after the network outage then it will cause a spike in the response from derivative part. These two issues were also identified by Chen *et al.* (2006).

To summarize, the performance of a control system depends on the controller tuning, network scheduling and the network ability to handle co-channel interference and to minimize packet drop outs and outages. The next section will explore methods which can address some of these issues.

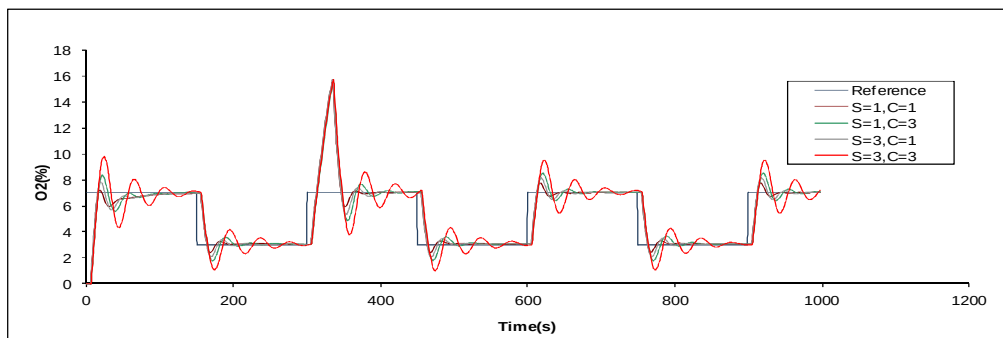


Figure 5.14. Control system response to a network outage of a 30 second duration. In the diagram s represents sensor and c represents controller execution period in seconds.

Table 5.1. Closed loop control performance evaluated in terms of Sum of Square Errors (SSE). Here, controller gain is 340 and T represents system response time and is taken as 30 seconds.

SAMPLING		NETWORK OUTAGE: CONTINUOUS	PERFORMANCE: SSE	
Ts (s)	Tc (s)		K=240	K=340
1	1		761	834
1	1	(1/2)T	821	986
1	1	T	1793	2173
1	3		957	1286
1	3	(1/2)T	1017	1424
1	3	T	1839	2596
3	1		805	1068
3	1	(1/2)T	877	1203
3	1	T	1708	2378
3	3		1361	2308
3	3	(1/2)T	1430	2861
3	3	T	2350	3258
1	5		1036	1792
1	5	(1/2)T	1094	1884
1	5	T	1909	2948
5	1		869	1306
5	1	(1/2)T	947	1412
5	1	T	1845	2607
5	5		1948	6901
5	5	(1/2)T	1974	7033
5	5	T	2954	5671

5.3.1. Data Recovery to Improve Integral and Derivative parts of PID Algorithm

The outcome of a PID controller comprise of three components: proportional, integral and derivative terms. Collectively a PID generates an output based on past, present and prediction of future system response (Vu, 2007). In a continuous (analog) form a PID is represented by Equation 5.5 (Vu, 2007).

$$u(T) = k_p\{y(T) + \frac{1}{T_i} \int_0^T y(t)dt + T_d \frac{d}{dt} y(t)|_{t=T}\} \quad \text{Equation 5.5}$$

Here $u(T)$ is the control variable, $y(T)$ is a continuous deviation of controlled variable relative to reference point, k_p is the controller gain, T_i and T_d are integral and derivative constants respectively. The digital version of this PID controller is represented using finite difference equations as shown in Equation 5.6 (Vu, 2007).

$$u_t = k_p y_t + k_i \sum_{j=0}^t y_j + k_d (y_t - y_{t-1}) \quad \text{Equation 5.6.}$$

Therefore, Equation 5.6 highlights that the integral term becomes a summation as a result of this conversion to discrete time. Similarly, the differential term becomes the difference. The step change to reference point during network outage drives the manipulated variable high. When the network re-establishes the difference between the last communicated and present value of process variable may have changed significantly and can cause a spike in controller output. However, these two issues can be resolved. This PhD work has led to an algorithm for improving the control performance when operating over a wireless network. This section describes the algorithm and demonstrates its performance.

During the network outage, the process output may have changed and using this to compute integral part can result in actuator saturation. Therefore, during network outage the following principle can be adopted. The controller output can behave as an open loop control due to outage between sensor and controller network. When the network is re-established the Integral and Derivative (ID) parts which were lost, and depend on present and previous values can be recovered. It is so because the IEEE 802.15.4 frame format has a maximum MAC payload between 102 and 118 bytes depending on the header format and security. Therefore, each data packet of IEEE 802.15.4 network originating from a sensor can transmit the present and a few previous values of sensor readings. The maximum number of readings which can be transmitted

depends on process variable type, for instance a temperature measurement may be represented by two bytes. Furthermore, depending on the network protocol overhead built on top of the IEEE 802.15.4 frame structure the maximum allowed packet size may be reduced. Even though, there will still be enough rough to transmit the present sensor reading with the previous because process variable data is only few bytes. As a result, the reception of every successful packet will help recover the ID parts.

Overall, the proposed mechanism can be depicted as a switched state model represented in Figure 5.15. During normal operations without data loss the controller behaves as a normal PID. When an outage occurs it switches to open-loop mode. If the duration of continuous data loss is below the maximum allowed outage and the data packet arrives within this time frame then the controller enters into recovered ID mode. In this case it switched back to closed loop control format from open loop by recovering the ID values from the received packet. However, if the network outage is above the maximum allowed outage then the device enters a fail safe mode, which is an intervention from the process safety system.

The Implementation of the proposed switched state mode of the PID controller yields Figure 5.16. Here, the network outage was from 10 seconds till 27 seconds. The outcome highlights that the proposed method is effective in improving the response of the system compared to the use of PID with the computation of ID based on the previously received value of process variable. In this implementation, fail safe mode did not occur as the outage was below the threshold level required to trigger the intervention from safety system.

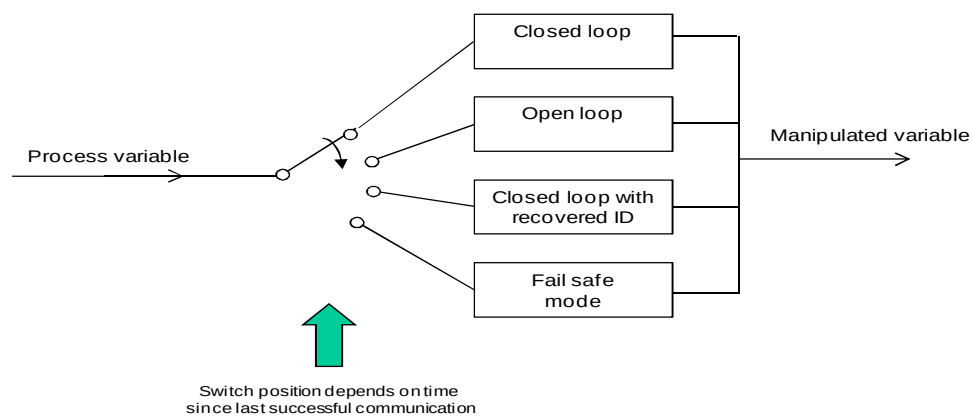


Figure 5.15. The switched state mode operation of the controller depending on the network status. Reference point is not shown explicitly and is considered to be known to each state.

5.3.2. Improving Data Delivery Success within a Time Frame

In the previous section a method to improve the control performance was suggested based on modification to the controller output. Here, the focus is to improve the network operations in order to minimize network delays and data losses.

In a TDMA based network such as WirelessHART and ISA 100.11a network the devices can be allocated time slots within a superframe. During each timeslot a transaction can occur between two or multiple devices depending on whether the data packet was of unicast or multicast type. Figure 5.17 shows the superframe structure with one highlighted time slot. For simplicity the CAP, CFP and inactive periods are not shown. TDMA networks are favored compared to CSMA based network because of determinism. However, as the network size grows the devices have to wait for a long period before they can transmit a data. For those devices which are allocated GTs they still need to wait for their time to transmit. If during their allocated time a packet is lost due to interference, jitter or similar effect then they need to wait for their turn in the next cycle. It is one of the limitations of the TDMA network. It can cause system degradation especially if the multiple control loops running over the same network are subjected to delays and losses during the transitional period. These issues were discussed and presented above.

Existing standardized protocols use frequency hopping to avoid interference and jamming and consequently increase their reliability. They use the diversity in frequency and time as depicted in Figure 5.17 (a) to achieve this. For instance, WirelessHART defines a time slot of duration of 10 ms. Moreover, it supports frequency hopping on per

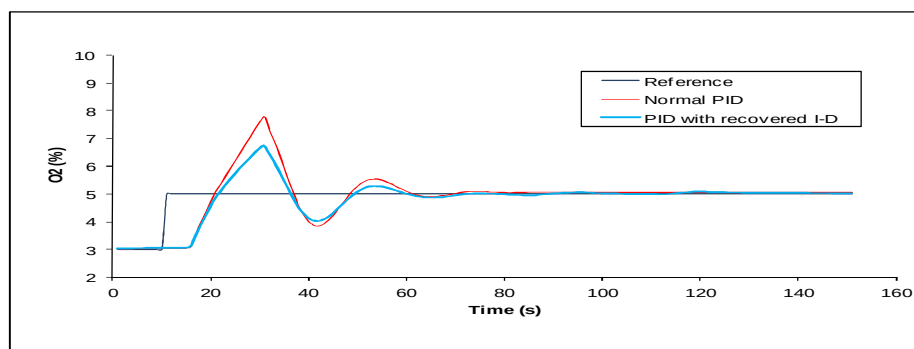


Figure 5.16. Comparison of the control system performance with recovered ID method.

packet basis. The standardized wireless networks do not distinguish between the uplink and downlink data flows explained earlier in this chapter. Dynamic allocation of resources like time slots to control related data can improve the wireless control system performance by reducing network linked imperfections.

A total of 16 channels are available in 2.45 GHz band of IEEE 802.15.4 network. The data rate of the entire band can yield a collective output which is 16 times the data rate of running the network over one static channel. However, to avoid jamming and interference mostly the data is routed around in a random manner between different channels. It essentially delivers the same result as one channel which would have delivered without interference and jamming.

In order to address the issues highlighted in Figures 5.10-5.14, here it is proposed that the required band available for frequency hopping can be divided into two segments. One segment can use the bulk of available channels with frequency hopping for cyclic

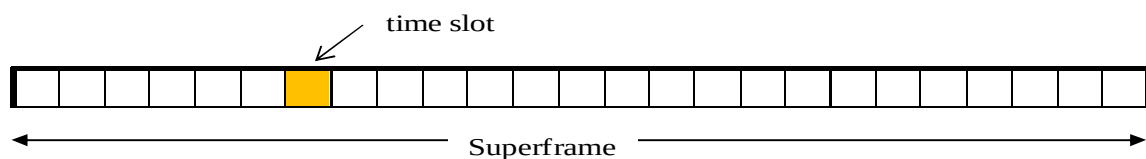
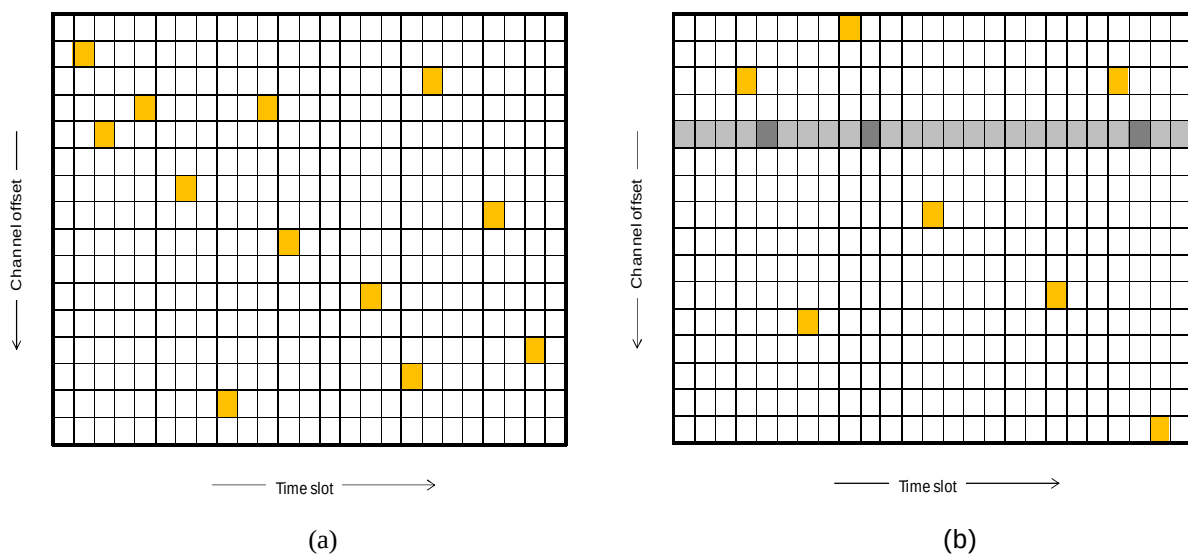


Figure 5.17. A superframe structure highlighting a time slot with the frame.



data. However, the other band which might have relatively few channels can be used as a mean to improve the data delivery within given bound. It can be explained from the graphical illustration shown in Figure 5.18 (b). Here it is assumed that the available 2.45 GHz band is divided into 15 channels and 1 channel band. This one channel highlighted in the figure is a channel which is expected to be least affected by interference and noise. This channel will act as a fast lane for the data which gets lost during normal scheduling. Hence, if during normal allocated slot the device does not receive acknowledgment of its delivery then it assumes that the data is lost. Now, instead of waiting for the next allocated time slot it accesses the fast lane and retransmits the data over a finite window of time. Doing so will help get the data across the network to its destination within a given time. The rules of fast lanes (i.e. dedicated lanes for control related data) are as follows:

- The NM broadcasts the information regarding the lanes (i.e. dedicated channels) which can be used in case of control-critical data.
- Devices are only allowed to access the dedicated channels if they are directly related to control loop or are in path of the flow of control related data.
- The access to dedicated lanes is only allowed if the acknowledgment was not received or a NACK was received.
- Furthermore, the access to the channel is also linked to the change in process value or control value since last successful communication. A concept adopted from Yopez *et al.*, (2003), where Large Error First (LEF) was used for scheduling. Here, it is used to help decide whether to access the dedicated channels for control-critical data. The LEF here is based on relative change.
- Regarding the scheduling in fast lane it is a shadow of the original superframe which is used. It is called *shadow* because it is a time lag version of the original superframe. However, it is only executable when the above mentioned criteria is satisfied. The shadow version of the superframe helps to keep the memory requirement to store the superframe minimum as it is already known to the field devices.
- To implement this proposed scheme the diversity in time and frequency is required with centric data flow.

- The duration of time lag for shadow superframe and the slot durations are set by the NM which has an over information about the network schedule.

Referring back to Figure 5.18 (b) it can be seen that inside the grey region (i.e. fast lane) only three time slots were used. It is because here three data packets were lost during normal superframe operation. And because the data were control-critical the devices accessed the fast lane immediate after their time slot and retransmitted their information. Here, the lag was one time slot and the mapping between normal superframe and shadow superframe was one-to-one. Figure 5.19 shows the operation of this proposed methodology when subjected to data loss. The data loss here is linked to the transactions taking place during normal superframe duration. A pulse stream shown in the figure highlights the regions in time where the control data was lost. From the figure it is visible that the use of shadow superframe helped to improve data delivery in time by using the hybrid methodology involving dedicated lanes, shadow superframe and LEF based scheduling.

To summarize, the performance results are shown for the star-based network topology. However, using this in a mesh will provide further improvement because it comprises of multiple links and data can be lost anywhere in the path. This proposed mechanism improves packet delivery on per link basis and therefore enhances overall availability leading to improved control performance.

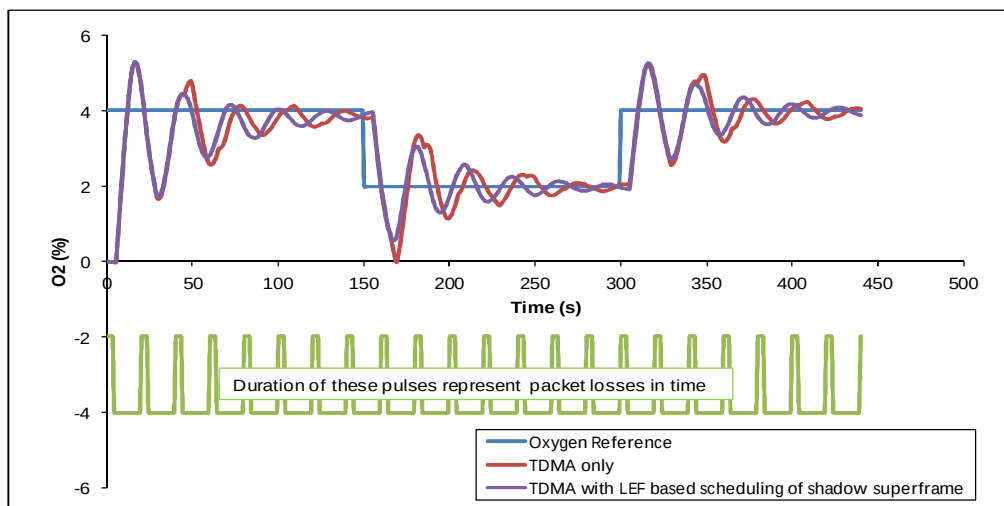


Figure 5.19. The control system performance subjected to data packet losses. The control loop was scheduled to be updated every second.

5.3.3. Fast Lane Selection based on Minimization of Spectrum Occupancy subject to time delay and throughput constraints

In this section, the concept of fast lane introduced earlier will be examined to identify the tradeoff between Spectrum Occupancy (SO) and network throughput. On one hand, to add more channels to the fast lane will improve the probability of successful communication and overall aggregated throughput, while constraining the network induced delay in the packet delivery. On the other hand, it will increase SO, which increases the collision probability for the devices operating in the same frequency band. Therefore, it should be kept minimum. Here, the selection of number of channels in a fast lane will be based on minimizing an objective function (i.e. SO) while using number of fast channels as a decision variable.

The discussion in this section will be confined to a star-based (i.e. single hop) network operating over an IEEE 802.15.4 PHY. For simplicity it is assumed that if interference occurs the packet is blocked (i.e. lost), and since the IEEE 802.15.4 standard does not implement Forward Error Control (FEC), hence it is a valid assumption.

The following subsections will introduce the models and methods which will be later used to formulate the optimization problem. Finally, based on the optimization problem a graphical illustration of the solution is provided and discussed.

The summary of notations referred to later in the text is as follows:

Notation	Summary
N_g	Total number of good channels.
N_b	Total number of bad channels.
P_g	Probability of a good state.
P_b	Probability of a bad state.
P_{gg}	Probability of a good state remaining good.
P_{gb}	Probability of a good state to go bad.
P_{bg}	Probability of a bad state to become good.
P_{bb}	Probability of a bad state to remain bad.
k	Denotes channel index.
K	Maximum number of channels available for fast lane communication.
$P_g^{(k)}$	Probability of channel k being in a good state.
N_c	Total channels in 2.4 GHz ISM band (IEEE 802.15.4 PHY specific).
$p_{per,k}$	PER of channel k .
SO_k	SO corresponding to channel k .
T_{slot}	A time slot within a superframe.
$DC_{T_{slot}}^{(k)}$	A duty cycle corresponding to channel k with a given time slot duration.
TP_{Σ}^K	Aggregated throughput over all available channels in a fast lane.

t_{active}	On-air time (i.e. time used for transmission of data and reception of acknowledgment)
$D_{packet,max}^{\mathfrak{a}}$	Maximum network induced delay corresponding to packet $\mathfrak{a}$.
SO_{Σ}^K	Aggregated SO over all available channels.
$D_{\Sigma}^{\mathfrak{a}}$	Aggregated delay introduced by the network on packet $\mathfrak{a}$.
$D_{Reg}^{\mathfrak{a}}$	Delay introduced by regular frequency hopping scheme.
$D_{Hig}^{\mathfrak{a}}$	Delay introduced by fast lane.

5.3.3.1. Channel model

To capture the behavior of a wireless channel, a two state Discrete Time Markov Chain (DTMC) model, also known as Gilbert-Elliott model is used (Schaar and Chau, 2007). The two states in the model are referred to as *good* and *bad* states. Every state is assigned a specific constant BER which defines a good channel and its violation leads to a bad state. In short, a good state enables the establishment of good communication with a confined BER. If the BER is defined and the packet length is known then a PER can be computed, which is important for throughput analysis.

Therefore, an IEEE 802.15.4 network can be represented as 16 Gilbert-Elliott channels with two-by-two transition matrix specifying the probabilities of transiting from one state to the other, i.e. $P_{gg}, P_{gb}, P_{bb}, P_{bg}$. Furthermore, if the Markov chain is ergodic then the stationary probabilities for the states of each channel are given by [Schaar and Chau (2007), Hung and Chen (2008)]:

$$P_g^{(k)} = \frac{1 - P_{bb}^{(k)}}{1 - P_{bb}^{(k)} + P_{gb}^{(k)}}$$

$$P_b^{(k)} = \frac{P_{gb}^{(k)}}{1 - P_{bb}^{(k)} + P_{gb}^{(k)}}$$

Therefore, the aggregated probability of the fast channels in the good state (P_g^{Σ}) is expressed as:

$$P_g^{\Sigma} = \frac{1}{K} \sum_{k=1}^K P_g^{(k)}$$

Here, it is assumed that there is an equal probability of a channel being in good state in the fast lane. To further simplify, it is assumed that the PERs in all channels qualified as good channels are above a certain threshold, $p_{per,thresh}$. This boundary condition will simplify the analysis to come later. From here onwards, $P_b^{(k)}$ will be replaced by $p_{per,k}$, and will represent an average PER for channel k .

5.3.3.2. Channel classification

The fast lane concept works by dividing the available frequency spectrum {let it be denoted by S_{total} } into two blocks (i.e. group of channels with related features), regular traffic block {Let it be denoted by, S_{Reg} } and high priority block {let it be denoted by, S_{Hig} }. S_{Hig} comprise of channels with the high probability of success (i.e. low PER compared to S_{Reg} channels). $S_{Reg}, S_{Hig} \in S_{Total}$. The number of good channels and number of bad channels is denoted by N_g and N_b respectively. This split can be achieved using channel selection schemes based on methods such as PER, RSSI, LQI, majority logic or other similar techniques. For now it is assumed that this split can be achieved. Furthermore, this process will help identify the availability of good channels, i.e. K .

5.3.3.3. Throughput analysis

In the throughput analysis, it is assumed that the MAC is TDMA-based, all devices are homogenous, the time slots are allocated to a pair of nodes (i.e. transmitter and sink node) and that all nodes have contention-free access to the network. A time slot governs the throughput of a network, therefore an equation to calculate maximum throughput is first derived which allows identifying the constraint of IEEE 802.15.4 channel. In each time slot, T_{slot} , the transmitter needs to send a packet and receive the corresponding acknowledgment. Therefore,

$$T_{slot} = \Gamma_{offset} + \Gamma_{PacketLength} + \Gamma_{AckDelay} + \Gamma_{Ack} + \Gamma_{error} \quad \text{Equation 5.7}$$

where, Γ_{offset} accounts for the delay before the start of transmission, $\Gamma_{PacketLength}$ is the frame transmission time, $\Gamma_{AckDelay}$ is the wait before the acknowledgment is sent, Γ_{Ack} is the time required to transmit the acknowledgment message, and Γ_{error} accounts for synchronization error. Further details are given in Appendix D2.

On one hand, T_{slot} minimum (i.e. $T_{slot,min}$) depends on data payload, protocol overheads and the hardware limitation. On the other hand, T_{slot} maximum is restricted by the superframe duration, which itself is restricted by the update period T_R and the number of nodes in a network, N_{HD} as given in Equation 5.8.

$$N_{HD} = \frac{T_R}{T_{slot}} \quad \text{Equation 5.8}$$

Furthermore, by ignoring the protocol related overhead, and by only considering t_{active} will give the following boundary condition:

$$T_{slot,min} \geq (\Gamma_{PacketLength} + \Gamma_{Ack})$$

where,

$$\begin{aligned} \Gamma_{PacketLength} &= \frac{(\text{maximum packet length} + \text{superframe delimiter} + \text{frame length})}{\text{transmission rate}} = \frac{(127 + 5 + 1)\text{bytes}}{(250,000)\text{bps}} \\ &= 4.256 \text{ ms} \end{aligned}$$

Moreover, Γ_{Ack} for IEEE 802.15.4 takes 0.352ms as the frame consists of 11 bytes. Therefore, if only the on-air time is considered with maximum payload then, $T_{slot,min} = 4.608\text{ms}$.

The network throughput (i.e. $\mathcal{T}_p$) under various schemes in terms of packets per second is expressed in Equation 5.9. The equation is divided into two pieces: *fast channels communication* and *regular hopping communication*.

$$\mathcal{T}_p = \begin{cases} TP_{\Sigma}^K = \frac{1}{T_{slot}} \cdot \sum_{k=1}^K (1 - p_{per,k})^2, & \text{fast channels communication} \\ \frac{1}{T_{slot}} \cdot \frac{N_g}{N_c}, & \text{regular frequency hopping} \end{cases} \quad \text{Equation 5.9}$$

Fast channels communication: If the sink node has the capability to operate concurrently (i.e. parallel communication) on all available fast channels then the maximum allowed theoretical throughput can be achieved, and is expressed in Equation 5.9.

Regular frequency hopping: In this case, it is assumed that all the available channels are used in frequency hopping equally. At every time slot a new frequency is selected for communication. For illustration purposes, it is assumed that all the channels which are good remain good and those which are bad remain the same during the operation. Equation 5.9 represents the throughput under these conditions.

A comparison between these two communication modes highlights that one good channel with PER equal to zero in the fast lane has the capacity to completely handle the traffic of all the data being hopped over multiple channels in the regular frequency hopping band. In a regular frequency hopping network, there is only one channel being used at any instance in time. Therefore, an increase in the number of bad channels will

decrease network throughput in regular frequency hopped network. The result of bad channels leads to the data backlog which is then accommodated by the fast lane.

5.3.3.4. Spectrum occupancy

An increase in SO will result in an increase of collision probability. Hence, it should be kept to minimum otherwise QoS will be affected. SO is defined as the product of frequency occupancy times the duty cycle (Hellbruck and Esemann, 2011), and for each channel it is given by Equation 5.10.

$$SO_k = \frac{\text{Channel Bandwidth}}{\text{Total available Bandwidth}} \cdot DC_{T_{slot}}^k \quad \text{Equation 5.10}$$

The $DC_{T_{slot}}^k$ refers to the duty cycle per node in channel k , and is calculated as follows:

$$DC_{T_{slot}}^k = \left(\frac{T_{slot}}{T_R} \right)$$

5.3.3.5. Delay model (TDMA-based MAC)

The MAC in the fast lane can be based on either: TDMA, slotted CSMA/CA or non-slotted CSMA/CA. For the purpose of optimization, the first mentioned case will be examined. The MAC for the fast lane can work by replicating the same superframe scheduling as is in the case of S_{Reg} and adding an offset to the superframe start. Multiple fast lanes can be employed, and each of them would have its own offset. These offset values are to be chosen such that each time slot assignment (i.e. for pair of communicating nodes) does not overlap in time in blocks S_{Reg} and S_{Hig} . The more the channels in fast lane, the higher the probability of getting the data through to the receiver. The delay in this case for an individual packet α is represented by D_Σ^α and is expressed as:

$$D_\Sigma^\alpha = D_{Reg}^\alpha + \sum_{k=1}^K \alpha_{off}^k + D_{Hig}^{\alpha,k}$$

Here, D_{Reg}^α is the delay introduced by timeslot in regular hopping channel since packet inception. Similarly, the delay induced by fast lane is represented by $D_{Hig}^{\alpha,k}$. The total number of available priority lanes are K . α_{off}^k represents time offset of allocated time slot in channel k since last allocated of time slot in the previous allocated time slot. Offset is assumed to be zero in the regular frequency hopping band and the fast lane (i.e. application time and network time are synchronized). Furthermore, to minimize delay

and satisfy the condition of non-overlapping time slots, and assuming that T_{slot} is similar in both domains then the above equation can be reduced to identify the maximum delay per received packet ($D_{packet,max}^{\oplus}$):

$$D_{packet,max}^{\oplus} = T_{slot}(1 + K)$$

This delay depends on application QoS requirement and the probability of achieving this will rely on the availability of fast lanes and the probability of successful communication in each channel. During optimization, $D_{\Sigma}^{\oplus}$ is used as a constraint.

5.3.3.6. Spectrum Occupancy Minimization

The aim is to minimize the overall spectrum occupancy (i.e. aggregated SO) in each superframe available over all fast channels. To this end, the optimization problem is formulated as follows:

$$\min: SO_{\Sigma}^K = SO_0 + \sum_{k=1}^K SO_k$$

$$s.t. \quad 1 \leq K < N_c$$

$$TP_{\Sigma}^k \geq TP_R$$

$$D_{\Sigma}^{\oplus} \leq D_R < T_R$$

$$T_{slot} > T_{air}$$

where the number of fast channels are denoted by k . The first constraint identifies that the maximum number of fast channels available will be a subset of all available channels in 2.4GHz frequency band. Therefore, N_c is the absolute limit, whereas K is a decision variable and is linked to minimum channels needed for frequency hopping in regular channels. The second constraint identifies the minimum throughput which the fast channels need to accommodate. Therefore, TP_R is specified by the user. The following constraint is to meet the maximum delay requirement, D_R and is defined by the application which uses the data. The final constraint is imposed by the IEEE 802.15.4 standard, protocol overhead and packet payload.

5.3.3.7. Graphical Illustration

The aforementioned optimization problem is visualized here using Figure 5.20. The graph shows SO versus network throughput in the fast lane with varying number of available fast channels, along with different probability of errors in channels and delay. The graph is based on the following:

$\alpha_{off}^k=0$ and $SO_0=10\text{ms}$, so that allocated time slots are back to back.

$K=14$, maximum number of available channels for fast lane (i.e. assuming that at minimum 2 channels are required in regular frequency hopping scheme for operation).

$T_{slot}=10\text{ms}$ and, $T_R = 1\text{s}$.

Furthermore, by applying the constraints mentioned above, either an exhaustive search or a graphical method can be used to find the solution. As an example, using $TP_R = 140$ packets/s and $D_{packet,max}^{\infty}=50\text{ms}$, the non-shaded region of the Figure 5.20 demonstrates the region with optimum solution. Therefore, $K=2$ for $p_{per} < 0.15$ (i.e. highlighted with blue markers) and $K=3$ for $p_{per} < 0.25$ (i.e. highlighted with red markers). Moreover, the figure highlights that the increase in magnitude of $p_{per,k}$ decreases network throughput.

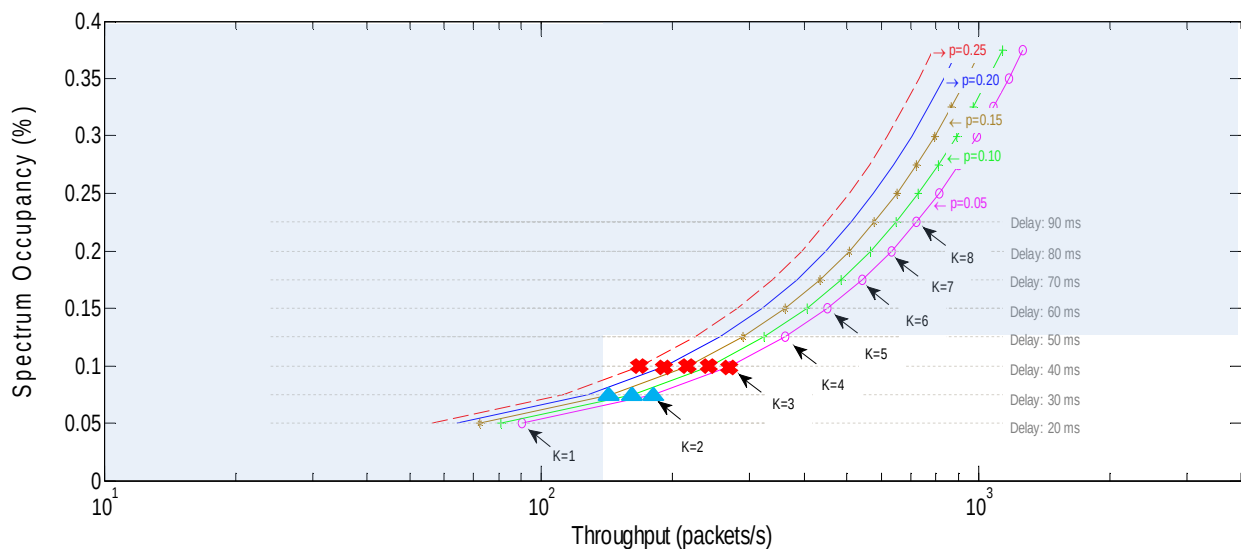


Figure 5.20. Aggregated SO versus network throughput in the fast lane. (Delay in the figure refers to D_x^{∞} and p refers to p_{per})

To conclude, this section has outlined a method to select the minimum number of fast channels while ensuring that the delay constraint is met and the SO (which is important for coexistence) is minimized. In addition, the fast lane concept has been shown to be effective in meeting the delay requirement with high probability of success, and is an important requirement for process control applications.

5.3.4. Overall Framework

The discussion presented in the previous few sub-sections has highlighted that the control loop execution rate (inclusive of sensors and controller execution cycle), the network induced delays, packet losses and the controller gain affect the overall control system performance. Mechanisms to address these have been presented. The overall performance of the control application depends on interaction and cooperation between network layers and field devices. The framework to improve the performance is summarized in Figure 5.21. In the figure the PHY is restricted to only 2.45 GHz band and the others supported by IEEE 802.15.4 standard are omitted. This PHY provides services such as RSSI and LQI which can be used to assess the wireless network performance. They will be explained in detail in the next chapter. For now, the argument is that the PHY offers adjustments to transmission power which can be used by the MAC layer to improve the probability of successful data delivery. Further, the MAC layer supports various features such as those highlighted in the figure. They are self-explanatory and can be adapted based on the network conditions to improve the network operations. The proposed shadow frame routing will be an example of adaption of MAC to network conditions. In addition, the NM can optimize the network operations to support low latency based on the ongoing network conditions and requires dynamic resource allocation. Furthermore, the control layer can adapt its control parameters (such as controller gain) or controller execution rate based on network status in order to improve the control performance. The recovered ID mechanism presented above resides at this layer and switches states based on network status.

To summarize, in this proposed framework the hierarchy is maintained between the communication layers. However, each layer adapts its configurable parameters based on the network status. This network status repository provides a common mean for

different layers to fetch information from other layers in the entire network stack. Each layer writes information about its configurable parameters and their current settings to this layer. As a result, the controller will adapt its parameters according based on the network status and if the network experiences bottlenecks then it will relax its update requirements. This will help to reduce the network burden and improve overall operations, because this time the control layer has an active participation in the network operations. Similarly, the layers below the control layers will adapt their parameters in order to deliver the required QoS to the control application.

5.4. Chapter Summary

This chapter has presented a case study involving the use of a wireless network for closing the control loops of an industrial furnace. A detailed examination of the limitation of an IEEE 802.15.4 network is presented in relation to the maximum supported update period. Further, scalability has been examined and the theoretical limits are analyzed. They help in identifying the processes which are suitable to be controlled over an IEEE 802.15.4 network.

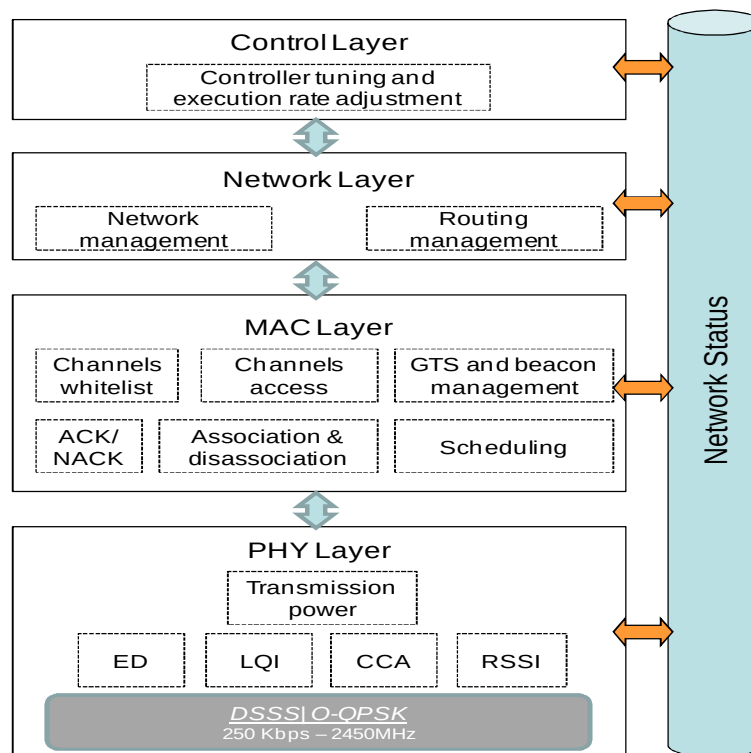


Figure 5.21. The layered model of interaction between different layers with information sharing via a common repository.

Moreover, a detailed examination of the control loop performance is presented and the effects of network induced delays, data losses and scheduling have been discussed. Based on this study a framework is proposed which can be used to improve the overall performance of the control application and requires collaboration between communication and control layers. The proposed framework is within the specifications of IEEE 802.15.4 network and can help reduce network delays and packet losses. This framework is about resource aware control and scheduling and optimises a wireless network by maintaining the control loop performance. The proposed method has been shown to be effective in addressing the impairments of a wireless network while delivering the required QoS to the control application.

CHAPTER 6

Transmission Power Control

The use of TPC can help address industrial issues concerning energy consumption, interference, fading and critical-data priority. However, the existing TPC algorithms are not designed for industrial applications with high interference and rapidly changing environment. Therefore, an algorithm is required which is tailored to meet industrial needs. The chapter begins by providing an overview of the industrial requirements concerning the use of TPC and the associated constraints which are found in industrial WSNs. The following section then introduces the system model. The model is used to formulate the problem and to identify the different parameters involved in TPC. To design a wireless data link, a key requirement is to ensure an adequate SINR at the receiver. A method to estimate the SINR is also presented based on the services available from IEEE 802.15.4 compliant radios. Later, the outcomes of empirical studies conducted to assess the link quality are presented. The results have highlighted that co-channel interference from co-habitated wireless networks affect the SINR and the received signal strength distribution. Therefore, an algorithm is designed for industrial applications based on these empirical findings and the literature review. The algorithm is then experimentally validated and the results are shown and discussed. Furthermore, it is shown that the proposed algorithm adapts to variations in link quality and is hardware-independent and practical.

6.1. Overview

The aim of this strand of research is to design an algorithm for TPC in industrial WSNs. The use of TPC is found in many applications such as fixed point-to-point networks, cellular networks and even short range Bluetooth networks. However, its use in short-range, low-power industrial strength wireless networks is new and has unique challenges. Within the framework of industrial standards, the provision for TPC is

included as part of the framework, but the details of its implementation are not specified in the standards. Therefore, it is an avenue of research.

6.1.1. Industrial Requirements

Chapter 1 provided a detailed breakdown of the objectives of this research. A review of link assessment techniques and available TPC algorithms were presented in Chapter 3.

The requirement for TPC is to estimate the minimum transmission power level which can deliver the required wireless link performance that ensures:

- Minimum overhead linked to TPC
- Adaptation to all channels and changing conditions
- Prevention of outage and is reactive
- Independence of hardware platform
- Working on pair-wise basis, to support topology-independency
- Adaptation to asymmetric links, varying transmission power levels and sensitivity threshold of the receiver.

These requirements are in-line with those identified in aims and objectives section of Chapter 1.

Requirements analysis

The designed TPC algorithm needs to ensure that it has light computational and communication requirements and can be implemented on standardized IEEE 802.15.4 compliant transceiver. The industrial standards such as WirelessHART supports frequency hopping on per packet basis, whereas ISA100.11a supports both slow and fast hopping (ISA, 2011). Therefore, a TPC algorithm needs to operate over all the available channels, a maximum of 16 in the 2.4 GHz band, and needs to adapt to the changing environment. Moreover, the algorithm has to ensure adequate link quality and needs to prevent outages. WirelessHART, ISA100.11a and WIA-PA support various topologies, ranging from simple star network to mesh networks. These were summarized in Chapter 2. Hence, a decentralised approach where TPC is implemented on pair-wise basis is important. As a result, each node will have its neighbour information stored in tables. For each neighbour and for all available communication channels, a set of minimum power levels are required to be calculated to ensure SINR.

To conclude, a TPC algorithm is required which can adapt to changing radio environment, is quick to respond, works on pair-wise basis to ensure topology-independency and autonomous operations, and is practical.

6.1.2. Constraints

The TPC algorithm has to operate under certain limitations, and they are summarized as follows:

Available transmission power

It depends on various factors such as:

- REGION SPECIFIC:

For instance in Europe, the total Effective Radiated Power, EIRP is -10 dBW (100mW). In addition, the maximum allowed power spectral density is -20 dBW (10 mW) per MHz, specified by ETSI EN 300 328 (2006).

- STANDARD SPECIFIC:

According to IEEE 802.15.4 (2006) the majority of the IEEE 802.15.4 devices are expected to operate with transmission power between -3dBm (0.5 mW) to 10 dBm (10 mW). The out-of-band emissions make it difficult to transmit above 10 dBm. The industrial standards are based on the IEEE 802.15.4 defined PHY. All devices in a WirelessHART network must support a nominal EIRP of +10 dBm (10 mW) and the transmission level has to be programmable from -10 dBm to +10 dBm (Chen et al., 2008). Modules from DUST networks are widely used in WirelessHART networks, and they offer an output transmission power of +10 dBm.

- HARDWARE SPECIFIC AND VENDOR SPECIFIC:

Furthermore, the commercially available IEEE 802.15.4 compliant transceivers offer different transmission power levels which can be selected. These power levels are often not uniformly distributed. The maximum and minimum selectable power level varies as well.

Therefore, the available transmission level is a limiting factor and the algorithm needs to adapt to each individual radio on which it operates.

Receiver sensitivity

- **HARDWARE SPECIFIC:**

As was highlighted in Figure 1.5, the minimum sensitivity of the receiver as defined by IEEE 802.15.4 standard is -85 dBm and the best case theoretical sensitivity can be -113.2 dBm. Therefore, receivers with improved sensitivity can be built which still comply with the IEEE 802.15.4 standard.

- **VENDOR SPECIFIC:**

Commercially available modules offer a sensitivity level better than -100 dBm. Therefore, it offers more than 15 dB margin in the link budget calculation. Having such a margin not only extends the coverage range of the data link but also provides a wider region in which the TPC algorithm can operate.

Power update

The periodic execution of a power control algorithm which involves both the transmitter and receiver to compute the required transmission power exerts an unnecessary burden on the network, especially if the radio is used exclusively for the purpose of power update. The frequent update of transmission power, such as in the case of W-CDMA where the inner loop is operated at 1500 Hz helps to maintain the signal to noise ratio at the specified value (Harri and Pederson, 2010). Such an approach will not be suitable for industrial WSNs because of limited shared radio bandwidth, limited available transmission power and receiver sensitivity.

Others

The other limiting factors include the selection of a metric which can be used for link quality assessment. The RSSI and LQI are two options, and will be explained in detail later. For now, it is worth to identify that LQI is implementation specific. Other limiting factors include: number of available channels, communication distance, antenna types, required reliability and link margin, and co-channel interference.

6.2. System Model

In this section, a system model is presented which identifies the factors which are to be considered during formulation of the algorithm.

6.2.1. Terminology

Useful definitions needed for the following text include:

- RECEIVED SIGNAL STRENGTH INDICATOR (RSSI):

RSSI provides an estimate of the received signal power in the transmission channel, and is calculated over 8 symbol periods (Srinivasan and Levis, 2006). It is the RF power input to the receiver (Helen and Stengel, 2005) given by Equation 6.1 (Hossian *et al.* 2009). S represents signal power, I is the total interference power, n is the noise power, and I_m is the interference from interferer number m . M is the total number of interferers. Time index is omitted for simplicity.

$$\text{RSSI} = 10\log(S + I + n) \quad \text{Equation 6.1}$$

$$I = \sum_{m=1}^M I_m$$

- LINK QUALITY INDICATOR (LQI):

LQI is a metric of link quality. It may be implemented using receiver energy detection, SNR estimation, or a combination of these methods [Shan Lin *et al.*, (2006) and AD (2010)]. In case of CC2420 radio chip from Texas Instruments, it is measured as a chip error rate (Chipcon, 2006). The standard does not specify how the LQI is to be obtained. The range of the reported value has to be between 0 and 255 (IEEE 802.15.4, 2006). Some commercially available chips map LQI to SNR (Chipcon, 2006).

- PACKET RECEPTION RATE (PRR):

PRR is the average of the ratio of number of received packets to those transmitted. It is a metric of link quality estimation [Lee *et al.* (2010)], and is obtained over a long period of time.

- SIGNAL TO NOISE RATIO (SNR):

It is the ratio of strength of desired signal to noise. It is expressed in dB, and is given in Equation 6.2 (Hossian *et al.*, 2009).

$$\text{SNR} = 10\log(S/n) \quad \text{Equation 6.2}$$

- SIGNAL TO INTERFERENCE AND NOISE RATIO (SINR):

It is the ratio of desired signal to interference plus noise. It is given in dB by Equation 6.3 (Hossian et al., 2009).

$$\text{SINR} = 10\log(S/I + n) \quad \text{Equation 6.3}$$

6.2.2. Problem Specification

It was identified in Chapter 1 that the signal power at reception is a result of gains and losses incurred in wireless link from transmitter to receiver. In addition to link gains and losses, the transmitted signal is subjected to interference and noise, and the final value of the signal power is reported as RSSI to the receiver. It is depicted in Figure 1.1.4. Moreover, the uncertainty in this measured value is hardware specific.

The requirement is to calculate the transmission power which can ensure a specified SINR at the receiver. This value has to be calculated while taking into consideration the link gains and losses, and also the constraints identified in Section 6.1.2. Therefore, it requires link budget analysis. Further, the transmitted power has to be calculated and selected from available power levels for each pairing neighbor and for all available channels.

Moreover, the algorithm has to compensate for interference. In general, a high value of RSSI is considered a sign of good link. However, a constructive interference from a co-channel interfere, like Wi-Fi, can cause a false increase in this value. This can compromise the network performance. Hence, it needs to be compensated for. In short, the RSSI value if used independently as a link quality estimator may not serve as a good estimate for channels which are subjected to higher interference.

Finally, the algorithm needs to adapt to varying channel conditions. Based on the user input, for instance, the reliability required from the link, the transmitted power needs to be adjusted such that the received SINR is greater than the threshold specified by the user. This can be achieved either by using statistical models or empirical data collected from the deployment. Next, a technique to estimate SINR and SNR is presented.

6.2.3. SINR and SNR Estimation

Empirical data can be used to estimate the SINR and SNR. It is assumed that the main source of interference is a co-existing Wi-Fi network (Shin et al., 2007). The IEEE 802.15.4 channels whose frequencies overlap with the Wi-Fi network are referred to as in-band channels and those which do not overlap are called out-of-band channels. The use of Wi-Fi channels is often limited to three channels as adjacent Wi-Fi channels in 2.4GHz band overlap (Enstad, 2009). This further simplifies the process of identifying in-band and out of band-channels. The amount of interference caused to in-band channels by a Wi-Fi network will depend on network traffic. However, the beacons are broadcast at regular intervals by a Wi-Fi network and will result in a constant source of interference. Equation 6.1 can be used to obtain the approximation presented in Equation 6.4 below, given that there is no interference. Here IB represents In-Band and Si represents Signal. A bar above e.g. $\overline{IB}$ means an out-of-band channel, which is not affected by interference. Furthermore, as the IEEE 802.15.4 compliant devices provide a mechanism to perform Clear Channel Assessment (CCA), they can be used to detect the energy present in a channel (Chipcon, 2008). The CCA modes along with RSSI register can be used to obtain the approximations presented in Equation 6.4 to 6.6. Without signal transmissions, in-band assessment results in Equation 6.5, and out-of-band is represented by Equation 6.6. Here, the Channel Energy Indicator (CEI) acronym is used instead of RSSI, because RSSI is only associated with the signal. In the absence of signal, channel energy can still be quantified. Periodic sampling of the radio channel in the absence of signal will help to quantify the noise power. Hardware linked noise power varies with temperature. However, it is quite stable over time periods of seconds or minutes (Srinivasan et al., 2010). Therefore, the most frequently recorded reading of channel energy in the absence of IEEE 802.15.4 packet is used as a noise floor of the node. In literature, various terms are used to denote the noise floor, such as SSI_{noise} and SSI , refer to Hauer et al. (2009) and Srinivasan et al., (2006) for further details.

$$RSSI|_{\overline{IB}, Si} \approx 10\log(S + n) \quad \text{Equation 6.4}$$

$$CEI|_{IB, \overline{Si}} \approx 10\log(I + n) \quad \text{Equation 6.5}$$

$$CEI|_{\overline{IB}, \overline{Si}} \approx 10\log(n) \quad \text{Equation 6.6}$$

Using an average RSSI, the following can be computed. Subtracting Equation 6.5 from Equation 6.1 gives an estimate for SINR as shown in Equation 6.7.

$$\begin{aligned} \text{SNR}_{\text{estimation}} &= 10\log(10^{(\Delta\text{RSSI}_i/10)} - 1) & \text{Equation 6.7} \\ \Delta\text{RSSI}_i &= \text{RSSI}|_{IB, Si} - \text{CEI}|_{IB, \bar{S}_i} \end{aligned}$$

These values are directly derived from the RSSI value reported by the receiver. Further subtracting Equation 6.6 from Equation 6.4 gives an estimate for SNR as in Equation 6.8.

$$\begin{aligned} \text{SNR}_{\text{estimation}} &= 10\log(10^{(\Delta\text{RSSI}/10)} - 1) & \text{Equation 6.8} \\ \Delta\text{RSSI} &= \text{RSSI}|_{IB, Si} - \text{CEI}|_{IB, \bar{S}_i} \end{aligned}$$

These estimates are based on empirical data, and can be approximated using same PRR test conducted over multiple channels. The Clear Channel Assessment (CCA) modes supported by the IEEE 802.15.4 standard can be used to estimate the energy present at the channel [Srinivasan et al. (2010) and IEEE802.15.4 (2006)]. These estimates along with the RSSI tracking will assist in the formulation of a TPC algorithm which can ensure that the received SINR is above the threshold specified by the user.

6.3. Empirical Studies on Link Quality Assessment

This section provides the outcome of an empirical study conducted and the performance analysis of a wireless link. All experiments are conducted using CC2430 wireless sensor nodes which employs CC2420 radio from Texas Instruments. Only RSSI values are used in this study, as they are specified by the standard and are available upon successful reception of each data packet. The purpose was to observe the trend seen in reported RSSI values in different channels and the results are needed to formulate an industrial strength TPC algorithm.

6.3.1. Hardware Implementation and Experimental Setup

All experiments are conducted using CC2430EM. These evaluation modules comply with the IEEE 802.15.4 standard and are used to study its performance. Further, they are compatible for use with the SmartRF04EB board. Refer to Panel 6.1 for details.

The transmission power of the radio transceiver was controlled by adjusting the radio parameters. On successful reception of a packet at the destination, a corresponding RSSI value is reported by CC2420 radio. The routines written to conduct the evaluation test

CC2430EM:	A system which incorporates a microcontroller and a transceiver based on CC2420 radio (Chipcon, 2008).
CC2420:	A wireless transceiver which complies with IEEE 802.15.4 standard (Chipcon, 2006).
SmartRF04EB:	An interface board used for programming, evaluation and connecting CC2430

Panel 6.1. Details of the hardware used.

and the network access are all handled by the CC2430EM module. The module was used in conjunction with the SmartRF04EB board which connects the module to the computer.

Figure 6.1 (a) shows the experimental setup and Figure 6.1 (b) shows the spatial distribution of wireless transceivers during experiments. The experiments involve the use of a pair of CC2430EM modules along with the evaluation board, SmartRF04EB. The boards are further connected to the laptop computer where the data is generated and logged in Matlab using Real-Time Windows Target toolbox.

In the experiment, the transmitter was programmed to send 3600 packets over a particular channel with given transmit power level to the receiver. The PRR was calculated at the receiver along with the archiving of RSSI values. The same experiment was repeated for another power level within the same channel. Once the available power levels were evaluated, the same procedure was repeated for another channel. The same practice was repeated for different locations of the receiver.

6.3.2. Results and Performance Analysis

The outcome of the experiment described in the previous section is presented here. Figure 6.2 (a) shows the spread observed in RSSI values during the experiment with varying transmission power and altering channels. It can be noticed that the spread in RSSI values changes from channel to channel and also depends on the transmission power. Figure 6.2 (b) shows the linear approximation of the data shown in Figure 6.2 (a). The same experiment was repeated later in which the receiver was placed at three different locations, where the difference between these locations was 2 meters. The result of this experiment for channel 15 is shown in Figure 6.3. It is noted here that as the distance increases, the path loss increases and as a result the linear approximation line shifts downwards.

In the results shown in Figure 6.2, it was observed that the average RSSI values recorded in Channel 24 were generally higher compared to the others. For one particular location, with same hardware and setup, and with the same environment such an increment needs to be justified. According to the Friis free-space path loss equation, an increase in frequency should result in higher path loss (Labrador and Wightman, 2009). Therefore, the difference in frequency from channel to channel is not the main contributor for this outcome.

Interference

Within the same vicinity where the experiment was conducted, an activity was recorded in Wi-Fi channels. A Wi-Fi network scanner referred to as NetSurveyor available from NaN (2011) was used as a diagnostic tool to monitor the activity. The outcome of a Wi-Fi network scan at location R1 is shown in Figure 6.4. In the figure, the heatmap panel is a representation of the data where channels are marked along the x-axis, the y-axis is a time scale and indicates the last 60 sweeps, and the z-axis is the colour scale. The horizontal lines in the heatmap panel display the percentage of maximal throughput for each channel measured over the time period of one scan. The panel underneath, the channel spectrogram is a 3D plot of 802.11 channels as a function of time where each channel is represented by its own set of bar graphs. The outcome signifies that channels 1, 6, 10 and 11 are in use by a cohabitated Wi-Fi network. Channel 11 in Wi-Fi overlaps with Channel 24 in the experimental system. Also, the highest activity was recorded in channel 11. Therefore, a considerable amount of interference is expected from IEEE 802.11 network.

Overlapping channels

The same 2.4 GHz ISM spectrum is used by Wi-Fi (IEEE 802.11) network as is used by IEEE 802.15.4 network. The channel numbering, bandwidth and centre frequency varies between these networks. On one hand, in an IEEE 802.15.4 network the channel bandwidth is 2 MHz and channel spacing amongst adjacent channels is 5 MHz. These channels do not overlap. On the other hand, an IEEE 802.11 channels overlap and the recommendations for the use of non-overlapping channels vary in different regions, and are highlighted in Figure 6.5. Further, the channel bandwidth also varies from 22 MHz in the case of IEEE 802.11b networks and up to 40 MHz in the case of IEEE 802.11n networks. Therefore, based on the channel usage spectrogram presented in Figure 6.4

and the physical relationship between the channels of these two networks presented in Figure 6.5, it is identified that other than channel 15 all other channels are likely to be influenced by Wi-Fi interference.

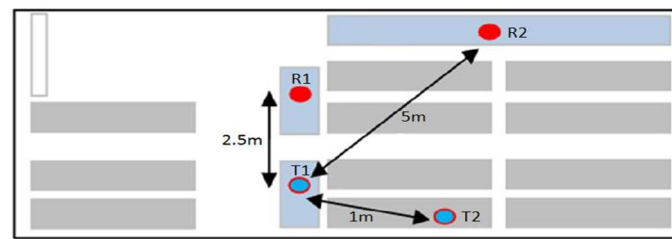
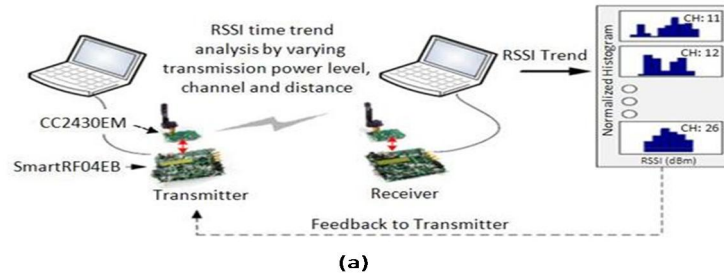


Figure 6.1. (a) Experimental setup and (b) spatial distribution of transmitter and receiver, not drawn to scale. The grey region represents the office cubicles, whereas blue regions are planes above those cubical with Line of Sight (LOS).

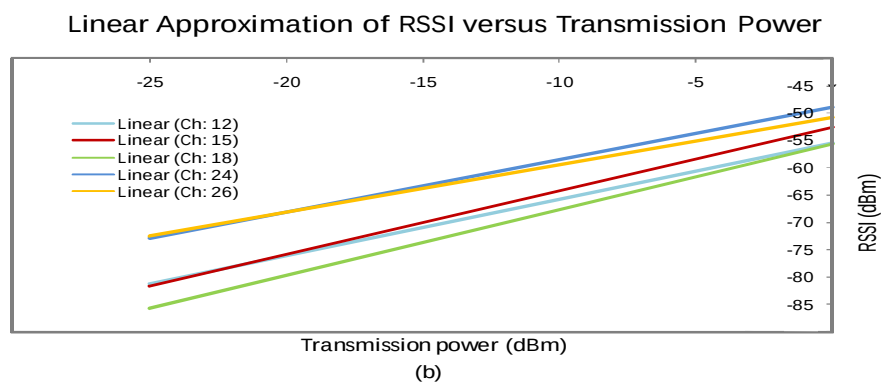
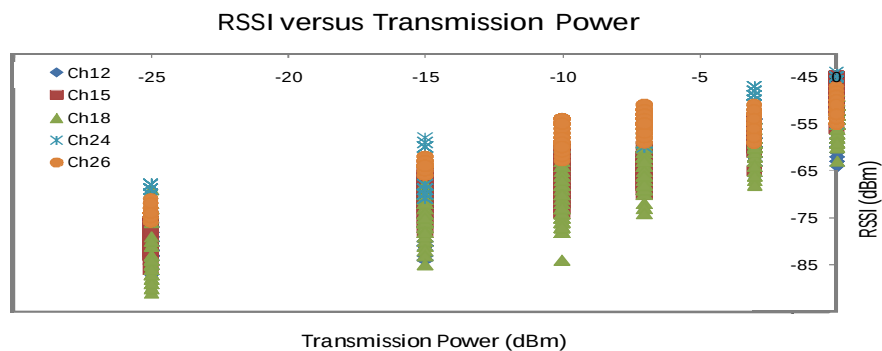


Figure 6.2. (a) RSSI distribution versus transmission power between T1 and R1, and (b) linear approximation of data presented in (a).

Linear Approximation of RSSI versus Transmission Power

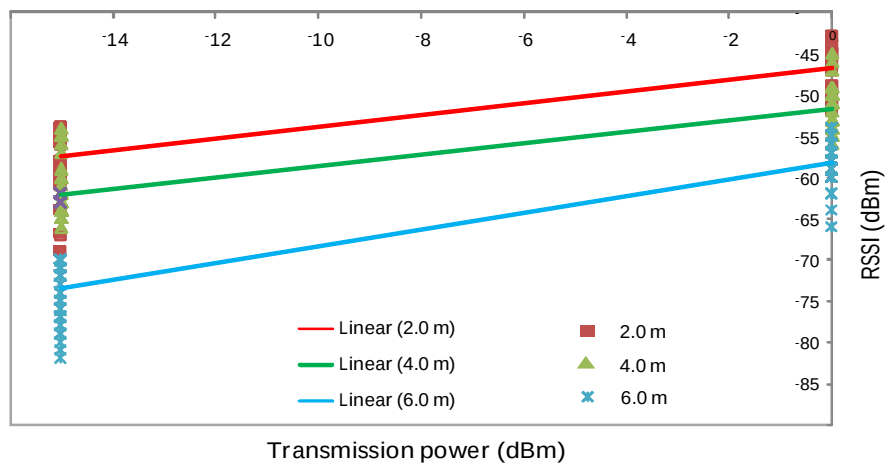


Figure 6.3. RSSI distribution versus transmission power of Channel 15 over varying distance.

Up to this point, it is shown that the Wi-Fi channel activity coincides with that of channels used by the IEEE 802.15.4 networks shown in Figure 6.1(b) with the exception of channel 15. For the plots where higher RSSI values are recorded in IEEE 802.15.4 packets shown in Figure 6.2, it is considered to be linked to interference. In order to analyze the effect of interference on the RSSI trend, comparative plots of normalized histograms are plotted in Figure 6.6. Here, channel 15 is selected as it is out-of-band channel which is not subjected to the Wi-Fi interference. Further, channel 24 is selected as it overlaps with the channel 11 of Wi-Fi.

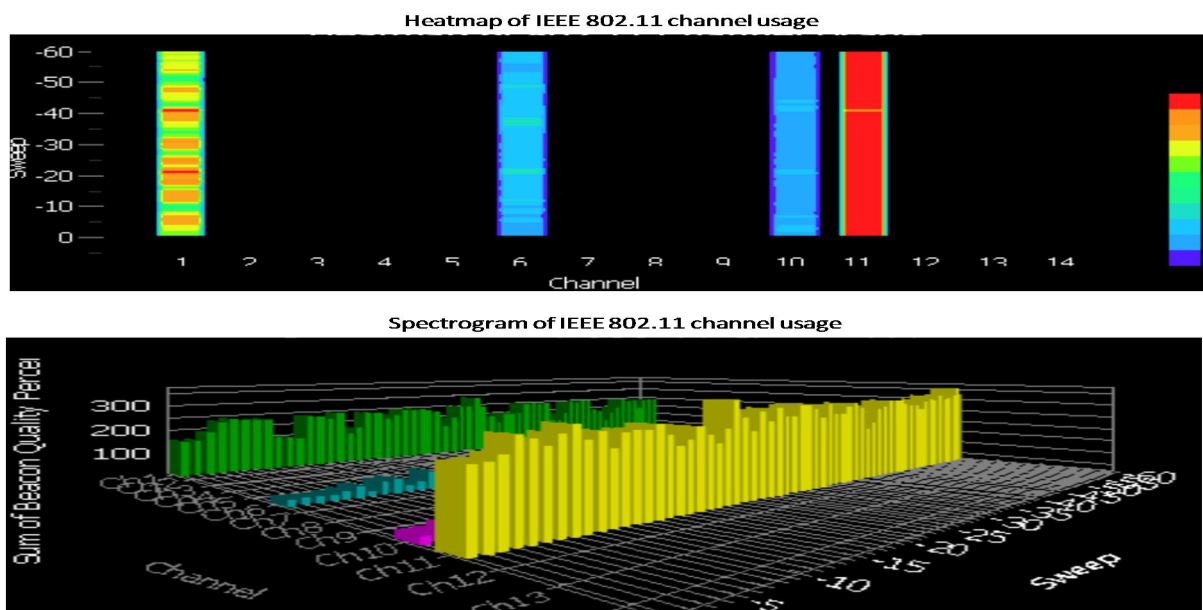
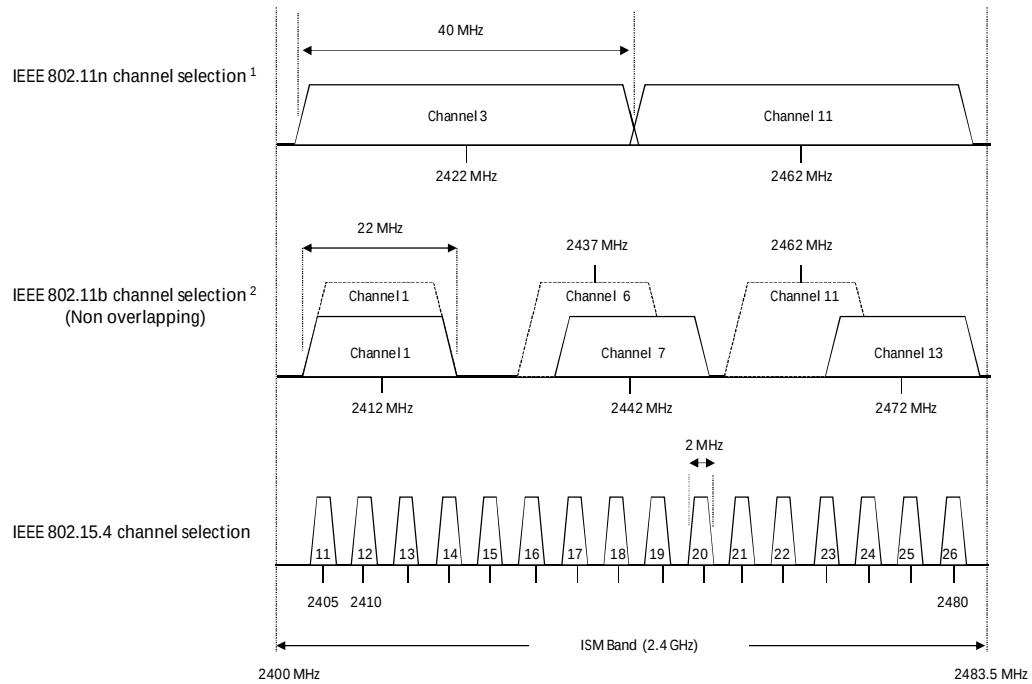


Figure 6.4. Heatmap and the spectrogram of activity recorded in IEEE 802.11 channels at location R1.



¹
²

In 2.4 GHz and 5 GHz frequency band each channel is approximately 20 MHz. Two adjacent channel can be bonded to get a bandwidth of 40 MHz .
 Recommended North American channel selection: Channel 1,6,11.
 Recommended European channel selection: Channel 1,7,13.

Figure 6.5. IEEE 802.15.4 channels and the recommended selection of IEEE 802.11 extension networks.

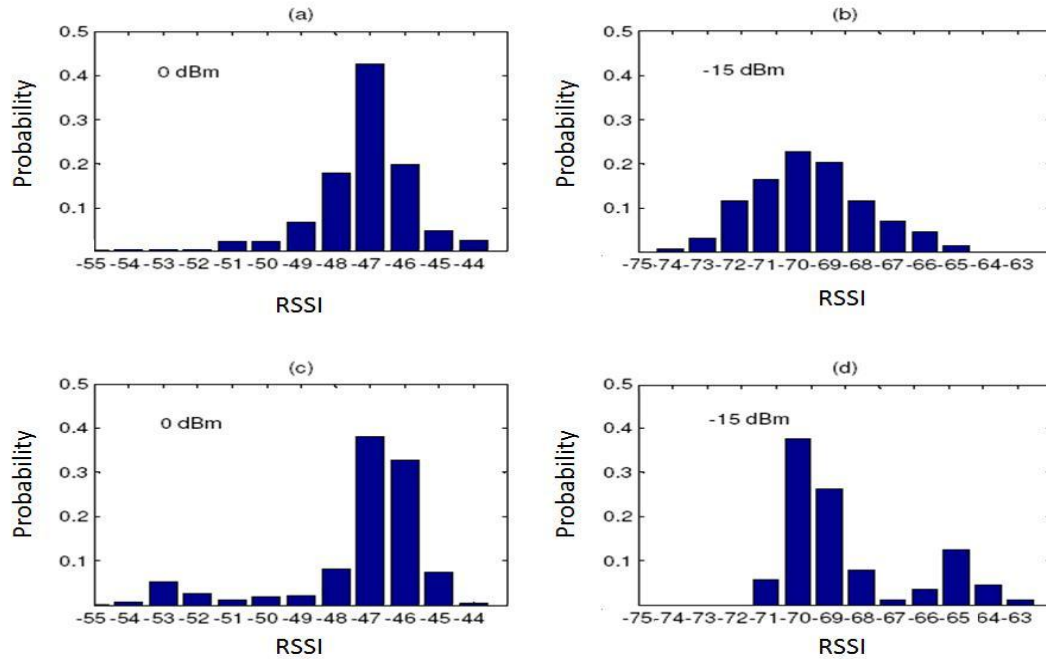


Figure 6.6. RSSI distributions for channel 15 are shown in (a) and (b), whereas for channel 24 are shown in (c) and (d). Power levels are indicated in plots.

Impact of Wi-Fi

The plots in Figure 6.6 represent the distribution as observed under Line-of-Sight (LOS) conditions. It can be seen that channel 15 which is outside of interference zone follows a Gaussian like distribution, whereas, channel 24 can be represented as a bimodal distribution. The reason for this behavior is explained as follows.

The received signal is represented as RSSI. This value comprises of received signal power, noise power and interference. During the PRR test the packets were generated periodically at the transmitter, and at the receiver the RSSI values were recorded. Based on the recorded values of RSSI, the distribution can be represented as a random variable having a probability function represented by $f_R(x)$. Here, it is assumed that the empirical distribution of collected packets is large enough to be statistically represented by $f_R(x)$. Further, it is assumed that Wi-Fi traffic bursts are shorter in duration compared to the symbol period used in the calculation of RSSI by IEEE 802.15.4 receiver. Further, if N_{PRR} packets are collected while conducting the PRR test, then it is assumed that only N_{PRR-i} packets are compromised by Wi-Fi interference, while the rest are not. This is also justified because of intermittent nature of Wi-Fi operations. Therefore, the probability that an interfering signal is present is given by $p_i = N_{PRR-i} / N_{PRR}$. Considering the interference from one source this can be expressed as Equation 6.9 (Khaleel *et al.*, 2009):

$$f_R(x) = p_0 f_0(x) + p_i f_i(x) \quad \text{Equation 6.9}$$

$f_0(x)$ and $f_i(x)$ in Equation 6.9 represents received signal distribution in the absence and presence of interference respectively. Therefore, it is a cause for bimodal distribution. In the presence of multiple sources of interference, multi-modes will appear in distribution.

A similar trend has also been reported by Khaleel *et al.* (2009), where it was identified that with higher Wi-Fi traffic rates the interference energy is higher and the probability of malfunctioning increases.

Additionally, if a channel is scanned to identify energy in the radio channel than a third peak can be visualized in Equation 6.10. This third peak will be linked to the noise floor, which will identify the minimum energy present in the receiver's front end matched

filter, and is calculated using noise power spectral density and receiver noise bandwidth. However, in the case of received packet this noise power will be embedded in the reported RSSI of the packet.

Wi-Fi interference at R2

The same experiment was later repeated after relocating the receiver. The receiver was moved to R2 and the transmitter was kept at T1. The outcome of the Wi-Fi channel scan is shown in Figure 6.7. It was noted that the same channels as those found in R1 were detected in location R2. However, the overall channel utilization was comparably higher at this instance in time. The outcome of the experiment is summarized in Table 6.1.

It is noted that the channel 15 distribution is concentrated within a confined region with low standard deviation, whereas, other channels have higher deviation linked to both constructive and destructive interference from IEEE 802.11 signals. Again, channel 24 has reported a higher mean in recorded RSSI value.

The results shown so far were observed under LOS conditions. Next, the results for non-LOS (NLOS) experiments are summarized in Table 6.2. It is observed that as the distance increased, the spread as observed also increased and the difference between the two channels narrowed.

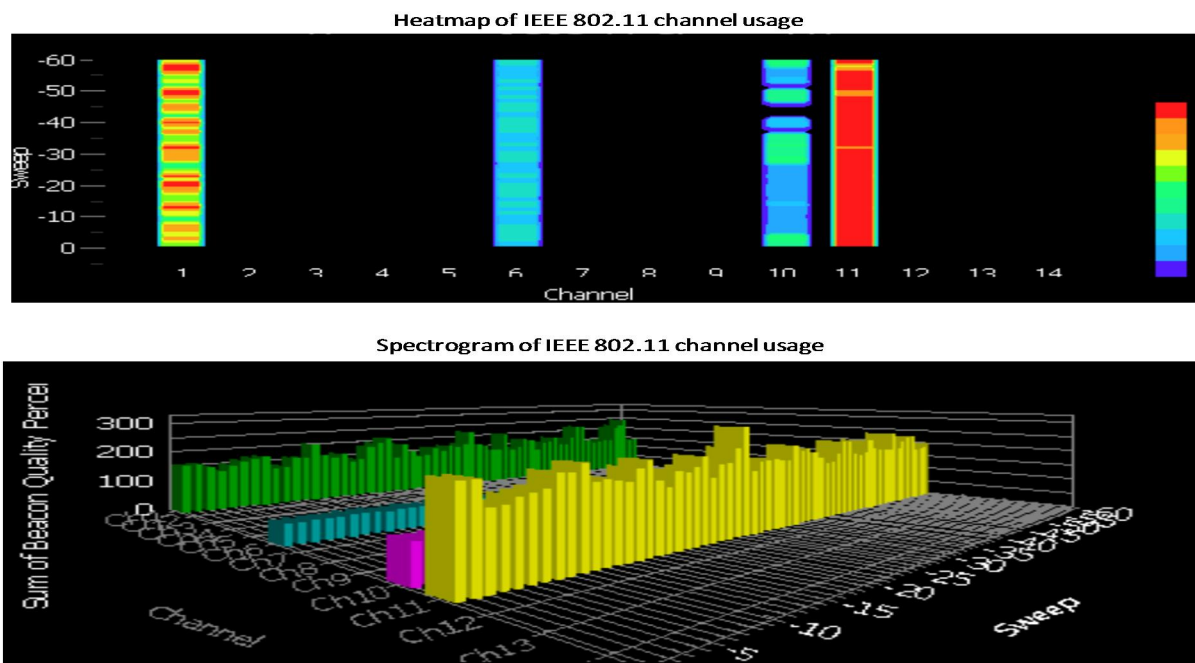


Figure 6.7. Heatmap and the spectrogram of activity recorded in IEEE 802.11 channels at location R2.

Table 6.1. Summary of RSSI distributions for various channels under LOS conditions and with T1 and R2 installations.

Channel	Mean RSSI (dBm)	Standard deviation
15	-53.1	0.96
22	-56.8	1.88
23	-54.6	1.40
24	-46.7	1.36
26	-51.5	1.06

Table 6.2. Summary of RSSI distributions for NLOS conditions with transmitter at T2 operating at 0 dBm.

Receiver location	Channel	Mean RSSI (dBm)	Standard deviation
R1	15	-58.6	3.22
R1	24	-54.5	1.60
R2	15	-69.5	5.12
R2	24	-68.3	4.72

The results show that RSSI varies from channel to channel. It is affected by the transmission power, link losses, noise power and also the interference. The investigation into the impact of Wi-Fi on IEEE 802.15.4 network has highlighted that it can result in both constructive and destructive interference. The discussion in this section has primarily focused on the constructive interference. It is so because a higher RSSI is often considered a sign of good link quality even though it may lead to a low SINR. On the other hand, lower RSSI values are handled by the TPC algorithm. The key findings can be summarized as follows:

- An RSSI is a good link quality indicator if the network is subjected to only noise power.
- Under the same transmission power and experimental setup the reported RSSI varies from channel to channel.
- In the case of interference from Wi-Fi, it may lead to a false increase in reported RSSI which can affect the network performance.
- The impact of Wi-Fi on the IEEE 802.15.4 network has resulted in a bimodal distribution. In the presence of multiple interferes it will result in multi-mode distribution.

- Further, the effect of this interference cannot be ignored if RSSI is used to estimate SINR.

6.3.3. Characterizing RSSIs

The TPC algorithm uses the mean, mode, maximum, minimum values of the RSSI and CEI distributions. The experimental results in the previous section show that the RSSI distributions are not necessarily simple Gaussians and, therefore, the algorithm requires an empirical estimate of the distribution. A TPC algorithm will sample RSSI values for a period of time and construct a sampled distribution from the measured values as an estimate of the true distribution.

In order to determine how many packets are needed to estimate the RSSI distribution, a statistical measure referred to as KLD is used. It quantifies the difference between two distributions. The method was introduced in Chapter 4.

The method requires a reference distribution to represent the true distribution of RSSI values. The best empirical approximation to the reference distribution is when a large amount of data has been collected. In this work, the reference distribution was determined from 4000 packets. The estimated RSSI distribution for comparison was then computed using fewer consecutive received packets. For both channels and for LOS and NLOS conditions, the average KLD stabilized after 1000 packets, as is shown in Figure 6.8. This result suggests that 1000 packets will be adequate for estimation of RSSI in a TCP algorithm.

To summarize, the RSSI distribution trend as observed depends on communication channel, distance, operating spatial environment, relative distance to interfering source, and on the transmission power. The effect of interference resulted in bimodal distribution due to fluctuation of two mean RSSI values. In addition, for channels without interference, the distribution followed a Gaussian like distribution.

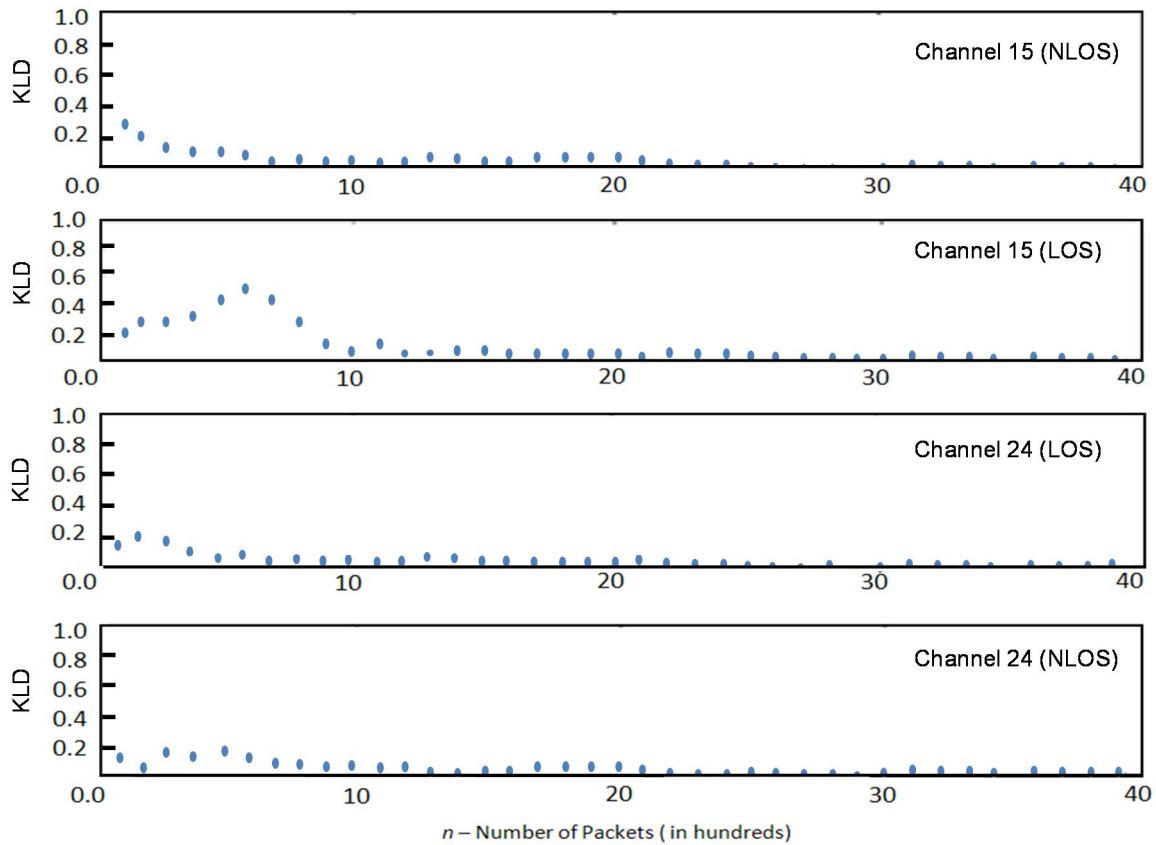


Figure 6.8. KLD with respect to final distribution versus number of packets.

6.4. Design of TPC Algorithm

This section proposes a TPC algorithm for industrial strength wireless network which is built on empirical studies, is adaptive, supports multi-channel operations and has light computational and communication requirements.

The distributed nature of industrial wireless instruments and mesh networking requires a decentralized approach for TPC. It should be vendor independent as well. Therefore, the algorithm has two key requirements:

- It should be executed pair-wise between two nodes at a time.
- It should track the link quality using RSSI rather than the vendor-specific LQI.

6.4.1. Overview of the Algorithm

The algorithm provides feedback control to maintain SINR at a reference value by adjustment of the transmission power level. Its main features are:

- Estimation by the receiving node of the SINR or SNR of the communications link making use of Equations 6.7 and 6.8.
- Computation of the transmission power level required for achieving the reference SINR value.
- Generation by the receiving node of a TPC command.
- Feedback of a TPC command from the receiver to the transmitter. The aim of the feedback is to reduce the transmission power to the lowest value which gives adequate SINR.

Detailed steps in the algorithm include:

- Modeling the relationship between RSSI and transmission power at the receiver.
- Building a TPC table in the transmitting node.
- Making a TPC decision in order to determine the TPC command to be fed back to the transmitter.
- Adjustment of the transmission power level in the transmitter by means of a power update controller.

6.4.2. Building the TPC Table

As shown in Figure 6.2(b) and Figure 6.3, the relationship between the transmission power and the RSSI is linear, as has also been observed by others [Srinivasan et al. (2010), Srinivasan, K. & Levis, P. (2006) and Shan Lin *et al.* (2006)]. To build the TPC table, it is important to model this linear relationship by means of a straight line fit. This model will be used to find the lowest value of transmission power required that will achieve the desired RSSI and, consequently, the reference SINR. The algorithm establishes a TPC table during network setup making use of the beacon packets which are transmitted periodically to announce the presence of the network. The table provides a relationship between transmission power and RSSI for all available communication links and channels. When a node has to transmit a packet it consults the TPC table to identify the minimum transmission power required for communication with a specific node.

As each node may offer different levels of transmission power, let that be denoted by a vector $\mathcal{TP}_A$, where element τ_i represents a discrete transmission power available at node A denoted by index i . N is the total number of available power levels.

$$\mathcal{TP}_A = \{\tau_1, \tau_2, \dots, \tau_N\}$$

The PRR test is conducted by varying the transmission power starting from the maximum power level and proceeding towards lower transmission levels and recording the RSSI values and the outcome of PRR test are represented by R_B and PRR_B respectively.

$$\begin{aligned} R_B &= \{r_1(\tau_1), r_2(\tau_2), \dots, r_N(\tau_N)\} \\ PRR_B &= \{prrr_1(\tau_1), prrr_2(\tau_2), \dots, prrr_N(\tau_N)\} \end{aligned}$$

As the R_B for each transmission power will lead to a distribution, this vector can represent the average, maximum, or minimum RSSI values as recorded. The outcome of PRR test will specify as to when to abort the initialization process. Further, as between each neighbor up to 16 channels may be available, a matrix can be formulated using Equation 6.10.

$$R_B(k, \tau_i) = a_k \tau_i + b_k \quad \text{Equation 6.10} \\ 11 \leq k \leq 26$$

Here, k represents the channel number as defined by IEEE 802.15.4, and a_k and b_k are parameters describing the linear relationship between R_B and τ_i . A corresponding matrix is built and stored for all available pairs of nodes. The values are estimated at the receiver node. These matrices are used to determine the transmission power required to yield a specific RSSI value at the receiving node. The values are conveyed to the transmitter where they are stored in the TPC table inside the Power Update Controller shown in Figure 6.9.

Once the TCP table is in place, the TCP algorithm can select a suitable transmission power level for detailed evaluation. This requires a minimum of 1000 packets per channel to determine the mean, mode, maximum and minimum RSSI values. The mode is the RSSI value corresponding to the largest peak in the distribution.

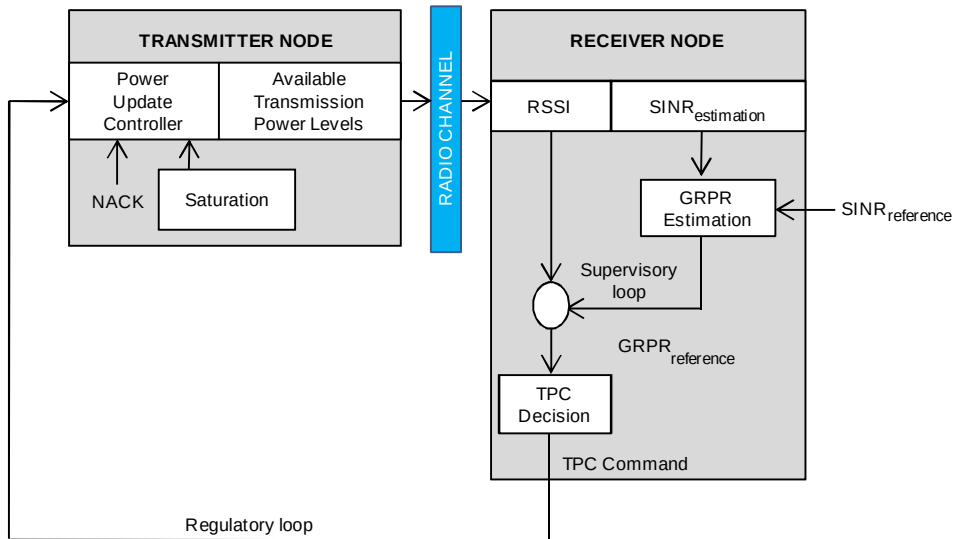


Figure 6.9. Illustration of TPC loops.

6.4.3. Estimation of Golden Receive Power Range

Figure 6.9 presents the proposed TPC system. The receiving node estimates the SINR values for specified channels over a given period of time. The desired RSSI value is determined which can ensure good link quality based on the estimated and reference SINR values, and the fade margin. Fading refers to the variation which a communication signal experiences due to interference arising from multipath propagation, and fade margin is a design margin where transmissions are sent at a higher power level to overcome fading. In the proposed algorithm, the range (max – min) of the RSSI as recorded between a pair of nodes is used in a fade margin calculation.

The proposed TPC algorithm adapts a concept from Bluetooth which specifies a range of RSSI values within which the operation of a pair of nodes is considered optimal (Lanzisera, *et al.*, 2007). This range is fixed in Bluetooth, whereas in this proposed algorithm this range is not fixed. It is estimated for each link and is dynamically adjusted. This range is referred here as Golden Receive Power Range (GRPR) and is estimated at the receiver. Based on the estimated SINR and SNR values obtained from Equations 6.7-6.8, the receiving node determines two threshold values: an upper threshold G_U , and lower threshold G_L for each link. Here G_L is estimated such that the received RSSI can ensure the minimum required reference SINR under channel fading conditions and G_U represents the expected RSSI at the receiver without signal fading. In the SNR calculation the mode of CEI distribution is used as noise power, whereas, in the case of SINR the mode of the distribution with the highest recorded CEI is used as a sum

of noise and interference power. GRPR values have to be above the receiver sensitivity. It is this value of G_U which is used to determine the required transmission power. Within the estimated GRPR, the operation of the transmitter is considered to be optimal and requires no further control action. If the recorded RSSI at the receiver is outside the GRPR then the transmission power level must be adjusted. The uncertainty in the recorded RSSI value at the receiver is linked to the receiver module. It is currently ignored in this formulation. If, however, the receiver is operated near the sensitivity then an additional margin can be added to the G_L value which is equivalent to the receiver uncertainty.

As a result the estimated GRPR will ensure minimum required SINR across all channels. For channels which are affected by Wi-Fi their GRPR will be different to those without interference. In particular, the values of G_L and G_U must both be set higher in channels with Wi-Fi interference. The bias added to the GRPR thresholds in channel i is $Pk_h(RSSI_i) - Pk(RSSI_j)$, where the Pk function returns the RSSI value at the peak of the distribution. Pk_h is the peak in a bimodal distribution with higher RSSI, i represents a channel with interference and j represents a channel known to be free of interference. If a channel without interference is not known then the mode of distribution of channel with interference can be used. As was seen in Figure 6.6, these values were similar. In general, if channels without interference are not known then all channels will be assumed to be prone to interference. The RSSI distribution formulated while conducting the PRR test can then be used to identify the channels which are affected by interference.

6.4.4. Setting the Transmission Power Level

The transmitter as shown in Figure 6.9 aims to match the actual power of its transmitted signal to the required transmission power level determined at the receiver. Feedback is expected from the receiver if the RSSI value goes outside GRPR. The transmitter then adjusts the transmission power value accordingly. However, there are limitations imposed by standards and the hardware. The minimum and maximum transmission power levels are indicated by the saturation block in Figure 6.9. Moreover, only limited numbers of discrete power levels are available in the transmitter, and are

dependent on the hardware. The available transmission power level which is nearest to the wanted value is to be selected.

The supervisory loop in the receiver node identifies the GRPR, as discussed. The objective of the regulatory loop between receiver and transmitter is to ensure that the RSSI value reported at the receiver is within the range of the GRPR. The supervisory loop needs to be executed only when the communicating nodes are relocated or when new interfering nodes appear. For a fixed installation, the SINR estimations and linear approximations are found to change only slowly. The regulatory loop is sufficient to compensate for changes in the link quality during normal operation.

There is a further procedure in place to address negative acknowledgment (NACK). NACK is information provided in the IEEE 802.15.4 transmission protocol. If NACK is active, it means the receiving node did not acknowledge the receipt of the transmitted packet. The usual action is to send the packet again, but persistent NACKS might indicate the presence of new interference source or the relocation of communicating nodes. The response is an increase in transmission power while the TPC tables are updated.

To summarize, the objective of the regulatory loop between receiver and transmitter is to ensure that the RSSI value reported at the receiver is within the range of the GRPR, while the supervisory loop updates the GRPR range which depends on the reference SINR value. The supervisory loop needs to be executed once the communicating nodes are relocated or when new interfering nodes appear. For a fixed installation, the SINR estimations are quite stable. Therefore, during normal operations only the regulatory loop is of interest and it compensates for any changes observed in the link quality.

6.4.5. Procedure of TPC

A detailed procedure for implementing TPC is highlighted in this section. Figure 6.10 illustrates the working of TPC algorithm. There are two stages involved in this process as specified in panels (a) and (b). The first process is about estimating the GRPR and building the TPC table, and is outlined in Figure 6.10(a), and is referred to as *initialization phase* of the TPC algorithm. The second process is referred to as *operational phase*, which is about steering the output of the transmitter such that the

received RSSI at the receiver is within the GRPR; its block diagram is shown in Figure 6.10(b).

The detailed description is as follows:

Initialization phase

- **USER INPUTS:**
 - k : List of all available channels for use in IEEE 802.15.4 network. In the case of WirelessHART, 15 channels are allowed. Some of these channels may even be blacklisted. Therefore, the user needs to specify the number of channels which are considered good for use, referred to as *whitelist* of channels.
 - $\mathcal{T}P_A$: Specifies the transmission power levels available for selection at the transmitter node.
 - PRR_{approx} : The criteria to conduct the test for approximating the linear relationship between RSSI and transmission power. It is a data structure which includes the following information:
 - The required PRR, $aPRR_{req}$.
 - The period of packet transmission, $aPRR_{Ts}$.
 - The number of packets to be transmitted, $aPRR_n$.
 - $k_{interference}$: The IEEE 802.15.4 channels which are effected by a cohabited Wi-Fi network.
 - $SINR_{req}$: The required signal to interference and noise ratio.
 - R_{sen} : The receiver sensitivity of the module in use.
 - $PRR_{validation}$: The same data structure as was highlighted in the case of PRR_{approx} . However, this time it is the data which will be used for validating the estimated GRPR, and not for linear approximation.
 - FM : Fade margin. This value can be computed by the algorithm using the maximum and minimum RSSI values recorded or the user can specify this value. Often the margin values are calculated using the probability functions such that the received SINR is greater than a particular required threshold. Slow-fading and fast-fading models

are used to calculate FM . Further details are provided by Pahlavan and Levesque (2005).

- **LINEAR APPROXIMATION:**
The process for linear approximation starts by conducting the PRR test. The transmitter conducts this test by first transmitting at the maximum available power level and recording the outcome of PRR test and the RSSI distribution. The same procedure is then repeated for another power level. This process is aborted in the following cases: either PRR test outcome fails to meet the specified criterion, or all available power levels are tested, or if the recorded RSSI readings are below the receiver sensitivity. After this process is aborted, the data collected is used for linear approximation between the RSSI and the transmission power.
- **SINR AND SNR CALCULATION:**
The data collected is then used for calculating the SINR or SNR. Section 6.2.3 gives further details.
- **CALCULATE G_L :**
Use the received SINR information along with $SINR_{req}$ to compute the lower value of GRPR, referred to as G_L .
- **ADD MARGIN, M :**
If the user has specified a fade margin value which needs to be incorporated in the model then use that value. Otherwise use the difference between maximum and minimum recorded in RSSI trend as M .
- **CALCULATE G_H :**
Add the fade margin to the calculated G_L value, and call it G_H .
- **CALCULATE τ_{est} :**
Using G_H and the linear approximation calculated above to estimate the transmission power, τ_{est} , required for transmission using Equation 6.10.
- **VALIDATION**
After the first estimation, the PRR test is conducted again using the $PRR_{validation}$ data. If the outcome satisfies the criteria then the value is stored in the TPC table. However, if the test is unsuccessful then the transmission power is increased and the test is conducted again till it satisfies the criteria. If the available power transmission power level does not permit the selection of the power level specified by the algorithm, then the GRPR is adjusted. This adjustment involves

the stepwise increase or decrease in G_L , where these steps are governed by the transmission levels available at transmitter.

Once this process is completed for one channel, it is repeated for all others. After that all the available channels are examined and the GRPR is set, and the TPC table is built. Thus, the initialization process is completed.

In short, this entire process has helped to configure and tune the proposed TPC algorithm with the specific transmitter, receiver and the operating environment.

The next phase of this algorithm is the operational phase.

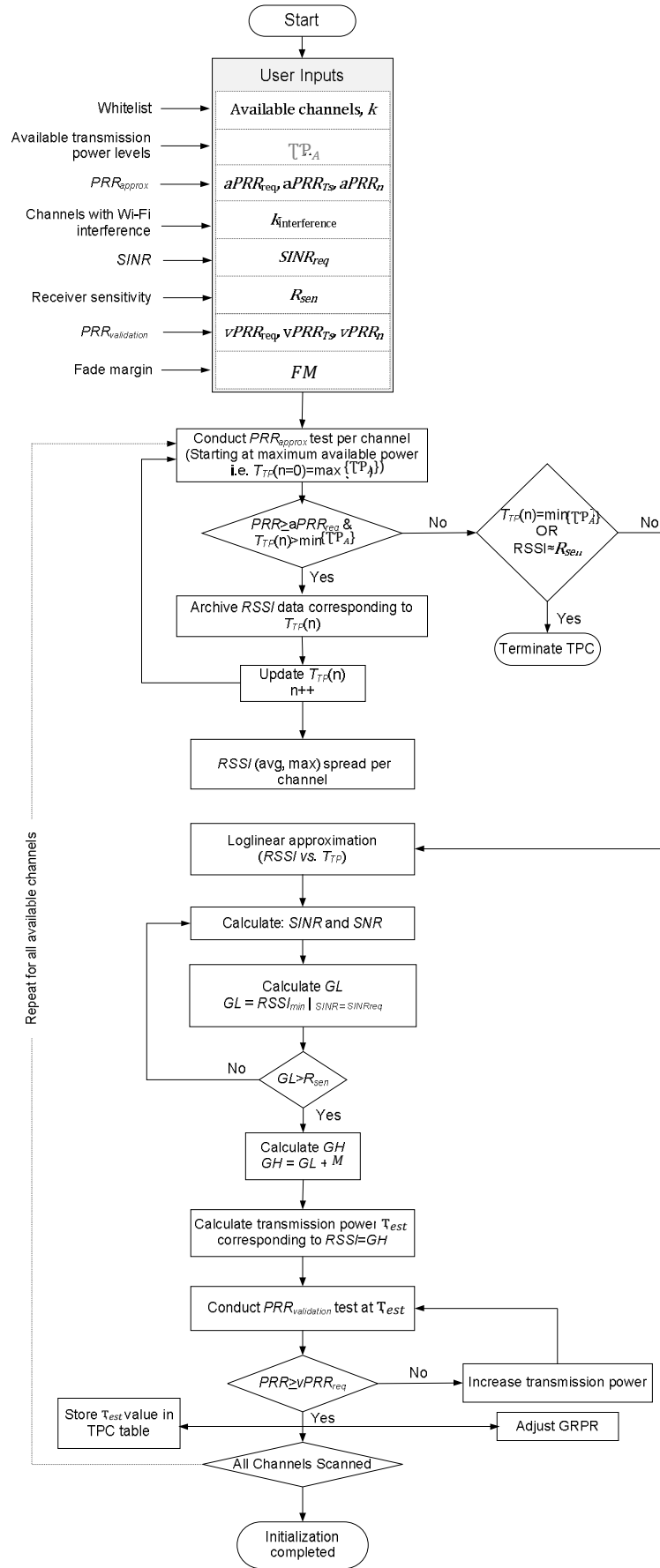
Operational phase

This phase deals with the operation of the regulatory control loop depicted in Figure 6.9. The detailed block diagram of this procedure is shown in Figure 6.10(b). Here, once the packet has received its RSSI value, it is checked against the GRPR. If the value is within the range then no action is taken. Otherwise, an action is taken which would either result in increase or decrease of transmission power. Furthermore, if continuous violations occur then it highlights a change in the operating conditions and suggests repeating the initialization procedure.

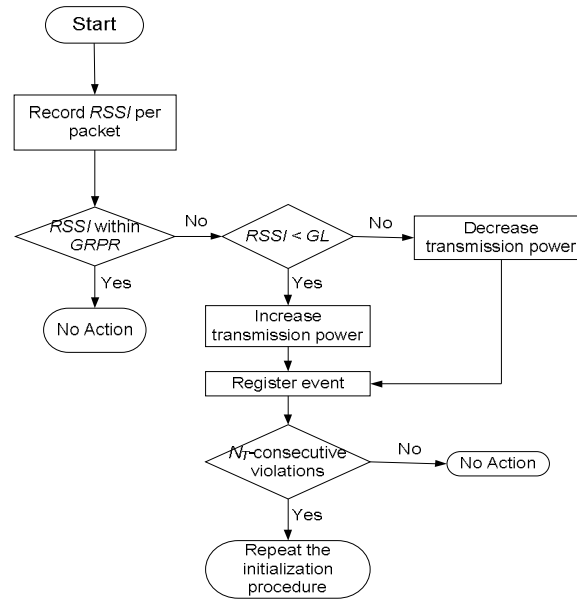
To summarize, during operations only RSSI values are tracked and the TPC algorithm is operated without any extra overhead. Once the violation occurs the regulatory control loop is executed. This will help to keep the overhead linked to TPC at the minimum.

6.4.6. Implementation of TPC

The majority of the processing for the TPC algorithm takes place at receiver, while the actuation takes place at the transmitter. The implementation of the proposed TPC algorithm is similar to the procedure defined in the previous sub-section. The process is divided into two phases: initialization phase and operational phase. The process starts with the initialization phase which involves the use of the supervisory loop and is responsible for building the TPC table and determining the GRPR.



(a)



(b)

Figure 6.10. (a) Initialization phase, and (b) operational phase of the proposed TPC algorithm.

During the operational phase, which involves only the use of regulatory loop, only the received RSSI values are tracked and compared to GRPR, based on which the TPC decisions are made.

A demonstration of the algorithm was done partly in CC2430EM modules and the rest on the attached computers as shown in Figure 6.1(a). The PRR test procedures were programmed onto the CC2430EM modules. The outcome of PRR tests and the recorded RSSI values of each packet were communicated to the computer. Estimation of the linear relationship between the transmission power and RSSI, and SINR estimation was carried out at the computer using Matlab. GRPR was then estimated and the outcome was conveyed back to the receiver. Moreover, the estimate of transmission power was sent to the transmitter. This configuration, therefore, implemented the initialization phase partly on the computers and partly on the CC2430EM modules while the operational phase was implemented on the CC2430EM modules. The reference SINR in the experiment was set to +7 dB and PRR_{req} was 0.8.

6.4.7. Implementation Results

Results from initialization phase

Figure 6.11 (upper panel) shows the transmission power level selected by the transmitter. During the first 20 seconds, the transmitter conducts the PRR tests at two different power levels (100 packets at each of 0dBm and -5dBm) in order to establish a linear relationship between transmission power and RSSI. The linear relationship permits extrapolation and selection of a transmission power level (-25 dBm) that is able to achieve the desired SINR at the receiver. If the PRR remained adequate, then the algorithm proceeds to determine the RSSI distribution and the GRPR. If the PRR were not adequate, the transmission power would have been increased to the next level. In fact, -25dBm is the lowest available transmission power level. Figure 6.11 (lower panel) represents the received RSSI values at the receiver for channels 15 and 24. The RSSI recorded in channel 24 with interference was higher, as expected from earlier results.

Results from operational phase

The upper and lower panels on the left of Figure 6.12 present the performance of transmitter and receiver for channel 15 during the operational phase. The regulatory control loop is executed when the received RSSI value goes outside the GRPR (-70 to -90 dBm, for channel 15). As a result of violation of the lower boundary condition due to channel fading, the transmitter was signaled to increase the transmission power three times in five hours. After the third occasion, the removal of the cause of channel fading stabilized the transmission power at -25dBm. The results show that GRPR calculated by the proposed TPC algorithm provides an effective response to fading.

Figure 6.12 also shows an experiment using channel 24 in which the distance between transmitter and receiver was changed. The results show that the transmitted power increased in order to keep the RSSI at the receiver within the GRPR. Until 200 sec, the receiver was close to the transmitter. The RSSI at the receiver was high and the algorithm selected the minimum transmission power level of -25 dBm. The receiver moved away at around 100 sec, and again at 200 sec. On the second move, the RSSI went below the lower limit of the GRPR (-90 dBm) and the algorithm responded by increasing the transmission power to meet the SINR reference value. The same

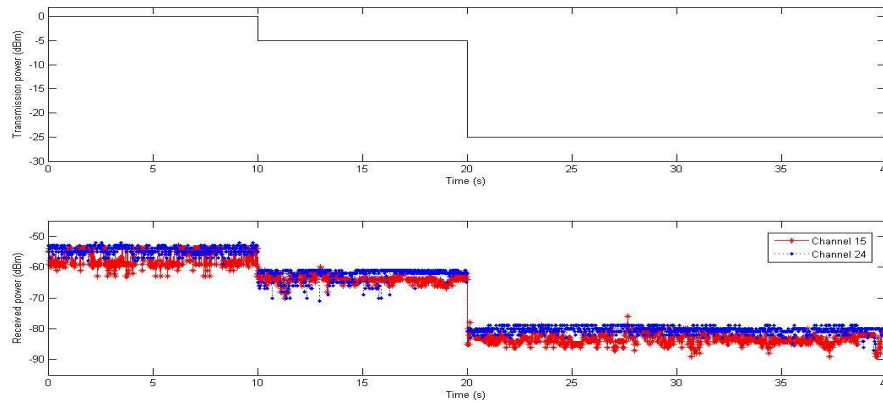


Figure 6.11. Upper: Transmission power. Lower: RSSI at receiver.

response can be seen on a move at 300 sec. At 350 sec, the receiver started to move back closer to the transmitter. The final move at 450 sec highlights the effectiveness of the algorithm in power saving. When the receiver moved closer, the transmitter was able to reduce the transmitted power while keeping the RSSI within the GRPR. The upper limit of GRPR after 200s was -80 dBm. Earlier, it was not possible to achieve this level due to limited available transmission power.

The GRPR is different in channels 15 and 24 in the demonstration in Figure 6.12 because GRPR adapts to the RSSI distributions, as described earlier.

In short, the initialization stage assists in finding the GRPR for a given installation, and during the run-time operations only RSSIs are tracked. The update frequency of the supervisory loop is application and deployment specific, whereas, the regulatory loop can be updated on per packet basis. The same experiment was also conducted at the same location over multiple days, and it was observed that both the fade margin and bias was found generally higher during week day compared to weekend. It was due to people moving around in the office and the higher traffic generated in IEEE 802.11 channels. The proposed TPC algorithm was able to identify the minimum transmission power which was adequate.

6.4.8. Energy Consumption Analysis

The total energy consumption at the transmitter with TPC implementation is calculated using transmission mode data, and is given by the following formula,

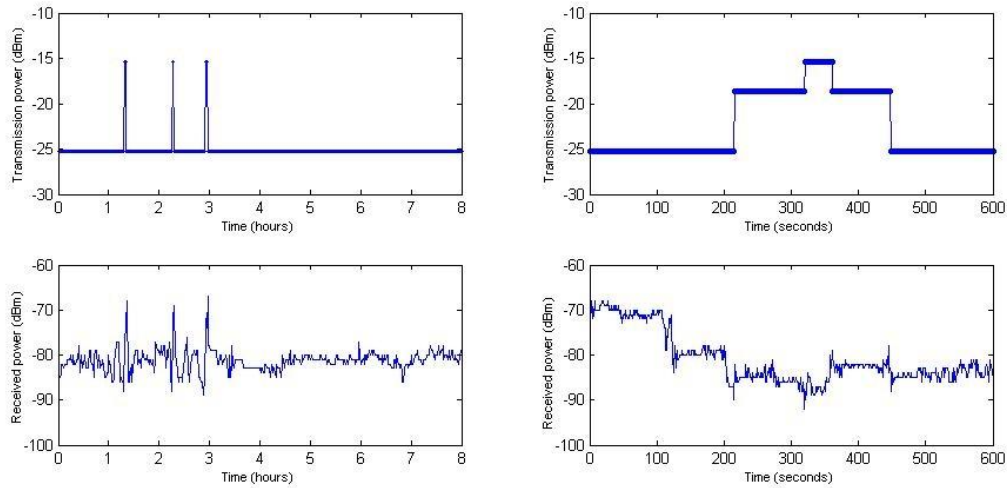


Figure 6.12. Run-time TPC operation. Left: transmission power responses to fading. Right: transmission power responses to changes in position of the receiver.

$$E_{total} = V_0[t_{op} \sum_{i=\min}^{\max} N_i I_i + t_{dp} \sum_{k=\min}^{\max} N_k I_k] \quad \text{Equation 6.11}$$

where, the first part on right in Equation 6.11 accounts for overhead introduced by the TPC algorithm and the second part takes into consideration the cost for data communications. Here, V_0 is the operating voltage, t_{op} is the time to transmit the control packet, and similarly t_{dp} for data packet. Furthermore, N_i represents the number of overhead packets generated during TPC initialization and the current consumption I_i during packet transmission at i -th power level. Subscript k represents the similar transmission level values during data transmission phase. E_{total} here refers to energy consumption in one channel. The total energy cost for operation over multiple channels would be an integer multiple of this overhead value, and the integer is equal to number of available channels. The equation does not take into consideration the cost for energy consumption at the receiver. The reasons are twofold. The first is that the energy savings at the transmitter is currently under discussion and not at the receiver. The other reason is that energy consumption at receiver during operation phase is negligible because the algorithm uses RSSI retrieved from individual data packets to make TPC decisions. Therefore, the overhead energy consumption at the receiver is considered insignificant during operational mode. Regarding the initialization phase, it is an energy cost which again is negligible considering the span of operation of wireless sensor nodes lifetime.

To estimate the energy cost of the proposed algorithm, a use case is considered which requires an update frequency of 1 Hz and packet sizes of 127 bytes. It is assumed that the initialization is required once at most during a day. The PRR linear approximation test comprises of 100 packets at each power level and the maximum numbers of channels available are 15. Taking into consideration the energy expenditure with and without TPC, it is found that if the TPC algorithm finds a suitable power level to be around 25 dBm or below then the cost for overhead introduced by TPC can be compensated within 6 hours. Panel 6.2 summarizes the calculation.

Scalability

The TPC algorithm has been designed to operate on a pair-wise basis between individual pair of nodes. The same TPC algorithm can be applied to all the nodes in the network and it can compute the minimum transmission power required for each link. The TPC table which is built as a result of this algorithm contains information about the transmission power required for communication with any node which is within the communication range of a transmitting node. Each wireless node compliant with the aforementioned industrial standards maintains a collection of tables, such as the neighbor table which contains the list of nodes which the device can directly communicate with. The TPC table is an enhancement to this table with two new columns specifying the transmission power required for communication with a specific node and at a given channel number. The TPC initialization is conducted once at the startup when the network is formed and afterwards, when new nodes join, the neighbor table is updated and so will be the TPC table. There will be only one TPC table per transmitting node and one power update controller. The memory and processing requirement is kept to a minimum as the initialization is required once in the beginning, and afterwards requires only the tracking of RSSI.

Furthermore, the use of TPC on pair-wise basis helps to achieve topology-independency. It also removes the need for a central controller to coordinate the TPC operations because such operation will need to have control over topology and can be slow to react. Lastly, all the nodes which are physically located in the same area as before can use an earlier built version of TPC stored for communication until the point where the information is outdated. This will offer substantial energy savings and quick start, as each entry in TPC table will only be updated when a violation occurs.

CALCULATION:

In the calculation shown in this panel the following values are used for illustration purposes:

I_{max} is the maximum current consumption when CC 2420 operates at maximum available power level and is 17.4 mA. I_p is current consumption corresponding to any other transmission power level below the maximum available. Here, 15.2 mA is considered as this value. Both of these values are taken from CC2420 data sheet.

t_{dp} and t_{op} data packets consume 4.064 ms (i.e. based on 127 byte packet size) to transmit and receive. Further, N_c represents the number of available channels to operate over and is taken as 15 in the given example.

N_D refers to the number of packets generated within a given operational duration. Here it is assumed that the duration is 6 hours and one data packet is transmitted every second. It is used to compare the energy cost of transmissions with and without TPC. Furthermore, N_a represents number of packets generated per channel during TPC linear approximation phase and N_v similarly represents the packets generated during validation stage.

Energy consumption without the use of TPC:

$$E_{without-TPC} = V_0(I_{max})(t_{dp})(N_D) \\ = 3(17.4)(4.064)(60)(60)(6) = 4582241 \mu\text{J}$$

Energy consumption with the use of TPC:

- Energy consumed during the initialization:

$$E_{linear-approx} = V_0(I_{max} + I_p)(t_{op})(N_a)(N_c) \\ = 3(4.064)(100)(15)[17.4+15.2] = 596188 \mu\text{J}$$

$$E_{validation} = V_0(t_{op})(I_{Tx})(N_v)(N_c) \\ = 3(4.064)(I_{Tx})(1000)(15) = 182880 I_{Tx} \mu\text{J}$$

$$E_{overhead} = E_{linear-approx} + E_{validation} \\ = 596188 + 182880 I_{Tx} \mu\text{J}$$

- Energy consumed during data transmission:

$$E_{data} = 3(4.064)(60)(60)(6)(I_{Tx}) = 263347 I_{Tx} \mu\text{J}$$

$$E_{TPC} = E_{overhead} + E_{data}$$

Equating: $E_{without-TPC} = E_{TPC}$, gives $I_{Tx} \approx 8.93 \text{mA}$

Panel 6.2. Energy cost estimation based on CC2420 transceiver specification.

An additional benefit of this process is that the pair of communicating nodes will have updated information regarding the performance of various available radio channels. This information can also be used to rank the performance of different channels and also to initiate the process of channel blacklisting if it is found to be the cause of deterioration of link quality.

6.5. Chapter Summary

The outcome of the research presented in this chapter is the development of a TPC algorithm which is succinct in response to interference and channel fading, is adaptive, supports multi-channel operation and is reliable. In addition, it is lightweight in terms of both computation and communication needs in order to address the inherent composition issues of these wireless nodes. The algorithm has been justified and presented in this chapter for TPC of industrial WSNs. It is based on RSSI and PRR for link estimation. A linear approximation is assumed between the transmission power and RSSI. The algorithm comprises two phases. The initialization phase is responsible for setting the limits of operation for the RSSI values which satisfy the SINR criteria and the fade margin. These limits are set taking into consideration the constraints of the transmitter and receiver. It was also highlighted in the chapter that the IEEE 802.15.4 compliant radios have varying available transmission power levels and receiver sensitivity which is vendor specific. To compensate for this difference, the algorithm is configured according to the available hardware transceivers. During the operational phase, the algorithm only considers whether the RSSI for the received packets falls within a Golden Receive Power Range (GRPR). Violation of the GRPR triggers an external feedback loop which adjusts the transmission power.

Additionally, it has been demonstrated that the co-channel interference from Wi-Fi affects the recorded RSSI values of IEEE802.15.4 packets. Therefore, the Wi-Fi influence on IEEE 802.15.4 network cannot be ignored, especially as it leads to a bimodal distribution. Moreover, as a result the transmission power needs to be adjusted in order to maintain the required SINR at the receiver across all the channels. Furthermore, fade margins have been observed to be time varying and application specific. Choosing a larger fade margin can counteract channel fading. However, it may result in unnecessary excessive energy being consumed.

The practicality and performance of the proposed TPC algorithm were studied through empirical data collected from hardware implementation. The experimental results show that the collective use of RSSI, PRR and SINR estimation can achieve a practical TPC algorithm for industrial wireless networks.

CHAPTER 7

Conclusions, Evaluation and Future Directions

This chapter gives a summary of the research work presented in this thesis. It highlights the conclusions and gives a critical evaluation of the achievements of the PhD and provides recommendations for possible future work. This chapter will reiterate the aims and objectives of the thesis, the methods and approaches used to address those outlined aims and objectives followed by the contributions made by the research presented in this thesis to both academia and industry.

Furthermore, the future work section offers recommendations on improvements that can be made on the techniques adopted in this thesis in order to cope with the underlined issues and other possible strands of research that can complement this area of research.

7.1. Overview

This section will revisit the research theme, the motivation for the project and the aims.

7.1.1. Topics of Research

The research presented in this thesis is about the use of wireless communication in process automation. Within this wide domain, monitoring, control and safety applications exist. The scope of this thesis is the use of wireless communication for process monitoring and control. Furthermore, within this avenue of research the three key issues investigated are:

- Time synchronization issue in distributed wireless systems
- Process control over a resource-constrained wireless network, and
- TPC for industrial wireless communications.

In order to deal with the aforementioned time synchronization issue, hardware-assisted time synchronization is proposed. It utilizes a broadcast time signal from a radio tower (i.e. MSF signal) to achieve and maintain time synchronization throughout network operations. The thesis reported an application to a metropolitan area network covering an entire city such as infrastructure monitoring of a pipeline network for a utility company. As a part of the research presented in this thesis, the hardware developed was deployed in a pipeline infrastructure monitoring system and the results are presented, analyzed and discussed.

The thesis addressed the topic of process control in a case study which concerned the use of short-range standardized industrial wireless networks. This study was complemented with both simulations and hardware-in-loop based evaluations. It highlights the limits of operation of an IEEE 802.15.4 based network and the compromises between control and communication. This designated area of research is known as WNCS. Due to multiple competing industrial wireless standards this case study has restricted its scope to the common denominator of all these standards which is the IEEE 802.15.4 standard.

The final issue which was addressed is the use of TPC for industrial wireless instrumentation. The thesis has analyzed the restrictions imposed by the need for reliability, availability and real-time operations on a resource-constrained wireless network. An algorithm was built to address these issues and was implemented and evaluated.

All throughout the research, application requirements and industrial implementation have been considered and the hardware and algorithms have been prepared carefully for seamless technology transfer.

7.1.2. Motivation, Aims and Objectives

Motivation

There are many motivations for using wireless communication in process automation; however the access to enhanced process information is the key driver. Plant or process knowledge can be enhanced by acquiring additional measurements from the underlying processes and equipment, and wireless communication networks can assist the process

industry to gather more data by providing low-cost connectivity when wired communications would be infeasible. Chapter 1 has given detailed insight to the motivations for each research issue and also presented examples of industrial applications.

Besides the business drive, the adoption of the wireless technology in NCS is the next phase in evolution of control and measurement technology as depicted in Figure 1.8 and 1.9. The thesis has investigated the stringent requirement of process automation, the emerging industrial wireless standards, the resource-constrained nature of short-range industrial wireless, the multi-disciplinary nature of this research area (which involves control, communication, embedded hardware and software design, and system integration). The gap between theory and in-situ practice was challenging and remained the motivation behind this research project.

Aims and objectives

The main aims and objectives highlighted in Chapter 1 were:

- TIME SYNCHRONIZATION AIM:
 “To design a solution for time synchronization of nodes in a distributed system, while ensuring that it is *energy-efficient, scalable, topology-independent, available* and *fast-converging* time synchronization solution”.
- TIME SYNCHRONIZATION OBJECTIVES:
 - Identification of different approaches available for time synchronization.
 - Identification of solutions which offer topology-independency.
 - Identification of solutions which are scalable and fast converging.
 - Identification of solutions which are available.
 - Identification of the sources of error in time synchronization.
 - Theoretical analysis of time synchronization accuracy.
 - Theoretical analysis of convergent time.
 - Theoretical analysis of energy-consumption.
 - Experimental results for the proposed solution.
 - Overall theoretical analysis and validation through empirical results.

- WIRELESS PROCESS CONTROL AIM:

“To identify the *suitability* of standardized wireless networks for use in process automation, and to formulate a mechanism for running a *closed-loop control* application over a *resource constraint* wireless network”.

- WIRELESS PROCESS CONTROL OBJECTIVES:

- Requirements analysis for using wireless in process automation.
- Identification of closed-loop control requirements.
- Identification of the control-loop structure used in NCS and industry practices.
- Identification of standardized short-range license-exempt wireless technologies.
- Analysis of the suitability of standardized wireless technologies for process control.
- Analyze the limits of operation of IEEE 802.15.4 compliant network.
- Formulate a mechanism suitable for process control over resource limited network.
- Performance evaluation of the proposed approach.

- TPC AIM:

“To develop an algorithm for TPC in wireless instruments which can *adapt* to changing radio environment, is *quick* to respond, works on *pair-wise* basis, is *vendor-independent*, and *practical*”.

- TPC OBJECTIVES:

- Identification of measures available for wireless link quality assessment.
- Determine a measure suitable for estimating link quality in IEEE 802.15.4 networks.
- Feasibility study of the selected measure through empirical results.
- Determine an approach suitable for TPC.
- Formulate an algorithm for TPC which is adaptable and practical.
- Implementation of the proposed algorithm and performance evaluation.
- Evaluation of associated energy consumption.

7.2. Summary of Main Findings and Conclusions

This section presents a summary of the contributions from all the chapters in this thesis. The contributions are categorized based on the aim they were targeted towards. A brief summary of methods and strategies that were used to address the problems has been highlighted along with the conclusions, contributions and achievements.

7.2.1. Time Synchronization in Distributed Networks

Identification of topology-independent, fast convergent, scalable, available and energy-efficient time synchronization solution

Chapter 3 compared the use of GPS, radio clocks and other options for time synchronization in wireless networks. It was concluded that radio clocks would meet the requirement for energy-efficient, scalable, topology-independent, available and fast-converging time synchronization. The arguments for this conclusion were:

- Topology independence and scalability can be achieved using dedicated radio clock onboard on the wireless nodes.
- Fast-convergence is achieved because all nodes use the same time broadcast signal. The signal has coverage of up to 1000 km from Anthorn, Cumbria, England.
- The MSF radio signal operates in the LF spectrum and works without the limitation of line-of-sight. The MSF signal is a continuous broadcast controlled by National Physical Laboratory (NPL). Therefore, collectively they offer good coverage and availability.
- The design of the radio clock receiver is less expensive and is energy-efficient compared to GPS.

Errors, accuracy, convergence time and energy considerations

Chapter 4 identified in detail the source of time synchronization error in the case of radio clock time synchronization.

The main conclusion is that the use of MSF time signal helps to eliminate and minimize three sources of time synchronization error introduced in normal sender-receiver synchronization systems, namely the send time, access time and propagation time. These errors remain between the sender and receiver, but amongst the receivers themselves, they are cancelled out. The network, hence, becomes susceptible merely to receiver related error. It was also identified that the time synchronization accuracy of an MSF receiver relative to the UTC has an uncontrollable error of up to one millisecond in magnitude introduced by the MSF transmitter. Therefore, inherently the accuracy is within a millisecond range.

A detailed analysis on time synchronization in relation to the incoming MSF signal led to the discovery that it is linked to the ongoing time at the start of the time synchronization process, the minute frame duration, distance from transmitter, and also on the MSF receiver switch-on time. Therefore, the main conclusion is that if the hardware variations are to be ignored, then the entire network should be able to synchronize (i.e. converge) within a few milliseconds (for e.g. 3.3ms in the case of ground wave) after the transmission of the on-time marker.

Furthermore, it was found that the energy ratio of MSF to GPS is significantly low. Using the energy calculation of EM2S (i.e. MSF receiver) and JN3 receiver (an energy-efficient GPS module available in market) still gives a ratio of (1:59). Therefore, it is concluded that the radio clocks are energy-efficient compared to GPS. However, the accuracy of GPS is superior.

Validation of theoretical analysis through empirical results

Chapter 4 presented designs for new circuits and interfacing software to incorporate a commercially available MSF receiver unit into a wireless MSF receiver node.

Quantitative empirical testing led to the following conclusions:

- TIME SYNCHRONIZATION ANALYSIS
 - The work has led to the conclusion that reports in the literature have only addressed synchronization among radio clock receivers. As far as can be ascertained, the study in this thesis is the first to consider synchronization relative to UTC time.

- Further, the results show that the different hardware modules of the same brand and even with the same part number have variation in receive time which adds to time synchronization error. Figure 4.15 and Figure 4.22 highlight these findings.
- RECEIVED SIGNAL QUALITY
 - The outcome of the experiments on the reliability of the MSF signal showed that the signal is available and reliable. The decoded time signal showed that the 95% of the decoded time frames were accurate.
 - Conclusions from field testing in Cumbria and London were that accuracy of the wireless MSF receiver node depends on the quality of the signal, the distance from the MSF transmitter, the time of day, meteorological conditions, and ultimately the one millisecond accuracy of the transmitter.
 - The conclusion from the study on the stability of the on-time markers recorded by the MSF receiver is that the receiver output is stable. Further, during long term operation the time accuracy is limited to the MSF transmitter accuracy.

Improving time synchronization accuracy

Section 4.4 incorporates a novel algorithm to improve the time synchronization accuracy and to address the uncertainty due to a hardware-linked readings mismatch. The algorithm development demonstrated that the accuracy of time synchronization can be enhanced by using a Kalman filter and the short term accuracy of local crystal oscillator.

Field deployments

This thesis describes the use of the MSF radio time signals for the global time synchronization of SCADA systems (including WSNs). It introduces the MSF time and date code signal in detail and how it can be used for time synchronization in location with both good and limited signal coverage.

The wireless MSF receiver nodes have been deployed in fire hydrants. These field deployments have proved that the LF signal can be received in an underground environment close to the surface.

To summarize, this hardware-assisted time synchronization approach has been analyzed theoretically and also practically, with results shown to be in agreement. The results have highlighted that it offers a good solution for time synchronization especially in terms of energy consumption, cost, compactness and coverage. The long term independent and continuous operation of the built version of the radio clocks highlight that the MSF time signal is reliable and stable.

7.2.2. WNCSSs

Requirements analysis for using wireless in process automation

During the PhD three industrial wireless standards (i.e. WirelessHART, ISA 100.11a and WIA-PA) have emerged, based on earlier standards such as ZigBee. In order to identify which technologies are inherently suitable for process automation, it is important to reflect on the networking requirements of process automation. One of the contributions of this section of the research work was to collect the requirements and use them as a benchmark to evaluate the suitability of these technologies for process automation.

Wireless technologies for process automation

A finding of the work was that Wi-Fi, Bluetooth and ZigBee cannot meet industrial needs for availability, reliability, scalability, energy-efficiency and quality of service. These conclusions are based on the comparison and feasibility analysis presented in Section 2.3.

Moreover, a detailed examination of the industrial wireless communication technologies identified that the industrial standards exploited the availability of spatial, frequency and time diversity techniques to address the aforementioned shortcomings. A key point to reiterate is that these industrial standards use mesh networking. On one hand, mesh networking improves reliability, whereas on the other hand it can lead to a variation in latency. Therefore, it is a concern for closed-loop control applications and for battery operated field devices.

In addition, it was identified that these industrial standards do not impose particular limitation in terms of number of devices which can join a network other than the limit of

the addressing space. However, several limitations hinder the use of wireless communication in process control, including the need for determinism.

Analysis of limits of IEEE 802.15.4 network for process control

In recent years, only a few wireless process control application deployments have surfaced. Even for those reported, their results and performance evaluation are not published in detail and not in journal papers. Furthermore, the research literature available within this domain is mostly based on simulations.

The comparison of industrial wireless standards revealed that they are all based on same PHY layer and in some cases even same MAC protocol, which is based on IEEE 802.15.4 standard. Therefore, this strand of contribution was to identify the absolute limits of the use of IEEE 802.15.4 network which will ultimately be applicable to industrial standards and will dictate whether it can support a particular control application or not. Chapter 5 documents these absolute limits.

A case study on performance of control loop over a wireless network

This thesis has presented a case study involving hardware in the loop simulation. The case study concluded that packet losses, delays and network outages cause deterioration of the control system performance. In addition, it was identified that the set point change during network outage can lead the actuator to saturation because of the integral error term in the PID control algorithm.

Strategies which can improve control performance

The three key contributions within this domain are:

- A new algorithm was presented in which the PID controller uses different state configurations depending on the network status to improve the system response. This approach is simple, energy-efficient and improves the system performance as demonstrated in Figure 5.16.
- To address the issue of latency, a mechanism has been proposed which utilizes dedicated communication channels, LEF based channel access and a shadow superframe. The results show that this method (referred to as fast lane) leads to an overall improved process response as shown in Figure 5.19. Furthermore, a method for selecting optimum number of channels to be used in the fast lane is

provided in Section 5.3.3. There, it is solved by minimizing the objective function (i.e. SO) and using the required network throughput and allowable maximum delay in packet delivery as constraints. The concept has been shown to be effective in meeting the delay requirement of process control applications.

- This thesis further presents a framework where collectively the network layers and the control layer adapt their parameters accordingly in order to address the limitation of short-range wireless networks. It is concluded that while keeping the segregation between the networking layers the use of common repository can help to improve the overall control system performance.

To summarize, the use of wireless communication in process control is a new research area and requires an understanding of control, communication and current industrial practices. Furthermore, the work shows that it is essential to consider the hardware limitations, communication limitations and network topology in the design of a wireless process control system.

7.2.3. TPC

Empirical study on link quality assessment

It is recommended to measure link quality using RSSI rather than LQI, for reasons explained in Chapter 6. RSSI distributions from channels which are subjected to co-channel interference from a neighboring Wi-Fi network yield a bimodal distribution. However, the channels without any interference follow a Gaussian like distribution. Therefore, it is concluded that the effect of Wi-Fi on IEEE 802.15.4 network cannot be ignored when designing an RSSI based TPC algorithm.

In addition, it was found that the transmission power available at the transmitter and the receiver sensitivity can be a limiting factor for TPC as shown in Figure A1.1 and A2.1.

An adaptable and practical TPC algorithm

This thesis presents a TPC algorithm designed for industrial communications. The algorithm is able to adapt the power levels and sensitivity to compensate for changes in operating environment.

The performance of the proposed TPC algorithm was studied through empirical data collected from hardware implementation. Based on the experimental results presented in Section 6.4 it is concluded that the proposed algorithm is effective in coping with both short and long term variations to the link quality.

Evaluation of associated energy requirement

The objective of the TPC algorithm is to reduce the transmission power. To do so, TPC algorithms themselves introduce overhead during the computation of this desired transmission power level. Detailed calculations in section 6.4.8 showed that the energy savings significantly outweigh the overhead.

To summarize, the outcome of the research into TPC for industrial wireless instrumentation is the development of a TPC algorithm which is able to handle interference and channel fading, is adaptive, supports multi-channel operation and is reliable.

7.3. Critical Evaluation

The methods, hardware and strategies that have been built as part of this research have been reviewed by the industrial partners (which include ABB and Sintef). Two conference papers have been published; many presentations have been given over the subject at the conferences, workshops and seminars. Furthermore, one journal paper has been submitted and two others are underway.

Discussions with industrial practitioners have given very useful feedback throughout the whole period of the PhD. The findings of the PhD have generated interest and occasionally controversy. Some highlights worth mentioning are:

- The hardware for time synchronization has been deployed in the field in collaboration with another department at Imperial College. The device was robust enough to be used by Dr. Ivan Stoianov and his colleagues showing that transfer of this technology is underway into a practical device.
- The willingness of the process industries to use wireless communications in closed loop control has increased markedly during the four years of the PhD. The

work of Chapter 5, which initially seemed speculative now seems well positioned to address real industrial requirements.

- The work on the TPC algorithm of Chapter 6 has been actively encouraged by the Norwegian WiCon Consortium. As far as is known, this TPC is the first time that any investigator has demonstrated a practical way to implement the provision in IEEE 802.15.4 for optimization of transmission power for industrial wireless.

Discussions and feedback have also prompted consideration of some potential drawbacks. These are outlined below, together with some comments.

- The proposed time synchronization solution uses an external time broadcast signal which is a security concern because it is controlled by a third party, which in this case is NPL. However, for an alternative solution same argument also exists because GPS is controlled by the US authorities and is made available to general public.
- The terrestrial radio time signals are not present worldwide, especially in some developing countries. However, most of the developed countries have them operational. Therefore, its applicability is region specific.
- The deployment of the radio receiver next to an electric source which generates frequencies within the operational frequency of MSF signal can compromise the MSF signal reception.
- Furthermore, for applications which require the deployment of radio clock well inside a closed environment either an active antenna or a rebroadcast of time signal may be required.
- The proposed method to improve the integral-derivative part in a PID algorithm requires packaging of the replica of the previously sensed process value. It is fine for applications with few bytes of process value, in future it may become restricted if the amount of sensed data at every sample time increases.
- The proposed TPC approach utilizes a decentralized approach to yield the required transmission power. This method is quick to adapt to network changes but may not yield an overall balanced network operation.

These were some of the key arguments which are linked to the selection of proposed methodologies adopted in this thesis.

7.4. Recommendations for Future Work

This section provides recommendations for possible future extensions of the work presented in this thesis. These extensions can be classified into two streams: enhancements which can be made to the presented hardware and algorithms, and other possible strands which can complement this research area:

Enhancements to the hardware and algorithms

- The designed system for time synchronization currently uses the MSF signal. The hardware can be enhanced by including other radio time signals as well, such as those operating in the US, Japan and Germany.
- Rebroadcasting using the same 60 kHz signal has not been tested. It will be useful to investigate as to whether the repeater introduces an offset which needs to be compensated.
- The hardware-in-loop setup has used only a one hop configuration for control system performance evaluation operating over a wireless network. This can be enhanced by using a multi-hop mesh network.
- The TPC control algorithm and its performance evaluations were carried out within an office environment. The next step would be to deploy and test the proposed TPC in an industrial environment.

Other strands of research

This research can further be complemented by designing the next generation of WNCSSs which use new control architectures and support field control. Network based services are increasing in other sectors and they could be used in future to provide the integrated communication and control architecture for future process automation. Furthermore, the adaption of the control and communication layers and their cooperation is essential to achieve the required control performance.

New radio resource management strategies, onboard power management and real-time operating systems can complement this research domain. On the other hand, for applications which support condition monitoring new algorithms are required to compress the data and use locally distributed computational resources to identify the equipment condition. Furthermore, the omni-present topic nowadays in WSNs is energy scavenging which can be explored in order to replace the traditional use of chemical batteries on wireless sensor nodes. To summarize, the use of wireless communication and internet is on rise in process automation as the industrial activities become more distributed and remote.

Long term evolution

In the past, the notion of wireless process automation was treated with suspicion. However, advancements in networking technology have reduced skepticism and there is now a drive from process automation to adopt wireless communication. In the near term, its role will continue to be of an auxiliary nature. In the long term, however, it can be anticipated that wireless communication will become an integral part of the future of process automation for many reasons already discussed in this thesis.

Having said that, it is worth to identify that there are technological barriers in this roadmap. A few of them are as follows:

The industrial wireless technologies are based on the IEEE 802.15.4 standard, which eventually will face two main limitations. Firstly, it operates in the 2.4 GHz ISM band which is becoming heavily crowded. Eventually, this will have an impact on reliability and availability. The other limitation is that the IEEE 802.15.4 standard is a low-rate communication standard, and the need to accommodate applications with high throughput requirements (which will arise in future) will require re-examination of the suitability of the IEEE 802.15.4 compliant wireless network.

On the other hand, battery lifetime remains a concern, and energy harvesting has the potential to lift the energy constraint found in wireless instruments today. However, the intermittent nature of these harvesting technologies and functional and process safety concerns may limit their adaption in safety-critical applications. To conclude, the examined industrial wireless technologies presented in this thesis are the first of their generation, and will transform the process automation industry.

7.5. Chapter Summary

This chapter has reviewed and given a critical evaluation of the work presented in this thesis with the recommendations for future work.

The subject of this thesis is the use of wireless communication in process automation for monitoring and closed loop control. This chapter has summarized the key contributions made, ranging from the evaluation of literature survey within this domain, examination of the wireless communication technologies and the suitability analysis based on process automation requirements. Furthermore, this chapter concludes the outcome of this research.

In addition, the thesis has made the following key contributions:

- A time synchronization system has been proposed based on the use of radio clocks for time synchronization of spatially distributed systems. The designed system is shown to be energy-efficient, cost-efficient, topology-independent, fast convergent and scalable.
- A case study is presented to identify the performance of control loops subjected to packet delays, losses and outages. The case study is complemented with both simulations and hardware-in-loop testing. Furthermore, methods and strategies have been proposed to improve the overall control system performance when subjected to these network disturbances.
- A new algorithm for TPC is proposed and tested. It is suitable for industrial wireless instruments and is shown to be effective and practical.

In addition, this chapter has further presented the evaluation of the strengths and weaknesses of the proposed strategies.

Overall, the future of wireless communication in process automation seems very promising. It is an exciting and fast-moving area with many opportunities. This thesis is now submitted as a record of the findings from the last four years of research. It has been a wonderful experience to learn, understand and explore some of these topics, and it is going to be very interesting to see how the future unfolds.

"Now this is not the end. It is not even the beginning of the end, but it is, perhaps, the end of the beginning."

Winston Churchill

Appendix A1. Energy Savings

For devices which communicate more often, the energy cost per transmission compared to energy cost during sleep mode in a cycle increases rapidly and is shown in Figure A1.1. Switching from a higher power, for instance 0 dBm on the graph to a low transmission level like -25 dBm will result in reduction in ratio of energy consumption per cycle of approximately 51%. The transmitter current drain is shown in relation to the transmission power levels indicated in the graph. It is assumed that there is only one transmission per frame and the device sleeps for the rest of time.

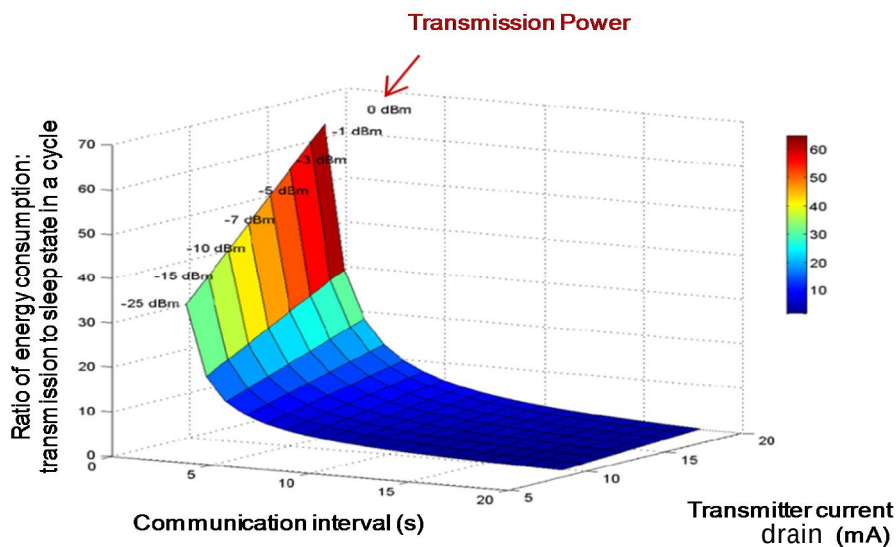


Figure A1.1 Ratio of energy consumption as a function of communication interval and transmitter current drain. Based on CC2430 module and 127 bytes packet size.

Appendix A2. Improved Receiver Sensitivity

The minimum sensitivity of the receiver as defined by IEEE 802.15.4 standard is -85 dBm and the best case theoretical sensitivity can be -113.2 dBm (Lanzisera *et al.* 2007). This improved sensitivity offers an opportunity for TPC as can be seen in Figure A2.1. The received signal calculations are based on the path loss model adapted from IEEE 802.15.4 (2006) and assuming omni-directional antennas. It can be seen that between the two planes at -85 dBm and -113.2 dBm various power level selection options exists which offers a window of opportunity for TPC leading to energy savings, interference minimization and topology control which are vital for wireless communication in process automation.

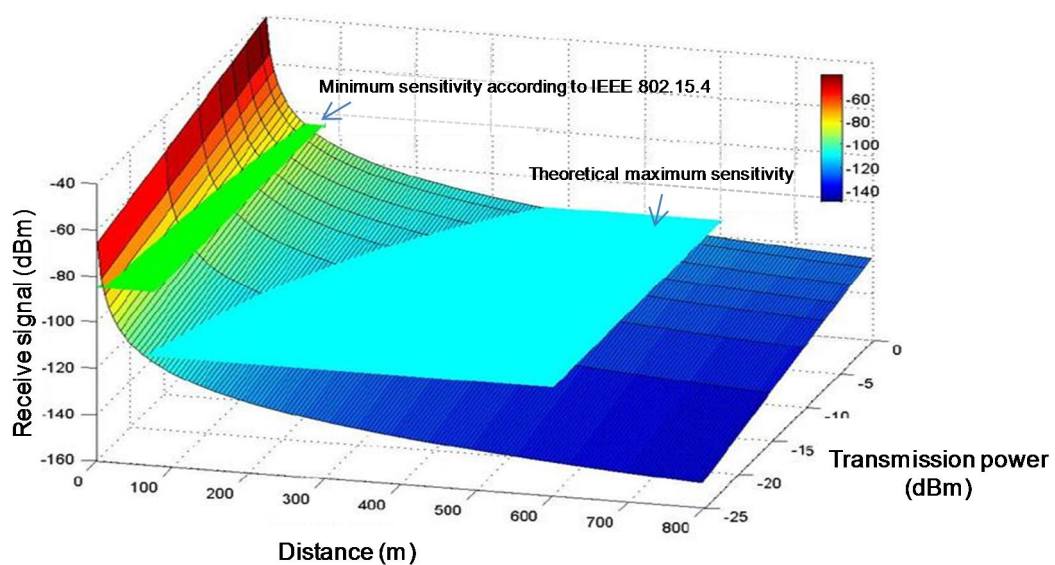


Figure A2.1. Receive signal as a function of distance and transmission power.

Appendix B1. WLAN and WPAN Technologies

This section provides an overview of the commercially available wireless communication technologies. The reason for their inclusion is to identify their suitability for process automation based on the requirements mentioned in Chapter 1. Wireless technologies are categorized based on coverage, which ranges from meters to several kilometers. The four specific groups based on the coverage and target application are Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metropolitan Area Network (WMAN) and Wireless Wide Area Network (WWAN) in the order of increasing range (Garg, 2007).

Figure B1.1 provides an overview of key wireless networks, their associated standards and properties. The figure has three axes: range (maximum distance between communicating devices), transmission power (output power level of transmitter) and channel transmission rate (speed of communication). The absolute transmission power levels vary across the globe. However, the trend is that power levels increase from WPAN to WWAN. Within this context, range is referred to as the communication distance between a pair of nodes which communicate directly. In the case of cellular networks, like GSM networks the mobile base station connects to base station. Base stations are connected to a Base Station Controller (BSC), which manages the distribution of resources. Furthermore, the BSCs are connected to Mobile Switching Centre (MSCs) which provides access to public telephone network (Garg, 2007). Therefore, in a complete architectural view of cellular networks they offer access to the wired backbone network for communication. However, the distance referred to in Figure B1.1 is that of between a mobile station and a base station. The radius of communication offered by a base stations vary from installations in urban areas to those in rural areas, and the available communication rate also depends on distance.

The range requirement is application and deployment specific. At an enterprise level (ISA-95 levels 3 and 4) the technologies such as GSM/GPRS and WiMAX which belongs to WWAN and WMAN can be used for long range communications. WiMAX technology is based on the of IEEE 802.16 family of standards. By contrast, within levels 0 to 2 technologies covering WPAN and WLAN are of interest, predominantly due to the

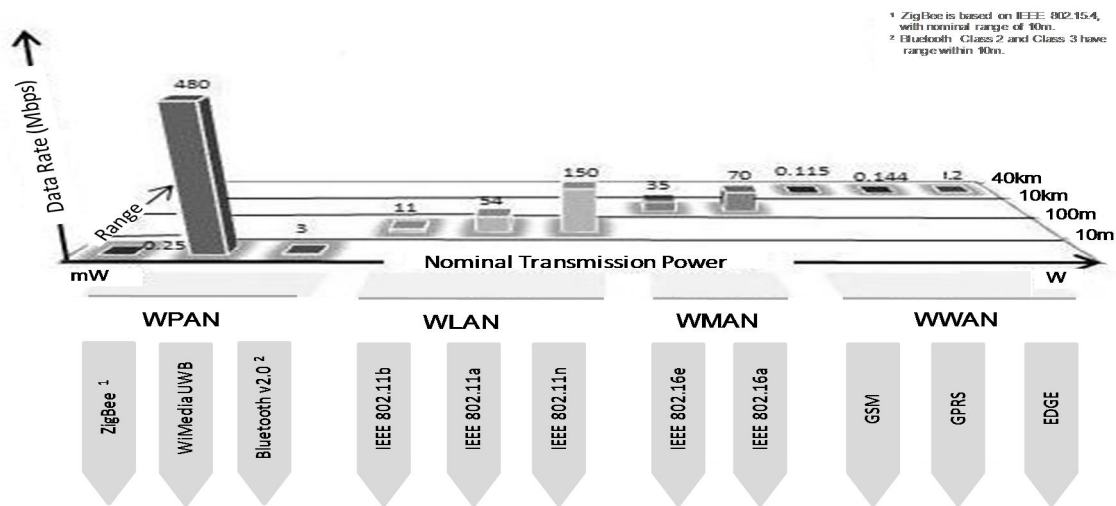


Figure B1.1. Illustration of wireless network technologies based on range, transmission power and data rate.

availability of commercial off-the-shelf license-free, low-power, short-range and economical radio modules. The communication range is around 100m and the transmission power is low, but the data rate depends on the technology being used as can be seen in Figure B1.1. Next, the wireless networking technologies which belong to WLAN and WPAN categories will be analyzed.

B1.1. IEEE 802.11 Family of Standards (Wi-Fi)

This section briefly examines the IEEE 802.11 group of standards which specifies the WLAN technology. They are commonly referred to as Wi-Fi. This section will evaluate its suitability for use at the instrumentation level. From here onwards the references will be made to the communication protocols and the OSI reference model.

Overview

A Wi-Fi certified device exchanges data using radio waves and complies with IEEE 802.11 suite of standards. The IEEE 802.11 and its extensions specify the Medium Access Control (MAC) and Physical Layer (PHY). Various extensions of IEEE 802.11 standard have emerged in recent years and a selected list is shown in Table B1.1. The IEEE 802.11 was the original standard and its later extensions which include IEEE 802.11a/b/g/n modified the PHY to support higher data rates. Furthermore, IEEE 802.11a/n extensions support the operation in 5GHz band which is less crowded

compared to the 2.4GHz band. On one hand, the trend has been towards extending the standard to support higher data transmission rates. On the other hand, IEEE 802.11e and IEEE 802.11i were the extensions made to the MAC layer to support QoS and enhance security features respectively.

The building block of a Wi-Fi network is referred to as *Basic Service Set (BSS)*, and is formed when two or more devices are connected. Within a BSS, the transmissions of wireless stations are controlled by a Coordination Function (CF). Distributed Coordination Function (DCF) is one of the supported and widely used CF specified by the IEEE 802.11 standard. It is a channel access technique based on CSMA/CA and binary exponential backoff algorithm (Acharya et al., 2010). Moreover, there are two types of operating modes, ad-hoc and infrastructure mode supported by the standard. Ad-hoc networks provide direct connectivity between devices, whereas, infrastructure mode requires access points to communicate.

Suitability

The PHY specified by the Wi-Fi standards support various transmission rates, and the data rate is adapted based on channel operating conditions (Niu et al. 2011). In general, in a Wi-Fi network the data rate drops as the user moves away from the access point or when the number of users on a network increases. In the latter case, it is because the same network resources get shared by more users. Furthermore, the packets are dealt in the order received. In addition, IEEE 802.11 compatible devices have high current consumption and cost compared to WPAN devices (Matheisen et al., 2005).

Performance analysis of Wi-Fi network for the purpose of feedback control is carried out by researchers such as Chen et al. (2008), Colandairaj et al. (2005), Irwin (2005) and Biasi (2008). Their research has highlighted the following issues which are to be addressed:

- Non-deterministic nature of the CSMA/CA based MAC protocol.
- Channel contention becomes an issue if there are more devices competing to get the message across the network.
- Wireless networks generally experience channel errors which leads to retransmission of data and therefore adds delay to the process information.

Table B1.1. IEEE 802.11 standard and its extensions.

Standard	Frequency (GHz)	Raw Data Rate (Mbps)	Features
IEEE 802.11	2.4	1, 2	The first standard ratified in 1997 and supported RF & IR transmissions.
IEEE 802.11a	5	54	5GHz PHY specification.
IEEE 802.11b	2.4	11	Enhancement to IEEE 802.11 standard. 2.4GHz (DSSS) PHY specification.
IEEE 802.11g	2.4	54	Extension in 2.4GHz band to support higher data rates.
IEEE 802.11n	2.4, 5	150 *	Enhancements for higher throughput.
IEEE 802.11e	MAC QoS enhancements to support broad range of applications.		
IEEE 802.11i	MAC security enhancements.		

* Maximum raw data rate per stream, given that $Gf=400ns$ and bandwidth is 40MHz.

- Sufficient bandwidth needs to be made available to wireless stations which are part of control loop. Therefore, the selection of appropriate CF is vital for successful operations.

The above mentioned issues affect the network QoS and its scalability. Consequently, they influence the performance of a control application. The highlighted issues presented above are linked to IEEE 802.11a/b/g/n networks. The IEEE802.11e MAC on the other hand incorporates features to support QoS in a centrally-controlled and contention-based access formats. The supported access mechanism known as Enhanced DCF (EDCF) can assist the devices with better access class (i.e. high priority information) to succeed the channel access based on contention-window assignment (IEEE 802.11e, 2005). The work from Ferre *et al.* (2004) shows that it leads to differential channel access, which helps to prioritize data, however, the differentiation is not guaranteed if wireless stations with same priority levels want to transmit at the same time. Despite the improvement in QoS, the other shortcomings which were mentioned before remains, which prevents Wi-Fi networks from being deployed at the field level.

B1.2. Bluetooth

Overview

The IEEE 802.15.1 specification standardized the MAC and PHY layers of Bluetooth technology. The original Bluetooth specification v1.0 consists of PHY, MAC, Link

Manager (LM), upper convergence layers and profiles that specified the protocols to be used (Obaidat et al., 2011). It operates in 2.4GHz band and supports data rate of 721 kbps. Since then the original version of Bluetooth specification 1.0 has evolved to support higher data rates, ensure coexistence, improve security, and enable low-energy consumption. Bluetooth v2.0 offers data rate up to 3 Mbps and Bluetooth v3 + HS offers data rates up to 24 Mbps (Obaidat et al., 2011). Further, there are three classes of Bluetooth technology, and they govern its coverage region which varies from 1m to 100m.

Piconet is the basic unit of networking in Bluetooth. It is an ad-hoc network with one master and up to seven active slave nodes. The master nodes clock and hopping sequence is used to synchronize nodes in a piconet (Obaidat et al., 2011). A slave in one piconet can become a master in another piconet. Several piconets can be interconnected and is referred to as a *scatternet*. Bluetooth uses frequency hopping to avoid interference by hopping to a new frequency 1600 times a second. All devices in a piconet share the same resources.

Suitability

Matheisen et al., (2005), Song et al., (2008), Bradac et al. (2002) and Gutierrez (2008) have identified that Bluetooth faces issues linked to its topology (which limits its scalability), wake-up times and overall protocol complexity. The latter case arises because Bluetooth specification addresses the need of wide range of applications. Therefore, to deliver the required QoS has resulted in increased complexity. Even though Bluetooth is regarded as low-power solution, yet it cannot support connectivity of low-rate applications in a range of months or years running on standalone battery as preferred in process automation (Matheisen et al., 2005).

In an effort to address the energy issue, Bluetooth v4.0 specification includes Bluetooth Low Energy protocols to cater the connectivity demand for applications with severe power constraints. This ultra-low power (ULP) Bluetooth technology is aimed for markets such as health care, sports, fitness and security. The key features of this technology include ultra-low power consumption, low-cost, small-size and lightweight protocol stack (Nordic, 2011). In order to reduce power consumption, ULP technology employs a variable connection interval. In addition, the time to scan the presence of

other devices in range is also reduced by limiting advertising channels. Bluetooth low energy wireless technology utilizes two types of transceivers: Bluetooth low energy chip and Bluetooth v4.0 chip (Nordic, 2011). The aforementioned chip can communicate with other low energy chips and with Bluetooth v4.0, whereas, the Bluetooth v4.0 version can further communicate with legacy Bluetooth chips (Nordic, 2011). In short, the ULP technology is optimized for power, whereas, the other shortcomings of the Bluetooth technology as mentioned before still hinder the adoption of Bluetooth technology in process automation. Also, as ULP is a relatively new endorsed standard, the compliant devices have started emerging and the technology is in its early stages of evaluation.

B1.3. ZigBee

Overview

The ZigBee is also a WPAN technology and is based on IEEE802.15.4 standard which specifies the MAC and PHY for Low-Rate WPAN applications. ZigBee provides inexpensive and short distance connectivity solution, and was primarily designed for applications in home and building automation, which are light-weight applications (Elahi *et al.*, 2010). ZigBee alliance specifies the higher level protocols for routing and networking operating over the IEEE802.15.4 stack. IEEE802.15.4 offers twenty seven channels over three bands: one in 868MHz (Europe), ten in 902-928MHz (USA), and sixteen available in 2.4GHz ISM band (Worldwide) (IEEE 802.15.4, 2006). In 2.4GHz band the theoretical bit rate is 250 kbps.

ZigBee defines three classes of devices: ZigBee Coordinator (responsible for network formation), ZigBee Router (responsible for routing) and ZigBee End Devices (which do not take part in routing). ZigBee network supports topologies such as star, tree and mesh. In *mesh networking* each node is connected to many other nodes within its communication range. As a result, mesh networks can extend the network coverage beyond LOS due to extra hops. Furthermore, alternate paths can be used to reroute the message around broken and blocked paths. Other relevant features supported by the standard include low-duty cycle and low-power consumption modes. ZigBee network devices like Reduced-Function Device (RFD) are designed to spend most of the time in sleep mode to save power. When these devices need to transmit they change their mode

to transmit mode. Time needed to transit from sleep to active mode is 15ms (Elahi *et al.*, 2010).

Suitability

ZigBee is a purpose built standard for lightweight automation applications which requires low-data rate and low-cost communications. It has been designed for applications where power consumption is critical and the frequent changing of onboard battery is cumbersome, expensive and undesirable. Therefore, it offers ultra-low power consumption (for extended lifetime), small protocol stack (simplicity), mesh networking (for reliability) and security features (Koubaa *et al.*, 2005). Investigation into the ZigBee standard and its supported features by Gustafsson (2009), Mathiesen *et al.* (2005), Biasi *et al.* (2008) and Lenvall (2008) have identified that ZigBee has low QoS guarantee which makes it less feasible for industrial applications. Moreover, it is also not industrial grade as it does not support determinism and also does not use frequency hopping mechanism which makes it susceptible to interference (Farahani, 2008). The reasons which make ZigBee unsuitable for process automation include: no support for message priority which can have severe consequences, covering a larger area using Full Function Device (FFD) with no sleeping routers consumes power, no path discovery, and lack of channel blacklisting further can add delays and affect QoS. Therefore, based on the arguments presented above ZigBee is not suited for process automation.

In order to address the shortcomings of the first version of the ZigBee standard, the ZigBee-2007 release has specified two stacks, one for light-duty applications and other known as ZigBeePRO for industrial applications. ZigBeePRO will be discussed in Section 2.4.

B1.4. Ultra-wideband (UWB)

Overview

For simplicity, UWB based technologies will be referred to as UWB in this document. If any particular UWB standard needs to be addressed then it will be explicitly mentioned. UWB technology aims at applications which require high bandwidth for communication and the desired range of operation is within 10m (Matin, 2009). Such applications include digital video and audio streams. UWB systems require a large bandwidth to

operate. Access to such a bandwidth is possible given that the transmission power is kept low and within the spectral power density limits set by the local regulator. As a result, the UWB signal would appear as a noise to the coexisting narrowband communication technologies. In 2002, FCC released the band from 3.1 to 10.6 GHz to be used by the UWB systems in the USA (Matin, 2009). UWB emission limits vary for both indoor and outdoor use, as the UWB band also covers regions which include bands used by GPS, cellular networks and WLANs. The maximum EIRP limit set by FCC is -41.25 dBm/MHz, and varies with frequency (Matin, 2009). More restrictive regulations regarding the frequency range and maximum power spectral densities allowed for UWB systems are found in Europe, Japan and China [Matin (2009), Xia *et al.* (2009)]. There are two incompatible schemes for the use of UWB systems proposed by WiMedia Alliance and UWB Forum (Garg, 2007). The specification of the WiMedia Alliance is based on Multiband OFDM (MB-OFDM) scheme and supports high data rates of up to 480 Mbps (Stieglitz, 2011). On the other hand, the specification of the UWB is based on Direct Sequence UWB (DS-UWB) (Stieglitz, 2011). WiMedia UWB has attained more attention in recent years and is backed by USB Forum to certify wireless USB (Akyildiz, 2009).

In MB-UWB, information is independently encoded in different bands. Higher data rate can be achieved with low signaling rate, which relaxes the need to use high power digital processing at the transceiver (Matin, 2009). WiMedia MAC is a peer-to-peer protocol, and considers every device in a network to be the peer of other devices in network (Akyildiz, 2009). The time axis in WiMedia MAC is divided into superframes, which are further subdivided to accommodate beacons and data transmission periods. WiMedia specification supports two access methods, Distributed Reservation Protocol (DRP) and Prioritized Contention Access (PCA). DRP provides exclusive access to channel, whereas, the latter method utilizes a CSMA/CA scheme. PCS is suitable for non-real time traffic.

Suitability

UWB offers enormous bandwidth which makes UWB eligible to tackle multipath fading and narrow band jamming, and also has better material penetration capability (Matin, 2009). UWB technology is not primarily designed for automation and has resulted in different frequency band allocation in Europe and the USA along with two distinct and

incompatible specifications. These regulatory and standardization issues are amongst the key barriers hindering the adoption of the UWB technology (Viitala *et al.*, 2006). Xia *et al.* (2009) have highlighted issues linked to MAC which needs to be addressed in order to gain full access to the PHY properties, based on MB-OFDM. These issues include beacon period (which varies with beacon group), frame payloads (aligned with respect to large payloads), and limited range of about 10 m. In addition, Cheri *et al.* (2008) have highlighted the challenges associated with UWB systems which include pulse shape distortion, high-frequency synchronization and short distance communication due to low transmission power. Akyldiz *et al.* (2009) have also highlighted the limitation of the WiMedia MAC concerning the multi hop resource allocation and mesh network formation.

There are still reservations related to use of UWB technology as it has potential to interfere with many other users, even though the emission levels are very low (Rahim, 2009). Kar *et al.* (2006) have identified the potential which this technology holds for automation, and has highlighted that the key application for UWB in automation is still to be defined.

Appendix B2. IEEE 802.15.4-2006

The 2006 revision of the IEEE 802.15.4 standard defines the MAC and PHY for devices which require low-data-rate, low-power, and short-range radio frequency transmissions. It applies to both fixed or moving portable devices. The standard offers small, power-efficient, less-complex and inexpensive connectivity solution (Lee et al., 2007). The coverage of the network may extend beyond 10 meters. However, the well-defined coverage area does not exist because wireless media characteristics are dynamic and uncertain.

The PHY defined in IEEE802.15.4 can operate at three different frequency bands: 2.4 GHz, 915 MHz and 868 MHz ISM bands. The number of channels available in each of these bands varies geographically. There are 16 channels in the 2450 MHz band, 30 channels in the 915 MHz band, and 3 channels in the 868 MHz band (IEEE 802.15.4, 2006). The standard defines four PHY layers, with over-the-air supported data rates ranging from 20 to 250 kbps. Different modulation schemes are allowed, and are summarized below.

- An 868/915 MHz DSSS PHY employing binary phase-shift keying (BPSK) modulation supports data rate of 20 Kbps in 868 MHz band and 40 Kbps in 915 MHz band.
- An 868/915 MHz DSSS PHY employing offset quadrature phase-shift keying (O-QPSK) modulation has data rate support for 100 Kbps in 868 MHz band and 250 Kbps in 915 MHz band.
- An 868/915 MHz parallel sequence spread spectrum (PSSS) PHY employing BPSK and amplitude shift keying (ASK) modulation offers data rates of 250 kbps in both bands.
- A 2450 MHz DSSS PHY employing O-QPSK modulation has data rate of 250 kbps.

In addition, the symbol rates as supported by the standard allow the delay spread found in industrial environment not to cause a reception problem (Willig *et al.*, 2005).

The access to the communication channel as specified by the IEEE 802.15.4 MAC is defined via two modes, beacon or non-beacon mode. In beacon mode, the Network

Coordinator (NC) imposes a superframe structure and transmits beacons periodically. The superframe starts with the contention-access period, in which the Reduced-Function Devices (RFDs) access the medium according to a slotted CSMA-CA variant. Beacon-mode helps conserve energy as the superframe structure can include an inactive period in which devices can go to sleep mode during non-operational time. In addition, collisions can be avoided by assigning guaranteed time slot (GTS) to the devices. On the other hand, the non-beaconed mode utilizes a variant of unslotted CSMA, where the packet initialization does not perform carrier sense immediately, but introduces a random back-off time to avoid collision. The throughput varies between beacon and non-beacon mode, due to the associated overheads. The CSMA/CA collision avoidance MAC is not suitable for time critical industrial applications, however, because the message delays cannot be controlled (Wagner, 2010). For process automation the time slots for transmission have to be guaranteed. The standard also supports acknowledgments and retransmissions. The maximum size of the PHY Protocol Data Unit (PPDU) is 127 bytes. The security of the network is essential, and the standard offers authentication, encryption (32 to 128 bit AES), and integrity services.

In summary, the MAC and PHY specified by the IEEE 802.15.4 standard is suitable for industrial applications, as it is license-free, energy-efficient, and has worldwide availability. The communication technologies which will be introduced next are based on IEEE 802.15.4 specification.

Appendix C1. EM2 MSF Datasheet

Receiver module EM2S MSF

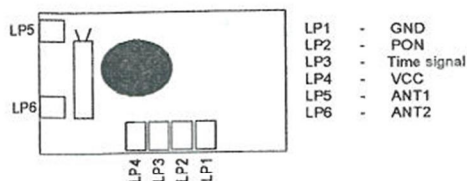
Order number: FBM 10020

The receiver module EM2S, working with a ferrite antenna, is a complete power stabilized receiver and demodulation unit for time signal senders. The output signal (at LP3) is the non inverted demodulated time signal.

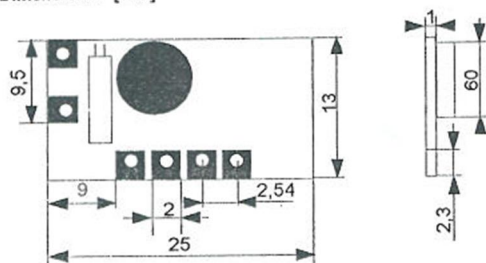
Pin configuration:



Original size



Dimensions: [mm]



Technische Rahmendaten :

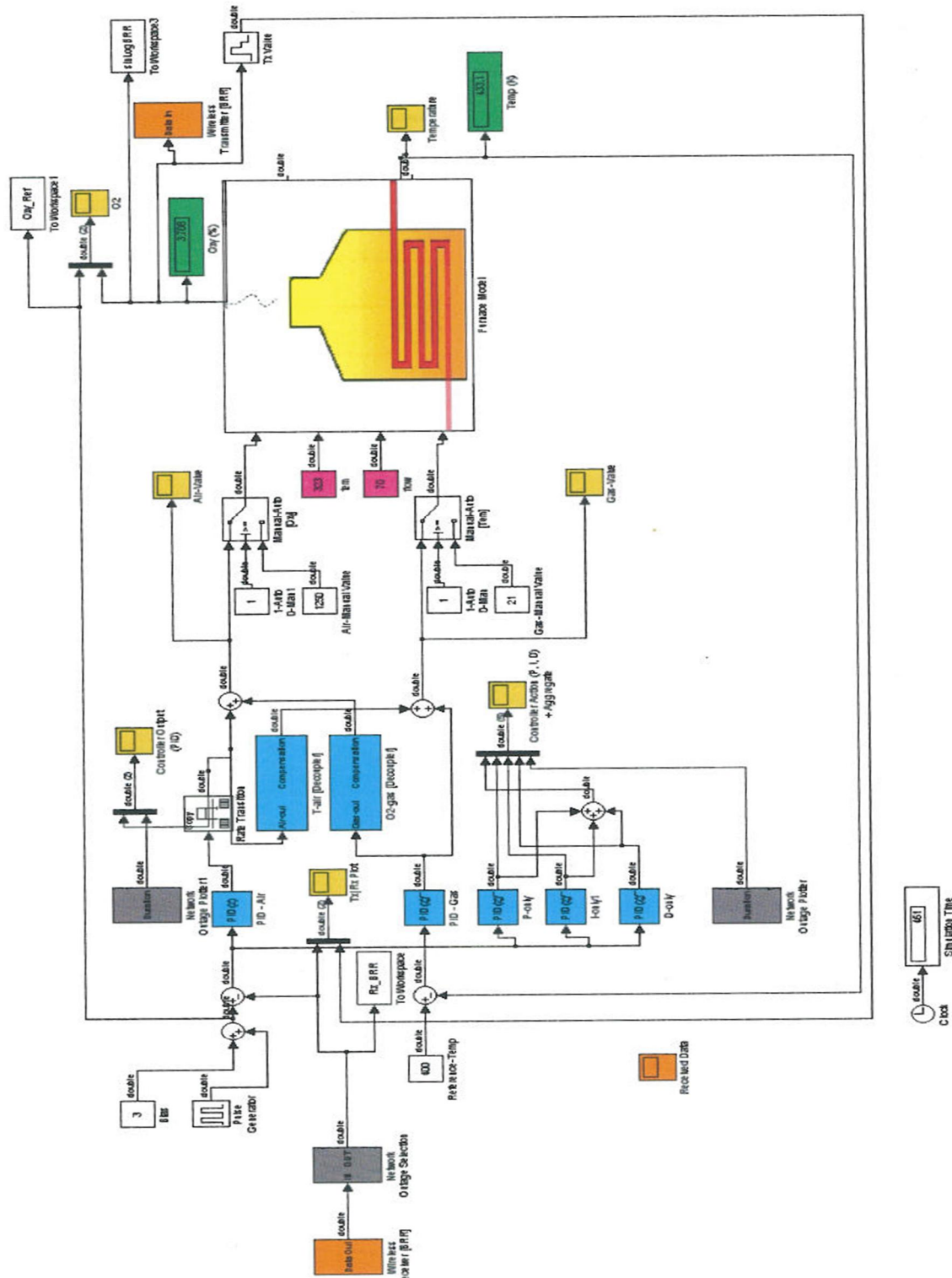
Parameters	Test conditions	Symbol	min	typ	max	Unit
Operating temperature range	$V_{CC} = 3V$	T	0		50	$^{\circ}C$
Power supply		V_{CC}	3		12	V
Power consumption	$V_{CC} = 3V, U_{PON} = 0V$	I_{CC}			200	μA
Input voltage ANT1-ANT2	$U_{CC} = 3V, U_{PON} = 0V$	U_{IN}		0,4	0,6	μV

Model :

Model (EM2S xxx)	Input signal	Note
EM2S MSF	MSF ; 60 kHz	Standard temperature range $0^{\circ}C - +50^{\circ}C$

Appendix D1. Simulink Model for Hardware in Loop

A scan of one of the Simulink models used in the hardware-in-loop simulation



Appendix D2. Time Slot Calculation

Parameter	Description
Γ_{offset}	Start of the time slot to the start of the preamble transmission.
Γ_{CCA}	Start of time to perform CCA and the time taken to perform CCA.
Γ_{error}	Accounts for the time synchronization error between transmitter and receiver.
$\Gamma_{PacketLength}$	Amount of time required to transmit a packet. Hence, it will take into consideration PhL, delimiter, payload and DLPDU.
$\Gamma_{AckDelay}$	End of the transmission to the start of ACK.
Γ_{Ack}	Time to transmit an ACK. This also takes into consideration the synchronization error.
Γ_{switch}	Time to switch from transmit to receive or vice versa.

Note: LIFS and SIFS are ignored.

$$\tau_{slot} = \Gamma_{offset} + \Gamma_{PacketLength} + \Gamma_{AckDelay} + \Gamma_{Ack} + \Gamma_{error}$$

$$\Gamma_{offset} = \Gamma_{CCA} + \Gamma_{switch}$$

References

- Alavi, S. M., Walsh, M. J., and Hayes, M.J. (2009), "Robust distributed active power control technique for IEEE 802.15.4 wireless sensor networks - A quantitative feedback theory approach", *Control Engineering Practice*, Vol. 17(7), pp. 805-814.
- ABB (2006), "What is process automation?"
<http://www.abb.com/cawp/db0003db002698/b3913fe3a1296b7bc12571f10040f47f.aspx>, (On-line Mar 12th, 2012).
- ABB (2009), "Wireless instrumentation driving down installation and maintenance cost with wireless connectivity",
[http://www05.abb.com/global/scot/scot203.nsf/veritydisplay/78e22efd3c8457dec125757b003a06f2/\\$File/PB_Wireless_Instrumentation_EN_Issue%201%20HR.pdf](http://www05.abb.com/global/scot/scot203.nsf/veritydisplay/78e22efd3c8457dec125757b003a06f2/$File/PB_Wireless_Instrumentation_EN_Issue%201%20HR.pdf) (On-line Feb 12th, 2012).
- Acharya, R., Vityanathan, V., Chellai, P. R. (2010), "WLAN QoS issues and IEEE 802.11e QoS enhancement", *International Journal of Computer Theory and Engineering*, 2(1), pp. 1793-8201.
- AD (2010), "ADF7242: low power IEEE 802.15.4/proprietary GFSK/FSK zero-IF 2.4 GHz transceiver IC", http://www.analog.com/static/imported-files/data_sheets/ADF7242.pdf (July. 15, 2012).
- Agbinya, J. I. (2009), "Planning and optimization of 3G and 4G wireless networks", River Publishers, Denmark.
- Akerberg, J., Gidlund, M., Bjorkman, M. (2011), "Future research challenges in wireless sensor and actuator networks targeting industrial automation", 9th International Conference on Industrial Informatics (INDIN), (July. 26-29, 2011).
- Akyildiz, I. Kasimoglu, H. (2004) "Wireless Sensor and Actor Networks: Research Challenges", Elsevier, Georgia Institute of Technology, Atlanta.
- Akyildiz (2009), "Wireless Mesh Networks", John Wiley and Sons, London.
- Akyol, B. A., Hirkham, H., Clements, S. L., Hadley, M. D. (2010), "A survey of wireless communications for the electric power system", US Department of Energy, USA.
- Allison, J., Hormigo, R., and Jovanov, E. (2003), "A low-power geographically distributed data acquisition system with WWVB synchronization", *Proceedings of the 35th Southeastern Symposium on System Theory*, Morgantown, (Mar. 16-18, 2003), pp. 162-166.
- Apprion (2012), "Apprion Dramatically Improves Industrial Safety With ION Safety Shower Application", <http://www.apprion.com/press/120417.asp> (On-line: Jul 12, 2012).
- Ares, Z.B., Park, P.G., Fischione, C., Speranzon, A., and Johansson, K.H. (2007), "On power control for wireless sensor networks: System model, middleware component and experimental evaluation", *Proceedings of IFAC European Control Conference*, Greece, (Jul. 2-5, 2007).
- Arzen, k. E., Bicchi, A., Johansson, K. H., and Legros, J. (2006), "On the design and control of wireless networked embedded systems", *Proceedings of the 2006 IEEE Conference*

- on Computer Aided Control Systems Design Munich, Germany, (Oct. 4-6, 2006), pp. 440-445.
- ASCE (1994), "Glossary of the Mapping Sciences", Edited by American Society of Civil Engineers, ASCE Publication, USA.
- Atmel (2009), "ZigBit 2.4GHz wireless modules, ATZB-24-A2/B0", <http://www.atmel.com/products/zigbee.asp> (On-line: Nov 18th, 2011).
- Bai, J., Eyisi, E. P., Xue, Y., Koutsoukos, X. D., (2011), "Distributed sampling rate adaptation for networked control systems", The 1st International Workshop on Cyber-Physical Networking Systems, Shanghai, China, (Apr. 10-15, 2011).
- Barr, M., Masa, A. (2007), "Programming Embedded Systems", Second Edition, O'Reilly Media Inc, Sebastopol, CA, USA.
- Bemporad, A., Heemles, M., Johansson, M. (2010), "Networked Control Systems", Springer, Berlin.
- Biasi, M. D. (2010), "Implementation of a WirelessHART Simulator and its use in Studying Packet Loss Compensation in Networked Control", Masters' Thesis, KTH, Stockholm, Sweden (Jan. 20, 2012).
- Biasi, M. Snickars, C, Landernas, K., Isaksson, A. J. (2008), "Simulation of process control with wireless HART networks subjected to packet losses", 4th IEEE Conference on Automation Science and Engineering, Washington DC, USA, (August 23-26), pp. 548-553.
- Bickerstaff, J., Phocas, M., and Haddrell, T. (2005), "The enemy inside GPS jammed by room", Host, Self. GPS World 16(3), pp.33-39.
- BIPM (2010), "Bureau International Des Poids et Mesures", Volume 5, BIPM, Paris.
- Bishop, R. H. (2005), "Mechatronics: An introduction", CRC Press, Stockholm, Sweden.
- Bishop, R. H. (2008), "Mechatronic Systems, Sensors, and Actuators: Fundamentals and Modeling", CRC Press, USA.
- Bletsas, A. (2005), "Evaluation of Kalman filtering for network time keeping", IEEE Transactions on Ultrasonics, Ferroelectrics and Frequency Control, Vol 52(9), pp.1452 -1460.
- Bluetooth Special Interest Group, (2001), "Specification of the Bluetooth system, specification Volume 1", <http://www.bluetooth.com> (July 15 2012)
- BP (2011), "Corrosion Management", Issue 2, <http://www.bp.com/sectiongenericarticle.do?categoryId=9039655&contentId=7069586> (Accessed on-line on Jan 12, 2012).
- Bradac, Z., Zezulka, F., and Kucera, P. (2002), "Bluetooth for low-level process control", International Carpathian Control Conference ICC' 2002, (May 27-30), Malenovice, Czech Republic.
- Bregni, S. (2011), "Synchronization of Digital Telecommunication Networks", John Wiley and Sons, Cornwall, Great Britain.
- BS6656:2002, "Assessment of inadvertent ignition of flammable atmospheres by radio-frequency radiation", BSI, London.

- Buda, A., Schuermann, V., and Wollert, J. F. (2010), "Wireless technologies in factory automation", Javier Silvestre-Blanes (Ed.), ISBN: 978-953-307-024-7, InTech.
- Calandrini, D. (2002), "The benefits of fieldbus technology in power plants", Siemens Westinghouse Power Corporation, Alpharetta, ISA, USA.
- Callaghan, S. A., Inglis, I., Hansell, P. (2006), "Impact of introducing automatic transmit power control in P-P fixed service systems operating in bands above 13 GHz".
- Carlsen, S. Petersen, S (2010), "When the industry goes wireless: drivers, requirements, technology and future trends", Javier Silvestre-Blanes (Ed.), ISBN: 978-953-307-024-7, InTech.
- Carlsen, S., Skavhug, A., Petersen, and S., Doyle, P. (2009), "Wireless sensor network installed on a north sea platform", World Oil, Vol. 230 (9).
- Caro, D. (2004), "Wireless Networks for Industrial Automation", 3rd Edition, ISA, North Carolina, USA.
- Che203.1 (2008), "Process Control Project Lecture Notes", Department of Chemical Engineering, Imperial College London, London.
- Chen J. Adrian, M., Irwin, g. W., and Scanlon, W. G. (2008), "Experimental characterization and analysis of wireless Network Control Systems", Irish Conference on Signals and Systems, Galway, Ireland, (June. 18-19, 2008), pp. 238-243.
- Chen, D. Nixon, M., and Mok, A. (2010), "WirelessHART: Real-Time Mesh Network for Industrial Automation", Springer Science + Business Media LLC, New York, USA.
- Chen, Y., Wang, Q., Chang, M. Terzis, A. (2011), "Ultra-low power time synchronization using passive radio receivers", The International Conference on Information Processing in Sensor Networks, Chicago, Illinois. (April. 12–14), pp. 235-245.
- Cheri, A., Fortier, P., and Tardif, P-M. (2008), "An investigation of UWB-based wireless networks in industrial automation", International Journal of Computer Science and Network Security, 8(2), pp. 179-188.
- Chen, Y., Wang, Q., Chang, M., and Terzis, A. (2011), "Ultra-low power time synchronization using passive radio receivers". 10th International Conference on Information Processing in Sensor Networks (IPSN), Chicago, Illinois , pp. 235-245, (April 12–14, 2011).
- Choi, D. & Kim, D. (2008), "Wireless fieldbus for networked control systems using LR-WPAN", International Journal of Control, Automation, and Systems, Vol. 6, pp.119-125.
- Christin, D., Mogre, P., and Hollick, M. (2010), "Survey on wireless sensor network technologies for industrial automation: The Security and Quality of Service Perspectives". www.mdpi.com/1999-5903/2/2/96/pdf (Retrieved on-line on: Sep 12, 2011).
- Cisco (2004), "Channel deployment issues for 2.4GHz band", <http://www.cisco.com/en/US/docs/wireless/technology/channel/deployment/guide/Channel.pdf> (Retrieved on-line on: Feb 17, 2010)
- Claesson, V., Lonn, H. and Suri, N. (2004), "An efficient TDMA start-up and restart synchronization approach for distributed embedded systems". parallel and distributed systems, IEEE Transactions, Vol. 15(8), pp. 725-739.

- Clark, D. (2004), "Use and restrictions in license free radio bands", <http://www.dur.ac.uk/d.j.clark/Reports/LicFreeBands.pdf> (Retrieved on-line: Aug 12, 2010)
- Clynch, J. R. (2002), "Precise time and time interval clocks, Time Frames and Frequency", http://www.gmat.unsw.edu.au/snap/gps/clynch_pdfs/pttinode.pdf (Retrieved on-line: Mar 8, 2010).
- C-MAX (2011), "The time code", <http://www.c-max-time.com/tech/msf.php>, (Jun. 8, 2011).
- Colandairaj, J., Irwin, G. W., Scanlon, G. W., (2005), "Analysis and co-simulation of an IEEE 802.11b wireless networked control system", 16th IFAC World Congress, Prague, Czech Republic, (July 4-8, 2005).
- Correia, L. H. A., Macedo, D. F., Santos, A. L., Loureiro, A. A. F., and Nogueira, J. S. (2007), "Transmission power control techniques for wireless sensor networks", *Computer Networks*, Vol. 51, pp. 4765-4779.
- Cover, T.M., and Thomas, J.A. (2006), *Elements of information theory*, 2nd Edition, John Wiley and Sons.
- Dargie, W. and Poellabauer, C. (2010), "Fundamentals of Wireless Sensor Networks: Theory and Practice", John Wiley and Sons, Chichester, West Sussex, United Kingdom.
- DCF77 (2010), "DCF77 longwave time signal", www.meinberg.de/english/info/dcf77.html (On-line: May. 4, 2011).
- Dedes, G., and Dempster, A.G. (2005), "Indoor GPS positioning: challenges and opportunities". *Vehicular Technology Conference*, Dallas, Texas, USA (Sep 28-25, 2005), pp. 412-415.
- Denbow (2011), "Which way for the wireless waves?" <http://www.controlglobal.com/industrynews/2011/052.html> (Jul. 21, 2011).
- DoE (2002), "Industrial wireless technology for the 21st Century", Department of Energy, USA.
- Doody, D. (2009), "Deep Space Craft: An Overview of Interplanetary Flight", Springer, California, USA.
- Dooley, S.R., and Nandi, A.K. (1998), "Adaptive time delay and frequency estimation for digital signal synchronization in CDMA systems". 32nd Conference on Signals, Systems & Computers, Pacific Grove, California, USA, (Nov 1-4, 1998), pp. 1838-1842.
- Douros, V.G. and Polyzos, G.C. (2011), "Review of some fundamental approaches for power control in wireless network", *Computer Communications*. 34(13), pp.1580-1592.
- Doyle, P. Petersen, S., Vatland, S., Aasland, C.S., Andersen, T.M. and Sjong, D. (2007), "Requirements, drivers and analysis of wireless sensor networks for the oil & gas industry", 12th IEEE International Conference on Emerging Technologies and Factory Automation, Patras, Greece (25-27 Dec, 2007).
- Drathen, H. (2009), "Process Automation Trends", *ACHEMA Worldwide News*, available at: http://www.dechema.de/dechema_media/ (Accessed on-line: Nov 20th, 2009).
- Drentea, C. (2010), "Modern communications receiver design and technology", Artech House, USA.

- EH (2010), "Unlock your plant's potential with WirelessHART", <http://www.uk.endress.com/eh/sc/europe/uk/en/home.nsf/#page/potential> (Apr. 26, 2011).
- Eidson (2006), "Measurement, control, and communication using IEEE 1588", Springer, London.
- Elahi, A., and Gschwender, A. (2010), "ZigBee Wireless Sensor and Control Network", Prentice Hall, Boston, USA.
- Elson, J. and Romer, K. (2003), "Wireless Sensor Networks : A new regime for time synchronization". *ACM Computer Communication Review*, Vol. 33(1), pp.149-154.
- Emerson (2008), "Emerson smart wireless technology used by BP cherry point and naperville to improve process equipment monitoring and availability", http://www2.emersonprocess.com/siteadmincenter/PM%20Central%20Web%20Documents/SmartWirelessApps_BP-CPN.pdf (Sep. 12, 2010)
- Emerson. (2009), "Emerson's smart wireless thum adapter upgrades existing HART instruments to access diagnostics and process variables", Emerson, USA.
- Emerson. (2009a), "Wireless technology offers mining operations improvement", http://www2.emersonprocess.com/siteadmincenter/PM%20Articles/MiningEngineering_Nov09.pdf mining Engineering (Feb. 16, 2012).
- Emerson. (2010), "Emerson's smart wireless and tyco thermal controls' trace Tek technologies combine to provide wireless hydrocarbon leak detection", <http://www2.emersonprocess.com/en-us/news/pr/pages/1007-702-tyco.aspx> (Jun. 12, 2012).
- Endruntechnologies (2009), 'Establishing Traceability to UTC', <http://www.endruntechnologies.com/pdf> (Oct. 9, 2011).
- Farahani (2008), "ZigBee wireless networks and transceivers", USA: Elsevier.
- FeedNetBack (2010), "Co-design for Networked Control Systems", <http://www.feednetback.eu/> (On-line: Sep 9, 2010).
- Ferre, P., Doufexi, A., Nix, A., and Bull, D. (2004), "Throughput analysis of IEEE 802.11 and IEEE 802.11e MAC", *Wireless Communications and Networking Conference*, Atlanta, (Mar 21-25, 2004), pp. 783-788.
- Ferris, M. (2010), "Next-Gen wireless in control systems. Real world wireless", (Feb. 23, 2010) [Presentation given at: IET Workshop on Next-Gen wireless in control systems]: IET London: Savoy Place, UK.(Feb. 23, 2010)
- FF (1999), "Foundation Fieldbus", http://www.samson.de/pdf_en/l454en.pdf, Samson. (Retrieved on-line on Jan. 4, 2012).
- Flammini, A., Ferrari, P., Marioli, D., Sissini, E., and Taroni, A. (2008), "Wired and wireless sensor networks for industrial applications", Elsevier: *Microelectronics Journal*, Vol. 40 (9), pp. 1322-1336.
- Forgue, B. (2010), "Next-Gen wireless in control systems, going wireless: why and how? (Feb. 23, 2010) [Presentation given at: IET Workshop on Next-Gen wireless in control systems]: IET London: Savoy Place, UK, (Feb. 23, 2010).
- Enstad, G. and Ralston, J. (2010), "Applying wireless to EtherNet/IP industrial automation systems",

Prosoft Technology Inc., Bakersfield, CA.

- Fodor, G., Racz, A., Reider, N. and Temesvary, A. (2009), "3GPP LTE Radio and Cellular Technology", Auerbach Publications Florida, USA.
- Galleon. (2009), "EM2S radio receiver module-datasheet", <http://www.galsys.co.uk/modules> (Retrieved on-line on Feb 2, 2009).
- Garg, V. (2007), "Wireless Communications and Networking", Morgan Koufmann, San Francisco, USA.
- Georgiev, B. (2003), "Field control systems", Proceedings of the 6th Scientific Conference on Electrical Engineering and Information Technology, Bratislava, Slovakia (Nov, 25, 2003).
- Goyal, M., Prakash, S., Xie, W., Bashir, Y., Hosseini, H., and Durrezi, A. (2010), "Evaluating the impact of signal to noise ratio on IEEE 802.15.4 PHY-level packet loss rate", 13th International Conference on Network-Based Information Systems, (pp.279-284), (Sep. 14-16, 2010).
- Gjendemsjø, A., Gesbert, D., Øien, G. E., and Kiani, S. G. (2007). "Binary power control for multi-cell capacity maximization", IEEE Workshop on Signal Processing Advances in Wireless Communications, pp. 1-5, (Jun 17-20, 2007).
- Groover, A. (2009), "Automation", <http://www.britannica.com/EBchecked/topic/44912/automation> (Sep. 10, 2010).
- Gungor, V.C and Hancke, G.P (2009) "Industrial wireless sensor networks: Challenges, design principles, and technical approaches", IEEE Transactions on Industrial Electronics, Vol. 56 (10), pp. 4258-4265.
- Gupta, R. A., and Chow, M-U. (2010), "Networked control system: Overview and research trends", IEEE Transactions on Industrial Electronics, Vol. 57 (7), pp. 2527-2535.
- Gustafsson, D. (2009), "WirelessHART-Implementation and Evaluation on Wireless Sensors", Masters' Thesis, KTH, Stockholm.
- Gutierrez, J. (2008), "WirelessHART: The industrial wireless standard", www.labmate-online.com/article_read/359 (Retrieved on-line on Sep 17, 2011).
- Han, S., Zhu, X., Aloysius, K.M., Nixon, M., Blevins, T., Chen, D. (2010), "Control over wireless HART network", 36th Annual Conference on IEEE Industrial Electronics Society, Glendale, USA (Nov 7-10, 2010).
- Hartebrodt, M. & Kabitzsch, K. (2004), "Fault detection in fieldbuses with time domain reflectometry", 7th AFRICON Conference in Africa, (17 Sep, 2004) pp. 391-396.
- Harmegnies, A., Panfilo, G., and Arias, E. F. (2009), "BIPM time activities update", <http://www.dtic.mil/dtic/tr/fulltext/u2/a517922.pdf> (On-line May 28, 2011).
- HBG (2008), "Description of the HBG time signal" http://www.metas.ch/root_legnet/HBG (May. 4, 2010).
- HCF (2009), "Control over wirelessHART", http://www.hartcomm.org/protocol/training/resources/wiHART_resources/Control_with_WirelessHART.pdf (Sep. 16, 2010).

- He, T., Stankovic, J. A., Lu, C., and Abdelzaher, T. (2003), "SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks", International Conference on Distributed Computing Systems, Providence, RI, USA, (19-22 May, 2003).
- Hellan, S., Stengel, O. (2005), "CC1020/1021 received signal strength Indicator", Application Note AN030, Chipcon Products from Texas Instruments, <http://www.ti.com/lit/an/swra062/swra062.pdf> (15th July 2012).
- Hellbrück, H. and Esemann, T. (2011), "Limitations of Frequency Hopping in 2.4 GHz ISM-Band for Medical Applications Due to Interference", In the Proceedings of the Workshop on Consumer eHealth Platforms, Services and Applications (CeHPSA), Las Vegas, USA, (9-12 Jan, 2011).
- Hellweg, J. F. (1940), "United States Navy Time Service", Journal, Publications of the Astronomical Society of the Pacific, Vol. 52, No. 305, p.17.
- Heidari, G. (2008), "Wimedia UWB: Technology of choice for Wireless USB and Bluetooth", John Wiley & Sons, Chichester, West Sussex, United Kingdom.
- Hespanha, j. P., Naghshtabrizi, P., Yonggang, Xu. (2007), "A survey of recent results in networked control systems", Proceedings of the IEEE Vol. 95 (1), pp. 138-162.
- Hofmann, R. and Hilgers, U. (1998), "Theory and tools for estimating global time in parallel and distributed systems". Proceedings of the sixth Euromicro Workshop on Parallel and Distributed Processing, Vol 98, pp. 173-179.
- Holma, H. and Toskala, A. (2010), "WCDMA FOR UMTS - HSPA evolution and LTE", 5th Edition, John Wiley and Sons New Jersey, USA.
- Honeywell (2012), "An open, standard-based wireless network: Connecting WirelessHART® Sensor Networks to Experion™ PKS using Honeywell's One Wireless™ Network", Honeywell, USA.
- Hossian, M.M.A., Mahmood, A., and Jäntti, R. (2009), "Channel ranking algorithms for cognitive coexistence of IEEE 802.15.4", 20th International IEEE Symposium on Personal, Indoor and Mobile Radio Communications, pp.112-116, (Sep 13-16, 2009).
- Hoult, N., Bennet, P.J., Stoianov, I., Fidler, P., Maksimovic, C., Middleton, C., Graham, N., Soga, K. (2009), "Wireless Sensor Networks : Creating Smart Infrastructure", Proceedings of the ICE – Civil Engineering, Vol 162(3), pp.136-143.
- Hong, S. H. (1995), "Scheduling algorithm of data sampling times in the integrated communication and control systems". IEEE Transactions on Control Systems Technology, Vol. 3(2), pp. 225–230.
- HP (1997), "The science of time keeping: application note 1289", http://www.allanstime.com/Publications/DWA/Science_Timekeeping/TheScienceOfTimekeeping.pdf (Retrieved on-line on Oct 12, 2010).
- Hristu-Varsakelis, D and Levine, W (2005), "Handbook of Networked and Embedded Control Systems", Birkhauser, Boston, USA.
- Hung, H-H. and Chen, L-J (2008), "An Analytical Study of Wireless Error Models for Bluetooth Networks", 22nd International Conference on Advanced Information Networking and Applications, Beijing, 25-28 March 2008, pp. 1317-1322.

- Humphrey, D. and Forbes, H. (2008), "Wireless in process automation- trend and outlook", <http://www.arcweb.com/pages/default.aspx> (Retrieved on-line on Sep 12, 2009).
- Hunn, N. (2010), "Essential of short-range wireless", Cambridge University Press, Cambridge, United Kingdom.
- IEC: International Electrotechnical Commission (2009) IEC/PAS62601:2009, "Industrial communication networks – Fieldbus specifications WIA-PA communication network and communication profile", British Standards Institute.
- IEC: International Electro technical Commission. (2010), IEC 62591:2010, "Industrial communication networks - Wireless communication network and communication profiles – Wireless HART".
- IEEE 802.15.4. (2006), "Part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)". Standard available at: <http://standards.ieee.org/findstds/standard/802.15.4-2006.html>.
- Ikram, W., Stoianov, I. and Thornhill, N.F. (2010), "Towards a radio-controlled time synchronized wireless sensor network: A work in-progress paper", IEEE Conference on Emerging Technologies and Factory Automation, (Sep 13-16, 2010), pp. 1-4.
- International Electro technical Commission., (2009), IEC/PAS62601:2009, "Industrial communication networks – Fieldbus specifications –WIA-PA communication network and communication profile", BSI, London.
- International Electro technical Commission. (2010), "IEC 62591:2010, Industrial communication networks - Wireless communication network and communication profiles – Wireless HART", BSI, London.
- Irwin, G. (2006), "Performance analysis of IEEE 802.11 technology for wireless feedback control", The IEE Control & Automation Professional Network. <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01599670>, (Retrieved on-line: May 8, 2010).
- ISA-95 Part 3 (ANSI/ISA-95, 2000), "Activity Models of Manufacturing Operations Management", ISA, USA.
- ISA 100.11a. (2011), "ISA-100.11a-2011 Wireless systems for industrial automation: Process control and related applications", ISA Publications, Research Triangle Park, North Carolina, USA.
- ISA-100.11a. (2009), "Wireless systems for industrial automation: Process control and related applications", ISA-100.11a-2009 Standard, 2009.
- Jafari, A. M., and Walter, L. (2011), "Optimal sample rate for wireless sensor actuator network", International Journal of Computer Science, Vol. 36 (4), pp. 24-32.
- Jämsä-Jounela, S.-L. (2007), "Future trends in process automation", Annual Reviews in Control, Vol. 31(2), pp. 211-220.
- Jespersen and Fitz-Randolph (1999), "From Sundials to Atomic Clocks: Understanding Time and Frequency" Second Edition, General Publishing Company, Ontario, Canada.

- Johansson, K. H. (2009), "Wireless Control: Opportunities and challenges", [Presentation given at: ACCESS Linnaeus Centre School of Electrical Engineering, KTH, Stockholm, Sweden], (Oct 31st, 2009).
- Johnston, G. and Munns, A. (2008), "WirelessHART: Signals a change at plants", [http://www05.abb.com/global/scot/scot212.nsf/veritydisplay/acbcd2bcb0e9f5478525748700540ccf/\\$file/pr-chemicalproc_wirelesshart\(7-08\).pdf](http://www05.abb.com/global/scot/scot212.nsf/veritydisplay/acbcd2bcb0e9f5478525748700540ccf/$file/pr-chemicalproc_wirelesshart(7-08).pdf), Publisher: www.chemicalprocessing.com (Retrieved on-line on Sep 12, 2010).
- Johnston, G. (2010), "Wireless for Process-Fortification of pillars", [Presentation given at: IET Workshop on Next-Gen wireless in control systems], London, Savoy Place, UK. (Feb. 23, 2010).
- Kar, E. D., Lukszo, Z., Leus, G. (2006), "Wireless networks in the process industry: opportunities for ultra wideband applications", International Conference on Networking, Sensing and Control, Florida, USA, (April. 23–25, 2006).
- Karl, H and Willig, A. (2007), "Protocols and architectures for wireless sensor networks", Wiley, Chippingham, Wiltshire, UK.
- Kennedy, J. F. & Mistry, J. (2003), "Instrumentation and Sensors for the Food Industry". Kress-Rogers, J.B. Brimelow (Eds.); Woodhead Publishing Ltd, Cambridge, UK, 2001.
- Khaleel, H., Pastrone, C., Penna, F., Spirito, M. A., and Garelo, R. (2009), "Impact of Wi-Fi traffic on the IEEE 802.15.4 channel occupation in indoor environments", International Conference on Electromagnetics in Advanced Applications (Sep 14-18, 2009), pp. 1042-1045.
- Khangura, K. Kaur, K. and R.S. Uppal, (2010), "Power control algorithms in wireless communication" International Journal of Computer Applications, Vol. 1 (12), pp. 82-87.
- Khemapech, I., Miller, A., and Duncan, I. (2007), "A survey of transmission power control in wireless sensor networks". 8th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting, pp.15-20.
- Kim, R., Nagayama, T., Jo, H., Spenser, B.F. (2012), "Preliminary study of low-cost GPS receivers for time synchronization of wireless sensors", Proceedings- SPIE The International Society For Optical Engineering : Sensors and Smart Structures Technologies for Civil, Mechanical, and Aerospace Systems, 2012 8345(1):8345 1A.
- Kim, D., Park, S., Kamg, k., and Lee, D. (2007), "Time-triggered wireless sensor network for feedback control", Mobile Communication Division, IEICE Electronics Express, Vol. 4 (21), pp. 644-649.
- Kim, A. N., Hekland, F. Petersen, S., and Doyle, P. (2010), "When HART goes wireless: Understanding and implementing the wirelessHART standard", <http://robotics.eecs.berkeley.edu/~pister/290Q/Papers/HART/When%20HART%20goes%20wireless%20NUST.pdf> (On-line: Aug. 12, 2011)
- Koscielniak, B. (2004), "About Time: A First Look at Time and Clocks", Houghton Mifflin Company, Singapore.
- Koubaa, A., Alves, M., Attia, M. and Nieuwenhuys, A. V. (2005), "IEEE 802.15.4 for wireless sensor networks: A Technical Overview", <http://www.hurray.isep.ipp.pt/docs> (May. 15, 2011).
- Kowoma (2007), "Composition of the data signal", <http://www.kowama.de> (Jun.19, 2011).

- Kuhn, M. (2006), "Low-frequency radio time signals", www.cl.cam.ac.uk/~mgk25/time/lf-clocks (On-line: May 4, 2010).
- Kuorilehto, M., Suhonen, J., and Hannikainen, M. (2007), "Ultra Low Energy Wireless Sensor Networks in Practice", Wiley, Chippingham, Great Britain.
- Labrador and Wightman. (2009), "Topology Control in Wireless Sensor Networks", Springer, Florida, USA.
- Lacatus, Catalin, David Akopian, and Mehdi Shadaram.(2012), "Reduced complexity cross-correlation interference mitigation in GPS-enabled collaborative Ad-hoc Wireless Networks", *Theory. Computers & Amp*, Vol. 38 (3), pp. 603-615.
- Lanzisera and Pister. (2007), "Theoretical and practical limits to sensitivity in IEEE802.15.4 receivers", 14th IEEE International Conference on Electronics, Circuits and Systems, (pp. 1344-1347) (Dec. 11-14, 2007).
- Lee, J-S., Su, Y-W., and Shen, C-C. (2007), "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi", 33rd Annual Conference of the IEEE Industrial Electronics Society, Taipei, Taiwan, (November 5-8, 2007).
- Lee, Y.D, Jeong, D., and Lee, H-J. (2010), "Performance analysis of wireless link quality in wireless sensor networks", 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), (2010), (pp.1006 -1010).
- Lemmon and Hu (2011), "Almost sure Stability of Networked Control Systems under Exponentially Bounded Bursts of Dropouts", In *Proceedings of the 14th International Conference on Hybrid Systems: Computation and Control*, pp. 301–310.
- Lennval, T., Svensson, S. and Hekland, F. (2008), "A comparison of wireless HART and ZigBee for industrial applications", *International Workshop on Factory Communication Systems*, Dresden, pp. 85-88, (May. 20-23, 2008).
- Lerner, L. S. (1996), "Physics: For Scientists and Engineers" Volume 2, Jones and Bartlett Publishers International, London.
- Lin, S., Zhou, G., Whitehouse, K., Wu, Y and Stankovic, J. A. (2009), "Towards Stable Network Performance in Wireless Sensor Networks, in Real-Time Systems", 30th International IEEE Symposium on Real-Time Systems, pp.227-237, (Dec 1-4, 2009).
- Lin, S., Zhang, G. J., Zhou, G., Gu, L., He, T., and Stankovic, J.A. (2006), "ATPC: Adaptive transmission power control for wireless sensor networks", 4th International ACM Conference on Embedded Networked Sensor Systems, pp. 223-236, (Nov 1-3, 2006).
- Liptak, B. G. (2012), "Instrument Engineers' Handbook: Process software and digital networks", fourth edition, CRC Press, New Jersey, USA.
- Lombardi, M. (2002), "NIST Time and Frequency Services". In *NIST Special Publication 432*, Vol. 2012: National Institute of Standards and Technology.
- Lombardi, M.(2010), "How accurate is a radio controlled clock". *Horological Journal* 152(3), pp.108-113.
- Lombardi (2003), "Radio Controlled Clocks", National Institute of Standards and Technology, <http://tf.nist.gov/general/pdf/1877.pdf> (On-line: May 26th, 2009).

- Lombardi (2008), "The accuracy and stability of quartz watches", <http://tf.nist.gov/general/pdf/2276.pdf> (On-line: Apr. 12, 2010).
- Lombardi (2010), 'How accurate is a radio clock?', <http://tf.nist.gov/general/pdf/2429.pdf> (On-line: Aug. 10, 2011).
- Luo, H. C., W, E. H-K., Chen, G.-H. "From Spatial Reuse to Transmission Power Control for CSMA/CA Based Wireless Ad Hoc Networks". In: International Conference on Parallel Processing Workshops.
- Maloco, J. McLoone, S. & Delaney, D. (2006), "Using rugby MSF broadcast for time division multiplexing synchronisation in a housing community sensor network", IET Conference Publications 2006, CP519, pp. 289-294.
- Maloco, J. (2010), "Design of a Wireless Mesh Sensor Network for a Housing Community", MEng Thesis, National University of Ireland, Maynooth. Ireland.
- Mathiesen, M., Thonef, G., and Aakvaag, N. (2005), "Wireless Ad-hoc networks for industrial automation: current trends and future prospects", 16th IFAC World Congress, Prague, Czech Republic, (July 4-8, 2005).
- Matin, M. (2009), "Ultra Wideband Preliminaries, Ultra Wideband", Boris Lembrikov (Ed.), ISBN: 978-953-307-139-8, InTech.
- Mazumder, S. K. (2011), "Wireless Networking Based Control", Springer, Illinois, USA.
- Meier, M. (2010), "Precise time synchronization for WSNs using the global positioning system", Masters' Thesis, Computer Engineering and Networks Laboratory (TIK), Department of Information Technology and Electrical Engineering, ETH, Zurich, Switzerland.
- Meshnetics (2007), "ZigBit-ZDM-A1281-PN/PN0", retrieved from <http://www.adaptivemodules.com> (Aug. 13, 2011).
- Meyer, F., Bahr, A., Lochmatter, T. and Borrani, F. (2012), "Wireless GPS-based phase-locked synchronization system for outdoor environment", Journal of Biomechanics 45(1), pp.188-190.
- Mitcheson, P. D., Yeatman, E. M., Rao, G. H., Holmes, A. S., and Green, T. C. (2008), "Energy harvesting from human and machine motion for wireless electronic devices", Proceedings of the IEEE, Vol. 96 (9), pp. 1457-1486.
- Miškinis, R., Smirnov, D., and Urba, E. (2011), "Timing and synchronization in mobile telecommunication networks", Joint Conference of the IEEE International and Frequency Control and the European Frequency and Time Forum (FCS), San Francisco, USA, pp. 1-5, (May 2-5, 2011).
- Mohammadi, A. and Akl, S. G. (2005), "Scheduling Algorithms for Real-Time Systems", Technical Report No. 2005-499, School of Computing, Queen's University, Kingston, Ontario, Canada.
- Moon, S. B., Skelly, P., and Towsley, D. (1999), "Estimation and removal of clock skew from network delay measurements", 18th Proceedings of the Annual Joint Conference of the IEEE Computer and Communications Societies, pp. 227-234 (Mar 21-25, 1999).
- Monition (2011), "Vibration Analysis", <http://www.monition.com/vibration-analysis.html> (On-line: Feb. 12, 2012).
- Motorola (2009), "Clock Functions and Synchronization", Motorola Inc., Illinois, USA.

- Muthukrishnan, K.; Koprnikov, G.; Meratnia, N. & Lijding, M. (2006), "Using time-of-flight for WLAN localization: Feasibility study", (TR-CTI), Centre for Telematics and Information Technology, University of Twente, Enschede.
- Myers, S., Megerian, S., Banerjee, S. and Potkonjak, M. (2007), "Experimental investigation of IEEE 802.15.4 transmission power control and interference minimization", 4th Annual IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks, San Diego, California, USA, pp. 294 -303), (Jun 18-21, 2007).
- Nair, G. N., Fagnani, F., Zampieri, S., and Evans, R. J. (2007), "Feedback control under data rate constraints: An overview", *Proceedings of the IEEE* Vol. 95 (1), pp. 108-137. .
- NAMUR (2011), "Wireless automation", <http://www.namur.de/index.php?id=189&L=2> (On-line: Jan 12, 2011)
- NaN (2011), "Netsurveyor-802.11 network discovery/ Wi-Fi Scanner", <http://nutsaboutnets.com/netsurveyor-wifi-scanner/> (On-line: Dec 12, 2011).
- Navigation Centre (NC) (2010), "LORAN-C", <http://www.navcen.uscg.gov/loran/default.html> (May. 14, 2010).
- Navman (2006), "Jupiter 30: 20-channel GPS receiver module", www.synes.co.th/product/gps-modules (Jul. 16, 2011).
- NC (2010), "Navigation Centre:, LORAN-C", from www.navcen.uscg.gov/loran (retrieved on May 14th, 2010).
- Nicholls, T. (2008), "How the energy industry works-an insider guide", Silverstone Communications Limited.
- NICT (2005), "The method of emitting standard time and frequency Signal Emissions", <http://jjy.nict.go.jp/jjy.html> (On-line: May 4, 2010).
- Niemann, L., Venzke, M., Renner, C., and Turau, V. (2009), "Clock synchronization of tinyOS-based sensor networks with DCF77". In *Proceedings of the 8th GI/ITG KuVS Fachgespräch "Drahtlose Sensornetze" (FGSN'09)*, Hamburg, Germany, pp. 45-47.
- NIST (2010), "NIST radio station WWVB", www.nist.gov/pml/div688/grp40/wwvb.cfm (On-line: May 4, 2010).
- Niu, J., Gao, Y., Guo, S., Tong, C., and Du, G. (2011), "An adaptive Wi-Fi rate selection algorithm for moving vehicles with motion prediction", 6th International Conference on FutureTech, Loutraki, Greece, (June 28-30, 2011).
- Nordic. (2011), "Bluetooth low energy wireless technology backgrounder", www.nordicsemi.com (On-line: Jun 14, 2011).
- NPL (2011), "MSF Bulletins", <http://www.npl.co.uk/science-technology/time-frequency/time/products-and-services/msf-bulletins> (Mar. 12, 2011).
- NPL (2010), "MSF Radio Time Signal", www.npl.co.uk/msf (Aug. 16, 2011).
- NPL (2010a), "Common problems with radio-controlled clocks", [www.npl.co.uk/science-technology/time-frequency/time/ common-clock-problems](http://www.npl.co.uk/science-technology/time-frequency/time/common-clock-problems) (Sep. 7, 2011).
- NPL (2007), "MSF radio time signal", <http://www.npl.co.uk/science-technology/timefrequency> (Oct. 4, 2011).

- NPL (2007a), "MSF: time from NPL", www.npl.co.uk/time/msf (Aug. 24, 2010).
- NPL (2007b), "NPL time & frequency services", www.npl.co.uk/upload/pdf/MSFTimeDateCode (Oct. 8, 2010).
- NRCC-National Research Council Canada (2010), "CHU broadcast codes", NRCC, Canada.
- Obaidat, M. S., Denko, M., and Woungang, I. (2011), "Pervasive Computing and Networking", John Wiley & Sons, London.
- Ohlin, M. (2007), "TrueTime Version 1.5 Reference Manual", www.control.ith.se/truetime (Accessed on-line on May 18, 2011).
- Paar, C., Pelzl, J. and Preneel, B. (2010), "Understanding Cryptography: A Textbook for Students and Practitioners", Springer, Berlin, Germany.
- Park, P. G., Fischione, C., and Johansson, K. H. (2007), "Experimental evaluation of power control algorithms for wireless sensor networks", 17th IFAC World Congress, Seoul, Korea, (June 6-11).
- Park, P. G., Aroujo, J., and Johansson, K. H. (2011), "Wireless networked control system co-design", International Conference on Networking, Sensing and Control, pp. 486-491, (Apr 11-13, 2011).
- Pennington, S., Bauge, T., and Murray, B. (2009), "Integrity-checking framework: an In-situ testing and validation framework for wireless sensor and actuator networks", Third International Conference on Sensor Technologies and Applications, Athens, Greece, pp. 575-579, (Jun 18-23, 2009).
- Pérez-Romero, J., Gelabert, X., and Sallent, O. (2009), "Radio resource management for heterogeneous wireless access networks", In: Heterogeneous Wireless Access Networks - Architectures and Protocols, Ed: E. Hossain, Springer.
- Pahlavan and Levesque (2005), "Wireless Information Networks", John Wiley and Sons, Toronto, Canada.
- Petersen, S. Carlsen, S. (2011), "Wireless instrumentation – Current status and future trends", Oil & Gas Telecommunications 2011, London, UK, (Mar. 23-24, 2011).
- Pister, K. S. J., and Dhortey, L. (2008), "TSMP: Time synchronized mesh protocol", Proceedings of the IASTED International Symposium of Distributed Sensor Networks, Florida, USA, (Nov 16-18).
- PoP (1884), "Political Geography of the United States Protocols of the Proceedings", Gibson brothers, USA.
- Rahim, A. (2010), "Interference mitigation techniques to support coexistence of ultra-wideband systems", Dresden: VOGT - Alle Rechte Vorbehalten.
- Ralston, J. (2007), "Improving plant production with wireless condition monitoring", <http://www.prosoft-technology.com/training/whitepapers/Improving-Plant-Production-with-Wireless-Condition-Monitoring.pdf> (Oct. 12, 2010).
- Ranganathan, P , and K Nygard.(2010), "Time synchronization in wireless sensor networks" A Survey. International Journal of UbiComp Vol. 1(2), pp. 92-102.
- Rao, Y. V. C. (2004), "Chemical Engineering Thermodynamics", Universities Press, India.

- Rashvand, H. F., Alcaraz Calero, J. M. (2012), "Distributed sensor systems: Practice and applications", John Wiley & Sons, Chippingham, United Kingdom.
- Raza, S., Slabbert, A., Voigt, T., and Landernäs, K. (2009) Security Considerations for the WirelessHART Protocol. In: 14th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'2009), 22 Sept 2009, Mallorca, Spain.
- Reijers, N., Halkes, G., and Langendoen, K. (2004), "Link layer measurements in sensor networks". In Proceedings of the 1st IEEE Conference on Mobile Ad-hoc and Sensor Systems, IEEE Computer Society, pp. 24–27.
- Ridoux, J. & Veitch, D. (2010), "Principles of robust timing over the internet", Communications of the ACM, Vol. 53, pp. 54-61.
- Riley, W. (2007), "Handbook of frequency stability analysis", NIST, USA.
- Rowe, A., R. Mangharam, and R. Rajkumar. (2008), "RT-Link: A global time-synchronized link protocol for sensor networks", Ad Hoc Networks, Vol. 6(8), pp. 1201-1220.
- Sai, B. (2009), "ISA100 Wireless Network", ISA, USA.
- Saifullah, A., Wu, C., Tiwari, P., Xu, Y., Fu, Y., Lu, C., and Chen, Y. (2012), "Near optimal rate selection for wireless control systems", Proceedings of the 18th IEEE Real-Time and Embedded Technology and Applications Symposium, pp. 231-240.
- Sauter, T. (2010), "The three generations of field-level networks—Evolution and compatibility issues", IEEE Transactions on Industrial Electronics, Vol. 57(11), pp. 3585-3595.
- Schaar, M. and Chou, A. P. (2007), "Multimedia over IP and Wireless Networks: Compression, Networking, and Systems". Elsevier, London.
- Schenato, L. (2007), "Foundations of control and estimation over lossy networks", Proceedings of the IEEE Vol. 95, No. 1, (Jan. 2007).
- Samad, T., McLaughlin, P., and Lu, J. (2007), "System architecture for process automation: Review and Trends", Journal of Process Control, Vol. 17, pp. 191-201.
- Saifullah, A., Lu, C., Xu, Y., and Chen, Y. (2010), "Real-Time Scheduling for WirelessHART Networks", Proceedings of the 31st IEEE Real-Time Systems Symposium, pp. 150-159.
- Shrivastava, V., Agrawal, D., Mishra, A., and Banerjee, S. (2007), "Understanding the limitations of transmit power control for indoor WLANs", 7th ACM SIGCOMM Conference on Internet Measurement, San Diego, pp.351-364, (Oct. 24-26, 2007).
- Shuaib, K., Alnuaimi, M., Boulmalf, M., Jawhar, K., Sallabi, F., and Lakas, A. (2007), "Performance evaluation of IEEE 802.15.4: Experimental and simulation results", Journal of Communications, Vol. 2(4), pp.29-37.
- Srinivasan, K and Levis, P. (2006), "RSSI is under appreciated" Proceedings of the Third Workshop on Embedded Networked Sensors, Harvard University, (May 30-31, 2006).
- Srinivasan, K., Dutta, P., Tavakoli, A., and Levis, P. (2010), "An empirical study of low-power wireless", ACM Transactions on Sensor Networks, 6(2), (pp.16-49).

- Schultz, S. (2007), "Wireless goes process automation – Challenges in hazardous areas" 4th European Conference on Electrical and Instrumentation Applications in the Petroleum & Chemical Industry, Paris, France, pp. 1-7, (Jun 13-15, 2007)
- SGER (2008), "Event-triggered control over sensor/actuator wireless networks", <http://www.cyphylab.ee.ucla.edu/Home/projects/event-triggered-control-over-wireless-sensor-actuator-networks> (May. 12, 2011)
- Sheth and Han (2003), "Adaptive power control and selective radio activation for low-power infrastructure-mode 802.11 LANS", IEEE workshop on mobile and wireless networking, 23rd International Conference on Distributed Computing Systems, pp. 812–818, (May. 19-22, 2003).
- Shin, S.Y., Park, H.S., and Kwon, W.H. (2007), "Mutual interference analysis of IEEE 802.15.4 and IEEE 802.11b", Computer Networks, 51(12).
- Siemens (2010), "Wireless HART at Siemens", Siemens, Germany.
- Sikora, A. (2007), "Wireless for Industrial and process automation-trends, challenges, and protocol", Available at: <http://www.baloerrach.de> (On-line: May. 10, 2009).
- Simcock, A. V. (1992), "Sir Howard Grubb's proposals for radio control of clocks and watches 1898-1899 [article]", Published in: Radio time : the radio-controlled clock and watch newsletter. - Vol.4/1 (Autumn), p.18-22 (1992).
- Sinha, D and Edward, R. D. (1998), "Introduction to computer-based imaging systems", Volume TT23, USA: SPIE - The International Society of Optical Engineering, ISBN 10: 0819421057 / 0-8194-2105-7.
- Sivrikaya, B. Yener (2004), "Time synchronization in sensor networks: A Survey", Network, IEEE, Vol. 18, No.4. (2004).
- SMI (2012), "Understanding the importance of satcomm and telecommunication channels", 5th annual conference on Oil and Gas Communications, (Mar. 21-22, 2012).
- Sommer, P. Wattenhofer, R. (2009), "Gradient clock synchronization in wireless sensor networks", IPSN '09 Proceedings on Information Processing in Sensor Networks.
- Song, J., Mok., A . K., Chen, D., and Nixon, M. (2005), "Challenges of wireless control in process industry", Workshop on Research Directions for Security and Networking in Critical Real-Time and Embedded Systems, <http://www.citeseerx.ist.psu.edu/viewdoc> (On-line: Aug 12, 2010).
- Song, J., Mok., A . K., Chen, D., and Nixon, M. (2006), "Improving PID Control with Unreliable Communications", ISA Publications, USA.
- Song, J., Mok., Han, S., A . K., Chen, D., Lucas, M., and Nixon, M. (2008), "WirelessHART: Applying wireless technology in real-time industrial process control", Proceedings of the 2008 IEEE Real-Time and Embedded Technology and Applications Symposium, Missouri, pp. 377-386, (April 22-24).
- Steven M. Kay (1993), "Fundamentals of statistical signal processing: estimation theory", Prentice-Hall, Upper Saddle River, NJ, USA.
- Stieglitz, K and Wollert, J. F. (2011), "Approach of using ultra-wideband-radio in industrial real-time ethernet networks", The 15th World Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, Florida, (July 19-22).
- Stoianov, I., Nachman, L., Madden, S., Tokmouline, T. (2007), "PIPENET: a wireless sensor network for pipeline monitoring. In 6th International Conference on Information

- Processing in Sensor Networks (IPSN'07), pp. 264-273, MIT, Cambridge, MA:ACM, Press, NY, USA.
- Suhonon, J., Kohvakka, M., Kaseva, V., and Hämäläinen, T.(2012), "Low-power wireless sensor networks: Protocols, services and applications", Springer, London.
- Sundararaman, Bharath, Ugo Buy, and Ajay D. Kshemkalyani.(2005), "Clock Synchronization for Wireless Sensor Networks: A Survey", Ad Hoc Networks 3(3), pp. 281-323.
- Taylor, G. W., Gagnepain, J. J., Meeker, T. R., Shuvalov, L. A. (1985), "Piezoelectricity", Gordon and Breach, USA.
- Texas Instruments, (2006), "CC2420: 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver", <http://www.ti.com/lit/ds/symlink/cc2420.pdf> (15th July 2012).
- Telit (2012), "JN3 Family", www.telit.com (On-line, Jul 12, 2012).
- Teng, Z. and Kim, K. (2010), "A Survey on Real-Time MAC Protocols in Wireless Sensor Networks," Communications and Network, Vol. 2 No. 2, 2010, pp. 104-112. doi: 10.4236/cn.2010.22017.
- Thomas, M.(1991), "Elements of Information Theory", John Wiley and Sons, New York, USA.
- Thomesse, J. P. (2005), "Fieldbus Technology in Industrial Automation". http://hal.inria.fr/docs/00/04/45/75/PDF/Thomesse-fieldbus_-_ieee.pdf (On-line: Aug 12, 2010).
- Tilborg, V., Henk, C.A., and Jajodia, S., (2011), "Encyclopedia of Cryptography and Security", Volume 1, Springer, Boston, USA.
- Tipsuwan, Y., & Chow, M.-Y., 2001. Network-based controller adaptation based on QoS negotiation and deterioration. 27th Annual Conference of the IEEE Industrial Electronics Society, Vol. 3, pp. 1794–1799, Denver, USA. .
- Tipsuwan, Y. and Chow, M-Y (2003), "Control methodologies in control systems", Control Engineering Practice, Vol. 11, pp. 1099-1111.
- Tipsuwan, Y. and Chow, M. Y. (2004), "Gain scheduler middleware: a methodology to enable existing controllers for networked control and teleoperation-part II: teleoperation," IEEE Transactions on Industrial Electronics, Vol. 51 (6) , pp. 1228-1237.
- Uchimura, Y.; Nasu, T. & Takahashi, M. (2007), "Time synchronized wireless sensor network and its application to building vibration measurement", 33rd Annual Conference of the IEEE Society on Industrial Electronics, pp. 2633 -2638.
- Vedantham, R. and Zhaoung, Z. (2006), "Addressing hazards in wireless sensor and actor networks", MobiCom, Vol. 10 (4).
- Vig, J. R. (2000), "Quartz crystal resonators and oscillators", Fort Monmouth, USA.
- Vilanova, R. (2012), "PID Control in the Third Millenium", Springer-Verlag, London.
- Viittala, M., Hämäläinen, M., and Iinatti, J. (2006), "Comparative studies of MB-OFDM and DS-UWB with co-existing systems in AWGN channel". The 17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Helsinki, Finland, (pp. 1336-1340), (Sept. 11-14).

- Wagner, R. S. (2010), "Standards-based wireless sensor networking protocols for spaceflight applications", Proceedings of IEEE Aerospace Conference, Big Sky, Montana, USA, pp. 1-7, (Mar. 2010).
- Wang, F., P. Zeng, and H. Yu.(2008), "Slot time synchronization for TDMA-Based Ad Hoc Networks", ISCST 2008: International Symposium on Computer Science and Computational Technology, Vol 2, Proceedings:(pp.544-548).
- Wang, F-Y and Liu, D. (2010), "Networked control systems-Theory and Applications", Springer, London.
- Wechsler, J. (1990), "The role of GPS in precise time and frequency dissemination", <http://ilrs.gsfc.nasa.gov> (On-line: May 2, 2010).
- Wedge, G. (2010), "Next-Gen wireless in control systems. Wireless as an enabler – imagine the possibilities", 23rd February [Presentation given at: IET Workshop on Next-Gen wireless in control systems]: IET London: Savoy Place, UK (Feb 23rd, 2010).
- Welch, G. and Bishop, G. (2006), "An Introduction to the Kalman Filter", University of North Carolina at Chapel Hill. http://www.cs.unc.edu/~welch/media/pdf/kalman_intro.pdf, (Retrieved on-line on 10th of Jun, 2010).
- Wheatley, C. (1999), "Self-Synchronizing a CDMA cellular network", www.eetasia.com/articles/CDMA (On-line: May. 4, 2010).
- WIA-PA (2009), "Industrial communication networks – Fieldbus specifications – WIA-PA communication network and communication profile" WIA-PA, China.
- WiCon (2010), "The WiCon Project", <http://www.wiconproject.com> (Dec. 1, 2010).
- Willig, A. (2003). "Polling-based MAC protocols for improving real-time performance in a wireless PROFIBUS", IEEE Transactions on Industrial Electronics, Vol. 50 (4), pp. 806-817.
- William, G. (2010), "Next-Gen Wireless in Control Systems. Wireless enabled mobile solutions", (Feb. 23, 2010) [Presentation given at: IET Workshop on Next-Gen wireless in control systems]: IET London: Savoy Place, UK.
- Willig, A., Matheus, K., and Wolisz, A. (2005), "Wireless technology in industrial networks", Proceedings of the IEEE, Vol. 93 (6), pp. 1130-1151.
- WiMon (2010), "Condition Monitoring WiMon 100 Wireless Vibration Sensor", ABB, Norway.
- WINA (2011), "Industrial wireless", <http://www.wina.org/> (Feb. 10, 2012).
- Winder, S. Carr, J. (2002), "Radio & RF Engineering", Newnes, Oxford.
- WirelessHART (2009), "Industrial communication network—Fieldbus specifications—WirelessHART communication network and communication profile, Edition 1.0, IEC/PAS 62591, 2009–01."
- Wu (2011), "High Performance Networking, Computing, and Communication Systems", Second Edition, Springer, Berlin.

- Xia, F. (2008), "QoS challenges and opportunities in wireless sensor/actuator networks", www.mdpi.org/sensors (On-line: Jan 12, 2011)
- Xia, I., Hu, C., and Chiang, P. (2011), "Ultra Wideband RF Transceiver Design in CMOS Technology, Ultra Wideband Communications: Novel Trends - System, Architecture and Implementation", ISBN: 978-953-307-461-0, InTech.
- Yang, T. C. (2006), "Networked control system: A Brief Survey", IEEE Proceedings: Control Theory Applications. Vol. 153 (4), pp. 403-412.
- Yang, G-Z. (2006), "Body Sensor Networks", Springer-Verlag, London.
- Yepez, J., Marti, P and Feurtes, J. M. (2002), "Control loop performance analysis over networked control systems", In Proceedings of the IEEE Industrial Electronics Conference, pp. Sevilla, Spain, pp. 2880-2885, (Nov 5-8, 2002).
- Yepez, J., Marti, P. and Fuertes, J.M. (2003), "Control Loop Scheduling Paradigm in Distributed Control Systems", The 29th Annual Conference on Industrial Electronics, IECON '03, pp. 1441-1446, (Nov 2-6, 2003).
- Yick, J., Mukherjee, B., and Ghosal. D. (2008), "Wireless sensor network survey", Computer Networks, Vol. 52, pp. 2292-2330, (April. 2008).
- Yokogawa (2011), "Wireless technology in industrial automation", http://www.yokogawa.com/de/dcs/funkloesungen/de_dokumente/ISA100-whitepaper.pdf (On-line: Jan. 12, 2012).
- Zhang, W., Braniky, M.S., and Phillips, S. M. (2001), "Stability of networked control systems", IEEE Control Systems Magazine, Vol. 21, pp. 84-99.
- Zhang, Y., Markham, P., Xia, T., Lang, C., Ye, Y., Wu, Z., Yuan, Z., Wang, I., and Liu, Y. (2010), "Wide-Area frequency monitoring network (FNET) architecture and applications", IEEE Transactions on Smart Grid, Vol. 1 (2), pp. 159-167.
- Zhong, T., Mengjin, C., Peng, Z., and Hong, W., (2010), "Real-time communication in WIA-PA industrial wireless networks", International Conference on Computer Science and Information Technology, Chengdu, China, Vol. 2, pp. 600-605, (Jul 9-11, 2010).
- Zhou, G., He, T., Krishnamurthy, S., and Stankovic, J. A. (2004), "Impact of radio irregularity on wireless sensor networks", In the Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services (MobiSys '04). ACM, pp. 125–138.
- Züge, C. T. Y., Pereira, S. L., and Dias, E. M. (2010), "Integration of information technology and automation: Facilitators and barriers", WSEAS Transactions on Systems and Control, 5(5), pp.372-381.
- Zurawski, R. (2005), "The Industrial Communication Technology Handbook", CRC Press, Florida, USA.